Configure IPS Override

For supported software information, click here.

An intrusion prevention system (IPS) mitigates security vulnerabilities by responding to inappropriate or anomalous activity. Responses can include dropping data packets and disconnecting connections that are transmitting unauthorized data.

You commonly place an IPS system at the perimeter of a corporate network.

IPS performs the following types of vulnerability detection to help prevent attacks, including zero-day attacks such as worms or viruses:

- Signature-based detection—Signatures are a set of rules that a vulnerability profile uses to detect intrusive activities. With signature-based detection, a security profile compares a software or application pattern with a database of signatures, identifying malicious activity by matching patterns to those in the database. Versa security packs (SPacks) provide a set of predefined signatures, and you can also create custom signatures.
- Anomaly detection—Anomaly detection monitors a network for unusual events or trends. You configure the vulnerability profile that compares an observed event with the baseline of the normal traffic. Anomaly detection detects patterns that are normally not present in the traffic, so it is useful for detecting new attacks

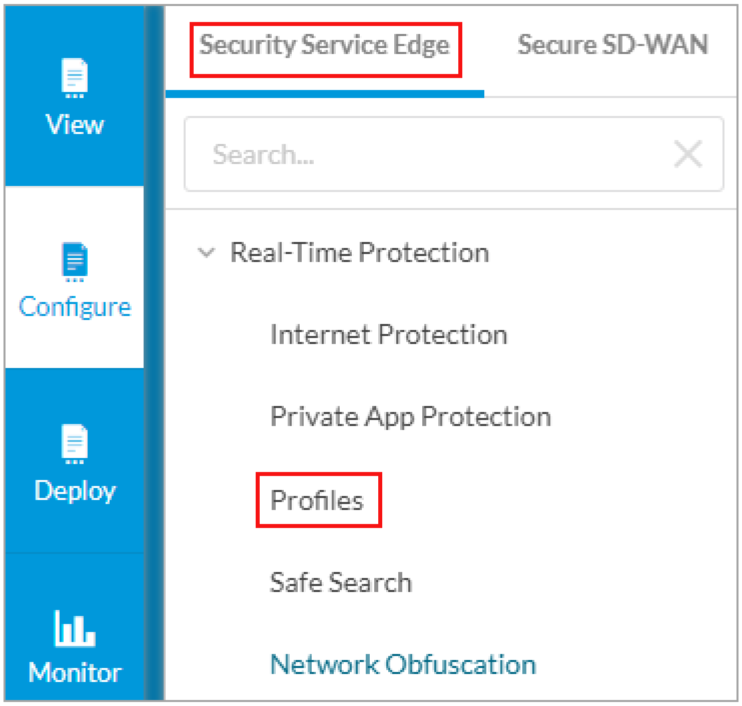
By default, Versa SASE provides a predefined IPS enforcement policy. This article describes how you can modify the parameters in the predefined vulnerability profile.

For more information about configuring custom IPS filtering profiles, see Configure Custom IPS Filtering Profiles.

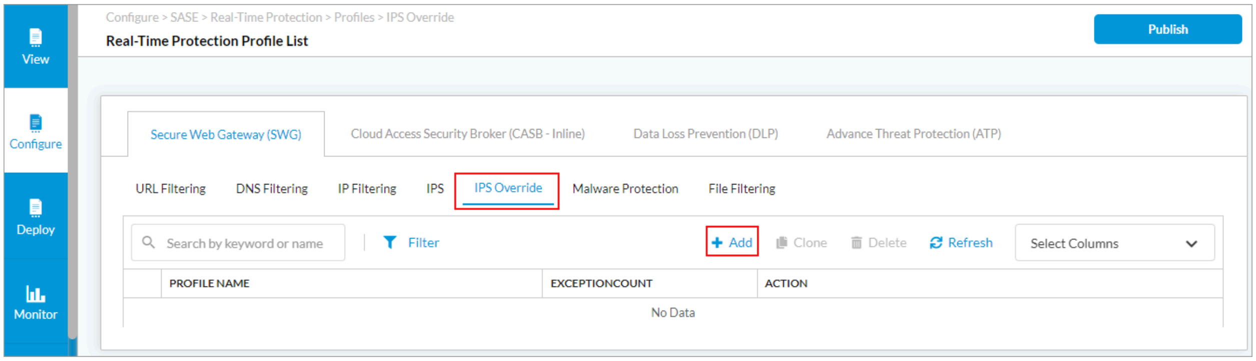
To modify the parameters in a predefined vulnerability profile, you create an override profile:

1. Go to Configure > Security Service Edge > Real-Time Protection > Profiles.

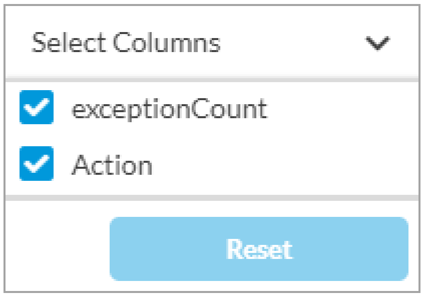
Copyright © 2024, Versa Networks, Inc.



The following screen displays:

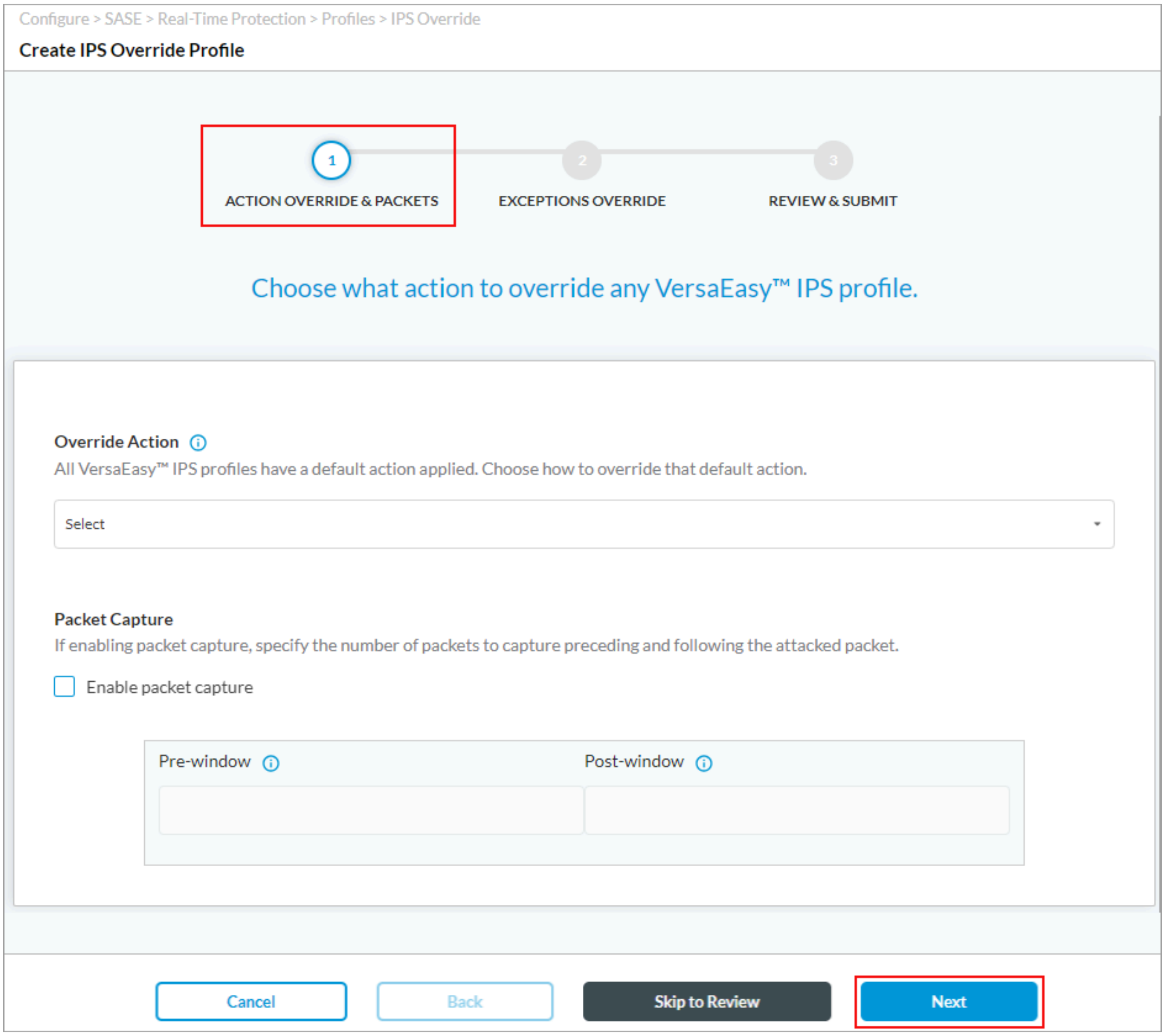

View
Configure
Deploy
Monitor
Configure > SASE > Real-Time Protection > Profiles > IPS Override
Real-Time Protection Profile List
Publish
Secure Web Gateway (SWG)
Cloud Access Security Broker (CASB - Inline)
Data Loss Prevention (DLP)
Advance Threat Protection (ATP)
URL Filtering
DNS Filtering
IP Filtering
IPS
IPS Override
Malware Protection
File Filtering
Search by keyword or name
Filter
+ Add
Clone
Delete
Refresh
Select Columns
PROFILE NAME
EXCEPTIONCOUNT
ACTION
No Data

2. Select the Secure Web Gateway (SWG) tab, and then select the IPS Override subtab.
