Configuration d'un tunnel partagé dynamique AnyConnect sur FTD géré par FMC

Table des matières

Introduction

Ce document décrit comment configurer AnyConnect Dynamic Split Tunnel sur Firepower Threat Defense (FTD) géré par Firepower Management Center (FMC).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco AnyConnect
- Connaissances de base de FMC

Composants utilisés

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

- FMC version 7.0
- FTD version 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 configuration AnyConnect Dynamic Split Tunnel sur FTD géré par FMC est entièrement disponible sur FMC version 7.0 et ultérieure. Si vous exécutez une version plus ancienne, vous devez la configurer via FlexConfig comme indiqué dans les Déploiements VPN AnyConnect avancés pour Firepower Threat Defense avec FMC.

Avec la configuration de tunnel partagé dynamique, vous pouvez affiner la configuration de tunnel partagé en fonction des noms de domaine DNS. Étant donné que les adresses IP associées aux noms de domaine complets (FQDN) peuvent changer, la configuration de tunnel partagé basée sur les noms DNS fournit une définition plus dynamique du trafic inclus ou non dans le tunnel VPN (Virtual Private Network) d'accès à distance. Si des adresses renvoyées pour des noms de domaine exclus se trouvent dans le pool d'adresses inclus dans le VPN, ces adresses sont alors exclues. Les domaines exclus ne sont pas bloqués. Au lieu de cela, le trafic vers ces domaines est maintenu en dehors du tunnel VPN.

Notez que vous pouvez également configurer un tunnel partagé dynamique pour définir les domaines à inclure dans le tunnel qui seraient autrement exclus en fonction de l'adresse IP.

Limites

Actuellement, ces fonctionnalités ne sont toujours pas prises en charge :

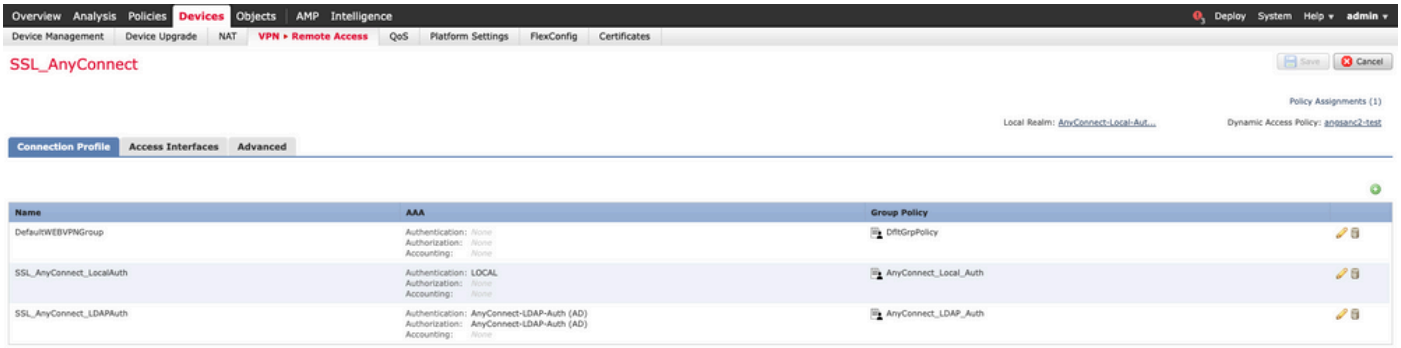
- Dynamic Split Tunnel n'est pas pris en charge sur les appareils iOS (Apple). Voir ID de bogue Cisco CSCvr54798
- Dynamic Split Tunnel n'est pas pris en charge sur les clients Anyconnect Linux. Voir bogue Cisco IDCSCvt64988

