
Configure SD-WAN IP-Filtering Policies

 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 policies and then associate them with security policies. You associate IP-filtering policies with basic and standard master profiles.

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

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 address objects 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 corresponding 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 the 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 policy with IP address deny lists (also called blacklists) or allow lists (also called 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 IP filter policies using the following predefined IP reputations:
 - BotNets
 - Cloud providers

- Denial of service
- Mobile threats
- Network
- Phishing
- Proxy
- Reputation
- Scanners
- Spam sources
- Tor proxy
- Web attacks
- Windows exploits
- Geolocation—Versa Networks provides a list of predefined regions that you can use to create IP filter policies based on geolocation.

You define IP-filtering policies to filter traffic based on the IP address attributes. Each IP-filtering policy consists of the following:

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

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

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

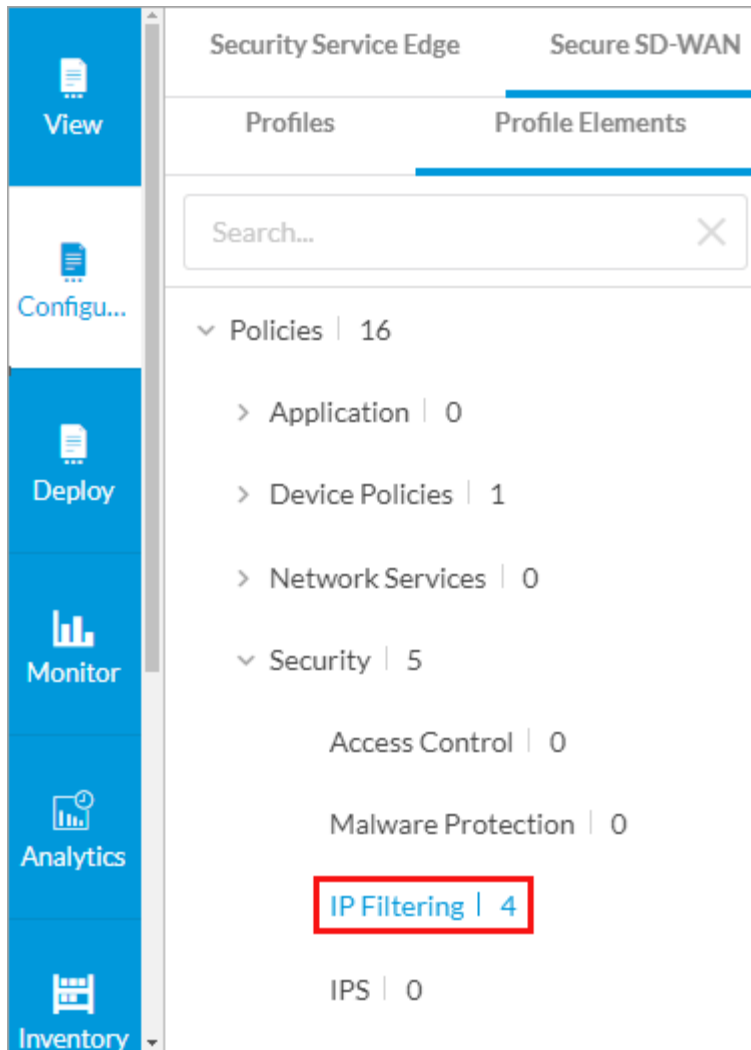
You can enforce the following actions when a session's IP address matches the conditions in the IP-filtering policy:

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

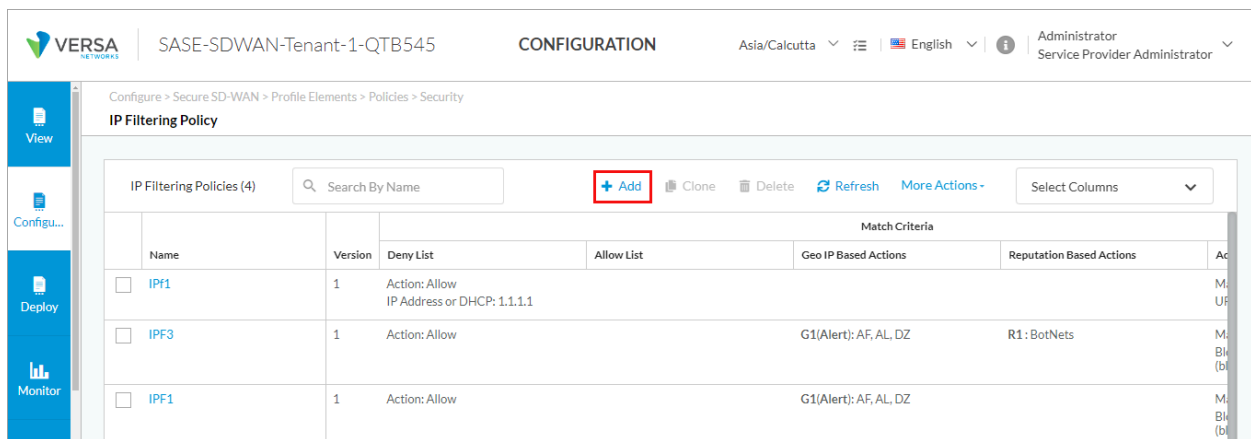
You can also configure custom actions in an IP-filtering file.