3. To customize which columns display, click the Select Columns down arrow and then click the columns to select or deselect the ones you want to display. Click Reset to return to the default column display settings.



4. Click + Add to add a new IPS override profile. The Create IPS Override Profile screen displays. In Step 1, Action Override and Packets, enter information for the following fields.

Copyright © 2024, Versa Networks, Inc.



Configure > SASE > Real-Time Protection > Profiles > IPS Override

Create IPS Override Profile

Choose what action to override any VersaEasy™ IPS profile.

Override Action

All VersaEasy™ IPS profiles have a default action applied. Choose how to override that default action.

Select

Packet Capture

If enabling packet capture, specify the number of packets to capture preceding and following the attacked packet.

☐ Enable packet capture

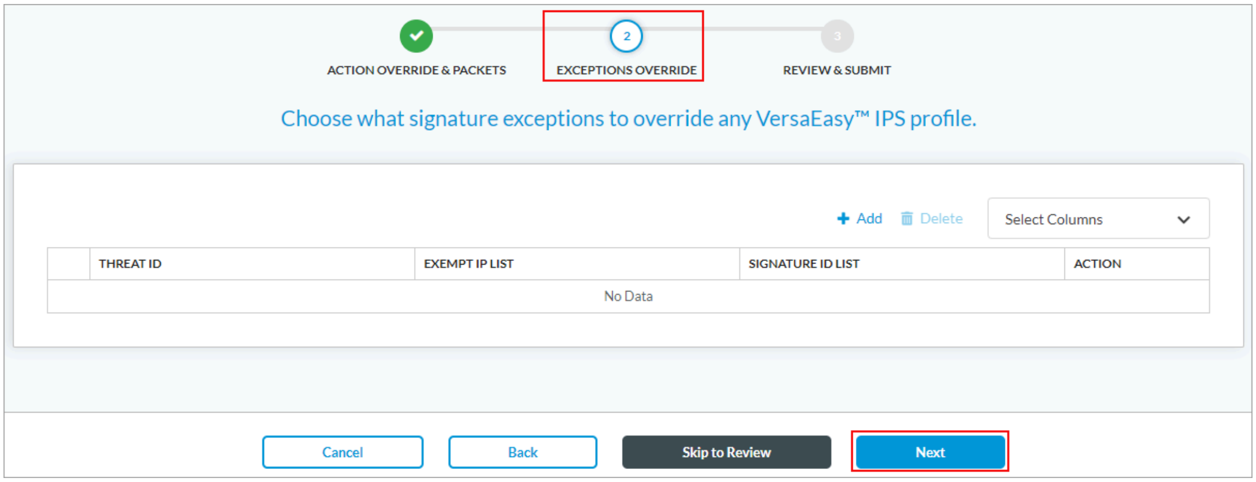
Pre-window

Post-window

Copyright © 2024, Versa Networks, Inc.

