vCloud Director Tenant Portal Guide

VMware vCloud Director for Service Providers 8.20

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002449-00

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

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

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

vCloud Director Tenant Portal Guide

The *VMware vCloud Director Tenant Portal Guide* provides information about how to use the VMware vCloud Director tenant portal. In this release, you use the tenant portal for configuring advanced networking capabilities that are available in this release of VMware vCloud Director. These advanced networking capabilities are provided by VMware NSX® for vSphere® within a vCloud Director environment.

Intended Audience

This guide is intended for anyone who wants to use the capabilities provided in the tenant portal. The information is written primarily for organization administrators who will use the tenant portal to manage networking capabilities for their organization virtual datacenter networks and vApp networks.

Related Documentation

See the *vCloud Director User's Guide* for information about the features and capabilities available to an organization administrator using the vCloud Director Web console instead of the vCloud Director tenant portal.

VMware Technical Publications Glossary

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

Getting Started with the vCloud Director Tenant Portal 1

You use the vCloud Director tenant portal to perform management tasks on an organization in a vCloud Director system. In this release, the tenant portal provides access to manage distributed firewalls and other advanced networking capabilities that are provided by the VMware NSX® software components made available to an organization by a vCloud Director system administrator.

For an introduction to the vCloud Director product overall and how an organization and its resources are set up in a vCloud Director system, see the *vCloud Director User's Guide*.

The typical users of the tenant portal are:

- vCloud Director system administrators, who might use the tenant portal to configure the distributed firewall and other advanced networking capabilities for an organization.
- Organization administrators, who use the tenant portal to manage the distributed firewall and other advanced networking capabilities that the system administrator has made available to that the organization.

User Prerequisites for Accessing the Tenant Portal

Before a user can use the tenant portal to work with the advanced networking capabilities:

- The organization must have the rights necessary to use the advanced networking capabilities through the tenant portal. See the VMware knowledge base article at http://kb.vmware.com/kb/2149016 for the steps a vCloud Director system administrator takes to grant the necessary rights to an organization.
- The user must be assigned a role that grants the necessary rights. When the rights have been added to the organization by the vCloud Director system administrator, the system administrator can grant those rights to the appropriate roles.

When viewing the properties of a role, the rights required to be able to use all of the advanced networking capabilities available through the tenant portal are:

Folder in the Role Properties window	Required Rights for Advanced Networking Using the Tenant Portal
Distributed Firewall folder	All rights listed in the folder **NOTE** The predefined Organization Administrator role includes the rights Configure Distributed Firewall Rules and View Distributed Firewall Rules by default. Only the System Administrator role has the Enable Distributed Firewall right by default.
General folder	All rights listed in the folder
Gateway folder	Convert to Advanced Gateway View Gateway

Folder in the Role Properties window	Required Rights for Advanced Networking Using the Tenant Portal
Gateway Advanced Services folder	All rights listed in the folder
Organization VDC folder	All rights listed in the folder

A vCloud Director system administrator can choose which individual rights to assign to the organization and which individual rights to grant to roles for users in that organization. If you find you cannot access areas of the tenant portal, contact your vCloud Director system administrator to request the rights for those portal areas.

Introducing Advanced Networking Capabilities for vCloud Director Tenants 2

vCloud Director provides the advanced networking capabilities powered by the NSX network virtualization software that offer enhanced security controls and routing and network scaling capabilities in a cloud environment.

Using these networking capabilities, you can achieve unprecedented security and isolation in your organization virtual datacenter. These capabilities deliver the following benefits:

- Dynamic routing. The NSX capabilities in your vCloud Director environment support routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) to simplify network integration between systems, to provide redundancy and continuity in cloud-hosted application deployment.
- Fine-grained network security and isolation. The NSX capabilities in your vCloud Director environment support the use of object-based rule definitions to provide stateful network traffic isolation without requiring multiple virtual networks. This zero-trust security model prevents intruders from gaining full network access if an application or virtual machine is compromised. Network configuration is simplified by using the same network security policies to protect applications wherever they are physically located in the vCloud Director environment and to extend your zero-trust security model for portable security no matter where an application is deployed.
- Additional capabilities provided by NSX are enhanced VPN support for point-to-site (IPsec VPN) and user (SSL VPN-Plus) connectivity, enhanced load balancing for HTTPS, and expanded network scalability.

Note You can configure two types of firewalls: the edge gateway firewall and the distributed firewall. For more information about the differences between these firewalls, see Chapter 5, "Firewall Configuration Using the Tenant Portal," on page 29.

In this vCloud Director release, you access these advanced networking capabilities using the vCloud Director tenant portal. The edge gateway must first be converted to an advanced edge gateway using the vCloud Director Web console. For the steps to convert an edge gateway to an advanced edge gateway, see the *vCloud Director Administrator's Guide*.

Advanced Routing Configuration Using the vCloud Director Tenant Portal 3

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the tenant portal to configure the static and dynamic routing capabilities that are provided by the NSX software for those advanced edge gateways.

To enable dynamic routing, you configure an advanced edge gateway using the Border Gateway Protocol (BGP) or the Open Shortest Path First (OSPF) protocol.

For detailed information about the routing capabilities that NSX provides, see the Routing topic in the *NSX Administration Guide* at http://www.vmware.com/support/pubs/nsx_pubs.html.

You can specify static and dynamic routing for each advanced edge gateway. The dynamic routing capability provided by NSX provides the necessary forwarding information between Layer 2 broadcast domains, which allows you to decrease Layer 2 broadcast domains and improve network efficiency and scale. NSX extends this intelligence to the workloads' locations for East-West routing. This capability allows more direct virtual machine to virtual machine communication without the added cost or time needed to extend hops.

This chapter includes the following topics:

Specify Default Routing Configurations for the Edge Gateway

Using the Routing screen in the vCloud Director tenant portal, you can specify the default settings for static routing and dynamic routing for your advanced edge gateway.

You can use the tenant portal to work with the default routing settings by launching the tenant portal from the vCloud Director Web console using the **Edge Gateway Services** action on an advanced edge gateway. When the tenant portal is displayed, you use the **Routing** tab to navigate to the routing-related screens.

NOTE To remove all configured routing settings, use the **CLEAR GLOBAL CONFIGURATION** at the bottom of the Routing Configuration screen. This action deletes all routing settings currently specified on the subscreens: default routing settings, static routes, OSPF, BGP, and route redistribution.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Navigate to **Routing > Routing Configuration**.

3 To enable Equal Cost Multipath (ECMP) routing for this edge gateway, turn on the **ECMP** toggle.

   As described in the *NSX Administration Guide*, ECMP is a routing strategy that allows next-hop packet forwarding to a single destination to occur over multiple best paths. NSX determines these best paths either statically, using configured static routes, or as a result of metric calculations by dynamic routing protocols like OSPF or BGP. You can specify the multiple paths for static routes by specifying multiple next hops on the Static Routes screen.

   For more details about ECMP and NSX, see the routing topics in the *NSX 6.2 Troubleshooting Guide*.

4 Specify settings for the default routing gateway.

   a Use the **Applied On** drop-down list to select an interface from which the next hop towards the destination network can be reached.

   To see details about the selected interface, click the blue information icon.

   b Type the gateway IP address.

   c Type the MTU.

   d (Optional) Type an optional description.

   e Click **Save changes**.

5 Specify default dynamic routing settings.

   NOTE If you have IPsec VPN configured in your environment, you should not use dynamic routing.

   a Select a router ID.

   You can select a router ID in the list or use the **+** icon to enter a new one. This router ID is the first uplink IP address of the edge gateway that pushes routes to the kernel for dynamic routing.

   b Configure logging by turning on the **Enable Logging** toggle and selecting the log level.

   c Click **OK**.

6 Click **Save changes**.

What to do next

Add static routes. See "Add a Static Route," on page 13.

Configure route redistribution. See "Configure Route Redistribution Using the Tenant Portal," on page 18.

Configure dynamic routing. See the following topics:

- "Configure BGP Using the Tenant Portal," on page 16
- "Configure OSPF Using the Tenant Portal," on page 14

Add a Static Route

Using the Static Route screen in the vCloud Director tenant portal, you can add a static route for a destination subnet or host.

As described in the NSX documentation, the static route's next hop IP address must exist in a subnet associated with one of the edge gateway's interfaces. Otherwise, configuration of that static route fails.

If ECMP is enabled in the default routing configuration, you can specify multiple next hops in the static routes. See "Specify Default Routing Configurations for the Edge Gateway," on page 11 for steps on enabling ECMP.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **Routing > Static Routes**.

3 Click the **+** icon.

   The Add Static Route dialog box appears.

4 Configure the following options for the static route:

Option	Description
Network	Type the network in CIDR notation.
Next Hop	Type the IP address of the next hop. The next hop IP address must exist in a subnet associated with one of the edge gateway's interfaces. If ECMP is enabled, you can type multiple next hops.
Interface	Optionally select the edge gateway interface on which you want to add a static route. By default, the interface is selected that matches the next hop address.
MTU	If necessary for your needs, edit the maximum transmission value for the data packets. The MTU value cannot be higher than the MTU value set on the selected edge gateway interface. You can see the MTU set on the edge gateway interface by default on the Routing Configuration screen.
Description	Optionally type a description for the static route.

5 Click **Save changes**.

What to do next

Configure a NAT rule for the static route. See "Add an SNAT or DNAT Rule Using the Tenant Portal," on page 86 .

Add a firewall rule to allow traffic to traverse the static route. See "Add an Edge Gateway Firewall Rule Using the Tenant Portal," on page 31 for information.

Configure OSPF Using the Tenant Portal

Using the OSPF screen in the vCloud Director tenant portal, you can configure the Open Shortest Path First (OSPF) routing protocol for the dynamic routing capabilities of your advanced edge gateway. A common application of OSPF on an edge gateway in a vCloud Director environment is to exchange routing information between edge gateways in vCloud Director.

The NSX edge gateway supports OSPF, an interior gateway protocol that routes IP packets only within a single routing domain. As described in the *NSX Administration Guide*, configuring OSPF on an NSX edge gateway enables the edge gateway to learn and advertise routes. The edge gateway uses OSPF to gather link state information from available edge gateways and construct a topology map of the network. The topology determines the routing table presented to the Internet layer, which makes routing decisions based on the destination IP address found in IP packets.

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

Prerequisites

A Router ID must be configured . "Specify Default Routing Configurations for the Edge Gateway," on page 11.

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **Routing > OSPF**.

3 If OSPF is not currently enabled, use the **OSPF Enabled** toggle to enable it.

4 Configure the OSPF settings according to your organization's needs.

Setting	Description
Enable Graceful Restart	Specifies that packet forwarding is to remain uninterrupted when OSPF services are restarted.
Enable Default Originate	Allows the edge gateway to advertise itself as a default gateway to its OSPF peers.

At this point, you can click **Save changes** or continue with configuring area definitions and interface mappings.

5 Add an OSPF area definition to the on-screen table by clicking the **+** icon, specifying details for the mapping in the dialog box, and then clicking **Keep**.

Note By default, the system configures a not-so-stubby area (NSSA) with area ID of 51, and this area is automatically displayed in the area definitions table on the OSPF screen. You can modify or delete this NSSA area if it does not meet your organization's needs.

Setting	Description
Area ID	Type an area ID in the form of an IP address or decimal number.
Area Type	Select **Normal** or **NSSA**. NSSAs prevent the flooding of AS-external link-state advertisements (LSAs) into NSSAs. They rely on default routing to external destinations. As a result, NSSAs must be placed at the edge of an OSPF routing domain. NSSA can import external routes into the OSPF routing domain, thereby providing transit service to small routing domains that are not part of the OSPF routing domain.
Area Authentication **Area Authentication Value**	Select the type of authentication for OSPF to perform at the area level. All edge gateways within the area must have the same authentication and corresponding password configured. For MD5 authentication to work, both the receiver and transmitter must have the same MD5 key. Choices are: ■ **None**, the default value. No authentication is required. ■ **Password**. With this choice, the password you specify in the **Area Authentication Value** field is included in the transmitted packet. ■ **MD5**. With this choice, the authentication uses MD5 (Message Digest type 5) encryption. An MD5 checksum is included in the transmitted packet. Type the Md5 key into the **Area Authentication Value** field.

6 Click **Save changes**, so that the newly configured area definitions are available for selection when you add interface mappings.

7 Add an interface mapping to the on-screen table by clicking the **+** icon, specifying details for the mapping in the dialog box, and then clicking **Keep**.

These mappings map the edge gateway's interfaces to the areas.

a In the dialog box, select the interface you want to map to an area definition.

The interface specifies the external network that both edge gateways are connected to.

b Select the area ID for the area to map to the selected interface.

c (Optional) Change the OSPF settings from the default values to customize them for this interface mapping.

When configuring a new mapping, the default values for these settings are displayed. In most cases, it is recommended to retain the default settings. If you do change the settings, make sure that the OSPF peers use the same settings.

Setting	Description
Hello Interval	Interval (in seconds) between hello packets that are sent on the interface.
Dead Interval	Interval (in seconds) during which at least one hello packet must be received from a neighbor before that neighbor is declared down.
Priority	Priority of the interface. The interface with the highest priority is the designated edge gateway router router.
Cost	Overhead required to send packets across that interface. The cost of an interface is inversely proportional to the bandwidth of that interface. The larger the bandwidth, the smaller the cost.

d Click **Keep**.

8 Click **Save changes** in the OSPF screen.

What to do next

Configure OSPF on the other edge gateways that you want to exchange routing information with.

Add a firewall rule that allows traffic between the OSPF-enabled edge gateways. See "Add an Edge Gateway Firewall Rule Using the Tenant Portal," on page 31 for information.

Make sure that the route redistribution and firewall configuration allow the correct routes to be advertised. See "Configure Route Redistribution Using the Tenant Portal," on page 18.

Configure BGP Using the Tenant Portal

Using the BGP screen in the vCloud Director tenant portal, you can configure Border Gateway Protocol (BGP) for the dynamic routing capabilities of your advanced edge gateway.

As described in the *NSX Administration Guide*, BGP makes core routing decisions by using a table of IP networks or prefixes, which designate network reachability among multiple autonomous systems. In the networking field, the term BGP speaker refers to a networking device that is running BGP. Two BGP speakers establish a connection before any routing information is exchanged. The term BGP neighbor refers to a BGP speaker that has established such a connection. After establishing the connection, the devices exchange routes and synchronize their tables. Each device sends keepalive messages to keep this relationship alive.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **Routing > BGP**.

3 If BGP is not currently enabled, use the **Enable BGP** toggle to enable it.

4 Configure the BGP settings according to your organization's needs.

Setting	Description
Enable Graceful Restart	Specifies that packet forwarding is to remain uninterrupted when BGP services are restarted.
Enable Default Originate	Allows the edge gateway to advertise itself as a default gateway to its BGP neighbors.
Local AS	Required. Specify the autonomous system (AS) ID number to use for the local AS feature of the protocol. The value you specify must be a globally unique number between 1 and 65534. The local AS is a feature of BGP. The system assigns the local AS number to the edge gateway you are configuring. The edge gateway advertises this ID when the edge gateway peers with its BGP neighbors in other autonomous systems. The path of autonomous systems that a route would traverse is used as one metric in the dynamic routing algorithm when selecting the best path to a destination.

At this point, you can click **Save changes**, or continue to configure settings for the BGP routing neighbors.

5 Add a BGP neighbor configuration to the on-screen table by clicking the **+** icon, specifying details for the neighbor in the dialog box, and then clicking **Keep**.

Setting	Description
IP Address	Type the IP address of a BGP neighbor for this edge gateway.
Remote AS	Type a globally unique number between 1-65534 for the autonomous system to which this BGP neighbor belongs. This remote AS number is used in the BGP neighbor's entry in the system's BGP neighbors table.
Weight	The default weight for the neighbor connection. Adjust as appropriate for your organization's needs.
Keep Alive Time	The frequency with which the software sends keepalive messages to its peer. The default frequency is 60 seconds. Adjust as appropriate for your organization's needs.
Hold Down Time	The interval for which the software declares a peer dead after not receiving a keep alive message. This interval must be three times the keep alive interval. The default interval is 180 seconds. Adjust as appropriate for your organization's needs. Once peering between two BGP neighbors is achieved, the edge gateway starts a hold down timer. Every keep alive message it receives from the neighbor resets the hold down timer to 0. If the edge gateway fails to receive three consecutive keep alive messages, so that the hold down timer reaches three times the keep alive interval, the edge gateway considers the neighbor down and deletes the routes from this neighbor.

Setting	Description
Password	If this BGP neighbor requires authentication, type the authentication password. Each segment sent on the connection between the neighbors is verified. MD5 authentication must be configured with the same password on both BGP neighbors, otherwise, the connection between them will not be made.
BGP Filters	Use this table to specify route filtering using a prefix list from this BGP neighbor. CAUTION A `block all` rule is enforced at the end of the filters. Add a filter to the table by clicking the **+** icon and configuring the options. Click **OK** to save each filter. ■ Select the direction to indicate whether you are filtering traffic to or from the neighbor. ■ Select the action to indicate whether you are allowing or denying traffic. ■ Type the network that you want to filter to or from the neighbor. Type `ANY` or a network in CIDR format. ■ Type the **IP Prefix GE** and **IP Prefix LE** to use the `le` and `ge` keywords in the IP prefix list.

