Cisco Umbrella

Vous pouvez configurer le périphérique pour rediriger les requêtes DNS vers Cisco Umbrella, afin que votre politique FQDN définie dans Cisco Umbrella puisse être appliquée aux connexions des utilisateurs. Les rubriques suivantes expliquent comment configurer Cisco Umbrella Connector pour intégrer l'appareil à Cisco Umbrella.

À propos de Cisco Umbrella Connector

Si vous utilisez Cisco Umbrella, vous pouvez configurer Cisco Umbrella Connector pour rediriger les requêtes DNS vers Cisco Umbrella. Cela permet à Cisco Umbrella d'identifier les demandes adressées à des noms de domaine non autorisés ou douteux et d'appliquer votre politique de sécurité basée sur DNS.

Le connecteur Cisco Umbrella fait partie de l'inspection DNS du système. Si votre liste de politiques d'inspection DNS existante décide de bloquer ou d'abandonner une demande en fonction de vos paramètres d'inspection DNS, la demande n'est pas transmise à Cisco Umbrella. Ainsi, vous avez deux lignes de protection : votre politique d'inspection DNS locale et votre politique basée sur le nuage Cisco Umbrella.

Lors de la redirection des demandes de recherche DNS vers Cisco Umbrella, le connecteur Cisco Umbrella ajoute un enregistrement EDNS (Extension mécanismes for DNS). Un enregistrement EDNS comprend les renseignements sur l'identifiant du périphérique , l'ID de l'organisation et l'adresse IP du client. Votre politique en nuage peut utiliser ces critères pour contrôler l'accès en plus de la réputation du nom de domaine complet. Vous pouvez également choisir de chiffrer la requête DNS à l'aide de DNSCrypt pour assurer la confidentialité des noms d'utilisateurs et des adresses IP internes.

Politique de sécurité entreprise Cisco Umbrella

Dans votre politique Cisco Umbrella Enterprise Security basée sur le nuage, vous pouvez contrôler l'accès en fonction de la réputation du nom de domaine complet (FQDN) dans la demande de recherche DNS. Votre politique de sécurité d'entreprise peut appliquer l'une des actions suivantes :

- Autoriser : si vous n'avez aucune règle de blocage pour un nom de domaine complet et que Cisco Umbrella détermine qu'il appartient à un site non malveillant, l'adresse IP réelle du site est renvoyée. Il s'agit du comportement normal de recherche DNS.
- Proxy : si vous n'avez aucune règle de blocage pour un nom de domaine complet et que Cisco Umbrella détermine qu'il appartient à un site suspect, la réponse DNS renvoie l'adresse IP du serveur proxy intelligent Cisco Umbrella. Le serveur proxy peut ensuite inspecter la connexion HTTP et appliquer le filtrage d'URL. Vous devez vous assurer que le proxy intelligent est activé à partir du tableau de bord Cisco Umbrella (**Security Setting (Paramètre de sécurité)** > **Enable Intelligent Proxy (Activer le proxy intelligent)**).
- Blocage : si vous bloquez explicitement un nom de domaine complet ou si Cisco Umbrella détermine qu'il appartient à un site malveillant, la réponse DNS renvoie l'adresse IP de la page de destination du nuage Cisco Umbrella pour les connexions bloquées.

Enregistrement de Cisco Umbrella

Lorsque vous configurez Cisco Umbrella Connector sur un périphérique, il s'enregistre auprès de Cisco Umbrella dans le nuage. Le processus d'enregistrement attribue un ID de périphérique unique, qui identifie l'un des éléments suivants :

- Un périphérique autonome en mode contexte unique.
- Une paire à haute disponibilité en mode contexte unique.
- Une grappe en mode contexte unique.
- Un contexte de sécurité dans un périphérique autonome multi-contexte.
- Un contexte de sécurité d'une paire à haute disponibilité
- Un contexte de sécurité d'une grappe.

Une fois enregistrés, les détails du périphérique s'affichent dans le tableau de bord de Cisco Umbrella. Vous pouvez ensuite modifier la politique associée à un périphérique. Lors de l'enregistrement, la politique que vous spécifiez dans la configuration est utilisée ou la politique par défaut est attribuée. Vous pouvez affecter la même politique Cisco Umbrella à plusieurs périphériques. Si vous spécifiez la politique, l'ID de périphérique que vous recevez est différent de ce que vous obtiendriez si vous ne spécifiez pas de politique.

Exigences de licence pour Cisco Umbrella Connector

Pour utiliser le Cisco Umbrella Connector, vous devez avoir une licence 3DES. Si vous utilisez Smart Licensing, votre compte doit être activé pour la fonctionnalité soumise au contrôle des exportations.

Le portail Cisco Umbrella comporte des exigences de licence distinctes.

