

# 配置在ASA的NAT反映VCS Expressway网真设备的

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[Cisco拓扑非推荐为VCS C和E实施](#)

[与单个VCS Expressway LAN接口的单个子网DMZ](#)

[与单个VCS Expressway LAN接口的3端口FW DMZ](#)

[Configure](#)

[与单个VCS Expressway LAN接口的单个子网DMZ](#)

[与单个VCS Expressway LAN接口的3端口FW DMZ](#)

[Verify](#)

[与单个VCS Expressway LAN接口的单个子网DMZ](#)

[与单个VCS Expressway LAN接口的3端口FW DMZ](#)

[Troubleshoot](#)

[申请与单个VCS Expressway LAN接口”方案的”3端口FW信息包获取DMZ](#)

[申请“与单个VCS Expressway LAN接口”方案的信息包获取单个子网DMZ](#)

[推荐](#)

1. [避免所有不支持的拓扑的实施](#)

2. [保证SIP/H.323检查在介入的防火墙完全地被禁用](#)

3. [保证您的实际Expressway实施符合思科网真开发人员建议的下一个需求](#)

[推荐的VCS Expressway实施](#)

[Related Information](#)

## Introduction

本文描述如何实现在Cisco可适应的安全工具上的一种网络地址转换(NAT)反映配置要求这种在防火墙的NAT配置的特殊思科网真方案的。

## Prerequisites

## Requirements

Cisco 建议您了解以下主题：

- Cisco ASA (可适应的安全工具)基本的NAT配置。
- 思科网真视频通信服务器(VCS)控制和VCS Expressway基本配置。

**Note:**本文，只有当不可能使用时，打算使用一个VCS Expressway或Expressway边缘的推荐

的配置方法与两个NIC接口用不同的DMZ。欲知关于推荐的配置的详情使用双NIC请检查以下链接在第60页：[思科网真视频通信服务器基本配置\(与Expressway的控制\)部署指南](#)

## Components Used

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及以后的Cisco ASA 5500和5500-X系列工具。
- Cisco VCS版本X8.x和以后。

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.

**Note:** 通过整个文档，VCS设备指VCS Expressway和VCS控制。然而，相同配置适用于ExpresswayE和ExpresswayC设备。

## 背景信息

根据思科网真文档，有两NAT规则配置在FWs要求为了允许VCS控制与VCS Expressway联络通过VCS Expressway公共IP地址的网真方案。

使用单个VCS Expressway LAN接口的第一个方案介入单个子网非敏感区域(DMZ)，并且第二个场景介入使用单个VCS Expressway LAN接口的3端口FW DMZ。

**提示：**为了得到关于网真实施的更多详细资料，请参见[思科网真视频通信服务器基本配置\(与Expressway的控制\)部署指南](#)。

## Cisco拓扑非推荐为VCS C和E实施

请注意以下拓扑没有由Cisco建议使用。VCS Expressway或Expressway边缘的推荐的配置方法是使用两个不同的DMZ以Expressway有NIC在其中每一个DMZ。此指南被认为用于不可能使用推荐的配置方法的环境。

### 与单个VCS Expressway LAN接口的单个子网DMZ

在此方案中，FW A能路由流量对FW B (反之亦然)。VCS Expressway允许视频数据流通过FW B，不用对通信流的减少在FW B从自内部接口的外面。VCS Expressway也处理在其公共侧的FW穿越。

这是此方案示例：



此配置使用这些组件：

- 包含的单个子网DMZ (10.0.10.0/24)：  
内部界面FW A (10.0.10.1)外部接口FW B (10.0.10.2)VCS Expressway (10.0.10.3)的LAN1接口
- 包含的LAN子网(10.0.30.0/24)：  
内部界面FW B (10.0.30.1)VCS控制(10.0.30.2)的LAN1接口思科网真管理服务器(TMS) (10.0.30.3)的网络接口

静态一对一的NAT在FW A被配置了，执行公共地址的64.100.0.10 NAT对VCS Expressway的LAN1 IP地址。静态NAT模式为在VCS Expressway的LAN1接口启动了，用64.100.0.10的一个静态NAT IP地址。

**Note:** 您必须输入VCS Expressway的完全合格的域名(FQDN)在VCS控制安全的穿越客户端区域(对等体地址)的和如何从网络外面被看到。对此的原因是那在静态NAT模式下，VCS Expressway请求Inbound信令和媒体数据流被发送到其外部FQDN而不是其专用的名字。这也意味着外部FW必须允许从VCS控制的数据流到VCS Expressway外部FQDN。这叫作NAT反映，并且也许不由FWs的所有类型支持。

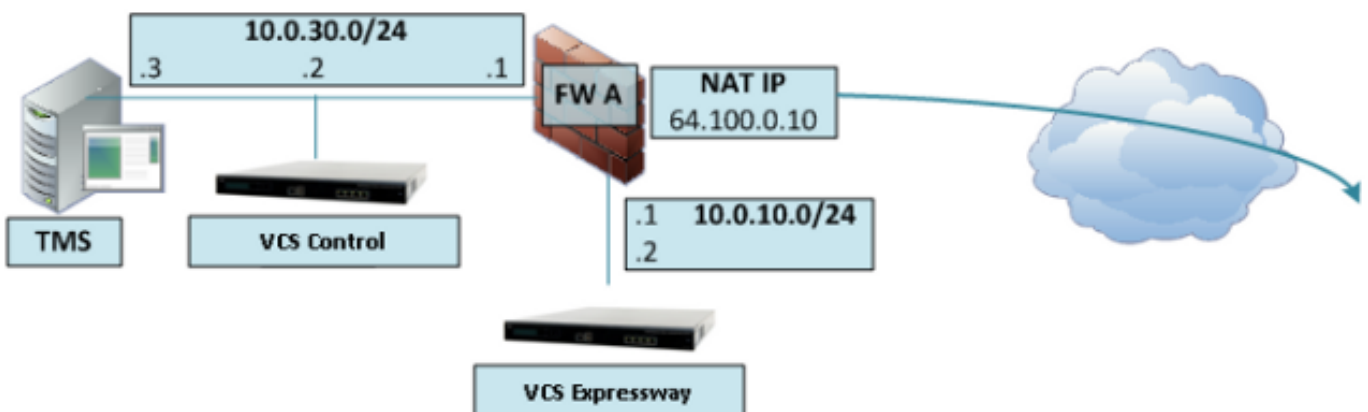
在本例中，FW B必须允许来自VCS控制为外部IP地址数据流的NAT反映(64.100.0.10)是注定的VCS Expressway。VCS控制的穿越区域必须有64.100.0.10作为对等体地址(在对IP转换的FQDN以后)。

应该配置有VCS Expressway 10.0.10.1默认网关。静态路由是否在此方案需要取决于FW A和FW B.功能和设置。从VCS控制的通信到VCS Expressway通过VCS发生Expressway的64.100.0.10 IP地址;并且从VCS Expressway的回程数据流对VCS控制也许必须通过默认网关通过。

VCS Expressway可以被添加到与IP地址10.0.10.3的Cisco TMS (或与IP地址64.100.0.10，如果FW B允许此)，因为Cisco TMS管理通讯没有受在VCS Expressway的静态NAT模式设置的影响。

## 与单个VCS Expressway LAN接口的3端口FW DMZ

这是此方案示例：



在此配置，3端口FW用于为了创建：

- 包含的DMZ子网(10.0.10.0/24)：  
DMZ接口FW A (10.0.10.1)VCS Expressway (10.0.10.2)的LAN1接口
- 包含的LAN子网(10.0.30.0/24)：  
LAN接口FW A (10.0.30.1)VCS控制(10.0.30.2)的LAN1接口Cisco TMS (10.0.30.3)的网络接口

静态一对一的NAT在FW A被配置了，执行公共NAT IP地址64.100.0.10对VCS Expressway的LAN1 IP地址。静态NAT模式为在VCS Expressway的LAN1接口启动了，用64.100.0.10的一个静态NAT IP地址。

