

# Configure Integration with Cisco Umbrella and Troubleshooting Common Problems

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Verify and Troubleshoot](#)

[Client Verification](#)

[cEdge Verification](#)

[Understand the Umbrella's EDNS Implementation](#)

[Verify it on vManage Dashboard](#)

[DNS Caching](#)

[Secure DNS](#)

[Conclusion](#)

## Introduction

This document describes vManage/Cisco IOS®-XE SDWAN software part of the integration with the Cisco Umbrella DNS security solution. However, it does not cover the Umbrella policies configuration itself. You can find more information about Cisco Umbrella here; <https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella>.

**Note:** You have to have already obtained Umbrella subscriptions and get Umbrella token that will be used in the configuration of cEdge routers. More about API token: <https://docs.umbrella.com/umbrella-api/docs/overview2>.

## Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

The information in this document is based on these software and hardware versions:

- vManage 18.4.0
- Cisco IOS®-XE SDWAN router running (cEdge) 16.9.3

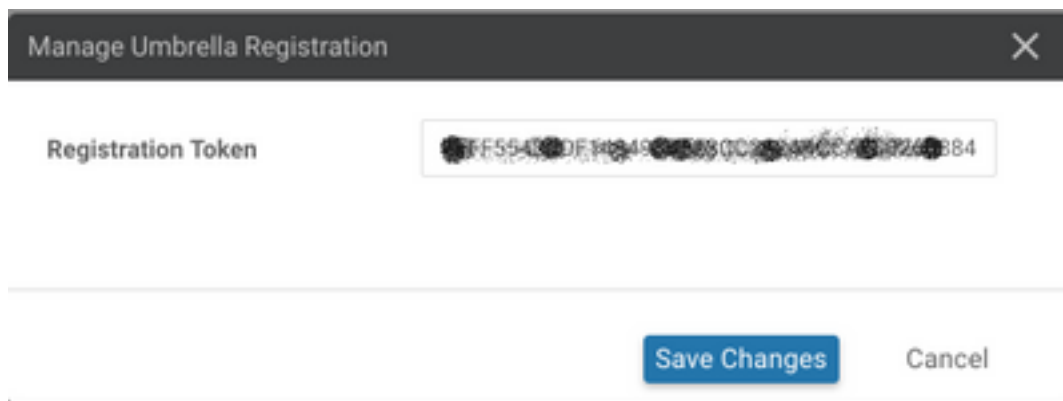
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, ensure that you understand the potential impact of any command.

## Configure

In order to configure your cEdge integration with Cisco Umbrella, you perform a set of simple steps on vManage:

Step 1. Under **Congifuration > Security**, select **Custom Options** drop-down list at the top right corner, and then select **Umbrella API token**. Enter your Umbrella registration token, as shown in the image:



Manage Umbrella Registration

Registration Token

FF5543DF1424902830C2346C309224884

Save Changes Cancel

Alternatively, starting from vManage software 20.1.1 release you can specify Organization ID, Registration Key, and Secret. These parameters can be retrieved automatically if you have configured your Smart Account credentials under **Administration > Settings > Smart Account Credentials**.

### Cisco Umbrella Registration Key and Secret ℹ

Organization ID	<input type="text" value="Enter Organization ID"/>
Registration Key	<input type="text" value="Enter Registration Key"/>
Secret	<input type="text" value="Enter Secret"/>

[Get Keys](#)

