Configurar a reflexão NAT no ASA para os dispositivos do TelePresence de Expressway do VCS

Índice

Introdução

Este original descreve como executar uma configuração da reflexão do Network Address Translation (NAT) nas ferramentas de segurança adaptáveis de Cisco para as encenações especiais do Cisco TelePresence que exigem este tipo da configuração de NAT no Firewall.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de NAT básica de Cisco ASA (ferramenta de segurança adaptável).
- Controle do server de comunicação de vídeo do Cisco TelePresence (VCS) e de Expressway do VCS configuração básica.

> **Note**: Este original está pretendido ser usado somente quando o método recomendado do desenvolvimento de VCS-Expressway ou de uma Expressway-borda com ambas as relações NIC em DMZ diferentes não pode ser usado. Para mais informações sobre do desenvolvimento recomendado que usa NIC dual satisfaça verificam o seguinte link na página 60: Guia de distribuição da configuração básica do server de comunicação de vídeo do Cisco TelePresence (controle com Expressway)

Componentes Utilizados

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

- Dispositivos do 5500 e 5500-X Series de Cisco ASA que executam a versão de software 8.3 e mais atrasado.
- Versão X8.x do VCS de Cisco e mais tarde.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

> **Note**: Através do original inteiro, os dispositivos do VCS são referidos como o controle do VCS Expressway e do VCS. Contudo, a mesma configuração aplica-se aos dispositivos de Expressway-e e de Expressway-C.

Informações de Apoio

Conforme a documentação do Cisco TelePresence, há dois tipos das encenações do TelePresence onde a configuração da reflexão NAT é exigida nos FW a fim permitir que o controle do VCS se comunique com o VCS Expressway através do endereço IP público de Expressway do VCS.

A primeira encenação envolve um De-Militarized Zone da sub-rede única (DMZ) esse usos uma única interface de LAN de Expressway do VCS, e a segunda encenação envolve um 3-port FW DMZ que use uma única interface de LAN de Expressway do VCS.

> Dica: A fim obter mais detalhes sobre a aplicação do TelePresence, refira o guia de distribuição da configuração básica do server de comunicação de vídeo do Cisco TelePresence (controle com Expressway).

Topologias de Cisco NON-recomendadas para o C do VCS e a aplicação E

Éimportante notar que as seguintes topologias não estão recomendadas por Cisco. A metodologia recomendada do desenvolvimento para um VCS Expressway ou a borda de Expressway é usar dois DMZ diferentes com Expressway que tem um NIC em cada um dos DMZ. Este guia é significado ser usado nos ambientes onde o método recomendado do desenvolvimento não pode ser usado.

Sub-rede única DMZ com única interface de LAN de Expressway do VCS

Nesta encenação, o FW A pode distribuir o tráfego a FW B (e vice-versa). O VCS Expressway permite que o tráfego de vídeo seja passado com FW B sem uma redução no fluxo de tráfego em FW B da parte externa às interfaces internas. O VCS Expressway igualmente segura o traversal FW em seu lado público.

Está aqui um exemplo desta encenação:

Este desenvolvimento usa estes componentes:

- Uma sub-rede única DMZ (10.0.10.0/24) que contenham:
  A interface interna de FW A (10.0.10.1)A interface externa de FW B (10.0.10.2)A relação LAN1 do VCS Expressway (10.0.10.3)
- Uma sub-rede de LAN (10.0.30.0/24) que contenham:
  A interface interna de FW B (10.0.30.1)A relação LAN1 do controle do VCS (10.0.30.2)A interface de rede do servidor de gerenciamento do Cisco TelePresence (TMS) (10.0.30.3)

Um NAT linear estático foi configurado no FW A, que executa o NAT para o endereço público 64.100.0.10 ao endereço IP de Um ou Mais Servidores Cisco ICM NT LAN1 do VCS Expressway. O modo do NAT estático foi permitido para a relação LAN1 no VCS Expressway, com um endereço IP de Um ou Mais Servidores Cisco ICM NT do NAT estático de 64.100.0.10.

> **Note**: Você deve incorporar o nome de domínio totalmente qualificado (FQDN) do VCS Expressway na zona segura do cliente do traversal do controle do VCS (endereço de peer) como como se vê fora da rede. A razão para esta reage aquela do modo do NAT estático, o VCS Expressway pede que a sinalização de entrada e os media traficam estejam enviados a seu FQDN externo um pouco do que seu nome privado. Isto igualmente significa que o FW externo deve permitir o tráfego do controle do VCS ao FQDN externo de Expressway do VCS. Isto é sabido como a reflexão NAT, e não pôde ser apoiado por todos os tipos de FW.