Lignes directrices et limites relatives à Cisco Umbrella

Mode contextuel

- En mode contexte multiple, vous configurez Cisco Umbrella Connector dans chaque contexte. Chaque contexte possède un ID de périphérique distinct et est représenté comme un périphérique distinct dans le tableau de bord de Cisco Umbrella Connector. Le nom du périphérique est le nom d'hôte configuré dans le contexte, plus le modèle matériel, plus le nom du contexte. Par exemple, CiscoASA-ASA5515-Context1.

Basculement

- L'unité active dans la paire à haute disponibilité enregistre la paire en tant qu'unité unique auprès de Cisco Umbrella. Les deux homologues utilisent le même ID de périphérique, qui est composé de leurs numéros de série : *numéro de série principal_numéro de série secondaire*. Pour le mode de contexte multiple, chaque paire de contextes de sécurité est considérée comme une unité unique. Vous devez configurer la haute disponibilité, et les unités doivent avoir formé avec succès un groupe de haute disponibilité (même si le périphérique de secours est actuellement en état d'échec) avant d'activer Cisco Umbrella, sinon l'enregistrement échouera.

Grappe

- L'unité de contrôle de grappe enregistre la grappe en tant qu'unité unique auprès de Cisco Umbrella. Tous les homologues utilisent le même ID de périphérique. Pour le mode de contexte multiple, un contexte de sécurité dans la grappe est considéré comme une unité unique pour tous les homologues.

Lignes directrices supplémentaires

- La redirection vers Cisco Umbrella est effectuée pour les demandes DNS dans le trafic de transit uniquement. Les requêtes DNS que le système lui-même lance ne sont jamais redirigées vers Cisco Umbrella. Par exemple, les règles de contrôle d'accès basées sur le nom de domaine complet ne sont jamais résolues en fonction de la politique Cisco Umbrella, ni les noms de domaine complets utilisés dans d'autres commandes ou paramètres de configuration.
- Cisco Umbrella Connector fonctionne sur toute demande DNS dans le trafic de transit. Cependant, les actions de blocage et de serveur proxy ne sont effectives que si la réponse DNS est ensuite utilisée pour les connexions HTTP/HTTPS, car l'adresse IP renvoyée concerne un site Web. Toutes les adresses bloquées ou relayées par proxy pour les connexions non HTTP/HTTPS échoueront ou se termineront de manière erronée. Par exemple, envoyer une requête ping à un nom de domaine complet bloqué entraînerait l'envoi d'une requête ping au serveur qui héberge la page de blocage Cisco Umbrella.

Remarque Cisco Umbrella tente d'identifier intelligemment les noms de domaine complets qui pourraient être non HTTP/HTTPS et ne renvoie pas l'adresse IP au proxy intelligent pour ces noms de domaine complets dans le cas des noms de domaine relayés par proxy.

- Le système envoie le trafic DNS/UDP uniquement à Cisco Umbrella. Si vous activez l'inspection DNS/TCP, le système n'envoie aucune demande DNS/TCP à Cisco Umbrella. Cependant, les requêtes DNS/TCP n'incrémentent pas le compteur de contournement Cisco Umbrella.
- Si vous activez DNScrypt pour l'inspection Cisco Umbrella, le système utilise UDP/443 pour la session chiffrée. Vous devez inclure UDP/443 avec UDP/53 dans la carte de trafic qui applique l'inspection DNS pour Cisco Umbrella pour que DNScrypt fonctionne correctement. UDP/443 et UDP/53 sont inclus dans la carte de trafic d'inspection par défaut pour DNS, mais si vous créez une carte personnalisée, veillez à définir une liste de contrôle d'accès qui inclut les deux ports pour la carte de correspondance.
- DNScrypt utilise IPv4 uniquement pour l'établissement de liaison de mise à jour de certificat. Cependant, DNScrypt chiffre le trafic IPv4 et IPv6.
- Il doit y avoir une route IPv4 vers Internet qui puisse atteindre api.umbrella.com et api.opendns.com (l'enregistrement utilise IPv4 uniquement). Vous devez également avoir des routes vers les résolveurs DNS suivants, et vos règles d'accès doivent autoriser le trafic DNS vers ces hôtes. Ces routes peuvent passer par les interfaces de données ou l'interface de gestion ; toute route valide fonctionnera à la fois pour l'enregistrement et la résolution DNS. Les serveurs par défaut utilisés par le système sont indiqués ; vous pouvez utiliser les autres serveurs en configurant le résolveur dans les paramètres globaux de Cisco Umbrella.
  - 208.67.220.220 (par défaut du système pour IPv4)
  - 208.67.222.222
  - 2620:119:53::53 (par défaut du système pour IPv6)
  - 2620:119:35::35
- Le système ne prend pas en charge le service Cisco Umbrella FamilyShield. Si vous configurez les résolveurs FamilyShield, vous pourriez obtenir des résultats inattendus.
- Lors de l'évaluation du mode ouvert en cas d'échec, le système détermine si le résolveur Cisco Umbrella est en panne ou si un périphérique intermédiaire abandonne la demande ou la réponse DNS en fonction du temps écoulé depuis l'envoi de la demande en attente de la réponse. D'autres facteurs, tels que l'absence de voie de routage vers le résolveur Cisco Umbrella, ne sont pas pris en compte.
- Pour annuler l'enregistrement d'un appareil, supprimez d'abord la configuration Cisco Umbrella, puis supprimez l'appareil du tableau de bord Cisco Umbrella.
- Toute demande Web qui utilise des adresses IP au lieu de FQDN contournera Cisco Umbrella. En outre, si un client itinérant obtient une résolution DNS à partir d'une connexion WAN différente de celle qui passe par un périphérique compatible avec Cisco Umbrella, les connexions qui utilisent ces résolutions contournent Cisco Umbrella.
- Si un utilisateur dispose d'un serveur proxy HTTP, le serveur proxy peut effectuer une résolution DNS, et les résolutions ne passeront pas par Cisco Umbrella.
- Les NAT DNS46 et DNS64 ne sont pas prises en charge. Vous ne pouvez pas traduire les demandes DNS entre l'adressage IPv4 et IPv6.
- L'enregistrement EDNS comprendra les adresses d'hôte IPv4 et IPv6.
- Si le client utilise DNS sur HTTPS, le service de sécurité en nuage n'inspectera pas le trafic DNS et HTTP/HTTPS.

Configurer le connecteur Cisco Umbrella

Vous pouvez configurer l'appareil pour interagir avec Cisco Umbrella dans le cloud. Le système redirige les demandes de recherche DNS vers Cisco Umbrella, qui applique ensuite votre politique de nom de domaine complet (FQDN) Enterprise Security en nuage. Pour le trafic malveillant ou suspect, les utilisateurs peuvent être bloqués d'un site ou redirigés vers un proxy intelligent qui peut effectuer le filtrage d'URL en fonction de votre politique en nuage.

La procédure suivante explique le processus de bout en bout pour configurer Cisco Umbrella Connector.

Avant de commencer

En mode de contexte multiple, effectuez cette procédure dans chaque contexte de sécurité qui doit utiliser Cisco Umbrella.

Procédure

Étape 1 Créez un compte sur Cisco Umbrella, https://umbrella.cisco.com.

Étape 2 Installer le certificat d'autorité de certification à partir du serveur d'enregistrement Cisco Umbrella, à la page 6.

L'enregistrement du périphérique utilise HTTPS, ce qui nécessite l'installation du certificat racine.

Étape 3 Si ce n'est pas déjà fait, configurez les serveurs DNS et activez la recherche DNS sur les interfaces.

Vous pouvez utiliser vos propres serveurs ou configurer les serveurs Cisco Umbrella. L'inspection DNS redirige automatiquement vers les résolveurs Cisco Umbrella, même si vous configurez des serveurs différents.

- 208.67.220.220
- 208.67.222.222
- 2620:119:53::53
- 2620:119:35::35

Exemple :

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220
```

Étape 4 Configurer les paramètres globaux du connecteur Cisco Umbrella, à la page 7.

Étape 5 Activer Cisco Umbrella dans la liste des politiques d'inspection DNS, à la page 9.

Étape 6 Vérifier l'enregistrement de Cisco Umbrella, à la page 10.

Installer le certificat d'autorité de certification à partir du serveur d'enregistrement Cisco Umbrella

Vous devez importer le certificat racine pour établir la connexion HTTPS avec le serveur d'enregistrement de Cisco Umbrella. Le système utilise la connexion HTTPS lors de l'enregistrement du périphérique. Dans Cisco Umbrella, choisissez **Deployments (Déploiements) > Configuration (Configuration) > Root Certificate (Certificat racine)** et téléchargez le certificat.

Avant de commencer

Lorsque Cisco Umbrella met à jour son certificat, vous devez télécharger le nouveau certificat. Le certificat racine peut également changer. Assurez-vous d'avoir téléchargé le bon certificat racine.

Lorsque vous mettez à jour le certificat, vous devez désactiver Cisco Umbrella, puis le réactiver, pour que le système prenne en compte le nouveau certificat et s'enregistre correctement auprès de Cisco Umbrella.

Procédure

Étape 1 Créez un point de confiance pour le serveur d'enregistrement Cisco Umbrella.

crypto ca trustpoint *name*

Vous pouvez utiliser le nom que vous souhaitez pour le point de confiance (jusqu'à 128 caractères), tel que ctx1 ou umbrella_server.

Exemple :

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)#
```

Étape 2 Indiquez que vous souhaitez vous inscrire manuellement en collant le certificat.

enrollment terminal

Exemple :

```
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)#
```

Étape 3 Importez le certificat.

crypto ca authenticate *name*

Saisissez le nom du point de confiance que vous avez créé pour ce certificat. Suivez les invites et collez le certificat codé en base 64. Ne pas inclure les lignes BEGIN CERTIFICATE et END CERTIFICATE.

```
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

Configurer les paramètres globaux du connecteur Cisco Umbrella

Les paramètres globaux de Cisco Umbrella définissent principalement le jeton API nécessaire pour enregistrer le périphérique auprès de Cisco Umbrella.

Les paramètres globaux ne sont pas suffisants pour activer Cisco Umbrella. Vous devez également activer Umbrella dans votre carte de politique d'inspection DNS, comme décrit dans Activer Cisco Umbrella dans la liste des politiques d'inspection DNS, à la page 9.

Avant de commencer

- Connectez-vous au tableau de bord des périphériques réseau Cisco Umbrella (https://login.umbrella.com/) et obtenez un jeton API de périphérique réseau hérité pour votre organisation. Un jeton sera une chaîne hexadécimale, par exemple, AABBA59A0BDE1485C912AF. Générez une clé API pour les appareils réseau hérités à partir du tableau de bord Cisco Umbrella.
- Installez le certificat pour le serveur d'enregistrement Cisco Umbrella.

Procédure

Étape 1 Entrez en mode de configuration Cisco Umbrella.

umbrella-global

Exemple :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)#
```

Étape 2 Configurez le jeton API nécessaire pour s'enregistrer auprès de Cisco Umbrella.

token *api_token*

Exemple :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

Étape 3 (Facultatif) Si vous avez l'intention d'activer DNScrypt dans la carte de politiques d'inspection DNS, vous pouvez éventuellement configurer la clé publique du fournisseur DNScrypt pour la vérification des certificats. Si vous ne configurez pas la clé, la clé publique par défaut actuellement distribuée est utilisée pour la validation.

public-key *hex_key*

La clé est une valeur hexadécimale de 32 octets. Saisissez la valeur hexadécimale en ASCII avec un séparateur de deux points tous les 2 octets. La clé fait 79 octets. Obtenez cette clé auprès de Cisco Umbrella.

La clé par défaut est :
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

Pour revenir à l'utilisation de la clé publique par défaut, saisissez **no public-key**. Vous pouvez soit omettre la clé que vous avez configurée, soit l'inclure dans la version **no** de la commande.

Exemple :

```
ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
```

Étape 4 (Facultatif) Configurez le délai d'inactivité après lequel une connexion d'un client au serveur Cisco Umbrella sera supprimée s'il n'y a pas de réponse du serveur.

timeout edns *hh:mm:ss*

Le délai d'expiration est au format heures:minutes:secondes et peut être compris entre 0:0:0 et 1193:0:0. La valeur par défaut est 0:02:00 (2 minutes).

Exemple :

```
ciscoasa(config-umbrella)# timeout edns 00:01:00
```

Étape 5 (Facultatif) Configurez les noms de domaine locaux pour lesquels Cisco Umbrella doit être contourné.

Spécifiez le nom des domaines locaux pour lesquels les demandes DNS doivent contourner Cisco Umbrella et aller directement aux serveurs DNS configurés. Par exemple, vous pouvez demander à votre serveur DNS interne de résoudre tous les noms pour le nom de domaine de l'organisation en supposant que toutes les connexions internes sont autorisées.

Vous pouvez saisir directement votre nom de domaine local. En option, vous pouvez créer les expressions régulières qui définissent le nom, puis créer une carte de classe d'expression régulière et la spécifier dans la commande suivante :

local-domain-bypass {*regular_expression* | **regex class** *regex_classmap*}

Exemple :

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

Étape 6 (Facultatif) Configurez les adresses des serveurs DNS Cisco Umbrella non par défaut, qui résolvent les demandes DNS, que vous souhaitez utiliser.

resolver {**ipv4** | **ipv6**} *ip_address*

Vous pouvez entrer la commande séparément pour définir les adresses IPv4 et IPv6 des résolveurs Cisco Umbrella autres que les valeurs par défaut.

Exemple :

```
ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222
ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

Activer Cisco Umbrella dans la liste des politiques d'inspection DNS

La configuration des paramètres globaux de Cisco Umbrella n'est pas suffisante pour enregistrer le périphérique et activer la redirection de recherche DNS. Vous devez ajouter Cisco Umbrella dans le cadre de votre inspection DNS active.

Vous pouvez activer Cisco Umbrella globalement en l'ajoutant à la liste des politiques d'inspection DNS preset_dns_map.

Toutefois, si vous avez personnalisé l'inspection DNS et appliqué différentes listes des politiques d'inspection à différentes classes de trafic, vous devez activer Cisco Umbrella sur chaque clesse pour laquelle vous souhaitez le service.

La procédure suivante explique comment mettre en œuvre Cisco Umbrella globalement. Si vous avez des listes des politiques DNS personnalisées, consultez Configurer la liste des politiques d'inspection DNS.

Procédure

Étape 1 Modifiez la liste des politiques d'inspection preset_dns_map et passez en mode de configuration des paramètres.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)#
```

Étape 2 Activez Cisco Umbrella et précisez éventuellement le nom de la politique de Cisco Umbrella à appliquer au périphérique.

umbrella [**tag** *umbrella_policy*] [**fail-open**]

La balise est le nom d'une politique telle qu'elle est définie dans Cisco Umbrella. Lors de l'enregistrement, Cisco Umbrella attribuera la politique au périphérique (si le nom de la politique existe). Si vous ne spécifiez pas de politique, la politique par défaut est appliquée.

