보안 방화벽 위협 방어에서 원격 액세스 VPN에 대한 지오로케이션 기반 정책 구성

목차

소개

이 문서에서는 FTD(Secure Firewall Threat Defense)의 특정 위치를 기반으로 RAVPN 연결을 허용하거나 거부하는 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항 및 제한 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(Secure Firewall Management Center)
- 원격 액세스 VPN(RAVPN)
- 기본 지오로케이션 컨피그레이션

지오로케이션 기반 정책의 현재 요구 사항 및 제한 사항은 다음과 같습니다.

- FTD 버전 7.7.0 이상에서만 지원되며 FMC 버전 7.7.0 이상에서 관리됩니다.
- FDM(Secure Firewall Device Manager)에서 관리되는 FTD에서는 지원되지 않습니다.
- 클러스터 모드에서 지원되지 않음

- 지리적 위치 기반 미분류 IP 주소는 지리적 출처별로 분류되지 않습니다. 이를 위해 FMC는 기본 서비스 액세스 정책 작업을 시행합니다.
- 지오로케이션 기반 서비스 액세스 정책은 WebLaunch 페이지에 적용되지 않으므로 제한 없이 Secure Client를 다운로드할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Secure Firewall 버전 7.7.0
- Secure Firewall Management Center 버전 7.7.0

이 기능에 대한 자세한 내용은 Cisco Secure Firewall Management Center 7.7 Device Configuration Guide의 Manage VPN Access of Remote Users Based on Geolocation(Cisco Secure Firewall Management Center 7.7 디바이스 컨피그레이션 가이드)에서 확인할 수 있습니다.

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.

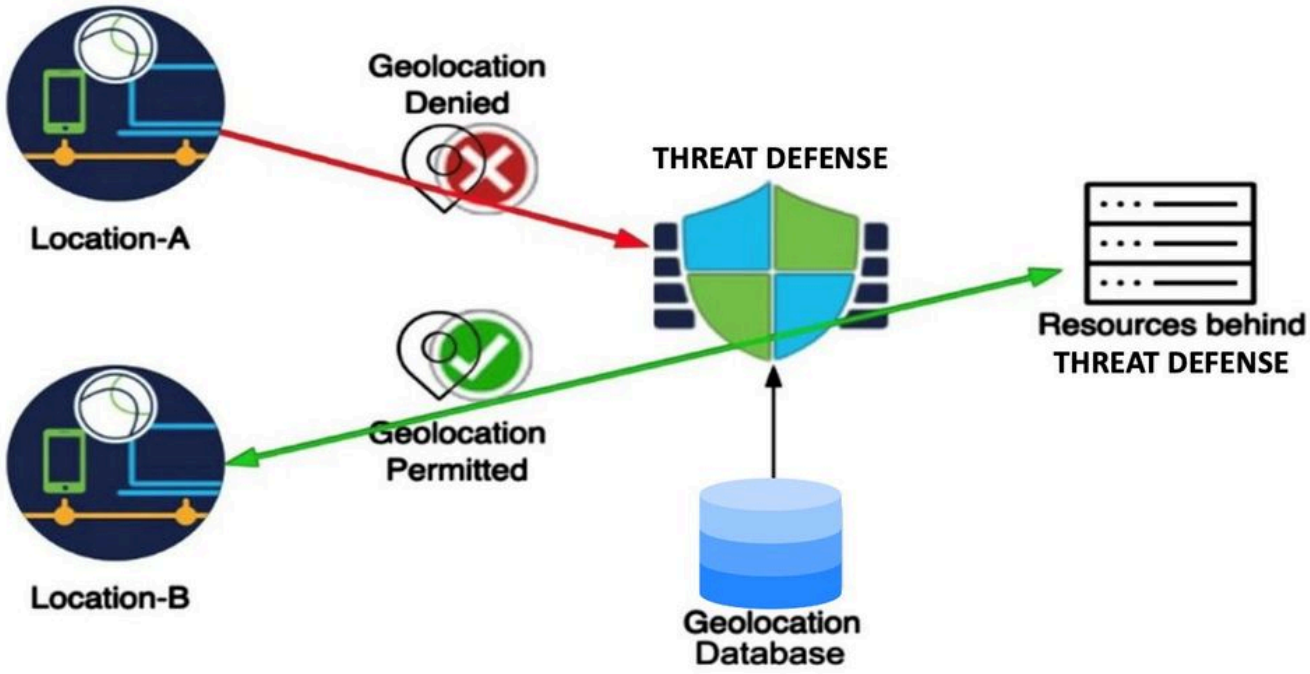
배경 정보

지리적 위치 기반 액세스 정책은 오늘날 네트워크 보안에 상당한 가치를 제공하므로 지리적 출처에 따라 트래픽을 차단할 수 있습니다. 기존에는 조직에서 방화벽을 통과하는 일반 네트워크 트래픽에 대한 트래픽 액세스 정책을 정의할 수 있었습니다. 이제 이 기능을 도입하면 원격 액세스 VPN 세션 요청에 대해 지오로케이션 기반 액세스 제어를 적용할 수 있습니다.

이 기능은 다음과 같은 이점을 제공합니다.

- 지오로케이션 기반 규칙: 고객은 국가나 대륙과 같은 특정 지리적 위치를 기반으로 RAVPN 요청을 허용하거나 거부하는 규칙을 생성할 수 있습니다. 이를 통해 어떤 지리적 위치에서 VPN 세션을 시작할 수 있는지 정밀하게 제어할 수 있습니다.
- 사전 인증 차단: 거부 작업에 대해 이러한 규칙으로 식별된 세션은 인증 전에 차단되며, 이러한 시도는 보안을 위해 올바르게 기록됩니다. 이러한 선제적 조치는 무단 액세스 시도를 차단하는 데 도움이 됩니다.
- 규정 준수 및 보안: 이 기능은 로컬 조직 및 거버넌스 정책을 준수하는 동시에 VPN 서버의 공격 표면을 줄이는 데 도움이 됩니다.

VPN 서버에 인터넷을 통해 액세스할 수 있는 공용 IP 주소가 있는 경우, 지오로케이션 기반 규칙이 도입됨에 따라 조직은 특정 지오로케이션의 사용자 요청을 효과적으로 제한함으로써 무차별 대입 공격에 대한 취약성을 줄일 수 있게 되었습니다.

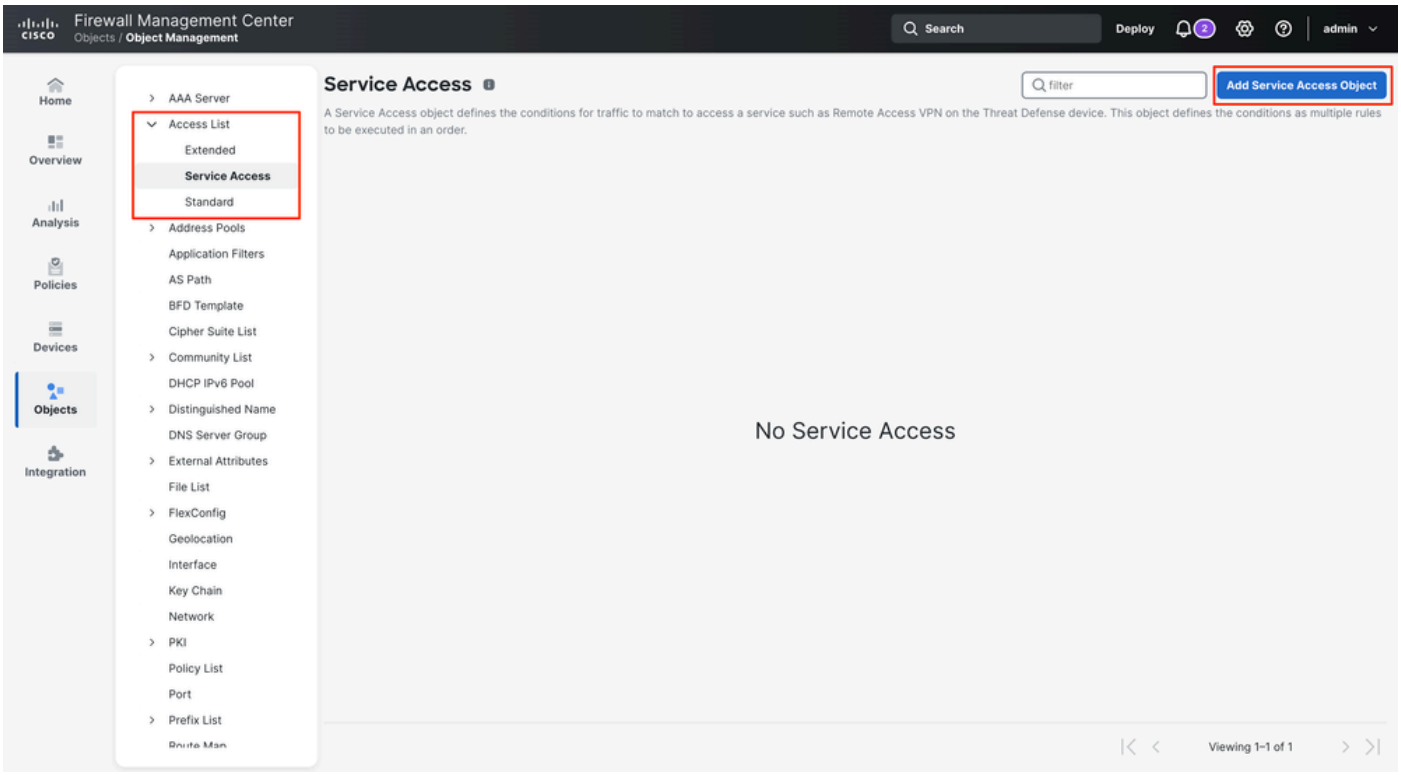


구성

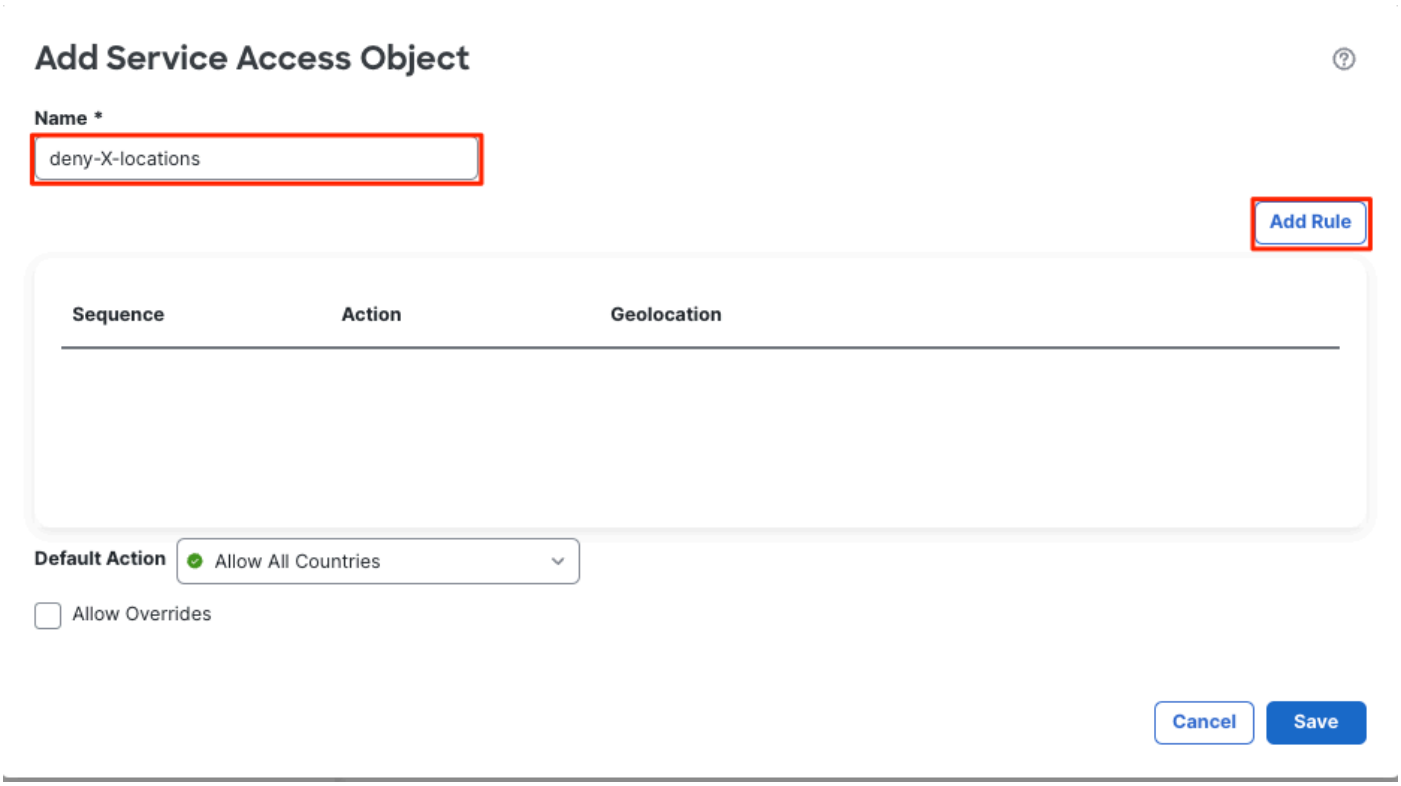
1단계. 서비스 액세스 객체 생성

1. Secure Firewall Management Center에 로그인합니다.

2. Objects(개체) > Object Management(개체 관리) > Access List(액세스 목록) > Service Access(서비스 액세스)로 이동하고 Add Service Access Object(서비스 액세스 개체 추가)를 클릭합니다1.



3. 규칙 이름을 정의한 다음 규칙 추가를 클릭합니다.

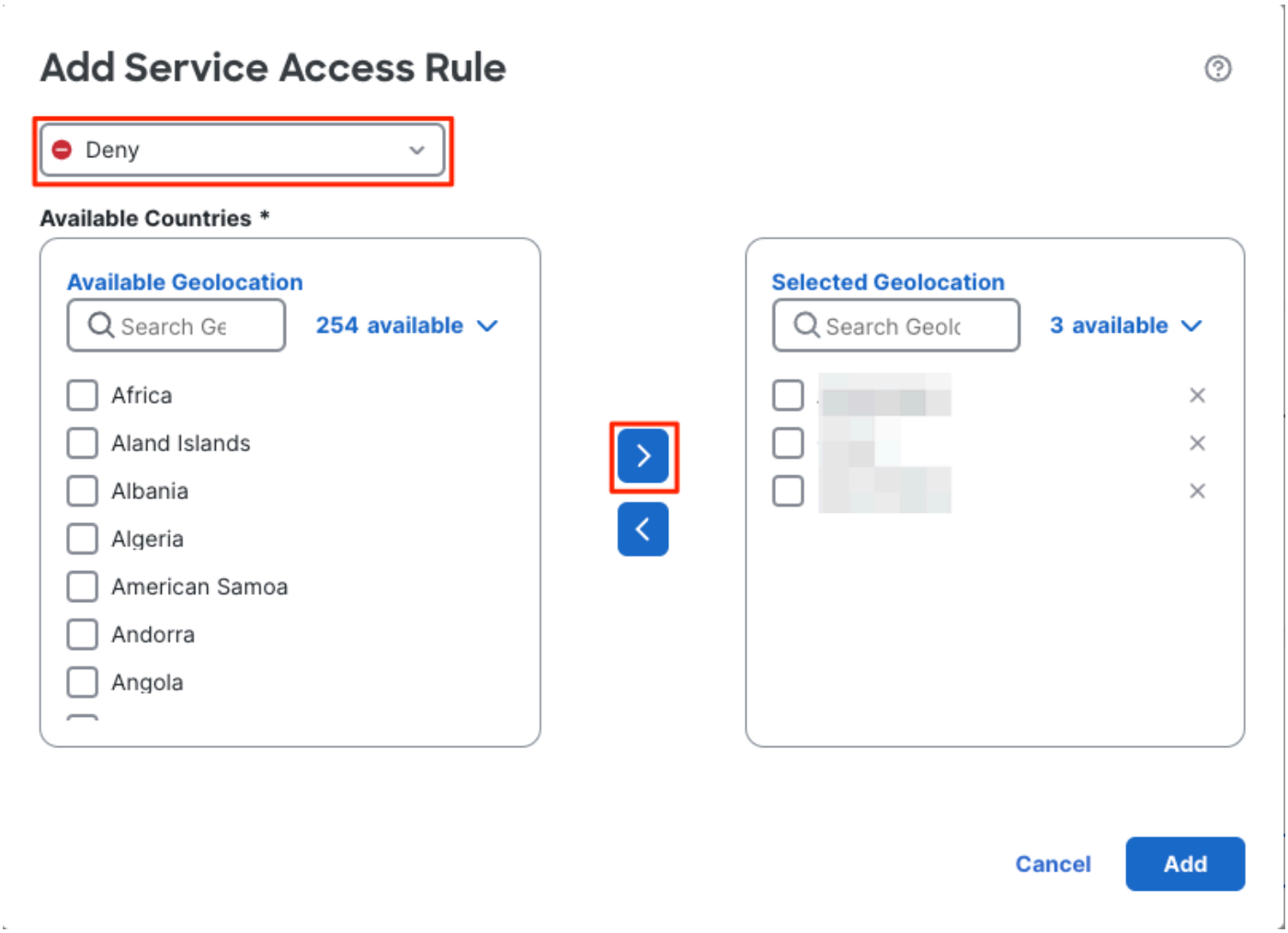


4. 서비스 액세스 규칙을 구성합니다.

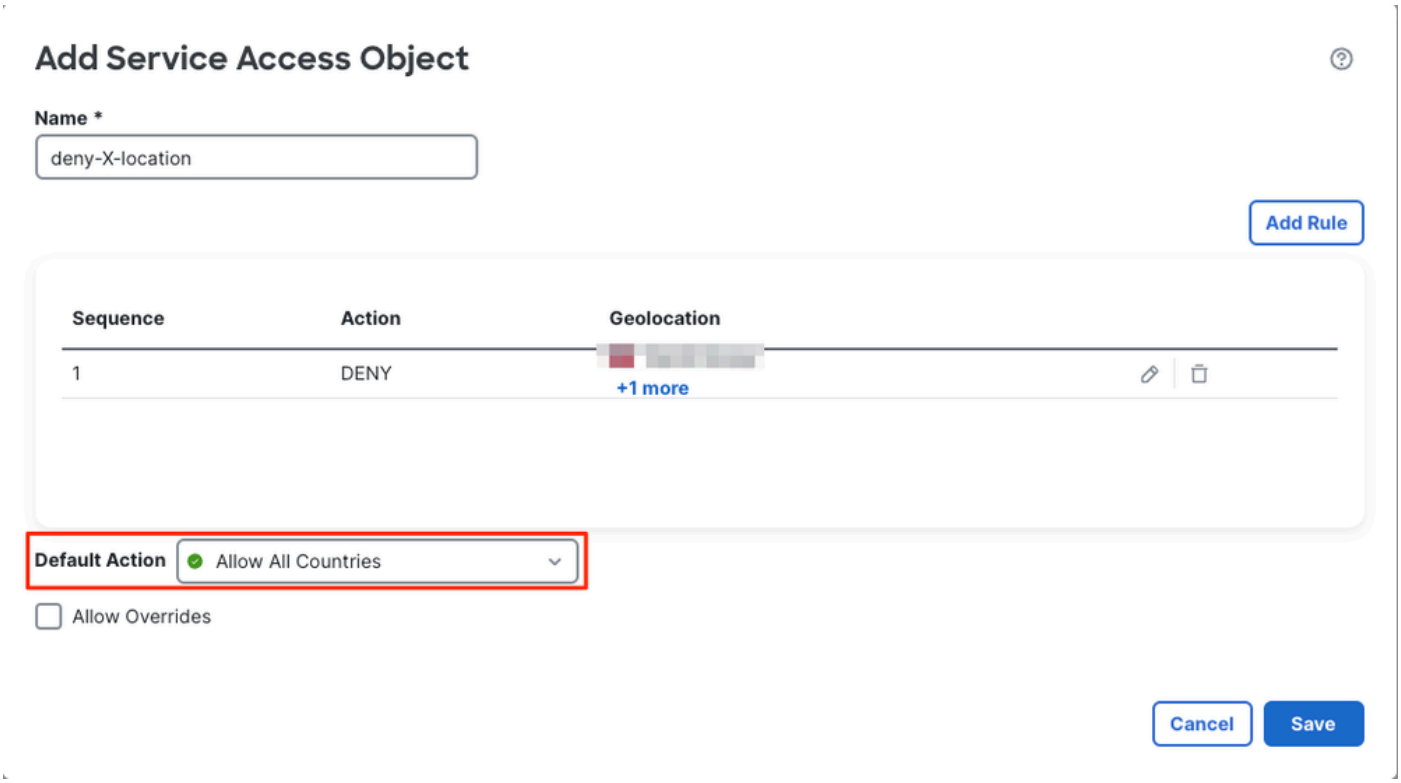
- 규칙의 작업(Allow 또는 Deny)을 선택합니다.
- 사용 가능한 국가에서 국가, 대륙 또는 사용자 정의 지오로케이션 객체를 선택하고 선택한 지오로케이션 목록으로 이동합니다.
- Add(추가)를 클릭하여 규칙을 생성합니다.

참고: 서비스 액세스 객체에서 지오로케이션 객체(국가, 대륙 또는 사용자 지정 지오로케이션)는 하나의 규칙에서만 사용할 수 있습니다.

참고: 서비스 액세스 규칙은 순서를 변경할 수 없으므로 올바른 순서로 구성해야 합니다.



5. 기본 조치를 선택합니다. 모든 국가를 허용하거나 모든 국가를 거부합니다. 이 작업은 구성된 서비스 액세스 규칙과 일치하지 않는 연결에 적용됩니다.

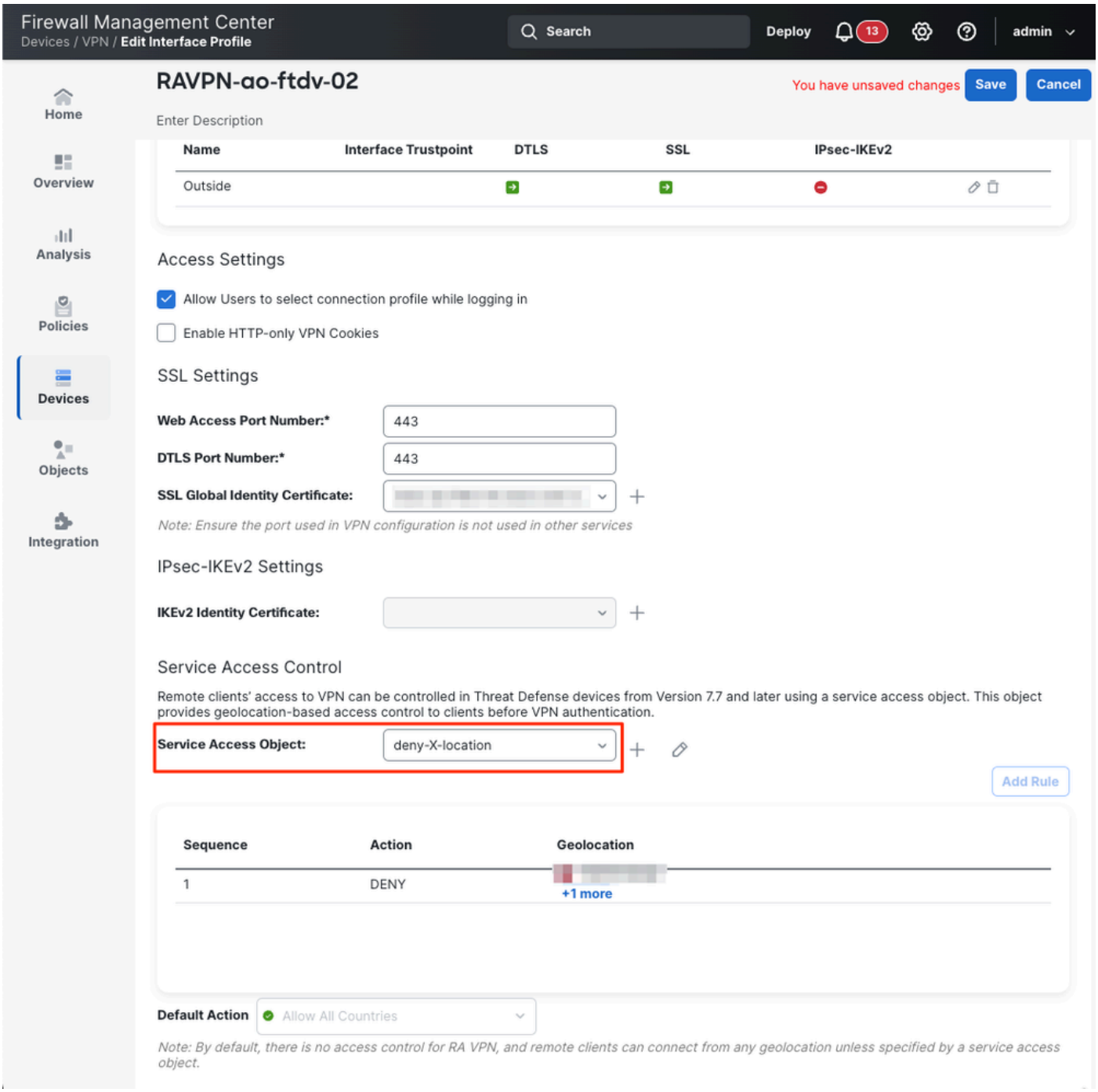


6. 저장을 클릭합니다.

2단계. RAVPN에서 서비스 개체 구성을 적용합니다.

1. Devices(디바이스) > Remote Access(원격 액세스) > RAVPN configuration object(RAVPN 컨피그레이션 개체) > Access interface(액세스 인터페이스)에서 RAVPN 컨피그레이션으로 이동합니다.

2. 서비스 액세스 제어 섹션에서 이전에 생성한 서비스 액세스 객체를 선택합니다.