Field	Description
Override Action	Select an override action. This action overrides the action in the predefined vulnerability profile. ◦ Allow ◦ Alert ◦ Drop Packet ◦ Drop Session ◦ Reset Client ◦ Reset Server ◦ Reject
Packet Capture (Group of Fields)	Click to enable packet capture. Packet capture information is automatically sent to the Analytics node, where you can view and download it.
◦ Pre-window	Enter the number of packets immediately preceding the attacked packet that you want to capture.
◦ Post-window	Enter the number of packets immediately following the attacked packet that you want to capture.

5. Click Next to go to Step 2, Exceptions Override.

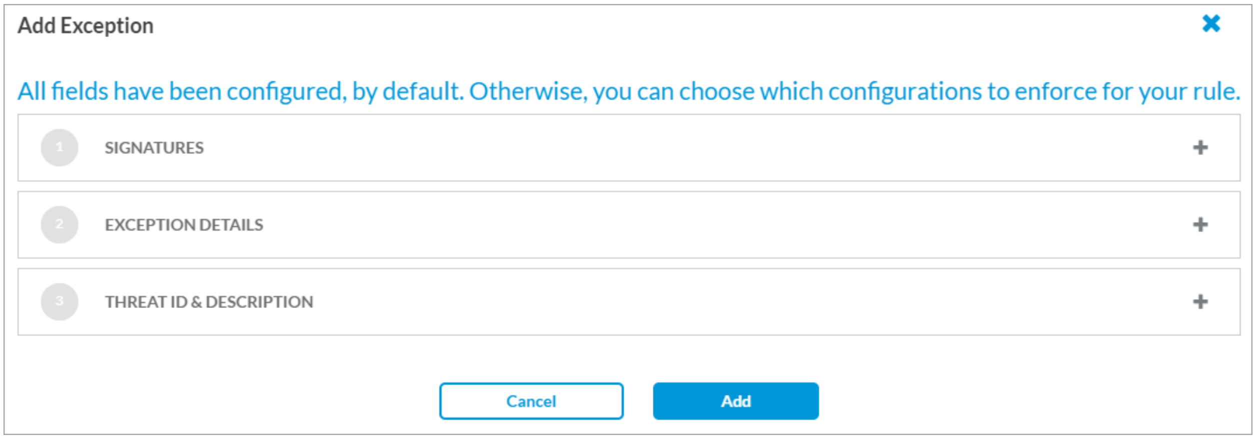


Choose what signature exceptions to override any VersaEasy™ IPS profile.

	THREAT ID	EXEMPT IP LIST	SIGNATURE ID LIST	ACTION
		No Data		

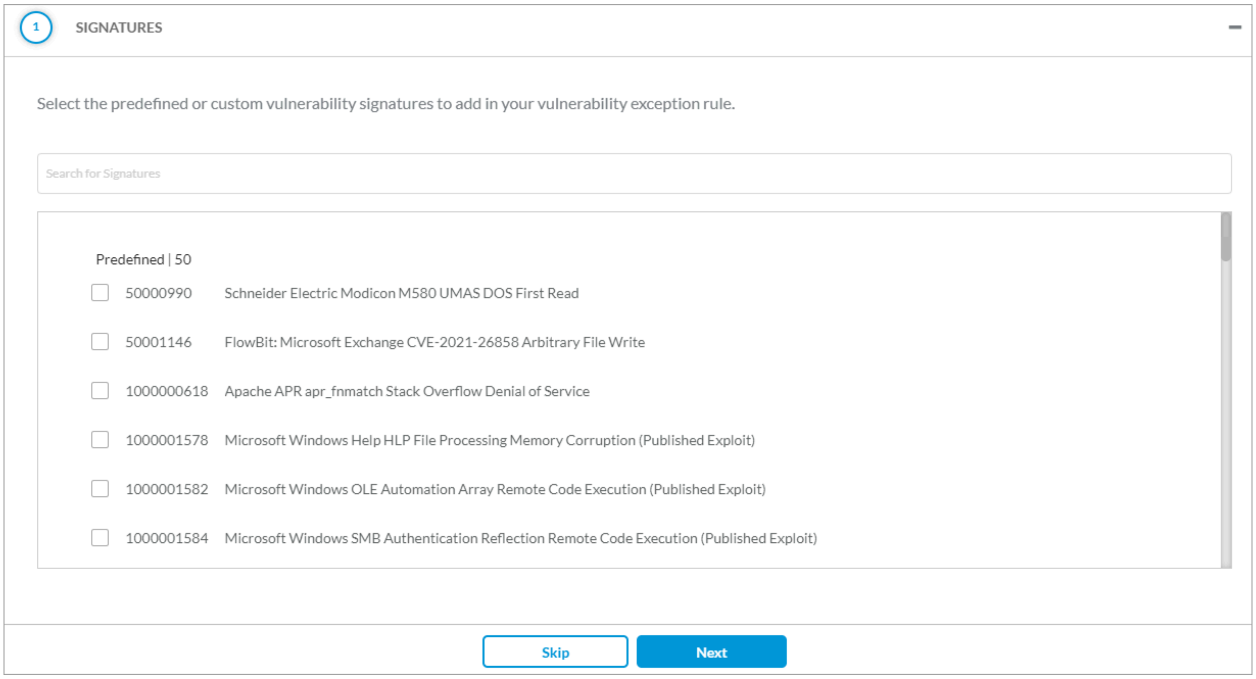
6. Click + Add. The Add Exception field displays.

