在ASA上為VCS Expressway網真裝置配置NAT反射

目錄

簡介

本文檔介紹如何在思科自適應安全裝置上實施網路地址轉換(NAT)反射配置，以滿足需要在防火牆上進行此類NAT配置的特殊思科網真場景。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ASA（自適應安全裝置）基本NAT配置。
- Cisco TelePresence Video Communication Server(VCS)Control和VCS Expressway基本配置。

> **附註**：本文檔旨在僅在不能使用具有不同DMZ中的兩個NIC介面的VCS-Expressway或Expressway-Edge的推薦部署方法時使用。有關建議使用雙NIC進行部署的更多資訊，請檢視第60頁上的以下連結：《Cisco TelePresence Video Communication Server Basic Configuration(Control with Expressway)部署指南》

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本8.3及更高版本的Cisco ASA 5500和5500-X系列裝置。
- Cisco VCS版本X8.x及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

> **注意**:在整個文檔中，VCS裝置稱為VCS Expressway和VCS Control。但是，同樣的配置適用於Expressway-E和Expressway-C裝置。

背景資訊

根據Cisco TelePresence文檔，有兩種TelePresence場景需要在FW上配置NAT反射，以允許VCS Control通過VCS Expressway公共IP地址與VCS Expressway通訊。

第一個場景涉及使用單個VCS Expressway LAN介面的單個子網非軍事化區域(DMZ)，第二個場景涉及使用單個VCS Expressway LAN介面的3埠防火牆DMZ。

> **提示：**要獲取有關網真實施的更多詳細資訊，請參閱思科網真影片通訊伺服器基本配置（使用Expressway控制）部署指南。

不推薦用於VCS C和E實施的思科拓撲

必須注意的是，思科不推薦以下拓撲。VCS Expressway或Expressway邊緣的推薦部署方法是：使用兩個不同的DMZ，並且Expressway在每個DMZ中都有一個NIC。本指南適用於無法使用推薦部署方法的環境。

具有單VCS Expressway LAN介面的單子網DMZ

在此案例中，防火牆A可將流量路由到防火牆B（反之亦然）。 VCS Expressway允許影片流量通過FW B，而不會減少FW B上從外部到內部介面的流量。VCS Expressway還在其公共端處理FW遍歷。

以下是一個情境範例：

此部署使用以下元件：

- 包含下列內容的單個子網DMZ(10.0.10.0/24):
  防火牆A(10.0.10.1)的內部介面防火牆B(10.0.10.2)的外部介面VCS Expressway的LAN1介面(10.0.10.3)
- LAN子網(10.0.30.0/24)包含：
  防火牆B(10.0.30.1)的內部介面VCS控制元件的LAN1介面(10.0.30.2)思科網真管理伺服器(TMS)的網路介面(10.0.30.3)

在FW A上配置了一個靜態一對一NAT，該NAT將公有地址64.100.0.10轉換為VCS Expressway的LAN1 IP地址。VCS Expressway上的LAN1介面已啟用靜態NAT模式，靜態NAT IP地址為64.100.0.10。

> **附註**：您必須在VCS Control安全遍歷客戶端區域（對等體地址）上輸入VCS Expressway的完全限定域名(FQDN)，就像從網路外部看到的那樣。原因是在靜態NAT模式下，VCS Expressway請求將入站信令和媒體流量傳送到其外部FQDN，而不是其專用名稱。這也意味著外部FW必須允許從VCS Control到VCS Expressway外部FQDN的流量。這稱為NAT反射，所有型別的防火牆可能都不支援。

