
Configure Custom IP-Filtering Profiles

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

Traffic passing through the network may have IP addresses that are associated with a bad reputation and that may cause security risk to your network. To block these IP addresses based on IP address reputation and IP address metadata such as geolocation, you can configure IP address–filtering profiles and then associate them with security policy. You associate IP-filtering profiles with devices that are connected to a Secure Web Gateway (SWG) and that need to send traffic to the internet.

Versa Operating System™ (VOS™) devices provide predefined IP reputations that you can use to create IP address filtering profiles.

You can filter and control traffic based on IP address in the following ways:

- Security access policy enforcement based on address objects with fully qualified domain names (FQDNs)—You can define address objects based on the FQDN by specifying source and destination IP address objects in the match criteria in a security policy rule. The VOS device queries the DNS server for the domain names and caches the resolved IP addresses. When the VOS device processes traffic, the IP address matching is done using the cached resolved IP addresses. This type of filtering minimizes latency associated with real-time DNS lookups, thus improving performance.
- Security access policy enforcement based on address objects with dynamic addresses—You can define an address object based on dynamic addresses by specifying a dynamic source and destination IP address object in the match criteria in a security policy rule. The VOS device does not perform any operations on its own to resolve the dynamic address objects to IP addresses. Instead, the VOS device depends on an external mechanism that pushes the most accurate IP address list that corresponds to the dynamic object to the VOS device. This external mechanism makes a REST API call to the Director node, which then pushes the updates to the VOS device. When a VOS device is processing traffic, it matches IP addresses using the translated IP addresses that are part of the dynamic address object. This type of filtering minimizes latency associated with real-time DNS lookups, thus improving performance.
- IP filtering based on the reputation associated with an IP address and its geolocation—You can filter traffic based on IP reputation and IP address metadata (that is, geolocation). Versa Networks provides an IP reputation feed that is updated both daily and in real time. Additionally, you can populate an IP-filtering profile with IP address blacklists or whitelists by using a custom script or an automated script that invokes REST APIs on the Director node.

IP address filters are based on the following IP address attributes:

- IP reputation—You can create an IP-filtering profile using the following predefined IP reputations:
 - BotNets
 - Denial of service
 - Phishing

- Proxy
- Reputation
- Scanners
- Spam sources
- Web attacks
- Windows exploits
- Geolocation—Versa Networks provides a list of predefined regions that you can use to create IP-filtering profiles based on geolocation.

You define IP-filtering profiles to filter traffic based on the IP address attributes. Each IP-filtering profile object consists of the following:

- Allowed IP addresses
- Denied IP addresses
- DNS reverse lookup configurations
- Rules for geolocation-based actions
- Rules for IP reputation-based actions

You can match the IP address based on the following match criteria:

- Destination IP address
- Source IP address
- Source or destination IP address
- Source and destination IP address

You can enforce the following actions when a session's IP address matches the conditions in the IP-filtering profile:

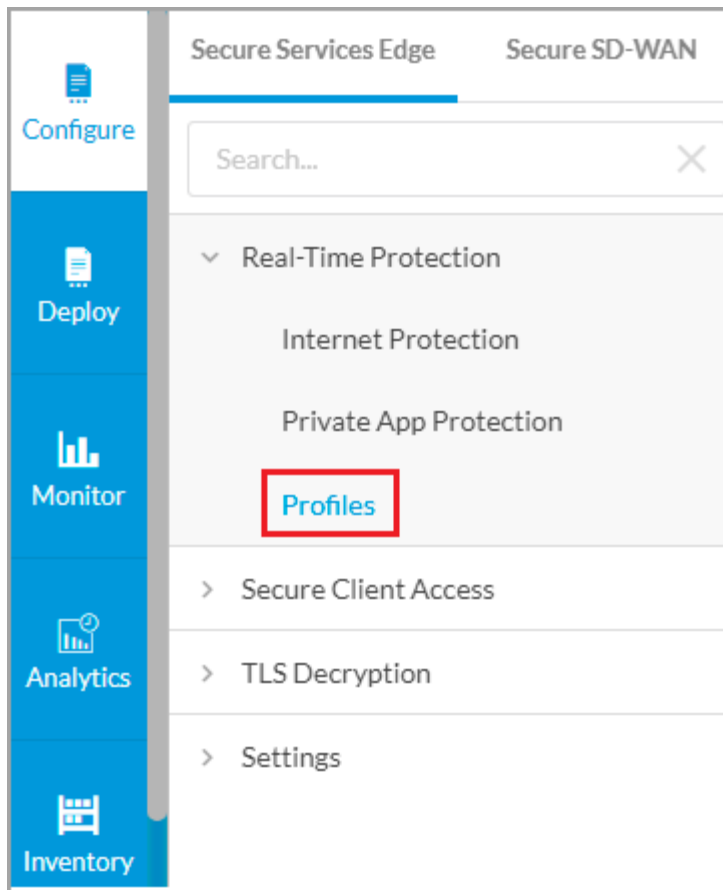
- Allow
- Alert
- Drop packet
- Drop session
- Reset