Incluez le mot-clé **fail-open** si vous souhaitez que la résolution DNS fonctionne si le serveur DNS Cisco Umbrella n'est pas disponible. En cas d'échec de l'ouverture, si le serveur DNS Cisco Umbrella n'est pas disponible, Cisco Umbrella se désactive dans cette liste des politiques et permet aux demandes DNS d'accéder aux autres serveurs DNS configurés sur le système, le cas échéant. Lorsque les serveurs DNS Cisco Umbrella sont de nouveau disponibles, la liste des politiques reprend de leur utilisation. Si vous n'incluez pas cette option, les requêtes DNS continuent d'être acheminées au résolveur Cisco Umbrella inaccessible, de sorte qu'elles ne recevront pas de réponse.

Exemple :

```
ciscoasa(config-pmap-p)# umbrella fail-open
```

Étape 3 (Facultatif) Activez DNScrypt pour chiffrer les connexions entre le périphérique et Cisco Umbrella.

dnscrypt

L'activation de DNScrypt démarre le fil d'échange de clés avec le résolveur Umbrella. Le fil d'échange de clés effectue l'établissement de liaison avec le résolveur toutes les heures et met à jour le périphérique avec une nouvelle clé secrète. Comme DNScrypt utilise UDP/443, vous devez vous assurer que la carte de trafic

utilisée pour l'inspection DNS comprend ce port. Notez que la classe d'inspection par défaut comprend déjà UDP/443 pour l'inspection DNS.

Exemple :

```
ciscoasa(config-pmap-p)# dnscrypt
```

Exemple

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

Vérifier l'enregistrement de Cisco Umbrella

Après avoir configuré les paramètres globaux de Cisco Umbrella et avoir activé Cisco Umbrella dans l'inspection DNS, l'appareil doit communiquer avec Cisco Umbrella et s'enregistrer. Vous pouvez vérifier la réussite de l'enregistrement en vérifiant si Cisco Umbrella a fourni un identifiant d'appareil.

Tout d'abord, vérifiez les statistiques de la politique de service et recherchez la ligne d'enregistrement Cisco Umbrella. Elle doit indiquer la politique appliquée par Cisco Umbrella (la balise), l'état HTTP de la connexion et l'ID de l'appareil.

L'état devrait être 200 Success (Réussite). Les codes d'erreur indiquent les éléments suivants : 401 indique que le jeton API était incorrect, et 409 indique que le périphérique existe déjà dans Cisco Umbrella.

Notez que les lignes du résolveur Cisco Umbrella ne doivent pas indiquer que les résolveurs ne répondent pas. Si tel est le cas, vérifiez que vous avez ouvert la communication DNS avec ces adresses IP dans votre politique de contrôle d'accès. Il peut s'agir d'une situation temporaire ou peut indiquer un problème de routage.

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
     Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
       umbrella registration: mode: fail-open tag: default, status: 200 success, device-id:
 010a13b8fbdfc9aa
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
       Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0 local-domain-bypass
 10
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
        DNScrypt: Certificate Update: completion 10, failure 1
```

Vous pouvez également vérifier la configuration en cours (filtre sur policy-map). La commande umbrella dans la liste des politiques est mise à jour pour afficher l'ID du périphérique. Vous ne pouvez pas configurer directement l'ID de l'appareil lorsque vous activez cette commande. L'exemple suivant modifie la sortie pour afficher les informations pertinentes.