Configurer

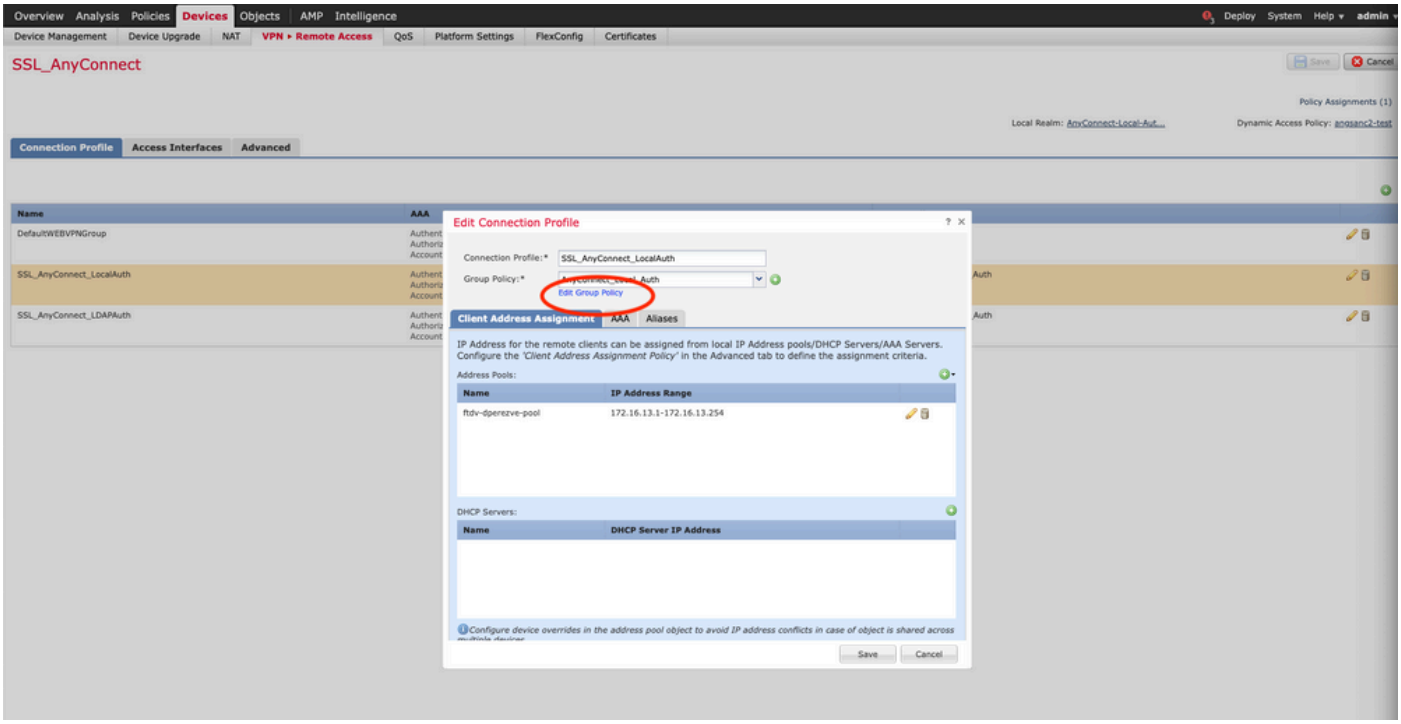
Cette section décrit comment configurer AnyConnect Dynamic Split Tunnel sur FTD géré par FMC.

Étape 1. Modifier la stratégie de groupe pour utiliser le tunnel de fractionnement dynamique

1. Sur le FMC, accédez à **Devices > VPN > Remote Access**, puis sélectionnez le **profil de connexion** auquel vous souhaitez appliquer la configuration.

