使用ISP冗餘時，EEM用於控制兩次NAT的NAT轉移行為配置示例

目錄

簡介

本文說明如何使用嵌入式事件管理器(EEM)小程式，以便在雙ISP場景（ISP冗餘）中控制網路地址轉換(NAT)轉移的行為。

必須瞭解的是，當通過自適應安全裝置(ASA)防火牆處理連線時，在確定資料包從哪個介面進入時，NAT規則可以優先於路由表。如果入站資料包與NAT語句中的轉換IP地址匹配，則使用NAT規則來確定相應的輸出介面。這稱為「NAT轉移」。

NAT轉移檢查（可以覆蓋路由表的內容）檢查是否存在指定到達介面的入站資料包的目標地址轉換的NAT規則。如果沒有明確指定如何轉換資料包的目的IP地址的規則，則會檢視全域性路由表以確定出口介面。如果有規則明確指定如何轉換資料包的目的IP地址，則NAT規則會將資料包「拉入」或「轉移」到轉換中的另一個介面，從而有效地繞過全域性路由表。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於運行軟體版本9.2.1的ASA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

配置了三個介面；內部、外部（主ISP）和備份ISP（輔助ISP）。 這兩條NAT語句已配置為在流量進入特定子網(203.0.113.0/24)時將流量從任一介面轉發出去。

```
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
```

配置路由跟蹤

```
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
```

主鏈路斷開時會發生什麼情況？

在主（外部）鏈路斷開之前，流量按預期從外部介面流出。使用表中的第一個NAT規則，並將流量轉換為外部介面(192.0.2.100_nat)的適當IP地址。 現在，外部介面關閉，或者路由跟蹤失敗。流量仍然遵循第一個NAT語句，並且是NAT轉移至外部介面，**而不**是BackupISP介面。這種行為稱為NAT轉移。目的地為203.0.113.0/24的流量實際上是黑洞。

可以使用**packet tracer**命令觀察此行為。注意**UN-NAT**階段的**NAT轉移**行。

```
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
```

這些NAT規則用於覆蓋路由表。有些ASA版本可能未發生轉移，並且此解決方案可能確實有效，但是使用思科錯誤ID CSCul98420的修復程式，這些規則（以及未來的預期行為）肯定會將資料包轉移到第一個配置的輸出介面。如果介面關閉或追蹤的路由被移除，此封包會遭到捨棄。

因應措施

由於在配置中存在NAT規則會強制流量轉移到錯誤的介面，因此需要臨時刪除配置行，以便解決問題。您可以輸入特定NAT線路的「否」形式，但此手動干預可能需要時間，並且可能會面臨中斷。為了加快這一過程，任務需要以某種方式實現自動化。這可以通過ASA 9.2.1版引入的EEM功能來實現。配置如下所示：

```
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
```

如果使用EEM在看到系統日誌時執行操作，此任務622001起作用。當刪除損壞的路由或將其重新新增到路由表中時，生成此系統日誌。根據前面顯示的路由跟蹤配置，如果外部介面關閉或跟蹤目標不再可訪問，將生成此系統日誌並呼叫EEM小程式。路由跟蹤配置的重要方面是**event syslog id**

622001 occurs 2 configuration line。這將導致NAT2小程式每次*生成*系統日誌時發生。每次看到系統日誌時都會呼叫NAT小程式。此組合導致在第一次看到syslog ID 622001（已刪除跟蹤路由）時刪除NAT線路，然後在第二次看到syslog 62201（將跟蹤路由重新新增到路由表）時重新新增NAT線路。 結合路由跟蹤功能，這可以自動刪除和重新新增NAT線路。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

模擬鏈路故障，該故障會導致跟蹤的路由從路由表中刪除，以便完成驗證。

關閉主ISP鏈路

首先關閉主（外部）鏈路。

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

介面停止運作

請注意，外部介面關閉，跟蹤對象指示可達性關閉。

```
%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
5 changes, last change 00:00:44
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0
```

EEM已觸發

路由622001除後會生成系統日誌消息，並呼叫EEM小程式「NAT」。show event manager命令的輸出反映了各個小程式的狀態和執行時間。

```
%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
```

刪除EEM第一個NAT規則

檢查運行配置表明第一個NAT規則已被刪除。

```
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
```

使用Packet Tracer驗證

```
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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。