

---

## Configure DNS Proxy for Concerto

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

A DNS proxy intercepts incoming Domain Name System (DNS) requests from a client and redirects them to a DNS server. The DNS server then resolves the DNS queries either using information in its DNS cache or by forwarding requests to other DNS servers.

You can configure a Concerto device to act as a DNS proxy. To do this, you create a DNS proxy profile that defines the DNS resolvers to use to resolve the domain names received in DNS requests, and you define which interfaces and source NAT (SNAT) pools to use to reach the DNS resolvers. You then create DNS profiles that define the domain name patterns and types to be resolved by a DNS proxy profile, and DNS then associates these profiles with DNS policies.

You can configure multiple DNS servers to ensure that incoming DNS requests are sent to the appropriate DNS server or servers. For example, the DNS path selection mechanism can send corporate DNS queries to a corporate DNS server while sending other queries to the ISP's DNS servers.

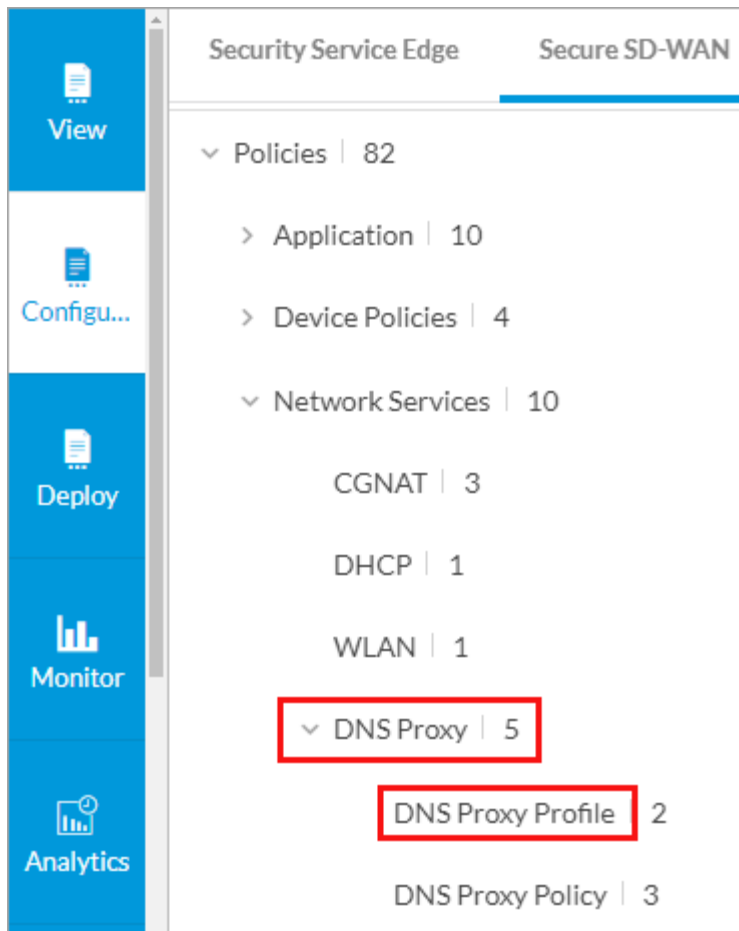
To direct incoming DNS requests to other DNS servers, you create a redirection rule in a DNS policy, and you then associate a DNS proxy profile with the rule. You can configure multiple redirection rules. You can also configure a redirection rule that responds to a domain name with a static IP address.

