

---

## Configure IP Filtering



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 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.

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 deny lists or allow lists (sometimes called blacklists and 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-filtering profiles with 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 can specify the following:

- Allow lists for IP addresses
- Deny lists for 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 and destination IP address
- Source or destination IP address

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

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

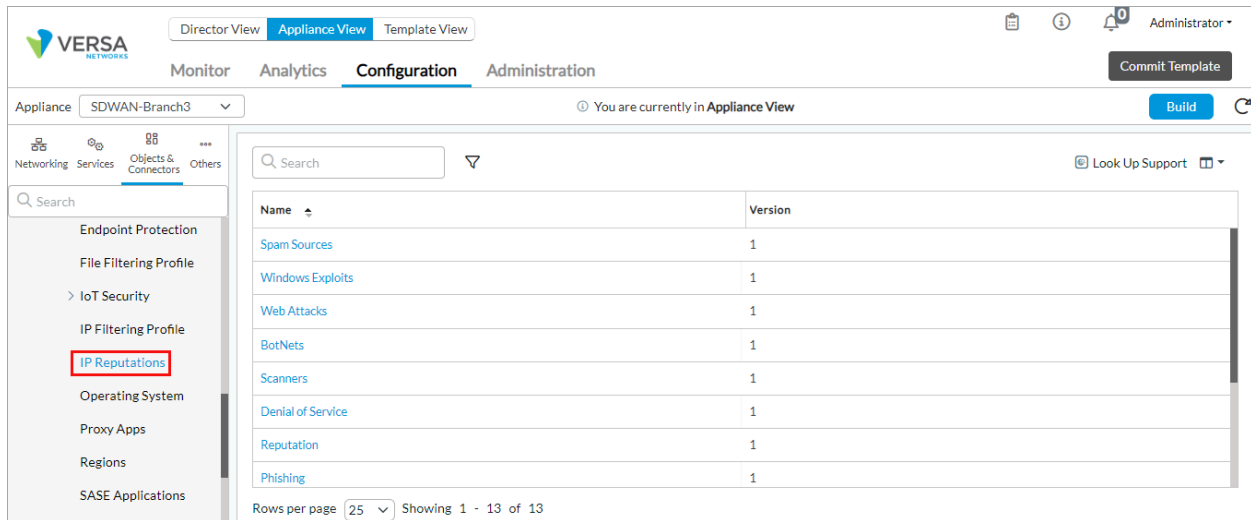
You can also configure custom actions in an IP-filtering profile.

---

## View Predefined IP Reputations

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.

3. Select Objects and Connectors > Objects > Predefined > IP Reputations to view the list of predefined reputations. The following table describes the predefined IP reputations.




The screenshot shows the Versa Networks configuration interface. The top navigation bar includes 'Director View', 'Appliance View' (selected), and 'Template View'. Below this, there are tabs for 'Monitor', 'Analytics', 'Configuration' (selected), and 'Administration'. The 'Appliance' dropdown is set to 'SDWAN-Branch3'. The left sidebar shows a navigation menu with 'IP Reputations' highlighted. The main area displays a table of predefined IP reputations.

Name	Version
Spam Sources	1
Windows Exploits	1
Web Attacks	1
BotNets	1
Scanners	1
Denial of Service	1
Reputation	1
Phishing	1

Rows per page: 25 Showing 1 - 13 of 13

IP Reputation	Description
Botnets	Networks of private computers infected with malicious software and controlled as a group without the owner's knowledge. This category includes botnet command-and-control (C&C) software and infected zombie machines controlled by the bot's originator (the bot master).
Denial of Service	Type of cyberattack in which a device is flooded so that it cannot perform its normal operations. This category includes DoS, distributed denial of service (DDoS), anomalous syn flood attacks, and anomalous traffic detection.
Network	This IP reputation is deprecated and is visible only for backward compatibility.
Phishing	Fraudulent practice of sending emails purporting to be from reputable companies to induce people to reveal personal information, such as passwords and credit card numbers. This category includes IP addresses that hosting phishing sites and other kinds of fraud activities such as click fraud and gaming fraud.
Proxy	IP addresses that provide proxy services.
Reputation	Deny access from IP addresses known to be infected with malware. This category also includes IP addresses that have low webroot reputation index scores. This category prevents access from sources that have been identified as malware distribution points.
Scanners	All reconnaissance such as probes, host scanning, domain scanning, and password brute-force attacks.
Spam Sources	Tunneling spam messages through a proxy, anomalous SMTP activities, and forum spam activities.
Web Attacks	Cross-site scripting, iFrame injection, SQL injection, cross-domain injection, and domain password brute-force attacks.
Windows Exploits	Active IP addresses that offer or distribute malware, shell code, rootkits, worms, and viruses.

4. To display the reputation of an IP address, click the  Look Up Support icon. In the Look Up URL popup window, enter information for the following fields.

Look Up Support

Organization \*

Tenant1

IP \*

Test

Cancel

Field	Description
Organization	Select the organization for which you want to look up the IP address.
URL	Enter the IP address whose reputation to look up.

- Click Test. The Look Up Support popup window displays information about the IP address, including its reputation and geographical location. For example:

Look Up Support

Organization \*

Tenant1

IP \*

Test

Reputation

IP Address

Status

Success

Result

Private address

Geo Location

IP Address

Status

Success

Result

Private address

Cancel

6. Click Cancel.

## View Predefined IP-Filtering Profiles

Versa provides a number of predefined IP-filtering profiles. The profile called Versa Recommended Profile includes filtering for destination IP addresses for botnets, DoS, phishing, proxy, reputation, scanners, spam sources, web attacks, and Windows exploits.