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

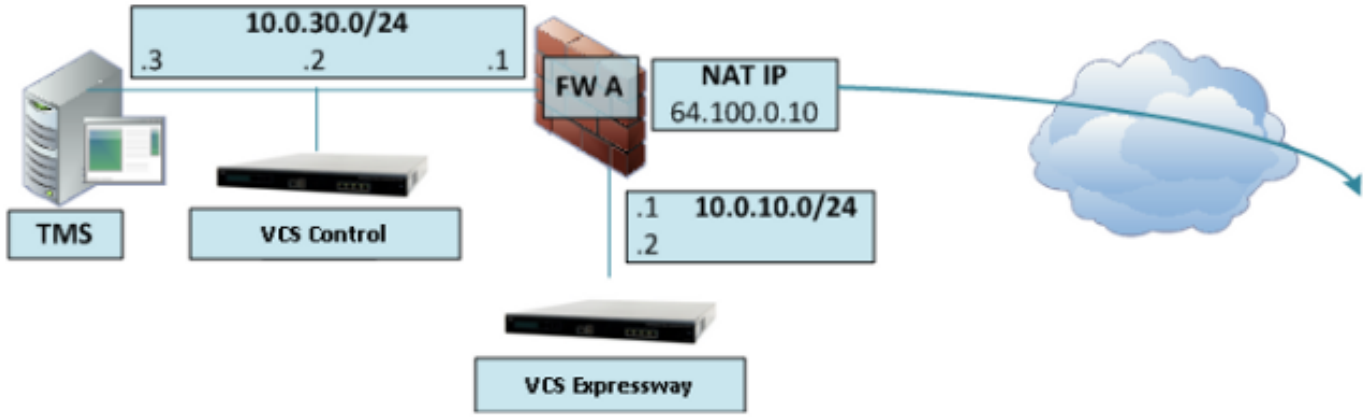
O VCS Expressway deve ser configurado com um gateway padrão de **10.0.10.1**. Se as rotas estáticas estão exigidas nesta encenação depende das capacidades e dos ajustes de FW A e de

FW B. A comunicação do controle do VCS ao VCS Expressway ocorre através do endereço IP 64.100.0.10 do VCS Expressway; e o tráfego de retorno do VCS Expressway ao controle do VCS pôde ter que passar através do gateway padrão.

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

3-Port FW DMZ com única interface de LAN de Expressway do VCS

Está aqui um exemplo desta encenação:



Neste desenvolvimento, um 3-port FW é usado a fim criar:

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

Um NAT linear estático foi configurado no FW A, que executa o NAT do endereço IP público 64.100.0.10 ao endereço IP de Um ou Mais Servidores Cisco ICM NT LAN1 do VCS Expressway. O modo do NAT estático foi permitido para a relação LAN1 no VCS Expressway, com um endereço IP de Um ou Mais Servidores Cisco ICM NT do NAT estático de 64.100.0.10.

O VCS Expressway deve ser configurado com um gateway padrão de 10.0.10.1. Desde que este gateway deve ser usado para todo o tráfego que sae do VCS Expressway, nenhuma rota estática é exigida neste tipo de desenvolvimento.

A zona do cliente do traversal no controle do VCS deve ser configurada com um endereço de peer que combine o endereço do NAT estático do VCS Expressway (64.100.0.10 neste exemplo) para as mesmas razões que aqueles descritos no cenário anterior.

> **Note**: Isto significa que o FW A deve permitir o tráfego do controle do VCS com um endereço IP de destino de 64.100.0.10. Isto é sabido igualmente como a reflexão NAT, e deve-se notar que este não está apoiado por todos os tipos de FW.

O VCS Expressway pode ser adicionado a Cisco TMS com o endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.0.10.2 (ou com endereço IP 64.100.0.10, se o FW A permite

este), desde que a comunicação de Gerenciamento de Cisco TMS não é afetada pelas configurações de modo do NAT estático no VCS Expressway.

Configurar

Esta seção descreve como configurar a reflexão NAT no ASA para as duas hipóteses de implementação diferentes do C e E do VCS.

