ASR1k NAT no puede intermitentemente traducir algunos paquetes

Contenido

Introducción

Este artículo demuestra una situación donde los paquetes que se deben traducir por el NAT en un ASR1k no se están traduciendo (NAT que es desviado). Esto podría dar lugar al error del tráfico pues el salto siguiente es probable no configurado para permitir que los Paquetes sin traducir sean procesados.

Antecedentes

En la versión de software 12.2(33)XND una característica llamada portero NAT fue introducida y habilitada por abandono. (Observe esto no tiene nada hacer con H.323). Diseñaron al portero NAT para evitar que los flujos del NON-NAT-ed usen el CPU excesivo en un esfuerzo para crear una traducción de NAT. Para alcanzar esto, dos pequeños cachés (uno para la dirección in2out y uno para la dirección out2in) se crean sobre la base de la dirección de origen. Cada entrada de caché consiste en una dirección de origen, un VRF ID, un valor del temporizador (usado para invalidar la entrada después de 10 segundos), y un contador de la trama. Hay las entradas 256 en la tabla que compone el caché. Si no lo hace hay flujos del tráfico múltiple de la misma dirección de origen donde algunos paquetes requieren el NAT y algo, podría dar lugar a los paquetes que no eran NAT-ed y enviado a través del router sin traducir. Cisco recomienda que los clientes deben evitar tener NAT-ed y el NON-NAT-ed fluye en la misma interfaz donde sea posible.

Demostración del NAT que es desviado

La sección siguiente describe cómo el NAT puede ser desviado debido a la característica del portero NAT. Revise por favor el diagrama detalladamente. Podemos ver que hay un router de

origen, un Firewall ASA, los ASR1k, y el router de destino.

Flujos de tráfico al destino del NON-NAT-ed:

1) El ping se inicia de la fuente: Fuente: Destino de 172.17.250.201: 198.51.100.11
2) El paquete llega en la interfaz interior del ASA que realiza la traducción de la dirección de origen. El paquete ahora tendrá fuente: Destino de 203.0.113.231: 198.51.100.11
3) El paquete llega el ASR1k en el NAT afuera a la interfaz interior. La traducción de NAT no encuentra ninguna traducción para la dirección destino y así que pueblan al portero “hacia fuera” ocultar con la dirección de origen 203.0.113.231
4) El paquete llega el destino. El destino valida los paquetes icmp y devuelve una respuesta de eco ICMP dando por resultado el éxito del ping.

El tráfico de la misma fuente intenta enviar el destino del NAT-ed:

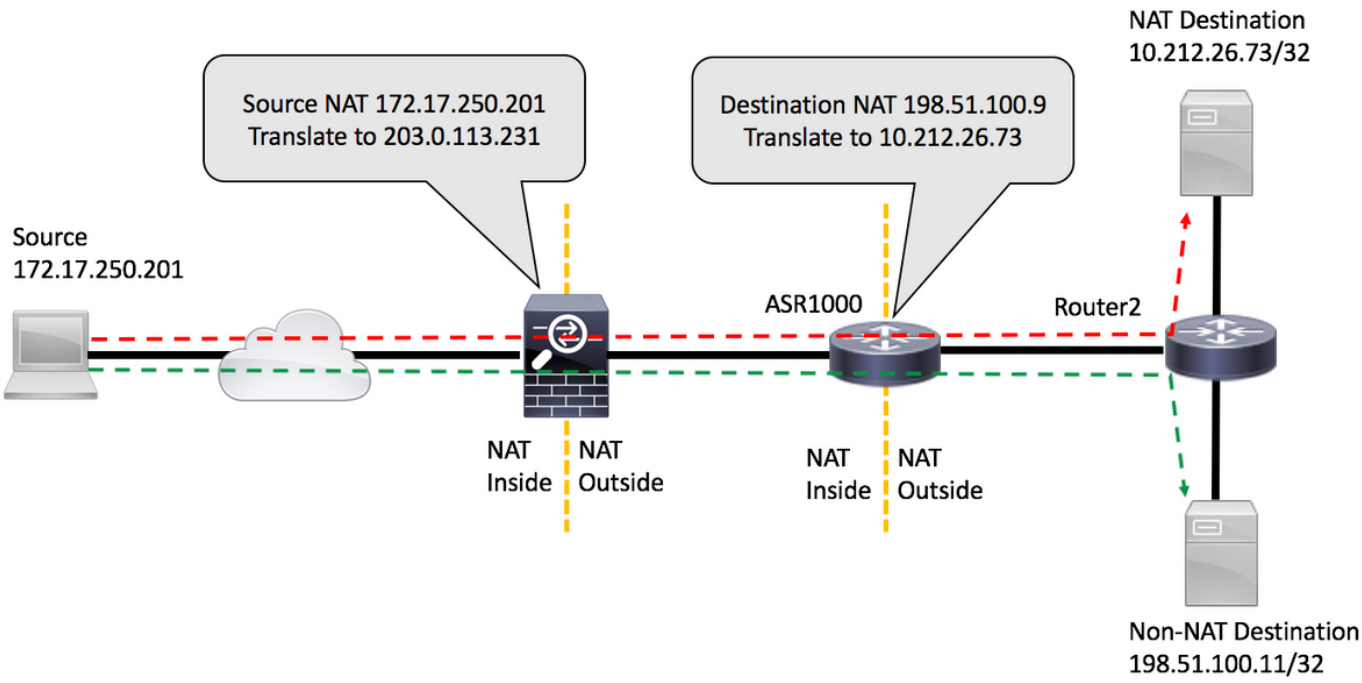
1) El ping se inicia de la fuente: Fuente: Destino de 172.17.250.201: 198.51.100.9
2) El paquete llega en la interfaz interior del ASA que realiza la traducción de la dirección de origen. El paquete ahora tendrá fuente: Destino de 203.0.113.231: 198.51.100.9
3) El paquete llega el ASR1k en el NAT afuera a la interfaz interior. El NAT primero busca una traducción para la fuente y el destino. No encontrando uno, marca al portero “” oculta y descubre a la dirección de origen 203.0.113.231. (Erróneamente) asume que el paquete no necesita la traducción y tampoco adelante el paquete si una ruta existe para el destino o cae el paquete. Cualquier manera, el paquete no alcanzará el destino deseado.

Restauración del tráfico del NAT-ed

1) Después de 10 segundos, la entrada para la dirección de origen 203.0.113.231 mide el tiempo hacia fuera en el portero hacia fuera oculta. (Nota que la entrada todavía existe físicamente en el caché pero porque ha expirado, no se utiliza).

2) Ahora si la misma fuente: 172.17.250.201 envía al destino 198.51.100.9 del NAT-ed, cuando el paquete llega la interfaz out2in en el ASR1K, ninguna traducción será encontrado. Cuando marcamos al portero hacia fuera ocultamos, no encontraremos una entrada activa y así que crearemos la traducción para el flujo del willl del destino y de los paquetes como se esperaba.

3) El tráfico en este flujo continuará mientras las traducciones no sean hacia fuera medido el tiempo debido a la inactividad. Si mientras tanto, la fuente envía otra vez el tráfico a un destino del NON-NAT-ed, haciendo otra entrada ser poblado en el portero hacia fuera oculte, él no afectará a las sesiones establecidas pero habrá un segundo período 10 en el cual las nuevas sesiones de esa misma fuente a los destinos del NAT-ed fallarán.



Ejemplo del problema

1) El ping se inicia del router de origen: Fuente: Destino de 172.17.250.201: 198.51.100.9. El ping se publica con el Repetir conteo de 2, repetidamente [FLOW1].

2) Entonces haga ping un diverso destino que no esté siendo NAT-ed por la fuente ASR1k: 172.17.250.201 Destination:198.51.100.11 [FLOW2].

3) Entonces envíe más paquetes a 198.51.100.9 [FLOW1]. Los primeros paquetes de este flujo desviarán el NAT según lo visto por la lista de acceso que corresponde con en el router 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#
```

La coincidencia ACL en el router de destino muestra a 3 paquetes que fallado, no fueron traducidos:

```
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 ASR1k podemos marcar las entradas del caché del portero:

```
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/arreglo:

En la mayoría de los entornos los trabajos de la funcionalidad de gatekeeper NAT muy bien sin causar los problemas. Sin embargo si usted se ejecuta en este problema hay algunas maneras de resolverlo.

Solución #1:

La opción preferida sería actualizar IOS-XE a una versión que incluye la mejora del portero:

Endurecimiento del portero CSCun06260 XE3.13

Esta mejora permite para que el portero NAT oculte la fuente **y a las** direcciones destino, así como haga el tamaño de la memoria caché configurable. Para girar al modo extendido, usted necesita aumentar el tamaño de la memoria caché con los siguientes comandos. Usted puede también monitorea el caché para ver si usted necesita aumentar el tamaño.

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

El modo extendido puede ser verificado marcando los siguientes comandos:

```
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 el arreglo para CSCun06260, la única opción es apagar la característica del portero. El único impacto negativo será levemente rendimiento reducido para el tráfico del NON-NAT-ed así como una utilización de la CPU más alta en el 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#
```

La utilización QFP se puede monitorear con:

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

Solución #3:

Separe los flujos de tráfico de modo que los paquetes NAT y NON-NAT no lleguen en la misma interfaz.

Resumen

Presentaron al comando gatekeeper NAT de aumentar el funcionamiento del router para los flujos del NON-NAT-ed. Bajo algunas condiciones la característica puede causar los problemas cuando una mezcla de los paquetes NAT y NON-NAT llega de la misma fuente. La solución es utilizar la funcionalidad de gatekeeper aumentada, o si eso no es posible, inhabilita la característica del portero.

Referencias

Cambios de software que permitieron que apagaran al portero:

CSCty67184 ASR1k NAT CLI - Portero con./desc.
CSCth23984 agregan la capacidad cli para dar vuelta a la funcionalidad de gatekeeper nacional

con./desc.

Mejora del portero NAT

Endurecimiento del portero CSCun06260 XE3.13