To view the predefined IP-filtering profiles:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a device name in the main panel. The view changes to Appliance view.

2. Select the Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Predefined > IP-Filtering Profile to view the list of predefined IP-filtering profiles. The following table describes the predefined IP-filtering profiles.

Name	Actions	Match Type	Profile ID	Reputation Based Action Names
Block bad traffic	reject	source-or-destination	1	Spam Sources, Windows Exploits, Web Attacks
Block bots	reject	source-or-destination	2	BotNets, Scanners, Denial of Service, Reputation
Web protection	reject	source-or-destination	3	Spam Sources, Web Attacks, BotNets, Denial of Service
Block DoS	reject	source-or-destination	4	BotNets, Scanners, Denial of Service, Reputation
Block spam	reject	source-or-destination	5	Spam Sources
Block scanners	reject	source-or-destination	6	Scanners
Block windows exploits	reject	source-or-destination	7	Windows Exploits

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

---

## Configure Custom IP Filters and Profiles

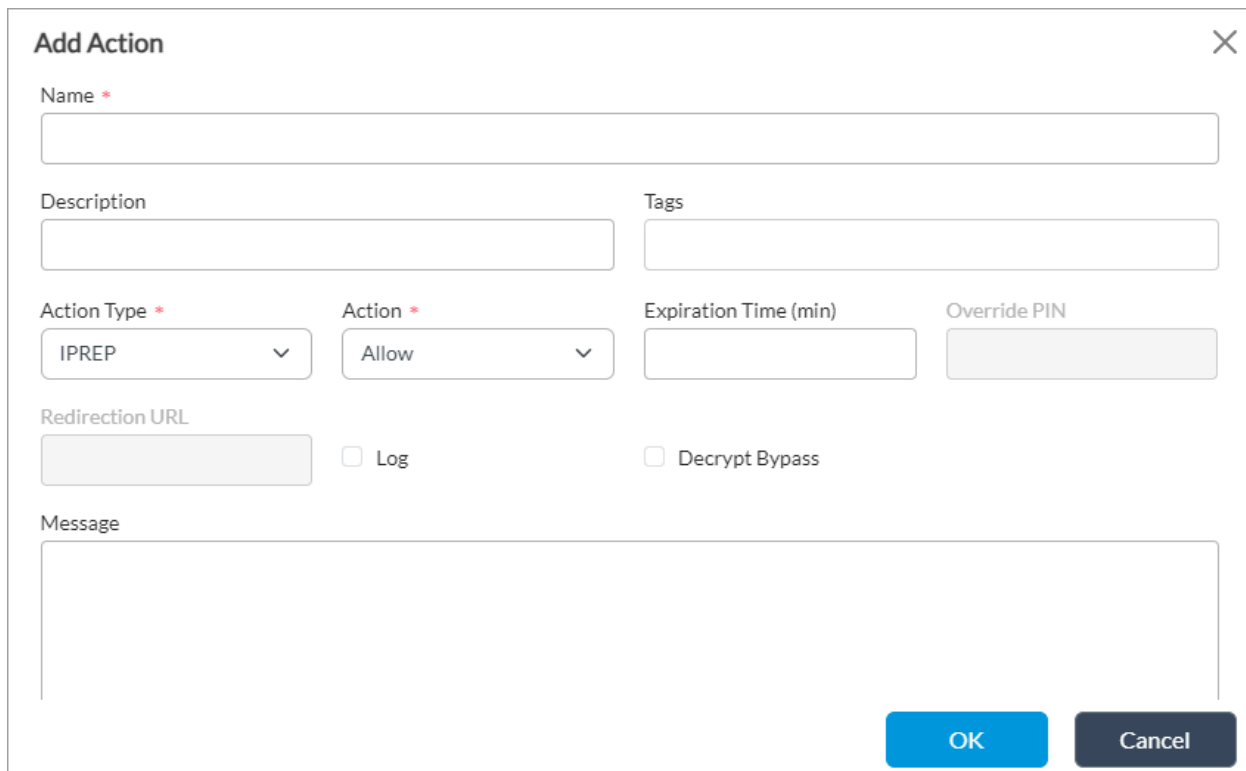
You can configure IP filters with actions that allow you to customize messages on captive portal pages or set an override PIN. You apply the filters when you configure custom IP-filtering profiles.

---

### Configure Custom IP Filters

To configure a custom IP filter, create a captive portal action and then associate it with an IP-filtering profile:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Configuration > Objects & Connectors > Custom Objects > User Defined Actions in the left menu bar.
4. Click the **Add** icon. In the Add Action popup window, enter information for the following fields.



The 'Add Action' popup window contains the following fields and controls:

- Name \***: A text input field.
- Description**: A text input field.
- Tags**: A text input field.
- Action Type \***: A dropdown menu with 'IPREP' selected.
- Action \***: A dropdown menu with 'Allow' selected.
- Expiration Time (min)**: A text input field.
- Override PIN**: A text input field.
- Redirection URL**: A text input field.
- Log**: A checkbox.
- Decrypt Bypass**: A checkbox.
- Message**: A large text area.
- OK** and **Cancel** buttons at the bottom right.



