Configure a integração com o Cisco Umbrella e solucione problemas comuns

Contents

Introduction

Este documento descreve o software vManage/Cisco IOS®-XE SDWAN como parte da integração com a solução de segurança Cisco Umbrella DNS. No entanto, ele não cobre a configuração das políticas Umbrella em si. Você pode encontrar mais informações sobre o Cisco Umbrella aqui; https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella.

> **Note**: Você já deve ter obtido assinaturas Umbrella e obter o token Umbrella que será usado na configuração dos roteadores cEdge. Mais informações sobre o token de API: https://docs.umbrella.com/umbrella-api/docs/overview2.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- vManage 18.4.0
- Roteador Cisco IOS®-XE SDWAN em execução (cEdge) 16.9.3

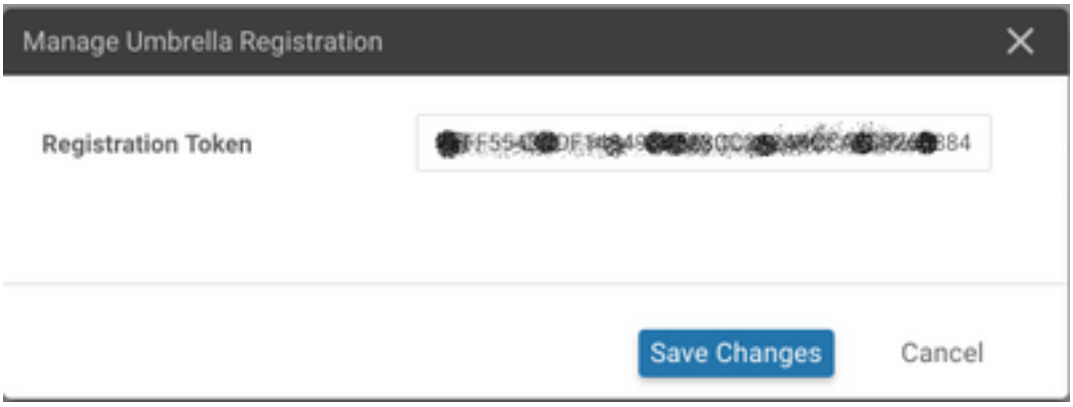
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

