



Gateway Profiles

A gateway profile is typically associated with the configuration of a network gateway by way of a device that connects different networks and routes traffic between them. Gateway profiles are used to manage the behavior and functionality of network gateways, ensuring efficient and secure communication between different parts of the network. These profiles generally include or apply to the following protective methods:

- Routing Policies
- Network Address Translation (NAT)
- Virtual Private Network (VPN) Settings
- Quality of Service (QoS)
- Authentication and Access Control

These profiles are generally applied to either a Multicloud Defense Gateway or a VPN tunnel that is associated with a gateway.

- [Packet Capture Profile, on page 1](#)
- [Log Forwarding Profile, on page 2](#)
- [Gateway Metrics Forwarding Profile, on page 3](#)
- [Network Time Protocol Profile, on page 5](#)
- [IPSec Profile, on page 5](#)
- [BGP Profile, on page 6](#)

Packet Capture Profile

Packet Capture (PCAP) captures data packets that are transmitted across the network, allowing for detailed analysis of the network traffic. PCAP can be used to monitor network traffic for signs of malicious activity by analyzing the captured packets, security systems can detect and respond to potential threats in real-time and allows you to reconstruct the sequence of events leading up to the incident and identify the source and nature of the attack. This information can be helpful in diagnosing a timeline or to troubleshoot events such as connectivity problems, latency, and packet loss.

Create a Packet Capture Profile

Use the following procedure to create a pack capture profile:

-
- Step 1** Navigate to **Manage > Profiles > Packet Capture**.
- Step 2** Click **Create**.
- Step 3** Specify a unique **Name**.
- Step 4** (Optional) Enter a **Description**. This may help differentiate between other profiles with a similar name.
- Step 5** Specify a **CSP Account**.
- Step 6** The type of cloud service provider may determine the parameters for the storage bucket. Be aware of the following requirements per cloud service provider:
- **AWS** - S3 Bucket.
 - **Azure** - Storage Account Name, Blog Container , and Storage Access Key.
 - **GCP** - Storage Bucket.
- Step 7** Click **Save**.
-

What to do next

Attach the profile to a policy rule set. See [Rule Sets and Rule Set Groups](#) for more information.

Log Forwarding Profile

A log forwarding profile allows you to send a collection of gateway, VPC, and VNet logs to a third party. The communication between Multicloud Defense and the third party of your choice contains the log type that needs to be forwarded and the destination server profiles the logs will be sent to. You can have a single profile, or a profile group that sends logs to multiple endpoints simultaneously.

Note that this profile does not include metrics. See [Gateway Metrics Forwarding Profile, on page 3](#) for more information about forwarding log metrics.

Create a Standalone Log Forwarding Profile

Use the following procedure to create a standalone profile to forward logs with:

- Step 1** Navigate to **Manager > Profiles > Log Forwarding**.
- Step 2** Click **Create**.
- Step 3** Enter a unique **Profile Name**.
- Step 4** (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.
- Step 5** Expand the **Type** drop-down menu and select **Standalone**.
- Step 6** Expand the **Destination** drop-down menu and select the third-party application to send logs to.
- Step 7** Based on the type of destination you select in step 6, enter the appropriate information when prompted to secure the final endpoint where the logs are forwarded to. Note that not all options are available based on the type of destination.

Step 8 Click **Save**.

What to do next

Attach the profile to a policy rule set. See [Rule Sets and Rule Set Groups](#) for more information.

Create a Log Forwarding Group

Use the following procedure to create a profile group to forward logs with:

Before you begin

- You must have at least one third party application to forward the metric to prior to creating this profile.
 - You must have at least two standalone metrics forwarding profiles already created. See [Create a Standalone Log Forwarding Profile, on page 2](#) for more information.
-

Step 1 Navigate to **Manager > Profiles > Log Forwarding**.

Step 2 Click **Create**.

Step 3 Enter a unique **Profile Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.

Step 5 Expand the **Type** drop-down menu and select **Group**.

Step 6 Under **Group Details**, click **Add** for every new row you need to add to the profile.

Step 7 Expand the drop-down menus for each row to select a profile to add to the group. If you want to remove a profile at any point prior to saving, select the profile's checkbox so it is highlighted and select **Remove**.

