WSA-Verhalten bei der MTU-Pfaderkennung mithilfe von WCCP

Inhalt

Einführung

Dieses Dokument beschreibt ein Problem, bei dem der Router Pakete verwirft, wenn Ihre Konfiguration sowohl die Erkennung des Web Cache Communication Protocol (WCCP) als auch die MTU-Erkennung (Maximum Transmission Unit) des Pfades umfasst, und bietet eine Lösung für das Problem.

Hintergrundinformationen

Vorphase

Bei separater Betrachtung sind viele Funktionen hervorragend geeignet, um ein bestimmtes Problem zu bewältigen. Wenn Sie jedoch zwei oder drei Techniken kombinieren, führt dies manchmal zu einem unangenehmen Verhalten, und Sie müssen ein anderes Feature oder eine andere Problemumgehung einführen, damit es richtig funktioniert. Beispielsweise dauert die Konvergenz von Spanning Tree und Open Shortest Path First (OSPF) und Layer 2 (L2) länger (20 s) als OSPF (1 s bei minimalem Dead-Intervall), ersetzt Spanning Tree durch Multiple Spanning Tree (MST) und funktioniert wieder einwandfrei.

Zwischen der WCCP- und der MTU-Pfaderkennung wurde dasselbe Interoperabilitäts-Verhalten beobachtet. viele denken, dass es sich um das GRE-Headerproblem (Generic Routing Encapsulation) handelt. In diesem Dokument wird jedoch die eigentliche Ursache erläutert.

Wie Pfad-MTU-Erkennung und WCCP getrennt funktionieren

MTU-Pfaderkennung

Für jede Zeile gibt es ein Limit, wie groß ein Paket sein kann. Wenn Sie ein größeres Paket senden, als unterstützt wird, wird es verworfen. Eine der Rollen, die die L3-Geräte (Router) unterwegs übernehmen, besteht darin, große Pakete von einer Leitung zur anderen zu schneiden, um sicherzustellen, dass die End-to-End-Kommunikation für die Funktionen der einzelnen Leitungen transparent ist.

Manchmal werden Endhosts jedoch so konfiguriert, dass ihre Pakete nicht gehackt werden können (z. B. verschlüsselte Dateien, Sprachanrufe). Diese Informationen werden im IP-Header über das DF-Bit (Don't Fragment) übermittelt. Router verwerfen Pakete wie diese, aber der Router versucht, über ICMP-Meldung (Internet Control Message Protocol) an den Endhost zu berichten (Typ 3-Ziel nicht erreichbar, Code 4 - Fragmentierung erforderlich, aber DF-Bit-Satz). Auf diese Weise kann der Host künftig kleinere Pakete senden.