### Cisco Umbrella Registration Token ℹ

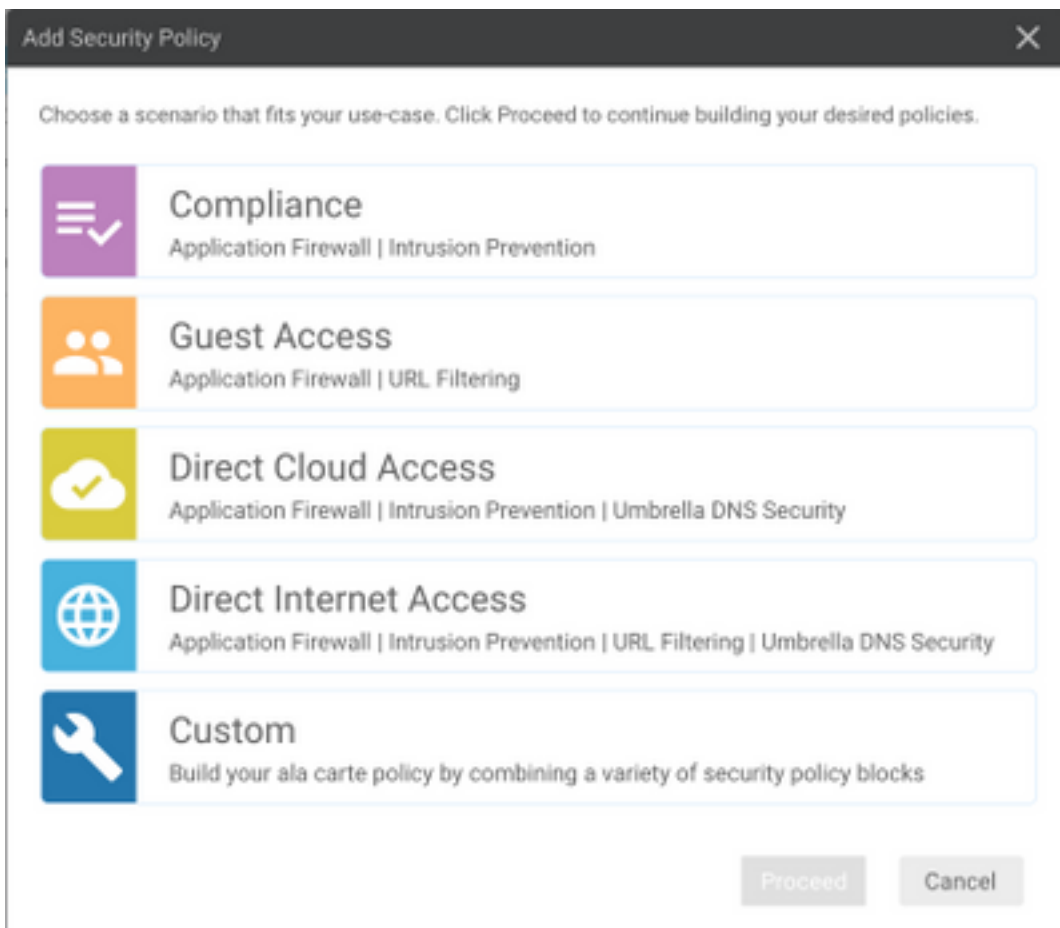
*Required for legacy devices*

Registration Token	<input type="text" value="Must be exactly 40 hexadecimal characters"/>
--------------------	--

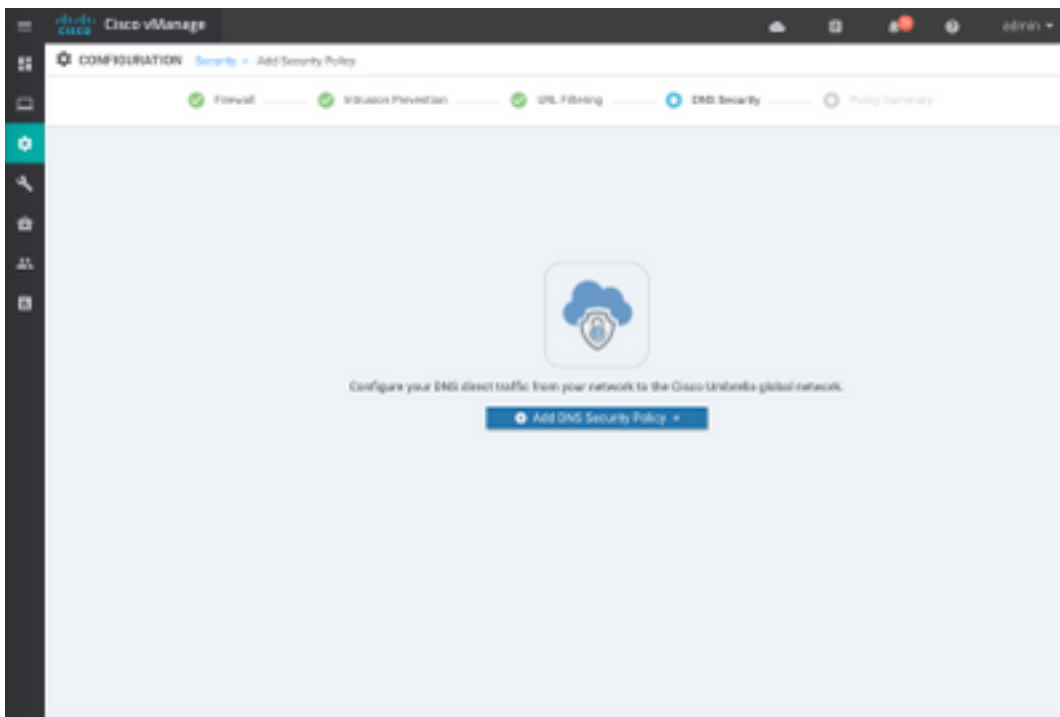
[Save Changes](#)

