Integration mit Cisco Umbrella konfigurieren und Fehlerbehebung für häufige Probleme durchführen

Inhalt

Einführung

Dieses Dokument beschreibt die SDWAN-Software vManage/Cisco IOS®-XE als Teil der Integration in die Cisco Umbrella DNS Security-Lösung. Die Konfiguration der Umbrella-Richtlinien selbst wird jedoch nicht behandelt. Weitere Informationen zu Cisco Umbrella finden Sie unter https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella.

> **Hinweis:** Sie müssen bereits Umbrella-Abonnements erworben haben und ein Umbrella-Token erhalten, das für die Konfiguration von cEdge-Routern verwendet wird. Weitere Informationen zu API-Token finden Sie unter https://docs.umbrella.com/umbrella-api/docs/overview2.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

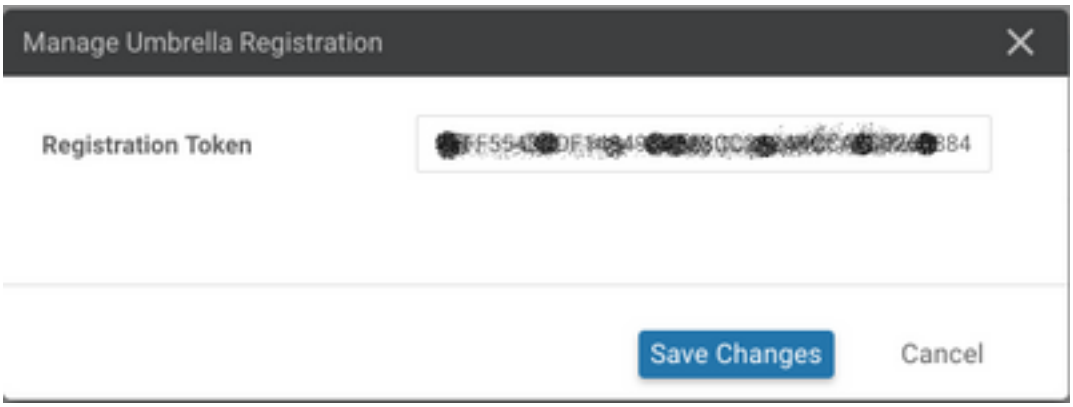
- vManage 18.4.0
- Cisco IOS®-XE SDWAN-Router mit cEdge 16.9.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

