

Configurazione dell'integrazione con Cisco Umbrella e risoluzione dei problemi comuni

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica e risoluzione dei problemi](#)

[Verifica client](#)

[Verifica cEdge](#)

[Comprendere l'implementazione EDNS dell'Umbrella](#)

[Verifica sul dashboard vManage](#)

[Cache DNS](#)

[DNS sicuro](#)

[Conclusioni](#)

Introduzione

Questo documento descrive il software vManage/Cisco IOS®-XE SDWAN come parte dell'integrazione con la soluzione di sicurezza Cisco Umbrella DNS. Tuttavia, non copre la configurazione dei criteri Umbrella stessa. Per ulteriori informazioni su Cisco Umbrella, visitare il sito Web <https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella>.

Nota: È necessario aver già ottenuto le sottoscrizioni Umbrella e ottenere il token Umbrella che verrà utilizzato nella configurazione dei router cEdge. Ulteriori informazioni sul token API: <https://docs.umbrella.com/umbrella-api/docs/overview2>.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.


Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- vManage 18.4.0
- Router Cisco IOS®-XE SDWAN con (cEdge) 16.9.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

Cisco Umbrella Registration Key and Secret ℹ

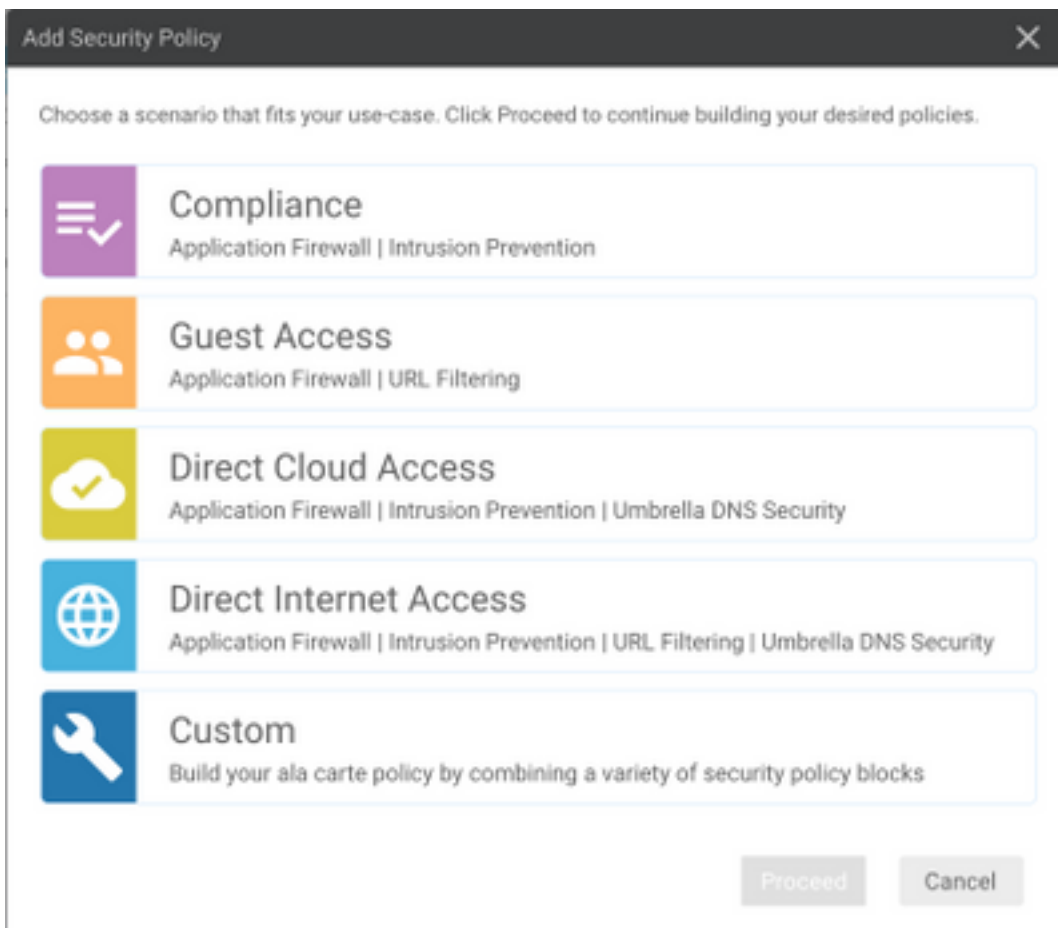
Organization ID	<input type="text" value="Enter Organization ID"/>	
Registration Key	<input type="text" value="Enter Registration Key"/>	
Secret	<input type="text" value="Enter Secret"/>	
		<input type="button" value="Get Keys"/>