---

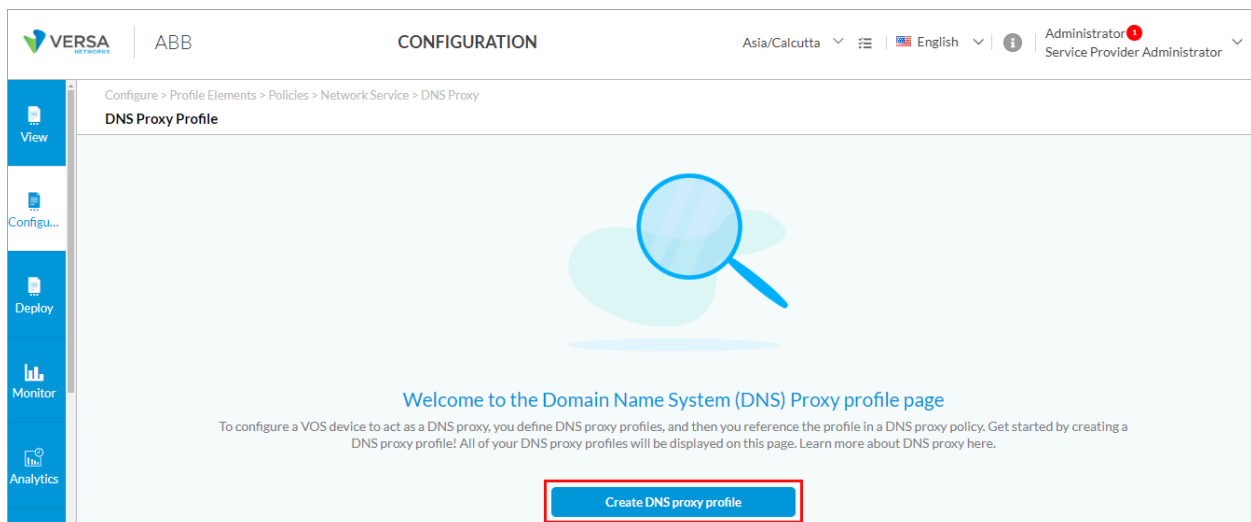
## Configure DNS Proxy Profiles

To configure DNS proxy profiles:

1. From the Tenants screen, select the tenant for which you want to configure DNS proxy profiles.
2. Go to Configure > Secure SD-WAN > Profile Elements > Policies > Network Services > DNS Proxy > DNS Proxy Profile.



The DNS Proxy Profile main screen displays.



3. If there are no existing profiles, click Create DNS Proxy Profile or click + Add. The Add DNS Proxy Profile window displays.

Add DNS Proxy Profile ✕

1  
Availability Mode
2  
Resolver
3  
Permissions
4  
Review & Submit

Select which mode to use to check the availability of the server.

**Availability Mode**

☐ Failover (default)  
DNS failover helps websites or network services remain accessible in the event of an outage.

☐ Round Robin  
Round-robin load distribution ensures that traffic is routed to each redundant endpoint randomly to ensure that no one endpoint receives more traffic than the other endpoints.

Cancel
Skip to Review
Next

4. In Step 1, Availability Mode, select the mode to use to check the availability of the server:
  - Failover (default)—Click to redirect the traffic through another resolver if the resolver fails or is not reachable. This is the default.
  - Round Robin—Click to use a round-robin method to distribute traffic among the resolvers. This ensures that no one endpoint receives more traffic than the other endpoints.
5. Click Next to go to Step 2, Resolver, to add DNS resolvers.

Add DNS Proxy Profile ✕

✓ Availability Mode
 2  
Resolver
3  
Permissions
4  
Review & Submit

Add resolvers for your domain names to receive in DNS requests.

Resolvers (0) 
[+ Add](#)
Delete
Select Columns ▼

Name	Mode	Type	Site / Network Name	DHCP Server Monitor	Servers
No Data					

Cancel
Back
Skip to Review
Next

- a. In the Resolver table, click the + Add icon. The Add Resolver Rule popup window displays.

Add Resolver Rule

1
Settings
2
DHCP Server Monitor
3
DNS Servers
4
Review & Submit

### Resolver Type

Choose which resolver type to use.

☒ Site
☐ Network

Appliance Name

Select

Mode

Select which mode to use to check the availability of the server.

☒ Failover (default)  
DNS failover helps websites or network services remain accessible in the event of an outage.

☐ Round Robin  
Round-robin load distribution ensures that traffic is routed to each redundant endpoint randomly to ensure that no one endpoint receives more traffic than the other endpoints.

Cancel
Skip to Review
Next

b. In Step 1, Settings, enter information for the following fields.

