You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to
docfeedback@vmware.com
Contents

About VMware Cloud on AWS Networking and Security  5

1  NSX-T Networking Concepts  6
   Features Supported with NSX-T  10

2  Configuring VMware Cloud on AWS Networking and Security Using NSX-T  12
   Assign NSX Service Roles to Organization Members  13
   Configure VMware Cloud on AWS to use AWS Direct Connect  14
      Set Up an AWS Direct Connect Connection  15
      Create a Private Virtual Interface for SDDC Management and Compute Network Traffic  15
      Create a Public Virtual Interface for Access to AWS Services  17
      Configure vMotion Interfaces for Use with Direct Connect  18
   Configure a VPN Connection Between Your SDDC and On-Premises Data Center  19
      Create a Route-Based VPN  19
      Create a Policy-Based VPN  22
      View VPN Tunnel Status and Statistics  24
      IPsec VPN Settings Reference  25
   Configure Management Gateway Networking and Security  26
      Set vCenter Server FQDN Resolution Address  27
      Set HCX FQDN Resolution Address  27
      Add or Modify Management Gateway Firewall Rules  28
   Configure Compute Gateway Networking and Security  30
      Create or Modify a Network Segment  31
      Configure a Layer 2 VPN and Extended Network Segment  33
      Add or Modify Compute Gateway Firewall Rules  35
      Add or Modify Distributed Firewall Rules  38
      Configure DNS Services  42
      Configure Compute Gateway DHCP Relay  44
   Working With Inventory Groups  44
      Add a Management Group  45
      Add or Modify a Compute Group  45
      Add a Custom Service  47
      View Virtual Machine Inventory  47
   Managing Workload Connections  48
      Attach a VM to or Detach a Workload VM from a Compute Network Segment  48
      Request or Release a Public IP Address  49
      Create or Modify NAT Rules  49
      Creating Firewall Rules to Manage Traffic Between the Compute and Management Networks  51
3 Configure Monitoring and Troubleshooting Features 53
   Configure IPFIX 53
   Configure Port Mirroring 54
   View Connected VPC Information 55
About VMware Cloud on AWS Networking and Security

The VMware Cloud on AWS Networking and Security guide provides information about configuring NSX-T networking and security for VMware Cloud on AWS.

Intended Audience

This information is intended for anyone who wants to use VMware Cloud on AWS to create an SDDC that has the networking and security infrastructure necessary to migrate workloads off premises and run them securely in the cloud. It was written for readers who have used vSphere in an on-premises environment and are familiar with the fundamentals of IP networking using NSX-T or another networking solution. In-depth knowledge of vSphere or Amazon Web Services is not required.

For a detailed discussion of how VMware Cloud on AWS uses NSX-T networking, see the VMware Press eBook VMware Cloud on AWS: NSX Networking and Security.
VMware Cloud on AWS uses NSX-T to create and manage internal SDDC networks and provide endpoints for VPN connections from your on-premises network infrastructure.

**Connecting to your SDDC**

To connect your on-premises data center to your VMware Cloud on AWS SDDC, you can create a VPN that uses the public Internet, a VPN that uses AWS Direct Connect, or just use AWS Direct Connect alone.

**Figure 1-1. SDDC Connections to your On-Premises Data Center**

Layer 3 (L3) VPN

A layer 3 VPN provides a management network that connects your on-premises data center to your SDDC. These IPsec VPNs can be either route-based or policy-based. You can create up to sixteen VPNs of each type, using any on-premises router that supports the settings listed in the IPsec VPN Settings Reference. An L3 VPN can connect your on-premises...
data center to the SDDC over the public Internet or over AWS Direct Connect.

**Layer 2 (L2) VPN**

A layer 2 VPN provides an extended, or stretched, network with a single IP address space that spans your on-premises data center and your SDDC and enables hot or cold migration of on-premises workloads to the SDDC. You can create only a single L2VPN tunnel in any SDDC. The on-premises end of the tunnel requires NSX. If you are not already using NSX in your on-premises data center, you can download a standalone NSX Edge appliance to provide the required functionality. An L2 VPN can connect your on-premises data center to the SDDC over the public Internet or over AWS Direct Connect.

**AWS Direct Connect (DX)**

AWS Direct Connect is a service provided by AWS that allows you to create a high-speed, low latency connection between your on-premises data center and AWS services. When you configure AWS Direct Connect, VPNs can use it instead of routing traffic over the public Internet. Because Direct Connect implements Border Gateway Protocol (BGP) routing, use of an L3VPN for the management network is optional when you configure Direct Connect. Traffic over Direct Connect is not encrypted. If you want to encrypt that traffic, configure your L3 VPN to use Direct Connect.

**VMware HCX**

VMware HCX, a multi-cloud app mobility solution, is provided free to all SDDCs and facilitates migration of workload VMs to and from your on-premises data center to your SDDC. For more information about installing, configuring, and using HCX, see the Hybrid Migration with HCX Checklist.

**SDDC Network Topology**

When you create an SDDC, it includes a Management Network and a Compute Network. The Management Network CIDR block must be specified when you created the SDDC and cannot be changed. The Management Network has two subnets:

**Appliance Subnet**

A subnet of the CIDR range you specified for the Management Subnet when you created the SDDC. This subnet is used by the vCenter, NSX, and HCX appliances in the SDDC. When you add appliance-based services such as SRM to the SDDC, they also connect to this subnet.

**Infrastructure Subnet**

A subnet of the CIDR range you specified for the Management Subnet when you created the SDDC. This subnet is used by the ESXi hosts in the SDDC.

The Compute Network includes an arbitrary number of logical segments for your workload VMs. In a Single Host SDDC starter configuration, we create a compute network with a single routed segment. In SDDC configurations that have more hosts, you'll have to create compute network segments to meet your needs. See Configuration Maximums for VMware Cloud on AWS for applicable limits.
An SDDC network has two notional tiers:

- Tier 0 is served by an NSX Edge appliance.
- Tier 1 is served by two NSX Edge firewalls (the Management Gateway and the Compute Gateway).

**Figure 1-2. SDDC Network Topology**

**NSX Edge Appliance**

All traffic between your on-premises networks and your SDDC networks passes through this appliance. Compute Gateway firewall rules, which control access to workload VMs, are applied on its uplink interfaces.

**Management Gateway (MGW)**

The MGW is an NSX Edge firewall that provides north-south network connectivity for the vCenter Server and other management appliances running in the SDDC. The Internet-facing IP address of the MGW is automatically assigned from the pool of AWS public IP addresses when the SDDC is created. See [Deploy an SDDC from the VMC Console](#) for more details.
about specifying this address range. If you don't specify a range when you create the SDDC, the system uses a default of 10.2.0.0/16.

**Compute Gateway (CGW)**

The CGW is an NSX Edge firewall that provides north-south network connectivity for virtual machines running in the SDDC. In a single-node SDDC, VMware Cloud on AWS creates a default logical network segment (CIDR block 192.168.1.0/24) to provide networking for these VMs. You can create additional logical networks on the **Networking & Security** tab.

### Routing Between Your SDDC and the Connected VPC

**Important** All SDDC subnets and any VPC subnets on which AWS services or instances communicate with the SDDC must be associated with the main route table of the connected VPC. Use of a custom route table or replacement of the main route table is not supported.

When you create an SDDC, we connect the ENI of the VPC owned by the AWS account you specify to the NSX Edge Appliance in the SDDC. That VPC becomes the Connected VPC, and the connection supports network traffic between SDDC VMs and AWS instances and native services in the Connected VPC. The main route table of the connected VPC includes all the subnets in the VPC as well as all SDDC (NSX-T network segment) subnets. When you create or delete routed network segments on the workload network, the main route table is automatically updated. When the NSX Edge Appliance in your SDDC is moved to another host, either to recover from a failure or during SDDC maintenance, the main route table is updated to reflect the ENI used by the new NSX Edge host. If you have replaced the main route table or are using a custom route table, that update fails and network traffic can no longer be routed between SDDC networks and the Connected VPC.

For more information, see [View Connected VPC Information](#).

### Reserved Network Addresses

The entire address range 100.64.0.0/10 (reserved for carrier-grade NAT per [RFC 6598](#)) is reserved by VMware Cloud on AWS for internal use. You cannot access any remote (on-premises) networks in that address range from workloads in the SDDC, and you cannot use any addresses in that range within the SDDC.

### Multicast Support in SDDC Networks

In SDDC networks, layer 2 multicast traffic is treated as broadcast traffic on the network segment where the traffic originates. It is not routed beyond that segment. Layer 2 multicast traffic optimization features such as IGMP snooping are not supported. Layer 3 multicast (such as Protocol Independent Multicast) is not supported in VMware Cloud on AWS.

This chapter includes the following topics:

- [Features Supported with NSX-T](#)
Features Supported with NSX-T

SDDCs backed by NSX-T support a wide range of networking and security solutions. NSX-T was designed specifically to support diverse data center environments at scale and provide robust capabilities for containers and the cloud.

Note NSX-T Configuration Maximums are now included in Configuration Maximums for VMware Cloud on AWS.

Networking and Connectivity Features

NSX-T provides all the networking capabilities required by workloads running in the SDDC. These capabilities allow you to:

- Deploy networks (L2, L3, and isolated) and define subnets and gateways for the workloads that will reside there.
  - L2VPNs extend your on-premises L2 domains to the SDDC, enabling workload migration without IP address changes.
  - Route-based IPSEC VPNs can connect to on-premises networks, VPCs, or other SDDCs. Route-based VPNs use BGP to learn new routes as networks become available.
  - Policy-based IPSEC VPNs can also be used to connect to on-premises networks, VPCs, or other SDDCs.
  - Isolated networks have no uplinks, and provide access only to those VMs connected to them.
- Use AWS Direct Connect (DX) to carry traffic between on-premises and SDDC networks over high bandwidth, low latency connectivity. You can optionally use a route-based VPN as backup for DX traffic.
- Enable native DHCP selectively for network segments or use DHCP relay to link with an on-premises IPAM solution.
- Create multiple DNS zones, allowing use of different DNS servers for network subdomains.
- Take advantage of distributed routing, managed by an NSX kernel module running on the host where the workload resides, so workloads can efficiently communicate with each other.

Security Features

NSX-T security features include network address translation (NAT) and advanced firewall capabilities.

- Source NAT (SNAT) is automatically applied to all workloads in the SDDC to enable Internet access. To provide a secure environment, Internet access is blocked at edge firewalls, but firewall policy can be changed to allow managed access. You can also request a public IP for workloads and create custom NAT policies for them.
- Edge firewalls run on the management and compute gateways. These stateful firewalls examine all traffic into and out of the SDDC.
- Distributed Firewall (DFW) is a stateful firewall that runs on all SDDC hosts. It provides protection for traffic within the SDDC and enables micro-segmentation to allow fine-grained control over traffic between workloads.

**Network Operations Tools**

NSX-T also provides several popular network operations management tools.

- Port mirroring can send mirrored traffic from a source to a destination appliance in the SDDC or your on-premises network.
- IPFIX supports segment-specific network traffic analysis by sending traffic flows to an IPFIX collector.
Follow this workflow to configure NSX-T networking and security in your SDDC.

Procedure

1 Assign NSX Service Roles to Organization Members
   Grant users in your organization the NSX Admin service role to allow them to view and configure features on the Networking & Security tab.

2 Configure VMware Cloud on AWS to use AWS Direct Connect
   Use of AWS Direct Connect is optional. If traffic between your on-premises network and your SDDC workloads requires higher speeds and lower latency than you can achieve with a connection over the public Internet, configure VMware Cloud on AWS to use AWS Direct Connect.

3 Configure a VPN Connection Between Your SDDC and On-Premises Data Center
   Configure a VPN to provide a secure connection to your SDDC over the public Internet or AWS Direct Connect. Route-based and policy-based VPNs are supported. Either type of VPN can connect to the SDDC over the Internet. A route-based VPN can also connect to the SDDC over AWS Direct Connect.

4 Configure Management Gateway Networking and Security
   The management network and Management Gateway are largely preconfigured in your SDDC, but you'll still need to configure access to management network services like vCenter and HCX and create management gateway firewall rules to allow traffic between the management network and other networks, including your on-premises networks and other SDDC networks.

5 Configure Compute Gateway Networking and Security
   Compute Gateway networking includes a compute network with one or more segments and the DNS, DHCP, and security (gateway firewall and distributed firewall) configurations that manage network traffic for workload VMs. It can also include a layer 2 VPN and extended network that provides a single broadcast domain that spans your on-premises network and your SDDC workload network.

6 Working With Inventory Groups
   Use VMware Cloud on AWS Networking & Security inventory to create groups of VMs and network services that you can use when you create firewall rules.
Managing Workload Connections

Workload VMs connect to the Internet by default. NAT rules and distributed firewall rules give you fine-grained control over these connections.

Assign NSX Service Roles to Organization Members

Grant users in your organization the NSX Admin service role to allow them to view and configure features on the Networking & Security tab.

Organization roles specify the privileges that an organization member has over organization assets. Service roles specify the privileges that an organization member has when accessing VMware Cloud Services that the organization uses. All service roles can be assigned and changed by a user with organization owner privileges, so restrictive roles such as Administrator (Delete Restricted) or NSX Cloud Auditor should be assigned along with the role of organization member to prevent modification.

A user must log out and then log back in for a new service role to take effect.

Prerequisites

You must be an Organization Owner to assign a role to an organization member.

Procedure

2. Click the services icon and select Identity & Access Management.
3. Select a user and click Edit Roles.
4. Select a role name from the Assign Organization Roles drop-down control.
   - The following roles are available:
     - **Organization Owner**: This role has full rights to manage organization members and assets.
     - **Organization Member**: This role has rights to access organization assets.
5. Select the VMware Cloud on AWS service name under Assign Service Roles.
6. Select an NSX service role to assign.
   - The following NSX service roles are available:
     - **NSX Cloud Auditor**: This role can view NSX service settings and events but cannot make any changes to the service.
     - **NSX Cloud Admin**: This role can perform all tasks related to deployment and administration of the NSX service.

   **Note**: When multiple service roles are assigned to an organization user, permissions are granted for the most permissive role. For example, an organization member who has both the NSX Cloud Admin and NSX Cloud Auditor roles is granted all the NSX Cloud Admin permissions, which include those granted to the NSX Cloud Auditor role.
Click **SAVE** to save your changes.

**What to do next**

Ensure that any users whose roles were changed log out and log back in for the changes to take effect.

**Configure VMware Cloud on AWS to use AWS Direct Connect**

Use of AWS Direct Connect is optional. If traffic between your on-premises network and your SDDC workloads requires higher speeds and lower latency than you can achieve with a connection over the public Internet, configure VMware Cloud on AWS to use AWS Direct Connect.

AWS Direct Connect (DX) provides a dedicated network connection between your on-premises network infrastructure and a virtual interface (VIF) in your AWS VPC. DX supports two kinds of virtual interfaces:

- A private VIF enables access to your AWS Virtual Private Cloud (VPC).
- A public VIF enables access to services such as Amazon EC2 and S3.

Configure DX over a private VIF to carry workload and management traffic, including VPN and vMotion, between your on-premises data center and your connected VPC. Configure DX over a public VIF if you need to connect to AWS public endpoints such as EC2 and S3. You can route VPN traffic over either kind of VIF to provide additional data security.

**Private and Public VIFs**

A DX connection over a private VIF can be used for all traffic between your on-premises data center and your SDDC. It terminates in your connected Amazon VPC, provides a private IP address space, and uses BGP to advertise routes in your SDDC and learn routes in your on-premise data center.

A DX connection over a public VIF is typically used only for traffic between your on-premises data center and public AWS services, which you cannot access over a private VIF. It terminates at the AWS region level in the region occupied by your connected Amazon VPC, and uses BGP to advertise AWS global routes.

**Specifying a Larger Maximum Transmissible Unit (MTU)**

The default MTU for all SDDC networks is 1500 bytes. You can enable DX over a private or public VIF to use a larger MTU when you create the VIF. If you do this, you’ll also need to open the Global Configuration page of the Networking & Security tab and set a higher Intranet MTU Value. The value you set must be less than or equal to the smallest MTU value for all your DX virtual interfaces. In practice this means that you should set all your VIFs to the same MTU value (the default, at 1500 or Jumbo, at 9001), since having any VIF that does not support a Jumbo MTU effectively limits all DX connections to an MTU of 1500.

**Note**

To leave room for Geneve (Generic Network Virtualization Encapsulation) headers, the SDDC intranet MTU is capped at 8900 bytes to avoid packet fragmentation at the VIF.
The Jumbo MTU applies only to DX connections. Any VPN, whether or not it connects over DX, uses an MTU of 1500, regardless of other settings. You should also verify that the interface MTU of workload VMs that use the DX connection is set to a value that matches the Intranet MTU Value. Otherwise, workload VMs won’t be able to take advantage of the larger MTU.

**Set Up an AWS Direct Connect Connection**

To set up an AWS Direct Connect connection, you must place an order through the AWS console. Refer to [Getting Started with AWS Direct Connect](#) for information about how to request an AWS Direct Connect connection.

**Prerequisites**

Request your Direct Connect access in a region where VMware Cloud on AWS is available.

**What to do next**

After your AWS Direct Connect connection is established, create a private virtual interface to connect to your VMware Cloud on AWS SDDC.

**Create a Private Virtual Interface for SDDC Management and Compute Network Traffic**

You DX connection requires a private virtual interface to enable vMotion, ESXi Management, Management Appliance, and workload traffic to use it.

Create one virtual interface for each Direct Connect link you want to make to your SDDC. For example, if you want to create two Direct Connect links for redundancy, create two virtual interfaces. See [Configuration Maximums for VMware Cloud on AWS](#) for limits on the number of segments supported by each private VIF.

**Prerequisites**

- Ensure that you meet the prerequisites for virtual interfaces as described in [Prerequisites for Virtual Interfaces](#).
Procedure

1. Log in to the AWS Console and complete the *Creating a Hosted Private Virtual Interface* procedure under Create a Hosted Virtual Interface.

   If you are using a hosted connection, work with your AWS partner to create the VIF in an AWS account you own, then skip to Step 2 of this procedure. If you are using a dedicated connection or hosted VIF, take these steps first.

   a. For the Interface Owner field, use the account shown in the AWS Account ID field of the Direct Connect page of the Networking & Security tab.

   b. Select Auto-generate peer IPs and Auto-generate BGP key.

   c. (Optional) Enable Jumbo MTU.

      The default MTU for all SDDC networks is 1500 bytes. To enable DX traffic to this private VIF to use a larger MTU, select Enable under Jumbo MTU (MTU size 9001). After the VIF has been created, you’ll also need to open the Global Configuration page of the Networking & Security tab and set a higher MTU value under Intranet Uplink.

      When the interface has been created, the AWS console reports that it is ready for acceptance.

2. In the VMC Console, select Networking & Security > Direct Connect and accept the virtual interface by clicking ATTACH.

   Before it has been accepted, a new VIF is visible in all SDDCs in your organization. After you accept the VIF, it is no longer visible in any other SDDC.

   It can take up to 10 minutes for the BGP session to become active. When the connection is ready, the State shows as Attached and the BGP Status as Up.

3. (Optional) Configure a route-based VPN as backup to Direct Connect

   In the default configuration, traffic on any route advertised over BGP by both DX and a route-based VPN uses the VPN by default. To have a route advertised by both DX and VPN use DX by default and failover to the VPN when DX is unavailable, select Networking & Security > Direct Connect and set the Use VPN as backup to Direct Connect switch to Enabled.

   **Note** This configuration requires a route-based VPN. You cannot use a policy-based VPN as a backup to Direct Connect.

   The system requires a minute or so to update your routing preference. When the operation completes, routes advertised by both DX and VPN default to the DX connection, using the VPN only when DX is unavailable.
Results

A list of Advertised BGP Routes and Learned BGP Routes is displayed as the routes are learned and advertised. Click the refresh icon to refresh these lists. All routed subnets in the SDDC are advertised as BGP routes, along with this subset of management network subnets:

- Subnet 1 includes routes used by ESXi host vmks and router interfaces.
- Subnet 2 includes routes used for Multi-AZ support and AWS integration
- Subnet 3 includes management VMs

Disconnected and extended networks are not advertised.

The actual CIDR blocks advertised depend on your management subnet CIDR block. The following table shows the CIDR blocks for these routes in an SDDC that uses the default management network CIDR of 10.2.0.0 in block sizes /16, /20, and /22.

<table>
<thead>
<tr>
<th>MGW CIDR</th>
<th>Subnet 1</th>
<th>Subnet 2</th>
<th>Subnet 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.0.0/23</td>
<td>10.2.0.0/24</td>
<td>10.2.1.0/26</td>
<td>10.2.1.128/25</td>
</tr>
<tr>
<td>10.2.0.0/20</td>
<td>10.2.0.0/21</td>
<td>10.2.8.0/23</td>
<td>10.2.12.0/22</td>
</tr>
<tr>
<td>10.2.0.0/16</td>
<td>10.2.0.0/17</td>
<td>10.2.128.0/19</td>
<td>10.2.192.0/18</td>
</tr>
</tbody>
</table>

What to do next

Ensure the vMotion interfaces are configured to use Direct Connect. See Configure vMotion Interfaces for Use with Direct Connect.

Create a Public Virtual Interface for Access to AWS Services

If your workload VMs need access to AWS EC2 instances and services such as S3 over a DX connection, configure a public virtual interface for that traffic in your VPC.

In typical configurations, traffic between your on-premises data center and your SDDC flows over a private VIF. When you need to access AWS services from your SDDC, use direct connect with a public VIF. You can configure AWS security groups to manage traffic between AWS services and VMs in your SDDC.

Prerequisites

- Ensure that you meet the prerequisites for virtual interfaces as described in Prerequisites for Virtual Interfaces.
Procedure

1 Log in to the AWS Console. and complete the steps for creating a hosted public virtual interface under Create a Hosted Virtual Interface.
   a In the Interface Owner field, select My AWS Account.
   b Specify Your router peer IP and Amazon router peer IP.
   c Select Auto-generate BGP key and list any on-premises routes that you want advertised on the AWS backbone in Prefixes you want to advertise.

When the interface has been created, the AWS console reports that it is ready for acceptance.

2 In the VMC Console, select Networking & Security > Direct Connect and accept the virtual interface by clicking ATTACH.

Configure vMotion Interfaces for Use with Direct Connect

If you are using a Direct Connect connection between your on-premises data center and your cloud SDDC, you must configure the vMotion interfaces for your on-premises hosts to route vMotion traffic over the Direct Connect connection.

Prerequisites

Configure Direct Connect and create a private virtual interface.

Procedure

1 Select one of the following methods to configure the vMotion interface on each host in your on-premises environment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Override the default gateway (works for vSphere 6.5 hosts only)</td>
<td>For each host, edit the VMkernel adapter used for vMotion traffic, and select the option to override the default gateway. Enter an IP address in your on-premises vMotion subnet that is capable of routing traffic to the on-premises side of the Direct Connect connection. See Edit a VMkernel Adapter Configuration.</td>
</tr>
<tr>
<td>Configure the vMotion TCP/IP stack</td>
<td>For each host:</td>
</tr>
<tr>
<td></td>
<td>a Remove any existing vMotion VMkernel adapters.</td>
</tr>
<tr>
<td></td>
<td>b Create a new VMkernel adapter and select the vMotion TCP/IP stack. See Place vMotion Traffic on the vMotion TCP/IP Stack of an ESXi Host.</td>
</tr>
<tr>
<td></td>
<td>c Edit the host vMotion TCP/IP stack to change the routing to use an IP address in your on-premises vMotion subnet that is capable of routing traffic to the on-premises side of the Direct Connect connection. See Change the Configuration of a TCP/IP Stack on a Host.</td>
</tr>
</tbody>
</table>

2 (Optional) Test connectivity between an on-premises host and a cloud SDDC host using vmkping. See https://kb.vmware.com/s/article/1003728 for more information.
Configure a VPN Connection Between Your SDDC and On-Premises Data Center

Configure a VPN to provide a secure connection to your SDDC over the public Internet or AWS Direct Connect. Route-based and policy-based VPNs are supported. Either type of VPN can connect to the SDDC over the Internet. A route-based VPN can also connect to the SDDC over AWS Direct Connect.

- **Create a Route-Based VPN**
  A route-based VPN creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created.

