

---

## Configure DNS Proxy with SD-WAN Traffic Steering for DIA

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

When you configure a Versa Operating System™ (VOS™) device to act as a DNS proxy, the VOS device can intercept incoming DNS requests from a client and redirect them to a DNS server. In the case of direct internet access (DIA), SD-WAN policies determine which applications use local breakout, and how. For example, if a branch has multiple internet circuits, the application traffic can be load-balanced among them, or you can configure policies so that an application uses the best performing circuit. In the same way that application traffic is subject to SD-WAN policies for DIA path selection, the DNS queries for the application can be subject to path selection via SD-WAN policies, ensuring path affinity between the DNS queries and subsequent application traffic. That is, instead of sending all DNS name requests to a centralized DNS server, you can configure split DNS to control which DNS requests from a branch are handled by a centralized enterprise (internal) DNS server and which are sent directly from a branch to the internet to be processed by a public (external) DNS server.

To configure split DNS and to configure path affinity between the DNS queries on behalf of an application and the subsequent application traffic itself, you configure the DNS proxy to consult an SD-WAN traffic-steering policy when deciding how to forward DNS queries.

By default, the paths used for sending a DNS query request and for sending application traffic are selected independently, and it is possible that two different paths can be chosen. This behavior is called *loose DNS path affinity*. For most enterprises and applications, loose DNS path affinity provides acceptable performance for SaaS and other applications. To fine-tune the application performance, you can send the DNS queries for an application, as well as the subsequent application traffic, on the same path. This behavior is called *strict DNS path affinity*.

The DNS proxy uses the VOS domain application cache, which maps domain names to applications, to look up the SD-WAN policy rule corresponding to a particular domain name, in order to subject the DNS query to the same path selection criteria as the subsequent application traffic.

If you use internet and cloud-based SaaS and other applications, it is strongly recommended that you configure DNS proxy.

---

## DNS Proxy and Split DNS Overview

When an application needs to resolve a domain name, it can do so in one of the following ways:

- Send all DNS requests to a centralized enterprise (internal) DNS server. This server is typically located behind a

hub device in a data center or at corporate headquarters.

- Have some DNS requests exit locally so that the domain name can be resolved by a public DNS server. Because public DNS servers use geolocation to resolve DNS requests, they can resolve the DNS query an address that is geographically close to the request's origin site.

To understand what happens when all an enterprise's DNS request are sent to a centralized enterprise DNS server, let's consider two cases. In one, the request is coming from a branch in San Jose and the enterprise DNS server is in San Francisco. Let's say the request is from the Salesforce application and there's a Salesforce application server in Mountain View. If all DNS requests go to the enterprise DNS server, the enterprise DNS server might resolve the request to a server in San Francisco, which is not too far from San Jose. However, let's consider a second case, where the branch making the DNS request is in New York. Its DNS requests would be resolved by the DNS server in San Francisco and then might resolve to a Salesforce server in San Francisco rather than to a server closer to New York.

Internet access is handled in one of the following ways:

- Use routing—This is basic, standard routing, with no policy of any kind. To perform standard routing for internet access, VOS devices run EBGp between transport (WAN) links and the LAN, and they use the routing information learned from BGP to build the entries in the route table and to route traffic. When a branch has two WAN links, you can set up routing to run in failover mode so that if the primary WAN link fails, traffic automatically switches to the secondary link and there is no interruption in service. For example, you can configure a branch devices to import routes from the higher-bandwidth provider (here, Comcast) and then fail over to the lower-bandwidth provider (here, ATT)
- Override routing with policy towards egress—Routing policy consists of rules that allow you to control how to handle specific types of traffic. For example, you can create a policy that has application-specific rules. So if you import default routes only from your higher-bandwidth provider, one policy rule can direct high-bandwidth and business traffic (high priority) to that provider and a second policy rule can direct low-priority traffic, such as games, to the lower-bandwidth provider. As a second example, instead of allowing internet access from an enterprise only at headquarters because security is done there (called central breakout, or CBO), you can create policy to do central breakout for all traffic except for critical applications, and for critical applications, such as Salesforce and Office365, the policy does local breakout (LBO), which provides direct internet access (DIA) from the branch to the public internet.

Regardless of which method you use to handle internet access, it is recommended that you configure DNS proxy, and it is further recommended that you implement split DNS. With split DNS, you can

- Resolve internal domain names using the enterprise DNS server.
- Resolve external domain names using DIA to reach an external DNS server. When you use an external DNS server, you can:
  - Resolve the name using a public DNS server.
  - For each internet link on the VOS device, you can use the DNS server of the service provider. For example, if a VOS device has two internet circuits, one from Comcast and one from AT&T, you can create a configuration to have traffic that is to be sent over the Comcast circuit use the Comcast DNS server and traffic that is to be sent over the AT&T circuit to use the ATT DNS server. You can configure the DNS servers statically, or if the links receive their IP addresses from DHCP, you can use the DNS servers provided by DHCP.

You implement split DNS by creating DNS redirection rules. In the simplest case, you can do this by creating two rules. Continuing with the example in the previous paragraph, the rules would conceptually achieve the following:

- Rule 1—Match domain name pattern "\*.my-company.com", and use the DNS resolver 10.48.0.99. This rule

matches all internal names for my-company.

- Rule 2—Match all other names, that is, all external domain names, and use the resolvers associated with the Comcast and AT&T circuits, or use the resolver 8.8.8.8.

To optimize the performance of SaaS and other applications, you can configure the path that the application traffic follows based on the path that the DNS query followed, in one of two ways:

- DNS query path selection—Consult SD-WAN policies when determining the path over which the DNS query should be sent. You do this by enabling the honor PBF setting in the DNS rule that matches external domain names. Doing this means that the same criteria that are used to select a path for the application traffic get used to select a path for the DNS query.  
For example, if the policy rule specifies that traffic for the application Salesforce should prefer the Comcast circuit instead of the AT&T circuit, the same policy rule applies to the DNS traffic as well, and the DNS query for a Salesforce domain name is sent over the Comcast circuit instead of the AT&T circuit. This method achieves loose path affinity, because it does not guarantee that the same path is used for the DNS query and the application traffic. For example, if the policy rule specifies that Salesforce traffic should use either the Comcast or the AT&T circuit and should fail over to an LTE circuit if both the Comcast and AT&T circuit are down, it is possible that the DNS query uses the Comcast circuit and the application traffic uses the AT&T circuit. However, this is reasonable in most cases, because both are direct internet access paths.
- DNS resolution-based path affinity—Steer all client-initiated sessions that follow the DNS query over the same path on which the DNS query was sent. This achieves strict path affinity, because it guarantees that the DNS query and the application traffic always use the same path. In VOS software Releases 21.1 and later, you configure strict path affinity on a per-SD-WAN rule basis. In earlier VOS releases prior, you configure strict path affinity by configuring application steering as a global setting for an organization.

For standard routing, you need split DNS for two main reasons. First, external DNS servers cannot resolve internal addresses. For example, the public Google or Cloudflare DNS server cannot resolve the address finance.my-company.com. Second, a random external DNS server might provide less-than-optimal resolution for a public domain, such as Salesforce. To handle these two cases, you can configure a DNS proxy with two rules:

- Rule 1—Match the domain name \*.my-company.com, and the action is to use the enterprise DNS server (for example, 10.48.0.99)
- Rule 2—No match is required (that is, match any external name), and the action is to use an external DNS server (for example, the Google DNS server at 8.8.8.8)

When choosing which interface to use for external DNS queries, if a WAN interface receives its IP address via DHCP, the DHCP server commonly provides the IP address of the DNS server. You can override this with a policy that sends the DNS query out a specific WAN interface. One case for doing this might be if the default route comes from the centralized SD-WAN hub, but you might want to policy to have Salesforce and Office365 traffic do local breakout. And if you create a policy for Salesforce to do local breakout, you might also want DNS queries related to Salesforce to do local breakout. Here are examples of policy rules for controlling these traffic flows:

- Rule 1—Same as above: match the domain name \*.my-company.com, and the action is to use the enterprise DNS server (for example, 10.48.0.99)
- Rule 2—Associate two DNS resolvers with the two WAN providers:
  - Associate one resolver with the higher-bandwidth link (10.48.0.99 or 8.8.8.8), and enable honor policy-based forwarding. With honor policy-based forwarding, when you apply policy-based forwarding in a redirection rule in a DNS profile, DNS proxy forwarding checks SD-WAN policies to select the path for the DNS query and the onward connection to the application server.

- Associate one resolver with the lower-bandwidth link (8.8.8.8), and enable honor policy-based forwarding.

Here are some examples for how these rules are applied to traffic bound to different destinations and applications:

- Yahoo.com—DNS request to yahoo.com matches Rule 2.
  - DNS request is sent to the DNS server at either 10.48.0.99 or 8.8.8.8.
  - Because honor policy-based forwarding is enabled, the decision regarding which of the two DNS servers to use is sent to the SD-WAN traffic-steering policy, and the appropriate policy rule is used to decide which DNS server to send the request to. Let's say the DNS query goes to the centralized enterprise server, 10.48.0.99
- Yahoo.com—Subsequent browser traffic to Yahoo
  - Traffic flow consults the SD-WAN traffic-steering policy.
  - Policy can select either the higher-bandwidth or the lower-bandwidth provider for the browser traffic. This is called *loose path affinity*. Loose path affinity is available for Releases 16.1R2 and later.
- Salesforce—DNS request to salesforce.com matches Rule 2.
  - Matches the rule for Salesforce, which specifies the DNS resolver 8.8.8.8 using the higher-bandwidth provider.
- Salesforce—Subsequent application traffic
  - Traffic follows the SD-WAN traffic-steering policy.
  - Loose path affinity—Policy can select either the higher-bandwidth or the lower-bandwidth provider for the browser traffic. Local egress can go through either WAN link. For most enterprise settings, loose path affinity is an acceptable behavior.
  - Strict path affinity—You might want the application traffic to follow the same path as the DNS query; that is, you might want the DNS query and the application traffic to use the same WAN link. This is called *strict path affinity*. You can configure this only globally, for all a tenant's DIA egress requirements. Strict path affinity is available for Releases 21.1.0 and later.

To allow DIA to work, you must configure CGNAT address pools to define the IP addresses to use when translating between private and public IP addresses and to specify the NAT mode to use to translate private addresses to public addresses.

