Configuración de proxies de explorador de Windows en Secure Client

Contenido

Introducción

Este documento describe cómo configurar los proxies del explorador de Windows para Cisco Secure Client conectado a FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre estos temas:

- Cisco Secure Firewall Device Manager (FDM)
- Cisco Firepower Threat Defence (FTD)
- Cisco Secure Client (CSC)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Firewall Device Manager versión 7.3
- Appliance Virtual Cisco Firepower Threat Defense Versión 7.3
- Cisco Secure Client versión 5.0.02075

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

El término "proxy" hace referencia a un servicio que se encuentra entre el usuario y el recurso al que desea llegar. Los proxies del navegador web, específicamente, son servidores que transmiten tráfico web por lo que, al navegar a un sitio web, Secure Client le pide al servidor proxy que solicite el sitio en lugar de hacerlo directamente.

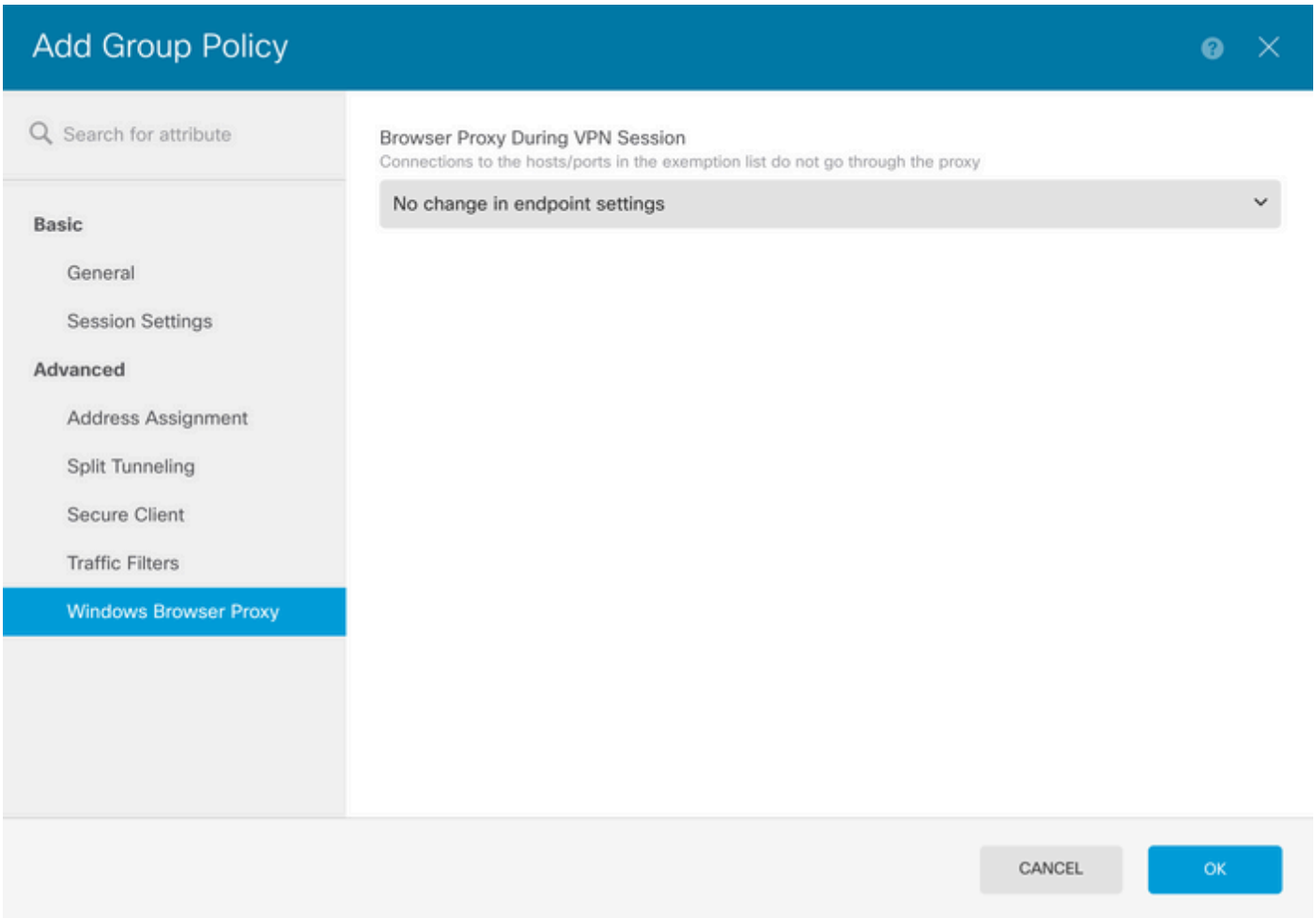
Los proxies se pueden utilizar para lograr diferentes objetivos, como el filtrado de contenido, la gestión del tráfico y la tunelización del tráfico.