Field	Description
Site	Click, and then in the Appliance Name field, select an SD-WAN site from to w site name is commonly used to optimize direct internet access (DIA) and direc
Network	Click, and then in the Network field, select which local WAN or LAN networks <div> <h3>Resolver Type</h3> <p>Choose which resolver type to use.</p> <p> <input type="radio"/> Site <input checked="" type="radio"/> Network </p> <p>Network</p> <div> Select </div> </div>
Mode	<p>Select the mode to use to check the availability of the DNS server:</p> <ul style="list-style-type: none"> <li>Failover—Click to redirect the traffic through another resolver server if the This is the default.</li> <li>Round-robin—Click to use a round-robin method to send traffic among the</li> </ul>

	<i>Default:</i> Failover
--	--------------------------

- c. Click Next to go to Step 2, DHCP Server Monitor, to configure a server monitor for the server assigned by Dynamic Host Configuration Protocol (DHCP). Enter information for the following fields.

Field	Description
DHCP Server Monitor	DHCP server monitor is enabled by default. When a WAN on which DHCP is provider to resolve IP addresses, the DHCP server monitor checks whether the server is unreachable. To disable the server monitor, slide the toggle button to disable.
Domain Name	Enter the domain name for the DNS server.
Network	Enter the network used to derive the source interface.
Next Hop Site Name	Enter the name of the next-hop SD-WAN site.
Interval	Click and enter the interval between monitor packets, in seconds. <i>Default:</i> 1 <i>Value:</i> 1 through 60 seconds
Maximum Threshold	Enter the maximum number of monitor packet retransmissions before the no... <i>Default:</i> 1

	Value: 1 through 60
--	---------------------

- d. Click Next to go to Step 3, DNS Servers, to add DNS resolvers. Enter information for the following fields.

Add Resolver Rule

3
DNS Servers

Add one or more DNS servers for the resolver.

DNS Server Name

Enter a name

IP Address

Enter an IPv4 or IPv6 address

Port

0

Monitor Object

Select

+

Cancel

Back

Skip to Review

Next

Field	Description
DNS Server Name	Enter a name for the DNS server.
IP Address	Enter the IPv4 or IPv6 address of the DNS server.
Port	Enter the port number to use to connect to the DNS server.
Monitor Object	<p>Select a monitor object to evaluate the state of the IP addresses configured when checking the availability of the DNS server using the method configured. If the result of the evaluation, the traffic is sent accordingly. Click the <span>+</span> Add icon to add a new monitor object.</p> <p>If you do not select a monitor object, all the IP addresses configured in the resolver will be in the actual status.</p>

- e. Click the + Add icon to add one or more DNS servers.
- f. Click Next to go to Step 4, Review and Submit, to review the information.

**Add Resolver Rule**

✓ Settings
✓ DHCP Server Monitor
✓ DNS Servers
4 Review & Submit

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

**General**

Name

Description

Tags

**Settings** [Edit](#)

Resolver Type

Type

Appliance Name

Mode

Site

Fallover

**DHCP Server Monitor** [Edit](#)

Enabled ☐

Domain Name

Network

Nexthop Site Name

Interval

Maximum Threshold

**DNS Servers** [Edit](#)

Name	IP Address	Port	Monitor Object
<input type="text"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text"/>

Cancel
Back
Save

- g. In the General section, enter a name for the DNS resolver and, optionally, a description.
  - h. For all other sections, review the information. To make changes, click the [Edit](#) icon.
  - i. Click Save.
6. Click Next to go to Step 3, 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 DNS Proxy Profile ✕

Availability Mode ✓ Resolver ✓ **Permissions 3** Review & Submit 4

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

Cancel Back Skip to Review Next

- Click Next to go to Step 4, Review and Submit, to review the information.



**Add DNS Proxy Profile**

✓ Availability Mode

✓ Resolver

✓ Permissions

4 Review & Submit

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

**General**

Name  Description

Tags

Press Enter to add

**Availability Mode** [Edit](#)

Availability Mode ROUNDROBIN

**Rules** [Edit](#)

Resolvers (0) Select Columns ▼

Name	Mode	Type	Site / Network Name	DHCP Server Monitor	Servers
No Data					

**Permissions** [Edit](#)

Enterprise Administrator	Edit
Service Provider Administrator	Edit
Service Provider Operator	Read
Enterprise Operator	Read

Cancel

Back

Save

- In the General section, enter a name for the DNS proxy profile and, optionally, a description.
- For all other sections, review the information. To make changes, click the [Edit](#) icon.
- Click Save.

