配置与Cisco Umbrella的集成并排除常见问题

目录

简介

本文档介绍vManage/Cisco IOS®-XE SDWAN软件与Cisco Umbrella DNS安全解决方案集成的一部分。但是，它不涵盖Umbrella策略配置本身。您可以在此处找到有关Cisco Umbrella的详细信息；https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella。

> **注意：**您必须已经获取Umbrella订用并获取将用于配置cEdge路由器的Umbrella令牌。有关API令牌的详细信息：https://docs.umbrella.com/umbrella-api/docs/overview2。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

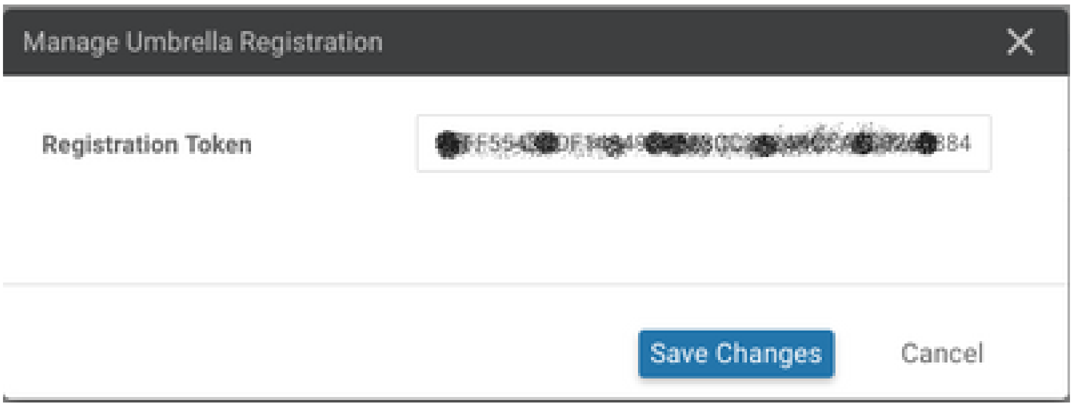
- vManage 18.4.0
- 运行(cEdge)16.9.3的Cisco IOS®-XE SDWAN路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

要配置与Cisco Umbrella的cEdge集成，请对vManage执行一组简单步骤：

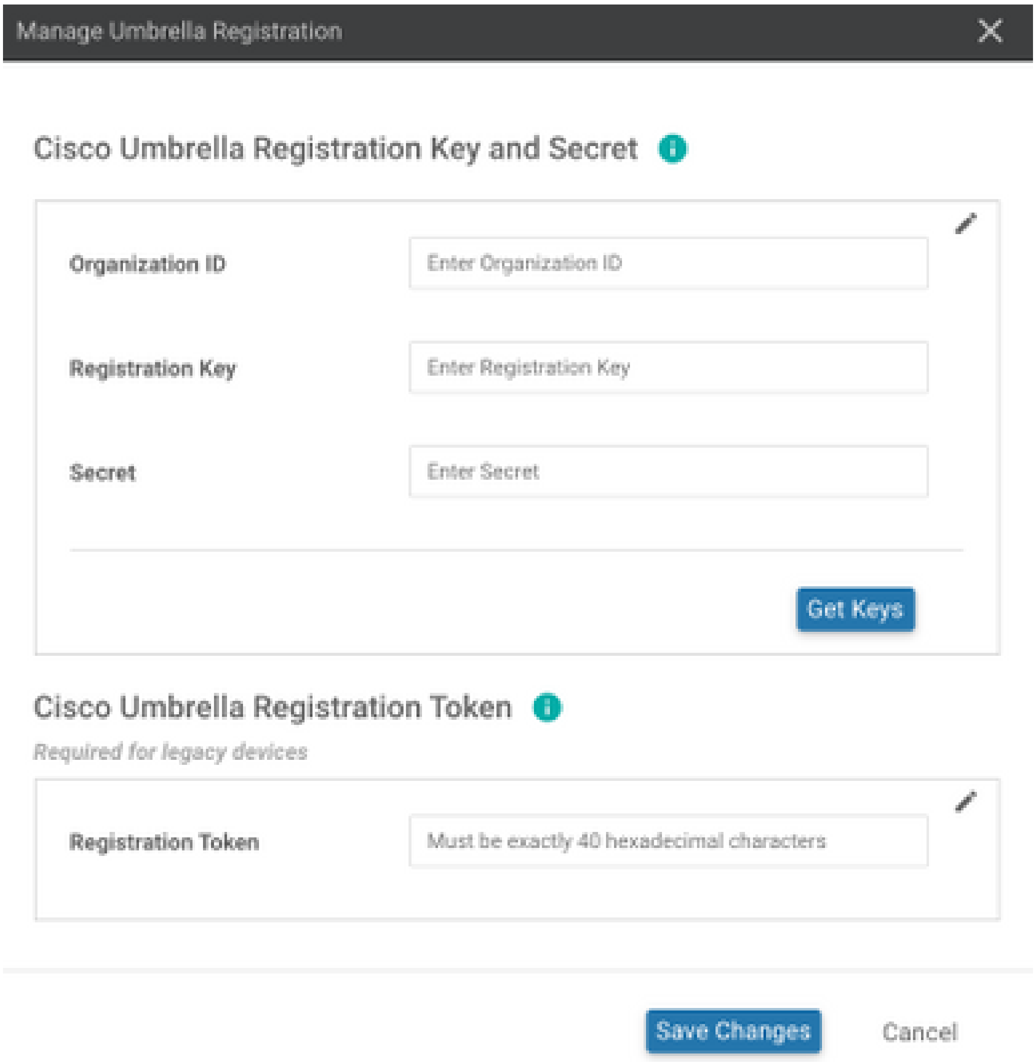
步骤1.在**Congifuration > Security**下，选择右上角的**Custom Options**下拉列表，然后选择**Umbrella API令牌**。输入Umbrella注册令牌，如图所示：



