Esempio di configurazione EEM utilizzato per controllare il comportamento di deviazione NAT di due NAT quando si utilizza la ridondanza ISP

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Configurazione](#)
[Configura route-tracking](#)
[Che cosa succede quando il collegamento principale si interrompe?](#)
[Soluzione alternativa](#)
[Verifica](#)
[Riduzione del collegamento all'ISP primario](#)
[Interfaccia inattiva](#)
[EEM Attivato](#)
[Con EEM La prima regola NAT viene rimossa](#)
[Verifica con Packet Tracer](#)
[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come utilizzare un'applet EEM (Embedded Event Manager) per controllare il comportamento di NAT (Network Address Translation) Devit in a Dual ISP Scenario (ISP Redundancy).

Èimportante capire che quando una connessione viene elaborata tramite un firewall ASA (Adaptive Security Appliance), le regole NAT possono avere la precedenza sulla tabella di routing quando si determina l'interfaccia da cui proviene il pacchetto. Se un pacchetto in entrata corrisponde a un indirizzo IP tradotto in un'istruzione NAT, viene utilizzata la regola NAT per determinare l'interfaccia di uscita appropriata. Questo processo è noto come "NAT Divert".

Il controllo deviazione NAT (che può ignorare la tabella di routing) verifica se esiste una regola NAT che specifica la conversione dell'indirizzo di destinazione per un pacchetto in entrata che arriva su un'interfaccia. Se non vi sono regole che specificano esplicitamente come convertire l'indirizzo IP di destinazione del pacchetto, viene consultata la tabella di routing globale per determinare l'interfaccia di uscita. Se esiste una regola che specifica in modo esplicito come tradurre l'indirizzo IP di destinazione del pacchetto, la regola NAT "preleva" o "devia" il pacchetto verso l'altra interfaccia nella conversione e la tabella di routing globale viene ignorata.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stata usata un'appliance ASA con software versione 9.2.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Sono state configurate tre interfacce; Interno, Esterno (ISP primario) e BackupISP (ISP secondario). Queste due istruzioni NAT sono state configurate per tradurre il traffico in uscita da entrambe le interfacce quando viene indirizzata a una subnet specifica (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
```

Configura route-tracking

```
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
```

Che cosa succede quando il collegamento principale si interrompe?

Prima che il collegamento principale (esterno) si arresti, il traffico scorre come previsto dall'interfaccia esterna. Viene utilizzata la prima regola NAT della tabella e il traffico viene

convertito nell'indirizzo IP appropriato per l'interfaccia esterna (192.0.2.100_nat). Ora le interfacce esterne si interrompono, o il tracciamento del percorso fallisce. Il traffico segue ancora la prima istruzione NAT e viene deviato da NAT all'interfaccia esterna, **NON** all'interfaccia BackupISP. Questo è un comportamento noto come NAT Divert. Il traffico diretto a 203.0.113.0/24 è effettivamente bloccato.

Questo comportamento può essere osservato con il comando **packet tracer**. Notare la linea di deviazione **NAT** nella 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
```

Queste regole NAT sono progettate per sostituire la tabella di routing. In alcune versioni ASA il trasferimento potrebbe non avvenire e la soluzione potrebbe funzionare, ma con la correzione dell'ID bug Cisco CSCul98420 queste regole (e il comportamento previsto in futuro) indirizzano definitivamente il pacchetto alla prima interfaccia in uscita configurata. Il pacchetto viene scartato qui se l'interfaccia non funziona o se il percorso viene rimosso.

Soluzione alternativa

Poiché la presenza della regola NAT nella configurazione forza il traffico a deviare all'interfaccia sbagliata, le linee di configurazione devono essere rimosse temporaneamente per risolvere il

problema. È possibile immettere la forma "no" della linea NAT specifica, tuttavia questo intervento manuale potrebbe richiedere tempo e potrebbe verificarsi un'interruzione dell'alimentazione. Per accelerare il processo, l'operazione deve essere in qualche modo automatizzata. A tale scopo, è possibile usare la funzione EEM introdotta in ASA versione 9.2.1. La configurazione è mostrata di seguito:

```
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
```

Questa attività funziona quando EEM viene utilizzato per eseguire un'azione se viene visualizzato syslog 62001. Questo syslog viene generato quando un route su rack viene rimosso o aggiunto nuovamente alla tabella di routing. Data la configurazione di tracciamento del percorso mostrata in precedenza, se l'interfaccia esterna diventa inattiva o la destinazione del percorso non è più raggiungibile, viene generato questo syslog e richiamata l'applet EEM. L'aspetto importante della configurazione di tracciamento route è che l'**evento syslog con ID 62001 si verifica su 2** linee di configurazione. In questo modo, l'applet NAT2 viene generata *ogni due* volte. L'applet NAT viene richiamata ogni volta che viene visualizzato il syslog. Questa combinazione determina la rimozione della riga NAT quando si rileva per la prima volta l'ID syslog 62001 (il percorso tracciato viene rimosso) e quindi la riga NAT viene aggiunta la seconda volta che si rileva il syslog 62201 (il percorso tracciato è stato aggiunto nuovamente alla tabella di routing). Questo ha l'effetto di rimuovere e riaggiungere automaticamente la linea NAT insieme alla funzione di tracciamento del percorso.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando show.

Simulare un errore di collegamento che provoca la rimozione del percorso dalla tabella di routing per completare la verifica.

Riduzione del collegamento all'ISP primario

Innanzitutto, abbassare il collegamento primario (esterno).

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

Interfaccia inattiva

Si noti che l'interfaccia Esterna diventa inattiva e l'oggetto di rilevamento indica che la raggiungibilità è inattiva.

```
%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 Attivato

Syslog 62001 viene generato in seguito alla rimozione della route e viene richiamata l'applet EEM 'NAT'. L'output del comando **show event manager** riflette lo stato e i tempi di esecuzione delle singole applet.

```
%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 La prima regola NAT viene rimossa

Un controllo della configurazione corrente mostra che la prima regola NAT è stata rimossa.

```
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
```

Verifica 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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.