Integración de la configuración con el paraguas de Cisco

Contenido

Introducción

Este documento describe el vManage/el ® del Cisco IOS - parte del software XE SDWAN de la integración con la solución acerca de la seguridad del paraguas DNS de Cisco. Sin embargo, no cubre la configuración sí mismo de las directivas de paraguas. Usted puede encontrar más información sobre el paraguas de Cisco aquí; https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella.

> Nota: Usted tiene que haber obtenido las suscripciones del paraguas y conseguir ya el token del paraguas que será utilizado en la configuración del Routers del cEdge. Más sobre el token API: https://docs.umbrella.com/umbrella-api/docs/overview2.

Prerrequisitos

Requisitos

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
- ® del Cisco IOS - Funcionamiento del router XE SDWAN (cEdge) 16.9.3

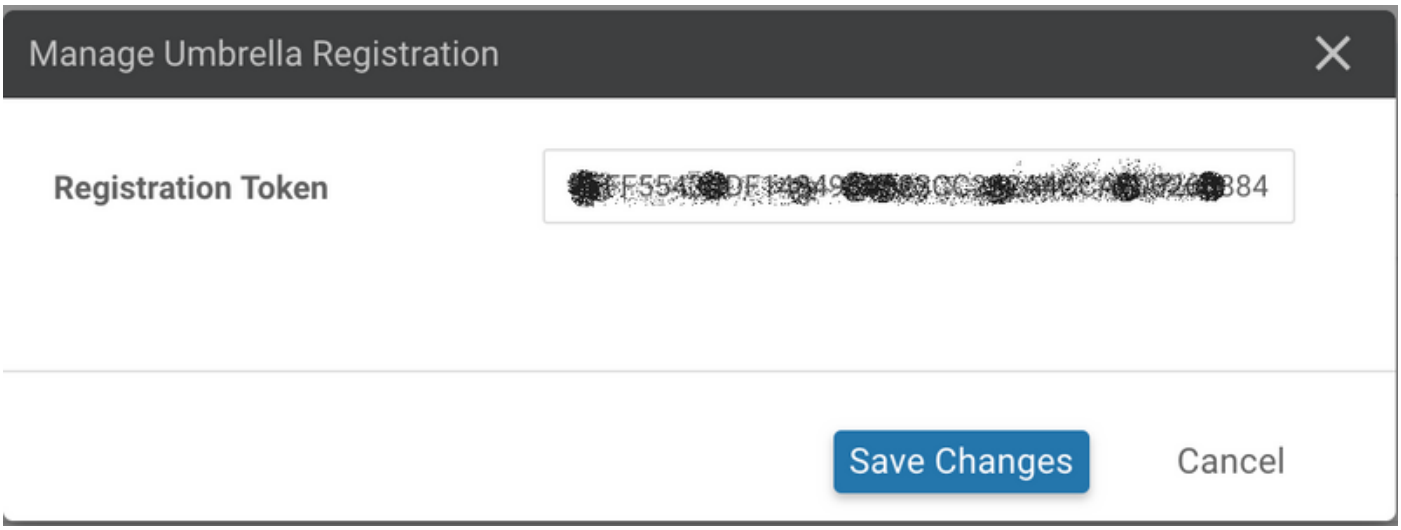
La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

