ASA 8.4(4) ：禁止的某一标识NAT配置

目录

简介

可适应安全工具(ASA)运行8.4(4)或更加高可能拒绝某些NAT配置和显示错误消息类似于此：

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

当您升级您的ASA到8.4(4)或高从一先前的版本时，此问题能也出现。您可以注意一些NAT命令不再是存在ASA的running-config。在这些实例，您应该查看打印出的控制台信息为了发现是否有消息现在上述格式。

您可以注意是的另一效果某些子网的流量在ASA后可能停止通过通过终止在ASA的虚拟专用网络(VPN)通道。本文描述如何解决这些问题。

开始使用前

要求

这些情况需要符合为了遇到此问题：

- 运行版本8.4(4)或以上的ASA或者升级对版本8.4(4)或以上从一先前的版本。
- ASA配置与在其接口之至少一的一个备用IP地址。
- NAT配置与上述接口，被映射的接口。

使用的组件

本文档中的信息根据此硬件和软件版本：

- ASA运行8.4(4)或更加高

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

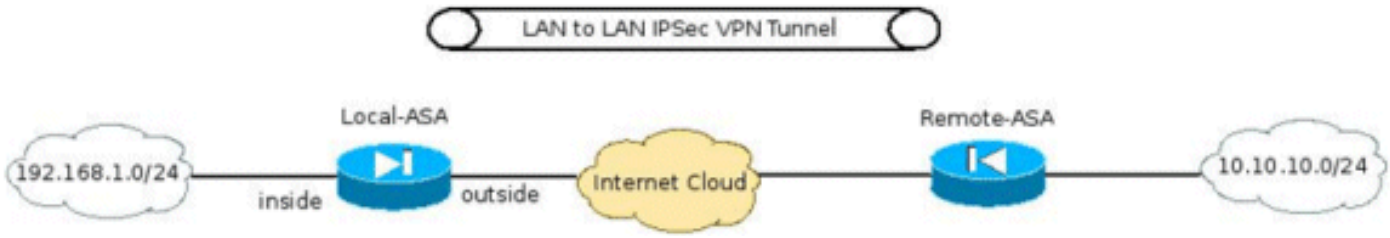
当错误消息建议，如果在一个静态NAT语句的被映射的地址范围包括“暂挂” IP地址分配到被映射的接口， nat命令拒绝。此行为为静态端口重定向总是存在，但是为静态一对一的NAT语句介绍与版本8.4(4)作为Cisco Bug ID的CSCtw82147 (仅限注册用户)一个修正。

归档了此bug，因为在8.4(4) ASA之前在一静态NAT配置里允许用户配置被映射的地址是同一样备用IP地址分配到被映射的接口的。例如，请查看配置此片断从ASA的：

```
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
```

即使命令接受，此NAT配置故意地不会工作。结果，从8.4(4)开始， ASA不允许这样NAT规则首先配置。

这导致另一未预见到的问题。例如，请考虑用户有终止在ASA的一个VPN通道并且要允许“里面”子网能与远程VPN子网谈的方案。



在配置的VPN通道其他required命令中，其中一更加重要的配置是保证VPN子网之间的流量没获得NAT。这实现与8.3和在使用手工上/两次nat命令此格式：

```
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)或更加高，此nat命令不会是存在ASA的running-config，并且此错误在ASA的控制台将打印：

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

结果，子网192.168.1.0/24和10.10.10.0/24之间的流量不再将流经VPN通道。

解决方案

有此情况的两可能的应急方案：

- 在升级前尽可能具体地做nat命令对8.4(4)，因此被映射的接口不是“中的任一个”。例如，上述nat命令可以更改到远程VPN子网是可及的接口(命名“外部”在上述方案) ：`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`
- 如果上述应急方案不是可能的，请完成这些步骤：当ASA运行8.4(4)或更加高时，请删除备用IP地址分配到接口。实施nat命令。重新应用在接口的备用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