应该配置有VCS Expressway 10.0.10.1默认网关。因为必须用于此网关离开VCS Expressway的所有数据流，静态路由在此种配置没有需要。

必须配置有VCS控制的穿越客户端区域匹配VCS Expressway的对等体地址(在本例中的64.100.0.10的)静态NAT地址原因的和在前一场景描述的那些一样。

**Note:**这意味着FW A必需允许从VCS控制的数据流与64.100.0.10的目的地IP地址。亦称这是NAT反映，并且值得注意的是，这不由FWs的所有类型支持。

VCS Expressway可以被添加到Cisco TMS用10.0.10.2的IP地址(或与IP地址64.100.0.10，如果FW A允许此)，因为Cisco TMS管理通讯没有受在VCS Expressway的静态NAT模式设置的影响。

## Configure

此部分描述如何配置在ASA的NAT反映两不同VCS C和E的实施方案。

### 与单个VCS Expressway LAN接口的单个子网DMZ

对于第一个方案，您必须运用在FW A的此NAT反映配置为了允许从被注定对外部IP地址的VCS控制(10.0.30.2)的通信(64.100.0.10)的VCS Expressway：



在本例中，VCS控制IP地址是10.0.30.2/24，并且VCS Expressway IP地址是10.0.10.3/24。

如果假设IP地址10.0.30.2 VCS的控制依然是，当从里面移动向FW B外部接口，当寻找与您您在FW B应该实现IP地址64.100.0.10的目的地，则时NAT反映配置的VCS Expressway在这些示例显示。

ASA版本8.3和以上的示例：

```
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和以下的示例：

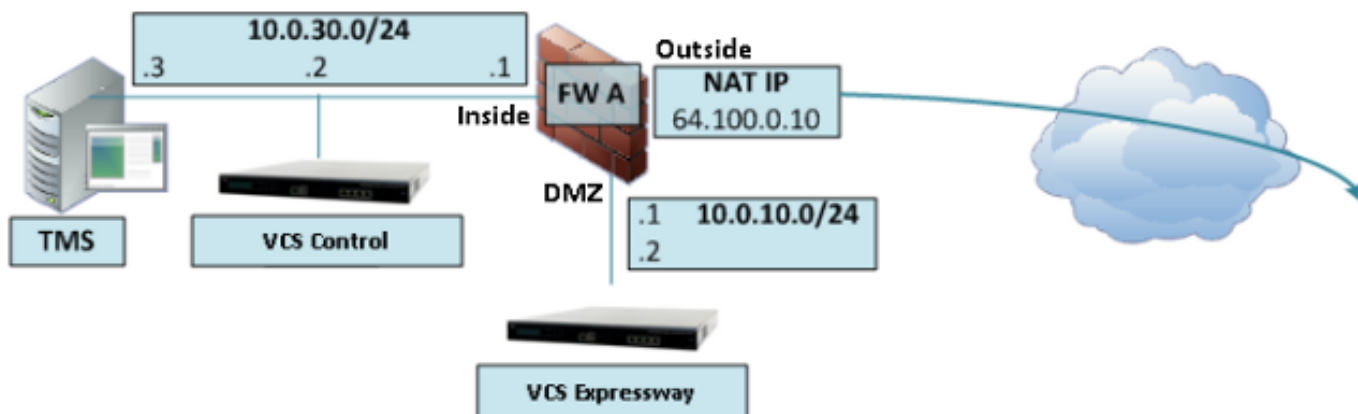
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10  
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
```

```
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
```

**Note:**此NAT反映配置主要目标将允许VCS控制能到达VCS高速公路，但是使用VCS高速公路公共IP地址而不是其专用IP地址。如果VCS控制的IP原地址在与一种NAT配置的此NAT转换时两次更改而不是显示的被建议的NAT配置，造成VCS Expressway看到从其自己的公共IP地址的数据流，则电话服务MRA设备的不会出现。这不是支持的配置根据关于下面推荐部分的第3部分。

## 与单个VCS Expressway LAN接口的3端口FW DMZ

对于第二个场景，您必须运用在FW A的此NAT反映配置为了允许Inbound数据流的NAT反映从被注  
定对外部IP地址的VCS控制10.0.30.2的(64.100.0.10)的VCS Expressway：



