Déployer Umbrella DNS pour les administrateurs WLAN Aruba

Table des matières

Introduction

Ce document décrit comment déployer le service Umbrella DNS pour les administrateurs WLAN d'Aruba.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

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.

Aperçu

Aruba Networks propose ces trois gammes de produits et systèmes d'exploitation WLAN

(Wireless LAN) pour différents segments de marché et scénarios de déploiement :

- ArubaOS : pour les grandes entreprises et les déploiements haute densité
- Aruba Instant / InstantOS : pour les petites et moyennes entreprises et les entreprises décentralisées
- Aruba Instant On : pour les particuliers et les petites entreprises

Cet article fournit des directives aux administrateurs WLAN d'Aruba pour l'adoption et le déploiement du service Umbrella DNS.

Méthodes de déploiement

Les méthodes de déploiement dépendent de votre système d'exploitation Aruba et de la façon dont vous prévoyez d'utiliser Umbrella.

Si vous exécutez l'un des trois systèmes d'exploitation Aruba mentionnés précédemment, vous pouvez commencer à déployer Umbrella DNS en consultant le guide de l'utilisateur d'Umbrella. Des didacticiels vidéo sont également disponibles.

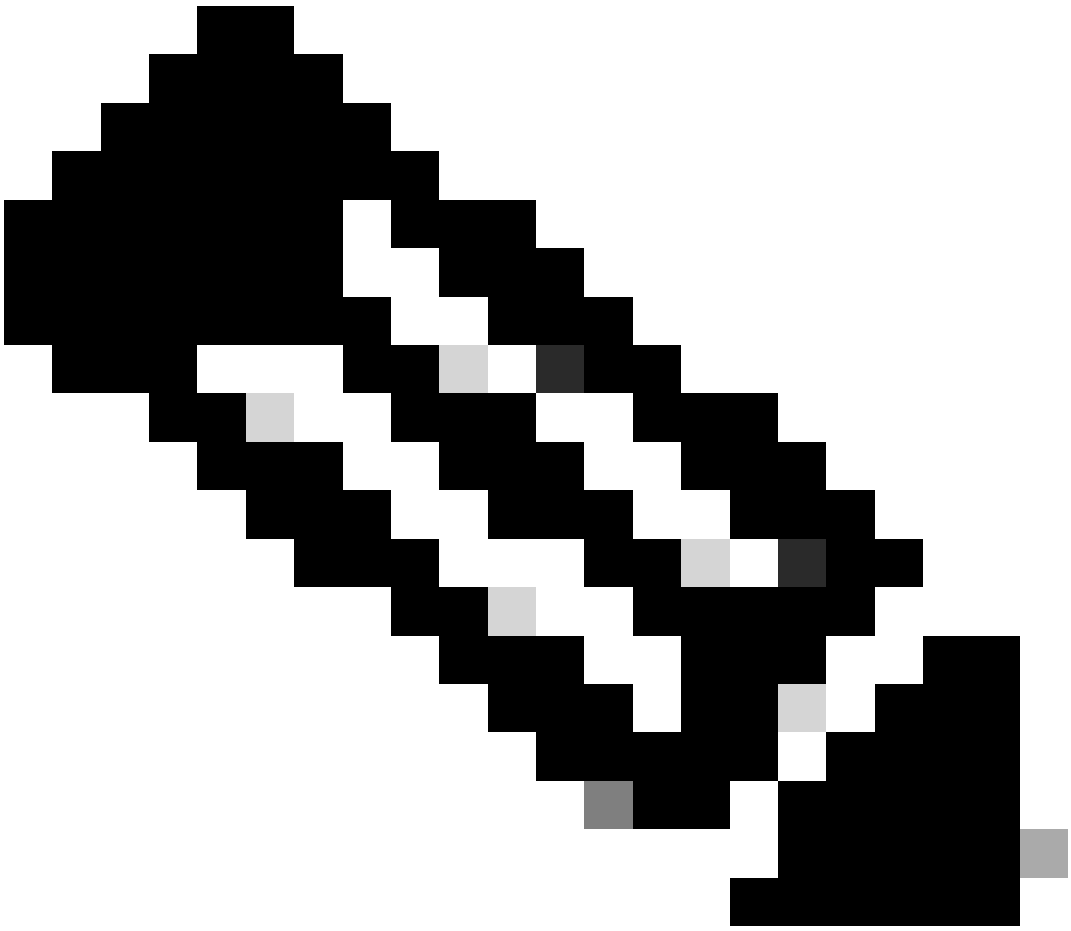
Si vous exécutez Aruba Instant, vous avez une option supplémentaire d'utiliser l'intégration de périphérique réseau Umbrella disponible dans InstantOS. Notez cependant que si vous choisissez cette option, vous ne pouvez pas voir les adresses IP internes/privées des clients sans fil sur le WLAN dans les rapports Umbrella, tels que le rapport de recherche d'activité. Les requêtes DNS des clients correspondent aux identités de périphériques réseau des clusters de points d'accès instantanés dans Umbrella, et les informations concernant les clients individuels ne sont pas disponibles. Du point de vue d'Umbrella Cloud, les requêtes DNS peuvent sembler provenir des clusters Instant AP plutôt que des clients Wi-Fi.

Par conséquent, si vous devez suivre les requêtes DNS de clients individuels ou personnaliser les stratégies DNS pour des clients individuels sur un WLAN, vous pouvez déployer Umbrella à l'aide des méthodes standard décrites dans le guide de l'utilisateur d'Umbrella DNS (sans utiliser l'intégration de périphérique réseau via Aruba Instant), et envisager d'inclure les appliances virtuelles Umbrella dans leurs plans de déploiement.

Element	Description
AD User	Identified by Virtual Appliance (VA) or Roaming Client (RC).
AD Computer	Identified by VA only.
Internal Network / Umbrella Site	Identified by VA only.
Default Umbrella Site	Traffic on VA with no other identity. Identified by VA only.
Roaming Client	Roaming Client only.
Network	Network Identity based on source IP of the DNS request.

