Configurazione di AnyConnect Dynamic Split Tunnel su FTD Gestito da FMC

Sommario

Introduzione

In questo documento viene descritto come configurare AnyConnect Dynamic Split Tunnel su Firepower Threat Defense (FTD) gestito da Firepower Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco AnyConnect
- Conoscenze base dei CCP

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- FMC versione 7.0
- FTD versione 7.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La configurazione AnyConnect Dynamic Split Tunnel su FTD gestito da FMC è completamente disponibile sulla versione 7.0 e successive di FMC. Se si esegue una versione precedente, è necessario configurarla tramite FlexConfig come indicato in Implementazioni avanzate della VPN AnyConnect per Firepower Threat Defense con FMC.

Con la configurazione Dynamic Split Tunnel è possibile ottimizzare la configurazione del tunnel suddiviso in base ai nomi di dominio DNS. Poiché gli indirizzi IP associati ai nomi di dominio completi (FQDN) possono variare, la configurazione del tunnel suddiviso in base ai nomi DNS offre una definizione più dinamica del traffico incluso o meno nel tunnel VPN (Virtual Private Network) di accesso remoto. Se uno degli indirizzi restituiti per i nomi di dominio esclusi si trova all'interno del pool di indirizzi incluso nella VPN, tali indirizzi verranno esclusi. I domini esclusi non sono bloccati. Al contrario, il traffico verso questi domini viene mantenuto all'esterno del tunnel VPN.

È inoltre possibile configurare il tunnel con split dinamico per definire i domini da includere nel tunnel che altrimenti sarebbero esclusi in base all'indirizzo IP.

Limitazioni

Al momento, queste funzionalità non sono ancora supportate:

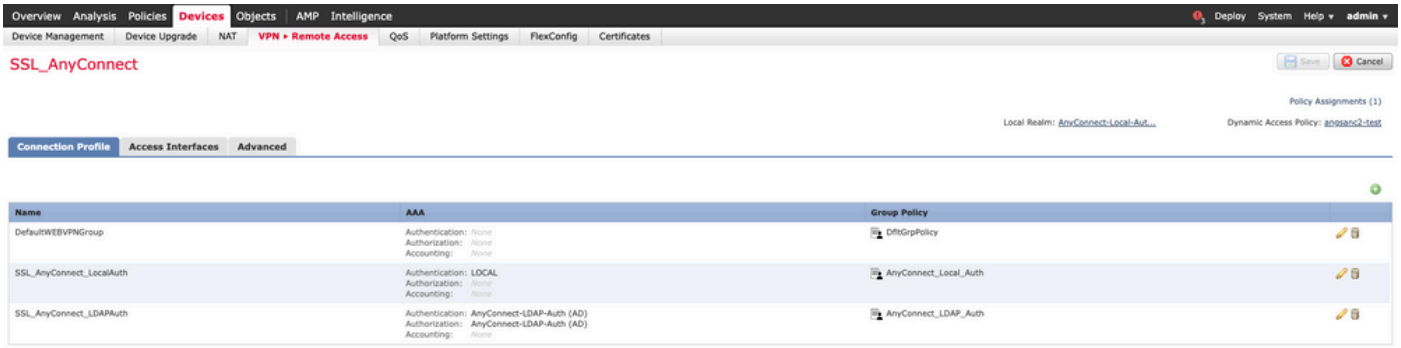
- Dynamic Split Tunnel non è supportato sui dispositivi iOS (Apple). Vedere l'ID bug Cisco CSCvr54798
- Il tunnel split dinamico non è supportato sui client Linux Anyconnect. Vedere il bug Cisco IDCSCvt64988

