Redirect DNS in a Service-Side VPN

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Table 1: Feature History

Feature Name	Release Information	Description
Redirect DNS in a Service-Side VPN	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	This feature allows you to configure a Cisco IOS XE Catalyst SD-WAN device to respond to Domain Name System (DNS) queries using proxy servers. This feature adds support for DNS proxy for servce-side VPN hosts and DNS redirects inside the service VPNs.

Information About Redirect DNS in a Service-Side VPN

The Redirect DNS feature enables Cisco IOS XE Catalyst SD-WAN devices to respond to DNS queries using a specific configuration and associated host table cache that are selected based on certain characteristics of the queries. In a redirect DNS environment, multiple DNS databases can be configured on the device. The Cisco Catalyst SD-WAN software can be configured to choose one of the DNS name server configurations whenever the device responds to a DNS query, by forwarding or resolving the query. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, redirect DNS is supported only through NAT Direct Internet Access (DIA) path.

When an application-aware routing policy allows a Cisco IOS XE Catalyst SD-WAN device to send application traffic to a service VPN and receive application traffic from a service VPN, the device performs a DNS lookup to determine the path to reach the application server. If the router does not have a connection to the internet, it sends DNS queries to an edge device that has such a connection, and that device determines how to reach a server for that application.

Note In a network in which the device that is connected to the internet is in a geographically distant data center, the resolved DNS address points to a server that is also geographically distant from the site where the service VPN is located.

Because you can configure a Cisco IOS XE Catalyst SD-WAN device to be an internet exit point, it is possible for any router to reach the internet directly to perform DNS lookups.

You can configure redirect DNS with either a centralized data policy or, if you want to apply SLA criteria to the data traffic, you can use application-aware routing policy.

Restrictions for Redirect DNS in a Service-Side VPN

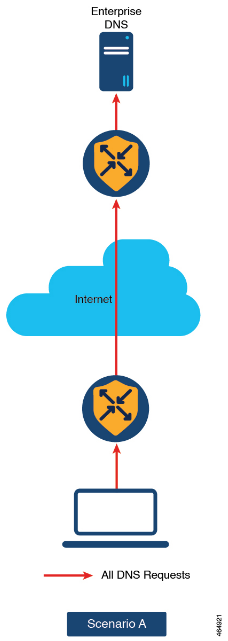
- A redirect DNS request is not accepted without NAT configuration if the request is from the same VPN with the same port from a different host.
- If you configure DNS server IP address using NAT, it cannot be changed through the data policy.
- DNS fragmented packets and self-generated DNS are not supported.
- DNS requests from the overlay tunnel are not supported.
- Redirect DNS is supported only on IPv4 traffic, and not on IPv6 traffic.
- DNS requests through User Datagram Protocol (UDP) are supported. However, requests from Transmission Control Protocol (TCP) are not supported.

Use Cases for Redirect DNS in a Service-Side VPN

Unconditional Redirect DNS

In unconditional redirect DNS (scenario A), a host sends all the DNS requests to a local edge router, and the local edge router redirects the DNS request to an enterprise DNS server in the data center (which is available only using a service-side VPN) and acts as a DNS forwarder. A use case for this feature redirects statically configured IP addresses for printers to an enterprise DNS server in a data center. In this use case, all the legacy printers are statically configured with an IP address of a local router as DNS server, which acts as DNS forwarder to forward all the DNS requests from printers.

Figure 1: Unconditional Redirect DNS

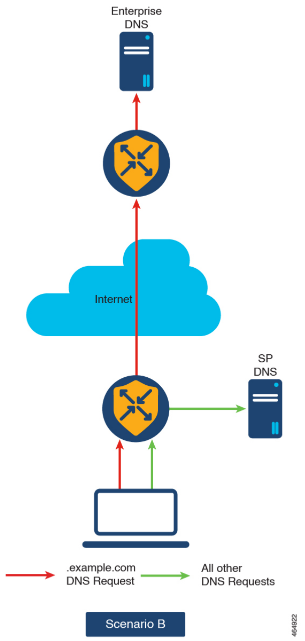


Conditional Redirect DNS

In conditional redirect DNS (scenario B), a host uses a service provider (SP) or managed service provider (MSP) DNS by default. For known applications that use an Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) or custom applications, for example, *.google.com, the DNS request is forwarded to the enterprise DNS server using a Cisco Catalyst SD-WAN overlay network. All the other DNS requests are sent to the SP or MSP DNS server.

