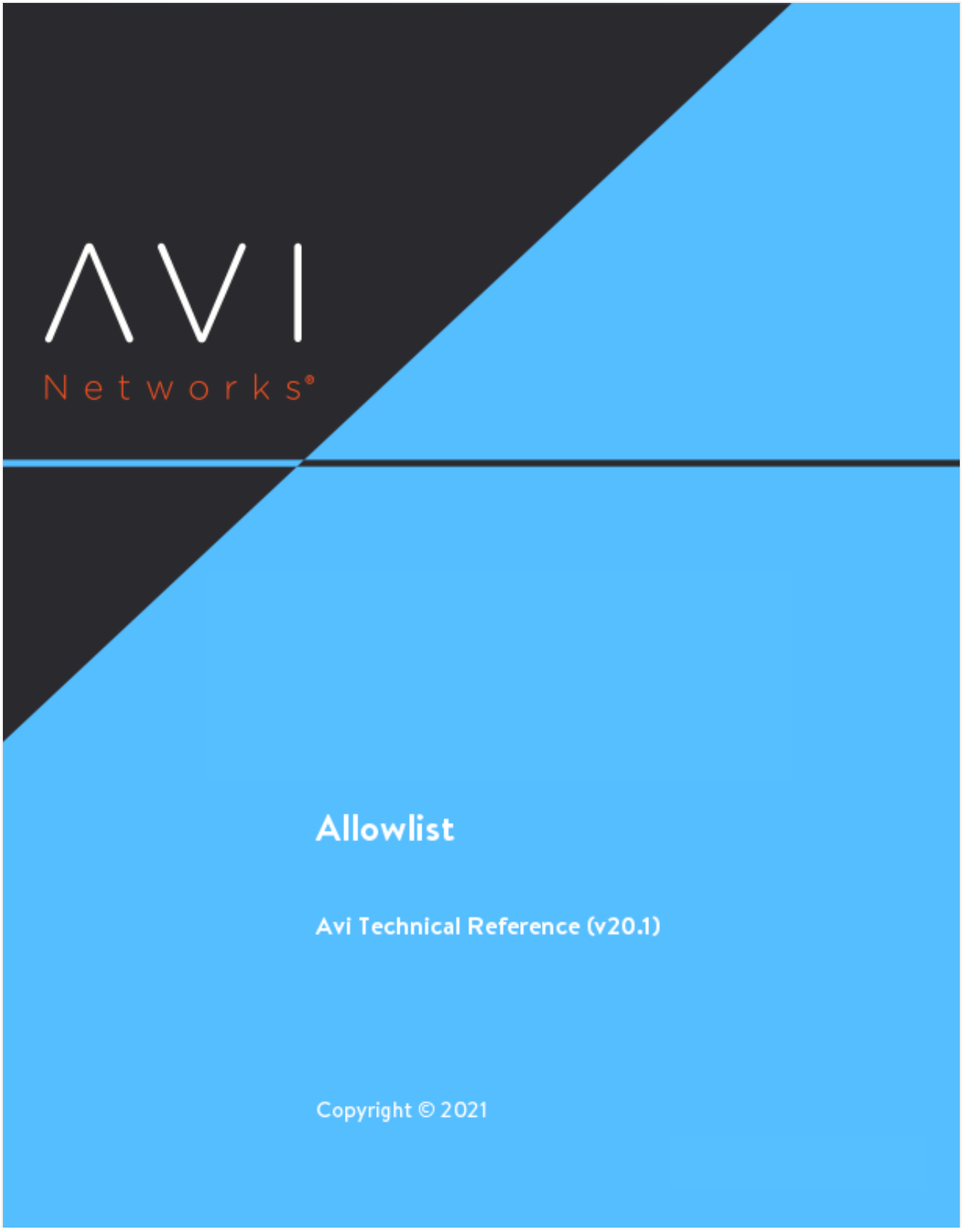



# Allowlist

Avi Technical Reference (v20.1)

