Configuration de la transmission tunnel partagée dynamique ASA et AnyConnect

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configuration
  - Diagramme du réseau
  - Étape 1 : création d'attributs personnalisés AnyConnect
  - Étape 2 : création d'un nom personnalisé AnyConnect et configuration des valeurs
  - Étape 3. Ajouter un type et un nom à la stratégie de groupe
- Exemple de configuration CLI
- Limites
- Vérifier
- Dépannage
  - Si un caractère générique est utilisé dans le champ Valeurs
  - Si les routes non sécurisées ne sont pas visibles dans l'onglet Détails de la route
  - Dépannage général
- Informations connexes

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 logicielles 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 l’incidence possible des commandes.

Informations générales

La transmission tunnel partagée AnyConnect permet au client Cisco AnyConnect Secure Mobility d'accéder de manière sécurisée 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 peut 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.

Comme le client AnyConnect Secure Mobility fournit une tunnellisation partagée vers une plage de sous-réseaux statiques, un hôte ou un pool d'IPV4 ou d'IPV6, il devient difficile pour les administrateurs réseau d'exclure des domaines/noms de domaine complets pendant qu'ils configurent 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.

En utilisant la tunnellisation Dynamic Split Exclude, AnyConnect résout dynamiquement l'adresse IPv4/IPv6 de l'application hébergée et garantit les modifications nécessaires dans la table de routage et les filtres pour permettre la connexion à l'extérieur du tunnel.

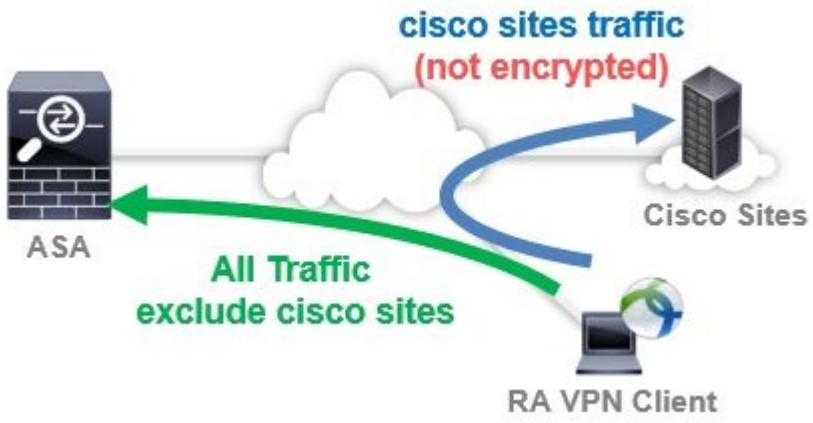
À partir de AnyConnect 4.5, la technologie Dynamic Spit Tunneling peut être utilisée. AnyConnect résout dynamiquement l'adresse IPv4/IPv6 de l'application hébergée et apporte les modifications nécessaires à la table de routage et aux filtres pour permettre la connexion en dehors du tunnel

Configuration

Cette section explique comment configurer le client pour la mobilité sécurisée Cisco AnyConnect sur l'ASA.