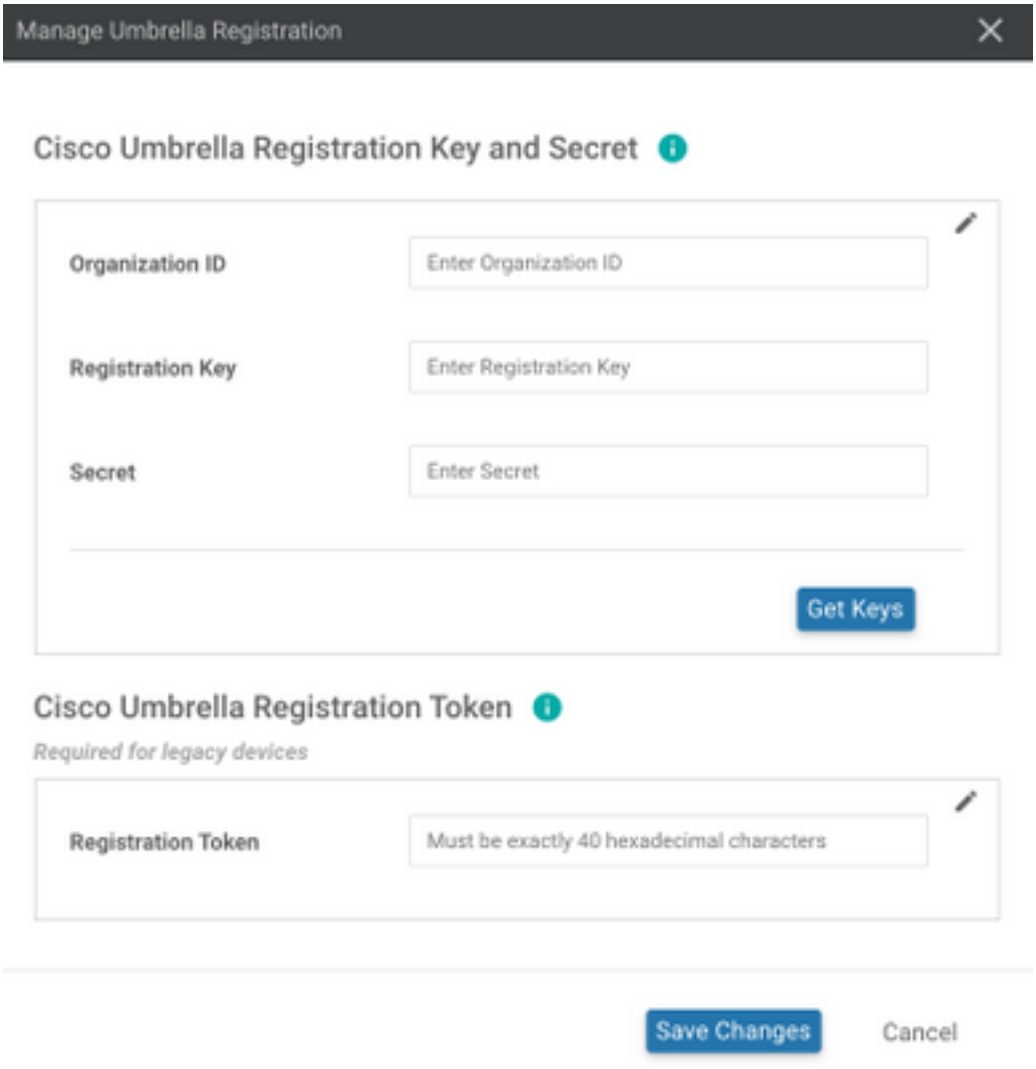
Configurar

Para configurar sua integração do cEdge com o Cisco Umbrella, você executa um conjunto de etapas simples no vManage:

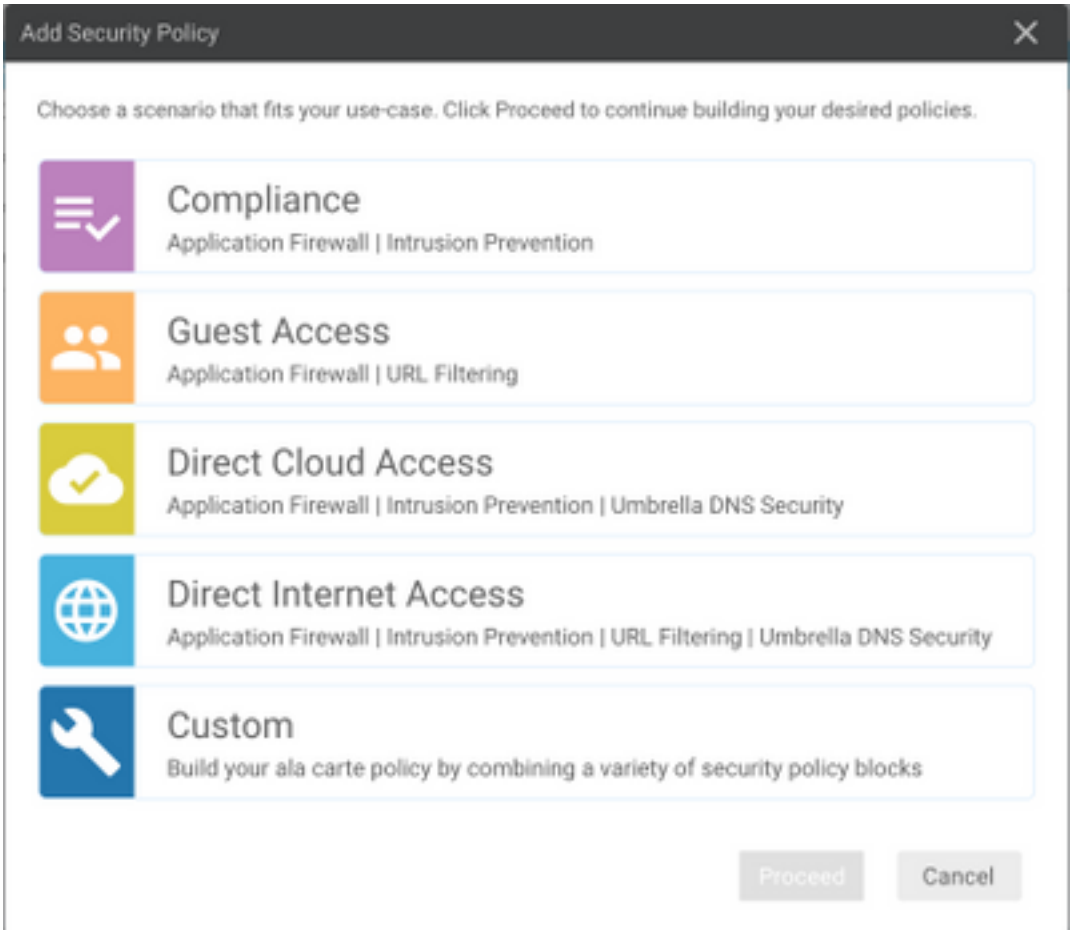
Etapa 1. Em **Configuração > Segurança**, selecione a lista suspensa **Opções personalizadas** no canto superior direito e selecione **token da API Umbrella**. Digite seu token de registro Umbrella, como mostrado na imagem:



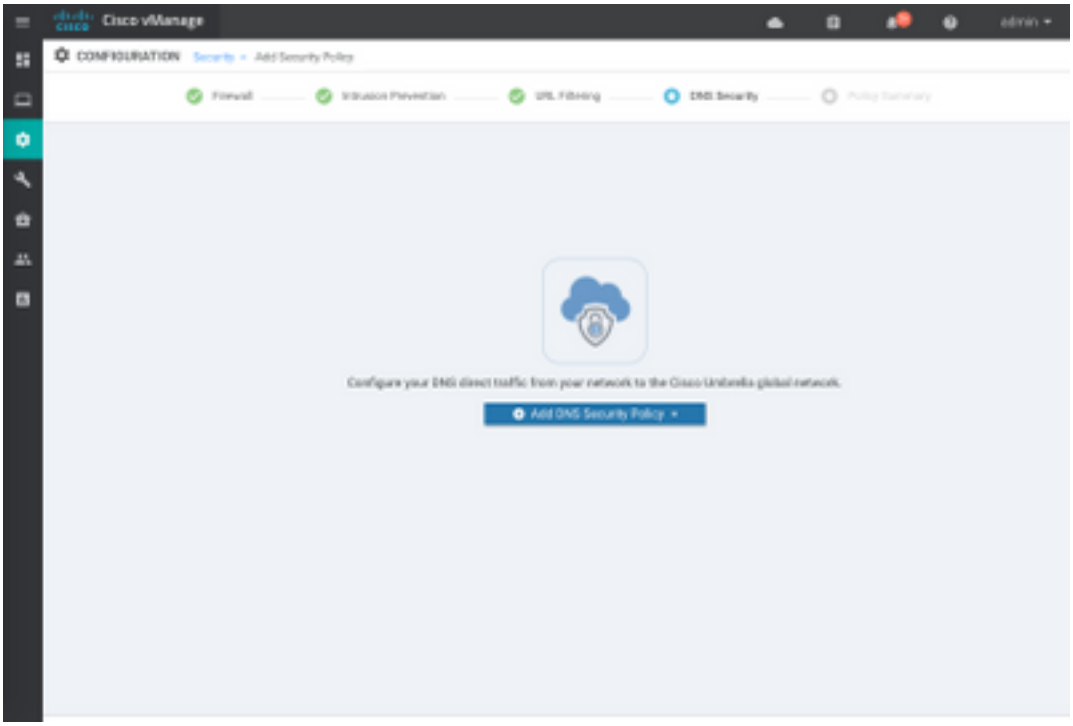
Como alternativa, a partir da versão 20.1.1 do software vManage, você pode especificar a ID da organização, a chave de registro e o segredo. Esses parâmetros podem ser recuperados automaticamente se você tiver configurado suas credenciais de Smart Account em **Administration > Settings > Smart Account Credentials**.



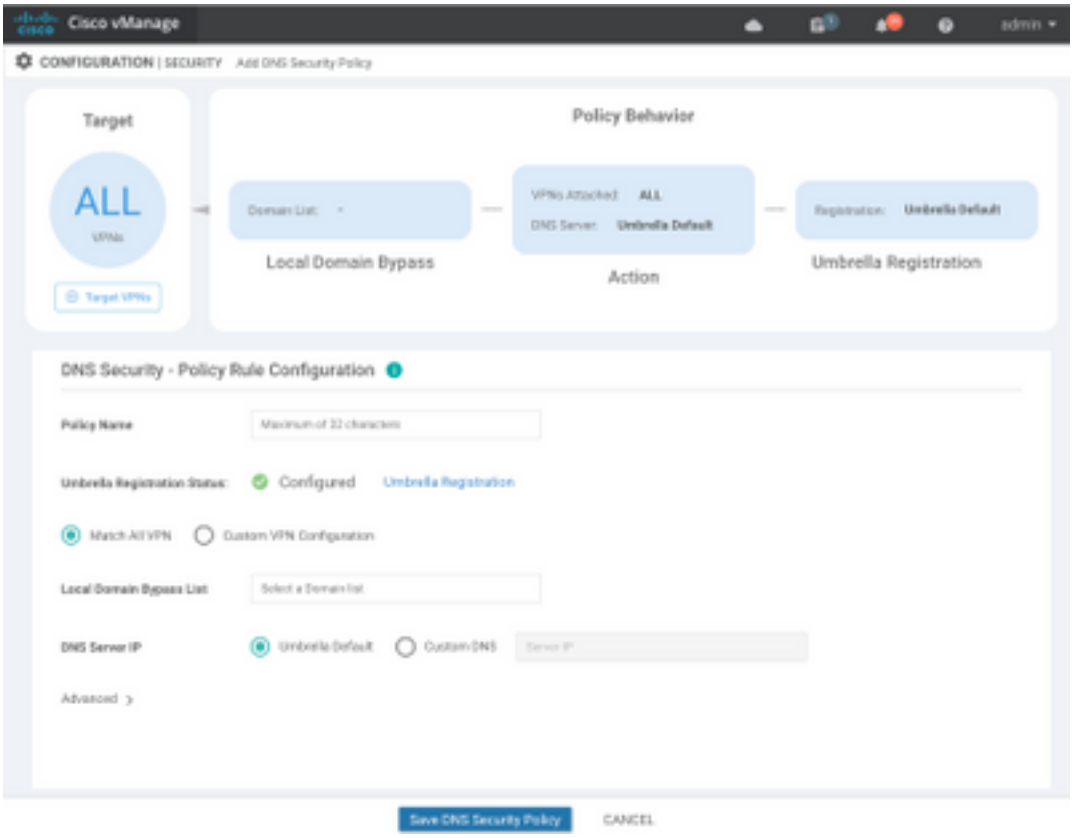
Etapa 2. Em **Configuration > Security**, selecione **Add Security Policy** e selecione um cenário que se ajuste ao seu caso de uso (por exemplo, personalizado), como mostrado na imagem:



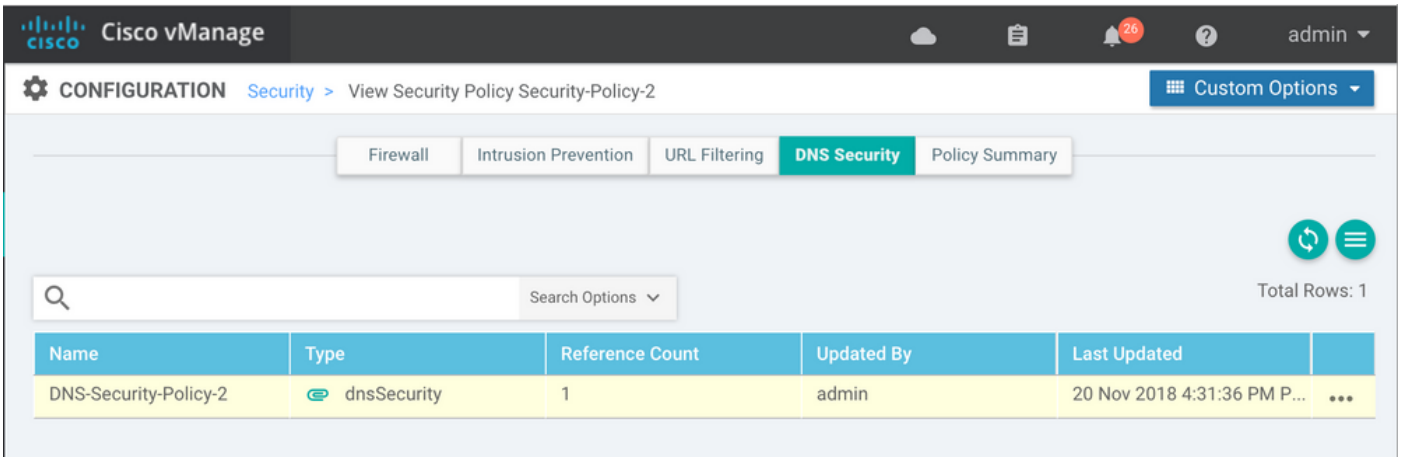
Etapa 3. Como mostrado na imagem, navegue para **Segurança DNS**, selecione **Adicionar política de segurança DNS** e selecione **Criar novo.**



