

Integratie met Cisco Umbrella en problemen oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Probleemoplossing controleren](#)

[Clientverificatie](#)

[cEdge-verificatie](#)

[Begrijp de EDNS-implementatie van Umbrella](#)

[Controleer dit op vManager-dashboard](#)

[DNS-routing](#)

[Secure DNS](#)

[Conclusie](#)

Inleiding

Dit document beschrijft vManager/Cisco IOS®-XE SDWAN-softwaredeel van de integratie met de Cisco Umbrella DNS-beveiligingsoplossing. Het heeft echter geen betrekking op de Umbrella-beleidsconfiguratie zelf. U kunt hier meer informatie vinden over Cisco Umbrella; <https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella>.

Opmerking: U moet al Umbrella-abonnementen hebben aangeschaft en Umbrella-token hebben die gebruikt zal worden in de configuratie van cEdge-routers. Meer informatie over API-token: <https://docs.umbrella.com/umbrella-api/docs/overview2>.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- vManager 18.4.0
- Cisco IOS-XE SDWAN-router (cEdge) 16.9.3

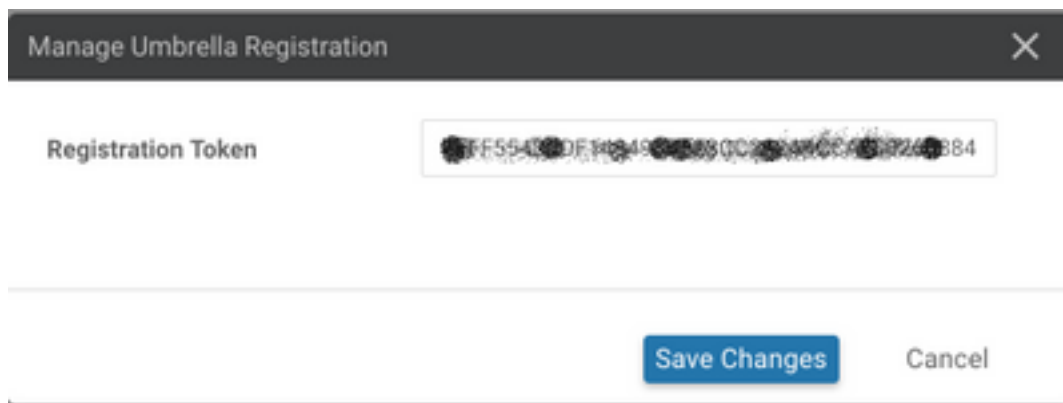
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Om uw cEdge-integratie met Cisco Umbrella te configureren voert u een verzameling eenvoudige stappen uit op vManager:


Stap 1. Onder **Verdeling > Beveiliging**, selecteert u **Aangepaste opties** in de vervolgkeuzelijst boven in de rechterhoek en vervolgens selecteert u **Umbrella API-token**. Voer uw Umbrella-registratoken in, zoals in de afbeelding:



The image shows a dialog box titled "Manage Umbrella Registration". It features a close button (X) in the top right corner. The main content area contains a label "Registration Token" and a text input field with a blurred hexadecimal string: "FF5540DE484908830C2544CC75B26884". At the bottom of the dialog, there are two buttons: "Save Changes" and "Cancel".

U kunt ook een Organisatie-id, een Registratiesleutel en een geheim instellen vanaf de release van vManager software 20.1.1. Deze parameters kunnen automatisch worden opgeroepen als u uw slimme accountreferenties hebt ingesteld onder **Beheer > Instellingen > 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

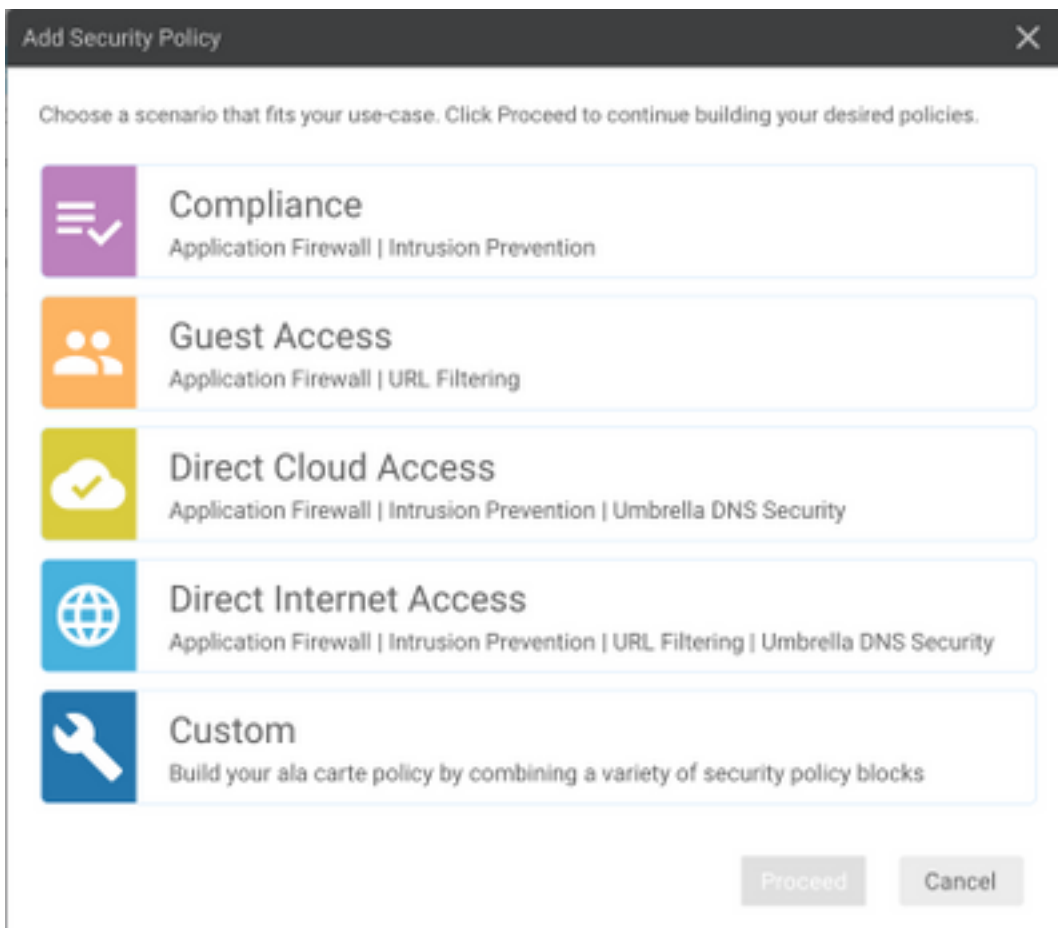
Required for legacy devices

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

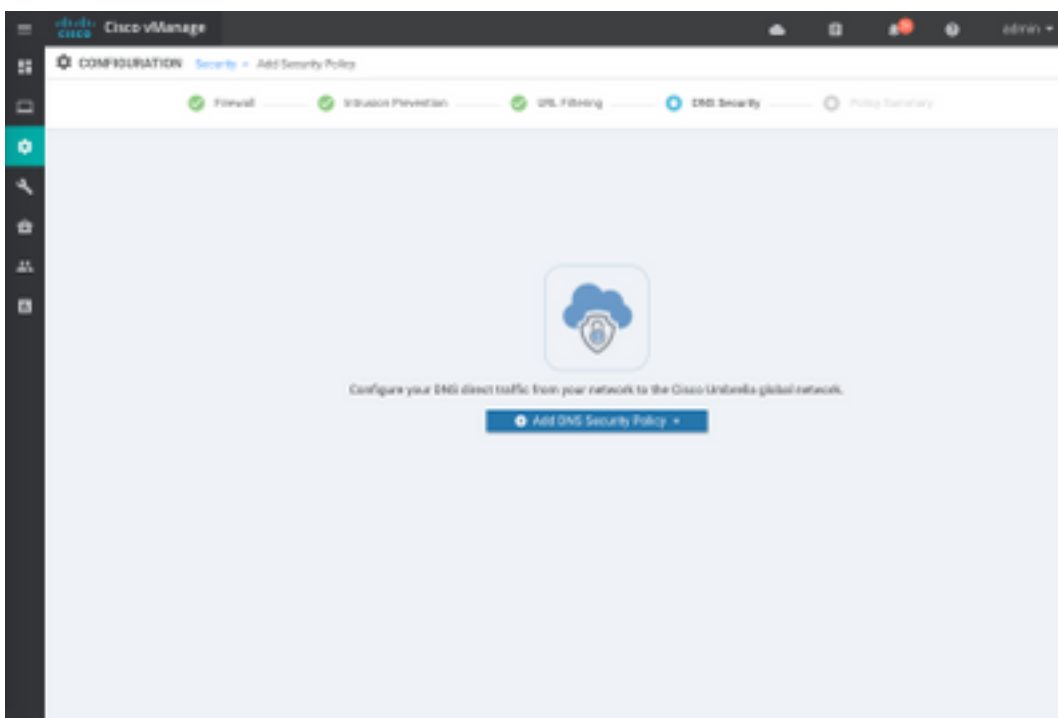
[Save Changes](#)

Cancel

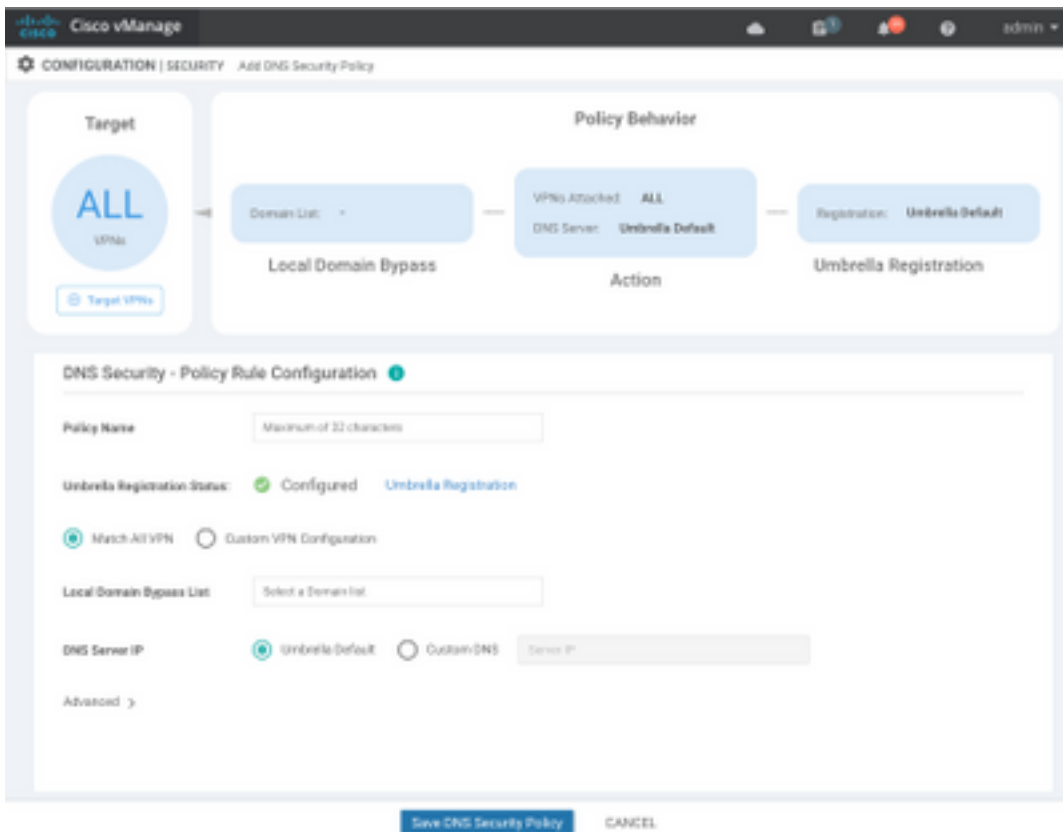
Stap 2. Onder **Configuration > Security**, selecteert u **Add Security Policy** en vervolgens selecteert u een scenario dat aansluit bij uw gebruikerscase (bijv. aangepaste), zoals in de afbeelding:



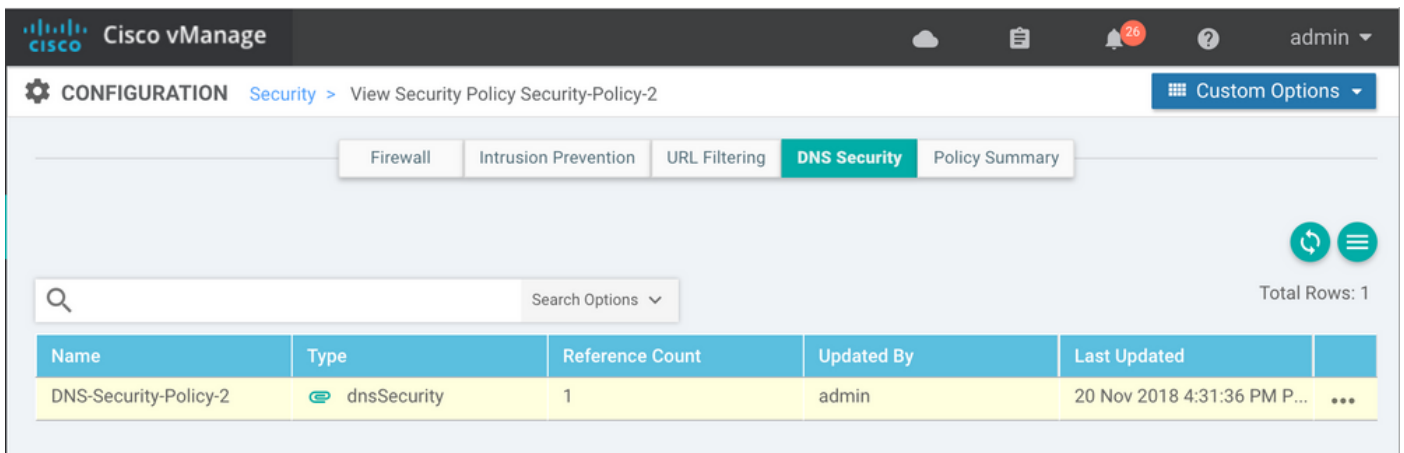
Stap 3. Zoals in de afbeelding wordt getoond, navigeer naar **DNS-beveiliging**, selecteer **DNS-beveiligingsbeleid toevoegen** en selecteer **Nieuw**.



Het scherm lijkt op het beeld dat hier wordt getoond:



Stap 4. Dit is de afbeelding van de manier waarop het wordt weergegeven, zodra het is geconfigureerd.



Stap 5. Navigeer naar ...> **Beeld** > **DNS Security** tab van uw beleid, u ziet een configuratie die vergelijkbaar is met dit beeld:

The screenshot displays the Cisco vManage configuration page for a DNS Security Policy. The top navigation bar shows 'Cisco vManage' and 'admin'. The main header is 'CONFIGURATION | SECURITY View DNS Security Policy'. The interface is divided into three main sections: 'Target', 'Policy Behavior', and 'DNS Security - Policy Rule Configuration'. The 'Target' section shows a blue circle with 'ALL VPNs'. The 'Policy Behavior' section shows three boxes: 'Local Domain Bypass' (Domain List: domainbypasslist), 'Action' (VPNs Attached: ALL, DNS Server: Umbrella Default), and 'Umbrella Registration' (Registration: Umbrella Default). The 'DNS Security - Policy Rule Configuration' section contains the following fields: Policy Name (DNS-Security-Policy-2), Umbrella Registration Status (Configured), Match All VPN (selected), Local Domain Bypass List (domainbypasslist), and DNS Server IP (Umbrella Default selected). An 'Advanced >' link is at the bottom left of the configuration section.

Houd in gedachten dat "Local Domain Bypass List" een lijst is van domeinen waarvoor de router DNS-verzoeken niet opnieuw naar Umbrella-cloud richt en een DNS-aanvraag naar een specifieke DNS-server (DNS-server binnen het ondernemingsnetwerk) stuurt, dit is niet uitgesloten van het Umbrella-beveiligingsbeleid. Om een aantal domeinen van de specifieke categorie te "witteren", wordt aangeraden om in plaats daarvan uitsluiting te configureren op een Umbrella-configuratieportal.

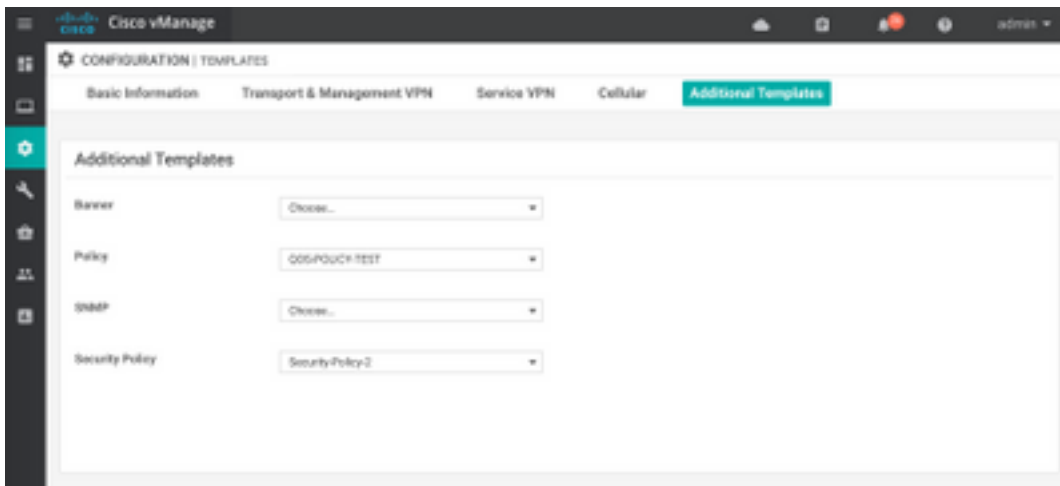
U kunt ook **Preview** selecteren om te begrijpen hoe de configuratie in CLI ziet:

```

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

```

Stap 6. U moet nu het beleid in de apparaatsjabloon bekijken. Selecteer onder **Configuration > Templates**, de configuratiesjabloon en referentie deze in het **gedeelte Extra sjablonen** zoals in de afbeelding.



Stap 7. Pas de sjabloon op het apparaat toe.

Probleemoplossing controleren

Gebruik deze sectie om te bevestigen dat uw configuratie correct werkt en het oplossen van problemen.

Clientverificatie

Vanuit een client die achter de cEdge zit, kunt u controleren of Umbrella correct werkt wanneer u door deze testsites bladert:

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

Zie voor meer informatie [Hoe: Test met succes om te controleren of u Umbrella correct gebruikt](#)

cEdge-verificatie

Verificatie en probleemoplossing kunnen ook op de cEdge zelf worden uitgevoerd. In het algemeen is het vergelijkbaar met Cisco IOS-XE procedures voor probleemoplossing bij softwareintegratie die kunnen worden gevonden in hoofdstuk 2 van Cisco Umbrella Integration op Cisco 4000 Series ISR's 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/xe-16-9/sec-data-umbrella-branch-xe-16-9-book.pdf.

Weinig nuttige opdrachten om te controleren:

Stap 1. Controleer dat parameter-map in cEdge-configuratie op het apparaat wordt weergegeven:

```
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
!
```

Merk op dat u geen verwijzing naar deze parameter-map op de interface kunt vinden zoals u gebruikt wordt om deze op Cisco IOS-XE te zien.

Dit komt doordat parameter-map is toegepast op VRF's en niet op interfaces, kunt u het hier controleren:

```
dmz2-site201-1#show umbrella config
Umbrella Configuration
=====
Token: XFFFX543XDF14X498X623CX222X4CCAX0026X88X
OrganizationID: 2525316
Local Domain Regex parameter-map name: domainbypasslist
DNSEncrypt: 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
```

Daarnaast kunt u deze opdracht gebruiken voor uitgebreide informatie:

```
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           Tunnel1  :  
   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. Controleer dat het apparaat met succes is geregistreerd in de Umbrella DNS-beveiligingscloud.
```

```
dmz2-site201-1#show umbrella deviceid
```

Device registration details

VRF	Tag	Status	Device-id
1	vpn1	200 SUCCESS	010aed3ffe56df

Stap 3. Hier is hoe u kunt controleren of een DNS-heroriëntering van de paraplu is ingeschakeld.

```
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
```

Stap 4. Controleer dat de DNS-resolutie bereikbaar is met generieke tools om problemen op te lossen zoals ping en traceroute.

Stap 5. U kunt ook de ingesloten pakketvastlegging van Cisco IOS-XE gebruiken om DNS-pakketten uit cEdge uit te voeren.

Raadpleeg de configuratiehandleiding voor meer informatie:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/xo-16-9/epc-xo-16-9-book/nm-packet-capture-xo.html>.

Begrijp de EDNS-implementatie van Umbrella

Controleer, wanneer een pakketvastlegging is gemaakt, of de DNS-vragen correct opnieuw naar de Umbrella DNS-resoluties worden gericht: 208.67.222.222 en 208.67.220.220 met de juiste DNS-DNS-laag (uitbreidingsmechanisme voor) met SD-WAN- laag inspectie-integratie, het cEdge-apparaat bevat EDNS0-opties wanneer het DNS-vragen naar de Umbrella-DNS-oplossing stuurt. Deze uitbreidingen omvatten de apparaatid-ID cEdge van Umbrella en de organisatie-ID voor Umbrella om het juiste beleid te bepalen dat moet worden gebruikt wanneer u de DNS-query beantwoordt. Hier is een voorbeeld van de EDNS0-pakketindeling:

```
▼ 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
```

Hier is de optie-uitsplitsing:

GEGEVENSbeschrijving:

0x4f70656e444e53: Data = "OpenDNS"

0x10afb86c9fb1aff: Device-ID

RDATA Remote IP-adresoptie:

0x4f444e53: MGGIC = 'ODNS'