Intégration instantanée d'Aruba

L'intégration de périphériques réseau OpenDNS (Umbrella) d'Aruba Instant peut être bénéfique dans des environnements où tous les clients Wi-Fi connectés à un cluster Instant AP sont soumis à une politique DNS Umbrella unique, et où il n'est pas nécessaire de revoir les requêtes DNS des clients individuels dans les rapports Umbrella. Cette section explique comment configurer l'intégration.



> Remarque : L'intégration utilise une version héritée de l'API des périphériques réseau d'Umbrella. La version héritée n'exige pas que les clients génèrent des jetons d'API à partir de leurs tableaux de bord Umbrella, contrairement aux versions plus récentes.

Les API héritées d'Umbrella ont atteint leur fin de vie le 01/09/2023, date après laquelle la prise en charge de l'intégration n'est plus assurée. Si vous rencontrez un problème avec l'intégration après le 01/09/2023, veuillez compléter la section « Mise en route » du guide de déploiement pour déployer Umbrella sans utiliser l'intégration.

Ces conditions doivent être remplies pour pouvoir utiliser l'intégration :

- Les AP doivent exécuter InstantOS version 8.10.0.1 ou ultérieure (à partir de mai 2022).
- Le compte de tableau de bord Umbrella utilisé pour l'intégration doit avoir le rôle d'administrateur complet.
- L'adresse e-mail du compte ne peut pas être associée à plusieurs tableaux de bord Umbrella. Si vous n'êtes pas sûr que l'adresse e-mail soit associée à un seul tableau de bord, vous pouvez contacter l'assistance Cisco Umbrella pour vérifier.
- L'authentification unique (SSO) et l'authentification à deux facteurs (2FA) ne peuvent pas être activées pour le compte.
- S'il existe une appliance de sécurité réseau (comme un pare-feu) entre les points d'accès et Internet, l'appliance doit autoriser les connexions non filtrées et non inspectées vers 208.67.220.220, 208.67.222.222, 67.215.92.210 et 146.112.255.152/29 (.152 ~ .159).

Configuration

L'activation de l'intégration s'effectue en quatre étapes :

1. Définissez un nom pour le cluster AP

2. Saisissez les informations de connexion du compte

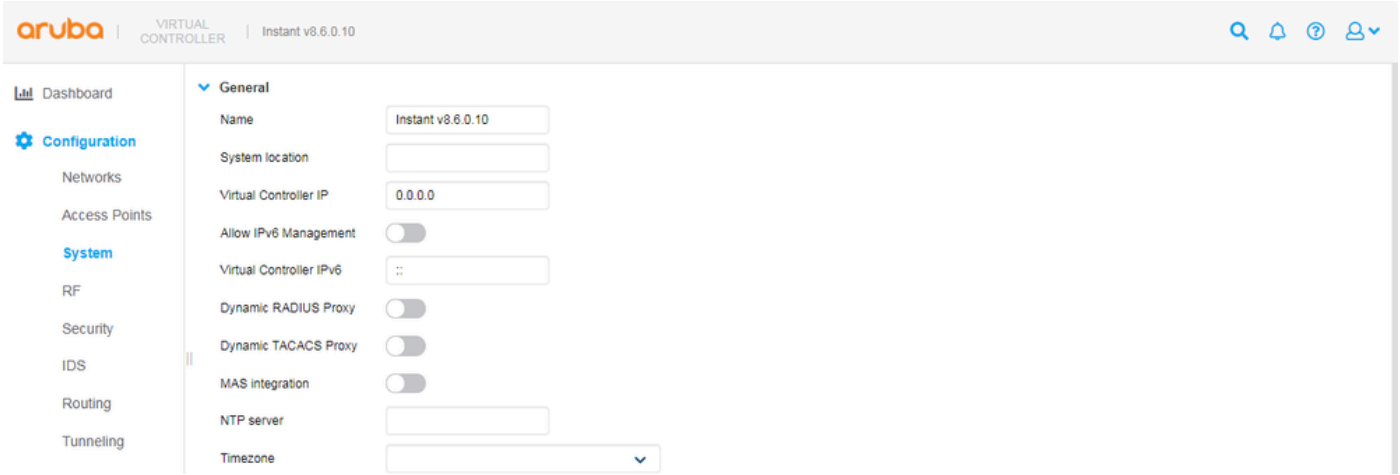
3. Intercepter les requêtes DNS

4. Appliquer la stratégie DNS

Définir un nom pour le cluster AP

Lorsqu'un cluster instantané s'enregistre auprès d'un tableau de bord Umbrella pour la première fois, une entrée de périphérique réseau est ajoutée au tableau de bord Umbrella sous Déploiements > Périphériques réseau. Le nom de périphérique d'une nouvelle entrée provient du nom système configuré sur le contrôleur virtuel d'un cluster.

Pour définir le nom du système sur un contrôleur virtuel instantané, accédez à Configuration > System.



4404011628308

Notez que la valeur du nom n'est copiée qu'une seule fois lors de l'enregistrement initial. Si le nom d'un système/périphérique est modifié par la suite du côté Instant ou Umbrella, vous devez mettre à jour manuellement le nom de l'autre côté.