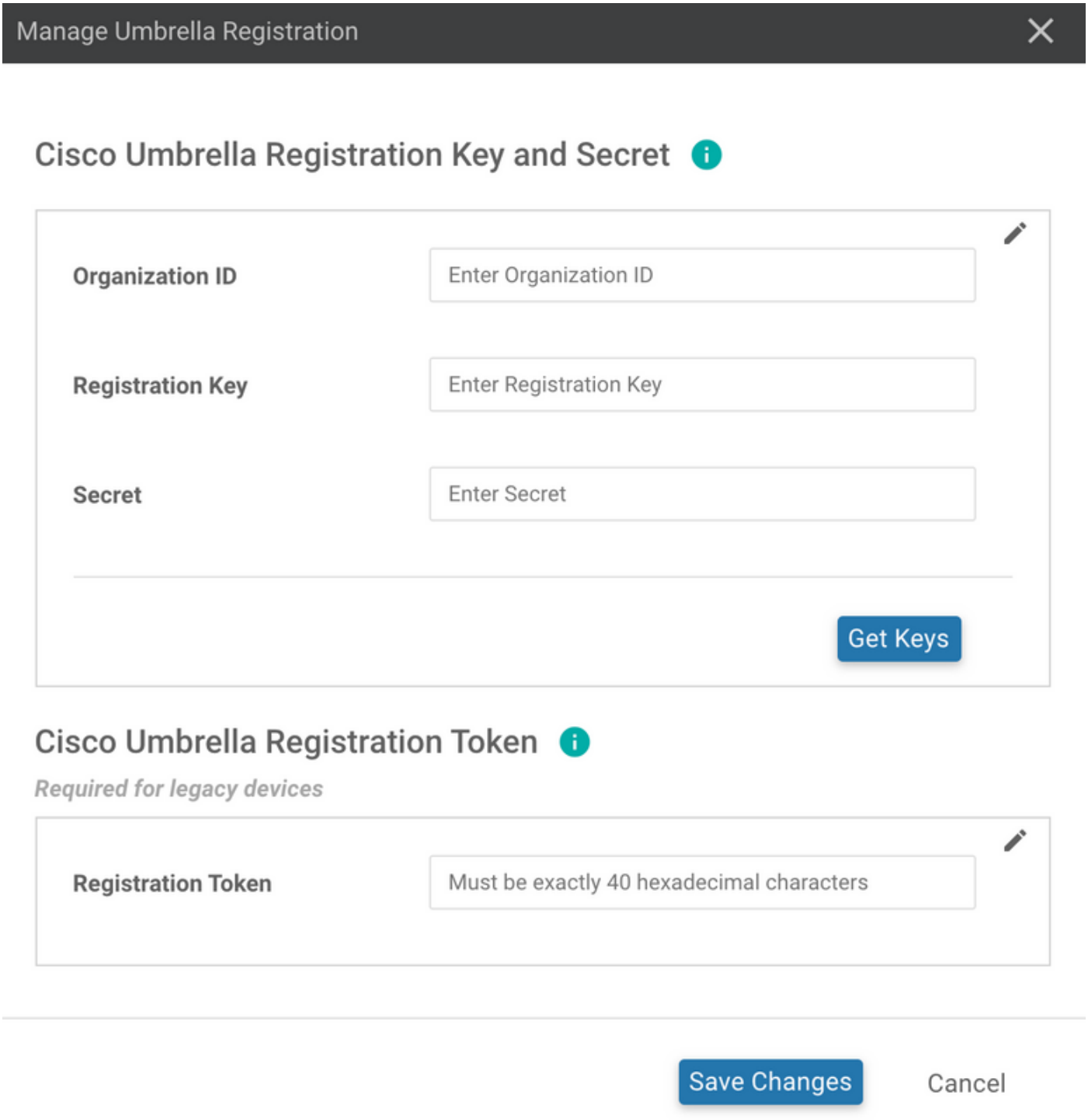
Configurar

Para configurar su integración del cEdge con el paraguas de Cisco, usted realiza un conjunto de los pasos simples en el vManage:

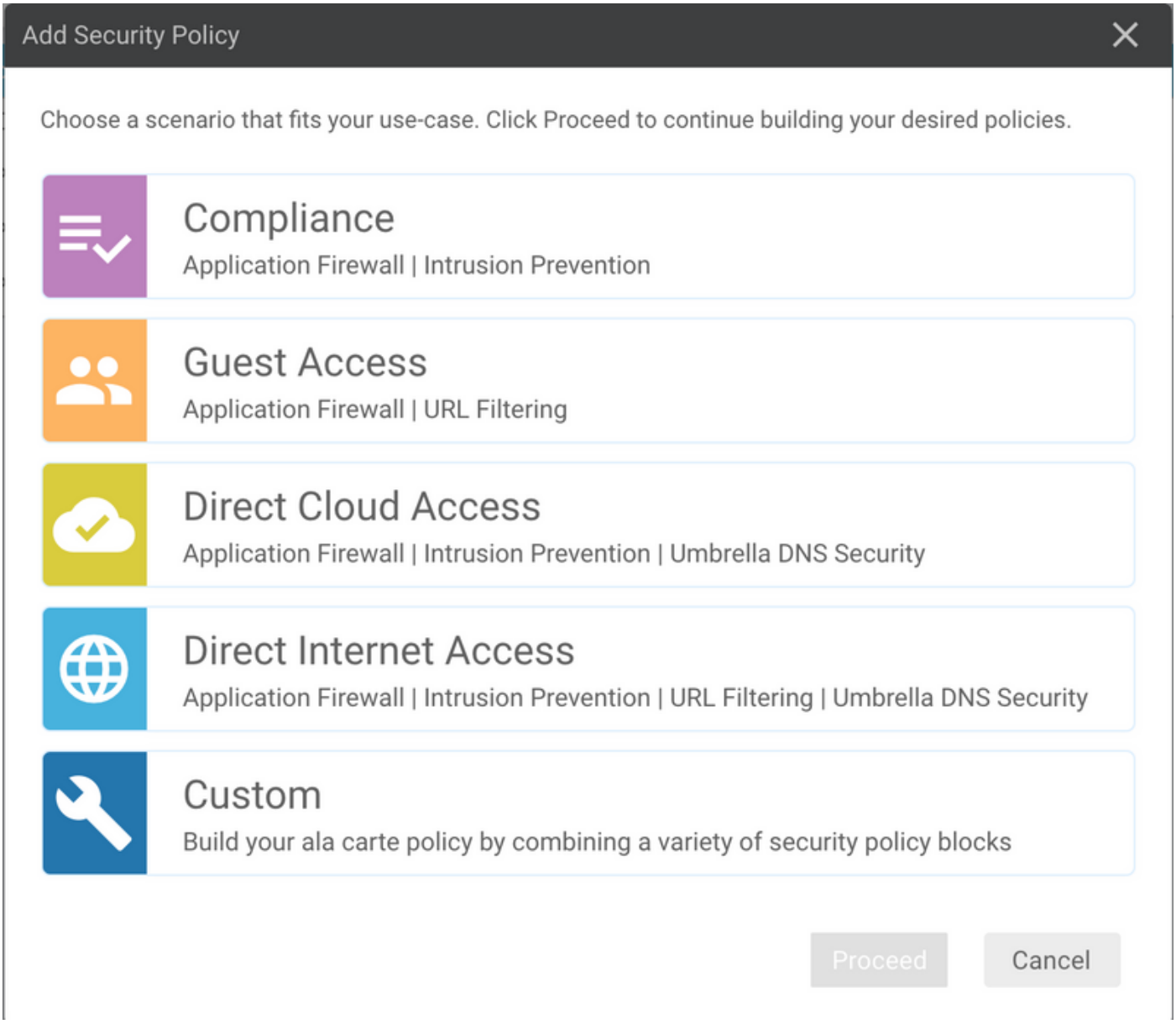
Paso 1. Bajo el **> Security (Seguridad) de Congifuration**, la lista desplegable selecta de las **opciones CUSTOM (Personalizada)** en la esquina superior derecha, y entonces selecciona el **token del paraguas API**. Ingrese su token del registro del paraguas, tal y como se muestra en de la imagen:



