ISP 이중화가 사용될 때 Twice NAT의 NAT 전환 동작을 제어하는 데 사용되는 EEM 컨피그레이션 예

목차

소개

이 문서에서는 듀얼 ISP 시나리오(ISP 이중화)에서 NAT(Network Address Translation) 전환 동작을 제어하기 위해 EEM(Embedded Event Manager) 애플릿을 사용하는 방법에 대해 설명합니다.

ASA(Adaptive Security Appliance) 방화벽을 통해 연결을 처리할 때 패킷 이그레스(egress) 인터페이스를 결정할 때 NAT 규칙이 라우팅 테이블보다 우선할 수 있음을 이해하는 것이 중요합니다.인바운드 패킷이 NAT 문의 변환된 IP 주소와 일치하는 경우 적절한 이그레스 인터페이스를 확인하기 위해 NAT 규칙이 사용됩니다.이를 "NAT 전환"이라고 합니다.

NAT Divert(NAT 전환) 확인(라우팅 테이블을 재정의할 수 있음)은 인터페이스에 도착하는 인바운드 패킷에 대해 목적지 주소 변환을 지정하는 NAT 규칙이 있는지 확인합니다.해당 패킷의 목적지 IP 주소를 변환하는 방법을 명시적으로 지정하는 규칙이 없으면 이그레스 인터페이스를 확인하기 위해 전역 라우팅 테이블이 참조됩니다.패킷의 목적지 IP 주소를 변환하는 방법을 명시적으로 지정하는 규칙이 있는 경우 NAT 규칙은 패킷을 변환의 다른 인터페이스로 "pull" 또는 "diverts"하며 전역 라우팅 테이블은 효과적으로 우회됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 릴리스 9.2.1을 실행하는 ASA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

3개의 인터페이스가 구성되었습니다.내부, 외부(기본 ISP) 및 BackupISP(보조 ISP) 이 두 NAT 문은 특정 서브넷(203.0.113.0/24)으로 이동할 때 두 인터페이스 중 하나에서 트래픽을 변환하도록 구성되었습니다.

```
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
```

경로 추적 구성

```
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
```

기본 링크가 다운되면 어떻게 됩니까?

Primary(Outside) 링크가 중단되기 전에 트래픽은 Outside(외부) 인터페이스에서 예상한 대로 이동합니다.테이블의 첫 번째 NAT 규칙이 사용되고 트래픽은 외부 인터페이스(192.0.2.100_nat)에 적합한 IP 주소로 변환됩니다. 이제 외부 인터페이스가 중단되거나 경로 추적이 실패합니다.트래픽은 여전히 첫 번째 NAT 문을 따르고 NAT는 BackupISP 인터페이스가 **아닌** 외부 인터페이스로 전환됩니다.이는 NAT Divert라고 하는 동작입니다.203.0.113.0/24으로 향하는 트래픽은 사실상 블랙홀입니다.

이 동작은 **packet tracer** 명령을 사용하여 확인할 수 있습니다.UN-NAT 단계에서 NAT 전환 **줄을** 확인합니다.

```
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
```

이러한 NAT 규칙은 라우팅 테이블을 재정의하도록 설계되었습니다.전환이 발생하지 않고 이 솔루션이 실제로 작동할 수 있는 일부 ASA 버전이 있지만, Cisco 버그 ID CSCul98420에 대한 수정(및 향후 예상되는 동작)이 패킷을 첫 번째 구성된 이그레스 인터페이스로 확실히 전환합니다.인터페이스가 중단되거나 추적된 경로가 제거되면 패킷이 여기에 삭제됩니다.

해결 방법

컨피그레이션에 NAT 규칙이 있으면 트래픽이 잘못된 인터페이스로 전환되므로 문제를 해결하려면 컨피그레이션 라인을 일시적으로 제거해야 합니다.특정 NAT 라인의 "no" 형식을 입력할 수 있지만, 이러한 수동 개입에 시간이 걸리고 중단이 발생할 수 있습니다.프로세스를 가속화하기 위해서는 어떤 방식으로든 작업을 자동화해야 합니다.이 작업은 ASA 릴리스 9.2.1에 도입된 EEM 기능을 사용하여 수행할 수 있습니다. 구성은 다음과 같습니다.

```
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
```

이 작업은 syslog 622001이 표시되면 EEM을 사용하여 작업을 수행할 때 작동합니다.이 syslog는 랙된 경로가 제거되거나 라우팅 테이블에 다시 추가될 때 생성됩니다.앞에서 설명한 경로 추적 컨피그레이션이 제공되면 외부 인터페이스가 다운되거나 추적 대상에 더 이상 연결할 수 없게 되면 이 syslog가 생성되고 EEM 애플릿이 호출됩니다.경로 추적 컨피그레이션의 중요한 측면은 **이벤트 syslog ID 622001이 2개의** 컨피그레이션 라인**에서 발생한다는 것입니다**.이로 인해 NAT2 애플릿은 syslog가 생성될 *때마다* 발생합니다.NAT 애플릿은 syslog가 표시될 때마다 호출됩니다.이 조합을 통해 syslog ID 622001이 처음 확인되면(추적 경로가 제거됨) NAT 라인이 제거되고 syslog 62201이 두 번째로 확인되면(추적 경로가 라우팅 테이블에 다시 추가됨) NAT 라인이 다시 추가됩니다. 이렇게 하면 경로 추적 기능과 함께 NAT 라인을 자동으로 제거하고 다시 추가할 수 있습니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령**을** 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

확인을 완료하기 위해 추적된 경로를 라우팅 테이블에서 제거하도록 하는 링크 실패를 시뮬레이션합니다.

기본 ISP 링크 해제

먼저 기본(외부) 링크를 끕니다.

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

인터페이스 다운

외부 인터페이스가 다운되고 추적 객체가 도달 범위가 다운되었음을 나타냅니다.

```
%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
```

EEM이 트리거됨

Syslog 622001은 경로 제거 결과로 생성되며 EEM 애플릿 'NAT'가 호출됩니다.**show event manager** 명령의 출력은 개별 애플릿의 상태 및 실행 시간을 반영합니다.

```
%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
```

EEM First NAT 규칙이 제거됨

실행 중인 컨피그레이션을 검사하면 첫 번째 NAT 규칙이 제거되었음을 보여줍니다.

```
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
```

패킷 추적기로 확인

```
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
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.