ASA NAT配置和Expressway E双网络接口实施建议

目录

简介

本文档介绍如何实施思科自适应安全设备(ASA)中为Expressway-E双网络接口实施所需的网络地址转换(NAT)配置。

提示：此部署是推荐用于Expressway-E实施的选项，而不是使用NAT反射的单NIC实施。

先决条件

要求

Cisco 建议您了解以下主题：

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

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8.0及更高版本的Cisco ASA 5500和5500-X系列设备。
- Cisco Expressway X8.0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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

> 注意:**在整个文档中，Expressway设备称为Expressway-E和Expressway-C。但是，视频通信服务器(VCS)Expressway和VCS控制设备的配置也相同。**

背景信息

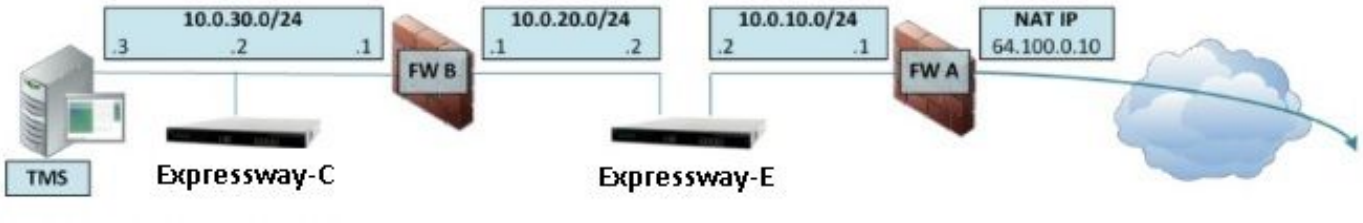
根据设计，Cisco Expressway-E可以放置在非军事区(DMZ)或面向互联网的接口中，同时能够与专用网络中的Cisco Expressway-C通信。当Cisco Expressway-E放置在DMZ中时，以下是额外优势：

- 在最常见的场景中，Cisco Expressway-E由专用网络管理。当Cisco Expressway-E位于DMZ中时，可使用边界（外部）防火墙阻止外部网络通过超文本传输协议安全(HTTPS)或安全外壳(SSH)请求对Expressway进行不需要的访问。
- 如果DMZ不允许内部网络和外部网络之间直接连接，则需要专用服务器来处理通过DMZ的流量。Cisco Expressway可充当会话初始协议(SIP)和/或H.323语音和视频流量的代理服务器。在这种情况下，您可以使用双网络接口选项，该选项允许Cisco Expressway有两个不同的IP地址，一个用于进出外部防火墙的流量，另一个用于进出内部防火墙的流量。
- 此设置可防止从外部网络直接连接到内部网络。这整体上提高了内部网络安全。

  提示：要获取有关网真实施的更多详细信息，请参阅Cisco Expressway-E和Expressway-C — 基本配置部署指南和将Cisco VCS Expressway放置在DMZ中，而不是公共互联网中。

Expressway C和E — 双网络接口/双NIC实施

此图显示了带双网络接口和静态NAT的Expressway-E的部署示例。Expressway-C用作穿越客户端。有两个防火墙（FW A和FWB）。 通常，在此DMZ配置中，防火墙A无法将流量路由到防火墙B，并且需要Expressway-E等设备来验证流量并将流量从防火墙A的子网转发到防火墙B的子网（反之亦然）。



此部署包括这些组件。

DMZ子网1 - 10.0.10.0/24

- 防火墙A内部接口 — 10.0.10.1
- Expressway-E LAN2接口 — 10.0.10.2

DMZ子网2 - 10.0.20.0/24

- 防火墙B外部接口 — 10.0.20.1
- Expressway-E LAN1接口 — 10.0.20.2

LAN子网 — 10.0.30.0/24

- 防火墙B内部接口 — 10.0.30.1
- Expressway-C LAN1接口 — 10.0.30.2
- 思科网真管理套件(TMS)服务器网络接口 — 10.0.30.3