- **Create a Policy-Based VPN**
  A policy-based VPN creates an IPsec tunnel and a policy that specifies how traffic uses it. When you use a policy-based VPN, you must update the routing tables on both ends of the network when new routes are added.

- **View VPN Tunnel Status and Statistics**
  The VMC Console provides status and statistics for IPSec VPNs and L2VPN segments.

- **IPsec VPN Settings Reference**
  The on-premises end of any IPsec VPN must be configured to match the settings you specified for the SDDC end of that VPN.

### Create a Route-Based VPN

A route-based VPN creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created.

VMware Cloud on AWS uses the same public IP for all VPN connections, so only a single VPN connection (Route-based, Policy-based, or L2VPN) can be created to a given remote public IP.

Route based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic and the Border Gateway Protocol (BGP) to discover and propagate routes as new networks are created. To create a route-based VPN, you configure BGP information for the local (SDDC) and remote (on-premises) endpoints, then specify tunnel security parameters for the SDDC end of the tunnel.

**Procedure**

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2. Click **Networking & Security > VPN > Route Based**.
3. (Optional) Change the default local Autonomous System Number (ASN).
   - All route-based VPNs in the SDDC default to ASN 65000. If the remote ASN for any configured VPN connection also has this value, click **EDIT LOCAL ASN**, enter a new value in the range 64521 to 65535, and click **APPLY**.
4 Click **ADD VPN** and give the new VPN a **Name**.

5 Select a **Local IP Address** from the drop-down menu.

   - If you have configured AWS Direct Connect for this SDDC and want the VPN to use it, select the private IP address. See [Create a Private Virtual Interface for SDDC Management and Compute Network Traffic](#). Note that VPN traffic over Direct Connect is limited to the default MTU of 1500 bytes even if the link supports a higher MTU.
   - Select a public IP address if you want the VPN to connect over the Internet.

6 For **Remote Public IP**, enter the address of your on-premises VPN endpoint. This is the address of the device that initiates or responds to IPsec requests for this VPN. This address must meet the following requirements:

   - It must not already be in use for another VPN. VMware Cloud on AWS uses the same public IP for all VPN connections, so only a single VPN connection (Route-based, Policy-based, or L2VPN) can be created to a given remote public IP.
   - It must be reachable over the Internet if you specified a public IP in **Step 5**.
   - It must be reachable over Direct Connect to a private VIF if you specified a private IP in **Step 5**.

Default gateway firewall rules allow inbound and outbound traffic over the VPN connection, but you must create firewall rules to manage traffic over the VPN tunnel.

7 For **BGP Local IP/Prefix Length**, enter the IP address, in CIDR format, of the local VPN tunnel.

   Choose a network of size of /30 from the 169.254.0.0/16 subnet. The second and third IP addresses in this range are configured as the remote and local VTI (VPN Tunnel interfaces). For example, in the CIDR block 169.254.111.0/30 (address range 169.254.111.0-169.254.111.3), the local (SDDC) interface is 169.254.111.2/30 and the remote (on-premises) interface 169.254.111.1/30.

   **Note** The following networks are reserved for internal use. The network you specify for **BGP Local IP/Prefix Length** must not overlap any of them.

   - 169.254.0.2/28
   - 169.254.10.1/24
   - 169.254.11.1/24
   - 169.254.12.1/24
   - 169.254.13.1/24
   - 169.254.101.253/30
   - 100.64.0.0/10 (Reserved for carrier-grade NAT per [RFC 6598](#).)

If you can't use a network from the 169.254.0.0/16 subnet (due to a conflict with an existing network), you must create a firewall rule that allows traffic from the BGP service to the subnet you choose here. See [Add or Modify Compute Gateway Firewall Rules](#).
8 For **BGP Remote IP**, enter the BGP interface address of your on-premises VPN gateway.

   This address must be a valid host IP on the subnet defined by the IP and Prefix Length you supplied in **Step 7**, and must not be the same as the **BGP Local IP**.

9 For **BGP Remote ASN**, enter the ASN of your on-premises VPN gateway.

10 Configure **Advanced Tunnel Parameters**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tunnel Encryption</strong></td>
<td>Select a Phase 2 security association (SA) cipher that is supported by your on-premises VPN gateway.</td>
</tr>
<tr>
<td><strong>Tunnel Digest Algorithm</strong></td>
<td>Select a Phase 2 digest algorithm that is supported by your on-premises VPN gateway.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you specify a GCM-based cipher for <strong>Tunnel Encryption</strong>, set <strong>Tunnel Digest Algorithm</strong> to <strong>None</strong>. The digest function is integral to the GCM cipher.</td>
</tr>
<tr>
<td><strong>Perfect Forward Secrecy</strong></td>
<td>Enable or Disable to match the setting of your on-premises VPN gateway. Enabling Perfect Forward Secrecy prevents recorded (past) sessions from being decrypted if the private key is ever compromised.</td>
</tr>
<tr>
<td><strong>Preshared Key</strong></td>
<td>Enter the preshared key string. The maximum key length is 128 characters. This key must be identical for both ends of the VPN tunnel.</td>
</tr>
<tr>
<td><strong>Remote Private IP</strong></td>
<td>Leave this blank to use the <strong>Remote Public IP</strong> as the remote ID for IKE negotiation. If your on-premises VPN gateway is behind a NAT device and/or uses a different IP for its local ID, you need to enter that IP here.</td>
</tr>
<tr>
<td><strong>IKE Encryption</strong></td>
<td>Select a Phase 1 (IKE) cipher that is supported by your on-premises VPN gateway.</td>
</tr>
<tr>
<td><strong>IKE Digest Algorithm</strong></td>
<td>Select a Phase 1 digest algorithm that is supported by your on-premises VPN gateway. The best practice is to use the same algorithm for both the <strong>IKE Digest Algorithm</strong> and the <strong>Tunnel Digest Algorithm</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you specify a GCM-based cipher for <strong>IKE Encryption</strong>, set <strong>IKE Digest Algorithm</strong> to <strong>None</strong>. The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher.</td>
</tr>
<tr>
<td><strong>IKE Type</strong></td>
<td>Specify <strong>IKE V1</strong> to initiate and accept the IKEv1 protocol.</td>
</tr>
<tr>
<td></td>
<td>Specify <strong>IKE V2</strong> to initiate and accept the IKEv2 protocol. You must use IKEv2 if you have specified a GCM-based <strong>IKE Digest Algorithm</strong>.</td>
</tr>
<tr>
<td></td>
<td>Specify <strong>IKE FLEX</strong> to accept either IKEv1 or IKEv2 and then initiate using IKEv2. If IKEv2 initiation fails, IKE FLEX will not fall back to IKEv1.</td>
</tr>
<tr>
<td><strong>Diffie Hellman</strong></td>
<td>Select a Diffie Hellman group that is supported by your on-premises VPN gateway. This value must be identical for both ends of the VPN tunnel. Higher group numbers offer better protection. The best practice is to select group 14 or higher.</td>
</tr>
</tbody>
</table>

11 (Optional) Under **Advanced BGP Parameters**, enter a BGP **Secret** that matches the one used by the on-premises gateway.

12 (Optional) Tag the VPN.

   See **Add Tags to an Object** for more information about tagging NSX-T objects.
13  Click **SAVE**.

**Results**

The VPN creation process might take a few minutes. When the route-based VPN becomes available, the tunnel status and BGP session state are displayed. The following actions are available to help you with troubleshooting and configuring the on-premises end of the VPN:

- Click **DOWNLOAD CONFIG** to download a file that contains VPN configuration details. You can use these details to configure the on-premises end of this VPN.
- Click **VIEW STATISTICS** to view packet traffic statistics for this VPN. See View VPN Tunnel Status and Statistics.
- Click **VIEW ROUTES** to open a display of routes advertised and learned by this VPN.
- Click **DOWNLOAD ROUTES** to download a list of **Advertised Routes** or **Learned Routes** in CSV format.

**What to do next**

Create or update firewall rules as needed. To allow traffic through the route-based VPN, specify **VPN Tunnel Interface** in the **Applied to** field. The **All Uplinks** option does not include the routed VPN tunnel.

**Create a Policy-Based VPN**

A policy-based VPN creates an IPsec tunnel and a policy that specifies how traffic uses it. When you use a policy-based VPN, you must update the routing tables on both ends of the network when new routes are added.

Policy-based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic. To create a policy-based VPN, you configure the local (SDDC) endpoint, then configure a matching remote (on-premises) endpoint. Because each policy-based VPN must create a new IPsec security association for each network, an administrator must update routing information on premises and in the SDDC whenever a new policy-based VPN is created. A policy-based VPN can be an appropriate choice when you have only a few networks on either end of the VPN, or if your on-premises network hardware does not support BGP (which is required for route-based VPNs).

**Procedure**

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2. Select **Networking & Security > VPN > Policy Based**.
3. Click **ADD VPN** and give the new VPN a **Name**.
4. Select a **Local IP Address** from the drop-down menu.
   - If you have configured AWS Direct Connect for this SDDC and want the VPN to use it, select the private IP address. See Create a Private Virtual Interface for SDDC Management and Compute Network Traffic. Note that VPN traffic over Direct Connect is limited to the default MTU of 1500 bytes even if the link supports a higher MTU.
Select a public IP address if you want the VPN to connect over the Internet.

5 Enter the **Remote Public IP** address of your on-premises gateway.

The address must not already be in use for another VPN. VMware Cloud on AWS uses the same public IP for all VPN connections, so only a single VPN connection (Route-based, Policy-based, or L2VPN) can be created to a given remote public IP. This address must be reachable over the Internet if you specified a public IP in **Step 4**. If you specified a private IP, it must be reachable over Direct Connect to a private VIF. Default gateway firewall rules allow inbound and outbound traffic over the VPN connection, but you must create firewall rules to manage traffic over the VPN tunnel.

6 (Optional) If your on-premises gateway is behind a NAT device, enter the gateway address as the **Remote Private IP**.

This IP address must match the local identity (IKE ID) sent by the on-premises VPN gateway. If this field is empty, the **Remote Public IP** field is used to match the local identity of the on-premises VPN gateway.

7 Specify the **Remote Networks** that this VPN can connect to.

This list must include all networks defined as local by the on-premises VPN gateway. Enter each network in CIDR format, separating multiple CIDR blocks with commas.

8 Specify the **Local Networks** that this VPN can connect to.

This list includes all routed compute networks in the SDDC, as well as the entire Management network and the appliance subnet (a subset of the Management network that includes vCenter and other management appliances, but not the ESXi hosts). It also includes the CGW DNS Network, a single IP address used to source requests forwarded by the CGW DNS service.

9 Configure **Advanced Tunnel Parameters**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tunnel Encryption</strong></td>
<td>Select a Phase 2 security association (SA) cipher that is supported by your on-premises VPN gateway.</td>
</tr>
<tr>
<td><strong>Tunnel Digest Algorithm</strong></td>
<td>Select a Phase 2 digest algorithm that is supported by your on-premises VPN gateway.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you specify a GCM-based cipher for <strong>Tunnel Encryption</strong>, set <strong>Tunnel Digest Algorithm</strong> to None. The digest function is integral to the GCM cipher.</td>
</tr>
<tr>
<td><strong>Perfect Forward Secrecy</strong></td>
<td>Enable or Disable to match the setting of your on-premises VPN gateway. Enabling Perfect Forward Secrecy prevents recorded (past) sessions from being decrypted if the private key is ever compromised.</td>
</tr>
<tr>
<td><strong>IKE Encryption</strong></td>
<td>Select a Phase 1 (IKE) cipher that is supported by your on-premises VPN gateway.</td>
</tr>
<tr>
<td><strong>IKE Digest Algorithm</strong></td>
<td>Select a Phase 1 digest algorithm that is supported by your on-premises VPN gateway. The best practice is to use the same algorithm for both the <strong>IKE Digest Algorithm</strong> and the <strong>Tunnel Digest Algorithm</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you specify a GCM-based cipher for <strong>IKE Encryption</strong>, set <strong>IKE Digest Algorithm</strong> to None. The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| IKE Type     | - Specify **IKE V1** to initiate and accept the IKEv1 protocol.  
- Specify **IKE V2** to initiate and accept the IKEv2 protocol. You must use IKEv2 if you have specified a GCM-based **IKE Digest Algorithm**.  
- Specify **IKE FLEX** to accept either IKEv1 or IKEv2 and then initiate using IKEv2. If IKEv2 initiation fails, IKE FLEX will not fall back to IKEv1. |
| Diffie Hellman | Select a Diffie Hellman group that is supported by your on-premises VPN gateway. This value must be identical for both ends of the VPN tunnel. Higher group numbers offer better protection. The best practice is to select group 14 or higher. |
| Preshared Key | Enter a preshared key used by both ends of the tunnel to authenticate with each other. The string has a maximum length of 128 characters.                                                                          |

10  (Optional) Tag the VPN.

