Comportamento WSA na descoberta de MTU de caminho com o uso de WCCP

Contents

[Introduction](#)
[Informações de Apoio](#)
[Pré-fase](#)
[Como o caminho MTU Dicovery e o WCCP funcionam separadamente](#)
[Descoberta da MTU do caminho](#)
[WCCP](#)
[Problema](#)
[Solução](#)
[Notas adicionais](#)

Introduction

Este documento descreve um problema encontrado em que o roteador descarta pacotes quando sua configuração inclui a descoberta do Protocolo de Comunicação de Cache da Web (WCCP - Web Cache Communication Protocol) e MTU (Maximum Transmission Unit) de caminho e fornece uma solução para o problema.

Informações de Apoio

Pré-fase

Quando vistos separadamente, muitos recursos são excelentes para lidar com um problema específico. No entanto, às vezes, se você combinar duas ou três técnicas, ele produz um comportamento estranho e você deve introduzir outro recurso ou solução para que funcione corretamente. Por exemplo, a convergência de Spanning Tree e OSPF (Open Shortest Path First) e L2 (Layer 2) leva mais tempo (20s) que OSPF (1s se for usado o intervalo inoperante mínimo), mas substitua o Spanning Tree por MST (Multiple Spanning Tree) e ele funciona corretamente novamente.

O mesmo comportamento de interoperabilidade foi observado entre WCCP e descoberta de MTU de caminho; muitos acham que é o problema do cabeçalho Generic Routing Encapsulation (GRE). No entanto, este documento explica a causa real.

Como o caminho MTU Dicovery e o WCCP funcionam separadamente

Descoberta da MTU do caminho

Cada linha tem seu limite sobre o tamanho de um pacote. Se você enviar um pacote maior do que o suportado, ele será descartado. Uma das funções dos dispositivos L3 (roteadores) no caminho é cuidar e cortar pacotes grandes de uma das linhas para a outra para garantir que a comunicação fim-a-fim seja transparente para os recursos de cada linha.

No entanto, às vezes, os hosts finais são configurados de forma que seus pacotes não possam ser cortados (por exemplo, arquivos criptografados, chamadas de voz). Essas informações são comunicadas através do bit Don't Fragment (DF) dentro do cabeçalho IP. Os roteadores descartam pacotes como esses, mas o roteador tenta reportar ao host final através da mensagem ICMP (Internet Control Message Protocol) (tipo 3-Destino inalcançável, código 4 - fragmentação necessária, mas conjunto de bits DF). Dessa forma, o host sabe enviar pacotes menores no futuro.

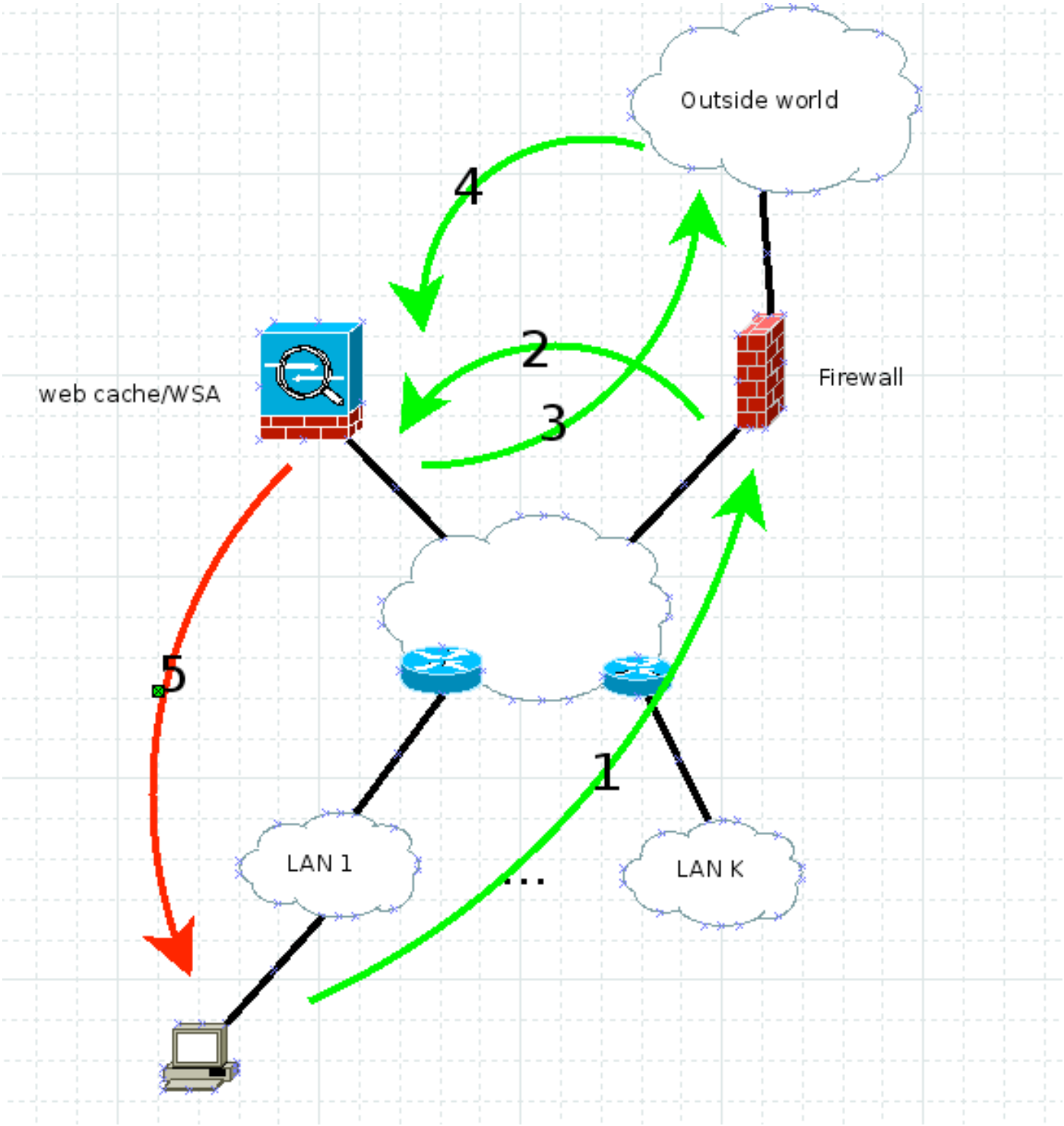
Esse é o coração do caminho da descoberta de MTU. Você pode enviar pacotes grandes com o bit DF definido para ver se eles o fazem na extremidade ou se você recebe um relatório ICMP conforme descrito anteriormente. Depois de determinar o tamanho máximo do pacote viável, use-o para qualquer comunicação adicional. Consulte RFC 1191 para obter mais informações.

