FMCによって管理されるFTDでのAnyConnectダイナミックスプリットトンネルの設定

内容

概要

このドキュメントでは、Firepower Management Center(FMC)によって管理されるFirepower Threat Defense(FTD)でAnyConnectダイナミックスプリットトンネルを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco AnyConnect
- FMCの基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- FMCバージョン7.0
- FTDバージョン7.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

背景説明

FMCによって管理されるFTDのAnyConnectダイナミックスプリットトンネル設定は、FMCバージョン7.0以降で完全に使用できます。古いバージョンを実行している場合は、『FMCを使用したFirepower Threat Defenseのための高度なAnyConnect VPN導入』の指示に従って、FlexConfigを使用して設定する必要があります。

ダイナミックスプリットトンネル設定を使用すると、DNSドメイン名に基づいてスプリットトンネル設定を微調整できます。完全修飾ドメイン名(FQDN)に関連付けられたIPアドレスは変更される可能性があるため、DNS名に基づくスプリットトンネルの設定では、リモートアクセス仮想プライベートネットワーク(VPN)トンネルに含まれるトラフィックと含まれないトラフィックをより動的に定義できます。除外されたドメイン名に対して返されたアドレスがVPNに含まれるアドレスプール内にある場合、それらのアドレスは除外されます。除外されたドメインはブロックされません。代わりに、これらのドメインへのトラフィックはVPNトンネルの外部に保持されます。

ダイナミックスプリットトンネルを設定することもできます IPアドレスに基づいて除外されるドメインをトンネルに含めるように定義します。

制限

現在のところ、次の機能はまだサポートされていません。

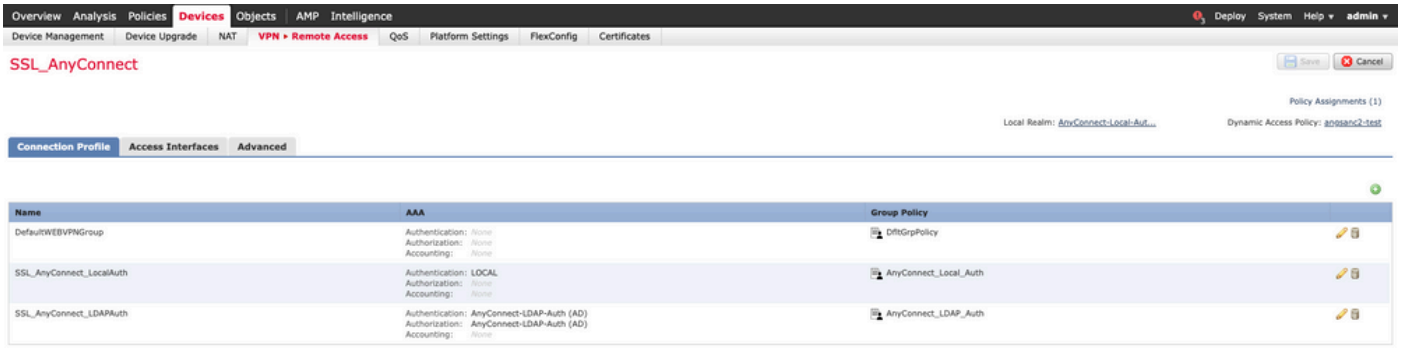
- ダイナミックスプリットトンネルは、iOS(Apple)デバイスではサポートされていません。 Cisco Bug ID CSCvr54798
- ダイナミックスプリットトンネルは、Anyconnect Linuxクライアントではサポートされていません。 Cisco Bug ID CSCvt64988を参照してください。