```
ciscoasa(config)# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnscrypt
  umbrella device-id 010a3e5760fdd6d3
  no tcp-inspection
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
```

Exemples pour le connecteur Cisco Umbrella

Les rubriques suivantes fournissent des exemples de configuration du connecteur Cisco Umbrella.

Exemple : activation de Cisco Umbrella dans la politique d'inspection DNS globale

L'exemple suivant montre comment activer Cisco Umbrella globalement. La configuration active DNScrypt à l'aide de la clé publique par défaut. Elle attribue la politique par défaut de sécurité entreprise Cisco Umbrella.

Remarque Cet exemple utilise le certificat DigiCert Global Root G2. Assurez-vous de télécharger le dernier certificat racine utilisé par le site Cisco Umbrella, car le certificat correct change avec le temps. Le certificat affiché ici n'est qu'un exemple.

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNNNx7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHxmx
1x7e/dfgy5SDN67sH0NO3Xss0r0upS/kqbitOtSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUtluNJbd134/tJS7SsVQepj5Wz
tCO7TG1F8PapspUwtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMWxM4MphQIDAQABo0IwQDAP
```

```
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
quit
...

Do you accept this certificate? [yes/no]: yes

...

% Certificate successfully imported
ciscoasa(config)#

ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license

ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

Exemple : activation de Cisco Umbrella sur une interface avec une politique d'inspection personnalisée

L'exemple suivant montre comment activer Cisco Umbrella pour une classe de trafic spécifique. Cisco Umbrella est activé sur l'interface interne uniquement pour le trafic DNS/UDP. Comme nous activons DNScrypt, UDP/443 doit être inclus dans la classe de trafic. Une politique de sécurité d'entreprise nommée mypolicy (définie dans Cisco Umbrella) est appliquée.

Remarque Cet exemple utilise le certificat DigiCert Global Root G2. Assurez-vous de télécharger le dernier certificat racine utilisé par le site Cisco Umbrella, car le certificat correct change avec le temps. Le certificat affiché ici n'est qu'un exemple.

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIDjjCCAnagAwIBAgIQAzrx5qcRqaC7KGSxHQn65TANBgkqhkiG9w0BAQsFADBh
```

```
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBH
MjAeFw0xMzA4MDExMjAwMDBaFw0zODAxMTUxMjAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IEcyMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuzfNNNx7a8myaJCtSnX/RrohCgiN9RlUyfuI
2/Ou8jqJkTx65qsGGmvPrC3oXgkkRLpimn7Wo6h+4FR1IAWsULecYxpsMNzaHxmx
1x7e/dfgy5SDN67sH0NO3Xss0r0upS/kqbitOtSZpLYl6ZtrAGCSYP9PIUkY92eQ
q2EGnI/yuum06ZIya7XzV+hdG82MHauVBJVJ8zUtluNJbd134/tJS7SsVQepj5Wz
tCO7TG1F8PapspUwtP1MVYwnSlcUfIKdzXOS0xZKBgyMUNGPHgm+F6HmIcr9g+UQ
vIOlCsRnKPZzFBQ9RnbDhxSJITRNrw9FDKZJobq7nMWxM4MphQIDAQABo0IwQDAP
BgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAdBgNVHQ4EFgQUTiJUIBiV
5uNu5g/6+rkS7QYXjzkwDQYJKoZIhvcNAQELBQADggEBAGBnKJRvDkhj6zHd6mcY
1Yl9PMWLSn/pvtsrF9+wX3N3KjITOYFnQoQj8kVnNeyIv/iPsGEMNKSuIEyExtv4
NeF22d+mQrvHRAiGfzZ0JFrabA0UWTW98kndth/Jsw1HKj2ZL7tcu7XUIOGZX1NG
Fdtom/DzMNU+MeKNhJ7jitralj41E6Vf8PlwUHBHQRFXGU7Aj64GxJUTFy8bJZ91
8rGOmaFvE7FBcf6IKshPECBV1/MUReXgRPTqh5Uykw7+U0b6LJ3/iyK5S9kJRaTe
pLiaWN0bfVKfjllDiIGknibVb63dDcY3fe0Dkhvld1927jyNxF1WW6LZZm6zNTfl
MrY=
quit

...

Do you accept this certificate? [yes/no]: yes
...

% Certificate successfully imported
ciscoasa(config)#

ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
ciscoasa(config-pmap-p)# dnscrypt

ciscoasa(config)# object-group service umbrella-service-object
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config-service-object-group)# service-object udp destination eq 443

ciscoasa(config)# access-list umbrella-acl extended permit
object-group umbrella-service-object any any

ciscoasa(config)# class-map dns-umbrella
ciscoasa(config-cmap)# match access-list umbrella-acl

ciscoasa(config)# policy-map inside-policy
ciscoasa(config-pmap)# class dns-umbrella
ciscoasa(config-pmap-c)# inspect dns umbrella-policy

ciscoasa(config)# service-policy inside-policy interface inside
```

Exemple : exclusion de certains hôtes ou réseaux de Cisco Umbrella globalement

Si vous devez exclure certains hôtes ou réseaux de l'utilisation de Cisco Umbrella et que le choix est global plutôt que basé sur l'interface, vous pouvez supprimer l'inspection DNS globale et créer des cartes distinctes pour exclure ou inclure l'inspection Cisco Umbrella.

L'exemple suivant modifie la politique d'inspection globale pour exclure le réseau 192.168.1.0/24 de Cisco Umbrella.

Avant de commencer

Cet exemple suppose que vous avez déjà activé le DNS et configuré les paramètres globaux de Cisco Umbrella.

Procédure

Étape 1 Supprimez l'inspection DNS globale par défaut.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect dns
```

Étape 2 Créez une liste des politiques DNS qui active Cisco Umbrella.

Dans cet exemple, la liste des politiques est nommée umbrella-policy.

```
ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
```

Étape 3 Créez une carte de trafic pour le trafic exclu.

L'exemple suivant utilise une liste de contrôle d'accès pour identifier le trafic UDP/53 à partir du réseau 192.168.1.0/24.

```
ciscoasa(config)# access-list Umb_Exclude permit udp 192.168.1.0 255.255.255.0 any eq 53
ciscoasa(config)# class-map Umbrella_Exclude
ciscoasa(config-cmap)# match access-list Umb_Exclude
```

Étape 4 Créez une carte de trafic pour les hôtes qui doivent utiliser Cisco Umbrella.

L'exemple suivant fait correspondre le trafic UDP/53 de n'importe quelle source.

