ASA 8.4(4): Bestimmte Identity NAT-Konfiguration deaktiviert

Inhalt

Einführung

Adaptive Security Appliances (ASAs) mit 8.4(4) oder höher können bestimmte NAT-Konfigurationen ablehnen und eine ähnliche Fehlermeldung anzeigen:

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

Dieses Problem kann auch auftreten, wenn Sie ein Upgrade Ihrer ASA-Version auf Version 8.4(4) oder höher durchführen. Möglicherweise stellen Sie fest, dass einige NAT-Befehle in der aktuellen Konfiguration der ASA nicht mehr vorhanden sind. In diesen Fällen sollten Sie sich die ausgedruckten Konsolenmeldungen ansehen, um festzustellen, ob Meldungen im obigen Format vorliegen.

Eine weitere Auswirkung ist, dass der Datenverkehr für bestimmte Subnetze hinter der ASA nicht mehr durch VPN-Tunnel (Virtual Private Network) geleitet wird, die auf der ASA enden. In diesem Dokument wird beschrieben, wie diese Probleme behoben werden.

Bevor Sie beginnen

Anforderungen

Diese Bedingungen müssen erfüllt sein, um dieses Problem zu lösen:

- ASA mit Version 8.4(4) oder höher oder Upgrade auf Version 8.4(4) oder höher aus einer früheren Version.
- ASA mit Standby-IP-Adresse auf mindestens einer ihrer Schnittstellen konfiguriert.
- Eine NAT wird mit der oben genannten Schnittstelle als zugeordnete Schnittstelle konfiguriert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dieser Hardware- und Softwareversion:

- ASAs ab Version 8.4(4)

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

Problem

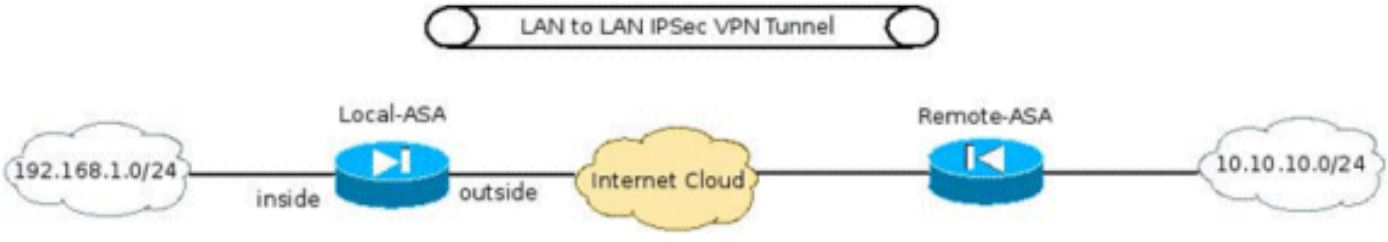
Wenn der zugeordnete Adressbereich in einer statischen NAT-Anweisung die der zugeordneten Schnittstelle zugewiesene "Standby"-IP-Adresse enthält, wird der NAT-Befehl abgelehnt. Dieses Verhalten existierte schon immer für die statische Portumleitung, wurde jedoch für statische One-to-One NAT-Anweisungen sowie für Version 8.4(4) als Behebung für die Cisco Bug-ID CSCtw82147 eingeführt (nur registrierte Kunden).

Dieser Fehler wurde behoben, da die ASA vor 8.4(4) Benutzern ermöglichte, die zugeordnete Adresse in einer statischen NAT-Konfiguration so zu konfigurieren, dass sie mit der Standby-IP-Adresse übereinstimmt, die der zugeordneten Schnittstelle zugewiesen wurde. Betrachten Sie zum Beispiel diesen Konfigurationsabschnitt einer 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
```

Obwohl der Befehl akzeptiert wird, funktioniert diese NAT-Konfiguration niemals planmäßig. Daher lässt die ASA, beginnend mit 8.4(4), eine solche NAT-Regel überhaupt nicht zu.

Dies hat zu einem weiteren unvorhergesehenen Problem geführt. Betrachten Sie beispielsweise das Szenario, in dem der Benutzer einen VPN-Tunnel auf der ASA hat, der das interne Subnetz in die Lage versetzen soll, mit dem Remote-VPN-Subnetz zu kommunizieren.



Neben anderen Befehlen, die für die Konfiguration des VPN-Tunnels erforderlich sind, ist eine der wichtigsten Konfigurationen, sicherzustellen, dass der Datenverkehr zwischen den VPN-Subnetzen nicht NATed erhält. Dies wird mit Version 8.3 und höher implementiert. Verwenden Sie hierzu einen manuellen/doppelten NAT-Befehl in diesem 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
```

Wenn dieses ASA-Upgrade auf 8.4(4) oder höher durchgeführt wird, ist dieser NAT-Befehl nicht in der aktuellen ASA-Konfiguration enthalten, und dieser Fehler wird in der ASA-Konsole ausgegeben:

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

Der Datenverkehr zwischen den Subnetzen 192.168.1.0/24 und 10.10.10.0/24 fließt daher nicht mehr durch den VPN-Tunnel.

Lösung

Es gibt zwei mögliche Problemumgehungen für diese Bedingung:

- Stellen Sie den NAT-Befehl so spezifisch wie möglich ein, bevor Sie auf 8.4(4) aktualisieren, damit die zugeordnete Schnittstelle nicht "any" ist. Der obige NAT-Befehl kann beispielsweise auf die Schnittstelle geändert werden, über die das Remote-VPN-Subnetz erreichbar ist (im obigen Szenario "extern" genannt):
  ```
  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
  ```
- Wenn die oben genannte Problemumgehung nicht möglich ist, gehen Sie wie folgt vor:Wenn die ASA Version 8.4(4) oder höher ausgeführt wird, entfernen Sie die der Schnittstelle zugewiesene Standby-IP-Adresse.Wenden Sie den NAT-Befehl an.Wenden Sie die Standby-IP-Adresse erneut auf die Schnittstelle an.Beispiel:
  ```
  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
  ```

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems