# 보안 클라이언트에서 Windows 브라우저 프록시 구성

## 목차



## 소개

이 문서에서는 FDM에서 관리하는 FTD에 연결된 Cisco Secure Client용 Windows 브라우저 프록시를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco FDM(Secure Firewall Device Manager)
- Cisco FTD(Firepower 위협 방어)
- CSC(Cisco Secure Client)

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

# 배경 정보

"프록시"란 사용자와 도달하려는 리소스 사이에 위치한 서비스를 의미합니다. 웹 브라우저 프록시는 특히 웹 트래픽을 전송하는 서버입니다. 따라서 웹 사이트로 이동할 때 Secure Client가 프록시 서버에 사이트를 직접 요청하는 대신 요청하도록 메시지를 표시합니다.

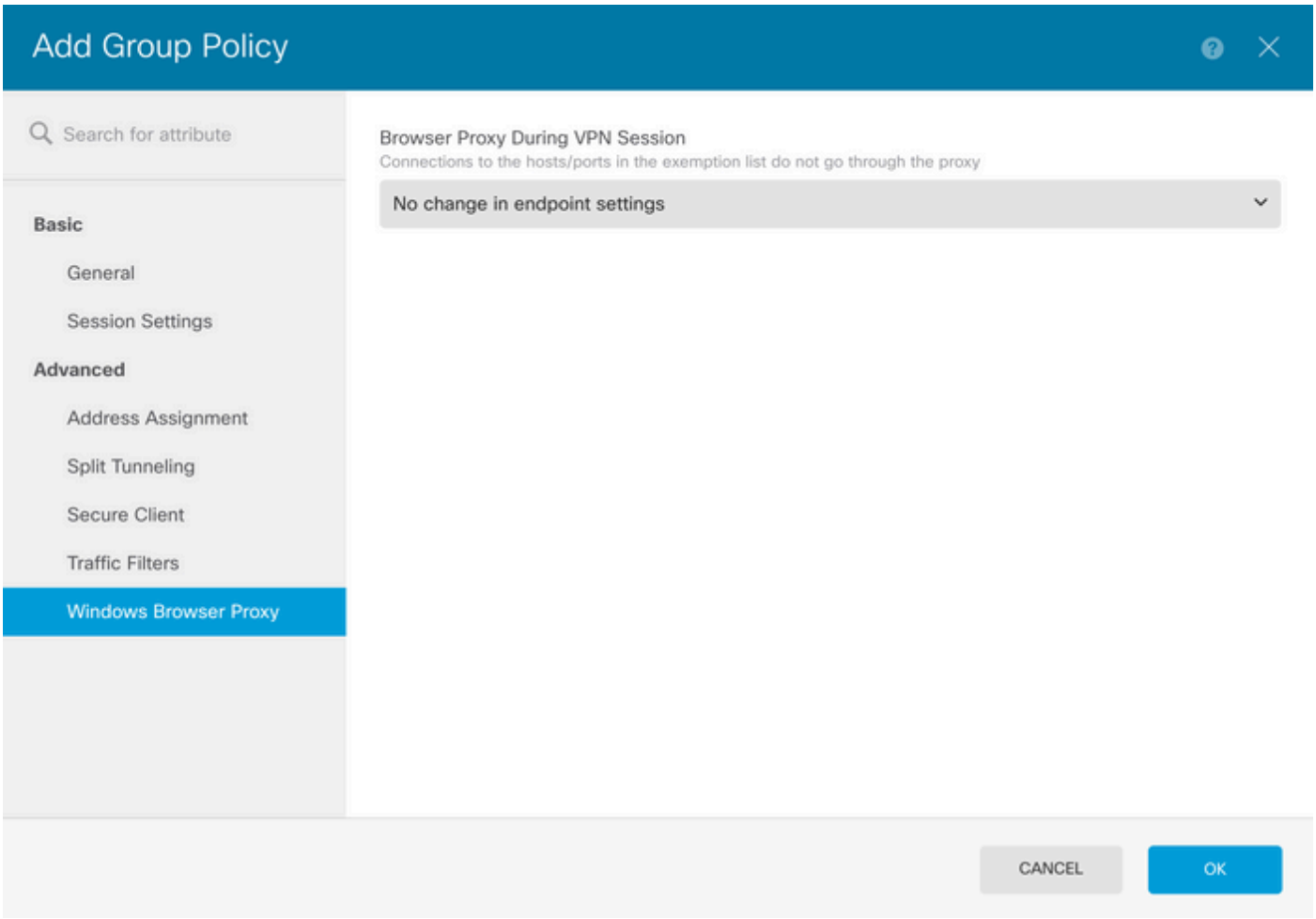
프록시를 사용하여 콘텐츠 필터링, 트래픽 처리, 트래픽 터널링과 같은 다양한 목적을 달성할 수 있습니다.

