Contents

NSX Administration Guide 12

1 System Requirements for NSX 13

2 Ports and Protocols Required by NSX 16

3 Overview of NSX 19
   NSX Components 20
      Data Plane 21
      Control Plane 22
      Management Plane 23
      Consumption Platform 23
   NSX Edge 23
   NSX Services 26

4 Overview of Cross-vCenter Networking and Security 28
   Benefits of Cross-vCenter NSX 28
   How Cross-vCenter NSX Works 29
   Support Matrix for NSX Services in Cross-vCenter NSX 30
   Universal Controller Cluster 32
   Universal Transport Zone 32
   Universal Logical Switches 32
   Universal Logical (Distributed) Routers 32
   Universal Firewall Rules 33
   Universal Network and Security Objects 33
   Cross-vCenter NSX Topologies 34
      Multi-Site and Single Site Cross-vCenter NSX 34
      Local Egress 36
   Modifying NSX Manager Roles 37

5 Transport Zones 39
   Add a Transport Zone 41
   View and Edit a Transport Zone 43
   Expand a Transport Zone 43
   Contract a Transport Zone 43
   Controller Disconnected Operation (CDO) Mode 44
      Enable Controller Disconnected Operation (CDO) Mode 44
      Disable Controller Disconnected Operation (CDO) Mode 45
6 Logical Switches 47
   Add a Logical Switch 49
   Add a Logical Switch 49
   Connect a Logical Switch to an NSX Edge 51
   Deploy Services on a Logical Switch 52
   Connect Virtual Machines to a Logical Switch 52
   Test Logical Switch Connectivity 53
   Prevent Spoofing on a Logical Switch 53
   Edit a Logical Switch 53
   Logical Switch Scenario 54
      John Admin Assigns Segment ID Pool and Multicast Address Range to NSX Manager 56
      John Admin Configures VXLAN Transport Parameters 57
      John Admin Adds a Transport Zone 58
      John Admin Creates a Logical Switch 58

7 Configuring Hardware Gateway 59
   Scenario: Hardware Gateway Sample Configuration 60
      Set Up the Replication Cluster 61
      Connect the Hardware Gateway to the NSX Controllers 62
      Add Hardware Gateway Certificate 63
      Bind the Logical Switch to the Physical Switch 65

8 L2 Bridges 67
   Add L2 Bridge 68
   Add L2 Bridge to a Logically Routed Environment 69

9 Routing 71
   Add a Logical (Distributed) Router 71
   Add an Edge Services Gateway 84
   Specify Global Configuration 94
   NSX Edge Configuration 96
      Working with Certificates 96
      FIPS Mode 101
      Managing Appliances 103
      Managing NSX Edge Appliance Resource Reservations 104
      Working with Interfaces 106
      Add a Sub Interface 109
      Change Auto Rule Configuration 112
      Change CLI Credentials 112
      About High Availability 112
      Force Sync NSX Edge with NSX Manager 115
Configure Syslog Servers for NSX Edge 115
View the Status of an NSX Edge 116
Redeploy NSX Edge 116
Download Tech Support Logs for NSX Edge 118
Add a Static Route 119
Configure OSPF on a Logical (Distributed) Router 120
Configure OSPF on an Edge Services Gateway 126
Configure BGP 131
Configure Route Redistribution 135
View the NSX Manager Locale ID 136
Configure Locale ID on a Universal Logical (Distributed) Router 136
Configure Locale ID on a Host or Cluster 137

10 Logical Firewall 139
Distributed Firewall 139
Session Timers 141
IP Discovery for Virtual Machines 144
Exclude Virtual Machines from Firewall Protection 145
View Firewall CPU and Memory Threshold Events 146
Distributed Firewall Resource Utilization 146
Edge Firewall 147
Working with NSX Edge Firewall Rules 147
Working with Firewall Rule Sections 157
Add a Firewall Rule Section 157
Merge Firewall Rule Sections 158
Delete a Firewall Rule Section 158
Working with Firewall Rules 159
Edit the Default Distributed Firewall Rule 159
Add a Distributed Firewall Rule 160
Force Sync Distributed Firewall Rules 165
Add a Universal Firewall Rule 165
Firewall Rules with a Custom Layer 3 Protocol 169
Save an Unpublished Configuration 170
Load a Saved Firewall Configuration 170
Filter Firewall Rules 171
Change the Order of a Firewall Rule 171
Delete a Firewall Rule 171
Firewall Logs 172

11 Identity Firewall Overview 177
Identity Firewall Workflow 178
12 Working with Active Directory Domains  179
   Register a Windows Domain with NSX Manager  179
   Synchronize a Windows Domain with Active Directory  181
   Edit a Windows Domain  181
   Enable Security Read-Only Log Access on Windows 2008  182
   Verifying Directory Privileges  183

13 Using SpoofGuard  184
   Create a SpoofGuard Policy  185
   Approve IP Addresses  186
   Edit an IP Address  186
   Clear an IP Address  187

14 Virtual Private Networks (VPN)  189
   SSL VPN-Plus Overview  189
      Configure Network Access SSL VPN-Plus  191
      Install SSL VPN-Plus Client  200
      Configure Proxy Server Settings in SSL VPN-Plus Client  202
      SSL VPN-Plus Logs  203
      Edit Client Configuration  204
      Edit General Settings  204
      Edit Web Portal Design  205
      Working with IP Pools for SSL VPN  206
      Working with Private Networks  207
      Working with Installation Packages  209
      Working with Users  209
      Working with Login and Logoff Scripts  210
   IPSec VPN Overview  211
      Configuring IPSec VPN Service  213
      Edit IPSec VPN Service  217
      Disable IPSec VPN Site  217
      Delete IPSec VPN Site  218
      IPSec VPN Configuration Examples  218
   L2 VPN Overview  229
      Configuring L2 VPN  230
      Configure L2 VPN Server  236
      Add Peer Sites  237
      Enable L2 VPN Service on Server  238
      Configure L2 VPN Client  239
      Enable L2 VPN Service on Client  240
      Configure Standalone Edge as L2 VPN Client  241
15 Logical Load Balancer 244

Setting Up Load Balancing 248
- Configure Load Balancer Service 250
- Create a Service Monitor 251
- Add a Server Pool 256
- Create an Application Profile 259
- Add an Application Rule 263
- Add Virtual Servers 270

Managing Application Profiles 271
- Edit an Application Profile 271
- Configure SSL Termination for a Load Balancer 271
- Delete an Application Profile 272

Managing Service Monitors 273
- Edit a Service Monitor 273
- Delete a Service Monitor 273

Managing Server Pools 274
- Edit a Server Pool 274
- Configure a Load Balancer to Use Transparent Mode 274
- Delete a Server Pool 275
- Show Pool Statistics 275

Managing Virtual Servers 276
- Edit a Virtual Server 276
- Delete a Virtual Server 276

Managing Application Rules 277
- Edit an Application Rule 277
- Delete an Application Rule 277

Load Balance Web Servers using NTLM Authentication 278

Load Balancer HTTP Connection Modes 278

Scenarios for NSX Load Balancer Configuration 280
- Configure a One-Armed Load Balancer 280
- Scenario: Configure NSX Load Balancer for Platform Service Controller 285
- Scenario: SSL Offloading 289
- Scenario: Import SSL Certificate 294
- Scenario: SSL Passthrough 297
- Scenario: SSL Client and Server Authentication 298

16 Other Edge Services 301

Managing DHCP Service 301
Add a DHCP IP Pool 301
Enable the DHCP Service 303
Edit DHCP IP Pool 304
Add a DHCP Static Binding 304
Edit DHCP Binding 305
Configuring DHCP Relay 305
Add DHCP Relay Server 306
Add Relay Agents 307
Configure a DNS Server 307

17 Service Composer 309
Using Service Composer 311
Create a Security Group in Service Composer 312
Create a Security Policy 314
Apply a Security Policy to a Security Group 319
Service Composer Canvas 319
Working with Security Tags 322
Unique ID Selection 322
View Applied Security Tags 323
Create a Security Tag 323
Assign a Security Tag 324
Edit a Security Tag 324
Delete a Security Tag 325
Viewing Effective Services 325
View Effective Services on a Security Policy 325
View Service Failures for a Security Policy 326
View Effective Services on a Virtual Machine 326
Working with Security Policies 326
Manage Security Policy Priority 327
Edit a Security Policy 327
Delete a Security Policy 327
Service Composer Scenarios 328
Quarantining Infected Machines Scenario 328
Backing up Security Configurations 332
Importing and Exporting Security Policy Configurations 334
Export a Security Policy Configuration 334
Import a Security Policy Configuration 335

18 Guest Introspection 337
Install Guest Introspection on Host Clusters 338
Install the Guest Introspection Thin Agent on Windows Virtual Machines 339
Install the Guest Introspection Thin Agent on Linux Virtual Machines 341
View Guest Introspection Status 343
Guest Introspection Audit Messages 343
Collecting Guest Introspection Troubleshooting Data 344
Uninstall a Guest Introspection Module 344
    Uninstall Guest Introspection for Linux 345

19 Network Extensibility 346
    Distributed Service Insertion 347
    Edge-Based Service Insertion 347
    Integrating Third Party Services 347
    Deploy a Partner Service 348
    Consuming Vendor Services through Service Composer 349
    Redirecting Traffic to a Vendor Solution through Logical Firewall 349
    Using a Partner Load Balancer 350
    Remove Third-Party Integration 351

20 User Management 352
    NSX Users and Permissions by Feature 352
    Configure Single Sign On 356
    Managing User Rights 358
    Managing the Default User Account 358
    Assign a Role to a vCenter User 359
    Create a User with Web Interface Access Using CLI 362
    Edit a User Account 364
    Change a User Role 364
    Disable or Enable a User Account 365
    Delete a User Account 365

21 Network and Security Objects 367
    Working with IP Address Groups 367
        Create an IP Address Group 367
        Edit an IP Address Group 368
        Delete an IP Address Group 369
    Working with MAC Address Groups 369
        Create a MAC Address Group 369
        Edit a MAC Address Group 370
        Delete a MAC Address Group 370
    Working with IP Pools 370
        Create an IP Pool 370
        Edit an IP Pool 371
Delete IP Pool 371

Working with Security Groups 371
  Create a Security Group 372
  Edit a Security Group 375
  Delete a Security Group 375

Working with Services and Service Groups 376
  Create a Service 376
  Create a Service Group 376
  Edit a Service or Service Group 377
  Delete a Service or Service Group 377

22 Operations and Management 379

Using the NSX Dashboard 379
  Check Communication Channel Health 383

NSX Controller 383
  Change Controller Password 383
  Download Technical Support Logs for NSX Controller 384
  Configuring a Syslog Server for NSX Controller 384

Change VXLAN Port 385

Customer Experience Improvement Program 387
  Edit the Customer Experience Improvement Program Option 387

About NSX Logs 388

Audit Logs 389
  Using NSX Ticket Logger 389
  View the Audit Log 390

System Events 390
  View the System Event Report 390
  Format of a System Event 390
  Alarms 391
  Format of an Alarm 392

Working with SNMP Traps 392

Management System Settings 396
  Log In to the NSX Manager Virtual Appliance 396
  Edit the NSX Manager Date and Time 397
  Configure a Syslog Server for NSX Manager 397
  Change FIPS Mode and TLS Settings on NSX Manager 398
  Edit DNS Servers 399
  Edit Lookup Service Details 400
  Edit vCenter Server 400
  Download Technical Support Logs for NSX 400
  NSX Manager SSL Certification 401
NSX Backup and Restore 404
   Back Up and Restore NSX Manager 404
   Back Up vSphere Distributed Switches 410
   Back Up vCenter 410

Flow Monitoring 410
   View Flow Monitoring Data 411
   Change the Date Range of the Flow Monitoring Charts 413
   Add or Edit a Firewall Rule from the Flow Monitoring Report 413
   View Live Flow 414
   Configure Flow Monitoring Data Collection 415
   Configure IPFIX 417

Application Rule Manager 428
   Create a Monitoring Session 429
   Analyze Flows 430
   Flow Consolidation and Customization 430
   Customizing Services in Flow Records 432
   Customizing Source and Destination in Flow Records 433
   Creating Firewall Rules from Application Rule Manager 435
   Publishing and Managing Firewall Rules From Application Rule Manager 436

Activity Monitoring 437
   Set Up Activity Monitoring 438
   Activity Monitoring Scenarios 442
   Enable Data Collection 444
   View Virtual Machine Activity Report 445
   View Inbound Activity 446
   View Outbound Activity 448
   View Interaction between Inventory Containers 449
   View Outbound AD Group Activity 451
   Override Data Collection 452

Endpoint Monitoring Data Collection 452
   Endpoint Monitoring 453

Traceflow 455
   About Traceflow 455
   Use Traceflow for Troubleshooting 457
NSX Administration Guide

The NSX Administration Guide describes how to configure, monitor, and maintain the VMware NSX® for vSphere® system by using the NSX Manager user interface and the vSphere Web Client. The information includes step-by-step configuration instructions, and suggested best practices.

Intended Audience

This manual is intended for anyone who wants to install or use NSX in a VMware vCenter environment. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with VMware vSphere, including VMware ESXi, vCenter Server, and the vSphere Web Client.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.
System Requirements for NSX

Before you install or upgrade NSX, consider your network configuration and resources. You can install one NSX Manager per vCenter Server, one instance of Guest Introspection per ESXi™ host, and multiple NSX Edge instances per datacenter.

**Hardware**

This table lists the hardware requirements for NSX appliances.

| Table 1-1. Hardware Requirements for Appliances |
|---|---|---|---|
| Appliance | Memory | vCPU | Disk Space |
| NSX Manager | 16 GB (24 GB for larger NSX deployments) | 4 (8 for larger NSX deployments) | 60 GB |
| NSX Controller | 4 GB | 4 | 28 GB |
| NSX Edge | Compact: 512 MB Large: 1 GB Quad Large: 2 GB X-Large: 8 GB | Compact: 1 Large: 2 Quad Large: 4 X-Large: 6 | Compact, Large: 1 disk 584 MB + 1 disk 512 MB Quad Large: 1 disk 584 MB + 2 disks 512 MB X-Large: 1 disk 584 MB + 1 disk 2 GB + 1 disk 512 MB |
| Guest Introspection | 2 GB | 2 | 5 GB (Provisioned space is 6.26 GB) |

As a general guideline, increase NSX Manager resources to 8 vCPU and 24 GB of RAM if your NSX-managed environment contains more than 256 hypervisors or more than 2000 VMs.

For specific sizing details contact VMware support.

For information about increasing the memory and vCPU allocation for your virtual appliances, see Allocate Memory Resources, and Change the Number of Virtual CPUs in vSphere Virtual Machine Administration.

The provisioned space for a Guest Introspection appliance shows as 6.26 GB for Guest Introspection. This is because vSphere ESX Agent Manager creates a snapshot of the service VM to create fast clones, when multiple hosts in a cluster shares a storage. For more information on how to disable this option via ESX Agent Manager, refer to ESX Agent Manager documentation.
Network Latency

You should ensure that the network latency between components is at or below the maximum latency described.

Table 1-2. Maximum network latency between components

<table>
<thead>
<tr>
<th>Components</th>
<th>Maximum latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager and NSX Controllers</td>
<td>150 ms RTT</td>
</tr>
<tr>
<td>NSX Manager and ESXi hosts</td>
<td>150 ms RTT</td>
</tr>
<tr>
<td>NSX Manager and vCenter Server system</td>
<td>150 ms RTT</td>
</tr>
<tr>
<td>NSX Manager and NSX Manager in a cross-vCenter NSX environment</td>
<td>150 ms RTT</td>
</tr>
<tr>
<td>NSX Controller and ESXi hosts</td>
<td>150 ms RTT</td>
</tr>
</tbody>
</table>

Software


For recommended versions of NSX, vCenter Server, and ESXi, see the release notes for the version of NSX to which you are upgrading. Release notes are available at the NSX for vSphere documentation site: [https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html](https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html).

For an NSX Manager to participate in a cross-vCenter NSX deployment the following conditions are required:

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>6.2 or later</td>
</tr>
<tr>
<td>NSX Controller</td>
<td>6.2 or later</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>ESXi</td>
<td>ESXi 6.0 or later</td>
</tr>
<tr>
<td></td>
<td>Host clusters prepared with NSX 6.2 or later VIBs</td>
</tr>
</tbody>
</table>

To manage all NSX Managers in a cross-vCenter NSX deployment from a single vSphere Web Client, you must connect your vCenter Servers in Enhanced Linked Mode. See Using Enhanced Linked Mode in [vCenter Server and Host Management](https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html).

Client and User Access

The following items are required to manage your NSX environment:

- Forward and reverse name resolution. This is required if you have added ESXi hosts by name to the vSphere inventory, otherwise NSX Manager cannot resolve the IP addresses.
- Permissions to add and power on virtual machines
- Access to the datastore where you store virtual machine files, and the account permissions to copy files to that datastore
- Cookies must be enabled on your Web browser to access the NSX Manager user interface.
- Port 443 must be open between the NSX Manager and the ESXi host, the vCenter Server, and the NSX appliances to be deployed. This port is required to download the OVF file on the ESXi host for deployment.
- A Web browser that is supported for the version of vSphere Web Client you are using. See Using the vSphere Web Client in the vCenter Server and Host Management documentation for details.
The following ports must be open for NSX to operate properly.

**Note** If you have a cross-vCenter NSX environment and your vCenter Server systems are in Enhanced Linked Mode, each NSX Manager appliance must have the required connectivity to each vCenter Server system in the environment to manage any NSX Manager from any vCenter Server system.

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
<th>Sensitive</th>
<th>TLS</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client PC</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>NSX Manager Administrative Interface</td>
<td>No</td>
<td>Yes</td>
<td>PAM Authentication</td>
</tr>
<tr>
<td>Client PC</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>NSX Manager VIB Access</td>
<td>No</td>
<td>No</td>
<td>PAM Authentication</td>
</tr>
<tr>
<td>ESXi Host</td>
<td>vCenter Server</td>
<td>443</td>
<td>TCP</td>
<td>ESXi Host Preparation</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>vCenter Server</td>
<td>ESXi Host</td>
<td>443</td>
<td>TCP</td>
<td>ESXi Host Preparation</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>ESXi Host</td>
<td>NSX Manager</td>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>No</td>
<td>Yes</td>
<td>RabbitMQ User/Password</td>
</tr>
<tr>
<td>ESXi Host</td>
<td>NSX Controller</td>
<td>1234</td>
<td>TCP</td>
<td>User World Agent Connection</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NSX Controller</td>
<td>NSX Controller</td>
<td>2878, 2888, 3888</td>
<td>TCP</td>
<td>Controller Cluster - State Sync</td>
<td>No</td>
<td>Yes</td>
<td>IPsec</td>
</tr>
<tr>
<td>NSX Controller</td>
<td>NSX Controller</td>
<td>7777</td>
<td>TCP</td>
<td>Inter-Controller RPC Port</td>
<td>No</td>
<td>Yes</td>
<td>IPsec</td>
</tr>
<tr>
<td>NSX Controller</td>
<td>NSX Controller</td>
<td>30865</td>
<td>TCP</td>
<td>Controller Cluster - State Sync</td>
<td>No</td>
<td>Yes</td>
<td>IPsec</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>NSX Controller</td>
<td>443</td>
<td>TCP</td>
<td>Controller to Manager Communication</td>
<td>No</td>
<td>Yes</td>
<td>User/Password</td>
</tr>
<tr>
<td>NSX Manager</td>
<td>vCenter Server</td>
<td>443</td>
<td>TCP</td>
<td>vSphere Web Access</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### Table 2-1. Ports and Protocols Required by NSX for vSphere (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
<th>Sensitive</th>
<th>TLS</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager</td>
<td>vCenter Server</td>
<td>902</td>
<td>TCP</td>
<td>vSphere Web Access</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>ESXi Host</td>
<td>443</td>
<td>TCP</td>
<td>Management and provisioning connection</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>ESXi Host</td>
<td>902</td>
<td>TCP</td>
<td>Management and provisioning connection</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>DNS Server</td>
<td>53</td>
<td>TCP</td>
<td>DNS client connection</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>DNS Server</td>
<td>53</td>
<td>UDP</td>
<td>DNS client connection</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Server</td>
<td>514</td>
<td>TCP</td>
<td>Syslog connection</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>Syslog Server</td>
<td>514</td>
<td>UDP</td>
<td>Syslog connection</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>NTP Time Server</td>
<td>123</td>
<td>TCP</td>
<td>NTP client connection</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>NTP Time Server</td>
<td>123</td>
<td>UDP</td>
<td>NTP client connection</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>vCenter Server</td>
<td>NSX Manager</td>
<td>80</td>
<td>TCP</td>
<td>Host Preparation</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>REST Client</td>
<td>NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>NSX Manager REST API</td>
<td>No</td>
<td>Yes</td>
<td>User/Password</td>
</tr>
<tr>
<td>VTEP</td>
<td>VTEP</td>
<td>8472</td>
<td>UDP</td>
<td>Transport network encapsulation between VTEPs</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(default in new installs of NSX 6.2.3 and later)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESXi Host</td>
<td>ESXi Host</td>
<td>6999</td>
<td>UDP</td>
<td>ARP on VLAN LIFs</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ESXi Host</td>
<td>NSX Manager</td>
<td>8301, 8302</td>
<td>UDP</td>
<td>DVS Sync</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NSX Manager</td>
<td>ESXi Host</td>
<td>8301, 8302</td>
<td>UDP</td>
<td>DVS Sync</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Guest Introspection VM</td>
<td>NSX Manager</td>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>No</td>
<td>Yes</td>
<td>RabbitMQ User/Password</td>
</tr>
<tr>
<td>Source</td>
<td>Target</td>
<td>Port</td>
<td>Protocol</td>
<td>Purpose</td>
<td>Sensitive</td>
<td>TLS</td>
<td>Authentication</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>------</td>
<td>----------</td>
<td>---------</td>
<td>-----------</td>
<td>-----</td>
<td>----------------</td>
</tr>
<tr>
<td>Primary NSX Manager</td>
<td>Secondary NSX Manager</td>
<td>443</td>
<td>TCP</td>
<td>Cross-vCenter NSX Universal Sync Service</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Primary NSX Manager</td>
<td>vCenter Server</td>
<td>443</td>
<td>TCP</td>
<td>vSphere API</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Secondary NSX Manager</td>
<td>vCenter Server</td>
<td>443</td>
<td>TCP</td>
<td>vSphere API</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Primary NSX Manager</td>
<td>NSX Universal Controller Cluster</td>
<td>443</td>
<td>TCP</td>
<td>NSX Controller REST API</td>
<td>No</td>
<td>Yes</td>
<td>User/Password</td>
</tr>
<tr>
<td>Secondary NSX Manager</td>
<td>NSX Universal Controller Cluster</td>
<td>443</td>
<td>TCP</td>
<td>NSX Controller REST API</td>
<td>No</td>
<td>Yes</td>
<td>User/Password</td>
</tr>
<tr>
<td>ESXi Host</td>
<td>NSX Universal Controller Cluster</td>
<td>1234</td>
<td>TCP</td>
<td>NSX Control Plane Protocol</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ESXi Host</td>
<td>Primary NSX Manager</td>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>No</td>
<td>Yes</td>
<td>RabbitMQ User/Password</td>
</tr>
<tr>
<td>ESXi Host</td>
<td>Secondary NSX Manager</td>
<td>5671</td>
<td>TCP</td>
<td>RabbitMQ</td>
<td>No</td>
<td>Yes</td>
<td>RabbitMQ User/Password</td>
</tr>
</tbody>
</table>
Overview of NSX

IT organizations have gained significant benefits as a direct result of server virtualization. Server consolidation reduced physical complexity, increased operational efficiency and the ability to dynamically re-purpose underlying resources to quickly and optimally meet the needs of increasingly dynamic business applications.

VMware’s Software Defined Data Center (SDDC) architecture is now extending virtualization technologies across the entire physical data center infrastructure. VMware NSX®, the network virtualization platform, is a key product in the SDDC architecture. With NSX, virtualization delivers for networking what it has already delivered for compute and storage. In much the same way that server virtualization programmatically creates, snapshots, deletes and restores software-based virtual machines (VMs), NSX network virtualization programmatically creates, snapshots, deletes, and restores software-based virtual networks. The result is a completely transformative approach to networking that not only enables data center managers to achieve orders of magnitude better agility and economics, but also allows for a vastly simplified operational model for the underlying physical network. With the ability to be deployed on any IP network, including both existing traditional networking models and next-generation fabric architectures from any vendor, NSX is a completely non-disruptive solution. In fact, with NSX, the physical network infrastructure you already have is all you need to deploy a software-defined data center.
The figure above draws an analogy between compute and network virtualization. With server virtualization, a software abstraction layer (server hypervisor) reproduces the familiar attributes of an x86 physical server (for example, CPU, RAM, Disk, NIC) in software, allowing them to be programatically assembled in any arbitrary combination to produce a unique VM in a matter of seconds.

With network virtualization, the functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewalling, QoS, and load balancing) in software. As a result, these services can be programatically assembled in any arbitrary combination, to produce unique, isolated virtual networks in a matter of seconds.

With network virtualization, benefits similar to server virtualization are derived. For example, just as VMs are independent of the underlying x86 platform and allow IT to treat physical hosts as a pool of compute capacity, virtual networks are independent of the underlying IP network hardware and allow IT to treat the physical network as a pool of transport capacity that can be consumed and repurposed on demand. Unlike legacy architectures, virtual networks can be provisioned, changed, stored, deleted, and restored programmatically without reconfiguring the underlying physical hardware or topology. By matching the capabilities and benefits derived from familiar server and storage virtualization solutions, this transformative approach to networking unleashes the full potential of the software-defined data center.

NSX can be configured through the vSphere Web Client, a command-line interface (CLI), and a REST API.

This chapter includes the following topics:

- NSX Components
- NSX Edge
- NSX Services

**NSX Components**

This section describes the components of the NSX solution.
Note that a cloud management platform (CMP) is not a component of NSX, but NSX provides integration into virtually any CMP via the REST API and out-of-the-box integration with VMware CMPs.

**Data Plane**

The NSX data plane consists of the NSX vSwitch, which is based on the vSphere Distributed Switch (VDS) with additional components to enable services. NSX kernel modules, userspace agents, configuration files, and install scripts are packaged in VIBs and run within the hypervisor kernel to provide services such as distributed routing and logical firewall and to enable VXLAN bridging capabilities.

The NSX vSwitch (vDS-based) abstracts the physical network and provides access-level switching in the hypervisor. It is central to network virtualization because it enables logical networks that are independent of physical constructs, such as VLANs. Some of the benefits of the vSwitch are:

- Support for overlay networking with protocols (such as VXLAN) and centralized network configuration. Overlay networking enables the following capabilities:
  - Reduced use of VLAN IDs in the physical network.
  - Creation of a flexible logical Layer 2 (L2) overlay over existing IP networks on existing physical infrastructure without the need to re-architect any of the data center networks
  - Provision of communication (east–west and north–south), while maintaining isolation between tenants
  - Application workloads and virtual machines that are agnostic of the overlay network and operate as if they were connected to a physical L2 network
Facilitates massive scale of hypervisors

Multiple features—such as Port Mirroring, NetFlow/IPFIX, Configuration Backup and Restore, Network Health Check, QoS, and LACP—provide a comprehensive toolkit for traffic management, monitoring, and troubleshooting within a virtual network.

The logical routers can provide L2 bridging from the logical networking space (VXLAN) to the physical network (VLAN).

The gateway device is typically an NSX Edge virtual appliance. NSX Edge offers L2, L3, perimeter firewall, load balancing, and other services such as SSL VPN and DHCP.

**Control Plane**

The NSX control plane runs in the NSX Controller cluster. NSX Controller is an advanced distributed state management system that provides control plane functions for NSX logical switching and routing functions. It is the central control point for all logical switches within a network and maintains information about all hosts, logical switches (VXLANs), and distributed logical routers.

The controller cluster is responsible for managing the distributed switching and routing modules in the hypervisors. The controller does not have any dataplane traffic passing through it. Controller nodes are deployed in a cluster of three members to enable high-availability and scale. Any failure of the controller nodes does not impact any data-plane traffic.

NSX Controllers work by distributing network information to hosts. To achieve a high level of resiliency the NSX Controller is clustered for scale out and HA. NSX Controllers must be deployed in a three-node cluster. The three virtual appliances provide, maintain, and update the state of all network functioning within the NSX domain. NSX Manager is used to deploy NSX Controller nodes.

The three NSX Controller nodes form a control cluster. The controller cluster requires a quorum (also called a majority) in order to avoid a "split-brain scenario." In a split-brain scenario, data inconsistencies originate from the maintenance of two separate data sets that overlap. The inconsistencies can be caused by failure conditions and data synchronization issues. Having three controller nodes ensures data redundancy in case of failure of one NSX Controller node.

A controller cluster has several roles, including:

- API provider
- Persistence server
- Switch manager
- Logical manager
- Directory server

Each role has a master controller node. If a master controller node for a role fails, the cluster elects a new master for that role from the available NSX Controller nodes. The new master NSX Controller node for that role reallocates the lost portions of work among the remaining NSX Controller nodes.
NSX supports three logical switch control plane modes: multicast, unicast and hybrid. Using a controller cluster to manage VXLAN-based logical switches eliminates the need for multicast support from the physical network infrastructure. You don’t have to provision multicast group IP addresses, and you also don’t need to enable PIM routing or IGMP snooping features on physical switches or routers. Thus, the unicast and hybrid modes decouple NSX from the physical network. VXLANs in unicast control-plane mode do not require the physical network to support multicast in order to handle the broadcast, unknown unicast, and multicast (BUM) traffic within a logical switch. The unicast mode replicates all the BUM traffic locally on the host and requires no physical network configuration. In the hybrid mode, some of the BUM traffic replication is offloaded to the first hop physical switch to achieve better performance. Hybrid mode requires IGMP snooping on the first-hop switch and access to an IGMP querier in each VTEP subnet.

**Management Plane**

The NSX management plane is built by the NSX Manager, the centralized network management component of NSX. It provides the single point of configuration and REST API entry-points.

The NSX Manager is installed as a virtual appliance on any ESX™ host in your vCenter Server environment. NSX Manager and vCenter have a one-to-one relationship. For every instance of NSX Manager, there is one vCenter Server. This is true even in a cross-vCenter NSX environment.

In a cross-vCenter NSX environment, there is both a primary NSX Manager and one or more secondary NSX Managers. The primary NSX Manager allows you to create and manage universal logical switches, universal logical (distributed) routers and universal firewall rules. Secondary NSX Managers are used to manage networking services that are local to that specific NSX Manager. There can be up to seven secondary NSX Managers associated with the primary NSX Manager in a cross-vCenter NSX environment.

**Consumption Platform**

The consumption of NSX can be driven directly through the NSX Manager user interface, which is available in the vSphere Web Client. Typically end users tie network virtualization to their cloud management platform for deploying applications. NSX provides rich integration into virtually any CMP through REST APIs. Out-of-the-box integration is also available through VMware vCloud Automation Center, vCloud Director, and OpenStack with the Neutron plug-in for NSX.

**NSX Edge**

You can install NSX Edge as an edge services gateway (ESG) or as a distributed logical router (DLR).
**Edge Services Gateway**

The ESG gives you access to all NSX Edge services such as firewall, NAT, DHCP, VPN, load balancing, and high availability. You can install multiple ESG virtual appliances in a data center. Each ESG virtual appliance can have a total of ten uplink and internal network interfaces. With a trunk, an ESG can have up to 200 subinterfaces. The internal interfaces connect to secured port groups and act as the gateway for all protected virtual machines in the port group. The subnet assigned to the internal interface can be a publicly routed IP space or a NATed/routed RFC 1918 private space. Firewall rules and other NSX Edge services are enforced on traffic between network interfaces.

Uplink interfaces of ESGs connect to uplink port groups that have access to a shared corporate network or a service that provides access layer networking. Multiple external IP addresses can be configured for load balancer, site-to-site VPN, and NAT services.

**Distributed Logical Router**

The DLR provides East-West distributed routing with tenant IP address space and data path isolation. Virtual machines or workloads that reside on the same host on different subnets can communicate with one another without having to traverse a traditional routing interface.

A logical router can have eight uplink interfaces and up to a thousand internal interfaces. An uplink interface on a DLR generally peers with an ESG, with an intervening Layer 2 logical transit switch between the DLR and the ESG. An internal interface on a DLR peers with a virtual machine hosted on an ESXi hypervisor with an intervening logical switch between the virtual machine and the DLR.

The DLR has two main components:

- The DLR control plane is provided by the DLR virtual appliance (also called a control VM). This VM supports dynamic routing protocols (BGP and OSPF), exchanges routing updates with the next Layer 3 hop device (usually the edge services gateway) and communicates with the NSX Manager and the NSX Controller cluster. High-availability for the DLR virtual appliance is supported through active-standby configuration: a pair of virtual machines functioning in active/standby modes are provided when you create the DLR with HA enabled.

- At the data-plane level, there are DLR kernel modules (VIBs) that are installed on the ESXi hosts that are part of the NSX domain. The kernel modules are similar to the line cards in a modular chassis supporting Layer 3 routing. The kernel modules have a routing information base (RIB) (also known as a routing table) that is pushed from the controller cluster. The data plane functions of route lookup and ARP entry lookup are performed by the kernel modules. The kernel modules are equipped with logical interfaces (called LIFs) connecting to the different logical switches and to any VLAN-backed port-groups. Each LIF has assigned an IP address representing the default IP gateway for the logical L2 segment it connects to and a vMAC address. The IP address is unique for each LIF, whereas the same vMAC is assigned to all the defined LIFs.
1 A DLR instance is created from the NSX Manager UI (or with API calls), and routing is enabled, using either OSPF or BGP.

2 The NSX Controller uses the control plane with the ESXi hosts to push the new DLR configuration including LIFs and their associated IP and vMAC addresses.

3 Assuming a routing protocol is also enabled on the next-hop device (an NSX Edge [ESG] in this example), OSPF or BGP peering is established between the ESG and the DLR control VM. The ESG and the DLR can then exchange routing information:
   - The DLR control VM can be configured to redistribute into OSPF the IP prefixes for all the connected logical networks (172.16.10.0/24 and 172.16.20.0/24 in this example). As a consequence, it then pushes those route advertisements to the NSX Edge. Notice that the next hop for those prefixes is not the IP address assigned to the control VM (192.168.10.3) but the IP address identifying the data-plane component of the DLR (192.168.10.2). The former is called the DLR “protocol address,” whereas the latter is the “forwarding address”.
   - The NSX Edge pushes to the control VM the prefixes to reach IP networks in the external network. In most scenarios, a single default route is likely to be sent by the NSX Edge, because it represents the single point of exit toward the physical network infrastructure.
4  The DLR control VM pushes the IP routes learned from the NSX Edge to the controller cluster.

5  The controller cluster is responsible for distributing routes learned from the DLR control VM to the hypervisors. Each controller node in the cluster takes responsibility of distributing the information for a particular logical router instance. In a deployment where there are multiple logical router instances deployed, the load is distributed across the controller nodes. A separate logical router instance is usually associated with each deployed tenant.

6  The DLR routing kernel modules on the hosts handle the data-path traffic for communication to the external network by way of the NSX Edge.

NSX Services

The NSX components work together to provide the following functional services.

Logical Switches

A cloud deployment or a virtual data center has a variety of applications across multiple tenants. These applications and tenants require isolation from each other for security, fault isolation, and non-overlapping IP addresses. NSX allows the creation of multiple logical switches, each of which is a single logical broadcast domain. An application or tenant virtual machine can be logically wired to a logical switch. This allows for flexibility and speed of deployment while still providing all the characteristics of a physical network's broadcast domains (VLANs) without physical Layer 2 sprawl or spanning tree issues.

A logical switch is distributed and can span across all hosts in vCenter (or across all hosts in a cross-vCenter NSX environment). This allows for virtual machine mobility (vMotion) within the data center without limitations of the physical Layer 2 (VLAN) boundary. The physical infrastructure is not constrained by MAC/FIB table limits, because the logical switch contains the broadcast domain in software.

Logical Routers

Routing provides the necessary forwarding information between Layer 2 broadcast domains, thereby allowing you to decrease the size of Layer 2 broadcast domains and improve network efficiency and scale. NSX extends this intelligence to where the workloads reside for East-West routing. This allows more direct VM-to-VM communication without the costly or timely need to extend hops. At the same time, NSX logical routers provide North-South connectivity, thereby enabling tenants to access public networks.

Logical Firewall

Logical Firewall provides security mechanisms for dynamic virtual data centers. The Distributed Firewall component of Logical Firewall allows you to segment virtual datacenter entities like virtual machines based on VM names and attributes, user identity, vCenter objects like datacenters, and hosts, as well as traditional networking attributes like IP addresses, VLANs, and so on. The Edge Firewall component helps you meet key perimeter security requirements, such as building DMZs based on IP/VLAN constructs, and tenant-to-tenant isolation in multi-tenant virtual data centers.
The Flow Monitoring feature displays network activity between virtual machines at the application protocol level. You can use this information to audit network traffic, define and refine firewall policies, and identify threats to your network.

**Logical Virtual Private Networks (VPNs)**

SSL VPN-Plus allows remote users to access private corporate applications. IPsec VPN offers site-to-site connectivity between an NSX Edge instance and remote sites with NSX or with hardware routers/VPN gateways from 3rd-party vendors. L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity while retaining the same IP address across geographical boundaries.

**Logical Load Balancer**

The NSX Edge load balancer distributes client connections directed at a single virtual IP address (VIP) across multiple destinations configured as members of a load balancing pool. It distributes incoming service requests evenly among multiple servers in such a way that the load distribution is transparent to users. Load balancing thus helps in achieving optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload.

**Service Composer**

Service Composer helps you provision and assign network and security services to applications in a virtual infrastructure. You map these services to a security group, and the services are applied to the virtual machines in the security group using a Security Policy.

**NSX Extensibility**

3rd-party solution providers can integrate their solutions with the NSX platform, thus enabling customers to have an integrated experience across VMware products and partner solutions. Data center operators can provision complex, multi-tier virtual networks in seconds, independent of the underlying network topology or components.
Overview of Cross-vCenter Networking and Security

NSX 6.2 and later allows you to manage multiple vCenter NSX environments from a single primary NSX Manager.

This chapter includes the following topics:

- Benefits of Cross-vCenter NSX
- How Cross-vCenter NSX Works
- Support Matrix for NSX Services in Cross-vCenter NSX
- Universal Controller Cluster
- Universal Transport Zone
- Universal Logical Switches
- Universal Logical (Distributed) Routers
- Universal Firewall Rules
- Universal Network and Security Objects
- Cross-vCenter NSX Topologies
- Modifying NSX Manager Roles

Benefits of Cross-vCenter NSX

NSX environments containing more than one vCenter Server system can be managed centrally.

There are many reasons multiple vCenter Server systems may be required, for example:

- To overcome scale limits of vCenter Server
- To accommodate products that require dedicated or multiple vCenter Server systems, such as Horizon View or Site Recovery Manager
- To separate environments, for example by business unit, tenant, organization, or environment type

In NSX 6.1 and earlier, if multiple vCenter NSX environments are deployed, they must be managed separately. In NSX 6.2 and later you can create universal objects on the primary NSX Manager, which are synchronized across all vCenter Servers systems in the environment.
Cross-vCenter NSX includes these features:

- Increased span of NSX logical networks. The same logical networks are available across the vCenter NSX environment, so it's possible for VMs on any cluster on any vCenter Server system to be connected to the same logical network.

- Centralized security policy management. Firewall rules are managed from one centralized location, and apply to the VM regardless of location or vCenter Server system.

- Support of new mobility boundaries in vSphere 6, including cross vCenter and long distance vMotion across logical switches.

- Enhanced support for multi-site environments, from metro distance to 150ms RTT. This includes both active-active and active-passive datacenters.

Cross-vCenter NSX environments have many benefits:

- Centralized management of universal objects, reducing administration effort.

- Increased mobility of workloads - VMs can be vMotioned across vCenter Servers without having to reconfigure the VM or change firewall rules.

- Enhanced NSX multi-site and disaster recovery capabilities.

**Note** Cross-vCenter NSX functionality is supported with vSphere 6.0 and later.

### How Cross-vCenter NSX Works

In a cross-vCenter NSX environment, you can have multiple vCenter Servers, each of which must be paired with its own NSX Manager. One NSX Manager is assigned the role of primary NSX Manager, and the others are assigned the role of secondary NSX Manager.

The primary NSX Manager is used to deploy a universal controller cluster that provides the control plane for the cross-vCenter NSX environment. The secondary NSX Managers do not have their own controller clusters.

The primary NSX Manager can create universal objects, such as universal logical switches. These objects are synchronized to the secondary NSX Managers by the NSX Universal Synchronization Service. You can view these objects from the secondary NSX Managers, but you cannot edit them there. You must use the primary NSX Manager to manage universal objects. The primary NSX Manager can be used to configure any of the secondary NSX Managers in the environment.

On both primary and secondary NSX Managers, you can create objects that are local to that specific vCenter NSX environment, such as logical switches, and logical (distributed) routers. They will exist only within the vCenter NSX environment in which they were created. They will not be visible on the other NSX Managers in the cross-vCenter NSX environment.
NSX Managers can be assigned the standalone role. This is equivalent to pre-NSX 6.2 environments with a single NSX Manager and single vCenter. A standalone NSX Manager cannot create universal objects.

**Note** If you change the role of a primary NSX Manager to standalone and any universal objects exist in the NSX environment, the NSX Manager will be assigned the transit role. The universal objects remain, but they cannot be changed, and no other universal objects can be created. You can delete universal objects from the transit role. The transit role should only be used temporarily, for example, when changing which NSX Manager is the primary.

### Support Matrix for NSX Services in Cross-vCenter NSX

A subset of NSX Services are available for universal synchronization in cross-vCenter NSX. Services that are not available for universal synchronization can be configured for use local to the NSX Manager.

**Table 4-1. Support matrix for NSX Services in cross-vCenter NSX**

<table>
<thead>
<tr>
<th>NSX Service</th>
<th>Details</th>
<th>Supports cross-vCenter NSX synchronization?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical switch</td>
<td>Transport zone</td>
<td>Yes</td>
</tr>
<tr>
<td>Logical switch</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>NSX Service</td>
<td>Details</td>
<td>Supports cross-vCenter NSX synchronization?</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>L2 bridges</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Routing</td>
<td>Logical (distributed) router</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Logical (distributed) router appliance</td>
<td>No by design. Appliances must be created on each NSX Manager if multiple appliances are required per universal logical router. This allows for different configurations per appliance, which may be required in an environment with local egress configured.</td>
</tr>
<tr>
<td></td>
<td>NSX Edge services gateway</td>
<td>No</td>
</tr>
<tr>
<td>Logical firewall</td>
<td>Distributed firewall</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Exclude list</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>SpoofGuard</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Flow monitoring for aggregate flows</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Network service insertion</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Edge firewall</td>
<td>No</td>
</tr>
<tr>
<td>VPN</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Logical load balancer</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Other edge services</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Service composer</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Network extensibility</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Network and security objects</td>
<td>IP address groups (IP sets)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>MAC address groups (MAC sets)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>IP pools</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Security groups</td>
<td>Yes, but membership configuration differs from non-universal security groups membership. See &quot;Create a Security Group&quot; in the NSX Administration Guide for details.</td>
</tr>
<tr>
<td></td>
<td>Services</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Service groups</td>
<td>Yes</td>
</tr>
<tr>
<td>Security tags</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Hardware Gateway (also known as Hardware VTEP)</td>
<td>No. See &quot;Hardware Gateway Sample Configuration&quot; in the NSX Administration Guide for details.</td>
<td></td>
</tr>
</tbody>
</table>
Universal Controller Cluster

Each cross-vCenter NSX environment has one universal controller cluster associated with the primary NSX Manager. Secondary NSX Managers do not have a controller cluster.

As the universal controller cluster is the only controller cluster for the cross-vCenter NSX environment, it maintains information about universal logical switches and universal logical routers as well as logical switches and logical routers that are local to a vCenter NSX pair.

In order to avoid any overlap in object IDs, separate ID pools are maintained for universal objects and local objects.

Universal Transport Zone

In a cross-vCenter NSX environment, there can be only one universal transport zone.

The universal transport zone is created on the primary NSX Manager, and is synchronized to the secondary NSX Managers. Clusters that need to participate in universal logical networks must be added to the universal transport zone from their NSX Managers.

Universal Logical Switches

Universal logical switches allow layer 2 networks to span multiple sites.

When you create a logical switch in a universal transport zone, you create a universal logical switch. This switch is available on all clusters in the universal transport zone. The universal transport zone can include clusters in any vCenter in the cross-vCenter NSX environment.

The segment ID pool is used to assign VNIs to logical switches, and the universal segment ID pool is used to assign VNIs to universal logical switches. These pools must not overlap.

You must use a universal logical router to route between universal logical switches. If you need to route between a universal logical switch and a logical switch, you must use an Edge Services Gateway.

Universal Logical (Distributed) Routers

Universal Logical (Distributed) Routers offer centralized administration and a routing configuration that can be customized at the universal logical router, cluster, or host level.

When you create a universal logical router you must choose whether to enable local egress, as this cannot be changed after creation. Local egress allows you to control what routes are provided to ESXi hosts based on an identifier, the locale ID.

Each NSX Manager is assigned a locale ID, which is set to the NSX Manager UUID by default. You can override the locale ID at the following levels:

- Universal logical router
- Cluster
- ESXi host
If you do not enable local egress the locale ID is ignored and all ESXi hosts connected to the universal logical router will receive the same routes. Whether or not to enable local egress in a cross-vCenter NSX environment is a design consideration, but it is not required for all cross-vCenter NSX configurations.

**Universal Firewall Rules**

Distributed Firewall in a cross-vCenter NSX environment allows centralized management of rules that apply to all vCenter Servers in your environment. It supports cross-vCenter vMotion which enables you to move workloads or virtual machines from one vCenter Server to another and seamlessly extends your software defined datacenter security.

As your datacenter needs scale out, the existing vCenter Server may not scale to the same level. This may require you to move a set of applications to newer hosts that are managed by a different vCenter Server. Or you may need to move applications from staging to production in an environment where staging servers are managed by one vCenter Server and production servers are managed by a different vCenter Server. Distributed Firewall supports these cross-vCenter vMotion scenarios by replicating firewall policies that you define for the primary NSX Manager on up to seven secondary NSX Managers.

From the primary NSX Manager you can create distributed firewall rule sections that are marked for universal synchronization. You can create more than one universal L2 rule section and more than one universal L3 rule section. Universal sections are always listed at the top of primary and secondary NSX Managers. These sections and their rules are synchronized to all secondary NSX Managers in your environment. Rules in other sections remain local to the appropriate NSX Manager.

The following Distributed Firewall features are not supported in a cross-vCenter NSX environment:

- Exclude list
- SpoofGuard
- Flow monitoring for aggregate flows
- Network service insertion
- Edge Firewall

Service Composer does not support universal synchronization, so you cannot use it to create distributed firewall rules in the universal section.

**Universal Network and Security Objects**

You can create custom network and security objects to use in Distributed Firewall rules in the universal section.

Universal Security Groups (USGs) can have the following:

- Universal IP Sets
- Universal MAC Sets
- Universal Security Groups
Universal Security Tags

Dynamic criteria

Universal network and security objects are created, deleted, and updated only on the primary NSX Manager, but are readable on the secondary NSX Manager. Universal Synchronization Service synchronizes universal objects across vCenters immediately, as well as on demand using force synchronization.

Universal security groups are used in two types of deployments: multiple live cross-vCenter NSX environments, and cross-vCenter NSX active standby deployments, where one site is live at a given time and the rest are on standby. Only active standby deployments can have universal security groups with dynamic membership based on VM name static membership based on universal security tag. Once a universal security group is created it cannot be edited to be enabled or disabled for the active standby scenario functionality. Membership is defined by included objects only, you cannot use excluded objects.

Universal security groups cannot be created from Service Composer. Security groups created from Service Composer will be local to that NSX Manager.

Cross-vCenter NSX Topologies

You can deploy cross-vCenter NSX in a single physical site, or across multiple sites.

Multi-Site and Single Site Cross-vCenter NSX

A cross-vCenter NSX environment allows you to use the same logical switches and other network objects across multiple vCenter NSX setups. The vCenter Server systems can be located in the same site, or in different sites.

Whether the cross-vCenter NSX environment is contained within a single site or crosses multiple sites, a similar configuration can be used. These two example topologies consist of the following:

- A universal transport zone that includes all clusters in the site or sites.
- Universal logical switches attached to the universal transport zone. Two universal logical switches are used to connect VMs and one is used as a transit network for the router uplink.
- VMs added to the universal logical switches
- A universal logical router with an NSX Edge appliance to enable dynamic routing. The universal logical router appliance has internal interfaces on the VM universal logical switches and an uplink interface on the transit network universal logical switch.
- Edge Services Gateways (ESGs) connected to the transit network and the physical egress router network.

For more information about cross-vCenter NSX topologies, see the Cross-vCenter NSX Design Guide at https://communities.vmware.com/docs/DOC-32552.
Figure 4-1. Cross-vCenter NSX in a single site

- Universal Controller Cluster
- vCenter with NSX Manager (Primary)
- vCenter with NSX Manager (Secondary)
- Physical Routers
- OSPF, BGP
- Peering x8
- Universal Logical Router Appliance
- Universal Routers
- Universal Transport Zone
- Site A
- NSX Administration Guide
- VMware, Inc. 35
Local Egress

All sites in a multi-site cross-vCenter NSX environment can use the same physical routers for egress traffic. However, if egress routes need to be customized, the local egress feature must be enabled when the universal logical router is created.

Local egress allows you to customize routes at the universal logical router, cluster, or host level. This example of a cross-vCenter NSX environment in multiple sites has local egress enabled. The edge services gateways (ESGs) in each site have a default route that sends traffic out through that site's physical routers. The universal logical router is configured with two appliances, one in each site. The appliances learn routes from their site's ESGs. The learned routes are sent to the universal controller...
Because local egress is enabled, the locale ID for that site is associated with those routes. The universal controller cluster sends routes with matching locale IDs to the hosts. Routes learned on the site A appliance are sent to the hosts in site A, and routes learned on the site B appliance are sent to the hosts in site B.

For more information about local egress, see the Cross-vCenter NSX Design Guide at https://communities.vmware.com/docs/DOC-32552.

Modifying NSX Manager Roles

An NSX Manager can have roles, such as primary, secondary, standalone, or transit. Special synchronization software runs on the primary NSX Manager, synchronizing all universal objects to secondary NSX Managers.
It is important to understand what happens when you change an NSX Manager's role.

**Set as primary**

This operation sets the role of an NSX Manager to primary and starts the synchronization software. This operation fails if the NSX Manager is already the primary or already a secondary.

**Set as standalone (from secondary)**

This operation sets the role of NSX Manager to standalone or transit mode. This operation might fail if the NSX Manager already has the standalone role.

**Set as standalone (from primary)**

This operation resets the primary NSX Manager to standalone or transit mode, stops the synchronization software, and unregisters all secondary NSX Managers. This operation might fail if the NSX Manager is already standalone or if any of the secondary NSX Managers are unreachable.

**Disconnect from primary**

When you run this operation on a secondary NSX Manager, the secondary NSX Manager is unilaterally disconnected from the primary NSX Manager. This operation should be used when the primary NSX Manager has experienced an unrecoverable failure, and you want to register the secondary NSX Manager to a new primary. If the original primary NSX Manager does come up again, its database continues to list the secondary NSX Manager as registered. To resolve this issue, include the `force` option when you disconnect or unregister the secondary from the original primary. The `force` option removes the secondary NSX Manager from the original primary NSX Manager's database.
Transport Zones

A transport zone controls to which hosts a logical switch can reach. It can span one or more vSphere clusters. Transport zones dictate which clusters and, therefore, which VMs can participate in the use of a particular network. In a cross-vCenter NSX environment you can create a universal transport zone, which can include clusters from any vCenter in the environment. You can create only one universal transport zone.

An NSX environment can contain one or more transport zones based on your requirements. A host cluster can belong to multiple transport zones. A logical switch can belong to only one transport zone. NSX does not allow connection of VMs that are in different transport zones. The span of a logical switch is limited to a transport zone, so virtual machines in different transport zones cannot be on the same Layer 2 network. A distributed logical router cannot connect to logical switches that are in different transport zones. After you connect the first logical switch, the selection of further logical switches is limited to those that are in the same transport zone.

The following guidelines are meant to help you design your transport zones:

- If a cluster requires Layer 3 connectivity, the cluster must be in a transport zone that also contains an edge cluster, meaning a cluster that has Layer 3 edge devices (distributed logical routers and edge services gateways).

- Suppose you have two clusters, one for web services and another for application services. To have VXLAN connectivity between the VMs in these two clusters, both of the clusters must be included in the transport zone.

- Keep in mind that all logical switches included in the transport zone will be available and visible to all VMs within the clusters that are included in the transport zone. If a cluster includes secured environments, you might not want to make it available to VMs in other clusters. Instead, you can place your secure cluster in a more isolated transport zone.

- The span of the vSphere distributed switch (VDS or DVS) should match the transport zone span. When creating transport zones in multi-cluster VDS configurations, make sure all clusters in the selected VDS are included in the transport zone. This is to ensure that the DLR is available on all clusters where VDS dvPortgroups are available.

The following diagram shows a transport zone correctly aligned to the VDS boundary.
If you do not follow this best practice, keep in mind that if a VDS spans more than one host cluster and the transport zone includes only one (or a subset) of these clusters, any logical switch included within this transport zone can access VMs within all clusters spanned by the VDS. In other words, the transport zone will not be able to constrain the logical switch span to a subset of the clusters. If this logical switch is later connected to a DLR, you must ensure that the router instances are created only in the cluster included in the transport zone to avoid any Layer 3 issues.

For example, when a transport zone is not aligned to the VDS boundary, the scope of the logical switches (5001, 5002 and 5003) and the DLR instances that these logical switches are connected to becomes disjointed, causing VMs in cluster Comp A to have no access to the DLR logical interfaces (LIFs).
This chapter includes the following topics:

- Add a Transport Zone
- View and Edit a Transport Zone
- Expand a Transport Zone
- Contract a Transport Zone
- Controller Disconnected Operation (CDO) Mode

**Add a Transport Zone**

A transport zone controls which hosts a logical switch can reach and can span one or more vSphere clusters. Transport zones dictate which clusters and, therefore, which VMs can participate in the use of a particular network. Universal transport zones can span vSphere cluster across a cross-vCenter NSX environment.

You can have only one universal transport zone in a cross-vCenter NSX environment.

**Prerequisites**

Determine the appropriate NSX Manager on which to make your changes.

- In a standalone or single vCenter NSX environment there is only one NSX Manager so you do not need to select one.
- Universal objects must be managed from the primary NSX Manager.
Objects local to an NSX Manager must be managed from that NSX Manager.

In a cross-vCenter NSX environment that does not have Enhanced Linked Mode enabled, you must make configuration changes from the vCenter linked to the NSX Manager that you want to modify.

In a cross-vCenter NSX environment in Enhanced Linked Mode, you can make configuration changes to any NSX Manager from any linked vCenter. Select the appropriate NSX Manager from the NSX Manager drop-down menu.

Procedure


2. Click Transport Zones and click the New Transport Zone () icon.

3. (Optional) To add a universal transport zone, select Mark this object for universal synchronization.

4. Select the replication mode:
   - Multicast: Multicast IP addresses in the physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP in the physical network.
   - Unicast: The control plane is handled by an NSX controller. All unicast traffic leverages optimized headend replication. No multicast IP addresses or special network configuration is required.
   - Hybrid: Offloads local traffic replication to the physical network (L2 multicast). This requires IGMP snooping on the first-hop switch and access to an IGMP querier in each VTEP subnet, but does not require PIM. The first-hop switch handles traffic replication for the subnet.

   **Important** If you create a universal transport zone and select hybrid as the replication mode, you must ensure that the multicast address used does not conflict with any other multicast addresses assigned on any NSX Manager in the environment.

5. Select the clusters to add to the transport zone

Results

Transport-Zone is a transport zone local to the NSX Manager on which it was created.

Universal-Transport-Zone is a universal transport zone which is available on all NSX Managers in a cross-vCenter NSX environment.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Control Plane Mode</th>
<th>Logical Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport-Zone</td>
<td></td>
<td>Multicast</td>
<td>1</td>
</tr>
<tr>
<td>Universal-Transport-Zone</td>
<td></td>
<td>Unicast</td>
<td>4</td>
</tr>
</tbody>
</table>

What to do next

If you added a transport zone, you can add logical switches.

If you added a universal transport zone, you can add universal logical switches.
If you added a universal transport zone, you can select the secondary NSX Managers and add their clusters to the universal transport zone.

**View and Edit a Transport Zone**

You can view the logical networks in a selected transport zone, the clusters in, and the control plane mode for that transport zone.

**Procedure**

1. In Transport Zones, double-click a transport zone.
   
   The Summary tab displays the name and description of the transport zone as well as the number of logical switches associated with it. Transport Zone Details displays the clusters in the transport zone.

2. Click the **Edit Settings** icon in the **Transport Zone Details** section to edit the name, description, or control plane mode of the transport zone.
   
   If you change the transport zone control plane mode, select **Migrate existing Logical Switches to the new control plane mode** to change the control plane mode for existing logical switches linked to this transport zone. If you do not select this check box, only the logical switches linked to this transport zone after the edit is done will have the new control plane mode.

3. Click OK.

**Expand a Transport Zone**

You can add clusters to a transport zone. All existing transport zones become available on the newly added clusters.

**Prerequisites**

The clusters you add to a transport zone have the network infrastructure installed and are configured for VXLAN. See the *NSX Installation Guide*.

**Procedure**

1. In Transport Zones, click a transport zone.

2. Click the **Add Cluster** icon.

3. Select the clusters you want to add to the transport zone and click OK.

**Contract a Transport Zone**

You can remove clusters from a transport zone. The size of existing transport zones is reduced to accommodate the contracted scope.

**Procedure**

1. In **Transport Zones**, double-click a transport zone.
In **Transport Zones Details**, click the **Remove Clusters** [icon](image).

Select the clusters that you want to remove.

Click **OK**.

## Controller Disconnected Operation (CDO) Mode

Controller Disconnected Operation (CDO) mode ensures that the data plane connectivity is unaffected when hosts lose connectivity with the controller. You can enable CDO mode to avoid temporary connectivity issues with the controller.

You can enable CDO mode for each host cluster connected to a transport zone. CDO mode is disabled by default.

**Note** To enable CDO mode, all prepared hosts in the system must be upgraded to NSX 6.3.2 or later.

When CDO mode is enabled, NSX Manager creates a special CDO logical switch, one for every transport zone. The VXLAN Network Identifier (VNI) of the special CDO logical switch is unique from all other logical switches. When CDO mode is enabled, one controller in the cluster is responsible for collecting all the VTEP information reported from all transport nodes, and replicating the updated VTEP information to all other transport nodes. When a controller fails, a new controller is elected as the new master to take the responsibility and all transport nodes connected to the original master are migrated to the new master and data is synced between the transport nodes and the controllers.

If you add a new cluster to a transport zone, NSX Manager pushes the CDO mode setting and the VNI to the newly added hosts. If you remove the cluster, NSX Manager removes the VNI data from the hosts.

When you disable CDO mode on a transport zone, NSX Manager removes the CDO logical switch from the controller.

In a Cross-vCenter NSX environment, you can enable CDO mode only on the local transport zones or in a topology where you do not have any local transport zones and have a single universal transport zone for the primary NSX Manager. CDO mode gets replicated on the universal transport zone for all secondary NSX Managers.

You can enable CDO mode on local transport zone for a secondary NSX Manager.

## Enable Controller Disconnected Operation (CDO) Mode

You can enable the Controller Disconnected Operation (CDO) mode for each host cluster through transport zone. CDO mode is disabled by default.

**Prerequisites**

- Verify that all prepared hosts in the system are upgraded to NSX 6.3.2 or later.

**Procedure**

1. Log in to the vSphere Web Client.
2 Click Networking & Security > Logical Network Preparation, and then click Transport Zones.

3 Select the required transport zone, and click the Actions icon. You can also right-click the transport zone.

4 Click Enable CDO mode.

A confirmation dialog box appears.

**Note**: If you receive an error message in a Cross-vCenter NSX environment, verify the following conditions:

- **Primary NSX Manager**: You can enable CDO mode only on transport zones that do not share the same distributed virtual switch. If the universal transport zone and the local transport zones share the same distributed virtual switch, then CDO mode can be enabled only on the universal transport zone.

- **Secondary NSX Manager**: CDO mode gets replicated on the universal transport zone for all secondary NSX Managers. You can enable CDO mode on local transport zones, if they do not share the same distributed virtual switch.

5 Click Yes.

CDO mode is enabled for the selected transport zone.

**Results**

The CDO Mode column displays the status as **Enabled**.

NSX Manager creates a CDO logical switch on the controller.

**Disable Controller Disconnected Operation (CDO) Mode**

You can disable the already enabled Controller Disconnected Operation (CDO) mode through transport zone when connectivity issues with the controller is resolved. CDO mode remains disabled by default.

**Procedure**

1 Log in to the vSphere Web Client.

2 Click Networking & Security > Logical Network Preparation, and then click Transport Zones.

3 Select the transport zone on which you want to disable CDO mode, and click the Actions icon. You can also right-click the transport zone.

4 Click Disable CDO mode.

A confirmation dialog box appears.

5 Click Yes.

CDO mode is disabled for the selected transport zone.

**Results**

The CDO Mode column displays the status as **Disabled**.
NSX Manager removes the CDO logical switch from the controller.
Logical Switches

A cloud deployment or a virtual data center has a variety of applications across multiple tenants. These applications and tenants require isolation from each other for security, fault isolation, and avoiding overlapping IP addressing issues. The NSX logical switch creates logical broadcast domains or segments to which an application or tenant virtual machine can be logically wired. This allows for flexibility and speed of deployment while still providing all the characteristics of a physical network’s broadcast domains (VLANs) without physical Layer 2 sprawl or spanning tree issues.

A logical switch is distributed and can span arbitrarily large compute clusters. This allows for virtual machine mobility (vMotion) within the datacenter without limitations of the physical Layer 2 (VLAN) boundary. The physical infrastructure does not have to deal with MAC/FIB table limits since the logical switch contains the broadcast domain in software.

A logical switch is mapped to a unique VXLAN, which encapsulates the virtual machine traffic and carries it over the physical IP network.
The NSX controller is the central control point for all logical switches within a network and maintains information of all virtual machines, hosts, logical switches, and VXLANs. The controller supports two new logical switch control plane modes, Unicast and Hybrid. These modes decouple NSX from the physical network. VXLANs no longer require the physical network to support multicast in order to handle the Broadcast, Unknown unicast, and Multicast (BUM) traffic within a logical switch. The unicast mode replicates all the BUM traffic locally on the host and requires no physical network configuration. In the hybrid mode, some of the BUM traffic replication is offloaded to the first hop physical switch to achieve better performance. This mode requires IGMP snooping to be turned on the first hop physical switch. Virtual machines within a logical switch can use and send any type of traffic including IPv6 and multicast.

You can extend a logical switch to a physical device by adding an L2 bridge. See Chapter 8 L2 Bridges.

You must have the Super Administrator or Enterprise Administrator role permissions to manage logical switches.

This chapter includes the following topics:

- Add a Logical Switch
- Connect Virtual Machines to a Logical Switch
- Test Logical Switch Connectivity
Add a Logical Switch

Prerequisites

- You have the Super Administrator or Enterprise Administrator role permission to configure and manage logical switches.
- VXLAN UDP port is opened on firewall rules (if applicable). The VXLAN UDP port can be configured through the API.
- Physical infrastructure MTU is at least 50 bytes more than the MTU of the virtual machine vNIC.
- Managed IP address is set for each vCenter Server in the vCenter Server Runtime Settings. See vCenter Server and Host Management.
- DHCP is available on VXLAN transport VLANs if you are using DHCP for IP assignment for VMKNics.
- A consistent distributed virtual switch type (vendor, and so on) and version is being used across a given transport zone. Inconsistent switch types can lead to undefined behavior in your logical switch.
- You have configured an appropriate LACP teaming policy and connected physical NICs to the ports. For more information on teaming modes, refer to the VMware vSphere documentation.
- 5-tuple hash distribution is enabled for Link Aggregation Control Protocol (LACP).
- Verify that for every host where you want to use LACP, a separate LACP port channel exists on the distributed virtual switch.
- For multicast mode, multicast routing is enabled if VXLAN traffic is traversing routers. You have acquired a multicast address range from your network administrator.
- Port 1234 (the default controller listening port) is opened on firewall for the ESXi host to communicate with controllers.
- (Recommended) For multicast and hybrid modes, you have enabled IGMP snooping on the L2 switches to which VXLAN participating hosts are attached. If IGMP snooping is enabled on L2, IGMP querier must be enabled on the router or L3 switch with connectivity to multicast enabled networks.

Add a Logical Switch

An NSX logical switch reproduces switching functionality (unicast, multicast, broadcast) in a virtual environment completely decoupled from underlying hardware. Logical switches are similar to VLANs, in that they provide network connections to which you can attach virtual machines. Logical switches are local to a single vCenter NSX deployment. In a cross-vCenter NSX deployment, you can create universal logical switches, which can span all vCenters. The transport zone type determines whether the new switch is a logical switch or a universal logical switch.
When you create a logical switch, in addition to selecting a transport zone and replication mode, you configure two options: IP discovery, and MAC learning.

IP discovery minimizes ARP traffic flooding within individual VXLAN segments---in other words, between VMs connected to the same logical switch. IP discovery is enabled by default.

**Note** You cannot disable IP discovery when you create a universal logical switch. You can disable IP discovery via the API after the universal logical switch is created. This setting is managed separately on each NSX Manager. See the *NSX API Guide*.

MAC learning builds a VLAN/MAC pair learning table on each vNIC. This table is stored as part of the dvfilter data. During vMotion, dvfilter saves and restores the table at the new location. The switch then issues RARPs for all the VLAN/MAC entries in the table. You might want to enable MAC learning if you are using virtual NICs that are trunking VLANs.

**Prerequisites**

**Table 6-1. Prerequisites for creating a logical switch or universal logical switch**

<table>
<thead>
<tr>
<th>Logical Switch</th>
<th>Universal Logical Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere distributed switches must be configured.</td>
<td>vSphere distributed switches must be configured.</td>
</tr>
<tr>
<td>NSX Manager must be installed.</td>
<td>NSX Manager must be installed.</td>
</tr>
<tr>
<td>Controllers must be deployed.</td>
<td>Controllers must be deployed.</td>
</tr>
<tr>
<td>Host clusters must be prepared for NSX.</td>
<td>Host clusters must be prepared for NSX.</td>
</tr>
<tr>
<td>VXLAN must be configured.</td>
<td>VXLAN must be configured.</td>
</tr>
<tr>
<td>A segment ID pool must be configured.</td>
<td>A primary NSX Manager must be assigned.</td>
</tr>
<tr>
<td>A transport zone must be created.</td>
<td>A universal segment ID pool must be configured.</td>
</tr>
<tr>
<td></td>
<td>A universal transport zone must be created.</td>
</tr>
</tbody>
</table>

Determine the appropriate NSX Manager on which to make your changes.

- In a standalone or single vCenter NSX environment there is only one NSX Manager so you do not need to select one.
- Universal objects must be managed from the primary NSX Manager.
- Objects local to an NSX Manager must be managed from that NSX Manager.
- In a cross-vCenter NSX environment that does not have Enhanced Linked Mode enabled, you must make configuration changes from the vCenter linked to the NSX Manager that you want to modify.
- In a cross-vCenter NSX environment in Enhanced Linked Mode, you can make configuration changes to any NSX Manager from any linked vCenter. Select the appropriate NSX Manager from the NSX Manager drop-down menu.

**Procedure**

2. Select the NSX Manager on which you want to create a logical switch. To create a universal logical switch, you must select the primary NSX Manager.
3 Click the **New Logical Switch**.

4 Type a name and optional description for the logical switch.

5 Select the transport zone in which you want to create the logical switch. Selecting a universal transport zone will create a universal logical switch.

   By default, the logical switch inherits the control plane replication mode from the transport zone. You can change it to one of the other available modes. The available modes are unicast, hybrid, and multicast.

   If you create a universal logical switch and select hybrid as the replication mode, you must ensure that the multicast address used does not conflict with other multicast addresses assigned on any NSX Manager in the cross-vCenter NSX environment.

6 (Optional) Click **Enable IP Discovery** to enable ARP suppression.

7 (Optional) Click **Enable MAC learning**

**Example: Logical Switch and Universal Logical Switch**

App is a logical switch connected to a transport zone. It is available only on the NSX Manager on which it was created.

Universal-App is a universal logical switch connected to a universal transport zone. It is available on any of the NSX Managers in the cross-vCenter NSX environment.

The logical switch and the universal logical switch have segment IDs from different segment ID pools.

<table>
<thead>
<tr>
<th>Virtual Wire ID</th>
<th>Segment ID</th>
<th>Name</th>
<th>Status</th>
<th>Transport Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtualwire-1</td>
<td>5000</td>
<td>App</td>
<td>Normal</td>
<td>Transport Zone</td>
</tr>
<tr>
<td>universalwire-2</td>
<td>900000</td>
<td>Universal-App</td>
<td>Normal</td>
<td>Universal-Transport-Zone</td>
</tr>
</tbody>
</table>

**What to do next**

Add VMs to a logical switch or universal logical switch.

Create a logical router and attach it to your logical switches to enable connectivity between VMs that are connected to different logical switches.

Create a universal logical router and attach it to your universal logical switches to enable connectivity between VMs that are connected to different universal logical switches.

**Connect a Logical Switch to an NSX Edge**

Connecting a logical switch to an NSX Edge services gateway or an NSX Edge logical router provides East-West traffic routing (among the logical switches) or North-South traffic routing to the external world or to provide advanced services.

**Procedure**
**Procedure**

1. In Logical Switches, select the logical switch to which you want to connect an NSX Edge.

2. Click the Connect an Edge (icon).

3. Select the NSX Edge to which you want to connect the logical switch and click Next.

4. Select the interface that you want to connect to the logical switch and click Next.
   
   A logical network is typically connected to an internal interface.

5. On the Edit NSX Edge interface page, type a name for the NSX Edge interface.

6. Click Internal or Uplink to indicate whether this is an internal or uplink interface.

7. Select the connectivity status of the interface.

8. If the NSX Edge to which you are connecting the logical switch has Manual HA Configuration selected, specify two management IP addresses in CIDR format.

9. Edit the default MTU if required.

10. Click Next.

11. Review the NSX Edge connection details and click Finish.

**Deploy Services on a Logical Switch**

You can deploy third party services on a logical switch.

**Prerequisites**

One or more third party virtual appliances must have been installed in your infrastructure.

**Procedure**

1. In Logical Switches, select the logical switch on which you want to deploy services.

2. Click the Add Service Profile (icon).

3. Select the service and service profile that you want to apply.

4. Click OK.

**Connect Virtual Machines to a Logical Switch**

You can connect virtual machines to a logical switch or universal logical switch.

**Procedure**

1. In Logical Switches, select the logical switch to which you want to add virtual machines.

2. Click the Add Virtual Machine (icon).

3. Select the virtual machines you want to add to the logical switch.
4  Select the vNICs that you want to connect.
5  Click Next.
6  Review the vNICs you selected.
7  Click Finish.

**Test Logical Switch Connectivity**

A ping test checks if two hosts in a VXLAN transport network can reach each other.

1  In Logical Switches, double click the logical switch that you want to test in the Name column.
2  Click the Monitor tab.
3  Click the Hosts tab.
4  Click Browse in the Source Host section. In the Select Host dialog box, select the destination host.
5  Select the size of the test packet.
   VXLAN standard size is 1550 bytes (should match the physical infrastructure MTU) without fragmentation. This allows NSX to check connectivity and verify that the infrastructure is prepared for VXLAN traffic.
   Minimum packet size allows fragmentation. Hence, with packet size minimized, NSX can check connectivity but not whether the infrastructure is ready for the larger frame size.
6  Click Browse in the Destination Host section. In the Select Host dialog box, select the destination host.
7  Click Start Test.
   The host-to-host ping test results are displayed.

**Prevent Spoofing on a Logical Switch**

After synchronizing with the vCenter Server, NSX Manager collects the IP addresses of all vCenter guest virtual machines from VMware Tools on each virtual machine, or from IP discovery if it is enabled. NSX does not trust all IP addresses provided by VMware Tools or IP discovery. If a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

SpoofGuard allows you to authorize the IP addresses reported by VMware Tools or IP discovery, and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vSphere SDK. Operating separately from the Firewall rules, you can use SpoofGuard to block traffic identified as spoofed.

For more information, see Chapter 13 Using SpoofGuard.

**Edit a Logical Switch**

You can edit the name, description, and control plane mode of a logical switch.
Procedure

1. In Logical Switches, select the logical switch that you want to edit.
2. Click the **Edit** icon.
3. Make the desired changes.
4. Click **OK**.

Logical Switch Scenario

This scenario presents a situation where company ACME Enterprise has several ESXi hosts on two clusters in a datacenter, ACME_Datacenter. The Engineering (on port group PG-Engineering) and Finance departments (on port group PG-Finance) are on Cluster1. The Marketing department (PG-Marketing) is on Cluster2. Both clusters are managed by a single vCenter Server.

**Figure 6-1. ACME Enterprise network before implementing logical switches**

ACME is running out of compute space on Cluster1 while Cluster2 is under-utilized. The ACME network supervisor asks John Admin (ACME’s virtualization administrator) to figure out a way to extend the Engineering department to Cluster2 in a way that virtual machines belonging to Engineering on both clusters can communicate with each other. This would enable ACME to utilize the compute capacity of both clusters by stretching ACME’s L2 layer.
If John Admin were to do this the traditional way, he would need to connect the separate VLANs in a special way so that the two clusters can be in the same L2 domain. This might require ACME to buy a new physical device to separate traffic, and lead to issues such as VLAN sprawl, network loops, and administration and management overhead.

John Admin remembers seeing a logical network demo at VMworld, and decides to evaluate NSX. He concludes that building a logical switch across dvSwitch1 and dvSwitch2 will allow him to stretch ACME’s L2 layer. Since John can leverage the NSX controller, he will not have to touch ACME’s physical infrastructure as NSX works on top of existing IP networks.

**Figure 6-2. ACME Enterprise implements a logical switch**

Once John Admin builds a logical switch across the two clusters, he can vMotion virtual machines from one cluster to another while keeping them attached to the same logical switch.
Let us walk through the steps that John Admin follows to build a logical network at ACME Enterprise.

**John Admin Assigns Segment ID Pool and Multicast Address Range to NSX Manager**

John Admin must specify the segment ID pool he received to isolate Company ABC's network traffic.

**Prerequisites**

1. John Admin verifies that dvSwitch1 and dvSwitch2 are VMware distributed switches version 5.5.
2. John Admin sets the Managed IP address for the vCenter Server.
   a. Select **Administration > vCenter Server Settings > Runtime Settings**.
   b. In vCenter Server Managed IP, type `10.115.198.165`.
   c. Click **OK**.
3. John Admin installs the network virtualization components on Cluster1 and Cluster 2. See *NSX Installation Guide*.
4. John Admin gets a segment ID pool (5000 - 5250) from ACME's NSX Manager administrator. Since he is leveraging the NSX controller, he does not require multicast in his physical network.
5 John Admin creates an IP pool so that he can assign a static IP address to the VXLAN VTEPs from this IP pool. See Add an IP Pool.

Procedure

1 In the vSphere Web Client, click Networking & Security > Installation.
2 Click the Logical Network Preparation tab and then click Segment ID.
3 Click Edit.
4 In Segment ID pool, type 5000 – 5250.
5 Do not select Enable multicast addressing.
6 Click OK.

John Admin Configures VXLAN Transport Parameters

John Admin configures VXLAN on Cluster 1 and Cluster 2, where he maps each cluster to a vDS. When he maps a cluster to a switch, each host in that cluster is enabled for logical switches.

Procedure

1 Click the Host Preparation tab.
2 For Cluster1, select Configure in the VXLAN column.
3 In the Configuring VXLAN networking dialog box, select dvSwitch1 as the virtual distributed switch for the cluster.
4 Type 10 for dvSwitch1 to use as the ACME transport VLAN.
5 In Specify Transport Attributes, leave 1600 as the Maximum Transmission Units (MTU) for dvSwitch1.
   MTU is the maximum amount of data that can be transmitted in one packet before it is divided into smaller packets. John Admin knows that VXLAN logical switch traffic frames are slightly larger in size because of the encapsulation, so the MTU for each switch must be set to 1550 or higher.
6 In VMKNic IP Addressing, select Use IP Pool and select an IP pool.
7 For VMKNic Teaming Policy, select Failover.
   John Admin wants to maintain the quality of service in his network by keeping the performance of logical switches the same in normal and fault conditions. Hence, he chooses Failover as the teaming policy.
8 Click Add.
9 Repeat steps 4 through step 8 to configure VXLAN on Cluster2.

Results

After John admin maps Cluster1 and Cluster2 to the appropriate switch, the hosts on those clusters are prepared for logical switches:

1 A VXLAN kernel module and vmknic is added to each host in Cluster 1 and Cluster 2.
2 A special dvPortGroup is created on the vSwitch associated with the logical switch and the VMKNic is connected to it.

John Admin Adds a Transport Zone

The physical network backing a logical network is called a transport zone. A transport zone is the compute diameter spanned by a virtualized network.

Procedure

1 Click Logical Network Preparation and then click Transport Zones.
2 Click the New Transport Zone icon.
3 In Name, type ACME Zone.
4 In Description, type Zone containing ACME’s clusters.
5 Select Cluster 1 and Cluster 2 to add to the transport zone.
6 In Control Plane Mode, select Unicast.
7 Click OK.

John Admin Creates a Logical Switch

After John Admin configures VXLAN transport parameters, he is ready to create a logical switch.

Procedure

1 Click Logical Switches and then click the New Logical Network icon.
2 In Name, type ACME logical network.
3 In Description, type Logical Network for extending ACME Engineering network to Cluster2.
4 In Transport Zone, select ACME Zone.
5 Click OK.

NSX creates a logical switch providing L2 connectivity between dvSwitch1 and dvSwitch2.

What to do next

John Admin can now connect ACME’s production virtual machines to the logical switch, and connect the logical switch to an NSX Edge services gateway or Logical Router.
Configuring Hardware Gateway

Hardware gateway configuration maps physical networks to virtual networks. The mapping configuration allows NSX to leverage the Open vSwitch Database (OVSDB).

