ASA에 구성된 시간 초과보다 긴 유휴 값을 가진 xlate 항목이 있는 이유는 무엇입니까?

목차

소개

이 문서에서는 유휴 값이 있는 xlate 항목이 구성된 시간 제한보다 긴 이유를 설명합니다. 또한 conn 및 xlate 값의 상관관계를 파악하고 확인하는 방법에 대한 정보도 제공합니다.

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

Q. ASA(Adaptive Security Appliance)에 구성된 시간 초과보다 긴 유휴 값을 가진 xlate 항목이 있는 이유는 무엇입니까?

A. 다음은 구성된 시간 제한보다 긴 유휴 값을 가진 xlate 항목을 보여주는 예입니다.

```
<#root>

ASA#

show xlate

26 in use, 16665 most used
Flags: D - DNS, e - extended, I - identity,
   I - dynamic, r - portmap, s - static,
   T - twice, N - net-to-net
TCP PAT from inside:10.20.33.2/54676 to outside:
   192.0.2.3/54676 flags ri idle 1:48:12
   timeout 0:00:30
TCP PAT from inside:10.20.33.2/54397 to outside:
   192.0.2.3/54397 flags ri idle 2:03:59
   timeout 0:00:30
TCP PAT from inside:10.20.33.2/54369 to outside:
   192.0.2.3/54369 flags ri idle 2:04:26
   timeout 0:00:30
TCP PAT from inside:10.20.33.3/56695 to outside:
   192.0.2.3/56695 flags ri idle 0:09:22
   timeout 0:00:30
TCP PAT from inside:10.20.33.3/55880 to outside:
   192.0.2.3/55880 flags ri idle 0:33:12
   timeout 0:00:30
TCP PAT from inside:10.20.33.3/54431 to outside:
   192.0.2.3/54431 flags ri idle 2:03:23
```

```
   timeout 0:00:30
```

연결이 ASA에서 변환(xlate)을 받는 경우 먼저 변환이 작성되고 연결이 작성되며, 마지막으로 연결이 해당 변환과 연결됩니다. xlate 유휴 시간 제한은 해당 xlate에 대한 모든 연결된 연결이 종료될 때만 시작됩니다.

show xlate 및 show conn의 출력의 상관관계를 파악하면 conn 값이 구성된 시간 초과보다 오랫동안 유휴 상태인 xlate 값과 매칭하는 것을 확인할 수 있습니다. 이제 DDoS 공격의 실제 사례를 살펴보겠습니다.

PAT(Port Address Translation) show xlate 명령을 입력합니다.

```
<#root>

ASA#

show xlate local port 54676


TCP PAT from inside:10.20.33.2/54676 to outside:192.0.2.3/54676 flags ri
   idle 1:48:12 timeout 0:00:30
```

그런 다음 show conn 명령에서 포트를 지정하여 연결된 연결 항목을 찾습니다.

```
<#root>

ASA#

show conn port 54676

TCP outside 192.168.22.3:443 events inside:10.20.33.2:54676, idle 0:03:52,
   bytes 1807, flags UIO
```

이 연결은 변환과 연결됩니다. 로컬 포트 54676은 연결 및 변환 항목 모두에 대해 동일합니다. 이 TCP 연결은 프로토콜(TCP FIN 또는 재설정 패킷)에 의해 닫힐 때까지 또는 ASA에 의해 시간 초과될 때까지(기본 시간 제한 1시간 이후) 존재합니다. 연결이 끊기면 변환도 삭제되지만 이 삭제는 "시간 초과"초 동안 지연됩니다.

관련 정보

- Cisco ASA 5500 Series Next Generation Firewall
- 기술 지원 및 문서 – Cisco Systems

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.