Configure SASE Private Application Protection Rules

For supported software information, click here.

SASE private application protection rules are firewall rules that you configure to define protection for custom applications. You configure these protection rules on a per-tenant basis. Private application protection is similar to internet protection, except that private application protection applies only to custom applications. You cannot configure private application protection for predefined applications or for application groups.

Private application protection rules consist of match criteria and enforcement actions. You can configure the following match criteria and enforcement actions:

- 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 groups—Match criteria based on individual users or groups of users.
- Geolocation—Match criteria based on the geographic location of the 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—Security enforcement actions that are applied to traffic that matches the match criteria. You can allow, deny, or reject the traffic, and you can also create custom security enforcement profiles.

After you configure match criteria and security enforcement actions, you review and deploy the private protection rule.

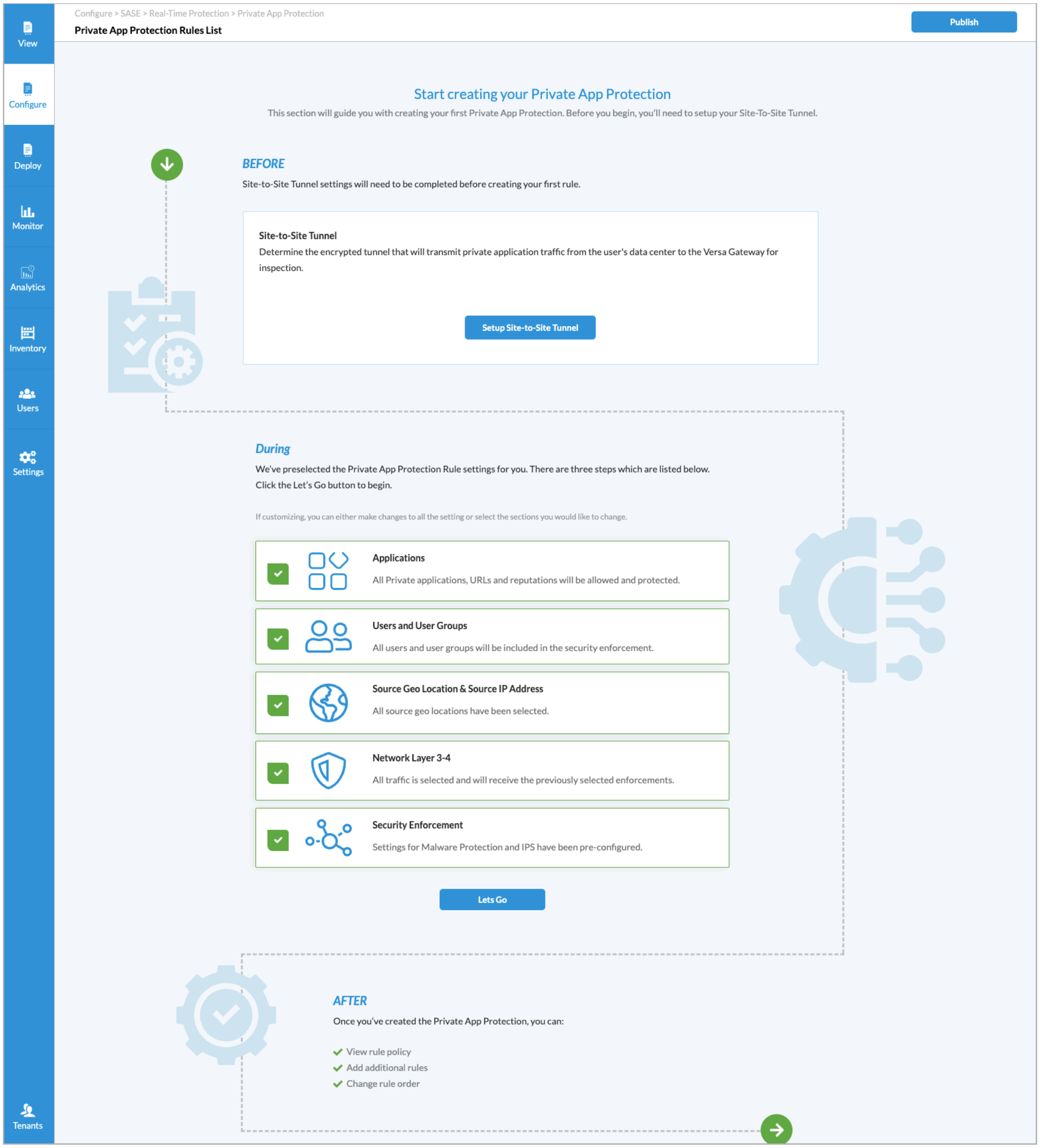
Note that you must configure the SASE rules, profiles, and settings in the following order:

1. Configure users and groups first and publish them to the gateway. For more information, see Configure Users and Device Authentication.
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, including the rules for protecting private applications discussed in this article, in any particular order.

To configure private application protection, you must first create one or more private applications under Configure > Settings > User-Defined Objects > Applications. For more information, see Configure SASE User-Defined Objects. After you have created a private application, you create a private application rule in much the same way that you configure an internet protection rule.

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



Private App Protection Rules List

Start creating your Private App Protection

This section will guide you with creating your first Private App Protection. Before you begin, you'll need to setup your Site-To-Site Tunnel.

BEFORE

Site-to-Site Tunnel settings will need to be completed before creating your first rule.

Site-to-Site Tunnel

Determine the encrypted tunnel that will transmit private application traffic from the user's data center to the Versa Gateway for inspection.

During

We've preselected the Private App Protection Rule settings for you. There are three steps which are listed below. Click the Let's Go button to begin.

If customizing, you can either make changes to all the setting or select the sections you would like to change.

☑ Applications

All Private applications, URLs and reputations will be allowed and protected.

☑ Users and User Groups

All users and user groups will be included in the security enforcement.

☑ Source Geo Location & Source IP Address

All source geo locations have been selected.

☑ Network Layer 3-4

All traffic is selected and will receive the previously selected enforcements.

☑ Security Enforcement

Settings for Malware Protection and IPS have been pre-configured.

AFTER

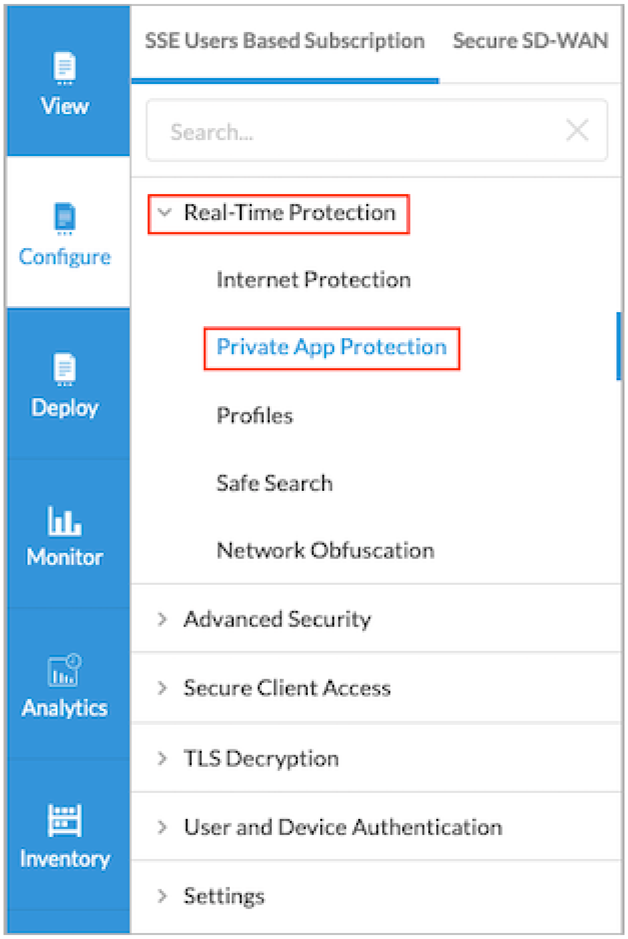
Once you've created the Private App Protection, you can:

- ✓ View rule policy
- ✓ Add additional rules
- ✓ Change rule order

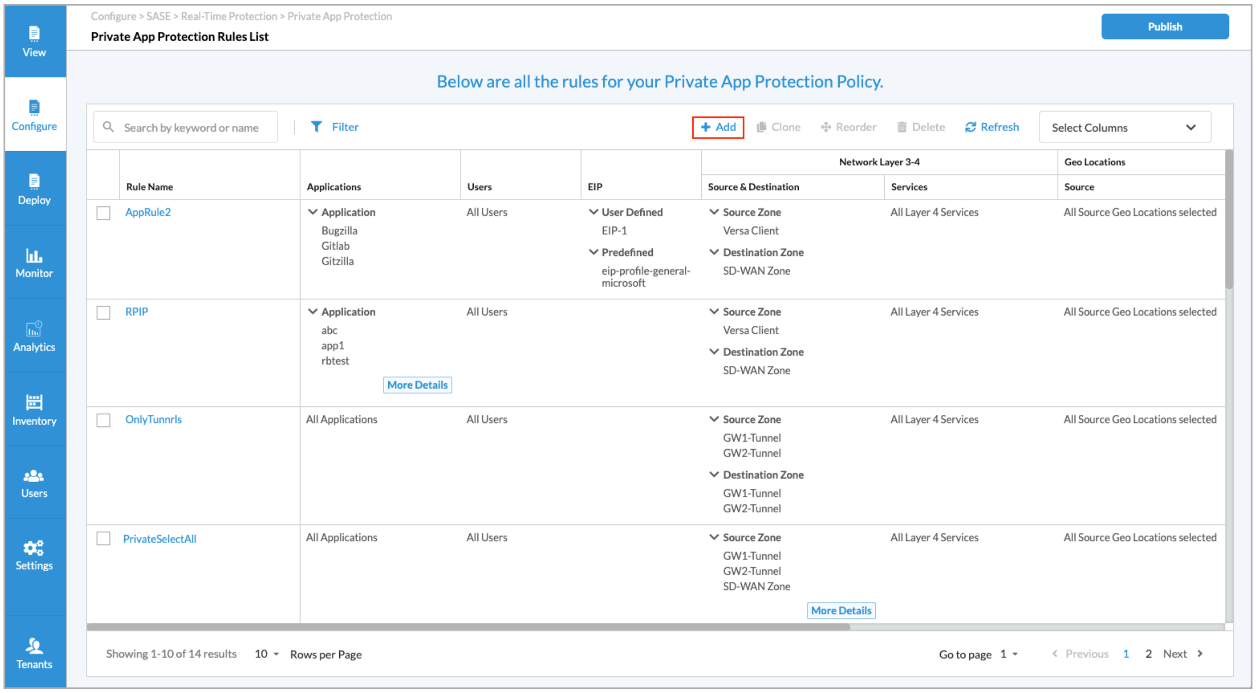
Configure SASE Private Application Protection Rule Match Criteria

To configure private application protection rule match criteria:

1. Go to Configure > Real-Time Protection > Private Application Protection.



The Private Application Protection Rules List screen displays all the private application protection rules that are already configured.



Configure > SASE > Real-Time Protection > Private App Protection

Private App Protection Rules List

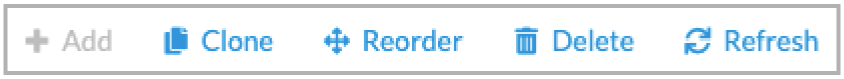
Below are all the rules for your Private App Protection Policy.

				Network Layer 3-4		Geo Locations
Rule Name	Applications	Users	EIP	Source & Destination	Services	Source
□ AppRule2	Application Bugzilla Gitlab Gitzilla	All Users	User Defined EIP-1 Predefined eip-profile-general-microsoft	Source Zone Versa Client Destination Zone SD-WAN Zone	All Layer 4 Services	All Source Geo Locations selected
□ RPIP	Application abc app1 rbtest More Details	All Users		Source Zone Versa Client Destination Zone SD-WAN Zone	All Layer 4 Services	All Source Geo Locations selected
□ OnlyTunnrls	All Applications	All Users		Source Zone GW1-Tunnel GW2-Tunnel Destination Zone GW1-Tunnel GW2-Tunnel	All Layer 4 Services	All Source Geo Locations selected
□ PrivateSelectAll	All Applications	All Users		Source Zone GW1-Tunnel GW2-Tunnel SD-WAN Zone More Details	All Layer 4 Services	All Source Geo Locations selected

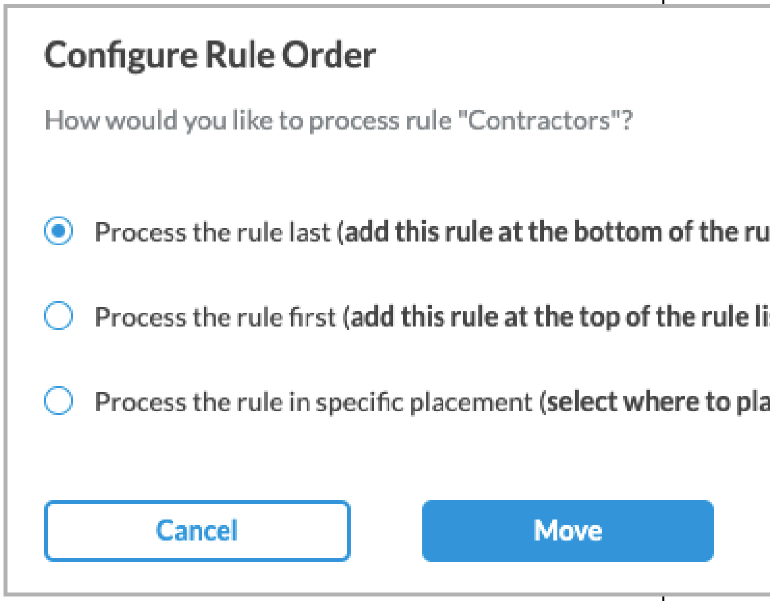
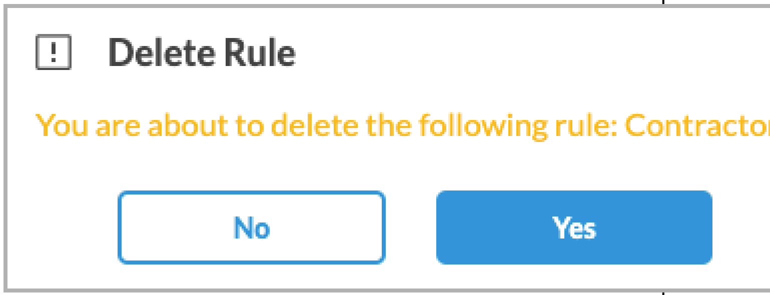
Showing 1-10 of 14 results 10 Rows per Page

Go to page 1 Previous 1 2 Next

2. In the horizontal menu bar, you can perform the following operations.

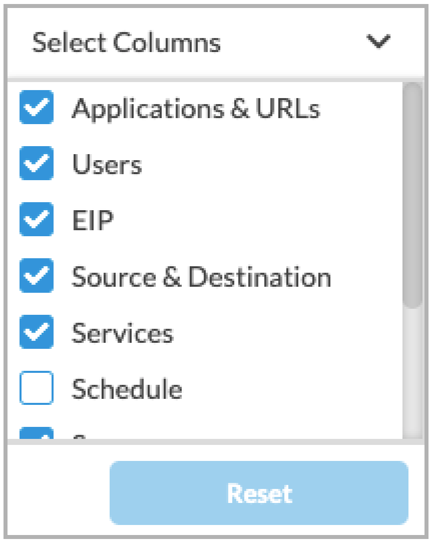


Operation	Description
Add	Create a new internet protection rule. This button is active when no existing rule is selected.
Clone	Clone the selected private application protection rule. If you select this option, the configuration wizard for the rule displays with the Review & Deploy screen selected. You can rename the default name of the cloned rule, if desired, then click Save.
Reorder	Reorder the selected private application protection rule. A popup window similar to the following displays.