The OVSDB database contains information about the physical hardware and the virtual network. The vendor hardware hosts the database server.

The hardware gateway switches in the NSX logical networks terminate VXLAN tunnels. To the virtual network, the hardware gateway switches are known as hardware VTEP. For more information about VTEPs, see the NSX Installation guide and NSX Network Virtualization Design guide.

A minimal topology with a hardware gateway includes the following components:

- Physical server
- Hardware gateway switch (L2 port)
- IP network
- Hypervisors a minimum of four, including two replication clusters with VMs
- Controller cluster with at least three nodes

The sample topology with a hardware gateway shows HV1 and HV2 as the two hypervisors. The VM1 virtual machine is on HV1. VTEP1 is on HV1, VTEP2 is on HV2, and VTEP3 is on the hardware gateway. The hardware gateway is located in a different subnet 211 compared to the two hypervisors that are located in the same subnet 221.
The hardware gateway underlying configuration can have any one of the following components:

- Single switch
- Multiple physical bus switches with different IP addresses
- Hardware switch controller with multiple switches

The NSX Controller communicates with the hardware gateway using its IP address on port 6640. This connection is used to send and receive OVSDB transactions from hardware gateways.

This chapter includes the following topics:

- Scenario: Hardware Gateway Sample Configuration

**Scenario: Hardware Gateway Sample Configuration**

This scenario describes typical tasks used to configure a hardware gateway switch with an NSX deployment. The sequence of tasks show how to connect the virtual machine VM1 to the physical server and to connect the WebService logical switch to the VLAN-Server VLAN 160 using the hardware gateway.

The sample topology shows that virtual machine VM1 and VLAN-Server are configured with an IP address in the subnet 10. VM1 is attached to WebService logical switch. The VLAN-Server is attached to VLAN 160 on the physical server.

**Important** In a cross-vCenter NSX environment, hardware gateway switch configurations are only supported on the primary NSX Manager. Hardware gateway switches must be bound to non-universal logical switches. Hardware gateway configurations are not supported on secondary NSX Managers.

**Prerequisites**

- Read the vendor documentation to meet the physical network requirements.
- Verify that you meet the NSX system and hardware requirements for hardware gateway configuration. See Chapter 1 System Requirements for NSX.
- Verify that the logical networks are set up properly. See the NSX Installation guide.
- Verify that the transport parameter mappings in the VXLAN are accurate. See the NSX Installation guide.
- Retrieve the vendor certificate for your hardware gateway.
Verify that the VXLAN port value is set to 4789. See Change VXLAN Port.

Procedure

1. Set Up the Replication Cluster
   A replication cluster is a set of hypervisors responsible for forwarding traffic sent from the hardware gateway. The traffic can be broadcast, unknown-unicast, and multicast traffic.

2. Connect the Hardware Gateway to the NSX Controllers
   You must configure the OVSDB manager table on the ToR physical switch to connect the hardware gateway to the NSX Controller.

3. Add Hardware Gateway Certificate
   Hardware gateway certificate must be added to the hardware device for the configuration to work.

4. Bind the Logical Switch to the Physical Switch
   The WebService logical switch attached to the virtual machine VM1 must communicate with the hardware gateway on the same subnet.

Set Up the Replication Cluster

A replication cluster is a set of hypervisors responsible for forwarding traffic sent from the hardware gateway. The traffic can be broadcast, unknown-unicast, and multicast traffic.

Note Hypervisors including the replication nodes and the hardware gateway switches must not be on the same IP subnet. This restriction is due to the limitation of the chipset used in most hardware gateways. Most hardware gateways, if not all, use the Broadcom Trident II chipset, which has a limitation that a layer 3 underlay network is required between the hardware gateway and the hypervisors.

Prerequisites

Verify that you have hypervisors to serve as replication nodes available.

Procedure

1. Log in to the vSphere Web Client.


3. Click the Hardware Devices tab.

4. Click Edit in the Replication Cluster section to select hypervisors to serve as replication nodes in this replication cluster.
5 Select hypervisors and click the blue arrow.

![Edit Replication Cluster Configuration](image)

The selected hypervisors move to the selected objects column.

6 Click OK.

**Results**

The replication nodes are added to the replication cluster. At least one host must exist in the replication cluster.

**Connect the Hardware Gateway to the NSX Controllers**

You must configure the the OVSDB manager table on the ToR physical switch to connect the hardware gateway to the NSX Controller.

The Controller passively listens to the connection attempt from ToR. Therefore, the hardware gateway must use the OVSDB manager table to initiate connection.

**Prerequisites**

Controllers must be deployed before any ToR instances are configured. If controllers are not deployed first, the error message "Failed to do the Operation on the Controller" is shown.

**Procedure**

1 Use the commands that apply to your environment to connect the hardware gateway to the NSX Controller.

Sample commands to connect hardware gateway and NSX Controller.

```
prmh-nsx-tor-7050sx-3#enable
prmh-nsx-tor-7050sx-3#configure terminal
prmh-nsx-tor-7050sx-3(config)#cvx
```
2 Set the OVSDB manager table on the hardware gateway.

3 Set the OVSDB port number value as 6640.

4 (Optional) Verify that the hardware gateway is connected to the NSX Controller through the OVSDB channel.
   - Check that the connection status is UP.
   - Ping the VM1 and VLAN 160 to verify that the connection succeeds.

5 (Optional) Verify that the hardware gateway is connected to correct NSX Controller.
   a Log in to the vSphere Web Client.
   b Select Networking & Security > Installation > NSX Controller nodes.

**Add Hardware Gateway Certificate**

Hardware gateway certificate must be added to the hardware device for the configuration to work.

**Prerequisites**

Verify that the hardware gateway certificate from your environment is available.

**Procedure**

1 Log in to the vSphere Web Client.

2 Select Networking & Security > Service Definitions.

3 Click the Hardware Devices tab.
4 Click the Add (➕) icon to create the hardware gateway profile details.

![Add Hardware Device](image)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>Specify a hardware gateway name. You can add details of the profile in the description section.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Paste the certificate that you extracted from your environment.</td>
</tr>
<tr>
<td>Enable BFD</td>
<td>Bidirectional Forwarding Detection (BFD) protocol is enabled by default. The protocol is used to synchronize the hardware gateway configuration information.</td>
</tr>
</tbody>
</table>

5 Click **OK**.

A profile that represents the hardware gateway is created.

6 Refresh the screen to verify that the hardware gateway is available and running.

The connectivity should be **UP**.

7 (Optional) Click the hardware gateway profile and right-click to select **View the BFD Tunnel Status** from the drop-down menu.
The dialog box shows diagnostic tunnel status details for troubleshooting.

**Bind the Logical Switch to the Physical Switch**

The WebService logical switch attached to the virtual machine VM1 must communicate with the hardware gateway on the same subnet.

**Note** If you bind multiple logical switches to hardware ports, you must apply these steps for each logical switch.

**Prerequisites**

- Verify that the WebService logical switch is available. See Add a Logical Switch.
- Verify that a physical switch is available.

**Procedure**

1. Log in to the vSphere Web Client.
2. Select *Networking & Security > Logical Switches*.
3. Locate the WebService logical switch and right-click to select *Manage Hardware Bindings* from the drop-down menu.
4. Select the hardware gateway profile.
5. Click the Add ((IDC)) icon and select the physical switch from the drop-down menu.
   - For example, AristaGW.
6. Click **Select** to choose a physical port from the Available Objects list.
   - For example, Ethernet 18.
7. Click **OK**.
8. Specify the VLAN name.
   - For example, 160.
9. Click **OK**.

**Results**

The binding is complete.
The NSX Controller synchronizes the physical and logical configuration information with the hardware gateway.
L2 Bridges

You can create an L2 bridge between a logical switch and a VLAN, which enables you to migrate virtual workloads to physical devices with no impact on IP addresses.

A Layer 2 bridge enables connectivity between the virtual and physical network by enabling virtual machines (VMs) to be connected to a physical server or network. Use cases include:

- Physical to virtual, or virtual to virtual migration. L2 bridging allows you to maintain connectivity between workloads inside NSX and outside NSX, without requiring IP re-addressing.

- Insertion into NSX of an appliance that cannot be virtualized, and that require L2 connectivity with its clients. This is common for some physical database servers.

- Service insertion. An L2 Bridge allows integrating transparently into NSX any physical appliance such as a router, load balancer or firewall

A logical network can leverage a physical L3 gateway and access existing physical networks and security resources by bridging the logical switch broadcast domain to the VLAN broadcast domain. The L2 bridge runs on the host that has the NSX Edge logical router virtual machine. An L2 bridge instance maps to a single VLAN, but there can be multiple bridge instances. The logical router cannot be used as a gateway for devices connected to a bridge. The VLAN port group and VXLAN logical switch that is bridged must be on the same vSphere distributed switch (VDS) and both must share same physical NICs.

VXLAN (VNI) network and VLAN-backed port groups must be on the same distributed virtual switch (VDS).
Note that you should not use an L2 bridge to connect a logical switch to another logical switch, a VLAN network to another VLAN network, or to interconnect datacenters. Also, you cannot use a universal logical router to configure bridging and you cannot add a bridge to a universal logical switch.

This chapter includes the following topics:

- Add L2 Bridge
- Add L2 Bridge to a Logically Routed Environment

**Add L2 Bridge**

You can add a bridge from a logical switch to a distributed virtual port group.

**Prerequisites**

A configured logical switch and a VLAN-backed distributed virtual port group.
The logical switch and the VLAN-backed distributed virtual port group that are to be bridged together must exist on the same Virtual Distributed Switch (VDS).

A DLR Control VM on a hypervisor where the VDS with the logical switch and VLAN-backed distributed virtual port group are instantiated must be deployed in your environment.

You cannot use a universal logical router to configure bridging, and you cannot add a bridge to a universal logical switch.

**Caution**  Bridged traffic enters and leaves an ESXi host through the uplink port on the dvSwitch that is used for the VXLAN traffic. VDS teaming or failover policy for VLAN is not used for the bridged traffic.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click a logical router.
4. Click **Manage** and then click **Bridging**.
5. Click the **Add (➕)** icon.
6. Enter a name for the bridge.
   
   **Caution**  Bridge name must not exceed 40 characters. Bridge configuration fails when the name exceeds 40 characters.
7. Select the logical switch that you want to create a bridge for.
8. Select the distributed virtual port group to which you want to bridge the logical switch.
9. Click **OK**.

**Add L2 Bridge to a Logically Routed Environment**

You can bridge a given logical switch to a single VLAN with one active bridge instance. One logical router can have multiple bridging instances, however, the same VXLAN and VLAN cannot connect to more than one bridge instance.

You can use a logical switch to participate in both distributed logical routing and layer 2 bridging. Therefore, the traffic from the bridged logical switch does not need to flow through the centralized Edge VM. The traffic from the bridged logical switch can flow to the physical VLAN through the L2 bridge instance. The bridge instance gets enabled on the ESXi host where the DLR control VM is running.

For more information about L2 bridging in NSX, see the "NSX Distributed Routing and Layer 2 Bridging Integration" section in the *NSX Network Virtualization Design Guide* at https://communities.vmware.com/docs/DOC-27683.

**Prerequisites**

- An NSX logical router must be deployed in your environment.
You cannot use a universal logical router to configure bridging, and you cannot add a bridge to a universal logical switch.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click the logical router that you want to use for bridging.

   **Note**  The bridge instance must be created in the same routing instance to which the VXLAN is connected. One bridge instance can have one VXLAN and one VLAN, and the VXLAN and VLAN cannot overlap. The same VXLAN and VLAN cannot connect to more than one bridge instance.

4. Click **Manage** and then click **Bridging**.

   The logical switch that is being used as a router will state Routing Enabled.

5. Click the **Add (+)** icon.
6. Type a name for the bridge.
7. Select the logical switch that you want to create a bridge for.
8. Select the distributed virtual port group to which you want to bridge the logical switch.
9. Click **OK**.
10. Click **OK** again in the Add Bridge window.
11. Click **Publish** for changes to the bridging configuration to take effect.

   The logical switch that is used for bridging appears with **Routing Enabled** specified. For more information, see Add a Logical Switch and Connect Virtual Machines to a Logical Switch.
**Routing**

You can specify static and dynamic routing for each NSX Edge.

Dynamic routing provides the necessary forwarding information between Layer 2 broadcast domains, thereby allowing you to decrease Layer 2 broadcast domains and improve network efficiency and scale. NSX extends this intelligence to where the workloads reside for doing East-West routing. This allows more direct virtual machine to virtual machine communication without the added cost or time needed to extend hops. At the same time, NSX also provides North-South connectivity, thereby enabling tenants to access public networks.

This chapter includes the following topics:

- Add a Logical (Distributed) Router
- Add an Edge Services Gateway
- Specify Global Configuration
- NSX Edge Configuration
- Add a Static Route
- Configure OSPF on a Logical (Distributed) Router
- Configure OSPF on an Edge Services Gateway
- Configure BGP
- Configure Route Redistribution
- View the NSX Manager Locale ID
- Configure Locale ID on a Universal Logical (Distributed) Router
- Configure Locale ID on a Host or Cluster

**Add a Logical (Distributed) Router**

Logical router kernel modules in the host perform routing between VXLAN networks, and between virtual and physical networks. An NSX Edge appliance provides dynamic routing ability if needed. Logical routers can be created on both primary and secondary NSX Managers in a cross-vCenter NSX environment, but universal logical routers can be created only on the primary NSX Manager.
When deploying a new logical router, consider the following:

- NSX version 6.2 and later allows logical router-routed logical interfaces (LIFs) to be connected to a VXLAN that is bridged to a VLAN.
- Logical router interfaces and bridging interfaces cannot be connected to a dvPortgroup with the VLAN ID set to 0.
- A given logical router instance cannot be connected to logical switches that exist in different transport zones. This is to ensure that all logical switches and logical router instances are aligned.
- A logical router cannot be connected to VLAN-backed port groups if that logical router is connected to logical switches spanning more than one vSphere distributed switch (VDS). This is to ensure correct alignment of logical router instances with logical switch dvPortgroups across hosts.
- Logical router interfaces should not be created on two different distributed port groups (dvPortgroups) with the same VLAN ID if the two networks are in the same vSphere distributed switch.
- Logical router interfaces should not be created on two different dvPortgroups with the same VLAN ID if two networks are in different vSphere distributed switches, but the two vSphere distributed switches share the same hosts. In other words, logical router interfaces can be created on two different networks with the same VLAN ID if the two dvPortgroups are in two different vSphere distributed switches, as long as the vSphere distributed switches do not share a host.
- If VXLAN is configured, logical router interfaces must be connected to distributed port groups on the vSphere Distributed Switch where VXLAN is configured. Do not connect logical router interfaces to port groups on other vSphere Distributed Switches.

The following list describes feature support by interface type (uplink and internal) on the logical router:

- Dynamic routing protocols (BGP and OSPF) are supported only on uplink interfaces.
- Firewall rules are applicable only on uplink interfaces and are limited to control and management traffic that is destined to the Edge virtual appliance.

**Important** If you enable high availability on an NSX Edge in a cross-vCenter NSX environment, both the active and standby NSX Edge appliances must reside within the same vCenter Server. If you migrate one of the members of an NSX Edge HA pair to a different vCenter Server system, the two HA appliances will no longer operate as an HA pair, and you might experience traffic disruption.

**Prerequisites**

- You must have been assigned the Enterprise Administrator or NSX Administrator role.
- You must create a local segment ID pool, even if you have no plans to create NSX logical switches.
- Make sure that the controller cluster is up and available before creating or changing a logical router configuration. A logical router cannot distribute routing information to hosts without the help of NSX controllers. A logical router relies on NSX controllers to function, while Edge Services Gateways (ESGs) do not.
If a logical router is to be connected to VLAN dvPortgroups, ensure that all hypervisor hosts with a logical router appliance installed can reach each other on UDP port 6999. Communication on this port is required for logical router VLAN-based ARP proxy to work.

Determine where to deploy the logical router appliance.

- The destination host must be part of the same transport zone as the logical switches connected to the new logical router's interfaces.

- Avoid placing it on the same host as one or more of its upstream ESGs if you use ESGs in an ECMP setup. You can use DRS anti-affinity rules to enforce this, reducing the impact of host failure on logical router forwarding. This guideline does not apply if you have one upstream ESG by itself or in HA mode. For more information, see the *VMware NSX for vSphere Network Virtualization Design Guide* at https://communities.vmware.com/docs/DOC-27683.

Verify that the host cluster on which you install the logical router appliance is prepared for NSX. See "Prepare Host Clusters for NSX" in the *NSX Installation Guide*.

Determine the appropriate NSX Manager on which to make your changes.

- In a standalone or single vCenter NSX environment there is only one NSX Manager so you do not need to select one.

- Universal objects must be managed from the primary NSX Manager.

- Objects local to an NSX Manager must be managed from that NSX Manager.

- In a cross-vCenter NSX environment that does not have Enhanced Linked Mode enabled, you must make configuration changes from the vCenter linked to the NSX Manager that you want to modify.

- In a cross-vCenter NSX environment in Enhanced Linked Mode, you can make configuration changes to any NSX Manager from any linked vCenter. Select the appropriate NSX Manager from the NSX Manager drop-down menu.

Determine which kind of logical router you need to add:

- If you need to connect a logical switch, you must add a logical router

- If you need to connect a universal logical switch, you must add a universal logical router

- If you are adding a universal logical router, determine if you need to enable local egress. Local egress allows you to selectively send routes to hosts. You may want this ability if your NSX deployment spans multiple sites. See *Cross-vCenter NSX Topologies* for more information. You cannot enable local egress after the universal logical router has been created.

**Procedure**

1. In the vSphere Web Client, navigate to Home > Networking & Security > NSX Edges.

2. Select the appropriate NSX Manager on which to make your changes. If you are creating a universal logical router, you must select the primary NSX Manager.

3. Click the Add (➕) icon.
Select the type of logical router you wish to add:

- Select **Logical (Distributed) Router** to add a logical router local to the selected NSX Manager.
- Select **Universal Logical (Distributed) Router** to add a logical router that can span the cross-vCenter NSX environment. This option will be available only if you have assigned a primary NSX Manager, and are making changes from the primary NSX Manager.

  If you select **Universal Logical (Distributed) Router**, you must also select whether to enable local egress.

Type a name for the device.

This name appears in your vCenter inventory. The name should be unique across all logical routers within a single tenant.

Optionally, you can also enter a hostname. This name appears in the CLI. If you do not specify the host name, the Edge ID, which gets created automatically, is displayed in the CLI.

Optionally, you can enter a description and tenant.

Deploy an Edge appliance.

**Deploy Edge Appliance** is selected by default. An Edge appliance (also called a logical router virtual appliance) is required for dynamic routing and the logical router appliance’s firewall, which applies to logical router pings, SSH access, and dynamic routing traffic.

You can deselect the edge appliance option if you require only static routes, and do not want to deploy an Edge appliance. You cannot add an Edge appliance to the logical router after the logical router has been created.

(Optional) Enable High Availability.

**Enable High Availability** is not selected by default. Select the **Enable High Availability** check box to enable and configure high availability. High availability is required if you are planning to do dynamic routing.

Type and re-type a password for the logical router.

The password must be 12-255 characters and must contain the following:

- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

(Optional) Enable SSH.

By default, SSH is disabled. If you do not enable SSH, you can still access the logical router by opening the virtual appliance console. Enabling SSH here causes the SSH process to run on the logical router virtual appliance. You must adjust the logical router firewall configuration manually to allow SSH access to the logical router’s protocol address. The protocol address is configured when you configure dynamic routing on the logical router.
10 (Optional) Enable FIPS mode and set the log level.

By default, FIPS mode is disabled. Select the **Enable FIPS mode** check box to enable the FIPS mode. When you enable the FIPS mode, any secure communication to or from the NSX Edge uses cryptographic algorithms or protocols that are allowed by FIPS.

By default, the log level is emergency.

For example:

```
<table>
<thead>
<tr>
<th>Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.</td>
</tr>
</tbody>
</table>

User Name: *admin*

Password: ************

Confirm password: ************

- [ ] Enable SSH access
- [ ] Enable FIPS mode

Edge Control Level Logging: **EMERGENCY**
```

11 Configure the deployment.

- If you did not select **Deploy Edge Appliance**, the **Add (avn)** icon is grayed. Click **Next** to continue with configuration.
- If you selected **Deploy Edge Appliance**, enter the settings for the logical router virtual appliance.

For example:

```
Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

- Cluster/Resource Pool: *Management & Edge...
- Datastore: *ds-1
- Host: esxmg-01a.corp.local
- Folder: Discovered virtual mac...
```
12 Configure interfaces. On logical routers, only IPv4 addressing is supported.
   a Configure the HA interface connection, and optionally an IP address.

   If you selected Deploy Edge Appliance, you must connect the HA interface to a distributed port group or logical switch. If you are using this interface as an HA interface only, use a logical switch. A /30 subnet is allocated from the link local range 169.254.0.0/16 and is used to provide an IP address for each of the two NSX Edge appliances.

   Optionally, if you want to use this interface to connect to the NSX Edge, you can specify an additional IP address and prefix for the HA interface.

   **Note** Before NSX 6.2, the HA interface was called the management interface. You cannot SSH into the HA interface from anywhere that is not on the same IP subnet as the HA interface. You cannot configure static routes that point out of the HA interface, which means that RPF will drop incoming traffic. You could, in theory, disable RPF, but this is counterproductive to high availability. For SSH access, you can also use the logical router's protocol address, which is configured later when you configure dynamic routing.

   In NSX 6.2 and later, the HA interface of a logical router is automatically excluded from route redistribution.

   b Configure interfaces of this NSX Edge.

   In Configure interfaces of this NSX Edge the internal interfaces are for connections to switches that allow VM-to-VM (sometimes called East-West) communication. Internal interfaces are created as pseudo vNICs on the logical router virtual appliance. Uplink interfaces are for North-South communication. A logical router uplink interface might connect to an Edge Services Gateway or a third-party router VM. You must have at least one uplink interface for dynamic routing to work. Uplink interfaces are created as vNICs on the logical router virtual appliance.

   The interface configuration that you enter here is modifiable later. You can add, remove, and modify interfaces after a logical router is deployed.

   The following example shows an HA interface connected to the management distributed port group. The example also shows two internal interfaces (app and web) and an uplink interface (to-ESG).
HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Configure interfaces of this NSX Edge

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Subnet Prefix Length</th>
<th>Connected To</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>172.16.20.1*</td>
<td>24</td>
<td>app</td>
</tr>
<tr>
<td>web</td>
<td>172.16.10.1*</td>
<td>24</td>
<td>web</td>
</tr>
<tr>
<td>to-ESG</td>
<td>192.168.10.2*</td>
<td>29</td>
<td>transit</td>
</tr>
</tbody>
</table>
13 Configure a default gateway.

For example:

![Gateway Configuration]

14 Make sure any VMs attached to the logical switches have their default gateways set properly to the logical router interface IP addresses.

**Results**

In the following example topology, the default gateway of app VM is 172.16.20.1. The default gateway of web VM is 172.16.10.1. Make sure the VMs can ping their default gateways and each other.
Connect to the NSX Manager using SSH or the console, and run the following commands:

- List all logical router instance information.

```
nsxmgr-l-01a> show logical-router list all
Edge-id     Vdr Name                      Vdr id              #Lifs
edge-1     default+edge-1                0x00001388          3
```

- List the hosts that have received routing information for the logical router from the controller cluster.

```
nsxmgr-l-01a> show logical-router list dlr edge-1 host
ID       HostName
host-25   192.168.210.52
host-26   192.168.210.53
host-24   192.168.110.53
```

The output includes all hosts from all host clusters that are configured as members of the transport zone that owns the logical switch that is connected to the specified logical router (edge-1 in this example).

- List the routing table information that is communicated to the hosts by the logical router. Routing table entries should be consistent across all the hosts.

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 route
VDR default+edge-1 Route Table
Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

<table>
<thead>
<tr>
<th>Destination</th>
<th>GenMask</th>
<th>Gateway</th>
<th>Flags</th>
<th>Ref Origin</th>
<th>UpTime</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>192.168.10.1</td>
<td>UG</td>
<td>1</td>
<td>AUTO</td>
<td>4101</td>
</tr>
</tbody>
</table>
```

VMware, Inc. 79
List additional information about the router from the point of view of one of the hosts. This output is helpful to learn which controller is communicating with the host.

```
snx-mgr-l-01a> show logical-router host host-25 dlr edge-1 verbose
```

**VDR Instance Information:**

- **Vdr Name:** default+edge-1
- **Vdr Id:** 0x00001388
- **Number of Lifs:** 3
- **Number of Routes:** 5
- **State:** Enabled
- **Controller IP:** 192.168.110.203
- **Control Plane IP:** 192.168.210.52
- **Control Plane Active:** Yes
- **Num unique nexthops:** 1
- **Generation Number:** 0
- **Edge Active:** No

Check the Controller IP field in the output of the `show logical-router host host-25 dlr edge-1 verbose` command.

SSH to a controller, and run the following commands to display the controller's learned VNI, VTEP, MAC, and ARP table state information.

```
192.168.110.202 # show control-cluster logical-switches vni 5000
```

<table>
<thead>
<tr>
<th>VNI</th>
<th>Controller</th>
<th>BUM-Replication</th>
<th>ARP-Proxy</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>192.168.110.201</td>
<td>Enabled</td>
<td>Enabled</td>
<td>0</td>
</tr>
</tbody>
</table>

The output for VNI 5000 shows zero connections and lists controller 192.168.110.201 as the owner for VNI 5000. Log in to that controller to gather further information for VNI 5000.

```
192.168.110.201 # show control-cluster logical-switches vni 5000
```

<table>
<thead>
<tr>
<th>VNI</th>
<th>Controller</th>
<th>BUM-Replication</th>
<th>ARP-Proxy</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>192.168.110.201</td>
<td>Enabled</td>
<td>Enabled</td>
<td>3</td>
</tr>
</tbody>
</table>

The output on 192.168.110.201 shows three connections. Check additional VNIs.

```
192.168.110.201 # show control-cluster logical-switches vni 5001
```

<table>
<thead>
<tr>
<th>VNI</th>
<th>Controller</th>
<th>BUM-Replication</th>
<th>ARP-Proxy</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>5001</td>
<td>192.168.110.201</td>
<td>Enabled</td>
<td>Enabled</td>
<td>3</td>
</tr>
</tbody>
</table>

```
192.168.110.201 # show control-cluster logical-switches vni 5002
```

<table>
<thead>
<tr>
<th>VNI</th>
<th>Controller</th>
<th>BUM-Replication</th>
<th>ARP-Proxy</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>5002</td>
<td>192.168.110.201</td>
<td>Enabled</td>
<td>Enabled</td>
<td>3</td>
</tr>
</tbody>
</table>
Because 192.168.110.201 owns all three VNI connections, we expect to see zero connections on the other controller, 192.168.110.203.

Because 192.168.110.201 owns all three VNI connections, we expect to see zero connections on the other controller, 192.168.110.203.

192.168.110.203 # show control-cluster logical-switches vni 5000
VNI   Controller     BUM-Replication ARP-Proxy Connections
5000  192.168.110.201 Enabled     Enabled     0

Before checking the MAC and ARP tables, ping from one VM to the other VM.

From app VM to web VM:

vmware@app-vm$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=64 time=2.605 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=64 time=1.490 ms
64 bytes from 172.16.10.10: icmp_req=3 ttl=64 time=2.422 ms

Check the MAC tables.

192.168.110.201 # show control-cluster logical-switches mac-table 5000
VNI   MAC               VTEP-IP         Connection-ID
5000  00:50:56:a6:23:ae 192.168.250.52  7

192.168.110.201 # show control-cluster logical-switches mac-table 5001
VNI   MAC               VTEP-IP         Connection-ID
5001  00:50:56:a6:8d:72 192.168.250.51  23

Check the ARP tables.

192.168.110.201 # show control-cluster logical-switches arp-table 5000
VNI   IP              MAC               Connection-ID
5000  172.16.20.10    00:50:56:a6:23:ae 7

192.168.110.201 # show control-cluster logical-switches arp-table 5001
VNI   IP              MAC               Connection-ID
5001  172.16.10.10    00:50:56:a6:8d:72 23

Check the logical router information. Each logical router Instance is served by one of the controller nodes.

The instance subcommand of show control-cluster logical-routers command displays a list of logical routers that are connected to this controller.

The interface-summary subcommand displays the LIFs that the controller learned from the NSX Manager. This information is sent to the hosts that are in the host clusters managed under the transport zone.
The routes subcommand shows the routing table that is sent to this controller by the logical router's virtual appliance (also known as the control VM). Unlike on the ESXi hosts, this routing table does not include directly connected subnets because this information is provided by the LIF configuration. Route information on the ESXi hosts includes directly connected subnets because in that case it is a forwarding table used by ESXi host's datapath.

- List all logical routers connected to this controller.

```
controller # show control-cluster logical-routers instance all
LR-Id LR-Name Universal Service-Controller Egress-Locale
0x1388 default+edge-1 false 192.168.110.201 local
```

Note the LR-Id and use it in the following command.

- Show control clustering logical routers interface summary.

```
controller # show control-cluster logical-routers interface-summary 0x1388
Interface Type Id IP[
13880000000b vxlan 0x1389 172.16.10.1/24
13880000000a vxlan 0x1388 172.16.20.1/24
138800000002 vxlan 0x138a 192.168.10.2/29
```

- Show control clustering logical routers routes.

```
controller # show control-cluster logical-routers routes 0x1388
Destination Next-Hop[] Preference Locale-Id Source
192.168.100.0/24 192.168.10.1 110 00000000-0000-0000-0000-000000000000 CONTROL_VM
0.0.0.0/0 192.168.10.1 0 00000000-0000-0000-0000-000000000000 CONTROL_VM
```

- Display the controller connections to the specific VNI.

```
[root@comp02a:-] esxcfg-route -l
VMkernel Routes:
Network Netmask Gateway Interface
10.20.20.0 255.255.255.0 Local Subnet vmk1
192.168.210.0 255.255.255.0 Local Subnet vmk0
default 0.0.0.0 192.168.210.1 vmk0
```

These Host-IP addresses are vmk0 interfaces, not VTEPs. Connections between ESXi hosts and controllers are created on the management network. The port numbers here are ephemeral TCP ports that are allocated by the ESXi host IP stack when the host establishes a connection with the controller.
On the host, you can view the controller network connection matched to the port number.

```
[root@192.168.110.53:~#] # esxcli network ip connection list | grep 26167
tcp 0 0 192.168.110.53:26167 192.168.110.101:1234 ESTABLISHED
96416 newreno netcpa-worker
```

Display active VNIs on the host. Observe how the output is different across hosts. Not all VNIs are active on all hosts. A VNI is active on a host if the host has a VM that is connected to the logical switch.

```
[root@192.168.210.52:~#] # esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS
VXLAN ID Multicast IP Control Plane Controller Connection
Port Count MAC Entry Count ARP Entry Count VTEP Count
-------- ------------------------- ----------------------------------- ---------------------
---------- --------------- --------------- ----------
5000 N/A (headend replication) Enabled (multicast proxy,ARP proxy) 192.168.110.203
(up) 1 0 0 0
5001 N/A (headend replication) Enabled (multicast proxy,ARP proxy) 192.168.110.202
(up) 1 0 0 0
```

**Note** To enable the vxlan namespace in vSphere 6.0 and later, run the `/etc/init.d/hostd restart` command.

For logical switches in hybrid or unicast mode, the `esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>` command contains the following output:

- Control Plane is enabled.
- Multicast proxy and ARP proxy are listed. AARP proxy is listed even if you disabled IP discovery.
- A valid controller IP address is listed and the connection is up.
- If a logical router is connected to the ESXi host, the port Count is at least 1, even if there are no VMs on the host connected to the logical switch. This one port is the vdrPort, which is a special dvPort connected to the logical router kernel module on the ESXi host.
First ping from VM to another VM on a different subnet and then display the MAC table. Note that the Inner MAC is the VM entry while the Outer MAC and Outer IP refer to the VTEP.

```bash
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5000
Inner MAC          Outer MAC          Outer IP        Flags
-----------------  -----------------  --------------  --------

~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5001
Inner MAC          Outer MAC          Outer IP        Flags
-----------------  -----------------  --------------  --------
00:50:56:f0:d7:e4  00:50:56:6a:65:c2  192.168.250.52  00000111
```

**What to do next**

When you install an NSX Edge appliance, NSX enables automatic VM startup/shutdown on the host if vSphere HA is disabled on the cluster. If the appliance VMs are later migrated to other hosts in the cluster, the new hosts might not have automatic VM startup/shutdown enabled. For this reason, VMware recommends that when you install NSX Edge appliances on clusters that have vSphere HA disabled, you should check all hosts in the cluster to make sure that automatic VM startup/shutdown is enabled. See "Edit Virtual Machine Startup and Shutdown Settings" in *vSphere Virtual Machine Administration*.

After the logical router is deployed, double-click the logical router ID to configure additional settings, such as interfaces, routing, firewall, bridging, and DHCP relay.

**Add an Edge Services Gateway**

You can install multiple NSX Edge services gateway virtual appliances in a data center. Each NSX Edge virtual appliance can have a total of ten uplink and internal network interfaces. The internal interfaces connect to secured port groups and act as the gateway for all protected virtual machines in the port group. The subnet assigned to the internal interface can be a publicly routed IP address space or a NATed/routed RFC 1918 private space. Firewall rules and other NSX Edge services are enforced on traffic between interfaces.

Uplink interfaces of an ESG connect to uplink port groups that have access to a shared corporate network or a service that provides access layer networking.

The following list describes feature support by interface type (internal and uplink) on an ESG.

- **DHCP**: Not supported on uplink interface.
- **DNS Forwarder**: Not supported on uplink interface.
- **HA**: Not supported on uplink interface, requires at least one internal interface.
- **SSL VPN**: Listener IP must belong to uplink interface.
- IPsec VPN: Local site IP must belong to uplink interface.
- L2 VPN: Only internal networks can be stretched.

The following figure shows a sample topology with an ESG’s uplink interface connected to physical infrastructure through the vSphere distributed switch and the ESG’s internal interface connect to an NSX logical router through an NSX logical transit switch.

![Diagram of NSX topology]

Multiple external IP addresses can be configured for load balancing, site-to-site VPN, and NAT services.

**Important** If you enable high availability on an NSX Edge in a cross-vCenter NSX environment, both the active and standby NSX Edge appliances must reside within the same vCenter Server. If you migrate one of the members of an NSX Edge HA pair to a different vCenter Server system, the two HA appliances will no longer operate as an HA pair, and you might experience traffic disruption.
Prerequisites

- You must have been assigned the Enterprise Administrator or NSX Administrator role.
- Verify that the resource pool has enough capacity for the edge services gateway (ESG) virtual appliance to be deployed. See Chapter 1 System Requirements for NSX.
- Verify that the host clusters on which the NSX Edge appliance will be installed are prepared for NSX. See Prepare Host Clusters for NSX in the NSX Installation Guide.

Procedure

1. In vCenter, navigate to Home > Networking & Security > NSX Edges and click the Add (➕) icon.
2. Select Edge Services Gateway and type a name for the device.
   This name appears in your vCenter inventory. The name should be unique across all ESGs within a single tenant.
   Optionally, you can also enter a hostname. This name appears in the CLI. If you do not specify the host name, the Edge ID, which gets created automatically, is displayed in the CLI.
   Optionally, you can enter a description and tenant and enable high availability.
   For example:
3 Type and re-type a password for the ESG.

The password must be at least 12 characters and must follow 3 of the following 4 rules:

- At least one upper case letter
- At least one lower case letter
- At least one number
- At least one special character

4 (Optional) Enable SSH, high availability, automatic rule generation, and FIPS mode, and set the log level.

If you do not enable automatic rule generation, you must manually add firewall, NAT, and routing configuration to allow control traffic for certain, NSX Edge services, including as load balancing and VPN. Auto rule generation does not create rules for data-channel traffic.

By default, SSH and high availability are disabled, and automatic rule generation is enabled.

By default, FIPS mode is disabled.

By default, the log level is emergency.
For example:

5 Select the size of the NSX Edge instance based on your system resources.

The **Large** NSX Edge has more CPU, memory, and disk space than the **Compact** NSX Edge, and supports a larger number of concurrent SSL VPN-Plus users. The **X-Large** NSX Edge is suited for environments that have a load balancer with millions of concurrent sessions. The Quad Large NSX Edge is recommended for high throughput and requires a high connection rate.

See Chapter 1 System Requirements for NSX.

6 Create an edge appliance.

Enter the settings for the ESG virtual appliance that will be added to your vCenter inventory. If you do not add an appliance when you install NSX Edge, NSX Edge remains in an offline mode until you add an appliance.

If you enabled HA you can add two appliances. If you add a single appliance, NSX Edge replicates its configuration for the standby appliance and ensures that the two HA NSX Edge virtual machines are not on the same ESX host even after you use DRS and vMotion (unless you manually vMotion them to the same host). For HA to work correctly, you must deploy both appliances on a shared datastore.

For example:
Select **Deploy NSX Edge** to add the Edge in a deployed mode. You must configure appliances and interfaces for the Edge before it can be deployed.

8 Configure interfaces.

On ESGs, both IPv4 and IPv6 addresses are supported.

You must add at least one internal interface for HA to work.

An interface can have multiple non-overlapping subnets.

If you enter more than one IP address for an interface, you can select the primary IP address. An interface can have one primary and multiple secondary IP addresses. NSX Edge considers the primary IP address as the source address for locally generated traffic, for example remote syslog and operator-initiated pings.

You must add an IP address to an interface before using it on any feature configuration.

Optionally, you can enter the MAC address for the interface.

If you change the MAC address using API call later, you must redeploy the edge after changing the MAC address.

If HA is enabled, you can optionally enter two management IP addresses in CIDR format. Heartbeats of the two NSX Edge HA virtual machines are communicated through these management IP addresses. The management IP addresses must be in the same L2/subnet and be able to communicate with each other.

Optionally, you can modify the MTU.

Enable proxy ARP if you want to allow the ESG to answer ARP requests intended for other machines. This is useful, for example, when you have the same subnet on both sides of a WAN connection.

Enable ICMP redirect to convey routing information to hosts.

Enable reverse path filtering to verify the reachability of the source address in packets being forwarded. In enabled mode, the packet must be received on the interface that the router would use to forward the return packet. In loose mode, the source address must appear in the routing table.
Configure fence parameters if you want to reuse IP and MAC addresses across different fenced environments. For example, in a cloud management platform (CMP), fencing allow you to run several cloud instances simultaneous with the same IP and MAC addresses completely isolated or “fenced.”

For example:

The following example shows two interfaces, one attaching the ESG to the outside world through an uplink portgroup on a vSphere distributed switch and the other attaching the ESG to a logical transit switch to which a distributed logical router is also attached.
9 Configure a default gateway.

You can edit the MTU value, but it cannot be more than the configured MTU on the interface.

For example:
Configure the firewall policy, logging, and HA parameters.

**Caution** If you do not configure the firewall policy, the default policy is set to deny all traffic.

By default, logs are enabled on all new NSX Edge appliances. The default logging level is NOTICE. If logs are stored locally on the ESG, logging may generate too many logs and affect the performance of your NSX Edge. For this reason, it is recommended that you configure remote syslog servers, and forward all logs to a centralized collector for analysis and monitoring.

If you enabled high availability, complete the HA section. By default, HA automatically chooses an internal interface and automatically assigns link-local IP addresses. NSX Edge supports two virtual machines for high availability, both of which are kept up to date with user configurations. If a heartbeat failure occurs on the primary virtual machine, the secondary virtual machine state is changed to active. Thus, one NSX Edge virtual machine is always active on the network. NSX Edge replicates the configuration of the primary appliance for the standby appliance and ensures that the two HA NSX Edge virtual machines are not on the same ESX host even after you use DRS and vMotion. Two virtual machines are deployed on vCenter in the same resource pool and datastore as
the appliance you configured. Local link IP addresses are assigned to HA virtual machines in the NSX Edge HA so that they can communicate with each other. Select the internal interface for which to configure HA parameters. If you select ANY for interface but there are no internal interfaces configured, the UI displays an error. Two Edge appliances are created but since there is no internal interface configured, the new Edge remains in standby and HA is disabled. Once an internal interface is configured, HA will get enabled on the Edge appliance. Type the period in seconds within which, if the backup appliance does not receive a heartbeat signal from the primary appliance, the primary appliance is considered inactive and the backup appliance takes over. The default interval is 15 seconds. Optionally, you can enter two management IP addresses in CIDR format to override the local link IP addresses assigned to the HA virtual machines. Ensure that the management IP addresses do not overlap with the IP addresses used for any other interface and do not interfere with traffic routing. You should not use an IP address that exists somewhere else on your network, even if that network is not directly attached to the NSX Edge.

For example:
Results
After the ESG is deployed, go to the Hosts and Clusters view and open the console of the edge virtual appliance. From the console, make sure you can ping the connected interfaces.

What to do next
When you install an NSX Edge appliance, NSX enables automatic VM startup/shutdown on the host if vSphere HA is disabled on the cluster. If the appliance VMs are later migrated to other hosts in the cluster, the new hosts might not have automatic VM startup/shutdown enabled. For this reason, VMware recommends that when you install NSX Edge appliances on clusters that have vSphere HA disabled, you should check all hosts in the cluster to make sure that automatic VM startup/shutdown is enabled. See “Edit Virtual Machine Startup and Shutdown Settings” in vSphere Virtual Machine Administration.

Now you can configure routing to allow connectivity from external devices to your VMs.

Specify Global Configuration
You can configure the default gateway for static routes and specify dynamic routing details for an Edge Services Gateway or Distributed Logical Router.

You must have a working NSX Edge instance before you can configure routing on it. For information on setting up NSX Edge, see NSX Edge Configuration.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click Routing and then click Global Configuration.
5. To enable equal-cost multi-path routing (ECMP), next to ECMP, click Start.

ECMP is a routing strategy that allows next-hop packet forwarding to a single destination over multiple best paths. These best paths can be added as static routes or as a result of metric calculations by dynamic routing protocols like OSPF or BGP. Multiple paths for static routes can be added by providing multiple next hops separated by commas in the Static Routes dialog box. For more information, see Add a Static Route.

The Edge Services Gateway uses the Linux network stack implementation, a round-robin algorithm with a randomness component. After a next hop is selected for a particular source and destination IP address pair, the route cache stores the selected next hop. All packets for that flow go to the selected next hop. The default IPv4 route cache timeout is 300 seconds (gc_timeout). If an entry is inactive for this time, it is eligible to be removed from the route cache. The actual removal happens when garbage collection timer activates (gc_interval = 60 seconds).

The Distributed Logical Router uses an XOR algorithm to determine the next hop from a list of possible ECMP next hops. This algorithm uses the source and destination IP address on the outgoing packet as sources of entropy.
Stateful services such as Load Balancing, VPN, NAT, and ESG firewall do not work with ECMP. However, from NSX 6.1.3 onwards, ECMP and Distributed Firewall can work together.

6 (Only for UDLR): To change the **Locale ID** on a universal distributed logical router, next to **Routing Configuration**, click **Edit**. Enter a locale ID and click **Save** or **OK**.

By default, the locale ID is set to the NSX Manager UUID. However, you can override the locale ID by enabling local egress at the time of creating the universal distributed logical router. Locale ID is used to selectively configure routes in a cross-vCenter NSX or multi-site environment. See [Cross-vCenter NSX Topologies](#) for more information.

The locale ID must be in UUID format. For example, XXXXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, where each X is replaced with a base 16 digit (0-F).

7 To specify the default gateway, click **Edit** next to **Default Gateway**.
   a Select an interface from which the next hop towards the destination network can be reached.
   b Type the Gateway IP.
   c (Optional) Type the locale ID. Locale ID is available only on universal logical routers.
   d (Optional) Edit the MTU.
   e If prompted, type the **Admin Distance**.
      Choose a value between 1 and 255. The admin distance is used to choose which route to use when there are multiple routes for a given network. The lower the admin distance, the higher the preference for the route.

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default admin distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>0</td>
</tr>
<tr>
<td>Static</td>
<td>1</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>OSPF Intra-Area</td>
<td>30</td>
</tr>
<tr>
<td>OSPF Inter-Area</td>
<td>110</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
</tbody>
</table>

f (Optional) Type a Description for the default gateway.

g Click **Save**.
8 To configure dynamic routing, click **Edit** next to **Dynamic Routing Configuration**.
   a **Router ID** displays the first uplink IP address of the NSX Edge that pushes routes to the kernel for dynamic routing.
   b Do not enable any protocols here.
   c Select **Enable Logging** to save logging information and select the log level.

**Note** If you have IPSec VPN configured in your environment, you should not use dynamic routing.

9 Click **Publish Changes**.

**What to do next**

To delete routing configuration, click **Reset**. This deletes all routing configurations (default, static, OSPF, and BGP configurations, as well as route redistribution).

**NSX Edge Configuration**

Once you have installed a working NSX Edge (i.e. added one or more appliances and interfaces, and configured the default gateway, firewall policy, and high availability), you can begin using NSX Edge services.

**Working with Certificates**

NSX Edge supports self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA.

**Configure a CA Signed Certificate**

You can generate a CSR and get it signed by a CA. If you generate a CSR at the global level, it is available to all NSX Edges in your inventory.

**Procedure**

1 Do one of the following.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To generate a global certificate</td>
<td>a Log in to the NSX Manager Virtual Appliance.</td>
</tr>
<tr>
<td></td>
<td>b Click the Manage tab and then click SSL Certificates.</td>
</tr>
<tr>
<td></td>
<td>c Click <strong>Generate CSR</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To generate a certificate for an NSX Edge</td>
<td>a Log in to the vSphere Web Client.</td>
</tr>
<tr>
<td></td>
<td>b Click <strong>Networking &amp; Security</strong> and then click <strong>Edge Services</strong>.</td>
</tr>
<tr>
<td></td>
<td>c Double-click an NSX Edge.</td>
</tr>
<tr>
<td></td>
<td>d Click the <strong>Manage</strong> tab and then click <strong>Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>e Click the <strong>Certificates</strong> link.</td>
</tr>
<tr>
<td></td>
<td>f Click <strong>Actions</strong> and select <strong>Generate CSR</strong>.</td>
</tr>
</tbody>
</table>

2 Type your organization unit and name.
3. Type the locality, street, state, and country of your organization.

4. Select the encryption algorithm for communication between the hosts.
   Note that SSL VPN-Plus only supports RSA certificates.

5. Edit the default key size if required.

6. For a global certificate, type a description for the certificate.

7. Click OK.
   The CSR is generated and displayed in the Certificates list.

8. Have an online Certification Authority sign this CSR.

9. Import the signed certificate.
   a. Copy the contents of the signed certificate.
   b. Do one of the following.
      i. To import a signed certificate at the global level, click Import in the NSX Manager Virtual Appliance.
      ii. To import a signed certificate for an NSX Edge, click Actions and select Import Certificate in the Certificates tab.
   c. In the Import CSR dialog box, paste the contents of the signed certificate.
   d. Click OK.
   The CA signed certificate appears in the certificates list.

Add a CA Certificate
By adding a CA certificate, you can become an interim CA for your company. You then have the authority for signing your own certificates.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then ensure that you are in the Settings tab.
5. Click Certificates.
6. Click the Add (/GPL) icon and select CA Certificate.
7. Copy and paste the certificate contents in the Certificate contents text box.
8. Type a description for the CA certificate.
9. Click OK.
   You can now sign your own certificates.
Add a Chained Certificate

To add a server certificate that is chained with the intermediary and root CA certificates, you require a server certificate (PEM file), a private key for the server, an intermediate and a root certificate.

To import the server certificate as a certificate that is chained with the intermediary certificate on the NSX Edge:

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then ensure that you are in the Settings tab.
5. Click Certificates.
6. Click the Add (➕) icon and select Certificate.
7. In the Certificates Contents text box, paste the contents of the server cert.pem file, and then append the content of the intermediary certificates and the root certificate.

   In the certificate chain, the order of certificates must be as follows:
   - Server certificate
   - Any number of intermediate CA certificates
   - Root CA certificate

   Each certificate must include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines, as shown in the following example:

   -----BEGIN CERTIFICATE-----
   Server cert
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   Intermediate cert
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   Root cert
   -----END CERTIFICATE-----

8. In the Private Key text box, paste the private key contents of the server.

   Following is an example of the private key content:

   -----BEGIN RSA PRIVATE KEY-----
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   -----END RSA PRIVATE KEY-----

9. Enter the password for the private key of the server and reenter the password to confirm.
10 (Optional) Enter a description for the chained certificate.

11 Click OK.

Results
After the certificates are imported the server certificate chained with its intermediary certificates should be displayed under Certificate Details.

Configure a Self-Signed Certificate
You can create, install, and manage self-signed server certificates.

Prerequisites
Verify that you have a CA certificate so that you can sign your own certificates.

Procedure
1 Log in to the vSphere Web Client.

2 Click Networking & Security and then click NSX Edges.

3 Double-click an NSX Edge.

4 Click the Manage tab and then ensure that you are in the Settings tab.

5 Click Certificates.

6 Follow the steps below to generate a CSR.
   a Click Actions and select Generate CSR.
   b In Common name, type the IP address or fully qualified domain name (FQDN) of the NSX Manager.
   c Type your organization name and unit.
   d Type the locality, street, state, and country of your organization.
   e Select the encryption algorithm for communication between the hosts.
      Note that SSL VPN-Plus only supports RSA certificates. VMware recommends RSA for backward compatibility.
   f Edit the default key size if required.
   g Type a description for the certificate.
   h Click OK.
The CSR is generated and displayed in the Certificates list.

7 Verify that the certificate you generated is selected.

8 Click Actions and select Self Sign Certificate.

9 Type the number of days the self sign certificate is valid for.

10 Click OK.
Using Client Certificates

After generating a client certificate, you can distribute this certificate to your remote users, who can install the certificate on their web browser.

The main benefit of implementing client certificates is that the NSX Edge Load Balancer can ask the client for its client certificate, and validate it before forwarding its web requests to the backend servers. If a client certificate is revoked because it has been lost, or the client doesn't work in the company anymore, NSX Edge will validate the client certificate doesn't belong to the Certification Revocation List.

NSX Edge Client certificates are configured under Application Profile.

For more information on generating client certificates, refer to Scenario: SSL Client and Server Authentication.

Add a Certificate Revocation List

A Certificate Revocation List (CRL) is a list of subscribers and their status, which is provided and signed by Microsoft.

The list contains the following items:

- The revoked certificates and the reasons for revocation
- The dates that the certificates are issued
- The entities that issued the certificates
- A proposed date for the next release

When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then ensure that you are in the Settings tab.
5. Click Certificates.
6. Click the Add (+) icon and select CRL.
7. In Certificate contents, paste the list.
8. (Optional) Type a description.
9. Click OK.
FIPS Mode

When you enable the FIPS mode, any secure communication to or from the NSX Edge uses cryptographic algorithms or protocols that are allowed by United States Federal Information Processing Standards (FIPS). FIPS mode turns on the cipher suites that comply with FIPS.

If you configure components those are not FIPS compliant on a FIPS enabled edge, or if you enable FIPS on a edge which has ciphers or authentication mechanism that is not FIPS compliant, NSX Manager will fail the operation and provide a valid error message.

Functionality Difference Between FIPS Mode And Non-FIPS Mode

<table>
<thead>
<tr>
<th>Component</th>
<th>Functionality</th>
<th>FIPS Mode</th>
<th>Non-FIPS Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL VPN</td>
<td>RADIUS Authentication</td>
<td>Not Available</td>
<td>Available</td>
</tr>
<tr>
<td>SSL VPN</td>
<td>RSA Authentication</td>
<td>Not Available</td>
<td>Available</td>
</tr>
<tr>
<td>TLS Protocol</td>
<td>TLSv1.0</td>
<td>Not Available</td>
<td>Available</td>
</tr>
<tr>
<td>Routing</td>
<td>OSPF, BGP - Password MD5 Authentication</td>
<td>Not Available</td>
<td>Available</td>
</tr>
<tr>
<td>IPSec VPN</td>
<td>PSK Authentication</td>
<td>Not Available</td>
<td>Available</td>
</tr>
<tr>
<td>IPSec VPN</td>
<td>DH2 and DH5 groups</td>
<td>Not Available</td>
<td>Available</td>
</tr>
<tr>
<td>IPSec VPN</td>
<td>DH14, DH15, and DH16 groups</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>IPSec VPN</td>
<td>AES-GCM Algorithm</td>
<td>Not Available</td>
<td>Available</td>
</tr>
</tbody>
</table>

Change FIPS Mode on NSX Edge

Enabling the FIPS mode turns on the cipher suites that comply with FIPS. Thus, any secure communication to or from the NSX Edge uses cryptographic algorithms or protocols that are allowed by FIPS.

Caution Changing FIPS mode reboots the NSX Edge appliance causing temporary traffic disruption. This applies whether or not high availability is enabled.

Depending on your requirements, you can enable FIPS on some or all of your NSX Edge appliances. FIPS-enabled NSX Edge appliances can communicate with NSX Edge appliances that do not have FIPS enabled.

If a logical (distributed) router is deployed without an NSX Edge appliance, you cannot modify the FIPS mode. The logical router automatically gets the same FIPS mode as the NSX Controller cluster. If the NSX Controller cluster is NSX 6.3.0 or later, FIPS is enabled.

To change FIPS mode on a universal logical (distributed) router in a cross-vCenter NSX environment that has multiple NSX Edge appliances deployed in the primary and secondary NSX Managers, you must change FIPS mode on all the NSX Edge appliances associated with the universal logical (distributed) router.

If you change FIPS mode on an NSX Edge appliances with high availability enabled, FIPS will be enabled on both appliances, and the appliances will be rebooted one after the other.
If you want to change FIPS mode for a standalone edge, use the `fips enable` or `fips disable` command. For more information, refer to *NSX Command Line Interface Reference*.

**Prerequisites**

- If you have upgraded from an earlier version of NSX, do not enable FIPS mode until the upgrade to NSX 6.3.0 is complete. See Understand FIPS Mode and NSX Upgrade in the *NSX Upgrade Guide*.
- Verify that the NSX Manager is NSX 6.3.0 or later.
- Verify that the NSX Controller cluster is NSX 6.3.0 or later.
- Verify that all host clusters running NSX workloads are prepared with NSX 6.3.0 or later.
- Verify that all NSX Edge appliances are version 6.3.0 or later.
- Verify that the messaging infrastructure has status GREEN. Use the API method `GET /api/2.0/nwfabric/status?resource={resourceId}`, where resourceId is the vCenter Managed Object ID of a host or cluster. Look for the `status` corresponding to the `featureId` of com.vmware.vshield.vsm.messagingInfra in the response body:

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

**Procedure**

1. Log in to the vSphere Web Client.

2. Click **Networking & Security** and then click **NSX Edges**.

3. Select the required edge or router, click **Actions (>)** and select **Change FIPS mode**.

The **Change FIPS mode** dialog box appears.
4 Select or deselect the **Enable FIPS** check box. Click **OK**.

The NSX Edge reboots, and FIPS mode is enabled.

**What to do next**

Optionally, **Change FIPS Mode and TLS Settings on NSX Manager**.

### Managing Appliances

You can add, edit, or delete appliances. An NSX Edge instance remains offline till at least one appliance has been added to it.

**Add an Appliance**

You must add at least one appliance to NSX Edge before deploying it.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click the **Manage** tab and then click the **Settings** tab.
5. In **Edge Gateway Appliances**, click the **Add (+)** icon.
6. Select the cluster or resource pool and datastore for the appliance.
7. (Optional) Select the host on which the appliance is to be added.
8. (Optional) Select the vCenter folder within which the appliance is to be added.
9. Click **Add**.

**Edit an Appliance**

You can edit a NSX Edge appliance.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click the **Manage** tab and then click the **Settings** tab.
5. In **Edge Gateway Appliances**, select the appliance to change.
6. Click the **Edit (EDIT)** icon.
7. In the Edit Edge Appliance dialog box, make the appropriate changes.
8. Click **Save**.
Delete an Appliance

You can delete an NSX Edge appliance.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the Settings tab.
5. In Edge Gateway Appliances, select the appliance to delete.
6. Click the Delete (x) icon.

Managing NSX Edge Appliance Resource Reservations

NSX for vSphere uses vSphere resource allocation to reserve resources for NSX Edge appliances. Reserving CPU and memory resources for NSX Edge ensures that the appliance has enough resources to function correctly.

You can set the resource reservation of an NSX Edge appliance using the API. You can configure the reservation when you create an NSX Edge using POST /api/4.0/edges. You can also update the reservation for an existing NSX Edge using PUT /api/4.0/edges/{edgeId}/appliances. You set the resource reservation using cpuReservation > reservation and memoryReservation > reservation. See the NSX API Guide for details.

Starting in NSX 6.3.3, you can also set the resource reservation of an NSX Edge appliance using the vSphere Web Client. You are prompted to provide a reservation method when you create an NSX Edge. You can also change the reservation of an existing NSX Edge by editing the appliance. Navigate to Networking & Security > NSX Edges > NSX Edge Instance > Manage > Settings > Configuration and edit the appliance.

There are three methods of resource reservation: System Managed, Custom, or No Reservation

**Important** If you select Custom or No Reservation reservations for an NSX Edge appliance, you cannot switch back to System Managed.

System Managed Resource Reservation

If you select System Managed, the system reserves CPU and memory resources for the new NSX Edge appliance. The reserved resources are equal to the system requirements for the appliance size, modified by any percentages that are set using the tuning configuration API.

If you create an NSX Edge appliance using the API and do not explicitly set CPU or memory reservations in the request, this is equivalent to setting the resource reservation to System Managed in the vSphere Web Client.
When an NSX Edge appliance with **System Managed** resource reservation is deployed (during install, upgrade, or redeploy), the reservation is applied on the resource pool after the appliance is powered on. If there are insufficient resources, the reservation fails and generates a system event, but the appliance deployment succeeds. The reservation is attempted the next time the appliance is deployed (during upgrade or deploy).

With **System Managed** resource reservations, if you change the appliance size, the system updates the resource reservations to match the system requirements of the new appliance size.

**Custom Resource Reservation**

If you select **Custom**, you determine the resource reservations for the NSX Edge appliance.

If you create an NSX Edge appliance using the API and explicitly set CPU or memory reservations in the request, this is equivalent to setting the resource reservation to **Custom** in the vSphere Web Client.

When an NSX Edge appliance with **Custom** resource reservation is deployed (during install, upgrade, or redeploy), the reservation is applied on the resource pool before the appliance is powered on. If there are insufficient resources, the appliance fails to power on and the appliance deployment fails.

You can apply **Custom** reservations after an NSX Edge appliance is deployed. The configuration change fails if the resource pool does not have sufficient resources.

With **Custom** resource reservations, the system does not add or change resource reservations for the appliance. If you change the appliance size, the appliance system requirements change, but the system does not update the resource reservations. You should change the resource reservation to reflect the system requirements of the new appliance size.

You can change a custom resource reservation using the vSphere Web Client or the API.

**No Resource Reservation**

If you select **No reservation**, no resources are reserved for the NSX Edge appliance. You are not prevented from deploying NSX Edge appliances on hosts that do not have sufficient resources, but the appliances might not operate correctly if there is resource contention.

If you create an NSX Edge appliance using the API and explicitly set the CPU and memory reservations to 0, this is equivalent to setting the resource reservation to **No reservation** in the vSphere Web Client.

**Modifying the System Managed Resource Reservation Using Tuning Configuration**

When facing lack of resources, you can temporarily disable the **System Managed** resource reservations or decrease the default value. You can change the reservation by configuring values for the `edgeVCpuReservationPercentage` and `edgeMemoryReservationPercentage` parameters in the tuning configuration API, `PUT /api/4.0/edgePublish/tuningConfiguration`. This change affects new NSX Edge appliance deployments, but not existing appliances. The percentages modify the default CPU and memory reserved for the relevant NSX Edge appliance size. To disable the resource reservation, set the values to 0. See the **NSX API Guide** for details.
NSX Edge Appliance System Requirements

The system requirements for NSX Edge appliances depend on the appliance size: Compact, Large, Quad Large, or X-Large. These values are used for the default System Managed resource reservation.

Table 9-2. NSX Edge System Requirements

<table>
<thead>
<tr>
<th>Appliance Size</th>
<th>CPU Reservation</th>
<th>Memory Reservation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact</td>
<td>1000 MHz</td>
<td>512 MB</td>
</tr>
<tr>
<td>Large</td>
<td>2000 MHz</td>
<td>1 GB</td>
</tr>
<tr>
<td>Quad Large</td>
<td>4000 MHz</td>
<td>2 GB</td>
</tr>
<tr>
<td>X-Large</td>
<td>6000 MHz</td>
<td>8 GB</td>
</tr>
</tbody>
</table>

Working with Interfaces

An NSX Edge services gateway can have up to ten internal, uplink, or trunk interfaces. An NSX Edge router can have eight uplink interfaces and up to a thousand internal interfaces.

An NSX Edge must have at least one internal interface before it can be deployed.

Configure an Interface

Internal interfaces are generally for East-West traffic, while uplink interfaces are for North-South traffic. When a logical router (DLR) is connected to an edge services gateway (ESG), the interface on the router is an uplink interface, while the interface on the ESG is an internal interface. An NSX trunk interface is for internal networks, not external networks. The trunk interface allows multiple internal networks (either VLAN or VXLAN) to be trunked.

An NSX edge services gateway (ESG) can have up to ten internal, uplink, or trunk interfaces. These limits are enforced by the NSX Manager.

An NSX deployment can have up to 1,000 distributed logical router (DLR) instances on a single ESXi host. On a single logical router, you can configure up to 8 uplink interfaces, and up to 991 internal interfaces. These limits are enforced by the NSX Manager. For more information about interface scaling in an NSX deployment, see the VMware® NSX for vSphere Network Virtualization Design Guide at https://communities.vmware.com/docs/DOC-27683.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the Interfaces tab.
5. Select an interface and click the Edit (-pencil) icon.
6. In the Edit Edge Interface dialog box, type a name for the interface.
7 Select Internal or Uplink to indicate whether this is an internal or external interface.
   Select Trunk when creating a sub interface. For more information, see Add a Sub Interface.

8 Select the port group or logical switch to which this interface should be connected.
   a. Click Select next to the Connected To field.
   b. Depending on what you want to connect to the interface, click the Logical Switch, Standard Portgroup, or Distributed Portgroup tab.
   c. Select the appropriate logical switch or portgroup.
   d. Click Select.

9 Select the connectivity status for the interface.

10 In Configure Subnets, click the Add (+) icon to add a subnet for the interface.
    An interface can have multiple non-overlapping subnets.

11 In Add Subnet, click the Add (+) icon to add an IP address.
    If you enter more than one IP address, you can select the Primary IP address. An interface can have one primary and multiple secondary IP addresses. NSX Edge considers the Primary IP address as the source address for locally generated traffic.
    You must add an IP address to an interface before using it on any feature configuration.

12 Type the subnet mask for the interface and click Save.

13 Change the default MTU if required.

14 In Options, select the required options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Proxy ARP</td>
<td>Supports overlapping network forwarding between different interfaces.</td>
</tr>
<tr>
<td>Send ICMP Redirect</td>
<td>Conveys routing information to hosts.</td>
</tr>
<tr>
<td>Reverse Path Filter</td>
<td>Verifies the reachability of the source address in packets being forwarded. In enabled mode, the packet must be received on the interface that the router would use to forward the return packet. In loose mode, the source address must appear in the routing table.</td>
</tr>
</tbody>
</table>

15 Type the fence parameters and click Add.

16 Click OK.

Delete an Interface
You can delete an NSX Edge interface.

Procedure
1 Log in to the vSphere Web Client.
2 Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the **Manage** tab and then click the **Interfaces** tab.
5. Select the interface to delete.
6. Click the **Delete (×)** icon

**Enable an Interface**

An interface must be enabled for NSX Edge to isolate the virtual machines within that interface (port group or logical switch).

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click the **Manage** tab and then click the **Interfaces** tab.
5. Select the interface to enable.
6. Click the **Enable (✓)** icon.

**Disable an Interface**

You can disable an interface on an NSX Edge.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click the **Manage** tab and then click the **Interfaces** tab.
5. Select the interface to disable.
6. Click the **Disable** icon.

**Change Traffic Shaping Policy**

You can change the traffic shaping policy on the vSphere Distributed Switch for an NSX Edge interface.

**Procedure**

1. Double-click an NSX Edge and navigate to **Manage > Settings > Interfaces**.
2. Select an interface.
3. Click **Actions > Configure Traffic Shaping Policy**.
4 Make appropriate changes.
   For more information on the options, see Traffic Shaping Policy.

5 Click OK.

**Add a Sub Interface**

You can add a sub interface on a trunk vNIC, which can then be used by NSX Edge services.

![Subinterface Diagram]

Trunk interfaces can be of the following types:

- VLAN trunk is standard and works with any version of ESXi. This is used to bring tagged VLAN traffic into Edge.
- VXLAN trunk works with NSX version 6.1, and later. This is used to bring VXLAN traffic into Edge.

A sub interface can be used by the following Edge services:

- DHCP
- Routing (BGP and OSPF)
- Load Balancer
- IPSec VPN: IPSec VPN can only configured as an uplink interface. Sub interface can be used for private traffic to traverse over the IPSec tunnel. If IPSec policy is configured for the private traffic, sub interface acts as a gateway for the private local subnet.
- L2 VPN
- NAT

A sub interface cannot be used for HA or Logical Firewall. You can, however, use the IP address of the sub interface in a firewall rule.

**Procedure**

1 In the Manage > Settings tab for an NSX Edge, click Interfaces.

2 Select an interface and click the Edit (📝) icon.

3 In the Edit Edge Interface dialog box, type a name for the interface.
4 In Type, select **Trunk**.

5 Select the standard portgroup or distributed portgroup to which this interface should be connected.
   a Click **Change** next to the **Connected To** field.
   b Depending on what you want to connect to the interface, click the **Standard Portgroup** or **Distributed Portgroup** tab.
   c Select the appropriate portgroup and click **OK**.
   d Click **Select**.

6 In Sub Interfaces, click the **Add** icon.

7 Click **Enable Sub interface** and type a name for the sub interface.

8 In **Tunnel Id**, type a number between 1 and 4094.
   The tunnel Id is used to connect the networks that are being stretched. This value must be the same on both the client and server sites.

9 In **Backin Type**, select one of the following to indicate the network backing for the sub interface.
   - **VLAN** for a VLAN network.
     Type the VLAN ID of the virtual LAN that your sub interface should use. VLAN IDs can range from 0 to 4094.
   - **Network** for a VLAN or VXLAN network.
     Click **Select** and select the distributed portgroup or logical switch. NSX Manager extracts the VLAN ID and uses it in trunk configuration.
   - **None** to create a sub interface without specifying a network or VLAN ID. This sub interface is internal to NSX Edge, and is used to route packets between a stretched network and an unstretched (untagged) network

10 To add subnets to the sub interface, click the **Add** icon in the Configure Subnets area.

11 In Add Subnets, click the **Add** icon to add an IP address. Type the IP address and click **OK**.
   If you enter more than one IP address, you can select the Primary IP address. An interface can have one primary and multiple secondary IP addresses. NSX Edge considers the Primary IP address as the source address for locally generated traffic.

12 Type the subnet prefix length and click **OK**.

13 Edit the default **MTU** value for the sub interface if required.
   The default MTU for a trunk interface is 1600 and the default MTU for a sub interface is 1500. The MTU for the sub interface should be equal to or less than the lowest MTU among all the trunk interfaces for the NSX Edge.

14 Select **Enable Send Redirect** to convey routing information to hosts.
Enable or Disable Reverse Path Filter.

Reverse Path Filter verifies the reachability of the source address in packets being forwarded. In enabled mode, the packet must be received on the interface that the router would use to forward the return packet. In loose mode, the source address must appear in the routing table.

Click OK to return to Trunk Interface window.

Enter the MAC address for the interface if needed. Enter two MAC addresses if using ESG HA. If not needed, they will be autogenerated.

Edit the default MTU of the trunk interface, if required.

The default MTU for a trunk interface is 1600, and the default MTU for a sub interface is 1500. The MTU for the trunk interface should be equal to or more than the MTU of the sub interface.

Click OK.

Results

You can now use the sub-interface on Edge services.

What to do next

Configure VLAN trunk if the sub interface added to a trunk vNic is backed by standard portgroup. See Configure VLAN Trunk.

Configure VLAN Trunk

When you add sub interfaces on the trunk vNic of an edge that is connected to a distributed portgroup, both VLAN trunk and VXLAN trunk are supported. When you add sub interfaces on the trunk vNic of an Edge that is connected to a standard portgroup, only VLAN trunk is supported.

Prerequisites

Verify that a sub interface with a trunk vNic backed by standard portgroup is available. See Add a Sub Interface.

Procedure

1 Log in to the vCenter Web Client.
2 Click Networking.
3 Select the standard portgroup and click Edit Settings.
4 Click the VLAN tab.
5 In VLAN Type, select VLAN Trunking and type the VLAN IDs to be trunked.
6 Click OK.
Change Auto Rule Configuration

If auto rule generation is enabled, NSX Edge adds firewall, NAT, and routing routes to enable control traffic to flow for these services. If auto rule generation is not enabled, you must manually add firewall, NAT, and routing configuration to allow control channel traffic for NSX Edge services such as Load Balancing, VPN, etc.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the Settings tab. Click Configuration.
5. In the Details panel, click Action ( ) and select Change Auto Rule configuration.
6. Make the appropriate changes and click OK.

Change CLI Credentials

You can edit the credentials to be used for logging in to the Command Line Interface (CLI).

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the Settings tab. Click Configuration.
5. In the Details panel, click Action ( ) and select Change CLI Credentials.
6. Enter and confirm the new password and click OK.

About High Availability

High Availability (HA) ensures that the services provided by NSX Edge appliances are available even when a hardware or software failure renders a single appliance unavailable. NSX Edge HA minimizes failover downtime instead of delivering zero downtime, as the failover between appliances might require some services to be restarted.

For example, NSX Edge HA synchronizes the connection tracker of the stateful firewall, or the stateful information held by the load balancer. The time required to bring all services backup is not null. Examples of known service restart impacts include a non-zero downtime with dynamic routing when an NSX Edge is operating as a router.
Sometimes, the two NSX Edge HA appliances are unable to communicate and unilaterally decide to become active. This behavior is expected to maintain availability of the active NSX Edge services if the standby NSX Edge is unavailable. If the other appliance still exists, when the communication is re-established, the two NSX Edge HA appliances renegotiate active and standby status. If this negotiation does not finish and if both appliances declare they are active when the connectivity is re-established, an unexpected behavior is observed. This condition, known as split brain, is observed due to the following environmental conditions:

- Physical network connectivity issues, including a network partition.
- CPU or memory contention on the NSX Edge.
- Transient storage problems that might cause at least one NSX Edge HA VM to become unavailable. For example, an improvement in NSX Edge HA stability and performance is observed when the VMs are moved off overprovisioned storage. In particular, during large overnight backups, large spikes in storage latency can impact NSX Edge HA stability.
- Congestion on the physical or virtual network adapter involved with the exchange of packets.

In addition to environmental issues, a split-brain condition is observed when the HA configuration engine falls into a bad state or when the HA daemon fails.

**Stateful High Availability**

The primary NSX Edge appliance is in the active state and the secondary appliance is in the standby state. NSX Manager replicates the configuration of the primary appliance for the standby appliance or you can manually add two appliances. Create the primary and secondary appliances on separate resource pools and datastores. If you create the primary and secondary appliances on the same datastore, the datastore must be shared across all hosts in the cluster for the HA appliance pair to be deployed on different ESXi hosts. If the datastore is local storage, both virtual machines are deployed on the same host.

All NSX Edge services run on the active appliance. The primary appliance maintains a heartbeat with the standby appliance and sends service updates through an internal interface.

If a heartbeat is not received from the primary appliance within the specified time (default value is 15 seconds), the primary appliance is declared dead. The standby appliance moves to the active state, takes over the interface configuration of the primary appliance, and starts the NSX Edge services that were running on the primary appliance. When the switch over takes place, a system event is displayed in the **System Events** tab of Settings & Reports. Load Balancer and VPN services need to re-establish TCP connection with NSX Edge, so service is disrupted for a short while. Logical switch connections and firewall sessions are synched between the primary and standby appliances however, service is disrupted during the switch over while waiting for the standby appliance to become active and take over.

If the NSX Edge appliance fails and a bad state is reported, HA force syncs the failed appliance to revive it. When revived, it takes on the configuration of the now-active appliance and stays in a standby state. If the NSX Edge appliance is dead, you must delete the appliance and add a new one.
NSX Edge ensures that the two HA NSX Edge virtual machines are not on the same ESXi host even after you use DRS and vMotion (unless you manually vMotion them to the same host). Two virtual machines are deployed on vCenter in the same resource pool and datastore as the appliance you configured. Local link IPs are assigned to HA virtual machines in the NSX Edge HA so that they can communicate. You can specify management IP addresses to override the local links.

If syslog servers are configured, logs in the active appliance are sent to the syslog servers.

**High Availability in a Cross-vCenter NSX Environment**

If you enable high availability on an NSX Edge in a cross-vCenter NSX environment, both the active and standby NSX Edge appliances must reside within the same vCenter Server. If you migrate one of the members of an NSX Edge HA pair to a different vCenter Server system, the two HA appliances will no longer operate as an HA pair, and you might experience traffic disruption.

**vSphere High Availability**

NSX Edge HA is compatible with vSphere HA. If the host on which a NSX Edge instance is running dies, the NSX Edge is restarted on the standby host, ensuring the NSX Edge HA pair is still available to take another failover.

If vSphere HA is not enabled, the active-standby NSX Edge HA pair will survive one fail-over. However, if another fail-over happens before the second HA pair was restored, NSX Edge availability can be compromised.

For more information on vSphere HA, see *vSphere Availability*.

**Change High Availability Configuration**

You can change the HA configuration that you had specified while installing NSX Edge.

**Note** In NSX 6.2.3 and later, enabling high availability (HA) on an existing Edge will fail when sufficient resources cannot be reserved for the second Edge VM appliance. The configuration will roll back to the last known good configuration.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click *Networking & Security* and then click *NSX Edges*.
3. Double-click an NSX Edge.
4. Click the *Manage* tab and then click the *Settings* tab.
5. In the *HA Configuration* panel, click *Change*. 
In the Change HA Configuration dialog box, make changes as explained in the NSX Installation Guide section, Add an Edge Services Gateway.

**Note** If L2 VPN is configured on this Edge appliance before HA is enabled, there must be at least two internal interfaces set up. If there is a single interface configured on this Edge which is already being used by L2 VPN, HA is disabled on the Edge appliance.

Click OK.

**Force Sync NSX Edge with NSX Manager**

You can send a synchronization request from NSX Manager to NSX Edge.

Force sync is used when you need to synchronize the edge configuration as known to the NSX Manager to all of the components.

**Note** For 6.2 and later, force sync avoids data loss for east-west routing traffic, however, north-south routing and bridging may experience an interruption.

Force sync results in the following actions:

- Edge appliances are rebooted, and the latest configuration is applied
- The connection to the host is closed
- If the NSX Manager is primary or stand alone, and the edge is a logical distributed router, then the controller cluster is synced
- A message is sent to all relevant hosts to sync the distributed router instance

**Important** In a cross-vCenter NSX environment, it is required that the NSX Edge instance be force synced first on the primary NSX Manager. When that is complete, force sync the NSX Edge instance on secondary NSX Managers.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Select an NSX Edge instance.
4. Click **Actions ( )** and select **Force Sync**.

**Configure Syslog Servers for NSX Edge**

You can configure one or two remote syslog servers. NSX Edge events and logs related to firewall events that flow from NSX Edge appliances are sent to the syslog servers.

**Procedure**

1. Log in to the vSphere Web Client.
2 Click Networking & Security and then click NSX Edges.

3 Double-click a NSX Edge.

4 Click the Manage tab, and then click the Settings tab.

5 In the Details panel, click Change next to Syslog servers.

6 Type the IP address of both remote syslog servers and select the protocol.

7 Click OK to save the configuration.

**View the Status of an NSX Edge**

The status page displays graphs for the traffic flowing through the interfaces of the selected NSX Edge and connection statistics for the firewall and load balancer services.

**Procedure**

1 Log in to the vSphere Web Client.

2 Click Networking & Security and then click NSX Edges.

3 Double-click an NSX Edge.

4 Click the Monitor tab.

5 Select the period for which you want to view the statistics.

**What to do next**

To view more details about NSX Edge, click Manage and then click Settings.

**Redeploy NSX Edge**

If NSX Edge services do not work as expected after a force sync, you can redeploy the NSX Edge instance.

**Note** Redeploying is a disruptive action. It is recommended that you first apply a force sync and if the issue is not fixed, then redeploy.

Redeploying an NSX Edge instance results in the following actions:

- Edge appliances are deleted and freshly deployed with the latest configuration applied.
- Logical routers are deleted from the controller and then recreated with the latest configuration applied.
- Distributed logical router instances on hosts are deleted and then recreated with the latest configuration applied.
OSPF adjacencies are withdrawn during redeploy if graceful restart is not enabled.

**Important** In a cross-vCenter environment, you must first redeploy the NSX Edge instance on the primary NSX Manager. After that is complete, redeploy the NSX Edge instance on the secondary NSX Managers. It is required that the NSX Edge instances on both the primary and the secondary NSX Managers are redeployed.

**Prerequisites**
- Verify that the hosts have enough resources to deploy additional NSX Edge Services Gateway appliances during the redeploy operation. See the [Chapter 1 System Requirements for NSX](#) for the resources required for each NSX Edge size.
  - For a single NSX Edge instance, there are two NSX Edge appliances of the appropriate size in the poweredOn state during redeploy.
  - For an NSX Edge instance with high availability, both replacement appliances are deployed before replacing the old appliances. This means that there are four NSX Edge appliances of the appropriate size in the poweredOn state during upgrade of a given NSX Edge. Once the NSX Edge instance is redeployed, either of the HA appliances can become active.
- Verify that the host clusters listed in the configured location and live location for the NSX Edge appliance are prepared for NSX and that their messaging infrastructure status is **GREEN**. If the configured location is not available, for example, because the cluster has been removed since the NSX Edge appliance was created, then verify the live location only.
  - Find the ID of the original configured location (configuredResourcePool > id) and the current live location (resourcePoolId) with the GET https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances API request.
  - Find the host preparation status and the messaging infrastructure status for those clusters with the GET https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId} API request, where resourceId is the ID of the configured and live location of the NSX Edge appliances found previously.
  - Look for the status corresponding to the **featureId** of com.vmware.vshield.vsm.nwfabric.hostPrep in the response body. The status must be **GREEN**.