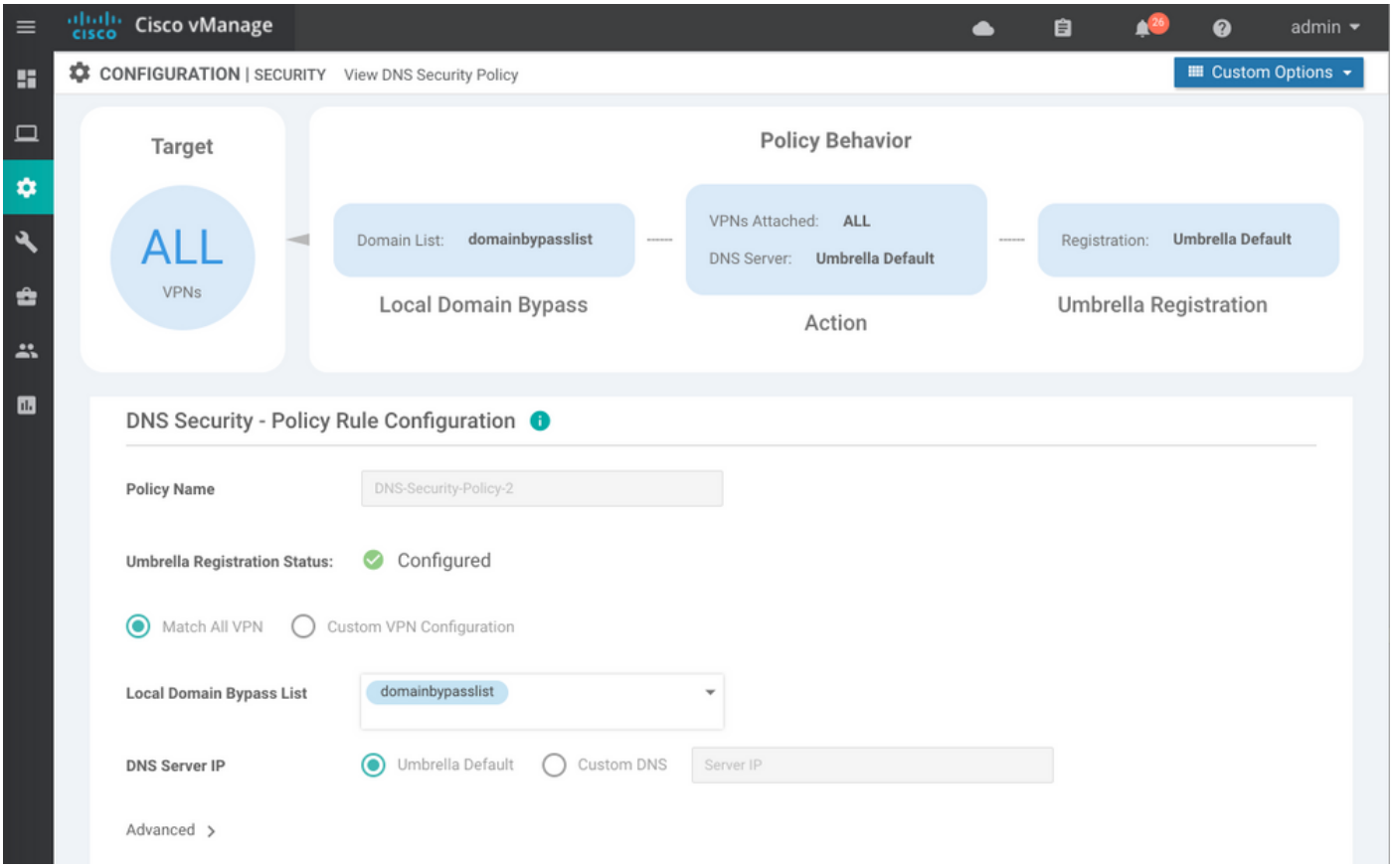
A tela é semelhante à imagem mostrada aqui:



Etapa 4. Esta é a imagem de como ele aparece, uma vez configurado.



Etapa 5. Navegue até **...> Exibir >** guia **Segurança DNS** de sua política, você verá uma configuração semelhante a esta imagem:

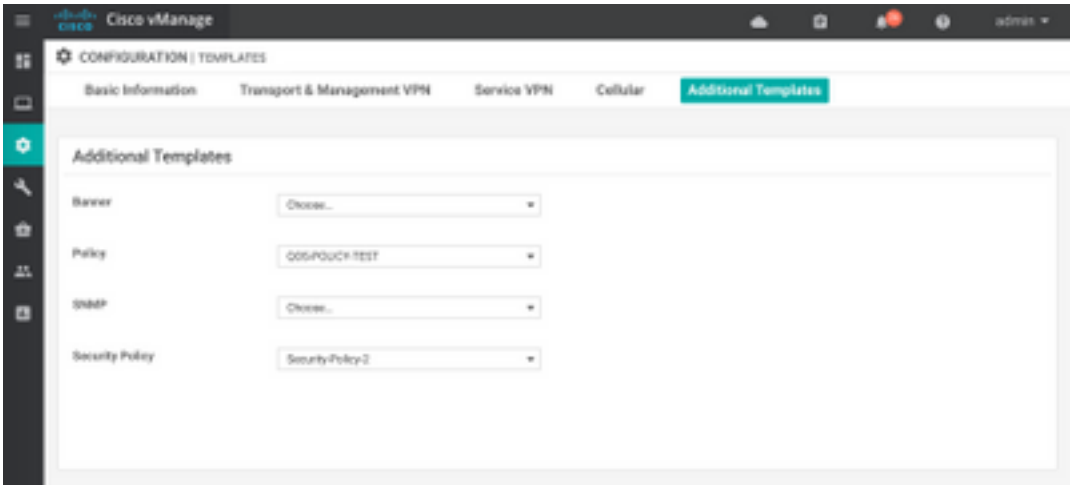


Lembre-se de que a "Lista de desvio de domínio local" é uma lista de domínios para os quais o roteador não redireciona solicitações de DNS para a nuvem Umbrella e envia solicitações de DNS para um servidor DNS específico (servidor DNS localizado na rede corporativa), isso não é exclusão das políticas de segurança Umbrella. Para "whitelist" alguns domínios da categoria específica, recomenda-se configurar a exclusão no portal de configuração Umbrella.

Além disso, você pode selecionar **Preview** para entender como a configuração é na 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
```

Etapa 6. Agora você deve fazer referência à política no modelo de dispositivo. Em **Configuration > Templates**, selecione seu modelo de configuração e faça referência a ele na seção **Additional Templates**, como mostrado na imagem.



Passo 7. Aplique o modelo ao dispositivo.

Verificar e solucionar problemas

Use esta seção para confirmar se sua configuração funciona corretamente e solucionar problemas.

Verificação do cliente

De um cliente sentado atrás do cEdge, você pode verificar se o Umbrella funciona corretamente quando navega nesses sites de teste:

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

Para obter mais detalhes, consulte Como: Teste com êxito para garantir que o Umbrella esteja sendo executado corretamente

Verificação cEdge

A verificação e a solução de problemas também podem ser realizadas no próprio cEdge. Em geral, é semelhante aos procedimentos de solução de problemas de integração do software Cisco IOS-XE que podem ser encontrados no Capítulo 2 do Cisco Umbrella Integration no 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/xe-16-9/sec-data-umbrella-branch-xe-16-9-book.pdf.

Poucos comandos úteis para verificar:

Etapa 1. Verifique se o mapa de parâmetros é apresentado na configuração do cEdge no 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 você não pode encontrar uma referência a este mapa de parâmetros na interface à medida que você se acostuma a vê-lo no Cisco IOS-XE.

Isso porque o mapa de parâmetros é aplicado a VRFs e não a interfaces, você pode verificá-lo aqui:

```
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
```

Além disso, você pode usar este comando para obter informações detalhadas:

```
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


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

Etapa 2. Verifique se o dispositivo foi registrado com êxito na nuvem Umbrella DNS Security.