## Configure DNS Policies

To direct incoming DNS requests to other DNS servers, you create DNS policies and add redirection rules. You can associate a DNS proxy profile with a DNS redirection rule if you select proxy settings as DNS action for a redirection rule

To configure a DNS policy:

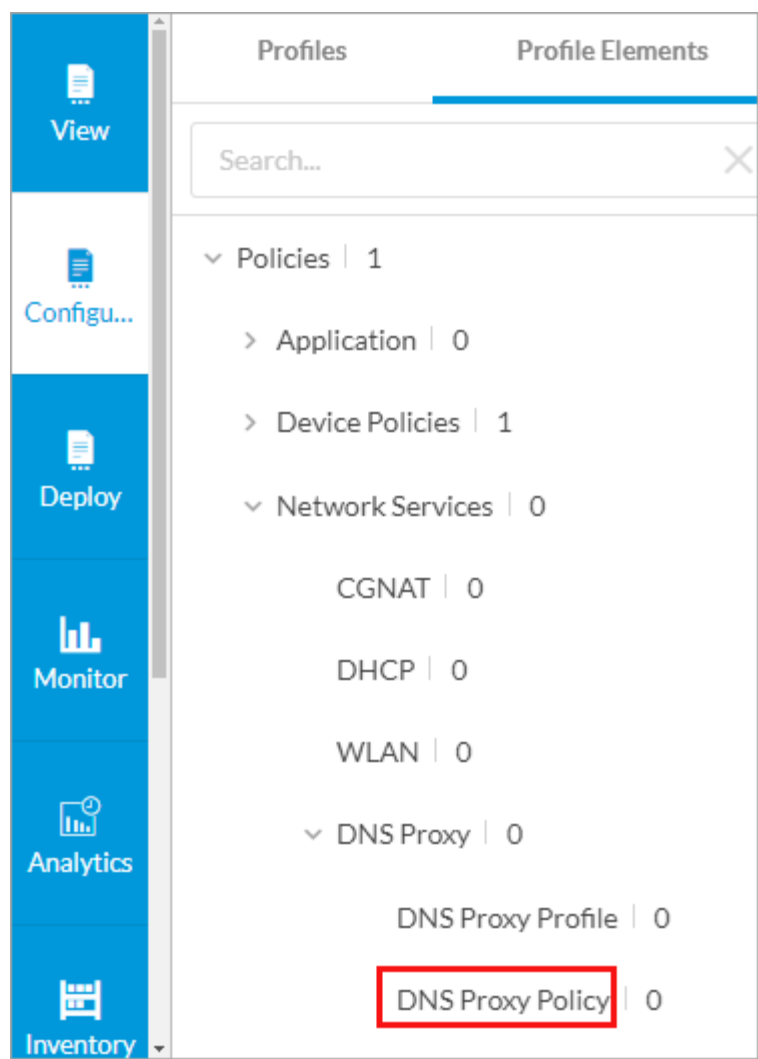
- From the Tenants screen, select the tenant for which you want to configure DNS proxy policies.

[https://docs.versa-networks.com/Secure\\_SD-WAN/02\\_Configuration\\_from\\_Concerto/Secure\\_SD-WAN\\_Configuration/Config...](https://docs.versa-networks.com/Secure_SD-WAN/02_Configuration_from_Concerto/Secure_SD-WAN_Configuration/Config...)

