Security Profiles

Decryption Profile

A decryption profile is used by the Multicloud Defense Gateway in a reverse proxy **or** forward proxy scenario. When a connection is proxied, the front-end session is terminated on the gateway and a new back-end session is established to the server. The intention of this termination is to decrypt and inspect the traffic to protect against malicious activity. In order to decrypt encrypted traffic, a decryption profile is necessary.

Create a Decryption Profile

Use the following procedure to create a decryption profile.

Step 1 Navigate to **Manage** > **Profiles** > **Decryption**.

Step 2 Click **Create**.

Step 3 Specify a **Profile Name** and a **Description**.

Step 4 For **Certificate Method** choose **Select Existing**.

Step 5 For **Certificate** choose the desired certificate.

Step 6 For **Min TLS Version** choose the lowest TLS version that is accepted by the decryption profile. The default is TLS 1.0.

Step 7 If using non-default (non-PFS) cipher suites, select the set of desired cipher suites from the Diffie- Hellman or PKCS (RSA) menus.

Step 8 Click **Save**.

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

TLS Versions in your Decryption Profile

The Multicloud Defense Gateway supports all TLS versions (TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0). Users can specify a minimum TLS version to use and Multicloud Defense Gateway will negotiate a TLS version that is equal to or higher than the specified minimum TLS version. The Multicloud Defense Gateway will always use the highest TLS version possible during the TLS negotiation. In the case where the Multicloud Defense Gateway cannot negotiate a version that meets the minimum TLS version specified, the Multicloud Defense Gateway will drop the session and logging a `TLS_ERROR` event.

Note Only a single minimum TLS version can be applied to a gateway. A consistent minimum TLS version must be used across all decryption profiles referenced by all service objects that are used within a policy ruleset or policy ruleset group. If different minimum TLS versions are specified, the minimum TLS version that will be applied cannot be predetermined.

Cipher Suites

The Multicloud Defense Gateway supports a set of default and user-selectable cipher suites. The default set are PFS cipher suites that are always selected. The user-selectable set are Diffie-Hellman and PKCS (RSA) cipher suites that can be selected by the user. The combined set of cipher suites (default and user-selected) are used by the gateway for establishing a secure front-end encrypted session. The client will send an ordered list of preferred cipher suites. The gateway will respond with a cipher suite chosen from the ordered set submitted by the client and the set available by the gateway. If the client allows the server to define the order, then the cpher suite chosen is from the ordered set available by the gateway and the set submitted by the client.

The following is an ordered list of cipher suites supported by the gateway and available in a decryption profile:

Category	Cipher Suite	Key Exchange	Cipher	Hash	Default
PFS	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA	AES256-GCM	SHA384	☐
PFS	ECDHE-RSA-AES256-CBC-SHA384	ECDHE-RSA	AES256-CBC	SHA384	☐
Diffie-Hellman	DH-RSA-AES256-GCM-SHA384	DH-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-GCM-SHA384	DHE-RSA	AES256-GCM	SHA384	☐
PFS	DHE-RSA-AES256-CBC-SHA256	DHE-RSA	AES256-CBC	SHA384	☐
PFS	DHE-RSA-AES256-CBC-SHA	DHE-RSA	AES256-CBC	SHA	☐

Category	Cipher Suite	Key Exchange	Cipher	Hash	Default
Diffie-Hellman	DH-RSA-AES256-SHA256	DH-RSA	AES256-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES256-SHA	DH-RSA	AES256-CBC	SHA160	
PKCS (RSA)	AES256-GCM-SHA384	PKCS-RSA	AES256-GCM	SHA384	
PKCS (RSA)	AES256-SHA256	PKCS-RSA	AES256-CBC	SHA256	
PKCS (RSA)	AES256-SHA	PKCS-RSA	AES256-CBC	SHA160	
PFS	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA	AES128-GCM	SHA256	□
PFS	ECDHE-RSA-AES128-CBC-SHA256	ECDHE-RSA	AES128-CBC	SHA256	□
Diffie-Hellman	DH-RSA-AES128-GCM-SHA256	DH-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-GCM-SHA256	DHE-RSA	AES128-GCM	SHA256	□
PFS	DHE-RSA-AES128-CBC-SHA256	DHE-RSA	AES128-CBC	SHA256	□
Diffie-Hellman	DH-RSA-AES128-SHA256	DH-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA	DH-RSA	AES128-CBC	SHA160	
PKCS (RSA)	AES128-GCM-SHA256	PKCS-RSA	AES128-GCM	SHA256	
PKCS (RSA)	AES128-SHA256	PKCS-RSA	AES128-CBC	SHA256	
PKCS (RSA)	AES128-SHA	PKCS-RSA	AES128-CBC	SHA160	
PFS	ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA	DES-CBC3	SHA	□
PFS	ECDHE-RSA-RC4-SHA	ECDHE-RSA	RC4	SHA	□
PKCS (RSA)	RC4-SHA	PKCS-RSA	RC4	SHA160	
PKCS (RSA)	RC4-MD5	PKCS-RSA	RC4	SHA160	

Network Intrusion (IDS/IPS) Profile

Network intrusion profiles are a collect of Intrusion Detection and Protection (IDS/IPS) rules that can be used to evaluate transactions to ensure the traffic is not malicious.

Multicloud Defense supports the following IDS/IPS rule sets:

Table 1: Multicloud Defense supports the following IDS/IPS Rule Sets

Rule Sets	Description
Talos Rules	The Talos rules are a premium set of rules from Cisco based on intelligence gathered from real-world investigations, penetration tests and research that provide an advanced level of protection for applications and frameworks.

Rule Sets	Description
Custom Rules	Custom rules are a particular set of rules written by customers that provide a specialized level of protection for custom applications.

Create an IPS/IDS Profile

Use the following procedure to create and add an IPS/IDS profile to a ruleset:

Step 1 Navigate to **Manage** > **Profiles** > **IPS/IDS**.

Step 2 Click **Create Intrusion Profile**.

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

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

Step 5 Specify the **Action** with one of the following options:

- **Rule Default** - Allow or Deny the requests based on the action specified in each triggered Rule and log an Event.
- **Allow Log** - Allow the requests and log an event.
- **Allow No Log** - Allow the requests and do not log an event.
- **Deny Log** - Deny the requests and log an event.
- **Deny No Log** - Deny the requests and do not log an event.

Step 6 Check for whether to generate a Threat PCAP file if the IDS/IPS Profile detects malicious activity.

Step 7 Specify the **Rule Set**. Note that at least one ruleset from a rules library (Talos, Custom) is required to be specified in the IDS/IPS profile. If Talos rules and custom rulesets are used, at least one of the two must be enabled. If the desire is to disable the entire IDS/IPS Profile, remove the IDS/IPS Profile from any policy ruleset so the IDS/IPS profile will not be evaluated.

epcify one of the following **Talos Rules** desginations:

- **Disabled** - Specify whether to disable the use of Talos rules.
- **Manual** - Specify the Talos rule's version.
- **Automatic** - Specify the number of days from publish date to delay automatic update to the latest Talos rule's version.

Step 8 Add specific **Custom Rulesets** to the IPS/IDS Profile.

Step 9 Specify the **Rules Suppression** for rules that can be suppressed for a specific IP or a list of CIDRs and click **Add**.

Step 10 Locate and select the **Advanced Settings** tab and under "Rule Suppression", click **Add**.

a) For **Rule ID List**, provide a comma-separated list of rule IDs. For **Source IP/CIDR List**, provide a comma-separated list of IPs or CIDRs.

b) For **Action**, provide a selection, but this selection does not apply since a rule being suppressed will not be evaluated.

Step 11 Select the **Event Filtering Type**; this reduces the number of security events that are generated when the IPS/IDS profile is triggered, and the event filtering can be configured to one of the following options:

- **Rate** - the generated events are rate limited based on the specified **Number of Events** triggered over a Timeevaluation interval (in seconds).
- **Type** - the generated events are sampled based on the specified **Number of Events**.

Step 12 Under **Rule Event Filtering**, click **Add**.

Step 13 For **Rule ID List**, specify a comma-separated list of rule IDs.

Step 14 Specify the rule event filtering **Type** with one of the following options:

- **Rate** - Specify the **Number of Events** and the **Time** evaluation interval (in seconds).
- **Sample** - Specify the **Number of Event**s.

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

Data Loss Prevention (DLP) Profile

The DLP (Data Loss Prevention) profile provides Multicloud Defense customers with the ability to specify policy rules to detect and take action upon finding exfiltration patterns in the data when the Multicloud Defense solution is deployed in the forward proxy (egress) mode.

Multicloud Defense allows customers to specify common pre-packaged data patterns such as Social Security Numbers (SSN), AWS secrets, credit card numbers etc., in addition to custom PCRE based regular expression patterns. This makes it easy to enforce protections for PCI, PII, and PHI data to meet compliance requirements. This feature is integrated with the existing Multicloud Defense feature set requiring no separate DLP services.

Create a Data Loss Prevention Profile

Step 1 Navigate to **Manage** > **Profiles** > **Network Threats**.

Step 2 Click **Create Intrusion Profile**.

Step 3 Select **Data Loss Prevention**.

Step 4 Provide a unique **Name** and enter a description for the profile.

Step 5 Enter the **DLP FIlter List** in the table.

Step 6 Click **Add** to insert more rows as needed.

Step 7 Provide a **Description** for the filter.

Step 8 Choose a predefined static pattern (e.g CVE Number) from the dropdown list or provide a custom Regular expression.

Step 9 Provide a **count** to define the number of times the pattern must be seen in the traffic.

Step 10 Select an **Action** to take if the pattern matches the count number of times.

Note There are cases where the pre-defined pattern for AWS Access Key and AWS Secret Key doesn't match in DLP inspection due to pattern being more restrictive. Use the following relaxed custom pattern in DLP profile to detect AWS Access Key and AWS Secret Key. Be aware that this could generate false positives log events.

```
AWS Access Key: (?<![A-Z0-9])[A-Z0-9]{20}(?![A-Z0-9])

AWS Secret Key: (?<![AZa-z0-9/+=])[A-Za-z0-9/+=]{40}(?![A-Za-z0-9/+=])
```

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

Anti-Malware Profile

An anti-malware profile enables anti-malware protection using the Talos ClamAV virus detection engine. ClamAV® is an antivirus engine for detecting trojans, viruses, malware and other malicious threats.

The following steps will guide you creating an anti-malware profile and associate it with a policy rule.

Create an Anti-Malware Profile

Step 1 Navigate to **Manage** > **Profiles** > **Network Threats**.

Step 2 Select **Anti-malware**.

Step 3 Provide a unique **Name** and enter a description.

Step 4 Select one of the following modes for Talos ruleset:

- **Manual Mode** - select the Talos Ruleset Version from dropdown. The selected ruleset version is used by the Multicloud Defense datapath engine on all Gateways which use this profile and is not automatically updated to newer ruleset versions.
- Automatic Mode - select how many days to delay the deployment by, after the ruleset version is published by Multicloud Defense. New rulesets are published daily by Multicloud Defense and the gateways using this profile are automatically updated to the latest ruleset version which is **N** days or older, where **N** is the "delay by days" argument selected from the dropdown. For example, if you select to delay the deployment by 5 days on Jan 10, 2024, the Multicloud Defense Controller will select a ruleset version which was published on Jan 5th or before. Note that Multicloud Defense may not publish on some days if our internal testing with that ruleset version fails for some reason.

Step 5 Select the desired **Action** to take when a match for a virus signature is found.

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

Web Application Firewall (WAF) Profile

Web protection profiles are a collection of Web Application Firewall (WAF) rules that can be used to evaluate web-based transactions to ensure the traffic is not malicious.

Multicloud Defense supports the following WAF rulesets:

Table 2: Multicloud Defense supports the following WAF Rulesets

Rulesets	Description
Core Rules	The Core rules are a standard set of rules from ModSecurity CRS (Core Rule Set) that provide a base level of protection for any web application.
Trustwave Rules	The Trustwave rules are a premium set of rules from ModSecurity based on intelligence gathered from real-world investigations, penetration tests and research that provide an advanced level of protection for specific web applications and frameworks.
Custom Rules	The Custom rules are a particular set of rules written by customers that provide a specialized level of protection for custom web applications.

Create WAF Profile

Use the following procedure to create a WAF profile.

Note If core Rulesets are specified, the core rules cannot be disabled. In order to disable the core rules, remove all core rulesets from the WAF profile so they will not be evaluated.

Step 1 Navigate to **Manage** > **Profiles** > **WAF**.

Step 2 Click **Create**.

Step 3 Specify the following general settings:

a) Enter a unique **Profile Name**.

b) (Optional) Enter a **Description**. This may help differentiate between profiles with a similar name.

c) Specify the action:

- **Rule Default** - Allow or deny the requests based on the action specified in each triggered rule and log an event.
- **Allow Log** - Allow the requests and log an event.

- **Deny Log** - Deny the requests and log an event.

d) Specify whether to generate a Threat HAR file if the WAF profile detects malicious activity. The gateway should have a Pcap profile attached, for this to work.
e) Specify whether to generate a HTTP Request HAR file if the WAF profile detects malicious activity.
f) In the **RULE SETS**section, in the vertical tab located to the left, click **Core Rules**. You must specify at least one ruleset from a rules library (Core, Trustwave, Custom):
   - Specify the following:
     - **Manual** - Specify the core rules version to use.
     - **Automatic** - Specify the numbers of days from publish date to delay automatic update to the latest core rules version.
   - Identify the rules you want to add to the profile and click **Add to Profile**. The selections appear in the table located to the right.
g) In the vertical tab located to the left, click **Trustwave Rules**.
   - Specify the following:
     - **Disabled** - Specify whether to disable the use of Trustwave rules.
     - **Manual** - Specify the Trustwave rules version to use.
     - **Automatic** - Specify the number of days from publish date to delay automatic update to the latest Trustwave rules version.
   - Identify the rules you want to add to the profile and click **Add to Profile**. The selections appear in the **Profile Selections** table located to the right.
h) In the vertical tab located to the left, click **Custom Rules**.
   - Specify one of the following options:
     - **Disabled** - Specify whether to disable the use of custom rules.
     - **Manual** - Specify the custom rules version to use.
     - **Automatic** - Specify the number of days from publish date to delay automatic update to the latest custom rules version.
   - Identify the rules you want to add to the profile and click **Add to Profile**. The selections appear in the **Profile Selections**table located to the right.

Step 4 Scroll to the top of the window and click the **Advanced Settings** tab:

a) Under "Rule Suppression", click **Add** to add one or more rows for rules. Rules can be suppressed for a specific IP or a list of CIDRs:
   - For **Source IP/CIDR List**, provide a comma-separated list of IPs or CIDRs.
   - For **Rule ID List**, provide a comma-separated list of rule IDs.
b) Under "Event Filtering" provide the following information:

- **Type - Rate** or **Sample**
- **Number of Events**
- **Time (Seconds)**

c) Under "Rule Event Filtering" click **Add** to add one or more rows for rules. For every new row you create, enter a valid **Rule ID List**, **Number of Events**, **Time (Sec)**, and choose either Type or Sample as the **Type**.
d) Under "Core Rule Set", select a value for both the **Request Anomaly** and **Response Anomaly**. Note that using a value less than 3 for the "Request Anomaly" results in a huge volume of alerts.
e) Select the **Paranoia Level**. Your options range from 1–4.

Step 5 Click **Save**.

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

Event Filtering

To reduce the number of security events that are generated when the WAF Profile is triggered, the Event Filtering under **Advanced Settings** can be configured to rate limit or sample the events. The configuration does not alter the detection or protection behavior.

When specifying Type as **Rate**, the generated events are rate limited based on the specified *Number of Events* triggered over a *Time* evaluation interval (in seconds). For example, if *Number of Events* is specified as 50 and *Time* is specified as 5 seconds, only 10 events per second will be generated.

When specifying Type as **Sample**, the generated events are sampled based on the specified *Number of Events*. For example, if *Number of Events* is specified as 10, only 1 event will be generated for every 10 events triggered.

Profile Event Filtering

Profile Event Filtering applies to all rules that are configured in the WAF Profile:

- Specify the Type as **Rate** or **Sample**:
  - **Rate**- Specify the *Number of Events* and the *Time* evaluation interval (in seconds).
  - **Sample**- Specify the *Number of Events*.

Rule Event Filtering

To reduce the number of security events that are generated when the WAF profile is triggered, event filtering can be configured to rate limit or sample the events. The configuration does not alter the detection or protection behavior.

Rule event filtering applies to specific rules that are configured in the WAF profile.

Step 1 Click **Add** under Rule Event Filtering.
Step 2 For **Rule ID List**, specify a comma-separated list of **Rule IDs**.

Step 3 Specify Type as **Rate** or **Sample**.

- **Rate**- Specify the **Number of Events** and the **Time** evaluation interval (in seconds).
- **Sample**- Specify the **Number of Events**.

What to do next

Associate WAF Profile with a Policy Rule

Create L7 DoS Profile

Multicloud Defense Gateways provide the ability to monitor, detect, and remediate application layer attacks by continuously monitoring the client requests to a backend web server. Layer 7 DoS attacks are targeted at depleting web server resources, affecting service availability by sending many HTTP requests. This feature is enabled when the gateways are enabled to proxy inbound connections to a backend web service to maintain availability of web based applications. Enabling this feature also allows the gateways to provide additional security for cases where a frontend load balancer may not support, or, may not be optimized to detect and remediate against application DoS attacks.

This feature can also be used to provide DoS protection against backend web servers hosting API services.

Step 1 Navigate to **Manage** > **Profiles**.

Step 2 Select **Layer 7 DOS**.

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

Step 4 (Optional) Enter a **Description**. This may help differentiate between other profiles that may have similar names.

Step 5 Add **Request Rate Limits**.

Limiting excessive requests to a resource is based on the following parameters. The values for these parameters should be based on measuring and understanding the traffic patterns for your web services to be protected by the Layer 7 DoS option.

Table 3: Parameters

Parameter	Description
URI	A relative URI used to indicate the path to limit requests for a resource. For example, if you intend to monitor and protect your service resource at https://www.example.com/login.html, you would enter /login.html as the URI parameter in the **Request Rate Limits** table.

Parameter	Description
HTTP Methods	HTTP methods can be specified per-resource URI to control which HTTP methods in the client requests are rate limited and which ones are not. You can select multiple methods from the drop down for each row in the table. An empty HTTP method list means that method is ignored and the rate applies to all calls to the resource. **Note** The rate is applied for each resource; therefore, multiple methods share the rate limit specified in the Request Rate in that row. For example, if the rate is 3 requests for every second, and GET, POST and PUT are specified in the HTTP Methods, and 2 GETs and 1 POST happen to that URI from a single client IP in the same second, a PUT will NOT be allowed in that same second.
Request Rate	The number of requests for every second. It determines the rate at which a single client can send requests to the URI resource mentioned in the URI part of the rule.
Burst Size	Specifies the maximum number of simultaneous requests that a client can send to the URI resource mentioned in the URI part of the rule. Any requests beyond this threshold, arriving at the proxy at the same time, will not be sent to the backend server.

Step 6 Click **Save** when completed. The order of the rules is important based on the URI as the rules are checked from the top down and applied on first match. If the URI added higher in the list includes a resource path that includes resources in the rules below it, the first rule matched will be applied.

What to do next

- View a Profile Details
- Add the L7 DoS profile to a **service object**. Then, Add a Gateway Association to a Profile. Note that if you update a rule set, changes may not be deployed immediately.

URL (Uniform Resource Locator) Filter Profile

A URL filtering profile evaluates the URL of an HTTP request and applies an action to either allow or deny the traffic. In order to evaluate the URL, the traffic must be processed by a **Forward Proxy** rule. The set of URLs in the profile can be specified as strings representing the full path or as strings representing a Perl Compatible Regular Expression (PCRE). If only domain filtering is required, it is best to use an FQDN filtering profile. An FQDN filtering profile can also be used in conjunction with URL filtering, where the domain is evaluated using the FQDN filtering profile and the URL is evaluated using the URL filtering profile.

The URL filtering profile can use a set of pre-defined categories. To view more information on categories, please see FQDN / URL Filtering Categories.

