Configurer les serveurs proxy du navigateur Windows sur le client sécurisé

Table des matières

Introduction

Ce document décrit comment configurer les proxys du navigateur Windows pour le client sécurisé Cisco connecté à FTD géré par FDM.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gestionnaire de périphériques Cisco Secure Firewall Version 7.3
- Appareil virtuel de défense contre les menaces Cisco Firepower version 7.3
- Client sécurisé Cisco version 5.0.02075

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le terme « proxy » fait référence à un service situé entre l'utilisateur et la ressource que vous souhaitez atteindre. Les serveurs proxy de navigateur Web, en particulier, sont des serveurs qui transmettent le trafic Web. Ainsi, lors de la navigation vers un site Web, le client sécurisé invite le serveur proxy à demander le site au lieu de le faire directement.

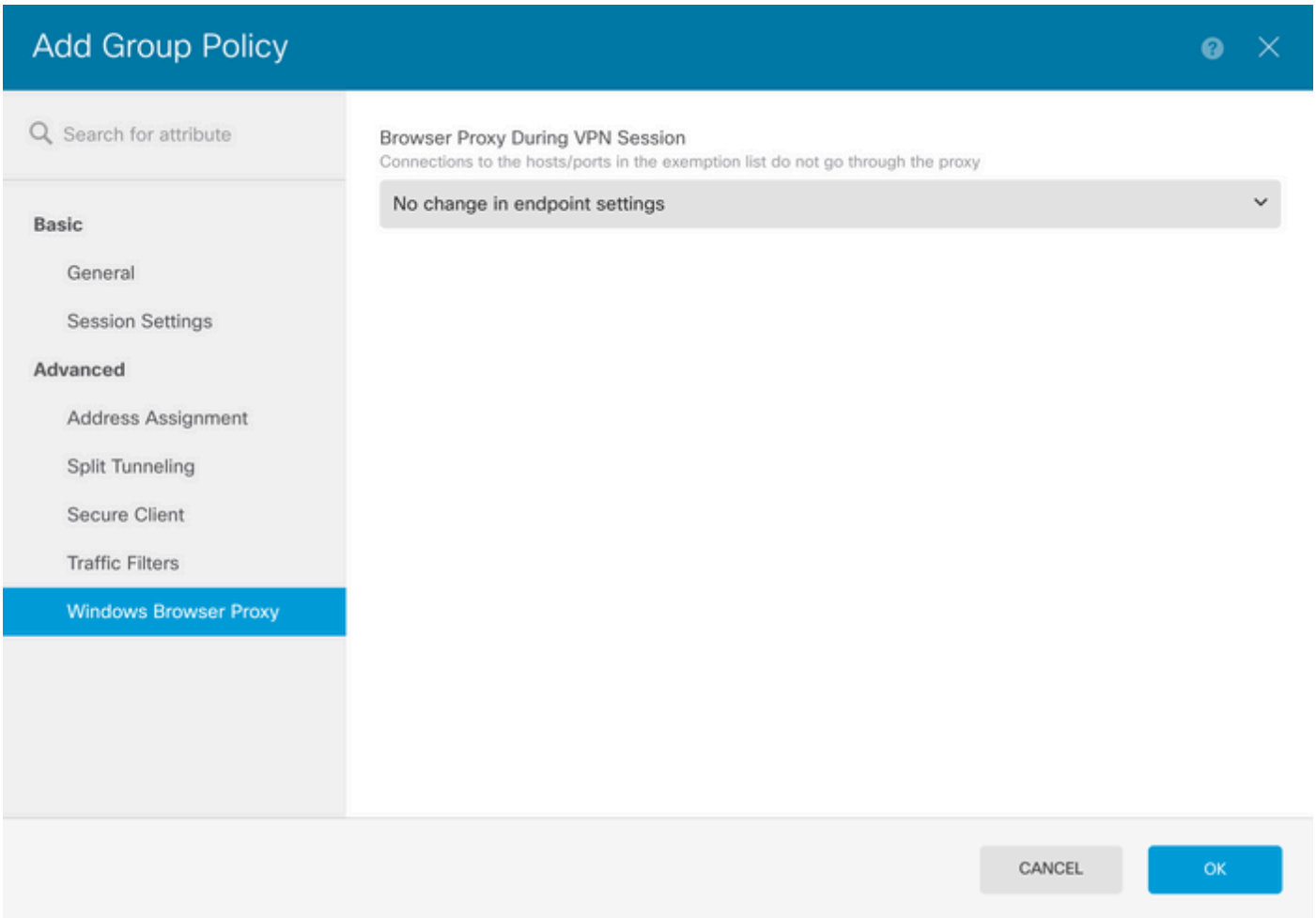
Les proxys peuvent être utilisés pour atteindre différents objectifs, tels que le filtrage de contenu, la gestion du trafic et la tunnellisation du trafic.