Manage Umbrella Registration

Registration Token [redacted]

或者，从vManage软件20.1.1版本开始，您可以指定组织ID、注册密钥和密钥。如果已在“管理”>“设置”>“智能帐户凭据”下配置了智能帐**户凭**据，则可**以自动**检索这**些参数**。



Manage Umbrella Registration

Cisco Umbrella Registration Key and Secret

Organization ID: Enter Organization ID

Registration Key: Enter Registration Key

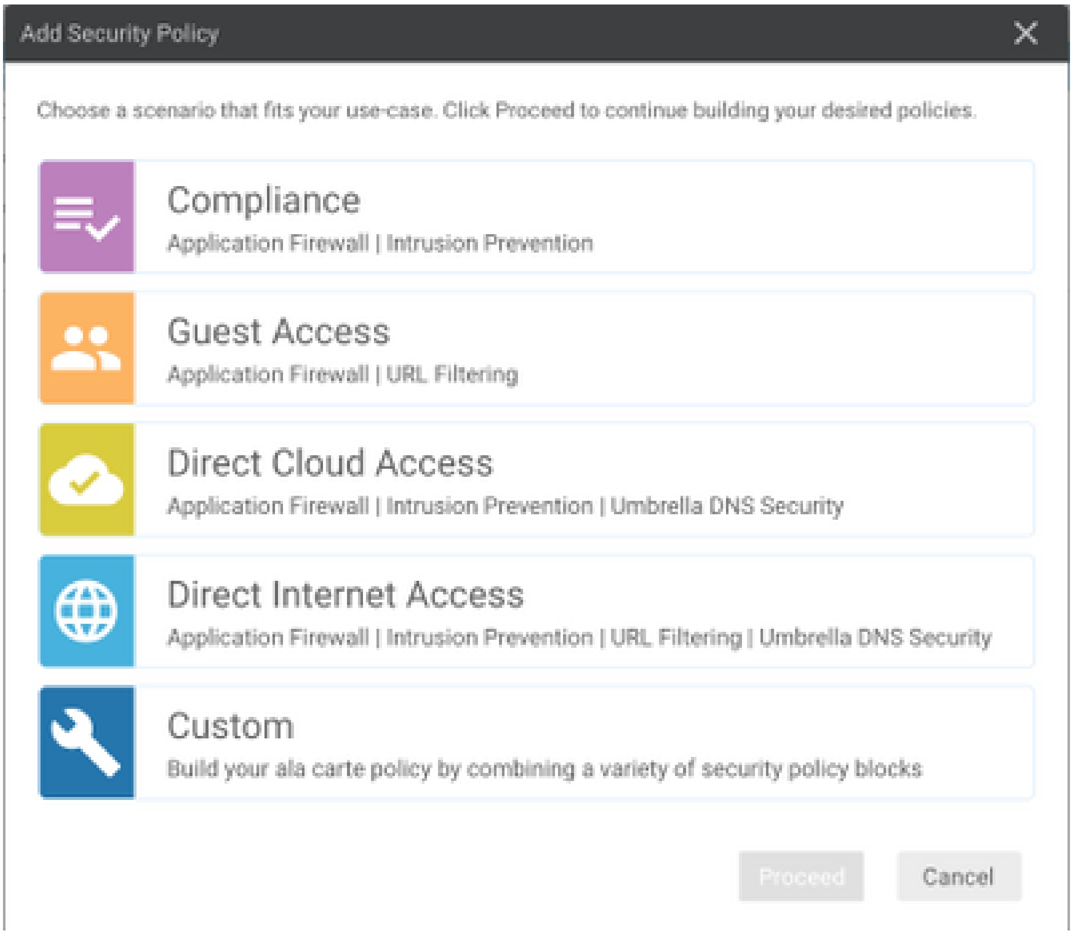
Secret: Enter Secret

Cisco Umbrella Registration Token

Required for legacy devices

Registration Token: Must be exactly 40 hexadecimal characters

步骤2.在**Configuration > Security**下，选择**Add Security Policy**，然后选择适合您的使用案例（例如自定义）的方案，如图所示：