Field	Description
Name	Enter a name for the IP-filtering action. The name is an alphanumeric string and can contain underscores (_) and hyphens (-). It cannot contain spaces or other special characters.
Description	Enter a text description for the IP-filtering action.
Tags	Enter a keyword or phrase that allows you to filter the IP-filtering action. This is useful when you have many actions and want to view those that are tagged with a particular keyword.
Action Type	Select the action to take when the page is redirected: <ul style="list-style-type: none"> <li>◦ All</li> <li>◦ IP reputation (IPREP)</li> </ul>
Action	Select the action to take when a user is redirected to a captive portal: <ul style="list-style-type: none"> <li>◦ Allow—Allow the IP address and do not generate an entry in the IP-filtering log.</li> <li>◦ Ask—The browser presents an information page that prompts the user to either cancel the operation by clicking Cancel or continue with the operation by clicking OK (for HTTP and HTTPS).</li> <li>◦ Block—Block the IP address and generate an entry in the IP-filtering log. No response page is displayed, and the user cannot continue with the website.</li> <li>◦ Custom redirection—The browser redirects the user to the specified URL. Session information such as the URL requested by the user, the IP address of the HTTP/HTTPS request, and URL-filtering profile to process are included in the redirected URL to the web server that hosts the redirected URL page. After the redirection occurs, the external web server, not the VOS device, handles the captive portal functionality. You can customize the session information parameters that are passed to the web server. For more information, see <a href="#">Modify Captive Portal Settings</a>.</li> <li>◦ Drop packet—The browser waits for a response from the server and then drops the packets. It is</li> </ul>

	<p>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.</p> <ul style="list-style-type: none"> <li>◦ 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.</li> <li>◦ Inform—The browser presents an information page that prompts the user to continue after clicking OK (for HTTP and HTTPS).</li> <li>◦ Justify—The browser presents an information page that prompts the user to either cancel the operation by clicking Cancel or continue with the operation after entering a justification message and clicking OK (for HTTP and HTTPS).</li> <li>◦ Override—The browser prompts the user to enter a PIN (4 to 6 digits). This action generates an entry in the URL-filtering log.</li> <li>◦ Reset client—The host responds by sending a TCP Reset packet to the client, and the browser displays an error message indicating that the connection has been reset. It is not possible to determine whether the web server reset the connection or the firewall reset the session.</li> <li>◦ Reset client and server—The host responds by sending a TCP Reset packet to both the client and server, and the browser displays an error message indicating that the connection has been reset. It is not possible to determine whether the web server reset the connection or the firewall reset the session.</li> <li>◦ Reset server—The host responds by sending a TCP Reset packet to the server. The browser waits for a response from the server and then 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.</li> </ul>
Log	<p>Click to log IP-filtering actions. If you do not enable logging, the custom message that you enter in the Message field is not displayed in the Analytics log display.</p>

Expiration Time	<p>Enter how often to redirect a user to the captive portal, in minutes. When a user first enters an IP address and is redirected to a captive portal page, the VOS device creates a cache entry, which expires after a global expiration time. While the cache entry is active, the device does not enforce the captive portal action, and users can view the webpage at the initial URL and at all URLs that belong to the same URL category, without seeing the captive portal page, with one exception. If the captive portal action is Block, all URLs are redirected to the Block page, regardless of the expiration time. For more information about the global expiration time setting, see <a href="#">Modify Captive Portal Settings</a>.</p> <p><i>Range:</i> 1 through 65535 minutes  <i>Default:</i> 30 minutes</p>
Override PIN	For the Override action, enter the PIN value, which is a 4-, 5-, or 6-digit number.
Redirection URL	For the Custom Redirection action, enter the URL to which to redirect the user.
Decrypt Bypass	Click to disable SSL encryption for matching traffic, to allow you to define websites that are not subject to decryption.
Message	Enter a message to display on the captive portal page.

5. Click OK.

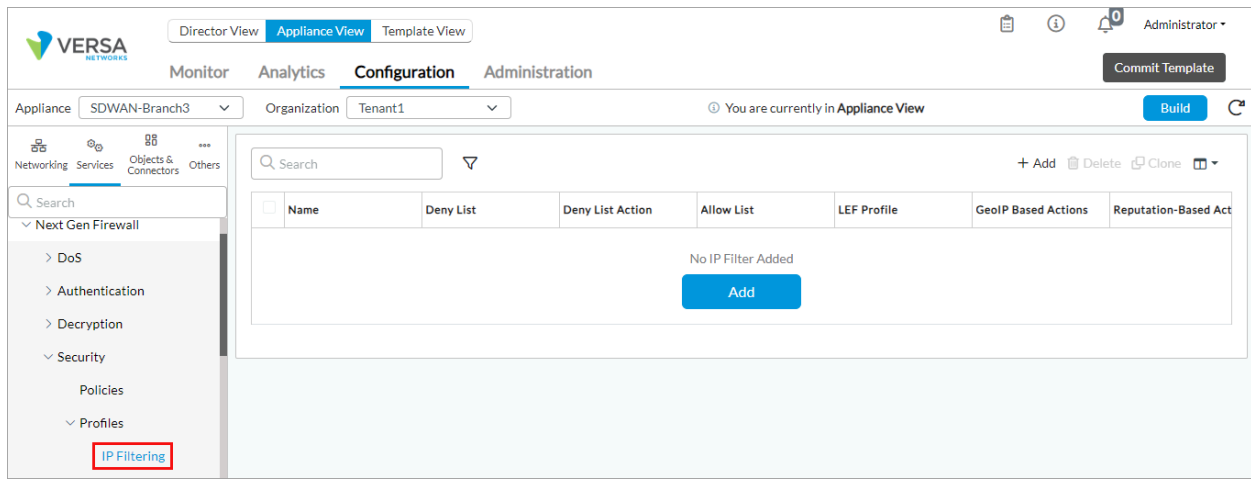
## Configure Custom IP-Filtering Profiles

When the predefined IP-filtering profiles do not meet your needs, you can configure custom profiles.