Sub-rede única DMZ com única interface de LAN de Expressway do VCS

Para a primeira encenação, você deve aplicar esta configuração da reflexão NAT em FW à fim permitir a comunicação do controle do VCS (10.0.30.2) que é destinado ao endereço IP externo (64.100.0.10) do VCS Expressway:

Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT do controle do VCS é **10.0.30.2/24**, e o endereço IP de Um ou Mais Servidores Cisco ICM NT de Expressway do VCS é **10.0.10.3/24**.

Se você supõe que o endereço IP 10.0.30.2 do controle do VCS permanece quando se move do interior para a interface externa de FW B quando procurando o VCS Expressway com o endereço IP de destino 64.100.0.10, a seguir a configuração da reflexão NAT que você deve executar em FW B está mostrado nestes exemplos.

Exemplo para as versões ASA 8.3 e mais atrasado:

```
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 as versões ASA 8.2 e mais adiantado:

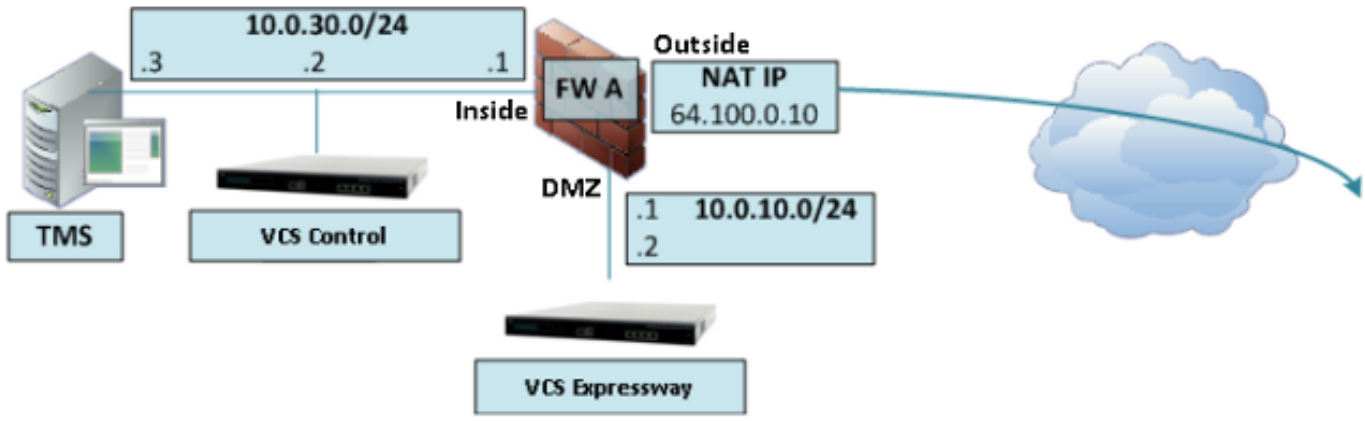
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
```

```
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 objetivo principal desta configuração da reflexão NAT é permitir que o controle do VCS possa alcançar a via expressa do VCS, mas a utilização do endereço IP público da via expressa do VCS em vez de seu endereço IP privado. Se o endereço IP de origem do controle do VCS é mudado durante esta tradução NAT com duas vezes uma configuração de NAT em vez da configuração de NAT sugerida apenas mostrada, tendo por resultado o VCS Expressway ver o tráfego de seu próprio endereço IP público, a seguir dos serviços de telefone para os dispositivos MRA não virá acima. Este não é um desenvolvimento apoiado conforme a seção 3 na seção das recomendações abaixo.

3-Port FW DMZ com única interface de LAN de Expressway do VCS

Para a segunda encenação, você deve aplicar esta configuração da reflexão NAT em FW à fim permitir a reflexão NAT do tráfego de entrada do controle 10.0.30.2 do VCS que é destinado ao endereço IP externo (64.100.0.10) do VCS Expressway:



Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT do controle do VCS é **10.0.30.2/24**, e o endereço IP de Um ou Mais Servidores Cisco ICM NT de Expressway do VCS é **10.0.10.2/24**.

Se você supõe que o endereço IP 10.0.30.2 do controle do VCS permanece quando se move do interior para a relação DMZ de FW A quando procurando o VCS Expressway com o endereço IP de destino 64.100.0.10, a seguir a configuração da reflexão NAT que você deve executar em FW A está mostrado nestes exemplos.

Exemplo para as versões ASA 8.3 e mais atrasado:

```
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 as versões ASA 8.2 e mais adiantado:

```
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 objetivo principal desta configuração da reflexão NAT é permitir que o controle do VCS possa alcançar a via expressa do VCS, mas com o endereço IP público da via expressa do VCS em vez de seu endereço IP privado. Se o endereço IP de origem do controle do VCS é mudado durante esta tradução NAT com duas vezes uma configuração de NAT em vez da configuração de NAT sugerida apenas mostrada, tendo por resultado o VCS Expressway ver o tráfego de seu próprio endereço IP público, a seguir dos serviços de telefone para os dispositivos MRA não virá acima. Este não é um desenvolvimento apoiado conforme a seção 3 na seção das recomendações abaixo.

Verificar

Esta seção fornece as saídas do projétil luminoso do pacote que você pode ver no ASA a fim confirmar a configuração da reflexão NAT trabalha como necessário em ambas as hipóteses de implementação do C e E do VCS.

Sub-rede única DMZ com única interface de LAN de Expressway do VCS

Está aqui o projétil luminoso do pacote FW B output para as versões ASA 8.3 e mais atrasado:

```
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
```

Está aqui o projétil luminoso do pacote FW B output para as versões ASA 8.2 e mais adiantado:

```
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-Port FW DMZ com única interface de LAN de Expressway do VCS

Está aqui o projétil luminoso do pacote FW A output para as versões ASA 8.3 e mais atrasado:

```
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
```

Está aqui o projétil luminoso do pacote FW A output para as versões ASA 8.2 e mais adiantado:

```
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
```

Troubleshooting

Você pode configurar capturas de pacote de informação nas relações ASA a fim confirmar a tradução NAT quando os pacotes incorporam e saem das relações FW que são involvidas.

Captura de pacote de informação aplicada para o "3-Port FW DMZ com encenação da única interface de LAN de Expressway do VCS”

```
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 de informação aplicada para “sub-rede única DMZ com a encenação da única interface de LAN de Expressway do VCS”

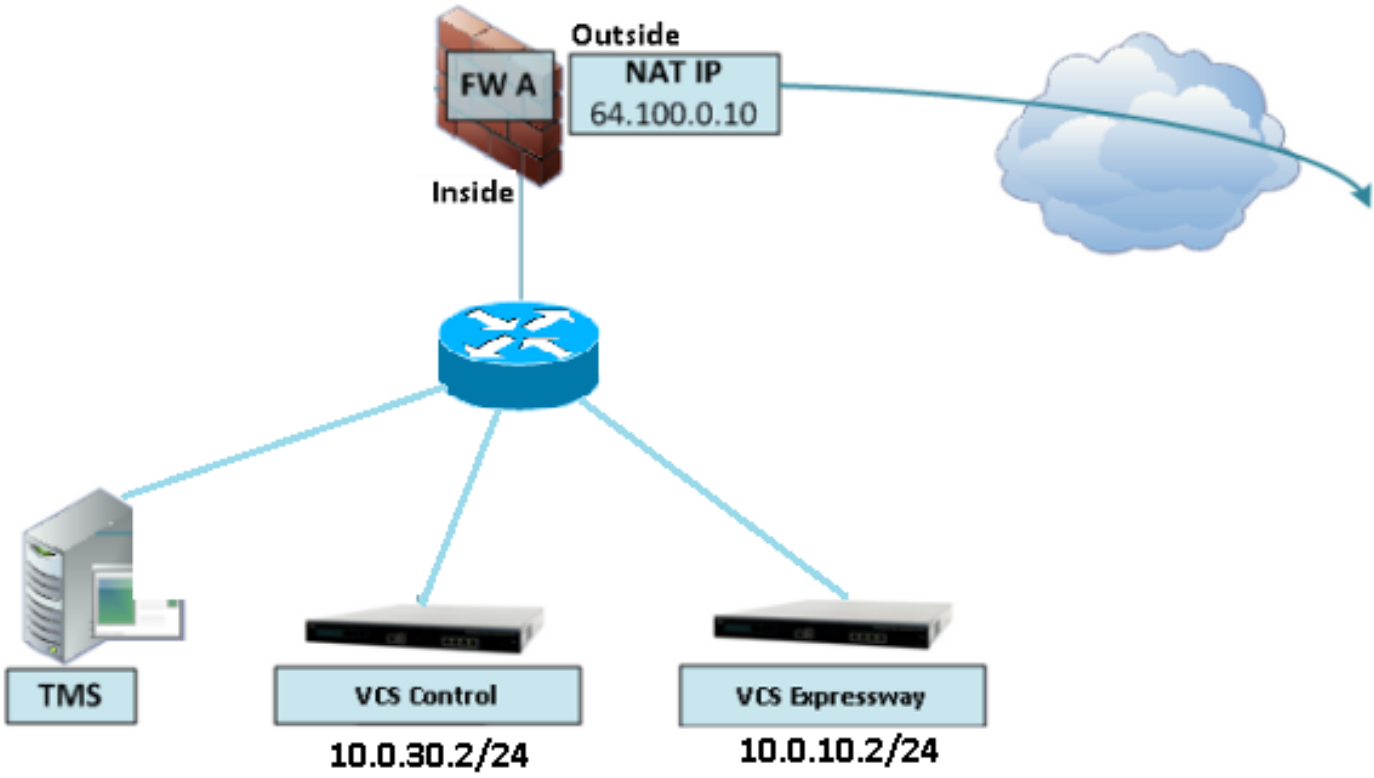
```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2

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 aplicação de toda a topologia unsupported

Por exemplo, se você tem o controle do VCS e o VCS Expressway conectado atrás da relação interna ASA, apenas segundo as indicações desta encenação:



Este tipo da aplicação exige o endereço IP de Um ou Mais Servidores Cisco ICM NT do controle do VCS ser traduzido ao endereço IP de Um ou Mais Servidores Cisco ICM NT interno do ASA a fim forçar o tráfego de retorno para vir para trás ao ASA evitar problemas assimétricos da rota para a reflexão NAT.

> **Nota: Se o endereço IP de origem do controle do VCS é mudado durante esta tradução NAT com duas vezes uma configuração de NAT em vez da configuração sugerida da reflexão NAT, a seguir o VCS Expressway verá o tráfego de seu próprio endereço IP público, a seguir os serviços de telefone para os dispositivos MRA não virão acima. Este não é um desenvolvimento apoiado conforme a seção 3 na seção das recomendações abaixo.**

Isso dito, é altamente recomendado executar o VCS Expressway como uma aplicação dupla das interfaces de rede de Expressway-e em vez do único NIC com reflexão NAT.

2. Assegure-se de que a inspeção SIP/H.323 esteja desabilitada completamente nos Firewall envolvidos

É altamente recomendado desabilitar o SORVO e a inspeção de H.323 nos Firewall que seguram o tráfego de rede a ou de Expressway-e. Quando permitida, a inspeção SIP/H.323 é encontrada frequentemente para afetar negativamente a funcionalidade incorporado do traversal de Expressway firewall/NAT.

Este é um exemplo de como desabilitar o SORVO e as inspeções de H.323 no ASA.

```
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
```

3. Assegure-se de que sua aplicação real de Expressway siga com as exigências seguintes sugeridas pelos colaboradores do Cisco TelePresence

- A configuração de NAT entre Expressway-C e Expressway-e não é apoiada.
- Não é apoiada quando Expressway-C e Expressway-e, obtêm o NATed ao mesmo endereço IP público, por exemplo:
  Expressway-C é configurado com endereço IP de Um ou Mais Servidores Cisco ICM NT 10.1.1.1
  Expressway-e tem o único NIC configurado com endereço IP 10.2.2.1 e um NAT estático é configurado no Firewall com endereço IP público 64.100.0.10
  Então Expressway-C não pode ser NATted ao mesmo endereço público 64.100.0.10

Aplicação recomendada de Expressway do VCS

A aplicação recomendada para o VCS Expressway em vez do VCS Expressway com a configuração da reflexão NAT é as interfaces de rede/a aplicação duplas de Expressway VCS do NIC dual, satisfaz para mais informações verifica o link seguinte.

A configuração de NAT e as recomendações ASA para Expressway-e Dual aplicação das interfaces de rede.

Informações Relacionadas

- A configuração de NAT e as recomendações ASA para Expressway-e Dual aplicação das interfaces de rede

- Guia de distribuição da configuração básica do server de comunicação de vídeo do Cisco TelePresence (controle com Expressway)
- Uso da porta IP de Cisco Expressway para o Firewall Traversal
- Colocando um VCS Expressway de Cisco em um DMZ um pouco do que no Internet público