# 在 ASA 上为 VCS Expressway TelePresence 设备配置 NAT 反射

## 目录


[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[背景信息](#)

[不推荐用于VCS C和E实施的思科拓扑](#)

- [带单VCS Expressway LAN接口的单子网DMZ](#)
- [带单VCS Expressway LAN接口的3 — 口防火墙DMZ](#)

[配置](#)

- [带单VCS Expressway LAN接口的单子网DMZ](#)
- [带单VCS Expressway LAN接口的3 — 口防火墙DMZ](#)

[验证](#)

- [带单VCS Expressway LAN接口的单子网DMZ](#)
- [带单VCS Expressway LAN接口的3 — 口防火墙DMZ](#)

[故障排除](#)

- [数据包捕获应用于“具有单个VCS Expressway LAN接口的3端口防火墙DMZ”方案](#)
- [数据包捕获应用于“具有单个VCS Expressway LAN接口的单子网DMZ”方案](#)
- [建议](#)
  - [1.避免实施任何不受支持的拓扑](#)
  - [2.确保在涉及的防火墙上完全禁用SIP/H.323检测](#)
  - [3.确保实际的Expressway实施符合思科网真开发人员建议的下一个要求](#)

[推荐的VCS Expressway实施](#)

[相关信息](#)


## 简介

本文档介绍如何在思科自适应安全设备上实施网络地址转换(NAT)反射配置，以满足需要在防火墙上进行此类NAT配置的特殊Cisco TelePresence场景。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Cisco ASA（自适应安全设备）基本NAT配置。

- Cisco TelePresence Video Communication Server(VCS)Control和VCS Expressway基本配置。

注意：本文档旨在仅在不能使用具有不同DMZ中的两个NIC接口的VCS-Expressway或Expressway-Edge的推荐部署方法时使用。有关建议使用双NIC进行部署的详细信息，请查看以下链接(位于第60页)：“Cisco TelePresence Video Communication Server Basic Configuration(Control with Expressway)Deployment Guide”(思科网真视频通信服务器基本配置（使用Expressway进行控制）部署指南)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本8.3及更高版本的Cisco ASA 5500和5500-X系列设备。
- Cisco VCS版本X8.x及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

注意:在整个文档中，VCS设备称为VCS Expressway和VCS Control。但是，相同配置适用于Expressway-E和Expressway-C设备。

## 背景信息

根据Cisco TelePresence文档，有两种类型的网真场景，需要在防火墙上进行NAT反射配置，以允许VCS Control通过VCS Expressway公有IP地址与VCS Expressway通信。

第一个场景涉及使用单个VCS Expressway LAN接口的单个子网非军事化区域(DMZ)，第二个场景涉及使用单个VCS Expressway LAN接口的3端口FW DMZ。

提示：要了解有关网真实施的更多详细信息，请参阅思科网真视频通信服务器基本配置（使用Expressway控制）部署指南。

## 不推荐用于VCS C和E实施的思科拓扑

请务必注意，思科不推荐以下拓扑。VCS Expressway或Expressway边缘的推荐部署方法是：使用两个不同的DMZ，并且Expressway在每个DMZ中都有一个NIC。本指南适用于无法使用推荐部署方法的环境。

### 带单VCS Expressway LAN接口的单子网DMZ

在此场景中，防火墙A可以将流量路由到防火墙B（反之亦然）。 VCS Expressway允许视频流量通过FW B，而不会减少FW B上从外部到内部接口的流量。VCS Expressway还在其公共端处理FW遍

历。

以下是此方案的示例：




此部署使用以下组件：

- 单个子网DMZ(10.0.10.0/24)，包含：
  - 防火墙A(10.0.10.1)的内部接口
  - 防火墙B的外部接口(10.0.10.2)
  - VCS Expressway的LAN1接口(10.0.10.3)
- LAN子网(10.0.30.0/24)包含：
  - 防火墙B的内部接口(10.0.30.1)
  - VCS控制的LAN1接口(10.0.30.2)
  - 思科网真管理服务器(TMS)的网络接口(10.0.30.3)

FW A上已配置静态的一对一NAT，该NAT将公有地址64.100.0.10执行到VCS Expressway的LAN1 IP地址的NAT。VCS Expressway上的LAN1接口已启用静态NAT模式，静态NAT IP地址为64.100.0.10。

---

注意：您必须输入VCS Control安全遍历客户端区域（对等体地址）上VCS Expressway的完全限定域名(FQDN)，就像从网络外部看到的那样。原因是在静态NAT模式下，VCS Expressway请求将入站信令和媒体流量发送到其外部FQDN而不是其专用名称。这也意味着外部FW必须允许从VCS Control到VCS Expressway外部FQDN的流量。这称为NAT反射，所有类型的防火墙可能都不支持。

