Konfiguration eines dynamischen AnyConnect Split-Tunnels auf einem von FMC verwalteten FTD

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den dynamischen AnyConnect Split-Tunnel auf dem vom FirePOWER Management Center (FMC) verwalteten FirePOWER Threat Defense (FTD) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco AnyConnect
- Grundkenntnisse von FMC

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- FMC Version 7.0
- FTD Version 7.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die AnyConnect Dynamic Split Tunnel-Konfiguration auf FTD, die von FMC verwaltet wird, ist ab FMC-Version 7.0 vollständig verfügbar. Wenn Sie eine ältere Version ausführen, müssen Sie diese über FlexConfig konfigurieren, wie in Advanced AnyConnect VPN Deployments for Firepower Threat Defense with FMC beschrieben.

Mit der Konfiguration des Dynamic Split Tunnels können Sie die Split-Tunnel-Konfiguration basierend auf DNS-Domänennamen optimieren. Da sich die IP-Adressen ändern können, die mit vollqualifizierten Domänennamen (FQDN) verknüpft sind, bietet die Konfiguration von Split-Tunneln auf Basis von DNS-Namen eine dynamischere Definition, welcher Datenverkehr im Virtual Private Network (VPN)-Tunnel für den Remote-Zugriff enthalten ist oder nicht. Wenn Adressen, die für ausgeschlossene Domänennamen zurückgegeben werden, innerhalb des im VPN enthaltenen Adresspools liegen, werden diese Adressen dann ausgeschlossen. Ausgeschlossene Domänen werden nicht blockiert. Stattdessen wird der Datenverkehr zu diesen Domänen außerhalb des VPN-Tunnels gehalten.

Beachten Sie, dass Sie auch Dynamic Split Tunnel konfigurieren können. Domänen definieren, die in den Tunnel aufgenommen werden sollen und andernfalls basierend auf der IP-Adresse ausgeschlossen würden.

Einschränkungen

Diese Funktionen werden derzeit noch nicht unterstützt:

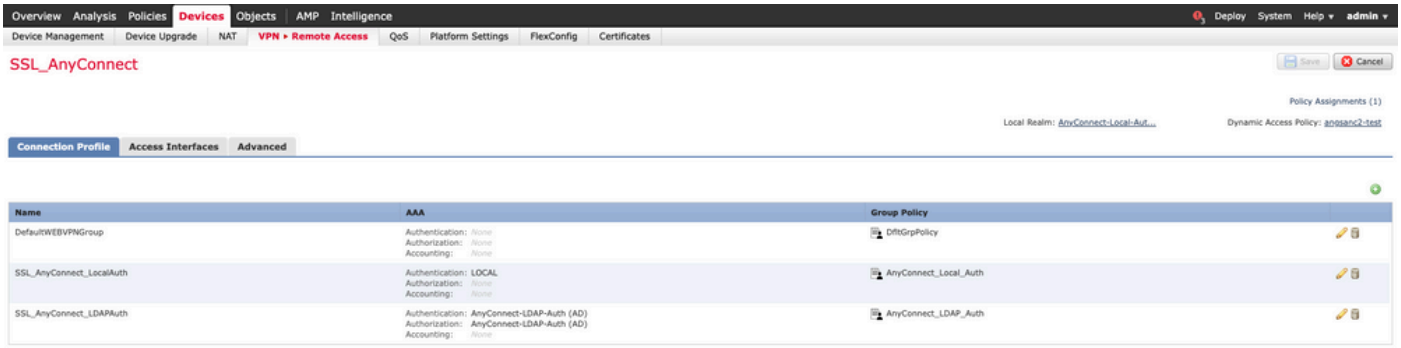
- Dynamic Split Tunnel wird auf iOS-Geräten (Apple) nicht unterstützt. Siehe Cisco Bug-ID CSCvr54798
- Dynamic Split Tunnel wird auf AnyConnect Linux Clients nicht unterstützt. Siehe Cisco Bug IDCSCvt64988