6 Click **Save changes** to save the configurations to the system.

What to do next

Configure BGP on the other edge gateways that you want to exchange routing information with.

Add a firewall rule that allows traffic to and from the BGP-configured edge gateways. See "Add an Edge Gateway Firewall Rule Using the Tenant Portal," on page 31 for information.

Configure Route Redistribution Using the Tenant Portal

Because default router behavior is to only share routes with other routers running the same protocol, when you have configured a multi-protocol environment, you must configure route redistribution to have cross-protocol route sharing. Use the Route Redistribution screen in the vCloud Director tenant portal to configure route redistribution for your advanced edge gateway.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **Routing > Route Redistribution**.

3 Use the protocol toggles to turn on those protocols for which you want to enable route redistribution.

4 Add IP prefixes to the on-screen table.

   a Click the **+** icon.

   b Type a name and the IP address of the network in CIDR format.

   c Click **Keep**.

5 Specify redistribution criteria for each IP prefix and add it to the on-screen table by clicking the **+** icon, specifying the criteria in the dialog box, and then clicking **Keep**.

Entries in the table are processed sequentially. Use the up and down arrows to adjust the sequence.

Setting	Description
Prefix Name	Select a specific IP prefix to apply this criteria to or select **Any** to apply the criteria to all network routes.
Learner Protocol	Select the protocol that is to learn routes from other protocols under this redistribution criteria.
Allow learning from	Select the types of networks from which routes can be learned for the protocol selected in the **Learner Protocol** list.
Action	Select whether to permit or deny redistribution from the selected types of networks.

6 Click **Save changes**.

SSL Certificate Management Using the Tenant Portal

4

The NSX software in the vCloud Director environment provides the ability to use Secure Sockets Layer (SSL) certificates with the SSL VPN-Plus and IPsec VPN tunnels you configure for your edge gateways. If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the vCloud Director tenant portal to work with that edge gateway's certificates.

The edge gateways in your vCloud Director environment support self-signed certificates, certificates signed by a Certification Authority (CA), and certificates generated and signed by a CA. Using the tenant portal, you can generate certificate signing requests (CSRs), import the certificates, manage the imported certificates, and create certificate revocation lists (CRLs).

About Using Certificates with Your Organization Virtual Datacenter

You can manage certificates for the following networking areas in your vCloud Director organization virtual datacenter.

- IPsec VPN tunnels between an organization virtual datacenter network and a remote network.
- SSL VPN-Plus connections between remote users to private networks and web resources in your organization virtual datacenter.
- An L2 VPN tunnel between two NSX edge gateways.
- The virtual servers and pools servers configured for load balancing in your organization virtual datacenter

How to Use Client Certificates

You can create a client certificate through a CAI command or REST call. You can then distribute this certificate to your remote users, who can install the certificate on their web browser.

The main benefit of implementing client certificates is that a reference client certificate for each remote user can be stored and checked against the client certificate presented by the remote user. To prevent future connections from a certain user, you can delete the reference certificate from the security server's list of client certificates. Deleting the certificate denies connections from that user.

This chapter includes the following topics:

- "Add a Certificate Revocation List to an Edge Gateway," on page 26
- "Add a Service Certificate to the Edge Gateway," on page 27

Generate a Certificate Signing Request for an Edge Gateway

Before you can order a signed certificate from a CA or create a self-signed certificate using the vCloud Director tenant portal, you must generate a Certificate Signing Request (CSR) for your edge gateway. If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the tenant portal's Certificates screen to generate the CSR.

A CSR is an encoded file that you need to generate on an NSX edge gateway that requires an SSL certificate. Using a CSR standardizes the way that companies send their public keys along with information that identifies their company names and domain names.

You generate a CSR with a matching private-key file that must remain on the edge gateway. The CSR contains the matching public key and other information such as your organization's name, location, and domain name.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Certificates** tab.

3 Click **+ CSR**.

4 Configure the following options for the CSR:

Option	Description
Common Name	Type the fully-qualified domain name (FQDN) for the organization that you will be using the certificate for (for example, `www.example.com`). Do not include the `http://` or `https://` prefixes in your common name.
Organization Unit	Use this field to differentiate between divisions within your vCloud Director organization with which this certificate is associate ; for example, Engineering or Sales.
Organization Name	Type name under which your company is legally registered. The listed organization must be the legal registrant of the domain name in the certificate request.
Locality	Type the city or locality where your company is legally registered.
State or Province Name	Type the full name (do not abbreviate) of the state, province, region, or territory where your company is legally registered.
Country Code	Type the country name where your company is legally registered.
Private Key Algorithm	Type the key type, either RSA or DSA, for the certificate. RSA is typically used. The key type defines the encryption algorithm for communication between the hosts. **NOTE** SSL VPN-Plus supports RSA certificates only.
Key Size	Type the key size in bits (2048 bit minimum).
Description	(Optional) Enter a description for the certificate.

5 Click**Keep**.

The system generates the CSR and adds a new entry with type CSR to the on-screen list.

In the on-screen list, when you select an entry with type CSR, its CSR details are displayed in the screen. You can copy the CSR's displayed PEM formatted data and submit it to a certificate authority (CA) to obtain a CA-signed certificate.

What to do next

Use the CSR to create a service certificate using one of these two options:

- Transmit the CSR to a CA to obtain a CA-signed certificate. When the CA sends you the signed certificate, import the signed certificate into the system. See "Import the CA-Signed Certificate Corresponding to the CSR Generated for an Edge Gateway," on page 23 for information.
- Use the CSR to create a self-signed certificate. See "Configure a Self-Signed Service Certificate," on page 24.

Import the CA-Signed Certificate Corresponding to the CSR Generated for an Edge Gateway

After using the vCloud Director tenant portal to generate a Certificate Signing Request (CSR) and obtaining the CA-signed certificate based on that CSR, you can import the CA-signed certificate to be used by your edge gateway.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Verify that you have obtained the CA-signed certificate that corresponds to the CSR. If the private key in the CA-signed certificate does not match the one for the selected CSR, the import process fails.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Certificates** tab.

3 Select the CSR in the on-screen table for which you are importing the CA-signed certificate.

4 Import the signed certificate by performing the following steps:

   a Click **+ SIGNED CERTIFICATE GENERATED FOR CSR**.

   b Provide the CA-signed certificate's PEM data using one of these methods:

   - If the data is in a PEM file on a system you can navigate to, click the import button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **Signed Certificate (PEM format)** field. Include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

c (Optional) Type an optional description.

d Click **Keep**.

> **Note** If the private key in the CA-signed certificate does not match the one for the CSR you selected on the Certificates screen, the import process fails.

The CA-signed certificate with type Service Certificate appears in the on-screen list.

What to do next

Attach the CA-signed certificate to your SSL VPN-Plus or IPsec VPN tunnels as required. See "Configure SSL VPN Server Settings," on page 57 and "Specify Global IPsec VPN Settings," on page 72 for information.

Configure a Self-Signed Service Certificate

You can configure self-signed service certificates with your edge gateways, to use in the edge gateways' VPN-related capabilities. If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the Certificates screen in the vCloud Director tenant portal to create, install, and manage self-signed certificates.

When the service certificate is available on the Certificates screen, you can specify that service certificate when you configure the edge gateway's VPN-related settings. The VPN presents the specified service certificate to the clients accessing the VPN.

Prerequisites

Verify that at least one CSR is available on the tenant portal's Certificates screen when you open the tenant portal for the edge gateway. See "Generate a Certificate Signing Request for an Edge Gateway," on page 22 for information.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Certificates** tab.

3 Select the CSR in the list that you want to use for this self-signed certificate and click **SELF-SIGN CSR**.

4 Type the number of days that the self-signed certificate is valid for.

5 Click **Keep**.

   The system generates the self-signed certificate and adds a new entry with type Service Certificate to the on-screen list.

The self-signed certificate is available on the edge gateway. In the on-screen list, when you select an entry with type Service Certificate, its details are displayed in the screen.

Add a CA Certificate to the Edge Gateway for SSL Certificate Trust Verification

Adding a CA certificate to an edge gateway enables trust verification of SSL certificates that are presented to the edge gateway for authentication, typically the client certificates used in VPN connections to the edge gateway.

You usually add your company's or organization's root certificate as a CA certificate. A typical use is for SSL VPN, where you want to authenticate VPN clients using certificates. Client certificates could be distributed to the VPN clients and when the VPN clients connect, their client certificates would be validated against the CA certificate.

Note When adding a CA certificate, you typically configure a relevant CRL (Certificate Revocation List). The CRL protects against clients that present revoked certificates. For the steps on adding a CRL to the edge gateway, see "Add a Certificate Revocation List to an Edge Gateway," on page 26.

Prerequisites

Verify you have the CA certificate data in PEM format. In the user interface, you can either paste in the CA certificate's PEM data or browse to a file that contains the data and is available in your network from your local system.

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Certificates** tab.

3 Click **+ CA CERTIFICATE**.

4 Provide the CA certificate's data using one of these methods:

   - If the data is in a PEM file on a system you can navigate to, click the import button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **CA Certificate (PEM format)** field. Include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

5 (Optional) Type an optional description.

6 Click **Keep**.

The CA certificate with type CA Certificate appears in the on-screen list. This CA certificate is now available for you to specify when you configure the edge gateway's VPN-related settings.

Add a Certificate Revocation List to an Edge Gateway

A Certificate Revocation List (CRL) is a list of certificate serial numbers that the issuing Certificate Authority (CA) says have been revoked, so that systems can be updated not to trust users that present those revoked certificates. If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the vCloud Director tenant portal to add CRLs to the edge gateway.

As described in the *NSX Administration Guide*, the CRL contains the following items:

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

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

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Certificates** tab.

3 Click **+ CLR**.

4 Provide the CLR's data using one of these methods:

   - If the data is in a PEM file on a system you can navigate to, click the import button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **CRL (PEM format)** field. Include the `-----BEGIN X509 CRL-----` and `-----END X509 CRL-----` lines.

5 (Optional) Type an optional description.

6 Click **Keep**.

The CRL appears in the on-screen list.

Add a Service Certificate to the Edge Gateway

Adding service certificates to an edge gateway makes those certificates available for use in the edge gateway's VPN-related settings. If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can add a service certificate to the tenant portal's Certificates screen.

Prerequisites

Verify you have the service certificate and its private key in PEM format. In the user interface, you can either paste in the PEM data or browse to a file that contains the data and is available in your network from your local system.

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Certificates** tab.

3 Click **+ SERVICE CERTIFICATE**.

4 Input the service certificate's PEM-formatted data.

   - If the data is in a PEM file on a system you can navigate to, click the import button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **Service Certificate (PEM format)** field. Include the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines.

5 Input the certificate's private key's PEM-formatted data.

   - If the data is in a PEM file on a system you can navigate to, click the import button to browse to the file and select it.
   - If you can copy and paste the PEM data, paste it into the **Private Key (PEM format)** field. Include the `-----BEGIN RSA PRIVATE KEY-----` and `-----END RSA PRIVATE KEY-----` lines.

6 Type in a private key passphrase and confirm it.

7 (Optional) Type an optional description.

8 Click**Keep**.

The certificate with type Service Certificate appears in the on-screen list. This service certificate is now available for you to select when you configure the edge gateway's VPN-related settings.

Firewall Configuration Using the Tenant Portal 5

Using the tenant portal, you can configure the firewall capabilities provided by the NSX software in your vCloud Director organization virtual datacenter. You can create firewall rules for distributed firewalls to provide security between virtual machines in an organization virtual datacenter and firewall rules to apply to an edge gateway firewall to protect the virtual machines in an organization virtual datacenter from outside network traffic.

Note The tenant portal provides the ability to configure both edge gateway firewalls and distributed firewalls.

The NSX logical firewall technology consists of two components to address different deployment use cases. The edge gateway firewall focuses on North-South traffic enforcement while the distributed firewall focuses on East-West access controls.

Key Differences Between Edge Gateway Firewalls and Distributed Firewalls

An edge gateway firewall monitors North-South traffic to provide perimeter security functionality including firewall, Network Address Translation (NAT) as well as site-to-site IPSec and SSL VPN functionality.

A distributed firewall provides the capability to isolate and secure each virtual machine and application down to the layer 2 (L2) level. Configuring distributed firewalls effectively quarantines any external or internal network security compromise, isolating East-West traffic between virtual machines on the same network segment. Security policies are centrally managed, inheritable, and nestable, so networking and security administrators can manage them at scale. Additionally, once deployed, defined security policies follow the virtual machines or applications when they move between different virtual datacenters.

About Firewall Rules

As described in the NSX product documentation, in NSX, the firewall rules defined on the centralized level are referred to as pre rules. You can also add rules at an individual edge gateway level, and those rules are referred to as local rules.

Each traffic session is checked against the top rule in the firewall table before moving down the subsequent rules in the table. The first rule in the table that matches the traffic parameters is enforced. Rules are displayed in the following order:

1. User-defined pre rules have the highest priority, and are enforced in top-to-bottom ordering with a per-virtual NIC level precedence.
2. Auto-plumbed rules (rules that enable control traffic to flow for edge gateway services).
3. Local rules defined at an edge gateway level.

4 Default distributed firewall rule

For more information about how the NSX software enforces firewall rules, see Change the Order of a Firewall Rule in the NSX product documentation.

This chapter includes the following topics:

- "Edge Gateway Firewall," on page 30
- "Manage an Edge Gateway Firewall Using the vCloud Director Tenant Portal," on page 30
- "Distributed Firewall," on page 33
- "Enable the Distributed Firewall on an Organization Virtual Datacenter using the Tenant Portal," on page 34
- "Manage Distributed Firewall Rules Using the Tenant Portal," on page 35

Edge Gateway Firewall

The firewall for the edge gateway helps you meet key perimeter security requirements, such as building DMZs based on IP/VLAN constructs, tenant-to-tenant isolation in multi-tenant virtual data centers, Network Address Translation (NAT), partner (extranet) VPNs, and user-based SSL VPNs.

The edge gateway firewall capability in the vCloud Director environment is provided by the NSX software. In NSX, this firewall capability is also referred to as the edge firewall. The edge gateway firewall monitors North-South traffic to provide perimeter security functionality including firewall, Network Address Translation (NAT) as well as site-to-site IPSec and SSL VPN functionality.

For more detailed information about the capabilities provided by the NSX software's edge gateway firewall, see the *NSX Administration Guide* in the NSX documentation.

Manage an Edge Gateway Firewall Using the vCloud Director Tenant Portal

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the vCloud Director tenant portal to work with that edge gateway's firewall rules.

In addition to the requirement that the edge gateway must be an advanced edge gateway to use the tenant portal with it, the firewall must also be enabled for that edge gateway before you can work with the advanced edge gateway's firewall's rules.

As described in the *NSX Administration Guide*, firewall rules applied to an edge gateway router only protect traffic to and from the router. They do not protect traffic traveling between virtual machines within an organization virtual data center.

Rules created on the distributed firewall screen that have an advanced edge gateway specified in their Applied To column are not displayed in the Firewall screen for that advanced edge gateway .

The edge gateway firewall rules that are displayed in the tenant portal's Firewall screen for an edge gateway are enforced in the following order:

1 Internal rules, also known as auto-plumbed rules. These internal rules enable control traffic to flow for edge gateway services.

2 User-defined rules.

3 Default rule.

The default rule's settings apply to traffic that does not match any of the user-defined firewall rules. The default rule is displayed at the bottom of the rules on the Firewall screen.

In the tenant portal, use the **Enable** toggle on the edge gateway's Firewall Rules screen to disable or enable an edge gateway's firewall.

Add an Edge Gateway Firewall Rule Using the Tenant Portal

You use the edge gateway's Firewall screen in the tenant portal to add firewall rules for that edge gateway. You can add multiple NSX edge interfaces and multiple IP address groups as the source and destination for these firewall rules

Specifying **internal** for a rule's source or destination indicates traffic for all subnets on the portgroups connected to the NSX edge gateway. If you select **internal** as the source, the rule is automatically updated when additional internal interfaces are configured on the NSX edge gateway.

Note Edge gateway firewall rules on internal interfaces do not work when the edge gateway is configured for dynamic routing.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with firewall rules for an edge gateway, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 If the Firewall Rules screen is not already visible, click the **Firewall** tab.

3 To add a rule below an existing rule in the firewall rules table, click in the existing row and then click the **+** icon.

   A row for the new rule is added below the selected rule, and is assigned any destination, any service, and the **Allow** action by default . When the system-defined default rule is the only rule in the firewall table, the new rule is added above the default rule.