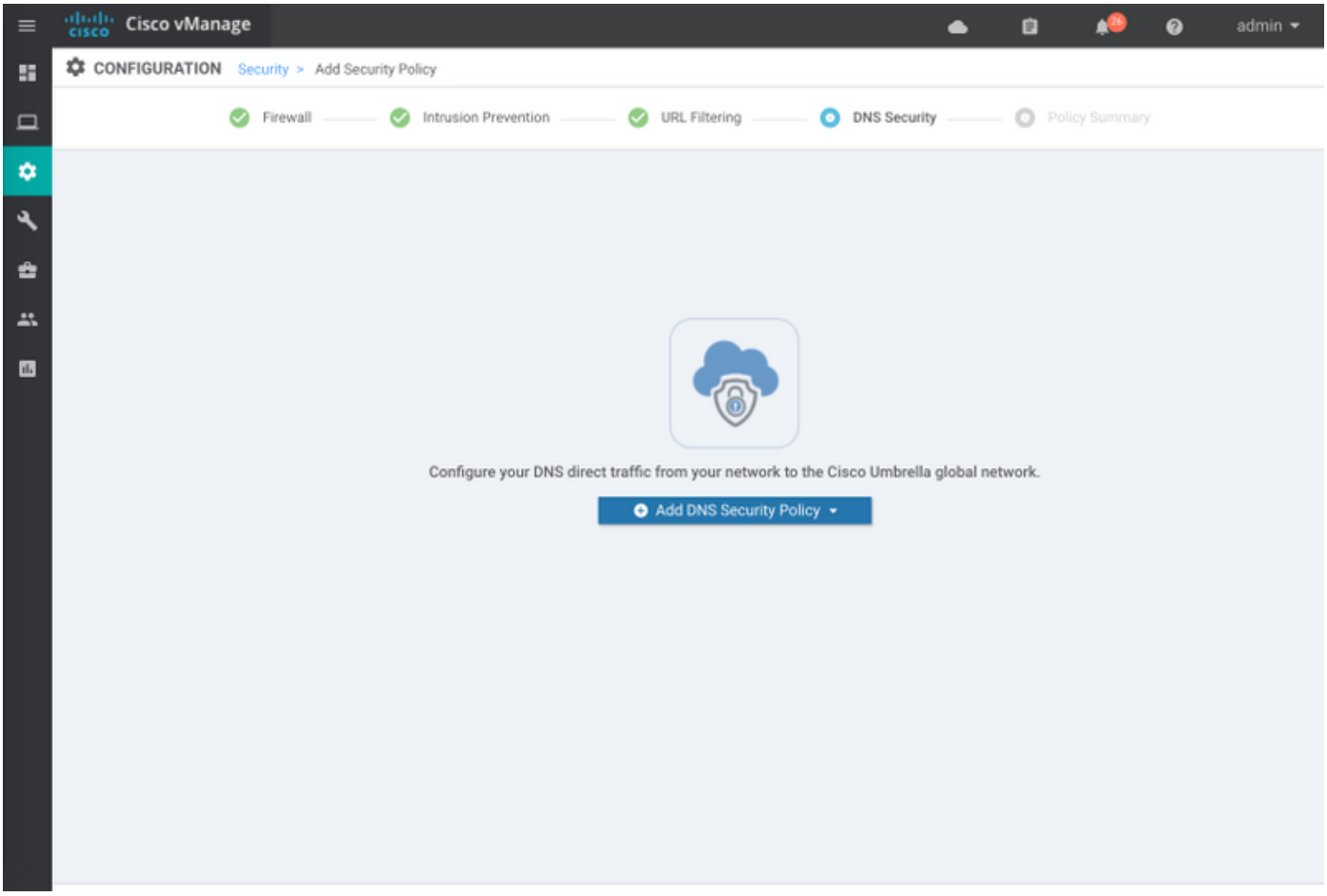
Alternativamente, a partir de la versión del software 20.1.1 del vManage usted puede especificar el ID de la organización, la clave del registro, y el secreto. Estos parámetros pueden ser extraídos automáticamente si usted ha configurado sus credenciales elegantes de la cuenta bajo la **administración > configuraciones >** las **credenciales elegantes de la cuenta**.



