在安全客戶端上配置Windows瀏覽器代理

目錄

簡介

本檔案介紹如何為連線至FDM管理的FTD的Cisco Secure Client設定Windows瀏覽器代理。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全防火牆裝置管理員(FDM)
- Cisco Firepower威脅防禦(FTD)
- 思科安全使用者端(CSC)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆裝置管理員版本7.3
- Cisco Firepower威脅防禦虛擬裝置版本7.3
- 思科安全使用者端5.0.02075版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

術語「代理」是指位於使用者和您想訪問的資源之間的服務。Web瀏覽器代理是傳輸Web流量的伺服器，因此，在導航到網站時，安全客戶端會提示代理伺服器請求站點，而不是直接請求。

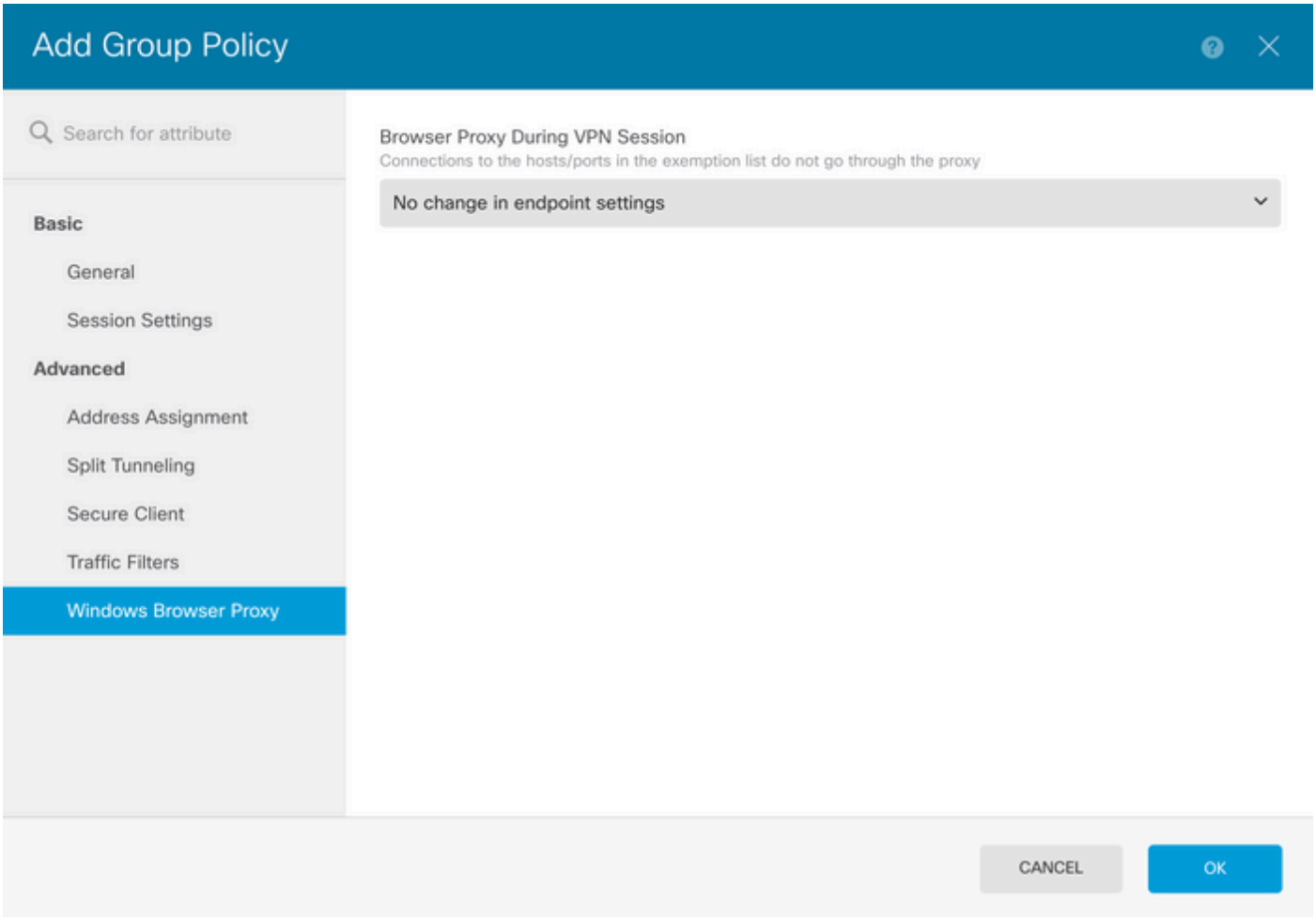
代理可用於實現不同的目標，例如內容過濾、流量處理和流量隧道。

設定

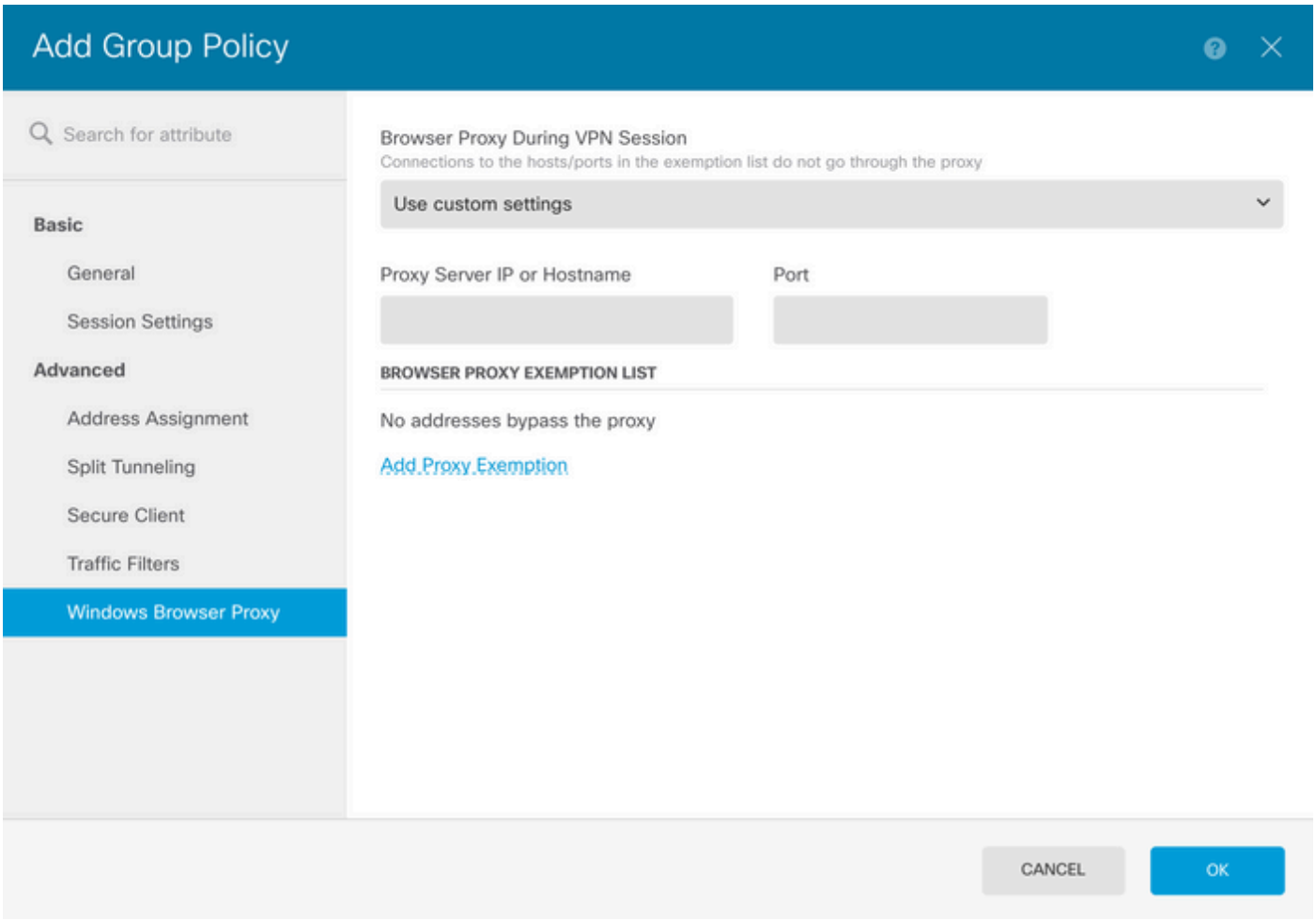
組態

在本文檔中，假定您已經有一個正在工作的遠端訪問VPN配置。

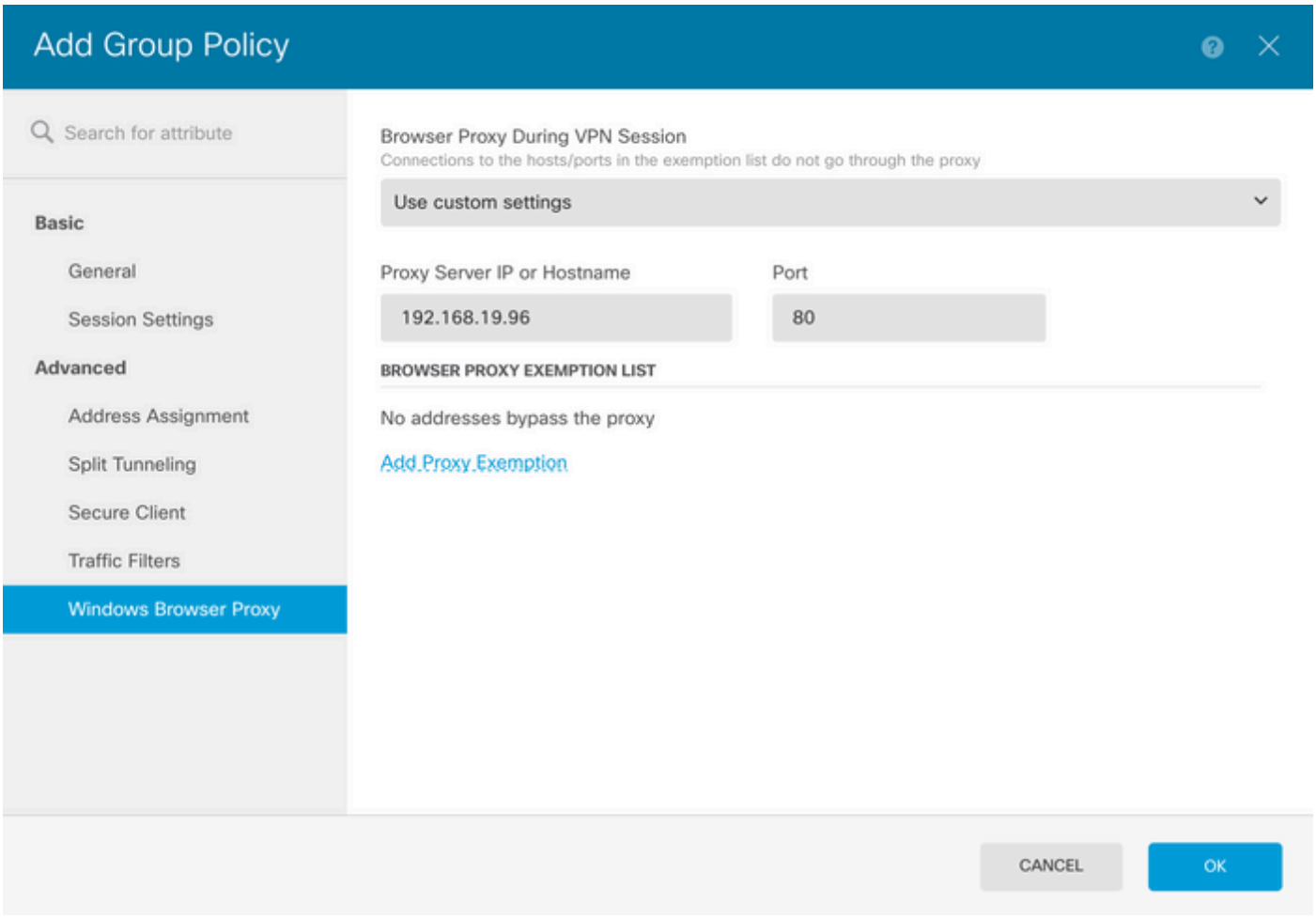
在FDM中，導航到遠端接入VPN >組策略，在要配置瀏覽器Proxy的組策略上按一下編輯按鈕，然後導航到Windows瀏覽器代理部分。



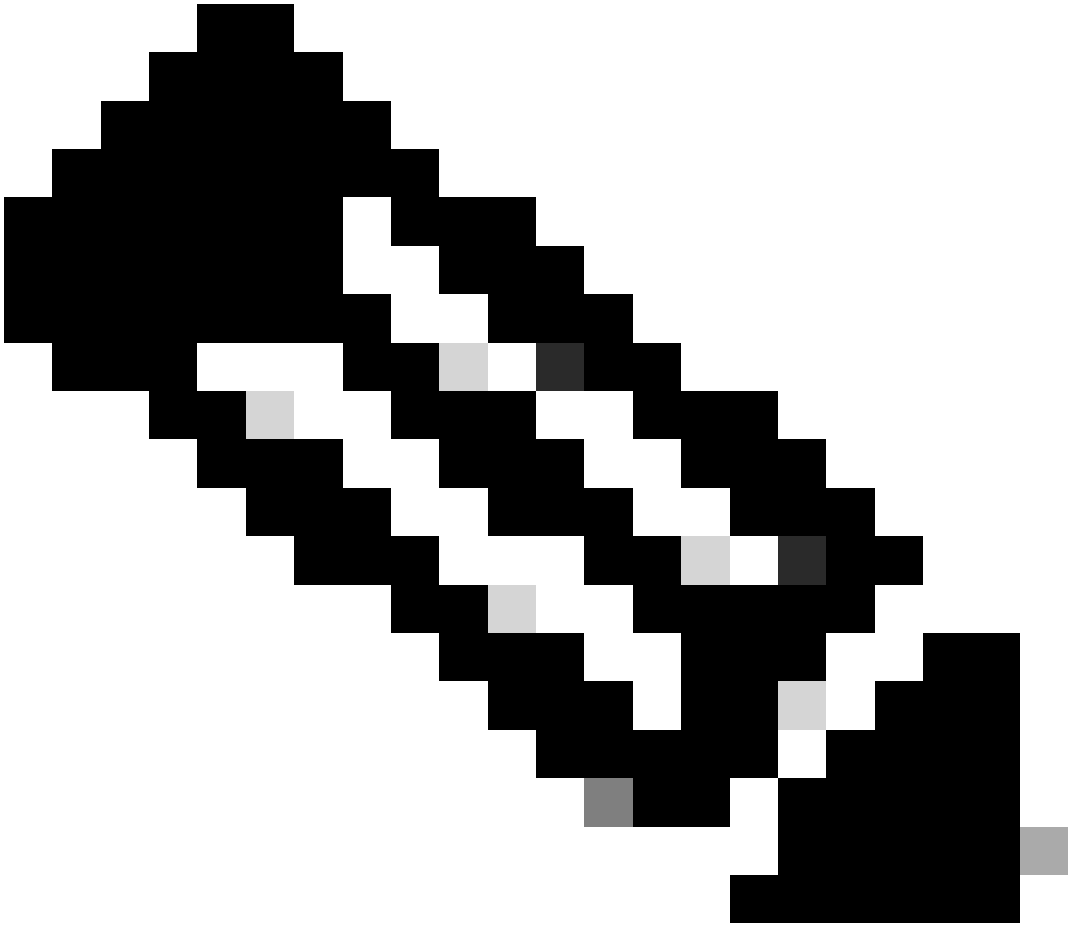
從Browser Proxy During VPN Session下拉選單中選擇Use custom settings。



