Vcs Expressway TelePresence 디바이스에 대해 Asa에서 NAT 반사 구성

목차

소개

이 문서에서는 방화벽에서 이러한 종류의 NAT 컨피그레이션이 필요한 특별한 Cisco TelePresence 시나리오에 대해 Cisco Adaptive Security Appliance에서 NAT(Network Address Translation) 반사 컨피그레이션을 구현하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA(Adaptive Security Appliance) 기본 NAT 구성
- Cisco TelePresence VCS(Video Communication Server) Control 및 VCS Expressway 기본 구성

참고: 이 문서는 서로 다른 DMZ에 있는 두 NIC 인터페이스가 모두 포함된 VCS-Expressway 또는 Expressway-Edge의 권장 구축 방법을 사용할 수 없는 경우에만 사용됩니다. 듀얼 NIC를 사용하는 권장 구축에 대한 자세한 내용은 60페이지의 Cisco TelePresence Video Communication Server Basic Configuration(Control with Expressway) 구축 설명서 링크를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.3 이상을 실행하는 Cisco ASA 5500 및 5500-X Series 어플라이언스.
- Cisco VCS 버전 X8.x 이상

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.

참고: 전체 문서에서 VCS 장치는 VCS Expressway 및 VCS 컨트롤이라고 합니다. 그러나 Expressway-E 및 Expressway-C 디바이스에도 동일한 컨피그레이션이 적용됩니다.

배경 정보

Cisco TelePresence 설명서에 따르면, VCS Control이 VCS Expressway 공용 IP 주소를 통해 VCS Expressway와 통신할 수 있도록 하려면 FW에 NAT 반사 컨피그레이션이 필요한 두 가지 유형의 텔레프레즌스 시나리오가 있습니다.

첫 번째 시나리오는 단일 VCS Expressway LAN 인터페이스를 사용하는 단일 서브넷 DMZ(De-Militarized Zone)이며 두 번째 시나리오는 단일 VCS Expressway LAN 인터페이스를 사용하는 3포트 FW DMZ입니다.

팁: TelePresence 구현에 대한 자세한 내용은 Cisco TelePresence Video Communication Server Basic Configuration(Control with Expressway) 구축 설명서를 참조하십시오.

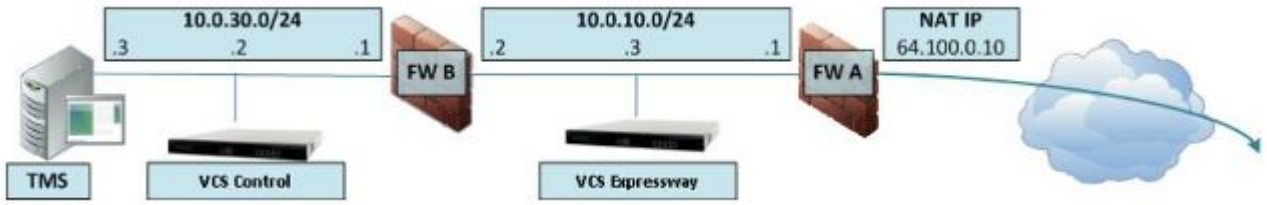
VCS C 및 E 구현에 대해 Cisco 토폴로지가 권장되지 않음

다음 토폴로지는 Cisco에서 권장하지 않습니다. VCS Expressway 또는 Expressway 에지에 권장되는 구축 방법론은 Expressway가 각 DMZ에 NIC가 있는 서로 다른 두 DMZ를 사용하는 것입니다. 이 설명서는 권장 구축 방법을 사용할 수 없는 환경에서 사용하기 위한 것입니다.

단일 VCS Expressway LAN 인터페이스가 포함된 단일 서브넷 DMZ

이 시나리오에서 FW A는 트래픽을 FW B로 라우팅할 수 있으며 그 반대의 경우도 가능합니다. VCS Expressway를 사용하면 외부에서 내부 인터페이스로 이동하는 FW B의 트래픽 흐름이 감소하지 않고 비디오 트래픽이 FW B를 통과할 수 있습니다. VCS Expressway는 또한 퍼블릭 측에서 FW 통과를 처리합니다.

이 시나리오의 예는 다음과 같습니다.



이 구축에서는 다음 구성 요소를 사용합니다.