Konfigurieren

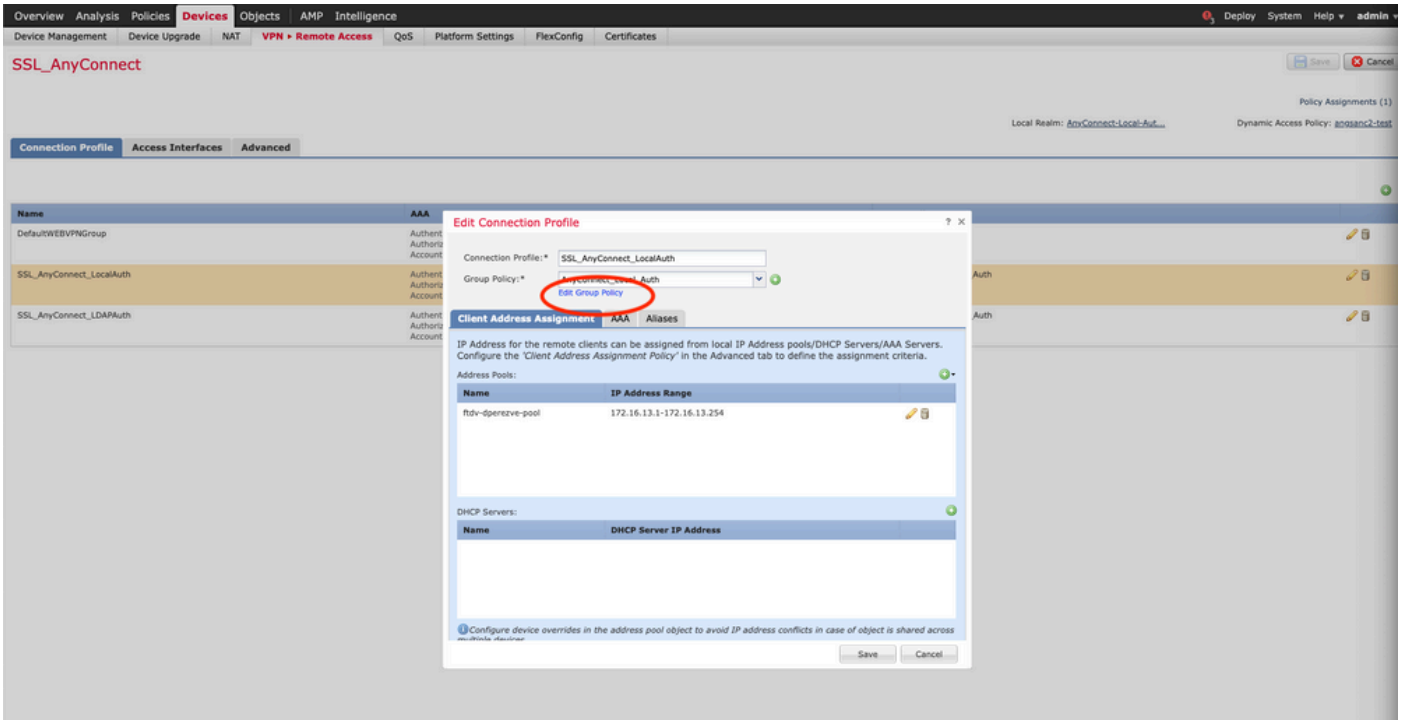
In diesem Abschnitt wird beschrieben, wie Sie einen dynamischen AnyConnect Split Tunnel auf einem von FMC verwalteten FTD konfigurieren.

Schritt 1: Bearbeiten der Gruppenrichtlinie zur Verwendung von dynamischem Split-Tunnel

1. Navigieren Sie auf dem FMC zu **Devices > VPN > Remote Access**, und wählen Sie dann das **Verbindungsprofil aus,** auf das die Konfiguration angewendet werden soll.

