

セキュアクライアント上でのWindowsブラウザプロキシの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、FDMによって管理されるFTDに接続されたCisco Secure ClientのWindowsブラウザプロキシを設定する方法について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

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

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Device Managerバージョン7.3
- Cisco Firepower Threat Defense仮想アプライアンスバージョン7.3
- Cisco Secure Clientバージョン5.0.02075

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

「プロキシ」という用語は、ユーザと到達したいリソースの間にあるサービスを指します。Webブラウザプロキシは、特にWebトラフィックを送信するサーバです。そのため、Webサイトに移動すると、Secure Clientはプロキシサーバに対して、サイトを直接要求する代わりに要求を出します。

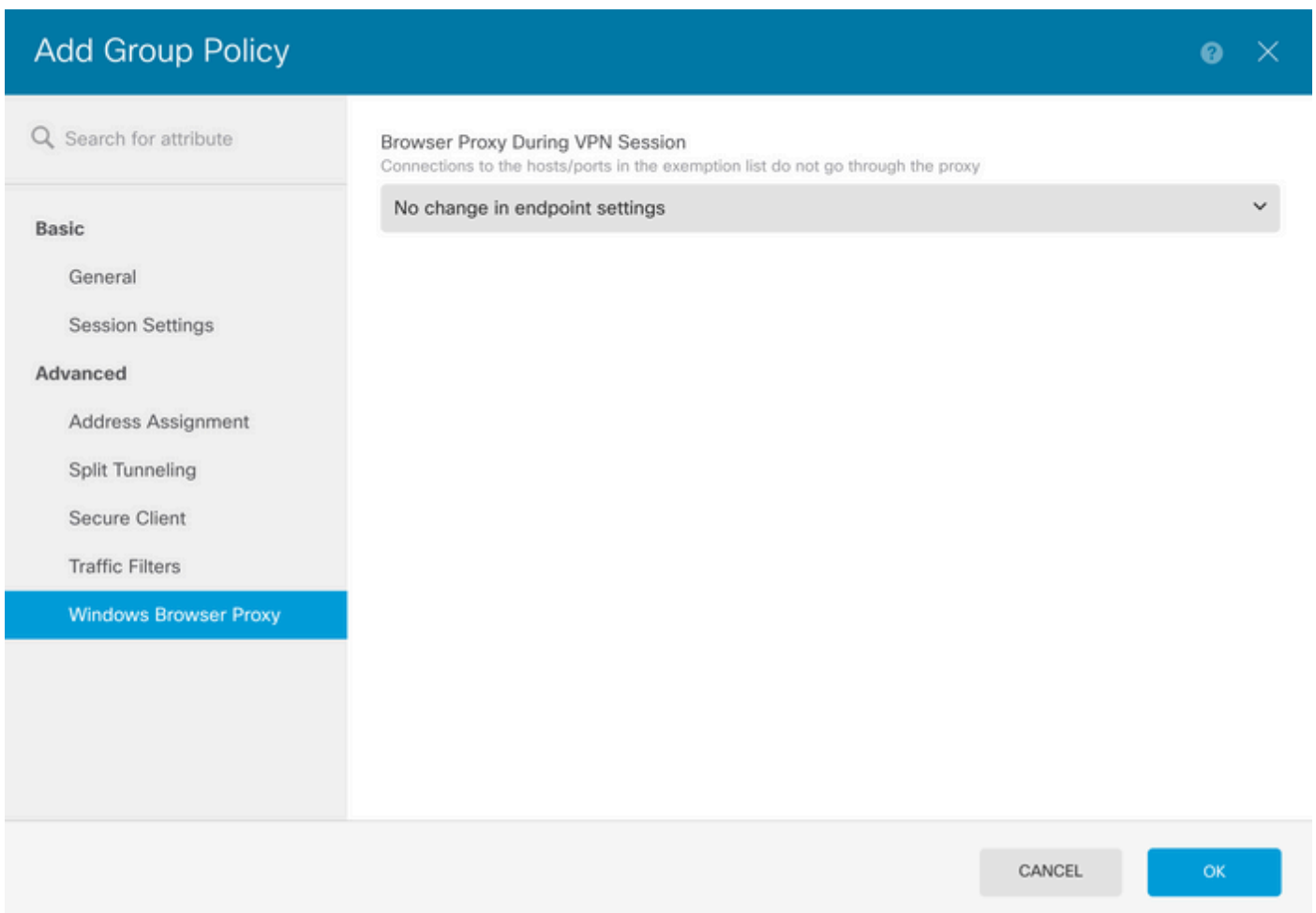
プロキシを使用すると、コンテンツフィルタリング、トラフィック処理、トラフィックトンネリングなどのさまざまな目的を達成できます。

設定

コンフィギュレーション

このドキュメントでは、すでに動作中のリモートアクセスVPN(RVPN)設定があることを前提としています。

FDMで、Remote Access VPN > Group Policiesの順に移動し、ブラウザプロキシを設定するグループポリシーのEditボタンをクリックして、Windows Browser Proxy セクションに移動します。



Browser Proxy During VPN Session ドロップダウンから、Use custom settings を選択します。

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

Proxy Server IP or Hostname ボックスにプロキシサーバ情報を入力し、Portボックスにサーバに到達するためのポートを入力します。

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

プロキシ経由で到達させたくないアドレスまたはホスト名がある場合は、Add Proxy Exemptionボタンをクリックして、ここで追加します。



注：ブラウザのプロキシ除外リストでポートを指定することはオプションです。

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

OKをクリックして、設定を展開します。

確認

設定が正常に適用されたかどうかを確認するには、FTDのCLIを使用します。

<#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

トラブルシューティング

DARTバンドルを収集して、VPNプロファイルが適用されていることを確認できます。

<#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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。