Contenu

Question :

Pourquoi voyons-nous 502/504 erreurs GATEWAY_TIMEOUT en parcourant à certains sites ?

Symptômes : Les utilisateurs reçoivent 502 ou 504 erreurs de dépassement de délai de passerelle de Cisco WSA en parcourant à certains sites Web

Les utilisateurs reçoivent 502 ou 504 erreurs de dépassement de délai de passerelle en parcourant aux sites Web. Les logs d'Access afficheraient 'NONE/504 ou 'NONE/502

Ligne de log d'Access témoin :

1233658928.496 153185 10.10.70.50 **NONE/504** 1729 OBTIENNENT http://www.example.com/ - www.example.com DIRECT - .....

Il y a beaucoup de raisons pour lesquelles WSA peut renvoyer une erreur de dépassement de délai de 502 ou 504 passerelles. Bien que ces réponses d'erreur soient semblables, il est important de comprendre les différences subtiles entre elles.

Voici quelques exemples des types de scénarios qui peuvent se produire :

- **502** : Le WSA a tenté d'établir une connexion TCP avec le web server, mais n'a pas reçu un SYN/ACK.
- **504** : Le WSA reçoit une Réinitialisation TCP (RST) terminant la connexion avec le web server.
- **504** : Le WSA n'obtient pas une réponse d'un service exigé avant de communiquer avec le web server, tel que des DN manque.
- **504** : Le WSA a établi une connexion TCP avec le web server et a envoyé une demande GET, mais le WSA ne reçoit jamais la réponse de HTTP.

Sont ci-dessous les exemples de chaque scénario et de plus de détails concernant des éventuels problèmes :

502 : Le WSA a tenté d'établir une connexion TCP avec le web server, mais n'a pas reçu un SYN/ACK.
Si le web server ne répond pas aux paquets de la synchronisation du WSA, après que des tentatives, le client soient envoyées à une erreur de dépassement de délai de 502 passerelles. Les causes typiques pour ceci sont : **1.** Le web server ou le réseau de web server a des questions. **2.** Un problème de réseau sur le réseau WSA empêche les paquets de synchronisation d'obtenir à l'Internet. **3.** Un Pare-feu ou un périphérique semblable relâche les paquets de synchronisation WSA ou le

SYN/ACK du web server
4. L'usurpation d'adresse IP est activée sur le WSA, mais n'est pas correctement configurée (aucune redirection de chemin de retour)

Étapes de dépannage :

La première étape est de vérifier si le WSA peut ping d'ICMP le web server. Ceci peut être fait à l'aide de la commande suivante CLI :
Ping www.example.com WSA>
Si le ping échoue, il ne signifie pas que le serveur est en panne. Il peut signifier que les paquets d'ICMP sont obtenir bloqué quelque part dans le chemin. Si le ping réussit, alors nous pouvons savoir à coup sûr que le WSA a un niveau layer3 de base de Connectivité au web server.
Un test de telnet vérifiera si le WSA a la capacité d'établir une connexion TCP sur le port 80 au web server. Voyez les instructions plus loin en cet article pour exécuter un test de telnet.

Bloc de problèmes de réseau ou de Pare-feu
Si le ping est réussi, mais le telnet échoue, il y a une bonne possibilité qu'un périphérique de filtrage, tel qu'un Pare-feu, empêche ce trafic d'obtenir par le réseau. L'il est recommandé que les journaux du pare-feu et/ou les captures de paquet du Pare-feu sont analysés d'autres détails.
Enable d'usurpation d'adresse IP, mais pas correctement configuré
Si proxying explicitement par le WSA ou le test de telnet est réussi, ceci affiche que le WSA peut communiquer directement au web server, mais quand des proxys d'un client par le WSA avec l'usurpation d'adresse IP, il y a un problème.

Sans usurpation d'adresse IP de client :

- Le WSA envoie une synchronisation au web server utilisant sa propre adresse IP comme source. Quand le paquet revient, il va directement au WSA.

Avec l'usurpation d'adresse IP de client :

- Le WSA envoie la synchronisation, mais à la place, utilise l'IP du client comme source. Sans configuration réseau spéciale, le paquet de retour sera envoyé au client au lieu du WSA.
- Afin d'utiliser l'usurpation d'adresse IP de client, le réseau doit être configuré d'une manière très spécifique afin de faciliter que les paquets sont réorientés correctement. Si les paquets de chemin de retour de web server sont envoyés au client au lieu du WSA, le WSA ne verra jamais les serveurs SYN/ACK et enverra une erreur de dépassement de délai de 502 passerelles de nouveau au client.

504 : Le WSA reçoit une Réinitialisation TCP (RST) terminant la connexion avec le web server.

Si le WSA reçoit un paquet de Réinitialisation TCP sur sa connexion en amont au web server, le WSA enverra une erreur de dépassement de délai de 504 passerelles au client.