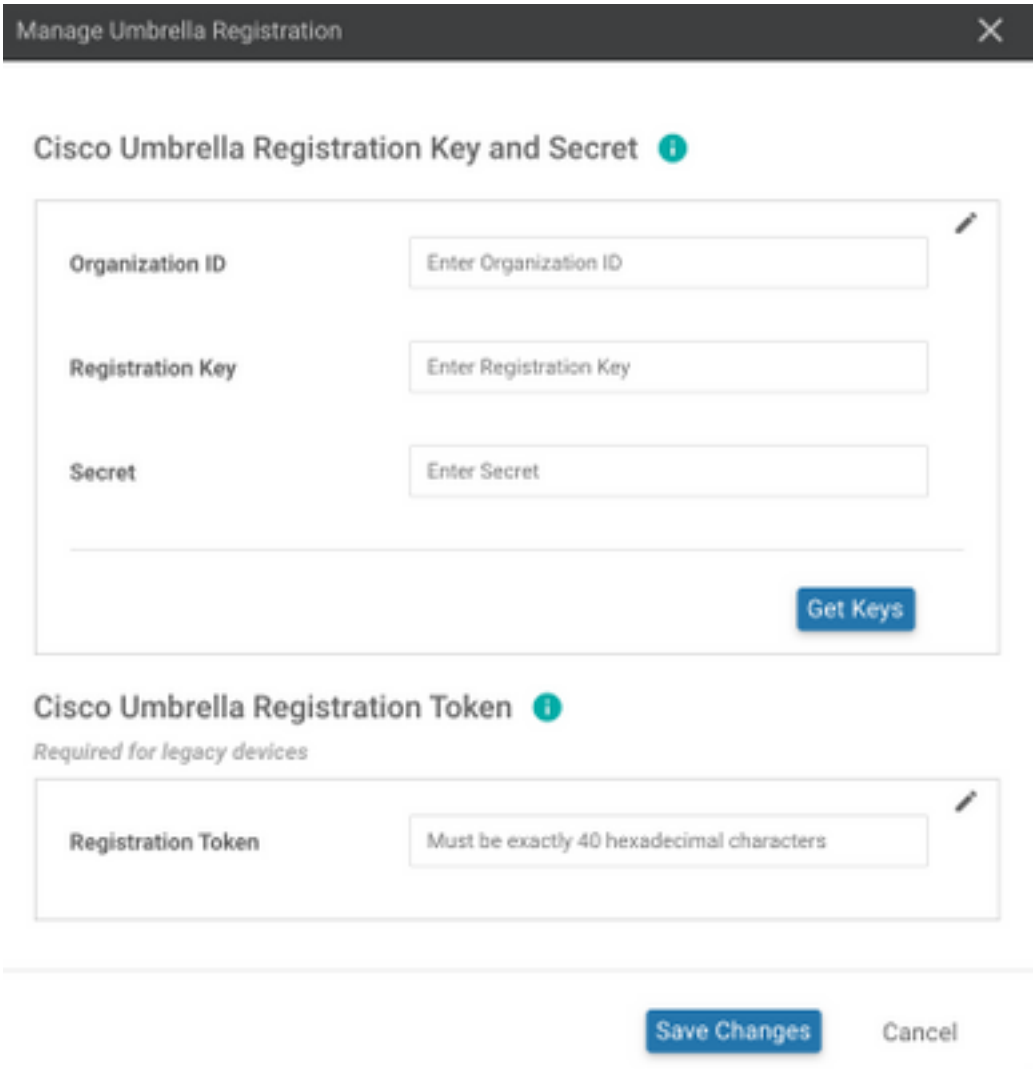
Konfiguration

Zur Konfiguration Ihrer cEdge-Integration mit Cisco Umbrella führen Sie in vManage eine Reihe einfacher Schritte aus:

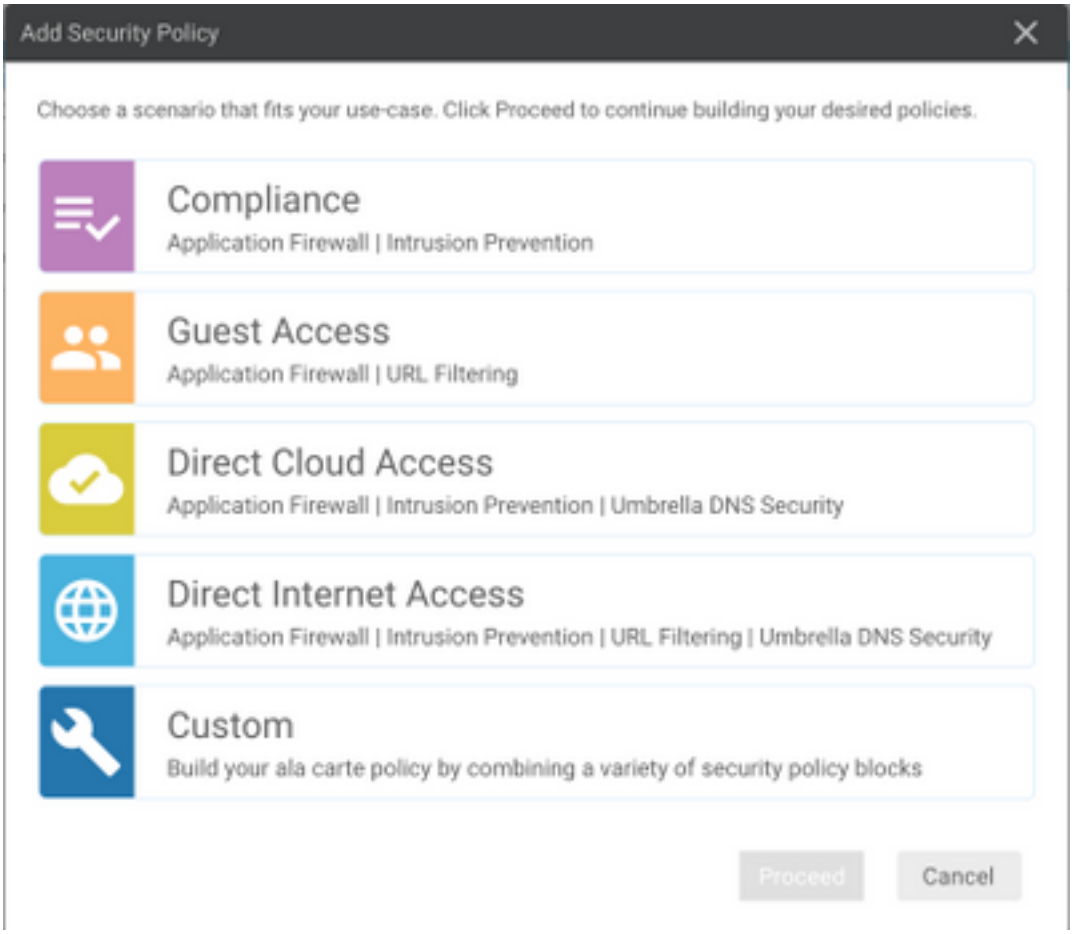
Schritt 1: Wählen Sie unter **Konfiguration > Sicherheit** in der rechten oberen Ecke die Option **Benutzerdefinierte Optionen** aus, und wählen Sie dann **Umbrella API Token aus**. Geben Sie Ihr Umbrella-Registrierungstoken ein, wie im Bild gezeigt:



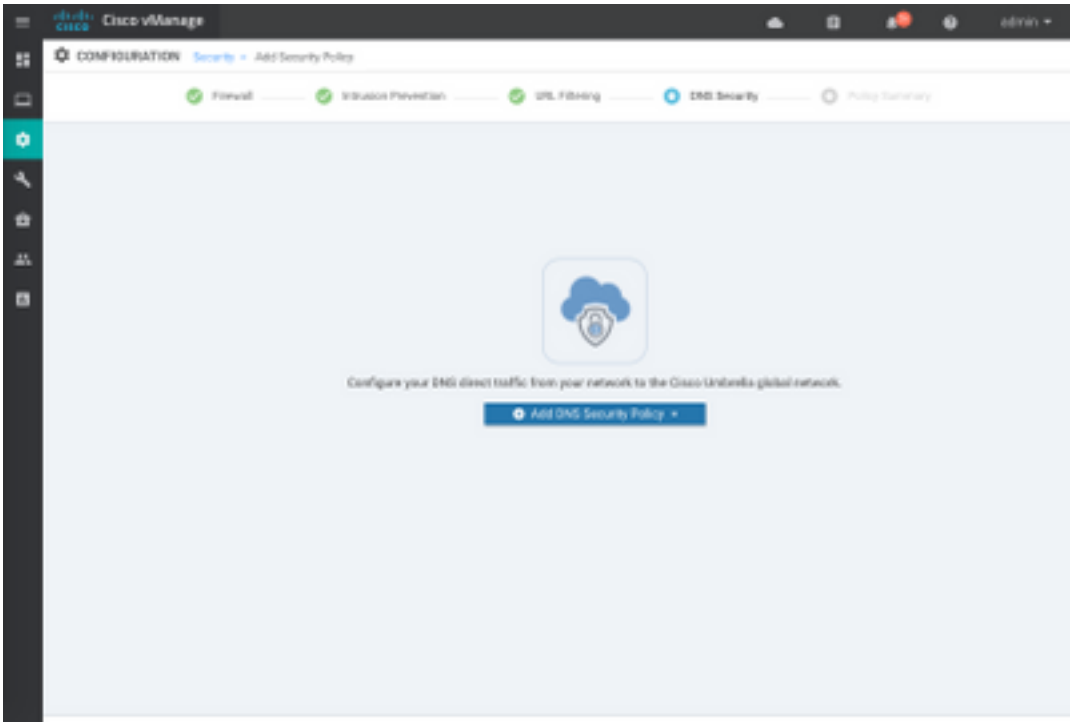
Alternativ können Sie ab Version 20.1.1 der vManage-Software Organisation-ID, Registrierungsschlüssel und Secret angeben. Diese Parameter können automatisch abgerufen werden, wenn Sie Ihre Smart Account-Anmeldeinformationen unter **Administration > Einstellungen > Smart Account Credentials** konfiguriert haben.



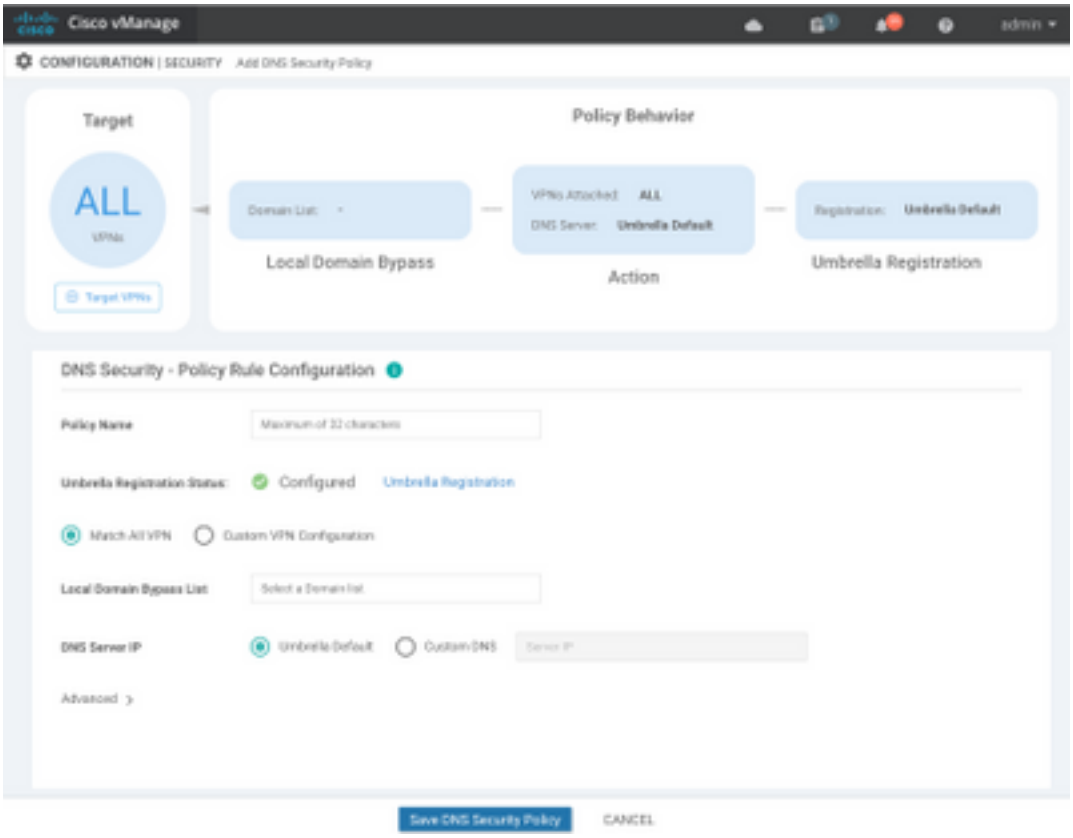
Schritt 2: Wählen Sie unter **Konfiguration > Sicherheit** die Option **Sicherheitsrichtlinie hinzufügen aus**, und wählen Sie dann ein Szenario aus, das zu Ihrem Anwendungsfall passt (z. B. benutzerdefiniert), wie im Bild gezeigt:



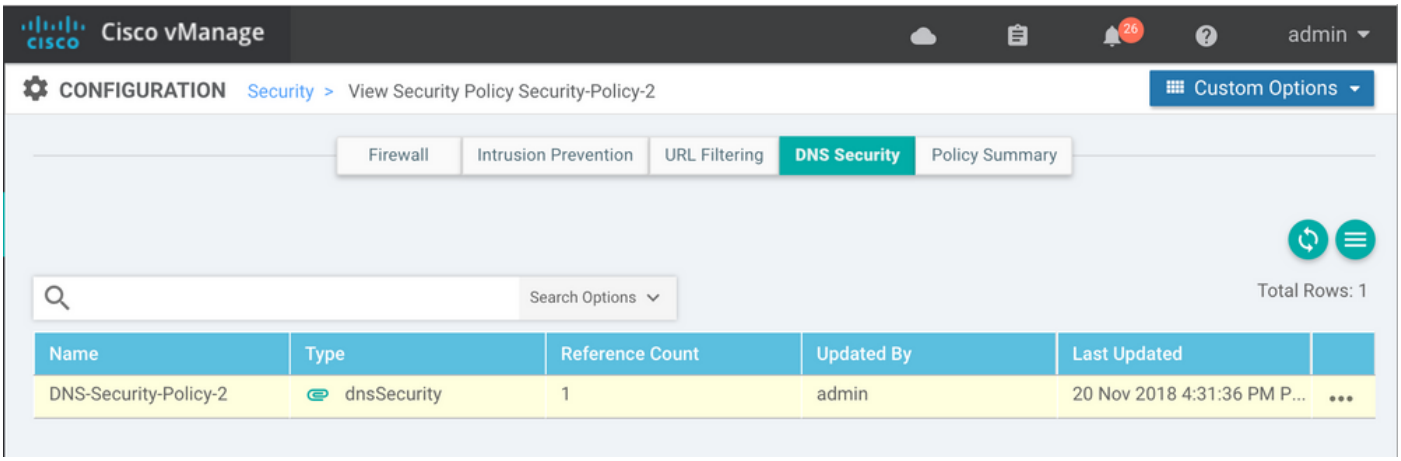
Schritt 3: Navigieren Sie, wie im Bild gezeigt, zu **DNS-Sicherheit**, wählen Sie **DNS-Sicherheitsrichtlinie hinzufügen aus,** und wählen Sie **Neues erstellen aus.**



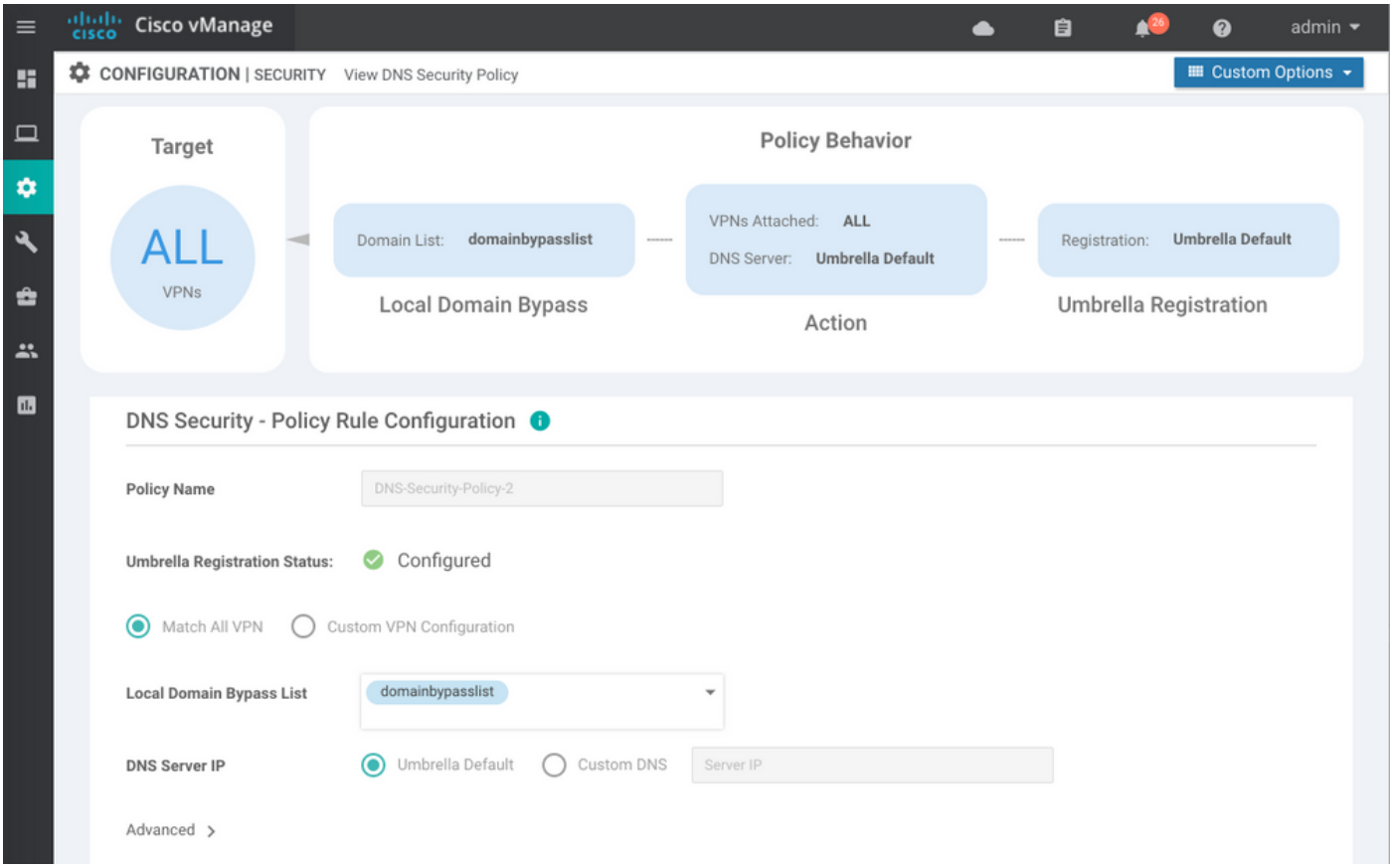
Der Bildschirm ähnelt dem hier gezeigten Bild:



Schritt 4: Dies ist das Bild, wie es angezeigt wird, sobald konfiguriert.



Schritt 5: Navigieren Sie zur Registerkarte **...> View > DNS Security** (**Ansicht > DNS-Sicherheit**) Ihrer Richtlinie. Die Konfiguration ähnelt der folgenden Abbildung:

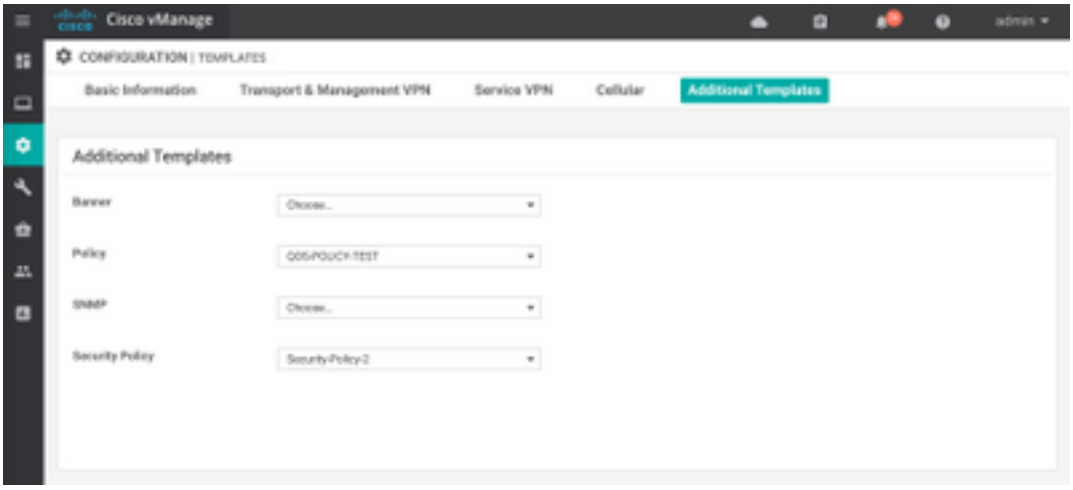


Beachten Sie, dass "Local Domain Bypass List" eine Liste von Domänen ist, für die der Router keine DNS-Anfragen an die Umbrella Cloud umleitet und eine DNS-Anfrage an einen bestimmten DNS-Server (DNS-Server im Unternehmensnetzwerk) sendet. Dies ist kein Ausschluss von Umbrella-Sicherheitsrichtlinien. Um einige Domänen aus der jeweiligen Kategorie "Whitelist" zu erstellen, wird empfohlen, den Ausschluss auf dem übergeordneten Konfigurationsportal zu konfigurieren.

Sie können auch **Vorschau** auswählen, um zu verstehen, wie die Konfiguration in der CLI aussieht:

```
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
```

Schritt 6: Nun müssen Sie in der Gerätevorlage auf Richtlinien verweisen. Wählen Sie unter **Konfiguration > Vorlagen** Ihre Konfigurationsvorlage aus, und verweisen Sie auf sie im Abschnitt **Zusätzliche Vorlagen**, wie im Bild gezeigt.



Schritt 7: Wenden Sie die Vorlage auf das Gerät an.

Überprüfung und Fehlerbehebung

In diesem Abschnitt können Sie überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert, und Fehler beheben.

Client-Verifizierung

Von einem Client hinter dem cEdge können Sie überprüfen, ob Umbrella korrekt funktioniert, wenn Sie diese Teststandorte durchsuchen:

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

Weitere Informationen finden Sie unter Gewusst wie: Erfolgreiche Tests, um sicherzustellen, dass Umbrella ordnungsgemäß ausgeführt wird

cEdge-Verifizierung

Die Überprüfung und Fehlerbehebung kann auch am cEdge selbst durchgeführt werden. Im Allgemeinen ähnelt sie den Verfahren zur Fehlerbehebung bei der Cisco IOS-XE-Softwareintegration, die in Kapitel 2 des Konfigurationsleitfadens für die Cisco Umbrella Integration in Cisco ISR der Serie 4000 beschrieben sind: 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.

Wenige nützliche Befehle zur Überprüfung:

Schritt 1: Überprüfen Sie, ob die Parameterzuordnung in der cEdge-Konfiguration des Geräts angezeigt wird:

```
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
!
```

Beachten Sie, dass Sie keinen Verweis auf diese Parameterzuordnung auf der Schnittstelle finden können, wenn Sie sie in Cisco IOS-XE sehen.

Dies liegt daran, dass die Parameterzuordnung auf VRFs und nicht auf Schnittstellen angewendet wird. Sie können sie hier überprüfen:

```
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
```

Außerdem können Sie mit diesem Befehl detaillierte Informationen abrufen:

```
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


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

Schritt 2: Überprüfen Sie, ob das Gerät erfolgreich in der Umbrella DNS Security Cloud registriert wurde.

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

Schritt 3: Hier sehen Sie, wie Sie Umbrella DNS Redirect Statistiken überprüfen können.

