Geolocation Deploy Failure Behavior with Threat Detection Enabled on Secure Firewall FTD(보안 방화벽 FTD에서 위협 탐지가 활성화된 상태에서 오류 동작 구축)

목차

문제

Cisco Secure Firewall FTD 3105에서 지리적 위치 기반 트래픽 필터링을 구성하려고 할 때 다음과 같은 몇 가지 문제가 발생했습니다.

- 지역 기반 ACP(Access Control Policy) 및 사전 필터 규칙은 FTD 외부 인터페이스에 대한 HTTPS RA-VPN(Remote Access VPN) 연결 시도 차단 영역을 차단하지 못했습니다.
- 버전 7.7.11로 업그레이드한 후, RA-VPN 지오 기반 서비스 액세스를 구성하는 데 실패했으며 네덜란드 또는 네덜란드령 안틸레스 국가가 정책에 포함되었습니다.
- FMC 구축이 83%에서 실패했습니다. 오류 메시지:

```
FMC >> object-group geolocation FMC_GEOLOCATION_184683596782_116848397
FMC >> location "Netherlands"
device >> [error] :
location "Netherlands"
^
ERROR: % Invalid input detected at '^' marker.
Config Error -- location "Netherlands"
```

환경

- Cisco Secure Firewall FTD(Firepower Threat Defense) 3105(FMC에서 관리)
- 업그레이드된 소프트웨어 버전: 7.7.11-1061

- 국가 기반 액세스 제한이 필요한 RA-VPN 구성

해결

이 해결책에는 작동 중인 지리적 위치 기반 액세스 제어를 제대로 검증하기 위한 여러 단계가 포함되었습니다. 또한 Threat Detection이 활성화된 제한이 발견되어 트래픽 매칭 동작에 대한 새로운 지침이 제공되었습니다.

1: FMC 및 FTD를 모두 버전 7.7.11-1061로 업그레이드하여 RA-VPN 지오 기반 서비스 액세스 기능을 활성화합니다. 이 기능은 버전 7.7.0 이상에서만 지원됩니다.

2: Cisco 설명서에 따라 RA-VPN 지오 기반 서비스 액세스를 구성하고 이를 RA-VPN 정책과 연결합니다.

3: Cisco 버그 ID CSCwq15499으로 인한 구축 실패를 해결하려면 네덜란드 또는 네덜란드 앤틸리스 같은 특정 국가를 추가할 때 다음 해결 방법을 적용합니다.

1. 구성된 국가가 없는 빈 RA-VPN 서비스 액세스 개체를 만듭니다.
2. 빈 서비스 액세스 개체를 RA-VPN 정책에 적용하고 성공적으로 구축합니다.
3. 동일한 서비스 액세스 객체를 수정하고 필요한 국가 규칙을 추가합니다.
4. 컨피그레이션을 다시 구축합니다. 이제 구축에 성공하고 지리적 위치 필터링이 활성화됩니다.

4: 구축이 성공적으로 완료되었으며 RA-VPN 액세스 및 로그에 의도한 국가 제한이 반영되었는지 확인합니다. 시스템을 모니터링하여 지리적 위치 제한이 예상대로 작동하는지 확인합니다.

5: FTD에서 이미 활성화된 위협 탐지 기능이 액세스 정책에 도달하기 전에 트래픽과 일치하는지 확인합니다. 이러한 컨피그레이션에서는 정책 적용 전에 위협 탐지가 인계되므로 지오로케이션 규칙을 건너뜁니다.

<#root>

```
device# show run threat-detection
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
```

threat-detection service invalid-vpn-access
threat-detection service remote-access-authentication hold-down 1440 threshold 5
threat-detection service remote-access-client-initiations hold-down 1440 threshold 5

6: 위협 탐지 일치 및 차단과 관련된 모든 syslog ID의 상관관계를 분석하여 트래픽이 Geolocation 대신 Threat Detection을 적중하는지 확인합니다.

- %FTD-4-401002: Shun이 추가됨: IP_address IP_address 포트 포트
- %FTD-4-401003: Shun 삭제됨: IP_주소
- %FTD-4-401004: 차단된 패킷: IP_address ==> interface_name 인터페이스의 IP_address
- %FTD-4-733102: 위협 감지는 차단 목록에 호스트 추가
- %FTD-4-733103: 위협 감지는 차단 목록에서 호스트 호스트 제거
- %FTD-4-733201: 위협 탐지: 서비스[remote-access-client-initiations] 피어[peer-ip]: 실패 임계값 초과: 인터페이스 인터페이스에 shun을 추가합니다. SSL: RA 과도한 클라이언트 시작 요청
- %FTD-4-733201: 위협 탐지: 서비스[remote-access-client-initiations] 피어[peer-ip]: 임계값 실패 임계값 초과: 인터페이스 인터페이스에 shun을 추가합니다. IKEv2:RA_excessive_client_initiation_requests

```
<164>Feb 26 2026 23:05:45: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:07:36: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:12:25: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:00:00: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
---
device# show shun
```

원인

발생한 문제에는 두 가지 고유한 근본 원인이 있습니다.

- 지리적 위치 규칙 일치 제한: RA-VPN 지오 기반 액세스 제어는 소프트웨어 버전 7.7.0 이상에서만 지원됩니다. 또한 구성된 RAVPN 위협 감지는 트래픽에 대해 작동할 수 있으므로 지리적 기반 규칙에서 매칭할 수 없습니다.
- Cisco 버그 ID CSCwq15499: 버전 7.7.11에서는 RA-VPN Geo 서비스 액세스 처리 메커니즘의 알려진 소프트웨어 버그로 인해 특정 국가를 RA-VPN Geo 기반 서비스 액세스 정책에 추가할 때 구축 실패가 발생합니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.