Operation	Description
	 **Configure Rule Order** How would you like to process rule "Contractors"? ● Process the rule last (**add this rule at the bottom of the ru** ○ Process the rule first (**add this rule at the top of the rule li** ○ Process the rule in specific placement (**select where to pla** 1. Select one of the three options: - Process the rule last - Process the rule first - Process the rule in specific placement—A list of the existing rules displays. Click the position in the list where you want to place the rule. 2. Click Move.
Delete	Delete the selected private application protection rule. A popup window similar to the following displays.  **Delete Rule** You are about to delete the following rule: Contracto Click Yes to delete the internet protection rule, or click

Operation	Description
	No to retain the rule.
Refresh	Refresh the list of existing rules.

3. To customize which columns display, click Select Columns and then click to select or deselect the columns you want to display. Click Reset to return to the default columns settings.



☑ Applications & URLs
☑ Users
☑ EIP
☑ Source & Destination
☑ Services
☐ Schedule

The options are:
—Applications & URLs
—Users
—EIP
—Source & Destination
—Services
—Schedule
—Source
—Destination
—Security Enforcement
—Enabled

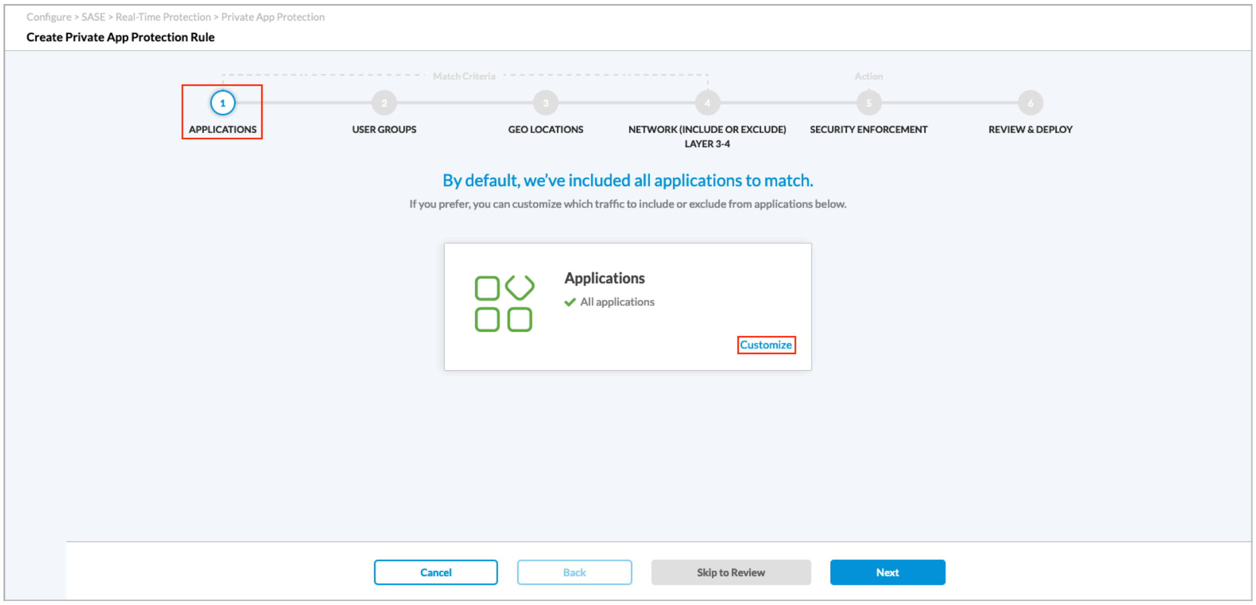
4. Proceed to the next section to configure application filtering match criteria.

Configure SASE Application Filtering Private Application Protection Rules

Private application protection rules are firewall rules for private applications, and they are applied on a per-tenant basis. Private application protection is similar to internet protection, except that it applies only to custom applications. For information about creating custom applications and application groups, see Configure SASE User-Defined Objects.

To configure application filtering for private applications:

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



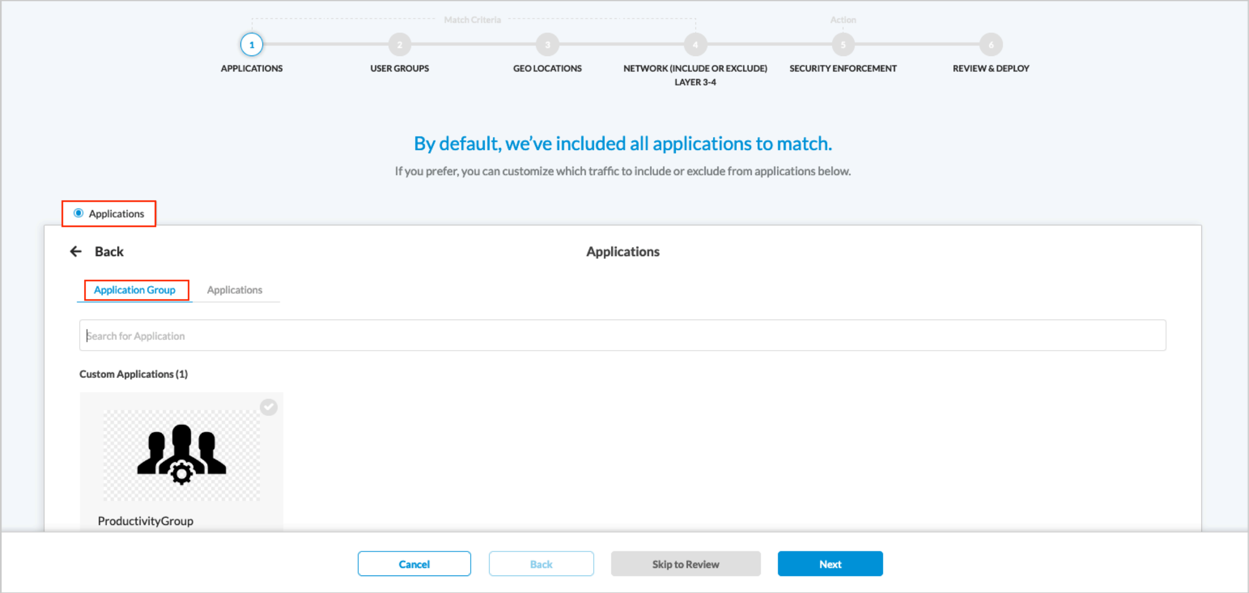
By default, we've included all applications to match.

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

Applications

✓ All applications

2. Select the first match criteria, Applications. By default, all private applications are included in the match list, which means that all private applications are matched by this rule.
3. To accept the default, click Next to continue to the next match criteria, User Groups.
4. To configure the private applications on which to filter, click Customize. The Applications screen displays, and the Application Group tab is selected by default. Any previously configured application groups display.

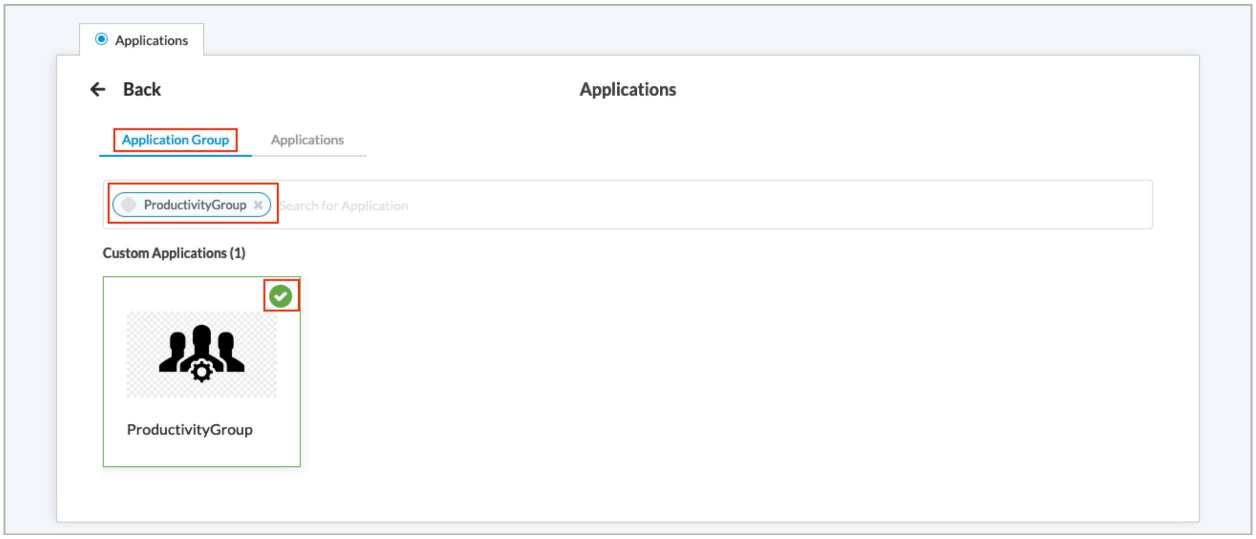


By default, we've included all applications to match.

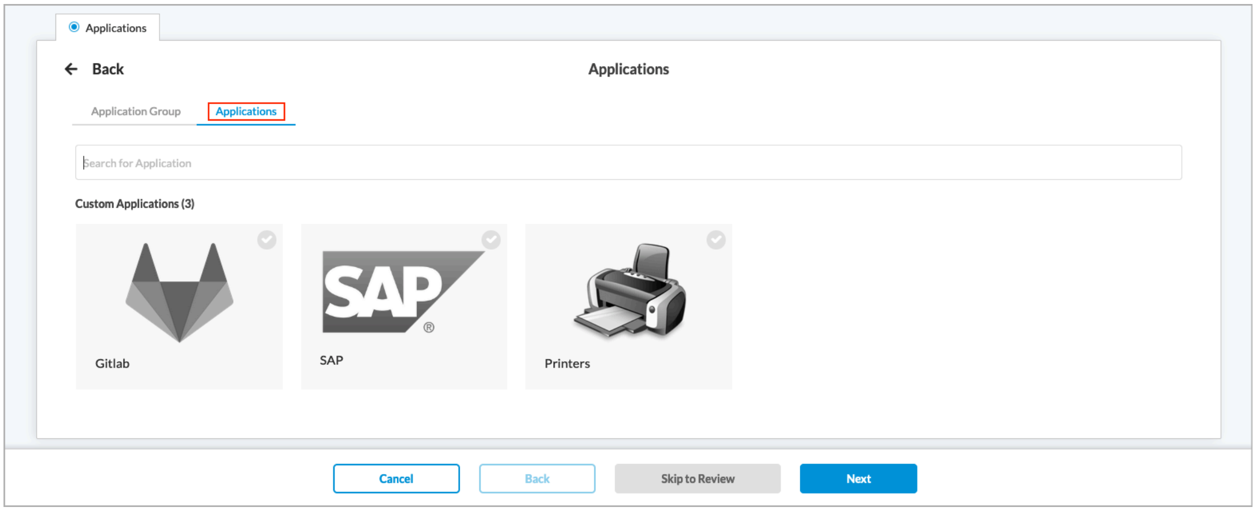
If you prefer, you can customize which traffic to include or exclude from applications below.

5. Select the application groups to include in the match list, or type the name of the application group in the search

box and then select it from the search results. In the following example, the application group ProductivityGroup is selected. To remove an application group from the list, click the X next to the application group name in the search box.



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



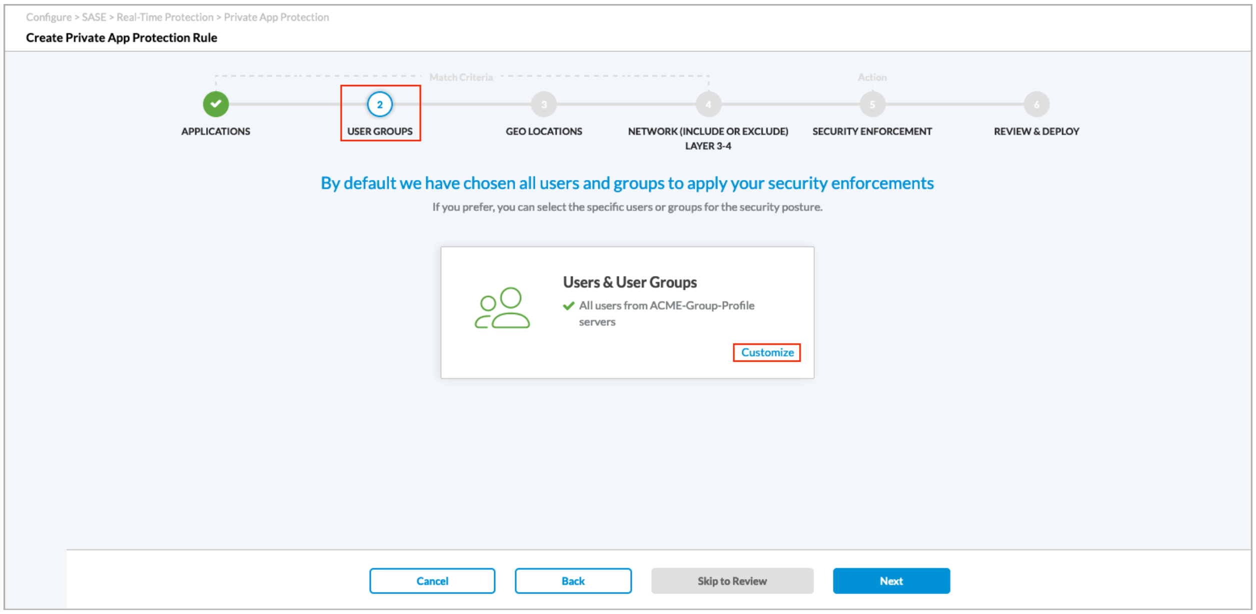
7. Select the applications to include in the match list, or type the name of the custom application in the search box and then select it from the search results.
8. Click Back to return to the Applications screen, or click Next to continue to the next match criteria, Step 2, User Groups.

Configure SASE User and User Group Private Application 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 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.

To configure user and user group private application protection rules:

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



Configure > SASE > Real-Time Protection > Private App Protection

Create Private App Protection Rule

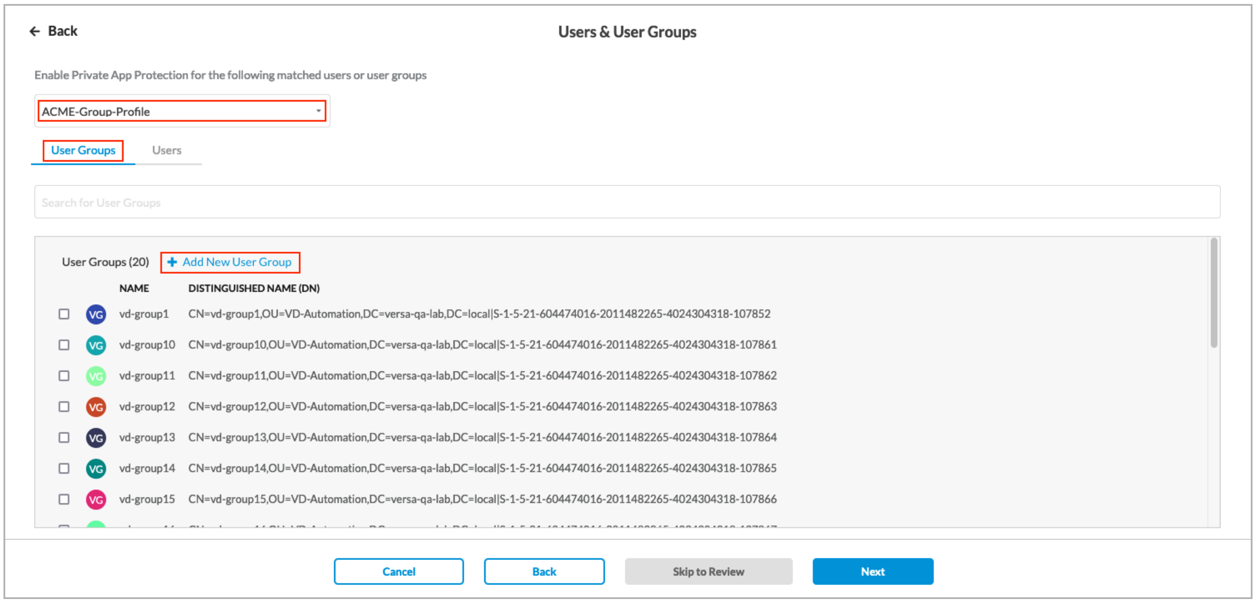
By default we have chosen all users and groups to apply your security enforcements

If you prefer, you can select the specific users or groups for the security posture.

Users & User Groups

✓ All users from ACME-Group-Profile servers

2. To accept the default, click Next to continue to Step 3, Geolocation, to configure geolocation match criteria.
3. To change the users and user groups to include in the match list, click Customize. The following screen displays. The screen displays all user groups that are already configured.



Users & User Groups

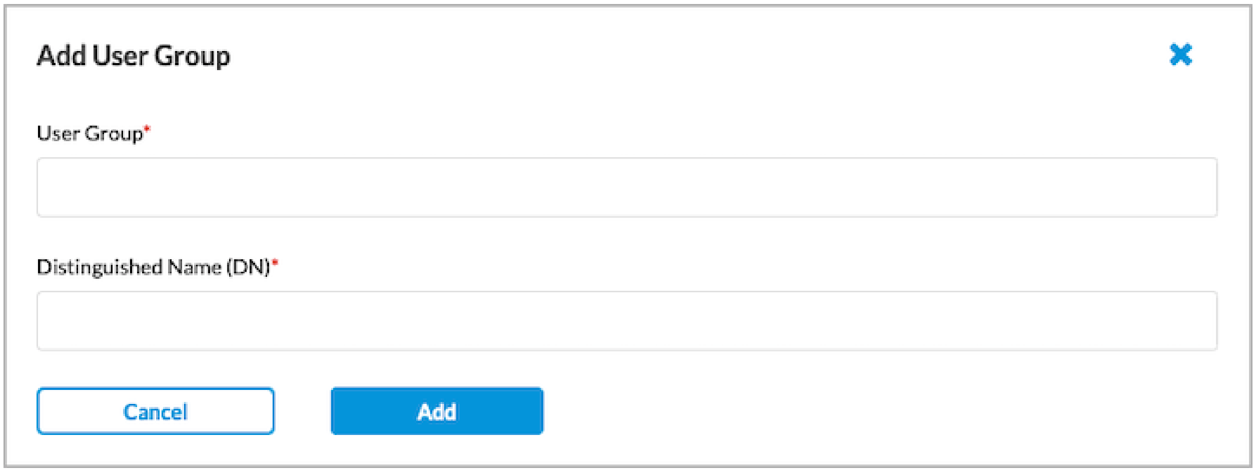
Enable Private App Protection for the following matched users or user groups

ACME-Group-Profile

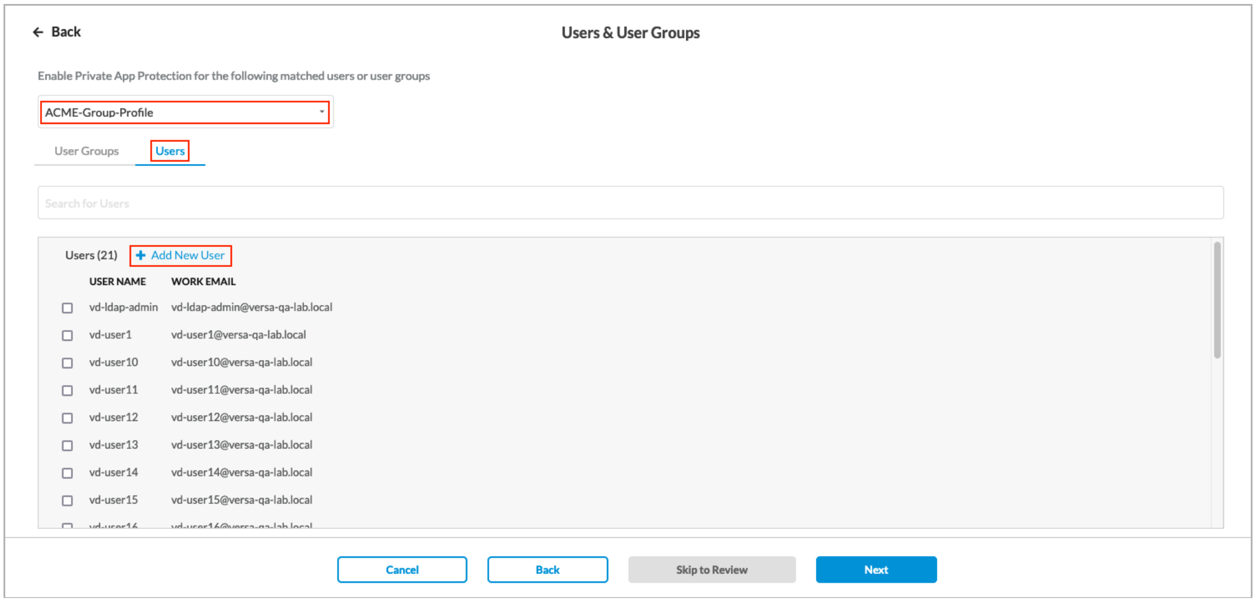
User Groups (20)

		NAME	DISTINGUISHED NAME (DN)
□	VG	vd-group1	CN=vd-group1,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107852
□	VG	vd-group10	CN=vd-group10,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107861
□	VG	vd-group11	CN=vd-group11,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107862
□	VG	vd-group12	CN=vd-group12,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107863
□	VG	vd-group13	CN=vd-group13,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107864
□	VG	vd-group14	CN=vd-group14,OU=VD-Automation,DC=versa-qa-lab,DC=local|S-1-5-21-604474016-2011482265-4024304318-107865
□	VG	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. Select the User Groups tab, and then 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 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).



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



Enable Private App Protection for the following matched users or user groups

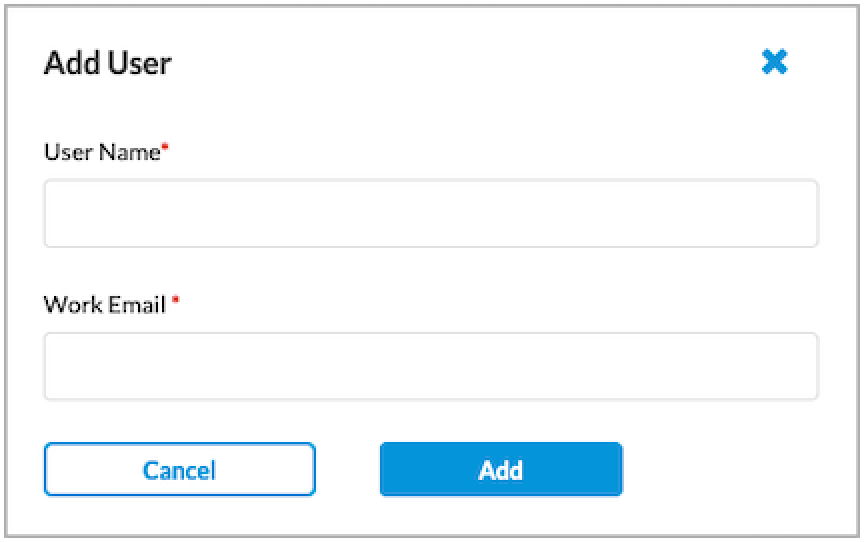
ACME-Group-Profile

Users (21)

	USER NAME	WORK EMAIL
□	vd-ldap-admin	vd-ldap-admin@versa-qa-lab.local
□	vd-user1	vd-user1@versa-qa-lab.local
□	vd-user10	vd-user10@versa-qa-lab.local
□	vd-user11	vd-user11@versa-qa-lab.local
□	vd-user12	vd-user12@versa-qa-lab.local
□	vd-user13	vd-user13@versa-qa-lab.local
□	vd-user14	vd-user14@versa-qa-lab.local
□	vd-user15	vd-user15@versa-qa-lab.local
□	vd-user16	vd-user16@versa-qa-lab.local

9. Select the group profile.
10. Select the Users tab, and then 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.



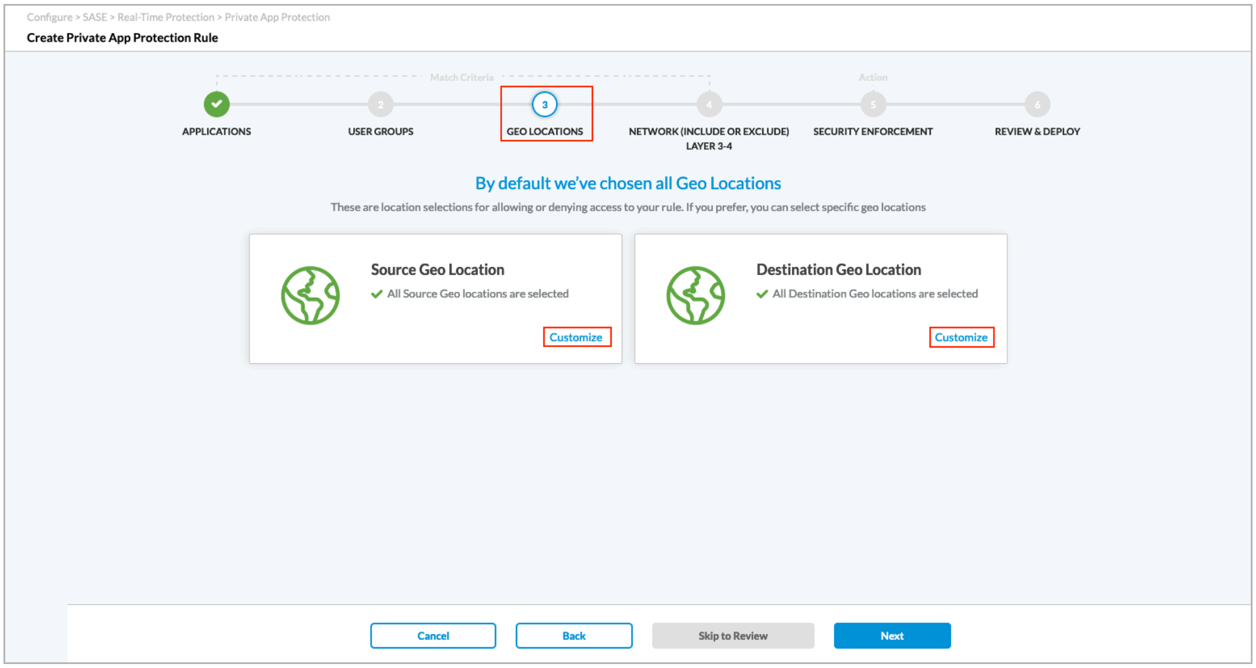
12. Click Add.
13. Click Next to continue to Step 3, Geolocation, to configure geolocation match criteria, or click Back to return to the Applications screen.

Configure SASE Geolocation Private Application Protection Rules

Versa SASE provides a list of predefined regions that you can use to create filter profiles based on both source and destination geolocation.