# Allowlist

view online

## Overview

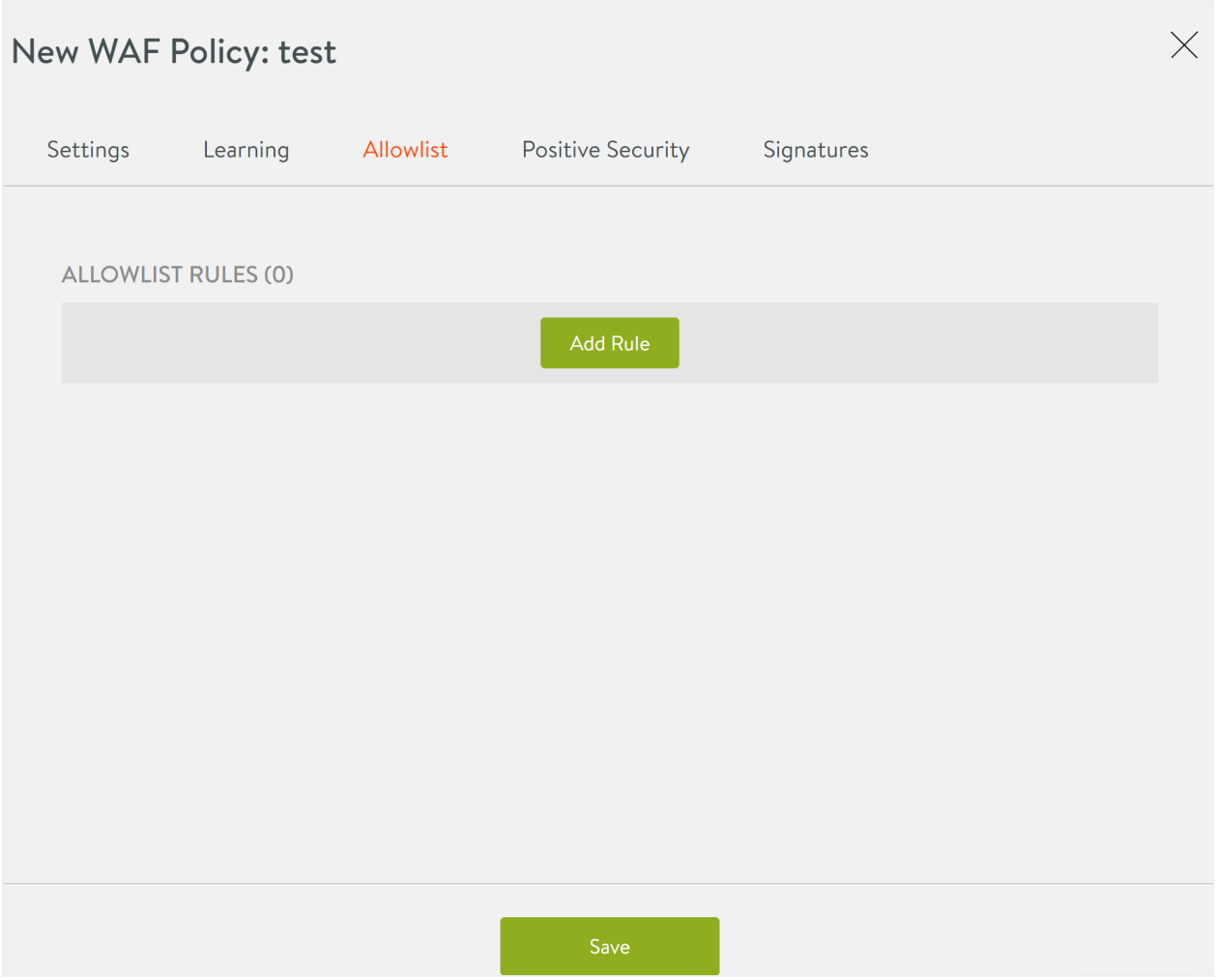
The Allowlist functionality allows the definition of match conditions for requests that will perform associated actions.

Examples
Directing WAF to not apply the WAF policy if: * The request comes from a specific IP range.
or
* The request matches the URL pattern specified using the HTTP Method match type.

Use cases
* Allow access from the internal network. * A security scanner that scans the application directly bypassing WAF protection. * Do not check special parts of the URL space, for example "/upload/*". * Run parts of the application in Detection mode.

## Configure Allowlist Rules

To define Allowlist rules, 1. From the Avi UI, navigate to Templates > WAF > WAF Policy and click on Create.
or
Edit an existing WAF Policy. 2. Enter the required details under the Settings tab. 3. Click on the Allowlist tab.




4. Click on the Add Rule button. 5. In the New Allowlist Rule screen, enter the details as shown below:

| General | |
|---|---|
| Field | Description |
| Rule Enabled | By default, the Allowlist rule is enabled. Click on the toggle button to disable it, if required. |
| Name | Enter a relevant name for the rule. |
| Description | Enter a description to define the rule. |

| Match | |
|---|---|

```
<td width="50%">Add Match Type</td>
<td width="50%">Select a <b>Match Type</b> from the options:<br>
```