Cisco Umbrella Registration Token ℹ

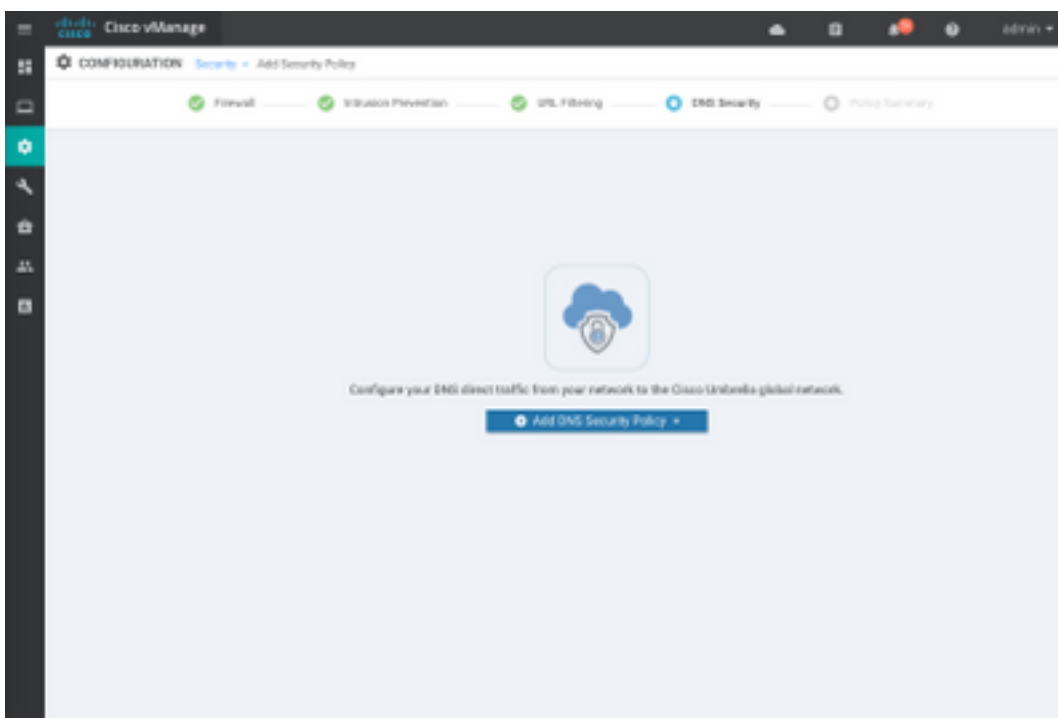
Required for legacy devices

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

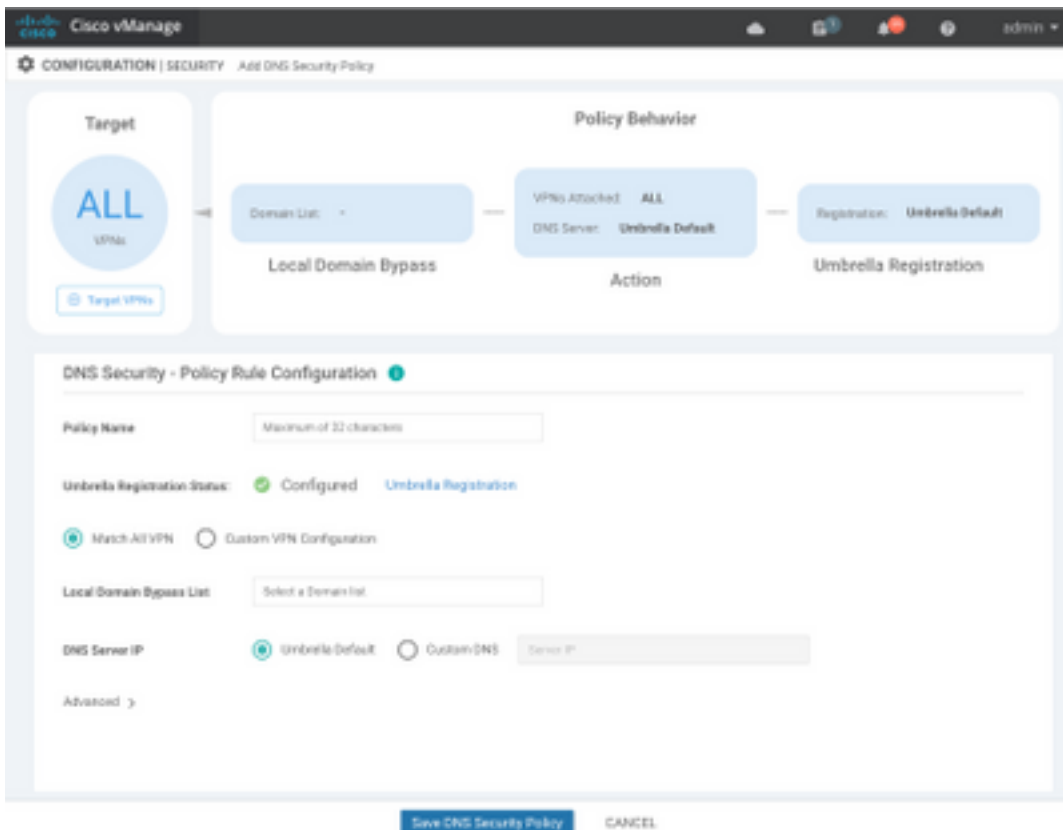
Passaggio 2. In **Configurazione > Protezione**, selezionare **Aggiungi criterio di protezione**, quindi