- 다음을 포함하는 단일 서브넷 DMZ(10.0.10.0/24):
  - FW A의 내부 인터페이스(10.0.10.1)
  - FW B의 외부 인터페이스(10.0.10.2)
  - VCS Expressway(10.0.10.3)의 LAN1 인터페이스
- 다음을 포함하는 LAN 서브넷(10.0.30.0/24):
  - FW B의 내부 인터페이스(10.0.30.1)
  - VCS 컨트롤의 LAN1 인터페이스(10.0.30.2)
  - Cisco TelePresence Management Server(TMS)의 네트워크 인터페이스(10.0.30.3)

고정 일대일 NAT는 VCS Expressway의 LAN1 IP 주소에 대한 공용 주소 64.100.0.10에 대해 NAT를 수행하는 FW A에서 구성되었습니다. 고정 NAT IP 주소가 64.100.0.10인 VCS Expressway의 LAN1 인터페이스에 대해 고정 NAT 모드가 활성화되었습니다.

참고: 네트워크 외부에서 VCS Control 보안 접근 클라이언트 영역(피어 주소)에 표시되는 방식으로 VCS Expressway의 FQDN(Fully Qualified Domain Name)을 입력해야 합니다. 그 이유는 고정 NAT 모드에서 VCS Expressway는 인바운드 신호 및 미디어 트래픽이 개인 이름이 아닌 외부 FQDN으로 전송되도록 요청하기 때문입니다. 이는 외부 FW가 VCS 컨트롤에서 VCS Expressway 외부 FQDN으로의 트래픽을 허용해야 함을 의미합니다. 이를 NAT 반사라고 하며, 모든 유형의 FW에서 지원되지 않을 수도 있습니다.

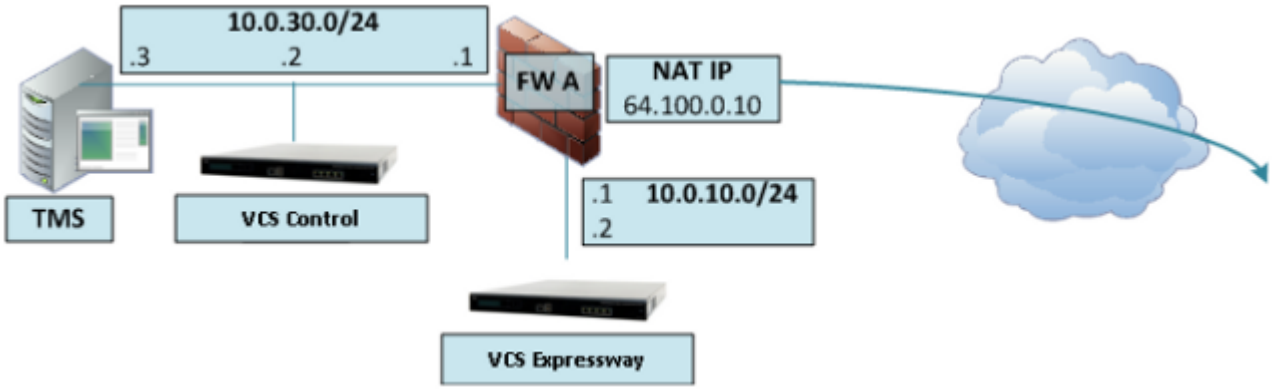
이 예에서 FW B는 VCS Expressway의 외부 IP 주소(64.100.0.10)를 대상으로 하는 VCS 컨트롤에서 오는 트래픽의 NAT 반영을 허용해야 합니다. VCS 컨트롤의 접근 영역은 피어 주소로 64.100.0.10을 가져야 합니다(FQDN에서 IP로 변환 후).

VCS Expressway는 10.0.1.1의 기본 게이트웨이로 구성해야 합니다. 이 시나리오에서 고정 경로가 필요한지 여부는 FW A 및 FW B의 기능 및 설정에 따라 달라집니다. VCS 컨트롤에서 VCS Expressway로의 통신은 VCS Expressway의 64.100.0.10 IP 주소를 통해 발생합니다. VCS Expressway에서 VCS Control로의 반환 트래픽은 기본 게이트웨이를 통과해야 할 수 있습니다.

Cisco TMS 관리 통신은 VCS Expressway의 고정 NAT 모드 설정의 영향을 받지 않으므로 IP 주소가 10.0.10.3인 경우(또는 FW B에서 허용하는 경우 IP 주소가 64.100.0.10인 경우) VCS Expressway를 Cisco TMS에 추가할 수 있습니다.

단일 VCS Expressway LAN 인터페이스가 포함된 3포트 FW DMZ

이 시나리오의 예는 다음과 같습니다.



이 구축에서는 3포트 FW를 사용하여 다음을 생성합니다.

- 다음을 포함하는 DMZ 서브넷(10.0.10.0/24):
  - FW A(10.0.10.1)의 DMZ 인터페이스
  - VCS Expressway(10.0.10.2)의 LAN1 인터페이스
- 다음을 포함하는 LAN 서브넷(10.0.30.0/24):
  - FW A(10.0.30.1)의 LAN 인터페이스
  - VCS 컨트롤의 LAN1 인터페이스(10.0.30.2)
  - Cisco TMS의 네트워크 인터페이스(10.0.30.3)

고정 일대일 NAT는 VCS Expressway의 LAN1 IP 주소에 대해 공용 IP 주소 64.100.0.10의 NAT를 수행하는 FW A에서 구성되었습니다. 고정 NAT IP 주소가 64.100.0.10인 VCS Expressway의 LAN1 인터페이스에 대해 고정 NAT 모드가 활성화되었습니다.

VCS Expressway는 10.0.10.1의 기본 게이트웨이로 구성해야 합니다. 이 게이트웨이는 VCS Expressway를 떠나는 모든 트래픽에 사용되어야 하므로 이 유형의 배포에서는 정적 경로가 필요하지 않습니다.

이전 시나리오에서 설명한 것과 같은 이유로 VCS Control의 접근 클라이언트 영역은 VCS Expressway의 고정 NAT 주소(이 예에서는 64.100.0.10)와 일치하는 피어 주소로 구성해야 합니다.

참고: 즉, FW A는 대상 IP 주소가 64.100.0.10인 VCS 컨트롤에서 오는 트래픽을 허용해야 합니다. 이를 NAT 반영이라고도 하며, 모든 유형의 FW에서 이를 지원하지 않는다는 점에 유의해야 합니다.

Cisco TMS 관리 통신은 VCS Expressway의 고정 NAT 모드 설정에 영향을 받지 않으므로 IP 주소가 10.0.10.2(또는 FW A에서 허용하는 경우 IP 주소가 64.10.0.10)인 Cisco TMS에 VCS Expressway를 추가할 수 있습니다.

구성

이 섹션에서는 두 가지 다른 VCS C 및 E 구현 시나리오에 대해 ASA에서 NAT 반사를 구성하는 방법에 대해 설명합니다.

단일 VCS Expressway LAN 인터페이스가 포함된 단일 서브넷 DMZ

첫 번째 시나리오의 경우 VCS Expressway의 외부 IP 주소(64.100.0.10)로 전달되는 VCS 컨트롤(10.0.30.2)에서 통신을 허용하려면 FW A에 이 NAT 반사 컨피그레이션을 적용해야 합니다.

이 예에서 VCS Control IP 주소는 10.0.30.2/24이고 VCS Expressway IP 주소는 10.0.10.3/24입니다.

대상 IP 주소가 64.100.0.10인 VCS Expressway를 찾을 때 VCS 제어 IP 주소 10.0.30.2가 FW B의 내부 인터페이스에서 외부 인터페이스로 이동할 때 유지된다고 가정할 경우, FW B에서 구현해야 하는 NAT 반사 컨피그레이션이 다음 예에 표시됩니다.

ASA 버전 8.3 이상의 예:

```
object network obj-10.0.30.2
 host 10.0.30.2

object network obj-10.0.10.3
 host 10.0.10.3

object network obj-64.100.0.10
 host 64.100.0.10

nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination static
 obj-64.100.0.10 obj-10.0.10.3

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.
```

ASA 버전 8.2 이하의 예:

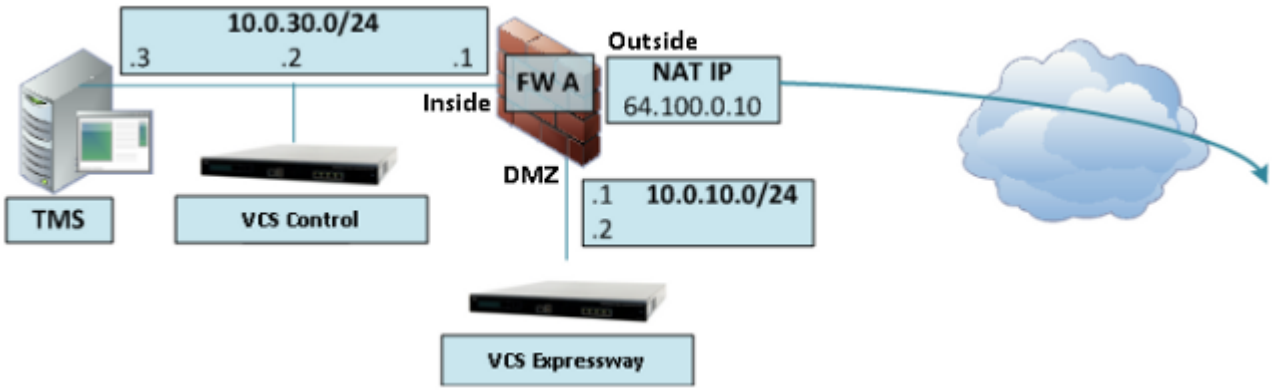
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
```

