

---

## Configure SASE Internet Protection Rules

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

Internet protection rules are firewall rules that are applied to internet-bound traffic on a per-tenant basis. They provide network protection by establishing match criteria and enforcement actions. To configure internet protection rules, you configure the following match criteria and enforcement actions, as described in this article.

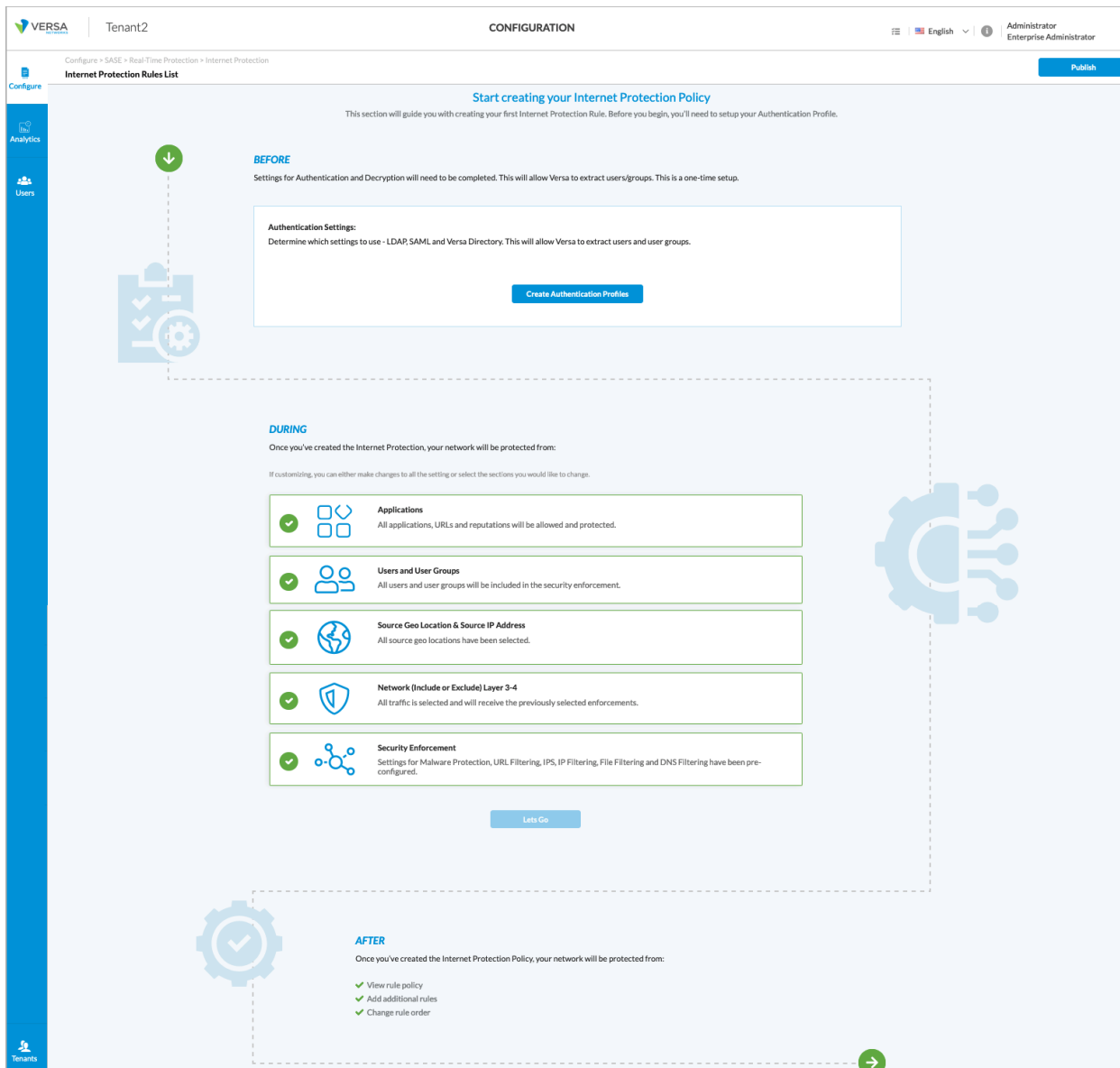
- Applications—Match criteria based on individual applications, groups of applications, categories of applications, predefined URL categories (such as business and economy, computer and internet security, and entertainment and arts), and predefined reputations (such as high and low risk).
- User and user groups—Match criteria based on individual users or groups of users.
- Source geolocation and source IP address—Match criteria based on the geographic location of source or destination traffic.
- Network Layer 3 and Layer 4—Match criteria based on the IP address of the source and destination traffic or on custom or predefined protocol-based services.
- Security enforcement—After you select the match conditions, you specify a security enforcement action, which is either allow, deny, or reject. You can also create custom security enforcement profiles in which you specify the enforcement criteria.
- Review and deploy—After you have configured match criteria and security enforcement actions, you review and then deploy the internet protection rule.

Note: You must configure the SASE rules, profiles, and settings in the following order:

1. Configure users and user groups first, and then publish them to the gateway. For more information, see [Configure SASE Users and Groups](#).
2. Configure site-to-site tunnels. For more information, see [Configure SASE Site-to-Site Tunnels](#).
3. Configure secure client access profiles and rules. For more information, see [Configure SASE Secure Client Access Rules](#).

You do not need to configure the remaining SASE rules, profiles, and settings in any particular order.

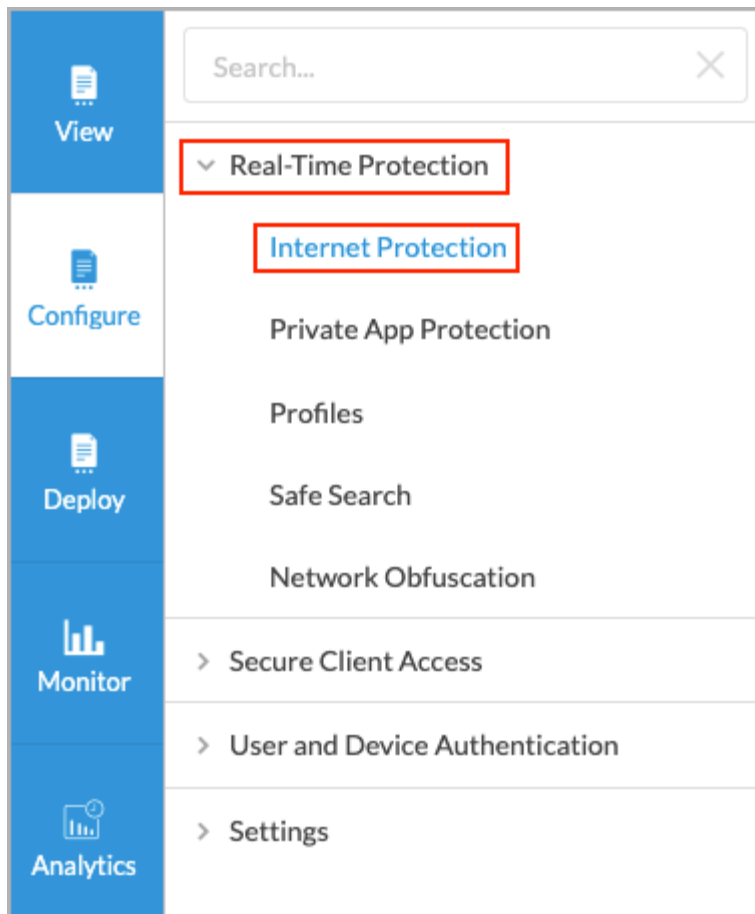
When you begin to configure your first internet protection policy, the following screen displays to guide you through the procedure:



## Configure SASE Internet Protection Rule Match Criteria

To configure internet protection rule match criteria:

1. Go to **Configure > Real-Time Protection > Internet Protection**.



The Internet Protection Rules List screen displays all configured internet protection rules.

View

Configure

Deploy

Monitor

Analytics

Inventory

Users

Settings

Tenants

Configure > SASE > Real-Time Protection > Internet Protection

Internet Protection Rules List

Publish

Below are all the rules for your Internet Protection Policy.

Q Search by keyword or name

Filter

Add

Clone

Reorder

Delete

Refresh

Select Columns

	Rule Name	Applications & URLs	Users	EIP	Source & Destination	Network Layer 3-4	Geo Locations
						Services	Source
<input type="checkbox"/>	Implicit_Drop_Quic	All Applications	All Users			<div>Services</div> <div>Implicit-QUIC-UDP-443</div>	All Source Geo Locations selected
<input type="checkbox"/>	Implicit-Allow-DNS	All Applications	All Users			<div>Services</div> <div>domain</div>	All Source Geo Locations selected
<input type="checkbox"/>	Implicit-Deny-All	All Applications	All Users			Layer 4 Services are not Enabled	All Source Geo Locations selected

Showing 1-3 of 3 results

10 Rows per Page

Go to page 1

< Previous

1

Next >

2. In the horizontal menu bar, you can select one of the following operations.

Add

Clone

Reorder

Delete

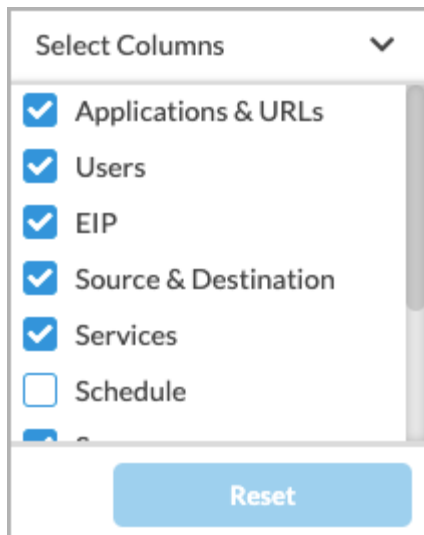
Refresh

Operation	Description
Add	Create a new internet protection rule. This button is active when no existing rule is selected.
Clone	Clone the selected internet protection rule. When you select this option, the configuration Review & Deploy screen selected. You can rename the default name of the cloned rule.
Reorder	Reorder the selected internet protection rule. A popup window similar to the following will appear.

Operation	Description
	<div> <div> <div> <div>×</div> <div> <h3>Configure Rule Order</h3> <p>How would you like to process rule "Contractors"?</p> <div> <input checked="" type="radio"/> Process the rule last (add this rule at the bottom of the rule list)           <input type="radio"/> Process the rule first (add this rule at the top of the rule list)           <input type="radio"/> Process the rule in specific placement (select where to place in rule list)         </div> <div> <div>Cancel</div> <div>Move</div> </div> </div> </div> </div> <ol style="list-style-type: none"> <li>Select the rule order:           <ul style="list-style-type: none"> <li>Process the rule last.</li> <li>Process the rule first.</li> <li>Process the rule in specific placement—A list of the existing rules displays. Click to place the rule.</li> </ul> </li> <li>Click Move.</li> </ol> </div>
Delete	<p>Delete the selected internet protection rule. A popup window similar to the following displays:</p> <div> <div> <div>!</div> <div>Delete Rule</div> </div> <p>You are about to delete the following rule: Contractors</p> <div> <div>No</div> <div>Yes</div> </div> </div> <p>Click Yes to delete the internet protection rule, or click No to retain the rule.</p>
Refresh	Refresh the list of existing rules.

3. To customize which columns display, click Select Columns and then click the columns to display or hide. Click

Reset to return to the default column settings.



The screenshot shows a 'Select Columns' dialog box. It has a title bar with 'Select Columns' and a dropdown arrow. Below the title bar is a list of columns with checkboxes: 'Applications & URLs' (checked), 'Users' (checked), 'EIP' (checked), 'Source & Destination' (checked), 'Services' (checked), and 'Schedule' (unchecked). At the bottom of the dialog is a blue 'Reset' button.

The options are:

- Applications & URLs
- Users
- EIP
- Source & Destination
- Services
- Schedule
- Source
- Destination
- Security Enforcement
- Enabled

4. Proceed to the next section to configure application and URL-filtering match criteria.

---

## Configure SASE Application and URL Filtering for Internet Protection Rules

You create application and URL filters to prevent access to specific applications and URLs, thus allowing you to control web-browsing activity within an organization. Uncontrolled access to internet websites can expose an organization to security risks, such as threat propagation, loss of data, and lack of compliance.

Application identification provides an effective detection capability for evasive applications such as Facebook, Skype, Torrent, and WhatsApp. It identifies applications and protocols at different network layers based on the protocol bundle rather than using the IP address and port number. You can create custom application and URL categories on a per-tenant basis. You can associate a reputation value with the URL category. Each custom URL category has a unique name and defines information about the URLs to match using a string match or a pattern match. For information about creating custom applications and application groups, see [Configure SASE User-Defined Objects](#).

To configure application and URL-filtering match criteria:

---

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

1. In the Internet Protection Rules List screen, click + Add to create a rule. The Create Internet Protection Rule screen displays.

Configure > SASE > Real-Time Protection > Internet Protection

Create Internet Protection Rule

1 APPLICATIONS & URLS 2 USER GROUPS 3 GEO LOCATIONS 4 NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4 5 SECURITY ENFORCEMENT 6 REVIEW & DEPLOY

By default, we've included all applications to match.

If you prefer, you can customize which traffic to include or exclude from applications, URLs, or reputations, below.