設定

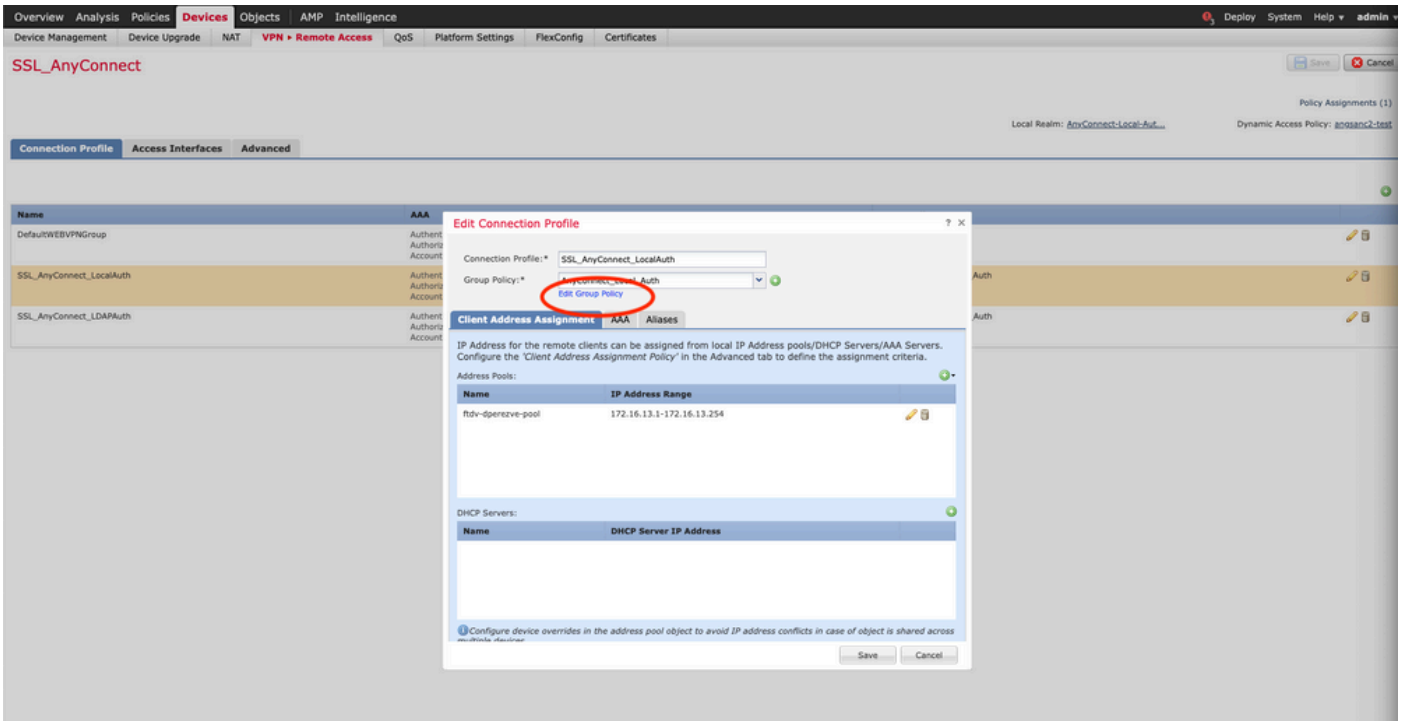
このセクションでは、FMCによって管理されるFTDにAnyConnectダイナミックスプリットトンネルを設定する方法について説明します。

