

Configuración de la integración con Cisco Umbrella y resolución de problemas comunes

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación y resolución de problemas](#)

[Verificación del cliente](#)

[Verificación de CEdge](#)

[Comprender la implementación de EDNS del paraguas](#)

[Verificarlo en el panel vManage](#)

[Almacenamiento en caché de DNS](#)

[DNS seguro](#)

[Conclusión](#)

Introducción

Este documento describe el software vManage/Cisco IOS®-XE SDWAN que forma parte de la integración con la solución de seguridad DNS de Cisco Umbrella. Sin embargo, no cubre la configuración de las políticas generales en sí. Puede encontrar más información sobre Cisco Umbrella aquí; <https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella>.

Nota: Ya tiene que haber obtenido suscripciones de Umbrella y obtener un token de Umbrella que se utilizará en la configuración de los routers cEdge. Más sobre el token de API: <https://docs.umbrella.com/umbrella-api/docs/overview2>.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

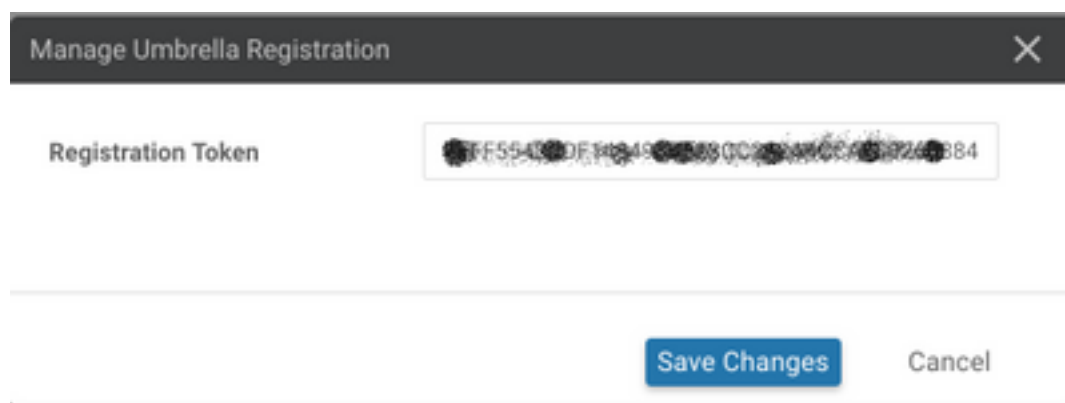
The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Para configurar la integración de cEdge con Cisco Umbrella, realice un conjunto de pasos sencillos en vManage:


Paso 1. En **Configuration > Security**, seleccione la lista desplegable **Custom Options** en la esquina superior derecha y, a continuación, seleccione **Umbrella API token**. Introduzca el token de registro de Umbrella, como se muestra en la imagen:



The image shows a dialog box titled "Manage Umbrella Registration". It contains a "Registration Token" field with the value "FF5540DF404908830C2040CC708224884". At the bottom, there are "Save Changes" and "Cancel" buttons.

Alternativamente, a partir de la versión 20.1.1 del software vManage puede especificar ID de organización, clave de registro y secreto. Estos parámetros se pueden recuperar automáticamente si ha configurado sus credenciales de Smart Account bajo **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

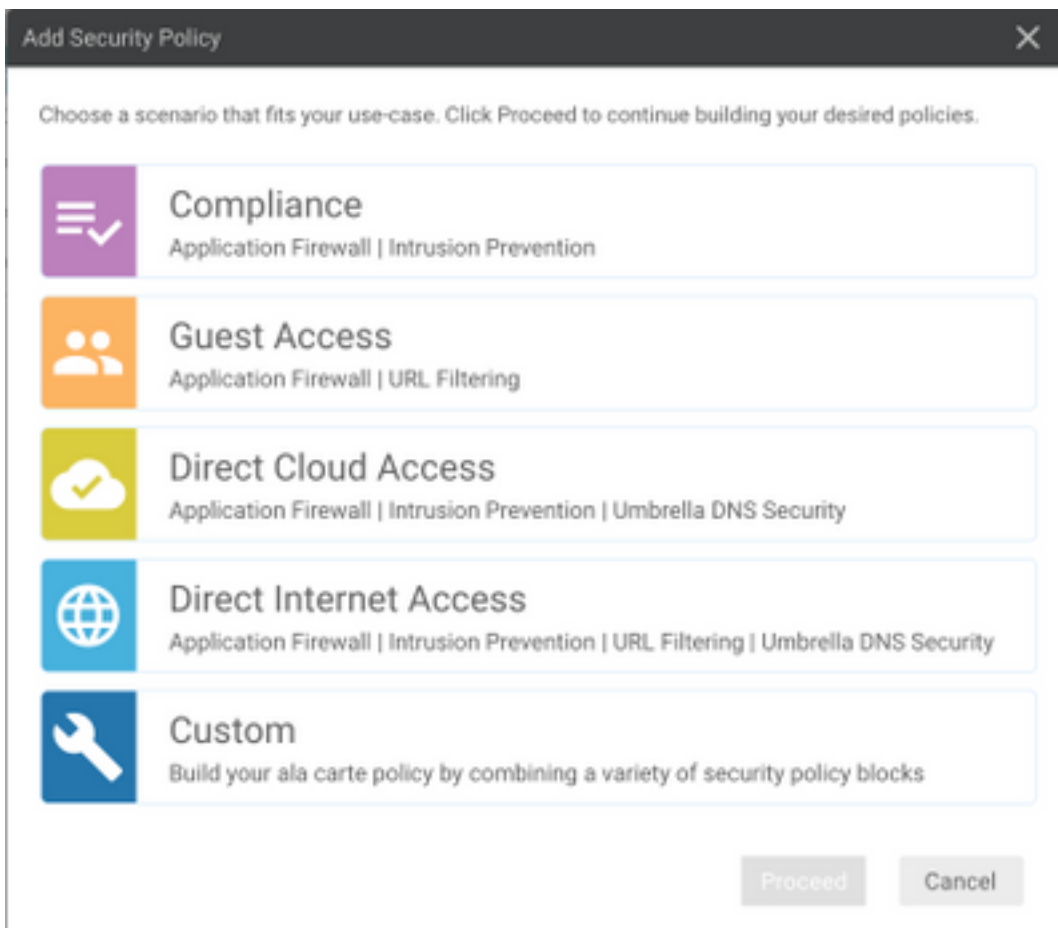
Required for legacy devices

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

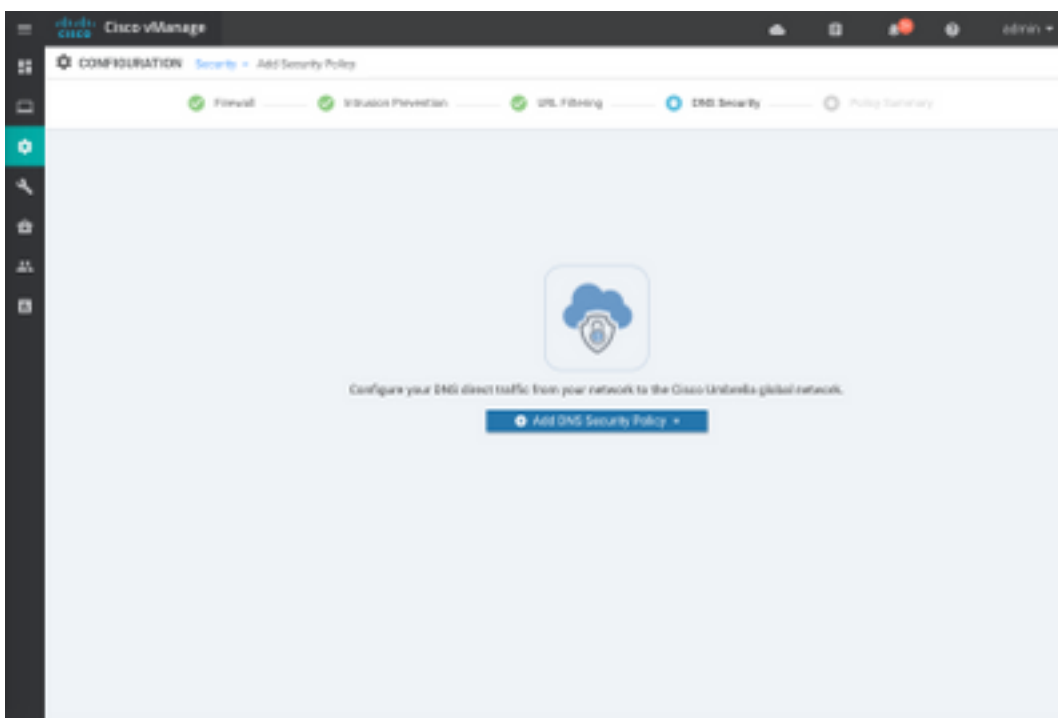
[Save Changes](#)

