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 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

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:

Procedure

Step 1 Navigate to **Infrastructure** > **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 requirments 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 4 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:

Procedure

Step 1 Navigate to **Infrastructure** > **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 7, 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.

Procedure

Step 1   Navigate to **Infrastructure** > **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. This forwarding profile allows you 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

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 metrics to, prior to creating this profile.

Procedure

Step 1   Navigate to **Infrastructure** > **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   (Optional) Send a **Test** message to the destination. Enter the content of the test message in the text field when prompted and clikc **Validate**. If the destination does not receive the test message, confirm the destination type and configuration in step 7.

Step 9   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.

Procedure

Step 1   In the Multicloud Defense Controller interface navigate to **Infrastructure** > **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.

(Preview Only) Network Packet Broker Profile

A Network Packet Broker (NPB) profile is a configuration set within a Network Packet Broker device that defines how network traffic should be managed, and directed; traffic is filtered based on various criteria such as IP addresses, protocols, ports, and application types. These profiles are specialized devices used to optimize the flow of network traffic to various monitoring, security, and performance management tools.

Create Network Packet Broker Profile

Use the following procedure to create a Network Packet Broker (NPB) profile:

Procedure

Step 1   Navigate to **Policies** > **Profiles** > **Network Packet Broker**.

Step 2   Click **Create**.

Step 3   Provide a unique **Name**.

Step 4   (Optional) Enter a **Description**. This may help differenatiate between other profiles with similar names.

Step 5   Under **Destinations** expand the drop-down menu and select the preferred destination for your NPB profile should direct matching traffic to.

Step 6   Define th capture format to ensure that network data is effectively captured, stored, and analyzed, leading to better network management and troubleshooting capabilities. Expand the **Capture Format** drop-down menu and select one of the following formats:

- **None** - Select this option if you have limited resources or operate within a highly dynamic environment that utilizes multiple formats. You can also select this option if you intend to change this field later on.

- **VXLAN** - Virtual Extensible LAN, is not a capture format itself but rather a network virtualization technology. It extends Layer 2 networks over a Layer 3 infrastructure, enabling the creation of a virtualized network overlay and contains Ethernet frames within UDP packets, allowing them to be transmitted over IP networks

- **Netflow** - Select this option if your environment is configured to export flow records to a designated collector or analysis tool, rather than capturing raw packets in formats like PCAP.

- **ERSPAN** - Select this protocol to mirror traffic from a source to a destination over a network and extend the capabilities of traditional SPAN (Switched Port Analyzer) by containing mirrored traffic into GRE packets that are then sent over Layer 3 networks. This is ideal for environments where network traffic needs to be monitored from a central location.

Step 7   Expand the **Slicing** drop-down menu and select how each network packet is sectioned and captured, rather than the entire packet. If you opt to configure this, be sure to also configure the following options:

Offset value - This field allows you to configure the number of bytes that are skipped from the start of each packet before beginning to capture data. This is set to **4** by default.

Strip Encrypted Payload - Check this option to remove an encrypted portion of a packet's data payload during capture or analysis.Enable this to concentrate on metadata and network behavior while respecting privacy and optimizing resource use.

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:

Procedure

Step 1	Navigate to **Infrastructure** > **Network** > **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. t 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:

Procedure

Step 1	Navigate to **Infrastructure** > **Network** > **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:

a) **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.

b) **Authentication** - Expand the drop-down menu to select the types of authentication you want for this tunnel.

c) **Encryption** - Intercepted stacks require encrypting and decrypting. Expand the drop-down menu to select your method of encryption.

d) **Hash** - SHA1 is a one-way hashing algorithm that produces a 160-bit digest. Use the drop-down menu to select the appropriate option.

e) **Key Lifetime** - Enter a time value in seconds for how long the key lasts. Avaialble values are between 60 sec and 86400 sec.

f) **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:

a) **Authentication** - Expand the drop-down menu to select an authentication method: None, SHA256, SHA, or Null.

b) **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.

c) **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 for the global Internet and 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.

You **must** create and add 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 depoys a gateway that uses dynamic routing with BGP between your networks and cloud service providers.

BGP Neighbors and Path Selection

BGP profiles utilize a property called "neighbors"; a neighbor refers to another BGP router with which a BGP session is established. The purpose of configuring neighbors in a BGP profile is to facilitate the exchange of routing information between autonomous systems (ASes) or within a singular AS.

