Exemple de configuration du module EEM utilisé pour contrôler le comportement de renvoi NAT de deux NAT lorsque la redondance ISP est utilisée

Contenu

Introduction

Ce document décrit comment utiliser une applet Embedded Event Manager (EEM) afin de contrôler le comportement du renvoi NAT (Network Address Translation) dans un double scénario ISP (ISP Redundancy).

Il est important de comprendre que lorsqu'une connexion est traitée via un pare-feu ASA (Adaptive Security Appliance), les règles NAT peuvent avoir préséance sur la table de routage lorsque la détermination de l'interface de sortie d'un paquet est effectuée. Si un paquet entrant correspond à une adresse IP traduite dans une instruction NAT, la règle NAT est utilisée afin de déterminer l'interface de sortie appropriée. C'est ce que l'on appelle le renvoi NAT.

Le contrôle NAT Divert (qui peut remplacer la table de routage) vérifie s'il existe une règle NAT qui spécifie la traduction d'adresse de destination pour un paquet entrant qui arrive sur une interface. S'il n'existe aucune règle qui spécifie explicitement comment traduire l'adresse IP de destination de ce paquet, alors la table de routage globale est consultée afin de déterminer l'interface de sortie. S'il existe une règle qui spécifie explicitement comment traduire l'adresse IP de destination du paquet, alors la règle NAT « extrait » ou « dévie » le paquet vers l'autre interface de la

traduction et la table de routage globale est effectivement contournée.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur un ASA qui exécute le logiciel version 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.

Configuration

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Trois interfaces ont été configurées ; Inside, Outside (ISP principal) et BackupISP (ISP secondaire). Ces deux instructions NAT ont été configurées pour traduire le trafic en sortie de l'une ou l'autre des interfaces lorsqu'il va à un sous-réseau spécifique (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
```

Configurer le suivi de route

```
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 se passe-t-il lorsque la liaison principale tombe en panne ?

Avant que la liaison principale (externe) ne tombe en panne, le trafic circule comme prévu depuis l'interface externe. La première règle NAT de la table est utilisée et le trafic est traduit en adresse IP appropriée pour l'interface externe (192.0.2.100_nat). Maintenant, les interfaces externes sont désactivées ou le suivi de route échoue. Le trafic suit toujours la première instruction NAT et est transféré à l'interface externe, **NOT** l'interface BackupISP. Il s'agit d'un comportement appelé renvoi NAT. Le trafic destiné au réseau 203.0.113.0/24 est en fait en noir.

Ce comportement peut être observé avec la commande **packet tracer**. Notez la ligne de **renvoi NAT** dans la phase **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
```

Ces règles NAT sont conçues pour remplacer la table de routage. Il existe certaines versions d'ASA où le renvoi pourrait ne pas se produire et cette solution pourrait effectivement fonctionner, mais avec la correction pour l'ID de bogue Cisco CSCul98420 ces règles (et le comportement attendu à l'avenir) détournent définitivement le paquet vers la première interface de sortie configurée. Le paquet est abandonné ici si l'interface tombe en panne ou si la route suivie est supprimée.

Solution de contournement

Puisque la présence de la règle NAT dans la configuration force le trafic à se dérouter vers la mauvaise interface, les lignes de configuration doivent être supprimées temporairement afin de contourner le problème. Vous pouvez entrer la forme « non » de la ligne NAT spécifique, mais cette intervention manuelle peut prendre du temps et être confrontée à une panne. Pour accélérer le processus, la tâche doit être automatisée d'une certaine manière. Cela peut être réalisé avec la fonctionnalité EEM introduite dans ASA version 9.2.1. La configuration est présentée ici :

```
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
```

Cette tâche fonctionne lorsque le module EEM est utilisé pour effectuer une action si syslog 622001 est vu. Ce syslog est généré lorsqu'une route en rack est supprimée ou ajoutée à nouveau dans la table de routage. Compte tenu de la configuration de suivi de route indiquée précédemment, si l'interface externe tombe en panne ou si la cible de la piste n'est plus accessible, ce syslog est généré et l'applet EEM appelée. L'aspect important de la configuration de suivi de route est l'**événement syslog id 622001 se produit 2** ligne de configuration. Cela entraîne l'exécution de l'applet NAT2 *tous les deux* fois que le syslog est généré. L'applet NAT est appelée chaque fois que le syslog est vu. Cette combinaison entraîne la suppression de la ligne NAT lorsque l'ID syslog 622001 est vu pour la première fois (route suivie supprimée), puis que la ligne NAT est réajoutée la deuxième fois que le syslog 62201 est vu (route suivie a été réajoutée à la table de routage). Cela a pour effet de supprimer et de réajouter automatiquement la ligne NAT en conjonction avec la fonctionnalité de suivi de route.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines **commandes d'affichage.** Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Simuler une défaillance de liaison qui entraîne la suppression de la route suivie de la table de routage afin de terminer la vérification.

Arrêt de la liaison principale du FAI

Déconnectez d'abord la liaison principale (externe).

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

L'interface s'arrête

Notez que l'interface Outside est désactivée et que l'objet de suivi indique que l'accessibilité est désactivée.

```
%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
```

Le module EEM est déclenché

Syslog 622001 est généré à la suite de la suppression de la route et l'applet EEM 'NAT' est appelée. La sortie de la commande **show event manager** reflète l'état et les temps d'exécution des applets individuels.

```
%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
```

Avec la première règle NAT EEM supprimée

Une vérification de la configuration en cours indique que la première règle NAT a été supprimée.

```
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
```

Vérification avec 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
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.