Configura proxy del browser di Windows su client protetto

Sommario

Introduzione

In questo documento viene descritto come configurare i proxy del browser di Windows per Cisco Secure Client connesso a FTD Gestito da FDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall Device Manager versione 7.3
- Cisco Firepower Threat Defense Virtual Appliance versione 7.3
- Cisco Secure Client versione 5.0.02075

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il termine "proxy" si riferisce a un servizio che si trova tra l'utente e la risorsa che si desidera raggiungere. I proxy del browser Web, in particolare, sono server che trasmettono il traffico Web, quindi, quando si naviga in un sito Web, il client sicuro richiede al server proxy di richiedere il sito invece di farlo direttamente.

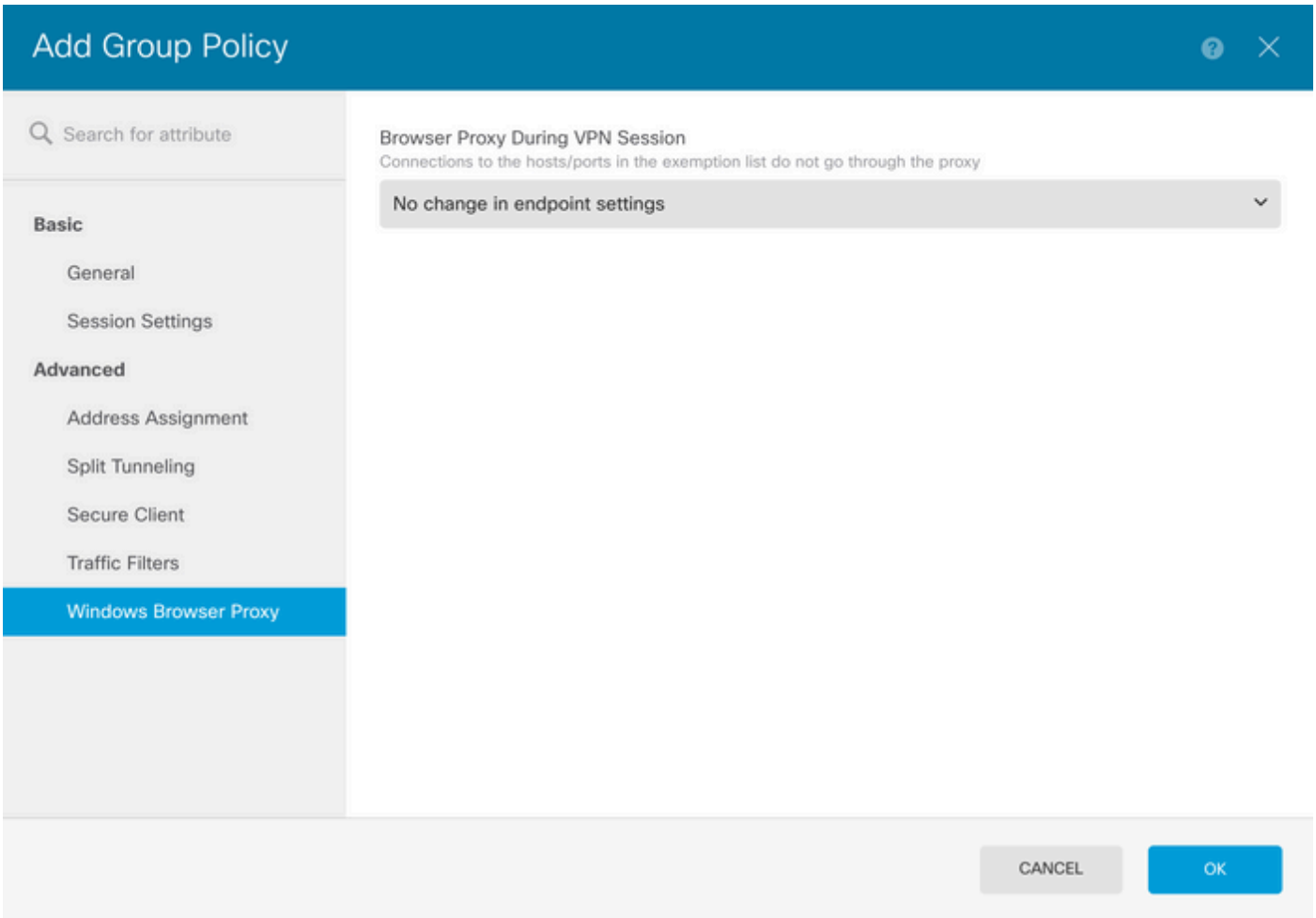
I proxy possono essere utilizzati per raggiungere diversi obiettivi, ad esempio il filtro dei contenuti, la gestione del traffico e il tunneling del traffico.

