

---

## Configure DNS Filtering

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

Domain Name System (DNS) filtering allows you to control access to websites, webpages, and IP addresses, to provide protection from malicious websites, such as known malware and phishing sites.

To use DNS filtering, you create a DNS-filtering profile and then associate it with an access policy. In a DNS-filtering profile you can configure the following components to use to filter DNS requests:

- Deny lists—Define the URLs and IP addresses of DNS requests for which access is blocked, and define the action to take when a URL or an IP address matches. Deny lists are sometimes referred to as blacklists.
- Allow lists—Define the URLs and IP addresses of DNS requests to which to explicitly allow access. Allow lists are sometimes referred to as whitelists.
- Query-based actions—Define rules for DNS operation codes (opcodes), which are the commands that are sent to DNS servers to have them perform an action.
- Reputation-based actions—Define how to handle DNS requests from newly observed website domains.
- Detection of DNS tunneling—Define parameters for identifying DNS tunneling, which is a type of cyberattack that encodes the data from other programs or protocols in DNS queries and responses. An attacker can create a command-and-control channel with the infected device, extract data (information) from the infected device, and then insert malware or other data into the infected device using only DNS query and DNS response.

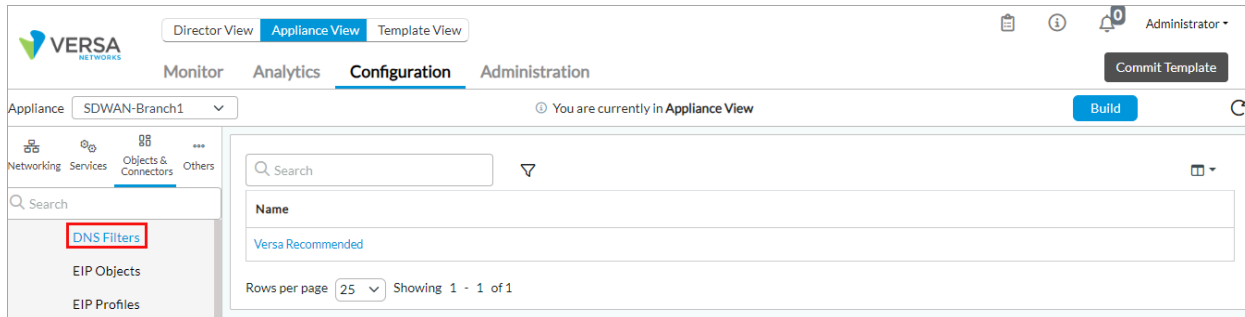
---

## View the Predefined DNS-Filtering Profile

Versa provides a predefined DNS-filter profile called Versa Recommended profile. This profile includes IP filtering to block bad traffic and the Versa Recommended URL filter, which is called Corporate. For more information, see [View Predefined URL-Filtering Profiles](#).

To view the predefined DNS-filtering profile:

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 Configuration tab in the top menu bar.
3. Select Objects and Connectors > Objects > Predefined > DNS Filters in the left menu bar.



4. Click Versa Recommended to view details of the DNS filtering profile. The Edit DNS Filter popup window displays.

## Edit DNS Filter

Name

Versa Recommended

☒ LEF Profile Default

IP Filters

Block bad traffic

Add Tag

URL Filters

corporate

Add Tag

Cancel

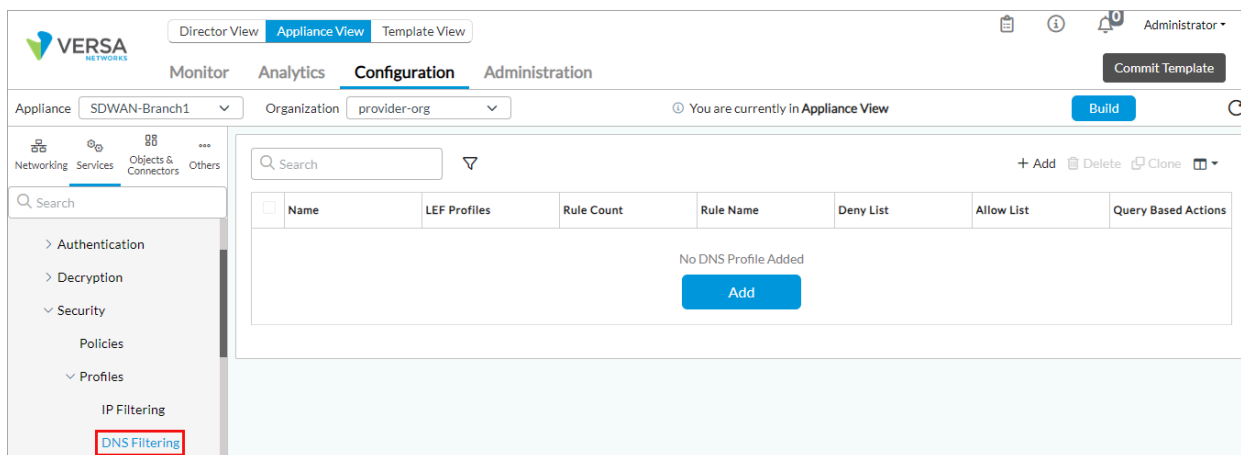
## Create a DNS-Filtering Profile

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

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

Updated: Wed, 23 Oct 2024 08:18:39 GMT

Copyright © 2024, Versa Networks, Inc.



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



The 'Add DNS Filter' popup window is shown. It contains the following fields and options:

- Name \***: A text input field.
- Description**: A text input field.
- Tags**: A text input field.
- LEF Profile**: A dropdown menu with '--Select--' and a 'Default Profile' checkbox.
- Deny List**: A tab selected with a red box, with other tabs: 'Allow List', 'Query Based Actions', 'Reputation-Based Actions', and 'Tunnel Detection'.
- Deny List Action**: A dropdown menu with '--Select--'.
- Pattern**: A section with a checkbox, a green status icon, and a 'Pattern Not Configured' message.
- Strings**: A section with a checkbox and a 'Strings Not Configured' message.
- Buttons**: 'OK' and 'Cancel' buttons at the bottom right.

Field	Description
Name	Enter a name for the DNS filter profile.
LEF Profile	Select the LEF profile to use to log the actions related to DNS filtering. Either select a LEF profile or check the Default Profile checkbox. For more information about applying a LEF profile to a feature or service, see <a href="#">Apply Log Export Functionality</a> .

Default Profile	Click to use the default LEF profile. For information about configuring a default LEF profile
-----------------	---

5. Select the Deny List tab to configure URLs and IP addresses of DNS requests for which access is blocked. Enter information for the following fields.

Field	Description
Deny List Actions	<p>Select the action to take for domain names or IP addresses when denying (blocking) incoming D</p> <ul style="list-style-type: none"> <li>◦ Alert—Allow the DNS response and generate an entry in the DNS filtering log in Versa Anal</li> <li>◦ Allow—Allow the DNS response without generating an entry in the DNS filtering log in Versa</li> <li>◦ Block—Block the DNS response and generate an entry in the DNS filtering log in Versa Ana displayed, and the user cannot continue with the website.</li> <li>◦ Drop Packet—The browser waits for a response from the DNS server and then drops the p whether the packet was dropped because of a delayed response from the DNS server or be the website.</li> <li>◦ Drop Session—The browser waits for a response from the server and drops the session. It the session was dropped because of a delayed response from the DNS server or because a website.</li> <li>◦ Reject—Send an ICMP unreachable message back to the client.</li> <li>◦ Sinkhole—(For Releases 22.1.3 and later.) Return a false IP address to the URL, thus block spoofs DNS servers to prevent the resolution of the hostnames associated with URLs. This hosts in a network if a firewall is unable to find the original source IP address of DNS requer queries create responses to the client host queries directed at malicious domains and try to instead of connecting to malicious domains. You can check the traffic logs to identify infecte</li> </ul> <p>You can enable deny actions in DNS filtering using either predefined or user-defined actions. Fo must be either DNS or All. For more information, see <a href="#">Configure User-Defined Actions</a>.</p>
Pattern	Click the  Add icon to add a regular expression (regex) for matching a domain name or an IP pattern matches the same domain name or IP address in a deny list and an allow list, the action
Strings	Click the  Add icon to add a complete string for matching a domain name or IP address to blo same domain name or IP address in a deny list and an allow list, the action in the deny list takes

6. Select the Allow List tab to configure URLs and IP addresses of DNS requests for which access is explicitly allowed. Enter information for the following fields.

Add DNS Filter

Name \*

Description

Tags

LEF Profile

--Select--

☐ Default Profile

Deny List

Allow List

Query Based Actions

Reputation-Based Actions

Tunnel Detection

☐ Enable Logging

☐ Pattern



Pattern Not Configured

☐ Strings

Strings Not Configured

OK

Cancel

Field	Description
Enable Logging	Click to log information about the allowed domain names and IP addresses.
Pattern	Click the  Add icon to add a regular expression (regex) pattern for matching a domain name or IP address. If the pattern matches the same domain name or IP address in a deny list and an allow list, the deny list has precedence.
Strings	Click the  Add icon to add a complete domain name for matching a domain name or IP address. If a string matches the same domain name or IP address in a deny list and an allow list, the deny list has precedence.

- Select the Query-Based Actions tab to define rules for DNS operation codes (opcodes), which are commands that are sent to have the DNS server perform an action.

Add DNS Filter

Name \*

Description

Tags

LEF Profile

--Select--

☐ Default Profile

Deny List

Allow List

Query Based Actions

Reputation-Based Actions

Tunnel Detection

+

1

25

	Request Type	Name	Rule Actions
No Rules Added			

OK

Cancel

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

Add Query Based Actions

Name \*

Rule Actions \*

--Select--

Request Type

--Select--

OK

Cancel

Field	Description
Name	Enter a name for the query-based action.
Rule Actions	Select the action to take on the DNS request: <ul style="list-style-type: none"> <li>Alert—Allow the DNS response and generate an entry in the DNS filtering log in Versa</li> </ul>

	<ul style="list-style-type: none"> <li>◦ Allow—Allow the DNS response and do not generate an entry in the DNS filtering log.</li> <li>◦ Block—Block the DNS response and generate an entry in the DNS filtering log in Versa Cloud Manager. The error message is displayed, and the user cannot continue with the website.</li> <li>◦ Drop Packet—The browser waits for a response from the DNS server and then drops the packet. The user cannot determine whether the packet was dropped because of a delayed response from the DNS server or because of blocked access to the website.</li> <li>◦ Drop Session—The browser waits for a response from the server and drops the session. The user cannot determine whether the session was dropped because of a delayed response from the DNS server or because of blocked access to the website.</li> <li>◦ Reject—Send an ICMP unreachable message back to the client.</li> <li>◦ Sinkhole—(For Releases 22.1.3 and later.) Return a false IP address to the URL, thus preventing the user from connecting to the website. Sinkhole spoofs DNS servers to prevent the resolution of the hostnames associated with the website. You can identify infected hosts in a network if a firewall is unable to find the original source IP address. Sinkhole malware DNS queries create responses to the client host queries directed at the website. The client connects to a sinkhole IP address instead of connecting to malicious domains. You can prevent infected hosts from connecting to malicious domains.</li> </ul> <p>You can enable query-based actions in DNS filtering either predefined or user-defined. For more information, see <a href="#">User-Defined Actions</a>.</p> <p>You can configure multiple rules.</p>
Request Type	<p>Select the type of DNS opcode to which the rule applies:</p> <ul style="list-style-type: none"> <li>◦ IQuery—Send a request for an inverse DNS query command.</li> <li>◦ Notify—Send a request for a DNS notify command.</li> <li>◦ Query—Send a request for a DNS query command.</li> <li>◦ Status—Send a request for a DNS status command.</li> <li>◦ Update—Send a request for a DNS update command.</li> </ul> <p>For each request type, you must enter additional information, as described in the following table:</p>

9. For the IQuery request type, enter information for the following fields.

Add Query Based Actions

Name \*

Rule Actions \*

Alert

Request Type

IQuery

Query Type

☐ v4

☐ Address

+

Address Not Configured

☐ Address Group

+

Address Group Not Configured

☐ v6

☐ Address

+

Address Not Configured





☐ Address Group

+

Address Group Not Configured

OK

Cancel

Field	Description
V4 (Group of Fields)	Click to send an inverse query to IPv4 addresses and address groups.
◦ Address	Click the  Add icon and select an IPv4 address record.
◦ Address Group	Click the  Add icon and select an IPv4 address group record.
V6 (Group of Fields)	Click to send an inverse query to IPv6 addresses and address groups.
◦ Address	Click the  Add icon and select an IPv6 address record.
◦ Address Group	Click the  Add icon and select an IPv6 address group record.

10. For the Query request type, enter information for the following fields.

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

Updated: Wed, 23 Oct 2024 08:18:39 GMT

Copyright © 2024, Versa Networks, Inc.

