WCCP를 사용하여 경로 MTU 검색에 대한 WSA 동작

목차

소개

이 문서에서는 컨피그레이션에 WCCP(Web Cache Communication Protocol) 및 MTU(Path Maximum Transmission Unit) 검색이 모두 포함되어 있을 때 라우터가 패킷을 삭제하는 문제에 대해 설명하고, 문제를 해결할 수 있는 솔루션을 제공합니다.

배경 정보

사전 단계

별도로 살펴보면 많은 기능이 특정 문제를 처리할 수 있습니다.그러나 두 가지 또는 세 가지 기술을 결합하면 다소 어색한 동작이 발생하고 제대로 작동하려면 다른 기능이나 해결 방법을 도입해야 합니다.예를 들어 스패닝 트리 및 OSPF(Open Shortest Path First) 및 L2(Layer 2) 컨버전스는 OSPF보다 더 오래(20s) 소요되지만(최소 데드 간격이 사용되는 경우 1초) 스패닝 트리를 MST(Multiple Spanning-Tree)로 대체하고 다시 정상적으로 작동합니다.

WCCP와 경로 MTU 검색 간에 동일한 상호 운용성 동작이 관찰되었습니다.많은 사람들은 이것이 GRE(Generic Routing Encapsulation) 헤더 문제라고 생각합니다.그러나 이 문서에서는 실제 원인을 설명합니다.

경로 MTU 검색 및 WCCP가 개별적으로 작동하는 방식

경로 MTU 검색

각 라인에는 패킷의 크기에 대한 제한이 있습니다.지원되는 것보다 큰 패킷을 전송하면 해당 패킷이 삭제됩니다.L3 디바이스(라우터)의 역할 중 하나는 각 라인의 기능에 대한 엔드 투 엔드 통신이 투명하게 이루어지도록 한 라인에서 큰 패킷을 다른 라인으로 나누어 처리하는 것입니다.

그러나 경우에 따라 엔드 호스트는 패킷이 분할될 수 없도록 구성됩니다(예: 암호화된 파일, 음성 통화). 이 정보는 IP 헤더 내의 DF(Don't Fragment) 비트를 통해 전달됩니다.라우터는 이와 같은 패킷을 삭제하지만 라우터는 ICMP(Internet Control Message Protocol) 메시지(type 3-Destination unreachable, code 4 - fragmentation needed, DF bit set)를 통해 최종 호스트에 보고하려고 시도합니다. 이렇게 하면 호스트는 향후 더 작은 패킷을 전송해야 한다는 것을 알고 있습니다.

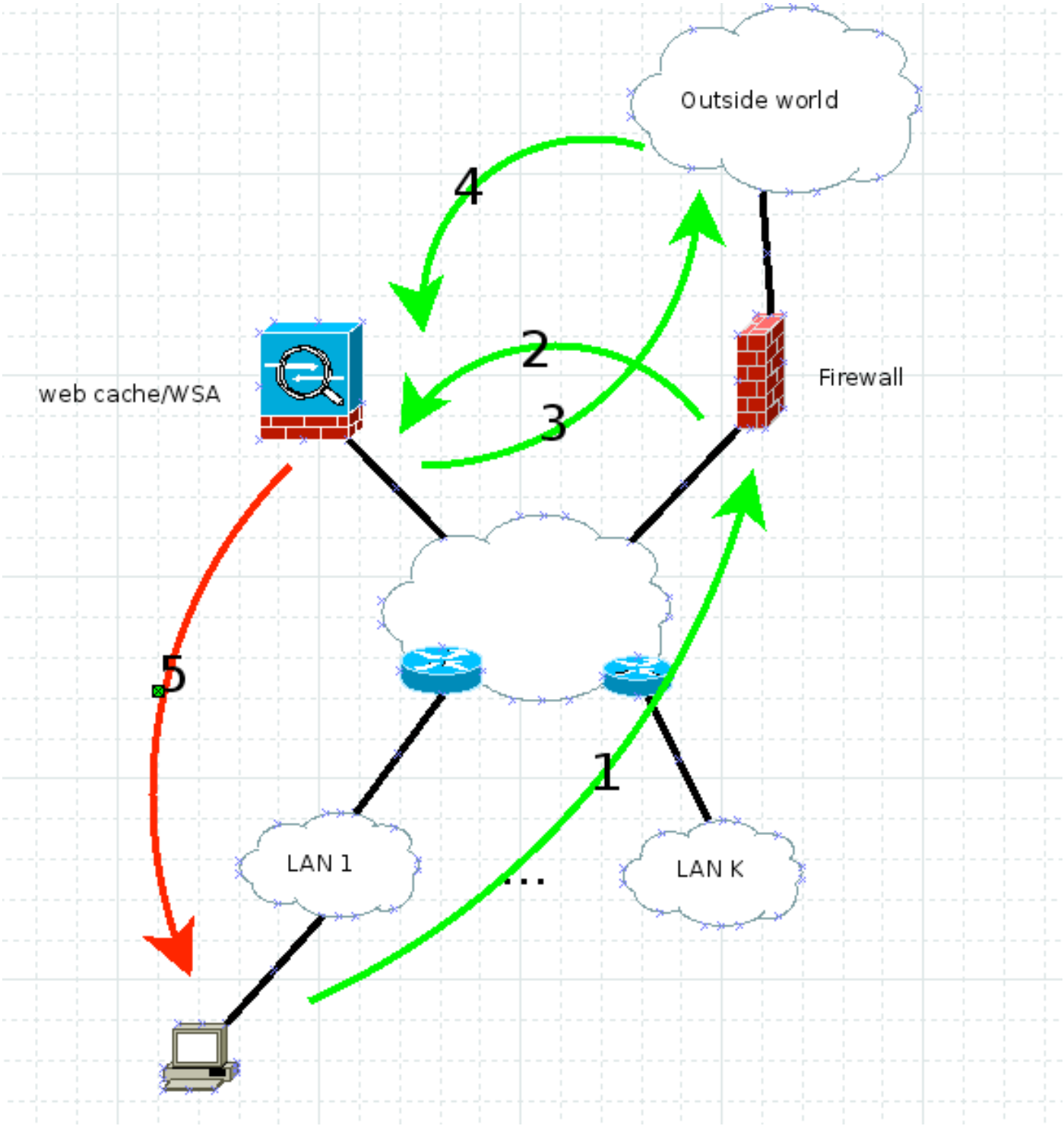
이것은 경로 MTU 검색의 핵심입니다.DF 비트가 설정된 대용량 패킷을 전송하여 해당 패킷이 끝을 향해 오는지 또는 이전에 설명한 대로 ICMP 보고서를 받는지 확인할 수 있습니다.실행 가능한 최대 패킷 크기를 결정하면 추가 통신에 사용합니다.자세한 내용은 RFC 1191을 참조하십시오.

