Comportamento WSA no Path MTU Discovery com uso do WCCP

Índice

[Introdução](#)
[Informações de Apoio](#)
[PRE-fase](#)
[Como o Path MTU Discovery e o WCCP trabalham separadamente](#)
[Descoberta da MTU do caminho](#)
[WCCP](#)
[Problema](#)
[Solução](#)
[Notas adicionais](#)

Introdução

Este documento descreve um problema encontrado onde o roteador deixa cair pacotes quando sua configuração inclui o Protocolo de Comunicação de Cache da Web (WCCP) e a descoberta da unidade de transmissão máxima do trajeto (MTU), e fornece uma solução ao problema.

Informações de Apoio

PRE-fase

Quando olhadas separadamente, muitas características são excelentes segurar um problema específico. Às vezes embora, se você combina duas ou três técnicas, produz algum comportamento inábil e você deve introduzir uma outra característica ou ação alternativa a fim fazê-la trabalhar corretamente. Por exemplo, o uso que mede - a árvore e o Open Shortest Path First (OSPF) e mergulham 2 (L2) que a convergência toma mais por muito tempo (20s) do que OSPF (1s se o intervalo inoperante mínimo é usado), mas substituem a medida - a árvore com Spanning Tree Múltipla (MST) e ele funciona corretamente outra vez.

O mesmo comportamento da Interoperabilidade foi observado entre o WCCP e o Path MTU Discovery; muitos pensam que é o problema do encabeçamento do Generic Routing Encapsulation (GRE). Contudo, este documento explica a causa real.

Como o Path MTU Discovery e o WCCP trabalham separadamente

Descoberta da MTU do caminho

Cada linha tem seu limite em como grande um pacote pode ser. Se você envia um pacote maior do que está apoiado, a seguir é deixado cair. Um dos papéis dos dispositivos L3 (Roteadores) na maneira é ciao e a costeleta grandes pacotes de uma das linhas à outra a fim certificar-se de que uma comunicação fim-a-fim é transparente às capacidades de cada linha.

Às vezes embora, os host finais são configurados de tal maneira que seus pacotes não podem ser desbastados (por exemplo, arquivos, chamadas de voz cifrados). Esta informação é comunicada através do mordeu don't fragment (DF) dentro do cabeçalho IP. O Roteadores deixa cair pacotes como estes, mas as tentativas do roteador para relatar ao host final através da mensagem do Internet Control Message Protocol (ICMP) (o tipo 3-Destination inacessível, codifica 4 - fragmentação necessária, mas jogo do bit DF). Esta maneira, o host sabe para enviar no futuro pacotes menores.

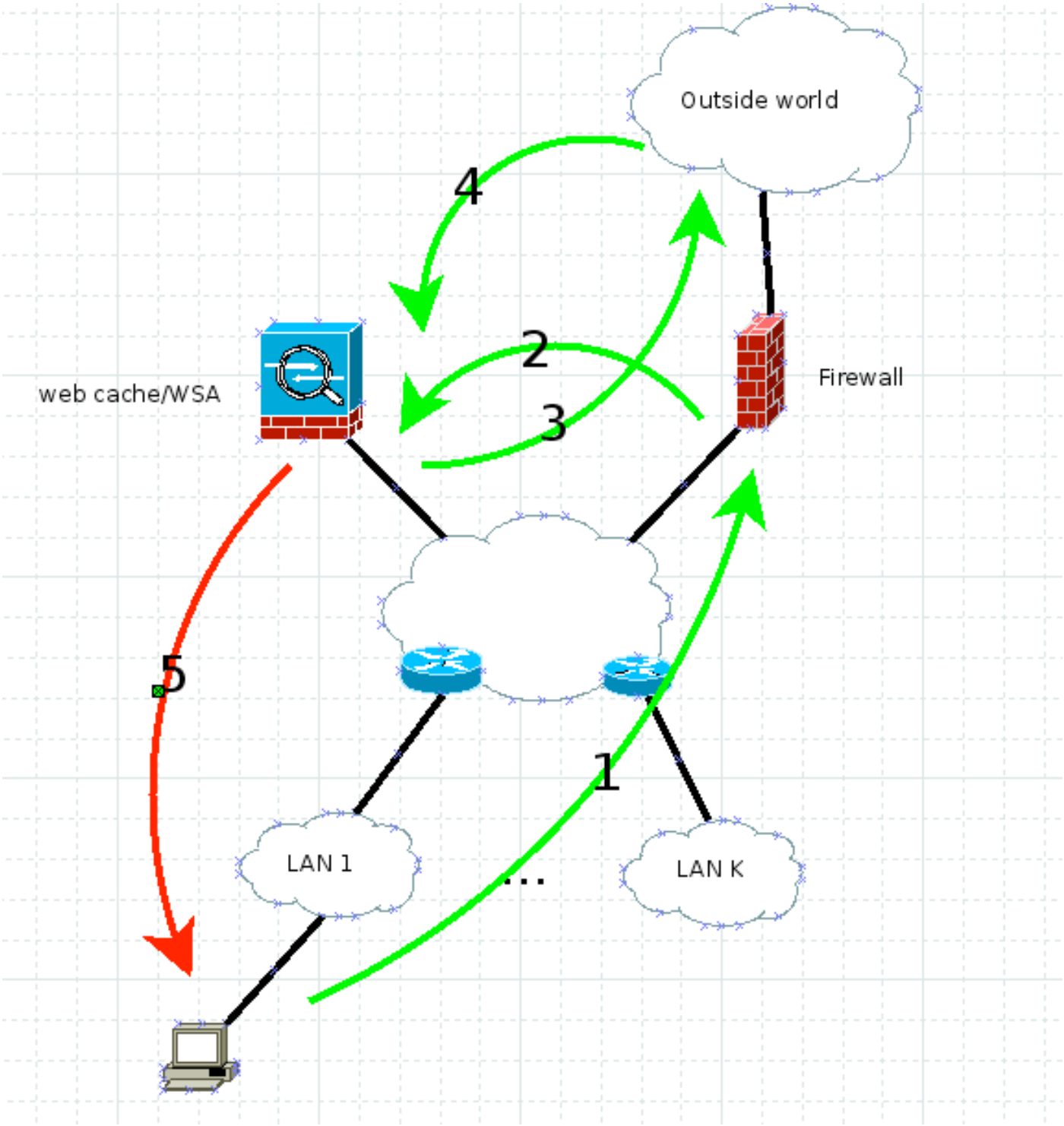
Este é o coração do Path MTU Discovery. Você pode enviar grandes pacotes com o jogo do bit DF a fim ver se o fazem para a extremidade ou se você recebe um relatório ICMP como descrito anteriormente. Uma vez que você determina o tamanho do pacote praticável máximo, use-o para todas as comunicações mais adicionais. Refira o RFC 1191 para mais informação.