O Web Security Appliance (WSA) emprega a descoberta de MTU do caminho por padrão. Assim, todos os pacotes gerados têm o bit DF definido pela configuração padrão.

WCCP

Se você precisar impor segurança à sua rede no tráfego da Web sem o conhecimento dos outros, você executará o tráfego por meio de um proxy que não é visível. O WCCP é o protocolo usado para se comunicar entre o dispositivo que intercepta (roteador/firewall) e o mecanismo/proxy de cache da Web, que é o WSA nesse caso.

Este diagrama ilustra como o tráfego flui neste cenário:



Funciona assim:

1. O cliente envia HTTP GET com a origem IP, seu endereço IP (endereço IP do cliente) e o endereço IP do servidor de destino.

2. O firewall ou roteador intercepta o HTTP GET e o encaminha via WCCP GRE ou L2 puro para o cache da Web/WSA. A origem ainda é o endereço IP do cliente e o destino ainda é o endereço IP do servidor web.

3. O WSA inspeciona a solicitação e, se for legítimo, a espelha no servidor Web. Aqui, o endereço IP destino é o endereço IP do servidor Web e o endereço IP origem pode ser o WSA ou o cliente, com base no fato de você ter habilitado o spoofing do endereço IP do cliente. Para este exemplo, não importa porque o tráfego de retorno em ambos os casos tem

que atingir o WSA.

4. O tráfego de retorno é inspecionado no WSA.

5. O WSA envia a resposta ao cliente com o endereço IP de origem, SEMPRE o endereço IP do servidor Web (para que o cliente não fique suspeito) e o endereço IP do cliente de destino.

Problema

O que acontece se um dos roteadores do diagrama precisar fragmentar o tráfego? O WSA coloca o bit DF no pacote número 5, mas ele precisa ser fragmentado. O roteador o descarta e informa ao remetente que a fragmentação é necessária, mas o bit DF está definido (código 4 do tipo 3 do ICMP). Afinal, o RFC 1191 tem que funcionar agora e o remetente deve reduzir o tamanho do pacote.

Com o WCCP, o endereço IP origem é o endereço IP do servidor web, de modo que este ICMP nunca vai para o WSA; em vez disso, ele tenta ir para o servidor web real (lembre-se, esse roteador na parte inferior não está ciente do WCCP). É assim que a descoberta de WCCP e MTU de caminho juntas, às vezes, rompe seu projeto de rede.

Solução

Há quatro maneiras de resolver esse problema:

- Descubra o MTU real e use **etherconfig** no WSA para reduzir o MTU da interface. Lembre-se de que o cabeçalho TCP é 60, o IP é 20 e quando você usa ICMP, isso adiciona 8 bytes ao cabeçalho IP.

- Desative a descoberta de MTU do caminho (comando **pathtudiscovery** CLI WSA). Isso resulta em TCP MSS de 536, o que pode causar um problema de desempenho.

- Altere a rede para que não haja fragmentação L3 entre o WSA e os clientes.

- Use o comando **ip tcp mss-adjust 1360** (ou outro número calculado) em cada roteador Cisco no caminho nas interfaces relevantes.

Notas adicionais

Enquanto esse problema estava sendo investigado, descobriu-se que se você definir o proxy explicitamente no cliente por alguns minutos e depois removê-lo, o problema será resolvido para as próximas quatro a cinco horas. Isso se deve ao fato de que, no modo explícito, o mecanismo de descoberta de MTU de caminho entre o WSA e o cliente funciona. Quando o WSA descobrir o MTU do caminho, ele o armazenará junto com o MSS TCP descoberto na tabela interna para referência. Aparentemente, essa tabela é atualizada a cada quatro a cinco horas, o que faz com que a solução não funcione novamente depois de tanto tempo.