Comportamiento de WSA en la Detección de MTU de Trayectoria con el Uso de WCCP

Contenido

Introducción

Este documento describe un problema encontrado donde el router descarta paquetes cuando su configuración incluye tanto el protocolo de comunicación de caché web (WCCP) como la detección de la unidad máxima de transmisión (MTU) de trayectoria, y proporciona una solución al problema.

Antecedentes

Pre-fase

Si se examinan por separado, muchas funciones son excelentes para tratar un problema específico. Aunque a veces, si se combinan dos o tres técnicas, se produce un comportamiento incómodo y se debe introducir otra característica o solución alternativa para que funcione correctamente. Por ejemplo, el uso del árbol de extensión y la convergencia Open Shortest Path First (OSPF) y Layer 2 (L2) lleva más tiempo (20) que OSPF (1 s si se utiliza un intervalo muerto mínimo), pero reemplace el árbol de extensión por un árbol de extensión múltiple (MST) y funciona correctamente de nuevo.

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

Cómo Funcionan por Separado la Detección de MTU de Trayectoria y WCCP

Descubrimiento de la MTU del trayecto

Cada línea tiene su límite sobre el tamaño de un paquete. Si envía un paquete más grande que el soportado, se descarta. Una de las funciones de los dispositivos L3 (routers) en el camino es cuidar y cortar paquetes grandes de una de las líneas a la otra para asegurarse de que la comunicación de extremo a extremo sea transparente para las capacidades de cada línea.

A veces, sin embargo, los hosts finales se configuran de tal manera que sus paquetes no se pueden cortar (por ejemplo, archivos cifrados, llamadas de voz). Esta información se comunica a través del bit Don't Fragment (DF) dentro del encabezado IP. Los routers descartan paquetes como estos, pero el router intenta informar al host final a través del mensaje de protocolo de mensajes de control de Internet (ICMP) (tipo 3-Destino inalcanzable, código 4: fragmentación necesaria, pero bit DF configurado). De esta manera, el host sabe enviar paquetes más pequeños en el futuro.

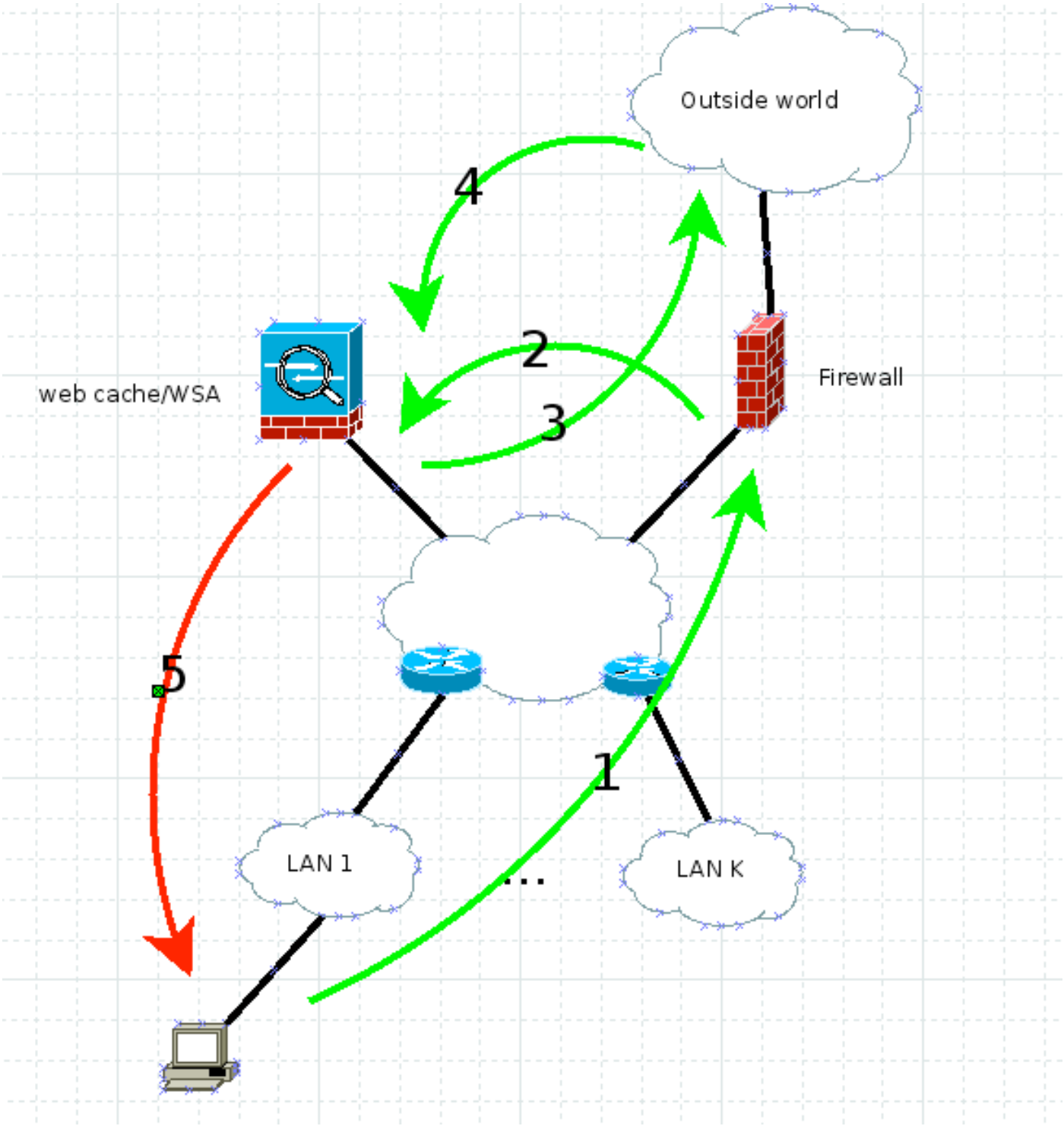
Este es el corazón del descubrimiento de MTU de trayectoria. Puede enviar paquetes grandes con el bit DF configurado para ver si llegan al final o si recibe un informe ICMP como se ha descrito anteriormente. Una vez que determine el tamaño máximo de paquete factible, utilícelo para cualquier otra comunicación. Consulte RFC 1191 para obtener más información.

