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.

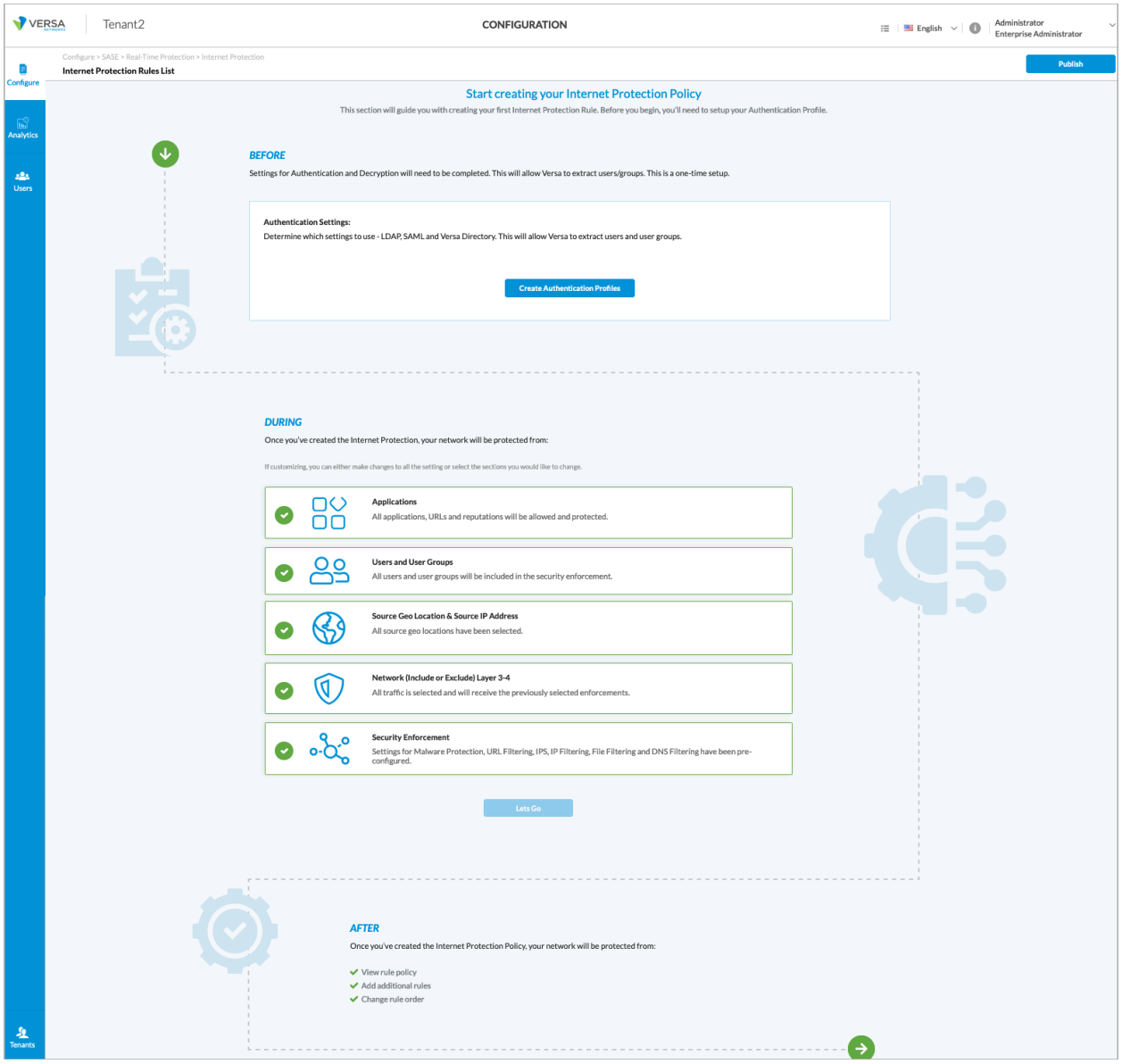
- Applications—Match criteria based on individual applications, groups of applications, categories of applications, predefined URL categories (such as business and economy, computer and internet security, and entertainment and arts), and predefined reputations (such as high and low risk).
- User and 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.

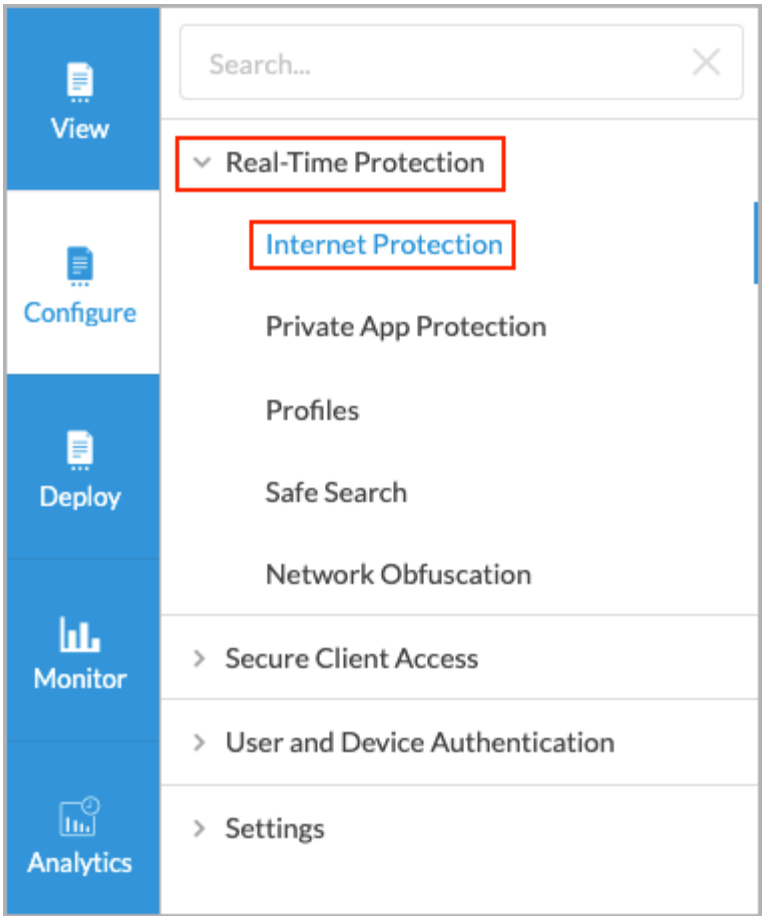
When you begin to configure your first internet protection policy, the following screen displays to guide you through the procedure:



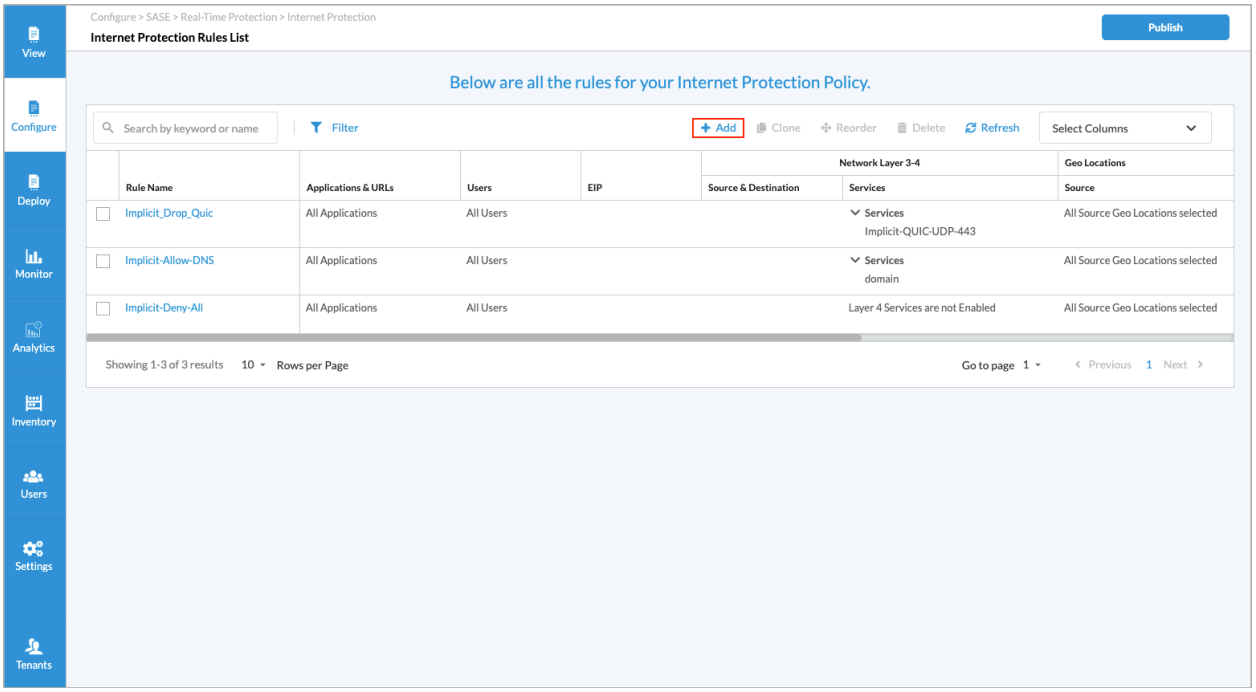
Configure SASE Internet Protection Rule Match Criteria

To configure internet protection rule match criteria:

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

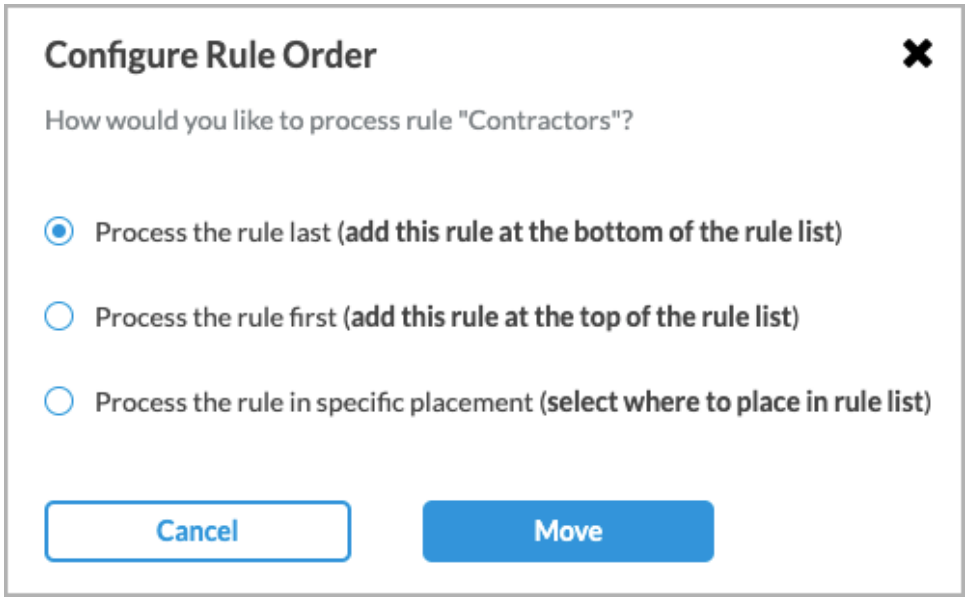
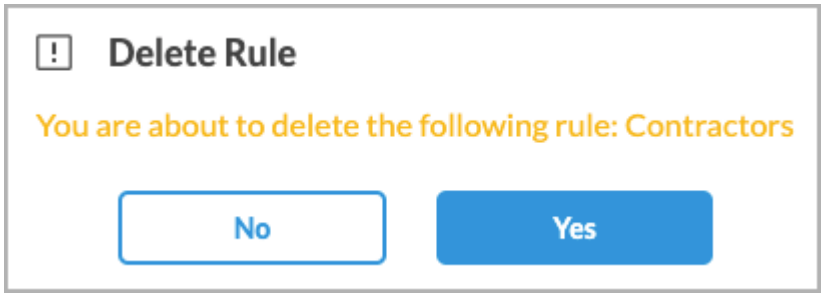


The Internet Protection Rules List screen displays all configured internet protection rules.



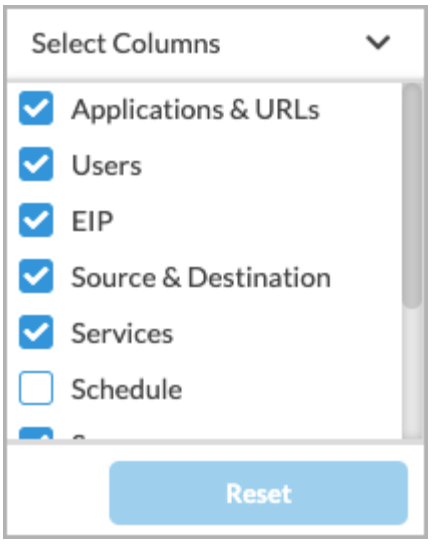
2. In the horizontal menu bar, you can select one of the following operations.

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

Operation	Description
	 1. Select the rule order: ◦ Process the rule last. ◦ Process the rule first. ◦ Process the rule in specific placement—A list of the existing rules displays. Click place the rule. 2. Click Move.
Delete	Delete the selected internet protection rule. A popup window similar to the following d  Click Yes to delete the internet protection rule, or click No to retain the rule.
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 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.

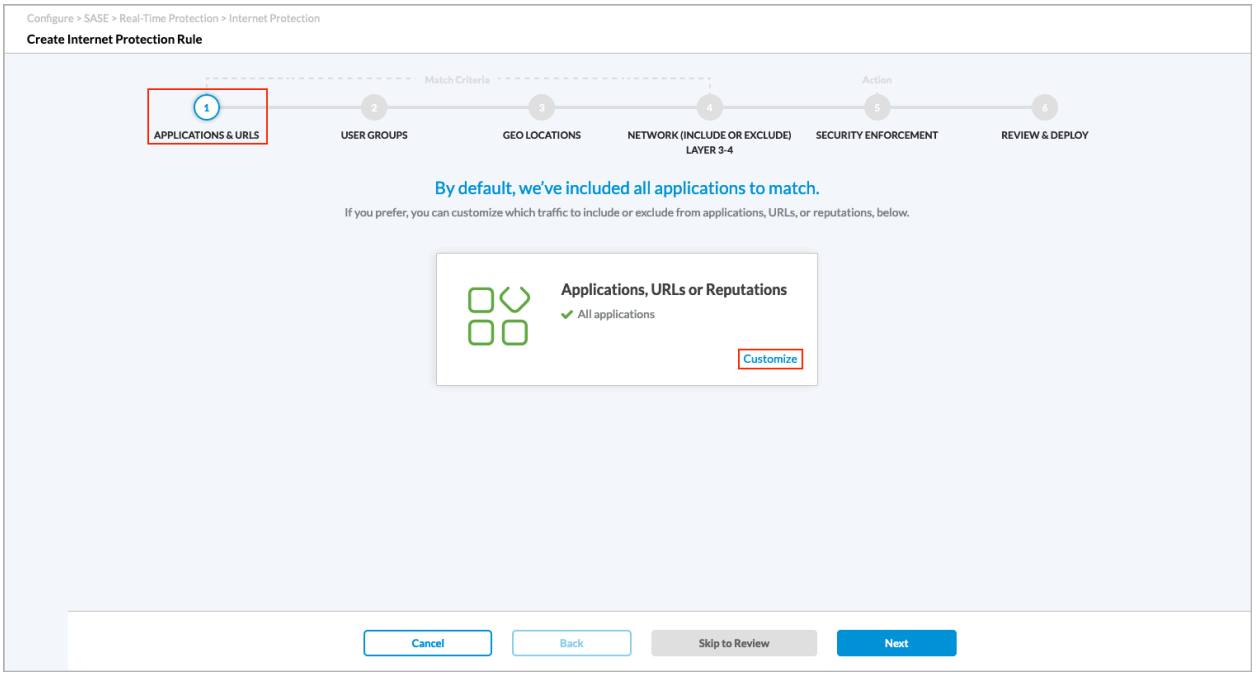
Configure SASE Application and URL Filtering for Internet Protection Rules

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.

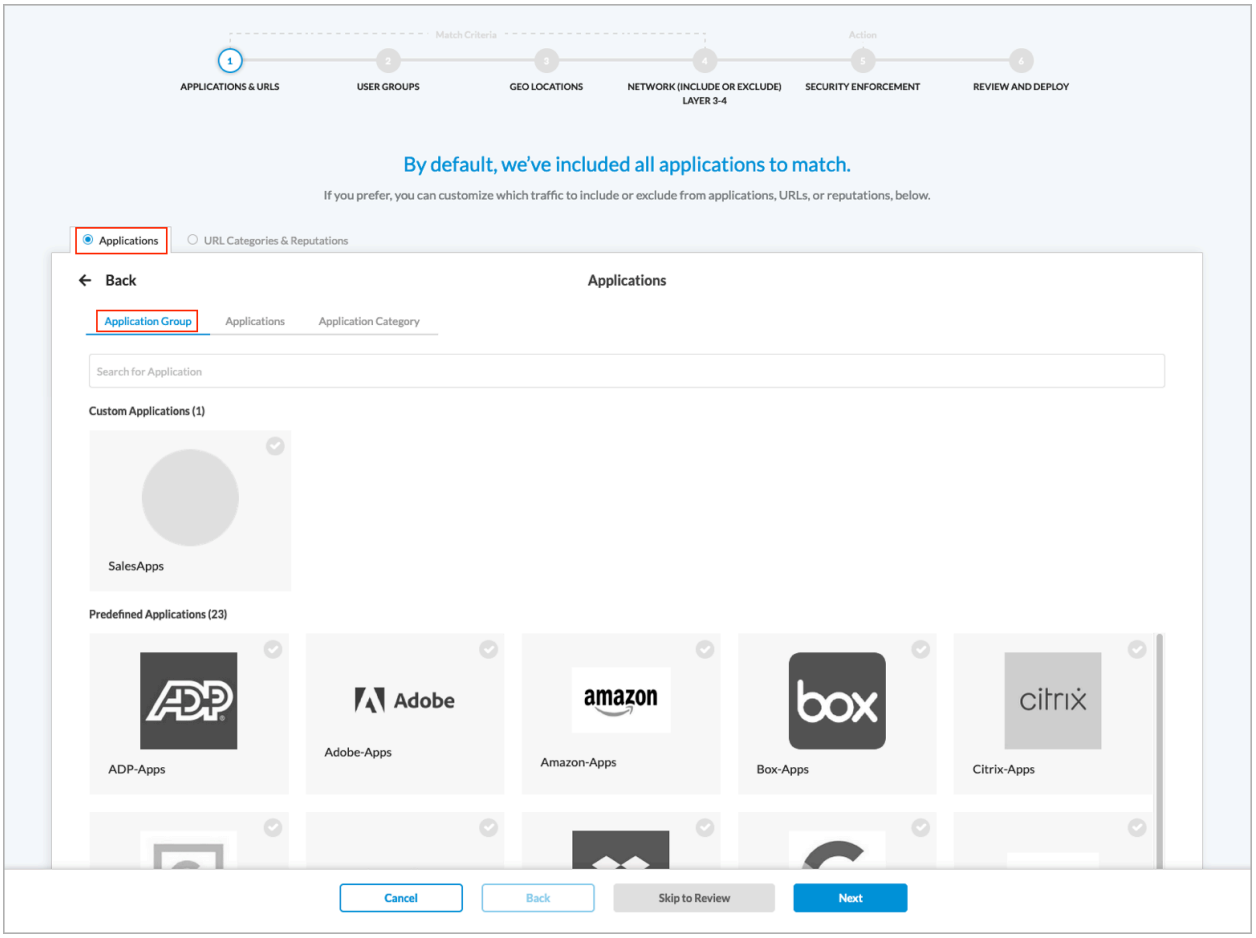
Application identification provides an effective detection capability for evasive applications such as Facebook, Skype, Torrent, and WhatsApp. It identifies applications and protocols at different network layers based on the protocol bundle rather than using the IP address and port number. You can create 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:

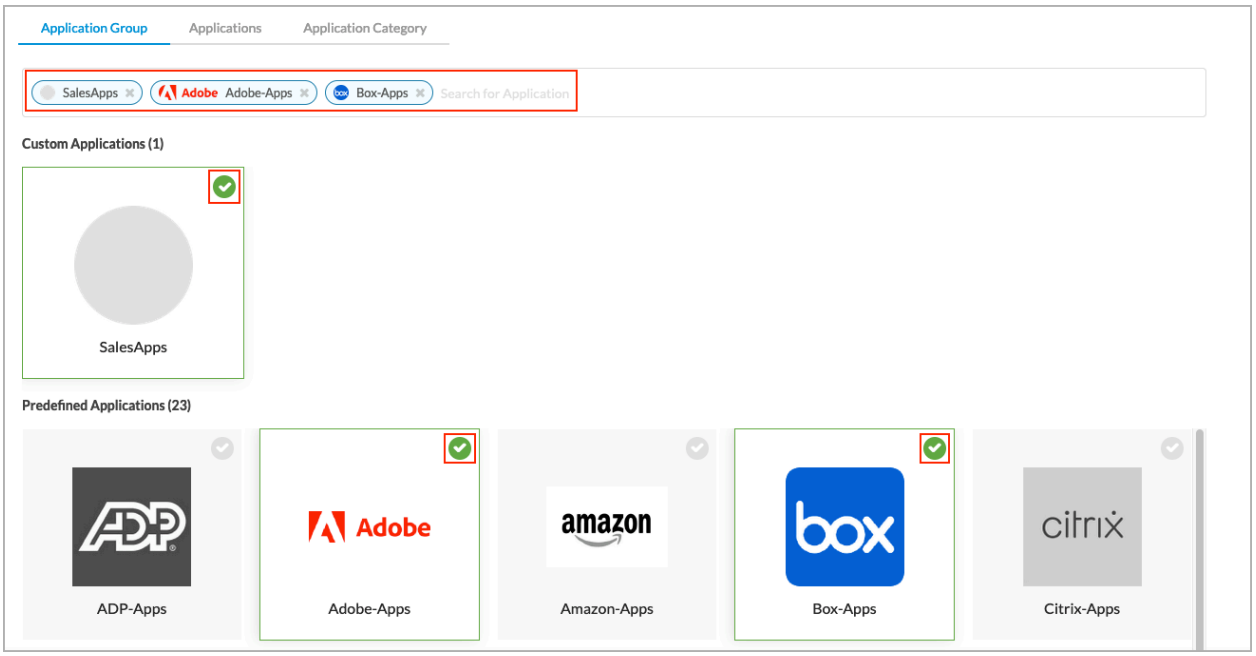
1. In the Internet Protection Rules List screen, click + Add to create a rule. The Create Internet Protection Rule screen displays.



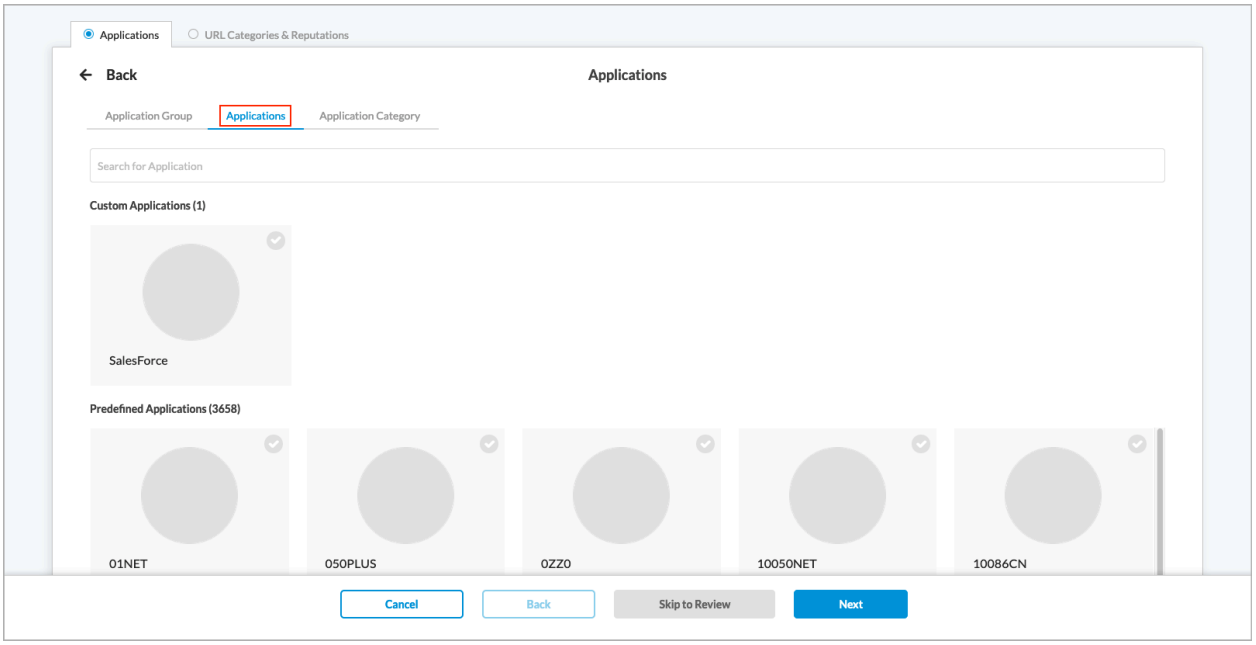
2. Select Step 1, Application and URLs. By default, all applications, URLs, and reputations are included in the match, which means that all applications, URLs, and reputations are matched by this rule.
3. To accept the default settings, click Next to continue to Step 2, User Groups.
4. To include only 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.



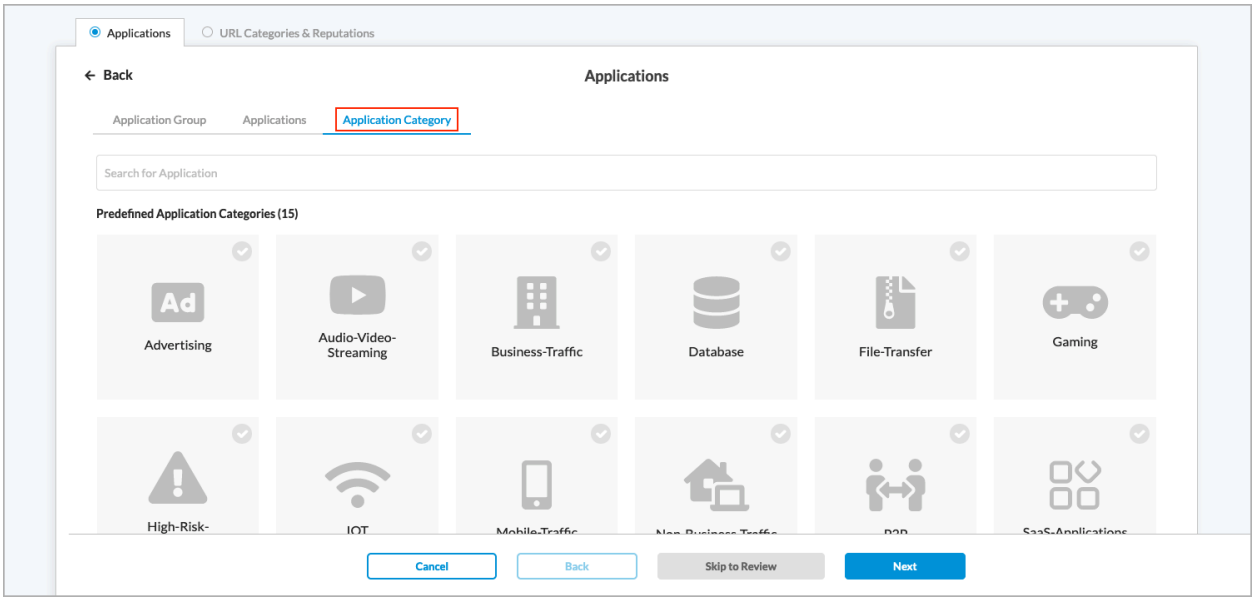
5. To create an internet protection rule based on applications, select the custom and predefined application groups to include in the match list, or type the name of the application group in the search box and select it from the search results. In the following example, the custom application group SalesApps 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.



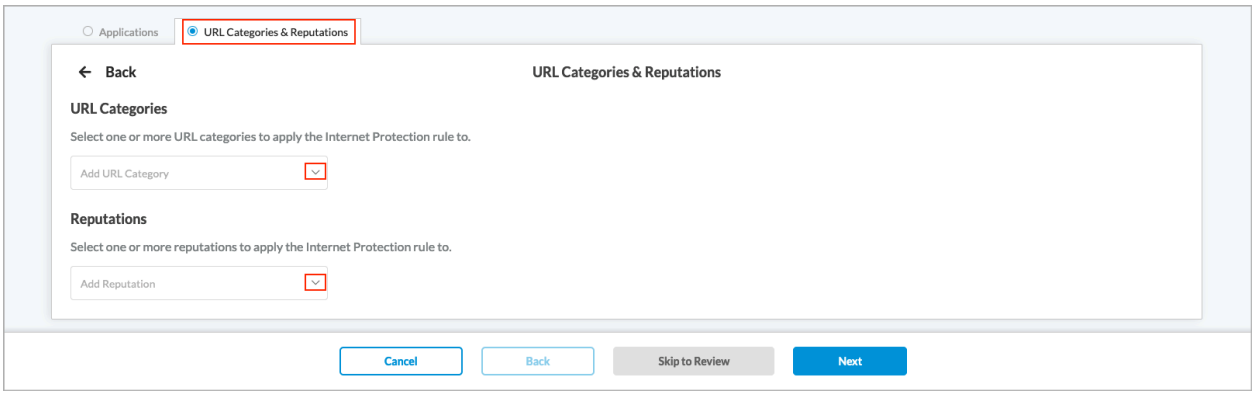
6. Click the Applications tab in the submenu. The following screen displays.



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.



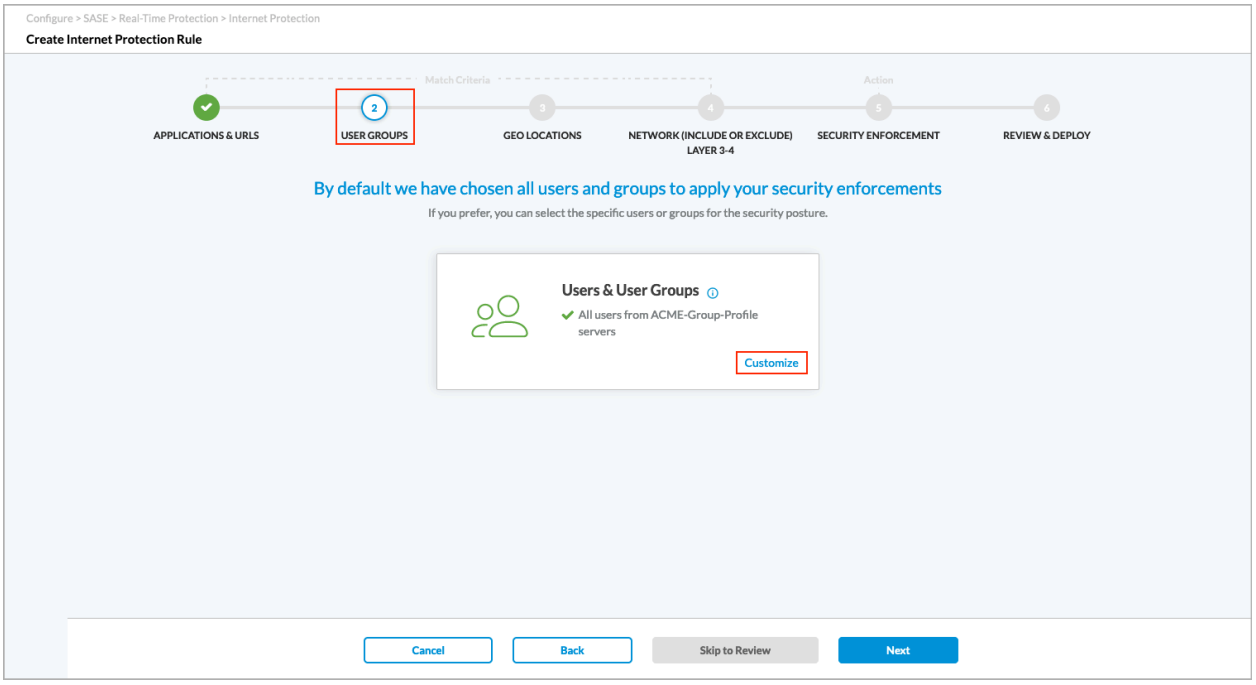
11. In the Add URL Category and Add Reputation fields, select one or more URL categories and reputations to include in the internet protection rule.
12. Click Next to configure User Groups match criteria, or click Back to return to the Create Internet Protection Rule screen and then click Next to configure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

Configure SASE User and User Group Filtering for Internet Protection Rules

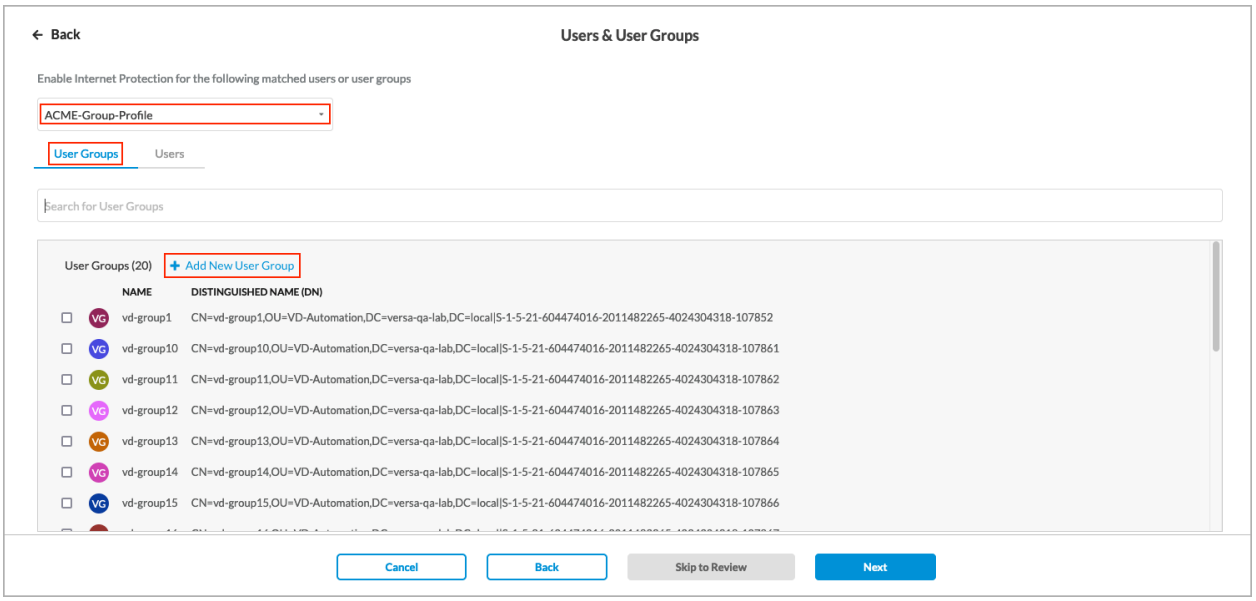
You create user and user group security rules to detect the users and user groups who are using applications on your network. These rules can help to identify users who may have transferred files or transmitted threats. User and user group rules identify users based on their name or role rather than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

To configure user and user group rules match criteria:

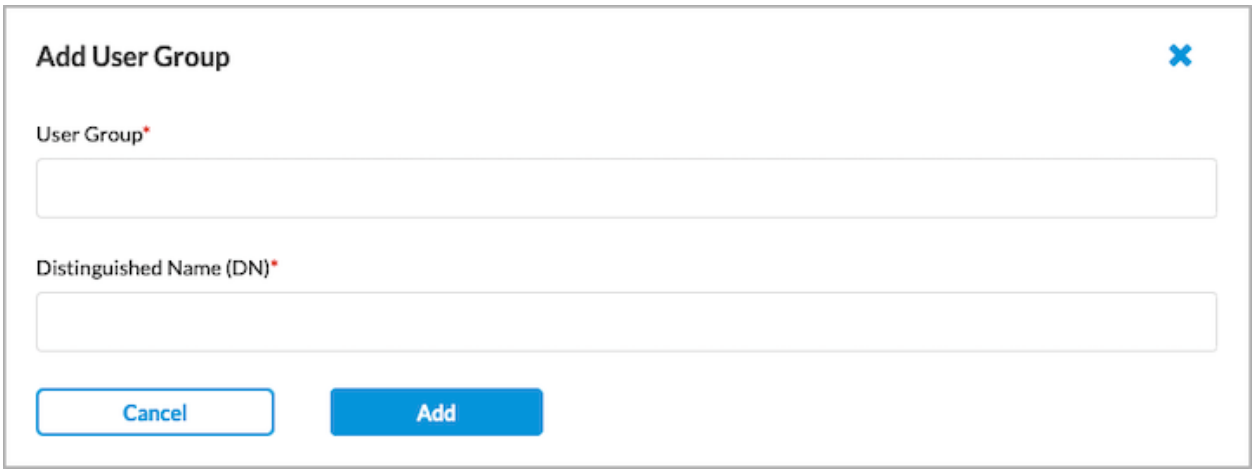
1. In the Create Internet Protection Rule screen, select Step 2, User Groups. By default, all users and user groups are included in the match, which means that no filtering is done on the basis of users and user groups.



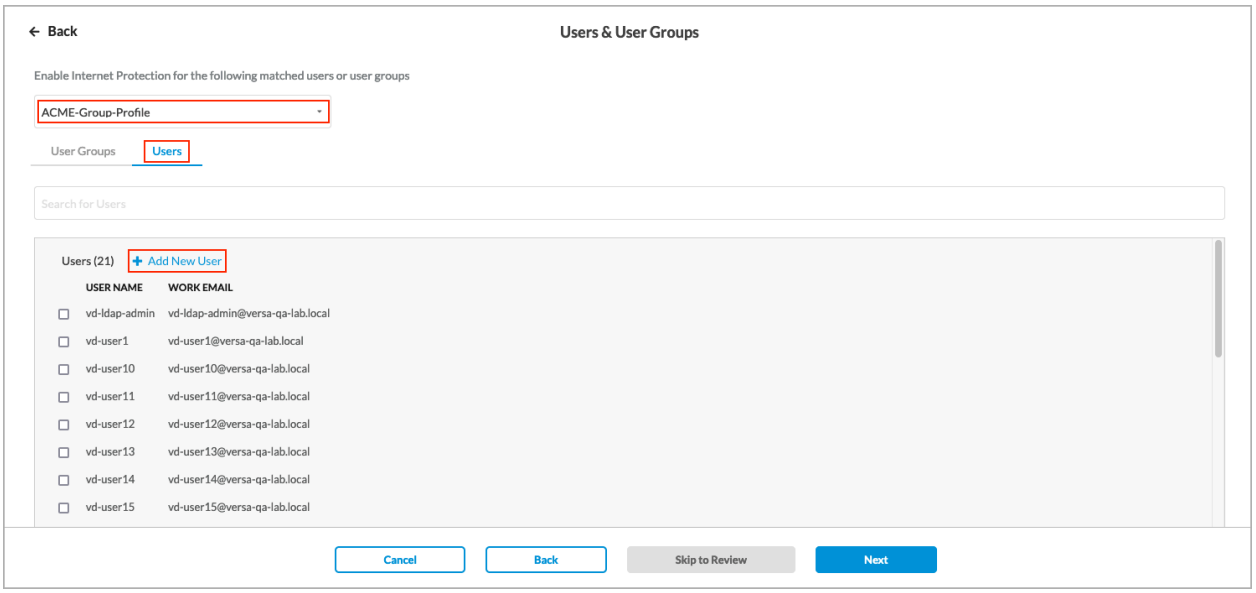
2. To accept the default, click Next to continue to Step 3, Geolocation match criteria.
3. To change the users and user groups to include in the match list, click Customize. The following screen displays, and the User Groups tab selected by default. The screen displays all user groups.



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.

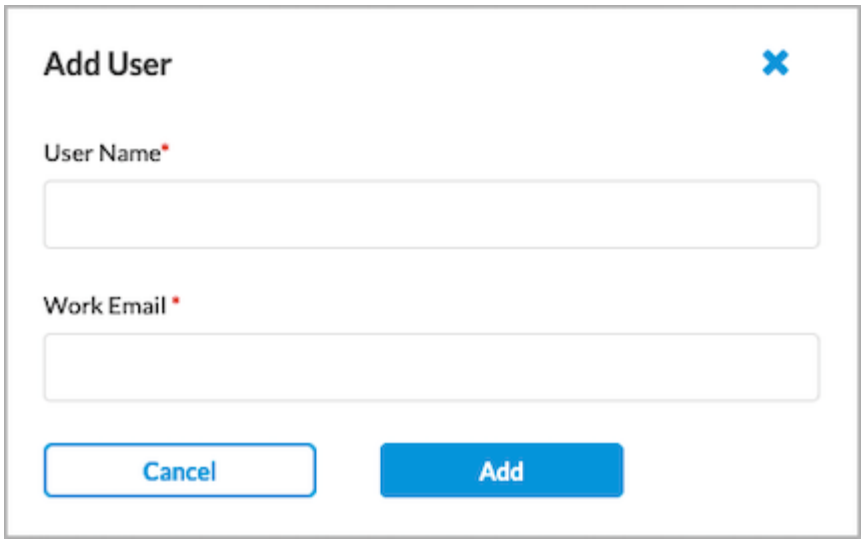


7. Click Add.
8. Click the Users tab in the submenu. The following screen displays.



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.



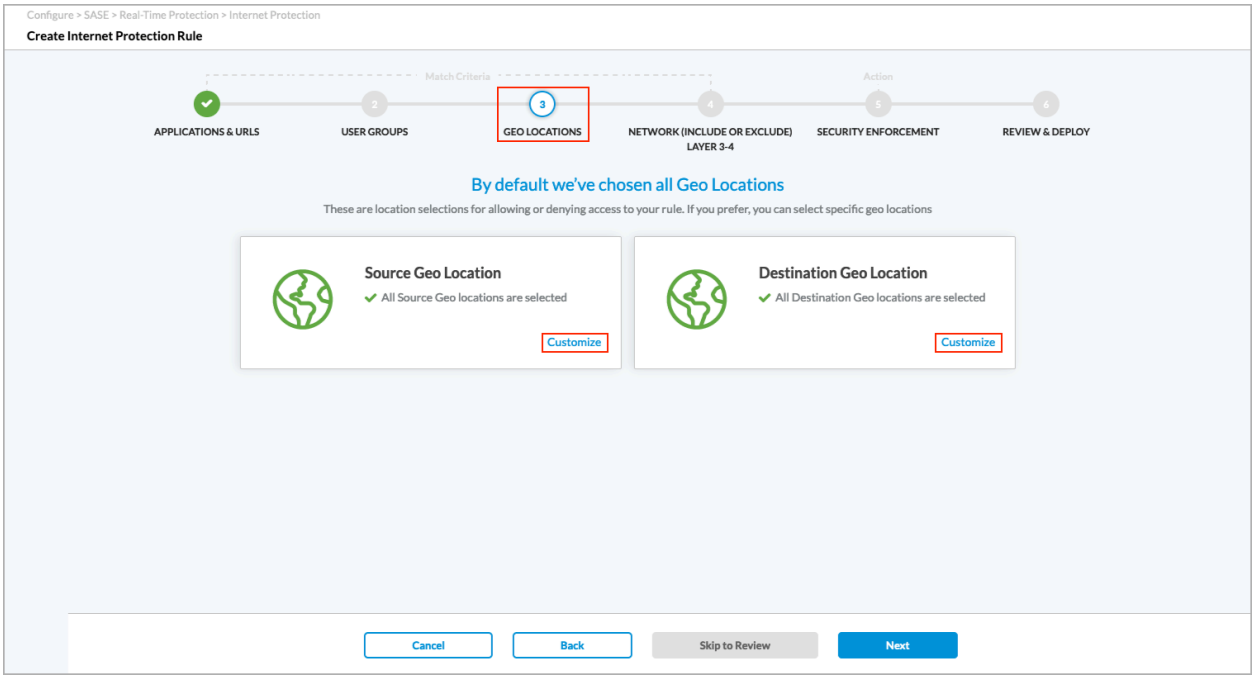
12. Click Add.
13. Click Next to continue to Step 3, Geolocation match criteria.

Configure SASE Geolocation for Internet Protection Rules

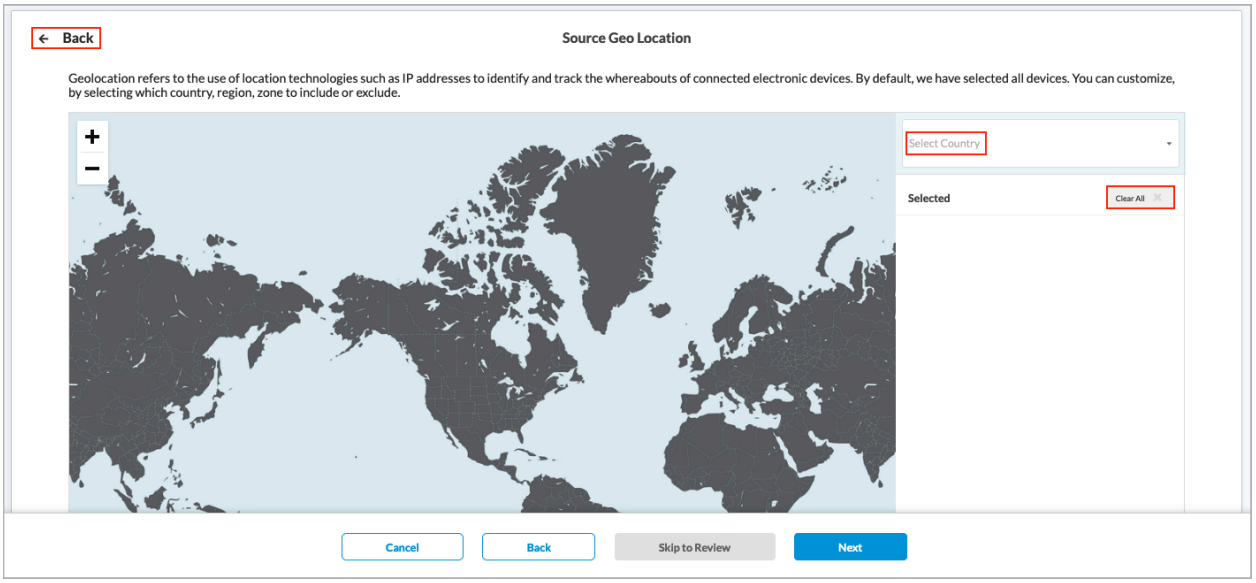
Versa SASE internet protection rules provide a list of predefined regions that you can use to create filter profiles based on both source and destination geographic areas.

To configure geolocation internet protection rule match criteria:

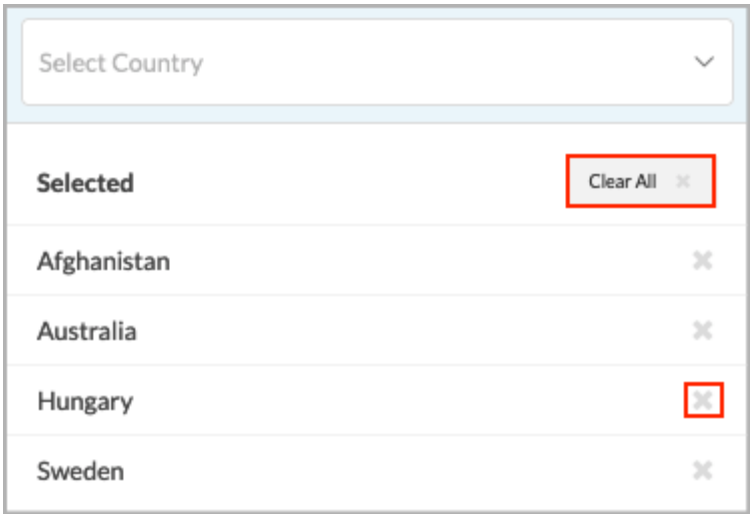
1. In the Create Internet Protection Rule screen, select Step 3, Geolocation. By default, all source and destination geographic locations are included in the match list, which means that no filtering is done based on geographic location and so traffic flows to all destinations.



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



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



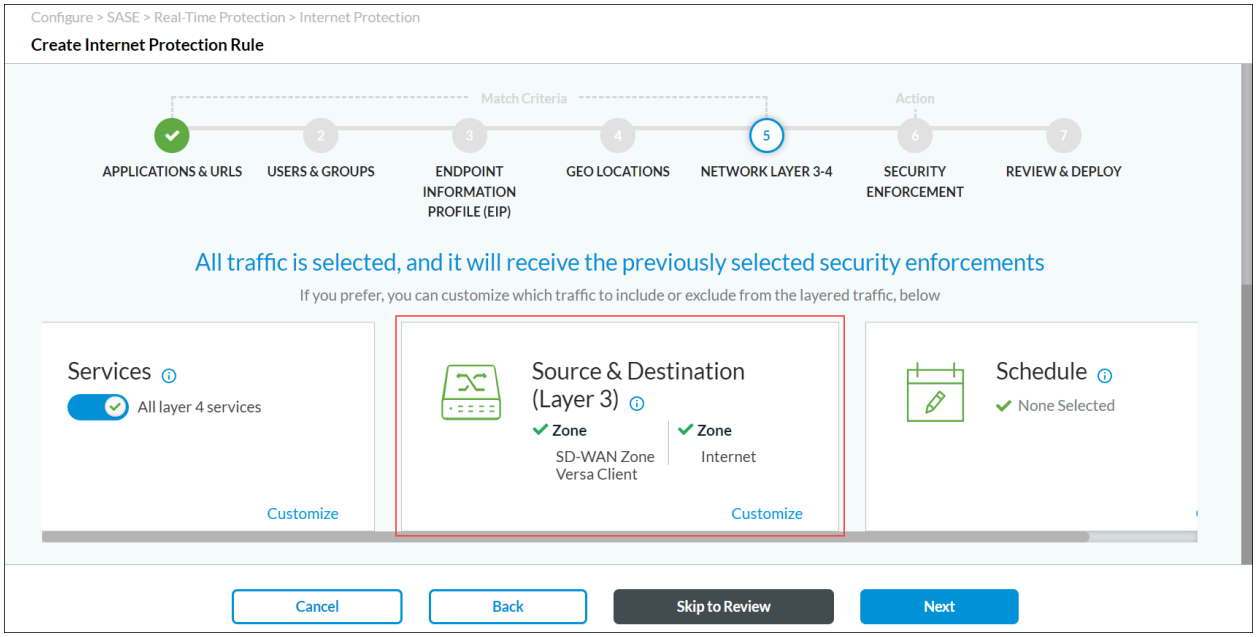
7. To remove a country from the list, click the X next to the country name.
8. To remove all countries from the list, click Clear All.
9. To customize the destination geographical locations, click Back. The Geolocation screen displays again.
10. To accept the default destination geographical locations 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

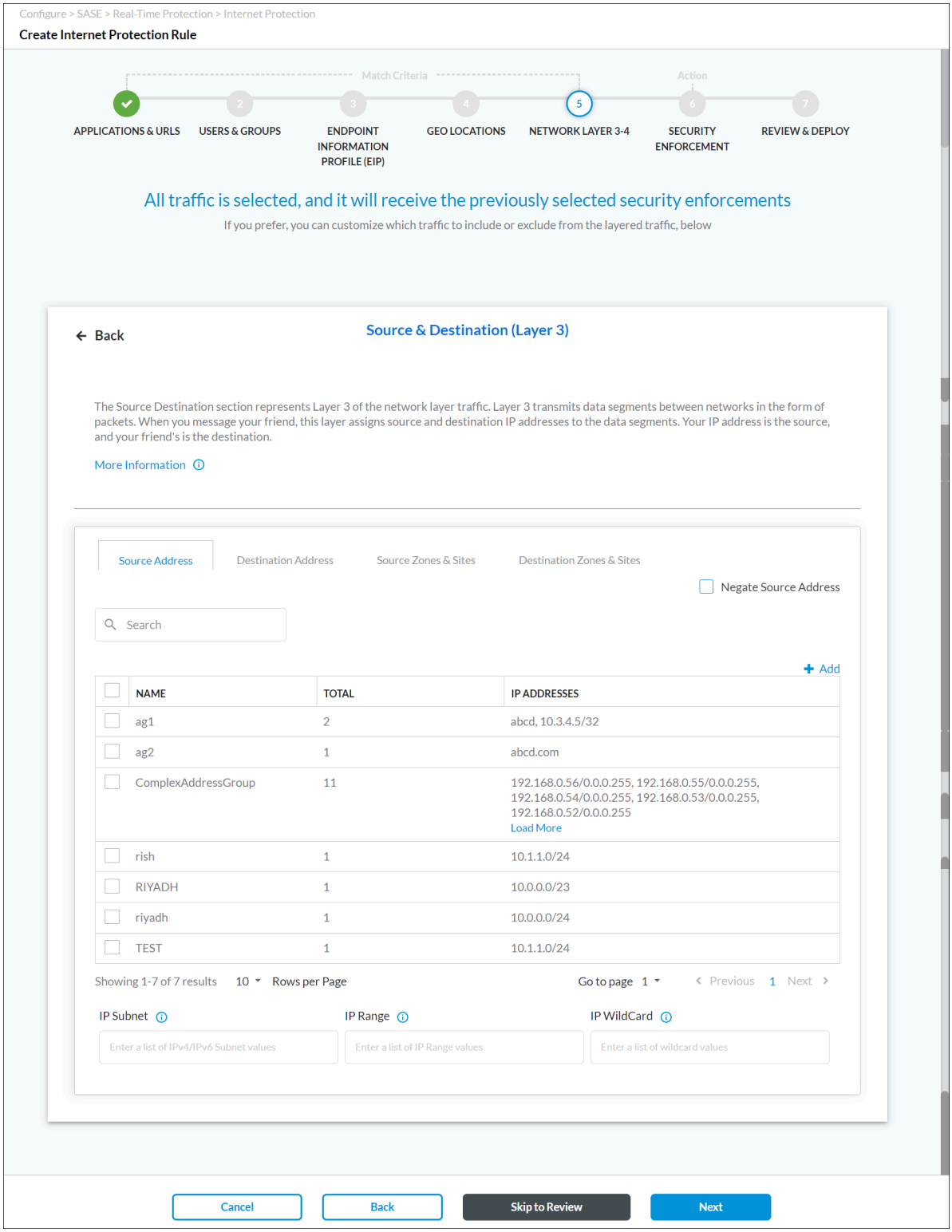
You can create internet protection rule criteria based on source and destination traffic.

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.

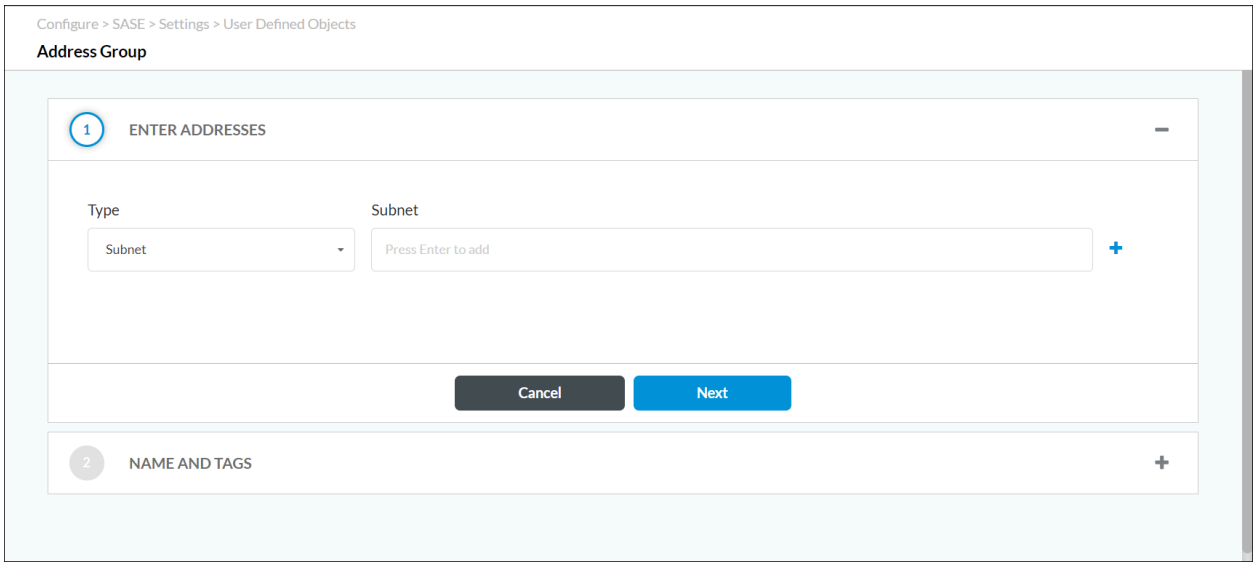


2. To accept the default, click Next to continue to Step 6, Security Enforcement rules.
3. To change the source and destination traffic to include in the match, click Customize in the Source & Destination (Layer 3) pane. In the Source & Destination (Layer 3) screen, select Source Address tab, and then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



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.

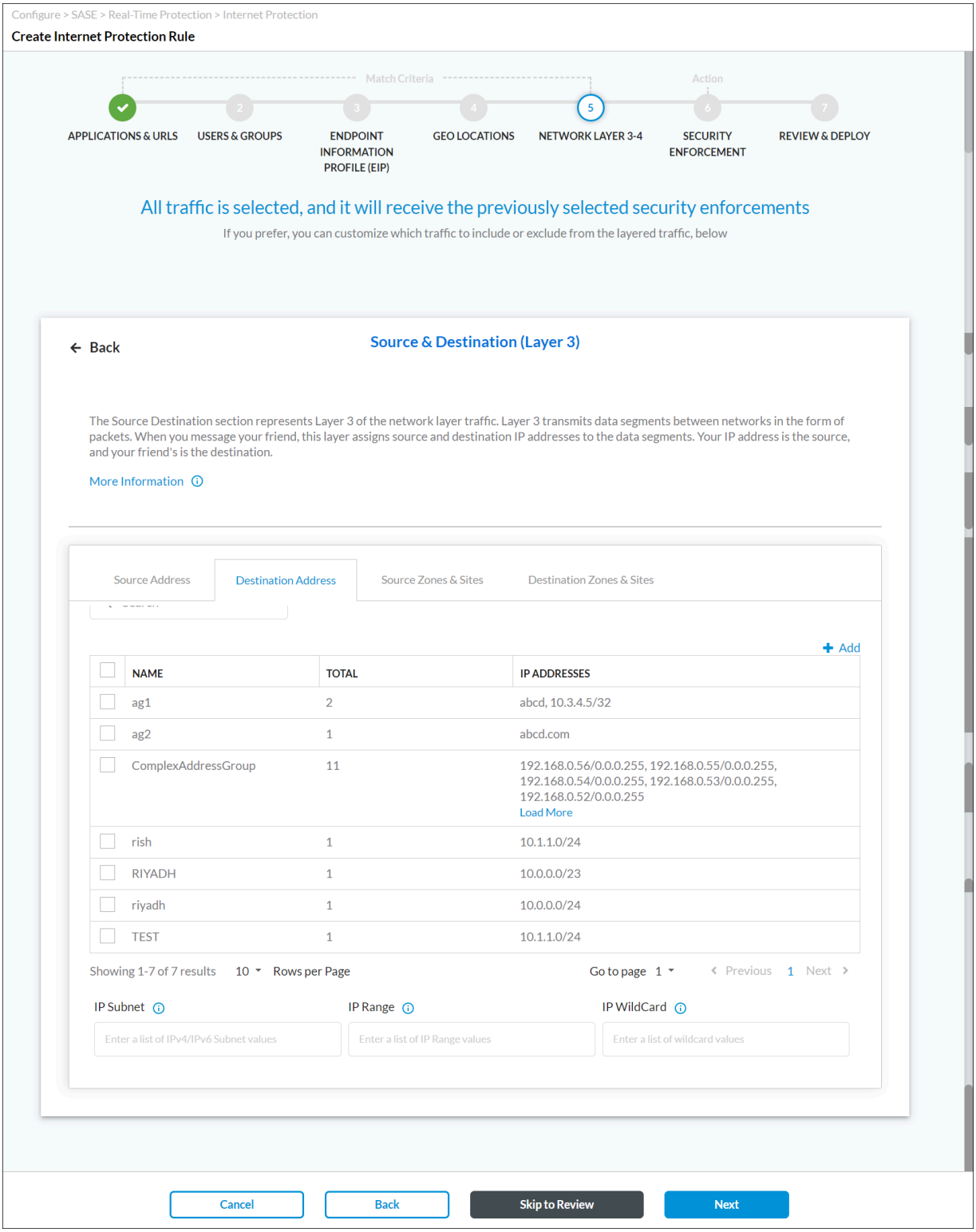
4. To create an address group, click the + Add icon in the Source Address tab. In the Enter Addresses section, enter information for the following fields. You configure the address groups in the User-Defined Objects section. If you want to configure one or more specific source IP addresses, you do not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



Field	Description
Type	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. ◦ Dynamic Address

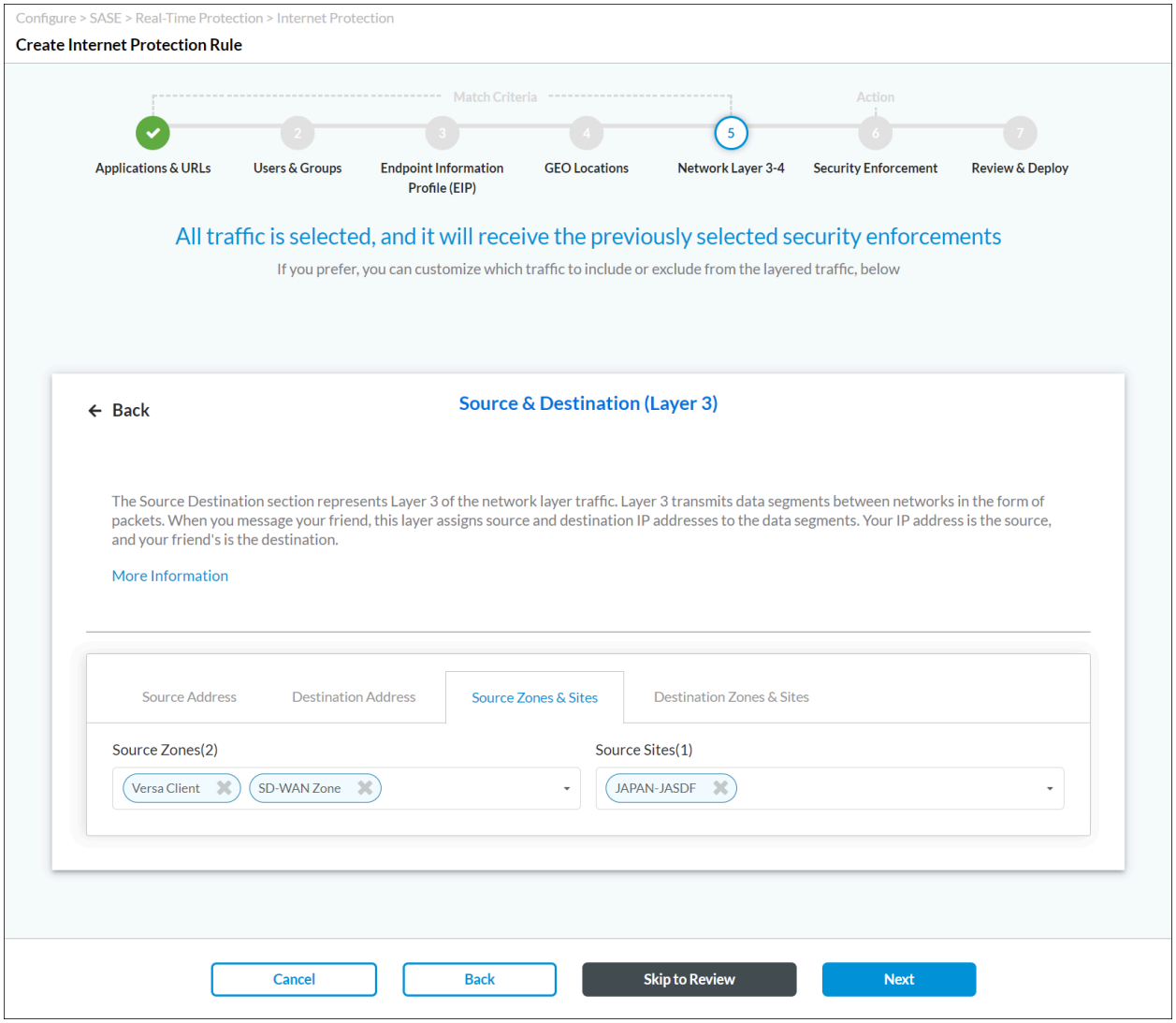
Field	Description
	◦ FQDN ◦ IP Range ◦ IP Wildcard ◦ IPv6 Subnet ◦ Subnet
◦ Subnet	Enter one or more IP addresses and subnet masks, for example, 10.2.1.0/24.
◦ IP Range	Enter one or more IP addresses within the IPv4 address range specified in the IPv4 Range field, for example, 10.2.1.1–10.2.2.2.
◦ IP 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.

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.



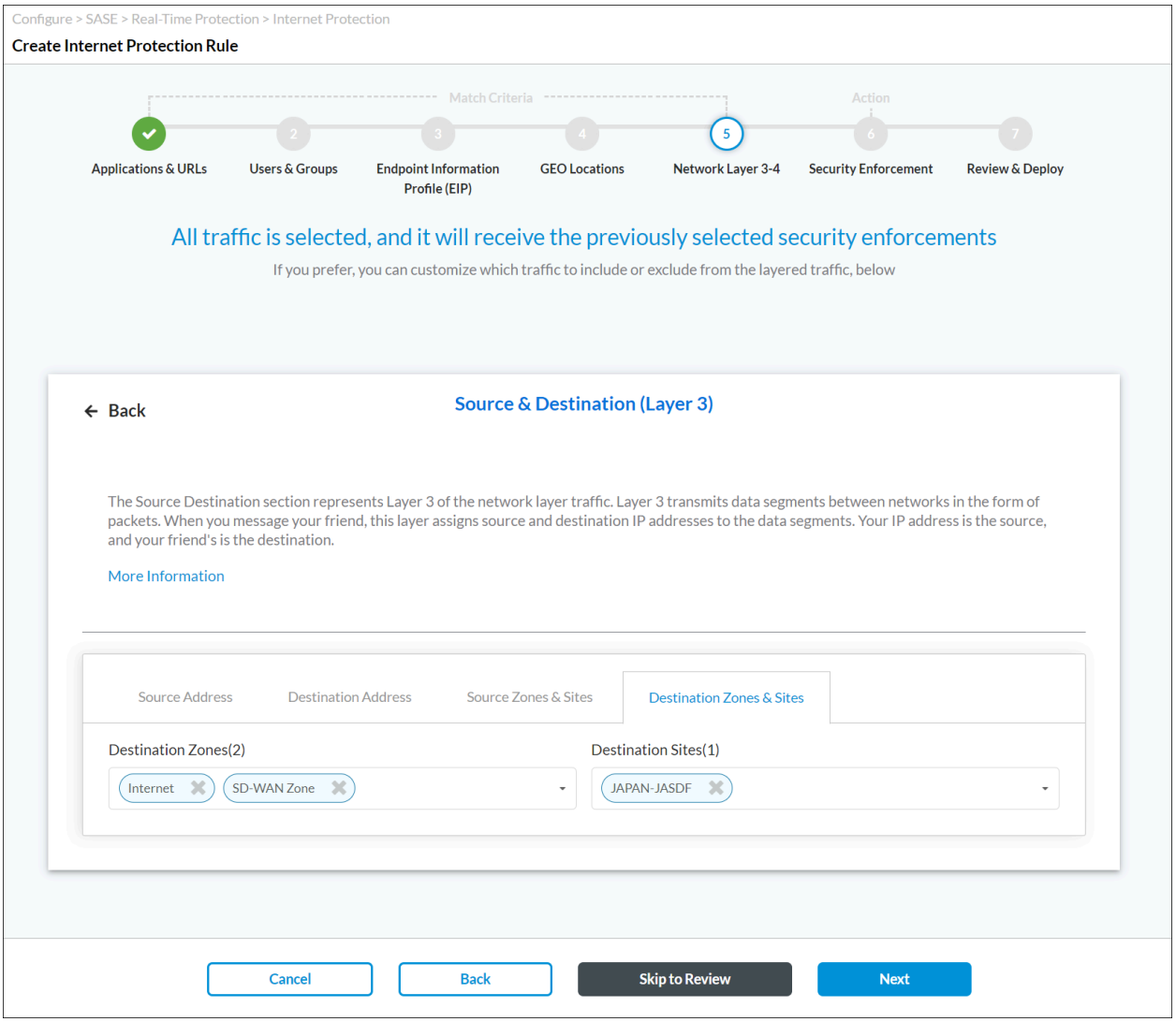
Field	Description
Negate Destination Address	Select to apply the rule to any destination addresses except the ones in the Destination Address field.
IP Subnet	Enter a list of comma-separated subnets to include in the match list, for example, 10.2.1.0/24.
IP Range	Enter a list of comma-separated IP addresses 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.



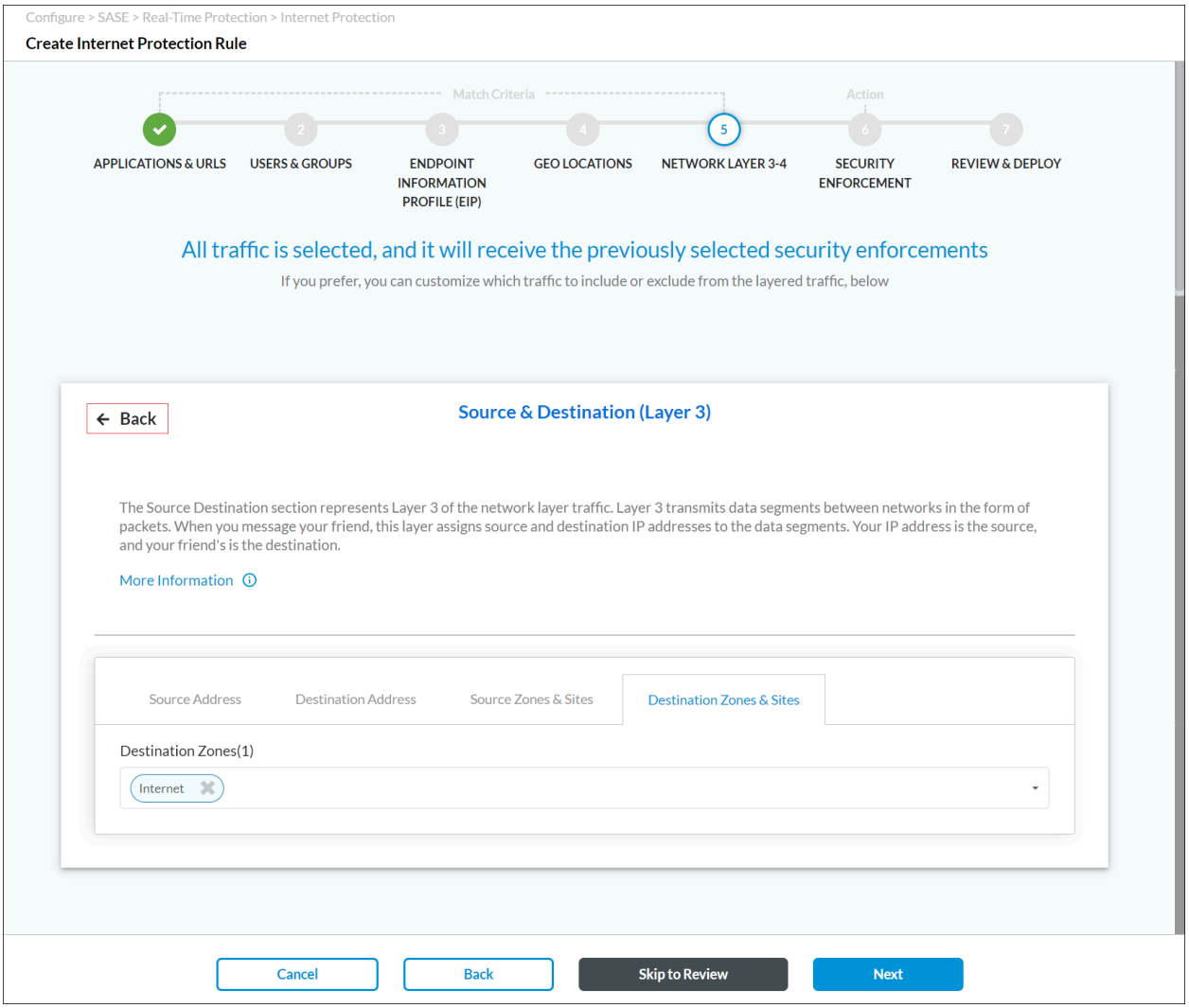
- In the Source Zones field, select one or more source zones to include in the match list. By default, three source zones are available. User-defined zones, such as zones for IPsec and GRE tunnels, also display in this list, and you can select them.
  - Internet—Select this zone if traffic comes from 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.



- 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.



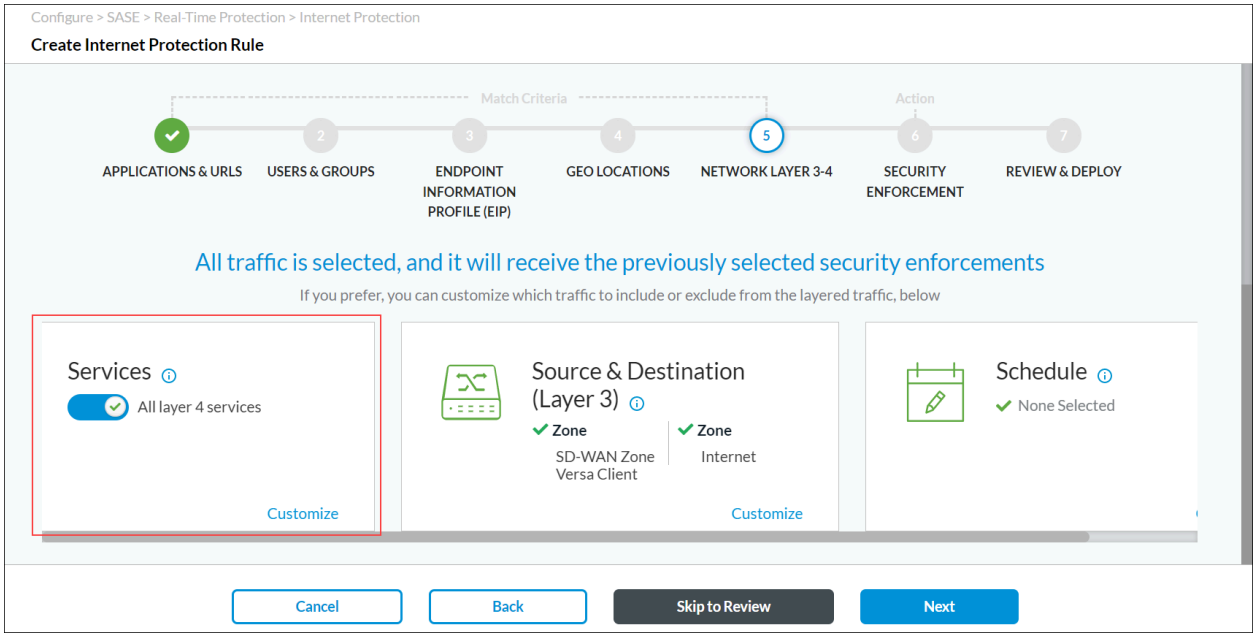
13. Click Next to continue to Step 6, Security Enforcement rules.

