Configurer l'intégration avec Cisco Umbrella et résoudre les problèmes courants

Contenu

Introduction

Ce document décrit le logiciel SDWAN vManage/Cisco IOS®-XE intégré à la solution de sécurité DNS Cisco Umbrella. Cependant, il ne couvre pas la configuration des politiques Umbrella elle-même. Vous trouverez plus d'informations sur Cisco Umbrella ici ; https://docs.umbrella.com/deployment-umbrella/docs/welcome-to-cisco-umbrella.

> **Note**: Vous devez déjà avoir obtenu des abonnements Umbrella et obtenir le jeton Umbrella qui sera utilisé dans la configuration des routeurs cEdge. En savoir plus sur le jeton API : https://docs.umbrella.com/umbrella-api/docs/overview2.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- vManage 18.4.0
- Routeur SDWAN Cisco IOS®-XE exécutant (cEdge) 16.9.3

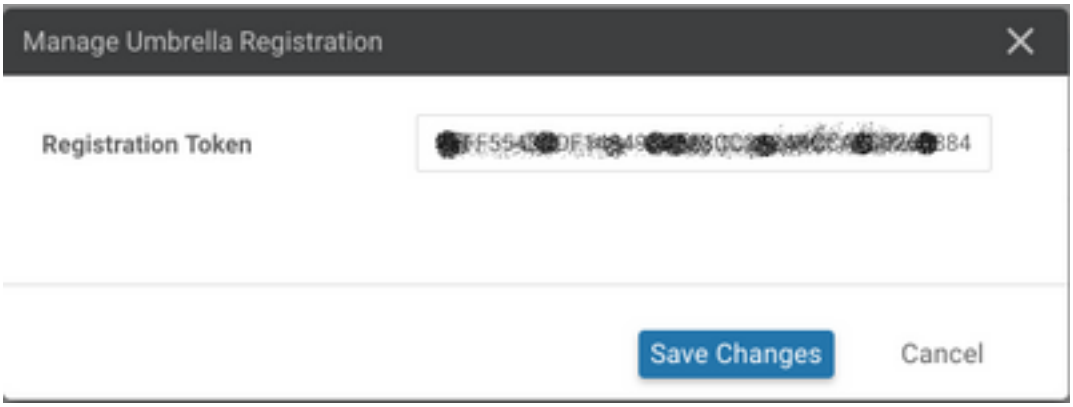
The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