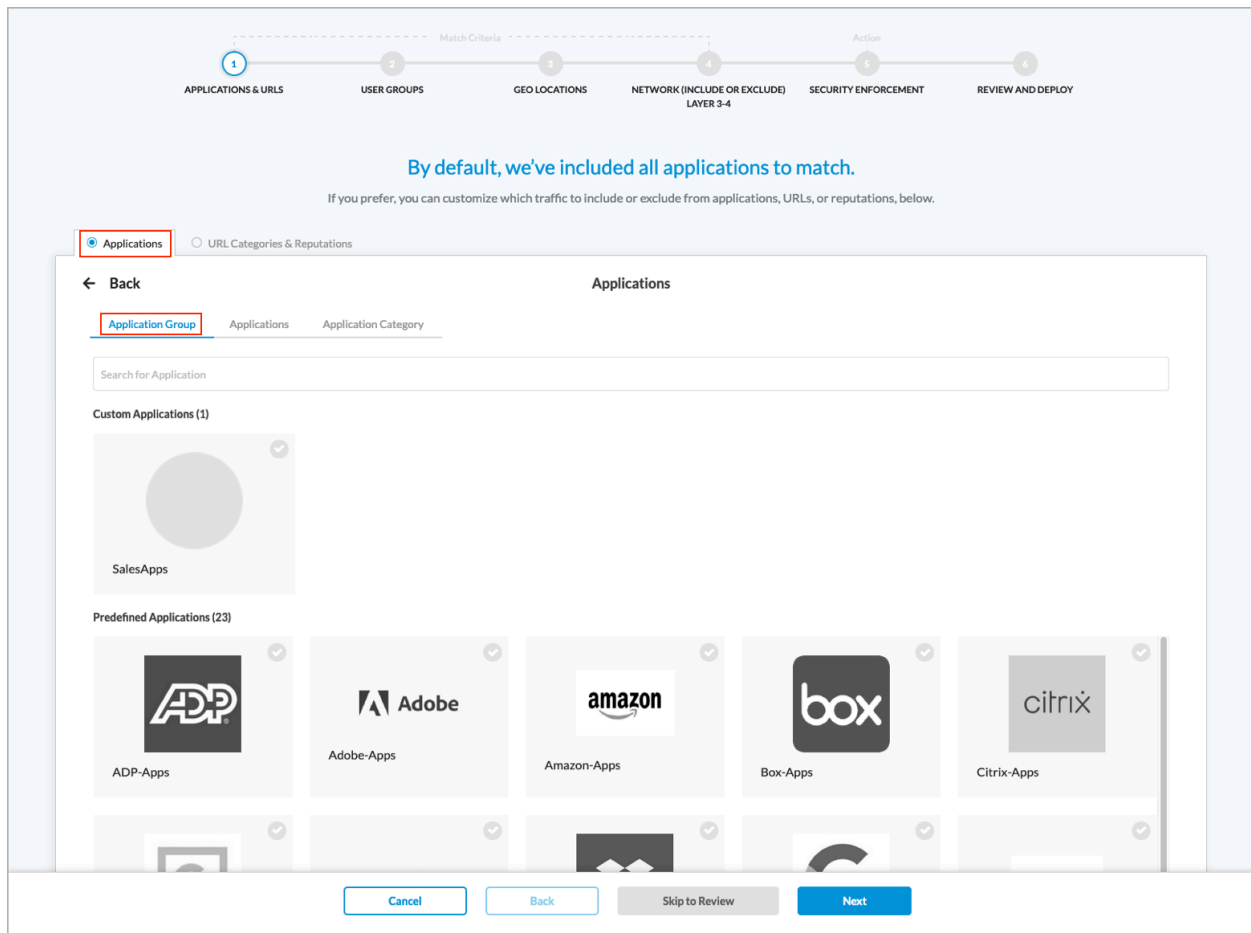
Applications, URLs or Reputations

✓ All applications

Customize

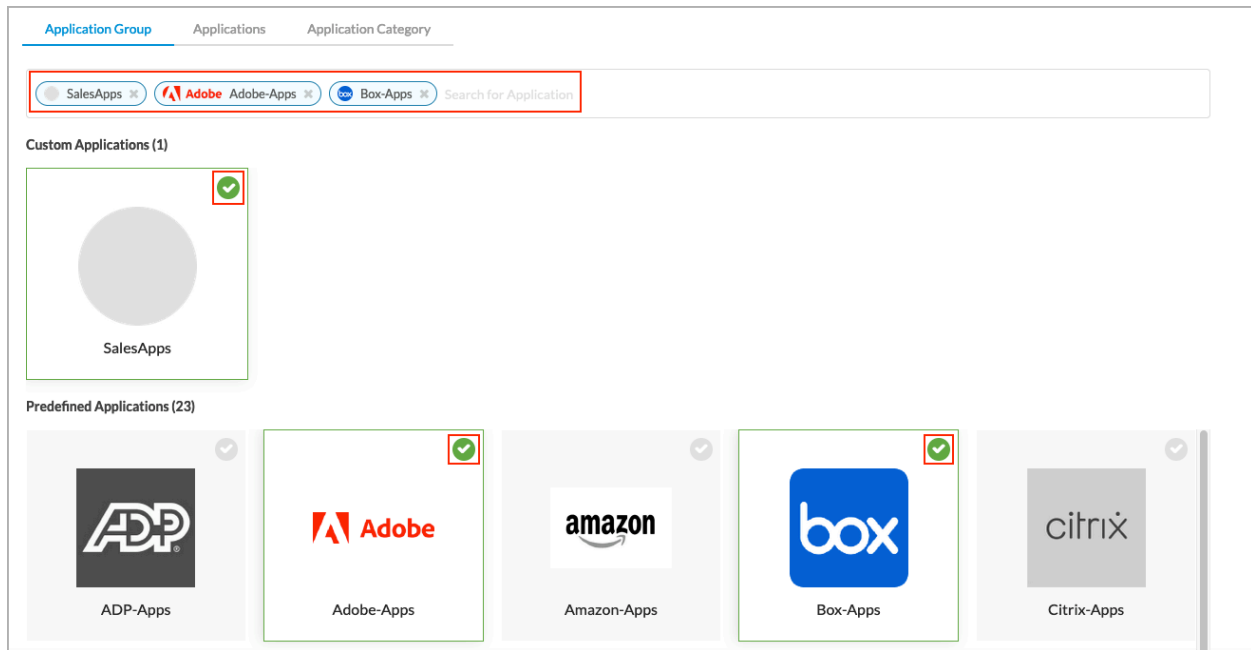
Cancel Back Skip to Review Next

2. Select Step 1, Application and URLs. By default, all applications, URLs, and reputations are included in the match, which means that all applications, URLs, and reputations are matched by this rule.
3. To accept the default settings, click Next to continue to Step 2, User Groups.
4. To include only certain application groups, applications, or application categories in the match list, click Customize. The following screen displays and Applications tab is selected by default in the top menu and Application Group is selected by default in the submenu. The screen displays all custom and predefined application groups. Note that you can create internet protection rules based on either applications or URL categories and reputations, but not both. To match both applications and URL categories or reputations, create two separate internet protection rules.

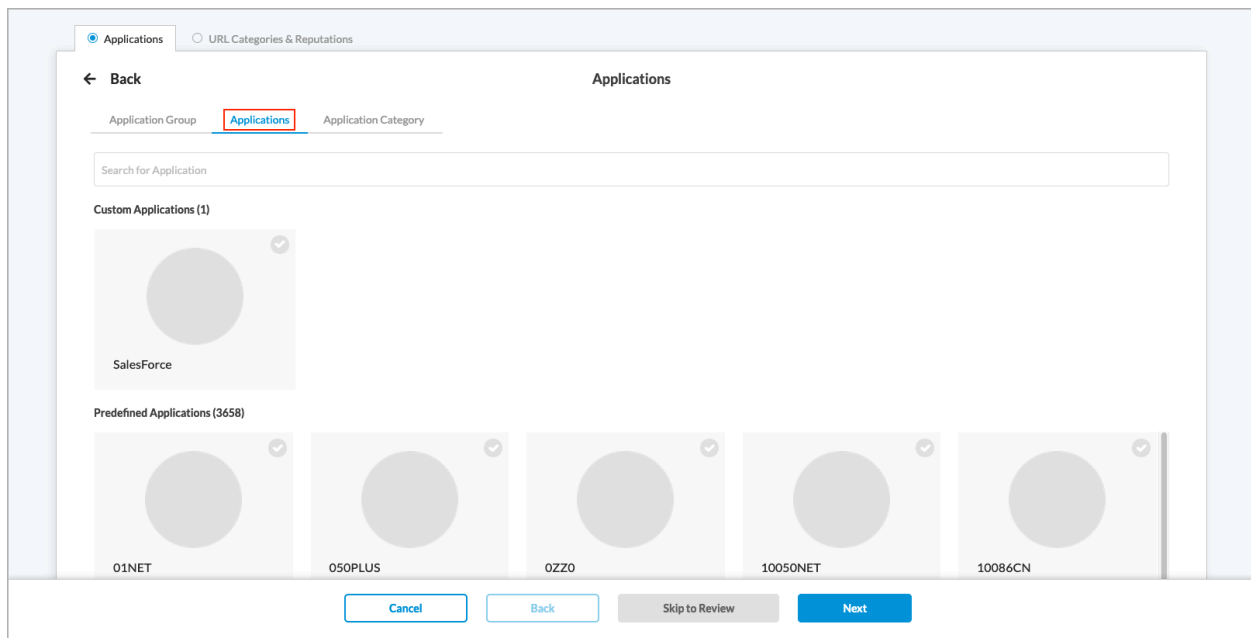


5. To create an internet protection rule based on applications, select the custom and predefined application groups to include in the match list, or type the name of the application group in the search box and select it from the search results. In the following example, the custom application group SalesApps and the predefined application groups Adobe-Apps and Box-Apps are selected. To remove an application from the list, click X next to the application in the search box.

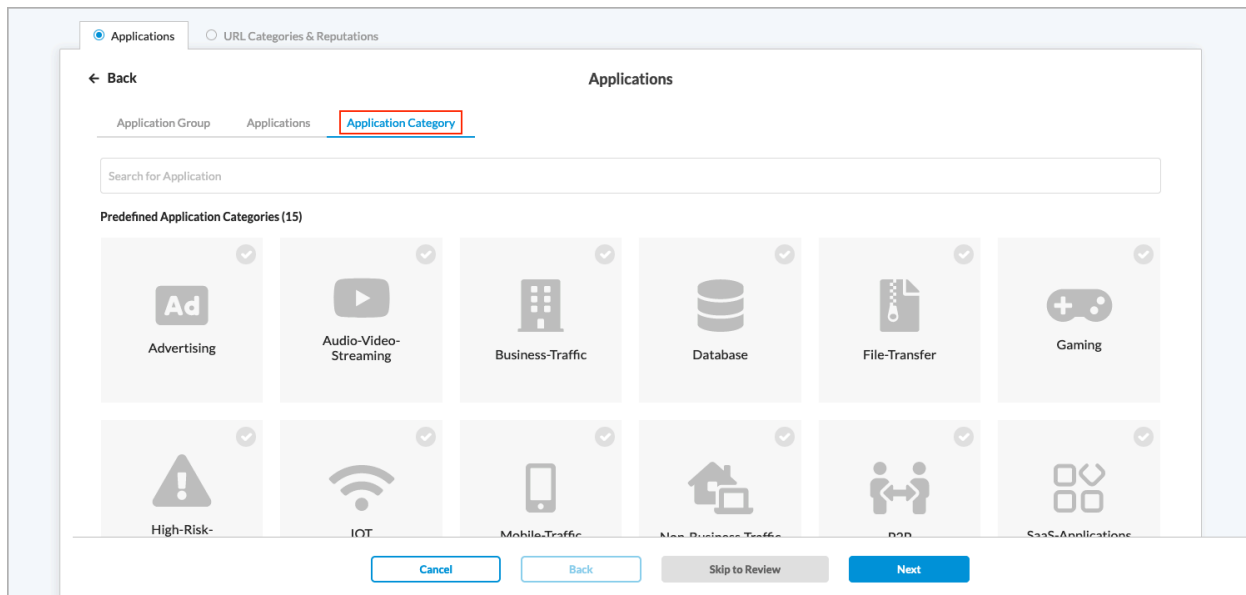




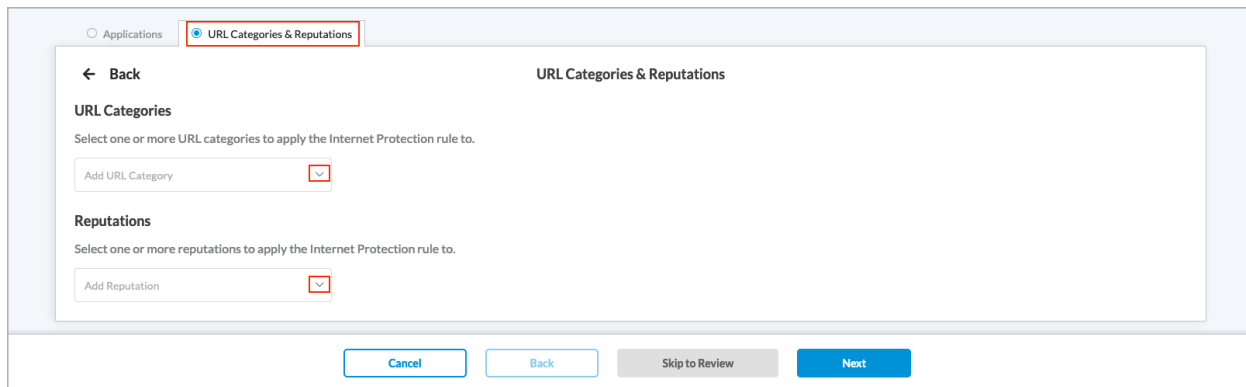
6. Click the Applications tab in the submenu. The following screen displays.



