특정 사이트를 검색할 때 502/504 GATEWAY_TIMEOUT 오류 발생

목차

질문:

질문:

특정 사이트를 검색할 때 502/504 GATEWAY_TIMEOUT 오류가 발생하는 이유는 무엇입니까?

증상:사용자가 특정 웹 사이트를 탐색할 때 Cisco WSA에서 502 또는 504 게이트웨이 시간 초과 오류를 수신함

사용자가 웹 사이트를 탐색할 때 502 또는 504 게이트웨이 시간 초과 오류를 수신합니다.액세스 로그에 'NONE/504' 또는 'NONE/502'가 표시됩니다.

샘플 액세스 로그 라인:

123658928.496 153185 10.10.70.50 **NONE/504** 1729 GET http://www.example.com/ - DIRECT/www.example.com - .....

WSA에서 502 또는 504 게이트웨이 시간 초과 오류를 반환할 수 있는 이유는 여러 가지가 있습니다.이러한 오류 응답은 비슷하지만 그 사이의 미묘한 차이를 이해하는 것이 중요합니다.

다음은 발생할 수 있는 시나리오 유형의 몇 가지 예입니다.

- 502:WSA에서 웹 서버와의 TCP 연결을 설정하려고 했지만 SYN/ACK를 수신하지 못했습니다.
- 504:WSA에서 웹 서버와의 연결을 종료하는 TCP 재설정(RST)을 수신합니다.
- 504:WSA가 웹 서버와 통신하기 전에 필요한 서비스로부터 응답을 받지 못하고 있습니다(예: DNS 실패).
- 504:WSA는 웹 서버와의 TCP 연결을 설정하고 GET 요청을 전송했지만 WSA는 HTTP 응답을 수신하지 않습니다.

다음은 각 시나리오의 예와 잠재적 문제에 대한 자세한 정보입니다.

502:WSA에서 웹 서버와의 TCP 연결을 설정하려고 했지만 SYN/ACK를 수신하지 못했습니다.
웹 서버가 WSA의 SYN 패킷에 응답하지 않을 경우, 일정 횟수의 시도 후 클라이언트가 502 게이트웨이 시간 초과 오류를 보냅니다. 이에 대한 일반적인 원인은 다음과 같습니다. 1. 웹 서버 또는 웹 서버 네트워크에 문제가 있습니다. 2. WSA 네트워크의 네트워크 문제로 인해 SYN 패킷이 인터넷에 연결되지 않습니다.

3. 방화벽 또는 유사한 디바이스에서 WSA SYN 패킷 또는 웹 서버의 SYN/ACK를 삭제합니다.
4. WSA에서 IP 스푸핑을 사용하도록 설정했지만 올바르게 구성되지 않았습니다(반환 경로 리디렉션 없음).

문제 해결 단계:

첫 번째 단계는 WSA에서 웹 서버에 ICMP를 ping할 수 있는지 확인하는 것입니다.이 작업은 다음 CLI 명령을 사용하여 수행할 수 있습니다.
WSA> *ping* www.example.com
Ping에 실패하면 서버가 다운된 것은 아닙니다.이는 ICMP 패킷이 경로의 어딘가에서 차단된다는 의미일 수 있습니다.ping이 성공하면 WSA에 웹 서버에 대한 기본 레이어3 수준의 연결이 있는지 확인할 수 있습니다.
텔넷 테스트는 WSA가 포트 80에서 웹 서버에 대한 TCP 연결을 설정할 수 있는지 확인합니다.텔넷 테스트를 수행하려면 이 문서의 추가 지침을 참조하십시오.

네트워크 문제 또는 방화벽 블록
ping에 성공했지만 텔넷에 실패하면 방화벽 같은 필터링 디바이스에서 이 트래픽이 네트워크를 통과하지 못할 가능성이 높습니다.자세한 내용은 방화벽의 로그 및/또는 패킷 캡처를 분석하는 것이 좋습니다.
IP 스푸핑은 활성화되지만 올바르게 구성되지 않음
WSA를 통해 명시적으로 프록시하거나 텔넷 테스트가 성공한 경우 WSA가 웹 서버와 직접 통신할 수 있음을 보여주지만, IP 스푸핑으로 WSA를 통해 클라이언트 프록시가 프록시되면 문제가 발생합니다.

클라이언트 IP 스푸핑이 없는 경우:
- WSA는 자체 IP 주소를 소스로 사용하여 웹 서버에 SYN을 전송합니다.패킷이 돌아오면 WSA로 직접 이동합니다.

클라이언트 IP 스푸핑 사용:
- WSA는 SYN을 전송하지만 대신 클라이언트의 IP를 소스로 사용합니다.특별한 네트워크 설정이 없으면 반환 패킷이 WSA 대신 클라이언트로 전송됩니다.
- 클라이언트 IP 스푸핑을 사용하려면 패킷이 제대로 리디렉션되도록 네트워크를 매우 구체적인 방법으로 구성해야 합니다.웹 서버가 반환 경로 패킷을 WSA 대신 클라이언트로 보내는 경우 WSA는 서버 SYN/ACK를 표시하지 않으며 클라이언트에 다시 502 게이트웨이 시간 초과 오류를 보냅니다.

504:WSA에서 웹 서버와의 연결을 종료하는 TCP 재설정(RST)을 수신합니다.

WSA가 웹 서버에 대한 업스트림 연결에서 TCP 재설정 패킷을 수신하면 WSA는 클라이언트에 504 게이트웨이 시간 초과 오류를 보냅니다.