To configure a custom IP-filtering profile:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Devices > Devices in the horizontal menu bar.
  - c. Select an organization in the left menu bar.

- d. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > Next-Gen Firewall > Security > Profiles > IP Filtering in the left menu bar.



4. Click the + Add icon. In the Add IP Filter popup window, enter information for the following fields.

Add IP Filter
✕

Name \*

Description
Tags

Default Action
--Select--
☒ Prioritize URL Reputation
Allow URL Reputation \*
--Select--

LEF Profile
--Select--
☐ Default Profile

Deny List
Allow List
GeoIP Based Actions
Reputation-Based Actions
Address Reverse Lookup

Deny List Action
--Select--
Match Type
--Select--

☒ IP Address
☐ IP Address Group

☐ IP Address
+ New Address
+

IP Address Not Configured

☐ IP Address Group
+ New Address Group
+

IP Address Group Not Configured


OK
Cancel


Field	Description
Name	<p>Enter a name for the IP-filtering profile.</p> <p><i>Value:</i> Text string from 1 through 255 characters  <i>Default:</i> None</p>
Description	<p>Enter a text description for the IP-filtering profile.</p> <p><i>Value:</i> Text string from 1 through 255 characters  <i>Default:</i> None</p>
Tags	<p>Enter a keyword or phrase to filter the IP-filtering profile name. Tags are useful when you have many profiles and want to view those that are tagged with a particular keyword.</p> <p><i>Value:</i> Text string from 1 through 255 characters.  <i>Default:</i> None</p>
Default Action	<p>Select the default action for this profile. This action is enforced when you do not configure any deny list, allow list, geographic IP-based action, or reputation-based action. The following are the predefined actions:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the IP address, and generate an entry in the IP-filtering log.</li> <li>◦ Allow—Allow the IP address, and do not generate an entry in the IP-filtering log.</li> <li>◦ 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.</li> <li>◦ 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.</li> <li>◦ Reject—Send an ICMP unreachable message</li> </ul>

	<p>back to the client and resets the connection to the server.</p> <p>For custom filters, select an IP-filtering action that you configured in <a href="#">Configure Custom IP Filters</a>, which are displayed under User Defined.</p>
LEF Profile	<p>Select an LEF profile to register IP-filtering logs for this profile. Logs are sent to the active collector of the LEF profile. For information about configuring a LEF profile, see <a href="#">Configure Log Export Functionality</a>. For information about associating a LEF profile with a feature or service, see <a href="#">Apply Log Export Functionality</a>.</p>
Default Profile	<p>Click to use the default LEF profile instead of the LEF profile from the previous field. For information about configuring a default LEF profile, see <a href="#">Configure Log Export Functionality</a>.</p>
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 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 Allow URL Reputation field, prioritizing URL reputation overrides the IP Reputation Action. For prioritizing of the URL reputation to work, for HTTP and HTTPS traffic, ensure that the security policy with which you associate the IP-filtering profile includes a URL-filtering profile for the HTTP/HTTPS traffic. For non-HTTP/HTTPS traffic, enable address reverse lookup, as discussed in Step 13, below.</p>
Allow URL Reputation	<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"> <li>◦ High risk (Priority 4)</li> <li>◦ Moderate risk (Priority 3)</li> <li>◦ Low risk (Priority 2)</li> <li>◦ Suspicious (Priority 1)</li> <li>◦ 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.</li> </ul>

5. Select the Deny List tab, and enter information for the following fields.



Field	Description
Deny List Actions	<p>Select the action to enforce when the IP-filtering profile encounters an IP address that is configured in deny list IP address or IP address group. The following are the predefined actions:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the IP address, and generate an entry in the IP-filtering log.</li> <li>◦ Allow—Allow the IP address, and do not generate an entry in the IP-filtering log.</li> <li>◦ 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.</li> <li>◦ 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.</li> <li>◦ Reject—Send an ICMP unreachable message back to the client and resets the connection to the server.</li> </ul> <p>For custom filters, select an IP-filtering action that you configured in <a href="#">Configure Custom IP Filters</a>, which are displayed under User Defined.</p>
Match Type	<p>Select the match criteria for the IP address:</p> <ul style="list-style-type: none"> <li>◦ Destination IP address</li> <li>◦ Source IP address</li> <li>◦ Source and destination IP address</li> <li>◦ Source or destination IP address</li> </ul>
IP Address	<p>Select to enforce the action for an individual IP address. Click  to add an IP address. The Add Address popup window displays. For more information, see <a href="#">Configure Address Objects</a>.</p>
IP Address Group	<p>Select to enforce the action for a group of IP</p>

addresses. Click  to add a group of IP addresses. The Add Address Group window displays. For more information about adding address group objects, see [Configure Address Objects](#). For more information about uploading address files from the Add Address Group window, see [Upload Address Files](#).

