在ASA上为VCS Expressway网真设备配置NAT反射

目录

简介

本文档介绍如何在思科自适应安全设备上为特殊思科网真场景实施网络地址转换(NAT)反射配置，这些场景需要在防火墙上进行此类NAT配置。

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。
- 思科网真视频通信服务器(VCS)控制和VCS Expressway基本配置。

注意：本文档仅在不能使用VCS-Expressway或Expressway-Edge的推荐部署方法（在不同

DMZ中同时具有两个NIC接口）时使用。有关使用双NIC的推荐部署的详细信息，请在第60页查看以下链接：Cisco TelePresence Video Communication Server基本配置（使用Expressway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 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：在整篇文档中，VCS设备称为VCS Expressway和VCS Control。但是，相同的配置适用于Expressway-E和Expressway-C设备。

背景信息

根据思科网真文档，有两种网真场景，其中需要在防火墙上配置NAT反射，以便VCS Control通过VCS Expressway公有IP地址与VCS Expressway通信。

第一种方案包括使用单个VCS Expressway LAN接口的单个子网非军事化区(DMZ)，第二种方案包括使用单个VCS Expressway LAN接口的3端口FW DMZ。

提示：要获取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。

VCS C和E实施不推荐的Cisco拓扑

请注意，思科不建议使用以下拓扑。VCS Expressway或Expressway边缘的建议部署方法是使用两个不同的DMZ，而Expressway在每个DMZ中都有网卡。本指南旨在用于无法使用推荐部署方法的环境。

单子网DMZ，带单个VCS Expressway LAN接口

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允许视频流量通过防火墙B，而不会减少防火墙B上从外部到内部接口的流量。VCS Expressway还处理其公共端的防火墙穿越。

以下是此场景的示例：

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的内部接口(10.0.10.1)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 Control(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

FW A上配置了静态一对一NAT，该NAT将公有地址64.100.0.10的NAT用于VCS Expressway的LAN1 IP地址。为VCS Expressway上的LAN1接口启用了静态NAT模式，静态NAT IP地址为64.100.0.10。

> **注意：**您必须在VCS Control安全穿越客户端区域（对等体地址）上输入VCS Expressway的完全限定域名(FQDN)，就像从网络外部看到它一样。其原因是，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，而不是其私有名称。这也意味着外部防火墙必须允许从VCS Control到VCS Expressway外部FQDN的流量。这称为NAT反射，可能并非所有类型的FW都支持。

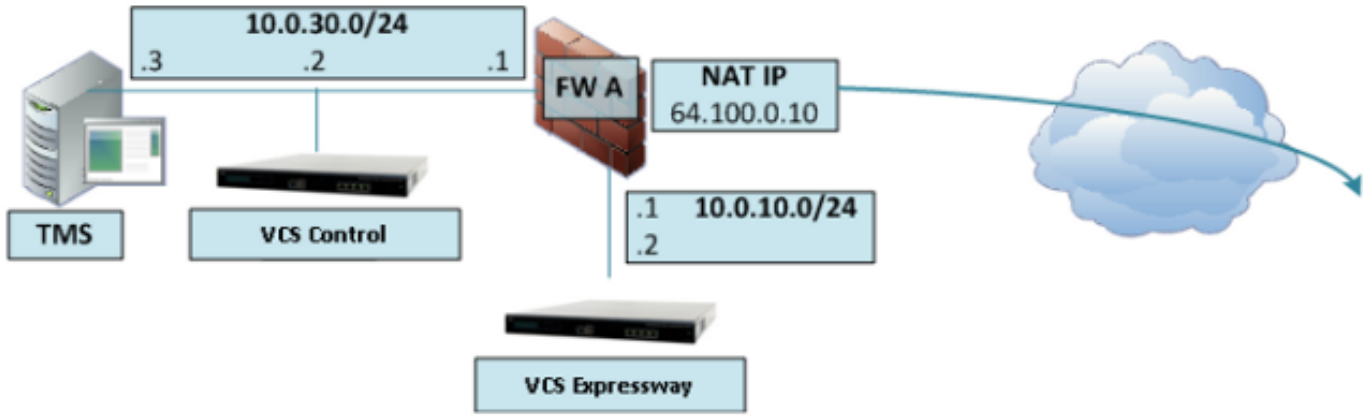
在本例中，FW B必须允许NAT反射来自VCS Control的流量，这些流量的目的地是VCS Expressway的外部IP地址(64.100.0.10)。VCS Control上的穿越区域必须具有64.100.0.10作为对等地址（在FQDN到IP转换后）。

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64.100.0.10 IP进行VCS Expressway的地址；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，则可以添加）的思科TMS，因为思科TMS管理通信不受VCS Expressway上静态NAT模式设置的影响。

带单个VCS Expressway LAN接口的3 — 口防火墙DMZ

以下是此场景的示例：



在此部署中，使用3端口FW创建：

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

FW A上配置了静态一对一NAT，该NAT将公有IP地址64.100.0.10的NAT用于VCS Expressway的LAN1 IP地址。为VCS Expressway上的LAN1接口启用了静态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，因此此类部署不需要静态路由。

VCS Control上的穿越客户端区域必须配置与VCS Expressway（本例中为64.100.0.10）的静态NAT地址匹配的对等地址，其原因与上一场景中描述的相同。

> **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，应注意，并非所有类型的FW都支持此功能。

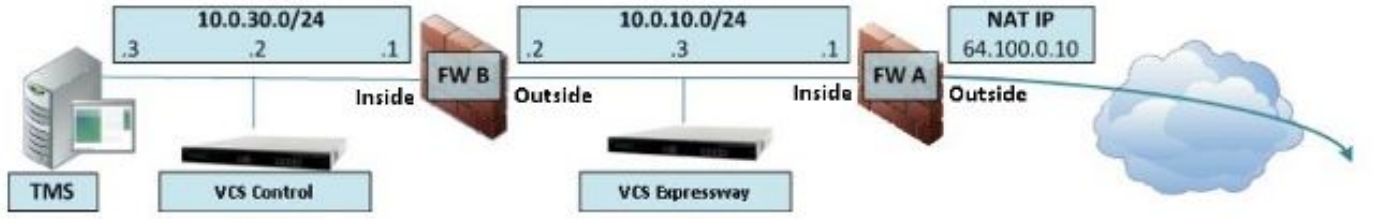
VCS Expressway可以添加到IP地址为10.0.10.2（或IP地址为64.100.0.10，如果FW A允许，则添加）的思科TMS，因为思科TMS管理通信不受VCS Expressway上静态NAT模式设置的影响。

配置

本节介绍如何在ASA中为两种不同的VCS C和E实施方案配置NAT反射。

单子网DMZ，带单个VCS Expressway LAN接口

对于第一个场景，您必须在FW A上应用此NAT反射配置，以便允许从VCS Control(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 Control IP地址**为10.0.30.2/24**,VCS Expressway IP地址**为10.0.10.3/24**。

如果在查找目标IP地址为64.100.0.10的VCS Expressway时，VCS Control IP地址10.0.30.2从防火墙B的内部接口移动到外部接口时仍保留，则本例中显示了您应在防火墙B上实施的NAT反射配置。

ASA 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 8.2及更低版本的示例：

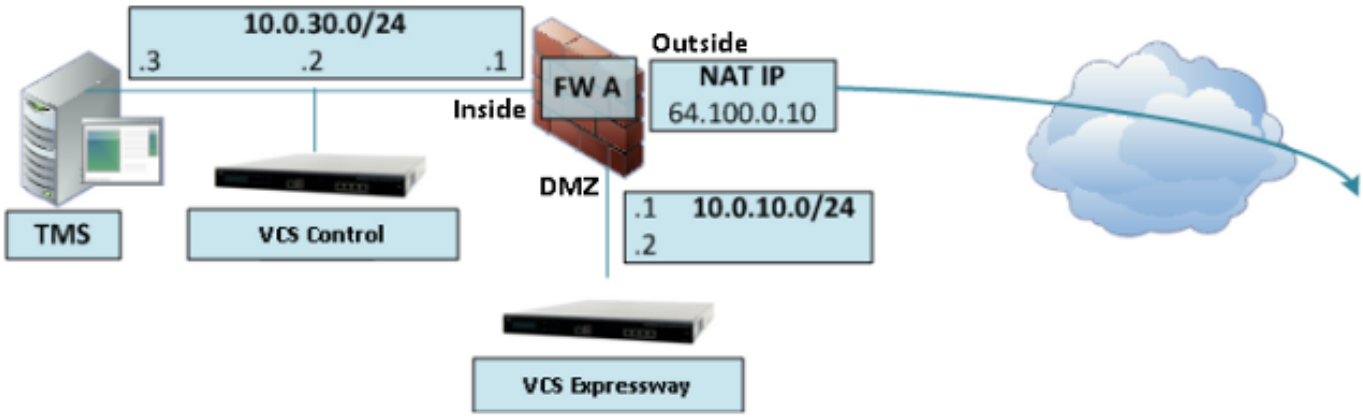
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

