VMware Cloud on AWS Networking and Security

19 June 2019

VMware Cloud on AWS

vmware®

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware Cloud on AWS Networking and Security 4

1 NSX-T Networking Concepts 5

Features Supported with NSX-T 8

2 Configuring VMware Cloud on AWS Networking Using NSX-T 9

Assign NSX Service Roles to Organization Members 9

Configure AWS Direct Connect for VMware Cloud on AWS 11

Set Up an AWS Direct Connect Connection 11

Create a Private Virtual Interface for vMotion, ESXi Management, Management Appliance, and Workload Traffic 11

Create a Public Virtual Interface for Access to AWS Services 13

Configure vMotion Interfaces for Use with Direct Connect 14

Configure a VPN Connection Between Your SDDC and On-Premises Data Center 14

Create a Route-Based VPN 15

Create a Policy-Based VPN 17

View Connected VPC Information 20

View VPN Tunnel Status and Statistics 20

IPsec VPN Settings Reference 21

Mapping NSX Parameters to VMC Console VPN Parameters 22

Configure Management Gateway Networking 23

Configure Compute Gateway and Workload Networking 27

Create a Network Segment 28

Configure a Layer 2 VPN and Extended Network 29

Add or Modify Compute Gateway Firewall Rules 33

Add or Modify Distributed Firewall Rules 36

Add a Compute Gateway DNS Zone 38

Configure Compute Gateway DHCP Relay 39

Managing Workload Connections 39

Attach a VM to or Detach a VM from a Logical Network 39

Request a Public IP Address 40

Configure NAT Settings 41

Creating Firewall Rules to Manage Traffic Between the Compute and Management Networks 42

3 Configure Monitoring and Troubleshooting Features 44

Configure IPFIX 44

Configure Port Mirroring 45

About VMware Cloud on AWS Networking and Security

The *VMware Cloud on AWS Networking and Security* provides information about configuring 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 basic features required to run workloads in the cloud and can serve as a starting point for your exploration of additional features and capabilities. The information is 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.