Step 8 Click **Save**.

What to do next

Attach the profile to a policy rule set. See [Rule Sets and Rule Set Groups](#) for more information.

Gateway Metrics Forwarding Profile

This profile is intended to forward gateway metrics generated by the Multicloud Defense Gateway for data monitoring and analysis. While the metrics are generated by the gateway, it is the Multicloud Defense Controller that forwards the metrics to the third party analysis application. With this forwarding profile you are able to monitor, analyze, and organize your gateway metrics without logging into Multicloud Defense. Use this information to gauge the performance and behavior of your gateway environment; you can also utilize this information for environmental troubleshooting.



Note As of Multicloud Defense Controller version 23.09, only Datadog is supported as a third party analytics application.

For the majority of analytics applications available, for example, Datadog, you must already be an authorized user to access the tool's APIs and rendered data.

Create a Standalone Metrics Forwarding Profile

Use the following procedure to create a standalone profile and forward metrics to be processed by a third party:

Before you begin

You must have at least one third party application to forward the metric to prior to creating this profile.

-
- Step 1** Navigate to **Manager > Profiles > Metrics Forwarding**.
 - Step 2** Click **Create**.
 - Step 3** Enter a unique profile **Name**.
 - Step 4** (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.
 - Step 5** Expand the **Type** drop-down menu and select **Standalone**.
 - Step 6** Expand the **Destination** drop-down menu and select the third-party application to process and analyze the metrics.
 - Step 7** Enter the **Endpoint** to be used as the endpoint location for the metrics.
 - Step 8** Click **Save**.

If you select Datadog as your analytics application, the **Endpoint** is filled in by default with an HTTPs webhook. This entry, if defaulted, can be modified prior to saving the profile.

What to do next

Attach the profile to a policy rule set. See [Rule Sets and Rule Set Groups](#) for more information.

Create a Group Metrics Forwarding Profile

In this process, you create a profile and then assign it to a specific gateway. A group profile combines up to five standalone metrics forwarding profile that can then be assigned to a single gateway. Use the following procedure to create a grouped metrics forward profile:

Before you begin

- You must have at least one third party application to forward the metric to prior to creating this profile.
- You must have at least two standalone metrics forwarding profiles already created. See [Create a Standalone Metrics Forwarding Profile, on page 4](#) for more information.

-
- Step 1** In the Multicloud Defense Controller interface navigate to **Manager > Profiles > Metrics Forwarding**.
 - Step 2** Click **Create**.
 - Step 3** Enter a unique **Profile Name**
 - Step 4** (Optional) Enter a **Description**. This may help differentiate between profiles with a similar name.

- Step 5** Expand the **Type** drop-down menu and select **Group**.
- Step 6** Under **Group Details**, click **Add** for every new row you need to add to the profile.
- Step 7** Expand the drop-down menus for each row to select a profile to add to the group. If you want to remove a profile at any point prior to saving, select the profile's checkbox so it is highlighted and select **Remove**.
- Step 8** Click **Save**.

What to do next

Attach the profile to a policy rule set. See [Rule Sets and Rule Set Groups](#) for more information.

Network Time Protocol Profile

Network Time Protocol synchronizes computer clocks to each other and to international standards via telephone modem, radio and satellite. As a profile, especially within distributed systems, synchronized time is essential for coordinating actions and ensuring that distributed processes work together seamlessly. Consistent time across devices is ideal in network management tasks, such as monitoring and troubleshooting. It ensures that logs from different devices can be correlated accurately and ensures the smooth and secure operation of the network.

Create a Profile

Use the following procedure to create an NTP profile:

-
- Step 1** Navigate to **Manage > Profiles > NTP**.
- Step 2** Click **Create**.
- Step 3** Specify a unique **Name**.
- Step 4** (Optional) Enter a **Description**. This may help differentiate between other profiles with a similar name.
- Step 5** Specify the **List** of NTP servers.
- Step 6** Click **Save**.

What to do next

Attach the profile to a policy rule set. See [Rule Sets and Rule Set Groups](#) for more information.

