Konfigurieren von Windows-Browserproxys auf dem sicheren Client

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Windows-Browser-Proxys für den Cisco Secure Client konfigurieren, der mit dem von FDM verwalteten FTD verbunden ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Firewall Device Manager Version 7.3
- Cisco FirePOWER Threat Defense Virtual Appliance Version 7.3
- Cisco Secure Client Version 5.0.02075

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Der Begriff "Proxy" bezieht sich auf einen Dienst, der sich zwischen dem Benutzer und der Ressource befindet, die Sie erreichen möchten. Webbrowser-Proxys sind Server, die Webdatenverkehr übertragen. Beim Navigieren zu einer Website fordert der Secure Client daher den Proxyserver auf, die Website anzufordern, anstatt sie direkt anzufordern.

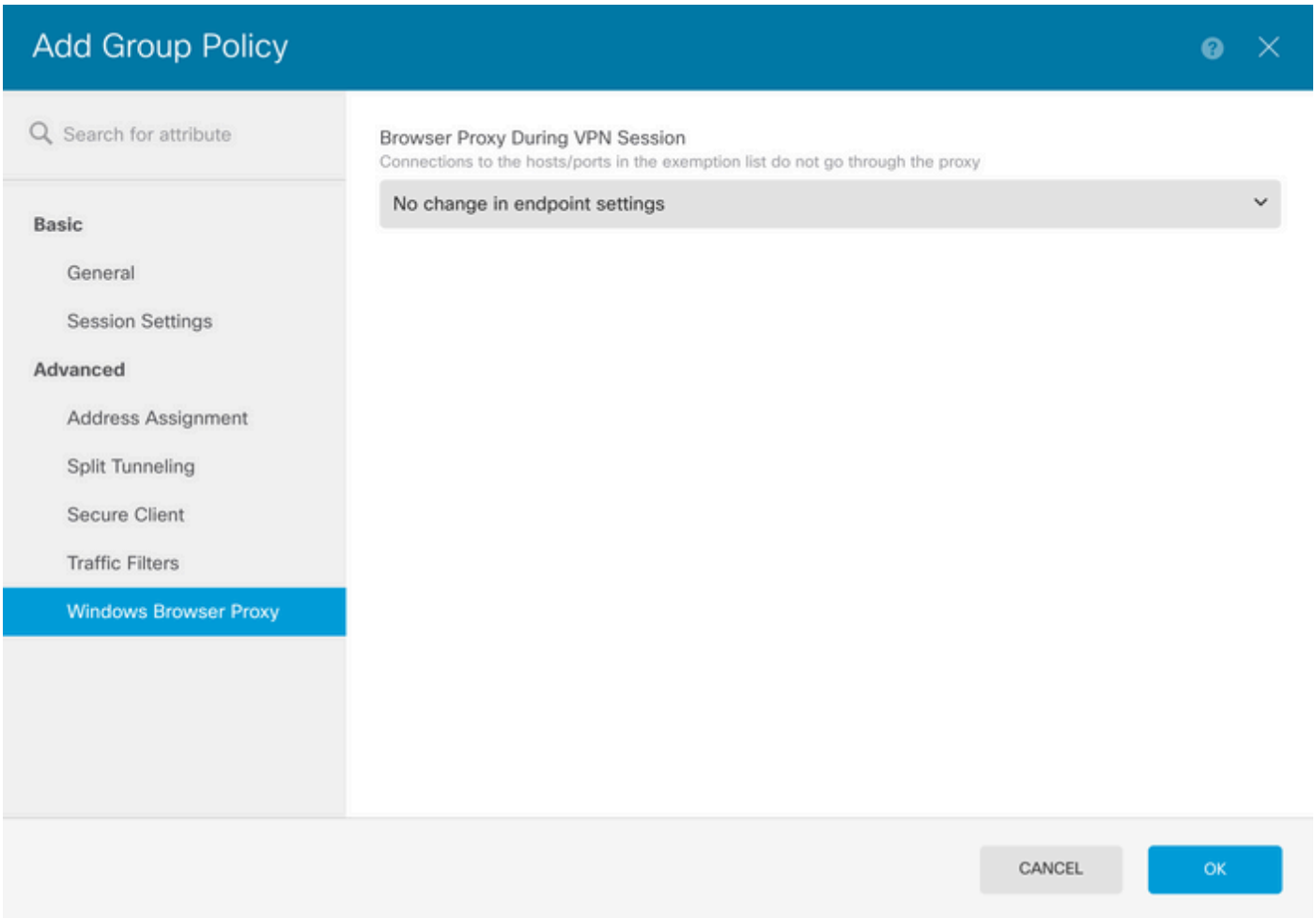
Proxys können verwendet werden, um unterschiedliche Ziele wie Content-Filterung, Datenverkehrsbehandlung und Datenverkehrstunneln zu erreichen.

