تكوين التكامل مع Cisco Umbrella واستكشاف المشاكل الشائعة وإصلاحها

المحتويات

المقدمة

يصف هذا المستند جزء برنامج vManage/Cisco IOS®-XE SDWAN من التكامل مع حل أمان Cisco Umbrella DNS. وهو ذلك، فإنه لا يغطي تكوين سياسات Umbrella نفسها. يمكنك العثور على مزيد من المعلومات حول Cisco Umbrella هنا: https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella.

> **ملاحظة**: يجب أن تكون قد حصلت بالفعل على اشتراكات Umbrella والحصول على رمز Umbrella المميز الذي سيتم إستخدامه في تكوين موجهات cEdge. المزيد حول رمز API المميز: https://docs.umbrella.com/umbrella-api/docs/overview2.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- vManage 18.4.0
- موجه Cisco IOS®-XE SDWAN الذي يشغل (cEdge) 16.9.3

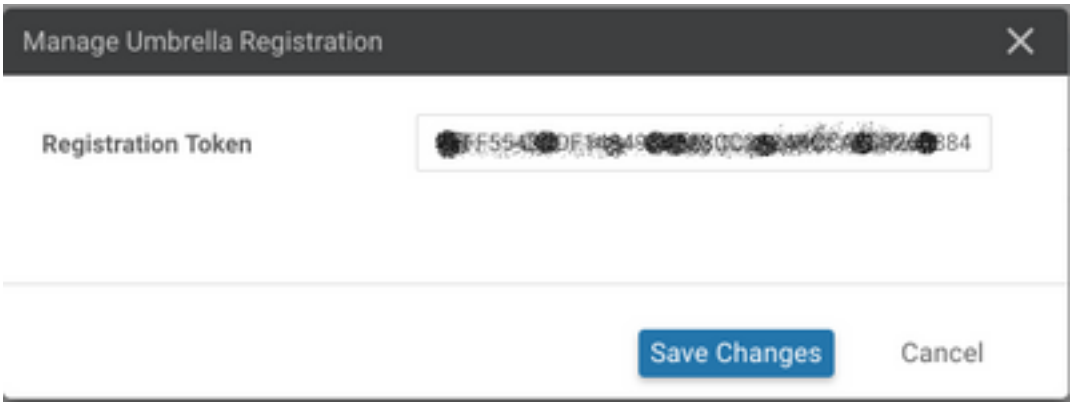
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

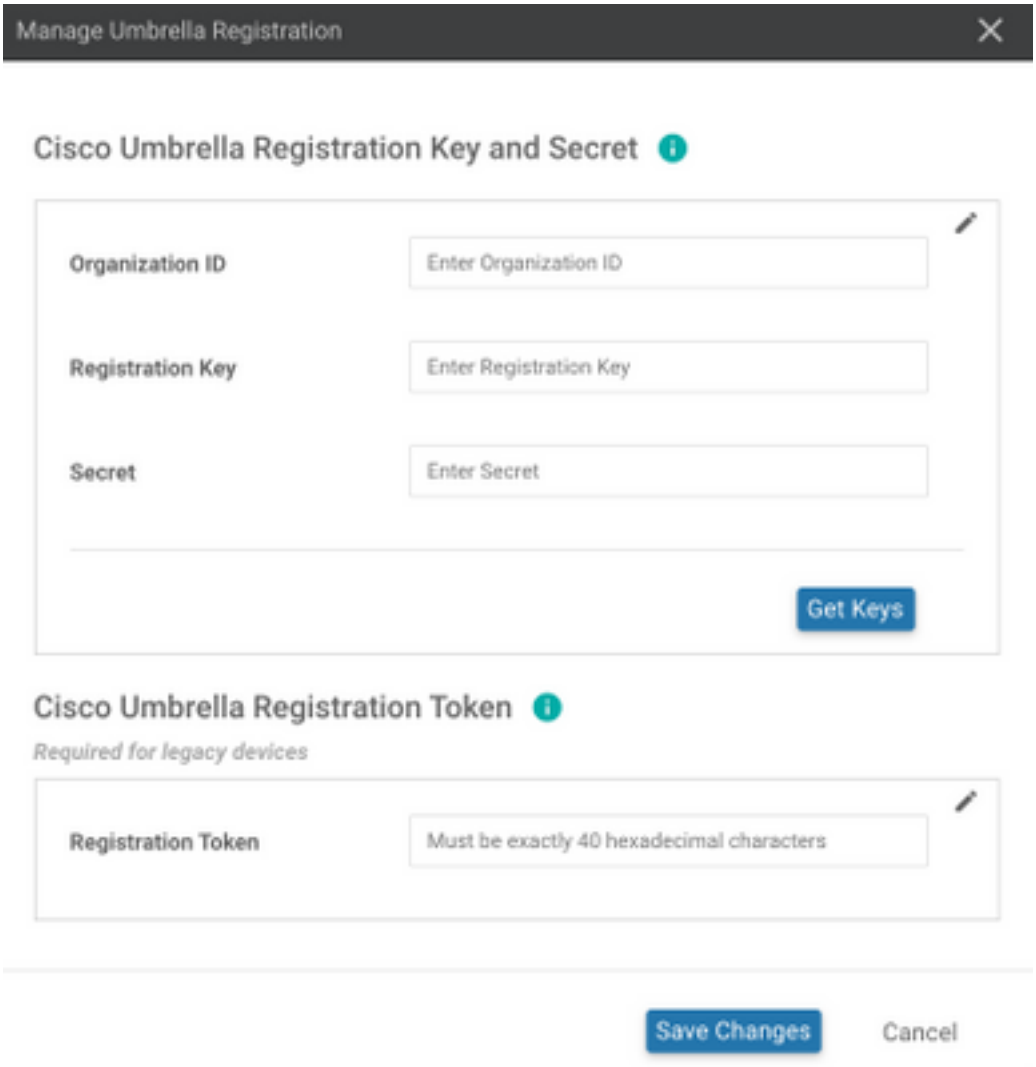
التكوين

لتكوين تكامل cEdge مع Cisco Umbrella، يمكنك تنفيذ مجموعة من الخطوات البسيطة على vManage:

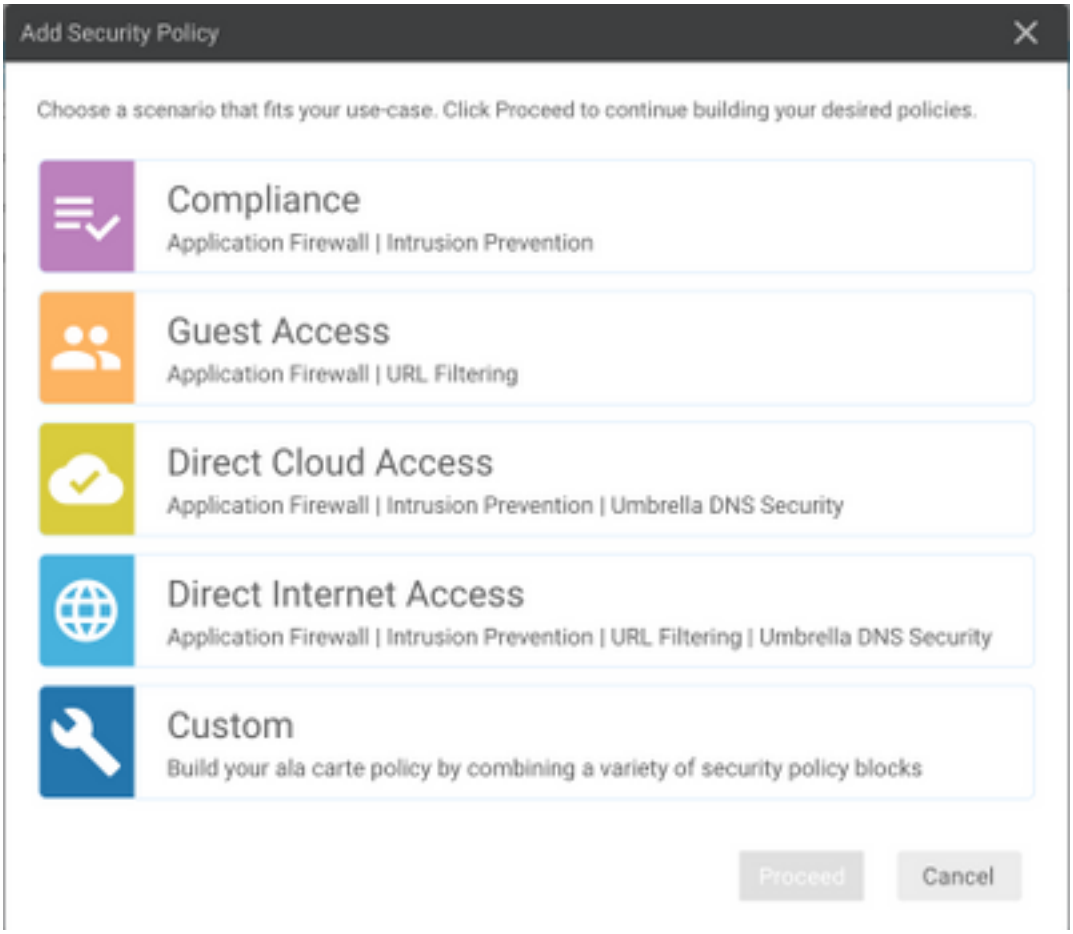
الخطوة 1. تحت **تكوين > الأمان**، حدد **القائمة المنسدلة خيارات مخصصة** في الركن العلوي الأيمن، ثم حدد **الرمز المميز لواجهة برمجة التطبيقات (API) الخاصة بالمظلة**. أدخل الرمز المميز لتسجيل Umbrella، كما هو موضح في الصورة:



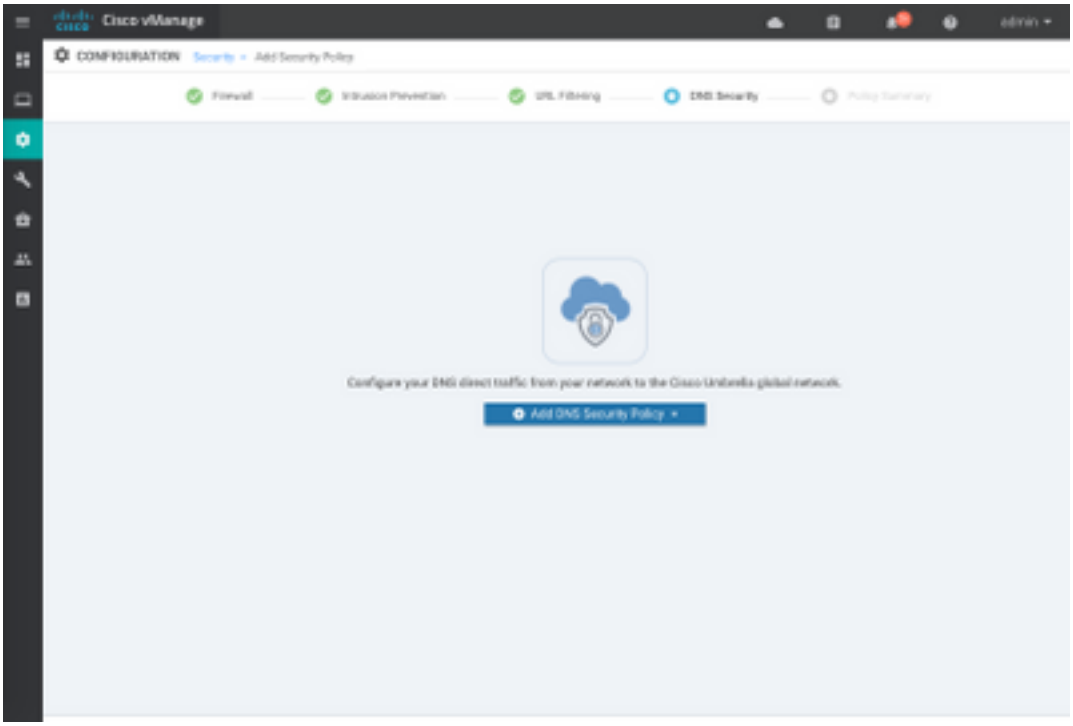
بدلا من ذلك، بدءا من إصدار برنامج vManage 20.1.1، يمكنك تحديد معرف المؤسسة ومفتاح التسجيل والسر. يمكن إستيراد هذه المعلومات تلقائيا إذا قمت بتكوين بيانات اعتماد الحساب الذكي" تحت إدارة **> إعدادات > بيانات اعتماد الحساب الذكي**.



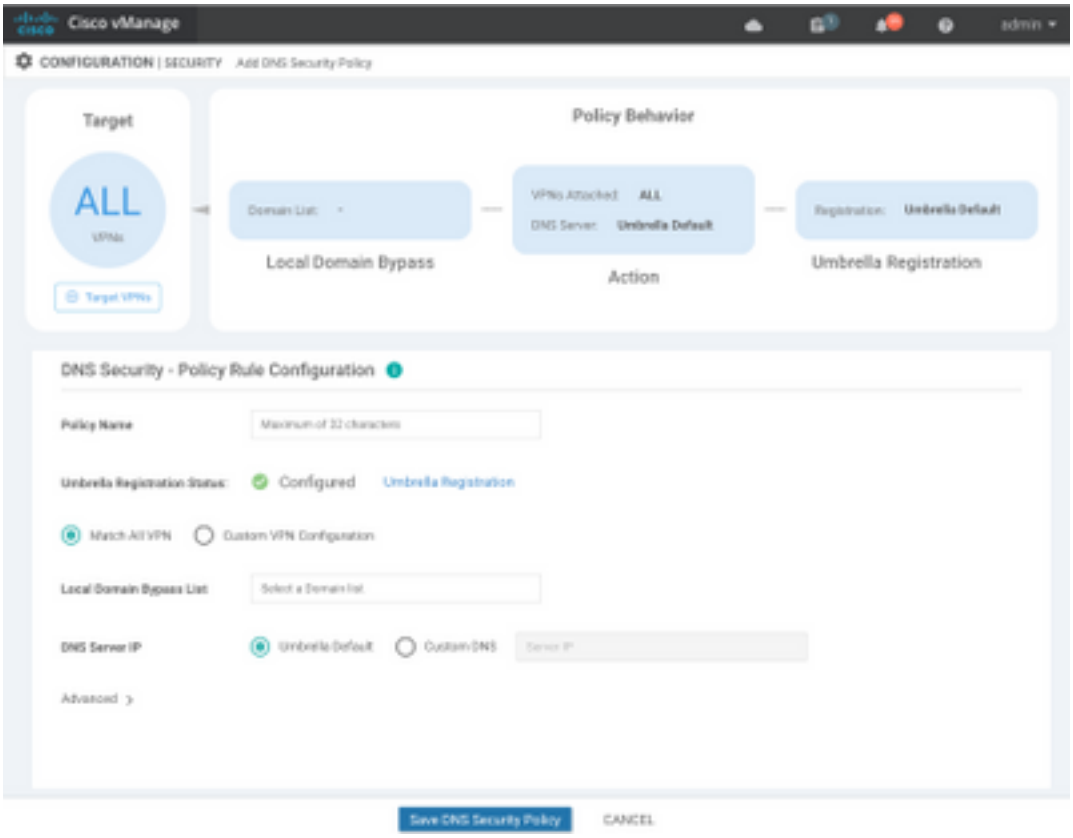
الخطوة 2. تحت **تشكيل > تأمين**، حدد **إضافة سياسة تأمين** ثم حدد سيناريو يناسب حالة الاستخدام الخاصة بك (على سبيل المثال، مخصص)، كما هو موضح في الصورة:



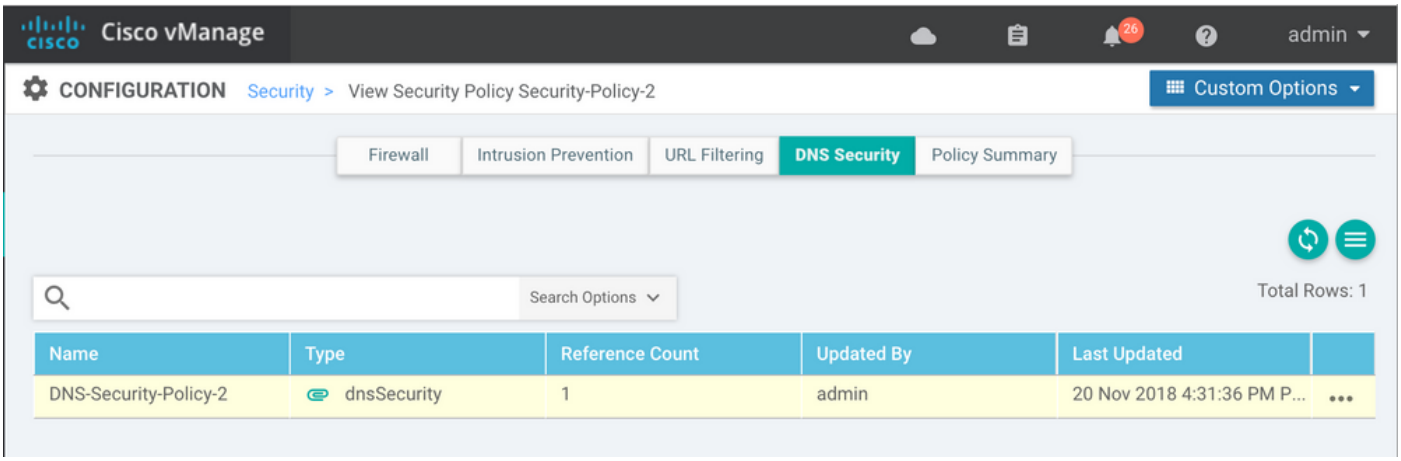
الخطوة 3. كما هو موضح في الصورة، انتقل إلى **أمان DNS**، وحدد **إضافة نهج أمان DNS**، ثم حدد **إنشاء جديد**.



