ASA 방화벽에서 NAT 및 ACL 구성

목차

소개

이 문서에서는 ASA 방화벽에서 NAT(Network Address Translation) 및 ACL(Access Control List)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 ASA 코드 버전 9.1(1)을 실행하는 ASA 5510 방화벽을 기반으로 합니다.

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

이 문서에서는 아웃바운드 및 인바운드 연결을 허용하기 위해 ASA 방화벽에서 NAT 및 ACL을 구성하는 방법의 단순하고 간단한 예를 설명합니다. ASA 코드 버전 9.1(1)을 실행하는 ASA(Adaptive Security Appliance) 5510 방화벽으로 작성되었지만 다른 모든 ASA 방화벽 플랫폼에 쉽게 적용할 수 있습니다. 물리적 인터페이스 대신 VLAN을 사용하는 ASA 5505와 같은 플랫폼을 사용하는 경우 인터페이스 유형을 적절하게 변경해야 합니다.

개요

목표

이 예제 컨피그레이션에서는 ASA 방화벽의 DMZ에 있는 웹 서버에 대한 인바운드 액세스를 허용하고 내부 및 DMZ 호스트로부터의 아웃바운드 연결을 허용하기 위해 어떤 NAT 및 ACL 컨피그레이션이 필요한지 살펴볼 수 있습니다. 이는 두 가지 목표로 요약할 수 있습니다.

1. 내부 및 DMZ 아웃바운드 연결의 호스트를 인터넷에 허용합니다.
2. 인터넷의 호스트가 IP 주소가 192.168.1.100인 DMZ의 웹 서버에 액세스하도록 허용합니다.

이 두 가지 목표를 달성하기 위해 완료해야 하는 단계를 수행하기 전에 이 문서에서는 ACL 및 NAT가 최신 버전의 ASA 코드(버전 8.3 이상)에서 작동하는 방식을 간략하게 살펴봅니다.

액세스 제어 목록 개요

ACL(Access Control Lists)은 ASA 방화벽에서 트래픽이 허용되거나 거부되는지 확인하는 방법입니다. 기본적으로 하위 보안 수준에서 상위 보안 수준으로 전달되는 트래픽은 거부됩니다. 이는 하위 보안 인터페이스에 적용되는 ACL에 의해 재정의될 수 있습니다. 또한 ASA는 기본적으로 더 높은 보안 인터페이스에서 더 낮은 보안 인터페이스로의 트래픽을 허용합니다. 이 동작은 ACL로 재정의할 수도 있습니다.

이전 버전의 ASA 코드(8.2 이하)에서는 ASA가 먼저 패킷을 변환하지 않고 들어오는 연결 또는 패킷을 인터페이스의 ACL과 비교했습니다. 즉, ACL은 인터페이스에서 패킷을 캡처하는 것처럼 패킷을 허용해야 했습니다. 버전 8.3 이상의 코드에서 ASA는 인터페이스 ACL을 확인하기 전에 해당 패킷을 변환하지 않습니다. 즉, 8.3 이상 코드 및 이 문서의 경우 호스트의 변환된 IP가 아니라 호스트의 실제 IP에 대한 트래픽이 허용됩니다.

ACL에 대한 자세한 내용은 책 2: Cisco ASA Series 방화벽 CLI 컨피그레이션 가이드, 9.1의 액세스 규칙 구성 섹션을 참조하십시오.