Note In Cisco vManage Release 20.7.1 and earlier releases, SAIE is called deep packet inspection (DPI).

Figure 2: Conditional Redirect DNS



Configure Redirect DNS in a Service-Side VPN

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. From the **Custom Options** drop-down list, choose **Traffic Policy** from the **Centralized Policy** menu.
3. Click **Traffic Data** to create a traffic data policy.
4. From the **Add Policy** drop-down list, choose **Create New**.
5. In the **Name** and **Description**, enter a name and a description for the data policy.
6. Click **Sequence Type**.

   The **Add Data Policy** dialog box is displayed.
7. Choose the type of data policy that you want to create—**Application Firewall**, **QoS**, **Service Chaining**, **Traffic Engineering**, or **Custom**.

   A policy sequence containing the selected type of data policy is added in the left pane.
8. Double-click the text string, and enter a name for the policy sequence.

   The name you type is displayed both in the **Sequence Type** list in the left pane and in the right pane.
9. Click **Sequence Rule**. The **Match/Action** dialog box is displayed, where **Match** is selected by default. The available policy match conditions are listed in the menu.
10. From the **Protocol** drop-down list, choose **IPv4** to apply the policy only to IPv4 address families.
11. To choose one or more **Match** conditions, click the fields and set the values as described.

Note Not all match conditions are available for all policy sequence types.

12. To select the actions to take on matching data traffic, click the **Actions** menu.
13. To drop matching traffic, click **Drop**.

    The available policy actions are listed on the right side.
14. To accept matching traffic, click **Accept**.

    The available policy actions are listed on the right side.
15. In the **Actions** menu, choose **Redirect DNS** to configure redirect DNS.
16. In the **Redirect DNS** condition field, enter the **IP Address** and click **Save Match and Actions**.
17. Click **Save Data Policy**.

Match Condition	Procedure
None (match all the packets)	Do not specify any match conditions.
Applications / Application Family List / Custom Applications	1. In the **Match** conditions menu, click **Applications/Application Family List**. 2. From the drop-down list, choose the application family. 3. To create an application list: a. Click **New Application List**. b. Enter a name for the list. c. Click **Application** to create a list of individual applications. Click **Application Family** to create a list of related applications. d. From the **Select Application** drop-down list, choose the corresponding applications or application families. e. Click **Save**.
DNS Application List	Add an application list to enable split DNS: 1. In the **Match** conditions menu, click **DNS Application List**. 2. From the drop-down list, choose the application family.
DNS	Add an application list to process split DNS: 1. In the **Match** conditions menu, click **DNS**. 2. From the drop-down list, choose **Request** to process DNS requests for the DNS applications.

Match Condition	Procedure
Destination Data Prefix	1. In the **Match** conditions menu, click **Destination Data Prefix**. 2. To match a list of destination prefixes, from the **Data Prefix** drop-down list, choose a list. 3. To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field.
Destination Port	1. In the **Match** conditions menu, click **Destination Port**. 2. In the **Destination Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with two numbers separated with a hyphen [-]).
DSCP	1. In the **Match** conditions menu, click **DSCP**. 2. In the **DSCP** field, enter the DSCP value—a number from 0 through 63.
Packet Length	1. In the **Match** conditions menu, click **Packet Length**. 2. In the **Packet Length** field, enter the length—a value from 0 through 65535.
PLP	1. In the **Match** conditions menu, click **PLP** to set the **Packet Loss Priority**. 2. From the **PLP** drop-down list, choose **Low** or **High**.
Protocol	1. In the **Match** conditions menu, click **Protocol**. 2. In the **Protocol** field, enter the Internet Protocol number—a number from 0 through 255.
Source Data Prefix	1. In the **Match** conditions menu, click **Source Data Prefix**. 2. To match a list of source prefixes, from the **Source Data Prefix List** drop-down list. choose a data prefix list. 3. To match an individual source prefix, enter the prefix in the **Source** field.
Source Port	1. In the **Match** conditions menu, click **Source Port**. 2. In the **Source** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Configure Redirect DNS in a Service-Side VPN Using the CLI