Konfigurieren

Konfigurationen

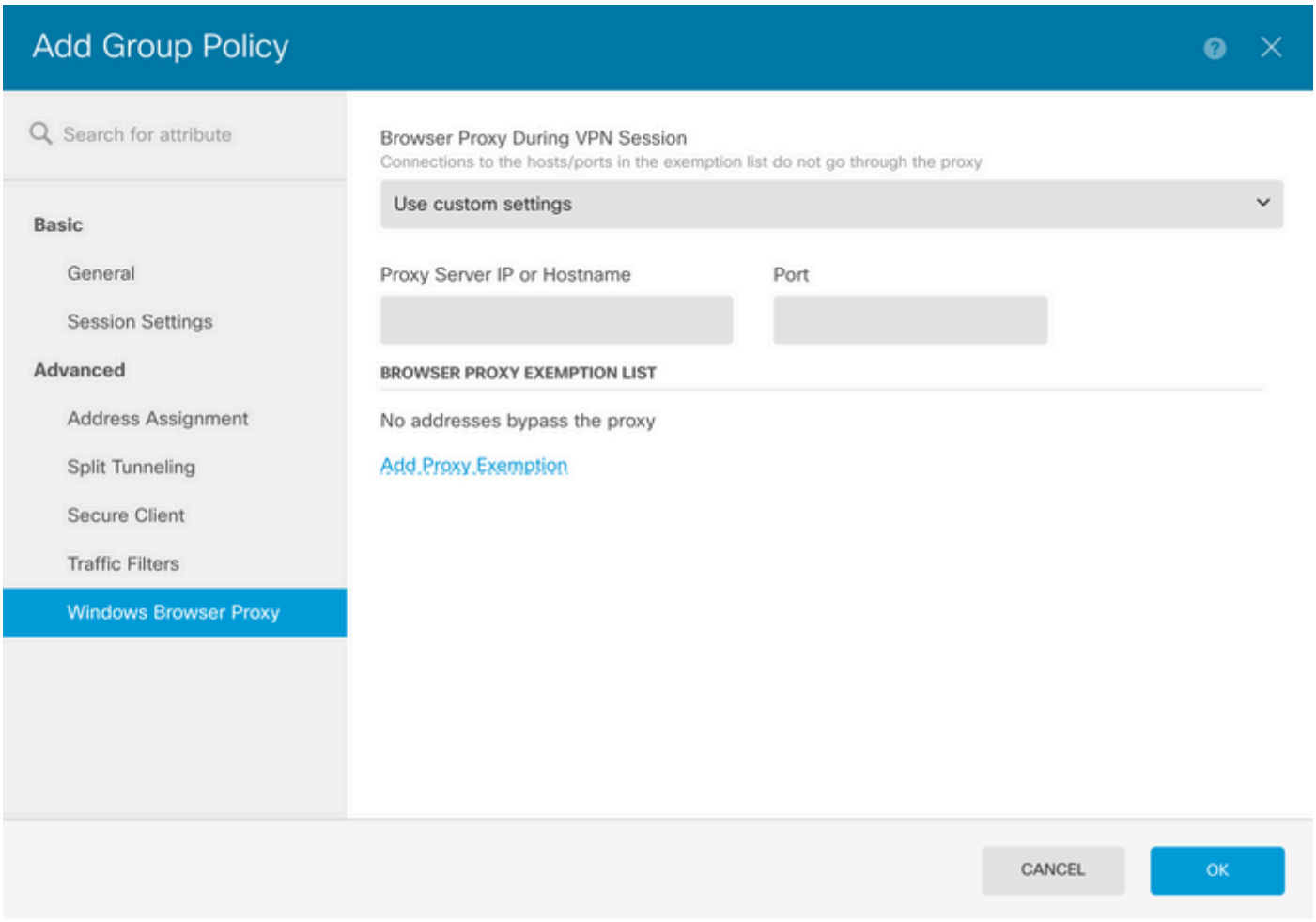
In diesem Dokument wird davon ausgegangen, dass Sie bereits über eine funktionierende VPN-Konfiguration verfügen.

Navigieren Sie im FDM zu Remotezugriff-VPN > Gruppenrichtlinien, klicken Sie auf die Schaltfläche Bearbeiten in der Gruppenrichtlinie, in der Sie den Browser-Proxy konfigurieren möchten, und navigieren Sie zum Abschnitt Windows-Browser-Proxy.

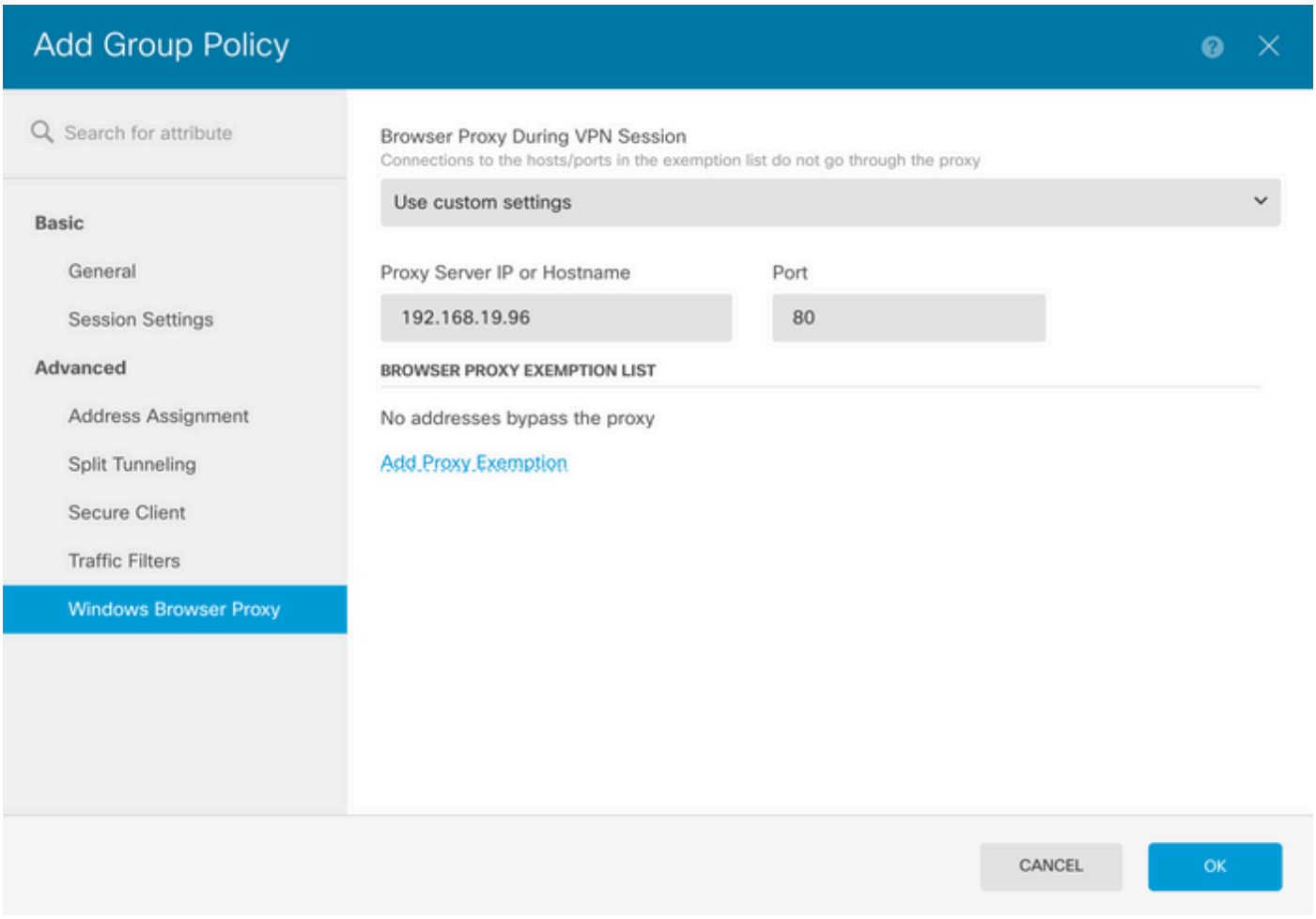


Wählen Sie aus dem Dropdown-Menü Browser Proxy While VPN Session (Browser-Proxy

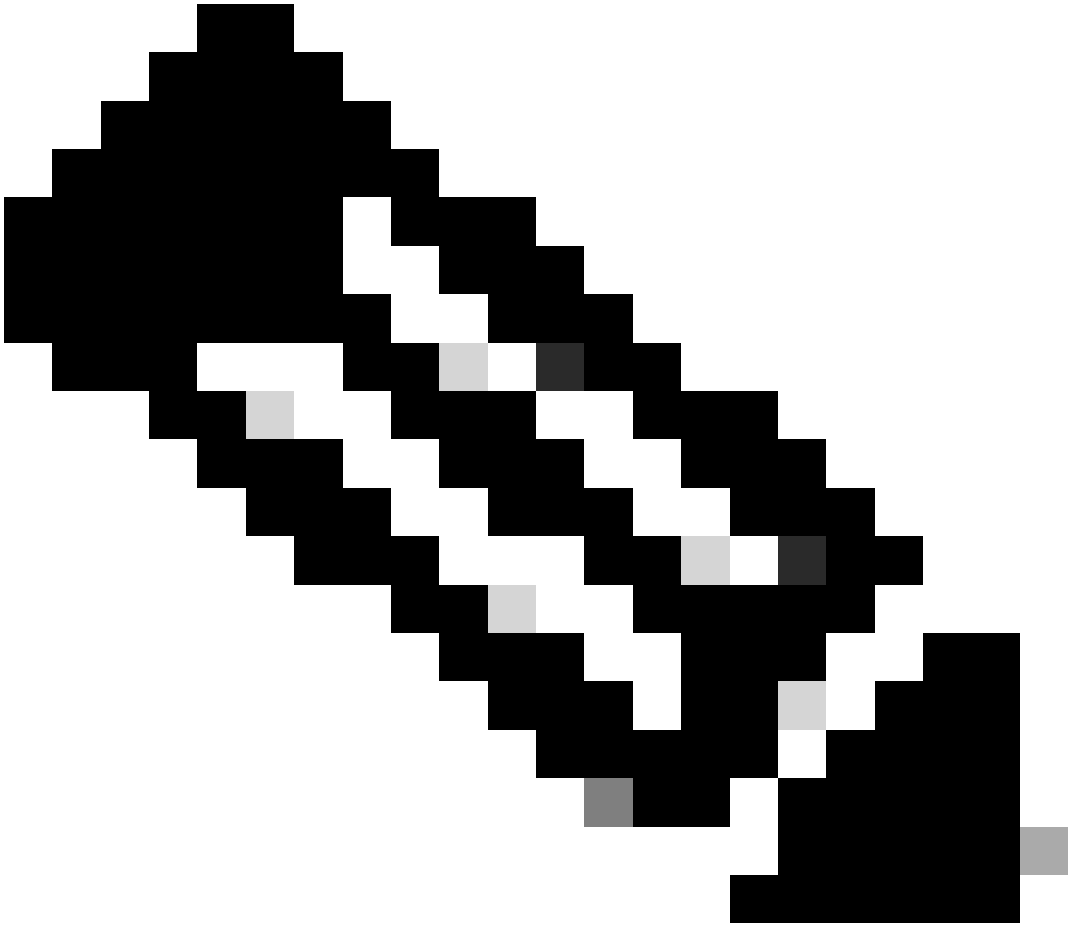
während VPN-Sitzung) die Option Use custom settings (Benutzerdefinierte Einstellungen verwenden) aus.



