使用ISP冗余时用于控制两次NAT的NAT转移行为的EEM配置示例

目录

简介

本文档介绍如何使用嵌入式事件管理器(EEM)小程序来控制双ISP场景（ISP冗余）中网络地址转换(NAT)转移的行为。

当通过自适应安全设备(ASA)防火墙处理连接时，当确定数据包从哪个接口发往时，NAT规则可以优先于路由表。如果入站数据包与NAT语句中的转换IP地址匹配，则使用NAT规则来确定适当的出口接口。这称为“NAT转移”。

NAT转移检查（即可覆盖路由表的内容）检查是否存在NAT规则，该规则指定到达接口的入站数据包的目标地址转换。如果没有明确指定如何转换该数据包的目的IP地址的规则，则会参考全局路由表以确定出口接口。如果有明确指定如何转换数据包的目的IP地址的规则，则NAT规则会“提取”或“转移”数据包到转换中的其他接口，并有效绕过全局路由表。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于运行软件版本9.2.1的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。

配置了三个接口；内部、外部（主ISP）和备用ISP（辅助ISP）。 这两条NAT语句已配置为在流量进入特定子网(203.0.113.0/24)时从任一接口转换流量。

```
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
```

当主链路断开时会发生什么情况？

在主（外部）链路断开之前，流量按预期从外部接口流出。使用表中的第一个NAT规则，并将流量转换为外部接口(192.0.2.100_nat)的适当IP地址。 现在，外部接口关闭，否则路由跟踪失败。流量仍遵循第一条NAT语句，并被NAT转移到外部接口，而**不是**BackupISP接口。这是一种称为NAT转移的行为。发往203.0.113.0/24的流量实际上已黑洞。

使用packet tracer命令可以观察**到此**行为。注意UN-NAT阶段的**NAT转移**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
```

这些NAT规则旨在覆盖路由表。有些ASA版本可能不会发生转移，此解决方案可能确实有效，但通过修复Cisco Bug ID CSCul98420这些规则（以及预期的未来行为），肯定会将数据包转移到第一个配置的出口接口。如果接口关闭或跟踪的路由被删除，则数据包将在此处丢弃。

解决方法

由于配置中存在NAT规则会迫使流量转移到错误的接口，因此需要暂时删除配置线路以解决问题。您可以输入特定NAT线路的“否”形式，但此手动干预可能需要时间，并且可能会面临中断。为了加快流程，需要以某种方式自动执行任务。这可以通过ASA版本9.2.1中引入的EEM功能实现。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
```

当发现系统日志622001时，使用EEM执行操作时，此任务会起作用。移除机架式路由或将机架式路由添加回路由表时，会生成此系统日志。根据前面所示的路由跟踪配置，如果外部接口关闭或跟踪目标不再可达，将生成此系统日志并调用EEM小程序。路由跟踪配置的一个重要方面是事件syslog

id 622001 occurs 2配置行。这会导致NAT2小程序在每次生*成系统*日志时都会发生。每次看到系统日志时都会调用NAT小程序。此组合导致在首次看到系统日志ID 622001（已删除跟踪路由）时删除NAT行，然后在第二次看到系统日志62201时重新添加NAT行（已将跟踪路由重新添加到路由表）。 这会与路由跟踪功能一起自动删除和重新添加NAT线路。

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。使用输出解释器工具来查看 show 命令输出的分析。

模拟链路故障，导致从路由表中删除跟踪的路由以完成验证。

关闭主ISP链路

首先关闭主（外部）链路。

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

接口关闭

请注意，外部接口关闭，跟踪对象指示可达性关闭。

```
%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已触发

删除路由后生成系统日志622001，并调用EEM小程序“NAT”。show event manager命令的**输出**反映了各个小程序的状态和执行时间。

```
%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第一个NAT规则被删除

检查运行配置后显示已删除第一个NAT规则。

```
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进行验证

```
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。