```xml
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
  <featureVersion>6.3.1.5124716</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```
Look for the status corresponding to the featureId of com.vmware.vshield.vsm.messagingInfra in the response body. The status must be GREEN.

```xml
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Select an NSX Edge instance.
4. Click the **Actions ()** icon and select **Redeploy Edge**.

**Results**

The NSX Edge virtual machine is replaced with a new virtual machine and all services are restored. If redeploy does not work, power off the NSX Edge virtual machine and redeploy NSX Edge again.

**Note**  
Redeploy might not work in the following cases.

- Resource pool on which the NSX Edge was installed is no longer in the vCenter inventory or its Managed Object ID (MoId) has changed.
- Datastore on which the NSX Edge was installed is corrupted/unmounted or in-accessible.
- dvportGroups on which the NSX Edge interfaces were connected are no longer in the vCenter inventory or their MoId (identifier in vCenter Server) has changed.

If any of the above is true, you must update the MoId of the resource pool, datastore, or dvPortGroup using a REST API call. See *NSX API Programming Guide*.

If FIPS mode is enabled on NSX Edge and something goes wrong, NSX Manager does not allow you to redeploy the edge. You must resolve infrastructure issues for communication failures instead of redeploying the edge.

**Download Tech Support Logs for NSX Edge**

You can download technical support logs for each NSX Edge instance. If high availability is enabled for the NSX Edge instance, support logs from both NSX Edge virtual machines are downloaded.

**Procedure**

1. Log in to the vSphere Web Client.
2 Click Networking & Security and then click NSX Edges.
3 Select an NSX Edge instance.
4 Click Actions ( ) and select Download Tech Support Logs.
5 After the tech support logs are generated, click Download.

**Add a Static Route**

You can add a static route for a destination subnet or host.

**Procedure**

1 Log in to the vSphere Web Client.
2 Click Networking & Security and then click NSX Edges.
3 Double-click an NSX Edge.
4 Click the Manage tab and then click the Routing tab.
5 Select Static Routes from the left panel.
6 Click the Add ( ) icon.
7 Type the Network in CIDR notation.
8 Type the IP address of the Next Hop.
   The router must be able to directly reach the next hop.
   If ECMP is enabled, you can type multiple next hops.
9 Select the Interface on which you want to add a static route.
10 For MTU, edit the maximum transmission value for the data packets if required.
   The MTU cannot be higher than the MTU set on the NSX Edge interface.
11 If prompted, type the Admin Distance.
   Choose a value between 1 and 255. The admin distance is used to choose which route to use when there are multiple routes for a given network. The lower the admin distance, the higher the preference for the route.

**Table 9-3. Default Admin Distances**

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default admin distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>0</td>
</tr>
<tr>
<td>Static</td>
<td>1</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>OSPF Intra-Area</td>
<td>30</td>
</tr>
</tbody>
</table>
Table 9-3. Default Admin Distances (continued)

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default admin distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Inter-Area</td>
<td>110</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
</tbody>
</table>

An administrative distance of 255 causes the static route to be excluded from the routing table (RIB) and the data plane, so the route is not used.

12  (Optional) Type the **Locale ID**.

By default, routes have the same locale ID as the NSX Manager. Specifying a locale ID here will associate the route with this locale ID. These routes will be sent only to hosts that have a matching locale ID. See Cross-vCenter NSX Topologies for more information.

13  (Optional) Type a **Description** for the static route.

14  Click **OK**.

**Configure OSPF on a Logical (Distributed) Router**

Configuring OSPF on a logical router enables VM connectivity across logical routers and from logical routers to edge services gateways (ESGs).

OSPF routing policies provide a dynamic process of traffic load balancing between routes of equal cost.

An OSPF network is divided into routing areas to optimize traffic flow and limit the size of routing tables. An area is a logical collection of OSPF networks, routers, and links that have the same area identification. Areas are identified by an Area ID.

**Prerequisites**

A Router ID must be configured, as shown in OSPF Configured on the Logical (Distributed) Router.

When you enable a router ID, the field is populated by default with the logical router’s uplink interface.

**Procedure**

1  Log in to the vSphere Web Client.

2  Click **Networking & Security** and then click **NSX Edges**.

3  Double-click a logical router.

4  Click **Routing** and then click **OSPF**.
5  Enable OSPF.
   a  Click **Edit** at the top right corner of the window and click **Enable OSPF**
   b  In **Forwarding Address**, type an IP address that is to be used by the router datapath module in the hosts to forward datapath packets.
   c  In **Protocol Address**, type a unique IP address within the same subnet as the **Forwarding Address**. The protocol address is used by the protocol to form adjacencies with the peers.

6  Configure the OSPF areas.
   a  Optionally, delete the not-so-stubby area (NSSA) 51 that is configured by default.
   b  In **Area Definitions**, click the **Add** icon.
   c  Type an Area ID. NSX Edge supports an area ID in the form of an IP address or decimal number.
   d  In **Type**, select **Normal** or **NSSA**.
      NSSAs prevent the flooding of AS-external link-state advertisements (LSAs) into NSSAs. They rely on default routing to external destinations. Hence, NSSAs must be placed at the edge of an OSPF routing domain. NSSA can import external routes into the OSPF routing domain, thereby providing transit service to small routing domains that are not part of the OSPF routing domain.

7  (Optional) Select the type of **Authentication**. OSPF performs authentication at the area level.
   All routers within the area must have the same authentication and corresponding password configured. For MD5 authentication to work, both the receiving and transmitting routers must have the same MD5 key.
   a  **None**: No authentication is required, which is the default value.
   b  **Password**: In this method of authentication, a password is included in the transmitted packet.
   c  **MD5**: This authentication method uses MD5 (Message Digest type 5) encryption. An MD5 checksum is included in the transmitted packet.
   d  For **Password** or **MD5** type authentication, type the password or MD5 key.

   **Note**
   - You cannot configure MD5 authentication when FIPS mode is enabled.
   - NSX always uses a key ID value of 1. Any non-NSX device peering with an NSX Edge or Logical Distributed Router must be configured to use a key ID of value 1 when MD5 authentication is used, or an OSPF session will not be established.

8  Map interfaces to the areas.
   a  In **Area to Interface Mapping**, click the **Add** icon to map the interface that belongs to the OSPF area.
   b  Select the interface that you want to map and the OSPF area that you want to map it to.
9  (Optional) If needed, edit the default OSPF settings.

In most cases, it is recommended to retain the default OSPF settings. If you do change the settings, make sure that the OSPF peers use the same settings.

a  **Hello Interval** displays the default interval between hello packets that are sent on the interface.

b  **Dead Interval** displays the default interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down.

c  **Priority** displays the default priority of the interface. The interface with the highest priority is the designated router.

d  **Cost** of an interface displays the default overhead required to send packets across that interface. The cost of an interface is inversely proportional to the bandwidth of that interface. The larger the bandwidth, the smaller the cost.

10  Click **Publish Changes**.

**Example: OSPF Configured on the Logical (Distributed) Router**

One simple NSX scenario that uses OSPF is when a logical router (DLR) and an edge services gateway (ESG) are OSPF neighbors, as shown here.
In the following screen, the logical router’s default gateway is the ESG’s internal interface IP address (192.168.10.1).

The router ID is the logical router’s uplink interface---in other words, the IP address that faces the ESG (192.168.10.2).
The logical router configuration uses 192.168.10.2 as its forwarding address. The protocol address can be any IP address that is in the same subnet and is not used anywhere else. In this case, 192.168.10.3 is configured. The area ID configured is 0, and the uplink interface (the interface facing the ESG) is mapped to the area.
What to do next

Make sure the route redistribution and firewall configuration allow the correct routes to be advertised.

In this example, the logical router's connected routes (172.16.10.0/24 and 172.16.20.0/24) are advertised into OSPF.

If you enabled SSH when you created the logical router, you must also configure a firewall filter that allows SSH to the logical router's protocol address. For example:
Configure OSPF on an Edge Services Gateway

Configuring OSPF on an edge services gateway (ESG) enables the ESG to learn and advertise routes. The most common application of OSPF on an ESG is on the link between the ESG and a Logical (Distributed) Router. This allows the ESG to learn about the logical interfaces (LIFS) that are connected to the logical router. This goal can be accomplished with OSPF, IS-IS, BGP or static routing.

OSPF routing policies provide a dynamic process of traffic load balancing between routes of equal cost. An OSPF network is divided into routing areas to optimize traffic flow and limit the size of routing tables. An area is a logical collection of OSPF networks, routers, and links that have the same area identification. Areas are identified by an Area ID.

Prerequisites

A Router ID must be configured, as shown in OSPF Configured on the Edge Services Gateway. When you enable a router ID, the field is populated by default with the ESG's uplink interface IP address.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an ESG.
4. Click Routing and then click OSPF.
5. Enable OSPF.
   a. Click Edit at the top right corner of the window and click Enable OSPF
   b. (Optional) Click Enable Graceful Restart for packet forwarding to be un-interrupted during restart of OSPF services.
   c. (Optional) Click Enable Default Originate to allow the ESG to advertise itself as a default gateway to its peers.
6. Configure the OSPF areas.
   a. (Optional) Delete the not-so-stubby area (NSSA) 51 that is configured by default.
   b. In Area Definitions, click the Add icon.
   c. Type an Area ID. NSX Edge supports an area ID in the form of an IP address or decimal number.
   d. In Type, select Normal or NSSA.

NSSAs prevent the flooding of AS-external link-state advertisements (LSAs) into NSSAs. They rely on default routing to external destinations. Hence, NSSAs must be placed at the edge of an OSPF routing domain. NSSA can import external routes into the OSPF routing domain, thereby providing transit service to small routing domains that are not part of the OSPF routing domain.
7 (Optional) If you select type as NSSA, the NSSA Translator Role field appears. Select the Always check box to translate Type-7 LSAs to Type-5 LSAs. All Type-7 LSAs are translated into Type-5 LSAs by the NSSA.

8 (Optional) Select the type of Authentication. OSPF performs authentication at the area level.

All routers within the area must have the same authentication and corresponding password configured. For MD5 authentication to work, both the receiving and transmitting routers must have the same MD5 key.

a None: No authentication is required, which is the default value.

b Password: In this method of authentication, a password is included in the transmitted packet.

c MD5: This authentication method uses MD5 (Message Digest type 5) encryption. An MD5 checksum is included in the transmitted packet.

d For Password or MD5 type authentication, type the password or MD5 key.

**Note**
- You cannot configure MD5 authentication when FIPS mode is enabled.
- NSX always uses a key ID value of 1. Any non-NSX device peering with an NSX Edge or Logical Distributed Router must be configured to use a key ID of value 1 when MD5 authentication is used, or an OSPF session will not be established.

9 Map interfaces to the areas.

a In Area to Interface Mapping, click the Add icon to map the interface that belongs to the OSPF area.

b Select the interface that you want to map and the OSPF area that you want to map it to.

10 (Optional) Edit the default OSPF settings.

In most cases, it is recommended to retain the default OSPF settings. If you do change the settings, make sure that the OSPF peers use the same settings.

a Hello Interval displays the default interval between hello packets that are sent on the interface.

b Dead Interval displays the default interval during which at least one hello packet must be received from a neighbor before the router declares that neighbor down.

c Priority displays the default priority of the interface. The interface with the highest priority is the designated router.

d Cost of an interface displays the default overhead required to send packets across that interface. The cost of an interface is inversely proportional to the bandwidth of that interface. The larger the bandwidth, the smaller the cost.

11 Click Publish Changes.

12 Make sure that the route redistribution and firewall configuration allow the correct routes to be advertised.
**Example: OSPF Configured on the Edge Services Gateway**

One simple NSX scenario that uses OSPF is when a logical router and an edge services gateway are OSPF neighbors, as shown here.

The ESG can be connected to the outside world through a bridge, a physical router (or as shown here) through an uplink portgroup on a vSphere distributed switch.

**Figure 9-2. NSX Topology**

In the following screen, the ESG's default gateway is the ESG's uplink interface to its external peer.

The router ID is the ESG's uplink interface IP address---in other words, the IP address that faces its external peer.
The area ID configured is 0, and the internal interface (the interface facing the logical router) is mapped to the area.

The connected routes are redistributed into OSPF so that the OSPF neighbor (the logical router) can learn about the ESG's uplink network.
**Note** Additionally, OSPF can be configured between the ESG and its external peer router, but more typically this link uses BGP for route advertisement.

Make sure that the ESG is learning OSPF external routes from the logical router.

To verify connectivity, make sure that an external device in the physical architecture can ping the VMs.

For example:

```
PS C:\Users\Administrator> ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=5ms TTL=61
Reply from 172.16.10.10: bytes=32 time=1ms TTL=61

Ping statistics for 172.16.10.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

```
PS C:\Users\Administrator> ping 172.16.20.10

Pinging 172.16.20.10 with 32 bytes of data:
Reply from 172.16.20.10: bytes=32 time=2ms TTL=61
Reply from 172.16.20.10: bytes=32 time=1ms TTL=61

Ping statistics for 172.16.20.10:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

**Configure BGP**

Border Gateway Protocol (BGP) makes core routing decisions. It includes a table of IP networks or prefixes, which designate network reachability among multiple autonomous systems.
An underlying connection between two BGP speakers is established before any routing information is exchanged. Keepalive messages are sent by the BGP speakers in order to keep this relationship alive. After the connection is established, the BGP speakers exchange routes and synchronize their tables.

Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click **Routing** and then click **BGP**.
5. Click **Edit**.
6. In the Edit BGP Configuration dialog box, click **Enable BGP**.
7. Click **Enable Graceful Restart** for packet forwarding to be un-interrupted during restart of BGP services.
8. Click **Enable Default Originate** to allow NSX Edge to advertise itself as a default gateway to its peers.
9. Type the router ID in **Local AS**. Type the Local AS. This is advertised when BGP peers with routers in other autonomous systems (AS). The path of ASs that a route traverses is used as one metric when selecting the best path to a destination.
10. Click **OK**.
11. In **Neighbors**, click the **Add** icon.
12. Type the IP address of the neighbor.
   
   When you configure BGP peering between an edge services gateway (ESG) and a logical router, use the logical router's protocol IP address as the ESG's BGP neighbor address.
13. (On a logical router only) Type the forwarding address.
   
   The forwarding address is the IP address that you assigned to the distributed logical router's interface facing its BGP neighbor (its uplink interface).
14. (On a logical router only) Type the protocol address.
   
   The protocol address is the IP address that the logical router uses to form a BGP neighbor relationship. It can be any IP address in the same subnet as the forwarding address (as long as it is not used anywhere else). When you configure BGP peering between an edge services gateway (ESG) and a logical router, use the logical router's protocol IP address as the ESG neighbor's IP address.
15. Type the remote AS.
16. Edit the default weight for the neighbor connection if required.
17. **Hold Down Timer** displays interval (180 seconds) after not receiving a keep alive message that the software declares a peer dead. Edit if required.
18 **Keep Alive Timer** displays the default frequency (60 seconds) with which the software sends keepalive messages to its peer. Edit if required.

19 If authentication is required, type the authentication password. Each segment sent on the connection between the neighbors is verified. MD5 authentication must be configured with the same password on both BGP neighbors, otherwise, the connection between them will not be made.

You cannot enter password when FIPS mode is enabled.

20 To specify route filtering from a neighbor, click the **Add** icon in the **BGP Filters** area.

**Caution** A "block all" rule is enforced at the end of the filters.

21 Select the direction to indicate whether you are filtering traffic to or from the neighbor.

22 Select the action to indicate whether you are allowing or denying traffic.

23 Type the network in CIDR format that you want to filter to or from the neighbor.

24 Type the IP prefixes that are to be filtered and click **OK**.

25 Click **Publish Changes**.

**Example: Configure BGP Between an ESG and a Logical Router**

In this topology, the ESG is in AS 64511. The logical router (DLR) is in AS 64512.
The logical router's forwarding address is 192.168.10.2. This is the address configured on the logical router's uplink interface. The logical router's protocol address is 192.168.10.3. This is the address that the ESG will use to form its BGP peering relationship with the logical router.

On the logical router, configure BGP as shown:

On the ESG, configure BGP as shown:

The ESG's neighbor address is 192.168.10.3, which is the logical router's protocol address.

Run the show ip bgp neighbors command on the logical router, and make sure the BGP state is Established.
Run the `show ip bgp neighbors` command on the ESG, and make sure the BGP state is Established.

```
NSX-edge-6-0> show ip bgp neighbors
BGP neighbor is 192.168.10.1, remote AS 64511,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv4 Unicast:advertised and received
    Graceful restart Capability:advertised and received
    Restart remain time: 0
Received 120 messages, Sent 125 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
    Index 1 Identifier 0x9aa20f3c
    Route refresh request:received 0 sent 0
    Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 5
Local host: 192.168.10.3, Local port: 179
Remote host: 192.168.10.1, Remote port: 43846
```

```
NSX-edge-7-0> show ip bgp neighbors
BGP neighbor is 192.168.10.3, remote AS 64512,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv4 Unicast:advertised and received
    Graceful restart Capability:advertised and received
    Restart remain time: 0
Received 121 messages, Sent 120 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
    Index 3 Identifier 0x40212c6c
    Route refresh request:received 0 sent 0
    Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 1
Local host: 192.168.10.1, Local port: 43846
Remote host: 192.168.10.3, Remote port: 179
```

**Configure Route Redistribution**

By default, routers share routes with other routers running the same protocol. In a multi-protocol environment, you must configure route redistribution for cross-protocol route sharing.

You can exclude an interface from route redistribution by adding a deny criterion for its network. In NSX 6.2, the HA (management) interface of a logical (distributed) router is automatically excluded from route redistribution.
Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click **Routing** and then click **Route Redistribution**.
5. Click **Edit** next to **Route Redistribution Status**.
6. Select the protocols for which you enable route redistribution and click **OK**.
7. Add an IP prefix.
   - Entries in the IP Prefix list are processed sequentially.
   - a. Click the **Add** icon in **IP Prefixes**.
   - b. Type a name and IP address of the network.
     - The IP prefix entered will be exactly matched, except if you include less-than-or-equal-to (LE) or greater-than-or-equal-to (GE) modifiers.
   - c. Click **OK**.
8. Specify redistribution criteria for the IP prefix.
   - a. Click the **Add** icon in **Route Redistribution table**.
   - b. In **Learner Protocol**, select the protocol that is to learn routes from other protocols.
   - c. In **Allow Learning from**, select the protocols from which routes should be learned.
   - d. Click **OK**.
9. Click **Publish Changes**.

View the NSX Manager Locale ID

Each NSX Manager has a locale ID. By default, it is set to the NSX Manager UUID. This setting can be overwritten at the universal logical router, cluster, or host level.

Procedure

1. In the vSphere Web Client, navigate to **Networking & Security**, then under **Networking & Security Inventory** click an NSX Manager.
2. Click the **Summary** tab. The **ID** field contains the UUID of the NSX Manager.

Configure Locale ID on a Universal Logical (Distributed) Router

If local egress is enabled when a universal logical router is created, routes are sent to hosts only when the host locale ID matches the locale ID associated with the route. You can change the locale ID on a
router, and this updated locale ID will be associated with all routes on this router (static and dynamic). The routes will be sent to hosts and clusters with matching locale IDs.

See Cross-vCenter NSX Topologies for information on routing configurations for cross-vCenter NSX environments.

Prerequisites
The universal logical (distributed) router must have been created with local egress enabled.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click a universal logical (distributed) router.
4. Click the Routing tab, then click Global Configuration.
5. Click Edit next to Routing Configuration.
6. Type a new Locale ID.

**Important** The locale ID must be in UUID format. For example, XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, where each X is replaced with a base 16 digit (0-F).

Configure Locale ID on a Host or Cluster

If local egress is enabled when a universal logical router is created, routes are sent to hosts only when the host locale ID matches the locale ID associated with the route. You can selectively send routes to hosts by configuring the locale ID on a cluster of hosts, or a host.

Prerequisites
The universal logical (distributed) router that performs routing for the hosts or clusters must have been created with local egress enabled.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Installation.
3. Click the Host Preparation tab
4. Select the NSX Manager that manages the hosts or clusters you need to configure.
5. Select the host or cluster you want to modify, expanding clusters to display hosts if needed.
6. Click the Settings icon (.sulake) and click Change Locale ID.
Type a new locale ID and click **OK**.

**Note**   The locale ID must be in UUID format. For example, XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, where each X is replaced with a base 16 digit (0-F).

**Results**

The universal controller cluster will send only routes matching this new locale ID to the hosts.

**What to do next**

Configure a static route with a locale ID specified.
Logical Firewall

Logical Firewall provides security mechanisms for dynamic virtual data centers, and consists of two components to address different deployment use cases. Distributed Firewall focuses on East-West access controls, and Edge Firewall focuses on the North-South traffic enforcement at the tenant or datacenter perimeter. Together, these components address the end-to-end firewall needs of virtual datacenters. You can choose to deploy either of these technologies independently, or deploy both of them.

This chapter includes the following topics:

- Distributed Firewall
- Edge Firewall
- Working with Firewall Rule Sections
- Working with Firewall Rules
- Firewall Logs

Distributed Firewall

A Distributed Firewall (DFW) runs in the kernel as a VIB package on all the ESXi host clusters that are prepared for NSX. Host preparation automatically activates DFW on the ESXi host clusters.

The fundamental constraints of traditional perimeter-centric security architecture impact both security posture and application scalability in modern data centers. For example, hair-pinning of traffic through physical firewalls at the perimeter of the network creates an extra latency for certain applications.

DFW complements and enhances your physical security by removing unnecessary hair-pinning from the physical firewalls and reduces the amount of traffic on the network. Rejected traffic is blocked before it leaves the ESXi host. There is no need for the traffic to traverse the network, only to be stopped at the perimeter by the physical firewall. Traffic destined to another VM on the same host or another host does not have to traverse through the network up to the physical firewall, and then go back down to the destination VM. Traffic is inspected at the ESXi level and delivered to the destination VM.
NSX DFW is a stateful firewall, meaning it monitors the state of active connections and uses this information to determine which network packets to allow through the firewall. DFW is implemented in the hypervisor and applied to virtual machines on a per-vNIC basis. That is, the firewall rules are enforced at the vNIC of each virtual machine. Inspection of traffic happens at the vNIC of a VM just as the traffic is about to exit the VM and enter the virtual switch (egress). Inspection also happens at the vNIC just as the traffic leaves the switch but before entering the VM (ingress).

NSX Manager virtual appliance, NSX Controller VMs, and NSX Edge Service Gateways are automatically excluded from DFW. If a VM does not require DFW service, you can manually add it to the exclusion list.

As DFW is distributed in the kernel of every ESXi host, firewall capacity scales horizontally when you add hosts to the clusters. Adding more hosts increases the DFW capacity. As your infrastructure expands and you buy more servers to manage your ever-growing number of VMs, the DFW capacity increases.

**DFW Policy Rules**

DFW policy rules are created by using the vSphere Web Client, and the rules are stored in the NSX Manager database. With DFW, you can create Ethernet rules (L2 rules) and General rules (L3 to L7 rules). The rules are published from NSX Manager to ESXi cluster and then from ESXi host down to VM level. All ESXi hosts in the same cluster have the same DFW policy rules.

A distributed firewall instance on an ESXi host contains the following two tables:

- Rules table to store all security policy rules.
- Connection Tracker table to cache flow entries for rules with an “allow” action.

DFW rules are run in a “top-down” order. Traffic that must go through a firewall is first matched against a firewall rules list. Each packet is checked against the top rule in the rule table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced. The last rule in the table is the DFW default rule. Packets not matching any rule above the default rule are enforced by the default rule.
Each VM has its own firewall policy rules and context. During vMotion, when VMs move from one ESXi host to another host, the DFW context (Rules table, Connection Tracker table) moves with the VM. In addition, all active connections remain intact during vMotion. In other words, DFW security policy is independent of VM location.

**Micro-Segmentation Using DFW**

Micro-segmentation makes the data center network more secure by isolating each related group of virtual machines onto a distinct logical network segment. Micro-segmentation allows the administrator to firewall traffic traveling from one logical segment of the data center to another logical segment (east-west traffic). So, firewalling of east-west traffic limits the attacker’s ability to move laterally in the data center.

Micro-segmentation is powered by the Distributed Firewall (DFW) component of NSX. The power of DFW is that the network topology is no longer a barrier to security enforcement. The same degree of traffic access control can be achieved with any type of network topology.

For a detailed example of micro-segmentation use case, see the "Micro-Segmentation with NSX DFW and Implementation" section in the [NSX Network Virtualization Design Guide](https://communities.vmware.com/docs/DOC-27683).

**DFW Policy Rules Based on User Identity**

Distributed firewall can help in creating identity-based rules too. Security administrators can enforce access control based on the user identity and the user's group memberships as defined in the enterprise Active Directory. For example, identity-based distributed firewall rules can be used in the following scenarios:

- Users want to virtual applications using a laptop or mobile device where Active Directory is used for user authentication.
- Users want to access virtual applications using VDI infrastructure where the virtual machines are running Microsoft Windows operating system.

For more information about Active-Directory user-based DFW rules, see Chapter 11 Identity Firewall Overview.

**Session Timers**

Session Timers can be configured for TCP, UDP, and ICMP sessions.

Session Timers define how long a session is maintained on the firewall after inactivity. When the session timeout for the protocol expires, the session closes.

On the firewall, a number of timeouts for TCP, UDP, and ICMP sessions can be specified to apply to a user-defined subset of virtual machines or vNICs. By default, any virtual machines or vNICs not included in the user-defined timer are included in the global session timer. All of these timeouts are global, meaning they apply to all of the sessions of that type on the host.

Default session values can be modified depending on your network needs. Note that setting a value too low could cause frequent timeouts, and setting a value too high could delay failure detection.
Create a Session Timer

Session Timers define how long a session is maintained on the firewall after inactivity in the session. On the firewall, you can define timeouts for TCP, UDP, and ICMP sessions for a set of user defined VMs or vNICS. The default timer is global, meaning that it applies to all virtual machines protected by firewall.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > Firewall.
2. Ensure that you are in the Settings tab. If there is more than one NSX Manager available, select one from the drop-down list.
3. Click the Add ( ) icon.
   The Add a Timeout Configuration dialogue box appears, populated with the default values.
4. Enter a name (required) and a description (optional) for the session timer.
5. Select the protocol. Accept the default values or enter your own values.

<table>
<thead>
<tr>
<th>TCP Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Packet</td>
<td>The timeout value for the connection after the first packet has been sent. The default is 120 seconds.</td>
</tr>
<tr>
<td>Open</td>
<td>The timeout value for the connection after a second packet has been transferred. The default is 30 seconds.</td>
</tr>
<tr>
<td>Established</td>
<td>The timeout value for the connection once the connection has become fully established.</td>
</tr>
<tr>
<td>Closing</td>
<td>The timeout value for the connection after the first FIN has been sent. The default is 120 seconds.</td>
</tr>
<tr>
<td>Fin Wait</td>
<td>The timeout value for the connection after both FINs have been exchanged and the connection is closed. The default is 45 seconds.</td>
</tr>
<tr>
<td>Closed</td>
<td>The timeout value for the connection after one endpoint sends an RST. The default is 20 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UDP Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Packet</td>
<td>The timeout value for the connection after the first packet is sent. This will be the initial timeout for the new UDP flow. The default is 60 seconds.</td>
</tr>
<tr>
<td>Single</td>
<td>The timeout value for the connection if the source host sends more than one packet and the destination host has not sent one back. The default is 30 seconds.</td>
</tr>
<tr>
<td>Multiple</td>
<td>The timeout value for the connection if both hosts have sent packets. The default is 60 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ICMP Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Packet</td>
<td>The timeout value for the connection after the first packet is sent. This is the initial timeout for the new ICMP flow. The default is 20 seconds.</td>
</tr>
<tr>
<td>Error reply</td>
<td>The timeout value for the connection after an ICMP error is returned in response to an ICMP packet. The default is 10 seconds.</td>
</tr>
</tbody>
</table>

6. Select the object type, vNIC or VM.
   The Available Objects list is automatically populated.
7. Select one or more objects and click the arrow to move them to the Selected Objects column.
8. Click OK.
Results
A timer has been created to apply to set of user defined hosts.

Edit a Session Timer
Configure timeout parameters for TCP, UDP and ICMP protocols.

After a session timer has been created it can be changed as needed. The default session timer can also be edited.

Procedure
1. In the vSphere Web Client, navigate to Networking & Security --> Firewall.
2. Ensure that you are in the Settings tab. If there is more than one NSX Manager available, select one from the drop-down list.
3. Select the timer you want to edit. Note that the default timer values can also be edited. Click the pencil icon.

The Edit a Timeout Configuration dialogue box appears, populated with the default values.
4. Enter a name (required) and a description (optional) for the session timer.
5. Select the protocol. Edit any default values that you want to change.

<table>
<thead>
<tr>
<th>TCP Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Packet</td>
<td>The timeout value for the connection after the first packet has been sent. The default is 120 seconds.</td>
</tr>
<tr>
<td>Open</td>
<td>The timeout value for the connection after a second packet has been transferred. The default is 30 seconds.</td>
</tr>
<tr>
<td>Established</td>
<td>The timeout value for the connection once the connection has become fully established.</td>
</tr>
<tr>
<td>Closing</td>
<td>The timeout value for the connection after the first FIN has been sent. The default is 120 seconds.</td>
</tr>
<tr>
<td>Fin Wait</td>
<td>The timeout value for the connection after both FINs have been exchanged and the connection is closed. The default is 45 seconds.</td>
</tr>
<tr>
<td>Closed</td>
<td>The timeout value for the connection after one endpoint sends an RST. The default is 20 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>UDP Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Packet</td>
<td>The timeout value for the connection after the first packet is sent. This will be the initial timeout for the new UDP flow. The default is 60 seconds.</td>
</tr>
<tr>
<td>Single</td>
<td>The timeout value for the connection if the source host sends more than one packet and the destination host has not sent one back. The default is 30 seconds.</td>
</tr>
<tr>
<td>Multiple</td>
<td>The timeout value for the connection if both hosts have sent packets. The default is 60 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ICMP Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Packet</td>
<td>The timeout value for the connection after the first packet is sent. This is the initial timeout for the new ICMP flow. The default is 20 seconds.</td>
</tr>
<tr>
<td>Error reply</td>
<td>The timeout value for the connection after an ICMP error is returned in response to an ICMP packet. The default is 10 seconds.</td>
</tr>
</tbody>
</table>
6 Select the object type, vNIC or VM.
   The Available Objects list is automatically populated.
7 Select one or more objects and click the arrow to move them to the Selected Objects column.
8 Click OK.

IP Discovery for Virtual Machines

VMware Tools runs on a VM and provides several services. One service that is essential to distributed firewall is associating a VM and its vNICs with IP addresses. Before NSX 6.2, if VMware Tools was not installed on a VM, its IP address was not learned. In NSX 6.2 and later, you can configure clusters to detect virtual machine IP addresses with DHCP snooping, ARP snooping, or both. This allows NSX to detect the IP address if VMware Tools is not installed on the virtual machine. If VMware Tools is installed, it can work in conjunction with DHCP and ARP snooping.

VMware recommends that you install VMware Tools on each virtual machine in your environment. In addition to providing vCenter with the IP address of VMs, it provides many other functions:

- allowing copy and paste between VM and host or client desktop
- synchronizing time with the host operating system
- allowing shutdown or restart of the VM from vCenter
- collecting network, disk, and memory usage from the VM and sending it to the host
- determining VM availability by sending and collecting heartbeat

Note that having two vNICs for a VM on the same network is not supported and can lead to unpredictable results around which traffic is blocked or allowed.

For those VMs that do not have VMware Tools installed, NSX will learn the IP address through ARP or DHCP snooping, if ARP and DHCP snooping is enabled on the VM’s cluster.

Change IP Detection Type

The IP address of a virtual machine can be detected by VMware Tools, which are installed on the VM, or by DHCP snooping and ARP snooping, which are enabled on the host cluster. These IP discovery methods can be used together in the same NSX installation.

Procedure

1 In the vSphere Web client, navigate to Networking & Security > Installation > Host Preparation.
2 Click the cluster you want to change, then click Actions (olicit) > Change IP Detection Type.
3 Select the desired detection types and click OK.

What to do next

Configure SpoofGuard.
Configure the default firewall rule.
Exclude Virtual Machines from Firewall Protection

You can exclude a set of virtual machines from NSX distributed firewall protection.

NSX Manager, NSX Controllers, and NSX Edge virtual machines are automatically excluded from NSX distributed firewall protection. In addition, VMware recommends that you place the following service virtual machines in the Exclusion List to allow traffic to flow freely.

- **vCenter Server.** It can be moved into a cluster that is protected by Firewall, but it must already exist in the exclusion list to avoid connectivity issues.

  **Note.** It is important to add the vCenter Server to the exclusion list before changing the "any any" default rule from allow to block. Failure to do so will result in access to the vCenter Server being blocked after creating a Deny All rule (or modifying default rule to block action). If this occurs, roll back the DFW to the default firewall rule set by running the following API command: https://NSX_Manager_IP/api/4.0/firewall/globalroot-config. The request must return a status of 204. This restores the default policy (with a default rule of allow) for DFW and re-enables access to vCenter Server and the vSphere Web Client.

- Partner service virtual machines.
- Virtual machines that require promiscuous mode. If these virtual machines are protected by NSX distributed firewall, their performance may be adversely affected.
- The SQL server that your Windows-based vCenter uses.
- vCenter Web server, if you are running it separately.

**Procedure**

1. In the vSphere Web Client, click **Networking & Security**.
2. In **Networking & Security Inventory**, click **NSX Managers**.
3. In the **Name** column, click an NSX Manager.
4. Click the **Manage** tab and then click the **Exclusion List** tab.
5. Click the **Add** icon.
6. Select the virtual machines that you want to exclude and click **Add**.
7. Click **OK**.

**Results**

If a virtual machine has multiple vNICs, all of them are excluded from protection. If you add vNICs to a virtual machine after it has been added to the Exclusion List, Firewall is automatically deployed on the newly added vNICs. In order to exclude these vNICs from firewall protection, you must remove the virtual machine from the Exclusion List and then add it back to the Exclusion List. An alternative workaround is to power cycle (power off and then power on) the virtual machine, but the first option is less disruptive.
View Firewall CPU and Memory Threshold Events

When a cluster is prepared for network virtualization, the Firewall module is installed on all hosts of that cluster. This module allocates three heaps, a module heap for module parameters; a rule heap for rules, containers, and filters; and a state heap for traffic flows. Heap size allocation is determined by the available host physical memory. Depending on the number of rules, container sets, and the connections, the heap size may grow or shrink over time. The Firewall module running in the hypervisor also uses the host CPUs for packet processing.

Knowing the host resource utilization at any given time can help you in better organizing your server utilization and network designs.

The default CPU threshold is 100, and the memory threshold is 100. You can modify the default threshold values through REST API calls. The Firewall module generates system events when the memory and CPU usage crosses the thresholds. For information on configuring default threshold values, see Working with Memory and CPU Thresholds in the NSX API Guide.

Procedure

1. In the vSphere Web Client, click Networking & Security and then click NSX Managers.

2. In the Name column, click the IP address of the appropriate NSX Manager.

3. Click the Monitor tab and then click System Events.

Distributed Firewall Resource Utilization

Memory is used by distributed firewall internal data structures, and can be configured for CPU, RAM and connections per second.

Each ESXi host is configured with three threshold parameters for DFW resource utilization: CPU, RAM, and connections per second (CPS). An alarm is raised if the respective threshold is crossed 20 consecutive times during a 200-second period. A sample is taken every 10 seconds.

100 percent of CPU corresponds to the total CPU available on the host.

100 percent of RAM corresponds to the memory allocated for distributed firewall ("total max size"), which is dependent on the total amount of RAM installed in the host.

Table 10-1. Total Max Size

<table>
<thead>
<tr>
<th>Physical Memory</th>
<th>Total Max Size (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - 8GB</td>
<td>160</td>
</tr>
<tr>
<td>8GB - 32GB</td>
<td>608</td>
</tr>
<tr>
<td>32GB - 64GB</td>
<td>992</td>
</tr>
<tr>
<td>64GB - 96GB</td>
<td>1920</td>
</tr>
<tr>
<td>96GB - 128GB</td>
<td>2944</td>
</tr>
<tr>
<td>128GB</td>
<td>4222</td>
</tr>
</tbody>
</table>
The memory is used by distributed firewall internal data structures, which include filters, rules, containers, connection states, discovered IPs, and drop flows. These parameters can be manipulated using the following API call:

```xml
https://NSX-MGR-IP/api/4.0/firewall/stats/eventthresholds

Request body:

<eventThresholds>
    <cpu>
        <percentValue>100</percentValue>
    </cpu>
    <memory>
        <percentValue>100</percentValue>
    </memory>
    <connectionsPerSecond>
        <value>100000</value>
    </connectionsPerSecond>
</eventThresholds>
```

**Edge Firewall**

Edge Firewall monitors the North-South traffic to provide perimeter security functionality including firewall, Network Address Translation (NAT), and site-to-site IPSec and SSL VPN functionality. This solution is available in the virtual machine form factor and can be deployed in a High Availability mode.

Firewall support is limited on the Logical Router. Only the rules on management or uplink interfaces work, however, the rules on internal interfaces do not work.

**Note** NSX-V Edge is vulnerable to Syn-Flood attacks, where an attacker fills the firewall state tracking table by flooding SYN packets. This DOS/DDOS attack creates a service disruption to genuine users. Edge must defend from Syn-Flood attacks by implementing logic to detect bogus TCP connections and stop them without consuming Firewall state tracking resources. This feature is disabled by default. To enable this feature in a high risk environment, set the REST API enableSynFloodProtection value to true as part of the Firewall Global Configuration.

For detailed information about the behavior when SynFloodProtection is enabled on an NSX Edge, see the VMware knowledge base article at [https://kb.vmware.com/s/article/54527](https://kb.vmware.com/s/article/54527).

**Working with NSX Edge Firewall Rules**

You can navigate to an NSX Edge to see the firewall rules that apply to it.

Firewall rules applied to a Logical Router only protect control plane traffic to and from the Logical Router control virtual machine. They do not enforce any data plane protection. To protect the data plane traffic, create Logical Firewall rules for East-West protection or rules at the NSX Edge Services Gateway level for North-South protection.
Rules are displayed and enforced in the following order:

1. Predefined distributed firewall rules that are applied to the edge.
   - These rules are defined on the Firewall user interface (Networking & Security > Security > Firewall)
   - These rules are displayed in read-only mode on the NSX Edge Firewall user interface.

2. Internal rules that enable the control traffic to flow for Edge services. For example, internal rules include the following auto-plumbed rules:
   - SSL VPN auto-plumb rule: The Edge Firewall tab displays the sslvpn auto-plumb rule when server settings are configured and SSL VPN service is enabled.
   - DNAT auto-plumb rule: The Edge NAT tab displays the DNAT auto-plumb rule as part of the default SSL VPN configuration.

3. User-defined rules that are added on the NSX Edge Firewall user interface.

4. Default rule.

**Edit the Default NSX Edge Firewall Rule**

Default firewall settings apply to traffic that does not match any of the user-defined firewall rules. The default Edge firewall policy blocks all incoming traffic. You can change the default action and logging settings.

**Procedure**

1. In the vSphere Web Client, navigate to Networking & Security > NSX Edges.
2. Double-click an NSX Edge.
3. Click the Manage tab and then click Firewall.
4. Select the Default Rule, which is the last rule in the firewall table.
5. Point to the Action cell of the new rule and click ⌨️.
   - Click Accept to allow traffic from or to the specified source and destination.
   - Click Log to log all sessions matching this rule.
     - Enabling logging can affect performance.
   - Click OK.
6. Click Publish Changes.

**Add an NSX Edge Firewall Rule**

The Edge Firewall tab displays rules created on the centralized Firewall tab in a read-only mode. Any rules that you add here are not displayed on the centralized Firewall tab.

You can add multiple NSX Edge interfaces and/or IP address groups as the source and destination for firewall rules.
Figure 10-1. Firewall rule for traffic to flow from an NSX Edge interface to an HTTP server

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Type</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>firewall</td>
<td>Internal</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Accept</td>
</tr>
<tr>
<td>2</td>
<td>Traffic to HTTP server</td>
<td>User</td>
<td>any</td>
<td>HTTP Address Group</td>
<td>For HTTP server</td>
<td>Accept</td>
</tr>
<tr>
<td>3</td>
<td>Default Rule</td>
<td>Default</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

Figure 10-2. Firewall rule for traffic to flow from all internal interfaces (subnets on portgroups connected to internal interfaces) of an NSX Edge to an HTTP Server

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Type</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>firewall</td>
<td>Internal</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Accept</td>
</tr>
<tr>
<td>2</td>
<td>Traffic to HTTP server</td>
<td>User</td>
<td>internal</td>
<td>HTTP Address Group</td>
<td>For HTTP server</td>
<td>Accept</td>
</tr>
<tr>
<td>3</td>
<td>Default Rule</td>
<td>Default</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

**Note** If you select internal as the source, the rule is automatically updated when you configure additional internal interfaces.

Figure 10-3. Firewall rule for traffic to allow SSH into a m/c in internal network

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Type</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>firewall</td>
<td>Internal</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Accept</td>
</tr>
<tr>
<td>2</td>
<td>Traffic to internal network</td>
<td>User</td>
<td>any</td>
<td>VM in internal network</td>
<td>Internal VM</td>
<td>Accept</td>
</tr>
<tr>
<td>3</td>
<td>Default Rule</td>
<td>Default</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

**Procedure**

1. In the vSphere Web Client, navigate to Networking & Security > NSX Edges.
2. Double-click an NSX Edge.
3. Click the Manage tab and then click the Firewall tab.
4 Do one of the following.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| To add a rule at a specific place in the firewall table | a Select a rule.  
b In the No. column, click and select **Add Above** or **Add Below**.  
A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule. |
| To add a rule by copying a rule | a Select a rule.  
b Click the Copy icon.  
c Select a rule.  
d In the No. column, click and select **Paste Above** or **Paste Below**. |
| To add a rule anywhere in the firewall table | a Click the Add icon.  
A new any any allow rule is added below the selected rule. If the system defined rule is the only rule in the firewall table, the new rule is added above the default rule. |

The new rule is enabled by default.

5 Point to the **Name** cell of the new rule and click .

6 Type a name for the new rule.

7 Point to the **Source** cell of the new rule and click .

   If you clicked , type an IP address.  
   a Select an object from the drop-down and then make the appropriate selections.  
      If you select **vNIC Group** and then select **vse**, the rule applies to traffic generated by the NSX Edge. If you select **internal** or **external**, the rule applies to traffic coming from any internal or uplink interface of the selected NSX Edge instance. The rule is automatically updated when you configure additional interfaces. Note that firewall rules on internal interfaces do not work for a Logical Router.  
      If you select **IP Sets**, you can create a new IP address group. After you create the new group, it is automatically added to the source column. For information on creating an IP, see Create an IP Address Group.  
   b Click **OK**.
8. Point to the **Destination** cell of the new rule and click ☞ or ☞.
   
a. Select an object from the drop-down and then make the appropriate selections.
   
   If you select **vNIC Group** and then select vse, the rule applies to traffic generated by the NSX Edge. If you select **internal** or **external**, the rule applies to traffic going to any internal or uplink interface of the selected NSX Edge instance. The rule is automatically updated when you configure additional interfaces. Note that firewall rules on internal interfaces do not work for a Logical Router.
   
   If you select **IP Sets**, you can create a new IP address group. After you create the new group, it is automatically added to the source column. For information on creating an IP Set, see [Create an IP Address Group](#).
   
b. Click **OK**.

9. Point to the **Service** cell of the new rule and click ☞ or ☞.
   
   - If you clicked ☞, select a service. To create a new service or service group, click **New**. After you create the new service, it is automatically added to the Service column. For more information on creating a new service, see [Create a Service](#).
   
   - If you clicked ☞, select a protocol. You can specify the source port by clicking the arrow next to **Advanced options**. VMware recommends that you avoid specifying the source port from release 5.1 and later. Instead, you can create a service for a protocol-port combination.
   
   **Note**: NSX Edge only supports services defined with L3 protocols.

10. Point to the **Action** cell of the new rule and click ☞. Make appropriate selections as described in the table below and click **OK**.

<table>
<thead>
<tr>
<th>Action selected</th>
<th>Results in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allows traffic from or to the specified source and destination.</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks traffic from or to the specified source and destination.</td>
</tr>
<tr>
<td>Reject</td>
<td>Sends reject message for unaccepted packets. RST packets are sent for TCP packets. ICMP unreachable (administratively restricted) packets are sent for other packets.</td>
</tr>
<tr>
<td>Log</td>
<td>Logs all sessions matching this rule. Enabling logging can affect performance.</td>
</tr>
<tr>
<td>Do not log</td>
<td>Does not log sessions.</td>
</tr>
<tr>
<td>Comments</td>
<td>Type comments if required.</td>
</tr>
<tr>
<td>Advanced options &gt; Match on Translated</td>
<td>Applies the rule to the translated IP address and services for a NAT rule</td>
</tr>
<tr>
<td>Enable Rule Direction</td>
<td>Indicates whether the rule is incoming or outgoing. VMware does not recommend specifying the direction for firewall rules.</td>
</tr>
</tbody>
</table>

11. Click **Publish Changes** to push the new rule to the NSX Edge instance.
What to do next

- Disable a rule by clicking 🌋 next to the rule number in the No. column.
- Hide generated rules or pre rules (rules added on the centralized Firewall tab) by clicking Hide Generated rules or Hide Pre rules.
- Display additional columns in the rule table by clicking ⬇️ and selecting the appropriate columns.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Tag</td>
<td>Unique system generated ID for each rule</td>
</tr>
<tr>
<td>Log</td>
<td>Traffic for this rule is being logged or not</td>
</tr>
<tr>
<td>Stats</td>
<td>Clicking 📈 shows the traffic affected by this rule (number of sessions, traffic packets, and size)</td>
</tr>
<tr>
<td>Comments</td>
<td>Comments for the rule</td>
</tr>
</tbody>
</table>
- Search for rules by typing text in the Search field.

Edit an NSX Edge Firewall Rule

You can edit only the user-defined edge firewall rules and make limited changes to the system-generated default firewall rule.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > NSX Edges.
2. Double-click an NSX Edge.
3. Click the Manage tab and then click the Firewall tab.
4. Select the rule to edit.

   **Note** You cannot edit the following types of rules on the NSX Edge Firewall user interface:
   - Internal rules (for example, auto-plumbed rules that enable the control traffic to flow for Edge services.)
   - Predefined distributed firewall rules that are applied to the edge. These firewall rules are defined on the Firewall user interface (Networking & Security > Security > Firewall).
5. Make changes and click OK.
6. Click Publish Changes.

Change the Priority of an NSX Edge Firewall Rule

You can change the order of user-defined firewall rules that were added in the Edge Firewall tab to customize traffic flowing through the NSX Edge. For example, suppose you have a rule to allow load balancer traffic. You can now add a rule to deny load balancer traffic from a specific IP address group, and position this rule above the LB allow traffic rule.
Procedure

1. In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.
2. Double-click an NSX Edge.
3. Click the **Manage** tab and then click the **Firewall** tab.
4. Select the rule for which you want to change the priority.
   
   **Note** You cannot change the priority of auto-generated rules or the default rule.

5. Click the **Move Up** (↑) or **Move Down** (↓) icon.
6. Click **OK**.
7. Click **Publish Changes**.

Delete an NSX Edge Firewall Rule

You can delete a user-defined firewall rule that was added in the NSX Edge Firewall tab. Rules added on the centralized Firewall tab cannot be deleted here.

Procedure

1. In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.
2. Double-click an NSX Edge.
3. Click the **Manage** tab and then click the **Firewall** tab.
4. Select the rule to delete.
   
   **Note** You cannot delete an auto-generated rule or the default rule.

5. Click the **Delete** (✗) icon.

Managing NAT Rules

NSX Edge provides network address translation (NAT) service to assign a public address to a computer or group of computers in a private network. Using this technology limits the number of public IP addresses that an organization or company must use, for economy and security purposes. You must configure NAT rules to provide access to services running on privately addressed virtual machines.

The NAT service configuration is separated into source NAT (SNAT) and destination NAT (DNAT) rules.

Add an SNAT Rule

You can create a source NAT (SNAT) rule to change the source IP address from a public to private IP address or the reverse.

Procedure

1. In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.
2. Double-click an NSX Edge.
3. Click the **Manage** tab, and then click the **NAT** tab.

4. Click the **Add** (➕) icon and select **Add SNAT Rule**.

5. Select the interface on which to add the rule.

6. Select the required protocol.

7. Type the original source (public) IP address in one of the following formats.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.0.2.0</td>
</tr>
<tr>
<td>IP address range</td>
<td>192.0.2.0-192.0.2.24</td>
</tr>
<tr>
<td>IP address/subnet</td>
<td>192.0.2.0/24</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

8. Type the original source port or port range.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>80</td>
</tr>
<tr>
<td>Port range</td>
<td>80-85</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

9. Type the destination IP address in one of the following formats.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.0.2.0</td>
</tr>
<tr>
<td>IP address range</td>
<td>192.0.2.0-192.0.2.24</td>
</tr>
<tr>
<td>IP address/subnet</td>
<td>192.0.2.0/24</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

10. Type the destination port or port range.

    | Format     | Example |
    |------------|---------|
    | Port number| 80      |
    | Port range | 80-85   |
    | any        |         |

11. Type the translated source IP address in one of the following formats.

    | Format            | Example            |
    |-------------------|--------------------|
    | IP address        | 192.0.2.0          |
    | IP address range  | 192.0.2.0-192.0.2.24 |
**Add a DNAT Rule**

You can create a destination NAT (DNAT) rule to change the destination IP address from a public to private IP address or the reverse.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click the **Manage** tab, and then click the **NAT** tab.
5. Click the **Add** icon and select **Add DNAT Rule**.
6. Select the interface on which to apply the DNAT rule.
7. Select the required protocol.
8. Type the source IP address in one of the following formats.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.0.2.0</td>
</tr>
<tr>
<td>IP address range</td>
<td>192.0.2.0-192.0.2.24</td>
</tr>
<tr>
<td>IP address/subnet</td>
<td>192.0.2.0/24</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

9. Type the translated port or port range.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>80</td>
</tr>
<tr>
<td>Port range</td>
<td>80-85</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

10. Select **Enabled** to enable the rule.
11. Click **Enable logging** to log the address translation.
12. Click **OK** to add the rule.
13. Click **Publish Changes**.
9  Type the source port or port range.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>80</td>
</tr>
<tr>
<td>Port range</td>
<td>80-85</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

10 Type the original (public) IP address in one of the following formats.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.0.2.0</td>
</tr>
<tr>
<td>IP address range</td>
<td>192.0.2.0 -192.0.2.24</td>
</tr>
<tr>
<td>IP address/subnet</td>
<td>192.0.2.0 /24</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

11 Type the original port or port range.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>80</td>
</tr>
<tr>
<td>Port range</td>
<td>80-85</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

12 Type the translated IP address in one of the following formats.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>192.0.2.0</td>
</tr>
<tr>
<td>IP address range</td>
<td>192.0.2.0 -192.0.2.24</td>
</tr>
<tr>
<td>IP address/subnet</td>
<td>192.0.2.0 /24</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

13 Type the translated port or port range.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number</td>
<td>80</td>
</tr>
<tr>
<td>Port range</td>
<td>80-85</td>
</tr>
<tr>
<td>any</td>
<td></td>
</tr>
</tbody>
</table>

14 Select Enabled to enable the rule.

15 Select Enable logging to log the address translation.

16 Click OK to add the rule.

17 Click Publish Changes.
Working with Firewall Rule Sections

You can add a section to segregate firewall rules. For example, you might want to have the rules for sales and engineering departments in separate sections.

You can create multiple firewall rule sections for L2 and L3 rules.

Cross-vCenter NSX environments can have multiple universal rule sections. Multiple universal sections allow rules to be easily organized per tenant and application. If rules are modified or edited within a universal section, only the universal distributed firewall rules for that section are synced to the secondary NSX Managers. You must manage universal rules on the primary NSX Manager, and you must create the universal section there before you can add universal rules. Universal sections are always listed above local sections on both primary and secondary NSX Managers.

Rules outside the universal sections remain local to the primary or secondary NSX Managers on which they are added.

Add a Firewall Rule Section

You can add a new section in the firewall table to organize your rules or to create a universal section for use in cross-vCenter NSX environments.

Prerequisites

Determine the appropriate NSX Manager on which to make your changes.

- In a standalone or single vCenter NSX environment there is only one NSX Manager so you do not need to select one.
- Universal objects must be managed from the primary NSX Manager.
- Objects local to an NSX Manager must be managed from that NSX Manager.
- In a cross-vCenter NSX environment that does not have Enhanced Linked Mode enabled, you must make configuration changes from the vCenter linked to the NSX Manager that you want to modify.
- In a cross-vCenter NSX environment in Enhanced Linked Mode, you can make configuration changes to any NSX Manager from any linked vCenter. Select the appropriate NSX Manager from the NSX Manager drop-down menu.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > Firewall.
2. If there is more than one NSX Manager available, select one. You must select the Primary NSX Manager to add a universal section.
3. Ensure that you are in the General tab to add a section for L3 rules. Click the Ethernet tab to add a section for L2 rules.
4. Click the Add Section (.btnAddSection) icon.
5 Type a name for the section and specify the position for the new section. Section names must be unique within NSX Manager.
6 (Optional) To create a universal section, select **Mark this section for Universal Synchronization**.
7 Click **OK** and then click **Publish Changes**.

**What to do next**

Add rules to the section. You can edit the name of a section by clicking the **Edit section** icon for that section.

**Merge Firewall Rule Sections**

You can merge sections and consolidate the rules within those sections. Note that you cannot merge a section with the Service Composer or Default sections. In a cross-vCenter NSX environment you cannot merge a section with the universal section.

Merging and consolidating a complex firewall configuration can help with maintenance and readability.

**Procedure**

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.
2 For the section you want to merge, click the **Merge** icon and specify whether you want to merge this section with the section above or below.
   Rules from both sections are merged. The new section keeps the name of the section with which the other section is merged.
3 Click **Publish Changes**.

**Delete a Firewall Rule Section**

You can delete a firewall rule section. All rules in that section are deleted.

You cannot delete a section and add it again at a different place in the firewall table. To do so, you must delete the section and publish the configuration. Then add the deleted section to the firewall table and re-publish the configuration.

**Procedure**

1 In the vSphere Web Client, navigate to **Networking & Security > Firewall**.
2 Ensure that you are in the **General** tab to delete a section for L3 rules. Click the **Ethernet** tab to delete a section for L2 rules.
3 Click the **Delete section** icon for the section you want to delete.
4 Click **OK** and then click **Publish Changes**.

**Results**

The section as well as all rules in that section are deleted.
Working with Firewall Rules

Distributed Firewall rules and Edge Firewall rules can be managed in a centralized manner on the Firewall tab. In a multi-tenant environment, providers can define high-level traffic flow rules on the centralized Firewall user interface.

Each traffic session is checked against the top rule in the Firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced. Rules are displayed in the following order:

1. Rules defined in the Firewall user interface by users have the highest priority, and are enforced in top-to-bottom ordering with a per-virtual NIC level precedence.
2. Auto-plumbed rules (rules that enable control traffic to flow for Edge services).
3. Rules defined in the NSX Edge interface by users.
4. Service Composer rules - a separate section for each policy. You cannot edit these rules in the Firewall table, but you can add rules at the top of a security policy firewall rules section. If you do so, you must re-synchronize the rules in Service Composer. For more information, see Chapter 17 Service Composer.
5. Default Distributed Firewall rules

Note that firewall rules are enforced only on clusters on which you have enabled firewall. For information on preparing clusters, see the NSX Installation Guide.

Edit the Default Distributed Firewall Rule

Default firewall settings apply to traffic that does not match any of the user-defined firewall rules. The Distributed Firewall default rule is displayed on the centralized firewall user interface, and the default rule for each NSX Edge is displayed at the NSX Edge level.

The default Distributed Firewall rule allows all L3 and L2 traffic to pass through all prepared clusters in your infrastructure. The default rule is always at the bottom of the rules table and cannot be deleted or added to. However, you can change the Action element of the rule from Allow to Block or Reject, add comments for the rule, and indicate whether traffic for that rule should be logged.

In a cross-vCenter NSX environment the default rule is not a universal rule. Any changes to the default rule must be made on each NSX Manager.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > Firewall.
2. Expand the Default Section and make the required changes.
   - You can only edit Action and Log, or add comments to the default rule.
Add a Distributed Firewall Rule

You add firewall rules at the NSX Manager scope. Using the Applied To field, you can then narrow down the scope at which you want to apply the rule. You can add multiple objects at the source and destination levels for each rule, which helps reduce the total number of firewall rules to be added.

The following vCenter objects can be specified as the source or destination for a firewall rule:

Table 10-2. Objects supported for firewall rules

<table>
<thead>
<tr>
<th>Source or Destination</th>
<th>Applied To</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster</td>
<td>All clusters on which Distributed Firewall has been installed (in other words, all clusters that have been prepared for network virtualization)</td>
</tr>
<tr>
<td>datacenter</td>
<td>All Edge gateways installed on prepared clusters</td>
</tr>
<tr>
<td>distributed port group</td>
<td>cluster</td>
</tr>
<tr>
<td>IP set</td>
<td>datacenter</td>
</tr>
<tr>
<td>legacy port group</td>
<td>distributed port group</td>
</tr>
<tr>
<td>logical switch</td>
<td>Edge</td>
</tr>
<tr>
<td>resource pool</td>
<td>legacy port group</td>
</tr>
<tr>
<td>security group</td>
<td>logical switch</td>
</tr>
<tr>
<td>vApp</td>
<td>security group</td>
</tr>
<tr>
<td>virtual machine</td>
<td>virtual machine</td>
</tr>
<tr>
<td>vNIC</td>
<td>vNIC</td>
</tr>
<tr>
<td>IP address (IPv4 or IPv6)</td>
<td></td>
</tr>
</tbody>
</table>

Prerequisites

Make sure the state of NSX distributed firewall is not in backward compatibility mode. To check the current state, use the REST API call GET https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state. If the current state is backward compatibility mode, you can change the state to forward by using the REST API call PUT https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state. Do not try to publish a distributed firewall rule while the distributed firewall is in backward compatibility mode.

If you are adding universal firewall rules, see Add a Universal Firewall Rule

If you are adding an identity-based firewall rule, ensure that:

- One or more domains have been registered with NSX Manager. NSX Manager gets group and user information as well as the relationship between them from each domain that it is registered with. See Register a Windows Domain with NSX Manager.

- A security group based on Active Directory objects has been created which can be used as the source or destination of the rule. See Create a Security Group.

If you are adding a rule based on a VMware vCenter object, ensure that VMware Tools is installed on the virtual machines. See NSX Installation Guide.

VMs that are migrated from 6.1.5 to 6.2.3 do not have support for TFTP ALG. To enable TFTP ALG support after migrating, add and remove the VM from the exclusion list or restart the VM. A new 6.2.3 filter is created, with support for TFTP ALG.
**Procedure**

1. In the vSphere Web Client, navigate to **Networking & Security > Firewall**.

2. Ensure that you are in the **General** tab to add an L3 rule. Click the **Ethernet** tab to add an L2 rule.

3. In the section in which you add a rule, click **Add rule** (➕) icon.

4. Click **Publish Changes**.

   A new any allow rule is added at the top of the section. If the system-defined rule is the only rule in the section, the new rule is added above the default rule.

   If you want to add a rule at a specific place in a section, select a rule. In the No. column, click ✂️ and select **Add Above** or **Add Below**.

5. Point to the **Name** cell of the new rule and click ✎.

6. Type a name for the new rule.

7. Point to the **Source** cell of the new rule. Additional icons are displayed as described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Click</strong></td>
<td>To specify source as an IP address.</td>
</tr>
<tr>
<td>a</td>
<td>Select the IP address format.</td>
</tr>
<tr>
<td></td>
<td>Firewall supports both IPv4 and IPv6 formats.</td>
</tr>
<tr>
<td>b</td>
<td>Type the IP address.</td>
</tr>
<tr>
<td></td>
<td>You can enter multiple IP addresses in a comma-separated list. The list can contain up to 255 characters.</td>
</tr>
</tbody>
</table>

| **Click** | To specify source as an object other than a specific IP address.           |
| a        | In **View**, select a container from which the communication originated.   |
|          | Objects for the selected container are displayed.                          |
| b        | Select one or more objects and click ✎.                                   |
|          | You can create a new security group or IPSet. Once you create the new object, it is added to the source column by default. For information on creating a new security group or IPSet, see [Chapter 21 Network and Security Objects](#). |
| c        | To exclude a source from the rule, click **Advanced options**.             |
| d        | Select **Negate Source** to exclude this source from the rule.             |
|          | If **Negate Source** is selected, the rule is applied to traffic coming from all sources except for the source you specified in the previous step. |
|          | If **Negate Source** is not selected, the rule applies to traffic coming from the source you specified in the previous step. |
| e        | Click **OK**.                                                              |
8 Point to the **Destination** cell of the new rule. Additional icons are displayed as described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click <strong>IP</strong></td>
<td>To specify destination as an IP address.</td>
</tr>
<tr>
<td>a</td>
<td>Select the IP address format.</td>
</tr>
<tr>
<td></td>
<td>Firewall supports both IPv4 and IPv6 formats.</td>
</tr>
<tr>
<td>b</td>
<td>Type the IP address.</td>
</tr>
<tr>
<td></td>
<td>You can enter multiple IP addresses in a comma-separated list. The list can contain up to 255 characters.</td>
</tr>
<tr>
<td>Click <strong>pencil</strong></td>
<td>To specify destination as an object other than a specific IP address.</td>
</tr>
<tr>
<td>a</td>
<td>In <strong>View</strong>, select a container which the communication is targeting.</td>
</tr>
<tr>
<td></td>
<td>Objects for the selected container are displayed.</td>
</tr>
<tr>
<td>b</td>
<td>Select one or more objects and click <img src="image" alt="pencil" /> .</td>
</tr>
<tr>
<td></td>
<td>You can create a new security group or IPSet. Once you create the new object, it is added to the Destination column by default. For information on creating a new security group or IPSet, see <a href="https://example.com">Chapter 21 Network and Security Objects</a>.</td>
</tr>
<tr>
<td>c</td>
<td>To exclude a destination port, click <strong>Advanced options</strong>.</td>
</tr>
<tr>
<td>d</td>
<td>Select <strong>Negate Destination</strong> to exclude this destination from the rule.</td>
</tr>
<tr>
<td></td>
<td><strong>Negate Destination</strong> is selected, the rule is applied to traffic going to all destinations except for the destination you specified in the previous step.</td>
</tr>
<tr>
<td></td>
<td><strong>Negate Destination</strong> is not selected, the rule applies to traffic going to the destination you specified in the previous step.</td>
</tr>
<tr>
<td>e</td>
<td>Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
9 Point to the **Service** cell of the new rule. Additional icons are displayed as described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Click  | To specify service as a port protocol combination.  
  a Select the service protocol.  
  Distributed Firewall supports ALG (Application Level Gateway) for the following protocols: TFTP, FTP, ORACLE TNS, MS-RPC, and SUN-RPC.  
  Edge supports ALG for FTP, TFTP, and SNMP_BASIC.  
  Note: VMs that are migrated from 6.1.5 to 6.2.3 do not have support for TFTP ALG. To enable TFTP ALG support after migrating, add and remove the VM from the exclusion list or restart the VM. A new 6.2.3 filter is created, with support for TFTP ALG.  
  b Type the port number and click **OK**. |
|        | Click **铅笔** | To select a pre-defined service/service group or define a new one.  
  a Select one or more objects and click **铅笔**.  
  You can create a new service or service group. Once you create the new object, it is added to the Selected Objects column by default.  
  b Click **OK**. |

In order to protect your network from ACK or SYN floods, you can set Service to TCP-all_ports or UDP-all_ports and set Action to Block for the default rule. For information on modifying the default rule, see *Edit the Default Distributed Firewall Rule*.

10 Point to the **Action** cell of the new rule and click **铅笔**. Make appropriate selections as described in the table below and click **OK**.

<table>
<thead>
<tr>
<th>Action</th>
<th>Results in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allows traffic from or to the specified source(s), destination(s), and service(s).</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks traffic from or to the specified source(s), destination(s), and service(s).</td>
</tr>
</tbody>
</table>
| Reject | Sends reject message for unaccepted packets.  
  RST packets are sent for TCP connections.  
  ICMP messages with administratively prohibited code are sent for UDP, ICMP, and other IP connections. |
| Log    | Logs all sessions matching this rule. Enabling logging can affect performance. |
| Do not log | Does not log sessions. |
11 In Applied To, define the scope at which this rule is applicable. Make appropriate selections as described in the table below and click OK.

<table>
<thead>
<tr>
<th>To apply a rule to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>All prepared clusters in your environment</td>
<td>Select <strong>Apply this rule on all clusters on which Distributed Firewall is enabled</strong>. After you click OK, the Applied To column for this rule displays Distributed Firewall.</td>
</tr>
<tr>
<td>All NSX Edge gateways in your environment</td>
<td>Select <strong>Apply this rule on all Edge gateways</strong>. After you click OK, the Applied To column for this rule displays All Edges. If both the above options are selected, the Applied To column displays Any.</td>
</tr>
</tbody>
</table>
| One or more cluster, datacenter, distributed virtual port group, NSX Edge, network, virtual machine, vNIC, or logical switch | 1 In **Container type**, select the appropriate object.  
2 In the Available list, select one or more objects and click |
Force Sync Distributed Firewall Rules

If you can't publish firewall rules to hosts, perform a force sync.

Force sync is used when you need to synchronize the firewall rules on an individual host with the NSX Manager.

Procedure

1. In the vSphere Web client, navigate to Networking & Security > Installation > Host Preparation.
2. Select the cluster you want to force sync, then click Actions (≡) > Force Sync Services.
3. Select Firewall from the services to force sync. Click OK.

The Firewall status changes to Busy while syncing.

Add a Universal Firewall Rule

In a cross-vCenter NSX environment, universal rules refer to the distributed firewall rules defined on the primary NSX Manager in the universal rules section. These rules are replicated on all secondary NSX Managers in your environment, which enables you to maintain a consistent firewall policy across vCenter boundaries. Edge firewall rules are not supported for vMotion between multiple vCenter Servers.

The primary NSX Manager can contain multiple universal sections for universal L2 rules and multiple universal sections for universal L3 rules. Universal sections are on top of all local and service composer sections. Universal sections and universal rules can be viewed but not edited on the secondary NSX Managers. The placement of the universal section with respect to the local section does not interfere with rule precedence.

Table 10-3. Objects supported for universal firewall rules

<table>
<thead>
<tr>
<th>Source and Destination</th>
<th>Applied To</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>universal MAC set</td>
<td>universal security group, which can contain a universal security tag, IP set, MAC set, or universal security group</td>
<td>pre-created universal services and service groups</td>
</tr>
<tr>
<td>universal IP set</td>
<td>universal logical switch</td>
<td>user created universal services and services groups</td>
</tr>
<tr>
<td>universal security group, which can contain a universal security tag, an IP set, MAC set, or universal security group</td>
<td>Distributed Firewall - applies rules on all clusters on which Distributed Firewall is installed</td>
<td></td>
</tr>
</tbody>
</table>

Note that other vCenter objects are not supported for universal rules.

Prerequisites

You must create a universal rule section before you can create universal rules. See Add a Firewall Rule Section.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > Firewall.
2 In NSX Manager, ensure that the primary NSX Manager is selected. Universal rules can only be added on the primary NSX Manager.

3 Ensure that you are in the **General** tab to add an L3 universal rule. Click the **Ethernet** tab to add an L2 universal rule.

4 In the universal section click the **Add rule** (.addButton ) icon and then click **Publish Changes**. A new any any allow rule is added at the top of the universal section.

5 Point to the **Name** cell of the new rule and click ✍️. Type a name for the rule.

6 Point to the **Source** cell of the new rule. Additional icons are displayed as described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click IP</td>
<td>To specify source as an IP address.</td>
</tr>
<tr>
<td></td>
<td>a Select the IP address format.</td>
</tr>
<tr>
<td></td>
<td>Firewall supports both IPv4 and IPv6 formats.</td>
</tr>
<tr>
<td></td>
<td>b Type the IP address.</td>
</tr>
<tr>
<td>Click ✍️</td>
<td>To specify a universal IPSet, MACSet, or security group as the source.</td>
</tr>
<tr>
<td></td>
<td>a In <strong>Object Type</strong>, select a container from which the communication originated.</td>
</tr>
<tr>
<td></td>
<td>Objects for the selected container are displayed.</td>
</tr>
<tr>
<td></td>
<td>b Select one or more objects and click ✍️</td>
</tr>
<tr>
<td></td>
<td>You can create a new security group or IPSet. Once you create the new object,</td>
</tr>
<tr>
<td></td>
<td>it is added to the source column by default. For information on creating a new</td>
</tr>
<tr>
<td></td>
<td>security group or IPSet, see Chapter 21 Network and Security Objects.</td>
</tr>
<tr>
<td></td>
<td>c To exclude a source from the rule, click <strong>Advanced options</strong>.</td>
</tr>
<tr>
<td></td>
<td>d Select <strong>Negate Source</strong> to exclude this source from the rule.</td>
</tr>
<tr>
<td></td>
<td>If <strong>Negate Source</strong> is selected, the rule is applied to traffic coming from all</td>
</tr>
<tr>
<td></td>
<td>sources except for the source you specified in the previous step.</td>
</tr>
<tr>
<td></td>
<td>If <strong>Negate Source</strong> is not selected, the rule applies to traffic coming from the source you specified in the previous step.</td>
</tr>
<tr>
<td></td>
<td>e Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
7  Point to the **Destination** cell of the new rule. Additional icons are displayed as described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Click **IP** | To specify destination as an IP address.  
  a  Select the IP address format.  
  b  Type the IP address. |

Click  

To specify a universal IPSet, MACSet, or security group as the destination.  

a  In **Object Type**, select a container which the communication is targeting.  

Objects for the selected container are displayed.  

b  Select one or more objects and click .  

You can create a new security group or IPSet. Once you create the new object, it is added to the Destination column by default. For information on creating a new security group or IPSet, see [Chapter 21 Network and Security Objects](#).  

c  To exclude a destination from the rule, click **Advanced options**.  

d  Select **Negate Destination** to exclude this destination from the rule.  

If **Negate Destination** is selected, the rule is applied to traffic going to all destinations except for the destination you specified in the previous step.  

If **Negate Destination** is not selected, the rule applies to traffic going to the destination you specified in the previous step.  

e  Click **OK**.

8  Point to the **Service** cell of the new rule. Additional icons are displayed as described in the table below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Click **File Path** | To specify a service as a port protocol combination.  
  a  Select the service protocol.  
  b  Type the port number and click **OK**. |

Click  

To select a pre-defined universal service/universal service group or define a new one.  

a  Select one or more objects and click .  

You can create a new service or service group. Once you create the new object, it is added to the Selected Objects column by default.  

b  Click **OK**.

To protect your network from ACK or SYN floods, set Service to TCP-all_ports or UDP-all_ports and set Action to Block for the default rule. For information on modifying the default rule, see [Edit the Default Distributed Firewall Rule](#).
9 Point to the **Action** cell of the new rule and click 🍉. Make appropriate selections as described in the table below and click **OK**.

<table>
<thead>
<tr>
<th>Action</th>
<th>Results in</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Allow</em></td>
<td>Allows traffic from or to the specified source(s), destination(s), and service(s).</td>
</tr>
<tr>
<td><em>Block</em></td>
<td>Blocks traffic from or to the specified source(s), destination(s), and service(s).</td>
</tr>
<tr>
<td><em>Reject</em></td>
<td>Sends reject message for unaccepted packets. RST packets are sent for TCP connections. ICMP messages with administratively prohibited code are sent for UDP, ICMP, and other IP connections.</td>
</tr>
<tr>
<td><em>Log</em></td>
<td>Logs all sessions matching this rule. Enabling logging can affect performance.</td>
</tr>
<tr>
<td><em>Do not log</em></td>
<td>Does not log sessions.</td>
</tr>
</tbody>
</table>

10 In **Applied To** cell, either accept the default setting, Distributed Firewall, to apply the rule on all clusters with Distributed Firewall enabled, or click the edit icon 🍉 to select the universal logical switches on which the rule is to be applied to.

11 Click **Publish Changes**.

**Results**

The universal rule is replicated on all secondary NSX Managers. The Rule ID stays the same across all NSX instances. To display the Rule ID, click 📊 and then click Rule ID.

Universal rules can be edited on the primary NSX Manager and are read only on secondary NSX Managers.

Firewall rules with Universal Section Layer3 and Default Section Layer3:

![Firewall Rules Diagram](image)

**What to do next**

- Disable a rule by clicking 🗑️ in the No. column, or enable a rule by clicking ✅.
Display additional columns in the rule table by clicking and selecting the appropriate columns.

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Information Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule ID</td>
<td>Unique system generated ID for each rule</td>
</tr>
<tr>
<td>Log</td>
<td>Traffic for this rule is being logged or not</td>
</tr>
<tr>
<td>Stats</td>
<td>Clicking shows the traffic related to this rule (traffic packets and size)</td>
</tr>
<tr>
<td>Comments</td>
<td>Comments for the rule</td>
</tr>
</tbody>
</table>

Search for rules by typing text in the Search field.

Move a rule up or down in the Firewall table.

Firewall Rules with a Custom Layer 3 Protocol

Firewall rules can be created using a custom protocol number that is not listed in the protocols drop-down menu.

A firewall rule with a custom protocol number can be created on the distributed firewall or the NSX Edge firewall.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > Firewall.
2. Ensure that you are in the General tab to add an L3 rule. Click the Add rule icon.
3. Click Publish Changes.
   A new any allow rule is added at the top of the section. If the system-defined rule is the only rule in the section, the new rule is added above the default rule.
   If you want to add a rule at a specific place in a section, select a rule. In the No. column, click and select Add Above or Add Below.
4. Point to the Name cell of the new rule and click.
5. Type a name for the new rule.
6. Specify the Source of the new rule. See Add a Distributed Firewall Rule for icon details.
7. Specify the Destination of the new rule. See Add a Distributed Firewall Rule for details.
8. Point to the Service cell of the new rule. Click the Add Service icon
9. Click New Service on the bottom left of the Specify Service window.
10. Enter the Name of the new protocol (such as OSPF).
11. From the Protocols drop-down menu select L3_OTHERS.
    A Protocol Number field appears under the drop-down menu.
12. Enter the Protocol Number (such as 89 for OSPF).
13 Click OK.

Results

A firewall rule has been created using a custom protocol number.

Save an Unpublished Configuration

You can add a rule and save the configuration without publishing it. You can then load and publish the saved configuration at a later time.

Procedure

1 Add a firewall rule. See Add a Distributed Firewall Rule.
2 Click Save Changes.
3 Type a name and description for the configuration and click OK.
4 Click Preserve Configuration to preserve this change.
   NSX can save up to 100 configurations. After this limit is exceeded, saved configurations marked with Preserve Configuration are preserved, while older non-preserved configurations are deleted to make room for preserved configurations.
5 Do one of the following:
   - Click Revert Changes to go back to the configuration that existed before you added the rule.
     When you want to publish the rule you just added, click the Load Configuration icon, select the rule that you saved in step 3 and click OK.
   - Click Update Changes to continue adding rules.

Load a Saved Firewall Configuration

You can load an autosaved or imported firewall configuration. If your current configuration contains rules managed by Service Composer, these are overridden after the import.

Procedure

1 In the vSphere Web Client, navigate to Networking & Security > Firewall.
2 Ensure that you are in the General tab to load an L3 firewall configuration. Click the Ethernet tab to load an L2 firewall configuration.
3 Click the Load configuration (_attach) icon.
4 Select the configuration to load and click OK.
   The current configuration is replaced by the selected configuration.

What to do next

If Service Composer rules in your configuration were overridden by the loaded configuration, click Actions > Synchronize Firewall Rules in the Security Policies tab within Service Composer.
Filter Firewall Rules

You can use a wide number of criteria to filter your ruleset, which allows for easy rule modification. Rules can be filtered by source or destination virtual machines or IP address, rule action, logging, rule name, comments, and rule ID.

Procedure

1. In the Firewall tab, click the Apply Filter (✓) icon.
2. Type or select the filtering criteria as appropriate.
3. Click Apply.

Rules matching your filtering criteria are displayed.

What to do next

To display all rules again, click the Remove applied filter (✗) icon.

Change the Order of a Firewall Rule

Firewall rules are applied in the order in which they exist in the rule table.

Rules are displayed (and enforced) in the following order:

1. User-defined pre rules have the highest priority and are enforced in top-to-bottom ordering with a per-virtual NIC level precedence.
3. Local rules defined at an NSX Edge level.
4. Service Composer rules - a separate section for each policy. You cannot edit these rules in the Firewall table, but you can add rules at the top of a security policy firewall rules section. If you do so, you must re-synchronize the rules in Service Composer. For more information, see Chapter 17 Service Composer.
5. Default Distributed Firewall rule

You can move a custom rule up or down in the table. The default rule is always at the bottom of the table and cannot be moved.

Procedure

1. In the Firewall tab, select the rule that you want to move.
2. Click the Move rule up (⬆) or Move rule down (⬇) icon.
3. Click Publish Changes.

Delete a Firewall Rule

You can delete firewall rules that you created. You cannot delete the default rule or rules managed by Service Composer.
Procedure

1. In the **Firewall** tab, select a rule.
2. Click **Delete selected rule** icon above the Firewall table.
3. Click **Publish Changes**.

**Firewall Logs**

Firewall generates and stores log files, such as audit log, rules message log, and system event log. You must configure a syslog server for each cluster that has enabled the firewall. The syslog server is specified in the `Syslog.global.logHost` attribute.

Firewall generates logs as described in the following table.

**Table 10-4. Firewall Logs**

<table>
<thead>
<tr>
<th>Log Type</th>
<th>Description</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules message logs</td>
<td>Include all access decisions such as permitted or denied traffic for each rule if logging was enabled for that rule. Contains DFW packet logs for the rules where logging has been enabled.</td>
<td><code>/var/log/dfwpktlogs.log</code></td>
</tr>
<tr>
<td>Audit logs</td>
<td>Include administration logs and Distributed Firewall configuration changes.</td>
<td><code>/home/secureall/secureall/logs/vsm.log</code></td>
</tr>
<tr>
<td>System event logs</td>
<td>Include Distributed Firewall configuration applied, filter created, deleted, or failed, and virtual machines added to security groups, and so on.</td>
<td><code>/home/secureall/secureall/logs/vsm.log</code></td>
</tr>
<tr>
<td>Data Plane/VMKernel logs</td>
<td>Capture activities related to a firewall kernel module (VSIP). It include log entries for messages generated by the system.</td>
<td><code>/var/log/vmkernel.log</code></td>
</tr>
<tr>
<td>Message Bus Client/ VSFWD logs</td>
<td>Capture activities of a firewall agent.</td>
<td><code>/var/log/vsfwd.log</code></td>
</tr>
</tbody>
</table>

**Note**  The `vsm.log` file can be accessed by running the `show log manager` command from the NSX Manager Command Line Interface (CLI) and performing `grep` for the keyword `vsm.log`. This file is accessible only to the user or user group having the `root` privilege.

**Rules Message Logs**

Rules message logs include all access decisions such as permitted or denied traffic for each rule, if logging was enabled for that rule. These logs are stored on each host in `/var/log/dfwpktlogs.log`.

Here are examples of firewall log message:

```bash
# more /var/log/dfwpktlogs.log
```
More examples:

2017-10-19T22:38:05.586Z INET match PASS domain-c8/1006 OUT 84 ICMP 172.18.8.121->172.18.8.119 RULE_TAG
2017-10-19T22:38:08.723Z INET match PASS domain-c8/1006 OUT 60 TCP 172.18.8.121/36485->172.18.8.119/22 S RULE_TAG
2017-10-19T22:38:18.785Z INET TERM domain-c8/1006 OUT ICMP 8 0 172.18.8.121->172.18.8.119 2/2 168/168 RULE_TAG

In the following example:

- 1002 is the distributed firewall rule ID.
- domain-c7 is cluster ID in the vCenter managed object browser (MOB).
- 192.168.110.10/138 is the source IP address.
- 192.168.110.255/138 is the destination IP address.
- RULE_TAG is an example of the text that you add in the Tag text box while adding or editing the firewall rule.

The following example shows the results of a ping 192.168.110.10 to 172.16.10.12.

# tail -f /var/log/dfwpktlogs.log | grep 192.168.110.10

2015-03-10T03:20:31.274Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
2015-03-10T03:20:35.794Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12

The following tables explain the text boxes in the firewall log message.

**Table 10-5. Components of a log File Entry**

<table>
<thead>
<tr>
<th>Component</th>
<th>Value in example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>2017-04-11T21:09:59</td>
</tr>
<tr>
<td>Firewall-specific portion</td>
<td>877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST</td>
</tr>
</tbody>
</table>

**Table 10-6. Firewall-Specific Portion of log File Entry**

<table>
<thead>
<tr>
<th>Entity</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter hash</td>
<td>A number that can be used to get the filter name and other information.</td>
</tr>
<tr>
<td>AF Value</td>
<td>INET, INET6</td>
</tr>
</tbody>
</table>
### Table 10-6. Firewall-Specific Portion of log File Entry (continued)

<table>
<thead>
<tr>
<th>Entity</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason</td>
<td>match: Packet matches a rule.</td>
</tr>
<tr>
<td></td>
<td>bad-offset: Datapath internal error while getting packet.</td>
</tr>
<tr>
<td></td>
<td>fragment: The non-first fragments after they are assembled to the first fragment.</td>
</tr>
<tr>
<td></td>
<td>short: Packet too short (for example, not even complete to include an IP header, or</td>
</tr>
<tr>
<td></td>
<td>TCP/UDP header).</td>
</tr>
<tr>
<td></td>
<td>normalize: Malformed packets that do not have a correct header or a payload.</td>
</tr>
<tr>
<td></td>
<td>memory: Datapath out of memory.</td>
</tr>
<tr>
<td></td>
<td>bad-timestamp: Incorrect TCP timestamp.</td>
</tr>
<tr>
<td></td>
<td>proto-cksum: Bad protocol checksum.</td>
</tr>
<tr>
<td></td>
<td>state-mismatch: TCP packets that do not pass the TCP state machine check.</td>
</tr>
<tr>
<td></td>
<td>state-insert: Duplicate connection is found.</td>
</tr>
<tr>
<td></td>
<td>state-limit: Reached the maximum number of states that a datapath can track.</td>
</tr>
<tr>
<td></td>
<td>SpoofGuard: Packet dropped by SpoofGuard.</td>
</tr>
<tr>
<td></td>
<td>TERM: A connection is terminated.</td>
</tr>
<tr>
<td>Action</td>
<td>PASS: Accept the packet.</td>
</tr>
<tr>
<td></td>
<td>DROP: Drop the packet.</td>
</tr>
<tr>
<td></td>
<td>NAT: SNAT rule.</td>
</tr>
<tr>
<td></td>
<td>NONAT: Matched the SNAT rule, but can not translate the address.</td>
</tr>
<tr>
<td></td>
<td>RDR: DNAT rule.</td>
</tr>
<tr>
<td></td>
<td>NORDR: Matched the DNAT rule, but cannot translate the address.</td>
</tr>
<tr>
<td></td>
<td>PUNT: Send the packet to a service VM running on the same hypervisor of the current VM.</td>
</tr>
<tr>
<td></td>
<td>REDIRECT: Send the packet to network service running out of the hypervisor of the current VM.</td>
</tr>
<tr>
<td></td>
<td>COPY: Accept the packet and make a copy to a service VM running on the same hypervisor of the current VM.</td>
</tr>
<tr>
<td></td>
<td>REJECT: Reject the packet.</td>
</tr>
<tr>
<td>Rule set and rule ID</td>
<td>rule set / rule ID</td>
</tr>
<tr>
<td>Direction</td>
<td>IN, OUT</td>
</tr>
<tr>
<td>Packet length</td>
<td>length</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP, UDP, ICMP, or PROTO (protocol number)</td>
</tr>
<tr>
<td></td>
<td>For TCP connections, the actual reason that a connection is terminated is indicated after the keyword TCP.</td>
</tr>
<tr>
<td></td>
<td>If TERM is the reason for a TCP session, then an additional explanation appears in the PROTO row. The possible reasons for terminating a TCP connection include: RST (TCP RST packet), FIN (TCP FIN packet), and TIMEOUT (idle for too long)</td>
</tr>
<tr>
<td></td>
<td>In the example above, it is RST. So it means that there is a RST packet in the connection that must be reset.</td>
</tr>
<tr>
<td></td>
<td>For non-TCP connections (UDP, ICMP or other protocols), the reason for terminating a connection is only TIMEOUT.</td>
</tr>
<tr>
<td>Source IP address and port</td>
<td>IP address / port</td>
</tr>
<tr>
<td>Destination IP address and port</td>
<td>IP address / port</td>
</tr>
<tr>
<td>TCP flags</td>
<td>S (SYN), SA (SYN-ACK), A (ACK), P (PUSH), U (URGENT), F (FIN), R (RESET)</td>
</tr>
</tbody>
</table>
Table 10-6. Firewall-Specific Portion of log File Entry (continued)

<table>
<thead>
<tr>
<th>Entity</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of packets</td>
<td>Number of packets.</td>
</tr>
<tr>
<td></td>
<td>22/14 - in packets / out packets</td>
</tr>
<tr>
<td>Number of bytes</td>
<td>Number of bytes.</td>
</tr>
<tr>
<td></td>
<td>7684/1070 - in bytes/ out bytes</td>
</tr>
</tbody>
</table>

To enable a rules message, log in to vSphere Web Client:

1. Enable the **Log** column on the **Networking & Security > Firewall** page.

![Log column](image1.png)

2. Enable logging for a rule by hovering over the Log table cell and clicking the pencil icon.

![Pencil icon](image2.png)

**Note** If you want customized text to be displayed in the firewall log message, you can enable the **Tag** column and add the required text by clicking the pencil icon.

### Audit and System Event Logs

Audit logs include administration logs and Distributed Firewall configuration changes. These are stored in `/home/secureall/secureall/logs/vsm.log`.

System event logs include Distributed Firewall configuration applied, filter created, deleted, or failed, and virtual machines added to security groups, and so on. These logs are stored in `/home/secureall/secureall/logs/vsm.log`.

To view the audit and system event logs on the UI, navigate to **Networking & Security > Installation > Management** and double-click the IP address of the NSX Manager. Then click the **Monitor** tab.
For more information, see *NSX Logging and System Events*. 
Identity Firewall Overview

Identity Firewall features allows an NSX administrator to create Active Directory user-based DFW rules.

A high level overview of the IDFW configuration workflow begins with preparing the infrastructure. This includes the administrator installing the host preparation components on each protected cluster, and setting up Active Directory synchronization so that NSX can consume AD users and groups. Next, IDFW must know which desktop an Active Directory user logs onto in order to apply DFW rules. There are two methods IDFW uses for logon detection: Guest Introspection and/or the Active Directory Event Log Scraper. Guest Introspection is deployed on ESXi clusters where IDFW virtual machines are running. When network events are generated by a user, a guest agent installed on the VM forwards the information through the Guest Introspection framework to the NSX Manager. The second option is the Active Directory event log scraper. Configure the Active Directory event log scraper in the NSX Manager to point at an instance of your Active Directory domain controller. NSX Manager will then pull events from the AD security event log. You can use both in your environment, or one or the other. Note that if both the AD event log scraper and Guest Introspection are used, the two are mutually exclusive: if one of these stops working, the other does not begin to work as a back up.

Once the infrastructure is prepared, the administrator creates NSX Security Groups and adds the newly available AD Groups (referred to as Directory Groups). The administrator can then create Security Policies with associated firewall rules and apply those policies to the newly created Security Groups.

Now, when a user logs into a desktop, the system will detect that event along with the IP address which is being used, look up the firewall policy that is associated with that user, and push those rules down. This works for both physical and virtual desktops. For physical desktops AD event log scraper is also required to detect that a user is logged into a physical desktop.

OS Supported With IDFW

AD Supported Servers
- Windows 2012
- Windows 2008
- Windows 2008 R2

Guest OS Supported
- Windows 2012
This chapter includes the following topics:

- **Identity Firewall Workflow**

## Identity Firewall Workflow

Identity Firewall (IDFW) allows user-based distributed firewall rules (DFW).

User-based distributed firewall rules are determined by membership in an Active Directory (AD) group membership. IDFW monitors where Active Directory users are logged into, and maps the login to an IP Address, which is used by DFW to apply firewall rules. Identity Firewall requires either guest introspection framework or active directory event log scraping.

### Procedure

1. Configure Active Directory Sync in NSX, see *Synchronize a Windows Domain with Active Directory*. This is required to use Active Directory groups in Service Composer.

2. Prepare the ESXi cluster for DFW. See Prepare the Host Cluster for NSX in the *NSX Installation Guide*.

3. Configure Identity Firewall logon detection options. One or both of these options must be configured.

   **Note** If you have a multi-domain AD architecture, and the log scraper isn't accessible due to security constraints, use Guest Introspection to generate login and logout events.

   - Configure Active Directory event log access. See *Register a Windows Domain with NSX Manager*.

   - Windows Guest OS with guest agent installed. This comes with a complete installation of VMware Tools™. Deploy Guest Introspection service to protected clusters. See *Install Guest Introspection on Host Clusters*. For troubleshooting Guest Introspection, see *Collecting Guest Introspection Troubleshooting Data*. 


You can register one or more Windows domains with an NSX Manager and associated vCenter server. NSX Manager gets group and user information as well as the relationship between them from each domain that it is registered with. NSX Manager also retrieves Active Directory (AD) credentials.

Once NSX Manager retrieves AD credentials, you can create security groups based on user identity, create identity-based firewall rules, and run Activity Monitoring reports.

This chapter includes the following topics:

- Register a Windows Domain with NSX Manager
- Synchronize a Windows Domain with Active Directory
- Edit a Windows Domain
- Enable Security Read-Only Log Access on Windows 2008
- Verifying Directory Privileges

### Register a Windows Domain with NSX Manager

**Prerequisites**

The domain account must have AD read permission for all objects in the domain tree. The event log reader account must have read permissions for security event logs.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Managers**.
3. Click an NSX Manager in the **Name** column and then click the **Manage** tab.
4. Click the **Domain** tab and then click the **Add domain** ( ![Add domain](https://docs.vmware.com/en/) ) icon.
5. In the **Add Domain** dialog box, enter the fully qualified domain name (for example, `eng.vmware.com`) and netBIOS name for the domain.

To retrieve the netBIOS name for your domain, type `nbtstat -n` in a command window on a Windows workstation that is part of a domain or on a domain controller. In the NetBIOS Local Name Table, the entry with a `<00>` prefix and type Group is the netBIOS name.
6 When adding a child domain, select Auto Merge.

7 During sync, to filter out users that no longer have active accounts click Ignore disabled users.

8 Click Next.

9 In the LDAP Options page, specify the domain controller that the domain is to be synchronized with and select the protocol.

10 Edit the port number if required.

11 Enter the user credentials for the domain account. This user must be able to access the directory tree structure.

12 Click Next.

13 (Optional) In the Security Event Log Access page, select either CIFS or WMI for the connection method to access security event logs on the specified AD server. Change the port number if required. This step is used by Active Directory Event Log Scraper. See Identity Firewall Workflow.

---

**Note** The event log reader looks for events with the following IDs from the AD Security event log: Windows 2008/2012: 4624, Windows 2003: 540. The event log server has a limit of 128 MB. When this limit is reached you may see Event ID 1104 in the Security Log Reader. See https://technet.microsoft.com/en-us/library/dd315518 for more information.

14 Select Use Domain Credentials to use the LDAP server user credentials. To specify an alternate domain account for log access, un-select Use Domain Credentials and specify the user name and password.

The specified account must be able to read the security event logs on the Domain Controller specified in step 10.

15 Click Next.

16 In the Ready to Complete page, review the settings you entered.

17 Click Finish.

---

**Attention**

- If an error message appears stating that the Adding Domain operation failed for the entity because of a domain conflict, select Auto Merge. The domains will be created and the settings displayed below the domain list.

---

**Results**

The domain is created and its settings are displayed below the domain list.

---

**What to do next**

Verify that login events on the event log server are enabled.
You can add, edit, delete, enable, or disable LDAP servers by selecting the **LDAP Servers** tab in the panel below the domain list. You can perform the same tasks for event log servers by selecting the **Event Log Servers** tab in the panel below the domain list. Adding more than one Windows server (Domain Controllers, Exchange servers, or File Servers) as an event log server improves the user identity association.

**Note** If using IDFW, only AD Servers are supported.

### Synchronize a Windows Domain with Active Directory

By default, all registered domains are automatically synchronized with Active Directory every 3 hours. You can also synchronize on demand.

Through the vSphere Web Client UI, you can perform a force sync for Active Directory domains. A periodic sync is automatically performed once a week, and a delta sync every 3 hours. It is not possible to selectively sync sub-trees through the UI.

With NSX 6.4 and later it is possible to selectively sync active directory sub trees using API calls. The root domain cannot have any parent-child relationships and must have a valid directory distinguished name.

- `/api/1.0/directory/updateDomain` has an option to specify the folder under root domain. And there is an option to perform a force update `private boolean forceUpdate`.
- `/api/directory/verifyRootDN`. Verify that the list of rootDN doesn't have any parent-child relationships. Verify each rootDN is a valid active directory distinguished name.

**Procedure**

1. In the vSphere Web Client, navigate to **Networking & Security > System > Users and Domains**.
2. Click the **Domains** tab, and then select the domain to be synchronized.

   **Important** Any changes made in Active Directory will NOT be seen on NSX Manager until a delta or full sync has been performed.

3. Select one of the following:

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>📐</td>
<td>Perform a delta synchronization, where local AD objects that changed since the last synchronization event are updated</td>
</tr>
<tr>
<td>📐</td>
<td>Perform a full synchronization, where the local state of all AD objects is updated</td>
</tr>
</tbody>
</table>

### Edit a Windows Domain

You can edit the name, netBIOS name, primary LDAP server, and account credentials of a domain.
Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Managers**.
3. Click an NSX Manager in the **Name** column and then click the **Manage** tab.
4. Select a domain and then click the **Edit domain** icon.
5. Make the desired changes and click **Finish**.

Enable Security Read-Only Log Access on Windows 2008

Read-only security log access is used by event log scraper in IDFW.

After creating a new user account, you must enable read-only security log access on a Windows 2008 server-based domain section to grant the user read-only access.

**Note** You must perform these steps on one Domain Controller of the domain, tree, or forest.

Procedure

1. Navigate to **Start > Administrative Tools > Active Directory Users and Computers**.
2. In the navigation tree, expand the node that corresponds to the domain for which you want to enable security log access.
3. Under the node that you just expanded, select the **Builtin** node.
4. Double-click on **Event Log Readers** in the list of groups.
5. Select the **Members** tab in the Event Log Readers Properties dialog box.
6. Click the **Add...** button.
   
   The Select Users, Contacts, Computers, or Groups dialog appears.
7. If you previously created a group for the “AD Reader” user, select that group in the Select Users, Contacts, Computers, or Groups dialog. If you created only the user and you did not create a group, select that user in the Select Users, Contacts, Computers, or Groups dialog.
8. Click **OK** to close the Select Users, Contacts, Computers, or Groups dialog
9. Click **OK** to close the Event Log Readers Properties dialog.

What to do next

After you have enabled security log access, verify directory privileges by following the steps in **Verifying Directory Privileges**.
Verifying Directory Privileges

Verify that the user account has the required privileges to read the security logs.

After you have created a new account and enabled security log access, you must verify the ability to read the security logs.

Prerequisites


Procedure

1. From any workstation that is part of the domain, log on to the domain as an administrator.
3. Select Connect to Another Computer... from the Action menu. The Select Computer dialog box appears. (Note that you must do this even if you are already logged on to the machine for which you plan to view the event log.)
4. Select the Another computer radio button, if it is not already selected.
5. In the text field adjacent to the Another computer radio button, enter the name of the Domain Controller. Alternatively, click the Browse... button and then select the Domain Controller.
6. Select the Connect as another user check box.
7. Click the Set User... button. The Event Viewer dialog box appears.
8. In the User name field, enter the user name for the user that you created.
9. In the Password field, enter the password for the user that you created.
10. Click OK
11. Click OK again.
12. Expand the Windows Logs node in the navigation tree.
13. Under the Windows Logs node, select the Security node. If you can see log events then the account has the required privileges.
Using SpoofGuard

After synchronizing with the vCenter Server, NSX Manager collects the IP addresses of all vCenter guest virtual machines from VMware Tools on each virtual machine. If a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

You create a SpoofGuard policy for specific networks that allows you to authorize the IP addresses reported by VMware Tools and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vSphere SDK. Operating separately from Firewall rules, you can use SpoofGuard to block traffic determined to be spoofed.

SpoofGuard supports both IPv4 and IPv6 addresses. The SpoofGuard policy supports multiple IP addresses assigned to a vNIC when using VMwareTools and DHCP snooping. If ARP snooping is enabled, multiple IP addresses are not supported. The SpoofGuard policy monitors and manages the IP addresses reported by your virtual machines in one of the following modes.

**Automatically Trust IP Assignments On Their First Use**

This mode allows all traffic from your virtual machines to pass while building a table of vNIC-to-IP address assignments. You can review this table at your convenience and make IP address changes. This mode automatically approves all IPv4 and IPv6 addresses that are first seen on a vNIC.

**Manually Inspect and Approve All IP Assignments Before Use**

This mode blocks all traffic until you approve each vNIC-to-IP address assignment. In this mode, multiple IPv4 address can be approved.

**Note** SpoofGuard inherently allows DHCP requests regardless of enabled mode. However, if in manual inspection mode, traffic does not pass until the DHCP-assigned IP address has been approved.

SpoofGuard includes a system-generated default policy that applies to port groups and logical networks not covered by the other SpoofGuard policies. A newly added network is automatically added to the default policy until you add the network to an existing policy or create a new policy for it.

SpoofGuard is one of the ways that an NSX distributed firewall policy can determine the IP address of a virtual machine. For information, see IP Discovery for Virtual Machines.

This chapter includes the following topics:

- Create a SpoofGuard Policy
Create a SpoofGuard Policy

You can create a SpoofGuard policy to specify the operation mode for specific networks. The system-generated (default) policy applies to port groups and logical switches not covered by existing SpoofGuard policies.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > SpoofGuard.
2. Click the Add icon.
3. Type a name for the policy.
4. Select Enabled or Disabled to indicate whether the policy is enabled.
5. For Operation Mode, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically Trust IP Assignments on Their First Use</td>
<td>Select this option to trust all IP assignments upon initial registration with the NSX Manager.</td>
</tr>
<tr>
<td>Manually Inspect and Approve All IP Assignments Before Use</td>
<td>Select this option to require manual approval of all IP addresses. All traffic to and from unapproved IP addresses is blocked.</td>
</tr>
</tbody>
</table>

6. Click Allow local address as valid address in this namespace to allow local IP addresses in your setup.

When you power on a virtual machine and it is unable to connect to the DHCP server, a local IP address is assigned to it. This local IP address is considered valid only if the SpoofGuard mode is set to Allow local address as valid address in this namespace. Otherwise, the local IP address is ignored.

7. Click Next.

8. To specify the scope for the policy, click Add and select the networks, distributed port groups, or logical switches that this policy should apply to.

A port group or logical switch can belong to only one SpoofGuard policy.

9. Click OK and then click Finish.

What to do next

You can edit a policy by clicking the Edit icon and delete a policy by clicking the Delete icon.
Approve IP Addresses

If you set SpoofGuard to require manual approval of all IP address assignments, you must approve IP address assignments to allow traffic from those virtual machines to pass.

Procedure

1. In the **SpoofGuard** tab, select a policy.

   Policy details are displayed below the policy table.

2. In **View**, click one of the option links.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Virtual NICs</td>
<td>List of all validated IP addresses</td>
</tr>
<tr>
<td>Active Virtual NICs Since Last Published</td>
<td>List of IP addresses that have been validated since the policy was last updated</td>
</tr>
<tr>
<td>Virtual NICs IP Required Approval</td>
<td>IP address changes that require approval before traffic can flow to or from these virtual machines</td>
</tr>
<tr>
<td>Virtual NICs with Duplicate IP</td>
<td>IP addresses that are duplicates of an existing assigned IP address within the selected datacenter</td>
</tr>
<tr>
<td>Inactive Virtual NICs</td>
<td>List of IP addresses where the current IP address does not match the published IP address</td>
</tr>
<tr>
<td>Unpublished Virtual NICs IP</td>
<td>List of virtual machines for which you have edited the IP address assignment but have not yet published</td>
</tr>
</tbody>
</table>

3. Do one of the following.

   - To approve a single IP address, click **Approve** next to the IP address.
   - To approve multiple IP addresses, select the appropriate vNICs and then click **Approve Detected IP(s)**.

Edit an IP Address

You can edit the IP address assigned to a MAC address to correct the assigned IP address.

**Note**  SpoofGuard accepts a unique IP address from virtual machines. However, you can assign an IP address only once. An approved IP address is unique across NSX. Duplicate approved IP addresses are not allowed.

Procedure

1. In the **SpoofGuard** tab, select a policy.

   Policy details are displayed below the policy table.
2 In **View**, click one of the option links.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Virtual NICs</td>
<td>List of all validated IP addresses</td>
</tr>
<tr>
<td>Active Virtual NICs Since Last Published</td>
<td>List of IP addresses that have been validated since the policy was last updated</td>
</tr>
<tr>
<td>Virtual NICs IP Required Approval</td>
<td>IP address changes that require approval before traffic can flow to or from these virtual machines</td>
</tr>
<tr>
<td>Virtual NICs with Duplicate IP</td>
<td>IP addresses that are duplicates of an existing assigned IP address within the selected datacenter</td>
</tr>
<tr>
<td>Inactive Virtual NICs</td>
<td>List of IP addresses where the current IP address does not match the published IP address</td>
</tr>
<tr>
<td>Unpublished Virtual NICs IP</td>
<td>List of virtual machines for which you have edited the IP address assignment but have not yet published</td>
</tr>
</tbody>
</table>

3 For the appropriate vNIC, click the **Edit** icon and make appropriate changes.

4 Click **OK**.

### Clear an IP Address

You clear an approved IP address assignment from a SpoofGuard policy.

**Procedure**

1 In the **SpoofGuard** tab, select a policy.

   Policy details are displayed below the policy table.

2 In **View**, click one of the option links.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Virtual NICs</td>
<td>List of all validated IP addresses</td>
</tr>
<tr>
<td>Active Virtual NICs Since Last Published</td>
<td>List of IP addresses that have been validated since the policy was last updated</td>
</tr>
<tr>
<td>Virtual NICs IP Required Approval</td>
<td>IP address changes that require approval before traffic can flow to or from these virtual machines</td>
</tr>
<tr>
<td>Virtual NICs with Duplicate IP</td>
<td>IP addresses that are duplicates of an existing assigned IP address within the selected datacenter</td>
</tr>
<tr>
<td>Inactive Virtual NICs</td>
<td>List of IP addresses where the current IP address does not match the published IP address</td>
</tr>
<tr>
<td>Unpublished Virtual NICs IP</td>
<td>List of virtual machines for which you have edited the IP address assignment but have not yet published</td>
</tr>
</tbody>
</table>

3 Do one of the following.
   - To clear a single IP address, click **Clear** next to the IP address.
To clear multiple IP addresses, select the appropriate vNICs and then click **Clear Approved IP(s).**
Virtual Private Networks (VPN)

NSX Edge supports several types of VPNs. SSL VPN-Plus allows remote users to access private corporate applications. IPSec VPN offers site-to-site connectivity between an NSX Edge instance and remote sites. L2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries.

You must have a working NSX Edge instance before you can use VPN. For information on setting up NSX Edge, see NSX Edge Configuration.

This chapter includes the following topics:

- SSL VPN-Plus Overview
- IPSec VPN Overview
- L2 VPN Overview

SSL VPN-Plus Overview

With SSL VPN-Plus, remote users can connect securely to private networks behind a NSX Edge gateway. Remote users can access servers and applications in the private networks.
The following client operating systems are supported.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>8, 10 (including Windows 10 Secure Boot option enabled)</td>
</tr>
<tr>
<td>Mac OS Sierra</td>
<td>10.12.6</td>
</tr>
<tr>
<td>Mac OS High Sierra</td>
<td>10.13.4</td>
</tr>
<tr>
<td>Linux Fedora</td>
<td>26, 28</td>
</tr>
<tr>
<td>Linux CentOS</td>
<td>6.0, 7.5</td>
</tr>
<tr>
<td>Linux Ubuntu</td>
<td>18.04</td>
</tr>
</tbody>
</table>

**Important**

- SSL VPN-Plus Client is not supported on computers that use ARM-based processors.
- In SSL VPN-Plus Client on Windows, the "auto-reconnect" feature does not work as expected when the Npcap loopback adapter is "enabled". This loopback adapter interferes with the function of the Npcap driver on a Windows computer. Make sure that the latest version of the Npcap driver (0.9983 or later) is installed on your Windows computer. This version of the driver does not require the loopback adapter for packet captures.
- Linux TCL, TK, and Network Security Services (NSS) libraries are required for the UI to work.
Configure Network Access SSL VPN-Plus

In network access mode, a remote user can access private networks after downloading and installing an SSL client.

Prerequisites

The SSL VPN gateway requires port 443 to be accessible from external networks and the SSL VPN client requires the NSX Edge gateway IP and port 443 to be reachable from client system.

Add SSL VPN-Plus Server Settings

You must add SSL VPN server settings to enable SSL on a NSX Edge interface.

Procedure

1. In the SSL VPN-Plus tab, Server Settings from the left panel.
2. Click Change.
3. Select the IPv4 or IPv6 address.
4. Edit the port number if required. This port number is required to configure the installation package.
5. Select one or more encryption methods or ciphers.

   Note   If any of the following GCM ciphers is configured on the SSL VPN server, backward compatibility issue can occur in some browsers:
   - AES128-GCM-SHA256
   - ECDHE-RSA-AES128-GCM-SHA256
   - ECDHE-RSA-AES256-GCM-SHA38

6. (Optional) From the Server Certificates table, use the default server certificate, or deselect the Use Default Certificate check box and click the server certificate that you want to add.

   Restriction
   - SSL VPN-Plus service supports only RSA certificates.
   - SSL VPN-Plus service supports server certificate that is signed only by the Root CA. Server certificate signed by an Intermediate CA is not supported.

7. Click OK.

Add an IP Pool

The remote user is assigned a virtual IP address from the IP pool that you add.

Procedure

1. In the SSL Vpn-Plus tab, select IP Pools from the left panel.
2. Click the Add (➕) icon.
3 Type the begin and end IP address for the IP pool.

4 Type the netmask of the IP pool.

5 Type the IP address which is to add the routing interface in the NSX Edge gateway.

6 (Optional) Type a description for the IP pool.

7 Select whether to enable or disable the IP pool.

8 (Optional) In the Advanced panel, type the DNS name.

9 (Optional) Type the secondary DNS name.

10 Type the connection-specific DNS suffix for domain based host name resolution.

11 Type the WINS server address.

12 Click OK.

**Add a Private Network**

Add the network that you want the remote user to be able to access.

**Procedure**

1 In the SSL VPN-Plus tab, select Private Networks from the left panel.

2 Click the Add (＋) icon

3 Type the private network IP address.

4 Type the netmask of the private network.

5 (Optional) Type a description for the network.

6 Specify whether you want to send private network and internet traffic over the SSL VPN-Plus enabled NSX Edge or directly to the private server by bypassing the NSX Edge.

7 If you selected Send traffic over the tunnel, select Enable TCP Optimization to optimize the internet speed.

   Conventional full-access SSL VPNs tunnel sends TCP/IP data in a second TCP/IP stack for encryption over the internet. This results in application layer data being encapsulated twice in two separate TCP streams. When packet loss occurs (which happens even under optimal internet conditions), a performance degradation effect called TCP-over-TCP meltdown occurs. In essence, two TCP instruments are correcting a single packet of IP data, undermining network throughput and causing connection timeouts. TCP Optimization eliminates this TCP-over-TCP problem, ensuring optimal performance.

8 When optimization is enabled, specify the port numbers for which traffic should be optimized.

   Traffic for remaining ports for that specific network will not be optimized.

---

**Note** Traffic for all ports are optimized, if port numbers are not specified.
When TCP traffic is optimized, the TCP connection is opened by the SSL VPN server on behalf of the client. Because the TCP connection is opened by the SSLVPN server, the first automatically generated rule is applied, which allows all connections opened from the Edge to get passed. Traffic that is not optimized will be evaluated by the regular Edge firewall rules. The default rule is allow any any.

9 Specify whether you want to enable or disable the private network.

10 Click OK.

What to do next

Add a corresponding firewall rule to allow the private network traffic.

Add Authentication

In addition to local user authentication, you can add an external authentication server (AD, LDAP, Radius, or RSA) which is bound to the SSL gateway. All users with accounts on the bound authentication server will be authenticated.

The maximum time to authenticate over SSL VPN is 3 minutes. This is because non-authentication timeout is 3 minutes and is not a configurable property. So in scenarios where AD authentication timeout is set to more than 3 minutes or there are multiple authentication servers in chain authorization and the time taken for user authentication is more than 3 minutes, you will not be authenticated.

Procedure

1 In the SSL VPN-Plus tab, select Authentication from the left panel.

2 Click the Add (+) icon.

3 Select the type of authentication server.

4 Depending on the type of authentication server you selected, complete the following fields.

- **AD authentication server**

<table>
<thead>
<tr>
<th>Table 14-1. AD Authentication Server Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>Enable SSL</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Timeout</td>
</tr>
<tr>
<td>Status</td>
</tr>
</tbody>
</table>
Table 14-1. AD Authentication Server Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search base</td>
<td>Part of the external directory tree to search. The search base may be something equivalent to the organizational unit (OU), domain controller (DC), or domain name (AD) of external directory. Examples:</td>
</tr>
</tbody>
</table>
|                      |   - OU=Users,DC=aslan,DC=local  
|                      |   - OU=VPN,DC=aslan,DC=local  |
| Bind DN              | User on the external AD server permitted to search the AD directory within the defined search base. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user. Example: CN=ldap.edge,OU=users,OU=Datacenter Users,DC=aslan,DC=local |
| Bind Password        | Password to authenticate the AD user.                                                                                                                                                                           |
| Retype Bind Password | Retype the password.                                                                                                                                                                                          |
| Login Attribute Name | Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is **sAMAccountName**.                                                           |
| Search Filter        | Filter values by which the search is to be limited. The search filter format is `attribute operator value`. If you need to limit the search base to a specific group in the AD and not allow searching across the entire OU, then  |
|                      |   - Do not put group name inside the search base, only put OU and DC.  
|                      |   - Do not put both **objectClass** and **memberOf** inside the same search filter string. Example of correct format for the search filter: **memberOf=CN=VPN_Users,OU=Users,DC=aslan,DC=local** |
| Use this server for secondary authentication | If selected, this AD server is used as the second level of authentication.                                                                                                                                    |
| Terminate Session if authentication fails | When selected, the session is ended if authentication fails.                                                                                                                                                 |

- LDAP authentication server

Table 14-2. LDAP Authentication Server Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSL</td>
<td>Enabling SSL establishes an encrypted link between a web server and a browser.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the external server.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays default port name. Edit if required.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Period in seconds within which the AD server must respond.</td>
</tr>
<tr>
<td>Status</td>
<td>Select <strong>Enabled</strong> or <strong>Disabled</strong> to indicate whether the server is enabled.</td>
</tr>
<tr>
<td>Search base</td>
<td>Part of the external directory tree to search. The search base may be something equivalent to the organization, group, or domain name (AD) of external directory.</td>
</tr>
</tbody>
</table>
Table 14-2. LDAP Authentication Server Options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind DN</td>
<td>User on the external server permitted to search the AD directory within the defined search base. Most of the time, the bind DN is permitted to search the entire directory. The role of the bind DN is to query the directory using the query filter and search base for the DN (distinguished name) for authenticating AD users. When the DN is returned, the DN and password are used to authenticate the AD user.</td>
</tr>
<tr>
<td>Bind Password</td>
<td>Password to authenticate the AD user.</td>
</tr>
<tr>
<td>Retype Bind Password</td>
<td>Retype the password.</td>
</tr>
<tr>
<td>Login Attribute Name</td>
<td>Name against which the user ID entered by the remote user is matched with. For Active Directory, the login attribute name is <code>sAMAccountName</code>.</td>
</tr>
<tr>
<td>Search Filter</td>
<td>Filter values by which the search is to be limited. The search filter format is <code>attribute operator value</code>.</td>
</tr>
<tr>
<td>Use this server for secondary authentication</td>
<td>If selected, this server is used as the second level of authentication.</td>
</tr>
<tr>
<td>Terminate Session if authentication fails</td>
<td>When selected, the session is ended if authentication fails.</td>
</tr>
</tbody>
</table>

- **RADIUS authentication server**

RADIUS authentication is disabled in FIPS mode.

Table 14-3. RADIUS authentication server options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the external server.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays default port name. Edit if required.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Period in seconds within which the AD server must respond.</td>
</tr>
<tr>
<td>Status</td>
<td>Select <strong>Enabled</strong> or <strong>Disabled</strong> to indicate whether the server is enabled.</td>
</tr>
<tr>
<td>Secret</td>
<td>Shared secret specified while adding the authentication agent in the RSA security console.</td>
</tr>
<tr>
<td>Retype secret</td>
<td>Retype the shared secret.</td>
</tr>
<tr>
<td>NAS IP Address</td>
<td>IP address to be configured and used as RADIUS attribute 4, NAS-IP-Address, without changing the source IP address in the IP header of the RADIUS packets.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Number of times the RADIUS server is to be contacted if it does not respond before the authentication fails.</td>
</tr>
<tr>
<td>Use this server for secondary authentication</td>
<td>If selected, this server is used as the second level of authentication.</td>
</tr>
<tr>
<td>Terminate Session if authentication fails</td>
<td>When selected, the session is ended if authentication fails.</td>
</tr>
</tbody>
</table>

- **RSA-ACE authentication server**
RSA authentication is disabled in FIPS mode.

### Table 14-4. RSA-ACE authentication server options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout</td>
<td>Period in seconds within which the AD server must respond.</td>
</tr>
<tr>
<td>Configuration File</td>
<td>Click <strong>Browse</strong> to select the <code>sdconf.rec</code> file that you downloaded from the RSA Authentication Manager.</td>
</tr>
<tr>
<td>Status</td>
<td>Select <strong>Enabled</strong> or <strong>Disabled</strong> to indicate whether the server is enabled.</td>
</tr>
<tr>
<td>Source IP Address</td>
<td>IP address of the NSX Edge interface through which the RSA server is accessible.</td>
</tr>
<tr>
<td>Use this server for secondary authentication</td>
<td>If selected, this server is used as the second level of authentication.</td>
</tr>
<tr>
<td>Terminate Session if authentication fails</td>
<td>When selected, the session is ended if authentication fails.</td>
</tr>
</tbody>
</table>

#### Local authentication server

### Table 14-5. Local authentication server options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable password policy</td>
<td>If selected, defines a password policy. Specify the required values.</td>
</tr>
<tr>
<td>Enable password policy</td>
<td>If selected, defines an account lockout policy. Specify the required values.</td>
</tr>
<tr>
<td></td>
<td>1 In Retry Count, type the number of times a remote user can try to access his or her account after entering an incorrect password.</td>
</tr>
<tr>
<td></td>
<td>2 In Retry Duration, type the time period in which the remote user's account gets locked on unsuccessful login attempts.</td>
</tr>
<tr>
<td></td>
<td>For example, if you specify Retry Count as 5 and Retry Duration as 1 minute, the remote user’s account will be locked if he makes 5 unsuccessful login attempts within 1 minute.</td>
</tr>
<tr>
<td></td>
<td>3 In Lockout Duration, type the time period for which the user account remains locked. After this time, the account is automatically unlocked.</td>
</tr>
<tr>
<td>Status</td>
<td>Select <strong>Enabled</strong> or <strong>Disabled</strong> to indicate whether the server is enabled.</td>
</tr>
<tr>
<td>Use this server for secondary authentication</td>
<td>If selected, this server is used as the second level of authentication.</td>
</tr>
<tr>
<td>Terminate Session if authentication fails</td>
<td>When selected, the session is ended if authentication fails.</td>
</tr>
</tbody>
</table>
(Optional) Add client certificate authentication.

a. Next to Certificate Authentication, click Change.
b. Select the Enable client certificate authentication check box.
c. Select a client certificate issued by the Root CA and click OK.

Restriction
- On the SSL VPN-Plus Web Portal and SSL VPN-Plus full access client (PHAT client), client or user certificate that is signed only by the Root CA is supported. Client certificate signed by an Intermediate CA is not supported.
- Client certificate authentication is supported only on an SSL VPN-Plus client that is installed on a Windows computer. This authentication is not supported on an SSL VPN-Plus client that is installed on Linux and Mac computers.

Add Installation Package

Create an installation package of the SSL VPN-Plus client for the remote user.

Procedure
1. In the SSL VPN-Plus tab, select Installation Package from the left panel.
2. Click the Add (✚) icon.
3. Type a profile name for the installation package.
4. In Gateway, type the IP address or FQDN of the public interface of NSX Edge.
   This IP address or FQDN is binded to the SSL client. When the client is installed, this IP address or FQDN is displayed on the SSL client.
5. Type the port number that you specified in the server settings for SSL VPN-Plus. See Add SSL VPN-Plus Server Settings.
6. (Optional) To bind additional NSX Edge uplink interfaces to the SSL client,
   a. Click the Add (✚) icon.
   b. Type the IP address and port number.
   c. Click OK.
7. The installation package is created for Windows operating system by default. Select Linux or Mac to create an installation package for Linux or Mac operating systems as well.
8. (Optional) Enter a description for the installation package.
9. Select Enable to display the installation package on the Installation Package page.
10 Select the following options as appropriate.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start client on logon</td>
<td>The SSL VPN client is started when the remote user logs on to his system.</td>
</tr>
<tr>
<td>Allow remember password</td>
<td>Enables the option.</td>
</tr>
<tr>
<td>Enable silent mode installation</td>
<td>Hides installation commands from remote user.</td>
</tr>
<tr>
<td>Hide SSL client network adapter</td>
<td>Hides the VMware SSL VPN-Plus Adapter, which is installed on the remote user's computer along with the SSL VPN installation package.</td>
</tr>
<tr>
<td>Hide client system tray icon</td>
<td>Hides the SSL VPN tray icon which indicates whether the VPN connection is active or not.</td>
</tr>
<tr>
<td>Create desktop icon</td>
<td>Creates an icon to invoke the SSL client on the user's desktop.</td>
</tr>
<tr>
<td>Enable silent mode operation</td>
<td>Hides the pop-up that indicates that installation is complete.</td>
</tr>
<tr>
<td>Server security certificate validation</td>
<td>The SSL VPN client validates the SSL VPN server certificate before establishing the secure connection.</td>
</tr>
<tr>
<td>Block user on certificate validation failure</td>
<td>If the certificate validation fails, then block the SSL VPN user.</td>
</tr>
</tbody>
</table>

11 Click OK.

Add a User

Add a remote user to the local database.

Procedure

1 In the SSL Vpn-Plus tab, select Users from the left panel.

2 Click the Add (➕) icon.

3 Type the user ID.

4 Type the password.

5 Retype the password.

6 (Optional) Type the first and last name of the user.

7 (Optional) Type a description for the user.

8 In Password Details, select Password never expires to always keep the same password for the user.

9 Select Allow change password to let the user change the password.

10 Select Change password on next login if you want the user to change the password the next time he logs in.

11 Set the user status.

12 Click OK.
Enable the SSL VPN-Plus Service

After configuring the SSL VPN-Plus service, enable the service for remote users to begin accessing private networks.

Procedure

1. In the SSL Vpn-Plus tab, select Dashboard from the left panel.
2. Click the [Enable] icon.

   The dashboard displays the status of the service, number of active SSL VPN sessions, and session statistics and data flow details. Click Details next to Number of Active Sessions to view information about the concurrent connections to private networks behind the NSX Edge gateway.

What to do next

1. Add an SNAT rule to translate the IP address of the NSX Edge appliance to the VPN Edge IP address.
2. Using a web browser, navigate to the IP address of the NSX Edge interface by typing https://NSXEdgeIPAddress.
3. Login using the user name and password that you created in the Add a User section and download the installation package.
4. Enable port forwarding on your router for the port number used in Add SSL VPN-Plus Server Settings.
5. Launch the VPN client, select your VPN server, and login. You can now navigate to the services on your network. SSL VPN-Plus gateway logs are sent to the syslog server configured on the NSX Edge appliance. SSL VPN-Plus client logs are stored in the following directory on the remote user's computer: %PROGRAMFILES%/VMWARE/SSLVPN Client/.

Add a Script

You can add multiple login or logoff scripts. For example, you can bind a login script for starting Internet Explorer with gmail.com. When the remote user logs in to the SSL client, Internet Explorer opens up gmail.com.

Procedure

1. In the SSL Vpn-Plus tab, select Login/Logoff Scripts from the left panel.
2. Click the Add (➕) icon.
3. In Script, click Browse and select the script you want to bind to the NSX Edge gateway.
4 Select the **Type** of script.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Performs the script action when remote user logs in to SSL VPN.</td>
</tr>
<tr>
<td>Logoff</td>
<td>Performs the script action when remote user logs out of SSL VPN.</td>
</tr>
<tr>
<td>Both</td>
<td>Performs the script action both when remote user logs in and logs out of SSL VPN.</td>
</tr>
</tbody>
</table>

5 Type a description for the script.

6 Select **Enabled** to enable the script.

7 Click **OK**.

### Install SSL VPN-Plus Client

Use the SSL VPN Full Access (PHAT) client to connect to a configured private network as a remote user. The client is supported on Windows, Mac, and Linux desktops.

### Install SSL VPN-Plus Client on a Remote Windows Site

Use the steps in this topic to install the SSL VPN-Plus client on a remote Windows site.

**Procedure**

1 On the remote client site, open a browser window, and type `https://ExternalEdgeInterfaceIP/sslvpn-plus/`, where `ExternalEdgeInterfaceIP` is the IP address of the Edge external interface where you enabled the SSL VPN-Plus service.

2 Log in to the portal using the credentials of the remote user.

3 Click the **Full Access** tab.

4 Click the name of the installer package from the list.

5 Click the **click here** link to download the installer package.

   The SSL client is downloaded.

6 Extract the downloaded files and run the `Installer.exe` file to install the client.

**What to do next**

Log in to the SSL client with the credentials specified in the Users section. The SSL VPN-Plus client validates the SSL VPN server certificate.

Windows client is authenticated as the **Server security certificate validation** option is selected by default, when the installation package was created.

For Internet Explorer (IE) browser, add a trusted CA to the trust certificate store. If server certificate validation fails, you are prompted to contact your system administrator. If server certificate validation succeeds, a login prompt is displayed.

Adding a trusted CA to the trust store is independent of SSL VPN work flow.
Install SSL VPN-Plus Client on a Remote Linux Site

Use the steps in this topic to install the SSL VPN-Plus client on a remote Linux site.

Prerequisites

Install Linux TCL and TK packages on the remote computer.

You must have root privileges to install the SSL VPN-Plus client.

Procedure

1. On the remote client site, open a browser window, and type
   \texttt{https://ExternalEdgeInterfaceIP/sslvpn-plus/}, where \texttt{ExternalEdgeInterfaceIP} is the IP
   address of the Edge external interface where you enabled the SSL VPN-Plus service.
2. Log in to the portal using the credentials of the remote user.
3. Click the \textbf{Full Access} tab.
4. Click the name of the installer package, and save the \texttt{linux_phat_client.tgz} compressed file on
   the remote computer.
5. Extract the compressed file. The \texttt{linux_phat_client} directory is created.
6. Open the Linux CLI and change to the \texttt{linux_phat_client} directory.
7. Run the \texttt{./install_linux_phat_client.sh} command.

What to do next

Log in to the SSL VPN GUI with the credentials specified in the Users section.

Attention

- Two-factor RSA authentication is not supported for logging in to the SSL VPN client on Linux
  operating systems.
- SSL VPN Linux client CLI does not validate server certificates. If server certificate validation is
  required, use the SSL VPN GUI for connecting to the gateway.

The SSL VPN Linux client validates the server certificate against the browser's certificate store by default.
If server certificate validation fails, you are prompted to contact your system administrator. If server
certificate validation succeeds, a login prompt is displayed.

Adding a trusted CA to the trust store (for example, Firefox certificate store) is independent of the SSL
VPN work flow.

Install SSL VPN-Plus Client on a Remote Mac Site

Use the steps in this topic to install the SSL VPN-Plus client on a remote Mac computer.

Prerequisites

You must have root privileges to install the SSL VPN-Plus client.
Procedure

1. On the remote client site, open a browser window, and type
   \[https://ExternalEdgeInterfaceIP/sslvpn-plus/\], where \(ExternalEdgeInterfaceIP\) is the IP address of the Edge external interface where you enabled the SSL VPN-Plus service.

2. Log in to the portal using the credentials of the remote user.

3. Click the **Full Access** tab.

4. Click the name of the installer package, and save the `mac_phat_client.tgz` compressed file on the remote computer.

5. Extract the compressed file. The `mac_phat_client` directory is created.

6. To install the SSL VPN-Plus client, double-click the `naclient.pkg` file.
   
   Follow the steps in the wizard to finish the installation.
   
   If your SSL VPN Client installation fails, check the installation log file at `/tmp/
   
   `naclient_install.log`. For troubleshooting installation problems on Mac OS High Sierra, see the *NSX Troubleshooting Guide*.

What to do next

Log in to the SSL client with the credentials specified in the Users section.

**Attention**  Two-factor RSA authentication is not supported for logging in to the SSL VPN client on Mac operating systems.

The SSL VPN Mac client validates the server certificate against Keychain, a database that stores certificates on Mac OS, by default. If server certificate validation fails, you are prompted to contact your system administrator. If server certificate validation succeeds, a login prompt is displayed.

**Configure Proxy Server Settings in SSL VPN-Plus Client**

Proxy server configuration is supported on an SSL VPN-Plus Client on a Windows computer, but not supported on Mac and Linux computers.

**Caution**

- Although, the SSL VPN-Plus Client on Mac OS provides the facility to configure proxy server settings, remote users must not configure the proxy server settings.

- Remote Linux OS users must avoid configuring the proxy server settings on the SSL VPN-Plus Client through the Linux CLI.

The following procedure explains the steps to configure the proxy server settings in an SSL VPN-Plus Client on a Windows computer.
Prerequisites

SSL VPN-Plus Client is installed on the remote Windows computer.

Procedure

1. Double-click the desktop icon of the SSL VPN-Plus Client on the Windows computer.
   
   The **SSL VPN-Plus Client - Login** window opens.

2. Click **Settings**, and then click the **Proxy Settings** tab.

3. Specify the proxy server settings.
   
   a. Select the **Use Proxy** check box.
   
   b. Under **Type Of Proxy**, configure one of the proxy server types.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use IE Settings</td>
<td>Use the proxy server configuration that is specified in your IE browser.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Specify the following settings for an HTTP proxy server:</td>
</tr>
<tr>
<td></td>
<td>■ Proxy server name or an IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>■ Proxy server port. The default port is 80, which you can edit.</td>
</tr>
<tr>
<td>SOCKS ver 4</td>
<td>Specify the following settings for a SOCKS 4.0 proxy server:</td>
</tr>
<tr>
<td></td>
<td>■ Proxy server name or an IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>■ Proxy server port. The default port is 1080, which you can edit.</td>
</tr>
<tr>
<td>SOCKS ver 5</td>
<td>Specify the following settings for a SOCKS 5.0 proxy server:</td>
</tr>
<tr>
<td></td>
<td>■ Proxy server name or an IP address of the proxy server.</td>
</tr>
<tr>
<td></td>
<td>■ Proxy server port. The default port is 1080, which you can edit.</td>
</tr>
<tr>
<td></td>
<td>■ (Optional) User name and password to access the SOCKS 5.0 server.</td>
</tr>
</tbody>
</table>

4. To save the proxy server settings, click **OK**.

SSL VPN-Plus Logs

SSL VPN-Plus gateway logs are sent to the syslog server configured on the NSX Edge appliance.

The following table lists the locations on the remote user's computer where the SSL VPN-Plus client logs are stored.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Location of Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 8</td>
<td>C:\Users\username\AppData\Local\VMware\vpn\svp_client.log</td>
</tr>
<tr>
<td>Windows 10</td>
<td>C:\Users\username\AppData\Local\VMware\vpn\svp_client.log</td>
</tr>
<tr>
<td>Linux</td>
<td>System log files</td>
</tr>
<tr>
<td>Mac</td>
<td>Installation log file at /tmp/naclient_install.log</td>
</tr>
<tr>
<td></td>
<td>System log files</td>
</tr>
</tbody>
</table>

Change SSL VPN-Plus Client Logs and Log Level

1. In the **SSL VPN-Plus** tab, click **Server Settings** from the left panel.
2 Go to the Logging Policy section and expand the section to view the current settings.

3 Click Change.

4 Select Enable logging check box to enable logging.
   OR
   Deselect Enable logging check box to disable logging.

5 Select the required log level.

   **Note**  SSL VPN-Plus client logs are enabled by default and log level is set to NOTICE.

6 Click OK.

**Edit Client Configuration**

You can change the way the SSL VPN client tunnel responds when the remote user logs in to SSL VPN.

**Procedure**

1 In the SSL VPN-Plus tab, select Client Configuration from the left panel.

2 Select the Tunneling Mode.
   
   In split tunnel mode, only the VPN flows through the NSX Edge gateway. In full tunnel, the NSX Edge gateway becomes the remote user's default gateway and all traffic (VPN, local, and internet) flows through this gateway.

3 If you selected the full tunnel mode:
   
   a Select Exclude local subnets to exclude local traffic from flowing through the VPN tunnel.
   
   b Type the IP address for the default gateway of the remote user's system.

4 Select Enable auto reconnect if you would like the remote user to automatically reconnect to the SSL VPN client after getting disconnected.

5 Select Client upgrade notification for the remote user to get a notification when an upgrade for the client is available. The remote user can then choose to install the upgrade.

6 Click OK.

**Edit General Settings**

You can edit the default VPN settings.

**Procedure**

1 In the SSL VPN-Plus tab, select General Settings from the left panel.
2 Make required selections.

<table>
<thead>
<tr>
<th>Select</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent multiple logon using same username</td>
<td>Allow a remote user to login only once with a username.</td>
</tr>
<tr>
<td>Enable compression</td>
<td>Enable TCP based intelligent data compression and improve data transfer speed.</td>
</tr>
<tr>
<td>Enable logging</td>
<td>Maintain a log of the traffic passing through the SSL VPN gateway.</td>
</tr>
<tr>
<td>Force virtual keyboard</td>
<td>Allow remote users to enter web or client login information only via the virtual keyboard.</td>
</tr>
<tr>
<td>Randomize keys of virtual keyboard</td>
<td>Make the virtual keyboard keys random.</td>
</tr>
<tr>
<td>Enable forced timeout</td>
<td>Disconnect the remote user after the specified timeout period is over. Type the timeout period in minutes.</td>
</tr>
<tr>
<td>Session idle timeout</td>
<td>If there is no activity on the user session for the specified period, end the user session after that period is over. SSLVPN idle timeout considers all packets, including control packets sent by any Application and user data, towards timeout detection. As a result, even if there is no user data, the session won't timeout if there is an application which transmits a periodic control packet (such as MDNS).</td>
</tr>
<tr>
<td>User notification</td>
<td>Type a message to be displayed to the remote user after he logs in.</td>
</tr>
</tbody>
</table>

3 Click OK.

**Edit Web Portal Design**

You can edit the client banner bound to the SSL VPN client.

**Procedure**

1 In the NSX Edges tab, double-click an NSX Edge.

2 Click the Manage tab and then click the SSL VPN-Plus tab.

3 Select Portal Customization from the left panel.

4 Type the portal title.

5 Type the remote user’s company name.

6 In Logo, click Change and preferably select a JPEG image for the company logo.

   There are no preferred dimensions for the logo size.

7 In Colors, click the color box next to numbered item for which you want to change the color, and select the desired color.

8 Change the client banner, if necessary. Select a BMP image for the banner.

   Preferred size for the client banner is 390 X 75 pixels.

9 Click OK.
Working with IP Pools for SSL VPN

You can edit or delete an IP pool.

For information on adding an IP pool, see Configure Network Access SSL VPN-Plus.

Edit an IP Pool

You can edit an IP pool.

Procedure

1. In the SSL VPN-Plus tab, click IP Pool in the left panel.
2. Select the IP pool that you want to edit.
3. Click the Edit (📝) icon.
   The Edit IP Pool dialog box opens.
4. Make the required edits.
5. Click OK.

Delete an IP Pool

You can delete an IP pool.

Procedure

1. In the SSL VPN-Plus tab, click IP Pool in the left panel.
2. Select the IP pool that you want to delete.
3. Click the Delete (🗑️) icon.
   The selected IP pool is deleted.

Enable an IP Pool

You can enable an IP pool if you want an IP address from that pool to be assigned to the remote user.

Procedure

1. In the SSL VPN-Plus tab, click IP Pool in the left panel.
2. Select the IP pool that you want to enable.
3. Click the Enable (✅) icon.

Disable an IP Pool

You can disable an IP pool if you do not want the remote user to be assigned an IP address from that pool.
Procedure
1 In the **SSL VPN-Plus** tab, select **IP Pool** from the left panel.
2 Select the IP pool that you want to disable.
3 Click the **Disable (🚫)** icon.

**Change the Order of an IP Pool**
SSL VPN assigns an IP address to a remote user from an IP pool based on its order in the IP pool table.

Procedure
1 In the **SSL VPN-Plus** tab, click **IP Pool** in the left panel.
2 Select the IP pool that you want to change the order for.
3 Click the **Move Up (⇑) or Move Down (⇓) icon.**

**Working with Private Networks**
You can edit or delete a private network that a remote user can access.

For information on adding a private network, see [Configure Network Access SSL VPN-Plus](#).

**Delete a Private Network**
You can delete a private network

Procedure
1 In the **SSL VPN-Plus** tab, click **Private Networks** in the left panel.
2 Select the network that you want to delete and click the **Delete (❌) icon.**

**Enable a Private Network**
When you enable a private network, the remote user can access it through SSL VPN-Plus.

Procedure
1 In the **SSL VPN-Plus** tab, click **Private Networks** in the left panel.
2 Click the network that you want to enable.
3 Click the **Enable** icon (✔).
   The selected network is enabled.

**Disable a Private Network**
When you disable a private network, the remote user cannot access it through SSL VPN-Plus.
Procedure

1. In the SSL VPN-Plus tab, click Private Networks in the left panel.
2. Click the network that you want to disable.
3. Click the Disable (🚫) icon.
   The selected network is disabled.

Change the Sequence of a Private Network

SSL VPN-Plus allows remote users to access private networks in the sequence in which they are displayed on the Private Networks panel.

If you select Enable TCP Optimization for a private network, some applications such as FTP in Active mode may not work within that subnet. To add an FTP server configured in Active mode, you must add another private network for that FTP server with TCP Optimization disabled. Also, the active TCP private network must be enabled, and must be placed above the subnet private network.

Procedure

1. In the SSL VPN-Plus tab, click Private Networks in the left panel.
2. Click the Change Order (⇅) icon.
3. Select the network that you want to change the order of.
4. Click the Move Up (⬆️) or Move Down (⬇️) icon.
5. Click OK.

What to do next

To add an FTP server configured in Active mode, refer to Configure Private Network for Active FTP Server.

Configure Private Network for Active FTP Server

You can add an FTP server configured in Active mode to the private network. For active FTP, the control connection is initiated by the back end FTP server to the client machine which does not support TCP optimization.

Prerequisites

FTP server is configured in Active mode.

Procedure

1. In the SSL VPN-Plus tab, click Private Networks in the left panel.
2. Add the private network that you want to configure for active FTP. For more information, refer to Add a Private Network.
3. Deselect the Enable TCP Optimization check box.
4 In the **Ports** field, add port number for the private network.

5 Select status as **Enabled** to enable the private network.

6 Place the private network that you want to configure for active FTP above other private networks that are configured. For more information, refer to [Change the Sequence of a Private Network](#).

**What to do next**

Add a corresponding firewall rule to allow the private network traffic.

## Working with Installation Packages

You can delete or edit an installation package for the SSL client.

For information on creating an installation package, see [Configure Network Access SSL VPN-Plus](#).

### Edit an Installation Package

You can edit an installation package.

**Procedure**

1 In the **SSL VPN-Plus** tab, click **Installation Package** in the left panel.

2 Select the installation package that you want to edit.

3 Click the **Edit** (✏️) icon.

   The Edit Installation Package dialog box opens.

4 Make the required edits.

5 Click **OK**.

### Delete an Installation Package

You can delete an installation package.

**Procedure**

1 In the **SSL VPN-Plus** tab, click **Installation Package** in the left panel.

2 Select the installation package that you want to delete.

3 Click the **Delete** (🗑️) icon.

## Working with Users

You can edit or delete users from the local database.

For information on adding a user, see [Configure Network Access SSL VPN-Plus](#).

### Edit a User

You can edit the details for a user except for the user ID.
Procedure

1. In the **SSL VPN-Plus** tab, click **Users** in the left panel.
2. Click the **Edit** icon.
3. Make the required edits.
4. Click **OK**.

Delete a User

You can delete a user.

Procedure

1. In the **SSL VPN-Plus** tab, click **Users** in the left panel.
2. **Users** in the Configure panel, click **Users**.
3. Select the user that you want to delete and click the **Delete** icon.

Change the Password for a User

You can change the password for a user.

Procedure

1. In the **SSL VPN-Plus** tab, click **Users** in the left panel.
2. Click the **Change Password** icon.
3. Type and re-type the new password.
4. Click **Change password on next login** to change the password when the user logs in to his system next time.
5. Click **OK**.

Working with Login and Logoff Scripts

You can bind a login or logoff script to the NSX Edge gateway.

Edit a Script

You can edit the type, description, and status of a login or logoff script that is bound to the NSX Edge gateway.

Procedure

1. In the **SSL VPN-Plus** tab, click **Login/Logoff Scripts** in the left panel.
2. Select a script and click the **Edit** icon.
3. Make the appropriate changes.
Delete a Script
You can delete a login or logoff script.

Procedure
1. In the SSL VPN-Plus tab, click Login/Logoff Scripts in the left panel.
2. Select a script and click the Delete (✕) icon.

Enable a Script
You must enable a script for it to work.

Procedure
1. In the SSL VPN-Plus tab, click Login/Logoff Scripts in the left panel.
2. Select a script and click the Enable (✔) icon.

Disable a Script
You can disable a login/logoff script.

Procedure
1. In the SSL VPN-Plus tab, click Login/Logoff Scripts in the left panel.
2. Select a script and click the Disable (🚫) icon.

Change the Order of a Script
You can change the order of a script. For example, suppose you have a login script for opening gmail.com in Internet Explorer placed above a login script for opening yahoo.com. When the remote user logs in to SSL VPN, gmail.com is displayed before yahoo.com. If you now reverse the order of the login scripts, yahoo.com is displayed before gmail.com.

Procedure
1. In the SSL VPN-Plus tab, click Login/Logoff Scripts in the left panel.
2. Select the script that you want to change the order of and click the Move Up (踊) or Move Down (ของตัวเอง) icon.
3. Click OK.

IPSec VPN Overview
NSX Edge supports site-to-site IPSec VPN between an NSX Edge instance and remote sites. Certificate authentication, preshared key mode, IP unicast traffic, and no dynamic routing protocol are supported between the NSX Edge instance and remote VPN routers.
Behind each remote VPN router, you can configure multiple subnets to connect to the internal network behind an NSX Edge through IPSec tunnels.

**Note** Subnets and the internal network behind a NSX Edge must have address ranges that do not overlap.

If the local and remote peer across an IPsec VPN have overlapping IP addresses, traffic forwarding across the tunnel might be not consistent depending on whether local connected routes and auto-plumbed routes exist.

You can deploy an NSX Edge agent behind a NAT device. In this deployment, the NAT device translates the VPN address of an NSX Edge instance to a publicly accessible address facing the Internet. Remote VPN routers use this public address to access the NSX Edge instance.

You can place remote VPN routers behind a NAT device as well. You must provide the VPN native address and the VPN Gateway ID to set up the tunnel. On both ends, static one-to-one NAT is required for the VPN address.

The number of tunnels needed is defined by the number of local subnets multiplied by the number of peer subnets. For example, if there are 10 local subnets and 10 peer subnets you need 100 tunnels. The maximum number of tunnels supported is determined by the ESG size, as shown below.

<table>
<thead>
<tr>
<th>ESG</th>
<th>Number of IPSec Tunnels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact</td>
<td>512</td>
</tr>
<tr>
<td>Large</td>
<td>1600</td>
</tr>
<tr>
<td>Quad-Large</td>
<td>4096</td>
</tr>
<tr>
<td>X-Large</td>
<td>6000</td>
</tr>
</tbody>
</table>

The following IPSec VPN algorithms are supported:

- AES (AES128-CBC)
- AES256 (AES256-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Diffie–Hellman group 2)
- DH-5 (Diffie–Hellman group 5)
- DH-14 (Diffie–Hellman group 14)
- DH-15 (Diffie–Hellman group 15)
- DH-16 (Diffie–Hellman group 16)

For IPSec VPN configuration examples, see **IPSec VPN Configuration Examples**.
For IPSec VPN troubleshooting, see https://kb.vmware.com/kb/2123580.

**Configuring IPSec VPN Service**

You can set up an NSX Edge tunnel between a local subnet and a peer subnet.

**Note** If you connect to a remote site via IPSec VPN, the IP address of that site cannot be learnt by Dynamic Routing on the Edge uplink.

**Enable IPSec VPN Service**

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the VPN tab.
5. Click IPSec VPN.
6. Click Enable.

**Use OpenSSL to Generate CA-Signed Certificates for IPSec VPNs**

To enable certificate authentication for IPSec, server certificates and corresponding CA-signed certificates must be imported. Optionally, you can use an open-source command-line tool such as OpenSSL to generate CA-signed certificates.

**Prerequisites**

OpenSSL must be installed.

**Procedure**

1. On a Linux or Mac machine where OpenSSL is installed, open the file: /opt/local/etc/openssl/openssl.cnf or /System/Library/OpenSSL/openssl.cnf.
2. Ensure that dir = .
3. Run the following commands:

   ```bash
   mkdir newcerts
   mkdir certs
   mkdir req
   mkdir private
   echo "01" > serial
   touch index.txt
   ```
4 Run the command to generate a CA-signed certificate:

```
openssl req -new -x509 -newkey rsa:2048 -keyout private/cakey.pem -out cacert.pem -days 3650
```

5 On NSX Edge1, generate a CSR, copy the privacy-enhanced mail (PEM) file content, and save it in a file in `req/edge1.req`.

6 Run the command to sign the CSR:

```
sudo openssl ca -policy policy_anything -out certs/edge1.pem -in req/edge1.req
```

7 On NSX Edge2, generate a CSR, copy the PEM file content, and save it in a file in `req/edge2.req`.

8 Run the command to sign the CSR:

```
sudo openssl ca -policy policy_anything -out certs/edge2.pem -in req/edge2.req
```

9 Upload the PEM certificate at the end of the file `certs/edge1.pem` to Edge1.

10 Upload the PEM certificate at the end of the file `certs/edge2.pem` to Edge2.

11 Upload the CA certificate in the file `cacert.pem` to Edge1 and Edge2 as CA-signed certificates.

12 In the IPSec global configuration for Edge1 and Edge2, select the uploaded PEM certificate and the uploaded CA certificate and save the configuration.

13 On the Certificate tab, click the uploaded certificate and record the DN string.

14 Reverse the DN string to the format

```
C=IN,ST=ka,L=blr,O=bmware,OU=vmware,CN=edge2.eng.vmware.com
```

and save it for Edge1 and Edge2.

15 Create IPsec VPN sites on Edge1 and Edge2 with Local ID and Peer ID as the distinguished name (DN) string in the specified format.

**Results**

Check the status by clicking Show IPsec Statistics. Click the channel to see the tunnel status. Both the channel and tunnel status should be green.

**Specify Global IPSec VPN Configuration**

This enables IPSec VPN on the NSX Edge instance.
Prerequisites
To enable certificate authentication, server certificates and corresponding CA-signed certificates must be imported. Optionally, you can use an open-source command-line tool such as OpenSSL to generate CA-signed certificates.

Self-signed certificates cannot be used for IPSec VPNs. They can only be used in load balancing and SSL VPNs.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the VPN tab.
5. Click IPSec VPN.
6. Click Change next to Global configuration status.
7. Type a global pre-shared key for those sites whose peer endpoint is set to any and select Display shared key to display the key.
8. Select Enable certificate authentication and select the appropriate certificate.
9. Click OK.

Enable Logging for IPSec VPN
You can enable logging of all IPSec VPN traffic.
By default, logging is enabled and is set to the WARNING level.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the VPN tab.
5. Click IPSec VPN.
6. Click Drag next to Logging Policy and click Enable logging to log the traffic flow between the local subnet and peer subnet and select the logging level.
7. Select the log level and click Publish Changes.

Configure IPSec VPN Parameters
You must configure at least one external IP address on the NSX Edge to provide IPSec VPN service.
Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the VPN tab.
5. Click IPSec VPN.
6. Click the Add (+) icon.
7. Type a name for the IPSec VPN.
8. Type the IP address of the NSX Edge instance in Local Id. This will be the peer Id on the remote site.
9. Type the IP address of the local endpoint.
   If you are adding an IP to IP tunnel using a pre-shared key, the local Id and local endpoint IP can be the same.
10. Type the subnets to share between the sites in CIDR format. Use a comma separator to type multiple subnets.
11. Type the Peer Id to uniquely identify the peer site. For peers using certificate authentication, this ID must be the common name in the peer’s certificate. For PSK peers, this ID can be any string. VMware recommends that you use the public IP address of the VPN or a FQDN for the VPN service as the peer ID.
12. Type the IP address of the peer site in Peer Endpoint. If you leave this blank, NSX Edge waits for the peer device to request a connection.
13. Type the internal IP address of the peer subnet in CIDR format. Use a comma separator to type multiple subnets.
   AES-GCM encryption algorithm is not FIPS compliant.
15. In Authentication Method, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSK (Pre Shared Key)</td>
<td>Indicates that the secret key shared between NSX Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes. PSK authentication is disabled in FIPS mode.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Indicates that the certificate defined at the global level is to be used for authentication.</td>
</tr>
</tbody>
</table>

16. Type the shared key in if anonymous sites are to connect to the VPN service.
17. Click Display Shared Key to display the key on the peer site.
18 In Diffie-Hellman (DH) Group, select the cryptography scheme that will allow the peer site and the NSX Edge to establish a shared secret over an insecure communications channel.

DH14 is default selection for both FIPS and non-FIPS mode. DH2 and DH5 are not available when FIPS mode is enabled.

19 In Extension, type one of the following:
- securelocaltrafficbyip=IPAddress to re-direct Edge's local traffic over the IPSec VPN tunnel. This is the default value. For more information see http://kb.vmware.com/kb/20080007.
- passthroughSubnets=PeerSubnetIPAddress to support overlapping subnets.

20 Click OK. NSX Edge creates a tunnel from the local subnet to the peer subnet.

What to do next
Enable the IPSec VPN service.

Edit IPSec VPN Service
You can edit an IPSec VPN service.

Procedure
1 Log in to the vSphere Web Client.
2 Click Networking & Security and then click NSX Edges.
3 Double-click an NSX Edge.
4 Click the Manage tab and then click VPN tab.
5 Click IPSec VPN.
6 Select the IPSec service that you want to edit.
7 Click the Edit (✏️) icon.
8 Make the appropriate edits.
9 Click OK.

Disable IPSec VPN Site
You can disable an IPSec VPN site.

Procedure
1 Log in to the vSphere Web Client.
2 Click Networking & Security and then click NSX Edges.
3 Double-click an NSX Edge.
4 Click the Manage tab and then click the VPN tab.
5 Click IPSec VPN.
6 Select the IPSec VPN site that you want to disable.
7 Click the Disable (🚫) icon.

**Delete IPSec VPN Site**

You can delete an IPSec VPN site.

**Procedure**

1 Log in to the vSphere Web Client.
2 Click Networking & Security and then click NSX Edges.
3 Double-click an NSX Edge.
4 Click the Manage tab and then click VPN tab.
5 Click IPSec VPN.
6 Select the IPSec VPN site that you want to delete.
7 Click the Delete (❌) icon.

**IPSec VPN Configuration Examples**

This scenario contains configuration examples for a basic point-to-point IPSEC VPN connection between an NSX Edge and a Cisco or WatchGuard VPN on the other end.

For this scenario, NSX Edge connects the internal network 192.168.5.0/24 to the internet. NSX Edge interfaces are configured as follows:

- Uplink interface: 192.168.5.1
- Internal interface: 10.115.199.103

The remote gateway connects the 172.15.0.0/16 internal network to the internet. The remote gateway interfaces are configured as follows:

- Uplink interface: 10.24.120.90
- Internal interface: 172.16.0.1
Figure 14-1. NSX Edge connecting to a remote VPN gateway

Note  For NSX Edge to NSX Edge IPSEC tunnels, you can use the same scenario by setting up the second NSX Edge as the remote gateway.

Terminology

IPSec is a framework of open standards. There are many technical terms in the logs of the NSX Edge and other VPN appliances that you can use to troubleshoot the IPSEC VPN.

These are some of the standards you may encounter:

- **ISAKMP (Internet Security Association and Key Management Protocol)** is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent.

- **Oakley** is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.

- **IKE (Internet Key Exchange)** is a combination of ISAKMP framework and Oakley. NSX Edge provides IKEv1.

- **Diffie-Hellman (DH)** key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. VSE supports DH group 2 (1024 bits) and group 5 (1536 bits).

**IKE Phase 1 and Phase 2**

IKE is a standard method used to arrange secure, authenticated communications.

**Phase 1 Parameters**

Phase 1 sets up mutual authentication of the peers, negotiates cryptographic parameters, and creates session keys. The Phase 1 parameters used by NSX Edge are:

- **Main mode**
- **TripleDES / AES [Configurable]**
- **SHA-1**
MODP group 2 (1024 bits)
pre-shared secret [Configurable]
SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying
ISAKMP aggressive mode disabled

Phase 2 Parameters
IKE Phase 2 negotiates an IPSec tunnel by creating keying material for the IPSec tunnel to use (either by using the IKE phase one keys as a base or by performing a new key exchange). The IKE Phase 2 parameters supported by NSX Edge are:

- TripleDES / AES [Will match the Phase 1 setting]
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between the two networks, using IPv4 subnets

Transaction Mode Samples
NSX Edge supports Main Mode for Phase 1 and Quick Mode for Phase 2.
NSX Edge proposes a policy that requires PSK, 3DES/AES128, sha1, and DH Group 2/5. The peer must accept this policy; otherwise, the negotiation phase fails.

Phase 1: Main Mode Transactions
This example shows an exchange of Phase 1 negotiation initiated from a NSX Edge to a Cisco device.
The following transactions occur in sequence between the NSX Edge and a Cisco VPN device in Main Mode.

1. NSX Edge to Cisco
   - proposal: encrypt 3des-cbc, sha, psk, group5(group2)
   - DPD enabled
2. Cisco to NSX Edge
   - contains proposal chosen by Cisco
     - If the Cisco device does not accept any of the parameters the NSX Edge sent in step one, the Cisco device sends the message with flag NO_PROPOSAL_CHOSEN and terminates the negotiation.
3. NSX Edge to Cisco
   - DH key and nonce
4 Cisco to NSX Edge
   - DH key and nonce

5 NSX Edge to Cisco (Encrypted)
   - include ID (PSK)

6 Cisco to NSX Edge (Encrypted)
   - include ID (PSK)
   - If the Cisco device finds that the PSK doesn't match, the Cisco device sends a message with flag INVALID_ID_INFORMATION; Phase 1 fails.

**Phase 2: Quick Mode Transactions**

The following transactions occur in sequence between the NSX Edge and a Cisco VPN device in Quick Mode.

1 NSX Edge to Cisco
   NSX Edge proposes Phase 2 policy to the peer. For example:
   
   Aug 26 12:16:09 weiqing-desktop
   ipsec[5789]:
   "s1-c1" #2: initiating Quick Mode
   PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
   {using isakmp#1 msgid:d20849ac
    proposal=3DES(3)_192-SHA1(2)_160
    pfsgroup=OAKLEY_GROUP_MODP1024}

2 Cisco to NSX Edge
   Cisco device sends back NO_PROPOSAL_CHOSEN if it does not find any matching policy for the proposal. Otherwise, the Cisco device sends the set of parameters chosen.

3 NSX Edge to Cisco
   To facilitate debugging, you can enable IPSec logging on the NSX Edge and enable crypto debug on Cisco (debug crypto isakmp <level>).

**Configuring IPSec VPN Service Example**

You must configure VPN parameters and then enable the IPSEC service.

**Procedure**

1 **Configure IPSec VPN Parameters Example**
   You must configure at least one external IP address on NSX Edge to provide IPSec VPN service.

2 **Enable IPSec VPN Service Example**
   You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.
Configure IPSec VPN Parameters Example
You must configure at least one external IP address on NSX Edge to provide IPSec VPN service.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the VPN tab.
5. Click IPSec VPN.
6. Click the Add (➕) icon.
7. Type a name for the IPSec VPN.
8. Type the IP address of the NSX Edge instance in Local Id. This will be the peer Id on the remote site.
9. Type the IP address of the local endpoint.
   If you are adding an IP to IP tunnel using a pre-shared key, the local Id and local endpoint IP can be the same.
10. Type the subnets to share between the sites in CIDR format. Use a comma separator to type multiple subnets.
11. Type the Peer Id to uniquely identify the peer site. For peers using certificate authentication, this ID must be the common name in the peer's certificate. For PSK peers, this ID can be any string. VMware recommends that you use the public IP address of the VPN or a FQDN for the VPN service as the peer ID.
12. Type the IP address of the peer site in Peer Endpoint. If you leave this blank, NSX Edge waits for the peer device to request a connection.
13. Type the internal IP address of the peer subnet in CIDR format. Use a comma separator to type multiple subnets.
15. In Authentication Method, select one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSK (Pre Shared Key)</td>
<td>Indicates that the secret key shared between NSX Edge and the peer site is to be used for authentication. The secret key can be a string with a maximum length of 128 bytes.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Indicates that the certificate defined at the global level is to be used for authentication.</td>
</tr>
</tbody>
</table>

16. Type the shared key in if anonymous sites are to connect to the VPN service.
17. Click Display Shared Key to display the key on the peer site.
In Diffie-Hellman (DH) Group, select the cryptography scheme that will allow the peer site and the NSX Edge to establish a shared secret over an insecure communications channel.

Change the MTU threshold if required.

Select whether to enable or disable the Perfect Forward Secrecy (PFS) threshold. In IPsec negotiations, Perfect Forward Secrecy (PFS) ensures that each new cryptographic key is unrelated to any previous key.

Click OK.

NSX Edge creates a tunnel from the local subnet to the peer subnet.

What to do next

Enable the IPSec VPN service.

Enable IPSec VPN Service Example

You must enable the IPSec VPN service for traffic to flow from the local subnet to the peer subnet.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the VPN tab.
5. Click IPSec VPN.
6. Click Enable.

What to do next

Click Enable Logging to log the traffic flow between the local subnet and peer subnet.

Using a Cisco 2821 Integrated Services Router

The following describes configurations performed using Cisco IOS.

Procedure

1. Configure Interfaces and Default Route

