EEM wordt gebruikt om het NAT-omleidingsgedrag van Twice NAT te controleren wanneer ISP-redundantie wordt gebruikt als Configuratievoorbeeld

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Configureren
Routetracering configureren
Wat gebeurt er als de primaire link omlaag gaat?
Werken
Verifiëren
Verlaag de primaire ISP-link
Interface wordt omlaag gebracht
EEM wordt geactiveerd
Met EEM First NAT-regel wordt verwijderd
Controleer met Packet Tracer
Problemen oplossen

Inleiding

In dit document wordt beschreven hoe u een EEM-applicatie (Embedded Event Manager) kunt gebruiken om het gedrag van NAT (Network Address Translation) Divert in een Dual ISP Scenario (ISP Redundantie) te controleren.

Het is belangrijk om te begrijpen dat wanneer een verbinding door een adaptieve security applicatie (ASA) firewall wordt verwerkt, NAT-regels voorrang kunnen krijgen boven de routingtabel wanneer de bepaling wordt uitgevoerd op welke interface een pakketjurk wordt gemaakt. Als een inkomende pakket overeenkomt met een vertaald IP-adres in een NAT-verklaring, wordt de NAT-regel gebruikt om de juiste opslaginterface te bepalen. Dit staat bekend als "NAT Divert".

De controle NAT Divert (wat is wat de routing tabel kan omzeilen) controleert om te zien of er een NAT-regel is die adresvertaling van een inkomende pakketreis specificeert die op een interface aankomt. Als er geen regel is die expliciet specificeert hoe u het IP-adres van de bestemming van dat pakket vertaalt, dan wordt de globale routingtabel geraadpleegd om de noodopdracht te bepalen. Als er een regel is die expliciet specificeert hoe u het IP-adres van de bestemming van

het pakket wilt vertalen, dan wordt de NAT-regel "gedempt" of "afgeleid" het pakket naar de andere interface in de vertaling en wordt de globale routingtabel effectief omzeild.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op een ASA die softwarerelease 9.2.1 uitvoert.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

> **Opmerking:** Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Er zijn drie interfaces ingesteld; Binnenin, Outside (Primaire ISP) en BackupISP (Secundaire ISP). Deze twee NAT verklaringen zijn gevormd om verkeer uit of interface te vertalen wanneer het naar een specifiek netwerk gaat (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
```

Routetracering configureren

```
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
```

Wat gebeurt er als de primaire link omlaag gaat?

Voordat de primaire (Outside) verbinding naar beneden gaat, stroomt het verkeer zoals verwacht vanuit de Outside Interface. De eerste NAT-regel in de tabel wordt gebruikt en het verkeer wordt vertaald naar het juiste IP-adres voor de externe interface (192.0.2.100_nat). Nu gaan de buiteninterfaces omlaag, of de route die volgt faalt. Het verkeer volgt nog steeds de eerste NAT-verklaring en is NAT omgekeerd naar de buiteninterface, **NIET** de back-upISP-interface. Dit is een gedrag dat bekend staat als NAT Divert. Het verkeer dat bestemd is voor de 203.0.113.0/24 is in feite zwart-wit.

Dit gedrag kan worden waargenomen met de opdracht **pakkettracer**. Let op de **lijn NAT Divert** in de **UN-NAT** fase.

```
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
```

Deze NAT-regels zijn ontworpen om de routingtabel te omzeilen. Er zijn een aantal ASA-versies waarin de conversie mogelijk niet heeft plaatsgevonden en deze oplossing misschien zelfs werkt, maar met de oplossing voor Cisco bug-ID CSCul98420 leiden deze regels (en het verwachte gedrag dat vooruit gaat) definitief het pakket naar de eerste geconfigureerde noodopinterface. Het pakje wordt hier ingetrokken als de interface naar beneden gaat of als de trackroute wordt verwijderd.

Werken

Aangezien de aanwezigheid van de NAT-regel in de configuratie het verkeer dwingt om naar de verkeerde interface te verschuiven, moeten de configuratielijnen tijdelijk worden verwijderd om rond het probleem te werken. U kunt het "nee"-formulier van de specifieke NAT-lijn invoeren, maar dit handmatige ingrijpen kan tijd in beslag nemen en er kan een storing optreden. Om het proces te versnellen, moet de taak op enige manier worden geautomatiseerd. Dit kan worden bereikt met de EEM-functie die is geïntroduceerd in ASA release 9.2.1. De configuratie wordt hier getoond:

```
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
```

Deze taak werkt wanneer EEM een beroep kan doen op een beroep op de overheid als er syslog 622001 wordt gezien. Dit wordt gegenereerd wanneer een rackroute wordt verwijderd of opnieuw in de routingtabel wordt toegevoegd. Gezien de eerder getoonde routeswitchconfiguratie, wordt, indien de buiteninterface omlaag gaat of het doel van het spoor niet langer bereikbaar wordt, deze syslog gegenereerd en wordt de EEM-applicatie geactiveerd. Het belangrijke aspect van de configuratie van het route volgen is de **gebeurtenis syslog id 62001 komt voor 2** configuratielijn. Hierdoor wordt de NAT2-applicatie *om* het *even* wanneer de slang gegenereerd wordt uitgevoerd. NAT-applet wordt elke keer dat het beeld wordt weergegeven opgeroepen. Deze combinatie resulteert in het verwijderen van de NAT-lijn wanneer syslog ID 622001 voor het eerst wordt gezien (trackroute verwijderd) en dan wordt de NAT-lijn opnieuw toegevoegd de tweede keer dat syslog 62201 wordt gezien (trackroute werd opnieuw toegevoegd aan de routingtabel). Dit heeft het effect dat de NAT-lijn automatisch wordt verwijderd en opnieuw wordt toegevoegd in combinatie met de volgende route.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht show.

Simuleer een verbindingsmislukking die ervoor zorgt dat de getraceerde route uit de routingtabel wordt verwijderd om verificatie te voltooien.

Verlaag de primaire ISP-link

Neem eerst de primaire (Outside) link naar beneden.

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

Interface wordt omlaag gebracht

Merk op dat de buiteninterface omlaag gaat en het volgobject aangeeft dat bereikbaarheid is weggevallen.

```
%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 wordt geactiveerd

Syslog 622001 wordt gegenereerd als gevolg van het wegvallen van de route en het EEM-applet "NAT" wordt ingeroepen. De output van de opdracht van de **show event manager** reflecteert de status en de uitvoertijden van de individuele 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
```

Met EEM First NAT-regel wordt verwijderd

Na controle van de actieve configuratie is gebleken dat de eerste NAT-regel is verwijderd.

```
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
```

Controleer met 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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.