ASA 8.4(4)：不允许某些身份NAT配置

目录

[简介](#)
[开始使用前](#)
[要求](#)
[使用的组件](#)
[规则](#)
[问题](#)
[解决方案](#)
[相关信息](#)

简介

运行8.4(4)或更高版本的自适应安全设备(ASA)可能拒绝某些NAT配置并显示类似以下的错误消息：

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

当您将ASA从先前版本升级到8.4(4)或更高版本时，也会出现此问题。您可能会注意到，ASA的运行配置中不再存在某些NAT命令。在这些情况下，您应查看打印出的控制台消息，以查看是否存在以上格式显示的消息。

您可能注意到的另一个效果是，ASA后面某些子网的流量可能停止通过ASA上终止的虚拟专用网络(VPN)隧道。本文档介绍如何解决这些问题。

开始使用前

要求

要遇到此问题，需要满足以下条件：

- 运行8.4(4)或更高版本的ASA，或从先前版本升级到8.4(4)或更高版本。
- ASA在其至少一个接口上配置了备用IP地址。
- NAT配置了上述接口作为映射接口。

使用的组件

本文档中的信息基于以下硬件和软件版本：

- 运行8.4(4)或更高版本的ASA

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题

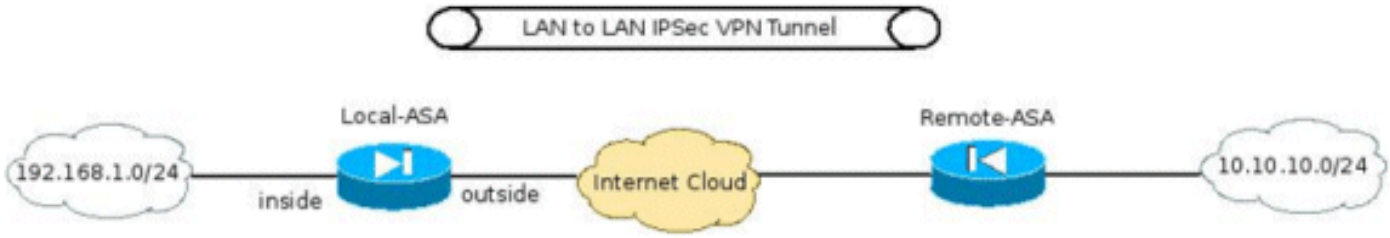
如错误消息所示，如果静态NAT语句中的映射地址范围包括分配给映射接口的“备用”IP地址，则NAT命令将被拒绝。静态端口重定向始终存在此行为，但是它已被引入到静态一对一NAT语句中，并且版本8.4(4)作为Cisco Bug ID CSCtw82147(仅注册客户)的修复。

此Bug被归档是因为在8.4(4)之前，ASA允许用户在静态NAT配置中将映射地址配置为与分配给映射接口的备用IP地址相同。例如，从ASA查看以下配置片段：

```
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
```

即使接受该命令，此NAT配置也无法按设计运行。因此，从8.4(4)开始，ASA不允许首先配置此类NAT规则。

这导致了另一个无法预料的问题。例如，假设用户在ASA上终止了VPN隧道，并希望允许“内部”子网能够与远程VPN子网通信。



除配置VPN隧道所需的其他命令外，更重要的配置之一是确保VPN子网之间的流量不被NATed。这是通过8.3及更高版本使用以下格式的手动/两次NAT命令实现的：

```
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
```

当此ASA升级到8.4(4)或更高版本时，此NAT命令不会出现在ASA的运行配置中，此错误将显示在ASA的控制台上：

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

因此，子网192.168.1.0/24和10.10.10.0/24之间的流量将不再通过VPN隧道。

解决方案

此情况有两种可能的解决方法：

- 在升级到8.4(4)之前，请尽可能明确NAT命令，使映射接口不是“any”。 例如，上述NAT命令可更改为可通过其访问远程VPN子网的接口（在上述场景中命名为“outside”）：
  ```
  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
  ```
- 如果上述解决方法不可能，请完成以下步骤：当ASA运行8.4(4)或更高版本时，删除分配给接口的备用IP地址。应用NAT命令。在接口上重新应用备用IP地址。例如：
  ```
  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
  ```

相关信息

- 技术支持和文档 - Cisco Systems