Malicious IP

Malicious IP

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 dynamically applied to a Policy Ruleset using the Automatic Update configuration of the Malicious IP Profile.

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 the Malicious IP Profile

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

Step 2 Click **Create**.

Step 3 Provide a name and description.

Step 4 Check the box to enable IP Reputation.

Step 5 Click Manual or Automatic mode for Trustwave Ruleset Version selection

Step 6 In Manual mode, select the *Trustwave Ruleset Version* from drop-down. 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.

Step 7 In Automatic mode, select how many days to delay the update by, after the Ruleset version is published by Multicloud Defense. New Rulesets are published frequently 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.

What to do next

Associate the Malicious IP Profile

Check this document to create/edit rules.

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 Rule, Malicious IP protection will be enforced. When unchecked and the Profile is attached to a Policy Ruleset Rule, Malicious IP protection will not be enforced. Our recommendation is to always check the IP Reputation checkbox for the Profile such that the Profile is enabled. If you want to disable the Malicious IP Profile, then remove its association from the Policy Ruleset Rule(s) rather than uncheck the checkbox.

Malicious IP Checker

Trustwave offers an online IP Reputation Service (https://rbladmin.marshal.com/) that can be used to check whether an IP address is listed as a Malicious IP.