Mixed Mode for WAF Policy

Avi Technical Reference (v18.2)

Mixed Mode for WAF Policy

view online

Overview

WAF Policy can be configured to operate in either detection only or in enforcement mode. With Mode Delegation introduced in Avi Vantage release 18.2.2, the policies can be enabled to operate in any of the following three modes:
* Detection * Enforcement * Mode Delegation

While in `Detection` mode, if a request matches a rule, then the request is flagged with an event log message and the request is allowed through.
While in `Enforcement` mode, if a request matches a rule, it is blocked by the Avi Service Engine, based on the defined action.

With `Mode Delegation`, WAF rules can overwrite the policy mode, where specific action can be defined for a single rule, irrespective of the action defined for the rule set. This is also referred to as the mixed mode, and allows fine tuning to avoid legitimate requests from being blocked, due to enforcement mode.

The following section discusses a few use cases relevant for enabling `Mode Delegation`:

Use Cases

1. Test new rules ? You can configure manually written rules or new CRS rule updates with mixed mode enabled to avoid false positives. You will be able to introduce new rules to operate in detection mode, so that legitimate requests are not rejected.

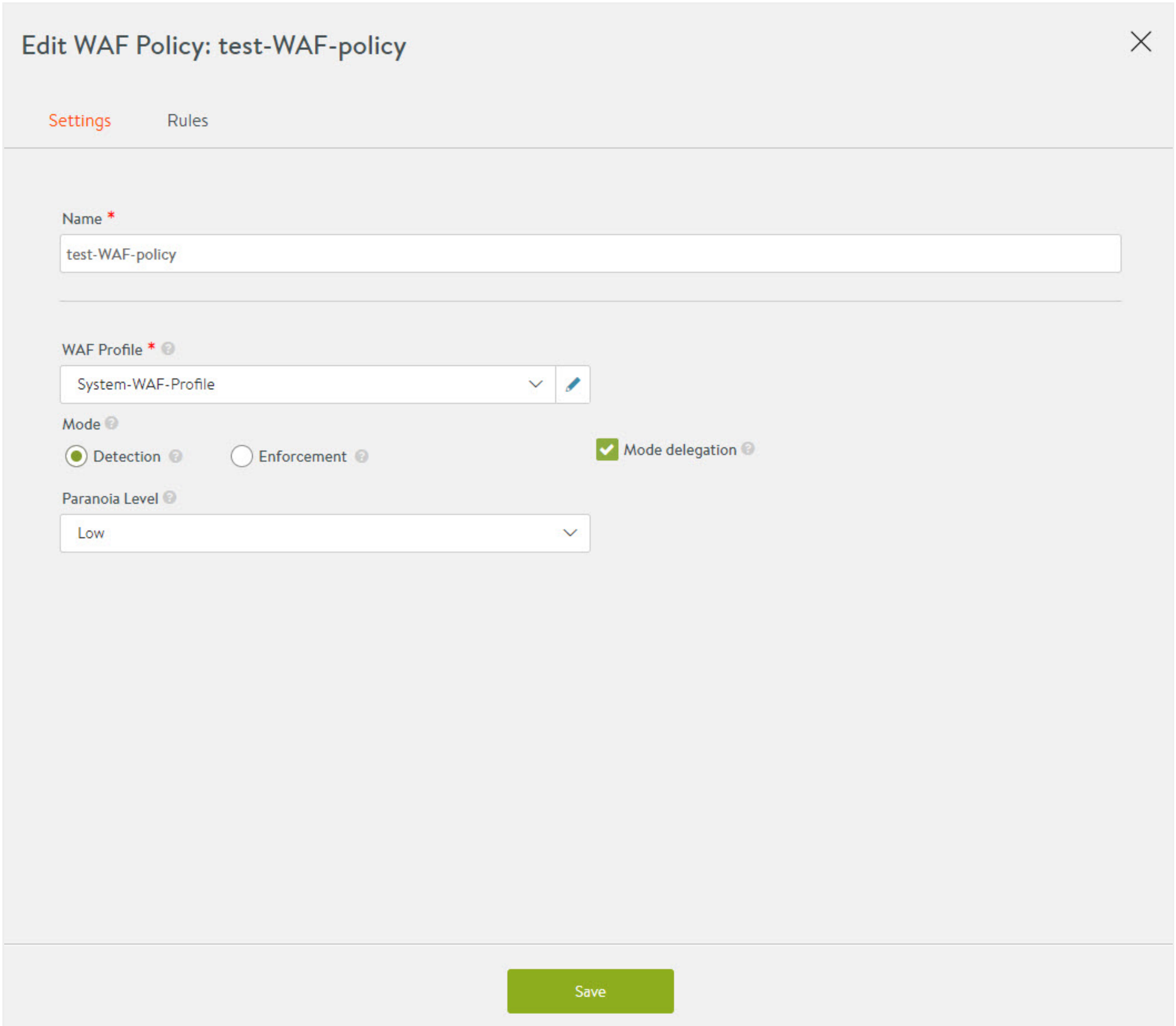
2. Partial detection ? You can configure a few rules in enforcement mode, while still retaining the policy in detection mode. With this you will not need to entirely enforce WAF implementation in detection mode.

