ASA 8.3:Cisco Security Appliance를 통한 연결 설정 및 문제 해결

목차

소개

Cisco ASA(Adaptive Security Appliance)가 처음 구성된 경우 내부 모든 사용자가 나갈 수 있는 기본 보안 정책이 있으며 외부 사용자가 들어갈 수 없습니다.사이트에 다른 보안 정책이 필요한 경우 외부 사용자가 ASA를 통해 웹 서버에 연결하도록 허용할 수 있습니다.

Cisco ASA를 통해 기본 연결을 설정한 후에는 방화벽에 대한 컨피그레이션을 변경할 수 있습니다 .ASA에 대한 컨피그레이션 변경 사항이 사이트 보안 정책을 준수하는지 확인합니다.

PIX/ASA 참조:버전 8.2 이하의 Cisco ASA에서 동일한 컨피그레이션을 위해 Cisco Security Appliance를 통해 연결을 설정하고 문제를 해결합니다.

사전 요구 사항

요구 사항

이 문서에서는 일부 기본 컨피그레이션이 Cisco ASA에서 이미 완료된 것으로 가정합니다.초기 ASA 컨피그레이션의 예는 다음 문서를 참조하십시오.

- ASA 8.3(x):인터넷에 단일 내부 네트워크 연결
- Cisco ASA(Adaptive Security Appliance)에서 PPPoE 클라이언트 구성

사용되는 구성 요소

이 문서의 정보는 버전 8.3 이상을 실행하는 Cisco ASA(Adaptive Security Appliance)를 기반으로 합니다.

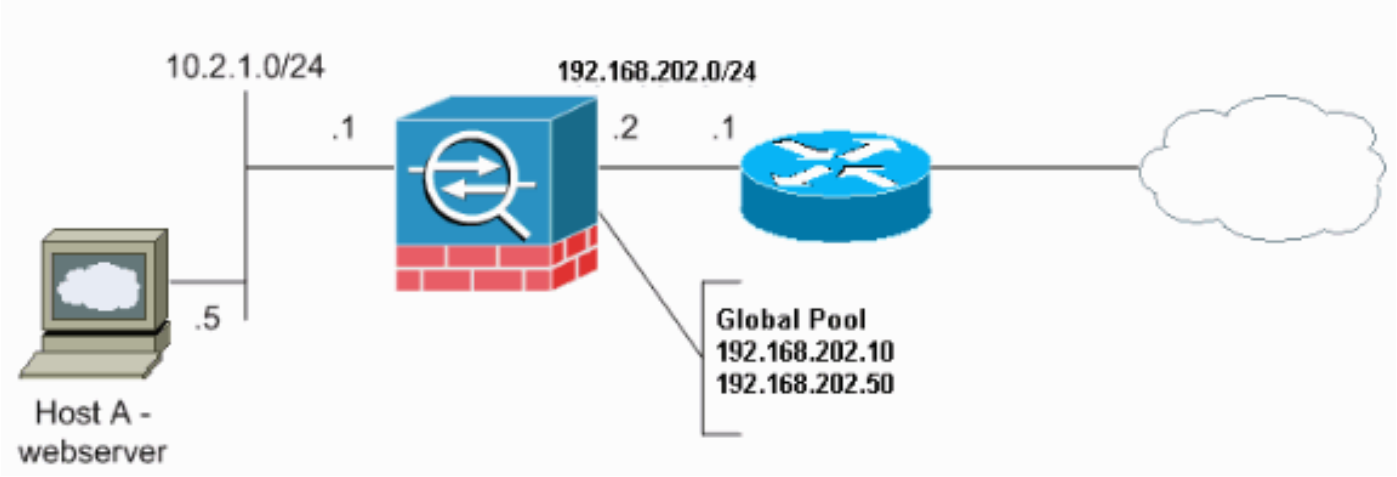
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

ASA를 통한 연결 작동 방식

이 네트워크에서 호스트 A는 내부 주소가 10.2.1.5인 웹 서버입니다. 웹 서버에는 외부(변환된) 주소가 192.168.202.5으로 할당됩니다. 웹 서버에 액세스하려면 인터넷 사용자가 192.168.202.5을 가리켜야 합니다.웹 서버의 DNS 항목은 해당 주소여야 합니다.다른 연결은 인터넷에서 허용되지 않습니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.이는 실습 환경에서 사용된 RFC 1918 주소입니다.

Cisco ASA를 통해 연결 구성

ASA를 통해 연결을 구성하려면 다음 단계를 완료하십시오.

1. 내부 서브넷을 정의하는 네트워크 개체와 IP 풀 범위에 대한 다른 네트워크 개체를 만듭니다.다음 네트워크 객체를 사용하여 NAT를 구성합니다.

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. 인터넷 사용자가 액세스할 수 있는 내부 호스트에 대해 고정 변환 주소를 할당합니다.