이에 대한 일반적인 원인은 다음과 같습니다.
1. Cisco Layer 4 Traffic Monitor(L4TM)가 WSA 프록시가 웹 서버 연결을 차단하고 있습니다.
2. 방화벽, IDS, IPS 또는 기타 패킷 검사 디바이스에서 WSA를 차단하고 있습니다.

문제 해결 단계:
먼저 TCP RST가 L4TM 또는 다른 디바이스에서 오는지 확인합니다.
L4TM이 이 트래픽을 차단하면 트래픽이 GUI 보고서에 "***Monitor -> L4 Traffic Monitor(모니터 -> L4 트래픽 모니터)***" 아래에 표시됩니다. 그렇지 않으면 RST가 다른 디바이스에서 오고 있습니다.
L4TM 차단:
L4TM이 차단되는 경우 WSA 프록시도 실행 중인 포트에서 차단하지 않는 것이 좋습니다.여기에는

여러 가지 이유가 있습니다.
1. WSA 프록시는 TCP만 연결을 재설정하는 대신 문제가 발생할 경우 오류 메시지를 제공합니다.이렇게 하면 최종 사용자가 차단될 때 혼동을 제한할 수 있습니다.
2. WSA 프록시는 특정 콘텐츠를 스캔 및 차단하는 기능을 제공하는 반면 L4TM은 블랙리스트 IP 주소와 일치하는 모든 트래픽을 차단합니다.
L4TM이 프록시 포트에서 차단되지 않도록 구성하려면 "*GUI -> Security Services -> L4 Traffic Monitor*"로 이동하십시오.
사이트가 악성으로 알려진 웹 사이트이지만 트래픽을 허용해야 하는 이유가 있는 경우 다음 사이트에 화이트리스트를 표시할 수 있습니다.
"*GUI -> Web Security Manager -> L4 Traffic Monitor -> Allow List(허용 목록)*"

방화벽/IDS/IPS 차단:
네트워킹의 다른 디바이스에서 WSA가 웹 서버에 연결되지 못하도록 차단하는 경우 다음을 분석하는 것이 좋습니다.
1. 방화벽 블록 로그
2. 문제 중 인그레스/이그레스 패킷 캡처

차단 로그는 디바이스가 WSA를 차단하고 있는지 신속하게 확인할 수 있습니다.방화벽, IPS 또는 IDS는 트래픽을 차단하며 적절하게 로깅하지 않는 경우가 있습니다.이 경우 TCP RST가 어디에서 오는지 확인할 수 있는 유일한 방법은 디바이스에서 인그레스 및 이그레스 캡처를 얻는 것입니다.RST가 인그레스(ingress) 인터페이스에서 전송되고 이그레스(egress) 면을 통과하는 패킷이 없는 경우, 보안 디바이스가 원인입니다.

504:WSA는 웹 서버와의 TCP 연결을 설정하고 GET 요청을 전송했지만 WSA는 HTTP 응답을 수신하지 않습니다.

WSA가 HTTP GET을 전송하지만 응답을 수신하지 않는 경우, 클라이언트에 504 게이트웨이 시간 초과 오류를 보냅니다.

이에 대한 일반적인 원인은 다음과 같습니다.

- 방화벽, IDS, IPS 또는 기타 패킷 검사 디바이스는 TCP 연결을 허용하지만 HTTP 콘텐츠가 웹 서버에 도달하는 것을 차단합니다.이 경우 텔넷 테스트를 통해 차단되는 HTTP 데이터의 종류를 파악할 수 있습니다.

방화벽 블록 로그는 디바이스가 WSA를 차단하는 이유를 빠르게 확인할 수 있습니다.방화벽, IPS 또는 IDS는 트래픽을 차단하며 적절하게 로깅하지 않는 경우가 있습니다.이 경우 TCP RST가 어디에서 오는지 확인할 수 있는 유일한 방법은 디바이스에서 인그레스 및 이그레스 캡처를 얻는 것입니다.RST가 인그레스(ingress) 인터페이스에서 전송되고 이그레스(egress) 면을 통과하는 패킷이 없는 경우, 보안 디바이스가 원인입니다.

텔넷을 사용하여 웹 서버와의 연결 테스트

WSA CLI에서 telnet 명령을 **실행합니다**.

WSA> **텔넷**
텔넷할 인터페이스를 선택하십시오.
1. 자동
2. 관리(192.168.15.200/24)wsa.hostname.com)
3. P1(192.168.113.199/24)data.com)
[1]> **3**

원격 호스트 이름 또는 IP 주소를 입력합니다.
[]> www.example.com

원격 포트를 입력합니다.
[25]> **80**

10.3.2.99...
www.example.com에 연결됨..
이스케이프 문자는 '^]'입니다.

메모:"Connected(연결됨)" 메시지는 WSA와 웹 서버 간에 TCP가 성공적으로 설정되었음을 나타냅니다.

HTTP 요청은 이 텔넷 세션을 통해 수동으로 전송할 수도 있습니다.다음은 "Connected" 메시지 뒤에 입력할 수 있는 샘플 요청입니다.
—
http://www.example.com 다운로드 HTTP/1.1
호스트: www.example.com
{Enter}
—

참고:끝에 추가 캐리지 리턴을 추가해야 합니다. 그렇지 않으면 서버가 요청에 응답하지 않습니다.