Fehlerbehebung: IOS-XE NAT - zeitweilige Fehler bei der Übersetzung einiger Pakete

Inhalt

Einleitung

In diesem Dokument werden nicht übersetzte Pakete beschrieben, die NAT auf einem Cisco IOS XE-Router umgehen und möglicherweise Datenverkehrsfehler verursachen.

Hintergrundinformationen

In Softwareversion 12.2(33)XND wurde eine Funktion namens Network Address Translation (NAT) Gatekeeper eingeführt und standardmäßig aktiviert. NAT Gatekeeper wurde entwickelt, um zu verhindern, dass Datenflüsse ohne NAT übermäßige CPU-Auslastung verwenden, um eine NAT-Übersetzung zu erstellen. Um dies zu erreichen, werden zwei kleine Caches (einer für die in2out-Richtung und einer für die out2in-Richtung) basierend auf der Quelladresse erstellt. Jeder Cache-Eintrag besteht aus einer Quelladresse, einer VRF-ID (Virtual Routing and Forwarding), einem Timer-Wert (mit dem der Eintrag nach 10 Sekunden ungültig gemacht wird) und einem Frame-Zähler. Die Tabelle enthält 256 Einträge, aus denen sich der Cache zusammensetzt. Wenn mehrere Datenverkehrsflüsse von derselben Quelladresse auftreten, für die einige Pakete NAT erfordern, andere jedoch nicht, kann dies dazu führen, dass Pakete nicht per NAT gesendet und nicht übersetzt über den Router gesendet werden. Cisco empfiehlt Kunden, NAT-gesteuerte und nicht NAT-gesteuerte Datenflüsse nach Möglichkeit nicht auf derselben Schnittstelle zu verwenden.

Hinweis: Das hat nichts mit H.323 zu tun.

Betroffene Plattformen

- ISR 1K
- ISR 4K
- C820
- C830
- C850

Demonstration der NAT-Umgehung

In diesem Abschnitt wird beschrieben, wie NAT aufgrund der NAT-Gatekeeper-Funktion umgangen werden kann. Überprüfen Sie das Diagramm im Detail. Hier sehen Sie einen Quellrouter, eine ASA-Firewall (Adaptive Security Appliance), den ASR1K und den Zielrouter.

Datenverkehrsflüsse zu nicht-NAT-Ziel

1. Der Ping wird von der Quelle initiiert: Quelle: 172.17.250.201 Ziel: 198.51.100.11.
2. Das Paket erreicht die interne Schnittstelle der ASA, die die Übersetzung der Quelladresse durchführt. Das Paket hat jetzt die Quelle: 203.0.113.231 Ziel: 198.51.100.11.
3. Das Paket erreicht den ASR1K auf der NAT-Schnittstelle für den Datenverkehr zwischen Außen- und Innen. Bei der NAT-Übersetzung wird keine Übersetzung für die Zieladresse gefunden, und so wird im Cache "out" des Gatekeepers die Quelladresse 203.0.113.231 eingetragen.
4. Das Paket kommt am Ziel an. Das Ziel akzeptiert das Internet Control Message Protocol (ICMP)-Paket und gibt eine ICMP-ECHO-Antwort zurück, die zu einem erfolgreichen Ping führt.