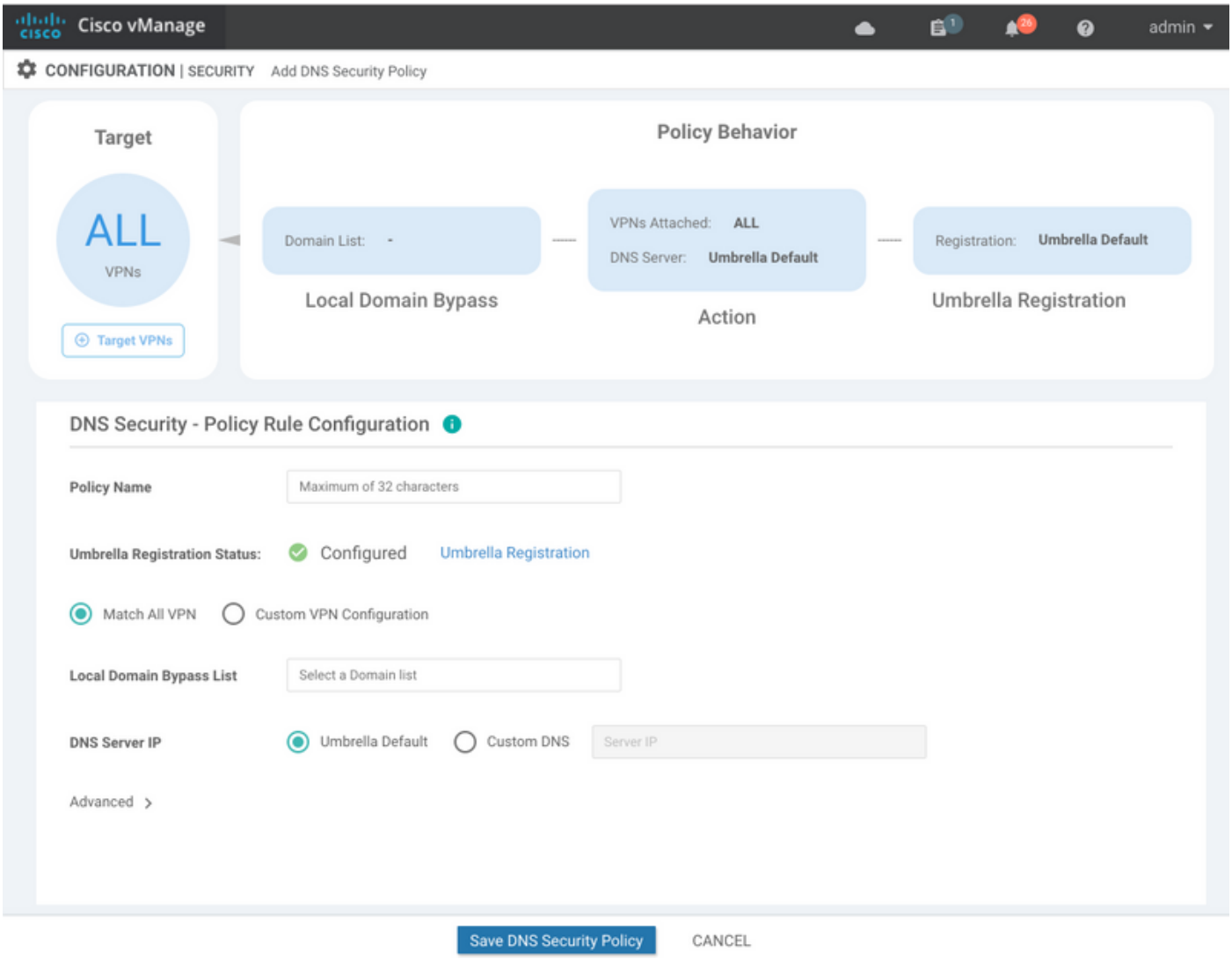
Paso 2. Bajo el **> Security (Seguridad) de la configuración**, selecto **agregue la política de seguridad** y después seleccione un escenario que quepa su uso-caso (e.g aduana), tal y como se muestra en de la imagen:



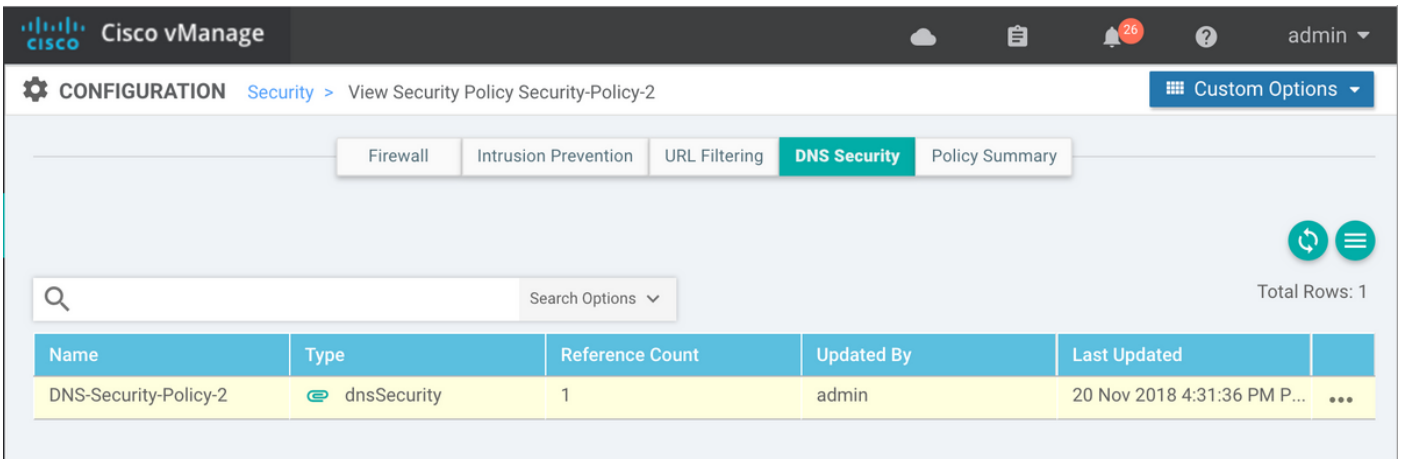
Paso 3. Tal y como se muestra en de la imagen, navegue a la **Seguridad DNS**, selecta **agregue la política de seguridad DNS** y después selecciónela **crean nuevo.**



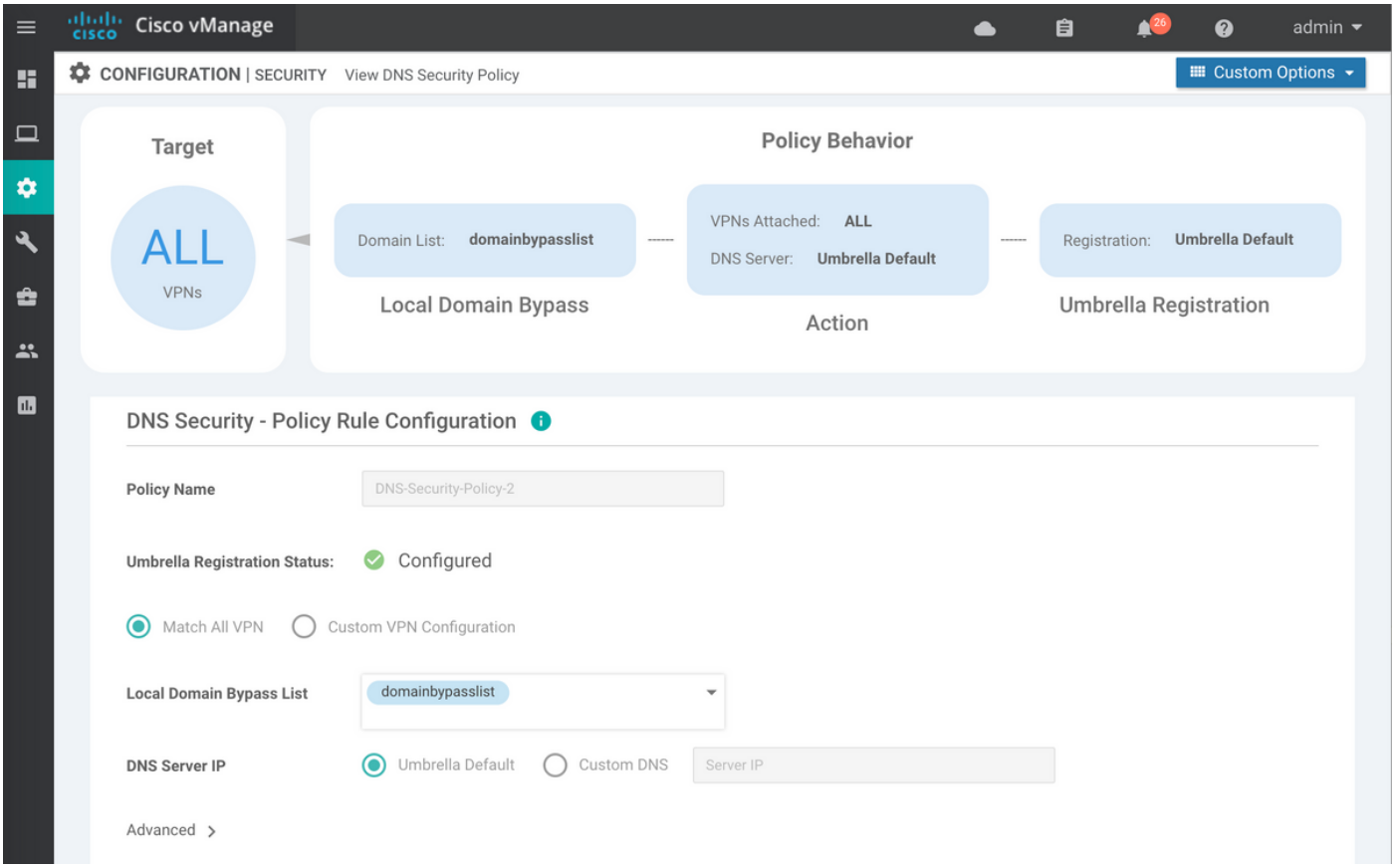
La pantalla aparece similar a la imagen mostrada aquí:



Paso 4. Ésta es la imagen de cómo aparece, una vez que está configurado.



Paso 5. Navegue a**… > visión > ficha de seguridad DNS de** su directiva, usted ven una configuración similar a esta imagen:

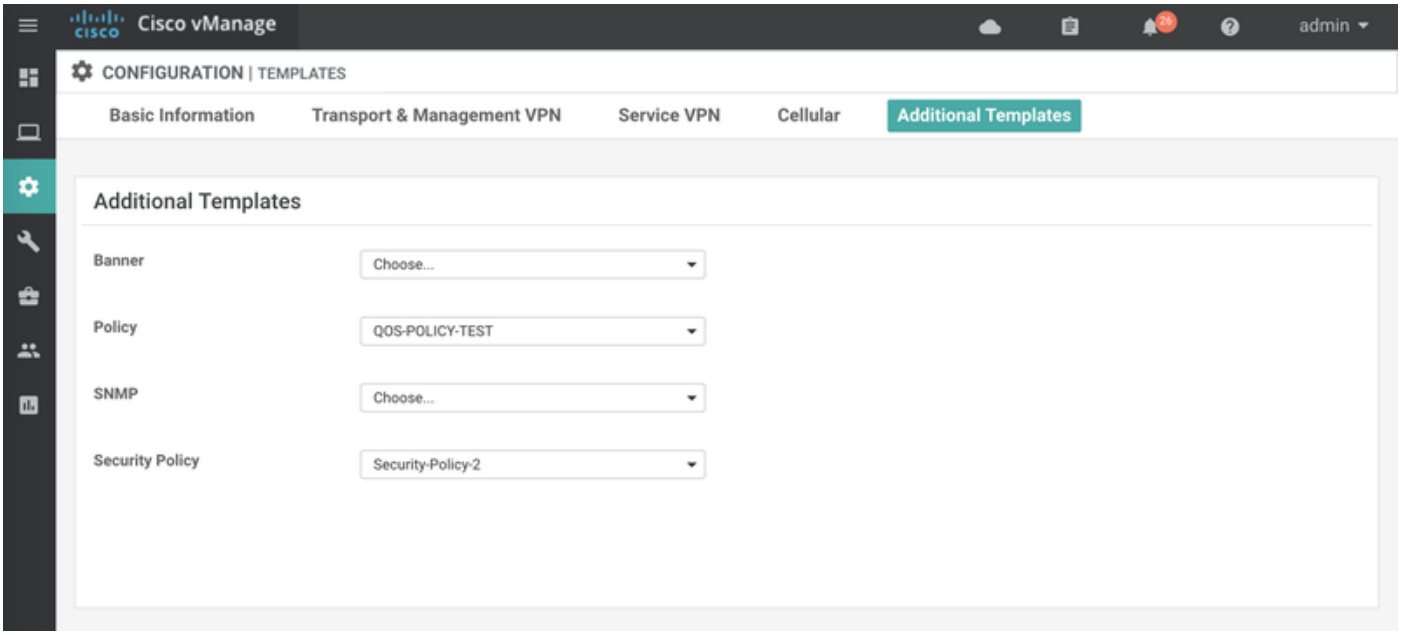


Tenga presente que “la lista de puente del dominio local” es un enumerar de los dominios para los cuales el router no reorienta las peticiones DNS a la nube del paraguas y envía la petición DNS a un servidor DNS específico (servidor DNS situado dentro de la red para empresas), esto no es exclusión de las políticas de seguridad del paraguas. Para “lista blanca” algunos dominios de la categoría específica, se recomienda para configurar la exclusión en el portal de la configuración del paraguas en lugar de otro.