7. Select the custom and predefined applications to include in the match list, or type the name of the application in the search box and then select it from the search results.
8. Click the Application Category tab in the submenu. The following screen displays.



9. Select the predefined application categories to include in the match list, or type the name of the application category in the search box and then select it from the search results.
10. To create an internet protection rule based on URL categories and reputations, click the URL Categories & Reputations tab in the top menu. The following screen displays.



11. In the Add URL Category and Add Reputation fields, select one or more URL categories and reputations to include in the internet protection rule.
12. Click Next to configure User Groups match criteria, or click Back to return to the Create Internet Protection Rule screen and then click Next to configure SASE user and user group filtering.

## Configure SASE User and User Group Filtering for Internet Protection Rules

You create user and user group security rules to detect the users and user groups who are using applications on your network. These rules can help to identify users who may have transferred files or transmitted threats. User and user group rules identify users based on their name or role rather than their IP address.

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

To configure user and user group rules match criteria:

1. In the Create Internet Protection Rule screen, select Step 2, User Groups. By default, all users and user groups are included in the match, which means that no filtering is done on the basis of users and user groups.

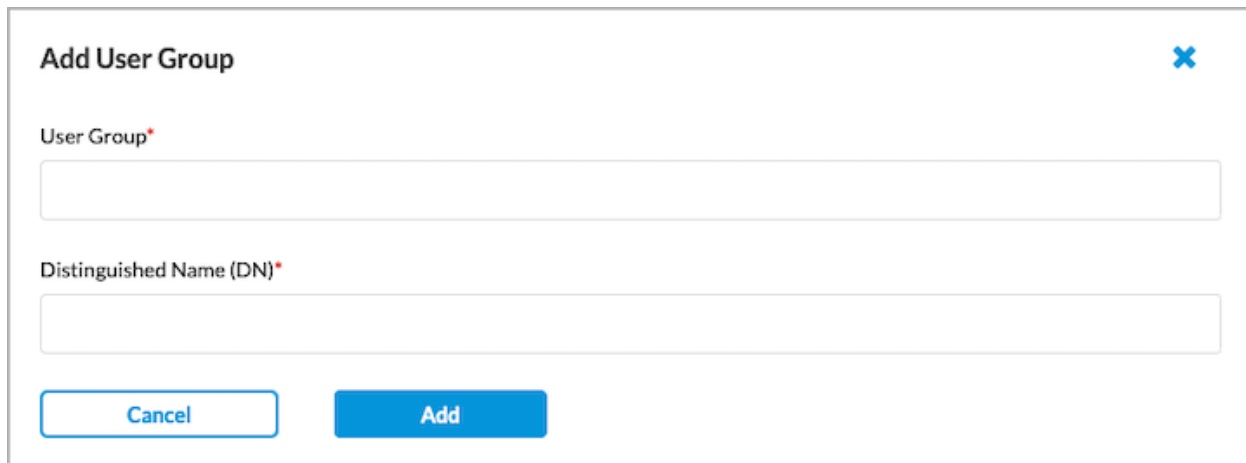
The screenshot shows the 'Create Internet Protection Rule' configuration screen. At the top, a progress bar indicates six steps: 1. APPLICATIONS & URLS, 2. USER GROUPS (highlighted with a red box), 3. GEO LOCATIONS, 4. NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4, 5. SECURITY ENFORCEMENT, and 6. REVIEW & DEPLOY. Below the progress bar, a blue message states: 'By default we have chosen all users and groups to apply your security enforcements. If you prefer, you can select the specific users or groups for the security posture.' A box titled 'Users & User Groups' contains a green checkmark and the text 'All users from ACME-Group-Profile servers'. A red box highlights the 'Customize' button. At the bottom, there are four buttons: 'Cancel', 'Back', 'Skip to Review', and 'Next'.

2. To accept the default, click Next to continue to Step 3, Geolocation match criteria.
3. To change the users and user groups to include in the match list, click Customize. The following screen displays, and the User Groups tab selected by default. The screen displays all user groups.

The screenshot shows the 'Users & User Groups' configuration screen. At the top left is a 'Back' button. The title is 'Users & User Groups'. Below the title, it says 'Enable Internet Protection for the following matched users or user groups'. A dropdown menu shows 'ACME-Group-Profile'. Below this, there are two tabs: 'User Groups' (highlighted with a red box) and 'Users'. A search bar labeled 'Search for User Groups' is present. Below the search bar, there is a list of 'User Groups (20)' with a red box around the '+ Add New User Group' button. The list has two columns: 'NAME' and 'DISTINGUISHED NAME (DN)'. The list contains 15 entries, each with a checkbox, a user group icon, a name, and a distinguished name. At the bottom, there are four buttons: 'Cancel', 'Back', 'Skip to Review', and 'Next'.

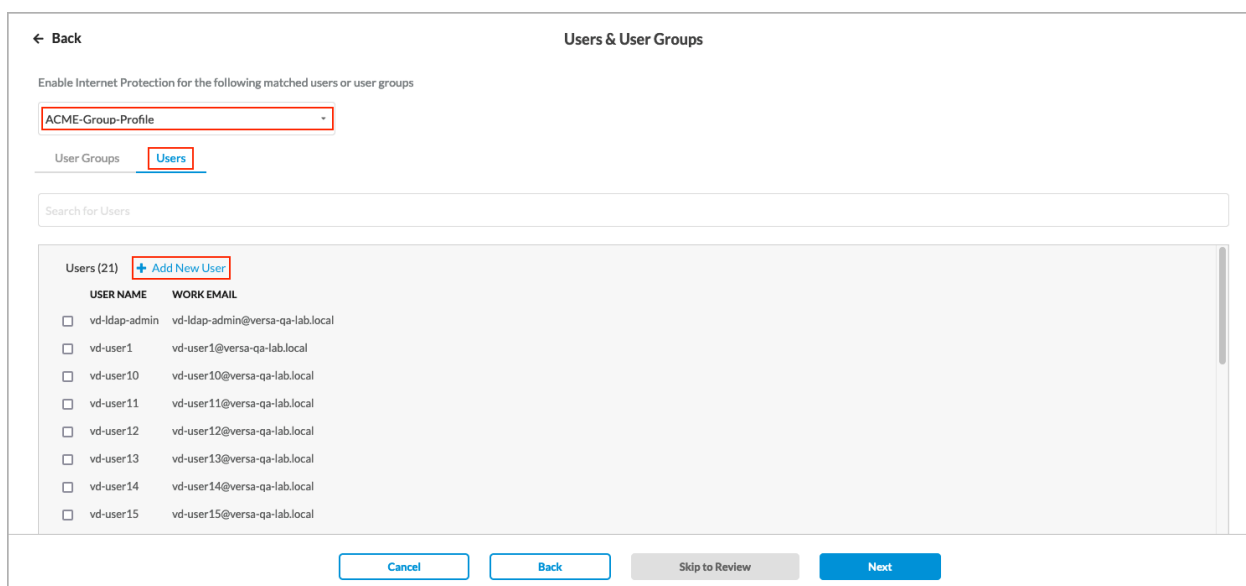
	NAME	DISTINGUISHED NAME (DN)
<input type="checkbox"/>	vd-group1	CN=vd-group1,OU=VD-Automation,DC=versa-qa-lab,DC=local[S-1-5-21-604474016-2011482265-4024304318-107852]
<input type="checkbox"/>	vd-group10	CN=vd-group10,OU=VD-Automation,DC=versa-qa-lab,DC=local[S-1-5-21-604474016-2011482265-4024304318-107861]
<input type="checkbox"/>	vd-group11	CN=vd-group11,OU=VD-Automation,DC=versa-qa-lab,DC=local[S-1-5-21-604474016-2011482265-4024304318-107862]
<input type="checkbox"/>	vd-group12	CN=vd-group12,OU=VD-Automation,DC=versa-qa-lab,DC=local[S-1-5-21-604474016-2011482265-4024304318-107863]
<input type="checkbox"/>	vd-group13	CN=vd-group13,OU=VD-Automation,DC=versa-qa-lab,DC=local[S-1-5-21-604474016-2011482265-4024304318-107864]
<input type="checkbox"/>	vd-group14	CN=vd-group14,OU=VD-Automation,DC=versa-qa-lab,DC=local[S-1-5-21-604474016-2011482265-4024304318-107865]
<input type="checkbox"/>	vd-group15	CN=vd-group15,OU=VD-Automation,DC=versa-qa-lab,DC=local[S-1-5-21-604474016-2011482265-4024304318-107866]

4. Select the group profile to use
5. Under the User Groups tab, select the user groups to include in the match list, or type the name of a user group in the search box and then select it from the search results.
6. To create a new user group based on LDAP authentication, select an LDAP group profile, and then click + Add New User Group. In the Add User Group window, enter a user group name and a distinguished name (DN) in the fields provided.



The 'Add User Group' dialog box features a title bar with a close button (X). It contains two text input fields: 'User Group\*' and 'Distinguished Name (DN)\*'. At the bottom, there are two buttons: 'Cancel' and 'Add'.

7. Click Add.
8. Click the Users tab in the submenu. The following screen displays.

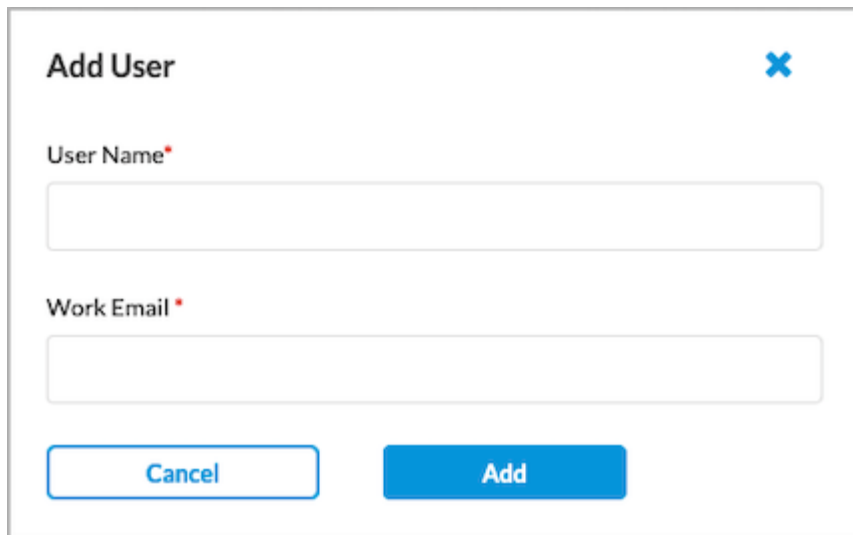


The 'Users & User Groups' screen shows a 'Back' button and a title 'Users & User Groups'. Below the title, it says 'Enable Internet Protection for the following matched users or user groups'. A dropdown menu shows 'ACME-Group-Profile'. Below this, there are two tabs: 'User Groups' and 'Users'. The 'Users' tab is selected. Below the tabs is a search bar labeled 'Search for Users'. Below the search bar is a list of users with checkboxes. The list is titled 'Users (21)' and has a '+ Add New User' button. The list has two columns: 'USER NAME' and 'WORK EMAIL'. The users listed are: vd-ldap-admin, vd-user1, vd-user10, vd-user11, vd-user12, vd-user13, vd-user14, and vd-user15. At the bottom of the screen, there are four buttons: 'Cancel', 'Back', 'Skip to Review', and 'Next'.

USER NAME	WORK EMAIL
<input type="checkbox"/> vd-ldap-admin	vd-ldap-admin@versa-qa-lab.local
<input type="checkbox"/> vd-user1	vd-user1@versa-qa-lab.local
<input type="checkbox"/> vd-user10	vd-user10@versa-qa-lab.local
<input type="checkbox"/> vd-user11	vd-user11@versa-qa-lab.local
<input type="checkbox"/> vd-user12	vd-user12@versa-qa-lab.local
<input type="checkbox"/> vd-user13	vd-user13@versa-qa-lab.local
<input type="checkbox"/> vd-user14	vd-user14@versa-qa-lab.local
<input type="checkbox"/> vd-user15	vd-user15@versa-qa-lab.local

9. Select the group profile to use.
10. Under the Users tab, select the users to include in the match list, or type the name of a user in the search box and then select it from the search results.
11. To create a new user based on LDAP authentication, select an LDAP group profile, and then click + Add New

User. In the Add User window, enter a username and the user's work email in the fields provided.

A screenshot of a web-based 'Add User' dialog box. The dialog has a title bar with the text 'Add User' and a blue 'X' icon in the top right corner. Inside the dialog, there are two text input fields. The first field is labeled 'User Name\*' and the second is labeled 'Work Email \*'. Below the input fields, there are two buttons: a light blue 'Cancel' button on the left and a dark blue 'Add' button on the right.

12. Click Add.
13. Click Next to continue to Step 3, Geolocation match criteria.

---

## Configure SASE Geolocation for Internet Protection Rules

Versa SASE internet protection rules provide a list of predefined regions that you can use to create filter profiles based on both source and destination geographic areas.

To configure geolocation internet protection rule match criteria:

1. In the Create Internet Protection Rule screen, select Step 3, Geolocation. By default, all source and destination geographic locations are included in the match list, which means that no filtering is done based on geographic location and so traffic flows to all destinations.

