ASA NAT配置和推荐对ExpresswayE双倍网络接口实施

Contents

Introduction

本文描述如何实现在Cisco可适应的安全工具是必需的网络地址转换(NAT)配置(ASA)对于ExpresswayE双重网络接口实施。

> **提示**： 此配置是ExpresswayE实施的推荐的选项，而不是与NAT反映的单一NIC实施。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Cisco ASA基本配置和NAT配置
- Cisco ExpresswayE和ExpresswayC基本配置

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8.0及以后的Cisco ASA 5500和5500-X系列工具。
- Cisco Expressway版本X8.0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.如果您的网络实际，请保证您了解所有命令的潜在影响。

> **Note**: 通过整个文档，高速公路设备指ExpresswayE和ExpresswayC。然而，相同配置适用视频通信服务器(VCS) Expressway和VCS控制设备。

背景信息

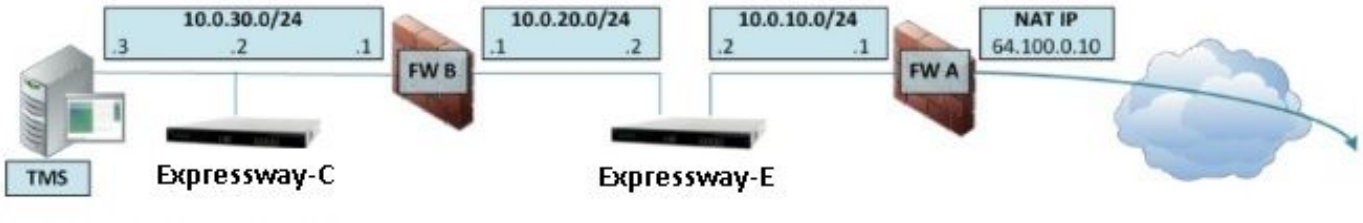
故意地， Cisco ExpresswayE可以放置在非敏感区域(DMZ)或与面向互联网的接口，而能与在专用网络的Cisco ExpresswayC沟通。当Cisco ExpresswayE在DMZ时安置，这些是其它好处：

- 在多数常见情况中， Cisco ExpresswayE通过专用网络管理。当Cisco ExpresswayE在DMZ时，周界(外部)防火墙可以用于通过超文本传输协议阻止对Expressway的不需要的访问从外部网络安全(HTTPS)或安全壳SSH请求。
- 如果DMZ不允许内部和外部网络之间的直接连接，要求专用服务器处理横断DMZ的数据流。Cisco Expressway能作为会话初始化协议(SIP)和H.323语音和视频数据流的一个代理服务器。在这种情况下，您能使用允许Cisco Expressway有两个不同的IP地址的双重网络接口选项，一个到/从外部防火墙的数据流和一个到/从内部防火墙的数据流的。
- 此设置防止直接连接外部网络与内部网络。这改进内部网络安全所有。

> **提示**：为了得到关于网真实施的更多详细资料，在公共互联网里请参见Cisco ExpresswayE和ExpresswayC -基本配置部署指南和安置Cisco VCS Expressway在DMZ而不是。

Expressway C和E -双重网络接口/双NIC实施

此镜像显示ExpresswayE的示例配置与双重网络接口和静态NAT。ExpresswayC作为穿越客户端。有两防火墙(FW A和FWB)。一般，在此非军事区配置， FW A不能路由流量对FW B，并且例如ExpresswayE要求设备验证和转发数据流从FW A的子网到FW B的子网(反之亦然)。



此配置包括这些组件。

DMZ子网1 – 10.0.10.0/24

- FW A内部界面– 10.0.10.1
- ExpresswayE LAN2接口– 10.0.10.2

DMZ子网2 – 10.0.20.0/24

- FW B外部接口– 10.0.20.1
- ExpresswayE LAN1接口– 10.0.20.2

LAN子网– 10.0.30.0/24

- FW B内部界面– 10.0.30.1
- ExpresswayC LAN1接口– 10.0.30.2
- 思科网真管理套件(TMS)服务器网络网络界面– 10.0.30.3

此实施特定：

- FW A是外部或周界防火墙;它配置有静态被转换为10.0.10.2的NAT IP (公有IP) 64.100.0.10 (ExpresswayE LAN2接口)
- FW B是内部防火墙
- ExpresswayE LAN1有被禁用的静态NAT模式
- ExpresswayE LAN2有静态NAT模式启用静态NAT地址64.100.0.10
- ExpresswayC有指向10.0.20.2的一个穿越客户端区域(ExpresswayE LAN1接口)
- 没有在10.0.20.0/24和10.0.10.0/24子网之间的路由。ExpresswayE桥接这些子网并且作为SIP/H.323信令和实时传输协议(RTP)/RTP控制协议(RTCP)媒体的一个代理。
- Cisco TMS有ExpresswayE配置有IP地址10.0.20.2

需求/限制

非重复子网

如果配置ExpresswayE使用两个LAN接口 ， LAN1和LAN2接口必须位于非交迭的子网保证数据流被派出对正确的接口。

集群

当集群Expressway设备用先进的网络选项配置时，每个簇对等体需要配置有其自己的LAN1接口地址。另外，在没有启动的静态NAT模式的接口必须配置集群。所以，建议您使用LAN2作为外部接口，您能适用和配置静态NAT在可适用地方。

外部LAN接口设置

在网络接口使用横截使用中继在NAT的IP配置页控制的外部LAN接口配置设置(轮)附近。在一种双重网络接口ExpresswayE配置中，这通常设置为ExpresswayE外部LAN接口。

静态路由

必须配置有ExpresswayE 10.0.10.1的默认网关地址此方案的。这意味着，默认情况下，通过LAN2被派出的所有数据流被发送到IP地址10.0.10.1。

如果FW B转换从10.0.30.0/24子网发送的数据流到ExpresswayE LAN1接口(例如，ExpresswayC穿越客户端的流量或TMS服务器管理数据流)，此数据流出现，当来自FWB外部接口(10.0.20.1)，到达ExpresswayE LAN1。因为该数据流的明显的来源位于相同子网，ExpresswayE然后能回复此数据流通过其LAN1接口。

如果NAT在FW B允许，从ExpresswayC发送的数据流到ExpresswayE LAN1显示，当来自10.0.30.2。如果Expressway没有为10.0.30.0/24子网添加的静态路由，发送此数据流的回复到其默认网关(10.0.10.1)从LAN2，因为不知道10.0.30.0/24子网在内部防火墙(FW B)后位于。所以，静态路由需要被添加，运行**xCommand RouteAdd** CLI命令通过SSH会话对Expressway。

在此特定的示例中， ExpresswayE必须知道能在FW B后到达10.0.30.0/24子网，通过LAN1接口是可及的。要完成此，请运行命令：

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

> **Note**: 静态路由配置可以适用通过ExpresswayE GUI以及部分**系统/network >接口/静态路由**。

在本例中，接口参数可能也设置为**自动**，因为网关地址(10.0.20.1)通过LAN1只是可及的。

如果NAT在FW B和ExpresswayE需要没有允许与在FW B后也位于的子网的设备沟通(除10.0.30.0/24之外)，必须为这些设备/子网添加静态路由。

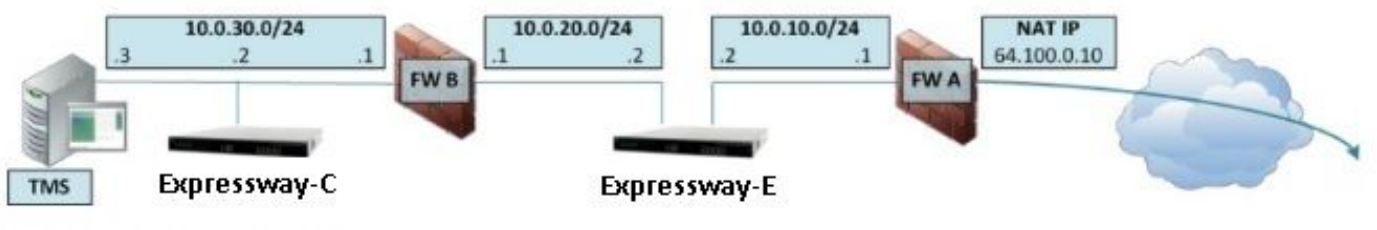
> **Note**:这包括SSH和HTTPS连接从网络管理工作站或网络服务的类似NTP、DNS、LDAP/AD或者Syslog。

xCommand RouteAdd命令和语法在VCS管理员指南的全面的详细信息描述。

配置

此部分描述如何配置静态NAT必需在ASA的ExpresswayE双重网络接口实施的。一些另外的ASA模块化政策架构(MPF)配置推荐为处理SIP/H323数据流是包括的。