NAT 개요

버전 8.3 이상에서 ASA의 NAT는 자동 NAT(Object NAT) 및 수동 NAT(Twice NAT)라는 두 가지 유형으로 나뉩니다. 두 NAT 중 첫 번째인 Object NAT는 네트워크 객체의 정의 내에서 구성됩니다. 이에 대한 예는 이 문서의 뒷부분에 나와 있습니다. 이 NAT 방법의 한 가지 주요 장점은 충돌을 피하기 위해 ASA에서 처리 규칙을 자동으로 주문한다는 것입니다. 이는 가장 쉬운 NAT 형식이지만, 이 경우 컨피그레이션 세분화에 한계가 발생합니다. 예를 들어, 두 번째 NAT 유형인 수동 NAT와 마찬가지로 패킷의 목적지를 기반으로 변환 결정을 내릴 수 없습니다. 수동 NAT는 세분성이 더 강력하지만, 올바른 동작을 수행하려면 올바른 순서로 행을 구성해야 합니다. 이로 인해 이 NAT 유형이 복잡해지기 때문에 이 컨피그레이션 예에서는 이 유형을 사용할 수 없습니다.

NAT에 대한 자세한 내용은 책 2: Cisco ASA Series Firewall CLI 컨피그레이션 가이드, 9.1의 NAT에 대한 정보 섹션을 참조하십시오.

구성

시작하기

기본 ASA 컨피그레이션 설정은 3개의 네트워크 세그먼트에 연결된 3개의 인터페이스입니다. ISP 네트워크 세그먼트가 Ethernet0/0 인터페이스에 연결되고 보안 수준 0으로 외부에 레이블이 지정됩니다. 내부 네트워크는 Ethernet0/1에 연결되어 있으며 보안 수준이 100인 inside로 레이블이 지정되어 있습니다. 웹 서버가 상주하는 DMZ 세그먼트는 Ethernet0/2에 연결되며 보안 수준이 50인 DMZ로 레이블이 지정됩니다.