WSA(Web Security Appliance)는 기본적으로 경로 MTU 검색을 사용합니다.따라서 생성된 모든 패킷에는 기본 컨피그레이션에 의해 DF 비트가 설정됩니다.

WCCP

다른 사람의 지식 없이 웹 트래픽에서 네트워크에 보안을 적용해야 하는 경우 표시되지 않는 프록시를 통해 트래픽을 실행합니다.WCCP는 인터셉트하는 디바이스(라우터/방화벽)와 웹 캐시 엔진/프록시(이 경우 WSA임) 간의 통신에 사용되는 프로토콜입니다.

다음 다이어그램은 이 시나리오의 트래픽 플로우를 보여줍니다.



다음과 같이 작동합니다.

1. 클라이언트는 IP 소스, 해당 IP 주소(클라이언트 IP 주소) 및 대상 서버 IP 주소로 HTTP GET을 전송합니다.

2. 방화벽 또는 라우터는 HTTP GET을 인터셉트하고 WCCP GRE 또는 순수 L2를 통해 웹 캐시/WSA로 전달합니다.소스는 여전히 클라이언트 IP 주소이며 대상은 여전히 웹 서버 IP 주소입니다.

3. WSA는 요청을 검사하고 합법적인 경우 웹 서버로 미러링합니다.여기서 대상 IP 주소는 웹 서버 IP 주소이고 소스 IP 주소는 클라이언트 IP 주소 스푸핑을 활성화했는지 여부에 따라 WSA 또는 클라이언트일 수 있습니다.이 예에서는 두 경우 모두 반환 트래픽이 WSA에 도달해야 하므로 문제가 되지 않습니다.

4. 반환 트래픽은 WSA에서 검사됩니다.

5. WSA는 소스 IP 주소, 항상 웹 서버 IP 주소(클라이언트가 의심되지 않도록), 대상 클라이언트 IP 주소를 사용하여 클라이언트에 응답을 보냅니다.

문제

다이어그램의 라우터 중 하나가 트래픽을 프래그먼트화하면 어떻게 됩니까?WSA는 패킷 번호 5에 DF 비트를 배치하지만 프래그먼트화되어야 합니다.라우터가 이를 삭제하고, 프래그먼트화가 필요하지만 DF 비트가 설정되었음을 발신자에게 알립니다(ICMP 유형 3 코드 4). 결국, RFC 1191은 지금 작동해야 하며 발신자는 패킷 크기를 줄여야 합니다.

WCCP에서는 소스 IP 주소가 웹 서버 IP 주소이므로 이 ICMP는 WSA로 이동하지 않습니다.실제 웹 서버로 이동하려고 합니다(맨 아래에 있는 이 라우터는 WCCP를 인식하지 못합니다). WCCP와 경로 MTU 검색이 함께 이루어지면 네트워크 설계가 손상되기도 합니다.

솔루션

이 문제를 해결하는 4가지 방법이 있습니다.

- 실제 MTU를 검색한 다음 WSA에서 etherconfig를 사용하여 인터페이스의 MTU를 낮춥니다 .TCP 헤더는 60, IP는 20, ICMP를 사용할 때는 IP 헤더에 8바이트를 추가한다는 점에 유의하십시오.

- 경로 MTU 검색을 비활성화합니다(**pathmtudiscovery** CLI WSA 명령). 이로 인해 TCP MSS 536이 발생하여 성능 문제가 발생할 수 있습니다.

- WSA와 클라이언트 간에 L3 단편화가 없도록 네트워크를 변경합니다.

- 관련 인터페이스를 진행하는 동안 각 Cisco 라우터에서 **ip tcp mss-adjust 1360**(또는 다른 계산된 번호) 명령을 사용합니다.

추가 참고 사항

이 문제가 조사 중인 동안, 프록시를 몇 분 동안 명시적으로 클라이언트에 설정한 다음 제거하면 향후 4~5시간 동안 문제가 해결된다는 사실을 발견했습니다.이는 명시적 모드에서 WSA와 클라이언트 간의 경로 MTU 검색 메커니즘이 작동하기 때문입니다.WSA에서 경로 MTU를 검색하면 검색된 TCP MSS와 함께 내부 테이블에 저장하여 참조할 수 있습니다.이 테이블은 4시간에서 5시간마다 새로 고쳐져, 그렇게 많은 시간이 지난 후에 솔루션이 다시 작동하지 않게 됩니다.