The path to the DNS server is determined by the SNAT pool configured in the profile. For example, if the pool is associated with WAN interface WAN1, the DNS query can be forwarded only through that WAN interface. For Releases 21.1.0 and later, you can enable honor policy-based forwarding in a DNS proxy profile to indicate that SD-WAN rules should be looked up to determine the path on which to send the DNS query. For this to work, a DNS resolver must be available for each path that policy-based forwarding can send the traffic on.

---

## Caches for Applications and Domain Names

The VOS domain name application cache (DAC) maps domain names to applications and URL categories. On VOS devices, the domain name application cache is always enabled. For Releases 21.1, and later domain name application caches entries are retained for 5 days if they are not used. For releases prior to Release 21.1, cache entries are retained forever. Note that, for performance reasons, only the applications and URL categories that are being referenced by policy are cached. Being aware of the applications and URL categories for a domain name helps the VOS software subject DNS requests to the same path selection behavior as the HTTP traffic.

---

## Configure Selective Local Breakout in Conjunction with a Web Proxy

Large enterprises commonly have deployment shown in figure. All hosts access internet through web proxy behind a DC/hub location. However for some business critical apps you want to configure LBO from branch itself.



performance.

To configure the DNS query path selection, you enable honor policy-based forwarding in an HTTP/HTTPS proxy rule, and you then associate this rule with the DNS proxy rule that is used to resolve external domain names.

For example, if a client sends a DNS request for `www.salesforce.com`, the DNS proxy can look up the SD-WAN policy rule corresponding to application "salesforce". If that rule's action specifies that traffic should be sent over the higher-bandwidth circuit, the the DNS proxy sends the DNS query over that circuit and to the resolver that is associated with that circuit. That resolver could be a public resolver such as `8.8.8.8`, or it could be the one provided by service provider and inherited via DHCP for the service provider's circuit.

To configure DNS query path selection, you do the following:

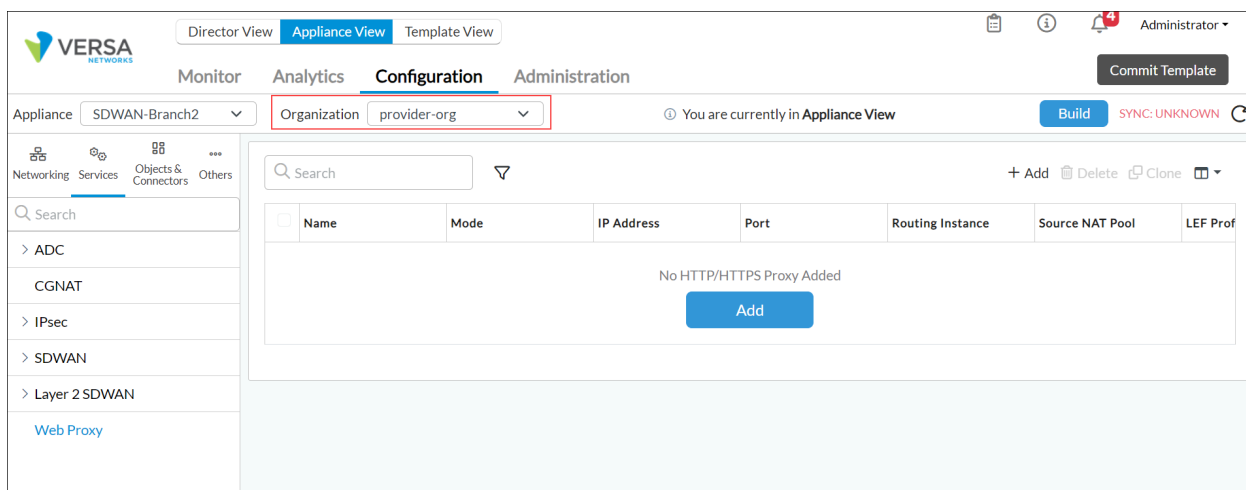
1. Configure an HTTP/HTTPS proxy. You can configure either a web proxy or a transparent explicit proxy.
2. Configure a DNS proxy.
3. Configure an SD-WAN traffic-steering forwarding profile and policy.

---

## Configure an HTTP/HTTPS Web Proxy

To configure DNS query path selection for an HTTP/HTTPS web proxy:

1. In Director view:
  - a. Select the Administration tab in the top menu bar.
  - b. Select Appliance in the left menu bar.
  - c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select an organization in the horizontal menu bar.
4. Select Services > Web Proxy in the left menu bar.



5. Click the + Add icon. The Add HTTP/HTTPS Proxy popup window displays.

6. Select the General tab.

Add HTTP/HTTPS Proxy

General

Cookie Based User Identification

Rules

Name \*

Description

Mode \*

--Select--

IP Address

Port \*

+

↗

Port Not Configured

Routing Instance

0 selected

0 selected

Provider Organization

--Select--

DNS Redirection Policy

--Select--

+ DNS Redirection Policy

Source NAT Pool

--Select--

+ SNAT Pool

☐ SNAT Pool Default

LEF Profile

--Select--

☒ Default Profile

Honour PBF

☐ Yes ☒ No

Parse Response

☐ Yes ☒ No

OK

Cancel

7. In the Name field, enter a name for the HTTP/HTTPS proxy.

8. In the Mode field, select Transparent.

9. In the port field, enter the port number to use to connect to the proxy.

10. In the Honor PBF field, click Yes so that when you apply policy-based forwarding in a redirection rule in a DNS profile, proxy forwarding can also check SD-WAN policies to select the path for the DNS query and the onward connection to the application server.

11. Select the Rules tab and then click the + Add icon.



Add HTTP/HTTPS Proxy

General
Cookie Based User Identification
Rules

+

	Name	Rule Mode	Rule Status
No Rules Added			

OK
Cancel

12. In the Add Rules popup window, select General tab and enter information for the following fields.

Add Rules

General
Match
Enforce

Name \*

Rule1

Monitor

--Select--

Rule Status

☒ Enabled
☐ Disabled

OK
Cancel

a. In the Name field, enter a name for the rule.

b. In the Rule Status field, click Enabled.

13. Select the Enforce tab.

**Add Rules** [X]

General Match **Enforce**

Rule Mode

☒ Proxy Chaining ☐ Local Breakout

Skip Local Breakout on DNS Failure

☒ Enabled ☐ Disabled

Proxy IP Address

Proxy Port \*

Honour PBF

☒ Enabled ☐ Disabled

FQDN

SNAT Pool

--Select--

+ SNAT Pool

OK Cancel

14. In the Rule Mode field, select Proxy Chaining.
15. In the Honor PBF field, click Enabled to honor policy-based forwarding. When policy-based forwarding is enabled, when you apply policy-based forwarding in a redirection rule in a DNS profile, proxy forwarding can also check SD-WAN policies to select the path for the DNS query and the onward connection to the application server
16. Click OK to add the rule.
17. Click OK to add the HTTP/HTTPS proxy.

For information about configuring additional HTTP/HTTPS web proxy features, see [Configure HTTP/HTTPS Proxy](#).

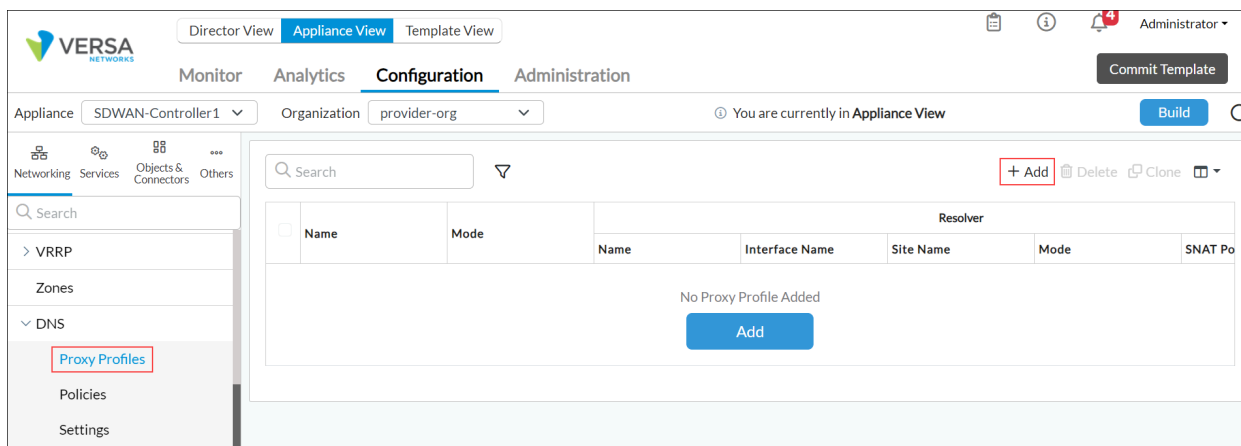
## Configure a DNS Proxy

To associate the HTTP/HTTPS proxy with a DNS proxy, you configure a DNS proxy profile and a DNS redirection rule.

To configure a DNS proxy profile:

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

3. Select Networking > DNS > Proxy Profiles in the left menu bar.



4. Click the + Add icon. The Add Proxy Profile popup window displays. In the Name field, enter a name for the DNS proxy profile.

### Add Proxy Profile

Name \*

Description

Mode

--Select--

Resolver

+

<1>

>25

	Name	Site Name	Network	Mode
No Resolver Added				

OK

Cancel

5. In the Resolver tab, click the + Add icon to add DNS resolvers, which resolve the domain names received in DNS requests. In the Add Resolver popup window, enter information for the following fields.

[https://docs.versa-networks.com/Secure\\_SD-WAN/01\\_Configuration\\_from\\_Director/SD-WAN\\_Configuration/Advanced\\_SD-W...](https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/SD-WAN_Configuration/Advanced_SD-W...)

Updated: Wed, 23 Oct 2024 08:11:17 GMT

Copyright © 2024, Versa Networks, Inc.