Configurazione

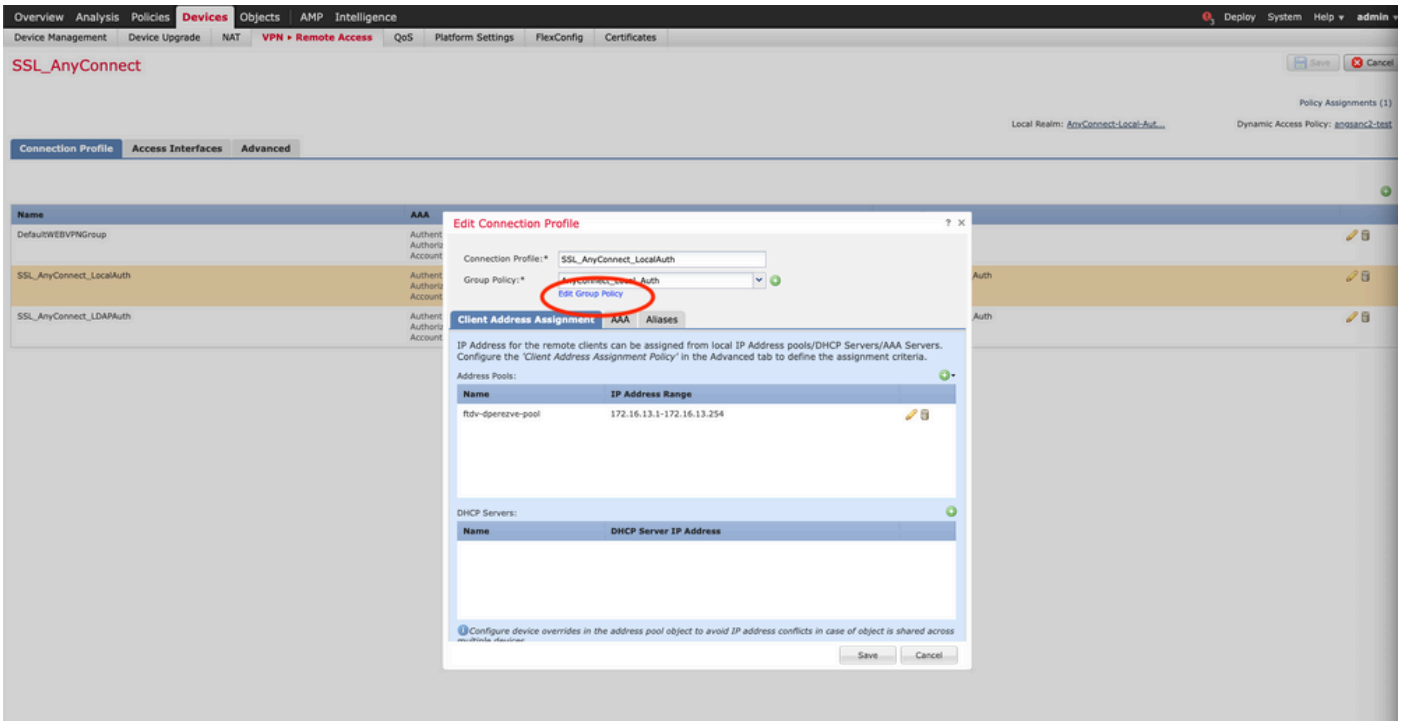
In questa sezione viene descritto come configurare AnyConnect Dynamic Split Tunnel su FTD gestito da FMC.

Passaggio 1. Modificare i Criteri di gruppo per l'utilizzo di Dynamic Split Tunnel

1. Dal FMC, selezionare **Devices > VPN > Remote Access** (Dispositivi > Accesso remoto), quindi selezionare il **profilo di connessione** a cui si desidera applicare la configurazione.

