Risoluzione dei problemi di intermittenza di IOS-XE NAT per la conversione di alcuni pacchetti

Sommario

Introduzione

Questo documento descrive i pacchetti non tradotti che ignorano NAT su un router Cisco IOS XE, causando potenzialmente un errore di traffico.

Premesse

Nella versione software 12.2(33)XND è stata introdotta e abilitata per impostazione predefinita una funzione chiamata Network Address Translation (NAT) Gatekeeper. Il Gatekeeper NAT è stato progettato per impedire che flussi non NAT utilizzino una CPU eccessiva per creare una traduzione NAT. A tale scopo, vengono create due piccole cache (una per la direzione in2out e una per la direzione out2in) in base all'indirizzo di origine. Ogni voce della cache è composta da un indirizzo di origine, un ID VRF (virtual routing and forwarding), un valore del timer (usato per invalidare la voce dopo 10 secondi) e un contatore di frame. La tabella contiene 256 voci che costituiscono la cache. Se sono presenti più flussi di traffico dallo stesso indirizzo di origine dove alcuni pacchetti richiedono il protocollo NAT e alcuni no, i pacchetti potrebbero non essere NAT-ed e inviati tramite il router non tradotti. Cisco consiglia ai clienti di evitare di avere flussi NAT-ed e non NAT-ed sulla stessa interfaccia, quando possibile.

 Nota: questo non ha nulla a che fare con H.323.

Piattaforme interessate

- ISR1K
- ISR4K
- C8200
- C8300
- C8500

Dimostrazione di NAT ignorato

In questa sezione viene descritto come ignorare NAT a causa della funzionalità Gatekeeper NAT. Esaminate il diagramma in dettaglio. Si può vedere che ci sono un router di origine, un firewall di ASA (Adaptive Security Appliance), l'ASR1K e il router di destinazione.

Flussi di traffico verso destinazioni non NAT

1. Il ping ha inizio dalla fonte: Fonte: 172.17.250.201 Destinazione: 198.51.100.11.
2. Il pacchetto arriva all'interfaccia interna dell'appliance ASA, che esegue la conversione dell'indirizzo di origine. Il pacchetto ora ha origine: 203.0.113.231 destinazione: 198.51.100.11.
3. Il pacchetto arriva all'ASR1K sul NAT dall'esterno all'interfaccia interna. La traduzione NAT non trova alcuna traduzione per l'indirizzo di destinazione e quindi la cache di uscita del gatekeeper viene popolata con l'indirizzo di origine 203.0.113.231.
4. Il pacchetto arriva alla destinazione. La destinazione accetta il pacchetto Internet Control Message Protocol (ICMP) e restituisce una risposta ECHO ICMP. Il ping ha esito positivo.

Il traffico proveniente dalla stessa origine tenta di inviare la destinazione NAT

1. .Ping viene avviato dalla fonte: Fonte: 172.17.250.201 Destinazione: 198.51.100.9.
2. Il pacchetto arriva all'interfaccia interna dell'appliance ASA, che esegue la conversione dell'indirizzo di origine. Il pacchetto ora ha origine: 203.0.113.231 destinazione: 198.51.100.9.
3. Il pacchetto arriva all'ASR1K sul NAT dall'esterno all'interfaccia interna. NAT cerca prima una traduzione per l'origine e la destinazione. Poiché non ne trova una, controlla la cache "out" del gatekeeper e trova l'indirizzo di origine 203.0.113.231. (erroneamente) presume che il pacchetto non debba essere tradotto e inoltra il pacchetto se esiste un percorso di destinazione o lo scarta. In entrambi i casi, il pacchetto non raggiunge la destinazione prevista.

Ripristino del traffico NAT

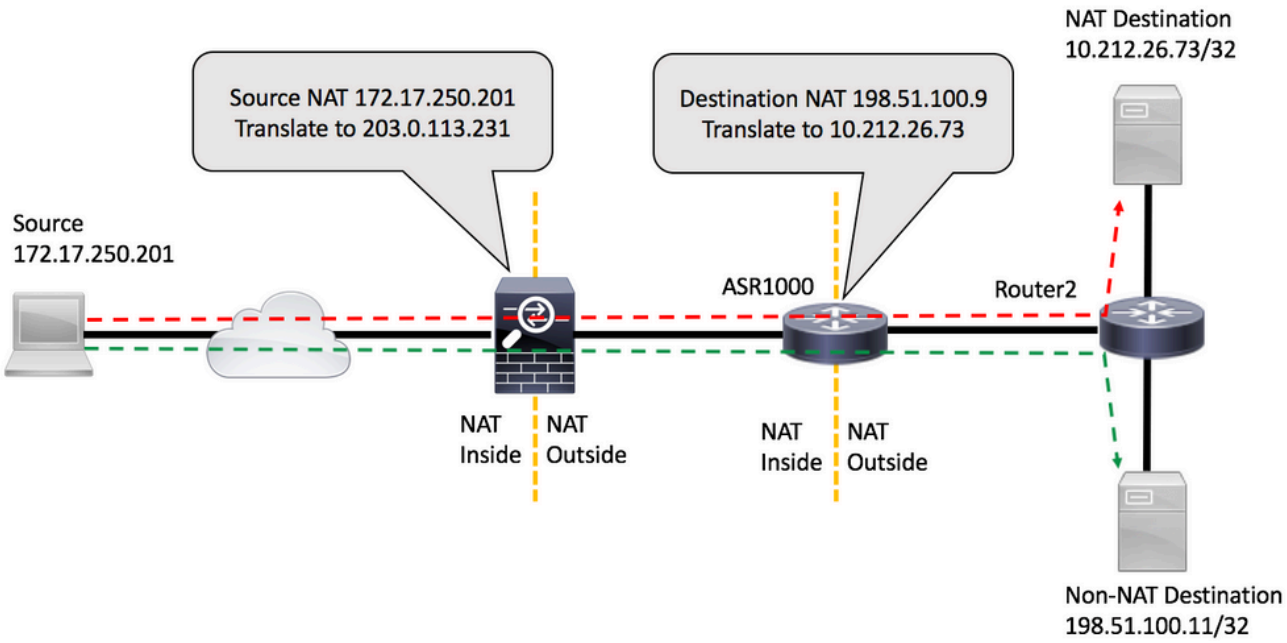
1. Dopo 10 secondi, la voce dell'indirizzo di origine 203.0.113.231 si è esaurita nella cache di uscita del gatekeeper.

