

ASA 8.4(4) : Configuration NAT de certaines identités refusée

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Problème](#)

[Solution](#)

[Informations connexes](#)

Introduction

Les dispositifs de sécurité adaptatifs (ASA) exécutant la version 8.4(4) ou ultérieure peuvent rejeter certaines configurations NAT et afficher un message d'erreur similaire à celui-ci :

```
ERROR: <mapped address range> overlaps with <interface> standby interface
      address
```

```
ERROR: NAT Policy is not downloaded
```

Ce problème peut également apparaître lorsque vous mettez à niveau votre ASA vers la version 8.4(4) ou ultérieure à partir d'une version antérieure. Vous remarquerez peut-être que certaines commandes NAT ne sont plus présentes dans la configuration en cours de l'ASA. Dans ces cas, vous devez regarder les messages de console imprimés afin de voir s'il y a des messages présents 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 pour faire face à ce problème :

- ASA exécutant la version 8.4(4) ou ultérieure, ou mis à niveau vers la version 8.4(4) ou ultérieure à partir d'une version antérieure.
- ASA configuré avec une adresse IP de secours sur au moins une de ses interfaces.
- Une NAT est configurée avec l'interface ci-dessus comme interface mappée.

Components Used

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

- ASA exécutant 8.4(4) ou version ultérieure

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

Problème

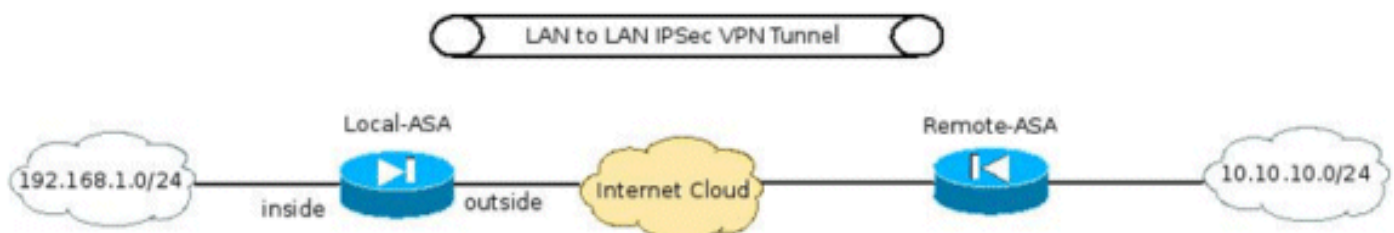
Comme l'indique le message d'erreur, si la plage d'adresses mappée d'une instruction NAT statique inclut l'adresse IP de secours attribuée à l'interface mappée, la commande NAT est rejetée. Ce comportement a toujours existé pour la redirection de port statique, mais il a été introduit pour les instructions NAT statiques un-à-un ainsi que pour la version 8.4(4) comme solution pour l'ID de bogue Cisco [CSCtw82147](#) (clients [enregistrés](#) uniquement).

Ce bogue a été signalé car avant la version 8.4(4), l'ASA permettait aux utilisateurs de configurer l'adresse mappée dans une configuration NAT statique de manière à ce qu'elle soit identique à l'adresse IP de secours attribuée à l'interface mappée. Par exemple, regardez cet extrait de configuration d'un 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
```

Même si la commande est acceptée, cette configuration NAT ne fonctionnera jamais par conception. Par conséquent, à partir de la version 8.4(4), l'ASA ne permet pas de configurer une telle règle NAT en premier lieu.

Cela a entraîné un autre problème imprévu. Par exemple, considérez le scénario dans lequel l'utilisateur a un tunnel VPN se terminant sur l'ASA et souhaite autoriser le sous-réseau « interne » à pouvoir parler au sous-réseau VPN distant.



Parmi les autres commandes requises pour configurer le tunnel VPN, une des configurations les plus importantes est de s'assurer que le trafic entre les sous-réseaux VPN n'est pas traité par NAT. Ceci est mis en oeuvre avec 8.3 et les versions ultérieures à l'aide d'une commande NAT

Manual/ Twice 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
```

Lorsque cet ASA est mis à niveau vers la version 8.4(4) ou ultérieure, cette commande NAT ne sera pas présente dans la configuration en cours de l'ASA et cette erreur sera imprimée sur la console ASA :

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

Par conséquent, le trafic entre les sous-réseaux 192.168.1.0/24 et 10.10.10.0/24 ne passera plus par le tunnel VPN.

Solution

Cette condition peut faire l'objet de deux solutions :

- Rendre la commande NAT aussi spécifique que possible avant de passer à la version 8.4(4), de sorte que l'interface mappée ne soit pas « any ». Par exemple, la commande NAT ci-dessus peut être modifiée en interface par laquelle le sous-réseau VPN distant est accessible (nommé « outside » 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 la solution de contournement ci-dessus n'est pas possible, procédez comme suit :Lorsque l'ASA exécute 8.4(4) ou une version ultérieure, supprimez l'adresse IP de secours attribuée à l'interface.Appliquez la commande NAT.Réappliquez l'adresse IP de secours 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](#)