Configure a reflexão de NAT no ASA para os dispositivos de telepresença do VCS Expressway

Contents

Introduction

Este documento descreve como implementar uma configuração de reflexão NAT (Network Address Translation) nos Cisco Adaptive Security Appliances para cenários especiais do Cisco TelePresence que exigem esse tipo de configuração NAT no Firewall.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de NAT básica do Cisco ASA (Adaptive Security Appliance).
- Configuração básica do Cisco TelePresence Video Communication Server (VCS) Control e VCS Expressway.

> **Note**: Este documento deve ser usado somente quando o método de implantação recomendado de um VCS-Expressway ou Expressway-Edge com ambas as interfaces NIC em DMZ diferentes não pode ser usado. Para obter mais informações sobre a implantação recomendada usando NICs duplas, consulte o link a seguir na página 60: Guia de implantação do Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Dispositivos Cisco ASA 5500 e 5500-X Series que executam o software versão 8.3 e posterior.
- Cisco VCS versão X8.x e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Observação**: por meio de todo o documento, os dispositivos VCS são chamados de VCS Expressway e VCS Control. No entanto, a mesma configuração se aplica aos dispositivos Expressway-E e Expressway-C.

Informações de Apoio

De acordo com a documentação do Cisco TelePresence, há dois tipos de cenários de TelePresence em que a configuração de reflexão do NAT é necessária nos FWs para permitir que o controle do VCS se comunique com o VCS Expressway através do endereço IP público do VCS Expressway.

O primeiro cenário envolve uma única zona desmilitarizada de sub-rede (DMZ) que usa uma única interface de LAN do VCS Expressway, e o segundo cenário envolve uma DMZ FW de 3 portas que usa uma única interface de LAN do VCS Expressway.

> **Tip**: Para obter mais detalhes sobre a implementação da TelePresence, consulte o guia de implantação Cisco TelePresence Video Communication Server Basic Configuration (Controle com Expressway).

Topologias da Cisco não recomendadas para a implementação do VCS C e E

Éimportante observar que as seguintes topologias NÃO são recomendadas pela Cisco. A

metodologia de implantação recomendada para um VCS Expressway ou Expressway edge é usar dois DMZs diferentes com o Expressway tendo uma placa de rede em cada DMZ. Este guia deve ser usado em ambientes onde o método de implantação recomendado não pode ser usado.

DMZ de sub-rede única com interface única de LAN VCS Expressway

Nesse cenário, o FW A pode rotear o tráfego para o FW B (e vice-versa). O VCS Expressway permite que o tráfego de vídeo passe através do FW B sem uma redução no fluxo de tráfego no FW B do exterior para as interfaces internas. O VCS Expressway também lida com a passagem do FW em seu lado público.

Aqui está um exemplo deste cenário:

Esta implantação usa estes componentes:

- Uma única DMZ de sub-rede (10.0.10.0/24) que contém:
  A interface interna do FW A (10.0.10.1)A interface externa do FW B (10.0.10.2)A interface LAN1 do VCS Expressway (10.0.10.3)
- Uma sub-rede de LAN (10.0.30.0/24) que contém:
  A interface interna do FW B (10.0.30.1)A interface LAN1 do VCS Control (10.0.30.2)A interface de rede do Cisco TelePresence Management Server (TMS) (10.0.30.3)

Um NAT estático de um para um foi configurado no FW A, que executa o NAT para o endereço público 64.100.0.10 para o endereço IP LAN1 do VCS Expressway. O modo NAT estático foi ativado para a interface LAN1 no VCS Expressway, com um endereço IP NAT estático de 64.100.0.10.

> **Note**: Você deve inserir o Nome de domínio totalmente qualificado (FQDN) do VCS Expressway na zona de cliente de passagem segura (endereço de peer) do controle VCS como se ele fosse visto de fora da rede. A razão para isso é que no modo NAT estático, o VCS Expressway solicita que a sinalização de entrada e o tráfego de mídia sejam enviados para seu FQDN externo em vez de seu nome privado. Isso também significa que o FW externo deve permitir o tráfego do VCS Control para o FQDN externo do VCS Expressway. Isso é conhecido como reflexão de NAT e pode não ser suportado por todos os tipos de FWs.

Neste exemplo, o FW B deve permitir a reflexão de NAT do tráfego que vem do Controle de VCS que é destinado ao endereço IP externo (64.100.0.10) do VCS Expressway. A zona de passagem no VCS Control deve ter 64.100.0.10 como o endereço de peer (após conversão de FQDN em IP).