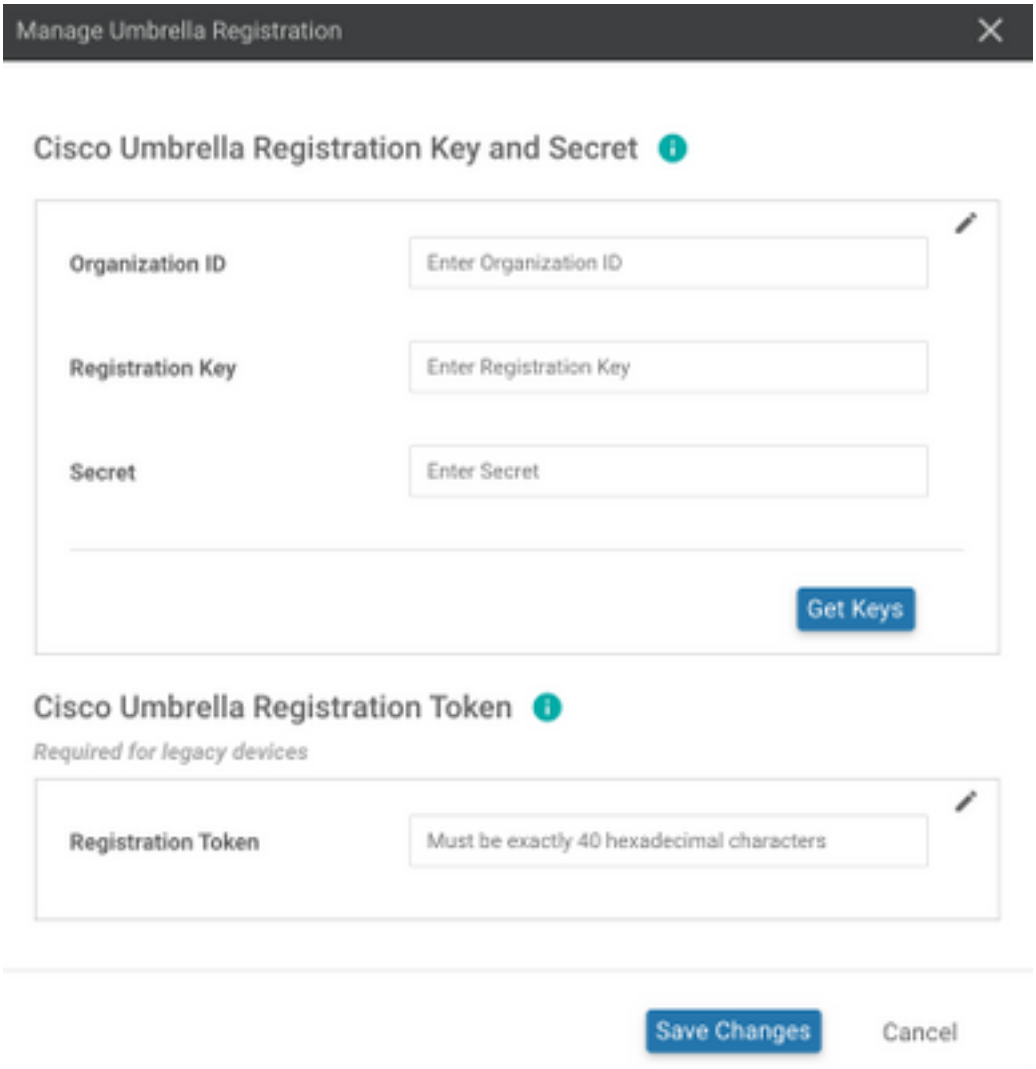
Configuration

Afin de configurer votre intégration cEdge avec Cisco Umbrella, vous devez effectuer un ensemble d'étapes simples sur vManage :

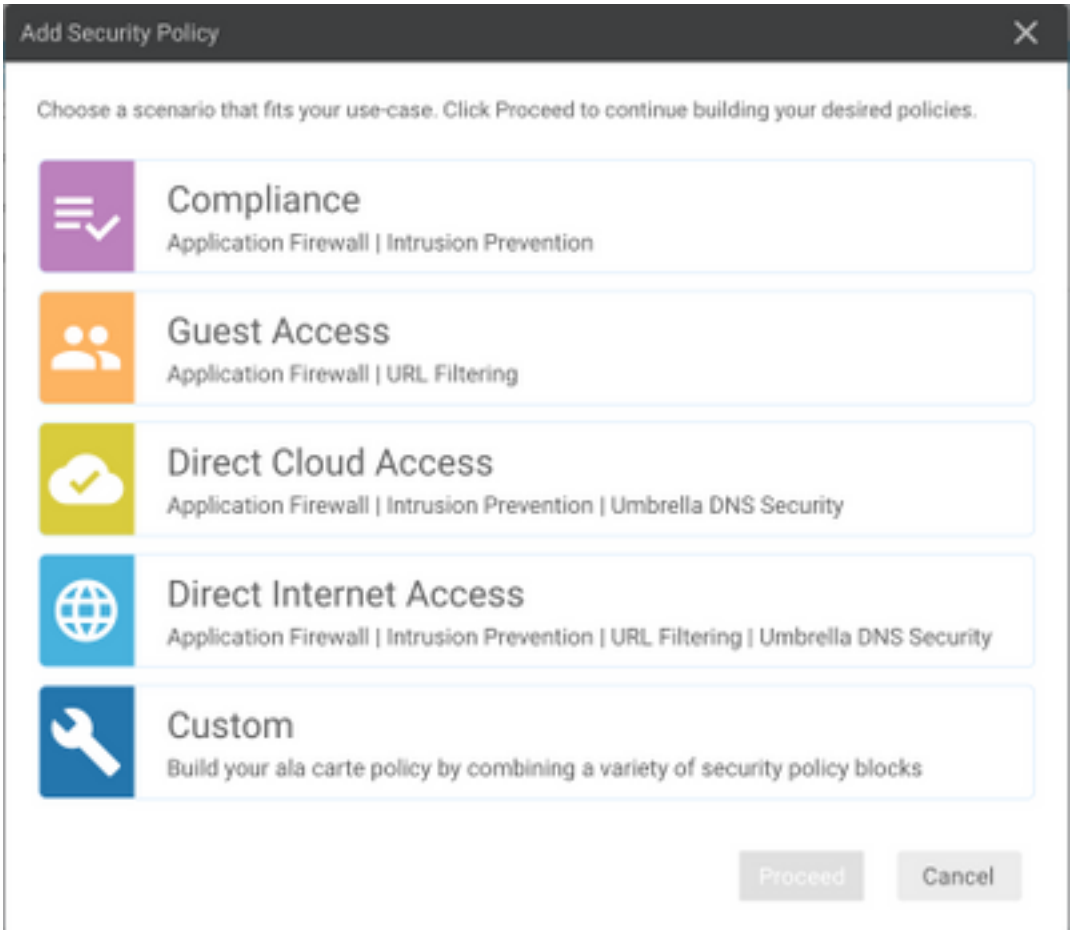
Étape 1. Sous **Configuration > Security**, sélectionnez **Custom Options** dans le coin supérieur droit, puis sélectionnez **Umbrella API token**. Saisissez votre jeton d'enregistrement Umbrella, comme illustré sur l'image :