```
access-list OUT-IN-INTERFACE extended permit ip host 10.0.10.3 host 10.0.30.2
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
```

참고: 이 NAT 리플렉션 컨피그레이션의 주요 목적은 VCS Control에서 VCS Expressway에 연결할 수 있도록 허용하는 것이지만 전용 IP 주소 대신 VCS Expressway 공용 IP 주소를 사용하는 것입니다. VCS Control의 소스 IP 주소가 방금 표시된 권장 NAT 컨피그레이션 대신 Twice NAT 컨피그레이션으로 이 NAT 변환 중에 변경되어 VCS Expressway에서 자체 공용 IP 주소의 트래픽이 표시되는 경우 MRA 디바이스에 대한 전화 서비스가 표시되지 않습니다. 이는 아래의 권장 사항 섹션의 섹션 3에 따라 지원되는 구축이 아닙니다.

단일 VCS Expressway LAN 인터페이스가 포함된 3포트 FW DMZ

두 번째 시나리오에서는 VCS Expressway의 외부 IP 주소(64.100.0.10)로 향하는 VCS Control 10.0.30.2의 인바운드 트래픽에 대한 NAT 반사를 허용하려면 FW A에서 이 NAT 반사 컨피그레이션을 적용해야 합니다.



이 예에서 VCS Control IP 주소는 10.0.30.2/24이고 VCS Expressway IP 주소는 10.0.10.2/24입니다.

대상 IP 주소가 64.100.0.10인 VCS Expressway를 찾을 때 VCS 제어 IP 주소 10.0.30.2가 내부에서 FW A의 DMZ 인터페이스로 이동할 때 유지된다고 가정할 경우 FW A에서 구현해야 하는 NAT 반사 컨피그레이션이 다음 예에 표시됩니다.

ASA 버전 8.3 이상의 예:

```
object network obj-10.0.30.2
 host 10.0.30.2

object network obj-10.0.10.2
 host 10.0.10.2

object network obj-64.100.0.10
 host 64.100.0.10

nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination static
 obj-64.100.0.10 obj-10.0.10.2
```

```
NOTE: After this NAT is applied you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the DMZ interface is being redirected.
WARNING: Users may not be able to access any service enabled on the DMZ interface.
```

ASA 버전 8.2 이하의 예:

```
access-list IN-DMZ-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,DMZ) 10.0.30.2 access-list IN-DMZ-INTERFACE

access-list DMZ-IN-INTERFACE extended permit ip host 10.0.10.2 host 10.0.30.2
static (DMZ,inside) 64.100.0.10 access-list DMZ-IN-INTERFACE
```

참고: 이 NAT 리플렉션 컨피그레이션의 주요 목적은 VCS Control에서 VCS Expressway에 연결할 수 있도록 허용하는 것이지만 전용 IP 주소 대신 VCS Expressway 공용 IP 주소를 사용하도록 허용하는 것입니다. VCS 컨트롤의 소스 IP 주소가 방금 표시된 권장 NAT 컨피그레이션 대신 Twice NAT 컨피그레이션으로 이 NAT 변환 중에 변경되어 VCS Expressway에서 자체 공용 IP 주소의 트래픽을 확인하는 경우 MRA 디바이스에 대한 전화 서비스가 표시되지 않습니다. 이는 아래 권장 사항 섹션의 섹션 3에 따라 지원되는 구축이 아닙니다.

다음을 확인합니다.

이 섹션에서는 VCS C 및 E 구현 시나리오 모두에서 필요에 따라 NAT 반사 컨피그레이션이 작동하는지 확인하기 위해 ASA에서 볼 수 있는 패킷 추적기 출력을 제공합니다.

단일 VCS Expressway LAN 인터페이스가 포함된 단일 서브넷 DMZ

다음은 ASA 버전 8.3 이상에 대한 FW B 패킷 추적기 출력입니다.

```
<#root>

FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80


Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
 static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/80 to 10.0.10.3/80

Phase: 2
Type: IP-OPTIONS
```

```
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
 static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
 static obj-64.100.0.10 obj-10.0.10.3
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 2, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

다음은 ASA 버전 8.2 이하의 FW B 패킷 추적기 출력입니다.