Add Security Policy

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

Compliance
Application Firewall | Intrusion Prevention

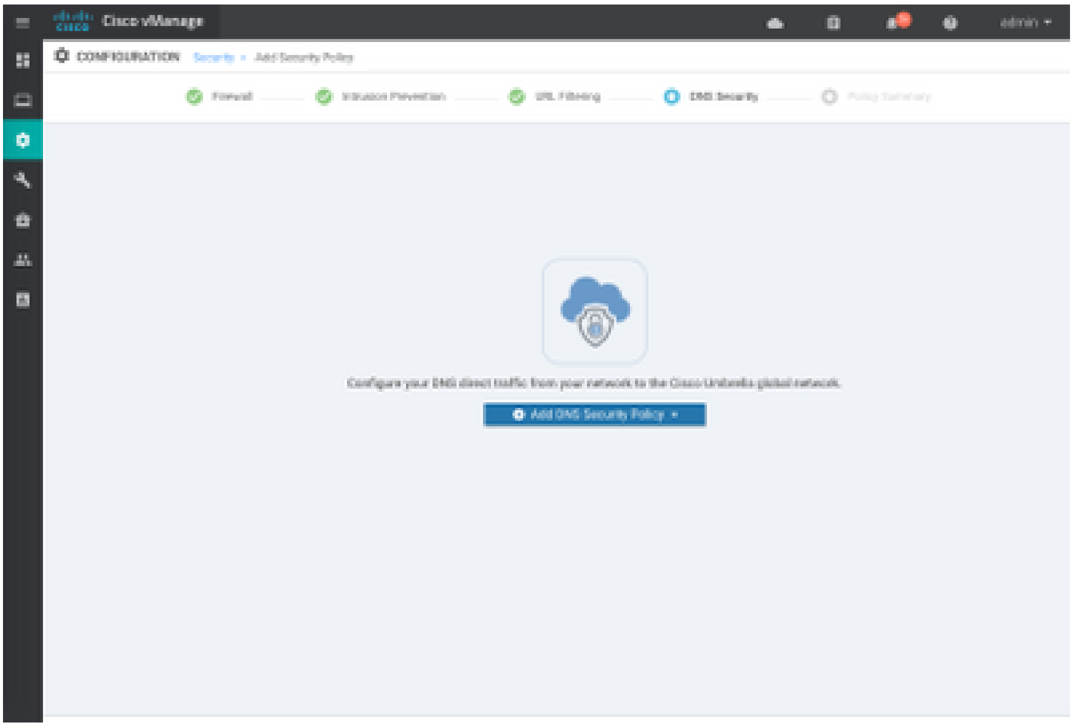
Guest Access
Application Firewall | URL Filtering

Direct Cloud Access
Application Firewall | Intrusion Prevention | Umbrella DNS Security

Direct Internet Access
Application Firewall | Intrusion Prevention | URL Filtering | Umbrella DNS Security