To configure geolocation rules:

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



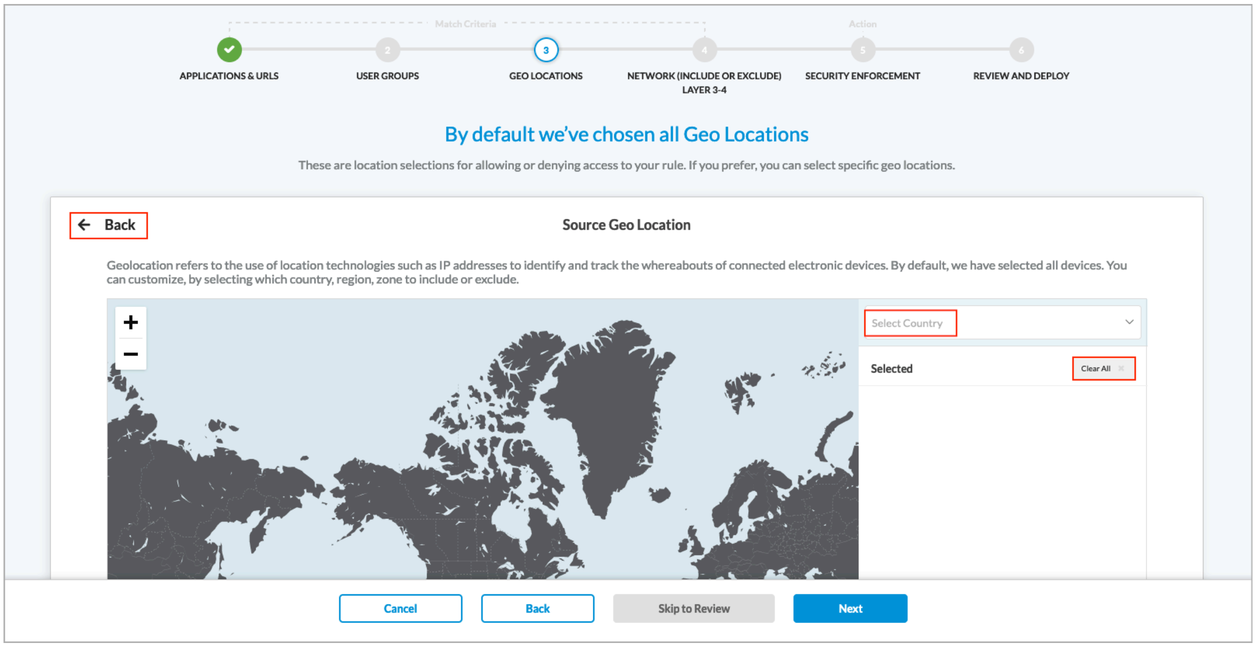
By default we've chosen all Geo Locations

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

✓ All Source Geo locations are selected

✓ All Destination Geo locations are selected

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

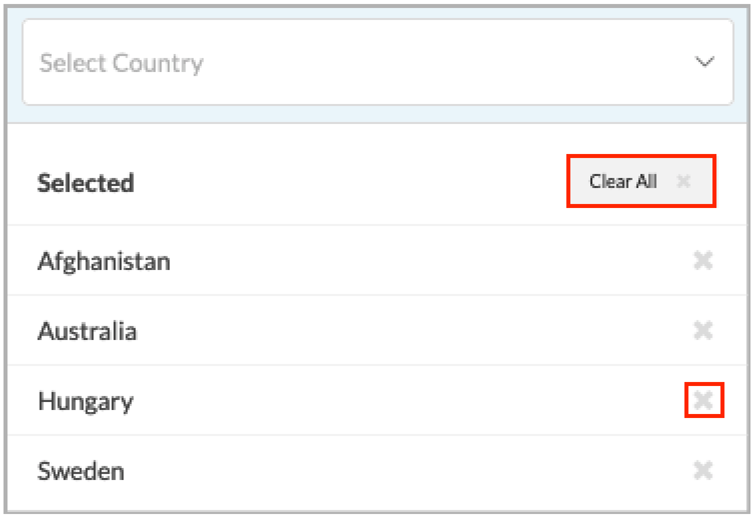


By default we've chosen all Geo Locations

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

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.

4. Click Clear All to remove any already selected source locations.
5. Click in the Select Country box, and then select one or more countries. After you select the countries, click the down arrow. The selected countries are displayed.



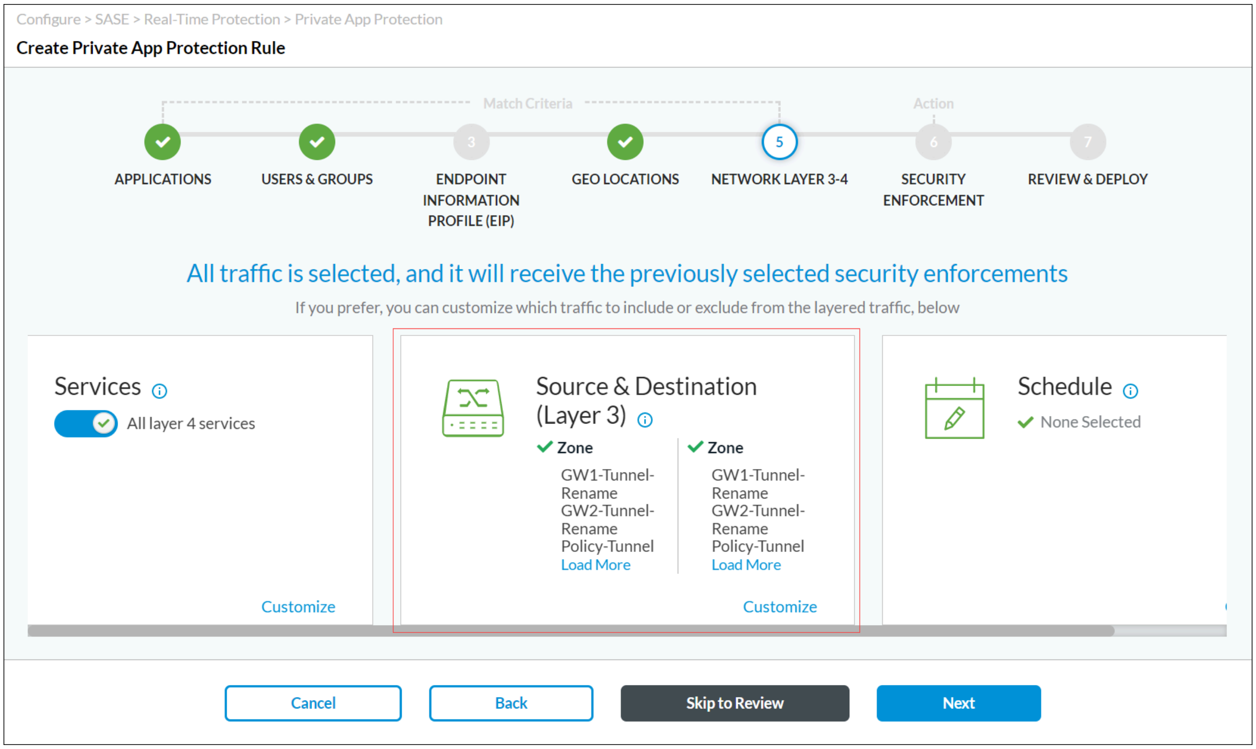
6. To remove a country from the list, click the X next to the country name.
7. To remove all countries from the list, click Clear All.
8. To customize the destination geographical locations, click Back. The Geolocation screen displays again.
9. To accept the default destination geographical locations and continue to the Step 4, Network (Include or Exclude) Layer 3-4 match criteria, click Next at the bottom of the screen.
10. To change the destination geographic locations to include in the match list, click Customize under Destination Geolocation. The Destination Geolocation screen displays.
11. Click Clear All to remove all the default destination locations.
12. Click in the Select Country box, and then select one or more countries.
13. To remove a country from the list, click the X next to the country name.
14. To remove all countries from the list, click Clear All.
15. Click Back. The Geolocations screen displays again.
16. In the Create Private Application Protection Rule screen, click the Network (Include or Exclude) Layer 3-4 match criteria, or click Next.

Configure SASE Source and Destination Traffic Private Application Protection Rules

You can create private application protection rule criteria based on the source and destination of the traffic.

To configure network rules based on source and destination traffic:

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


Configure > SASE > Real-Time Protection > Private App Protection
Create Private App Protection Rule
Match Criteria
Action
APPLICATIONS
USERS & GROUPS
3
ENDPOINT INFORMATION PROFILE (EIP)
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

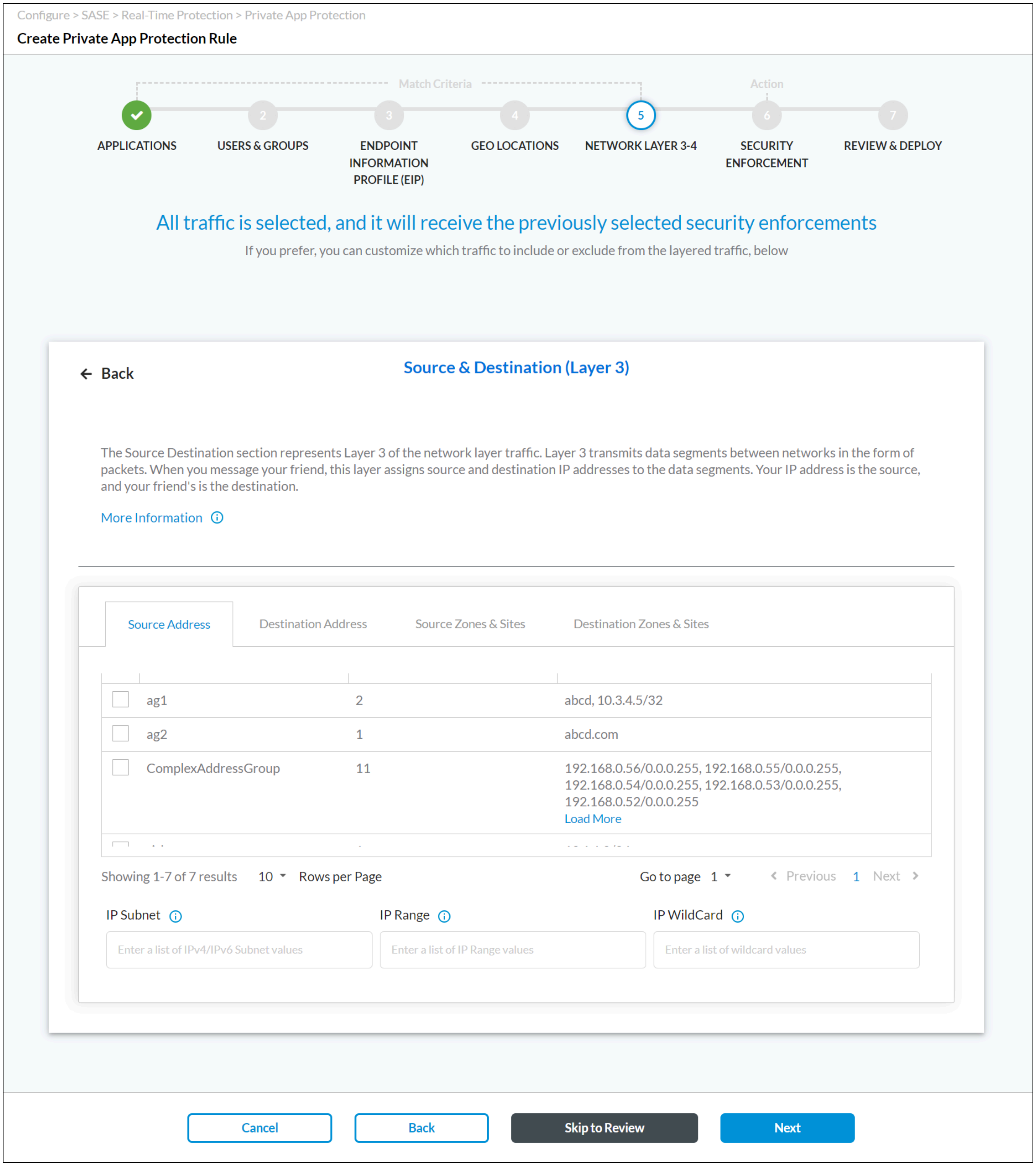
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

Services
All layer 4 services
Customize

Source & Destination (Layer 3)
✓ Zone
GW1-Tunnel-Rename
GW2-Tunnel-Rename
Policy-Tunnel
Load More
✓ Zone
GW1-Tunnel-Rename
GW2-Tunnel-Rename
Policy-Tunnel
Load More
Customize

Schedule
✓ None Selected

2. To accept the default, click Next to continue to Step 6, Security Enforcement.
3. To change the source and destination traffic to include in the match, click Customize in the Source & Destination (Layer 3) box. In the Source & Destination (Layer 3) screen, select the 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.