```
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
```

Schritt 4: Stellen Sie sicher, dass der DNS-Resolver mit generischen Tools erreichbar ist, um Fehler wie Ping und Traceroute zu beheben.

Schritt 5: Sie können auch die integrierte Paketerfassung von Cisco IOS-XE verwenden, um die DNS-Paketerfassung vom cEdge aus durchzuführen.

Weitere Informationen finden Sie im Konfigurationsleitfaden: 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.

Verständnis der EDNS-Implementierung des Umbrella

Nachdem eine Paketerfassung durchgeführt wurde, stellen Sie sicher, dass die DNS-Abfragen korrekt an die Umbrella-DNS-Resolver umgeleitet werden: 208.67.222.222 und 208.67.220.220 mit den richtigen EDNS0 (Extension Mechanism for DNS)-Informationen. Durch die Integration von SD-WAN Umbrella DNS Layer Inspection (DNS-Layer-Inspektion) enthält das cEdge-Gerät ENDS0-Optionen, wenn es DNS-Abfragen an die Umbrella DNS-Auflösungen sendet. Zu diesen Erweiterungen gehören die Geräte-ID cEdge, die von Umbrella empfangen wird, und die Organisation-ID für Umbrella, um die richtige Richtlinie zu identifizieren, die beim Beantworten der DNS-Abfrage verwendet wird. Das folgende Beispiel zeigt das EDNS0-Paketformat:

Im Folgenden finden Sie eine Aufschlüsselung der Optionen:

RDATA-Beschreibung:

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

IP-Adressenoption RDATA Remote:

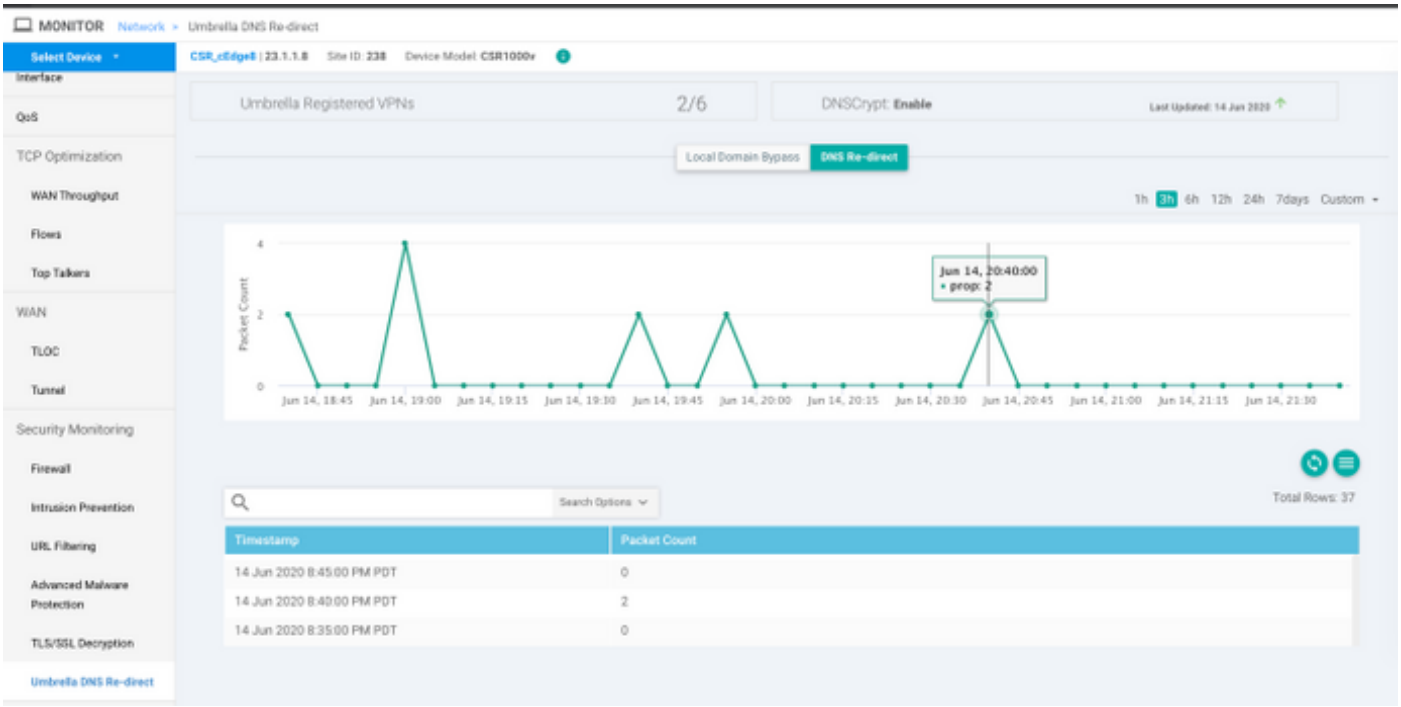
```
0x4f444e53: MGGIC = 'ODNS'
0x00      : Version
0x00      : Flags
0x08      : Organization ID Required
0x00225487: Organization ID
0x10 type : Remote IPv4
0x0b010103: Remote IP Address = 11.1.1.3
```

Überprüfen und vergewissern Sie sich, dass die Geräte-ID korrekt ist und die Organisation-ID mit dem übergeordneten Konto übereinstimmt.

> **Hinweis:** Bei aktivierter DNSCrypt-Funktion werden DNS-Abfragen verschlüsselt. Wenn die Paketerfassungen zeigen, dass DNSCrypt-Paket an den Umbrella-Resolver geleitet wird, aber kein Rückgabeverkehr vorhanden ist, versuchen Sie, DNSCrypt zu deaktivieren, um zu überprüfen, ob das Problem vorliegt.

Überprüfen Sie es auf dem vManage Dashboard.

Jeder von Cisco Umbrella gesteuerte Datenverkehr kann über das vManage Dashboard angezeigt werden. Sie kann unter **Monitor > Network > Umbrella DNS Re-direct** angezeigt werden. Das Bild dieser Seite ist wie folgt:



DNS-Caching

Auf einem Cisco cEdge-Router stimmen lokale Domänen-Umgehungsmarkierungen manchmal nicht überein. Dies geschieht, wenn ein Zwischenspeichern im Hostcomputer/Client stattfindet. Beispiel: Wenn die lokale Domänen-Umgehung so konfiguriert ist, dass sie www.cisco.com (**.*cisco.com**) konform und umgeht. Zum ersten Mal wurde die Abfrage für www.cisco.com ausgeführt, die auch CDN-Namen als CNAMEs zurückgab, die auf dem Client zwischengespeichert wurden. Spätere Abfragen für nslookup für www.cisco.com sollten nur die Abfragen für die CDN-Domäne (akamaiedge) senden.