Configure SASE Network Services for Internet Protection Rules

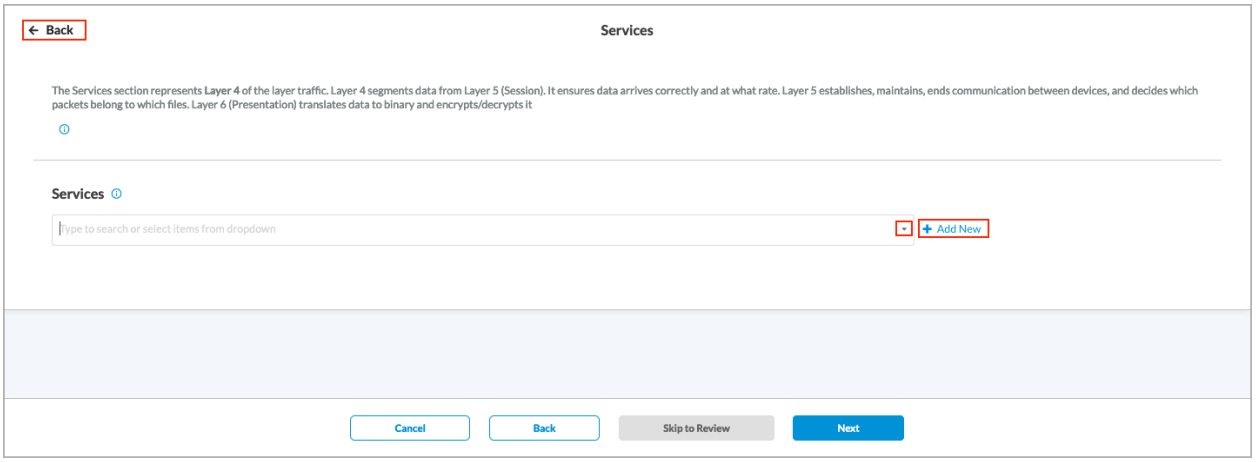
You can configure internet protection rules to filter traffic according to the network service being provided. By default, all network services are selected, which means that security enforcement rules are applied to the traffic of all network service types. If desired, you can specify the services to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

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

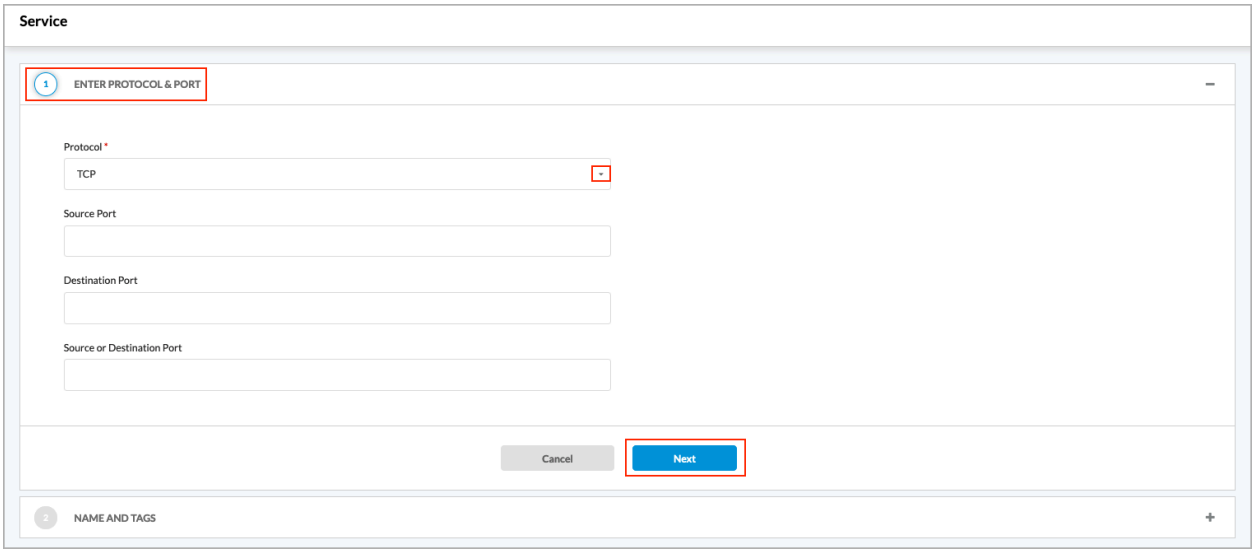
1. In the Create Internet Protection Rule screen, select Step 5, Network (Include or Exclude) Layer 3-4, and then select Services. By default, all Layer 4 services included in the match.



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



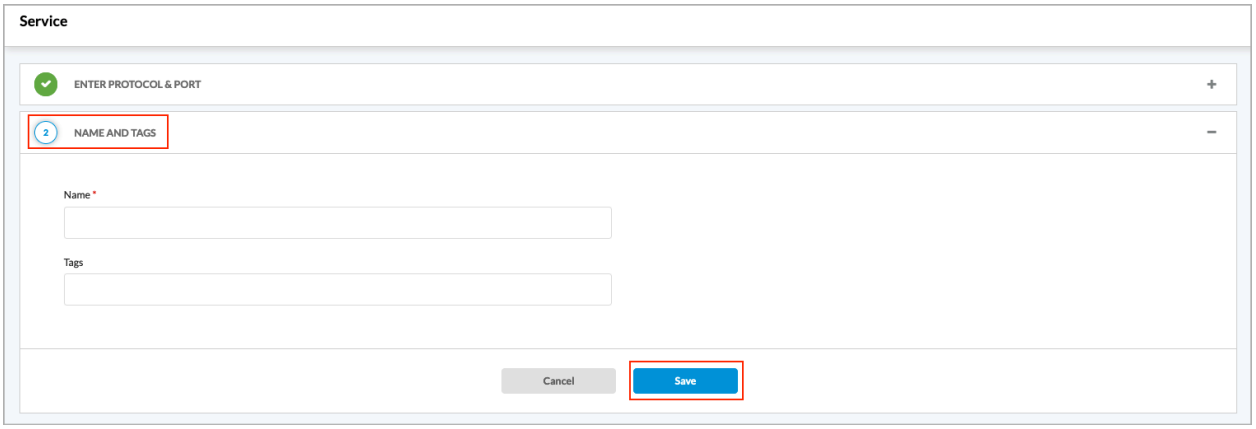
3. In the Services field, select one or more of the predefined services. To add a custom service, click + Add New. The following screen displays.



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	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.



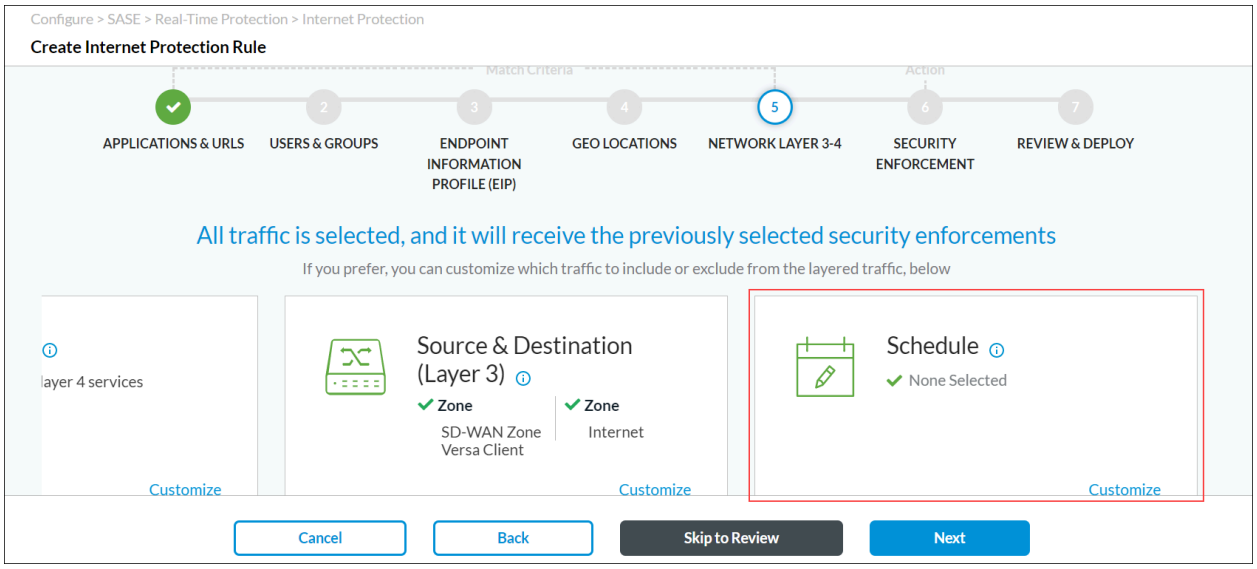
6. In the Name field, enter a name for the new service.
7. In the Tags field, enter optional tags.
8. Click Save to add the new service to the protocol list. You can then select the new service.
9. Click Back to return to the Step 4, Network (Include or Exclude) Layer 3-4 screen. From this screen you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

Configure Schedules for SASE Internet Protection Rules

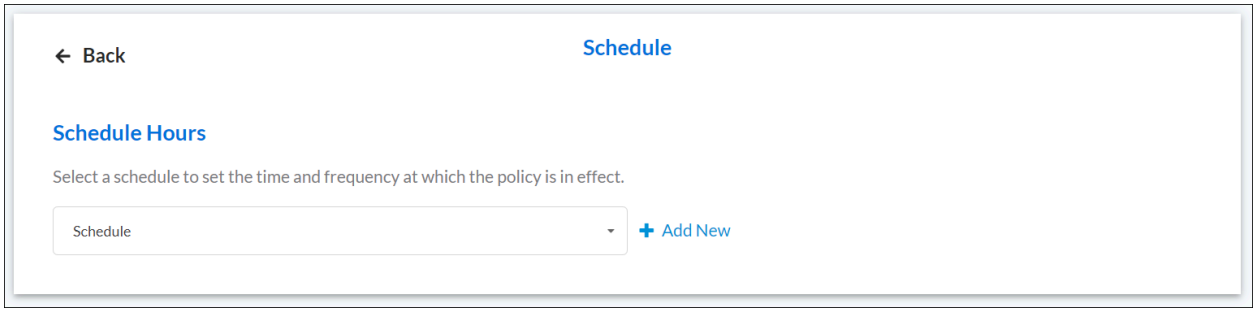
Security policy rules are in effect on all days and at all times. You can define a schedule to limit a security policy so that it is in effect only at specific times. You can also create schedules to limit when to apply internet protection rules to filter traffic. You then apply the schedule to the desired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

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

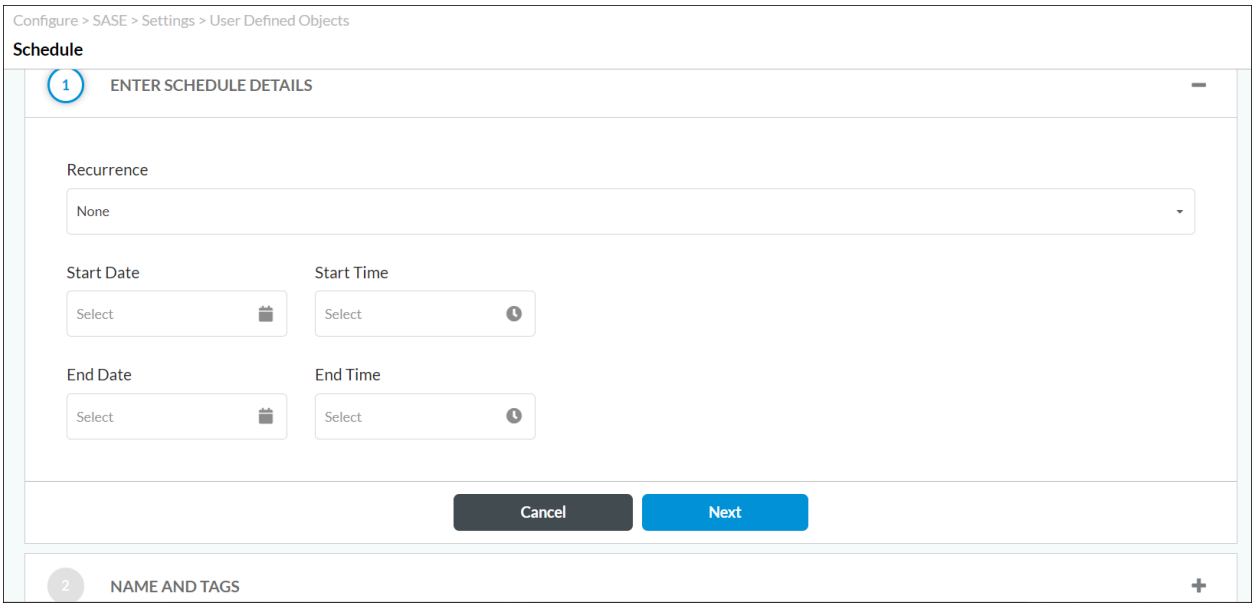
1. In the Create Internet Protection Rule screen, select Step 5, Network Layer 3-4, and then select Schedules. By default, no schedules are configured.

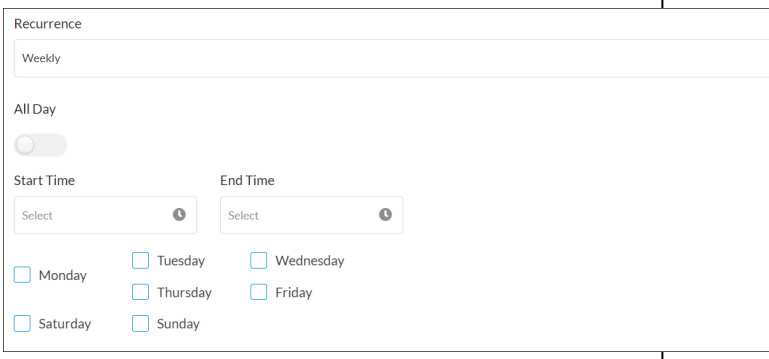


2. To select or create a schedule, click Customize under Schedule.
3. In Schedule Hours, select a schedule. If no schedules exist, click + Add New to create a schedule to set the time and frequency at which the rule is in effect.

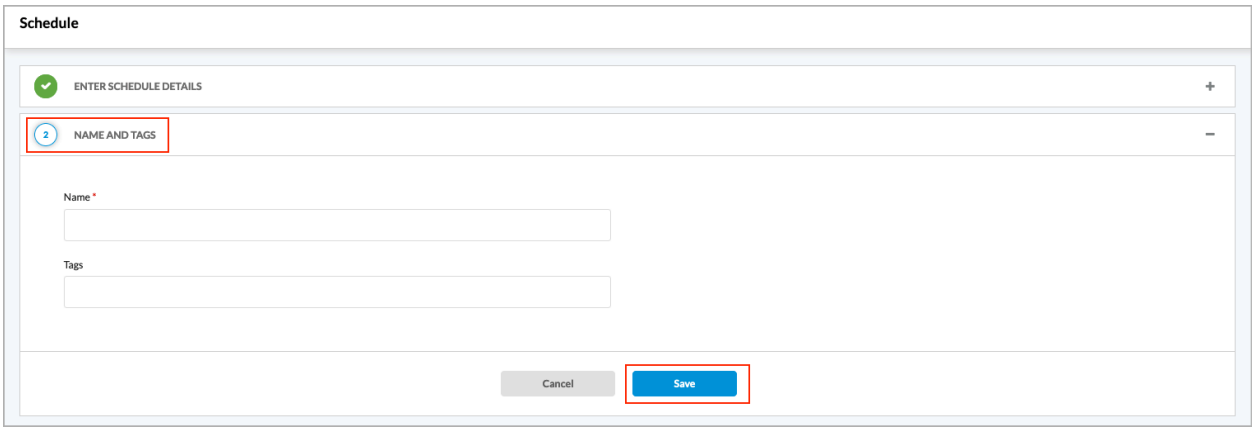


4. In the Enter Schedule Details section, enter information for the following fields.



Field	Description
Recurrence	Select how often the policy is to be in effect: ◦ Daily ◦ None ◦ Weekly
All Day	If you select Daily or Weekly, click the slider to schedule the policy to be in effect all day. 
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	If you select Weekly, select the days of the week for the policy to be in effect. 

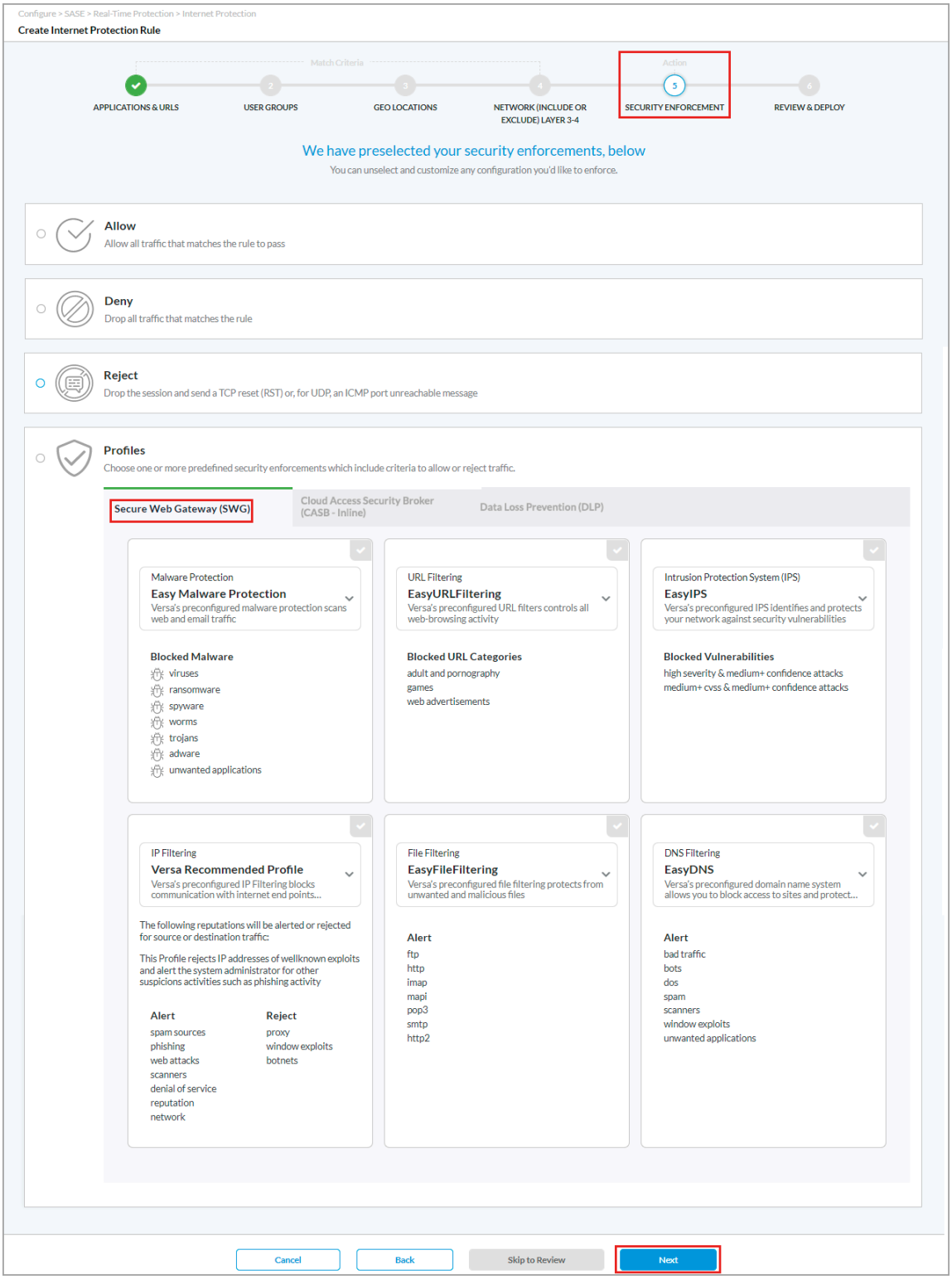
5. Click Next. The following screen displays.



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.