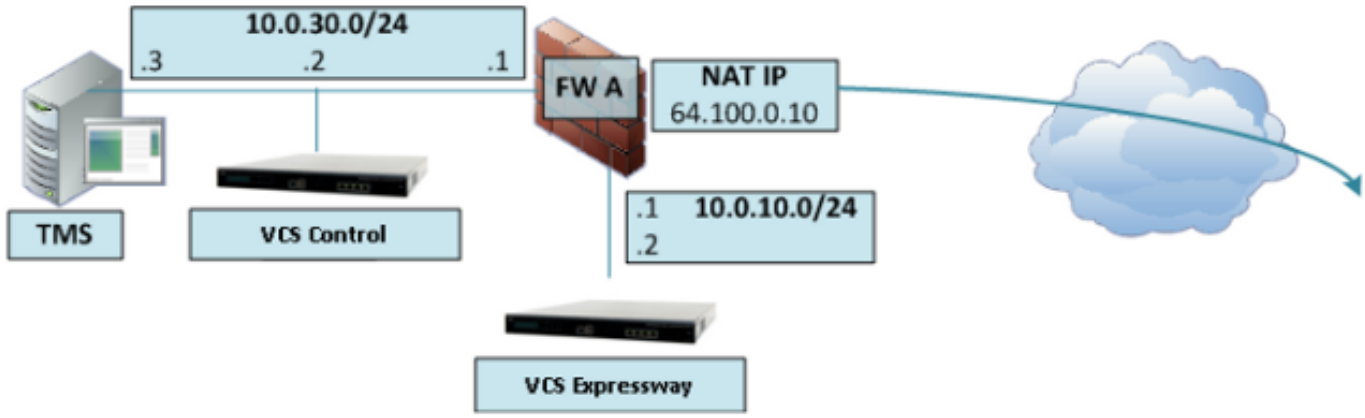
在本示例中，FW B必須允許來自VCS Control且目的地為VCS Expressway的外部IP地址(64.100.0.10)的流量的NAT反射。VCS控制元件上的遍歷區域必須將64.100.0.10作為對等體地址（在FQDN到IP轉換之後）。

VCS Expressway應配置預設網關**10.0.10.1**。此方案中是否需要靜態路由取決於防火牆A和防火牆B的功能和設定。從VCS控制到VCS Expressway的通訊通過VCS Expressway的64.100.0.10 IP地址進行；從VCS Expressway到VCS Control的返回流量可能必須通過預設網關。

VCS Expressway可以新增至IP地址為10.0.10.3的Cisco TMS（或者，如果FW B允許，則新增IP地址為64.100.0.10的），因為Cisco TMS管理通訊不會受到VCS Expressway上的靜態NAT模式設定的影響。

帶單VCS Expressway LAN介面的3埠防火牆DMZ

以下是一個情境範例：



在此部署中，使用3埠防火牆來建立：

- 一個DMZ子網(10.0.10.0/24)，它包含：
  防火牆A(10.0.10.1)的DMZ介面VCS Expressway的LAN1介面(10.0.10.2)
- LAN子網(10.0.30.0/24)包含：
  防火牆A(10.0.30.1)的LAN介面VCS控制元件的LAN1介面(10.0.30.2)思科TMS(10.0.30.3)的網路介面

在FW A上配置了靜態一對一NAT，該NAT將公共IP地址64.100.0.10轉換為VCS Expressway的LAN1 IP地址。VCS Expressway上的LAN1介面已啟用靜態NAT模式，靜態NAT IP地址為64.100.0.10。

VCS Expressway應配置預設網關10.0.10.1。由於此網關必須用於離開VCS Expressway的所有流量，因此這種部署型別不需要靜態路由。

由於與前面場景中描述的原因相同，VCS Control上的遍歷客戶端區域必須配置一個與VCS Expressway的靜態NAT地址（本示例中為64.100.0.10）匹配的對等地址。

> **附註**：這表示防火牆A必須允許來自目標IP地址為64.100.0.10的VCS控制的流量。這也稱為NAT反射，應該注意的是，並非所有型別的防火牆都支援此功能。

