L'utilisation du processeur ASA est élevée en raison d'une boucle de trafic lorsque les clients VPN se déconnectent

Contenu

Introduction

Ce document décrit un problème courant qui se produit lorsque des clients VPN se déconnectent d'un appareil de sécurité adaptatif (ASA) Cisco qui fonctionne comme une tête de réseau VPN d'accès à distance. Ce document décrit également la situation dans laquelle une boucle de trafic se produit lorsque les utilisateurs VPN se déconnectent d'un pare-feu ASA. Ce document ne couvre pas la façon de configurer ou de configurer l'accès à distance au VPN, seulement la situation spécifique qui provient de certaines configurations de routage courantes.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN d'accès à distance sur l'ASA
- Concepts de routage de couche 3 de base

Components Used

Les informations de ce document sont basées sur un modèle ASA 5520 qui exécute le code ASA version 9.1(1).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Ce document peut être utilisé avec les versions matérielles et logicielles suivantes :

- Tout modèle ASA
- Toute version de code ASA

Informations générales

Lorsqu'un utilisateur se connecte à l'ASA en tant que concentrateur VPN d'accès à distance, l'ASA installe une route basée sur l'hôte dans la table de routage ASA qui achemine le trafic vers ce client VPN depuis l'interface externe (vers Internet). Lorsque cet utilisateur se déconnecte, la route est supprimée de la table et les paquets du réseau interne (destinés à cet utilisateur VPN déconnecté) peuvent être bouclés entre l'ASA et un périphérique de routage interne.

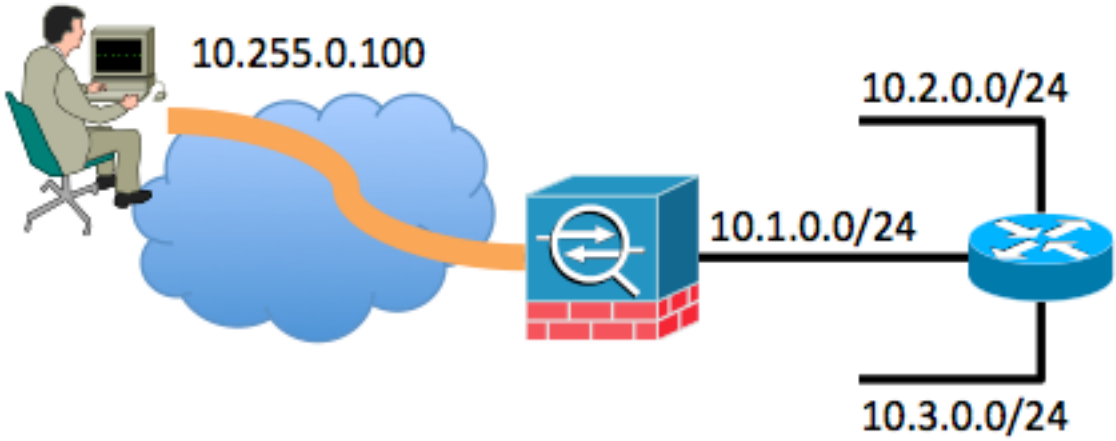
Un autre problème est que les paquets de diffusion dirigés (réseau) (générés par la suppression des clients VPN) peuvent être transférés par l'ASA en tant que trame de monodiffusion vers le réseau interne. Cela peut le renvoyer à l'ASA, ce qui entraîne le bouclage du paquet jusqu'à l'expiration de la durée de vie (TTL).

Ce document explique ces problèmes et indique quelles techniques de configuration peuvent être utilisées afin d'éviter le problème.

Problème : Paquets destinés à une boucle client VPN déconnectée à l'intérieur d'un réseau interne

Lorsqu'un utilisateur VPN d'accès à distance se déconnecte d'un pare-feu ASA, les paquets toujours présents sur le réseau interne (destinés aux utilisateurs déconnectés) et l'adresse IP VPN attribuée peuvent devenir bouclés dans le réseau interne. Ces boucles de paquets peuvent entraîner une augmentation de l'utilisation du CPU sur l'ASA jusqu'à ce que la boucle s'arrête soit en raison de la valeur TTL IP dans l'en-tête de paquet IP décrémentant à 0, soit que l'utilisateur se reconnecte et que l'adresse IP soit réattribuée à un client VPN.

Afin de mieux comprendre ce scénario, considérez cette topologie :



Dans cet exemple, l'adresse IP 10.255.0.100 a été attribuée au client d'accès distant. L'ASA dans cet exemple est connecté au même segment de réseau interne avec un routeur. Deux segments réseau de couche 3 supplémentaires sont connectés au routeur. Les configurations d'interface (routage) et de VPN de l'ASA et du routeur sont illustrées dans les exemples.

Les points forts de la configuration ASA sont présentés dans cet exemple :

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

Les points forts de la configuration du routeur sont présentés dans cet exemple :

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

La table de routage du routeur connecté à l'intérieur de l'ASA a simplement une route par défaut pointée vers l'interface interne de l'ASA de 10.1.0.1.

Pendant que l'utilisateur est connecté via un VPN à l'ASA, la table de routage ASA affiche les

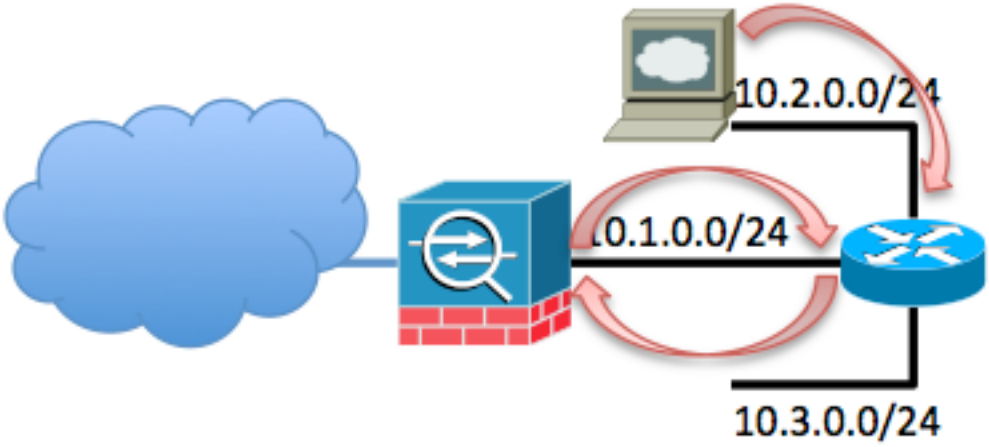
informations suivantes :

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Le problème se produit lorsque l'utilisateur VPN d'accès à distance se déconnecte du VPN. À ce stade, la route basée sur l'hôte est supprimée de la table de routage ASA. Si un hôte du réseau tente d'envoyer du trafic au client VPN, ce trafic est acheminé vers l'interface interne ASA par le routeur. Cette série d'étapes se produit :

1. Le paquet destiné à 10.255.0.100 arrive sur l'interface interne de l'ASA.
2. Les contrôles de liste de contrôle d'accès standard sont effectués.
3. La table de routage ASA est vérifiée afin de déterminer l'interface de sortie pour ce trafic.
4. La destination du paquet correspond à la route étendue 10.0.0.0/8 qui pointe vers le routeur en dehors de l'interface interne.
5. L'ASA vérifie si le trafic d'épilation est autorisé - il recherche **une autorisation de même sécurité à l'intérieur de l'interface** et constate qu'elle est autorisée.
6. Une connexion est établie vers et depuis l'interface interne et le paquet est renvoyé au routeur en tant que tronçon suivant.
7. Le routeur reçoit un paquet destiné à 10.255.0.100 sur l'interface qui fait face à l'ASA. Le routeur recherche dans sa table de routage un saut suivant approprié. Le routeur détecte que le saut suivant serait l'interface interne ASA et que le paquet est envoyé à l'ASA.
8. Revenez à l'étape 1.

Un exemple est montré ici :



Cette boucle se produit jusqu'à ce que la durée de vie de ce paquet décrémente à 0. Notez que le pare-feu ASA **ne** décrémente **pas** la valeur TTL par défaut lorsqu'il traite un paquet. Le routeur décrémente la durée de vie au fur et à mesure qu'il achemine le paquet. Ceci empêche l'occurrence de cette boucle indéfiniment, mais cette boucle augmente la charge de trafic sur l'ASA et entraîne une augmentation de l'utilisation du CPU.

Problème : Les paquets de diffusion dirigés (réseau) générés par des clients VPN sont bouclés sur un réseau interne

Ce problème est similaire au premier problème. Si un client VPN génère un paquet de diffusion dirigé vers son sous-réseau IP assigné (10.255.0.255 dans l'exemple précédent), ce paquet peut être transféré en tant que trame de monodiffusion par l'ASA au routeur interne. Le routeur interne peut ensuite le renvoyer à l'ASA, ce qui entraîne la boucle du paquet jusqu'à l'expiration de la durée de vie.

Cette série d'événements se produit :

1. La machine cliente VPN génère un paquet destiné à l'adresse de diffusion réseau 10.255.0.255, et le paquet arrive à l'ASA.
2. L'ASA traite ce paquet comme une trame de monodiffusion (en raison de la table de routage) et le transfère au routeur interne.

3. Le routeur interne, qui traite également le paquet comme une trame de monodiffusion, décrète la durée de vie du paquet et le renvoie à l'ASA.

4. Le processus se répète jusqu'à ce que la durée de vie du paquet soit réduite à 0.

Solutions au problème

Il existe plusieurs solutions possibles à ce problème. Selon la topologie du réseau et la situation spécifique, une solution peut être plus facile à mettre en oeuvre qu'une autre.

Solution 1 - Route statique pour interface Null0 (ASA version 9.2.1 et ultérieure)

Lorsque vous envoyez du trafic à une interface **Null0**, cela entraîne l'abandon des paquets

destinés au réseau spécifié. Cette fonctionnalité est utile lorsque vous configurez RTBH (Remote Triggered Black Hole) pour le protocole BGP (Border Gateway Protocol). Dans cette situation, si vous configurez une route vers Null0 pour le sous-réseau du client d'accès distant, il force l'ASA à abandonner le trafic destiné aux hôtes de ce sous-réseau si une route plus spécifique (fournie par Injection de route inverse) n'est pas présente.

```
route Null0 10.255.0.0 255.255.255.0
```

Solution 2 - Utiliser un pool d'adresses IP différent pour les clients VPN

Cette solution consiste à attribuer aux utilisateurs VPN distants une adresse IP qui ne chevauche aucun sous-réseau de réseau interne. Cela empêcherait l'ASA de transférer les paquets destinés à ce sous-réseau VPN vers le routeur interne si l'utilisateur VPN n'était pas connecté.

Solution 3 - Rendre la table de routage ASA plus spécifique aux routes internes

Cette solution consiste à s'assurer que la table de routage de l'ASA ne comporte pas de routes très larges qui chevauchent le pool IP VPN. Pour cet exemple de réseau spécifique, supprimez la route 10.0.0.0/8 de l'ASA et configurez des routes statiques plus spécifiques pour les sous-réseaux qui résident hors de l'interface interne. En fonction du nombre de sous-réseaux et de la topologie du réseau, il peut s'agir d'un grand nombre de routes statiques et cela peut ne pas être possible.

Solution 4 : ajout d'une route plus spécifique pour le sous-réseau VPN sortant de l'interface externe

Cette solution est plus compliquée que les autres décrites dans ce document. Cisco vous recommande d'essayer d'utiliser les autres solutions d'abord en raison de la situation décrite dans la note plus loin dans cette section. Cette solution est d'empêcher l'ASA de transférer les paquets IP provenant du sous-réseau IP VPN au routeur interne ; vous pouvez le faire si vous ajoutez une route plus spécifique pour le sous-réseau VPN à partir de l'interface externe. Puisque ce sous-réseau IP est réservé aux utilisateurs VPN externes, les paquets avec une adresse IP source de ce sous-réseau IP VPN ne doivent jamais arriver en entrée sur l'interface interne ASA. La façon la plus simple d'y parvenir est d'ajouter une route pour le pool d'adresses IP VPN d'accès distant en dehors de l'interface externe avec une adresse IP de tronçon suivant du routeur FAI en amont.

Dans cet exemple de topologie de réseau, cette route ressemblerait à ceci :

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

En plus de cette route, ajoutez la commande **ip verify inverse-path inside** afin que l'ASA abandonne tous les paquets reçus en entrée sur l'interface interne provenant du sous-réseau IP VPN en raison de la route la plus préférée qui existe sur l'interface externe :

```
ip verify reverse-path inside
```

Une fois ces commandes implémentées, la table de routage ASA ressemble à ceci lorsque l'utilisateur est connecté :

```
ASA# show route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Lorsque le client VPN est connecté, la route basée sur l'hôte vers cette adresse IP VPN est présente dans la table et est préférée. Lorsque le client VPN se déconnecte, le trafic provenant de l'adresse IP du client qui arrive sur l'interface interne est comparé à la table de routage et abandonné en raison de la commande **ip verify inverpath inside**.

Si le client VPN génère une diffusion réseau dirigée vers le sous-réseau IP VPN, ce paquet est transféré au routeur interne et renvoyé par le routeur vers l'ASA, où il est abandonné en raison de la commande **ip verify inverpath inside**.

> **Note**: Une fois cette solution implémentée, si la commande **same-security permit intra-interface** est présente dans la configuration et que les stratégies d'accès l'autorisent, le trafic provenant d'un utilisateur VPN et destiné à une adresse IP dans le pool IP VPN pour un utilisateur non connecté peut être routé hors de l'interface externe en texte clair. Il s'agit d'une situation rare qui peut être atténuée par l'utilisation de filtres VPN dans la politique VPN. Cette situation se produit uniquement si la commande **same-security permit intra-interface** est présente dans la configuration de l'ASA.
>
> De même, si les hôtes internes génèrent du trafic destiné à une adresse IP dans le pool VPN et que cette adresse IP n'est pas attribuée à un utilisateur VPN distant, ce trafic peut sortir de l'extérieur de l'ASA en texte clair.