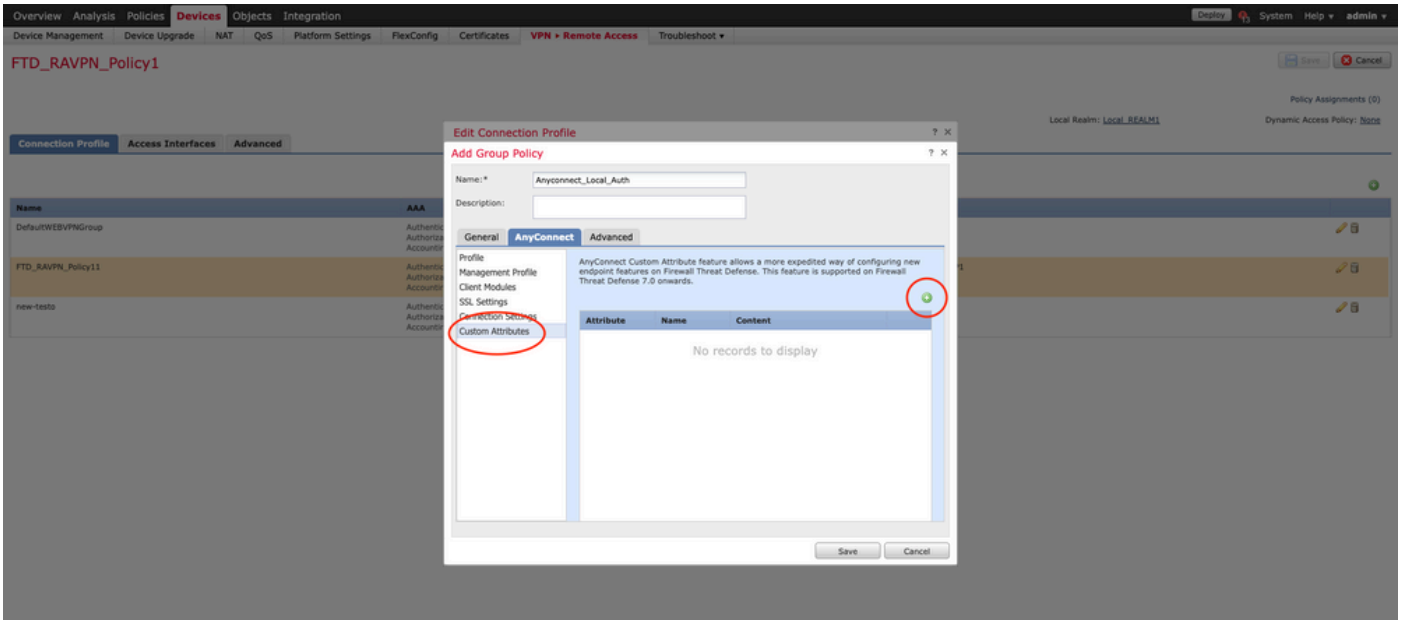


2. Selezionare **Modifica Criteri di gruppo** per modificare uno dei Criteri di gruppo già creati.

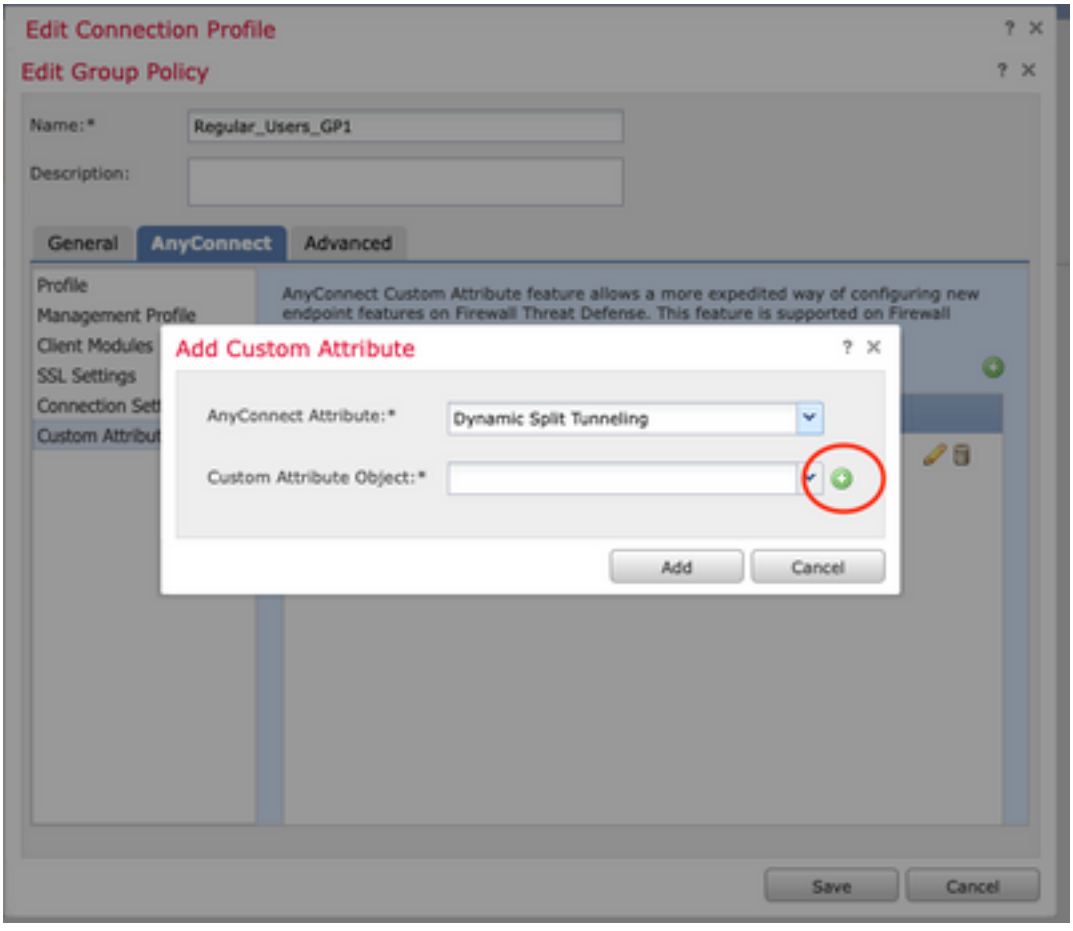


Passaggio 2. Configurazione dell'attributo personalizzato AnyConnect

1. In Configurazione Criteri di gruppo, passare a **Anyconnect > Attributi personalizzati**, quindi fare clic sul pulsante **Aggiungi (+)**:

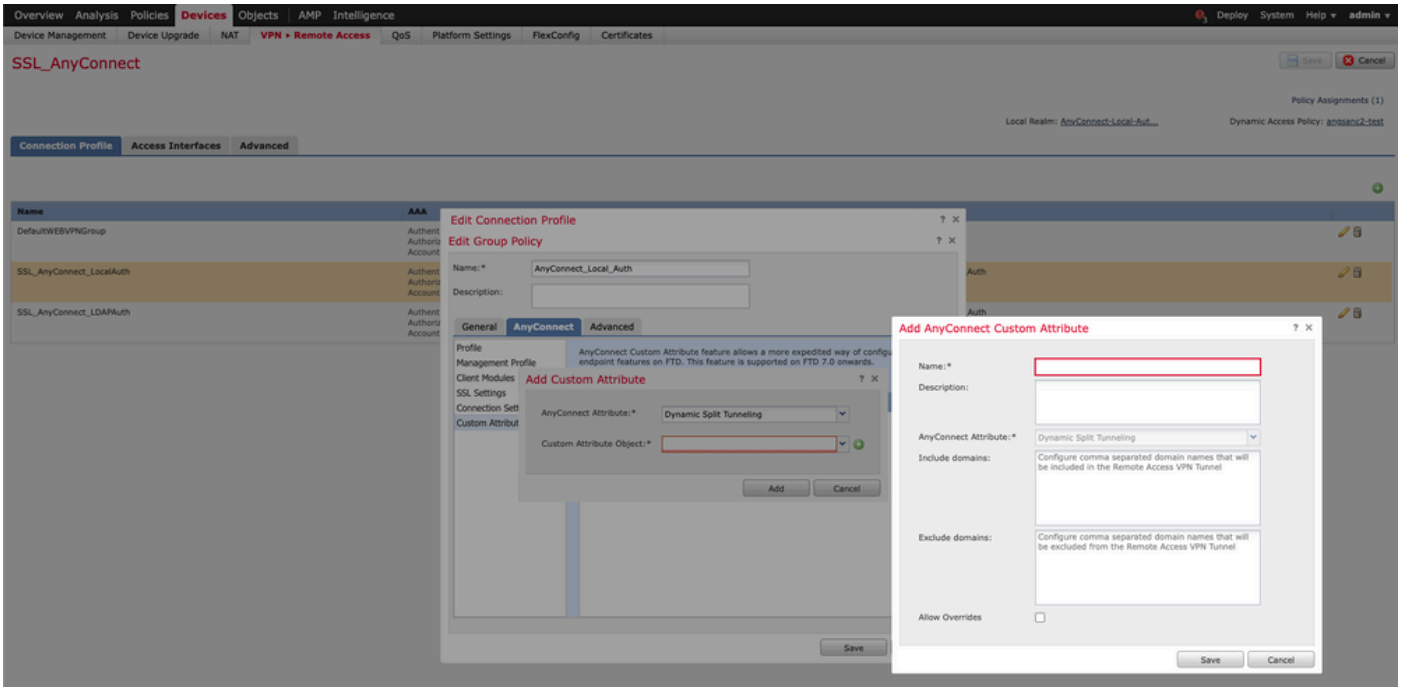


2. Selezionare l'attributo AnyConnect **Dynamic Split Tunneling** e fare clic sul pulsante **Aggiungi (+)** per creare un nuovo oggetto attributo personalizzato:

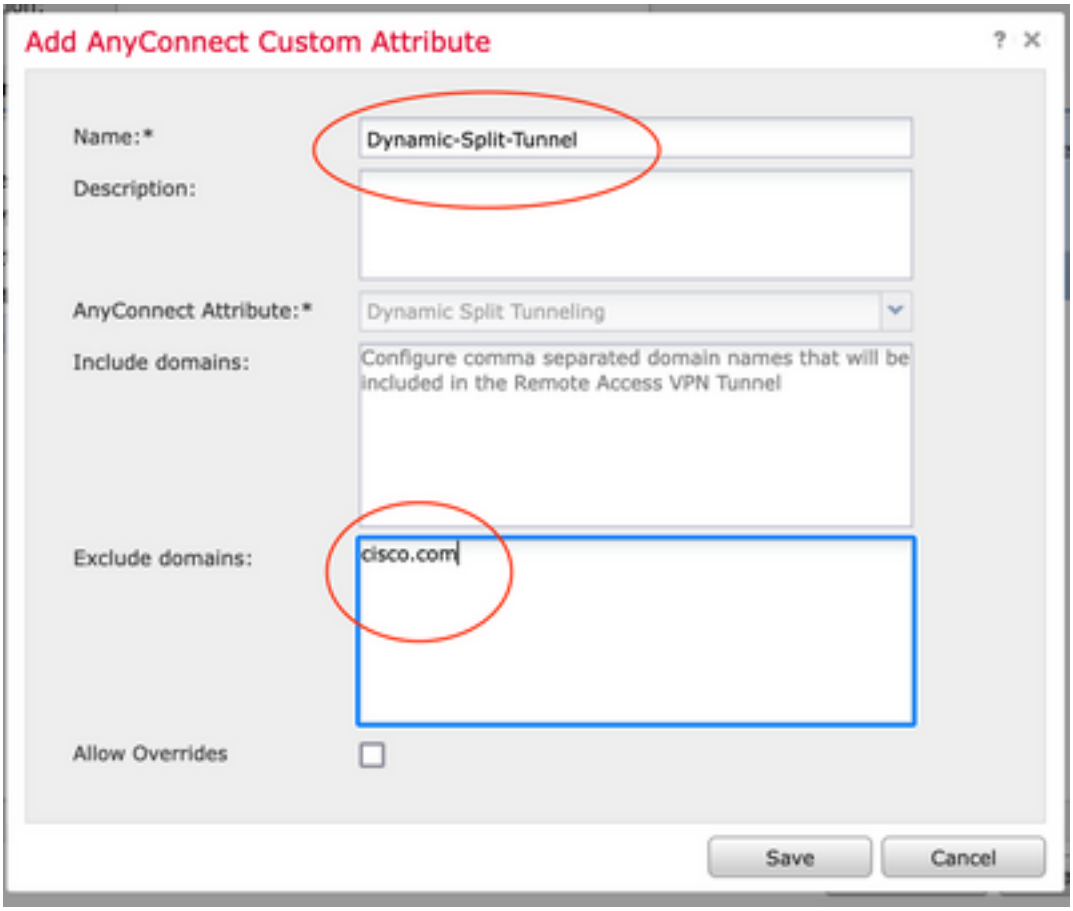


3. Inserire il **nome** dell'**attributo personalizzato AnyConnect** e configurare i domini in modo che vengano inclusi o esclusi in modo dinamico.

> **Nota**: è possibile configurare solo **Includi domini** o **Escludi domini**.

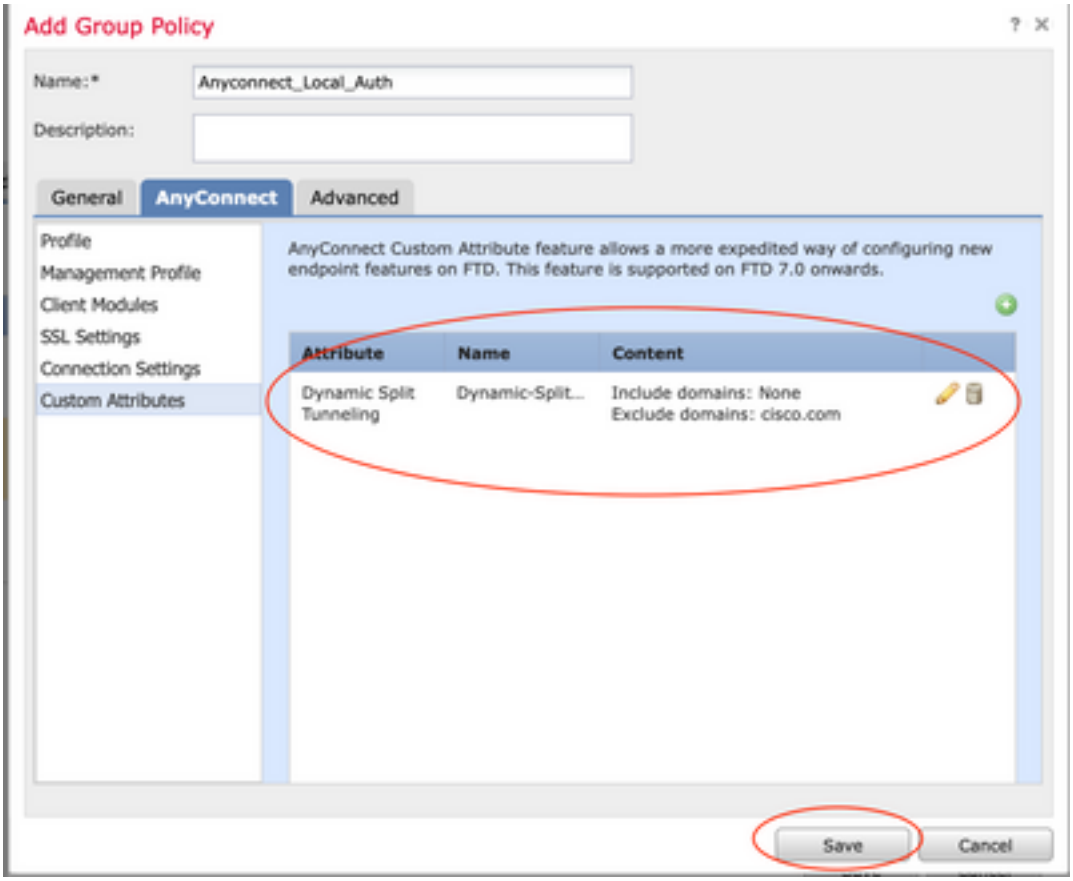


Nell'esempio, è stato configurato **cisco.com** come dominio da escludere e l'attributo personalizzato **Dynamic-Split-Tunnel** è stato denominato, come mostrato nell'immagine:



Passaggio 3. Verifica della configurazione, salvataggio e distribuzione

Verificare che l'attributo personalizzato configurato sia corretto, salvare la configurazione e distribuire le modifiche all'FTD in questione.



