Когда Резервирование интернет-провайдера является Используемым Примером конфигурации, EEM, Используемые для Управления NAT, Отклоняют Поведение Дважды NAT

Содержание

Введение

Этот документ описывает , как использовать апплет встроенного диспетчера событий (EEM) для управления поведением Технологии NAT, Отклоняют в Двойном Сценарии интернет-провайдера (Резервирование интернет-провайдера).

Важно понять, что, когда соединение обработано через межсетевой экран Устройства адаптивной защиты (ASA), правила NAT могут иметь приоритет по таблице маршрутизации, когда определение сделано на который интерфейс пакет выходы. Если входящий пакет совпадает с преобразованным IP-адресом в Выражении NAT, правило NAT используется для определения соответствующего исходящего интерфейса. Это известно, поскольку "NAT Отклоняет".

NAT Отклоняет проверку (который является тем, что может отвергнуть таблицу маршрутизации), проверки, чтобы видеть, существует ли правило NAT, которое задает трансляцию адреса назначения (DA) для входящего пакета, который поступает в

интерфейс. Если нет никакого правила, которое явно задает, как преобразовать IP - адрес назначения того пакета, то с таблицей глобальной маршрутизации консультируются для определения исходящего интерфейса. Если существует правило, которое явно задает, как преобразовать IP - адрес назначения пакета, то правило NAT "вытягивает" или "отклоняет" пакет к другому интерфейсу в трансляции, и таблица глобальной маршрутизации эффективно обойдена.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на ASA, который выполняет выпуск ПО 9.2.1.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Были настроены три интерфейса; Внутри, Вне (Основного поставщика услуг Интернет) и BackupISP (Вторичный интернет-провайдер). Эти два Выражения NAT были настроены для перевода трафика любой интерфейс, когда это переходит к определенной подсети (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
```

Настройте отслеживание маршрута

```
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
```

Когда Основное соединение Выключается, что Происходит?

До Основной (Внешней) ссылки потеря работоспособности, трафики как ожидалось Внешний интерфейс. Первое правило NAT в таблице используется, и трафик преобразован в соответствующий IP-адрес для Внешний интерфейс (192.0.2.100_nat). Теперь Внешние интерфейсы выключаются, или маршрут, отслеживающий сбои. Трафик все еще придерживается первого Выражения NAT и является NAT, Отклоненным к Внешнему интерфейсу, **НЕ** интерфейсу BackupISP. Это - поведение, известное, поскольку NAT Отклоняет. Трафик, предназначенный к 203.0.113.0/24, эффективно помещен в черный список.

Это поведение может наблюдаться с **пакетной** командой **трассировщика**. Обратите внимание **, что NAT Отклоняет** линию в фазе **неNAT**.

```
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
```

Эти правила NAT разработаны для переопределения таблицы маршрутизации. Существуют некоторые версии ASA, где отклонение не могло бы произойти, и это решение могло бы фактически работать, но с исправлением для идентификатора ошибки Cisco CSCul98420, эти правила (и нормальное поведение продвижение) определенно отклоняют пакет к первому настроенному исходящему интерфейсу. Пакет отброшен здесь, если интерфейс

выключается, или отслеживаемый маршрут удален.

Обходной путь

Так как присутствие правила NAT в конфигурации вынуждает трафик отклонить к неверному интерфейсу, строки настройки должен быть удален временно для обхождения проблемы. Можно ввести " никакая" форма определенной линии NAT, однако это ручное вмешательство могло бы занять время и и с простоем можно было стоять. Для ускорения процесса задача должна быть автоматизирована некоторой формой. Это может быть достигнуто с функцией EEM, представленной в Выпуске 9.2.1 ASA. Конфигурацию показывают здесь:

```
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
```

Эта задача работает, когда EEM усилен для принятия мер, если замечен системный журнал 622001. Когда установленный в стойку маршрут удален или добавил назад в таблицу маршрутизации, этот системный журнал генерируется. Учитывая маршрут, отслеживающий конфигурацию, показанную ранее, должен, Внешний интерфейс выключиться или цель дорожки становится больше не достижимым, этот системный журнал генерируется, и апплет EEM вызван. Важный аспект маршрут, отслеживающий конфигурацию, является **идентификатором event syslog 622001, происходит 2** строки настройки. Это заставляет апплет NAT2 происходить *любое* время, системный журнал генерируется.

Апплет NAT вызван каждый раз, когда системный журнал замечен. Эта комбинация приводит к линии NAT, удаляемой, когда идентификатор системного журнала 622001 увиден в первый раз (удаленный отслеживаемый маршрут), и затем линия NAT повторно добавлена во второй раз, когда системный журнал 62201 замечен (отслеживаемый маршрут был повторно добавлен к таблице маршрутизации). Это имеет эффект автоматического удаления и передобавления линии NAT в сочетании с характеристикой отслеживания маршрута.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show** . **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Моделируйте отказ соединения, который заставляет отслеживаемый маршрут быть удаленным из таблицы маршрутизации для завершения проверки.

Переведите ссылку основного поставщика услуг Интернет в нерабочее состояние

Сначала переведите основную (Внешнюю) ссылку в нерабочее состояние.

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

Интерфейс выключается

Заметьте, что Внешний интерфейс выключается, и объект отслеживания указывает, что достижимость не работает.

```
%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 инициирован

Системный журнал 622001 генерируется в результате удаления маршрута, и апплет EEM 'NAT' вызван. Выходные данные **Диспетчера событий показа** отражают статус и время выполнения отдельных апплетов.

```
%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
```

С EEM Удалено Первое Правило NAT

Проверка рабочей конфигурации показывает, что было удалено первое правило NAT.

```
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
```

Проверьте с пакетным трассировщиком

```
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
```

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.