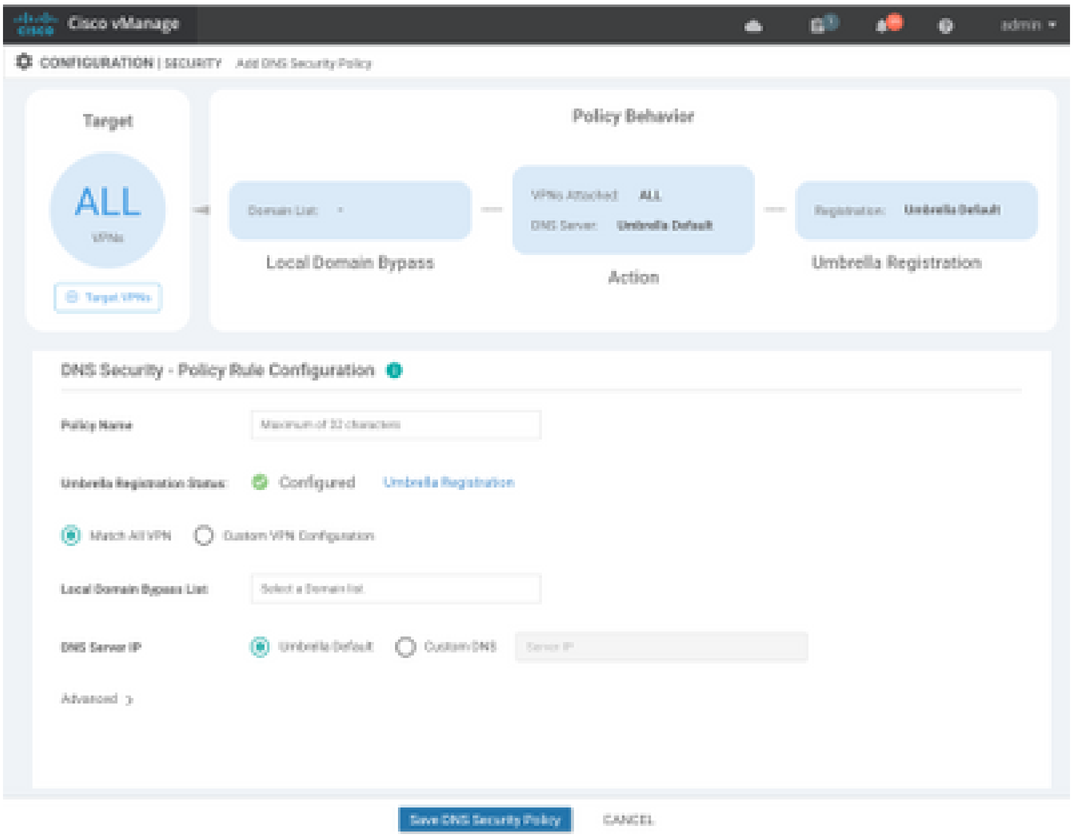
Custom
Build your ala carte policy by combining a variety of security policy blocks

步骤3.如图所示，导航至DNS安全，**选择添**加DNS安**全策略**，然后选**择新建。**



Configure your DNS direct traffic from your network to the Cisco Umbrella global network.

屏幕显示与下面所示的图像类似：



Domain List: -

VPNs Attached: ALL

DNS Server: Umbrella Default

Registration: Umbrella Default

DNS Security - Policy Rule Configuration

Policy Name: Maximum of 32 characters

Umbrella Registration Status: Configured Umbrella Registration

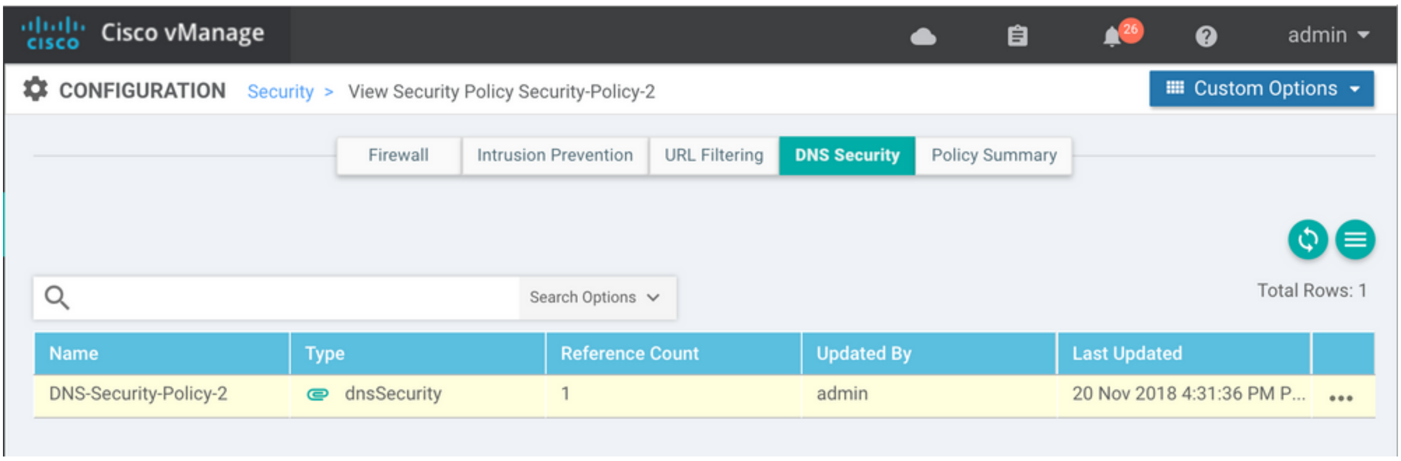
● Match All VPN ○ Custom VPN Configuration

Local Domain Bypass List: Select a Domain list

DNS Server IP: ● Umbrella Default ○ Custom DNS Server IP

Advanced >

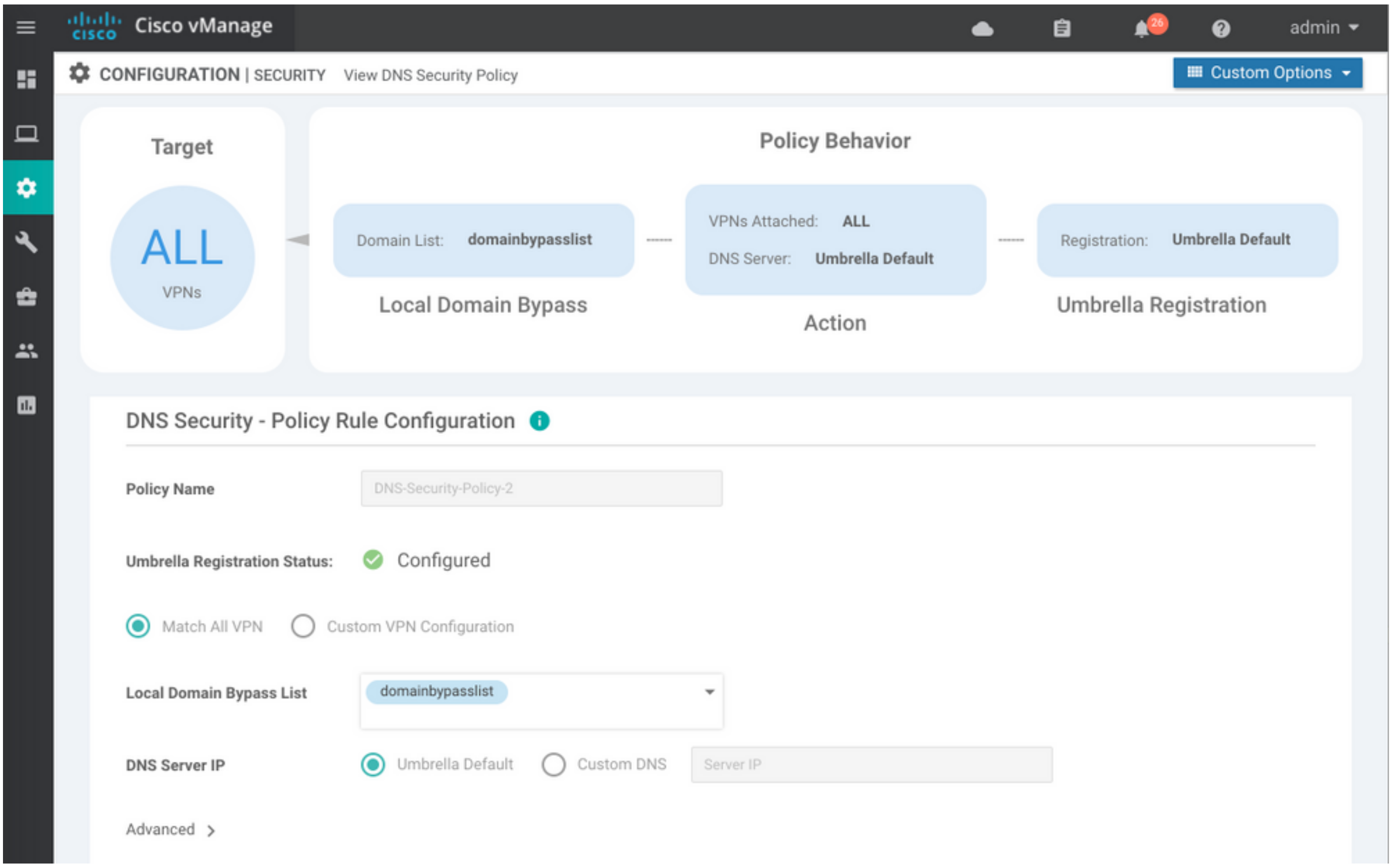
步骤4.这是配置后的显示方式。



Total Rows: 1

Name	Type	Reference Count	Updated By	Last Updated	
DNS-Security-Policy-2	dnsSecurity	1	admin	20 Nov 2018 4:31:36 PM P...	•••

步骤5.导航至策**略的......>查看> DNS**安全选项卡，您会看到类似于此映像的配置：



Domain List: domainbypasslist

VPNs Attached: ALL
DNS Server: Umbrella Default

Registration: Umbrella Default

DNS Security - Policy Rule Configuration

Policy Name: DNS-Security-Policy-2

Umbrella Registration Status: ✓ Configured

● Match All VPN ○ Custom VPN Configuration

Local Domain Bypass List: domainbypasslist

DNS Server IP: ● Umbrella Default ○ Custom DNS Server IP

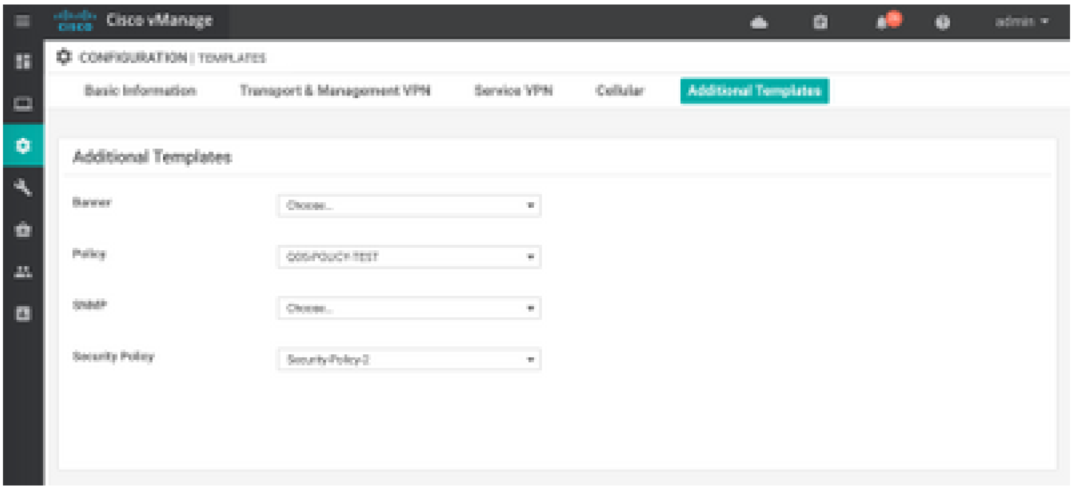
Advanced >

请记住，“本地域绕行列表”是一列域，路由器不会将DNS请求重定向到Umbrella云并将DNS请求发送到特定DNS服务器（位于企业网络内的DNS服务器），这不排除在Umbrella安全策略之外。为了将特定类别中的某些域“列入白名单”，建议改为在Umbrella配置门户上配置排除。

此外，您可以选择**预览**，以了解配置在CLI中的显示方式：

```
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
```

步骤6.现在必须在设备模板中引用策略。在**Configuration > Templates**下，选择您的配置模板，并在“Additional Templates”**部分中**引用它，如图所示。



Additional Templates

Banner: Choose...

Policy: QOS-POLICY-TEST

SNMP: Choose...

Security Policy: Security-Policy-2

步骤7.将模板应用于设备。

验证与故障排除

使用此部分确认您的配置工作正常并排除故障。

客户端验证

从位于cEdge后面的客户端，您可以在浏览以下测试站点时验证Umbrella是否正常工作：

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

有关详细信息，请参阅操作方法：成功测试以确保您正确运行Umbrella

边缘验证

验证和故障排除也可在cEdge本身上执行。一般来说，它类似于Cisco IOS-XE软件集成故障排除步骤，可在《安全配置指南》第2章的Cisco Umbrella Integration on Cisco 4000系列ISR中找到：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。

需要检查的有用命令很少：

步骤1.检查设备上的cEdge配置中是否显示了参数映射：

```
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
!
```

请注意，由于您习惯了在Cisco IOS-XE上查看此参数映射，因此在接口上找不到对此参数映射的引用。

这是因为参数映射应用于VRF而不是接口，因此您可以在此处进行检查：

```
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
```

此外，您还可以使用此命令获取详细信息：

```
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


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

步骤2.检查设备是否已成功注册到Umbrella DNS安全云。

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

步骤3.以下是如何检查雨伞DNS重定向统计信息。

```
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
```

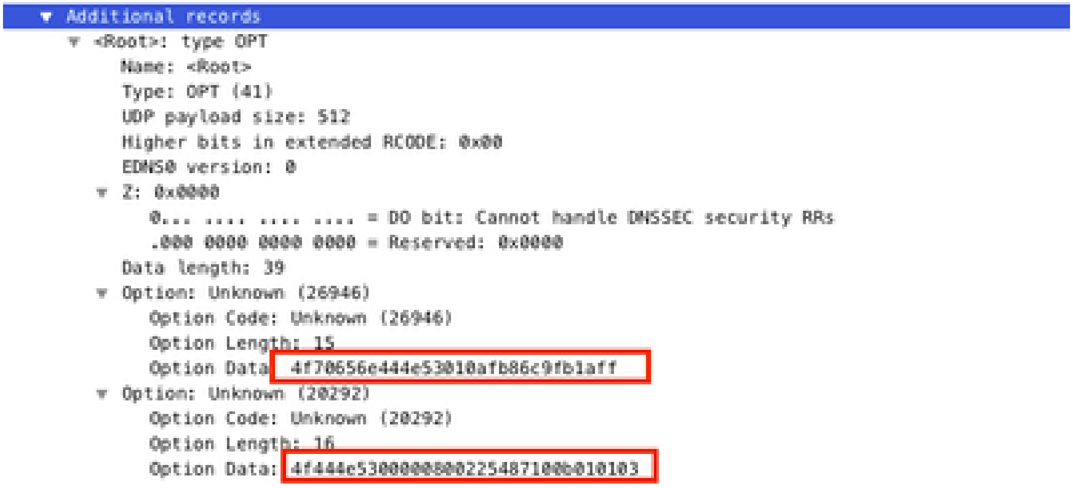
步骤4.检查DNS解析器是否可通过通用工具访问，以便对ping和traceroute等故障进行故障排除。

步骤5.您还可以使用Cisco IOS-XE的嵌入式数据包捕获，以执行从cEdge发出的DNS数据包捕获。

有关详细信息，请参阅配置指南：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。

了解Umbrella的EDNS实施

捕获数据包后，确保DNS查询已正确重定向到Umbrella DNS解析器:208.67.222.222和208.67.220.220，其中包含正确的EDNS0（DNS扩展机制）信息。-WAN Umbrella DNS层检测集成，当cEdge设备将DNS查询发送到Umbrella DNS解析时，它包含ENDS0选项。这些扩展包括从Umbrella接收的设备ID cEdge和Umbrella的组织ID，以便确定在您应答DNS查询时要使用的正确策略。以下是EDNS0数据包格式的示例：



```
  ▼ 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
```

以下是选项细分：

RDATA说明：

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

RDATA远程IP地址选项：

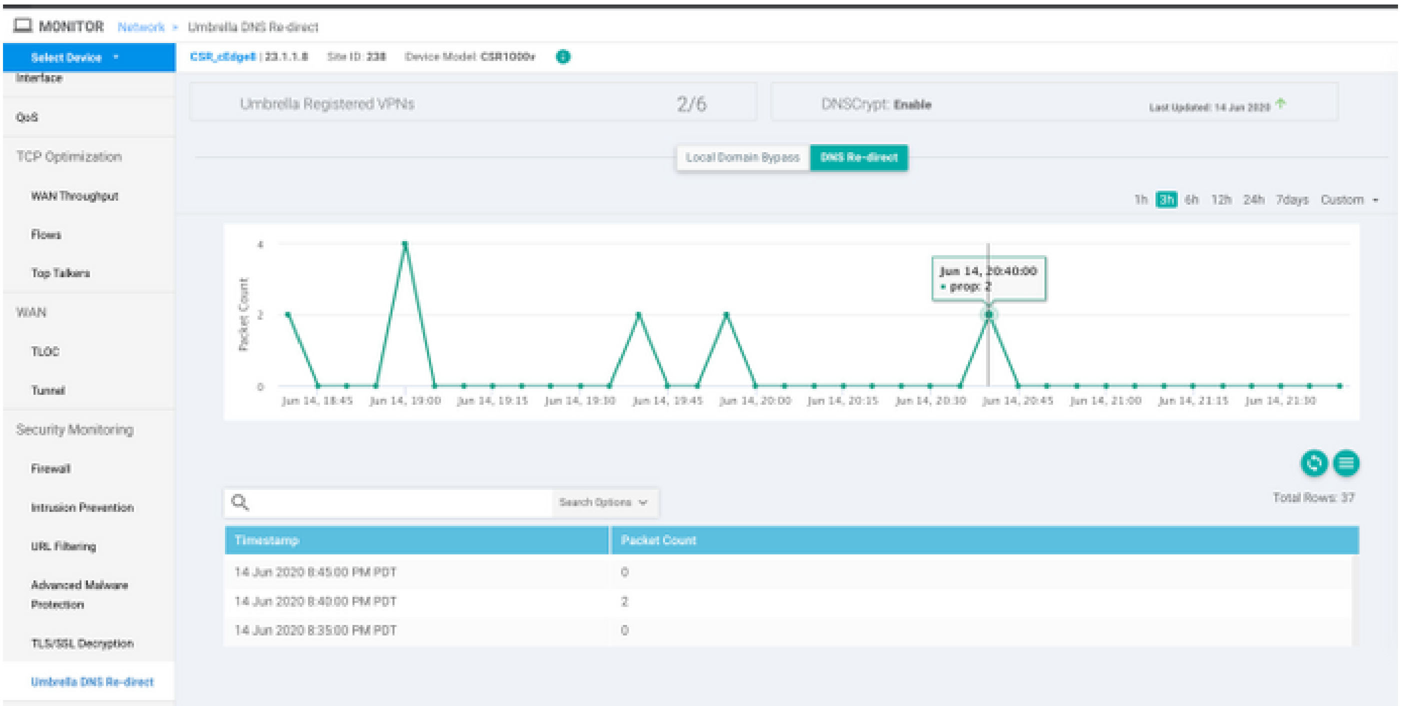
```
0x4f444e53: MGGIC = 'ODNS'
0x00       : Version
0x00       : Flags
0x08       : Organization ID Required
0x00225487: Organization ID
0x10 type : Remote IPv4
0x0b010103: Remote IP Address = 11.1.1.3
```

检查并确保设备ID正确，并且组织ID使用Umbrella门户与Umbrella帐户匹配。

> **注意：**启用DNSCrypt后，DNS查询将被加密。如果数据包捕获显示DNScrypt数据包进入Umbrella解析器，但没有返回流量，请尝试禁用DNSCrypt，以查看这是否是问题。

在vManage控制面板上验证

任何思科Umbrella定向流量都可从vManage控制面板查看。可以在“监视”**>“网络”>“Umbrella DNS Re-direct”下查看**。以下是此页的图像：



CSR_cEdge8 | 23.1.1.8 Site ID: 238 Device Model: CSR1000v

Umbrella Registered VPNs 2/6

DNSCrypt: Enable

Last Updated: 14 Jun 2020

Total Rows: 37

Timestamp	Packet Count
14 Jun 2020 8:45:00 PM PDT	0
14 Jun 2020 8:40:00 PM PDT	2
14 Jun 2020 8:35:00 PM PDT	0

DNS缓存

在Cisco cEdge路由器上，本地域旁路标志有时不匹配。当主机/客户端中涉及缓存时，会发生这种情况。例如，如果本地域旁路配置为匹配和绕过www.cisco.com(**.*cisco.com**)。 第一次，查询是针对www.cisco.com,也返回CDN名称作为CNAME，CNAME缓存在客户端上。对www.cisco.com的nslookup的后续查询只发送CDN域(akamaiedge)的查询。

```
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
```

如果本地域绕行工作正常，您将看到解析器OpenDNS重定向的计数器增加。以下是缩写输出。

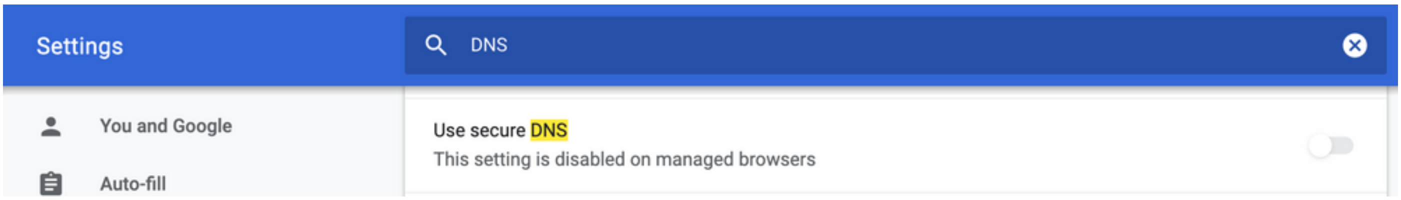
```
dmz2-site201-1#show platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats:
    Parser statistics:
      parser unknown pkt: 0
      parser fmt error: 0
      parser count nonzero: 0
      parser pa error: 0
      parser non query: 0
      parser multiple name: 0
```

```
        parser dns name err: 0
        parser matched ip: 0
        parser opendns redirect: 3
        local domain bypass: 0 <<<<<<<<<<<
```

这可能是路由器上看不到本地域旁路的原因。清除主机/客户端计算机上的缓存时，您会看到查询正确输出。

安全DNS

Google Chrome等从83版开始的现代浏览器使用安全DNS，也称为HTTPS(DoH)或TLS(DoT)DNS。如果未经过精心规划，此功能可能使Umbrella DNS安全功能无法使用。安全DNS可通过集中策略禁用，默认情况下禁用，例如，对于企业托管计算机。


Use secure DNS
This setting is disabled on managed browsers

对于非托管BYOD设备，存在的选项很少。第一个选项是阻止安全DNS使用的TCP端口853。您可以使用思科基于区域的防火墙(ZBFW)来实现此目的。第二个选项是在Umbrella门户上启用“代理/匿名程序”类别阻止。您可以在此处找到有关此项的详细信息

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

结论

如您所见，从cEdge端与Umbrella DNS安全云的集成非常简单，只需几分钟即可完成。