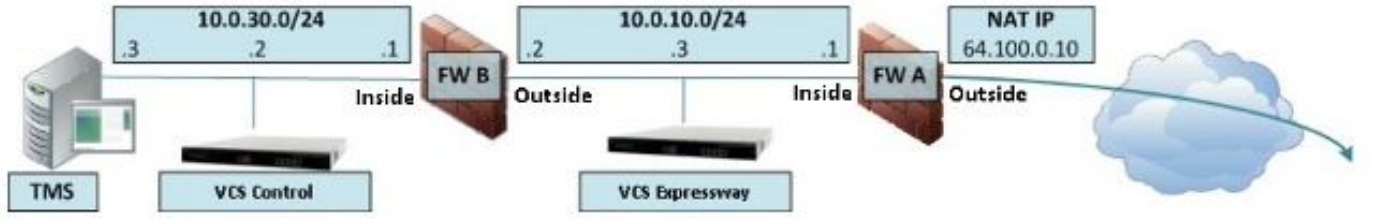
VCS Expressway可以新增到Cisco TMS中，IP地址為10.0.10.2（如果FW A允許，則其地址為64.100.0.10），因為Cisco TMS管理通訊不會受到VCS Expressway上的靜態NAT模式設定的影響。

設定

本節介紹如何為兩個不同的VCS C和E實施方案在ASA中配置NAT反射。

具有單VCS Expressway LAN介面的單子網DMZ

在第一個場景中，必須在FW A上應用此NAT反射配置，以允許從VCS控制元件(10.0.30.2)發往外部IP地址(64.100.0.10)的通訊：



在本示例中，VCS控制IP地址為**10.0.30.2/24**,VCS Expressway IP地址為**10.0.10.3/24**。

如果在查詢目標IP地址為64.100.0.10的VCS Expressway時，VCS控制IP地址10.0.30.2從防火牆B的內部介面移動到外部介面時仍保留，則您應在FW B上實施的NAT反射配置如以下示例所示。

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-10.0.10.3
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：

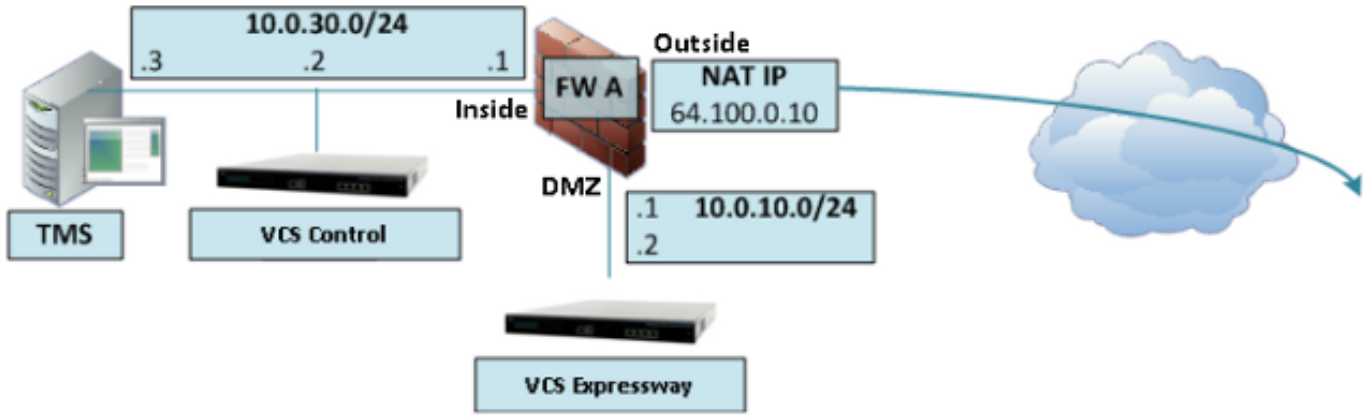
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

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
```

> **附註**：此NAT反射配置的主要目標是允許VCS控制能夠到達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轉換期間VCS控制元件的源IP地址使用兩次NAT配置而不是剛才所示的建議NAT配置進行更改，導致VCS Expressway看到來自其自己的公共IP地址的流量，則MRA裝置的電話服務將不會啟動。根據下文建議部分的第3節，這不是支援的部署。

帶單VCS Expressway LAN介面的3埠防火牆DMZ

對於第二個場景，必須在FW A上應用此NAT反射配置，以允許對來自VCS控制10.0.30.2且目的地為VCS Expressway外部IP地址(64.100.0.10)的入站流量進行NAT反射：



在本示例中，VCS控制IP地址為**10.0.30.2/24**,VCS Expressway IP地址為**10.0.10.2/24**。

如果在查詢目標IP地址為64.100.0.10的VCS Expressway時，VCS控制IP地址10.0.30.2從內部移動到FW A的DMZ介面時仍保留，則您應在FW A上實施的NAT反射配置如以下示例所示。

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
```