8



Add Query Based Actions

×

Name \*

Rule Actions \*

Alert

▼

Request Type

Query

▼

Number of Additional Record

--Select--

▼

Number of Questions

--Select--

▼

Queries

Query Type	Domain Name	
--Select--		+
No Records to Display		

OK

Cancel

Field	Description
Number of Additional Records	Enter the number of additional records and select one of the following operators: <ul style="list-style-type: none"> <li>◦ equal-to</li> <li>◦ greater-than</li> <li>◦ less-than</li> <li>◦ not-equal-to</li> </ul>
Number of Questions	Enter the number of questions and select one of the following operators: <ul style="list-style-type: none"> <li>◦ equal-to</li> <li>◦ greater-than</li> <li>◦ less-than</li> </ul>

	◦ not-equal-to
Queries (Group of Fields)	
◦ Query Type	Select the query type.
◦ Domain Name	Enter the domain name.

11. For the Notify or Status request type, click the + Add icon to add zone names.

### Add Query Based Actions ✕

Name \*
Rule Actions \*
Request Type

Alert
Notify

Zones

<input type="checkbox"/>	Zone Name	+	🗑	↗
Zone Name Not Configured				

OK
Cancel

### Add Query Based Actions

Name \*

Rule Actions \*

Alert

Request Type

Status

Zones

<input type="checkbox"/>	Zone Name	<div>+🗑️🔗</div>
Zone Name Not Configured		

OK

Cancel

12. For the Update request type, enter information for the following fields.

Add Query Based Actions

Name \*

Rule Actions \*

Request Type

Alert

Update

Number of Zone Record

--Select--

Number of Prerequisite Record

--Select--

Number of Additional Record

--Select--

Number of Update Record

--Select--

☐


Domain Name

+

OK

Cancel

Field	Description
Number of Zone Records	Enter the number of zone records and select one of the following operators <ul style="list-style-type: none"> <li>◦ equal-to</li> <li>◦ greater-than</li> <li>◦ less-than</li> <li>◦ not-equal-to</li> </ul>
Number of Prerequisite Records	Enter the number of prerequisite records and select one of the following operators <ul style="list-style-type: none"> <li>◦ equal-to</li> <li>◦ greater-than</li> <li>◦ less-than</li> <li>◦ not-equal-to</li> </ul>

Number of Additional Records	Enter the number of additional records and select one of the following operators: <ul style="list-style-type: none"> <li>◦ equal-to</li> <li>◦ greater-than</li> <li>◦ less-than</li> <li>◦ not-equal-to</li> </ul>
Number of Update Records	Enter the number of update records and select one of the following operators: <ul style="list-style-type: none"> <li>◦ equal-to</li> <li>◦ greater-than</li> <li>◦ less-than</li> <li>◦ not-equal-to</li> </ul>
Domain Name	Click the  Add icon to add domain names.

13. Select the Reputation-Based Actions tab to define how to handle DNS requests from newly observed website domains. Enter information for the following fields.

Add DNS Filter

Name \*

Description

Tags

LEF Profile

--Select--

☐ Default Profile

Deny List

Allow List

Query Based Actions

Reputation-Based Actions

Tunnel Detection

Newly Observed Domains

Duration (in hours)

Action

--Select--

IP Filtering

--Select--

URL Filtering

--Select--

OK

Cancel

Field	Description
Newly Observed Domains (Group of Fields)	Configure how to handle requests from newly observed domains.
<ul style="list-style-type: none"> <li>Duration</li> </ul>	<p>How long to wait, in hours, before taking the configured action on a newly observed domain.</p> <p><i>Range:</i> 1 through 168 hours</p>
<ul style="list-style-type: none"> <li>Action</li> </ul>	<p>Action to take on the newly observed domain:</p> <ul style="list-style-type: none"> <li>Alert—Allow the DNS response and generate an entry in the DNS filtering log in Versa Cloud Manager.</li> <li>Allow—Allow the DNS response and do not generate an entry in the DNS filtering log in Versa Cloud Manager.</li> <li>Block—Block the DNS response and generate an entry in the DNS filtering log in Versa Cloud Manager. The block message is displayed, and the user cannot continue with the website.</li> <li>Drop Packet—Have the browser wait for a response from the DNS server and then drop the packet.</li> </ul>