- Client IP
- HTTP Method
- Path
- Host Header

Field Description

Action

Field

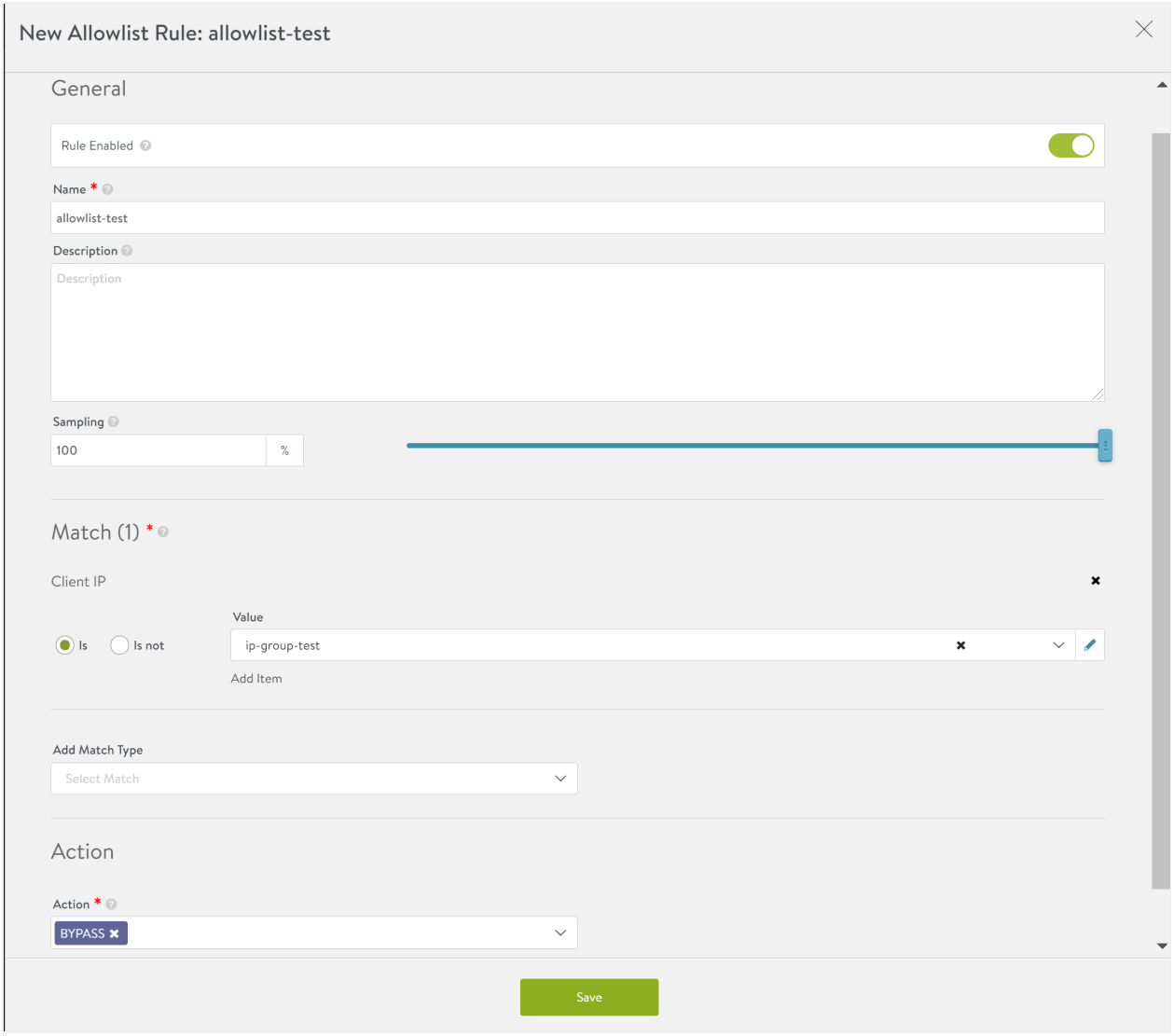
Description

From the following options, select the action to be performed when the request matches the criteria specified:

Action

- Bypass: When Bypass is selected, WAF does not execute any further rules. HTTP requests are considered safe and can be directly forwarded to the application
- Continue: Selecting Continue, stops the allowlist execution and directs WAF to continue its activity.
- Detection Mode: When set the WAF Engine will be set to Detection Mode for that request.

The New Allowlist Rule screen is as shown below:



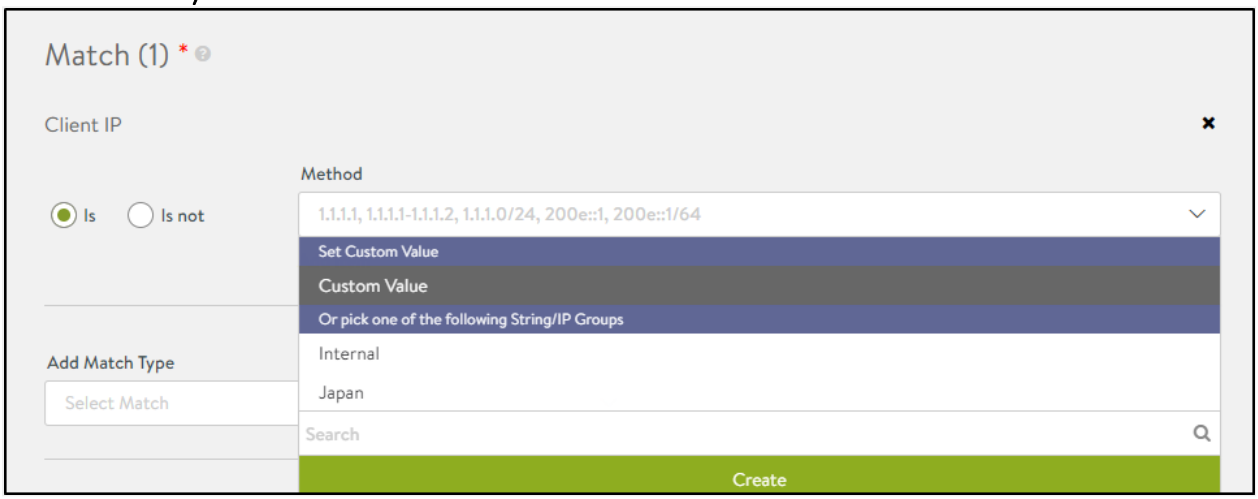
6. Click on Save.

## Match Types

### Client IP

Use this match type to provide access to only a trusted list of client IPs or client IP groups.

To enter the client IPs that can be allowed access, 1. Select the match type as Client IP under Add Match Type. 2. Select Is or Is Not to provide permissions accordingly. 3. Click on the drop down under Method. 4. Either select Custom Value and enter the IP Addresses manually or select Internal.




Note: This client IP match type supports IP Groups. Refer to the IP Group article to know more.

### HTTP Method

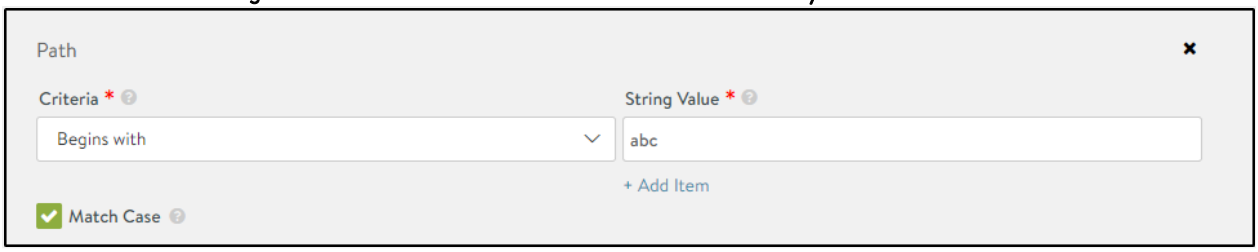
Use this to provide access to only specific types of HTTP requests using the HTTP request methods like Get, Connect, Delete, and more.

To define allowlisting rules based on HTTP methods, 1. Select the match type as HTTP Method under Add Match Type. 2. Select Is or Is Not to provide permissions accordingly. 3. Select the Methods as shown below:

**Path**

Use this method to approve traffic from specific websites by defining the parameters to be matched in the URL.

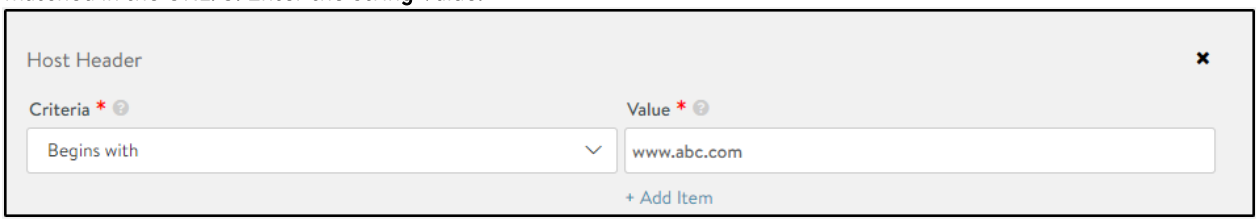
To allowlist URLs, 1. Select the match type as Path under Add Match Type. 2. Select the criterion that needs to be matched in the URL. 3. Enter the String Value. 4. Select Match Case to enable case sensitivity.




**Host Header**

Use this method to apply rules to only requests that match the specified host header criterion.

To allowlist host headers, 1. Select the match type as Host Header under Add Match Type. 2. Select the criterion that needs to be matched in the URL. 3. Enter the String Value.




