Configuración del túnel dividido dinámico de AnyConnect en FTD administrado por FMC

Contenido

Introducción

Este documento describe cómo configurar el túnel dividido dinámico de AnyConnect en Firepower Threat Defense (FTD) administrado por Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco AnyConnect
- Conocimientos básicos de FMC

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- FMC versión 7.0
- FTD versión 7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La configuración del túnel dividido dinámico de AnyConnect en FTD administrado por FMC está totalmente disponible en FMC versión 7.0 y posteriores. Si ejecuta una versión anterior, debe configurarla mediante FlexConfig como se indica en Advanced AnyConnect VPN Deployments for Firepower Threat Defense with FMC.

Con la configuración de túnel dividido dinámico, puede ajustar la configuración de túnel dividido en función de los nombres de dominio DNS. Dado que las direcciones IP asociadas con los nombres de dominio completos (FQDN) pueden cambiar, la configuración de túnel dividido basada en nombres DNS proporciona una definición más dinámica del tráfico que se incluye o no en el túnel de acceso remoto de la red privada virtual (VPN). Si alguna de las direcciones devueltas para los nombres de dominio excluidos se encuentra dentro del conjunto de direcciones incluido en la VPN, esas direcciones se excluyen. Los dominios excluidos no están bloqueados. En su lugar, el tráfico a esos dominios se mantiene fuera del túnel VPN.

Observe que también puede configurar el túnel dividido dinámico para definir los dominios que se incluirán en el túnel y que, de lo contrario, se excluirían en función de la dirección IP.

Limitaciones

Actualmente, estas funciones aún no son compatibles:

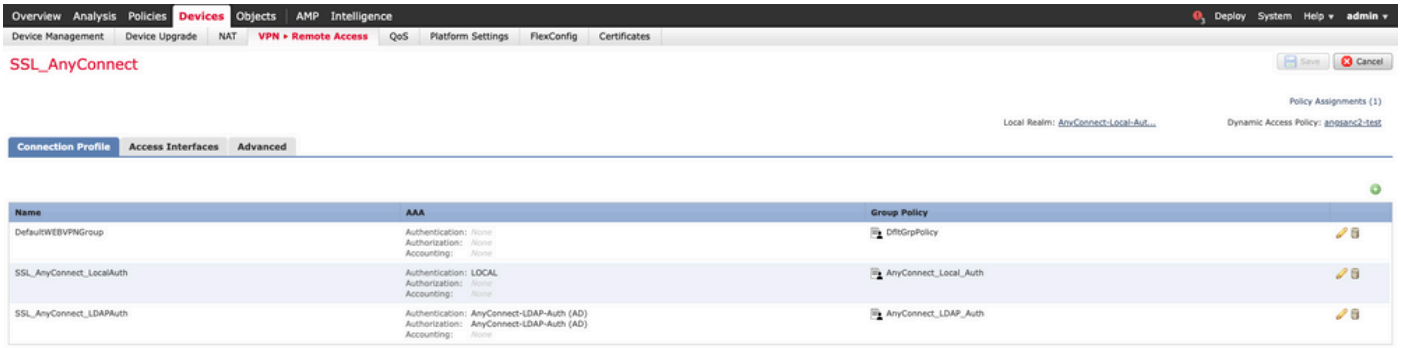
- El túnel dividido dinámico no es compatible con dispositivos iOS (Apple). Consulte Cisco bug ID CSCvr54798
- El túnel dividido dinámico no es compatible con los clientes Linux de Anyconnect. Consulte Cisco bug IDCSCvt64988

Configurar

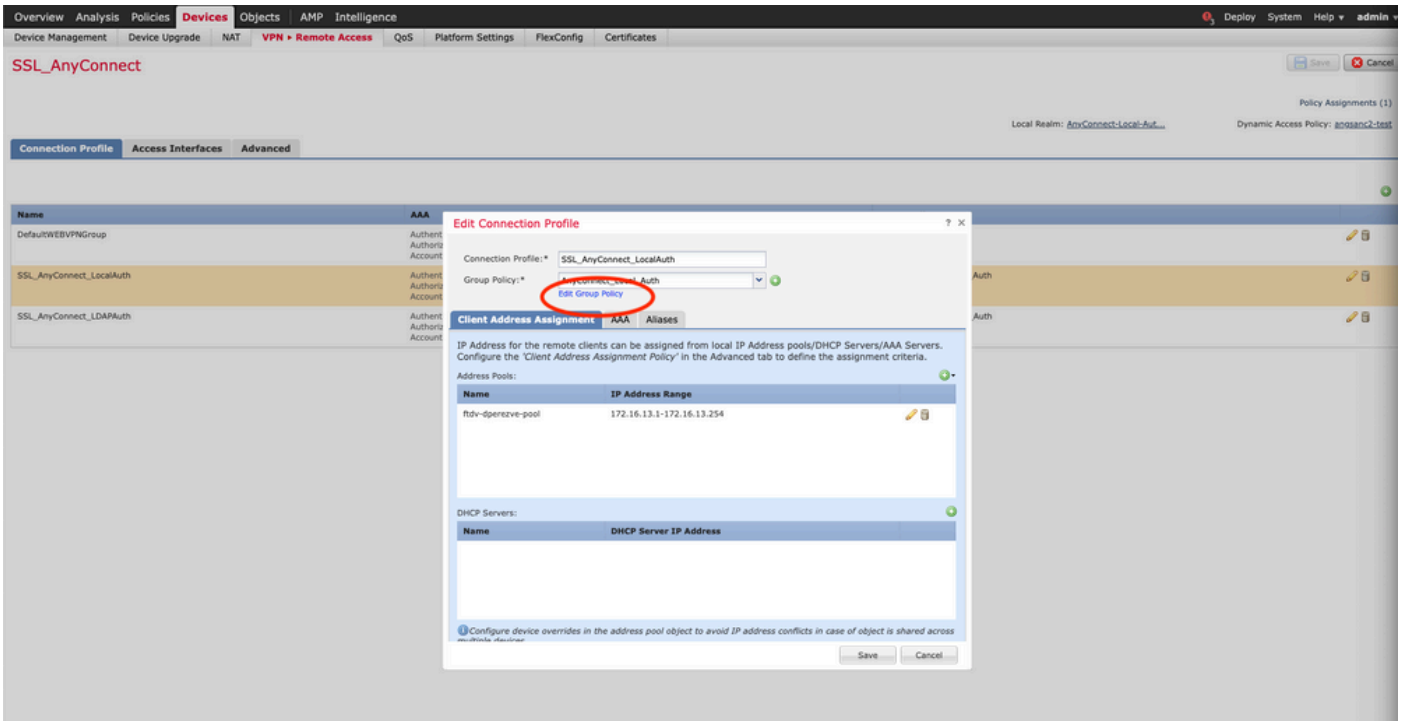
En esta sección se describe cómo configurar el túnel dividido dinámico de AnyConnect en FTD gestionado por FMC.

Paso 1. Edite la directiva de grupo para utilizar el túnel dividido dinámico

1. En el FMC, navegue hasta **Devices > VPN > Remote Access**, luego seleccione el **perfil de conexión** al que desea aplicar la configuración.

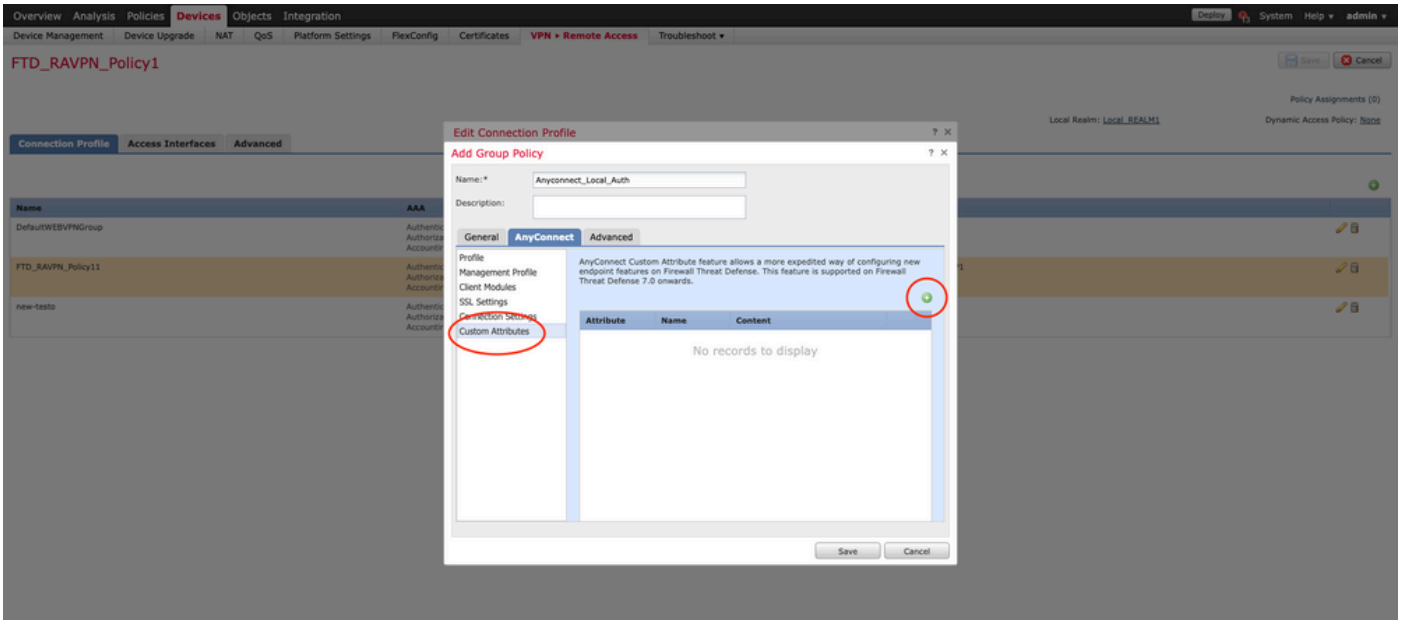


2. Seleccione **Editar Política de Grupo** para modificar una de las políticas de grupo ya creadas.

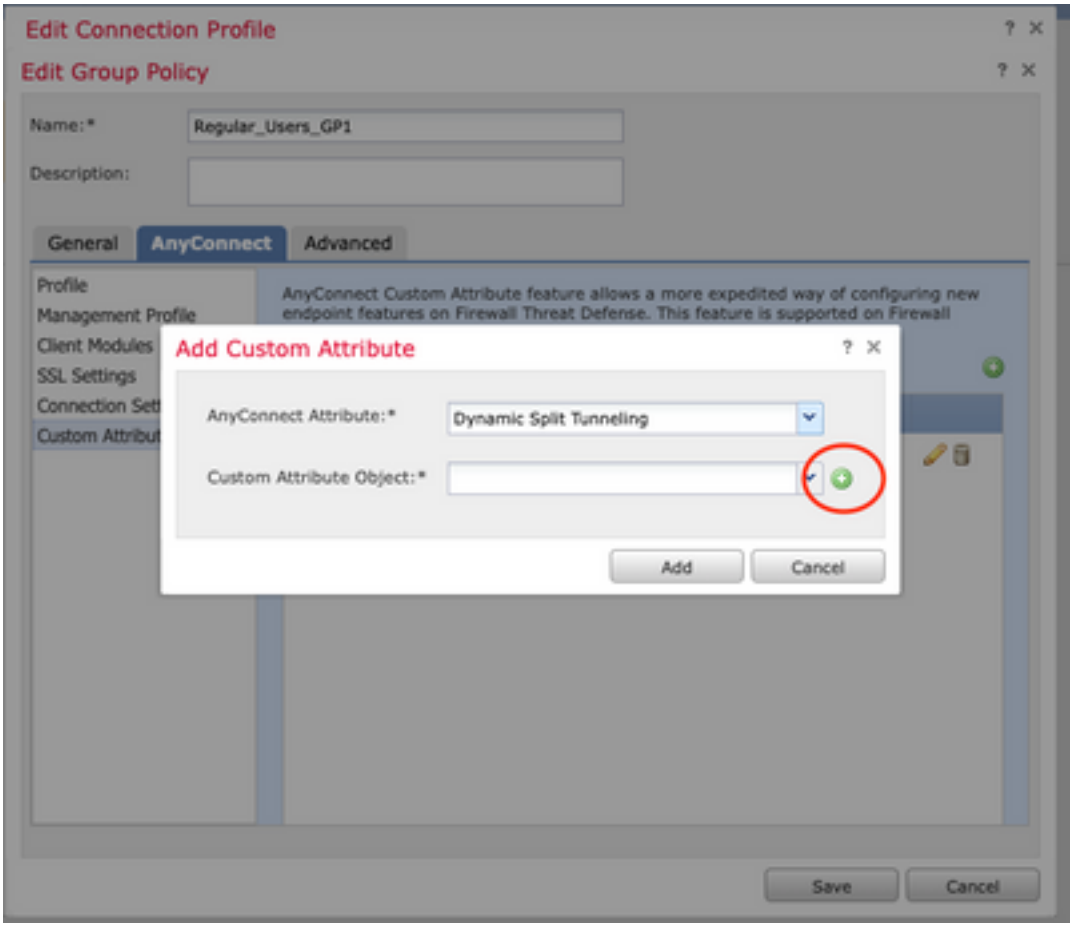


Paso 2. Configuración del atributo personalizado de AnyConnect

1. En la configuración de Directiva de grupo, navegue hasta **Anyconnect > Atributos personalizados**, haga clic en el **botón Agregar (+)**:

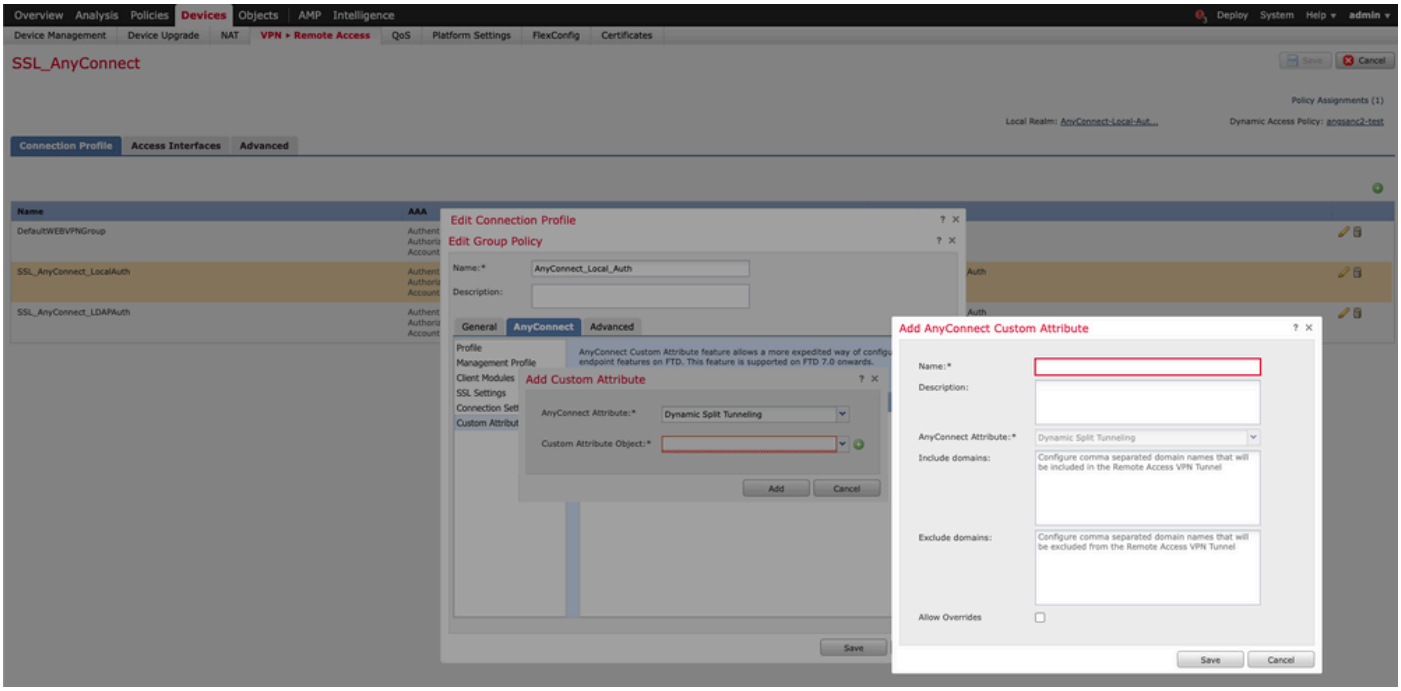


2. Seleccione el atributo **Dynamic Split Tunneling** AnyConnect y haga clic en el botón **Agregar (+)** para crear un nuevo objeto de atributo personalizado:

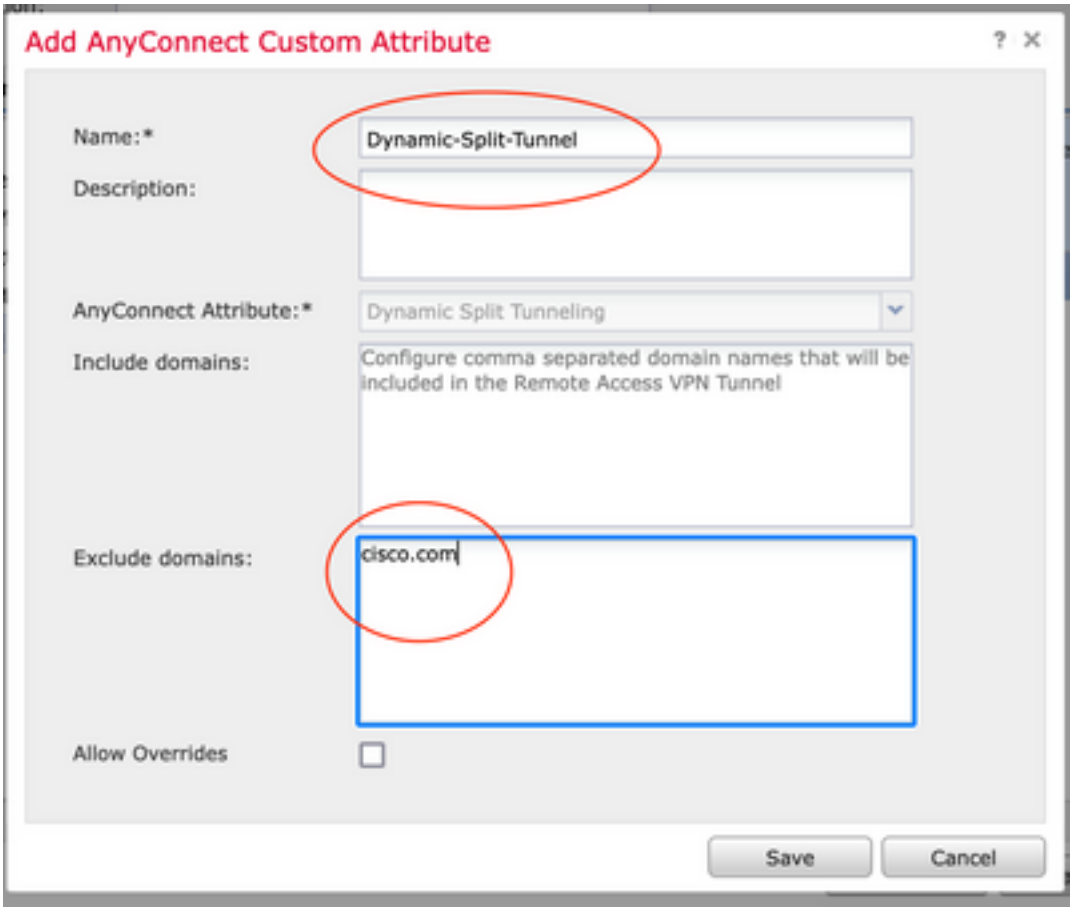


3. Introduzca el **nombre** del **atributo personalizado de AnyConnect** y configure los dominios que se incluirán o excluirán dinámicamente.

Nota: Solo puede configurar **Incluir dominios** o **Excluir dominios**.

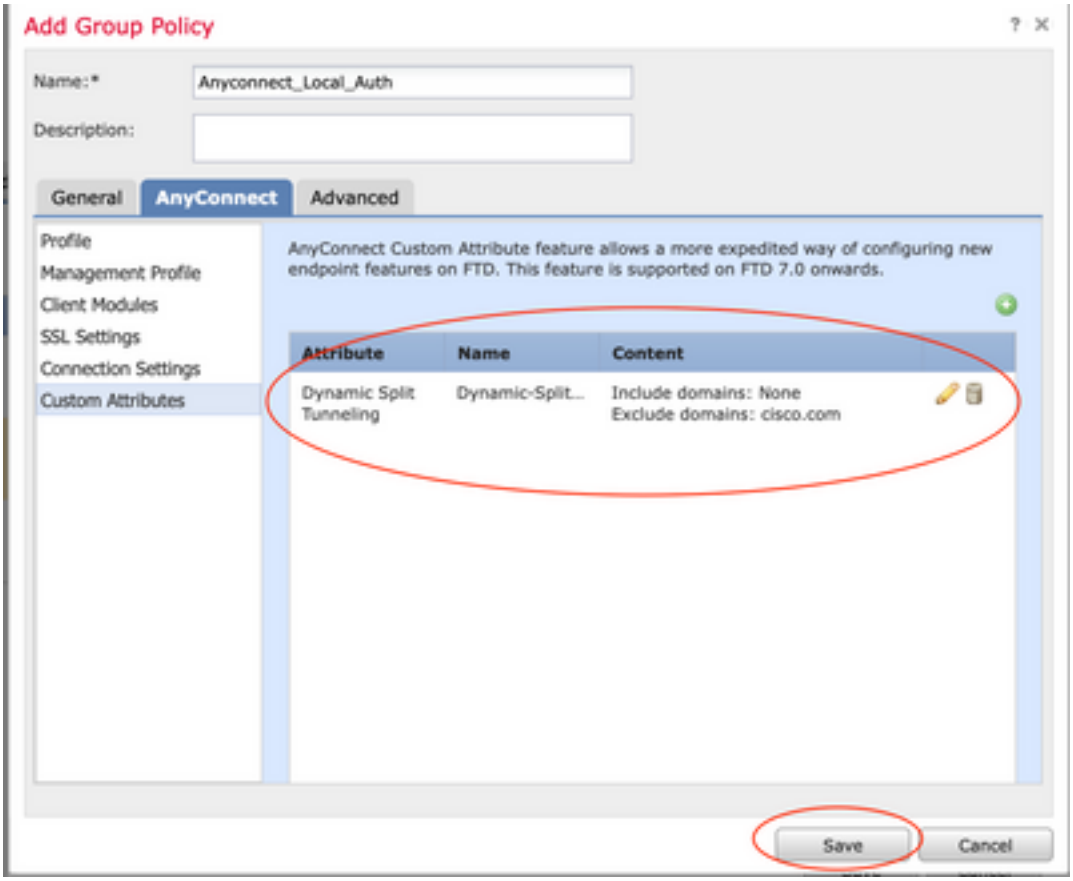


En este ejemplo, configuramos **cisco.com** como el dominio que se excluirá y denominamos el atributo personalizado **Dynamic-Split-Tunnel**, como se muestra en la imagen:



Paso 3. Verificar la configuración, guardar e implementar

Verifique que el atributo personalizado configurado sea correcto, guarde la configuración e implemente los cambios en el FTD en cuestión.



Verificación

Puede ejecutar estos comandos en el FTD mediante la interfaz de línea de comandos (CLI) para confirmar la configuración del túnel dividido dinámico:

- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy **<Name of the group-policy>**

En este ejemplo, la configuración es la siguiente:

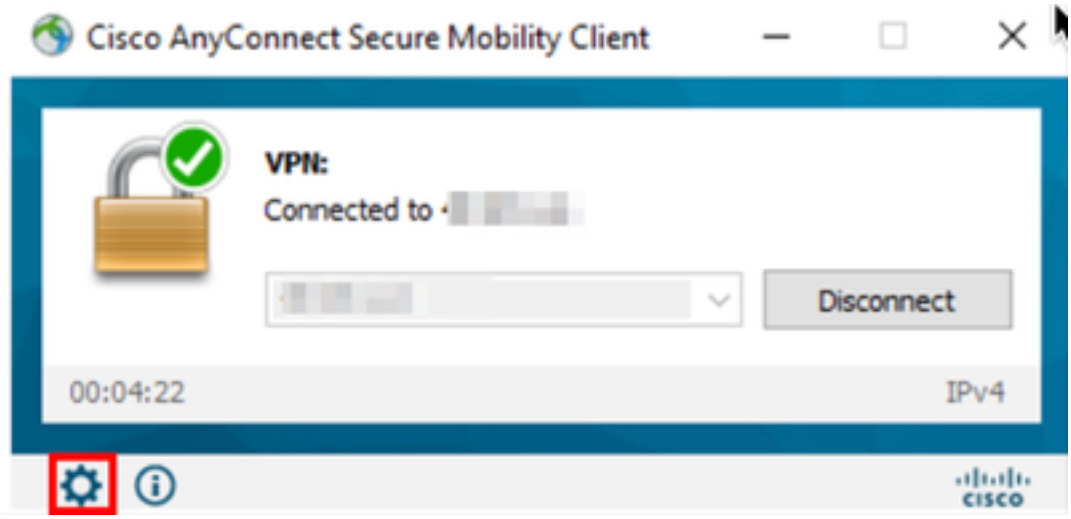
```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list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

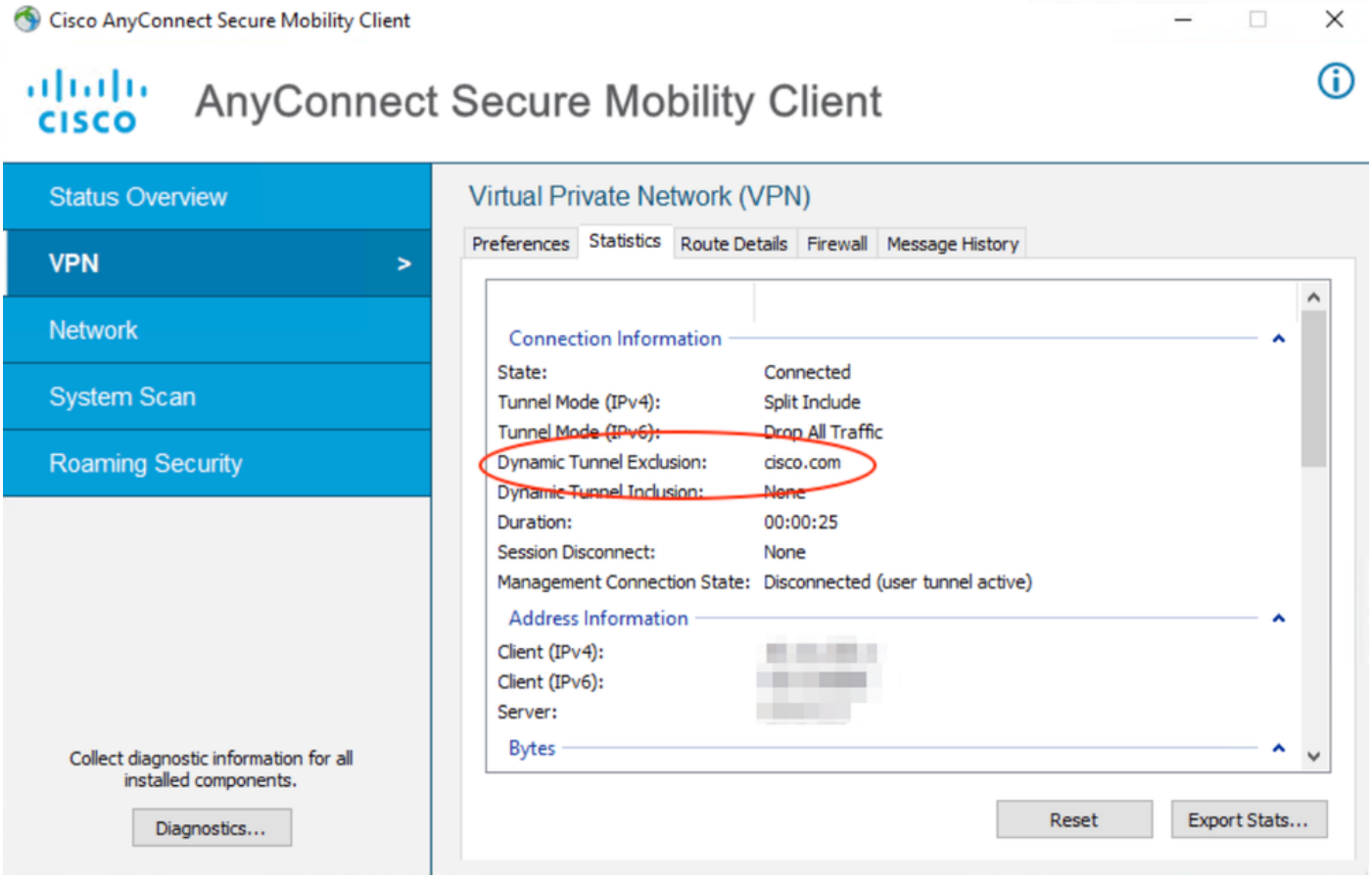
```
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml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

Para verificar las exclusiones de túnel dinámico configuradas en el cliente:

1. Inicie el software AnyConnect y haga clic en el icono del engranaje, como se muestra en la imagen:



2. Navegue hasta **VPN > Statistics** y confirme los dominios mostrados en **Dynamic Split Exclusion/Inclusion**:



Troubleshoot

Puede utilizar la herramienta de diagnóstico e informes (DART) de AnyConnect para recopilar los datos que son útiles para solucionar los problemas de instalación y conexión de AnyConnect.

La DART reúne los registros, el estado y la información de diagnóstico para el análisis de Cisco Technical Assistance Center (TAC) y no requiere privilegios de administrador para ejecutarse en la máquina del cliente.

Problema

Si se configura un comodín en los atributos personalizados de AnyConnect, por ejemplo, ***.cisco.com**, la sesión de AnyConnect se desconecta.

Solución

Puede utilizar el valor del dominio **cisco.com** para permitir el reemplazo del comodín. Este cambio le permite incluir o excluir dominios como **www,cisco.com** y **tools.cisco.com**.

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el centro de asistencia técnica (TAC). Se necesita un contrato de soporte válido: Contactos de soporte a nivel mundial de Cisco.
- También puede visitar Cisco VPN Community aquí.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).