ASA NAT配置和Expressway-E雙網路介面實施建議

目錄

簡介

本文檔介紹如何實施Expressway-E雙網路介面實施所需的思科自適應安全裝置(ASA)中的網路地址轉換(NAT)配置。

提示：對於Expressway-E實施，此部署是推薦選項，而不是採用NAT反射的單NIC實施。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ASA基本配置和NAT配置
- Cisco Expressway-E和Expressway-C基本配置

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8.0及更高版本的Cisco ASA 5500和5500-X系列裝置。
- Cisco Expressway 8.0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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

> **註**：在整篇文檔中，expressway裝置稱為Expressway-E和Expressway-C。但是，同一配置適用於影片通訊伺服器(VCS)Expressway和VCS控制裝置。

背景資訊

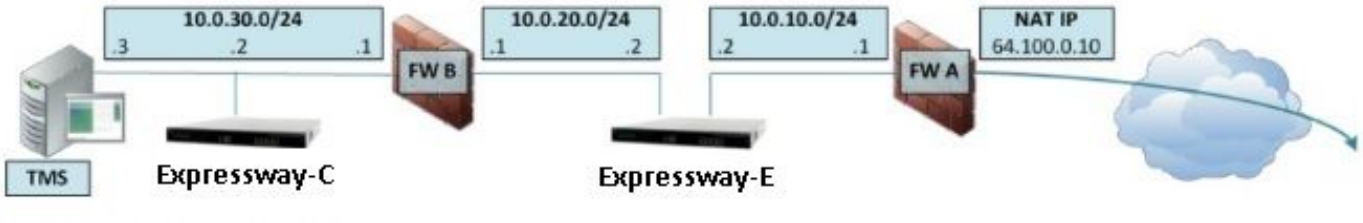
根據設計，Cisco Expressway-E可置於非軍事區(DMZ)或具有面向網際網路的介面，同時可在專用網路中與Cisco Expressway-C通訊。將Cisco Expressway-E置於DMZ中時，還有以下優勢：

- 在最常見的情況下，Cisco Expressway-E由專用網路管理。當Cisco Expressway-E在DMZ中時，可以使用邊界（外部）防火牆阻止通過超文本傳輸協定安全(HTTPS)或安全外殼(SSH)請求從外部網路不需要的訪問Expressway。
- 如果DMZ不允許內部和外部網路之間的直接連線，則需要專用伺服器來處理通過DMZ的流量。Cisco Expressway可以作為會話發起協定(SIP)和/或H.323語音和影片流量的代理伺服器。在這種情況下，您可以使用雙網路介面選項，該選項允許Cisco Expressway具有兩個不同的IP地址，一個用於進出外部防火牆的流量，另一個用於進出內部防火牆的流量。
- 此設定防止從外部網路直接連線到內部網路。這提高了整個內部網路的安全性。

> **提示：**要獲取有關TelePresence實施的更多詳細資訊，請參閱Cisco Expressway-E和Expressway-C — 基本配置部署指南和將Cisco VCS Expressway放置在DMZ中而不是放置在公共網際網路中。

Expressway C和E — 雙網路介面/雙NIC實施

此圖顯示了具有雙網路介面和靜態NAT的Expressway-E的部署示例。Expressway-C充當穿越客戶端。有兩個防火牆（FW A和FWB）。 通常，在該DMZ配置中，防火牆A無法將流量路由到防火牆B，並且需要Expressway-E等裝置來驗證流量並將其從防火牆A的子網轉發到防火牆B的子網（反之亦然）。



此部署包含以下元件。

DMZ子網1 - 10.0.10.0/24

- FW A內部介面 — 10.0.10.1
- Expressway-E LAN2介面 — 10.0.10.2

DMZ子網2 - 10.0.20.0/24

- 防火牆B外部介面 — 10.0.20.1
- Expressway-E LAN1介面 — 10.0.20.2

LAN子網 — 10.0.30.0/24

- 防火牆B內部介面 — 10.0.30.1
- Expressway-C LAN1介面 — 10.0.30.2
- Cisco TelePresence管理套件(TMS)伺服器網路介面 — 10.0.30.3