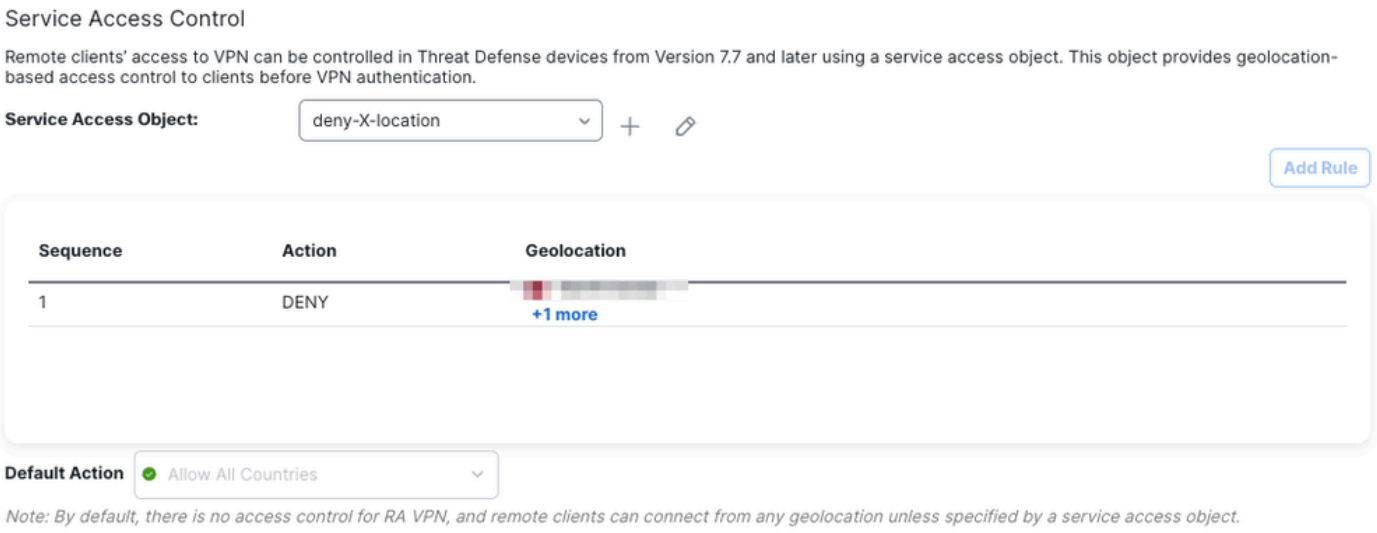


3. 선택한 서비스 액세스 객체에 이제 규칙 요약 및 기본 작업이 표시됩니다. 이것이 정확한지 확인합니다.

4. 마지막으로 변경 사항을 저장하고 구성을 배포합니다.

다음을 확인합니다.

컨피그레이션이 저장되면 규칙이 Service Access Control(서비스 액세스 제어) 섹션에 나타나 어떤 그룹과 국가를 차단하거나 허용할지 검증할 수 있습니다.



show running-config service-access 명령을 실행하여 FTD CLI에서 서비스 액세스 규칙을 사용할 수 있는지 확인합니다.

<#root>

```
firepower#
```

`show running-config service-access`

```
service-access deny ra-ssl-client geolocation FMC_GEOLOCATION_146028889448_536980902
service-access permit ra-ssl-client geolocation any

firepower# show running-config object-group idFMC_GEOLOCATION_146028889448_536980902
object-group geolocation FMC_GEOLOCATION_146028889448_536980902
location "Country X"
location "Country Y"
```

Syslogs 및 모니터링

보안 방화벽에는 지오로케이션 기반 정책에 의해 차단된 RAVPN 연결과 관련된 이벤트를 캡처하기 위해 새로운 syslog ID가 도입되었습니다.

- 761031: IKEv2 연결이 지오로케이션 기반 정책에 의해 거부되는 경우를 나타냅니다. 이 syslog는 기존 VPN 로깅 클래스의 일부입니다.

%FTD-6-751031: 지리적 기반 규칙(geo=<country_name>, id=<country_code>)에 의해 faddr <client_ip> laddr <device_ip>에 대한 IKEv2 원격 액세스 세션이 거부되었습니다.

- 751031: SSL 연결이 지오로케이션 기반 정책에 의해 거부되는 경우를 나타냅니다. 이 syslog는 기존 WebVPN 로깅 클래스의 일부입니다.

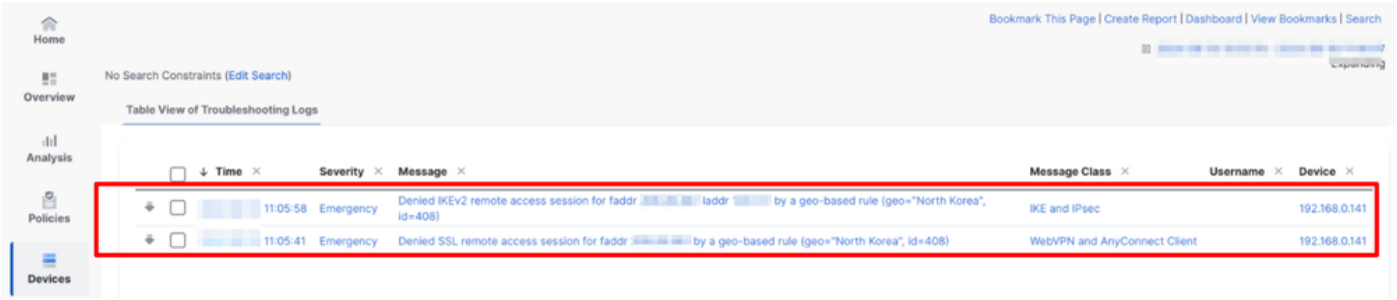
%FTD-6-716166: 지오 기반 규칙(geo=<country_name>, id=<country_code>)에 의해 주소 <client_ip>에 대한 SSL 원격 액세스 세션이 거부되었습니다.