Configurar

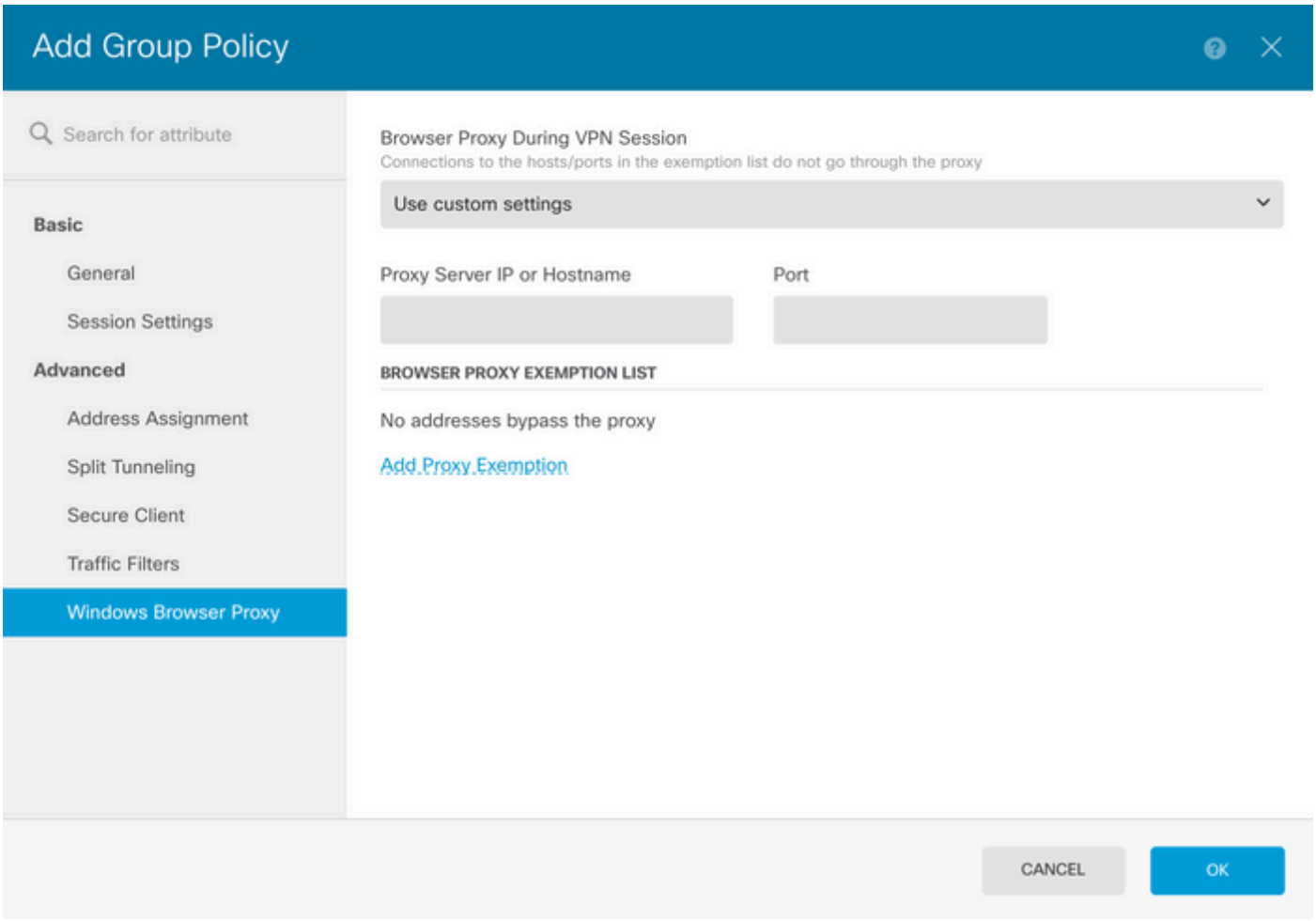
Configuraciones

En este documento, se supone que ya tiene una configuración de VPN de acceso remoto en funcionamiento.

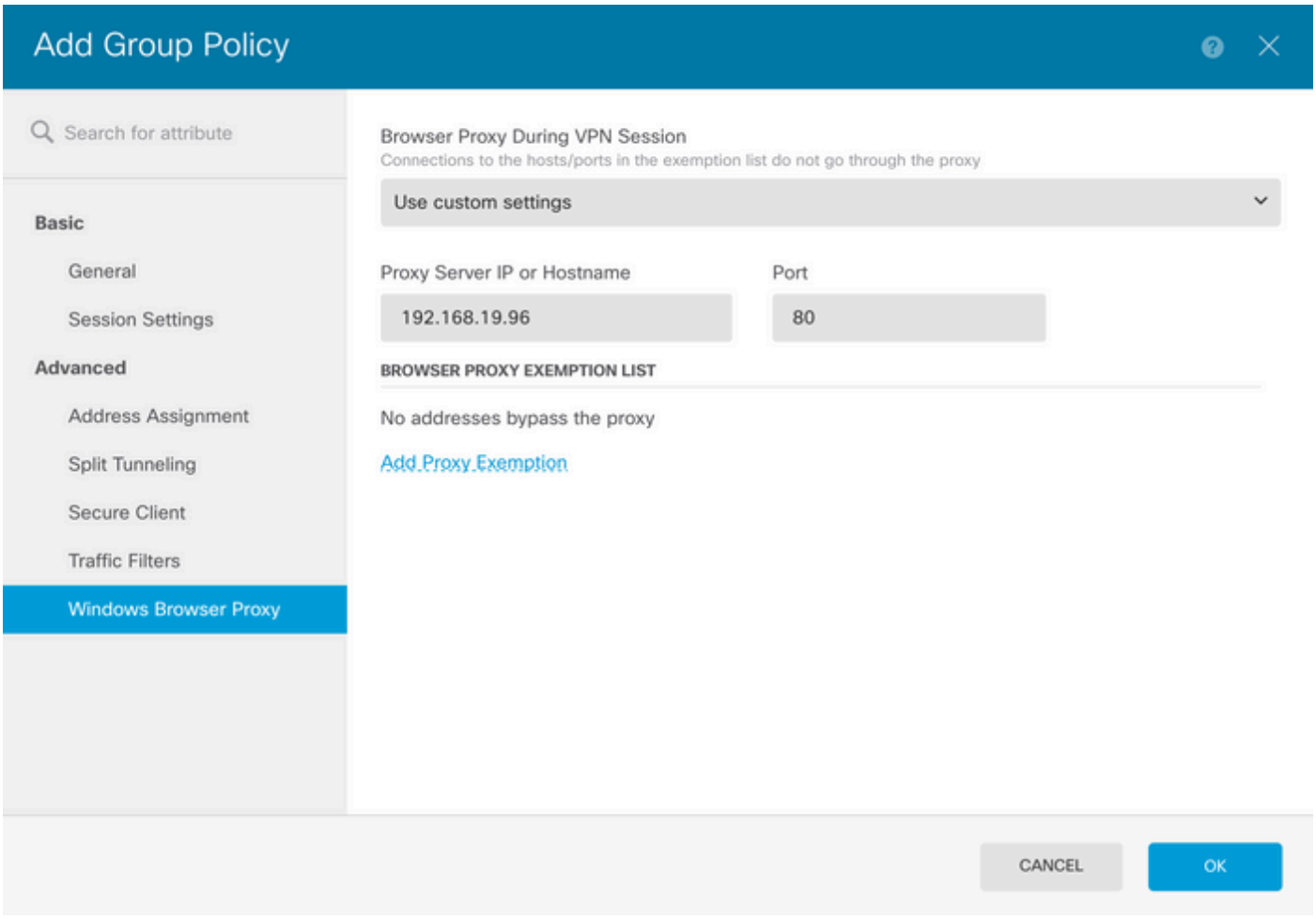
En FDM, navegue hasta Remote Access VPN > Group Policies, haga clic en el botón Edit en la Directiva de Grupo donde desea configurar el proxy del navegador, y navegue a la sección Windows Browser Proxy.



