EEM Used to Control the NAT Divert Behavior of Twice NAT When ISP Redundancy is Used Configuration Example

Contents

Introduction

This document describes how to use an Embedded Event Manager (EEM) applet in order to control the behavior of Network Address Translation (NAT) Divert in a Dual ISP Scenario (ISP Redundancy).

It is important to understand that when a connection is processed through an Adaptive Security Appliance (ASA) firewall, NAT rules can take precedence over the routing table when the determination is made on which interface a packet egresses. If an inbound packet matches a translated IP address in a NAT statement, the NAT rule is used in order to determine the appropriate egress interface. This is known as "NAT Divert".

The NAT Divert check (which is what can override the routing table) checks to see if there is a NAT rule that specifies destination address translation for an inbound packet that arrives on an interface. If there is no rule that explicitly specifies how to translate that packet's destination IP address, then the global routing table is consulted in order to determine the egress interface. If there is a rule that explicitly specifies how to translate the packet's destination IP address, then the NAT rule "pulls" or "diverts" the packet to the other interface in the translation and the global routing table is effectively bypassed.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on an ASA that runs software Release 9.2.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Three interfaces have been configured; Inside, Outside (Primary ISP), and BackupISP (Secondary ISP). These two NAT statements have been configured to translate traffic out either interface when it goes to a specific subnet (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
```

Configure Route-Tracking

```
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
```

What Happens when the Primary Link Goes Down?

Prior to the Primary (Outside) link going down, traffic flows as expected out the Outside interface. The first NAT rule in the table is used and traffic is translated to the appropriate IP address for the the Outside interface (192.0.2.100_nat). Now the Outside interfaces goes down, or the route tracking fails. Traffic still follows the first NAT statement and is NAT Diverted to the Outside interface, **NOT** the BackupISP interface. This is a behavior known as NAT Divert. Traffic destined to the 203.0.113.0/24 is effectively black-holed.

This behavior can be observed with the **packet tracer** command. Note the **NAT Divert** line in the **UN-NAT** phase.

```
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
```

These NAT rules are designed to override the routing table. There are some ASA versions where the divert might not happen and this solution might actually work, but with the fix for Cisco bug ID CSCul98420 these rules (and the expected behavior going forward) definitely divert the packet to the first configured egress interface. The packet is dropped here if the interface goes down or the tracked route is removed.

Workaround

Since the presence of the NAT rule in the configuration forces the traffic to divert to the wrong interface, configuration lines needs to be removed temporarily in order to work around the problem. You can enter the "no" form of the specific NAT line, however this manual intervention might take time and and an outage could be faced. In order to speed up the process, the task needs to be automated in some fashion. This can be achieved with the EEM feature introduced in ASA Release 9.2.1. The configuration is shown here:

```
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
```

This task works when EEM is leveraged to take an action if syslog 622001 is seen. This syslog is generated when a racked route is removed or added back into the routing table. Given the route tracking configuration shown earlier, should the Outside interface go down or the track target become no longer reachable, this syslog is generated and the EEM applet invoked. The important aspect of the the route tracking configuration is the **event syslog id 622001 occurs 2** configuration line. This causes the NAT2 applet to happen *every other* time the syslog is generated. The NAT applet is invoked every time the syslog is seen. This combination results in the NAT line being removed when syslog ID 622001 is first seen (tracked route removed) and then the NAT line is re-added the second time the syslog 62201 is seen (tracked route was re-added to routing table). This has the effect of automatic removal and re-addition of the NAT line in conjunction with the route tracking feature.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Simulate a link failure which causes the tracked route to be removed from the routing table in order to complete verification.

Bring Down the Primary ISP Link

First bring down the primary (Outside) link.

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

Interface Goes Down

Notice that the Outside interface goes down and the tracking object indicates that reachability is down.

```
%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 Is Triggered

Syslog 622001 is generated as a result of the route removal and the EEM applet 'NAT' is invoked. The output of the **show event manager** command reflects the status and execution times of the individual applets.

```
%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
```

With EEM First NAT Rule is Removed

A check of the running configuration shows that the first NAT rule has been removed.

```
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
```

Verify with Packet Tracer

```
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
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.