Comportamiento WSA en la detección de MTU de trayecto con el uso del WCCP

Contenido

Introducción

Este documento describe un problema encontrado donde el router cae los paquetes cuando su configuración incluye el protocolo web cache communication (WCCP) y detección de la Unidad máxima de transmisión (MTU) de la trayectoria (MTU), y proporciona una solución al problema.

Antecedentes

PRE-fase

Cuando están miradas por separado, muchas características son excelentes manejar un problema específico. A veces sin embargo, si usted combina dos o tres técnicas, produce un cierto comportamiento torpe y usted debe introducir otra característica o solución alternativa para hacer que trabaja correctamente. Por ejemplo, el uso que atraviesa - el árbol y el Open Shortest Path First (OSPF) y acodan 2 (L2) que la convergencia dura (20s) que OSPF (1s si se utiliza el Intervalo muerto mínimo), pero substituyen atravesar - el árbol con Múltiples Árboles de expansión (MST) y la funciona correctamente otra vez.

El mismo comportamiento de la Interoperabilidad se ha observado entre el WCCP y la detección de MTU de trayecto; muchos piensan que es el problema de la encabezado del Generic Routing Encapsulation (GRE). Sin embargo, este documento explica la causa real.

Cómo la detección de MTU de trayecto y el WCCP trabajan por separado

Descubrimiento de la MTU del trayecto

Cada línea tiene su límite en cómo es grande un paquete puede ser. Si usted envía un paquete más grande que se soporta, después se cae. Uno del papeles de los dispositivos L3 (Routers) en la manera es llevar el cuidado y la tajada los paquetes grandes a partir de la una de las líneas la otra para aseegurarse que la comunicación de punta a punta es transparente a las capacidades de cada línea.

A veces sin embargo, se configuran los host extremos de una manera tal que sus paquetes no puedan ser tajados (por ejemplo, los archivos, las llamadas de voz cifrados). Esta información se comunica vía el don't fragment (DF) mordido dentro del encabezado IP. El Routers cae los paquetes como éstos, pero los intentos del router para señalar al final el host vía el mensaje del Internet Control Message Protocol (ICMP) (el tipo 3-Destination inalcanzable, cifra 4 - fragmentación necesaria, pero al conjunto de bits DF). Esta manera, el host sabe para enviar paquetes más pequeños en el futuro.

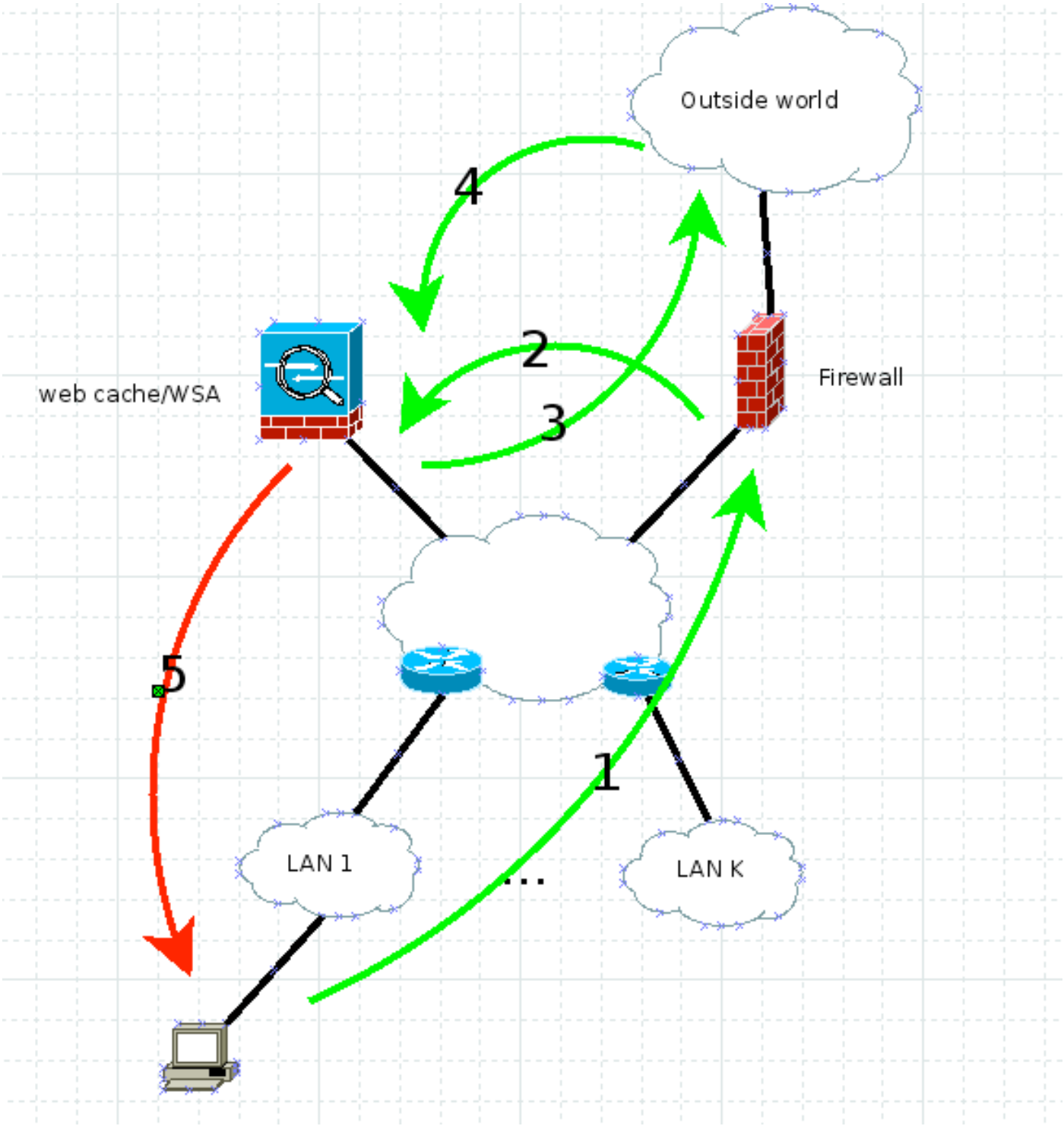
Éste es el corazón de la detección de MTU de trayecto. Usted puede enviar los paquetes grandes con el conjunto de bits DF para ver si lo hacen hacia el extremo o si usted recibe un informe ICMP según lo descrito previamente. Una vez que usted determina el tamaño de paquetes realizable máximo, utilícelo para cualquier comunicaciones más otra. Refiera al RFC 1191 para más información.

El dispositivo de seguridad de la red (WSA) emplea la detección de MTU de trayecto por abandono. Así, todos sus paquetes generados tienen el conjunto de bits DF por la configuración predeterminada.

WCCP

Si usted necesita imponer la Seguridad en su red ante el tráfico de la Web sin otros conocimiento, usted ejecuta su tráfico vía un proxy que no sea visible. El WCCP es el protocolo que se utiliza para comunicar entre el dispositivo que intercepta (router/Firewall) y caché Web el motor/proxy, que es WSA en este caso.

Este diagrama ilustra cómo los flujos de tráfico en este escenario:



Trabaja como esto:

1. El cliente envía HTTP GET con el IP de origen, su dirección IP (dirección IP del cliente), y la dirección IP del servidor de destino.

2. El Firewall o el router intercepta el HTTP GET y adelante él vía WCCP GRE o L2 puro a la red cache/WSA. La fuente sigue siendo el dirección IP del cliente y el destino sigue siendo la dirección IP del servidor Web.

3. El WSA examina la petición y, si es legítimo, la duplica hacia el servidor Web. Aquí el IP Address de destino es el IP Address del servidor Web y la dirección IP de origen pudo ser el WSA o el cliente, sobre la base de si usted habilitó el spoofing del dirección IP del cliente. Por este ejemplo, no importa porque el tráfico de retorno en ambos casos tiene que golpear

el WSA.

4. El tráfico de retorno se examina en el WSA.

5. El WSA envía la respuesta al cliente con la dirección IP de origen, SIEMPRE la dirección IP del servidor Web (así que el cliente no consigue sospechoso), y el dirección IP del cliente del destiantion.

Problema

¿Qué sucede si uno del Routers del diagrama tiene que el fragmento traficar? El WSA pone el DF mordido en el paquete número 5, pero tiene que ser hecho fragmentos. El router lo cae y dice a remitente que la fragmentación es necesaria pero el bit DF está fijado (el código del tipo 3 ICMP 4). Con todo el RFC 1191 tiene que ahora trabajar y el remitente debe bajar su tamaño de paquetes.

Con el WCCP, la dirección IP de origen es la dirección IP del servidor Web, así que este ICMP nunca va al WSA; bastante, intenta ir al servidor Web real (recuerde, este router en la parte inferior no es consciente del WCCP). Éste es cómo el WCCP y la detección de MTU de trayecto junto rompen a veces su diseño de red.

Solución

Hay cuatro maneras de solucionar este problema:

- Descubra el MTU real y después utilice el **etherconfig** en el WSA para bajar el MTU de la interfaz. Recuerde que el encabezado TCP es 60, el IP es 20, y cuando usted utiliza el ICMP, que agrega 8 bytes al encabezado IP.

- Inhabilite la detección de MTU de trayecto (comando del **pathmtudiscovery** CLI WSA). Esto da lugar a TCP MSS de 536, que pudieron causar un problema de rendimiento.

- Cambie la red tan allí no es ninguna fragmentación L3 entre el WSA y los clientes.

- Utilice el **IP tcp mss-ajustan** números calculados) el comando **1360** (u otros en cada router Cisco en la manera en las interfaces pertinentes.

Notas complementarias

Mientras que este problema estaba bajo investigación, fue descubierto que si usted fija el proxy explícitamente en el cliente por un par de minutos y después lo quita, el problema está resuelto para las cuatro a cinco horas próximas. Esto es debido al hecho de que, en el modo explícito, el mecanismo de la detección de MTU de trayecto entre el WSA y el cliente trabaja. Una vez que el WSA descubre el mtu de trayectoria, lo salva junto con el TCP descubierto MSS sobre la tabla interna para la referencia. Esta tabla se restaura al parecer cada cuatro a cinco horas, que rinde la solución para no trabajar otra vez después tanto del tiempo.