Comportement WSA sur la découverte MTU de chemin avec l'utilisation de WCCP

Contenu

Introduction

Ce document décrit un problème rencontré lorsque le routeur abandonne des paquets lorsque votre configuration inclut à la fois le protocole WCCP (Web Cache Communication Protocol) et la découverte MTU (Path Maximum Transmission Unit), et il fournit une solution au problème.

Informations générales

Pré-phase

Lorsqu'elles sont examinées séparément, de nombreuses fonctionnalités sont idéales pour traiter un problème spécifique. Parfois, cependant, si vous combinez deux ou trois techniques, cela produit un comportement délicat et vous devez introduire une autre fonctionnalité ou contourner le problème pour le faire fonctionner correctement. Par exemple, la convergence Spanning Tree et Open Shortest Path First (OSPF) et de couche 2 (L2) prend plus de temps (20) qu'OSPF (1 si l'intervalle d'arrêt minimal est utilisé), mais remplacez spanning tree par Multiple Spanning Tree (MST) et il fonctionne à nouveau correctement.

Le même comportement d'interopérabilité a été observé entre WCCP et la détection de MTU de chemin ; beaucoup pensent qu'il s'agit du problème d'en-tête GRE (Generic Routing Encapsulation). Cependant, ce document explique la véritable cause.

Fonctionnement séparé de la découverte MTU du chemin et de WCCP

Découverte MTU du chemin

Chaque ligne a sa limite quant à la taille d’un paquet. Si vous envoyez un paquet plus grand que ne le prend en charge, il est abandonné. L'un des rôles des périphériques de couche 3 (routeurs) sur le chemin est de prendre soin et de couper les paquets volumineux de l'une des lignes à l'autre afin de s'assurer que la communication de bout en bout est transparente pour les capacités de chaque ligne.

Parfois, cependant, les hôtes finaux sont configurés de telle sorte que leurs paquets ne puissent pas être coupés (par exemple, les fichiers chiffrés, les appels vocaux). Ces informations sont communiquées via le bit DF (Don't Fragment) situé dans l'en-tête IP. Les routeurs abandonnent des paquets comme ceux-ci, mais le routeur tente de signaler à l'hôte final via le message ICMP (Internet Control Message Protocol) (type 3-Destination inaccessible, code 4 - fragmentation requise, mais bit DF défini). De cette façon, l’hôte sait envoyer des paquets plus petits à l’avenir.

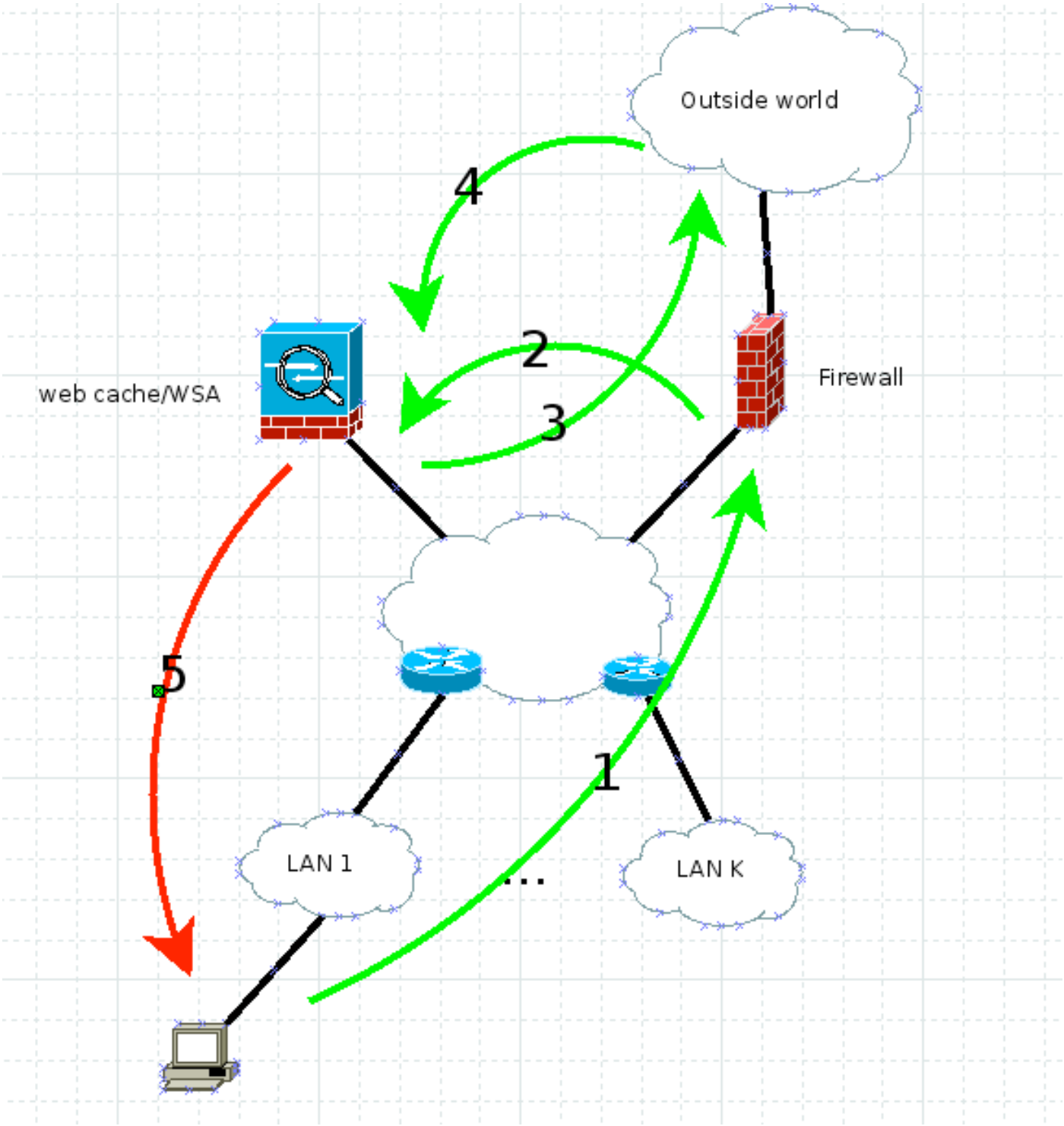
C'est le coeur de la découverte de MTU de chemin. Vous pouvez envoyer des paquets volumineux avec le bit DF défini afin de voir s'ils arrivent vers la fin ou si vous recevez un rapport ICMP comme décrit précédemment. Une fois que vous avez déterminé la taille maximale de paquet utilisable, utilisez-la pour toute autre communication. Référez-vous à RFC 1191 pour plus d'informations.

L'appareil de sécurité Web (WSA) utilise par défaut la détection MTU du chemin. Ainsi, tous ses paquets générés ont le bit DF défini par la configuration par défaut.

WCCP

Si vous devez imposer la sécurité à votre réseau sur le trafic Web à l'insu des autres, vous exécutez leur trafic via un proxy qui n'est pas visible. WCCP est le protocole utilisé pour communiquer entre le périphérique qui intercepte (routeur/pare-feu) et le moteur/proxy de cache Web, qui est WSA dans ce cas.

Ce schéma illustre les flux de trafic dans ce scénario :



Ça marche comme ça :

1. Le client envoie HTTP GET avec la source IP, son adresse IP (adresse IP du client) et l'adresse IP du serveur de destination.

2. Le pare-feu ou le routeur intercepte l'GET HTTP et le transfère via WCCP GRE ou L2 pur vers le cache Web/WSA. La source est toujours l'adresse IP du client et la destination est toujours l'adresse IP du serveur Web.

3. Le WSA inspecte la requête et, s'il est légitime, la met en miroir vers le serveur Web. Ici, l'adresse IP de destination est l'adresse IP du serveur Web et l'adresse IP source peut être le WSA ou le client, selon que vous avez activé ou non l'usurpation d'adresse IP du client. Pour cet exemple, cela n'a pas d'importance car le trafic de retour dans les deux cas doit

toucher le WSA.

4. Le trafic de retour est inspecté au niveau de l'appareil de sécurité Web.

5. Le WSA envoie la réponse au client avec l'adresse IP source, TOUJOURS l'adresse IP du serveur Web (pour que le client ne devienne pas suspect) et l'adresse IP du client de destination.

Problème

Que se passe-t-il si l'un des routeurs du schéma doit fragmenter le trafic ? Le WSA place le bit DF sur le paquet numéro 5, mais il doit être fragmenté. Le routeur le supprime et indique à l'expéditeur que la fragmentation est nécessaire mais que le bit DF est défini (code ICMP 3 4). Après tout, le RFC 1191 doit fonctionner maintenant et l'expéditeur doit réduire sa taille de paquet.

Avec WCCP, l'adresse IP source est l'adresse IP du serveur Web, de sorte que ce protocole ICMP ne va jamais au WSA ; il tente plutôt d'accéder au serveur web réel (souvenez-vous que ce routeur en bas ne connaît pas WCCP). C'est ainsi que la découverte de WCCP et de MTU de chemin rompent parfois la conception de votre réseau.

Solution

Il existe quatre façons de résoudre ce problème :

- Découvrez le MTU réel, puis utilisez **etherconfig** sur le WSA pour diminuer le MTU de l'interface. N'oubliez pas que l'en-tête TCP est 60, l'IP 20 et que lorsque vous utilisez ICMP, il ajoute 8 octets à l'en-tête IP.

- Désactivez la découverte MTU du chemin (commande WSA de CLI **pathmtudiscovery**). Cela entraîne un MSS TCP de 536, ce qui peut entraîner un problème de performances.

- Modifiez le réseau de sorte qu'il n'y ait pas de fragmentation de couche 3 entre le WSA et les clients.

- Utilisez la commande **ip tcp mss-adjust 11360** (ou un autre nombre calculé) sur chaque routeur Cisco sur le chemin des interfaces concernées.

Remarques supplémentaires

Pendant que ce problème était en cours d'investigation, il a été découvert que si vous configurez explicitement le proxy dans le client pendant quelques minutes, puis que vous le supprimez, le problème est résolu pendant les quatre à cinq heures suivantes. Ceci est dû au fait que, en mode explicite, le mécanisme de découverte MTU du chemin entre le WSA et le client fonctionne. Une fois que le WSA découvre le MTU du chemin, il le stocke avec le MSS TCP découvert sur la table interne pour référence. Apparemment, cette table est actualisée toutes les quatre à cinq heures, ce qui rend la solution de ne plus fonctionner après tant de temps.