El dispositivo de seguridad web (WSA) utiliza la detección de MTU de ruta de forma predeterminada. Por lo tanto, todos sus paquetes generados tienen el bit DF configurado por la configuración predeterminada.

WCCP

Si necesita imponer la seguridad en su red en el tráfico web sin el conocimiento de otros, su tráfico se ejecuta a través de un proxy que no es visible. WCCP es el protocolo que se utiliza para comunicarse entre el dispositivo que intercepta (router/firewall) y el motor/proxy de caché web, que es WSA en este caso.

Este diagrama ilustra cómo fluye el tráfico en este escenario:



Funciona así:

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

2. El firewall o router intercepta el HTTP GET y lo reenvía a través de WCCP GRE o L2 puro a la caché web/WSA. El origen sigue siendo la dirección IP del cliente y el destino sigue siendo la dirección IP del servidor web.

3. El WSA inspecciona la solicitud y, si es legítima, la duplica con el servidor web. Aquí, la dirección IP de destino es la dirección IP del servidor web y la dirección IP de origen puede ser el WSA o el cliente, en función de si habilitó la suplantación de dirección IP del cliente. Para este ejemplo, no importa porque el tráfico de retorno en ambos casos tiene que llegar

al WSA.

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

5. El WSA envía la respuesta al cliente con la dirección IP de origen, SIEMPRE la dirección IP del servidor web (de modo que el cliente no se sienta sospechoso) y la dirección IP del cliente de destino.

Problema

¿Qué sucede si uno de los routers del diagrama tiene que fragmentar el tráfico? El WSA coloca el bit DF en el paquete número 5, pero debe fragmentarse. El router lo descarta y le indica al remitente que se necesita fragmentación pero que el bit DF está configurado (código ICMP tipo 3 4). Después de todo, RFC 1191 debe funcionar ahora y el remitente debe reducir su tamaño de paquete.

Con WCCP, la dirección IP de origen es la dirección IP del servidor web, por lo que este ICMP nunca va al WSA; más bien, intenta ir al servidor web real (recuerde, este router de la parte inferior no conoce WCCP). Así es como el WCCP y el descubrimiento de MTU de trayectoria juntas a veces rompen el diseño de la red.

Solución

Hay cuatro maneras de resolver este problema:

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

- Inhabilite la detección de MTU de trayectoria (comando CLI WSA **pathmtudiscovery**). Esto da como resultado el TCP MSS de 536, que podría causar un problema de rendimiento.

- Cambie la red para que no haya fragmentación L3 entre el WSA y los clientes.

- Utilice el comando **ip tcp mss-adjust 1360** (u otro número calculado) en cada router Cisco en el camino en las interfaces relevantes.

Notas complementarias

Mientras se investigaba este problema, se descubrió que si establece el proxy explícitamente en el cliente durante un par de minutos y después lo elimina, el problema se resuelve durante las siguientes cuatro o cinco horas. Esto se debe al hecho de que, en el modo explícito, funciona el mecanismo de detección de MTU de trayectoria entre el WSA y el cliente. Una vez que WSA detecta la MTU de trayectoria, la almacena junto con el TCP MSS detectado en la tabla interna para su referencia. Aparentemente esta tabla se actualiza cada cuatro o cinco horas, lo que hace que la solución no funcione de nuevo después de tanto tiempo.