ASA에서 헤어핀 구성

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

구성

- 네트워크 다이어그램
- 설정
- 1단계. 개체 만들기
- 2단계. NAT 생성
- 다음을 확인합니다.

문제 해결

- 1단계: NAT 규칙 컨피그레이션 확인
- 2단계: ACL(액세스 제어 규칙) 확인
- 3단계: 추가 진단

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)에서 헤어핀을 성공적으로 구성하는 데 필요한 단계에 대해 설명합니다

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- ASA의 NAT 컨피그레이션
- ASA의 ACL 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Adaptive Security Appliance Software 버전 9.18(4)22

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.

구성

NAT 루프백 또는 NAT 반사라고도 하는 헤어핀 NAT(Network Address Translation)는 사설 네트워크의 장치가 공용 IP 주소를 통해 동일한 사설 네트워크의 다른 장치에 액세스할 수 있는 네트워크 라우팅에 사용되는 기술입니다.

이 기능은 서버가 라우터 뒤에서 호스팅되는 경우, 서버와 동일한 로컬 네트워크의 장치가 외부 장치처럼 공용 IP 주소(인터넷 서비스 공급자가 라우터에 할당한 주소)를 사용하여 서버에 액세스하도록 하려는 경우에 사용됩니다.

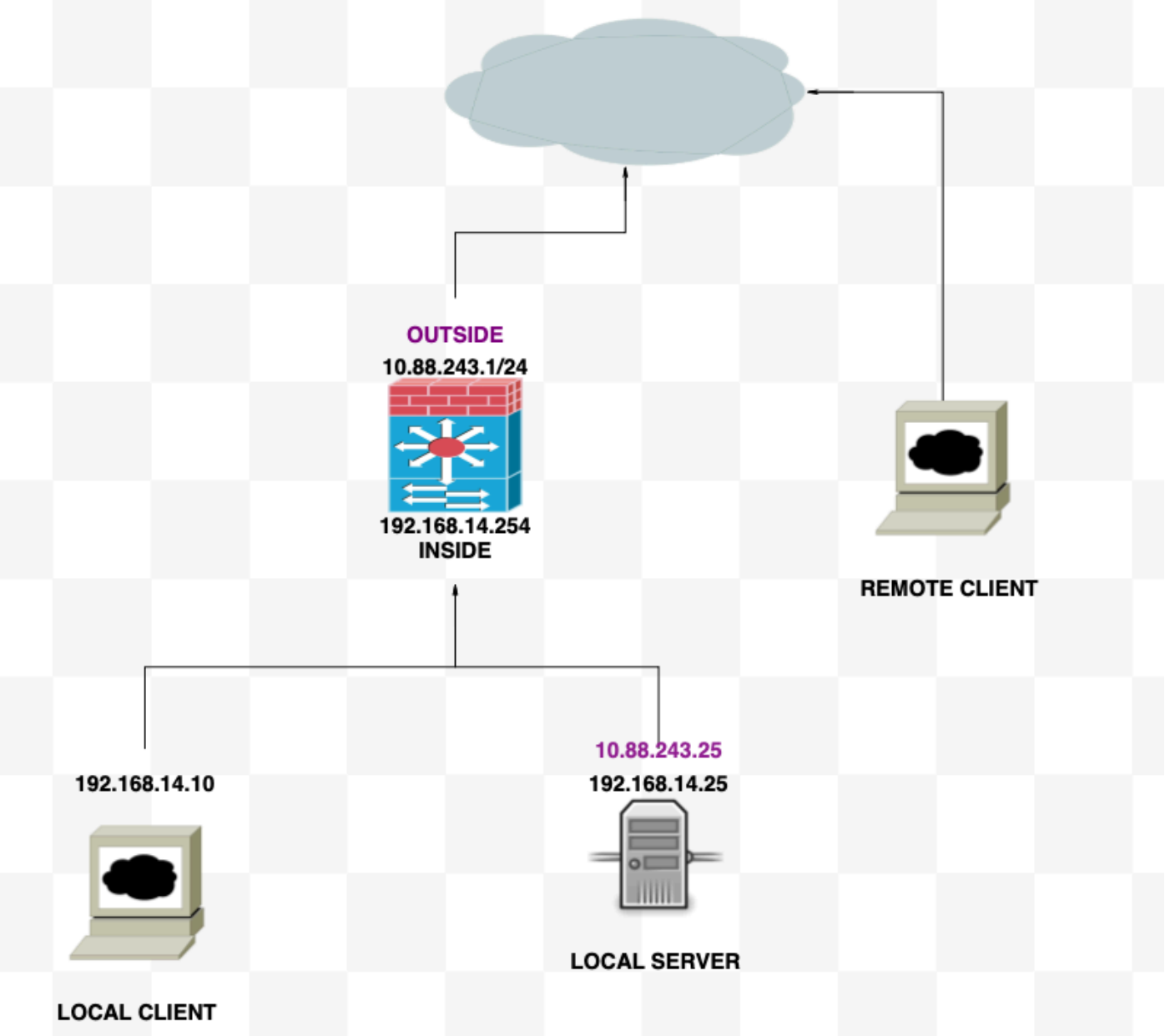
클라이언트의 트래픽이 라우터(또는 NAT를 구현하는 방화벽)로 이동한 다음 서버의 개인 IP 주소에 액세스하기 위해 변환 후 내부 네트워크로 가는 헤어핀처럼 "돌아가기"되므로 "헤어핀"이라는 용어가 사용됩니다.

예를 들어, 로컬 네트워크에 사설 IP 주소를 가진 웹 서버가 있습니다. 동일한 로컬 네트워크에 있는 경우에도 공용 IP 주소 또는 공용 IP 주소로 확인되는 도메인 이름을 사용하여 이 서버에 액세스하려고 합니다.

Hairpin NAT가 없으면 공용 IP 주소에 대한 요청이 네트워크 외부에서 들어올 것으로 예상하므로 라우터가 이 요청을 이해하지 못할 수 있습니다.

헤어핀 NAT는 공용 IP에 대한 요청이 이루어지고 있지만 로컬 네트워크의 디바이스로 라우팅되어야 함을 라우터가 인식할 수 있도록 하여 이 문제를 해결합니다.

네트워크 다이어그램



설정

1단계. 개체 만들기

- 내부 네트워크:192.168.14.10
- 웹 서버: 192.168.14.25
- 공용 웹 서버: 10.88.243.25
- 포트: 80

<#root>

```
ciscoasa(config)#
 object network Local_Client
ciscoasa(config-network-object)#
 host 192.168.14.10
```

```
ciscoasa(config)#
 object network Web_Server
ciscoasa(config-network-object)#
 host 192.168.14.25
ciscoasa(config)#
 object network P_Web_Server
ciscoasa(config-network-object)#
 host 10.88.243.25
ciscoasa(config)#
 object service HTTP
ciscoasa(config-service-object)#
 service tcp destination eq 80
```

2단계. NAT 생성

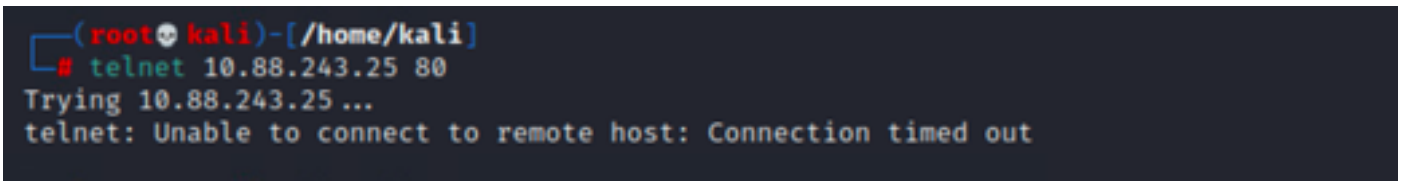
<#root>

```
ciscoasa
(config-service-object)# nat (Inside,Inside) source dynamic Local_Client interface destination static P_
```

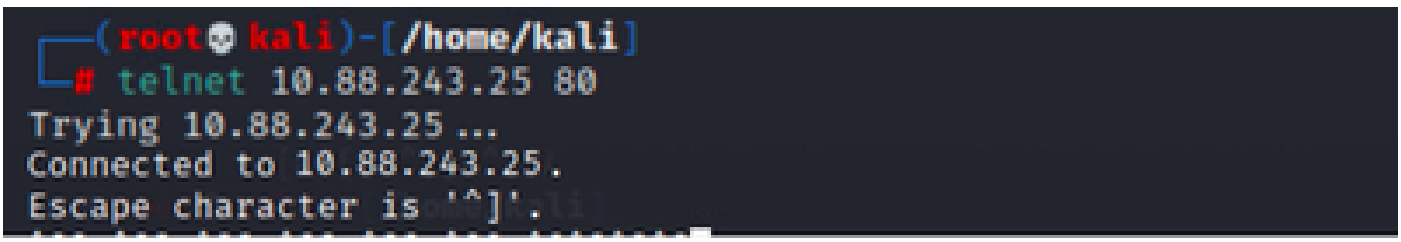
다음을 확인합니다.

로컬 클라이언트에서 대상 포트가 없는 텔넷 대상 IP를 수행합니다.

"텔넷이 원격 호스트에 연결할 수 없습니다. 연결 시간이 초과되었습니다"라는 메시지가 표시되면 컨피그레이션 중 특정 지점에서 오류가 발생한 것입니다.



하지만 "Connected"라고 말하면 효과가 있습니다!



문제 해결

NAT(Network Address Translation)에 문제가 있는 경우 이 단계별 가이드를 사용하여 일반적인 문제를 해결하고 해결하십시오.

1단계: NAT 규칙 컨피그레이션 확인

- NAT 규칙 검토: 모든 NAT 규칙이 올바르게 구성되었는지 확인합니다. 소스 및 목적지 IP 주소와 포트가 정확한지 확인합니다.
- Interface Assignment(인터페이스 할당): 소스 인터페이스와 목적지 인터페이스가 모두 NAT 규칙에서 올바르게 할당되었는지 확인합니다. 매핑이 잘못되면 트래픽이 제대로 변환되거나 라우팅되지 않을 수 있습니다.
- NAT 규칙 우선순위: NAT 규칙이 동일한 트래픽과 일치할 수 있는 다른 어떤 규칙보다 우선순위가 높게 지정되었는지 확인합니다. 규칙은 순차적으로 처리되므로, 위에 있는 규칙의 우선순위가 높습니다.

2단계: ACL(액세스 제어 규칙) 확인

- ACL 검토: ACL이 NAT 트래픽 허용에 적합한지 확인하려면 ACL을 선택합니다. 변환된 IP 주소를 인식하도록 ACL을 구성해야 합니다.
- 규칙 순서: 액세스 제어 목록이 올바른 순서인지 확인하십시오. NAT 규칙과 마찬가지로 ACL은 위에서 아래로 처리되며 트래픽과 일치하는 첫 번째 규칙이 적용됩니다.
- Traffic Permissions(트래픽 권한): 내부 네트워크에서 변환된 목적지로의 트래픽을 허용하기 위한 적절한 액세스 제어 목록이 있는지 확인합니다. 규칙이 누락되거나 잘못 구성된 경우 원하는 트래픽을 차단할 수 있습니다.

3단계: 추가 진단

- Use Diagnostic Tools(진단 도구 사용): 디바이스를 통과하는 트래픽을 모니터링하고 디버깅하는 데 사용할 수 있는 진단 도구를 활용합니다. 여기에는 실시간 로그 및 연결 이벤트 보기가 포함됩니다.
- Restart Connections(연결 재시작): 경우에 따라 기존 연결은 재시작될 때까지 NAT 규칙 또는 ACL에 대한 변경 사항을 인식하지 못합니다. 새 규칙을 강제로 적용하려면 기존 연결을 지우는 것이 좋습니다.

<#root>

ciscoasa(config)#

 clear xlate

- 변환 확인: ASA 디바이스로 작업하여 NAT 변환이 예상대로 수행되고 있는지 확인하려면 명령줄에서 `show xlate` 및 `show nat` 등의 명령을 사용합니다.

<#root>

ciscoasa(config)#

show xlate

<#root>

ciscoasa(config)#

show nat

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.