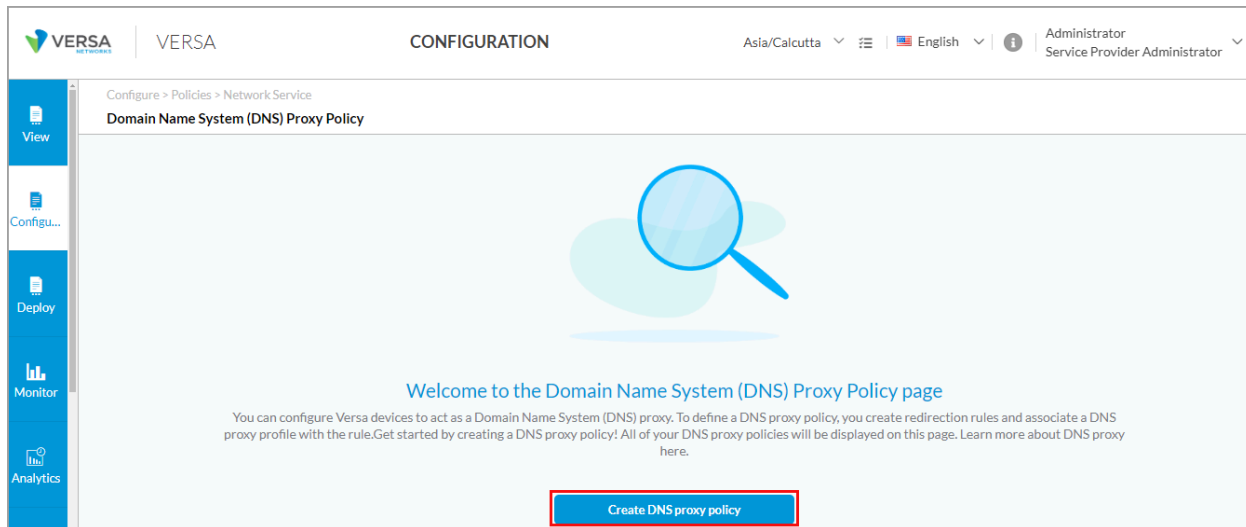
Updated: Wed, 23 Oct 2024 08:03:21 GMT

Copyright © 2024, Versa Networks, Inc.

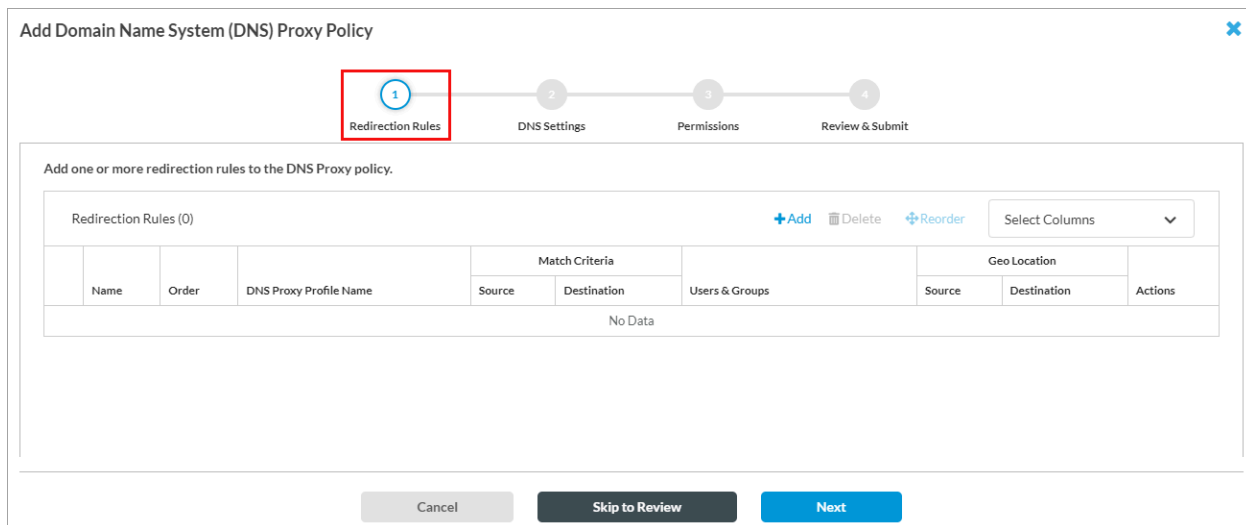
2. Go to Configure > Secure SD-WAN > Profile Elements > Policies > Network Services > DNS Proxy > DNS Proxy Policy.



The Domain Name System (DNS) Proxy Policy main screen displays.



3. If there are no existing profiles, click Create DNS Proxy Policy or click + Add. The Add Domain Name System (DNS) Proxy Policy window displays.



4. In Step 1, Redirection Rules, click + Add to add a redirection rule. The Add Redirection Rule popup window displays. By default, all source and destination traffic is included. You can specify the source and destination addresses and zones from which traffic originates.

### Add Redirection Rule

1 2 3 4 5 6

Source & Destination Zone Users & Groups Source Geo Location DNS Headers DNS Action Review & Submit

Define how traffic originates and directed using source and destination zones and IP addresses.

