排除IOS-XE NAT间歇性故障以转换某些数据包

目录

简介

本文档介绍在Cisco IOS XE路由器上绕过NAT的未转换数据包，这些数据包可能导致流量故障。

背景信息

在软件版本12.2(33)XND中，引入并默认启用了一个名为网络地址转换(NAT)网守的功能。NAT网守旨在防止非NAT处理的流使用过多的CPU来创建NAT转换。为此，将根据源地址创建两个小型缓存（一个用于in2out方向，一个用于out2in方向）。每个缓存条目都包含一个源地址、一个虚拟路由和转发(VRF)ID、一个计时器值（用于在10秒后使条目失效）和一个帧计数器。表中有256个条目组成缓存。如果存在来自同一源地址的多个流量，其中有些数据包需要NAT，有些则不需要NAT，这可能会导致数据包无法进行NAT处理，并通过路由器发送，而不进行转换。Cisco建议客户尽可能避免在同一接口上进行NAT和非NAT流量。

注：这与H.323无关。

受影响的平台

- ISR1K
- ISR4000
- C8200
- C8300
- C8500

绕过NAT的演示

本节介绍如何通过NAT网守功能绕过NAT。详细查看该图。您可以看到存在源路由器、自适应安全设备(ASA)防火墙、ASR1K和目标路由器。

流向非NAT转换目标的流量

1. 从源设备发起Ping：源：172.17.250.201目的：198.51.100.11。
2. 数据包到达执行源地址转换的ASA的内部接口。数据包现在具有源：203.0.113.231目的：198.51.100.11。
3. 数据包到达NAT外部到内部接口的ASR1K。NAT转换找不到目标地址的转换，因此网守“out”缓存填充源地址203.0.113.231。
4. 数据包到达目的地。目标接受Internet控制消息协议(ICMP)数据包并返回ICMP应答，从而导致ping成功。

来自相同源的流量尝试发送NAT转换的目标

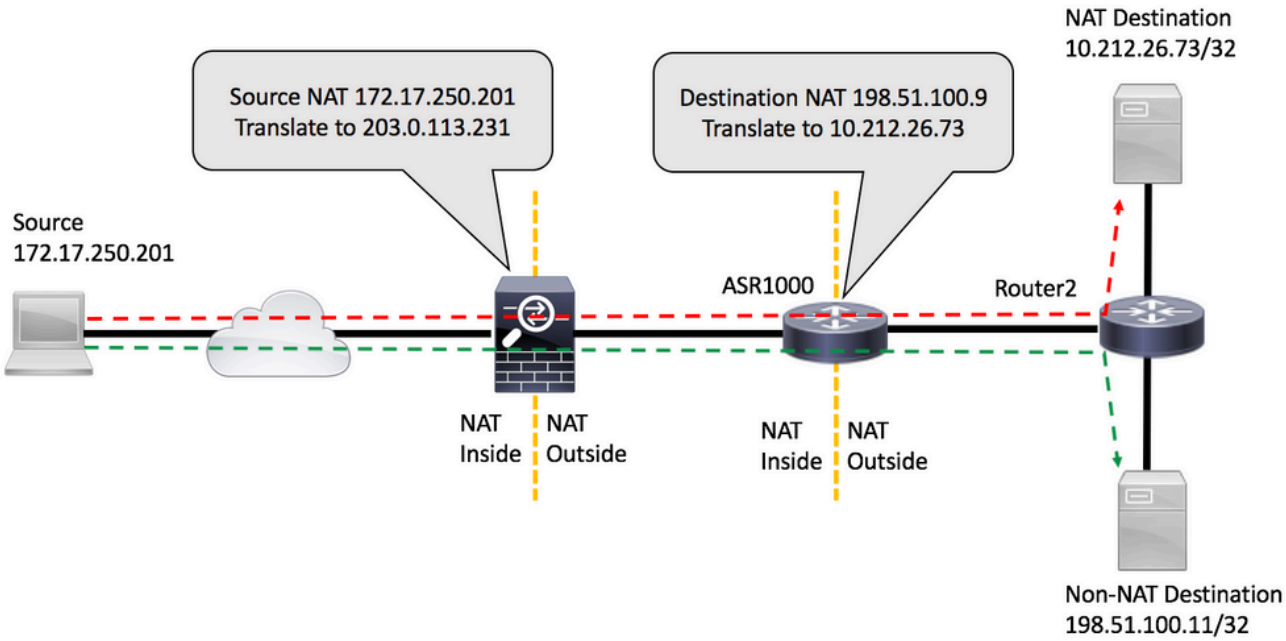
1. .ping从源设备启动：源：172.17.250.201目的：198.51.100.9。
2. 数据包到达执行源地址转换的ASA的内部接口。数据包现在具有源：203.0.113.231目的：198.51.100.9。
3. 数据包到达NAT外部到内部接口的ASR1K。NAT首先查找源和目标的转换。由于它没有找到一个，因此它会检查网守“out”缓存并查找源地址203.0.113.231。它（错误）假设数据包不需要转换，如果存在目的地的路由，它会转发数据包，或者丢弃数据包。无论哪种方式，数据包都无法到达预定目的地。