selezionare uno scenario che si adatti allo Use Case (ad esempio personalizzato), come mostrato nell'immagine:



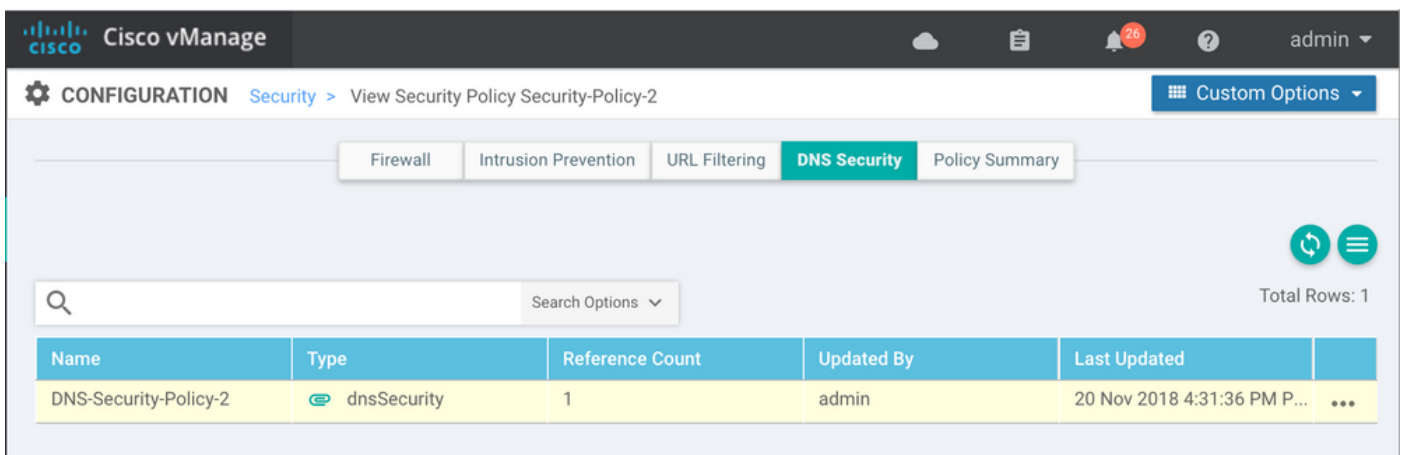
Passaggio 3. Come mostrato nell'immagine, passare a **Sicurezza DNS**, selezionare **Aggiungi criterio di sicurezza DNS**, quindi selezionare **Crea nuovo**.