Source Address Destination Address Source Zones Destination Zones

+ Add Variable

Search or select from list


Name	Addresses
<input type="checkbox"/> Address-Group1	10.1.1.2-10.1.1.10, 10.2.1.0/24

Showing 1-1 of results 10 Rows per Page Go to page 1 < Previous 1 Next >

IP Address or IP Range + Add Variable IP Subnet + Add Variable IP WildCard + Add Variable

Enter IP address or range Enter a list of IPv4/IPv6 Subnet values Enter a list of wildcard values

Cancel Skip to Review Next

- Select a source address group from which traffic originates, or use the search box to find a source address group. You can click + Add Variable to create a variable for the source address. Enter a name for the variable, click the  Plus icon, and then click Add. You can add multiple variables before clicking the Add button.


Add Variable

\$

- +

Cancel Add

You can also enter values for the IP address or IP range, IPv4 or the IPv6 subnet, or the IP wildcard for the rule to match. To create variables for these values, click + Add Variable for that field. You can add multiple variables for each field.

- To add a variable for the IP address or IP range, select IPv4 Address, IPv4 Range, or IPv6 Address in the drop-down list, click the  Plus icon, the click Add.

- To add a variable for the IP subnet, select IP Subnet or IPv6 Subnet in the drop-down list, click the Plus icon, then click Add.

- To add a variable for the IP wildcard, enter a name for the variable, click the Plus icon, and then click Add.

6. Click the Destination Address tab, select a destination address group from which traffic originates, or use the search box to find a destination address group. You can also enter values for the IP address or IP range, IPv4 or the IPv6 subnet, or the IP wildcard for the rule to match. You can click + Add Variable to create variables for these values. For more information on adding variables, see step 5.

7. Select the Source Zone tab. In the Source Zones field, click the down arrow, and then select one or more zones.  
To create a variable for the source zone, click **+** Add Variable.

Define how traffic originates and directed using source and destination zones and IP addresses.

Source Address   Destination Address   **Source Zones**   Destination Zones

Source Zones **+** Add Variable

Search or select from list

8. Select the Destination Zone tab, and then enter the information for the destination zone. The fields are the same as for the Source Zone, described above.
9. Click Next to go to Step 2, Users and Groups. By default, all users and groups are included. To customize the specific users or groups to be included, enter the following information.

Add Redirection Rule

Source & Destination Zone   **Users & Groups**   Source Geo Location   DNS Headers   DNS Action   Review & Submit

By default we have chosen all users and groups to apply your security enforcements If you prefer, you can select the specific users or groups for the security posture.

**Users & Groups**

Enable Rule for the following matched users or user groups

User Type

☒ All Users   ☐ Known Users   ☐ Unknown Users   ☐ Selected Users

Cancel   Back   Skip to Review   Next

10. Select the user type to match from All Users, Known Users, Unknown Users, and Selected Users.
11. If you select Selected Users, the following options display.

Enable Rule for the following matched users or user groups

**User Type**

☐ All Users
 ☐ Known Users
 ☐ Unknown Users
 ☒ Selected Users

Select Users & Groups Profile ▼

**User Groups** Users

Search for User Groups

▼ User Groups (0)

Name	Distinguished Name (DN)
------	-------------------------

12. Select a Users and Groups Profile. For more information, see [Configure User and Device Authentication](#).
13. Select the User Groups tab to search for and select user groups.
14. Select the Users tab to search for and select users.

Enable Rule for the following matched users or user groups

**User Type**

☐ All Users
 ☐ Known Users
 ☐ Unknown Users
 ☒ Selected Users

Select Users & Groups Profile ▼

User Groups **Users**

Search for Users

▼ Users (0)


User Name	First Name	Last Name
-----------	------------	-----------

15. Click Next to go to Step 3, Source Geo Location, to specify the geographic regions for source and destination traffic source.
  - a. On the Source Address tab, click Select Country to select one or more countries.
  - b. Click the Destination tab, and then click Select Country to select one or more countries.