6. Click OK.
7. Select the Allow List tab and enter information for the following fields.

Add IP Filter

Name \*

Description

Tags

Default Action

--Select--

☒ Prioritize URL Reputation

Allow URL Reputation \*

--Select--

LEF Profile

--Select--

☐ Default Profile

Deny List

Allow List

GeoIP Based Actions

Reputation-Based Actions

Address Reverse Lookup

☐ Enable Logging

Match Type

--Select--

☒ IP Address

☐ IP Address Group

☐

IP Address

+ New Address +

IP Address Not Configured

☐



IP Address Group

+ New Address Group +

IP Address Group Not Configured

OK

Cancel

Field	Description
Enable Logging	Select to enable LEF logging of the allow-listed IP addresses.
Match Type	<p>Select the match criteria for the IP address:</p> <ul style="list-style-type: none"> <li>◦ Destination IP address</li> <li>◦ Source IP address</li> <li>◦ Source and destination IP address</li> <li>◦ Source or destination IP address</li> </ul>
IP Address	Select to enforce the action for an individual IP address. Click  to add an IP address. The Add Address popup window displays. For more information, see <a href="#">Configure Address Objects</a> .
IP Address Group	Select to enforce the action on a group of IP addresses. Click  to add a group of IP addresses. The Add Address Group window displays. For more information about adding address group objects, see <a href="#">Configure Address Objects</a> . For more information about uploading address files from the Add Address Group window, see <a href="#">Upload Address Files</a> .

8. Click OK.
9. Select the Geo IP-Based Actions tab.

Add IP Filter

Name \*

Description

Tags

Default Action

--Select--

Allow URL Reputation \*

--Select--

Prioritize URL Reputation

☒

LEF Profile

--Select--

Default Profile

☐

Deny List

Allow List

**GeoIP Based Actions**

Reputation-Based Actions

Address Reverse Lookup

+

<

1

>

25

Name

Action

Match Type

Regions

No Actions Added

OK

Cancel

Name \*

Description

## Tags

Default Action

--Select--

☒ Prioritize URL Reputation

Allow URL Reputation \*

--Select--

LEF Profile

--Select--

☐ Default Profile

Deny List   Allow List   **GeoIP Based Actions**   Reputation-Based Actions   Address Reverse Lookup

      1  25 

<input type="checkbox"/>	Name	Action	Match Type	Regions
No Actions Added				

No Actions Added

OK

Cancel

- Click the + Add icon to add actions for geographical reputation-based IP filtering. In the Add Geo IP-Based Action popup window, enter information for the following fields.

Add GeolP based Action

Name \*

Match Type

--Select--

Action

--Select--

☐

Regions

+

Regions Not Configured

OK

Cancel

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_IP\\_Filt...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_IP_Filt...)  
Updated: Wed, 23 Oct 2024 08:18:04 GMT  
Copyright © 2024, Versa Networks, Inc.

21

Field	Description
Name	Select the name of the geographical 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 geographical reputation.</p> <p>The following are the predefined actions:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the IP address, and generate an entry in the IP-filtering log.</li> <li>◦ Allow—Allow the IP address, and do not generate an entry in the IP-filtering log.</li> <li>◦ 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.</li> <li>◦ 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.</li> <li>◦ Reject—Send an ICMP unreachable message back to the client and resets the connection to the server.</li> </ul> <p>For custom filters, select an IP-filtering action that you configured in <a href="#">Configure Custom IP Filters</a>, which are displayed under User Defined.</p>
Match Type	<p>Select the match criteria for the IP address:</p> <ul style="list-style-type: none"> <li>◦ Destination IP address</li> <li>◦ Source IP address</li> <li>◦ Source and destination IP address</li> <li>◦ Source or destination IP address</li> </ul>
Regions	Select a geographical region.

11. Click OK.

12. Select the Reputation-Based Actions tab.

Add IP Filter

Name \*

Description

Tags

Default Action

Allow URL Reputation \*

☒ Prioritize URL Reputation

LEF Profile

☐ Default Profile

Deny List
Allow List
GeoIP Based Actions
Reputation-Based Actions
Address Reverse Lookup

+

25


	Name	Predefined Action	User Defined Action	Match Type	URL Reputations
No Actions Added					

OK
Cancel

- Click the + Add icon. In the Add Reputation-Based Action popup window, enter information for the following fields.





Field	Description
Name	Select the name of the IP 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 reputation. The following are the predefined actions:</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the IP address, and generate an entry in the IP-filtering log.</li> <li>◦ Allow—Allow the IP address, and do not generate an entry in the IP-filtering log.</li> <li>◦ 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.</li> <li>◦ 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.</li> <li>◦ Reject—Send an ICMP unreachable message back to the client and resets the connection to the server.</li> </ul> <p>For custom filters, select an IP-filtering action that you configured in <a href="#">Configure Custom IP Filters</a>, which are displayed under User Defined.</p>
Match Type	<p>Select the match criteria for the IP address:</p> <ul style="list-style-type: none"> <li>◦ Destination IP address</li> <li>◦ Source IP address</li> <li>◦ Source and destination IP address</li> <li>◦ Source or destination IP address</li> </ul>
Reputations	<p>Click the  Add icon and select a reputation:</p> <ul style="list-style-type: none"> <li>◦ Botnets</li> </ul>

	<ul style="list-style-type: none"> <li>◦ Denial of service</li> <li>◦ Phishing</li> <li>◦ Proxy</li> <li>◦ Reputation</li> <li>◦ Scanners</li> <li>◦ Spam sources</li> <li>◦ Web attacks</li> <li>◦ Windows exploits</li> </ul>
--	---