참고: 이러한 새 syslogs의 기본 심각도 수준은 해당 로깅 클래스에서 활성화된 경우 정보를 제공합니다. 그러나 이러한 syslog ID를 개별적으로 활성화하고 심각도를 맞춤화할 수 있습니다.

차단된 연결 모니터링

차단된 연결을 확인하려면 Devices(디바이스) > Troubleshoot(문제 해결) > Troubleshooting Logs(문제 해결 로그)로 이동합니다. 여기에는 연결에 영향을 주는 규칙 및 세션 유형에 대한 정보를 포함하여 차단된 연결과 관련된 로그가 표시됩니다.

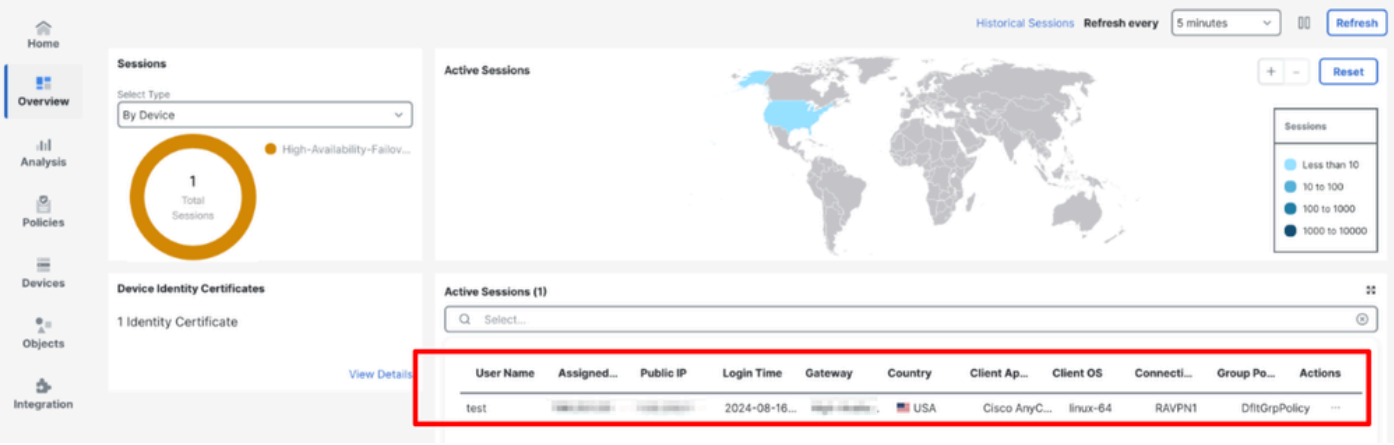
참고: 문제 해결 로그에서 이 정보를 수집하도록 Syslog를 구성해야 합니다.



허용된 연결 모니터링

허용되는 세션은 Overview(개요) > Remote Access VPN(원격 액세스 VPN) 대시보드에서 모니터링됩니다. 이 대시보드에서는 출발지를 비롯한 세션 정보가 표시됩니다.

참고: 이 대시보드에는 허용된 국가의 연결 및 연결이 허용된 사용자만 표시됩니다. 거부된 연결은 이 대시보드에 표시되지 않습니다.



문제 해결

트러블슈팅을 위해 다음 단계를 수행합니다.

1. Service Access 개체에 규칙이 올바르게 구성되어 있는지 확인합니다.
2. 허용된 위치 정보가 세션을 요청할 때 Troubleshooting Logs(문제 해결 로그) 섹션에 거부 syslog가 나타나는지 확인합니다.
3. FMC에 표시된 컨피그레이션이 FTD CLI의 컨피그레이션과 일치하는지 확인합니다.
4. 문제 해결에 유용한 세부 정보를 수집하려면 다음 명령을 사용합니다.

- 디버그 위치 정보 <1-255>
- 서비스 액세스 표시
- 서비스 액세스 세부 정보 표시
- show service-access interface
- 서비스 액세스 위치 표시
- show service-access service
- show geodb ipv4 location <국가> detail
- geodb 카운터 표시
- show geodb ipv4 [lookup <IP address>]
- geodb ipv6 표시

관련 정보

- 추가 지원이 필요한 경우 TAC에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco Worldwide Support 연락처.
- 여기서 Cisco VPN 커뮤니티를 방문할 수도 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.