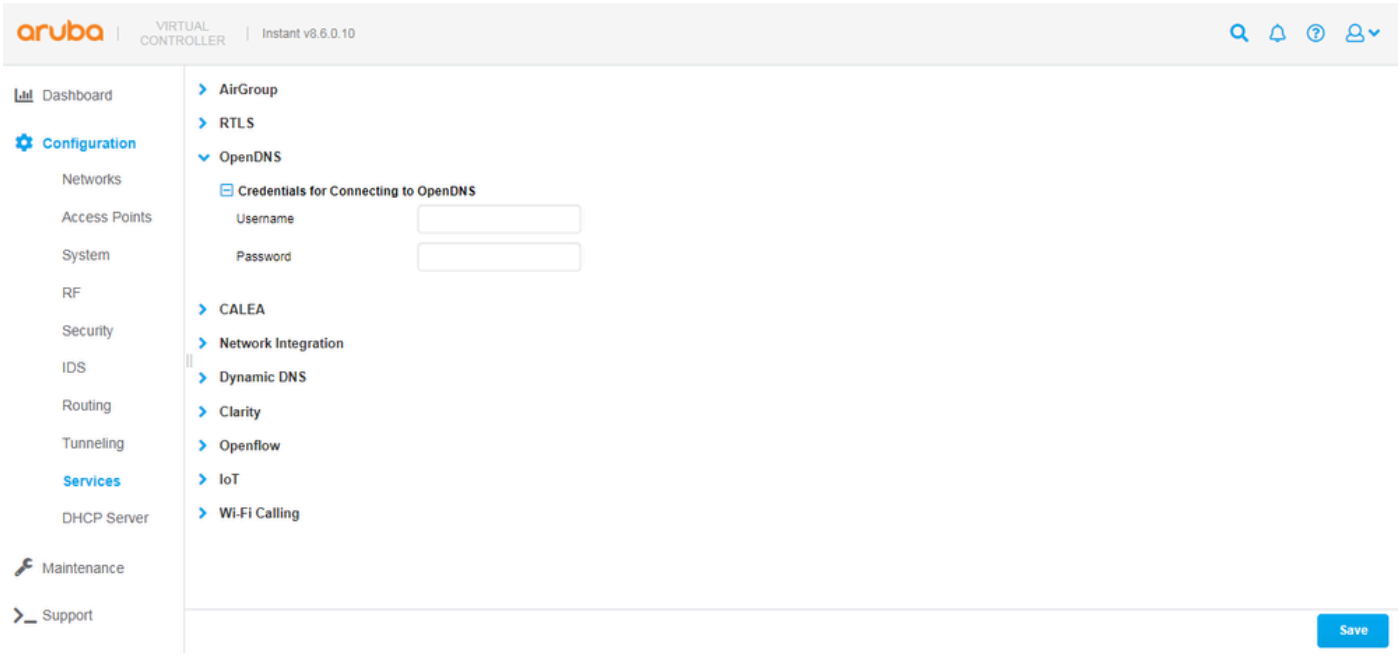
Saisir les identifiants de compte

Si les conditions requises répertoriées dans la section Prerequisites sont remplies, vous pouvez ajouter un cluster instantané à votre tableau de bord Umbrella en tant que périphérique réseau. Pour ce faire, à partir du contrôleur virtuel d'un cluster :

1. Accédez à Configuration > Services > OpenDNS.

2. Saisissez les identifiants de connexion d'un compte Umbrella.

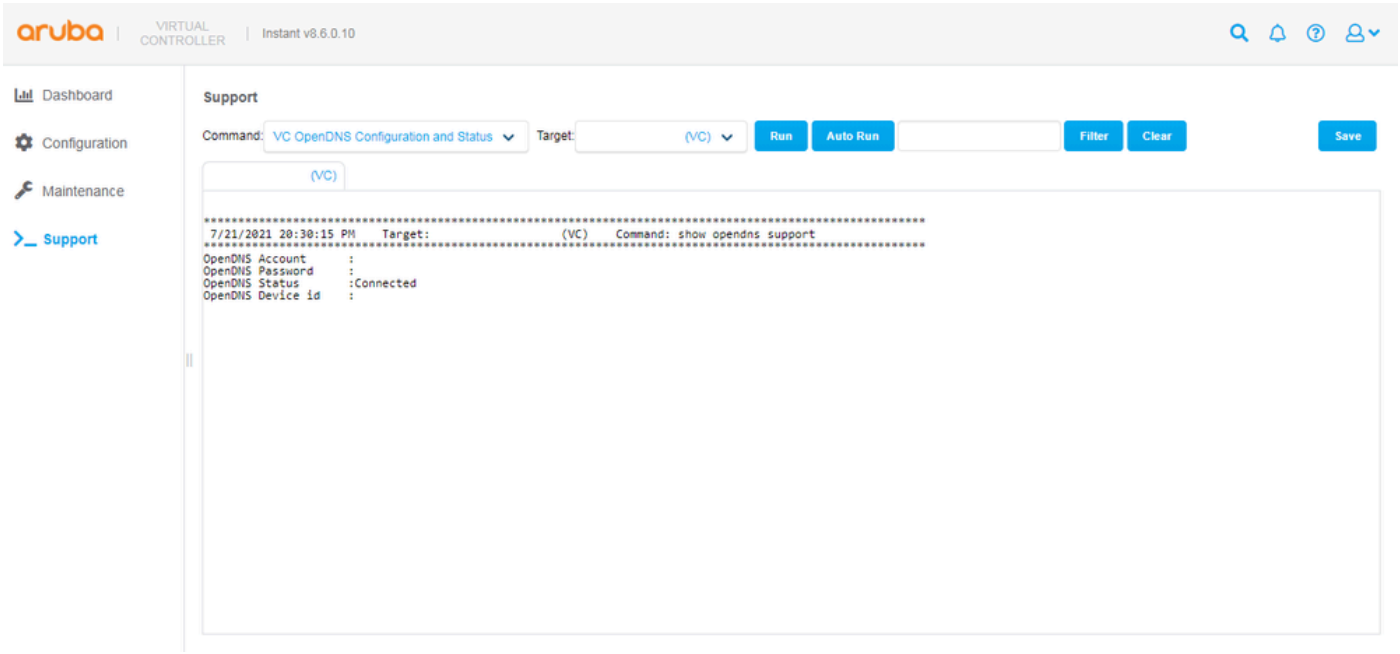
3. Sélectionnez Enregistrer.



4404019266196

Si le contrôleur virtuel (VC) se connecte avec succès à Umbrella, vous pouvez voir un état Connected quand vous naviguez vers Support et exécutez la commande "VC OpenDNS Configuration and Status" (`show opendns support`).

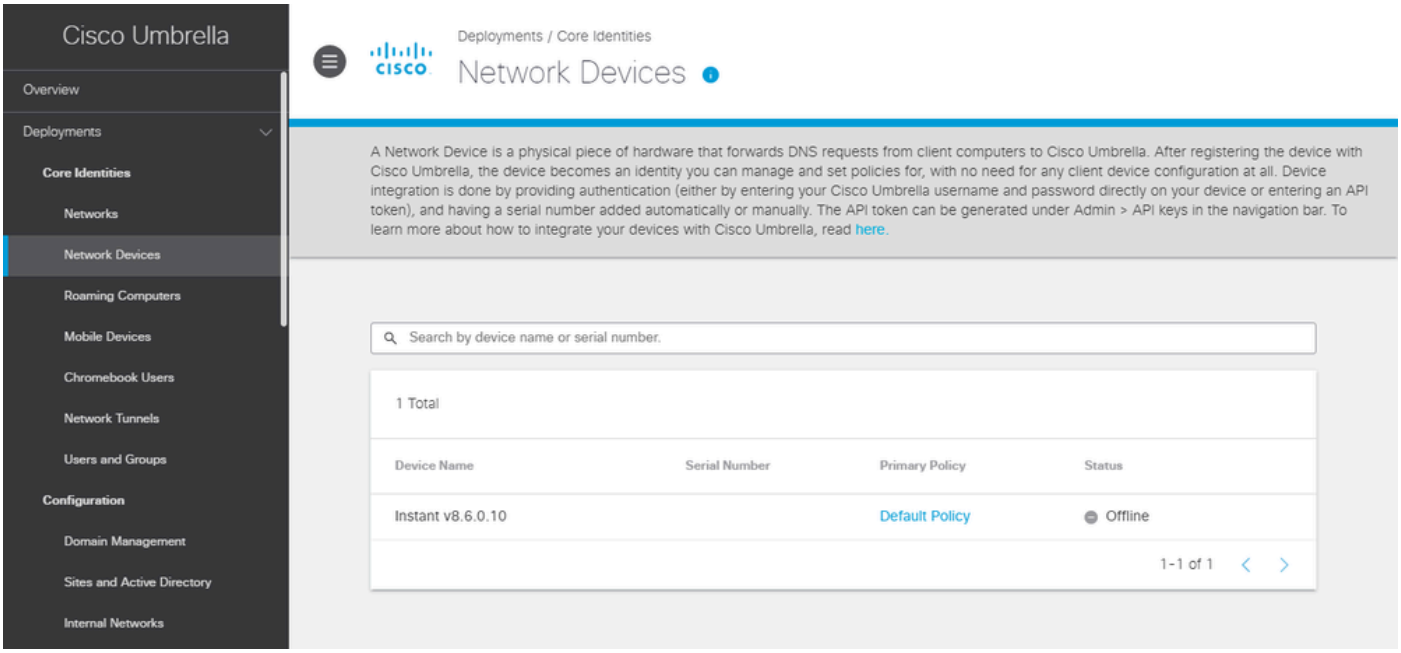
Vous pouvez également voir un ID de périphérique, qui est généré par Umbrella lorsqu'un nouveau périphérique réseau est créé et enregistré dans la configuration Instant VC. Cette dernière partie est importante. Étant donné que chaque cluster instantané doit avoir un ID de périphérique réseau Umbrella unique, l'ID de périphérique ne doit pas être copié d'une configuration de cluster à une autre. Un ID de périphérique valide comporte généralement 16 chiffres.



4404019268116

Si le résultat de la commande indique un état Not connected, vous pouvez essayer de découvrir pourquoi en exécutant les commandes « AP Tech Support Dump » (`show tech-support`) et « AP Tech Support Dump Supplemental » (`show tech-support supplemental`), puis en recherchant « opendns » dans les journaux. Les résultats de la commande peuvent également être partagés avec Aruba TAC à des fins de dépannage.

Si tout fonctionne correctement, vous pouvez voir une nouvelle entrée dans le tableau de bord Umbrella sous Déploiements > Périphériques réseau, où vous pouvez rechercher un cluster Instant AP par son nom ou supprimer une entrée existante si vous souhaitez générer un nouvel ID de périphérique.



4404011658516

Intercepter les requêtes DNS

Après avoir confirmé qu'un cluster a été ajouté avec succès à votre tableau de bord Umbrella en tant que périphérique réseau, vous pouvez configurer le cluster pour commencer à intercepter les requêtes DNS envoyées à partir de clients sans fil (qui sont connectés à des points d'accès dans le cluster). Une fois définies, quelles que soient les adresses IP du serveur DNS configurées sur les cartes réseau des clients sans fil, les requêtes DNS des clients peuvent être interceptées par le cluster et transmises aux résolveurs anycast d'Umbrella aux adresses 208.67.220.220 et 208.67.222.222.

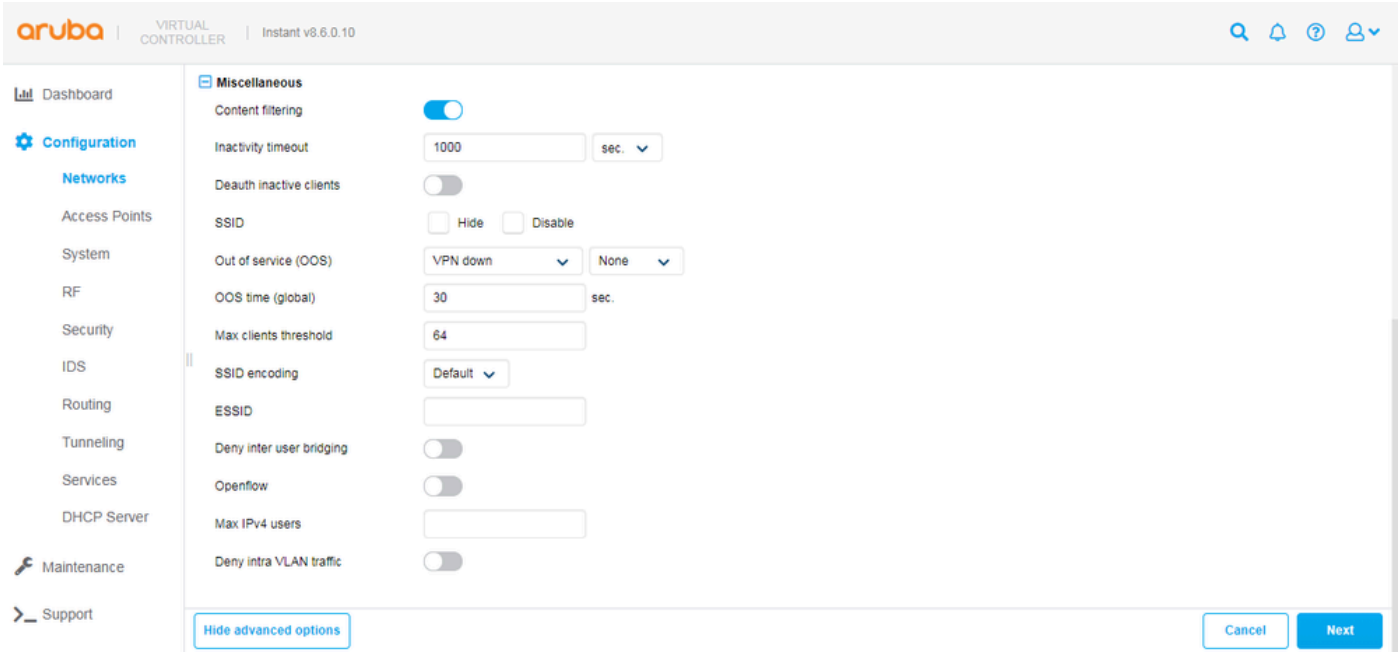
Pour intercepter des requêtes DNS :

1. Accédez au contrôleur virtuel d'un cluster sous Configuration > Networks.

2. Sélectionnez un réseau sans fil.

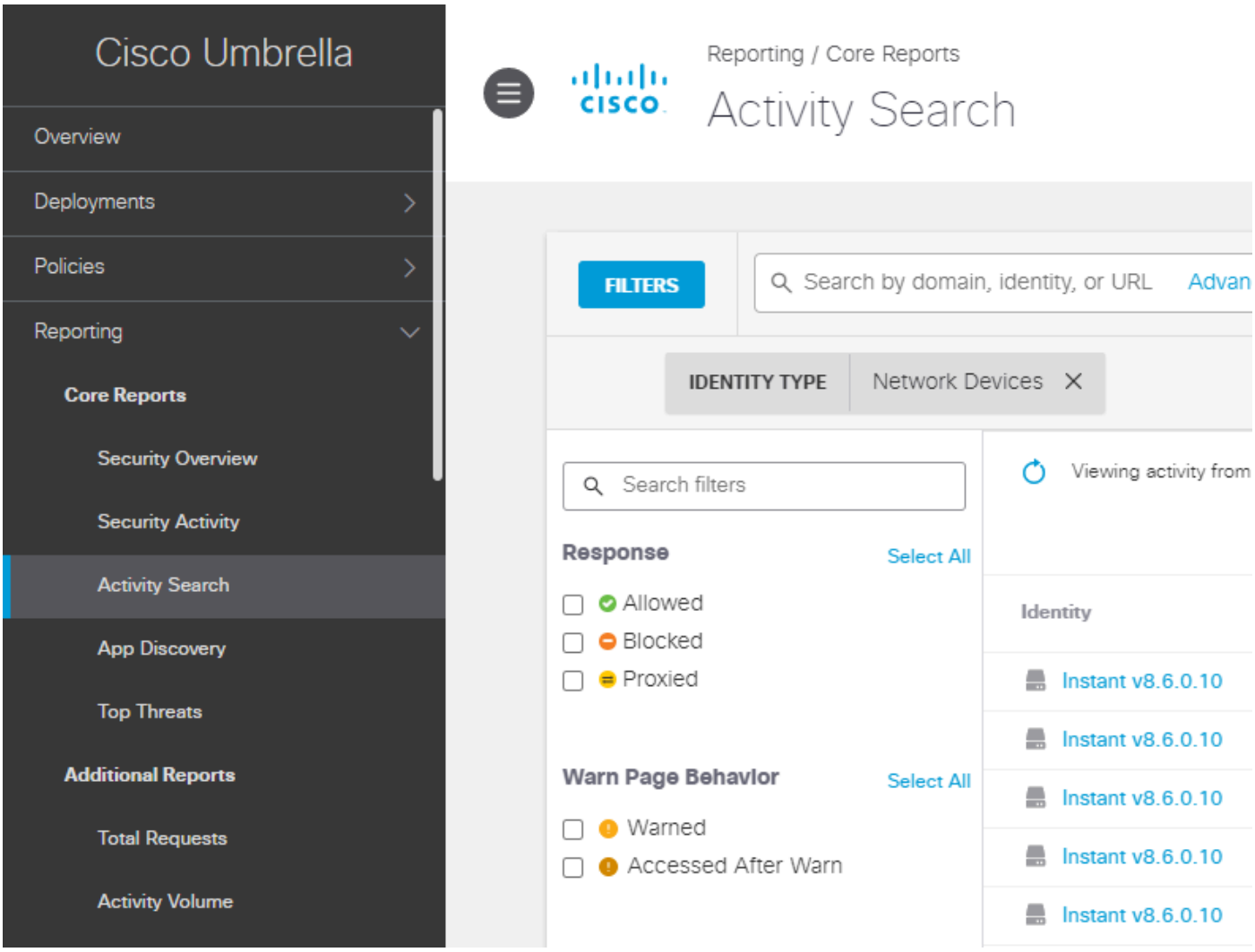
3. Modifiez le réseau, sélectionnez Afficher les options avancées, puis accédez à la section Divers.

4. Activez l'option Filtrage du contenu et continuez à sélectionner Suivant jusqu'à ce que vous puissiez sélectionner le bouton Terminer pour enregistrer la modification.



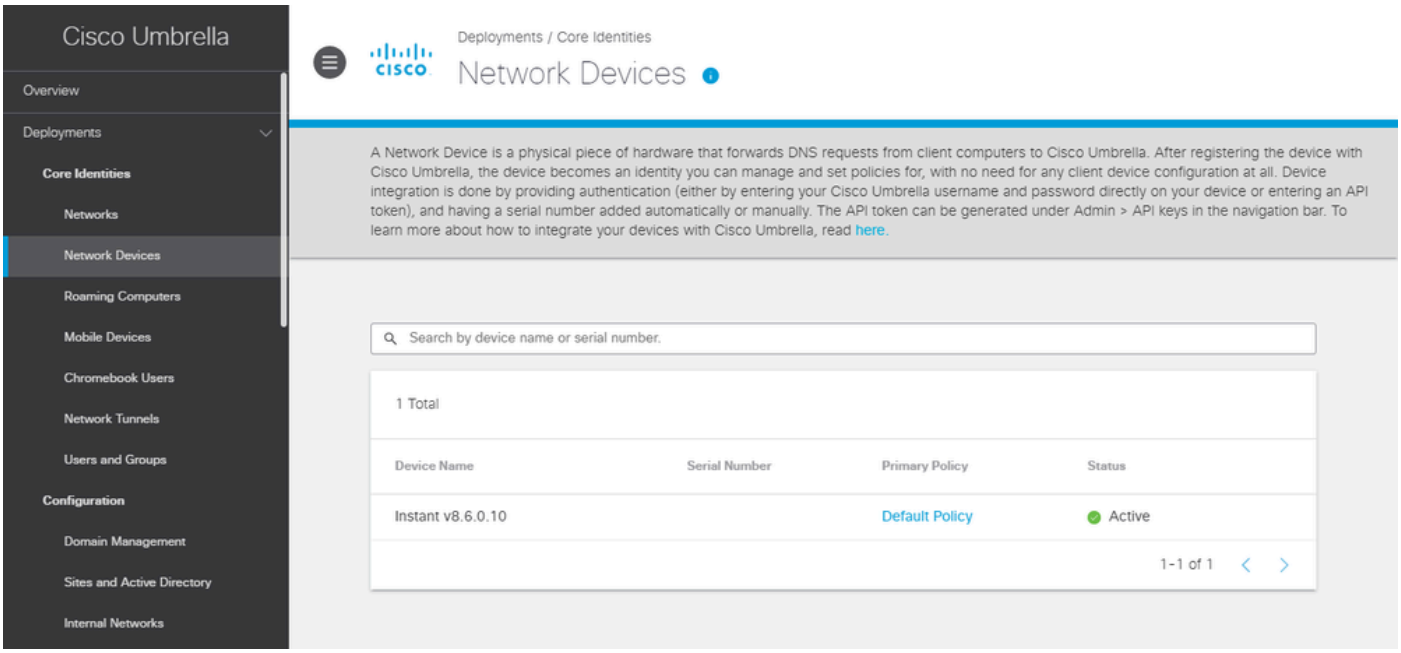
4404011668500

Une fois l'option activée, vous pouvez commencer à voir les requêtes DNS dans le tableau de bord Umbrella sous Reporting > Activity Search.L'identité des requêtes peut mapper à un nom de périphérique réseau, qui est généralement le nom système configuré sur le contrôleur virtuel d'un cluster AP. Notez que le traitement et l'affichage des requêtes dans l'interface graphique du tableau de bord peuvent prendre un certain temps (environ 15 minutes).



4404011721620

Dans le tableau de bord Umbrella sous Déploiements > Périphériques réseau, il peut prendre jusqu'à 24 heures pour qu'un périphérique passe à un état actif/en ligne. L'état d'un périphérique réseau indique simplement si les requêtes DNS ont été interceptées par le périphérique et transmises à Umbrella au cours des 24 heures précédentes, et n'influence pas la façon dont un périphérique communique avec Umbrella. Un état hors ligne/inactif peut simplement signifier qu'aucun client sans fil n'a été connecté à un cluster AP au cours des dernières 24 heures et ne peut pas empêcher le cluster d'utiliser le service Umbrella.

