Resolución de Problemas de Fallo Intermitente de NAT IOS-XE para Traducir Algunos Paquetes

Contenido

Introducción

Este documento describe los paquetes no traducidos que omiten la NAT en un router Cisco IOS XE, lo que puede causar una falla de tráfico.

Antecedentes

En la versión de software 12.2(33)XND, se introdujo y habilitó de forma predeterminada una función denominada Gatekeeper de traducción de direcciones de red (NAT). El gatekeeper NAT fue diseñado para evitar que los flujos que no son de NAT utilicen una CPU excesiva para crear una traducción NAT. Para lograr esto, se crean dos pequeñas memorias caché (una para la dirección de entrada y salida y otra para la dirección de salida y salida) basadas en la dirección de origen. Cada entrada de caché consta de una dirección de origen, un ID de routing y reenvío virtual (VRF), un valor de temporizador (utilizado para invalidar la entrada después de 10 segundos) y un contador de tramas. Hay 256 entradas en la tabla que componen la caché. Si hay varios flujos de tráfico de la misma dirección de origen en los que algunos paquetes requieren NAT y otros no, podría provocar que los paquetes no se traduzcan y no se envíen a través del router. Cisco recomienda que los clientes eviten tener flujos con y sin NAT en la misma interfaz siempre que sea posible.

Nota: Esto no tiene nada que ver con H.323.

Plataformas afectadas

- ISR1K
- ISR4K
- C8200
- C8300
- C8500

Demostración de la omisión de NAT

Esta sección describe cómo se puede omitir NAT debido a la función de gatekeeper NAT. Revise el diagrama en detalle. Puede ver que hay un router de origen, un firewall Adaptive Security Appliance (ASA), ASR1K y el router de destino.

Flujos de tráfico hacia un destino sin NAT

1. El ping se inicia desde la fuente: Fuente: 172.17.250.201 Destino: 198.51.100.11.
2. El paquete llega a la interfaz interna del ASA que realiza la traducción de la dirección de origen. El paquete ahora tiene Origen: 203.0.113.231 Destino: 198.51.100.11.
3. El paquete llega al ASR1K en la interfaz NAT externa a la interfaz interna. La traducción NAT no encuentra ninguna traducción para la dirección de destino y por lo tanto la memoria caché de "salida" del gatekeeper se llena con la dirección de origen 203.0.113.231.
4. El paquete llega al destino. El destino acepta el paquete de protocolo de mensajes de control de Internet (ICMP) y devuelve una respuesta de ECO ICMP que da como resultado un ping correcto.

El tráfico del mismo origen intenta enviar un destino con NAT

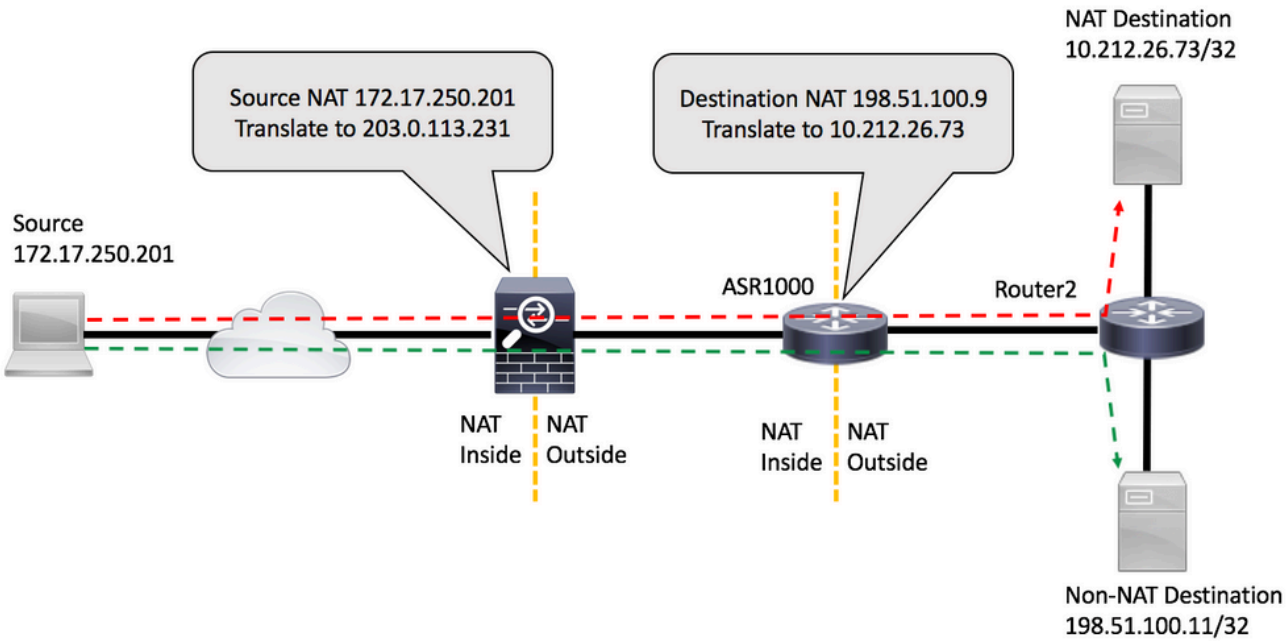
1. .Ping se inicia desde la fuente: Fuente: 172.17.250.201 Destino: 198.51.100.9.
2. El paquete llega a la interfaz interna del ASA que realiza la traducción de la dirección de origen. El paquete ahora tiene Origen: 203.0.113.231 Destino: 198.51.100.9.
3. El paquete llega al ASR1K en la interfaz NAT externa a la interfaz interna. NAT busca primero una traducción para el origen y el destino. Como no encuentra uno, verifica la memoria caché "fuera" del gatekeeper y encuentra la dirección de origen 203.0.113.231. Supone (erróneamente) que el paquete no necesita traducción y reenvía el paquete si existe una ruta para el destino o descarta el paquete. En cualquier caso, el paquete no llega al destino deseado.