A ferramenta de segurança da Web (WSA) emprega o Path MTU Discovery à revelia. Assim, todos seus pacotes gerados têm o jogo do bit DF pela configuração padrão.

WCCP

Se você precisa de impor a Segurança em sua rede no tráfego de web sem outro conhecimento, você executa seu tráfego através de um proxy que não é visível. O WCCP é o protocolo que é usado para se comunicar entre o dispositivo que intercepta (roteador/Firewall) e o motor do cache de web/proxy, que é WSA neste caso.

Este diagrama ilustra como fluxos de tráfego nesta encenação:



Trabalha como este:

1. O cliente envia HTTP GET com o origem de IP, seu endereço IP de Um ou Mais Servidores Cisco ICM NT (endereço IP cliente), e o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de destino.

2. O Firewall ou o roteador interceptam o HTTP GET e para a frente ele através de WCCP GRE ou L2 puro à Web cache/WSA. A fonte é ainda o endereço IP cliente e o destino é ainda o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de Web.

3. O WSA inspeciona o pedido e, se é legítimo, espelha-o para o servidor de Web. Aqui o endereço IP de destino é o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de Web e o endereço IP de origem pôde ser o WSA ou o cliente, com base em se

você permitiu a falsificação do endereço IP cliente. Para este exemplo, não importa porque o tráfego de retorno em ambos os casos tem que bater 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 de Um ou Mais Servidores Cisco ICM NT do servidor de Web (assim que o cliente não obtém suspeito), e o endereço IP cliente do destiantion.

Problema

Que acontece se um do Roteadores do diagrama tem que o fragmento traficar? O WSA põe o DF mordido sobre o número 5 do pacote, mas tem que ser fragmentado. O roteador deixa-o cair e di-lo ao remetente que a fragmentação está precisada mas o bit DF está ajustado (tipo 3 código 4 ICMP). Apesar de tudo, o RFC 1191 tem que trabalhar agora e o remetente deve abaixar seu tamanho do pacote.

Com WCCP, o endereço IP de origem é o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor de Web, assim que este ICMP nunca vai ao WSA; um pouco, tenta ir ao servidor de Web real (recorde, este roteador na parte inferior não está ciente do WCCP). Isto é como o WCCP e o Path MTU Discovery junto quebram às vezes seu projeto de rede.

Solução

Há quatro maneiras de resolver este problema:

- Descubra o MTU real e use então o **etherconfig no** WSA para abaixar o MTU da relação. Recorde que o cabeçalho de TCP é 60, o IP é 20, e quando você usa o ICMP, que adiciona 8 bytes ao cabeçalho IP.

- Desabilite o Path MTU Discovery (comando do **pathmtudiscovery** CLI WSA). Isto conduz a TCP MSS de 536, que puderam causar um problema de desempenho.

- Não mude a rede tão lá é nenhuma fragmentação L3 entre o WSA e os clientes.

- Use o **IP tcp mss-ajustam** outros **1360** (ou números calculados) o comando em cada roteador Cisco na maneira nas interfaces relevantes.

Notas adicionais

Quando este problema estava sob a investigação, descobriu-se que se você ajusta o proxy explicitamente no cliente por um par minutos e o remove então, a edição é resolved para as próximas quatro a cinco horas. Isto é devido ao fato de que, no modo explícito, o mecanismo do Path MTU Discovery entre o WSA e o cliente trabalha. Uma vez que o WSA descobre o MTU de caminho, armazena-o junto com o TCP descoberto MSS na tabela interna para a referência. Esta tabela é refrescada aparentemente cada quatro a cinco horas, que rende a solução para não trabalhar outra vez tanto após o tempo.