WSA-gedrag op Pad MTU-detectie met gebruik van WCCP

Inhoud

Inleiding

Dit document beschrijft een probleem dat is ondervonden wanneer de router pakketjes daalt wanneer de configuratie zowel Web Cache Communication Protocol (WCCP) als path Max Transmission Unit (MTU) bevat om het probleem op te lossen.

Achtergrondinformatie

Voorstadium

Wanneer afzonderlijk bekeken, zijn veel eigenschappen zeer goed om een specifiek probleem aan te pakken. Soms echter, als je twee of drie technieken combineert, veroorzaakt het een onhandig gedrag en moet je een andere functie of werkronden introduceren om het goed te laten werken. Bijvoorbeeld, gebruik het overspannen van boom en Open Kortste Pad Eerst (OSPF) en Layer 2 (L2) convergentie duurt langer (20s) dan OSPF (1s als minimum dood interval wordt gebruikt), maar vervang het overspannen van boom met Meervoudig Spanning-Tree (MST) en het functioneert behoorlijk opnieuw.

Hetzelfde interoperabiliteitsgedrag is waargenomen tussen WCCP en het opsporen van een MTU-pad; velen denken dat het het Generic Routing Encapsulation-probleem (GRE) is. In dit document wordt echter de werkelijke oorzaak toegelicht.

Hoe Path MTU-detectie en WCCP afzonderlijk werken

Detectie Pad MTU

Elke regel heeft zijn limiet op hoe groot een pakje kan zijn. Als u een groter pakket verzenden dan wordt ondersteund, wordt dit ingetrokken. Een van de rollen van de L3 apparaten (routers) op weg is om grote pakketten van één van de lijnen naar het andere te zorgen en te wissen om ervoor te zorgen dat de end-to-end communicatie transparant is voor de mogelijkheden van elke lijn.

Soms echter, worden eindgastheren op dusdanige wijze gevormd dat hun pakketten niet kunnen worden versnipperd (bijvoorbeeld, gecodeerde bestanden, spraakoproepen). Deze informatie wordt gecommuniceerd via het DF-bit (Don't Fragment) in de IP-header. Routers zetten pakketten zoals deze neer, maar de router probeert om aan het eind host via het ICMP-bericht (Internet Control Message Protocol) te melden (type 3-Destination onbereikbaar, code 4 - fragmentatie nodig, maar DF bit set). Op deze manier weet de host in de toekomst kleinere pakketten te verzenden.

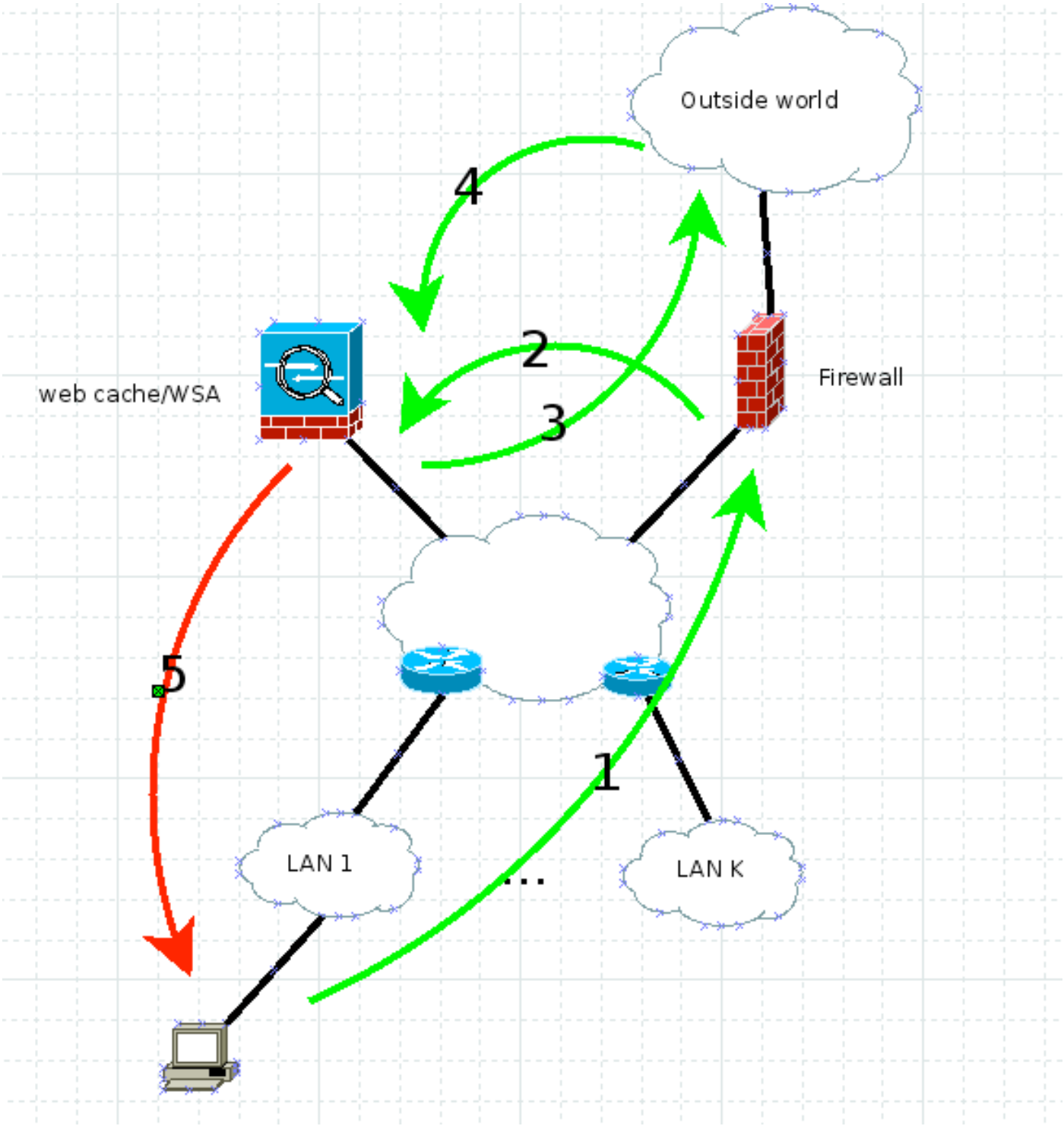
Dit is het hart van pad MTU ontdekking. U kunt grote pakketten verzenden met het PDF-bit dat is ingesteld om te zien of ze tegen het einde worden gemaakt of als u een ICMP-rapport ontvangt zoals eerder beschreven. Zodra u de maximale werkbare pakketgrootte hebt bepaald, gebruikt u deze voor verdere communicatie. Raadpleeg RFC 1191 voor meer informatie.

Web security applicatie (WSA) maakt standaard gebruik van 'path MTU discovery'. Zodoende hebben alle gegenereerde pakketten het PDF-bit dat door de standaardconfiguratie is ingesteld.

WCCP

Als je beveiliging in je netwerk op het web verkeer moet leggen zonder de medeweten van anderen, runt je hun verkeer via een proxy die niet zichtbaar is. WCCP is het protocol dat wordt gebruikt om tussen het apparaat te communiceren dat (router/firewall) onderschept en de webcachemachine/proxy, wat in dit geval WSA is.

In dit schema wordt aangegeven hoe het verkeer in dit scenario stroomt:



Het werkt als volgt:

1. De client stuurt HTTP GET met de IP-bron, zijn IP-adres (client-IP-adres) en het IP-adres van de doelserver.

2. De firewall of router intercepteert HTTP GET en stuurt het door via WCCP GRE of pure L2 naar web cache/WSA. De bron is nog steeds het IP-adres van de client en de bestemming is nog steeds het IP-adres van de webserver.

3. De WSA inspecteert het verzoek en, als het legitiem is, spiegelt het op de webserver. Hier is het IP-adres van de doelserver het IP-adres van de webserver en het IP-adres kan het WSA of de client zijn, gebaseerd op de vraag of u IP-adresspoofing van de client hebt ingeschakeld. In dit voorbeeld doet het er niet toe omdat het retourverkeer in beide gevallen

de WSA moet raken.

4. Het retourverkeer wordt geïnspecteerd bij de WSA.

5. WSA stuurt de reactie op de client met het bron IP adres, ALTIJD het IP-adres van de webserver (zodat de client niet verdacht wordt) en het IP-adres van de doelclient.

Probleem

Wat gebeurt er als een van de routers uit het diagram het verkeer moet fragmenteren? De WSA zet het DF bit op pakketnummer 5, maar het moet gefragmenteerd zijn. De router laat het vallen en vertelt de zender dat fragmentatie nodig is maar het DF-bit is ingesteld (ICMP type 3 code 4). RFC 1911 moet nu immers werken en de zender moet zijn pakketgrootte verlagen.

Met WCCP is het IP-bronadres het IP-adres van de webserver, zodat dit ICMP nooit naar de WSA gaat; In plaats daarvan probeert het naar de echte webserver te gaan (vergeet niet dat deze router onderaan niet op de hoogte is van WCCP). Dit is hoe de ontdekking van WCCP en pad MTU samen soms uw netwerkontwerp breken.

Oplossing

Er zijn vier manieren om dit probleem op te lossen:

- Ontdek de 'real MTU' en gebruik dan **etherfig** op de WSA om de MTU van de interface te verlagen. Onthoud dat de TCP header 60 is, IP 20, en wanneer je ICMP gebruikt, dat 8 bytes aan de IP header toevoegt.

- Schakel pad MTU discovery (**pathmtudiscovery** CLI WSA-opdracht) uit. Dit resulteert in TCP MSS van 536, wat een prestatiesprobleem kan veroorzaken.

- Verander het netwerk zodat er geen L3-fragmentatie is tussen de WSA en de klanten.

- Gebruik het opdracht **ip tcp mss-aanpassen 1360** (of een ander berekend nummer) op elke Cisco-router op de weg naar de relevante interfaces.

Extra opmerkingen

Terwijl dit probleem onderzocht werd, werd ontdekt dat als je de proxy voor een paar minuten expliciet in de client instelt en deze vervolgens verwijdert, de kwestie de komende vier tot vijf uur opgelost wordt. Dit is te wijten aan het feit dat het "path MTU"-ontdekkingsmechanisme tussen de WSA en de cliënt in de expliciete modus werkt. Zodra de WSA de weg MTU ontdekt, slaat het samen met de ontdekte TCP MSS op de interne tabel op ter referentie. Blijkbaar wordt deze tabel om de vier tot vijf uur ververst, wat de oplossing maakt om na zo veel tijd niet meer te werken.