```
ciscoasa(config)# class-map Umbrella_Include
ciscoasa(config-cmap)# match port udp eq 53
```

Étape 5 Mettre à jour la politique d'inspection globale pour activer l'inspection DNS pour les cartes de trafic à l'aide de la liste des politiques DNS appropriée.

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)#  class Umbrella_Exclude
ciscoasa(config-pmap-c)# inspect dns
```

```
ciscoasa(config-pmap)#  class Umbrella_Include
ciscoasa(config-pmap-c)# inspect dns umbrella-policy
```

Surveillance du connecteur Cisco Umbrella

Les rubriques suivantes expliquent comment surveiller Cisco Umbrella Connector.

Surveillance des statistiques de politique de service Cisco Umbrella

Vous pouvez afficher les statistiques récapitulées et détaillées pour l'inspection DNS avec Cisco Umbrella activé.

show service-policy inspect dns [**detail**]

Sans le mot-clé **detail**, vous voyez tous les compteurs d'inspection DNS de base ainsi que les informations de configuration Cisco Umbrella. Le champ d'état fournit le code d'état HTTP pour la tentative du système de s'enregistrer auprès de Cisco Umbrella.

Les lignes Resolver (résolveur) indiquent quels serveurs Cisco Umbrella sont utilisés. Ces lignes indiqueront si le serveur est **ne répond pas**, ou si le système **sonde** actuellement le serveur pour déterminer s'il est devenu disponible. Si le mode est fail-open, le système permet aux demandes DNS d'être acheminées vers d'autres serveurs DNS (le cas échéant); sinon, les requêtes DNS ne recevront pas de réponse tant que les serveurs Cisco Umbrella ne répondront pas.

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
     Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
       umbrella registration: mode: fail-open tag: default, status: 200 success, device-id:
 010a13b8fbdfc9aa
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
       Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0 local-domain-bypass
 10
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
        DNScrypt: Certificate Update: completion 10, failure 1
```

La sortie détaillée affiche les statistiques DNScrypt et les clés utilisées.

```
asa(config)# show service-policy inspect dns detail
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: dnscrypt30000
      Inspect: dns dns_umbrella, packet 12, lock fail 0, drop 0, reset-drop 0,
```