Configure > SASE > Real-Time Protection > Internet Protection


### Create Internet Protection Rule

Match Criteria

1 APPLICATIONS & URLS 2 USER GROUPS 3 **GEO LOCATIONS** 4 NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4 5 SECURITY ENFORCEMENT 6 REVIEW & DEPLOY

By default we've chosen all Geo Locations


These are location selections for allowing or denying access to your rule. If you prefer, you can select specific geo locations



**Source Geo Location**

✓ All Source Geo locations are selected

[Customize](#)



**Destination Geo Location**

✓ All Destination Geo locations are selected

[Customize](#)


Cancel Back Skip to Review Next

- To accept the default, click Next to continue to Step 4, Network (Include or Exclude) Layer 3-4 match criteria.
- To change the source geographic locations to include in the match list, click Customize under Source Geolocation. The following screen displays.

[← Back](#)

### Source Geo Location

Geolocation refers to the use of location technologies such as IP addresses to identify and track the whereabouts of connected electronic devices. By default, we have selected all devices. You can customize, by selecting which country, region, zone to include or exclude.



[+ Select Country](#)

Selected [Clear All](#)

Cancel Back Skip to Review Next

- Click Clear All to remove all the default source locations. (Because all locations are selected by default, they are not displayed).
- Click in the Select Country box, and then select one or more countries. The map changes to highlight the countries you select.
- Click the down arrow in the Select Country box to display the selected countries.

Selected	Clear All X
Afghanistan	X
Australia	X
Hungary	X
Sweden	X

7. To remove a country from the list, click the X next to the country name.
8. To remove all countries from the list, click Clear All.
9. To customize the destination geographical locations, click Back. The Geolocation screen displays again.
10. To accept the default destination geographical locations and go to Step 4, Network (Include or Exclude) Layer 3-4 match criteria, click Next at the bottom of the screen.
11. To change the destination geographic locations to include in the match list, click Customize under Destination Geolocation. The Destination Geolocation screen displays.
12. Click Clear All to remove all the default destination locations. (Because all locations are selected by default, they are not displayed).
13. Repeat Steps 4 and 5 to change the destination geographic locations.
14. Click Next to go to Step 4, Network (Include or Exclude) Layer 3-4 screen, or click Back to return to the Geolocation screen.

---

## Configure SASE Source and Destination Traffic for Internet Protection Rules

You can create internet protection rule criteria based on source and destination traffic.

To configure network rules based on source and destination traffic match criteria:

1. In the Create Internet Protection Rule screen, select Step 5, Network Layer 3-4. By default, all source and destination traffic is included in the match.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

7

APPLICATIONS & URLS

USERS & GROUPS

ENDPOINT INFORMATION PROFILE (EIP)

GEO LOCATIONS

NETWORK LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services ⓘ

☒ All layer 4 services

Customize

Source & Destination (Layer 3) ⓘ

☒ Zone  
SD-WAN Zone  
Versa Client

☒ Zone  
Internet

Customize

Schedule ⓘ

☒ None Selected

Cancel

Back

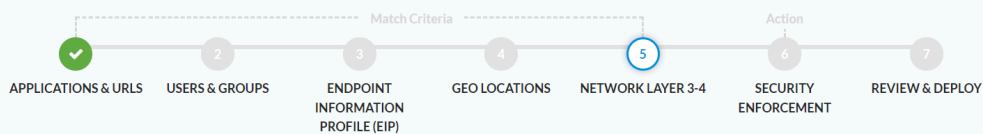
Skip to Review

Next

2. To accept the default, click Next to continue to Step 6, Security Enforcement rules.
3. To change the source and destination traffic to include in the match, click Customize in the Source & Destination (Layer 3) pane. In the Source & Destination (Layer 3) screen, select Source Address tab, and then enter information for the following fields. Note that in Releases 11.3.2 and earlier, you configure the source and destination on a single screen.



## Create Internet Protection Rule



All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

[← Back](#)

## Source &amp; Destination (Layer 3)

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination.

[More Information ⓘ](#)

Source Address

Destination Address

Source Zones &amp; Sites

Destination Zones &amp; Sites

☐ Negate Source Address[+ Add](#)

<input type="checkbox"/>	NAME	TOTAL	IP ADDRESSES
<input type="checkbox"/>	ag1	2	abcd, 10.3.4.5/32
<input type="checkbox"/>	ag2	1	abcd.com
<input type="checkbox"/>	ComplexAddressGroup	11	192.168.0.56/0.0.0.255, 192.168.0.55/0.0.0.255, 192.168.0.54/0.0.0.255, 192.168.0.53/0.0.0.255, 192.168.0.52/0.0.0.255 <a href="#">Load More</a>
<input type="checkbox"/>	rish	1	10.1.1.0/24
<input type="checkbox"/>	RIYADH	1	10.0.0.0/23
<input type="checkbox"/>	riyadh	1	10.0.0.0/24
<input type="checkbox"/>	TEST	1	10.1.1.0/24

Showing 1-7 of 7 results

10 ▾ Rows per Page

Go to page 1 ▾

[< Previous](#) [1](#) [Next >](#)

IP Subnet ⓘ

IP Range ⓘ

IP WildCard ⓘ

Cancel

Back

Skip to Review

Next

Field	Description
Negate Source Address	Select to apply the rule to any source addresses except the ones in the Source Address field.
IP Subnet	Enter a list of comma-separated subnets to include in the match list, for example, 10.2.1.0/24.
IP Range	Enter a list of comma-separated IP addresses or ranges to include in the match list, for example, 10.2.1.1–10.2.2.2.
IP Wildcard	Enter a list of comma-separated IP addresses and masks to include in the match list, for example, 192.68.0.56/255.255.0.255.

4. To create an address group, click the **+ Add** icon in the Source Address tab. In the Enter Addresses section, enter information for the following fields. You configure the address groups in the User-Defined Objects section. If you want to configure one or more specific source IP addresses, you do not need to select an address group. Instead, use the IP Wildcard field to enter the IP addresses.

Configure > SASE > Settings > User Defined Objects

**Address Group**

1 ENTER ADDRESSES

Type

Subnet

Subnet

Press Enter to add

+

Cancel



Next

2 NAME AND TAGS

+

Field	Description
Type	<p>Select the type of IP address to match and the value to match. The name of the Address/Prefix field changes depending on the value you select in the Type field.</p> <ul style="list-style-type: none"> <li>Dynamic Address</li> </ul>

Field	Description
	<ul style="list-style-type: none"> <li>◦ FQDN</li> <li>◦ IP Range</li> <li>◦ IP Wildcard</li> <li>◦ IPv6 Subnet</li> <li>◦ Subnet</li> </ul>
◦ Subnet	Enter one or more IP addresses and subnet masks, for example, 10.2.1.0/24.
◦ IP Range	Enter one or more IP addresses within the IPv4 address range specified in the IPv4 Range field, for example, 10.2.1.1–10.2.2.2.
◦ IP Wildcard	Enter one or more wildcard masks for specific IP addresses, for example, 192.68.0.56/255.255.0.255.
◦ IPv6 Subnet	Enter one or more IP addresses and subnet masks within the IPv6 subnet range specified in the IPv6 subnet.
◦ FQDN	Enter one or more IP addresses returned in a DNS query that resolves the fully qualified domain name (FQDN) into an IP address. The FQDN cannot contain any wildcard characters.
◦ Dynamic Address	Enter a dynamic address object, which is a container for an IP address list that can change dynamically.

- To add IP address types, click the  Plus icon. To remove an address type, click the  Minus icon.
- Click Next. In the Name and Tags section, enter a name (required) and, optionally, tags.
- Click Save.
- Select the Destination Address tab, and then enter information for the following fields.



[More Information](#) ⓘ

IPSubnet ⓘ	IP Range ⓘ	IP WildCard ⓘ
<input type="text" value="Enter a list of IPv4/IPv6 Subnet values"/>	<input type="text" value="Enter a list of IP Range values"/>	<input type="text" value="Enter a list of wildcard values"/>

Field	Description
Negate Destination Address	Select to apply the rule to any destination addresses except the ones in the Destination Address field.
IP Subnet	Enter a list of comma-separated subnets to include in the match list, for example, 10.2.1.0/24.
IP Range	Enter a list of comma-separated IP addresses or ranges to include in the match list, for example, 10.2.1.1–10.2.2.2.
IP Wildcard	Enter a list of comma-separated IP addresses and masks to include in the match list, for example, 192.68.0.56/255.255.0.255.

9. To create an address group, perform Steps 4 through 7.
10. Select the Source Zones and Sites tab, and then enter information for the following fields.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1 Applications & URLs
 2 Users & Groups
 3 Endpoint Information Profile (EIP)
 4 GEO Locations
 5 Network Layer 3-4
 6 Security Enforcement
 7 Review & Deploy

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

← Back
Source & Destination (Layer 3)

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination.

[More Information](#)

Source Address	Destination Address	Source Zones & Sites	Destination Zones & Sites
		Source Zones(2) <div> <span>Versa Client</span> <span>SD-WAN Zone</span> </div>	Source Sites(1) <div> <span>JAPAN-JASDF</span> </div>

Cancel
Back
Skip to Review
Next

- In the Source Zones field, select one or more source zones to include in the match list. By default, three source zones are available. User-defined zones, such as zones for IPsec and GRE tunnels, also display in this list, and you can select them.
    - Internet—Select this zone if traffic comes from the internet.
    - SD-WAN Zone—Select this zone if traffic comes from an SD-WAN device.
    - VSA Application—Select this zone if traffic comes from a VSA client application.
  - In the Source Sites field, select one or more source sites to include in the match list.
11. Select Destination Zones and Sites tab, and then enter information for the following fields.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1 Applications & URLs
 2 Users & Groups
 3 Endpoint Information Profile (EIP)
 4 GEO Locations
 5 Network Layer 3-4
 6 Security Enforcement
 7 Review & Deploy

**All traffic is selected, and it will receive the previously selected security enforcements**  
 If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

← Back **Source & Destination (Layer 3)**

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination.

[More Information](#)

Source Address

Destination Address

Source Zones & Sites

Destination Zones & Sites

Destination Zones(2)

Internet

SD-WAN Zone

Destination Sites(1)

JAPAN-JASDF

Cancel

Back

Skip to Review

Next

- In the Destination Zones field, select one or more destination zones to include in the match list. User-defined zones, such as zones for IPsec and GRE tunnels, also display in this list, and you can select them. By default, three destination zones are available:
    - Internet—Select this zone if traffic comes from the internet.
    - SD-WAN Zone—Select this zone if traffic comes from an SD-WAN device.
    - VSA Application—Select this zone if traffic comes from a VSA client application
  - In the Destination Sites field select one or more destination sites to include in the match list.
12. Click Back to return to the Network Layer 3-4 screen. From this screen you can configure network services and create policy schedules.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

7

APPLICATIONS & URLS

USERS & GROUPS

ENDPOINT INFORMATION PROFILE (EIP)

GEO LOCATIONS

NETWORK LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

← Back

Source & Destination (Layer 3)

The Source Destination section represents Layer 3 of the network layer traffic. Layer 3 transmits data segments between networks in the form of packets. When you message your friend, this layer assigns source and destination IP addresses to the data segments. Your IP address is the source, and your friend's is the destination.

[More Information](#)

Source Address

Destination Address

Source Zones & Sites

Destination Zones & Sites

Destination Zones(1)

Internet

Cancel

Back

Skip to Review

Next

13. Click Next to continue to Step 6, Security Enforcement rules.

## Configure SASE Network Services for Internet Protection Rules

You can configure internet protection rules to filter traffic according to the network service being provided. By default, all network services are selected, which means that security enforcement rules are applied to the traffic of all network service types. If desired, you can specify the services to which to apply security enforcement rules.

To configure the network services to which to apply security enforcement rules:

1. In the Create Internet Protection Rule screen, select Step 5, Network (Include or Exclude) Layer 3-4, and then select Services. By default, all Layer 4 services included in the match.



Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

7

APPLICATIONS & URLS

USERS & GROUPS

ENDPOINT INFORMATION PROFILE (EIP)

GEO LOCATIONS

NETWORK LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services ⓘ

☒ All layer 4 services

Customize

Source & Destination (Layer 3) ⓘ

☒ Zone  
SD-WAN Zone  
Versa Client

☒ Zone  
Internet

Customize

Schedule ⓘ

☒ None Selected

Cancel

Back

Skip to Review

Next

- To configure the network services to which to apply security enforcement rules, click **Customize** under **Services**. The following screen displays.

← Back

Services

The Services section represents Layer 4 of the layer traffic. Layer 4 segments data from Layer 5 (Session). It ensures data arrives correctly and at what rate. Layer 5 establishes, maintains, ends communication between devices, and decides which packets belong to which files. Layer 6 (Presentation) translates data to binary and encrypts/decrypts it ⓘ

---

Services ⓘ

☒ + Add New

Cancel

Back

Skip to Review

Next

- In the **Services** field, select one or more of the predefined services. To add a custom service, click **+ Add New**. The following screen displays.

4. In the Protocol field, select a protocol. If you select TCP, UDP, or TCP and UDP, enter information for the following fields.

Field	Description
Source Port	<p>Enter the source port number.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>
Destination Port	<p>Enter the destination port number.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>
Source or Destination Port	<p>Enter the source or destination port number.</p> <p><i>Range:</i> 0 through 65535</p> <p><i>Default:</i> None</p>

5. Click Next. The Name and Tags screen displays.

Service

1 ENTER PROTOCOL & PORT

2 NAME AND TAGS

Name \*

Tags

Cancel Save

6. In the Name field, enter a name for the new service.
7. In the Tags field, enter optional tags.
8. Click Save to add the new service to the protocol list. You can then select the new service.
9. Click Back to return to the Step 4, Network (Include or Exclude) Layer 3-4 screen. From this screen you can configure policy schedules.

---

## Configure Schedules for SASE Internet Protection Rules

Security policy rules are in effect on all days and at all times. You can define a schedule to limit a security policy so that it is in effect only at specific times. You can also create schedules to limit when to apply internet protection rules to filter traffic. You then apply the schedule to the desired policy and rule. No default schedules are configured.

To create schedules for when to apply internet protection rules to filter traffic:

1. In the Create Internet Protection Rule screen, select Step 5, Network Layer 3-4, and then select Schedules. By default, no schedules are configured.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

Match Criteria

1 APPLICATIONS & URLS 2 USERS & GROUPS 3 ENDPOINT INFORMATION PROFILE (EIP) 4 GEO LOCATIONS 5 NETWORK LAYER 3-4 6 SECURITY ENFORCEMENT 7 REVIEW & DEPLOY

All traffic is selected, and it will receive the previously selected security enforcements

If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

layer 4 services

Customize

Source & Destination (Layer 3)

Zone SD-WAN Zone Versa Client

Zone Internet

Customize

Schedule

None Selected

Customize

Cancel Back Skip to Review Next

- To select or create a schedule, click Customize under Schedule.
- In Schedule Hours, select a schedule. If no schedules exist, click + Add New to create a schedule to set the time and frequency at which the rule is in effect.

← Back Schedule

### Schedule Hours

Select a schedule to set the time and frequency at which the policy is in effect.

Schedule + Add New

- In the Enter Schedule Details section, enter information for the following fields.

## Schedule

1

### ENTER SCHEDULE DETAILS

#### Recurrence

None

#### Start Date

Select



#### Start Time

Select



#### End Date

Select



#### End Time

Select




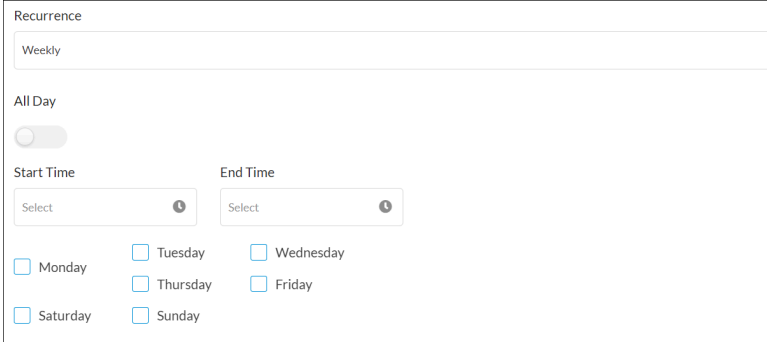
Cancel

Next

2

### NAME AND TAGS



Field	Description
Recurrence	<p>Select how often the policy is to be in effect:</p> <ul style="list-style-type: none"> <li>◦ Daily</li> <li>◦ None</li> <li>◦ Weekly</li> </ul>
All Day	<p>If you select Daily or Weekly, click the slider to schedule the policy to be in effect all day.</p> 
Start Time	If you do not select All Day, enter the start time for the policy to be in effect.
End Time	If you do not select All Day, enter the end time for the policy to be in effect.
Days of the Week	<p>If you select Weekly, select the days of the week for the policy to be in effect.</p> 

5. Click Next. The following screen displays.

Schedule

ENTER SCHEDULE DETAILS +

2 NAME AND TAGS -

Name \*

Tags

Cancel Save

6. In the Name and Tags fields, enter a name for the schedule and enter optional tags.
7. Click Save.

---

## Configure Security Enforcement Actions for SASE Internet Protection Rules

You use Versa SASE security enforcement rules to define the actions to take on traffic that meets previously defined match conditions and to define the security enforcement actions that you can apply to matching traffic. You can select profiles under Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Data Loss Prevention (DLP) profiles. The following screen shows the available security enforcement actions.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

APPLICATIONS & URLS

2

USER GROUPS

3

GEO LOCATIONS

4

NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4

5

SECURITY ENFORCEMENT

6

REVIEW & DEPLOY

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

✓

Allow

Allow all traffic that matches the rule to pass

☐

✗

Deny

Drop all traffic that matches the rule

☒

✗

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☐

✓

Profiles

Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Data Loss Prevention (DLP)

Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

Blocked Malware

✗

 viruses

✗

 ransomware

✗

 spyware

✗

 worms

✗

 trojans

✗

 adware

✗

 unwanted applications

URL Filtering

EasyURLFiltering

Versa's preconfigured URL filters controls all web-browsing activity

Blocked URL Categories

✗

 adult and pornography

✗

 games

✗

 web advertisements

Intrusion Protection System (IPS)

EasyIPS

Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

Blocked Vulnerabilities

✗

 high severity & medium+ confidence attacks

✗

 medium+ cvss & medium+ confidence attacks

IP Filtering

Versa Recommended Profile

Versa's preconfigured IP Filtering blocks communication with internet end points...

The following reputations will be alerted or rejected for source or destination traffic:

This Profile rejects IP addresses of wellknown exploits and alert the system administrator for other suspicious activities such as phishing activity

Alert

✗

 spam sources

✗

 phishing

✗

 web attacks

✗

 scanners

✗

 denial of service

✗

 reputation

✗

 network

Reject

✗

 proxy

✗

 window exploits

✗

 botnets

File Filtering

EasyFileFiltering

Versa's preconfigured file filtering protects from unwanted and malicious files

Alert

✗

 ftp

✗

 http

✗

 imap

✗

 mapl

✗

 pop3

✗

 smtp

✗

 http2

DNS Filtering

EasyDNS

Versa's preconfigured domain name system allows you to block access to sites and protect...

Alert

✗

 bad traffic

✗

 bots

✗

 dos

✗

 spam

✗

 scanners

✗

 window exploits

✗

 unwanted applications

Cancel

Back

Skip to Review

Next

You can apply either one security enforcement action or one security enforcement profile to matching traffic.

You can specify the following security enforcement actions:

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.



- Allow—Allow all traffic that matches the rule to pass unfiltered.
- Deny—Drop all traffic that matches the rule.
- Reject—Drop the session and send a TCP reset (RST) message or a UDP ICMP port unreachable message.
- Profiles—Allow all traffic that match the selected security profile rules.

For SWG, you can choose a predefined security enforcement profiles to allow or reject traffic, or you can create a customized version of any of the predefined profiles. The following are the predefined security enforcement profiles:

- Malware protection—Scans web and email traffic for all types of malicious software (malware), which is a file or code that infects, explores, steals or otherwise damages servers and host devices.
- URL filtering—Prevents access to specific URLs, controlling access to secure (HTTPS) and unsecure (HTTP) websites, thus allowing you to limit web-browsing activity and reduce risks from uncontrolled access to internet websites, including threat propagation, loss of data, and lack of compliance.  
Note: In addition to using predefined URL-filtering profiles, you can create custom URL-filtering profiles and associate them with internet protection rules. For more information, see [Configure Custom URL-Filtering Profiles](#).
- Intrusion protection system (IPS)—Identifies malicious activity using signatures, which are rules for matching suspicious software or patterns in an application's traffic, and by monitoring for unusual events or trends in network traffic.
- IP filtering—Identifies network traffic based on the source or destination IP address or fully qualified domain name (such as www.acme.com) and filters or blocks traffic based on its IP address or FQDN and based on the reputation associated with an IP address or FQDN and its geographic location.  
Note: In addition to using predefined IP-filtering profiles, you can create custom IP-filtering profiles and associate them with internet protection rules. For more information, see [Configure Custom IP-Filtering Profiles](#).
- File filtering—Reduces the risk of attacks from unwanted and malicious files, protecting against virus and vulnerabilities that are associated with various types of files. File filtering is performed based on the file type and the hash of the file. File filtering can block files associated with specific applications, files of specific sizes, files associated with specific protocols, and files traveling in a particular direction. SHA-based hash lists of files can mark potentially dangerous files for blocking and to mark safe files for allowing. File filtering to perform reputation-based file hash lookups on a cloud server.  
Note: In addition to using predefined file-filtering profiles, you can create custom file-filtering profiles and associate them with internet protection rules. For more information, see [Configure Custom File-Filtering Profiles](#).
- Domain Name System (DNS) filtering—Blocks access to websites, webpages, and IP addresses, to provide protection from malicious websites, such as known malware and phishing sites.  
Note: In addition to using predefined DNS-filtering profiles, you can create custom DNS-filtering profiles and associate them with internet protection rules. For more information, see [Configure Custom DNS-Filtering Profiles](#).

For CASB, you can use custom CASB profiles or add CASB profiles from the CASB tab. For more information, see [Configure CASB Profiles](#).

For DLP, you can use predefined or user-defined profiles. For more information, see [Configure Data Loss Prevention in Concerto](#).

By default, each security enforcement profile has a predefined VersaEasy configuration. You can use the predefined VersaEasy configurations, or you can customize a profile.

Note: The file-filtering profile displays only if the tenant to which you want to apply the profile is subscribed to the SWG Professional service. The malware protection and IPS profiles display only if the tenant is subscribed to both the SWG and VSA Professional services.

---

## Configure a Malware Protection Profile for SASE Internet Protection Rules

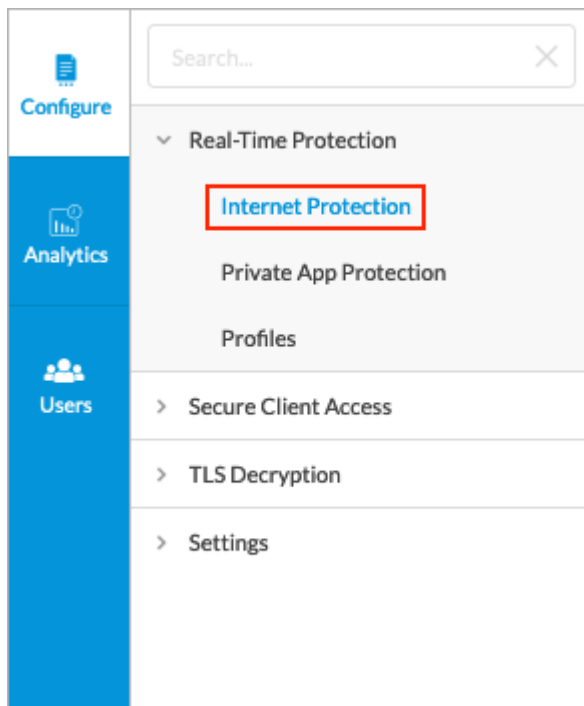
Malware is malicious software software that is specifically designed to disrupt computers and computer systems. There are many types of malware, including computer viruses, worms, Trojan viruses, spyware, adware, and ransomware. Among the things malware can do is leak private information, gain unauthorized access to information or systems, and deprive users access to information.

By default, Versa SASE provides a predefined security enforcement policy to protect against malware. You can customize the malware protection profile.

Note: The malware protection profile displays only if the tenant is subscribed to both the SWG and VSA Professional services.

To configure a malware protection profile:

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



The Internet Protection Rules List screen displays all configured internet protection rules.

Configure > SASE > Real-Time Protection > Internet Protection

**Internet Protection Rules List** Publish

Below are all the rules for your Internet Protection Policy.

Search by keyword or name | Filter + Add Clone Reorder Delete Refresh Select Columns

	Rule Name	Applications & URLs	Users	EIP	Network Layer 3-4		Geo Locations
					Source & Destination	Services	Source
<input type="checkbox"/>	Implicit_Drop_Quic	All Applications	All Users			Services Implicit-QUIC-UDP-443	All Source Geo Locations selected
<input type="checkbox"/>	Implicit-Allow-DNS	All Applications	All Users			Services domain	All Source Geo Locations selected
<input type="checkbox"/>	Implicit-Deny-All	All Applications	All Users			Layer 4 Services are not Enabled	All Source Geo Locations selected

Showing 1-3 of 3 results 10 Rows per Page Go to page 1 < Previous 1 Next >

- To customize which columns display, click Select Columns and then click the columns to display or hide. Click Reset to return to the default column settings.

Select Columns

- ☒ Security Enforcement
- ☒ Applications
- ☒ Users
- ☒ Source & Destination

Reset

- Click + Add to create a rule. The Create Internet Protection Rule screen displays.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

APPLICATIONS & URLS

USER GROUPS

GEO LOCATIONS

NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

Allow

Allow all traffic that matches the rule to pass

☐

Deny

Drop all traffic that matches the rule

☐

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☐

Profiles

Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Data Loss Prevention (DLP)

Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

Blocked Malware

viruses

ransomware

spyware

worms

trojans

adware

unwanted applications

URL Filtering

EasyURLFiltering

Versa's preconfigured URL filters controls all web-browsing activity

Blocked URL Categories

adult and pornography

games

web advertisements

Intrusion Protection System (IPS)

EasyIPS

Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

Blocked Vulnerabilities

high severity & medium+ confidence attacks

medium+ cvss & medium+ confidence attacks

IP Filtering

Versa Recommended Profile

Versa's preconfigured IP Filtering blocks communication with internet end points...