You can also configure custom actions in an IP-filtering file.

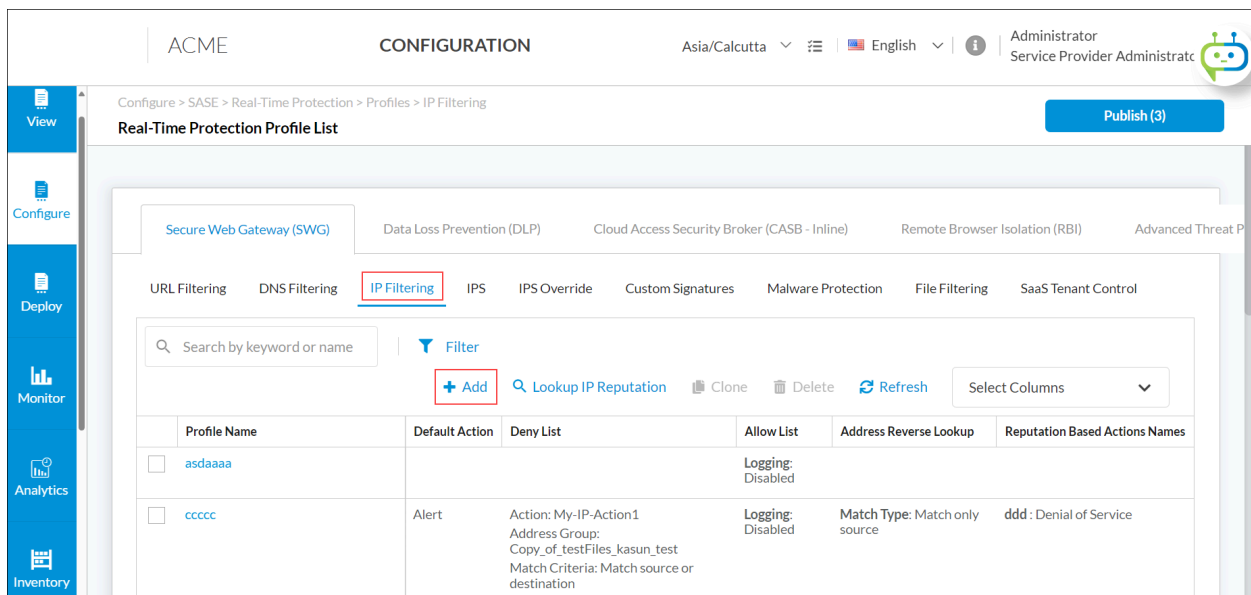
This article describes how to configure custom IP-filtering profiles and how to view IP reputation categories.

