

Windows-browserproxy's op beveiligde client configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u Windows Browser Proxies kunt configureren voor Cisco Secure Client die is aangesloten op FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over deze onderwerpen:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Firewall Device Manager versie 7.3
- Cisco Firepower Threat Defense virtuele applicatie versie 7.3
- Cisco Secure-client versie 5.0.02075

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De term "proxy" verwijst naar een service die zich bevindt tussen de gebruiker en de bron die u wilt bereiken. Web browser proxies, specifiek, zijn servers die webverkeer overbrengen, dus wanneer het navigeren naar een website, de Secure Client vraagt de proxy server om de site te vragen in plaats van het direct te doen.

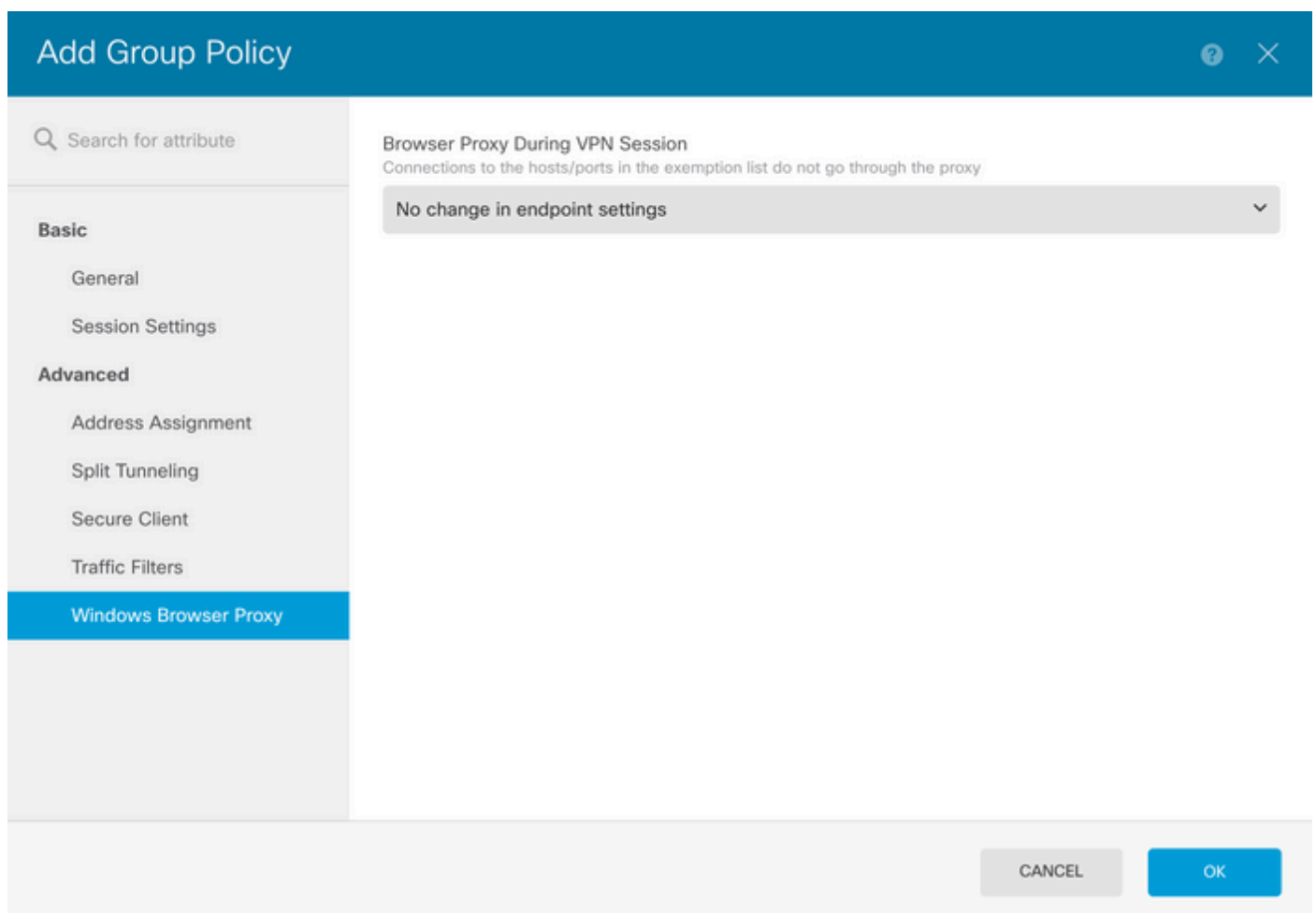
Proxies kunnen worden gebruikt om verschillende doelstellingen te bereiken, zoals contentfiltering, traffic handling en traffic tunneling.

Configureren

Configuraties

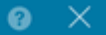
In dit document wordt aangenomen dat u al een werkende Remote Access VPN-configuratie hebt.

In de FDM, navigeer aan Verre Toegang VPN > het Beleid van de Groep, klik de Edit knop op het Beleid van de Groep waar u de browser volmacht wilt vormen, en navigeer aan de sectie van de Browser van Windows Proxy.



Selecteer Aangepaste instellingen gebruiken in de vervolgkeuzelijst Browser Proxy tijdens VPN-sessie.

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

Voer in het vak Proxyserver IP of Hostname de gegevens van de proxyserver in en voer in het vak Poortserver de poort in om de server te bereiken.

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

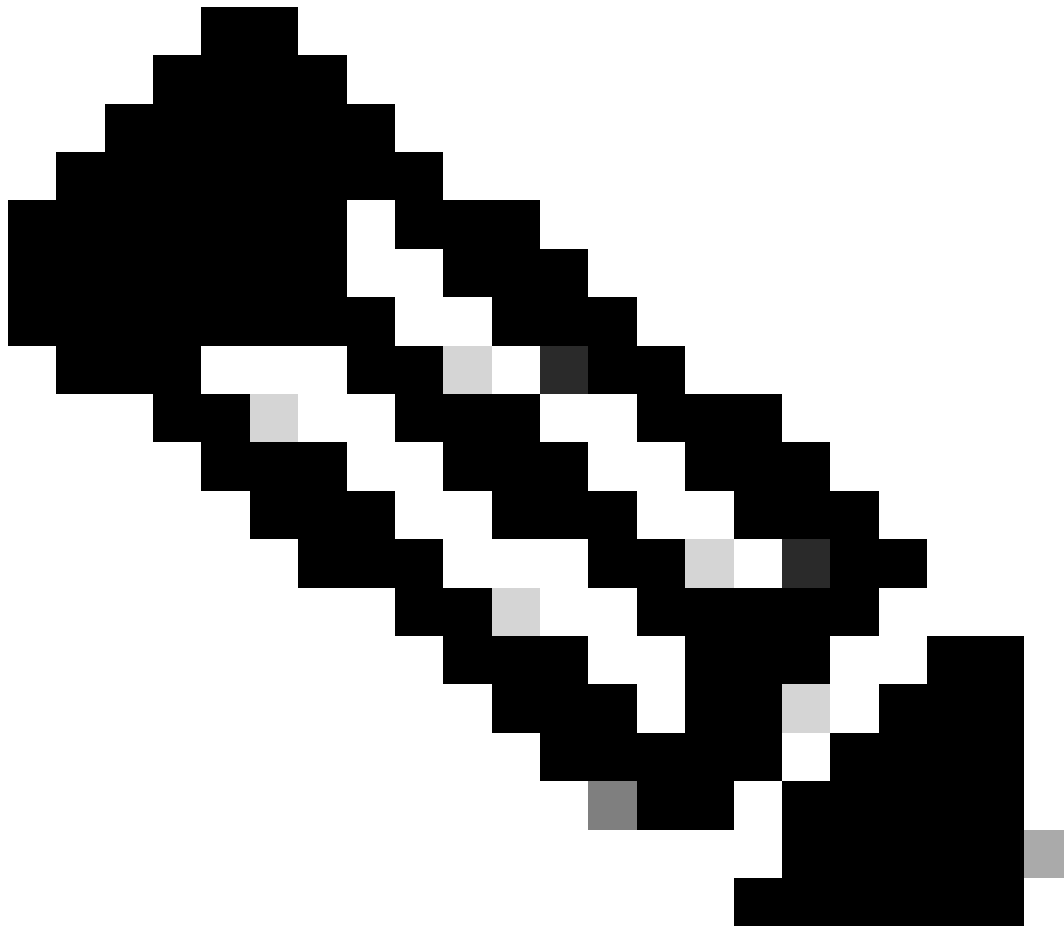
No addresses bypass the proxy

[Add Proxy Exemption](#)

CANCEL

OK

Als er een adres of hostname is dat u niet wilt bereiken via de proxy, klik dan op de knop Proxy-vrijstelling toevoegen en voeg het hier toe.



Opmerking: het opgeven van een poort in de vrijstellingslijst voor browserproxy is optioneel.

Edit Group Policy
? X

🔍 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

Klik op OK en implementeer de configuratie.

Verifiëren

Om te verifiëren of de configuratie met succes is toegepast, kunt u de CLI van de FTD gebruiken.

<#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

Problemen oplossen

U kunt een DART-bundel verzamelen en controleren of het VPN-profiel is toegepast:

<#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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.