Verifica

Èpossibile eseguire questi comandi sull'FTD tramite l'interfaccia della riga di comando (CLI) per confermare la configurazione del tunnel di divisione dinamico:

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config criteri-gruppo **<Nome del criterio-gruppo>**

Nell'esempio, la configurazione è la seguente:

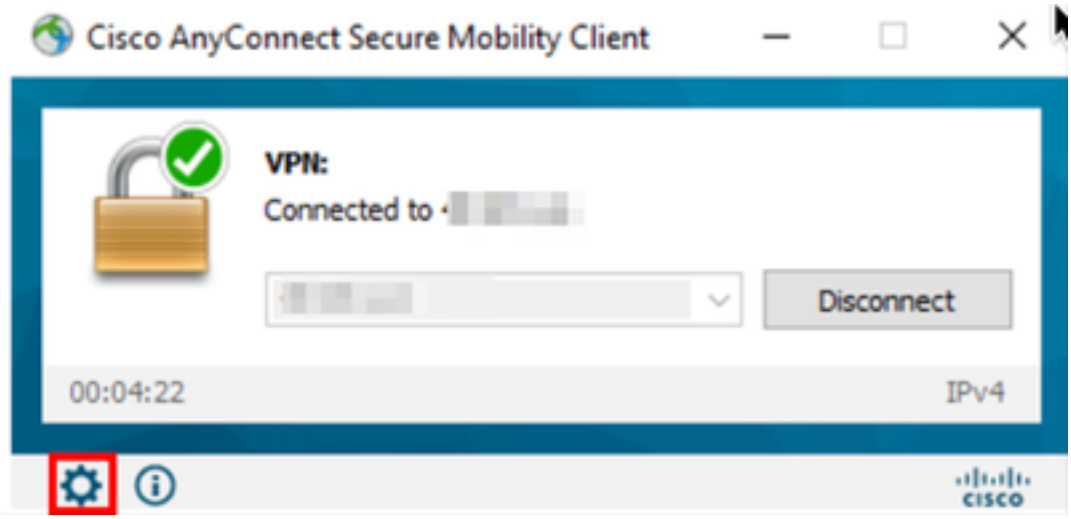
```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list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

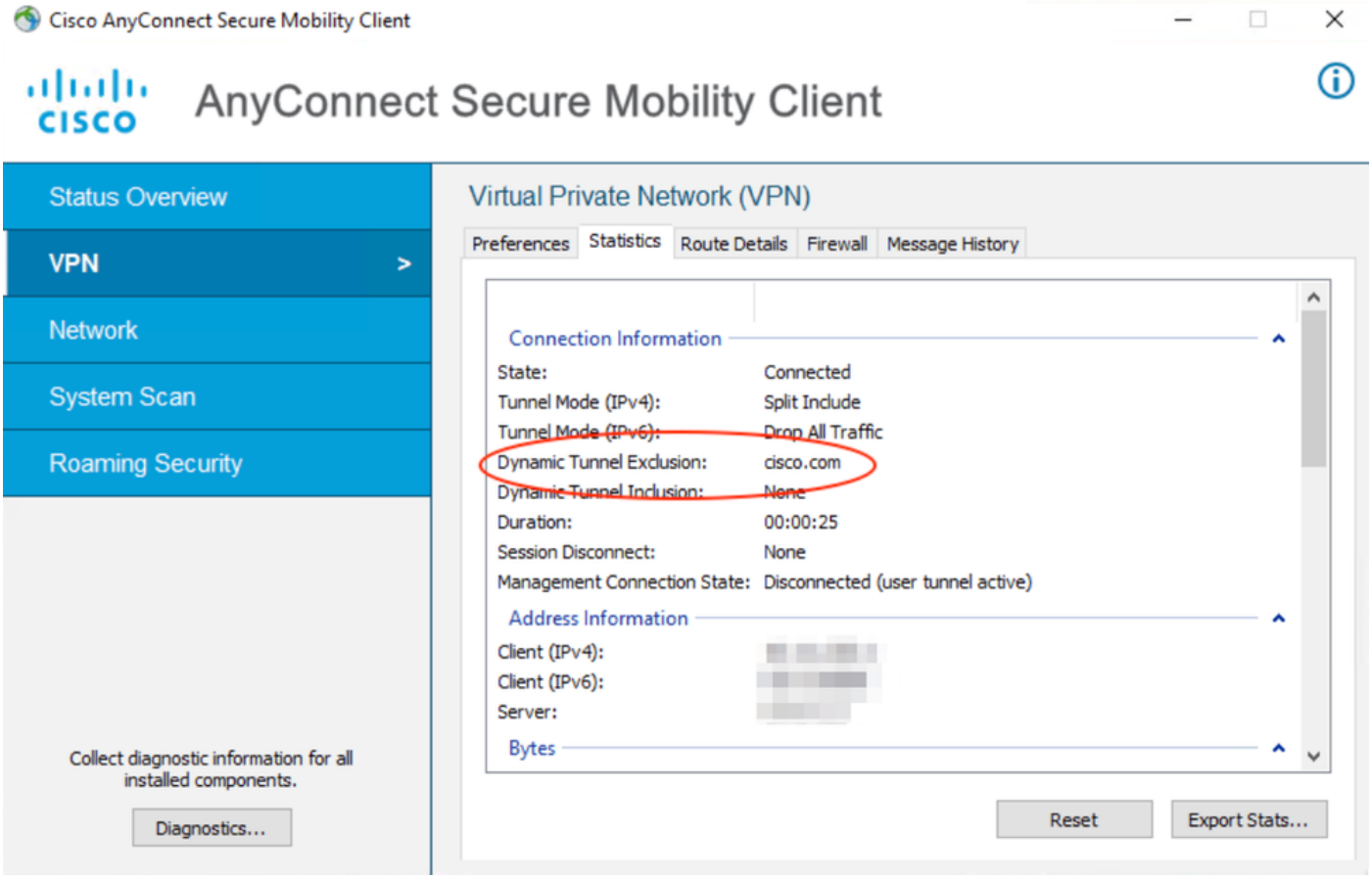
```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml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