Restauración del tráfico basado en NAT

1. Después de 10 segundos, la entrada para la dirección de origen 203.0.113.231 agota el tiempo de espera en la memoria caché de salida del gatekeeper.

> Nota: La entrada aún existe físicamente en la caché, pero no se utiliza porque ha caducado.

2. Ahora, si el mismo origen 172.17.250.201 envía al destino NAT-ed 198.51.100.9. Cuando el paquete llega a la interfaz out2in en el ASR1K, no se encuentra ninguna traducción. Cuando verifica la memoria caché de salida del control de acceso, no puede encontrar una entrada activa, por lo que crea la traducción para el destino y el flujo de paquetes como se espera.
3. El tráfico en este flujo continúa mientras no se agote el tiempo de espera de las traducciones debido a la inactividad. Si, mientras tanto, el origen vuelve a enviar tráfico a un destino sin NAT, lo que hace que otra entrada se llene en el gatekeeper fuera de la memoria caché, esto no afecta a las sesiones establecidas pero hay un período de 10 segundos en el que las nuevas sesiones de ese mismo origen a destinos con NAT fallan.



Ejemplo del problema

1. El ping se inicia desde el router de origen: Origen: 172.17.250.201 Destino: 198.51.100.9. El ping se emite con un conteo repetido de dos, una y otra vez [FLOW1].
2. A continuación, haga ping en un destino diferente que no esté siendo NAT-ed por el ASR1K: Origen: 172.17.250.201 Destino: 198.51.100.11 [FLOW2].
3. Luego envíe más paquetes a 198.51.100.9 [FLOW1]. Los primeros paquetes de este flujo omiten la NAT tal como lo ve la coincidencia de la lista de acceso en el router de 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#
```

La coincidencia de ACL en el router de destino muestra que los tres paquetes que fallaron no fueron traducidos:

<#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#
```

En el ASR1K puede verificar las entradas de la memoria caché del 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
```

Solución/Solución

En la mayoría de los entornos, la funcionalidad del gatekeeper de NAT funciona bien y no causa problemas. Sin embargo, si se encuentra con este problema, hay algunas maneras de resolverlo.

Solución 1

La opción preferida sería actualizar Cisco IOS® XE a una versión que incluya la mejora del gatekeeper:

ID de bug de Cisco CSCun06260 XE3.13 Refuerzo del gatekeeper

Esta mejora permite que el gatekeeper NAT almacene en memoria caché las direcciones de origen y destino, además de hacer configurable el tamaño de la memoria caché. Para activar el modo extendido, debe aumentar el tamaño de la memoria caché con estos comandos. También puede supervisar la caché para ver si necesita aumentar el tamaño.

```
<#root>

PRIMARY(config)#

ip nat settings gatekeeper-size 1024


PRIMARY(config)#

end
```

El modo extendido se puede verificar mediante la verificación de estos 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
```

Solución 2

Para las versiones que no tienen la corrección para el ID de bug Cisco CSCun06260, la única opción es desactivar la función de gatekeeper. El único impacto negativo es una ligera reducción del rendimiento para el tráfico sin NAT, así como una mayor utilización de la CPU en el

procesador 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#
```

La utilización de QFP se puede monitorear con estos comandos:

```
<#root>

show platform hardware qfp active data utilization summary


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

Solución 3

Separe los flujos de tráfico para que los paquetes NAT y los que no son NAT no lleguen a la misma interfaz.

Summary

El comando NAT Gatekeeper se introdujo para mejorar el rendimiento del router para los flujos sin NAT. En algunas condiciones, la función puede causar problemas cuando una mezcla de paquetes NAT y no NAT llega del mismo origen. La solución es utilizar la funcionalidad mejorada del gatekeeper, o si eso no es posible, inhabilite la función del gatekeeper.

Referencias

Cambios de software que permitieron desactivar el gatekeeper:
Id. de error de Cisco CSCty67184 ASR1k NAT CLI - Gatekeeper activado/desactivado

ID de bug de Cisco CSCth23984 Agregue la capacidad de cli para activar/desactivar la funcionalidad del gatekeeper NAT

Mejora de NAT Gatekeeper
ID de bug de Cisco CSCun06260 XE3.13 Refuerzo del gatekeeper

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).