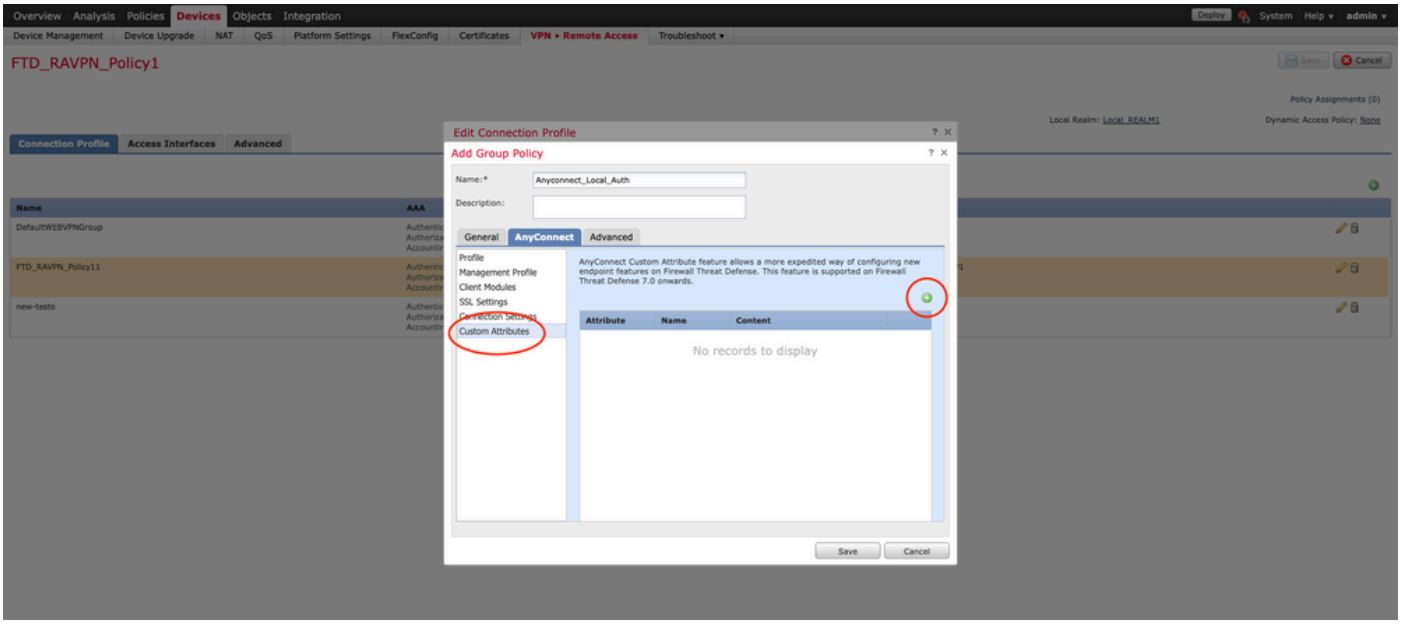


2. Sélectionnez **Modifier la stratégie de groupe** pour modifier l'une des stratégies de groupe déjà créées.

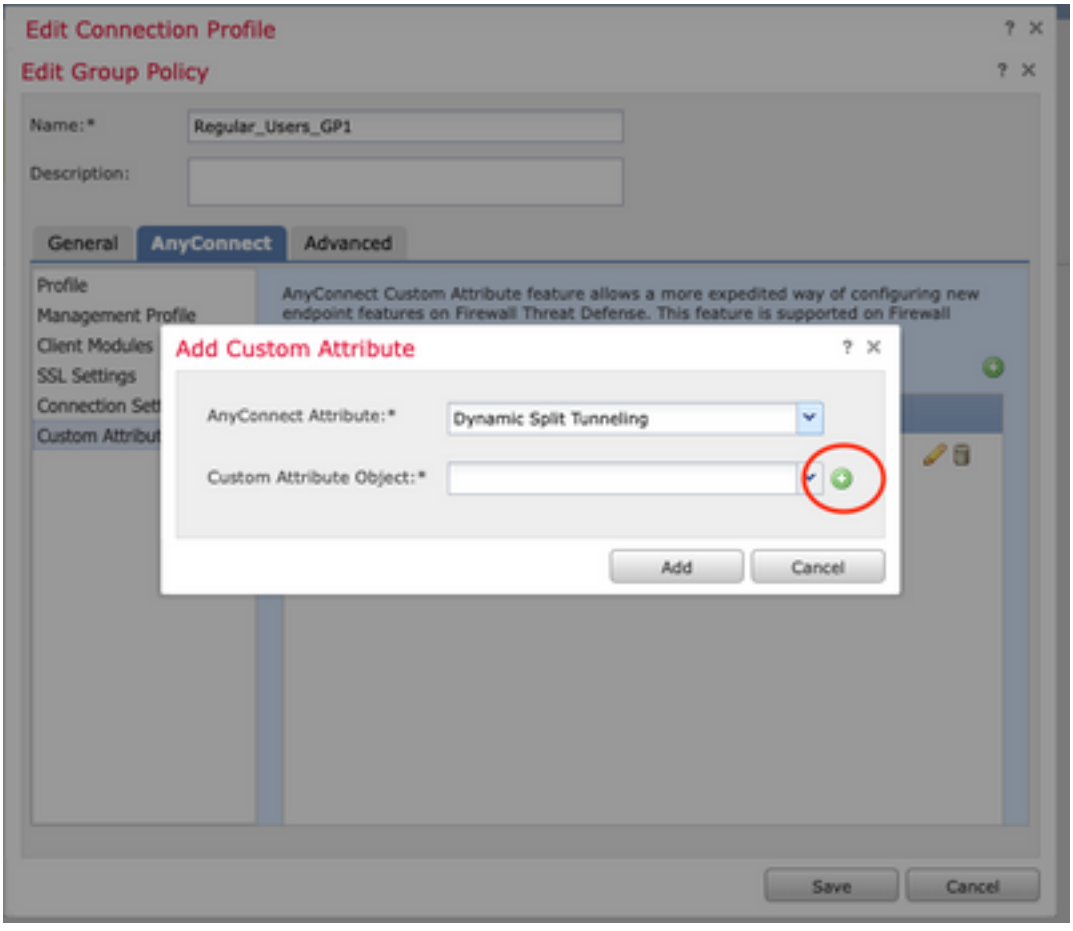


Étape 2. Configuration de l'attribut personnalisé AnyConnect

1. Dans la configuration Stratégie de groupe, accédez à **Anyconnect > Attributs personnalisés**, cliquez sur le bouton **Ajouter (+)** :