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

Etapa 3. Veja como você pode verificar as estatísticas de redirecionamento de DNS de guarda-chuva.

```
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
```

Etapa 4. Verifique se o resolvedor DNS está acessível com ferramentas genéricas para solucionar problemas como ping e traceroute.

Etapa 5. Você também pode usar a Captura de Pacotes Incorporados do Cisco IOS-XE para executar a captura de pacotes DNS a partir do cEdge.

Consulte o guia de configuração para obter detalhes: [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)

Entenda a implementação EDNS do Umbrella

Depois de capturar um pacote, certifique-se de que as consultas de DNS sejam redirecionadas corretamente para os resolvedores de DNS Umbrella: 208.67.222.222 e 208.67.220.220 com as informações corretas de EDNS0 (Extension Engine para DNS). Com a integração de inspeção da camada DNS Umbrella SD-WAN, o dispositivo cEdge inclui opções ENDS0 quando envia consultas DNS para a resolução do DNS Umbrella. Esses ramais incluem o ID do dispositivo que o cEdge recebe do Umbrella e o ID da organização do Umbrella para identificar a política correta a ser usada ao responder à consulta DNS. Aqui está um exemplo do formato do pacote EDNS0:

Aqui está o detalhamento das opções:

Descrição do RDATA:

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

Opção de endereço IP remoto RDATA:

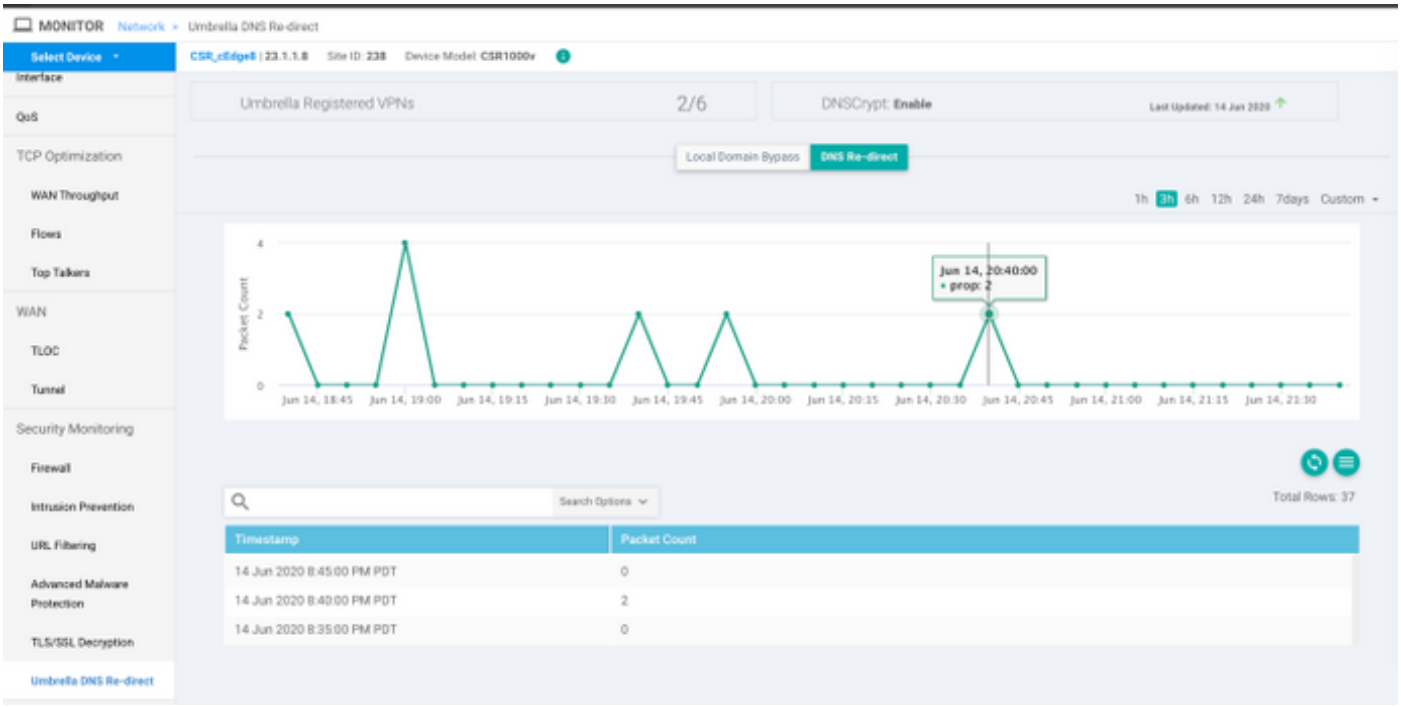
```
0x4f444e53: MGGIC = 'ODNS'
0x00      : Version
0x00      : Flags
0x08      : Organization ID Required
0x00225487: Organization ID
0x10 type : Remote IPv4
0x0b010103: Remote IP Address = 11.1.1.3
```

