ASR1K NAT间歇性转换某些数据包失败

目录

简介

本文档介绍在Cisco 1000系列聚合服务路由器(ASR1K)上应通过网络地址转换(NAT)进行转换的数据包不进行转换（绕过NAT）的情况。 这可能导致流量失败，因为可能未将下一跳配置为允许处理未转换的数据包。

背景信息

在软件版本12.2(33)XND中，默认引入并启用了名为NAT网守的功能。NAT网守旨在防止非NAT流在创建NAT转换时使用过多的CPU。为此，根据源地址创建两个小缓存（一个用于in2out方向，一个用于out2in方向）。每个缓存条目都包括源地址、虚拟路由和转发(VRF)ID、计时器值（用于在10秒后使条目失效）和帧计数器。表中有256个条目构成缓存。如果来自同一源地址的多个流量传输，其中一些数据包需要NAT，而另一些则不需要，则可能导致数据包未通过NAT传输并通过路由器进行未转换的发送。思科建议客户尽可能避免在同一接口上出现NAT和非NAT流。

> **注意**：这与H.323无关。

NAT被绕过的演示

本节介绍如何由于NAT网守功能而绕过NAT。详细查看图。您可以看到源路由器、自适应安全设备(ASA)防火墙、ASR1K和目标路由器。

流向非NAT目的地的流量

1. 从源启动Ping:来源：172.17.250.201 目的地址：198.51.100.11 的多播地址发送一次邻居消息。

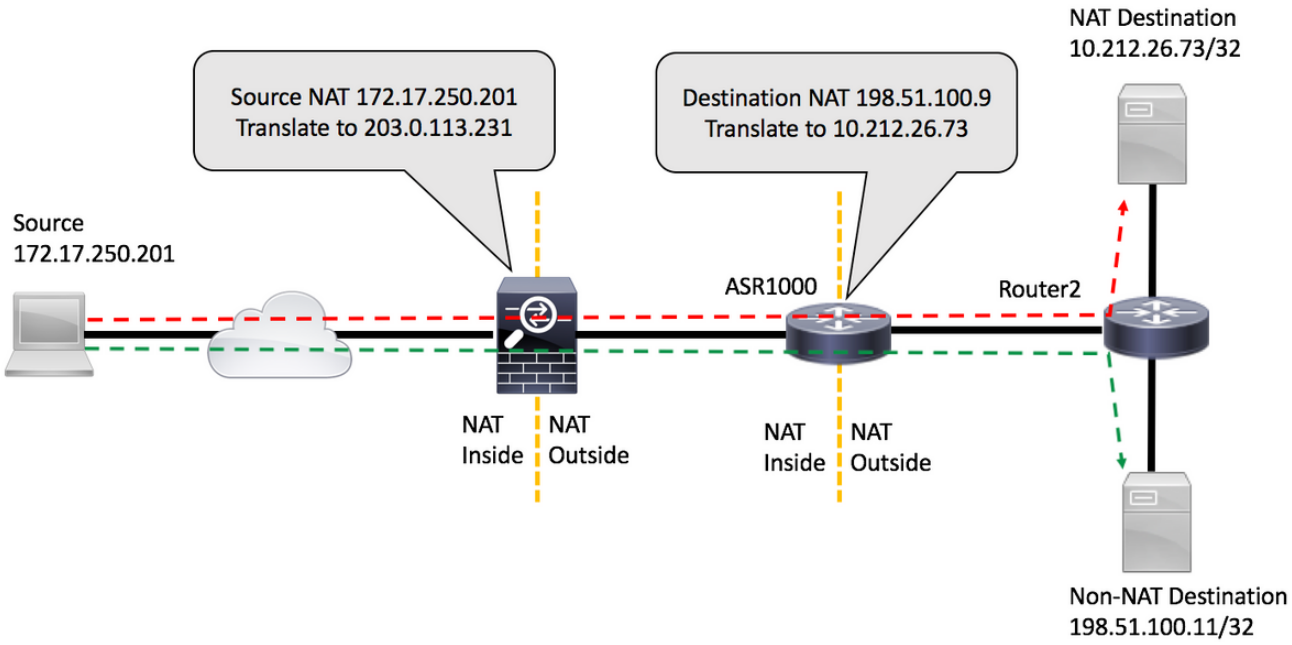
2. 数据包到达执行源地址转换的ASA的内部接口。数据包现在将具有Source:203.0.113.231 目的地址：198.51.100.11 的多播地址发送一次邻居消息。
3. 数据包到达NAT外部到内部接口上的ASR1K。NAT转换找不到目标地址的转换，因此网守“out”缓存填充了源地址203.0.113.231。
4. 数据包到达目的地。目的地接受互联网控制消息协议(ICMP)数据包并返回ICMP ECHO应答，从而导致ping成功。