Cancel

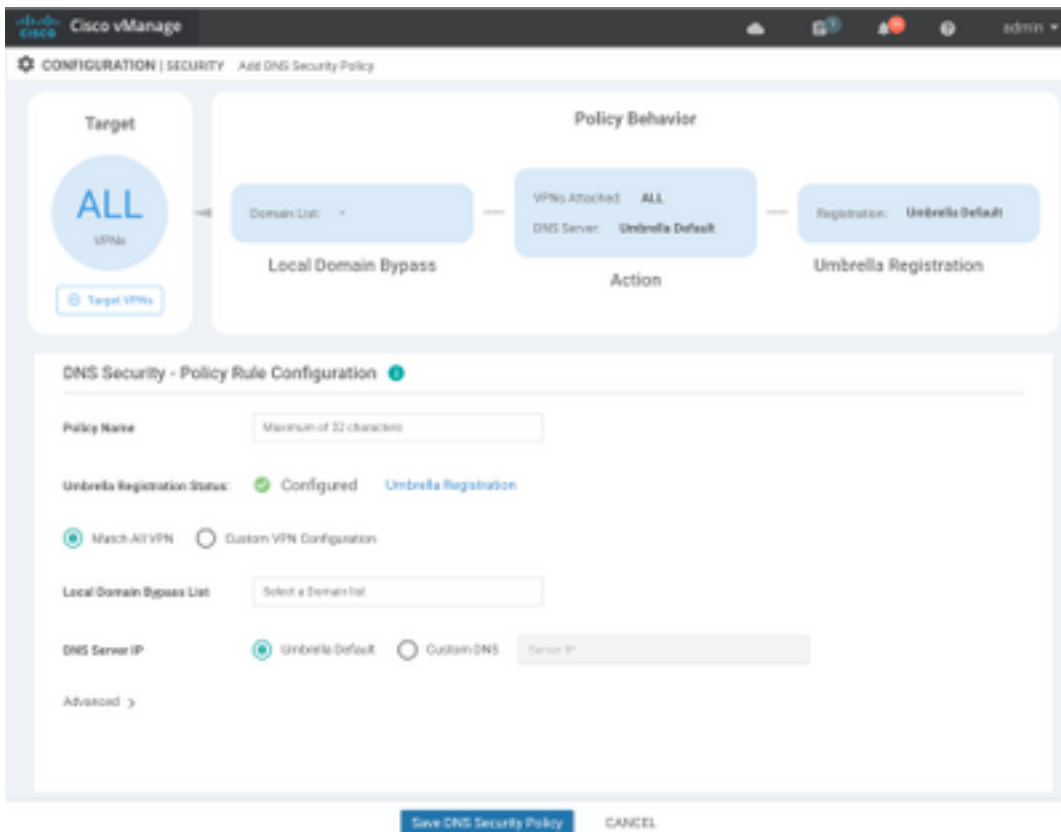
Step 2. Under **Configuration > Security**, select **Add Security Policy** and then select a scenario that fits your use-case (e.g. custom), as shown in the image:



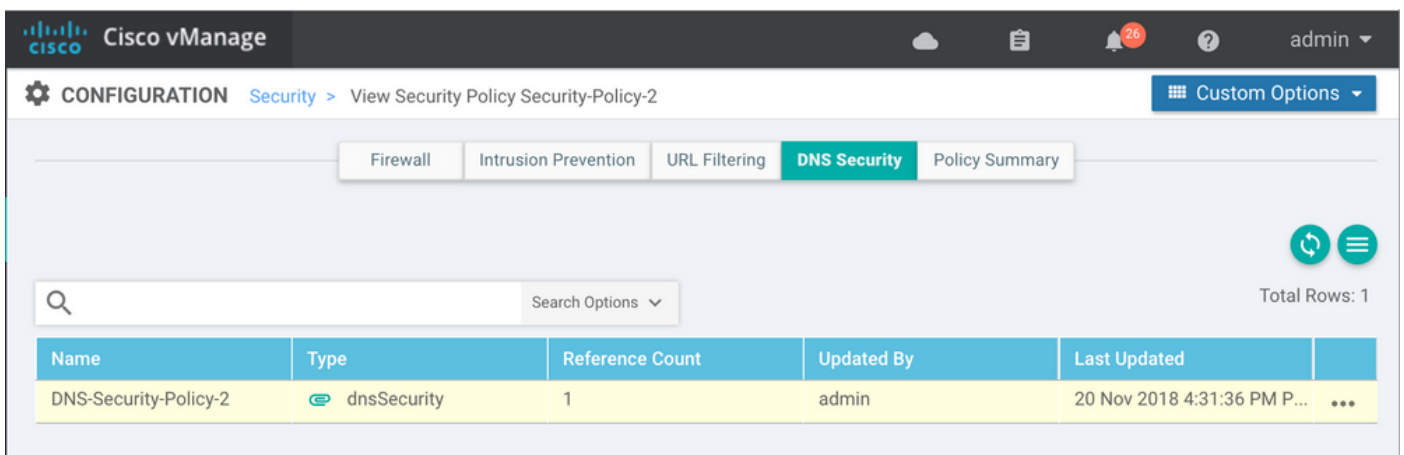
Step 3. As shown in the image, navigate to **DNS Security**, select **Add DNS Security Policy** and then select **Create New**.