Note The URL filtering is organized as a table containing user-specified rows (URLs and Categories) along with two default rows (**Uncategorized** and **ANY**). Categories and URLs can be combined within each row if desired.

The limits for each URL filtering profile are as follows:

- Maximum user-specified rows: 254 (Standalone or a group of standalones)
- Maximum Categories and URLs per row: 60
- Maximum URL character length: 2048

When specifying a multi-level domain (e.g., `www.example.com`), it's important to escape the `.` character (e.g., `www\.example\.com`) otherwise it will be treated as a wildcard for any single character

Uncategorized

- The penultimate row in a URL filtering profile, which is represented as **Uncategorized**.
- Specifies the policy action to take for URLs that do not match the user-specified URLS or do not have a category.
- If a standalone profile is used in a group profile and the group profile is applied to a policy ruleset, the **Uncategorized** row will be taken from the group profile. The **Uncategorized** row of a standalone profile is only applicable if the standalone profile is directly applied to a policy ruleset.

Default (ANY)

- The final row in a URL filtering profile, which is represented as **ANY**.
- Specifies the policy action to take for URLs that do not match the user-specified URLs or categories, or are not uncategorized.
- If a standalone profile is used in a group profile and the group profile is applied to a policy ruleset, the **ANY** row will be taken from the group profile. The **ANY** row of a standalone profile is only applicable if the standalone profile is directly applied to a policy ruleset.

Create the URL Filtering Profile

Use the following procedure to create a standalone URL filtering profile:

Step 1 Navigate to **Manage** > **Profiles** > **URL Filtering**.

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 Click **Add** to create a new row.

Step 6 Specify individual URLs (e.g., https://www.google.com):

- Each URL is specified as a PCRE (Perl Compatible Regular Expression).

- Each URL must be specified as a full path.
- Consider escaping the decimal "." character else it will be treated as a single character wildcard.

Step 7 Specify **Categories** (e.g., Gambling, Sports, Social Networking).

Step 8 Specify the HTTP methods to which the policy is applied.

Step 9 Select on of the following as a subset of methods:

- Delete
- Get
- Head
- Options
- Patch
- Post
- Put

Step 10 Specify **All** for all methods.

Step 11 Specify the policy **Action** for the user-specified URLs/Categories, Uncategorized and ANY rows:

- **Allow Log** - Allow the requests and log an event.
- **Allow No Log** - Allow the requests and do not log an event.
- **Deny Log** - Deny the requests and log an event.
- **Deny No Log** - Deny the requests and do not log an event.

Step 12 Specify the **Return Status Code**.

Step 13 Specify an integer value **greater than or equal to 100 and less than 600**. The value represents the HTTP status that will be returned to the client making the request. A common return code is **503**.

Step 14 Click **Save**.

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

Fully Qualified Domain Name Filter Profile

A Fully Qualified Domain Name (FQDN) filter profile evaluates the FQDN associated with traffic and applies an action to either allow or deny the traffic. In order to evaluate the FQDN, traffic must be TLS encrypted and contain an FQDN in the SNI field of a TLS hello header. The FQDN can be evaluated for traffic that is processed by either a **Forwarding** or **Forward Proxy** rule. The set of FQDNs in the profile can be specified as strings representing the full domain or as strings represented by a Perl Compatible Regular Expression

(PCRE). If only domain allowlisting is required, it is best to use an FQDN filtering profile. An FQDN filtering profile can also be used in conjunction with a URL filtering profile, where the domain is evaluated using the FQDN filtering profile and the URL is evaluated using the URL filtering profile.

The FQDN filtering profile can also use a set of pre-defined categories. To view more information on categories, see FQDN / URL Filtering Categories.

Note The FQDN filtering profile is organized as a table containing user-specified rows (FQDNs and categories) along with two default rows (Uncategorized and ANY). Categories and FQDNs can be combined within each row if desired.

The limits for each FQDN filter profile are as follows:

- Maximum user-specified rows: 254 (standalone or group of standalones)
- Maximum categories and FQDNs per row: 60
- Maximum FQDN character length: 255

When specifying a multi-level domain (e.g., 'www.example.com'), it's important to escape the `.` character (e.g.,`www\.example\.com`) otherwise it will be treated as a wildcard for any single character.