The following reputations will be alerted or rejected for source or destination traffic:

This Profile rejects IP addresses of wellknown exploits and alert the system administrator for other suspicious activities such as phishing activity

Alert

spam sources

phishing

web attacks

scanners

denial of service

reputation

network

Reject

proxy

window exploits

botnets

File Filtering

EasyFileFiltering

Versa's preconfigured file filtering protects from unwanted and malicious files

Alert

ftp

http

imap

mapl

pop3

smtp

http2

DNS Filtering

EasyDNS

Versa's preconfigured domain name system allows you to block access to sites and protect...

Alert

bad traffic

bots

dos

spam

scanners

window exploits

unwanted applications

Cancel

Back

Skip to Review

Next

4. Select the Security Enforcement action.

5. Select the Secure Web Gateway (SWG) tab, and then click in the Malware Protection box to enable the default EasyMalwareProtection security enforcement profile. By default, the EasyMalwareProtection profile blocks the

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

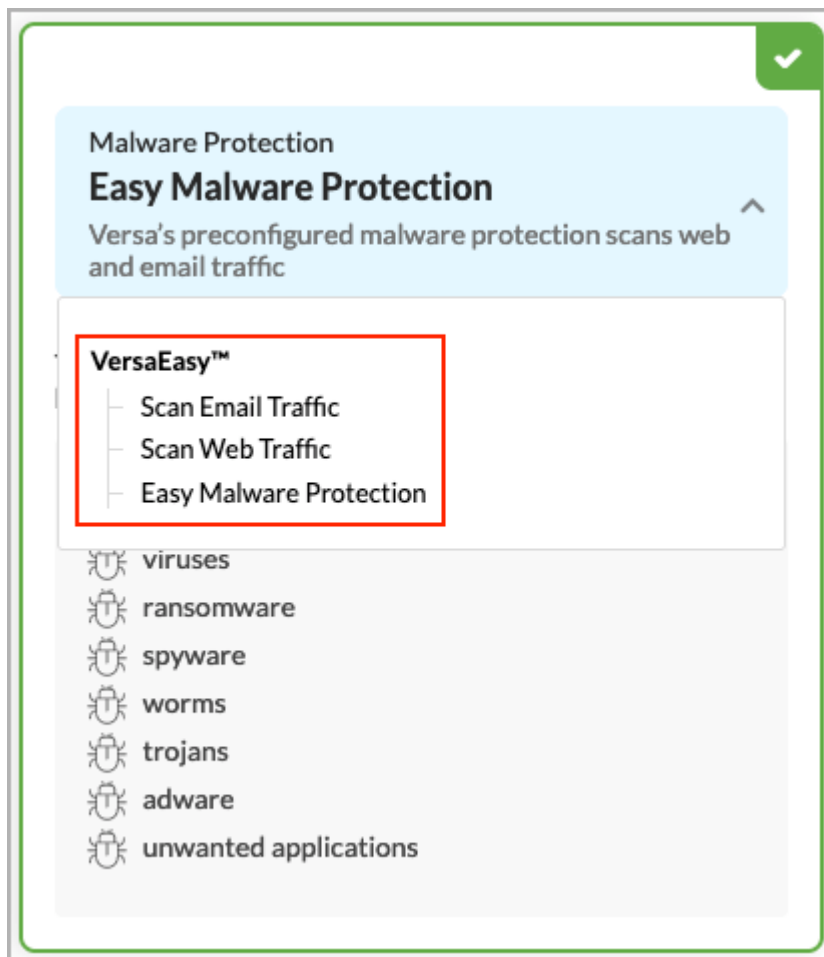
Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

following types of malware:

- Adware
- Ransomware
- Spyware
- Trojans
- Unwanted applications
- Viruses
- Worms

6. Click the down arrow to display other options.



7. Select Scan Email Traffic to send alerts about the following malware in both the upload and download directions:

- IMAP
- MAPI
- POP3
- SMTP

8. Select Scan Web Traffic to deny the following malware in both the upload and download directions:

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

- FTP
  - HTTP
9. Select Easy Malware Protection to restore the default Easy Malware Protection settings.
  10. Select other profiles to customize or click Next to continue to the Review and Deploy screen.

---

## Configure a URL-Filtering Profile for SASE Internet Protection Rules

By default, Versa SASE provides a predefined security enforcement policy for URL filtering. You can customize the predefined URL-filtering protection profile.

In addition to using predefined URL-filtering profiles, you can create custom URL-filtering profiles and associate them with internet protection rules. For more information, see [Configure Custom URL-Filtering Profiles](#).

To configure a URL-filtering protection profile:

1. In the Security Enforcement screen > Secure Web Gateway (SWG) tab, select URL Filtering in the Profiles section to enable the preselected EasyURLFiltering security enforcement policies. By default, the EasyURLFiltering policies provide URL filtering for the following types of websites:
  - Adult and pornography
  - Games
  - Web advertisements

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

APPLICATIONS & URLS

USER GROUPS

GEO LOCATIONS

NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

Allow

Allow all traffic that matches the rule to pass

☐

Deny

Drop all traffic that matches the rule

☐

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☐

Profiles

Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Data Loss Prevention (DLP)

Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

Blocked Malware

viruses

ransomware

spyware

worms

trojans

adware

unwanted applications

URL Filtering

EasyURLFiltering

Versa's preconfigured URL filters controls all web-browsing activity

Blocked URL Categories

adult and pornography

games

web advertisements

Intrusion Protection System (IPS)

EasyIPS

Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

Blocked Vulnerabilities

high severity & medium+ confidence attacks

medium+ cvss & medium+ confidence attacks

IP Filtering

Versa Recommended Profile

Versa's preconfigured IP Filtering blocks communication with internet end points...

The following reputations will be alerted or rejected for source or destination traffic:

This Profile rejects IP addresses of wellknown exploits and alert the system administrator for other suspicious activities such as phishing activity

Alert

spam sources

phishing

web attacks

scanners

denial of service

reputation

network

Reject

proxy

window exploits

botnets

File Filtering

EasyFileFiltering

Versa's preconfigured file filtering protects from unwanted and malicious files

Alert

ftp

http

imap

mapl

pop3

smtp

http2

DNS Filtering

EasyDNS

Versa's preconfigured domain name system allows you to block access to sites and protect...

Alert

bad traffic

bots

dos

spam

scanners

window exploits

unwanted applications

Cancel

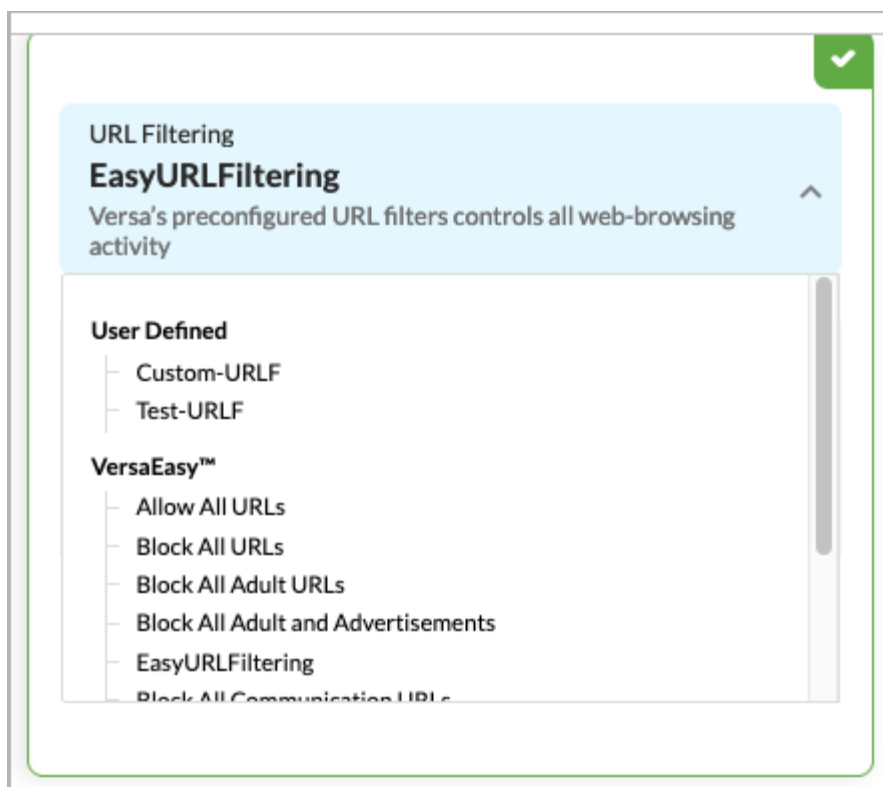
Back

Skip to Review

Next

2. To change the default settings, click the down arrow.

Note: The URL filtering profile below includes user-defined profiles in addition to predefined profiles. For more information, see [Configure Custom URL-Filtering Profiles](#).



3. Select one of the URL filters to enable only that filter. Select EasyURLFiltering to restore the default URL filtering.
4. Select other profiles to customize, or click Next to continue to Step 6, Review and Deploy.

## Configure an IPS Profile for SASE Internet Protection Rules

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.

By default, Versa SASE provides a predefined IPS enforcement policy. You can customize the IPS profile.

Note: The IPS profile displays only if the tenant is subscribed to the SWG and VSA Professional services.

To configure an IPS profile:

1. In the Security Enforcement screen > Secure Web Gateway (SWG) tab, select Intrusion Protection System (IPS) in the Profiles section to enable the preselected EasyIPS filtering security enforcement policies. By default, the following vulnerabilities are blocked from all servers and clients:
  - High-severity and medium+ confidence attacks
  - Medium+ common vulnerability scoring system (CVSS) and medium+ confidence attacks



Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

APPLICATIONS & URLS

USER GROUPS

GEO LOCATIONS

NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

Allow

Allow all traffic that matches the rule to pass

☐

Deny

Drop all traffic that matches the rule

☐

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☐

Profiles

Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Data Loss Prevention (DLP)

Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

Blocked Malware

viruses

ransomware

spyware

worms

trojans

adware

unwanted applications

URL Filtering

EasyURLFiltering

Versa's preconfigured URL filters controls all web-browsing activity

Blocked URL Categories

adult and pornography

games

web advertisements

Intrusion Protection System (IPS)

EasyIPS

Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

Blocked Vulnerabilities

high severity & medium+ confidence attacks

medium+ cvss & medium+ confidence attacks

IP Filtering

Versa Recommended Profile

Versa's preconfigured IP Filtering blocks communication with internet end points...

The following reputations will be alerted or rejected for source or destination traffic:

This Profile rejects IP addresses of wellknown exploits and alert the system administrator for other suspicious activities such as phishing activity

Alert

spam sources

phishing

web attacks

scanners

denial of service

reputation

network

Reject

proxy

window exploits

botnets

File Filtering

EasyFileFiltering

Versa's preconfigured file filtering protects from unwanted and malicious files

Alert

ftp

http

imap

mapl

pop3

smtp

http2

DNS Filtering

EasyDNS

Versa's preconfigured domain name system allows you to block access to sites and protect...

Alert

bad traffic

bots

dos

spam

scanners

window exploits

unwanted applications

Cancel

Back

Skip to Review

Next

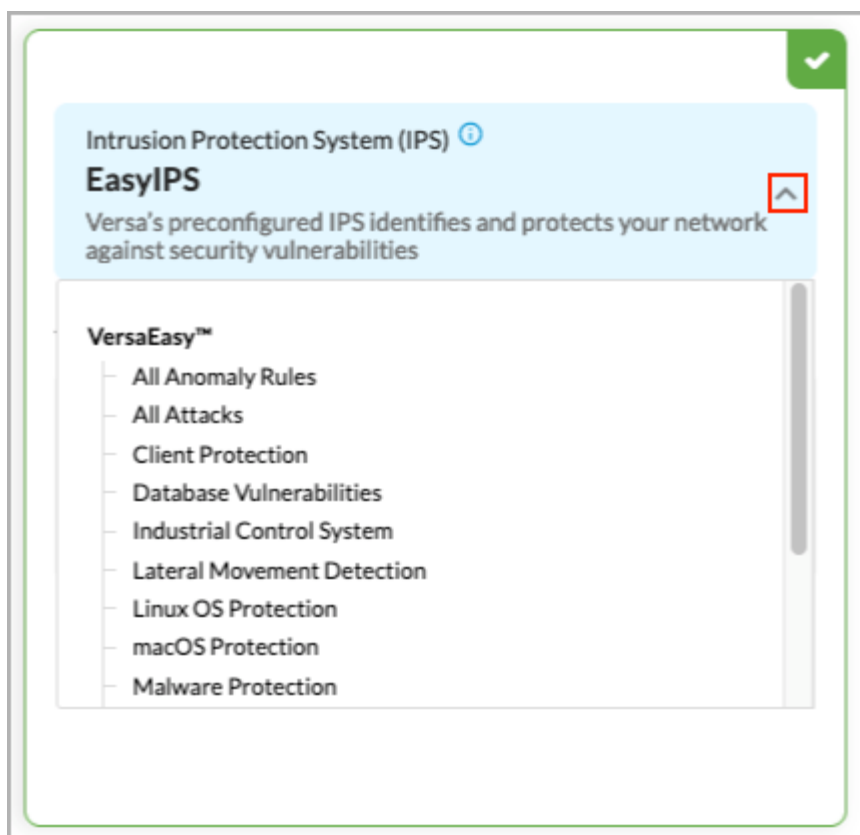
2. To change the default settings, click the down arrow.

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

41



3. Select one of the IPS filters listed to enable only that filter, and then enter information for the following fields. Select EasyIPS to restore the default IPS-filtering settings.