Copyright © 2024, Versa Networks, Inc.



All fields have been configured, by default. Otherwise, you can choose which configurations to enforce for your rule.

7. In the Signatures section, click the + icon, and then select the vulnerability signatures to add to the vulnerability profiles exception rule.



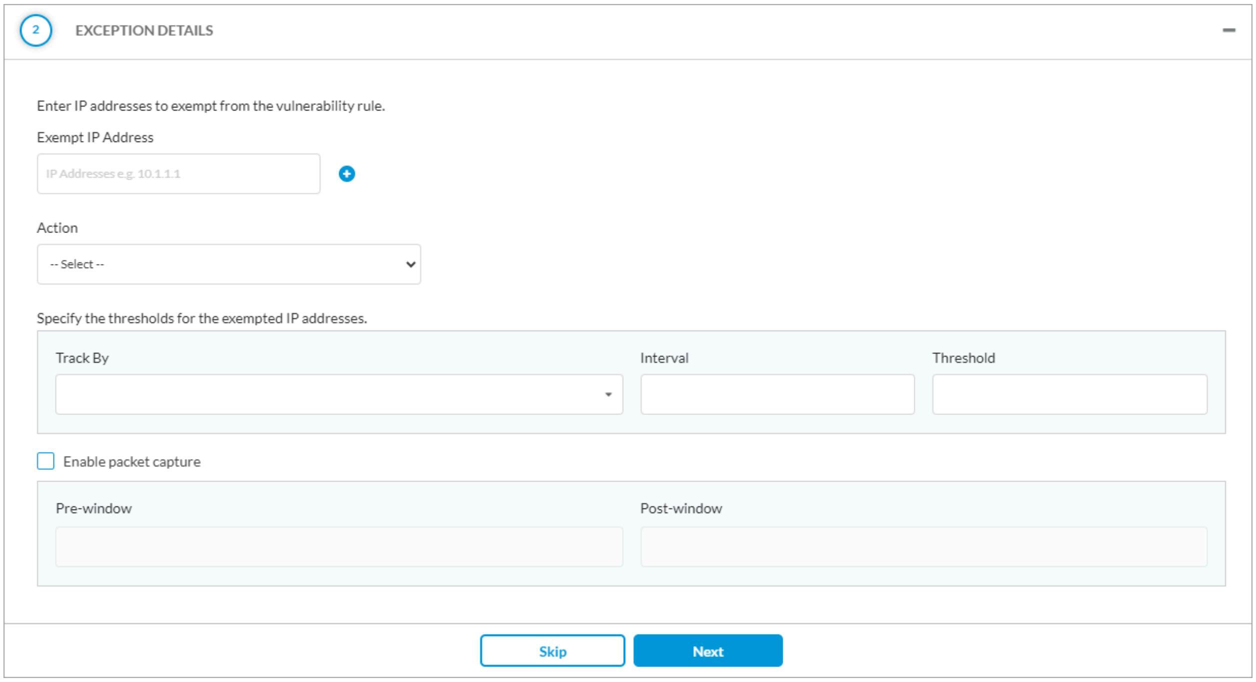
Select the predefined or custom vulnerability signatures to add in your vulnerability exception rule.