ステップ 1：ダイナミックスプリットトンネルを使用するためのグループポリシーの編集

1. FMCで、[Devices] > [VPN] > [Remote Access] に移動し、設定を適用する**接続プロファイル**を選択します。

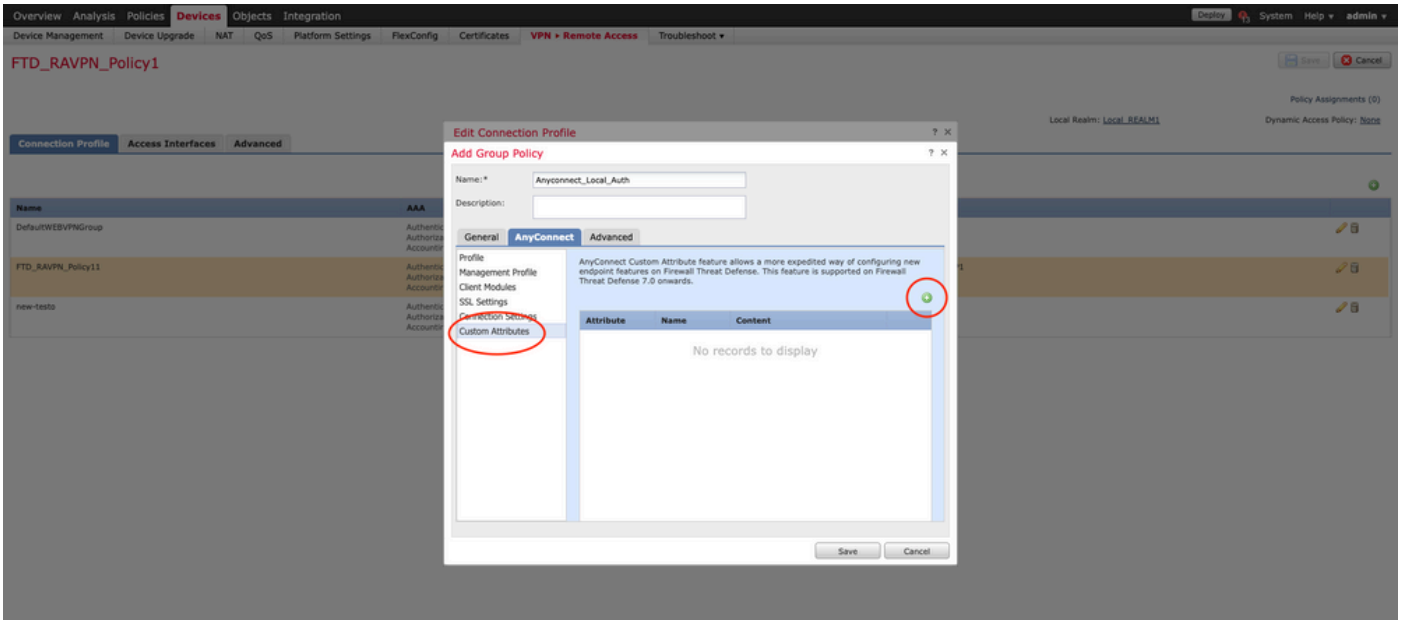