See Add Tags to an Object for more information about tagging NSX-T objects.

11  Click **SAVE**.

**Results**

The VPN creation process might take a few minutes. When the policy-based VPN becomes available, the following actions are available to help you with troubleshooting and configuring the on-premises end of the VPN:

- Click **DOWNLOAD CONFIG** to download a file that contains VPN configuration details. You can use these details to configure the on-premises end of this VPN.
- Click **VIEW STATISTICS** to view packet traffic statistics for this VPN. See View VPN Tunnel Status and Statistics.

**What to do next**

Create or update firewall rules as needed. To allow traffic through the policy-based VPN, specify **Internet Interface** in the **Applied to** field.

**View VPN Tunnel Status and Statistics**

The VMC Console provides status and statistics for IPSec VPNs and L2VPN segments.

**Procedure**

1  Log in to the VMC Console at https://vmc.vmware.com.

2  Click **Networking & Security** > **VPN**.
Click ROUTE BASED VPN, POLICY BASED VPN, or LAYER 2 VPN to list VPNs of the selected type.

Take one of the following actions:

- Click the Information icon to display a status message that provides more information about channel (IKE Phase 1 negotiation) and tunnel status.
- Expand a VPN row to show VPN details, then click VIEW STATISTICS to display traffic statistics. You can retrieve aggregated status and statistics for all tunnels or for the tunnel used by the selected VPN (0.0.0.0/0). When viewing aggregated statistics, you can click View More in the Stats column to see a list of error statistics.
- Click the Refresh icon to refresh tunnel statistics. All VPN statistics are reset to 0 when the tunnel is disabled or re-enabled.

What to do next

For more information about troubleshooting VPN connection issues, see Troubleshooting Virtual Private Networks (VPN) in the NSX Data Center for vSphere documentation and also the NSX-T Data Center Troubleshooting Guide.

IPsec VPN Settings Reference

The on-premises end of any IPsec VPN must be configured to match the settings you specified for the SDDC end of that VPN.

Information in the following tables summarizes the available SDDC IPsec VPN settings. Some of the settings can be configured. Some are static. Use this information to verify that your on-premises VPN solution can be configured to match the one in your SDDC. Choose an on-premises VPN solution that supports all the static settings and any of the configurable settings listed in these tables.

Phase 1 Internet Key Exchange (IKE) Settings

Table 2-2. Configurable IKE Phase 1 Settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Allowed Values</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>IKEv1, IKEv2, IKE FLEX</td>
<td>IKEv2</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>AES (128, 256), AES-GCM (128, 192, 256)</td>
<td>AES GCM</td>
</tr>
<tr>
<td>Tunnel/IKE Digest Algorithm</td>
<td>SHA-1, SHA-2</td>
<td>SHA-2</td>
</tr>
<tr>
<td>Diffie Hellman</td>
<td>DH Groups 2, 5, 14-16</td>
<td>DH Group 14-16</td>
</tr>
</tbody>
</table>
Table 2-3. Static IKE Phase 1 Settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAKMP mode</td>
<td>Main mode (Disable aggressive mode)</td>
</tr>
<tr>
<td>ISAKMP/IKE SA lifetime</td>
<td>86400 seconds (24 hours)</td>
</tr>
<tr>
<td>IPsec Mode</td>
<td>Tunnel</td>
</tr>
<tr>
<td>IKE Authentication</td>
<td>Pre-Shared Key</td>
</tr>
</tbody>
</table>

Phase 2 IKE Settings

Table 2-4. Configurable IKE Phase 2 Settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Allowed Values</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Algorithm</td>
<td>AES-256, AES-GCM, AES</td>
<td>AES-GCM</td>
</tr>
<tr>
<td>Perfect forward secrecy (PFS)</td>
<td>Enabled, Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Diffie Hellman</td>
<td>DH Groups 2, 5, 14-16</td>
<td>DH Group 14-16</td>
</tr>
</tbody>
</table>

Table 2-5. Static IKE Phase 2 Settings

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing Algorithm</td>
<td>SHA-1</td>
</tr>
<tr>
<td>Tunnel Mode</td>
<td>Encapsulating Security Payload (ESP)</td>
</tr>
<tr>
<td>SA lifetime</td>
<td>3600 seconds (one hour)</td>
</tr>
</tbody>
</table>

On-Premises IPsec VPN Configuration

Click **DOWNLOAD CONFIG** on the status page of any VPN to download a file that contains VPN configuration details. You can use these details to configure the on-premises end of the VPN.

**Note** Do not configure the on-premises side of a VPN to have an idle timeout (for example, the NSX Session idle timeout setting). On-premises idle timeouts can cause the VPN to become periodically disconnected.

Sample configuration files for several popular endpoint devices are available on VMware {code}.

- Palo Alto Networks Firewall

Configure Management Gateway Networking and Security

The management network and Management Gateway are largely preconfigured in your SDDC, but you'll still need to configure access to management network services like vCenter and HCX and create
management gateway firewall rules to allow traffic between the management network and other networks, including your on-premises networks and other SDDC networks.

**Procedure**

1. **Set vCenter Server FQDN Resolution Address**
   You can connect to the SDDC vCenter Server at either a public or private IP address. A private IP address can be resolved from an SDDC VPN. A public IP address can be resolved from the Internet.

2. **Set HCX FQDN Resolution Address**
   You can connect to HCX at either a public or private IP address. A private IP address can be resolved from an SDDC VPN. A public IP address can be resolved from the internet.

3. **Add or Modify Management Gateway Firewall Rules**
   By default, the management gateway blocks traffic to all destinations from all sources. Add Management Gateway firewall rules to allow traffic as needed.

**Set vCenter Server FQDN Resolution Address**

You can connect to the SDDC vCenter Server at either a public or private IP address. A private IP address can be resolved from an SDDC VPN. A public IP address can be resolved from the Internet.

**Prerequisites**

Before you can access the SDDC vCenter Server at a private IP address, you'll need to set up a VPN connecting your SDDC to your on-premises datacenter. See [Create a Route-Based VPN](#) or [Create a Policy-Based VPN](#).

**Procedure**

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2. Navigate to the **Settings** tab of your SDDC.
3. Expand **vCenter FQDN**, and click **Edit**.
4. Under **Resolution Address** Select either the **Public IP** address or the **Private IP** address and click **SAVE**.

**Set HCX FQDN Resolution Address**

You can connect to HCX at either a public or private IP address. A private IP address can be resolved from an SDDC VPN. A public IP address can be resolved from the internet.

**Prerequisites**

Before you can access HCX at a private IP address, you'll need to set up a VPN connecting your SDDC to your on-premises datacenter. See [Create a Route-Based VPN](#) or [Create a Policy-Based VPN](#).

**Procedure**

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2 Navigate to the **Settings** tab of your SDDC.

3 Expand **HCX FQDN**, and click **Edit**.

4 Under **Resolution Address** select either the **Public IP** address or the **Private IP** address and click **SAVE**.

### Add or Modify Management Gateway Firewall Rules

By default, the management gateway blocks traffic to all destinations from all sources. Add Management Gateway firewall rules to allow traffic as needed.

Management Gateway firewall rules specify actions to take on network traffic from a specified source to a specified destination. Sources and destinations can be defined as **Any** or as members of a system-defined or user-defined inventory group. See **Add a Management Group** for information about viewing or modifying inventory groups.

**Procedure**

1 Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).

2 On the **Networking & Security** tab, click **Gateway Firewall**.

3 On the **Gateway Firewall** card, click **Management Gateway**, then click **ADD RULE** and give the new rule a **Name**.

4 Enter the parameters for the new rule.

Parameters are initialized to their default values (for example, **All** for **Sources** and **Destinations**). To edit a parameter, move the mouse cursor over the parameter value and click the pencil icon (✏️) to open a parameter-specific editor.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Sources**  | Select **Any** to allow traffic from any source address or address range. Select **System Defined Groups** and select one of the following source options:  
- ESXi to allow traffic from your SDDC's ESXi hosts.  
- NSX Manager to allow traffic from your SDDC's NSX-T manager appliance.  
- vCenter to allow traffic from your SDDC's vCenter Server.  
Select **User Defined Groups** to use a management group that you have defined. See **Add a Management Group**. |
| **Destinations** | Select **Any** to allow traffic to any destination address or address range. Select **System Defined Groups** and select one of the following destination options:  
- ESXi to allow traffic to your SDDC's ESXi management.  
- NSX Manager to allow traffic to your SDDC's NSX-T.  
- vCenter to allow traffic to your SDDC's vCenter Server. |
Option | Description
--- | ---
**Services** | Select the service types that the rule applies to. The list of service types depends on your choices for Sources and Destinations.

**Action** | The only action available for a new management gateway firewall rule is Allow.

The new rule is enabled by default. Slide the toggle to the left to disable it.

5 Click **PUBLISH** to create the rule.

Firewall rules are applied in order from top to bottom. Because there is a default Drop rule at the bottom and the rules above are always Allow rules, management gateway firewall rule order has no impact on traffic flow.

**Example: Create a Management Gateway Firewall Rule**

To create a management gateway firewall rule that enables vMotion traffic from the on-premises ESXi hosts to the ESXi hosts in the SDDC:

1. Create a management inventory group that contains the on-premises ESXi hosts that you want to enable for vMotion to the SDDC.
2. Create a management gateway rule with source ESXi and destination on-premises ESXi hosts.
3. Create another management gateway rule with source on-premises ESXi hosts group and destination ESXi with a vMotion service.

**What to do next**

You can take any or all of these optional actions with an existing firewall rule.

- Click the gear icon 🔄 to view or modify rule logging settings. Log entries are sent to the VMwarevRealize Log Insight Cloud Service. See Using vRealize Log Insight Cloud in the VMware Cloud on AWS Operations Guide.

- Click the graph icon 📈 to view statistics for the rule, including:
  - **Popularity Index** Number of times the rule was triggered in the past 24 hours.
  - **Hit Count** Number of times the rule was triggered since it was created.

Statistics start accumulating as soon as the rule is enabled.

**Example Management Gateway Firewall Rules**

Some common firewall rule configurations include opening access to the vSphere Client from the internet, allowing access to vCenter Server through the management VPN tunnel, and allowing remote console access.

**Commonly Used Firewall Rules**

The following table shows the Service, Source, and Destination settings for commonly-used firewall rules.
Table 2-6. Commonly-Used Firewall Rules

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>Service</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide access to vCenter Server from the internet. Use for general vSphere Client access as well as for monitoring vCenter Server</td>
<td>HTTPS</td>
<td>public IP address</td>
<td>vCenter</td>
</tr>
<tr>
<td>Provide access to vCenter Server over VPN tunnel. Required for Management Gateway VPN, Hybrid Linked Mode, Content Library.</td>
<td>HTTPS</td>
<td>IP address or CIDR block from on-premises data center</td>
<td>vCenter</td>
</tr>
<tr>
<td>Provide access from cloud vCenter Server to on-premises services such as Active Directory, Platform Services Controller, and Content Library.</td>
<td>Any</td>
<td>vCenter</td>
<td>IP address or CIDR block from on-premises data center.</td>
</tr>
<tr>
<td>Provisioning operations involving network file copy traffic, such as cold migration, cloning from on-premises VMs, snapshot migration, replication, and so on.</td>
<td>Provisioning</td>
<td>IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel</td>
<td>ESXi Management</td>
</tr>
<tr>
<td>VMRC remote console access Required for vRealize Automation</td>
<td>Remote Console</td>
<td>IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel</td>
<td>ESXi Management</td>
</tr>
<tr>
<td>vMotion traffic over VPN</td>
<td>Any</td>
<td>ESXi Management</td>
<td>IP address or CIDR block from on-premises data center</td>
</tr>
</tbody>
</table>

Configure Compute Gateway Networking and Security

Compute Gateway networking includes a compute network with one or more segments and the DNS, DHCP, and security (gateway firewall and distributed firewall) configurations that manage network traffic for workload VMs. It can also include a layer 2 VPN and extended network that provides a single broadcast domain that spans your on-premises network and your SDDC workload network.