# 구성

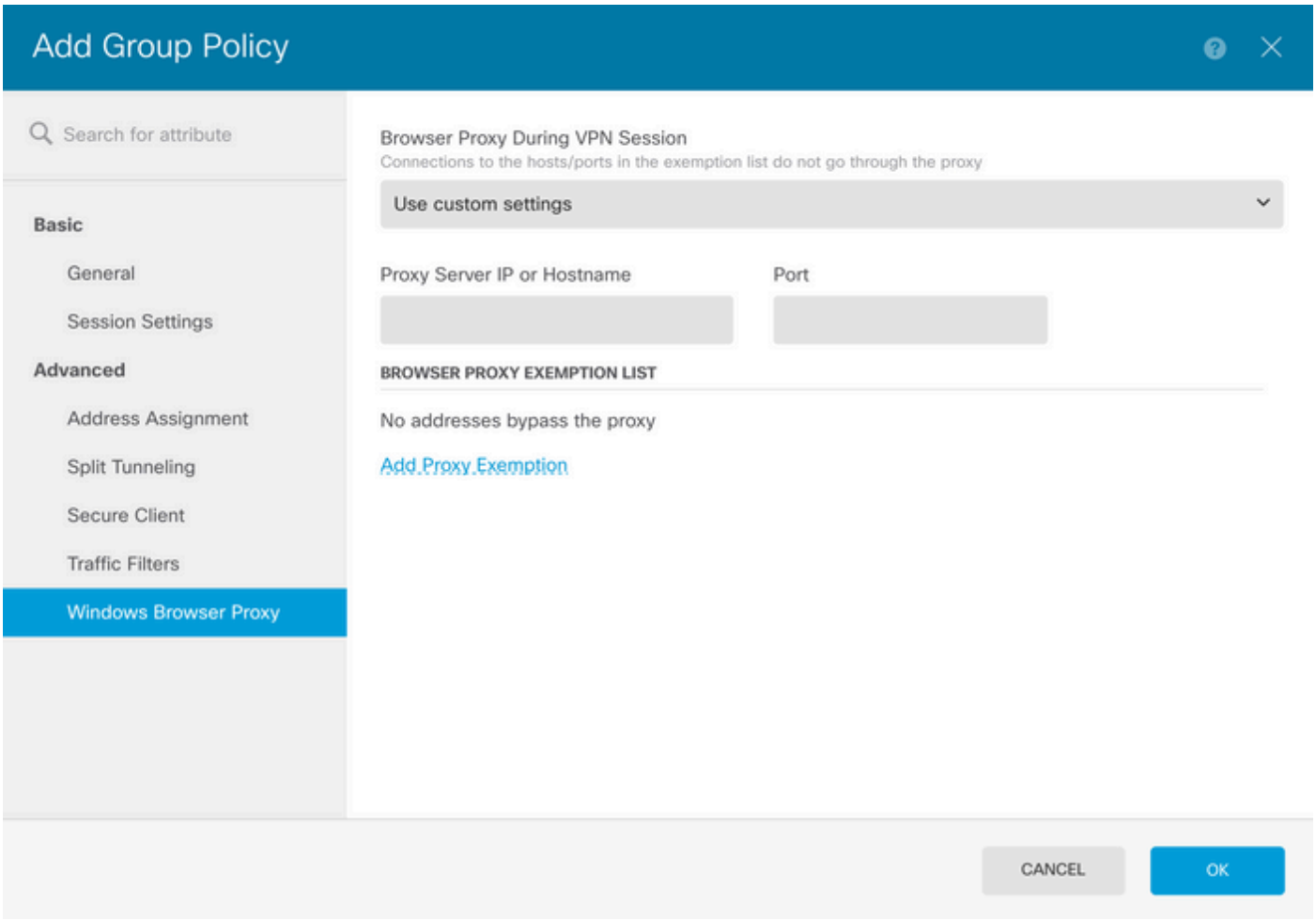
## 설정

이 문서에서는 이미 작동하는 원격 액세스 VPN 컨피그레이션이 있는 것으로 가정합니다.

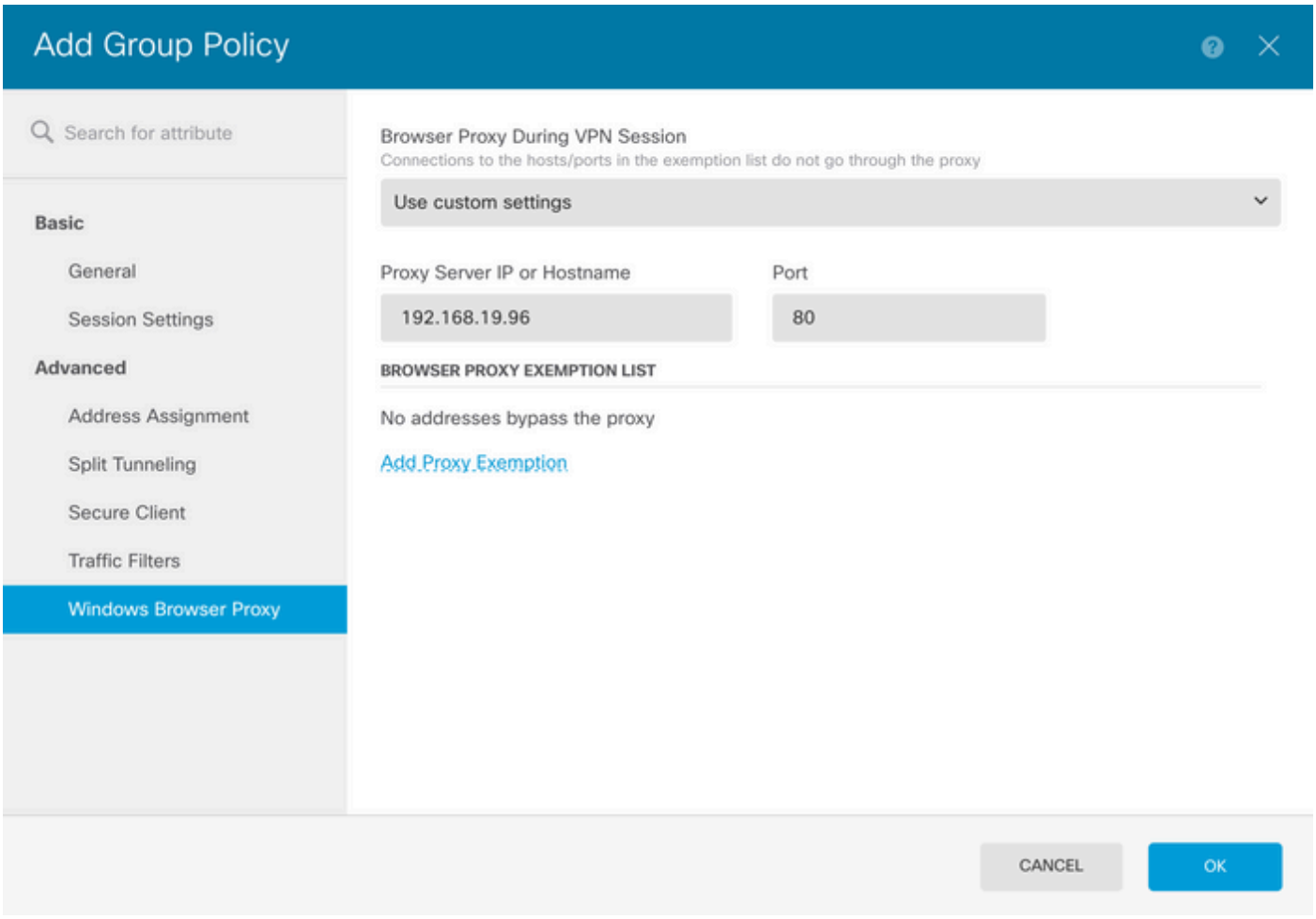
FDM에서 Remote Access VPN(원격 액세스 VPN) > Group Policies(그룹 정책)로 이동하고, 브라우저 프록시를 구성하려는 그룹 정책에서 Edit(편집) 버튼을 클릭하고, Windows Browser Proxy(Windows 브라우저 프록시) 섹션으로 이동합니다.