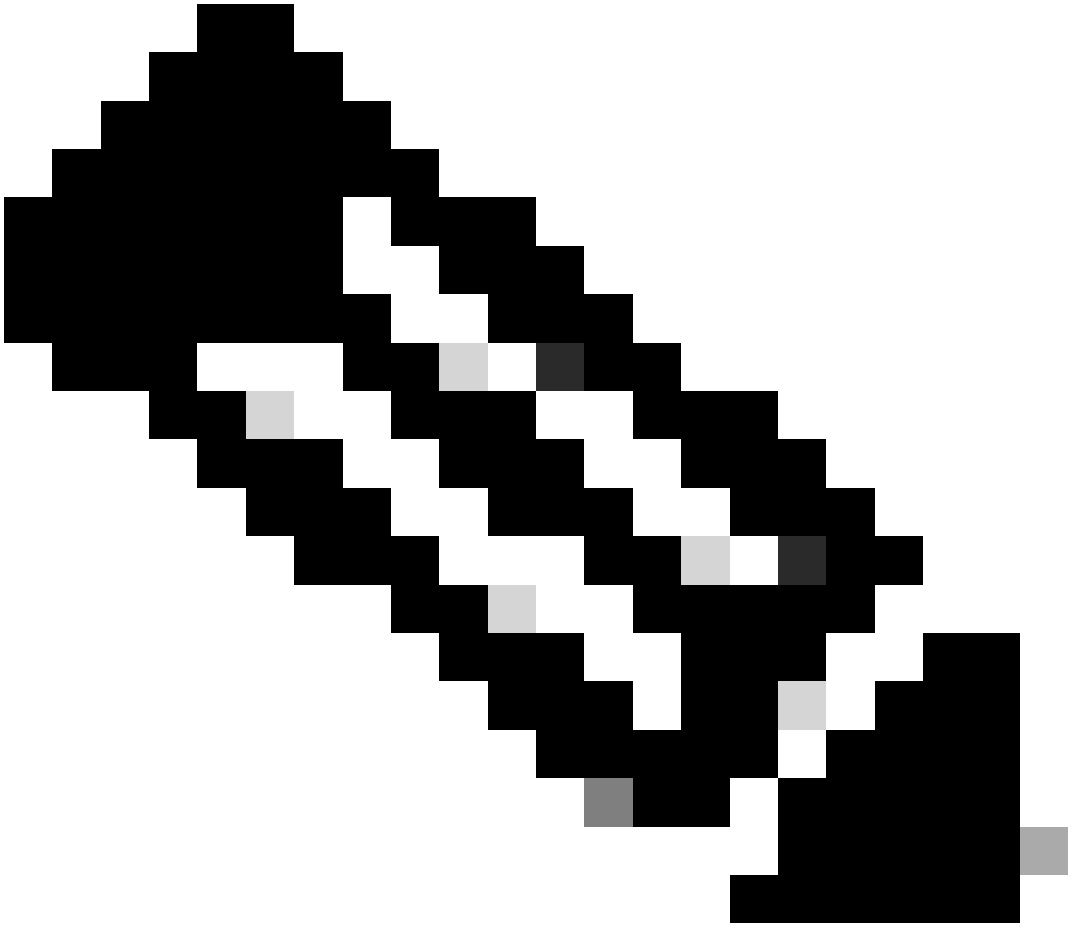
En el menú desplegable Browser Proxy During VPN Session, seleccione Use custom settings .