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

You can specify 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.
- 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

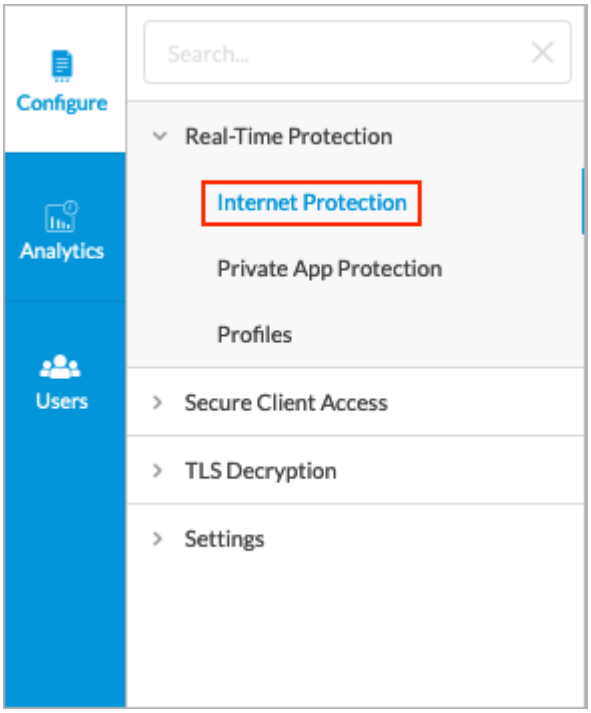
Malware is malicious software software that is specifically designed to disrupt computers and computer systems. There are many types of malware, including computer viruses, worms, Trojan viruses, spyware, adware, and ransomware. Among the things malware can do is leak private information, gain unauthorized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

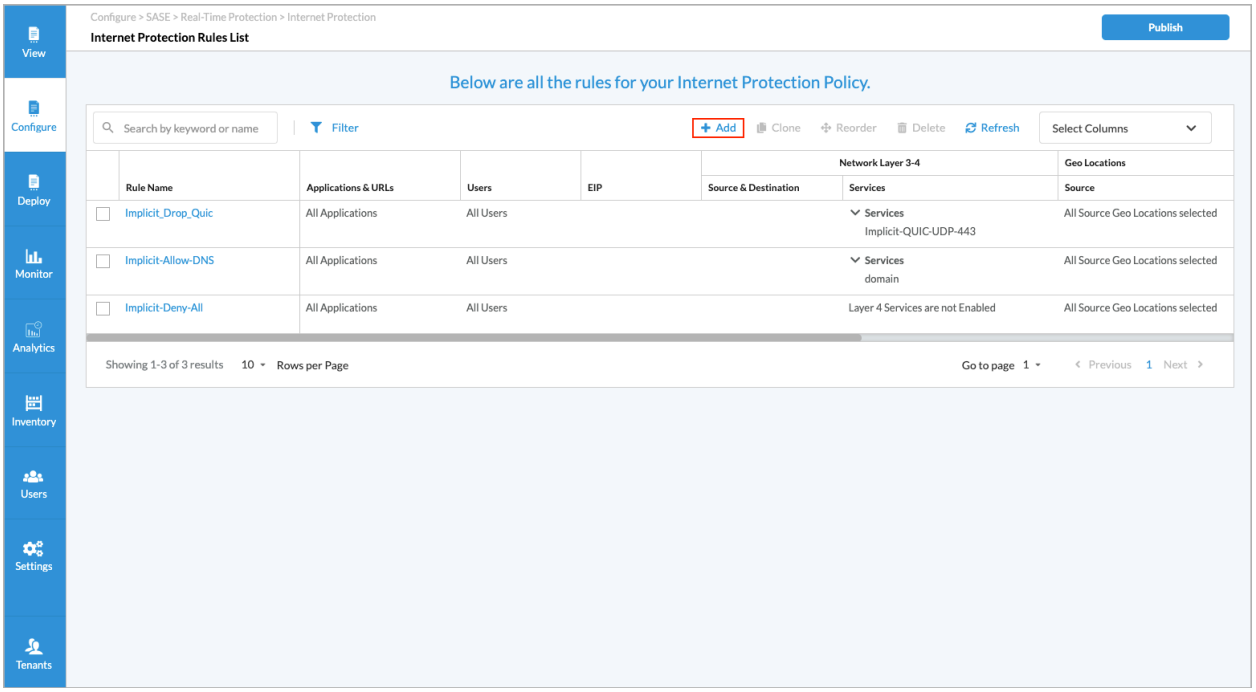
Note: The malware protection profile displays only if the tenant is subscribed to both the SWG and VSA Professional services.

To configure a malware protection profile:

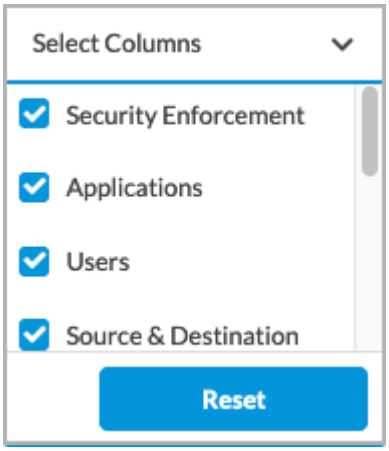
1. Go to Configure > Real-Time Protection > Internet Protection.



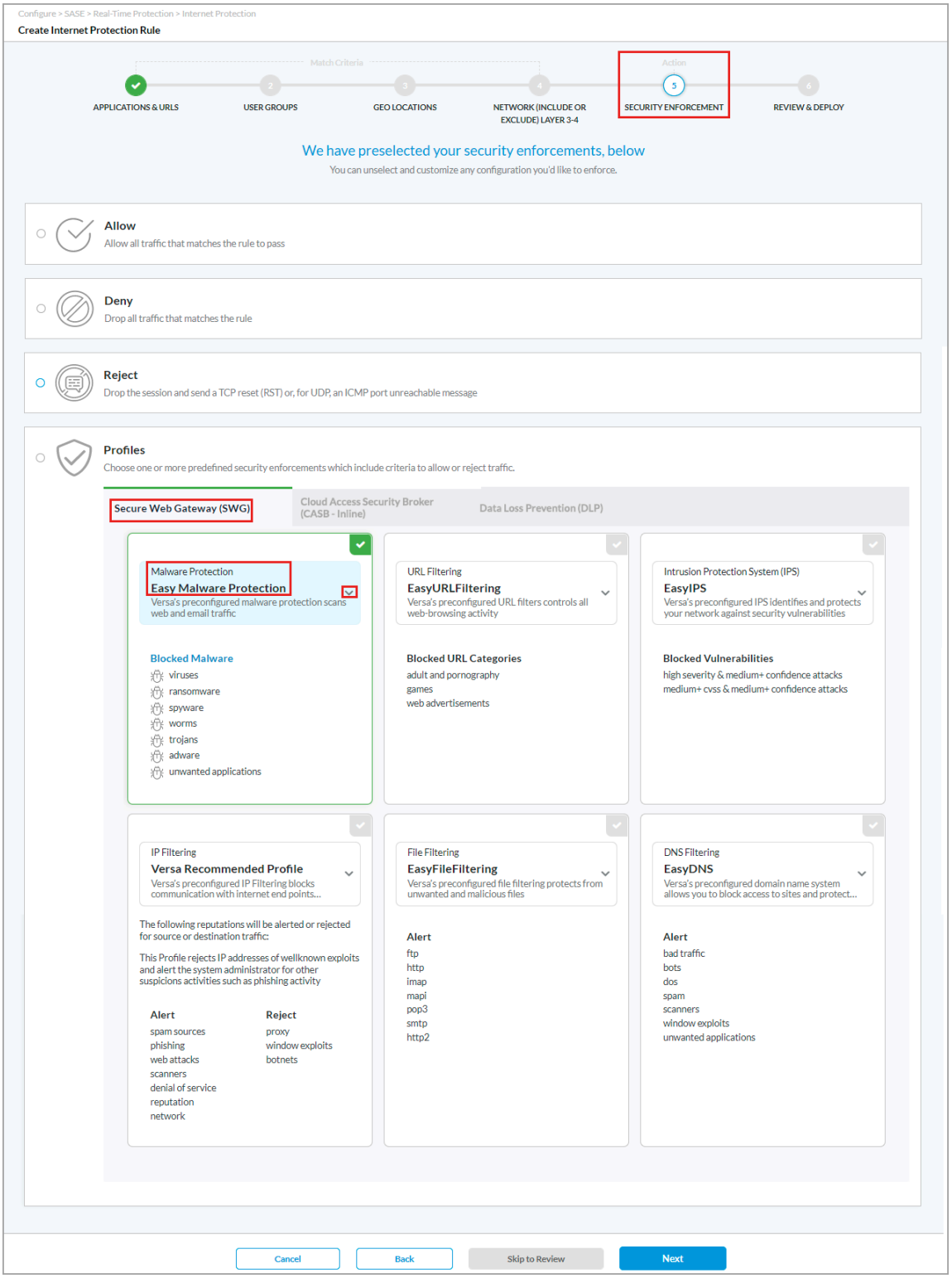
The Internet Protection Rules List screen displays all configured internet protection rules.



2. 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.



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

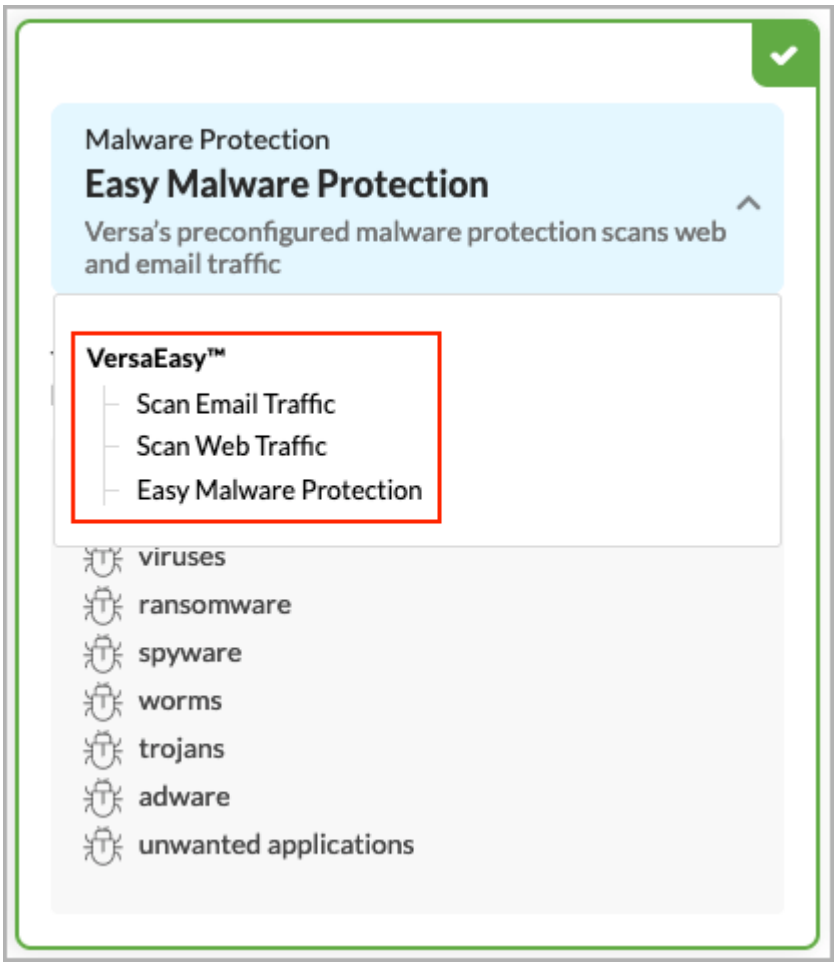


4. Select the Security Enforcement action.
5. Select the Secure Web Gateway (SWG) tab, and then click in the Malware Protection box to enable the default EasyMalwareProtection security enforcement profile. By default, the EasyMalwareProtection profile blocks the

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:

- 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.

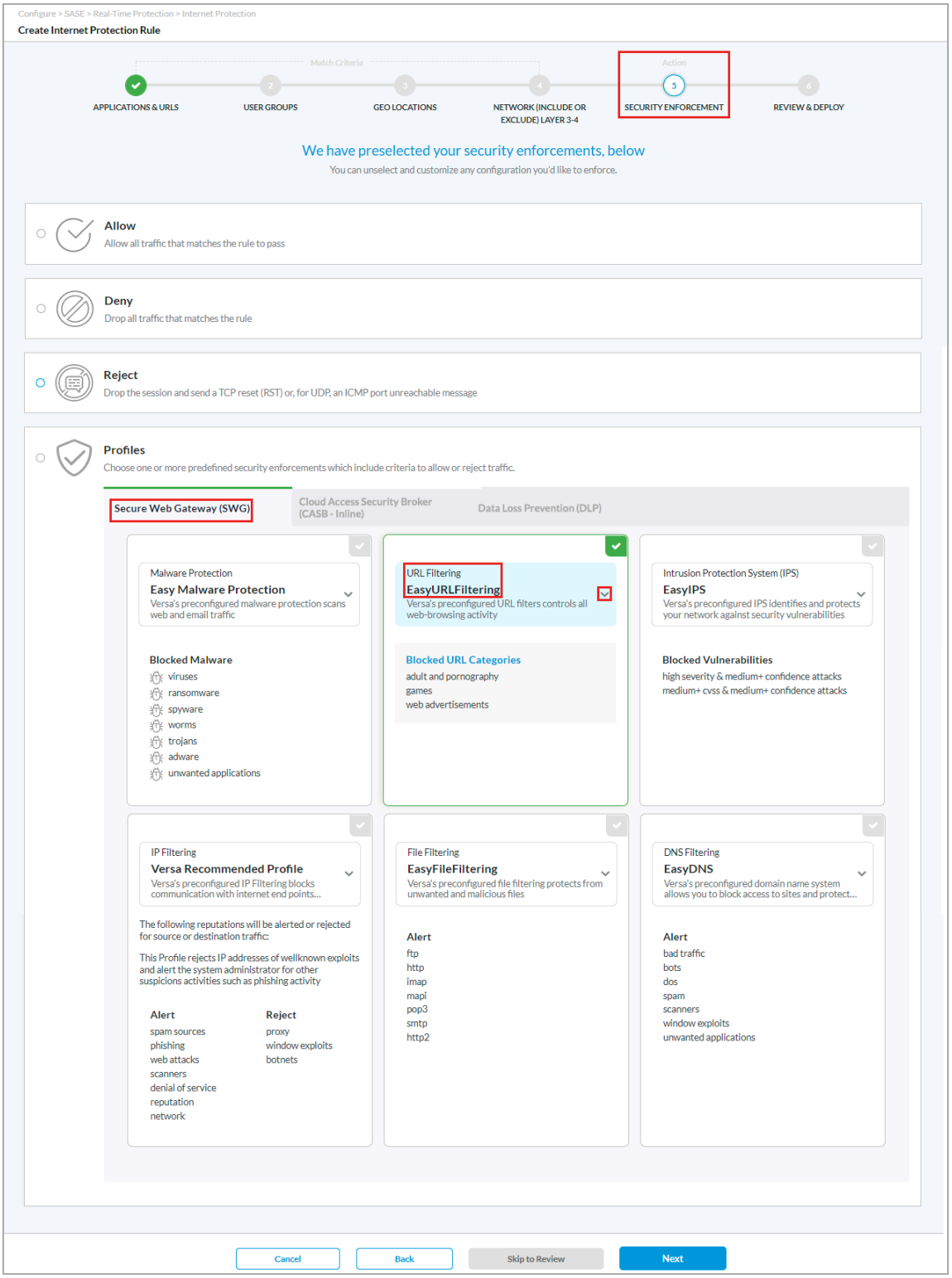
Configure a URL-Filtering Profile for SASE Internet Protection Rules

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

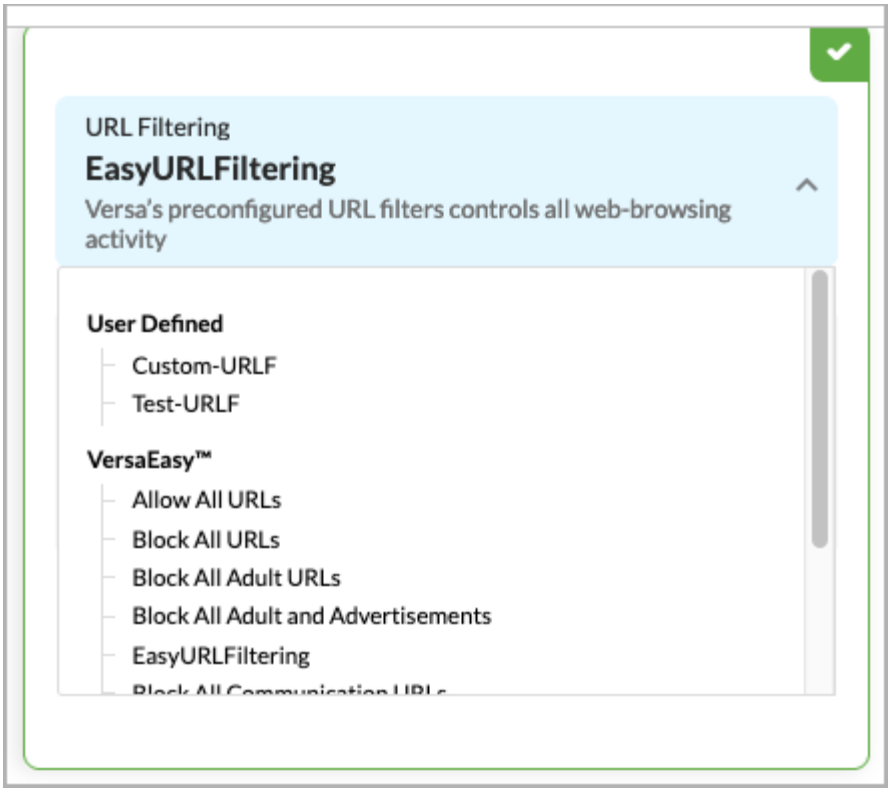
In addition to using predefined URL-filtering profiles, you can create custom URL-filtering profiles and associate them with internet protection rules. For more information, see Configure Custom URL-Filtering Profiles.

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



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

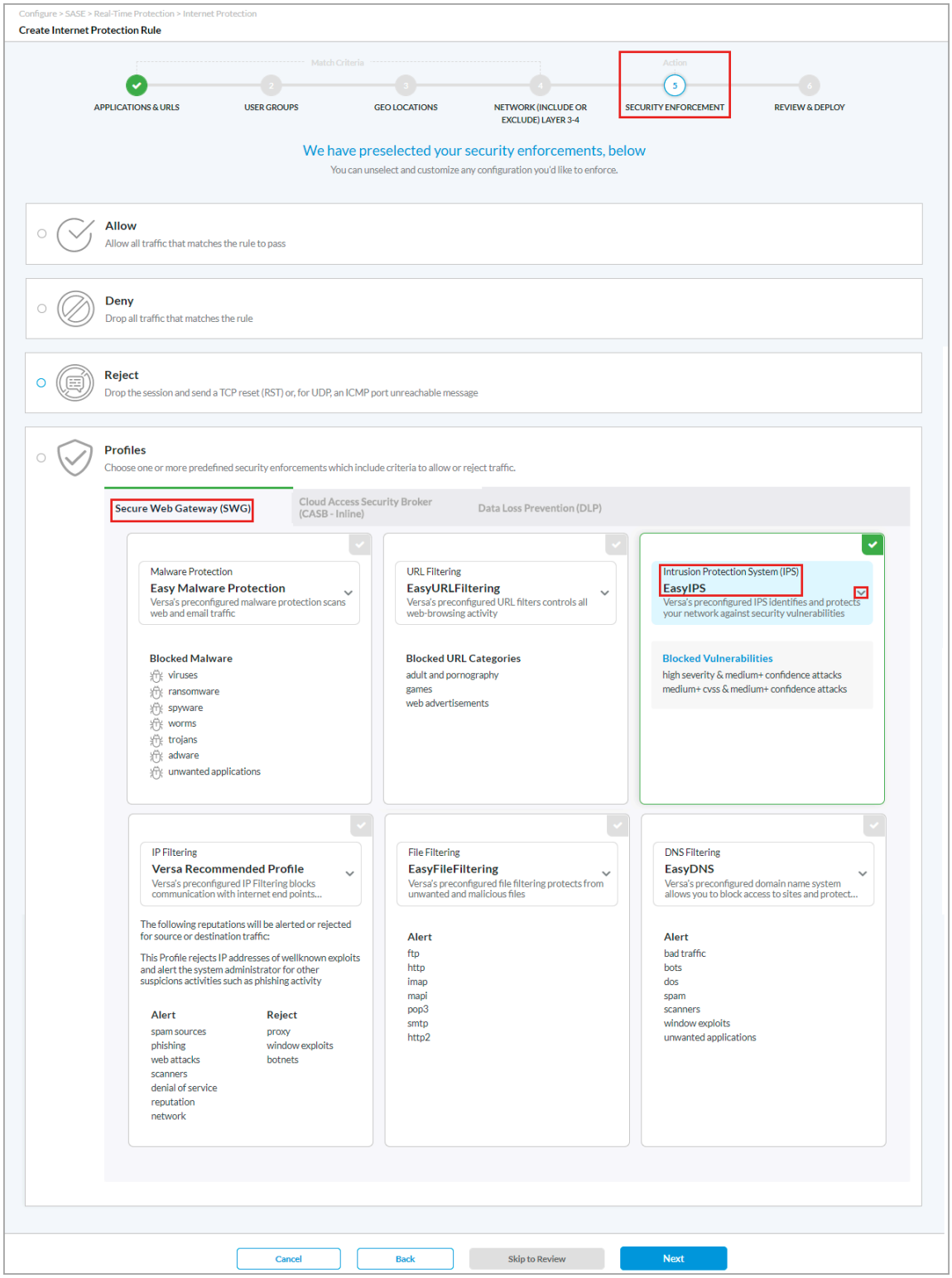
The intrusion prevention system (IPS) mitigates security vulnerabilities by responding to inappropriate or anomalous activity. Responses can include dropping data packets and disconnecting connections that are transmitting unauthorized data.

