EEM usado para controlar o comportamento de desvio de NAT de duas vezes NAT quando a redundância de ISP é usada Exemplo de configuração

Contents

Introduction

Este documento descreve como usar um miniaplicativo Embedded Event Manager (EEM) para controlar o comportamento da conversão de endereço de rede (NAT) em um cenário de ISP duplo (redundância de ISP).

Éimportante entender que quando uma conexão é processada por meio de um firewall do Adaptive Security Appliance (ASA), as regras de NAT podem ter precedência sobre a tabela de roteamento quando a determinação é feita em que interface um pacote sai. Se um pacote de entrada corresponder a um endereço IP convertido em uma instrução NAT, a regra NAT será usada para determinar a interface de saída apropriada. Isso é conhecido como "desvio de NAT".

A verificação de desvio de NAT (que é o que pode substituir a tabela de roteamento) verifica se há uma regra de NAT que especifica a conversão do endereço de destino para um pacote de entrada que chega em uma interface. Se não houver uma regra que especifique explicitamente como converter o endereço IP de destino do pacote, a tabela de roteamento global será consultada para determinar a interface de saída. Se houver uma regra que especifique explicitamente como converter o endereço IP de destino do pacote, a regra de NAT "puxa" ou

"encaminha" o pacote para a outra interface na tradução e a tabela de roteamento global será efetivamente ignorada.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas em um ASA que executa o software versão 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

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

Três interfaces foram configuradas; Dentro, fora (ISP principal) e BackupISP (ISP secundário). Essas duas instruções NAT foram configuradas para converter o tráfego de qualquer interface quando ele vai para 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 Rastreamento de Rota

```
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
```

O que acontece quando o link principal cai?

Antes do enlace principal (externo) ser desativado, o tráfego flui conforme esperado para fora da interface externa. A primeira regra NAT na tabela é usada e o tráfego é convertido para o endereço IP apropriado para a interface externa (192.0.2.100_nat). Agora as interfaces externas ficam inativas ou o rastreamento de rota falha. O tráfego ainda segue a primeira instrução NAT e é NAT Divertido para a interface externa, **NÃO** a interface BackupISP. Este é um comportamento conhecido como desvio de NAT. O tráfego destinado ao 203.0.113.0/24 é efetivamente preto.

Esse comportamento pode ser observado com o comando **packet tracer**. Observe a linha **NAT Divert** 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
```

Essas regras de NAT são projetadas para substituir a tabela de roteamento. Há algumas versões do ASA em que o desvio pode não acontecer e essa solução pode realmente funcionar, mas com a correção para o bug da Cisco ID CSCul98420 essas regras (e o comportamento esperado em frente) definitivamente encaminha o pacote para a primeira interface de saída configurada. O pacote será descartado aqui se a interface ficar inativa ou se a rota rastreada for removida.

Solução

Como a presença da regra NAT na configuração força o tráfego a ser desviado para a interface errada, as linhas de configuração precisam ser removidas temporariamente para resolver o problema. Você pode inserir a forma "não" da linha NAT específica, no entanto, essa intervenção manual pode demorar um pouco e uma interrupção pode ser enfrentada. Para acelerar o processo, a tarefa precisa ser automatizada de alguma forma. Isso pode ser feito com o recurso EEM introduzido no ASA versão 9.2.1. 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 funciona quando o EEM é utilizado para tomar uma ação se o syslog 622001 for exibido. Esse syslog é gerado quando uma rota em rack é removida ou adicionada novamente à tabela de roteamento. Dada a configuração de rastreamento de rota mostrada anteriormente, se a interface externa for desativada ou o destino de rastreamento não for mais alcançável, esse syslog será gerado e o applet EEM será chamado. O aspecto importante da configuração de rastreamento de rota é o **evento syslog id 622001 ocorre em 2** linhas de configuração. Isso faz com que o miniaplicativo NAT2 aconteça *em* qualquer *outra* vez que o syslog é gerado. O miniaplicativo NAT é chamado toda vez que o syslog é visto. Essa combinação faz com que a linha NAT seja removida quando o syslog ID 622001 é visto pela primeira vez (rota rastreada removida) e, em seguida, a linha NAT é adicionada novamente na segunda vez em que o syslog 62201 é visto (a rota rastreada foi adicionada novamente à tabela de roteamento). Isso tem o efeito da remoção e readição automáticas da linha NAT em conjunto com o recurso de rastreamento de rota.

Verificar

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

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Simule uma falha de link que faça com que a rota rastreada seja removida da tabela de roteamento para concluir a verificação.

Desative o link principal do ISP

Primeiro, ative o link principal (Externo).

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

Interface Inativa

Observe que a interface externa fica inativa e o objeto de rastreamento indica que a acessibilidade está inativa.

```
%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 acionado

O syslog 622001 é gerado como resultado da remoção da rota e o applet EEM 'NAT' é chamado. A saída do comando **show event manager** reflete o status e os tempos de execução dos applets 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 a primeira regra NAT do EEM removida

Uma verificação da configuração atual mostra que a primeira regra de NAT foi 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
```

Verificar com o 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta

configuração.