14. Click OK.
15. Select the Address Reverse Lookup tab 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.

Add IP Filter

Name \*

Description

Tags

Default Action

--Select--

☒ Prioritize URL Reputation

Allow URL Reputation \*

--Select--

LEF Profile

--Select--

☐ Default Profile

Deny List

Allow List

GeoIP Based Actions

Reputation-Based Actions

Address Reverse Lookup

Lookup For

--Select--

URLF Profile

--Select--

DNS Redirection Policy

--Select--

☐ Enabled

Mode

--Select--

OK

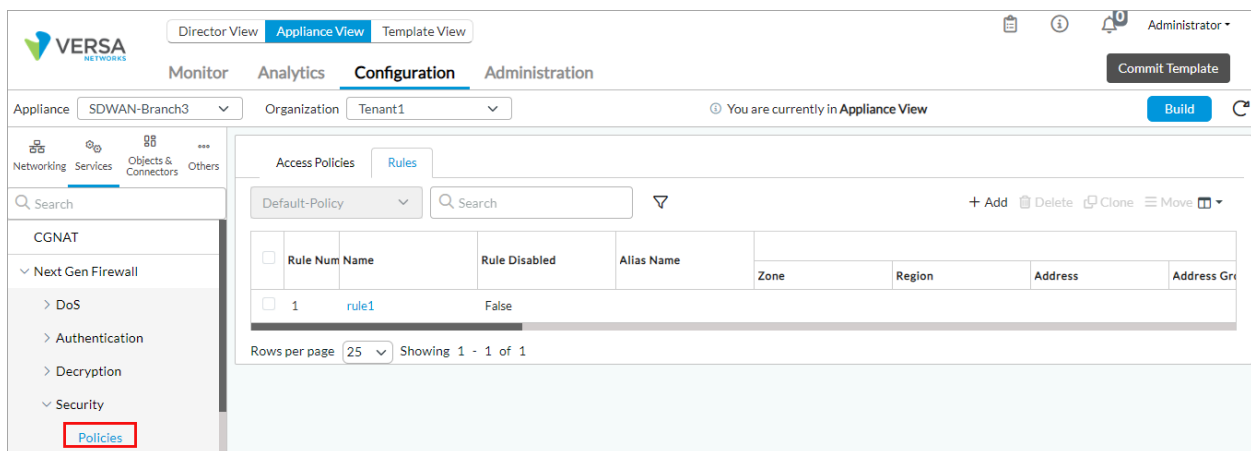
Cancel

Field	Description
Lookup For	Select the address type on which to perform a reverse lookup: <ul style="list-style-type: none"> <li>◦ Destination IP address</li> <li>◦ Source IP address</li> <li>◦ Source and destination IP address</li> </ul>
URLF Profile	Select the URL-filtering profile to associate with IP address reverse lookup.

16. Click OK.

## Apply an IP-Filtering Profile to an Access Policy

- In Director view:
  - Select the Configuration tab in the top menu bar.
  - Select Devices > Devices in the horizontal menu bar.
  - Select an organization in the left menu bar.
  - Select a device name in the main panel. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Services > Next-Gen Firewall > Security > Policies in the left menu bar, and select the Rules tab.



- Select a security access policy rule in the table in the main pane. The Edit Rule popup window displays.

5. Select the Enforce tab
6. In the Actions group of fields, click Apply Security Profile.
7. Click Profiles, and then click IP Filtering and select the IP-filtering profile to use for the access policy rule. The drop-down list displays the predefined and custom IP filtering profiles.
8. If you have created profile groups, click Profile Groups, and then click IP Filtering and select the IP-filtering profile to use for the access policy rule. The drop-down list displays the predefined and custom IP -filtering profiles. For more information, see [Configure Security Profile Groups](#).
9. Click OK.

## Monitor IP-Filtering Policies

You monitor IP-filtering policies to view the traffic flow details when a policy is used. For more information, see [Monitor Device Services](#).

To monitor IP-filtering policies:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliances in the left menu bar.
  - c. Select a device name in the main panel. The view changes to Appliance view.
2. Select the Monitor tab in the top menu bar.
3. Select the Provider Organization > Services tab.
4. Select NGFW > IP Filtering and select User-Defined or Predefined in the drop-down list. The IP-filtering policy


statistics displays.

