EEM zur Kontrolle des NAT-Divert-Verhaltens von doppelter NAT bei Verwendung der ISP-Redundanz - Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument beschreibt die Verwendung eines EEM-Applets (Embedded Event Manager), um das Verhalten des Network Address Translation (NAT) Diverts in einem Dual-ISP-Szenario (ISP-Redundanz) zu steuern.

Wenn eine Verbindung über eine ASA-Firewall (Adaptive Security Appliance) verarbeitet wird, müssen die NAT-Regeln der Routingtabelle übergeordnet werden, wenn bestimmt wird, über welche Schnittstelle ein Paket ausgeht. Wenn ein eingehendes Paket mit einer übersetzten IP-Adresse in einer NAT-Anweisung übereinstimmt, wird die NAT-Regel verwendet, um die entsprechende Ausgangsschnittstelle zu bestimmen. Dies wird als "NAT Divert" bezeichnet.

Die NAT-Prüfung (die die Routing-Tabelle überschreiben kann) überprüft, ob eine NAT-Regel vorliegt, die die Zieladressenumwandlung für ein eingehendes Paket angibt, das an einer Schnittstelle eingeht. Wenn keine Regel explizit angibt, wie die Ziel-IP-Adresse des Pakets übersetzt werden soll, wird die globale Routing-Tabelle zur Bestimmung der Ausgangsschnittstelle herangezogen. Wenn eine Regel explizit festlegt, wie die Ziel-IP-Adresse des Pakets übersetzt werden soll, wird die NAT-Regel das Paket in die andere Schnittstelle der Übersetzung "abruft" oder "umleitet", und die globale Routing-Tabelle wird effektiv umgangen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer ASA, die Softwareversion 9.2.1 ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Es wurden drei Schnittstellen konfiguriert: Inside, Outside (Primary ISP) und BackupISP (Secondary ISP). Diese beiden NAT-Anweisungen wurden so konfiguriert, dass Datenverkehr aus jeder Schnittstelle übersetzt wird, wenn er zu einem bestimmten Subnetz (203.0.113.0/24) geht.

```
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
```

Konfigurieren der Routen-Nachverfolgung

```
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
```

Was passiert, wenn die primäre Verbindung ausfällt?

Bevor die primäre (externe) Verbindung ausfällt, fließt der Datenverkehr wie erwartet über die

externe Schnittstelle. Die erste NAT-Regel in der Tabelle wird verwendet, und der Datenverkehr wird in die entsprechende IP-Adresse für die externe Schnittstelle (192.0.2.100_nat) umgewandelt. Jetzt fallen die externen Schnittstellen aus, oder die Routenverfolgung schlägt fehl. Der Datenverkehr folgt weiterhin der ersten NAT-Anweisung und wird NAT an die externe Schnittstelle weitergeleitet, **NICHT** an die BackupISP-Schnittstelle. Dies ist ein Verhalten, das als NAT-Divert bezeichnet wird. Datenverkehr, der an die Adresse 203.0.113.0/24 gerichtet ist, ist im Grunde schwarz gehalten.

Dieses Verhalten kann mit dem Befehl **Packet Tracer** beobachtet werden. Beachten Sie die **NAT-**Leitung in der **UN-NAT-**Phase.

```
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
```

Diese NAT-Regeln wurden entwickelt, um die Routing-Tabelle zu überschreiben. Es gibt einige ASA-Versionen, bei denen die Umleitung möglicherweise nicht erfolgt und diese Lösung tatsächlich funktionieren könnte. Mit der Behebung für die Cisco Bug-ID CSCul98420 leiten diese Regeln (und das erwartete Verhalten wird fortgeführt) das Paket definitiv an die erste konfigurierte Ausgangsschnittstelle weiter. Das Paket wird hier verworfen, wenn die Schnittstelle ausfällt oder die verfolgte Route entfernt wird.

Problemumgehung

Da die NAT-Regel in der Konfiguration den Datenverkehr zur Umleitung an die falsche Schnittstelle zwingt, müssen Konfigurationsleitungen vorübergehend entfernt werden, um das Problem zu umgehen. Sie können die "Nein"-Form für die jeweilige NAT-Leitung eingeben. Dieser manuelle Eingriff kann jedoch Zeit in Anspruch nehmen und bei einem Ausfall auftreten. Um den Prozess zu beschleunigen, muss der Vorgang in gewisser Weise automatisiert werden. Dies kann mithilfe der EEM-Funktion erreicht werden, die in ASA Version 9.2.1 eingeführt wurde. Die Konfiguration wird hier angezeigt:

```
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
```

Diese Aufgabe funktioniert, wenn EEM zum Ausführen einer Aktion verwendet wird, wenn Syslog 622001 angezeigt wird. Dieses Syslog wird generiert, wenn eine Rack-Route entfernt oder der Routing-Tabelle wieder hinzugefügt wird. Wenn die zuvor gezeigte Konfiguration für die Routenverfolgung bei einem Ausfall der externen Schnittstelle oder bei Nichterreichbarkeit des Spurziels ausfällt, wird dieses Syslog generiert und das EEM-Applet aufgerufen. Der wichtige Aspekt der Routenverfolgungskonfiguration ist die **Syslog-Ereignisnummer 622001 tritt bei 2** Konfigurationszeilen auf. Dies bewirkt, dass das NAT2-Applet *jedes zweite* Mal ausgeführt wird, wenn das Syslog generiert wird. Das NAT-Applet wird jedes Mal aufgerufen, wenn das Syslog angezeigt wird. Diese Kombination bewirkt, dass die NAT-Leitung entfernt wird, wenn die Syslog-ID 622001 zum ersten Mal angezeigt wird (verfolgte Route entfernt) und die NAT-Leitung beim zweiten Auftreten des Syslog 62201 neu hinzugefügt wird (die verfolgte Route wurde der Routing-Tabelle erneut hinzugefügt). Dies führt dazu, dass die NAT-Leitung automatisch entfernt und erneut hinzugefügt wird, zusammen mit der Funktion zur Routenverfolgung.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Simulieren Sie einen Verbindungsausfall, bei dem die verfolgte Route aus der Routing-Tabelle entfernt wird, um die Überprüfung abzuschließen.

Herunterfahren des primären ISP-Links

Deaktivieren Sie zuerst die primäre (externe) Verbindung.

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

Schnittstelle wird deaktiviert

Beachten Sie, dass die Outside-Schnittstelle ausfällt und das Tracking-Objekt anzeigt, dass die Erreichbarkeit deaktiviert ist.

```
%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 wird ausgelöst

Syslog 622001 wird durch das Entfernen der Route generiert, und das EEM-Applet 'NAT' wird aufgerufen. Die Ausgabe des Befehls **show event manager** gibt den Status und die Ausführungszeiten der einzelnen Applets wieder.

```
%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
```

Mit EEM wird die erste NAT-Regel entfernt.

Eine Überprüfung der aktuellen Konfiguration zeigt, dass die erste NAT-Regel entfernt wurde.

```
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
```

Überprüfen mit 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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung

verfügbar.