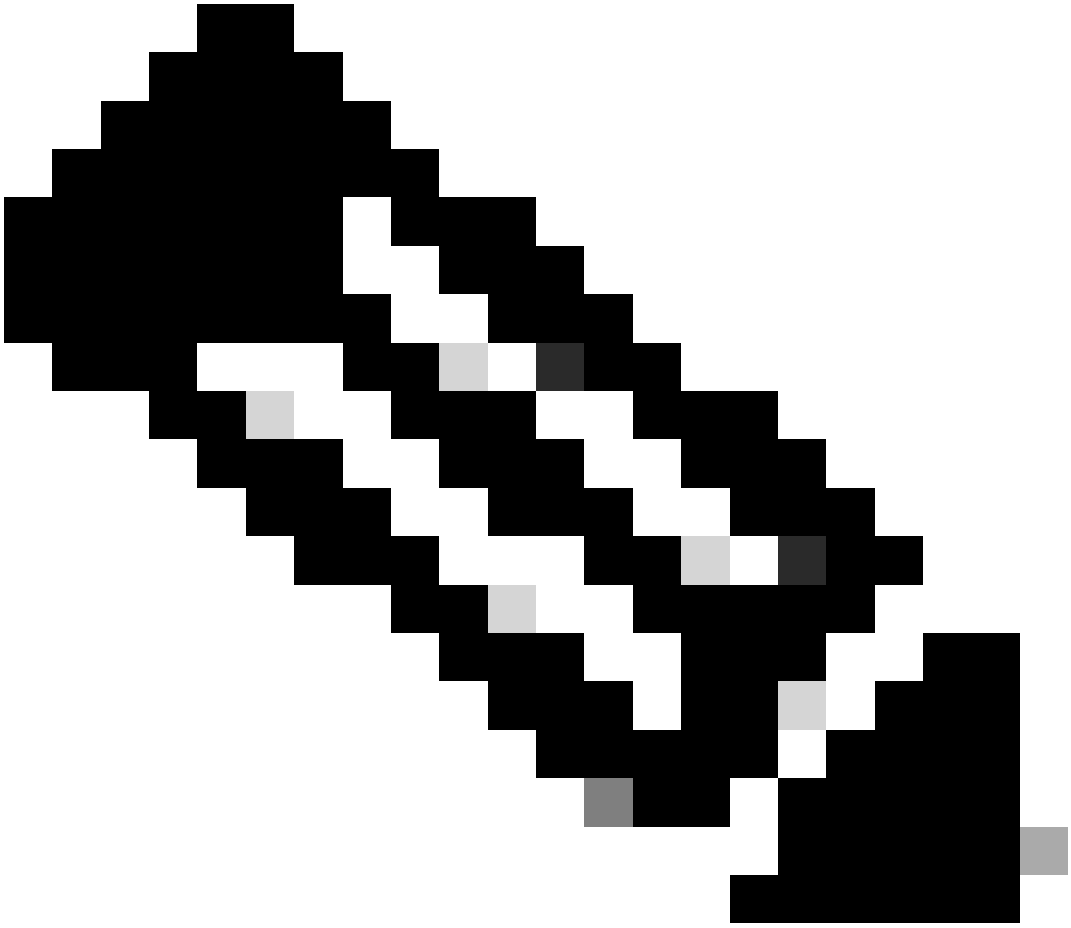

Browser Proxy During VPN Session 드롭다운에서 Use custom settings(사용자 지정 설정 사용)를 선택합니다.



