
Configure Custom IPS-Filtering Profiles

For supported software information, click [here](#).

The 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.

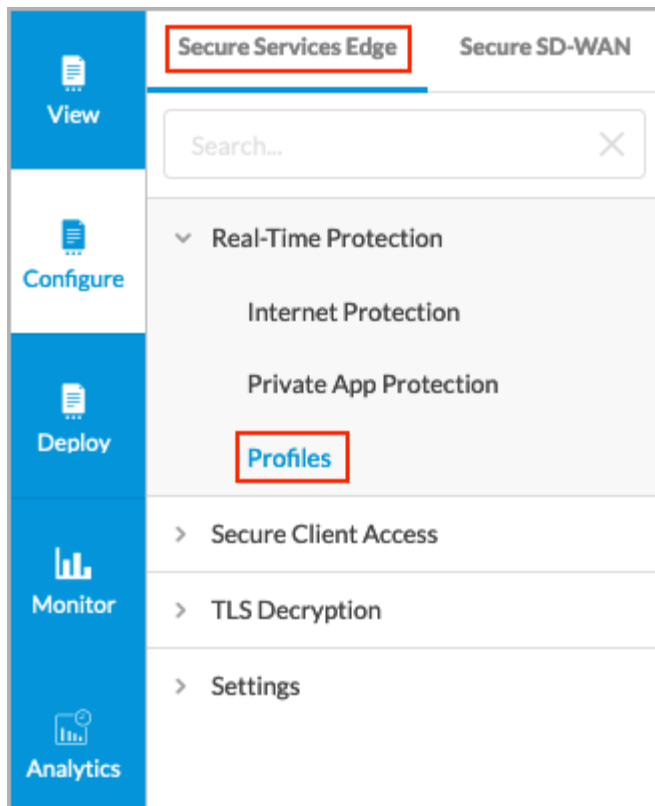
You commonly place an IPS system at the perimeter of a corporate network. IPS performs the following types of vulnerability detection to help prevent attacks, including zero-day attacks such as worms or viruses:

- 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

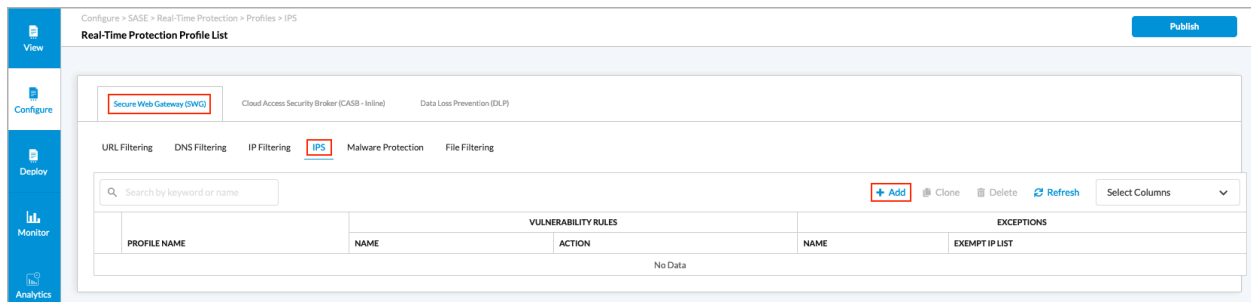
By default, Versa SASE provides a predefined IPS enforcement policy. This article describes how you can configure custom IPS-filtering profiles.

To configure a custom IPS-filtering profile:

1. Go to Configure > Real-Time Protection > Profiles.



The following screen displays.



2. Select the Secure Web Gateway (SWG) tab, and then select the IPS subtab.
3. Click + Add to add a new IPS-filtering profile. The Create IPS Profile screen displays.

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

Create IPS Profile

1 VULNERABILITY RULES
 2 EXCEPTIONS
 3 REVIEW & SUBMIT

By default, all rules have been configured. Otherwise, you can choose which rules to enforce for your IPS.

+ Add Delete Select Columns

| NAME | OS | PRODUCT | APPLICATION | ACTION |
|---------|----|---------|-------------|--------|
| No Data | | | | |

- To customize which columns display, click 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.

Select Columns

☒ OS
 ☒ Product
 ☒ Application
 ☒ Action

Reset

- Click + Add to add a new IPS profile. The Add Vulnerability Rule screen displays.

