ASR1k NAT периодически не в состоянии преобразовывать некоторые пакеты

Содержание

Введение

Эта статья демонстрирует ситуацию, где пакеты, которые должны быть преобразованы NAT на ASR1k, не преобразовываются (обойденный NAT). Это могло привести к сбою трафика, поскольку следующий переход, вероятно, не настроен, чтобы позволить непереданный пакетам быть обработанными.

Общие сведения

В версии программного обеспечения 12.2 (33) XND опция под названием Сторожевое устройство NAT была представлена и активирована по умолчанию. (Обратите внимание, что это не имеет никакого отношения к H.323). Сторожевое устройство NAT было разработано, чтобы препятствовать тому, чтобы непреобразованные посредством NAT потоки использовали чрезмерный ЦП, чтобы создать преобразование NAT. Для достижения этого два маленьких кэша (один для in2out направления и один для out2in направления) созданы на основе адреса источника. Каждая запись в кэше состоит из адреса источника, ID VRF, значение таймера (использовал лишать законной силы запись после 10 секунд), и счетчик кадра. Существует 256 записей в таблице, которая составляет кэш. Если существует несколько классов трафика, вытекает из того же адреса источника, где некоторые пакеты требуют NAT, и некоторые не делают, это могло привести к пакетам, не являющимся преобразованным посредством NAT и передаваемым через непреобразованный маршрутизатор. Cisco рекомендует, чтобы клиенты избежали иметь преобразованные посредством NAT и непреобразованные посредством NAT потоки на том же интерфейсе по мере возможности.

Демонстрация обойденного NAT

Следующий раздел описывает , как NAT может быть обойден из-за функции сторожевого устройства NAT. Рассмотрите схему подробно. Мы видим, что существует исходный маршрутизатор, межсетевой экран ASA, ASR1k и маршрутизатор назначения.

Трафики назначению Non-NAT-ed:

1) Эхо-запрос инициируется из источника: Источник: 172.17.250.201 Назначение: 198.51.100.11
2) Пакет поступает во внутренний интерфейс ASA, который выполняет трансляцию адреса источника. Пакет будет теперь иметь Источник: 203.0.113.231 Назначение: 198.51.100.11
3) Пакет поступает в ASR1k на NAT снаружи к внутреннему интерфейсу. Преобразование NAT не находит трансляции для адреса назначения (DA) и так сторожевое устройство, кэш заполнен с адресом источника 203.0.113.231
4) Пакет прибывает к месту назначения. Назначение принимает пакет ICMP и возвращает ЭХО - ОТВЕТ ICMP, приводящее к успеху эхо-запроса.

Трафик из того же источника пытается передать преобразованному посредством NAT назначению:

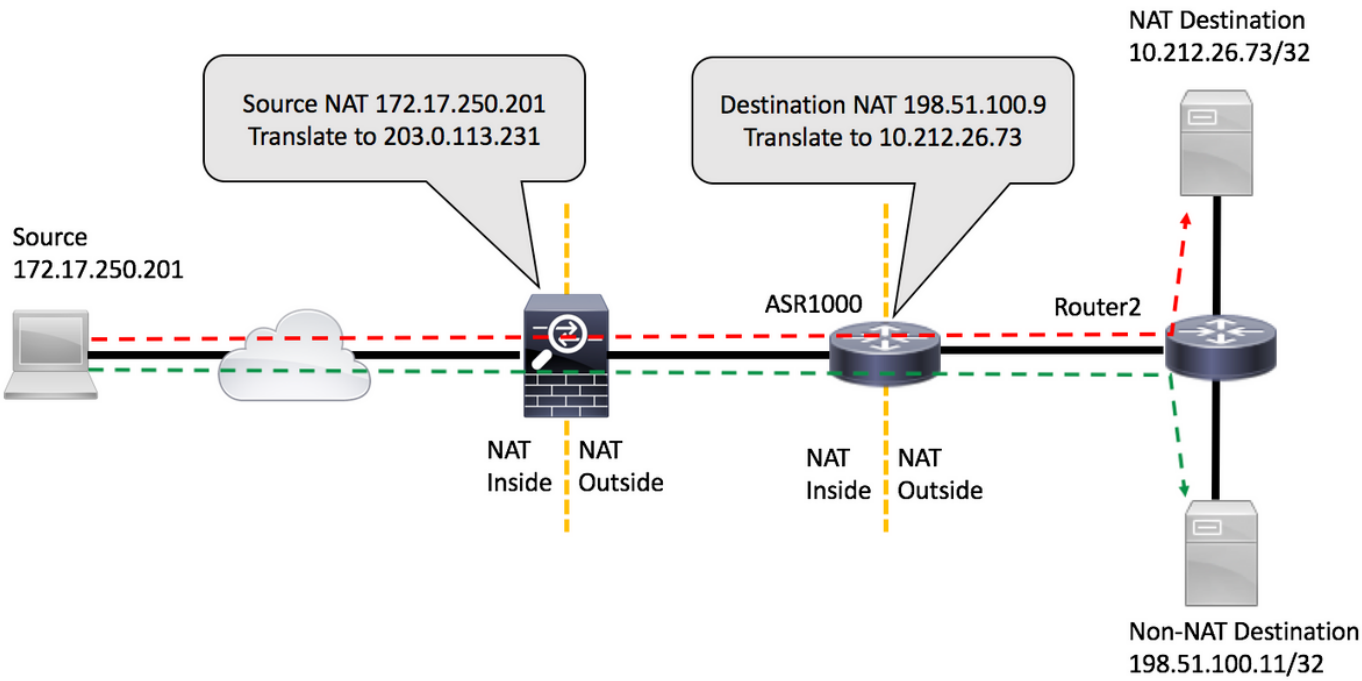
1) Эхо-запрос инициируется из источника: Источник: 172.17.250.201 Назначение: 198.51.100.9
2) Пакет поступает во внутренний интерфейс ASA, который выполняет трансляцию адреса источника. Пакет будет теперь иметь Источник: 203.0.113.231 Назначение: 198.51.100.9
3) Пакет поступает в ASR1k на NAT снаружи к внутреннему интерфейсу. NAT сначала ищет трансляцию для Источника и Назначения. Не находя один, это проверяет сторожевое устройство кэш и находит Адрес источника 203.0.113.231. Это (ошибочно) предполагает, что пакет не нуждается в трансляции и или передает пакет, если маршрут существует для назначения или отбрасывает пакет. Так или иначе пакет не достигнет целевого места назначения.