---

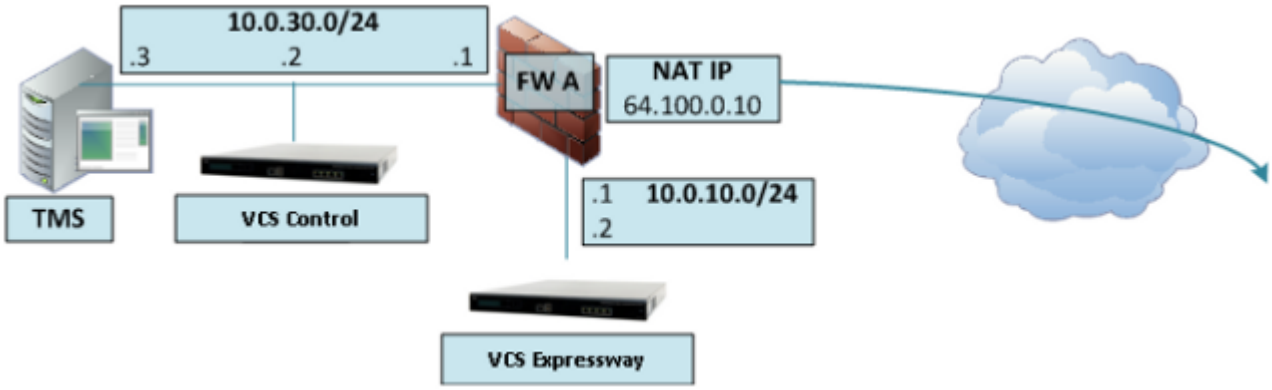
在本示例中，FW B必须允许来自VCS Control且目的地为VCS Expressway的外部IP地址(64.100.0.10)的流量的NAT反射。VCS Control上的遍历区域必须将64.100.0.10作为对等体地址（在FQDN到IP转换之后）。

VCS Expressway应配置默认网关10.0.10.1。此场景中是否需要静态路由取决于FW A和FW B的功能和设置。从VCS Control到VCS Expressway的通信通过VCS Expressway的64.100.0.10 IP地址进行；从VCS Expressway到VCS Control的返回流量可能必须通过默认网关。

VCS Expressway可以添加到IP地址为10.0.10.3（或IP地址为64.100.0.10，如果FW B允许这样做）的Cisco TMS，因为思科TMS管理通信不会受到VCS Expressway上的静态NAT模式设置的影响。

## 带单VCS Expressway LAN接口的3 — 口防火墙DMZ

以下是此方案的示例：




在此部署中，使用3端口防火墙以创建：

- 一个DMZ子网(10.0.10.0/24)，包含：
  - 防火墙A(10.0.10.1)的DMZ接口
  - VCS Expressway的LAN1接口(10.0.10.2)
- LAN子网(10.0.30.0/24)包含：
  - FW A(10.0.30.1)的LAN接口
  - VCS控制的LAN1接口(10.0.30.2)
  - 思科TMS的网络接口(10.0.30.3)

FW A上已配置静态一对一NAT，它执行从VCS Expressway的公有IP地址64.100.0.10到LAN1 IP地址的NAT。VCS Expressway上的LAN1接口已启用静态NAT模式，静态NAT IP地址为64.100.0.10。

VCS Expressway应配置默认网关10.0.10.1。由于此网关必须用于离开VCS Expressway的所有流量，因此这种部署类型不需要静态路由。

VCS Control上的遍历客户端区域必须配置一个与VCS Expressway的静态NAT地址（本例中为64.100.0.10）匹配的对等地址，原因与前一场景中所述的原因相同。

---

注意：这意味着FW A必须允许来自目标IP地址为64.100.0.10的VCS Control的流量。这也称为NAT反射，应该注意的是，并非所有类型的防火墙都支持此功能。

---

VCS Expressway可以添加IP地址为10.0.10.2（或IP地址为64.100.0.10，如果FW A允许），因为思科TMS管理通信不会受到VCS Expressway上的静态NAT模式设置的影响。

# 配置

本节介绍如何为两个不同的VCS C和E实施方案在ASA中配置NAT反射。

## 带单VCS Expressway LAN接口的单子网DMZ

对于第一个场景，必须在FW A上应用此NAT反射配置，以允许从VCS控制(10.0.30.2)发往VCS Expressway的外部IP地址(64.100.0.10)的通信：




在本示例中，VCS控制IP地址为10.0.30.2/24，而VCS Expressway IP地址为10.0.10.3/24。

如果您假设在查找目标IP地址为64.100.0.10的VCS Expressway时，VCS控制IP地址10.0.30.2从FW B的内部接口移动到外部接口时仍保留，则您应在FW B上实施的NAT反射配置如下例所示。