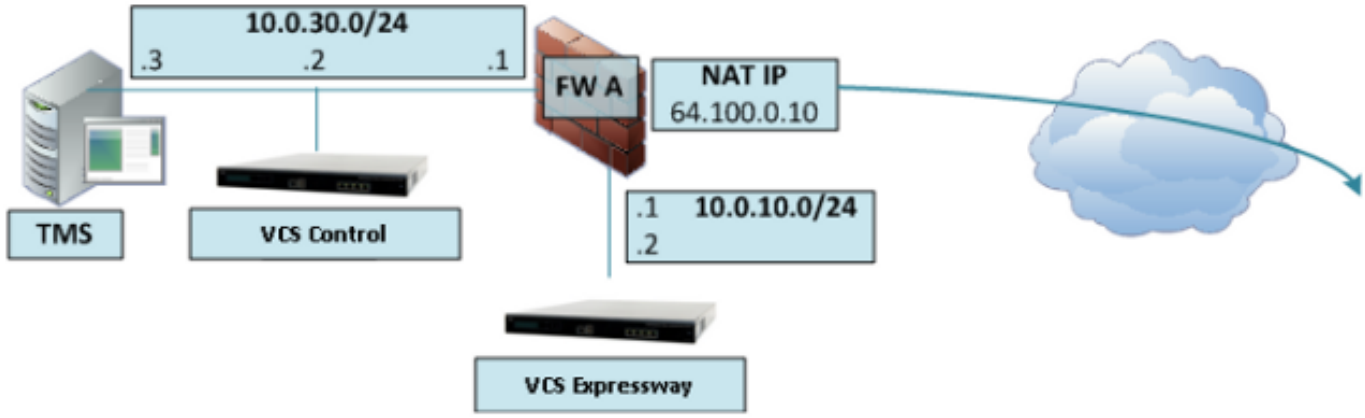
O VCS Expressway deve ser configurado com um gateway padrão de **10.0.10.1**. Se as rotas estáticas são necessárias neste cenário depende dos recursos e das configurações do FW A e do FW B. A comunicação do VCS Control com o VCS Expressway ocorre por meio do endereço IP

64.100.0.10 do VCS Expressway; e o tráfego de retorno do VCS Expressway para o controle VCS pode ter que passar pelo gateway padrão.

O VCS Expressway pode ser adicionado ao Cisco TMS com o endereço IP 10.0.10.3 (ou com o endereço IP 64.100.0.10, se o FW B permitir isso), já que a comunicação de gerenciamento do Cisco TMS não é afetada pelas configurações do modo NAT estático no VCS Expressway.

3 portas FW DMZ com interface única de LAN VCS Expressway

Aqui está um exemplo deste cenário:



Nesta implantação, um FW de 3 portas é usado para criar:

- Uma sub-rede DMZ (10.0.10.0/24) que contém:
  A interface DMZ do FW A (10.0.10.1)A interface LAN1 do VCS Expressway (10.0.10.2)
- Uma sub-rede de LAN (10.0.30.0/24) que contém:
  A interface LAN do FW A (10.0.30.1)A interface LAN1 do VCS Control (10.0.30.2)A interface de rede do Cisco TMS (10.0.30.3)

Um NAT estático de um para um foi configurado no FW A, que executa o NAT do endereço IP público 64.100.0.10 para o endereço IP LAN1 do VCS Expressway. O modo NAT estático foi ativado para a interface LAN1 no VCS Expressway, com um endereço IP NAT estático de 64.100.0.10.

O VCS Expressway deve ser configurado com um gateway padrão de 10.0.10.1. Como esse gateway deve ser usado para todo o tráfego que sai do VCS Expressway, nenhuma rota estática é necessária nesse tipo de implantação.

A zona do cliente transversal no controle VCS deve ser configurada com um endereço de peer que corresponda ao endereço NAT estático do VCS Expressway (64.100.0.10 neste exemplo) pelas mesmas razões descritas no cenário anterior.

> **Note**: Isso significa que o FW A deve permitir o tráfego do VCS Control com um endereço IP destino de 64.100.0.10. Isso também é conhecido como reflexão de NAT, e deve-se observar que isso não é suportado por todos os tipos de FWs.

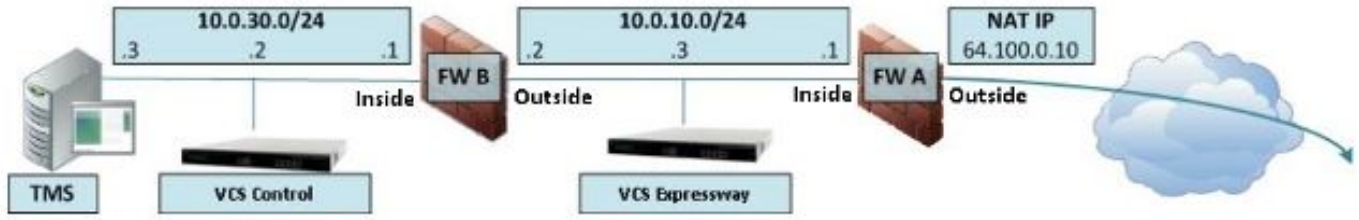
O VCS Expressway pode ser adicionado ao Cisco TMS com o endereço IP 10.0.10.2 (ou com o endereço IP 64.100.0.10, se o FW A permitir isso), já que a comunicação de gerenciamento do Cisco TMS não é afetada pelas configurações do modo NAT estático no VCS Expressway.

Configurar

Esta seção descreve como configurar a reflexão de NAT no ASA para os dois cenários de implementação de VCS C e E diferentes.

DMZ de sub-rede única com interface única de LAN VCS Expressway

Para o primeiro cenário, você deve aplicar essa configuração de reflexão de NAT no FW A para permitir a comunicação do Controle de VCS (10.0.30.2) destinado ao endereço IP externo (64.100.0.10) do VCS Expressway:



Neste exemplo, o endereço IP do controle VCS é **10.0.30.2/24**, e o endereço IP do VCS Expressway é **10.0.10.3/24**.

Se você supor que o endereço IP do controle VCS 10.0.30.2 permanece quando ele se move de dentro para fora da interface do FW B quando procura o VCS Expressway com o endereço IP destino 64.100.0.10, a configuração de reflexão NAT que você deve implementar no FW B é mostrada nesses exemplos.

Exemplo para ASA versões 8.3 e posteriores:

```
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.
```

Exemplo para ASA versões 8.2 e anteriores:

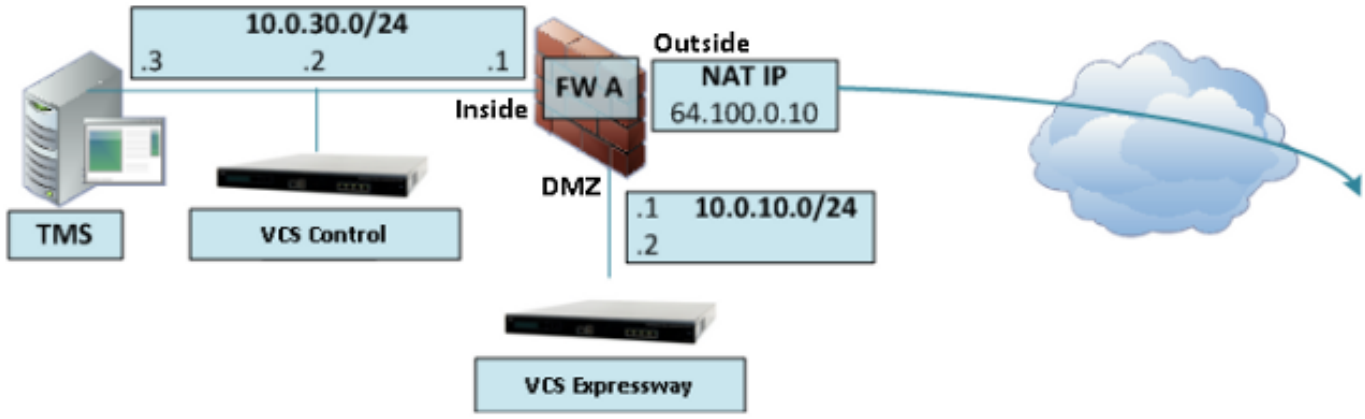
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

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
```

Note: O principal objetivo dessa configuração de reflexão de NAT é permitir que o controle

de VCS possa acessar a expressway de VCS, mas usando o endereço IP público da expressway de VCS em vez de seu endereço IP privado. Se o endereço IP de origem do controle VCS for alterado durante essa conversão de NAT com duas configurações de NAT em vez da configuração de NAT sugerida mostrada, resultando no VCS Expressway vendo o tráfego de seu próprio endereço IP público, os serviços de telefone para os dispositivos de MRA não serão ativados. Esta não é uma implantação compatível de acordo com a seção 3 da seção de recomendações abaixo.

3 portas FW DMZ com interface única de LAN VCS Expressway

Para o segundo cenário, você deve aplicar essa configuração de reflexão de NAT no FW A para permitir a reflexão de NAT do tráfego de entrada do VCS Control 10.0.30.2 que é destinado ao endereço IP externo (64.100.0.10) do VCS Expressway:



Neste exemplo, o endereço IP do controle VCS é **10.0.30.2/24**, e o endereço IP do VCS Expressway é **10.0.10.2/24**.

Se você supor que o endereço IP do controle VCS 10.0.30.2 permanece quando ele se move de dentro para a interface DMZ do FW A quando procura o VCS Expressway com o endereço IP destino 64.100.0.10, a configuração de reflexão NAT que você deve implementar no FW A é mostrada nesses exemplos.

Exemplo para ASA versões 8.3 e posteriores:

```
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.
```

Exemplo para ASA versões 8.2 e anteriores:

```
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
```

> **Note**: O principal objetivo dessa configuração de reflexão de NAT é permitir que o controle de VCS possa acessar a expressway de VCS, mas com o endereço IP público da expressway de VCS em vez de seu endereço IP privado. Se o endereço IP de origem do VCS Control for alterado durante essa conversão de NAT com uma configuração de NAT duas vezes em vez da configuração de NAT sugerida mostrada, resultando no VCS Expressway vendo o tráfego de seu próprio endereço IP público, os serviços de telefone para os dispositivos de MRA não serão ativados. Esta não é uma implantação compatível de acordo com a seção 3 da seção de recomendações abaixo.

Verificar

Esta seção fornece as saídas do packet tracer que você pode ver no ASA para confirmar que a configuração de reflexão do NAT funciona conforme necessário em ambos os cenários de implementação do VCS C e E.

DMZ de sub-rede única com interface única de LAN VCS Expressway

Aqui está a saída do packet tracer do FW B para as versões 8.3 e posteriores do ASA:

```
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
```

Aqui está a saída do packet tracer do FW B para as versões 8.2 e anteriores do ASA:

```
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
```

3 portas FW DMZ com interface única de LAN VCS Expressway

Esta é a saída do FW A packet tracer para as versões 8.3 e posteriores do ASA:

```
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
```

Esta é a saída do FW A packet tracer para as versões 8.2 e anteriores do ASA:

```
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
```

Troubleshoot

Você pode configurar capturas de pacotes nas interfaces do ASA para confirmar a conversão de NAT quando os pacotes entram e saem das interfaces de FW envolvidas.

Captura de pacote aplicada para o cenário "DMZ FW de 3 portas com interface LAN Expressway VCS única"

```
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
```

Captura de pacote aplicada para o cenário "DMZ de sub-rede única com interface de LAN VCS Expressway única"

```
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]
```

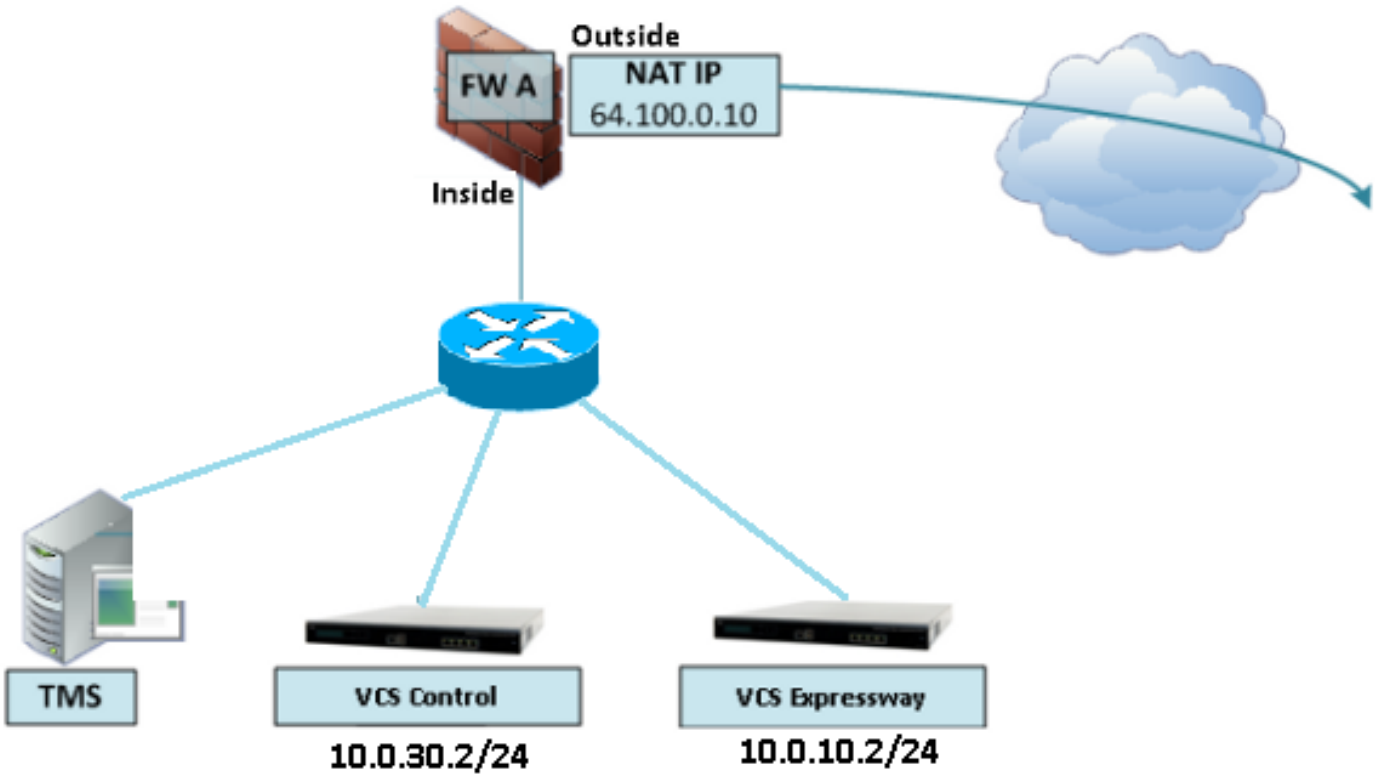
```
  match ip host 10.0.10.3 host 10.0.30.2

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
```

Recomendações

1. Evite a implementação de topologia não suportada

Por exemplo, se você tiver o VCS Control e o VCS Expressway conectados por trás da interface interna do ASA, como mostrado neste cenário:



Esse tipo de implementação exige que o endereço IP de controle do VCS seja convertido para o endereço IP interno do ASA para forçar o tráfego de retorno a voltar para o ASA para evitar problemas de rota assimétrica para a reflexão do NAT.

> **Observação: se o endereço IP de origem do controle VCS for alterado durante essa conversão NAT com uma configuração de NAT duas vezes em vez da configuração de reflexão NAT sugerida, o VCS Expressway verá o tráfego de seu próprio endereço IP público, então os serviços de telefone para os dispositivos MRA não serão ativados. Esta não é uma implantação compatível de acordo com a seção 3 da seção de recomendações abaixo.**

Dito isso, é altamente recomendável implementar o VCS Expressway como uma Implementação de Interfaces de Rede Dupla Expressway-E em vez de uma placa de rede única com reflexão de NAT.

2. Verifique se a inspeção SIP/H.323 está completamente desabilitada nos firewalls envolvidos

É altamente recomendado desativar a inspeção SIP e H.323 em firewalls que tratam do tráfego de rede de ou para um Expressway-E. Quando ativada, a inspeção de SIP/H.323 frequentemente afeta negativamente a funcionalidade de passagem de firewall/NAT incorporada do Expressway.

Este é um exemplo de como desativar as inspeções SIP e H.323 no ASA.

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

3. Verifique se a implementação real do Expressway está em conformidade com os próximos requisitos sugeridos pelos desenvolvedores da Cisco Telepresence

- A configuração de NAT entre o Expressway-C e o Expressway-E não é suportada.
- Ele não é suportado quando o Expressway-C e o Expressway-E, obtenha NATed para o mesmo endereço IP público, por exemplo:
  O Expressway-C está configurado com o endereço IP 10.1.1.1
  O Expressway-E tem uma única NIC configurada com o endereço IP 10.2.2.1 e um NAT estático é configurado no firewall com o endereço IP público 64.100.0.10
  Em seguida, o Expressway-C não pode ser NATted para o mesmo endereço público 64.100.0.10

Implementação recomendada do VCS Expressway

A implementação recomendada para o VCS Expressway em vez do VCS Expressway com a configuração de reflexão NAT é a implementação de interfaces de rede duplas/NIC VCS Expressway dupla, para obter mais informações, consulte o próximo link.

Configuração e recomendações do ASA NAT para a implementação das interfaces de rede duplas do Expressway-E.

Informações Relacionadas

- Configuração e recomendações do ASA NAT para a implementação das interfaces de rede duplas do Expressway-E
- Guia de implantação do Cisco TelePresence Video Communication Server Basic Configuration (Controle com Expressway)
- Uso da porta IP do Cisco Expressway para passagem de firewall
- Como colocar um Cisco VCS Expressway em uma DMZ em vez de na Internet pública