此实施的具体内容：

- 防火墙A是外部或外围防火墙；它配置了NAT IP（公有IP）64.100.0.10，静态转换为10.0.10.2（Expressway-E LAN2接口）
- 防火墙B是内部防火墙
- Expressway-E LAN1禁用了静态NAT模式
- Expressway-E LAN2启用了静态NAT模式，静态NAT地址为64.100.0.10
- Expressway-C有一个指向10.0.20.2（Expressway-E LAN1接口）的穿越客户端区域
- 10.0.20.0/24和10.0.10.0/24子网之间没有路由。Expressway-E桥接这些子网，并充当SIP/H.323信令和实时传输协议(RTP)/RTP控制协议(RTCP)媒体的代理。
- 思科TMS已为Expressway-E配置IP地址10.0.20.2

要求/限制

非重叠子网

如果Expressway-E配置为同时使用两个LAN接口，则LAN1和LAN2接口必须位于不重叠的子网中，以确保流量发送到正确的接口。

集群

在配置了Advanced Networking选项的Expressway设备集群时，每个集群对等体需要配置其自己的LAN1接口地址。此外，必须在未启用静态NAT模式的接口上配置集群。因此，建议使用LAN2作为外部接口，在适用的情况下，可以在该接口上应用和配置静态NAT。

外部LAN接口设置

IP配置页面上的外部LAN接口配置设置控制哪个网络接口使用围绕NAT(TURN)的中继的横向使用。在双网络接口Expressway-E配置中，这通常设置为Expressway-E外部LAN接口。

静态路由

此场景必须为Expressway-E配置默认网关地址10.0.10.1。这意味着默认情况下，通过LAN2发送的所有流量都发送到IP地址10.0.10.1。

如果FW B将从10.0.30.0/24子网发送的流量转换到Expressway-E LAN1接口（例如，Expressway-C穿越客户端流量或TMS服务器管理流量），则当流量从FWB外部接口(10.0.20.1)到达Expressway-E LAN1时，此流量将显示。通过其LAN1接口对此流量做出应答，因为该流量的明显来源位于同一子网。

如果FW B上启用了NAT，则从Expressway-C发送到Expressway-E LAN1的流量显示为来自10.0.30.2。如果Expressway没有为10.0.30.0/24子网添加静态路由，它会将此流量的应答从LAN2发送到其默认网关(10.0.10.1)，因为不知道10.0.30.0/24子网位于内部防火墙(FW B)后面。 因此，需要添加静态路由，通过与Expressway的SSH会话运行**xCommand RouteAdd** CLI命令。

在本例中，Expressway-E必须知道它可以到达FW B后面的10.0.30.0/24子网，该子网可通过LAN1接口访问。为此，请运行以下命令：

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

> **注意**：S静态路由配置可通过Expressway-E GUI以及“系统/网络”>“接口/静态路由”部分应用。

在本例中，Interface参数也可设置为**Auto**，因为网关地址(10.0.20.1)只能通过LAN1到达。

如果FW B上未启用NAT，并且Expressway-E需要与子网(10.0.30.0/24以外)中的设备（也位于FW B后面）通信，则必须为这些设备/子网添加静态路由。

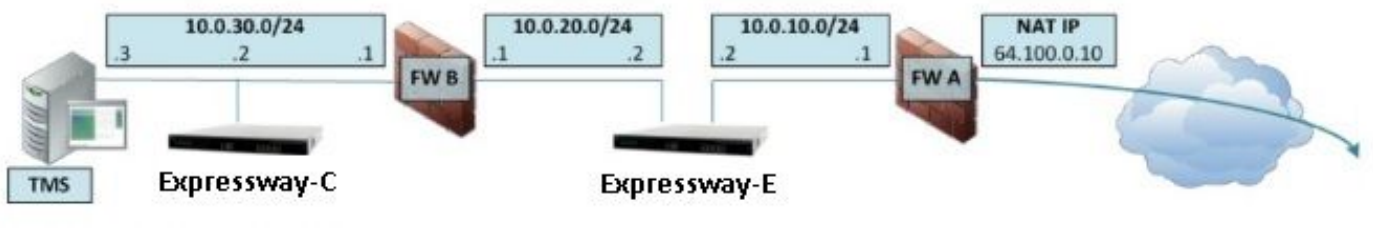
> **注意：**这包括 从网络管理工作站或NTP、DNS、LDAP/AD或Syslog等网络服务进行SSH和HTTPS连接。

《VCS管理员指南》中对**xCommand RouteAdd**命令和语法进行了详细说明。

配置

本节介绍如何在ASA上配置Expressway-E双网络接口实施所需的静态NAT。为处理SIP/H323流量，还包含一些额外的ASA模块化策略框架(MPF)配置建议。

Expressway C和E — 双网络接口/双NIC实施



在本例中，IP地址分配是下一个。

Expressway-C IP地址：10.0.30.2/24

Expressway-C默认网关：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默认网关：10.0.10.1(FW-A)

TMS IP地址：10.0.30.3/24

FW-A配置

步骤1. Expressway-E的静态NAT配置。

如本文档的“背景信息”部分所述，FW-A具有静态NAT转换，允许从公有IP地址为64.100.0.10的Internet访问Expressway-E。最后一个是NAT，NAT到Expressway-E LAN2 IP地址10.0.10.2/24。也就是说，需要FW-A静态NAT配置。

对于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**:当应用静态PAT命令时，您会在ASA命令行界面上收到以下错误消息，“**ERROR:NAT无法保留端口**”。 之后，继续清除ASA上的xlate条目，为此，运行命令**clearxlatelocal x.x.x.x**，从其中x.x.x.x对应于ASA外部IP地址。此命令清除与此IP地址关联的所有转换，并在生产环境中谨慎运行。

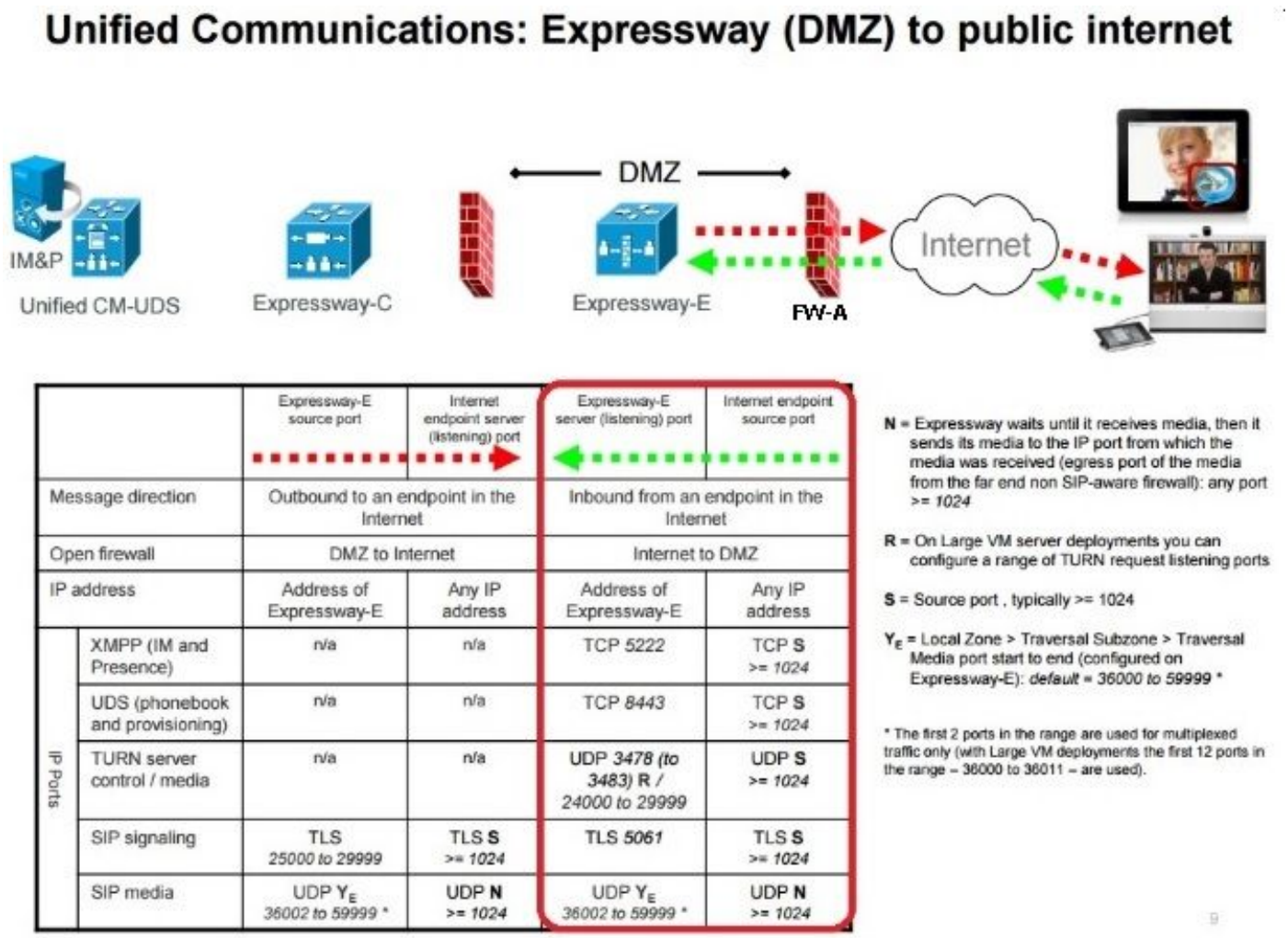
对于ASA 8.2及更低版本：

```
! 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
```