Восстановление преобразованного посредством NAT трафика

1) После 10 секунд, записи для Адреса источника 203.0.113.231 таймаутов в сторожевом устройстве кэш. (Обратите внимание на то, что запись все еще физически существует в кэше, но потому что это истекло, это не используется).

2) Теперь, если тот же Источник: 172.17.250.201 передает преобразованному посредством NAT назначению 198.51.100.9, когда пакет поступит в интерфейс out2in на ASR1K, никакая трансляция не будет найдена. Когда мы проверим сторожевое устройство кэш, мы не найдем активную запись и таким образом, мы создадим трансляцию для назначения и пакетов willl поток как ожидалось.

3) Трафик в этом потоке продолжится, пока трансляции не вызваны таймаут из-за бездействия. Если тем временем, источник снова передаст трафик непреобразованному посредством NAT назначению, заставляя другую запись быть заполненным в сторожевом устройстве кэш, то это не будет влиять на установленные сеансы, но будет 10 вторых периодов, в которых откажут новые сеансы от того же самого источника до преобразованных посредством NAT назначений.



Пример проблемы

1) Эхо-запрос инициируется от исходного маршрутизатора: Источник: 172.17.250.201 Назначение: 198.51.100.9. Эхо-запрос выполнен с повторным счетом 2, много раз [FLOW1].

2) Затем пропингуйте другое назначение, которое не преобразовано посредством NAT Источником ASR1k: 172.17.250.201 Destination:198.51.100.11 [FLOW2].

3) Затем передайте больше пакетов к 198.51.100.9 [FLOW1]. Первые несколько пакетов этого потока обойдут NAT, как замечено access-list, совпадающим на маршрутизаторе назначения.

```
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#
```

Соответствие ACL на маршрутизаторе назначения показывает 3 пакета, которые отказали, не были преобразованы:

```
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#
```

На ASR1k мы можем проверить записи в кэше сторожевого устройства:

```
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
```

Обходной путь / Исправляет:

В большинстве сред функциональные возможности сторожевого устройства NAT хорошо работают, не вызывая проблемы. Однако, при столкновении с этой проблемой существует несколько способов решить его.

Решение 1:

Предпочтительный вариант состоял бы в том, чтобы обновить XE IOS к версии, которая включает усовершенствование сторожевого устройства:

Укрепление сторожевого устройства CSCun06260 XE3.13

Это усовершенствование обеспечивает сторожевое устройство NAT для кэширования источника **и** адресов назначения (DA), а также создания конфигурируемого размера кэша. Для включения расширенного режима необходимо увеличить размер кэша со следующими командами. Можно также контролировать кэш, чтобы

видеть, необходимо ли увеличить размер.

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

Расширенный режим может быть проверен путем проверки следующих команд:

```
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
```

Решение 2:

Для версий, которые не имеют исправления для CSCun06260, единственная опция должна выключить функцию сторожевого устройства. Единственное негативное воздействие будет немного пониженной производительностью для непреобразованного посредством NAT трафика, а также повышенной загрузкой ЦП на 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#
```

Использование QFP может быть проверено с:

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

Решение 3:

Отдельные трафики так, чтобы NAT и пакеты не-NAT не поступали в тот же интерфейс.

Сводка

Команда NAT Gatekeeper была представлена для улучшения производительности маршрутизатора для непреобразованных посредством NAT потоков. Когда соединение NAT и пакетов не-NAT поступает из того же источника, при некоторых условиях функция может вызвать проблемы. Решение состоит в том, чтобы использовать расширенные функциональные возможности сторожевого устройства, или если это не возможно, отключите опцию сторожевого устройства.

Ссылки

Изменения ПО, которые позволили сторожевому устройству быть выключенным:

CSCty67184 ASR1k NAT CLI - сторожевое устройство вкл\выкл
CSCth23984 Добавляют возможность cli повернуть туземные функциональные возможности сторожевого устройства включения - выключения

Усовершенствование Сторожевого устройства NAT

Укрепление сторожевого устройства CSCun06260 XE3.13