Site-to-Site VPN Tunnel Connection

A site-to-site VPN tunnel connects networks in different geographic locations. You can create site-to-site IPsec connections between two different Multicloud Defense Gateways or between a Multicloud Defense Gateway and a cloud service provider that complies with all relevant standards. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

Typically, the dynamic peer must be the one that initiates the connection as the other peer would not know the IP address of the dynamic peer. When the remote peer attempts to establish the connection, the other peer validates the connection using the preshared key, IKE settings, and IPsec configurations.

Because the VPN connection is established only after the remote peer initiates the connection, any outbound traffic that matches access control rules that allow traffic in the VPN tunnel will be dropped until that connection is established. This ensures that data does not leave your network without the appropriate encryption and VPN protection.

At this time, Multicloud Defense supports site-to-site VPN tunnel connections with the following platforms or products:

- AWS
- Azure
- GCP
- ASA device
- FTD device
- Extranet or a third party firewall

Prerequisites and Limitations for Site-to-Site VPN Tunnels

Supported VPN Tunnel Connection Endpoints

You can create a VPN tunnel connection with any of the following setups:

- Multicloud Defense Gateway to a Multicloud Defense Gateway.
- Multicloud Defense Gateway to a cloud service provider (AWS, Azure, GCP).
- Multicloud Defense Gateway to an ASA device hosted in Security Cloud Control.

Multicloud Defense Gateway Prerequisites and Limitations

You must have the following prerequisites completed prior to creating a VPN tunnel regardless of the type of device or platform involved:

- Multicloud Defense Gateway and Multicloud Defense Terraform Provider **must** be running version 24.04 or later.
- At least one cloud service provider or third party device must be already connected to Multicloud Defense.
- Your cloud service provider or third party device must be configured to allow and create VPN tunnel connections. See the service or platform documentation for more information.
- You must have at least **one** IPSec profile. This profile must be attached to the VPN tunnel connection.
- You **must** add the Service VPC or VNet to the gateway prior to deploying.
- The VPC and VNet must be deployed **without** Network Address Translation gateway on both sides.
- You **must** create at least one BGP profile. This profile must be attached to the gateway instance associated with the VPN tunnel connection. VPN tunnels can be more effective when paired with a BGP profile as the profile offers additional control over how traffic flows in your networks. See BGP Profile for more information.

Note When you create a BGP profile, the BGP profile must be enabled for traffic and same value to be used in the tunnel as in the BGP Profile

Be aware of the following limitations when creating a VPN tunnel connection:

- The Multicloud Defense Gateway you select **must** be an egress/east-west gateway.
- AWS and Azure gateways must be **8 core** instance type. 2-core and 4-core are not supported at this time.
- Enable AWS inventory for the region the gateway deploys to. Without this enabled, not all traffic flow is passed.
- Site-to-site VPN connections only support up to 10 VPN peers.
- VPCs and VNETs for either AWS or Azure environment must be created with a **single** availability zone. Multiple availability zones are not supported at this time.

- Site-to-site VPN tunnels **do not** support forward-proxy firewall rules at this time.
- Your bandwidth must be at least 800 Mbps.

Note If you disable or enable a gateway, you **must** delete the site-to-site connection associated with the gateway and recreate the VPN connection.

Limitations for VPN Tunnel Between Multicloud Defense and an ASA Device

Be aware of the following limitations when creating a VPN tunnel connection between the Multicloud Defense Gateway and an ASA device:

- When choosing the endpoints for the VPN tunnel, ensure at least one endpoint is an ASA device and the one endpoint is an Multicloud Defense Gateway (step 4-6).
- If you create a site-to-site VPN tunnel for a third-party or an on-premises device, the table of VPN connections only displays the status of the IPSec profile on Multicloud Defense's endpoint of the connection.
- Autoscaling is not currently supported.

For more information on VPN Tunnels to an ASA device that is hosted in Security Cloud Control, see ASA Site-to-Site VPN Configuration.

Note If you are using a third-party device or an on-premises management center, only the Multicloud Defense's side of the IPSEC status is displayed at this time.

Limitations for VPN Tunnel Between Multicloud Defense and an FTD Device

Be aware of the following limitations when creating a VPN tunnel connection between the Multicloud Defense Gateway and an FTD device:

- Both IPsec IKEv1 & IKEv2 protocols are supported.
- Automatic or manual pre-shared keys for authentication.
- IPv4 and IPv6. All combinations of inside and outside are supported.
- IPsec IKEv2 site-to-site VPN topologies provide configuration settings to comply with Security Certifications.
- Static and dynamic interfaces.
- Support for the dynamic IP address for the extranet device as an endpoint.

For more information on VPN Tunnels to an FTD device that is hosted in Security Cloud Control, see Configure Site-to-Site VPN for an FDM-Managed Device.

Enable VPN Within the Gateway

Use the following procedure to enable the VPN for a gateway in the Multicloud Defense Controller dashboard:

Before you begin

Before you can establish a VPN connection between two devices using Multicloud Defense, you must enable the gateway to utilize a BGP profile. See Prerequisites and Limitations for Site-to-Site VPN Tunnels, on page 2 for the complete list of pre-requisites for creating and deploying a gateway.