	<p>determine whether the packet was dropped because of a non-responsive DNS server or because of a non-responsive connection to the website.</p> <ul style="list-style-type: none"> <li>◦ Drop Session—Have the browser wait for a response from the server and then determine whether the session was dropped because of a non-responsive DNS server or because of a non-responsive connection to the website.</li> <li>◦ Reject—Send an ICMP unreachable message back to the client.</li> <li>◦ Sinkhole—(For Releases 22.1.3 and later.) Return a false IP address to the URL, then the sinkhole spoofs DNS servers to prevent the resolution of the hostnames associated with the URL. This action can be used to identify infected hosts in a network if a firewall is unable to find the original source IP address. Sinkhole malware DNS queries create responses to the client host queries directed to the sinkhole IP address instead of connecting to malicious domains. You can use sinkhole to identify infected hosts.</li> </ul> <p>You can enable reputation-based actions in DNS filtering either predefined or user-defined. For more information, see <a href="#">Configure User-Defined Actions</a>.</p>
IP Filtering	Select an IP-filtering profile to use to evaluate the resolved IP addresses and destination domain. The action taken based on the IP-filtering profile applies to the session.
URL Filtering	Select the URL-filtering profile to use to evaluate domain names and common names in messages. The action taken based on the URL-filtering profile applies to the session.

14. (For Releases 22.1.3 and later.) Select the Tunnel Detection tab, and then enter information for the following fields.

Add DNS Filter

Name \*

Description

Tags

LEF Profile

--Select--

☐ Default Profile

Deny List

Allow List

Query Based Actions

Reputation-Based Actions

Tunnel Detection

Tunnel Detection Action

--Select--

Post Detection Parameters

Detection Parameters

Quarantine Period

Max Domains To Track

OK

Cancel

Field	Description
Tunnel Detection Action	<p>Action to take when DNS tunneling is detected:</p> <ul style="list-style-type: none"> <li>◦ Allow—Allow the DNS response and do not an entry in the DNS filtering l</li> <li>◦ Alert—Allow the DNS response and generate an entry in the DNS filtering</li> <li>◦ Block—Block the DNS response and generate an entry in the DNS filtering displayed, and the user cannot continue with the website.</li> <li>◦ Drop Packet—Have the browser wait for a response from the DNS server determine whether the packet was dropped because of a non-responsive the website.</li> <li>◦ Drop Session—Have the browser waits for a response from the server and determine whether the session was dropped because of a non-responsive the website</li> <li>◦ Reject—Send an ICMP unreachable message back to the client.</li> <li>◦ Sinkhole—(For Releases 22.1.3 and later.) Return a false IP address to the sinkhole spoofs DNS servers to prevent the resolution of the hostnames and identify infected hosts in a network if a firewall is unable to find the original malware DNS queries create responses to the client host queries directed to the sinkhole IP address instead of connecting to malicious domains. You can</li> </ul>



Post-Detection Parameters (Tab)	
◦ Quarantine Period	Enter how long to quarantine a domain after a DNS tunnel has been detected. <i>Default: 14400 minutes (24 hours)</i>
◦ Maximum Domains To Track	Enter the maximum number of domains to track for DNS tunneling. <i>Default: 128</i>

15. Select the Detection Parameters, and enter information for the following fields.

Add DNS Filter

Name \*

Description

Tags

LEF Profile

--Select--

☐ Default Profile

Deny List

Allow List

Query Based Actions

Reputation-Based Actions

Tunnel Detection

Tunnel Detection Action

--Select--

Post Detection Parameters

Detection Parameters

☐ Frequency Based Detection

☐ Invalid Char Detection

OK

Cancel

Field	Description
Frequency-Based Detection	Click to detect DNS tunneling based on the number of requests, the number of DNS requests for uncommon DNS request types. For more information, see S
Invalid Character Detection	Click to detect DNS tunneling based on the invalid (non-RFC) characters that invalid character-based detection, the configured action is taken directly on the found in the FQDN. Also note that these domains are not quarantined.

16. On the Tunnel Detection tab, if you select the Detection Parameters tab and click Frequency-Based detection, configure parameters for detecting the frequency of DNS tunneling based on the frequency of the DNS requests. Enter information for the following fields.