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

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 ⓘ

□	ag1	2	abcd, 10.3.4.5/32
□	ag2	1	abcd.com
□	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 Load More

Showing 1-7 of 7 results 10 ▾ Rows per Page Go to page 1 ▾ ‹ Previous 1 Next ›

IP Subnet ⓘ: Enter a list of IPv4/IPv6 Subnet values

IP Range ⓘ: Enter a list of IP Range values

IP WildCard ⓘ: Enter a list of wildcard values

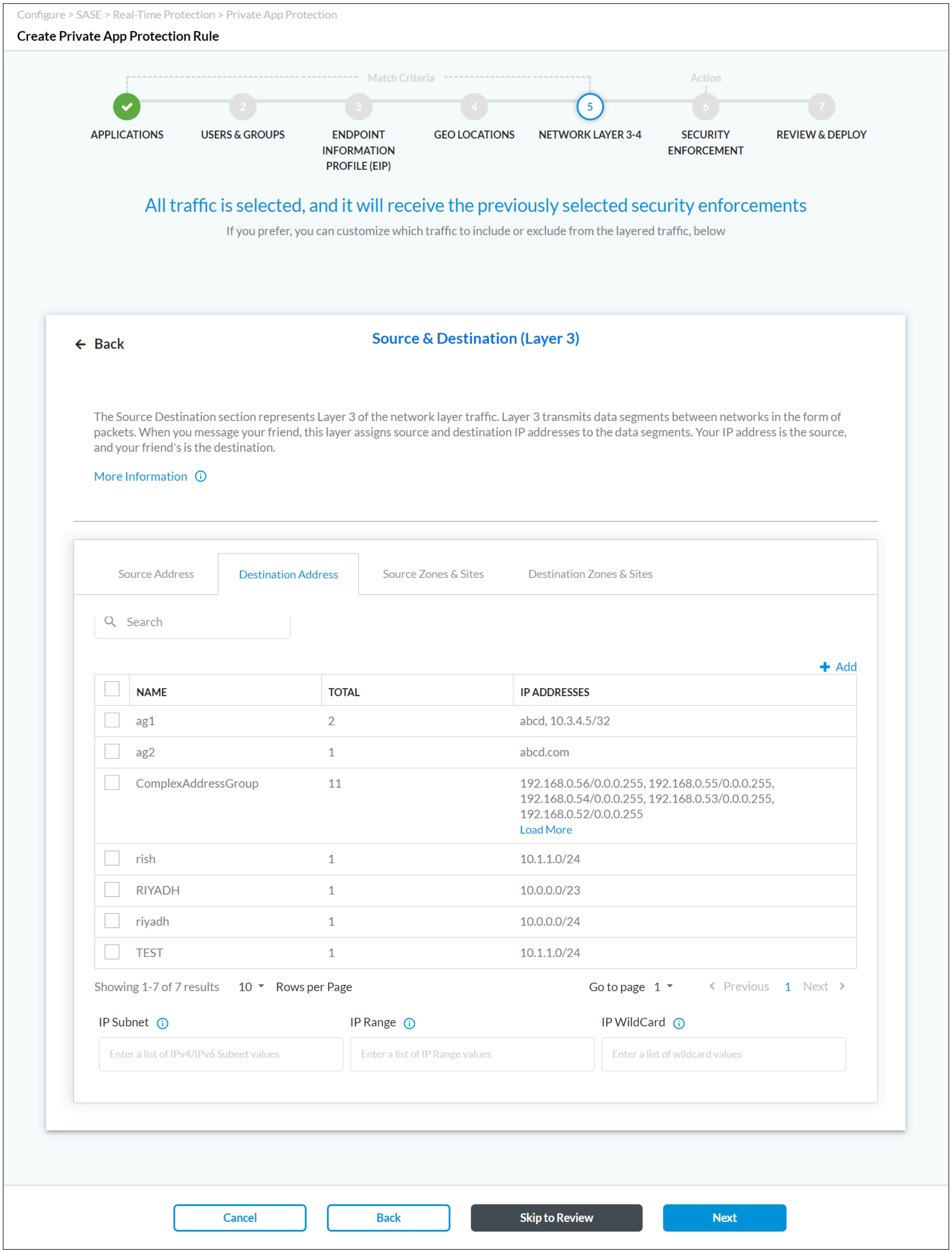
Field	Description
Negate Source Address	Select to apply the rule to any source addresses except the ones in the So
IP Subnet	Enter a list subnets to include in the match list, for example, 10.2.1.0/24. S

Field	Description
IP Range	Enter a list of IP addresses or ranges to include in the match list, for examp addresses or ranges with commas.
IP Wildcard	Enter a list IP addresses and masks to include in the match list, for examp addresses and masks with commas.

4. To create an address group, click the 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. To configure one or more specific source IP addresses, you do not need to create an address group. Instead, use the IP Wildcard field to enter the IP addresses.

Field	Description
Type	Select the type of IP address to match and the value to match. The name of the A on the value you select in the Type field. ◦ Dynamic Address ◦ FQDN ◦ IP Range ◦ IP Wildcard ◦ IPv6 Subnet ◦ Subnet
◦ Subnet	Enter one or more IP addresses and subnet masks, for example, 10.2.1.0/24. Sep
◦ IP Range	Enter one or more IP addresses within the IPv4 address range specified in the IPv 10.2.1.1–10.2.2.2. Separate the IP addresses or ranges with commas.
◦ IP Wildcard	Enter one or more wildcard masks for specific IP addresses, for example, 192.68.0 addresses or masks with commas.
◦ IPv6 Subnet	Enter one or more IP addresses and subnet masks within the IPv6 subnet range s the IP addresses and subnet masks with commas.
◦ FQDN	Enter one or more IP addresses returned in a DNS query that resolves the fully qu 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 ca

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



Create Private App 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

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 ⓘ

□	NAME	TOTAL	IP ADDRESSES
□	ag1	2	abcd, 10.3.4.5/32
□	ag2	1	abcd.com
□	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 Load More
□	rish	1	10.1.1.0/24
□	RIYADH	1	10.0.0.0/23
□	riyadh	1	10.0.0.0/24
□	TEST	1	10.1.1.0/24

Showing 1-7 of 7 results   10 ▾ Rows per Page   Go to page 1 ▾   ‹ Previous 1 Next ›

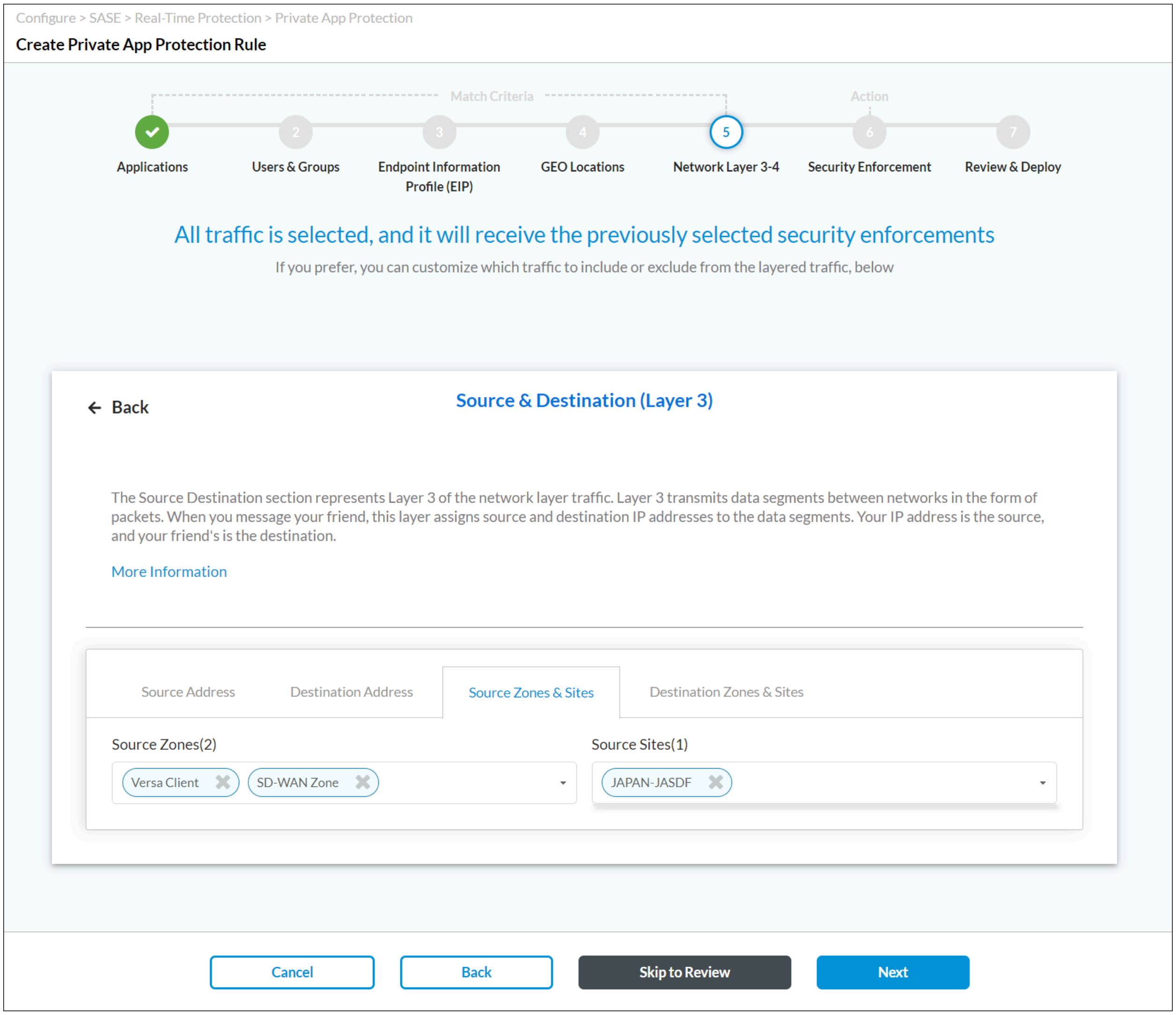
IP Subnet ⓘ: Enter a list of IPv4/IPv6 Subnet values

IP Range ⓘ: Enter a list of IP Range values

IP WildCard ⓘ: Enter a list of wildcard values

Field	Description
IP Range	Enter a list of IP addresses or ranges to include in the match list, for examp addresses or ranges with commas.
IP Subnet	Enter a list subnets to include in the match list, for example, 10.2.1.0/24. Se
IP Wildcard	Enter a list IP addresses and masks to include in the match list, for exampl addresses and masks with commas.
Negate Destination Address	Select to apply the rule to any destination addresses except the ones in the

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



Configure > SASE > Real-Time Protection > Private App Protection

Create Private App 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

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.

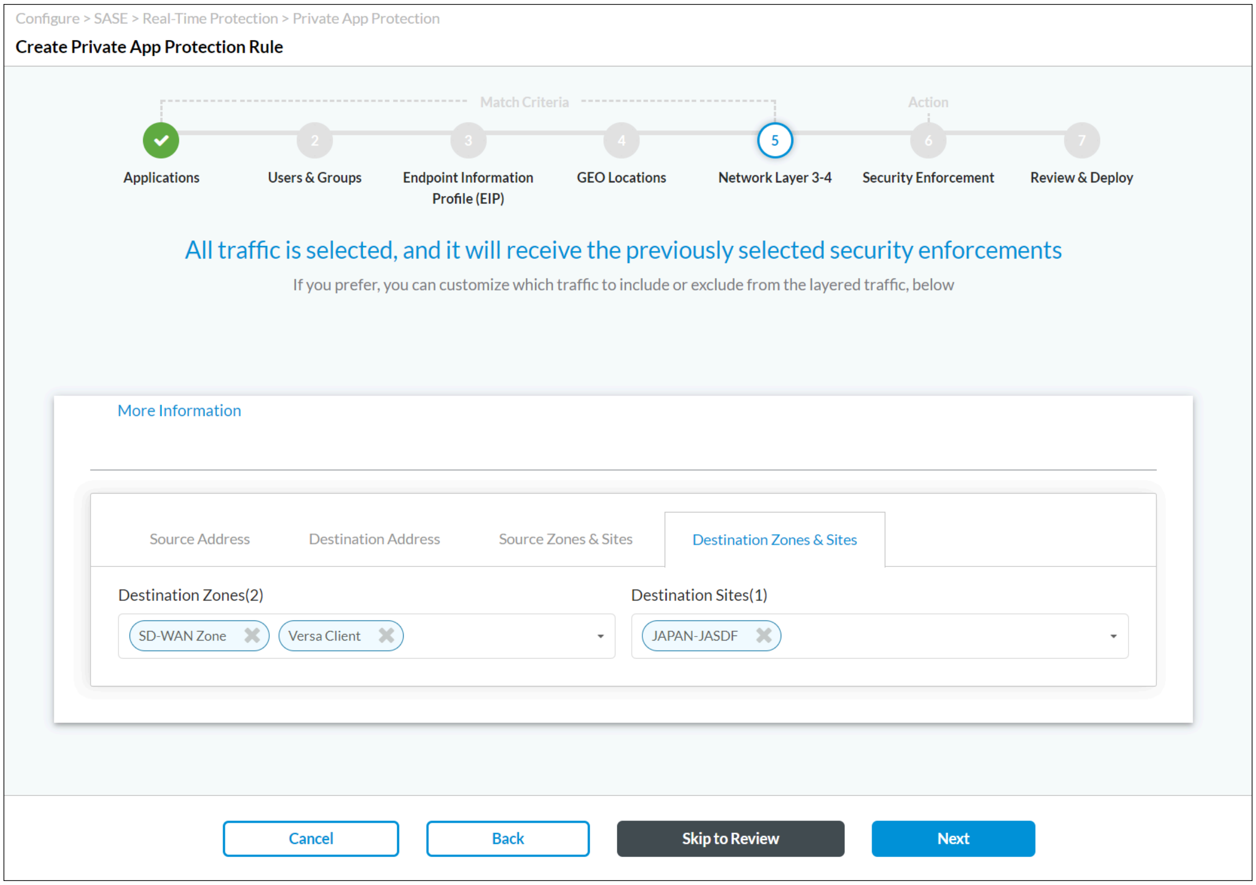
More Information

Source Zones(2): Versa Client, SD-WAN Zone

Source Sites(1): JAPAN-JASDF

Field	Description
Source Zone	Select one or more source zones to include in the match list. User-defined tunnels, also display in this list, and you can select them. By default, three ◦ Internet—Select if traffic comes from the internet. ◦ SD-WAN Zone—Select if traffic comes from an SD-WAN device. ◦ VSA Application—Select if traffic comes from a VSA client application.
Source Sites	Select one or more source sites to include in the match list.

11. Select the Destination Zones & Sites tab, and then enter information for the following fields.



Configure > SASE > Real-Time Protection > Private App Protection

Create Private App 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

Destination Zones(2): SD-WAN Zone, Versa Client

Destination Sites(1): JAPAN-JASDF

Field	Description
Destination Zone	Select one or more destination zones to include in the match list. User-defi tunnels, also display in this list, and you can select them. By default, three ◦ Internet—Select if traffic goes to the internet. ◦ SD-WAN Zone—Select if traffic goes to an SD-WAN device. ◦ VSA Application—Select if traffic goes to a VSA client application.
Destination Sites	Select one or more destination sites to include in the match list.

12. Click Back to return to the Network Layer 3-4 screen. On this screen, you configure network services and create policy schedules.