To configure IP-filtering policies:

1. Go to Configure > Secure SD-WAN > Profile Elements > Policies > Security > IP Filtering.



The following screen displays.



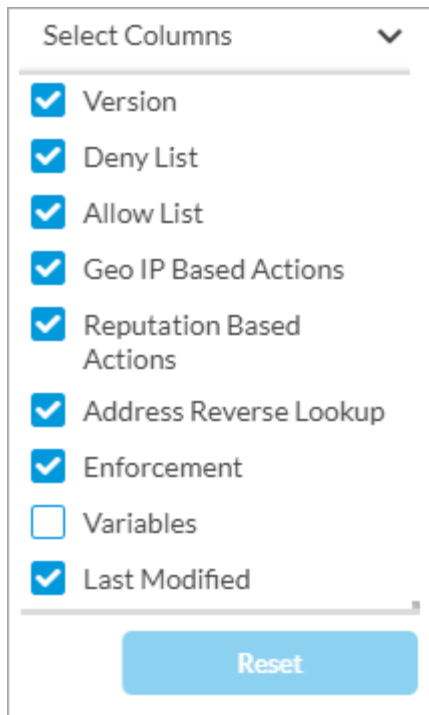
- To customize which columns to display, click Select Columns and then click the columns to select or deselect the

https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...

Updated: Wed, 23 Oct 2024 08:02:52 GMT

Copyright © 2024, Versa Networks, Inc.

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



Select Columns

- ☒ Version
- ☒ Deny List
- ☒ Allow List
- ☒ Geo IP Based Actions
- ☒ Reputation Based Actions
- ☒ Address Reverse Lookup
- ☒ Enforcement
- ☐ Variables
- ☒ Last Modified

Reset

3. Click + Add to create a policy. The Add IP Filtering Policy screen displays.
4. By default, all fields are configured. To customize IP-filtering actions, in Step 1, Deny and Allow List, 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.

Add IP Filtering Policy

1
2
3
4
5
6
7

Deny & Allow List
GEO IP Based Actions
Reputation Based Actions
Address Reverse Lookup
Enforcement
Permissions
Review & 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 actions and URLs to deny (blacklist).

Action

-- Select --

☒ Address Group
☐ IP Address

Address Group

Select 1 or more Address Groups

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 URLs to allow (whitelist).

☒ Address Group
☐ IP Address

Address Group

Select 1 or more Address Groups

Specify the match criteria for the IP Address.

Match only source

Match only destination

Match source or destination

Match source and destination

Cancel
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 policy 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

Field	Description
	<p>dropped because of a delayed response from the server or because a firewall blocked access to the website.</p> <ul style="list-style-type: none"> ◦ 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 reset the connection to the server.
◦ 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 .
◦ IPv4/IPv6 Subnet	Enter a list of IPv4 or IPv6 subnets.
◦ IP Range	Enter a list of IP address ranges.
◦ IP Wildcard	Enter a list of IP address wildcard values.
◦ 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
Allow List (Group of Fields)	Choose the IP addresses and groups to allow.
◦ 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 .
◦ IPv4/IPv6 Subnet	Enter a list of IPv4 or IPv6 subnet values.
◦ IP Range	Enter a list of IP address range values.

Field	Description
<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 Step 2, Geo IP-Based Actions, to add actions for geographic reputation-based IP filtering.

Add IP Filtering Policy

Deny & Allow List (1) **GEO IP Based Actions (2)** Reputation Based Actions (3) Address Reverse Lookup (4) Enforcement (5) Permissions (6) Review & Submit (7)

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

Geo Location (0)

+Add Clone 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.

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 up to 32 geographical regions.

+

−



Select Country

Cancel

Add

https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...

Updated: Wed, 23 Oct 2024 08:02:52 GMT

Copyright © 2024, Versa Networks, Inc.

8

Field	Description
Location Name	Select the name of the geographic reputation-based IP-filtering policy.
Action	<p>Select the action to enforce when the IP-filtering policy 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 reset 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 Step 3, Reputation-Based Actions.

