Configuration de la transmission tunnel partagée dynamique ASA/AnyConnect

Table des matières

Introduction

Ce document décrit comment configurer AnyConnect Secure Mobility Client pour la tunnellisation dynamique avec exclusion de fractionnement via ASDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base sur ASA.
- Connaissances de base du client Cisco Anyconnect Security Mobility.

Composants utilisés

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

- ASA 9.12(3)9
- Adaptive Security Device Manager (ASDM) 7.13(1)
- AnyConnect 4.7.0

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 lâ€™incidence possible des commandes.

Informations générales

La transmission tunnel partagée AnyConnect permet au client Cisco AnyConnect Secure Mobility d'accéder en toute sécurité aux ressources de l'entreprise via IKEV2 ou SSL (Secure Sockets Layer).

Avant AnyConnect version 4.5, en fonction de la stratégie configurée sur l'appliance de sécurité adaptatif (ASA), le comportement de tunnel partagé pouvait être Tunnel Specified, Tunnel All ou Exclude Specified.

Avec l'avènement des ressources informatiques hébergées dans le cloud, les services se résolvent parfois en une adresse IP différente en fonction de l'emplacement de l'utilisateur ou de la charge des ressources hébergées dans le cloud.

Étant donné quâ€™Anyconnect Secure Mobility Client fournit une tunnellisation partagée vers une plage de sous-réseaux statiques, un hôte ou un pool dâ€™IPV4 ou dâ€™IPV6, il devient difficile pour les administrateurs réseau dâ€™exclure des domaines/noms de domaine complets pendant la configuration dâ€™AnyConnect.

Par exemple, un administrateur réseau souhaite exclure le domaine Cisco.com de la configuration du tunnel partagé, mais le mappage DNS de Cisco.com change car il est hébergé dans le cloud.

À l'aide de la tunnellisation Dynamic Split Exclude, Anyconnect résout dynamiquement l'adresse IPv4/IPv6 de l'application hébergée et apporte les modifications nécessaires à la table de routage et aux filtres pour permettre l'établissement de la connexion en dehors du tunnel.

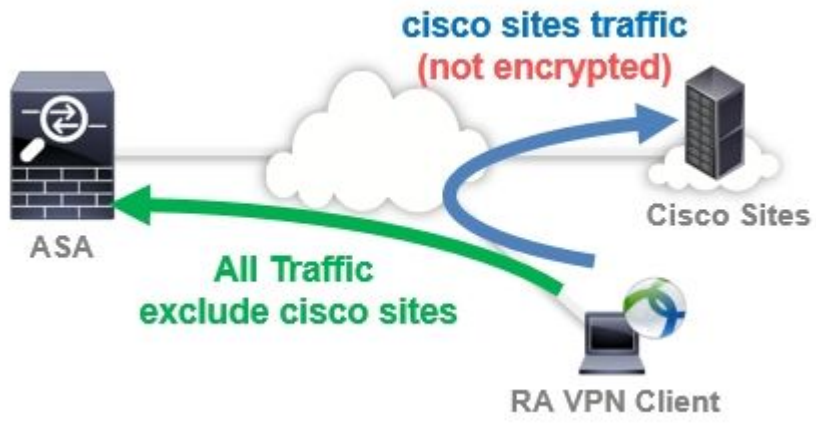
À partir de AnyConnect 4.5, la tunnellisation dynamique de broches peut être utilisée, dans laquelle AnyConnect résout dynamiquement l'adresse IPv4/IPv6 de l'application hébergée et apporte les modifications nécessaires dans la table de routage et les filtres pour permettre à la connexion d'être effectuée en dehors du tunnel

Configuration

Cette section explique comment configurer le client pour la mobilité sécurisée Cisco AnyConnect sur lâ€™ASA.

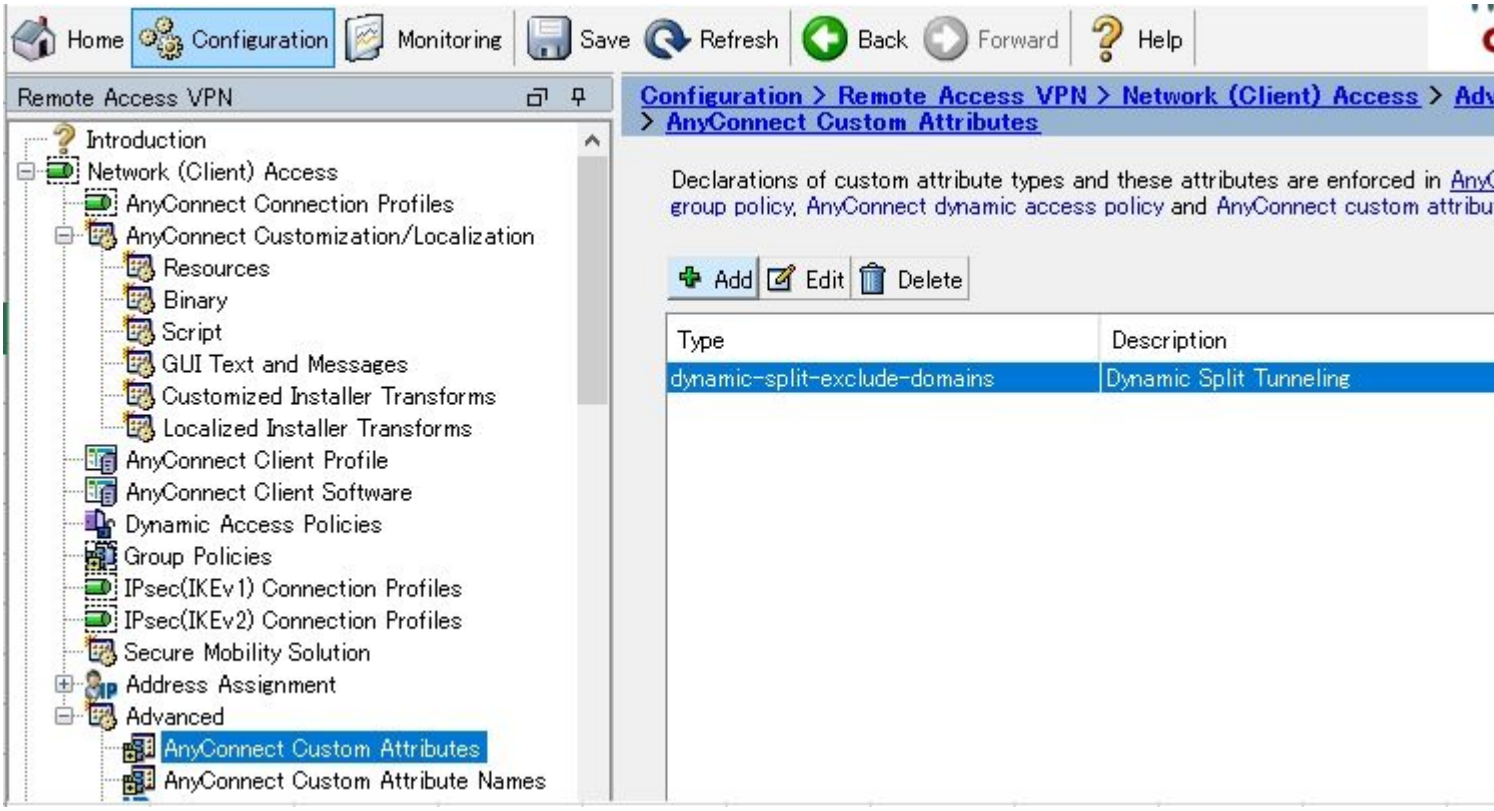
Diagramme du réseau

Cette image présente la topologie utilisée pour les exemples de ce document.



Étape 1. Créez des attributs personnalisés AnyConnect.

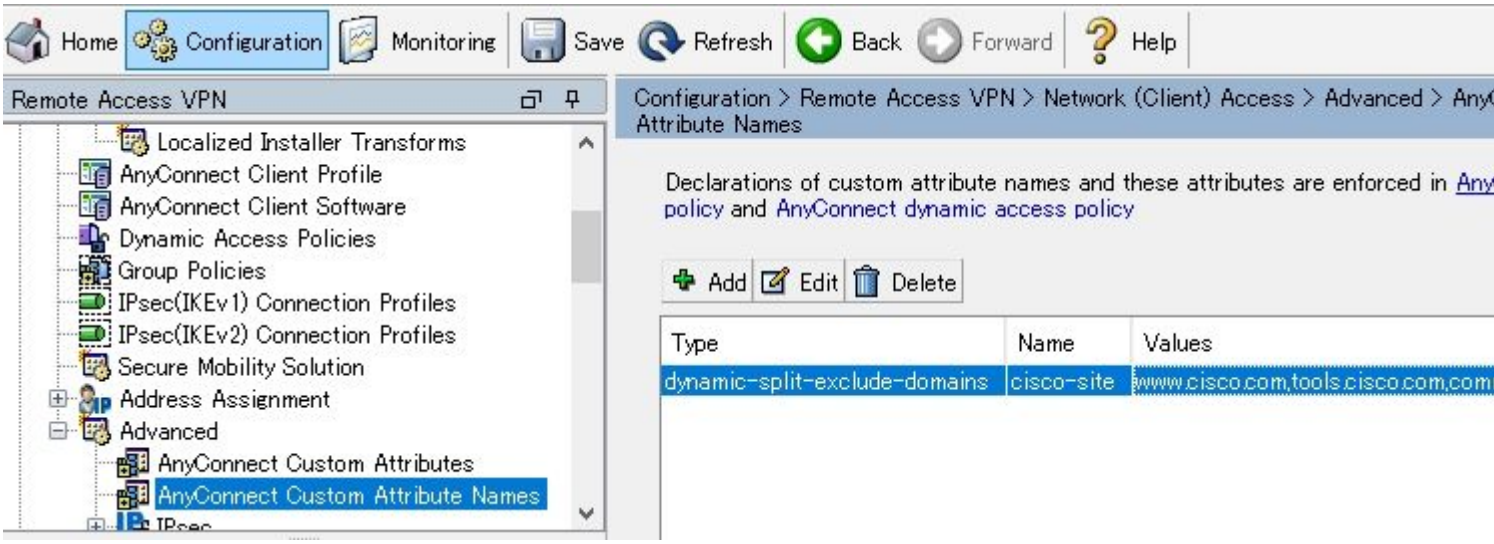
Naviguez jusqu'à **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.** cliquez sur **Add** et définir **dynamic-split-exclude-domains** attribut et description facultative, comme indiqué dans l'image :



Étape 2. Créez un nom personnalisé AnyConnect et configurez les valeurs.

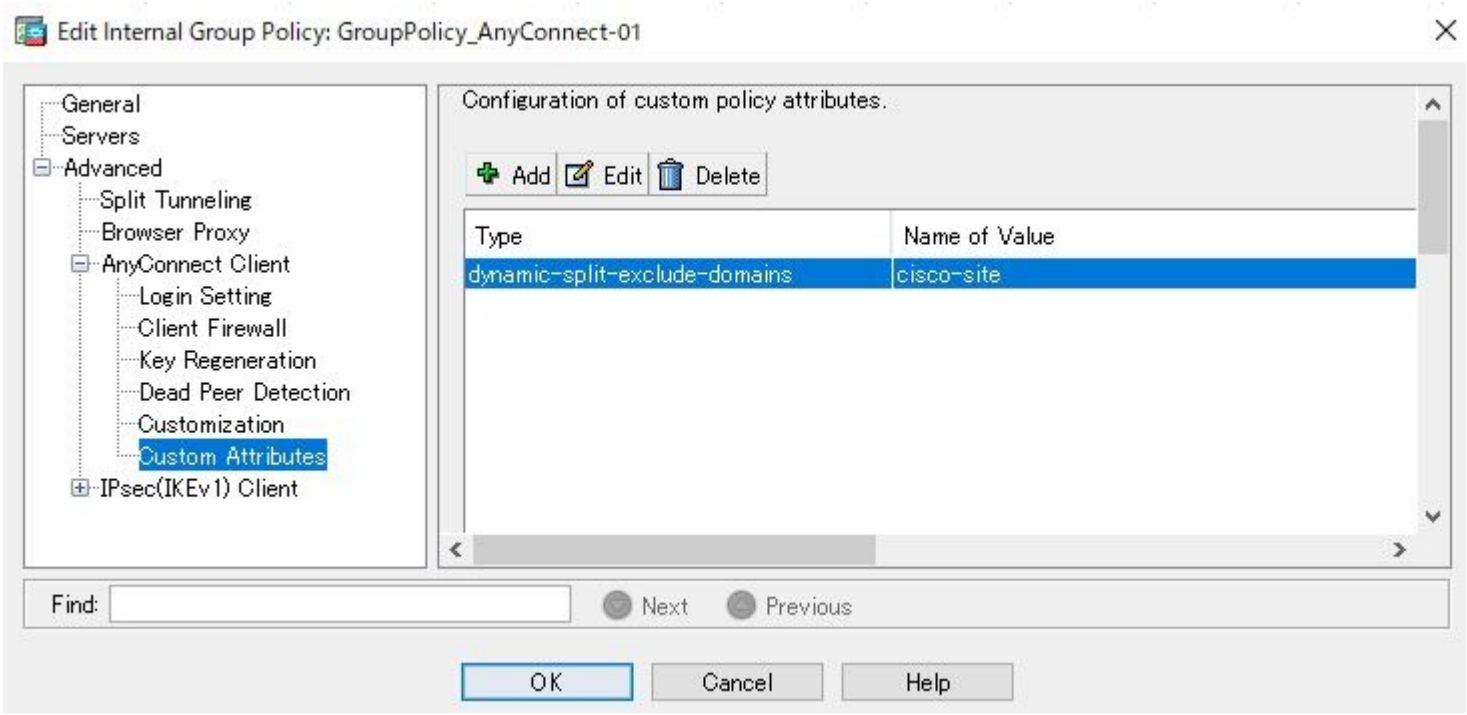
Naviguez jusqu'à **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names.** cliquez sur **Add** , puis définissez le **dynamic-split-exclude-domains** Attribut créé précédemment à partir de Type, un nom arbitraire et de Values, comme illustré dans l'image :