Procedure

1. Create or Modify a Network Segment
   Network segments are logical networks for use by workload VMs in the SDDC compute network.

2. Configure a Layer 2 VPN and Extended Network Segment
   You can use a VMware Cloud on AWS layer 2 Virtual Private Network (L2VPN) to extend your on-premises network to one or more VLAN-based networks in your SDDC. This extended network is a single subnet with a single broadcast domain. You can use it to migrate VMs to and from your cloud SDDC without having to change their IP addresses.
Add or Modify Compute Gateway Firewall Rules
By default, the Compute Gateway blocks traffic to all uplinks. Add Compute Gateway firewall rules to allow traffic as needed.

Add or Modify Distributed Firewall Rules
Distributed firewall rules apply at the VM level and control East-West traffic within the SDDC.

Configure DNS Services
VMware Cloud on AWS DNS forwarding services run in DNS zones, and enable VMs to resolve fully-qualified domain names to IP addresses by forwarding their queries to a DNS server.

Configure Compute Gateway DHCP Relay
In the default configuration a local server handles DHCP requests for workload VMs on all routed segments. If you have an external DHCP server that manages IP addresses on your workload networks, you can configure the Compute Gateway to forward DHCP requests to that server.

Create or Modify a Network Segment
Network segments are logical networks for use by workload VMs in the SDDC compute network.
VMware Cloud on AWS supports three types of logical network segments: routed, extended and disconnected.

- A routed network segment (the default type) has connectivity to other logical networks in the SDDC and, through the SDDC firewall, to external networks.
- An extended network segment extends an existing L2VPN tunnel, providing a single IP address space that spans the SDDC and an on-premises network.
- A disconnected network segment has no uplink, and provides an isolated network accessible only to VMs connected to it. Disconnected segments are created when needed by HCX (see Getting started with VMware HCX). You can also create them yourself, and can convert them to other segment types.

See Configuration Maximums for VMware Cloud on AWS for limits on segments per SDDC and network connections per segment.

A Single Host Starter SDDC is created with a single routed network segment named sddc-cgw-network-1. This network uses CIDR block 192.168.1.0/24, unless that conflicts with the CIDR block you chose for the SDDC management network. Multi-host SDDCs are created without a default network segment, so you must create at least one for your workload VMs.

Procedure

2. Click Networking & Security > Segments.

   To modify the configuration of an existing segment, click the ellipsis button and select Edit. To create a new segment, click ADD SEGMENT and give the new segment a Name.
3 Specify a segment **Type** and fill in the required configuration parameters.

Parameter requirements depend on the segment type

### Table 2-7. Routed Segment Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Tunnel ID</td>
<td>N/A for Routed or Disconnected segment types.</td>
</tr>
<tr>
<td>Gateway IP/Prefix Length</td>
<td>Specify a CIDR block for the segment. The block must not overlap your management network or any of the subnets in your connected Amazon VPC.</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>Disabled by default. Select <strong>Enabled</strong> to enable native NSX DHCP services for VMs on this segment. Specify a DHCP IP address range and a DNS suffix for the segment. VMs connecting to the segment get their IP addresses from the specified DHCP server and their FQDN has the specified DNS suffix.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you enable native NSX DHCP services on a compute network segment you cannot enable DHCP relay for the Compute Gateway. See Configure Compute Gateway DHCP Relay.</td>
</tr>
<tr>
<td>DHCP IP Range</td>
<td>If DHCP is <strong>Enabled</strong>, specify a DHCP IP address range for VMs attached to the segment.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>If DHCP is <strong>Enabled</strong>, specify an FQDN to be assigned to VMs attached to the segment.</td>
</tr>
</tbody>
</table>

### Table 2-8. Extended Segment Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Tunnel ID</td>
<td>Specify the tunnel ID of an existing L2VPN tunnel. N/A for Routed or Disconnected segment types. If you have not already created an L2VPN, see Configure a Layer 2 VPN Tunnel in the SDDC.</td>
</tr>
<tr>
<td>Gateway IP/Prefix Length</td>
<td>N/A for Extended segments.</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>N/A for Extended segments.</td>
</tr>
<tr>
<td><strong>DHCP IP Range</strong></td>
<td>N/A for Extended segments.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>N/A for Extended segments.</td>
</tr>
</tbody>
</table>

### Table 2-9. Disconnected Segment Configuration Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Tunnel ID</td>
<td>N/A for Routed or Disconnected segment types.</td>
</tr>
<tr>
<td>Gateway IP/Prefix Length</td>
<td>Specify a CIDR block for the segment. The block must not overlap your management network or any of the subnets in your connected Amazon VPC.</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>N/A for Disconnected segments.</td>
</tr>
<tr>
<td><strong>DHCP IP Range</strong></td>
<td>N/A for Disconnected segments.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>N/A for Disconnected segments.</td>
</tr>
</tbody>
</table>
4. Click **SAVE** to create or update the segment.

   The system creates the requested segment. This operation can take up to 15 seconds to complete. When the segment **Status** transitions to **Up**, the segment is ready for use. If the segment **Status** is **Down**, you can click the information icon 🔄 for more information about the cause of the problem.

---

**Configure a Layer 2 VPN and Extended Network Segment**

You can use a VMware Cloud on AWS layer 2 Virtual Private Network (L2VPN) to extend your on-premises network to one or more VLAN-based networks in your SDDC. This extended network is a single subnet with a single broadcast domain. You can use it to migrate VMs to and from your cloud SDDC without having to change their IP addresses.

In addition to data center migration, you can use an extended L2VPN network for disaster recovery, or for dynamic access to cloud computing resources as needed (often referred to as "cloud bursting").

An L2VPN can extend up to 100 of your on-premises networks. VMware Cloud on AWS uses NSX-T to provide the L2VPN server in your cloud SDDC. L2VPN client functions can be provided by a standalone NSX Edge that you download and deploy into your on-premises data center.

The VMware Cloud on AWS L2VPN feature supports extending VLAN networks. The L2VPN connection to the NSX-T server uses an IPsec tunnel. The L2VPN extended network is used to extend Virtual Machine networks and carries only workload traffic. It is independent of the VMkernel networks used for migration traffic (ESXi management or vMotion), which use either a separate IPsec VPN or a Direct Connect connection.

**Important** You cannot bring up an L2VPN tunnel until you have configured the L2VPN client and server and created an extended network that specifies the tunnel ID you assigned to the client.

---

**Procedure**

1. **Configure a Layer 2 VPN Tunnel in the SDDC**
   
   Specify a local (AWS) IP address, a remote (on-premises) public IP address, and a remote private IP address to create the SDDC end of the Layer 2 VPN tunnel.

2. **Configure an Extended Segment for the Layer 2 VPN**
   
   Extended networks require a layer 2 Virtual Private Network (L2VPN), which provides a secure communications tunnel between an on-premises network and one in your cloud SDDC.

3. **Download and Configure the Autonomous NSX Edge**
   
   The on-premises end of your L2VPN requires a specially configured standalone NSX Edge appliance called the Autonomous Edge. You must download, install, and configure this appliance and related on-premises vSphere networking before you can create an L2VPN.

---

**Configure a Layer 2 VPN Tunnel in the SDDC**

Specify a local (AWS) IP address, a remote (on-premises) public IP address, and a remote private IP address to create the SDDC end of the Layer 2 VPN tunnel.
VMware Cloud on AWS supports a single Layer 2 VPN tunnel between your on-premises installation and your SDDC.

**Procedure**

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
3. Click ADD VPN TUNNEL.
4. Configure the VPN parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local IP Address</td>
<td>Select the private IP address if you have configured AWS Direct Connect for this SDDC and want the VPN to use it. See <a href="https://vmc.vmware.com">Create a Private Virtual Interface for SDDC Management and Compute Network Traffic</a> or select the public IP address if you want the VPN to connect to the SDDC over Internet.</td>
</tr>
<tr>
<td>Remote Public IP</td>
<td>Enter the remote public IP address of your on-premise L2VPN gateway. For an L2VPN, this is always the standalone NSX Edge appliance (see <a href="https://vmc.vmware.com">Download and Configure the Autonomous NSX Edge</a>).</td>
</tr>
<tr>
<td>Remote Private IP</td>
<td>Enter the remote private IP address if the on-premise gateway is configured behind NAT.</td>
</tr>
</tbody>
</table>

5. (Optional) Tag the VPN.

   See [Add Tags to an Object](https://vmc.vmware.com) for more information about tagging NSX-T objects.

6. (Optional) Add a **Description**.

7. Click **SAVE**.

Depending on your SDDC environment, the Layer 2 VPN creation process might take a few minutes. When the Layer 2 VPN tunnel becomes available, the status changes to Up.

**Configure an Extended Segment for the Layer 2 VPN**

Extended networks require a layer 2 Virtual Private Network (L2VPN), which provides a secure communications tunnel between an on-premises network and one in your cloud SDDC.

Each end of this tunnel has an ID. When the tunnel ID matches on the cloud SDDC and the on-premises side of the tunnel, the two networks become part of the same broadcast domain. Extended networks use an on-premises gateway as the default gateway. Other network services such as DHCP and DNS are also provided on-premises.

You can change a logical network from routed to extended or from extended to routed. For example, you might configure a logical network as extended to allow migration of VMs from your on-premises data center to your cloud SDDC. When the migration is complete, you might then change the network to routed to allow the VMs to use VMware Cloud on AWS networking services.
Prerequisites

Verify that Layer 2 VPN tunnel is available. See Configure a Layer 2 VPN Tunnel in the SDDC.

Procedure

2. Follow the procedure in Create or Modify a Network Segment to create an Extended segment bound to the Tunnel ID of the L2VPN tunnel.
3. Click SAVE.
4. Click DOWNLOAD CONFIG to download a file containing the peer code and other information you'll need when configuring the on-premises of the remote side VPN configuration.
5. Click REMOTE STANDALONE EDGE DOWNLOAD to download an NSX Standalone Edge image in OVF format that you must install and configure as the client side of the L2VPN. See Download and Configure the Autonomous NSX Edge.

Download and Configure the Autonomous NSX Edge

The on-premises end of your L2VPN requires a specially configured standalone NSX Edge appliance called the Autonomous Edge. You must download, install, and configure this appliance and related on-premises vSphere networking before you can create an L2VPN.

Before you can create an L2VPN, you must download and configure a standalone NSX Edge appliance. See Configure Layer 2 VPN Extended Segment. You cannot use your on-premises NSX-T Edge as the client side of an L2VPN that connects to your SDDC.

Procedure

1. Download the standalone NSX Edge.
   On the L2VPN page, click AUTONOMOUS EDGE DOWNLOAD to download the autonomous standalone NSX-T Edge as an OVF file.
2. See Add an Autonomous Edge as an L2 VPN Client in the NSX-T Data Center Administration Guide for information about how to install and configure the Autonomous Edge in your on-premises vCenter Server.

Add or Modify Compute Gateway Firewall Rules

By default, the Compute Gateway blocks traffic to all uplinks. Add Compute Gateway firewall rules to allow traffic as needed.

Compute Gateway firewall rules specify actions to take on network traffic from a specified source to a specified destination. Actions can be either allow (allow the traffic) or drop (drop all packets matching the specified source and destination). Sources and destinations can be chosen from a list of a physical network interfaces, or a generic specification of All Uplinks that refers to all traffic leaving the gateway and going to the VPC interface, Internet Interface, or Direct Connect interface. A firewall rule applied to All Uplinks does not apply to the VPN Tunnel Interface (VTI), which is a virtual interface and not a physical uplink. The VPN Tunnel Interface must be specified explicitly in the Applied To parameter of
any firewall rule that manages workload VM communications over a route-based VPN. The Compute Gateway includes a Default VTI Rule that drops all traffic to the VTI. To enable workload VMs to communicate over the VTI, modify this rule or move it to a lower rank in the rule hierarchy, after more permissive rules.

All traffic attempting to pass through the firewall is subjected to the rules in the order shown in the rules table, beginning at the top. A packet allowed by the first rule is passed on to the second rule, and so on through subsequent rules until the packet is dropped, rejected, or hits the default rule, which allows all traffic.