IPSec Profile

The use of Internet Protocol Security (IPSec) profiles for a virtual tunnel interface can simplify the configuration process when you need to provide protection for remote access. An IPSec profile contains the required security protocols and algorithms required to ensure a secure, logical communication path between two site-to-site VPN peers. It is a required component when creating a tunnel as the VPN depends on IPSec tunnels for network-to-network, host-to-network and host-to-host communications. The IPSec profile allows you to configure both IKE and IPSEC parameters in one place for additional security and encryption protection.

If you choose to include an IPSec profile within your site-to-site tunnel configuration, the profile provides robust network security by encrypting and authenticating data as it travels between points on the network as well as the flexibility of being compatible with site-to-site, client-to-site, and client-to-client tunnels.

Create an IPSec Profile

Use the following procedure to create an IPSec profile from the Multicloud Defense Controller dashboard:

-
- Step 1** Navigate to **Manage > Profiles > IPSec**.
- Step 2** Click **Create**.
- Step 3** Enter a unique **Profile Name**.
- Step 4** (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.
- Step 5** Enter the appropriate IKE information when prompted:
- DH Group** - Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Expand the drop-down menu to select the appropriate groups for the profile.
 - Authentication** - Expand the drop-down menu to select the types of authentication you want for this tunnel.
 - Encryption** - Intercepted stacks require encrypting and decrypting. Expand the drop-down menu to select your method of encryption.
 - Hash** - SHA1 is a one-way hashing algorithm that produces a 160-bit digest. Use the drop-down menu to select the appropriate option.
 - Key Lifetime** - Enter a time value in seconds for how long the key lasts. Available values are between 60 sec and 86400 sec.
 - IKE Version** - The Internet Key Exchange (IKE) is a protocol that is used to set up a security association in the IPSec protocol suite that provides robust authentication and encryption of IP packets. Use the drop-down menu to select either IKE version 1 or version 2. There are significant differences between the versions so be sure to select the one most appropriate for your environment.
- Step 6** Enter the appropriate IPsec information when prompted:
- Authentication** - Expand the drop-down menu to select an authentication method: None, SHA256, SHA, or Null.
 - Encryption** - Expand the drop-down and select a type of key: AES GCM 256, AES GCM 192, or AES GCM. This generates a unique key exchange between the connected devices, so that each device can decrypt the other device's messages.
 - Mode** - Expand the drop-down menu to select the IPSec policy authentication protocol. You can select more than one.
-

What to do next

Attach the profile to a policy rule set. See [Rule Sets and Rule Set Groups](#) for more information.

BGP Profile

Border Gateway Protocol (BGP) is an Internet Engineering Task Force (IETF) standard, and the most scalable of all routing protocols. BGP is the routing protocol of the global Internet, as well as for service provider private networks. BGP enables the VPN gateways and your BGP neighbors to exchange routes that inform the gateways on both sides of the connectoin of the availability of the gateways or routers involved.

We **strongly** recommend creating and adding a BGP profile to your gateway if you are establishing a site-to-site VPN tunnel connection to another platform or device. Deploying with a BGP profile deploys a gateway that uses dynamic routing with BGP between your networks and cloud service providers.

Create a BGP Profile

Use the following procedure to create a BGP profile from the Multicloud Defense Controller dashboard:

-
- Step 1** Navigate to **Manage > Profiles > BGP**.
 - Step 2** Click **Create**.
 - Step 3** Enter a unique **Profile Name**.
 - Step 4** (Optional) Enter a **Description**. This may help differentiate from other profiles with a similar name.
 - Step 5** Enter the **LocalAS** value. This value represents the local autonomous system (AS) in which the BGP4 device resides.
 - Step 6** Click **Add Neighbor** to add at least one peer to the profile.
 - Step 7** Add the following information for the **Neighbor**:
 - a) **IP Address** - Enter a singular address or a range of IP addresses and BGP peer groups. If you are adding multiple addresses, separate each address with a **space**.
 - b) **Autonomous System** - Enter the **LocalAS** for where the neighbor resides.
 - Step 8** Click **Save**.
-

What to do next

Add your BGP profile to a Multicloud Defense Gateway. You can either [create a new gateway](#) or edit an existing gateway to include the new profile.

