ASA 8.4(4): Determinada configuração de NAT da identidade recusada

Índice

Introdução

O corredor das ferramentas de segurança (ASA) 8.4(4) ou mais alto adaptável podem rejeitar determinadas configurações de NAT e indicar um Mensagem de Erro similar a este:

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

Este problema pode igualmente aparecer quando você promove seu ASA a 8.4(4) ou mais alto de uma liberação prévia. Você pode observar que alguns comandos nat estão já não atuais na executar-configuração do ASA. Nestes exemplos, você deve olhar os mensagens do console impressos - para fora a fim ver se há umas mensagens atuais 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

Requisitos

Estas circunstâncias precisam de ser estadas conformes a fim encontrar este problema:

- Versão 8.4(4) ou mais recente running ASA, ou promovido à versão 8.4(4) ou mais recente de uma liberação prévia.
- ASA configurado com um endereço IP em standby pelo menos em uma de suas relações.
- Um NAT é configurado com a relação acima como a relação traçada.

Componentes Utilizados

A informação neste documento é baseada nesta versão de hardware e software:

- Corredor ASA 8.4(4) ou mais alto

Convenções

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

Problema

Enquanto o Mensagem de Erro sugere, se a escala de endereço traçada em uma indicação do NAT estático inclui o endereço IP de Um ou Mais Servidores Cisco ICM NT “à espera” atribuído à relação traçada, o comando nat está rejeitado. Este comportamento existiu sempre para a reorientação da porta estática, mas foi introduzido para declarações NAT lineares estáticas também com versão 8.4(4) como um reparo para a identificação de bug Cisco CSCtw82147 (clientes registrados somente).

Este erro foi arquivado porque antes 8.4(4) do ASA permitiu que os usuários configurassem o endereço traçado em uma configuração do NAT estático para ser o mesmos como o endereço IP em standby atribuiu à relação traçada. Por exemplo, olhe este snippet da 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
```

Mesmo que o comando seja aceitado, esta configuração de NAT nunca trabalhará pelo projeto. Em consequência, começando com o 8.4(4), o ASA não permite que tal regra NAT seja configurada no primeiro lugar.

Isto conduziu a um outro problema imprevisto. Por exemplo, considere a encenação onde o usuário tem um túnel VPN que termina no ASA e o quer permitir que a sub-rede do “interior” possa falar à sub-rede VPN remota.

Entre outros comandos required para configurar o túnel VPN, uma das configurações mais importantes é assegurar-se de que o tráfego entre as sub-redes VPN não obtenha o NATed. Isto é executado com 8.3 e acima de usar um manual/duas vezes um comando nat deste 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 este ASA é promovido a 8.4(4) ou mais alto, este comando nat não esta presente na executar-configuração do ASA e este erro será imprimido 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
```

Em consequência, o tráfego entre as sub-redes 192.168.1.0/24 e 10.10.10.0/24 já não correrá através do túnel VPN.

Solução

Há duas alternativas possíveis para esta circunstância:

- Faça o comando nat o mais específico possível antes de promover a 8.4(4) assim que a relação traçada não é “alguma”. Por exemplo, o comando nat acima pode ser mudado à relação através de que a sub-rede VPN remota é alcançável (nomeado “parte externa” na encenação 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 ação alternativa acima não é possível, termine estas etapas:Quando o ASA está executando 8.4(4) ou mais alto, remova o endereço IP em standby atribuído à relação.Aplique o comando nat.Reaplique o endereço IP em standby na relação.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