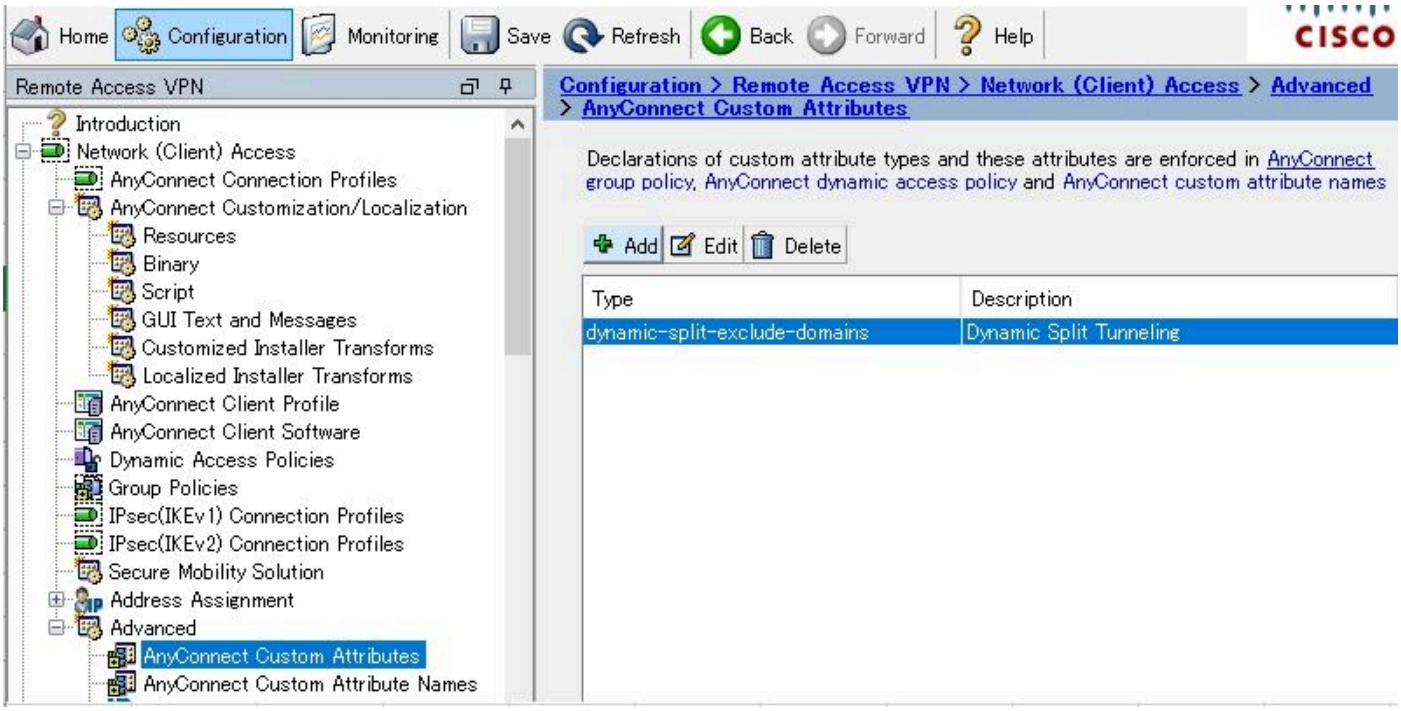
Diagramme du réseau

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



Étape 1 : création d'attributs personnalisés AnyConnect

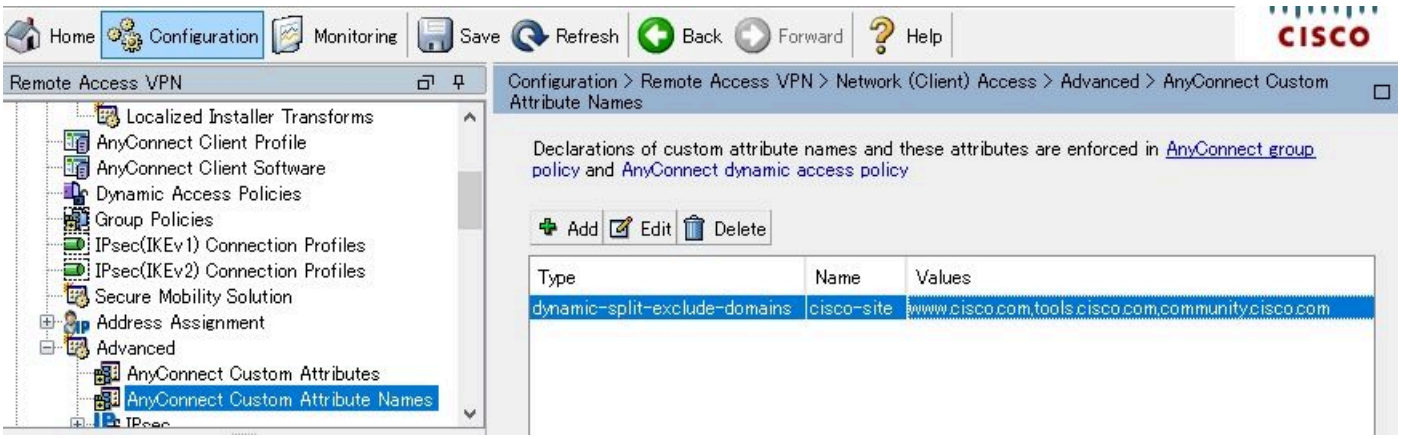
Accédez à Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Cliquez sur le bouton Add, et définissez l'attribut dynamic-split-exclude-domains et la description facultative.