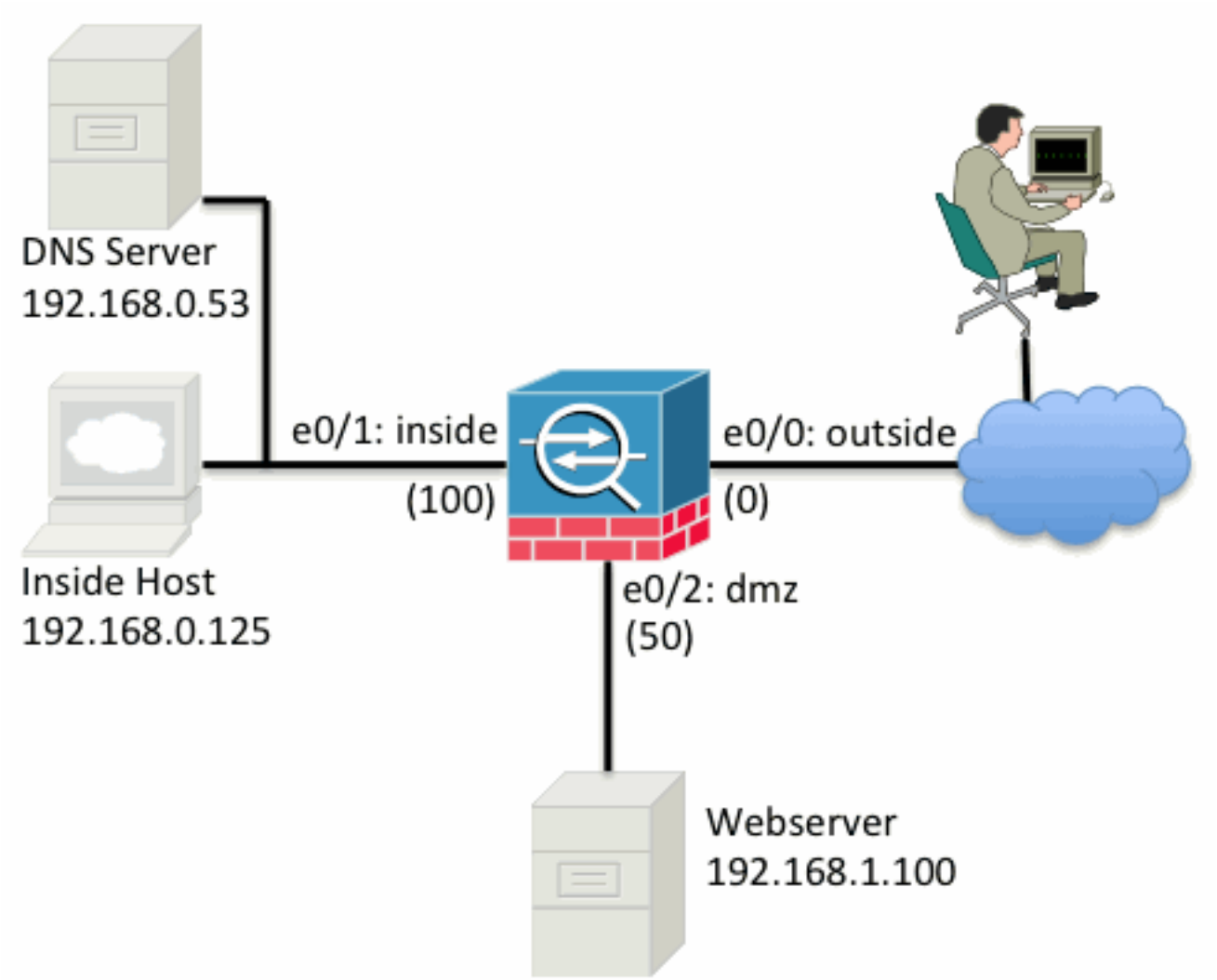
이 예의 인터페이스 컨피그레이션 및 IP 주소는 다음과 같습니다.

```
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

여기서 ASA의 내부 인터페이스가 IP 주소 192.168.0.1로 설정되어 있으며 내부 호스트의 기본 게이트웨이임을 확인할 수 있습니다. ASA의 외부 인터페이스는 ISP에서 얻은 IP 주소로 구성됩니다. 기본 경로가 있으며, 이 경로는 next-hop을 ISP 게이트웨이로 설정합니다. DHCP를 사용하는 경우 자동으로 제공됩니다. DMZ 인터페이스는 IP 주소 192.168.1.1로 구성되며, DMZ 네트워크 세그먼트의 호스트에 대한 기본 게이트웨이입니다.

토폴로지

이 케이블 연결 및 구성 방법을 시각적으로 살펴보면 다음과 같습니다.



1단계. 호스트가 인터넷으로 나갈 수 있도록 NAT 구성

이 예에서는 AutoNAT라고도 하는 Object NAT가 사용됩니다. 가장 먼저 구성할 사항은 내부 및 DMZ 세그먼트의 호스트가 인터넷에 연결할 수 있도록 허용하는 NAT 규칙입니다. 이러한 호스트는 사설 IP 주소를 사용하므로 인터넷에서 라우팅 가능한 주소로 변환해야 합니다. 이 경우 ASA의 외부 인터페이스 IP 주소처럼 보이도록 주소를 변환합니다. 외부 IP가 자주 변경되는 경우(DHCP 때문인지), 가장 간단하게 설정할 수 있는 방법입니다.

이 NAT를 구성하려면 내부 서브넷을 나타내는 네트워크 개체와 DMZ 서브넷을 나타내는 네트워크 개체를 만들어야 합니다. 각 개체에서 이러한 클라이언트가 해당 인터페이스에서 외부 인터페이스로 전달될 때 PAT(Port Address Translation)를 수행할 수 있는 동적 nat 규칙을 구성합니다.

이 컨피그레이션은 다음과 유사합니다.