Les causes typiques pour ceci sont :
1. Cisco posent 4 que le moniteur du trafic (L4TM) bloque le proxy WSA de connecter le web server.
2. Un Pare-feu, les ID, l'IPS, ou tout autre périphérique d'inspection de paquet bloque le WSA.

Étapes de dépannage :
Déterminez d'abord si le TCP RST provient le L4TM ou d'un autre périphérique.
Si le L4TM bloque ce trafic, le trafic apparaîtra dans les états GUI sous le « ***moniteur - > moniteur du trafic L4*** ». Autrement, le RST provient un différent périphérique.
Blocage L4TM :
L'il est recommandé que si le L4TM bloque, ne bloquent pas sur des ports que le proxy WSA

s'exécute également en fonction. Il y a de plusieurs raisons pour ceci :
1. Le proxy WSA fournit un message d'erreur amical dans le cas du problème, au lieu juste du TCP remettant à l'état initial la connexion. Ceci aidera la confusion de limite des utilisateurs finaux quand ils sont bloqués.
2. Le proxy WSA a la capacité de balayer et bloquer le contenu spécifique, tandis que le L4TM bloque tout le trafic appariant une adresse IP mise sur la liste noire.
Afin de configurer le L4TM pour ne pas bloquer sur des ports de proxy, allez au « ***GUI - > des Services de sécurité - > moniteur du trafic L4*** ».
Si le site est un mauvais site Web connu, mais il y a des raisons pour lesquelles on devrait permettre le trafic, le site peut être blanc répertorié dans :
« ***GUI - > gestionnaire de sécurité Web - > moniteur du trafic L4 - > permettez la liste*** »

Pare-feu/ID/IPS de blocage :
Si un autre périphérique sur le réseau bloque le WSA de se connecter au web server, il est recommandé d'analyser ce qui suit :
1. Logs de bloc de Pare-feu
2. Captures de paquet d'entrée/de sortie pendant le problème

Les logs de bloc peuvent rapidement confirmer si le périphérique bloque le WSA. Parfois un Pare-feu, un IPS, ou des ID bloqueront le trafic et ne se connecteront pas le convenablement. Si c'est le cas, la seule manière de prouver où le TCP RST provient, est d'obtenir des captures d'entrée et de sortie du périphérique. Si un RST est envoyé l'interface d'entrée et paquet ne voyageait pas par le côté de sortie, le périphérique de sécurité est certainement la cause.

504 : Le WSA a établi une connexion TCP avec le web server et a envoyé une demande GET, mais le WSA ne reçoit jamais la réponse de HTTP.

Si le WSA envoie un HTTP OBTENEZ, mais ne recevez jamais une réponse, il enverra une erreur de dépassement de délai de 504 passerelles au client.

Les causes typiques pour ceci sont :

- Un Pare-feu, les ID, l'IPS, ou tout autre périphérique d'inspection de paquet permet la connexion TCP, mais bloque le contenu de HTTP d'atteindre le web server. Dans ce cas, le test de telnet peut aider à isoler que le genre de données de HTTP est bloqué.

Les logs de bloc de Pare-feu peuvent rapidement confirmer si/pourquoi le périphérique bloque le WSA. Parfois un Pare-feu, un IPS, ou des ID bloqueront le trafic et ne se connecteront pas le convenablement. Si c'est le cas, la seule manière de prouver où le TCP RST provient, est d'obtenir des captures d'entrée et de sortie du périphérique. Si un RST est envoyé l'interface d'entrée et paquet ne voyageait pas par le côté de sortie, le périphérique de sécurité est certainement la cause.

Test de la connectivité avec un web server utilisant le telnet

Du WSA CLI, exécutez la **commande telnet** :
Telnet WSA>
Sélectionnez s'il vous plaît dont reliez-vous veulent au telnet.
1. Automatique
2. Gestion (192.168.15.200/24 : wsa.hostname.com)
3. P1 (192.168.113.199/24 : data.com)
[1]> **3**

Écrivez l'adresse Internet ou l'adresse IP distante.
[] > www.example.com

Entrez dans le port distant.
[25]> 80

Essayant 10.3.2.99…
Connecté à www.example.com.
Le caractère d'échappement est « ^] ».

Remarque: Le message « connecté » en rouge, indique que TCP avec succès établi entre le WSA et le web server.

Une demande de HTTP peut manuellement être aussi bien envoyée par cette session de telnet. Ce qui suit est une demande d'échantillon qui peut être tapée après le message « connecté » :

OBTENEZ http://www.example.com HTTP/1.1
HÔTE : www.example.com
{Entrez}

Remarque: Veillez à ajouter le retour chariot supplémentaire à l'extrémité, autrement le serveur ne répondrez pas à la demande.