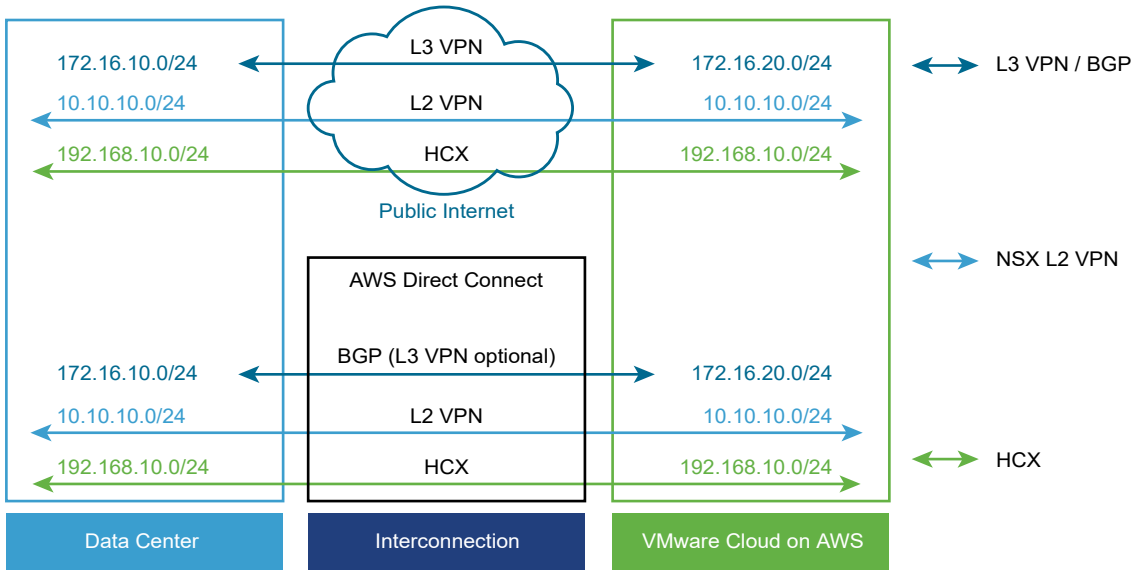
1 NSX-T Networking Concepts

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

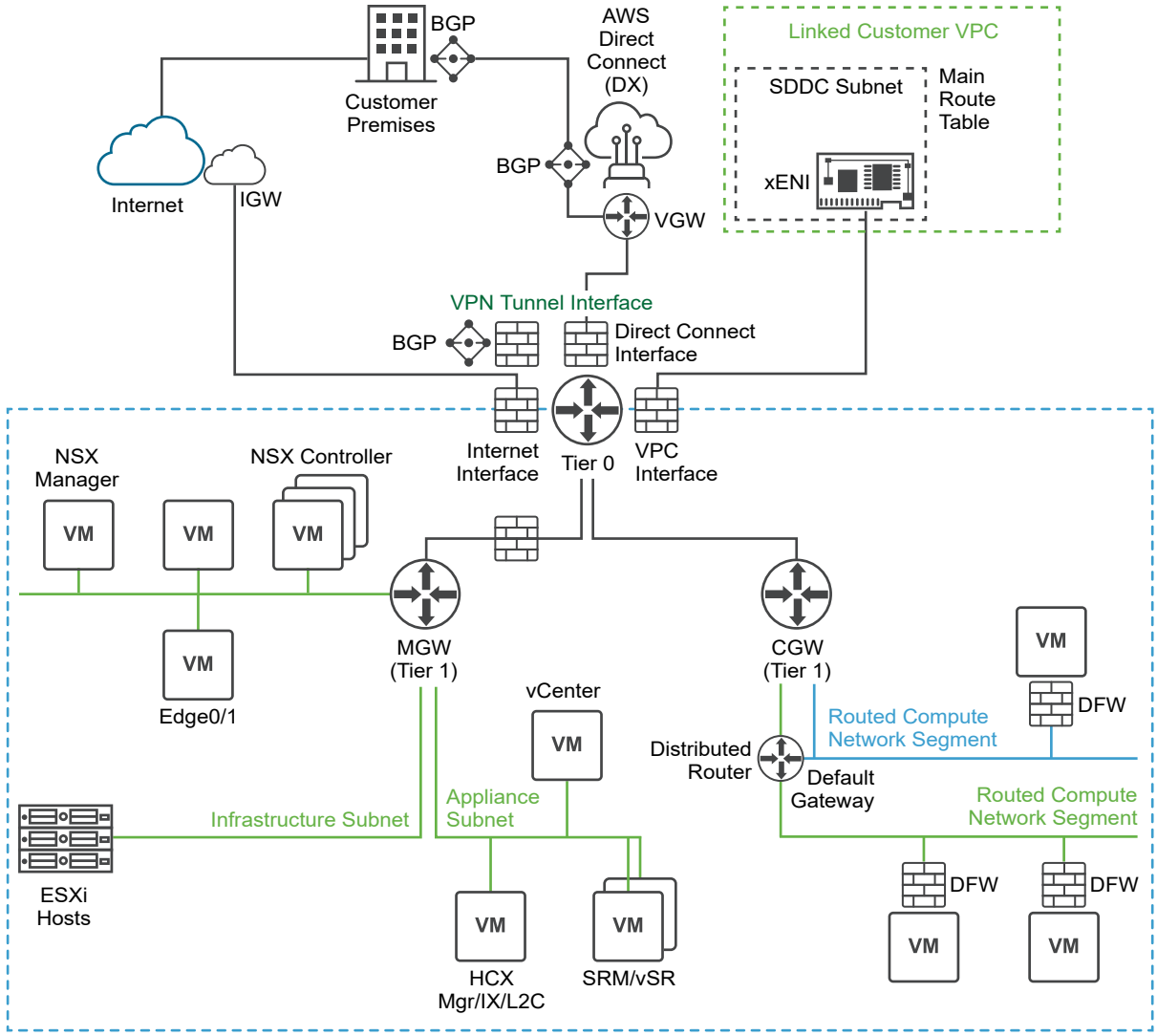
When you create an SDDC, it includes a Management Network and a Compute Network. The Management Network has two subnets:

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 can have up to 16 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.

A Tier 0 NSX Edge appliance sits between your on-premises networks and your SDDC networks, and routes traffic to either the management network or the compute network as appropriate.

Figure 1-2. SDDC Network Topology



Tier 0 Edge Appliance All traffic between your on-premises networks and the SDDC 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 Security gateway that provides north-south network connectivity for the vCenter Server and other management appliances running in the SDDC. The Internet-facing IP address (Public IP #1) is automatically assigned from the pool of AWS public IP addresses when the SDDC is created. Pick an address range (CIDR block) for the management subnet that can support the number of ESXi hosts in your

	SDDC. 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 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.

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.

Table 1-1. Features supported with NSX-T.

Feature or Solution	NSX-T
Policy-based IPsec VPN	Yes
Route-based IPsec VPN	Yes
Direct Connect for All Traffic	Yes
L2 VPN	Yes
Edge Firewall	Yes
Logical Networks, DHCP, DNS, NAT	Yes
Distributed Firewall	Yes
IPFIX, Port Mirroring	Yes
Management Appliance and ESXi access to and from the overlay network and AWS VPC	Yes
Multiple Clusters	Yes
Multiple Availability Zone Stretched Clusters	Yes
Bi-directional migration with vMotion	Yes
VMware Site Recovery	Yes
VMware Hybrid Cloud Extension	Yes
Horizon	Yes
3rd Party Solutions - Storage Partners	Yes
2nd Party Solutions - vRA, vROps	Yes

NSX-T Configuration Maximums

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

Configuring VMware Cloud on AWS Networking Using NSX-T

2

Follow this workflow to configure networking in your SDDC using NSX-T.

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 AWS Direct Connect for VMware Cloud on AWS

If traffic between your on-premises network and your SDDC requires higher speeds and lower latency than you can achieve with a connection over the public Internet, you can 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 Compute Gateway and Workload Networking

Compute gateway networking includes a compute network with one or more segments and the DNS, DHCP, and 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 you SDDC workload network.

5 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

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

7. 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 AWS Direct Connect for VMware Cloud on AWS

If traffic between your on-premises network and your SDDC requires higher speeds and lower latency than you can achieve with a connection over the public Internet, you can 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) 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.

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 vMotion, ESXi Management, Management Appliance, and Workload Traffic

The private virtual interface allows vMotion, ESXi management, management appliance, and workload traffic to flow over the Direct Connect connection between your on-premises environment and your SDDC.

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.

Each private virtual interface allows you to expose up to 16 logical segments to your on-premises infrastructure.

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 under Create a Hosted Virtual Interface.
   - 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.
   - Select **Auto-generate peer IPs** and **Auto-generate BGP key**.

   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** in the VMC Console.
3. Configure DX failover behavior.

   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 DX failover requires a route-based VPN.