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

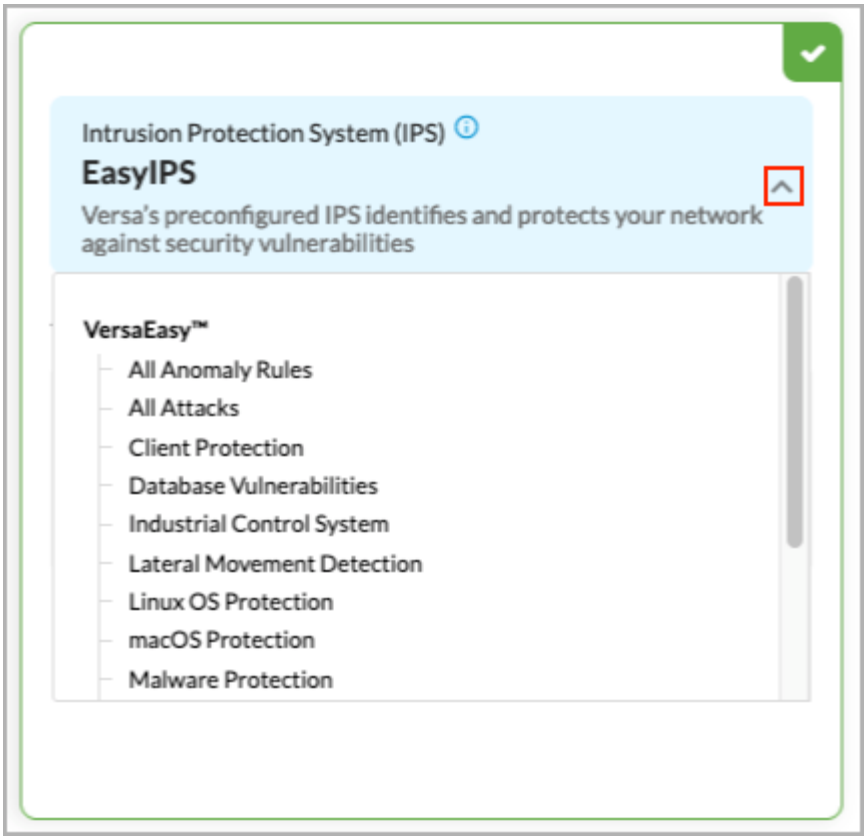
Note: The IPS profile displays only if the tenant is subscribed to the SWG and VSA Professional services.

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



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



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.

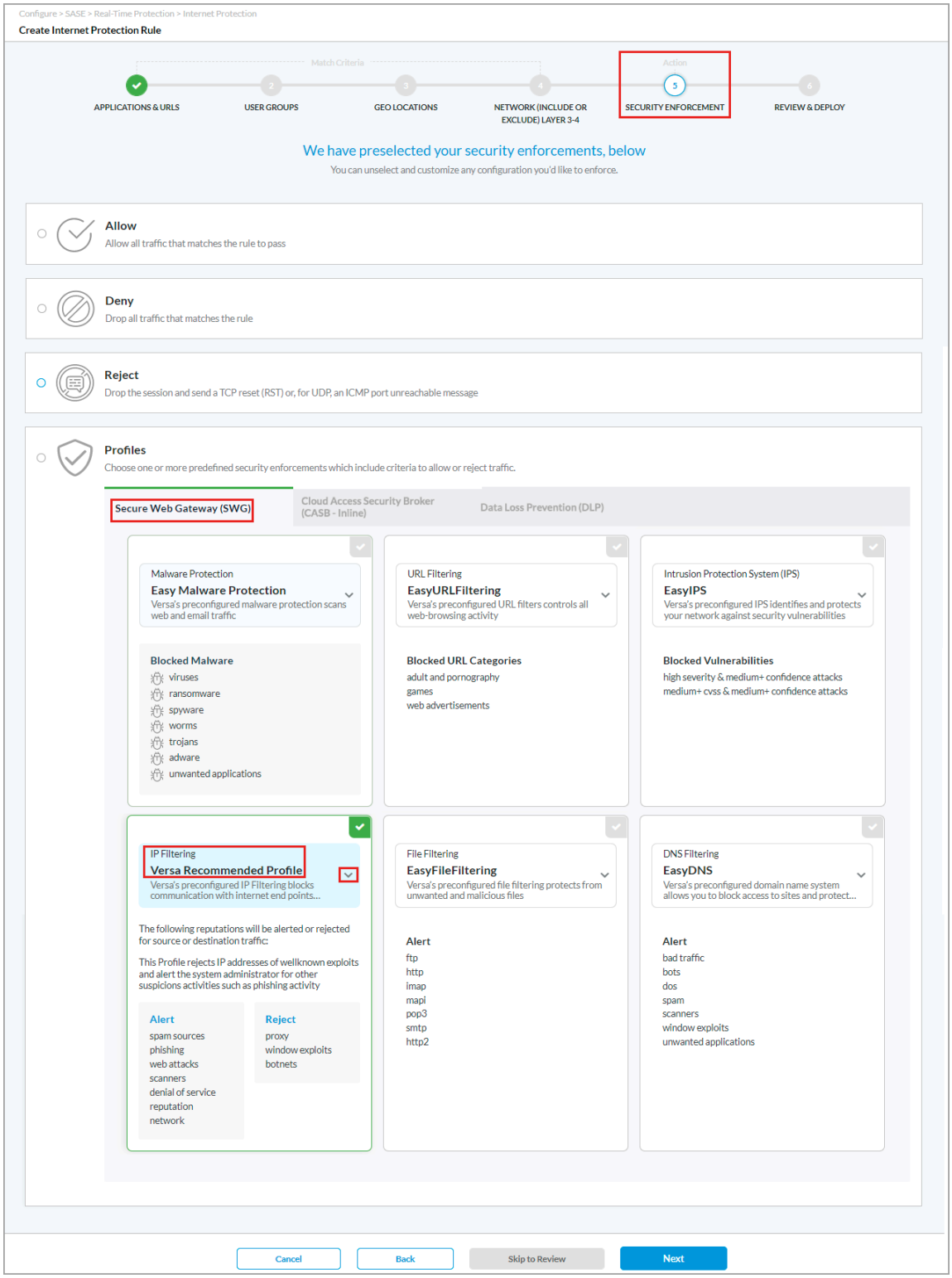
To configure an IP-filtering profile:

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

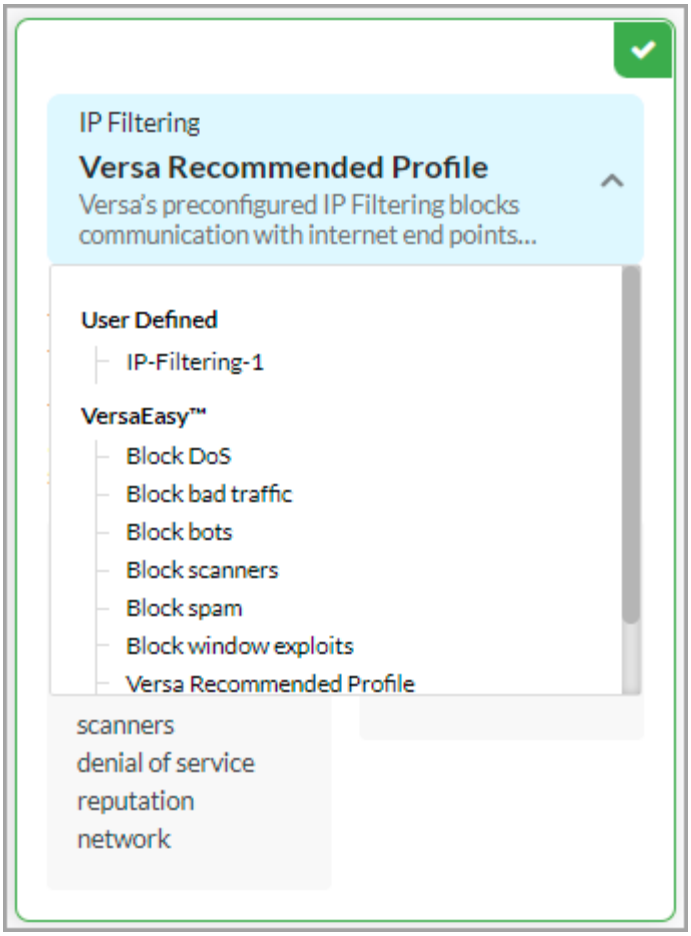
- Spam sources
- Web attacks

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

- Botnets
- Proxy
- Window exploits



2. 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 Versa 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, metwork, 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

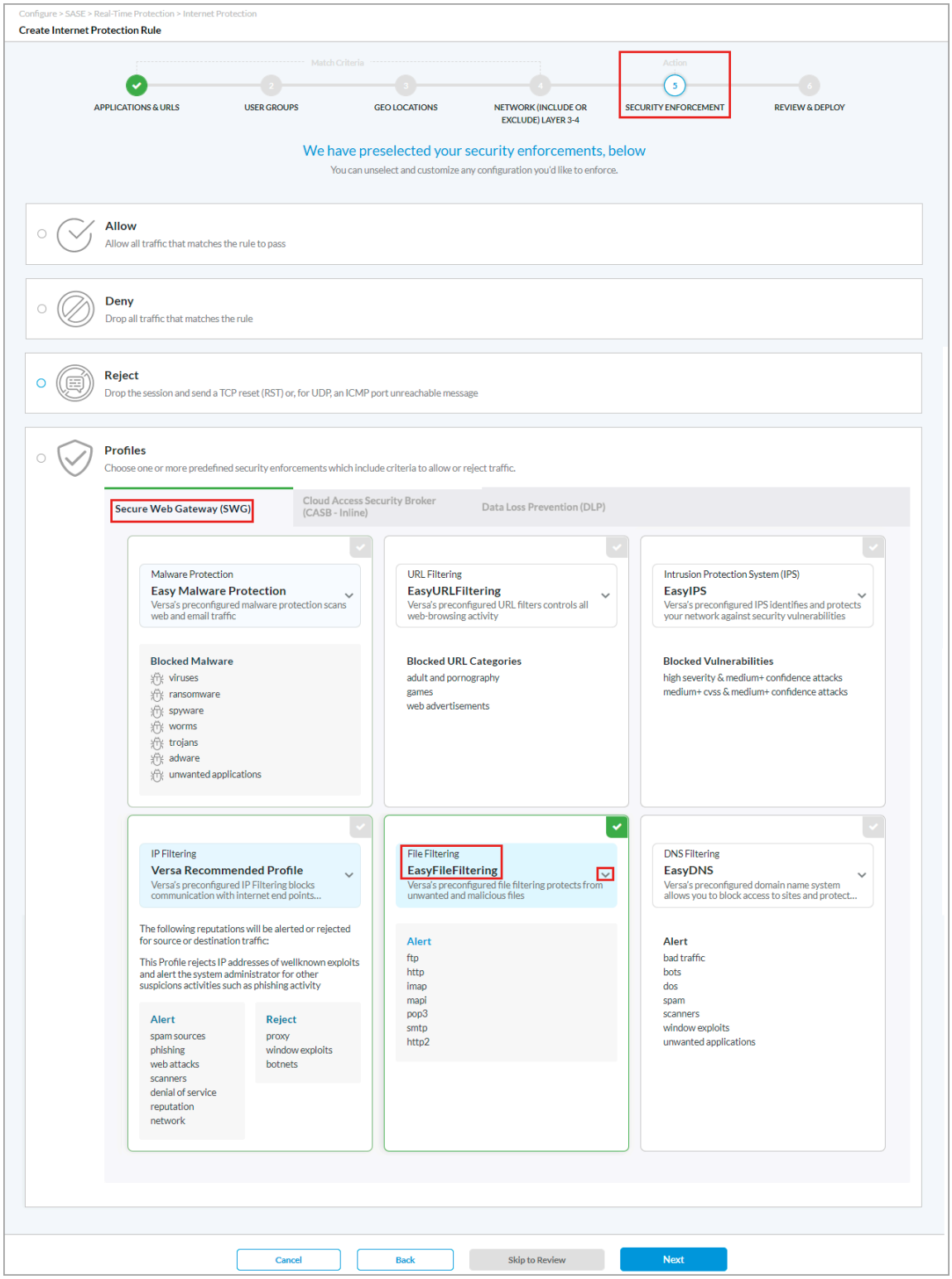
File filtering helps to reduce the risk of attacks from unwanted and malicious files associated with various protocols. By blocking the transfer of potentially dangerous files and types of files, you decrease an attacker's ability to attack your organization.

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.

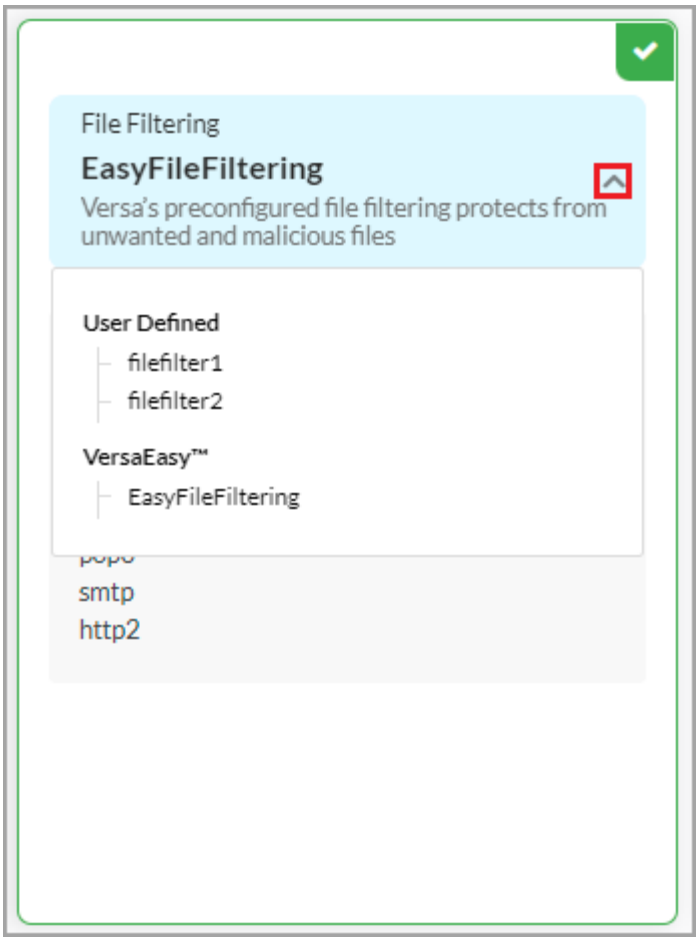
To configure an file-filtering profile:

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



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.

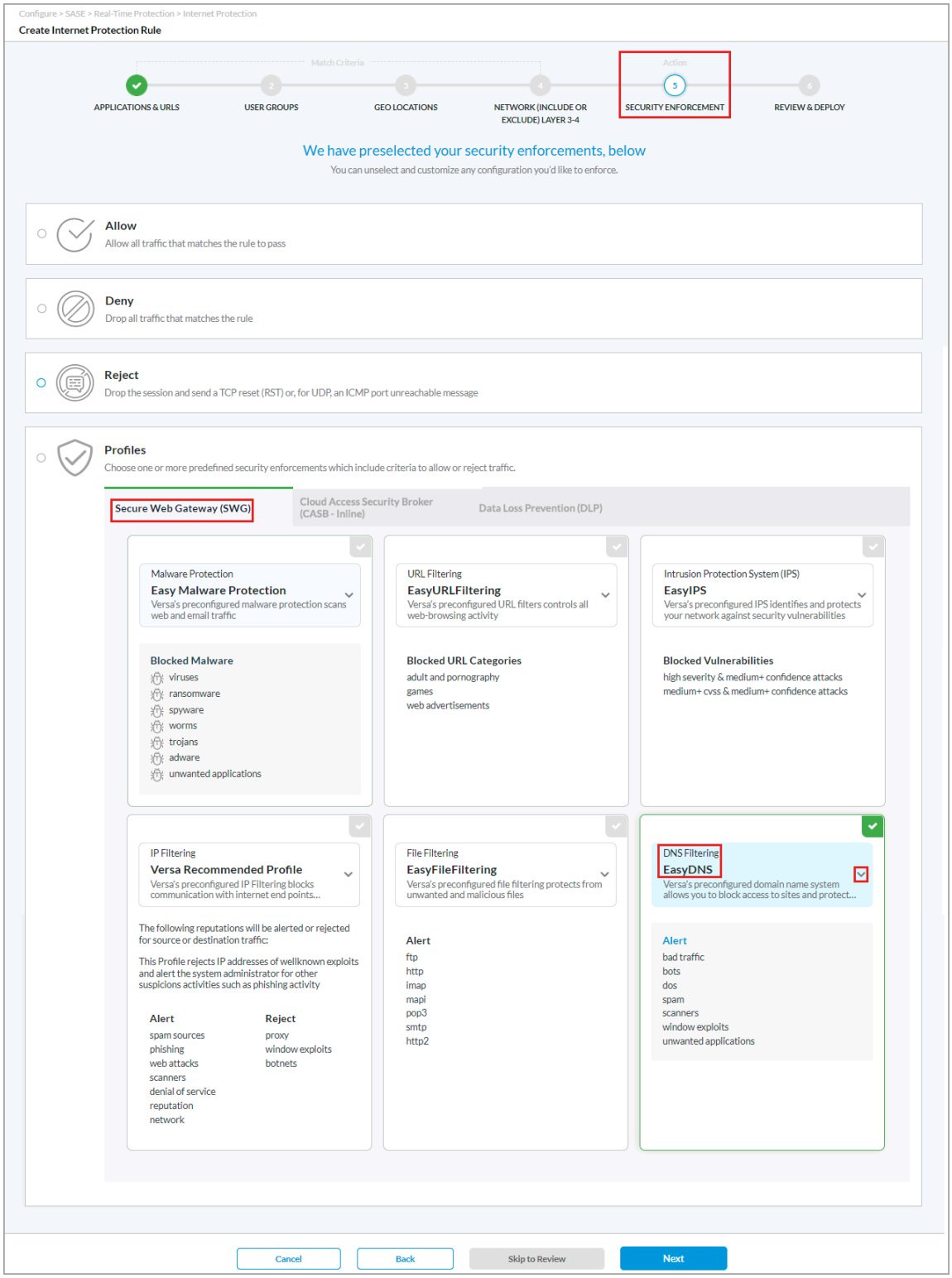
In addition to using predefined DNS-filtering profiles, you can create custom DNS-filtering profiles and associate them with internet protection rules. For more information, see Configure Custom DNS-Filtering Profiles.