> **附註**：此NAT反射配置的主要目標是允許VCS控制能夠到達VCS Expressway，但使用VCS Expressway公有IP地址而不是其私有IP地址。如果VCS控制元件的源IP地址在此NAT轉換期間使用兩次NAT配置而不是剛剛顯示的建議的NAT配置發生了更改，導致VCS Expressway看到來自其自己的公共IP地址的流量，則MRA裝置的電話服務將不會啟動。根據下文建議部分的第3節，這不是支援的部署。

驗證

本節提供在ASA中看到的Packet Tracer輸出，以確認NAT反射配置在VCS C和E實施方案中均根據需要工作。

具有單VCS Expressway LAN介面的單子網DMZ

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

```
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及更低版本的FW B Packet Tracer輸出：

```
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
```

帶單VCS Expressway LAN介面的3埠防火牆DMZ

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

```
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及更低版本的FW A Packet Tracer輸出：

```
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
```

疑難排解

您可以在ASA介面上配置資料包捕獲，以便在資料包進入和離開所涉及的FW介面時確認NAT轉換。

資料包捕獲應用於「使用單個VCS Expressway LAN介面的3埠防火牆DMZ」方案

```
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
```

資料包捕獲應用於「使用單個VCS Expressway LAN介面的單個子網DMZ」方案

```
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
```

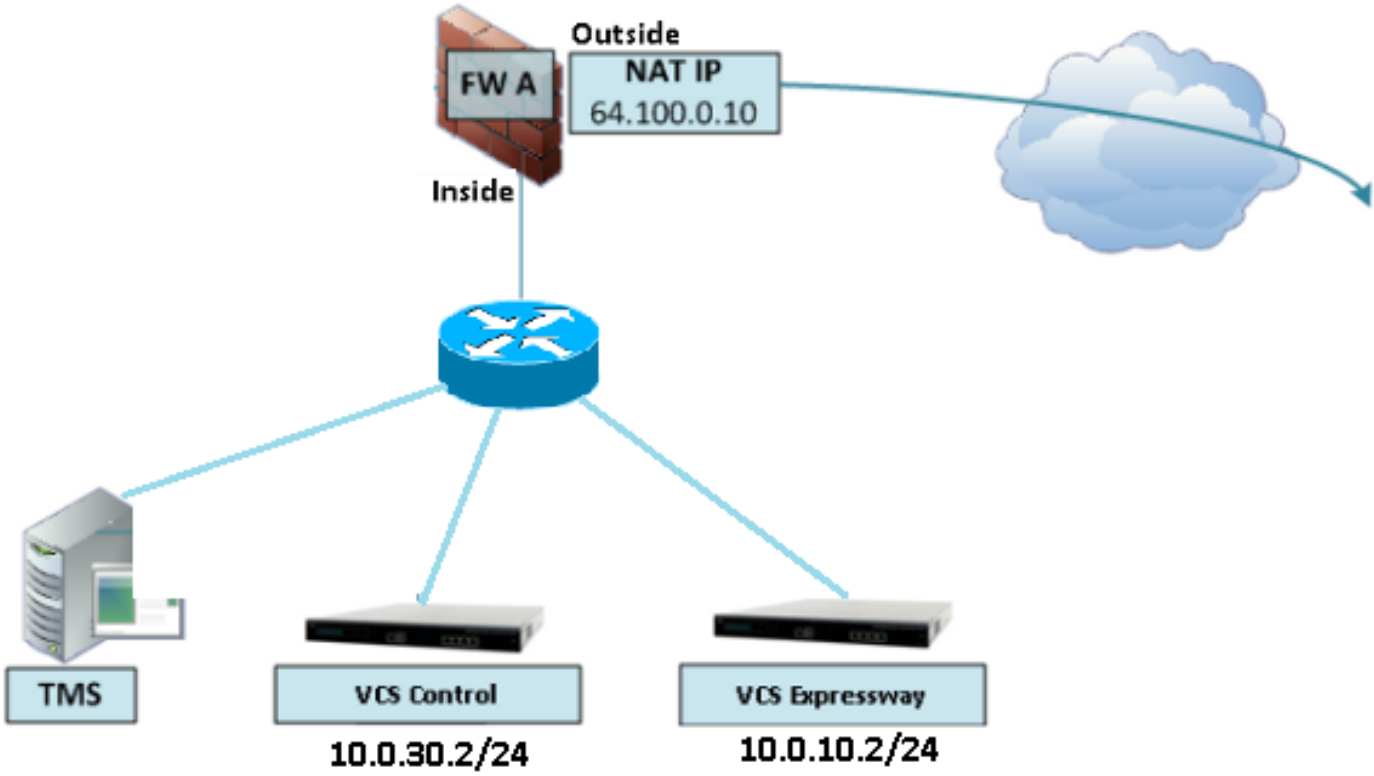
```
2006020262:2006020268(6)
ack 1119515706 win 4116 21: 22:30:14.052151 10.0.30.2.41596 > 64.100.0.10.23: P
1119515706:1119515709(3)
ack 2006020256 win 4076 22: 22:30:14.089183 10.0.30.2.41596 > 64.100.0.10.23: P
1119515709:1119515712(3)
ack 2006020256 win 4076
ASA1# show cap capout

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
```