4 Click in the **Name** cell and type in a name.

5 Click in the **Source** cell and use the now visible icons to select a source to add to the rule:

Option	Description
Click the IP icon	Type the source value you want to use. Valid values are an IP address, CIDR, an IP range, or the keyword **any**. The edge gateway firewall supports both IPv4 and IPv6 formats.
Click the + icon	Use the **+** icon to specify the source as an object other than a specific IP address: ■ Use the Select objects window to add objects that match your selections and click **Keep** to add them to the rule. ■ To exclude a source from the rule, add it to this rule using the Select objects window and then select the toggle exclusion icon to exclude that source from this rule. When the toggle exclusion is selected on the source, the rule is applied to traffic coming from all sources except for the source you excluded. When the toggle exclusion is not selected, the rule applies to traffic coming from the source you specified in the Select objects window

6 Click in the **Destination** cell and perform one of the following options:

Option	Description
Click the IP icon	Type the destination value you want to use. Valid values are an IP address, CIDR, an IP range, or the keyword **any**. The edge gateway firewall supports both IPv4 and IPv6 formats.
Click the + icon	Use the **+** icon to specify the source as an object other than a specific IP address: ■ Use the Select objects window to add objects that match your selections and click **Keep** to add them to the rule. ■ To exclude a source from the rule, add it to this rule using the Select objects window and then select the toggle exclusion icon to exclude that source from this rule. When the toggle exclusion is selected on the source, the rule is applied to traffic coming from all sources except for the source you excluded. When the toggle exclusion is not selected, the rule applies to traffic coming from the source you specified in the Select objects window

7 Click in the **Service** cell of the new rule and click the **+** icon to specify the service as a port-protocol combination:

a Select the service protocol.

b Type the port numbers for the source and destination ports, or specify **any**.

c Click **Keep**.

8 In the **Action** cell of the new rule, configure the action for the rule.

Option	Description
Accept	Allows traffic from or to the specified sources, destinations, and services.
Deny	Blocks traffic from or to the specified sources, destinations, and services.

9 Click **Save changes**.

The save operation can take a minute to complete.

Modify Edge Gateway Firewall Rules Using the Tenant Portal

You can edit and delete only the user-defined firewall rules that were added to an edge gateway. You cannot edit or delete an auto-generated rule or the default rule, except for changing the default rule's action setting. You can change the priority order of user-defined rules.

For details about the available settings for the rule's various cells, see "Add an Edge Gateway Firewall Rule Using the Tenant Portal," on page 31.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 If the Firewall Rules screen is not already visible, click the **Firewall** tab.

3 Click the **Firewall** tab.

4 Perform any of the following actions to manage the firewall rules:

   - Disable a rule by clicking the green check mark in its **No.** cell. The green check mark turns to a red disabled icon. If the rule is disabled and you want to enable the rule, click the red disabled icon.
   - Edit a rule's name by double-clicking in its **Name** cell and typing the new name.
   - Modify the settings for a rule, such as the source or action settings, by selecting the appropriate cell and using the displayed controls.
   - Delete a rule by selecting it and clicking the **x** icon located above the rules table.
   - Hide system-generated rules by using the **Show only user-defiend rules** toggle.
   - Move a rule up or down in the rules table by selecting the rule and clicking the up and down arrow icons located above the rules table.

   Note You can move a user-defined rule up or down in the table. The system-generated internal rules are always at the top of the table, the default rule is always at the bottom of the table, and those rules cannot be moved.

5 Click **Save changes**.

Distributed Firewall

The distributed firewall allows you to segment organization virtual datacenter entities, such as virtual machines, based on virtual machine names and attributes.

The distributed firewall capability in the vCloud Director environment is provided by the NSX software. As described in the NSX documentation, this distributed firewall is a hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks. You can create access control policies based on objects like virtual machine names and on network constructs like IP addresses or IP set addresses. Firewall rules are enforced at the vNIC level of each virtual machine to provide consistent access control even when the virtual machine is moved to a new ESXi host by vSphere vMotion. This distributed firewall supports a micro-segmentation security model where East-West traffic can be inspected at near line rate processing.

As described in the NSX documentation, for layer 2 (L2) packets, the distributed firewall creates a cache for performance boost. Layer 3 (L3) packets are processed in the following sequence:

1. All packets are checked for an existing state.
2. When a state match is found, the packets are processed.
3. When a state match is not found, the packets are processed through the rules until a match is found.

- For TCP packets, a state is set only for packets with a SYN flag. However, rules that do not specify a protocol (service ANY), can match TCP packets with any combination of flags.
- For UDP packets, 5-tuple details are extracted from the packet. When a state does not exist in the state table, a new state is created using the extracted 5-tuple details. Subsequently received packets are matched against the state that was just created.
- For ICMP packets, ICMP type, code, and packet direction are used to create a state.

The distributed firewall can help in creating identity-based rules as well. Administrators can enforce access control based on the user's group membership as defined in the enterprise Active Directory (AD). Some use cases for when you might use identity-based firewall rules are:

- Users accessing virtual applications using a laptop or mobile device where AD is used for user authentication
- Users accessing virtual applications using VDI infrastructure where the virtual machines are Microsoft Windows based

For more detailed information about the capabilities provided by the NSX software's distributed firewall, see the *NSX Administration Guide* in the NSX documentation.

Enable the Distributed Firewall on an Organization Virtual Datacenter using the Tenant Portal

Before you can use the tenant portal to work with the distributed firewall capabilities on an organization virtual datacenter, the distributed firewall must be enabled for that organization virtual datacenter. A vCloud Director system administrator or a user granted the ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE right can enable the distributed firewall on an organization virtual datacenter.

You use the Distributed Firewall screen in the tenant portal to enable the distributed firewall for an organization virtual datacenter. To open the tenant portal at the Distributed Firewall screen, you must first log in to the vCloud Director Web console, navigate to the organization virtual datacenter for which you want to enable the distributed firewall, right-click that organization virtual datacenter, and click **Manage Firewall**.

Prerequisites

Verify that the organization to which the organization virtual datacenter belongs has the following rights assigned to it:

- Organization vDC Distributed Firewall: Enable/Disable
- Organization vDC Distributed Firewall: Configure Rules
- Organization vDC Distributed Firewall: View Rules

The vCloud Director system administrator assigns rights to an organization. The Organization vDC Distributed Firewall: Enable/Disable right is required for enabling the distributed firewall using the tenant portal's user interface. The Organization vDC Distributed Firewall: View Rules right is required for viewing the firewall rules in the tenant portal and the Organization vDC Distributed Firewall: Configure Rules right is required for configuring the firewall rules using the tenant portal.

Verify that you have an assigned role that grants you the right named Organization vDC Distributed Firewall: Enable/Disable. Of the pre-defined roles in a vCloud Director system, only the System Administrator role has that right by default.

Procedure

1 In the vCloud Director Web console, navigate to the organization virtual datacenter for which you want to enable the distributed firewall.

2 Right-click the name of the organization virtual datacenter and click the **Manage Firewall** action.

  The tenant portal opens and displays the Distributed Firewall screen. If the distributed firewall is not yet enabled for this organization virtual datacenter, the screen displays a message to select the option to enable the distributed firewall.

3 Use the **Enable Distributed Firewall** control to enable the distributed firewall.

After the distributed firewall is enabled, the screen displays the default distributed firewall rule.

What to do next

For a description of the default distributed firewall rule, see "Manage Distributed Firewall Rules Using the Tenant Portal," on page 35.

Manage Distributed Firewall Rules Using the Tenant Portal

As described in the *NSX Administration Guide*, default firewall settings apply to traffic that does not match any of the user-defined firewall rules. In the vCloud Director tenant portal, the default distributed firewall rule is labeled Default Allow Rule.

The distributed firewall capability must be enabled on an organization virtual datacenter before you can manage the distributed firewall settings using the tenant portal.

The default distributed firewall rule is displayed in the tenant portal's Distributed Firewall screen when you open the tenant portal from the vCloud Director Web Console using the **Manage Firewall** menu choice on an organization virtual datacenter. Both the General tab for layer 3 traffic and the Ethernet tab for layer 2 traffic have a default distributed firewall rule.

The default distributed firewall rule is configured to allow all layer 3 and layer 2 traffic to pass through the organization virtual datacenter. This setting is indicated by the Allow set in the Action column in the user interface. The default rule is always at the bottom of the rules table.

Add a Distributed Firewall Rule Using the Tenant Portal

You first add distributed firewall rules at the scope of the organization virtual datacenter. Then using the **Applied To** setting, you can narrow down the scope at which you want to apply the rule. The distributed firewall allows you to add multiple objects at the source and destination levels for each rule, which helps reduce the total number of firewall rules to be added.

Prerequisites

The organization virtual datacenter must be enabled for the distributed firewall before you can configure distributed firewall rules for that organization virtual datacenter. See "Enable the Distributed Firewall on an Organization Virtual Datacenter using the Tenant Portal," on page 34.

Procedure

1 Log in to the vCloud Director Web console and navigate to the organization virtual datacenter.

2 Launch the tenant portal by right-clicking the name of the organization virtual datacenter and clicking **Manage Firewall** in the context menu.

The tenant portal opens in a new browser tab and displays the Distributed Firewall screen.

3 Select the type of rule you want to create. You have the option to create a general rule or an Ethernet rule.

Layer 3 (L3) rules are configured on the **General** tab. Layer 2 (L2) rules are configured on the **Ethernet** tab.

4 To add a rule below an existing rule in the firewall table, click in the existing row and then click the **+** icon.

A row for the new rule is added below the selected rule, and is assigned any destination, any service, and the **Allow** action by default . When the system-defined Default Allow rule is the only rule in the firewall table, the new rule is added above the default rule.

5 Click in the **Name** cell and type in a name.

6 Click in the **Source** cell and use the now visible icons to select a source to add to the rule:

Option	Description
Click the IP icon	Applicable for rules defined on the **General** tab. Type the source value you want to use. Valid values are an IP address, CIDR, an IP range, or the keyword **any**. The distributed firewall supports IPv4 format only.
Click the + icon	Use the **+** icon to specify the source as an object other than a specific IP address: ■ Use the Select objects window to add objects that match your selections and click **Keep** to add them to the rule. ■ To exclude a source from the rule, add it to this rule using the Select objects window and then select the toggle exclusion icon to exclude that source from this rule. When the toggle exclusion is selected on the source, the rule is applied to traffic coming from all sources except for the source you excluded. When the toggle exclusion is not selected, the rule applies to traffic coming from the source you specified in the Select objects window

7 Click in the **Destination** cell and perform one of the following options:

Option	Description
Click the IP icon	Applicable for rules defined on the **General** tab. Type the destination value you want to use. Valid values are an IP address, CIDR, an IP range, or the keyword **any**. The distributed firewall supports IPv4 format only.
Click the + icon	Use the **+** icon to specify the source as an object other than a specific IP address: ■ Use the Select objects window to add objects that match your selections and click **Keep** to add them to the rule. ■ To exclude a source from the rule, add it to this rule using the Select objects window and then select the toggle exclusion icon to exclude that source from this rule. When the toggle exclusion is selected on the source, the rule is applied to traffic coming from all sources except for the source you excluded. When the toggle exclusion is not selected, the rule applies to traffic coming from the source you specified in the Select objects window

8 Click in the **Service** cell of the new rule and perform one of the following options:

Option	Description
Click the IP icon	To specify the service as a port–protocol combination: a Select the service protocol. b Type the port numbers for the source and destination ports, or specify **any**, and click **Keep**.
Click the + icon	To select a pre-defined service or service group, or define a new one: a Select one or more objects and add them to the filter. b Click **Keep**.

9 In the **Action** cell of the new rule, configure the action for the rule.

Option	Description
Allow	Allows traffic from or to the specified sources, destinations, and services.
Deny	Blocks traffic from or to the specified sources, destinations, and services.

10 In the **Direction** cell of the new rule, select whether the rule applies to incoming traffic, outgoing traffic, or both.

11 If this is a rule on the **General** tab, in the **Packet Type** cell of the new rule, select a packet type of **Any**, **IPV4**, or **IPV6**.

12 Select the **Applied To** cell, and use the **+** icon to define the object scope at which this rule is applicable.

NOTE When the rule contains virtual machines in the **Source** and **Destination** cells, you must add both the source and destination virtual machines to the rule's **Applied To** for the rule to work correctly.

13 Click **Save Changes**.

Edit a Distributed Firewall Rule

In a vCloud Director environment, to modify a organization virtual datacenter's existing distributed firewall rule, use the vCloud Director tenant portal's Distributed Firewall screen.

You can edit and delete only the user-defined firewall rules that were configured for an organization virtual datacenter. You cannot edit or delete an auto-generated rule or the default distributed firewall rule.

For details about the available settings for the rule's various cells, see “Add a Distributed Firewall Rule Using the Tenant Portal,” on page 35.

Procedure

1 Log in to the vCloud Director Web console and navigate to the organization virtual datacenter.

2 Launch the tenant portal by right-clicking the name of the organization virtual datacenter and clicking **Manage Firewall** in the context menu.

The tenant portal opens in a new browser tab and displays the Firewall screen, with the **General** tab visible.

3 Perform any of the following actions to manage the distributed firewall rules:

- Disable a rule by clicking the green check mark in its **No.** cell. The green check mark turns to a red disabled icon. If the rule is disabled and you want to enable the rule, click the red disabled icon.
- Edit a rule's name by double-clicking in its **Name** cell and typing the new name.
- Modify the settings for a rule, such as the source or action settings, by selecting the appropriate cell and using the displayed controls.

- Delete a rule by selecting it and clicking the **x** icon located above the rules table.
- Move a rule up or down in the rules table by selecting the rule and clicking the up and down arrow icons located above the rules table.

  Note You can move a custom rule up or down in the table. The default rule is always at the bottom of the table and cannot be moved.

4 Click **Save Changes**.

Custom Grouping Objects 6

The NSX software in your vCloud Director environment provides the capability for defining sets and groups of certain entities, which you can then use when specifying other network-related configurations, such as in firewall rules.

This chapter includes the following topics:

Create an IP Set for Use in Firewall Rules and DHCP Relay Configuration

An IP set is a group of IP addresses that you can add as the source or destination in a firewall rule or in DHCP relay configuration.

You create an IP set using the Grouping Objects page of the vCloud Director tenant portal. The Grouping Objects page is available on both the Distributed Firewall and Edge Gateway screens.

Prerequisites

If you choose to launch the tenant portal using the **Edge Gateway Services** action on an edge gateway, that edge gateway must have already been converted to an advanced gateway.

Procedure

1. Log in to the vCloud Director Web console.
2. Launch the tenant portal using of these two methods.
   - Right-click the name of the organization virtual datacenter and click **Manage Firewall** in the context menu.
   - Right-click the name of an edge gateway that has been converted to an advanced gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Firewall page.
3. Click the **Grouping Objects** tab to display the Grouping Objects page.
4. Click the **IP Sets** tab to display the IP Sets screen if it is not already visible.

   The IP sets that are already defined are displayed on the screen.
5. Click the **+** icon to add a new IP set.

6 Type a name for the set, an optional description, and the IP addresses to be included in the set.

7 (Optional) If you are specifying the IP set using the Grouping Objects page on the Distributed Firewall screen, use the **Inheritance** toggle to enable inheritance to allow visibility at underlying scopes.

Inheritance is enabled by default.

8 Click **Keep** to save this IP set.

The new IP set is available for selection as the source or destination in firewall rules or in DHCP relay configuration.

Create a MAC Set for Use in Firewall Rules

A MAC set is a group of MAC addresses that you can add as the source or destination in a firewall rule.

You create a MAC set using the Grouping Objects page of the vCloud Director tenant portal. The Grouping Objects page is available on both the Distributed Firewall and Edge Gateway screens.

Prerequisites

If you choose to launch the tenant portal using the **Edge Gateway Services** action on an edge gateway, that edge gateway must have already been converted to an advanced gateway.

Procedure

1 Log in to the vCloud Director Web console.

2 Launch the tenant portal using of these two methods.

- Right-click the name of the organization virtual datacenter and click **Manage Firewall** in the context menu.
- Right-click the name of an edge gateway that has been converted to an advanced gateway and click **Edge Gateway Services** in the context menu.

The tenant portal opens in a new browser tab and displays the Firewall page.

3 Click **Grouping Objects** to display the Grouping Objects page.

4 Click the **MAC Sets** tab to display the MAC Sets screen if it is not already visible.

The MAC sets that are already defined are displayed on the screen.

5 Click the **+** icon to add a new MAC set.

6 Type a name for the set, an optional description, and the MAC addresses to be included in the set.

7 (Optional) If you are specifying the MAC set using the Grouping Objects page on the Distributed Firewall screen, use the **Inheritance** toggle to enable inheritance to allow visibility at underlying scopes.

Inheritance is enabled by default.

8 Click **Keep** to save this MAC set.

The new MAC set is available for selection as the source or destination in firewall rules.

View Services Available for Firewall Rules Using the Tenant Portal

Use the vCloud Director tenant portal to view the list of services that are available for use in firewall rules. In this context, a service is a protocol-port combination.

You can view the available services using the Grouping Objects page of the vCloud Director tenant portal. The Grouping Objects page is available on both the Distributed Firewall and Edge Gateway screens.

You cannot add new services to the list using the tenant portal. The set of services available for your use is managed by your vCloud Director system administrator.