16. Click Next to go to Step 4, DNS Headers, to define DNS operation codes and matching criteria for incoming packets.

17. In the Operating Code field, select the type of DNS opcode to which the rule applies:
  - IQuery—Send a request for an inverse DNS query command.
  - Notify—Send a request for a DNS notify command.
  - Query—Send a request for a DNS query command.
  - Status—Send a request for a DNS status command.
  - Update—Send a request for a DNS update command.

For each request type, you must enter additional information, as described in the following steps.

18. If you select the IQuery request type, enter IPv4 or IPv6 addresses to which to send an inverse query. Click the  to add one or more IP addresses.



Operation Code (OPCodes)

iQuery

IP Address

Enter IPv4 or IPv6 address

19. If you select the Query request type, enter information for the following fields.

Operation Code (OPCodes)

Query

Query Type

Select

Domain Name


Enter domain name

☐ Negate

Field	Description
Query Type	<p>Select the DNS resource record (RR) types to query:</p> <ul style="list-style-type: none"> <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>AXFR—Asynchronous Transfer Full Range</li> <li>CAA—Certification Authority Authorization</li> <li>CERT—Certificates</li> <li>CNAME—Canonical name for an alias</li> <li>DHCID—DHCP ID</li> <li>DNSKEY—DNS key</li> <li>DS—Delegation signer</li> <li>EID—Endpoint identifier</li> <li>GPOS—Geographical position</li> <li>HINFO—Host information</li> </ul>

- 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
- MR—Mail rename domain name
- 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
- OPT—Options
- PTR—Domain name pointer
- PX—X.400 mail mapping information
- RKEY—Record key
- RP—Responsible person
- RRSIG—Resource resource digital signature
- RT—Route through
- SIG—Security signature
- SINK—Kitchen sink
- SOA—Marks the start of a zone of authority
- SPF—Sender policy framework



	<ul style="list-style-type: none"> <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>
Domain Name	Enter the domain name.
Negate	Click to apply the rule to any query type and domain name, except those selected.


20. If you select the Notify or Status request type, click the  Add icon to add zone names.

Operation Code (OPCodes)

Status ▾

DNS Zones






21. If you select the Update request type, click the  Add icon to add domain names.

Operation Code (OPCodes)

Update ▾

Domain Name

22. Click Next to go to Step 5, DNS Action, to define the proxy settings for the rule.

**Add Redirection Rule**

Match Criteria

Source & Destination Zone Users & Groups Source Geo Location DNS Headers **DNS Action** Review & Submit

Select which action to take when a DNS rule matches. Each action has a set of settings. If no action is taken, you can choose to use a proxy profile for proxy settings or a set of public IP addresses for server settings.

**Actions**

☒ None ☐ Use proxy settings ☐ Use server settings

☒ Enable Logging

Cancel Back Skip to Review Next

23. To take no action, select None (this is the default). By default, the Enable Logging toggle button is enabled. Slide the toggle button to disable logging.
24. If you select Use Proxy Settings, enter information for the following fields.

**Actions**

☐ None ☒ Use proxy settings ☐ Use server settings

☒ Enable Logging

**DNS Proxy Profile**

--Select--

**Number of Domains to Cache** **DNS-64 Prefix**

0

**Cache TTL Upper Limit** **Seconds**

0

**Override Question**

☒ Only if IPv4 WAN Available

☒ Apply Policy Based Forwarding

Field	Description
Enable Logging	By default, the Enable Logging toggle button is enabled. Click to disable logs.
DNS Proxy Profile	Select a DNS proxy profile to associate with the redirection rule. For more info see <a href="#">above</a> .
Number of Domains To Cache	Enter the number of DNS domains to cache. The DNS server uses information from the cache to respond to queries. When a DNS domain entry in the DNS domain name cache times out depends on the TTL value as defined in the DNS protocol.  <i>Range: 0 through 65535</i>
DNS-64 Prefix	Enter the DNS extensions for network address translation from IPv6 clients to IPv4. For more info see <a href="#">Configure Profiles</a> .
Cache TTL Upper Limit	Enter the upper limit of the time to live for the network obfuscation cache, in seconds.
Override Question	Enter the domain name to have DNS proxy override the domain name in the query before it sends the query to the server. When DNS forwards the response, it replaces the domain name.
Only IPv4 WAN Available	Click when the WAN uses only IPv4. This option is disabled by default.
Apply Policy-Based Forwarding	Click to look up SD-WAN policy rules to determine the path on which to send traffic. This option is disabled by default.