Cancel

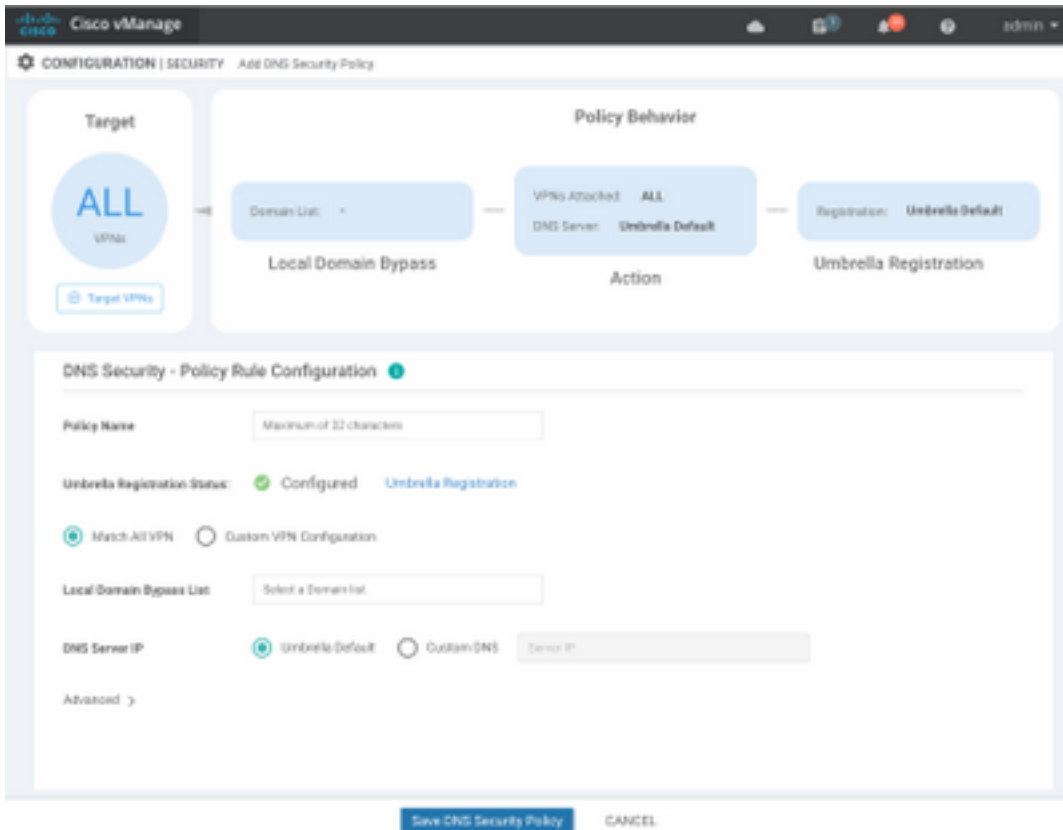
Paso 2. En **Configuration > Security**, seleccione **Add Security Policy** y, a continuación, seleccione un escenario que se ajuste al caso práctico (por ejemplo, personalizado), como se muestra en la imagen:



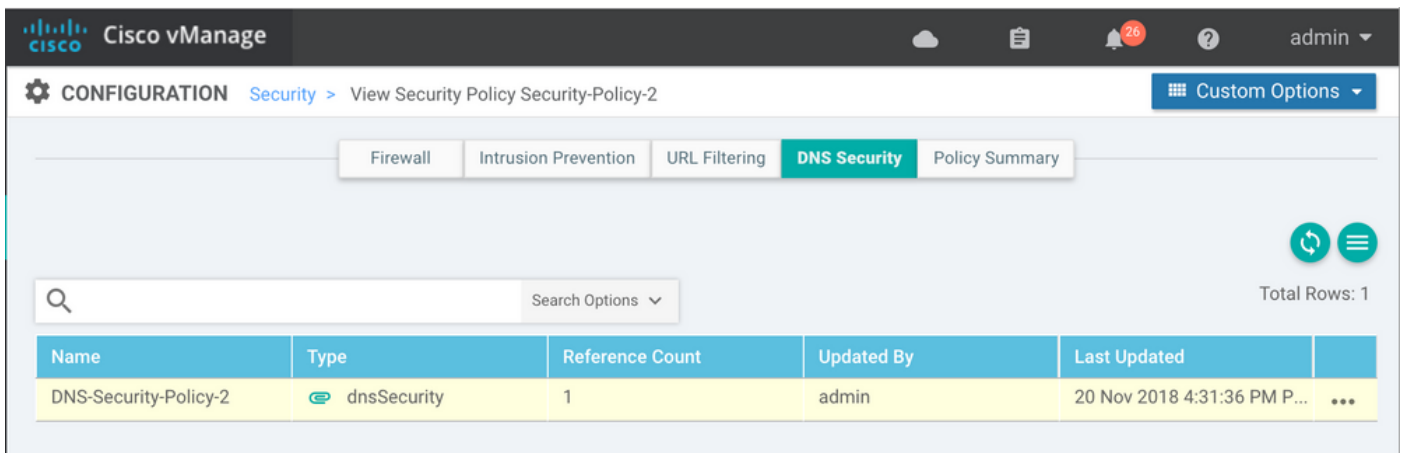
Paso 3. Como se muestra en la imagen, navegue hasta **Seguridad DNS**, seleccione **Agregar política de seguridad DNS** y, a continuación, seleccione **Crear nuevo**.



