L'ASA a l'utilisation du CPU élevée due à une boucle du trafic quand débranchement de clients vpn

Contenu

Introduction

Ce document décrit un problème courant qui se produit quand le démonter de clients vpn d'une appliance de sécurité adaptable Cisco (ASA) cette fonctionne comme headend de l'Accès à distance VPN. Ce document décrit également la situation où une boucle du trafic se produit quand débranchement d'utilisateurs VPN d'un Pare-feu ASA. Ce document ne couvre pas comment configurer ou Accès à distance d'installation au VPN, seulement la situation spécifique qui résulte de certaines configurations communes de routage.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration du VPN d'Accès à distance sur l'ASA
- Concepts de acheminement de la couche 3 de base

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Ce document peut être utilisé avec des ces matériel et versions de logiciel :

- Tout modèle ASA
- Toute version de code ASA

Informations générales

Quand un utilisateur se connecte à l'ASA comme concentrateur de l'Accès à distance VPN, l'ASA installe une artère gérée par le système central dans la table de routage ASA qui conduit le trafic à ce client vpn hors de l'interface extérieure (vers l'Internet). Quand des débranchements de cet utilisateur, l'artère est enlevés de la table, et les paquets sur le réseau intérieur (destiné à cet utilisateur déconnecté VPN) pourrait être fait une boucle entre l'ASA et un périphérique interne de routage.

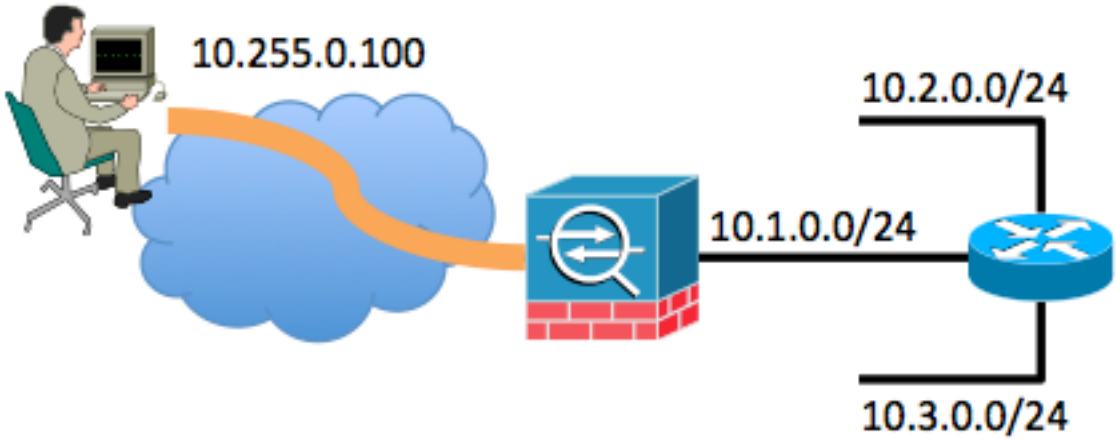
Un autre problème est que des paquets dirigés d'émission (de réseau) (générés par la suppression des clients vpn) pourraient être expédiés par l'ASA comme trame de monodiffusion vers le réseau interne. Ceci pourrait l'expédier de nouveau à l'ASA, qui cause le paquet d'être fait une boucle jusqu'à ce que le Time to Live (TTL) expire.

Ce document explique ces questions et affiche quelles techniques de configuration peuvent être utilisées afin d'empêcher le problème.

Problème : Paquets destinés pour une boucle déconnectée de client vpn à l'intérieur de réseau interne

Quand les démonter d'un utilisateur de l'Accès à distance VPN d'un Pare-feu ASA, les paquets encore actuels sur le réseau interne (destiné pour ces utilisateurs déconnectés) et l'adresse de l'adresse IP attribuée VPN pourraient devenir faits une boucle dans le réseau interne. Ces boucles de paquet pourraient faire augmenter l'utilisation du CPU sur l'ASA jusqu'aux arrêts bouclés ou dus à la valeur d'IP TTL dans l'en-tête de paquet IP décrémentant de 0, ou l'utilisateur rebranche et l'adresse IP est attribuée à nouveau à un client vpn.

Afin de comprendre ce scénario mieux, considérez cette topologie :



Dans cet exemple, le client d'Accès à distance a été assigné l'adresse IP de 10.255.0.100. L'ASA dans cet exemple est connectée à la même chose segment de réseau d'intérieur avec un routeur. Le routeur a deux segments supplémentaires de réseau de la couche 3 connectés à lui. L'interface appropriée (routage) et des configurations du VPN de l'ASA et du routeur sont affichées dans les exemples.

Des points culminants de configuration ASA sont affichés 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
```

Des points culminants de configuration de routeur sont affichés 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 un default route indiqué l'interface interne ASA de 10.1.0.1.

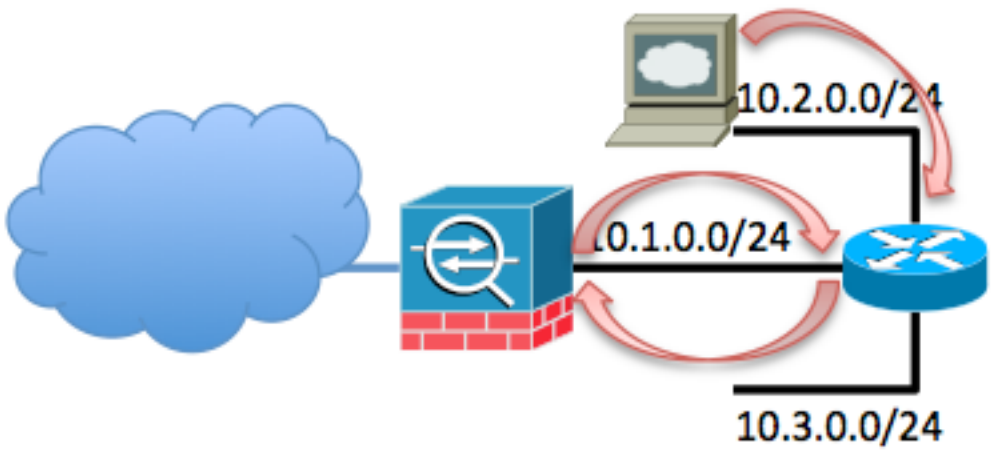
Tandis que l'utilisateur est connecté par l'intermédiaire du VPN à l'ASA, la table de routage ASA affiche comme suit :

```
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 pose quand les débranchements d'utilisateur de l'Accès à distance VPN du VPN. En ce moment, l'artère gérée par le système central est retirée de la table de routage ASA. Si un hôte à l'intérieur des tentatives de réseau d'envoyer le trafic au client vpn, ce trafic est conduit à l'interface interne ASA par le routeur. Cette gamme d'étapes se produit :

1. Le paquet destiné à 10.255.0.100 arrive sur l'interface interne de l'ASA.
2. Des contrôles standard d'ACL sont exécutés.
3. La table de routage ASA est vérifiée afin de déterminer l'interface de sortie pour ce trafic.
4. La destination du paquet apparie la large artère 10.0.0.0/8 que les points soutiennent de l'interface interne vers le routeur.
5. L'ASA vérifie si des cheveux goupillant le trafic sont permis - ils recherchent l'**autorisation de même-Sécurité intra-interface** et les découvertes qu'on leur permet.
6. Une connexion est établie à et de l'interface interne et le paquet est renvoyé au routeur comme prochain saut.
7. Le routeur reçoit un paquet destiné à 10.255.0.100 sur l'interface qui fait face à l'ASA. Le routeur vérifie sa table de routage pour un prochain saut approprié. Les découvertes de routeur que le prochain saut serait l'interface interne ASA, et le paquet est envoyées à l'ASA.
8. Revenez à l'étape 1.

Un exemple est montré ici :



Cette boucle se produit jusqu'à ce que le TTL de ce paquet décrémente à 0. Notez que le Pare-feu ASA ne décrémente pas la valeur de TTL par défaut quand il traite un paquet. Le routeur décrémente le TTL pendant qu'il conduit le paquet. Ceci empêche l'occurrence de cette boucle indéfiniment, mais cette boucle augmente la charge de la circulation sur l'ASA et fait clouer l'utilisation du CPU.

Problème : Des paquets dirigés d'émission (de réseau) générés par des clients vpn sont faits une boucle sur un réseau intérieur

Cette question est semblable au premier problème. Si un client vpn génère un paquet de diffusion dirigée à son sous-réseau d'adresse IP attribuée (10.255.0.255 dans l'exemple précédent), alors ce paquet pourrait être expédié comme trame de monodiffusion par l'ASA au routeur interne. Le routeur interne pourrait alors l'expédier de nouveau à l'ASA, qui fait faire une boucle le paquet jusqu'à ce que le TTL expire.

Cette gamme d'événements se produit :

1. L'ordinateur de client vpn génère un paquet destiné à l'adresse 10.255.0.255 de diffusion réseau, et le paquet arrive à l'ASA.
2. L'ASA traite ce paquet comme trame de monodiffusion (due à la table de routage) et en avant elle au routeur interne.

3. Le routeur interne, qui traite également le paquet comme trame de monodiffusion, décrémente le TTL du paquet et en avant de lui de nouveau à l'ASA.

4. Les répétitions de processus jusqu'au TTL du paquet est réduites à 0.

Solutions au problème

Il y a plusieurs solutions potentielles à cette question. Selon la topologie du réseau et la situation spécifique, il pourrait être plus facile implémenter une solution que des autres.

Artère statique de la solution 1 pour l'interface Null0 (version 9.2.1 et ultérieures ASA)

Quand vous envoyez le trafic à une interface **Null0**, elle entraîne les paquets destinés au réseau spécifié à abandonner. Cette caractéristique est utile quand vous configurez le trou noir à distance déclenché (RTBH) pour le Protocole BGP (Border Gateway Protocol). Dans cette situation, si vous configurez une artère à Null0 pour le sous-réseau de client d'Accès à distance, il force l'ASA pour relâcher le trafic destiné aux hôtes dans ce sous-réseau si plus d'artère spécifique (fournie par le Reverse Route Injection) n'est pas présente.

```
route Null0 10.255.0.0 255.255.255.0
```

Solution 2 - Utilisez un différent pool d'IP pour des clients vpn

Cette solution est d'assigner aux utilisateurs du distant VPN une adresse IP qui ne superpose avec aucun sous-réseau de réseau interne. Ceci empêcherait l'ASA des transferts des paquets destinés à ce sous-réseau VPN de nouveau au routeur interne si l'utilisateur VPN n'était pas

connecté.

Solution 3 - Rendez le Tableau de routage ASA plus spécifique pour des routes internes

Cette solution est de s'assurer que la table de routage de l'ASA n'a aucune artère très large qui superposent avec le pool d'IP VPN. Pour cet exemple spécifique de réseau, retirez l'artère 10.0.0.0/8 de l'ASA et configurez plus d'artères statiques spécifiques pour les sous-réseaux qui résident hors fonction de l'interface interne. La personne à charge sur le nombre de sous-réseaux et de la topologie du réseau, ceci pourrait être un grand nombre d'artères de charge statique et il ne pourrait pas être possible.

Solution 4 - Ajoutez plus d'artère spécifique pour le sous-réseau VPN soutiennent de l'interface extérieure

Cette solution est plus compliquée qui les autres qui sont décrites dans ce document. Cisco recommande que vous tentiez d'utiliser les autres solutions d'abord dues à la situation qui est décrite dans la note plus tard dans cette section. Cette solution est d'empêcher l'ASA des paquets IP d'expédition originaires de l'IP de sous-réseau VPN de nouveau au routeur interne ; vous pouvez faire ceci si vous ajoutez plus d'artère spécifique pour le sous-réseau VPN hors de l'interface extérieure. Puisque cet IP de sous-réseau est réservé pour les utilisateurs extérieurs VPN, les paquets avec une adresse IP source de cet IP de sous-réseau VPN devraient ne jamais arriver d'arrivée sur l'interface interne ASA. Le moyen le plus simple de réaliser ceci est d'ajouter une artère pour le pool d'IP de l'Accès à distance VPN hors de l'interface extérieure avec une prochaine adresse IP de saut du routeur de l'ISP en amont.

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

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

En plus de cette artère, ajoutez l'**IP vérifient le chemin inverse à l'intérieur de la** commande afin de faire relâcher l'ASA tous les paquets a reçu d'arrivée sur l'interface interne originaire de l'IP de sous-réseau VPN dû à plus de route préférée qui existe sur l'interface extérieure :

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

Après que ces commandes implemeted, la table de routage ASA semble semblable à ceci quand 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
```

Quand le client vpn est connecté, l'artère gérée par le système central à cette adresse IP VPN est présente dans la table et est préférée. Quand le client vpn déconnecte, trafiquez originaire de cette adresse IP de client qui arrive sur l'interface interne est vérifiée contre la table de routage et en raison relâchés de l'**IP vérifient le chemin inverse à l'intérieur de la** commande.

Si le client vpn génère une diffusion réseau dirigée à l'IP de sous-réseau VPN, alors ce paquet est expédié au routeur interne et expédié par le routeur de nouveau à l'ASA, où elle est due relâché à l'**IP vérifiez le chemin inverse à l'intérieur de la** commande.

> Remarque: Après que cette solution soit mise en application, si la commande **intra-interface d'autorisation de même-Sécurité** est présente dans la configuration et les stratégies d'accès la permettent, trafiquez originaire d'un utilisateur VPN destiné à une adresse IP du pool d'IP VPN pour un utilisateur qui n'est pas connecté pourrait être conduit soutiennent de l'interface extérieure en libellé. C'est une situation rare et peut être atténuée avec l'utilisation des VPN-filtres dans la règle VPN. Cette situation se produit seulement si la commande **intra-interface d'autorisation de même-Sécurité** est présente dans la configuration de l'ASA.
>
> De même, si les hôtes internes génèrent le trafic destiné à une adresse IP dans le groupe VPN et cette adresse IP n'est pas assignée à un utilisateur du distant VPN, ce trafic pourrait de sortie l'extérieur de l'ASA en libellé.