Security Profiles

A security profile typically refers to a set of rules and configurations applied to network traffic to enforce security policies. These profiles include the following protective measures:

- Firewall Rules
- Intrusion Prevention Systems (IPS)
- Antivirus/Antimalware
- Web Filtering
- Data Loss Prevention (DLP)
- Application Control

These particular profiles are generally added to a policy rule, policy rule set, or a policy rule set group and ordered by priority.

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.

TLS Versions in your Decryption Profile

The Multicloud Defense Gateway supports all TLS versions: TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. 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 gateway always uses the highest TLS version possible combined with the strongest cipher suite during the TLS negotiation. In the case where the Multicloud Defense Gateway cannot negotiate a version that meets the minimum TLS version specified, the gateway drops 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 cipher suite chosen is from the ordered set available by the gateway and the set submitted by the client.

With version 24.10 and later, the Multicloud Defense Controller assists the creation of your decryption profile by auto-selecting the strongest cipher suites once you've chosen the minimum TLS version. Note that both the Multicloud Defense Controller and the Multicloud Defense Gateway must be running at least version 24.10. Older gateway versions do not support this automated help feature and you cannot edit the ciphers suites of an existing decrpytion profile. We strongly recommend updating your gateway to version 24.10 or later to take advantage of this functionality.

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	☐
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	

Category	Cipher Suite	Key Exchange	Cipher	Hash	Default
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	

Create a Decryption Profile

Use the following procedure to create a decryption profile.

Procedure

Step 1 Navigate to **Policies** > **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. Note that the Multicloud Defense Controller filters the available cipher suites so only the strongest ciphers are listed, dependent on the min TLS version you selected in step 6.

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 Intrusion (IDS/IPS) Profile

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

An Intrusion Detection System (IDS) is defined as a solution that monitors network events and analyzes them to detect security incidents and imminent threats, specifically suspicious or abnormal activity such as malicious transactions, and sends immediate alerts when it is observed. IDS searches for and against hosts and networks.

An Intrustion Protection System (IPS) actively analyzes network traffic and compared it against known attack patterns and signatures. When the system detects suspicious traffic, it blocks it from entering the network. IPS rules cover both network-bsed IPs and host-based IPs.

Multicloud Defense combines both of these systems within a singular profile to create an easy-to-configure network intrusion profile made to detect malicious probes or new network patterns from a compromised system that both detects, rejects, and reports supsicious traffic. Preemptive blocking and reporting can mitigate any downtime on your network and further improve blocking activity in the future. A network intrusion profile in Multicloud Defense comprises the following 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.

Note that the IDS/IPS profile does not include web applications that might be malicious. See Web Application Firewall (WAF) Profile, on page 8 for more information.

Create an IPS/IDS Profile

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

Procedure

Step 1 Navigate to **Policies** > **Profiles** > **IPS/IDS**.
Step 2 Click **Create**.
Step 3 Click into the **General Settings** tab.
Step 4 Enter a unique **Profile Name**.
Step 5 (Optional) Enter a **Description**. This may help differntiate between other profiles with a similar name.

Step 6 Toggle the Threat PCAP option file if the IDS/IPS Profile detects malicious activity. Note that if you toggle this option **on**, you must have a PCAP profile attached to the gateway.

Step 7 In the **Rule Set** section of the general settings, 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. Use the drop-down menu to select one of the followingsettings that are applied to all rulsets within this profile:

- **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.

Use the other drop-down menu to select when the rules within this profile are updated. You can opt to update the rule set **Immediately** after Talos sends out an update, or any number of days after the update.

Step 8 Click **Talos Rules: Policy** and choose from the table which policy profile to use as a base. You can only select one profile.

Unless your window view is maximized, scroll to the right of the window and assign an **action** for the selected profile:

- **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 9 Click the **Talos Rules: Category** tab and choose at least one category from the table to the profile.

Step 10 Click the **Talos rules: Class** tab and choose at least one class from the table to the profile.

Step 11 At the top of the screen click into the **Advanced Settings** tab.

Step 12 Under **Rule Supression** click **Add** and enter a valid **Source IP/CIDR List** of IP addresses and a corresponding **Rule ID List**. To remove a row of lists simply click the minus icon to the right of the row.

Step 13 Under **Event Filtering: Profile Event Filtering**, enter the following information:

- **Type** - You can opt for either Rate or Sample. Generated events are rate- or sample-limited based on the specified **Number of Events** triggered over a **Time** evaluation interval (in seconds).
- **Number of Events** - Manually enter a value of allowed number of events.
- (Available for the Rate type) **Time (Seconds)** - enter a numerical value in seconds.

Step 14 Under **Event Filtering: Rule Event Filtering**, click **Add**. Enter the following information:

- **Rule ID List** - Specify a comma-separated list of rule IDs.
- **Number of Events** - Manually enter a value of allowed number of events.
- (Available for the Rate type) **Time (Sec)** - enter a numerical value in seconds.

- **Type** - Select either Rate or Sample. Generated events are rate- or sample-limited based on the specified **Number of Events** triggered over a Timeevaluation interval (in seconds).

Step 15 Under the **Rule Setting List** section of the advanced settings, click **Add** and enter the following:

- **Source IP/CIDR List** - provide a comma-separated list of IPs or CIDRs
- **Rule ID List** - provide a comma-separated list of rule IDs. Note that for high number rules, only the rule ID is necessary. For low number rules, the GID and ID need to be specified for the rule ID as GID:ID. An example is 119:3.
- **Action** - Select an action for when the source IP/CIDR list or rule ID list is triggered on. Note that if a rule is suppressed, no action is taken and no logs are sent or captured.
  - **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.

What to do next

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

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

Procedure

Step 1 Navigate to **Policies** > **Profiles** > **Data Loss Prevention**.
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

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

Anti-Malware Profile

An anti-malware profile prevents malware attacks by scanning all incoming data to prevent malware from being installed and infecting a computer. Anti-malware programs can also detect advanced forms of malware and offer protection against ransomware attacks. Currently, the Talos ClamAV virus detection engine is a large portion of the profile. ClamAV® is an antivirus engine for detecting trojans, viruses, malware and other malicious threats.

If you opt to create an anti-malware profile, we **strongly** recommend immediately adding it to a policy by configuring it to a rule.

Create an Anti-Malware Profile

Procedure

Step 1 Navigate to **Policies** > **Profiles** > **Anti Malware**.

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 certain days if internal testing with that ruleset version fails.

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

What to do next

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

Web Application Firewall (WAF) Profile

Web protection profiles are a collection of Web Application Firewall (WAF) rules that can detect and block known web application attacks. You can configure WAF profiles to use signatures and constraints to examine web traffic. You can also enforce an HTTP method policy, which controls the HTTP method that matches the specified pattern. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.

Table 2: Supported WAF rule sets

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.

Note that the WAF profile does not include malicious IPs. See Malicious IP Profile, on page 18 and Network Intrusion (IDS/IPS) Profile, on page 4 for more information.

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.

Procedure

Step 1 Navigate to **Policies** > **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

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

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.

Procedure

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

Layer 7 DOS

A Layer 7 DoS (Denial of Service) profile is a network security configuration designed to protect applications and services from application Layer 7 denial-of-service attacks. Unlike traditional network-layer DoS attacks, Layer 7 attacks exploit the application layer, making them more complex and harder to detect. A Layer 7 DoS profile can be specifically tailored to identify and reduce these complex attacks.

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 provide DoS protection for backend web servers hosting API services.

Procedure

Step 1 Navigate to **Policies** > **Profiles** > **Layer 7 DOS**.

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.
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:

Procedure

Step 1 Navigate to **Policies** > **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

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

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.

Use FQDN filtering to filter categories that you want to allow or deny based on criteria, after a rule match. You can set filters at a granular level. The FQDN filter rows contain log-related actions such as deny or allow that you can use.

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:

Procedure

Step 1 Navigate to **Policies** > **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

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

Create a Group FQDN Filter Profile

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

Procedure

Step 1 Navigate to **Policies** > **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

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

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 18.

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:

Procedure

Step 1 Navigate to **Policies** > **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 certain days if internal testing with that ruleset version fails.

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.

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.

(Preview Only) Identity Profile

The primary purpose of an Identity Profile is to identify and authenticate users or devices attempting to access the network to ensure that only authorized users can gain access to network resources. Once a user or device is authenticated, the Identity Profile helps enforce security policies based on the identity of the user or device.

Create an Identity Profile

Use the following procedure to create an Identity profile:

Procedure

Step 1 Navigate to **Policies** > **Profiles** > **Identity**.

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 Use the drop-down menu to select your **Provider** type:

- **AFDS** - Active Directory Federation Services (AFDS) is a service provided by Microsoft that allows for single sign-on (SSO) and identity federation across different applications and systems; selecting this configures the system to use AFDS for handling authentication and identity management tasks.
- **OKTA** - Selecting OKTA as your provider implies organizations can streamline identity management processes and enhance security. This is an ideal cloud-based configuration point for environments that require scalability and stringent security requirements.

Step 6 Enter a valid **IDP Redirect URL**.

Step 7 Enter a vlid **SAML Portal URL**.

Step 8 Copy and paste your **SAML Certificate** into the text field provided.