2. [Edit Group Policy] を選択して、作成済みのグループポリシーの1つを変更します。

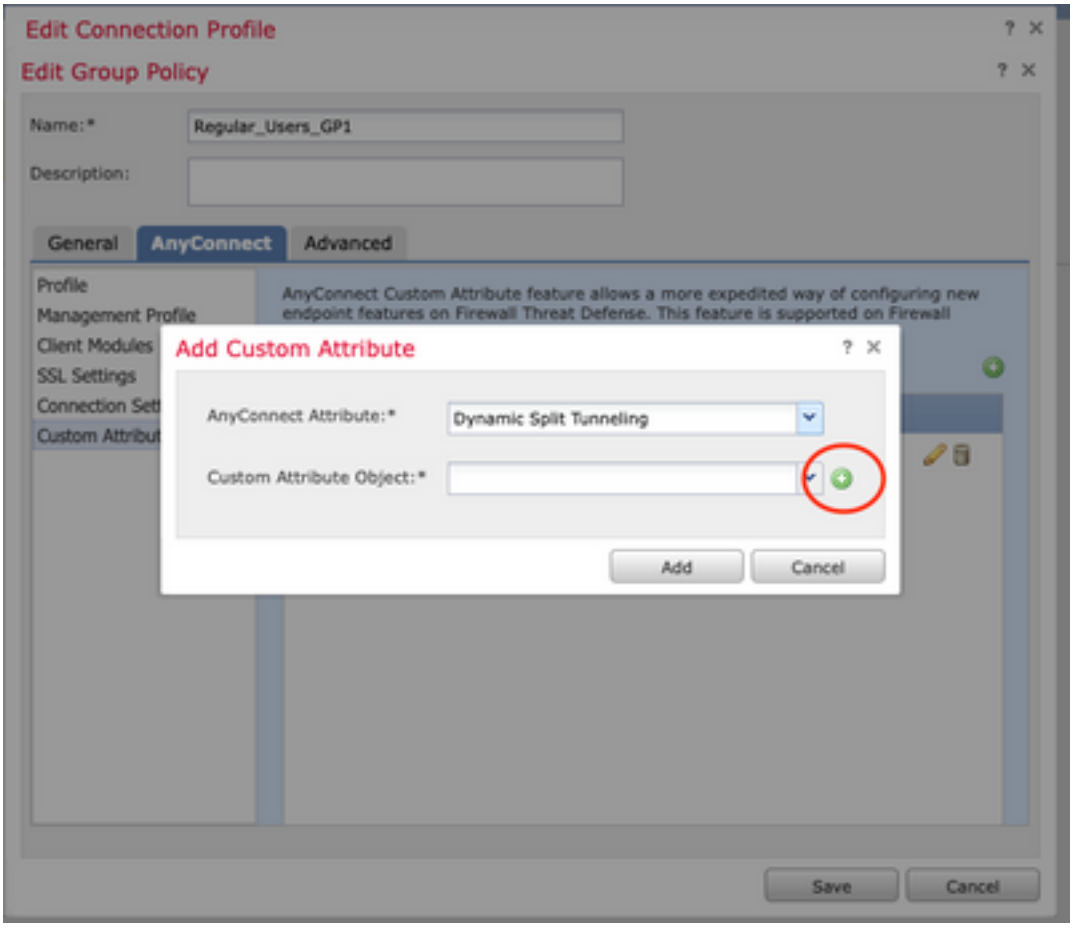


ステップ 2：AnyConnectカスタム属性の設定

1.グループポリシー設定で、[Anyconnect] > [Custom Attributes] に移動し、[Add (+)] ボタンをクリックします。

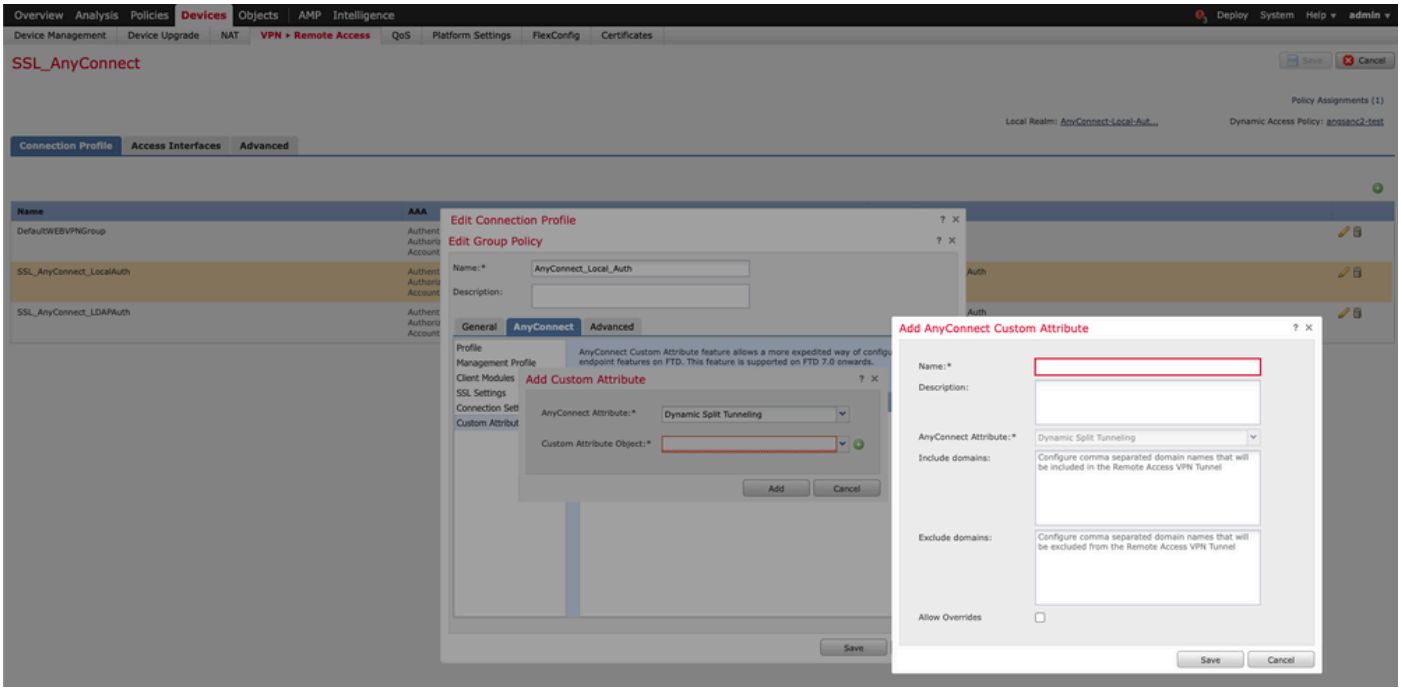


2. [Dynamic Split Tunneling] の[AnyConnect Attribute]を選択し、[Add (+)] ボタンをクリックして新しいカスタム属性オブジェクトを作成します。

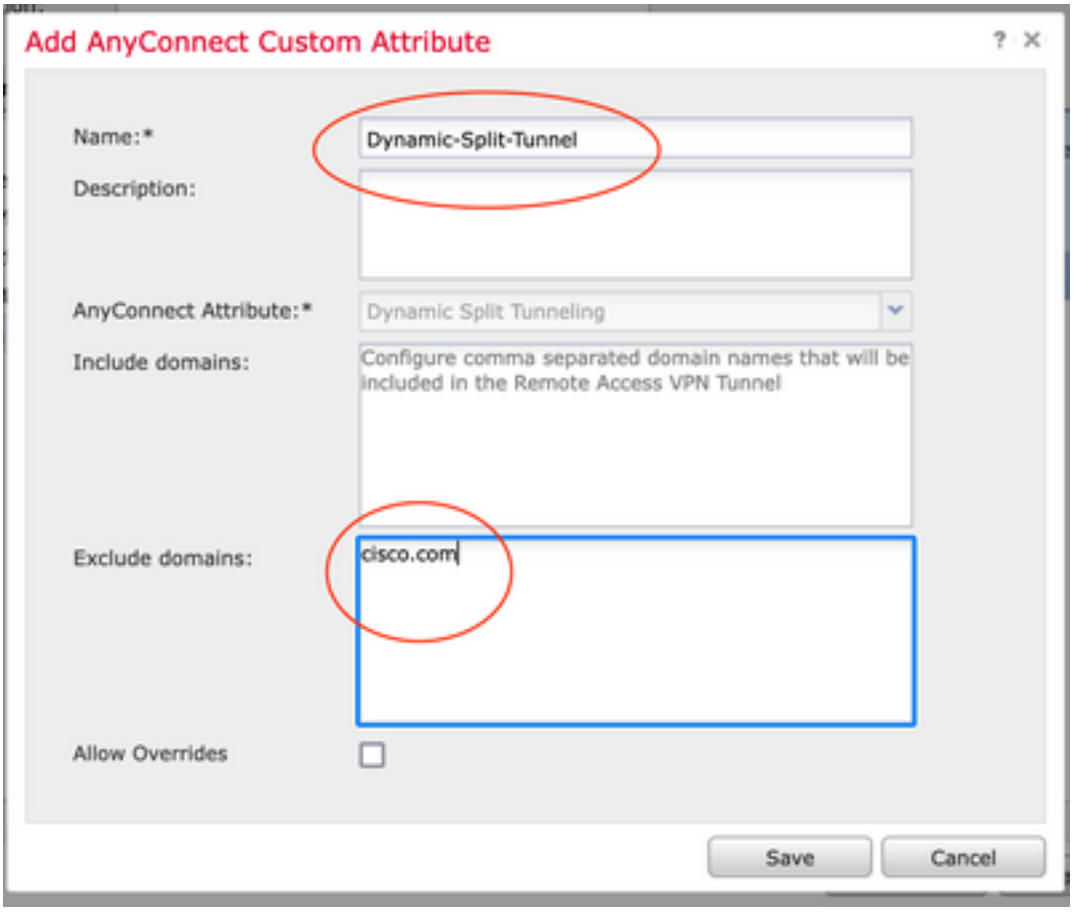


3. [AnyConnect Custom Attribute] の[Name] を入力し、ドメインを動的に含めるか除外するかを設定します。

注：設定できるのは、[Include domains] または[Exclude domains] だけです。

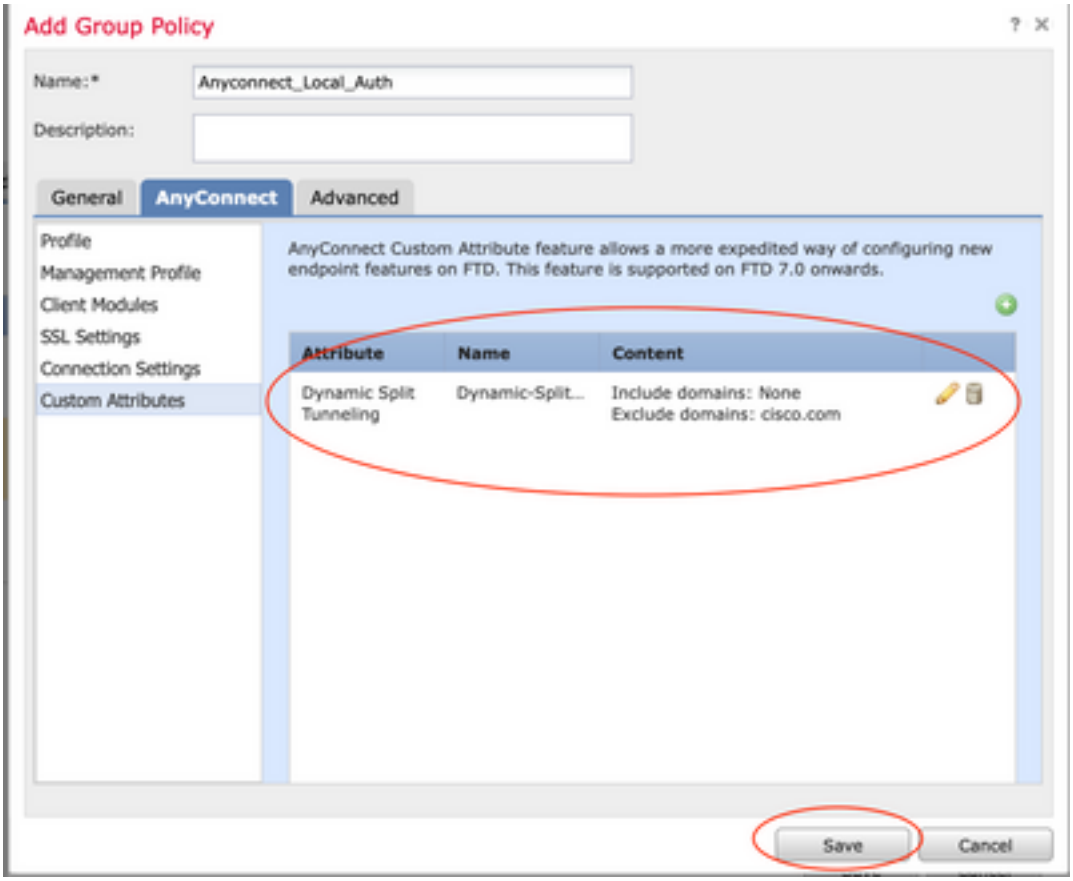


この例では、図に示すように、除外するドメインとしてcisco.comを設定し、カスタム属性にDynamic-Split-Tunnelという名前を付けています。



ステップ 3：設定の確認、保存と展開

設定したカスタム属性が正しいことを確認し、設定を保存して、問題のFTDに変更を適用します。



確認

Command Line Interface（CLI；コマンドラインインターフェイス）を使用してFTDで次のコマンドを実行し、ダイナミックスプリットトンネルの設定を確認できます。

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy **<グループポリシーの名前>**

この例では、設定は次のようになります。

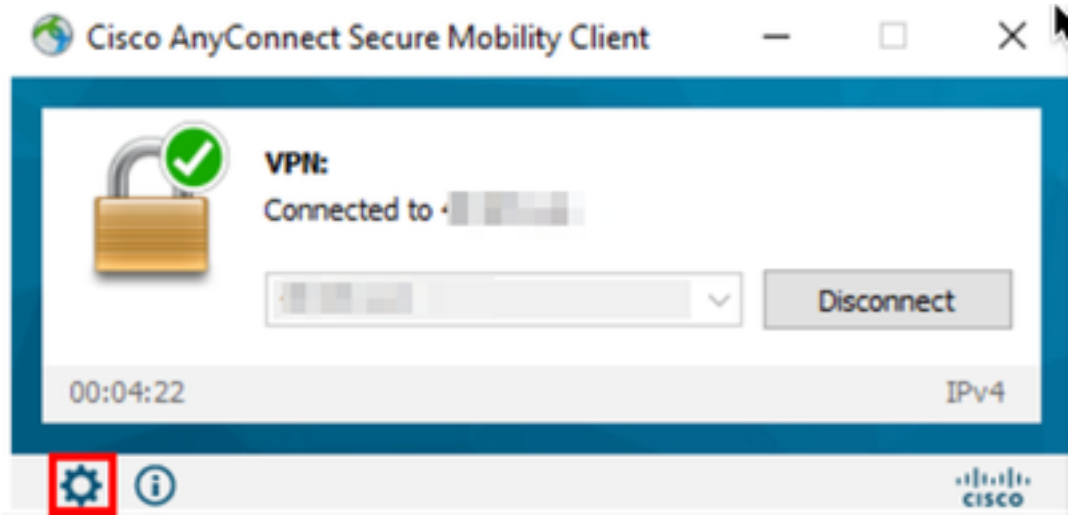
```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list 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
```

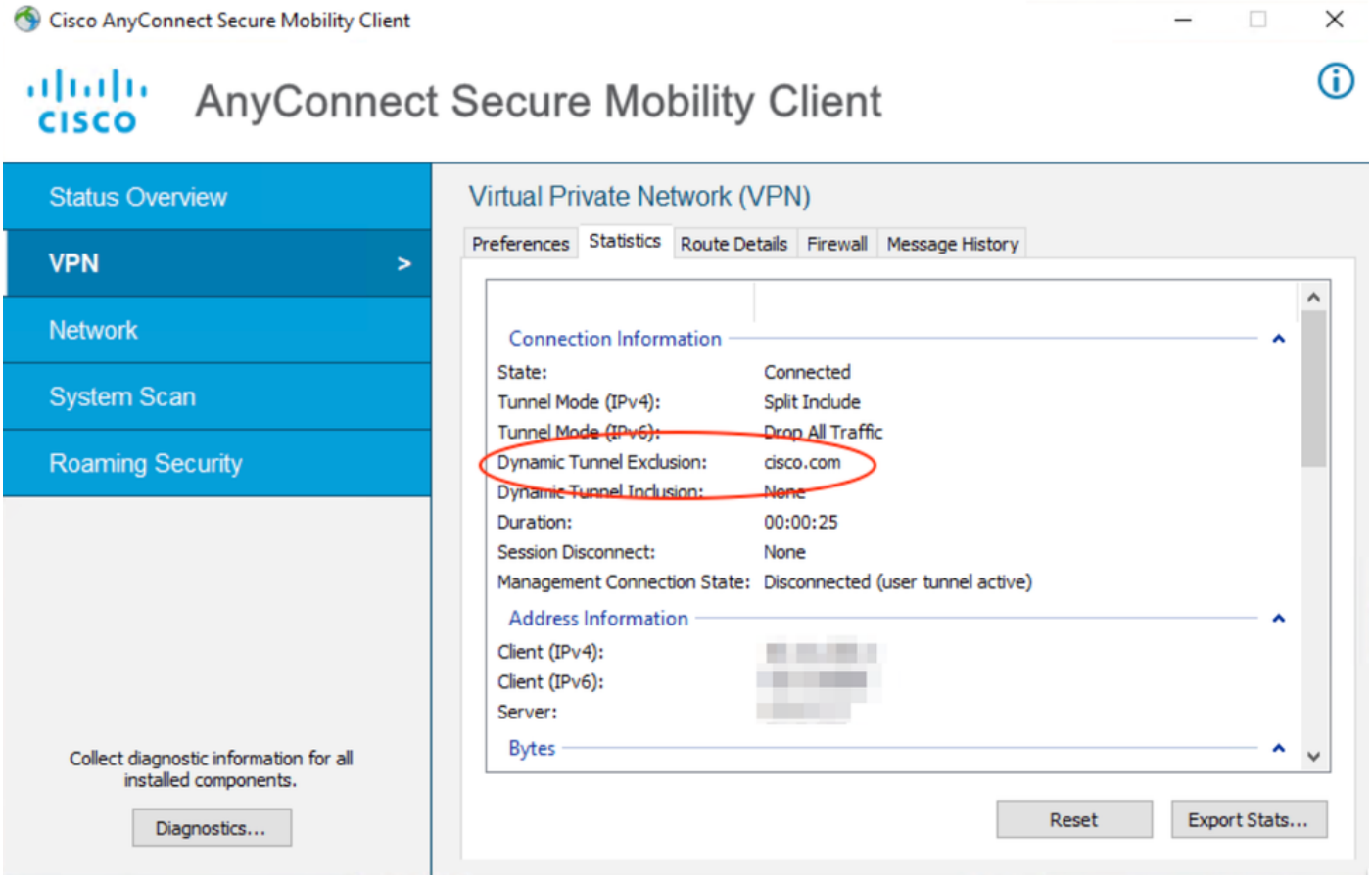
```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml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

クライアントで設定されているダイナミックトンネル除外を確認するには、次の手順を実行します。

1. AnyConnectソフトウェアを起動し、次の図に示すように歯車アイコンをクリックします。



2. [VPN] > [Statistics] に移動し、[Dynamic Split Exclusion/Inclusion] に表示されるドメインを確認します。



トラブルシュート

AnyConnect Diagnostics and Reporting Tool(DART)を使用して、AnyConnectのインストールおよび接続の問題のトラブルシューティングに役立つデータを収集できます。

DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。クライアントマシンで実行するために管理者権限は不要です。

問題

AnyConnectカスタム属性(***.cisco.com**など)にワイルドカードが設定されている場合、AnyConnectセッションは切断されます。

解決方法

cisco.comドメイン値を使用して、ワイルドカードを置き換えることができます。この変更により、**www,cisco.com**や**tools.cisco.com**などのドメインを含めるか除外するかを選択できます。

関連情報

- 詳細については、Technical Assistance center(TAC)にお問い合わせください。有効なサポート契約が必要です。 [各国のシスコ サポートの連絡先.]
- また、Cisco VPN Community here.

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。