ASA版本8.3及更高版本的示例：

```
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版本8.2及更早版本的示例：

```
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
```

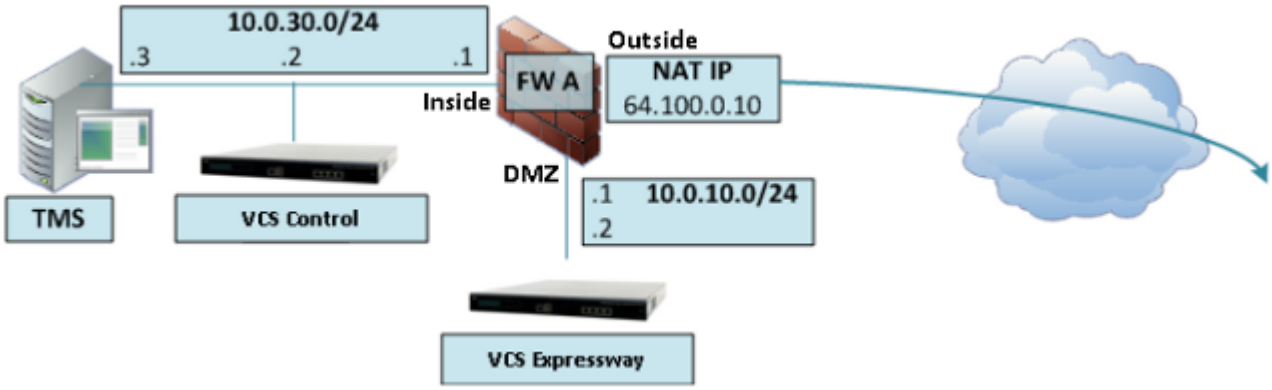
---

注意：此NAT反射配置的主要目标是允许VCS控制能够到达VCS Expressway，但使用VCS Expressway公有IP地址而不是私有IP地址。如果在此NAT转换期间，VCS控制的源IP地址使用两次NAT配置而不是刚才所示的建议NAT配置进行更改，导致VCS Expressway看到来自其自身公有IP地址的流量，则MRA设备的电话服务不会启动。根据下面建议部分的第3部分，这不是支持的部署。

---

## 带单VCS Expressway LAN接口的3 — 口防火墙DMZ

对于第二个场景，您必须在FW　A上应用此NAT反射配置，以允许对来自VCS控制10.0.30.2的入站流量进行NAT反射，该入站流量指向VCS Expressway的外部IP地址(64.100.0.10):




在本示例中，VCS控制IP地址为10.0.30.2/24，而VCS Expressway IP地址为10.0.10.2/24。

如果您假设在查找目标IP地址为64.100.0.10的VCS　Expressway时，VCS控制IP地址10.0.30.2从FW A的内部移动到DMZ接口时仍保留，则您应在FW A上实施的NAT反射配置如下例所示。

ASA版本8.3及更高版本的示例：

```
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版本8.2及更早版本的示例：

```
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
```

注意：此NAT反射配置的主要目标是允许VCS控制能够到达VCS　Expressway，但使用VCS

Expressway公有IP地址而非私有IP地址。如果VCS控制的源IP地址在此NAT转换期间使用两次NAT配置而不是刚才所示的建议NAT配置进行了更改，导致VCS Expressway看到来自其自己的公有IP地址的流量，则MRA设备的电话服务不会出现。根据下面建议部分的第3部分，这不是支持的部署。

# 验证

本部分提供您在ASA中看到的Packet Tracer输出，以确认NAT反射配置可根据需要在VCS C和E实施场景中运行。

## 带单VCS Expressway LAN接口的单子网DMZ

以下是ASA版本8.3及更高版本的FW B Packet Tracer输出：

<#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
```

以下是ASA版本8.2及更低版本的FW B Packet Tracer输出：

<#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
```

## 带单VCS Expressway LAN接口的3 — 口防火墙DMZ

以下是ASA版本8.3及更高版本的FW A Packet Tracer输出：

```
<#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
```

以下是ASA版本8.2及更低版本的FW A Packet Tracer输出：

<#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
```

# 故障排除

您可以在ASA接口上配置数据包捕获，以便在数据包进入和离开所涉及的FW接口时确认NAT转换。

数据包捕获应用于“具有单个VCS Expressway LAN接口的3端口防火墙DMZ”方案

<#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
```