Add IP Filtering Policy

Deny & Allow List GEO IP Based Actions **Reputation Based Actions** Address Reverse Lookup Enforcement Permissions Review & Submit

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

Reputations (0) +Add Clone Delete Select Columns

Name	Action	Match Type	Reputations
No Data			

Cancel Back Skip to Review Next

9. 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.

☒ Proxy
 ☒ Reputation
 ☒ Scanners
 ☒ Spam Sources
 ☒ Tor Proxy
 ☒ Web Attacks

☒ Windows Exploits

Cancel Add

Field	Description
Reputation Name (Required)	Enter a name for the IP reputation-based IP-filtering policy.

https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...

Updated: Wed, 23 Oct 2024 08:02:52 GMT

Copyright © 2024, Versa Networks, Inc.

Action	<p>Select the action to enforce when the IP-filtering policy encounters an IP address with 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 blocked access to the website. ◦ Drop Session—The browser waits for a response from the server and drops the session. It then determines whether the session was dropped because of a delayed response or 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 Step 4, Address Reverse Lookup, 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 policy 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.

Add IP Filtering Policy

Progress: 1. Deny & Allow List (✓) 2. GEO IP Based Actions (✓) 3. Reputation Based Actions (✓) 4. Address Reverse Lookup (4) 5. Enforcement (3) 6. Permissions (6) 7. Review & Submit (7)

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).

Specify the match criteria for the IP Address.

☒ 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: -- Select --

Cancel Back Skip to Review Next

Field	Description
Specify the address type to perform reverse lookup	Select the address type on which to perform a reverse lookup: <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	Select the URL-filtering profile to associate with IP address reverse lookup. For more information, see Configure Custom URL-Filtering Profiles .

- Click Next to go to Step 5, Default Action, to select the default action to perform when there are no matching criteria.

Add IP Filtering Policy

1

Deny & Allow List

2

GEO IP Based Actions

3

Reputation Based Actions

4

Address Reverse Lookup

5

Enforcement

6

Permissions

7

Review & 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

-- Select --

☐ 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 reset the connection to the server.
Prioritize URL Reputation	<p>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 policy 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.</p>

- Click Next to go to Step 6, Permissions, to set or update the permission for each role. The roles are Enterprise Administrator, Enterprise Operator, Service Provider Administrator, and Service Provider Operator. The permission for each role is selected by default, and you can update it. The role permissions are Edit, Hide, and Read.

Add IP Filtering Policy

Progress: 1. Deny & Allow List (✓) 2. GEO IP Based Actions (✓) 3. Reputation Based Actions (✓) 4. Address Reverse Lookup (✓) 5. Enforcement (✓) 6. **Permissions** (6) 7. Review & Submit (7)

We have preselected the permissions for the roles, below You can change the permission for each of the roles.

Role	Permissions
Enterprise Administrator (Inherited)	Edit
Service Provider Administrator (Inherited)	Edit
Service Provider Operator (Inherited)	Read
Enterprise Operator (Inherited)	Read

Buttons: Cancel, Back, Skip to Review, Next

14. Click Next to go to Step 7, Review and Submit.

Add IP Filtering Policy

Deny & Allow List GEO IP Based Actions Reputation Based Actions Address Reverse Lookup Enforcement Permissions **Review & Submit**

Review your configurations. Before submitting, review and edit any steps of your configuration below..

General

Name Description

Tags

☐ Logging Disabled

Deny & Allow List [Edit](#)

Deny List

Allow List

GEO IP Based Actions [Edit](#)

Reputation Based Actions [Edit](#)

Address Reverse Lookup [Edit](#)

Address Type Match only source

Enforcement [Edit](#)

Prioritize URL Reputation Disabled

Permissions [Edit](#)

test-EA	Edit
Enterprise Administrator	Edit
Service Provider Administrator	Edit
EA-Parent2	Edit
Eo-parent	Read
Auth_Read	Edit
Service Provider Operator	Read
EA-Parent	Edit
Enterprise Operator	Read

Cancel Back **Save**

- In the General section, enter a name for the IP-filtering policy and, optionally, a description and tags.
- For all other sections, review the information. If you need to make changes, click the Edit icon.
- Click Save.

https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...

Updated: Wed, 23 Oct 2024 08:02:52 GMT

Copyright © 2024, Versa Networks, Inc.

You associate IP-filtering policies with basic or standard master profiles. For more information, see [Configure Profiles](#).

Supported Software Information

Releases 12.1.1 and later support all content described in this article.

Additional Information

[Configure Custom URL-Filtering Profiles](#)

[Configure SASE Internet Protection Rules](#)

[Configure SASE User-Defined Objects](#)