ASA 8.4(4): 특정 ID NAT 컨피그레이션이 허용되지 않음

목차

소개

8.4(4) 이상을 실행하는 ASA(Adaptive Security Appliances)는 특정 NAT 컨피그레이션을 거부하고 다음과 유사한 오류 메시지를 표시할 수 있습니다.

```
ERROR: <mapped address range> overlaps with <interface> standby interface
   address
ERROR: NAT Policy is not downloaded
```

이전 릴리스에서 ASA를 8.4(4) 이상으로 업그레이드할 때도 이 문제가 나타날 수 있습니다. 일부 NAT 명령이 더 이상 ASA의 running-config에 없는 것을 알 수 있습니다. 이러한 경우 위의 형식으로 메시지가 있는지 확인하기 위해 인쇄된 콘솔 메시지를 확인해야 합니다.

ASA 뒤에 있는 특정 서브넷에 대한 트래픽이 ASA에서 종료되는 VPN(Virtual Private Network) 터널을 통해 전달되지 않을 수 있다는 점도 알 수 있습니다. 이 문서에서는 이러한 문제를 해결하는 방법에 대해 설명합니다.

시작하기 전에

요구 사항

이 문제를 해결하려면 다음 조건을 충족해야 합니다.

- 이전 릴리스에서 버전 8.4(4) 이상을 실행하거나 버전 8.4(4) 이상으로 업그레이드했습니다.
- 하나 이상의 인터페이스에 대기 IP 주소를 사용하여 구성된 ASA입니다.
- NAT는 위 인터페이스로 매핑된 인터페이스로 구성됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- 8.4(4) 이상을 실행하는 ASA

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

문제

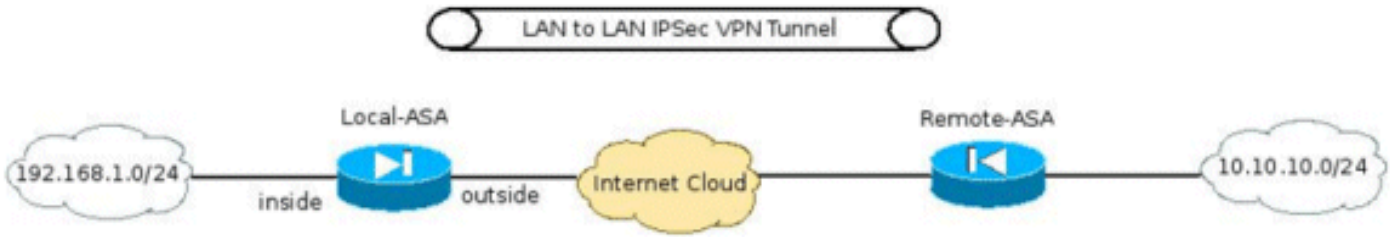
오류 메시지가 보여주는 것처럼 고정 NAT 문의 매핑된 주소 범위에 매핑된 인터페이스에 할당된 "standby" IP 주소가 포함되어 있으면 NAT 명령이 거부됩니다. 이 동작은 항상 정적 포트 리디렉션에 사용되었지만, Static one-to-one NAT 문과 Cisco 버그 ID CSCtw82147의 수정으로 버전 8.4(4)에 대해 도입되었습니다(등록된 고객만 해당).

8.4(4) 이전의 ASA에서는 사용자가 매핑된 인터페이스에 할당된 대기 IP 주소와 동일하게 고정 NAT 컨피그레이션에서 매핑된 주소를 구성할 수 있도록 허용했기 때문에 이 버그가 발생했습니다. 예를 들어, ASA의 컨피그레이션 조각을 살펴보십시오.

```
ciscoasa(config)# show run int e0/0
!
interface Ethernet0/0
 nameif vm
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config)# show run nat
!
object network obj-10.76.76.160
 nat (tftp,vm) static 192.168.1.2
```

명령이 승인되더라도 이 NAT 컨피그레이션은 설계에서 작동하지 않습니다. 따라서 8.4(4)부터 ASA는 이러한 NAT 규칙을 처음부터 구성할 수 없습니다.

이로 인해 또 다른 예기치 못한 문제가 발생했습니다. 예를 들어, 사용자가 ASA에서 종료되는 VPN 터널을 가지고 "내부" 서브넷이 원격 VPN 서브넷과 통신할 수 있도록 허용하려는 시나리오를 가정해보겠습니다.



VPN 터널을 구성하는 데 필요한 다른 명령 중 가장 중요한 구성 중 하나는 VPN 서브넷 간의 트래픽이 NATed가 되지 않도록 하는 것입니다. 이는 다음 형식의 Manual/Twice NAT 명령을 사용하여 8.3 이상에서 구현됩니다.

```
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
```

```
object network obj-192.168.1.0
 description Inside subnet
 subnet 192.168.1.0 255.255.255.0
object network obj-10.10.10.0
 description Remote VPN subnet
 subnet 10.10.10.0 255.255.255.0
!
nat (inside,any) source static obj-192.168.1.0 obj-192.168.1.0 destination
   static obj-10.10.10.0 obj-10.10.10.0
!
object network obj-192.168.1.0
 nat (inside,outside) dynamic interface
```

이 ASA가 8.4(4) 이상으로 업그레이드되면 이 NAT 명령이 ASA의 running-config에 표시되지 않으며 이 오류는 ASA의 콘솔에 인쇄됩니다.

```
ERROR: 192.168.1.0-192.168.1.255 overlaps with inside standby interface
   address
ERROR: NAT Policy is not downloaded
```

따라서 서브넷 192.168.1.0/24과 10.10.10.0/24 간의 트래픽은 더 이상 VPN 터널을 통해 전달되지 않습니다.

솔루션

이 조건에 대한 해결 방법은 두 가지가 있습니다.

- 매핑된 인터페이스가 "any"가 되도록 8.4(4)로 업그레이드하기 전에 NAT 명령을 최대한 구체적으로 지정합니다. 예를 들어 위의 NAT 명령을 원격 VPN 서브넷에 연결할 수 있는 인터페이스로 변경할 수 있습니다(위의 시나리오에서 "outside"라는 이름).
  ```
  nat (inside,outside) source static obj-192.168.1.0 obj-192.168.1.0 destination
     static obj-10.10.10.0 obj-10.10.10.0
  ```
- 위의 해결 방법이 불가능한 경우 다음 단계를 완료합니다.ASA가 8.4(4) 이상을 실행하는 경우 인터페이스에 할당된 대기 IP 주소를 제거합니다.NAT 명령을 적용합니다.인터페이스에서 대기 IP 주소를 다시 적용합니다.예를 들면 다음과 같습니다.
  ```
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
  ciscoasa(config-if)# exit
  ciscoasa(config)# nat (inside,any) 1 source static obj-192.168.1.0
     obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  ```

관련 정보

- 기술 지원 및 문서 – Cisco Systems