```
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
nat (inside,outside) dynamic interface
!
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
nat (dmz,outside) dynamic interface
```

이 시점에서 실행 중인 컨피그레이션을 보면(show run 명령의 출력) 객체 정의가 출력의 두 부분으로 분할됨을 확인할 수 있습니다. 첫 번째 부분은 객체(호스트/서브넷, IP 주소 등)의 내용만 나타내고, 두 번째 섹션에서는 NAT 규칙이 해당 객체와 연결되어 있음을 보여줍니다. 이전 출력의 첫 번째

항목을 선택하는 경우

192.168.0.0/24 서브넷과 일치하는 호스트가 내부 인터페이스에서 외부 인터페이스로 이동할 때 외부 인터페이스로 동적으로 변환하려는 경우

2단계. 인터넷에서 웹 서버에 액세스하도록 NAT 구성

이제 내부 및 DMZ 인터페이스의 호스트가 인터넷에 연결될 수 있으므로 인터넷의 사용자가 TCP 포트 80의 웹 서버에 액세스할 수 있도록 컨피그레이션을 수정해야 합니다. 이 예에서는 인터넷에 있는 사용자가 ISP에서 제공한 다른 IP 주소(*보유한* 추가 IP 주소)에 연결할 수 있도록 *설정합니다*. 이 예에서는 198.51.100.101을 사용합니다. 이 구성에서는 인터넷의 사용자가 TCP 포트 80에서 198.51.100.101에 액세스하여 DMZ 웹 서버에 연결할 수 있습니다. 이 작업에 개체 NAT를 사용하면 ASA가 웹 서버의 TCP 포트 80(192.168.1.100)을 외부의 TCP 포트 80의 198.51.100.101처럼 변환할 수 있습니다. 이전에 수행했던 것과 마찬가지로 객체를 정의하고 해당 객체에 대한 변환 규칙을 정의합니다. 또한 이 호스트를 변환할 수 있는 IP를 나타내는 두 번째 객체를 정의합니다.

이 컨피그레이션은 다음과 유사합니다.

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

이 예에서 NAT 규칙이 의미하는 바를 요약하면 다음과 같습니다.

DMZ 세그먼트에서 IP 주소 192.168.1.100과 일치하는 호스트가 TCP 포트 80(www)에서 제공된 연결을 설정하고 해당 연결이 외부 인터페이스로 나가는 경우 외부 인터페이스의 TCP 포트 80(www)으로 변환하고 해당 IP 주소를 198.51.100.101로 변환해야 합니다.

약간 이상하게 보이지만, 웹 트래픽은 포트 80을 목적지로 합니다. 이러한 NAT 규칙은 기본적으로 양방향임을 이해하는 것이 중요합니다. 그 결과 이 문장을 다시 표현하기 위해 단어를 뒤집어 쓸 수 있습니다. 그 결과는 훨씬 더 의미가 있습니다.

외부의 호스트가 대상 TCP 포트 80(www)의 198.51.100.101에 대한 연결을 설정하면 대상 IP 주소를 192.168.1.100으로 변환하고 대상 포트는 TCP 포트 80(www)일 수 있으며 DMZ로 전송할 수 있습니다.

이렇게 표현하면 더 이해가 됩니다. 다음으로, ACL을 설정해야 합니다.

3단계. ACL 구성

NAT가 구성되었으며 이 컨피그레이션의 끝이 가깝습니다. ASA의 ACL을 사용하면 다음과 같은 기본 보안 동작을 재정의할 수 있습니다.

- 하위 보안 인터페이스에서 이동하는 트래픽은 상위 보안 인터페이스로 이동할 때 거부됩니다.
- 더 높은 보안 인터페이스에서 나가는 트래픽은 더 낮은 보안 인터페이스로 이동할 때 허용됩니다.

따라서 컨피그레이션에 ACL을 추가하지 않은 경우 이 예에서 이 트래픽은 작동합니다.

- 내부의 호스트(보안 수준 100)는 DMZ의 호스트(보안 수준 50)에 연결할 수 있습니다.

- 내부의 호스트(보안 수준 100)는 외부의 호스트(보안 수준 0)에 연결할 수 있습니다.
- DMZ(보안 수준 50)의 호스트는 외부(보안 수준 0)의 호스트에 연결할 수 있습니다.

그러나 이 트래픽은 거부됩니다.

- 외부(보안 수준 0)의 호스트는 내부(보안 수준 100)의 호스트에 연결할 수 없습니다.
- 외부(보안 수준 0)의 호스트는 DMZ(보안 수준 50)의 호스트에 연결할 수 없습니다.
- DMZ(보안 수준 50)의 호스트는 내부(보안 수준 100)의 호스트에 연결할 수 없습니다.

외부에서 DMZ 네트워크로 향하는 트래픽은 현재 컨피그레이션의 ASA에서 거부하므로, 2단계의 NAT 컨피그레이션에도 불구하고 인터넷의 사용자가 웹 서버에 연결할 수 없습니다. 이 트래픽을 명시적으로 허용해야 합니다. 8.3 이상 코드에서는 변환된 IP가 아니라 ACL에 있는 호스트의 실제 IP를 사용해야 합니다. 즉, 컨피그레이션에서 포트 80에서 192.168.1.100으로 향하는 트래픽은 허용하고 198.51.100.101로 향하는 트래픽은 허용하지 않아야 합니다. 간소화를 위해 2단계에서 정의한 객체를 이 ACL에도 사용할 수 있습니다. ACL이 생성되면 외부 인터페이스에서 인바운드에 적용해야 합니다.

다음은 이러한 컨피그레이션 명령의 모습입니다.

