FMC에서 관리하는 FTD에 AnyConnect 동적 스플릿 터널 구성

목차

소개

이 문서에서는 FMC(Firepower Management Center)에서 관리하는 FTD(Firepower Threat Defense)에서 AnyConnect 동적 스플릿 터널을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco AnyConnect
- FMC에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- FMC 버전 7.0
- FTD 버전 7.0

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

FMC에서 관리하는 FTD의 AnyConnect 동적 스플릿 터널 컨피그레이션은 FMC 버전 7.0 이상에서 완전히 사용할 수 있습니다. 이전 버전을 실행하는 경우 FMC를 사용하는 Firepower Threat Defense용 Advanced AnyConnect VPN Deployments의 지침에 따라 FlexConfig를 통해 구성해야 합니다.

동적 스플릿 터널 컨피그레이션을 사용하면 DNS 도메인 이름을 기반으로 스플릿 터널 컨피그레이션을 세부적으로 조정할 수 있습니다. FQDN(Full-Qualified Domain Name)과 연결된 IP 주소가 변경될 수 있으므로 DNS 이름을 기반으로 하는 스플릿 터널 컨피그레이션을 통해 원격 액세스 VPN(Virtual Private Network) 터널에 어떤 트래픽이 포함되는지 또는 포함되지 않는지 좀 더 동적으로 정의할 수 있습니다. 제외된 도메인 이름에 대해 반환된 주소가 VPN에 포함된 주소 풀 내에 있는 경우 해당 주소는 제외됩니다. 제외된 도메인은 차단되지 않습니다. 대신 이러한 도메인에 대한 트래픽은 VPN 터널 외부에 유지됩니다.

동적 스플릿 터널도 구성할 수 있습니다 IP 주소를 기반으로 제외되는 터널을 포함할 도메인을 정의합니다.

제한 사항

현재 이러한 기능은 여전히 지원되지 않습니다.

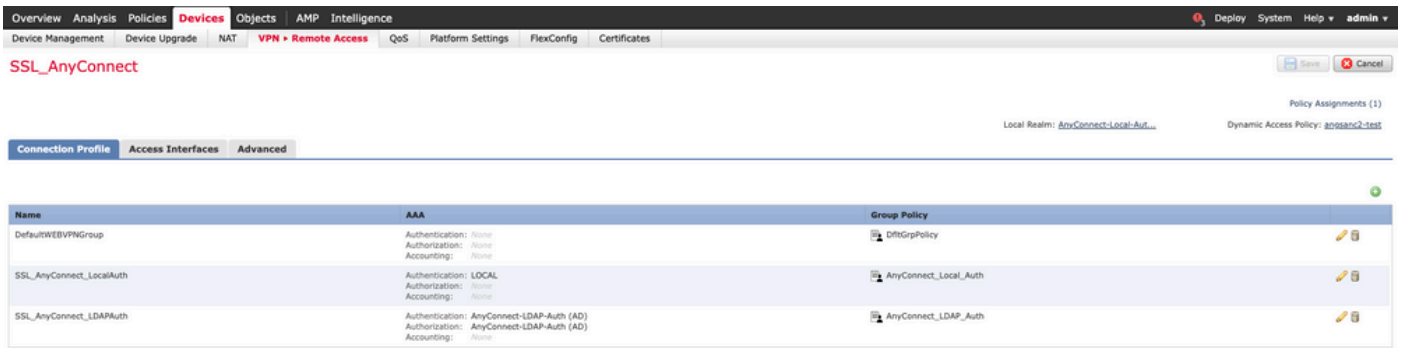
- 동적 스플릿 터널은 iOS(Apple) 디바이스에서 지원되지 않습니다. Cisco 버그 ID CSCvr을 참조하십시오54798
- 동적 스플릿 터널은 Anyconnect Linux 클라이언트에서 지원되지 않습니다. Cisco 버그 IDCSCvt를 참조하십시오64988