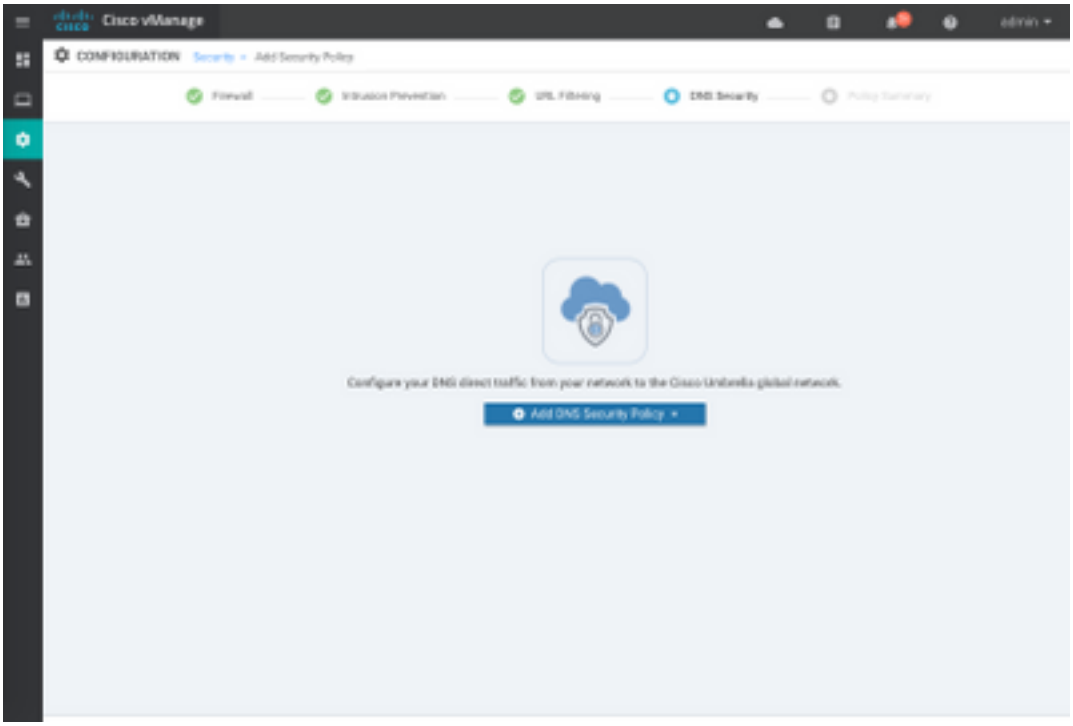
Sinon, à partir de la version 20.1.1 du logiciel vManage, vous pouvez spécifier l'ID d'organisation, la clé d'enregistrement et le secret. Ces paramètres peuvent être récupérés automatiquement si vous avez configuré vos informations d'identification de compte Smart sous **Administration > Settings > Smart Account Credential**.



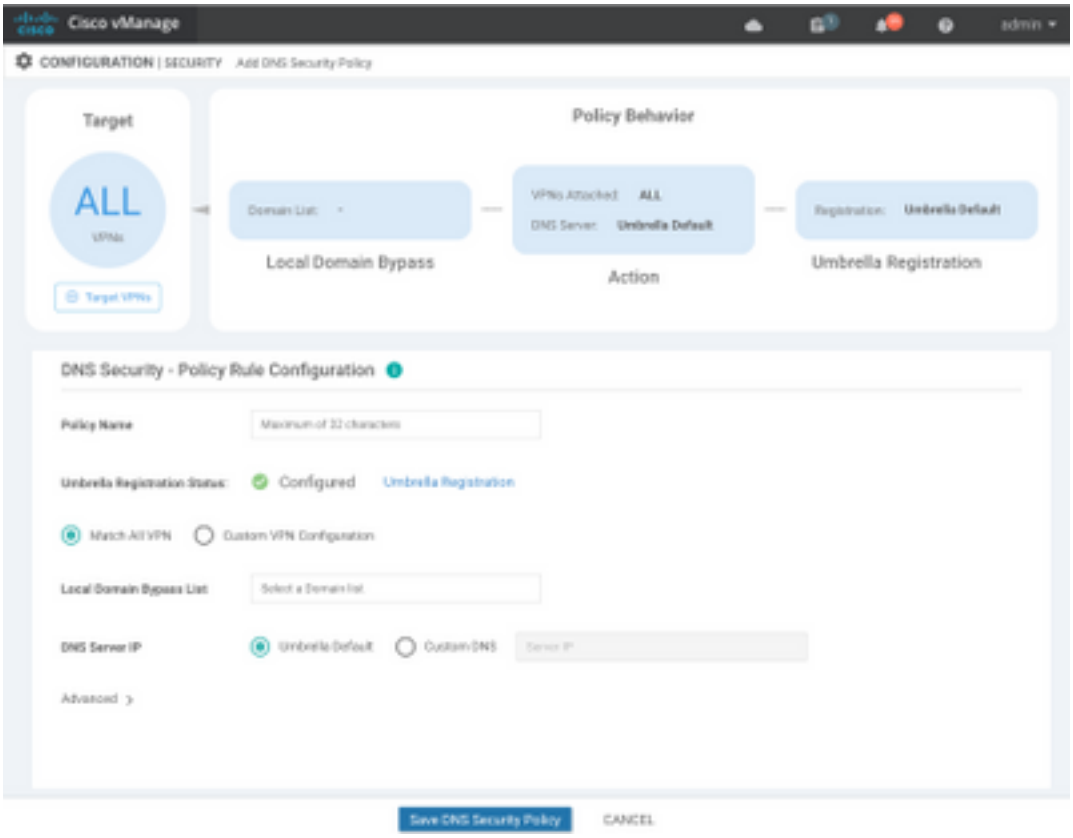
Étape 2. Sous **Configuration > Security**, sélectionnez **Add Security Policy**, puis sélectionnez un scénario correspondant à votre cas d'utilisation (personnalisé, par exemple), comme illustré dans l'image :



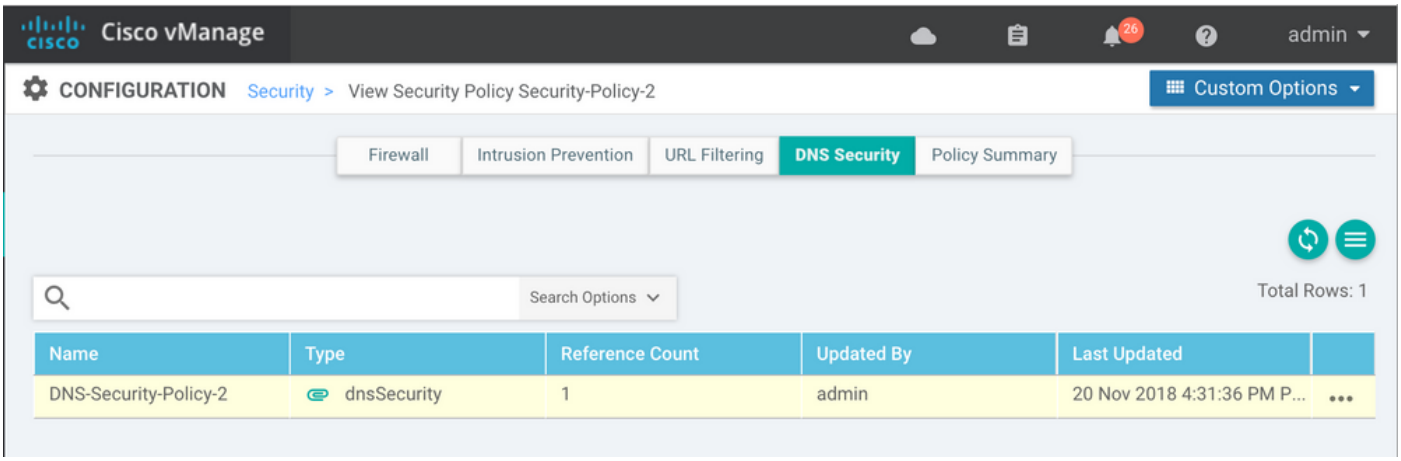
Étape 3. Comme l'illustre l'image, accédez à **Sécurité DNS**, sélectionnez **Ajouter une stratégie de sécurité DNS**, puis sélectionnez **Créer.**



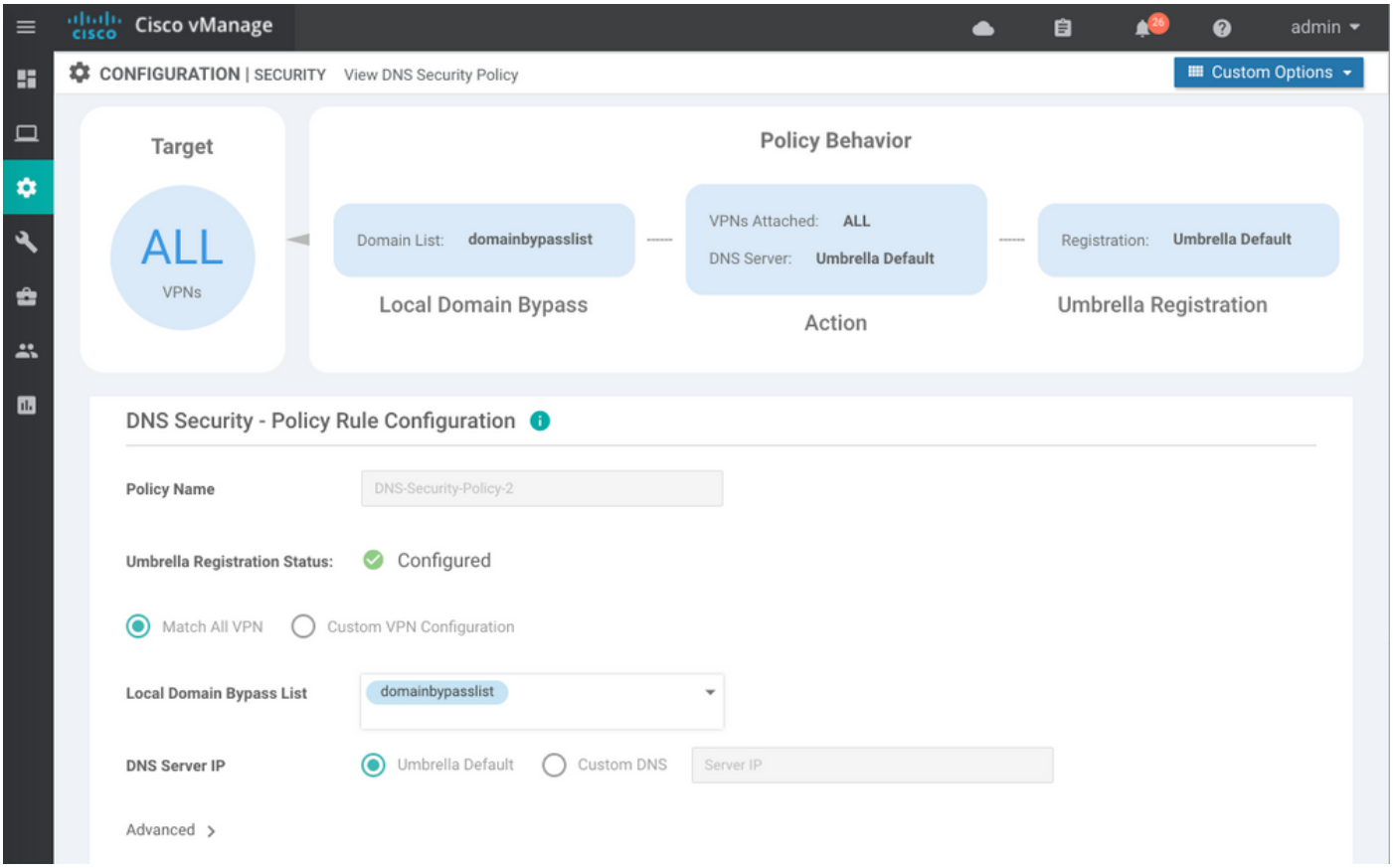
L'écran s'affiche comme l'image ci-dessous :



Étape 4. Il s'agit de l'image de son apparence, une fois configurée.