步骤2.访问控制列表(ACL)配置允许从互联网到Expressway E的所需端口。

根据统一通信：Expressway(DMZ)到公共互联网文档，Expressway-E在FW-A中需要允许的TCP和UDP端口列表如图所示：



		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).

这是FW-A外部接口入站时所需的ACL配置。

对于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
```

对于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

如本文档的背景信息部分所述，FW B可能需要动态NAT或PAT配置，以便在内部子网10.0.30.0/24到达FW B的外部接口时将其转换为IP地址10.0.20.1。

对于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
```

对于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**：请确保所有必需的TCP和UDP端口都允许Expressway-C正常工作并在防火墙B中打开，如本Cisco文档中所指定：Cisco Expressway IP端口用于防火墙穿越

验证

使用本部分可确认配置能否正常运行。

Packet Tracer可用于ASA，以确认Expressway-E静态NAT转换是否按需工作。

Packet Tracer在TCP/5222上测试64.100.0.10

```
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在TCP/8443上测试64.100.0.10

```
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在TCP/5061上测试64.100.0.10

```
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在UDP/24000上测试64.100.0.10

```
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在UDP/36002上测试64.100.0.10

```
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
```

故障排除

步骤1.比较数据包捕获。

数据包捕获可在ASA入口和出口接口进行。

```
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的数据包捕获：

```
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64.100.0.10的数据包捕获：

```
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
```

步骤2.检查加速安全路径(ASP)丢弃数据包捕获。

ASA丢弃的数据包由ASA ASP捕获捕获。选项**all**捕获ASA丢弃数据包的所有可能原因。如果有任何疑似原因，可以缩小范围。有关ASA用于对这些丢包进行分类的原因列表，请运行命**令show asp drop**。

```
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**：在此场景中使用ASA ASP捕获来确认ASA是否因丢失ACL或NAT配置而丢弃数据包，这需要为Expressway-E打开特定TCP或UDP端口。

> **提示**：每个ASA捕获的默认缓冲区大小为512 KB。如果ASA丢弃了太多数据包，缓冲区将快速填充。缓冲区大小可通过缓冲区选**项增**大。

建议

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
```

替代VCS Expressway实施

使用双网络接口/双NIC实施Expressway-E的替代解决方案是实施Expressway-E，但在防火墙上使用单个NIC和NAT反射配置。下一个链接显示有关此实施的更多详细信息在ASA上为VCS Expressway网真设备配置NAT反射。

> **提示：**VCS Expressway的建议实施是本文档中描述的双网络接口/双NIC VCS Expressway实施。

相关信息

- 在ASA上为VCS Expressway网真设备配置NAT反射
- 技术支持和文档 - Cisco Systems
- Cisco Expressway-E和Expressway-C — 基本配置部署指南
- 将Cisco VCS Expressway放置在DMZ中，而不是公共互联网中
- 防火墙穿越的Cisco Expressway IP端口使用