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. Cisco ASA를 통해 외부 사용자를 허용하려면 **access-list** 명령을 사용합니다.항상 access-**list** 명령에서 변환된 주소**를** 사용합니다.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

ARP 브로드캐스트 트래픽 허용

보안 어플라이언스는 내부 및 외부 인터페이스에서 동일한 네트워크를 연결합니다.방화벽은 라우팅 홉이 아니므로 기존 네트워크에 투명 방화벽을 쉽게 도입할 수 있습니다.IP 주소 재지정이 필요하지 않습니다.IPv4 트래픽은 액세스 목록 없이 상위 보안 인터페이스에서 하위 보안 인터페이스로 자동 투명 방화벽을 통해 허용됩니다.ARP(Address Resolution Protocols)는 액세스 목록 없이 양방향으로 투명 방화벽을 통과할 수 있습니다.ARP 트래픽은 ARP 검사를 통해 제어할 수 있습니다.낮은 보안 인터페이스에서 높은 보안 인터페이스로 이동하는 레이어 3 트래픽의 경우 확장 액세스 목록이 필요합니다.

참고: 투명 모드 보안 어플라이언스는 CDP(Cisco Discovery Protocol) 패킷 또는 IPv6 패킷 또는 0x600보다 크거나 같은 유효한 EtherType이 없는 패킷을 전달하지 않습니다. 예를 들어, IS-IS 패킷을 전달할 수 없습니다.지원되는 BPDU(Bridge Protocol Data Unit)에 대해서는 예외가 발생했습니다.

허용된 MAC 주소

이러한 대상 MAC 주소는 투명 방화벽을 통해 허용됩니다.이 목록에 없는 MAC 주소는 삭제됩니다.

- FFFF.FFFF.FFFF와 같은 TRUE 브로드캐스트 대상 MAC 주소
- 0100.5E00.0000에서 0100.5EFE.FFFF 사이의 IPv4 멀티캐스트 MAC 주소
- 3333.0000.0000~3333.FFFF.FFFF의 IPv6 멀티캐스트 MAC 주소
- 0100.0CCC.CCCD와 같은 BPDU 멀티캐스트 주소
- 0900.0700.0000~0900.07FF.FFFF의 멀티캐스트 MAC 주소 적용

라우터 모드에서 트래픽을 전달할 수 없음

라우터 모드에서는 일부 유형의 트래픽이 보안 어플라이언스를 통과할 수 없습니다(액세스 목록에서 허용하더라도).그러나 투명 방화벽은 확장 액세스 목록(IP 트래픽용) 또는 EtherType 액세스 목록(비 IP 트래픽용)을 사용하여 거의 모든 트래픽을 허용할 수 있습니다.

예를 들어 투명 방화벽을 통해 라우팅 프로토콜 인접성을 설정할 수 있습니다.확장 액세스 목록을 기반으로 OSPF(Open Shortest Path First), RIP(Routing Information Protocol), EIGRP(Enhanced Interior Gateway Routing Protocol) 또는 BGP(Border Gateway Protocol) 트래픽을 허용할 수 있습니다.마찬가지로 HSRP(Hot Standby Router Protocol) 또는 VRRP(Virtual Router Redundancy Protocol)와 같은 프로토콜은 보안 어플라이언스를 통과할 수 있습니다.

비 IP 트래픽(예: AppleTalk, IPX, BPDU, MPLS)은 이더 타입 액세스 목록을 사용하여 통과하도록 구성할 수 있습니다.

투명 방화벽에서 직접 지원되지 않는 기능의 경우 업스트림 및 다운스트림 라우터가 기능을 지원할 수 있도록 트래픽을 통과하도록 허용할 수 있습니다.예를 들어, 확장 액세스 목록을 사용하면 지원되지 않는 DHCP 릴레이 기능 대신 DHCP(Dynamic Host Configuration Protocol) 트래픽 또는 IP/TV에서 생성한 멀티캐스트 트래픽을 허용할 수 있습니다.

연결 문제 해결

인터넷 사용자가 웹 사이트에 액세스할 수 없는 경우 다음 단계를 완료하십시오.

1. 구성 주소를 올바르게 입력했는지 확인합니다.유효한 외부 주소올바른 내부 주소외부 DNS에 변환된 주소가 있음
2. 외부 인터페이스에서 오류를 확인합니다.Cisco Security Appliance는 인터페이스에서 속도 및 듀플렉스 설정을 자동으로 탐지하도록 미리 구성되어 있습니다.그러나 자동 협상 프로세스가 실패할 수 있는 몇 가지 상황이 있습니다.이로 인해 속도 또는 듀플렉스 불일치(및 성능 문제)가 발생합니다. 미션 크리티컬 네트워크 인프라의 경우, Cisco는 오류 발생 가능성이 없도록 각 인터페이스에서 속도와 듀플렉스를 수동으로 하드코딩합니다.이러한 디바이스는 일반적으로 이동하지 않습니다.따라서 적절히 구성할 경우 변경할 필요가 없습니다.**예:**

   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex full
   asa(config-if)#speed 100
   asa(config-if)#exit
   ```

   경우에 따라 속도 및 이중 설정을 하드 코딩하면 오류가 발생합니다.따라서 다음 예와 같이 인터페이스를 자동 감지 모드의 기본 설정으로 구성해야 합니다.**예:**

   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex auto
   asa(config-if)#speed auto
   asa(config-if)#exit
   ```

3. 트래픽이 ASA 또는 헤드엔드 라우터의 인터페이스를 통해 전송되거나 수신되지 않을 경우, ARP 통계를 지워 보십시오.