Étape 5. Accédez à **...> Affichage >** onglet **Sécurité DNS** de votre stratégie. Une configuration similaire à cette image s'affiche :

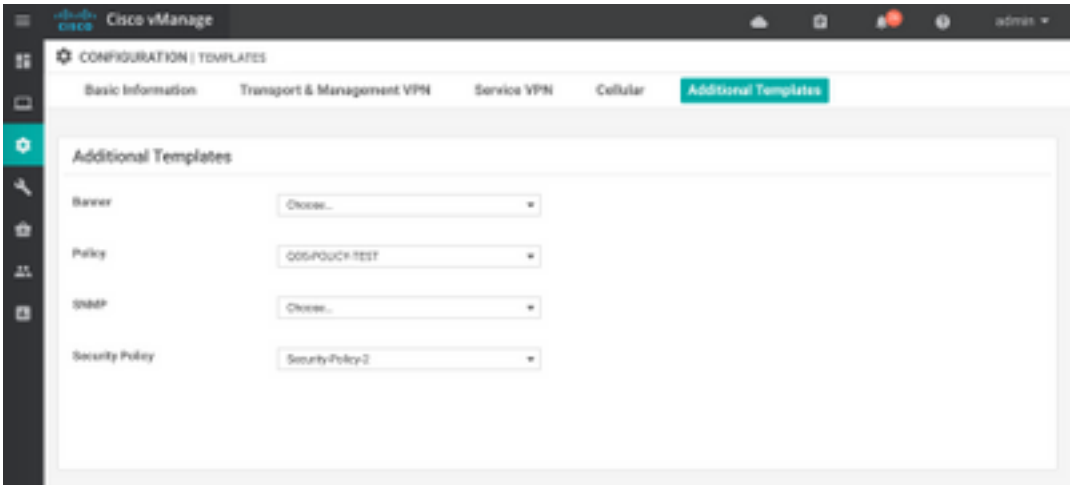


Gardez à l'esprit que « Local Domain Bypass List » est une liste de domaines pour lesquels le routeur ne redirige pas les requêtes DNS vers le nuage Umbrella et envoie la requête DNS à un serveur DNS spécifique (serveur DNS situé dans le réseau de l'entreprise), ceci n'est pas exclu des stratégies de sécurité Umbrella. Afin de « blanchir » certains domaines de la catégorie spécifique, il est recommandé de configurer l'exclusion sur le portail de configuration Umbrella à la place.

Vous pouvez également sélectionner **Aperçu** afin de comprendre l'aspect de la configuration dans l'interface de ligne de commande :

```
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
```

Étape 6. Vous devez maintenant référencer la stratégie dans le modèle de périphérique. Sous **Configuration > Modèles**, sélectionnez votre modèle de configuration et référencez-le dans la section **Modèles supplémentaires** comme indiqué dans l'image.



Étape 7. Appliquez le modèle au périphérique.

Vérifiez et dépannez

Utilisez cette section pour vérifier que votre configuration fonctionne correctement et pour résoudre les problèmes.

Vérification du client

Àpartir d'un client situé derrière cEdge, vous pouvez vérifier si Umbrella fonctionne correctement lorsque vous parcourez ces sites de test :

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

Pour plus d'informations, reportez-vous à Comment : Test réussi pour vous assurer que vous exécutez Umbrella correctement

Vérification cEdge

La vérification et le dépannage peuvent également être effectués sur cEdge lui-même. En général, il est similaire aux procédures de dépannage d'intégration du logiciel Cisco IOS-XE que vous trouverez au chapitre 2 du Guide de configuration de Cisco Umbrella Integration sur les routeurs ISR de la gamme Cisco 4000 : 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.

Peu de commandes utiles à vérifier :

Étape 1. Vérifiez que le paramètre-map est présenté dans la configuration cEdge sur le périphérique :

```
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
!
```

Notez que vous ne trouvez pas de référence à ce paramètre-map sur l'interface lorsque vous vous habituez à le voir sur Cisco IOS-XE.

Ceci est dû au fait que le paramètre-map est appliqué aux VRF et non aux interfaces, vous pouvez le vérifier ici :

```
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
```

En outre, vous pouvez utiliser cette commande pour obtenir des informations détaillées :

```
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


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

Étape 2. Vérifiez que le périphérique est enregistré avec succès dans le nuage de sécurité DNS Umbrella.

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

Étape 3. Voici comment vérifier les statistiques de redirection DNS parapluie.