```
interface GigabitEthernet0/0
  ip address 10.24.120.90 255.255.252.0
duplex auto
  speed auto
crypto map MyVPN
!  
  interface GigabitEthernet0/1
  ip address 172.16.0.1 255.255.0.0
```
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 10.24.123.253

2 Configure IKE Policy

Router# config term
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encryption 3des
Router(config-isakmp)# group 2
Router(config-isakmp)# hash sha
Router(config-isakmp)# lifetime 28800
Router(config-isakmp)# authentication
    pre-share
Router(config-isakmp)# exit

3 Match Each Peer with Its Pre-Shared Secret

Router# config term
Router(config)# crypto isakmp key vshield
    address 10.115.199.103
Router(config-isakmp)# exit

4 Define the IPSEC Transform

Router# config term
Router(config)# crypto ipsec transform-set
    myset esp-3des esp-sha-hmac
Router(config-isakmp)# exit

5 Create the IPSEC Access List

Router# config term
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# access-list 101 permit ip
    172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
Router(config)# exit

6 Bind the Policy with a Crypto Map and Label It

In the following example, the crypto map is labeled MYVPN

Router# config term
Router(config)# crypto map MYVPN 1
    ipsec-isakmp
% NOTE: This new crypto map will remain
    disabled until a peer and a valid
    access list have been configured.
Router(config-crypto-map)# set transform-set
    myset
Router(config-crypto-map)# set pfs group1
Router(config-crypto-map)# set peer
10.115.199.103
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit

Example: Configuration

router2821#show running-config output
Building configuration...

Current configuration : 1263 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2821
!
boot-start-marker
boot-end-marker
!
! card type command needed for slot 0
! card type command needed for slot 1
enable password cisco
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
!no ip dhcp use vrf connected
!
! no ip ips deny-action ips-interface
!
crypto isakmp policy 1
encr 3des
authentication pre-share

group 2
crypto isakmp key vshield address 10.115.199.103
!
crypto ipsec transform-set myset esp-3des
   esp-sha-hmac
!
crypto map MYVPN 1 ipsec-isakmp
set peer 10.115.199.103
set transform-set myset
set pfs group1
match address 101
!
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN

interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto

ip classless
ip route 0.0.0.0 0.0.0.0 10.24.123.253

ip http server
no ip http secure-server

access-list 101 permit ip 172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255

control-plane

line con 0
line aux 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login

scheduler allocate 20000 1000

end

Using a Cisco ASA 5510

Use the following output to configure a Cisco ASA 5510.

ciscoasa# show running-config output
: Saved:
ASA Version 8.2(1)18

hostname ciscoasa
enable password 2KFQmbNIDI.2KYOU encrypted
passwd 2KFQmbNIDI.2KYOU encrypted
names

interface Ethernet0/0
nameif untrusted
security-level 100
ip address 10.24.120.90 255.255.252.0

interface Ethernet0/1
nameif trusted
security-level 90
ip address 172.16.0.1 255.255.0.0
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
boot system disk0:/asa821-18-k8.bin
ftp mode passive
access-list ACL1 extended permit ip 172.16.0.0 255.255.0.0
192.168.5.0 255.255.0.0
access-list ACL1 extended permit ip 192.168.5.0 255.255.0.0
172.16.0.0 255.255.0.0
access-list 101 extended permit icmp any any
pager lines 24
mtu untrusted 1500
mtu trusted 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any untrusted
icmp permit any trusted
no asdm history enable
arp timeout 14400
access-group 101 in interface untrusted
access-group 101 out interface untrusted
access-group 101 in interface trusted
access-group 101 out interface trusted
route untrusted 10.115.0.0 255.255.0.0 10.24.123.253 1
route untrusted 192.168.5.0 255.255.255.0 10.115.199.103 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac
Configuring a WatchGuard Firebox X500

You can configure your WatchGuard Firebox X500 as a remote gateway.

**Note**   Refer to your WatchGuard Firebox documentation for exact steps.

**Procedure**

1. In Firebox System Manager, select **Tools > Policy Manager >**.
2. In Policy Manager, select **Network > Configuration**.
3. Configure the interfaces and click **OK**.
4. (Optional) Select **Network > Routes** to configure a default route.
5. Select **Network > Branch Office VPN > Manual IPSec** to configure the remote gateway.
6. In the IPSec Configuration dialog box, click **Gateways** to configure the IPSEC Remote Gateway.
7. In the IPSec Configuration dialog box, click **Tunnels** to configure a tunnel.
8. In the IPSec Configuration dialog box, click **Add** to add a routing policy.
9  Click Close.

10  Confirm that the tunnel is up.

**L2 VPN Overview**

With L2 VPN, you can stretch multiple logical networks (both VLAN and VXLAN) across geographical sites. In addition, you can configure multiple sites on an L2 VPN server. Virtual machines remain on the same subnet when they are moved between sites and their IP addresses do not change. Egress optimization enables Edge to route any packets sent towards the Egress Optimization IP address locally, and bridge everything else.

L2 VPN thus allows enterprises to seamlessly migrate workloads backed by VXLAN or VLAN between physically separated locations. For cloud providers, L2 VPN provides a mechanism to on-board tenants without modifying existing IP addresses for workloads and applications.

Figure 14-2. Extending VXLAN across Multiple Sites using L2 VPN
The L2 VPN client and server learn the MAC addresses on both local and remote sites based on the traffic flowing through them. Egress optimization maintains local routing since the default gateway for all virtual machines are always resolved to the local gateway using firewall rules. Virtual machines that have been moved to Site B can also access L2 segments that are not stretched on Site A.

If one of the sites is not backed by NSX, a standalone NSX Edge can be deployed on that site.

In the following graphic, L2 VPN stretches network VLAN 10 to VXLAN 5010 and VLAN 11 to VXLAN 5011. So VM 1 bridged with VLAN 10 can access VMs 2, 5, and 6.

Figure 14-3. Extending Non-NSX Site with VLAN Based Network to NSX-Site with VXLAN Based Network

Configuring L2 VPN

To stretch your network using L2 VPN, you configure an L2 VPN server (destination Edge) and an L2 VPN client (source Edge). You must then enable the L2 VPN service on both the server and the client.
Prerequisites
A sub interface must have been added on a trunk interface of the NSX Edge. See Add a Sub Interface.

L2 VPN Best Practices
Configuring L2 VPN according to best practices can avoid problems such as looping and duplicate pings and responses.

L2VPN Options to Mitigate Looping
There are two options to mitigate looping. Either the NSX Edges and VMs can be on different ESXi hosts, or the NSX Edges and VMs can be on the same ESXi host.

Option 1: Separate ESXi hosts for the L2VPN Edges and the VMs

1. Deploy L2VPN Edges and VMs on separate ESXi hosts

   1. Deploy the Edges and the VMs on separate ESXi hosts.
   2. Configure the Teaming and Failover Policy for the Distributed Port Group associated with the Edge’s Trunk vNic as follows:
      a. Load balancing as “Route based on originating virtual port.”
      b. Configure only one uplink as Active and the other uplink as Standby.
   3. Configure the teaming and failover policy for the distributed port group associated with the VMs as follows:
      a. Any teaming policy is okay.
      b. Multiple active uplinks can be configured.
Configure Edges to use sink port mode and disable promiscuous mode on the trunk vNic.

**Note**
- Disable promiscuous mode: If you are using vSphere Distributed Switch.
- Enable promiscuous mode: If you are using virtual switch to configure trunk interface.

If a virtual switch has promiscuous mode enabled, some of the packets that come in from the uplinks that are not currently used by the promiscuous port, are not discarded. You should enable and then disable ReversePathFwdCheckPromisc that will explicitly discard all the packets coming in from the currently unused uplinks, for the promiscuous port.

To block the duplicate packets, activate RPF check for the promiscuous mode from the ESXi CLI where NSX Edge is present:

```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
esxcli system settings advanced list -o /Net/ReversePathFwdCheckPromisc
```

Path: /Net/ReversePathFwdCheckPromisc
Type: integer
Int Value: 1
Default Int Value: 0
Max Value: 1
Min Value: 0
String Value: 
Default String Value: 
Valid Characters: 
Description: Block duplicate packet in a teamed environment when the virtual switch is set to Promiscuous mode.

In **PortGroup** security policy, set **PromiscuousMode** from **Accept** to **Reject** and back to **Accept** to activate the configured change.

- **Option 2: Edges and VMs on the same ESXi host**
2. Deploy L2VPN Edges and VMs on the same host

**Route based on originating virtual port**

**Promiscuous mode: Disabled**

<table>
<thead>
<tr>
<th>Uplinks</th>
<th>Route based on originating virtual port</th>
<th>Uplinks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The order of the Active/Standby uplinks must be the same for both dvPortGroups.

| Uplinks | | |
|---------|---------|
|         |         |
|         |         |
|         |         |

| dvPortGroup | | |
|-------------|---------|
| SINK        |         |
| vDS         |         |

The order of the Active/Standby uplinks must be the same for both dvPortGroups.

<table>
<thead>
<tr>
<th>dvPortGroup</th>
<th>dvPortGroup</th>
<th>vDS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**a** Configure the teaming and failover policy for the distributed port group associated with Edge’s trunk vNic as follows:

1. Load balancing as “Route based on originating virtual port.”
2. Configure one uplink as active and the other uplink as standby.

**b** Configure the teaming and failover policy for the distributed port group associated with the VMs as follows:

1. Any teaming policy is okay.
2. Only one uplink can be active.
3. The order of the active/standby uplinks must be the same for the VMs' distributed port group and the Edge's trunk vNic distributed port group.

**c** Configure the client-side standalone edge to use sink port mode and disable promiscuous mode on the trunk vNic.

**Configure a Sink Port**

When an NSX-managed NSX Edge is set up as a L2 VPN client, some configuration is automatically done by NSX. When a standalone NSX Edge is set up as a L2 VPN client, these configuration steps must be done manually.

If one of the VPN sites does not have NSX deployed, you can configure an L2 VPN by deploying a standalone NSX Edge at that site. A standalone Edge is deployed using an OVF file on a host that is not managed by NSX. This deploys an Edge Services Gateway appliance to function as an L2 VPN client.
If a standalone edge trunk vNIC is connected to a vSphere Distributed Switch, either promiscuous mode or a sink port is required for L2 VPN function. Using promiscuous mode can cause duplicate pings and duplicate responses. For this reason, use sink port mode in the L2 VPN standalone NSX Edge configuration.

**Procedure**

1. Retrieve the port number for the trunk vNIC that you want to configure as a sink port.
   - a. Log in to the vSphere Web Client, and navigate to **Home > Networking**.
   - b. Click the distributed port group to which the NSX Edge trunk interface is connected, and click **Ports** to view the ports and connected VMs. Note the port number associated with the trunk interface.
     
     Use this port number when fetching and updating opaque data.

2. Retrieve the dvsUuid value for the vSphere Distributed Switch.
   - b. Click **content**.
   - c. Click the link associated with the **rootFolder** (for example: `group-d1 (Datacenters)`).
   - d. Click the link associated with the **childEntity** (for example: `datacenter-1`).
   - e. Click the link associated with the **networkFolder** (for example: `group-n6`).
   - f. Click the DVS name link for the vSphere distributed switch associated with the NSX Edges (for example: `dvs-1 (Mgmt_VDS)`).
   - g. Copy the value of the uuid string.

     Use this value for dvsUuid when fetching and updating opaque data.

3. Verify if opaque data exists for the specified port.
   - b. Click **fetchOpaqueDataEx**.
   - c. In the **selectionSet** value box paste the following XML input:

     ```xml
     <selectionSet xsi:type="DVPortSelection">
     <dvsUuid>c2 1d 11 50 6a 7c 77 6e 2a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid -->
     <portKey>393</portKey>  <!-- example port number -->
     </selectionSet>
     
     Use the port number and dvsUuid value that you retrieved for the NSX Edge trunk interface.
   
   d. Set **isRuntime** to **false**.
   
   e. Click **Invoke Method**.
If the result shows values for `vim.dvs.OpaqueData.ConfigInfo`, then there is already opaque data set, use the `edit` operation when you set the sink port. If the value for `vim.dvs.OpaqueData.ConfigInfo` is empty, use the `add` operation when you set the sink port.

4 Configure the sink port in the vCenter managed object browser (MOB).
   a Go to https://<vc-ip>/mob/?moid=DVSManager&vmodl=1.
   b Click `updateOpaqueDataEx`.
   c In the `selectionSet` value box paste the following XML input:

   ```xml
   <selectionSet xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
     <dvsUuid>c2 1d 11 50 6a 7c 77 68 e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid -->
     <portKey>393</portKey> <!-- example port number -->
   </selectionSet>
   ```

   Use the `dvsUuid` value that you retrieved from the vCenter MOB.
d  On the opaqueDataSpec value box paste one of the following XML inputs:

Use this input to enable a SINK port if opaque data is not set (operation is set to add):

```
<opaqueDataSpec>
  <operation>add</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData xsi:type="vmodl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

Use this input to enable a SINK port if opaque data is already set (operation is set to edit):

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData xsi:type="vmodl.Binary">AAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

Use this input to disable a SINK port:

```
<opaqueDataSpec>
  <operation>edit</operation>
  <opaqueData>
    <key>com.vmware.etherswitch.port.extraEthFRP</key>
    <opaqueData xsi:type="vmodl.Binary">AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

```
```
```
```
```
```

```
e  Set isRuntime to false.

f  Click Invoke Method.

Configure L2 VPN Server

The L2 VPN server is the destination NSX Edge to which the client is to be connected.
Procedure

1. In the L2 VPN tab, select Server and click Change.
2. In Listener IP, type the primary or secondary IP address of an external interface of the NSX Edge.
3. The default port for the L2 VPN service is 443. Edit the port number, if necessary.
4. Select the encryption algorithm for communication between the server and the client.
5. Select the certificate to be bound to SSL VPN server.
   
   **Important**  L2 VPN over SSL service supports only RSA certificates.

6. Click OK.

Add Peer Sites

You can connect multiple sites to the L2 VPN server.

**Note**  Changing site configuration settings causes the NSX Edge to disconnect and reconnect all existing connections.

Procedure

1. In the L2 VPN tab, ensure that the L2 VPN Mode is Server.
2. In Site Configuration Details, click the Add icon.
3. Type a unique name for the peer site.
4. Type the user name and password with which the peer site is to be authenticated. User credentials on the peer site should be the same as those on the client side.
5. In Stretched Interfaces, click Select Sub Interfaces to select the sub interfaces to be stretched with the client.
   a. In Select Object, select the trunk interface for the Edge.
      
      Sub interfaces configured on the trunk vNIC are displayed.
   b. Double-click the sub interfaces to be stretched.
   c. Click OK.

6. If the default gateway for virtual machines is the same across the two sites, type the gateway IP addresses in the Egress Optimization Gateway Address text box. These IP addresses are the addresses for which the traffic is to be locally routed or for which the traffic is to be blocked over the tunnel.
7  (Optional) Select the **Enable Unstretched Networks** check box when you want the VMs on the unstretched networks to communicate with the VMs that are behind the L2 VPN client edge on the stretched network. In addition, you want this communication to be routed through the same L2 VPN tunnel. Unstretched subnets can either be behind the L2 VPN server edge or the L2 VPN client edge or both.

For example, imagine that you have created an L2 VPN tunnel to stretch the 192.168.10.0/24 subnetwork between two data center sites using the NSX L2 VPN service.

Behind the L2 VPN server edge, you have two additional subnets (for example, 192.168.20.0/24 and 192.168.30.0/24). When unstretched networks are enabled, the VMs on 192.168.20.0/24 and 192.168.30.0/24 subnets can communicate with the VMs that are behind the L2 VPN client edge on the stretched network (192.168.10.0/24). This communication is routed through the same L2 VPN tunnel.

8  If you have enabled unstretched networks, do these steps depending on where the unstretched subnets are situated:

- When unstretched subnets are behind the L2 VPN client edge, enter the network address of the unstretched network in the CIDR format while adding the peer (client) site on the L2 VPN server edge. To enter multiple unstretched networks, separate the network addresses by commas.

- When unstretched subnets are behind the L2 VPN server edge, keep the **Unstretched Networks** text box blank. In other words, do not enter the network address of the unstretched networks while adding the client (peer) site on the L2 VPN server.

In the earlier example, because the unstretched subnets are behind the L2 VPN server edge, you must keep the **Unstretched Networks** text box blank in the **Add Peer Site** window.

9  Click **OK** and then click **Publish Changes**.

**Enable L2 VPN Service on Server**

You must enable the L2 VPN service on the L2 VPN server (destination NSX Edge). If HA is already configured on this Edge appliance, ensure that Edge has more than one internal interface configured on it. If only a single interface is present and that has already been used by HA, L2 VPN configuration on the same internal interface fails.

**Procedure**

1  Log in to the vSphere Web Client.

2  Click **Networking & Security** and then click **NSX Edges**.

3  Double-click a destination NSX Edge, and navigate to **Manage > VPN > L2 VPN**.

4  Next to **L2 VPN Service Status**, click **Start**.

**What to do next**

Create NAT or firewall rule on the Internet facing firewall side to enable the client and server to connect to each other.
Configure L2 VPN Client

The L2 VPN client is the source NSX Edge that initiates communication with the destination Edge (L2 VPN server).

You can also configure a standalone Edge as the L2 VPN client. See Configure Standalone Edge as L2 VPN Client.

Procedure

1. In the L2 VPN tab, set the **L2 VPN Mode** to **Client** and click **Change**.

2. Type the address of the L2 VPN server to which this client is to be connected. The address can be the host name or IP address.

3. Edit the default port to which the L2 VPN client must connect to, if necessary.

4. Select the encryption algorithm for communicating with the server.

5. In **Stretched Interfaces**, click **Select Sub Interfaces** to select the sub interfaces to be stretched to the server.
   a. In **Select Object**, select the trunk interface for the Edge.
      Sub interfaces configured on the trunk vNIC are displayed.
   b. Double-click the sub interfaces to be stretched.
   c. Click **OK**.

6. Type a description.

7. In **Egress Optimization Gateway Address**, type the gateway IP address of the sub interfaces or the IP addresses to which traffic should not flow over the tunnel.

8. (Optional) Select the **Enable Unstretched Networks** check box when you want the VMs on the unstretched networks to communicate with the VMs that are behind the L2 VPN server edge on the stretched network. In addition, you want this communication to be routed through the same L2 VPN tunnel. Unstretched subnets can either be behind the L2 VPN server edge or the L2 VPN client edge or both.

   For example, imagine that you have created an L2 VPN tunnel to stretch the 192.168.10.0/24 subnetwork between two data center sites using the NSX L2 VPN service.

   Behind the L2 VPN server edge, you have two additional subnets (for example, 192.168.20.0/24 and 192.168.30.0/24). When unstretched networks are enabled, the VMs on 192.168.20.0/24 and 192.168.30.0/24 subnets can communicate with the VMs that are behind the L2 VPN server edge on the stretched network (192.168.10.0/24). This communication is routed through the same L2 VPN tunnel.
9 If you have enabled unstretched networks, do these steps depending on where the unstretched subnets are situated:
   - When unstretched subnets are behind the L2 VPN server edge, enter the network address of the unstretched network in the CIDR format while configuring the L2 VPN client edge. To enter multiple unstretched networks, separate the network addresses by commas.
   - When unstretched subnets are behind the L2 VPN client edge, keep the **Unstretched Networks** text box blank. In other words, do not enter the network address of the unstretched networks on the L2 VPN client edge.

In the earlier example, because the unstretched subnets are behind the L2 VPN server edge, you must enter the unstretched networks as `192.168.20.0/24, 192.168.30.0/24` while configuring the L2 VPN client edge.

10 In **User Details**, type the user credentials to get authenticated at the server.

11 Click the **Advanced** tab.

   If the client NSX Edge does not have direct access to the Internet and must reach the source (server) NSX Edge through a proxy server, specify **Proxy Settings**.

12 To enable only secure proxy connections, select **Enable Secure Proxy**.

13 Type the proxy server address, port, user name, and password.

14 To enable server certificate validation, select **Validate Server Certificate** and select the appropriate CA certificate.

15 Click **OK** and then click **Publish Changes**.

**What to do next**

Ensure that the Internet facing firewall allows traffic to flow from L2 VPN Edge to the Internet. The destination port is 443.

**Enable L2 VPN Service on Client**

You must enable the L2 VPN service on the L2 VPN client (source NSX Edge).

**Procedure**

1. For the source NSX Edge, navigate to **Manage > VPN > L2 VPN**.

2. Next to **L2 VPN Service Status**, click **Start**.

**What to do next**

- To enable the client and server to connect to each other, create NAT or firewall rules on the Internet facing firewall side.

- If a trunk vNic backed by a standard portgroup is being stretched, enable the L2 VPN traffic manually by doing the following steps:

  a. Set **Promiscuous mode** to **Accept**.
b Set Forged Transmits to Accept.

For more information about promiscuous mode operation and forged transmits, see Securing vSphere Standard Switches in the VMware vSphere Documentation.

**Configure Standalone Edge as L2 VPN Client**

If one of the sites that you want to stretch is not backed by NSX, you can deploy a standalone edge as the L2 VPN client on that site.

If you want to change FIPS mode for a standalone edge, use the fips enable or fips disable command. For more information, refer to NSX Command Line Interface Reference.

**Prerequisites**

You have created a trunk port group for the trunk interface of the standalone edge to connect to. This port group requires some manual configuration:

- If the trunk port group is on a vSphere Standard Switch you must do the following:
  - Enable forged transmits
  - Enable promiscuous mode

  See the vSphere Networking Guide.

- If the trunk port group is on a vSphere Distributed Switch you must do the following:
  - Enable forged transmits. See the vSphere Networking Guide.
  - Enable sink port for the trunk vNic, or enable promiscuous mode. Enabling a sink port is the recommended best practice.

  Sink port configuration must be done after the standalone edge has been deployed, because you need to change the configuration of the port connected to the edge trunk vNIC.

**Procedure**

1. Using vSphere Web Client, log in to the vCenter Server that manages the non-NSX environment.
2. Select Hosts and Clusters and expand clusters to show the available hosts.
3. Right-click the host where you want to install the standalone Edge and select Deploy OVF Template.
4. Enter the URL to download and install the OVF file from the internet or click Browse to locate the folder on your computer that contains the standalone Edge OVF file and click Next.
5. On the OVF Template Details page, verify the template details and click Next.
6. On the Select name and folder page, type a name for the standalone Edge and select the folder or datacenter where you want to deploy. Then click Next.
7. On the Select storage page, select the location to store the files for the deployed template.
8. On the Select networks page, configure the networks the deployed template should use. Click Next.

   - The Public interface is the uplink interface.
The Trunk interface is used to create sub-interfaces for the networks that will be stretched. Connect this interface to the trunk port group you created.

9 On the Customize Template page, specify the following values.
   a Type and retype the CLI admin password.
   b Type and retype the CLI enable password.
   c Type and retype the CLI root password.
   d Type the uplink IP address and prefix length, and optionally default gateway and DNS IP address.
   e Select the cipher to be used for authentication. This should match the cipher used on the L2VPN server.
   f To enable Egress Optimization, type the gateway IP addresses for which traffic should be locally routed or for which traffic is to be blocked over the tunnel.
   g Type the L2 VPN server address and port.
   h Type the user name and password with which the peer site is to be authenticated.
   i In Sub Interfaces VLAN (Tunnel ID), type VLAN ID(s) of the network(s) you want to stretch. You can list the VLAN IDs as a comma separated list or range. For example, 2,3,10-20.
      If you want to change the VLAN ID of the network before stretching it to the standalone Edge site, you can type the VLAN ID of the network and then type the tunnel ID in brackets. For example, 2(100),3(200). The Tunnel ID is used to map the networks that are being stretched. However, you cannot specify the tunnel ID with a range. So this would not be allowed: 10(100)-14(104). You would need to rewrite this as 10(100),11(101),12(102),13(103),14(104).
   j If the standalone NSX Edge does not have direct access to the internet and needs to reach the source (server) NSX Edge via a proxy server, type the proxy address, port, user name, and password.
   k If a Root CA is available, you can paste it in to the Certificate section.
   l Click Next.

10 On the Ready to complete page, review the standalone Edge settings and click Finish.

What to do next
Power on the standalone Edge virtual machine.

Note the trunk vNIC port number and configure a sink port. See Configure a Sink Port.

Make any further configuration changes with the standalone edge command line interface. See the NSX Command Line Interface Reference.

View L2 VPN Statistics
You can view L2 VPN tunnel statistics, such as tunnel status, bytes sent and received, and other statistics, on both the L2 VPN server and client edges.
Procedure

1. View statistics on the L2 VPN client edge.
   a. Double-click the NSX Edge that you configured in L2 VPN client mode.
   b. Navigate to Manage > VPN > L2 VPN.
   c. Expand the Tunnel Status section, and click the Refresh icon to view the tunnel statistics.

2. View statistics on the L2 VPN server edge.
   a. Double-click the NSX Edge that you configured in L2 VPN server mode.
   b. Navigate to the L2 VPN page.
   c. In the Site Configuration Details section, click the Show L2VPN Statistics link.

What to do next

To see the networks configured on a trunk interface, navigate to Manage > Settings > Interfaces for the Edge and click Trunk in the Type column.

Remove a Stretched VLAN

An L2VPN can stretch multiple logical networks across geographical sites.

To remove a stretched VLAN from an L2 VPN Edge without affecting other stretched VLANS, you first remove the VLAN and then remove the sub-interface from both the L2 VPN client (source NSX Edge) and the L2 VPN server (destination NSX Edge).

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > NSX Edges.
2. Double-click an NSX Edge.
3. Click the Manage tab, then navigate to VPN > L2VPN.
4. In Site Configuration Details, stretched interfaces, remove the VLAN associated with the sub-interface.
5. Set the L2 VPN Mode to Client and remove the sub-interface for this VLAN.
6. Set the L2 VPN Mode to Server and remove the sub-interface for this VLAN.
7. Publish the changes.
The NSX Edge load balancer enables high-availability service and distributes the network traffic load among multiple servers. It distributes incoming service requests evenly among multiple servers in such a way that the load distribution is transparent to users. Load balancing thus helps in achieving optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload. NSX Edge provides load balancing up to Layer 7.

You map an external, or public, IP address to a set of internal servers for load balancing. The load balancer accepts TCP, UDP, HTTP, or HTTPS requests on the external IP address and decides which internal server to use. Port 80 is the default port for HTTP and port 443 is the default port for HTTPs.

You must have a working NSX Edge instance before you can configure load balancing. For information on setting up NSX Edge, see [NSX Edge Configuration](#).

For information on configuring an NSX Edge certificate, see [Working with Certificates](#).

NSX load balancing features are as follows:

- **Protocols**: TCP, UDP, HTTP, HTTPS
- **Algorithms**: Weighted round robin, IP hash, URI, least connection
- **SSL termination with AES-NI acceleration**
- **SSL bridging (client-side SSL + server-side SSL)**
- **SSL certificates management**
- **X-header forwarding for client identification**
- **L4/L7 transparent mode**
- **Connection throttling**
- **Enable/disable individual servers (pool members) for maintenance**
- **Health check methods (TCP, UDP, HTTP, HTTPS)**
- **Enhanced health check monitor**
- **Persistence/sticky methods**: SourceIP, MSRDIP, COOKIE, SSLSESSIONID
- **One-arm mode**
- Inline mode
- URL rewrite and redirection
- Application Rules for advanced traffic management
- HA session sticky support for L7 proxy load balancing
- IPv6 support
- Enhanced load balancer CLI for troubleshooting
- Available on all flavors of an NSX edge services gateway, with a recommendatory of X-Large or Quad Large for production traffic

**Topologies**

There are two types of load balancing services to configure in NSX, a one-armed mode, also known as a proxy mode, or the Inline mode, otherwise known as the transparent mode.

**NSX Logical Load Balancing: Inline Topology**

Inline or Transparent mode deploys the NSX edge inline to the traffic destined to the server farm. Transparent mode traffic flow is processed as follows:

- The external client sends traffic to the virtual IP address (VIP) exposed by the load balancer.
- The load balancer – a centralized NSX edge – performs only destination NAT (DNAT) to replace the VIP with the IP address of one of the servers deployed in the server farm.
- The server in the server farm replies to the original client IP address. The traffic is received again by the load balancer since it is deployed inline, usually as the default gateway for the server farm.
- The load balancer performs source NAT to send traffic to the external client, leveraging its VIP as source IP address.
**NSX Logical Load Balancing: One-Armed Topology**

One-Armed or Proxy mode consists of deploying an NSX edge directly connected to the logical network where load-balancing services are required.

- The external client sends traffic to the Virtual IP address (VIP) exposed by the load balancer.
- The load balancer performs two address translations on the original packets received from the client: destination NAT (DNAT) to replace the VIP with the IP address of one of the servers deployed in the server farm, and source NAT (SNAT) to replace the client IP address with the IP address identifying the load balancer itself. SNAT is required to force through the load balancer the return traffic from the server farm to the client.
- The server in the server farm replies by sending the traffic to the load balancer per SNAT functionality.
- The load balancer again performs a source and destination NAT service to send traffic to the external client, leveraging its VIP as source IP address.
Phase 1

<table>
<thead>
<tr>
<th>IP</th>
<th>DST 192.168.1.20</th>
<th>SRC 172.30.40.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>DST 80</td>
<td>SRC 1025</td>
</tr>
</tbody>
</table>

Phase 2 (DNAT+SNAT)

<table>
<thead>
<tr>
<th>IP</th>
<th>DST 192.168.1.3</th>
<th>SRC 192.168.1.20</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>DST 80</td>
<td>SRC 4099</td>
</tr>
</tbody>
</table>

Phase 3

<table>
<thead>
<tr>
<th>IP</th>
<th>DST 192.168.1.20</th>
<th>SRC 192.168.1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>DST 4099</td>
<td>SRC 80</td>
</tr>
</tbody>
</table>

Phase 4

<table>
<thead>
<tr>
<th>IP</th>
<th>DST 172.30.40.7</th>
<th>SRC 192.168.1.20</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>DST 1025</td>
<td>SRC 80</td>
</tr>
</tbody>
</table>

SLB

VIP

192.168.1.3 (Selected)

192.168.1.20

TCP 80

Logical Switch (VXLAN)

NSX Edge Services Gateway

Client Address 172.30.40.7

VLAN

Easy Insertion

Client IP is not detected

Workaround for HTTP X-Forwarded-For HTTP header

VM

192.168.1.2

VM

192.168.1.1

VM
This chapter includes the following topics:

- Setting Up Load Balancing
- Managing Application Profiles
- Managing Service Monitors
- Managing Server Pools
- Managing Virtual Servers
- Managing Application Rules
- Load Balance Web Servers using NTLM Authentication
- Load Balancer HTTP Connection Modes
- Scenarios for NSX Load Balancer Configuration

## Setting Up Load Balancing

The NSX Edge load balancer distributes network traffic across multiple servers to achieve optimal
resource use, provide redundancy, and distribute resource utilization.

NSX load balancer supports layer 4 and layer 7 load balancing engines. The layer 4 load balancer is
packet-based, providing fast path processing and the layer 7 load balancer is socket-based, allowing for
advanced traffic manipulations and DDOS mitigation for back-end services.

Packet-based load balancing is implemented on the TCP and UDP layer. Packet-based load balancing
does not stop the connection or buffer the whole request, it sends the packet directly to the selected
server after manipulating the packet. TCP and UDP sessions are maintained in the load balancer so that
packets for a single session are directed to the same server. You can select Acceleration Enable in both
the global configuration and relevant virtual server configuration to enable packet-based load balancing.

Socket-based load balancing is implemented on top of the socket interface. Two connections are
established for a single request, a client-facing connection and a server-facing connection. The server-facing
connection is established after server selection. For HTTP socket-based implementation, the whole
request is received before sending to the selected server with optional L7 manipulation. For HTTPS
socket-based implementation, authentication information is exchanged either on the client-facing
connection or on the server-facing connection. Socket-based load balancing is the default mode for TCP,
HTTP, and HTTPS virtual servers.

Key concepts of the NSX load balancer include:

**Virtual Server**

- Abstract of an application service, represented by a unique combination of IP, port, protocol and
  application profile such as TCP or UDP.

**Server Pool**

- Group of backend servers.
**Server Pool Member**

Represents the backend server as member in a pool.

**Service Monitor**

Defines how to probe the health status of a backend server.

**Application Profile**

Represents the TCP, UDP, persistence, and certificate configuration for a given application.

You begin by setting global options for the load balancer, then create a server pool of backend server members, and associate a service monitor with the pool to manage and share the backend servers efficiently.

Next, you create an application profile to define the common application behavior in a load balancer such as client SSL, server SSL, x-forwarded-for, or persistence. Persistence sends subsequent requests with similar characteristic such as source IP or cookie are required to be dispatched to the same pool member, without running the load balancing algorithm. Application profiles can be reused across virtual servers.

You then create an optional application rule to configure application-specific settings for traffic manipulation such as matching a certain URL or hostname so that different requests can be handled by different pools. Next, you create a service monitor that is specific to your application, or use a previously created service monitor.

Optionally, you can create an application rule to support advanced functionality of L7 virtual servers. Some use cases for application rules include content switching, header manipulation, security rules, and DOS protection.

Finally, you create a virtual server that connects your server pool, application profile, and any potential application rules together.

When the virtual server receives a request, the load balancing algorithm considers pool member configuration and runtime status. The algorithm then calculates the appropriate pool to distribute the traffic comprising one or more members. The pool member configuration includes settings such as, weight, maximum connection, and condition status. The runtime status includes current connections, response time, and health check status information. The calculation methods can be round-robin, weighted round-robin, least connection, source IP hash, weighted least connections, URL, URI, or HTTP header.

Each pool is monitored by the associated service monitor. When the load balancer detects a problem with a pool member, it is marked as DOWN. Only UP server is selected when choosing a pool member from the server pool. If the server pool is not configured with a service monitor, all the pool members are considered as UP.

---

**Note**  For load balancer troubleshooting information, refer to *NSX Troubleshooting Guide*.

- Configure Load Balancer Service
- **Create a Service Monitor**
  You create a service monitor to define health check parameters for a particular type of network traffic. When you associate a service monitor with a pool, the pool members are monitored according to the service monitor parameters.

- **Add a Server Pool**
  You can add a server pool to manage and share backend servers flexibly and efficiently. A server pool manages load balancer distribution methods and has a service monitor attached to it for health check parameters.

- **Create an Application Profile**
  Use application profiles to enhance your control over managing network traffic, and make traffic-management tasks easier and more efficient.

- **Add an Application Rule**
  You can write application rules by using the HAProxy syntax to manipulate and manage application traffic.

- **Add Virtual Servers**
  Add an NSX Edge internal or uplink interface as a virtual server.

### Configure Load Balancer Service

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click **Manage** and then click the **Load Balancer** tab.
5. Click **Edit**.
6 Select the check boxes next to the options to enable. Global load balancer configuration parameters can be specified.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Load Balancer</td>
<td>Allows the NSX Edge load balancer to distribute traffic to internal servers for load balancing.</td>
</tr>
<tr>
<td>Enable Acceleration</td>
<td>When disabled, all virtual IP addresses (VIPs) use the L7 LB engine. When enabled, the virtual IP uses the faster L4 LB engine or L7 LB engine (based on the VIP configuration). The L4 VIP (&quot;acceleration enabled&quot; in the VIP configuration and no L7 setting such as AppProfile with cookie persistence or SSL-Offload) is processed before the edge firewall, and no edge firewall rule is required to reach the VIP. However, if the VIP is using a pool in non-transparent mode, the edge firewall must be enabled (to allow the auto-created SNAT rule). The L7 HTTP/HTTPS VIPs (&quot;acceleration disabled&quot; or L7 setting such as AppProfile with cookie persistence or SSL-Offload) are processed after the edge firewall, and require an edge firewall allow rule to reach the VIP. Note: To validate which LB engine is used for each VIP by the NSX Load Balancer, on the NSX Edge CLI (ssh or console) run the following command: &quot;show service loadbalancer virtual&quot; and look for the field &quot;LB PROTOCOL [L4</td>
</tr>
<tr>
<td>Logging</td>
<td>The NSX Edge load balancer collects traffic logs. You can select the log level from the drop-down menu. The logs are exported to the configured syslog server. You can also use the show log follow command to list the load balancing logs. The debug and info options log end-user requests. Warning, error, and critical options do not log end-users requests. If the NSX Edge Control level log is set as debug or info, the load balancer logs lb, vip, pool, and pool member statistics every minute. Note that running in debug or info consumes CPU usage and edge log partition space, and might have a slight impact on maximum traffic management capability.</td>
</tr>
<tr>
<td>Enable Service Insertion</td>
<td>Allows the load balancer to work with third party vendor services. If you have a third party vendor load balancer service deployed in your environment, see Using a Partner Load Balancer.</td>
</tr>
</tbody>
</table>

7 Click OK.

Create a Service Monitor

You create a service monitor to define health check parameters for a particular type of network traffic. When you associate a service monitor with a pool, the pool members are monitored according to the service monitor parameters.

Five types of monitors are supported: ICMP, TCP, UDP, HTTP, and HTTPS.

Procedure

1 Log in to the vSphere Web Client.

2 Click Networking & Security and then click NSX Edges.
3 Double-click an NSX Edge.
4 Click Manage and then click the Load Balancer tab.
5 In the left navigation panel, click Service Monitoring.
6 Click the Add icon.
7 Enter a Name for the service monitor.
   Interval, Timeout, and Max Retries are common parameters for all types of health checks.
8 Enter the Interval in seconds in which a server is to be tested.
   The interval is the period of time in seconds that the monitor sends requests to the backend server.
9 Enter the Timeout. In each health check, the timeout value is the maximum time in seconds within which a response from the server must be received.
10 Enter the Max Retries. This value is the number of times the server is tested before it is declared DOWN.
   For example, if Interval is set as 5 seconds, Timeout as 15 seconds, and Max Retries as 3, it means NSX load balancer will probe backend server every 5 seconds. In each probe, if the expected response is received from server within 15 seconds, then the health check result is OK. If not, then the result is CRITICAL. If the recent three health check results are all DOWN, the server is marked as DOWN.
11 Select the way in which to send the health check request to the server from the drop-down menu. 
   Five types of monitors are supported- ICMP, TCP, UDP, HTTP, and HTTPS. Three predefined monitors are embedded in the system: default_tcp_monitor, default_http_monitor, and default_https_monitor.
12 If you select ICMP as the monitor type, then no other parameters are applicable. Leave other parameters empty.
13 If you select **TCP** as the monitor type, three more parameters are available: Send, Receive, and Extension.

a Send (optional) - The string sent to the backend server after a connection is established.

b Receive (optional) Enter the string to be matched. This string can be a header or in the body of the response. Only when the received string matches this definition is the server considered UP.

c Extension- Enter advanced monitor parameters as key=value pairs in the Extension section.

A sample extension, warning=10, indicates that if a server does not respond within 10 seconds, the status is set as warning.

All extension items should be separated with a carriage return character.

<table>
<thead>
<tr>
<th>Table 15-1. Extensions for TCP Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitor Extension</strong></td>
</tr>
<tr>
<td>escape</td>
</tr>
<tr>
<td>all</td>
</tr>
<tr>
<td>quit=STRING</td>
</tr>
<tr>
<td>refuse=ok</td>
</tr>
<tr>
<td>mismatch=ok</td>
</tr>
<tr>
<td>jail</td>
</tr>
<tr>
<td>maxbytes=INTEGER</td>
</tr>
<tr>
<td>delay=INTEGER</td>
</tr>
<tr>
<td>certificate=INTEGER[,INTEGER]</td>
</tr>
<tr>
<td>warning=DOUBLE</td>
</tr>
<tr>
<td>critical=DOUBLE</td>
</tr>
</tbody>
</table>

14 If you select **HTTP** or **HTTPS** as the monitor type, perform the steps below.

a Expected (optional) - Enter the string that the monitor expects to match in the status line of HTTP response in the Expected section. This is a comma separated list.

For example, 200,301,302,401.

b Method (optional) - Select the method to detect server status from the drop-down menu: GET, OPTIONS, or POST.
c URL (optional) - Enter the URL to GET or POST ("/") by default.

d If you select the POST method, enter the data to be sent in the Bold section.
Enter the string to be matched in the response content in the **Receive** section. This string can be a header or in the body of the response.

If the string in the Expected section is not matched, the monitor does not try to match the Receive content.

Extension - Enter advanced monitor parameters as key=value pairs in the Extension section.

A sample extension, warning=10, indicates that if a server does not respond within 10 seconds, the status is set as warning.

All extension items should be separated with a carriage return character.

**Table 15-2. Extensions for HTTP/HTTPS Protocol**

<table>
<thead>
<tr>
<th>Monitor Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-body</td>
<td>Do not wait for document body: stop reading after headers. Note that this still does an HTTP GET or POST, not a HEAD.</td>
</tr>
<tr>
<td>ssl-version=3</td>
<td>Force SSL handshake using ss1v3. ss1v3 and tlsv1 are disabled in the health check option by default.</td>
</tr>
<tr>
<td>ssl-version=10</td>
<td>Force SSL handshake using tls 1.0.</td>
</tr>
<tr>
<td>ssl-version=11</td>
<td>Force SSL handshake using tls 1.1.</td>
</tr>
<tr>
<td>ssl-version=12</td>
<td>Force SSL handshake using tls 1.2.</td>
</tr>
<tr>
<td>max-age=SECONDS</td>
<td>Warn if document is more than SECONDS old. The number can also be in the form 10m for minutes, 10h for hours, or 10d for days.</td>
</tr>
<tr>
<td>content-type=STRING</td>
<td>Specify Content-Type header media type in POST calls.</td>
</tr>
<tr>
<td>linespan</td>
<td>Allow regex to span newlines (must precede -r or -R).</td>
</tr>
<tr>
<td>regex=STRING or ereg=STRING</td>
<td>Search page for regex STRING.</td>
</tr>
<tr>
<td>eregi=STRING</td>
<td>Search page for case-insensitive regex STRING.</td>
</tr>
<tr>
<td>invert-regex</td>
<td>Return CRITICAL if found, OK if not.</td>
</tr>
<tr>
<td>proxy-authorization=AUTH_PAIR</td>
<td>Username:password on proxy-servers with basic authentication.</td>
</tr>
<tr>
<td>useragent=STRING</td>
<td>String to be sent in HTTP header as User Agent.</td>
</tr>
<tr>
<td>header=STRING</td>
<td>Any other tags to be sent in HTTP header. Use multiple times for additional headers.</td>
</tr>
<tr>
<td>onredirect=ok</td>
<td>warning</td>
</tr>
<tr>
<td>pagesize=INTEGER:INTEGER</td>
<td>Minimum page size required (bytes) : Maximum page size required (bytes).</td>
</tr>
<tr>
<td>warning=DOUBLE</td>
<td>Response time in seconds to result in warning status.</td>
</tr>
<tr>
<td>critical=DOUBLE</td>
<td>Response time in seconds to result in critical status.</td>
</tr>
</tbody>
</table>
Table 15-2. Extensions for HTTP/HTTPS Protocol (continued)

<table>
<thead>
<tr>
<th>Monitor Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>expect = STRING</code></td>
<td>Comma-delimited list of strings, at least one of them is expected in the first (status) line of the server response (default: HTTP/1. If specified skips all other status line logic (ex: 3xx, 4xx, 5xx processing))</td>
</tr>
<tr>
<td><code>string = STRING</code></td>
<td>String to expect in the content.</td>
</tr>
<tr>
<td><code>url = PATH</code></td>
<td>URL to GET or POST (default: <code>/</code>).</td>
</tr>
<tr>
<td><code>post = STRING</code></td>
<td>URL to encode http POST data.</td>
</tr>
<tr>
<td><code>method = STRING</code></td>
<td>Set HTTP method (for example, HEAD, OPTIONS, TRACE, PUT, DELETE).</td>
</tr>
<tr>
<td><code>timeout = INTEGER</code></td>
<td>Seconds before connection times out (default is 10 seconds).</td>
</tr>
<tr>
<td><code>header=Host:host_name -H host_name --sni</code></td>
<td><code>host_name</code> is a valid host name or an FQDN of the host. Create a separate service monitor for each virtual host, and add a server name indication (SNI) extension in each service monitor.</td>
</tr>
</tbody>
</table>

Table 15-3. Extensions for HTTPS Protocol

<table>
<thead>
<tr>
<th>Monitor Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>certificate=INTEGER</code></td>
<td>Minimum number of days a certificate has to be valid. Port defaults to 443. When this option is used the URL is not checked.</td>
</tr>
<tr>
<td><code>authorization=AUTH_PAIR</code></td>
<td>Username:password on sites with basic authentication.</td>
</tr>
<tr>
<td><code>ciphers='ECDHE-RSA-AES256-GCM-SHA384'</code></td>
<td>Display ciphers used in HTTPS health check.</td>
</tr>
</tbody>
</table>

15 If you select **UDP** as the monitor type, perform the steps below:

- a Send (required): Enter the string to be sent to backend server after a connection is established.
- b Receive (required): Enter the string expected to receive from backend server. Only when the received string matches this definition, is the server is considered as UP.

**Note** No extension is supported by UDP monitor.

16 Click **OK**.

**What to do next**

Associate a service monitor with a pool.

**Add a Server Pool**

You can add a server pool to manage and share backend servers flexibly and efficiently. A server pool manages load balancer distribution methods and has a service monitor attached to it for health check parameters.
Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click **Manage** and then click the **Load Balancer** tab.
5. In the left navigation panel, click **Pools**.
6. Click the **Add** icon.
7. Type a name and description for the load balancer pool.
8. Select the algorithm balancing method for each enabled service.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-HASH</td>
<td>Selects a server based on a hash of the source IP address and the total weight of all the running servers. Algorithm parameters are disabled for this option.</td>
</tr>
<tr>
<td>LEASTCONN</td>
<td>Distributes client requests to multiple servers based on the number of connections already on the server. New connections are sent to the server with the fewest connections. Algorithm parameters are disabled for this option.</td>
</tr>
<tr>
<td>ROUND_ROBIN</td>
<td>Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed. Algorithm parameters are disabled for this option.</td>
</tr>
<tr>
<td>URI</td>
<td>The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server receives the request. This ensures that a URI is always directed to the same server as long as no server goes up or down. The URI algorithm parameter has two options <code>uriLength=&lt;len&gt;</code> and <code>uriDepth=&lt;dep&gt;</code>. The length parameter range should be <code>1&lt;=len&lt;256</code>. The depth parameter range should be <code>1&lt;=dep&lt;10</code>. Length and depth parameters are followed by a positive integer number. These options can balance servers based on the beginning of the URI only. The length parameter indicates that the algorithm should only consider the defined characters at the beginning of the URI to compute the hash. The depth parameter indicates the maximum directory depth to be used to compute the hash. One level is counted for each slash in the request. If both parameters are specified, the evaluation stops when either is reached.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| HTTPHEADER    | HTTP header name is looked up in each HTTP request. The header name in parenthesis is not case sensitive which is similar to the ACL `hdr()` function. If the header is absent or does not contain any value, the round robin algorithm is applied. The HTTPHEADER algorithm parameter has one option `headerName=<name>`.
|               | For example, you can use `host` as the HTTPHEADER algorithm parameter.                                                                                                                                          |
| URL           | URL parameter specified in the argument is looked up in the query string of each HTTP GET request. If the parameter is followed by an equal sign `=` and a value, then the value is hashed and divided by the total weight of the running servers. The result designates which server receives the request. This process is used to track user identifiers in requests and ensure that a same user ID is always sent to the same server as long as no server goes up or down.
|               | If no value or parameter is found, then a round robin algorithm is applied. The URL algorithm parameter has one option `urlParam=<url>`.                                                                          |

9  (Optional) Select an existing default or custom monitor from the **Monitors** drop-down menu.

10 Add members to the pool.

a  Click the **Add** icon (➕).

b  Enter the name and IP address of the server member or click **Select** to assign grouping objects.

**Note**  VMware Tools must be installed on each VM, or an enabled IP discovery method (DHCP snooping or ARP snooping, or both) must be in place to when using grouping objects instead of IP addresses. For more details, refer to the IP Discovery for Virtual Machines. The grouping objects can be either vCenter or NSX.

c  Select the member state as **Enable**, **Disable**, or **Drain**.

- **Drain** - Forces the server to shut down gracefully for maintenance. Setting the pool member as "drain" removes the back end server from load balancing, while allowing it to be used for exiting connections and new connections from clients with persistence to that server. The persistence methods that work with drain state are source IP persistence, cookie insert, and cookie prefix.

  **Note**  Enabling and disabling High Availability configuration on the NSX Edge can break the persistence and drain state with source IP persistence method.

- **Enable** - Removes the server from maintenance mode and brings it back into operation. The pool member state should be either **Drain** or **Disabled**.

- **Disable** - The server remains in maintenance mode.

  **Note**  You cannot change the pool member state from **Disabled** to **Drain**.
Enter the port where the member is to receive traffic, and the monitor port where the member is to receive health monitor pings.

Port value should be null if the related virtual server is configured with a port range.

Enter the proportion of traffic this member is to handle in the Weight section.

Enter the maximum number of concurrent connections the member can handle.

If the incoming requests goes higher than the maximum, they are queued and wait for a connection be released.

Enter the minimum number of concurrent connections a member must always accept.

Click OK.

Check Transparent to make client IP addresses visible to the backend servers. For more details, refer to Chapter 15 Logical Load Balancer.

If Transparent is not selected (default value), backend servers see the traffic source IP address as a load balancer internal IP address. If Transparent is selected, the source IP address is the real client IP address and the NSX Edge must be set as the default gateway to ensure that return packets go through the NSX Edge device.

Click OK.

Create an Application Profile

Use application profiles to enhance your control over managing network traffic, and make traffic-management tasks easier and more efficient.

You create an application profile to define the behavior of a particular type of network traffic. After configuring a profile, you associate the profile with a virtual server. The virtual server then processes traffic according to the values specified in the profile.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click Manage and then click the Load Balancer tab.
5. In the left navigation panel, click Application Profiles.
6. Click the Add (✚) icon.
7 Type a name for the profile and select the traffic type for which you are creating the profile from the drop-down menu.

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Persistence Method Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Source IP, MSRDP</td>
</tr>
<tr>
<td>HTTP</td>
<td>Cookie, Source IP</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Cookie, SSL Session ID (SSL Passthrough enabled), Source IP</td>
</tr>
<tr>
<td>UDP</td>
<td>Source IP</td>
</tr>
</tbody>
</table>

8 Enter the URL to which you want to redirect HTTP traffic.

   For example, you can direct traffic from http://myweb.com to https://myweb.com.

9 Specify persistence type for the profile from the drop-down menu.

   Persistence tracks and stores session data, such as the specific pool member that serviced a client request. With persistence, client requests are directed to the same pool member throughout the life of a session or during subsequent sessions.

   - Select **Cookie** persistence to insert a unique cookie to identify the session the first time a client accesses the site.

     The cookie is referred in subsequent requests to persist the connection to the appropriate server.

   - Select **Source IP** persistence to track sessions based on the source IP address.

     When a client requests a connection to a virtual server that supports source address affinity persistence, the load balancer checks to see if that client previously connected, and if so, returns the client to the same pool member.

   - Select Microsoft Remote Desktop Protocol **MSRDP** persistence to maintain persistent sessions between Windows clients and servers that are running the Microsoft Remote Desktop Protocol (RDP) service.

     The recommended scenario for enabling MSRDP persistence is to create a load balancing pool that consists of members running Windows Server 2003 or Windows Server 2008, where all members belong to a Windows cluster and participate in a Windows session directory.
10 Enter a cookie name and select the mode by which the cookie should be inserted.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insert</td>
<td>NSX Edge sends a cookie. If the server sends one or more cookies, the client receives an extra cookie (the server cookie(s) + the Edge cookie). If the server does not send a cookie, the client receives the Edge cookie.</td>
</tr>
<tr>
<td>Prefix</td>
<td>This option is selected if your client does not support more than one cookie. Note All browsers accept multiple cookies. If you have a proprietary application using a proprietary client that supports only one cookie. The Web server sends its cookie as usual. NSX Edge injects (as a prefix) its cookie information in the server cookie value. This cookie added information is removed when NSX Edge sends it to the server.</td>
</tr>
<tr>
<td>App Session</td>
<td>The server does not send a cookie. Instead, it sends the user session information as a URL. For example, <a href="http://mysite.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD">http://mysite.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD</a>, where jsessionid is the user session information and is used for the persistence. It is not possible to see the App Session persistence table for troubleshooting.</td>
</tr>
</tbody>
</table>

11 Enter the persistence expiration time in seconds. The default value of persistence is 300 seconds (five minutes). Note that the persistence table is of limited size. A large timeout value may lead to the persistence table quickly filling up if the traffic is heavy. When the persistence table fills up, the oldest entry is deleted to accept the newest entry.

The load balancer persistence table maintains entries to record that client requests are directed to the same pool member.

- If no new connection requests are received from the same client within the timeout period, the persistence entry expires and is deleted.
- If a new connection request from same client is received within the timeout period, the timer is reset, and the client request is sent to a sticky pool member.
- After the timeout period has expired, new connection requests will be sent to a pool member allocated by the load balancing algorithm.

For the L7 load balancing TCP source IP persistence scenario, the persistence entry times out if no new TCP connections are made for a period of time, even if the existing connections are still alive.

12 (Optional) Create an application profile for HTTPS traffic.

Supported HTTPS traffic patterns:

- SSL Offloading - Client -> HTTPS -> LB (terminate SSL) -> HTTP -> server
- SSL Proxy - Client -> HTTPS -> LB (terminate SSL) -> HTTPS -> server
- SSL Passthrough - Client -> HTTPS -> LB (SSL passthrough) -> HTTPS -> server
- Client -> HTTP -> LB -> HTTP -> servers
  
a  (Optional) Check **Insert X-Forwarded-For HTTP header** to identify the originating IP address of a client connecting to a Web server through the load balancer.

b  Check **Configure Service Certificate** to select the applicable service certificate, CA certificates, and CRLs used to terminate the HTTPS traffic from the client on the load balancer in the **Virtual Server Certificates** tab.

  This is only required if the Client -> LB connection is HTTPS.

c  (Optional) Check **Enable Pool Side SSL** to enable the HTTPS communication between the load balancer and the backend servers.

  You can use the pool side SSL to configure End-to-End SSL.

d  (Optional) Check **Configure Service Certificate** to select the applicable service certificate, CA certificates, and CRLs used to authenticate the load balancer from the server side in the **Pool Certificates** tab.

  This is only required for the pattern Client -> HTTPS -> LB -> HTTPS -> servers.

  You can configure service certificate if the NSX Edge load balancer has CA certificate and CRL already configured and needs to verify service certificate from backend servers. This option can also be used to provide load balancer certificate to backend server if the backend server needs to verify the load balancer side service certificate.

13 Enter the cipher algorithms or cipher suite negotiated during the SSL/TLS handshake. Multiple ciphers can be added, separated with a colon (:). Make sure that the approved cipher suite contains DH key length more than or equal to 1024 bits.

You can use approved ciphers suite as below:

<table>
<thead>
<tr>
<th>Cipher Value</th>
<th>Cipher Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
<td>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
<td>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES256-SHA</td>
<td>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>ECDH-ECDSA-AES256-SHA</td>
<td>TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>ECDH-RSA-AES256-SHA</td>
<td>TLS_ECDH_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>AES256-SHA</td>
<td>TLS_RSA_WITH_AES_256_CBC_SHA</td>
</tr>
<tr>
<td>AES128-SHA</td>
<td>TLS_RSA_WITH_AES_128_CBC_SHA</td>
</tr>
<tr>
<td>DES-CBC3-SHA</td>
<td>TLS_RSA_WITH_3DES_EDE_CBC_SHA</td>
</tr>
</tbody>
</table>

14 Specify whether client authentication is to be ignored or required from the drop-down menu.

If you select required, the client must provide a certificate after the request or the handshake is aborted.
15 Click OK.

**Add an Application Rule**

You can write application rules by using the HAProxy syntax to manipulate and manage application traffic.

For information about the application rule syntax, see HAProxy documentation at [http://cbonte.github.io/haproxy-dconv/](http://cbonte.github.io/haproxy-dconv/).

For examples of commonly used application rules, see Application Rule Examples.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click **Manage** and then click the **Load Balancer** tab.
5. In the left navigation panel, click **Application Rules**.
6. Click the **Add (✚)** icon.
7. Type the name and script for the rule.
8. Click **OK**.

**Application Rule Examples**

Commonly used application rules.

**HTTP/HTTPS Redirection Based on Condition**

An application profile allows you to specify HTTP/HTTPS redirection, which always redirects traffic regardless of the request URLs. You also have the flexibility to specify the conditions in which HTTP/HTTPS traffic should be redirected.

```
move the login URL only to HTTPS.
acl clear dst_port 80
acl secure dst_port 8080
acl login_page url_beg /login
acl logout url_beg /logout
acl uid_given url_reg /login?userid=\[^&\]+\)
acl cookie_set hdr_sub(cookie) SEEN=1
redirect prefix https://mysite.com set-cookie SEEN=1 if !cookie_set
redirect prefix https://mysite.com if login_page !secure
redirect prefix http://mysite.com drop-query if login_page !uid_given
redirect location http://mysite.com/ if !login_page secure
    redirect location / clear-cookie USERID= if logout
```
Routing by Domain Name

You can create an application rule to direct requests to a specific load balancer pool according to domain name. The following rule direct requests to foo.com to pool_1, and requests to bar.com to pool_2.

```
  acl is_foo hdr_dom(host) = i foo
  acl is_bar hdr_dom(host) = i bar
  use_backend pool_1 if is_foo
  use_backend pool_2 if is_bar
```

Microsoft RDP Load Balancing and Protection

In the following sample scenario, the load balancer balances a new user to the less loaded server and resumes a broken session. The NSX Edge internal interface IP address for this scenario is 10.0.0.18, internal interface IP address is 192.168.1.1, and the virtual servers are 192.168.1.100, 192.168.1.101, and 192.168.1.102.

1. Create a application profile for TCP traffic with MSRDP persistence.
2. Create a TCP health monitor (tcp_monitor).
4. Associate tcp_monitor to rdp-pool.
5. Create the following application rule.

```
tcp-request content track-sc1 rdp_cookie(mstshash) table rdp-pool
tcp-request content track-sc2 src table ipv4_ip_table

#   each single IP can have up to 2 connections on the VDI infrastructure
tcp-request content reject if { sc2_conn_cur ge 2 }

#   each single IP can try up to 5 connections in a single minute
tcp-request content reject if { sc2_conn_rate ge 10 }

# Each user is supposed to get a single active connection at a time, block the second one
tcp-request content reject if { sc1_conn_cur ge 2 }

# if a user tried to get connected at least 10 times over the last minute,
# it could be a brute force
tcp-request content reject if { sc1_conn_rate ge 10 }
```
6. Create a virtual server (named rdp-vs).
7. Associate the application profile to this virtual server and add the application rule created in step 4.

The newly applied application rule on the virtual server protects the RDP servers.
Advanced Logging

By default, NSX load balancer supports basic logging. You can create an application rule as follows to view more detailed logging messages for troubleshooting.

```plaintext
# log the name of the virtual server
capture request header Host len 32

# log the amount of data uploaded during a POST
capture request header Content-Length len 10

# log the beginning of the referrer
capture request header Referer len 20

# server name (useful for outgoing proxies only)
capture response header Server len 20

# logging the content-length is useful with "option logasap"
capture response header Content-Length len 10

# log the expected cache behaviour on the response
capture response header Cache-Control len 8

# the Via header will report the next proxy's name
capture response header Via len 20

# log the URL location during a redirection
capture response header Location len 20
```

After you associate the application rule to the virtual server, logs include detailed messages such as the following example.

```
2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 - - [25/Apr/2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" "" 
```

To troubleshoot the HTTPS traffic, you may need to add more rules. Most web application use 301/302 responses with a location header to redirect the client to a page (most of the time after a login or a POST call) and also require an application cookie. So your application server may have difficulty in getting to know client connection information and may not be able to provide the correct responses: it may even stop the application from working.
To allow the web application to support SSL offloading, add the following rule.

```plaintext
# See clearly in the log if the application is setting up response for HTTP or HTTPS
capture response header Location len 32
capture response header Set-Cookie len 32

# Provide client side connection info to application server over HTTP header
http-request set-header X-Forwarded-Proto https if { ssl_fc }
http-request set-header X-Forwarded-Proto http if !{ ssl_fc }
```

The load balancer inserts the following header when the connection is made over SSL.

```plaintext
X-Forwarded-Proto: https
```

The load balancer inserts the following header when the connection is made over HTTP.

```plaintext
X-Forwarded-Proto: http
```

**Block Specific URLs**

You can block requests that contain specific keywords in the URL. The following sample rule checks if the request starts with `/private` or `/finance` and blocks the requests that have those terms.

```plaintext
# Check if the request starts with "/private" or "/finance" (case insensitive)
acl block_url_list path_beg -i /private /finance

# If the request is part of the list forbidden urls, reply "Forbidden" (HTTP response code 403)
block if block_url_list
```

**Authentication HTTP Redirect If No Cookies**

You can redirect a client request that does not have a cookie to get an authentication. The following sample rule checks if the HTTP request is authentic and has cookies in the header. If the request does not have cookies then the rule redirects the request to `/authent.php` for authentication.

```plaintext
acl authent_url url /authent.php
acl cookie_present hdr_sub(cookie) cookie1=
redirect prefix /authent.php if !authent_url !cookie_present
```

**Default Page Redirect**

You can redirect the client request `/` to a default page. The following sample rule checks if the HTTP request is `/` and redirects the request to a default login page.

```plaintext
acl default_url url /
redirect location /login.php if default_url
```
Redirect to Maintenance Site
When the primary pool is down, you can use a maintenance server pool and redirect the URL to the maintenance Web site.

```plaintext
redirect location http://maintenance.xyz.com/maintenance.htm
```

NT LAN Manager (NTLM) Authentication
By default on the server side NSX closes the TCP connection after each request. When you do not want to close the server session after each request, you can keep the server session alive and secure with the NTLM protocol.

```plaintext
no option http-server-close
```

By default on the client side NSX keeps the TCP connection established between requests. However with option "X-Forwarded-For", the session is closed after each request. The following option keeps the client connection open between requests even if XFF is configured.

```plaintext
no option httpclose
```

Replace Server Header
You can delete the existing response server header and replace it with another server. The following sample rule deletes the server header and replaces it with the NGINX Web server that can act as a reverse proxy server for HTTP, HTTPS, SMTP, POP3, and IMAP protocols, HTTP cache, and a load balancer.

```plaintext
rspidel Server
rspadd Server: \ nginx
```

Rewrite Redirect
You can rewrite the Location header from HTTP to HTTPS. The following sample rule identifies the Location header and replaces the HTTP with HTTP.

```plaintext
rspirep ^Location:\ http://(.*) Location:\ https://\1
```

Select Specific Pool Based on Host
You can redirect requests with a specific host to defined pools. The following sample rule checks for the request for specific hosts app1.xyz.com, app2.xyz.com, and host_any_app3 and redirects these requests respectively to defined pools, pool_app1, or pool_app2, and pool_app3. All other requests are redirected to existing pools defined in the Virtual Server.

```plaintext
acl host_app1 hdr(Host) -i app1.xyz.com
acl host_app2 hdr(Host) -i app2.xyz.com
acl host_any_app3 hdr_beg(host) -i app3
```
Use a specific pool for each hostname.

```
use_backend pool_app1 if host_app1
use_backend pool_app2 if host_app2
use_backend pool_app3 if host_any_app3
```

**Select Specific Pool Based on URLs**

You can redirect requests with URL keywords to specific pools. The following sample rule checks if the request starts with /private or /finance and redirects these requests to defined pools, pool_private or pool_finance. All other requests are redirected to existing pools defined in the Virtual Server.

```
acl site_private path_beg -i /private
acl site_finance path_beg -i /finance
use_backend pool_private if site_private
use_backend pool_finance if site_finance
```

**Redirect When Primary Pool is Down**

If your servers in the primary pool are down, you can redirect users to use the servers in the secondary pool. The following sample rule checks if the pool_production is down and transfers users to pool_sorry_server.

```
acl pool_production_down nbsrv(pool_production) eq 0
use_backend pool_sorry_server if pool_production_down
```

**Whitelist TCP Connection**

You can block client IP addresses from accessing your server. The following sample rule blocks the defined IP address and resets the connection if the client IP address is not in the whitelist.

```
acl whitelist src 10.10.10.0 20.20.20.0
tcp-request connection reject if !whitelist
```

**Enable sslv3 and tlsv1**

By default, sslv3 and tlsv1 are disabled service monitor extensions. You can enable them using the following application rule.

```
sslv3 enable
tlsv1 enable
```

**Configure Client Session Timeout**

Session timeout is the maximum connection inactivity time on the client side. The inactivity timeout applies when the client is expected to acknowledge or send data. In the HTTP mode, this timeout is particularly important to consider during the first phase, when the client sends the request, and during the response while the client is reading the data sent by the server. The default timeout value is five minutes.
The following sample rule sets the timeout period to 100 seconds.

```
timeout client 100s
```

Time can be set as an integer with milliseconds, seconds, minutes, hour, or days.

**Redirect to HTTPS Site**

You can redirects the clients coming on HTTP to the same page on HTTPS.

```
# Redirect all HTTP requests to same URI but HTTPS redirect scheme
https if !{ ssl_fc }
```

Other option is as follows:

```
rspirep ^Location:\ http://(.*) Location:\ https://\1
```

**Redirect Non Authentic Clients**

Redirect the client requests to "/authent.php" if they do not have a cookie.

```
# Check the HTTP request if request is "/authent.php"
acl authent_url url /authent.php
# Check the cookie "cookie1" is present
acl cookie_present hdr_sub(cookie) cookie1=
# If the request is NOT "/authent.php" and there is no cookie, then redirect to "/authent.php"
redirect prefix /authent.php if !authent_url !cookie_present
```

**HTTP Response Header Rewrite**

Replace the response server header "Server" with the value "nginx".

```
# Delete the existing Response Server header "Server"
rspidel Server
# Add the Response Server header "Server" with the value "nginx"
rspadd Server:
```

**Sorry Server**

In case of servers in the primary pool are all dead, use servers in the secondary pool.

```
# detect if pool "pool_production" is still up
acl pool_production_down nbsrv(pool_production) eq 0
# use pool "pool_sorry_server" if "pool_production" is dead
use_backend pool_sorry_server if pool_production_down
# Option 1: # Redirect everything to maintenance site
redirect location http://maintenance.xyz.com/maintenance.htm
# Option 2: #Use a specific maintenance server pool and rewrite all URLs to maintenance.php
acl match_all always_true
use_backend maint_pool if match_all
reqirep ^GET/(.*)\HTTP/(.*) GET\ /maintenance.php\ HTTP/\2
Add Virtual Servers

Add an NSX Edge internal or uplink interface as a virtual server.

**Prerequisites**

- Verify that an application profile is available. See Create an Application Profile.
- If you are associating an application rule with the virtual server, see Create an Application Profile.
- If you are enabling acceleration to use the faster load balancer, the acceleration should be enabled when configuring the load balancer. See Configure Load Balancer Service.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click Manage and then click the Load Balancer tab.
5. In the left navigation panel, click Virtual Servers.
6. Click the Add icon.
7. Check Enable Virtual Server to make this virtual server available for use.
8. (Optional) Check Enable Acceleration for the NSX Edge load balancer to use the faster L4 load balancer engine rather than L7 load balancer engine.

**Note** This configuration requires firewall enabled on the edge.

If a virtual server configuration such as application rules, HTTP type, or cookie persistence, is using the L7 load balancer engine, then the L7 load balancer engine is used even if you enabled acceleration or not. The Acceleration Enabled option must be selected under Global Configuration.

You can use the `show service loadbalancer virtual` CLI command to confirm the load balancer engine in use.

9. Select the application profile to be associated with the virtual server.

You can associate only an application profile with the same protocol as the virtual server that you are adding. The services supported by the selected pool appear.

10. Enter a name and description for the virtual server.

11. Click Select IP Address to set the IP address that the load balancer is listening on and type the protocol that the virtual server will handle.

The Select IP Address dialog box shows only the primary IP address. If you are creating a VIP using a secondary IP address, enter it manually.

12. Select the protocol that the virtual server handles from the drop-down menu.
13 Enter the port number that the load balancer listens on.

You can also set a range of ports for example, 80,8001-8004,443, to share the virtual server configuration such as, server pool, application profile, and application rule.

To use FTP, the TCP protocol must have port 21 assigned to it.

14 Select the application rule.

15 Enter the maximum concurrent connections that the virtual server can process in the Connection Limit section.

16 Enter the maximum incoming new connection requests per second in the Connection Rate Limit section.

17 (Optional) Click the Advanced tab and add the application rule to associate it with the virtual server.

18 Click OK.

Managing Application Profiles

After you create an application profile and associate it with a virtual server, you can update the existing profile or delete it to save system resources.

Edit an Application Profile

You can edit an application profile.

Procedure

1 Log in to the vSphere Web Client.

2 Click Networking & Security and then click NSX Edges.

3 Double-click an NSX Edge.

4 Click the Manage tab and then click the Load Balancer tab.

5 In the left navigation panel, click Application Profiles.

6 Select a profile and click the Edit (✓) icon.

7 Make the appropriate changes to traffic, persistence, certificate, or cipher configuration and click Finish.

Configure SSL Termination for a Load Balancer

Without SSL termination configured, HTTP request are not inspected. The load balancer sees the source and destination IP addresses and encrypted data. If you want to inspect the HTTP requests, you can terminate the SSL session on the load balancer and then create a new SSL session towards the cell pool.
Prerequisites

Go to Manage > Settings > Certificates to ensure that a valid certificate is present. You can upload a certificate for load balancer as follows:

- In PEM format, or
- Generate a CSR, or
- Create a self signed certificate

Procedure

1. In the application profile at Manage > Load Balancer > Application Profiles.
2. Select HTTPS type from the drop-down menu.
3. Verify that Enable SSL Passthrough is not selected.
4. Verify that Configure Service Certificate is selected.
5. Select the appropriate certificate from the list.

Delete an Application Profile

You can delete an application profile.

Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.

3. Double-click an NSX Edge.

4. Click **Manage** and then click the **Load Balancer** tab.

5. In the left navigation panel, click **Application Profiles**.

6. Select a profile and click the **Delete** icon.

**Managing Service Monitors**

A service monitor defines health check parameters for the load balancer.

If using the load balancer service monitor with high availability (HA), HA must be enabled on a dedicated interface.

After you create a service monitor and associate it with a pool, you can update the existing service monitor or delete it to save system resources.

For more information about service monitors, refer to [Create a Service Monitor](#).

**Edit a Service Monitor**

You can edit a service monitor.

**Procedure**

1. Log in to the vSphere Web Client.

2. Click **Networking & Security** and then click **NSX Edges**.

3. Double-click an NSX Edge.

4. Click **Manage** and then click the **Load Balancer** tab.

5. In the left navigation panel, click **Service Monitoring**.

6. Select a service monitor and click the **Edit** icon.

7. Make the appropriate changes and click **OK**.

**Delete a Service Monitor**

You can delete a service monitor.

**Procedure**

1. Log in to the vSphere Web Client.

2. Click **Networking & Security** and then click **NSX Edges**.

3. Double-click an NSX Edge.

4. Click **Manage** and then click the **Load Balancer** tab.

5. In the left navigation panel, click **Service Monitoring**.
Select a service monitor and click the **Delete** icon.

### Managing Server Pools

After you add a server pool to manage load balancer distribution, you can update the existing pool or delete it to save system resources.

### Edit a Server Pool

You can edit a server pool.

#### Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click the **Manage** tab and then click the **Load Balancer** tab.
5. Ensure that you are in the Pool tab.
6. Select the pool to edit.
7. Click the **Edit (📝)** icon.
8. Make the appropriate changes and click **OK**.

### Configure a Load Balancer to Use Transparent Mode

Transparent indicates whether client IP addresses are visible to the backend servers. If Transparent is not selected (default value), backend servers see the traffic source IP as a Load balancer internal IP. If Transparent is selected, source IP is the real client IP and NSX Edge must be on the path of the server response. A typical design is to have the server default gateway be the NSX Edge.

For more information, refer to [Chapter 15 Logical Load Balancer](#).
Procedure

- In the server pool configuration at Manage > Load Balancer > Pools, enable transparent mode.

Delete a Server Pool

You can delete a server pool.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the Load Balancer tab.
5. Ensure that you are in the Pool tab.
6. Select the pool to delete
7. Click the Delete (×) icon.

Show Pool Statistics

You can view the latest health status of pool and associated pool members.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click **Manage** and then click the **Load Balancer** tab.

5. In the left navigation panel, click **Pools**.

6. Select the required pool, and then click the **Show Pool Statistics** link.
   
   Pool status can be UP or DOWN. Pool is marked as DOWN when all the members in the pool are DOWN; otherwise the pool is UP.
   
   Member status would be one of the following:
   
   - **UP**: Member is enabled, and the health status of the member is UP. Or monitor is not defined on the pool.
   - **DOWN**: Member is enabled, and the health status of the member is DOWN.
   - **MAINT**: Member is disabled.
   - **DRAIN**: Member is in drain state.

### Managing Virtual Servers

After you add virtual servers, you can update the existing virtual server configuration or delete it.

#### Edit a Virtual Server

You can edit a virtual server.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4. Click the **Manage** tab and then click the **Load Balancer** tab.
5. Click **Virtual Servers** tab.
6. Select the virtual server to edit.
7. Click the **Edit** (✏️) icon.
8. Make the appropriate changes and click **Finish**.

#### Delete a Virtual Server

You can delete a virtual server.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. Double-click an NSX Edge.
4 Click the **Manage** tab and then click the **Load Balancer** tab.
5 Click **Virtual Servers** tab.
6 Select the virtual server to delete.
7 Click the **Delete** (🔮) icon.

### Managing Application Rules

After you create application rules to configure application traffic, you can edit the existing rule or remove it.

#### Edit an Application Rule

Use the HAProxy syntax to add or edit application rules for manipulating application traffic.

For information about the application rule syntax, see HAProxy documentation at [http://cbonte.github.io/haproxy-dconv/](http://cbonte.github.io/haproxy-dconv/).

For examples of commonly used application rules, see Application Rule Examples.

**Procedure**

1 Log in to the vSphere Web Client.
2 Click **Networking & Security** and then click **NSX Edges**.
3 Double-click an NSX Edge.
4 Click **Manage** and then click the **Load Balancer** tab.
5 In the left navigation panel, click **Application Rules**.
6 Select a rule and click the **Edit** icon.
7 Make the appropriate changes and click **OK**.

#### Delete an Application Rule

You can delete an application rule.

**Procedure**

1 Log in to the vSphere Web Client.
2 Click **Networking & Security** and then click **NSX Edges**.
3 Double-click an NSX Edge.
4 Click **Manage** and then click the **Load Balancer** tab.
5 In the left navigation panel, click **Application Profiles**.
6 Select a profile and click the **Delete** icon.
Load Balance Web Servers using NTLM Authentication

NSX Load Balancer and NTLM authentication require the server connection to be kept alive.

By default, NSX Load Balancer closes the server TCP connection after each client request, however, Windows NT LAN Manager (NTLM) authentication requires the same connection for the lifetime of the authenticated request, connections are kept alive for the duration of the requests.

To keep the server connection open between requests, add the following application rule on the Virtual IP load balancing the Web servers using NTLM authentication:

```
add # NTLM authentication and keep the server connection open between requests
no option http-server-close
```

Load Balancer HTTP Connection Modes

In NSX 6.1.5 and later, when enabling x-forwarded-for, the HTTP connection mode changes from passive close (option httpclose) to the default HTTP server-close (option http-server-close) mode. This keeps the client-facing connection open, while the server-facing connection is closed after receiving a response from the server. Previous to NSX 6.1.5, the NSX Load Balancer did not close the connection proactively, but inserted the "Connection:close" header in both directions to indicate to the client or server to close the connection. If an HTTP/HTTPS transaction fails on NSX Load Balancer after upgrading to NSX 6.1.5 or later, add an application rule with the script option httpclose and associate with the virtual server that is no longer working.

HTTP Server Close (default) - The server-facing connection is closed once the end of the response is received, and the client-facing connection remains open. HTTP Server Close provides latency on the client side (slow network) and the fastest session reuse on the server side to save server resources. It also permits non-keepalive capable servers to be served in keep-alive from a client perspective. This mode is suitable for most common use cases, especially for slow client-facing networks and fast server-facing networks.

HTTP Keep Alive - All requests and responses are processed and connections remain open but idle between responses and new requests. The advantages are reduced latency between transactions, and less processing power required on the server side. Note that memory requirements will increase to accommodate the number of active sessions, which will be higher because connections are no longer closed after each request. The client-facing idle timeout can be configured via application rule “timeout http-keep-alive [time]”. By default the idle timeout is 1 second. This mode is mandatory when an application requires NTLM authentication.

HTTP Tunnel - Only the first request and response are processed and a tunnel is established between the client and the server, allowing them to talk without further analysis of HTTP protocol. Once established, the connection is persistent on both the client and server sides. To enable this mode, none of the following options should be set: passive-close mode, server-close mode, force-close mode.
HTTP tunnel mode impacts the following features, and applies to only the first request and response in a session:

- no logs are generated
- HTTP header parsing
- HTTP header manipulation
- cookie processing
- content switching
- insertion of X-Forwarded-For header

HTTP Passive Close - The same as tunnel mode, but with a "Connection: close" header added in both the client and server directions. Both ends close after the first request and response exchange. If "option httpclose" is set, the NSX Load Balancer works in HTTP tunnel mode and checks if a "Connection: close" header is present in each direction. If the header is not present, a "Connection: close" header is added. Each end then actively closes the TCP connection after each transfer, resulting in a switch to the HTTP close mode. Any connection header other than "close" is removed. Applications that cannot process the second and subsequent requests properly, such as an inserted cookie by the NSX Load Balancer then carried back by the following requests from client, can use tunnel mode or passive close mode.

Some HTTP servers do not necessarily close the connections when they receive the "Connection: close" set by "option httpclose". If the client also does not close, the connection remains open until the timeout expires. This causes a high number of simultaneous connections on the servers, and shows high global session times in the logs. For this reason, they are not compatible with older HTTP 1.0 browsers. If this occurs, use the "option forceclose" which actively closes the request connection once the server responds. Option "forceclose" also releases the server connection earlier because it does not have to wait for the client to acknowledge it.

HTTP Force Close - Both the client and the server connections are actively closed by the NSX Load Balancer after the end of a response. Some HTTP servers do not necessarily close the connections when they receive the "Connection: close" set by "option httpclose". If the client also does not close, the connection remains open until the timeout expires. This causes a high number of simultaneous connections on the servers and shows high global session times in the logs. When this happens, "option forceclose" will actively close the outgoing server channel as soon as the server has finished to respond and release some resources earlier than with "option httpclose".

### NSX Load Balancer Configuration

<table>
<thead>
<tr>
<th>NSX</th>
<th>Default Connection Mode</th>
<th>Connection Mode when X-Forwarded-For enabled</th>
<th>Available Application Rules to switch connection mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.x, 6.1.0, 6.1.1</td>
<td>HTTP Server Close</td>
<td>&quot;option httpclose&quot; is automatically added to the virtual server to force xff to be added to each request as specified in the HAProxy document. xff header is added into each request from the client when dispatching to a backend server.</td>
<td>No</td>
</tr>
<tr>
<td>6.1.2 - 6.1.4</td>
<td>HTTP Server Close</td>
<td>HTTP Passive Close (&quot;option httpclose&quot; is added automatically to virtual server)</td>
<td>&quot;no option http-server-close&quot; &quot;option httpclose&quot; &quot;no option httpclose&quot;</td>
</tr>
<tr>
<td>6.1.5 - 6.1.x 6.2.0 - 6.2.2</td>
<td>HTTP Server Close</td>
<td>HTTP Server Close xff header is added onto each request from the client when dispatching to backend server.</td>
<td>&quot;no option http-server-close&quot; &quot;option httpclose&quot; &quot;no option httpclose&quot;</td>
</tr>
<tr>
<td>6.2.3-6.2.5</td>
<td>HTTP Server Close</td>
<td>HTTP Server Close xff header is added onto each request from the client when dispatching to backend server.</td>
<td>&quot;no option http-server-close&quot; &quot;option httpclose&quot; &quot;no option httpclose&quot;</td>
</tr>
<tr>
<td>6.2.5 - 6.2.x</td>
<td>HTTP Server Close</td>
<td>HTTP Server Close xff header is added onto each request from the client when dispatching to backend server.</td>
<td>&quot;no option http-server-close&quot; &quot;option http-keep-alive&quot; &quot;option http-tunnel&quot; &quot;option httpclose&quot; &quot;option forceclose&quot;</td>
</tr>
</tbody>
</table>

### Scenarios for NSX Load Balancer Configuration

You can use the NSX load balancer configuration scenarios to get an understanding of the required end-to-end workflow.

#### Configure a One-Armed Load Balancer

The Edge Services Gateway (ESG) can be thought of as a proxy for incoming client traffic.
**Easy Insertion**  
Client IP is not detected  
Workaround for HTTP X-Forwarded-For HTTP header

### Phase 1

<table>
<thead>
<tr>
<th>IP</th>
<th>DST</th>
<th>SRC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.1.20</td>
<td>172.30.40.7</td>
</tr>
<tr>
<td>TCP</td>
<td>DST</td>
<td>SRC</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>1025</td>
</tr>
</tbody>
</table>

### Phase 2 (DNAT+SNAT)

<table>
<thead>
<tr>
<th>IP</th>
<th>DST</th>
<th>SRC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.1.3</td>
<td>192.168.1.20</td>
</tr>
<tr>
<td>TCP</td>
<td>DST</td>
<td>SRC</td>
</tr>
<tr>
<td></td>
<td>80</td>
<td>4099</td>
</tr>
</tbody>
</table>

### Phase 3

<table>
<thead>
<tr>
<th>IP</th>
<th>DST</th>
<th>SRC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.1.20</td>
<td>192.168.1.3</td>
</tr>
<tr>
<td>TCP</td>
<td>DST</td>
<td>SRC</td>
</tr>
<tr>
<td></td>
<td>4099</td>
<td>80</td>
</tr>
</tbody>
</table>

### Phase 4

<table>
<thead>
<tr>
<th>IP</th>
<th>DST</th>
<th>SRC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>172.30.40.7</td>
<td>192.168.1.20</td>
</tr>
<tr>
<td>TCP</td>
<td>DST</td>
<td>SRC</td>
</tr>
<tr>
<td></td>
<td>1025</td>
<td>80</td>
</tr>
</tbody>
</table>

**Client Address** 172.30.40.7

**NSX Edge Services Gateway**

**SLB**

VIP 192.168.1.3 (Selected)

192.168.1.20 TCP 80

192.168.1.2

192.168.1.1

VM

VM

VM
In proxy mode, the load balancer uses its own IP address as the source address to send requests to a backend server. The backend server views all traffic as being sent from the load balancer and responds to the load balancer directly. This mode is also called SNAT mode or non-transparent mode. For more information, refer to NSX Administration Guide.

A typical NSX one-armed load balancer is deployed on the same subnet with its backend servers, apart from the logical router. The NSX load balancer virtual server listens on a virtual IP for incoming requests from client and dispatches the requests to backend servers. For the return traffic, reverse NAT is required to change the source IP address from the backend server to a virtual IP (VIP) address and then send the virtual IP address to the client. Without this operation, the connection to the client would break.

After the ESG receives the traffic, it performs two operations: Destination Network Address Translation (DNAT) to change the VIP address to the IP address of one of the load balanced machines, and Source Network Address Translation (SNAT) to exchange the client IP address with the ESG IP address.

Then the ESG server sends the traffic to the load balanced server and the load balanced server sends the response back to the ESG then back to the client. This option is much easier to configure than the Inline mode, but has two potentials caveats. The first is that this mode requires a dedicated ESG server, and the second is that the load balancer servers are not aware of the original client IP address. One workaround for HTTP/HTTPS applications is to enable Insert X-Forwarded-For in the HTTP application profile so that the client IP address will be carried in the X-Forwarded-For HTTP header in the request sent to the backend server.

If client IP address visibility is required on the backend server for applications other than HTTP/HTTPS, you can configure the IP pool to be transparent. In case clients are not on the same subnet as the backend server, inline mode is recommended. Otherwise, you must use the load balancer IP address as the default gateway of the backend server.

**Note** Usually, there are three methods to guarantee connection integrity:

- Inline/transparent mode
- SNAT/proxy/non-transparent mode (discussed above)
- Direct server return (DSR) - Currently, this is unsupported

In DSR mode, the backend server responds directly to the client. Currently, NSX load balancer does not support DSR.

**Procedure**

1. As an example, lets configure a one-armed virtual server with SSL offload. Create a certificate by double-clicking the Edge and then selecting Manage > Settings > Certificate.
2 Enable the load balancer service by selecting Manage > Load Balancer > Global Configuration > Edit.

![Edit Load balancer global configuration](image)

3 Create an HTTPS application profile by selecting Manage > Load Balancer > Application Profiles.

![New Profile](image)

**Note** The screenshot above uses self-signed certificates for documentation-purposes only.

4 Optionally, click Manage > Load Balancer > Service Monitoring and edit the default service monitoring to change it from basic HTTP/HTTPS to specific URL/URIs, as required.

5 Create server pools by selecting Manage > Load Balancer > Pools.

To use SNAT mode, leave the Transparent check box unchecked in the pool configuration.
Ensure that the VMs are listed and enabled.

6 Optionally, click Manage > Load Balancer > Pools > Show Pool Statistics to check the status. Make sure that the member status is UP.

7 Create a virtual server by selecting Manage > Load Balancer > Virtual Servers.

If you would like to use the L4 load balancer for UDP or higher-performance TCP, check Enable Acceleration. If you check Enable Acceleration, make sure that the firewall status is Enabled on the load balancer NSX Edge, because a firewall is required for L4 SNAT.

Ensure that the IP address is tied to the server pool.
8 Optionally, if using an application rule, check the configuration in Manage > Load Balancer > Application Rules.

![Add Application Rule](image)

9 If using an application rule, ensure that the application rule is associated with the virtual server in Manage > Load Balancer > Virtual Servers > Advanced.

For supported examples, see: [https://communities.vmware.com/docs/DOC-31772](https://communities.vmware.com/docs/DOC-31772).

![Edit Virtual Server](image)

In non-transparent mode, the backend server cannot see the client IP, but can see the load balancer internal IP address. As a workaround for HTTP/HTTPS traffic, check **Insert X-Forwarded-For HTTP header**. With this option checked, the Edge load balancer adds the header "X-Forwarded-For" with the value of the client source IP address.

![Edit Profile](image)

**Scenario: Configure NSX Load Balancer for Platform Service Controller**

Platform Services Controller (PSC) provides infrastructure security functions such as vCenter Single Sign-On, licensing, certificate management and server reservation.

After you configure the NSX load balancer, you can provide the NSX Edge device uplink interface IP address for vCenter Single Sign-On.
Prerequisites

- Save the /ha/lb.crt and /ha/lb_rsa.key from first PSC node to configure certificates.
- Verify that an NSX Edge device is configured.
- Verify that you have at least one uplink for configuring VIP and one interface attached to internal logical switch.

Procedure

1. Add PSC CA certificates to the NSX Edge.
   a. Save the PSC root.cer and certificate, RSA and passphrase generated from the OpenSSL command.
   b. Double-click the Edge and select Manage > Settings > Certificate.
   c. Add the saved content root.cer file to the CA certificate contents.
   d. Add the saved passphrase to the private key section.

2. Enable the load balancer service.
   a. Select Manage > Load Balancer > Edit.
   b. Check the Enable Load Balancing and Logging options.
3. Create application profiles with TCP and HTTPS protocols.
   
a. Select Manage > Load Balancer > Application Profiles.

b. Create a TCP application profile.

c. Create an HTTPS application profile.
4 Create application pools to add member PSC nodes.
   
   a Select Manage > Load Balancer > Pools.

   b Create two application pools with monitor port 443.

   Use the PSC node IP address.

   ![Application Pool Configuration](image1)

   c Create two application pools with monitor port 389.

   Use the PSC node IP address.

   ![Application Pool Configuration](image2)
5 Create virtual servers for the TCP and HTTPS protocols.
   a Select Manage > Load Balancer > Virtual Servers.
   b Create a virtual server for TCP VIP.

   ![TCP Virtual Server]

   c Create a virtual server for HTTPS VIP.

   ![HTTPS Virtual Server]

**Scenario: SSL Offloading**

Edge terminates client HTTPS (SSL sessions). Edge load balances the clients on HTTP to the servers. L7 application rules can be applied.
Procedure

1. Import the Web server certificate.
   a. Log in to the vSphere Web Client.
   b. Click **Networking & Security** and then click **NSX Edges**.
   c. Double-click an NSX Edge.
   d. Click **Manage**, and then click the **Settings** tab.
   e. In the left navigation panel, click **Certificates**.
   f. Click the **Add** (➕) icon, and select **Certificate**. For more details, refer to **Working with Certificates**.
g Copy and paste the certificate contents in the **Certificate Contents** text box. Text should include "-----BEGIN xxx-----" and "-----END xxx-----".

For chained certificates (server certificate and an intermediate or root CA certificate), select the **Certificate** option. Following is example of a chained certificate content:

```
-----BEGIN CERTIFICATE-----
Server cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root cert
-----END CERTIFICATE-----
```

h Copy and paste the private key contents in the **Private Key** text box.

Following is example of the private key content:

```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END RSA PRIVATE KEY-----
```

The certificate content (PEM for certificate or private key) should be prefixed with one of the following strings:

```
-----BEGIN PUBLIC KEY-----
-----BEGIN RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE REQUEST-----
-----BEGIN NEW CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
-----BEGIN PKCS7-----
-----BEGIN X509 CERTIFICATE-----
-----BEGIN X509 CRL-----
-----BEGIN ATTRIBUTE CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN DSA PRIVATE KEY-----
-----BEGIN EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
```

For complete examples of certificate and private key, refer to the [Example: Certificate and Private Key](#) topic.

**Note** The following prefix is not supported in NSX Manager:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```
2. Create the HTTPS application profile.
   a. Log in to the vSphere Web Client.
   b. Click **Networking & Security** and then click **NSX Edges**.
   c. Double-click an NSX Edge.
   d. Click **Manage**, and then click the **Load Balancer** tab.
   e. In the left navigation panel, click **Application Profile**. For more details, refer to Managing Application Profiles.
   f. Create a new application profile with the following parameters:
      - Select Type as **HTTPS** from the list.
      - Select the **Configure Service Certificates** check box.
      - Select the service certificate configured in step 1.

3. Create a virtual server.
   a. Log in to the vSphere Web Client.
   b. Click **Networking & Security** and then click **NSX Edges**.
   c. Double-click an NSX Edge.
   d. Click **Manage**, and then click the **Load Balancer** tab.
   e. In the left navigation panel, click **Virtual Servers**. For more details, refer to Managing Virtual Servers.
   f. Create a new virtual server with the following parameters:
      - Select the **Enable Virtual Server** check box to make the virtual server available for use.
      - Select Protocol as **HTTPS**.
      - Select the default pool that is composed of HTTP servers (not HTTPS servers).
      - Select the application profile configured in step 2.

Example: Certificate and Private Key

Following are the examples of certificates and private key.

**Web Server Certificate**

```
-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjET
MBEGA1UECAwKU29tZS1TdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERp
bWwvczAJBgNVBAYTAkZSMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJ
bnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxFDASBgNVBAMMC3d3dy5kaW1pLmZyMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvpnaPKLIKdvx98Kw681z8pGo
RRCyrsNGqPjptfMVjjeBLuCoXgPU8HePnPNTUpShBrynKCvrtWhNhokvKbSp+QwX
-----END CERTIFICATE-----
```
Web Server Certificate with Chain (Including Root CA)

BEGIN CERTIFICATE

MIID0DCArigAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjETMBEAGA1UECAwKU29tZS1TdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERp

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIDyTCCArGgAwIBAgIBADANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjETMBEAGA1UECAwKU29tZS1TdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERp

-----END CERTIFICATE-----

VMware, Inc. 293

NSX Administration Guide
Scenario: Import SSL Certificate

SSL end-to-end: The NSX Edge terminates client HTTPS (SSL sessions). Edge load balances the client on new HTTPS connection to the servers. L7 application rules can be applied.

Procedure

1 Import the Web server certificate.
   a Log in to the vSphere Web Client.
   b Click Networking & Security and then click NSX Edges.
   c Double-click an NSX Edge.
d  Click **Manage**, and then click the **Settings** tab.

e  In the left navigation panel, click **Certificates**.

f  Click the **Add (➕)** icon, and select **Certificate**. For more details, refer to **Working with Certificates**.
g Copy and paste the certificate contents in the **Certificate Contents** text box. Text should include "-----BEGIN xxx-----" and "-----END xxx-----".

For chained certificates (server certificate and an intermediate or root CA certificate), select the **Certificate** option. Following is example of a chained certificate content:

```
-----BEGIN CERTIFICATE-----
Server cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root cert
-----END CERTIFICATE-----
```

h Copy and paste the private key contents in the **Private Key** text box.

Following is example of the private key content:

```
-----BEGIN RSA PRIVATE KEY-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
-----END RSA PRIVATE KEY-----
```

The certificate content (PEM for certificate or private key) should be prefixed with one of the following strings:

```
-----BEGIN PUBLIC KEY-----
-----BEGIN RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE REQUEST-----
-----BEGIN NEW CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
-----BEGIN PKCS7-----
-----BEGIN X509 CERTIFICATE-----
-----BEGIN X509 CRL-----
-----BEGIN ATTRIBUTE CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN DSA PRIVATE KEY-----
-----BEGIN EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
```

For complete examples of certificate and private key, refer to the [Example: Certificate and Private Key](#) topic.

**Note**  The following prefix is not supported in NSX Manager:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```
2 Create the HTTPS application profile.
   a Log in to the vSphere Web Client.
   b Click Networking & Security and then click NSX Edges.
   c Double-click an NSX Edge.
   d Click Manage, and then click the Load Balancer tab.
   e In the left navigation panel, click Application Profile. For more details, refer to Managing Application Profiles.
   f Create a new application profile with the following parameters:
      ■ Select Type as HTTPS from the list.
      ■ Select the Enable Pool Side SSL check box.
      ■ Select the Configure Service Certificates check box.
      ■ Select the service certificate configured in step 1.

3 Create a virtual server.
   a Log in to the vSphere Web Client.
   b Click Networking & Security and then click NSX Edges.
   c Double-click an NSX Edge.
   d Click Manage, and then click the Load Balancer tab.
   e In the left navigation panel, click Virtual Servers. For more details, refer to Managing Virtual Servers.
   f Create a new virtual server with the following parameters:
      ■ Select the Enable Virtual Server check box to make the virtual server available for use.
      ■ Select Protocol as HTTPS.
      ■ Select the default pool that is composed of HTTPS servers.
      ■ Select the application profile configured in step 2.

Scenario: SSL Passthrough
Edge do not terminate clients HTTPS (SSL sessions). Edge load balances TCP sessions to the servers. Client SSL sessions are terminated to the servers (not the edge). L7 application rules can not be applied.

Prerequisites

Note Certificates are not required for the HTTPS passthrough scenario.
Procedure

1. Create the HTTPS application profile.
   a. Log in to the vSphere Web Client.
   b. Click Networking & Security and then click NSX Edges.
   c. Double-click an NSX Edge.
   d. Click Manage, and then click the Load Balancer tab.
   e. In the left navigation panel, click Application Profile. For more details, refer to Managing Application Profiles.
   f. Create a new application profile with the following parameters:
      - Select Type as HTTPS from the list.
      - Select the Enable SSL Passthrough check box.
      - Select the Persistence as None.

   Note: Certificates are not required for the HTTPS passthrough scenario.

2. Create a virtual server.
   a. Log in to the vSphere Web Client.
   b. Click Networking & Security and then click NSX Edges.
   c. Double-click an NSX Edge.
   d. Click Manage, and then click the Load Balancer tab.
   e. In the left navigation panel, click Virtual Servers. For more details, refer to Managing Virtual Servers.
   f. Create a new virtual server with the following parameters:
      - Select the Enable Virtual Server check box to make the virtual server available for use.
      - Select Protocol as HTTPS.
      - Select the default pool that is composed of HTTPS servers.
      - Select the application profile configured in step 1.

   Note: If Enable Acceleration check box is selected and there are no L7 related configurations, the session would NOT be terminated by the edge. If Enable Acceleration check box is not selected, the session would be treated as L7 TCP mode, and edge will terminate it into two sessions.

Scenario: SSL Client and Server Authentication

SSL client and server authentication.
Client Authentication

Clients access the Web application through HTTPS. HTTPS is terminated on the edge VIP and requests for client certificate.

1. Import the Web server certificate along with root CA. For details, refer to Scenario: Import SSL Certificate.

2. Create the HTTPS application profile with the following parameters:
   a. Select Type as HTTPS from the list.
   b. Select the Virtual Server Certificates tab, and then select CA Certificates tab. CA is used to verify client certificate.
   c. Select the service certificate configured in step 1.
   d. Select Client Authentication as Required from the list.

   **Note** If the Client Authentication option is set to Ignore, load balancer ignores the client certificate authentication.

3. Create a virtual server. For details, refer to Scenario: Import SSL Certificate.

   **Note** If the Enable Pool Side SSL option is disabled in the application profile, the pool selected is composed of HTTP servers. If the Enable Pool Side SSL option is enabled in the application profile, the pool selected is composed of HTTPS servers.

4. Import a client certificate signed by the root CA in the browser.

   b. Convert certificate and private key to the .pfx file. For complete examples of certificate and private key, refer to the Example: Certificate and Private Key topic.
   c. Import the .pfx file in the browser.

Server Authentication

Clients access the Web application through HTTPS. HTTPS is terminated on the edge VIP. The edge establish new HTTPS connections to the servers, it requests and verifies server certificate.
Only specific ciphers are accepted by the edge.

1. Import the Web server certificate and root CA certificate for server certificate authentication. For details, refer to Scenario: Import SSL Certificate.

2. Create the HTTPS application profile with the following parameters:
   a. Select Type as HTTPS from the list.
   b. Select the Enable Pool Side SSL check box.
   c. Select the Pool Certificates tab, and then select CA Certificates tab. CA is used to verify client certificate from backend HTTPS server.
   d. Select the Server Authentication check box.
   e. Select the CA certificate configured in step 1.
   f. Select the required cipher from the Ciphers list.

   **Note**  If cipher is not in approved ciphers suite, it resets to Default.

   After upgrading from old version, if cipher is null/empty or not in approved ciphers suite in the old version, it resets to Default.

3. Create a virtual server. For details, refer to Scenario: Import SSL Certificate.

   **Note**  If the Enable Pool Side SSL option is disabled in the application profile, the pool selected is composed of HTTP servers. If the Enable Pool Side SSL option is enabled in the application profile, the pool selected is composed of HTTPS servers.
Other Edge Services

An NSX services gateway offers IP address pooling and one-to-one static IP address allocation and external DNS server configuration.

You must have a working NSX Edge instance before you can use any of the above services. For information on setting up NSX Edge, see NSX Edge Configuration.

This chapter includes the following topics:

- Managing DHCP Service
- Configuring DHCP Relay
- Configure a DNS Server

Managing DHCP Service

NSX Edge supports IP address pooling and one-to-one static IP address allocation. Static IP address binding is based on the vCenter managed object ID and interface ID of the requesting client.

NSX Edge DHCP service adheres to the following guidelines:

- Listens on the NSX Edge internal interface for DHCP discovery.
- Uses the IP address of the internal interface on NSX Edge as the default gateway address for all clients (except for non-directly connected pools), and the broadcast and subnet mask values of the internal interface for the container network.

You must restart the DHCP service on client virtual machines in the following situations:

- You changed or deleted a DHCP pool, default gateway, or DNS server.
- You changed the internal IP address of the NSX Edge instance.

Add a DHCP IP Pool

DHCP service requires a pool of IP addresses.

An IP pool is a sequential range of IP addresses within the network. Virtual machines protected by NSX Edge that do not have an address binding are allocated an IP address from this pool. An IP pool's range cannot intersect one another, thus one IP address can belong to only one IP pool.
Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click DHCP.
5. Click the Add (➕) icon.
6. On the General tab, configure the pool.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Configure DNS</td>
<td>Select to use the DNS service configuration for the DHCP binding.</td>
</tr>
<tr>
<td>Lease never expires</td>
<td>Select to bind the address to the MAC address of the virtual machine forever. If you select this, Lease Time is disabled.</td>
</tr>
<tr>
<td>Start IP</td>
<td>Enter the starting IP address for the pool.</td>
</tr>
<tr>
<td>End IP</td>
<td>Enter the ending IP address for the pool.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the domain name of the DNS server. This is optional.</td>
</tr>
<tr>
<td>Primary Name Server</td>
<td>If you did not select Auto Configure DNS, type the Primary Nameserver for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution. This is optional.</td>
</tr>
<tr>
<td>Secondary Name Server</td>
<td>If you did not select Auto Configure DNS, type the Secondary Nameserver for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution. This is optional.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the default gateway address. If you do not specify the default gateway IP address, the internal interface of the NSX Edge instance is taken as the default gateway. This is optional.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify the subnet mask. The subnet mask must be same as the subnet mask of the Edge interface or the DHCP Relay, in case of distributed router.</td>
</tr>
<tr>
<td>Lease Time</td>
<td>Select whether to lease the address to the client for the default time (1 day), or enter a value in seconds. You cannot specify the lease time if you selected Lease never expires. This is optional.</td>
</tr>
</tbody>
</table>

7. (Optional) On the DHCP Options tab, configure DHCP options.

In NSX 6.2.5 and later, if a DHCP pool is configured on an Edge Services Gateway with both classless static routes and a default gateway, the default gateway is added as a classless static route.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Server</td>
<td>Next boot TFTP server, used by the PXE boot or bootp.</td>
</tr>
<tr>
<td>TFTP server name (option 66)</td>
<td>Enter a unicast IPv4 address or a host name that the device should use to download the file specified in bootfile name (option 67).</td>
</tr>
<tr>
<td>TFTP server address (option 150)</td>
<td>Enter one or more TFTP server IPv4 addresses.</td>
</tr>
<tr>
<td>Bootfile name (option 67)</td>
<td>Enter the bootfile file name that is to be downloaded from the server specified in TFTP server name (option 66).</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interface MTU (option 26)</td>
<td>The Maximum Transmission Unit (MTU) is the maximum frame size that can be sent between two hosts without fragmentation. This option specifies the MTU size to be used on the interface. One MTU size (in bytes) can be set for each pool and static binding. The MTU minimum value is 68 bytes and the maximum value is 65535 bytes. If the interface MTU is not set on the DHCP server, DHCP clients will keep the OS default setting of the interface MTU.</td>
</tr>
</tbody>
</table>
| Classless static route (option 121) | Each classless static route option may have multiple routes with the same destination. Each route includes a destination subnet, subnet mask, next hop router. Note that 0.0.0.0/0 is an invalid subnet for a static route. For information about classless static routes and option 121, refer to RFC 3442.  
  a) Click the Add (.addButton) icon.  
  b) Enter the destination and the next hop router IP address. |

8 Click OK.

Enable the DHCP Service

Enable the DHCP service to allow NSX Edge to automatically assign an IP address to a virtual machine from a defined IP pool.

Prerequisites

A DHCP IP pool must have been added.

Procedure

1 Log in to the vSphere Web Client.
2 Click Networking & Security and then click NSX Edges.
3 Double-click an NSX Edge.
4 Click the Manage tab and then click the DHCP tab.
5 Click Enable.
6 Select Enable logging if required and select the log level.
7 Click Publish Changes.

Results

Note VMware strongly recommends creating a firewall rule to prevent malicious users from introducing rogue DHCP servers. To do this, add a firewall rule that allows UDP traffic only on ports 67 and 68 when the traffic is going to or from a valid DHCP server IP address. For details, refer to Working with Firewall Rules.

What to do next

Create an IP pool and bindings.
Edit DHCP IP Pool

You can edit the DHCP IP pool to add or remove IP addresses.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the DHCP tab.
5. Select a DHCP pool and click the Edit icon.
6. Make the appropriate changes and click OK.

Add a DHCP Static Binding

If you have services running on a virtual machine and do not want the IP address to be changed, you can bind an IP address to the MAC address of a virtual machine. The IP address you bind must not overlap an IP pool.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Edges.
3. Double-click an NSX Edge.
4. Click the Manage tab and then click the DHCP tab.
5. SelectBindings from the left panel.
6. Click the Add icon.
7. Configure the binding.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto Configure DNS</td>
<td>Select to use the DNS service configuration for the DHCP binding.</td>
</tr>
<tr>
<td>Lease never expires</td>
<td>Select to bind the address to the MAC address of the virtual machine forever.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the NSX Edge interface to bind.</td>
</tr>
<tr>
<td>VM Name</td>
<td>Select the virtual machine to bind.</td>
</tr>
<tr>
<td>VM vNic Index</td>
<td>Select the virtual machine NIC to bind to the IP address.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Type the host name of the DHCP client virtual machine.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Type the address to which to bind the MAC address of the selected virtual machine.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Specify the subnet mask. The subnet mask should be same as the subnet mask of the Edge interface or the DHCP Relay, in case of distributed router.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Type the domain name of the DNS server.</td>
</tr>
<tr>
<td>Option</td>
<td>Action</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Primary Name Server</td>
<td>If you did not select Auto Configure DNS, type the Primary Nameserver for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.</td>
</tr>
<tr>
<td>Secondary Name Server</td>
<td>If you did not select Auto Configure DNS, type the Secondary Nameserver for the DNS service. You must enter the IP address of a DNS server for hostname-to-IP address resolution.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Type the default gateway address. If you do not specify the default gateway IP address, the internal interface of the NSX Edge instance is taken as the default gateway.</td>
</tr>
<tr>
<td>Lease Time</td>
<td>If you did not select Lease never expires, select whether to lease the address to the client for the default time (1 day), or type a value in seconds.</td>
</tr>
</tbody>
</table>

8 Click Add.

9 Click Publish Changes.

### Edit DHCP Binding

You assign a different static IP address that is bound to a MAC address of a virtual machine.

**Procedure**

1 Log in to the vSphere Web Client.

2 Click Networking & Security and then click NSX Edges.

3 Double-click an NSX Edge.

4 Click the Manage tab and then click the DHCP tab.

5 Select Bindings from the left panel and click the binding to edit.

6 Click the Edit icon.

7 Make the appropriate changes and click OK.

### Configuring DHCP Relay

Dynamic Host Configuration Protocol (DHCP) relay enables you to leverage your existing DHCP infrastructure from within NSX without any interruption to the IP address management in your environment. DHCP messages are relayed from virtual machine(s) to the designated DHCP server(s) in the physical world. This enables IP addresses within NSX to continue to be in synch with IP addresses in other environments.

DHCP configuration is applied on the logical router port and can list several DHCP servers. Requests are sent to all listed servers. While relaying the DHCP request from the client, the relay adds a Gateway IP Address to the request. The external DHCP server uses this gateway address to match a pool and allocate an IP address for the request. The gateway address must belong to a subnet of the NSX port on which the relay is running.
You can specify a different DHCP server for each logical switch and can configure multiple DHCP servers on each logical router to provide support for multiple IP domains.

**Note** If the DHCP Offer contains an IP address that doesn't match a logical interface (LIF), the DLR does not relay it back to the VM. The packet is dropped.

When configuring pool and binding at DHCP server, ensure that the subnet mask of the pool/binding for the relayed queries is same as the interface of the DHCP relay. Subnet mask information must be provided in API while DLR is acting as DHCP relay between VMs and Edge providing DHCP service. This subnet mask should match the one configured on gateway interface for VMs on DLR.

**Note**
- DHCP relay does not support overlapping IP address space (option 82).
- DHCP Relay and DHCP service cannot run on a port/vNic at the same time. If a relay agent is configured on a port, a DHCP pool cannot be configured on the subnet(s) of this port.

**Add DHCP Relay Server**

Add the external relay server(s) to which you want the DHCP messages to be relayed to. The relay server can be an IP set, IP address block, domain, or a combination of all of these. Messages are relayed to each listed DHCP server.
Prerequisites

- DHCP relay does not support overlapping IP address space (option 82).
- DHCP Relay and DHCP service cannot run on a port/vNic at the same time. If a relay agent is configured on a port, a DHCP pool cannot be configured on the subnet(s) of this port.
- If the DHCP Offer contains an IP address that doesn't match a logical interface (LIF), the DLR does not relay it back to the VM. The packet is dropped.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > NSX Edges.
2. Double-click the appropriate Edge and ensure that you are in the Manage > DHCP tab.
3. Click Edit next to DHCP Relay Global Configuration.
4. To add an IP set as a server:
   a. Click the Add icon and select the IP set.
   b. Move the selected IP set to the Selected Objects list by clicking the icon.
   c. Click OK.
5. To add IP addresses or domain names, type the address or name in the appropriate area.
6. Click OK.

Add Relay Agents

Add the Edge interfaces from which DHCP messages are to be relayed to the external DHCP relay server(s).

Procedure

1. In the DHCP Relay Agents area, click the Add icon.
2. In vNIC, ensure that an internal vNIC is selected.
   The Gateway IP Address displays the primary IP address of the selected vNic.
3. Click OK.

Configure a DNS Server

You can configure external DNS servers on an NSX Edge. The edge forwards DNS requests from client applications to the DNS servers to resolve a network name. The edge can also cache the response that it receives from the DNS servers. DNS service is supported on an Edge Services Gateway, DLR, and UDLR in a Cross-vCenter NSX environment.

Procedure

1. Log in to the vSphere Web Client.
2 Click **Networking & Security** and then click **NSX Edges**.

3 Double-click a NSX Edge.

4 Click the **Manage** tab and then click the **Settings** tab.

5 In the **DNS Configuration** panel, click **Change**.

6 Click **Enable DNS Service** to enable the DNS service.

7 Type IP addresses for both DNS servers.

8 Change the default cache size if necessary.

9 Click **Enable Logging** to log DNS traffic and select the log level.

   Generated logs are sent to the syslog server.

10 Click **Ok**.
Service Composer

Service Composer helps you provision and assign network and security services to applications in a virtual infrastructure. You map these services to a security group, and the services are applied to the virtual machines in the security group.

Security Group

You begin by creating a security group to define assets that you want to protect. Security groups may be static (including specific virtual machines) or dynamic where membership may be defined in one or more of the following ways:

- vCenter containers (clusters, port groups, or datacenters)
- Security tags, IPset, MACset, or even other security groups. For example, you may include a criteria to add all members tagged with the specified security tag (such as AntiVirus.virusFound) to the security group.
- Directory Groups (if NSX Manager is registered with Active Directory)
- Regular expressions such as virtual machines with name VM1

Note that security group membership changes constantly. For example, a virtual machine tagged with the AntiVirus.virusFound tag is moved into the Quarantine security group. When the virus is cleaned and this tag is removed from the virtual machine, it again moves out of the Quarantine security group.

Security Policy

A security policy is a collection of the following service configurations.

**Table 17-1. Security services contained in a security policy**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall rules</td>
<td>Rules that define the traffic to be allowed to, from, or within the security group.</td>
<td>vNIC</td>
</tr>
<tr>
<td>Endpoint service</td>
<td>Third party solution provider services such as anti-virus or vulnerability management services.</td>
<td>virtual machines</td>
</tr>
<tr>
<td>Network introspection services</td>
<td>Services that monitor your network such as IPS.</td>
<td>virtual machines</td>
</tr>
</tbody>
</table>

During service deployment in NSX, the third party vendor selects the service category for the service being deployed. A default service profile is created for each vendor template.
When third party vendor services are upgraded to NSX 6.1, default service profiles are created for the vendor templates being upgraded. Existing service policies that include Guest Introspection rules are updated to refer to the service profiles created during the upgrade.

Mapping Security Policy to Security Group

You map a security policy (say SP1) to a security group (say SG1). The services configured for SP1 are applied to all virtual machines that are members of SG1.

**Note** When you have many security groups to which you need to attach the same security policy, create an umbrella security group that includes all these child security groups, and apply the common security policy to the umbrella security group. This will ensure that the NSX distributed firewall utilises ESXi host memory efficiently.

Figure 17-1. Service Composer overview

If a virtual machine belongs to more than one security group, the services that are applied to the virtual machine depends on the precedence of the security policy mapped to the security groups.

Service Composer profiles can be exported and imported as backups or for use in other environments. This approach to managing network and security services helps you with actionable and repeatable security policy management.

This chapter includes the following topics:

- Using Service Composer
- Service Composer Canvas
- Working with Security Tags
- Viewing Effective Services
- Working with Security Policies
- Service Composer Scenarios
- Importing and Exporting Security Policy Configurations
Using Service Composer

Service Composer helps you consume security services with ease.

Let us walk through an example to show how Service Composer helps you protect your network end-to-end. Let us say you have the followings security policies defined in your environment:

- An initial state security policy that includes a vulnerability scanning service (InitStatePolicy)
- A remediation security policy that includes a network IPS service in addition to firewall rules and an anti-virus service (RemPolicy)

Ensure that the RemPolicy has higher weight (precedence) than InitStatePolicy.

You also have the followings security groups in place:

- An applications assets group that includes the business critical applications in your environment (AssetGroup)
- A remediation security group defined by a tag that indicates the virtual machine is vulnerable (VULNERABILITY_MGMT.VulnerabilityFound.threat=medium) named RemGroup

You now map the InitStatePolicy to AssetGroup to protect all business critical applications in your environment. You also map RemPolicy to RemGroup to protect vulnerable virtual machines.

When you initiate a vulnerability scan, all virtual machines in AssetGroup are scanned. If the scan identifies a virtual machine with a vulnerability, it applies the VULNERABILITY_MGMT.VulnerabilityFound.threat=medium tag to the virtual machine.

Service Composer instantly adds this tagged virtual machine to RemGroup, where a network IPS solution is already in place to protect this vulnerable virtual machine.
This topic will now take you through the steps required to consume the security services offered by Service Composer.

**Procedure**

1. **Create a Security Group in Service Composer**
   You create a security group at the NSX Manager level.

2. **Create a Security Policy**
   A security policy is a set of Guest Introspection, firewall, and network introspection services that can be applied to a security group. The order in which security policies are displayed is determined by the weight associated with the policy. By default, a new policy is assigned the highest weight so that it is at the top of the table. However, you can modify the default suggested weight to change the order assigned to the new policy.

3. **Apply a Security Policy to a Security Group**
   You can apply a security policy to a security group to secure your virtual desktops, business critical applications, and the connections between them. You can also view a list of the services that were not applied and the reason they failed to apply.

**Create a Security Group in Service Composer**

You create a security group at the NSX Manager level.

**Procedure**
Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **Service Composer**.
3. Click the **Security Groups** tab and then click the **Add Security Group** icon.
4. Type a name and description for the security group and click **Next**.
5. On the Dynamic Membership page, define the criteria that an object must meet for it to be added to the security group you are creating.
   
   For example, you may include a criteria to add all members tagged with the specified security tag (such as `AntiVirus.virusFound`) to the security group.

   Or you can add all virtual machines containing the name `W2008` AND virtual machines that are in the logical switch `global_wire` to the security group.

   Security tags are case sensitive.

   **Note** If you define a security group by virtual machines that have a certain security tag applied to them, you can create a dynamic or conditional workflow. The moment the tag is applied to a virtual machine, the virtual machine is automatically added to that security group.

6. Click **Next**.
7. On the Select objects to include page, select the object type from the drop-down.
8. Double-click the object you want to add to the include list. You can include the following objects in a security group.
   - Other security groups to nest within the security group you are creating.
   - Cluster
   - Logical switch
   - Network
   - Virtual App
   - Datacenter
   - IP sets
   - AD groups

   **Note** The AD configuration for NSX security groups is different from the AD configuration for vSphere SSO. NSX AD group configuration is for end users accessing guest virtual machines while vSphere SSO is for administrators using vSphere and NSX.
MAC Sets

**Note** Service Composer allows use of Security Groups that contain MAC Sets in Policy configurations, however, Service Composer fails to enforce rules for that specific MAC Set. Service Composer works on Layer 3 and does not support Layer 2 constructs.

- Security tag
- vNIC
- Virtual Machine
- Resource Pool
- Distributed Virtual Port Group

The objects selected here are always included in the security group regardless of whether or not they match the dynamic criteria.

When you add a resource to a security group, all associated resources are automatically added. For example, when you select a virtual machine, the associated vNIC is automatically added to the security group.

9 Click **Next** and double-click the objects that you want to exclude from the security group.

The objects selected here are always excluded from the security group even if they match the dynamic criteria or are selected in the include list.

10 Click **Finish**.

**Example**

Membership of a security group is determined as follows:

\[
\{\text{Expression result (derived from Step step 4)} + \text{Inclusions (specified in Step step 7)} \} - \text{Exclusion (specified in Step step 8)}
\]

which means that inclusion items are first added to the expression result. Exclusion items are then subtracted from the combined result.

**Create a Security Policy**

A security policy is a set of Guest Introspection, firewall, and network introspection services that can be applied to a security group. The order in which security policies are displayed is determined by the weight associated with the policy. By default, a new policy is assigned the highest weight so that it is at the top of the table. However, you can modify the default suggested weight to change the order assigned to the new policy.

**Prerequisites**

Ensure that:

- the required VMware built in services (such as Distributed Firewall, and Guest Introspection) are installed.
the required partner services have been registered with NSX Manager.

the desired default applied to value is set for Service Composer firewall rules. See Edit Service Composer Firewall Applied To Setting.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Service Composer.
3. Click the Security Policies tab.
4. Click the Create Security Policy icon.
5. In the Add Security Policy dialog box, type a name for the security policy.
6. Type a description for the security policy.

   NSX assigns a default weight (highest weight +1000) to the policy. For example, if the highest weight amongst the existing policy is 1200, the new policy is assigned a weight of 2200.

   Security policies are applied according to their weight - a policy with the higher weight has precedence over a policy with a lower weight.

7. Select Inherit security policy from specified policy if you want the policy that you are creating to receive services from another security policy. Select the parent policy.

   All services from the parent policy are inherited by the new policy.

8. Click Next.

9. In the Guest Introspection Services page, click the Add Guest Introspection Service icon.
   a. In the Add Guest Introspection Service dialog box, type a name and description for the service.
   b. Specify whether you want to apply the service or block it.
      When you inherit a security policy, you may choose to block a service from the parent policy.
      If you apply a service, you must select a service and service profile. If you block a service, you must select the type of service to block.
   c. If you chose to block the service, select the type of service.
   d. If you chose to apply the Guest Introspection service, select the service name.
      The default service profile for the selected service is displayed, which includes information about the service functionality types supported by the associated vendor template.
   e. In State, specify whether you want to enable the selected Guest Introspection service or disable it.
      You can add Guest Introspection services as placeholders for services to be enabled at a later time. This is especially useful for cases where services need to be applied on-demand (for example, new applications).
f  Select whether the Guest Introspection service is to be enforced (i.e. it cannot be overridden). If the selected service profile supports multiple service functionality types, then this is set to **Enforce** by default and cannot be changed.

If you enforce an Guest Introspection service in a security policy, other policies that inherit this security policy would require that this policy be applied before the other child policies. If this service is not enforced, an inheritance selection would add the parent policy after the child policies are applied.

g  Click **OK**.

You can add additional Guest Introspection services by following the above steps. You can manage the Guest Introspection services through the icons above the service table.

You can export or copy the services on this page by clicking the icon on the bottom right side of the Guest Introspection Services page.

10  Click **Next**.

11  On the Firewall page, click the **Add Firewall Rule** icon.

Here, you are defining firewall rules for the security groups(s) that this security policy will be applied to.

a  Type a name and description for the firewall rule you are adding.

b  Select **Allow** or **Block** to indicate whether the rule needs to allow or block traffic to the selected destination.

c  Select the source for the rule. By default, the rule applies to traffic coming from the security groups to which this policy gets applied to. To change the default source, click **Change** and select the appropriate security groups.

d  Select the destination for the rule.

**Note** Either the Source or Destination (or both) must be security groups to which this policy gets applied to.

Say you create a rule with the default Source, specify the Destination as Payroll, and select **Negate Destination**. You then apply this security policy to security group Engineering. This would result in Engineering being able to access everything except for the Payroll server.

e  Select the services and/or service groups to which the rule applies to.

f  Select **Enabled** or **Disabled** to specify the rule state.

g  Select **Log** to log sessions matching this rule.

Enabling logging may affect performance.

h  Click **OK**.

You can add additional firewall rules by following the above steps. You can manage the firewall rules through the icons above the firewall table.
You can export or copy the rules on this page by clicking the icon on the bottom right side of the Firewall page.

The firewall rules you add here are displayed on the Firewall table. VMware recommends that you do not edit Service Composer rules in the firewall table. If you must do so for an emergency troubleshooting, you must re-synchronize Service Composer rules with firewall rules by selecting **Synchronize Firewall Rules** from the **Actions** menu in the Security Policies tab.

12 Click **Next**.

The Network Introspection Services page displays NetX services that you have integrated with your VMware virtual environment.

13 Click the **Add Network Introspection Service** (增添) icon.

   a In the Add Network Introspection Service dialog box, type a name and description for the service you are adding.

   b Select whether or not to redirect to service.

   c Select the service name and profile.

   d Select the source and destination

   e Select the network service that you want to add.

   You can make additional selections based on the service you selected.

   f Select whether to enable or disable the service.

   g Select Log to log sessions matching this rule.

   h Click **OK**.

You can add additional network introspection services by following the above steps. You can manage the network introspection services through the icons above the service table.

You can export or copy the services on this page by clicking the icon on the bottom right side of the Network Introspection Service page.

**Note**  
Bindings created manually for the Service Profiles used in Service Composer policies will be overwritten.

14 Click **Finish**.

The security policy is added to the policies table. You can click the policy name and select the appropriate tab to view a summary of the services associated with the policy, view service errors, or edit a service.

**What to do next**

Map the security policy to a security group.
Edit Service Composer Firewall Applied To Setting

You can set the applied to setting for all firewall rules created though Service Composer to either Distributed Firewall or Policy's Security Groups. By default, the applied to is set to Distributed Firewall.

When Service Composer firewall rules have an applied to setting of distributed firewall, the rules are applied to all clusters on which distributed firewall is installed. If the firewall rules are set to apply to the policy's security groups, you have more granular control over the firewall rules, but may need multiple security policies or firewall rules to get the desired result.

Procedure

1. Log in to the vSphere Web Client.
3. Click Actions > Edit Firewall Policy Settings. Select a default setting for Applied To and click OK.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Firewall</td>
<td>Firewall rules are applied to all clusters on which Distributed Firewall is installed.</td>
</tr>
<tr>
<td>Policy's Security Groups</td>
<td>Firewall rules are applied to security groups on which the security policy is applied.</td>
</tr>
</tbody>
</table>

The default Applied To setting can also be viewed and changed via the API. See the NSX API Guide.

Example: Applied To Behavior

In this example scenario, your default firewall rule action is set to block. You have two security groups: web-servers and app-servers, which contain VMs. You create a security policy, allow-ssh-from-web, which contains the following firewall rule, and apply it to the security group app-servers.

- Name: allow-ssh-from-web
- Source: web-servers
- Destination: Policy's Security Group
- Service: ssh
- Action: allow

If the firewall rule applies to Distributed Firewall, you will be able to ssh from a VM in the security group web-servers to a VM in the security group app-servers.

If the firewall rule applies to Policy's Security Group, you will not be able to ssh, as the traffic will be blocked from reaching the app servers. You will need to create an additional security policy to allow ssh to the app servers, and apply this policy to the security group web-servers.

- Name: allow-ssh-to-app
- Source: Policy's Security Group
- Destination: app-servers
- Service: ssh
- Action: allow
Apply a Security Policy to a Security Group

You can apply a security policy to a security group to secure your virtual desktops, business critical applications, and the connections between them. You can also view a list of the services that were not applied and the reason they failed to apply.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Service Composer.
3. Click the Security Policy tab.
4. Select a security policy and click the Apply Security Policy icon.
5. Select the security group that you want to apply the policy to.
   
   If you select a security group defined by virtual machines that have a certain security tag applied to them, you can create a dynamic or conditional workflow. The moment the tag is applied to a virtual machine, the virtual machine is automatically added to that security group.
   
   Network Introspection rules and Endpoint rules associated with the policy will not take effect for security groups containing IPSet and/or MacSet members.
6. Click the Preview Service Status icon to see the services that cannot be applied to the selected security group and the reason for the failure.
   
   For example, the security group may include a virtual machine that belongs to a cluster on which one of the policy services has not been installed. You must install that service on the appropriate cluster for the security policy to work as intended.
7. Click OK.

Service Composer Canvas

The Service Composer canvas tab offers a graphical view displaying all security groups within the selected NSX Manager. The view also displays details such as members of each security group as well as the security policy applied on it.

This topic introduces Service Composer by walking you through a partially configured system so that you can visualize the mappings between security groups and security policy objects at a high level from the canvas view.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Service Composer.
3 Click the **Canvas** tab.

All security groups within the selected NSX Manager (that are not contained within another security group) are displayed along with the policies applied on them. The **NSX Manager** drop-down lists all NSX Managers on which the currently logged in user has a role assigned.

**Figure 17-3. Service Composer canvas top level view**

Results

Each rectangular box in the canvas represents a security group and the icons within the box represents security group members and details about the security policy mapped to the security group.

**Figure 17-4. Security group**

A number next to each icon indicates the number of instances - for example, ![1](image) indicates that 1 security policy is mapped to that security group.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Click to display</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="1" /></td>
<td>Security groups nested within the main security group.</td>
</tr>
<tr>
<td><img src="image" alt="1" /></td>
<td>Virtual machines that are currently part of the main security group as well as nested security groups. Click the Errors tab to see virtual machines with service errors.</td>
</tr>
</tbody>
</table>
Effective security policies mapped to the security group.

- You can create a new security policy by clicking the Create Security Policy icon. The newly created security policy object is automatically mapped to the security group.
- Map additional security policies to the security group by clicking the Apply Security Policy icon.

Effective Endpoint services associated with the security policy mapped to the security group. Suppose you have two policies applied to a security group and both have the same category Endpoint service configured. The effective service count in this case will be 1 (since the second lower priority service is overridden).

Endpoint service failures, if any, are indicated by the alert icon. Clicking the icon displays the error.

Effective firewall rules associated with the security policy mapped to the security group.

Service failures, if any, are indicated by the alert icon. Clicking the icon displays the error.

Effective network introspection services associated with the security policy mapped to the security group.

Service failures, if any, are indicated by the alert icon. Clicking the icon displays the error.

Clicking an icon displays a dialog box with appropriate details.

Figure 17-5. Details displayed when you click an icon in the security group

You can search for security groups by name. For example, if you type PCI in the search field in the top right corner of the canvas view, only the security groups with PCI in their names are displayed.

To see the security group hierarchy, click the Top Level icon at the top left of the window and select the security group you want to display. If a security group contains nested security groups, click to display the nested groups. The top bar displays the name of the parent security group and the icons in the bar display the total number of security policies, endpoint services, firewall services, and network introspection services applicable to the parent group. You can navigate back up to the top level by clicking the Go up one level icon in the top left part of the window.

You can zoom in and out of the canvas view smoothly by moving the zoom slider on the top right corner of the window. The Navigator box shows a zoomed out view of the entire canvas. If the canvas is much bigger than what fits on your screen, it will show a box around the area that is actually visible and you can move it to change the section of the canvas that is being displayed.

What to do next

Now that we have seen how the mapping between security groups and security policies work, you can begin creating security policies to define the security services you want to apply to your security groups.
Map Security Group to Security Policy

You can map the selected security group to a security policy.

Procedure

1. Select the security policy that you want to apply to the security group.
2. To create a new policy, select New Security Group. See Create a Security Policy.
3. Click Save.

Working with Security Tags

You can view security tags applied on a virtual machine or create a user defined security tag.

Security tags are labels which can be associated with a Virtual Machine (VM). Numerous security tags can be created to identify a specific workload. The matching criteria of a Security Group can be a security tag, and a workload that is tagged can be automatically placed into a Security Group.

Adding or removing security tags to a VM can be done dynamically in response to various criteria such as antivirus or vulnerability scans, and intrusion prevention systems. Tags can also be added and removed manually by an administrator.

In a cross-vCenter NSX environment, universal security tags are created on the primary NSX manager and are marked for universal synchronization with secondary NSX managers. Universal security tags can be assigned to VMs statically, based on unique ID selection.

Unique ID Selection

The unique ID selection criteria is used when assigning tags to Virtual Machines on active standby deployments.

Unique ID is used by the NSX Manager when a Virtual Machine (VM) goes from standby to active deployment. The unique ID can be based on VM instance UUID, VM BIOS UUID, or VM name or a combination of these options. Note that if the criteria changes (such as a VM name changes) after universal security tags have been created and attached to VMs, the security tag must be detached and reattached to the VMs.

Procedure

1. In the vSphere Web Client, navigate to Home > Networking & Security > Installation, select the Management tab.
2. Click the primary NSX Manager. Then select Actions > Unique ID Selection Criteria.
3 Select one or more of the unique ID options:

- Use Virtual Machine instance UUID (recommended) - The VM instance UUID is generally unique within a VC domain, however there are exceptions such as when deployments are made through snapshots. If the VM instance UUID is not unique we recommend you use the VM BIOS UUID in combination with the VM name.

- Use Virtual Machine BIOS UUID - The BIOS UUID is not guaranteed to be unique within a VC domain, but it is always preserved in case of disaster. We recommend you use BIOS UUID in combination with VM name.

- Use Virtual Machine Name - If all of the VM names in an environment are unique, then VM name can be used to identify a VM across vCenters. We recommend you use VM name in combination with VM BIOS UUID.

4 Click OK.

**What to do next**

Next, create security tags.

**View Applied Security Tags**

You can view the security tags applied to virtual machines in your environment.

**Prerequisites**

An antivirus scan must have been run, and a tag applied to the appropriate virtual machine.

**Note** Refer to the third party solution documentation for details of the tags applied by those solutions.

**Procedure**

1 Log in to the vSphere Web Client.

2 Click Networking & Security and then click NSX Managers.

3 Click an NSX Manager in the Name column and then click the Manage tab.

4 Click the Security Tags tab.

   A list of tags applied in your environment is displayed along with details about the virtual machines to which those tags have been applied. Note down the exact tag name if you plan on adding a security group to include virtual machines with a specific tag.

5 Click the number in the VM Count column to view the virtual machines to which that tag in that row has been applied.

**Create a Security Tag**

You can create a security tag and apply it to a virtual machine. In a cross-vCenter environment, security tags are synchronized between primary and secondary NSX managers.
Prerequisites

If creating a universal security tag in an active standby deployment scenario, first set the unique ID selection criteria on the primary NSX Manager.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
4. Click the Security Tags tab.
5. Click the New Security Tag icon.
6. (Optional) To create a universal security tag for use in cross-vCenter NSX environments, select Mark this object for universal synchronization.
7. Type a name and description for the tag and click OK.

What to do next

Assign virtual machines to the security tag.

Assign a Security Tag

In addition to creating a conditional workflow with a dynamic membership-based security tag, you can manually assign a security tag to virtual machines.

Security tags can be used as the matching criteria in security groups. In a cross-vCenter environment, security tags are synchronized between primary and secondary NSX managers.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
4. Click the Security Tags tab.
5. Right-click a security tag and select Assign Security Tag.
   The Assign Security Tag to Virtual Machine window appears, populated with available VMs.
6. Double-click one or more virtual machines to move them to the Selected Objects column. Click OK.
   The Security Tags tab appears with an updated VM count for the security tag.

Edit a Security Tag

You can edit a user-defined security tag. If a security group is based on the tag you are editing, changes to the tag may affect security group membership.
Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
4. Click the Security Tags tab.
5. Right-click a security tag and select Edit Security Tag.
6. Make the appropriate changes and click OK.

Delete a Security Tag

You can delete a user-defined security tag. If a security group is based on the tag you are deleting, changes to the tag may affect security group membership.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
4. Click the Security Tags tab.
5. Select a security tag and click the Delete Security Tag (X) icon.

Viewing Effective Services

You can view the services that are effective on a security policy object or on a virtual machine.

View Effective Services on a Security Policy

You can view the services effective on a security policy, including those services inherited from a parent policy.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Service Composer.
3. Click the Security Policies tab.
4. Click a security policy in the Name column.
5. Ensure that you are in the Manage > Information Security tab.

Results

Each of the three tabs (Endpoint Services, Firewall, Network Introspection Services) displays the corresponding services for the security policy.
Services that are not effective are greyed out. The **Overridden** column displays the services that are actually applied on the security policy and the **Inherited from** column displays the security policy from which services are inherited.

### View Service Failures for a Security Policy

You can see the services associated with a security policy that failed to apply to the security group(s) mapped to the policy.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **Service Composer**.
3. Click the **Security Policies** tab.
4. Click a security policy in the **Name** column.
5. Ensure that you are in the **Monitor > Service Errors** tab.
   
   Clicking the link in the **Status** column takes you to the Service Deployment page where you can correct service errors.

### View Effective Services on a Virtual Machine

You can view the services effective on a virtual machine. If multiple security policies are getting applied on a virtual machine (i.e. a virtual machine is part of multiple security groups that have policies mapped to them), then this view lists all effective services from all these policies, in the order in which they get applied. The service status column displays the status for each service.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **vCenter** and then click **Virtual Machines**.
3. Click a virtual machine in the **Name** column.
4. Ensure that you are in the **Monitor > Service Composer** tab.

### Working with Security Policies

A security policy is a group of network and security services.

The following network and security services can be grouped into a security policy:

- Endpoint services - anti-virus, and vulnerability management
- Distributed Firewall rules
- Network introspection services - network IPS and network forensics
Manage Security Policy Priority

Security policies are applied according to their weight - a security policy with a higher weight has a higher priority. When you move a policy up or down in the table, its weight is adjusted accordingly.

Multiple security policies may be applied to a virtual machine either because the security group that contains the virtual machine is associated with multiple policies or because the virtual machine is part of multiple security groups associated with different policies. If there is a conflict between services grouped with each policy, the weight of the policy determines the services that will be applied to the virtual machine. For example, say policy 1 blocks internet access and has a weight value of 1000 while policy 2 allows internet access and has a weight value of 2000. In this particular case, policy 2 has a higher weight and hence the virtual machine will be allowed internet access.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Service Composer.
3. Click the Security Policies tab.
4. Click the Manage Precedence icon.
5. In the Manage Precedence dialog box, select the security policy that you want to change the precedence for and click the Move Up or Move Down icon.
6. Click OK.

Edit a Security Policy

You can edit the name or description of a security policy, as well as the associated services and rules.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Service Composer.
3. Click the Security Policies tab.
4. Select the security policy that you want to edit and click the Edit Security Policy icon.
5. In the Edit Security Policy dialog box, make the appropriate changes and click Finish.

Delete a Security Policy

You can delete a security policy.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Service Composer.
3 Click the **Security Policies** tab.

4 Select the security policy that you want to delete and click the **Delete Security Policy** icon.

### Service Composer Scenarios

This section illustrates some hypothetical scenarios for Service Composer. It is assumed that the Security Administrator role has been created and assigned to the administrator in each use case.

#### Quarantining Infected Machines Scenario

Service Composer can identify infected systems on your network with 3rd party antivirus solutions and quarantine them to prevent further outbreaks.

Our sample scenario shows how you can protect your desktops end to end.

**Figure 17-6. Configuring Service Composer**
Figure 17-7. Service Composer Conditional Workflow

Prerequisites

We are aware that Symantec tags infected virtual machine with the `AntiVirus.virusFound` tag.

Procedure

1. Install, register, and deploy the Symantec Antimalware solution.
2. Create a security policy for your desktops.
   a. Click the Security Policies tab and click the Add Security Policy icon.
   b. In Name, type DesktopPolicy.
   c. In Description, type Antivirus scan for all desktops.
   d. Change the weight to 51000. The policy precedence is set very high so as to ensure that it is enforced above all other policies.
   e. Click Next.
On the Add Endpoint Service page, click and fill in the following values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Do not modify the default value</td>
</tr>
<tr>
<td>Service Type</td>
<td>Anti Virus</td>
</tr>
<tr>
<td>Service Name</td>
<td>Symantec Antimalware</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Silver</td>
</tr>
<tr>
<td>State</td>
<td>Do not modify the default value</td>
</tr>
<tr>
<td>Enforce</td>
<td>Do not modify the default value</td>
</tr>
<tr>
<td>Name</td>
<td>Desktop AV</td>
</tr>
<tr>
<td>Description</td>
<td>Mandatory policy to be applied on all desktops</td>
</tr>
</tbody>
</table>

Click OK.

Do not add any firewall or network introspection services and click Finish.

Create a security policy for infected virtual machines.

a. Click the Security Policies tab and click the Add Security Policy icon.

b. In Name, type QuarantinePolicy.

c. In Description, type Policy to be applied to all infected systems.

d. Do not change the default weight.

e. Click Next.

f. On the Add Endpoint Service page, do not do anything and click Next.

g. In Firewall, add three rules - one rule to block all outgoing traffic, the next rule to block all traffic with groups, and the last rule to allow incoming traffic only from remediation tools.

h. Do not add any network introspection services and click Finish.

Move QuarantinePolicy to the top of the security policy table to ensure that it is enforced before all other policies.

a. Click the Manage Priority icon.

b. Select QuarantinePolicy and click the Move Up icon.

Create a security group for all desktops in your environment.

a. Log in to the vSphere Web Client.

b. Click Networking & Security and then click Service Composer.

c. Click the Security Groups tab and click the Add Security Group icon.

d. In Name, type DesktopSecurityGroup.

e. In Description, type All desktops.
Click **Next** on the next couple of pages.

Review your selections on the Ready to Complete page and click **Finish**.

### 6 Create a Quarantine security group where the infected virtual machines are to be placed.

- Click the **Security Groups** tab and click the **Add Security Group** icon.
- In **Name**, type **QuarantineSecurityGroup**.
- In **Description**, type
  
  *Dynamic group membership based on infected VMs identified by the antivirus scan.*

- On the Define membership Criteria page click ![icon](image) and add the following criteria.

- Do not do anything on the Select objects to include or Select objects to exclude pages and click **Next**.
- Review your selections on the Ready to Complete page and click **Finish**.

### 7 Map the **DesktopPolicy** policy to the **DesktopSecurityGroup** security group.

- On the Security Policies tab, ensure that the **DesktopPolicy** policy is selected.
- Click the **Apply Security Policy** ( ![icon](image) ) icon and select the SG_Desktops group.
- Click **OK**.
  
  This mapping ensures that all desktops (part of the **DesktopSecurityGroup**) are scanned when an antivirus scan is triggered.

### 8 Navigate to the canvas view to confirm that **QuarantineSecurityGroup** does not include any virtual machines yet.

- Click the **Information Security** tab.
  
  ![image](image)

- Confirm that there are 0 virtual machines in the group ( ![image](image) )

### 9 Map **QuarantinePolicy** to **QuarantineSecurityGroup**.

This mapping ensures that no traffic flows to the infected systems.

### 10 From the Symantec Antimalware console, trigger a scan on your network.

The scan discovers infected virtual machine and tags them with the security tag **AntiVirus.virusFound**. The tagged virtual machines are instantly added to **QuarantineSecurityGroup**. The **QuarantinePolicy** allows no traffic to and from the infected systems.
Back up Security Configurations

Service Composer can be effectively used to back up your security configurations and restore them at a later time.

Procedure

1. Install, register, and deploy the Rapid 7 Vulnerability Management solution.

2. Create a security group for the first tier of the Share Point application - web servers.
   a. Log in to the vSphere Web Client.
   b. Click Networking & Security and then click Service Composer.
   c. Click the Security Groups tab and click the Add Security Group icon.
   d. In Name, type SG_Web.
   e. In Description, type Security group for application tier.
   f. Do not do anything on the Define membership Criteria page and click Next.
   g. On the Select objects to include page, select the web server virtual machines.
   h. Do not do anything on the Select objects to exclude page and click Next.
   i. Review your selections on the Ready to Complete page and click Finish.

3. Now create a security group for your database and share point servers and name them SG_Database, and SG_Server_SharePoint respectively. Include the appropriate objects in each group.

4. Create a top level security group for your application tiers and name it SG_App_Group. Add SG_Web, SG_Database, and SG_Server_SharePoint to this group.

5. Create a security policy for your web servers.
   a. Click the Security Policies tab and click the Add Security Policy icon.
   b. In Name, type SP_App.
   c. In Description, type SP for application web servers.
   d. Change the weight to 50000. The policy precedence is set very high so as to ensure that it is enforced above most other policies (with the exception of quarantine).
   e. Click Next.
f On the Endpoint Services page, click and fill in the following values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Do not modify the default value</td>
</tr>
<tr>
<td>Service Type</td>
<td>Vulnerability Management</td>
</tr>
<tr>
<td>Service Name</td>
<td>Rapid 7</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Silver</td>
</tr>
<tr>
<td>State</td>
<td>Do not modify the default value</td>
</tr>
<tr>
<td>Enforce</td>
<td>Do not modify the default value</td>
</tr>
</tbody>
</table>

g Do not add any firewall or network introspection services and click Finish.

6 Map SP_App to SG_App_Group.

7 Navigate to the canvas view to confirm that the SP_App has been mapped to SG_App_Group.
   a Click the Information Security tab.
   b Click the number next to the icon to see that the SP_App is mapped.

8 Export the SP_App policy.
   a Click the Security Policies tab and then click the Export Blueprint icon.
   b In Name, type Template_App_ and in Prefix, type FromAppArchitect.
   c Click Next.
   d Select the SP_App policy and click Next.
   e Review your selections and click Finish.
   f Select the directory on your computer where you want to download the exported file and click Save.

The security policy as well as all the security groups to which this policy has been applied (in our case, the Application security group as well as the three security groups nested within it) are exported.

9 In order to demonstrate how the exported policy works, delete the SP_App policy.

10 Now we will restore the Template_App_DevTest policy that we exported in step 7.
   a Click Actions and then click the Import Service Configuration icon.
   b Select the FromAppArchitect_Template_App file from your desktop (you saved it in step 7).
   c Click Next.
The Ready to complete page displays the security policies along with associated objects (security groups on which these have been applied, as well as Endpoint services, firewall rules, and network introspection services) to be imported.

Click Finish.

The configuration and associated objects are imported to the vCenter inventory and are visible in the canvas view.

Importing and Exporting Security Policy Configurations

You can use the Service Composer to export the security policy configuration to a specific file format from one NSX Manager and import the exported configuration in to another NSX Manager.

In the Service Composer, you cannot directly export security groups. You must first ensure that a security policy is assigned to a security group, and then export that security policy. All the contents of the security policy, such as DFW rules, guest introspection rules, network introspection rules, and the security groups that are bound to the security policy are exported.

When a container security group contains nested security groups, the nested security groups are not exported. While exporting, you can add a prefix to the policy. The prefix gets applied to policy name, policy actions name, and security group name.

When importing the configuration onto a different NSX Manager, you can specify a suffix. The suffix gets applied to policy name, policy actions name, and, security group name. If a security group or security policy with the same name exists on the NSX Manager where the import is happening, the import of the security policy configuration fails.

Export a Security Policy Configuration

You can export a security policy configuration and save it to your desktop. The saved configuration can be used as a backup for situations where you may accidentally delete a policy configuration, or it can be exported for use in another NSX Manager environment.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then click Service Composer.
3. Click the Security Policies tab.
4. Select the security policy that you want to export.
5. Click Actions and then click Export Configuration.
6. Type a name and description for the configuration that you are exporting.
7. If necessary, type a prefix to be added to the security policies and security groups that are being exported.
   
   If you specify a prefix, it is added to the target security policy names thus ensuring that they have unique names.
8 Click **Next**.

9 In the **Select security policies** page, select the security policy that you want to export and click **Next**.

10 The **Ready to complete page** displays the security policies, endpoint services, firewall rules, and network introspection services to be exported.

   This page also displays the security groups on which the security policies are applied.

11 Click **Finish**.

12 Select the directory on your computer where you want to download the exported blueprint and click **Save**.

   The security policy configuration file is saved at the specified location.

### Import a Security Policy Configuration

You can import a saved security policy configuration either as a backup or to restore a similar configuration on a different NSX Manager.

When importing the configuration, an empty security group is created. All the services, service profiles, applications, and application groups must exist in the destination environment, otherwise the import fails.

**Procedure**

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Service Composer**.

3 Click the **Security Policies** tab.

4 Click **Actions** and then click the **Import Service Configuration** icon.

5 Select the configuration file that you want to import.

6 If necessary, type a suffix to be added to the security policies and security groups that are being imported.

   If you specify a suffix, it is added to the security policy names being imported thus ensuring that they have unique names.

7 Click **Next**.

   Service Composer verifies that all services referred to in the configuration are available in the destination environment. If not, the **Manage Missing Services** page is displayed, where you can map missing services to available target services.

   The **Ready to complete** page displays the security policies, endpoint services, firewall rules, and the network introspection services to be imported. This page also displays the security groups on which the security policies are applied.
8 Click **Finish**.

The imported security policy configuration is added to the top of the security policy table (above the existing policies) in the target NSX Manager. The original order of the imported rules and security services in the security policy is preserved.
Guest Introspection

Guest Introspection offloads antivirus and anti-malware agent processing to a dedicated secure virtual appliance delivered by VMware partners. Since the secure virtual appliance (unlike a guest virtual machine) doesn’t go offline, it can continuously update antivirus signatures thereby giving uninterrupted protection to the virtual machines on the host. Also, new virtual machines (or existing virtual machines that went offline) are immediately protected with the most current antivirus signatures when they come online.

Guest Introspection health status is conveyed by using alarms that show in red on the vCenter Server console. In addition, more status information can be gathered by looking at the event logs.

Important  Your environment must be correctly configured for Guest Introspection security:

- All hosts in a resource pool containing protected virtual machines must be prepared for Guest Introspection so that virtual machines continue to be protected as they are vMotioned from one ESXi host to another within the resource pool.
- Virtual machines must have the Guest Introspection thin agent installed to be protected by Guest Introspection security solution. Not all guest operating systems are supported. Virtual machines with non-supported operating systems are not protected by the security solution.

This chapter includes the following topics:

- Install Guest Introspection on Host Clusters
- Install the Guest Introspection Thin Agent on Windows Virtual Machines
- Install the Guest Introspection Thin Agent on Linux Virtual Machines
- View Guest Introspection Status
- Guest Introspection Audit Messages
- Collecting Guest Introspection Troubleshooting Data
- Uninstall a Guest Introspection Module
Install Guest Introspection on Host Clusters

Installing Guest Introspection automatically installs a new VIB and a service virtual machine on each host in the cluster. Guest Introspection is required for Activity Monitoring, and several third-party security solutions.

**Note** You cannot migrate a Service VM (SVM) using vMotion/SvMotion. SVMs must remain on the host on which they were deployed for correct operation.

### Prerequisites

The installation instructions that follow assume that you have the following system:

- A datacenter with supported versions of vCenter Server and ESXi installed on each host in the cluster.
- If the hosts in your clusters were upgraded from vCenter Server version 5.0 to 5.5, you must open ports 80 and 443 on those hosts.
- Hosts in the cluster where you want to install Guest Introspection have been prepared for NSX. See Prepare Host Clusters for NSX in the *NSX Installation Guide*. Guest Introspection cannot be installed on standalone hosts. If you are using NSX for deploying and managing Guest Introspection for anti-virus offload capability only, you do not need to prepare the hosts for NSX, and the NSX for vShield Endpoint license does not allow it.
- NSX Manager installed and running.
- Ensure the NSX Manager and the prepared hosts that will run Guest Introspection services are linked to the same NTP server and that time is synchronized. Failure to do so may cause VMs to be unprotected by anti-virus services, although the status of the cluster will be shown as green for Guest Introspection and any third-party services.
  
  If an NTP server is added, VMware recommends that you then redeploy Guest Introspection and any third-party services.

If you want to assign an IP address to the NSX Guest Introspection service virtual machine from an IP pool, create the IP pool before installing NSX Guest Introspection. See Working with IP Pools in the *NSX Administration Guide*.

vSphere Fault Tolerance does not work with Guest Introspection.

### Procedure

1. On the **Installation** tab, click **Service Deployments**.
2. Click the **New Service Deployment** (+] icon.
3. In the Deploy Network and Security Services dialog box, select **Guest Introspection**.
4. In **Specify schedule** (at the bottom of the dialog box), select **Deploy now** to deploy Guest Introspection as soon as it is installed or select a deployment date and time.
5 Click **Next**.

6 Select the datacenter and cluster(s) where you want to install Guest Introspection, and click **Next**.

7 On the Select storage and Management Network Page, select the datastore on which to add the service virtual machines storage or select **Specified on host**. It is recommended that you use shared datastores and networks instead of “specified on host” so that deployment workflows are automated.

   The selected datastore must be available on all hosts in the selected cluster.

   If you selected **Specified on host**, follow the steps below for each host in the cluster.

   a On the vSphere Web Client home page, click **vCenter** and then click **Hosts**.

   b Click a host in the **Name** column and then click the **Manage** tab.

   c Click **Agent VMs** and click **Edit**.

   d Select the datastore and click **OK**.

8 Select the distributed virtual port group to host the management interface. If the datastore is set to **Specified on host**, the network must also be **Specified on host**.

   The selected port group must be able to reach the NSX Manager’s port group and must be available on all hosts in the selected cluster.

   If you selected **Specified on host**, follow the substeps in Step 7 to select a network on the host.

   When you add a host (or multiple hosts) to the cluster, the datastore and network must be set before each host is added to the cluster.

9 In IP assignment, select one of the following:

<table>
<thead>
<tr>
<th>Select</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Assign an IP address to the NSX Guest Introspection service virtual machine through Dynamic Host Configuration Protocol (DHCP). Select this option if your hosts are on different subnets.</td>
</tr>
<tr>
<td>An IP pool</td>
<td>Assign an IP address to the NSX Guest Introspection service virtual machine from the selected IP pool.</td>
</tr>
</tbody>
</table>

10 Click **Next** and then click **Finish** on the Ready to complete page.

11 Monitor the deployment until the **Installation Status** column displays **Succeeded**.

12 If the **Installation Status** column displays **Failed**, click the icon next to Failed. All deployment errors are displayed. Click **Resolve** to fix the errors. In some cases, resolving the errors displays additional errors. Take the required action and click **Resolve** again.

### Install the Guest Introspection Thin Agent on Windows Virtual Machines

To protect VMs using a Guest Introspection security solution, you must install Guest Introspection thin agent, also called Guest Introspection drivers, on the VM. Guest Introspection drivers are included with
VMware Tools for Windows, but are not part of the default installation. To install Guest Introspection on a Windows VM, you must perform a custom install and select the drivers.

- If you are using vSphere 6.5, see these instructions for installing VMware Tools: [https://www.vmware.com/support/pubs/vmware-tools-pubs.html](https://www.vmware.com/support/pubs/vmware-tools-pubs.html).

Windows virtual machines with the Guest Introspection drivers installed are automatically protected whenever they are started up on an ESXi host that has the security solution installed. Protected virtual machines retain the security protection through shut downs and restarts, and even after a vMotion move to another ESXi host with the security solution installed.

For Linux instructions, see Install the Guest Introspection Thin Agent on Linux Virtual Machines.

**Prerequisites**

Ensure that the guest virtual machine has a supported version of Windows installed. The following Windows operating systems are supported for NSX Guest Introspection:

- Windows XP SP3 and above (32 bit)
- Windows Vista (32 bit)
- Windows 7 (32/64 bit)
- Windows 8 (32/64 bit) -- vSphere 5.5 only
- Windows 8.1 (32/64) -- from vSphere 5.5 Patch 2 and later
- Windows 10
- Windows 2003 SP2 and above (32/64 bit)
- Windows 2003 R2 (32/64 bit)
- Windows 2008 (32/64 bit)
- Windows 2008 R2 (64 bit)
- Win2012 (64) -- vSphere 5.5 only
- Win2012 R2 (64) -- from vSphere 5.5 Patch 2 and later

**Procedure**

1. Start the VMware Tools installation, following the instructions for your version of vSphere. Select **Custom** install.

2. Expand the **VMCI Driver** section.
   
   The options available will vary depending on the version of VMware Tools.
Driver Description

vShield Endpoint Drivers Installs File Introspection (vsepflt) and Network Introspection (vnetflt) drivers.

Guest Introspection Drivers Installs File Introspection (vsepflt) and Network Introspection (vnetflt) drivers.

NSX File Introspection Driver and NSX Network Introspection Driver Select NSX File Introspection Driver to install vsepflt. Optionally select NSX Network Introspection Driver to install vnetflt (vnetWFP on Windows 10).

**Note** Select NSX Network Introspection Driver only if you are using the Identity Firewall or Endpoint Monitoring features.

3 In the drop-down menu next to the drivers you want to add, select **This feature will be installed on the local hard drive**.

4 Follow the remaining steps in the procedure.

**What to do next**

Check if the thin agent is running using the `fltmc` command with the administrative privileges. The Filter Name column in the output lists the thin agent with an entry `vsepflt`.

**Install the Guest Introspection Thin Agent on Linux Virtual Machines**

Guest Introspection supports File Introspection in Linux for anti-virus only. To protect Linux VMs using a Guest Introspection security solution, you must install the Guest Introspection thin agent.

The GI thin agent is available as part of the VMware Tools operating system-specific packages (OSPs). Installing VMware Tools is not required. GI thin agent installation and upgrade is not connected to NSX installation and upgrade. Also, Enterprise or Security Administrator (non-NSX Administrator) can install the agent on guest VMs outside of NSX.

To install the GI thin agent on RHEL or SLES Linux systems, use the `RPM` package. To install the GI thin agent on Ubuntu Linux systems, use the `DEB` package.

For Windows instructions, see [Install the Guest Introspection Thin Agent on Windows Virtual Machines](#).

**Prerequisites**

- Ensure that the guest virtual machine has a supported version of Linux installed:
  - Red Hat Enterprise Linux (RHEL) 7 GA (64 bit)
  - SUSE Linux Enterprise Server (SLES) 12 GA (64 bit)
  - Ubuntu 14.04 LTS (64 bit)
- Verify GLib 2.0 is installed on the Linux VM.
Download the GI thin agent package (vmware-nsx-gi-file) by visiting the VMware package repository at https://packages.vmware.com/packages/index.html.

**Procedure**

- Based on your Linux operating system, perform the following steps with root privilege:
  - For Ubuntu systems:
    a. Obtain and import the VMware packaging public keys using the following commands:

    ```bash
    curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
    apt-key add VMWARE-PACKAGING-GPG-RSA-KEY.pub
    ```

    b. Create a new file named `vm.list` file under `/etc/apt/sources.list.d`.

    c. Edit the file with the following content:

    ```bash
    vi /etc/apt/sources.list.d/vm.list
    deb https://packages.vmware.com/packages/ubuntu/ trusty main
    ```

    d. Now, install the package as follows:

    ```bash
    apt-get update
    apt-get install vmware-nsx-gi-file
    ```

  - For RHEL7 systems:
    a. Obtain and import the VMware packaging public keys using the following commands:

    ```bash
    curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
    rpm --import VMWARE-PACKAGING-GPG-RSA-KEY.pub
    ```

    b. Create a new file named `vm.repo` file under `/etc/yum.repos.d`.

    c. Edit the file with the following content:

    ```bash
    vi /etc/yum.repos.d/vm.repo
    [vm]
    name = VMware
    baseurl = https://packages.vmware.com/packages/rhel7/x86_64
    enabled = 1
    gpgcheck = 1
    metadata_expire = 86400
    ui_repoid_vars = basearch
    ```
Now, install the package as follows:

```bash
yum install vmware-nsx-gi-file
```

For SLES systems:

a. Obtain and import the VMware packaging public keys using the following commands:

```bash
curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-GPG-RSA-KEY.pub
```

b. Add the following repository:

```bash
zypper ar -f "https://packages.vmware.com/packages/sle12/x86_64/" VMware
```

c. Now, install the package as follows:

```bash
zypper install vmware-nsx-gi-file
```

What to do next

Check if the thin agent is running using the `service vsepd status` command with the administrative privileges. The status should be running.

View Guest Introspection Status

Monitoring a Guest Introspection instance involves checking for status coming from the Guest Introspection components: the security virtual machine (SVM), the ESXi host-resident Guest Introspection module, and the protected virtual machine-resident thin agent.

Procedure

1. In the vSphere Web Client, click **vCenter Inventory Lists**, and then click **Datacenters**.
2. In the **Name** column, click a data center.
3. Click **Monitor** and then click **Guest Introspection**.

   The Guest Introspection Health and Alarms page displays the health of the objects under the data center you selected, and the active alarms. Health status changes are reflected within a minute of the actual occurrence of the event that triggered the change.

Guest Introspection Audit Messages

Audit messages include fatal errors and other important audit messages and are logged to `vmware.log`.

The following conditions are logged as AUDIT messages:

- Thin agent initialization success (and version number.)
- Thin agent initialization failure.
Established first time communication with SVM.

Failure to establish communication with SVM (when first such failure occurs).

Generated log messages have the following substrings near the beginning of each log message: vf-AUDIT, vf-ERROR, vf-WARN, vf-INFO, vf-DEBUG.

**Collecting Guest Introspection Troubleshooting Data**

VMware Technical Support routinely requests diagnostic information or a support bundle when a support request is handled. This diagnostic information contains logs and configuration files for your virtual machines.

**Identity Firewall Troubleshooting Data**

If your identity-based firewall environment uses Guest Introspection, diagnostic information is found in the [NSX Troubleshooting Guide](#) and [NSX Logging and System Events](#).

**Uninstall a Guest Introspection Module**

Uninstalling guest introspection removes a VIB from the hosts in the cluster and removes the service virtual machine from each host in the cluster. Guest Introspection is required for Identity Firewall, Endpoint Monitoring, and several third-party security solutions. Uninstalling guest introspection can have wide ranging impacts.

**Caution** Before you uninstall a Guest Introspection module from a cluster, you must uninstall all third-party products that are using Guest Introspection from the hosts on that cluster. Use the instructions from the solution provider.

There is a loss of protection for VMs in the NSX cluster. You must vMotion the VMs out of the cluster before you uninstall.

To uninstall Guest Introspection:

1. In vCenter, navigate to **Home > Networking & Security > Installation** and select the **Service Deployments** tab.
2. Select a Guest Introspection instance and click the delete icon.
3. Either delete now or schedule the deletion for a later time.
Uninstall Guest Introspection for Linux

You can uninstall Linux thin agent for Guest Introspection from guest virtual machine.

Prerequisites

Guest Introspection for Linux is installed. You have root privileges on the Linux system.

Procedure

◆ For uninstalling package from Ubuntu system, run the `apt-get remove vmware-nsx-gi-file` command.

◆ For uninstalling package from RHEL7 system, run the `yum remove vmware-nsx-gi-file` command.

◆ For uninstalling package from SLES system, run the `zypper remove vmware-nsx-gi-file` command.

Results

The thin agent installed on Linux virtual machine is uninstalled.
Datacenter networks typically involve a wide range of network services, including switching, routing, firewalling, load balancing, and so on. In most cases, these services are delivered by different vendors. In the physical world, connecting these services in the network is a complicated exercise of racking and stacking physical network devices, establishing physical connectivity, and managing these services separately. NSX simplifies the experience of connecting the right services in the right traffic paths and can help you build complex networks within a single ESX Server host or across multiple ESX server hosts for production, testing, or development purposes.

There are various deployment methods for inserting third party services into NSX.

This chapter includes the following topics:
Distributed Service Insertion

In distributed service insertion, a single host has all service modules, kernel modules, and virtual machine implementations on a single physical machine. All components of the system interact with components within the physical host. This allows for faster module-to-module communication and compact deployment models. The same configuration can be replicated on physical systems in the network for scalability, while control and data plane traffic to and from the service modules to the vmkernel stay on the same physical system. During vMotion of the protected virtual machines, the partner security machine moves the virtual machine state from the source to the destination host.

Vendor solutions that make use of this type of service insertion include Intrusion Prevention Service (IPS)/Intrusion Detection Service (IDS), Firewall, Anti Virus, File Identity Monitoring (FIM), and Vulnerability Management.

Edge-Based Service Insertion

NSX Edge is deployed as a virtual machine in the Edge Services Cluster along with other network services. NSX Edge has the capability to redirect specific traffic to 3rd-party network services.

Vendor solutions that make use of this type of service insertion include ADC/Load Balancer devices.

Integrating Third Party Services

This is a generic high-level workflow for inserting a third-party service into the NSX platform.

Procedure

1. Register the third-party service with NSX Manager on the vendor's console.

   You need NSX login credentials to register the service. For more information, refer to the vendor documentation.
2 Deploy the service in NSX. See Deploy a Partner Service.

Once deployed, the third-party service is displayed in the NSX Service Definitions window and is ready to be used. The procedure for using the service in NSX depends on the type of service inserted.

For example, you can enable a host-based firewall service by creating a security policy in Service Composer or creating a firewall rule to redirect traffic to the service. See Consuming Vendor Services through Service Composer or Redirecting Traffic to a Vendor Solution through Logical Firewall. For information on using an Edge based service, see Using a Partner Load Balancer.

**Deploy a Partner Service**

If the partner solution includes a host-resident virtual appliance, you can deploy the service after the solution is registered with NSX Manager.

**Prerequisites**

Ensure that:

- The partner solution is registered with NSX Manager.
- NSX Manager can access the partner solution’s management console.
- The required license edition has been assigned. See https://kb.vmware.com/kb/2145269.

**Procedure**

1. Click Networking & Security and then click Installation.
2. Click the Service Deployments tab and click the New Service Deployment (⊕) icon.
3. In the Deploy Network and Security Services dialog box, select the appropriate solution(s).
4. In Specify schedule (at the bottom of the dialog box), select Deploy now to deploy the solution immediately or select a deployment date and time.
5. Click Next.
6. Select the datacenter and cluster(s) where you want to deploy the solution and click Next.
7. Select the datastore on which to add the solution service virtual machines storage or select Specified on host.

The selected datastore must be available on all hosts in the selected cluster.

If you selected Specified on host, the datastore for the ESX host must be specified in the AgentVM Settings of the host before it is added to the cluster. See vSphere API/SDK Documentation.
8. Select the distributed virtual port group to host the management interface. This port group must be able to reach the NSX Manager’s port group.

If the network is set to Specified on host, the network to be used must be specified in the Agent VM Settings > Network property of each host in the cluster. See vSphere API/SDK Documentation.
You must set the agent VM network property on a host before you add it to a cluster. Navigate to Manage > Settings > Agent VM Settings > Network and click Edit to set the agent VM network.

The selected port group must be available on all hosts in the selected cluster.

9 In IP assignment, select one of the following:

<table>
<thead>
<tr>
<th>Select</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Assign an IP address to the service virtual machine through Dynamic Host Configuration Protocol (DHCP).</td>
</tr>
<tr>
<td>An IP pool</td>
<td>Assign an IP address to the service virtual machine from the selected IP pool.</td>
</tr>
</tbody>
</table>

10 Click Next and then click Finish on the Ready to complete page.

11 Monitor the deployment until the Installation Status displays Successful. If the status displays Failed, click the icon next to Failed and take action to resolve the error.

What to do next

You can now consume the partner service through NSX UI or NSX API.

**Consuming Vendor Services through Service Composer**

Third-party vendor services include traffic redirection, load balancer, and guest security services such as data loss prevention, anti virus, and so on. Service Composer enables you to apply these services to a set of vCenter objects.

A security group is a set of vCenter objects such as clusters, virtual machines, vNICs, and logical switches. A security policy is a set of Guest Introspection services, firewall rules, and network introspection services.

When you map a security policy to a security group, redirection rules are created on the appropriate third-party vendor service profile. As traffic flows from virtual machines belonging to that security group, it is redirected to registered third-party vendor services that determine how to process that traffic. For more information on Service Composer, see Using Service Composer.

**Redirecting Traffic to a Vendor Solution through Logical Firewall**

You can add firewall rules to redirect traffic to registered vendor solutions. Redirected traffic is then processed by the vendor service.

**Prerequisites**

- The third party service must be registered with NSX Manager, and the service must be deployed in NSX.
- If the default firewall rule action is set to Block, you must add a rule to allow the traffic to be redirected.
**Procedure**

1. In the vSphere Web Client, navigate to **Networking & Security > Firewall**.
2. Click the **Partner security services** tab.
3. In the section to which you want to add a rule, click the **Add rule** (➕) icon. A new any any allow rule is added at the top of the section.
4. Point to the **Name** cell of the new rule, click ☑, and type a name for the rule.
5. Specify the **Source**, **Destination**, and **Service** for the rule. For more information, see **Add a Distributed Firewall Rule**
6. Point to the **Action** cell of the new rule, and click ☑.
   a. In **Action**, select **Redirect**.
   b. In **Redirect To**, select the service profile and the logical switch or security group to which you want to bind the service profile.
      The service profile is applied to virtual machines connected to or contained in the selected logical switch or security group.
   c. Indicate whether the redirected traffic is to be logged and type comments, if any.
   d. Click **OK**.
      The selected service profile is displayed as a link in the **Action** column. Clicking the service profile link displays the service profile bindings.
7. Click **Publish Changes**.

**Using a Partner Load Balancer**

You can use a third-party load balancer to balance the traffic for a specific NSX Edge.

**Prerequisites**

The third-party load balancer must be registered with NSX Manager, and it must be deployed in NSX.

**Procedure**

1. In the vSphere Web Client, navigate to **Networking & Security > NSX Edges**.
2. Double-click an NSX Edge.
3. Click **Manage** and then click the **Load Balancer** tab.
4. Click **Edit** next to Load balancer global configuration.
5. Select **Enable Load Balancer** and **Enable Service Insertion**.
6. In **Service Definition**, select the appropriate partner load balancer.
7. In **Service Configuration**, select the appropriate service configuration.
8 Complete the remaining fields and set up the load balancer by adding a service monitor, server pool, application profile, application rules, and a virtual server. When adding a virtual server, select the template provided by the vendor. For more information, see Setting Up Load Balancing.

Results
Traffic for the specified Edge is load balanced by the third party vendor's management console.

Remove Third-Party Integration

This example describes how to remove a third-party integration solution from NSX.

There is a correct order of software when removing any third-party software solution. If this sequence is not followed and specifically if the third-party solution is uninstalled or deleted before it is unregistered with NSX Manager, the removal operation will fail. See https://kb.vmware.com/kb/2126678 for instructions on how to resolve this.

Procedure

1 In the Sphere Web Client, navigate to Networking & Security > Service Composer, and delete the rules (or security polices) that are redirecting traffic to the 3rd-party solution.

2 Navigate to Service Definitions and double-click the name of the third-party solution.

3 Click Related Objects and delete the related objects.

4 Navigate to Installation > Service Deployments and delete the third-party deployment.
   This action uninstalls the associated VMs.

5 Return to Service Definitions and delete any sub-components of the definition.

6 In the service instance, delete the service profile.

7 Delete the service instance.

8 Delete the service definition.

Results
The third-party integration solution is removed from NSX.

What to do next
Make notes of the configuration settings, and then remove NSX from the third-party solution. For example, you may need to delete rules that reference other objects and then delete the objects.
In many organizations, networking and security operations are handled by different teams or members. Such organizations may require a way to limit certain operations to specific users. This topic describes the options provided by NSX to configure such access control.

NSX also supports Single Sign On (SSO), which enables NSX to authenticate users from other identity services such as Active Directory, NIS, and LDAP.

User management in the vSphere Web Client is separate from user management in the CLI of any NSX component.

This chapter includes the following topics:

- NSX Users and Permissions by Feature
- Configure Single Sign On
- Managing User Rights
- Managing the Default User Account
- Assign a Role to a vCenter User
- Create a User with Web Interface Access Using CLI
- Edit a User Account
- Change a User Role
- Disable or Enable a User Account
- Delete a User Account

NSX Users and Permissions by Feature

To deploy and administer NSX, certain vCenter permissions are required. NSX provides extensive read and read/write permissions for various users and roles.
# Feature List with Roles and Permissions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Auditor</th>
<th>Security Admin</th>
<th>NSX Admin</th>
<th>Enterprise Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrator</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td>vCenter and SSO Configuration with NSX</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Update</td>
<td>No Access</td>
<td>No Access</td>
<td>No Access</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>System Events</td>
<td>System Events</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Audit Logs</td>
<td>Audit Logs</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td><strong>User Account Management (URM)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Account Management</td>
<td>User Management</td>
<td>No Access</td>
<td>No Access</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Object Access Control</td>
<td>No Access</td>
<td>No Access</td>
<td>No Access</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Feature Access Control</td>
<td>No Access</td>
<td>No Access</td>
<td>No Access</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td><strong>Edge</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>System refers to general system parameters</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Appliance</td>
<td>Different form factors of NSX Edge (Compact /Large/X-Large/ QuadLarge)</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>High availability</td>
<td></td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>vNic</td>
<td>Interface configuration on NSX Edge</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>DNS</td>
<td></td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>SSH</td>
<td>SSH configuration on NSX Edge</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Auto plumbing</td>
<td></td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Statistics</td>
<td></td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>NAT</td>
<td>NAT configuration on NSX Edge</td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>DHCP</td>
<td></td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Load balance</td>
<td></td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>VPN</td>
<td></td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Syslog</td>
<td>Syslog configuration on NSX Edge</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Routing</td>
<td>All routing static and dynamic routing (BGP/OSPF) on NSX Edge</td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Firewall</td>
<td>Firewall configuration on NSX Edge</td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Bridging</td>
<td></td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Roles</td>
<td>Auditor</td>
<td>Security Admin</td>
<td>NSX Admin</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Certificate</td>
<td>System control refers to system kernel parameters such as maximum limits, IP forwarding, networking, and system settings. For example: <code>sysct1.net.ipv4.conf.vNic_1 rp_filter</code> <code>sysct1.net.netfilter.nf_conntrack_tcp_timeout_established</code></td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>System control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Firewall</td>
<td>Firewall config</td>
<td>Layer3 (General) and Layer2 (Ethernet) firewall rules</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>Firewalls</td>
<td>Flows</td>
<td>Flow monitoring is for monitoring traffic flows in the system. Live Flows can also be monitored</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>Flows</td>
<td>IPFix config</td>
<td>IPFix enable/disable and assigning collectors</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>IPFix config</td>
<td>ForceSync</td>
<td>ForceSync does full sync from the Installation &gt; Host Preparation page</td>
<td>R</td>
<td>R</td>
<td>No Access</td>
</tr>
<tr>
<td>ForceSync</td>
<td>Install DFW (host preparation)</td>
<td>Install VIBS on clusters</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Install DFW (host preparation)</td>
<td>Saved Configurations (drafts)</td>
<td>Every publish will automatically save existing DFW configuration as a draft</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>Saved Configurations (drafts)</td>
<td>Exclusion List</td>
<td>Add VMs to exclusion list to be NOT protected by DFW or to remove them</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>Exclusion List</td>
<td>DFW Tech Support</td>
<td>Collecting DFW Tech Support bundle from a host (only NSX config shell)</td>
<td>No Access</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>DFW Tech Support</td>
<td>DFW Session Timers</td>
<td>Configure TCP/UDP/Other protocol connection timeout configuration</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>DFW Session Timers</td>
<td>IP Discovery (DHCP/ARP Snooping)</td>
<td>IP discovery when VMware Tools are not running on Guest VMs</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>IP Discovery (DHCP/ARP Snooping)</td>
<td>Application Rule Manager</td>
<td>Flows are collected for selected set of applications. Firewall rules are then created based on the collected flows.</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>Application Rule Manager</td>
<td>NameSpace</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NameSpace</td>
<td>Config</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Config</td>
<td>SpoofGuard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Auditor</td>
<td>Security Admin</td>
<td>NSX Admin</td>
<td>Enterprise Admin</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
<td>-------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Config</td>
<td>SpoofGuard publish in TOFU or Manual Mode</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
<td>R, W</td>
</tr>
<tr>
<td><strong>Endpoint Security (EPSEC)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td></td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Registration</td>
<td>Manage [Register, Unregister, Query registered solutions, Activate] Solutions</td>
<td>R</td>
<td>No Access</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Health monitoring</td>
<td>Retrieve health status of VM, SVM to the NSX Manager</td>
<td>No Access</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Policy</td>
<td>Manage security policies [Create, Read, Update, Delete]</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Scan scheduling</td>
<td></td>
<td>R</td>
<td>No Access</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td><strong>Library</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host preparation</td>
<td>Host preparation action on cluster</td>
<td>No Access</td>
<td>No Access</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Tagging</td>
<td>Security tag (for example, attach or detach VMs)</td>
<td>R</td>
<td>R, W</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td><strong>Install</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App</td>
<td></td>
<td>No Access</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>EPSEC</td>
<td></td>
<td>No Access</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>DLP</td>
<td></td>
<td>No Access</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td><strong>VDN</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Config NSM</td>
<td>Configure Network Security Manager</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Provision</td>
<td></td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td><strong>ESX Agent Manager (EAM)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>ESX Agent Manager</td>
<td>No Access</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td><strong>Service Insertion</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td></td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Service profile</td>
<td></td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td><strong>Trust Store</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>trustentity_management</td>
<td>NSX certificate management</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td><strong>IP Address Management (IPAM)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Roles</td>
<td>Auditor</td>
<td>Security Admin</td>
<td>NSX Admin</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>-------</td>
<td>---------</td>
<td>----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>IP allocation</td>
<td>IP allocation and release</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Security Fabric</td>
<td>Deploy</td>
<td>Deploy service or security VM on cluster using the Service Deployment page</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Alarms</td>
<td>From the Service Deployment page, manage alarms that are generated by security VM</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Agent health status</td>
<td>Managing agent health status alarm over rest call, mainly used by partner VMs</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Messaging</td>
<td>Messaging framework used by NSX Edge and Guest Introspection to communicate with NSX Manager</td>
<td>R</td>
<td>R, W</td>
<td>R, W</td>
<td>R, W</td>
</tr>
<tr>
<td>Replicator (Multi vCenter setup with secondary NSX Manager)</td>
<td>Configuration</td>
<td>Select or deselect Primary role for NSX Manager, and add or remove Secondary NSX Manager</td>
<td>R</td>
<td>R</td>
<td>R, W</td>
</tr>
<tr>
<td>Security Policy</td>
<td>Configuration</td>
<td>Configure security policy to create, update, edit, or delete</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
</tr>
<tr>
<td>Security group binding</td>
<td>Associate security group with a security policy</td>
<td>R</td>
<td>R, W</td>
<td>No Access</td>
<td>R, W</td>
</tr>
</tbody>
</table>

### Configure Single Sign On

SSO makes vSphere and NSX more secure by allowing the various components to communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately.

You can configure lookup service on the NSX Manager and provide the SSO administrator credentials to register NSX Management Service as an SSO user. Integrating the single sign on (SSO) service with NSX improves the security of user authentication for vCenter users and enables NSX to authenticate users from other identity services such as AD, NIS, and LDAP. With SSO, NSX supports authentication using authenticated Security Assertion Markup Language (SAML) tokens from a trusted source via REST API calls. NSX Manager can also acquire authentication SAML tokens for use with other VMware solutions.
NSX caches group information for SSO users. Changes to group memberships will take up to 60 minutes to propagate from the identity provider (for example, active directory) to NSX.

Prerequisites

- To use SSO on NSX Manager, you must have vCenter Server 5.5 or later, and single sign on (SSO) authentication service must be installed on the vCenter Server. Note that this is for embedded SSO. Instead, your deployment might use an external centralized SSO server.
  
  For information about SSO services provided by vSphere, see [http://kb.vmware.com/kb/2072435](http://kb.vmware.com/kb/2072435) and [http://kb.vmware.com/kb/2113115](http://kb.vmware.com/kb/2113115).

- NTP server must be specified so that the SSO server time and NSX Manager time is in sync.
  
  For example:

<table>
<thead>
<tr>
<th>Time Settings</th>
<th>Unconfigure NTP Servers</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>192.168.110.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timezone</td>
<td>UTC</td>
</tr>
<tr>
<td>Date/Time</td>
<td>12/28/2016 21:31:49</td>
</tr>
</tbody>
</table>

Procedure

1. Log in to the NSX Manager virtual appliance.
   
   In a Web browser, navigate to the NSX Manager appliance GUI at https://<nsx-manager-ip> or https://<nsx-manager-hostname>, and log in as admin with the password that you configured during NSX Manager installation.

2. Log in to the NSX Manager virtual appliance.

3. From the home page, click Manage Appliance Settings > NSX Management Service.

4. Click Edit in the Lookup Service URL section.

5. Enter the name or IP address of the host that has the lookup service.

6. Enter the port number.
   - Enter port 443 if you are using vSphere 6.0. For vSphere 5.5, use port number 7444.
   - The Lookup Service URL is displayed based on the specified host and port.

7. Enter the SSO Administrator user name and password, and click OK.
   - The certificate thumbprint of the SSO server is displayed.
8. Check that the certificate thumbprint matches the certificate of the SSO server.

If you installed a CA-signed certificate on the CA server, you are presented with the thumbprint of the CA-signed certificate. Otherwise, you are presented with a self-signed certificate.

9. Confirm that the Lookup Service status is **Connected**.

For example:

<table>
<thead>
<tr>
<th>Lookup Service URL:</th>
<th><a href="https://psc-01a.corp.local:443/lookupservice/sdk">https://psc-01a.corp.local:443/lookupservice/sdk</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO Administrator User Name:</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Status:</td>
<td><img src="connected.png" alt="Connected" /></td>
</tr>
</tbody>
</table>

**What to do next**

See Assign a Role to a vCenter User, in the *NSX Administration Guide*.

**Managing User Rights**

A user’s role defines the actions the user is allowed to perform on a given resource. The role determines the user’s authorized activities on the given resource, ensuring that a user has access only to the functions necessary to complete applicable operations. This allows domain control over specific resources, or system-wide control if your right has no restrictions.

The following rules are enforced:

- A user can have only one role.
- You cannot add a role to a user or remove an assigned role from a user. You can, however, change the assigned role for a user.

**Table 20-1. NSX Manager User Roles**

<table>
<thead>
<tr>
<th>Right</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Administrator</td>
<td>NSX operations and security.</td>
</tr>
<tr>
<td>NSX Administrator</td>
<td>NSX operations only: for example, install virtual appliances, configure port groups.</td>
</tr>
<tr>
<td>Security Administrator</td>
<td>NSX security only: for example, define distributed firewall rules, configure NAT and load balancer services.</td>
</tr>
<tr>
<td>Auditor</td>
<td>Read only.</td>
</tr>
</tbody>
</table>

The Enterprise Administrator and NSX Administrator roles can be assigned only to vCenter users.

**Managing the Default User Account**

The NSX Manager user interface includes a user account, which has access rights to all resources. You cannot edit the rights of or delete this user. The default user name is **admin** and the default password is **default** or the password you specified during NSX Manager installation.

You can manage NSX Manager appliance **admin** user only through CLI commands.
Assign a Role to a vCenter User

When you assign a role to an SSO user, vCenter authenticates the user with the identity service configured on the SSO server. If the SSO server is not configured or is not available, the user is authenticated either locally or with Active Directory based on vCenter configuration.

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Managers**.
3. Click an NSX Manager in the Name column and then click the **Manage** tab.
4. Click **Users**.
5. Click **Add**.
   - The Assign Role window opens.
6. Click **Specify a vCenter user** or **Specify a vCenter group**.
7. Type the vCenter **User** or **Group** name for the user.
   - Refer to the example below for more information.
   - Domain name: corp.vmware.com
   - Alias: corp
   - Group name: group1@corp.vmware.com
   - User name: user1@corp.vmware.com
   - When a group is assigned a role on the NSX Manager any user from that group can be logged in to the NSX Manager user interface.
   - When assigning a role to a user, type the user alias. For example, user1@corp.
8. Click **Next**.
9. Select the role for the user and click **Next**. For more information on the available roles, see Managing User Rights.
10. Click **Finish**.
   - The user account appears in the Users table.

Understanding Group-Based Role Assignments

Organizations create user groups for proper user management. After integration with SSO, NSX Manager can get the details of groups to which a user belongs. Instead of assigning roles to individual users who may belong to the same group, NSX Manager assigns roles to groups. The following scenarios illustrate how NSX Manager assigns roles.

Example: Role-Based Access Control Scenario

This scenario provides an IT network engineer (Sally Moore) access to NSX components in the following environment.
AD domain: corp.local, vCenter group: neteng@corp.local, user name: smoore@corp.local

Prerequisites: vCenter Server has been registered with NSX Manager, and SSO has been configured. Note that SSO is required only for Groups.

1. Assign a role to Sally.
   a. Log in to the vSphere Web Client.
   b. Click Networking & Security and then click NSX Managers.
   c. Click an NSX Manager in the Name column and then click the Manage tab.
   d. Click Users and then click Add.
      The Assign Role window opens.
   e. Click Specify a vCenter group and type neteng@corp.local in Group.
   f. Click Next.
   g. In Select Roles, click NSX Administrator and then click Next.

2. Grant Sally permission to the datacenter.
   a. Click the Home icon and then click vCenter Home > Datacenters.
   b. Select a datacenter and click Actions > All vCenter Actions > Add Permission.
   c. Click Add and select the domain CORP.
   d. In Users and Groups, select Show Groups First.
   e. Select NetEng and click OK.
   f. In Assigned Role, select Read-only and un-select Propagate to children and click OK.

3. Log out of vSphere Web Client and log back in as smoore@corp.local.
   Sally can perform NSX operations only. For example, install virtual appliances, create logical switches, and so on.

Example: Inherit Permissions Through a User-Group Membership Scenario

<table>
<thead>
<tr>
<th>Group option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>G1</td>
</tr>
<tr>
<td>Role assigned</td>
<td>Auditor (Read only)</td>
</tr>
<tr>
<td>Resources</td>
<td>Global root</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>John</td>
</tr>
<tr>
<td>Belongs to group</td>
<td>G1</td>
</tr>
<tr>
<td>Role assigned</td>
<td>None</td>
</tr>
</tbody>
</table>
John belongs to group G1, which has been assigned the auditor role. John inherits the group role and resource permissions.

**Example: User Member of Multiple Groups Scenario**

<table>
<thead>
<tr>
<th>Group option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>G1</td>
</tr>
<tr>
<td>Role assigned</td>
<td>Auditor (Read only)</td>
</tr>
<tr>
<td>Resources</td>
<td>Global root</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>G2</td>
</tr>
<tr>
<td>Role assigned</td>
<td>Security Administrator (Read and Write)</td>
</tr>
<tr>
<td>Resources</td>
<td>Datacenter1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Joseph</td>
</tr>
<tr>
<td>Belongs to group</td>
<td>G1, G2</td>
</tr>
<tr>
<td>Role assigned</td>
<td>None</td>
</tr>
</tbody>
</table>

Joseph belongs to groups G1 and G2 and inherits a combination of the rights and permissions of the Auditor and Security Administrator roles. For example, John has the following permissions:

- Read, write (Security Administrator role) for Datacenter1
- Read only (Auditor) for global root

**Example: User Member of Multiple Roles Scenario**

<table>
<thead>
<tr>
<th>Group option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>G1</td>
</tr>
<tr>
<td>Role assigned</td>
<td>Enterprise Administrator</td>
</tr>
<tr>
<td>Resources</td>
<td>Global root</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Bob</td>
</tr>
<tr>
<td>Belongs to group</td>
<td>G1</td>
</tr>
<tr>
<td>Role assigned</td>
<td>Security Administrator (Read and Write)</td>
</tr>
<tr>
<td>Resources</td>
<td>Datacenter1</td>
</tr>
</tbody>
</table>

Bob has been assigned the Security Administrator role, so he does not inherit the group role permissions.

Bob has the following permissions:

- Read, write (Security Administrator role) for Datacenter1 and its child resources
- Enterprise Administrator role on Datacenter1
Create a User with Web Interface Access Using CLI

You can create an NSX user having web interface access using CLI. You can use this user account to access and operate different plug-ins or use it for auditing purposes.

Procedure

1. Create a CLI user account. You can create a CLI user account for each NSX virtual appliance. To create a CLI user account, perform the following steps:

   a. Log in to the vSphere Web Client, and select an NSX Manager virtual appliance.
   b. Click the Console tab to open a CLI session.
   c. Log in to the CLI session using the Administrator account and password that you specified while installing NSX Manager. For example,

      ```
      nsx-mgr> enable
      Password:
      nsx-mgr>
      ```

   d. Switch to Privileged mode from Basic mode using the `enable` command as follows:

      ```
      nsx-mgr> enable
      Password:
      nsx-mgr#
      ```

   e. Switch to Configuration mode from Privileged mode using the `configure terminal` command as follows:

      ```
      nsx-mgr# configure terminal
      nsx-mgr(config)#
      ```

   f. Add a CLI user account using the `user username password (hash | plaintext) password` command. For example,

      ```
      nsx-mgr(config)# user cliuser password plaintext abcd1234
      ```

      **Note**  User name with capital letter is not allowed.

   g. Save the configuration as follows:

      ```
      nsx-mgr(config)# write memory
      Configuration saved
      [OK]
      ```
2  Now provide web interface privilege which will enable the user to login to NSX Manager virtual appliance and allows the execution of appliance management REST APIs as follows:
   a  Verify that you are in Configuration mode as follows:

```bash
nsx-mgr# configure terminal
nsx-mgr(config)#
```

   b  Allow the created CLI user to run the REST API calls using the user username privilege web-interface command. For example:

```bash
nsx-mgr(config)# user userName privilege web-interface
nsx-mgr(config)# user cliuser privilege web-interface
```

3  (Optional) You can verify the running configuration as follows:

```bash
nsx-mgr# show running-config
Building configuration...

Current configuration:
!
user cliuser
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
hostname nsxmgr-01a
!
interface mgmt
  ip address 192.168.110.15/24
!
ip route 0.0.0.0/0 192.168.110.1
!
web-manager
```

4  Exit from the CLI session.

```bash
nsx-mgr#(config)# exit
nsx-mgr# exit
```

The created user is not listed under Networking & Security > NSX Managers “Select your NSX Manager” > Manage > Users tab. Also there is no role assigned to the user.
Assign the required role to the user using the REST API. You can assign auditor (Auditor), security_admin (Security Administrator), or super_user (System Administrator) role as follows:

```xml
POST - https://<NSX-IP>/api/2.0/services/usermgmt/role/<username>?isCli=true
<accessControlEntry>
  <role>auditor</role> # Enter the required role #
  <resource>
    <resourceId>globalroot-0</resourceId>
  </resource>
</accessControlEntry>
```

Results

The NSX CLI user is created with web interface access.

What to do next

You can log in to vSphere Web Client using the credentials provided while creating the user.

For more information on CLI, refer to NSX Command Line Interface Reference.

For more information on API, refer to NSX API Guide.

Edit a User Account

You can edit a user account to change the role or scope. You cannot edit the admin account.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
4. Click Users.
5. Select the user you want to edit.
6. Click Edit.
7. Make changes as necessary.
8. Click Finish to save your changes.

Change a User Role

You can change the role assignment for all users, except for the admin user.

Procedure

1. Log in to the vSphere Web Client.
2 Click Networking & Security and then under Networking & Security Inventory click NSX Managers.

3 Click an NSX Manager in the Name column and then click the Manage tab.

4 Click Users.

5 Select the user you want to change the role for.

6 Click Change Role.

7 Make changes as necessary.

8 Click Finish to save your changes.

**Disable or Enable a User Account**

You can disable a user account to prevent that user from logging in to the NSX Manager. You cannot disable the admin user or a user who is currently logged into the NSX Manager.

**Procedure**

1 Log in to the vSphere Web Client.

2 Click Networking & Security and then under Networking & Security Inventory click NSX Managers.

3 Click an NSX Manager in the Name column and then click the Manage tab.

4 Click Users.

5 Select a user account.

6 Click the Enable or Disable icon.

**Delete a User Account**

You can delete any created user account. You cannot delete the admin account. Audit records for deleted users are maintained in the database and can be referenced in an Audit Log report.

**Procedure**

1 Log in to the vSphere Web Client.

2 Click Networking & Security and then under Networking & Security Inventory click NSX Managers.

3 Click an NSX Manager in the Name column and then click the Manage tab.

4 Click Users.

5 Select a user account.

6 Click Delete.
7 Click **OK** to confirm deletion.

If you delete a vCenter user account, only the role assignment for NSX Manager is deleted. The user account on vCenter is not deleted.
Network and Security Objects

This section describes custom network and security containers. These containers can be used in Distributed Firewall and Service Composer. In a cross-vCenter NSX environment you can create universal network and security containers to be used in universal distributed firewall rules. You cannot use universal network and security objects in Service Composer.

Note Duplicate names are allowed when you create a group with universal scope. You can provide duplicate names when you select Mark this object for Universal Synchronization option while creating the following groups:

- IP Address Group
- MAC Address Group
- Security Group
- Services and Service Group

This chapter includes the following topics:

- Working with IP Address Groups
- Working with MAC Address Groups
- Working with IP Pools
- Working with Security Groups
- Working with Services and Service Groups

Working with IP Address Groups

Create an IP Address Group

You can create an IP address group and then add this group as the source or destination in a firewall rule. Such a rule can help protect physical machines from virtual machines or the reverse.
**Prerequisites**

VMware Tools must be installed on each VM, or an enabled IP discovery method (DHCP snooping or ARP snooping, or both) must be in place to when using grouping objects instead of IP addresses. For more details, refer to [IP Discovery for Virtual Machines](#).

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then under **Networking & Security Inventory** click **NSX Managers**.
3. Click an NSX Manager in the **Name** column and then click the **Manage** tab.
   - You must select the primary NSX Manager if you need to manage universal IP address groups.
4. Click the **Grouping Objects** tab, then click **IP Sets**.
5. Click the **Add (✚)** icon.
6. Type a name for the address group.
7. (Optional) Type a description for the address group.
8. Type the IP addresses or a range of IP addresses to be included in the group.

   **Caution** While entering IPv6 address ranges in the IP sets, ensure that you break the address ranges into /64. Otherwise, the publishing of the firewall rules fails.

9. (Optional) Select **Enable inheritance to allow visibility at underlying scopes**.
10. (Optional) Select **Mark this object for Universal Synchronization** to create a universal IP address group.
11. Click **OK**.

**Edit an IP Address Group**

**Prerequisites**

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then under **Networking & Security Inventory** click **NSX Managers**.
3. Click an NSX Manager in the **Name** column and then click the **Manage** tab.
   - You must select the primary NSX Manager if you need to manage universal IP address groups.
4. Click the **Grouping Objects** tab, then click **IP Sets**.
5. Select the group that you want to edit and click the **Edit (✎)** icon.
6  In the Edit IP Sets dialog box, make the appropriate changes.
7  Click OK.

**Delete an IP Address Group**

**Procedure**

1  Log in to the vSphere Web Client.
2  Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3  Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal IP address groups.
4  Click the Grouping Objects tab and then click IP Sets.
5  Select the group that you want to delete and click the Delete (x) icon.

**Working with MAC Address Groups**

**Create a MAC Address Group**

You can create a MAC address group consisting of a range of MAC addresses and then add this group as the source or destination in a Distributed Firewall rule. Such a rule can help protect physical machines from virtual machines or vice versa.

**Procedure**

1  Log in to the vSphere Web Client.
2  Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3  Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal MAC address groups.
4  Click the Grouping Objects tab and then click MAC Sets.
5  Click the Add (+) icon.
6  Type a name for the address group.
7  (Optional) Type a description for the address group.
8  Type the MAC addresses to be included in the group.
9  (Optional) Select Enable inheritance to allow visibility at underlying scopes.
10  (Optional) Select Mark this object for Universal Synchronization to create a universal MAC address group.
11  Click OK.

**Edit a MAC Address Group**

**Procedure**
1  Log in to the vSphere Web Client.
2  Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3  Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal MAC address groups.
4  Click the Grouping Objects tab and then click MAC Sets.
5  Select the group that you want to edit and click the Edit (📝) icon.
6  In the Edit MAC Set dialog box, make the appropriate changes.
7  Click OK.

**Delete a MAC Address Group**

**Procedure**
1  Log in to the vSphere Web Client.
2  Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3  Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal MAC address groups.
4  Click the Grouping Objects tab and then click MAC Sets.
5  Select the group that you want to delete and click the Delete (❌) icon.

**Working with IP Pools**

You can create an IP pool to specify a range of IP addresses.

**Create an IP Pool**
Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
4. Click the Grouping Objects tab and then click IP Pool.
5. Click the Add New IP Pool icon.
6. Type a name for the IP pool and type the default gateway and prefix length.
7. (Optional) Type the primary and secondary DNS and the DNS suffix.
8. Type the IP address ranges to be included in the pool and click OK.

Edit an IP Pool
You can edit an IP pool - you cannot edit the CIDR and gateway.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
4. Click the Grouping Objects tab and then click IP Pools.
5. Select an IP pool and click the Edit icon.
6. Make the appropriate changes and click OK.

Delete IP Pool

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
4. Click the Grouping Objects tab and then click IP Pool.
5. Select the IP pool that you want to delete and click the Delete icon.

Working with Security Groups
A security group is a collection of assets or grouping objects from your vSphere inventory.
Security Groups are containers that can contain multiple object types including logical switch, vNIC, IPset, and Virtual Machine (VM). Security groups can have dynamic membership criteria based on security tags, VM name or logical switch name. For example, all VM's that have the security tag "web" will be automatically added to a specific security group destined for Web servers. After creating a security group, a security policy is applied to that group.

In a cross-vCenter NSX environment, universal security groups are defined on the primary NSX manager and are marked for universal synchronization with secondary NSX managers. Universal security groups cannot have dynamic membership criteria defined unless they are marked for use in an active standby deployment scenario.

In a cross-vCenter NSX environment with an active standby deployment scenario, the SRM creates a placeholder VM on the recovery site for every protected VM on the active site. The placeholder VMs are not active, and stay in the standby mode. When the protected VM goes down, the placeholder VMs on the recovery site are powered on and take over the tasks of the protected VM. Users create distributed firewall rules with universal security groups containing universal security tags on the active site. The NSX manager replicates the distributed firewall rule with the universal security groups containing universal security tags on the placeholder VMs and when the placeholder VMs are powered on the replicated firewall rules with the universal security groups and universal security tags are enforced correctly.

Note

- Universal security groups created prior to 6.3 cannot be edited for use in active standby deployments.

Create a Security Group

You create a security group at the NSX Manager level.

Universal security groups are used in two types of deployments: active active cross-vCenter NSX environments, and active standby cross-vCenter NSX environments, where one site is live at a given time and the rest are on standby.

- Universal security groups in an active active environment can contain the following included objects only: security groups, IP sets, MAC sets. You cannot configure dynamic membership or excluded objects.
- Universal security groups in an active standby environment can contain the following included objects: security groups, IP sets, MAC sets, universal security tags. You can also configure dynamic membership using VM Name only. You cannot configure excluded objects.

Note

- Universal security groups created prior to 6.3 cannot be edited for use in active standby deployments.

Prerequisites

If you are creating a security group based on Active Directory group objects, ensure that one or more domains have been registered with NSX Manager. NSX Manager gets group and user information as well as the relationship between them from each domain that it is registered with. See Register a Windows Domain with NSX Manager.
Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then under **Networking & Security Inventory** click **NSX Managers**.
3. Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal security groups.
4. Click the Grouping Objects tab, click Security Group, then click the Add Security Group icon.
5. Type a name and optionally a description for the security group.
6. (Optional) If you are creating a universal security group, select **Mark this object for universal synchronization**.
7. (Optional) If you are creating a universal security group for use in an active standby deployment, select both **Mark this object for universal synchronization** and **Use for active standby deployments**. Dynamic membership for universal security groups with active standby deployment is based on virtual machine name.
8. Click Next.
9. On the Dynamic Membership page, define the criteria that an object must meet for it to be added to the security group you are creating. This gives you the ability to include virtual machines by defining a filter criteria with a number of parameters supported to match the search criteria.
   
   **Note** If you are creating a universal security group, the Define dynamic membership step is not available in active active deployments. It is available in active standby deployments, based on virtual machine name only.

For example, you may include a criterion to add all virtual machines tagged with the specified security tag (such as AntiVirus.virusFound) to the security group. Security tags are case sensitive.

Or you can add all virtual machines containing the name W2008 and virtual machines that are in the logical switch global_wire to the security group.

10. Click Next.
On the Select objects to include page, select the tab for the resource you want to add and select one or more resources to add to the security group. You can include the following objects in a security group.

Table 21-1. Objects that can be included in security groups and universal security groups.

<table>
<thead>
<tr>
<th>Security Group</th>
<th>Universal Security Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other security groups to nest within the security</td>
<td>Other universal security groups to nest within the universal</td>
</tr>
<tr>
<td>group you are creating.</td>
<td>security group you are creating.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Universal IP sets</td>
</tr>
<tr>
<td>Logical Switch</td>
<td>Universal MAC sets</td>
</tr>
<tr>
<td>Network</td>
<td>Universal Security Tag (active standby deployments only)</td>
</tr>
<tr>
<td>Virtual App</td>
<td></td>
</tr>
<tr>
<td>Datacenter</td>
<td></td>
</tr>
<tr>
<td>IP sets</td>
<td></td>
</tr>
<tr>
<td>Directory Groups</td>
<td></td>
</tr>
</tbody>
</table>

**Note** The Active Directory configuration for NSX security groups is different from the AD configuration for vSphere SSO. NSX AD group configuration is for end users accessing guest virtual machines, while vSphere SSO is for administrators using vSphere and NSX. In order to consume these directory groups you must sync with Active Directory. See Chapter 11 Identity Firewall Overview.

| MAC Sets                                           |                                                                |
| Security tag                                       |                                                                |
| vNIC                                               |                                                                |
| Virtual Machine                                    |                                                                |
| Resource Pool                                      |                                                                |
| Distributed Virtual Port Group                     |                                                                |

The objects selected here are always included in the security group regardless of whether or not they match the criteria in **Step Step 8**.

When you add a resource to a security group, all associated resources are automatically added. For example, when you select a virtual machine, the associated vNIC is automatically added to the security group.

12 Click **Next** and select the objects that you want to exclude from the security group.

**Note** If you are creating a universal security group, the **Select objects to exclude** step is not available.

The objects selected here are always excluded from the security group regardless of whether or not they match the dynamic criteria.

13 Click **Next**.

The **Ready to Complete** window appears with a summary of the security group.

14 Click **Finish**.
Example

Membership of a security group is determined as follows:

\[ \text{Expression result (derived from Define dynamic membership)} + \text{Inclusions (specified in Select objects to include)} - \text{Exclusion (specified in Select objects to exclude)} \]

This means that inclusion items are first added to the expression result. Exclusion items are then subtracted from the combined result.

Edit a Security Group

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal security groups.
4. Click the Grouping Objects tab and then click Security Group.
   - Note that universal security groups created prior to 6.3 cannot be edited for use in active standby deployments.
5. Select the group that you want to edit and click the Edit (📝) icon.
6. In the Edit Security Group dialog box, make the appropriate changes.
7. Click OK.

Delete a Security Group

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal security groups.
4. Click the Grouping Objects tab and then click Security Group.
5. Select the group that you want to delete and click the Delete (☒) icon.
Working with Services and Service Groups

A service is a protocol-port combination, and a service group is a group of services or other service groups.

Create a Service

You can create a service and then define rules for that service.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal services.
4. Click the Grouping Objects tab and then click Service.
5. Click the Add \(\text{add button}^{\text{icon}}\) icon.
6. Type a Name to identify the service.
7. (Optional) Type a Description for the service.
8. Select a Protocol.
   - Depending on the protocol selected, you may be prompted to enter further information, such as destination port.
9. (Optional) Select Enable inheritance to allow visibility at underlying scopes.
10. (Optional) Select Mark this object for Universal Synchronization to create a universal service.
11. Click OK.

Results

The service appears in the Services table.

Create a Service Group

You can create a service group and then define rules for that service group.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Manage tab.
   - You must select the primary NSX Manager if you need to manage universal service groups.
4. Click the **Grouping Objects** tab and then click **Service Groups**.

5. Click the **Add** icon.

6. Type a **Name** to identify the service group.

7. (Optional) Type a **Description** for the service group.

8. (Optional) Select **Mark this object for Universal Synchronization** to create a universal service group.

9. In Members, select the services or service groups that you want to add to the group.

10. (Optional) Select **Enable inheritance to allow visibility at underlying scopes**.

11. Click **OK**.

### Edit a Service or Service Group

You can edit services and service groups.

**Procedure**

1. Log in to the vSphere Web Client.

2. Click **Networking & Security** and then under **Networking & Security Inventory** click **NSX Managers**.

3. Click an NSX Manager in the **Name** column and then click the **Manage** tab.

   - You must select the primary NSX Manager if you need to manage universal services or service groups.

4. Click the **Grouping Objects** tab and then click **Service** or **Service Groups**.

5. Select a custom service or service group and click the **Edit (📝)** icon.

6. Make the appropriate changes.

7. Click **OK**.

### Delete a Service or Service Group

You can delete services or service group.

**Procedure**

1. Log in to the vSphere Web Client.

2. Click **Networking & Security** and then under **Networking & Security Inventory** click **NSX Managers**.

3. Click an NSX Manager in the **Name** column and then click the **Manage** tab.

   - You must select the primary NSX Manager if you need to manage universal services or service groups.
4 Click the **Grouping Objects** tab and then click **Service** or **Service Groups**.

5 Select a custom service or service group and click the **Delete (×) icon**.

6 Click **Yes**.

   The service or service group is deleted.
This chapter includes the following topics:

- Using the NSX Dashboard
- Check Communication Channel Health
- NSX Controller
- Change VXLAN Port
- Customer Experience Improvement Program
- About NSX Logs
- Audit Logs
- System Events
- Management System Settings
- NSX Backup and Restore
- Flow Monitoring
- Application Rule Manager
- Activity Monitoring
- Endpoint Monitoring Data Collection
- Traceflow

Using the NSX Dashboard

The NSX dashboard provides visibility to the overall health of NSX components in one central view. NSX dashboard simplifies troubleshooting by displaying status of different NSX components such as NSX Manager, controllers, logical switches, host preparation, service deployment, backup as well as edge notifications.

1. Log in to the vSphere Web Client.
2. Click Networking & Security, and then click Dashboard. The Dashboard page is displayed.
3. In a Cross-vCenter NSX environment, select the NSX Manager with primary role or secondary role.
Dashboard provides the following information:

- **NSX infrastructure—NSX Manager component status for following services is monitored:**
  - Database service (vPostgres).
  - Message bus service (RabbitMQ).
  - Replicator service—Also monitors for replication errors (if Cross-vCenter NSX is enabled).

- **NSX Manager disk usage:**
  - Yellow indicates disk usage > 80%.
  - Red indicates disk usage > 90%.

- **NSX infrastructure—NSX Controller status:**
  - Controller node status (up/down/running/deploying/removing/failed/unknown).
  - Controller peer connectivity status is displayed. If controller is down indicated as Red, then peer controllers are displayed as Yellow.
  - Controller VM status (powered off/deleted).
  - Controller disk latency alerts.

- **NSX Manager backup status:**
  - Backup schedule.
  - Last backup status (Failed/successful/not scheduled along with date and time).
  - Last backup attempt (date and time with details).
  - Last successful backup (date and time with details).
- NSX infrastructure—Host status for following services is monitored:
  - Deployment related:
    - Number of clusters with installation failed status.
    - Number of clusters that need upgrade.
    - Number of clusters where installation is in progress.
    - Number of unprepared clusters.
  - Firewall:
    - Number of clusters with firewall disabled.
    - Number of clusters where firewall status is yellow/red:
      - Yellow indicates that the distributed firewall is disabled on any of the clusters.
      - Red indicates that the distributed firewall was unable to get installed on any of the hosts/clusters.
  - VXLAN:
    - Number of clusters with VXLAN not configured.
    - Number of clusters where VXLAN status is green/yellow/red:
      - Green indicates that the feature was successfully configured.
      - Yellow means busy when VXLAN configuration is in-progress.
      - Red (error) indicates the state when VTEP creation failed, VTEP could not find the IP address, VTEP got LinkLocal IP address assigned, and so on.
- NSX infrastructure—Service deployment status
  - Deployment failures—installation status for the failed deployments.
- Service status—for all the failed services.

- NSX infrastructure—NSX Edge notifications

  Edge notifications dashboard highlights active alarms for certain services. It monitors list of critical events that are listed below and tracks them till the issue is unresolved. Alarms are auto resolved when recovery event is reported, or edge is force synced, redeployed or upgraded.

  - Load balancer (edge load balancer server status):
    - Edge load balancer back end server is down.
    - Edge load balancer back end server warning status.

  - VPN (IPSec tunnel / IPSec channel status):
    - Edge IPSec channel is down.
    - Edge IPSec tunnel is down.

  - Appliance (edge VM, edge gateway, edge file system, NSX Manager, and edge services gateway reports status):
    - Edge services gateway missing health check pulse.
    - Edge VM got powered off.
    - Edge VM missing health check pulse.
    - NSX Edge reports bad state.
    - NSX Manager reports that edge services gateway is in bad state.
    - Edge VM is not present in VC inventory.
    - HA split brain detected.

  **Note** Load balancer and VPN alarms are not auto cleared on configuration update. Once the issue is resolved, you have to clear the alarms manually with API using the `alarm-id` command. Here is the example of API that you can use to clear the alarms. For details, refer to *NSX API Guide*.

  ```plaintext
  GET https://<<NSX-IP>>/api/2.0/services/alarms/{source-Id}
  POST https://<<NSX-IP>>/api/2.0/services/alarms?action=resolve

  GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
  POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
  ```

- NSX services—Firewall Publish status:

  - Number of hosts with Firewall Publish status as failed. Status is Red when any host do not successfully apply the published distributed firewall configuration.

- NSX services—Logical Networking status:

  - Number of logical switches with status Error or Warning.
- Flags when backed distributed virtual port group is deleted from vCenter Server.

Check Communication Channel Health

NSX checks on the status of communication between NSX Manager and firewall agent, NSX Manager and control plane agent, and control plane agent and controllers.

Procedure

1. In the vSphere Web Client, navigate to Networking & Security > Installation > Host Preparation.
2. Select a cluster or expand clusters and select a host. Click Actions (≡) then Communication Channel Health.

The communication channel health information is displayed.

![Communication Channel Health screen](image)

NSX Controller

You can manage NSX Controller instances.

For information about troubleshooting controller cluster issues, including deleting controllers safely, refer to the NSX Controller section in the NSX Troubleshooting Guide.

Change Controller Password

To ensure security, you can change passwords for NSX controllers.
Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **Installation**.
3. Under Management, select the controller for which you want to change the password.
4. Click **Actions** and then click **Change Controller Cluster Password**.
5. Type a new password and click **OK**.

   The controller password has changed.

**Download Technical Support Logs for NSX Controller**

You can download technical support logs for each NSX Controller instance. These product specific logs contain diagnostic information for analysis.

To collect NSX Controller logs:

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security**, and then click **Installation**.
3. Under **Management**, select the controller that you want to download logs from.
4. Click **Download tech support logs**.
5. Click **Download**.

   The NSX Manager starts downloading the NSX Controller log and acquires the lock.

   **Note**   Download one NSX Controller log at a time. Once the first one completes, start downloading the other. An error might occur if you download logs from multiple controllers simultaneously.

6. After the log is ready, click **Save** to download the log to your desktop.

   The log is compressed and has **.gz** file extension.

**Results**

You can now analyze the downloaded logs.

**What to do next**

If you want to upload diagnostic information for VMware technical support, refer to the Knowledge Base article 2070100.

**Configuring a Syslog Server for NSX Controller**

If you configure a syslog server for NSX controllers, NSX Manager sends all audit logs and system events to the syslog server. Syslog data is useful for troubleshooting and reviewing data logged during
installation and configuration. The only supported method on configuring the syslog server on the NSX controllers is through the NSX API. VMware recommends using UDP as the protocol for syslog.

**Procedure**

1. To enable syslog on NSX Controller, use the following NSX API. It adds controller syslog exporter and configures a syslog exporter on the specified controller node.

   ```xml
   Request
   POST https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
   Request Body:
   <controllerSyslogServer>
   <syslogServer>10.135.14.236</syslogServer>
   <port>514</port>
   <protocol>UDP</protocol>
   <level>INFO</level>
   </controllerSyslogServer>
   ```

2. You can query the controller syslog exporter and retrieve details about the configured syslog exporter on the specified controller node using the following NSX API.

   ```xml
   Request
   GET https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
   Response Body:
   <?xml version="1.0" encoding="UTF-8"?>
   <controllerSyslogServer>
   <syslogServer>10.135.14.236</syslogServer>
   <port>514</port>
   <protocol>UDP</protocol>
   <level>INFO</level>
   </controllerSyslogServer>
   ```

3. If not required, you can delete controller syslog exporter on the specified controller node using the following NSX API.

   ```xml
   Request
   DELETE https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
   ```

**What to do next**

For more details on API, refer to *NSX API Guide*.

**Change VXLAN Port**

You can change the port used for VXLAN traffic.

In NSX 6.2.3 and later, the default VXLAN port is 4789, the standard port assigned by IANA. Before NSX 6.2.3, the default VXLAN UDP port number was 8472.

Any new NSX installations will use UDP port 4789 for VXLAN.
If you upgrade from NSX 6.2.2 or earlier to NSX 6.2.3 or later, and your installation used the old default (8472), or a custom port number (for example, 8888) before the upgrade, that port will continue to be used after the upgrade unless you take steps to change it.

If your upgraded installation uses or will use hardware VTEP gateways (ToR gateways), you must switch to VXLAN port 4789.

Cross-vCenter NSX does not require that you use 4789 for the VXLAN port, however, all hosts in a cross-vCenter NSX environment must be configured to use the same VXLAN port. If you switch to port 4789, this will ensure that any new NSX installations added to the cross-vCenter NSX environment are using the same port as the existing NSX deployments.

Changing the VXLAN port is done in a three phase process, and will not interrupt VXLAN traffic.

1. NSX Manager configures all hosts to listen for VXLAN traffic on both the old and new ports. Hosts continue to send VXLAN traffic on the old port.
2. NSX Manager configures all hosts to send traffic on the new port.
3. NSX Manager configures all hosts to stop listening on the old port, all traffic is sent and received on the new port.

In a cross-vCenter NSX environment you must initiate the port change on the primary NSX Manager. For each stage, the configuration changes are made on all hosts in the cross-vCenter NSX environment before proceeding to the next stage.

**Prerequisites**

- Verify that the port you want to use for VXLAN is not blocked by a firewall.
- Verify that host preparation is not running at the same time as the VXLAN port change.

**Procedure**

1. Click the Logical Network Preparation tab, then click VXLAN Transport.
2. Click the Change button in the VXLAN Port panel. Enter the port you want to switch to. 4789 is the port assigned by IANA for VXLAN.
   
   It will take a short time for the port change to propagate to all hosts.
3. (Optional) Check the progress of the port change with the GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus API request.

   ```
   GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
   ```

   ```xml
   <?xml version="1.0" encoding="UTF-8"?
   <vxlanPortUpdatingStatus>
     <prevPort>8472</prevPort>
     <targetPort>4789</targetPort>
     <taskPhase>PHASE_TWO</taskPhase>
     <taskStatus>PAUSED</taskStatus>
   </vxlanPortUpdatingStatus>
   ```
Customer Experience Improvement Program

NSX participates in VMware’s Customer Experience Improvement Program (CEIP).

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at https://www.vmware.com/solutions/trustvmware/ceip.html.

To join or leave the CEIP for NSX, or edit program settings, see Edit the Customer Experience Improvement Program Option.

Edit the Customer Experience Improvement Program Option

When you install or upgrade NSX Manager, you can choose to join the CEIP. You can join or leave the CEIP at a later time. You can also define the frequency and the days the information is collected.

Prerequisites

- Verify that the NSX manager is connected and can sync with vCenter Server.
- Verify that DNS is configured on NSX Manager.
- Verify that NSX is connected to a public network for uploading data.

Procedure

1. Log in to the vSphere Web Client.
4. Double-click the NSX Manager you want to modify.
5. Click the Summary tab.
6. Click Edit in the Customer Experience Improvement Program dialog box.
7. Select or deselect the Join the VMware Customer Experience Improvement Program option.
8. (Optional) Configure the recurrence settings.
9. Click OK.
About NSX Logs

You can configure the syslog server and view technical support logs for each NSX component. Management plane logs are available through NSX Manager and data plane logs are available through vCenter Server. Hence, it is recommended that you specify the same syslog server for the NSX component and vCenter Server in order to get a complete picture when viewing logs on the syslog server. For information on configuring a syslog server for hosts managed by a vCenter Server, see the appropriate version of vSphere documentation at https://docs.vmware.com.

**Note**  Syslog or jump servers used to collect logs and access an NSX Distributed Logical Router (DLR) Control VM can't be on the logical switch that is directly attached to that DLR's logical interfaces.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Logs</td>
<td>These logs are collected as part of the VM support bundle generated from vCenter Server. For more information on ESXi log files, refer to vSphere documentation.</td>
</tr>
<tr>
<td>NSX Edge Logs</td>
<td>Use the `show log [follow</td>
</tr>
<tr>
<td>NSX Manager Logs</td>
<td>Use the <code>show log</code> CLI command in the NSX Manager CLI. Download Technical Support Log bundle via the NSX Manager Virtual Appliance UI.</td>
</tr>
<tr>
<td>Routing Logs</td>
<td>See the NSX Logging and System Events Guide.</td>
</tr>
<tr>
<td>Firewall Logs</td>
<td>See NSX Logging and System Events Guide.</td>
</tr>
<tr>
<td>Guest Introspection Logs</td>
<td>See NSX Logging and System Events Guide.</td>
</tr>
</tbody>
</table>

### NSX Manager

To specify a syslog server, see [Configure a Syslog Server for NSX Manager](#).

To download technical support logs, see [Download Technical Support Logs for NSX](#).

### NSX Edge

To specify a syslog server, see [Configure Syslog Servers for NSX Edge](#).

To download technical support logs, see [Download Tech Support Logs for NSX Edge](#).

### NSX Controller

To specify a syslog server, see [Configuring a Syslog Server for NSX Controller](#).

To download technical support logs, see [Download Technical Support Logs for NSX Controller](#).

### Firewall

For more details, refer to [Firewall Logs](#).
Audit Logs

Audit logs for operations tracked by a ticket includes the ticket ID. With the NSX ticket logger feature, you can track the changes you make with a ticket ID.

Using NSX Ticket Logger

The NSX Ticket Logger allows you to track the infrastructure changes that you make. All operations are tagged with the specified ticket ID, and audit logs for these operations include the ticket ID. Log files for these operations are tagged with the same ticked ID.

Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click the **Manage** tab.
3. Click **Edit** next to **NSX Ticket Logger Settings**.
4. Type a ticket ID and click **Turn On**.

The NSX Ticket Logging pane is displayed at the right side of the vSphere Web Client window. Audit logs for the operations that you perform in the current UI session include the ticket ID in the **Operation Tags** column.

Figure 22-1. NSX Ticket Logger pane

If multiple vCenter Servers are being managed by the vSphere Web Client, the ticket ID is used for logging on all applicable NSX Managers.

What to do next

Ticket logging is session based. If ticket logging is on and you log out or if the session is lost, ticket logging will be turned off by default when you re-login to the UI. When you complete the operations for a ticket, you turn logging off by repeating steps 2 and 3 and clicking **Turn Off**.
View the Audit Log
The Audit Logs tab provides a view into the actions performed by all NSX Manager users. The NSX Manager retains up to 100,000 audit logs.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. In the Name column, click an NSX server and then click the Monitor tab.
4. Click the Audit Logs tab.
5. When details are available for an audit log, the text in the Operation column for that log is clickable. To view details of an audit log, click the text in the Operation column.
6. In the Audit Log Change Details, select Changed Rows to display only those properties whose values have changed for this audit log operation.

System Events
System events are events that are related to NSX operations. They are raised to detail every operational event. Events might relate to basic operation (Informational) or to a critical error (Critical).

View the System Event Report
From vSphere Web Client you can view the system events for all the components that are managed by NSX Manager.

Procedure
1. Log in to the vSphere Web Client.
2. Click Networking & Security and then under Networking & Security Inventory click NSX Managers.
3. Click an NSX Manager in the Name column and then click the Monitor tab.
4. Click the System Events tab.
   You can click the arrows in the column headers to sort events, or use the Filter text box to filter events.

Format of a System Event
If you specify a syslog server, NSX Manager sends all system events to the syslog server.

These messages have a format similar to the message displayed below:

```
Jan 8 04:35:00 NSXMGR 2017-01-08 04:35:00.422 GMT+00:00
INFO TaskFrameworkExecutor-18 SystemEventDaoImpl:133 –
```
System event contains the following information.

Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Event Message: Text containing detailed information about the event.
Module: Event component. May be the same as event source.
Universal Object: Value displayed is True or False.

Alarms

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an object. Alarms, along with other alerts, are displayed on the NSX Dashboard and other screens on the vSphere Web Client UI.

You can use the GET api/2.0/services/systemalarms API to view alarms on NSX objects.

NSX supports two methods for an alarm:

- Alarm corresponds to a system event and has an associated resolver that will attempt to resolve the issue that triggers the alarm. This approach is designed for network and security fabric deployment (for example, EAM, Message Bus, Deployment Plug-In), and is also supported by Service Composer. These alarms use the event code as the alarm code. For more details, refer to NSX Logging and System Events document.

- Edge notifications alarms are structured as a triggering and resolving alarm pair. This method is supported by several Edge functions, including IPSec VPN, load balancer, high availability, health check, edge file system, and resource reservation. These alarms use a unique alarm code which is not the same as the event code. For more details, refer to NSX Logging and System Events document.

Generally, an alarm gets automatically deleted by the system when the error condition is rectified. Some alarms are not auto cleared on a configuration update. Once the issue is resolved, you have to clear the alarms manually.

Here is an example of the API that you can use to clear the alarms.

You can get alarms for a specific source, for example, cluster, host, resource pool, security group, or NSX Edge. View alarms for a source by sourceld:

GET https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}
Resolve all alarms for a source by `sourceId`:

```plaintext
POST https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}?action=resolve
```

You can view NSX alarms, including Message Bus, Deployment Plug-In, Service Composer, and Edge alarms:

```plaintext
GET https://<<NSX-IP>>/api/2.0/services/systemalarms
```

You can view a specific NSX alarm by `alarmId`:

```plaintext
GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
```

You can resolve a specific NSX alarm by `alarmId`:

```plaintext
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

For more information on API, refer to NSX API Guide.

**Format of an Alarm**

You can view format of an alarm through API.

The format of an alarm contains the following information.

- **Event ID and Time**
- **Severity**: Possible values include informational, low, medium, major, critical, high.
- **Event Source**: Source where you should look to resolve the reported event.
- **Event Code**: Unique identifier for the event.
- **Message**: Text containing detailed information about the event.
- **Alarm ID**: ID of an alarm.
- **Alarm Code**: Event code which uniquely identifies the system alarm.
- **Alarm Source**: Source where you should look to resolve the reported event.

**Working with SNMP Traps**

The NSX Manager receives system events that are informational, warning, and critical from for example, the NSX Edge and hypervisor. The SNMP agent forwards the SNMP traps with OIDs to the SNMP receiver.

SNMP traps must have the SNMPv2c version. The traps must be associated with a management information base (MIB) so that the SNMP receiver can process the traps with object identifiers (OID).

By default, the SNMP trap mechanism is disabled. Enabling the SNMP trap only activates the critical and high severity notifications so that the SNMP manager does not get inundated by a high volume of notifications. An IP address or a host name defines the trap destination. For the host name to work for the trap destination, the device must be set up to query a Domain Name System (DNS) server.

When you enable the SNMP service, a `coldStart` trap with OID 1.3.6.1.6.3.1.1.5.1 is sent out the first time. A `warmStart` trap with OID 1.3.6.1.6.3.1.1.5.2 is sent out later on each stop-start to the configured SNMP receivers.
If the SNMP service remains enabled, a heartbeat trap vmwHbHeartbeat with OID 1.3.6.1.4.1.6876.4.190.0.401 is sent out every five minutes. When you disable the service, a vmwNsxMSnmpDisabled trap with OID 1.3.6.1.4.1.6876.90.1.2.1.0.1 is sent out. This process stops the vmwHbHeartbeat trap from running and disables the service.

When you add, modify, or delete a SNMP receiver value, a warmStart trap with OID 1.3.6.1.6.3.1.1.5.2 and vmwNsxMSnmpManagerConfigUpdated trap with OID 1.3.6.1.4.1.6876.90.1.2.1.0.2 is sent to the new or updated set of SNMP receivers.

**Note**  SNMP Polling is not supported.

**Configure SNMP Settings**

You can enable the SNMP settings and configure destination receivers to send traps that are critical, high, or informational.

**Prerequisites**

- Familiarize yourself with the SNMP trap mechanism. See [Working with SNMP Traps](#).
- Verify that an SNMP receiver is configured.
- Download and install the MIB module for the NSX Manager so that the SNMP receiver can process the traps with OID. See [http://kb.vmware.com/kb/1013445](http://kb.vmware.com/kb/1013445).

**Procedure**

1. Log in to the vSphere Web Client.
2. Select **Networking & Security > Networking & Security Inventory > NSX Managers**.
3. Select an NSX Manager IP address.
4. Select the Manage > System Events tabs.
5  Click **Edit** to configure the SNMP settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Sends out SNMP trap. By default, this option is disabled.</td>
</tr>
<tr>
<td>Group Notification</td>
<td>Predefined set of groups for some system events that are used to aggregate the events that are raised. By default, this option is enabled. For example, if a system event belongs to a group, the trap for these grouped events are withheld. Every five minutes a trap is sent out detailing the number of system events that have been received from the NSX Manager. The fewer traps being sent out save the SNMP receiver resources.</td>
</tr>
<tr>
<td>Receivers</td>
<td>Configure up to four receivers for traps to be sent out to. You must complete the following sections when you add an SNMP receiver. Receiver Address - IP address or the fully qualified domain name of the receiver host. Receiver Port - SNMP receiver default UDP port is 162. Community String - Information to be sent out as part of the notification trap. Enabled - Indicates whether this receiver is sending a trap.</td>
</tr>
</tbody>
</table>

6  Click **OK**.

**Results**

The SNMP service is enabled and traps are sent out to the receivers.

**What to do next**

Check whether the SNMP configuration works. See **Verify SNMP Trap Configuration**.

**Verify SNMP Trap Configuration**

Before you start editing an existing system trap, you must check whether the newly enabled SNMP service or updated SNMP is working properly.

**Prerequisites**

Verify that you have SNMP configured. See **Configure SNMP Settings**.

**Procedure**

1  Verify SNMP configuration and receiver connection.
   a  Select the **Manage > System Events** tabs.
   b  Click **Edit** to configure the SNMP settings.
      Do not change the settings in the dialog box.
   c  Click **OK**.

A warmStart trap with OID 1.3.6.1.6.3.1.1.5.2 is sent out to all the SNMP receivers.
2 Debug SNMP configuration or receiver problems.
   a If the SNMP receiver does not receive the traps, verify that the SNMP receiver is running on a configured port.
   b Check the accuracy of the receiver details under the SNMP settings section.
   c If the SNMP receiver stops receiving a vmwHbHeartbeat trap with OID 1.3.6.1.4.1.6876.4.190.0.401 every five minutes, check whether the NSX Manager appliance or the NSX Manager SNMP agent is working.
   d If the Heartbeat trap stops, check whether the SNMP service is disabled or test whether the network connectivity between the NSX Manager and the SNMP receiver is working.

Edit System Traps

You can edit a system trap to increase or decrease the severity and enablement of a trap so that traps are either sent out to receivers or withheld.

When the Module, SNMP OID, or SNMP trap enabled column value appears as --, it means that those events have not been allocated a trap OID. Therefore, a trap for these events is not going to be sent out.

A system trap has several columns that list different aspects of a system event.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Code</td>
<td>Static event code associated with an event.</td>
</tr>
<tr>
<td>Description</td>
<td>Summary describing the event.</td>
</tr>
<tr>
<td>Module</td>
<td>Sub component that triggers an event.</td>
</tr>
<tr>
<td>Severity</td>
<td>Level of an event can be informational, low, medium, major, critical, or high. By default when the SNMP service is enabled, traps are sent out for only critical and high severity events to highlight the traps that require immediate attention.</td>
</tr>
<tr>
<td>SNMP OID</td>
<td>Represents the individual OID and this OID is sent out when a system event is raised. Group notification is enabled by default. When group notifications is enabled, the events or traps under this group show the OID of the group the event or trap belongs to. For example, group notification OID categorized under configuration group has the OID 1.3.6.1.4.1.6876.90.1.2.0.1.0.1.</td>
</tr>
<tr>
<td>SNMP trap enabled</td>
<td>Shows whether sending out of the trap for this event is enabled or disabled. You can toggle the icon to individually an event or trap enablement. When group notification is enabled, you cannot toggle the trap enablement.</td>
</tr>
<tr>
<td>Filter</td>
<td>Search terms to filter the system traps.</td>
</tr>
</tbody>
</table>

Prerequisites

Verify that the SNMP settings are available. See Configure SNMP Settings.

Procedure

1 Log in to the vSphere Web Client.

3 Select an NSX Manager IP address.

4 Select the Manage > System Events tabs.

5 Select a system event under the System Traps section.

6 Click the Edit (edit) icon.

   Editing a trap enablement is not allowed when group notification is enabled. You can change the enablement of traps that do not belong to a group.

7 Change the severity of the system event from the drop-down menu.

8 If you change the severity from Informational to critical, check the Enable as SNMP Trap checkbox.

9 Click OK.

10 (Optional) Click the Enable (✓) icon or Disable (✗) icon in the header to enable or disable sending a system trap.

11 (Optional) Click the Copy (copy) icon to copy one or more event rows to your clipboard.

**Management System Settings**

You can edit the vCenter Server, DNS and NTP server, and Lookup server that you specified during initial login. NSX Manager requires communication with your vCenter Server and services such as DNS and NTP to provide details on your VMware Infrastructure inventory.

**Log In to the NSX Manager Virtual Appliance**

After you have installed and configured the NSX Manager virtual machine, log in to the NSX Manager virtual appliance to review the settings specified during installation.

**Procedure**

1 Open a Web browser window and type the IP address assigned to the NSX Manager. For example, https://192.168.110.42. The NSX Manager user interface opens in a web browser window using SSL.

2 Accept the security certificate.

   **Note** You can use an SSL certificate for authentication.

   The NSX Manager login screen appears.

3 Log in to the NSX Manager virtual appliance by using the user name admin and the password you set during installation.

4 Click Log In.

**NSX Manager Virtual Appliance Events**
The following events are specific to the NSX Manager virtual appliance.

### Table 22-2. NSX Manager Virtual Appliance Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Power Off</th>
<th>Power On</th>
<th>Interface Down</th>
<th>Interface Up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local CLI</td>
<td>Run show log follow command.</td>
<td>Run show log follow command.</td>
<td>Run show log follow command.</td>
<td>Run show log follow command.</td>
</tr>
<tr>
<td>GUI</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

### Table 22-3. NSX Manager Virtual Appliance Events

<table>
<thead>
<tr>
<th>Event</th>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local CLI</td>
<td>Run show process monitor command.</td>
<td>Run show system memory command.</td>
<td>Run show filesystem command.</td>
</tr>
<tr>
<td>GUI</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

### Edit the NSX Manager Date and Time

You can change the NTP server specified during initial login.

**Procedure**

1. Log in to the NSX Manager virtual appliance.
2. Under **Appliance Management**, click **Manage Appliance Settings**.
3. Click **Edit** next to **Time Settings**.
4. Make the appropriate changes.
5. Click **OK**.
6. Reboot the NSX Manager.

### Configure a Syslog Server for NSX Manager

If you specify a syslog server, NSX Manager sends all audit logs and system events to the syslog server. Syslog data is useful for troubleshooting and reviewing data logged during installation and configuration. NSX Edge supports two syslog servers. NSX Manager and NSX Controllers support one syslog server.

**Procedure**

1. Log in to the NSX Manager virtual appliance.
   - In a Web browser, navigate to the NSX Manager appliance GUI at https://<nsx-manager-ip> or https://<nsx-manager-hostname>, and log in as admin with the password that you configured during NSX Manager installation.
2. From the home page, click **Manage Appliance Settings > General**.
3. Click **Edit** next to **Syslog Server**.
4 Type the IP address or hostname, port, and protocol of the syslog server.

For example:

<table>
<thead>
<tr>
<th>Syslog Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).</td>
</tr>
<tr>
<td>Syslog Server:</td>
</tr>
<tr>
<td>Port:</td>
</tr>
<tr>
<td>Protocol:</td>
</tr>
</tbody>
</table>

5 Click OK.

Results

NSX Manager remote logging is enabled, and logs are stored in your standalone syslog server.

**Change FIPS Mode and TLS Settings on NSX Manager**

When you enable the FIPS mode, any secure communication to or from the NSX Manager will use cryptographic algorithms and protocols that are allowed by the United States Federal Information Processing Standards (FIPS).

- In a Cross-vCenter NSX environment, you should enable the FIPS mode on each NSX Manager separately.
- If one of the NSX Managers is not configured for FIPS, you must still ensure that it uses a secure communication method which complies with the FIPS standards.
- Both primary and secondary NSX Managers must be on the same TLS version for universal synchronization to work correctly.

**Important** Changing FIPS mode reboots the NSX Manager virtual appliance.

**Prerequisites**

- If you have upgraded from an earlier version of NSX, do not enable FIPS mode until the upgrade to NSX 6.3.0 is complete. See Understand FIPS Mode and NSX Upgrade in the NSX Upgrade Guide.
- Verify that the NSX Manager is NSX 6.3.0 or later.
- Verify that the NSX Controller cluster is NSX 6.3.0 or later.
- Verify that all host clusters running NSX workloads are prepared with NSX 6.3.0 or later.
- Verify that all NSX Edge appliances are version 6.3.0 or later, and that FIPS mode has been enabled on the required NSX Edge appliances. See Change FIPS Mode on NSX Edge.

**Procedure**

1. Log in to the NSX Manager virtual appliance.
2. Under **Appliance Management**, click **Manage Appliance Settings**.
3. From the Settings panel, click **General**.
4. Click **Edit** next to **FIPS Mode and TLS settings**.
   
   ![FIPS Mode and TLS settings dialog box](image)

   - **Changing FIPS mode will restart NSX Manager Appliance automatically.**
   - **Enable FIPS Mode**
   - **Server**: TLSv1, TLSv1.1, TLSv1.2
   - **Client**: TLSv1, TLSv1.1, TLSv1.2

5. To enable FIPS mode, select the **Enable FIPS Mode** check box.
6. For Server and Client, select the check boxes for the required TLS protocol version.

   **Note**: When FIPS mode is enabled, NSX Manager disables the TLS protocols that are not complaint to the FIPS standards.

7. Click **OK**.

   The NSX Manager appliance reboots, and FIPS is enabled.

**Edit DNS Servers**

You can change the DNS servers specified during Manager installation.

**Procedure**

1. Log in to the NSX Manager virtual appliance.
2. Under **Appliance Management**, click **Manage Appliance Settings**.
3. From the Settings panel, click **Network**.
4. Click **Edit** next to **DNS Servers**.
5. Make the appropriate changes.
6. Click **OK**.
Edit Lookup Service Details

You can change the Lookup Service details specified during initial login.

Procedure
1. Log in to the NSX Manager virtual appliance.
2. Under Appliance Management, click Manage Appliance Settings.
3. From the Settings panel, click NSX Management Service.
4. Click Edit next to Lookup Service.
5. Make the appropriate changes.
6. Click OK.

Edit vCenter Server

You can change the vCenter Server with which you registered NSX Manager during installation. You should do this only if you change the IP address of your current vCenter Server.

Procedure
1. If you are logged in to the vSphere Web Client, log out.
2. Log in to the NSX Manager virtual appliance.
4. From the Settings panel, click NSX Management Service.
5. Click Edit next to vCenter Server.
6. Make the appropriate changes.
7. Click OK.

Download Technical Support Logs for NSX

You can download NSX Manager system logs and Web Manager logs to your desktop.

Procedure
1. Log in to the NSX Manager virtual appliance.
2. Under Appliance Management, click Manage Appliance Settings.
3. Click and then click Download Tech Support Log.
4. Click Download.
5. After the log is ready, click the Save to download the log to your desktop.
   The log is compressed and has the file extension .gz.
What to do next

You can open the log using a decompression utility by browsing for All Files in the directory where you saved the file.

**NSX Manager SSL Certification**

NSX Manager requires a signed certificate to authenticate the identity of the NSX Manager web service and encrypt information sent to the NSX Manager web server. The process entails generating a certificate signing request (CSR), getting it signed by a CA, and importing the signed SSL certificate into NSX Manager. As a security best practice, you should use the generate certificate option to generate a private key and public key, where the private key is saved to the NSX Manager.

To obtain the NSX Manager certificate, you can use NSX Manager's built-in CSR generator or you can use another tool such as OpenSSL.

A CSR generated using NSX Manager's built-in CSR generator cannot contain extended attributes such as subject alternate name (SAN). If you wish to include extended attributes, you must use another CSR generation tool. If you are using another tool such as OpenSSL to generate the CSR, the process is 1) generate the CSR, 2) have it signed, and 3) proceed to the section Convert the NSX Manager Certificate File to PKCS 12 Format.

**Use the Built-In CSR Generator**

One method of obtaining an SSL certificate for NSX Manager is use the built-in CSR generator.

This method is limited in that the CSR cannot contain extended attributes such as subject alternate name (SAN). If you wish to include extended attributes, you must you another CSR generation tool. If you are using another CSR generation tool, skip this procedure.

**Procedure**

1. Log in to the NSX Manager virtual appliance.
2. Click **Manage Appliance Settings**.
3. From the Settings panel, click **SSL Certificates**.
4. Click **Generate CSR**.
5 Complete the form by filling in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key Size</td>
<td>Select the key length used in the selected algorithm.</td>
</tr>
<tr>
<td>Common Name</td>
<td>Type the IP address or fully qualified domain name (FQDN) of the NSX Manager. VMware recommends that you enter the FQDN.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Enter the department in your company that is ordering the certificate.</td>
</tr>
<tr>
<td>Organization Name</td>
<td>Enter the full legal name of your company.</td>
</tr>
<tr>
<td>City Name</td>
<td>Enter the full name of the city in which your company resides.</td>
</tr>
<tr>
<td>State Name</td>
<td>Enter the full name of the state in which your company resides.</td>
</tr>
<tr>
<td>Country Code</td>
<td>Enter the two-digit code that represents your country. For example, the United States is US.</td>
</tr>
</tbody>
</table>

6 Click OK.

7 Send the CSR to your CA for signing.
   a Download the generated request by clicking Download CSR.
      Using this method, the private key never leaves the NSX Manager.
   b Submit this request to your CA.
   c Get the Signed Certificate and Root CA and any intermediary CA certificates in PEM format.
   d To convert CER/DER formatted certificates to PEM, use the following OpenSSL command:
      ```bash
      openssl x509 -inform der -in Cert.cer -out 4-nsx_signed.pem
      ```
   e Concatenate all the certificates (server, intermediary and root certificates) in a text file.
   f In the NSX Manager UI, click Import and browse to the text file with all of the certificates.
   g Once the import is successful, the server certificate and all the CA certificates will be shown on the SSL Certificates page.

What to do next
Import the signed SSL certificate into NSX Manager.

Convert the NSX Manager Certificate File to PKCS 12 Format

If you used another tool, such as OpenSSL, to create the NSX Manager certificate, make sure that the certificate and private key are in the PKCS 12 format. If the NSX Manager certificate and private key are not in the PKCS 12 format, you must convert them to PKCS 12 format and then import the PKCS 12 certificate file into NSX Manager.