Predefined | 50

□	50000990	Schneider Electric Modicon M580 UMAS DOS First Read
□	50001146	FlowBit: Microsoft Exchange CVE-2021-26858 Arbitrary File Write
□	1000000618	Apache APR apr_fnmatch Stack Overflow Denial of Service
□	1000001578	Microsoft Windows Help HLP File Processing Memory Corruption (Published Exploit)
□	1000001582	Microsoft Windows OLE Automation Array Remote Code Execution (Published Exploit)
□	1000001584	Microsoft Windows SMB Authentication Reflection Remote Code Execution (Published Exploit)

8. Click Next. In the Exception Details section, enter information for the following fields.

Copyright © 2024, Versa Networks, Inc.



2 EXCEPTION DETAILS

Enter IP addresses to exempt from the vulnerability rule.

Exempt IP Address

IP Addresses e.g. 10.1.1.1

Action

-- Select --

Specify the thresholds for the exempted IP addresses.

Track By

Interval

Threshold

□ Enable packet capture

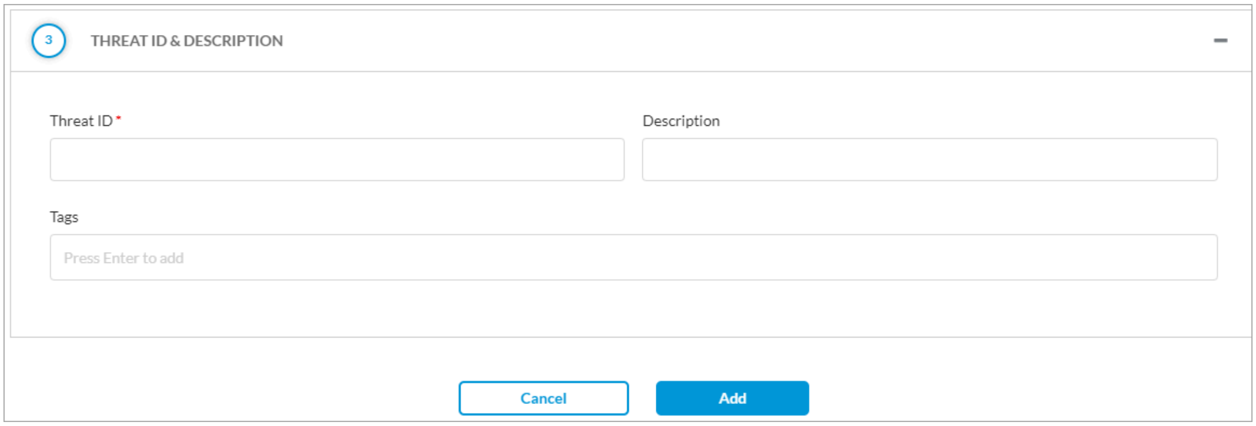
Pre-window

Post-window

Field	Description
Exempt IP Address	Click the + Add icon to enter the IP addresses that are exempt from the vulnerability rule.
Action	Select the action to take: ◦ Allow ◦ Alert ◦ Drop packet ◦ Drop session ◦ Reject ◦ Reset client ◦ Reset server
Threshold (Group of Fields)	Select the threshold application on the exempted IP address: ◦ Interval—Enter an interval, in seconds. ◦ Threshold—Enter the number of hits per interval based on the traffic direction. ◦ Track By—Select the threshold tracking based on either source address, destination address, or both source and destination addresses.
Packet Capture (Group of Fields)	Click Enable Packet Capture, and then enter the following information: ◦ Pre-window—Enter the number of packets immediately preceding the attacked packet that you want to capture. ◦ Post-window—Enter the number of packets immediately following the attacked packet that you want to capture.

