Troubleshooting de Falha Intermitente de NAT do IOS-XE para Converter alguns Pacotes

Contents

Introdução

Este documento descreve os pacotes não traduzidos que ignoram o NAT em um roteador Cisco IOS XE, podendo causar falha de tráfego.

Informações de Apoio

Na versão de software 12.2(33)XND, um recurso chamado Network Address Translation (NAT) Gatekeeper foi introduzido e ativado por padrão. O NAT Gatekeeper foi projetado para impedir que fluxos não-NAT-ed usem excesso de CPU para criar uma conversão NAT. Para conseguir isso, dois caches pequenos (um para a direção in2out e outro para a direção out2in) são criados com base no endereço de origem. Cada entrada de cache consiste em um endereço de origem, um ID de roteamento e encaminhamento virtual (VRF), um valor de temporizador (usado para invalidar a entrada após 10 segundos) e um contador de quadros. Há 256 entradas na tabela que formam o cache. Se houver vários fluxos de tráfego do mesmo endereço de origem em que alguns pacotes exigem NAT e outros não, isso pode fazer com que os pacotes não sejam submetidos à NAT e enviados pelo roteador sem serem convertidos. A Cisco recomenda que os clientes evitem ter fluxos NAT e não NAT-ed na mesma interface sempre que possível.

Observação: isso não tem nada a ver com o H.323.

Plataformas afetadas

- ISR1K
- ISR4K
- C8200
- C8300
- C8500

Demonstração de que o NAT está sendo ignorado

Esta seção descreve como o NAT pode ser ignorado devido ao recurso de gatekeeper NAT. Reveja o diagrama em detalhes. Você pode ver que há um roteador de origem, um firewall Adaptive Security Appliance (ASA), o ASR1K e o roteador de destino.

Fluxos de tráfego para destino não NAT-ed

1. O ping é iniciado na origem: Origem: 172.17.250.201 Destino: 198.51.100.11.
2. O pacote chega à interface interna do ASA que executa a conversão do endereço de origem. O pacote agora tem Origem: 203.0.113.231 Destino: 198.51.100.11.
3. O pacote chega ao ASR1K na interface NAT externa para interna. A conversão de NAT não encontra conversão para o endereço de destino e, portanto, o cache "out" do gatekeeper é preenchido com o endereço de origem 203.0.113.231.
4. O pacote chega ao destino. O destino aceita o pacote ICMP (Internet Control Message Protocol) e retorna uma Resposta de ECO ICMP que resulta no sucesso do ping.

O tráfego da mesma origem tenta enviar o destino definido por NAT

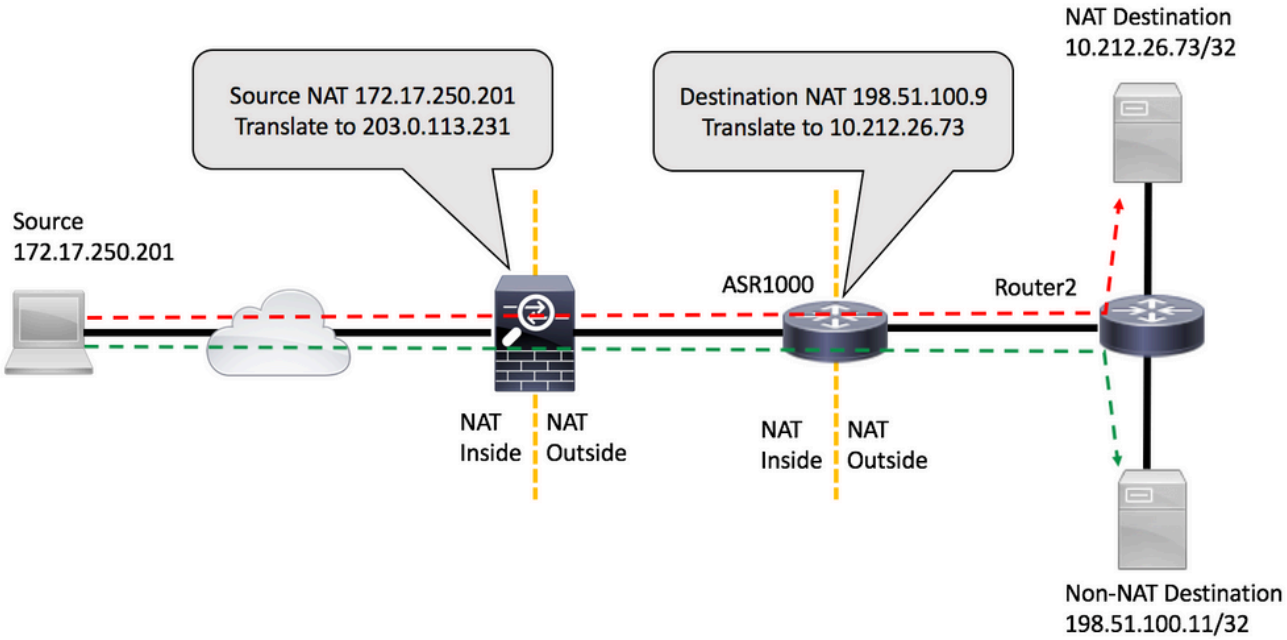
1. .Ping é iniciado a partir da origem: Origem: 172.17.250.201 Destino: 198.51.100.9.
2. O pacote chega à interface interna do ASA que executa a conversão do endereço de origem. O pacote agora tem Origem: 203.0.113.231 Destino: 198.51.100.9.
3. O pacote chega ao ASR1K na interface NAT externa para interna. Primeiro, o NAT procura uma conversão para a origem e o destino. Como não encontra um, ele verifica o cache "out" do gatekeeper e encontra o endereço de origem 203.0.113.231. Ele (erroneamente) supõe que o pacote não precisa de conversão e encaminha o pacote se houver uma rota para o destino ou descarta o pacote. De qualquer forma, o pacote não alcança o destino pretendido.