Configure Custom IP-Filtering Profiles

1. Go to Configure > Secure Services Edge > Real-Time Protection > Profiles.



The following screen displays:



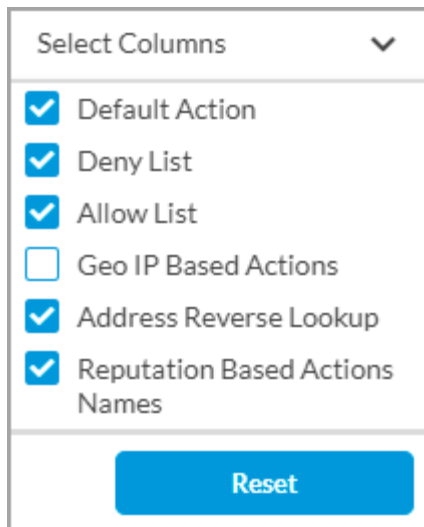
2. Select the IP Filtering tab.
3. To customize which columns display, click Select Columns and then click the columns to select or deselect the

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

Updated: Wed, 23 Oct 2024 08:35:45 GMT

Copyright © 2024, Versa Networks, Inc.

ones you want to display. Click Reset to return to the default column display settings.



Select Columns ▼

- ☒ Default Action
- ☒ Deny List
- ☒ Allow List
- ☐ Geo IP Based Actions
- ☒ Address Reverse Lookup
- ☒ Reputation Based Actions Names

Reset

4. Click + Add to create a profile. The Create IP Filtering screen displays, and the Deny and Allow List step is selected. By default, all fields are configured. To customize IP-filtering actions, enter information for the following fields. Note that if the traffic matches both a deny list and an allow list, the action in the deny list takes precedence.

Configure > SASE > Real-Time Protection > Profiles > IP Filtering

Create IP Filtering Profile

1

2

3

4

5

6

DENY & ALLOW LISTGEO IP BASED ACTIONSREPUTATION BASED ACTIONSADDRESS REVERSE LOOKUPDEFAULT ACTIONREVIEW & SUBMIT

By default, all fields have been configured. Otherwise, you can choose which Deny list and Allow list actions to enforce for your IP filtering.

If traffic is matched in both the Deny list (black list) and Allow list (white list), then the action in the Deny list takes precedence.

Deny List

Choose which domains and actions to deny (blacklist).

Action

Alert

Address Group

Select 1 or more Address Groups

IPv4/IPv6 Subnet

Enter a list of IP Subnet values

IP Range

Enter a list of IP Range values

IP WildCard

Enter a list of wildcard values

Specify the match criteria for the IP address.

Match only source

Match only destination

Match source or destination

Match source and destination

Allow List

Choose which domains to allow (whitelist).

Address Group

Select 1 or more Address Groups

IPv4/IPv6 Subnet

Enter a list of IP Subnet values

IP Range

Enter a list of IP Range values

IP WildCard

Enter a list of wildcard values

Specify the match criteria for the IP address.

Match only source

Match only destination

Match source or destination

Match source and destination

Cancel

Back

Skip to Review

Next

Field	Description
Deny List (Group of Fields)	Choose the IP addresses and groups to deny (block).
<ul style="list-style-type: none"> Action 	<p>Select the action to enforce when the IP-filtering profile encounters an IP address that is configured in a deny-listed IP address or IP address group:</p> <ul style="list-style-type: none"> Alert—Allow the IP address, and generate an entry in the IP-filtering log. Allow—Allow the IP address, and do not generate an entry in the IP-filtering log. Drop Packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website. Drop Session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website. Reject—Send an ICMP unreachable message back to the client and resets the connection to the server.
<ul style="list-style-type: none"> Address Group 	Select the IP address groups for which to enforce the action. For more information about adding address group objects, see Configure Address Objects .
<ul style="list-style-type: none"> IPv4/IPv6 Subnet 	Enter a list of IPv4 or IPv6 subnets.
<ul style="list-style-type: none"> IP Range 	Enter a list of IP address ranges.
<ul style="list-style-type: none"> IP Wildcard 	Enter a list of IP address wildcard values.
<ul style="list-style-type: none"> Specify the Match Criteria for IP Address 	<p>Select the match criteria for the IP address:</p> <ul style="list-style-type: none"> Match only source IP address. Match only destination IP address. Match source or destination IP address.

