ASR1k NAT间歇地不能转换一些数据包

目录

简介

此条款展示数据包应该由在ASR1k的NAT翻译没有翻译的一个情况(绕过的NAT)。因为可能不已配置的允许未翻译的数据包的下一跳将处理，这可能导致流量失败。

背景信息

默认情况下在软件版本12.2(33)XND中呼叫NAT网守的功能介绍并且启用。 (请注释此与H.323无关)。 NAT网守设计防止非NAT ED流使用额外的CPU创建NAT转换。 要达到此，两个小缓存(一in2out方向的和一out2in方向的)根据源地址创建。 每缓存条目包括源地址、VRF ID、计时器值(用于在10秒之后无效条目)和帧计数器。 有256个条目在组成缓存的表里。 如果有从一些数据包要求NAT和一些的同一源地址的多个信息数据流运输流量不，可能导致不NAT的数据包，并且发送通过路由器取消转译。 思科建议客户应该避免在任何可能的情况下NAT和在同一个接口的非NAT ED流。

绕过的NAT的演示

以下部分描述NAT如何可以绕过的归结于NAT关守功能。 请详细请查看图表。 我们能看到有源路由器、ASA防火墙、ASR1k和目标路由器。

对非NAT ED目的地的通信流：

1) Ping从来源启动：来源：172.17.250.201目的地：198.51.100.11
2) 数据包在进行源地址地址转换ASA的内部接口到达。 数据包当前将有来源：203.0.113.231目的地：198.51.100.11
3) 数据包从外部到达在NAT的ASR1k对内部接口。 NAT转换不查找目的地址的转换和，因此网守“”缓存带有源地址203.0.113.231

4) 数据包到达在目的地。目的地接受ICMP数据包并且返回ICMP echo应答造成ping成功。

从同样来源的流量尝试发送NAT的目的地：

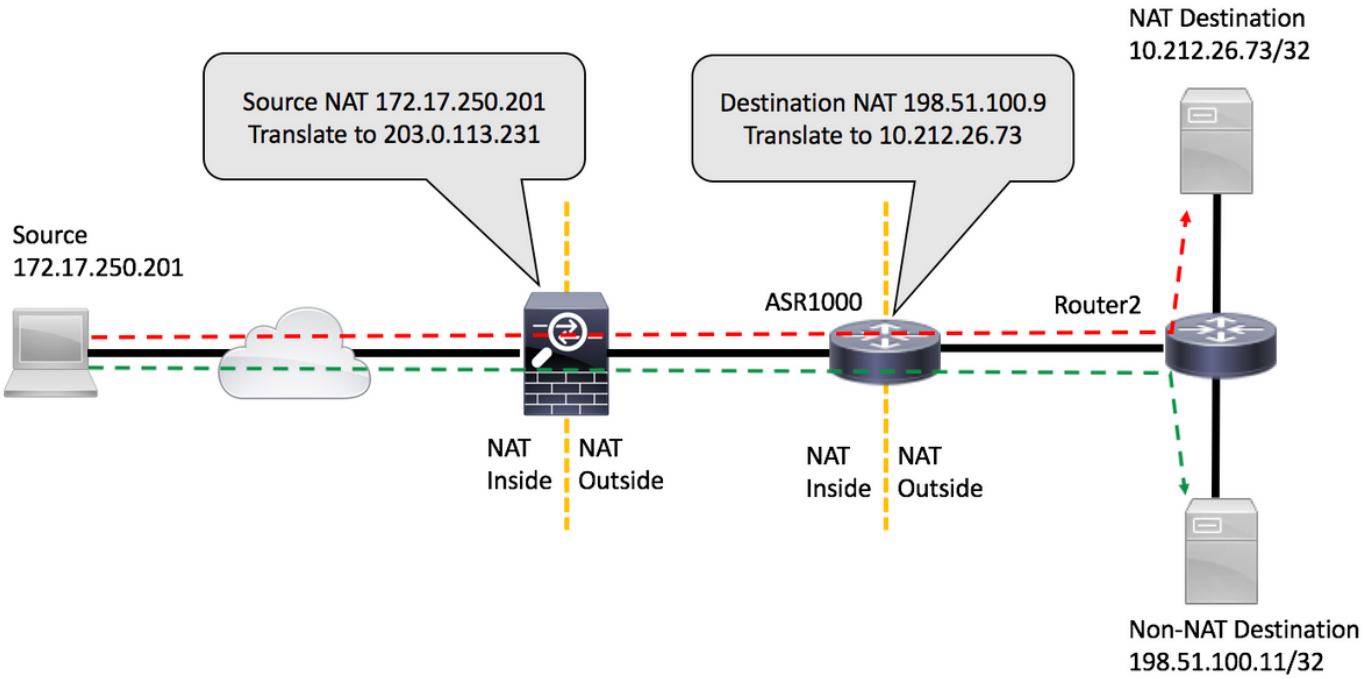
1) Ping从来源启动：来源：172.17.250.201目的地：198.51.100.9
2) 数据包在进行源地址地址转换ASA的内部接口到达。 数据包当前将有来源：203.0.113.231目的地：198.51.100.9
3) 数据包从外部到达在NAT的ASR1k对内部接口。 NAT首先寻找源和目的一个转换。 不查找一，它检查网守“”缓存并且发现源地址203.0.113.231。 它(不正确)假设，数据包不需要转换和或者转发数据包，如果路由为目的地存在或丢弃数据包。 不管怎样，数据包不会到达有意目的地。

