ASR1k NAT は断続的にいくつかのパケットを変換しません

目次

概要

この技術情報は ASR1k の NAT によって変換する必要があるパケットが変換されていない状況を示します (バイパスされる NAT) 。 これはトラフィック失敗という結果に未翻訳パケットが処理されるように設定されないネクスト ホップが本当らしいので終る可能性があります。

背景説明

ソフトウェア バージョン 12.2(33)XND で NAT ゲートキーパーと呼ばれた機能はデフォルトで導入され、有効に なりました。 (これに関係ありません H.323 とは全く注意して下さい) 。 NAT ゲートキーパーは NAT 変換を作成するのに非 NAT ED フローが余分な CPU を使用することを防ぐように設計されていました。 これを実現させるために、2 つの小さいキャッシュ (1 および out2in 方向のための in2out 方向のための 1) は送信元アドレスに基づいて作成されます。 各キャッシュ エントリは送信元アドレス、VRF ID、タイマー値 (10 秒後にエントリを無効にするのに使用される) 、およびフレーム カウンターで構成されています。 キャッシュを構成する表に 256 のエントリがあります。 いくつかのパケットが NAT およびいくつかを必要とする同じ送信元アドレスから多重トラフィック トラフィック フローがある場合、未翻訳ルータを通してネットワークアドレス交換されないし、送信されたパケットという結果に終る可能性があります。 Cisco は顧客がネットワークアドレス交換することを避ける必要があり、同じの非 NAT ED がフロー可能な限りインターフェイスすることを推奨します。

バイパスされる NAT のデモ

以降のセクションは NAT が NAT ゲートキーパー 機能がバイパスされた原因どのようにである場合もあるか記述します。 ダイアグラムを詳しく検討して下さい。 ソースルータ、ASA ファイア

ウォール、ASR1k およびデスティネーションルータがあることを見る場合があります。

非 NAT ED 宛先へのトラフィックフロー:

1) PING はソースから始められます: 出典： 172.17.250.201 宛先: 198.51.100.11
2) パケットは送信元アドレス 変換を行う ASA の内部インターフェイスに着きます。 パケットに今ソースがあります: 203.0.113.231 宛先: 198.51.100.11
3) パケットは内部インターフェイスに NAT の ASR1k で外部で着きます。 NAT 変換は宛先アドレスのための変換を見つけないし、従ってゲートキーパーは「送信元アドレス 203.0.113.231 と」キャッシュするために読み込まれます
4) パケットは宛先で着きます。 宛先は ICMPパケットを受け入れ、PING 成功に終って ICMP工コー応答を戻します。

同じソースからのトラフィックはネットワークアドレス交換された宛先を送信 するように試みます:

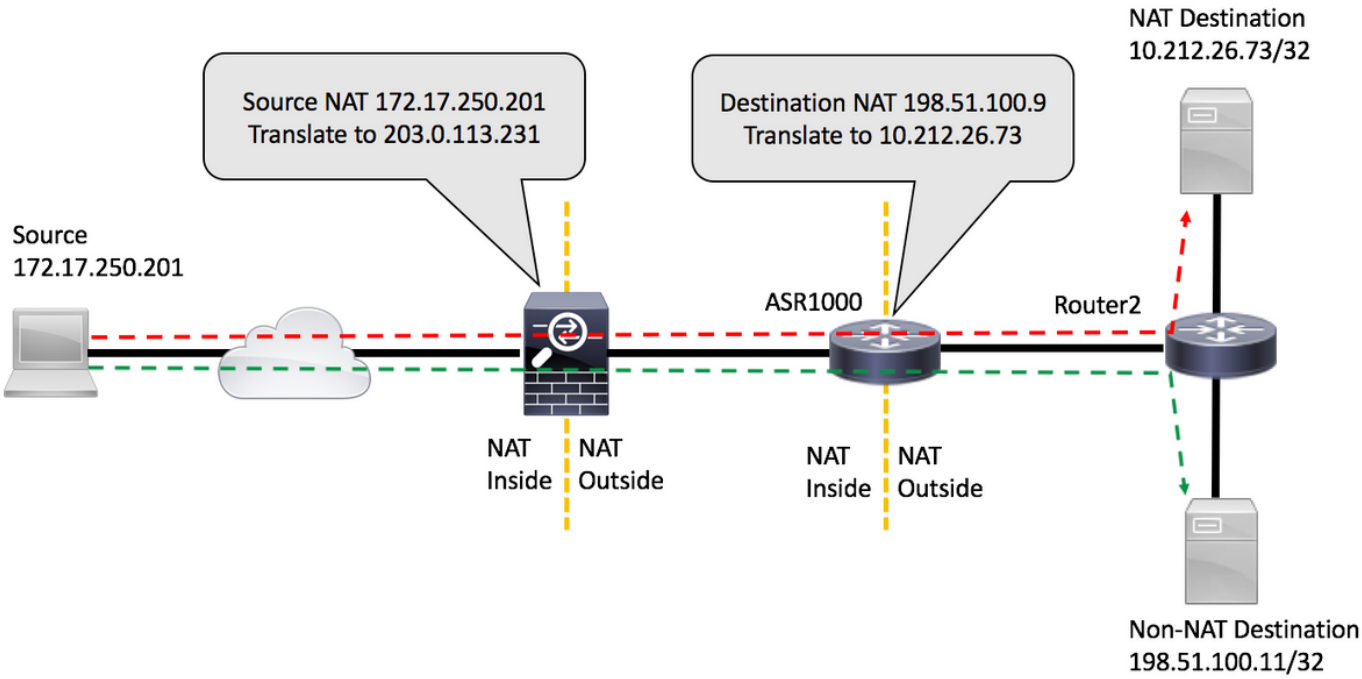
1) PING はソースから始められます: 出典： 172.17.250.201 宛先: 198.51.100.9
2) パケットは送信元アドレス 変換を行う ASA の内部インターフェイスに着きます。 パケットに今ソースがあります: 203.0.113.231 宛先: 198.51.100.9
3) パケットは内部インターフェイスに NAT の ASR1k で外部で着きます。 NAT は最初に送信元および宛先のための変換を探します。 1 つを見つけなくて、それはゲートキーパーを「」キャッシュし、調べます送信元アドレス 203.0.113.231 をチェックします。 パケットが変換を必要としないし、廃棄しますと (間違って) パケットを宛先のために存在 する ルート転送するか、またはパケットを仮定します。 いずれにしても、パケットは意図されたデスティネーションに到着しません。