   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.

Only a subset of management network routes are advertised over BGP.

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

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

Table 2-1. Advertised Routes for 10.2.0.0 Default MGW CIDR

MGW CIDR	Subnet 1	Subnet 2	Subnet 3
10.2.0.0/23	10.2.0.0/24	10.2.1.0/26	10.2.1.128/25
10.2.0.0/20	10.2.0.0/21	10.2.8.0/23	10.2.12.0/22
10.2.0.0/16	10.2.0.0/17	10.2.128.0/19	10.2.192.0/18

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

You can configure a public virtual interface to provide your workload VMs with access to AWS EC2 instances and services such as S3 without having to route that traffic over the Internet.

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.
   - In the **Interface Owner** field, select **My AWS Account**.
   - Specify **Your router peer IP** and **Amazon router peer IP**.
   - 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.

Option	Description
Override the default gateway (works for vSphere 6.5 hosts only)	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.
Configure the vMotion TCP/IP stack	For each host: a Remove any existing vMotion VMkernel adapters. 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. 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.

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 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.

- 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.

- Mapping NSX Parameters to VMC Console VPN Parameters

  The table below matches terms for VPN parameters used in NSX Edge configuration to the terms used in the VMC Console.

- Configure Management Gateway Networking

  To complete configuration of management gateway networking, set up a DNS server for the management network, specify whether you want to access the SDDC vCenter at a public or private IP address, and create management gateway firewall rules.

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.

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.
2. Click **Networking & Security > VPN > Route Based**.
3. (Optional) Change the default local Autonomous System Number (ASN).

   All route-based VPNs in the SDDC use the same local ASN value in their implementation of BGP. It cannot be the same as the remote ASN for any configured VPN connections. The default value is 65000. To change this, 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 vMotion, ESXi Management, Management Appliance, and Workload Traffic.

- Select the public IP address if you want the VPN to connect over Internet.

6 (Optional) If your on-premises gateway has a NAT address, enter that address as the **Remote Public 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 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

8 For **BGP Remote IP**, enter the IP address of your on-premises VPN gateway.

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

10 Configure **Advanced Tunnel Parameters**.

Option	Description
Tunnel Encryption	Select a Phase 2 security association (SA) cipher that is supported by your on-premises VPN gateway.
Tunnel Digest Algorithm	Select a Phase 2 digest algorithm that is supported by your on-premises VPN gateway. **Note** If you specify a GCM-based cipher for **Tunnel Encryption**, set **Tunnel Digest Algorithm** to **None**. The digest function is integral to the GCM cipher.
Perfect Forward Secrecy	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.
Preshared Key	Enter the preshared key string. The maximum key length is 128 characters. This key must be identical for both ends of the VPN tunnel.
IKE Encryption	Select a Phase 1 (IKE) cipher that is supported by your on-premises VPN gateway.

Option	Description
IKE Digest Algorithm	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 **IKE Digest Algorithm** and the **Tunnel Digest Algorithm**. **Note** If you specify a GCM-based cipher for **IKE Encryption**, set **IKE Digest Algorithm** to **None**. The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher .
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.

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

12 Click **Save**.

The VPN creation process might take a few minutes. When the 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.
2. Select **Networking & Security > VPN > Policy Based**.
3. Click **ADD VPN** and give the new VPN a **Name**.
4. Select a **Local IP Address** for the VPN.

   Specify a public IP address to have the VPN connect over the Internet. If you have configured AWS Direct Connect for this SDDC, you can select an available private IP address to create a VPN that uses Direct Connect and a private VIF. See Using AWS Direct Connect with VMware Cloud on AWS for more information about Direct Connect.

   Note Because of the way Direct Connect handles the security association (SA) required by the IPSec protocol (only a single SA is supported), a route-based VPN is usually a better choice for use with Direct Connect. And while you can configure a policy-based VPN to use Direct Connect, you cannot configure Direct Connect failover to a policy-based VPN.

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

   This IP 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**.

Option	Description
Tunnel Encryption	Select a Phase 2 security association (SA) cipher that is supported by your on-premises VPN gateway.
Tunnel Digest Algorithm	Select a Phase 2 digest algorithm that is supported by your on-premises VPN gateway. **Note** If you specify a GCM-based cipher for **Tunnel Encryption**, set **Tunnel Digest Algorithm** to **None**. The digest function is integral to the GCM cipher.
Perfect Forward Secrecy	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.
IKE Encryption	Select a Phase 1 (IKE) cipher that is supported by your on-premises VPN gateway.
IKE Digest Algorithm	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 **IKE Digest Algorithm** and the **Tunnel Digest Algorithm**. **Note** If you specify a GCM-based cipher for **IKE Encryption**, set **IKE Digest Algorithm** to **None**. The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher .
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 Click **Save**.

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.

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.
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.

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. Select **Networking & Security > VPN**.
3. Click either **Route Based**, **Policy Based**, or **Layer 2**.

   You can retrieve status and statistics for any tunnel that is up.

Operation	Icon
Click the Information icon to display a Status Detail message that provides more information about channel (IKE Phase 1 negotiation) and tunnel status. For a VPN with a Status of Disconnected, the Status Detail tab displays any relevant log messages. You can use these messages in conjunction with the **Tunnel Statistics** and **Error Counts** to help understand channel or tunnel failures.	
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 in the *NSX for vSphere* documentation.

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

Attribute	Allowed Values	Recommended Value
Protocol	IKEv1, IKEv2, IKE FLEX	IKEv2
Encryption Algorithm	AES (128, 256), AES-GCM (128, 192, 256)	AES GCM
Tunnel/IKE Digest Algorithm	SHA-1, SHA-2	SHA-2
Diffie Hellman	DH Groups 2, 5, 14-16	DH Group 14-16

Table 2-3. Static IKE Phase 1 Settings

Attribute	Value
ISAKMP mode	Main mode (Disable aggressive mode)
ISAKMP/IKE SA lifetime	28800 seconds
IPsec Mode	Tunnel
IKE Authentication	Pre-Shared Key

Phase 2 IKE Settings

Table 2-4. Configurable IKE Phase 2 Settings

Attribute	Allowed Values	Recommended Value
Encryption Algorithm	AES-256, AES-GCM, AES	AES-GCM
Perfect forward secrecy (PFS)	Enabled, Disabled	Enabled
Diffie Hellman	DH Groups 2, 5, 14-16	DH Group 14-16

Table 2-5. Static IKE Phase 2 Settings

Attribute	Value
Hashing Algorithm	SHA-1
Tunnel Mode	Encapsulating Security Payload (ESP)
SA lifetime	3600 seconds (one hour)

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.

Mapping NSX Parameters to VMC Console VPN Parameters

The table below matches terms for VPN parameters used in NSX Edge configuration to the terms used in the VMC Console.

NSX Property Name	VMC Console Property Name
Name	VPN Name
Peer ID	On-prem Gateway IP
Peer Endpoint	On-prem Gateway IP
Peer Subnets	On-prem Network
Local ID	Uplink SNAT (not a user-entered value)
Local Endpoint	Uplink IP (not a user-entered value)
Local Subnets	Local Network
Encryption Algorithm	Encryption
Perfect Forward Secrecy	Perfect Forward Secrecy
Authentication	PSK (not a user-entered value)
Diffie Hellman Group	Diffie Hellman
Pre-Shared Key	Pre-Shared Key
Enabled	True (not a user-entered value)

Configure Management Gateway Networking

To complete configuration of management gateway networking, set up a DNS server for the management network, specify whether you want to access the SDDC vCenter at a public or private IP address, and create management gateway firewall rules.

Procedure

1 Specify Management Gateway DNS Servers

Specifying a DNS server allows the management gateway to resolve fully-qualified domain names (FQDNs) to IP addresses on the management network.

2 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.

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.

Specify Management Gateway DNS Servers

Specifying a DNS server allows the management gateway to resolve fully-qualified domain names (FQDNs) to IP addresses on the management network.

Unless you intend to use only static routing, you must specify a DNS server that can resolve IP addresses on both sides of the management gateway to VM FQDNs. Specify the IP address of at least one DNS server when you configure the management gateway. If you specify an optional backup DNS server, be sure that both servers are configured identically.

Procedure

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

2 Select **Networking & Security > DNS**.

3 Under **Management Gateway**, click the ellipses button.

4 Click **Edit** and enter the IP address for **DNS Server 1**.

5 (Optional) Enter the IP address for **DNS Server 2**.

If you specify an address for **DNS Server 2**, be sure that both DNS servers are configured identically.

6 Click **Save**.

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 you 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.
2. Navigate to the **Settings** tab of your SDDC.
3. Expand **vCenter FQDN**, and click **Edit**.
4. 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.

Prerequisites

Verify that management groups and services are configured. See Add a Management Group.

Procedure

1. Log in to the VMC Console at 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 NEW RULE**.
4. Enter the firewall rule parameters.

Option	Description
Rule Name	Enter a descriptive name for the rule.
Source	Click **Set Source** and enter or select one of the following options: 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.
Destination	Click **Set Destination** and enter or select one of the following options: 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 one of the following service types to apply the rule to: ■ Provisioning and Remote Console (TCP 902) applies only to the ESXi system-defined group as a **Destination**. ■ vMotion (TCP 8000). See Required Firewall Rules for vMotion. ■ HTTPS (TCP 443) applies only to vCenter Server system-defined group as a **Destination**. ■ ICMP (All ICMP) ■ SSO (TCP 7444) applies only to vCenter Serversystem-defined group as a **Destination**.
Action	The only action available for a management gateway firewall rule is **Allow**.
Logging	Enable or disable packet logging for this firewall rule. If enabled, the packet logs are forwarded to the Log Intelligence service. To access the logs, visit the Log Intelligence service console.

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

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

Example: Create a Firewall Rule

To create a 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.

Add a Management Group

Management inventory groups contain managed SDDC infrastructure components and on-premises infrastructure components. You can use these groups in management gateway firewall policies.

Management inventory groups are created automatically for SDDC infrastructure components such as vCenter and NSX Manager. You can create additional management inventory groups by specifying the CIDR blocks to which group members are connected. For example, you could create an inventory group for ESXi hosts in the on-premises data center.

Procedure

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

2 Select **Networking & Security > Groups > Management Groups**.

3 Click **Add Group** and give the new group a **Name**.

4 In the **Members** column, enter one or more IP addresses in CIDR format specifying the subnets to which group members are connected.

   Member Type must be an IP Address. Separate multiple addresses with commas.

5 Click **Save** to create the group.

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

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

Use Cases	Service	Source	Destination
VMRC remote console access Required for vRealize Automation	Remote Console	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel	ESXi Management
vMotion traffic over VPN	Any	ESXi Management	IP address or CIDR block from on-premises data center

Important AWS imposes a limit of 50 custom routes for workload logical networks in a VPC. Because these routes are allocated on a first-come, first-served basis, an SDDC can exceed the AWS custom route limit for its VPC. When this happens, workload access to management network addresses can fail with an error of the form:

```
vmcd: [ERROR] errorCode:VMCD00327 [106559563520] Aws route table limit exceeded when adding
192.168.144.0/24 in rtb-02382b7a (routeTables.onpremTable)
```

Configure Compute Gateway and Workload Networking

Compute gateway networking includes a compute network with one or more segments and the DNS, DHCP, and 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 you SDDC workload network.

Procedure

1 Create a Network Segment

Network segments are logical networks for use by workload VMs in the SDDC.

2 Configure a Layer 2 VPN and Extended Network

A VMware Cloud on AWS extended network uses a layer 2 Virtual Private Network (L2VPN) to extend an on-premises network to multiple VLAN based networks that can be extended with different tunnel IDs on the same L2VPN tunnel. This extended network is a single subnet with a single broadcast domain, so you can migrate VMs to and from your cloud SDDC without having to change their IP addresses.

3 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.

4 Add or Modify Distributed Firewall Rules

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

5 Add a Compute Gateway DNS Zone

The Compute Gateway is configured with a single default DNS zone. You can add up to four more zones if you want to provide the flexibility of having multiple DNS servers.

6 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 a Network Segment

Network segments are logical networks for use by workload VMs in the SDDC.

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.

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. In that case, the default network uses CIDR block 172.10.1.0/24.

Multi-host SDDCs are not created with a default network segment, so you must create at least one for your workload VMs. You can use the VMC Console to create additional network segments or delete ones that are no longer in use.

When you create a network segment, ensure that it does not overlap your management network or any of the subnets in your connected Amazon VPC.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Select **Networking & Security > Segments > Add Segments**.
3. Enter a **Name** for the segment.

4 Select a segment **Type** from the drop-down menu and configure the segment.

Type	Configuration
Routed	a Specify the CIDR block of the segment in the **Gateway/Prefix Length** field. b (Optional) Select **Enabled** to enable DHCP. Specify a DHCP IP Range and DNS Suffix such as example.com for the segment. VMs connecting to the segment get their IP addresses from the specified DHCP server and their FQDN has the specified suffix. If you enable DHCP on a logical network and you have configured an on-premises DNS server, you must edit your compute gateway VPN to enable DNS queries to be correctly forwarded over the VPN.
Extended	Specify the ID of an existing L2VPN tunnel block of the segment in the **Tunnel ID** field.
Disconnected	Specify the CIDR block of the segment in the **Gateway/Prefix Length** field.

Note You cannot connect more than 1000 VMs to a network segment of any type.

5 Click **Save**.

The system creates the requested segment. This operation can take up to 15 seconds to complete.

Configure a Layer 2 VPN and Extended Network

A VMware Cloud on AWS extended network uses a layer 2 Virtual Private Network (L2VPN) to extend an on-premises network to multiple VLAN based networks that can be extended with different tunnel IDs on the same L2VPN tunnel. This extended network is a single subnet with a single broadcast domain, so you can 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 on the Compute Gateway 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 Layer 2 VPN Extended Segment

   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 Standalone NSX Edge

   The on-premises end of your L2VPN requires a specially configured standalone NSX Edge appliance. 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.

2 Select **Networking & Security > VPN > Layer 2**.

3 Click **Add VPN Tunnel**.

4 Configure the VPN parameters.

Option	Description
Local IP Address	■ 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 vMotion, ESXi Management, Management Appliance, and Workload Traffic. ■ Select the public IP address if you want the VPN to connect over Internet.
Remote Public IP	Enter the remote public IP address of your on-premise L2VPN gateway. For an L2VPN, this is always the standalone NSX Edge appliance (see Download and Configure the Standalone NSX Edge).
Remote Private IP	Enter the remote private IP address if the on-premise gateway is configured behind NAT.

5 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 Layer 2 VPN Extended Segment

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

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

2 Select **Networking & Security > VPN > Layer 2**.

3 Click **ADD EXTENDED SEGMENT**.

4 Enter the extended segment name.

5 Enter the L2VPN tunnel ID.

6 Click **SAVE**.

7 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.

8 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 Standalone NSX Edge.

Download and Configure the Standalone NSX Edge

The on-premises end of your L2VPN requires a specially configured standalone NSX Edge appliance. 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 to create the L2VPN client side.

Procedure

1 Create a vSphere distributed switch.

2 Add multiple hosts to the newly created vSphere distributed switch.

3 Add a distributed uplink port group to the vSphere Distributed Switch you created in Step 1.

Follow the procedure in Add a distributed uplink port group and use these customization values on the **Configure Settings** and **Security** pages.

Page	Configuration Details
Configure Settings	■ Select **VLAN trunking** from the drop-down menu. ■ Set the VLAN trunk range value to the V:LAN IDs of the VLANs that you plan to extend to the SDDC. ■ Select the Customize default policies configuration option.
Security	■ Set **Promiscuous mode** to **Reject**. ■ Set **MAC address changes** to **Reject**. ■ Set **Forged transmits** to **Accept**.

4 Add a distributed trunk port group to the vSphere Distributed Switch you created in Step 1.

Follow the procedure in Add a distributed trunk port group and use these customization values on the **Configure Settings** and **Security** pages.

Page	Configuration Details
Configure Settings	■ Select **VLAN** from the drop-down menu. ■ Select the **Customize default policies** configuration option.
Security	■ Set **Promiscuous mode** to **Reject**. ■ Set **MAC address changes** to **Reject**. ■ Set **Forged transmits** to **Reject**.