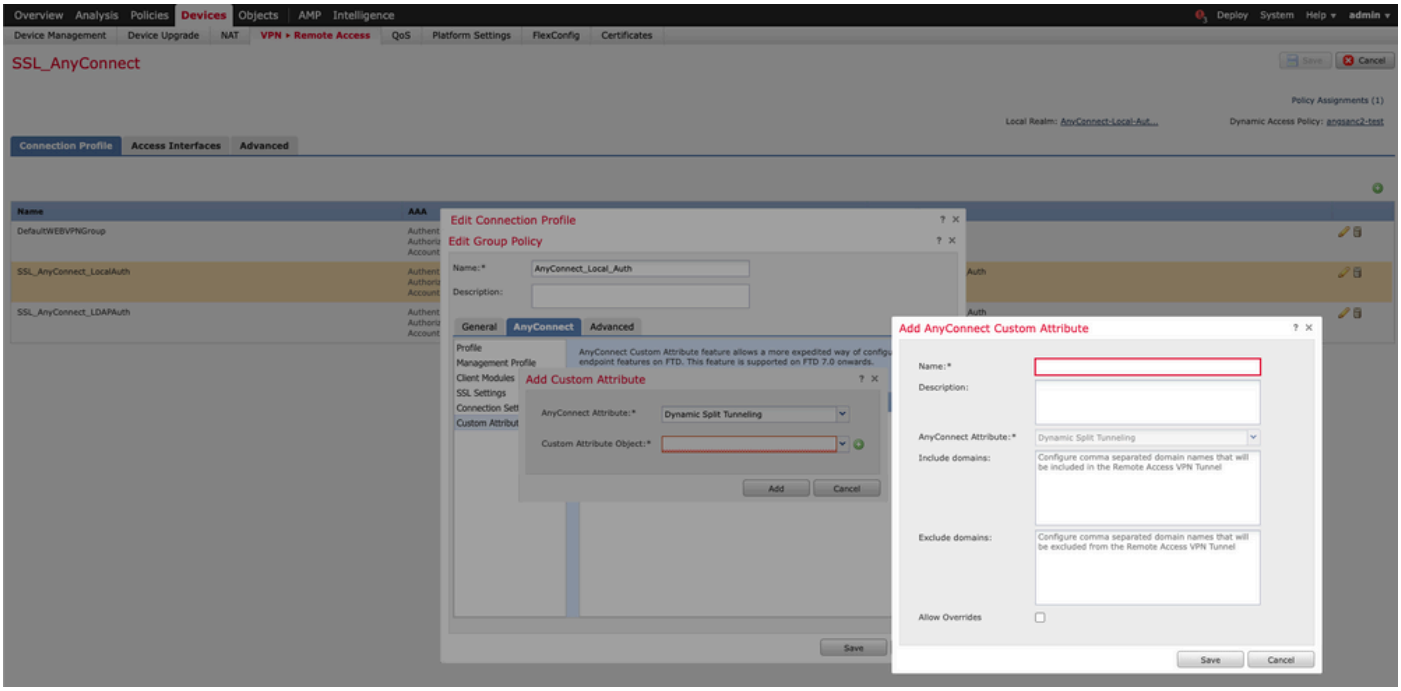


2. Sélectionnez l'attribut **Dynamic Split Tunneling** AnyConnect et cliquez sur le bouton **Add (+)** pour créer un nouvel objet d'attribut personnalisé :