NAT-ed流量的恢复

1) 在10秒之后，源地址的203.0.113.231条目在网守计时缓存。(请注意条目在缓存物理的仍然存在，但是，因为超时，没有使用)。

2) 现在，如果同样来源：，当数据包到达在ASR1K的out2in接口，没有转换将找到对NAT的目的地198.51.100.9的172.17.250.201发送。 当我们检查网守缓存，我们不会查找一个活动条目，并且，因此我们将创建目的地和数据包willl流的转换正如所料。

3) 只要转换不被计时的归结于非活动，在此流的流量将继续。如果同时，来源再发送流量对非NAT ED目的地，造成另一个条目填充在网守请缓存，它不会影响建立的会话，但是那里是从该同样来源的新建的会话到NAT的目的地失效的10第二个周期。



问题的示例

1) Ping从源路由器启动：来源：172.17.250.201目的地：198.51.100.9。 ping发出与重复计数2，多次[FLOW1]。

2) 然后请ping没有由ASR1k来源NAT的一个不同的目的地：172.17.250.201 Destination:198.51.100.11 [FLOW2]。

3) 然后请发送更多数据包对198.51.100.9 [FLOW1]。 最初的少数数据包此流将绕过NAT如看到通过访问列表匹配在目标路由器。

```
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#
```

在目标路由器的ACL匹配显示失败，未翻译的3数据包：

```
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#
```

在ASR1k我们能检查网守缓存条目：

```
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
```

应急方案/修正：

在多数环境良好NAT网守功能工作没有导致问题。 然而，如果遇到此问题有一些个方式解决它。

解决方案#1 ：

首选是升级IOS-XE对包括网守增强的版本：

CSCun06260 XE3.13网守硬化

此增强允许NAT网守缓存来源**和**目的地址，以及进行可配置的缓存容量。 为了打开扩展模式，您需要增加缓存容量用以下命令。 您能也监控缓存发现是否需要增加大小。

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

扩展模式可以通过检查以下命令验证：

```
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
```

解决方案#2 ：

对于没有CSCun06260的修正的版本，唯一选择是关闭关守功能。 唯一的负面影响将轻微是非NATED流量的降低的性能以及在QFP的更加高的CPU利用率。

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

PRIMARY#
```

QFP利用率可以监控与：

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

解决方案#3 ：

分离通信流，以便NAT和非NAT数据包在同一个接口不到达。

摘要

gatekeeper命令的NAT介绍提高路由器的性能非NAT ED流的。 在某些条件下，当NAT的混合和非NAT数据包从同一来源时，到达功能可能引起问题。 解决方案将使用增强版网守功能，或者，如果那不是可能的，禁用关守功能。

参考

软件变更将被关闭的允许网守：

CSCty67184 ASR1k NAT CLI -网守开/关
CSCth23984添加cli功能启用开/关nat网守功能

NAT网守增强

CSCun06260 XE3.13网守硬化