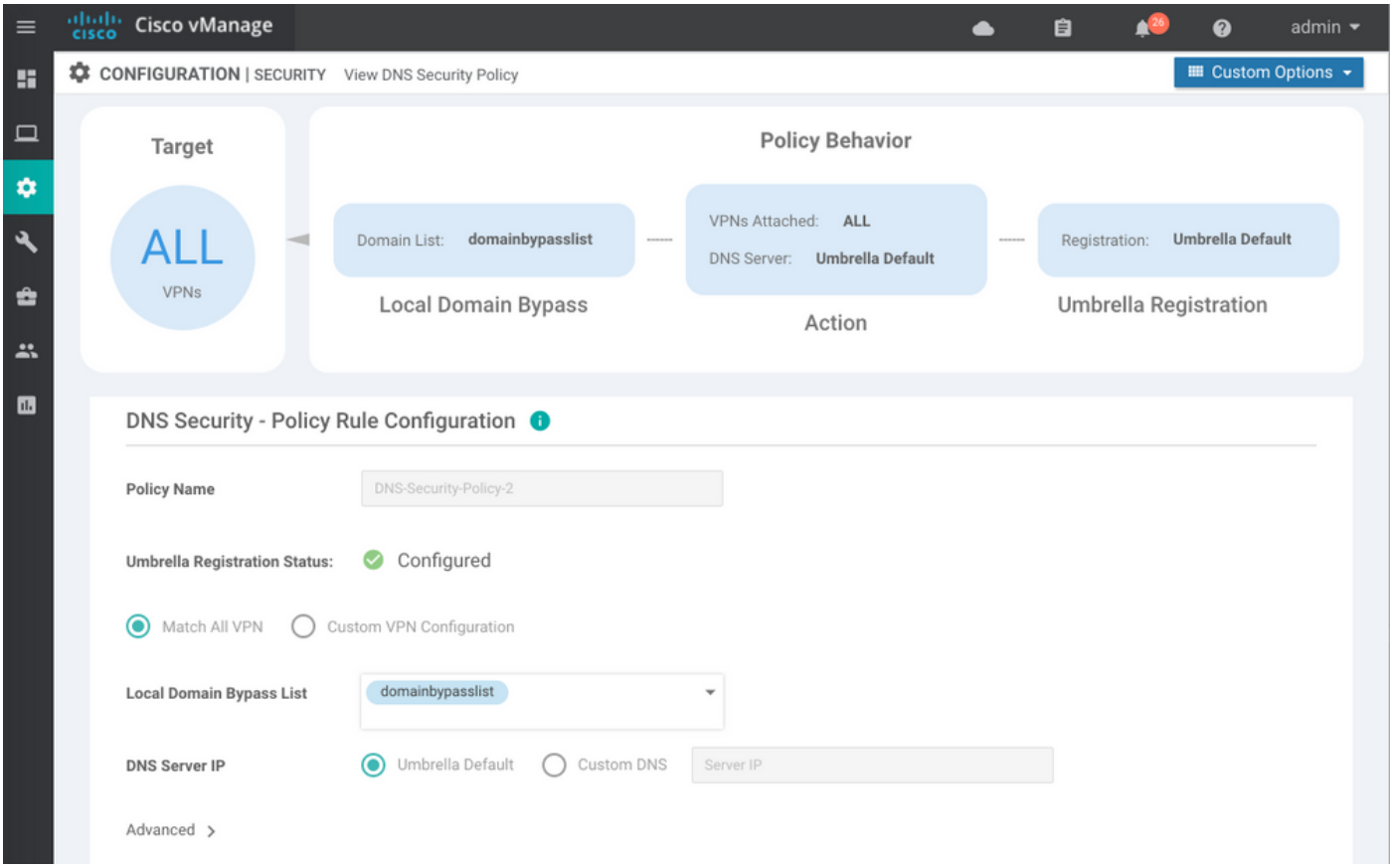
تظهر الشاشة شبيهة بالصورة المعروضة هنا:



الخطوة 4. هذه هي الصورة التي تظهر بها، بمجرد تكوينها.



الخطوة 5. انتقل إلى **..> عرض >** علامة التبويب **أمان DNS** في النهج الخاص بك، يمكنك مشاهدة تكوين مشابه لهذه الصورة:

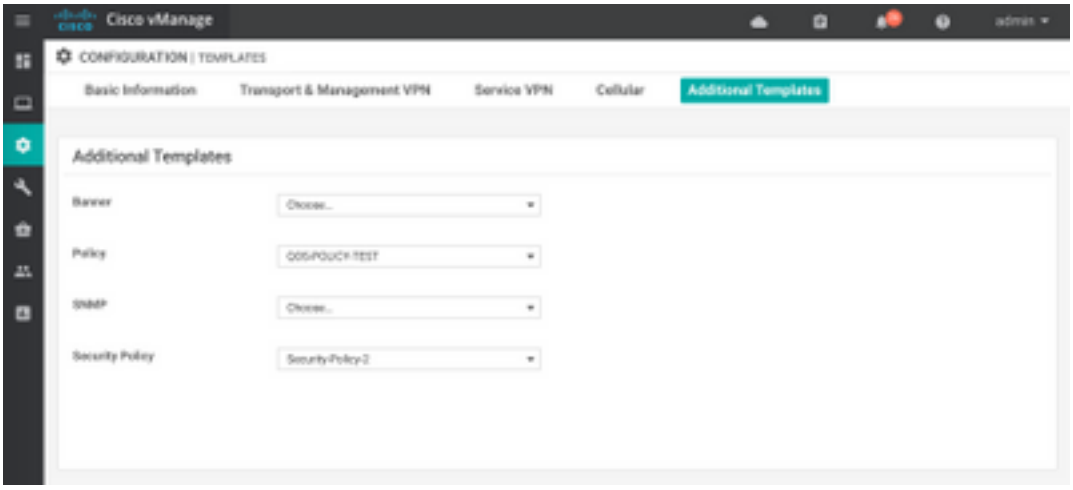


تذكر أن "قائمة تجاوز المجال المحلي" هي قائمة بالمجالات التي لا يقوم الموجه بإعادة توجيه طلبات DNS لها إلى سحابة Umbrella ويرسل طلب DNS إلى خادم DNS محدد (خادم DNS الموجود داخل شبكة المؤسسة)، وهذا ليس إستثناء من سياسات أمان Umbrella. من أجل "الكشف عن الهوية" عن بعض المجالات من الفئة المحددة، يوصى بتكوين الاستباعاد على مدخل تكوين Umbrella بدلا من ذلك.

أيضا، أنت يستطيع حددت **معاينة** in order to فهمت كيف التشكيل يظهر في 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
```

الخطوة 6. يجب الآن الإشارة إلى النهج في قالب الجهاز. تحت **تشكيل > قوالب**، حدد قالب التكوين الخاص بك وأرجع إليه في قسم **قوالب إضافية** كما هو موضح في الصورة.



الخطوة 7. تطبيق القالب على الجهاز.

التحقق من الصحة واستكشاف الأخطاء وإصلاحها

أستخدم هذا القسم للتأكد من أن التكوين لديك يعمل بشكل صحيح واستكشاف أخطائه وإصلاحها.

التحقق من العميل

من عميل يجلس خلف خادم cEdge، يمكنك التحقق مما إذا كانت Umbrella تعمل بشكل صحيح عند إستعراض مواقع الاختبار هذه:

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

لمزيد من التفاصيل، ارجع إلى كيفية: الاختبار بنجاح للتأكد من تشغيل Umbrella بشكل صحيح

التحقق من الخادم cEdge

كما يمكن إجراء التحقق من الصحة واستكشاف الأخطاء وإصلاحها على الخادم نفسه. بصفة عامة، يشبه إجراءات أستكشاف أخطاء برنامج Cisco IOS-XE وإصلاحها والتي يمكن العثور عليها في الفصل 2 Cisco Umbrella Integration في 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.

بعض الأوامر المفيدة للتحقق:

الخطوة 1. تحقق من تقديم خريطة المعلمة في تكوين cEdge على الجهاز:

```
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
!
```

الحظ أنه لا يمكن العثور على مرجع إلى خريطة المعلمة هذه على الواجهة عند إستخدامه لمشاهدتها على Cisco IOS-XE.

وذلك نظرا لتطبيق خريطة المعلمة على VRFs وليس على الواجهات، يمكنك التحقق منها هنا:

```
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
```

وبالإضافة إلى ذلك، يمكن إستخدام هذا الأمر للحصول على معلومات تفصيلية:

```
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


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

الخطوة 2. تحقق من تسجيل الجهاز بنجاح مع سحابة أمان DNS Umbrella.

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

الخطوة 3. فيما يلي كيفية التحقق من إحصائيات إعادة توجيه DNS المظلة.

```
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
```

الخطوة 4. تحقق من إمكانية الوصول إلى محلل DNS باستخدام الأدوات العامة لاستكشاف الأخطاء وإصلاحها مثل ping و traceroute.

الخطوة 5. يمكنك أيضا إستخدام التقاط الحزمة المضمنة من Cisco IOS-XE لتنفيذ التقاط حزم DNS من cEdge.

ارجع إلى دليل التكوين للحصول على التفاصيل: 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.

فهم تنفيذ Umbrella EDNS

بمجرد التقاط حزمة، تأكد من إعادة توجيه استعلامات DNS بشكل صحيح إلى محولات DNS (آلية الصحيحة EDNS0 باستخدام معلومات 208.67.220.220 و 208.67.222.222 Umbrella: الامتداد ل DNS). باستخدام كامل فحص طبقة SD-WAN Umbrella DNS، يتضمن جهاز cEdge خيارات END0 عندما يرسل استعلامات DNS إلى حلول DNS Umbrella. تتضمن هذه الملحقات إستقبال معرف الجهاز Device Id من Umbrella ومعرف المؤسسة ل Umbrella لتحديد السياسة الصحيحة التي يجب إستخدامها عند الإجابة على استعلام DNS. هنا مثال من ال EDNS0 رطب تنسيق:

فيما يلي تصنيف الخيارات:

وصف RDATA:

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

خيار عنوان IP البعيد ل RDATA:

```
0x4f444e53: MGGIC = 'ODNS'
0x00      : Version
```

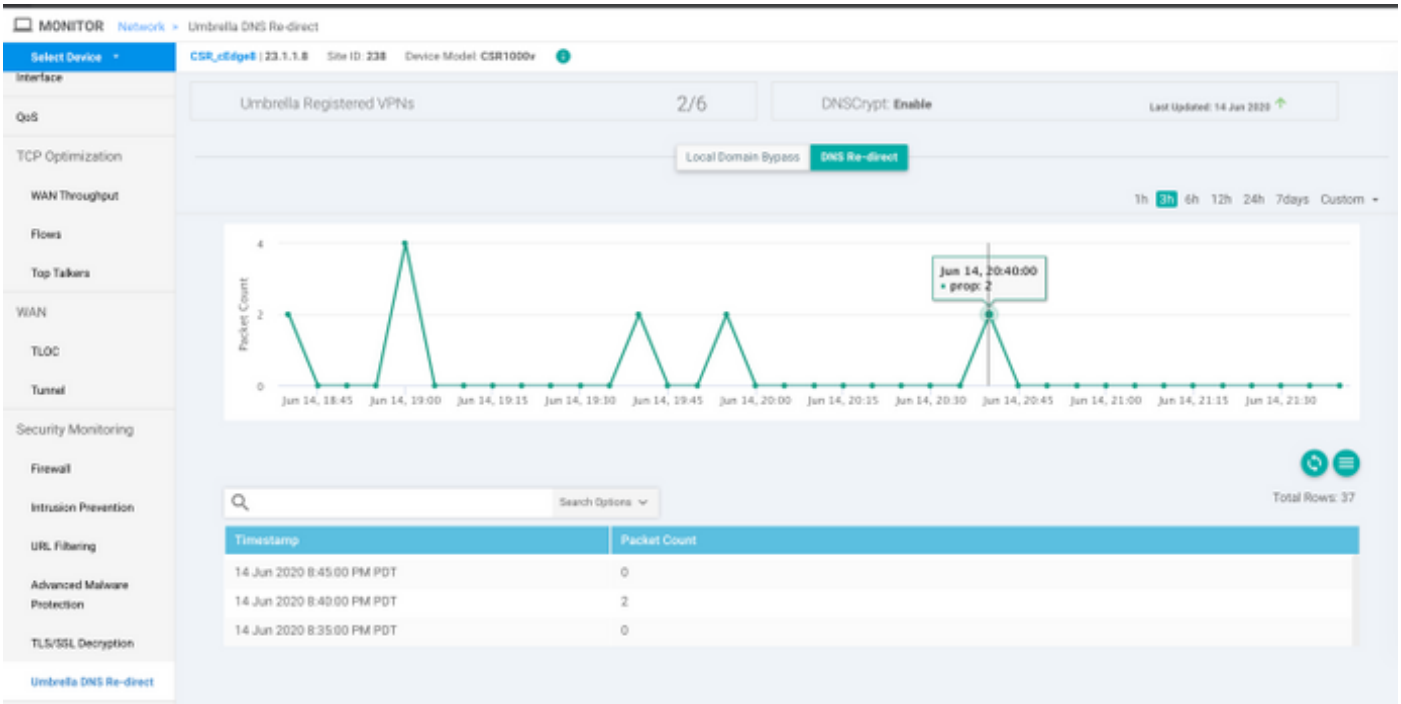
```
0x00      : Flags
0x08      : Organization ID Required
0x00225487: Organization ID
0x10 type : Remote IPv4
0x0b010103: Remote IP Address = 11.1.1.3
```

تحقق من صحة معرف الجهاز وتأكد من تطابق معرف المؤسسة مع حساب Umbrella باستخدام مدخل Umbrella.

> **ملاحظة**: مع تمكين تشفير DNSCrypt، يتم تشفير استعلامات DNS. إذا كانت الحزمة تظهر حزمة DNScrypt تنتقل إلى محلل المظلة ولكن لا توجد حركة مرور إرجاع، فحاول تعطيل DNSCrypt لمعرفة ما إذا كانت هذه هي المشكلة.

التحقق من ذلك على لوحة المعلومات vManage

يمكن عرض أي حركة مرور موجهة ل Cisco Umbrella من لوحة معلومات vManage. ويمكن عرضها تحت **الشاشة > الشبكة > إعادة توجيه DNS Umbrella**. انه صورة لهذه الصفحة:



التخزين المؤقت ل DNS

على موجه Cisco cEdge، لا تتطابق عمليات تجاوز المجال المحلية في بعض الأحيان. يحدث هذا عند وجود ذاكرة تخزين مؤقت مشتركة في الجهاز المضيف/العميل. على سبيل المثال، إذا تم تكوين تجاوز المجال المحلي لمطابقة www.cisco.com وتجاوزه (**.*cisco.com**). في المرة الأولى، كان الاستعلام عن www.cisco.com الذي أرجع أيضا أسماء CDN ك CNAME، والتي تم تخزينها مؤقتا على العميل. كانت الاستعلامات التالية ل nslookup ل www.cisco.com هي التي تقوم بإرسال الاستعلامات فقط لمجال 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
```

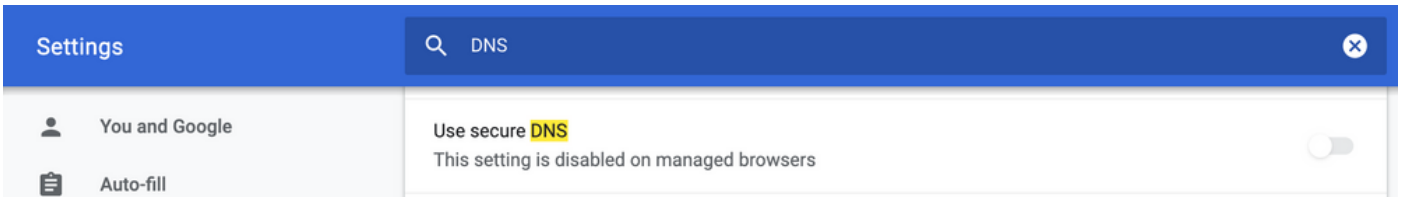
إذا عمل تجاوز المجال المحلي بشكل صحيح، ستزيد العدادات لإعادة توجيه OpenDNS المحلل. فيما يلي مخرج مختصر.

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

هذا يمكن أن يكون السبب، as to لما محلي domain overver ال يرى على المسجاح تخديد. عند مسح ذاكرة التخزين المؤقت على الجهاز المضيف/العميل، ستزى أن الاستعلامات تخرج بشكل صحيح.

DNS الآمن

تستخدم المستعرضات الحديثة مثل Google Chrome بدءا من الإصدار 83 نظام أسماء المجالات (DNS) الآمن عبر HTTPS (DoH) أو DNS عبر TLS (DoT). يمكن أن تجعل هذه الميزة قدرة أمان Umbrella DNS مستحيلة الاستخدام إذا لم يتم التخطيط لها بعناية. يمكن تعطيل DNS الآمن عبر السياسات المركزية وتعطيله بشكل افتراضي، على سبيل المثال، لأجهزة الكمبيوتر المدارة من فئة المؤسسات.



بالنسبة لأجهزة BYOD غير المدارة، توجد خيارات قليلة. الخيار الأول وهو حظر منفذ TCP 853 الذي يتم إستخدامه من قبل DNS الآمن. يمكنك إستخدام جدار الحماية المستند إلى منطقة Cisco (ZBFW) لهذا الغرض. الخيار الثاني وهو تمكين حظر فئة "الوكيل/المجهول" على مدخل Umbrella. يمكنك العثور على المزيد من المعلومات حول هذا الموضوع هنا

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

القرار

وكما ترى، فإن التكامل مع سحابة أمان DNS Umbrella بسيط جدا من جانب CEdge ويمكن تنفيذه في غضون دقائق قليلة.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).