在本例中，VCS控制IP地址是10.0.30.2/24，并且VCS Expressway IP地址是10.0.10.2/24。

如果假设IP地址10.0.30.2 VCS的控制依然是，当从里面移动向FW A DMZ接口，当寻找与您在FW A应该实现IP地址64.100.0.10的目的地，则时NAT反映配置的VCS Expressway在这些示例显示。

ASA版本8.3和以上的示例：

```
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和以下的示例：

```
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
```

**Note:**此NAT反映配置主要目标将允许VCS控制能到达VCS高速公路，但是用VCS高速公路公共IP地址而不是其专用IP地址。如果VCS控制的IP原地址在与一种NAT配置的此NAT转换时两次更改而不是显示的被建议的NAT配置，造成VCS Expressway看到从其自己的公共IP地址的数据流，则电话服务MRA设备的不会出现。这不是支持的配置根据在下面推荐部分的第3部分

。

## Verify

此部分提供您在ASA在两个能看到为了确认NAT反映配置工作当必要时VCS C和E实施方案的信息包跟踪程序输出。

### 与单个VCS Expressway LAN接口的单个子网DMZ

这是为ASA版本8.3和以上输出的FW B信息包跟踪程序：

```
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

这是为ASA版本8.2和以下输出的FW B信息包跟踪程序：

**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
```

## 与单个VCS Expressway LAN接口的3端口FW DMZ

这是为ASA版本8.3和以上输出的FW A信息包跟踪程序：