Datenverkehr von derselben Quelle versucht, NAT-Ziel zu senden

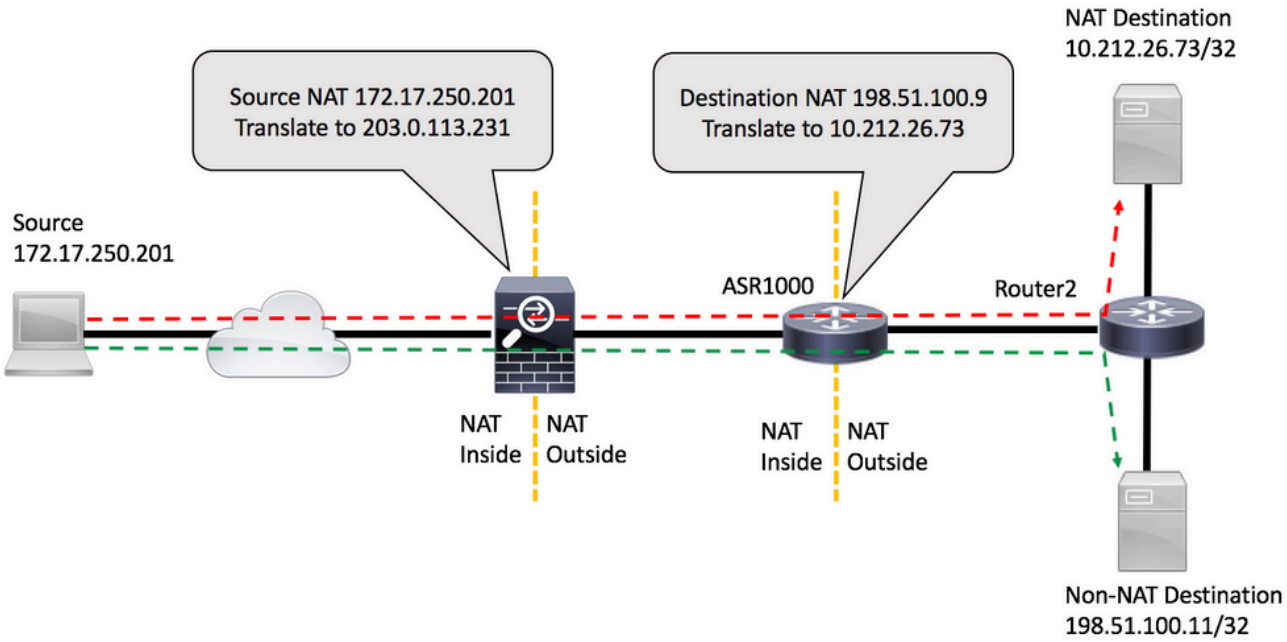
1. .Ping wird von der Quelle initiiert: Quelle: 172.17.250.201 Ziel: 198.51.100.9.
2. Das Paket erreicht die interne Schnittstelle der ASA, die die Übersetzung der Quelladresse durchführt. Das Paket hat jetzt die Quelle: 203.0.113.231 Ziel: 198.51.100.9.
3. Das Paket erreicht den ASR1K auf der NAT-Schnittstelle für den Datenverkehr zwischen Außen- und Innen. NAT sucht zunächst nach einer Übersetzung für Ausgangs- und Zielort. Da er keinen findet, überprüft er den Gatekeeper "out" Cache und findet die Quelladresse 203.0.113.231. Er geht (fälschlicherweise) davon aus, dass das Paket keine Übersetzung benötigt, und leitet das Paket entweder weiter, wenn eine Route für das Ziel vorhanden ist, oder verwirft das Paket. In beiden Fällen erreicht das Paket nicht das beabsichtigte Ziel.

Wiederherstellung des NAT-gesteuerten Datenverkehrs

1. Nach 10 Sekunden wird der Eintrag für die Quelladresse 203.0.113.231 im Gatekeeper-Out-Cache deaktiviert.

Hinweis: Der Eintrag existiert zwar noch physisch im Cache, wird aber aufgrund seines Ablaufs nicht verwendet.

2. Wenn nun dieselbe Quelle wie 172.17.250.201 an das NAT-Ziel 198.51.100.9 sendet. Wenn das Paket an der out2in-Schnittstelle auf dem ASR1K ankommt, wird keine Übersetzung gefunden. Wenn Sie den Gatekeeper-Out-Cache überprüfen, können Sie keinen aktiven Eintrag finden, sodass Sie die Übersetzung für das Ziel erstellen und die Pakete wie erwartet übertragen.
3. Der Datenverkehr in diesem Fluss wird so lange fortgesetzt, wie bei Übersetzungen aufgrund von Inaktivität keine Zeitüberschreitung auftritt. Wenn die Quelle in der Zwischenzeit erneut Datenverkehr an ein nicht-NAT-gebundenes Ziel sendet, wodurch ein anderer Eintrag im Gatekeeper aus dem Cache gefüllt wird, wirkt sich dies nicht auf die etablierten Sitzungen aus. Es gibt jedoch einen Zeitraum von 10 Sekunden, in dem neue Sitzungen von derselben Quelle zu NAT-gebundenen Zielen fehlschlagen.