## Sampling Traffic to WAF Allowlist

Sampling feature is used to enhance allowlist feature for the WAF traffic. It is useful when there is a requirement to expose only a particular percentage of traffic for WAF allowlisting. It is beneficial only if want to send a subset of all traffic through WAF. The `sampling_rate` flag is used to allot a range for each allowlist rule. The `sampling_rate` value can range from 0 to 100%.
If the request is in the sampling range, the configured action is applied to the request.
If the request is not in the sampling range,the configured action is not applied to the request. The request is skipped and the next rule will be applied.

### Examples

Example 1
Consider the following configuration: * Match client IP address: 1.2.3.4 * Sampling percentage: 10 * Action: CONTINUE

For all traffic whose client IP address is 1.2.3.4, 10% of them will run action CONTINUE(executing WAF), the other 90% of them will continue to the next allowlist rule.

Example 2
If the requirement is to subject 10% of traffic from a specific subnet other than the particular URI to WAF, the rules can be written like this:

- Rule : !x.x.x.x/x
- Sampling percentage: 100

- Action: allow

- Rule: uri_path
- Sampling percentage: 100

- Action: allow

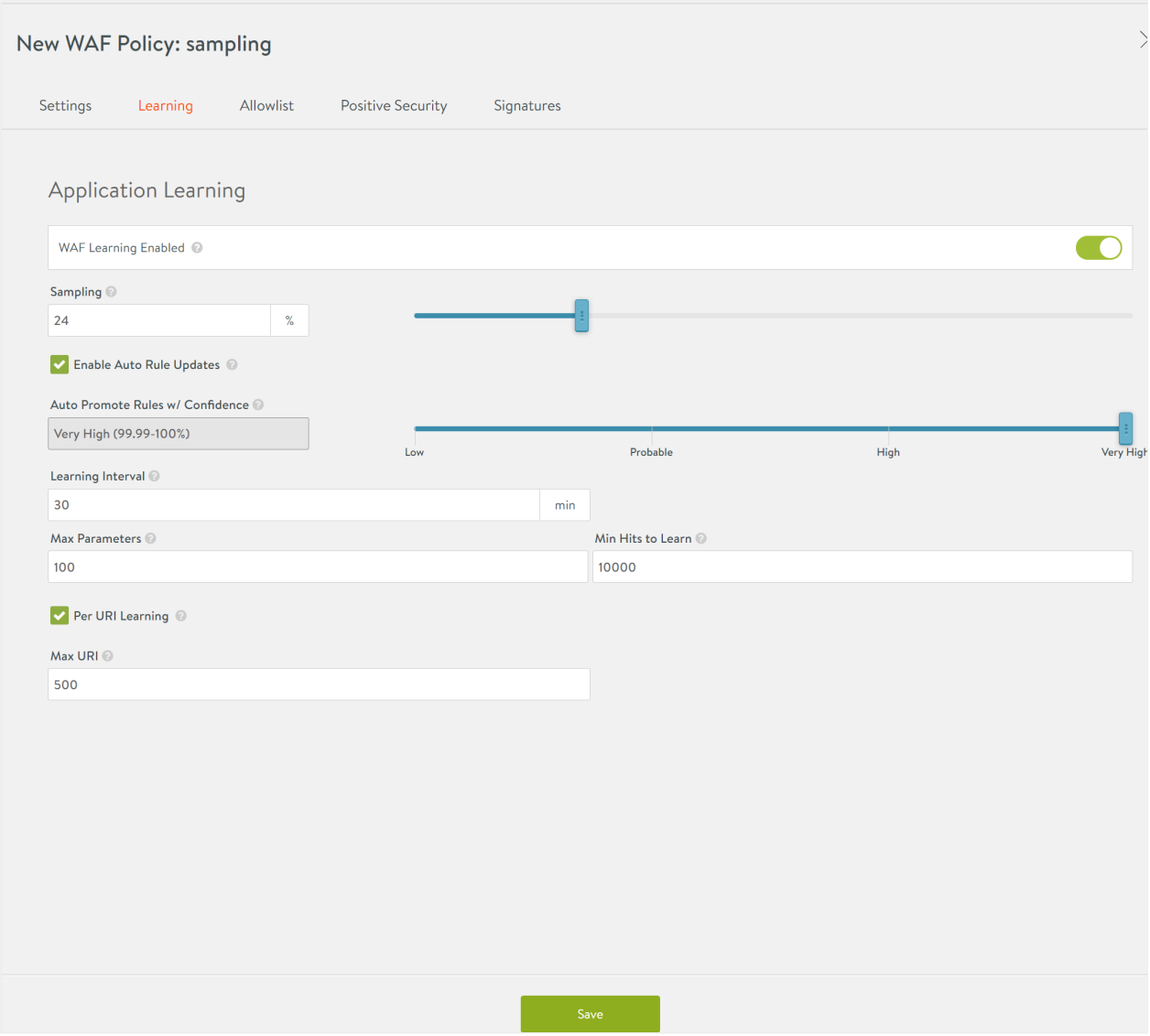
- Rule: All
- Sampling percentage: 90

- Action: allow

The request, which misses the above rules, will continue with WAF.