Veillez à ne pas entrer d'espace dans le champ Nom. (Exemple : possible « cisco-site » Impossible « cisco site ») Lorsque plusieurs domaines ou noms de domaine complets dans Values sont enregistrés, séparez-les par une virgule (,).



Étape 3. Ajoutez un type et un nom à la stratégie de groupe.

Naviguez jusqu'à **Configuration> Remote Access VPN> Network (Client) Access> Group Policies** et Sélectionnez une stratégie de groupe. Ensuite, accédez à **Advanced> AnyConnect Client> Custom Attributes** et ajoutez les paramètres **Type** et **Name,** comme l'illustre l'image :



Exemple de configuration CLI

Cette section fournit la configuration CLI de Dynamic Split Tunneling à des fins de référence.

<#root>

```
ASAv10# show run
  --- snip ---
```

webvpn

```
 enable outside
```

anyconnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling

```
 hsts
  enable
  max-age 31536000
  include-sub-domains
  no preload
 anyconnect image disk0:/anyconnect-win-4.7.04056-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
```

anyconnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community.

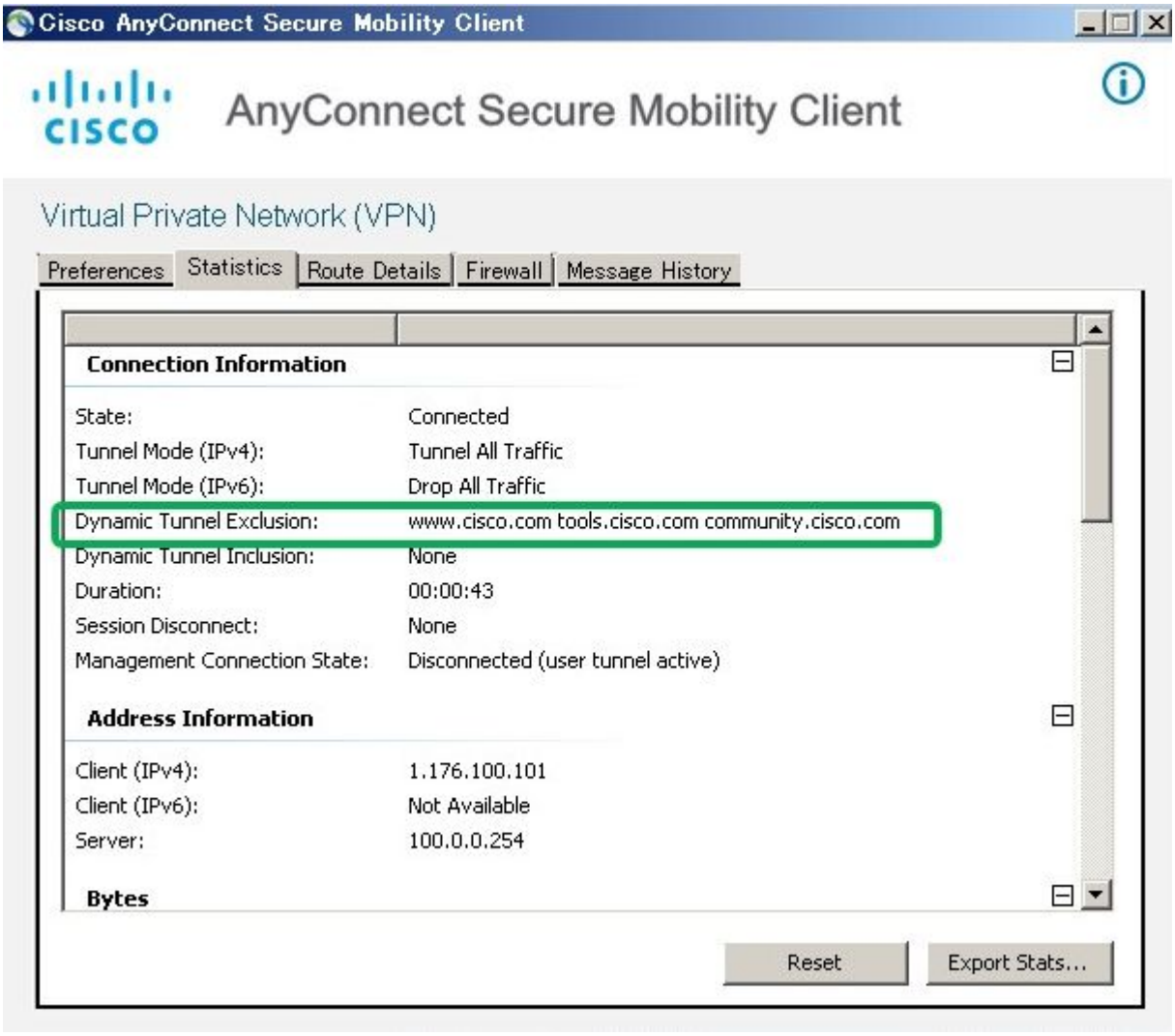
```
group-policy GroupPolicy_AnyConnect-01 internal

group-policy GroupPolicy_AnyConnect-01 attributes


 wins-server none
 dns-server value 10.0.0.0
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelall
 split-tunnel-network-list value SplitACL
 default-domain value cisco.com

 anyconnect-custom dynamic-split-exclude-domains value cisco-site
```