```
access-list outside_acl extended permit tcp any object webserver eq www
!
access-group outside_acl in interface outside
```

액세스 목록 줄 상태는 다음과 같습니다.

any(where)에서 포트 80의 객체 웹 서버(192.168.1.100)가 나타내는 호스트로의 트래픽을 허용합니다.

컨피그레이션에서 여기서 any 키워드를 사용해야 합니다. 클라이언트의 소스 IP 주소는 웹 사이트에 도달하므로 알 수 없으므로 '모든 IP 주소'라는 의미를 지정합니다.

내부 네트워크 세그먼트의 호스트로 향하는 DMZ 세그먼트의 트래픽은 어떻습니까? 예를 들어, DMZ의 호스트가 연결해야 하는 내부 네트워크의 서버. ASA에서 내부 서버로 향하는 특정 트래픽만 허용하고 DMZ에서 내부 세그먼트로 향하는 다른 모든 트래픽은 차단하려면 어떻게 해야 합니까?

이 예에서는 DMZ의 호스트가 DNS 확인을 위해 액세스해야 하는 IP 주소 192.168.0.53의 내부 네트워크에 DNS 서버가 있다고 가정합니다. 필요한 ACL을 생성하여 DMZ 인터페이스에 적용하면 ASA에서 해당 인터페이스로 들어오는 트래픽에 대해 앞에서 언급한 기본 보안 동작을 재정의할 수 있습니다.

다음은 이러한 컨피그레이션 명령의 모습입니다.