Step 9 Manually enter the following User Attributes in SAML Message configuration:

- **Attribute Display Name**.
- **Attribute Group Name**.
- **Attribute Department Name**.
- **Attribute Email**.

Step 10 (Okta only) The **Okta API access management** is Okta's identity management platform that provides secure and centralized management of API access and authorization. Manually enter the following configuation:

- **API Endpoint**.
- **API Key Name**.
- **API Key**.

Step 11 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) User Profile

User Profiles help in defining what resources a user can access and what actions they can perform. With a User profile added to a policy rule or ruleset, it can enforce security policies such as authentication methods, session timeouts, and encryption requirements.

Create a User Profile

Use the following procedure to create a User profile:

Before you begin

We recommend having at least **one** Identity profile already created prior to creating a user profile, although it is possible to create an identity profile within this procedure.

Procedure

Step 1 Navigate to **Policies** > **Profiles** > **User**.

Step 2 Click **Create**.

Step 3 Provide a unique **Name**.

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

Step 5 Use the drop-down menu to select the desired **Identity profile** to pair with this User profile. If you do not have any Identity profiles configured already, select "Create Identity profile".

Step 6 In the User table, click **Add** to add additional entries to associate more users to this profile. Manually enter a first and last name with a valid email address.

To **Remove** a user from the table, click the checkbox beside the row of the user you want to remove and then click "Remove" at the top of the table.

Step 7 (Optional) Scroll down to view the Groups table. Click **Add** to add additional entries to associate a group of users to this profile. Manually enter the name of the group.

To **Remove** a group of users from the table, click the checkbox beside the row of the group you want to remove and then click "Remove" at the top of the table.

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.

AI Guardrails Profile

This profile is required for those who have enabled AI Defense and integrated it with their Multicloud Defense tenant. Guardrails (security rules and policies) are applied across different use cases; this profile allows you to configure a security profile within Multicloud Defense that is a direct reflection of the guardrails available in the AI Defense policy. By configuring this profile you set up secure communication between Multicloud Defense and AI Defense to to allow the enforcement of the following types of AI guardrails:

- **Security guardrails** - The security guardrail detects attempts to override the LLM's internal safety and alignment rules via direct and indirect prompt injection. This guardrail also detects software code in the model endpoint interactions, reducing risks such as malicious code execution, and more.
- **Privacy guardrails** - Privacy attacks attempt to reveal sensitive information contained an ML model or its data. The privacy guardrail detects personal, confidential, or sensitive information that can be cause harm if leaked to unauthorized parties. This guardrail detects Personally Identifiable Information (PII), Protected health information (PHI), and Payment Card Industry (PCI) data.
- **Safety guardrails** - Safety harms can encompass various categories, including user-specific, societal, reputational, and financial impacts. This guardrail examines prompts and responses to detect harmful language including toxic content, hate speech, harassment, profanity, sexual content and exploitation, messages driving social division and polarization, violence and public safety threats.

Create an AI Guardrails Profile

Use the following procedure to create an AI Guardrail profile:

Before you begin

You **must** have the following completed before you create this profile:

- Enable AI Defense for your Multicloud Defense tenant.

- Integrate and connect your Multicloud Defense tenant in the AI Defense dashboard.

Procedure

Step 1 Navigate to **Policies** > **Profiles** > **AI Guardrails**.

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 Log into your AI Defense dashboard and navigate to **Applications** > **Create Application** > **Add Connection** > **Generate API Token**. Generate an API integration key.

Step 6 In the Multicloud Defense's AI Guardrails profile page, enter the AI Defense **API Integration Key** into the appropriate text field.

Step 7 Expand the **Direction** drop-down menu and select **Response**.

At this time, **Prompt** is the only option supported.

Step 8 Expand the **Fallback Action** drop-down menu and select one of the options; this setting designates what the Multicloud Defense Gateway executes if it ever loses connection with AI Defense. If you do not have any preference, we recommend allowing

Step 9 Click through the three tabs for the following **Guardrail Details** and toggle the switch all the entities you want to enable:

- **Security Guardrail** - This selection protects against threats and unauthorized access.
- **Privacy Guardrail** - These selections protect against users and AI models from disclosing protected data to preserve user confidentiality.
- **Safety Guardrail** - These selections protect against harmful language including toxic content, hate speech, harassment, profanity, sexual content, exploitative language, and messages that promote polarization, violence, or public safety threats.

Note that you must click the toggle of the entity and then individually enable the features available for each entity. Enabling the entity alone does not include any of the listed features.

Step 10 Click **Save**.

What to do next

Attach the profile to a policy rule set. See Rule Sets and Rule Set Groups for more information.

Note At this time, AI Guardrail profiles only support **egress** gateways.

Optionally, observe and monitor your event logs for this particular AI Defense integration in the AI Guardrails Log page.