Prerequisites
- Verify that OpenSSL is installed on the system. You can download openssl from http://www.openssl.org.
Generate a public and private key pair. For example, run the following OpenSSL command:

```
openssl req -x509 -days [number of days] -newkey rsa:2048 -keyout my-key.pem -out my-cert.pem
```

**Procedure**

- After receiving the signed certificate from the authorized signer, run an OpenSSL command to generate a PKCS 12 (.pfx or .p12) keystore file from the public certificate file and your private key. For example:

```
openssl pkcs12 -export -in my-cert.pem -inkey my-key.pem -out nsx-manager.p12
```

Where:

- `my-cert.pem` is the signed certificate.
- `my-key.pem` is the private key.
- `nsx-manager.p12` is the name of the generated output file after the conversion to PKCS 12 format.

**What to do next**

Import the PKCS 12 certificate file into NSX Manager.

**Import an SSL Certificate**

You can import a pre-existing or CA-signed SSL certificate for use by the NSX Manager.

**Prerequisites**

When installing a certificate on NSX Manager, only the PKCS#12 keystore format is supported, and it must contain a single private key and its corresponding signed certificate or certificate chain.

**Procedure**

1. Log in to the NSX Manager virtual appliance.
2. Click **Manage Appliance Settings**.
3. From the Settings panel, click **SSL Certificates**.
4. Click **Upload PKCS#12 Keystore**.
5. Click **Choose File** to locate the file.
6 Click **Import**.

7 To apply the certificate, reboot the NSX Manager appliance.

**Results**

The certificate is stored in NSX Manager.

---

**NSX Backup and Restore**

Proper backup of all NSX components is crucial to restore the system to its working state in the event of a failure.

The NSX Manager backup contains all of the NSX configuration, including controllers, logical switching and routing entities, security, firewall rules, and everything else that you configure within the NSX Manager UI or API. The vCenter database and related elements like the virtual switches need to be backed up separately.

At a minimum, we recommend taking regular backups of NSX Manager and vCenter. Your backup frequency and schedule might vary based on your business needs and operational procedures. We recommend taking NSX backups frequently during times of frequent configuration changes.

NSX Manager backups can be taken on demand or on an hourly, daily, or weekly basis.

We recommend taking backups in the following scenarios:

- Before an NSX or vCenter upgrade.
- After an NSX or vCenter upgrade.
- After Day Zero deployment and initial configuration of NSX components, such as after the creation of NSX Controllers, logical switches, logical routers, edge services gateways, security, and firewall policies.
- After infrastructure or topology changes.
- After any major Day 2 change.

To provide an entire system state at a given time to roll back to, we recommend synchronizing NSX component backups (such as NSX Manager) with your backup schedule for other interacting components, such as vCenter, cloud management systems, operational tools, and so on.

---

**Back Up and Restore NSX Manager**

NSX Manager backup and restore can be configured from the NSX Manager virtual appliance web interface or through the NSX Manager API. Backups can be scheduled on an hourly, daily or weekly basis.

The backup file is saved to a remote FTP or SFTP location that NSX Manager can access. NSX Manager data includes configuration, events, and audit log tables. Configuration tables are included in every backup.
Restore is only supported on the same NSX Manager version as the backup version. For this reason, it is important to create a backup file before and after performing an NSX upgrade, one backup for the old version and another backup for the new version.

**Back Up NSX Manager Data**

You can back up NSX Manager data by performing an on-demand backup or a scheduled backup.

**Procedure**

1. Log in to the **NSX Manager Virtual Appliance**.
2. Click **Backup & Restore**.
3. To specify the backup location, click **Change** next to FTP Server Settings.
   a. Enter the IP address or host name of the backup system.
   b. From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**, based on what the destination supports.
   c. Edit the default port if necessary.
   d. Enter the user name and password required to log in to the backup system.
   e. In the **Backup Directory** text box, enter the absolute path for storing the backups.

   **Note**  If you do not provide a backup directory, backup is stored to the default directory (home directory) of the FTP server.

To determine the absolute path, log in to the FTP server, navigate to the directory that you want to use, and run the present working directory command (**pwd**). For example:

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password: 
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```
f Enter a text string in **Filename Prefix**.

This text is prepended to each backup filename to help you easily recognize the file on the backup system. For example, if you enter **ppdb**, the resulting backup file is named as `ppdbHH_MM_SS_YYYY_Mon_Day`.

**Note** Files in the Backup Directory must be limited to 100. If the number of files in the directory exceeds this limit, a warning message is displayed.

g Enter a pass phrase to secure the backup.

Pass phrase is required to restore the backup.

h Click **OK**.

For example:

<table>
<thead>
<tr>
<th>Option</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/Host name</td>
<td>192.168.110.60</td>
</tr>
<tr>
<td>Transfer Protocol</td>
<td>FTP</td>
</tr>
<tr>
<td>Port</td>
<td>21</td>
</tr>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>*****</td>
</tr>
<tr>
<td>Backup Directory</td>
<td>/datastore-01</td>
</tr>
<tr>
<td>Filename Prefix</td>
<td>nsxmgmt-backup</td>
</tr>
<tr>
<td>Pass Phrase</td>
<td>*****</td>
</tr>
</tbody>
</table>

4 For an on-demand backup, click **Backup**.

A new file is added under **Backup History**.

5 (Required) For scheduled backups, click **Change** next to Scheduling.

a From the **Backup Frequency** drop-down menu, select **Hourly**, **Daily**, or **Weekly**. The Day of Week, Hour of Day, and Minute drop-down menus are disabled based on the selected frequency. For example, if you select Daily, the Day of Week drop-down menu is disabled because this drop-down menu is not applicable to a daily frequency.

b For a weekly backup, select the day of the week the data should be backed up.

c For a weekly or daily backup, select the hour at which the backup should begin.

d Select the minute to begin and click **Schedule**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Frequency</td>
<td>Weekly</td>
</tr>
<tr>
<td>Day of week</td>
<td>Friday</td>
</tr>
</tbody>
</table>
To exclude logs and flow data from being backed up, click **Change** next to **Exclude**.

a Select the items that you want to exclude from the backup.

b Click **OK**.

Save your FTP server IP/hostname, credentials, directory details, and pass phrase. This information is required to restore the backup.

### Restore an NSX Manager Backup

Restoring NSX Manager causes a backup file to be loaded on an NSX Manager appliance. The backup file must be saved to a remote FTP or SFTP location that NSX Manager can access. NSX Manager data includes configuration, events, and audit log tables.

**Important** Back up your current data before restoring a backup file.

### Prerequisites

Before restoring NSX Manager data, we recommend reinstalling the NSX Manager appliance. Running the restore operation on an existing NSX Manager appliance might work, too, but is not supported. The assumption is that the existing NSX Manager has failed, and therefore a new NSX Manager appliance is deployed.

The best practice is to take note of the current settings for the old NSX Manager appliance so that they can be used to specify IP information and backup location information for the newly deployed NSX Manager appliance.

### Procedure

1. Take note of all settings on the existing NSX Manager appliance. Also, note down FTP server settings.

2. Deploy a new NSX Manager appliance.

   The version must be the same as the backed up NSX Manager appliance.

3. Log in to the new NSX Manager appliance.

4. Under Appliance Management, click **Backups & Restore**.

5. In FTP Server Settings, click **Change** and add the FTP server settings.

   The **Host IP Address**, **User Name**, **Password**, **Backup Directory**, **Filename Prefix**, and **Pass Phrase** fields in the Backup Location screen must identify the location of the backup to be restored.
The **Backup History** section displays the backup folder.

**Note** If the backup folder does not appear in the **Backup History** section, verify the FTP server settings. Check if you can connect to FTP server and view the backup folder.

6 In the **Backup History** section, select the required backup folder to restore, and click **Restore**.

Restoring the NSX Manager data begins.

**Results**

NSX configuration is restored to the NSX Manager.

**Caution** After restoring an NSX Manager backup, you might need to take additional action to ensure correct operation of NSX Edge appliances and logical switches. See **Restore NSX Edges** and **Resolve Out of Sync Errors on Logical Switches**.

**Restore NSX Edges**

All NSX Edge configurations (logical routers and edge services gateways) are backed up as part of NSX Manager data backup.

Taking individual NSX Edge backups is not supported.
If you have an intact NSX Manager configuration, you can recreate an inaccessible or failed Edge appliance VM by redeploying the NSX Edge (click **Redeploy NSX Edge** (Life) in the vSphere Web Client). See "Redeploy NSX Edge" in the **NSX Administration Guide**.

**Caution** After restoring an NSX Manager backup, you might need to take additional action to ensure correct operation of NSX Edge appliances.

- Edge appliances created after last backup are not removed during restore. You must delete the VM manually.
- Edge appliances deleted after the last backup are not restored unless redeployed.
- If both the configured and current locations of an NSX Edge appliance saved in the backup no longer exist when the backup is restored, operations such as redeploy, migrate, enable or disable HA will fail. You must edit the appliance configuration and provide valid location information. Use `PUT /api/4.0/edges/{edgeId}/appliances` to edit the appliance location configuration (resourcePoolId, datastoreId, hostId and vmFolderId as necessary). See "Working With NSX Edge Appliance Configuration" in the **NSX API Guide**.

If any of the following changes have occurred since the last NSX Manager backup, the restored NSX Manager configuration and the configuration present on the NSX Edge appliance will differ. You must **Force Sync** the NSX Edge to revert these changes on the appliance and ensure correct operation of the NSX Edge. See "Force Sync NSX Edge with NSX Manager" in the **NSX Administration Guide**.

- Changes made via Distributed Firewall for preRules for NSX Edge firewall.
- Changes in grouping objects membership.

If any of the following changes have occurred since the last NSX Manager backup, the restored NSX Manager configuration and the configuration present on the NSX Edge appliance will differ. You must **Redeploy** the NSX Edge to revert these changes on the appliance and ensure correct operation of the NSX Edge. See "Redeploy NSX Edge" in the **NSX Administration Guide**.

- Changes in Edge appliance settings:
  - HA enabled or disabled
  - appliance moved from deployed to undeployed state
  - appliance moved from undeployed to deployed state
  - resource reservation settings have been changed

- Changes in Edge appliance vNic settings:
  - add, remove, or disconnect vNic
  - port groups
  - trunk ports
  - fence parameters
  - shaping policy
Resolve Out of Sync Errors on Logical Switches

If logical switch changes have occurred between taking the NSX Manager backup and restoring the backup, logical switches might report being out of sync.

Procedure

1. Log in to the vSphere Web Client.
3. If present, click the Out of sync link in the Status column to display error details.
4. Click Resolve to recreate missing backing port groups for the logical switch.

Back Up vSphere Distributed Switches

You can export vSphere Distributed Switch and distributed port group configurations to a file. The file preserves valid network configurations, enabling distribution of these configurations to other deployments.

vSphere Distributed Switch settings and port-group settings are imported as part of the import.

As a best practice, export the vSphere Distributed Switch configuration before preparing the cluster for VXLAN. For detailed instructions, see http://kb.vmware.com/kb/2034602.

Back Up vCenter

To secure your NSX deployment, it is important to back up the vCenter database and take snapshots of the VMs.

Refer to the vCenter documentation for your vCenter version for vCenter backup and restore procedures and best practices.

For VM snapshots, see http://kb.vmware.com/kb/1015180.

Useful links for vCenter 5.5:
- http://kb.vmware.com/kb/2057353
- http://kb.vmware.com/kb/2034505

Useful links for vCenter 6.0:
- http://kb.vmware.com/kb/2110294

Flow Monitoring

Flow monitoring is a traffic analysis tool that provides a detailed view of the traffic to and from protected virtual machines. When flow monitoring is enabled, its output defines which machines are exchanging
data and over which application. This data includes the number of sessions and packets transmitted per session. Session details include sources, destinations, applications, and ports being used. Session details can be used to create firewall to allow or block rules.

You can view flow data for many different protocol types, including TCP, UDP, ARP, ICMP, and so on. You can live monitor TCP and UDP connections to and from a selected vNIC. You can also exclude flows by specifying filters.

Flow monitoring can thus be used as a forensic tool to detect rogue services and examine outbound sessions.

**View Flow Monitoring Data**

You can view traffic sessions on virtual machines within the specified time span. The last 24 hours of data are displayed by default, the minimum time span is one hour and the maximum is two weeks.

**Prerequisites**

Flow monitoring data is only available for virtual machines in clusters that have the network virtualization components installed and firewall enabled. See the *NSX Installation Guide*.

**Procedure**

1. Log in to the vSphere Web Client.
2. Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.
3. Ensure that you are in the **Dashboard** tab.
4 Click Flow Monitoring.

The page might take several seconds to load. The top of the page displays the percentage of allowed traffic, traffic blocked by firewall rules, and traffic blocked by SpoofGuard. The multiple line graph displays data flow for each service in your environment. When you point to a service in the legend area, the plot for that service is highlighted.

Traffic statistics are displayed in three tabs:

- **Top Flows** displays the total incoming and outgoing traffic per service over the specified time period based on the total bytes value (not based on sessions/packets). The top five services are displayed. Blocked flows are not considered when calculating top flows.

- **Top Destinations** displays incoming traffic per destination over the specified time period. The top five destinations are displayed.

- **Top Sources** displays outgoing traffic per source over the specified time period. The top five sources are displayed.

5 Click the Details by Service tab.

Details about all traffic for the selected service is displayed. The **Allowed Flows** tab displays the allowed traffic sessions and the **Blocked Flows** tab displays the blocked traffic.
You can search on service names.

<table>
<thead>
<tr>
<th>Type</th>
<th>Service</th>
<th>Source</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCP</td>
<td>DHCP-DHCP</td>
<td>654</td>
<td>6</td>
</tr>
<tr>
<td>TCP</td>
<td>TCP 17.17.4</td>
<td>274</td>
<td>1</td>
</tr>
<tr>
<td>OTHER</td>
<td>IP6-ICMPv0</td>
<td>1872</td>
<td>18</td>
</tr>
<tr>
<td>OTHER</td>
<td>ARP</td>
<td>1196</td>
<td>26</td>
</tr>
<tr>
<td>OTHER</td>
<td>ODM</td>
<td>162</td>
<td>2</td>
</tr>
<tr>
<td>UCP</td>
<td>NTP Time Server</td>
<td>152</td>
<td>1</td>
</tr>
</tbody>
</table>

6 Click an item in the table to display the rules that allowed or blocked that traffic flow.

7 Click the **Rule Id** for a rule to display the rule details.

## Change the Date Range of the Flow Monitoring Charts

You can change the date range of the flow monitoring data for both the Dashboard and Details tabs.

**Procedure**

1 Log in to the vSphere Web Client.

2 Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.

3 Click next to **Time interval**.

4 Select the time period or type a new start and end date.

   The maximum time span for which you can view traffic flow data is the previous two weeks.

5 Click **OK**.

## Add or Edit a Firewall Rule from the Flow Monitoring Report

By drilling down into the traffic data, you can evaluate the use of your resources and send session information to Distributed Firewall to create a new allow or block rule at any level.
Procedure

1. Log in to the vSphere Web Client.
2. Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.
3. Click the **Details by Service** tab.
4. Click a service to view the traffic flow for it.
   Depending on the selected tab, rules that allowed or denied traffic for this service are displayed.
5. Click a rule ID to view rule details.
6. Do one of the following:
   - To edit a rule:
     1. Click **Edit Rule** in the **Actions** column.
     2. Change the name, action, or comments for the rule.
     3. Click **OK**.
   - To add a rule:
     1. Click **Add Rule** in the **Actions** column.
     2. Complete the form to add a rule. For information on completing the firewall rule form, see Add a Distributed Firewall Rule.
     3. Click **OK**.
     The rule is added at the top of the firewall rule section.

**View Live Flow**

You can view UDP and TCP connections from and to a selected vNIC. In order to view traffic between two virtual machines, you can view live traffic for one virtual machine on one computer and the other virtual machine on a second computer. You can view traffic for a maximum of two vNICs per host and for 5 vNICs per infrastructure.

Viewing live flows can affect the performance of NSX Manager and the corresponding virtual machine.

**Procedure**

1. Log in to the vSphere Web Client.
2. Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.
3. Click the **Live Flow** tab.
4. Click **Browse** and select a vNIC.
5 Click **Start** to begin viewing live flow.

The page refreshes every 5 seconds. You can select a different frequency from the **Refresh Rate** drop-down.

6 Click **Stop** when your debugging or troubleshooting is done to avoid affecting the performance of NSX Manager or the selected virtual machine.

### Configure Flow Monitoring Data Collection

After you have viewed and filtered the flow monitoring data that you want to collect, you can configure data collection. You can filter the data being displayed by specifying exclusion criterion. For example, you may want to exclude a proxy server to avoid seeing duplicate flows. Or if you are running a Nessus scan on the virtual machines in your inventory, you may not want to exclude the scan flows from being collected. You can configure IPFix so that information for specific flows are exported directly from a firewall to a flow collector. The flow monitoring graphs do not include the IPFix flows. These are displayed on the IPFix collector's interface.

#### Procedure

1. Log in to the vSphere Web Client.
2. Select **Networking & Security** from the left navigation pane and then select **Flow Monitoring**.
3. Select the **Configuration** tab.
4. Ensure that **Global Flow Collection Status** is **Enabled**.

   All firewall related flows are collected across your inventory except for the objects specified in **Exclusion Settings**.
5 To specify filtering criteria, click **Flow Exclusion** and follow the steps below.

   a Click the tab corresponding to the flows you want to exclude.

   - **Collect Blocked Flows**
     - Yes
   - **Collect Layer2 Flows**
     - Yes
   - **Source**
     - **Destination**
     - 139.137
   - **Destination ports**
     - System-generated: broadcast macsrcd, 224.0.0.4, 255.255.255.255
   - **Service**

   b Specify the required information.

   - **Collect Blocked Flows**
     - Select No to exclude blocked flows.
   - **Collect Layer2 Flows**
     - Select No to exclude Layer2 flows.
   - **Source**
     - Flows are not collected for the specified sources.
     - 1 Click the Add icon.
     - 2 In View, select the appropriate container.
     - 3 Select the objects to exclude.
   - **Destination**
     - Flows are not collected for the specified destinations.
     - 1 Click the Add icon.
     - 2 In View, select the appropriate container.
     - 3 Select the objects to exclude.
   - **Destination ports**
     - Excludes flows to the specified ports.
     - Type the port numbers to exclude.
   - **Service**
     - Excludes flows for the specified services and service groups.
     - 1 Click the Add icon.
     - 2 Select the appropriate services and/or service groups.

   c Click **Save**.

6 To configure flow collection, click **IPFix** and follow the steps as described in **IPFIX for Distributed Firewall**.
7 Click **Publish Changes**.

**Configure IPFIX**

IPFIX (Internet Protocol Flow Information Export) is an IETF protocol that defines the standard of exporting flow information from an end device to a monitoring system. NSX supports IPFIX to export IP flow information to a collector.

You can enable IPFIX on:
- vSphere Distributed Switch (VDS)
- Distributed Firewall (DFW)

In the vSphere environment, vSphere Distributed Switch is the exporter and the collector is any monitoring tool available from any networking vendor.

The IPFIX standard specifies how IP flow information is presented and transferred from an exporter to a collector.

After you enable IPFIX on the vSphere Distributed Switch, it periodically sends messages to the collector tool. The contents of these messages are defined using the templates. For more information on templates, refer to [IPFIX Templates](#).

**IPFIX for Distributed Firewall**

You can enable IPFIX on a distributed firewall. Distributed firewall implements stateful tracking of flows and the tracked flows go through a set of state changes. IPFIX can be used to export data about the status of a flow. The tracked events include a flow creation, flow denial, flow update, and flow tear down.
You can enable a flow export for IPFIX on a distributed firewall as follows:

1. Log in to the vSphere Web Client.
2. Click **Networking & Security**, and then under **Tools**, click **Flow Monitoring**.
3. Select the **Configuration** tab.
4. Ensure that **Global Flow Collection Status** is **Enabled**.
5. To configure flow collection, click **IPFix** and follow the preceding steps.
   a. Click **Edit** next to IPFix Configuration and click **Enable IPFix Configuration**.
   b. In **Observation DomainID**, enter a 32-bit identifier that identifies the firewall exporter to the flow collector. Valid range is 0–65535.
   c. In **Active Flow Export Timeout**, type the time (in minutes) after which active flows are to be exported to the flow collector. The default value is five. For example, if the flow is active for 30 minutes and the export timeout is five minutes, then the flow is exported seven times during its lifetime. One for each creation and deletion, and five times during the active period.
   d. In **Collector IPs**, click the Add (Add) icon and enter the IP address and UDP port of the flow collector. Refer to your NetFlow collector documentation to determine the port number.
   e. Click **OK**.
6. Click **Publish Changes**.
**IPFIX for Logical Switch**

You can enable IPFIX on vSphere Distributed Switch.

You can enable IPFIX for a logical switch as follows:

1. Configure the NetFlow collector on the vSphere Distributed Switch backing the NSX transport zone (Logical Switch). For more information on how to configure NetFlow collector, see "Configure the NetFlow Settings of a vSphere Distributed Switch" topic in the vSphere Networking Guide.

2. You can enable NetFlow monitoring on the distributed port group corresponding to the Logical Switch. If the NSX transport zone spans multiple vSphere Distributed Switches (VDS), then repeat these steps for each VDS/distributed port group. For more information on how to enable NetFlow monitoring, see "Enable or Disable NetFlow Monitoring on a Distributed Port Group or Distributed Port in the vSphere documentation.

In an NSX environment, the virtual machine data traffic on a logical switch traversing the NSX uplink of ESXi is VXLAN encapsulated. When NetFlow is enabled on the host uplink, the IP flow records are exported using a custom IPFIX flow-record template. The template includes the outer VXLAN UDP/IP header information and the information of the inner encapsulated IP packet. Such flow record, as a result provides visibility on the VTEP that is encapsulating the packet (outer header) and the details of the virtual machine that generated inter-host traffic (inner header) on a NSX logical switch (VXLAN).

For more details on the IPFIX templates for vSphere Distributed Switch, refer to IPFIX Templates.

**IPFIX Templates**

IPFIX templates provides the visibility into the VXLAN and non-VXLAN flows. The templates have additional parameters that provide more information regarding the encapsulated traffic.
The templates are supported in vSphere Distributed Switch (exporter). IPFIX support on vSphere Distributed Switch provides the required visibility into the virtual machine flows and VXLAN flows. If you are using any third party collector tool, you can use additional information available in the templates to provide correlation between the internal and external flows and the port connections.

**IPv4 Template**

```plaintext
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access port, N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

**IPv4 VXLAN Template**

```plaintext
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_VXLAN)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
```
IPv4 ICMP VXLAN Template

IPv4 ICMP Template
IPv6 ICMP VXLAN Template

IPv6 ICMP Template
IPv6 Template

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX TEMPLATE_FIELD(vxlanId, 8)
IPFIX TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX TEMPLATE_FIELD(tcpFlags, 1)
IPFIX TEMPLATE Field(IPv6TOS, 1)
IPFIX TEMPLATE FIELD(maxTTL, 1)
IPFIX TEMPLATE FIELD(flowDir, 1)
// Specify the Interface port– Uplink Port, Access Port, or NA.
IPFIX_VMw TEMPLATE FIELD(ingressInterfaceAttr, 2)
IPFIX_VMw TEMPLATE FIELD(egressInterfaceAttr, 2)
IPFIX TEMPLATE FIELD(vxlanExportRole, 1)
IPFIX TEMPLATE Padding(paddingOctets, 2)
IPFIX TEMPLATE END()
```

IPv6 VXLAN Template

```
IPFIX TEMPLATE FIELD(sourceIPv4Address, 4)
IPFIX TEMPLATE FIELD(destinationIPv4Address, 4)
IPFIX TEMPLATE FIELD(octetDeltaCount, 8)
IPFIX TEMPLATE FIELD(packetDeltaCount, 8)
IPFIX TEMPLATE FIELD(flowStartSysUpTime, 8)
IPFIX TEMPLATE FIELD(flowEndSysUpTime, 8)
IPFIX TEMPLATE FIELD(sourceTransportPort, 2)
IPFIX TEMPLATE FIELD(destinationTransportPort, 2)
IPFIX TEMPLATE FIELD(ingressInterface, 4)
IPFIX TEMPLATE FIELD(egressInterface, 4)
IPFIX TEMPLATE FIELD(vxlanExportRole, 1)
IPFIX TEMPLATE Padding(paddingOctets, 1)
IPFIX TEMPLATE END()
```
Additional Parameters

Following are the additional parameters:

1. **VXLAN Specific Parameters:** The tenant specific fields are the inner flow IPs, ports and protocol information.
   - tenantSourceIPv4
   - tenantSourceIPv6
   - tenantDestIPv4
   - tenantDestIPv6
   - tenantSourcePort
   - tenantDestPort
   - tenantProtocol

2. **Interface Port Parameters:** These parameters can be used for both VXLAN and non-VXLAN templates.
   - ingressInterfaceAttr
   - egressInterfaceAttr
   - vxlanExportRole

The ingress and egress interface attributes can take the following values based on type of the port:

- IPFIX_UPLINK_PORT 0X01
- IPFIX_ACCESS_PORT 0X02
- IPFIX_VXLAN_TUNNEL_PORT 0X03
The `vxlanExportRole` defines if the exporter is an ESXi host or any other network device. `IPFIX_END_POINT 0x01` means host is exporting the data. If other devices export the IPFIX templates, this field might have different value (not defined yet).

**Flows Monitored by the IPFIX for vSphere Distributed Switch**

The preceding diagrams show the communication between the two VMs running on two different hosts and the flows monitored by the IPFIX feature for vSphere Distributed Switch.

**Figure 22-2. Flow on Host 1**

**Flow 1: IPv4 Template**

<table>
<thead>
<tr>
<th>Standard Elements...</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IngressInterfaceAttr:</td>
<td>0x02 - port1</td>
</tr>
<tr>
<td>EgressInterfaceAttr:</td>
<td>0x03 - Management port</td>
</tr>
<tr>
<td>vxlanExportRole:</td>
<td>01</td>
</tr>
</tbody>
</table>

**Flow 2: IPv4 VXLAN Template**

<table>
<thead>
<tr>
<th>Standard Elements...</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>vxlanID:</td>
<td>5003</td>
</tr>
<tr>
<td>tenantProtocol:</td>
<td>TCP</td>
</tr>
<tr>
<td>tenantSourceIPv4:</td>
<td>IP1</td>
</tr>
<tr>
<td>tenantDestIPv4:</td>
<td>IP2</td>
</tr>
<tr>
<td>tenantSourcePort:</td>
<td>10000</td>
</tr>
<tr>
<td>tenantDestPort:</td>
<td>80</td>
</tr>
<tr>
<td>IngressInterfaceAttr:</td>
<td>0x03 - Management port</td>
</tr>
<tr>
<td>EgressInterfaceAttr:</td>
<td>0x01 - dvuplink</td>
</tr>
<tr>
<td>vxlanExportRole:</td>
<td>01</td>
</tr>
</tbody>
</table>

The **Figure 22-2. Flow on Host 1** shows the flows are collected from Host 1. The IPv4 template has additional information about the ingress and egress port and the standard elements.
The `ingressInterfaceAttr` text box 0x02 indicates it is an access port where the virtual machine is connected. The access port number is assigned to the `ingressInterface` parameter in the template.

The `egressInterfaceAttr` value of 0x03 shows that it is a VXLAN tunnel port and the port number associated with it is a management VMKNic port. This port number is assigned to the `egressInterface` parameter in the template.

The IPv4 VXLAN template on the other hand has additional information about the VXLAN ID, inner source, and destination IP/Port and protocol. The ingress and egress interfaces are `VXLAN tunnel port` and `dvuplink port` respectively.

**Figure 22-3. Flow on Host 2**

![Figure 22-3. Flow on Host 2](image)

The `Flow 4: IPv4 Template` shows the flows on Host 2.

The `Flow 3: IPv4 VXLAN Template` shows the flows on Host 1.
The templates in the Figure 22-2. Flow on Host 1 differs from the Figure 22-2. Flow on Host 1 only in the Ingress and egress attributes and port numbers.

The additional information provided through this template helps the collector tool vendors to correlate the external VXLAN flows and the internal virtual machine flows.

**Information Relevant to the Collector Tool Vendor**

IPFIX support on vSphere Distributed Switch provides the required visibility into the virtual machine flows and VXLAN flows. If you are using any collector tool vendor, you can use additional information available in the templates to provide a correlation between the internal and external flows and the port connections.

The following section provides the details regarding how to decode the new parameters that are added in the VXLAN templates. IANA defines IPFIX information elements and their element IDs. You can find the list of standard element IDs at [http://www.iana.org/assignments/ipfix/ipfix.xml](http://www.iana.org/assignments/ipfix/ipfix.xml).

All the new elements defined as part of VXLAN template have their new element IDs.

These custom parameters or elements provide additional information about the VXLAN and internal flows. The following are the new elements and their IDs:

**Table 22-4. Custom Parameters**

<table>
<thead>
<tr>
<th>Element ID</th>
<th>Parameter Name</th>
<th>Data Type</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>880</td>
<td>tenantProtocol</td>
<td>unsigned8</td>
<td>1 byte</td>
</tr>
<tr>
<td>881</td>
<td>tenantSourceIPv4</td>
<td>ipv4Address</td>
<td>4 bytes</td>
</tr>
<tr>
<td>882</td>
<td>tenantDestIPv4</td>
<td>ipv4Address</td>
<td>4 bytes</td>
</tr>
<tr>
<td>883</td>
<td>tenantSourceIPv6</td>
<td>ipv6Address</td>
<td>16 bytes</td>
</tr>
<tr>
<td>884</td>
<td>tenantDestIPv6</td>
<td>ipv6Address</td>
<td>16 bytes</td>
</tr>
<tr>
<td>886</td>
<td>tenantSourcePort</td>
<td>unsigned16</td>
<td>2 bytes</td>
</tr>
<tr>
<td>887</td>
<td>tenantDestPort</td>
<td>unsigned16</td>
<td>2 bytes</td>
</tr>
<tr>
<td>888</td>
<td>egressInterfaceAttr</td>
<td>unsigned16</td>
<td>2 bytes</td>
</tr>
<tr>
<td>889</td>
<td>vxlanExportRole</td>
<td>unsigned8</td>
<td>1 byte</td>
</tr>
<tr>
<td>890</td>
<td>ingressInterfaceAttr</td>
<td>unsigned16</td>
<td>2 bytes</td>
</tr>
</tbody>
</table>

**Note** The **Enterprise ID** is appended to all the custom elements defined above. The enterprise ID for VMware is 6876.

The following table shows an example of complete list of element IDs. You can find data type and unit for standard element IDs at [http://www.iana.org/assignments/ipfix/ipfix.xml](http://www.iana.org/assignments/ipfix/ipfix.xml).

<table>
<thead>
<tr>
<th>Element ID</th>
<th>Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>octetDeltaCount</td>
</tr>
<tr>
<td>2</td>
<td>packetDeltaCount</td>
</tr>
<tr>
<td>4</td>
<td>protocolIdentifier</td>
</tr>
<tr>
<td>5</td>
<td>IPv4TOS</td>
</tr>
</tbody>
</table>
### Application Rule Manager

The Application Rule Manager tool simplifies the process of microsegmenting an application by creating security groups and firewall rules for existing applications.

Flow monitoring is used for long term data collection across the system, while the application rule manager is used for a targeted modeling of an application.

<table>
<thead>
<tr>
<th>Element ID</th>
<th>Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>IPv6TOS</td>
</tr>
<tr>
<td>6</td>
<td>tcpFlags</td>
</tr>
<tr>
<td>7</td>
<td>sourceTransportPort</td>
</tr>
<tr>
<td>8</td>
<td>sourceIPv4Address</td>
</tr>
<tr>
<td>10</td>
<td>ingressInterface</td>
</tr>
<tr>
<td>11</td>
<td>destinationTransportPort</td>
</tr>
<tr>
<td>12</td>
<td>destinationIPv4Address</td>
</tr>
<tr>
<td>14</td>
<td>egressInterface</td>
</tr>
<tr>
<td>15</td>
<td>nextHopIPv4</td>
</tr>
<tr>
<td>27</td>
<td>sourceIPv6Address</td>
</tr>
<tr>
<td>28</td>
<td>destinationIPv6Address</td>
</tr>
<tr>
<td>53</td>
<td>maxTTL</td>
</tr>
<tr>
<td>61</td>
<td>flowDir</td>
</tr>
<tr>
<td>136</td>
<td>flowEndReason</td>
</tr>
<tr>
<td>152</td>
<td>flowStartSysUpTime</td>
</tr>
<tr>
<td>153</td>
<td>flowEndSysUpTime</td>
</tr>
<tr>
<td>210</td>
<td>paddingOctets</td>
</tr>
<tr>
<td>351</td>
<td>vxlanId</td>
</tr>
<tr>
<td>880</td>
<td>tenantProtocol</td>
</tr>
<tr>
<td>881</td>
<td>tenantSourceIPv4</td>
</tr>
<tr>
<td>882</td>
<td>tenantDestIPv4</td>
</tr>
<tr>
<td>883</td>
<td>tenantSourceIPv6</td>
</tr>
<tr>
<td>884</td>
<td>tenantDestIPv6</td>
</tr>
<tr>
<td>886</td>
<td>tenantSourcePort</td>
</tr>
<tr>
<td>887</td>
<td>tenantDestPort</td>
</tr>
<tr>
<td>888</td>
<td>egressInterfaceAttr</td>
</tr>
<tr>
<td>889</td>
<td>vxlanExportRole</td>
</tr>
<tr>
<td>890</td>
<td>ingressInterfaceAttr</td>
</tr>
</tbody>
</table>
There are three steps in the application rule manager workflow:

1. Select virtual machines (VM) that form the application and need to be monitored. Once configured, all incoming and outgoing flows for a defined set of VNICs (Virtualized Network Interface Cards) on the VMs are monitored. There can be up to five sessions collecting flows at a time.

2. Stop the monitoring to generate the flow tables. The flows are analyzed to reveal the interaction between VMs. The flows can be filtered to bring the flow records to a limited working set.

3. Use flow tables to create grouping objects such as security groups, IP sets, services and service groups and firewall rules.

Create a Monitoring Session

A monitoring session collects all incoming and outgoing flows for up to 30 vNICs in a given session.

Prerequisites

Before starting a monitoring session, you need to define the VMs and vNICs that need to be monitored. VMware Tools must be running and current on your Windows desktop VMs. Selected VMs need to be in a cluster that has firewall enabled (they cannot be on the exclude list). A default firewall rule of "any allow" that applies to the selected vNICs must be created for the duration of the monitoring session, so that flows to and from the vNICs are not dropped by any other firewall rule.

Procedure

1. Log in to the vSphere Web Client, then select Networking & Security from the left navigation pane.

2. Select Flow Monitoring.

3. Select the Application Rule Manager tab.

4. Click Start New Session.

5. In the Start New Session dialogue box, enter a name for the session.

6. Select either vNICs or VMs as the object type.

   The Available Objects column is populated with the available objects.

7. Double-click the vNICs or VMs you want monitored. The selected vNICs or VMs move to the Selected Objects column.

8. Click OK to begin collecting flows.

   The status is now Collecting Data. The latest set of flows collected is shown in the flow table.

9. Click Stop to end collecting flows.

Results

A flow monitoring session has been created for the selected vNICs and VMs.
What to do next

After collecting flows, analyze the flows.

**Analyze Flows**

After a flow monitoring session has been collected, the results are analyzed and can be filtered for use in grouping objects and firewall rules.

Analyzed flows can be filtered to limit the number of flows in a working set. The filter option icon is next to the Processed View drop-down menu on the right.

**Prerequisites**

Before analysis, a flow monitoring session must have been collected from selected vNICs or VMs.

**Procedure**

1. After flows have been collected, click **Analyze**.

   Defined services are resolved, the IP address to VM translation begins, and duplicates are removed.

2. Once analyzed, the following data is provided for flows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Direction</strong></td>
<td>IN - flow is coming into one of the VM and VNIC selected as part of the input seed.</td>
</tr>
<tr>
<td></td>
<td>OUT - flow is generated from one of the VM and VNIC selected as part of the input seed.</td>
</tr>
<tr>
<td></td>
<td>INTRA- flow is between VM- and VNIC selected as part of the input seed.</td>
</tr>
<tr>
<td><strong>Source</strong></td>
<td>VM Name, if the Source IP address of the flow record is resolved to one VM in the NSX inventory. Note that IP address can be resolved to VM, only if VM Tools has been enabled on those VMs.</td>
</tr>
<tr>
<td></td>
<td>Raw IP, if there is no VM found for this source IP address in NSX Inventory. Note that multicast and broadcast IP addresses will not be resolved to VMs.</td>
</tr>
<tr>
<td></td>
<td>Number of VMs (Ex:2 Virtual Machines) if the IP address is an overlapping IP address mapped to multiple VMs in different networks, the user needs to resolve Virtual machines to the correct Virtual Machine related to this flow record.</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td>Same values as Source field.</td>
</tr>
<tr>
<td><strong>Service</strong></td>
<td>NSX defined service for protocol/port.</td>
</tr>
<tr>
<td></td>
<td>Raw protocol/port, if there is no defined service in the NSX Manager.</td>
</tr>
<tr>
<td></td>
<td>Number of services. If there is more than one service mapped to the same protocol/port and the user needs to resolve it to one service applicable to the flow record.</td>
</tr>
</tbody>
</table>

What to do next

Analyzed flows can be modified for further customization. Next, use the analyzed flows to create firewall rules.

**Flow Consolidation and Customization**
After system analysis is complete, the analyzed flow table is available in the **Processed View**. Users can further consolidate the flows by changing the source, destination, and service fields. See [Customizing Services in Flow Records](#) and [Customizing Source and Destination in Flow Records](#).

**Note** Processed View

Collected flows are displayed in a table with the following columns:

<table>
<thead>
<tr>
<th>Field</th>
<th>Options</th>
</tr>
</thead>
</table>
| **Direction** | IN - flow is coming into one of the VMs or vNICs selected as part of the input seed.  
OUT - flow is generated from one of the VMs or vNICs selected as part of the input seed.  
INTRA- flow is between the VM or vNIC selected as part of the input seed. |
| **Source** | VM Name, if the Source IP address of the flow record is resolved to one VM in the NSX inventory.  
Raw IP if there is no VM found for this source IP address in the NSX Inventory. Note than multicast and broadcast IPs will not be resolved to VMs.  
Number of VMs if IP address is an overlapping IP address mapped to multiple VMs in different networks. The user needs to resolve multiple VMs to one VM related to this flow record. |
| **Destination** | Same values as Source field. |
| **Service** | NSX defined service for protocol/port.  
Raw protocol/port, if there is no defined service in the NSX Manager.  
Number of services. If there is more than one service mapped to the same protocol/port and the user needs to resolve it to one service applicable to the flow record. |

Flow tables can be edited and the flows consolidated for easier rule creation. For example, the source field can be replaced with ANY. Multiple VMs receiving flows with HTTP and HTTPs can be replaced with “WEB-Service” service group, which includes both HTTP and HTTPS service. By doing so, Multiple flows may look similar and flow patterns may emerge that can be easily translated to a firewall rule.

Note that while each cell of the flow table can be modified, the cells are not auto-populated. For instance, if the IP address 196.1.1.1 is added to the DHCP-Server IPSSet, the subsequent occurrences of that IP are not auto-populated to show the DHCP-Server group. There is a prompt asking if you want to replace all instances of the IP address with the IPSSet. This allows the flexibility to make that IP part of multiple IPSSet groups.

**Note** Consolidated View

The consolidated view is accessed from the drop-down list in the right-hand corner. The consolidated view eliminates duplicate flows and displays the minimal number of flows. This view can be used to create firewall rules.

Clicking the arrow in the left hand corner of the Direction column shows the corresponding related raw flow information:

- for intra flows the corresponding IN and OUT flows with raw data are shown
- the original source IP, destination IP, port, and protocol information in all of the raw flows that were consolidated into the record
- for ALG flows, the corresponding data flow for the control flow is shown
Customizing Services in Flow Records

Services flow cells can be customized on an individual cell basis by the user.

After flow analysis, users can associate any undefined protocol/port combinations and create a service. Service groups can be created for any of the services listed in the flows collected. For more information on modifying flow records see Flow Consolidation and Customization.

Prerequisites

Flow data must have been collected from a set of vNICs and VMs. See Create a Monitoring Session.

Procedure

- After the flow state is Analysis Completed, the flow table is populated with data, in the Processed View. To customize cell data, hover the cursor over a cell. A gear icon appears in the right-hand corner of the cell. Click the gear icon in the Service column and select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve Services</td>
<td>If the port and protocol has been translated to multiple services, use this option to select the correct service.</td>
</tr>
<tr>
<td>Create Services and Replace</td>
<td>To add a service:</td>
</tr>
<tr>
<td></td>
<td>a Enter a name for the service.</td>
</tr>
<tr>
<td></td>
<td>b From the drop-down list, select the protocol.</td>
</tr>
<tr>
<td></td>
<td>c Enter the destination ports for the service.</td>
</tr>
<tr>
<td></td>
<td>d Click Advanced options to enter the source ports of the service. The source port is used to track of new incoming connections and data streams.</td>
</tr>
<tr>
<td></td>
<td>e Optional - check Enable inheritance to allow visibility at underlying scopes to create a common group or criteria can be reused at the level of individual Edges.</td>
</tr>
<tr>
<td></td>
<td>f Click OK and a new service is created and populated in the Service column. Note that if there are other flow records with the same undefined port and protocol combination you will be asked for confirmation to replace all of them with the newly created Service. This occurs only for the flows with undefined services found in the Analysis phase.</td>
</tr>
<tr>
<td>Create Services Group and Replace</td>
<td>You can create a new service group with the service from the flow included in it. Then, the new service group will replace the service.</td>
</tr>
<tr>
<td></td>
<td>To add a service group:</td>
</tr>
<tr>
<td></td>
<td>a Enter a name for the service group.</td>
</tr>
<tr>
<td></td>
<td>b Optional - enter a description of the Service Group.</td>
</tr>
<tr>
<td></td>
<td>c Select the Object type.</td>
</tr>
<tr>
<td></td>
<td>d Select the available objects you want to be added to the Service Group and click the arrow to move the object to the Selected Objects column.</td>
</tr>
<tr>
<td></td>
<td>e A new services group is created and populated in the Service column.</td>
</tr>
<tr>
<td>Replace Service with Any</td>
<td>Replaces the specific service with any service.</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
Replace Service with Service Group | If the selected service is a member of multiple service groups, you select the specific service group you want to apply.  
a. Click the desired Service Group from the list of available objects.  
b. Click OK.
Revert Protocol and Port | Reverts any cell modifications back to the original data.

**Results**

The changed flow record has a pink bar on the side. When the cursor is hovered over any cell which has been modified there is a green checkmark. Clicking the checkmark displays a pop-up window with the previous and new values for that cell. The modified flow record is easier to translate into firewall rules.

**What to do next**

Next, the flow record can be used to create firewall rules.

After flows have been modified, they can be further grouped together to get the smallest distinct working set. The **Processed View** is used to create Service Groups and IP Sets and modify the flows. The **Consolidated View** further compresses these modified flows to make it easier to create firewall rules.

**Customizing Source and Destination in Flow Records**

Source and destination flow cells can be customized on an individual cell basis by the user.

After flow analysis is complete, flow cells can be customized by the user.

**Prerequisites**

Flow data must have been collected from a set of vNICs and VMs. See [Create a Monitoring Session](#).

**Procedure**

- After the flow state shows **Analysis Completed**, the flow table is populated with data. To customize cell data, hover the cursor over a cell. A gear icon appears in the right-hand corner of the cell. Click the gear icon in the **Source** or **Destination** column and select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolve VMs</td>
<td>This option is available if multiple VMs have the same IP address. This option is used to chose the applicable VM name for the flow record.</td>
</tr>
<tr>
<td>Replace with any</td>
<td>If the source should be accessible to everyone then any source IP address is the correct option. In all other cases, you should specify the source address. Configuring a destination value of any for the destination IP address is discouraged.</td>
</tr>
<tr>
<td>Replace with Membership</td>
<td>If the VM is part of Security Groups they will be displayed here and can replace the VM name.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Create Security Group</td>
<td>a. Enter a Name and (optional) description of the security group. &lt;br&gt;b. Click Next. &lt;br&gt;c. Define the criteria that an object must meet for it to be added to the security group you are creating. This gives you the ability to include virtual machines by defining a filter criteria with a number of parameters supported to match the search criteria. &lt;br&gt;d. Select one or more resources to add to the security group. Note that when you add a resource to a security group, all associated resources are automatically added. For example, when you select a virtual machine, the associated vNIC is automatically added to the security group. You can include the following objects in a security group: &lt;br&gt;Cluster &lt;br&gt;Logical Switch &lt;br&gt;Legacy Port Group &lt;br&gt;vApp &lt;br&gt;Datacenter &lt;br&gt;e. Click Next. &lt;br&gt;f. Select the objects to exclude from the security group. The objects selected here are always excluded from the security group, regardless of whether or not they match the dynamic criteria. &lt;br&gt;g. Click Next. &lt;br&gt;h. Review the Security Group details on the Ready to complete window. Click Finish.</td>
</tr>
<tr>
<td>Add to existing Security Group and Replace</td>
<td>For VMs, if the selected VM is a member of multiple security groups, select the specific security group you want to apply. This option is not available if the IP address is present in the source or destination field. For raw IP addresses, use Add to existing IPset and Replace option. &lt;br&gt;a. Click the desired Service Group from the list of available objects. &lt;br&gt;b. Click OK.</td>
</tr>
<tr>
<td>Create IPSet and Replace</td>
<td>An IPSet allows you to apply a firewall rule to an entire set of IP addresses at once. &lt;br&gt;a. Enter a name for the IPSet. &lt;br&gt;b. Optional - enter a description. &lt;br&gt;c. Enter IP addresses or range of address in the new IP set. &lt;br&gt;d. Click OK.</td>
</tr>
<tr>
<td>Add to existing IPset and Replace</td>
<td>An IP address may be part of several IPsets. Use this option to replace the shown IP address and replace it with another. &lt;br&gt;a. Select the desire IPset from the Available Objects. &lt;br&gt;b. Click OK.</td>
</tr>
<tr>
<td>Revert to initial data</td>
<td>Reverts any cell modifications back to the original data.</td>
</tr>
</tbody>
</table>

**What to do next**

Create a firewall rule based on flow monitoring.
Creating Firewall Rules from Application Rule Manager

Firewall rules can be edited, deleted, moved up and moved down as part of the Application Rule Manager.

Prerequisites

After the flow record has been analyzed you can create firewall rules.

Procedure

1. Open a flow session. If you are in the **Processed View**, right-click on a single flow cell or shift + first cell > last cell to select several cells, and then right-click. If you are in the **Consolidated View** select a flow cell and click the **Action** icon. Select **Create Firewall rule**.

   The *New Firewall Rule* pop-up window appears with all of the cells populated based on the selected row data. If several cells were selected, all the source, destination, service objects are added to the corresponding fields of the rule.

2. Enter a name for the new rule.

3. (Optional) To select a different source or destination click **Select** next to the Source or Destination box. Specify a new source or destination from the available objects and click **OK**.

4. (Optional) To select a different service click **Select** the Service box. Distributed Firewall supports ALG (Application Level Gateway) for the following protocols: FTP, CIFS, ORACLE TNS, MS-RPC, and SUN-RPC. Edge supports ALG for FTP only. Specify a new service from the available objects and click **OK**.

5. (Optional) To apply the rule to a different scope click **Select** next to the Applied To box. Make appropriate selections as described in the table below and click **OK**. By default, the rule is applied to the VNICs you originally right-clicked on.

<table>
<thead>
<tr>
<th>To apply a rule to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>All prepared clusters in your environment</td>
<td>Select <strong>Apply this rule on all clusters on which Distributed Firewall is enabled</strong>. After you click <strong>OK</strong>, the Applied To column for this rule displays <strong>Distributed Firewall</strong>.</td>
</tr>
</tbody>
</table>
| One or more cluster, datacenter, distributed virtual port group, NSX Edge, network, virtual machine, vNIC, or logical switch | 1. In **Container type**, select the appropriate object.  
2. In the **Available** list, select one or more objects and click ![Icon] |

If the rule contains virtual machines and vNICS in the source and destination fields, you must add both the source and destination virtual machines and vNICS to **Applied To** for the rule to work correctly.
6  Select the **Action** described in the table below.

<table>
<thead>
<tr>
<th>Action</th>
<th>Results in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allows traffic from or to the specified source(s), destination(s), and service(s).</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks traffic from or to the specified source(s), destination(s), and service(s).</td>
</tr>
<tr>
<td>Reject</td>
<td>Sends reject message for unaccepted packets. RST packets are sent for TCP connections. ICMP messages with administratively prohibited code are sent for UDP, ICMP, and other IP connections.</td>
</tr>
</tbody>
</table>

7  Specify the rule **Direction** of the rule by clicking the drop-down arrow.

8  **Click OK**

**What to do next**

Publish the firewall rules. See *Publishing and Managing Firewall Rules From Application Rule Manager*.

**Publishing and Managing Firewall Rules From Application Rule Manager**

Firewall rules can be edited and published from the Application Rule Manager.

After firewall rules have been created they can be managed in the **Firewall Rules** tab of the Application Rule Manager.

**Prerequisites**

Create firewall rules from a flow monitoring session.

**Procedure**

◆ After you have created firewall rules from a flow monitoring session, they appear in the **Firewall Rules** tab. Select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Publish | a Click **Publish** to publish the created firewall rules. The rules are published as a new section.  
b Enter a **Section Name** for the firewall rule  
c Select where the new firewall section will be inserted in the existing firewall configuration.  
d **Click OK.** |
<p>| Edit   | Select the pencil icon to edit the firewall rules. |
| Delete | Select the red X icon to delete the firewall rule. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down Arrow</td>
<td>Select the down arrow icon to move the rule down</td>
</tr>
<tr>
<td>Up Arrow</td>
<td>Select the up arrow icon to move the rule up.</td>
</tr>
</tbody>
</table>

**Note** When firewall rules are published from Application Rule Manager, the section name is added to the Publish button. Any subsequent publishing from the Application Rule Manager overrides the existing section in the Firewall Configuration with the rules which are currently available in the Application Rule Manager.

### Activity Monitoring

Activity monitoring provides visibility into the applications that are in use on the Windows desktop virtual machines that are managed by vCenter. This visibility helps ensure that security policies at your organization are being enforced correctly.

**Note** As of NSX 6.3.0, the NSX Activity Monitoring feature has been deprecated. You can continue to use this feature at your discretion, but be aware that it will be removed from NSX in a future release. From 6.3.0 onwards, we recommend you use Endpoint Monitoring instead of Activity Monitoring.

A security policy may mandate who is allowed access to what applications. The cloud administrator can generate Activity Monitoring reports to see if the IP based firewall rule that they set is doing the intended work. By providing user and application level detail, activity monitoring translates high level security policies to low level IP address and network based implementation.

**Figure 22-4. Your virtual environment today**

![Diagram showing virtual environment]

Once you enable data collection for Activity Monitoring, you can run reports to view inbound traffic (such as virtual machines being accessed by users) as well as outbound traffic (resource utilization, interaction between inventory containers, and AD groups that accessed a server).
Figure 22-5. Your virtual environment with Activity Monitoring

<table>
<thead>
<tr>
<th>User</th>
<th>AD group</th>
<th>App Name</th>
<th>Originating VM name</th>
<th>Destination VM name</th>
<th>Source IP</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>John</td>
<td>Doctors</td>
<td>Epic.exe</td>
<td>DoctorsWS13</td>
<td>EpicSVR3</td>
<td>172.16.254.1</td>
<td>172.16.112.2</td>
</tr>
</tbody>
</table>

**Important** Activity monitoring is not supported on Linux VMs.

**Set Up Activity Monitoring**

For activity monitoring to work, there are several required procedures that must be performed, including installation of the guest introspection driver, installation of guest introspection VMs, and enabling NSX activity monitoring. Optionally, you can also use service composer to control which VMs are monitored.

**Prerequisites**

- NSX must be installed and operational.
- NSX Manager must be linked with the AD server where it will get groups to which to match Windows VMs users.
- The vCenter inventory must contain one or more Windows desktop VMs.
- VMware Tools must be running and current on your Windows desktop VMs.
Procedure

1. On the Windows VMs in your vCenter inventory, install the Guest Introspection driver if it is not already installed.
   a. Navigate to Control Panel\Programs\Programs and Features, right-click VMware Tools and select Change.
   b. Select Modify.
   c. Under VMCI Driver, click Guest Introspection Drivers > Will be installed on local hard drive.

The guest introspection driver detects what applications are running on each Windows VM and sends this information to the guest introspection VM.
Install the guest introspection VMs.

When first launching the VMware Tools install, choose the **Custom** option. In the VMCI folder, select **Guest Introspection Driver**. The driver is not selected by default.

To add the driver after VMware Tools is already installed:

a. In the vCenter Web Client, navigate to **Networking & Security > Installation > Service Deployments**.

b. Add a new service deployment.

c. Select **Guest Introspection**.

d. Select the host clusters that contain Windows VMs.

e. Select the appropriate datastores, networks, and IP addressing mechanism. If you are not using DHCP for your guest introspection VMs, create and assign an IP pool.

Two guest introspection VMs are installed, one on each host within each cluster.
3  Enable activity monitoring on the Windows VMs.
   a  In the **Hosts and Clusters** view, select the Windows VM, and select the **Summary** tab.
   b  In NSX Activity Monitoring, click **Edit** and click **Yes**.

![NSX Activity Monitoring](image)

Repeat this step for all Windows VMs that you want to monitor.

4  (Optional) Modify the list of vCenter objects that are monitored, or define a dynamic membership rule.
   a  In the vCenter Web Client, navigate to **Networking & Security > Service Composer**.
   b  Edit the **Activity Monitoring Data Collection** security group.
   c  Define a dynamic membership rule so that as new Windows VMs are added to the cluster, the VM will automatically be monitored.
   d  Select vCenter objects to include or exclude in the activity monitoring security group.

   The VMs on which you enabled activity monitoring are automatically included in the activity monitoring security group.

   In this example, all VMs with names starting with "win" are automatically added to the activity monitoring security group. This means that activity monitoring will be automatically enabled on them.
Activity Monitoring Scenarios

This section describes some hypothetical scenarios for Activity Monitoring.

User Access to Applications

Our hypothetical company, ACME Enterprise, only permits approved users to access specific applications on corporate assets.

Their security policy mandates are:

- Allow only authorized users to access critical business applications
- Allow only authorized applications on corporate servers
- Allow access to only required ports from specific networks

Based on the above, they need controlled access for employees based on user identity to safeguard corporate assets. As a starting point, the security operator at ACME Enterprise needs to be able to verify that only administrative access is allowed to the MS SQL servers.

Procedure

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then Activity Monitoring.
3. Click the Inbound Activity tab.
4. In Outbound from leave value as All Observed AD Groups to see access from any and all employees.
In **Where destination virtual machine**, select **includes**, and leave **all observed destination virtual machines** selected.

6. In **And where destination application**, select **includes**, click **all observed destination applications** and select the MS SQL servers.

7. Click **Search**.

The search results show that only administrative users are accessing the MS SQL servers. Notice that are no groups (such as Finance or HR) accessing these servers.

8. We can now invert this query by setting the **Outbound from** value to HR and Finance AD groups.

9. Click **Search**.

No records are displayed, confirming that no users from either of these groups can access MS SQL servers.

**Applications on Datacenter**

As part of their security policies, ACME Enterprise needs Visibility into all data center applications. This can help Identify rogue applications that either capture confidential information or siphon sensitive data to external sources.

John, Cloud Administrator at ACME Enterprise, wants to confirm that access to the SharePoint server is only through Internet Explorer and no rogue application (such as FTP or RDP) can access this server.

**Procedure**

1. Log in to the vSphere Web Client.

2. Click **Networking & Security** and then **Activity Monitoring**.

3. Click the **VM Activity** tab.

4. In **Where source VM**, select **includes**, and leave **All observed virtual machines** selected to capture traffic originating from all virtual machines in the datacenter.

5. In **Where destination VM**, select **includes**, click **All observed virtual machines**, and select the SharePoint server.

6. Click **Search**.

**Results**

The **Outbound App Product Name** column in the search results show that all access to the SharePoint server was only through Internet Explorer. The relatively homogenous search results indicate that there is a firewall rule applied to this SharePoint server preventing all other access methods.

Also note that the search results display the source user of the observed traffic rather than the source group. Clicking the arrow in the search result displays details about the source user such as the AD group to which the user belongs.
Verify Open Ports

Once John Admin knows that the ACME Enterprise share point server is being accessed only by authorized applications, he can ensure that the company allows only required ports to be open based on expected use.

Prerequisites

In the Applications on Datacenter scenario, John Admin had observed traffic to the ACME Enterprise share point server. He now wants to ensure that all access from the share point server to the MSSQL server is through expected protocols and applications.

Procedure

1. Click the Go Home icon.
2. Click vCenter Home and then click Virtual Machines.
3. Select win_sharepoint and then click the Monitor tab.
4. Click Activity Monitoring.
5. In Where destination, select win2K-MSSQL.
6. Click Search.

Results

Search results show traffic from the share point server to the MSSQL server. The User and Outbound App columns show that only systems processes are connecting to the MSSQL server, which is what John expected to see.

The Inbound Port and App columns show that all access is to the MSSQL server running on the destination server.

Since there are too many records in the search results for John to analyze in a web browser, he can export all the entire result set and save the file in a CSV format by clicking the icon on the bottom right side of the page.

Enable Data Collection

You must enable data collection for one or more virtual machines on a vCenter Server before running an Activity Monitoring report. Before running a report, ensure that the enabled virtual machines are active and are generating network traffic.

You should also register NSX Manager with the AD Domain Controller. See Register a Windows Domain with NSX Manager.

Note that only active connections are tracked by Activity Monitoring. Virtual machine traffic blocked by firewall rules at the vNIC level is not reflected in reports.
Enable Data Collection on a Single Virtual Machine
You must enable data collection at least five minutes before running an Activity Monitoring report.

**Prerequisites**

**Procedure**
1. Log in to the vSphere Web Client.
2. Click **vCenter** and then click **VMs and Templates**.
3. Select a virtual machine from the left inventory panel.
4. Click the **Manage** tab and then click the **Settings** tab.
5. Click **NSX Activity Monitoring** from the left panel.
6. Click **Edit**.
7. In the Edit NSX Activity Monitoring Data Collection Settings dialog box, click **Yes**.

Enable Data Collection for Multiple Virtual Machines
The Activity Monitoring Data Collection security group is a pre-defined security group. You can add multiple virtual machines to this security group at a time, and data collection is enabled on all of these virtual machines.

You must enable data collection at least five minutes before running an Activity Monitoring report.

**Procedure**
1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **Service Composer**.
3. Click the **Security Groups** tab.
4. Select the Activity Monitoring Data Collection security group and click the **Edit (✏️)** icon.
5. Follow the wizard to add virtual machines to the security group.

Data collection is enabled on all virtual machines you added to this security group, and disabled on any virtual machines you excluded from the security group.

View Virtual Machine Activity Report
You can view traffic to or from a virtual machine or a set of virtual machines in your environment.

You can either do a quick query using the default search criteria by clicking **Search**, or tailor the query according to your requirements.

**Prerequisites**
- Guest Introspection must be installed in your environment.
A domain must be registered with NSX Manager. For information on domain registration, see Register a Windows Domain with NSX Manager.

Data collection must be enabled on one or more virtual machines.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then **Activity Monitoring**.
3. Click the **VM Activity** tab.
4. Click the link next to **Where source**. Select the virtual machines for which you want to view outbound traffic. Indicate whether you want to include or exclude the selected virtual machine(s) from the report.
5. Click the link next to **Where destination**. Select the virtual machines for which you want to view inbound traffic. Indicate whether you want to include or exclude the selected virtual machine(s) from the report.
6. Click the **During period** icon and select the time period for the search.
7. Click **Search**.

**Results**

Search results filtered by the specified criterion are displayed. Click a row to view detailed information about the user for that row.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the icon on the bottom right side of the page.

**View Inbound Activity**

You can view all inbound activity to a server by desktop pool, security group, or AD group.
You can either do a quick query using the default search criteria by clicking Search, or tailor the query according to your requirements.

**Prerequisites**

- Guest Introspection must be installed in your environment.
- A domain must be registered with NSX Manager. For information on domain registration, see Register a Windows Domain with NSX Manager.
- Data collection must be enabled on one or more virtual machines.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click Networking & Security and then Activity Monitoring.
3. Click the Inbound Activity tab.
4. Click the link next to Originating from.
5. Select the type of user group that you want to view activity for.
6. In Filter type, select one or more group and click OK.
7. In Where destination virtual machine, select includes or excludes to indicate whether the selected virtual machines should be included in or excluded from the search.
8. Click the link next to And where destination virtual machine.
9. Select one or more virtual machine and click OK.
10. In And where destination application, select includes or excludes to indicate whether the selected applications should be included in or excluded from the search.
11 Click the link next to And where destination application.

12 Select one or more application and click OK.

13 Click the During period (.monitor) icon and select the time period for the search.

14 Click Search.

Results

Search results filtered by the specified criterion are displayed. Click anywhere in the results table to view information about the users that accessed the specified virtual machines and applications.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the icon on the bottom right side of the page.

View Outbound Activity

You can view what applications are being run by a security group or desktop pool and then drill down into the report to find out which client applications are making outbound connections by a particular group of users. You can also discover all user groups and users who are accessing a particular application, which can help you determine if you need to adjust identity firewall in your environment.

Figure 22-7. View Outbound activity

Prerequisites

- Guest Introspection must be installed in your environment.
- A domain must be registered with NSX Manager. For information on domain registration, see Register a Windows Domain with NSX Manager.
- Data collection must be enabled on one or more virtual machines.

Procedure

1 Log in to the vSphere Web Client.

2 Click Networking & Security and then Activity Monitoring.

3 Ensure that the Outbound Activity tab is selected in the left pane.

4 Click the link next to Originating from.

   All groups discovered through guest introspection are displayed.

5 Select the type of user group that you want to view resource utilization for.

6 In Filter, select one or more group and click OK.
7 In **Where application**, select *includes* or *excludes* to indicate whether the selected application should be included in or excluded from the search.

8 Click the link next to **Where application**.

9 Select one or more application and click **OK**.

10 In **And where destination**, select *includes* or *excludes* to indicate whether the selected virtual machines should be included in or excluded from the search.

11 Click the link next to **And where destination**.

12 Select one or more virtual machine and click **OK**.

13 Click the **During period** icon and select the time period for the search.

14 Click **Search**.

Scroll to the right to see all the information displayed.

**Results**

Search results filtered by the specified criterion are displayed. Click a row to view information about users within that AD group that used the specified application to access the specified virtual machines.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the icon on the bottom right side of the page.

**View Interaction between Inventory Containers**

You can view the traffic passing between defined containers such as AD groups, security groups and/or desktop pools. This can help you identify and configure access to shared services and to resolve mis-configured relationships between Inventory container definitions, desktop pools and AD groups.

**Figure 22-8. Interaction between containers**

You can either do a quick query using the default search criteria by clicking **Search**, or tailor the query according to your requirements.

**Prerequisites**

- Guest Introspection must be installed in your environment.

- A domain must be registered with NSX Manager. For information on domain registration, see [Register a Windows Domain with NSX Manager](#).
Data collection must be enabled on one or more virtual machines.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then **Activity Monitoring**.
3. Select the **Inter Container Interaction** tab in the left pane.
4. Click the link next to **Originating from**.
   - All groups discovered through guest introspection are displayed.
5. Select the type of user group that you want to view resource utilization for.
6. In **Filter**, select one or more group and click **OK**.
7. In **Where the destination is**, select **is** or **is not** to indicate whether the selected group should be included in or excluded from the search.
8. Click the link next to **Where the destination is**.
9. Select the group type.
10. In **Filter**, select one or more group and click **OK**.
11. Click the **During period** (📅) icon and select the time period for the search.
12. Click **Search**.

**Results**

Search results filtered by the specified criterion are displayed. Click in a row to view information about the users that accessed the specified containers.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the icon on the bottom right side of the page.

**Example: Interaction between Inventory Containers Query**

- **Verify allowed communication**
  
  If you have defined containers in your vCenter inventory and then added a rule to allow communication between these containers, you can verify that the rule is working by running this query with the two containers specified in the **Originating from** and **Where the destination is** fields.

- **Verify denied communication**
  
  If you have defined containers in your vCenter inventory and then added a rule to deny communication between these containers, you can verify that the rule is working by running this query with the two containers specified in the **Originating from** and **Where the destination is** fields.

- **Verify denied intra-container communication**
If you have implemented a policy that does not allow members of a container communicating with other members of the same container, you can run this query to verify that the policy works. Select the container in both **Originating from** and **Where the destination is** fields.

- Eliminate unnecessary access

Suppose you have defined containers in your vCenter inventory and then added a rule to allow communication between these containers. There may be members in either container that do not interact with the other container at all. You may then choose to remove these members from the appropriate container to optimize security control. To retrieve such a list, select the appropriate containers in both **Originating from** and **Where the destination is** fields. Select **is not** next to the **Where the destination is** field.

**View Outbound AD Group Activity**

You can view the traffic between members of defined Active Directory groups and can use this data to fine-tune your firewall rules.

You can either do a quick query using the default search criteria by clicking **Search**, or tailor the query according to your requirements.

**Prerequisites**

- Guest Introspection must be installed in your environment.
- A domain must be registered with NSX Manager. For information on domain registration, see **Register a Windows Domain with NSX Manager**.
- Data collection must be enabled on one or more virtual machines.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then **Activity Monitoring**.
3. Select the **AD Groups & Containers** tab in the left pane.
4. Click the link next to **Originating from**.
   
   All groups discovered through guest introspection are displayed.
5. Select the type of user group that you want to include in the search.
6. In **Filter**, select one or more group and click **OK**.
7. In **Where AD Group**, select **includes** or **excludes** to indicate whether the selected AD group should be included in or excluded from the search.
8. Click the link next to **Where AD Group**.
9. Select one or more AD groups and click **OK**.
10. Click the **During period** icon and select the time period for the search.
11. Click **Search**.

**Results**

Search results filtered by the specified criterion are displayed. Click in a row to view information about the members of the specified AD group that are accessing network resources from within the specified security group or desktop pool.

You can export a specific record or all records on this page and save them to a directory in a .csv format by clicking the **Export** icon on the bottom right side of the page.

**Override Data Collection**

In case of an emergency such as a network overload, you can turn off data collection at a global level. This overrides all other data collection settings.

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then **Activity Monitoring**.
3. Click the **Settings** tab.
4. Select the vCenter Server for which you want to overwrite data collection.
5. Click **Edit**.
6. De-select **Collect reporting data**.
7. Click **OK**.

**Endpoint Monitoring Data Collection**

Endpoint monitoring enables users to map specific processes inside the guest OS to the network connections the processes are using.

**Note** After data is gathered, it is purged daily at 2:00 a.m. During the data purge the number of flow records across all sessions combined is checked, and any records above 20 million (or ~4GB) are deleted. Deletion begins with the oldest session, and continues until the number of flow records in the database is below 15 million records. If a session is in progress during the data purge, some records could be lost.

**Prerequisites**

- Endpoint Monitoring is supported on following Windows Operating systems:
- Guest introspection must be installed on Virtual Machines (VMs).
- VMware Tools must be running and current on your Windows desktop VMs.
Security Groups with 20 or fewer VMs are needed for data collection before Endpoint Monitoring can begin. See Create a Security Group for more information.

Data collection must be enabled for one or more virtual machines on a vCenter Server before running an Endpoint Monitoring report. Before running a report, verify that the enabled virtual machines are active, and are generating network traffic.

Procedure

1. Log in to the vSphere Web Client, then select Networking & Security from the left navigation pane.
2. Select Endpoint Monitoring.
3. On the Summary tab, click Start Collecting Data.
4. On the Start Data Collection for Security Groups pop-up window, select the security groups for which you want to collect data. Click OK.
   The VMs are listed in the field box.
5. Turn data collection ON.
6. Click OK.
   The main Endpoint Monitoring Screen appears. In the left hand corner the status is Collecting Data.
7. Click Stop Collecting Data to end the data collection.
   The EndPoint Monitoring screen appears with the Summary tab populated with data.

Endpoint Monitoring

Endpoint Monitoring enables visibility into specific application processes and their associated network connections.

Summary Tab

After data collection is completed, the summary screen displays the details of the NSX manager, the security group and the time slot of the collected data. The number of running virtual machines (VMs) and the total number of processes generating traffic is shown in the first box. Clicking the number of virtual machines running takes you to the VM Flows tab, described below. Clicking the number of processes generating traffic takes you to the Process Flows tab, described below.

The second box displays a donut with the total number of flows. A flow is any unique stream of network traffic as identified by its packet type, source and destination IP, and port. Hover the cursor over each section and the number of flows within the security group or outside the security group is shown.

VM Flows Tab

This screen displays the details of the flows within the VMs including:

- VM name - Name of the VM that is being monitored
- Flows within security group - Traffic flowing between the VMs where the source or destination is inside the monitored security group
- Flows outside security group - Traffic flowing between the VMs where the source or destination is outside the monitored security group
- Shared service flows outside group - Shared service flows such as DHCP, LDAP, DNS, or NTP, outside the monitored security group
- Shared service flows inside security group - Shared service such as DHCP, LDAP, DNS, or NTP, inside the monitored security group

Clicking on a specific VM name in the table displays a bubble graph that shows the following:
- flows between VMs in the same security group
- flows that contain shared services
- flows between different security groups

Click on a bubble to view the details of the VM. The detailed flow view includes the process name, version and number of flows being generated by each process. If it contains shared services there is a special icon that is visible. Clicking on a line between two VM bubbles displays the process flow details of the flows between those two VMs including:
- Source process - Name of application/exe generating traffic and initiating the flow
- Source version - File version of source
- Protocol - TCP
- Destination process - Name of the server application/exe of the process that is the destination of the flow
- Destination port - Port number of the destination

**Process Flows Tab**

This screen displays a list of all the applications that are generating flows. The table displays the following:
- Process Name - The name of application generating traffic
- VM name
- Flows within security group - Traffic flowing between the VMs where the source or destination is inside the monitored security group
- Flows outside security group - Traffic flowing between the VMs where the source or destination is outside the monitored security group
- Shared flows within security group - Shared flows, within the monitored security group
- Shared flows outside security group - Shared flows, outside the monitored security group
The bubble graph depicts the flows that are occurring with the process or application on the selected VM as the anchor. Click on any of the bubbles for the process name and version. Click on any line to display the following:

- Source VM - The name of client VM that is hosting the client process
- Source IP - IP address of the flow
- Protocol - TCP
- Destination VM - The name of the server VM that is hosting the server process
- Destination IP - IP address of the destination
- Destination port - Port number of the destination

**Traceflow**

Traceflow is a troubleshooting tool that provides the ability to inject a packet and observe where that packet is seen as it passes through the physical and logical network. The observations allow you to determine information about the network, such as identifying a node that is down or a firewall rule that is preventing a packet from being received by its destination.

**About Traceflow**

Traceflow injects packets into a vSphere distributed switch (VDS) port and provides various observation points along the packet’s path as it traverses physical and logical entities (such as ESXi hosts, logical switches, and logical routers) in the overlay and underlay networks. This allows you to identify the path (or paths) a packet takes to reach its destination or, conversely, where a packet is dropped along the way. Each entity reports the packet handling on input and output, so you can determine whether issues occur when receiving a packet or when forwarding the packet.

Keep in mind that traceflow is not the same as a ping request/response that goes from guest-VM stack to guest-VM stack. What traceflow does is observe a marked packet as it traverses the overlay network. Each packet is monitored as it crosses the overlay network until it reaches and is deliverable to the destination guest VM. However, the injected traceflow packet is never actually delivered to the destination guest VM. This means that a traceflow can be successful even when the guest VM is powered down.

Traceflow supports the following traffic types:

- Layer 2 unicast
- Layer 3 unicast
- Layer 2 broadcast
- Layer 2 multicast
You can construct packets with custom header fields and packet sizes. The source for the traceflow is always a virtual machine virtual NIC (vNIC). The destination endpoint can be any device in the NSX overlay or in the underlay. However, you cannot select a destination that is north of an NSX edge services gateway (ESG). The destination must be on the same subnet or must be reachable through NSX distributed logical routers.

The traceflow operation is considered Layer 2 if the source and destination vNICs are in the same Layer 2 domain. In NSX, this means that they are on the same VXLAN network identifier (VNI or segment ID). This happens, for example, when two VMs are attached to the same logical switch.

If NSX bridging is configured, unknown Layer 2 packets are always be sent to the bridge. Typically, the bridge forwards these packets to a VLAN and reports the traceflow packet as delivered. A packet reported as delivered does not necessarily mean that the trace packet was delivered to the specified destination.

For Layer 3 traceflow unicast traffic, the two end points are on different logical switches and have different VNIs, connected to a distributed logical router (DLR).

For multicast traffic, the source is a VM vNIC, and the destination is a multicast group address.

Traceflow observations may include observations of broadcasted traceflow packets. The ESXi host broadcasts a traceflow packet if it does not know the destination host's MAC address. For broadcast traffic, the source is a VM vNIC. The Layer 2 destination MAC address for broadcast traffic is FF:FF:FF:FF:FF:FF. To create a valid packet for firewall inspection, the broadcast traceflow operation requires a subnet prefix length. The subnet mask enables NSX to calculate an IP network address for the packet.

**Caution** Depending on the number of logical ports in your deployment, multicast and broadcast traceflow operations might generate high traffic volume.

There are two ways to use traceflow: through the API and through the GUI. The API is the same API that the GUI uses, except the API allows you to specify the exact settings within the packet, while the GUI has more limited settings.

The GUI allows you to set the following values:

- Protocol---TCP, UDP, ICMP.
- Time-to-live (TTL). The default is 64 hops.
- TCP and UDP source and destination port numbers. The default values are 0.
- TCP flags.
- ICMP ID and sequence number. Both are 0 by default.
- An expiry timeout, in milliseconds (ms), for the traceflow operation. The default is 10,000 ms.
- Ethernet frame size. The default is 128 bytes per frame. The maximum frame size is 1000 bytes per frame.
- Payload encoding. The default is Base64.
Payload value.

Use Traceflow for Troubleshooting

There are multiple scenarios in which traceflow is useful.

Traceflow is useful in the following scenarios:

- Troubleshooting network failures to see the exact path that traffic takes
- Performance monitoring to see link utilization
- Network planning to see how a network will behave when it is in production

Prerequisites

- Traceflow operations require communication among vCenter, NSX Manager, the NSX Controller cluster and the netcpa user world agents on the hosts.
- For Traceflow to work as expected, make sure that the controller cluster is connected and in healthy state.

Procedure


2. Select the traffic type: Unicast, broadcast, or multicast.

3. Select the source VM vNIC.

   If the VM is managed in the same vCenter Server where you are running the traceflow, you can select the VM and vNIC from a list.
4 For a unicast traceflow, enter the destination vNIC information.

The destination can be a vNIC of any device in the NSX overlay or underlay, such as a host, a VM, a logical router, or an edge services gateway. If the destination is a VM that is running VMware Tools and is managed in the same vCenter Server from which you are running the traceflow, you can select the VM and vNIC from a list.

Otherwise, you must enter the destination IP address (and the MAC address for a unicast Layer 2 traceflow). You can gather this information from the device itself in the device console or in an SSH session. For example, if it is a Linux VM, you can get its IP and MAC address by running the `ifconfig` command in the Linux terminal. For a logical router or edge services gateway, you can gather the information from the `show interface` CLI command.

5 For a Layer 2 broadcast traceflow, enter the subnet prefix length.

The packet is switched based on MAC address only. The destination MAC address is `FF:FF:FF:FF:FF:FF`.

Both the source and destination IP addresses are required to make the IP packet valid for firewall inspection.

6 For a Layer 2 multicast traceflow, enter the multicast group address.

The packet is switched based on MAC address only.

Both the source and destination IP addresses are required to make the IP packet valid. In the case of multicast, the MAC address is deduced from the IP address.

7 Configure other required and optional settings.

8 Click **Trace**.

**Example: Scenarios**

The following example shows a Layer 2 traceflow involving two VMs that are running on a single ESXi host. The two VMs are connected to a single logical switch.
The following example shows a Layer 2 traceflow involving two VMs that are running on two different ESXi hosts. The two VMs are connected to a single logical switch.
The following example shows a Layer 3 traceflow. The two VMs are connected to two different logical switches that are separated by a logical router.
The following example shows a broadcast traceflow in a deployment that has three VMs connected to a single logical switch. Two of the VMs are on one host (esx-01a), and the third is on another host (esx-02a). The broadcast is sent from one of the VMs on host 192.168.210.53.
The following example shows what happens when multicast traffic is sent in a deployment that has multicast configured.
The following example shows what happens when a traceflow is dropped because of a distributed firewall rule that blocks ICMP traffic sent to the destination address. Notice that the traffic never leaves the original host, even though the destination VM is on another host.
The following example shows what happens when a traceflow destination is on the other side of an edge services gateway, such as an IP address on the Internet or any internal destination that must be routed through the edge services gateway. The traceflow is not allowed, by design, because traceflow is supported for destinations that are either on the same subnet or are reachable through distributed logical routers (DLRs).

The following example shows what happens when the traceflow destination is a VM that is on another subnet and is powered off.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Observation Type</th>
<th>Host</th>
<th>Component Type</th>
<th>Component Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>injected</td>
<td>esx-02a.corp.local</td>
<td>vNIC</td>
<td>vNIC</td>
</tr>
<tr>
<td>1</td>
<td>Received</td>
<td>esx-02a.corp.local</td>
<td>Firewall</td>
<td>Firewall</td>
</tr>
<tr>
<td>2</td>
<td>Forwarded</td>
<td>esx-02a.corp.local</td>
<td>Firewall</td>
<td>Firewall</td>
</tr>
<tr>
<td>3</td>
<td>Forwarded</td>
<td>esx-02a.corp.local</td>
<td>Logical Switch</td>
<td>App-Tier-01</td>
</tr>
<tr>
<td>4</td>
<td>Received</td>
<td>esx-02a.corp.local</td>
<td>Logical Router</td>
<td>Local-Distributed Router</td>
</tr>
<tr>
<td>5</td>
<td>Forwarded</td>
<td>esx-02a.corp.local</td>
<td>Logical Router</td>
<td>Local-Distributed Router</td>
</tr>
<tr>
<td>6</td>
<td>Received</td>
<td>esx-02a.corp.local</td>
<td>Logical Switch</td>
<td>DB-Tier-01</td>
</tr>
</tbody>
</table>