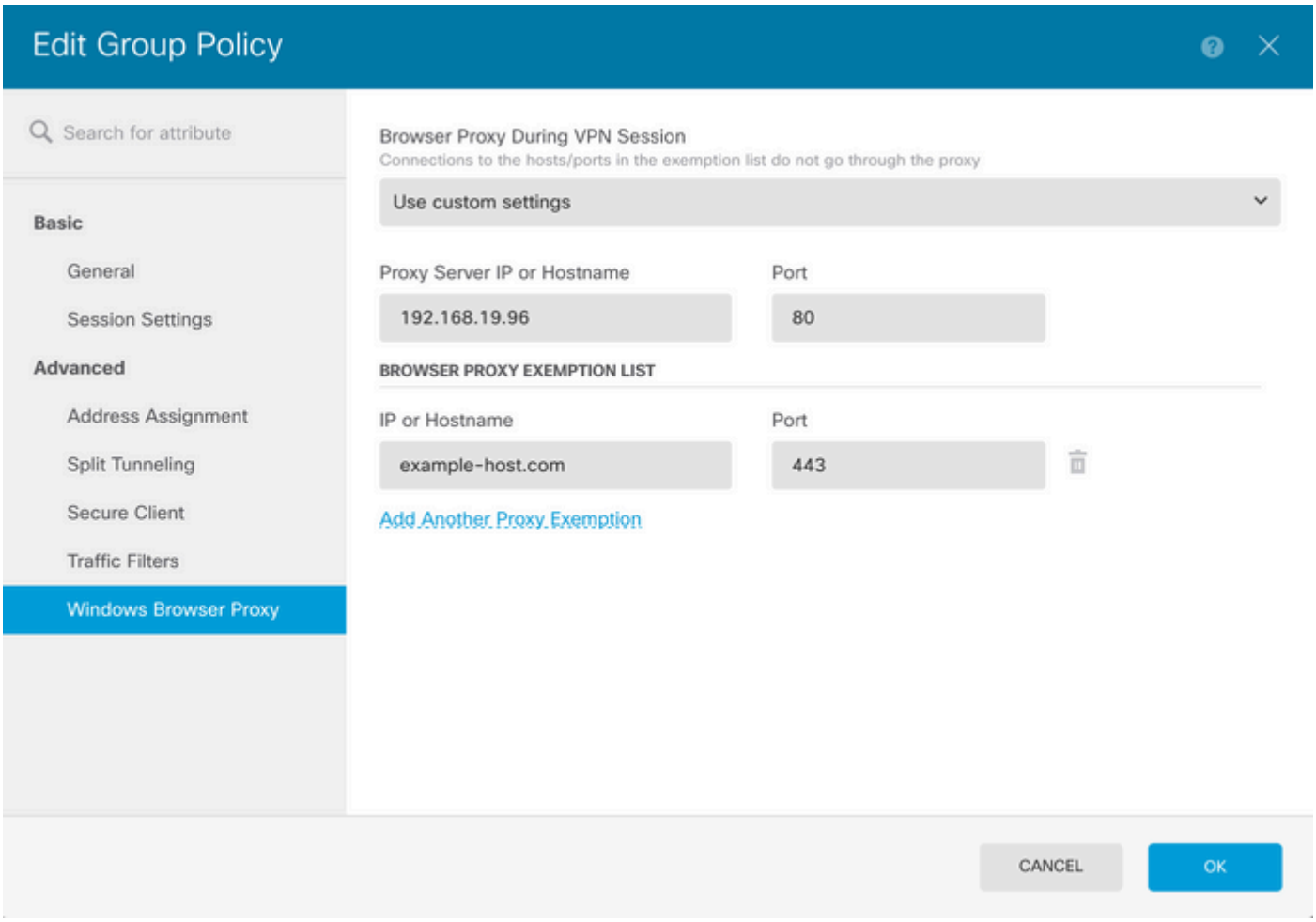

Proxy Server IP or Hostname(프록시 서버 IP 또는 호스트 이름) 상자에 프록시 서버 정보를 입력하고 Port(포트) 상자에 서버에 연결할 포트를 입력합니다.




프록시를 통해 연결하지 않으려는 주소 또는 호스트 이름이 있는 경우 Add Proxy Exemption(프록시 예외 추가) 버튼을 클릭하고 여기에 추가합니다.



참고: 브라우저 프록시 예외 목록에서 포트를 지정하는 것은 선택 사항입니다.




OK(확인)를 클릭하고 컨피그레이션을 구축합니다.

# 다음을 확인합니다.

컨피그레이션이 성공적으로 적용되었는지 확인하려면 FTD의 CLI를 사용할 수 있습니다.

<#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
```

# 문제 해결

DART 번들을 수집하고 VPN 프로파일이 적용되었는지 확인할 수 있습니다.

<#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

**********

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.