Add DNS Filter
✕

Name \*

Description
Tags

LEF Profile

--Select--
☐ Default Profile

Deny List
Allow List
Query Based Actions
Reputation-Based Actions
Tunnel Detection

Tunnel Detection Action

--Select--

Post Detection Parameters
Detection Parameters

☒ Frequency Based Detection
☐ Invalid Char Detection

Max Domains To Track

Max IP to track

Detection Window

Repetitive FQDN Limit

Uncommon Requests Limit

URL Reputation

--Select--

☐ Include Domains
+

☐ Exclude Domains
+

☐ Common Query Types
+

Include Domains Not Configured

Exclude Domains Not Configured

Common Query Types Not Configured

Global Average FQDN Size

Average Size
Maximum FQDNs

No Records to Display

Per IP Average FQDN Size




Average Size
Maximum FQDNs

No Records to Display

OK

Cancel

Field	Description
-------	-------------

Maximum Domains To Track	Enter the maximum number of domains to track in parallel for DNS tunneling. <i>Default: 16384</i>
Maximum IP To Track	Enter the maximum number of source IP addresses per domain to track for DNS tunneling. <i>Default: 32</i>
Detection Window	Set the length of time window to use to detect DNS tunneling. <i>Default: 10 minutes</i>
Repetitive FQDN Limit	Enter the maximum number of repeating DNS requests for an FQDN per source IP address. <i>Default: 400</i>
Uncommon Requests Limit	Enter the maximum number of uncommon DNS requests per source that are not in the common query types list. <i>Default: 80</i>
URL Reputation	Set the URL reputation to ignore tunnel detection for FQDNs having a URL reputation of: <ul style="list-style-type: none"> <li>Low risk</li> <li>High risk</li> <li>Moderate risk. This is the default.</li> <li>Suspicious</li> <li>Trustworthy</li> </ul> <i>Default: Moderate risk</i>
Include Domains	Click and then click the  Add icon to add user-defined domains to include in tunnel detection.
Exclude Domains	Click and then click the  Add icon to add user-defined domains to exclude from tunnel detection.
Common Query Types	Click and then click the  Add icon to select the DNS resource record (RR) type to include in tunnel detection. <ul style="list-style-type: none"> <li>A—Host address</li> <li>A6—A6</li> <li>AAAA—IPv6 address</li> <li>AFSDB—AFS database location</li> <li>ALL—All resource record types</li> <li>APL—Address prefix list</li> <li>ATM—ATM address</li> <li>CERT—Certificates</li> <li>CNAME—Canonical name for an alias</li> <li>DHCID—DHCP ID</li> </ul>

- DNSKEY—DNS key
- DS—Delegation signer
- EID—Endpoint identifier
- GPOS—Geographical position
- HINFO—Host information
- HIP—Host identity protocol
- ISDN—ISDN address
- ISECKEY\*—IPsec key
- IXFR—Incremental transfer
- KEY—Security key
- KX—Key exchanger
- LOC—Location information
- MAILA—Mail agent route records
- MAILB—Mailbox-related route records (MB, MG, or MR)
- MB—Mailbox domain name
- MD—Mail destination
- MF—Mail forwarder
- MG—Mail group member
- MINFO—Mailbox or mail list information
- MX—Mail exchange
- NAPTR—Naming authority pointer
- NIMLOC—Nimrod locator
- NINFO—Identical to TXT RR [RR56]
- NS—Authoritative name server
- NSAP-PTR—Domain name pointer for an NSAP style
- NSEC—Authenticated denial of existence
- NSEC3—Authenticated denial of existence
- NSEC3PARAM—NSEC3 parameters
- NULL—Null resource record
- NXT—Next domain
- OPR
- PTR—Domain name pointer
- PX—X.400 mail mapping information
- RKEY—Record key
- RP—Responsible person
- RRSIG—Resource resource digital signature
- RT—Route through