구성

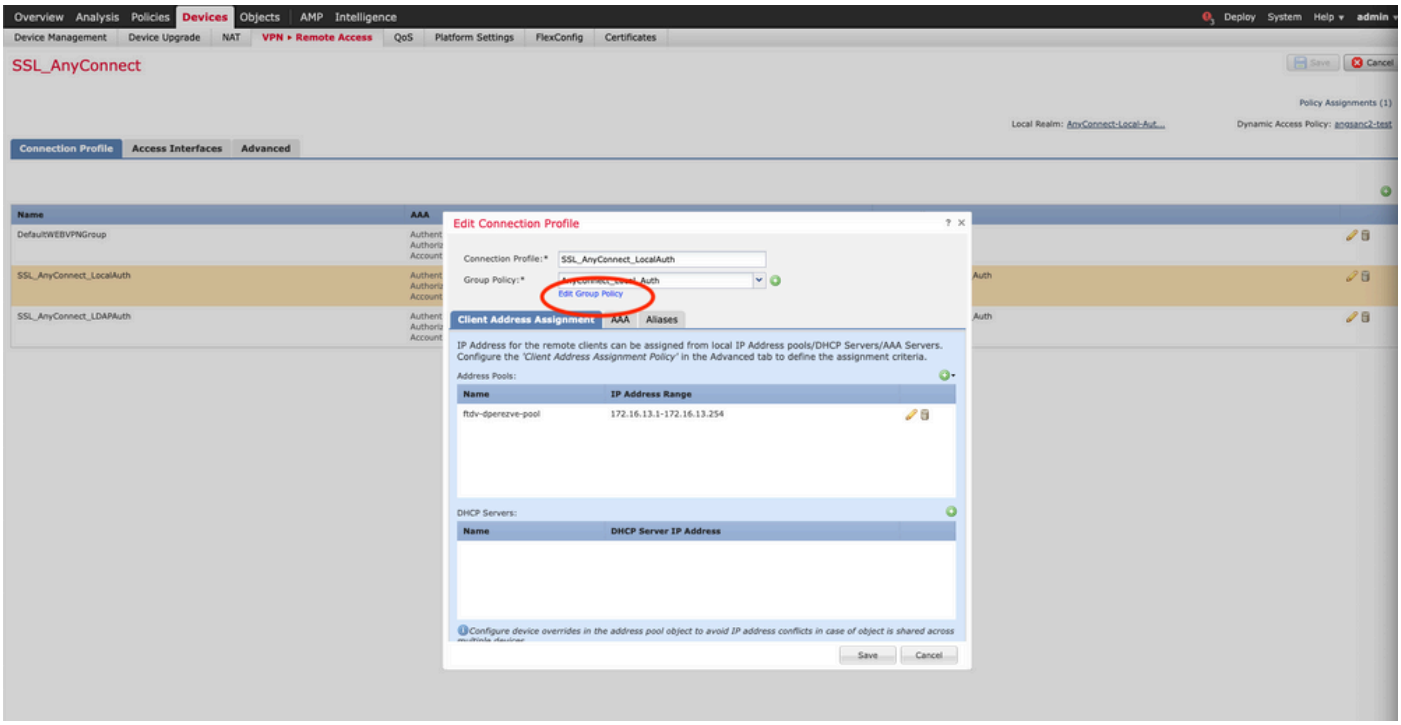
이 섹션에서는 FMC에서 관리하는 FTD에서 AnyConnect 동적 스플릿 터널을 구성하는 방법에 대해 설명합니다.