Per verificare le esclusioni del tunnel dinamico configurate sul client:

1. Avviare il software AnyConnect e fare clic sull'icona dell'ingranaggio, come mostrato nell'immagine:



2. Passare a **VPN > Statistiche** e confermare i domini visualizzati in **Inclusione/esclusione divisione dinamica**:



Risoluzione dei problemi

Èpossibile usare lo strumento di diagnostica e segnalazione di AnyConnect (DART) per raccogliere i dati utili per risolvere i problemi di installazione e connessione di AnyConnect.

DART raggruppa i registri, lo stato e le informazioni di diagnostica per l'analisi di Cisco Technical Assistance Center (TAC) e non richiede privilegi di amministratore per l'esecuzione sul computer client.

Problema

Se negli attributi personalizzati di AnyConnect è configurato un carattere jolly, ad esempio ***.cisco.com**, la sessione AnyConnect viene disconnessa.

Soluzione

Èpossibile utilizzare il valore del dominio **cisco.com** per consentire la sostituzione del carattere jolly. Questa modifica consente di includere o escludere domini quali **www,cisco.com** e **tools.cisco.com**.

Informazioni correlate

- Per ulteriore assistenza, contattare il Technical Assistance Center (TAC). È necessario un contratto di supporto valido: Contatti del supporto Cisco internazionali.
- Puoi anche visitare la Cisco VPN Community qui.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).