此實施的具體資訊：

- 防火牆A是外部或外圍防火牆；它配置了64.100.0.10（公共IP）的NAT IP（公共IP），靜態轉換為10.0.10.2（Expressway-E LAN2介面）
- FW B是內部防火牆
- Expressway-E LAN1已禁用靜態NAT模式
- Expressway-E LAN2已啟用靜態NAT模式，靜態NAT地址為64.100.0.10
- Expressway-C具有指向10.0.20.2（Expressway-E LAN1介面）的遍歷客戶端區域
- 10.0.20.0/24和10.0.10.0/24子網之間沒有路由。Expressway-E橋接這些子網並充當SIP/H.323信令和即時傳輸協定(RTP)/RTP控制協定(RTCP)介質的代理。
- Cisco TMS為Expressway-E配置了IP地址10.0.20.2

要求/限制

非重疊子網

如果將Expressway-E配置為使用兩個LAN介面，則LAN1和LAN2介面必須位於非重疊子網中，以確保將流量傳送到正確的介面。

集群

當集群配置了高級網路選項的Expressway裝置時，每個集群對等裝置都需要配置其自己的LAN1介面地址。此外，必須在未啟用靜態NAT模式的介面上配置集群。因此，建議使用LAN2作為外部介面，您可以在該介面上應用和配置靜態NAT（如果適用）。

外部LAN介面設定

IP配置頁面上的外部LAN介面配置設定控制哪個網路介面使用繞過NAT的中繼的橫向連線(TURN)。在雙網路介面Expressway-E配置中，這通常設定為Expressway-E外部LAN介面。

靜態路由

此場景的Expressway-E必須配置預設網關地址10.0.10.1。這表示預設情況下，所有通過LAN2發出的流量都會傳送到IP地址10.0.10.1。

如果FW B將從10.0.30.0/24子網傳送的流量轉換為Expressway-E LAN1介面（例如，Expressway-C穿越客戶端流量或TMS伺服器管理流量），則當該流量到達Expressway-E LAN1時，該流量將顯示為來自FWB外部介面(10.0.20.1)。然後，Expressway-E可以通過其LAN1介面回覆該流量，因為該流量的明顯來源位於同一子網上。

如果在FW B上啟用了NAT，則從Expressway-C傳送到Expressway-E LAN1的流量將顯示為來自10.0.30.2。如果Expressway沒有為10.0.30.0/24子網新增靜態路由，則會將此流量的應答從LAN2傳送到其預設網關(10.0.10.1)，因為它不知道10.0.30.0/24子網位於內部防火牆(FW B)的後面。 因此，需要新增靜態路由，請通過SSH**會話運**行xCommand RouteAdd CLI命令到Expressway。

在此特定示例中，Expressway-E必須知道可以到達FW B後面的10.0.30.0/24子網，該子網可通過LAN1介面訪問。要完成此操作，請運行命令：

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

> **註**:S可以通過Expressway-E GUI以及**System/Network > Interfaces/Static Routes**部分應用靜態路由配置。

在本範例中，介面引數也可以設定為**自動**，因為閘道位址(10.0.20.1)只能透過LAN1到達。

如果在防火牆B上未啟用NAT，並且Expressway-E需要與也位於防火牆B後面的子網(10.0.30.0/24除外)中的裝置通訊，則必須為這些裝置/子網新增靜態路由。

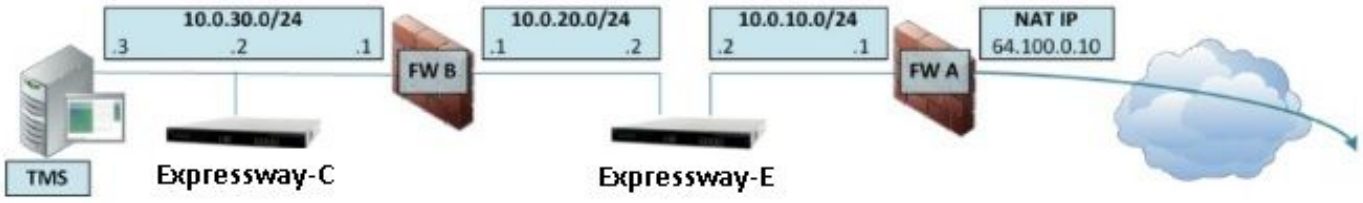
> **附註**：其中包括 來自網路管理工作站的SSH和HTTPS連線，或用於網路服務（如NTP、DNS、LDAP/AD或Syslog）。

xCommand **RouteAdd命令**和語法在《VCS管理員指南》中進行了詳細描述。

組態

本節介紹如何在ASA上配置Expressway-E雙網路介面實施所需的靜態NAT。包括一些用於處理SIP/H323流量的其他ASA模組化策略框架(MPF)配置建議。

Expressway C和E — 雙網路介面/雙NIC實施



在本示例中，IP地址分配是下一個分配。

Expressway-C IP地址：10.0.30.2/24

Expressway-C default-gateway:10.0.30.1(FW-B)

Expressway-E IP地址：

在LAN2上：10.0.10.2/24

在LAN1上：10.0.20.2/24

Expressway-E預設網關：10.0.10.1(FW-A)

TMS IP地址：10.0.30.3/24

FW-A配置

步驟1. Expressway-E的靜態NAT配置。

如本文檔的背景資訊部分所述，FW-A具有靜態NAT轉換，以允許從公共IP地址為64.100.0.10的網際網路訪問Expressway-E。最後一個NAT到Expressway-E LAN2 IP地址10.0.10.2/24。也就是說，這是所需的FW-A靜態NAT配置。

對於ASA 8.3及更高版本：

```
! To use PAT with specific ports range:

object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
(inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
obj-udp_5061 OR ! To use with static one-to-one NAT: object network obj-10.0.10.2 nat
(inside,outside) static interface
```

注意:應用靜態PAT命令時，您在ASA命令列介面上收到此錯誤消息「**ERROR:NAT無法保留**

埠」。 執行此操作後，繼續清除ASA上的xlate條目，為此，請運行命令**clearxlatelocal x.x.x.x**，其中x.x.x.x對應於ASA外部IP地址。此命令將清除與此IP地址關聯的所有轉換，在生產環境中運行該命令時應謹慎。