0x00 : Version

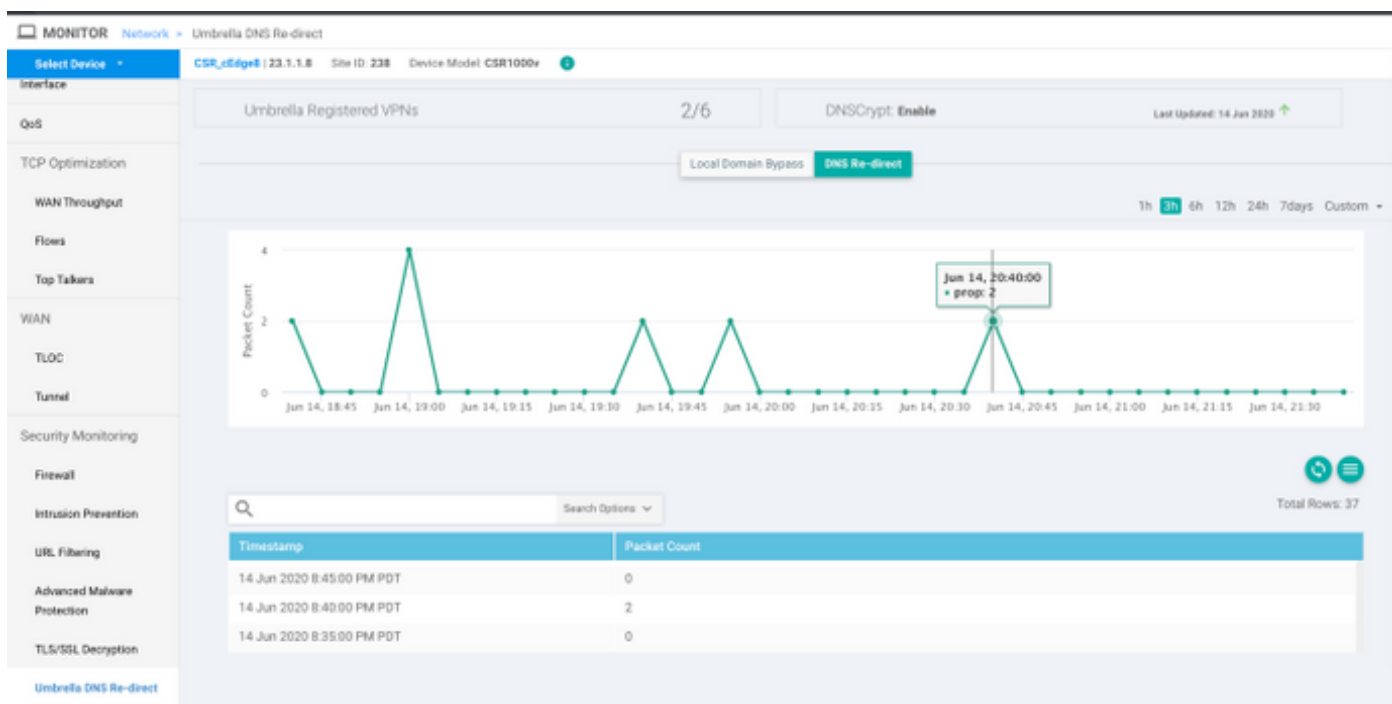
0x00 : Flags
0x08 : Organization ID Required
0x00225487: Organization ID
0x10 type : Remote IPv4
0x0b010103: Remote IP Address = 11.1.1.3

Controleer en zorg ervoor dat de machine-ID juist is en dat de organisatie-ID overeenkomt met de Umbrella-account met het gebruik van de Umbrella-portal.

Opmerking: Indien DNSCrypt ingeschakeld is, worden DNS vragen versleuteld. Als het pakket DNS-crypt-pakje bij de Umbrella-oplossing levert maar er geen retourverkeer is, probeert u DNSCrypt uit te schakelen om te zien of dat het probleem is.

Controleer dit op vManager-dashboard

Elk Cisco Umbrella-gericht verkeer kan vanaf vManager-dashboard worden bekeken. U kunt het bekijken onder **Monitor > Network > Umbrella DNS Re-direct**. Dit is de afbeelding van deze pagina:



DNS-routing

Op een router van Cisco cEdge komen de vlaggen van de lokale domein-bypass soms niet overeen. Dit gebeurt wanneer er een caching betrokken is bij de host machine/client. Als voorbeeld, als de lokale domein-bypass om te passen en te omzeilen www.cisco.com (*cisco.com). De eerste keer was de query voor www.cisco.com die ook CDN-namen als CNAME's teruggaf, die op de client waren gecached. Latere vragen voor nslookup voor www.cisco.com waren alleen de vragen voor het CDN-domein (akamaiedge) verzenden.

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