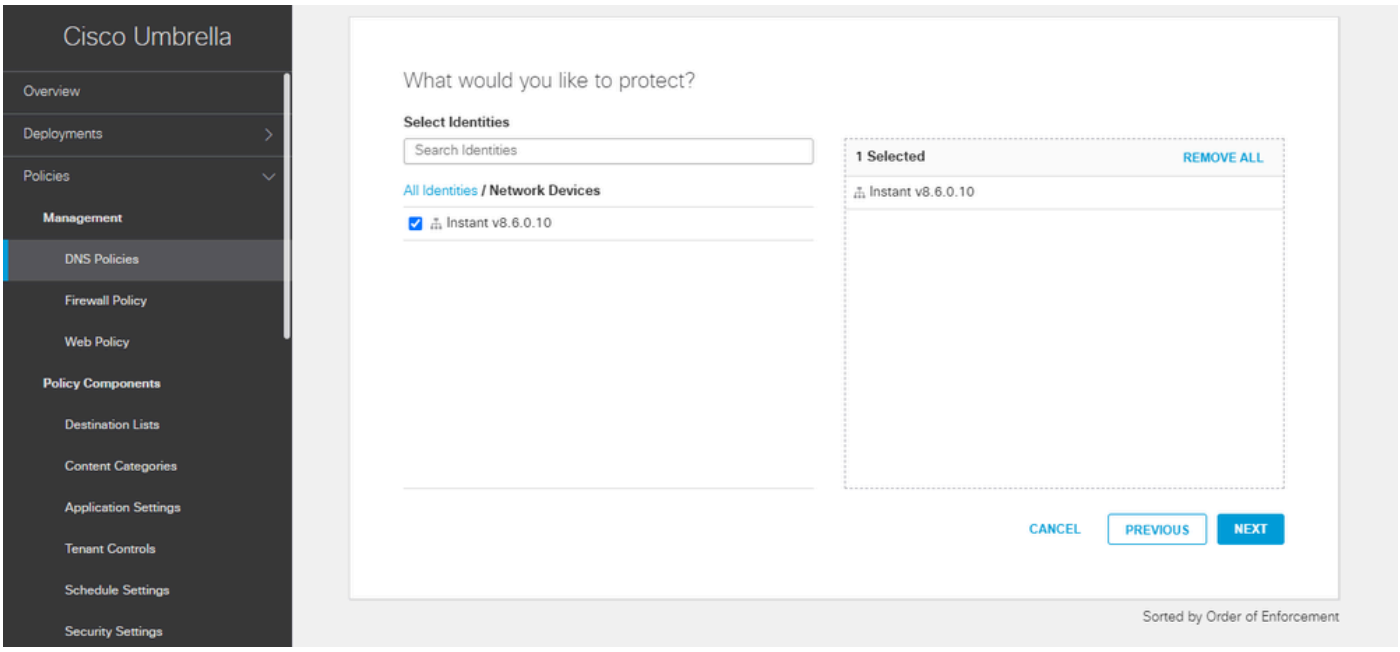


4404011756308

Appliquer la stratégie DNS

Dans Umbrella, la « politique par défaut » inclut automatiquement toutes les identités (comme les périphériques réseau) ajoutées à un tableau de bord. Il n'est pas nécessaire de créer des stratégies DNS supplémentaires si tous les clusters AP de votre déploiement peuvent être soumis à la même stratégie. Si c'est le cas pour vous, passez à la section suivante.

Si vous souhaitez également appliquer une stratégie personnalisée à un périphérique réseau spécifique, vous devez ajouter une nouvelle stratégie dans le tableau de bord Umbrella sous Policies > All Policies (DNS Policies), et sélectionner le périphérique réseau dans la stratégie.



4404011773588

Lorsqu'il existe plusieurs stratégies sur la page Stratégies DNS (Toutes les stratégies), les

stratégies sont évaluées de haut en bas selon la méthode de la première correspondance. Pour plus d'informations, reportez-vous à la documentation relative aux priorités des stratégies et aux meilleures pratiques de définition de la documentation relative aux stratégies.

DNS interne

Dans un environnement où des serveurs DNS internes existent et où vous souhaitez transférer des requêtes DNS pour certains domaines (internes) vers les serveurs DNS internes, vous pouvez utiliser la fonctionnalité Domaines d'entreprise d'Instant.

Les requêtes DNS peuvent continuer à être interceptées par le cluster AP après que la fonctionnalité est activée, sauf que les requêtes pour les domaines spécifiés ne peuvent plus être transférées à Umbrella. Au lieu de cela, ils peuvent être transférés aux adresses IP du serveur DNS configurées à l'origine sur les cartes réseau des clients sans fil (par exemple via DHCP). Cette fonctionnalité est similaire à la fonctionnalité Domaines internes disponible dans les méthodes de déploiement Umbrella standard (avec les appliances virtuelles), où l'intégration instantanée d'Aruba n'est pas utilisée.

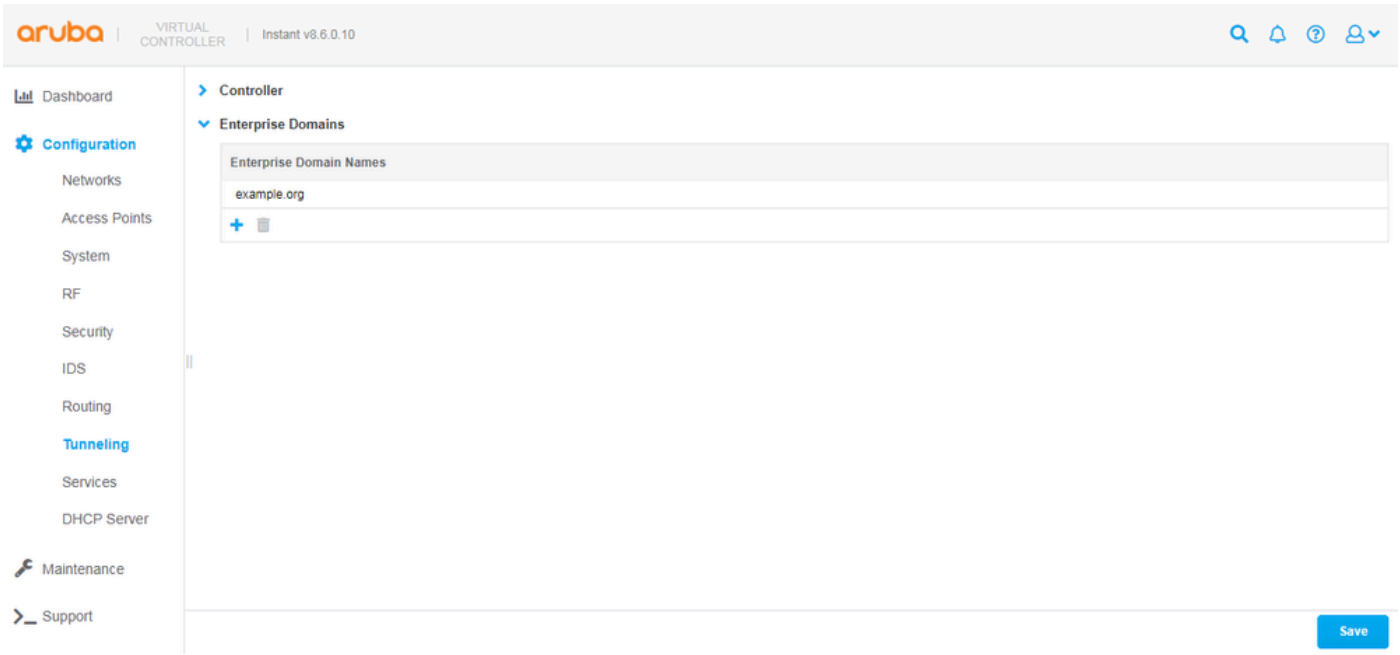
Pour configurer la fonctionnalité sur un contrôleur virtuel instantané :