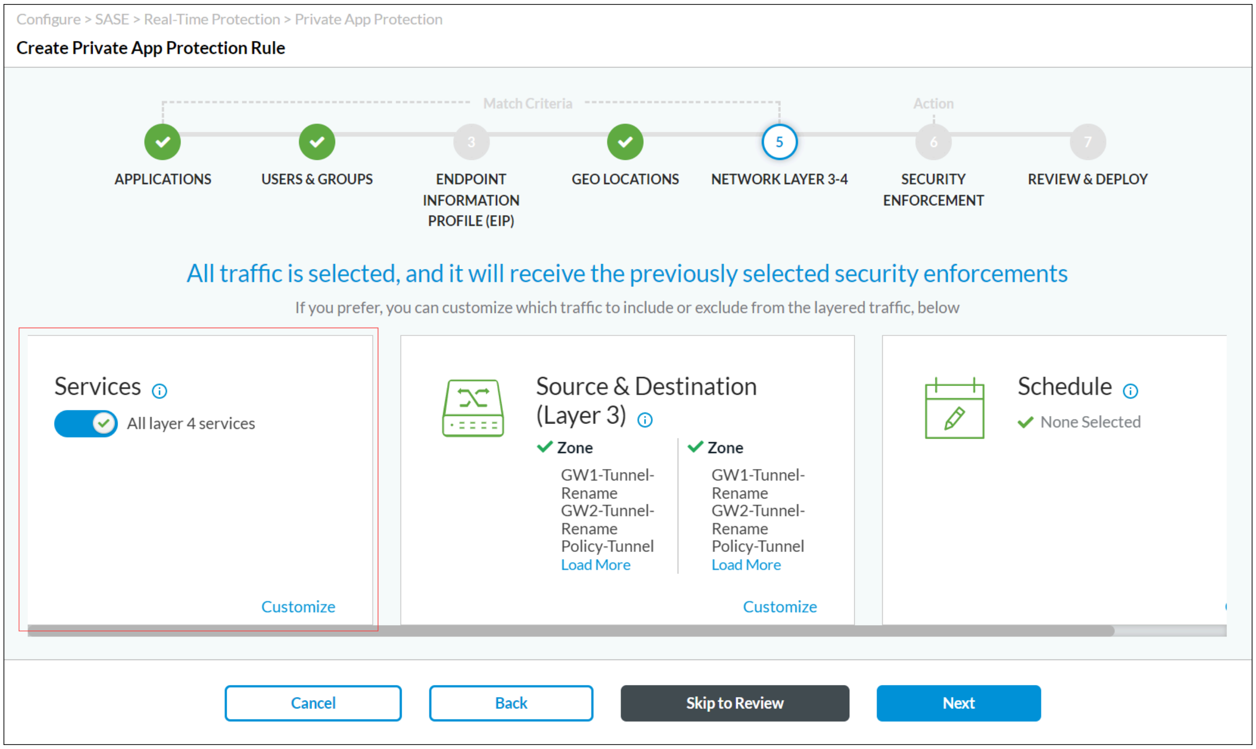
13. Click Next to continue to Step 6, Security Enforcement rules.

Configure SASE Network Services for Private Application Protection Rules

You can configure private application 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 traffic of all network service types. You can also configure the services to which security enforcement rules are applied.

To configure the network services to which security enforcement rules are applied:

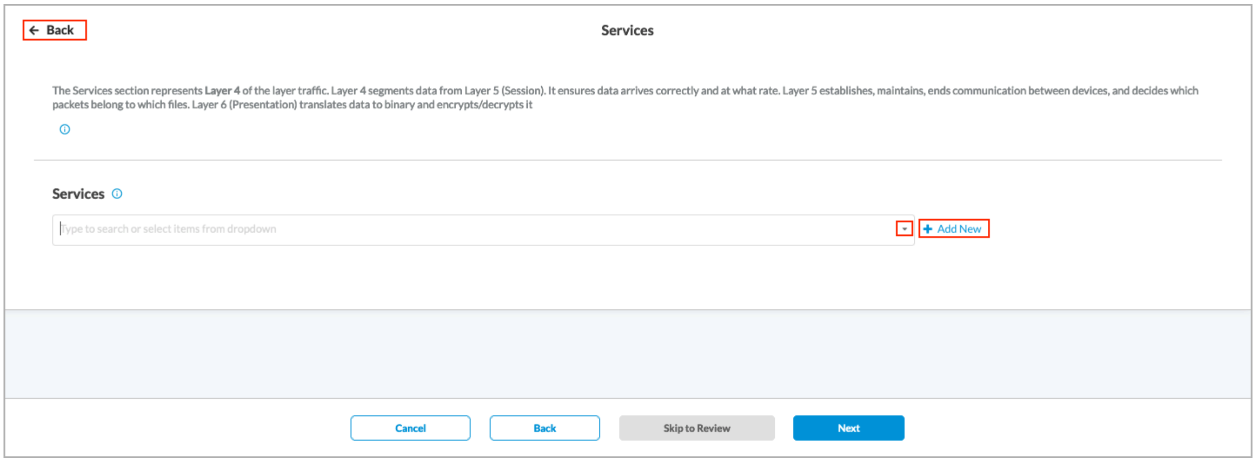
1. In Step 4, Network (Include or Exclude) Layer 3-4, click Customize in the Services box.


Configure > SASE > Real-Time Protection > Private App Protection
Create Private App Protection Rule
Match Criteria
Action
APPLICATIONS
USERS & GROUPS
3
ENDPOINT INFORMATION PROFILE (EIP)
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

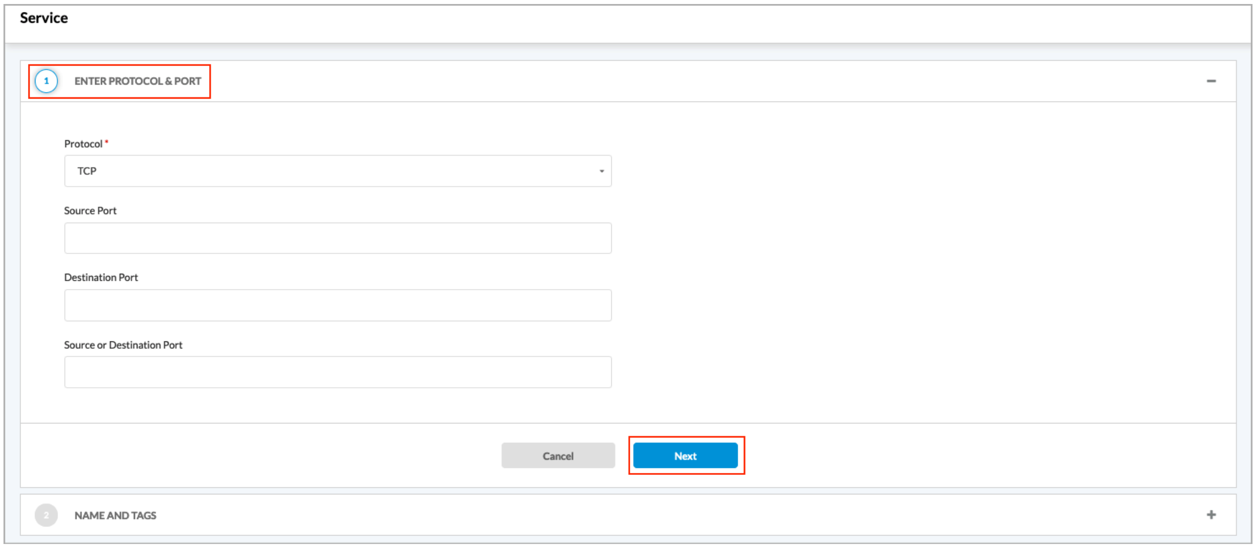
If you prefer, you can customize which traffic to include or exclude from the layered traffic, below

2. In the Services screen, select one or more custom or predefined 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

3. To add a custom service, click + Add New. The following screen displays.

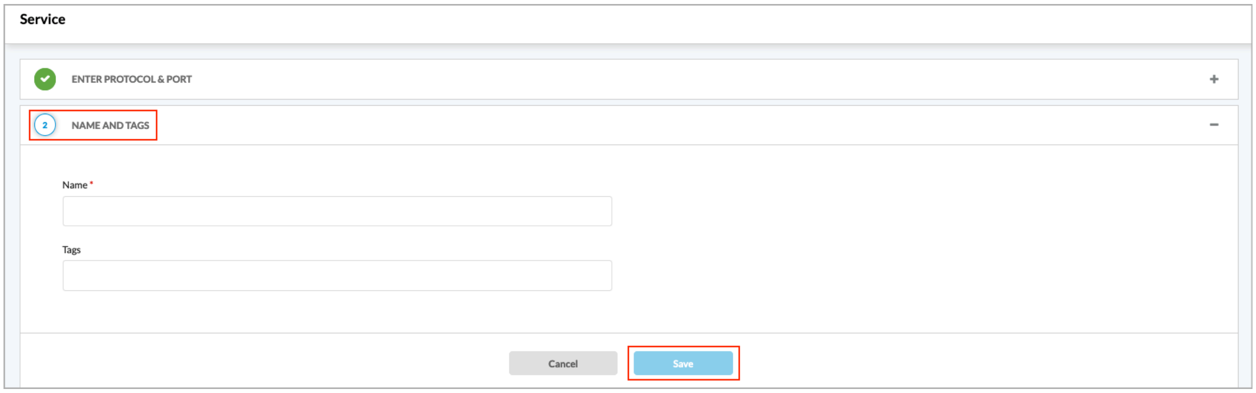


Protocol *: TCP

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	Enter the source port number. *Range*: 0 through 65535 *Default*: None
Destination Port	Enter the destination port number. *Range*: 0 through 65535 *Default*: None
Source or Destination Port	Enter the source or destination port number. *Range*: 0 through 65535 *Default*: None

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



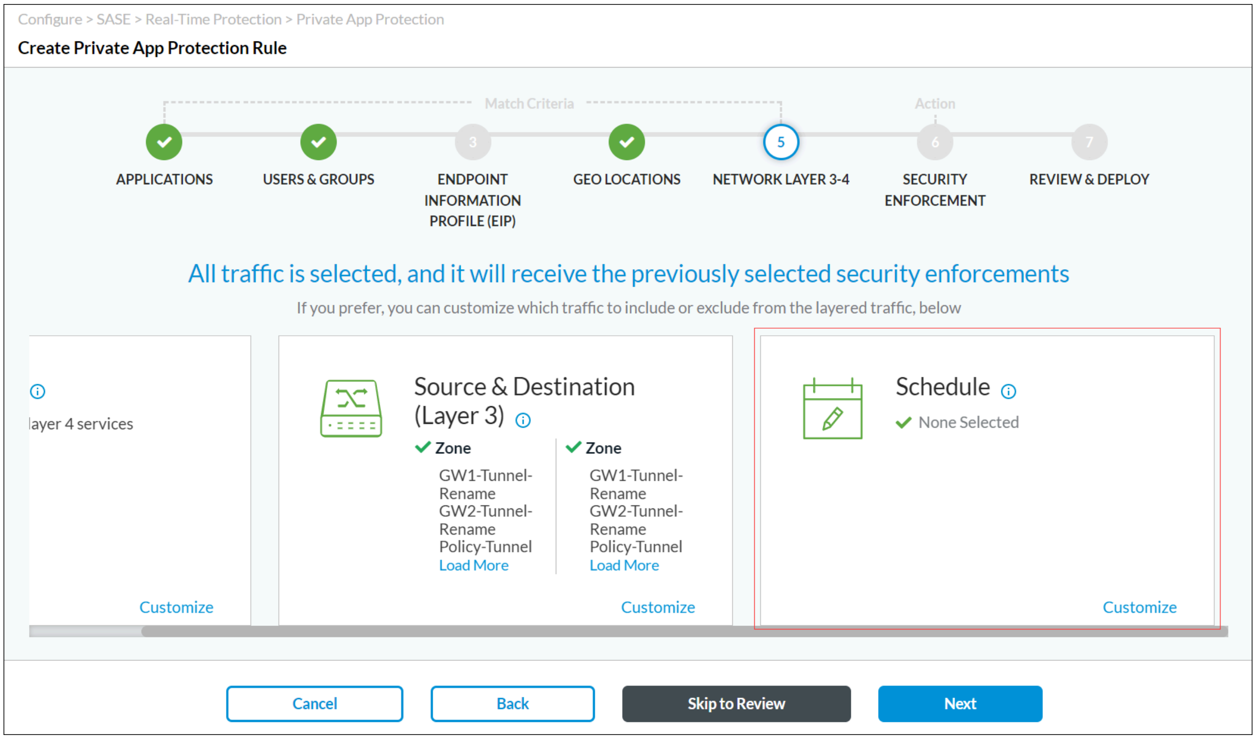
6. In the Name field, enter a name for the service.
7. In the Tags field, enter optional tags.
8. Click Save to add the new service to the protocol list. You can then select the new service.

Configure Schedules for SASE Private Application 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 private application 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 private application protection rules to filter traffic:

1. In Step 4, Network (Include or Exclude) Layer 3-4, click Customize in the Schedule box.



Configure > SASE > Real-Time Protection > Private App Protection

Create Private App 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

layer 4 services

Customize

Source & Destination (Layer 3)

✓ Zone
GW1-Tunnel-Rename
GW2-Tunnel-Rename
Policy-Tunnel
Load More

✓ Zone
GW1-Tunnel-Rename
GW2-Tunnel-Rename
Policy-Tunnel
Load More

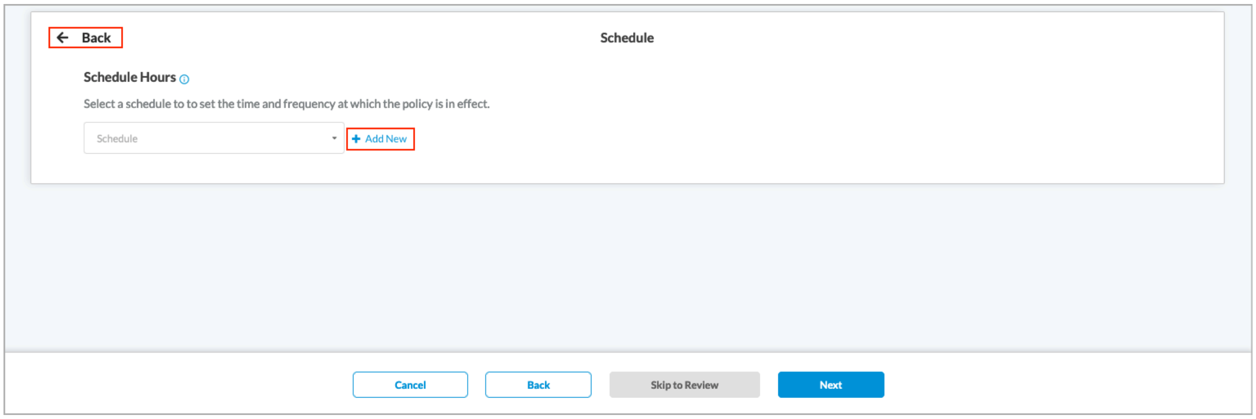
Customize

Schedule

✓ None Selected

Customize

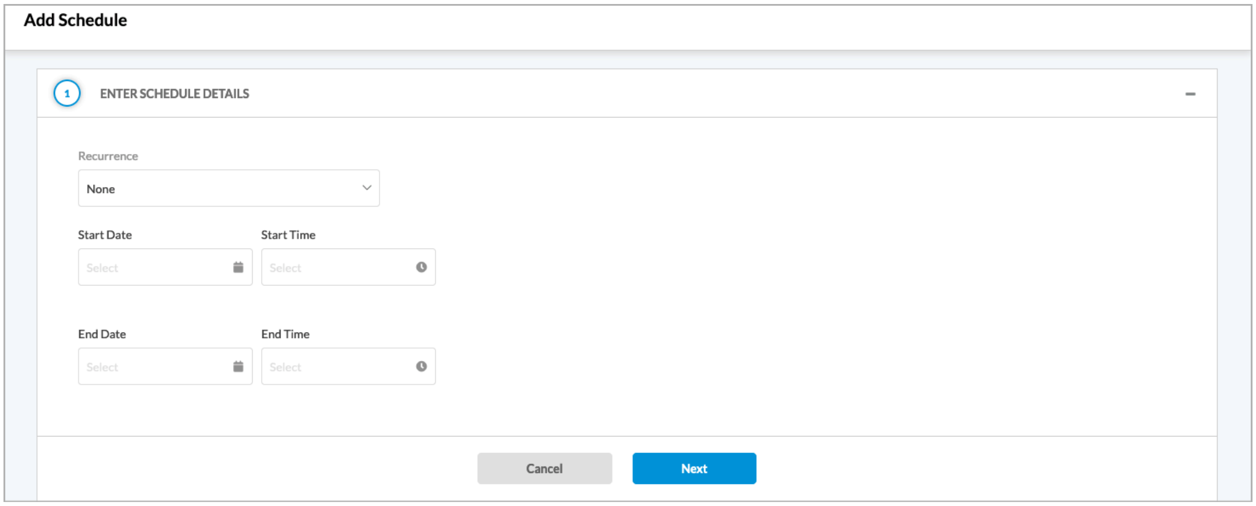
2. In Schedule Hours, select a schedule.



Schedule Hours

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

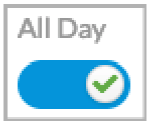
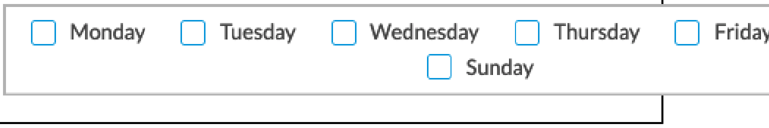
3. If no schedules exist or if you want to create a schedule, click + Add New to create a schedule to set the time and frequency at which the rule is in effect. In Enter Schedule Details, enter information for the following fields.



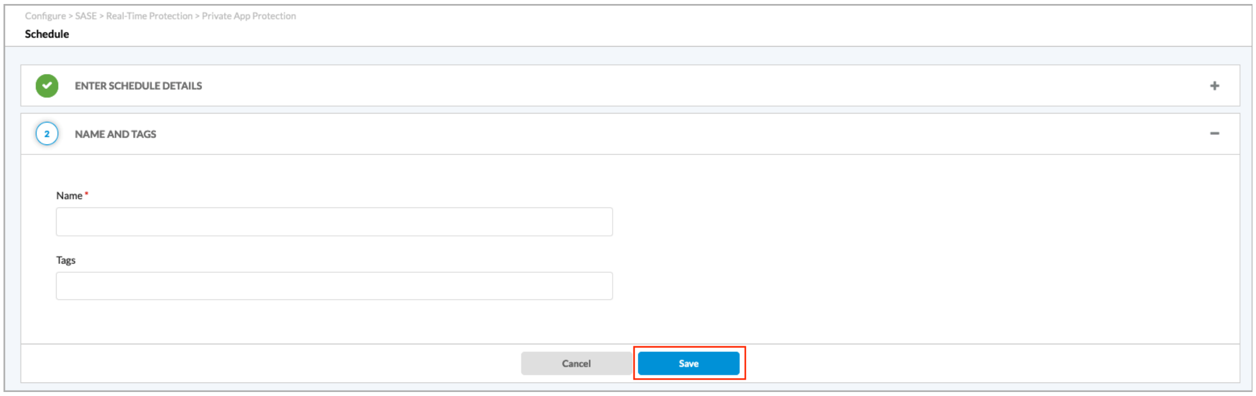
Add Schedule

1 ENTER SCHEDULE DETAILS

Recurrence: None

Field	Description
Recurrence	Select how often the policy is in effect: ◦ Daily ◦ None ◦ Weekly
All Day	If you select Daily or Weekly, click the slider to have the policy be in effect all day. 
Start Time	If you do not select All Day, enter the start time for the policy.
End Time	If you do not select All Day, enter the stop time for the policy.
Days of the Week	If you select Weekly, select the days of the week for the policy to be in effect.  □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Sunday

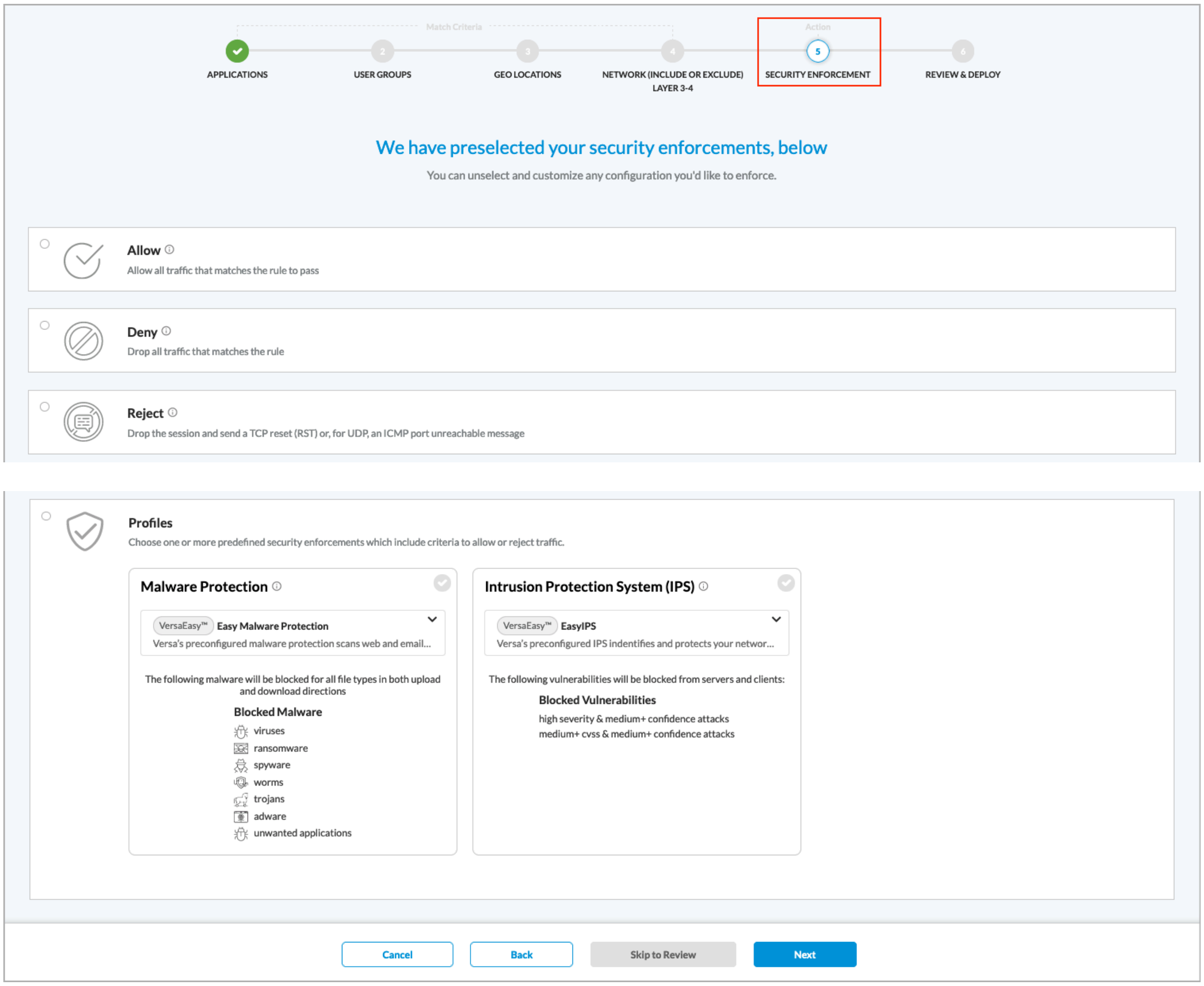
4. Click Next. The Name and Tags screen displays.



5. Enter a name for the schedule, and enter any tags.
6. Click Save.

Configure Security Enforcement Actions for SASE Private Application Protection Rules

You configure 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 to apply to matching traffic. The following screen shows the available security enforcement actions.



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.

Malware Protection ⓘ
VersaEasy™ **Easy Malware Protection**
Versa's preconfigured malware protection scans web and email...

The following malware will be blocked for all file types in both upload and download directions

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

Intrusion Protection System (IPS) ⓘ
VersaEasy™ **EasyIPS**
Versa's preconfigured IPS indentifies and protects your networ...

The following vulnerabilities will be blocked from servers and clients:

Blocked Vulnerabilities
high severity & medium+ confidence attacks
medium+ cvss & medium+ confidence attacks

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

You can select the following security enforcement actions:

- 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.

You can choose a predefined security enforcement profile 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:

- Intrusion protection system (IPS)—For more information, see Configure an IPS Profile for Private Application Protection Rules.
- Malware protection—For more information, see Configure a Malware Protection SASE Profile for Private Application Protection Rules.

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

Note: The malware protection and IPS profiles display only if the tenant to which you want to apply the profile is subscribed to the SWG and VSA professional services.

Configure a Malware Protection Profile for SASE Private Application Protection Rules

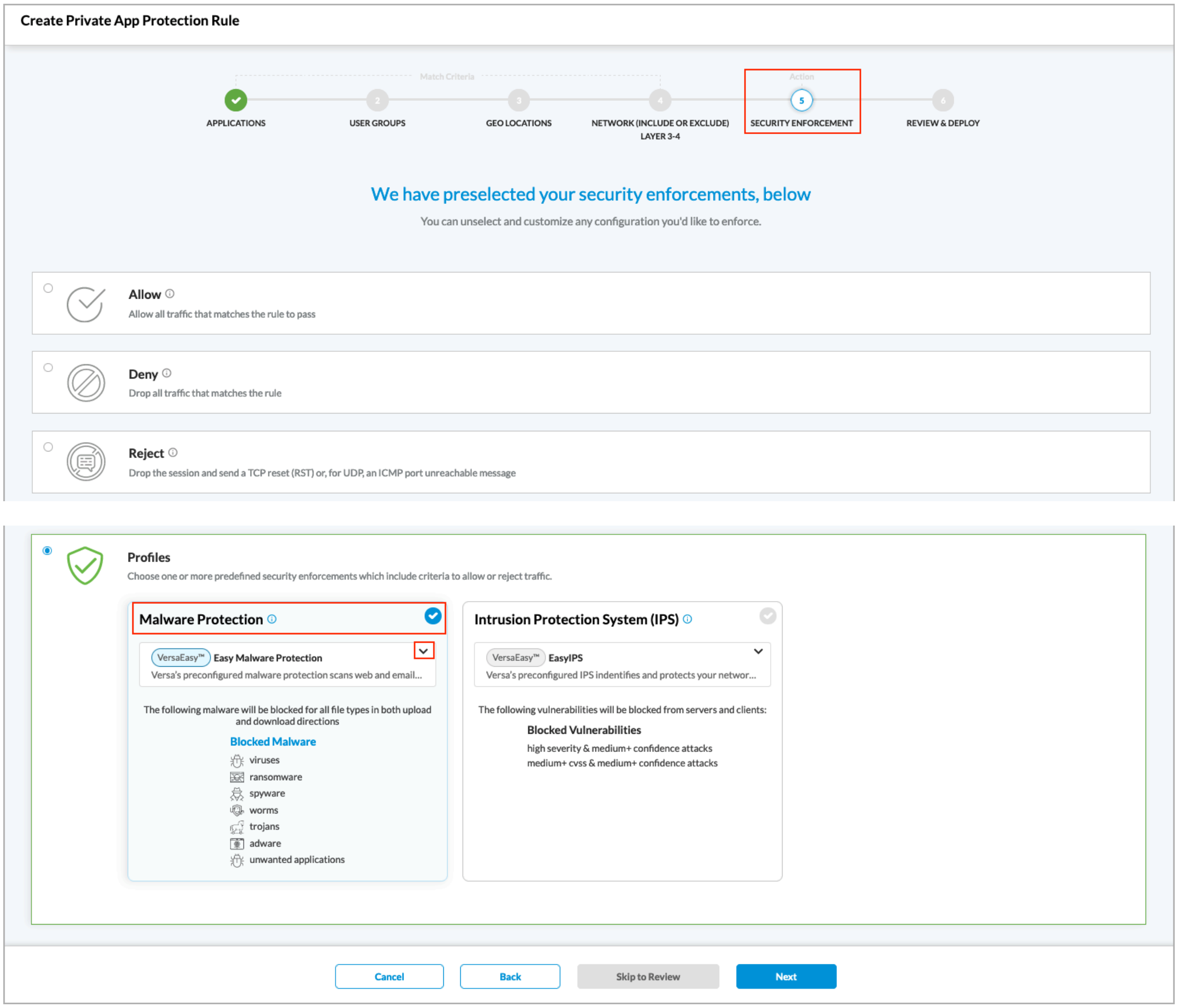
Malware is malicious software that is specifically designed to disrupt computers and computer systems. There are many types of malware, including computer viruses, worms, Trojan viruses, spyware, adware, and ransomware. Among the things malware can do is leak private information, gain unauthorized access to information or systems, and deprive users of 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 profiles display only if the tenant to which you want to apply the profile is subscribed to the SWG and VSA professional services.