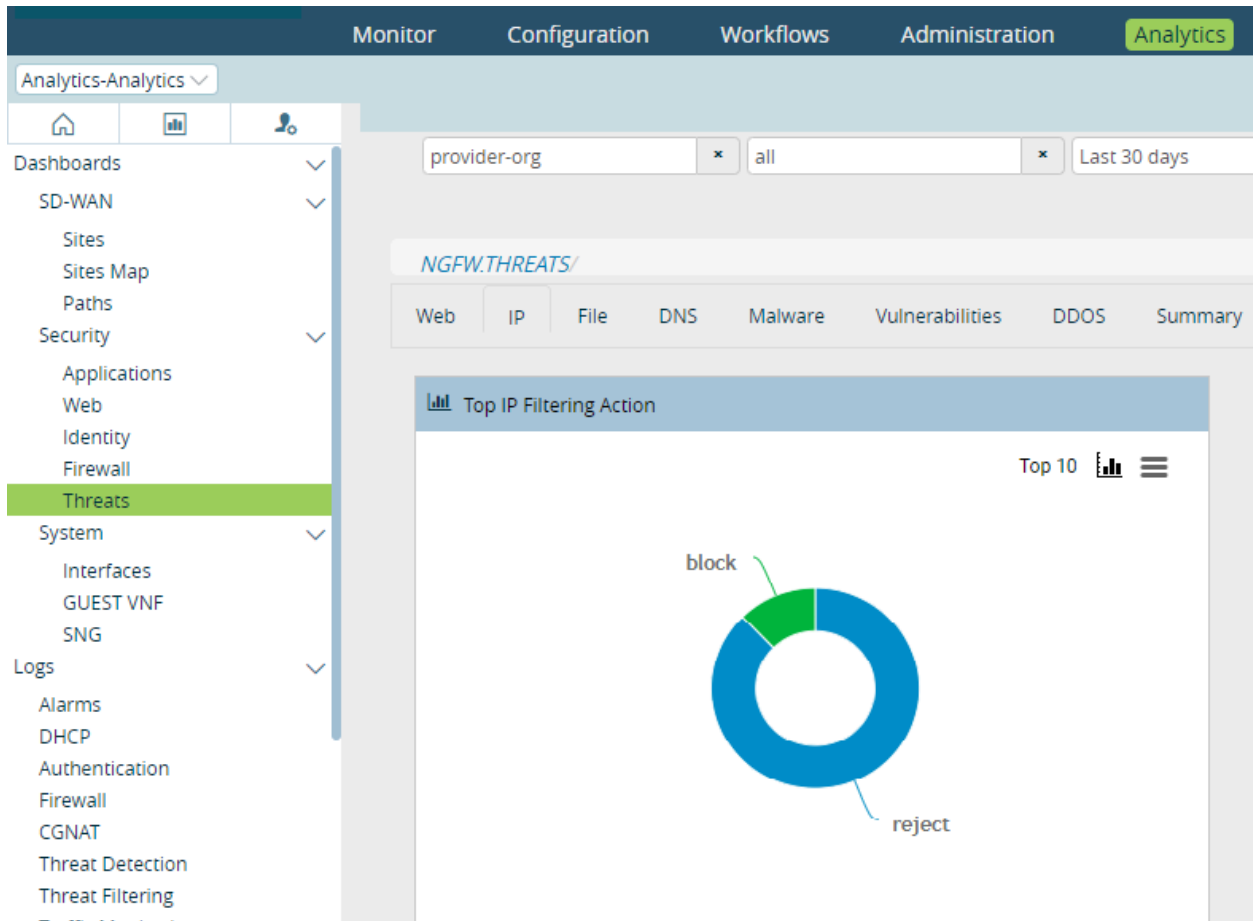
The screenshot shows the Versa Networks Appliance View interface. At the top, there are tabs for Director View, Appliance View (selected), and Template View. Below this is a navigation bar with Monitor, Analytics, Configuration, and Administration. The main content area shows the SDWAN-Branch3 configuration page. The left sidebar has tabs for Summary, Services (selected), Networking, System, and Tools. The Services tab is active, and the IP Filtering section is highlighted in the sub-menu. The IP Filtering table displays various threat categories and their corresponding counts.

Name	Hit Count	Blacklist Hit C...	White List Hit	GeolIP Rule Hi...	Reputation Ru...	No Match Cou...	Log Count	Drop Count	Fall Count	Reverse Looku...	URL Filtering ...	Captive Porta
Block bad traffic	0	0	0	0	0	0	0	0	0	0	0	0
Block bots	0	0	0	0	0	0	0	0	0	0	0	0
Web protection	0	0	0	0	0	0	0	0	0	0	0	0
Block DoS	0	0	0	0	0	0	0	0	0	0	0	0
Block spam	0	0	0	0	0	0	0	0	0	0	0	0
Block scanners	0	0	0	0	0	0	0	0	0	0	0	0
Block window...	0	0	0	0	0	0	0	0	0	0	0	0
Versa Recom...	0	0	0	0	0	0	0	0	0	0	0	0