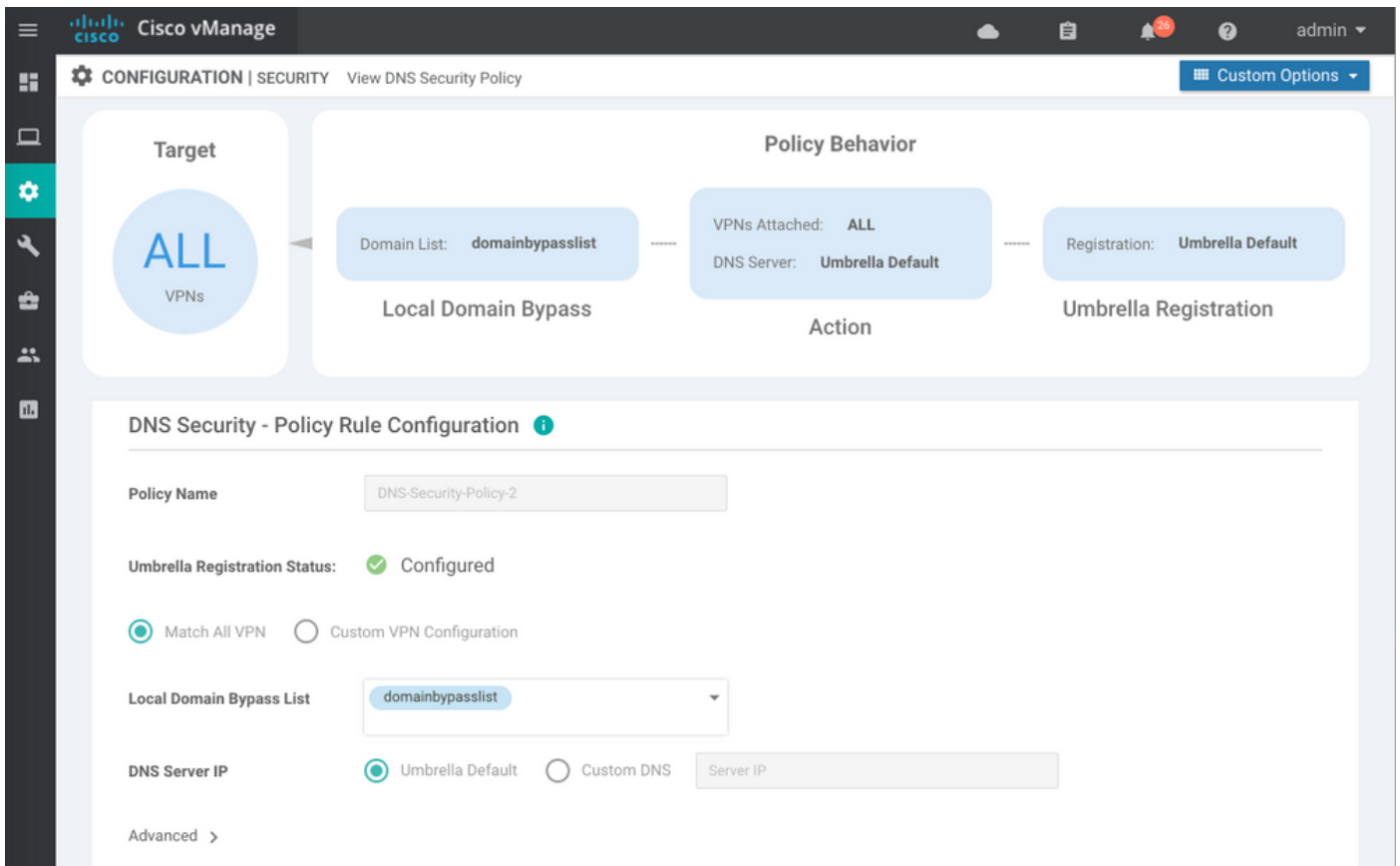
The screen appears similar to the image shown here:



Step 4. This is the image of how it appears, once configured.