Profile	Description
All Anomaly Rules	Load all the anomaly signatures. Anomaly rules have predefined threshold values for each signature.
All Attacks	Load all attack signatures and implement all the available rules.
Client Protection	Load all client-side attacks (for example, browser-based vulnerabilities and client software vulnerabilities).
Database Vulnerabilities	Load the Oracle database server vulnerability signatures.
Industrial Control System	Load the industrial control system (ICS) vulnerability signatures.

Profile	Description
Lateral Movement Detection	Detect post-exploitation activities in Windows OS.
Linux OS Protection	Detect all attacks specific to Linux OS.
MacOS Protection	Detect all attacks specific to MacOS.
Malware Protection	Detect all antivirus attacks.
Server Protection	Detect server-side attacks.
Versa Branch Protection	Enable rules to detect vulnerabilities against servers and client, but by using less memory. These profiles cover the CVSS range 6 through 10 vulnerabilities for the last 5 years and the CVSS range 7 through 10 for the last 10 years.
EasyIPS	Enable rules to detect vulnerabilities against servers and clients. These profiles cover the CVSS range 6 through 10 vulnerabilities for the last 10 years and critical vulnerabilities older than 10 years. Versa recommends that you use this profile.
Windows OS Protection	Detect attacks specific to all Windows OSs.

4. Select other profiles to customize, or click Next to continue to Step 6, Review and Deploy.

---

## Configure an IP-Filtering Profile for Internet Protection Rules

Traffic passing through the network may have IP addresses that may cause security risks to your network. By default, Versa SASE provides a predefined security enforcement policy to filter traffic by IP address. You can customize the IP-filtering profile if desired.

In addition to using predefined IP-filtering profiles, you can create custom IP-filtering profiles and associate them with internet protection rules. For more information, see [Configure Custom IP-Filtering Profiles](#).

To configure an IP-filtering profile:

1. In the Security Enforcement screen > Secure Web Gateway (SWG) tab, select IP Filtering in the Profiles section to enable the preselected IP-filtering security enforcement policies. By default, traffic associated with the following types of security risks generates alerts:
  - Denial of service
  - Network
  - Phishing
  - Reputation
  - Scanners

- Spam sources
- Web attacks

By default, traffic associated with the following types of security risks is rejected:

- Botnets
- Proxy
- Window exploits

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

APPLICATIONS & URLS

USER GROUPS

GEO LOCATIONS

NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

Allow

Allow all traffic that matches the rule to pass

☐

Deny

Drop all traffic that matches the rule

☐

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☐

Profiles

Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Data Loss Prevention (DLP)

Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

Blocked Malware

viruses

ransomware

spyware

worms

trojans

adware

unwanted applications

URL Filtering

EasyURLFiltering

Versa's preconfigured URL filters controls all web-browsing activity

Blocked URL Categories

adult and pornography

games

web advertisements

Intrusion Protection System (IPS)

EasyIPS

Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

Blocked Vulnerabilities

high severity & medium+ confidence attacks

medium+ cvss & medium+ confidence attacks

IP Filtering

Versa Recommended Profile

Versa's preconfigured IP Filtering blocks communication with internet end points...

The following reputations will be alerted or rejected for source or destination traffic:

This Profile rejects IP addresses of wellknown exploits and alert the system administrator for other suspicious activities such as phishing activity

Alert

spam sources

phishing

web attacks

scanners

denial of service

reputation

network

Reject

proxy

window exploits

botnets

File Filtering

EasyFileFiltering

Versa's preconfigured file filtering protects from unwanted and malicious files

Alert

ftp

http

imap

mapl

pop3

smtp

http2

DNS Filtering

EasyDNS

Versa's preconfigured domain name system allows you to block access to sites and protect...

Alert

bad traffic

bots

dos

spam

scanners

window exploits

unwanted applications

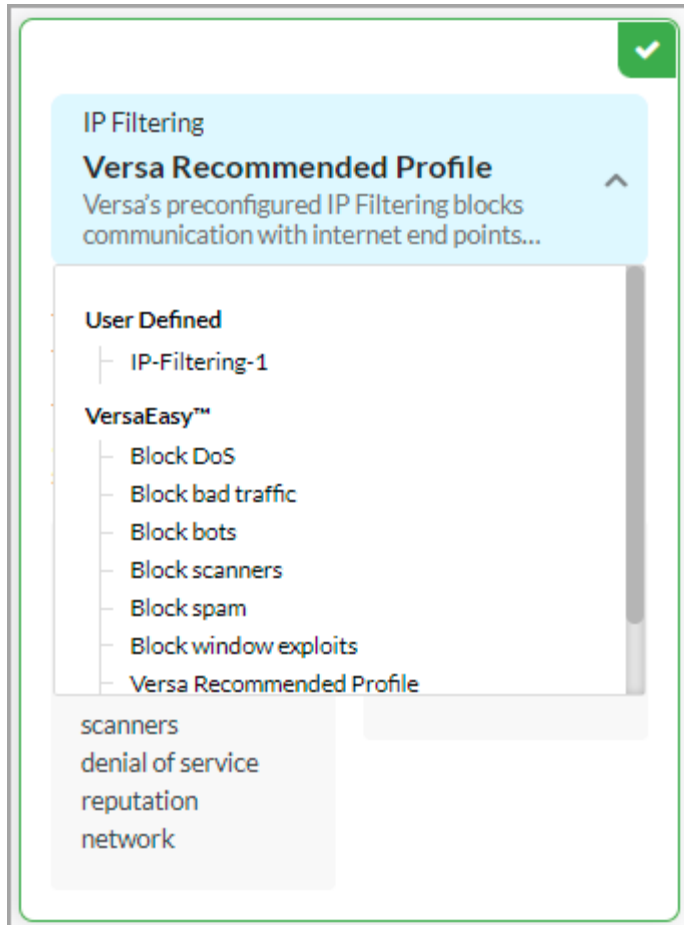
Cancel

Back

Skip to Review

Next

- To change the default settings, click the down arrow.  
Note: The IP-filtering profile below includes user-defined profiles in addition to predefined profiles. For more information, see [Configure Custom IP-Filtering Profiles](#).



3. Select one of the items listed to enable only that filter, and then enter information for the following fields. Select Vera Recommended Profile to restore the default IP-filtering settings.

Field	Description
Block DoS	Apply reputation-based actions for the botnets, DoS, network, reputation, and scanners reputations.
Block Bad Traffic	Apply reputation-based actions for the botnets, DoS, network, phishing, proxy, reputation, scanners, spam sources, web attacks, and Windows exploits reputations.
Block Bots	Apply reputation-based actions for the botnets, DoS, network, reputation, and scanners reputations.
Block Scanners	Apply reputation-based actions for the scanners reputation.
Block Spam	Apply reputation-based actions for the spam sources reputation.
Block Window Exploits	Apply reputation-based actions for the Windows exploits reputation
Web Protection	Apply reputation-based actions for the botnet, DoS, phishing, reputation, spam sources, and web attacks reputations.

4. Select other profiles to customize, or click Next to continue to Step 6, Review and Deploy.

---

## Configure a File-Filtering Profile for Internet Protection Rules

File filtering helps to reduce the risk of attacks from unwanted and malicious files associated with various protocols. By blocking the transfer of potentially dangerous files and types of files, you decrease an attacker's ability to attack your organization.

In addition to using predefined file-filtering profiles, you can create custom file-filtering profiles and associate them with internet protection rules. For more information, see [Configure Custom File-Filtering Profiles](#).

To configure an file-filtering profile:

1. In the Security Enforcement screen > Secure Web Gateway (SWG) tab, select File Filtering in the Profiles section to enable the preselected file-filtering security enforcement policies. By default, files associated with the following protocols generate alerts. You cannot change the default file-filtering alert settings.
  - FTP
  - HTTP
  - HTTP2
  - IMAP
  - MAPI

- POP3
- SMTP

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

Match Criteria

1 APPLICATIONS & URLS 2 USER GROUPS 3 GEO LOCATIONS 4 NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4 5 SECURITY ENFORCEMENT 6 REVIEW & DEPLOY

We have preselected your security enforcements, below  
You can unselect and customize any configuration you'd like to enforce.

☐ **Allow**  
Allow all traffic that matches the rule to pass

☐ **Deny**  
Drop all traffic that matches the rule

☒ **Reject**  
Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☐ **Profiles**  
Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

**Secure Web Gateway (SWG)** Cloud Access Security Broker (CASB - Inline) Data Loss Prevention (DLP)

**Malware Protection**  
**Easy Malware Protection**  
Versa's preconfigured malware protection scans web and email traffic

**Blocked Malware**

- viruses
- ransomware
- spyware
- worms
- trojans
- adware
- unwanted applications

**URL Filtering**  
**EasyURLFiltering**  
Versa's preconfigured URL filters controls all web-browsing activity

**Blocked URL Categories**

- adult and pornography
- games
- web advertisements

**Intrusion Protection System (IPS)**  
**EasyIPS**  
Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

**Blocked Vulnerabilities**

- high severity & medium+ confidence attacks
- medium+ cvss & medium+ confidence attacks

**IP Filtering**  
**Versa Recommended Profile**  
Versa's preconfigured IP Filtering blocks communication with internet end points...

The following reputations will be alerted or rejected for source or destination traffic:

This Profile rejects IP addresses of wellknown exploits and alert the system administrator for other suspicious activities such as phishing activity

**Alert**

- spam sources
- phishing
- web attacks
- scanners
- denial of service
- reputation
- network

**Reject**

- proxy
- window exploits
- botnets

**File Filtering**  
**EasyFileFiltering**  
Versa's preconfigured file filtering protects from unwanted and malicious files

**Alert**

- ftp
- http
- imap
- mapl
- pop3
- smtp
- http2

**DNS Filtering**  
**EasyDNS**  
Versa's preconfigured domain name system allows you to block access to sites and protect...

**Alert**

- bad traffic
- bots
- dos
- spam
- scanners
- window exploits
- unwanted applications

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

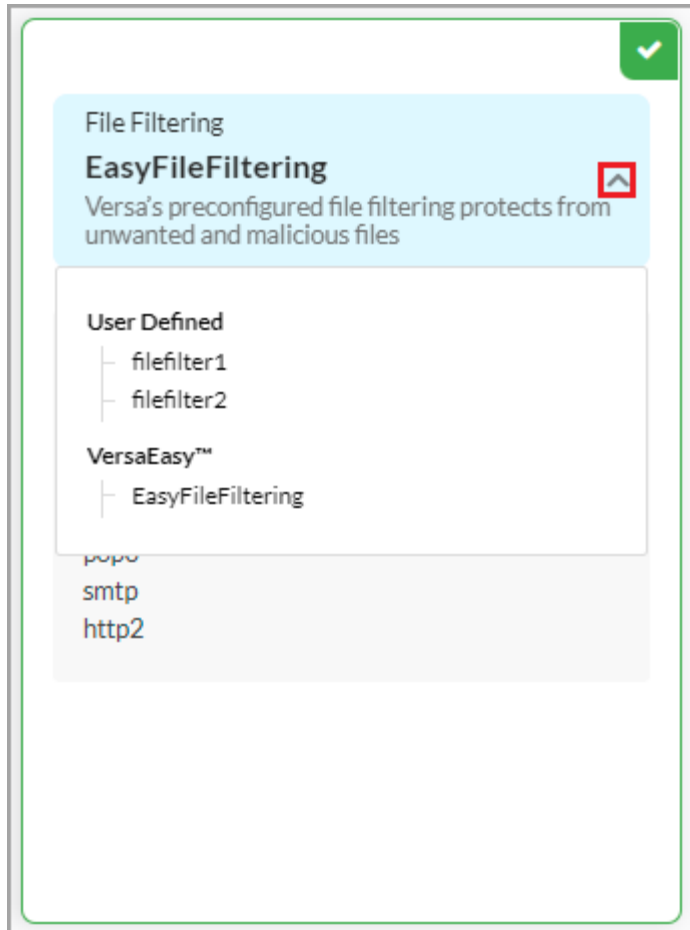
Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.



2. To change the default settings, click the down arrow.

Note: The file-filtering profile below includes user-defined profiles in addition to predefined profiles. For more information, see [Configure Custom File-Filtering Profiles](#).



3. Select one of the items listed to enable only that filter. Select EasyFileFiltering to restore the default file-filtering settings.
4. Select other profiles to customize, or click Next to continue to Step 6, Review and Deploy.

---

## Configure a DNS-Filtering Profile for Internet Protection Rules

Domain Name System (DNS) filtering blocks access to DNS queries for websites, webpages, and IP addresses, to provide protection from malicious websites, such as known malware and phishing sites. DNS filtering uses the DNS service to block web sites either by domain name or by IP address.

In addition to using predefined DNS-filtering profiles, you can create custom DNS-filtering profiles and associate them with internet protection rules. For more information, see [Configure Custom DNS-Filtering Profiles](#).

To configure a DNS-filtering profile:

1. In the Security Enforcement screen > Secure Web Gateway (SWG) tab, select DNS Filtering in the Profiles section

---

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

to enable the preselected DNS-filtering security enforcement policies. By default, the following cloud service file types generate alerts:

- Bad traffic
- Bots
- DoS
- Spam
- Scanners
- Unwanted applications
- Window exploits

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

APPLICATIONS & URLS

USER GROUPS

GEO LOCATIONS

NETWORK (INCLUDE OR EXCLUDE) LAYER 3-4

SECURITY ENFORCEMENT

REVIEW & DEPLOY

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

Allow

Allow all traffic that matches the rule to pass

☐

Deny

Drop all traffic that matches the rule

☐

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☐

Profiles

Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Data Loss Prevention (DLP)

Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

Blocked Malware

viruses

ransomware

spyware

worms

trojans

adware

unwanted applications

URL Filtering

EasyURLFiltering

Versa's preconfigured URL filters controls all web-browsing activity

Blocked URL Categories

adult and pornography

games

web advertisements

Intrusion Protection System (IPS)

EasyIPS

Versa's preconfigured IPS identifies and protects your network against security vulnerabilities

Blocked Vulnerabilities

high severity & medium+ confidence attacks

medium+ cvss & medium+ confidence attacks

IP Filtering

Versa Recommended Profile

Versa's preconfigured IP Filtering blocks communication with internet end points...

