EEM usados para controlar o NAT desviam o comportamento duas vezes do NAT quando a Redundância ISP é exemplo de configuração usado

Índice

Introdução

Este documento descreve como usar um applet encaixado do gerente do evento (EEM) a fim controlar o comportamento do Network Address Translation (NAT) desvia em uma encenação dupla ISP (Redundância ISP).

Éimportante compreender que quando uma conexão está processada com um Firewall adaptável da ferramenta de segurança (ASA), as regras NAT podem tomar a precedência sobre a tabela de roteamento quando a determinação é feita que na relação saídas de um pacote. Se um pacote de entrada combina um endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido em uma declaração NAT, a regra NAT está usada a fim determinar a interface de saída apropriada. Isto é sabido como o “NAT desvia”.

O NAT desvia verificações da verificação (que é o que pode cancelar a tabela de roteamento) para ver se há uma regra NAT que especifique a tradução de endereço de destino para um pacote de entrada que chegue em uma relação. Se há nenhuma regra que especifica explicitamente como traduzir o endereço IP de destino, a seguir a tabela de roteamento global desse pacote está consultada a fim determinar a interface de saída. Se há uma regra que

especifique explicitamente como traduzir o endereço IP de destino do pacote, a seguir a regra NAT “puxa” ou “desvia” o pacote à outra relação na tradução e a tabela de roteamento global é contorneada eficazmente.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em um ASA que execute o Software Release 9.2.1.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Três relações foram configuradas; Interno, fora de (ISP principal), e BackupISP (ISP secundário). Estas duas declarações NAT estiveram configuradas para traduzir para fora o tráfego uma ou outra relação quando vai a uma sub-rede 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
```

Configurar o Rota-seguimento

```
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
```

Que acontece quando o link principal vai para baixo?

Antes (fora) do link preliminar que vai para baixo, fluxos de tráfego como esperado para fora a interface externa. A primeira regra NAT na tabela é usada e o tráfego é traduzido ao endereço IP de Um ou Mais Servidores Cisco ICM NT apropriado para o a interface externa (192.0.2.100_nat). Agora as interfaces externas vão para baixo, ou o seguimento da rota falha. O tráfego ainda segue a primeira declaração NAT e é NAT desviado à interface externa, **NÃO a** relação de BackupISP. Este é um comportamento conhecido como o NAT desvia. O tráfego destinado aos 203.0.113.0/24 preto-é furado eficazmente.

Este comportamento pode ser observado com o comando do **projétil luminoso do pacote**. Note o **NAT desviam a** linha na 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 regras NAT são projetadas cancelar a tabela de roteamento. Há algumas versões ASA onde o desvio não pôde acontecer e esta solução pôde realmente trabalhar, mas com o reparo para a identificação de bug Cisco CSCul98420 estas regras (e o comportamento esperado que vai para a frente) desviam definidamente o pacote à primeira interface de saída configurada. O pacote está deixado cair aqui se a relação vai para baixo ou a rota seguida está removida.

Solução

Desde que a presença da regra NAT na configuração força o tráfego para desviar à interface

errada, as linhas de configuração precisam de ser removidas temporariamente a fim trabalhar em torno do problema. Você pode incorporar “não” o formulário da linha específica NAT, porém esta intervenção manual pôde tomar o tempo e e uma indisponibilidade poderia ser enfrentada. A fim acelerar o processo, a tarefa precisa de ser automatizada em alguma forma. Isto pode ser conseguido com a característica EEM introduzida na liberação 9.2.1 ASA. A configuração é mostrada aqui:

```
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 tarefa trabalha quando EEM leveraged para tomar uma ação se o Syslog 622001 está visto. Este Syslog é gerado quando uma rota submetida é removida ou adicionada de novo na tabela de roteamento. Dado a configuração de seguimento da rota mostrada mais cedo, a interface externa for para baixo ou o alvo da trilha se torna já não alcançável, este Syslog é gerado e o applet EEM é invocado. O aspecto importante o da configuração de seguimento da rota é a **identificação 622001 do Syslog do evento ocorre a** linha de configuração **2**. Isto faz com que o applet NAT2 aconteça *cada outra* hora onde o Syslog é gerado. O applet NAT é invocado cada vez que o Syslog é visto. Esta combinação conduz à linha NAT que está sendo removida quando o Syslog ID 622001 é primeira considerada (rota seguida removida) e a linha NAT é adicionar novamente então a segunda vez o Syslog 62201 é considerada (a rota seguida foi adicionar novamente à tabela de roteamento). Isto tem o efeito da remoção automática e da re-adição da linha NAT conjuntamente com os recursos de tracking da rota.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Simule uma falha do link que faça com que a rota seguida seja removida da tabela de roteamento a fim terminar a verificação.

Derrube o link do ISP principal

Derrube primeiramente (fora) o link preliminar.

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

A relação vai para baixo

Observe que a interface externa vai para baixo e o objeto de seguimento indica que a

alcançabilidade está para baixo.

```
%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 é provocado

O Syslog 622001 é gerado em consequência da remoção da rota e o applet “NAT” EEM é invocado. A saída do **comando manager do evento da mostra** reflete os tempos do estado e de execução dos applet individuais.

```
%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
```

Com regra EEM NAT é removido primeiramente

Uma verificação da configuração running mostra que a primeira regra NAT esteve removida.

```
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 com projétil luminoso do pacote

```
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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.