NAT-ed トラフィックのリストア

1) 10 秒後に、送信元アドレス 203.0.113.231 のためのエントリはゲートキーパーでキャッシュします時間を計ります。 (ことに注目して下さい物理的に キャッシュ切れたので、それで存在 する エントリはまだ使用されませんが、) 。

2) 同じがソースをたどればこの場合: パケットが ASR1K の out2in インターフェイスで着く場合ネットワークアドレス交換された宛先 198.51.100.9 への 172.17.250.201 送信は、変換見つけられません。 ゲートキーパーをキャッシュするチェックする場合、アクティブなエントリを検出しないし、従って宛先およびパケット willl フロー のための変換を予想通り作成します。

3) このフローのトラフィックは変換が非アクティブが時間を計られなかった原因ではない限り続きます。 一方、ソースが非 NAT ED 宛先に再度トラフィックを送信 したら、ゲートキーパーで読み込みます別のエントリを、それ影響を与えません確立されたセッションにキャッシュして下さいしかしそこにその同じソースからのネットワークアドレス交換された宛先への新しいセッションが失敗する 10 第 2 期間です。



問題の例

1) PING はソースルータから始められます: 出典： 172.17.250.201 宛先: 198.51.100.9。 PING は 2 の反復数においての、何回も [FLOW1] 実行されます。

2) それから ASR1k ソースによってネットワークアドレス交換されていない別の宛先を ping して下さい: 172.17.250.201 Destination:198.51.100.11 [FLOW2]。

3) それから 198.51.100.9 [FLOW1] により多くのパケットを送信して下さい。 このフローのはじめの幾つかのパケットはデスティネーションルータで一致する access-list によって見られるように NAT をバイパスします。

```
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#
```

デスティネーションルータの ACL 一致は失敗する、変換されなかった 3 つのパケットを示します:

```
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#
```

ASR1k でゲートキーパー キャッシュ エントリをチェックできます:

```
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
```

回避策/修正:

ほとんどの環境うまく NAT ゲートキーパー機能性働問題を引き起こすことなしで。 ただしこの問題に動作すればそれを解決する少数の方法があります。

ソリューション #1:

優先 する オプションはゲートキーパー 機能拡張を含むバージョンへ IOS XE をアップグレードすることです:

CSCun06260 XE3.13 ゲートキーパー堅くなること

この機能拡張はソース**および**宛先アドレスをキャッシュすることを、またキャッシュサイズを設定可能にすることができる NAT ゲートキーパーがように可能にします。 拡張 モードをつけるために、次のコマンドでキャッシュサイズを増加する必要があります。 また監視しますサイズを増加する必要があるかどうか見るためにキャッシュをできます。

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

```
PRIMARY(config)#end
```

拡張 モードは次のコマンドのチェックによって確認することができます:

```
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
```

ソリューション #2:

リリースに関しては CSCun06260 のための修正がない、唯一のオプションはゲートキーパー 機能をオフにすることです。 唯一の悪影響はわずかに非 NAT ED トラフィックのための低下したパフォーマンス、また QFP のより高い CPU稼働率です。

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

PRIMARY#
```

QFP 利用は下記のものでモニタすることができます:

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

ソリューション #3:

NAT および NAT 以外のパケットが同じインターフェイスに着かないようにトラフィックフローを分けて下さい。

要約

NAT Gatekeeper コマンドは非 NAT ED フローのためのルータのパフォーマンスを高めるもたらされました。 状況によっては機能は NAT のミックスおよび NAT 以外のパケットが同じソースから着くとき問題を引き起こすかもしれません。 ソリューションはそれが可能性のあるでなければ拡張 な ゲートキーパー機能性を使用することまたは、ゲートキーパー 機能をディセーブルにします。

参考資料

ゲートキーパーがうんざりすることを可能にしたソフトウェアの変更:

CSCty67184 ASR1k NAT CLI -オン/オフ ゲートキーパー
CSCth23984 はオン/オフ NAT ゲートキーパー機能性を回すために cli 機能を追加します

NAT ゲートキーパー 機能拡張

CSCun06260 XE3.13 ゲートキーパー堅くなること