Procedure

1 Log in to the vCloud Director Web console.

2 Launch the tenant portal using of these two methods.

- Right-click the name of the organization virtual datacenter and click **Manage Firewall** in the context menu.
- Right-click the name of an edge gateway that has been converted to an advanced gateway and click **Edge Gateway Services** in the context menu.

The tenant portal opens in a new browser tab and displays the Firewall page.

3 Click the **Grouping Objects** tab to display the Grouping Objects page.

4 Click the **Services** tab to display the Services screen if it is not already visible.

The available services are displayed on the screen.

View Service Groups Available for Firewall Rules Using the Tenant Portal

Use the vCloud Director tenant portal to view the list of service groups that are available for use in firewall rules. In this context, a service is a protocol-port combination, and a service group is a group of services or other service groups.

You can view the available service groups using the Grouping Objects page of the vCloud Director tenant portal. The Grouping Objects page is available on both the Distributed Firewall and Edge Gateway screens.

You cannot create new service groups using the tenant portal. The set of service groups available for your use is managed by your vCloud Director system administrator.

Procedure

1 Log in to the vCloud Director Web console.

2 Launch the tenant portal using of these two methods.

- Right-click the name of the organization virtual datacenter and click **Manage Firewall** in the context menu.
- Right-click the name of an edge gateway that has been converted to an advanced gateway and click **Edge Gateway Services** in the context menu.

The tenant portal opens in a new browser tab and displays the Firewall page.

3 Click the **Grouping Objects** tab to display the Grouping Objects page.

4 Click the **Service Groups** tab to display the screen if it is not already visible.

The available service groups are displayed on the screen. The Description column displays the services that are grouped in each service group.

Load Balancing 7

The load balancer distributes incoming service requests among multiple servers in such a way that the load distribution is transparent to users. Load balancing helps achieve optimal resource utilization, maximizing throughput, minimizing response time, and avoiding overload.

About Load Balancing

The NSX load balancer supports two load balancing engines. The layer 4 load balancer is packet-based and provides fast-path processing. The layer 7 load balancer is socket-based and supports advanced traffic management strategies and DDOS mitigation for back-end services.

Load balancing for an edge gateway is configured on the external interface because the edge gateway load balances incoming traffic from the external network. When configuring virtual servers for load balancing, specify one of the available IP addresses you have in your organization VDC. See the *vCloud Director User's Guide*.

Load Balancing Strategies and Concepts

A packet-based load balancing strategy is implemented on the TCP and UDP layer. Packet-based load balancing does not stop the connection or buffer the whole request, instead it sends the packet directly to the selected server after manipulating the packet. TCP and UDP sessions are maintained in the load balancer so that packets for a single session are directed to the same server. You can select Acceleration Enable in both the global configuration and relevant virtual server configuration to enable packet-based load balancing.

A socket-based load balancing strategy is implemented on top of the socket interface. Two connections are established for a single request, a client-facing connection and a server-facing connection. The server-facing connection is established after server selection. For HTTP socket-based implementation, the whole request is received before sending to the selected server with optional L7 manipulation. For HTTPS socket-based implementation, authentication information is exchanged either on the client-facing connection or server-facing connection. Socket-based load balancing is the default mode for TCP, HTTP, and HTTPS virtual servers.

The key concepts of the NSX load balancer are, virtual server, server pool, server pool member, and service monitor.

Virtual Server
Abstract of an application service, represented by a unique combination of IP, port, protocol and application profile such as TCP or UDP.

Server Pool
Group of backend servers.

Server Pool Member
Represents the backend server as member in a pool.

Service Monitor Defines how to probe the health status of a backend server.

Application Profile Represents the TCP, UDP, persistence, and certificate configuration for a given application.

Setup Overview

You begin by setting global options for the load balancer. You now create a server pool consisting of backend server members and associate a service monitor with the pool to manage and share the backend servers efficiently.

You then create an application profile to define the common application behavior in a load balancer such as client SSL, server SSL, x-forwarded-for, or persistence. Persistence sends subsequent requests with similar characteristic such as, source IP or cookie are required to be dispatched to the same pool member, without running the load balancing algorithm. The application profile can be reused across virtual servers.

You then create an optional application rule to configure application-specific settings for traffic manipulation such as, matching a certain URL or hostname so that different requests can be handled by different pools. Next, you create a service monitor that is specific to your application or you may use an already existing service monitor if it meets your needs.

Optionally you can create an application rule to support advanced functionality of L7 virtual servers. Some use cases for application rules include content switching, header manipulation, security rules, and DOS protection.

Finally, you create a virtual server that connects your server pool, application profile, and any potential application rules together.

When the virtual server receives a request, the load balancing algorithm considers pool member configuration and runtime status. The algorithm then calculates the appropriate pool to distribute the traffic comprising one or more members. The pool member configuration includes settings such as, weight, maximum connection, and condition status. The runtime status includes current connections, response time, and health check status information. The calculation methods can be round-robin, weighted round-robin, least connection, source IP hash, weighted least connections, URL, URI, or HTTP header.

Each pool is monitored by the associated service monitor. When the load balancer detects a problem with a pool member, it is marked as DOWN. Only UP server is selected when choosing a pool member from the server pool. If the server pool is not configured with a service monitor, all the pool members are considered as UP.

Configure the Load Balancer Service

Global load balancer configuration parameters include overall enablement, selection of the layer 4 or layer 7 engine, and specification of the types of events to log.

Procedure

1. Launch the tenant portal using the following steps.
   a. Log in to the vCloud Director Web console and navigate to the edge gateway.
   b. Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

      The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.
2. Click the **Load Balancer** tab and click **Global Configuration**.

3 Select the options you want to enable:

Option	Description
Status	Click the **Enabled** icon to enable the load balancer. Click the **Acceleration Enabled** icon to configure the load balancer to use the faster L4 engine rather than L7 engine. The L4 TCP VIP is processed before the edge gateway firewall so no Allow firewall rule is required. **Note** L7 VIPs for HTTP and HTTPS are processed after the firewall, so when **Acceleration Enabled** is not selected, an edge gateway firewall rule must exist to allow access to the L7 VIP for those protocols. When **Acceleration Enabled** is selected and the server pool is in non-transparent mode, an SNAT rule is added, so you must ensure that the firewall is enabled on the edge gateway.
Enable Logging	Click the **Enabled** icon to enable the edge gateway load balancer to collect traffic logs..
Log Level	Choose the severity of events to be logged.

4 Click **Save changes**.

The save operation can take a minute to complete.

What to do next

Configure application profiles for the load balancer. See "Create an Application Profile," on page 45.

Create an Application Profile

An application profile defines the behavior of the load balancer for a particular type of network traffic. After configuring a profile, you associate it with a virtual server. The virtual server then processes traffic according to the values specified in the profile. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

When you create a profile for HTTPS traffic, the following HTTPS traffic patterns are allowed:

- Client -> HTTPS -> LB (terminate SSL) -> HTTP -> servers
- Client -> HTTPS -> LB (terminate SSL) -> HTTPS -> servers
- Client -> HTTPS-> LB (SSL passthrough) -> HTTPS -> servers
- Client -> HTTP-> LB -> HTTP -> servers

Procedure

1 Launch the tenant portal using the following steps.

a Log in to the vCloud Director Web console and navigate to the edge gateway.

b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Load Balancer** tab and **Application Profiles**.

3 Click the **+** icon.

The Edit Item dialog box appears.

4 Type a name for the profile.

5 Configure the application profile.

Option	Description
Type	Select the protocol type used to send requests to the server. The list of required parameters depends on the protocol you select. Parameters that are not applicable to the protocol you selected cannot be entered. All other parameters are required.
HTTP Redirect URL	(HTTP and HTTPS) Type the URL to which traffic that arrives at the destination address should be redirected. .
Enable SSL Passthrough	Click to enable SSL authentication to be passed through to the virtual server. Otherwise SSL authentication takes place at the destination address.
Persistence	Specify a persistence mechanism for the profile. Persistence tracks and stores session data, such as the specific pool member that serviced a client request. This ensures that client requests are directed to the same pool member throughout the life of a session or during subsequent sessions. **Source IP** persistence tracks sessions based on the source IP address. When a client requests a connection to a virtual server that supports source address affinity persistence, the load balancer checks to see if that client previously connected, and if so, returns the client to the same pool member. (TCP Only) Microsoft Remote Desktop Protocol (**MSRDP**) persistence maintains persistent sessions between Windows clients and servers that are running the Microsoft Remote Desktop Protocol (RDP) service. The recommended scenario for enabling MSRDP persistence is to create a load balancing pool that consists of members running a Windows Server guest OS, where all members belong to a Windows cluster and participate in a Windows session directory.
Cookie Name	(HTTP and HTTPS) If you specified **Cookie** as the persistence mechanism, type the cookie name. Cookie persistence uses a cookie to uniquely identify the session the first time a client accesses the site. The load balancer refers to this cookie when connecting subsequent requests in the session, so that they all go to the same virtual server.
Mode	Select the mode by which the cookie should be inserted. The following modes are supported: ■ **Insert** The edge gateway sends a cookie. When the server sends one or more cookies, the client will receive one extra cookie (the server cookies plus the edge gateway cookie). When the server does not send any cookies, the client will receive the edge gateway cookie only. ■ **Prefix** Select this option when your client does not support more than one cookie. **Note** All browsers accept multiple cookies. But you might have a proprietary application using a proprietary client that supports only one cookie. The Web server sends its cookie as usual. The edge gateway injects (as a prefix) its cookie information in the server cookie value. This cookie added information is removed when the edge gateway sends it to the server. ■ **App Session** For this option, the server does not send a cookie; instead, it sends the user session information as a URL. For example, `http://example.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD`, where `jsessionid` is the user session information and is used for the persistence. It is not possible to see the App Session persistence table for troubleshooting.

Option	Description
Expires in (Seconds)	Enter a length of time in seconds that persistence stays in effect. Must be a positive integer in the range 1-86400. NOTE For L7 load balancing using TCP source IP persistence, the persistence entry times out if no new TCP connections are made for a period of time, even if the existing connections are still alive.
Insert X-Forwarded-For HTTP header	(HTTP and HTTPS) Select **Insert X-Forwarded-For HTTP** header for identifying the originating IP address of a client connecting to a Web server through the load balancer.

6 (HTTPS only) Configure the certificates to be used with the application profile. If the certificates you need do not exist, you can create them from the **Certificates** tab.

Option	Description
Virtual Server Certificates	Select the certificate, CAs, or CRLs used to decrypt HTTPS traffic.
Pool Certificates	Define the certificate, CAs, or CRLs used to authenticate the load balancer from the server side. NOTE Select **Enable Pool Side SSL** to enable this tab.
Cipher	Select the cipher algorithms (or cipher suite) negotiated during the SSL/TLS handshake.
Client Authentication	Specify whether client authentication is to be ignored or required. NOTE When set to required, the client must provide a certificate after the request or the handshake is canceled.

7 Click **Keep** to preserve your changes.

The operation can take a minute to complete.

What to do next

Add service monitors for the load balancer to define health checks for different types of network traffic. See "Create a Service Monitor," on page 47.

Create a Service Monitor

You create a service monitor to define health check parameters for a particular type of network traffic. When you associate a service monitor with a pool, the pool members are monitored according to the service monitor parameters.

Procedure

1 Launch the tenant portal using the following steps.

a Log in to the vCloud Director Web console and navigate to the edge gateway.

b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Load Balancer** tab and **Service Monitoring**.

3 Click the **+** icon.

The New Service Monitor dialog box appears.

4 Type a name for the service monitor.

5 (Optional) Configure the following options for the service monitor:

Option	Description
Interval	Type the interval at which a server is to be monitored using the specified **Method**.
Timeout	Type the maximum time in seconds within which a response from the server must be received.
Max Retries	Type the number of times the specified monitoring **Method** must fail sequentially before the server is declared down.
Type	Select the way in which you want to send the health check request to the server—HTTP, HTTPS, TCP, ICMP, or UDP. Depending on the type selected, the remaining options in the **New Service Monitor** dialog are enabled or disabled.
Expected	(HTTP and HTTPS) Type the string that the monitor expects to match in the status line of the HTTP or HTTPS response (for example, HTTP/1.1).
Method	(HTTP and HTTPS) Select the method to be used to detect server status.
URL	(HTTP and HTTPS) Type the URL to be used in the server status request. **Note** When you select the POST method, you must specify a value for **Send**.
Send	(HTTP, HTTPS, UDP) Type the data to be sent.
Receive	(HTTP, HTTPS, and UDP) Type the string to be matched in the response content. **Note** When **Expected** is not matched, the monitor does not try to match the **Receive** content.

Extension	(ALL) Type advanced monitor parameters as key=value pairs. For example, warning=10 indicates that when a server does not respond within 10 seconds, its status is set as warning. All extension items should be separated with a carriage return character. For example:
	`<extension>delay=2`
	`critical=3`
	`escape</extension>`

6 Click **Keep** to preserve your changes.

The operation can take a minute to complete.

Example: Extensions Supported for Each Protocol

Table 7-1. Extensions for HTTP/HTTPS Protocols

Monitor Extension	Description
no-body	Does not wait for a document body and stops reading after the HTTP/HTTPS header. **Note** An HTTP GET or HTTP POST is still sent; not a HEAD method.
max-age=*SECONDS*	Warns when a document is more than SECONDS old. The number can be in the form 10m for minutes, 10h for hours, or 10d for days.
content-type=*STRING*	Specifies a Content-Type header media type in POST calls.
linespan	Allows regex to span newlines (must precede -r or -R).
regex=*STRING* or ereg=*STRING*	Searches the page for regex STRING.
eregi=*STRING*	Searches the page for case-insensitive regex STRING.
invert-regex	Returns CRITICAL when found and OK when not found.

Table 7-1. Extensions for HTTP/HTTPS Protocols (Continued)

Monitor Extension	Description
proxy-authorization=*AUTH_PAIR*	Specifies the username:password on proxy servers with basic authentication.
useragent=*STRING*	Sends the string in the HTTP header as `User Agent`.
header=*STRING*	Sends any other tags in the HTTP header. Use multiple times for additional headers.
onredirect=ok|warning|critical|follow|sticky|stickyport	Indicates how to handle redirected pages. `sticky` is like `follow` but stick to the specified IP address. `stickyport` ensures the port stays the same.
pagesize=*INTEGER:INTEGER*	Specifies the minimum and maximum page sizes required in bytes.
warning=DOUBLE	Specifies the response time in seconds to result in a warning status.
critical=DOUBLE	Specifies the response time in seconds to result in a critical status.

Table 7-2. Extensions for HTTPS Protocol Only

Monitor Extension	Description
sni	Enables SSL/TLS hostname extension support (SNI).
certificate=**INTEGER**	Specifies the minimum number of days a certificate has to be valid. The port defaults to 443. When this option is used, the URL is not checked.
authorization=AUTH_PAIR	Specifies the username:password on sites with basic authentication.

Table 7-3. Extensions for TCP Protocol

Monitor Extension	Description
escape	Allows for the use of `\n`, `\r`, `\t`, or `\` in a send or quit string. Must come before a send or quit option. By default, nothing is added to send and `\r\n` is added to the end of quit.
all	Specifies all expect strings need to occur in a server response. By default, `any` is used.
quit=*STRING*	Sends a string to the server to cleanly close the connection.
refuse=ok|warn|crit	Accepts TCP refusals with states `ok`, `warn`, or `criti`. By default, uses state `crit`.
mismatch=ok|warn|crit	Accepts expected string mismatches with states `ok`, `warn`, or `crit`. By default, uses state `warn`.
jail	Hides output from the TCP socket.
maxbytes=*INTEGER*	Closes the connection when more than the specified number of bytes are received.
delay=*INTEGER*	Waits the specified number of seconds between sending the string and polling for a response.
certificate=*INTEGER*[,*INTEGER*]	Specifies the minimum number of days a certificate has to be valid. The first value is `#days` for warning and the second value is critical (if not specified - 0).
ssl	Uses SSL for the connection.

Table 7-3. Extensions for TCP Protocol (Continued)

Monitor Extension	Description
warning=DOUBLE	Specifies the response time in seconds to result in a warning status.
critical=DOUBLE	Specifies the response time in seconds to result in a critical status.

What to do next

Add server pools for your load balancer. See "Add a Server Pool for Load Balancing," on page 50.

Add a Server Pool for Load Balancing

You can add a server pool to manage and share backend servers flexibly and efficiently. A pool manages load balancer distribution methods and has a service monitor attached to it for health check parameters.

Procedure

1 Launch the tenant portal using the following steps.

  a Log in to the vCloud Director Web console and navigate to the edge gateway.

  b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

  The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Load Balancer** tab and **Pools**.

3 Click the **+** icon.

  The Add Pool window displays.

4 Type a name and description for the load balancer pool.

5 Select a balancing method for the service from the **Algorithm** drop-down menu:

Option	Description
ROUND-ROBIN	Each server is used in turn according to the weight assigned to it. This is the smoothest and fairest algorithm when the server processing time remains equally distributed.
IP-HASH	Selects a server based on a hash of the source and destination IP address of each packet.
LEASTCONN	Distributes client requests to multiple servers based on the number of connections already open on the server. New connections are sent to the server with the fewest open connections.
URI	The left part of the URI (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. This option ensures that a URI is always directed to the same server as long as the server does not go down.