<#root>

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80
```

```
Phase: 1
Type: UN-NAT
Subtype: static
```

```
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
 match ip outside host 10.0.10.3 inside host 10.0.30.2
 static translation to 64.100.0.10
 translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/0 to 10.0.10.3/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
 match ip inside host 10.0.30.2 outside host 64.100.0.10
 static translation to 10.0.30.2
 translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
 match ip inside host 10.0.30.2 outside host 64.100.0.10
 static translation to 10.0.30.2
 translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
 match ip outside host 10.0.10.3 inside host 10.0.30.2
 static translation to 64.100.0.10
 translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
 match ip outside host 10.0.10.3 inside host 10.0.30.2
 static translation to 64.100.0.10
 translate_hits = 0, untranslate_hits = 2
Additional Information:
```

```
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1166, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

단일 VCS Expressway LAN 인터페이스가 포함된 3포트 FW DMZ

다음은 ASA 버전 8.3 이상에 대한 FW A 패킷 추적기 출력입니다.

<#root>

FW-A#

packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
 static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/80 to 10.0.10.2/80

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
```

```
Subtype:
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
 static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
 static obj-64.100.0.10 obj-10.0.10.2
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: DMZ
output-status: up
output-line-status: up
Action: allow
```

다음은 ASA 버전 8.2 이하의 FW A 패킷 추적기 출력입니다.

<#root>

FW-A#

packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
```

```
 match ip DMZ host 10.0.10.2 inside host 10.0.30.2
 static translation to 64.100.0.10
 translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/0 to 10.0.10.2/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
 match ip inside host 10.0.30.2 DMZ host 64.100.0.10
 static translation to 10.0.30.2
 translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
 match ip inside host 10.0.30.2 DMZ host 64.100.0.10
 static translation to 10.0.30.2
 translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
 match ip DMZ host 10.0.10.2 inside host 10.0.30.2
 static translation to 64.100.0.10
 translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
 match ip DMZ host 10.0.10.2 inside host 10.0.30.2
 static translation to 64.100.0.10
 translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1166, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: DMZ
output-status: up
output-line-status: up
Action: allow
```

문제 해결

패킷이 관련된 FW 인터페이스로 들어오고 나갈 때 NAT 변환을 확인하기 위해 ASA 인터페이스에서 패킷 캡처를 구성할 수 있습니다.

"3-Port FW DMZ with Single VCS Expressway LAN Interface" 시나리오에 적용되는 패킷 캡처

<#root>

```
FW-A#

sh cap

capture capin type raw-data interface inside [Capturing - 5735 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capdmz type raw-data interface DMZ [Capturing - 5735 bytes]
  match ip host 10.0.10.2 host 10.0.30.2
FW-A# sh cap capin

71 packets captured
   1: 22:21:37.095270 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:21:37.100672 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101313 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:21:37.114373 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157371 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:21:37.174429 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234164 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:21:39.238528 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261110 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:21:39.270234 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170614 10.0.30.2.38953 > 64.100.0.10.23: S 1841210281:1841210281(0)
win 4128 <mss 536>
  12: 22:21:47.198933 64.100.0.10.23 > 10.0.30.2.38953: S 3354834096:3354834096(0)
ack 1841210282 win 4128 <mss 536>
  13: 22:21:47.235186 10.0.30.2.38953 > 64.100.0.10.23: . ack 3354834097
```

```
win 4128
  14: 22:21:47.242815 64.100.0.10.23 > 10.0.30.2.38953: P 3354834097:3354834109(12)
ack 1841210282 win 4128
  15: 22:21:47.243014 10.0.30.2.38953 > 64.100.0.10.23: P 1841210282:1841210294(12)
ack 3354834097 win 4128
  16: 22:21:47.243258 10.0.30.2.38953 > 64.100.0.10.23: . ack 3354834097
win 4128
  17: 22:21:47.261094 64.100.0.10.23 > 10.0.30.2.38953: P 3354834109:3354834151(42)
ack 1841210282 win 4128
  18: 22:21:47.280411 64.100.0.10.23 > 10.0.30.2.38953: P 3354834151:3354834154(3)
ack 1841210294 win 4116
  19: 22:21:47.280625 64.100.0.10.23 > 10.0.30.2.38953: P 3354834154:3354834157(3)
ack 1841210294 win 4116
  20: 22:21:47.280838 64.100.0.10.23 > 10.0.30.2.38953: P 3354834157:3354834163(6)
ack 1841210294 win 4116
  21: 22:21:47.281082 10.0.30.2.38953 > 64.100.0.10.23: P 1841210294:1841210297(3)
ack 3354834109 win 4116
  22: 22:21:47.281296 10.0.30.2.38953 > 64.100.0.10.23: P 1841210297:1841210300(3)
ack 3354834109 win 4116

FW-A#
```