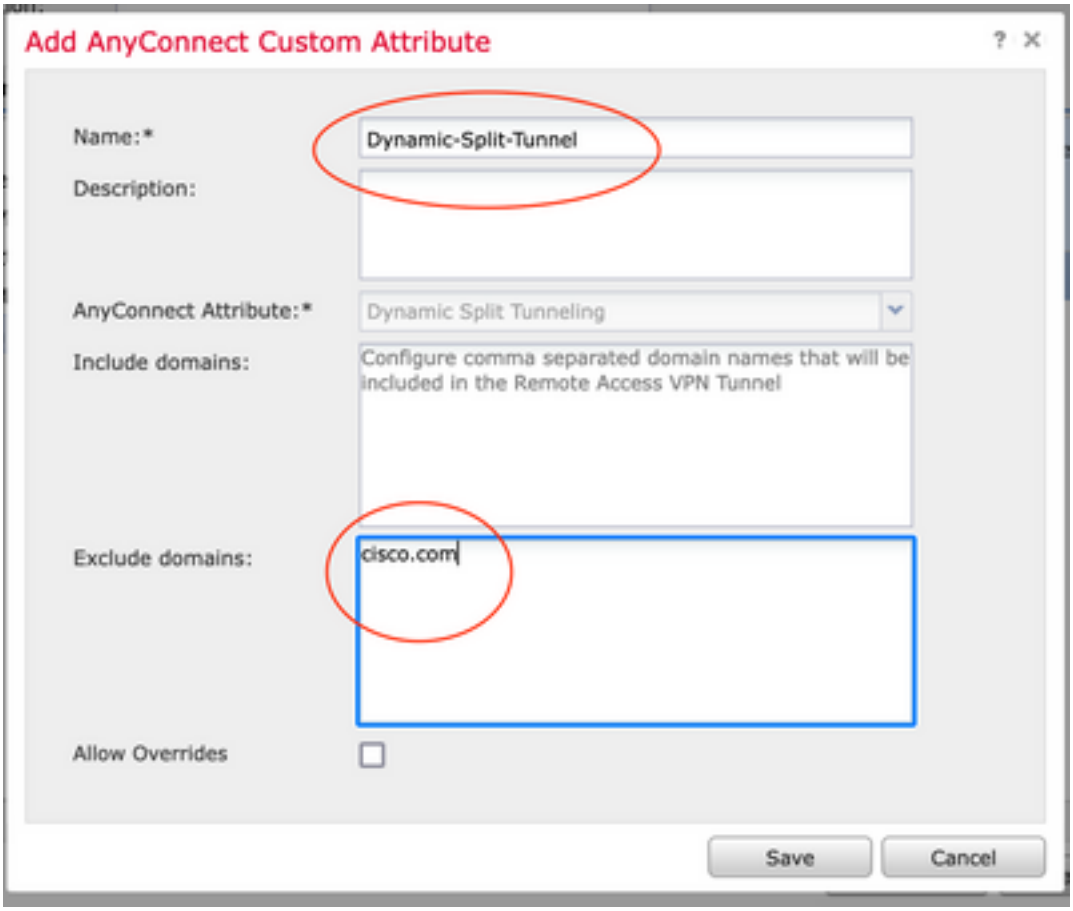


3. Entrez le **nom** de l'**attribut personnalisé AnyConnect** et configurez les domaines à inclure ou à exclure de manière dynamique.

> **Remarque** : vous pouvez uniquement configurer **Inclure des domaines** ou **Exclure des domaines**.

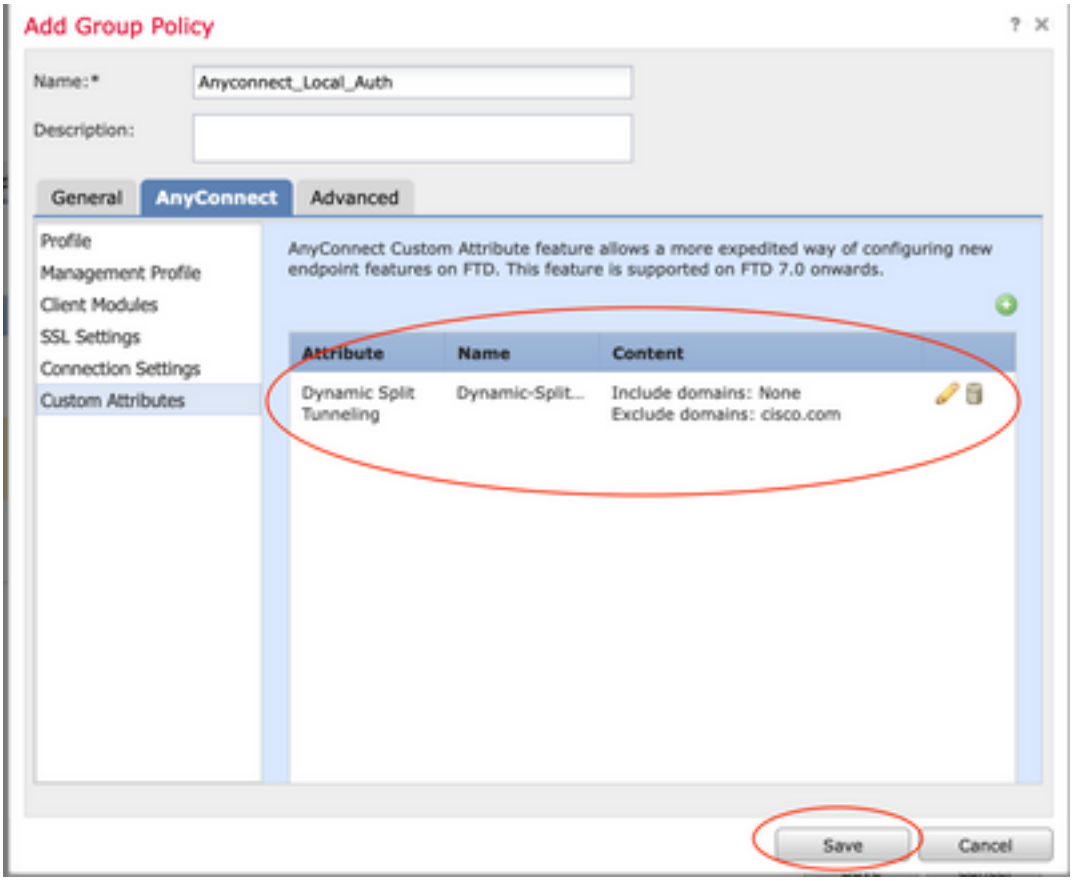


Dans cet exemple, nous avons configuré **cisco.com** en tant que domaine à exclure et nommé l'attribut personnalisé **Dynamic-Split-Tunnel**, comme indiqué dans l'image :



Étape 3. vérification de la configuration, enregistrement et déploiement

Vérifiez que l'attribut personnalisé configuré est correct, enregistrez la configuration et déployez les modifications sur le FTD en question.



Vérifier

Vous pouvez exécuter ces commandes sur le FTD via l'interface de ligne de commande (CLI) pour confirmer la configuration du tunnel partagé dynamique :

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy **<Nom de la stratégie de groupe>**

Dans cet exemple, la configuration est la suivante :

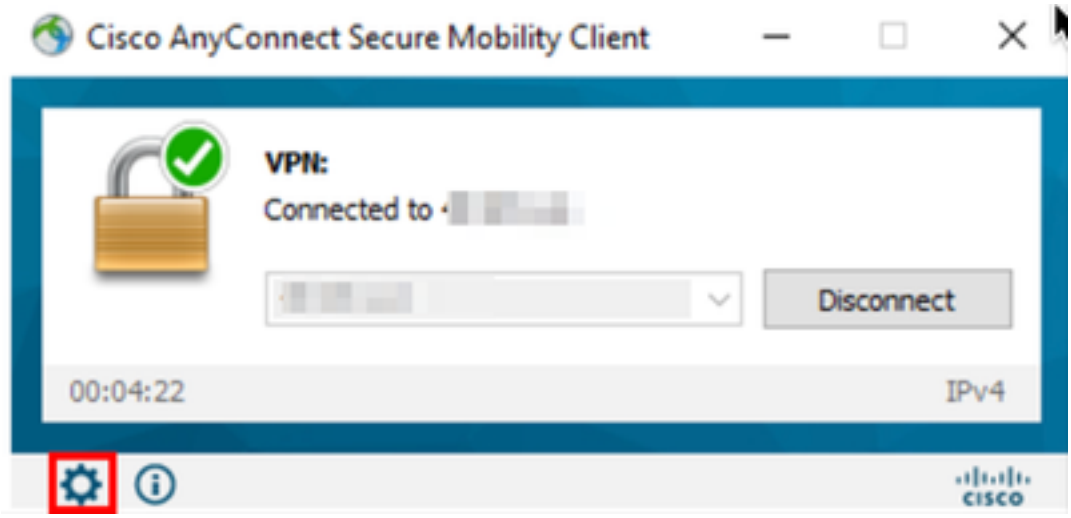
```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
anyconnect-custom dynamic-split-exclude-domains value cisco.com
anyconnect-custom dynamic-split-include-domains none

ftd# show run webvpn
webvpn
enable outside
anyconnect-custom-attr dynamic-split-exclude-domains
```