Field	Description
	<ul style="list-style-type: none"> Match source and destination IP address.
Allow List (Group of Fields)	Choose the IP addresses and groups to allow.
<ul style="list-style-type: none"> Address Group 	Select the IP address groups for which to enforce the action. For more information about adding address group objects, see Configure Address Objects .
<ul style="list-style-type: none"> IPv4/IPv6 Subnet 	Enter a list of IPv4 or IPv6 subnet values.
<ul style="list-style-type: none"> IP Range 	Enter a list of IP address range values.
<ul style="list-style-type: none"> IP Wildcard 	Enter a list of IP address wildcard values.
<ul style="list-style-type: none"> Specify the Match Criteria for IP Address 	Select the match criteria for the IP address: <ul style="list-style-type: none"> Match only source IP address. Match only destination IP address. Match source or destination IP address. Match source and destination IP address.

5. Click Next to go to the Geo IP-Based Actions screen, to add actions for geographic reputation-based IP filtering.

Configure > SASE > Real-Time Protection > Profiles > IP Filtering

Create IP Filtering Profile

1 **2** 3 4 5 6

DENY & ALLOW LIST **GEO IP BASED ACTIONS** REPUTATION BASED ACTIONS ADDRESS REVERSE LOOKUP DEFAULT ACTION REVIEW & SUBMIT

By default, all locations have been selected. Otherwise, you can choose which locations to enforce for your IP filtering.

+ Add Delete Select Columns

NAME	ACTION	MATCH TYPE	REGIONS
No Data			

Cancel Back Skip to Review **Next**

6. Click the **+** Add icon, and in the Add Location popup window, enter information for the following fields.

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

Updated: Wed, 23 Oct 2024 08:35:45 GMT

Copyright © 2024, Versa Networks, Inc.

Add Location

Choose which action and configurations to apply for your location.

Location Name

Action

Alert

Specify the match criteria for the IP address.

Match only source

Match only destination

Match source or destination

Match source and destination

Select one or more geographical regions.

Google

Keyboard shortcuts | Imprints ©2022 Google, INEGI | Terms of Use | Map data ©2022 Google, INEGI

Select Country

Cancel

Add

Field	Description
Location Name	Select the name of the geographic reputation-based IP-filtering profile.
Action	<p>Select the action to enforce when the IP-filtering profile encounters an IP address or IP address group that has an unacceptable geographic reputation:</p> <ul style="list-style-type: none"> ◦ Alert—Allow the IP address, and generate an entry in the IP-filtering log. ◦ Allow—Allow the IP address, and do not generate an entry in the IP-filtering log. ◦ Drop Packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website. ◦ Drop Session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website. ◦ Reject—Send an ICMP unreachable message back to the client and resets the connection to the server.
Specify the Match Criteria for IP Address	<p>Select the match criteria for the IP address:</p> <ul style="list-style-type: none"> ◦ Match only source IP address. ◦ Match only destination IP address. ◦ Match source or destination IP address. ◦ Match source and destination IP address.
Select Country	Select one or more countries to specify the geographic region.

7. Click Add.
8. Click Next to go to the Reputation-Based Actions screen.

Configure > SASE > Real-Time Protection > Profiles > IP Filtering

Create IP Filtering Profile

1 DENY & ALLOW LIST
 2 GEO IP BASED ACTIONS
 3 REPUTATION BASED ACTIONS
 4 ADDRESS REVERSE LOOKUP
 5 DEFAULT ACTION
 6 REVIEW & SUBMIT

By default, all fields have been configured. Otherwise, you can choose which reputations to enforce for your IP filtering.

+ Add + Reorder 🗑 Delete Select Columns

NAME	ACTION	MATCH TYPE	REPUTATIONS
No Data			

Cancel Back Skip to Review Next

- Click the + Add icon, and in the Add Reputation popup window, enter information for the following fields.

Add Reputation
✕

Choose which action and configurations to apply for your reputation.

Reputation Name

Action

Alert

Specify the match criteria for the IP address.

Match only source
Match only destination
Match source or destination
Match source and destination

Select one or more reputations.