Step 5. Navigate to ...> **View** > **DNS Security** tab of your policy, you see a configuration similar to this image:



Keep in mind that "Local Domain Bypass List" is a list of domains for which router does not redirect DNS requests to Umbrella cloud and sends DNS request to a specific DNS server (DNS server located within the enterprise network), this is not exclusion from Umbrella security policies. In order to "whitelist" some domains from the specific category, it is recommended to configure exclusion on Umbrella configuration portal instead.

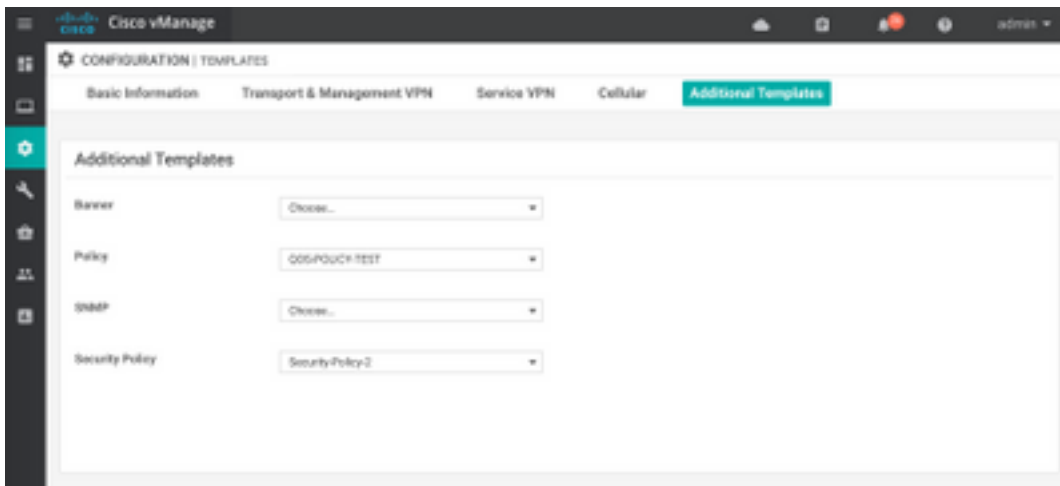
Also, you can select **Preview** in order to understand how the configuration looks in CLI:

```

policy
 lists
  local-domain-list domainbypasslist
  cisco.com
  !
  !
  !
exit
!
security
 umbrella
  token XFFFX543XDF14X498X623CX222X4CCAX0026X88X
  dnscrypt
  !
exit
!
vpn matchAllVpn
 dns-redirect umbrella match-local-domain-to-bypass

```

Step 6. Now you must reference policy in the device template. Under **Configuration > Templates**, select your configuration template and reference it in the **Additional Templates** section as shown in the image.



Step 7. Apply the template to the device.

## Verify and Troubleshoot

Use this section to confirm that your configuration works properly and troubleshoot it.

### Client Verification

From a client sitting behind the cEdge, you can verify whether Umbrella works correctly when you browse these test sites:

- <http://welcome.opendns.com>
- <http://www.internetbadguys.com>

For more details, refer to [How To: Successfully test to ensure you're running Umbrella correctly](#)

### cEdge Verification

Verification and troubleshooting can also be performed on the cEdge itself. In general, it's similar to Cisco IOS-XE software integration troubleshoot procedures that can be found in chapter 2 Cisco Umbrella Integration on Cisco 4000 Series ISRs of Security Configuration Guide: Cisco Umbrella Integration, Cisco IOS-XE Fuji 16.9.x: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_umbrbran/configuration/xs-16-9/sec-data-umbrella-branch-xe-16-9-book.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_umbrbran/configuration/xs-16-9/sec-data-umbrella-branch-xe-16-9-book.pdf).

Few useful commands to check:

Step 1. Check that parameter-map is presented in cEdge configuration on the device:

```
dmz2-site201-1#show run | sec parameter-map type umbrella
parameter-map type umbrella global
 token XFFFFX543XDF14X498X623CX222X4CCAX0026X88X
 local-domain domainbypasslist
 dnscrypt
 udp-timeout 5
 vrf 1
 dns-resolver umbrella
 match-local-domain-to-bypass
```

!

Note that you are unable to find a reference to this parameter-map on the interface as you get used to seeing it on Cisco IOS-XE.

This is because parameter-map is applied to VRFs and not to interfaces, you can check it here:

```
dmz2-site201-1#show umbrella config
Umbrella Configuration
=====
Token: XFFFX543XDF14X498X623CX222X4CCAX0026X88X
OrganizationID: 2525316
Local Domain Regex parameter-map name: domainbypasslist
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
UDP Timeout: 5 seconds
Resolver address:
  1. 208.67.220.220
  2. 208.67.222.222
  3. 2620:119:53::53
  4. 2620:119:35::35
Registration VRF: default
VRF List:
  1. VRF 1 (ID: 2)
      DNS-Resolver: umbrella
      Match local-domain-to-bypass: Yes
```

Besides that, you can use this command to get detailed info:

```
dmz2-site201-1#show platform hardware qfp active feature umbrella client config
+++ Umbrella Config +++

Umbrella feature:
-----

Init: Enabled
Dnscrypt: Enabled

Timeout:
-----

udp timeout: 5

Orgid:
-----

orgid: 2525316

Resolver config:
-----

RESOLVER IP's
208.67.220.220
```



```
208.67.222.222
2620:119:53::53
2620:119:35::35
```

Dnscrypt Info:

-----

public\_key:

```
A7:A1:0A:38:77:71:D6:80:25:9A:AB:83:B8:8F:94:77:41:8C:DC:5E:6A:14:7C:F7:CA:D3:8E:02:4D:FC:5D:21
magic_key: 71 4E 7A 69 6D 65 75 55
serial number: 1517943461
```

Umbrella Interface Config:

-----

```
09 GigabitEthernet0/0/2 :
    Mode      : IN
    DeviceID  : 010aed3ffe56df
    Tag       : vpn1
10          Loopback1 :
    Mode      : IN
    DeviceID  : 010aed3ffe56df
    Tag       : vpn1
08 GigabitEthernet0/0/1 :
    Mode      : OUT
12          Tunnell1 :
    Mode      : OUT
```

Umbrella Profile Deviceid Config:

-----

```
ProfileID: 0
    Mode      : OUT
ProfileID: 2
    Mode      : IN
    Resolver  : 208.67.220.220
    Local-Domain: True
    DeviceID  : 010aed3ffe56df
    Tag       : vpn1
```

Umbrella Profile ID CPP Hash:

-----

```
VRF ID :: 2
    VRF NAME : 1
    Resolver  : 208.67.220.220
    Local-Domain: True
```

=====

Step 2. Check that the device is successfully registered with the Umbrella DNS Security cloud.

```
dmz2-site201-1#show umbrella deviceid
Device registration details
```

VRF	Tag	Status	Device-id
1	vpn1	200 <b>SUCCESS</b>	010aed3ffe56df

Step 3. Here is how you can check umbrella DNS redirect statistics.

dmz2-site201-1#show platform hardware qfp active feature umbrella datapath stats

Umbrella Connector Stats:

Parser statistics:

parser unknown pkt: 12991  
parser fmt error: 0  
parser count nonzero: 0  
parser pa error: 0  
parser non query: 0  
parser multiple name: 0  
parser dns name err: 0  
parser matched ip: 0  
parser.opendns.redirect: 1234  
local domain bypass: 0  
parser dns others: 9  
no device id on interface: 0  
drop.erc.dnscrypt: 0  
regex locked: 0  
regex not matched: 0  
parser malformed pkt: 0

Flow statistics:

feature object allocs : 1234  
feature object frees : 1234  
flow create requests : 1448  
flow create successful: 1234  
flow create failed, CFT handle: 0  
flow create failed, getting FO: 0  
flow create failed, malloc FO : 0  
flow create failed, attach FO : 0  
flow create failed, match flow: 214  
flow create failed, set aging : 0  
flow lookup requests : 1234  
flow lookup successful: 1234  
flow lookup failed, CFT handle: 0  
flow lookup failed, getting FO: 0  
flow lookup failed, no match : 0  
flow detach requests : 1233  
flow detach successful: 1233  
flow detach failed, CFT handle: 0  
flow detach failed, getting FO: 0  
flow detach failed freeing FO : 0  
flow detach failed, no match : 0  
flow ageout requests : 1  
flow ageout failed, freeing FO: 0  
flow ipv4 ageout requests : 1  
flow ipv6 ageout requests : 0  
flow update requests : 1234  
flow update successful: 1234  
flow update failed, CFT handle: 0  
flow update failed, getting FO: 0  
flow update failed, no match : 0

DNSCrypt statistics:

bypass pkt: 1197968  
clear sent: 0  
enc sent: 1234  
clear rcvd: 0  
dec rcvd: 1234  
pa err: 0  
enc lib err: 0  
padding err: 0  
nonce err: 0  
flow bypass: 0  
disabled: 0

```
flow not enc: 0
DCA statistics:
  dca match success: 0
  dca match failure: 0
```

Step 4. Check that the DNS resolver are reachable with generic tools in order to troubleshoot like ping and traceroute.

Step 5. You can also use Embedded Packet Capture of Cisco IOS-XE in order to perform DNS packets capture going from cEdge.

Refer to the configuration guide for details: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/xs-16-9/epc-xe-16-9-book/nm-packet-capture-xe.html>.