3. Switch between two modes ? If your policy is in enforcement mode and is blocking all legitimate traffic, then you can switch the policy to detection mode for a while. After verifying legitimate traffic, you can switch back to enforcement mode. Mixed mode enables effective switching between the modes.

Enabling Mode Delegation

In Avi UI, navigate to Templates > WAF > WAF Policy. Click on the policy to be edited or create a new policy as required.

In the Settings tab, under Mode, click on the checkbox for Mode delegation to enable mixed mode.

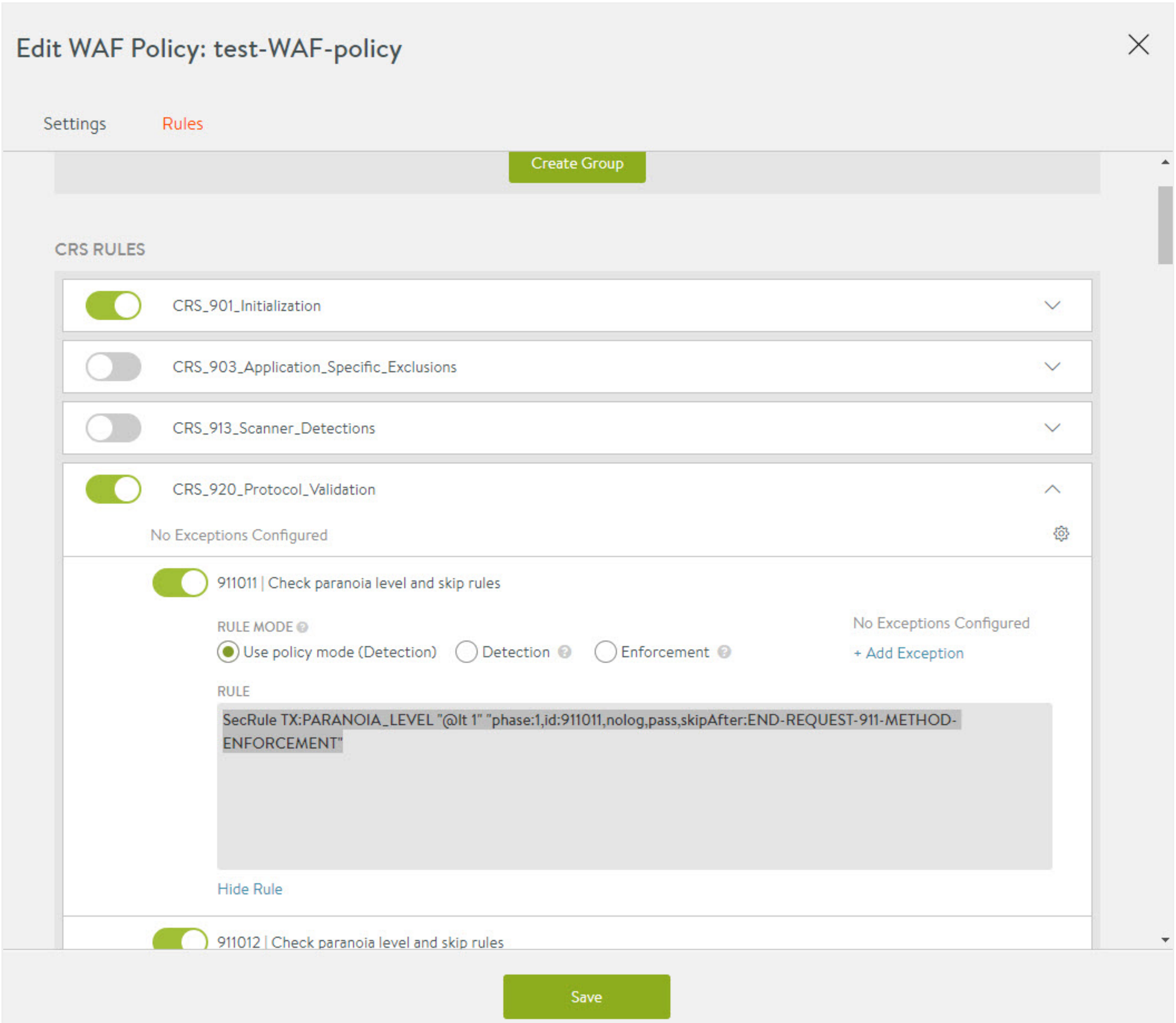


Enabling Policy Mode for a Rule

To enable policy mode (Detection) for a certain rule, navigate to the Rules tab and click on the dropdown for the selected rule.

Under RULE MODE, select the option for Use policy mode (Detection). This allows the selected rule to be in detection mode, even if the entire rule set is in enforcement.

Screenshot of an example where the `mixed mode` is selected, is as shown below.



Related Reading

[Positive Security](#)
[Whitelist](#)
[WAF Policy Signatures](#)