sh cap capdmz

```
71 packets captured
   1: 22:21:37.095621 10.0.30.2 > 10.0.10.2: icmp: echo request
   2: 22:21:37.100626 10.0.10.2 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101343 10.0.30.2 > 10.0.10.2: icmp: echo request
   4: 22:21:37.114297 10.0.10.2 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157920 10.0.30.2 > 10.0.10.2: icmp: echo request
   6: 22:21:37.174353 10.0.10.2 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234713 10.0.30.2 > 10.0.10.2: icmp: echo request
   8: 22:21:39.238452 10.0.10.2 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261659 10.0.30.2 > 10.0.10.2: icmp: echo request
  10: 22:21:39.270158 10.0.10.2 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170950 10.0.30.2.38953 > 10.0.10.2.23: S 2196345248:2196345248(0)
win 4128 <mss 536>
  12: 22:21:47.198903 10.0.10.2.23 > 10.0.30.2.38953: S 1814294604:1814294604(0)
ack 2196345249 win 4128 <mss 536>
  13: 22:21:47.235263 10.0.30.2.38953 > 10.0.10.2.23: . ack 1814294605 win 4128
  14: 22:21:47.242754 10.0.10.2.23 > 10.0.30.2.38953: P 1814294605:1814294617(12)
ack 2196345249 win 4128
  15: 22:21:47.243105 10.0.30.2.38953 > 10.0.10.2.23: P 2196345249:2196345261(12)
ack 1814294605 win 4128
  16: 22:21:47.243319 10.0.30.2.38953 > 10.0.10.2.23: . ack 1814294605 win 4128
  17: 22:21:47.260988 10.0.10.2.23 > 10.0.30.2.38953: P 1814294617:1814294659(42)
ack 2196345249 win 4128
  18: 22:21:47.280335 10.0.10.2.23 > 10.0.30.2.38953: P 1814294659:1814294662(3)
ack 2196345261 win 4116
  19: 22:21:47.280564 10.0.10.2.23 > 10.0.30.2.38953: P 1814294662:1814294665(3)
ack 2196345261 win 4116
  20: 22:21:47.280777 10.0.10.2.23 > 10.0.30.2.38953: P 1814294665:1814294671(6)
ack 2196345261 win 4116
  21: 22:21:47.281143 10.0.30.2.38953 > 10.0.10.2.23: P 2196345261:2196345264(3)
ack 1814294617 win 4116
  22: 22:21:47.281357 10.0.30.2.38953 > 10.0.10.2.23: P 2196345264:2196345267(3)
ack 1814294617 win 4116
```

"단일 VCS Expressway LAN 인터페이스가 있는 단일 서브넷 DMZ" 시나리오에 적용되는 패킷 캡처

<#root>

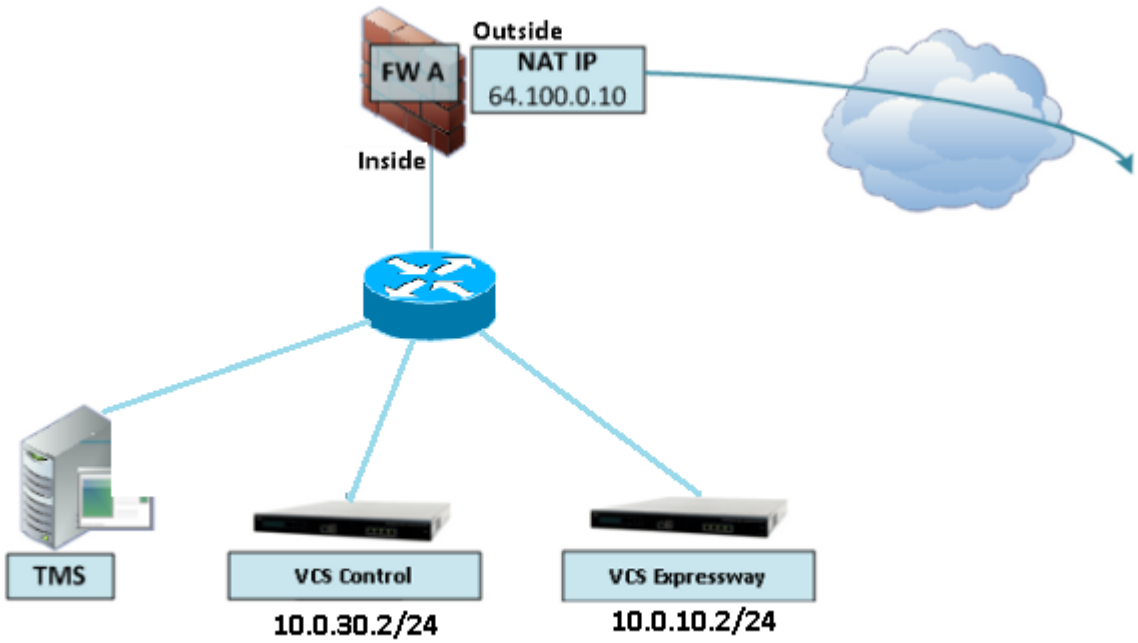
```
FW-B#

sh cap

capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2

FW-B#

sh cap capin


72 packets captured
   1: 22:30:06.783681 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:30:06.847856 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.877624 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:30:06.900710 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.971598 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:30:06.999551 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.075649 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:30:07.134499 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156409 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:30:07.177496 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.802525 10.0.30.2.41596 > 64.100.0.10.23: S 1119515693:1119515693(0)
win 4128 <mss 536>
  12: 22:30:13.861100 64.100.0.10.23 > 10.0.30.2.41596: S 2006020203:2006020203(0)
ack 1119515694 win 4128 <mss 536>
  13: 22:30:13.935864 10.0.30.2.41596 > 64.100.0.10.23: . ack 2006020204 win 4128
  14: 22:30:13.946804 10.0.30.2.41596 > 64.100.0.10.23: P 1119515694:1119515706(12)
ack 2006020204 win 4128
  15: 22:30:13.952679 10.0.30.2.41596 > 64.100.0.10.23: . ack 2006020204 win 4128
  16: 22:30:14.013686 64.100.0.10.23 > 10.0.30.2.41596: P 2006020204:2006020216(12)
ack 1119515706 win 4116
  17: 22:30:14.035352 64.100.0.10.23 > 10.0.30.2.41596: P 2006020216:2006020256(40)
ack 1119515706 win 4116
  18: 22:30:14.045758 64.100.0.10.23 > 10.0.30.2.41596: P 2006020256:2006020259(3)
ack 1119515706 win 4116
  19: 22:30:14.046781 64.100.0.10.23 > 10.0.30.2.41596: P 2006020259:2006020262(3)
ack 1119515706 win 4116
  20: 22:30:14.047788 64.100.0.10.23 > 10.0.30.2.41596: P 2006020262:2006020268(6)
ack 1119515706 win 4116
  21: 22:30:14.052151 10.0.30.2.41596 > 64.100.0.10.23: P 1119515706:1119515709(3)
ack 2006020256 win 4076
  22: 22:30:14.089183 10.0.30.2.41596 > 64.100.0.10.23: P 1119515709:1119515712(3)
ack 2006020256 win 4076


ASA1#

show cap capout


72 packets captured
   1: 22:30:06.784871 10.0.30.2 > 10.0.10.3: icmp: echo request
```

```
   2: 22:30:06.847688 10.0.10.3 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.878769 10.0.30.2 > 10.0.10.3: icmp: echo request
   4: 22:30:06.900557 10.0.10.3 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.972758 10.0.30.2 > 10.0.10.3: icmp: echo request
   6: 22:30:06.999399 10.0.10.3 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.076808 10.0.30.2 > 10.0.10.3: icmp: echo request
   8: 22:30:07.134422 10.0.10.3 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156959 10.0.30.2 > 10.0.10.3: icmp: echo request
  10: 22:30:07.177420 10.0.10.3 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.803104 10.0.30.2.41596 > 10.0.10.3.23: S 2599614130:2599614130(0)
win 4128 <mss 536>
  12: 22:30:13.860947 10.0.10.3.23 > 10.0.30.2.41596: S 4158597009:4158597009(0)
ack 2599614131 win 4128 <mss 536>
  13: 22:30:13.936017 10.0.30.2.41596 > 10.0.10.3.23: . ack 4158597010 win 4128
  14: 22:30:13.946941 10.0.30.2.41596 > 10.0.10.3.23: P 2599614131:2599614143(12)
ack 4158597010 win 4128
  15: 22:30:13.952801 10.0.30.2.41596 > 10.0.10.3.23: . ack 4158597010 win 4128
  16: 22:30:14.013488 10.0.10.3.23 > 10.0.30.2.41596: P 4158597010:4158597022(12)
ack 2599614143 win 4116
  17: 22:30:14.035108 10.0.10.3.23 > 10.0.30.2.41596: P 4158597022:4158597062(40)
ack 2599614143 win 4116
  18: 22:30:14.045377 10.0.10.3.23 > 10.0.30.2.41596: P 4158597062:4158597065(3)
ack 2599614143 win 4116
  19: 22:30:14.046384 10.0.10.3.23 > 10.0.30.2.41596: P 4158597065:4158597068(3)
ack 2599614143 win 4116
  20: 22:30:14.047406 10.0.10.3.23 > 10.0.30.2.41596: P 4158597068:4158597074(6)
ack 2599614143 win 4116
  21: 22:30:14.052395 10.0.30.2.41596 > 10.0.10.3.23: P 2599614143:2599614146(3)
ack 4158597062 win 4076
  22: 22:30:14.089427 10.0.30.2.41596 > 10.0.10.3.23: P 2599614146:2599614149(3)
ack 4158597062 win 4076
```