## Understand the Umbrella's EDNS Implementation

Once a packet capture is taken, ensure the DNS queries are correctly redirected to the Umbrella DNS resolvers: 208.67.222.222 and 208.67.220.220 with the correct EDNS0 (Extension Mechanism for DNS) information. With SD-WAN Umbrella DNS layer inspection integration, the cEdge device includes EDNS0 options when it sends DNS queries to the Umbrella DNS resolves. These extensions include the Device ID cEdge receives from Umbrella and the Organization ID for Umbrella in order to identify the correct policy to be used when you answer the DNS query. Here is an example of the EDNS0 packet format:

```
▼ Additional records
  ▼ <Root>: type OPT
    Name: <Root>
    Type: OPT (41)
    UDP payload size: 512
    Higher bits in extended RCODE: 0x00
    EDNS0 version: 0
    ▼ Z: 0x0000
      0... .... = DO bit: Cannot handle DNSSEC security RRs
      .000 0000 0000 0000 = Reserved: 0x0000
    Data length: 39
    ▼ Option: Unknown (26946)
      Option Code: Unknown (26946)
      Option Length: 15
      Option Data: 4f70656e444e53010afb86c9fb1aff
    ▼ Option: Unknown (20292)
      Option Code: Unknown (20292)
      Option Length: 16
      Option Data: 4f444e5300000000225487100b010103
```

Here is the option breakdown:

### RDATA Description:

```
0x4f70656e444e53: Data = "OpenDNS"
0x10afb86c9fb1aff: Device-ID
```

### RDATA Remote IP Address Option:

```
0x4f444e53: MGGIC = 'ODNS'
0x00       : Version
0x00       : Flags
0x08       : Organization ID Required
0x00225487: Organization ID
0x10 type  : Remote IPv4
0x0b010103: Remote IP Address = 11.1.1.3
```

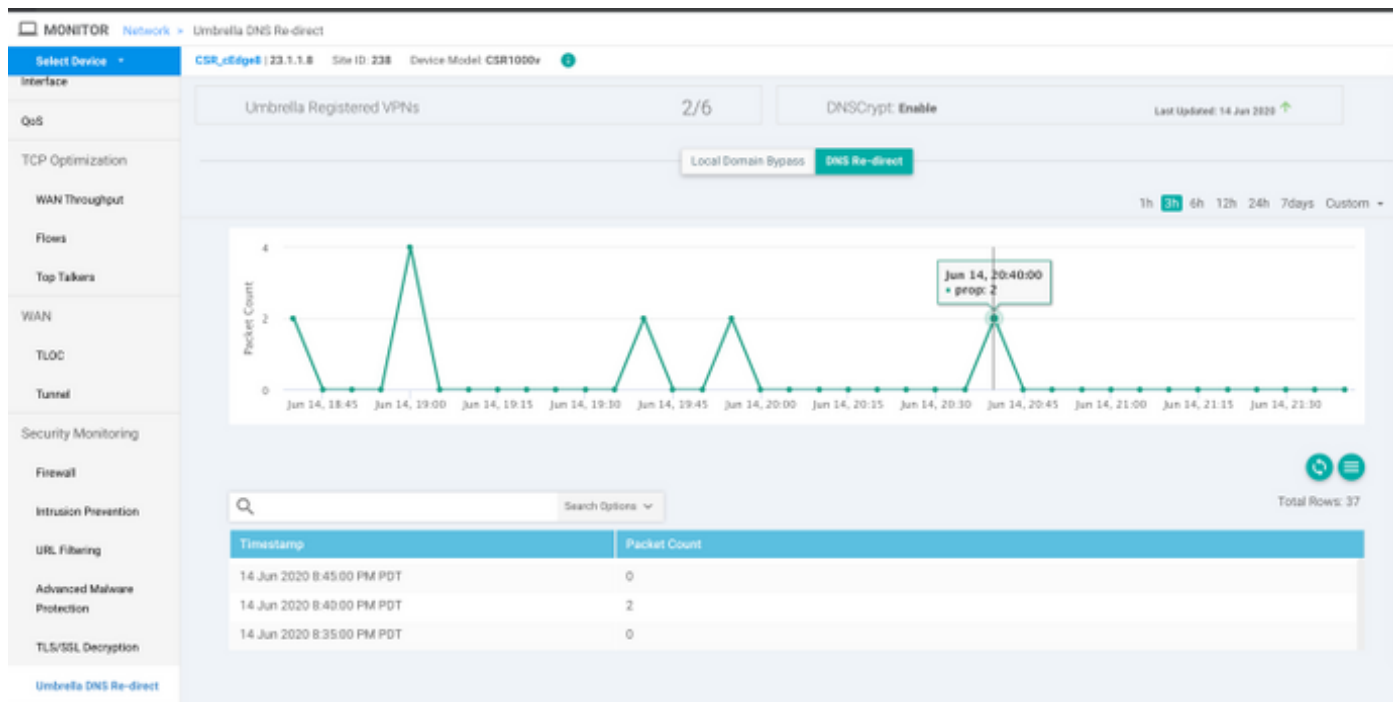
Check and ensure that the Device-ID is correct and the Organization ID matches the Umbrella

account with the use of the Umbrella portal.