9. Click Next. In the Threat ID and Description section, enter information for the following fields.

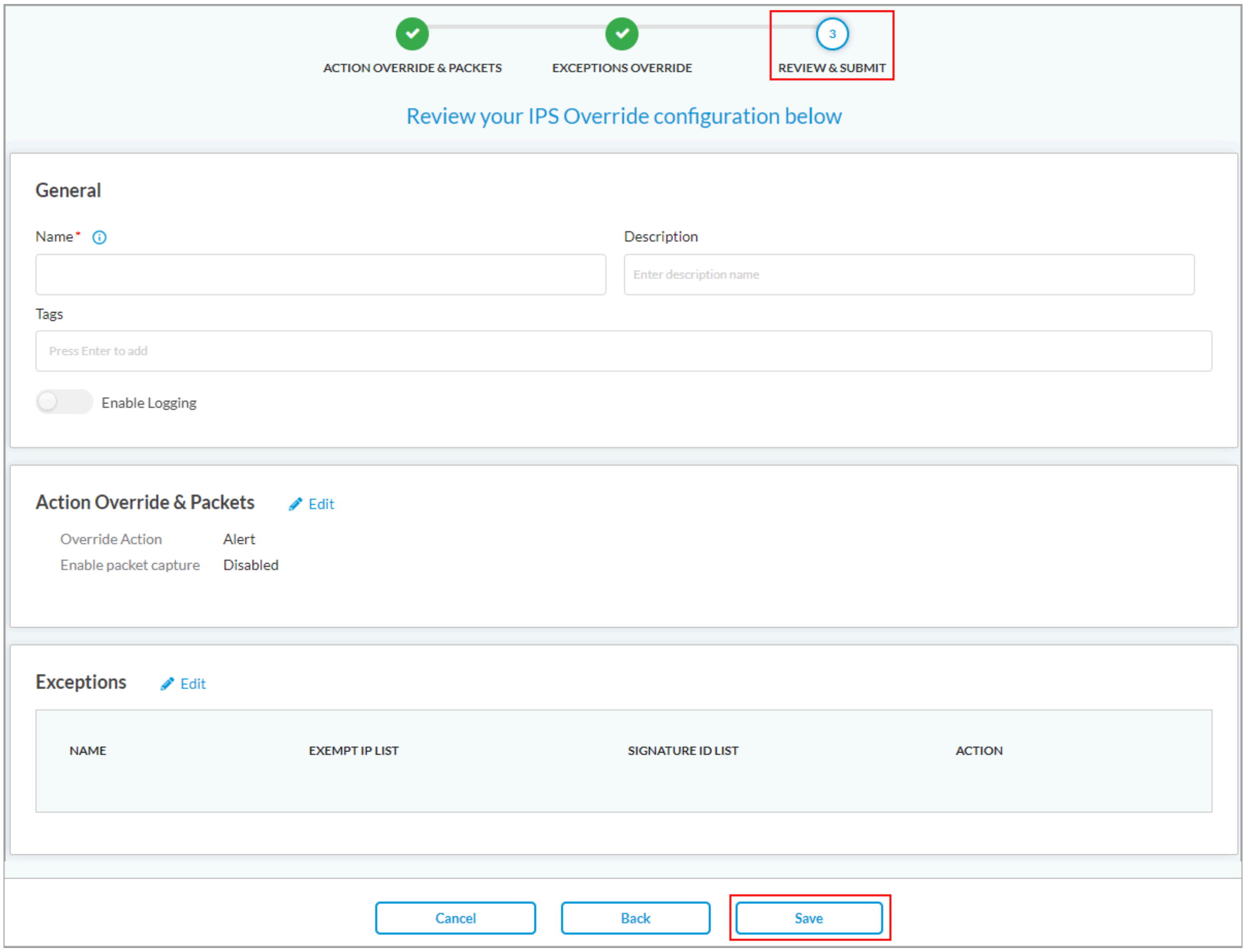
Copyright © 2024, Versa Networks, Inc.



Field	Description
Threat ID	Enter the threat ID.
Description	Enter a text description for the threat.
Tags	Enter a keyword or phrase that allows you to filter the threat exception. This is useful when you have many threat exceptions and want to view those that are tagged with a particular keyword.

10. Click Add.
11. Click Next to go to Step 3, Review and Submit.

Copyright © 2024, Versa Networks, Inc.



Review your IPS Override configuration below

General

Name*

Description: Enter description name

Tags: Press Enter to add

Enable Logging

Action Override & Packets

Override Action	Alert
Enable packet capture	Disabled

Exceptions

NAME	EXEMPT IP LIST	SIGNATURE ID LIST	ACTION

12. In the General section, enter a name for the IPS override profile and, optionally, a description and tags.
13. For all other sections, review the information. To make changes, click the ✎ Edit icon.
14. Click Save.

Supported Software Information

Releases 11.4.1 and later support all content described in this article.

Additional Information

[Configure Custom IPS Filtering Profiles]

Copyright © 2024, Versa Networks, Inc.