## Enabling Sampling

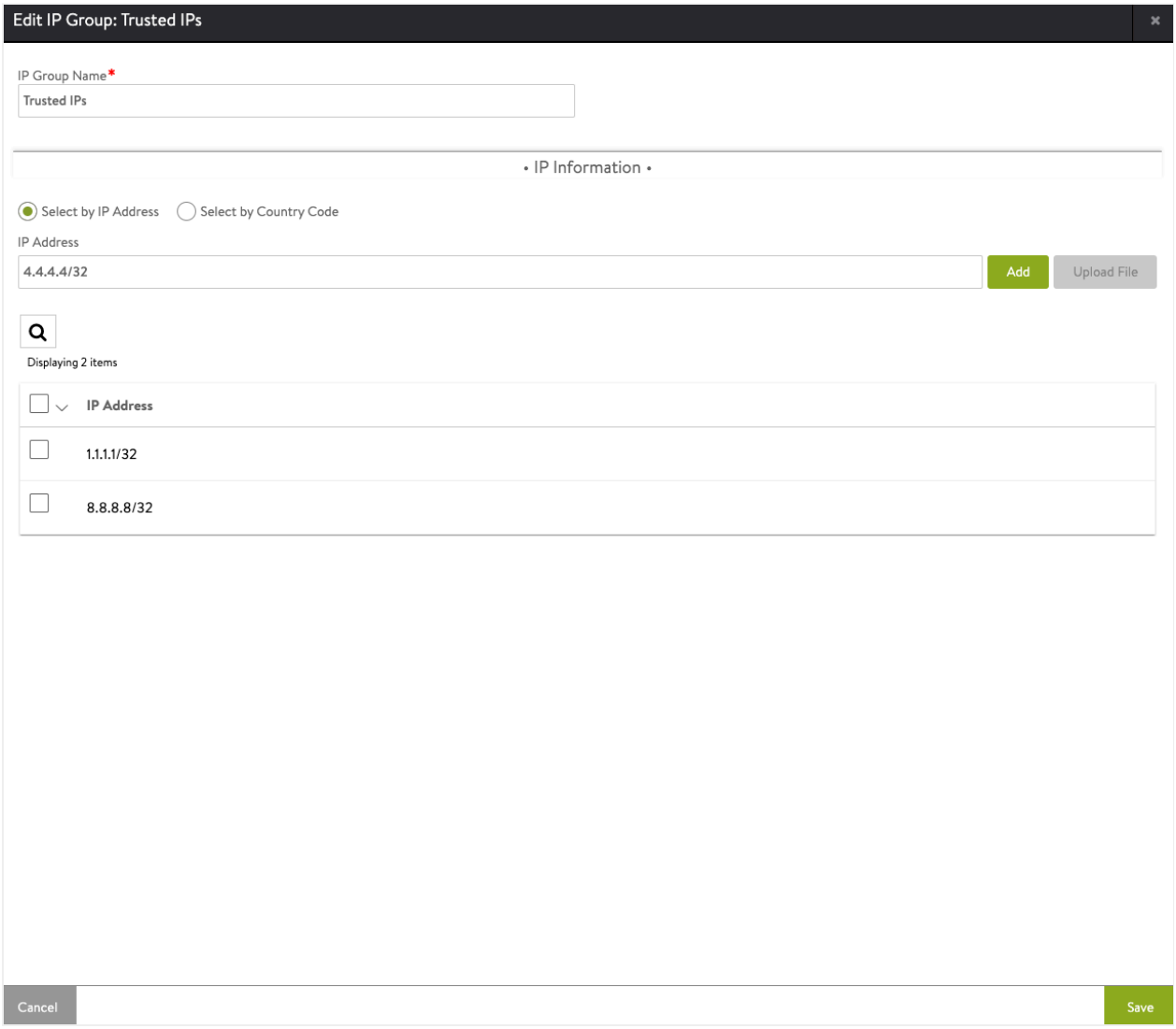
To enable sampling, navigate to Templates > WAF > WAF Policy and create a new policy as shown below.



