ASR1k NAT intermitentemente não traduz alguns pacotes

Índice

Introdução
Informações de Apoio
Demonstração do NAT que está sendo contorneado
Fluxos de tráfego ao destino do NON-NAT-ed:
O tráfego da mesma fonte tenta enviar o destino do NAT-ed:
Restauração do tráfego do NAT-ed
Exemplo da edição
Workaround/reparo:
Solução #1:
Solução #2:
Solução #3:
Resumo
Referências

Introdução

Este artigo demonstra uma situação onde os pacotes que devem ser traduzidos pelo NAT em um ASR1k não estejam sendo traduzidos (NAT que está sendo contorneado). Isto poderia conduzir à falha do tráfego porque o salto seguinte é provável não configurado para permitir que os pacotes não convertidos sejam processados.

Informações de Apoio

Na versão de software 12.2(33)XND uma característica chamada porteiro NAT foi introduzida e permitida à revelia. (Note isto não não tem nada fazer com H.323). O porteiro NAT foi projetado impedir que os fluxos do NON-NAT-ed usem o CPU excessivo em um esforço para criar uma tradução NAT. Para conseguir isto, dois esconderijos pequenos (um para o sentido in2out e um para o sentido out2in) são criados com base no endereço de origem. Cada entrada de cache consiste em um endereço de origem, em um VRF ID, em um valor de temporizador (usado para invalidar a entrada após os segundos 10), e em um contador do quadro. Há as entradas 256 na tabela que compõe o esconderijo. Se há uns fluxos de tráfego múltiplo do mesmo endereço de origem onde alguns pacotes exigem o NAT e o algum não faz, poderia conduzir aos pacotes que não são NAT-ed e enviado através do roteador untranslated. Cisco recomenda que os clientes devem evitar ter o NAT-ed e o NON-NAT-ed flui na mesma relação na medida do possível.

Demonstração do NAT que está sendo contorneado

A seguinte seção descreve como o NAT pode ser contorneado devido à característica do porteiro NAT. Reveja por favor o diagrama em detalhe. Nós podemos ver que há um roteador de origem, um Firewall ASA, os ASR1k, e o roteador de destino.

Fluxos de tráfego ao destino do NON-NAT-ed:

1) O sibilo é iniciado da fonte: Fonte: Destino de 172.17.250.201: 198.51.100.11
2) O pacote chega na interface interna do ASA que executa a tradução de endereço de origem. O pacote terá agora a fonte: Destino de 203.0.113.231: 198.51.100.11
3) O pacote chega no ASR1k no NAT fora à interface interna. A tradução NAT não encontra nenhuma tradução para o endereço de destino e assim que o porteiro “para fora” para pôr em esconderijo é povoado com o endereço de origem 203.0.113.231
4) O pacote chega no destino. O destino aceita o pacote ICMP e retorna uma resposta de eco ICMP tendo por resultado o sucesso do sibilo.

O tráfego da mesma fonte tenta enviar o destino do NAT-ed:

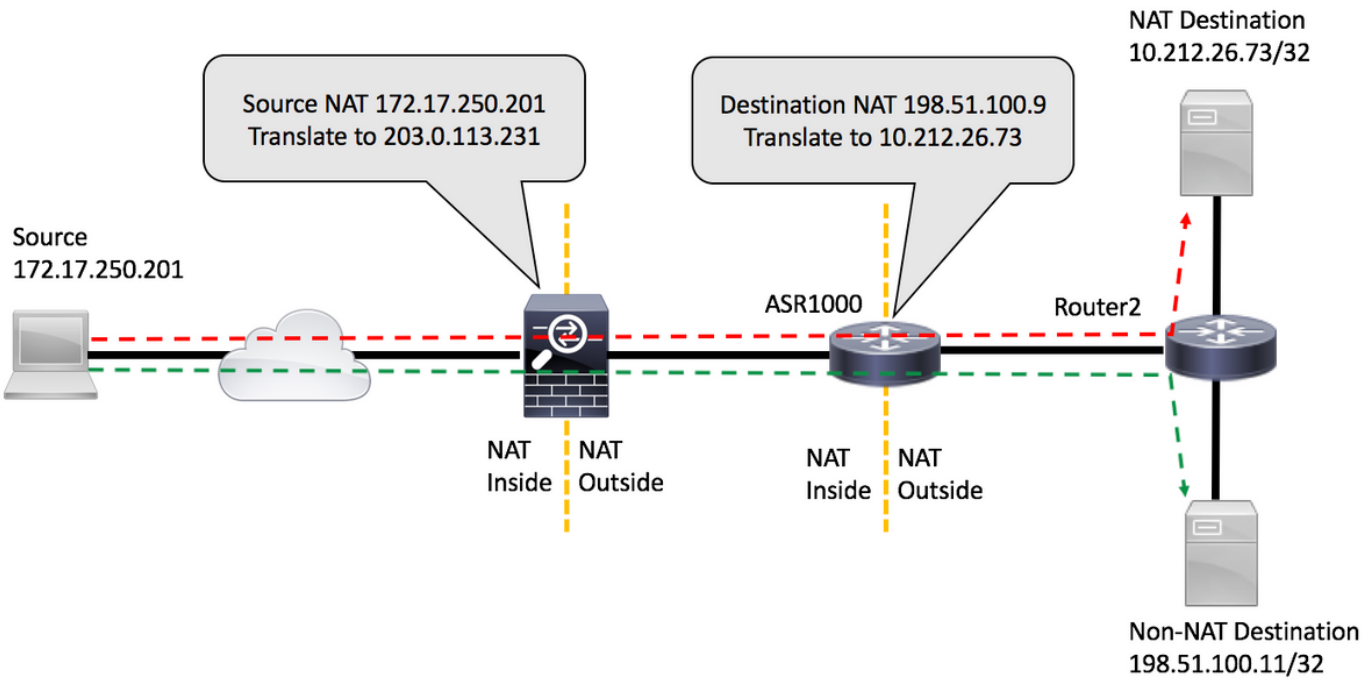
1) O sibilo é iniciado da fonte: Fonte: Destino de 172.17.250.201: 198.51.100.9
2) O pacote chega na interface interna do ASA que executa a tradução de endereço de origem. O pacote terá agora a fonte: Destino de 203.0.113.231: 198.51.100.9
3) O pacote chega no ASR1k no NAT fora à interface interna. O NAT procura primeiramente uma tradução para a fonte e o destino. Não encontrando um, verifica o porteiro “” põe em esconderijo e encontra o endereço de origem 203.0.113.231. (Erroneamente) supõe que o pacote não precisa a tradução e tampouco para a frente o pacote se uma rota existe para o destino ou deixa cair o pacote. De qualquer maneira, o pacote não alcançará o destino pretendido.

Restauração do tráfego do NAT-ed

1) Após os segundos 10, a entrada para o endereço de origem 203.0.113.231 cronometra para fora no porteiro para fora põe em esconderijo. (Nota que a entrada ainda existe fisicamente no esconderijo mas porque expirou, não é usada).

2) Agora se a mesma fonte: 172.17.250.201 envia ao destino 198.51.100.9 do NAT-ed, quando o pacote chega na relação out2in no ASR1K, nenhuma tradução será encontrado. Quando nós verificamos o porteiro para fora pomos em esconderijo, nós não encontraremos uma entrada ativa e assim que nós criaremos a tradução para o fluxo do willl do destino e dos pacotes como esperado.

3) O tráfego neste fluxo continuará enquanto as traduções não são para fora cronometrado devido à inatividade. Se entretanto, a fonte envia outra vez o tráfego a um destino do NON-NAT-ed, fazendo com que uma outra entrada esteja povoada no porteiro para fora põe em esconderijo, ele não afetará sessões estabelecidas mas haverá um segundo período 10 em que as sessões novas dessa mesma fonte aos destinos do NAT-ed falharão.



Exemplo da edição

1) O sibilo é iniciado do roteador de origem: Fonte: Destino de 172.17.250.201: 198.51.100.9. O sibilo é emitido com contagem de repetição de 2, repetidamente [FLOW1].

2) Sibile então um destino diferente que não esteja sendo NAT-ed pela fonte ASR1k: 172.17.250.201 Destination:198.51.100.11 [FLOW2].

3) Envie então mais pacotes a 198.51.100.9 [FLOW1]. Os pacotes primeiros deste fluxo contornearão o NAT como visto pela lista de acesso que combina no roteador de destino.

```
source#ping 198.51.100.9 source lo1 rep 2

Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.9 source lo1 rep 2

Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.11 source lo1 rep 200000

Type escape sequence to abort.
Sending 200000, 100-byte ICMP Echos to 198.51.100.11, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
```

```
Success rate is 99 percent (3007/3008), round-trip min/avg/max = 1/1/16 ms
source#ping 198.51.100.9 source lo1 rep 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
...!!!!!!!
Success rate is 70 percent (7/10), round-trip min/avg/max = 1/1/1 ms
source#
```

O fósforo ACL no roteador de destino mostra aos 3 pacotes que falhado, não estiveram traduzidos:

```
Router2#show access-list 199
Extended IP access list 199
   10 permit udp host 172.17.250.201 host 198.51.100.9
   20 permit udp host 172.17.250.201 host 10.212.26.73
   30 permit udp host 203.0.113.231 host 198.51.100.9
   40 permit udp host 203.0.113.231 host 10.212.26.73 (4 matches)
   50 permit icmp host 172.17.250.201 host 198.51.100.9
   60 permit icmp host 172.17.250.201 host 10.212.26.73
    70 permit icmp host 203.0.113.231 host 198.51.100.9 (3 matches) <<<<<<<
   80 permit icmp host 203.0.113.231 host 10.212.26.73 (42 matches)
   90 permit udp any any log (2 matches)
   100 permit icmp any any log (4193 matches)
   110 permit ip any any (5 matches)
Router2#
```

Em ASR1k nós podemos verificar as entradas de cache do porteiro:

```
PRIMARY#show platform hardware qfp active feature nat datapath gatein
Gatekeeper on
sip 203.0.113.231 vrf 0 cnt 1 ts 0x17ba3f idx 74
sip 10.203.249.226 vrf 0 cnt 0 ts 0x36bab6 idx 218
sip 10.203.249.221 vrf 0 cnt 1 ts 0x367ab4 idx 229

PRIMARY#show platform hardware qfp active feature nat datapath gateout
Gatekeeper on
sip 198.51.100.11 vrf 0 cnt 1 ts 0x36db07 idx 60
sip 10.203.249.225 vrf 0 cnt 0 ts 0x36bb7a idx 217
sip 10.203.249.222 vrf 0 cnt 1 ts 0x367b7c idx 230
```

Workaround/reparo:

Na maioria de ambientes os trabalhos da funcionalidade de gatekeeper NAT muito bem sem causar edições. Contudo se você é executado neste problema há algumas maneiras de resolvê-lo.

Solução #1:

A opção preferida seria promover IOS-XE a uma versão que incluísse o realce do porteiro:

Endurecimento do porteiro CSCun06260 XE3.13

Este realce permite o porteiro NAT pôr em esconderijo a fonte **e os** endereços de destino, assim como fazer o tamanho de cache configurável. A fim girar sobre o modo estendido, você precisa de aumentar o tamanho de cache com os comandos seguintes. Você pode igualmente monitora o esconderijo para ver se você precisa de aumentar o tamanho.

```
PRIMARY(config)#ip nat settings gatekeeper-size 1024
PRIMARY(config)#end
```

O modo estendido pode ser verificado verificando os comandos seguintes:

```
PRIMARY#show platform hardware qfp active feature nat datapath gatein
Gatekeeper on
sip 10.203.249.221 dip 10.203.249.222 vrf 0 ts 0x5c437 idx 631

PRIMARY#show platform hardware qfp active feature nat datapath gateout
Gatekeeper on
sip 10.203.249.225 dip 10.203.249.226 vrf 0 ts 0x5eddf idx 631

PRIMARY#show platform hardware qfp active feature nat datapath gatein active
Gatekeeper on
ext mode Size 1024, Hits 2, Miss 4, Aged 0 Added 4 Active 1

PRIMARY#show platform hardware qfp active feature nat datapath gateout active
Gatekeeper on
ext mode Size 1024, Hits 0, Miss 1, Aged 1 Added 2 Active 0
```

Solução #2:

Para as liberações que não têm o reparo para CSCun06260, a única opção é desligar a característica do porteiro. O único impacto negativo será levemente desempenho reduzido para o tráfego do NON-NAT-ed assim como uma utilização CPU mais alta no QFP.

```
PRIMARY(config)#no ip nat service gatekeeper
PRIMARY(config)#end
PRIMARY#PRIMARY#Sh platform hardware qfp active feature nat datapath gatein
Gatekeeper off

PRIMARY#
```

A utilização QFP pode ser monitorada com:

```
show platform hardware qfp active data utilization summary
show platform hardware qfp active data utilization qfp 0
```

Solução #3:

Separe fluxos de tráfego de modo que os pacotes NAT e NON-NAT não cheguem na mesma relação.

Resumo

O comando gatekeeper NAT foi introduzido aumentar o desempenho do roteador para fluxos do NON-NAT-ed. Sob algumas circunstâncias a característica pode causar problemas quando uma mistura dos pacotes NAT e NON-NAT chega da mesma fonte. A solução é usar a funcionalidade de gatekeeper aumentada, ou se aquela não é possível, desabilita a característica do porteiro.

Referências

Alterações de software que permitiram que o porteiro fosse desligado:

CSCty67184 ASR1k NAT CLI - Porteiro de ligar/desligar
CSCth23984 adicionam a capacidade CLI de girar a funcionalidade de gatekeeper nat de ligar/desligar

Realce do porteiro NAT

Endurecimento do porteiro CSCun06260 XE3.13