5 Configure a sink port in the distributed trunk port group you created in Step 4.

See Configure a Sink Port in the *VMware NSX Data Center for vSphere* documentation.

6 Download and configure the standalone NSX Edge.

On the L2VPN page, click **REMOTE STANDALONE EDGE DOWNLOAD**. From the download, select the files `NSX-l2t-client-large.ovf`, `NSX-l2t-client-large.mf`, and `nsx-edge-disk*.vmdk` (8 files altogether). Follow the procedure in Deploy the OVF template to deploy these files and create the standalone Edge appliance VM. Specify the following configuration details on the **Select networks** and **Customize template** pages of the **Deploy OVF Template** page.

Page	Configuration Details
Select networks	■ Connect the Trunk network to the uplink port group you created in Step 3. ■ Connect the Public network to the trunk port group you created in Step 4. ■ Accept the default HA interface setting (0). (Optional) Enable the HA interface to deploy the Edge appliance in HA mode. See Configure HA on Standalone L2 VPN Clients.
Customize template	■ Add the peer address and peer code values from the download config file. See Configure Layer 2 VPN Extended Segment. ■ Enter the ID of the VLAN extended by the segment and the L2VPN tunnel ID in the form *`VLAN-ID(tunnel-number)`* where *VLAN-ID* is the ID of the VLAN you are extending and *tunnel-number* is the L2VN tunnel number. In the default configuration the VLAN ID is 100 and the tunnel number is 10, which you enter as `100(10)`. ■ Assign the Edge appliance a static IP address. ■ Assign the unused IP address as the NSX Edge IP address, subnet, and gateway for internet access. ■ Enter the admin and root passwords for the Edge appliance. ■ Select **Power on after deployment**.

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.

Prerequisites

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

Procedure

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

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

3 On the **Gateway Firewall** card, click **Compute Gateway**, then click **ADD NEW RULE**.

You can also select an existing rule, then click the ellipsis button and select **Add Rule Above** or **Add Rule Below**.

4 Enter the firewall rule parameters.

Option	Description
Name	Give the rule a descriptive name.
Source	Click **Set Source** and select an inventory group for source network traffic and click SAVE.
Destination	Click **Set Destination** and select an inventory group for destination network traffic and click SAVE.
Services	Select a service from the drop-down list, or type **Any** if you want the rule to apply to any protocol or port.
Action	Select **Allow** to allow the specified traffic or **Drop** to deny it.
Applied To	Define the type of traffic that the rule applies to: ■ Select **VPN Tunnel Interface** if you want the rule to apply to traffic over the route-based VPN. ■ Select **VPC Interface** if you want the rule to apply to traffic over the linked AWS VPC connection. ■ Select **Internet Interface** if you want the rule to apply to traffic over the Internet, including over policy-based VPNs using Public IP. ■ Select **Direct Connect Interface** if you want the rule to allow traffic over AWS Direct Connect (private VIF), including over policy-based VPNs using Private IP. ■ **All Uplinks** if you want the rule to apply to the **VPC Interface**, the **Internet Interface**, and the **Direct Connect Interface**, but not to the **VPN Tunnel Interface**. (The **VPN Tunnel Interface** is not classified as an uplink.)
Logging	Enable or disable packet logging for this firewall rule. If enabled, the packet logs are forwarded to the Log Intelligence service. To access the logs, visit the Log Intelligence service console.

5 (Optional) Reorder firewall rules.

A rule created from the **ADD NEW RULE** button is placed at the top of the list. Firewall rules are applied in order from top to bottom. To change the position of a rule in the list, select it, then click the ellipsis button and select **Move Rule Up** or **Move Rule Down**.

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

Add or Modify an Inventory Group

Inventory groups categorize VMs based on VM names, IP addresses, and matching criteria of VM name and tag. You use inventory groups to specify sources and destinations when you create firewall rules, and to simplify managing workload VMs that require similar configurations.

Firewall rules often 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
- security tags

VMC Networking & Security inventory groups, like AWS Security Groups, give you a way to create named groups of management or workload VMs that you can reference in firewall rules.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. On the **Networking & Security** tab, click **Inventory > Groups**.
3. On the **Groups** card, click **Management Groups** or **Workload Groups**, then click **ADD GROUP**.

   Management groups contain VMs on the Management Network. Workload groups contain VMs on the Compute network. To modify an existing group, select it and click the ellipsis button.
4. Enter a descriptive **Name** for the group.
5. Select a Member Type.

   The choices are **Virtual Machine**, **IP address**, or **Membership Criteria**.
6. Enter a definition for your group.

   The group definition comprises one or more membership criteria. VMs that match all of the selected criteria are included in the group.

Option	Description
Virtual Machine	Select one or more VMs from the list. **Note** This member type is available only for Workload Groups
IP address	Enter an IP address, CIDR block, or a range of IP addresses in the form *ip-ip* (for example `192.168.1.1–192.168.1.100`) .

Membership Criteria	Click **Set Membership Criteria** to open the **Membership Criteria** page. Click **ADD CRITERIA** and specify one or more criteria as **Property**, **Condition**, **Value** tuples. For example:
	`VM Name Contains db_`
	to include VMs whose names contain the string `db_` in the group, or
	`Tag Equals Secure`
	to include VMs tagged with the tag `Secure`.
	Note This member type is available only for Workload Groups

7. Click **SAVE** to create the group.
8. (Optional) Review group members. Select the newly created group and click the ellipsis button.