To configure a DNS-filtering profile:

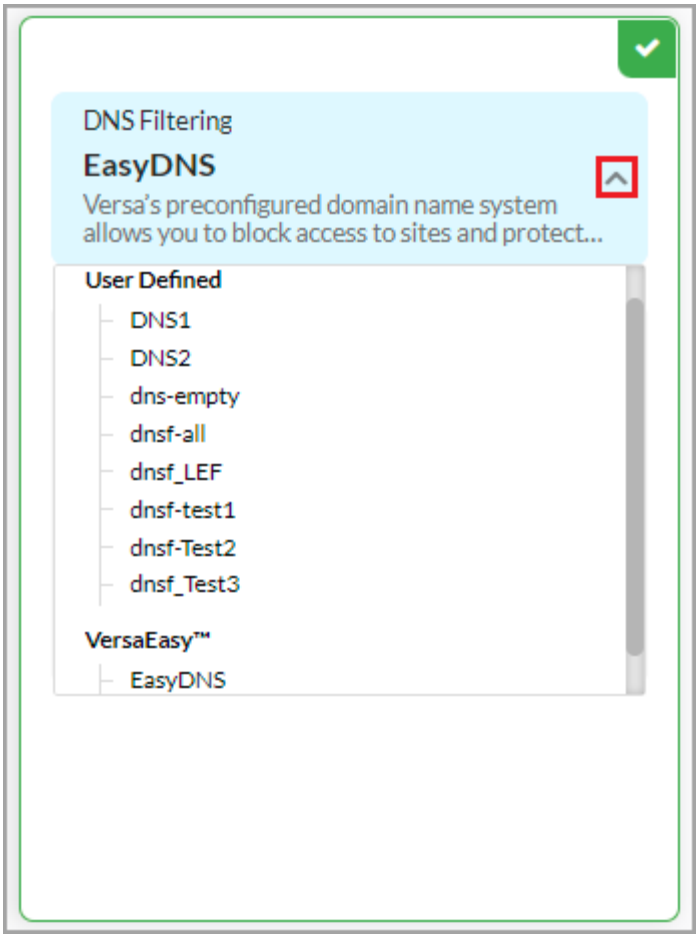
1. In the Security Enforcement screen > Secure Web Gateway (SWG) tab, select DNS Filtering in the Profiles section

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



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.



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.

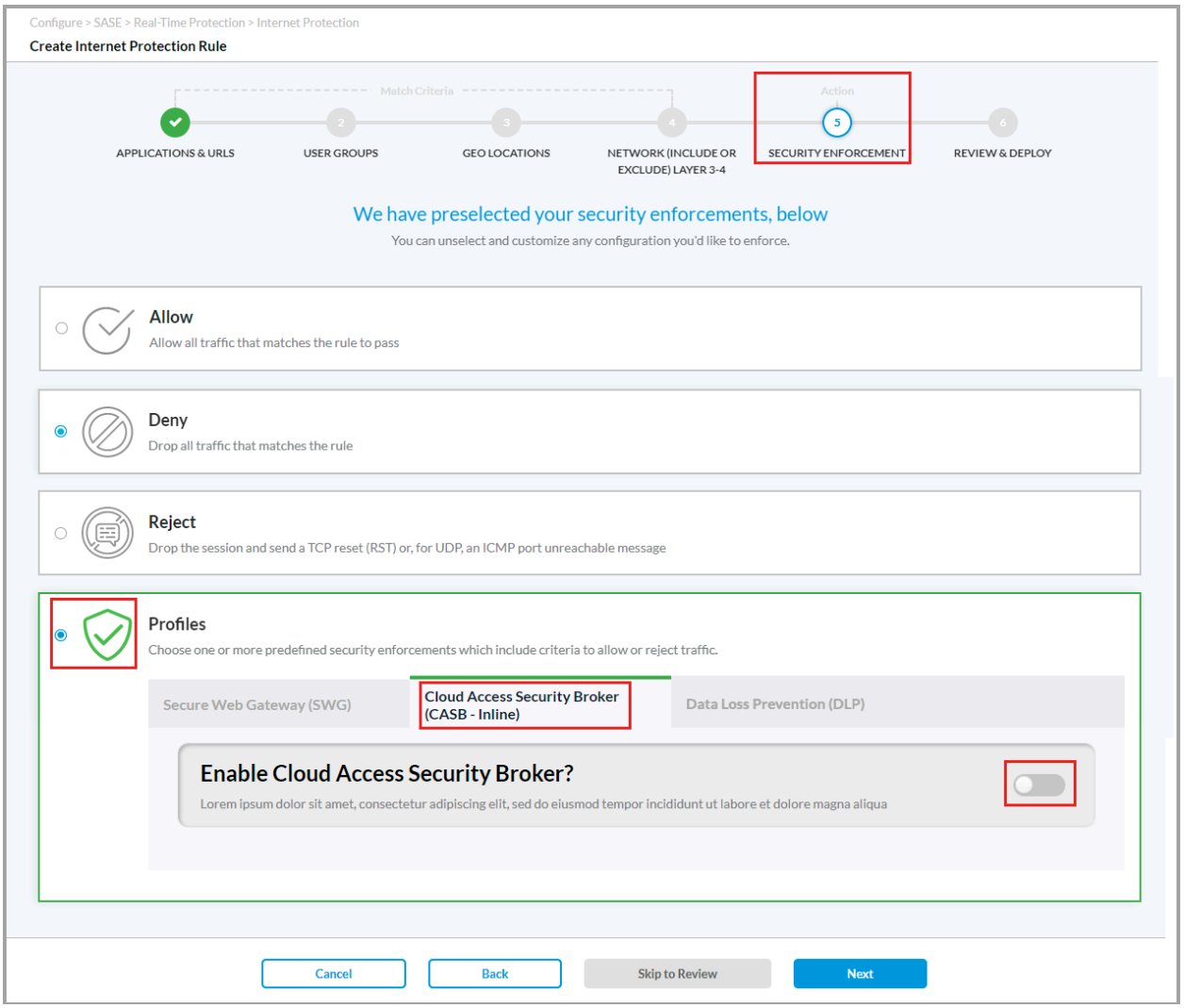
Configure a CASB Profile for Internet Protection Rules

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.

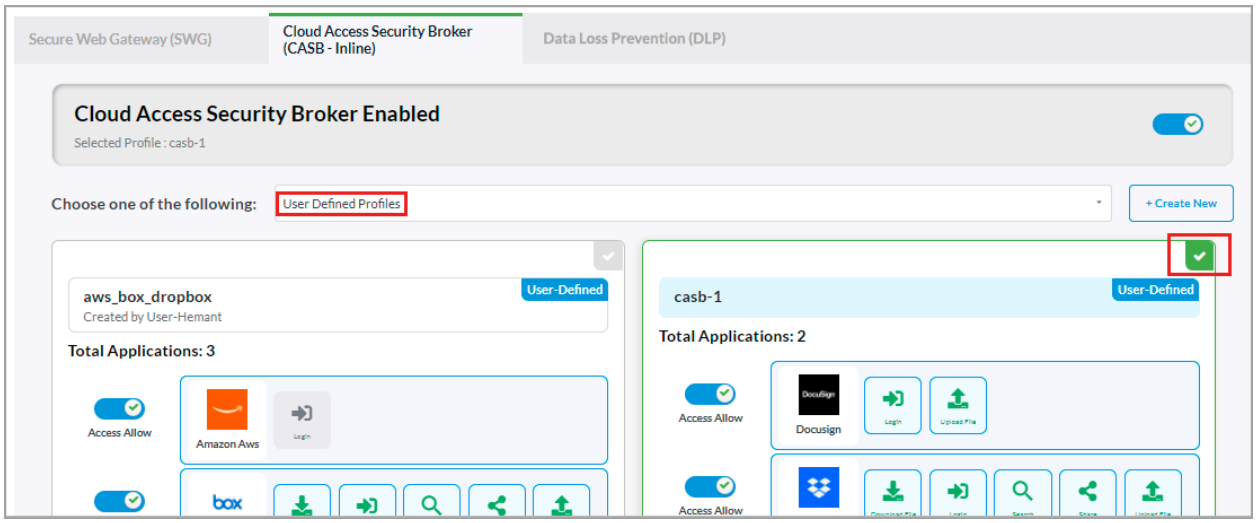
You can associate a CASB profile with a SASE internet protection rule to allow or deny traffic. CASB secures the data flowing between users and cloud applications to comply with corporate and regulatory requirements. For more information, see Configure CASB Profiles.

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.



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



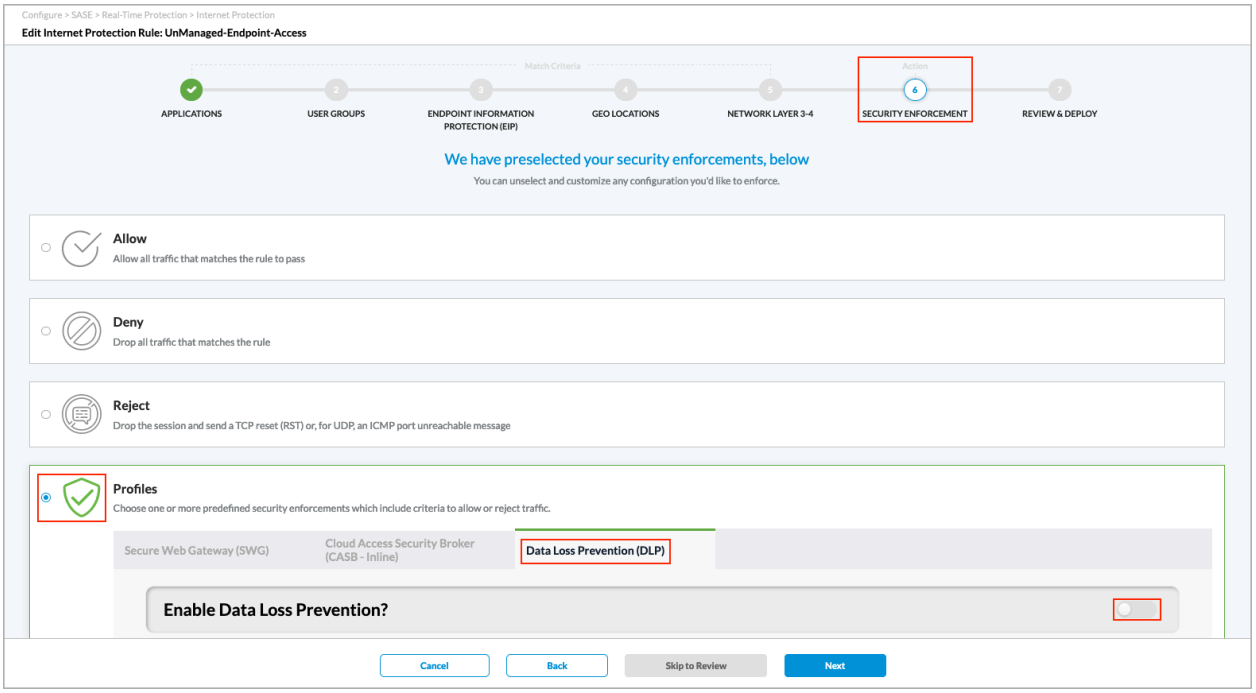
3. To add a CASB profile, click Create New. The Create Cloud Access Security Broker Profile screen displays. For more information, see Configure CASB Profiles.
4. Click Next to go to Step 6, Review and Deploy.

Configure a DLP Profile for Internet Protection Rules

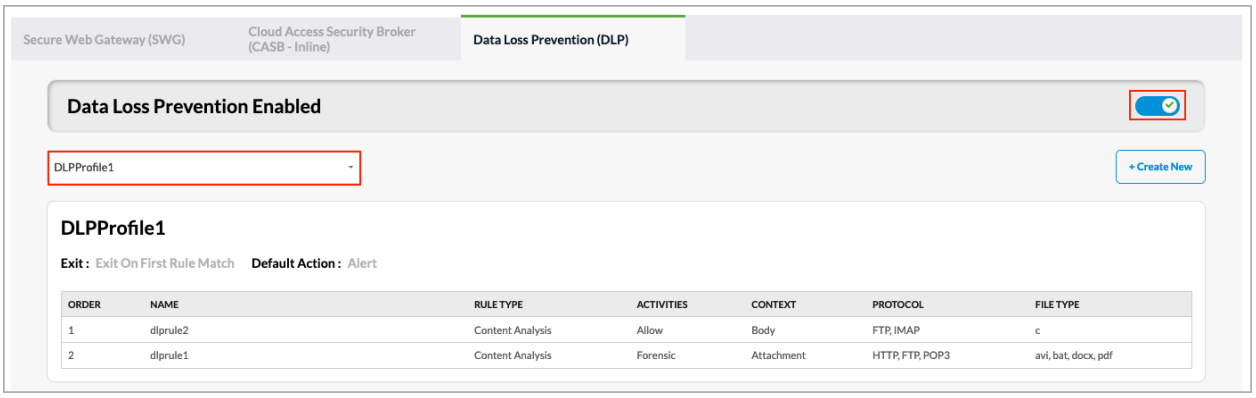
To oversee, track, and report all data transactions in the network and to scan all content that passes through an organization's ports and protocols to ensure data security in the organization you associate a DLP profile with a SASE internet protection rule. DLP provides a set of tools and processes 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.



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



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

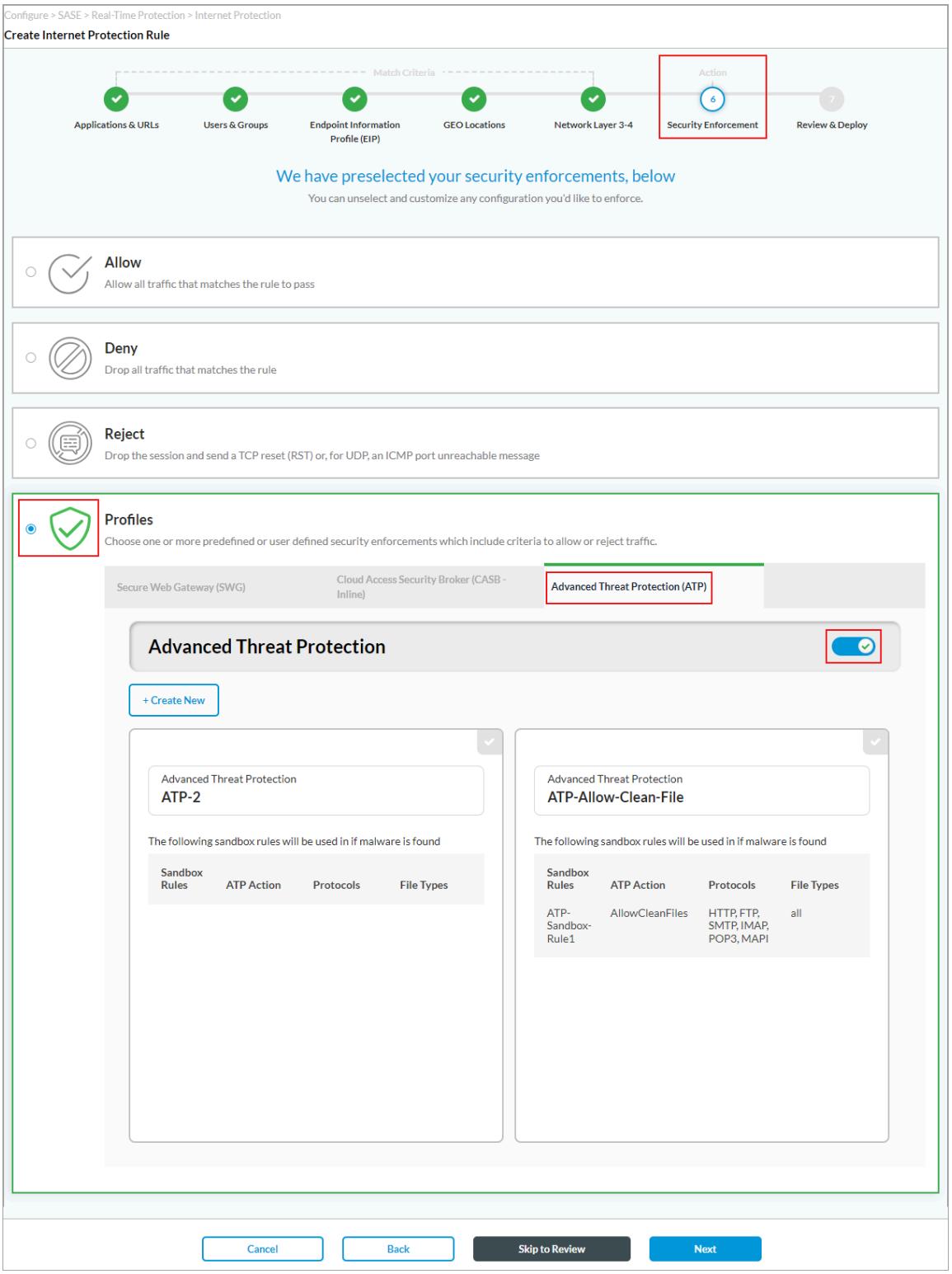
Configure an ATP Profile for Internet Protection Rules

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.



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,

see Configure ATP Profiles.

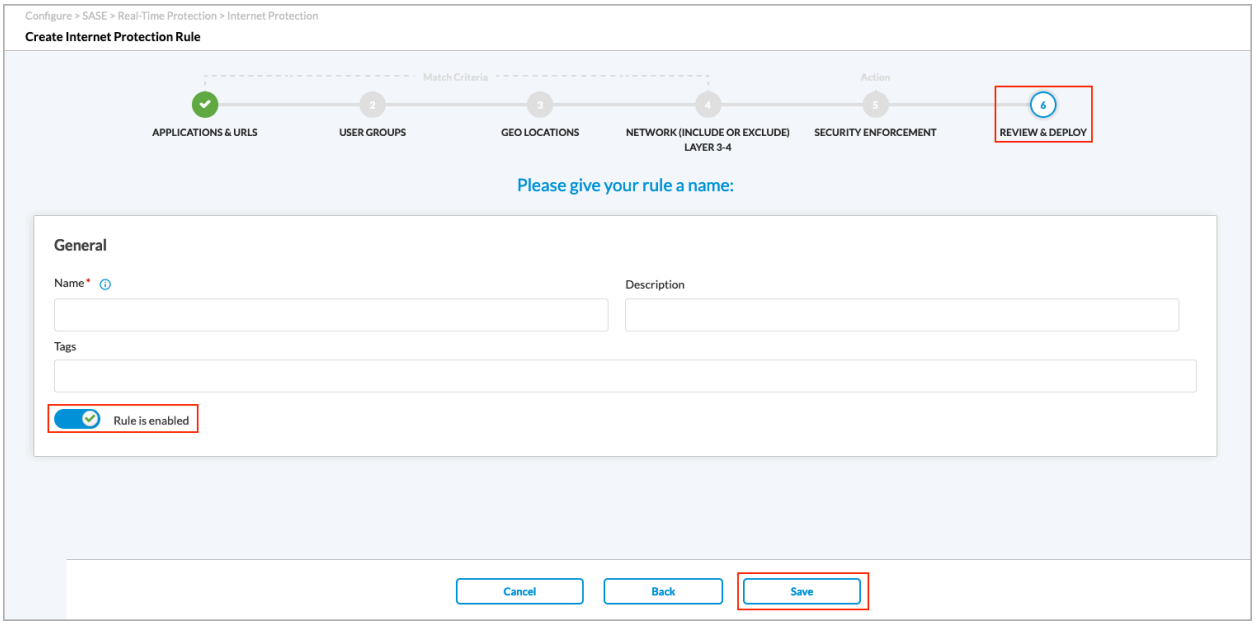
4. Click Next to review and then deploy the internet protection rule.

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	Click the slide bar to enable the rule:  Click the slide bar again to disable the rule: 

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

Configure SASE Private Application Protection Rules
Configure SASE Secure Client Access Rules