Add Resolver
✕

Name \*

☒ Site Name
☐ Network

Site Name

--Select--

Mode

--Select--

SNAT Pool

--Select--

+ SNAT Pool

DHCP Server Monitor
Domain Name \*

Nexthop
Network \*

--Select--

Interval (seconds)
Threshold

Servers

<  >

Name *	Address	Port	Monitor Object	
<div></div>	<div></div>	53	--Select--	<div>+</div>

No MEP List Added

OK

Cancel

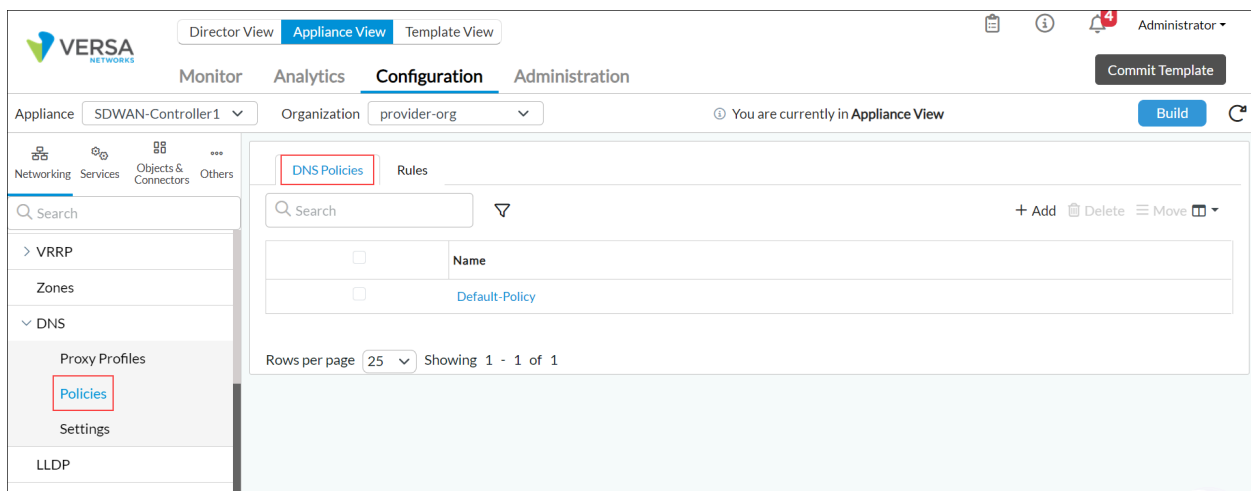
Field	Description
Name (Required)	Enter a name for the resolver profile.
Site Name	Click and select an SD-WAN site to which to send traffic for DNS resolution. Configuring a s direct internet access (DIA) and direct cloud access (DCA).

Network	Click and select which local WAN or LAN networks to use to proxy a DNS request.
Mode	<p>Select the mode to use to check the availability of the DNS server:</p> <ul style="list-style-type: none"> <li>◦ Failover</li> <li>◦ Round-Robin</li> </ul> <p><i>Default: Failover</i></p>
SNAT Pool	Select an SNAT pool to associate with the DNS profile. The address in this pool can be used to proxy a DNS request. Click to add an SNAT pool. For more information, see <a href="#">Configure SNAT Pools</a> .
DHCP Server Monitor (Group of Fields)	(For Releases 22.1.3 and later.) Click to configure a server monitor for the server provided by the service provider. If the VOS is configured to use DNS servers from a service provider to resolve IP addresses, the VOS can detect that the DNS servers assigned by the service provider are incorrect or unreachable.
◦ Domain Name (Required)	Enter the domain name for the DNS server.
◦ Next Hop	Enter the name of the next-hop SD-WAN site.
◦ Network (Required)	Enter the network used to derive the source interface.
◦ Interval	Click and enter the interval between monitor packets, in seconds.
◦ Threshold	Enter the maximum number of monitor packet retransmissions before the node is declared unreachable.
Servers (Group of Fields)	
◦ Name	Enter a name for the DNS server.
◦ Address	Enter the IP address of the DNS server. The address can be an IPv4 or an IPv6 address.
◦ Port	Enter the port number to use to connect to the DNS server.
◦ Monitor	<p>Click to evaluate the state of the IP addresses configured in the resolver. This evaluation is performed for each DNS server using the method configured in the Mode field. After the evaluation, the traffic is sent to the active DNS server.</p> <p>If you do not click this field, all the IP addresses configured in the resolver appear active regardless of their state.</p>

6. Click OK.

To configure a DNS redirection rule in a DNS policy:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar
  - b. Select Devices > Devices in the left menu bar.
  - c. Select an organization from the left menu bar.
  - d. Select a Controller from the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking > DNS > Policies in the left menu bar.
4. Select the DNS Policies tab in the horizontal menu bar.



