IM المستخدم للتحكم في سلوك تحويل NAT لمثال ISP في تكرار إستخدام nat عند لمرتين التكوين

المحتويات

المقدمة

يوضح هذا المستند كيفية إستخدام تطبيق مدير الحدث المضمن (IM) للتحكم في سلوك تحويل ترجمة عنوان الشبكة (NAT) في سيناريو ISP مزدوج (تكرار ISP).

من المهم فهم أنه عندما تتم معالجة اتصال من خلال جدار حماية جهاز الأمان القابل للتكيف (ASA)، يمكن لقواعد NAT أن تكون لها الأولوية على جدول التوجيه عند إجراء التحديد على أي واجهة يتم تصنيف الحزمة عليها. إذا تطابقت حزمة واردة مع عنوان IP مترجم في عبارة NAT، فسيتم إستخدام قاعدة NAT لتحديد واجهة الخروج المناسبة. وهذا يعرف باسم "NAT Divert".

ال nat تحويل تدقيق (أي يكون ما يمكن أن يتجاوز التحشد طاولة) يتحقق أن هناك يكون قاعدة nat أن يعين غاية عنوان ترجمة لحزمة واردة أن يصل على قارن. إن هناك ما من قاعدة أن يعين صراحة كيف أن يترجم أن ربط غاية عنوان، بعد ذلك الشامل تحشد طاولة in order to حددت المخرج قارن. إذا كانت هناك قاعدة تحدد بشكل صريح كيفية ترجمة عنوان IP لوجهة الحزمة، فعندئذ تقوم قاعدة NAT "بسحب" أو "تحويل" الحزمة إلى الواجهة الأخرى في الترجمة ويتم تجاوز جدول التوجيه العام بشكل فعال.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على ASA أن يركض برمجية إطلاق 9.2.1.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

تم تكوين ثلاث واجهات، من الداخل والخارج (ISP أساسي) و BackupISP (ISP الثانوي). شكلت هذا إثنان nat عبارة أن يترجم حركة مرور خارج إما قارن عندما يذهب إلى subnet خاص (24/203.0.113.0).

```
nat (any,Outside) source dynamic any 192.0.2.100_nat destination
                                    static obj_203.0.113.0 obj_203.0.113.0
nat (any,BackupISP) source dynamic any 198.51.100.100_nat destination
                                    static obj_203.0.113.0 obj_203.0.113.0
```

تكوين تعقب المسار

```
                                                    sla monitor 40
type echo protocol ipIcmpEcho 192.0.2.254 interface Outside
                                                   num-packets 2
                                                    timeout 2000
                                                   threshold 500
                                                    frequency 10
sla monitor schedule 40 life forever start-time now

route Outside 203.0.113.0 255.255.255.0 192.0.2.254 1 track 40
route BackupISP 203.0.113.0 255.255.255.0 198.51.100.254 100
```

ماذا يحدث عندما ينهار الرابط الرئيسي؟

قبل انتقال الارتباط الأساسي (الخارجي) إلى أسفل، تتدفق حركة مرور البيانات كما هو متوقع من الواجهة الخارجية. يتم إستخدام قاعدة NAT الأولى في الجدول وترجمة حركة المرور إلى عنوان IP المناسب للواجهة الخارجية (nat_192.0.2.100). الآن الواجهات الخارجية تنزل إلى أسفل، أو مسار يفشل. حركة المرور لا تزال تتبع بيان NAT الأول ويتم تحويل NAT إلى الواجهة الخارجية، **وليس** واجهة BackupISP. هذا هو السلوك المعروف باسم NAT Divert. حركة المرور الموجهة إلى 24/203.0.113.0 هي فعليا ذات حجرة سوداء.

يمكن ملاحظة هذا السلوك باستخدام أمر **حزمة tracer**. لاحظ سطر **تحويل NAT** في مرحلة **UN-NAT**.

```
ASA(config-if)#packet-tracer input inside tcp 10.180.10.10 1024 203.0.113.50 80 detailed

                                                                Phase: 1
                                                          Type: ACCESS-LIST
                                                                  :Subtype
                                                             Result: ALLOW
                                                                   :Config
                                                            Implicit Rule
                                                        :Additional Information
                                                :Forward Flow based lookup yields rule
                                    in id=0x7fff2af839a0, priority=1, domain=permit, deny=false
                                         hits=1337149272, user_data=0x0, cs_id=0x0, l3_type=0x8
                                                    src mac=0000.0000.0000, mask=0000.0000.0000
                                                    dst mac=0000.0000.0000, mask=0100.0000.0000
                                                            input_ifc=inside, output_ifc=any

                                                                Phase: 2
                                                             Type: UN-NAT
                                                          Subtype: static
                                                            Result: ALLOW
                                                                   :Config
                                    nat (any,Outside) source dynamic any 192.0.2.100_nat destination
                                                    static obj_203.0.113.0 obj_203.0.113.0
                                                        :Additional Information
                                                NAT divert to egress interface Outside
                                            Untranslate 203.0.113.50/80 to 203.0.113.50/80

                                                              <Output truncated>

                                                                  :Result
                                                      input-interface: inside
                                                             input-status: up
                                                        input-line-status: up
                                                    output-interface: Outside
                                              output-status: administratively down
                                                        output-line-status: down
                                                            Action: allow
```

تم تصميم قواعد NAT هذه لتجاوز جدول التوجيه. هناك بعض إصدارات ASA حيث قد لا يحدث التحويل وقد يعمل هذا الحل بالفعل، ولكن مع الإصلاح لمعرف تصحيح الأخطاء من CSCul98420 Cisco هذه القواعد (والسلوك المتوقع الجاري قدما) يؤدي بالتأكيد إلى تحويل الحزمة إلى واجهة مخرج تم تكوينها أول. يتم إسقاط الحزمة هنا إذا تم إسقاط الواجهة أو تم إزالة المسار المتتبع.

الحل

بما أن وجود قاعدة NAT في التكوين يفرض على حركة المرور التحويل إلى الواجهة الخطأ، يلزم إزالة خطوط التكوين مؤقتا للعمل حول المشكلة. أنت يستطيع دخلت ال "ما من" شكل من خاص nat خط، غير أن هذا تدخل يدوي قد يأخذ وقت ويمكن واجهت انقطاع. من أجل تسريع العملية، يجب أتمتة المهمة بطريقة ما. ويمكن تحقيق ذلك باستخدام ميزة IM التي أدخلت في إصدار ASA 9.2.1. يتم عرض التكوين هنا:

```
                                                    event manager applet NAT
                                                      event syslog id 622001
action 1 cli command "no nat (any,Outside) source dynamic any 192.0.2.100_nat destination
                                                "static obj_203.0.113.0 obj_203.0.113.0
                                                                output none
                                                    event manager applet NAT2
                                                event syslog id 622001 occurs 2
```

```
action 1 cli command "nat (any,Outside) 1 source dynamic any 192.0.2.100_nat destination
"static obj_203.0.113.0 obj_203.0.113.0
output none
```

تعمل هذه المهمة عندما يتم الاستفادة من IM لاتخاذ إجراء في حالة رؤية 622001 syslog. يتم إنشاء syslog هذا عند إزالة مسار مكدس أو إضافته مرة أخرى إلى جدول التوجيه. بافتراض تكوين تعقب المسار الموضح مسبقا، إذا تم إيقاف الواجهة الخارجية أو لم يعد هدف المسار قابلا للوصول، يتم إنشاء syslog هذا واستدعاء التطبيق IM. الجانب المهم لتكوين تعقب المسار هو **معرف الحدث 622001 syslog id يحدث** سطر تكوين **إثنين**. هذا يتسبب في حدوث التطبيق NAT2 *كل* مرة *أخرى* يتم فيها إنشاء syslog. ال nat استعملت بريمج يكون كل مرة ال syslog يكون رأيت. ينتج عن هذه المجموعة سطر NAT الذي تتم إزالته عندما يتم رؤية معرف 622001 ID syslog أولا (المسار المتتبع الذي تمت إزالته) ثم تتم إعادة إضافة سطر NAT في المرة الثانية التي يتم فيها رؤية 62201 syslog (تمت إعادة إضافة المسار المتتبع إلى جدول التوجيه). ويكون لهذا تأثير الإزالة التلقائية وإعادة إضافة سطر NAT بالاقتران مع ميزة تعقب المسار.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر show.

قم بمحاكاة فشل إرتباط يتسبب في إزالة المسار الذي تم تتبعه من جدول التوجيه لإكمال التحقق.

تنزيل إرتباط ISP الأساسي

قم أولا بإنزال الارتباط الأساسي (الخارجي).

```
ciscoasa(config-if)# int gi0/0
ciscoasa(config-if)# shut
```

يتم قطع الواجهة

لاحظ أن الواجهة الخارجية تنزل إلى أسفل وأن كائن التعقب يشير إلى أن إمكانية الوصول متوقفة.

```
ASA-4-411004: Interface Outside, changed state to administratively down%
ASA-4-411004: Interface GigabitEthernet0/0, changed state to administratively down%

ciscoasa(config-if)# show track
Track 40
Response Time Reporter 40 reachability
Reachability is Down
changes, last change 00:00:44 5
Latest operation return code: Timeout
:Tracked by
STATIC-IP-ROUTING 0
```

تم تشغيل IM

يتم إنشاء Syslog 622001 كنتيجة لإزالة المسار ويتم إستدعاء برنامج nat "IM". يعكس إخراج الأمر **show event manager** حالة التطبيقات الفردية وأوقات تنفيذها.

```
,ASA-6-622001: Removing tracked route 203.0.113.0 255.255.255.0 192.0.2.254%
                                    distance 1, table default, on interface Outside
 ASA-5-111008: User 'eem' executed the 'no nat (any,Outside) source dynamic%
.any 192.0.2.100_nat destination static obj_203.0.113.0 obj_203.0.113.0' command
 ASA-5-111010: User 'eem', running 'CLI' from IP 0.0.0.0, executed 'no nat%
any,Outside) source dynamic any 192.0.2.100_nat destination static obj_203.0.113.0)
                                                                'obj_203.0.113.0
        ASA-6-305010: Teardown static translation from Outside:203.0.113.0 to%
                                                    any:203.0.113.0 duration 0:01:20

                                          ciscoasa(config-if)# show event manager
                                    Last Error: Command failed @ 2014/05/13 05:17:07
                                            Consolidated syslog range: 622001-622001
                          event manager applet NAT, hits 3, last 2014/05/13 05:18:27
                                                                last file none
                    event syslog id 622001, hits 3, last 622001 @ 2014/05/13 05:18:27
       action 1 cli command "no nat (any,Outside) source dynamic any 192.0.2.100_nat
destination static obj_203.0.113.0 obj_203.0.113.0", hits 3, last 2014/05/13 05:18:27
                           event manager applet NAT2, hits 1, last 2014/05/13 05:17:07
                                                                last file none
                    event syslog id 622001, hits 3, last 622001 @ 2014/05/13 03:11:47
          action 1 cli command "nat (any,Outside) source dynamic any 192.0.2.100_nat
destination static obj_203.0.113.0 obj_203.0.113.0", hits 1, last 2014/05/13 05:17:07
```

مع حذف قاعدة IM First NAT

يظهر فحص التكوين الجاري تشغيله أنه قد تمت إزالة قاعدة NAT الأولى.

```
                                          ciscoasa(config-if)# show run nat
      nat (any,BackupISP) source dynamic any 198.51.100.100_nat destination static
                                                    obj_203.0.113.0 obj_203.0.113.0
```

التحقق باستخدام متتبع الحزم

```
ciscoasa(config-if)# packet-tracer input inside icmp 10.180.10.10 8 0 203.0.113.100


                                                            Phase: 1
                                                       Type: ACCESS-LIST
                                                               :Subtype
                                                        Result: ALLOW
                                                               :Config
                                                         Implicit Rule
                                                   :Additional Information
                                          :Forward Flow based lookup yields rule
                              in id=0x7fff2b1862a0, priority=1, domain=permit, deny=false
                                        hits=1, user_data=0x0, cs_id=0x0, l3_type=0x8
                                          src mac=0000.0000.0000, mask=0000.0000.0000
                                          dst mac=0000.0000.0000, mask=0100.0000.0000
                                                    input_ifc=inside, output_ifc=any

                                                            Phase: 2
                                                         Type: UN-NAT
                                                      Subtype: static
                                                        Result: ALLOW
                                                               :Config
            nat (any,BackupISP) source dynamic any 198.51.100.100_nat destination
```

```
                                    static obj_203.0.113.0 obj_203.0.113.0
                                                    :Additional Information
                                          NAT divert to egress interface BackupISP
                                       Untranslate 203.0.113.50/80 to 203.0.113.50/80

                                                                  Phase: 3
                                                                Type: NAT
                                                                :Subtype
                                                             Result: ALLOW
                                                                   :Config
nat (any,BackupISP) source dynamic any 198.51.100.100_nat destination
                                    static obj_203.0.113.0 obj_203.0.113.0
                                                    :Additional Information
                                 Dynamic translate 10.180.10.10/0 to 198.51.100.100/47312
                                                :Forward Flow based lookup yields rule
                                 in id=0x7fff2b226090, priority=6, domain=nat, deny=false
   hits=0, user_data=0x7fff2b21f590, cs_id=0x0, flags=0x0, protocol=0
                                          src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
   dst ip/id=203.0.113.0, mask=255.255.255.0, port=0, tag=0, dscp=0x0
                                       input_ifc=any, output_ifc=BackupISP

                                ----------------- Output Omitted-------------

                                                                   :Result
                                                 input-interface: inside
                                                        input-status: up
                                                   input-line-status: up
                                               output-interface: BackupISP
                                                         output-status: up
                                                output-line-status: up
                                                          Action: allow
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).