Configurazione

Configurazioni

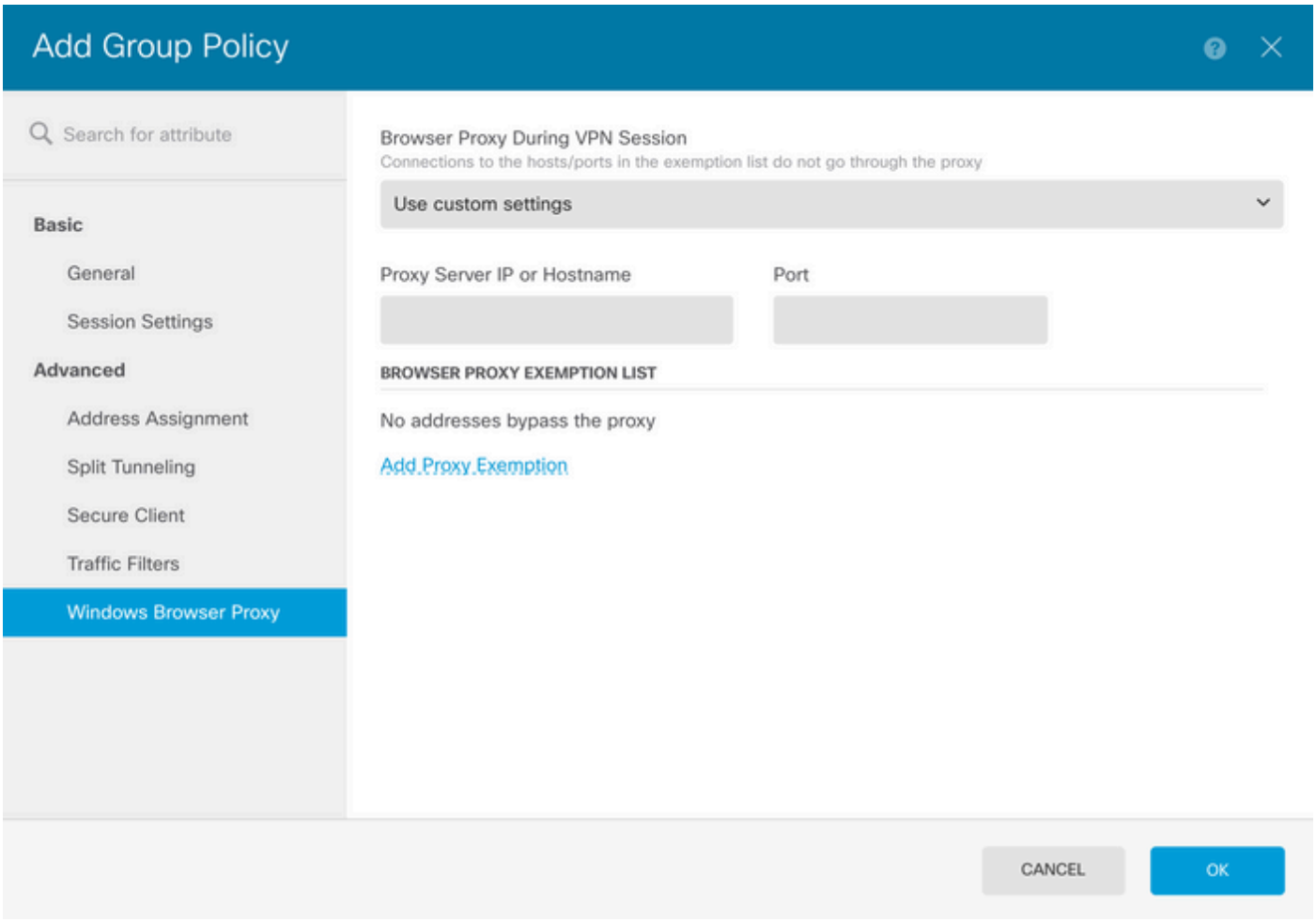
In questo documento si presume che l'utente disponga già di una configurazione VPN ad accesso remoto funzionante.