来自同一源的流量尝试发送NAT目的地

1. .Ping从源启动：来源：172.17.250.201 目的地址：198.51.100.9 的多播地址发送一次邻居消息。
2. 数据包到达执行源地址转换的ASA的内部接口。数据包现在将具有Source:203.0.113.231 目的地址：198.51.100.9 的多播地址发送一次邻居消息。
3. 数据包到达NAT外部到内部接口上的ASR1K。NAT首先查找源和目标的转换。由于没有找到，它会检查网守“out”缓存并找到源地址203.0.113.231。它（错误地）假设数据包不需要转换，如果存在通往目的地的路由，则转发数据包或丢弃数据包。无论哪种方式，数据包都无法到达预期目的地。

恢复NAT流量

1. 10秒后，源地址203.0.113.231的条目在网守外缓存中超时。 **注意**：该条目在物理上仍存在于缓存中，但因为它已过期，所以不会使用它。
2. 现在，如果同一源172.17.250.201发送到NAT-ed目标198.51.100.9。当数据包到达ASR1K的out2in接口时，将找不到转换。当您将网守签出缓存时，您将找不到活动条目，因此您将创建目标的转换，数据包将按预期流量。
3. 只要转换没有因不活动而超时，此流中的流量将继续。同时，如果源再次将流量发送到非NAT目的地，导致另一个条目在网守缓存外填充，则不会影响已建立的会话，但会有10秒的时间段，从同一源到NAT目的地的新会话将失败。



问题示例

1. 从源路由器启动Ping:来源：172.17.250.201 目的地址：198.51.100.9。发出ping命令，重复计数为2，上过[FLOW1]。
2. 然后，对ASR1K未通过NAT的其他目标执行ping操作：来源：172.17.250.201目的地：198.51.100.11 [FLOW2]。
3. 然后向198.51.100.9 [FLOW1]发送更多数据包。此流的前几个数据包将绕过NAT，如目的路由器上的访问列表匹配所示。

```
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#
```

目的路由器上的ACL匹配显示失败的三个数据包未转换：

```
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上，您可以检查网守缓存条目：

```
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
```

解决方法/修复

在大多数环境中，NAT网守功能工作正常，不会导致问题。但是，如果您确实遇到此问题，有几种方法可以解决它。

解决方案 1

首选选项是将Cisco IOS® XE升级到包含网守增强功能的版本：

Cisco Bug ID CSCun06260 XE3.13网守加固

此增强功能允许NAT网守缓存源**地址**和目标地址，并使缓存大小可配置。要打开扩展模式，您需要使用这些命令增加缓存大小。您还可以监控缓存，以查看是否需要增加大小。

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

可通过检查以下命令来验证扩展模式：

```
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Cisco Bug ID CSCun06260修复的版本，唯一的选项是关闭网守功能。唯一的负面影响是非NAT流量的性能略有下降，以及量子流处理器(QFP)的CPU利用率更高。

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

PRIMARY#
```

可以使用以下命令监控QFP利用率：

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

解决方案 3

分离流量，使NAT和非NAT数据包不到达同一接口。

摘要

引入NAT网守命令是为了增强路由器对非NAT流的性能。在某些情况下，当NAT和非NAT数据包混合从同一源到达时，该功能可能会导致问题。解决方案是使用增强的网守功能，或者如果不能，请禁用网守功能。

参考

允许关闭网守的软件更改：
Cisco Bug ID CSCty67184 ASR1k NAT CLI — 网守开/关
Cisco Bug ID CSCth23984添加cli功能以打开/关闭nat网守功能

NAT网守增强
Cisco Bug ID CSCun06260 XE3.13网守加固