Probleemoplossing voor IOS-XE NAT intermitterend falen om bepaalde pakketten te vertalen

Inhoud

Inleiding

Dit document beschrijft niet-vertaalde pakketten die NAT op een Cisco IOS XE-router omzeilen, wat mogelijk een verkeersfout kan veroorzaken.

Achtergrondinformatie

In softwareversie 12.2(33)XND werd standaard een functie genaamd Network Address Translation (NAT) Gatekeeper geïntroduceerd en ingeschakeld. NAT Gatekeeper is ontworpen om te voorkomen dat niet-NAT-ed stromen buitensporige CPU's gebruiken om een NAT-vertaling te maken. Om dit te bereiken, worden twee kleine caches (één voor de in2out richting en één voor de out2in richting) gecreëerd gebaseerd op het bronadres. Elke cache-ingang bestaat uit een bronadres, een VRF-id (Virtual Routing and Forwarding), een timerwaarde (gebruikt om de ingang na 10 seconden ongeldig te maken) en een frameteller. Er zijn 256 inzendingen in de tabel die samen het cachegeheugen vormen. Als er meerdere verkeersstromen zijn van hetzelfde bronadres waar sommige pakketten NAT vereisen en sommige niet, kan dit ertoe leiden dat pakketten niet NAT-ed zijn en niet door de router worden verzonden. Cisco raadt klanten aan te voorkomen dat ze waar mogelijk NAT-ed en niet-NAT-ed stromen op dezelfde interface hebben.

Opmerking: Dit heeft niets te maken met H.323.

Betrokken platforms

- ISR1K
- ISR4K
- C820
- C830
- C850

Demonstratie van NAT die wordt omzeild

In deze sectie wordt beschreven hoe NAT kan worden overgeslagen vanwege de NAT-gatekeeper-functie. Bekijk het diagram in detail. U kunt zien dat er een bronrouter, een adaptieve security applicatie (ASA) firewall, de ASR1K en de doelrouter zijn.

Verkeersstromen naar niet-NAT-ed bestemming

1. Ping is geïnitieerd vanuit de bron: Bron: 172.17.250.201 Bestemming: 198.51.100.11.
2. Het pakket komt op de binneninterface van ASA aan die bronadresomzetting uitvoert. Het pakket heeft nu Bron: 203.0.13.231 Bestemming: 198.51.100.11.
3. Het pakket komt bij ASR1K op NAT buiten aan binneninterface aan. NAT-vertaling vindt geen vertaling voor het doeladres en dus wordt het gatekeeper-out-cache gevuld met het bronadres 203.0.113.231.
4. Het pakket komt bij de bestemming aan. De bestemming accepteert het ICMP-pakket (Internet Control Message Protocol) en retourneert een ICMP ECHO-antwoord dat resulteert in succes bij het pingen.

Het verkeer van de zelfde bron probeert om NAT-ed bestemming te verzenden

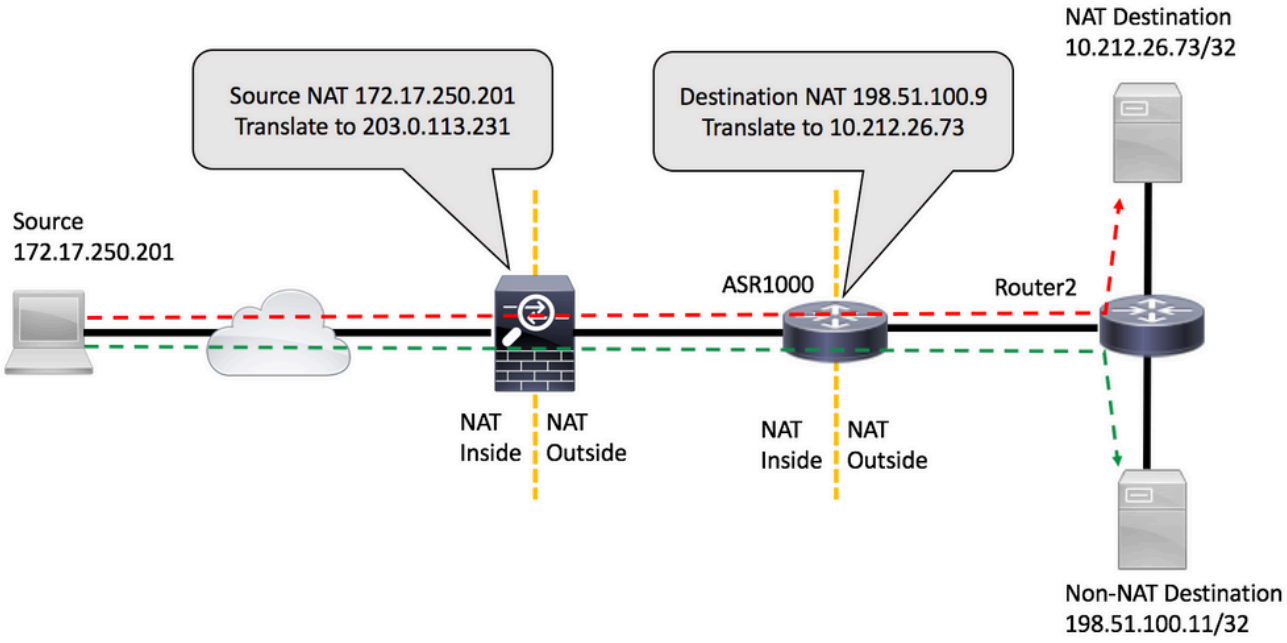
1. .Ping is geïnitieerd vanuit de bron: Bron: 172.17.250.201 Bestemming: 198.51.100.9.
2. Het pakket komt op de binneninterface van ASA aan die bronadresomzetting uitvoert. Het pakket heeft nu Bron: 203.0.13.231 Bestemming: 198.51.100.9.
3. Het pakket komt bij ASR1K op NAT buiten aan binneninterface aan. NAT zoekt eerst naar een vertaling voor de bron en de bestemming. Aangezien het geen één vindt, controleert het gatekeeper "uit"geheim voorgeheugen en vindt het bronadres 203.0.113.231. Het veronderstelt (verkeerd) dat het pakket geen vertaling nodig heeft en of door:sturen het pakket als een route voor de bestemming bestaat of het pakket laat vallen. Hoe dan ook, het pakket bereikt niet de beoogde bestemming.