Verifique se a ID do dispositivo está correta e se a ID da empresa corresponde à conta Umbrella com o uso do portal Umbrella.

> **Note**: Com DNSCrypt habilitado, as consultas DNS são criptografadas. Se as capturas de pacote mostrarem o pacote DNScrypt indo para o resolvedor Umbrella, mas não houver tráfego de retorno, tente desabilitar o DNSCrypt para ver se esse é o problema.

Verificar no painel do vManage

Qualquer tráfego direcionado do Cisco Umbrella pode ser visualizado no painel do vManage. Ele pode ser visualizado em **Monitor > Network > Umbrella DNS Re-direct**. Aqui está a imagem desta página:



Cache DNS

Em um roteador Cisco cEdge, os sinalizadores de desvio de domínio local às vezes não correspondem. Isso acontece quando há um cache envolvido na máquina/cliente host. Por exemplo, se o desvio de domínio local estiver configurado para corresponder e ignorar www.cisco.com (**.*cisco.com**). Na primeira vez, a consulta foi para www.cisco.com, que também retornou nomes CDN como CNAMEs, que foram armazenados em cache no cliente. As consultas subsequentes para nslookup para www.cisco.com enviavam apenas as consultas para o domínio 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
```

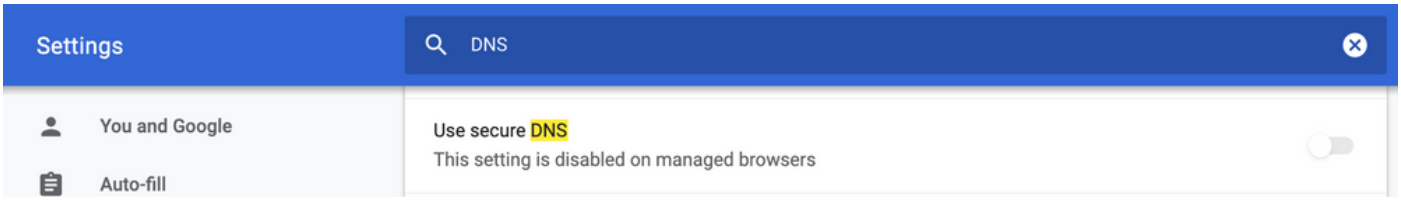
Se o desvio de domínio local funcionar corretamente, você verá que os contadores aumentam para o redirecionamento OpenDNS do analisador. Aqui está uma saída abreviada.

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

Esse pode ser o motivo pelo qual o desvio de domínio local não é visto no roteador. Quando você limpa o cache na máquina host/cliente, você vê que as consultas saem corretamente.

DNS seguro

Navegadores modernos como o Google Chrome a partir da versão 83 estão usando DNS seguro também conhecido como DNS sobre HTTPS (DoH) ou DNS sobre TLS (DoT). Esse recurso pode tornar impossível o uso do recurso de segurança de DNS Umbrella, se não cuidadosamente planejado. O DNS seguro pode ser desabilitado por meio de políticas centralizadas e desabilitado por padrão, por exemplo, para computadores gerenciados pela empresa.



Para dispositivos BYOD não gerenciados, existem poucas opções. A primeira opção é bloquear a porta TCP 853 usada pelo DNS seguro. Você pode usar o Cisco Zone Based Firewall (ZBFW) para esse fim. A segunda opção seria ativar o bloqueio de categoria "Proxy/Anonymizer" no portal Umbrella. Você pode encontrar mais informações sobre isso aqui

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

Conclusão

Como você pode ver, a integração com a nuvem Umbrella DNS Security é muito simples do lado do cEdge e pode ser feita em poucos minutos.