También, usted puede seleccionar el **avance** para entender cómo la configuración mira en el 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 usted debe referirse a la directiva a la plantilla del dispositivo. Bajo la **configuración > plantillas**, seleccione su plantilla de configuración y refiérase a ella a la sección **adicional de las plantillas** tal y como se muestra en de la imagen.



Paso 7. Aplique la plantilla al dispositivo.

Verificación y resolución de problemas

Utilice esta sección para confirmar que su configuración trabaja correctamente y resuelvala problemas.

Verificación del cliente

De un cliente que se sienta detrás del cEdge, usted puede verificar si el paraguas funciona correctamente cuando usted hojea estos sitios de prueba:

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

Para más detalles, refiérase a cómo: Pruebe con éxito para asegurarse que usted está funcionando con el paraguas correctamente

verificación del cEdge

La verificación y Troubleshooting se puede también realizar en el cEdge sí mismo. Es generalmente similar a los procedimientos del Troubleshooting de la integración del Software Cisco IOS XE que se pueden encontrar en la integración del paraguas de Cisco del capítulo 2 en las Cisco 4000 Series ISR de guía de configuración de seguridad: Integración del paraguas de Cisco, 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 de marcar:

Paso 1. Marque que el parámetro-mapa está presentado en configuración del cEdge en el dispositivo:

```
dmz2-site201-1#show run | sec parameter-map type umbrella
```

```
parameter-map type umbrella global
 token XFFFX543XDF14X498X623CX222X4CCAX0026X88X
 local-domain domainbypasslist
 dnscrypt
 udp-timeout 5
 vrf 1
  dns-resolver umbrella
  match-local-domain-to-bypass
!
```

Observe que usted no puede encontrar una referencia a este parámetro-mapa en la interfaz pues usted se acostumbra a verla en el Cisco IOS XE.

Esto es porque el parámetro-mapa se aplica a los VRF y no a las interfaces, usted puede marcarlo aquí:

```
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
```

Además de eso, usted puede utilizar este comando de conseguir la 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 : 010aed3ffebc56df
      Tag      : vpn1
 10             Loopback1 :
      Mode     : IN
      DeviceID : 010aed3ffebc56df
      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 : 010aed3ffebc56df
          Tag      : vpn1

Umbrella Profile ID CPP Hash:

-----------------------------

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

```
======================================
```

Paso 2. Marque que el dispositivo está registrado con éxito con la nube de la Seguridad del paraguas DNS.

```
dmz2-site201-1#show umbrella deviceid
Device registration details
VRF                     Tag             Status          Device-id
1                       vpn1            200 SUCCESS     010aed3ffebc56df
```

Paso 3. Aquí es cómo usted puede marcar el paraguas DNS reorienta las estadísticas.

```
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. Marque que el solucionador de DNS es accesible con las herramientas genéricas para resolver problemas como el ping y el traceroute.

Paso 5. Usted puede también utilizar a la captura de paquetes integrada del Cisco IOS XE para realizar la captura de los paquetes DNS que va del cEdge.

Refiera a la guía de configuración para los detalles: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/xe-16-9/epc-xe-16-9-book/nm-packet-capture-xe.html.](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/xe-16-9/epc-xe-16-9-book/nm-packet-capture-xe.html)

Entienda la implementación EDNS del paraguas

Una vez que toman una captura de paquetes, asegúrese que las interrogaciones DNS estén reorientadas correctamente a los solucionadores de DNS del paraguas: 208.67.222.222 y 208.67.220.220 con (mecanismo de la extensión para el DNS) la información correcta EDNS0. Con la integración del examen de la capa del paraguas DNS SD-WAN, el dispositivo del cEdge incluye las opciones ENDS0 cuando envía las interrogaciones DNS a las resoluciones del paraguas DNS. Estas Extensiones incluyen el cEdge del ID del dispositivo reciben del paraguas y del ID de la organización para el paraguas para identificar la directiva correcta que se utilizará cuando usted contesta a la interrogación DNS. Aquí está un ejemplo del formato de paquetes 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: 4f444e5300000800225487100b010103
```

Aquí está la ruptura de la opción:

Descripción RDATA:

```
0x4f70656e444e53: Data ="OpenDNS"
0x10afb86c9b1aff: Device-ID
```

Opción del IP Address remoto RDATA:

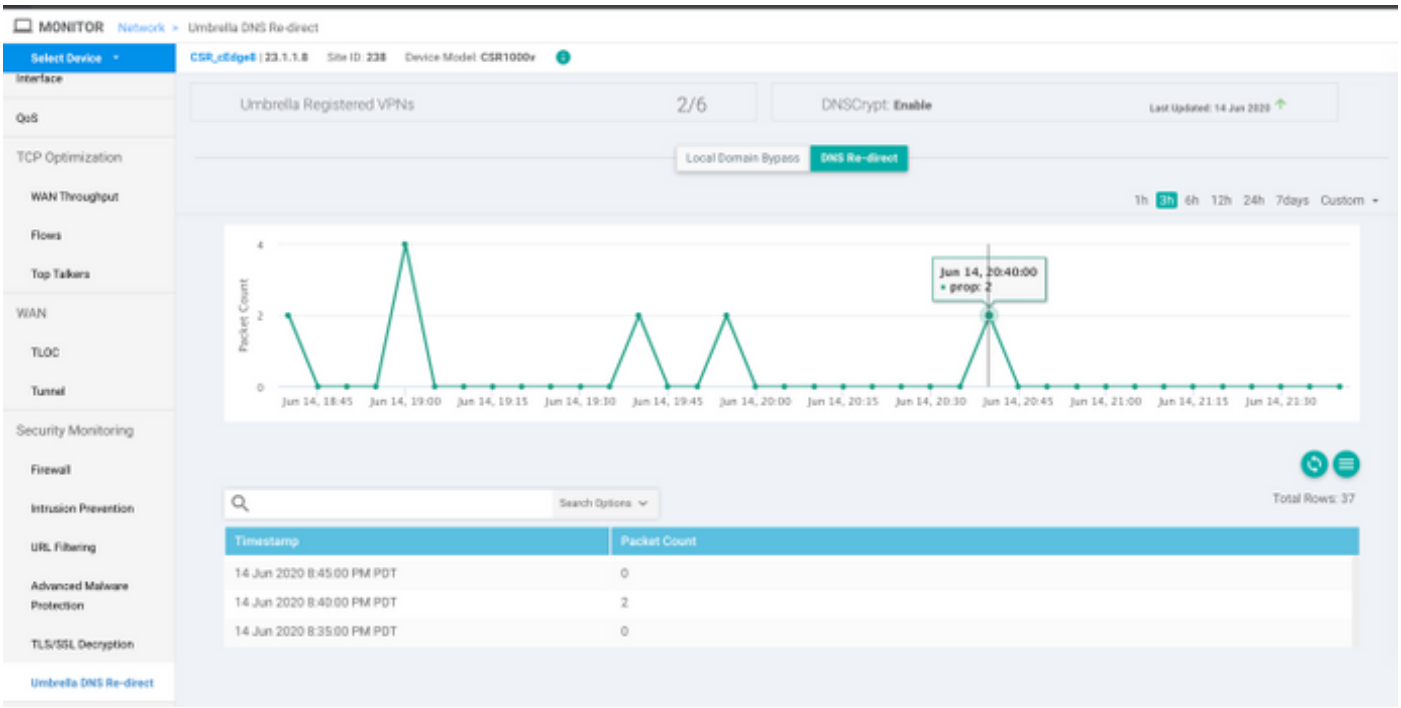
```
0x4f444e53: MGGIC = 'ODNS'
0x00      : Version
0x00      : Flags
0x08      : Organization ID Required
0x00225487: Organization ID
0x10 type : Remote IPv4
0x0b010103: Remote IP Address = 11.1.1.3
```

Marque y asegúrese de que el Dispositivo-ID está correcto y el ID de la organización hace juego la cuenta del paraguas con el uso del portal del paraguas.

> Nota: Con DNSCrypt habilitó, las interrogaciones DNS se cifran. Si el paquete de DNScrypt de la demostración de las capturas de paquetes que va al software de resolución de nombres del paraguas pero allí no es ningún tráfico de retorno, intente inhabilitar DNSCrypt para ver si ése es el problema.

Verifiquelo en el panel del vManage

Cualquier tráfico dirigido del paraguas de Cisco se puede ver del panel del vManage. Puede ser visto bajo el **monitor > la red > el paraguas DNS reorienta**. Aquí está la imagen de esta página:



Almacenamiento en memoria inmediata DNS

En un router del cEdge de Cisco, los indicadores locales de dominio-puente no hacen juego a veces. Esto sucede cuando hay un almacenamiento en memoria inmediata implicado en el equipo del host/el cliente. Como un ejemplo, si dominio-puente local se configura para hacer juego y para

desviar www.cisco.com (**. *cisco.com).** La primera vez que, la interrogación estaba para www.cisco.com que también volvieron los nombres CDN como CNAME, que fueron ocultados en el cliente. Las interrogaciones subsiguientes para el nslookup para www.cisco.com eran enviar solamente las interrogaciones 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 dominio-puente local funciona correctamente, usted verá que los contadores aumentan para el analizador de sintaxis OpenDNS reorientan. Aquí está 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 <<<<<<<<<<<
```

Ésta podría ser la razón, en cuanto a porqué puente del dominio local no se considera en el router. Cuando usted borra el caché en el host/la máquina del cliente, usted ve que salen las interrogaciones correctamente.

Conclusión

Como usted puede ver, la integración con la nube de la Seguridad del paraguas DNS es muy simple del lado del cEdge y se puede hacer en unos minutos.