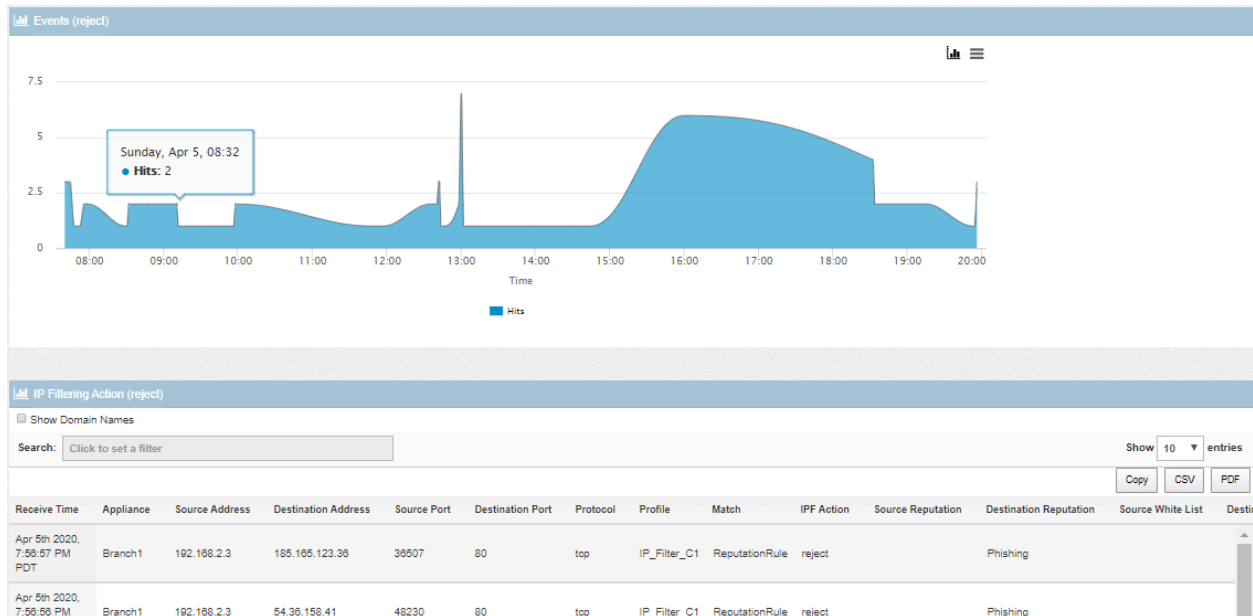
## Analyze IP-Filtering Threats

To monitor the IP-filtering threats that are occurring in your network, view IP filtering threat monitoring reports:

1. In Director view, select the Analytics tab in the top menu bar. The view changes to Analytics view.
2. Select Home  > Security > Threats in the left menu bar to view the security threats dashboard. For more information, see [Security Dashboard](#).
3. Select the IP tab to display information about the top IP-filtering actions.




4. Drill down to display detailed IP logs matching the drill key.

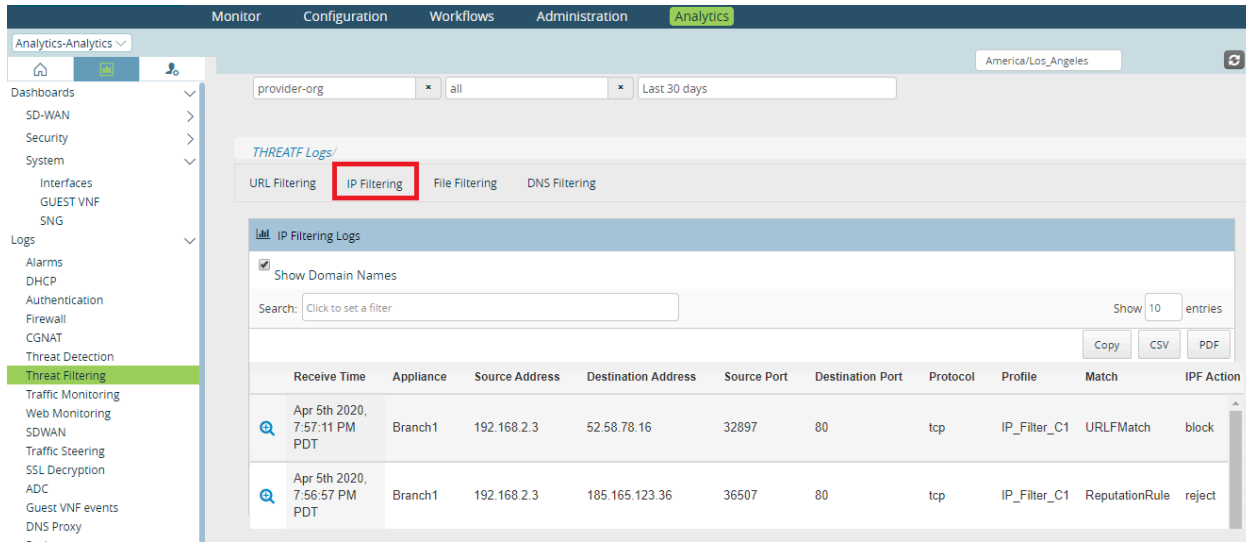


[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/Security\\_Configuration/Configure\\_IP\\_Filt...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_IP_Filt...)

Updated: Wed, 23 Oct 2024 08:18:04 GMT

Copyright © 2024, Versa Networks, Inc.

5. Select Home  > Logs > Threat Filtering in the left menu bar. Select the IP Filtering tab in the main pane.



The screenshot shows the Versa Analytics interface. The left sidebar contains a menu with categories like Dashboards, Logs, and Threat Filtering. The 'Threat Filtering' category is expanded, and the 'IP Filtering' tab is selected. The main pane displays a table of IP Filtering logs. The table has columns for Receive Time, Appliance, Source Address, Destination Address, Source Port, Destination Port, Protocol, Profile, Match, and IPF Action. Two log entries are visible, both from Branch1 on Apr 5th 2020. The first entry shows a match with URLFilter\_C1 and a block action. The second entry shows a match with ReputationRule and a reject action.

Receive Time	Appliance	Source Address	Destination Address	Source Port	Destination Port	Protocol	Profile	Match	IPF Action
Apr 5th 2020, 7:57:11 PM PDT	Branch1	192.168.2.3	52.58.78.16	32897	80	tcp	IP_Filter_C1	URLFilter_C1	block
Apr 5th 2020, 7:56:57 PM PDT	Branch1	192.168.2.3	185.165.123.36	36507	80	tcp	IP_Filter_C1	ReputationRule	reject

## Supported Software Information

Releases 20.2 and later support all content described in this article.

## Additional Information

- [Apply Log Export Functionality](#)
- [Configure Address Objects](#)
- [Configure Log Export Functionality](#)
- [Configure Security Profile Groups](#)
- [Configure Stateful Firewall](#)
- [Configure URL Filtering](#)
- [Monitor Device Services](#)
- [Security Dashboards](#)
- [Versa Analytics Scaling Recommendations](#)