恢复NAT转换的流量

1. 10秒后，源地址203.0.113.231的条目在网守输出缓存中超时。

   注意：条目在缓存中仍然实际存在，但由于其已过期，因此未使用它。

2. 现在，如果同一个源172.17.250.201发送到NAT转换的目标198.51.100.9。当数据包到达ASR1K的out2in接口时，找不到转换。当您检查网守输出缓存时，您找不到活动条目，因此您可以按照预期为目标和数据包流创建转换。
3. 只要转换不因不活动而超时，此流量中的流量就会继续。同时，如果源再次向非NAT目标发送流量，导致从缓存中填充另一个条目到网守中，则不会影响已建立的会话，但有10秒的时间段内从同一源到NAT目标的新会话失败。



问题示例

1. 从源路由器发起ping：源：172.17.250.201目的：198.51.100.9。在[FLOW1]上重复计数为2时发出ping。
2. 然后ping ASR1K未进行NAT处理的另一个目的地：源：172.17.250.201目的地：198.51.100.11 [FLOW2]。
3. 然后将更多数据包发送到198.51.100.9 [FLOW1]。从目标路由器上的访问列表匹配可以看出，此流的前几个数据包绕过NAT。

<#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#
```

目标路由器上的ACL匹配显示未转换失败的三个数据包：

<#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#
```

在ASR1K上，您可以检查网守缓存条目：

<#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
```

解决方法/修复

在大多数环境中，NAT gatekeeper功能运行正常，不会引起问题。但是，如果确实遇到此问题，有几种方法可以解决。

解决方案 1

首选方法是将Cisco IOS® XE升级为包含网守增强功能的版本：

Cisco Bug ID CSCun06260 XE3.13网守强化

此增强功能允许NAT网守缓存源地址和目的地地址，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。

```
<#root>

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：

```
<#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
```

解决方案 2

对于没有Cisco Bug ID CSCun06260修复程序的版本，唯一的选项是关闭网守功能。唯一的负面影响是非NAT流量的性能略有降低，以及量子流处理器(QFP)上的CPU使用率较高。

```
<#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#
```

可以使用以下命令监控QFP利用率：

<#root>

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

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

解决方案 3

分隔流量，使NAT和非NAT数据包不会到达同一接口。

摘要

引入了NAT Gatekeeper命令来增强路由器对非NAT流量的性能。在某些情况下，当NAT和非NAT数据包混合从同一源到达时，此功能可能会引起问题。解决方案是使用增强的网守功能，或者如果不可能的话，禁用网守功能。

参考

允许关闭网守的软件更改：
思科漏洞ID CSCty67184 ASR100 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网守强化

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。