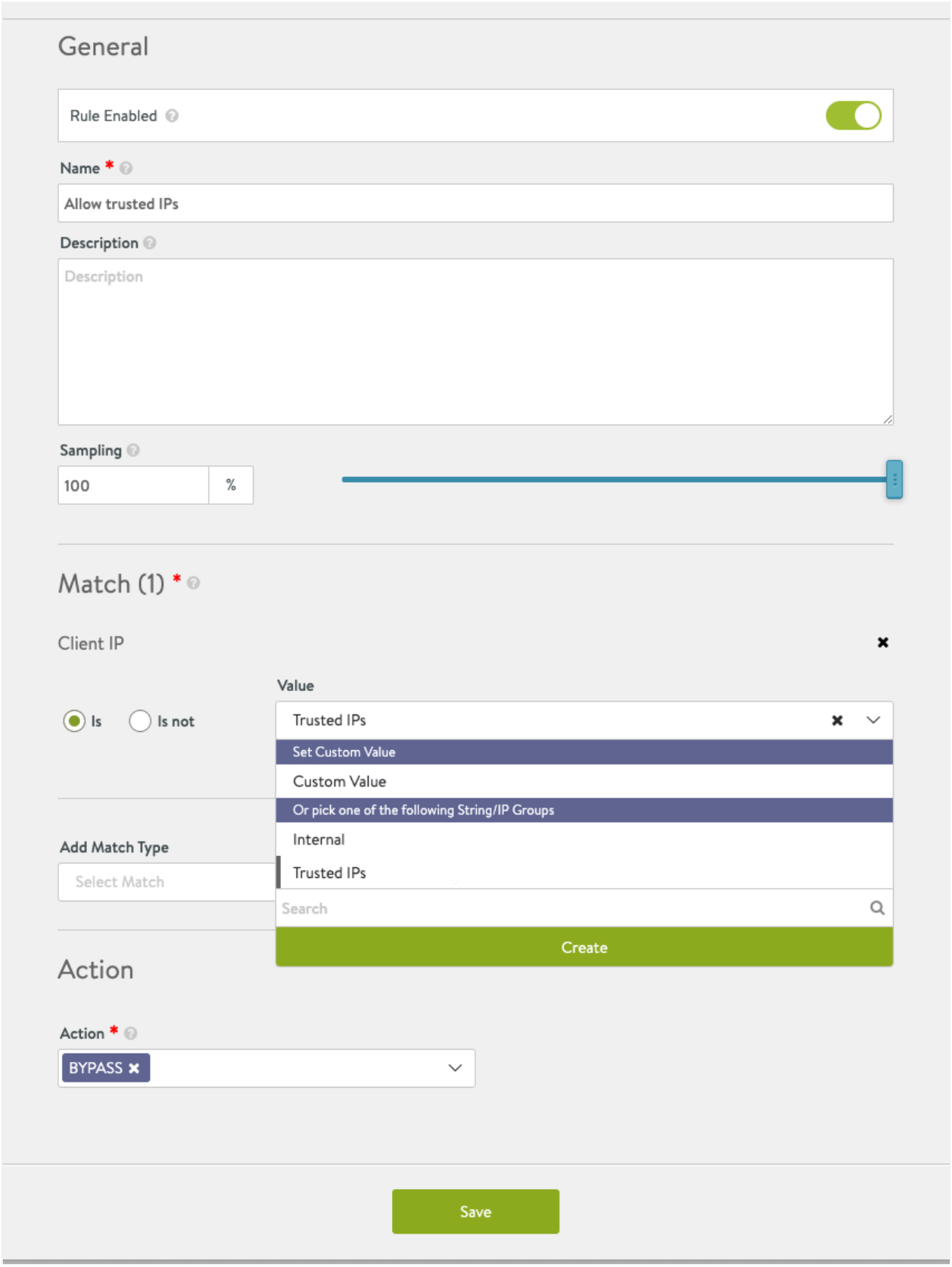
The above configuration is to achieve sampling for 24% of the traffic once it matches the configured rule. The rule configured here is to match the traffic for which the HTTP method is *COPY*.