Beispiel des Problems

1. Der Ping wird vom Quellrouter initiiert: Quelle: 172.17.250.201 Ziel: 198.51.100.9. Der Ping-Befehl wird mit einer Wiederholungszahl von zwei ausgegeben, und zwar über und über [FLOW1].
2. Senden Sie dann einen Ping an ein anderes Ziel, das nicht von der ASR1K NAT-geleitet wird: Quelle: 172.17.250.201 Ziel: 198.51.100.11 [FLOW2].
3. Senden Sie dann weitere Pakete an 198.51.100.9 [FLOW1]. Die ersten Pakete dieses Datenflusses umgehen die NAT, wie die Zugriffsliste zeigt, die auf dem Zielrouter übereinstimmt.

<#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#
```

Die ACL-Übereinstimmung auf dem Zielrouter zeigt, dass die drei fehlgeschlagenen Pakete nicht umgewandelt wurden:

<#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#
```

Auf dem ASR1K können Sie die Gatekeeper-Cache-Einträge überprüfen:

<#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
```

Problemumgehung/Fehlerbehebung

In den meisten Umgebungen funktioniert die NAT-Gatekeeper-Funktion einwandfrei und verursacht keine Probleme. Wenn Sie jedoch auf dieses Problem stoßen, gibt es einige Möglichkeiten, es zu beheben.

Lösung 1

Die bevorzugte Option wäre ein Upgrade von Cisco IOS® XE auf eine Version, die die Gatekeeper-Erweiterung enthält:

Cisco Bug-ID CSCun06260 XE3.13 Gatekeeper Hardening

Diese Erweiterung ermöglicht es dem NAT-Gatekeeper, die Quell- und Zieladressen zwischenzuspeichern und die Cachegröße zu konfigurieren. Um den erweiterten Modus zu aktivieren, müssen Sie die Cachegröße mit diesen Befehlen erhöhen. Sie können auch den Cache überwachen, um festzustellen, ob Sie die Größe erhöhen müssen.

<#root>

PRIMARY(config)#

ip nat settings gatekeeper-size 1024

PRIMARY(config)#

end

Der erweiterte Modus kann mithilfe der folgenden Befehle überprüft werden:

<#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

Lösung 2

Bei Versionen, die nicht die Korrektur für Cisco Bug-ID CSCun06260 enthalten, besteht die einzige Option darin, die Gatekeeper-Funktion auszuschalten. Die einzigen negativen Auswirkungen sind eine geringfügig reduzierte Leistung für Datenverkehr ohne NAT sowie eine höhere CPU-Auslastung beim 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#
```

Die QFP-Nutzung kann mit folgenden Befehlen überwacht werden:

```
<#root>

show platform hardware qfp active data utilization summary

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

Lösung 3

Separater Datenverkehr fließt, sodass NAT- und Nicht-NAT-Pakete nicht an derselben Schnittstelle ankommen.

Zusammenfassung

Der NAT-Gatekeeper-Befehl wurde eingeführt, um die Leistung des Routers für Datenflüsse ohne NAT zu verbessern. Unter bestimmten Bedingungen kann diese Funktion Probleme verursachen, wenn eine Kombination aus NAT- und Nicht-NAT-Paketen von derselben Quelle eingeht. Die

Lösung besteht darin, die erweiterte Gatekeeper-Funktion zu verwenden oder, falls dies nicht möglich ist, die Gatekeeper-Funktion zu deaktivieren.

Referenzen

Softwareänderungen, die das Deaktivieren des Gatekeepers ermöglichten:
Cisco Bug-ID CSCty67184 ASR1k NAT CLI - Ein/Aus für Gatekeeper
Cisco Bug-ID CSCth23984 Hinzufügen einer CLI-Funktion zum Aktivieren/Deaktivieren der Funktion "nat gatekeeper"

NAT Gatekeeper-Erweiterung
Cisco Bug-ID CSCun06260 XE3.13 Gatekeeper Hardening

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.