**Note:** With DNSCrypt enabled, DNS queries are encrypted. If the packet captures show DNSCrypt packet going to the Umbrella resolver but there is no return traffic, try to disable DNSCrypt to see if that's the problem.

## Verify it on vManage Dashboard

Any Cisco Umbrella directed traffic can be viewed from vManage Dashboard. It can be viewed under **Monitor > Network > Umbrella DNS Re-direct**. Here is the image of this page:



## DNS Caching

On a Cisco cEdge router, local domain-bypass flags sometimes don't match. This happens when there is a caching involved in the host machine/client. As an example, if local domain-bypass is configured to match and bypass [www.cisco.com](http://www.cisco.com) (**.\*cisco.com**). The first time, the query was for [www.cisco.com](http://www.cisco.com) which also returned CDN names as CNAMEs, which were cached on the client. Subsequent queries for nslookup for [www.cisco.com](http://www.cisco.com) were to send only the queries for the CDN domain (akamaiedge).

Non-authoritative answer:

```
www.cisco.com canonical name = www.cisco.com.akadns.net.  
www.cisco.com.akadns.net canonical name = wwwds.cisco.com.edgekey.net.  
wwwds.cisco.com.edgekey.net canonical name = wwwds.cisco.com.edgekey.net.globalredir.akadns.net.  
wwwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e2867.dsca.akamaiedge.net.  
Name: e2867.dsca.akamaiedge.net  
Address: 104.103.35.55  
Name: e2867.dsca.akamaiedge.net  
Address: 2600:1408:8400:5ab::b33  
Name: e2867.dsca.akamaiedge.net  
Address: 2600:1408:8400:59c::b33
```

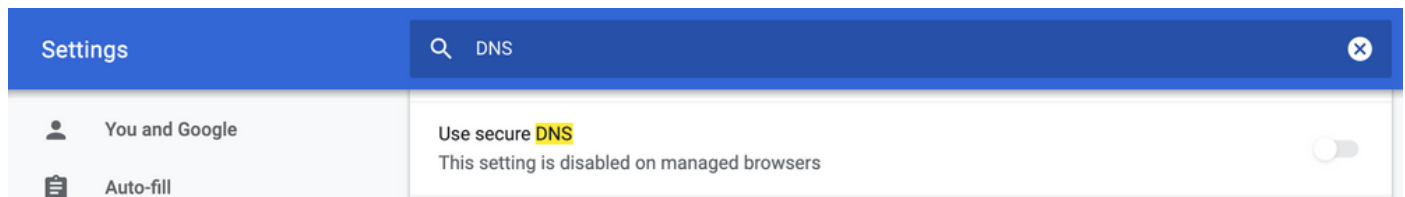
If local domain-bypass works properly, you will see that the counters increase for parser OpenDNS redirect. Here is an abbreviated output.

```
dmz2-site201-1#show platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats:
  Parser statistics:
    parser unknown pkt: 0
    parser fmt error: 0
    parser count nonzero: 0
    parser pa error: 0
    parser non query: 0
    parser multiple name: 0
    parser dns name err: 0
    parser matched ip: 0
    parser.opendns.redirect: 3
    local domain bypass: 0 <<<<<<<<<<<<<
```

This could be the reason, as to why local domain bypass is not seen on the router. When you clear the cache on the host/client machine, you see that the queries go out correctly.

## Secure DNS

Modern browsers like Google Chrome starting from version 83 are using Secure DNS also known as DNS over HTTPS (DoH) or DNS over TLS (DoT). This feature can make Umbrella DNS security capability impossible to use if not carefully planned. Secure DNS can be disabled via centralized policies and disabled by default, for example, for Enterprise managed computers.



For unmanaged BYOD devices there are few options exist. First option is to block TCP port 853 which is used by Secure DNS. You can use Cisco Zone Based Firewall (ZBFW) for this puurpose. Second option would be to enable "Proxy/Anonymizer" category blocking on Umbrella portal. You can find more information about this here

<https://support.umbrella.com/hc/en-us/articles/360001371526-Web-Browsers-and-DNS-over-HTTPS-default>

## Conclusion

As you can see, integration with the Umbrella DNS Security cloud is very simple from cEdge side and can be done in a few minutes.