Expressway C和E -双重网络接口/双NIC实施



在本例中， IP地址分配是下一个。

ExpresswayC IP地址： 10.0.30.2/24

ExpresswayC默认网关：10.0.30.1 (FW-B)

ExpresswayE IP地址：

在LAN2 ： 10.0.10.2/24

在LAN1 ：10.0.20.2/24

ExpresswayE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. ExpresswayE的静态NAT配置。

按照本文的Background Information部分说明， FW-A有允许一个的静态NAT转换ExpresswayE是可及的从有公共IP地址64.100.0.10的互联网。最后一个NAT对ExpresswayE LAN2 IP地址10.0.10.2/24。说的那，这是必需的FW-A静态NAT配置。

ASA版本8.3和以上：

```
! 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
```

> **警告：** 当您适用时静态PAT发出命令您收到在ASA命令行界面的此错误信息， “**错误：无法的NAT保留端口”**。在此以后，继续清除在ASA的xlate条目，此的，运行命令**clearxlatelocal x.x.x.x， fromwhere** x.x.x.x对应于ASA外部IP地址。此命令在生产环境里清除与此IP地址产生关联的所有转换，小心地运行它。

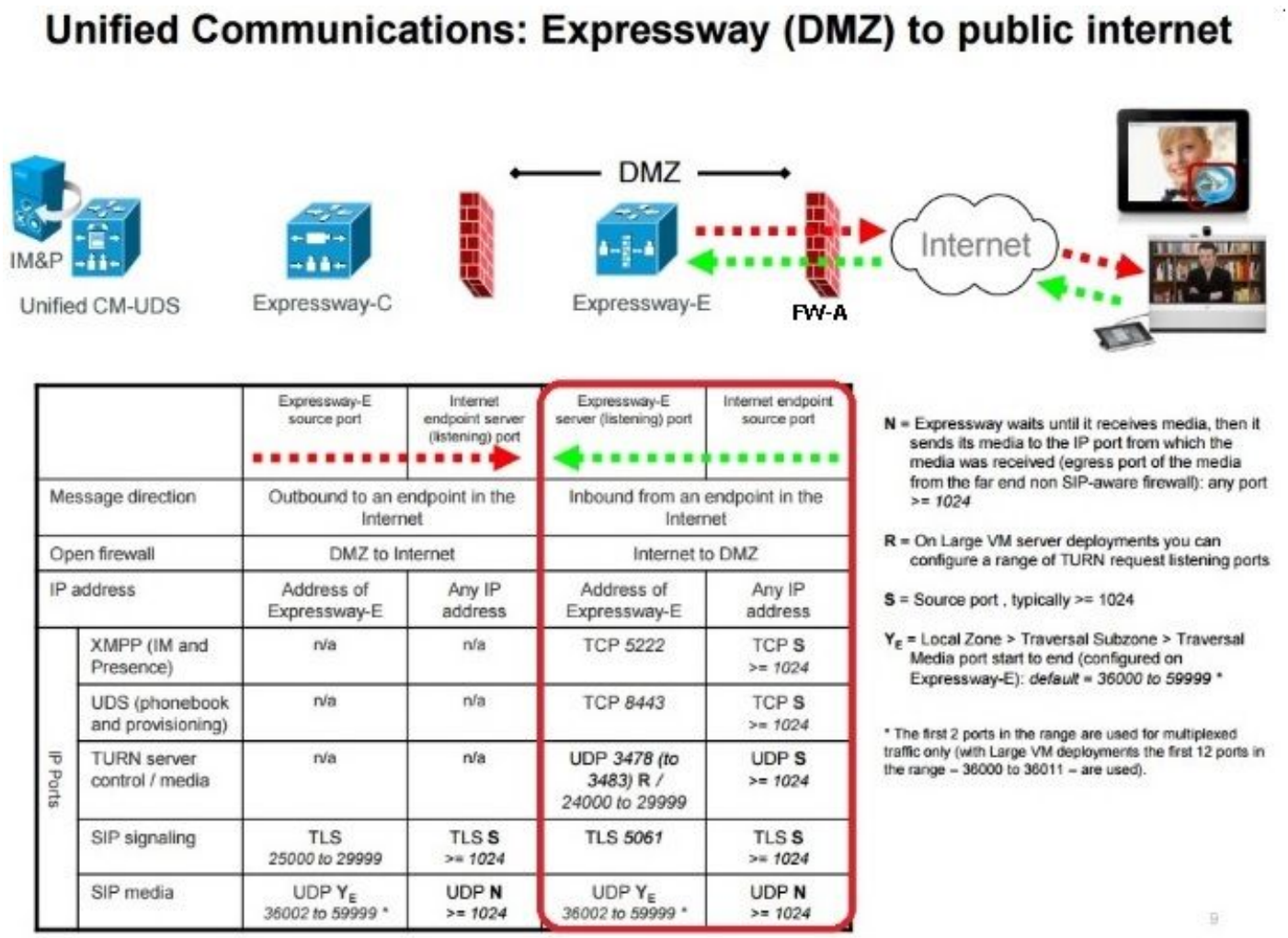
ASA版本8.2和以下：

```
! 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.访问控制表(ACL)配置允许从互联网的必需的端口到ExpresswayE。

根据统一的通信：Expressway (DMZ)如镜像所显示，对公共互联网文档， ExpresswayE在FW-A要求允许的TCP和UDP端口列表，是：



		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).

这是如入站需要的ACL配置在FW-A外部接口。

ASA版本8.3和以上：