```
              5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 1500, drop 0
        dns-guard, count 3
        protocol-enforcement, drop 0
        nat-rewrite, count 0
      Umbrella registration: mode: fail-open tag: default, status: 200 SUCCESS, device-id:
010af97abf89abc3, retry 0
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
      Umbrella: bypass 0, req inject 6 - sent 6, res recv 6 - inject 6 local-domain-bypass
10
          Umbrella app-id fail, count 0
          Umbrella flow alloc fail, count 0
          Umbrella block alloc fail, count 0
          Umbrella client flow expired, count 0
          Umbrella server flow expired, count 0
          Umbrella request drop, count 0
          Umbrella response drop, count 0
        DNScrypt egress: rcvd 6, encrypt 6, bypass 0, inject 6
        DNScrypt ingress: rcvd 18, decrypt 6, bypass 12, inject 6
          DNScrypt length error, count 0
          DNScrypt add padding error, count 0
          DNScrypt encryption error, count 0
          DNScrypt magic_mismatch error, count 0
          DNScrypt disabled, count 0
          DNScrypt flow error, count 0
          DNScrypt nonce error, count 0
        DNScrypt: Certificate Update: completion 1, failure 1
          DNScrypt Receive internal drop count 0
          DNScrypt Receive on wrong channel drop count 0
          DNScrypt Receive cannot queue drop count 0
          DNScrypt No memory to create channel count 0
          DNScrypt Send no output interface count 1
          DNScrypt Send open channel failed count 0
          DNScrypt Send no handle count 0
          DNScrypt Send dupb failure count 0
          DNScrypt Create cert update no memory count 0
          DNScrypt Store cert no memory count 0
          DNScrypt Certificate invalid length count 0
          DNScrypt Certificate invalid magic count 0
          DNScrypt Certificate invalid major version count 0
          DNScrypt Certificate invalid minor version count 0
          DNScrypt Certificate invalid signature count 0
          Last Successful: 01:42:29 UTC May 2 2018, Last Failed: None
          Magic DNSC, Major Version 0x0001, Minor Version 0x0000,
          Query Magic 0x714e7a696d657555, Serial Number 1517943461,
          Start Time 1517943461 (18:57:41 UTC Feb 6 2018)
          End Time 1549479461 (18:57:41 UTC Feb 6 2019)
          Server Public Key
240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836
          Client Secret Key Hash
48DD:E6D3:C058:D063:1098:C6B4:BA6F:D8A7:F0F8:0754:40B0:AFB3:CB31:2B22:A7A4:9CEE
          Client Public key
6CB9:FA4B:4273:E10A:8A67:BA66:76A3:BFF5:2FB9:5004:CD3B:B3F2:86C1:A7EC:A0B6:1A58
          NM key Hash
9182:9F42:6C01:003C:9939:7741:1734:D199:22DF:511E:E8C9:206B:D0A3:8181:CE57:8020
```

Surveillance des messages Syslog Cisco Umbrella

Vous pouvez surveiller les messages de journal système liés à Cisco Umbrella suivants :

- %ASA-3-339001 : Échec de la mise à jour du certificat DNSCRYPT pour *number* tentatives.

  Vérifiez qu'il y a une route vers le serveur Cisco Umbrella et que l'interface de sortie est opérationnelle et fonctionne correctement. Vérifiez aussi que la clé publique configurée pour DNScrypt est correcte. Vous devrez peut-être obtenir une nouvelle clé de Cisco Umbrella.

- %ASA-3-339002 : L'enregistrement de l'appareil Cisco Umbrella a échoué avec le code d'erreur *error_code*.

  Les codes d'erreur ont les significations suivantes :

  - 400 : il y a un problème de format ou de contenu de la demande. Le jeton est probablement trop court ou corrompu. Vérifiez que le jeton correspond à celui sur le tableau de bord Cisco Umbrella.
  - 401 : le jeton API n'est pas autorisé. Essayez de reconfigurer le jeton. Si vous avez actualisé le jeton dans le tableau de bord Cisco Umbrella, vous devez vous assurer d'utiliser le nouveau jeton.
  - 409 : l'ID de l'appareil est en conflit avec une autre organisation. Veuillez vérifier auprès de l'Administrateur Cisco Umbrella pour voir quel est le problème.
  - 500 : il y a une erreur de serveur interne. Vérifiez auprès de l'Administrateur Cisco Umbrella pour voir quel est le problème.

- %ASA-6-339003 : l'enregistrement de l'appareil Cisco Umbrella a réussi.

- %ASA-3-339004 : l'enregistrement de l'appareil Cisco Umbrella a échoué en raison d'un jeton manquant.

  Vous devez obtenir un jeton API de Cisco Umbrella et le configurer dans les paramètres globaux de Cisco Umbrella.

- %ASA-3-339005 : l'enregistrement de l'appareil Cisco Umbrella a échoué après *number* tentatives.

  Consultez les messages du journal système 339002 pour identifier les erreurs que vous devez corriger.

- %ASA-3-339006 : l'*IP_address* du résolveur Cisco Umbrella est accessible, ce qui reprend la redirection Umbrella.

  Ce message indique que le système fonctionne normalement. Aucune autre mesure n'est nécessaire.

- %ASA-3-339007 : l'*IP_address* du résolveur Cisco Umbrella ne répond pas et le mode de fermeture en cas de non-conformité est utilisé, démarrant la sonde pour le résolveur.

  Comme vous utilisez le mode de fermeture en cas de non-conformité, les utilisateurs ne recevront pas de réponses à leurs demandes DNS tant que le serveur DNS Cisco Umbrella ne sera pas de nouveau en ligne. Si le problème persiste, vérifiez qu'il existe une voie de routage entre le système et les serveurs Cisco Umbrella, et que vous autorisez le trafic DNS vers les serveurs dans votre politique de contrôle d'accès.

Historique du connecteur Cisco Umbrella

Nom de la caractéristique	Versions de plateforme	Description
Prise en charge de Cisco Umbrella	9.10(1)	Vous pouvez configurer le périphérique pour rediriger les requêtes DNS vers Cisco Umbrella, afin que votre politique de sécurité d'entreprise définie dans Cisco Umbrella puisse être appliquée aux connexions des utilisateurs. Vous pouvez autoriser ou bloquer les connexions en fonction du FQDN ou, pour les FQDN suspects, vous pouvez rediriger l'utilisateur vers le mandataire intelligent Cisco Umbrella, qui peut effectuer le filtrage d'URL. La configuration de Cisco Umbrella fait partie de la politique d'inspection DNS. Nous avons ajouté ou modifié les commandes suivantes : **umbrella**, **umbrella-global**, **token**, **public-key**, **timeout edns**, **dnscrypt**, **show service-policy inspect dns detail**.
Améliorations de Cisco Umbrella.	9.12(1)	Vous pouvez maintenant identifier les noms de domaine locaux qui doivent contourner Cisco Umbrella. Les demandes DNS pour ces domaines sont directement transmises aux serveurs DNS sans passer par Cisco Umbrella. Vous pouvez également identifier les serveurs Cisco Umbrella à utiliser pour la résolution des demandes DNS. Enfin, vous pouvez définir la politique d'inspection de Cisco Umbrella pour qu'elle s'ouvre même en cas de non-conformité, afin que les demandes DNS ne soient pas bloquées si le serveur Cisco Umbrella n'est pas disponible. Nous avons ajouté ou modifié les commandes suivantes : **local-domain-bypass**, **resolver**, **umbrella fail-open**.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.