In FDM, passare a VPN ad accesso remoto > Criteri di gruppo, fare clic sul pulsante Modifica in Criteri di gruppo in cui si desidera configurare il proxy del browser e passare alla sezione Proxy browser Windows.

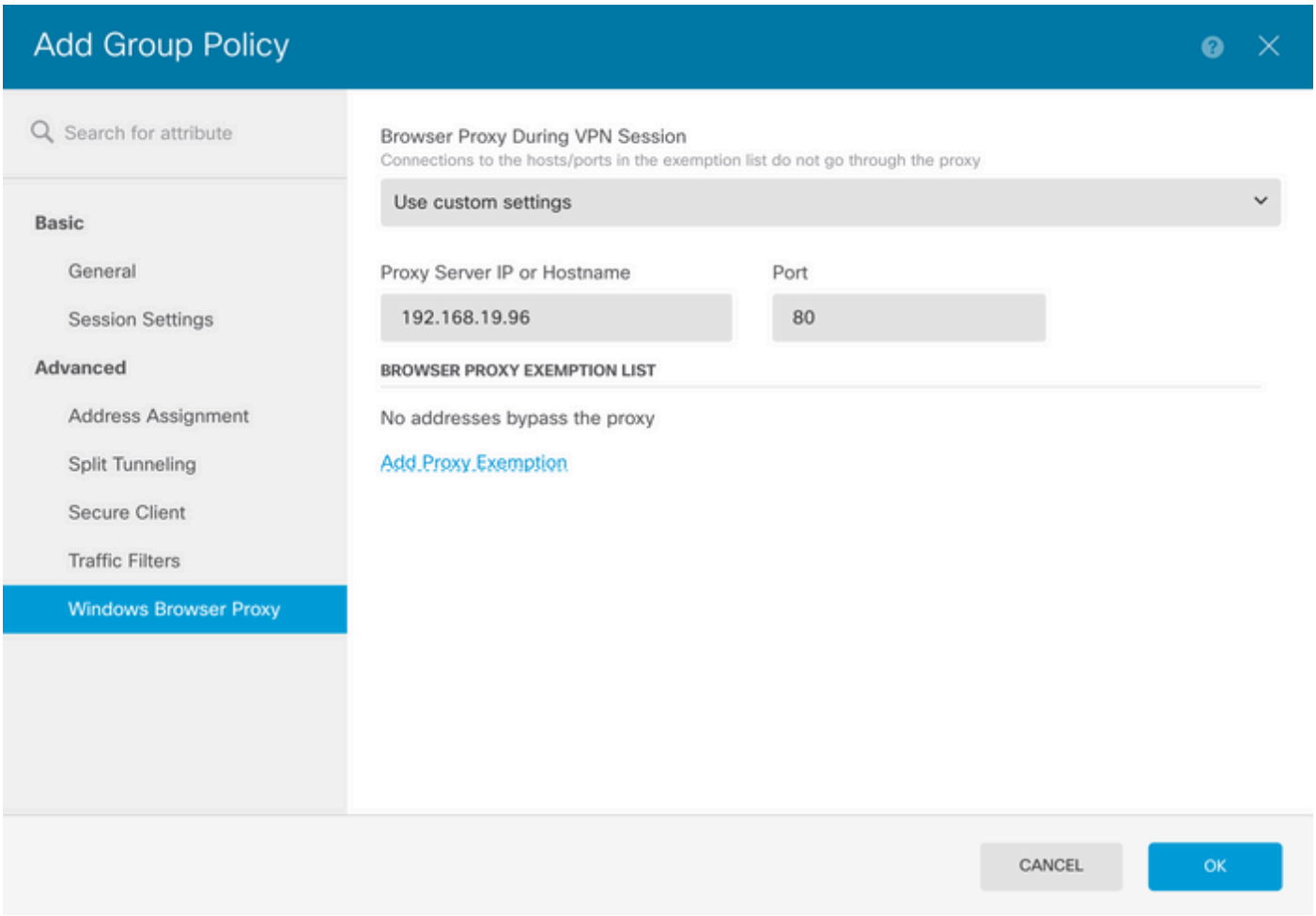


Dall'elenco a discesa Browser Proxy During VPN Session, selezionare Use custom settings (Usa

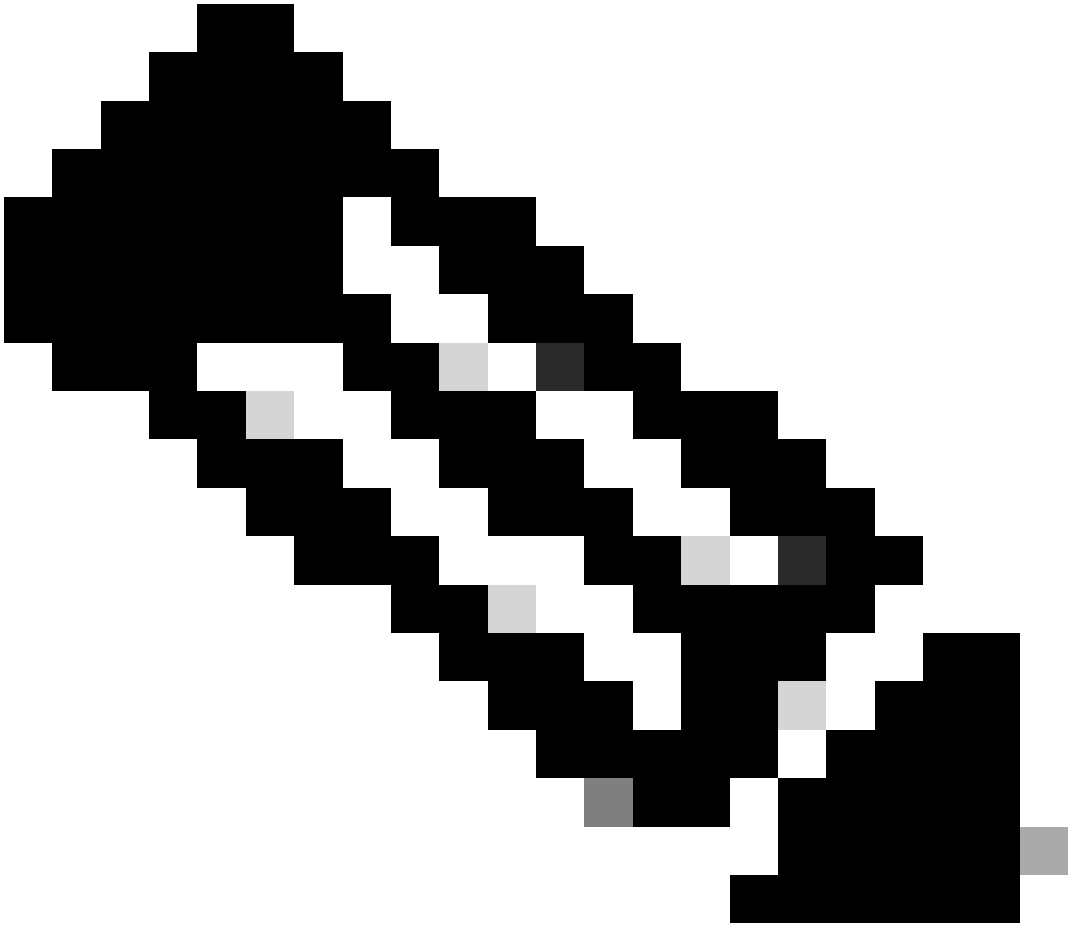
impostazioni personalizzate).