Option	Description
View Members	View the members of the group.
View References	View any firewall rules that reference the group.

Add a Custom Service

Predefined and custom services can be used in firewall rules.

When you create a firewall rule, you can specify that the rule applies to one or more of the network services defined in your SDDC. 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

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Select **Networking & Security > Services**.

   The predefined services appear.
3. Click **ADD NEW SERVICE** and type the service name.
4. Select **Set Service Entries > ADD NEW SERVICE ENTRY**.
5. Select the **Service Type** from the drop-down menu and specify any **Additional Properties** of the service.
6. Click **SAVE** to create the service definition.

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 firewall is subjected to the rules in the order shown in the rules table, beginning at the top and proceeding to the rules at the bottom. In some cases, the order of precedence of two or more rules might be important in determining the disposition of a packet. The default firewall rules apply to traffic that does not match any of the user-defined firewall rules, and allows all L3 and L2 traffic.

Note The default L3 firewall rule applies to all traffic, including DHCP. If you change the **Action** in this rule to **Drop** or **Reject**, DHCP traffic is blocked.

Prerequisites

Verify that multiple security groups and services are configured. See Add or Modify an Inventory Group and Add a Custom Service.

Procedure

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

3 If you are an NSX Administrator, you can edit an existing section to add, remove, or reorder rules.

To create a new section, click **ADD NEW SECTION** and give the section a **Name**.

Option	Description
Emergency Rules	Applies to temporary rules needed in emergency situations. For example, block traffic to a Web server due to malicious content.
Infrastructure Rules	Applies to infrastructure rules only. Such as, ESXi, vCenter Server or connectivity to on-premise data center.
Environment Rules	Applies to broad groups. Such as, setting rules so that the production environment cannot reach the test enviroment.
Application Rules	Applies to specific application rules.
Default Rules	The default rules allows all traffic.

4 To add a rule to a new or existing section, select the section and click **ADD NEW RULE**.

5 Enter the parameters for the new rule.

Option	Description
Name	Give the rule a descriptive name.
Sources	Click **Set Source** and select an inventory group for source network traffic, or click **CREATE NEW GROUP** to create a new user-defined inventory group to use for this rule. Click **SAVE**.
Destinations	Click **Set Destination** 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**.
Services	Select a service from the drop-down list, or select **Any** if you want the rule to apply to any protocol or port. Click **SAVE**.
Action	■ Select **Allow** to allow all L2 and L3 traffic to pass through the firewall. ■ Select **Drop** to drop packets with the specified source, destination, and service protocol. Drop 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 with the specified source, destination, and service protocol. Reject action returns a "destination unreachable message" to the sender. If the protocol is TCP, a TCP RST message is sent. ICMP messages with administratively prohibited code are sent for UDP, ICMP, and other IP connections. One benefit of using Reject is that the sending application is notified after only one attempt that the connection cannot be established.
Logging	Enable or disable packet logging for this firewall rule. If enabled, the packet logs are forwarded to the Log Intelligence service. To access the logs, visit the Log Intelligence service console.

6 Click **PUBLISH**.

Manage Distributed Firewall Rules

Traffic packet attempting to pass through the firewall is subjected to the rules in the order shown in the rules table, beginning at the top and proceeding to the rules at the bottom of the list.

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.

When you delete a firewall rule section, all rules in that section are deleted. You cannot delete a section and add it again at a different place in the firewall table. To do so, you must delete the section and publish the configuration. Then add the deleted section to the firewall table and re-publish the configuration.

Prerequisites

Verify that you have multiple distributed firewall sections and rules configured. See Add or Modify Distributed Firewall Rules.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Select **Networking & Security > Distributed Firewall**.
3. Manage rules in a new or existing section, select the section and click the vertical ellipses button.
   - Reorder the firewall rules within a section or reorder the sections.
   - Edit a firewall section or rule configuration.
   - Clone a distributed firewall rule.

     You cannot clone a firewall rule section.
   - Delete a firewall section or a rule within the section.
4. Click **PUBLISH**.

Add a Compute Gateway DNS Zone

The Compute Gateway is configured with a single default DNS zone. You can add up to four more zones if you want to provide the flexibility of having multiple DNS servers.

Compute gateway Domain Name Servers (DNS) enable workload VMs to resolve fully-qualified domain names (FQDNs) to IP addresses.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Select **Networking & Security > DNS**.
3. Click **ADD DNS ZONE** and give the new zone a **Name**.

   You use this **Name** if you create DNS firewall rules that apply to traffic in this zone.
4. Enter a **Domain Name** for the zone.

   This must be a fully qualified domain name, such as example.com.

5 Enter the IP address for **DNS Server 1**.

6 (Optional) Enter the IP address for **DNS Server 2**.

If you specify an address for **DNS Server 2**, be sure that both DNS servers are configured identically.

7 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. For more information about how NSX-T implements DHCP relay, see Configuring DHCP Relay in the NSX for vSphere documentation.

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

Procedure

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

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.

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 VM from a Logical Network

You can connect and disconnect a single or multiple VMs from a logical network.

