

Configurar Proxies de Navegador do Windows em Cliente Seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar os proxies do Navegador do Windows para o Cisco Secure Client conectado ao FTD Gerenciado pelo FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Gerenciador de dispositivos do Cisco Secure Firewall (FDM)
- Defesa contra ameaças (FTD) do Cisco Firepower
- Cisco Secure Client (CSC)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall Device Manager versão 7.3
- Dispositivo virtual Cisco Firepower Threat Defense versão 7.3
- Cisco Secure Client Versão 5.0.02075

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O termo "proxy" refere-se a um serviço localizado entre o usuário e o recurso que você deseja acessar. Os proxies do navegador da Web, especificamente, são servidores que transmitem o tráfego da Web; portanto, ao navegar para um site, o Secure Client solicita que o servidor proxy solicite o site em vez de fazê-lo diretamente.

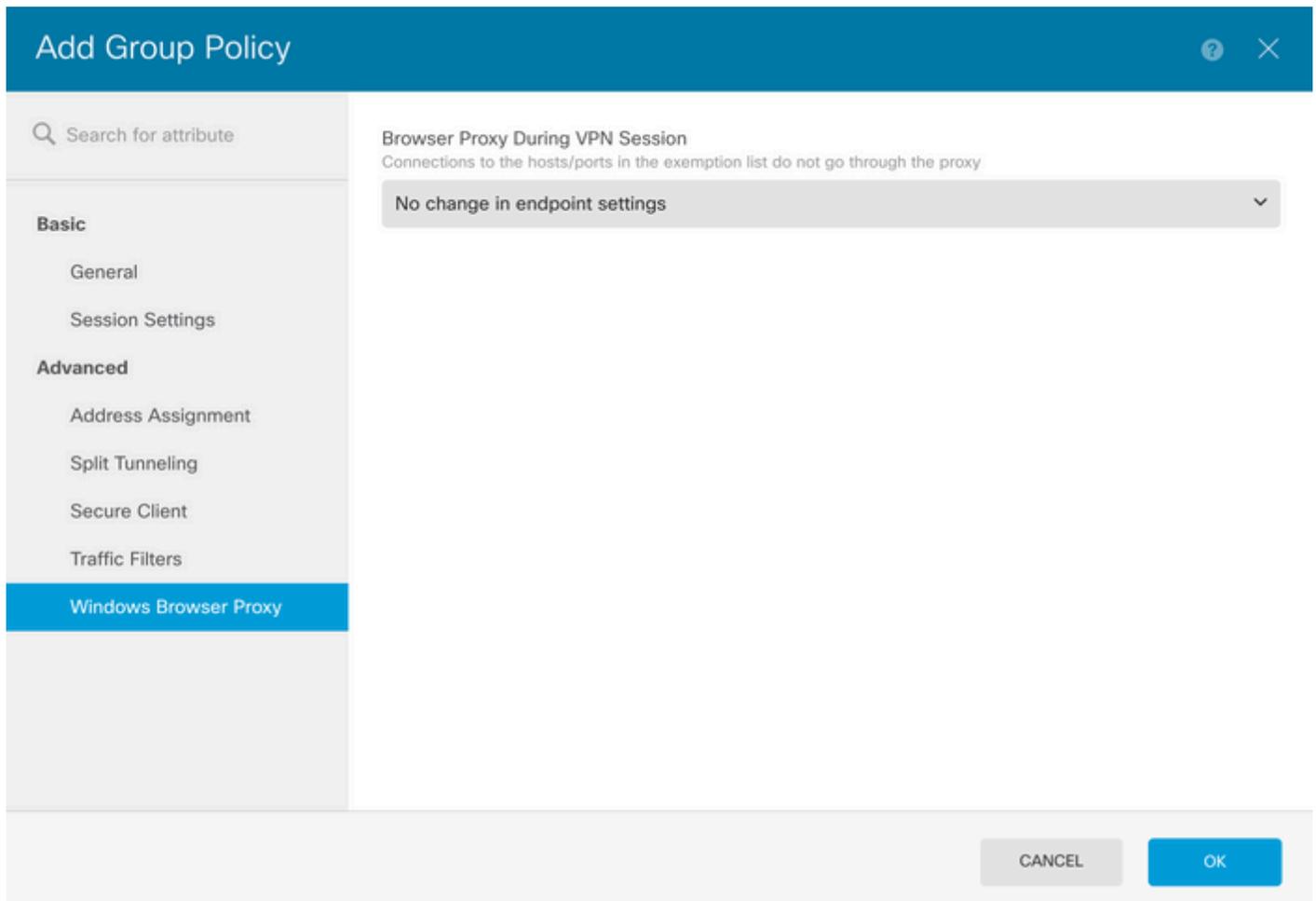
Os proxies podem ser usados para atingir diferentes objetivos, como filtragem de conteúdo, tratamento de tráfego e tunelamento de tráfego.

Configurar

Configurações

Neste documento, supõe-se que você já tenha uma configuração de VPN de acesso remoto em funcionamento.

No FDM, navegue até Acesso Remoto VPN > Políticas de Grupo, clique no botão Editar na Política de Grupo onde deseja configurar o proxy do navegador e navegue até a seção Proxy do Navegador do Windows .



No menu suspenso Browser Proxy During VPN Session, selecione Use custom settings.

Add Group Policy ? ×

Search for attribute

Basic

- General
- Session Settings

Advanced

- Address Assignment
- Split Tunneling
- Secure Client
- Traffic Filters
- Windows Browser Proxy**

Browser Proxy During VPN Session
Connections to the hosts/ports in the exemption list do not go through the proxy

Use custom settings

Proxy Server IP or Hostname Port

BROWSER PROXY EXEMPTION LIST

No addresses bypass the proxy

[Add Proxy Exemption](#)

CANCEL OK

Na caixa Proxy Server IP or Hostname, insira as informações do servidor proxy e, na caixa Port, insira a porta para acessar o servidor.

Add Group Policy



Search for attribute

Basic

General

Session Settings

Advanced

Address Assignment

Split Tunneling

Secure Client

Traffic Filters

Windows Browser Proxy

Browser Proxy During VPN Session

Connections to the hosts/ports in the exemption list do not go through the proxy

Use custom settings

Proxy Server IP or Hostname

192.168.19.96

Port

80

BROWSER PROXY EXEMPTION LIST

No addresses bypass the proxy

[Add Proxy Exemption](#)

CANCEL

OK

Se houver um endereço ou nome de host que você não deseja acessar por meio do proxy, clique no botão Add Proxy Exemption e adicione-o aqui.



Observação: a especificação de uma porta na Lista de Isenção de Proxy do Navegador é opcional.

Edit Group Policy
? ×

🔍 Search for attribute

Basic

- General
- Session Settings

Advanced

- Address Assignment
- Split Tunneling
- Secure Client
- Traffic Filters
- Windows Browser Proxy

Browser Proxy During VPN Session

Connections to the hosts/ports in the exemption list do not go through the proxy

Use custom settings
▼

Proxy Server IP or Hostname	Port
192.168.19.96	80

BROWSER PROXY EXEMPTION LIST

IP or Hostname	Port
example-host.com	443 🗑️

[Add Another Proxy Exemption](#)

CANCEL
OK

Clique em Ok e implante a configuração.

Verificar

Para verificar se a configuração foi aplicada com êxito, você pode usar a CLI do 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

Troubleshooting

Você pode coletar um pacote DART e verificar se o perfil VPN foi aplicado:

<#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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.