Option	Description
HTTPHEADER	HTTP header name is looked up in each HTTP request. The header name in parenthesis is not case sensitive which is similar to the ACL 'hdr()' function. If the header is absent or does not contain any value, the round robin algorithm is applied. The HTTPHEADER algorithm parameter has one option `headerName=<name>`. For example, you can use **`host`** as the HTTPHEADER algorithm parameter.
URL	URL parameter specified in the argument is looked up in the query string of each HTTP GET request. If the parameter is followed by an equal sign = and a value, then the value is hashed and divided by the total weight of the running servers. The result designates which server receives the request. This process is used to track user identifiers in requests and ensure that a same user ID is always sent to the same server as long as no server goes up or down. If no value or parameter is found, then a round robin algorithm is applied. The URL algorithm parameter has one option `urlParam=<url>`.

6 Add members to the pool.

a Click the **+** icon.

b Type a **Name** for the pool member.

c Type the **IP Address** of the pool member.

d Type the **Port** at which the member is to receive traffic from the load balancer.

e Type the **Monitor Port** at which the member is to receive health monitor requests.

f In **Weight**, type the proportion of traffic this member is to handle. Must be an integer in the range 1-256.

g For **Max Connections**, type the maximum number of concurrent connections the member can handle.

When the number of incoming requests exceeds the maximum, requests are queued and the load balancer waits for a connection to be released.

h For **Min Connections**, type the minimum number of concurrent connections a member must always accept.

i Click **Keep** to add the new member to the pool.

The operation can take a minute to complete.

7 (Optional) To make client IP addresses visible to the backend servers, select **Transparent**.

When **Transparent** is not selected (the default value), backend servers see the IP address of the traffic source as the internal IP address of the load balancer.

When **Transparent** is selected, the source IP address is the actual IP address of the client and the edge gateway must be set as the default gateway to ensure that return packets go through the edge gateway.

8 Click **Keep** to preserve your changes.

The operation can take a minute to complete.

What to do next

Add virtual servers for your load balancer. A virtual server has a public IP address and services all incoming client requests. See "Add a Virtual Server," on page 52.

Add a Virtual Server

Add an edge gateway internal or uplink interface as a virtual server. A virtual server has a public IP address and services all incoming client requests.

By default, the load balancer closes the server TCP connection after each client request.

Procedure

1 Launch the tenant portal using the following steps.

a Log in to the vCloud Director Web console and navigate to the edge gateway.

b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Load Balancer** tab and **Virtual Servers**.

3 Click the **+** icon.

The Add Virtual Server dialog appears.

4 Configure the following options for the virtual server:

Option	Description
Enable Virtual Server	Click to enable the virtual server.
Enable Acceleration	Click to enable acceleration.
Application Profile	Choose an application profile to be associated with the virtual server.
Name	Type a name for the virtual server.
Description	Type a description for the virtual server.
IP Address	Type the IP address that the load balancer listens on.
Protocol	Select the protocol that the virtual server accepts. You must select the same protocol used by the selected **Application Profile**.
Port	Type the port number that the load balancer listens on.
Default Pool	Choose the server pool that the load balancer will use.
Connection Limit	(Optional) Type the maximum concurrent connections that the virtual server can process.
Connection Rate Limit (CPS)	(Optional) Type the maximum incoming new connection requests per second.

5 (Optional) To associate application rules with the virtual server, click the **Advanced** tab and complete the following steps:

a Click the **+** icon.

The application rules created for the load balancer appear. If necessary, add application rules for the load balancer. See "Add an Application Rule," on page 53.

b

6 Click **Keep** to preserve your changes.

The operation can take a minute to complete.

What to do next

Create an edge gateway firewall rule to permit traffic to the new virtual server (the destination IP address). See "Add an Edge Gateway Firewall Rule Using the Tenant Portal," on page 31.

Add an Application Rule

You can write an application rule to directly manipulate and manage IP application traffic.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Load Balancer** tab and **Application Rules**.

3 Click the **+** icon.

   The Add Application Rule dialog box appears.

4 Type the name for the application rule.

5 Type the script for the application rule.

   For information on the application rule syntax, see http://cbonte.github.io/haproxy-dconv/configuration-1.5.html.

6 Click **Keep** to preserve your changes.

   The operation can take a minute to complete.

What to do next

Associate the new application rule to a virtual server added for the load balancer. See "Add a Virtual Server," on page 52 for the steps to associate applications rules with a virtual server.

Secure Access Using Virtual Private Networks 8

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the tenant portal to configure the VPN capabilities that are provided by the NSX software for those advanced edge gateways. You can configure VPN connections to your organization virtual datacenter using an SSL VPN-Plus tunnel, an IPsec VPN tunnel, or an L2 VPN tunnel.

As described in the *NSX Administration Guide*, the NSX edge gateway supports these VPN services:

- SSL VPN-Plus, which allows remote users to access private corporate applications.
- IPsec VPN, which offers site-to-site connectivity between an NSX edge gateway and remote sites which also have NSX or which have third-party hardware routers or VPN gateways.
- L2 VPN, which allows extension of your organization virtual datacenter by allowing virtual machines to retain network connectivity while retaining the same IP address across geographical boundaries.

In a vCloud Director environment, you can create VPN tunnels between:

- Organization virtual datacenter networks on the same organization
- Organization virtual datacenter networks on different organizations
- Between an organization virtual datacenter network and an external network

NOTE vCloud Director does not support multiple VPN tunnels between the same two edge gateways. If there is an existing tunnel between two edge gateways and you want to add another subnet to the tunnel, delete the existing VPN tunnel and create a new one that includes the new subnet.

After you configure VPN tunnels for an edge gateway, you can use a VPN client from a remote location to connect to the organization virtual datacenter that is backed by that edge gateway.

This chapter includes the following topics:

Configure SSL VPN-Plus Using the Tenant Portal

The SSL VPN-Plus services for a vCloud Director environment's edge gateway enable remote users to connect securely to the private networks and applications in the organization virtual datacenters backed by that edge gateway. If the edge gateway for your organization virtual datacenter has been converted to an advanced edge gateway, you can use the tenant portal's SSL VPN-Plus screen to configure various SSL VPN-Plus services on the edge gateway.

In your vCloud Director environment, the edge gateway's SSL VPN-Plus capability supports network access mode. Remote users must install an SSL client to make secure connections and access the networks and applications behind the edge gateway. As part of the edge gateway's SSL VPN-Plus configuration, you add the installation packages for the operating system and configure certain parameters. See "Add an SSL VPN-Plus Client Installation Package," on page 64 for details.

Configuring SSL VPN-Plus on an edge gateway is a multi-step process.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Verify that all of the SSL certificates needed for the SSL VPN-Plus have been added to the tenant portal's Certificates screen. See Chapter 4, "SSL Certificate Management Using the Tenant Portal," on page 21.

NOTE On an edge gateway, port 443 is the default port for HTTPS. For the SSL VPN functionality, the edge gateway's HTTPS port must be accessible from external networks. The SSL VPN client requires the edge gateway IP address and port that are configured in the Server Settings screen on the tenant portal's **SSL VPN-Plus** tab be reachable from the client system. See "Configure SSL VPN Server Settings," on page 57.

Procedure

1 Navigate to the SSL-VPN Plus Screen in the Tenant Portal on page 57

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can navigate to the vCloud Director tenant portal's SSL-VPN Plus screen to begin configuring the SSL-VPN Plus service for that edge gateway.

2 Configure SSL VPN Server Settings on page 57

These server settings configure the SSL VPN server, such as the IP address and port the service listens on, the service's cipher list, and its service certificate. When connecting to the edge gateway, remote users specify the same IP address and port you set in these server settings.

3 Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway on page 59

The remote users are assigned virtual IP addresses from the static IP pools that you configure using the IP Pools screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab.

4 Add a Private Network for Use with SSL VPN-Plus on an Edge Gateway on page 60

Use the Private Networks screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to configure the private networks. The private networks are the ones you want the VPN clients to have access to, when the remote users connect using their VPN clients and the SSL VPN tunnel. The enabled private networks will be installed in the routing table of the VPN client.

5 Configure an Authentication Service for SSL VPN-Plus on an Edge Gateway on page 61

Use the Authentication screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to set up a local authentication server for the edge gateway's SSL VPN service and optionally enable client certificate authentication. This authentication server is used to authenticate the connecting users. All users configured in the local authentication server will be authenticated.

6 Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server on page 63

Use the Users screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to add accounts for your remote users to the local authentication server for the edge gateway's SSL VPN service.

7 Add an SSL VPN-Plus Client Installation Package on page 64

Use the Installation Packages screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to create named installation packages of the SSL VPN-Plus client for the remote users.

8 Edit SSL VPN-Plus Client Configuration on page 65

Use the Client Configuration screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to customize the way the SSL VPN client tunnel responds when the remote user logs in to SSL VPN.

9 Customize the General SSL VPN-Plus Settings for an Edge Gateway on page 66

By default, the system sets some SSL VPN-Plus settings on an edge gateway in your vCloud Director environment. You can use the General Settings screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to customize these settings.

Navigate to the SSL-VPN Plus Screen in the Tenant Portal

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can navigate to the vCloud Director tenant portal's SSL-VPN Plus screen to begin configuring the SSL-VPN Plus service for that edge gateway.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

  a Log in to the vCloud Director Web console and navigate to the edge gateway.

  b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

  The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, click the **SSL VPN-Plus** tab.

What to do next

Use the **General** screen to configure the default SSL VPN-Plus settings. See "Customize the General SSL VPN-Plus Settings for an Edge Gateway," on page 66.

Configure SSL VPN Server Settings

These server settings configure the SSL VPN server, such as the IP address and port the service listens on, the service's cipher list, and its service certificate. When connecting to the edge gateway, remote users specify the same IP address and port you set in these server settings.

If your edge gateway is configured with multiple, overlay IP address networks on its external interface, the IP address you select for the SSL VPN server can be different than the default external interface of the edge gateway.

While configuring the SSL VPN server settings, you must choose which encryption algorithms to use for the SSL VPN tunnel. You can choose one or more ciphers. Carefully choose the ciphers according to the strengths and weaknesses of your selections.

By default, the system uses the default, self-signed certificate that the system generates for each edge gateway as the default server identity certificate for the SSL VPN tunnel. Instead of this default, you can choose to use a digital certificate that you have added to the system on the Certificates screen.

Prerequisites

Verify you have met the prerequisites described in "Configure SSL VPN-Plus Using the Tenant Portal," on page 56.

If you choose to use a service certificate different than the default one, import the required certificate into the system. See "Add a Service Certificate to the Edge Gateway," on page 27 for information.

Verify that you have completed the steps described in "Navigate to the SSL-VPN Plus Screen in the Tenant Portal," on page 57.

Procedure

1 In the tenant portal, on the SSL VPN-Plus screen, click **Server Settings**.

2 Select an IPv4 address.

3 (Optional) Type a TCP port number.

   This TCP port number is used by the SSL client installation package. By default, the system uses port 443, which is the default port for HTTPS/SSL traffic. Even though port number is required you can set any TCP port for communications.

   NOTE The SSL VPN client requires the IP address and port configured here to be reachable from your remote users' client systems. If you change the port number from the default, ensure the IP address and port combination will be reachable from your intended users' systems.

4 Select an encryption method in the cipher list.

5 Configure the service's syslog logging policy.

   Logging is enabled by default. You can change the level of messages to log or disable logging.

6 (Optional) If you want to use a service certificate instead of the system-generated self-signed certificate that the system uses by default, click **CHANGE SERVER CERTIFICATE**, make your selection, and click **OK**.

7 Click **Save changes**.

What to do next

NOTE The edge gateway IP address and the TCP port number you set must be reachable by your remote users. Add an edge gateway firewall rule that allows access to the SSL VPN-Plus IP address and port configured in this procedure. See "Add an Edge Gateway Firewall Rule Using the Tenant Portal," on page 31 for information.

Add an IP pool so that remote users are assigned IP addresses when they connect using SSL VPN-Plus. See "Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway," on page 59 for information.

Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway

The remote users are assigned virtual IP addresses from the static IP pools that you configure using the IP Pools screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab.

Each IP pool added in this screen results in an IP address subnet configured on the edge gateway. The IP address ranges used in these IP pools must be different from all other networks configured on the edge gateway.

Note SSL VPN assigns IP addresses to the remote users from the IP pools based on the top-down order the IP pools appear in the on-screen table. After you add the IP pools to the on-screen table, you can adjust their positions in the table using the up and down arrows.

Prerequisites

Verify you have completed the steps described in "Configure SSL VPN Server Settings," on page 57.

Procedure

1 On the tenant portal's **SSL VPN-Plus** tab, click **IP Pools**.

2 Click the **+** icon.

3 Configure the following options for the IP pool.

Options	Description
IP Range	Type an IP address range for this IP pool, such as `127.0.0.1–127.0.0.9.`. These IP addresses will be assigned to VPN clients when they authenticate and connect to the SSL VPN tunnel.
Netmask	Type the netmask of the IP pool, such as `255.255.255.0`.
Gateway	Type the IP address that you want the edge gateway to create and assign as the gateway address for this IP pool. When the IP pool is created, a virtual adapter is created on the edge gateway VM and this IP address is configured on that virtual interface. This IP address can be any IP within the subnet that is not also in the range in the **IP Range** field.
Description	(Optional) Type a description for this IP pool.
Status	Select whether to enable or disable this IP pool.
Primary DNS	(Optional) In the **Advanced** section, type the name of the primary DNS server that will be used for name resolution for these virtual IP addresses.
Secondary DNS	(Optional) Type the name of the secondary DNS server to use.
DNS Suffix	(Optional) Type DNS suffix for the domain the client systems are hosted on, for domain-based host name resolution.
WINS Server	(Optional) Type the WINS server address if needed for your organization's needs.

4 Click **Keep**.

The IP pool configuration is added to the on-screen table.

What to do next

Add private networks that you want accessible to your remote users connecting with SSL VPN-Plus. See "Add a Private Network for Use with SSL VPN-Plus on an Edge Gateway," on page 60.

Add a Private Network for Use with SSL VPN-Plus on an Edge Gateway

Use the Private Networks screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to configure the private networks. The private networks are the ones you want the VPN clients to have access to, when the remote users connect using their VPN clients and the SSL VPN tunnel. The enabled private networks will be installed in the routing table of the VPN client.

The private networks is a list of all reachable IP networks behind the edge gateway that you want to encrypt traffic for a VPN client, or exclude from encrypting. Each private network that requires access through an SSL VPN tunnel must be added as a separate entry. You can use route summarization techniques to limit the number of entries.

Note

- SSL VPN-Plus allows remote users to access private networks based on the top-down order the IP pools appear in the on-screen table. After you add the private networks to the on-screen table, you can adjust their positions in the table using the up and down arrows.
- If you select **Enable TCP Optimization** for a private network, some applications such as FTP in active mode may not work within that subnet. To add an FTP server configured in active mode, you must add another private network for that FTP server and disable TCP optimization for that private network. Also, the private network for that FTP server must be enabled and appear in the on-screen table above the TCP-optimized private network.

Prerequisites

Verify you have completed the steps described in "Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway," on page 59.

Open the tenant portal and browse to the SSL-VPN Plus screen as described in "Navigate to the SSL-VPN Plus Screen in the Tenant Portal," on page 57.

Procedure

1. On the tenant portal's **SSL VPN-Plus** tab, click **Private Networks**.
2. Click the **+** icon.
3. In the window that opens, configure the following options for the private network.

Options	Description
Network	Type the private network IP address in CIDR format, such as **`192169.1.0/24`**.
Description	(Optional) Type a description for the network.
Send Traffic	Specify whether you want the VPN client to send private network and Internet traffic over the SSL VPN-Plus enabled edge gateway (**Over Tunnel**) or bypass the edge gateway and send the traffic directly to the private server (**Bypass Tunnel**).

Options	Description
Enable TCP Optimization	(Optional) As a best practice, when you select **Over Tunnel** for sending the traffic, also select **Enable TCP Optimization** to best optimize the Internet speed. This option is enabled by default. Selecting this option enhances the performance of TCP packets within the VPN tunnel but does not improve performance of UDP traffic. Conventional full-access SSL VPNs tunnel sends TCP/IP data in a second TCP/IP stack for encryption over the Internet. This conventional method encapsulates application layer data in two separate TCP streams. When packet loss occurs, which can happen even under optimal Internet conditions, a performance degradation effect called TCP-over-TCP meltdown occurs. In TCP-over-TCP meltdown, two TCP instruments correct the same single packet of IP data, undermining network throughput and causing connection timeouts. Selecting **Enable TCP Optimization** eliminates the risk of this TCP-over-TCP problem occurring. **Note** When TCP optimization is enabled: ■ You must use the **Ports** field and specify the port numbers for which traffic should be optimized. ■ The SSL VPN server opens the TCP connection on behalf of the VPN client. When the TCP connection is opened by the SSL VPN server, the first automatically generated edge firewall rule is applied, which allows all connections opened from the edge gateway to get passed. Traffic that is not optimized will be evaluated by the regular edge firewall rules. The default generated TCP rule is allow any any.
Ports	When **Over Tunnel** is selected, type a range of port numbers that you want opened for the remote user to access the internal servers, such as **20–21** for FTP traffic and **80–81** for HTTP traffic. To give unrestricted access to users, leave this field blank.
Status	Specify whether you want to enable or disable the private network.

