HairPin 트래픽을 사용하여 FTD의 VPN 사용자에 대한 내부 리소스 액세스 구성

목차

문제

목표는 Cisco Secure Firewall FTD에서 RADIUS(Windows 도메인에 가입된 서버에 대한)를 사용하여 VPN 인증에 성공한 후 VPN 사용자가 내부 네트워크 리소스에 완전히 액세스할 수 있도록 하는 것입니다.

VPN 설정이 이미 작동 중입니다. 사용자는 VPN 클라이언트를 다운로드 및 설치하고 성공적으로 인증할 수 있습니다. 이 문제는 VPN을 통해 필요한 내부 리소스 액세스를 허용하는 데 필요한 액세스 제어 및 NAT 규칙을 구성하는 데 중점을 둡니다.

환경

- 제품: Cisco FTD(Secure Firewall Firepower), 버전 7.6.0(예: CSF1220CX 어플라이언스)
- 관리: FMC(Firepower Management Center), cdFMC(클라우드 제공 FMC) 또는 FDM(Firepower Device Manager)
- VPN: NPS(Windows 도메인 가입 서버)에 대한 RADIUS 인증으로 구성됨
- VPN 주소 풀: 192.168.250.1 - 192.168.250.200
- 대상 내부 서브넷 예: 192.168.95.0/24
- 소프트웨어 버전: 9.22.1(워크플로에서 참조)
- 관련 인터페이스: VPN 인그레스(ingress)에 대한 '외부' 인터페이스
- VPN 연결을 통해 필요한 RDP 및 Active Directory 액세스

해결

이 단계에서는 VPN 사용자가 Cisco FTD의 내부 리소스(예: RDP 및 Active Directory)에 액세스할 수 있도록 허용하는 데 필요한 컨피그레이션에 대해 자세히 설명합니다. 여기에는 액세스 정책 규칙 생성, VPN 트래픽용 NAT 예외 및 헤어핀 NAT 구성, 트러블슈팅 명령을 사용하여 컨피그레이션을 확인하는 것이 포함됩니다.

1단계: VPN 주소 풀이 내부 리소스에 액세스할 수 있도록 access-list 항목을 추가합니다.

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

2단계: 내부 리소스가 반환 트래픽을 VPN 풀로 전송하도록 허용하는 access-list 규칙을 추가합니다.

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

나중에 필요에 따라 이러한 규칙을 강화하여 특정 소스 및 대상을 제한할 수 있습니다.

3단계: VPN 트래픽용 NAT 예외 또는 헤어핀 NAT 구성

두 가지 일반적인 접근 방식이 있습니다.

- ◦ 옵션 A: 내부 서브넷에 대한 VPN 풀의 NAT 예외

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- ◦ 옵션 B: 동일한 인터페이스의 VPN 풀용 헤어핀 NAT(no-proxy-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- ◦ 옵션 C: 외부 인터페이스의 VPN 풀용 동적 헤어핀 NAT

```
nat (outside,outside) dynamic VPN_Pool interface
```

올바른 방법은 내부 리소스가 동일한 물리적 인터페이스(헤어핀 NAT 필요)에 있는지 또는 다른 인터페이스(NAT 제외)에 있는지에 따라 다릅니다.

4단계: packet-tracer 명령을 사용하여 VPN 풀에서 내부 리소스로의 트래픽 흐름을 시뮬레이션하고 트래픽이 의도한 규칙, NAT 및 경로에 의해 허용되는지 검증합니다.

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
--
Phase 5
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
```

```
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

참고: WebVPN 단계에 대한 패킷 추적기 출력에는 외부 인터페이스의 VPN 트래픽에 대해 "DROP"이 표시될 수 있습니다. 이는 외부 인터페이스의 일반 텍스트 트래픽에 대해 예상된 동작이며 NAT를 확인하는 데 계속 사용될 수 있습니다.

추가 참고 사항:

- Threat Defense UI의 패킷 캡처에는 들어오는 요청만 표시될 수 있습니다. 삭제는 관찰되지 않지만 트래픽이 내부 리소스에 도달하지 않는 경우 NAT 및 access-list 규칙을 확인하십시오.
- SSH를 사용할 수 없는 경우 cdFMC의 Threat Defense UI 기능을 통해 모든 트러블슈팅을 수행할 수 있지만 명령 사용은 제한됩니다.
- 엔드 투 엔드 연결을 위해 인접한 디바이스에서 일부 수정이 필요할 수 있습니다.

원인

근본 원인은 VPN-내부 및 내부-VPN 풀 트래픽에 대한 액세스 정책 및 NAT 컨피그레이션이 충분하지 않았기 때문입니다. 기본 컨피그레이션에서는 VPN 풀에서 내부 리소스로, 그리고 내부 리소스로 완전히 양방향 통신을 허용하지 않았으며, 동일한 인터페이스에서 트래픽 인그레이싱 및 이그레싱에 대한 헤어핀 NAT 요구 사항을 처리하지 않았습니다.

관련 콘텐츠

- FTD에서 NAT 예외 구성
- 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.