Procedure

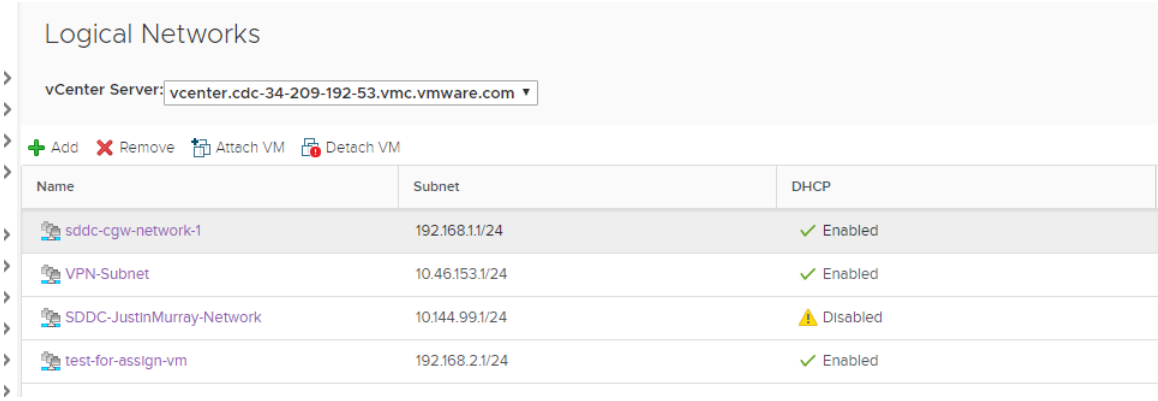
1 Log in to the vSphere Client for your SDDC.

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 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.

2 Select **Networking & Security > Public IPs**.

3 Click **Request Public IP**.

4 Enter applicable notes about the IP address.

5 Click **Save**.

After a few moments, the 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 Configure NAT Settings.

Configure NAT Settings

Inbound Network Address Translation (NAT) allows you to map internet traffic to a public-facing IP address and port to a private IP address and port inside your SDDC's compute network.

When configuring NAT rules, you can configure either one-to-one NAT or one-to-many NAT. Use one-to-one NAT when you want to map a single public IP address and port to a single internal IP address and port.

For example, a public IP of 198.51.100.5 and port 443 is mapped to 172.100.100.20 and port 443. In some cases, you might choose to map a source port to a different destination port. For example, 198.51.100.5 and port 80 might be mapped to 172.100.100.20 and port 8080.

Use one-to-many NAT when a single public IP address and port is mapped to one internal IP address and multiple ports, or to multiple internal IP addresses and ports.

Prerequisites

Before you can assign a public IP address to a virtual machine, you must assign the virtual machine to a logical network and give it a static IP address. See Request a Public IP Address.

Procedure

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

2 Select **Networking & Security > NAT** .

3 Enter the NAT parameter details.

Option	Description
Name	Enter a NAT rule name.
Public IP	Provisioned public IP address for the VM is populated.
Service	Select one of the following. ■ Select Any Traffic for a rule that applies to all inbound traffic. ■ Select a particular service to create a rule that applies only to traffic using that protocol and port.
Public Ports	If you selected Any Traffic, the default public port is Any. If you selected a particular service, then the designated public port for that service appears.
Internal IP	Enter the internal (private) IP address to direct the traffic from the public address to.
Internal Ports	If you selected Any Traffic, the default internal port is Any. If you selected a particular service, then the designated internal port for that service appears.

4 Click **Save**.

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** 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 2-7. Compute Gateway Rule to Allow Outbound Traffic to ESXi and vCenter

Name	Source	Destination	Services	Action	Applied To
Outbound to management network on port 443	Workload VM private IP	VMC Management Network	HTTPS	Allow	All Uplinks

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 2-8. Management Gateway Rule to Allow Inbound Traffic to ESXi and vCenter

Name	Source	Destination	Services	Action
Inbound to ESXi port 443	Workload VM private IP	ESXi	HTTPS (TCP 443)	Allow
Inbound to vCenter port 443	Workload VM private IP	vCenter	HTTPS (TCP 443)	Allow

Configure Monitoring and Troubleshooting Features

3

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.

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 IPFIX collector can be in the on-premise data center on one of the logical segment.

You can control sampling rate and timeout parameters and capture specific granularity of data. If you have large number of flows, you can lower the sampling rate.

After you enable IPFIX, all configured segments send IPFIX messages to the IPFIX collectors using the default port UDP 4739. You can also assign another port number.

Prerequisites

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

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Select **Networking & Security > IPFIX > Configure Collectors**.
3. Enter the collector IP address and port.

   The default UDP port is 4739. You can add up to 4 IPFIX collectors.
4. Click **Save**.
5. Click **Add IPFIX Session**.
6. Enter IPFIX session name.
7. Set the IPFIX session active and idle timeout in seconds.

   The active timeout indicates the time the session must remain active for collecting the data. Idle timeout indicates the time the session can be idle without triggering a session failure.

   The minimum timeout duration should be 60 seconds.
8. Enter the sampling probability of the IPFIX session.

Probability	Description
100%	All the exported data packets are captured.
2%	Two percent of the exported data is captured and the rest of the data packets are dropped.

9. Assign a logical segment tag to this IPFIX session.
10. (Optional) Click the ellipses button next to a IPFIX session and click **Edit** to make configuration changes.
11. Click **Save**.

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.

Prerequisites

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

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Select **Networking & Security > Port Mirroring**.
3. Click **ADD SESSION** and give the session a **Name**.
4. Select a **Source** workload group name and click **SAVE**.
5. Select a **Destination** IP address for the group and click **SAVE**.
6. Select a traffic **Direction** from the drop-down menu.
7. Click **SAVE** to save the session.
8. Click the ellipses button next to a port mirroring session and select **Edit** to make configuration changes.