数据包捕获应用于“具有单个VCS Expressway LAN接口的单子网DMZ”方案

<#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**

```

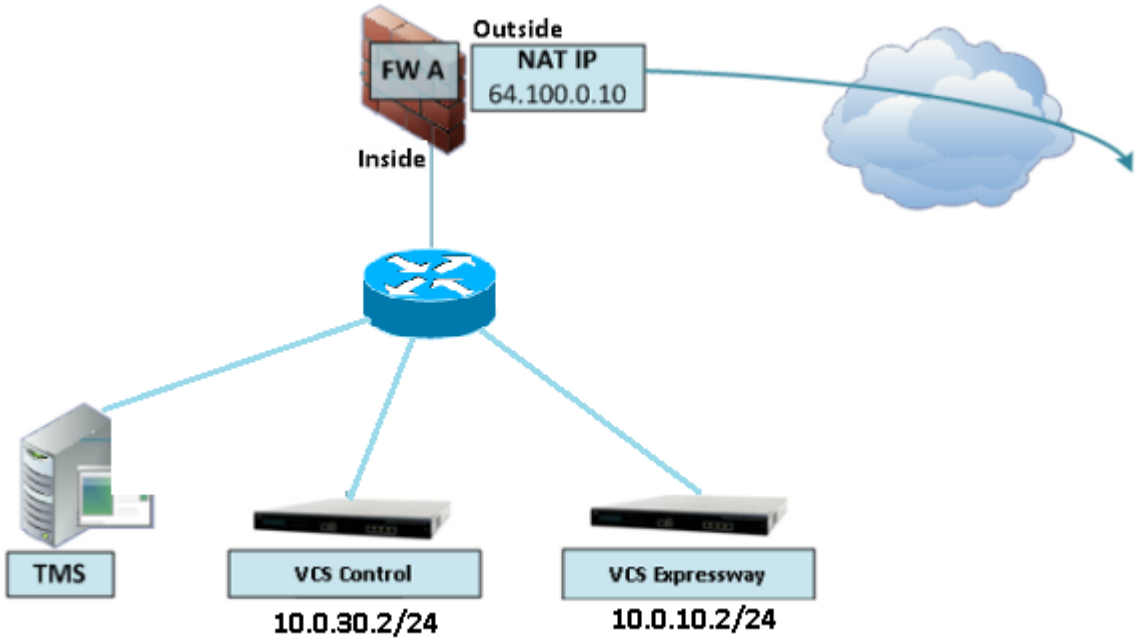
72 packets captured
   1: 22:30:06.784871 10.0.30.2 > 10.0.10.3: icmp: echo request
   2: 22:30:06.847688 10.0.10.3 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.878769 10.0.30.2 > 10.0.10.3: icmp: echo request
   4: 22:30:06.900557 10.0.10.3 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.972758 10.0.30.2 > 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
```

## 建议

1.避免实施任何不受支持的拓扑

例如，如果您将VCS Control和VCS Expressway都连接到内部ASA接口的后面，如下例所示：




这种实施需要将VCS控制IP地址转换为ASA的内部IP地址，以强制返回流量返回到ASA，从而避免NAT反射出现非对称路由问题。

---

注意：如果VCS控制的源IP地址在此NAT转换期间使用两次NAT配置而不是建议的NAT反射配置更改，则VCS Expressway将看到来自其自身公有IP地址的流量，则MRA设备的电话服务不会出现。根据下面建议部分的第3部分，这不是支持的部署。

---

也就是说，强烈建议将VCS Expressway实施为Expressway-E双网络接口实施，而不是采用NAT反射的单个网卡。

2.确保在涉及的防火墙上完全禁用SIP/H.323检测

强烈建议在处理Expressway-E传入或传出网络流量的防火墙上禁用SIP和H.323检测。启用时，经常发现SIP/H.323检测会对Expressway内置防火墙/NAT穿越功能产生负面影响。

以下示例说明如何在ASA上禁用SIP和H.323检测。

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

3.确保实际的Expressway实施符合思科网真开发人员建议的下一个要求

- 不支持Expressway-C和Expressway-E之间的NAT配置。
- 当Expressway-C和Expressway-E将NAT转换为同一公有IP地址时，不支持该协议，例如：
  Expressway-C配置了IP地址10.1.1.1
  Expressway-E具有配置了IP地址10.2.2.1的单个网卡，并且在防火墙中配置了一个具有公有IP地址64.100.0.10的静态NAT
  则Expressway-C无法通过NAT连接到相同的公有地址64.100.0.10

# 推荐的VCS Expressway实施

VCS Expressway（而不是具有NAT反射配置的VCS Expressway）的建议实施是双网络接口/双NIC VCS Expressway实施，有关详细信息，请检查下一链接。

ASA NAT 配置以及有关 Expressway-E 双网络接口实现的建议.

# 相关信息

- ASA NAT 配置以及有关 Expressway-E 双网络接口实现的建议
- 思科网真视频通信服务器基本配置（使用Expressway进行控制）部署指南
- 用于防火墙穿越的Cisco Expressway IP端口使用
- 将Cisco VCS Expressway放置在DMZ中而不是放置在公共互联网中

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。