Limites

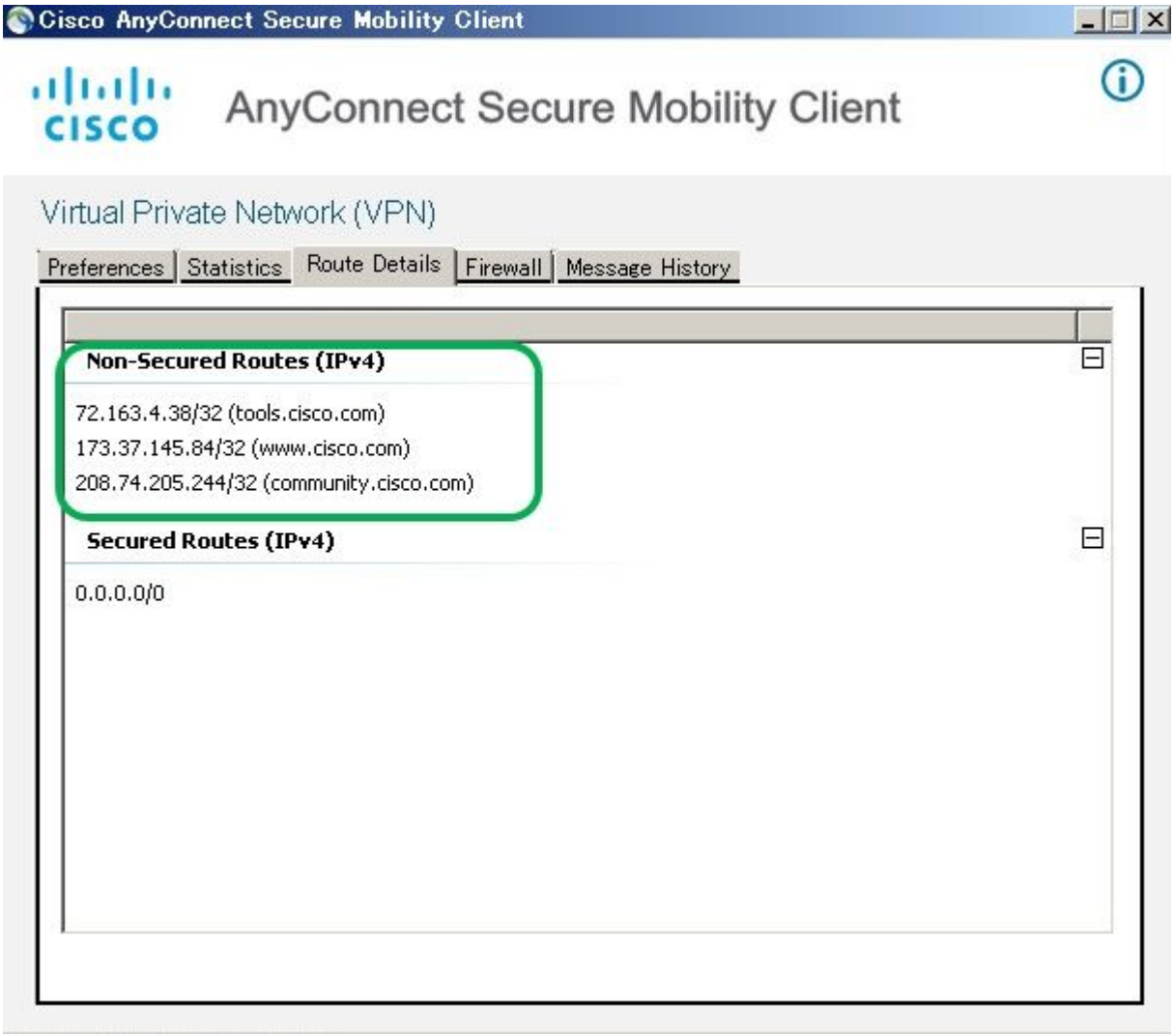
- ASA version 9.0 ou ultérieure est nécessaire pour utiliser les attributs personnalisés de Dynamic Split Tunneling.
- Le caractère générique n'est pas pris en charge dans le champ Valeurs.
- La tunnellisation partagée dynamique n'est pas prise en charge sur les