Étape 2 : création d’un nom personnalisé AnyConnect et configuration des valeurs

Accédez à Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Cliquez sur le bouton Add, et définissez l'attribut dynamic-split-exclude-domains créé précédemment à partir de Type, un nom arbitraire et Values.

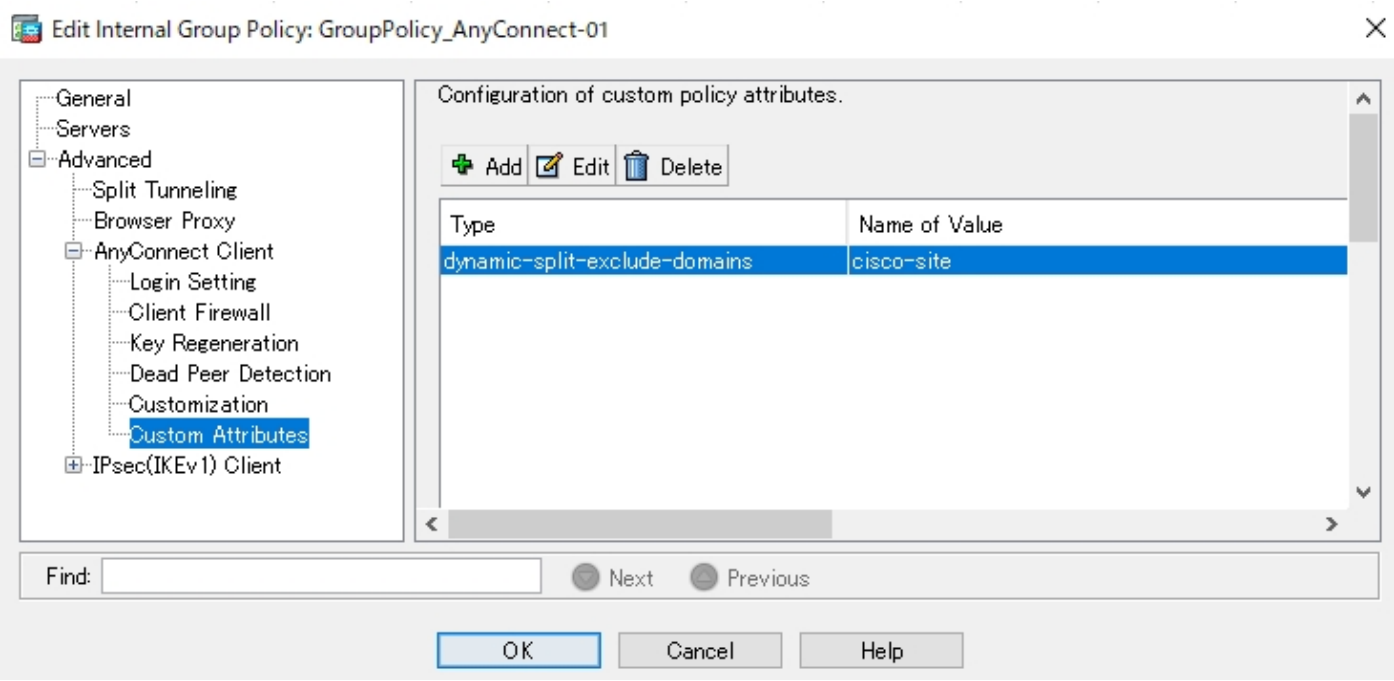
Veillez à ne pas entrer d'espace dans le champ Nom (par exemple, il est possible d'utiliser cisco-site, mais il est impossible d'utiliser cisco-site). Lorsque plusieurs domaines ou noms de domaine complets dans Valeurs sont enregistrés, séparez-les par une virgule (,).