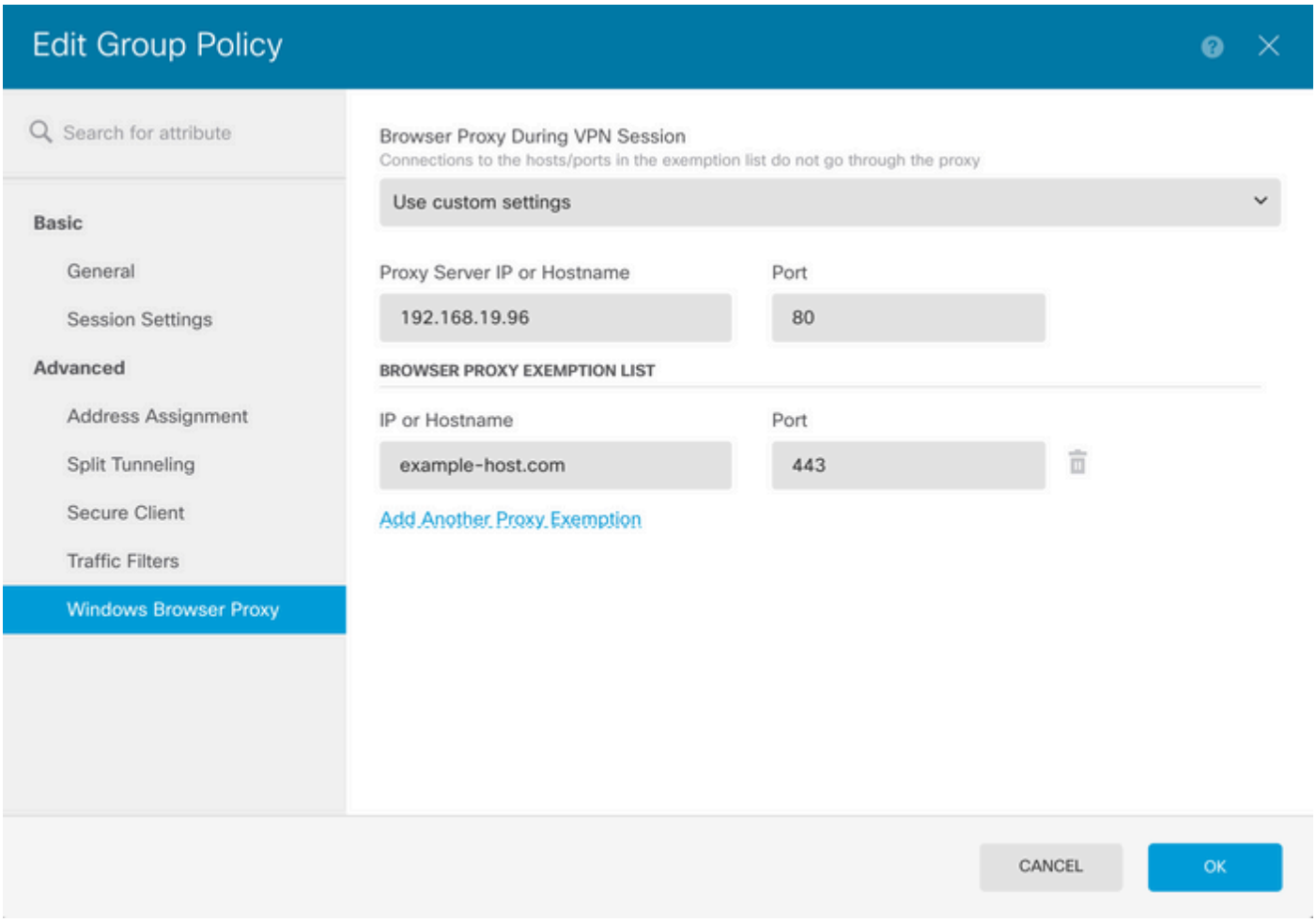
Geben Sie im Feld Proxy Server IP or Hostname (Proxy-Server-IP oder Hostname) die Informationen zum Proxy-Server ein, und geben Sie im Feld Port (Port) den Port ein, über den Sie den Server erreichen möchten.



Wenn es eine Adresse oder einen Hostnamen gibt, die bzw. den Sie nicht über den Proxy erreichen möchten, klicken Sie auf die Schaltfläche Add Proxy Exemption (Proxyausnahme hinzufügen), und fügen Sie sie hier hinzu.



Hinweis: Die Angabe eines Ports in der Browser Proxy Exemption List ist optional.



Klicken Sie auf OK, und stellen Sie die Konfiguration bereit.

Überprüfung

Um zu überprüfen, ob die Konfiguration erfolgreich angewendet wurde, können Sie die CLI des FTD verwenden.

<#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
```

Fehlerbehebung

Sie können ein DART-Paket erfassen und überprüfen, ob das VPN-Profil angewendet wurde:

<#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

****

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.