4 Click **Keep** to add the private network configuration to the on-screen table.

5 Click **Save changes** to save the configuration to the system.

What to do next

Add an authentication server. See "Configure an Authentication Service for SSL VPN-Plus on an Edge Gateway," on page 61.

Important Add the corresponding firewall rules to allow network traffic to the private networks you have added in this screen. See "Add an Edge Gateway Firewall Rule Using the Tenant Portal," on page 31 for information.

Configure an Authentication Service for SSL VPN-Plus on an Edge Gateway

Use the Authentication screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to set up a local authentication server for the edge gateway's SSL VPN service and optionally enable client certificate authentication. This authentication server is used to authenticate the connecting users. All users configured in the local authentication server will be authenticated.

You can have only one local SSL VPN-Plus authentication server configured on the edge gateway. If you click **+ LOCAL** and specify additional authentication servers, an error message is displayed when you try to save the configuration.

The maximum time to authenticate over SSL VPN is three (3) minutes. This maximum is determined by the non-authentication timeout, which is 3 minutes by default and is not configurable. As a result, if you have multiple authentication servers in chain authorization and user authentication takes more than 3 minutes, the user will not be authenticated.

Prerequisites

Verify you have completed the steps described in "Add a Private Network for Use with SSL VPN-Plus on an Edge Gateway," on page 60.

If you intend to enable client certificate authentication, verify that a CA certificate has been added to the edge gateway. See "Add a CA Certificate to the Edge Gateway for SSL Certificate Trust Verification," on page 25.

Open the tenant portal and browse to the SSL-VPN Plus screen as described in "Navigate to the SSL-VPN Plus Screen in the Tenant Portal," on page 57.

Procedure

1 Click the **SSL VPN-Plus** tab and **Authentication**.

2 Click **+ LOCAL**.

3 In the window that opens, configure the following options for the authentication server.

To enable the authentication server, turn on the **Enabled** toggle located in the Status section of the window.

a (Optional) Configure the password policy.

Options	Description
Enable password policy	Turn on enforcement of the password policy settings you configure here.
Password Length	Type the minimum and maximum allowed values for password length.
Minimum no. of alphabets	(Optional) Type the minimum number of alphabetic characters, such as `A b c D`, that are required in the password.
Minimum no. of digits	(Optional) Type the minimum number of numeric characters, such as `1 2 3`, that are required in the password.
Minimum no. of special characters	(Optional) Type the minimum number of special characters, such as `& # %`, that are required in the password.
Password should not contain user ID	(Optional) Turn on this toggle to enforce that the password must not contain the user ID.
Password expires in	(Optional) Type the maximum number of days that a password can exist before the user must change it.
Expiry notification in	(Optional) Type the number of days prior to the **Password expires in** value at which the user is notified the password is about to expire.

b (Optional) Configure the account lockout policy.

Options	Description
Enable password policy	Turn on enforcement of the account lockout policy settings you configure here.
Retry Count	Type the number of times a remote user can try to access his or her account after entering an incorrect password.
Retry Duration	Type the time period in minutes in which the remote user's account gets locked on unsuccessful login attempts. For example, if you specify the **Retry Count** as 5 and **Retry Duration** as 1 minute, the remote user's account will be locked if he makes 5 unsuccessful login attempts within 1 minute.
Lockout Duration	Type the time period for which the user account remains locked. After this time has elapsed, the account is automatically unlocked.

c In the Status section, enable this authentication server by turning on the **Enabled** toggle.

d (Optional) Configure secondary authentication.

Options	Description
Use this server for secondary authentication	(Optional) Specify whether to use the server as the second level of authentication.
Terminate Session if authentication fails	(Optional) Specify whether to end the VPN session when authentication fails.

e Click **Keep** to add this entry to the on-screen table.

4 (Optional) To enable client certification authentication, click **CHANGE CERTIFICATE**, then turn on the enablement toggle, select the CA certificate to use, and click **OK**.

What to do next

Add local users to the local authentication server so that they can connect with SSL VPN-Plus. See "Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server," on page 63.

Create an installation package containing the SSL Client so remote users can install it on their local systems. See "Add an SSL VPN-Plus Client Installation Package," on page 64

Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server

Use the Users screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to add accounts for your remote users to the local authentication server for the edge gateway's SSL VPN service.

Note If a local authentication server is not already configured, adding a user on the Users screen automatically adds a local authentication server with default values. You can then use the edit button on the Authentication screen to view and edit the default values. For information about using the Authentication screen, see "Configure an Authentication Service for SSL VPN-Plus on an Edge Gateway," on page 61.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Open the tenant portal and browse to the SSL-VPN Plus screen as described in "Navigate to the SSL-VPN Plus Screen in the Tenant Portal," on page 57.

Procedure

1 On the tenant portal's **SSL VPN-Plus** tab, click **Users**.

2 Click the **+** icon.

3 In the window that opens, configure the following options for the user.

Option	Description
User ID	Type the user ID.
Password	Type a password for the user.
Retype Password	Retype the password.
First name	(Optional) Type the first name of the user.
Last name	(Optional) Type the last name of the user.
Description	(Optional) Type a description for the user.
Enabled	Specify whether this user is enabled or disabled.

Option	Description
Password never expires	(Optional) Specify whether to always keep the same password for this user.
Allow change password	(Optional) Specify whether to let the user change the password.
Change password on next login	(Optional) Specify whether you want this user to change the password the next time the user logs in.

4. Click **Keep** to add this entry to the on-screen table.
5. Repeat the steps to add additional users.

What to do next

Add local users to the local authentication server so that they can connect with SSL VPN-Plus. See "Add SSL VPN-Plus Users to the Local SSL VPN-Plus Authentication Server," on page 63.

Create an installation package containing the SSL Client so the remote users can install it on their local systems. See "Add an SSL VPN-Plus Client Installation Package," on page 64

Add an SSL VPN-Plus Client Installation Package

Use the Installation Packages screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to create named installation packages of the SSL VPN-Plus client for the remote users.

Adding an SSL VPN-Plus client installation package to the edge gateway provides the capability for prompting new users to download and install the client package when they log in to use the VPN connection for the first time. When added, these client installation packages are then downloadable from the FQDN of the edge gateway's public interface.

You can create installation packages that run on Windows, Linux, and Mac operating systems. If you require different installation parameters per SSL VPN client, create an installation package for each configuration.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Open the tenant portal and browse to the SSL-VPN Plus screen as described in "Navigate to the SSL-VPN Plus Screen in the Tenant Portal," on page 57.

Procedure

1. On the tenant portal's **SSL VPN-Plus** tab, click **Installation Packages**.
2. Click the **+** icon.
3. In the window that opens, configure the following options.

Option	Description
Profile Name	Type a profile name for this installation package. This name is displayed to the remote user to identify this SSL VPN connection to the edge gateway.
Gateway	Type the IP address or FQDN of the edge gateway's public interface. This IP address or FQDN is bound to the SSL VPN client. When the client is installed on the remote user's local system, this IP address or FQDN is displayed on that SSL VPN client. To bind additional edge gateway uplink interfaces to this SSL VPN client, use the + icon to add rows and type in their interface IP addresses or FQDNs and ports.

Option	Description
Port	(Optional) To modify the port value from the displayed default, double-click the value and type in a new one.
Windows **Linux** **Mac**	Select the operating systems for which you want to provide installation packages. By default, the system creates an installation package for the Windows operating system. Select **Linux** or **Mac** to create an installation package for installing the client on those operating systems.
Description	(Optional) Type a description for the user.
Enabled	Specify whether this package is enabled or disabled.

4 Select the following options as required for your organization's needs.

These options apply to the Windows client.

Option	Description
Start client on logon	Starts the SSL VPN client when the remote user logs on to their local system.
Allow remember password	Enables the client to remember the user's password.
Enable silent mode installation	Hides installation commands from remote users.
Hide SSL client network adapter	Hides the VMware SSL VPN-Plus Adapter, which is installed on the remote user's computer along with the SSL VPN client installation package.
Hide client system tray icon	Hides the SSL VPN tray icon which indicates whether the VPN connection is active or not.
Create desktop icon	Creates an icon to invoke the SSL client on the user's desktop.
Enable silent mode operation	Hides the pop-up that indicates that installation is complete.
Server security certificate validation	The SSL VPN client validates the SSL VPN server certificate before establishing the secure connection.

5 Click **Keep** to add the entry to the on-screen table.

What to do next

Edit the client configuration. See "Edit SSL VPN-Plus Client Configuration," on page 65.

Edit SSL VPN-Plus Client Configuration

Use the Client Configuration screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to customize the way the SSL VPN client tunnel responds when the remote user logs in to SSL VPN.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Open the tenant portal and browse to the SSL-VPN Plus screen as described in "Navigate to the SSL-VPN Plus Screen in the Tenant Portal," on page 57.

Procedure

1 On the tenant portal's **SSL VPN-Plus** tab, click **Client Configuration**.

2 Select the **Tunneling mode**.

- In split tunnel mode, only the VPN traffic flows through the edge gateway.

- In full tunnel mode, the edge gateway becomes the remote user's default gateway and all traffic (VPN, local, and Internet) flows through the edge gateway.

3 If you select full tunnel mode, type the IP address for the default gateway used by the remote users' clients, and optionally select whether to exclude local subnet traffic from flowing through the VPN tunnel

4 (Optional) Optionally disable auto reconnect to have the SSL VPN client automatically reconnect users when they get disconnected.

   Enable auto reconnect is enabled by default.

5 (Optional) Optionally enable the ability for the client to notify remote users when a client upgrade is available.

   This option is disabled by default. If you enable this option, remote users can choose to install the upgrade.

6 Click **Save changes**.

Customize the General SSL VPN-Plus Settings for an Edge Gateway

By default, the system sets some SSL VPN-Plus settings on an edge gateway in your vCloud Director environment. You can use the General Settings screen on the vCloud Director tenant portal's **SSL VPN-Plus** tab to customize these settings.

Prerequisites

Open the tenant portal and browse to the SSL-VPN Plus screen as described in "Navigate to the SSL-VPN Plus Screen in the Tenant Portal," on page 57.

Procedure

1 On the tenant portal's **SSL VPN-Plus** tab, click **General Settings**.

2 Modify the following options as required for your organization's needs.

Option	Description
Prevent multiple logon using same username	Turn on to restrict a remote user to having only one active login session under his or her user name.
Compression	Turn on to enable TCP-based intelligent data compression and improve data transfer speed.
Enable Logging	Turn on to maintain a log of the traffic that passes through the SSL VPN gateway. Logging is enabled by default.
Force virtual keyboard	Turn on to require remote users to use a virtual (on-screen) keyboard only to enter login information.
Randomize keys of virtual keyboard	Turn on to have the virtual keyboard use a randomized key layout.
Session idle timeout	Type a time in minutes. If there is no activity on a user's session for the specified time period, the system disconnects the user's session. The system default is 10 minutes.
User notification	Type a message to be displayed to remote users after they log in.
Enable public URL access	Turn on to allow remote users to access sites that are not explicitly configured by you for remote user access.
Enable forced timeout	Turn on to have the system disconnect remote users after the time period specified in the **Forced timeout** field is over.
Forced timeout	This field is displayed when **Enable forced timeout** toggle is turned on. Type the timeout period in minutes.

3 Click **Save changes** to apply the updated settings to the system.

Configure IPsec VPN Using the Tenant Portal

The edge gateways in a vCloud Director environment support site-to-site Internet Protocol Security (IPsec) to secure VPN tunnels between organization virtual datacenter networks or between an organization virtual datacenter network and an external IP address. If the edge gateway for your organization virtual datacenter has been converted to an advanced edge gateway, you can use the tenant portal's IPsec VPN screen to configure the IPsec VPN service on that edge gateway.

Setting up an IPsec VPN connection from a remote network to your organization virtual datacenter is the most common scenario. The NSX software provides an edge gateway's IPsec VPN capabilities, including support for certificate authentication, preshared key mode, and IP unicast traffic between itself and remote VPN routers. You can also configure multiple subnets to connect through IPsec tunnels to the internal network behind an edge gateway. When you configure multiple subnets to connect through IPsec tunnels to the internal network, those subnets and the internal network behind the edge gateway must not have address ranges that overlap.

Note If the local and remote peer across an IPsec tunnel have overlapping IP addresses, traffic forwarding across the tunnel might not be consistent depending on whether local connected routes and auto-plumbed routes exist.

The following IPsec VPN algorithms are supported:

- AES (AES128-CBC)
- AES256 (AES265-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Diffie-Hellman group 2)
- DH-5 (Diffie-Hellman group 5)
- DH-14 (Diffie-Hellman group 14)

Note Dynamic routing protocols are not supported with IPsec VPN. When you configure an IPsec VPN tunnel between an organization virtual datacenter's edge gateway and a physical gateway VPN at a remote site, you cannot configure dynamic routingfor that connection.The IP address of that remote site cannot be learned by dynamic routing on the edge gateway's uplink.

As described in the IPSec VPN Overview topic in the *NSX Administration Guide*, the maximum number of tunnels supported on an edge gateway is determined by its configured size: compact, large, x-large, quad large. You can view the size of your edge gateway by logging in to the vCloud Director Web console, navigating to the edge gateway, and using the **Properties** action to view the edge gateway's configuration. See the *vCloud Director Administrator's Guide* for information about using the vCloud Director Web console.

Configuring IPsec VPN on an edge gateway is a multi-step process.

Note If a firewall is between the tunnel endpoints, after you configure the IPsec VPN service, update the firewall rules to allow the following IP protocols and UDP ports:

- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)
- UDP Port 500 (IKE)
- UDP Port 4500

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Navigate to the IPsec VPN Screen in the Tenant Portal on page 68

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can navigate to the vCloud Director tenant portal's IPsec VPN screen to begin configuring the IPsec VPN service for that edge gateway.

2 Configure the IPsec VPN Site Connections for the Edge Gateway on page 69

Use the IPsec VPN Sites screen in the vCloud Director tenant portal to configure settings needed to create an IPsec VPN connection between your organization virtual datacenter and another site using the edge gateway's IPsec VPN capabilities.

3 Enable the IPsec VPN Service on an Edge Gateway on page 71

When at least one IPsec VPN connection is configured, you can enable the IPsec VPN service on the edge gateway using the vCloud Director tenant portal.

4 Specify Global IPsec VPN Settings on page 72

Use the Global Configuration screen in the vCloud Director tenant portal to configure IPsec VPN authentication settings at an edge gateway level. On this screen, you can set a global pre-shared key and enable certification authentication.

Navigate to the IPsec VPN Screen in the Tenant Portal

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can navigate to the vCloud Director tenant portal's IPsec VPN screen to begin configuring the IPsec VPN service for that edge gateway.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

a Log in to the vCloud Director Web console and navigate to the edge gateway.

b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **VPN > IPsec VPN**.

What to do next

Use the **IPsec VPN Sites** screen to configure an IPsec VPN connection. At least one connection must be configured before you can enable the IPsec VPN service on the edge gateway. See "Configure the IPsec VPN Site Connections for the Edge Gateway," on page 69.

Configure the IPsec VPN Site Connections for the Edge Gateway

Use the IPsec VPN Sites screen in the vCloud Director tenant portal to configure settings needed to create an IPsec VPN connection between your organization virtual datacenter and another site using the edge gateway's IPsec VPN capabilities.

When you configure an IPsec VPN connection between sites, you configure the connection from the point of view of your current location. Setting up the connection requires that you understand the concepts in the context of the vCloud Director environment so that you configure the VPN connection correctly.

- The local and peer subnets specify the networks to which the VPN connects. When you specify these subnets in the configurations for IPsec VPN sites, enter a network range and not a specific IP address. Use CIDR format, such as **`192.168.99.0/24`**.
- The peer ID is an identifier that uniquely identifies the remote device that terminates the VPN connection, typically its public IP address. For peers using certificate authentication, this ID must be the distinguished name set in the peer's certificate. For PSK peers, this ID can be any string. An NSX best practice is to use the remote device's public IP address or FQDN as the peer ID. If the peer IP address is from another organization virtual datacenter network, you enter the peer’s native IP address. If NAT is configured for the peer, you enter the peer's private IP address.
- The peer endpoint specifies the public IP address of the remote device to which you are connecting. The peer endpoint might be a different address from the peer ID if the peer's gateway is not directly accessible from the Internet, but connects through another device. If NAT is configured for the peer, you enter the public IP address that the devices uses for NAT.
- The local ID specifies the public IP address of the organization virtual datacenter's edge gateway. You can enter an IP address or hostname in conjunction with the edge gateway's firewall.
- The local endpoint specifies the network in your organization virtual datacenter on which the edge gateway transmits. Typically the edge gateway's external network is the local endpoint.