5. In the Add DNS Policy popup window, enter a name for the DNS policy and then click OK.

### Add DNS Policy

Name \*

Default-Policy

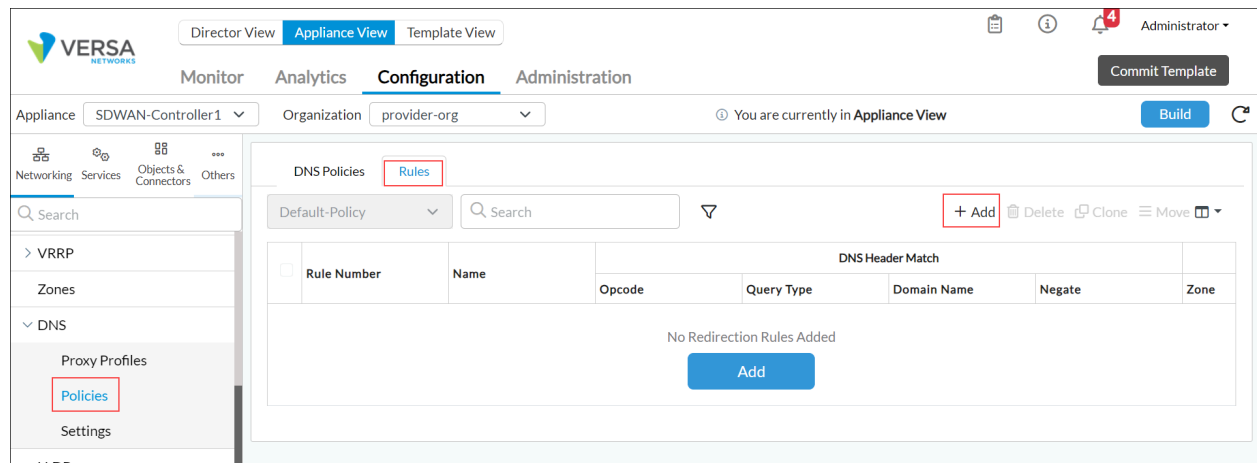
Description

Tags

OK

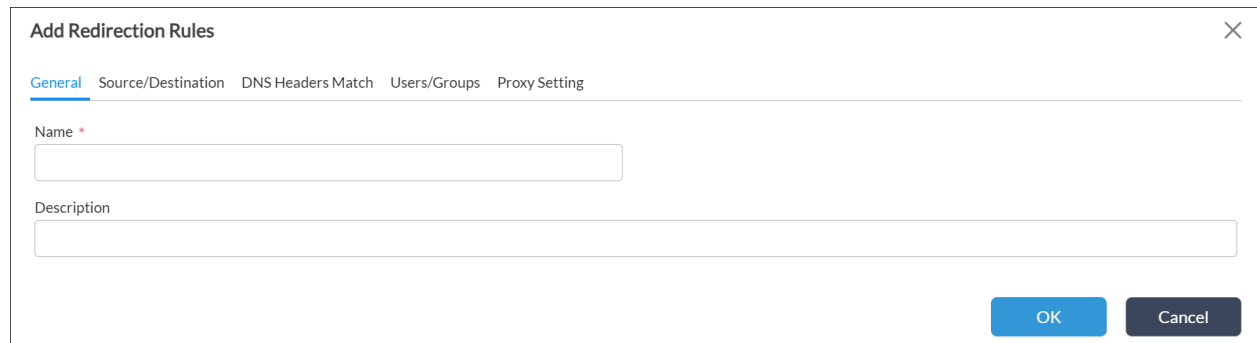
Cancel

6. Select the Rules tab in the horizontal menu bar.



7. Click the + Add icon. The Add Redirection Rules popup window displays.

8. Select the General tab and enter a name for the redirection rule, and then click OK.



9. Select the Proxy Setting tab and enter information for the following fields.

## Add Redirection Rules

General Source/Destination DNS Headers Match Users/Groups Proxy Setting

### Actions

### Proxy Setting

☐ Server Setting

☐ None

### Proxy Setting

## Proxy Profile

--Select--

Number of Domains to Cache

DNS64 Prefix

+ Proxy Profile

### Override Question

☐ Only IPv4 WAN Available☐ Apply Policy Based Forwarding☐ Network Obfuscation☐ Unique IP Per Client

### Dynamic Destination IP Pool

--Select--

Cache TTL Upper Limit (seconds)

### Server Setting

Address 

Monitor Object



No Records to Display

### Logging Setting

LEF Profile

--Select--

☐ Default Profile

+ LEF Profile

10. In the Actions group, click Proxy Setting.
11. In the Proxy Profile field, select the name of the HTTP/HTTPS proxy profile.
12. Click Apply Policy-Based Forwarding to look up SD-WAN policy rules to determine the path on which to send the DNS query.
13. Click OK.

For information about configuring other DNS proxy parameters, see [Configure DNS Proxy](#).

## Configure SD-WAN Traffic Steering

As the final step, you configure the SD-WAN traffic-steering policy that a traffic flow consults when you enable honor policy-based forwarding. For information about creating an SD-WAN traffic-steering policy, see the [Configure SD-WAN Traffic Steering](#) article.

Note that while you can also configure a policy-based forwarding (PBF) policy, it is recommended that you configure an SD-WAN traffic-steering policy.



---

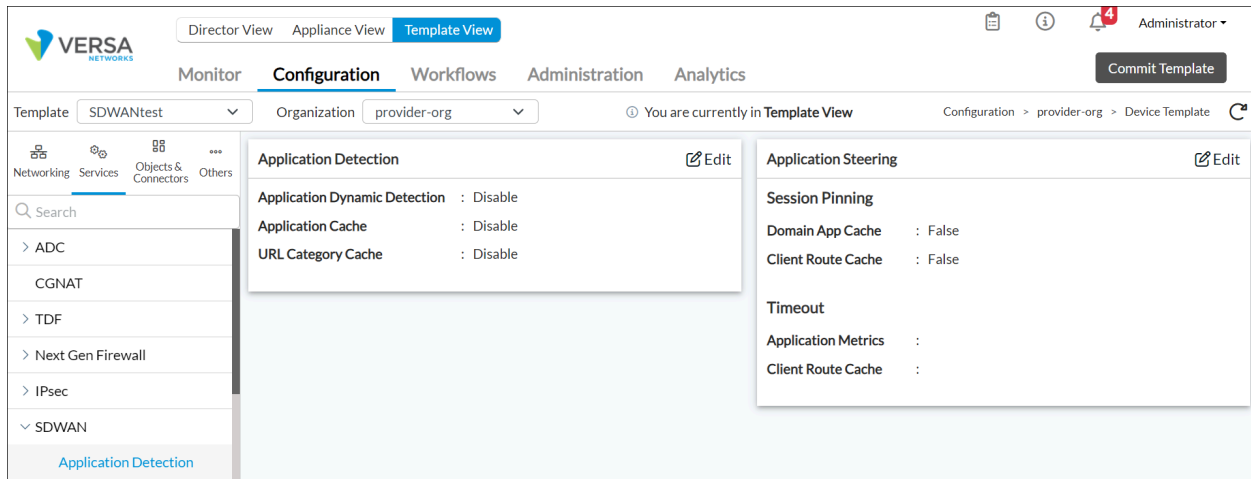
## Configure DNS Resolution-Based Path Affinity