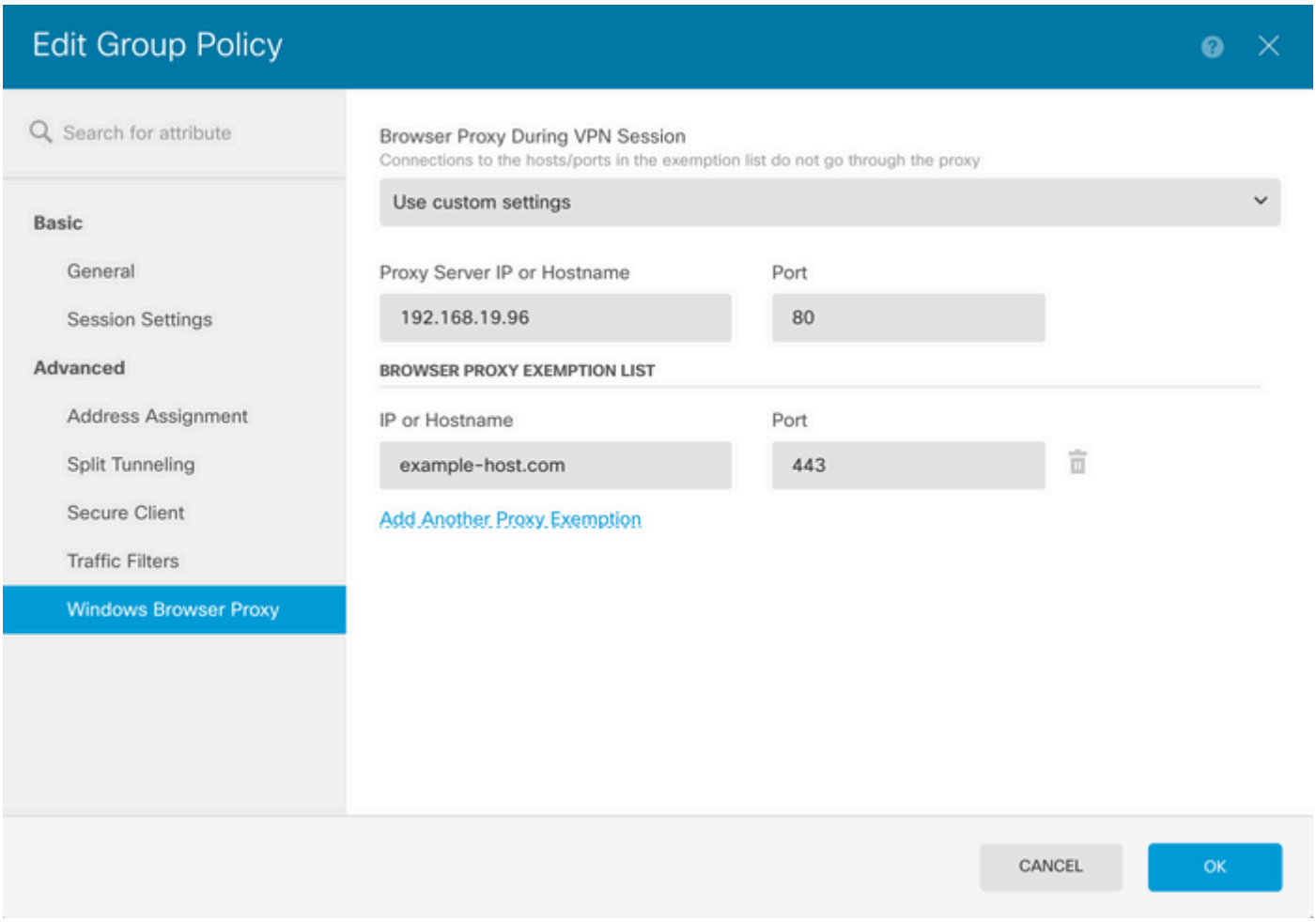
在Proxy Server IP or Hostname框中，輸入代理伺服器資訊，並在Port框中輸入用於訪問伺服器的埠。



如果不想透過Proxy訪問某個地址或主機名，請按一下Add Proxy Exemption 按鈕並在此處增加。



注意：在瀏覽器代理免除清單上指定埠是可選的。



按一下Ok並部署配置。

驗證

若要驗證組態是否成功套用，您可以使用FTD的CLI。

<#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
```

疑難排解

您可以收集DART捆綁包並驗證是否已應用VPN配置檔案：

<#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

****

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。