Prerequisites

Verify you have completed the steps described in “Configure IPsec VPN Using the Tenant Portal,” on page 67 and in “Navigate to the IPsec VPN Screen in the Tenant Portal,” on page 68.

If you intend to use a global certificate as the authentication method, verify that certificate authentication is enabled on the Global Configuration screen. See “Specify Global IPsec VPN Settings,” on page 72 for details.

Procedure

1 On the tenant portal's **IPsec VPN** tab, click **IPsec VPN Sites**.

2 Click the **+** icon.

3 In the window that opens, configure the following options for the IPsec VPN connection.

Option	Description
Enabled	Toggle on to enable this connection between the two VPN endpoints.
Enable perfect forward secrecy (PFS)	Toggle on to have the system generate unique public keys for all IPsec VPN sessions your users initiate. Enabling PFS ensures that the system does not create a link between the edge gateway's private key and each session key. The compromise of a session key will not affect data other than that exchanged in the specific session protected by that particular key. Compromise of the server's private key cannot be used to decrypt archived sessions or future sessions. When PFS is enabled, IPsec VPN connections to this edge gateway experience a slight processing overhead. IMPORTANT The unique session keys must not be used to derive any additional keys. Additionally, both sides of the IPsec VPN tunnel must support PFS for it to work.
Name	(Optional) Enter a name for this connection.
Local Id	Type the external IP address of the edge gateway instance, which is the public IP address of the edge gateway. This IP address will be the one used for the peer Id in the IPsec VPN configuration on the remote site.
Local Endpoint	Type the network that is the local endpoint for this connection. The local endpoint specifies the network in your organization virtual datacenter on which the edge gateway transmits. Typically, the external network is the local endpoint. NOTE If you are adding an IP-to-IP tunnel using a pre-shared key, the local Id and local endpoint IP can be the same.
Local Subnets	Type the networks to share between the sites. Use a comma separator to type multiple subnets. NOTE Enter a network range (not a specific IP address) by entering the IP address using CIDR format; for example, `192.168.99.0/24`.
Peer Id	Type a peer ID to uniquely identify the peer site. The peer ID is an identifier that uniquely identifies the remote device that terminates the VPN connection, typically its public IP address. For peers using certificate authentication, this ID must be the distinguished name in the peer's certificate. For PSK peers, this ID can be any string. An NSX best practice is to use the remote device's public IP address or FQDN as the peer ID. If the peer IP address is from another organization virtual datacenter network, you enter the peer’s native IP address. If NAT is configured for the peer, you enter the peer's private IP address.
Peer Endpoint	Type the IP address or FQDN of the peer site, which is the public-facing address of the remote device to which you are connecting. NOTE When NAT is configured for the peer, enter the public IP address that the device uses for NAT.
Peer Subnets	Enter the remote network to which the VPN connects. Use a comma separator to type multiple subnets. NOTE Enter a network range (not a specific IP address) by entering the IP address using CIDR format; for example, `192.168.99.0/24`.
Encryption Algorithm	Select the encryption type from the drop-down list. NOTE The encryption type you select must match the encryption type configured on the remote site VPN device.

Option	Description
Authentication	Select one of the following options: ■ **PSK** (Pre Shared Key) specifies that the secret key shared between the edge gateway and the peer site is to be used for authentication. ■ **Certificate** specifies that the certificate defined at the global level is to be used for authentication. This option is not available unless you have configured the global certificate on the **IPsec VPN** tab's Global Configuration screen.
Change Shared Key	(Optional) When you are updating an existing connection's settings, you can turn on this toggle to make the **Pre-Shared Key** field available so that you can update the shared key.
Pre-Shared Key	If you selected **PSK** as the authentication type, type an alphanumeric string. The secret key can be a string with a maximum length of 128 bytes. NOTE The shared key must match the key that is configured on the remote site VPN device. IMPORTANT A best practice is to configure a shared key when anonymous sites will connect to the VPN service.
Display Shared Key	(Optional) Toggle this on to make the shared key visible in the screen.
Diffie-Hellman Group	Select the cryptography scheme that will allow the peer site and this edge gateway to establish a shared secret over an insecure communications channel. NOTE The Diffie-Hellman Group must match what is configured on the remote site VPN device.
Extension	(Optional) Type one of the following options: ■ `securelocaltrafficbyip=`*IPAddress* to re-direct the edge gateway's local traffic over the IPsec VPN tunnel. This is the default value. ■ `passthroughSubnets=`*PeerSubnetIPAddress* to support overlapping subnets.

4 Click**Keep** to add the entry to the on-screen table.

5 Click **Save changes**.

The save operation can take a minute to complete.

What to do next

Configure the connection for the remote site. You must configure the IPsec VPN connection on both sides of the connection: your organization virtual datacenter and the peer site.

Enable the IPsec VPN service on this edge gateway. When at least one IPsec VPN connection is configured, you can enable the service. See "Enable the IPsec VPN Service on an Edge Gateway," on page 71.

Enable the IPsec VPN Service on an Edge Gateway

When at least one IPsec VPN connection is configured, you can enable the IPsec VPN service on the edge gateway using the vCloud Director tenant portal.

Prerequisites

Verify that at least one IPsec VPN connection is configured for this edge gateway. See the steps described in "Configure the IPsec VPN Site Connections for the Edge Gateway," on page 69.

Open the tenant portal and navigate to the IPsec VPN screen. See "Navigate to the IPsec VPN Screen in the Tenant Portal," on page 68.

Procedure

1 On the tenant portal's **IPsec VPN** tab, click **Activation Status**.

2 Turn on the **IPsec VPN Service Status** toggle.

3 Click **Save changes**.

The edge gateway's IPsec VPN service is active.

Specify Global IPsec VPN Settings

Use the Global Configuration screen in the vCloud Director tenant portal to configure IPsec VPN authentication settings at an edge gateway level. On this screen, you can set a global pre-shared key and enable certification authentication.

A global pre-shared key is used for those sites whose peer endpoint is set to **any**.

Prerequisites

If you intend to enable certificate authentication, verify you have at least one service certificate and corresponding CA-signed certificates in the tenant portal's Certificates screen. Self-signed certificates cannot be used for IPsec VPNs. See "Add a Service Certificate to the Edge Gateway," on page 27.

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Navigate to **VPN > IPsec VPN > Global Configuration**

3 (Optional) Set a global pre-shared key:

   a Turn on the **Change Shared Key** toggle.

   b Type a pre-shared key.

   c (Optional) Optionally turn on the **Display Shared Key** toggle to make the pre-shared key visible.

   d Click **Save changes**.

4 Configure certification authentication:

   a Turn on the **Enable Certification Authentication** toggle.

   b Select the appropriate service certificate, CA certificates, and CRLs.

   c Click **Save changes**.

What to do next

You can optionally enable logging for the edge gateway's IPsec VPN service. See Chapter 11, "Statistics and Logs in the vCloud Director Tenant Portal," on page 89.

Configure L2 VPN Using the Tenant Portal

The edge gateways in a vCloud Director environment support L2 VPN, which allows extension of your organization virtual datacenter by allowing virtual machines to retain network connectivity while retaining the same IP address across geographical boundaries. If the edge gateway for your organization virtual datacenter has been converted to an advanced edge gateway, you can use the tenant portal's L2 screen to configure the L2 VPN service on that edge gateway.

The NSX software provides an edge gateway's L2 VPN capabilities. L2 VPN allows you to configure a tunnel between two sites. Virtual machines remain on the same subnet in spite of being moved between these sites, which enables you to extend your organization virtual datacenter by stretching its network using L2 VPN. An edge gateway at one site can provide all services to virtual machines on the other site.

To create the L2 VPN tunnel, you configure an L2 VPN server and L2 VPN client. As described in the NSX Administration Guide, the L2 VPN server is the destination edge gateway and the L2 VPN client is the source edge gateway. After configuring the L2 VPN settings on each edge gateway, you must then enable the L2 VPN service on both the server and the client.

Note A routed organization virtual datacenter network created as a subinterface must exist on the edge gateways. See the *vCloud Director Administrator's Guide* for the steps on creating an external routed organization virtual datacenter network.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Navigate to the L2 VPN Screen in the Tenant Portal

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can navigate to the vCloud Director tenant portal's L2 VPN screen to begin configuring the L2 VPN service for that edge gateway.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **VPN > L2 VPN**.

What to do next

Configure the L2 VPN server. See "Configure the Edge Gateway as an L2 VPN Server," on page 74.

Configure the Edge Gateway as an L2 VPN Server

The L2 VPN server is the destination NSX edge to which the L2 VPN client is going to connect.

As described in the *NSX Administration Guide*, you can connect multiple peer sites to this L2 VPN server.

Note Changing site configuration settings causes the edge gateway to disconnect and reconnect all existing connections.

You must have the server's listener IP, listener port, encryption algorithm, and at least one peer site configured before you can enable the L2 VPN service.

Prerequisites

Verify the edge gateway has a routed organization virtual datacenter network that is configured as a subinterface on the edge gateway. See the *vCloud Director Administrator's Guide* for the steps on creating an external routed organization virtual datacenter network.

Verify you have completed the steps described in "Navigate to the L2 VPN Screen in the Tenant Portal," on page 73.

If you want to bind a service certificate to the L2 VPN connection, verify that the server certificate has already been uploaded to the edge gateway. See "Add a Service Certificate to the Edge Gateway," on page 27.

Procedure

1 On the tenant portal's **L2 VPN** tab, for the L2 VPN mode, select **Server**.

2 Click the **Server Global** tab if it is not already selected.

3 Configure the L2 VPN server's global configuration details.

Option	Description
Listener IP	Type the primary or secondary IP address of an external interface of the edge gateway.
Listener Port	The default port for the L2 VPN service is 443. Edit the displayed value as appropriate for your organization's needs.
Encryption Algorithm	Select the encryption algorithm for the communication between the server and the client.
Service Certificate Details	Click **CHANGE SERVER CERTIFICATE** to select the certificate to be bound to the L2 VPN server. In the window that opens, turn on the **Validate Server Certificate** toggle, select a server certificate from the list, and click **OK**.

4 Configure the peer sites by clicking the **Server Sites** tab.

5 Click the **+** icon.

6 In the window that opens, configure the following options for an L2 VPN peer site.

Option	Description
Enabled	Toggle on to enable this peer site.
Name	Type a unique name for this peer site.
Description	(Optional) Type a description.
User Id **Password** **Confirm Password**	Type the user name and password with which the peer site is to be authenticated. User credentials on the peer site should be the same as those on the client side.

Option	Description
Stretched Interfaces	Select the subinterfaces to be stretched with the client. The subinterfaces available to select are those organization virtual datacenter networks configured as subinterfaces on the edge gateway.
Egress Optimization Gateway Address	(Optional) If the default gateway for virtual machines is the same across the two sites, type the gateway IP addresses of the subinterfaces for which you want the traffic locally routed or blocked over the L2 VPN tunnel.

7 Click**Keep** to add the entry to the on-screen table.

8 Click **Save changes**.

The save operation can take a minute to complete.

What to do next

Enable the L2 VPN service on this edge gateway. See "Enable the L2 VPN Service on an Edge Gateway," on page 76.

Configure the Edge Gateway as an L2 VPN Client

The L2 VPN client is the source NSX edge that initiates communication with the destination NSX edge, the L2 VPN server.

Prerequisites

Verify you have completed the steps described "Navigate to the L2 VPN Screen in the Tenant Portal," on page 73.

If this L2 VPN client is connecting with an L2 VPN server that uses a server certificate, verify that the corresponding CA certificate is uploaded to the edge gateway to enable server certificate validation for this L2 VPN client. See "Add a CA Certificate to the Edge Gateway for SSL Certificate Trust Verification," on page 25.

Procedure

1 On the tenant portal's **L2 VPN** tab, for the L2 VPN mode, select **Client**.

2 Click the **Client Global** tab if it is not already selected.

3 Configure the L2 VPN client's global configuration details.

Option	Description
Server Address	Type the IP address of the L2 VPN server to which this client is to be connected.
Server Port	Type the L2 VPN server's port to which the client should connect. The default port is 443.
Encryption Algorithm	Select the encryption algorithm for communicating with the server.
Stretched Interfaces	Select the subinterfaces to be stretched to the server. The subinterfaces available to select are those organization virtual datacenter networks configured as subinterfaces on the edge gateway.
Egress Optimization Gateway Address	(Optional) If the default gateway for virtual machines is the same across the two sites, type the gateway IP addresses of the subinterfaces or the IP addresses to which traffic should not flow over the tunnel.
User Id **Password** **Confirm Password**	Type the user credentials for authentication at the server.

4 Click **Save changes**.

The save operation can take a minute to complete.

5 (Optional) To configure advanced options, click the **Client Advanced** tab.

6 If this L2 VPN client edge does not have direct access to the Internet and needs to reach the L2 VPN server edge using a proxy server, specify the proxy settings.

Option	Description
Enable Secure Proxy	Select **Enable Secure Proxy**.
Address	Type the proxy server IP address.
Port	Type the proxy server's port.
User Name **Password**	Type the proxy server's authentication credentials.

7 To enable server certification validation, click **CHANGE CA CERTIFICATE** and select the appropriate CA certificate.

8 Click **Save changes**.

The save operation can take a minute to complete.

What to do next

If it is not already enabled, enable the L2 VPN service on this edge gateway. See "Enable the L2 VPN Service on an Edge Gateway," on page 76.

Enable the L2 VPN Service on an Edge Gateway

When the required L2 VPN settings are configured, you can enable the L2 VPN service on the edge gateway, using the vCloud Director tenant portal.

NOTE If HA is already configured on this edge gateway, ensure the edge gateway has more than one internal interface configured on it. If only a single interface exists and that has already been used by the HA capability, the L2 VPN configuration on the same internal interface will fail.

Prerequisites

If this edge gateway is an L2 VPN server, the destination NSX edge, verify that the required L2 VPN server settings and at least one L2 VPN peer site are configured. See the steps described in "Configure the Edge Gateway as an L2 VPN Server," on page 74.

If this edge gateway is an L2 VPN client, the source NSX edge, verify that the L2 VPN client settings are configured. See the steps described in "Configure the Edge Gateway as an L2 VPN Client," on page 75.

Open the tenant portal and navigate to the L2 VPN screen. See "Navigate to the L2 VPN Screen in the Tenant Portal," on page 73.

Procedure

1 On the tenant portal's **L2 VPN** tab, turn on the **Enable** toggle.

2 Click **Save changes**.

The edge gateway's L2 VPN service is active.

What to do next

Create NAT or firewall rules on the Internet-facing firewall side to enable the L2 VPN server to connect to the L2 VPN client.

Remove the L2 VPN Service Configuration from an Edge Gateway

If the edge gateway for your organization virtual datacenter has been converted to an advanced edge gateway, you can use the tenant portal's L2 VPN screen to remove the edge gateway's existing L2 VPN service configuration. This action also disables the L2 VPN service on the edge gateway.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Navigate to the tenant portal's L2 VPN screen. See "Navigate to the L2 VPN Screen in the Tenant Portal," on page 73.

Procedure

1 Scroll to the bottom of the tenant portal's L2 VPN screen and click **DELETE CONFIGURATION**.

2 Confirm the deletion in the pop-up window.

The L2 VPN service is disabled and the configuration details are removed from the edge gateway.

Managing Edge Gateway DHCP Using the Tenant Portal 9

You configure your edge gateways in your vCloud Director environment to provide Dynamic Host Configuration Protocol (DHCP) services to virtual machines connected to the associated organization virtual datacenter networks. If the edge gateway has been converted to an advanced edge gateway, you can use the vCloud Director tenant portal to configure DHCP services for that edge gateway.

As described in the NSX documentation, An NSX edge gateway capabilities include IP address pooling, one-to-one static IP address allocation, and external DNS server configuration. Static IP address binding is based on the managed object ID and interface ID of the requesting client virtual machine.

The DHCP service for an NSX edge gateway:

- Listens on the edge gateway's internal interface for DHCP discovery.
- Uses the IP address of the edge gateway's internal interface as the default gateway address for all clients.
- Uses the broadcast and subnet mask values of the internal interface for the container network.

In the following situations, you must restart the DHCP service on the client virtual machines that have the DHCP-assigned IP addresses:

- You changed or deleted a DHCP pool, default gateway, or DNS server.
- You changed the internal IP address of the edge gateway instance.

NOTE If the DNS settings on a DHCP-enabled edge gateway are changed, the edge gateway might stop providing DHCP services. If this situation occurs, use the **DHCP Service Status** toggle on the DHCP Pools screen to disable and then reenable DHCP on that edge gateway. See "Add a DHCP IP Pool," on page 80.

This chapter includes the following topics:

Add a DHCP IP Pool

Use the vCloud Director tenant portal to configure the IP pools needed for an advanced edge gateway's DHCP service. DHCP automates IP address assignment to virtual machines connected to organization virtual datacenter networks.

As described in the NSX documentation, the DHCP service requires a pool of IP addresses. An IP pool is a sequential range of IP addresses within the network. Virtual machines protected by the edge gateway that do not have an address binding are allocated an IP address from this pool. An IP pool's range cannot intersect one another, thus one IP address can belong to only one IP pool.