## Partial Buffering for Chuncked Mode Encoding

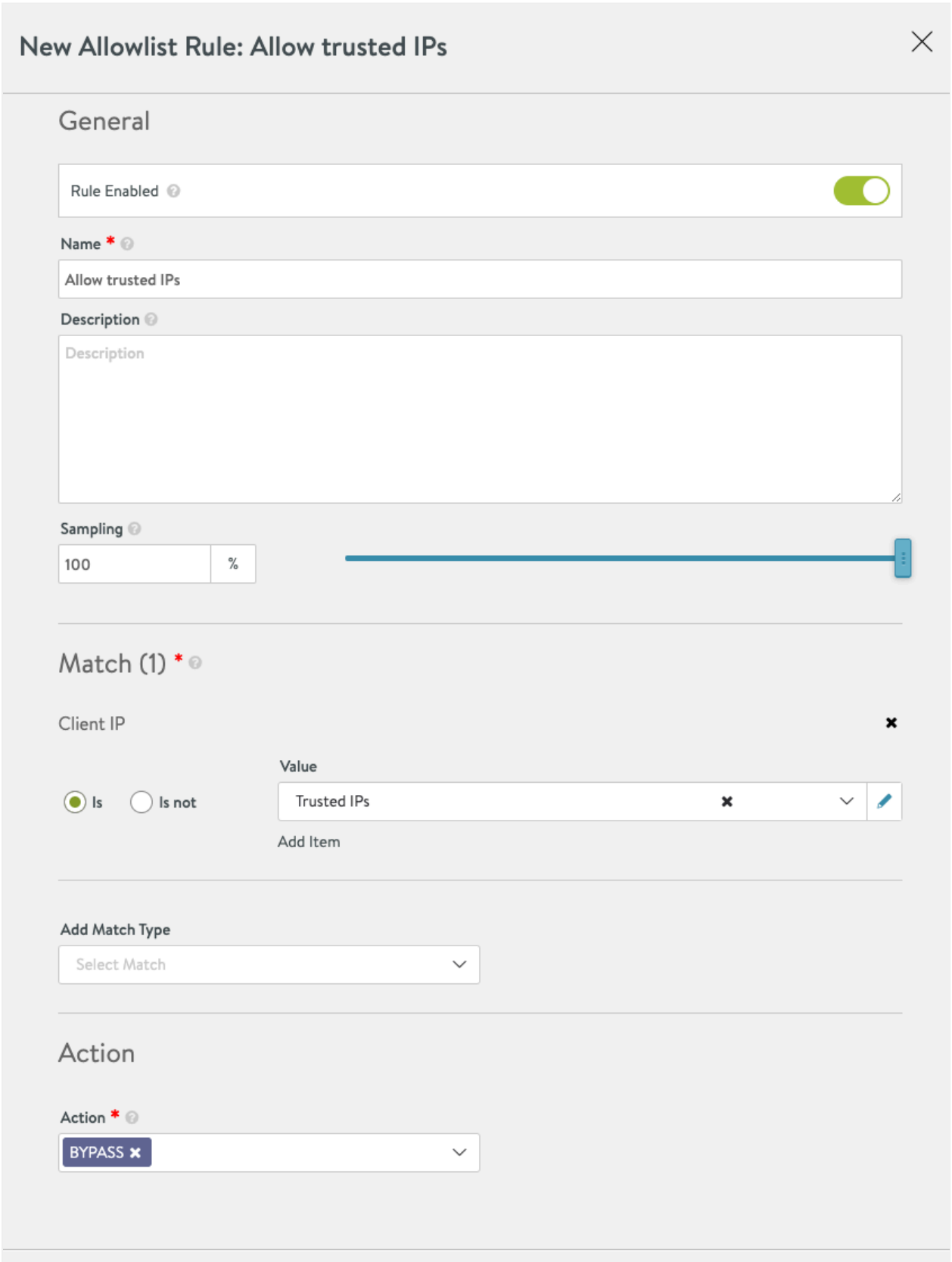
Prior to the Avi Vantage release 20.1.3, only full buffering for POST payloads with chunked-encoding was supported. Starting with Avi Vantage release 20.1.3, partial buffering for chunked-encoded payload is supported. The remaining payload is streamed while maintaining the original chunk boundaries sent from the client. ## Support for IP Groups in Allowlist Prior to Avi Vantage release 20.1.3, only ranges, prefixes or lists of IP addresses is supported while configuring allowlist. Starting with Avi Vantage release 20.1.3, configuration using IP groups is supported for allowlist. ### Configuring Using Avi Vantage This section explains how to configure an IP group and use it in a WAF allowlist for making all requests from IPs in the IP group called *Trusted IPs* bypass WAF checks. 1. Configure an IP group * Provide the required name * Use the *Select by IP Address* option and add the required IP address.

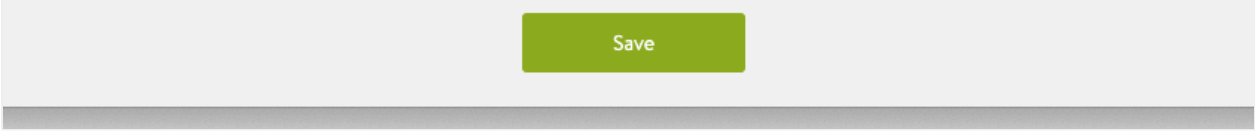



2. Select the IP group created in the previous step as the value for the Match option while creating a new allowlist rule.


General
Rule Enabled
Name *
Allow trusted IPs
Description
Description
Sampling
100
%
Match (1) *
Client IP
Is
Is not
Value
Trusted IPs
Set Custom Value
Custom Value
Or pick one of the following String/IP Groups
Internal
Trusted IPs
Search
Create
Add Match Type
Select Match
Action
Action *
BYPASS
Save

3. Select the desired action and save the WAF allowlist, as shown below.






4. The following shows a complete WAF policy using IP group. As shown below, action is set as *bypass* for any client IP address which is part of the IP address group created in the previous step.