用于的EEM两次控制NAT NAT转移行为，当ISP冗余是使用的配置示例

目录

简介

本文描述如何使用一嵌入式活动管理器(EEM) applet为了控制网络地址转换(NAT)转移行为在一个双重ISP方案(ISP冗余)的。

请注意，当连接通过一可适应安全工具(ASA)时防火墙处理， NAT规则能优先于路由表，当确定被做时在哪些接口数据包出口。如果入站数据包匹配在NAT语句的一转换后的IP地址， NAT规则用于为了确定适当的出口接口。这叫作“NAT转移”。

看到NAT (是的转移检查什么能改写路由表)的检查是否有指定入站数据包的目的地址地址转换在接口到达的NAT规则。如果没有明确地指定如何翻译该数据包目的IP地址，则全球路由表的规则参见为了确定出口接口。如果有明确地指定如何翻译数据包目的IP地址，则NAT规则“的规则拉”或“将”数据包转变为在转换的另一个接口，并且全球路由表有效绕过。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

运行软件版本9.2.1的本文档中的信息根据ASA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

> **注意**：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

三个接口配置;内部的外部(主ISP)和BackupISP (第二ISP)。这两个NAT语句配置转换流量任一个接口，当去一特定子网时(203.0.113.0/24)。

```
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
```

配置路由追踪

```
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
```

当主链路断开，什么发生？

在断开主要的(从外部)的链路之前，通信流正如所料外部接口。在表里使用第一个NAT规则，并且流量翻译对外部接口的(192.0.2.100_nat)适当的IP地址。现在外部接口断开，或者路由追踪发生故障。流量仍然跟随第一个NAT语句并且是NAT将转变为外部接口，**不是**BackupISP接口。这是作为NAT转移认为的行为。流量被注定到203.0.113.0/24有效黑洞。

此行为可以用**数据包跟踪程序**命令观察。注意在**UN-NAT**相位的**NAT转移**线路。

```
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
```

这些NAT规则设计改写路由表。有转移也许不发生的一些ASA版本，并且此解决方案也许实际上运作，但是以Cisco Bug ID的CSCul98420修正这些规则(和去的预料之中的行为向前)明确地将数据包转变为第一配置的出口接口。数据包丢弃此处，如果接口断开或被跟踪的路由删除。

解决方法

因为NAT规则的出现在配置里强制流量牵制到错误接口，配置行需要临时地删除为了在问题附近工作。您能输入特定NAT线路的no表，然而此人工干预也许花费时间，并且和中断可能面对。为了加速进程，任务需要有点自动化。这可以用在ASA版本介绍的EEM功能完成9.2.1。配置显示此处：

```
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
```

此任务工作，当EEM被有效利用采取行动时，如果Syslog 622001被看到。当一个被安置的路由删除或被添加回到路由表时，此Syslog生成。给显示的路由追踪配置前，应该外部接口断开或不再变得的跟踪目标可及的，此Syslog生成，并且EEM applet被调用。路由追踪配置的重要方面是**event syslog id 622001发生2**配置行。这造成NAT2 applet发生Syslog生成的*隔*时刻。在Syslog被看到时候， NAT applet被调用。此组合导致删除的NAT线路，当Syslog ID 622001是被看到时的第一(删除的被跟踪的路由) NAT线路第二次然后被重新加写Syslog 62201被看到(被跟踪的路由被重新加写了对路由表)。这有自动NAT线路的删除和再新增内容效果与路由追踪功能一道。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

模拟造成被跟踪的路由从路由表删除为了完成验证的链路故障。

减少主ISP林克

首先请减少主要的(从外部)链路。

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

接口断开

注意外部接口断开，并且跟踪对象表明可接通性发生故障。

```
%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被触发

Syslog 622001生成由于路由删除，并且EEM applet ‘NAT’被调用。**manager命令的在显示事件的**输出反射各自的applet的状态和执行时间。

```
%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
```

使用EEM NAT规则首先删除

运行的配置的检查显示第一个NAT规则删除。

```
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
```

验证与数据包跟踪程序

```
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
```

故障排除

目前没有针对此配置的故障排除信息。