```
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
```

ASA版本8.2和以下：

```
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

按照本文的Background Information部分说明，当去FW B.的外部接口时， FW B可能要求一种动态NAT或PAT配置允许内部子网10.0.30.0/24被转换为IP地址10.0.20.1。

ASA版本8.3和以上：

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

ASA版本8.2和以下：

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

> **提示**： 在此Cisco文档上指定请务必所有必需的TCP和UDP端口允许ExpresswayC适当地运作并且是开放的在FW B， ： Cisco Expressway IP防火墙穿越的端口使用方法

Verify

使用本部分可确认配置能否正常运行。

信息包跟踪程序在ASA可以用于确认ExpresswayE静态NAT转换运转得如所需求。

测试64.100.0.10的信息包跟踪程序在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
```

测试64.100.0.10的信息包跟踪程序在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
```

测试64.100.0.10的信息包跟踪程序在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
```

测试64.100.0.10的信息包跟踪程序在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
```

测试64.100.0.10的信息包跟踪程序在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
```

Troubleshoot

步骤1.比较信息包获取。

信息包获取可以被采取在ASA入口和输出接口。

```
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
```

64.100.0.10的信息包获取在TCP/5222 ：

```
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
```

64.100.0.10的信息包获取在TCP/5061 ：

```
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. Inspect加速的安全路径(ASP)丢弃数据包捕获。

由ASA的信息包丢弃由ASA ASP捕获捕获。选项**全部**，捕获所有可能的来源ASA为什么丢弃了信息包。如果有任何怀疑的原因，这可以缩小。对于ASA使用分类这些丢包原因的列表，请运行show命令**asp丢弃。**

```
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**：ASA ASP捕获是否用于此方案确认ASA丢包信息包由于一种丢失的ACL或NAT配置，将要求打开ExpresswayE的一个特定TCP或UDP端口。

> **提示**：每个ASA捕获的默认缓冲大小是512 KB。 如果过多的信息包由ASA丢弃，缓冲区迅速被充满。缓冲大小可以增加与**缓冲区**选项。

推荐

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 ：

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

选择VCS Expressway实施

实现与双重网络接口/双NIC的ExpresswayE的其它方案将实现ExpresswayE，但是与在防火墙的单个NIC和NAT反映配置。下条链路显示关于此实施的更详细的资料配置在ASA的NAT反映VCS Expressway网真设备的。

> **提示**：VCS的Expressway推荐的实施是双重网络接口/在本文描述的双NIC VCS Expressway实施。

Related Information

- 配置在ASA的NAT反映VCS Expressway网真设备的
- **Technical Support & Documentation - Cisco Systems**
- Cisco ExpresswayE和ExpresswayC -基本配置部署指南
- 安置Cisco VCS Expressway在DMZ而不是在公共互联网里
- Cisco Expressway IP防火墙穿越的端口使用方法