Herstel van NAT-verkeer

1. Na 10 seconden, de ingang voor bronadres 203.0.113.231 keer uit in het gatekeeper out cachegeheugen.

> Opmerking: de vermelding bestaat nog steeds fysiek in het cache, maar omdat het is verlopen, wordt het niet gebruikt.

2. Nu, als dezelfde bron 172.17.250.201 naar NAT-ed bestemming 198.51.100.9 verzendt. Wanneer het pakket bij de out2in-interface op de ASR1K aankomt, is er geen vertaling gevonden. Wanneer u het gatekeeper out cache controleert, kunt u geen actieve ingang vinden, zodat u de vertaling voor de bestemming en de pakketstroom zoals verwacht creëert.
3. Het verkeer in deze stroom gaat door zolang de vertalingen niet uit zijn gezet vanwege inactiviteit. Als, in de tussentijd, de bron opnieuw verkeer naar een niet-NAT-ed bestemming verzendt, wat veroorzaakt dat een andere ingang wordt bevolkt in de poortwachter uit het cachegeheugen, beïnvloedt het geen gevestigde sessies maar er is een 10 tweede periode waarin nieuwe sessies van dezelfde bron naar NAT-ed bestemmingen mislukken.



Voorbeeld van de uitgifte

1. Ping wordt geïnitieerd vanuit de bronrouter: Bron: 172.17.250.201 Bestemming: 198.51.100.9. Pingel wordt uitgegeven met een herhalingstelling van twee, over en over [FLOW1].
2. Dan pingel een andere bestemming die niet NAT-ed door ASR1K wordt: Bron: 172.17.250.201 Bestemming:198.51.100.11 [FLOW2].
3. Verzend vervolgens meer pakketten naar 198.51.10.9 [FLOW1]. De eerste pakketten van deze stroom omzeilen NAT zoals gezien door de toegang-lijst aanpassing op de bestemmingsrouter.

<#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#
```

De ACL-overeenkomst op de doelrouter toont de drie mislukte pakketten die niet zijn vertaald:

<#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#
```

Op de ASR1K kunt u de gatekeeper cache items controleren:

<#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
```

Oplossing/oplossing

In de meeste omgevingen werkt de NAT gatekeeper functionaliteit prima en veroorzaakt geen problemen. Als je echter met dit probleem geconfronteerd wordt, zijn er een paar manieren om het op te lossen.

Oplossing 1

De voorkeursoptie zou zijn om Cisco IOS® XE te upgraden naar een versie die de gatekeeper-verbetering bevat:

Cisco bug-id CSCun06260 XE3.13 Gatekeeper hardening

Deze verbetering staat voor de NAT gatekeeper toe om de bron en de bestemmingsadressen in het voorgeheugen onder te brengen, evenals maakt de cachegrootte configureerbaar. Om de uitgebreide modus in te schakelen, moet u de cachegrootte vergroten met deze opdrachten. U kunt ook de cache controleren om te zien of u de omvang moet vergroten.

<#root>

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

PRIMARY(config)#
end
```

De uitgebreide modus kan worden geverifieerd door de volgende opdrachten te controleren:

<#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
```

Oplossing 2

Voor releases die geen oplossing hebben voor Cisco bug-id CSCun06260, is de enige optie de gatekeeper-functie uit te schakelen. De enige negatieve impact is een iets lagere prestatie voor niet-NAT-ed verkeer en een hoger CPU-gebruik voor de Quantum Flow Processor (QFP).

```
<#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#
```

Het gebruik van QFP kan met deze opdrachten worden gecontroleerd:

```
<#root>

show platform hardware qfp active data utilization summary

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

Oplossing 3

Aparte verkeersstromen zodat NAT- en niet-NAT-pakketten niet op dezelfde interface aankomen.

Samenvatting

Het NAT Gatekeeper-commando werd geïntroduceerd om de prestaties van de router voor niet-NAT-ed stromen te verbeteren. Onder bepaalde omstandigheden kan de functie problemen veroorzaken wanneer een combinatie van NAT- en niet-NAT-pakketten uit dezelfde bron arriveert. De oplossing is om de verbeterde gatekeeper functionaliteit te gebruiken, of als dat niet mogelijk is, de gatekeeper optie uit te schakelen.

Referenties

Software veranderingen waardoor gatekeeper uitgeschakeld kon worden:
Cisco bug-id CSCty67184 ASR1k NAT CLI - gatekeeper aan/uit
Cisco bug-id CSCth23984 Clich-mogelijkheid om NAT-gatekeeper functionaliteit in en uit te schakelen

NAT-gatekeeper verbetering
Cisco bug-id CSCun06260 XE3.13 Gatekeeper hardening

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.