ASA 8.4(4): Determinada configuração de NAT de identidade não permitida

Contents

Introduction

Os ASAs (Adaptive Security Appliances, Dispositivos de segurança adaptável) executando 8.4(4) ou posterior podem rejeitar determinadas configurações de NAT e exibir uma mensagem de erro semelhante a esta:

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

Esse problema também pode aparecer quando você atualiza seu ASA para 8.4(4) ou superior a partir de uma versão anterior. Você pode observar que alguns comandos NAT não estão mais presentes na configuração atual do ASA. Nesses casos, você deve examinar as mensagens do console impressas para ver se há mensagens presentes no formato acima.

Outro efeito que você pode observar é que para determinadas sub-redes por trás do ASA podem cessar ao passar pelos túneis de Rede Privada Virtual (VPN) terminando no ASA. Este documento descreve como resolver esses problemas.

Antes de Começar

Requirements

Estas condições têm de ser satisfeitas para que este problema possa ser encontrado:

- ASA com a versão 8.4(4) ou posterior, ou atualizado para a versão 8.4(4) ou posterior de uma versão anterior.
- ASA configurado com um endereço IP em standby em pelo menos uma de suas interfaces.
- Um NAT é configurado com a interface acima como a interface mapeada.

Componentes Utilizados

As informações neste documento são baseadas nesta versão de hardware e software:

- ASAs executando 8.4(4) ou superior

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Problema

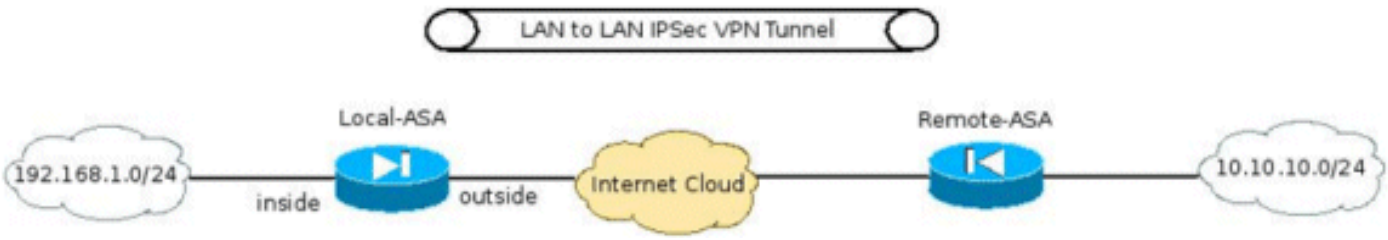
Como a mensagem de erro sugere, se o intervalo de endereços mapeado em uma instrução NAT estática incluir o endereço IP "standby" atribuído à interface mapeada, o comando NAT será rejeitado. Esse comportamento sempre existiu para o redirecionamento de porta estática, mas foi introduzido para instruções NAT estáticas um para um, bem como para a versão 8.4(4) como uma correção para o bug da Cisco ID CSCtw82147 (somente clientes registrados) .

Este bug foi arquivado porque antes da 8.4(4), o ASA permitiu que os usuários configurassem o endereço mapeado em uma configuração de NAT estático para ser o mesmo que o endereço IP em standby atribuído à interface mapeada. Por exemplo, examine este trecho de configuração de um 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
```

Embora o comando seja aceito, essa configuração de NAT nunca funcionará por projeto. Como resultado, começando com 8.4(4), o ASA não permite que tal regra de NAT seja configurada em primeiro lugar.

Isso resultou em outro problema imprevisto. Por exemplo, considere o cenário em que o usuário tem um túnel VPN terminando no ASA e deseja permitir que a sub-rede "interna" possa se comunicar com a sub-rede VPN remota.



Entre outros comandos necessários para configurar o túnel VPN, uma das configurações mais importantes é garantir que o tráfego entre as sub-redes VPN não obtenha NATed. Isso é implementado com 8.3 e acima usando um comando de NAT manual/duas vezes neste formato:

```
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
```

Quando esse ASA é atualizado para 8.4(4) ou superior, esse comando NAT não estará presente na configuração atual do ASA e esse erro será impresso no console do ASA:

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

Como resultado, o tráfego entre as sub-redes 192.168.1.0/24 e 10.10.10.0/24 não fluirá mais pelo túnel VPN.

Solução

Há duas alternativas possíveis para esta condição:

- Tornar o comando NAT o mais específico possível antes de atualizar para 8.4(4) para que a interface mapeada não seja "nenhuma". Por exemplo, o comando NAT acima pode ser alterado para a interface através da qual a sub-rede de VPN Remota pode ser alcançada (chamada "externa" no cenário acima):
  ```
  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
  ```
- Se a solução alternativa acima não for possível, faça o seguinte:Quando o ASA estiver executando 8.4(4) ou posterior, remova o endereço IP em standby atribuído à interface.Aplique o comando NAT.Reaplique o endereço IP em standby na interface.Por exemplo:
  ```
  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
  ```

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems