Umbrella 구성 요소에서 포트 주소 변환을 사용할 때 포트 소모 문제 해결

목차

소개

이 문서에서는 로밍 클라이언트 및/또는 가상 어플라이언스를 사용하는 Umbrella 고객이 포트 주소 변환을 사용하는 방화벽에서 포트 소진 문제를 겪는 것에 대해 설명합니다. 이 문제는 로밍 클라이언트 수가 많거나 VA를 통해 실행되는 트래픽 양이 많은 환경에서 발생할 수 있습니다. 증상으로는 느리게 반환되거나 시간 초과되는 DNS 쿼리가 포함될 수 있습니다.

원인

로밍 클라이언트와 가상 어플라이언스 모두 DNS 쿼리에 대한 응답을 캐시하지 않습니다. 또한 로밍 클라이언트는 네트워크 환경을 분석하고 상태를 확인하기 위해 자주 "프로브" DNS 요청을 보냅니다.

권장 사항

- Umbrella 대시보드의 Domain Management(도메인 관리) 내에서 내부 도메인이 올바르게 구성되어 있는지 확인합니다. 이러한 쿼리는 Active Directory 영역(및/또는 기타 내부 영역)을 포함해야 빈도가 높은 쿼리의 볼륨을 줄일 수 있습니다.
- 방화벽에서 일부 PAT 설정을 검토합니다.
  - 긴 UDP 세션 시간 초과가 문제가 될 수 있습니다. 일반적으로 UDP 세션 시간 제한은 약 15초로 설정하는 것이 좋습니다. 그러나 네트워크의 다른 애플리케이션에서 UDP를 많이 사용하는 경우, 반드시 고려해야 할 시간 초과가 더 길어질 수 있습니다.
  - 방화벽에 따라 동시 연결 수를 늘리기 위해 PAT 풀의 크기를 늘릴 수 있습니다.
- VA 전용으로 지정할 수 있는 IP 주소가 있는 경우 방화벽에서 PAT 대신 1:1 NAT를 사용합니다. 참고: "1:1 NAT"는 "직접 NAT"라고도 하지만, 잘못된 이름입니다. 올바른 기술 용어는 "1:1 NAT"입니다.
- IP별 연결 제한을 검토합니다. 해당 디바이스에 적용되지 않을 것으로 예상되는 정책이 실제로 제한을 적용하는 경우가 많습니다. 확인 방법은 다음 섹션을 참조하십시오.

ASA에서 IP별 연결 제한 확인

다음 단계를 따르십시오.

- 패킷이 방화벽에 의해 삭제된 이유를 보려면 캡처로 ASA를 구성합니다.

```
capture asp type asp-drop all match ip any host 208.67.222.222
```

- 문제의 IP에 대해 삭제되는 패킷을 확인합니다. 연결 제한 사유는 "Drop-reason: (conn-limit)"
- 다음 명령을 사용하여 호스트 연결 제한을 검사합니다.

```
show local-host detail | begin <IP Address of VA or roaming client>
```

  - 이 수는 일정한 한도(즉, 999)에서 정적이고 절대 증가하지 않습니까? 연결 제한이 있는 경우 연결 제한을 나타냅니다.
- 이를 적용할 서비스 정책을 확인합니다. 찾을 경우 policy-map을 확인합니다.

```
show run service-policy, show policy-map NAME
```

  - 호스트별 연결 제한을 1000으로 설정하는 정책 맵 "NAME"이 있는 경우(예:), 이렇게 하면 더 많은 연결을 사용할 수 있을 때까지 디바이스의 모든 새 DNS 패킷이 삭제됩니다. UDP는 스테이트리스(stateless)이며 재시도하지 않습니다.
- 문제를 해결하려면 해당 service-policy를 제거합니다(서비스 정책 이름 없음). 연결은 1K 제한을 초과해야 합니다(이 예에서). 이는 로밍 클라이언트보다 VA에서 더 빠르게 발생합니다.

추가 권장 사항

이러한 권장 사항이 도움이 되지 않을 경우 가능한 해결 방법은 다음과 같습니다.

1. Umbrella 대시보드 —> 보고 —> 상위 대상 보고서를 사용하여 최근 24시간 내에 요청이 많은 하나 이상의 도메인을 식별할 수 있습니다.
2. Umbrella 대시보드 —> 구성 —> 도메인 관리에서 하나 이상의 고용량 도메인을 목록에 추가하고 "적용 대상"을 "모든 어플라이언스 및 디바이스"로 설정합니다.
3. 그런 다음 해당 도메인에 대한 쿼리는 VA에 의해 로컬 DNS로 전달됩니다. 이상적으로 로컬 DNS는 208.67.220.220/208.67.222.222의 Umbrella DNS로 전달하도록 구성해야 하지만, 외부 DNS로 전달하도록 구성할 수도 있습니다.
4. 로컬 DNS는 권한 있는 도메인에 대한 쿼리를 처리합니다.
5. 로컬 DNS가 로컬이 아닌 도메인에 대한 쿼리를 수락한다고 가정할 경우, 다른 도메인에 대한 쿼리는 외부 DNS로 전달됩니다.

로컬 DNS는 DNS 결과를 캐시할 수 있지만 로밍 클라이언트 및 가상 어플라이언스는 캐시하지 않기 때문입니다. 이 해결 방법을 사용하면 내부 DNS에 더 많은 트래픽과 로드가 발생하므로 과부하가 발생하지 않도록 신중하게 모니터링하십시오.

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.