1. Accédez à Configuration > Tunneling > Enterprise Domains.

2. Ajoutez des domaines à la liste Noms de domaine d'entreprise ou supprimez-en.

3. Sélectionnez Enregistrer.

Il y a un caractère générique implicite pour tout domaine ajouté à la liste, donc example.org implique *.example.org.



4404238114452

Vérification

Que vous ayez déployé Umbrella sur votre WLAN à l'aide des méthodes standard référencées dans la section « Vue d'ensemble du déploiement » de ce guide, ou de l'intégration décrite dans la section « Intégration instantanée d'Aruba », vous pouvez vérifier que les clients sans fil utilisent Umbrella DNS en naviguant sur https://welcome.umbrella.com/ à partir de l'un des clients. Une coche verte semblable à la capture d'écran affichée dans la documentation Umbrella s'affiche ensuite.

4404011960212

Vous pouvez également le vérifier en exécutant cette commande à l'invite d'un client sans fil.

```
nslookup -type=txt debug.opendns.com.
```

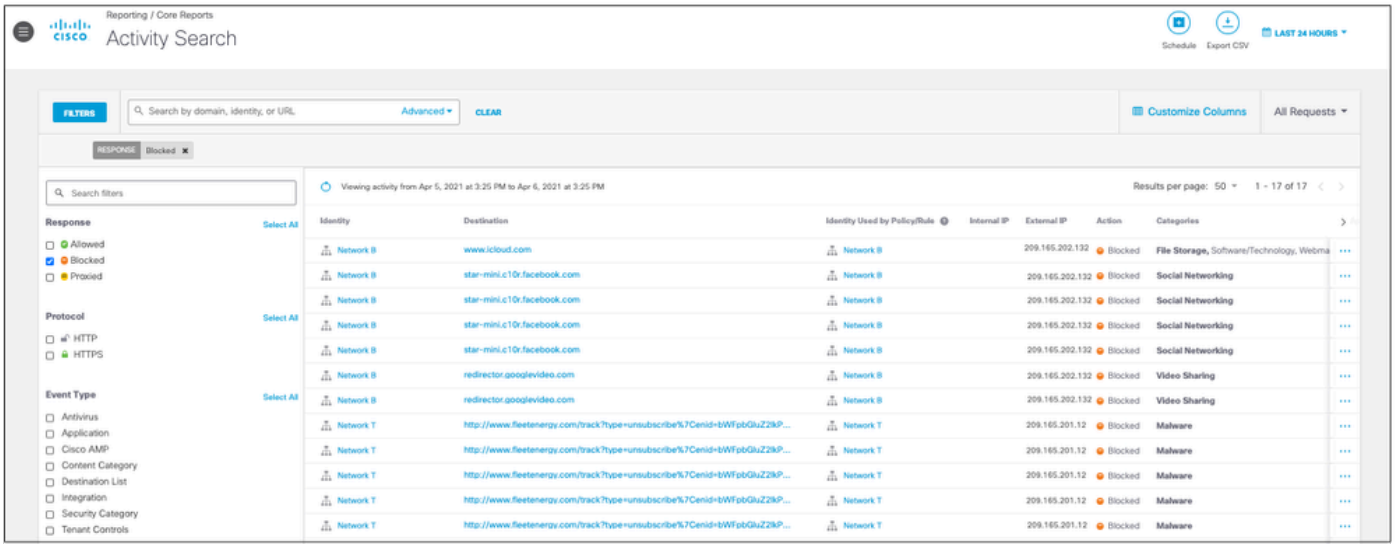
Vous pouvez voir une sortie avec un certain nombre de lignes de texte, semblable à cette capture d'écran :

```
anthony@ubuntu:~/Desktop$ nslookup -type=txt debug.opendns.com.
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
debug.opendns.com       text = "server 7.pao"
debug.opendns.com       text = "organization id [redacted]
debug.opendns.com       text = "appliance id [redacted]
debug.opendns.com       text = "host id [redacted]
debug.opendns.com       text = "user id [redacted]
debug.opendns.com       text = "remoteip [redacted]
debug.opendns.com       text = "flags [redacted]
debug.opendns.com       text = "id [redacted]
debug.opendns.com       text = "source [redacted]
debug.opendns.com       text = "fw: flags [redacted]
debug.opendns.com       text = "fw: id [redacted]
debug.opendns.com       text = "fw: source [redacted]

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

À partir du résultat de la commande, vous pouvez voir l'ID d'organisation de votre tableau de bord Umbrella dans la ligne « orgid » ou « organization id », et si vous utilisez l'intégration instantanée, vous pouvez voir la ligne supplémentaire « device » qui contient un ID de périphérique.

Pour consulter les requêtes DNS dans votre tableau de bord Umbrella, accédez à Reporting > Activity Search. Notez que l'affichage des requêtes dans l'interface graphique du tableau de bord peut prendre un certain temps (environ 15 minutes). Des instructions sur l'utilisation de la recherche d'activité sont disponibles à l'adresse dans la documentation Umbrella.



4404019393044

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.