Note At least one DHCP IP pool must be configured to have the DHCP service status turned on.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **DHCP > Pools**.

3 If DHCP service is not currently enabled, turn on the **DHCP Service Status** toggle.

   Note Add at least one DHCP IP pool before saving changes after turning on the **DHCP Service Status** toggle. If no DHCP IP pools are listed on the screen and you turn on the **DHCP Service Status** toggle and save the changes, the screen re-displays with the toggle turned off.

4 Configure a DHCP IP pool and add its configuration to the on-screen table by clicking the **+** icon, specifying details for the DHCP pool in the dialog box, and then clicking **Keep**.

Setting	Description
IP Range	Type in a range of IP addresses
Domain Name	Domain name of the DNS server.
Auto Configure DNS	Enable this toggle to use the DNS service configuration for this IP pool's DNS binding. If enabled, the **Primary Name Server** and **Secondary Name Server** are set to **Auto**.
Primary Name Server	When you do not select **Auto Configure DNS**, type your primary DNS server's IP address of your primary DNS server. This IP address is used for hostname-to-IP address resolution.
Secondary Name Server	When you do not select **Auto Configure DNS**, type your secondary DNS server's IP address. This IP address is used for hostname-to-IP address resolution.
Default Gateway	Type the default gateway address. When you do not specify the default gateway IP address, the internal interface of the edge gateway instance is taken as the default gateway.
Subnet Mask	Type the edge gateway interface's subnet mask.

Setting	Description
Lease Never Expires	Enable this toggle to keep the IP addresses that are assigned out of this pool bound to their assigned virtual machines forever. When you select this option, **Lease Time** is set to infinite.
Lease Time (Seconds)	Length of time (in seconds) that the DHCP-assigned IP addresses are leased to the clients. The default lease time is one day (86400 seconds). NOTE You cannot specify a lease time when you select **Lease never expires**.

5 Click **Save changes**.

vCloud Director updates the edge gateway to provide DHCP services.

Add DHCP Bindings

If you have services running on a virtual machine (VM) and do not want the IP address to be changed, you can bind the VMs MAC address to the IP address. The IP address you bind must not overlap a DHCP IP pool.

Use the Bindings screen in the vCloud Director tenant portal to configure DHCP bindings for your advanced edge gateway.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

You have the MAC addresses for the VMs for which you want to set up bindings.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **DHCP > Bindings**.

3 Specify each binding and add it to the on-screen table by clicking the **+** icon, specifying details for the binding in the dialog box, and then clicking **Keep**.

Setting	Description
MAC Address	Type the MAC address of the VM that you want bound to the IP address.
Host Name	Type the host name you want set for that VM when the VM requests a DHCP lease.
IP Address	Type the IP address you want bound to the MAC address.
Subnet Mask	Type the edge gateway interface's subnet mask.
Domain Name	Type the domain name of the DNS server.
Auto Configure DNS	Enable this toggle to use the DNS service configuration for this DNS binding. If enabled, the **Primary Name Server** and **Secondary Name Server** are set to **Auto**.
Primary Name Server	When you do not select **Auto Configure DNS**, type your primary DNS server's IP address of your primary DNS server. This IP address is used for hostname-to-IP address resolution.

Setting	Description
Secondary Name Server	When you do not select **Auto Configure DNS**, type your secondary DNS server's IP address. This IP address is used for hostname-to-IP address resolution.
Default Gateway	Type the default gateway address. When you do not specify the default gateway IP address, the internal interface of the edge gateway instance is taken as the default gateway.
Lease Never Expires	Enable this toggle to keep the IP address bound to that MAC address forever. When you select this option, **Lease Time** is set to infinite.
Lease Time (Seconds)	Length of time (in seconds) that the DHCP-assigned IP addresses are leased to the clients. The default lease time is one day (86400 seconds). NOTE You cannot specify a lease time when you select **Lease never expires**.

4 Click **Save changes**.

Configuring DHCP Relay for Edge Gateways

The DHCP relay capability provided by NSX in your vCloud Director environment enables you to leverage your existing DHCP infrastructure from within your vCloud Director environment without any interruption to the IP address management in your existing DHCP infrastructure. DHCP messages are relayed from virtual machines to the designated DHCP servers in your physical DHCP infrastructure, which allows IP addresses controlled by the NSX software to continue to be in synch with IP addresses in the rest of your DHCP-controlled environments.

The edge gateway's DHCP relay configuration can list several DHCP servers. Requests are sent to all listed servers. While relaying the DHCP request from the VMs, the edge gateway adds a gateway IP address to the request. The external DHCP server uses this gateway address to match a pool and allocate an IP address for the request. The gateway address must belong to a subnet of the edge gateway's interface.

You can specify a different DHCP server for each edge gateway and can configure multiple DHCP servers on each edge gateway to provide support for multiple IP domains.

NOTE

- DHCP relay does not support overlapping IP address spaces.
- DHCP relay and DHCP service cannot run on the same vNIC at the same time. If a relay agent is configured on a vNIC, a DHCP pool cannot be configured on the subnets of that vNIC. See the *NSX Administration Guide* for details.

Specify an Edge Gateway's DHCP Relay Configuration Using the Tenant Portal

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the vCloud Director tenant portal to configure the edge gateway's DHCP relay capability. The NSX software in your vCloud Director environment provides the capability for the edge gateway to relay DHCP messages to DHCP servers external to your vCloud Director organization virtual datacenter.

As described in the *NSX Administration Guide*, the DHCP servers can be specified using an existing IP set, IP address block, domain, or a combination of all of these. DHCP messages are relayed to every specified DHCP server.

You must also configure at least one DHCP relay agent. A DHCP relay agent is an interface on the edge gateway from which the DHCP requests are relayed to the external DHCP servers.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

If you want to use an IP set to specify a DHCP server, verify that IP set exists as a grouping object available to the edge gateway. See "Create an IP Set for Use in Firewall Rules and DHCP Relay Configuration," on page 39.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 In the tenant portal, navigate to **DHCP** > **Relay**.

3 Use the on-screen fields to specify the DHCP servers by IP addresses, domain names, or IP sets.

   You select from existing IP sets using the **+** icon to browse the available IP sets.

4 Configure a DHCP relay agent and add its configuration to the on-screen table by clicking the **+** icon, selecting a vNIC and its gateway IP address, and then clicking **Keep**.

   By default, the Gateway IP Address matches the primary address of the selected vNIC. You can keep the default or select an alternate address if one is available on that vNIC.

5 Click **Save changes**.

Managing Network Address Translation Using the Tenant Portal 10

The NSX software in your vCloud Director environment enables the edge gateways to provide a network address translation (NAT) service. Using this capability reduces the number of public IP addresses that an organization must use, for economy and security purposes.

The edge gateway's NAT service provides the ability to assign a public address to a virtual machine or group of virtual machines in a private network. To enable your edge gateways to provide access to services running on privately addressed virtual machines in your organization virtual datacenter, you must configure NAT rules on the edge gateways. In the most common case, you associate a NAT service with an uplink interface on an edge gateway in your vCloud Director environment so that addresses on organization virtual datacenter networks are not exposed on the external network.

The NAT service configuration is separated into source NAT (SNAT) and destination NAT (DNAT) rules. When you configure an SNAT or a DNAT rule on an edge gateway in the vCloud Director environment, you always configure the rule from the perspective of your organization virtual datacenter. Specifically, that means you configure the rules in the following ways:

- SNAT: the traffic is traveling from a virtual machine on an internal network in your organization virtual datacenter (the source) through the Internet to the external network (the destination). The SNAT rule translates the source IP address of an organization virtual datacenter network's outgoing packets that are being sent to an external network or to another organization virtual datacenter network.
- DNAT: the traffic is traveling from the Internet (the source) to a virtual machine inside your organization virtual datacenter (the destination). A DNAT rule translates the IP address, and optionally the port, of packets received by an organization virtual datacenter network that are coming from an external network or from another organization virtual datacenter network.

You can configure NAT rules to create a private IP address space inside your organization virtual datacenter. This configuration provides the ability to port a private IP address space from one organization virtual datacenter to another. Configuring NAT rules allows you to use the same private IP addresses for your virtual machines in one organization virtual datacenter that were used in another.

The NAT rule capability in your vCloud Director environment supports:

- Creating subnets within the private IP address space
- Creating multiple private IP address spaces for an edge gateway

- Configuring multiple NAT rules on multiple edge gateway interfaces

IMPORTANT You must configure both firewall and NAT rules on an edge gateway for the virtual machines on an edge gateway network to be accessible. By default, edge gateways are deployed with firewall rules configured to deny all network traffic to and from the virtual machines on the edge gateway networks. Also, NAT is disabled by default on the edge gateways so that edge gateways are unable to translate the IP addresses of the incoming and outgoing traffic unless you configure NAT on the edge gateways. Attempting to ping a virtual machine on a network after configuring a NAT rule will fail unless you add a firewall rule to allow the corresponding traffic.

Add an SNAT or DNAT Rule Using the Tenant Portal

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the vCloud Director tenant portal to work with that edge gateway's NAT rules. You can create a source NAT (SNAT) rule to change the source IP address from a public to private IP address or the reverse. You can create a destination NAT (DNAT) rule to change the destination IP address from a public to private IP address or the reverse.

When creating NAT rules, you can specify the original and translated IP addresses by using the following formats:

- IP address; for example, 192.0.2.0
- IP address range; for example, 192.0.2.0-192.0.2.24
- IP address/subnet mask; for example, 192.0.2.0/24
- `any`

When you configure an SNAT or a DNAT rule on an edge gateway in the vCloud Director environment, you always configure the rule from the perspective of your organization virtual datacenter. A SNAT rule translates the source IP address of packets sent from an organization virtual datacenter network out to an external network or to another organization virtual datacenter network. A DNAT rule translates the IP address, and optionally the port, of packets received by an organization virtual datacenter network that are coming from an external network or from another organization virtual datacenter network.

Prerequisites

The public IP addresses must have been added to the edge gateway interface on which you want to add the rule. For DNAT rules, the original (public) IP address must have been added to the edge gateway interface and for SNAT rules, the translated (public) IP address must have been added to the interface.

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **NAT** to view the NAT screen.

3 Depending on which type of NAT rule you are creating, click **+ DNAT RULE** or **+ SNAT RULE**.

   The rule configuration dialog box displays.

4 Depending on which type of NAT rule you are creating, complete the following options:

Destination NAT (DNAT) (outside coming inside)

Option	Description
Applied On	Select the interface on which to apply the rule.
Original IP/Range	This address must be the public IP address of the edge gateway for which you are configuring the DNAT rule. Type the required IP address. In the packet being inspected, this IP address or range would be those that appear as the packet's destination IP address. These packet destination addresses are the ones translated by this DNAT rule.
Protocol	Select the protocol to which the rule applies. To apply this rule on all protocols, select **Any**.
Original Port/Range	(Optional) Select the port or port range that the incoming traffic uses on the edge gateway to connect to the internal network on which the virtual machines are connected. This selection is not available when the **Protocol** is set to **ICMP** or **Any**.
ICMP Type	When you select **ICMP** (an error reporting and a diagnostic utility used between devices to communicate error information) for **Protocol**, select the **ICMP Type** from the drop-down menu. ICMP messages are identified by the type field. By default, the ICMP type is set to any.
Translated IP/Range	Type the IP address or a range of IP addresses to which destination addresses on inbound packets will be translated. These addresses are the IP addresses of the one or more virtual machines for which you are configuring DNAT so that they can receive traffic from the external network.
Translated Port/Range	(Optional) Select the port or port range that inbound traffic is connecting to on the virtual machines on the internal network. These ports are the ones into which the DNAT rule is translating for the packets inbound to the virtual machines.
Description	(Optional) Type a description that helps identify what this rule is doing.
Enabled	Toggle on to enable this rule.
Enable logging	Toggle on to have the address translation performed by this rule logged.

Source NAT (SNAT) (inside going outside)

Option	Description
Applied On	Select the interface on which to apply the rule.
Original Source IP/Range	Type the original IP address or range of IP addresses to apply to this rule. These addresses are the IP addresses of one or more virtual machines for which you are configuring SNATrule so that they can send traffic to the external network.
Translated Source IP/Range	This address is always the public IP address of the gateway for which you are configuring the SNAT rule. Type the required IP address. Specifies the IP address to which source addresses (the virtual machines) on outbound packets are translated to when they send traffic to the external network.
Description	(Optional) Type a description that helps identify what this rule is doing.
Enabled	Toggle on to enable this rule.
Enable logging	Toggle on to have the address translation performed by this rule logged.

5 Click **Keep** to add the rule to the on-screen table.

6 Repeat the steps to configure additional rules.

7 When you are finished adding rules, click **Save changes** to save them to the system.

What to do next

Add corresponding edge gateway firewall rules for the SNAT or DNAT rules you just configured. See "Add an Edge Gateway Firewall Rule Using the Tenant Portal," on page 31.

Statistics and Logs in the vCloud Director Tenant Portal

11

If the edge gateway for your vCloud Director organization virtual datacenter has been converted to an advanced edge gateway, you can use the vCloud Director tenant portal to view statistics and logs for that edge gateway.

Statistics

You can use the tenant portal to view statistics by launching the tenant portal from the vCloud Director Web console using the **Edge Gateway Services** action on an advanced edge gateway. When the tenant portal is displayed, you can then click the **Statistics** tab to navigate to additional screens to view statistics for:

- Connections
- IPsec VPN
- L2 VPN

Tab	Description
Connections	The Connections screen provides operational visibility. The screen displays graphs for the traffic flowing through the interfaces of the selected edge gateway and connection statistics for the firewall and load balancer services. Select the period for which you want to view the statistics.
IPSEC VPN	The IPSEC VPN screen displays the IPsec VPN status and statistics, and status and statistics for each tunnel.
L2 VPN	The L2 VPN screen displays the L2 VPN status and statistics.

Logs

You can use the tenant portal to enable logging for the following individual capabilities of the advanced edge gateway. In addition to enabling logging for those features for which you want to collect log data, to complete the configuration to collect the enabled logs from the edge gateway, the Edge Settings screen must have a specified syslog server that is to receive the collected log data. When a syslog server is configured on the Edge Settings screen, you are able to access the logged data from that syslog server.

Navigation to Enable Logging Per Feature	Description
Edge Settings > EDIT SYSLOG SERVER	You can customize the syslog server for your edge gateway's networking-related logs for those services that have logging enabled. If the vCloud Director system administrator has configured a syslog server for the vCloud Director environment using the vCloud Director Web console's System Settings, the system uses that syslog server by default and its IP address is displayed on the tenant portal's Edge Settings screen.
NAT > + DNAT RULE, and turn on the **Enable logging** toggle.	Logs the address translation.
NAT > + SNAT RULE, and turn on the **Enable logging** toggle.	Logs the address translation.
Routing > Routing Configuration > Dynamic Routing Configuration, and turn on the **Enable logging** toggle.	Logs the dynamic routing activities. Use the **Log Level** drop-down to select the lowerbound of the message status level to log.
Load Balancer > Global Configuration, and turn on the **Enable logging** toggle.	Logs the traffic flow for the load balancer. Use the **Log Level** drop-down to select the lowerbound of the message status level to log.
VPN > IPSec VPN > Logging Settings, and turn on the **Enable logging** toggle.	Logs the traffic flow between the local subnet and peer subnet. Use the **Log Level** drop-down to select the lowerbound of the message status level to log.
SSL VPN-Plus > General Settings, and turn on the **Enable logging** toggle.	Maintains a log of the traffic passing through the SSL VPN gateway.
SSL VPN-Plus > Server Settings, and turn on the **Enable logging** toggle.	Logs the activities that occur on the SSL VPN server, for syslog. Use the **Log Level** drop-down to select the lowerbound of the message status level to log.

Enable SSH Command Line Access to an Edge Gateway 12

If the edge gateway for your organization virtual datacenter has been converted to an advanced edge gateway, you can use the tenant portal's Edge Settings screen to enable SSH command line access to the edge gateway.

Prerequisites

For the ability to use the vCloud Director tenant portal to work with an edge gateway's settings, the edge gateway must have already been converted to an advanced edge gateway using the **Convert to Advanced Gateway** action on the edge gateway in the vCloud Director Web console. See the *vCloud Director Administrator's Guide* for details.

Procedure

1 Launch the tenant portal using the following steps.

   a Log in to the vCloud Director Web console and navigate to the edge gateway.

   b Right-click the name of the edge gateway and click **Edge Gateway Services** in the context menu.

   The tenant portal opens in a new browser tab and displays the Edge Gateway screen for that edge gateway.

2 Click the **Edge Settings** tab.

3 Configure the SSH settings.

Option	Description
Username **Password** **Retype Password**	Type the credentials to use for SSH access to this edge gateway. By default, the SSH username is `admin`.
Password Expiry	Type the expiration period for the password, in days
Login Banner	Type the text to be displayed to users when they begin an SSH connection to the edge gateway.

4 Turn on the **Enabled** toggle.

What to do next

Configure the appropriate NAT or firewall rules to allow SSH access to this edge gateway.

Index