Add Vulnerability Rule

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

1 COMMON VULNERABILITIES AND EXPOSURES (CVE) & SIGNATURE SET

2 GENERAL

3 OS/PRODUCT

4 APPLICATION

5 REFERENCE/SEVERITY



6 ENFORCEMENT

7 NAME & DESCRIPTION

Cancel

Add

| Field | Description |
|---------------|---|
| Confidence | <p>Select one or more confidence levels to use to match the signatures.</p> <p><i>Range:</i> 0 through 9, unselected</p> <p><i>Default:</i> None</p> |
| Action Filter | <p>Select one or more action filters to use to match the signatures:</p> <ul style="list-style-type: none"> ◦ Alert ◦ Drop Packet ◦ Drop Session ◦ Reject |
| CVSS Score | <p>Select one or more CVSS scores to use to match the signatures.</p> <p><i>Range:</i> 1 through 10</p> |
| Class Type | <p>Select one or more class types of vulnerabilities to use to match the signatures.</p> |
| Direction | <p>Click to select the direction:</p> <ul style="list-style-type: none"> ◦ Both ◦ Client ◦ Server |
| Rule Type | <p>Click to select the rule type to use to match the signatures:</p> <ul style="list-style-type: none"> ◦ All Rules ◦ Anomaly Rules ◦ Signature Rules |

8. Click Next. In the OS/Product section, click Operating System Version and then select an operating system and operating system version to match for signatures. Click the  Plus icon to add an operating system; click the 

Minus icon to remove an operating system.

3 OS/PRODUCT



Select which operating systems and products to match for the signatures.

☒ Operating System Version ☐ Product

Operating System -- Select -- Operating System Version -- Select -- - +

Product -- Select -- Product Version -- Select -- - +

Skip Next

9. Click Product, and then select a product and a product version to match for signatures. Click the  Plus icon to add a product; click the  Minus icon to remove a product.

3 OS/PRODUCT

Select which operating systems and products to match for the signatures.

☐ Operating System Version ☒ Product

Operating System -- Select -- Operating System Version -- Select -- - +

Product -- Select -- Product Version -- Select -- - +

Skip Next

10. Click Next. The Application screen displays all predefined applications. Click an application to add it to the list of applications to match. Use the search box to find specific applications. You can include or exclude the selected applications by clicking the appropriate checkbox.

4
APPLICATION

1000010956

Autodesk

Citrix

Search for Application

Clear All
☒ Include the following applications
☐ Exclude the following applications

Predefined Applications (1444)

1000010917

✓

1000010942

✓

1000010955

✓

1000010956

✓

1000010957

✓

1000010973

✓

1000010975

✓

1000011212

✓

1000012279

✓

1000012280

✓

1000016052

✓

1000016053

✓

Skip

Next

11. Click Next, and then enter information for the following fields.

5
REFERENCE/SEVERITY

Select which reference values to match for the signatures.

Severity

References

-- Select --

Value

-- Select --

-

+

Skip

Next



| Field | Description |
|----------|--|
| Severity | <div>Select one or more severity-level match criteria:</div> <ul style="list-style-type: none"> Any Critical High Informational Low Medium |

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Concerto/Configure_Custom_IPS-Filteri...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_Custom_IPS-Filteri...)

Updated: Wed, 23 Oct 2024 08:39:47 GMT

Copyright © 2024, Versa Networks, Inc.

7

| Field | Description |
|------------|---|
| | ◦ Unspecified |
| References | Select and use signatures that match a specific reference type. Click the  Add icon to add the reference type to the rule. |
| Value | Select and use signatures that match a specific reference value. Click the  Add icon to add the reference value to the rule. |

12. Click Next. In the Enforcement screen, enter information for the following fields.

6

ENFORCEMENT

Select which action to enforce for the signatures.

Action

-- Select --

☒ Enable packet capture

Pre-window

Post-window

1

1

Skip

Next

| Field | Description |
|---|--|
| Action | <p>Select an enforcement action to apply to the signatures:</p> <ul style="list-style-type: none"> ◦ Default ◦ Predefined <ul style="list-style-type: none"> ▪ Allow ▪ Alert ▪ Deny ▪ Drop Packet ▪ Drop Session ▪ Reset Client ▪ Reset Server ▪ Reject ◦ Predefined-Persistent <ul style="list-style-type: none"> ▪ Versa_Action_Block_SIP ▪ Versa_Action_Block_SP ▪ Versa_Action_Block_DIP ▪ Versa_Action_Block_DP ▪ Versa_Action_Block_SIP_SP ▪ Versa_Action_Block_DIP_DP ▪ Versa_Action_Block_SIP_SP_DIP_DP ▪ Versa_Action_Block_SIP_SP_DIP_DP_Protocol |
| Enable Packet Capture (Group of Fields) | Click to enable packet capture. When enabled, packet capture logs are sent to Versa Analytics. |
| ◦ Pre-window | <p>Enter the number of packets immediately preceding the attacked packet that you want to capture.</p> <p><i>Range:</i> 0 through 10</p> <p><i>Default:</i> 1</p> |
| ◦ Post-window | <p>Enter the number of packets immediately following the attacked packet that you want to capture.</p> <p><i>Range:</i> 0 through 10</p> |

| | |
|--|-------------------|
| | <i>Default: 1</i> |
|--|-------------------|

13. Click Next, and then enter a name for the IPS profile and, optionally, a description and one or more tags. A tag is an alphanumeric descriptor, with no white spaces or special characters, that you can use to search the objects.

7
NAME & DESCRIPTION

Name * ⓘ

description

Tags

Cancel Add

14. Click Add to add the IPS profile.

Supported Software Information

Releases 11.3.1 and later support all content described in this article.

Additional Information

[Versa Concerto Overview](#)