EEM usados para controlar el NAT desvían el comportamiento dos veces del NAT cuando la Redundancia ISP es ejemplo de configuración usado

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Configurar
Ruta-seguimiento de la configuración
¿Qué sucede cuando va el link principal abajo?
Solución Aternativa
Verificación
Derribe el link del ISP primario
La interfaz va abajo
Se acciona EEM
Con EEM primero NAT la regla se quita
Verifique con el trazalíneas del paquete
Troubleshooting

Introducción

Este documento describe cómo utilizar un applet integrado del administrador del evento (EEM) para controlar el comportamiento del Network Address Translation (NAT) desvía en un escenario dual ISP (Redundancia ISP).

Es importante entender que cuando una conexión se procesa con un Firewall adaptante del dispositivo de seguridad (ASA), las reglas NAT pueden tomar la precedencia sobre la tabla de ruteo cuando se hace la determinación en la cual interfaz las salidas de un paquete. Si un paquete de entrada corresponde con un IP Address traducido en una sentencia NAT, la regla NAT se utiliza para determinar la interfaz de egreso apropiada. Esto se conoce como “NAT desvía”.

El NAT desvía los controles del control (que es qué puede reemplazar la tabla de ruteo) para ver si hay una regla NAT que especifica la traducción de la dirección destino para un paquete de entrada que llegue en una interfaz. Si hay no se consulta ninguna regla que especifica explícitamente cómo traducir el IP Address de destino, después la tabla de Global Routing de ese paquete para determinar la interfaz de egreso. Si hay una regla que especifica explícitamente

cómo traducir el IP Address de destino del paquete, después la regla NAT “tira” o “desvía” el paquete a la otra interfaz en la traducción y la tabla de Global Routing se desvía con eficacia.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en un ASA que funcione con el Software Release 9.2.1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

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, fuera de (ISP primario), y BackupISP (ISP secundario). Estas dos sentencias NAT se han configurado para traducir el tráfico hacia fuera 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
```

Ruta-seguimiento de la configuración

```
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 sucede cuando va el link principal abajo?

Antes (afuera) del link primario que va abajo, flujos de tráfico como se esperaba hacia fuera la interfaz exterior. La primera regla NAT en la tabla se utiliza y el tráfico se traduce a la dirección IP apropiada para el interfaz exterior (192.0.2.100_nat). Ahora las interfaces exteriores van abajo, o el seguimiento de la ruta falla. El tráfico sigue la primera sentencia NAT y sigue siendo NAT desviado a la interfaz exterior, **NO la** interfaz de BackupISP. Esto es un comportamiento conocido como NAT desvía. El tráfico destinado a los 203.0.113.0/24 negro-se agujerea con eficacia.

Este comportamiento se puede observar con el comando del **trazalíneas del paquete**. Observe el **NAT desvían la** línea 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 se diseñan para reemplazar la tabla de ruteo. Hay algunas Versiones de ASA donde el desviar no pudo suceder y esta solución pudo trabajar realmente, pero con el arreglo para el Id. de bug Cisco CSCul98420 estas reglas (y la conducta esperada que va adelante) desvían definitivamente el paquete a la primera interfaz de egreso configurada. El paquete se cae aquí si va la interfaz abajo o se quita la ruta seguida.

Solución Aternativa

Puesto que la presencia de la regla NAT en la configuración fuerza el tráfico para desviar a la interfaz incorrecta, las líneas de configuración necesitan ser quitadas temporalmente para trabajar

alrededor del problema. Usted puede ingresar la forma del “no” de la línea específica NAT, no obstante esta intervención manual pudo tardar el tiempo y y una interrupción podría ser hecha frente. Para acelerar el proceso, la tarea necesita ser automatizada de alguna manera. Esto se puede alcanzar con la característica EEM introducida en la versión 9.2.1 ASA. La configuración se muestra aquí:

```
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
```

Esta tarea trabaja cuando EEM leveraged para tomar medidas si se ve el Syslog 622001. Se genera este Syslog cuando una ruta atormentada se quita o se agrega nuevamente dentro de la tabla de ruteo. Dado la configuración de seguimiento de la ruta mostrada anterior, va la interfaz exterior abajo o la blanco de la pista llega a ser no más accesible, este Syslog se genera y se invoca el applet EEM. El aspecto importante el configuración de seguimiento de la ruta es el **ID de syslog 622001 del evento ocurre la** línea de configuración **2**. Esto hace el applet NAT2 suceder *cada otra* hora que se genera el Syslog. Se invoca el applet NAT cada vez que se ve el Syslog. Esta combinación da lugar a la línea NAT que es quitada cuando el ID de syslog 622001 es primera considerada (ruta seguida quitada) y entonces la línea NAT es reagregada el Syslog 62201 se considera la segunda vez (la ruta seguida era reagregada a la tabla de ruteo). Esto tiene el efecto de la extracción automática y de la re-adición de la línea NAT conjuntamente con la característica de seguimiento de la ruta.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Simule una falla de link que haga la ruta seguida ser quitada de la tabla de ruteo para completar la verificación.

Derribe el link del ISP primario

Primero derribe (afuera) el link primario.

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

La interfaz va abajo

Note que va la interfaz exterior abajo y el objeto de seguimiento indica que el accesibilidad está abajo.

```
%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
```

Se acciona EEM

El Syslog 622001 se genera como resultado del retiro de la ruta y se invoca el applet “NAT” EEM. La salida del comando del **administrador del evento de la demostración** refleja los tiempos del estatus y de ejecución de los applet 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 la regla EEM primero NAT se quita

Un control de la configuración corriente muestra que se ha quitado 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
```

Verifique con el trazalíneas del paquete

```
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
```

Troubleshooting

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