Network Threats

Anti-Malware

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

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

Step 2 Select **Anti-malware**.

Step 3 Provide a Name and Description.

Step 4 Click Manual or Automatic mode for Talos Ruleset Version selection

Step 5 In 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.

Step 6 In 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, 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 Select the desired Action to take when a match for a virus signature is found.

What to do next

Associate the AntiMalware Profile with a Ruleset

Check this document to create/edit rules

Data Loss Prevention (DLP)

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 data loss prevention (DLP) services.

The following steps will guide you through creating a DLP profile and associate it with a Policy Rule.

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 Name and Description for the profile.

Step 5 Enter the **DLP FIlter List** in the table. Click **Add** to insert more rows as needed

- Provide a description for the filter.
- Choose a predefined static pattern (e.g CVE Number) from the dropdown list or provide a custom Regular expression.
- Provide a count to define the number of times the pattern must be seen in the traffic.
- 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, but 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

Associate the Data Loss Prevention Profile with a Ruleset

Check this document to create/edit rules.

Network Intrusion (IDS/IPS)

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
Custom Rules	The Custom Rules are a particular set of Rules written by customers that provide a specialized level of protection for custom applications

Custom Rules

A Custom Rules Ruleset containing one or more Rules can be uploaded and used by the Multicloud Defense IDS/IPS security engine. The Rules contained within the Ruleset provide specialized application evaluations required by a customer for their specific applications and frameworks. The Custom Rules included in the IDS/IPS Profile will be evaluated first before evaluating any other Rulesets configured in the IDS/IPS Profile.

When uploading a Custom Rules Ruleset, the file should be a Gzip compressed TAR file with extension tar.gz. The compressed TAR file will consist of the following files:

- Readme File - File that gives a description of the Ruleset.
- Changelog File - File that represents the change history.
- Rules Folder - Folder that consists of one or more ModSecurity formatted Rules files. Each file must have an extension .conf. The folder must contain at least one Rule file (cannot be empty). Each file must follow the ModSecurity Rules format guidelines.

Upload Custom IDS/IPS Rules

Step 1 Navigate to **Manage** > **Threat Research** > **Network Intrusion**.

Step 2 Click the **Custom** tab.

Step 3 Click the **Import** button and upload the Custom Rules Ruleset file.

Create IDS/IPS Profile

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

Step 2 Click **Create Intrusion Profile** > **Network Intrusion**.

a) Specify the following general settings:

1. Specify a Profile Name and Description.
2. Specify the Action.
   - Specify a Profile Name and Description.
   - **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.
3. Specify whether to generate a Threat PCAP file if the IDS/IPS Profile detects malicious activity.

b) Specify the rule set.

Note 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 Rules 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 Rules so the IDS/IPS Profile will not be evaluated.

Talos Rules:

1. Specify *Disabled*, *Manual* or *Automatic**.
   - *Disabled* - Specify whether to disable the use of Talos Rules (see Tech Notes above).
   - *Manual* - Specify the Talos Rules *Version* to use.
   - *Automatic* - Specify the number of days from publish date to delay automatic update to the latest Talos Rules version.
2. Add specific Talos Rules Rulesets to the IDS/IPS Profile.

Custom Rules:

1. Specify *Disabled*, *Manual* or *Automatic**.
   - *Disabled* - Specify whether to disable the use of Custom Rules (see Tech Notes above).
   - *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.
2. Add specific Custom Rules Rulesets to the IDS/IPS Profile.

c) Specify the Advanced Settings:

Rules Suppression: Rules can be suppressed for a specific IP or a list of CIDRs.

1. Click **Advanced Settings** tab.
2. Under Rule Suppression, click **Add**.
3. For **Source IP/CIDR List**, provide a comma-separated list of IPs or CIDRs.
4. For **Rule ID List**, provide a comma-separated list of Rule IDs.
5. For **Action**, provide a selection, but this selection does not apply since a Rule being Suppressed will not be evaluated.

d) Specify event filtering:

To reduce the number of security Events that are generated when the IDS/IPS Profile is triggered, the Event Filtering 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:

- 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

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

Check this document to create/edit rules.