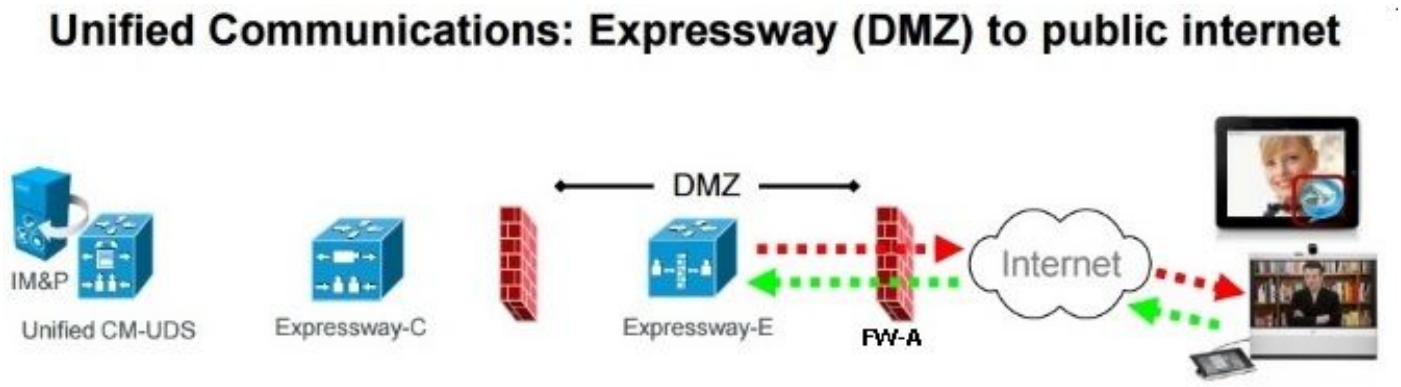
對於ASA 8.2及更低版本：

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

步驟2.訪問控制清單(ACL)配置允許從Internet到Expressway-E所需的埠。

根據統一通訊：Expressway(DMZ)到公共Internet文檔中，Expressway-E要求在FW-A中允許的TCP和UDP埠清單如下圖所示：



		Expressway-E source port	Internet endpoint server (listening) port	Expressway-E server (listening) port	Internet endpoint source port
Message direction		Outbound to an endpoint in the Internet		Inbound from an endpoint in the Internet	
Open firewall		DMZ to Internet		Internet to DMZ	
IP address		Address of Expressway-E	Any IP address	Address of Expressway-E	Any IP address
IP Ports	XMPP (IM and Presence)	n/a	n/a	TCP *5222*	TCP **S** *>= 1024*
	UDS (phonebook and provisioning)	n/a	n/a	TCP *8443*	TCP **S** *>= 1024*
	TURN server control / media	n/a	n/a	UDP *3478 (to 3483)* **R** / *24000 to 29999*	UDP **S** *>= 1024*
	SIP signaling	TLS *25000 to 29999*	TLS **S** *>= 1024*	TLS *5061*	TLS **S** *>= 1024*
	SIP media	UDP Y_E *36002 to 59999 **	UDP **N** *>= 1024*	UDP Y_E *36002 to 59999 **	UDP **N** *>= 1024*

N = Expressway waits until it receives media, then it sends its media to the IP port from which the media was received (egress port of the media from the far end non SIP-aware firewall): any port *>= 1024*

R = On Large VM server deployments you can configure a range of TURN request listening ports

S = Source port , typically >= 1024

Y_E = Local Zone > Traversal Subzone > Traversal Media port start to end (configured on Expressway-E): *default = 36000 to 59999* *

* The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

這是FW-A外部介面中作為入站所需的ACL配置。

對於ASA 8.3及更高版本：

```
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
access-list outside-in extended permit udp any host 10.0.10.2 lt 3484
access-list outside-in extended permit udp any host 10.0.10.2 gt 23999
```

```
access-list outside-in extended permit udp any host 10.0.10.2 lt 30000
access-list outside-in extended permit udp any host 10.0.10.2 gt 36001
access-list outside-in extended permit udp any host 10.0.10.2 lt 60000
access-list outside-in extended permit udp any host 10.0.10.2 eq 5061
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061

access-group outside-in in interface outside
```

對於ASA 8.2及更低版本：

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5222
access-list outside-in extended permit tcp any host 64.100.0.10 eq 8443
access-list outside-in extended permit udp any host 64.100.0.10 gt 3477
access-list outside-in extended permit udp any host 64.100.0.10 lt 3484
access-list outside-in extended permit udp any host 64.100.0.10 gt 23999
access-list outside-in extended permit udp any host 64.100.0.10 lt 30000
access-list outside-in extended permit udp any host 64.100.0.10 gt 36001
access-list outside-in extended permit udp any host 64.100.0.10 lt 60000
access-list outside-in extended permit udp any host 64.100.0.10 eq 5061
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5061

access-group outside-in in interface outside
```

FW-B配置

如本文背景資訊一節所述，FW B可能需要動態NAT或PAT配置，以允許內部子網10.0.30.0/24在進入FW B的外部介面時轉換為IP地址10.0.20.1。

對於ASA 8.3及更高版本：

```
object network obj-10.0.30.0
   subnet 10.0.30.0 255.255.255.0
   nat (inside,outside) dynamic interface
```

對於ASA 8.2及更低版本：