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 Control能够到达VCS Expressway，但使用VCS Expressway公有IP地址而不是其私有IP地址。如果在此NAT转换期间更改了VCS Control的源IP地址，并使用了两次NAT配置，而不是刚才显示的建议NAT配置，则VCS Expressway会看到来自其公有IP地址的流量，则MRA设备的电话服务将无法启动。根据以下建议部分的第3部分，这不是受支持的部署。

带单个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，以便允许NAT反射从VCS Control 10.0.30.2发往VCS Expressway的外部IP地址(64.100.0.10)的入站流量：



在本示例中，VCS Control IP地址**为10.0.30.2/24**,VCS Expressway IP地址**为10.0.10.2/24**。

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

ASA 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 8.2及更低版本的示例：

```
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 Control能够到达VCS Expressway，但使用VCS Expressway公有IP地址而不是其私有IP地址。如果在此NAT转换期间更改了VCS Control的源IP地址，而使用两次NAT配置，而不是刚才显示的建议NAT配置，则VCS Expressway会看到来自其公有IP地址的流量，则MRA设备的电话服务将不会启动。这不是以下建议部分第3部分中支持的部署。

验证

本部分提供您在ASA中可以看到的Packet Tracer输出，以确认NAT反射配置在VCS C和E实施场景中根据需要工作。

单子网DMZ，带单个VCS Expressway LAN接口

以下是ASA 8.3及更高版本的FW B数据包跟踪器输出：

```
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 8.2版及更低版本的FW B数据包跟踪器输出：

```
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
```

带单个VCS Expressway LAN接口的3 — 口防火墙DMZ

以下是ASA 8.3及更高版本的FW A packet tracer输出：

```
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 8.2版及更低版本的FW A packet tracer输出：

```
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，以便在数据包进入并离开相关的防火墙接口时确认NAT转换。

应用于“带单VCS Expressway LAN接口的3端口防火墙DMZ”场景的数据包捕获

```
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
```

应用于“带单VCS Expressway LAN接口的单子网DMZ”场景的数据包捕获

```
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)
```

