패치할 수 없는 트래픽을 사용하는 동적 NAT의 예기치 않은 동작

목차

소개

이 문서에서는 IOS® 디바이스에서 Non-Pattable 트래픽이 있는 동적 NAT(Network Address Translation)의 예기치 않은 동작에 대해 설명합니다.

문제

Non-Pattable 트래픽은 동적 NAT의 경우 NAT 변환 테이블에 1/2 엔트리를 생성합니다. 이러한 항목은 외부-내부 트래픽에 대해 작동하므로 보안 위험으로 작용합니다.

NAT 구성:

<#root>

```
ip nat pool ATT_FIBER 10.10.10.1 10.10.10.6 netmask  255.255.255.248
ip nat inside source list GUEST_SUBNET pool ATT_FIBER overload
ip nat inside source list OFFICE_SUBNETS pool ATT_FIBER overload

ip access-list extended OFFICE_SUBNETS
 deny   ip 172.16.26.0 0.0.0.127 any
 permit ip 172.16.8.0 0.0.1.255 any

ip access-list extended GUEST_SUBNET
 permit ip 172.16.26.0 0.0.0.127 any

udp 10.10.10.1:49370    172.16.9.9:49370      192.168.1.1:53      192.168.1.1:53
udp 10.10.10.1:49535    172.16.9.9:49535      192.168.2.2:53    192.168.2.2:53
tcp 10.10.10.1:53133    172.16.9.9:53133      192.168.3.3:80     192.168.3.3:80
tcp 10.10.10.1:56311    172.16.9.9:56311      192.168.4.4:5816    192.168.4.4:5816

--- 10.10.10.1         172.16.9.9            ---                  ---
```

내부 -> 외부 매핑이 있거나 패킷이 내부 -> 외부에서 시작된 경우 중간 항목이 생성됩니다.

라우터가 NAT 오버로드(PAT(Port Address Translation))에 대해 구성되어 있고 비 패치 트래픽이 라우터에 도달하면 이 트래픽에 대해 비 패치 바인딩 항목이 생성됩니다. 이는 NAT 테이블에서 다

음과 같은 종류의 항목으로 이어집니다.

```
--- 10.10.10.1        172.16.9.9            ---                   ---
```

이 바인드 엔트리는 풀의 전체 주소를 소비합니다. 이 예에서 10.10.10.1은 오버로드된 풀의 주소입니다.

즉, 내부 로컬 IP 주소가 고정 NAT와 유사한 외부 전역 IP에 바인딩됩니다. 따라서 현재 항목의 시간이 초과될 때까지 새로운 내부 로컬 IP 주소에서 이 전역 IP 주소를 사용할 수 없습니다. 이 바인딩에 대해 생성된 모든 변환은 오버로드가 아닌 1:1 변환입니다.

솔루션

이 문제를 해결하려면 동적 NAT와 함께 경로 맵을 사용할 수 있습니다. 경로 맵에서는 NAT가 하프 엔트리를 생성하거나 풀 오버로드 대신 인터페이스 오버로드를 사용하지 않습니다. 패치 불가능한 바인딩은 인터페이스 오버로드의 경우 생성되지 않습니다.

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.