☞

Important   We **strongly** recommend adding at least one nighbor to your BGP profile.

Within the neighbor section of the BGP profile, you have the chance to opt to **Route Map In** or **Route Map Out**. The route maps provide us a mechanism to only advertise (outbound) or accept (inbound), based on whats identified in that route map.

Allowing a route map **in** enables the following actions:

- **Incoming Route Filtering:** Control which routes are accepted from a BGP neighbor. Filter out unwanted routes to optimize the routing table to ensure only the relevant routes are considered.

- **Attribute Modification**: Adjust attributes of incoming routes, such as the local preference or metric, to influence the path selection process within your network. This helps prioritize certain routes over others based on your deployed network policies.

- **Security and Policy Compliance**: Prevent routes that do not comply with your network policies from being accepted to enhance security and ensure policy compliance.

Adversely, allowing a route map **out** enables the following actions:

- **Outgoing Route Filtering**: Control which routes are advertised to a BGP neighbor. This helps manage the visibility of your network to external peers and has the potential to prevent the advertisement of specific internal routes.

- **Attribute Setting**: Modify route attributes before they are sent to a neighbor.

- **Traffic Engineering**: Influence inbound traffic paths by adjusting route attributes like AS path length to guide traffic through preferred routes.

BGP may receive multiple advertisements for the same route from different sources. BGP selects only one path as the best path. When this path is selected, BGP puts the selected path in the IP routing table and propagates the path to its neighbors. BGP uses the following criteria, in the order presented, to select a path for a destination:

- If the path specifies a next hop that is inaccessible, drop the update.

- Prefer the path with the largest weight.

- If the weights are the same, prefer the path with the largest local preference.

- If the local preferences are the same, prefer the path that was originated by BGP running on this router.

- If no route was originated, prefer the route that has the shortest AS_path.

- If all paths have the same `AS_path` length, prefer the path with the lowest origin type (where IGP is lower than EGP, and EGP is lower than incomplete).

- If the origin codes are the same, prefer the path with the lowest MED attribute.

- If the paths have the same MED, prefer the external path over the internal path.

- If the paths are still the same, prefer the path through the closest IGP neighbor.

- If both paths are external, prefer the path that was received first (the oldest one).

- Prefer the path with the lowest IP address, as specified by the BGP router ID.

• If the originator or router ID is the same for multiple paths, prefer the path with the minimum cluster list length.

• Prefer the path that comes from the lowest neighbor address.

Create a BGP Profile

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

Before you begin

✎

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

Procedure

Step 1   Navigate to **Infrastructure** > **Network** > **BGP**.

Step 2   Click **Create**.

Step 3   In the **General Settings** tab of the creation window 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 the **Neighbors** tab at the top of the window to switch views. For more information on neighbors and what this configuration can do for you environment, see BGP Neighbors and Path Selection, on page 8.

Step 7   Click **Add Neighbors**.

Step 8   Expand the **Neighbor 1** space.

Step 9   Manually enter a singular address or a range of IP addresses and BGP peer groups in the **IP Address** text box. If you are adding multiple addresses, separate each address with a space.

Step 10   Enter the **Autonomous System** value, the LocalAS for where the neighbor resides.

Step 11   If you opt to include **Route Map In**, note that enabling this option applies the route map on all matching traffic in the inbound direction on the interface. If you opt to include **Route Map Out**, enabling this option applies the routemap to all matching traffic in the outbound direction on the interface. Check the appropriate option for your environment and then enter the following information:

   a)   **Local Preference** - By default, this value is "100". Optionally, enter a 32-bit unsigned integer value between 0 to 4,294,967,295. Note that with a higher local preference value indicating a more preferred route within an autonomous system.

   Local preference is only exchanged between BGP routers within the same autonomous system (iBGP) and not advertised externally (eBGP).

   b)   **AS Path Prepend** - Maually enter a value for this; if you enter more than one separate each value with a **space**. This value influences the path selection process by artificially lengthening the AS path attribute of a route. While it is unconventional to include this for inbound traffic, prepending additional AS numbers to incoming routes can make these routes appear less preferable to your internal BGP speakers when selecting paths for routing traffic.

c) Click **Add** to include an IP address or a network and enter an IP address, a range of IP addresses seperated by commas, or a network comprised of both the IP and netmask. These are routes or networks that you want to allow in or out within the bgp session(s). At any point, click **Remove** to remove an IP address from the neighbor.

Step 12 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.