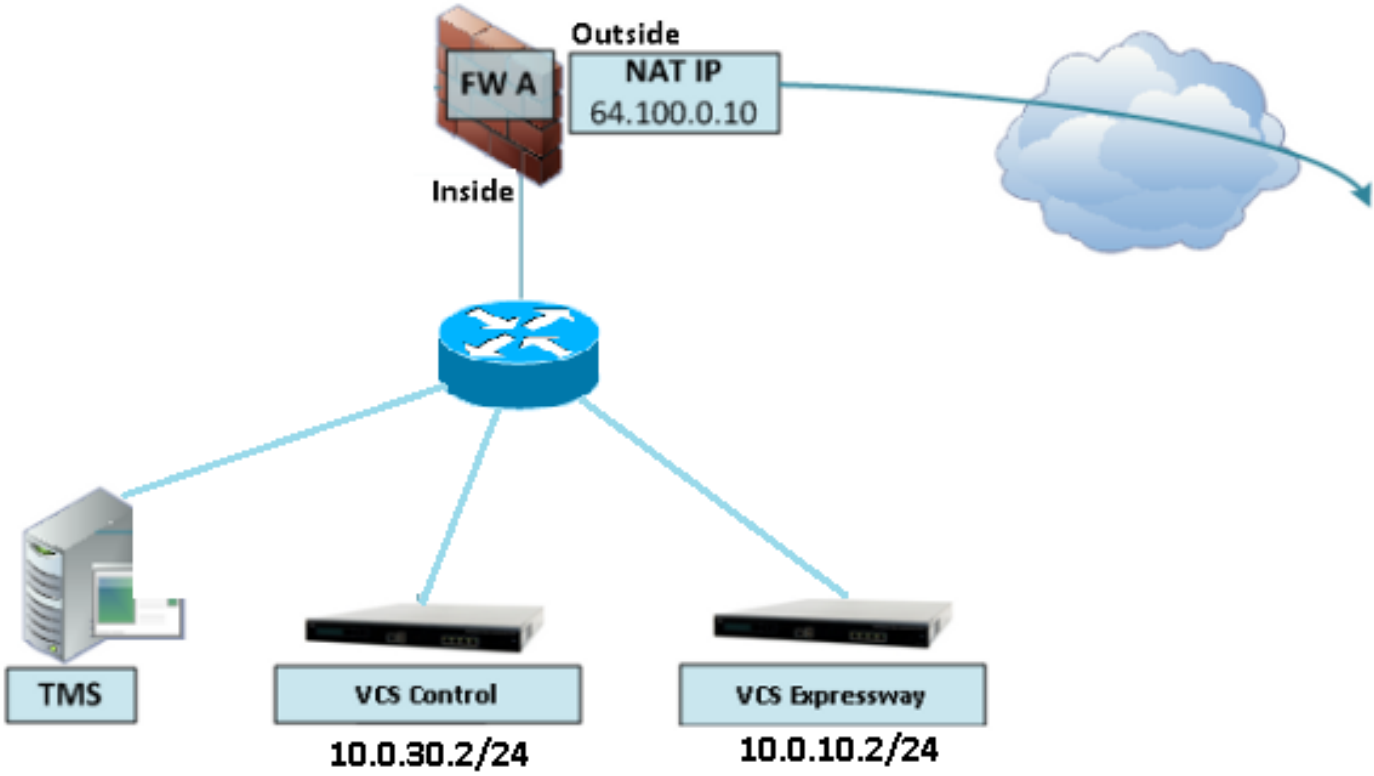
```
ack 1119515706 win 4116 20: 22:30:14.047788 64.100.0.10.23 > 10.0.30.2.41596: P
2006020262:2006020268(6)
ack 1119515706 win 4116 21: 22:30:14.052151 10.0.30.2.41596 > 64.100.0.10.23: P
1119515706:1119515709(3)
ack 2006020256 win 4076 22: 22:30:14.089183 10.0.30.2.41596 > 64.100.0.10.23: P
1119515709:1119515712(3)
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VCS Control和VCS Expressway都连接在内部ASA接口后，如以下场景所示：



这种实施要求将VCS Control IP地址转换为ASA的内部IP地址，以强制返回的流量返回到ASA，以避免NAT反射出现非对称路由问题。

> **注意：如果在此NAT转换期间使用两次NAT配置而不是建议的NAT反射配置更改了VCS Control的源IP地址，则VCS Expressway将看到来自其自己公有IP地址的流量，则MRA设备的电话服务将不会启动。这不是以下建议部分第3部分中支持的部署。**

尽管如此，强烈建议将VCS Expressway作为Expressway-E双网络接口实施，而不是使用带NAT反射的单个NIC实施。

2.确保在涉及的防火墙上完全禁用SIP/H.323检测

强烈建议在处理进出Expressway-E的网络流量的防火墙上禁用SIP和H.323检查。启用后，SIP/H.323检测经常会对Expressway内置防火墙/NAT穿越功能产生负面影响。

以下是如何在ASA上禁用SIP和H.323检测的示例。

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

3.确保您的实际Expressway实施符合思科网真开发人员建议的下一要求

- 不支持Expressway-C和Expressway-E之间的NAT配置。
- 当Expressway-C和Expressway-E将NAT转换到同一公有IP地址时，不支持此功能，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NIC，而且防火墙中配置了静态NAT，公有IP地址为64.100.0.10

然后，Expressway-C无法NAT到同一公有地址64.100.0.10

推荐的VCS Expressway实施

VCS Expressway的建议实施是双网络接口/双NIC VCS Expressway实施，而不是NAT反射配置的VCS Expressway。有关详细信息，请查看下一个链接。

ASA NAT配置和Expressway-E双网络接口实施建议。

相关信息

- Expressway-E双网络接口实施的ASA NAT配置和建议
- 思科网真视频通信服务器基本配置（使用Expressway控制）部署指南
- 防火墙穿越的Cisco Expressway IP端口使用
- 将Cisco VCS Expressway放置在DMZ中，而不是公共互联网中