```
object network dns-server
host 192.168.0.53
!
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
access-group dmz_acl in interface dmz
```

ACL은 단순히 UDP 포트 53의 DNS 서버로 트래픽을 허용하는 것보다 더 복잡합니다. 첫 번째 허용 회선만 사용했다면 DMZ에서 인터넷의 호스트로 전송되는 모든 트래픽이 차단됩니다. ACL은 ACL의 끝에 암시적 'deny ip any any'가 있습니다. 따라서 DMZ 호스트가 인터넷에 연결되지 않습니다. DMZ에서 외부로의 트래픽은 DMZ 인터페이스에 ACL을 적용하여 기본적으로 허용되지만 DMZ

인터페이스에 대한 기본 보안 동작은 더 이상 적용되지 않으며 인터페이스 ACL에서 트래픽을 명시적으로 허용해야 합니다.

4단계. 패킷 추적기 기능을 사용하여 컨피그레이션 테스트

이제 컨피그레이션이 완료되었으므로, 제대로 작동하는지 확인하기 위해 테스트해야 합니다. 가장 쉬운 방법은 실제 호스트를 사용하는 것입니다(네트워크인 경우). 그러나 CLI에서 이를 테스트하고 일부 ASA 툴을 자세히 살펴보려면 패킷 추적기를 사용하여 발생한 문제를 테스트하고 잠재적으로 디버깅하십시오.

패킷 추적기는 일련의 매개 변수를 기반으로 패킷을 시뮬레이션하고 해당 패킷을 인터페이스 데이터 경로에 삽입하는 방식으로 작동하는데, 이는 실제 패킷이 와이어에서 픽업될 때와 비슷합니다. 이 패킷은 방화벽을 통과할 때 수행되는 수많은 검사 및 프로세스를 통해 뒤따르며, 패킷 추적기는 결과를 기록합니다. 인터넷상의 호스트로 나가는 내부 호스트를 시뮬레이션합니다. 이 명령은 방화벽에 다음을 수행하도록 지시합니다.

소스 포트 12345의 IP 주소 192.168.0.125에서 내부 인터페이스로 들어오는 TCP 패킷을 시뮬레이션하여 포트 80의 IP 주소 203.0.113.1로 지정합니다.

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config: Additional Information:
in 0.0.0.0 0.0.0.0 outside Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

결과적으로 트래픽이 허용되며, 이는 컨피그레이션에서 모든 NAT 및 ACL 검사를 통과했고 이그레스 인터페이스 외부로 전송되었음을 의미합니다. 패킷은 3단계에서 변환되었으며, 해당 단계의 세부 정보에는 적중된 규칙이 표시됩니다. 호스트 192.168.0.125는 구성에 따라 198.51.100.100으로 동적으로 변환됩니다.

이제 인터넷에서 웹 서버로의 연결을 위해 실행하십시오. 인터넷의 호스트는 외부 인터페이스의 198.51.100.101에 연결하여 웹 서버에 액세스할 수 있습니다. 다음 명령은 다시 다음으로 변환됩니다.

소스 포트 12345의 IP 주소 192.0.2.123에서 외부 인터페이스로 들어오는 TCP 패킷을 시뮬레이션하여 포트 80의 IP 주소 198.51.100.101로 지정합니다.

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
```

```
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

이 경우에도 패킷이 허용됩니다. ACL이 체크 아웃되고 컨피그레이션이 정상적으로 표시되며 인터넷 사용자(외부)가 외부 IP를 사용하여 해당 웹 서버에 액세스할 수 있습니다.

다음을 확인합니다.

확인 절차는 4단계 - 패킷 추적기 기능으로 컨피그레이션 테스트에 포함되어 있습니다.

문제 해결

현재 이 구성의 문제를 해결하는 방법에 대한 특정 정보가 없습니다.

결론

기본 NAT를 수행하도록 ASA를 구성하는 것은 그리 어려운 작업이 아닙니다. 예제 컨피그레이션에서 사용되는 IP 주소 및 포트를 변경하는 경우 이 문서의 예제를 특정 시나리오에 맞게 수정할 수 있습니다. 이에 대한 최종 ASA 컨피그레이션이 결합될 경우 ASA 5510의 경우와 유사합니다.

```
ASA Version 9.1(1)
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

예를 들어, ASA 5505에서 인터페이스가 앞서 표시된 대로 연결된 경우(Ethernet0/0에 연결된 외부,

Ethernet0/1에 연결된 내부 및 Ethernet0/2에 연결된 DMZ):

```
ASA Version 9.1(1)
!
interface Ethernet0/0
description Connected to Outside Segment
switchport access vlan 2
!
interface Ethernet0/1
description Connected to Inside Segment
switchport access vlan 1
!
interface Ethernet0/2
description Connected to DMZ Segment
switchport access vlan 3
!
interface Vlan2
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53



!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

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.