La schermata appare simile all'immagine mostrata di seguito:



Passaggio 4. Questa è l'immagine di come appare, una volta configurata.



Passaggio 5. Passare a ...> **Visualizza** > scheda **Sicurezza DNS** del criterio. Verrà visualizzata una configurazione simile a questa immagine:

The screenshot displays the Cisco vManage configuration interface for a DNS Security Policy. The top navigation bar shows 'CONFIGURATION | SECURITY View DNS Security Policy' and a 'Custom Options' dropdown. The main content area is divided into two sections: 'Target' and 'Policy Behavior'. The 'Target' section shows a blue circle with 'ALL VPNs'. The 'Policy Behavior' section is divided into three sub-sections: 'Local Domain Bypass' (Domain List: domainbypasslist), 'Action' (VPNs Attached: ALL, DNS Server: Umbrella Default), and 'Umbrella Registration' (Registration: Umbrella Default). Below these sections is the 'DNS Security - Policy Rule Configuration' form, which includes fields for 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 visible at the bottom of the form.

Tenere presente che "Local Domain Bypass List" è un elenco di domini per i quali il router non reindirizza le richieste DNS al cloud Umbrella e invia la richiesta DNS a un server DNS specifico (server DNS situato nella rete aziendale), questa non è un'esclusione dai criteri di sicurezza Umbrella. Per poter "elencare" alcuni domini della categoria specifica, si consiglia di configurare l'esclusione sul portale di configurazione Umbrella.

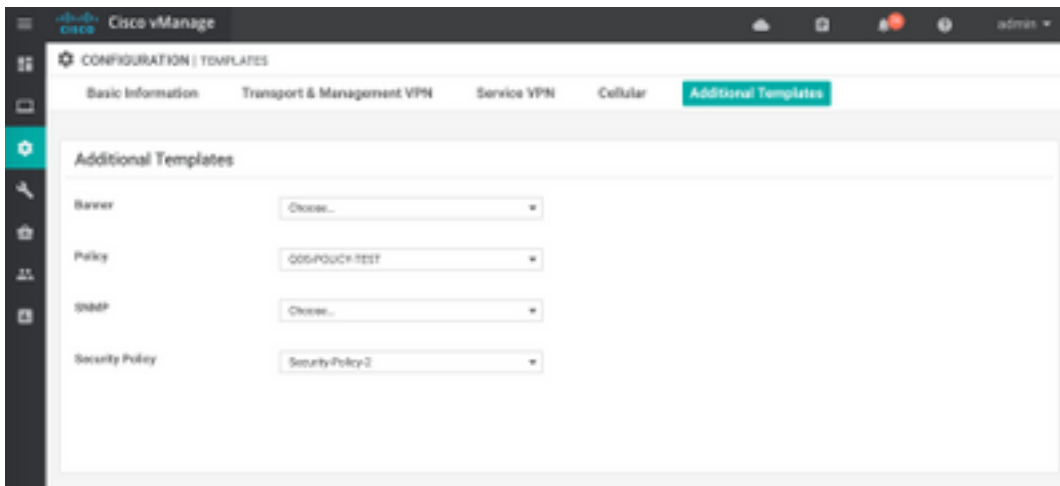
Inoltre, è possibile selezionare **Preview** per comprendere come appare la configurazione nella CLI:

```

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

```

Passaggio 6. A questo punto è necessario fare riferimento ai criteri nel modello di dispositivo. In **Configurazione > Modelli**, selezionare il modello di configurazione e fare riferimento a esso nella sezione **Modelli aggiuntivi** come mostrato nell'immagine.