建議

1.避免實施任何不受支援的拓撲

例如，如果您在內部ASA介面後面同時連線VCS Control和VCS Expressway，如下例所示：



這種實施需要將VCS控制IP地址轉換為ASA的內部IP地址，以強制返回流量返回ASA，從而避免NAT反射出現非對稱路由問題。

> **注意：如果VCS控制元件的源IP地址在此NAT轉換期間使用兩次NAT配置而不是建議的NAT反射配置進行了更改，則VCS Expressway將看到來自其自己的公共IP地址的流量，MRA裝置的電話服務將不會啟動。根據下文建議部分的第3節，這不是支援的部署。**

也就是說，強烈建議將VCS Expressway實施為Expressway-E雙網路介面實施，而不是採用NAT反射的單個NIC。

2.確保在涉及的防火牆上完全禁用SIP/H.323檢測

強烈建議在處理Expressway-E來往網路流量的防火牆上禁用SIP和H.323檢測。啟用時，經常發現SIP/H.323檢測會對Expressway內建防火牆/NAT遍歷功能產生負面影響。

以下示例說明如何在ASA上禁用SIP和H.323檢測。

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

3.確保實際的Expressway實施符合思科網真開發人員建議的下一個要求

- 不支援Expressway-C和Expressway-E之間的NAT配置。
- 當Expressway-C和Expressway-E將NAT設定為相同的公共IP地址時，不支援此功能，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的單個NIC，並且在防火牆中配置了一個靜態NAT，其公有IP地址為64.100.0.10
因此Expressway-C不能通過NAT連線到相同的公有地址64.100.0.10

建議的VCS Expressway實施

建議採用VCS Expressway實施方式而不是採用NAT反射配置的VCS Expressway實施方式是雙網路介面/雙NIC VCS Expressway實施，有關詳細資訊，請檢查下一連結。

ASA NAT配置和Expressway-E雙網路介面實施建議。

相關資訊

- 適用於Expressway-E雙網路介面實施的ASA NAT配置和建議
- 思科網真影片通訊伺服器基本配置（使用Expressway進行控制）部署指南
- 用於防火牆穿越的Cisco Expressway IP埠使用
- 將Cisco VCS Expressway放在DMZ中而不是公共網際網路中