The following steps show the minimum policy components required to enable redirect DNS with a centralized data policy:

1. Create a list of overlay network sites to which the centralized control policy is to be applied:

```
vsmart(config)# policy
vSmart(config-policy)# lists site-list list-name
vSmart(config-lists-list-name)# site-id site-id
```

The list can contain as many site IDs as necessary. Include one **site-id** command for each site ID. For contiguous site IDs, you can specify a range of numbers separated with an en dash (–). Create additional site lists, as needed.

2. Create lists of applications or application families for which you want to enable redirect DNS. Refer to these lists in the **match** section of the data policy.

```
vSmart(config)# policy lists
vSmart(config-lists)# app-list list-name
vSmart(config-app-list)# app application-name | app-family family-name
```

3. Create list VPNs to which the redirect DNS policy is to be applied:

```
vSmart(config)# policy lists
vSmart(config-lists)# vpn-list list-name
vSmart(config-lists)# vpn vpn-id
```

4. Create a data policy instance and associate it with a list of VPNs:

```
vSmart(config)# policy data-policy policy-name
vSmart(config-data-policy)# vpn-list list-name
```

5. Create a series of match–action pair sequences:

```
vSmart(config-vpn-list)# sequence number
```

The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. Or, if no match occurs, the default action is taken (either rejecting the route or accepting it as is).

6. Process the DNS server resolution for the applications or application families contained in an application list. For the *list-name* argument, specify the list name.

```
vSmart(config-sequence)# match dns-app-list list-name
```

7. Configure the match–action pair sequence to process DNS requests (for outbound data traffic) or responses (for inbound data traffic):

```
vSmart(config-sequence)# match dns (request | response)
```

8. By default, the DNS servers configured in the VPN in which the policy is applied are used to process DNS lookups for the applications. You can direct the DNS requests to a particular DNS server. For a data policy condition that applies to outbound traffic (from the service network), configure the IP address of the DNS server:

```
vSmart(config-sequence)# action accept redirect-dns ip-address
```

For a data policy condition that applies to inbound traffic (from the tunnel), include the following action so that the DNS response can be correctly forwarded back to the service VPN:

```
vSmart(config-sequence)# action accept redirect-dns host
```

9. Apply the policy to one or more sites in the Cisco Catalyst SD-WAN overlay network:

```
vSmart(config)# apply-policy site-list list-name
data-policy policy-name (all | from-service)
```

Verify Redirect DNS in a Service-Side VPN

The following is a sample output from the **show sdwan policy from-vsmart** command that shows how to verify the redirect DNS configuration:

```
vSmart# show sdwan policy from-vsmart
from-vsmart data-policy vpn1_dns-redirect-prefer-lte
 direction from-service
 vpn-list vpn1
  sequence 1
   match
    source-ip 10.0.0.0/0
    dns       request
   action accept
    count        gdns2_-396115821
    redirect-dns 10.255.255.254
  default-action accept
from-vsmart lists vpn-list vpn1
 vpn 1
```

Configuration Examples for Redirect DNS

Unconditional DNS Redirect

The following example shows how to configure an unconditional DNS redirect, where all the DNS requests are matched:

```
policy
 data-policy rdns
  vpn-list vpn10
   sequence 10
    match
     source-ip 0.0.0.0/0
     dns       request
    !
    action
     redirect-dns 209.165.200.225
    !
   default-action accept
   !
  !
!
apply-policy
 site-list siteA
  data-policy rdns from-service
```

Conditional DNS Redirect

The following example shows how to configure a conditional DNS redirect, where a selective DNS request is defined using an app list:

```
policy
 data-policy rdns
  vpn-list vpn10
   sequence 10
```

```
    match
     source-ip 10.0.0.0/8
     dns       request
     dns-app-list YouTube
    !
    action
     redirect-dns 209.165.200.225
    !
   default-action accept
   !
  !
!
apply-policy
 site-list siteA
  data-policy rdns from-service
```