Rules

Add / Edit Policy Ruleset Rules

Note

- A single Policy Rule Set can have a maximum of 2047 Rules
- A Policy Rule Set Group can have a maximum combined set of 2047 Rules

Step 1 Navigate to **Manage** > **Security Policies** > **Rule Sets**.

Step 2 Click the Policy Ruleset name to view the Policy Ruleset.

Step 3 Click **Add Rule** to add a new Rule or select an existing Rule and click **Edit**.

Step 4 Specify or modify the following Rule information:

Parameter	Deonticity	Description
Name	Required	A friendly and unique name used to reference the Rule.
Description	Optional	A brief description of the Rule.
Type	Required	The Rule type (*Forwarding*, *ReverseProxy*, *ForwardProxy*).
Service	Required	The Service Object used to determine the protocols and ports for which the Rule will apply.
Source	Required	The Address Object used to determine the resources for which the Rule will apply.

Parameter	Deonticity	Description
Destination	Required	The Address Object used to determine the destination resources for which the Rule will apply. For ReverseProxy Rule type, the destination is always the Multicloud Defense Gateway. For ForwardProxy Rule types, the destination is always any.
Target	Required	The Address Object used to specify the destination for which the Multicloud Defense Gateway will establish a Gateway to Server connection. Applies only to ReverseProxy Rule types.
Action	Required	The Action to take when traffic matches the Rule's Source, Destination, and Service configuration. The Action defines whether the traffic should be allowed or denied, and whether the traffic should be logged or not logged in Events. Traffic is always logged in Traffic Summary, no matter whether the Action is set to Log or No Log. For traffic that is allowed by the Rule, the advanced security profiles will then be evaluated (AV, DLP, FQDN, IPS, MIP, URL, WAF). Each advanced security profile has its own Action that will either use or override this Action.
Reset On Deny	Optional	Applies only to Forwarding Rules. If enabled, the Multicloud Defense Gateway will send a TCP Reset packet for the sessions that matches this policy and is dropped by the Gateway.
Network Intrusion	Optional	The Network Intrusion (IPS) profile to be used for advanced security.Applies to all Rule types.
Antivirus	Optional	The Antivirus (AV) profile to be used for advanced security. Applies to all Rule types.
Data Loss Prevention	Optional	The Data Loss Prevention (DLP) profile to be used for advanced security. Applies only to ForwardProxy Rule types.

Parameter	Deonticity	Description
URL Filtering	Optional	The URL Filtering (URL) profile to be used for advanced security.Applies only to ForwardProxy and ReverseProxy Rule types.
FQDN Filtering	Optional	The FQDN Filtering (FQDN) profile to be used for advanced security.Applies to all Rule types.
Web Protection	Optional	The Web Protection (WAF) profile to be used for advanced security.Applies only to ReverseProxy Rule types.
Malicious IPs	Optional	The Malicious IPs (MIP) profile to be used for advanced security.Applies to all Rule types.
PCAP	Optional	Whether packet capture is enabled or disabled for the Rule. Whenever traffic matches a Rule with PCAP enabled, a packet capture of the session traffic will occur and the PCAP will be stored in the location specified by the PCAP profile. The PCAP profile is configured on the Multicloud Defense Gateway.

Step 5 After specifying the configuration for the Rule, click **Save**.

Step 6 Continue adding more rules. Once all desired Rules have been added, click **Save Changes**. You will be presented with a before and after view of all changes made to the Ruleset. If satisfied with your changes, click **Save**. If you need to make further changes, click **Cancel** to return to editing your Ruleset.

Edit, Clone, Delete, or Disable Rules

To Edit, Clone, Delete, or Disable a Rule, check the box for one and only one Rule and then click the button for the desired action. Remember to click **Save** after modifying the Rule to apply any changes made. This save action will only save the changes to the individual Rule. It will not save the Policy Ruleset as a whole. You must further click **Save Changes** to apply the Rule changes to the Policy Ruleset. You will be presented with a before and after view of all changes made to the Ruleset. If satisfied with your changes, click **Save**. If you need to make further changes, click **Cancel** to return to editing your Ruleset.