Note If you opt to use a BGP profile, the BGP profile is run over the IPSEC tunnel with the remote peer.

Procedure

Step 1 Navigate to **Infrastructure** > **Gateways** > **Gateways**.

Step 2 Click **Add Gateway** to create a new gateway or select an existing gateway and choose to **Edit** it in the Actions drop-down menu.

Step 3 When you create or edit the gateway, scroll to the bottom of the window and select a **BGP profile** from the drop-down menu when prompted.

Step 4 Locate the **VPN Connection** options under **Advanced Settings**. Check the **Enable VPN** option to opt into VPN tunnel connection.

Step 5 Expand the **BGP Profile** drop-down menu and select a profile that has already been created.

What to do next

Create a site-to-site tunnel connection.

Create a Site-to-Site VPN Connection

This procedure allows you to create a site-to-site VPN tunnel connection between your gateway and an ASA device, Azure, AWS, and GCP cloud service providers or even a third party firewall of your choice.

Note When entering the **virtual interface IP address**, we strongly recommend using an IP from the 169.254.xx/16 range, excluding the threat defense reserved range 169.254.1.x/24.

For the net mask, we recommend using /30; this allows you to only use two IP addresses for the endpoints of the virtual tunnel interface connection. For example, 169.254.100.1/30.

Use the following procedure to create an site-to-site VPN tunnel using the Multicloud Defense Controller dashboard:

Before you begin

You must have at least one IPSec profile already created prior to creating a VPN connection tunnel.

We **strongly** recommend creating a BGP profile and adding it to your Multicloud Defense Gateway before you create a VPN tunnel connection. See BGP Profile for more information.

Procedure

Step 1 Navigate to **Infrastructure** > **Network** > **VPN Connections**.

Step 2 Click **Create VPN Connection**.

Step 3 Enter a **Name** for the connection.

Step 4 Expand the **Device 1** drop-down menu to select a Multicloud Defense Gateway or manually enter a public IP address of a remote endpoint.

Step 5 Enter the **Device 1 Virtual Interface IP** address. Read the **Note** at the beginning of this procedure for guidance on how to optimize this field.

Step 6 Expand the **Device 2** drop-down menu to select your Multicloud Defense Gateway or manually enter a public IP address of a remote endpoint. Do not use the same device or gateway for both device 1 and device 2.

Step 7 Enter the **Device 2 Virtual Interface IP** address. Read the **Note** at the beginning of this procedure for guidance on how to optimize this field.

Step 8 Enter the **Authentication Value** for the tunnel. At this time, PreShared Key is the preferred authentication method.

Step 9 Expand the **IPSec Profile** drop-down menu to select a profile that has already been created.

Step 10 Click **Save**.

What to do next

View the connection status to review the statistics for incoming and outgoing bytes at both ends of the connection.

If you want to associate a BGP profile with your VPN tunnel connection, create a gateway or edit an existing one and add the desired BGP profile. Note that the IPSec profile of the VPN connection remains the primary profile used and the BGP profile is executed on top of the IPSEC tunnel with the remote peer.

Edit a Site-to-Site VPN Tunnel

Use the following procedure to edit an existing site-to-site VPN connection using the Multicloud Defense Controller dashboard:

Procedure

Step 1 Navigate to **Infrastructure** > **Network** > **VPN Connections**.

Step 2 Select a VPN connection so it is highlighted.

Step 3 In the **Actions** drop-down menu, select **Edit**.

Step 4 Modify any of the following information:

- Name.
- Device 1.
- Device 1 Virtual Interface IP.
- Device 2.
- Device 1 Virtual Interface IP.
- Authentication Value.
- IPSec profile selection.

Step 5 Click **Save**. You can **Cancel** at any time.

Clone a Site-2-Site VPN Tunnel Connection

Use the following procedure to clone a VPN Tunnel connection using the Multicloud Defense Controller dashboard:

Procedure

Step 1 Navigate to **Infrastructure** > **Network** > **VPN Connections**.

Step 2 Select a VPN connection so it is highlighted.

Step 3 In the **Actions** drop-down menu, select **Clone**.

Step 4 Enter a **Name** for the connection. It must be different from the connection that is being cloned.

Step 5 Modify any of the following information that is cloned:

- Device 1.
- Device 1 Virtual Interface IP.
- Device 2.
- Device 1 Virtual Interface IP.
- IPSec Profile selection.

Step 6 The Authentication type is cloned, but the key value for it is not. Enter the **Authentication Value** for the tunnel.

Step 7 Click **Save.**

Delete a VPN Tunnel Connection

Use the following procedure to delete a VPN Tunnel connection using the Multicloud Defense Controller dashboard:

Procedure

Step 1 Navigate to **Infrastructure** > **Network** > **VPN Connections**.

Step 2 Select a VPN connection so it is highlighted.

Step 3 In the **Actions** drop-down menu, select **Delete**.

Step 4 Confirm the deletion action and click **Delete**.

What to do next

We strongly recommend deleting any BGP profiles that you created for the VPN tunnel you just deleted.