ASA 8.4(4) : Configuration NAT de certaine identité rejetée

Contenu

Introduction

L'exécution des appliances de sécurité adaptable (ASA) 8.4(4) ou plus élevé peut rejeter certaines configurations NAT et afficher un message d'erreur semblable à ceci :

```
ERROR: <mapped address range> overlaps with <interface> standby interface
   address
ERROR: NAT Policy is not downloaded
```

Ce problème peut également apparaître quand vous améliorez votre ASA à 8.4(4) ou plus élevé d'une release antérieure. Vous pouvez noter que quelques commandes NAT ne sont plus présentes dans le running-config de l'ASA. Dans ces exemples, vous devriez regarder les messages console imprimés afin de voir s'il y a des messages actuels dans le format ci-dessus.

Il se peut que vous notiez un autre effet, à savoir que le trafic de certains sous-réseaux derrière l'ASA peut cesser de traverser le(s) tunnel(s) du Réseau privé virtuel (VPN) se terminant au niveau de l'ASA. Ce document décrit comment résoudre ces problèmes.

Avant de commencer

Conditions requises

Ces conditions doivent être remplies afin de rencontrer ce problème :

- Version 8.4(4) ou ultérieures courante ASA, ou amélioré à la version 8.4(4) ou ultérieures d'une version antérieure.
- ASA configurée avec une adresse IP de réserve sur au moins une de ses interfaces.
- UN NAT est configuré avec l'interface ci-dessus comme l'interface tracée.

Composants utilisés

Les informations dans ce document sont basées sur cette version matérielle et logicielle :

- Exécution ASA 8.4(4) ou plus élevé

Conventions

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

Problème

Pendant que le message d'erreur suggère, si la plage d'adresses tracée dans une déclaration NAT statique inclut l'adresse IP « de réserve » assignée à l'interface tracée, la commande NAT est rejetée. Ce comportement a toujours existé pour la redirection de port statique, mais il a été aussi bien introduit pour des déclarations NAT linéaires statiques avec la version 8.4(4) comme difficulté pour l'ID de bogue Cisco CSCtw82147 (clients enregistrés seulement).

Cette bogue a été classée parce qu'avant 8.4(4) l'ASA a permis à des utilisateurs pour configurer l'adresse tracée dans une configuration NAT statique pour être les mêmes que l'adresse IP de réserve a assignés à l'interface tracée. Par exemple, regardez cet extrait de configuration d'une ASA :

```
ciscoasa(config)# show run int e0/0 ! interface Ethernet0/0 nameif vm security-level 0 ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2 ciscoasa(config)# show run nat ! object
network obj-10.76.76.160 nat (tftp,vm) static 192.168.1.2
```

Quoique la commande soit reçue, cette configuration NAT ne fonctionnera jamais à côté de conception. En conséquence, commençant par 8.4(4), l'ASA ne permet pas une telle règle NAT d'être configuré en premier lieu.

Ceci a eu comme conséquence un autre problème imprévu. Par exemple, considérez le scénario où l'utilisateur a un tunnel VPN se terminant sur l'ASA et veut permettre au sous-réseau de « intérieur » pour pouvoir parler au sous-réseau du distant VPN.

Entre d'autres commandes exigées pour configurer le tunnel VPN, une des configurations plus importantes est de s'assurer que le trafic entre les sous-réseaux VPN n'obtient pas NATed. Ceci est mis en application avec 8.3 et au-dessus d'utiliser un manuel/deux fois une commande NAT de ce format :

```
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
object network obj-192.168.1.0
 description Inside subnet
 subnet 192.168.1.0 255.255.255.0
object network obj-10.10.10.0
 description Remote VPN subnet
 subnet 10.10.10.0 255.255.255.0
!
nat (inside,any) source static obj-192.168.1.0 obj-192.168.1.0 destination
   static obj-10.10.10.0 obj-10.10.10.0
!
object network obj-192.168.1.0
 nat (inside,outside) dynamic interface
```

Quand cette ASA est mise à jour à 8.4(4) ou plus élevé, cette commande NAT ne sera pas présente dans le running-config de l'ASA et cette erreur sera imprimée sur la console de l'ASA :

```
ERROR: 192.168.1.0-192.168.1.255 overlaps with inside standby interface
   address
ERROR: NAT Policy is not downloaded
```

En conséquence, le trafic entre les sous-réseaux 192.168.1.0/24 et 10.10.10.0/24 ne traversera plus le tunnel VPN.

Solution

Il y a deux contournements possibles pour cette condition :

- Faites la commande NAT aussi précis que possible avant l'évolution à 8.4(4) ainsi l'interface tracée n'en est pas « ». Par exemple, la commande NAT ci-dessus peut être changée à l'interface par laquelle le sous-réseau du distant VPN est accessible (nommé « extérieur » dans le scénario ci-dessus) :`nat (inside,outside) source static obj-192.168.1.0 obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0`
- Si le contournement ci-dessus n'est pas possible, terminez-vous ces étapes :Quand l'ASA exécute 8.4(4) ou plus élevé, retirez l'adresse IP de réserve assignée à l'interface.Appliquez la commande NAT.Réappliquez l'adresse IP de réserve sur l'interface.Exemple :`ciscoasa(config)# interface Ethernet0/0 ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 ciscoasa(config-if)# exit ciscoasa(config)# nat (inside,any) 1 source static obj-192.168.1.0 obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0 ciscoasa(config)# interface Ethernet0/0 ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2`

Informations connexes

- Support et documentation techniques - Cisco Systems