Configurer

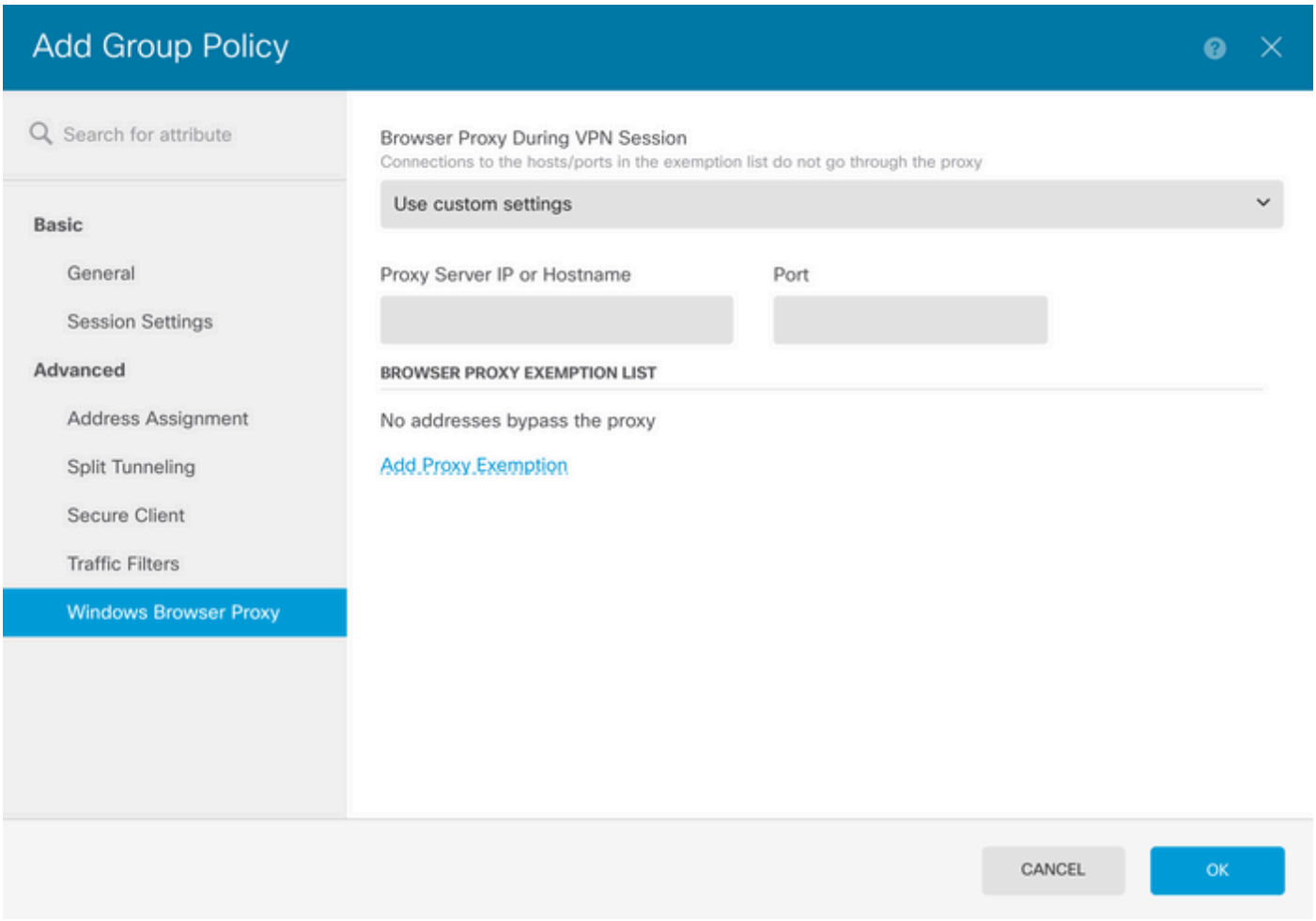
Configurations

Dans ce document, il est supposé que vous avez déjà une configuration VPN d'accès à distance opérationnelle.