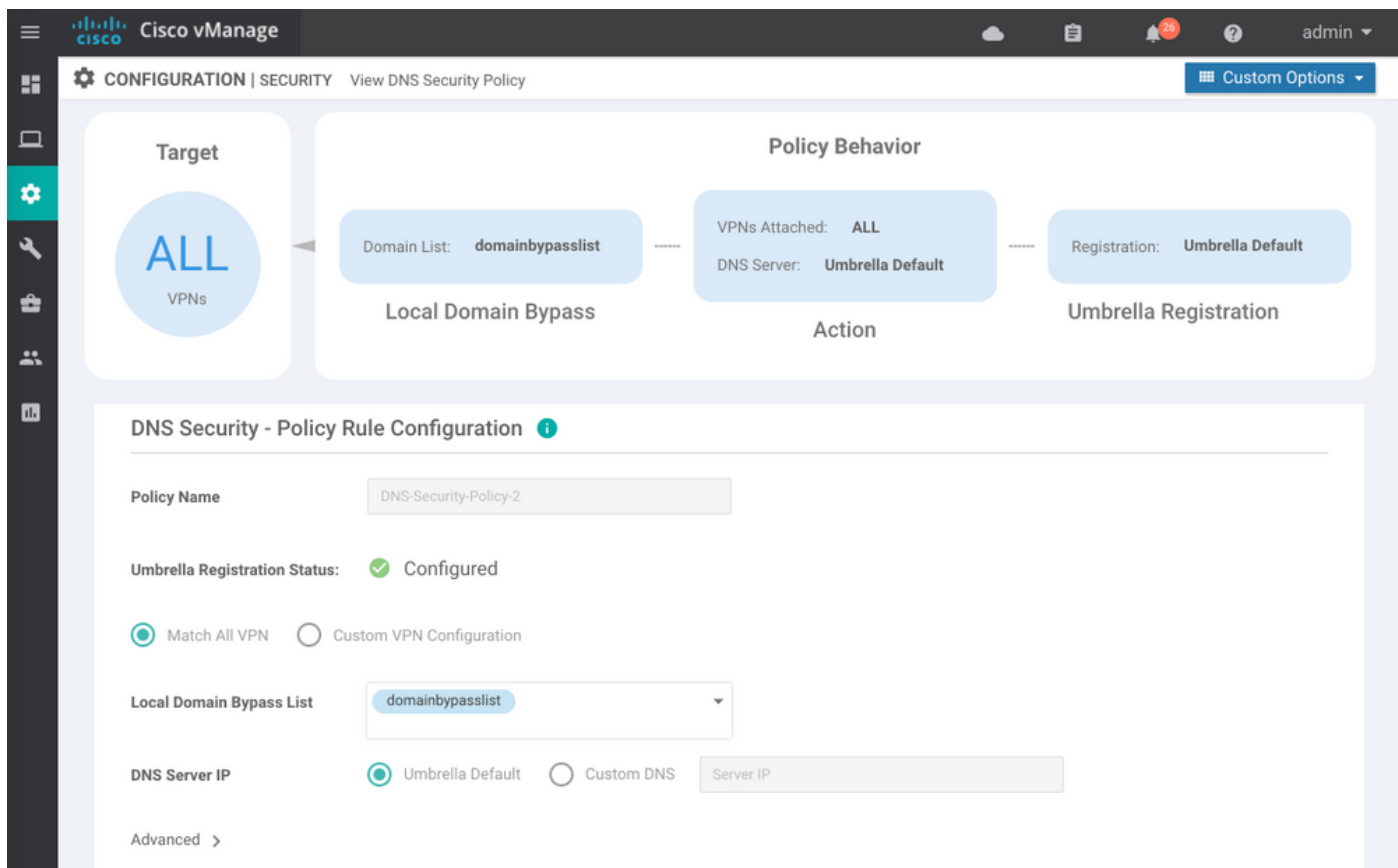
La pantalla parece similar a la imagen que se muestra aquí:



Paso 4. Esta es la imagen de cómo aparece, una vez configurada.



Paso 5. Navegue hasta ...> Ver > Seguridad DNS ficha de su política, verá una configuración similar a esta imagen:



Tenga en cuenta que "Lista de omisión de dominio local" es una lista de dominios para los que el router no redirige las solicitudes DNS a la nube de Umbrella y envía una solicitud DNS a un servidor DNS específico (servidor DNS ubicado dentro de la red empresarial), esto no se excluye de las políticas de seguridad de Umbrella. Para "lista blanca" algunos dominios de la categoría específica, se recomienda configurar la exclusión en el portal de configuración de Umbrella en su lugar.