BotNets

Denial of Service

Network

Phishing

Proxy

Reputation

Scanners

Spam Sources

Web Attacks

Windows Exploits

Cancel Add

Field	Description
Reputation Name (Required)	Enter a name for the IP reputation-based IP-filtering profile.
Action	<p>Select the action to enforce when the IP-filtering profile encounters an IP address with an unacceptable reputation:</p> <ul style="list-style-type: none"> Alert—Allow the IP address, and generate an entry in the IP-filtering log. Allow—Allow the IP address, and do not generate an entry in the IP-filtering log. Drop Packet—The browser waits for a response from the server and then determines whether the packet was dropped because of a delayed response or because of blocked access to the website. Drop Session—The browser waits for a response from the server and then determines whether the session was dropped because of a delayed response or because of blocked access to the website. Reject—Send an ICMP unreachable message back to the client and reset the connection.
Specify the Match Criteria for IP Address	<p>Select the match criteria for the IP address:</p> <ul style="list-style-type: none"> Match only source IP address. Match only destination IP address. Match source or destination IP address. Match source and destination IP address.
Select one or more reputations	<p>Select one or more reputations:</p> <ul style="list-style-type: none"> Botnets Denial of service Phishing Proxy Reputation Scanners Spam sources Web attacks Windows exploits

10. Click Add.

11. Click Next to go to the Address Reverse Lookup screen, to configure address reverse lookup, which performs a reverse lookup of an IP tuple (source IP address and destination IP address) and can then apply a URL-filtering profile on the reverse lookup domain. You can use this in conjunction with host reputation-based actions for non-HTTP or non-HTTPS traffic (for example, FTP traffic). Enter information for the following fields.

Configure > SASE > Real-Time Protection > Profiles > IP Filtering

Create IP Filtering Profile

1 DENY & ALLOW LIST 2 GEO IP BASED ACTIONS 3 REPUTATION BASED ACTIONS 4 ADDRESS REVERSE LOOKUP 5 DEFAULT ACTION 6 REVIEW & SUBMIT

By default, all fields have been configured. Otherwise, you can choose which address reverse lookup to enforce for your IP filtering.

Configure an address reverse lookup, which performs a reverse lookup of an IP tuple (source IP address and destination IP address).
Select the address type to perform a reverse lookup.

Match only source ☒ Match only destination ☒ Match source and destination ☒

Select the URL filtering profile to associate with the IP address reverse lookup.

URL Filtering Profile
Search for URL Filtering

Cancel Back Skip to Review Next

Field	Description
Specify the address type to perform reverse lookup	<p>Select the address type on which to perform a reverse lookup:</p> <ul style="list-style-type: none"> Match only source IP address. Match only destination IP address. Match source and destination IP address.
URL Filtering Profile	<p>Select the URL-filtering profile to associate with IP address reverse lookup. For more information, see Configure Custom URL-Filtering Profiles.</p>

- Click Next to go to the Default Action screen, to select the default action to perform when there are no matching criteria.

Configure > SASE > Real-Time Protection > Profiles > IP Filtering

Create IP Filtering Profile

1

2

3

4

5

6

DENY & ALLOW LISTGEO IP BASED ACTIONSREPUTATION BASED ACTIONSADDRESS REVERSE LOOKUPDEFAULT ACTIONREVIEW & SUBMIT

By default, we will allow all files that do not match any criteria specified. Otherwise, you can choose which default action to enforce if there are no criteria matched.

Specify the default action to enforce if there are no criteria matched.