권장 사항

1. 지원되지 않는 토폴로지는 구현하지 마십시오

예를 들어, 이 시나리오에서와 같이 VCS Control 및 VCS Expressway가 모두 내부 ASA 인터페이스 뒤에 연결되어 있는 경우



이러한 종류의 구현에서는 NAT 반사를 위한 비대칭 경로 문제를 방지하기 위해 반환 트래픽이 ASA로 다시 돌아가도록 강제하려면 VCS 제어 IP 주소를 ASA의 내부 IP 주소로 변환해야 합니다.

참고: VCS 컨트롤의 소스 IP 주소가 제안된 NAT 리플렉션 구성 대신 Twice NAT 컨피그레이션으로 이 NAT 변환 중에 변경되는 경우 VCS Expressway에서 자체 공용 IP 주소의 트래픽을 볼 수 있으며, MRA 디바이스에 대한 전화 서비스가 표시되지 않습니다. 이는 아래 권장 사항 섹션의 섹션 3에 따라 지원되는 구축이 아닙니다.

즉, NAT가 반영되는 단일 NIC 대신 VCS Expressway를 Expressway-E 듀얼 네트워크 인터페이스 구현으로 구현하는 것이 좋습니다.

2. 관련된 방화벽에서 SIP/H.323 검사가 완전히 비활성화되었는지 확인합니다.

Expressway-E를 오가는 네트워크 트래픽을 처리하는 방화벽에서 SIP 및 H.323 검사를 비활성화하는 것이 좋습니다. 활성화된 경우 SIP/H.323 검사는 Expressway에 내장된 방화벽/NAT 접근 기능에 부정적인 영향을 주는 것으로 자주 확인됩니다.

ASA에서 SIP 및 H.323 검사를 비활성화하는 방법의 예입니다.

```
policy-map global_policy
 class inspection_default
  no inspect h323 h225
  no inspect h323 ras
  no inspect sip
```

3. 실제 Expressway 구현이 Cisco telepresence 개발자가 제안하는 다음 요구 사항을 준수하는지 확인합니다

- Expressway-C와 Expressway-E 간의 NAT 컨피그레이션은 지원되지 않습니다.
- Expressway-C 및 Expressway-E가 동일한 공용 IP 주소에 NATed를 가져오는 경우에는 지원되지 않습니다. 예를 들면 다음과 같습니다.
  Expressway-C는 IP 주소 10.1.1.1로 구성됩니다.
  Expressway-E에는 IP 주소 10.2.2.1로 구성된 단일 NIC가 있으며 방화벽에는 공용 IP 주소 64.100.0.10으로 고정 NAT가 구성되어 있습니다
  그러면 Expressway-C를 동일한 공용 주소 64.100.0.10으로 NAT할 수 없습니다

권장 VCS Expressway 구현

NAT 반사 컨피그레이션을 사용하는 VCS Expressway 대신 VCS Expressway를 구현하는 것은 듀얼 네트워크 인터페이스/듀얼 NIC VCS Expressway 구현입니다. 자세한 내용은 다음 링크를 확인하십시오.

Expressway-E 듀얼 네트워크 인터페이스 구현을 위한 ASA NAT 컨피그레이션 및 권장 사항.

관련 정보

- Expressway-E 듀얼 네트워크 인터페이스 구현을 위한 ASA NAT 컨피그레이션 및 권장 사항
- Cisco TelePresence Video Communication Server 기본 구성(Expressway를 통한 제어) 구축 설명서
- 방화벽 통과를 위한 Cisco Expressway IP 포트 사용
- Cisco VCS Expressway를 공용 인터넷이 아닌 DMZ에 배치

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.