```
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
```

Étape 4. Vérifiez que le résolveur DNS est accessible à l'aide d'outils génériques afin de dépanner comme ping et traceroute.

Étape 5. Vous pouvez également utiliser la capture de paquets intégrée de Cisco IOS-XE afin d'effectuer la capture de paquets DNS à partir de cEdge.

Reportez-vous au guide de configuration pour plus de détails : [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)

Comprendre l'implémentation EDNS de l'Umbrella

Une fois qu'une capture de paquets est prise, assurez-vous que les requêtes DNS sont correctement redirigées vers les résolveurs DNS Umbrella : 208.67.222.222 et 208.67.220.220 avec les informations EDNS0 (Extension Mechanism for DNS) correctes. Avec l'intégration de l'inspection de couche DNS SD-WAN Umbrella, le périphérique cEdge inclut des options ENDS0 lorsqu'il envoie des requêtes DNS aux résolutions DNS Umbrella. Ces extensions incluent l'ID de périphérique que cEdge reçoit d'Umbrella et l'ID d'organisation pour Umbrella afin d'identifier la stratégie correcte à utiliser lorsque vous répondez à la requête DNS. Voici un exemple du format de paquet EDNS0 :

Voici la répartition des options :

Description RDATA :

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

Option d'adresse IP distante RDATA :

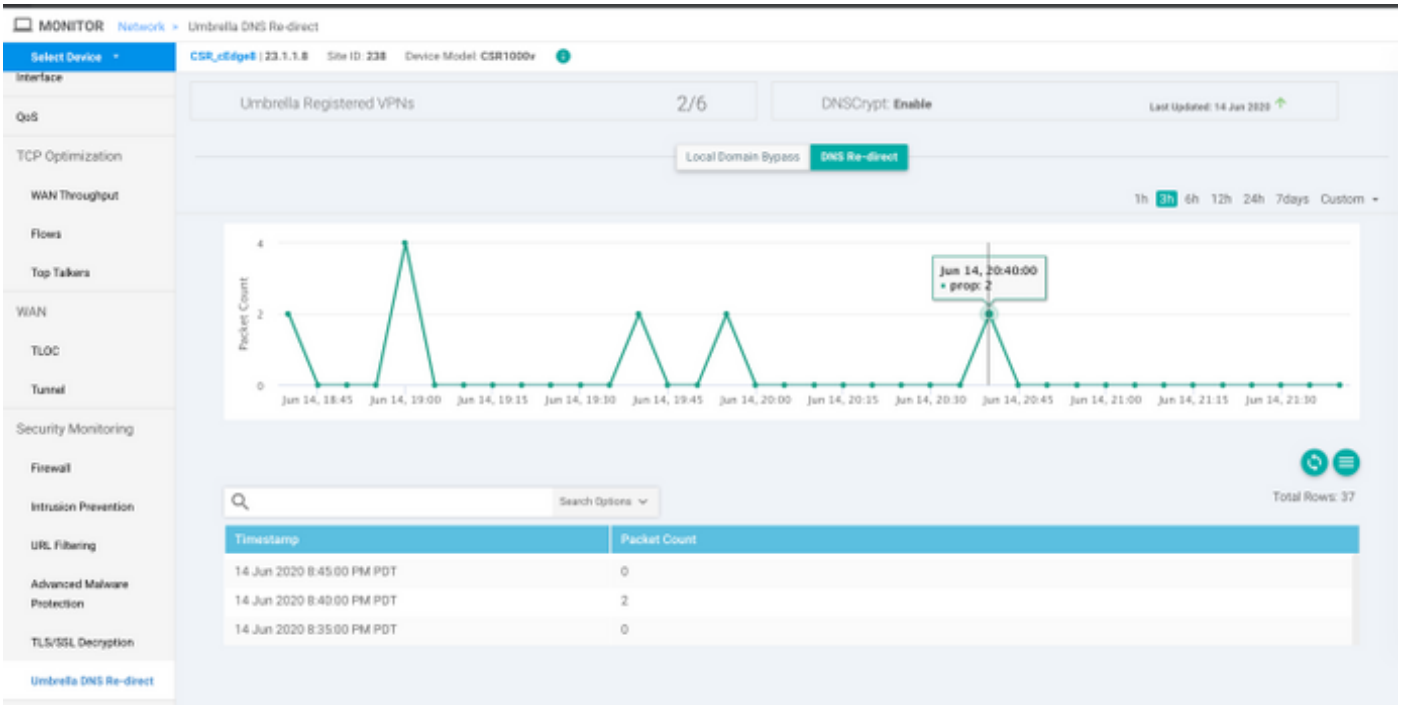
```
0x4f444e53: MGGIC = 'ODNS'
0x00      : Version
0x00      : Flags
0x08      : Organization ID Required
0x00225487: Organization ID
0x10 type : Remote IPv4
0x0b010103: Remote IP Address = 11.1.1.3
```

Vérifiez et assurez-vous que l'ID de périphérique est correct et que l'ID d'organisation correspond au compte Umbrella avec l'utilisation du portail Umbrella.

> **Note**: Lorsque DNSCrypt est activé, les requêtes DNS sont chiffrées. Si les captures de paquet montrent le paquet DNScrypt allant au résolveur Umbrella mais qu'il n'y a pas de trafic de retour, essayez de désactiver DNSCrypt pour voir si c'est le problème.

Vérifier sur le tableau de bord vManage

Tout trafic dirigé par Cisco Umbrella peut être consulté à partir du tableau de bord vManage. Il peut être affiché sous **Monitor > Network > Umbrella DNS Re-direct**. Voici l'image de cette page :



Cache DNS

Sur un routeur Cisco cEdge, les indicateurs de contournement de domaine local ne correspondent parfois pas. Cela se produit lorsqu'une mise en cache est impliquée dans la machine/le client hôte. Par exemple, si le contournement de domaine local est configuré pour correspondre et contourner www.cisco.com (**.*cisco.com**). La première fois, la requête était pour www.cisco.com qui retournait également les noms CDN sous forme de CNAME, qui étaient mis en cache sur le client. Les requêtes subséquentes pour nslookup pour www.cisco.com devaient envoyer uniquement les requêtes pour le domaine 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
```

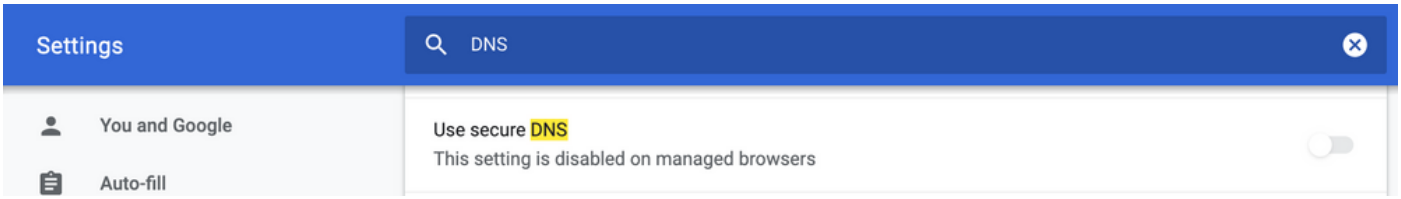
Si le contournement de domaine local fonctionne correctement, vous verrez que les compteurs augmentent pour la redirection OpenDNS de l'analyseur. Voici un résultat abrégé.

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

Ceci peut être la raison pour laquelle le contournement du domaine local n'est pas vu sur le routeur. Lorsque vous effacez le cache sur l'ordinateur hôte/client, vous voyez que les requêtes sortent correctement.

DNS sécurisé

Les navigateurs modernes comme Google Chrome à partir de la version 83 utilisent Secure DNS également appelé DNS sur HTTPS (DoH) ou DNS sur TLS (DoT). Cette fonctionnalité peut rendre la fonctionnalité de sécurité DNS Umbrella impossible à utiliser si elle n'est pas planifiée avec soin. Le DNS sécurisé peut être désactivé via des stratégies centralisées et désactivé par défaut, par exemple, pour les ordinateurs gérés par l'entreprise.



Pour les périphériques BYOD non gérés, il existe peu d'options. La première option consiste à bloquer le port TCP 853 utilisé par Secure DNS. Vous pouvez utiliser Cisco Zone Based Firewall (ZBFW) à cette fin. La deuxième option consisterait à activer le blocage de catégorie « Proxy/Anonymizer » sur le portail Umbrella. Vous trouverez plus d'informations ici

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

Conclusion

Comme vous pouvez le voir, l'intégration avec le nuage de sécurité DNS Umbrella est très simple

du côté de cEdge et peut être effectuée en quelques minutes.