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

Accédez à Configuration > Remote Access VPN > Network (Client) Access > Group Policies et

sélectionnez une stratégie de groupe. Accédez ensuite à Advanced > AnyConnect Client > Custom Attributes et ajoutez le type et le nom configurés.



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

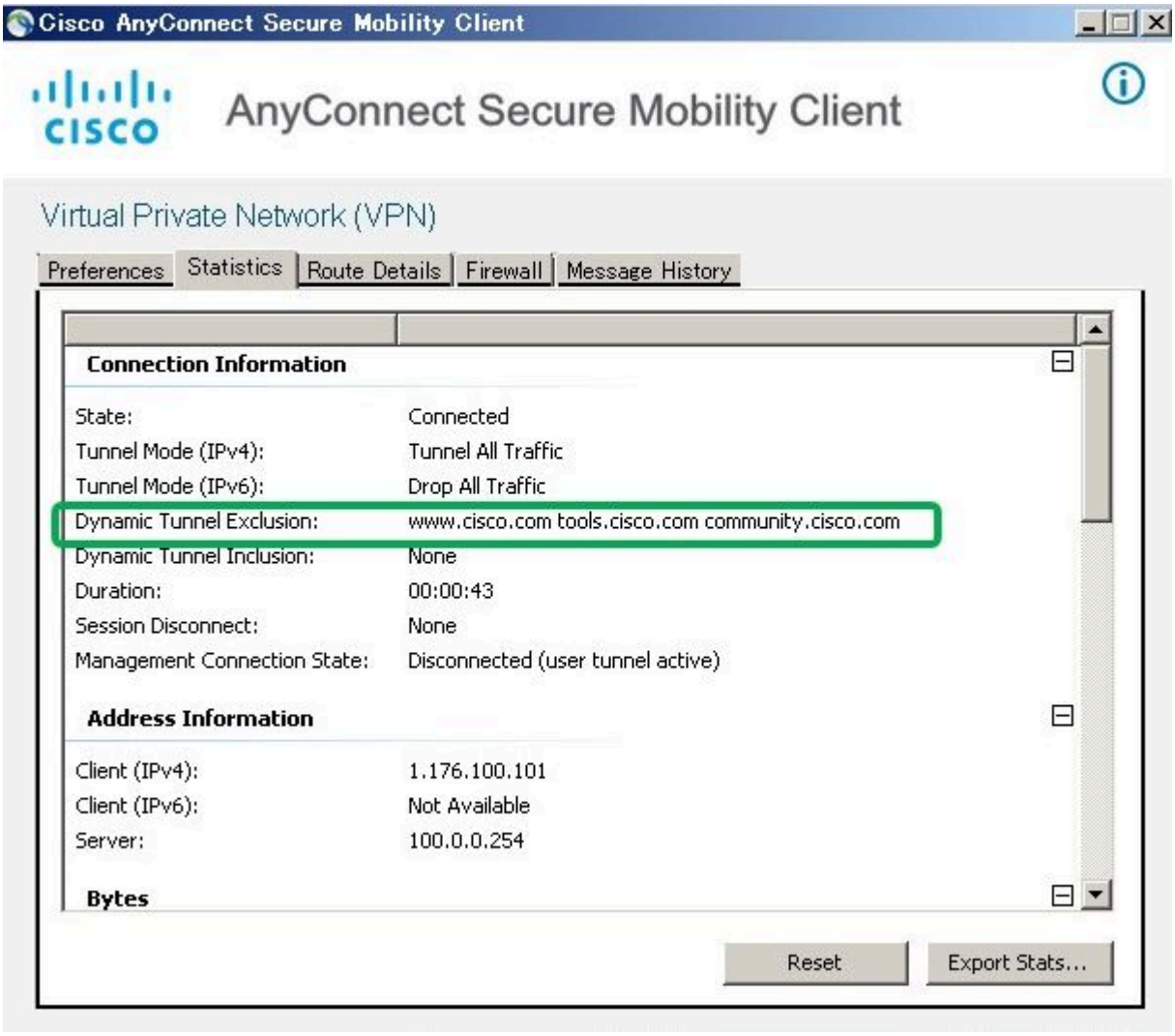
 AnyConnect-custom dynamic-split-exclude-domains value cisco-site
```

Limites

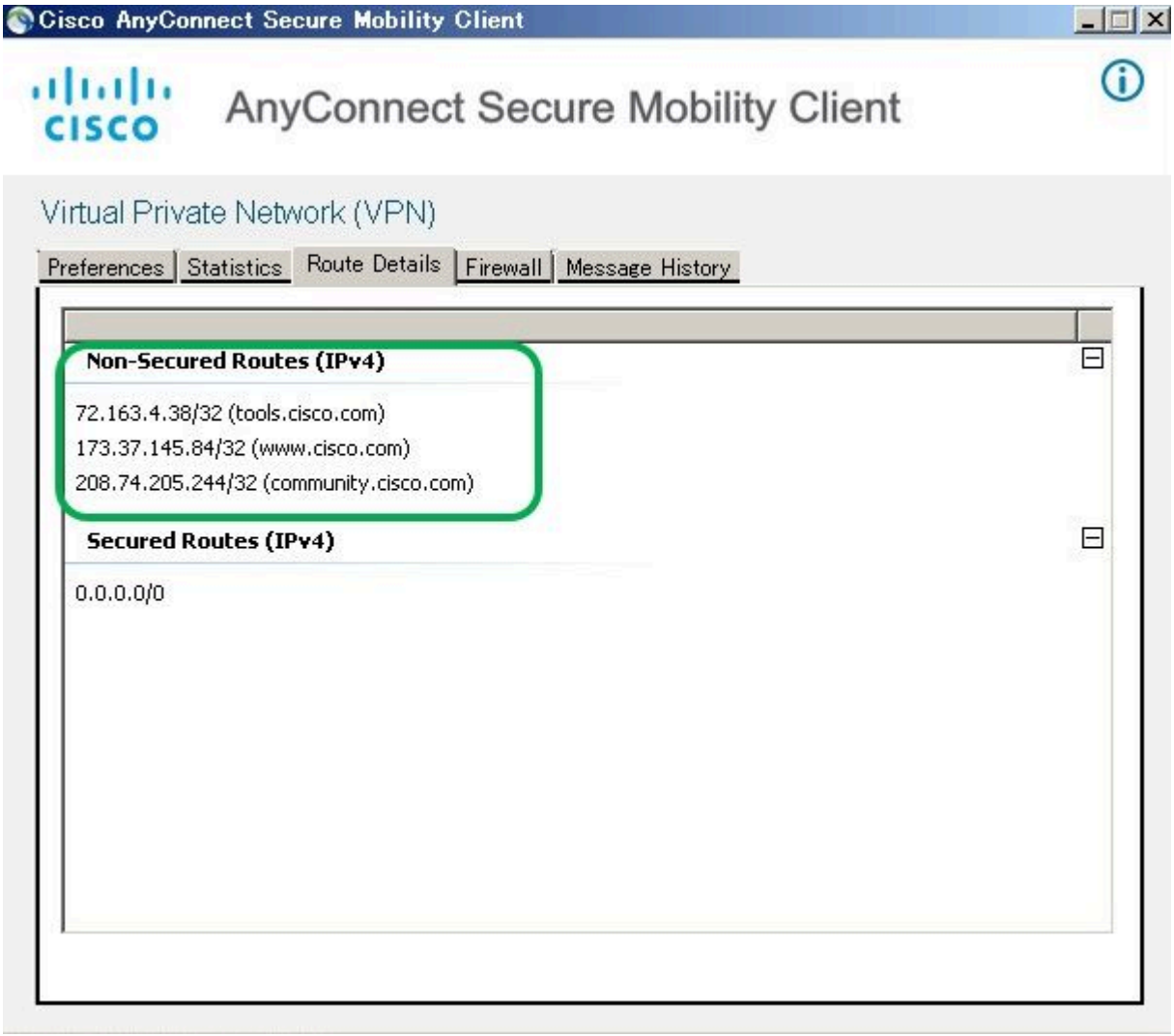
- ASA version 9.0 ou ultérieure est requis pour utiliser les attributs personnalisés de la transmission tunnel partagée dynamique.
- Un caractère générique dans le champ Valeurs n'est pas pris en charge.
- La tunnellisation partagée dynamique n'est pas prise en charge sur les périphériques Cisco IOS® (Apple) (demande d'amélioration : ID de bogue Cisco CSCvr54798).

Vérifier

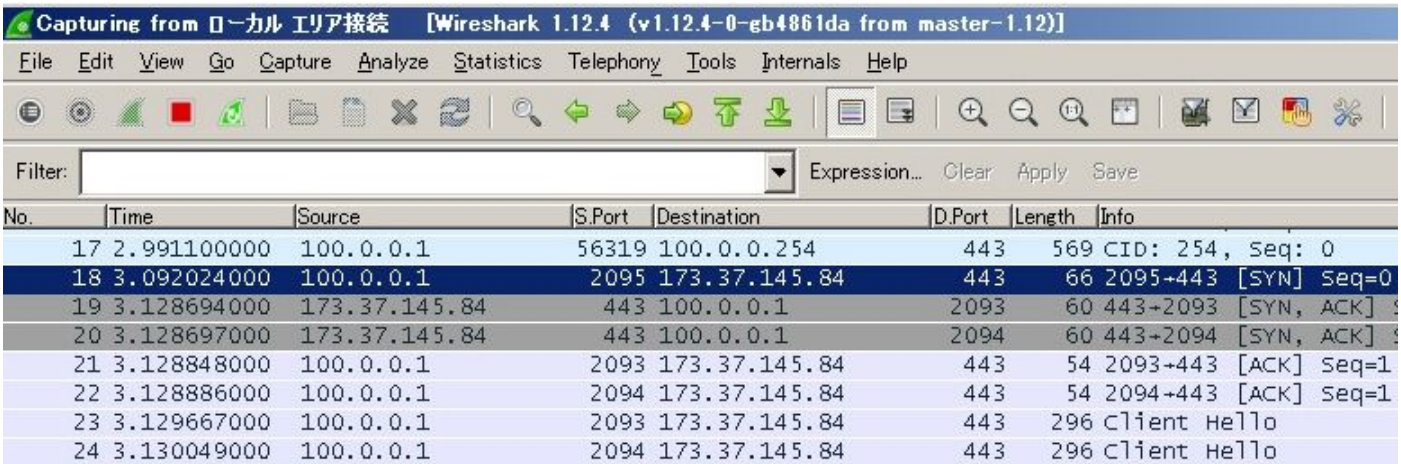
Pour vérifier les exclusions de tunnel dynamiques configurées,AnyConnectlancez le logiciel sur le client, sélectionnez Advanced Window > Statistics.



Vous pouvez également accéder à l'onglet Advanced Window > Route Details, où vous pouvez vérifier que les exclusions de tunnel dynamique sont répertoriées sous Non-Secured Routes.



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



Dépannage

Si un 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> Fir
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> Cli
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (17
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> Web
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session
```

Remarque : Vous pouvez également utiliser le domaine cisco.com dans Values pour autoriser les noms de domaine complets tels que www.cisco.com et tools.cisco.com.

Si les routes non sécurisées ne sont pas visibles dans l'onglet Détails de la route

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

Pour 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 <username>.

<#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) pour collecter des données utiles au dépannage des problèmes d'installation et de connexion d'AnyConnect. L'assistant DART est utilisé sur l'ordinateur qui utilise AnyConnect. DART rassemble les journaux, l'état et les informations de diagnostic pour l'analyse du centre d'assistance technique Cisco (TAC) et ne nécessite pas de privilèges d'administrateur pour s'exécuter sur l'ordinateur client.

Informations connexes

- Guide de l'administrateur du client Cisco AnyConnect Secure Mobility, version 4.7 - À propos de la tunnellisation partagée dynamique
- Livre 3 ASDM : Guide de configuration de l'ASDM VPN de la gamme Cisco ASA, 7.13 - Configuration de la tunnellisation partagée dynamique

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.