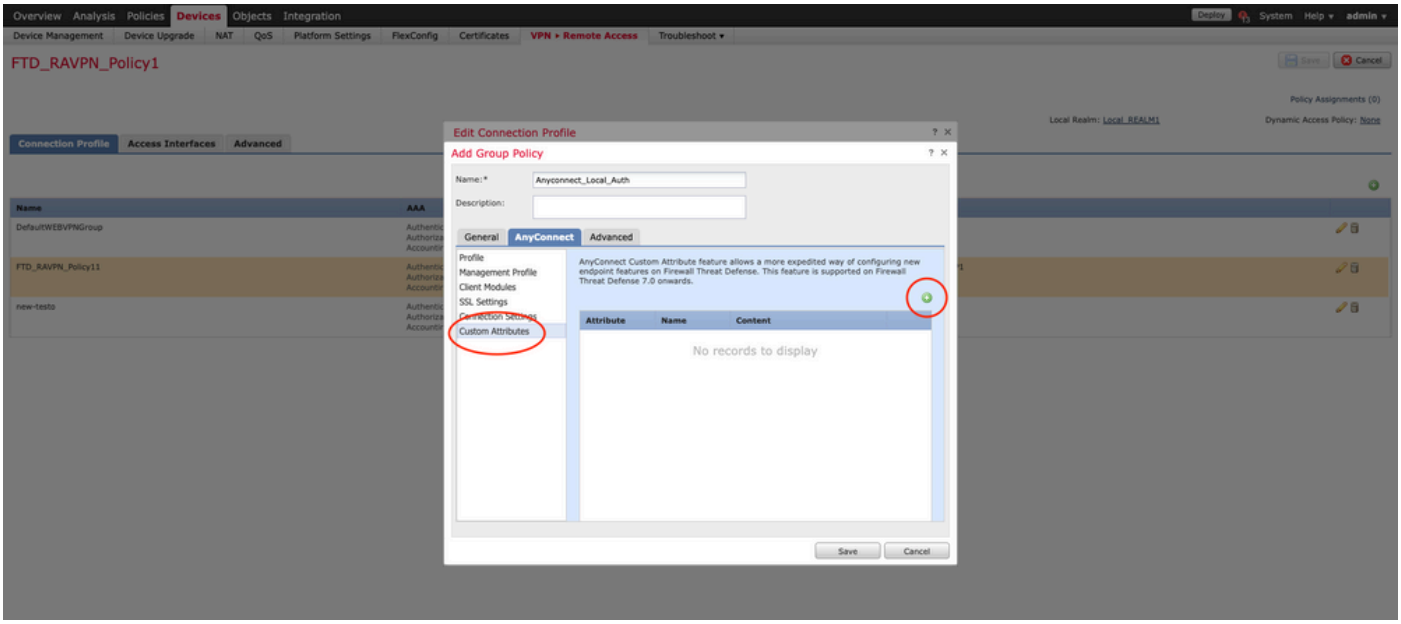


2. Wählen Sie **Gruppenrichtlinie bearbeiten**, um eine der bereits erstellten Gruppenrichtlinien zu ändern.

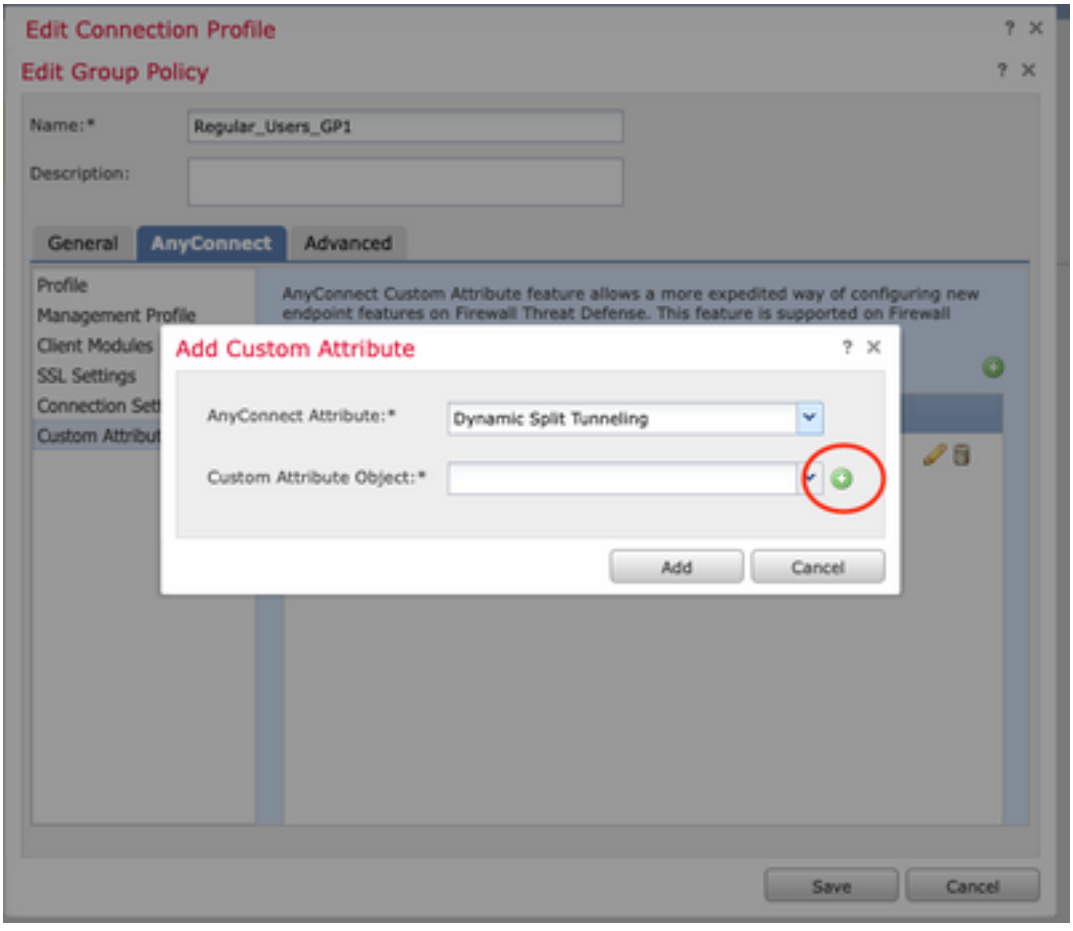


Schritt 2: Konfigurieren des benutzerdefinierten AnyConnect-Attributs

1. Navigieren Sie unter der Gruppenrichtlinienkonfiguration zu **AnyConnect > Benutzerdefinierte Attribute,** und klicken Sie auf die Schaltfläche **Hinzufügen (+)**:

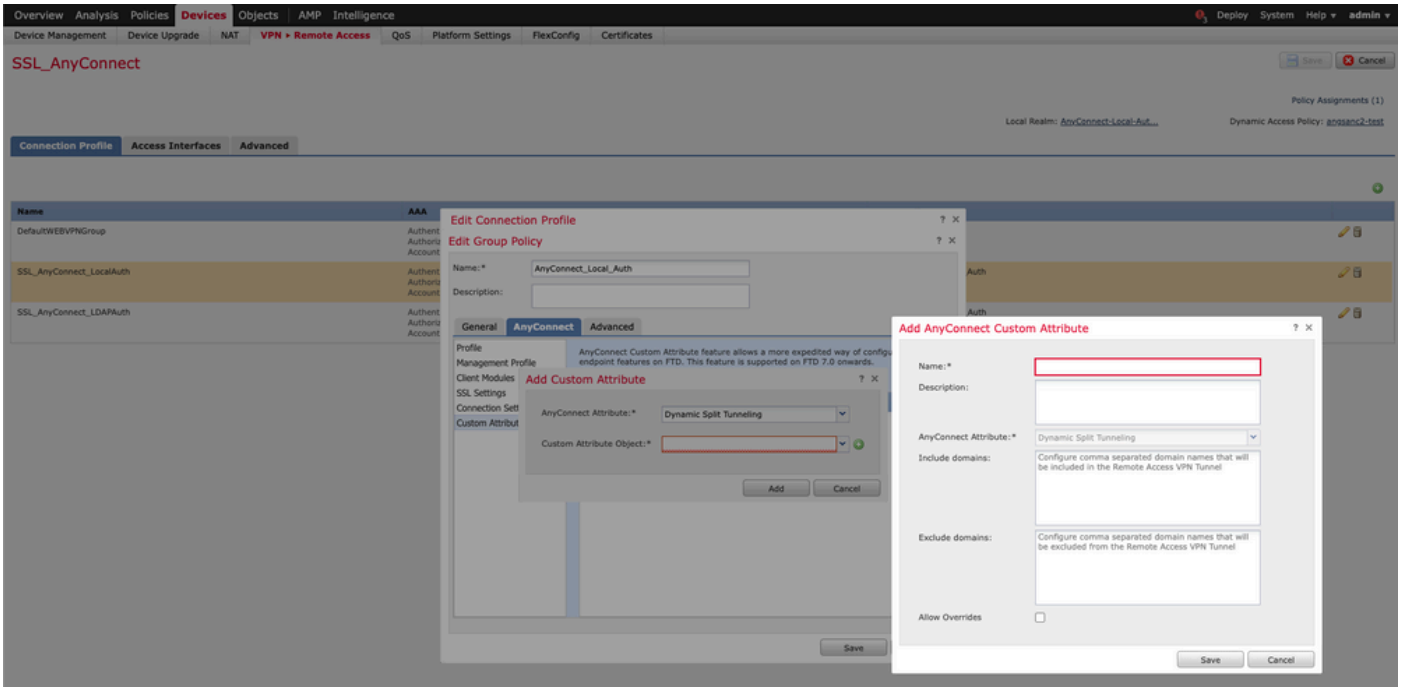


2. Wählen Sie das **Dynamic Split Tunneling** AnyConnect-Attribut, und klicken Sie auf die Schaltfläche **Hinzufügen (+)**, um ein neues benutzerdefiniertes Attributobjekt zu erstellen:

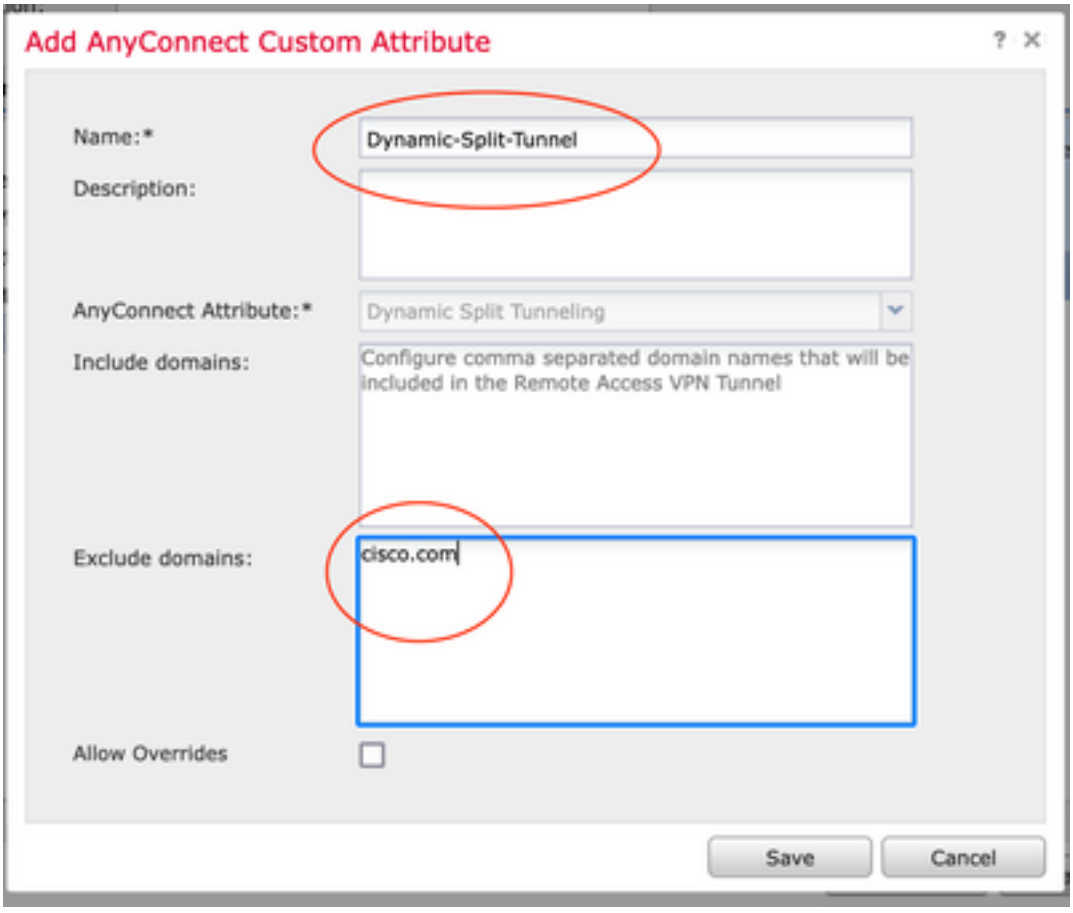


3. Geben Sie den **Namen** des **benutzerdefinierten AnyConnect-Attributs ein**, und konfigurieren Sie die Domänen so, dass sie dynamisch ein- oder ausgeschlossen werden.

> **Hinweis**: Sie können nur **Domänen einschließen** oder **ausschließen** konfigurieren.

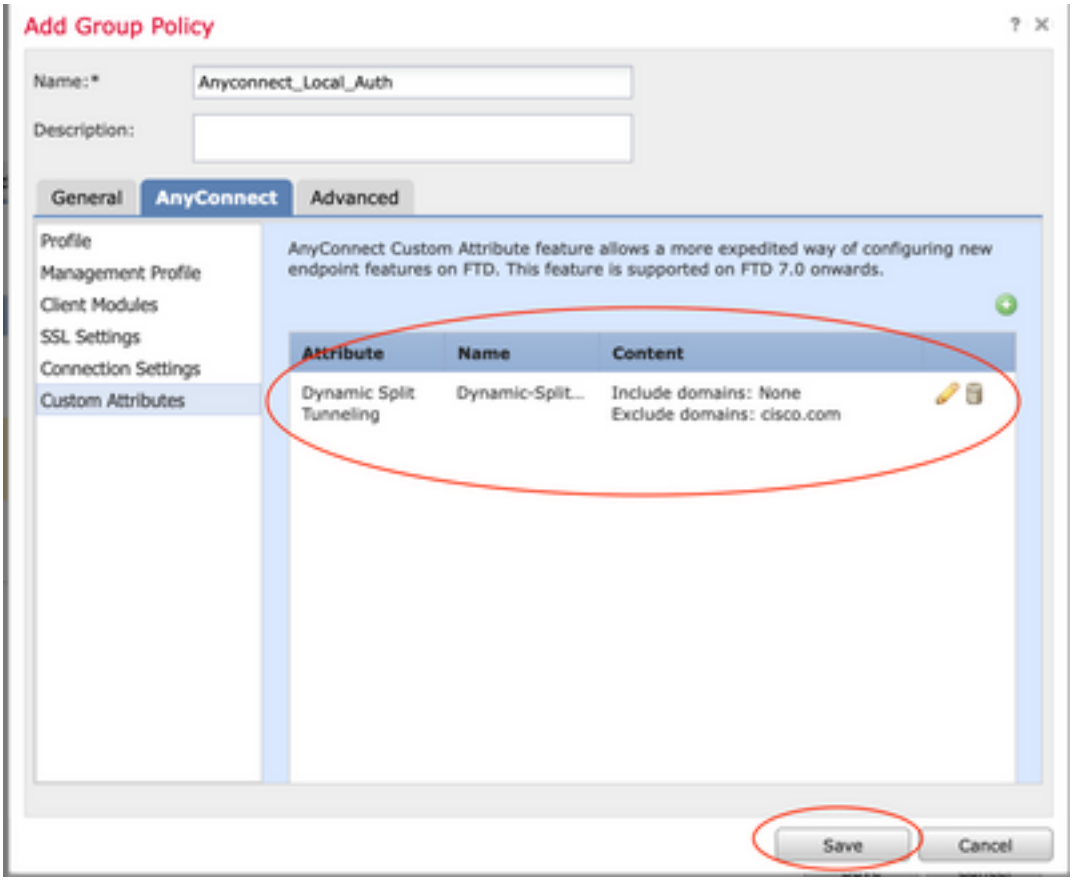


In diesem Beispiel haben wir **cisco.com** als auszuschließende Domäne konfiguriert und das benutzerdefinierte Attribut **Dynamic-Split-Tunnel** benannt, wie im Bild gezeigt:



Schritt 3: Überprüfen der Konfiguration, Speichern und Bereitstellen

Überprüfen Sie, ob das konfigurierte benutzerdefinierte Attribut korrekt ist, speichern Sie die Konfiguration, und stellen Sie die Änderungen im betreffenden FTD bereit.