```
nat (inside) 1 10.0.30.0 255.255.255.0
global (outside) 1 interface
```

> **提示**：確保所有所需的TCP和UDP埠都允許Expressway-C正常工作並在防火牆B中開啟，如思科文檔Cisco Expressway IP Port Usage for Firewall Traversal中所指定

驗證

使用本節內容，確認您的組態是否正常運作。

可以在ASA上使用Packet Tracer來確認Expressway-E靜態NAT轉換是否按要求工作。

Packet Tracer測試64.100.0.10的TCP/5222

```
FW-A#packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5222

Phase: 1
Type: UN-NAT
```

```
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5222 to 10.0.10.2/5222

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 13, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Packet Tracer測試64.100.0.10的TCP/8443

```
FW-A# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 8443

Phase: 1
```

```
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/8443 to 10.0.10.2/8443

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 14, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Packet Tracer測試64.100.0.10的TCP/5061

```
FW-1# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5061
```

```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5061 to 10.0.10.2/5061

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 15, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Packet Tracer測試64.100.0.10的UDP/24000

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 24000
```

```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/24000 to 10.0.10.2/24000

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 16, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

Packet Tracer測試64.100.0.10的UDP/36002

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 36002

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/36002 to 10.0.10.2/36002

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 17, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
```

疑難排解

步驟1.比較封包擷取。

資料包捕獲可以在ASA入口和出口介面上執行。

```
FW-A# sh cap
capture capout interface outside match ip host 64.100.0.100 host 64.100.0.10
capture capin interface inside match ip host 64.100.0.100 host 10.0.10.2
```

TCP/5222上64.100.0.10的資料包捕獲：

```
FW-A# sh cap capout

2 packets captured
   1: 21:39:33.646954 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
   2: 21:39:35.577652 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
2 packets shown

FW-A# sh cap capin

2 packets captured
   1: 21:39:33.647290 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
   2: 21:39:35.577683 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
2 packets shown
```

TCP/5061上針對64.100.0.10的資料包捕獲：

```
FW-A# sh cap capout
2 packets captured

   1: 21:42:14.920576 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
   2: 21:42:16.992380 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
2 packets shown
FW-A# sh cap capin 2 packets captured 1: 21:42:14.920866 64.100.0.100.50820 > 10.0.10.2.5061: S
2082904361:2082904361(0) win 4128 <mss 1380> 2: 21:42:16.992410 64.100.0.100.50820 >
10.0.10.2.5061: S 2082904361:2082904361(0) win 4128 <mss 1380> 2 packets shown
```

步驟2.檢查加速安全路徑(ASP)丟棄資料包捕獲。

ASA的丟包由ASA ASP捕獲捕獲。**all**選項可擷取ASA捨棄封包的所有可能原因。如有任何可疑原因，可以縮小範圍。有關ASA對這些丟棄進行分類的原因清單，請運行**show asp drop命令。**

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

提示：在此方案中，使用ASA ASP捕獲來確認ASA是否由於遺漏的ACL或NAT配置而丟棄資料包，而後者需要為Expressway-E開啟特定的TCP或UDP埠。

提示：每個ASA捕獲的預設緩衝區大小為512 KB。如果ASA丟棄的資料包太多，緩衝區將快速填充。可以使用**buffer**選項增加緩衝區大小。

建議

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
```

替代VCS Expressway實施

使用雙網路介面/雙NIC實施Expressway-E的另一種解決方案是在防火牆上實施單NIC和NAT反射配置。下一個連結顯示有關此實現的詳細資訊在ASA上為VCS Expressway TelePresence裝置配置NAT反射。

提示：VCS Expressway的建議實施是本文檔中介紹的雙網路介面/雙NIC VCS Expressway實施。

相關資訊

- 在ASA上為VCS Expressway TelePresence裝置配置NAT反射
- 技術支援與文件 - Cisco Systems
- Cisco Expressway-E和Expressway-C — 基本配置部署指南
- 將Cisco VCS Expressway放在DMZ中而不是公共網際網路中
- 用於防火牆穿越的Cisco Expressway IP埠使用