25. If you select Use Server Settings, enter information for the following fields.

**Actions**

☐ None
☐ Use proxy settings
☒ Use server settings

☒ Enable Logging


IP Address

Enter IPv4 or IPv6 address

Monitor Object

--Select--

Field	Description
Enable Logging	By default, the Enable Logging toggle button is enabled. Click to disable logs.
IP Address	For type A/AAAA DNS queries only, enter the static IPv4 or IPv6 address to send traffic.

Monitor Object	<p>Select a monitor object to evaluate the state of the IP addresses configured in t checking the availability of the DNS server using the method configured in the M</p> <p>evaluation, the traffic is sent accordingly. Click the  Add icon to add a monitor</p> <p>If you do not select a monitor object, all the IP addresses configured in the reso actual status.</p>
----------------	--

26. Click Next to go to Step 4, Review and Submit, to review the information.

**Add Redirection Rule**

Source & Destination Zone   Users & Groups   Source Geo Location   DNS Headers   DNS Action   **Review & Submit**

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

**General**

Name  Description

Tags

Press Enter to add

**Source & Destination Traffic** [Edit](#)

**Users & Groups** [Edit](#)

Users & Groups

**Source & Destination Geo Location** [Edit](#)

**DNS Headers** [Edit](#)

Operation Code (OPCodes)

**DNS Action** [Edit](#)

Enable Logging Actions   Enabled SERVER

[Cancel](#) [Back](#) [Save](#)

- a. In the General section, enter a name for the DNS redirection rule and, optionally, a description.
  - b. For all other sections, review the information. To make changes, click the [Edit](#) icon.
  - c. Click Save.
27. In the Add Domain Name System (DNS) Proxy Policy window, click Next to go to Step 2, DNS Settings, to configure DNS cache details.

Add Domain Name System (DNS) Proxy Policy

Redirection Rules **DNS Settings** Permissions Review & Submit

The DNS cache is a temporary DNS storage on a device that contains DNS records of already visited domain names (A records for IPv4 addresses, AAAA records for IPv6, etc.). It keeps those records, depending on their time-to-live (TTL). Choose whether to enable DNS cache.

☒ Enable Domain Cache

Cache Size  Maximum TTL  Seconds

Cancel Back Skip to Review Next

- a. By default, the Enable Domain Cache toggle button is enabled. Click to disable domain cache.
- b. Enter the domain cache size and the maximum TTL to cache (in seconds). When a DNS domain entry in the DNS domain name cache times out depends on the TTL value in the DNS response, as defined in the DNS protocol.

28. Click Next to go to Step 3, Permissions.

Add Domain Name System (DNS) Proxy Policy

Redirection Rules DNS Settings **Permissions** Review & Submit

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 <input type="checkbox"/>
Service Provider Administrator (Inherited)	Edit <input type="checkbox"/>
Service Provider Operator (Inherited)	Read <input type="checkbox"/>
Enterprise Operator (Inherited)	Read <input type="checkbox"/>

Cancel Back Skip to Review Next

29. Change the permissions for one or more roles, if needed.
30. Click Next to go to Step 4, Review and Submit, to review the information.



Add Domain Name System (DNS) Proxy Policy

✓ ✓ ✓ 4  
 Redirection Rules DNS Settings Permissions Review & Submit

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

**General**

Name Description

	Name	Order	DNS Proxy Profile Name	Match Criteria		Users & Groups	Geo Location		Actions
				Source	Destination		Source	Destination	
No Data									

**DNS Settings** [Edit](#)

IP to Domain Cache

Enabled Yes

Cache Size

Maximum TTL

**Permissions** [Edit](#)

hideparant	Edit
Enterprise Administrator	Edit
Service Provider Administrator	Edit
Service Provider Operator	Read
Enterprise Operator	Read

Cancel Back Save

31. In the General section, enter a name for the DNS proxy policy and, optionally, a description.
32. For all other sections, review the information. To make changes, click the Edit icon.
33. Click Save.

## Supported Software Information

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

## Additional Information

[Configure Profiles](#)

[Configure User and Device Authentication](#)