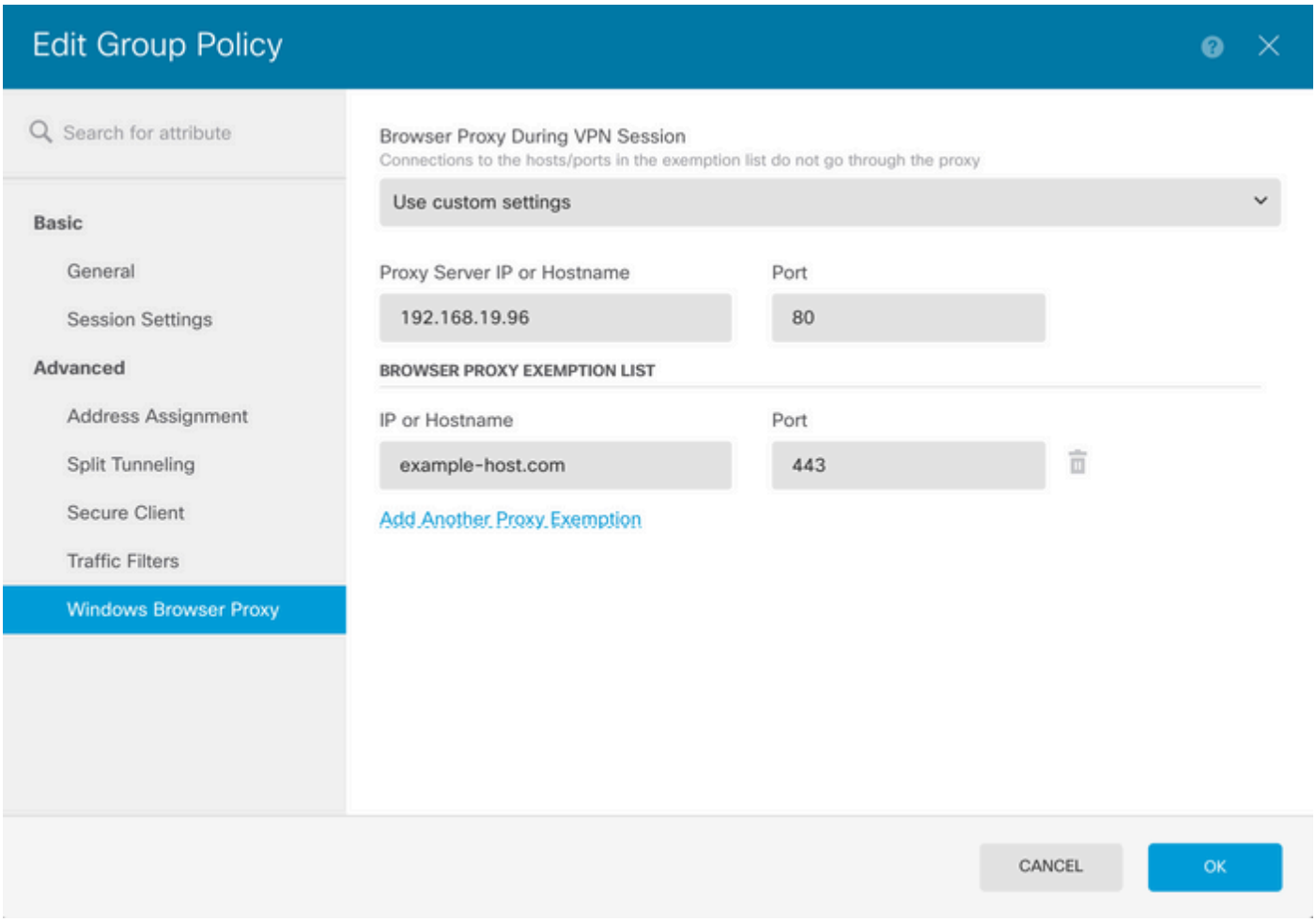
En el cuadro Proxy Server IP or Hostname, ingrese la información del servidor proxy y en el cuadro Port, ingrese el puerto para alcanzar el servidor.