1단계. 동적 스플릿 터널을 사용하도록 그룹 정책 편집

1. FMC에서 Devices(**디바이스**) > **VPN** > **Remote Access(원격 액세스)**로 이동한 다음 컨피그레이션을 적용할 **연결** 프로필을 선택합니다.

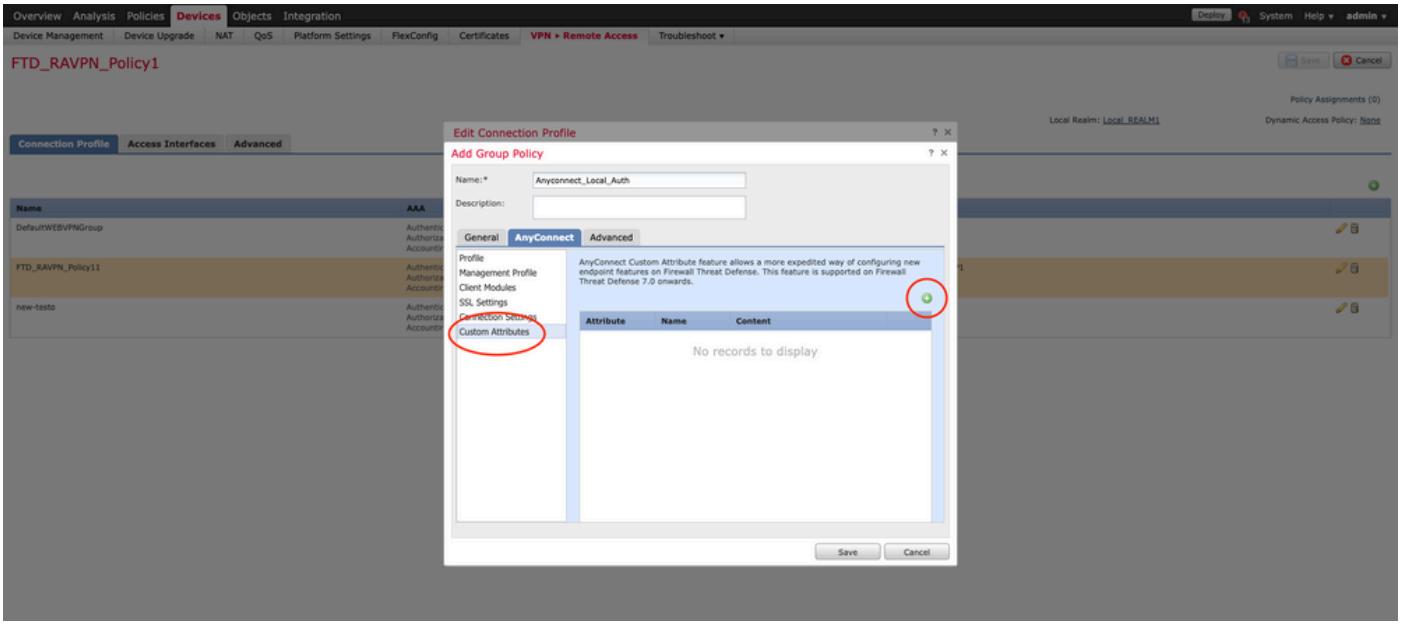


2. 이미 생성된 **그룹 정책** 중 하나를 수정하려면 그룹 정책 편집을 선택합니다.

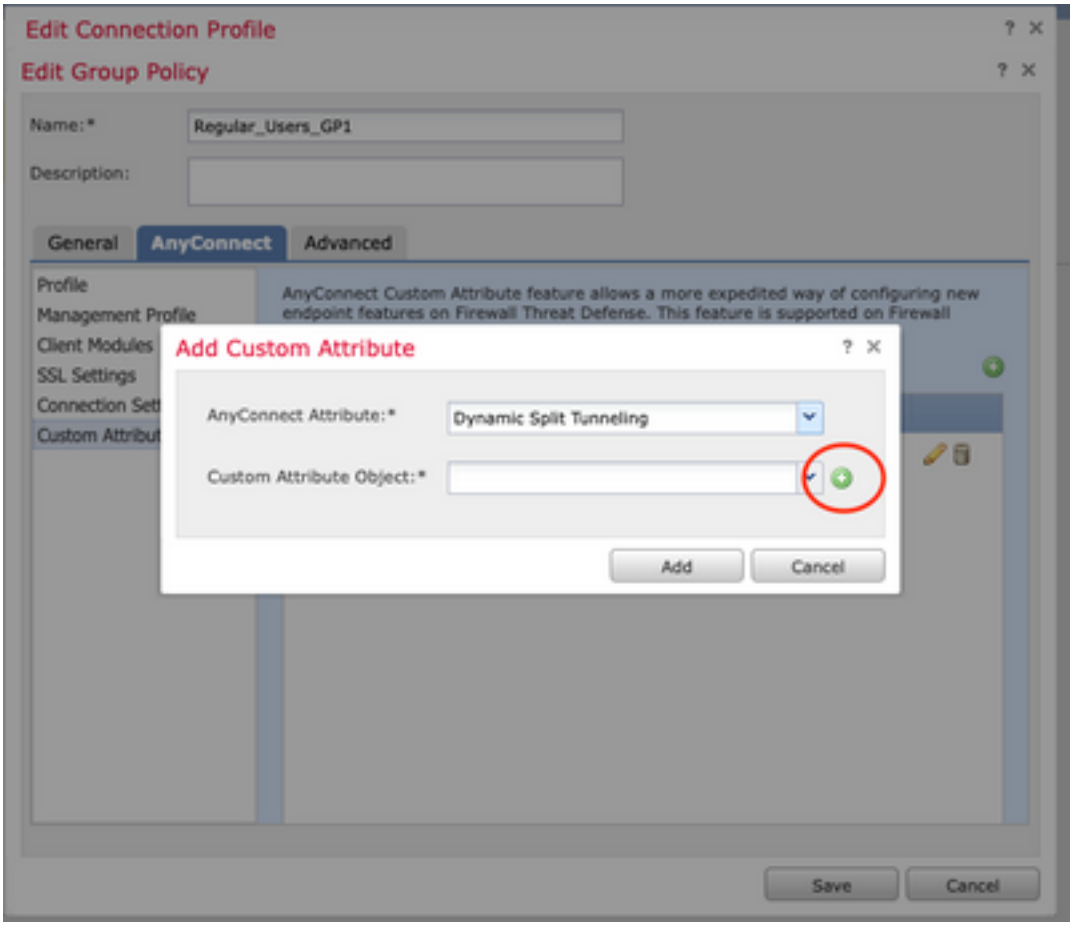


2단계. AnyConnect 사용자 지정 특성 구성

1. Group Policy(그룹 정책) 컨피그레이션에서 Anyconnect **> Custom Attributes(사용자 지정 특성**)로 이동하고 **Add(+) 버튼을** 클릭합니다.

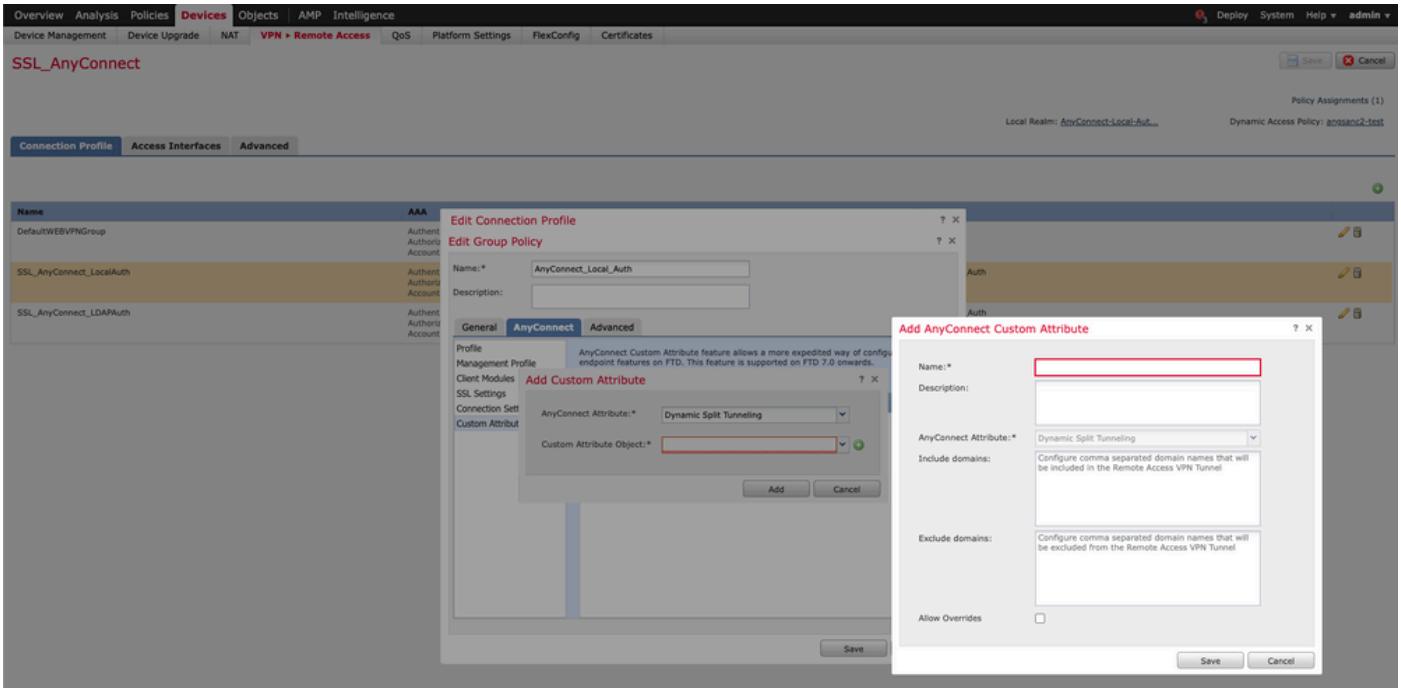


2. **동적 스플릿 터널링 AnyConnect 특성**을 선택하고 **추가(+) 버튼**을 클릭하여 새 사용자 지정 특성 개체를 만듭니다.

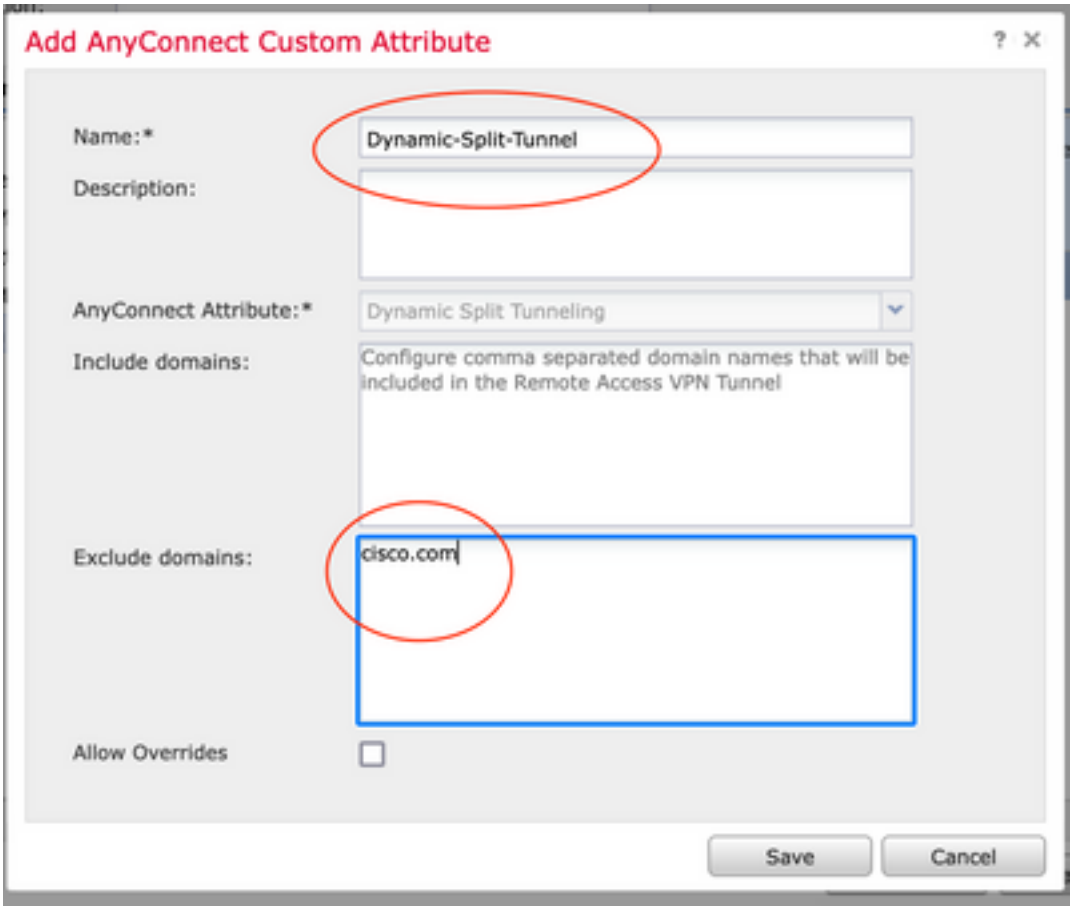


3. AnyConnect 사용자 **지정** 특성의 **이름**을 입력하고 동적으로 포함하거나 제외할 도메인을 구성합니다.

> **참고**: Include domains(도메인 포함) 또는 **Exclude domains(도메인** 제외)**만** 구성할 수 있습니다.

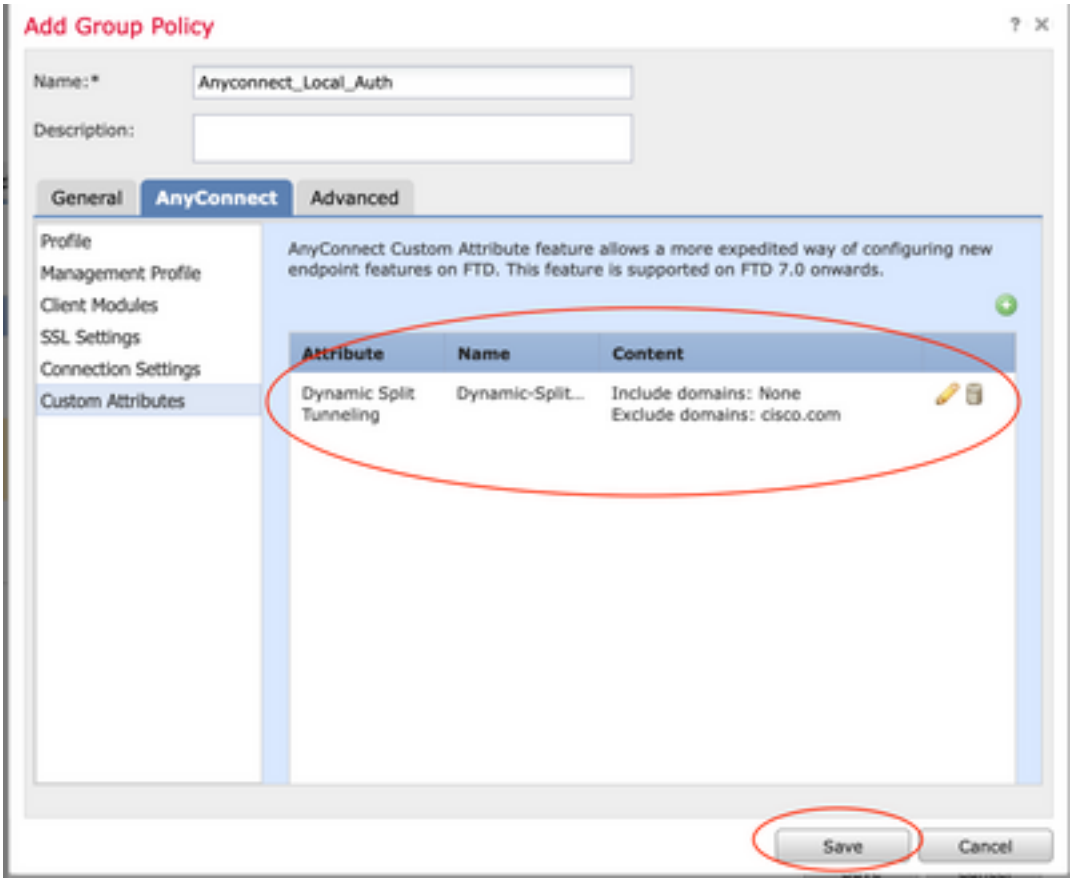


이 예에서는 **cisco.com**을 제외할 도메인으로 구성하고 이미지에 표시된 대로 사용자 지정 특성 **Dynamic-Split-Tunnel**을 명명했습니다.



3단계. 컨피그레이션 확인, 저장 및 구축

구성된 사용자 지정 특성이 올바른지 확인하고 컨피그레이션을 저장하고 변경 사항을 문제의 FTD에 배포합니다.



다음을 확인합니다.

CLI(Command Line Interface)를 통해 FTD에서 다음 명령을 실행하여 동적 스플릿 터널 컨피그레이션을 확인할 수 있습니다.

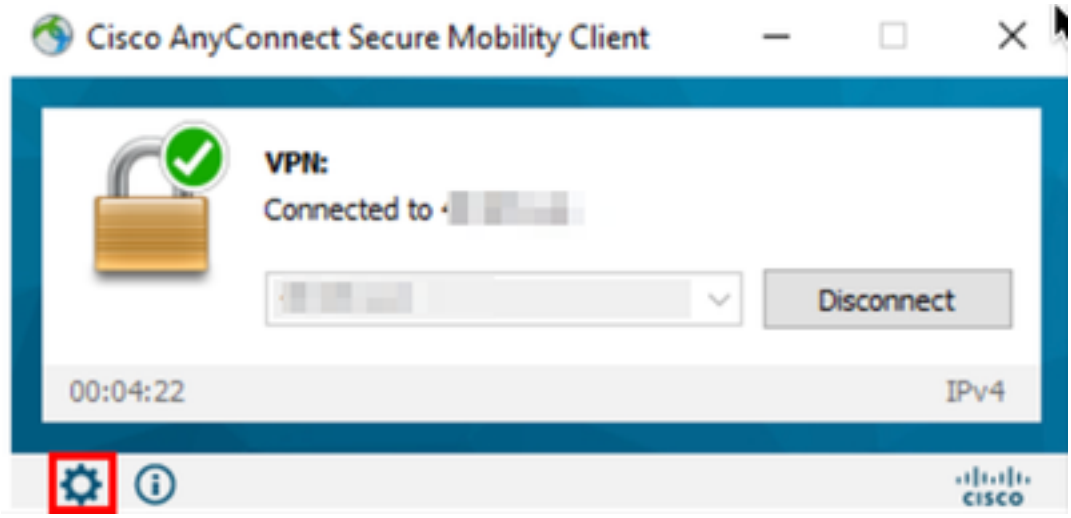
- show running-config webvpn
- show running-config anyconnect-custom-data
- show running-config group-policy **<그룹 정책의 이름>**

이 예에서 컨피그레이션은 다음과 같습니다.

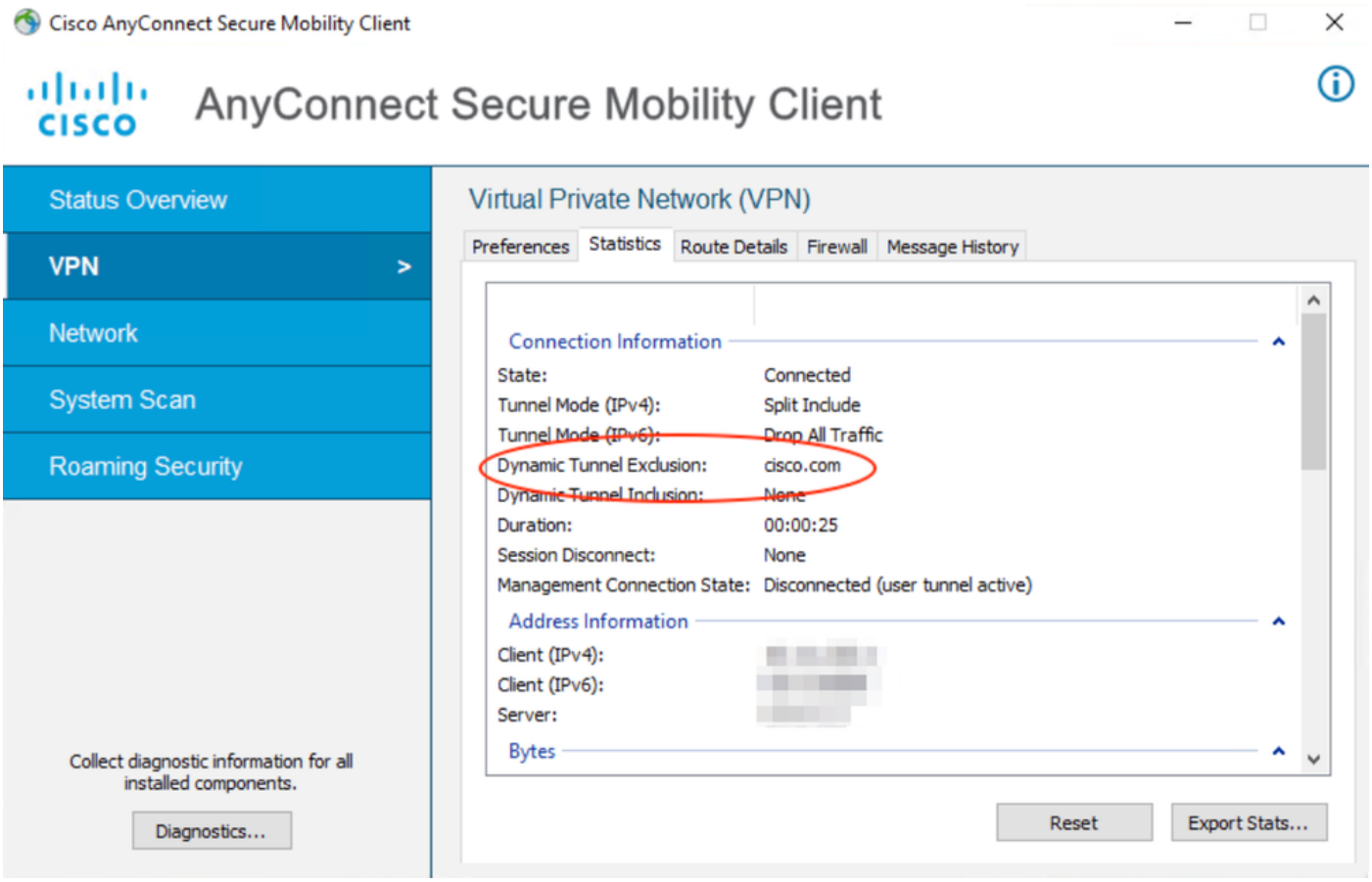
```
ftd# show run group-policy Anyconnect_Local_Auth
group-policy Anyconnect_Local_Auth attributes
vpn-idle-timeout 30
vpn-simultaneous-logins 3
vpn-session-timeout none
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
ipv6-split-tunnel-policy-tunnelall
split-tunnel-network-list value AC_networks
Default-domain none
split-dns none
address-pools value AC_pool
anyconnect-custom dynamic-split-exclude-domains value cisco.com
anyconnect-custom dynamic-split-include-domains none

ftd# show run webvpn
webvpn
enable outside
anyconnect-custom-attr dynamic-split-exclude-domains
anyconnect-custom-attr dynamic-split-include-domains
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
content-security-policy
anyconnect image disk0:/csm/anyconnect-win-4.1005111-webdeploy-k9.pkg regex "Windows"
anyconnect profiles xmltest disk0:/csm/xmltest.xml
anyconnect enable
tunnel-group-list enable
cache
disable
certificate-group-map cert_map_test 10 cert_auth
error-recovery disable
```

클라이언트에서 구성된 동적 터널 제외를 확인하려면 다음을 수행합니다.

1. AnyConnect 소프트웨어를 실행하고 그림과 같이 톱니바퀴 모양 아이콘을 클릭합니다.



2. **VPN > Statistics(통계)**로 이동하여 **Dynamic Split Exclusion/Inclusion(동적 분할 제외/포함) 아래에 표시된 도메인을 확인합니다**.



문제 해결

AnyConnect Diagnostics and Reporting Tool(DART)을 사용하여 AnyConnect 설치 및 연결 문제를 해결하는 데 유용한 데이터를 수집할 수 있습니다.

DART는 Cisco TAC(Technical Assistance Center) 분석을 위해 로그, 상태 및 진단 정보를 취합하며 클라이언트 시스템에서 실행하는 데 관리자 권한이 필요하지 않습니다.

문제

와일드카드가 AnyConnect 사용자 지정 특성(예: ***.cisco.com)**에 구성된 경우 AnyConnect 세션의 연결이 끊어집니다.

솔루션

cisco.com 도메인 값을 사용하여 와일드카드 대체를 허용할 수 있습니다. 이 변경을 통해 www,**cisco.com** 및 **tools.cisco.com과** 같은 도메인을 포함하거나 제외할 수 있습니다.

관련 정보

- 추가 지원이 필요한 경우 TAC(Technical Assistance Center)에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco 전 세계 지원 문의처.
- 또한 Cisco VPN Community를 방문하여 여기.

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.