```
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

这是为ASA版本8.2和以下输出的FW A信息包跟踪程序：

**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

您能配置在ASA接口的信息包获取为了确认NAT转换，当信息包进入并且离开是包含的FW接口时。

### 申请与单个VCS Expressway LAN接口”方案的”3端口FW信息包获取DMZ

```
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
```

申请“与单个VCS Expressway LAN接口”方案的信息包获取单个子网DMZ

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

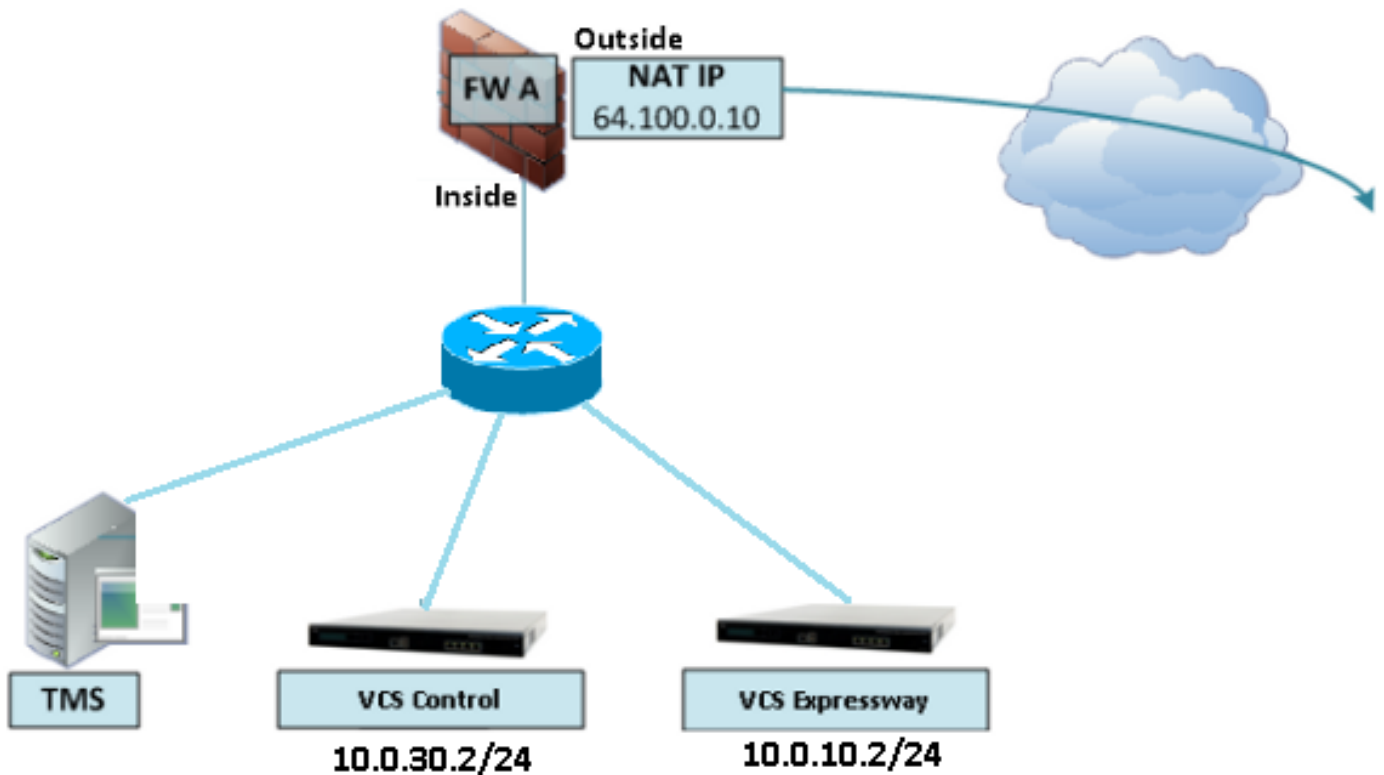
```
 1: 22:30:06.784871 10.0.30.2 > 10.0.10.3: icmp: echo request
 2: 22:30:06.847688 10.0.10.3 > 10.0.30.2: icmp: echo reply
 3: 22:30:06.878769 10.0.30.2 > 10.0.10.3: icmp: echo request
 4: 22:30:06.900557 10.0.10.3 > 10.0.30.2: icmp: echo reply
 5: 22:30:06.972758 10.0.30.2 > 10.0.10.3: icmp: echo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

## 推荐

### 1. 避免所有不支持的拓扑的实施

例如，如果有VCS控制和VCS在内部的ASA接口后被连接的Expressway，如此方案所显示，：



这种实施要求VCS控制IP地址被转换为ASA的内部的IP地址为了强制回程数据流回到ASA避免NAT反映的不对称的路由问题。

**Note:** 如果VCS控制的IP原地址在与一种NAT配置的此NAT转换时两次更改而不是被建议的NAT反映配置，则VCS Expressway将看到从其自己的公共IP地址的数据流，则MRA设备的电话服务不会出来。这不是支持的配置根据在下面推荐部分的第3部分。

它是高度推荐的实现VCS Expressway作为[ExpresswayE双重网络接口实施](#)而不是与NAT反映的单个NIC。

### 2. 保证SIP/H.323检查在介入的防火墙完全地被禁用

它是高度推荐的禁用SIP和H.323检查在处理网络流量到/从ExpresswayE的防火墙。当启用，SIP/H.323频繁地发现检查负影响Expressway内置的firewall/NAT穿越功能。

这是示例如何禁用SIP和H.323检验在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. 保证您的实际Expressway实施符合思科网真开发人员建议的下一个需求

- 不支持在ExpresswayC和ExpresswayE之间的NAT配置。
- 不支持它，当ExpresswayC和ExpresswayE，获得NAT对同样公共IP地址时，例如：  
ExpresswayC配置有IP地址10.1.1.1  
ExpresswayE有单个NIC配置有IP地址10.2.2.1，并且静态NAT在防火墙被配置用公共IP地址  
64.100.0.10  
然后ExpresswayC不可以是NATted到同一个公共地址64.100.0.10

## 推荐的VCS Expressway实施

VCS的Expressway推荐的实施而不是与NAT反映配置的VCS Expressway是双重网络接口/双NIC VCS Expressway实施，请欲知详情检查下条链路。

[ASA NAT配置和推荐对ExpresswayE双倍网络接口实施。](#)

## Related Information

- [ASA NAT配置和推荐对ExpresswayE双倍网络接口实施](#)
- [思科网真视频通信服务器基本配置\(与Expressway的控制\)部署指南](#)
- [Cisco Expressway IP防火墙穿越的端口使用方法](#)
- [安置Cisco VCS Expressway在DMZ而不是在公共互联网里](#)