appareils iOS (Apple) (Demande d'amélioration : 'ID de bogue Cisco CSCvr54798'.

Vérifier

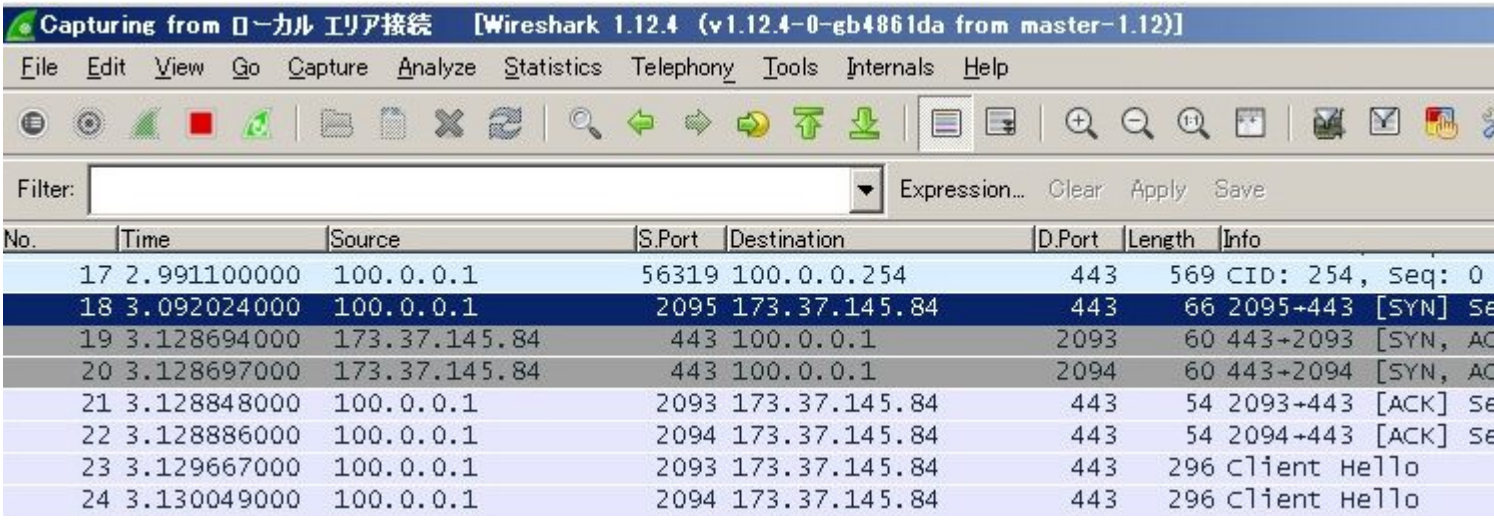
Afin de vérifier la configuration **Dynamic Tunnel Exclusions,** Lancer **AnyConnect** sur le client, cliquez sur **Advanced Window** > **Statistics,** comme l'illustre l'image :



