ASA 8.4(4):不允許某些標識NAT配置

目錄

簡介

運行8.4(4)或更高版本的自適應安全裝置(ASA)可能會拒絕某些NAT配置並顯示類似於以下內容的錯誤消息：

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

將ASA從先前版本升級到8.4(4)或更高版本時，也可能出現此問題。您可能注意到，某些NAT命令不再出現在ASA的運行配置中。在這些情況下，您應該檢視列印出的控制檯消息，以檢視是否存在以上格式的消息。

您可能注意到的另一個影響是，ASA後方的某些子網的流量可能停止通過ASA上終止的虛擬專用網路(VPN)隧道。本文說明如何解決這些問題。

開始之前

需求

為了解決此問題，需要滿足以下條件：

- 運行8.4(4)或更高版本的ASA，或者從先前版本升級到8.4(4)或更高版本。
- ASA在其至少一個介面上配置了備用IP地址。
- NAT將以上介面配置為對映介面。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- 運行8.4(4)或更高版本的ASA

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題

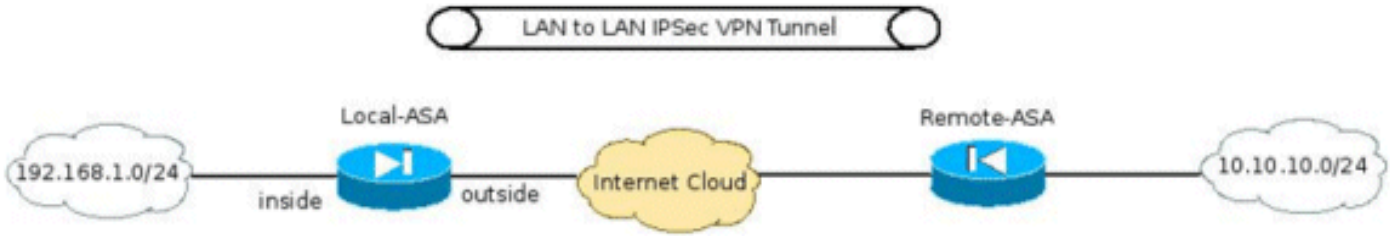
如錯誤消息所示，如果靜態NAT語句中的對映地址範圍包含分配給對映介面的「備用」IP地址，則會拒絕NAT命令。靜態連線埠重新導向一直存在此行為，但靜態一對一NAT陳述式以及版本8.4(4)已加入此行為，作為思科錯誤ID CSCtw82147(僅限註冊客戶)的修復程式。

此錯誤之所以被發現，是因為ASA在8.4(4)之前允許使用者將靜態NAT配置中的對映地址配置為與分配給對映介面的備用IP地址相同。例如，從ASA檢視以下配置片段：

```
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
```

即使命令被接受，此NAT配置在設計上也永遠不會起作用。因此，從8.4(4)開始，ASA首先不允許配置此類NAT規則。

這導致了另一個無法預見的問題。例如，考慮以下情況：使用者具有在ASA上終止的VPN隧道，並希望允許「內部」子網能夠與遠端VPN子網通訊。



在配置VPN隧道所需的其他命令中，其中一個較為重要的配置是確保VPN子網之間的流量不進行NAT轉換。8.3及更高版本使用下列格式的Manual/Two NAT命令實現此功能：

```
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
```

當此ASA升級到8.4(4)或更高版本時，此NAT命令不會出現在ASA的運行配置中，並且此錯誤將列印在ASA的控制檯上：

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

因此，子網192.168.1.0/24和10.10.10.0/24之間的流量將不再通過VPN隧道。

解決方案

這種情況有兩種可能的解決方法：

- 在升級到8.4(4)之前，儘可能具體化NAT命令，以便對映介面不是「any」。 例如，可以將上述NAT命令更改為可訪問遠端VPN子網的介面（在上述場景中命名為「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
  ```
- 如果無法採取上述解決方法，請完成以下步驟：當ASA運行8.4(4)或更高版本時，刪除分配給介面的備用IP地址。應用NAT命令。在介面上重新應用備用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
  ```

相關資訊

- 技術支援與文件 - Cisco Systems