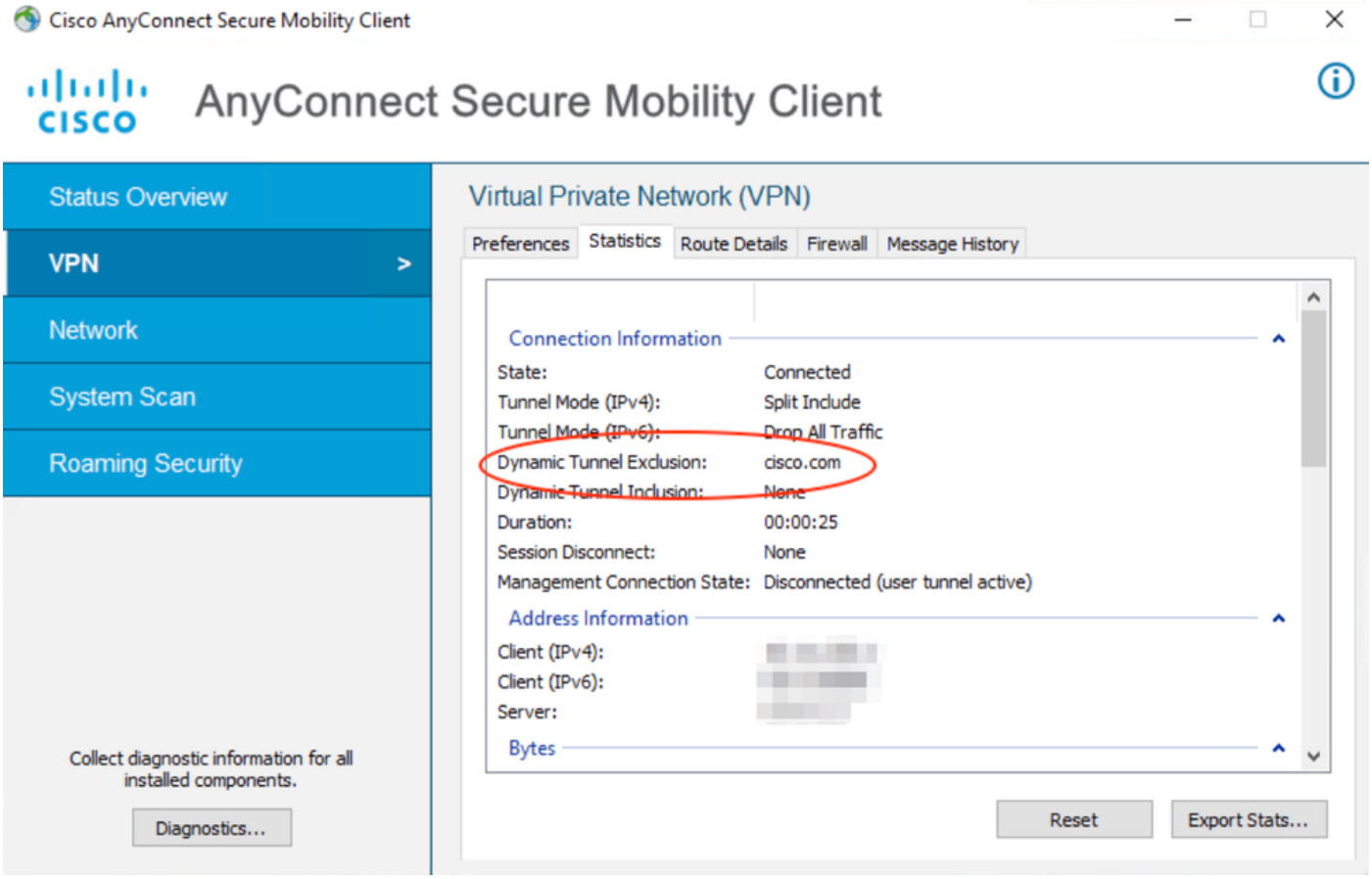
```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
```

Afin de vérifier les exclusions de tunnel dynamique configurées sur le client :

1. Lancez le logiciel AnyConnect et cliquez sur l'icône d'engrenage, comme illustré dans l'image :



2. Accédez à **VPN > Statistics**, et confirmez les domaines affichés sous **Dynamic Split Exclusion/Inclusion** :



Dépannage

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.

L'outil DART regroupe les journaux, l'état et les renseignements de diagnostic pour l'analyse du Centre d'assistance technique de Cisco et n'exige aucun privilège administrateur pour fonctionner sur la machine du client.

Problème

Si un caractère générique est configuré dans les attributs personnalisés AnyConnect, par exemple, ***.cisco.com**, la session AnyConnect est déconnectée.

Solution

Vous pouvez utiliser la valeur de domaine **cisco.com** pour permettre le remplacement du caractère générique. Cette modification vous permet d'inclure ou d'exclure des domaines tels que **www,cisco.com** et **tools.cisco.com**.

Informations connexes

- Pour obtenir de l'aide supplémentaire, veuillez contacter le centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : [Coordonnées du service d'assistance Cisco à l'échelle mondiale.]

- Vous pouvez également visiter la communauté VPN Cisco ici.

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.