ASA : L'accès entrant aux adresses NAT échoue après mise à jour à 8.4(3)

Contenu

Introduction

Ce document fournit des informations au sujet des adresses NAT qui échouent après évolution de l'appliance de sécurité adaptable (ASA) à la version 8.4(3). Ce document fournit également une résolution à cette question.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir la connaissance de ces thèmes.

- Compréhension de base du concept du Protocole ARP (Address Resolution Protocol) et du proxy ARP

Composants utilisés

Les informations dans ce document sont basées sur des ces matériel et versions de logiciel.

- Toute appliance de sécurité adaptatif de la gamme Cisco ASA 5500
- Version 8.4(3) ou ultérieures d'appliance de sécurité adaptable

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Symptômes

Commençant par la version 8.4(3) ASA, l'ASA ne répond pas aux demandes d'ARP reçues sur une interface, pour les IP address qui ne sont pas une partie de l'IP de sous-réseau de cette interface. Avant version 8.4(3), l'ASA répondrait aux demandes d'ARP qui n'étaient pas dans l'IP de sous-réseau de l'interface de l'ASA.

Cette modification peut se manifester juste après améliorer l'ASA à la version 8.4(3). Dans certains cas, les internautes ne peuvent pas se connecter à l'adresse globale d'un serveur traduit par l'ASA.

Ce message est affiché si cette situation est produite, et le « debug arp » est activé sur le CLI de l'ASA :

```
arp-in: Arp packet received from 192.168.10.1 which is in different subnet
than the connected interface 192.168.11.1/255.255.255.0
```

La cause principale de cette question n'est pas une bogue. Voyez les informations ci-dessous pour se renseigner plus sur des causes et des solutions potentielles à la question.

Conditions/environnement

Afin de rencontrer cette situation, l'ASA doit recevoir une demande d'ARP d'une adresse IP qui apparie une adresse globale dans une traduction NAT configurée. L'adresse IP globale doit résider dans un IP de sous-réseau qui est différente de l'IP de sous-réseau configuré sur l'interface de l'ASA.

Cause/description du problème

Afin de comprendre les pleines ramifications de cette question, il est important d'obtenir une compréhension complète de la façon dont ce numéro peut apparaître et la meilleure manière d'atténuer le problème.

Ce sont quelques exemples où cette situation peut être produite :

Le périphérique en amont a des artères IP configurées sans l'adresse IP de prochain-saut

C'est probablement la plupart de cause classique de cette situation. Il est dû à une configuration non-optimale d'un périphérique en amont. On le préfère configurer l'IP conduit tels que le prochain saut de l'artère IP est une adresse IP dans le même sous-réseau que l'adresse de cette interface :

```
ip route 10.1.2.0 255.255.255.0 192.168.1.2
```

Cependant, parfois les administrateurs réseau configurent une interface au lieu d'une adresse IP comme prochain saut :

```
ip route 10.1.2.0 255.255.255.0 FastEthernet0/1
```

Ceci fait conduire le routeur le trafic destiné au réseau 10.1.2.0/24 à l'interface FastEthernet0/1, et envoie une demande d'ARP de l'adresse IP de destination dans le paquet IP. On le suppose qu'un certain périphérique répondra à la demande d'ARP, et le routeur puis en avant le paquet à l'adresse MAC qui était due résolu au processus d'ARP. Les avantages de ce type de configuration est qu'il est très facile de configurer et gérer. L'administrateur ne doit pas

explicitement configurer une prochaine adresse IP de saut pour l'artère, et ils supposent qu'un périphérique contigu aura le proxy-arp activé et répondra à la demande d'ARP s'il est capable du routage les paquets à l'adresse IP de destination.

Cependant, il y a des sérieux problème avec ce type de configuration de route IP :

- En envoyant une demande d'ARP de déterminer le prochain saut pour le trafic IP, le routeur est exposé aux problèmes provoqués par d'autres périphériques qui pourraient inexactement répondre à cette demande d'ARP. Le résultat est le trafic peut noir-être troué une fois envoyé à un périphérique incorrect.
- L'artère fera envoyer le périphérique une demande d'ARP de chaque seule adresse de destination dans les paquets qui apparient l'artère. Ceci peut entraîner un grand nombre de trafic ARP sur le sous-réseau et négativement affecter la représentation aussi bien que l'espace mémoire exigé pour tenir potentiellement un grand nombre d'entrées d'un ARP.
- Puisque l'espace de table ARP est une ressource attachée en mémoire, un nombre excessif d'entrées peut négativement affecter la représentation du routeur et stabilty.

Par conséquent, la pratique recommandée est de configurer toutes les artères avec les adresses du prochain saut explicites IP et de ne pas utiliser les artères qui ont un nom d'interface par lui-même pour identifier l'interface sortante. Si l'interface est nécessaire pour attacher l'artère à l'interface de sortie pour le Basculement, entrez dans chacun des deux le nom d'interface de sortie et le prochain saut dans l'artère statique.

Etant donné les implications administratives pour quelques clients de Cisco, une demande d'amélioration a été ouverte afin de rendre le nouveau comportement sécurisé configurable : ID de bogue Cisco CSCty95468 (clients enregistrés seulement) (ENH : Ajoutez la commande de permettre le cache entries d'ARP des sous-réseaux Non-connectés).

Masques mal adaptés d'IP de sous-réseau sur des périphériques contigus

Les masques mal adaptés d'IP de sous-réseau configurés sur l'interface de l'ASA et l'interface de périphérique contigu peuvent entraîner une situation semblable. Si le périphérique contigu avait un masque de sous-réseau qui était des super-réseaux (255.255.240.0) du masque de sous-réseau IP de l'interface de l'ASA (255.255.255.0), le périphérique contigu ARP pour les adresses IP qui ne sont pas dans l'IP de sous-réseau d'interface ASA. Assurez-vous que les masques de sous-réseau sont corrects.

Implications de mode transparent

Un autre effet secondaire de cette modification est l'incapacité d'apprendre des adresses MAC des sous-réseaux non-direct-connectés en mode transparent. Ceci affecte la transmission dans ces scénarios :

- L'ASA transparente n'a pas une adresse IP de Gestion configurée ou la configuration est incorrecte.
- L'ASA transparente utilise des sous-réseaux secondaires sur le même segment.

Il n'y a aucun contournement pour cette question en mode transparent autre que le downgrade. Cependant, cette demande d'amélioration a été ouverte afin de faire l'ASA interopérer avec des sous-réseaux secondaires en mode transparent : ID de bogue Cisco CSCty49855 (clients enregistrés seulement) (ENH : Hôtes connectés de support non directement dans le mécanisme de détection de MAC).

Résolution

La solution au problème (dans le cas que l'adresse IP en question n'est pas dans le même sous-réseau layer-3 que l'IP de l'interface de l'ASA) est d'apporter les modifications nécessaires de s'assurer que les périphériques à côté de l'artère ASA trafiquent directement à l'adresse IP de l'interface de l'ASA comme prochain périphérique de saut, au lieu de compter sur un périphérique au proxy-arp au nom de l'adresse IP.

Informations connexes

- Support et documentation techniques - Cisco Systems