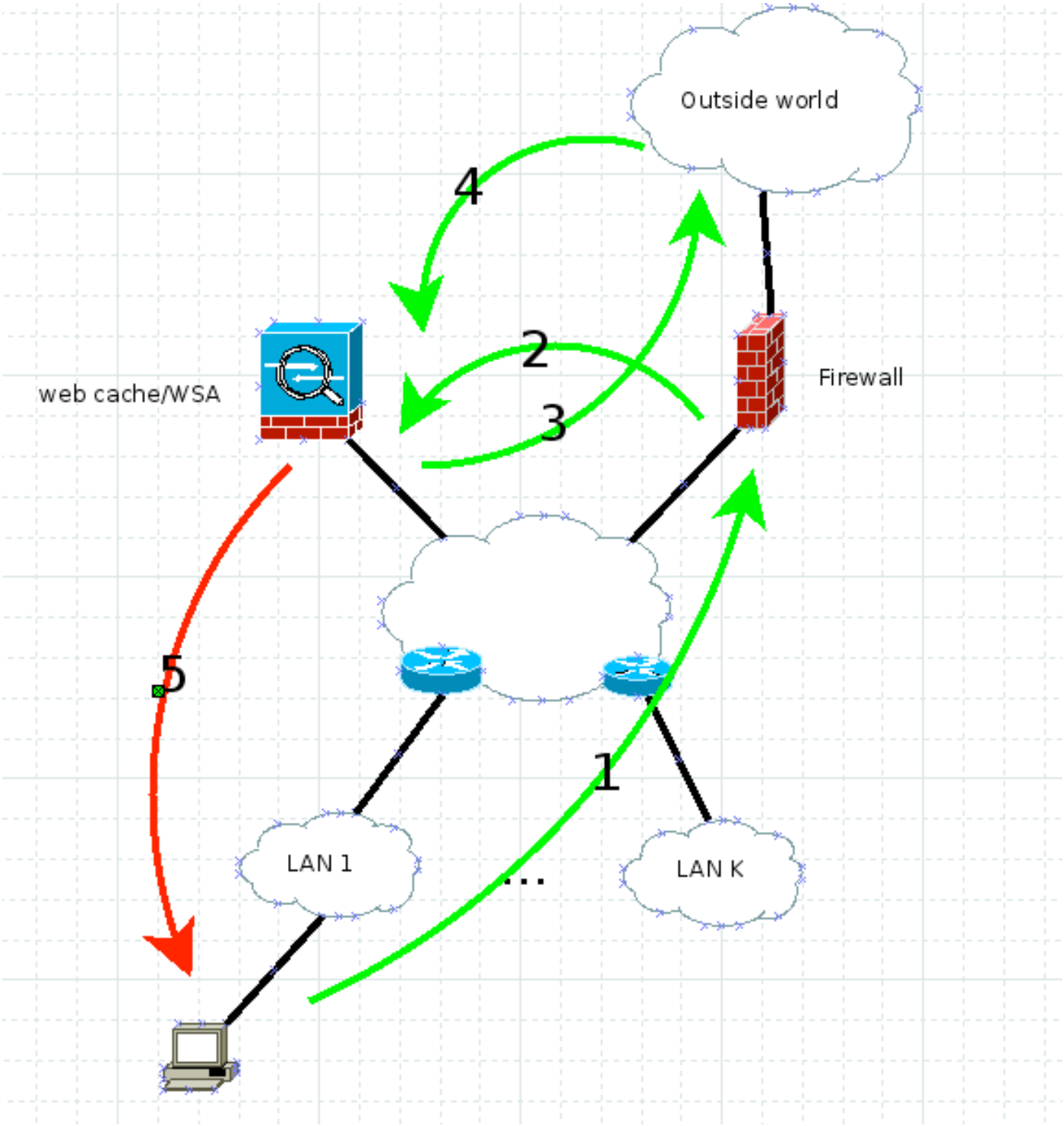
Dies ist der Kern der MTU-Pfaderkennung. Sie können große Pakete mit festgelegtem DF-Bit senden, um zu sehen, ob diese am Ende auftreten oder wenn Sie einen ICMP-Bericht wie oben beschrieben erhalten. Sobald Sie die maximal verwendbare Paketgröße bestimmen, können Sie sie für weitere Kommunikationszwecke verwenden. Weitere Informationen finden Sie in RFC 1191.

Die Web Security Appliance (WSA) verwendet standardmäßig die MTU-Pfaderkennung. Daher ist das DF-Bit für alle generierten Pakete standardmäßig festgelegt.

WCCP

Wenn Sie dem Web-Datenverkehr ohne Wissen der anderen Sicherheit in Ihrem Netzwerk auferlegen müssen, führen Sie dessen Datenverkehr über einen Proxy aus, der nicht sichtbar ist. WCCP ist das Protokoll, das für die Kommunikation zwischen dem Gerät verwendet wird, das (Router/Firewall) abfängt, und der Web-Cache-Engine/dem Webproxy, der in diesem Fall WSA ist.

Dieses Diagramm veranschaulicht den Datenverkehrsfluss in diesem Szenario:



Es funktioniert wie folgt:

1. Der Client sendet HTTP GET mit der IP-Quelle, der IP-Adresse (Client-IP-Adresse) und der IP-Adresse des Zielservers.

2. Die Firewall oder der Router fängt das HTTP GET ab und leitet es über WCCP GRE oder reines L2 an den Web-Cache/die WSA weiter. Die Quelle ist immer noch die Client-IP-Adresse, und das Ziel ist immer noch die IP-Adresse des Webservers.

3. Die WSA überprüft die Anforderung und spiegelt sie, wenn sie legitim ist, auf den Webserver. Hier ist die Ziel-IP-Adresse die IP-Adresse des Webservers, und die Quell-IP-Adresse kann die WSA oder der Client sein, je nachdem, ob Sie die IP-Adressen-Spoofing-Funktion des Clients aktiviert haben. In diesem Beispiel spielt dies keine Rolle, da der Rückverkehr in

beiden Fällen die WSA aufrufen muss.

4. Der Rückverkehr wird in der WSA überprüft.

5. Die WSA sendet die Antwort an den Client mit der Quell-IP-Adresse, IMMER der Webserver-IP-Adresse (sodass der Client nicht verdächtig wird) und der Ziel-Client-IP-Adresse.

Problem

Was passiert, wenn einer der Router im Diagramm den Datenverkehr fragmentieren muss? Die WSA legt das DF-Bit auf Paketnummer 5 ab, muss jedoch fragmentiert werden. Der Router verwirft diesen und teilt dem Absender mit, dass eine Fragmentierung erforderlich ist, das DF-Bit jedoch festgelegt ist (ICMP-Typ 3 Code 4). Schließlich muss RFC 1191 jetzt funktionieren, und der Absender muss seine Paketgröße verringern.

Bei WCCP ist die Quell-IP-Adresse die IP-Adresse des Webservers, sodass dieser ICMP nie zur WSA geht. Stattdessen versucht es, zum echten Webserver zu gehen (denken Sie daran, dieser Router unten ist nicht bekannt WCCP). Auf diese Weise wird das Netzwerkdesign manchmal durch WCCP und die MTU-Pfaderkennung gestört.

Lösung

Es gibt vier Möglichkeiten, dieses Problem zu lösen:

- Ermitteln Sie die tatsächliche MTU, und verwenden Sie dann **etherconfig** auf der WSA, um die MTU der Schnittstelle zu senken. Beachten Sie, dass der TCP-Header 60, die IP 20 und bei Verwendung von ICMP 8 Byte zum IP-Header hinzufügt.

- Deaktivieren Sie die MTU-Pfaderkennung (CLI WSA-Befehl **pathmtudiscovery**). Dies führt zu einer TCP-MSS von 536, die ein Leistungsproblem verursachen kann.

- Ändern Sie das Netzwerk, sodass es keine L3-Fragmentierung zwischen der WSA und den Clients gibt.

- Verwenden Sie den Befehl **ip tcp mss-adjust 1360** (oder eine andere berechnete Zahl) auf jedem Cisco Router auf dem Weg zu den entsprechenden Schnittstellen.

Zusätzliche Hinweise

Während dieses Problem untersucht wurde, wurde entdeckt, dass das Problem für die nächsten vier bis fünf Stunden behoben wird, wenn Sie den Proxy für einige Minuten explizit in den Client setzen und ihn dann entfernen. Dies liegt daran, dass der MTU-Erkennungsmechanismus für den Pfad zwischen der WSA und dem Client im expliziten Modus funktioniert. Sobald die WSA die Pfad-MTU erkennt, speichert sie zusammen mit der erkannten TCP-MSS zur Referenz in der internen Tabelle. Offenbar wird diese Tabelle alle vier bis fünf Stunden aktualisiert, wodurch die Lösung nicht mehr nach so langer Zeit funktioniert.