Überprüfung

Sie können diese Befehle über die FTD-Befehlszeilenschnittstelle (CLI) ausführen, um die Konfiguration des Dynamic Split Tunnels zu bestätigen:

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy **<Name der Gruppenrichtlinie>**

In diesem Beispiel ist die Konfiguration die nächste:

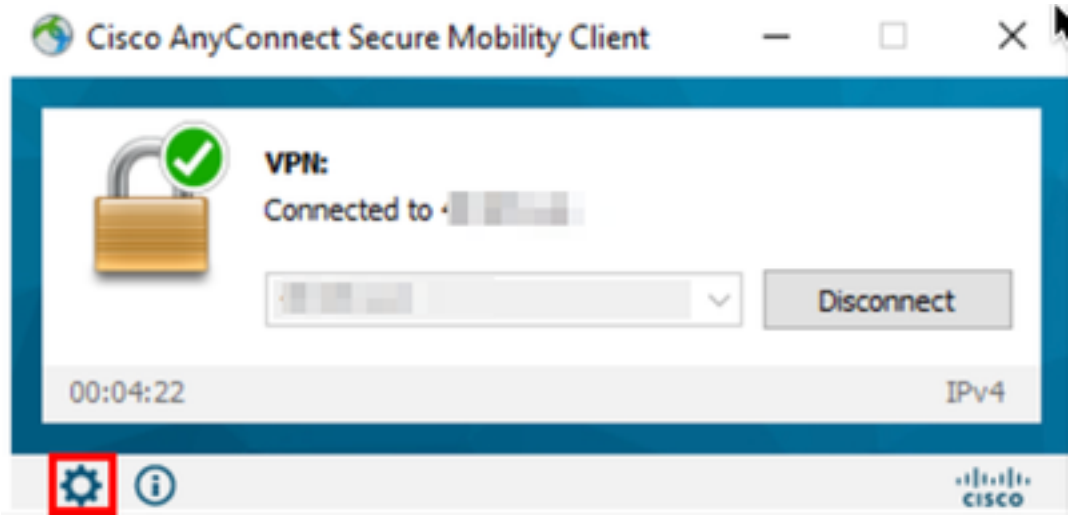
```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list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

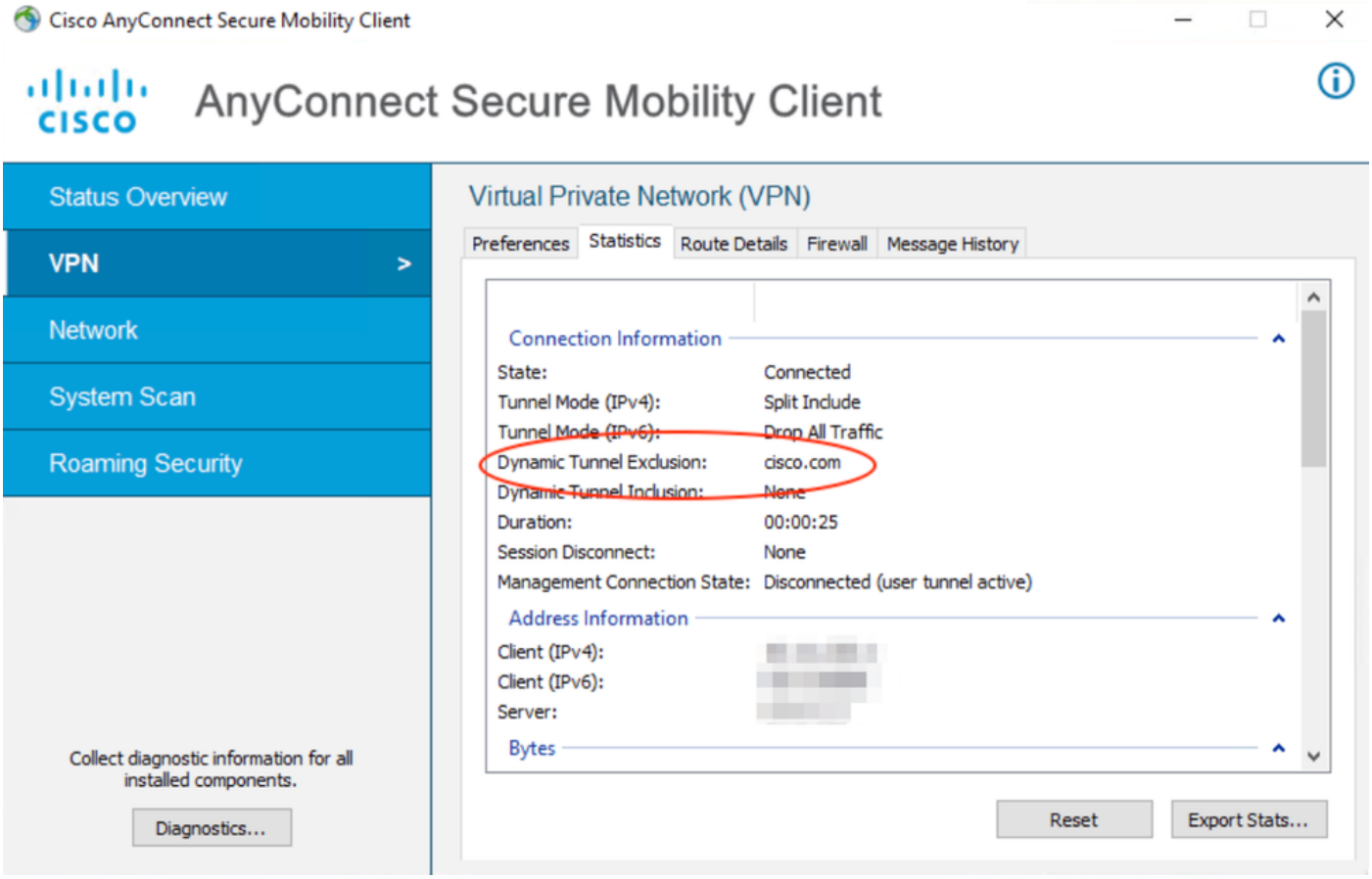
```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml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

So überprüfen Sie die konfigurierten dynamischen Tunnelausschlüsse auf dem Client:

1. Starten Sie die AnyConnect-Software und klicken Sie auf das Zahnrad-Symbol, wie im Bild gezeigt:



2. Navigieren Sie zu **VPN > Statistics**, und bestätigen Sie die unter "**Dynamic Split Exclusion/Inclusion**" angezeigten Domänen:



Fehlerbehebung

Sie können das AnyConnect Diagnostics and Reporting Tool (DART) verwenden, um die Daten zu erfassen, die zur Behebung von AnyConnect-Installations- und Verbindungsproblemen nützlich sind.

DART stellt die Protokolle, Status und Diagnoseinformationen für die Analyse durch das Cisco Technical Assistance Center (TAC) zusammen. Für die Ausführung von DART auf dem Client-Computer sind keine Administratorrechte erforderlich.

Problem

Wenn ein Platzhalter in den benutzerdefinierten AnyConnect-Attributen konfiguriert ist, z. B. ***.cisco.com**, wird die Verbindung zur AnyConnect-Sitzung getrennt.

Lösung

Sie können den **cisco.com**-Domänenwert verwenden, um den Ersatz des Platzhalters zu ermöglichen. Mit dieser Änderung können Sie Domänen wie **www,cisco.com** und **tools.cisco.com** ein- oder ausschließen.

Zugehörige Informationen

- Wenden Sie sich für weitere Unterstützung an das Technical Assistance Center (TAC). Ein gültiger Supportvertrag ist erforderlich: Weltweiter Kontakt zum Cisco Support.
- Besuchen Sie auch die Cisco VPN Community. hier.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.