Ejemplo de Configuración de EEM Utilizado para Controlar el Comportamiento de Desviación NAT de Dos Veces NAT Cuando se Utiliza Redundancia ISP

Contenido

Introducción

Este documento describe cómo utilizar un applet Embedded Event Manager (EEM) para controlar el comportamiento del desvío de traducción de direcciones de red (NAT) en un escenario ISP dual (redundancia ISP).

Es importante comprender que cuando se procesa una conexión a través de un firewall de dispositivo de seguridad adaptable (ASA), las reglas NAT pueden tener prioridad sobre la tabla de routing cuando se determina en qué interfaz se dirige un paquete. Si un paquete entrante coincide con una dirección IP traducida en una sentencia NAT, se utiliza la regla NAT para determinar la interfaz de salida adecuada. Esto se conoce como "Desvío NAT".

La verificación de desvío NAT (que es lo que puede invalidar la tabla de ruteo) verifica si hay una regla NAT que especifica la traducción de dirección de destino para un paquete entrante que llega a una interfaz. Si no hay ninguna regla que especifique explícitamente cómo traducir la dirección IP de destino de ese paquete, se consulta la tabla de ruteo global para determinar la interfaz de egreso. Si hay una regla que especifica explícitamente cómo traducir la dirección IP de destino del paquete, entonces la regla NAT "extrae" o "desvía" el paquete a la otra interfaz en la

traducción y la tabla de ruteo global se omite de manera efectiva.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en un ASA que ejecuta la versión de software 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.

Configurar

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Se han configurado tres interfaces; Interior, Exterior (ISP principal) y BackupISP (ISP secundario). Estas dos sentencias NAT se han configurado para traducir el tráfico de cualquier interfaz cuando va a una subred específica (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
```

Configuración del Seguimiento de Rutas

```
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
```

¿Qué ocurre cuando el link principal se desactiva?

Antes de que el enlace principal (externo) se interrumpa, el tráfico fluye según lo esperado en la interfaz externa. Se utiliza la primera regla NAT de la tabla y el tráfico se traduce a la dirección IP adecuada para la interfaz externa (192.0.2.100_nat). Ahora las interfaces externas se desactivan o el seguimiento de la ruta falla. El tráfico sigue a la primera instrucción NAT y se desvía NAT a la interfaz externa, **NO** a la interfaz BackupISP. Este es un comportamiento conocido como NAT Divert. El tráfico destinado a 203.0.113.0/24 está en espera negra.

Este comportamiento se puede observar con el comando **packet tracer**. Observe la línea **NAT Divert** en la **fase 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
```

Estas reglas NAT están diseñadas para reemplazar la tabla de ruteo. Hay algunas versiones de ASA en las que puede que no se produzca el desvío y esta solución podría funcionar realmente, pero con la corrección para el ID de bug de Cisco CSCul98420 estas reglas (y el comportamiento esperado en el futuro) definitivamente desvía el paquete a la primera interfaz de salida configurada. El paquete se descarta aquí si la interfaz se desactiva o se elimina la ruta de seguimiento.

Solución Aternativa

Puesto que la presencia de la regla NAT en la configuración fuerza al tráfico a desviarse a la interfaz incorrecta, las líneas de configuración deben eliminarse temporalmente para solucionar el problema. Puede introducir la forma "no" de la línea NAT específica, sin embargo, esta intervención manual puede tardar y se podría enfrentar una interrupción. Para acelerar el proceso, la tarea debe automatizarse de alguna manera. Esto se puede lograr con la función EEM introducida en ASA versión 9.2.1. La configuración se muestra aquí:

```
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
```

Esta tarea funciona cuando EEM se aprovecha para realizar una acción si se ve syslog 622001. Este syslog se genera cuando una ruta en rack se elimina o se agrega de nuevo a la tabla de ruteo. Dada la configuración de seguimiento de ruta mostrada anteriormente, si la interfaz externa se desactiva o el destino de pista deja de ser accesible, se genera este syslog y se invoca el applet EEM. El aspecto importante de la configuración de seguimiento de ruta es el **evento syslog id 622001 ocurre 2** líneas de configuración. Esto hace que el applet NAT2 suceda *cada dos* veces que se genera el syslog. El applet NAT se invoca cada vez que se ve el syslog. Esta combinación hace que la línea NAT se elimine cuando se ve por primera vez el ID de syslog 622001 (ruta de seguimiento eliminada) y luego se vuelve a agregar la línea NAT la segunda vez que se ve el syslog 62201 (la ruta de seguimiento se volvió a agregar a la tabla de ruteo). Esto tiene el efecto de la remoción y readición automáticas de la línea NAT junto con la función de seguimiento de ruta.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Simula una falla de link que hace que la ruta de seguimiento se elimine de la tabla de ruteo para completar la verificación.

Apagar el enlace ISP principal

Primero, desactive el enlace primario (externo).

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

La interfaz se desactiva

Observe que la interfaz externa se desactiva y el objeto de seguimiento indica que la disponibilidad está inactiva.

```
%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 está activado

Syslog 622001 se genera como resultado de la eliminación de la ruta y se invoca el applet EEM 'NAT'. La salida del comando **show event manager** refleja el estado y los tiempos de ejecución de los applets individuales.

```
%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
```

Con EEM, se elimina la primera regla NAT

Una verificación de la configuración en ejecución muestra que se ha eliminado la primera regla NAT.

```
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
```

Verificar con 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

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.