Vous pouvez également accéder à **Advanced Window** > **Route Details** dans lequel vous pouvez vérifier **Dynamic Tunnel Exclusions** sont répertoriées sous **Non-Secured Routes,** comme illustré dans l'image.



Dans cet exemple, vous avez configuré www.cisco.com sous **Dynamic Tunnel Exclusion list** et la capture Wireshark collectée sur l'interface physique du client AnyConnect confirme que le trafic vers www.cisco.com (198.51.100.0) n'est pas chiffré par DTLS.



Dépannage

Dans le cas où le caractère générique est utilisé dans le champ Valeurs

Si un caractère générique est configuré dans le champ Valeurs, par exemple, ***.cisco.com** est configuré dans Valeurs, la session AnyConnect est déconnectée, comme indiqué dans les journaux :

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01>
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Firs
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Clie
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv4
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (172
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> WebV
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session d
```

> **Remarque** : vous pouvez également utiliser le domaine **cisco.com** dans Valeurs pour autoriser les noms de domaine complets tels que www.cisco.com et tools.cisco.com.

Dans le cas où les routes non sécurisées ne s'affichent pas dans l'onglet Détails de route

Le client AnyConnect apprend et ajoute automatiquement lâ€™adresse IP et le nom de domaine complet dans lâ€™onglet Détails de la route, lorsque le client initie le trafic pour les destinations exclues.

Afin de vérifier que les utilisateurs AnyConnect sont affectés à la stratégie de groupe Anyconnect correcte, vous pouvez exécuter la commande '**show vpn-sessiondb anyconnect filter name**
'

<#root>

```
ASAv10# show vpn-sessiondb anyconnect filter name cisco

Session Type: AnyConnect

Username     : cisco                  Index : 7
Assigned IP  : 172.16.0.0          Public IP : 10.0.0.0
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx     : 7795373                Bytes Rx : 390956
```

Group Policy : GroupPolicy_AnyConnect-01

```
Tunnel Group : AnyConnect-01
Login Time   : 13:20:48 UTC Tue Mar 31 2020
Duration     : 20h:19m:47s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN : none
Audt Sess ID : 019600a9000070005e8343b0
Security Grp : none
```

Dépannage général

Vous pouvez utiliser l'outil DART (AnyConnect Diagnostics and Reporting Tool) afin de collecter les données utiles pour résoudre les problèmes d'installation et de connexion d'AnyConnect. Lâ€™assistant DART est utilisé sur lâ€™ordinateur qui utilise AnyConnect. Lâ€™outil DART regroupe les journaux, lâ€™état et les renseignements de diagnostic pour lâ€™analyse du Centre dâ€™assistance technique de Cisco et nâ€™exige aucun privilège administrateur pour fonctionner sur la machine du client.

Informations connexes

- **Guide de l'administrateur du client Cisco AnyConnect Secure Mobility, version 4.7 - À propos de la tunnellisation partagée dynamique**
- **ASDM Book 3 : Cisco ASA Series VPN ASDM Configuration Guide, 7.13 - Configure Dynamic Split Tunneling**

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.