Si hay una dirección o un nombre de host al que no desea acceder a través del proxy, haga clic en el botón Add Proxy Exemption y agréguelo aquí.



Nota: la especificación de un puerto en la lista de excepciones de proxy del explorador es opcional.



Haga clic en Aceptar e implemente la configuración.

Verificación

Para comprobar si la configuración se ha aplicado correctamente, puede utilizar la CLI del FTD.

<#root>

```
firepower# show running-config group-policy
group-policy ProxySettings internal
group-policy ProxySettings attributes
dns-server value 10.28.28.1
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
```

msie-proxy server value 192.168.19.96:80

```
msie-proxy method use-server


msie-proxy except-list value example-host.com:443


msie-proxy local-bypass enable


vlan none
address-pools value AC_Pool
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles none
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting
```

Troubleshoot

Puede recopilar un paquete DART y comprobar que se ha aplicado el perfil VPN:

<#root>

```
****************************************

Date : 07/20/2023
Time : 21:50:08
Type : Information
Source : csc_vpnagent

Description : Current Profile: none
Received VPN Session Configuration Settings:
Keep Installed: enabled
Rekey Method: disabled

Proxy Setting: bypass-local, server


Proxy Server: 192.168.19.96:80


Proxy PAC URL: none
```

Proxy Exceptions: example-host.com:443

Proxy Lockdown: enabled

IPv4 Split Exclude: disabled
IPv6 Split Exclude: disabled
IPv4 Dynamic Split Exclude: 3 excluded domain(s)
IPv6 Dynamic Split Exclude: disabled
IPv4 Split Include: disabled
IPv6 Split Include: disabled
IPv4 Dynamic Split Include: disabled
IPv6 Dynamic Split Include: disabled
IPv4 Split DNS: disabled
IPv6 Split DNS: disabled
Tunnel all DNS: disabled
IPv4 Local LAN Wildcard: disabled
IPv6 Local LAN Wildcard: disabled
Firewall Rules: none
Client Address: 172.16.28.1
Client Mask: 255.255.255.0
Client IPv6 Address: FE80:0:0:0:ADSD:3F37:374D:3141 (auto-generated)
Client IPv6 Mask: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFC
TLS MTU: 1399
TLS Compression: disabled
TLS Keep Alive: disabled
TLS Rekey Interval: none
TLS DPD: 0 seconds
DTLS: disabled
DTLS MTU: none
DTLS Compression: disabled
DTLS Keep Alive: disabled
DTLS Rekey Interval: none
DTLS DPD: 30 seconds
Session Timeout: none
Session Timeout Alert Interval: 60 seconds
Session Timeout Remaining: none
Disconnect Timeout: 1800 seconds
Idle Timeout: 1800 seconds
Server: ASA (9.19(1))
MUS Host: unknown
DAP User Message: n
Quarantine State: disabled
Always On VPN: not disabled
Lease Duration: 1209600 seconds
Default Domain: unknown
Home page: unknown
Smart Card Removal Disconnect: enabled
License Response: unknown
SG TCP Keep Alive: enabled
Peer's Local IPv4 Address: N/A
Peer's Local IPv6 Address: N/A
Peer's Remote IPv4 Address: N/A
Peer's Remote IPv6 Address: N/A
Peer's host name: firepower
Client Protocol Bypass: false
Tunnel Optimization: enabled

****

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).