For DNS resolution-based path affinity, you steer all client-initiated sessions that follow the DNS query over the same path that the DNS query was sent on. This behavior is called strict affinity. To understand how strict affinity works, let's first describe loose affinity. If, for example, a "salesforce" rule dictates that Salesforce traffic can use either the Comcast or ATT circuit, the DNS query could be sent over the Comcast circuit. However, when the subsequent application traffic (the HTTPS sessions) matches the same SD-WAN traffic-steering policy rule, the policy could select the ATT circuit. This behavior achieves loose path affinity, because while the DNS query and HTTP traffic are not going on the same circuit, they are still both using local egress (local direct internet access).

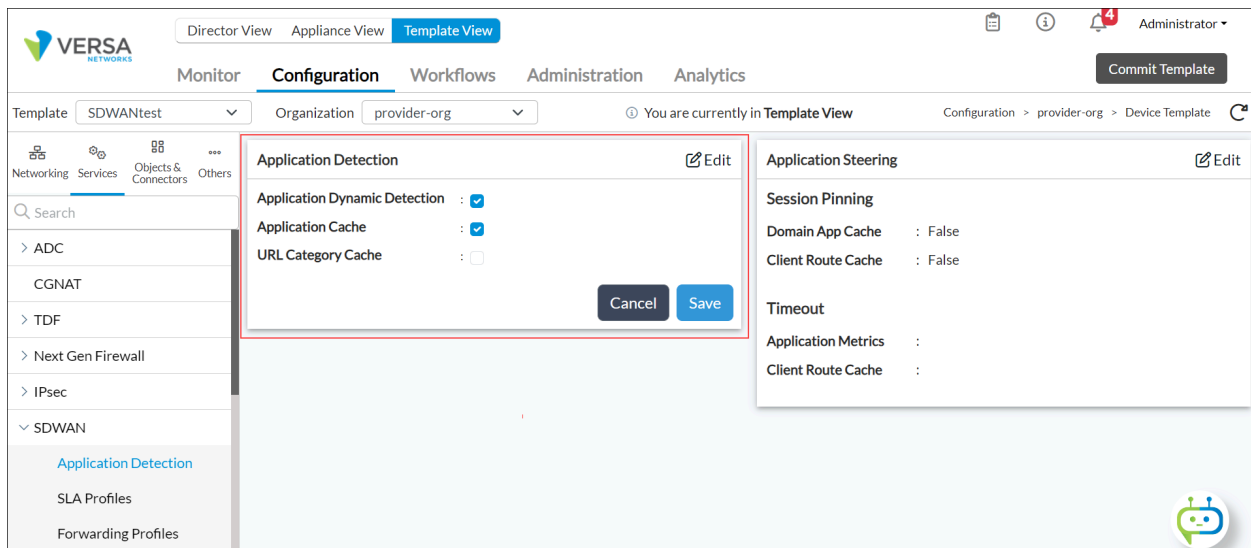
DNS resolution-based path affinity, or strict affinity, steers all client-initiated sessions subsequent to the DNS query over the same path that the DNS query was sent on. When the VOS software receives the response from the DNS query, it creates the path affinity by caching the path in a client route cache (CRC) entry. When a new session between a client and server is established, the VOS software consults the CRC to check whether a previously chosen path exists. If a match is found, the new session is pinned to this path instead of making a new path selection decision. With the strict path affinity, if the DNS query for salesforce uses the Comcast circuit, all subsequent client-initiated HTTP traffic for salesforce uses the Comcast circuit as well. The salesforce HTTP traffic continues to use the Comcast circuit until the next time the client does a DNS query for salesforce. At that time, the SD-WAN traffic-steering policy might choose to send the query over the ATT circuit. If so, subsequent HTTP session use the ATT circuit, again until the next time the client does a DNS query.

To configure path affinity between the DNS resolution and data traffic paths:

1. In Director view:
  - a. Select the Configuration tab in the top menu bar.
  - b. Select Templates > Device Templates in the horizontal menu bar.
  - c. Select an organization in the left menu bar.
  - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Services > SD-WAN > Application Detection in the left menu bar. The main pane displays the Application Detection and Application Steering panes.