**Prerequisites**

Compute Gateway firewall rules require named inventory groups for Source and Destination values. See Add or Modify a Compute Group.

**Procedure**

3. On the GATEWAY FIREWALL page, click Compute Gateway.
4. To add a rule, click ADD RULE and give the new rule a Name.
5. Enter the parameters for the new rule.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources</td>
<td>Click Any in the Sources column and select an inventory group for source network traffic, or click ADD GROUP to create a new user-defined inventory group to use for this rule. Click SAVE.</td>
</tr>
<tr>
<td>Destinations</td>
<td>Click Any in the Destinations column and select an inventory group for destination network traffic, or click CREATE NEW GROUP to create a new user-defined inventory group to use for this rule. Click SAVE.</td>
</tr>
<tr>
<td>Services</td>
<td>Click Any in the Services column and select a service from the list. Click SAVE.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Applied To</td>
<td>Define the type of traffic that the rule applies to:</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>VPN Tunnel Interface</strong> if you want the rule to apply to traffic</td>
</tr>
<tr>
<td></td>
<td>over the route-based VPN.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>VPC Interface</strong> if you want the rule to apply to traffic over the</td>
</tr>
<tr>
<td></td>
<td>linked AWS VPC connection.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Internet Interface</strong> if you want the rule to apply to traffic</td>
</tr>
<tr>
<td></td>
<td>over the Internet, including over policy-based VPNs using Public IP.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Direct Connect Interface</strong> if you want the rule to allow traffic</td>
</tr>
<tr>
<td></td>
<td>over AWS Direct Connect (private VIF), including over policy-based VPNs</td>
</tr>
<tr>
<td></td>
<td>using Private IP.</td>
</tr>
<tr>
<td></td>
<td>- <strong>All Uplinks</strong> if you want the rule to apply to the <strong>VPC Interface</strong>,</td>
</tr>
<tr>
<td></td>
<td><strong>Internet Interface</strong>, and the <strong>Direct Connect Interface</strong>, but not to</td>
</tr>
<tr>
<td></td>
<td>the <strong>VPN Tunnel Interface</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The <strong>VPN Tunnel Interface</strong> is not classified as an uplink.</td>
</tr>
<tr>
<td>Action</td>
<td>Select <strong>Allow</strong> to allow all L2 and L3 traffic to pass through the firewall.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Drop</strong> to drop packets that match any specified <strong>Sources</strong>,</td>
</tr>
<tr>
<td></td>
<td><strong>Destinations</strong>, and <strong>Services</strong>. This is a silent action with no</td>
</tr>
<tr>
<td></td>
<td>notification to the source or destination systems. Dropping the packet</td>
</tr>
<tr>
<td></td>
<td>causes the connection to be retried until the retry threshold is reached.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Reject</strong> to reject packets that match any specified <strong>Sources</strong>,</td>
</tr>
<tr>
<td></td>
<td><strong>Destinations</strong>, and <strong>Services</strong>. This action returns a &quot;destination</td>
</tr>
<tr>
<td></td>
<td>unreachable message&quot; to the sender. For TCP packets, the response includes</td>
</tr>
<tr>
<td></td>
<td>a TCP RST message. For UDP, ICMP and other protocols, the response</td>
</tr>
<tr>
<td></td>
<td>includes an &quot;administratively prohibited&quot; code (9 or 10). The sender is</td>
</tr>
<tr>
<td></td>
<td>notified immediately (without any re-tries) when connection cannot be</td>
</tr>
<tr>
<td></td>
<td>established.</td>
</tr>
</tbody>
</table>

The new rule is enabled by default. Slide the toggle to the left to disable it.

6 Click **PUBLISH** to create the rule.

**What to do next**

You can take any or all of these optional actions with an existing firewall rule.

- Click the gear icon 🔄 to view or modify rule logging settings. Log entries are sent to the VMware vRealize Log Insight Cloud Service. See **Using vRealize Log Insight Cloud** in the **VMware Cloud on AWS Operations Guide**.

- Click the graph icon 🎨 to view statistics for the rule, including:
  - **Popularity Index** Number of times the rule was triggered in the past 24 hours.
  - **Hit Count** Number of times the rule was triggered since it was created.

  Statistics start accumulating as soon as the rule is enabled.

- Reorder firewall rules.
A rule created from the **ADD NEW RULE** button is placed at the top of the list of rules. Firewall rules are applied in order from top to bottom. To change the position of a rule in the list, select it and drag it to a new position. Click **PUBLISH** to publish the change.

### Add or Modify Distributed Firewall Rules

Distributed firewall rules apply at the VM level and control East-West traffic within the SDDC.

All traffic attempting to pass through the distributed firewall is subjected to the rules in the order shown in the rules table, beginning at the top. A packet allowed by the first rule is passed on to the second rule, and so on through subsequent rules until the packet is dropped, rejected, or hits the default rule, which allows all traffic.

Distributed firewall rules are grouped into policies. Policies are organized by category. Each category has an evaluation precedence. Rules in a category that has a higher precedence are evaluated before rules in category that has a lower precedence.

#### Table 2-10. Distributed Firewall Rule Categories

<table>
<thead>
<tr>
<th>Precedence</th>
<th>Category Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ethernet</td>
<td>Applied to all level 2 SDDC network traffic</td>
</tr>
<tr>
<td>2</td>
<td>Emergency</td>
<td>Used for quarantine and allow rules</td>
</tr>
<tr>
<td>3</td>
<td>Infrastructure</td>
<td>Define access to shared services. Global rules, AD, DNS, NTP, DHCP, backup, management servers.</td>
</tr>
<tr>
<td>4</td>
<td>Environment</td>
<td>Rules between security zones such as production zones, development zones, or zones dedicated to specific business purposes.</td>
</tr>
<tr>
<td>5</td>
<td>Application</td>
<td>Rules between applications, application tiers, or microservices</td>
</tr>
</tbody>
</table>

See **Security Terminology** in the *NSX-T Data Center Administration Guide* for more information about Distributed Firewall terminology.

### Prerequisites

Distributed firewall rules require inventory groups as sources and destinations and must be applied to a service, which can be a predefined service or a custom service that you define for your SDDC. You can create these groups and services while you are creating a rule, but it can speed up the process if you take care of some of this beforehand. See **Add or Modify a Compute Group** and **Add a Custom Service**.

### Procedure

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2. Select **Networking & Security > Distributed Firewall**.

   Click **CATEGORY SPECIFIC RULES** and select a category to view and modify policies and rules in that category, or click **ALL RULES** to view (but not modify) rules in all policies and categories.
3 (Optional) Change the default connectivity strategy.

By default, the Distributed Firewall includes an implicit Allow rule for all traffic. This rule, which does not appear in any list of rules, is evaluated after all other rules, and allows traffic that doesn't match a preceding rule to pass through the firewall. Click the connectivity strategy icon ( ) to see a list of available strategies. To change the current strategy, select a different one and click SAVE. See Select a Default Connectivity Strategy in the NSX-T Data Center Administration Guide for more information about available connectivity strategies.

4 To add a policy at the top of the list, click ADD POLICY and give the new policy a Name.

To add a policy before or after an existing policy, click the vertical ellipsis button at the beginning of the policy row to open the policy settings menu, then click Add Policy Above or Add Policy Below. By default a new policy applies to the distributed firewall (DFW), but you can specify one or more inventory groups for it to apply to instead. The policy's APPLIED TO value is propagated to all the rules in the policy.

5 To add a rule, select a policy, click ADD NEW RULE, and give the rule a Name.

6 Enter the parameters for the new rule.

Parameters are initialized to their default values (for example, All for Sources and Destinations). To edit a parameter, move the mouse cursor over the parameter value and click the pencil icon ( ) to open a parameter-specific editor.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources</td>
<td>Click Any in the Sources column and select an inventory group for source network traffic, or click ADD GROUP to create a new user-defined inventory group to use for this rule. Click SAVE.</td>
</tr>
<tr>
<td>Destinations</td>
<td>Click Any in the Destinations column and select an inventory group for destination network traffic, or click CREATE NEW GROUP to create a new user-defined inventory group to use for this rule. Click SAVE.</td>
</tr>
<tr>
<td>Services</td>
<td>Click Any in the Services column and select a service from the list. Click SAVE.</td>
</tr>
<tr>
<td>Applied To</td>
<td>The rule inherits its APPLIED TO value from the containing policy.</td>
</tr>
</tbody>
</table>
| Action      | Select Allow to allow all L2 and L3 traffic to pass through the firewall.  
Select Drop to drop packets that match any specified Sources, Destinations, and Services. This is a silent action with no notification to the source or destination systems. Dropping the packet causes the connection to be retried until the retry threshold is reached.  
Select Reject to reject packets that match any specified Sources, Destinations, and Services. This action returns a "destination unreachable message" to the sender. For TCP packets, the response includes a TCP RST message. For UDP, ICMP and other protocols, the response includes an "administratively prohibited" code (9 or 10). The sender is notified immediately (without any re-tries) when connection cannot be established. |

The new rule is enabled by default. Slide the toggle to the left to disable it.
7 (Optional) Configure advanced settings.

To change the directionality or logging behavior of the rule, click the gear icon to open the Settings page.

**Direction**
By default, this value is **In/Out**, forcing the rule to apply to traffic to and from the destination object. You can also choose **In** to specify that only traffic to the object is checked, or **Out** to specify that only traffic from the object is checked. Note that changing this value can cause asymmetric routing and other traffic anomalies, so be sure you understand the likely outcome for all sources and destinations before you make the change.

**Logging**
Logging for a new rule is disabled by default. Slide the toggle to the right to enable logging of rule actions.

8 Click **PUBLISH** to create the rule.

**What to do next**
You can take any or all of these optional actions with an existing firewall rule.

- Click the gear icon to view or modify rule logging settings. Log entries are sent to the VMware vRealize Log Insight Cloud Service. See Using vRealize Log Insight Cloud in the *VMware Cloud on AWS Operations Guide*.

- Click the graph icon to view statistics for the rule, including:
  - **Popularity Index** Number of times the rule was triggered in the past 24 hours.
  - **Hit Count** Number of times the rule was triggered since it was created.

Statistics start accumulating as soon as the rule is enabled.

- Reorder firewall rules.

  A rule created from the **ADD NEW RULE** button is placed at the top of the list of rules in the policy. Firewall rules in each policy are applied in order from top to bottom. To change the position of a rule in the list, select it and drag it to a new position. Click **PUBLISH** to publish the change.

**Manage Distributed Firewall Rules**
Traffic attempting to pass through the firewall is subjected to the rules in the order shown in the **ALL RULES**.

The order of distributed firewall rules in the **ALL RULES** list is the union of the ordered list of policies and the ordered list of rules in each policy. You can reorder the distributed firewall sections and rules within a section. You can also edit existing distributed firewall configuration, delete, or clone a firewall rule or section.
Procedure

1 Log in to the VMC Console at https://vmc.vmware.com.

2 Select Networking & Security > Distributed Firewall.

3 (Optional) Modify policy settings.

   Click the vertical ellipsis button at the beginning of the policy row to take bulk actions, which affect all rules in the policy.

4 (Optional) Reorder policies.

   A policy created from the ADD POLICY button is placed at the top of the list of policies. Firewall rules in each policy are applied in policy order from top to bottom. To change the position of a policy (and all the rules it contains) in the list, select it and drag it to a new position. Click PUBLISH to publish the change.

5 (Optional) Clone or copy a rule.

   Click the vertical ellipsis button at the beginning of the rule row.

   - **Clone Rule** to make a copy of the rule in this policy.
   - **Copy Rule** to make a copy of the rule that you can add to another policy.

6 (Optional) Add or delete a rule.

   Click the vertical ellipsis button at the beginning of the rule row.

   - **Add Rule** to add a rule in this policy.
   - **Delete Rule** to delete the rule from this policy.

7 (Optional) Save or View configurations.

   Distributed firewall configurations are similar to Firewall Drafts feature of on-premises NSX-T. Click ACTIONS > Configurations > View to view a list of saved configurations. Click ACTIONS > Configurations > Save to save the current configuration. Configurations are auto-saved by default. Click ACTIONS > Settings > General Settings to disable Auto Save Drafts.

Manage the Distributed Firewall Exclusion List

The Distributed Firewall Exclusion List lets you specify inventory groups to exclude from distributed firewall coverage. East-West network traffic to and from members of excluded groups is exempt from distributed firewall rules that would otherwise apply.