   ```
   asa#clear arp
   ```

4. **show run 객체** 및 **show run static** 명령을 사용하여 고정 변환이 활성화되었는지 확인합니다.**예:**

   ```
   object service www
   service tcp source eq www
   object network 192.168.202.2
   host 192.168.202.2
   object network 10.2.1.5
   host 10.2.1.5
   object service 1025
   service tcp source eq 1025
   nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
   ```

   이 시나리오에서는 외부 IP 주소가 웹 서버의 매핑된 IP 주소로 사용됩니다.

   ```
   nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
   ```

5. 웹 서버의 기본 경로가 ASA의 내부 인터페이스를 가리키는지 확인합니다.
6. 변환이 생성되었는지 확인하려면 show xlate 명령을 사용하여 변환 테이블을 확인합니다.

7. 로그 파일을 **검사하여 거부가 발생하는지** 확인하려면 logging buffered 명령을 사용합니다.(변환된 주소를 찾아 거부가 표시되는지 확인합니다.)
8. capture 명령을 사용합니다.

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

참고: 이 명령은 상당한 양의 출력을 생성합니다.트래픽이 많을 때 라우터가 정지되거나 다시 로드될 수 있습니다.

9. 패킷이 ASA에 도달하면 ASA에서 웹 서버에 대한 경로가 올바른지 확인하십시오.(ASA 컨피그레이션에서 **route 명령**을 확인합니다.)
10. 프록시 ARP가 비활성화되었는지 확인합니다.ASA 8.3에서 **show running-config sysopt 명령**을 실행합니다.여기서 프록시 ARP는 sysopt noproxyarp outside 명령**에 의해 비활성화됩니다**.

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

프록시 ARP를 다시 활성화하려면 글로벌 컨피그레이션 모드에서 다음 명령을 입력합니다.

```
ciscoasa(config)#no sysopt noproxyarp outside
```

호스트가 동일한 이더넷 네트워크의 다른 디바이스로 IP 트래픽을 전송할 경우, 호스트는 디바이스의 MAC 주소를 알아야 합니다.ARP는 MAC 주소로 IP 주소를 확인하는 레이어 2 프로토콜입니다.호스트가 ARP 요청을 전송하고 "이 IP 주소는 누구입니까?"라고 묻습니다. IP 주소를 소유하는 디바이스는 "I own that IP address;여기 내 MAC 주소가 있다."프록시 ARP를 사용하면 보안 어플라이언스가 뒤에 있는 호스트를 대신하여 ARP 요청에 응답할 수 있습니다.이렇게 하려면 해당 호스트의 정적 매핑된 주소에 대한 ARP 요청에 응답합니다.보안 어플라이언스는 고유한 MAC 주소로 요청에 응답한 다음 IP 패킷을 적절한 내부 호스트로 전달합니다.예를 들어 이 문서의 다이어그램에서 웹 서버의 전역 IP 주소 192.168.202.5에 대해 ARP 요청을 하면 보안 어플라이언스는 자체 MAC 주소로 응답합니다.이 상황에서 프록시 ARP가 활성화되지 않은 경우 보안 어플라이언스의 외부 네트워크에 있는 호스트는 주소 192.168.202.5에 대한 ARP 요청을 실행하여 웹 서버에 연결할 수 없습니다. sysopt 명령에 대한 자세한 내용은 명령 참조를 참조하십시오.
11. 모든 것이 올바르게 표시되고 사용자가 여전히 웹 서버에 액세스할 수 없는 경우 Cisco 기술 지원을 통해 케이스를 여십시오.

오류 메시지 - %ASA-4-407001:

일부 호스트가 인터넷에 연결할 수 없으며 `- %ASA-4-407001:local-host interface_name:inside_address . syslog` 오류 메시지가 수신됩니다.이 오류는 어떻게 해결됩니까?

사용자 수가 사용된 라이센스의 사용자 제한을 초과하면 이 오류 메시지가 표시됩니다.이 오류를 해결하려면 라이센스를 더 많은 수의 사용자로 업그레이드하십시오.필요한 경우 50, 100 또는 무제한 사용자 라이센스가 가능합니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- 보안 제품 필드 알림(Cisco ASA(Adaptive Security Appliance) 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems