EEM utilisés pour contrôler le NAT détournent le comportement deux fois de NAT quand la Redondance ISP est exemple utilisé de configuration

Contenu

Introduction

Ce document décrit comment employer un applet encastré du gestionnaire d'événement (EEM) afin de contrôler le comportement du Traduction d'adresses de réseau (NAT) détournent dans un double scénario ISP (Redondance ISP).

Il est important de comprendre que quand une connexion est traitée par un Pare-feu de l'appliance de sécurité adaptable (ASA), les règles NAT peuvent avoir la priorité au-dessus de la table de routage quand la détermination est faite sur laquelle l'interface des de sortie d'un paquet. Si un paquet entrant apparie une adresse IP traduite dans une déclaration NAT, la règle NAT est utilisée afin de déterminer l'interface de sortie appropriée. Ceci est connu en tant que « NAT détournent ».

Le NAT détournent des contrôles de contrôle (qui est ce qui peut ignorer la table de routage) pour voir s'il y a une règle NAT qui spécifie la translation d'adresses d'adresse de destination pour un paquet entrant qui arrive sur une interface. S'il y a aucune règle qui spécifie explicitement comment traduire l'adresse IP de la destination de ce paquet, alors la table de routage globale n'est consultée afin de déterminer l'interface de sortie. S'il y a une règle qui spécifie explicitement

comment traduire l'adresse IP de la destination du paquet, alors la règle NAT « tire » ou « détourne » le paquet à l'autre interface dans la traduction et la table de routage globale est efficacement sautée.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur une ASA qui exécute la version de logiciel 9.2.1.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

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

Trois interfaces ont été configurées ; Intérieur, en dehors de (ISP primaire), et BackupISP (ISP secondaire). Ces deux déclarations NAT ont été configurées pour traduire le trafic l'un ou l'autre d'interface quand 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
```

Configurez l'Artère-cheminement

```
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 produit quand la liaison principale descend ?

Avant (dehors) le lien primaire allant vers le bas, la circulation comme prévue l'interface extérieure. La première règle NAT dans la table est utilisée et le trafic est traduit à l'adresse IP appropriée pour la l'interface extérieure (192.0.2.100_nat). Maintenant les interfaces extérieures va vers le bas, ou le cheminement d'artère échoue. Le trafic suit la première déclaration NAT et est toujours NAT détourné à l'interface extérieure, **PAS l'**interface de BackupISP. C'est un comportement connu sous le nom de NAT détournent. Le trafic destiné aux 203.0.113.0/24 noir-est efficacement troué.

On peut observer ce comportement avec la commande de **traceur de paquet**. Notez le **NAT détournent la** ligne pendant 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 d'ignorer la table de routage. Il y a quelques versions ASA où le détournement ne pourrait pas se produire et cette solution pourrait réellement fonctionner, mais avec la difficulté pour l'ID de bogue Cisco CSCul98420 ces règles (et le comportement prévu allant en avant) détournent certainement le paquet à la première interface de sortie configurée. Le paquet est lâché ici si l'interface descend ou l'artère dépistée est retirée.

Contournement

Puisque la présence de la règle NAT dans la configuration force le trafic pour détourner à l'interface fausse, des lignes de configuration doit être retirées temporairement afin de fonctionner autour du problème. Vous pouvez entrer dans « non » la forme de la ligne NAT spécifique, toutefois cette intervention manuelle pourrait prendre du temps et et une panne pourrait être faite face. Afin d'accélérer le processus, la tâche doit être automatisée d'une certaine façon. Ceci peut être réalisé avec la fonctionnalité introduite EEM dans la version 9.2.1 ASA. La configuration est affichée 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
```

Ce des tâches quand EEM est accru pour prendre un Syslog 622001 d'action if est vues. Ce Syslog est généré quand une artère étirée est retirée ou ajoutée de nouveau dans la table de routage. Etant donné la configuration illustrée de cheminement d'artère plus tôt, l'interface extérieure descend ou la cible de piste ne deviennent plus accessible, ce Syslog est généré et l'applet EEM est appelé. L'important aspect la de la configuration de cheminement d'artère est l'**id 622001 d'event syslog se produit** ligne de **2** configurations. Ceci fait produire l'applet NAT2 *chaque autre* heure où le Syslog est généré. L'applet NAT est appelé chaque fois que le Syslog est vu. Cette combinaison a comme conséquence la ligne NAT étant retirée quand l'ID 622001 de Syslog est première vue (artère dépistée retirée) et alors la ligne NAT re-est ajoutée la deuxième fois le Syslog 62201 est vue (l'artère dépistée re-a été ajoutée à la table de routage). Ceci a l'effet de la suppression et du re-ajout automatiques de la ligne NAT en même temps que la fonctionnalité de suivi d'artère.

Vérifiez

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

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Simulez une panne de lien qui cause l'artère dépistée d'être retirée de la table de routage afin de se terminer la vérification.

Réduisez le lien primaire ISP

Réduisez d'abord (dehors) le lien primaire.

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

L'interface descend

Notez que l'interface extérieure descend et l'objet de cheminement indique que l'accessibilité est vers le bas.

```
%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 est déclenché

Le Syslog 622001 est généré en raison de la suppression d'artère et l'applet EEM « NAT » est appelé. La sortie de l'ordre de **gestionnaire d'événement d'exposition** reflète les temps d'état et d'exécution des différents 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
```

Avec EEM d'abord la règle NAT est retirée

Un contrôle de la configuration en cours prouve que la première règle NAT a été retirée.

```
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
```

Vérifiez 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
```

Dépannez

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