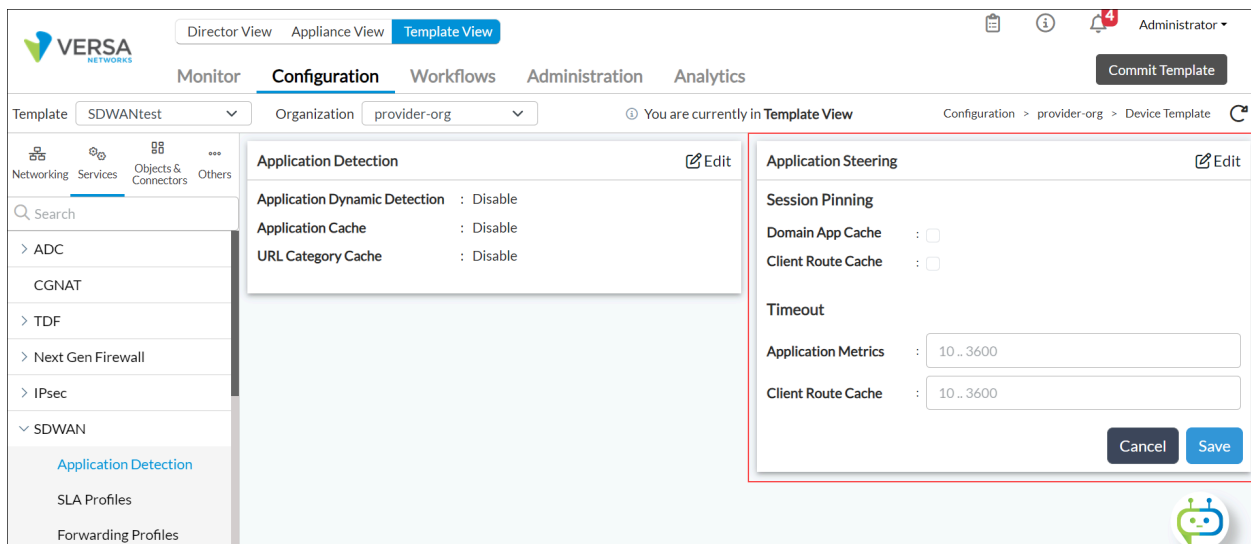
4. In the Application Detection pane, click the  Edit icon to enable the application detection options.



Field	Description
Application Dynamic Detection	Click to enable dynamically re-evaluate SD-WAN traffic-steering rules when an application or URL category is detected in a traffic flow even if the packet being inspected is not the first packet in the flow. <i>Default:</i> Disabled
Application Cache	Click to enable cache applications associated with server IP address and port numbers. <i>Default:</i> Disabled
URL Category Cache	Click to enable cache URL categories associated with HTTP and HTTPS server IP addresses and port numbers. <i>Default:</i> Disabled

5. Click Save.

6. In the Application Steering pane, click the  Edit icon and enter information for the following fields.



The screenshot shows the Versa Networks configuration interface. The top navigation bar includes 'Director View', 'Appliance View', and 'Template View'. The main navigation menu on the left lists 'Networking', 'Services', 'Objects & Connectors', and 'Others'. Under 'Services', 'SDWAN' is expanded, showing 'Application Detection', 'SLA Profiles', and 'Forwarding Profiles'. The 'Application Detection' pane is active, showing 'Application Dynamic Detection', 'Application Cache', and 'URL Category Cache', all set to 'Disable'. The 'Application Steering' pane is also visible, showing 'Session Pinning' (Domain App Cache and Client Route Cache) and 'Timeout' (Application Metrics and Client Route Cache), all set to '10..3600'. The 'Edit' icon is visible in the top right of both panes.

Field	Description
Session Pinning (Group of Fields)	Configure path affinity between DNS query requests and application traffic.
<ul style="list-style-type: none"> <li>Domain Application Cache</li> </ul>	<p>Click to enable strict path affinity, to ensure that all the sessions of an application flow use the same path that was used by the DNS query to resolve the path to the application server.</p> <p>Do not click to use loose path affinity. This is the default. Here, the DNS query and the application sessions follow paths to the same geographic location, but the DNS query and the application traffic may be sent on different links. In general, it is recommended that you use loose path affinity, because it provides the best balance between ensuring optimal performance and ensuring load balancing of traffic among all eligible paths.</p> <p><i>Default:</i> Loose path affinity</p>
<ul style="list-style-type: none"> <li>Client Route Cache</li> </ul>	Click to pin the subsequent consecutive sessions of an application flow between a specific client and server to the same path.
Timeout (Group of Fields)	Configure the session-pinning timeout periods.
<ul style="list-style-type: none"> <li>Application Metrics</li> </ul>	<p>Enter the maximum time, in seconds, that a link with the worst metric must wait before trying again.</p> <p><i>Default:</i> 300 seconds</p>
<ul style="list-style-type: none"> <li>Client Route Cache</li> </ul>	<p>Enter the maximum time, in seconds, that sessions between a host and client remain pinned to the same link.</p> <p><i>Default:</i> 30 seconds</p>

7. Click Save.

---

## Supported Software Information

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

- Release 22.1.3 adds configuration of DHCP server monitors.

---

## Additional Information

[Configure a DNS Proxy](#)

[Configure HTTP/HTTPS Proxy](#)

[Configure SD-WAN Policy](#)

[Configure SD-WAN Traffic Steering](#)

[Overview of Policy-Based Forwarding in an SD-WAN Network](#)