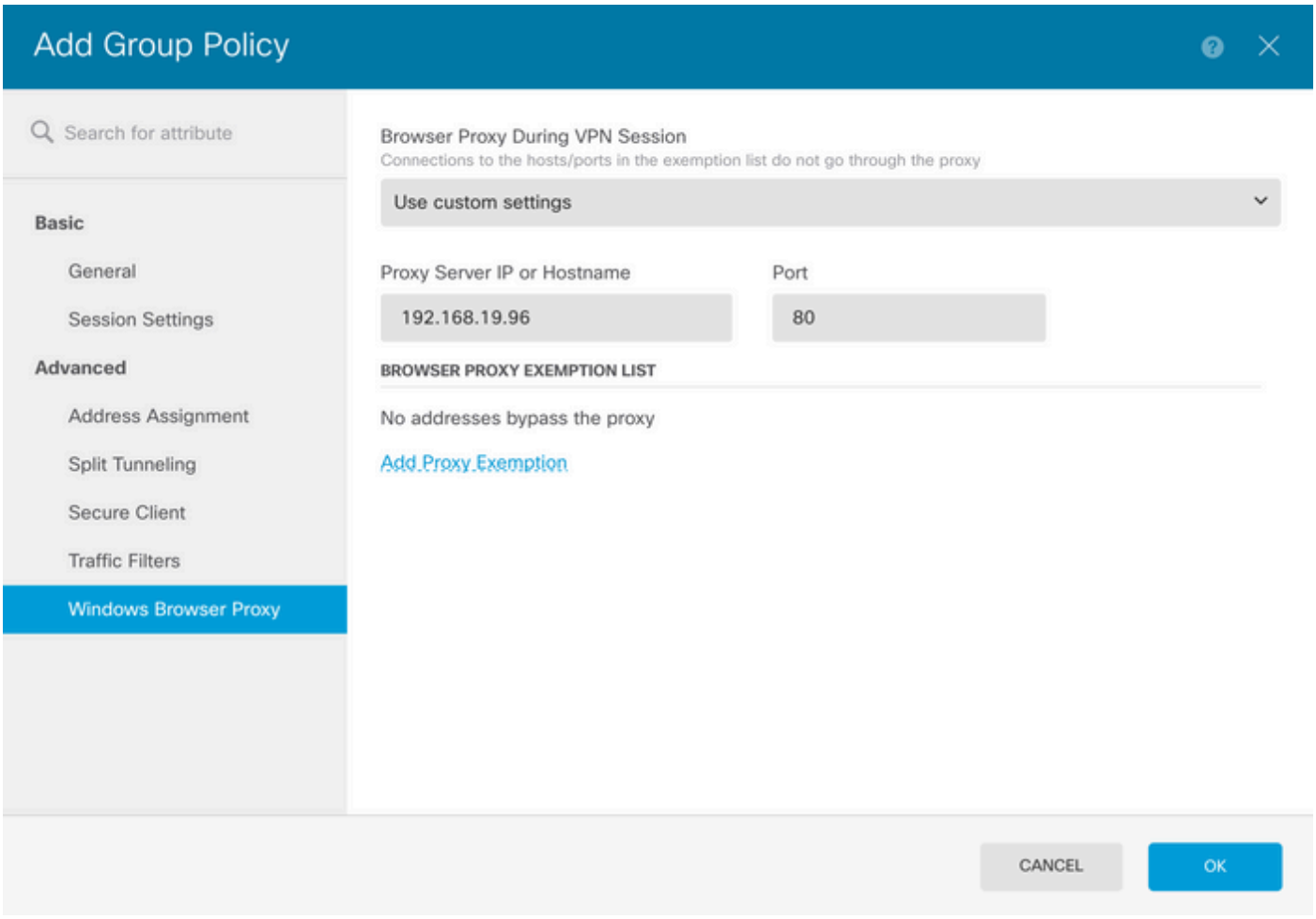
Dans FDM, accédez à Remote Access VPN > Group Policies, cliquez sur le bouton Edit sur la stratégie de groupe où vous voulez configurer le navigateur proxy, et accédez à la section Windows Browser Proxy.



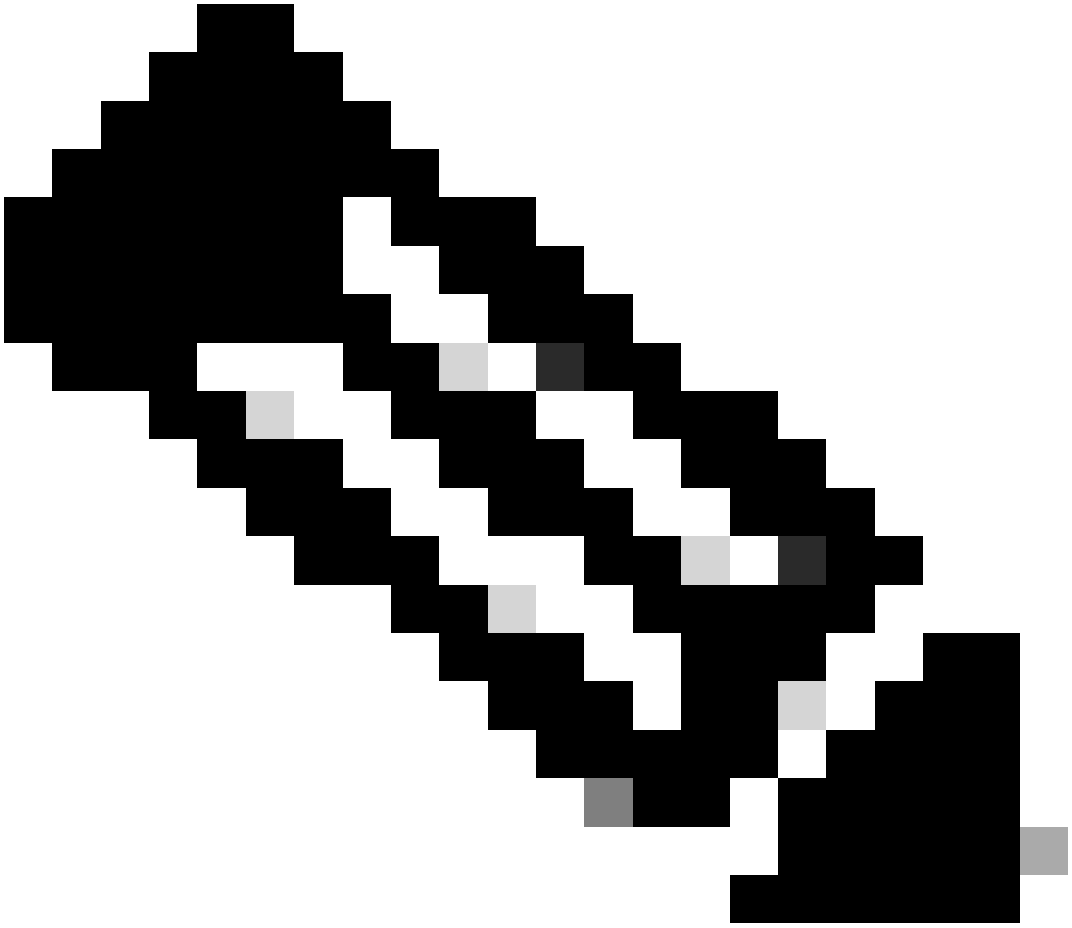
Dans la liste déroulante Browser Proxy During VPN Session, sélectionnez Use custom settings.



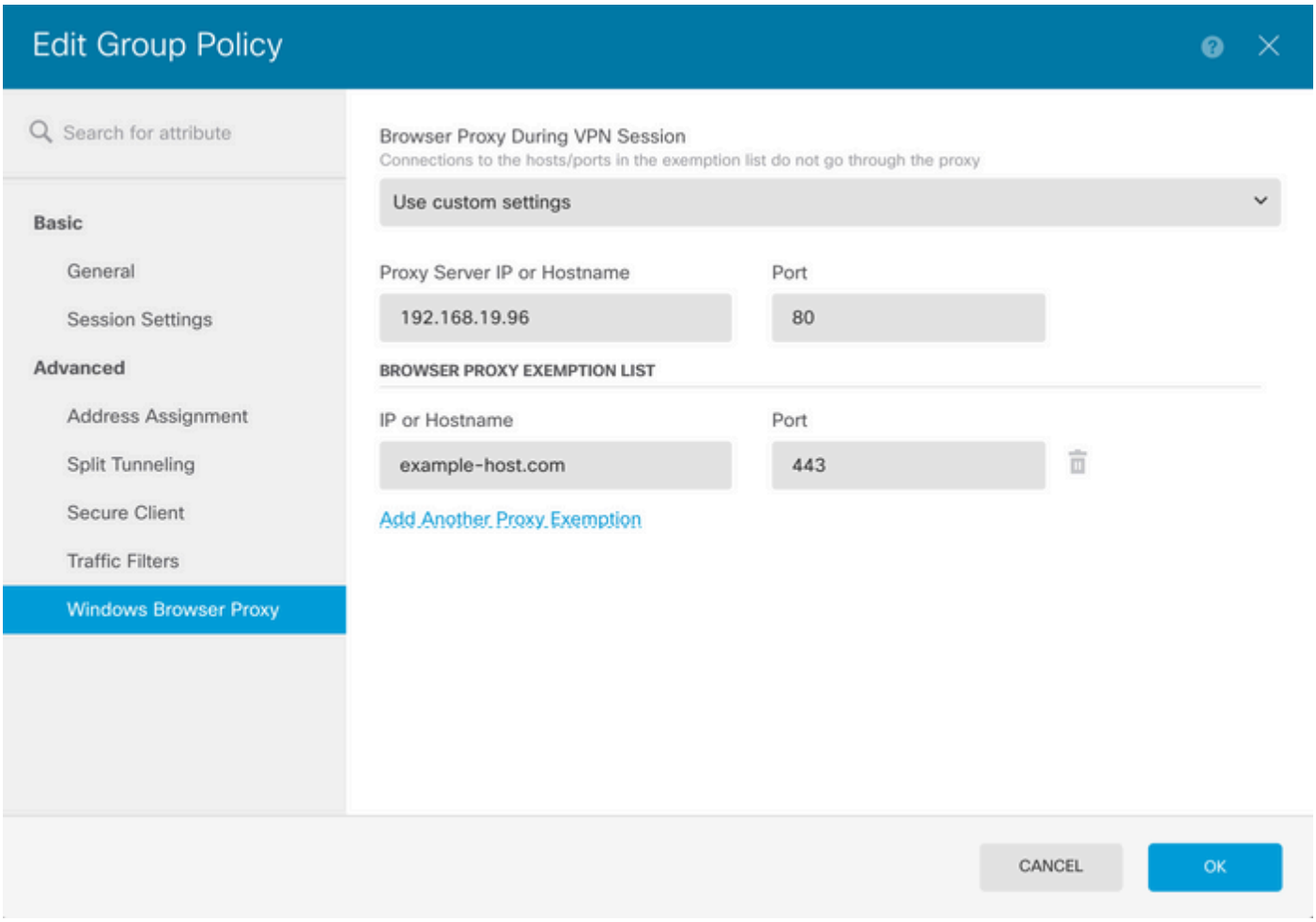
Dans la zone Proxy Server IP or Hostname, entrez les informations du serveur proxy et dans la zone Port, entrez le port permettant d'atteindre le serveur.



S'il y a une adresse ou un nom d'hôte que vous ne voulez pas atteindre par le proxy, cliquez sur le bouton Add Proxy Exemption et ajoutez-le ici.



Remarque : la spécification d'un port dans la liste d'exemptions de proxy de navigateur est facultative.



Cliquez sur Ok et déployez la configuration.

Vérifier

Pour vérifier si la configuration a été correctement appliquée, vous pouvez utiliser l'interface de ligne de commande du 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
```

Dépannage

Vous pouvez collecter un bundle DART et vérifier que le profil VPN a été appliqué :

<#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

****

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.