Passaggio 7. Applicare il modello al dispositivo.

Verifica e risoluzione dei problemi

Per verificare che la configurazione funzioni correttamente e per risolvere i problemi, consultare questa sezione.

Verifica client

Da un cliente seduto dietro il cEdge, è possibile verificare se Umbrella funziona correttamente quando si navigano questi siti di test:

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

Per ulteriori informazioni, vedere [Procedura: Prova per verificare che Umbrella funzioni correttamente](#)

Verifica cEdge

La verifica e la risoluzione dei problemi possono essere eseguite anche sullo stesso cEdge. In generale, è simile alle procedure di risoluzione dei problemi di integrazione del software Cisco IOS-XE riportate nel capitolo 2 Cisco Umbrella Integration sulla guida alla configurazione dei Cisco serie 4000 ISR di sicurezza: 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.

Pochi comandi utili da controllare:

Passaggio 1. Verificare che la mappa dei parametri sia presentata nella configurazione cEdge nel dispositivo:

```
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
!
```

Si noti che non è possibile trovare un riferimento a questa mappa dei parametri sull'interfaccia in quanto ci si abitua a vederla su Cisco IOS-XE.

Questo perché la mappa dei parametri viene applicata ai VRF e non alle interfacce, è possibile verificarla qui:

```
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
```

Inoltre, è possibile usare questo comando per ottenere informazioni dettagliate:

```
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

=====

Passaggio 2. Verificare che il dispositivo sia stato registrato correttamente nel cloud di sicurezza DNS Umbrella.

dmz2-site201-1#show umbrella deviceid

Device registration details

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

Passaggio 3. Di seguito viene riportata la procedura per verificare le statistiche di reindirizzamento DNS umbrella.

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
```

Passaggio 4. Verificare che il resolver DNS sia raggiungibile con strumenti generici per risolvere problemi quali ping e traceroute.

Passaggio 5. È inoltre possibile utilizzare Embedded Packet Capture di Cisco IOS-XE per eseguire l'acquisizione dei pacchetti DNS da cEdge.

Fare riferimento alla guida alla configurazione per i dettagli:

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

Comprendere l'implementazione EDNS dell'Umbrella

Una volta acquisito un pacchetto, assicurarsi che le query DNS vengano reindirizzate correttamente ai resolver DNS Umbrella: 208.67.222.222 e 208.67.220.220 con le informazioni EDNS0 (Extension Mechanism for DNS) corrette. Con l'integrazione SD-WAN Umbrella DNS Layer Inspection, il dispositivo cEdge include le opzioni EDNS0 quando invia query DNS alle resolve DNS Umbrella. Queste estensioni includono l'ID dispositivo cEdge ricevuto da Umbrella e l'ID organizzazione per Umbrella per identificare il criterio corretto da utilizzare quando si risponde alla query DNS. Di seguito è riportato un esempio del formato del pacchetto EDNS0:

```
▼ 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
```

Di seguito è riportata la suddivisione delle opzioni:

Descrizione RDATA:

0x4f70656e444e53: Data = "OpenDNS"

0x10afb86c9fb1aff: Device-ID

Opzione RDATA Remote IP Address:

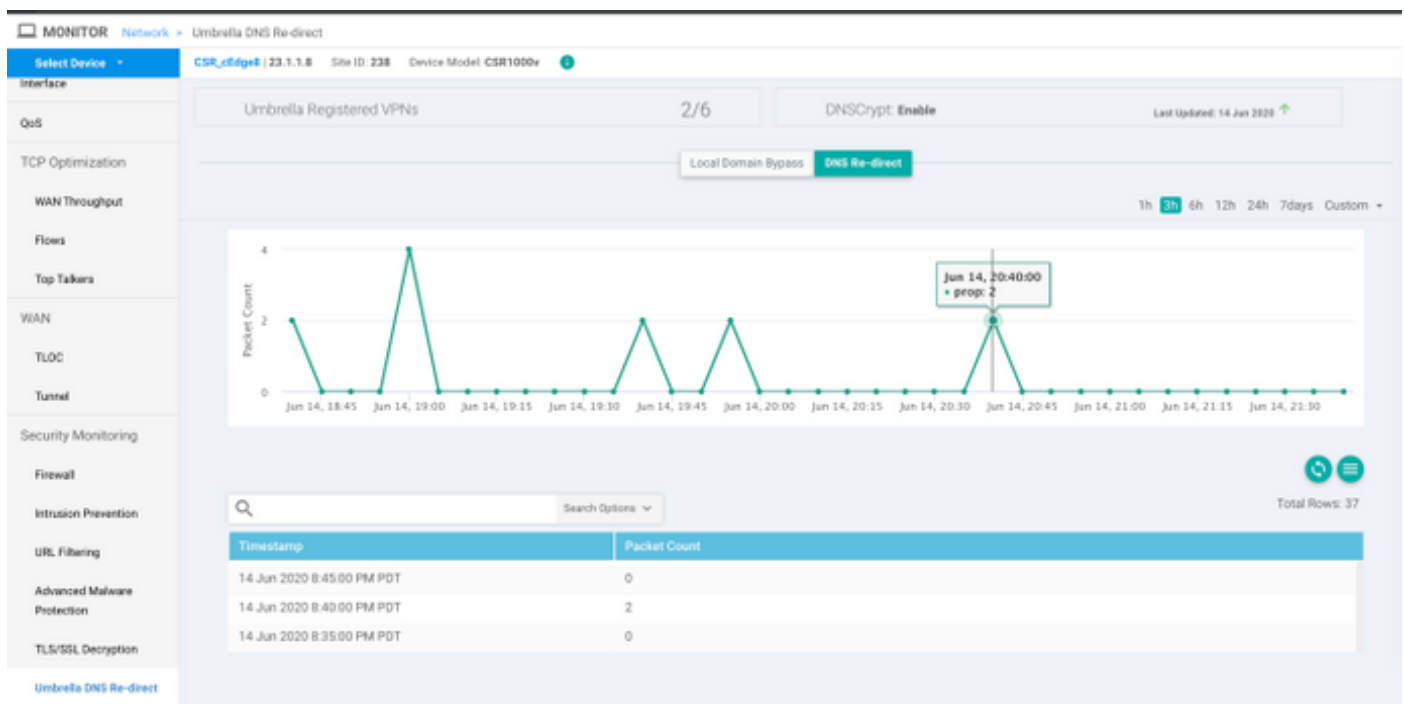
```
0x4f444e53: MGGIC = 'ODNS'  
0x00      : Version  
0x00      : Flags  
0x08      : Organization ID Required  
0x00225487: Organization ID  
0x10 type : Remote IPv4  
0x0b010103: Remote IP Address = 11.1.1.3
```

Verificare e verificare che l'ID dispositivo sia corretto e che l'ID organizzazione corrisponda all'account Umbrella con l'utilizzo del portale Umbrella.

Nota: Se DNSCrypt è abilitato, le query DNS vengono crittografate. Se il pacchetto viene acquisito e il pacchetto DNSCrypt va al resolver Umbrella, ma non c'è traffico di ritorno, provare a disabilitare DNSCrypt per verificare se è questo il problema.

Verifica sul dashboard vManage

Qualsiasi traffico diretto da Cisco Umbrella può essere visualizzato da vManage Dashboard. Può essere visualizzato in **Monitor > Network > Umbrella DNS Re-direct**. Ecco l'immagine di questa pagina:



Cache DNS

Su un router Cisco cEdge, i flag di bypass del dominio locale a volte non corrispondono. Ciò si verifica quando è presente una cache nel computer host/client. Ad esempio, se la funzione di bypass del dominio locale è configurata in modo da corrispondere e ignorare www.cisco.com (*.cisco.com). La prima volta, la query è stata eseguita per www.cisco.com che ha restituito anche nomi CDN come CNAME, memorizzati nella cache del client. Le query successive per nslookup per www.cisco.com dovevano inviare solo le query per il dominio CDN (akamaiedge).

Non-authoritative answer:

www.cisco.com canonical name = www.cisco.com.akadns.net.

cEdge e può essere fatta in pochi minuti.