The Distributed Firewall exclusion list lets you keep specific inventory groups from being considered by distributed firewall rules. By default, management VMs and appliances, such as vCenter, NSX manager, and NSX controllers are on the exclusion list. You can edit the list to add or remove entries.

Procedure

1 Log in to the VMC Console at https://vmc.vmware.com.

2 Select Networking & Security > Distributed Firewall.
3. Click **ACTIONS > Settings > Exclusion List** to display the **Manage Exclusion List** page.

- To add an existing group to the exclusion list, click **ADD GROUP** and select an existing **Group Name**.
- To create a group from the **Manage Exclusion List**, type a name for the group in the **Group Name** field, then click **Set Members** to open the inventory group creation page. See **Add or Modify a Compute Group** for more information about using this page.
- To remove a group from the list, click the vertical ellipsis button at the beginning of the group row and click **Delete**.

4. Click **APPLY** to save your changes.

### Configure DNS Services

VMware Cloud on AWS DNS forwarding services run in DNS zones, and enable VMs to resolve fully-qualified domain names to IP addresses by forwarding their queries to a DNS server.

Your SDDC includes default DNS zones for the Management Gateway and Compute Gateway. Each zone includes a preconfigured DNS forwarding service. Use the **DNS Services** tab on the **DNS Services** page to disable, enable, or update some properties of DNS forwarding services for the default zones. To create additional DNS zones or configure additional properties of DNS forwarders in any zone, use the **DNS Zones** tab.

For more information about DNS configuration choices for VMware Cloud on AWS, see **DNS Strategies for VMware Cloud on AWS**.

**Procedure**

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2. Select **Networking & Security > DNS**.
3. Click **DNS Services** to open the **DNS Services** tab.
4. View or edit DNS service parameters.

Most Management Gateway DNS Forwarder parameters are read-only but you can click the vertical ellipses button and choose **Edit DNS Server IPs** to add or modify the DNS Server IP addresses for this service. You can view and edit most Compute Gateway DNS Forwarder parameters. Click the vertical ellipses button and click **Edit**. You can also modify DNS Service parameters of any additional DNS zones that you create.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of this DNS service. Cannot be modified for the Management and</td>
</tr>
<tr>
<td></td>
<td>Compute Gateway DNS Forwarder.</td>
</tr>
<tr>
<td>DNS Service IP</td>
<td>The IP address of this DNS service. Read-only in this view.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default DNS Zone</td>
<td>You can add or modify DNS server IP addresses for the default DNS zone for the Management Gateway and Compute Gateway DNS Forwarders. DNS queries from VMs in the default zone are forwarded to these IP addresses by default if they don't match the criteria for an FQDN zones.</td>
</tr>
<tr>
<td>FQDN Zones</td>
<td>Optional. For the Compute Gateway DNS Forwarder, specify one or more FQDNs to enable DNS forwarding. A DNS forwarder is associated with a default DNS zone and up to 5 FQDN DNS zones. When a DNS query is received from a VM in the zone, the DNS forwarder compares the domain name in the query with the domain names in the FQDN DNS zones. If a match is found, the query is forwarded to the DNS servers specified in the FQDN DNS zone. Otherwise the query is forwarded to the DNS servers specified in the default DNS zone.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Read-only for the Management Gateway DNS Forwarder and Compute Gateway DNS Forwarder.</td>
</tr>
<tr>
<td>Tags</td>
<td>See Add Tags to an Object for more information about tagging NSX-T objects.</td>
</tr>
</tbody>
</table>

5  Click SAVE.

**Add a DNS Zone**

Each DNS zone in your SDDC network represents a piece of the DNS namespace that you manage yourself.

DNS zones in the SDDC fall into two categories:

- Default zones, where the servers listen for DNS queries from all SDDC VMs on a subnet in the zone.
- FQDN zones, where the servers listen for DNS requests forwarded from a default zone.

The compute and management gateways are each configured with a single default DNS zone. You can add up to four more zones of either type to provide the flexibility of having multiple DNS servers and subdomains. See Add a DNS Zone in the *NSX-T Data Center Administration Guide* for more information about how NSX-T implements DNS zones.

**Procedure**

1  Log in to the VMC Console at https://vmc.vmware.com.

2  Click Networking & Security > DNS and open the DNS Zones tab.

3  To add a default zone, select ADD DNS ZONE > Add Default Zone

   a  Enter a name and optionally a description. You use this Name if you create DNS firewall rules that apply to traffic in this zone.

   b  Enter the IP addresses of up to three DNS servers. All of the DNS servers you specify must be configured identically.

   c  (Optional) Enter an IP address in the Source IP field.
To add an FQDN zone, select **ADD DNS ZONE > Add FQDN Zone**

- a. Enter a name and optionally a description. You use this **Name** if you create DNS firewall rules that apply to traffic in this zone.
- b. Enter a FQDN for the domain. This must be a fully qualified domain name, such as example.com.
- c. Enter the IP address of up to three DNS servers.
- d. (Optional) Enter an IP address in the **Source IP** field.

(Optional) Tag the DNS zone.

See [Add Tags to an Object](#) for more information about tagging NSX-T objects.

Click **SAVE**.

### Configure Compute Gateway DHCP Relay

In the default configuration a local server handles DHCP requests for workload VMs on all routed segments. If you have an external DHCP server that manages IP addresses on your workload networks, you can configure the Compute Gateway to forward DHCP requests to that server.

Organizations that want to use an existing IP Address Management (IPAM) solution for workload VMs in their SDDC can use the NSX-T DHCP relay feature to specify the server and attach it to the Compute Gateway.

**Note** You cannot configure DHCP Relay if the Compute Gateway includes any segments that provide their own DHCP services.

**Procedure**

2. Select **Networking & Security > DHCP**.
3. Click **CONFIGURE DHCP RELAY**.

   Fill in the name and IP address of your DHCP server, then click **Attach** to attach the server to the Compute Gateway. If you specify an on-premises DHCP server, be sure that your on-premises firewall allows DHCP traffic (ports 67 and 68) to reach its address.

4. Enable DHCP on all segments that should forward requests to the relay.

   See [Create or Modify a Network Segment](#). You must enter a **DHCP IP Range**. The range is currently ignored, so you can specify any convenient value that falls within the IP range of the subnet. Note that before you can disable DHCP relay, you must disable it on all segments.

### Working With Inventory Groups

Use VMware Cloud on AWS Networking & Security inventory to create groups of VMs and network services that you can use when you create firewall rules.
Firewall rules typically apply to a group of VMs that have certain common characteristics including:

- names that follow a naming convention (like Win* for Windows VMs or Photon* for Photon VMs)
- IP addresses within a specific range or CIDR block
- tags

They can also apply to network services, which are distinguished by characteristics like service type and network protocol. The VMware Cloud on AWS Networking & Security Inventory feature simplifies the process of creating groups of VMs that have similar needs for firewall protection. It also allows you to add new network services to the built-in list of services, so that you can include those services in firewall rules.

VMware Cloud on AWS creates management groups and a service inventory in all new SDDCs. It also maintains a list of your workload VMs and their tags. You can add or modify your own inventory groups of management or compute VMs.

### Add a Management Group

Management inventory groups contain SDDC infrastructure components. Use these groups in management gateway firewall rules.

Pre-defined management inventory groups are created automatically for SDDC infrastructure components such as vCenter and NSX Manager. You cannot modify a pre-defined management group, but you can create additional management inventory groups by specifying the CIDR blocks to which group members are connected.

#### Procedure

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2. On the Networking & Security tab, click Inventory > Groups.
3. On the Groups card, click MANAGEMENT GROUPS, then click ADD GROUP and give the group a Name and an optional Description.
4. Click Set Members to open the Select Members page.
   - Enter one or more IP addresses of management VMs in CIDR format.
5. (Optional) Tag the group.
   - See Add Tags to an Object for more information about tagging NSX-T objects.
6. Click SAVE to create the group.

#### What to do next

You can modify or delete any management group that you created by clicking the vertical ellipse button and selecting Edit or Delete.

### Add or Modify a Compute Group

Compute inventory groups categorize compute VMs using criteria such as names, IP addresses, and tags.
Because compute inventory groups are made up of the compute VMs you deploy on your compute network segments. VMware Cloud on AWS cannot create them for you. You'll need to create them yourself before you can develop compute gateway firewall rules.

**Procedure**


2. On the Networking & Security tab, click Inventory > Groups.

3. On the Groups card, click COMPUTE GROUPS, then click ADD GROUP and give the group a Name and an optional Description.

   To modify an existing group, select it and click the ellipsis button at the beginning of the group row.

4. Click Set Members to open the Select Members page.

   Management groups contain VMs on the Management Network. Management group members must be specified by IP address. Compute groups contain VMs or network objects such as segments the Compute network. There are several ways to designate membership in a compute group.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Membership Criteria</td>
<td>Click ADD CRITERIA and use the drop-down controls to specify one or more criteria in the form of <strong>Object Type, Property, Condition, Value</strong> tuples. For example, a group with these criteria: <strong>Virtual Machine Name Contains db_</strong> includes VMs whose names contain the string <code>db_</code> in the group. You can also create groups of tagged network segments, segment ports, or IP sets by specifying a tag, or <strong>Segment Tag Equals testbeds</strong> to include network segments that have the tag <code>testbeds</code>. Objects that match all of the selected criteria are included in the group.</td>
</tr>
<tr>
<td>Members</td>
<td>Select a membership category from the Select Category drop-down list, then select members from the list.</td>
</tr>
<tr>
<td>IP/MAC address</td>
<td>Enter an IP address, MAC addresses, CIDR block, or a range of IP addresses in the form <code>ip-ip</code> (for example <code>192.168.1.1–192.168.1.100</code>).</td>
</tr>
</tbody>
</table>

5. (Optional) Tag the group.

   See Add Tags to an Object for more information about tagging NSX-T objects.

6. Click SAVE to create the group.

**What to do next**

To review group members, select a group and click View Members to review the list of group members to view group members and membership criteria. Click Where Used to see a list of firewall rules that include the group.
Add a Custom Service

Firewall rules often apply to traffic from a network service. A new SDDC includes inventory entries for most of the common network service types, but you can add custom services if you need to.

When you create a firewall rule, you can specify that it applies to network traffic from one or more of the services defined in your SDDC's Services inventory. The default list includes VMware services such as remote console and provisioning, standard services such as IKE, ICMP, and TCP, and many well-known third party services. You can add services to this list by selecting values, typically ports and protocols, from a list of service types and additional service properties.

Procedure

2. On the Networking & Security tab, click Inventory > Services.
   The Services card lists the predefined services.
3. Click ADD NEW SERVICE and give the new service a Name.
4. Click Set Service Entries to open the Set Service Entries page.
5. On the Set Service Entries page, click ADD NEW SERVICE ENTRY.
   To view the list of known services, use the drop-down controls to scroll through the Service Type and Additional Properties lists. To add a service, select a Service Type from the drop-down menu and specify Additional Properties such as Source or Destination Ports of the service, then click APPLY.
6. (Optional) Provide a service Description and tag the service.
   See Add Tags to an Object for more information about tagging NSX-T objects.
7. Click SAVE to create the service definition.

View Virtual Machine Inventory

VMware Cloud on AWS maintains an inventory of workload virtual machines in your SDDC. VMs are listed by name and number of tags.

The Virtual Machines inventory is generated automatically. You can edit the tags assigned to a VM in this list, but you cannot add or remove VMs. The system does that automatically as VMs are created and destroyed.

Procedure

2. On the Networking & Security tab, click Inventory > Virtual Machines.
   If a virtual machine has any tags, the number of tags is shown in the Tags column. Click the number to view the tags. To add or remove VM tags, click the vertical ellipsis at the beginning of the VM row and select Edit to display the tag editor. Click the icon to add more tags.
See Add Tags to an Object for more information about tagging NSX-T objects.

**Managing Workload Connections**

Workload VMs connect to the Internet by default. NAT rules and distributed firewall rules give you fine-grained control over these connections.

**Attach a VM to or Detach a Workload VM from a Compute Network Segment**

Use the vSphere Web Client to manage attachment of workload VMs to compute network segments.

**Prerequisites**

Your SDDC compute network must have at least one segment. See Create or Modify a Network Segment.