Standalone vs. Group

A FQDN filter profile can be specified as standalone or group.

A standalone FQDN filter profile contains FQDNs and categories. The profile will be applied directly to a set of one or more policy rulesets or associated with a FQDN group profile.

A FQDN filter group profile contains an ordered list of standalone profiles that can be defined for different purposes and combined together into a group profile. The group profile can be applied directly to a set of one or more policy rulesets. Each team can create and manage specific standalone profiles. These standalone profiles can be combined together into a group profile to create hierarchies or different combinations based on the use case. An example combination could be a global FQDN list that would apply to everything, a CSP-specific list that would apply to each different CSP, and an application-specific list that would apply to each different application.

Uncategorized

- The second-to-last row in an FQDN filter profile which is represented as **Uncategorized**.
- Specifies the policy action to take for FQDNs that do not match the user-specified FQDNs or do not have a category.
- If a standalone profile is used in a group profile and the group profile is applied to a policy ruleset, the **Uncategorized** row will be taken from the group profile. The **Uncategorized** row of a standalone profile is only applicable if the standalone profile is directly applied to a policy ruleset.

Default (ANY)

- The final row in an FQDN filter profile, which is represented as **ANY**.
- Specifies the policy action to take for FQDNs that do not match the user-specified FQDNs or categories, or are not **Uncategorized**.

- If a standalone profile is used in a group profile and the group profile is applied to a policy ruleset, the **ANY** row will be taken from the group profile. The **ANY** row of a standalone profile is only applicable if the standalone profile is directly applied to a policy ruleset.

Create a Standalone FQDN Filter Profile

Use the following procedure to create a standalone FQDN filter profile:

Step 1 Navigate to **Manage** > **Profiles** > **FQDN Filtering**.

Step 2 Click **Create**.

Step 3 Provide a unique **Name**.

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

Step 5 Specify the Type as **Standalone**.

Step 6 Click **Add** to create a new row.

Step 7 Specify individual FQDNs (for example, google.com).

a) Each FQDN is specified as a PCRE (Perl Compatible Regular Expression).

b) Consider escaping the "**.**" character else it will be treated as a single character wildcard.

Step 8 Specify a **Category** (for example, Gambling, Sports, Social Networking).

Step 9 Specify the policy **Action** for the user-specified FQDNs/Categories, Uncategorized and ANY rows.

- **Allow Log** - Allow the requests and log an event.
- **Allow No Log** - Allow the requests and do not log an event.
- **Deny Log** - Deny the requests and log an event.
- **Deny No Log** - Deny the requests and do not log an event.

Step 10 (Optional) Specify **Decryption Exception** for any FQDNs where decryption is not desired or possible. Possible reasons for considering decryption exception include:

- Desire to not inspect encrypted traffic (for example, financial services, defense, health care, etc.).
- SSO authentication traffic where decryption is not possible.
- NTLM traffic that cannot be proxied.

Step 11 Click **Save** when completed.

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

Create a Group FQDN Filter Profile

Use the following procedure to create a group FQDN filter profile with at least two standalone profiles:

Step 1 Navigate to **Manage** > **Profiles** > **FQDN Filtering**.

Step 2 Click **Create**.

Step 3 Provide a unique **Name**.

Step 4 (Optional) Enter a **Description**. This may help differentiate between profiles that may have a similar name.

Step 5 Specify the Type as **Group**.

Step 6 Select an initial standalone profile (at least one standalone profile is required).

Step 7 Click **Add FQDN Profile** to create a new row for additional profiles.

Step 8 Select a standalone profile.

Step 9 Specify the policy **Action** for uncategorized FQDNs.

Step 10 Specify the policy **Action** for **ANY** FQDNs (default).

Step 11 (Optional) Specify the **Decryption Exception** for uncategorized or ANY if decryption is not desired or possible. Possible reasons for considering decryption exception include:

- Desire to not inspect encrypted traffic (financial services, defense, health care, etc.).
- SSO authentication traffic where decryption is not possible.
- NTLM traffic that cannot be proxied.

Step 12 Click **Save**.