	<ul style="list-style-type: none"> <li>◦ SIG—Security signature</li> <li>◦ SINK—Kitchen sink</li> <li>◦ SOA—Marks the start of a zone of authority</li> <li>◦ SPF—Sender policy framework</li> <li>◦ SRV—Server selection</li> <li>◦ SSHFP—SSH key fingerprint</li> <li>◦ TALINK—Trusted anchor link</li> <li>◦ TKEY—Transaction key</li> <li>◦ TSIG—Transaction signature</li> <li>◦ TXT—Text strings</li> <li>◦ WKS—Well-known service description</li> <li>◦ X25—X.25 PSDN address</li> </ul> <p><i>Default: A, AAAA, and A6</i></p>
Global Average FQDN Size	Enter the global mappings on which to detect DNS tunneling based on the average number of subdomains per base domain. You can configure up to six mappings.
<ul style="list-style-type: none"> <li>◦ Average Size, Maximum FQDNs</li> </ul>	<p>Configure global mapping for the average size of the subdomain and the maximum number of FQDNs. You can configure up to six mappings. The following are the default values:</p> <ul style="list-style-type: none"> <li>◦ FQDN size—1, maximum number of FQDNs—250</li> <li>◦ FQDN size—20, maximum number of FQDNs—200</li> <li>◦ FQDN size—30, maximum number of FQDNs—150</li> <li>◦ FQDN size—40, maximum number of FQDNs—100</li> <li>◦ FQDN size—50, maximum number of FQDNs—50</li> <li>◦ FQDN size—60, maximum number of FQDNs—30</li> </ul>
Per-IP Average FQDN Size	Enter per-single-source IP address mappings on which to detect DNS tunneling based on the number of subdomains from single source IP address. You can configure up to six mappings.
Average Size, Maximum FQDNs	<p>Configure the average size of the subdomains and the maximum number of FQDNs. You can configure up to six mappings. The following are the default values:</p> <ul style="list-style-type: none"> <li>◦ FQDN size—1, maximum number of FQDNs—200</li> <li>◦ FQDN size—20, maximum number of FQDNs—160</li> <li>◦ FQDN size—30, maximum number of FQDNs—120</li> <li>◦ FQDN size—40, maximum number of FQDNs—80</li> <li>◦ FQDN size—50, maximum number of FQDNs—50</li> </ul>

- FQDN size—60, maximum number of FQDNs—30

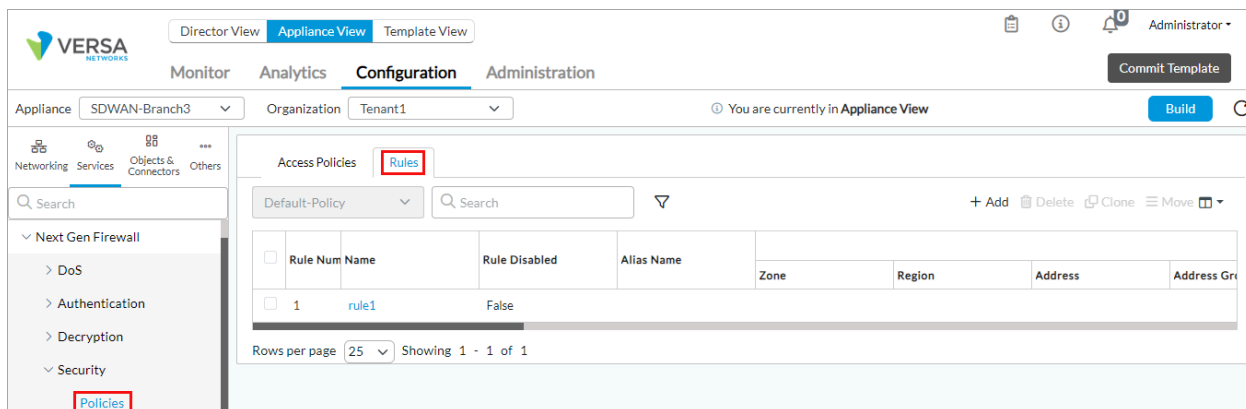
- Click OK.
- Enable DNS filtering in the security access policy rule to enforce DNS filtering. For more information, see [Configure Access Rules in Configure NGFW](#).

## Apply a DNS-Filtering Profile in an Access Policy

You can apply a predefined or custom DNS-filtering profile to a rule in a security access policy. To define and configure a security access policy, see [Configure Security Access Policy Rules](#).

To apply a DNS-filtering profile to an access policy rule:

- In Director view:
  - Select the Administration tab in the top menu bar.
  - Select Appliances 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 an access policy rule. The Edit Rule popup window displays.

**Edit Rule - rule1**

General Source Destination Headers/Schedule Applications/URL IoT Security Users/Groups **Enforce**

Actions | Log

**Actions**  
☐ Allow ☐ Deny ☐ Reject ☒ **Apply Security Profile**

**Set-Type**  
☒ Public ☐ Private ☐ None

Synced Flow: --Select-- Session Timeout (secs):  ☐ Send TCP Keep Alive at Session Timeout

☒ **Profiles** ☐ Profile Groups

☐ IP Filtering --Select-- 
 ☐ Antivirus --Select-- 
 ☐ File Filtering --Select--  
☐ Vulnerability --Select-- 
 ☐ URL Filtering --Select-- 
 ☒ **DNS Filtering** --Select--  
☐ Predefined Vulnerability Profile Override --Select-- 
 ☐ CASB Profile --Select-- 
 ☐ DLP Profile --Select--  
☐ ATP Profile --Select--

**OK** **Cancel**

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

## Monitor DNS Filtering

To monitor the DNS filtering that you associate with an access policy, you view the statistics about where and when the policy is used. For more information, see [Monitor Device Services](#).

To monitor DNS-filtering profiles:

1. In Director view:
  1. Select the Administration tab in the top menu bar.
  2. Select Appliances in the left menu bar.
  3. 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 a tenant in the left menu bar.

4. Select the Services tab.
5. Select NGFW > DNS Filtering. The DNS filtering statistics display.

The screenshot shows the Versa Networks Appliance View interface. The top navigation bar includes 'Director View', 'Appliance View' (selected), and 'Template View'. The main menu has 'Monitor', 'Analytics', 'Configuration', and 'Administration'. The 'Administration' tab is active, showing 'Summary', 'Devices', and 'Cloud Workload'. The 'Devices' section shows 'Total Appliances: 9' and a search filter for 'SDWAN-Branch3'. The device details for 'SDWAN-Branch3' are displayed, including its location, management address, and system bridge address. The 'Services' tab is selected, showing a list of services: 'SDWAN', 'NGFW' (highlighted), 'CGNAT', 'Secure Access', 'SDLAN', 'IPsec', 'Sessions', 'SCI', and 'APM'. The 'NGFW' service is expanded, showing a list of sub-services: 'Antivirus', 'ATP', 'Authentication Policies', 'CASB', 'Cloud File Export', 'Decryption', 'DLP', 'DNS Filtering' (highlighted), 'DoS Policies', 'File Filtering', 'IP Filtering', and 'Microsegmentation'. The 'DNS Filtering' sub-service is selected, showing a 'Predefined - Statistics' dropdown and a search bar. Below the search bar is a table with the following columns: 'DNS Profile N...', 'Blacklist Hit', 'Whitelist Hit', 'URL Filtering ...', 'IPf Hit', 'Newly Observ...', 'DNS Tunnel D...', 'DNS Tunnel Hit', 'DNS Invalid C...', 'DNS Request ...', 'DNS Response...', 'DNS Incomple...', and 'DNS A Count'. The table contains one row of data with all values set to 0.

## Display DNS-Filtering Threat Logs

To display the DNS-filtering threat logs:

1. In Director view, select the Analytics tab from the top menu bar. The view changes to Analytics view.
2. Select Home > Logs > Threat Filtering in the left menu bar.
3. Select the DNS Filtering tab to display information about the DNS filtering threat logs.

The screenshot shows the Versa Networks Analytics view interface. The top navigation bar includes 'Director View', 'Appliance View', and 'Template View'. The main menu has 'Monitor', 'Configuration', 'Workflows', 'Administration', and 'Analytics' (selected). The 'Analytics' tab is active, showing 'Threat Filtering Logs > DNS Filtering >'. The left sidebar has 'Dashboard', 'Logs', 'Reporting', and 'Admin'. The 'Logs' section is selected, showing a list of log types: 'URL Filtering', 'IP Filtering', 'File Filtering', 'DNS Filtering' (highlighted), and 'CASB'. The 'DNS Filtering' log type is selected, showing a 'DNS Filtering Logs' section. The 'DNS Filtering Logs' section has a 'Show Domain Names' checkbox and a search bar. Below the search bar is a table with the following columns: 'Receive Time', 'Appliance', 'Profile Name', 'Msg Type', 'EV Type', 'Action', 'Domain', 'Rule Name', 'Bad Resolved Addr', 'Bad C Name', and 'Domain Reputati'. The table contains one row of data with all values set to 0.

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

Updated: Wed, 23 Oct 2024 08:18:39 GMT

Copyright © 2024, Versa Networks, Inc.



---

## Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 22.1.3 and later allow configuration of tunnel detection parameters in a DNS-filtering profile and the sinkhole action.

---

## Additional Information

[Apply Log Export Functionality](#)

[Configure DNS Proxy](#)

[Configure DNS Servers](#)

[Configure IP Filtering](#)

[Configure Log Export Functionality](#)

[Configure NGFW](#)

[Configure Security Profile Groups](#)

[Configure Stateful Firewall](#)

[Configure URL Filtering](#)

[Configure User and Group Policy](#)

[Configure User-Defined Actions](#)

[Monitor Device Services](#)