**Procedure**

1. Log in to the vSphere Client for your SDDC.
2. Select **Menu > Global Inventory Lists**.
3. Select **Logical Networks**.
4. In the **vCenter Server** drop down menu, select the vCenter Server that manages the logical network you want to use.
5. Click next to the logical network name to select it.
6. Select whether to attach or detach VMs.
   - Click **Attach VM** to attach VMs to the selected network.
   - Click **Detach VM** to detach VMs from the selected network.
7. Select the virtual machine(s) you want to attach or detach, click >> to move them to the **Selected Objects** column, and click **Next**.
8. For each VM, select the virtual NIC you want to attach and click **Next**.
9 Click Finish.

**Request or Release a Public IP Address**

You can request public IP addresses to assign to workload VMs to allow access to these VMs from the internet. VMware Cloud on AWS provisions the IP address from AWS.

As a best practice, release the public IP addresses that are not in use.

**Prerequisites**

Verify that your VM has a static IP address assigned from its logical network.

**Procedure**

1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2. Select Networking & Security > Public IPs.
3. To request a new public IP address, click REQUEST NEW IP.
   
   You can optionally enter your notes about the request.
4. To release an existing public IP address that you no longer need, click the ellipsis button and click Release IP.
   
   Requests to release a public IP address fail if the address is in use by a NAT rule.
5. Click SAVE.
   
   After a few moments, a new Public IP address is provisioned.

**What to do next**

After the public IP address is provisioned, configure NAT to direct traffic from the public IP address to the internal IP address of a VM in your SDDC. See Create or Modify NAT Rules.

**Create or Modify NAT Rules**

Network Address Translation (NAT) maps internal IP addresses on your compute network to addresses exposed on the public Internet. To create a NAT rule, you provide the internal address and port number of a workload VM or service and a public IP address and port number that you have obtained from the system.
NAT rules have to run on the SDDC's internet interface, since that's where your workload VMs' public addresses are exposed. Firewall rules, which examine packet sources and destinations, run on the Compute Gateway, and process traffic after it has been transformed by any applicable NAT rules. When you create a NAT rule, you can specify whether a VM's internal or external IP address and port number are exposed to firewall rules that affect network traffic to and from that VM.

**Important** Inbound traffic to the SDDC's public IP address is always processed by the NAT rules you create. Outbound traffic (reply packets from SDDC workload VMs) is routed along the advertised routes and is processed by NAT rules when the default route for your SDDC network goes through the SDDC's Internet interface. But if the default route goes through a Direct Connect or VPN connection (for example, if 0.0.0.0/0 is advertised through BGP or there is a policy-based VPN with a remote network of 0.0.0.0/0), NAT rules run for inbound traffic but not for outbound traffic, creating an asymmetric path that leaves the VM unreachable at its public IP address. When the default route is advertised from the on-premises environment, you must configure NAT rules on the on-premises network, using the on-premises Internet connection and public IPs.

**Prerequisites**
- The VM must be connected to a compute network segment. You can create NAT rules for VMs whether they have static or dynamic (DHCP) addresses, but bear in mind that NAT rules for VMs using DHCP address assignment can be invalidated when the VM is assigned an internal address that no longer matches the one specified in the rule.
- You must request a public IP address for the VM. See Request or Release a Public IP Address.

**Procedure**
1. Log in to the VMC Console at [https://vmc.vmware.com](https://vmc.vmware.com).
2. Select **Networking & Security > NAT**.
3. Click **ADD NAT RULE** and give the rule a **Name**.
4. Enter the NAT rule parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public IP</td>
<td>Provisioned public IP address for the VM is populated.</td>
</tr>
<tr>
<td>Service</td>
<td>Select one of the following.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>All Traffic</strong> to create a rule that applies to all traffic.</td>
</tr>
<tr>
<td></td>
<td>- Select one of the listed services to create a rule that applies only to traffic using that protocol and port.</td>
</tr>
<tr>
<td>Public Port</td>
<td>If you specified <strong>Service</strong> as <strong>All Traffic</strong>, the default public port is <strong>Any</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you selected a particular <strong>Service</strong>, then the rule applies to the assigned public port for that service.</td>
</tr>
<tr>
<td>Internal IP</td>
<td>Enter the internal IP address of the VM.</td>
</tr>
</tbody>
</table>
Creating Firewall Rules to Manage Traffic Between the Compute and Management Networks

In the default configuration, firewall rules prevent VMs on the compute network from accessing VMs on the management network. To allow individual workload VMs to access management VMs, create Workload and Management inventory groups, then create management gateway firewall rules that reference them.

### Procedure

1. Create Workload inventory groups: one for the management network and one for the workload VM that you want to have access to it.
   - On the Networking & Security tab, click Groups in the Inventory category, then click Workload Groups. Create two workload groups:
     - Click ADD GROUP and create a group with a Member Type of IP address and the CIDR block of the management network. Click SAVE to create the group.
     - Click ADD GROUP and create a group with a Member Type of Virtual Machine and a Member VM from your vSphere inventory. Click SAVE to create the group.

2. Create a Management inventory group to represent the management network that you want to access from the Workload group.
   - On the Networking & Security tab, click Groups in the Inventory category, then click Management Groups. Click ADD GROUP and create a group with a Member Type of IP address and the management network CIDR block. Click SAVE to create the group.

3. Create a compute gateway firewall rule allowing outbound traffic to the management network.
   - See Add or Modify Compute Gateway Firewall Rules for information about creating compute gateway firewall rules. Assuming your workload VMs only need to access vSphere and PowerCLI/OVFtool on management VMs, then the rule need only allow access on port 443.
Table 2-11. Compute Gateway Rule to Allow Outbound Traffic to ESXi and vCenter

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Applied To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound to management network on port 443</td>
<td>Workload VM private IP</td>
<td>VMC Management Network</td>
<td>HTTPS</td>
<td>Allow</td>
<td>All Uplinks</td>
</tr>
</tbody>
</table>

4 Create a management gateway firewall rule allowing inbound traffic to the vCenter server and ESXi.

See Add or Modify Management Gateway Firewall Rules for information about creating management gateway firewall rules. Assuming your workload VMs only need to access vSphere, PowerCLI, or OVFtool on vCenter and ESXi, then the rule need only allow access on port 443.

Table 2-12. Management Gateway Rule to Allow Inbound Traffic to ESXi and vCenter

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound to ESXi port 443</td>
<td>Workload VM private IP</td>
<td>ESXi</td>
<td>HTTPS (TCP 443)</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound to vCenter port 443</td>
<td>Workload VM private IP</td>
<td>vCenter</td>
<td>HTTPS (TCP 443)</td>
<td>Allow</td>
</tr>
</tbody>
</table>
Configure Monitoring and Troubleshooting Features

Use IPFIX and Port Mirroring functionality provided by NSX-T to monitor and troubleshoot SDDC networking and security.

By default, SDDC ESXi hosts have access to the overlay network, allowing them to communicate with monitoring and troubleshooting applications deployed as VM workloads in your SDDC. However, you must configure the firewall to allow traffic between the ESXi hosts and the logical segment the VMs are attached to.

- **Configure IPFIX**
  IPFIX (Internet Protocol Flow Information Export) is a standard for the format and export of network flow information for troubleshooting, auditing, or collecting analytics information.

- **Configure Port Mirroring**
  Port mirroring lets you replicate and redirect all of the traffic coming from a source. The mirrored traffic is sent encapsulated within a Generic Routing Encapsulation (GRE) tunnel to a collector so that all of the original packet information is preserved while traversing the network to a remote destination.

- **View Connected VPC Information**
  The Connected Amazon VPC contains your SDDC and all its networks. Information about this VPC, including the active ENI, VPC subnet, and VPC ID, is available on the **Networking & Security** tab.

**Configure IPFIX**

IPFIX (Internet Protocol Flow Information Export) is a standard for the format and export of network flow information for troubleshooting, auditing, or collecting analytics information.

You can configure flow monitoring on a logical segment. All the flows from the VMs connected to that logical segment are captured and sent to the IPFIX collector. The collector names is specified as a parameter for each IPFIX switch profile.

**Prerequisites**

Verify that a logical segment is configured. See Create or Modify a Network Segment.
Procedure

2. Select **Networking & Security > IPFIX**.
3. To add a new collector, click **COLLECTORS > ADD NEW COLLECTOR** and give the collector a **Name**.
   
Enter the collector IP address and port. The default UDP port is 4739. You can add up to 4 IPFIX collectors.
4. Click **SAVE** to create the collector.
5. Click **SWITCH IPFIX PROFILES** to create or edit a switch IPFIX profile.
   
   See **Configure Switch IPFIX Profiles** in the **NSX-T Data Center Administration Guide** for more information about NSX-T switch IPFIX profile parameters.
6. (Optional) Tag the profile.
   
   See **Add Tags to an Object** for more information about tagging NSX-T objects.
7. Click **SAVE** to create the profile.

**What to do next**

Click the ellipses button next to a switch IPFIX profile and click **Edit** to make configuration changes.

**Configure Port Mirroring**

Port mirroring lets you replicate and redirect all of the traffic coming from a source. The mirrored traffic is sent encapsulated within a Generic Routing Encapsulation (GRE) tunnel to a collector so that all of the original packet information is preserved while traversing the network to a remote destination.

Port mirroring is used in the following scenarios:

- Troubleshooting - Analyze the traffic to detect intrusion and debug and diagnose errors on a network.
- Compliance and monitoring - Forward all of the monitored traffic to a network appliance for analysis and remediation.

Port mirroring includes a source group where the data is monitored and a destination group where the collected data is copied to. The source group membership criteria require VMs to be grouped based on the workload such as web group or application group. The destination group membership criteria require VMs to be grouped based on IP addresses.

Port mirroring has one enforcement point, where you can apply policy rules to your SDDC environment.

The traffic direction for port mirroring is Ingress, Egress, or Bi Directional traffic.

- Ingress is the outbound network traffic from the VM to the logical network.
- Egress is the inbound network traffic from the logical network to the VM.
Bi Directional is the two-way of traffic from the VM to the logical network and from the logical network to the VM. This is the default option.

See Add a Port Mirroring Profile in the NSX-T Data Center Administration Guide for more information about port mirroring with NSX-T.

Prerequisites

Verify that workload groups with IP address and VM membership criteria are available. See Add or Modify a Compute Group.

Procedure

3. On the Port Mirroring page Click ADD PROFILE and give the profile a Name and an optional Description.
4. Specify the profile parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction</td>
<td>Select a traffic direction from the drop-down list.</td>
</tr>
<tr>
<td>Snap Length</td>
<td>Specify the number of bytes to capture from a packet.</td>
</tr>
<tr>
<td>Source</td>
<td>Sources can include segments, segment ports, groups of VMs, and groups vNICs.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destinations are groups of up to 3 IP addresses. You can use existing inventory groups or create new ones from the Set Destination page.</td>
</tr>
<tr>
<td>Encapsulation Type</td>
<td>Must be GRE.</td>
</tr>
<tr>
<td>GRE Key</td>
<td>A value that identifies a particular GRE data stream. See RFC 6245.</td>
</tr>
</tbody>
</table>

5. (Optional) Tag the port mirroring profile.

See Add Tags to an Object for more information about tagging NSX-T objects.

6. Click SAVE to save the session.

What to do next

Click the ellipses button next to a port mirroring profile and select Edit to make configuration changes.

View Connected VPC Information

The Connected Amazon VPC contains your SDDC and all its networks. Information about this VPC, including the active ENI, VPC subnet, and VPC ID, is available on the Networking & Security tab.
Click **Connected VPC** in the **System** category on the **Networking & Security** tab to open the **Connected Amazon VPC** page, which provides the following information:

**AWS Account ID**  
The AWS account ID you specified when you created your SDDC.

**VPC ID**  
The AWS ID of this VPC.

**VPC Subnet**  
The AWS ID of the VPC subnet you specified when you created your SDDC.

**Active Network Interface**  
The identifier for the ENI used by VMC in this VPC.

**IAM Role Names**  
AWS Identity and Access Management role names defined in this VPC. See [AWS Roles and Permissions](VMware Cloud on AWS Operations Guide) in the **VMware Cloud on AWS Operations Guide**.

**Cloud Formation Stack Names**  
The name of the AWS Cloud Formation stack used to create your SDDC.

**Service Access**  
A list of AWS services enabled in this VPC.