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

Malicious IP Profile

Additional security protections can be enabled to prevent communication from and to known malicious IPs. These malicious IPs are defined by Trustwave and integrated into Multicloud Defense as a security profile ruleset. The ruleset is updated frequently as updates are made available by Trustwave. The updates can be either dynamically or manually applied to a policy ruleset using the automatic update configuration or manual update configuration. For more information, see Create a Malicious IP Profile, on page 17.

Note Malicious IP are identified by Trustwave based on various learned behavior:

- Malicious attackers identified from web honeypots
- Botnet C&C hosts
- TOR exit nodes
- Other learned behavior

Create a Malicious IP Profile

Use the following procedure to create a malicious IP profile:

Step 1 Navigate to **Manage** > **Profiles** > **Malicious IPs**.

Step 2 Click **Create**.

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

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

Step 5 Check the box to enable **IP Reputation**.

Step 6 Choose one of the two options for the **Trustwave Ruleset Version** drop-down menu:

- **Manual** - The selected ruleset version is used by the Multicloud Defense datapath engine on all gateways which use this profile. The profile will not be automatically updated to newer ruleset versions.
- **Automatic** - Select the number of days to delay the update, after the ruleset version is published by Multicloud Defense. New rulesets are published frequently by Multicloud Defense. The gateways using this profile are automatically updated to the latest ruleset version which is **N** days or older, where **N** is the "delay by days" argument selected from the dropdown. For example, if you select to delay the deployment by 5 days on Jan 10, 2021, the Multicloud Defense controller will select a ruleset version which was published on Jan 5th or before. Note that Multicloud Defense may not publish on some days if our internal testing with that ruleset version fails for some reason.

Step 7 Click **Save**.

What to do next

- View a Profile Details
- Add a Gateway Association to a Profile

IP Reputation

The IP reputation checkbox is used as a means to **enable** or **disable** the profile. When checked and the profile is attached to a policy ruleset, malicious IP protection will be enforced. When unchecked and the profile is attached to policy rules, malicious IP protection will not be enforced. Our recommendation is to always check

the IP reputation checkbox. If you want to disable the malicious IP profile, then remove its association from the policy rules rather than uncheck the checkbox.

Packet Capture Profiles

Packet capture profiles are configured and associated with a Multicloud Defense Gateway and enabled in policy rules, network threat profiles, and web protection profiles. A packet capture can capture traffic flows (PCAP files), and application and network threats (HAR files).

Packet Capture Formats

Consider the following format rules:

`Policy Rule Capture` - `<bucketname>/<cspaccountname>/<gatewayname>/flow-packet-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<policyname>.pcap.gz`

`IPS Threat Capture` - `<bucketname>/<cspaccountname>/<gatewayname>/network-threats-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.pcap.gz`

`WAF Threat Capture` - `<bucketname>/<cspaccountname>/<gatewayname>/web-protection-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz`

`API Logging` - `<bucketname>/<cspaccountname>/<gatewayname>/api-logging-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz`

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 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

- View a Profile Details
- Add a Gateway Association to a Profile

Log Forwarding Profile

A log forwarding profile allows you to send a collection of gateway, VPC, and VNet logs to a third party. The comunication 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 20 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

- View a Profile Details
- Add a Gateway Association to a Profile

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 19 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

- View a Profile Details
- Add a Gateway Association to a Profile

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 analyitics 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

- View a Profile Details
- Add a Gateway Association to a Profile

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 20 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

- View a Profile Details
- Add a Gateway Association to a Profile

NTP

The Multicloud Defense Gateway uses NTP to ensure its time in sychronized. NTP operates through the Management interface and is configured as part of the Linux shell used for management purposes. The NTP default configuration is slightly different for each CSP as follows:

- **AWS:** `2.centos.pool.ntp.org`, `169.254.169.123`
- **Azure:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`
- **GCP:** `metadata.google.internal`
- **OCI:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`, `169.254.169.254`

In order to override the default configuration, the NTP profile can be created and applied to each gateway. Once the NTP profile is applied to the gateway, the new configuration will be used. This operation applies immediately.

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

- View a Profile Details
- Add a Gateway Association to a Profile