Restauração de tráfego NAT-ed

1. Após 10 segundos, a entrada do endereço de origem 203.0.113.231 expira no cache de saída do gatekeeper.

> Observação: a entrada ainda existe fisicamente no cache, mas como expirou, ela não é usada.

2. Agora, se a mesma origem 172.17.250.201 enviar para o destino NAT 198.51.100.9. Quando o pacote chega à interface out2in no ASR1K, nenhuma conversão é encontrada. Quando você verifica o cache de saída do gatekeeper, não é possível encontrar uma entrada ativa, de modo que você crie a conversão para o destino e o fluxo de pacotes conforme o esperado.
3. O tráfego nesse fluxo continua enquanto as conversões não tiverem o tempo limite devido à inatividade. Se, nesse meio tempo, a origem enviar novamente o tráfego para um destino não NAT-ed, o que faz com que outra entrada seja preenchida no gatekeeper fora do cache, isso não afeta as sessões estabelecidas, mas há um período de 10 segundos em que novas sessões dessa mesma origem para destinos NAT-ed falham.



Exemplo do problema

1. O ping é iniciado no roteador de origem : Origem: 172.17.250.201 Destino: 198.51.100.9. O ping é emitido com uma contagem de repetição de dois, mais e mais [FLOW1].
2. Em seguida, faça ping em um destino diferente que não esteja sendo configurado para NAT pelo ASR1K: Origem: 172.17.250.201 Destino:198.51.100.11 [FLUXO2].
3. Em seguida, envie mais pacotes para 198.51.100.9 [FLOW1]. Os primeiros pacotes desse fluxo ignoram o NAT conforme visto pela correspondência da lista de acesso no roteador destino.

<#root>

```
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#
```

A correspondência da ACL no roteador de destino mostra que os três pacotes que falharam não foram convertidos:

<#root>

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#
```

No ASR1K, você pode verificar as entradas de cache do gatekeeper:

<#root>

```
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
```

Solução alternativa/correção

Na maioria dos ambientes, a funcionalidade do gatekeeper de NAT funciona bem e não causa problemas. No entanto, se você tiver esse problema, há algumas maneiras de resolvê-lo.

Solução 1

A opção preferencial seria atualizar o Cisco IOS® XE para uma versão que inclua o aprimoramento do gatekeeper:

ID de bug da Cisco CSCun06260 XE3.13 Endurecimento de gatekeeper

Esse aprimoramento permite que o gatekeeper NAT armazene em cache os endereços origem e destino, bem como torna o tamanho do cache configurável. Para ativar o modo estendido, você precisa aumentar o tamanho do cache com esses comandos. Você também pode monitorar o cache para ver se precisa aumentar o tamanho.

<#root>

```
PRIMARY(config)#
```

ip nat settings gatekeeper-size 1024

```
PRIMARY(config)#
end
```

O modo estendido pode ser verificado verificando-se estes comandos:

```
<#root>
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 versões que não têm a correção para o bug da Cisco ID CSCun06260, a única opção é desativar o recurso de gatekeeper. O único impacto negativo é um desempenho ligeiramente reduzido para tráfego não-NAT-ed, bem como uma maior utilização da CPU no Quantum Flow Processor (QFP).

```
<#root>

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 de QFP pode ser monitorada com estes comandos:

```
<#root>

show platform hardware qfp active data utilization summary

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

Solução 3

Separe os fluxos de tráfego para que os pacotes NAT e não NAT não cheguem na mesma interface.

Summary

O comando NAT Gatekeeper foi introduzido para melhorar o desempenho do roteador para fluxos não-NAT-ed. Sob algumas condições, o recurso pode causar problemas quando uma combinação de pacotes NAT e não NAT chega da mesma origem. A solução é usar a funcionalidade de gatekeeper aprimorada ou, se isso não for possível, desativar o recurso de gatekeeper.

Referências

Alterações de software que permitiram que o gatekeeper fosse desligado:
ID de bug Cisco CSCty67184 ASR1k NAT CLI - Gatekeeper On/Off
ID de bug Cisco CSCth23984 Adicionar recurso cli para ativar/desativar a funcionalidade de gatekeeper nat

Aprimoramento de gatekeeper NAT
ID de bug da Cisco CSCun06260 XE3.13 Endurecimento de gatekeeper

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.