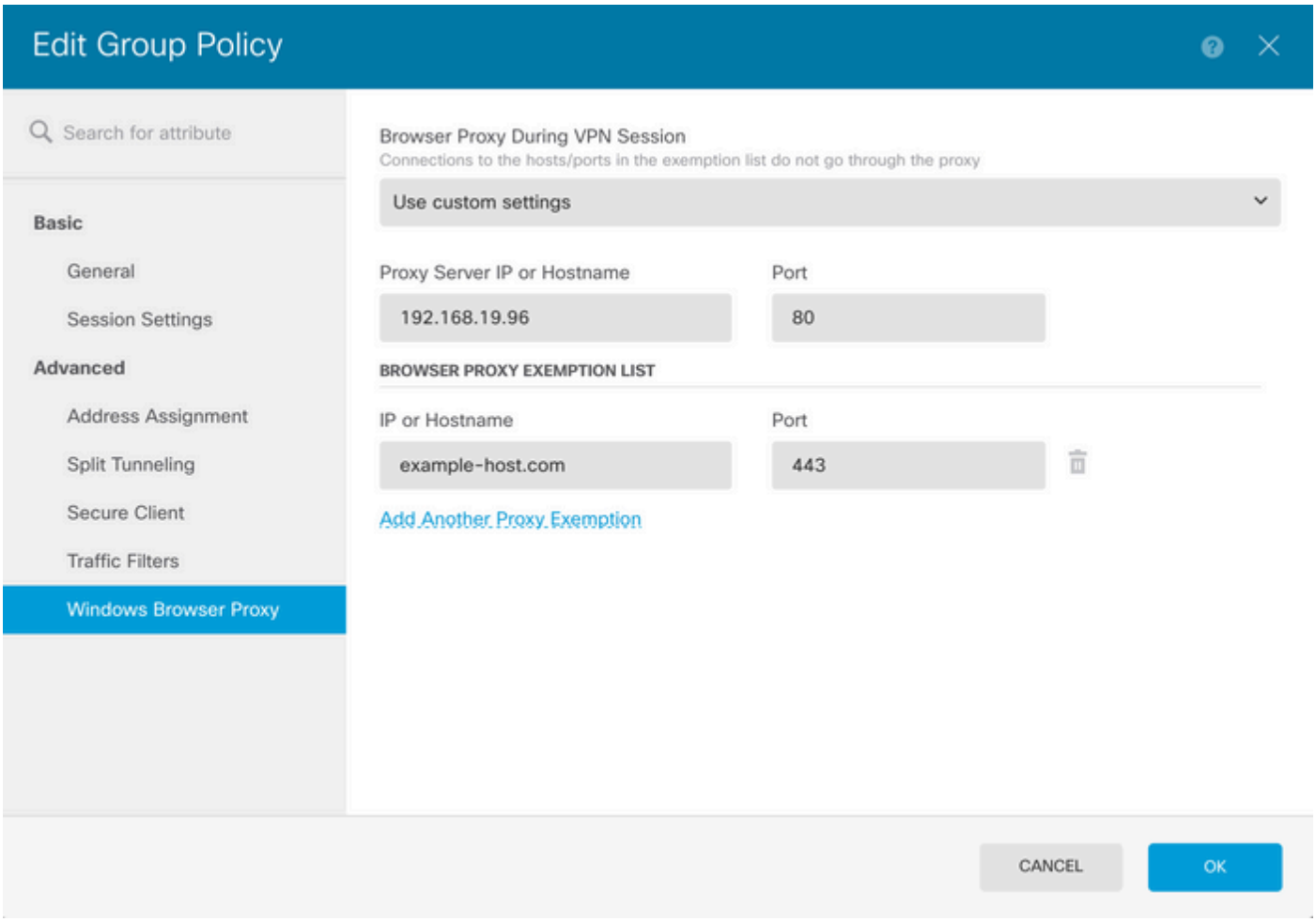
Nella casella Proxy Server IP or Hostname, immettere le informazioni sul server proxy e nella casella Port, immettere la porta per raggiungere il server.



Se non si desidera raggiungere un indirizzo o un nome host tramite il proxy, fare clic sul pulsante Add Proxy Exemption (Aggiungi esenzione proxy) e aggiungerlo qui.



Nota: la specifica di una porta nell'elenco di esenzione proxy browser è facoltativa.



Fare clic su Ok e distribuire la configurazione.

Verifica

Per verificare se la configurazione è stata applicata correttamente, è possibile usare la CLI dell'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
```

Risoluzione dei problemi

È possibile raccogliere un bundle DART e verificare che il profilo VPN sia stato applicato:

<#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

****

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).