```
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
```

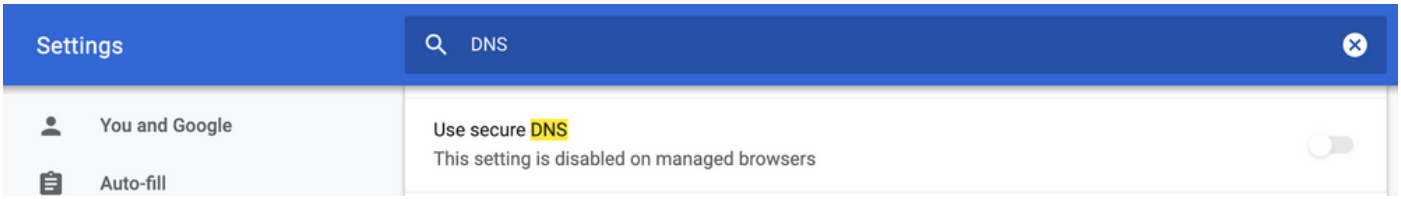
Wenn die lokale Domain-Bypass-Funktion ordnungsgemäß funktioniert, werden Sie sehen, dass die Zähler für Parser-OpenDNS-Umleitung erhöht werden. Dies ist eine abgekürzte Ausgabe.

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

Dies könnte der Grund dafür sein, warum die Umgehung lokaler Domänen auf dem Router nicht sichtbar ist. Wenn Sie den Cache auf dem Host-/Clientcomputer löschen, sehen Sie, dass die Abfragen ordnungsgemäß ausgeführt werden.

Sicheres DNS

Moderne Browser wie Google Chrome ab Version 83 verwenden Secure DNS auch bekannt als DNS over HTTPS (DoH) oder DNS over TLS (DoT). Diese Funktion kann dazu führen, dass Umbrella-DNS-Sicherheitsfunktionen nicht genutzt werden können, wenn sie nicht sorgfältig geplant sind. Secure DNS kann über zentrale Richtlinien deaktiviert und standardmäßig deaktiviert werden, z. B. für von Unternehmen verwaltete Computer.



Für nicht verwaltete BYOD-Geräte gibt es nur wenige Optionen. Die erste Option besteht darin, den TCP-Port 853 zu blockieren, der von Secure DNS verwendet wird. Zu diesem Zweck können Sie die Cisco Zone Based Firewall (ZBFW) verwenden. Die zweite Option wäre die Aktivierung der "Proxy/Anonymizer"-Kategoriensperrung im Umbrella-Portal. Weitere Informationen hierzu finden Sie hier

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

Fazit

Wie Sie sehen können, ist die Integration in die Umbrella DNS Security Cloud auf cEdge-Seite sehr einfach und kann in wenigen Minuten erfolgen.