Dépannage de la saturation des ports lors de l'utilisation de la traduction d'adresses de port avec les composants Umbrella

Table des matières

Introduction

Ce document décrit les clients Umbrella qui utilisent des clients itinérants et/ou des appareils virtuels et rencontrent des problèmes d'épuisement des ports dans les pare-feu qui utilisent la traduction d'adresses de port. Cela est le plus probable dans les environnements qui ont un grand nombre de clients itinérants et/ou un volume élevé de trafic s'exécutant à travers les VA. Les symptômes peuvent inclure des requêtes DNS renvoyées lentement ou une temporisation.

Causes

Ni les clients itinérants ni les appareils virtuels ne mettent en cache les réponses aux requêtes DNS. En outre, les clients itinérants envoient fréquemment des requêtes DNS « d'exploration » pour analyser l'environnement réseau et effectuer des contrôles d'intégrité.

Recommandations

- Assurez-vous que vos domaines internes sont correctement configurés dans Gestion des domaines sur votre tableau de bord Umbrella. Ils doivent contenir votre zone Active Directory (et/ou d'autres zones internes) afin de réduire le volume des requêtes à haute fréquence.
- Passez en revue certains paramètres PAT du pare-feu :
    - Un délai d'attente de session UDP trop long peut être un problème. Nous recommandons généralement des délais d'expiration de session UDP d'environ 15 secondes. Cependant, notez que si le protocole UDP est largement utilisé par d'autres applications sur votre réseau, elles peuvent avoir des délais d'attente plus longs que vous devez prendre en compte.
    - Selon votre pare-feu, il est possible d'augmenter la taille de son pool PAT afin d'augmenter le nombre de connexions simultanées.
- Si vous avez des adresses IP que vous pouvez dédier aux VA, utilisez la NAT 1:1 au lieu de

la PAT sur le pare-feu. Remarque : "NAT 1:1" est parfois appelé "NAT direct", mais c'est un nom erroné ; le terme technique correct est « NAT 1:1 ».
- Vérifiez vos limites de connexion par IP. Souvent, une politique qui ne devrait pas s'appliquer à l'appareil en question est en effet l'application d'une limite. Reportez-vous à la section suivante pour savoir comment confirmer.

Vérifier les limites de connexion par IP sur un ASA

Suivez les étapes ci-dessous :

- Configurez l'ASA avec une capture pour voir pourquoi les paquets ont été abandonnés par le pare-feu :

```
capture asp type asp-drop all match ip any host 208.67.222.222
```

- Recherchez les paquets abandonnés pour l'adresse IP en question. Un motif de limite de connexion apparaît sous la forme « Raison de suppression : (conn-limit)"
- Examinez la limite de connexion de l'hôte à l'aide de la commande :

```
show local-host detail | begin <IP Address of VA or roaming client>
```

    - Ce nombre est-il statique à une certaine limite (999) et n'augmente-t-il jamais ? Si tel est le cas, cela indique une limite de connexion.
- Vérifier si une politique de service est appliquée à ce service ; si vous le trouvez, consultez sa carte-politique :

```
show run service-policy, show policy-map NAME
```

    - Si vous trouvez un « NOM » de carte de stratégie qui définit la limite de connexion par hôte à 1000 (par exemple), cela entraîne l'abandon de tout nouveau paquet DNS du périphérique jusqu'à ce que davantage de connexions soient disponibles. Le protocole UDP est sans état et ne réessaie pas.
- Pour résoudre le problème, supprimez cette stratégie de service (aucun NOM de stratégie de service interne). Les connexions doivent commencer à dépasser la limite de 1000 (de notre exemple). Cela se produit plus rapidement pour une appliance virtuelle qu'un client itinérant.

Autres recommandations

Si ces recommandations n'aident pas, une solution de contournement possible serait :

1. Utilisez le rapport Umbrella dashboard —> Reporting —> Top Destinations pour identifier un ou plusieurs domaines ayant reçu un grand nombre de demandes au cours des dernières 24

heures.
2. Dans le tableau de bord Umbrella —> Configuration —> Gestion des domaines, ajoutez un ou plusieurs domaines de volume élevé à la liste, en définissant « S'applique à » sur « Tous les appareils et périphériques ».
3. Ensuite, les requêtes pour ces domaines sont transmises par les VA au DNS local. Idéalement, le DNS local doit être configuré pour transférer vers le DNS-parapluie à l'adresse 208.67.220.220/208.67.222.222, mais il peut être configuré pour transférer vers n'importe quel DNS externe.
4. Le DNS local gère les requêtes pour tous les domaines pour lesquels il fait autorité.
5. En supposant que le DNS local accepte les requêtes pour les domaines non locaux, les requêtes pour ces autres domaines sont transmises au DNS externe.

En effet, le serveur DNS local peut mettre en cache les résultats DNS, tandis que les clients et les appliances virtuels itinérants ne le font pas. Veuillez noter que l'utilisation de cette solution de contournement entraîne un trafic plus important et une charge plus lourde sur le DNS interne, donc surveillez-les attentivement pour vous assurer qu'ils ne sont pas surchargés.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.