Nota: la voce è ancora fisicamente presente nella cache, ma poiché è scaduta non

---

viene utilizzata.

2. Ora, se la stessa origine 172.17.250.201 invia alla destinazione NAT-ed 198.51.100.9. Quando il pacchetto arriva all'interfaccia out2in sull'ASR1K, non viene trovata alcuna traduzione. Quando si controlla la cache di uscita del gatekeeper, non è possibile trovare una voce attiva, quindi si crea la traduzione per la destinazione e il flusso dei pacchetti come previsto.
3. Il traffico in questo flusso continua finché le traduzioni non scadono a causa di inattività. Se, nel frattempo, l'origine invia nuovamente il traffico a una destinazione non NAT, causando l'inserimento di un'altra voce nel gatekeeper al di fuori della cache, il traffico non influisce sulle sessioni stabilite, ma esiste un periodo di 10 secondi durante il quale le nuove sessioni dalla stessa origine alle destinazioni NAT falliscono.



Esempio del problema

1. Il ping ha inizio dal router di origine : Origine: 172.17.250.201 Destinazione: 198.51.100.9. Il comando ping viene emesso con un conteggio di ripetizioni pari a due su [FLOW1].
2. Eseguire quindi il ping su una destinazione diversa non NAT-ed da ASR1K: Origine: 172.17.250.201 Destinazione:198.51.100.11 [FLOW2].
3. Quindi invia altri pacchetti a 198.51.100.9 [FLOW1]. I primi pacchetti di questo flusso ignorano NAT come mostrato dalla corrispondenza dell'elenco degli accessi sul router di destinazione.

<#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#
```

La corrispondenza ACL sul router di destinazione mostra i tre pacchetti che non sono stati convertiti:

<#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#
```

Sull'ASR1K è possibile controllare le voci della cache del gatekeeper:

<#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
```

Soluzione/correzione

Nella maggior parte degli ambienti, la funzionalità NAT gatekeeper funziona correttamente e non causa problemi. Tuttavia, se si incontra questo problema, ci sono alcuni modi per risolverlo.

Soluzione 1

L'opzione preferibile sarebbe quella di aggiornare Cisco IOS® XE a una versione che includa il miglioramento gatekeeper:

ID bug Cisco CSCun06260 XE3.13 Protezione avanzata Gatekeeper

Questo miglioramento permette al gatekeeper NAT di memorizzare nella cache gli indirizzi di origine e di destinazione, oltre a rendere configurabile la dimensione della cache. Per attivare la modalità estesa, è necessario aumentare le dimensioni della cache con questi comandi. È inoltre possibile monitorare la cache per verificare se è necessario aumentare le dimensioni.

<#root>

```
PRIMARY(config)#
```

```
ip nat settings gatekeeper-size 1024

PRIMARY(config)#
end
```

La modalità estesa può essere verificata selezionando i seguenti comandi:

<#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
```

Soluzione 2

Per le versioni che non dispongono della funzione di correzione per il bug Cisco con ID CSCun06260, l'unica opzione è disattivare la funzione gatekeeper. L'unico impatto negativo è una leggera riduzione delle prestazioni per il traffico non NAT e un maggiore utilizzo della CPU sul 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#
```

L'utilizzo di QFP può essere monitorato con i seguenti comandi:

```
<#root>

show platform hardware qfp active data utilization summary

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

Soluzione 3

Flussi di traffico separati in modo che i pacchetti NAT e non NAT non arrivino sulla stessa interfaccia.

Riepilogo

Il comando NAT Gatekeeper è stato introdotto per migliorare le prestazioni del router per i flussi non NAT. In alcune condizioni, questa funzione può causare problemi quando una combinazione di pacchetti NAT e non NAT arriva dalla stessa origine. La soluzione è usare la funzionalità gatekeeper avanzata, o se ciò non è possibile, disabilitare la funzione gatekeeper.

Riferimenti

Modifiche software che hanno consentito di disattivare il gatekeeper:
ID bug Cisco CSCty67184 ASR1k NAT CLI - Gatekeeper On/Off
ID bug Cisco CSCth23984 Aggiunta della funzionalità cli per attivare/disattivare la funzionalità gatekeeper nat

Miglioramento NAT Gatekeeper
ID bug Cisco CSCun06260 XE3.13 Protezione avanzata Gatekeeper

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).