FMC에서 관리하는 FTD의 RAVPN에 대한 사용자 지정 포트 구성

목차

소개

이 문서에서는 FMC에서 관리하는 FTD(Firepower Threat Defense)에서 SSL 및 IKEv2 AnyConnect에 대한 사용자 지정 포트를 구성하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- RAVPN(Remote Access VPN)에 대한 기본적인 이해
- FMC(Firepower 관리 센터) 경험

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD - 7.6
- Cisco FMC - 7.6
- Windows 10

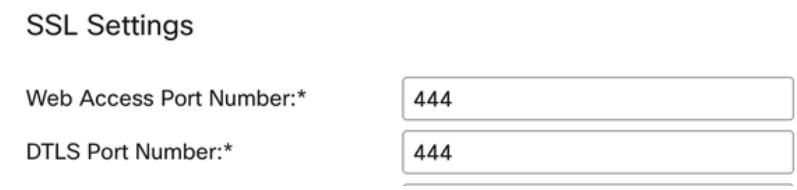
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설정

AnyConnect에 대한 SSL/DTLS 포트 변경

1. Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동하여 기존 원격 액세스 정책을 수정합니다.

2. Access Interfaces(액세스 인터페이스) 섹션으로 이동하여 SSL 설정의 Web Access Port Number(웹 액세스 포트 번호) 및 DTLS Port Number(DTLS 포트 번호)를 선택의 포트로 변경합니다.



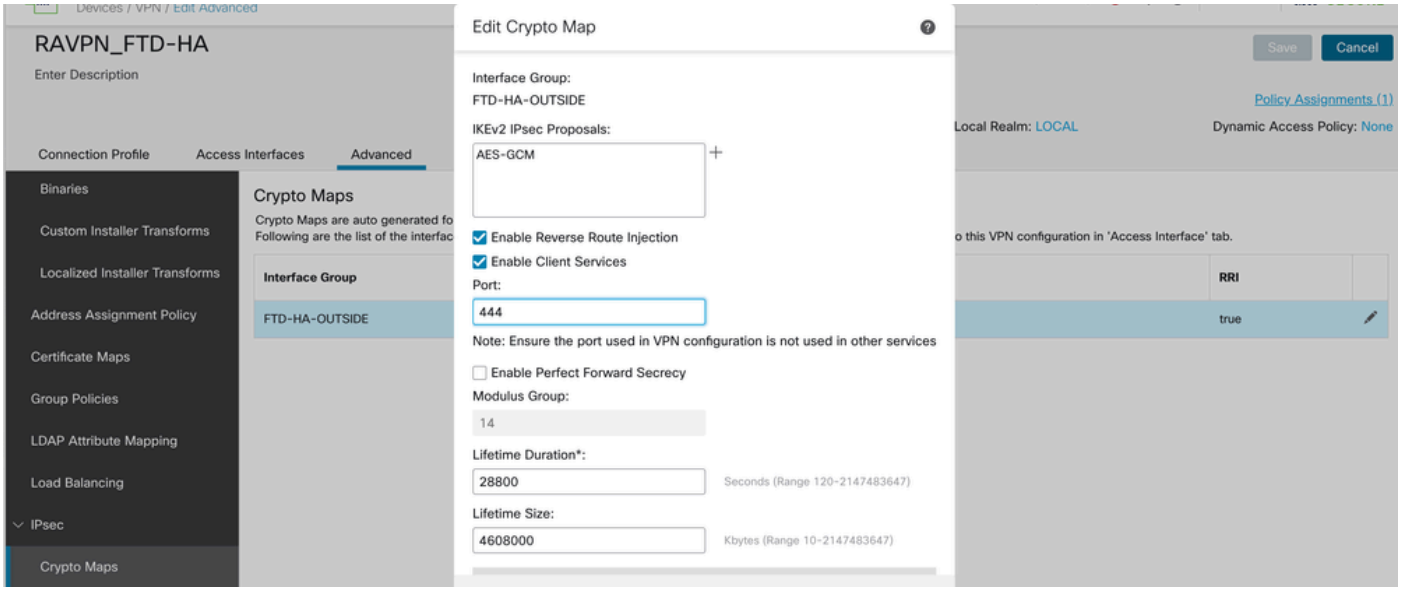
AnyConnect에 대한 SSL 및 DTLS 포트 변경

3. 구성을 저장합니다.

AnyConnect에 대한 IKEv2 포트 변경

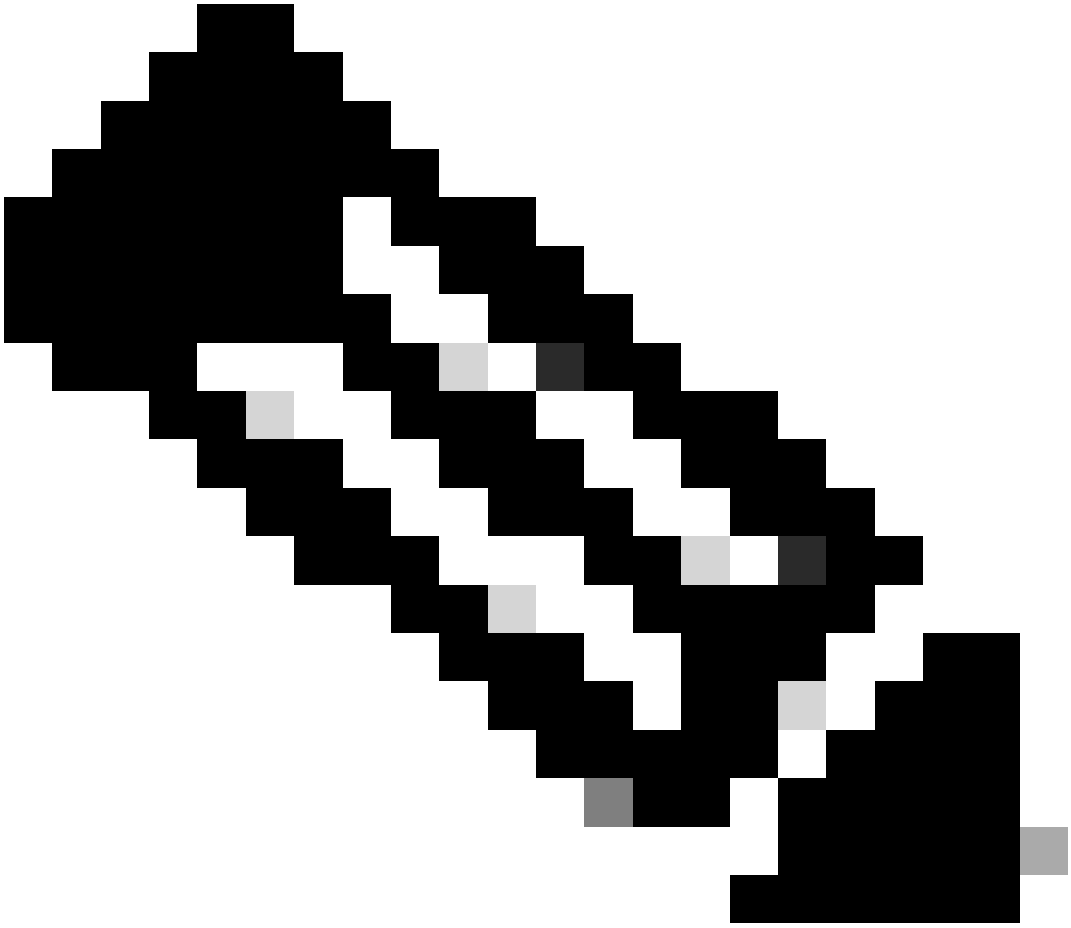
1. Devices(디바이스) > VPN > Remote Access(원격 액세스)로 이동하여 기존 원격 액세스 정책을 수정합니다.

2. 고급 섹션으로 이동한 다음 IPsec > 암호화 맵으로 이동합니다. 정책을 수정하고 포트를 원하는 포트로 변경합니다.



AnyConnect에 대한 IKEv2 포트 변경

3. 구성을 저장하고 구축합니다.



참고: AnyConnect 클라이언트 프로파일과 함께 사용자 지정 포트를 사용하는 경우 서버 목록의 호스트 주소 필드에 연결용 X.X.X.X:port(192.168.50.5:444)가 있어야 합니다.

다음을 확인합니다.

1. 구축 후, show run webvpn 및 show run crypto ikev2 명령으로 컨피그레이션을 확인할 수 있습니다.

<#root>

>

show run webvpn

webvpn

port 444 <----- Custom Port that has been configured for SSL

```
enable outside
```

dtls port 444 <----- Custom Port that has been configured for DTLS

```
http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
anyconnect image disk0:/csm/cisco-secure-client-win-X.X.X.X-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable
```

<#root>

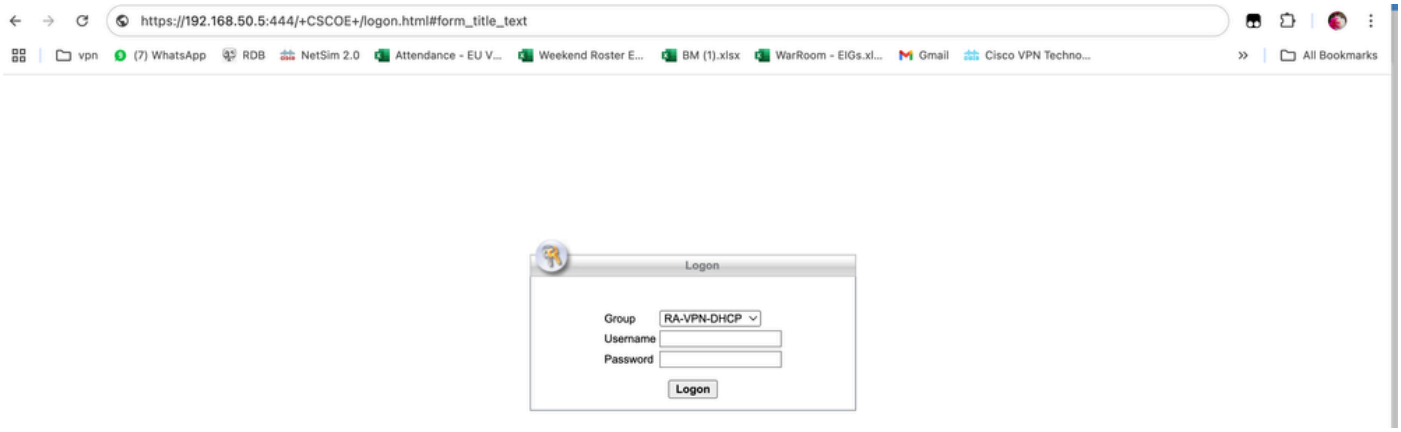
>

show run crypto ikev2

```
crypto ikev2 policy 10
 encryption aes-gcm-256 aes-gcm-192 aes-gcm
 integrity null
 group 21 20 19 16 15 14
 prf sha512 sha384 sha256 sha
 lifetime seconds 86400
```

crypto ikev2 enable outside client-services port 444 <----- Custom Port configured for IKEv2 Client Serv

2. 사용자 지정 포트를 사용하여 브라우저/AnyConnect 애플리케이션에서 원격 액세스에 액세스하여 확인합니다.



사용자 지정 포트로 AnyConnect에 액세스하여 확인

문제 해결

- 원격 액세스 컨피그레이션에 사용된 포트가 다른 서비스에 사용되지 않는지 확인합니다.
- 포트가 ISP 또는 중간 디바이스에 의해 차단되지 않았는지 확인합니다.
- 패킷이 방화벽에 도달하고 응답이 전송되는지 여부를 확인하기 위해 FTD에서 캡처를 수행할 수 있습니다.

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.