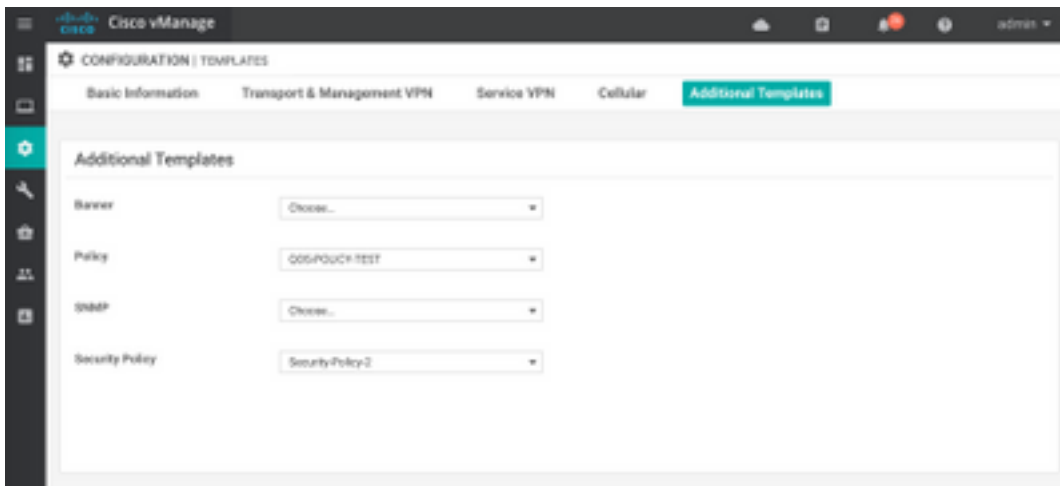
Además, puede seleccionar **Preview** para entender cómo se ve la configuración en la CLI:

```

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

```

Paso 6. Ahora debe hacer referencia a la política en la plantilla de dispositivo. En **Configuration > Templates**, seleccione la plantilla de configuración y haga referencia a ella en la sección **Additional Templates** como se muestra en la imagen.



Paso 7. Aplique la plantilla al dispositivo.

Verificación y resolución de problemas

Utilice esta sección para confirmar que su configuración funciona correctamente y solucionar los problemas.

Verificación del cliente

Desde un cliente que se encuentra detrás de cEdge, puede verificar si Umbrella funciona correctamente cuando navega por estos sitios de prueba:

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

Para obtener más detalles, consulte [Cómo: Pruebe correctamente para asegurarse de que está ejecutando Umbrella correctamente](#)

Verificación de CEdge

La verificación y la resolución de problemas también se pueden realizar en el propio extremo c. En general, es similar a los procedimientos de solución de problemas de integración de software Cisco IOS-XE que se pueden encontrar en el capítulo 2 de la Guía de Configuración de Cisco Umbrella Integration en los ISR de seguridad de Cisco serie 4000: 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.

Pocos comandos útiles para verificar:

Paso 1. Verifique que el mapa de parámetro se presente en la configuración de cEdge en el 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
!
```

Observe que no puede encontrar una referencia a este mapa de parámetro en la interfaz a medida que se acostumbra a verlo en Cisco IOS-XE.

Esto se debe a que el mapa de parámetro se aplica a los VRF y no a las interfaces, puede verificarlo aquí:

```
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
```

Además, puede utilizar este comando para obtener información detallada:

```
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

=====

Paso 2. Compruebe que el dispositivo se ha registrado correctamente en la nube de seguridad DNS de Umbrella.

dmz2-site201-1#show umbrella deviceid

Device registration details

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

Paso 3. Así puede verificar las estadísticas de redireccionamiento de DNS general.

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
```

Paso 4. Verifique que la resolución de DNS sea accesible con herramientas genéricas para resolver problemas como ping y traceroute.

Paso 5. También puede utilizar la captura de paquetes integrada de Cisco IOS-XE para realizar la captura de paquetes DNS desde el extremo c.

Consulte la guía de configuración para obtener más detalles:

<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>.

Comprender la implementación de EDNS del paraguas

Una vez que se toma una captura de paquetes, asegúrese de que las consultas de DNS se redirigen correctamente a los resolvers de DNS general: 208.67.222.222 y 208.67.220.220 con la información EDNS0 (mecanismo de extensión para DNS) correcta. Con la integración de la inspección de capa DNS del paraguas SD-WAN, el dispositivo cEdge incluye las opciones EDNS0 cuando envía consultas DNS a las resoluciones DNS del paraguas. Estas extensiones incluyen la ID de dispositivo que cEdge recibe de Umbrella y la ID de organización de Umbrella para identificar la política correcta que se utilizará cuando responda a la consulta DNS. Este es un ejemplo del formato de paquete 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
```

Aquí está el desglose de opciones:

Descripción de RDATA:

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

Opción de dirección IP remota RDATA:

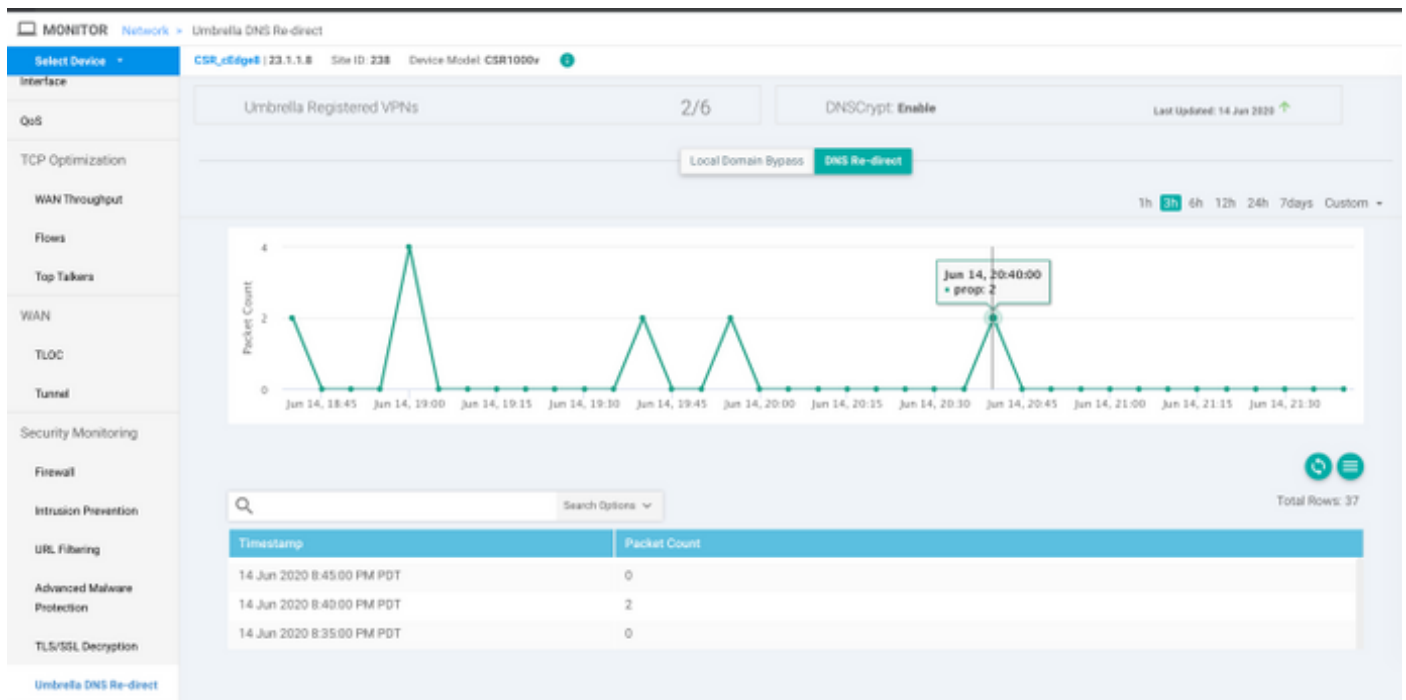
```
0x4f444e53: MGGIC = 'ODNS'  
0x00      : Version  
0x00      : Flags  
0x08      : Organization ID Required  
0x00225487: Organization ID  
0x10 type : Remote IPv4  
0x0b010103: Remote IP Address = 11.1.1.3
```

Verifique y asegúrese de que Device-ID sea correcto y que la ID de organización coincida con la cuenta de Umbrella con el uso del portal de Umbrella.

Nota: Con DNSCrypt habilitado, las consultas DNS se cifran. Si las capturas de paquetes muestran el paquete DNSCrypt yendo a la resolución de Umbrella pero no hay tráfico de retorno, intente inhabilitar DNSCrypt para ver si ese es el problema.

Verificarlo en el panel vManage

Cualquier tráfico dirigido por Cisco Umbrella se puede ver desde vManage Dashboard. Se puede ver en **Monitor > Network > Umbrella DNS Re-direct**. Aquí está la imagen de esta página:



Almacenamiento en caché de DNS

En un router Cisco cEdge, los indicadores de omisión de dominio local a veces no coinciden. Esto sucede cuando hay un almacenamiento en caché involucrado en la máquina/cliente host. Por ejemplo, si se configura la omisión del dominio local para coincidir y omitir www.cisco.com (*.cisco.com). La primera vez, la consulta fue para www.cisco.com que también devolvió nombres CDN como CNAME, que se almacenaban en caché en el cliente. Las consultas posteriores para nslookup para www.cisco.com debían enviar solamente las consultas para el dominio CDN (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
```

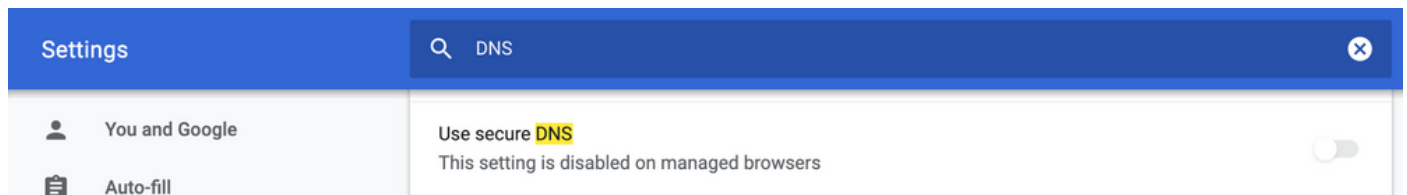
Si la omisión del dominio local funciona correctamente, verá que los contadores aumentan para la redirección OpenDNS del analizador. Esta es una salida abreviada.

```
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 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Esta podría ser la razón, por la cual no se ve la omisión del dominio local en el router. Cuando borra la memoria caché en el equipo host/cliente, verá que las consultas se agotan correctamente.

DNS seguro

Los navegadores modernos como Google Chrome a partir de la versión 83 utilizan DNS seguro también conocido como DNS sobre HTTPS (DoH) o DNS sobre TLS (DoT). Esta función puede hacer que la capacidad de seguridad de DNS de Umbrella sea imposible de usar si no se planifica cuidadosamente. El DNS seguro se puede inhabilitar mediante políticas centralizadas y, de forma predeterminada, se puede inhabilitar, por ejemplo, para ordenadores gestionados por empresas.



En el caso de los dispositivos BYOD no gestionados, existen pocas opciones. La primera opción es bloquear el puerto TCP 853 que utiliza el DNS seguro. Puede utilizar Cisco Zone Based Firewall (ZBFW) para este fin. La segunda opción sería habilitar el bloqueo de la categoría "Proxy/Anonymizer" en el portal de Umbrella. Puede encontrar más información al respecto aquí

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

Conclusión

Como puede ver, la integración con la nube de seguridad DNS de Umbrella es muy sencilla desde

el extremo cEdge y se puede realizar en unos minutos.