The following reputations will be alerted or rejected for source or destination traffic:

This Profile rejects IP addresses of wellknown exploits and alert the system administrator for other suspicious activities such as phishing activity

Alert

spam sources

phishing

web attacks

scanners

denial of service

reputation

network

Reject

proxy

window exploits

botnets

File Filtering

EasyFileFiltering

Versa's preconfigured file filtering protects from unwanted and malicious files

Alert

ftp

http

imap

mapl

pop3

smtp

http2

DNS Filtering

EasyDNS

Versa's preconfigured domain name system allows you to block access to sites and protect...

Alert

bad traffic

bots

dos

spam

scanners

window exploits

unwanted applications

Cancel

Back

Skip to Review

Next

2. To change the default settings, click the down arrow.

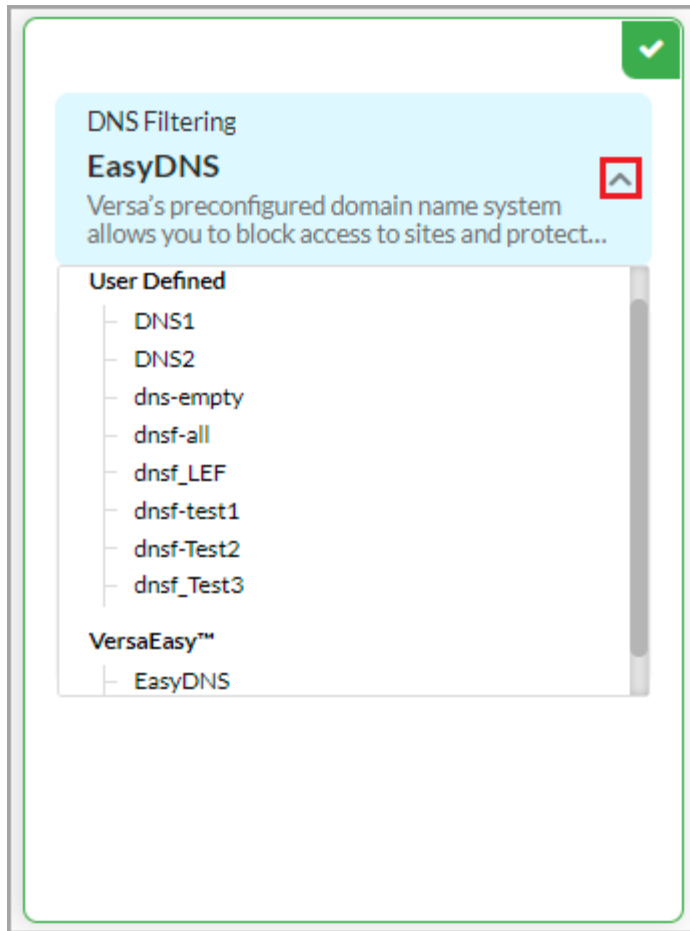
Note: The DNS-filtering profile below includes user-defined profiles in addition to predefined profiles. For more information, see [Configure Custom DNS-Filtering Profiles](#).

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

51



3. Select one of the items listed to enable only that filter. Select EasyDNS to restore the default file-filtering settings.
4. Select other profiles to customize, or click Next to continue to Step 6, Review and Deploy.

---

## Configure a CASB Profile for Internet Protection Rules

Cloud Access Security Broker (CASB) is on-premises or cloud-based policy enforcement software that secures the data flowing between users and cloud applications to comply with corporate and regulatory requirements. CASB applies enterprise security policies when users access cloud-based resources.

You can associate a CASB profile with a SASE internet protection rule to allow or deny traffic. CASB secures the data flowing between users and cloud applications to comply with corporate and regulatory requirements. For more information, see [Configure CASB Profiles](#).

To associate a CASB profile with a SASE internet protection rule:

1. In the Security Enforcement screen, select Profiles. Then, select the Cloud Access Security Broker (CASB - Inline) tab and enable CASB.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

APPLICATIONS & URLS

2

3

4

5

SECURITY ENFORCEMENT

6

Match Criteria

Action

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.

☐

✓

Allow

Allow all traffic that matches the rule to pass

☒

⊘

Deny

Drop all traffic that matches the rule

☐

⊘

Reject

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☒

✓

Profiles

Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

Data Loss Prevention (DLP)

Enable Cloud Access Security Broker?

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

⊘

Cancel

Back

Skip to Review

Next

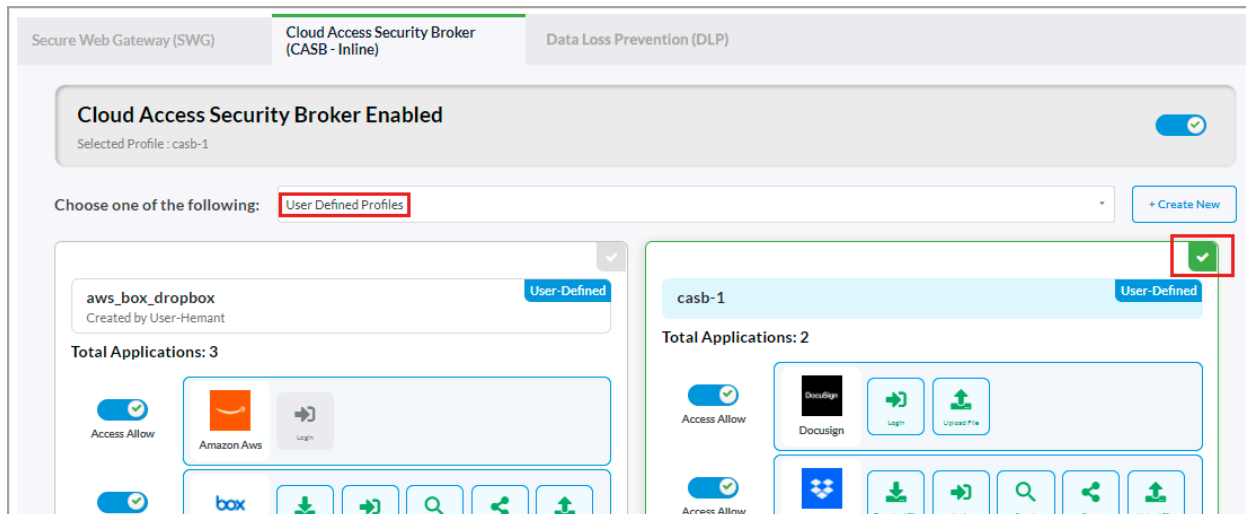
2. Select User-Defined Profiles, and then select the CASB profile to associate with the internet protection rule.

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

53



3. To add a CASB profile, click Create New. The Create Cloud Access Security Broker Profile screen displays. For more information, see [Configure CASB Profiles](#).
4. Click Next to go to Step 6, Review and Deploy.

## Configure a DLP Profile for Internet Protection Rules

To oversee, track, and report all data transactions in the network and to scan all content that passes through an organization's ports and protocols to ensure data security in the organization you associate a DLP profile with a SASE internet protection rule. DLP provides a set of tools and processes for detecting and preventing data breaches, cyber exfiltration, and unwanted destruction of sensitive data. You use DLP to protect and secure an organization's data and to comply with regulations. To create DLP profiles, see [Configure Data Loss Prevention in Concerto](#).

To associate a DLP profile with a SASE internet protection rule:

1. In the Security Enforcement screen, select Profiles, and then select the Data Loss Prevention (DLP) tab.

Configure > SASE > Real-Time Protection > Internet Protection  
 Edit Internet Protection Rule: UnManaged-Endpoint-Access

1 APPLICATIONS 2 USER GROUPS 3 ENDPOINT INFORMATION PROTECTION (EIP) 4 GEO LOCATIONS 5 NETWORK LAYER 3-4 6 SECURITY ENFORCEMENT 7 REVIEW & DEPLOY

We have preselected your security enforcements, below  
 You can unselect and customize any configuration you'd like to enforce.

☐ **Allow**  
 Allow all traffic that matches the rule to pass

☐ **Deny**  
 Drop all traffic that matches the rule

☐ **Reject**  
 Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☒ **Profiles**  
 Choose one or more predefined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG) Cloud Access Security Broker (CASB - Inline) **Data Loss Prevention (DLP)**

**Enable Data Loss Prevention?** ☐

Cancel Back Skip to Review Next

2. Click the slider to enable DLP, and then choose a DLP profile.

Secure Web Gateway (SWG) Cloud Access Security Broker (CASB - Inline) **Data Loss Prevention (DLP)**

**Data Loss Prevention Enabled** ☒

DLPProfile1 [+ Create New](#)

**DLPProfile1**  
 Exit: Exit On First Rule Match Default Action: Alert

ORDER	NAME	RULE TYPE	ACTIVITIES	CONTEXT	PROTOCOL	FILE TYPE
1	dlprule2	Content Analysis	Allow	Body	FTP, IMAP	c
2	dlprule1	Content Analysis	Forensic	Attachment	HTTP, FTP, POP3	avi, bat, docx, pdf

3. Click Next to continue to Step 6, Review and Deploy.

## Configure an ATP Profile for Internet Protection Rules

Versa advanced threat protection (ATP) provides mechanisms that detect zero-day threats and prevent these threats from affecting organizations. To enforce Versa ATP detection mechanisms for internet traffic, you associate an ATP profile with a SASE internet protection rule. For more information, see [Configure Advanced Threat Protection](#).

To associate an ATP profile with a SASE internet protection rule:

1. In the Security Enforcement screen, select Profiles. Then select the Advanced Threat Protection (ATP) tab and

click the toggle to enable ATP.

Configure > SASE > Real-Time Protection > Internet Protection

### Create Internet Protection Rule

1

2

3

4

5

6

7

Applications & URLs

Users & Groups

Endpoint Information Profile (EIP)

GEO Locations

Network Layer 3-4


Security Enforcement

Review & Deploy

We have preselected your security enforcements, below

You can unselect and customize any configuration you'd like to enforce.


☐



**Allow**

Allow all traffic that matches the rule to pass


☐



**Deny**

Drop all traffic that matches the rule


☐



**Reject**

Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

☒



**Profiles**


Choose one or more predefined or user defined security enforcements which include criteria to allow or reject traffic.

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB - Inline)

**Advanced Threat Protection (ATP)**

**Advanced Threat Protection**



+ Create New

Advanced Threat Protection  
ATP-2

The following sandbox rules will be used in if malware is found

Sandbox Rules	ATP Action	Protocols	File Types
---------------	------------	-----------	------------

Advanced Threat Protection  
ATP-Allow-Clean-File

The following sandbox rules will be used in if malware is found

Sandbox Rules	ATP Action	Protocols	File Types
ATP-Sandbox-Rule1	AllowCleanFiles	HTTP,FTP,SMTP,IMAP,POP3,MAPI	all

Cancel

Back

Skip to Review

Next

2. Select the ATP profile to associate with the internet protection rule.
3. To create a new ATP profile, click + Create New. The Create ATP Profile screen displays. For more information,

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.



see [Configure ATP Profiles](#).

4. Click Next to review and then deploy the internet protection rule.



---

## Review and Deploy Internet Protection Rules

The final step in configuring internet protection rules is to review the choices you have made, edit them if needed, and then deploy the rule.

To review and deploy the internet protection rule:

1. In the Security Enforcement screen, select Review and Deploy and then enter information for the following fields.

Field	Description
Name (Required)	Enter a name for the rule. The name can be a maximum of 63 characters and can include alphanumeric characters, underscores, and hyphens.
Description (Optional)	Enter a description for the rule.
Tags (Optional)	Enter a text string or phrase to associate with the rule. A tag is an alphanumeric text descriptor with no white spaces or special characters that you can use to search rules. You can specify multiple tags.
Rule is Enabled	<p>Click the slide bar to enable the rule:</p>  <p>Click the slide bar again to disable the rule:</p> 

2. Click Save to deploy the new internet protection rule.

## Supported Software Information

Releases 11.1.1 and later support all content described in this article, except:

- Release 11.4.1 provides separate tabs for Source Address, Destination Address, Source Zones and Sites, and Destination Zones and Sites for SASE Source and Destination Traffic for Internet Protection Rules.
- Release 12.1.1 allows you to clone Internet Protection Rules.

## Additional Information

[Configure CASB Profiles](#)

[Configure Custom DNS-Filtering Profiles](#)

[Configure Custom File-Filtering Profiles](#)

[Configure Custom IP-Filtering Profiles](#)

[Configure Data Loss Prevention in Concerto](#)

[https://docs.versa-networks.com/Security\\_Service\\_Edge\\_\(SSE\)/Configuration\\_from\\_Concerto/Configure\\_SASE\\_Internet\\_Pro...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Concerto/Configure_SASE_Internet_Pro...)

Updated: Wed, 23 Oct 2024 08:35:03 GMT

Copyright © 2024, Versa Networks, Inc.

[Configure SASE Private Application Protection Rules](#)

[Configure SASE Secure Client Access Rules](#)