Action

Alert

☐ Enable Logging ⓘ

☐ Prioritize URL Reputation

Cancel

Back

Skip to Review

Next

Field	Description
Specify the the default action to enforce if there are no criteria matched	<p>Select the default action to perform when there are no matching criteria:</p> <ul style="list-style-type: none"> ◦ Alert—Allow the IP address, and generate an entry in the IP-filtering log. ◦ Allow—Allow the IP address, and do not generate an entry in the IP-filtering log. ◦ Drop Packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website. ◦ Drop Session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website. ◦ Reject—Send an ICMP unreachable message back to the client and resets the connection to the server.
Enable Logging	Click to log IP-filtering actions.
Prioritize URL Reputation	Click to prioritize the URL reputation over the IP reputation. Instead of blocking the traffic in IP filtering based on reputation, traffic is further evaluated with URL filtering. URL reputation correlates with an actual website. When you configure an IP-filtering profile that blocks traffic based on IP reputation, some legitimate websites may be blocked. When the URL reputation meets the threshold you select in the URL Reputation Priority field, prioritizing URL reputation overrides the IP Reputation Action.
URL Reputation Priority	<p>When you use Prioritize URL Reputation, select the priority to assign to the URL reputation when traffic is evaluated:</p> <ul style="list-style-type: none"> ◦ High risk (Priority 4) ◦ Moderate risk (Priority 3) ◦ Low risk (Priority 2) ◦ Suspicious (Priority 1)

- Trustworthy (Priority 0)—Ignore a website that is labeled as one with a bad reputation, or ignore an HTTP/SSL URL reputation check that indicates a bad IP reputation.

13. Click Next to go to the Review and Submit screen.

14. In the General section, enter a name for the IP-filtering profile and, optionally, a description and tags.

15. For all other sections, review the information. If you need to make changes, click the Edit icon.

16. Click Save.


To delete an IP-filtering profile, select the profile in the IP Filtering tab and click the  Delete icon.

Display IP Reputations

For Releases 12.1.1 and later.

You can look up the reputation for an IP address in the database of predefined IP reputations, and you can display information about the IP address, such as its geographic location.

To display information about IP reputations:

1. Go to Configure > Real-Time Protection > Profiles > Secure Web Gateway (SWG) > IP Filtering.
2. Click  Lookup IP Reputation.

View

Configure

Deploy

Monitor

Analytics

Inventory

ACME

CONFIGURATION

Asia/Calcutta | English | Administrator | Service Provider Administrator

Configure > SASE > Real-Time Protection > Profiles > IP Filtering

Real-Time Protection Profile List

Publish (3)

Secure Web Gateway (SWG) | Data Loss Prevention (DLP) | Cloud Access Security Broker (CASB - Inline) | Remote Browser Isolation (RBI) | Advanced Threat Protection

URL Filtering | DNS Filtering | **IP Filtering** | IPS | IPS Override | Custom Signatures | Malware Protection | File Filtering | SaaS Tenant Control

Search by keyword or name

Filter

+ Add

Lookup IP Reputation

Clone

Delete

Refresh

Select Columns

	Profile Name	Default Action	Deny List	Allow List	Address Reverse Lookup	Reputation Based Actions Names
<input type="checkbox"/>	asdaaaa			Logging: Disabled		
<input type="checkbox"/>	cccc	Alert	Action: My-IP-Action1 Address Group: Copy_of_testFiles_kasun_test Match Criteria: Match source or destination	Logging: Disabled	Match Type: Match only source	ddd : Denial of Service

Lookup IP Reputation and Geo Location

Gateway Name

USA-East-GW-1

IP

10.48.80.15

Test

Reputation

IP Address:

Geo Location

IP Address:

Cancel

Field	Description
Gateway Name	Select the organization for which you want to look up the IP address reputation.
IP	Enter the IP address for which you want to look up the reputation.

- Click Test. The IP Reputation and Geo Location popup window displays information about the IP address, including its reputation and geographic location. For example:

Lookup IP Reputation and Geo Location
✕

Gateway Name

USA-East-GW-1

IP

Test

Reputation
IP Address: 10.48.80.15
Status: Success
Result: Private address

Geo Location
IP Address: 10.48.80.15
Status: Success
Result: Private address

Cancel

- Click Cancel.

Supported Software Information

Releases 11.2.1 and later support all content described in this article, except:

- Release 12.1.1 adds support for looking up the reputation and geographic location of an IP address.

Additional Information

[Configure Custom URL-Filtering Profiles](#)

[Configure SASE Internet Protection Rules](#)

[Configure SASE User-Defined Objects](#)