To customer a malware protection profile in a private application protection rule:

1. In the Create Private Application Protection Rule screen, select Step 5, Security Enforcement.



Create Private App Protection Rule

Match Criteria

Action

APPLICATIONS — 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

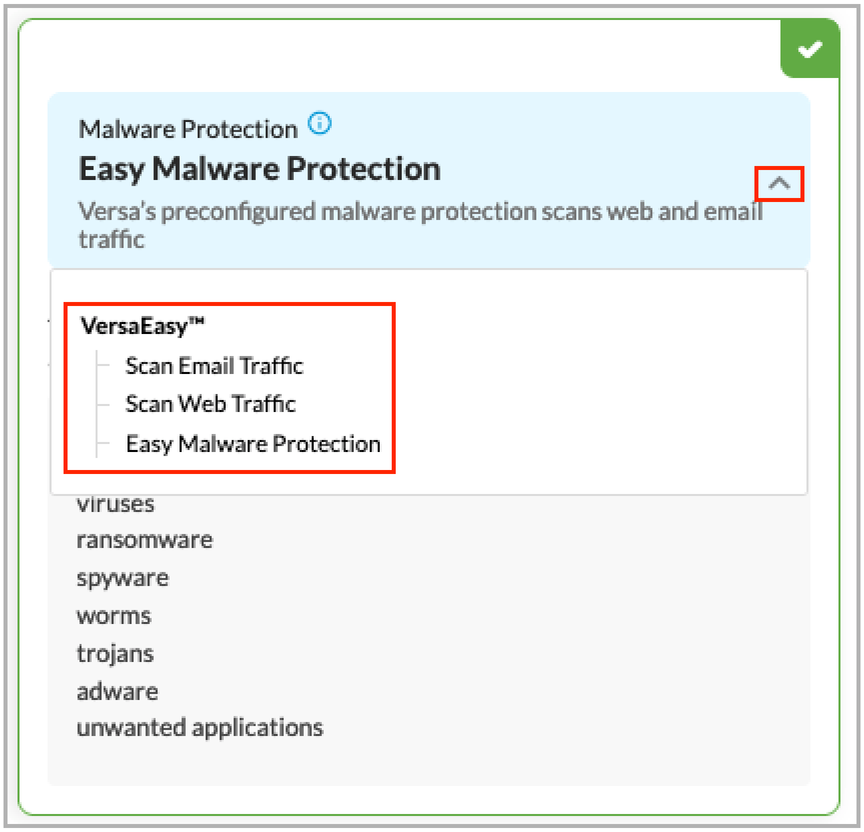
○ Reject ⓘ
Drop the session and send a TCP reset (RST) or, for UDP, an ICMP port unreachable message

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

Malware Protection ⓘ ✓
VersaEasy™ Easy Malware Protection
Versa's preconfigured malware protection scans web and email...
The following malware will be blocked for all file types in both upload and download directions
Blocked Malware
- viruses
- ransomware
- spyware
- worms
- trojans
- adware
- unwanted applications

Intrusion Protection System (IPS) ⓘ
VersaEasy™ EasyIPS
Versa's preconfigured IPS indentifies and protects your networ...
The following vulnerabilities will be blocked from servers and clients:
Blocked Vulnerabilities
high severity & medium+ confidence attacks
medium+ cvss & medium+ confidence attacks

2. To enable the preselected Easy Malware Protection security enforcement policies, click the Malware Protection box. By default, this profile blocks the following types of malware:
    - Adware
    - Ransomware
    - Spyware
    - Trojans
    - Unwanted applications
    - Viruses
    - Worms
3. Click the down arrow to display other options.



Malware Protection

Easy Malware Protection

Versa's preconfigured malware protection scans web and email traffic

viruses

ransomware

spyware

worms

trojans

adware

unwanted applications

4. To send email alerts about the following malware in both the upload and download directions, select Scan Email Traffic:
   - IMAP
   - MAPI
   - POP3
   - SMTP
5. To deny the following malware in both the upload and download directions, select Scan Web Traffic:
   - FTP
   - HTTP
6. To restore the default Easy Malware Protection settings, select Easy Malware Protection.
7. Select another profile to customize, or click Next to go to the Step 6, Review and Deploy screen.

Configure an IPS Profile for SASE Private Application Protection Rules

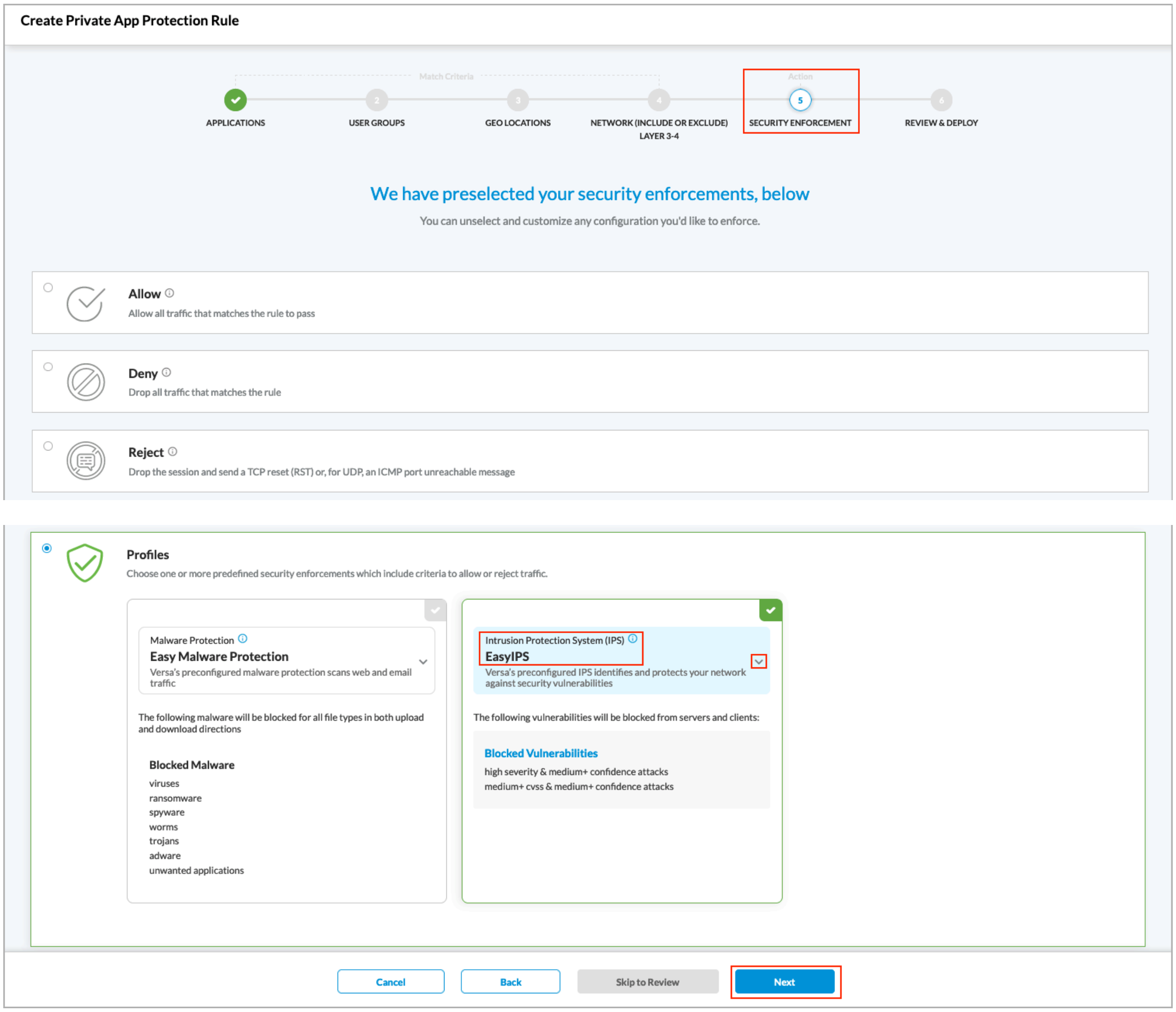
The intrusion protection system (IPS) mitigates security vulnerabilities by responding to inappropriate or anomalous activity. Responses can include dropping data packets and disconnecting connections that are transmitting unauthorized data.

By default, Versa SASE provides a predefined IPS enforcement policy. You can also 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 in a private application protection rule:

1. Select Step 5, Security Enforcement screen in the Create Private Application Protection Rule screen.



Create Private App Protection Rule

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.

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

The following malware will be blocked for all file types in both upload and download directions

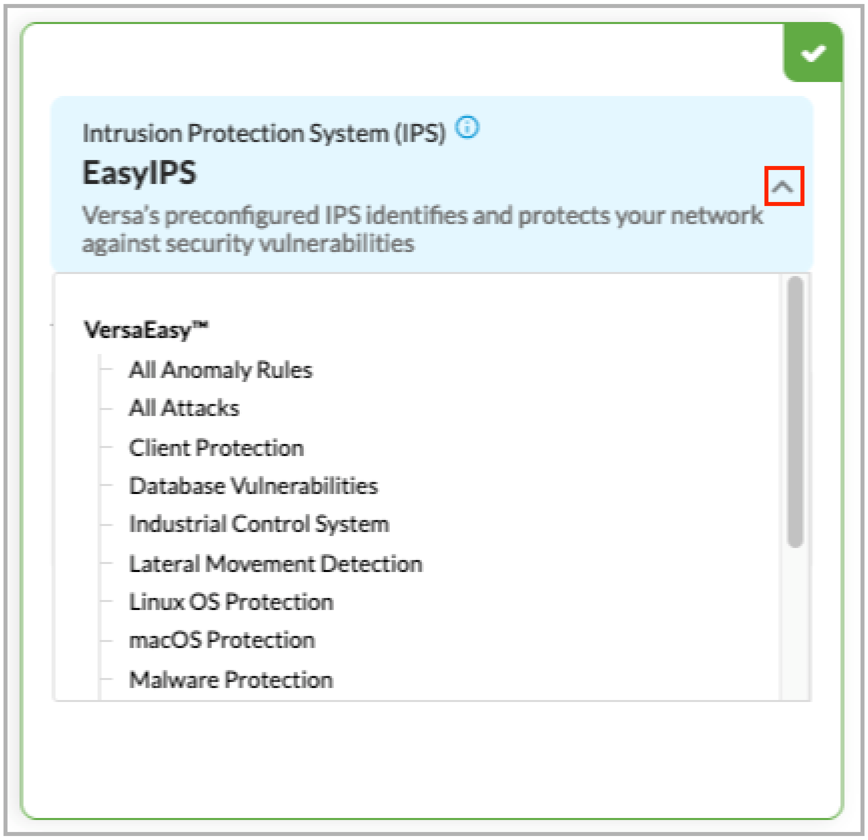
Blocked Malware
viruses
ransomware
spyware
worms
trojans
adware
unwanted applications

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

The following vulnerabilities will be blocked from servers and clients:

Blocked Vulnerabilities
high severity & medium+ confidence attacks
medium+ cvss & medium+ confidence attacks

2. To enable the preselected EasyIPS security enforcement policies, click the Intrusion Protection System (IPS) box s. By default, the following vulnerabilities are blocked from all servers and clients:
   - High-severity and medium+ confidence attacks
   - Medium+ CVSS (common vulnerability scoring system) and medium+ confidence attacks
3. To change the default settings, click the down arrow.



Intrusion Protection System (IPS)

EasyIPS

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

VersaEasy™

- All Anomaly Rules
- All Attacks
- Client Protection
- Database Vulnerabilities
- Industrial Control System
- Lateral Movement Detection
- Linux OS Protection
- macOS Protection
- Malware Protection

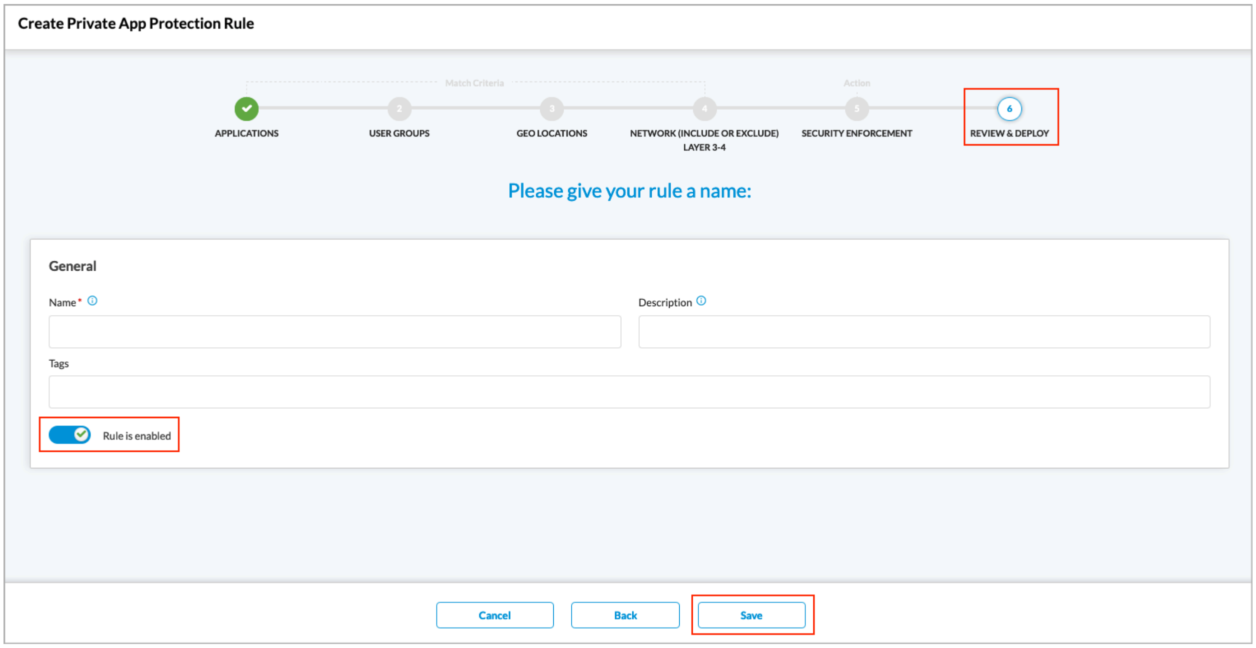
4. To enable a filter, select one of the IPS filters.
5. To restore the default IPS filtering settings, select EasyIPS.
6. Click Next to go to the Step 6, Review and Deploy screen.

Review and Deploy Private Application Protection Rules

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

To review and deploy a private application protection rule:

1. Select Step 6, Review and Deploy in the Create Private Application Protection Rule screen, 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 any alphanumeric characters, underscores, and hyphens.
Description	Enter a description for the rule.
Tags	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 enter multiple tags.
Rule is Enabled	Click the slide bar to enable the rule: Click the slide bar again to disable the rule:

2. Click Save to deploy the private application 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 Private Application Protection Rules.
- Release 12.1.1 allows you to clone Private Application Protection Rules.

Additional Information

Configure SASE Internet Protection Rules
Configure SASE Secure Client Access Rules