

ASA NAT配置和建议ExpresswayE的和ExpresswayC双倍网络接口实施。

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[Expressway C和E -双重网络接口/双NIC实施](#)

[需求/限制](#)

[非重复子网](#)

[集群](#)

[外部LAN接口设置](#)

[静态路由](#)

[配置](#)

[Expressway C和E -双重网络接口/双NIC实施](#)

[FW-A配置：](#)

[步骤1. ExpresswayE的静态NAT配置](#)

[步骤2.允许端口的访问控制表\(ACL\)配置要求从互联网到ExpresswayE](#)

[FW-B配置。](#)

[验证](#)

[故障排除](#)

[步骤1.数据包捕获。](#)

[步骤2.加速的安全路径\(ASP\)丢弃数据包捕获。](#)

[建议](#)

[保证SIP/H.323检验完全禁用在介入的防火墙](#)

[其它方案](#)

[相关链接](#)

简介

本文描述如何实现在思科可适应安全工具要求的网络地址转换(NAT)配置(ASA) ExpresswayE和ExpresswayC双重网络接口/双重网络接口控制器(NIC)实施的。

使用NAT反射，此部署是实现的ExpresswayE和ExpresswayC设备一个推荐的选项而不是。

贡献由基督徒埃尔南德斯和塞萨尔省卢佩茨Zamarripa，Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ASA基本NAT和配置
- 思科ExpresswayE和ExpresswayC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及以后的Cisco ASA 5500和5500-X系列设备。
- Cisco Expressway版本8.x和以上。

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：通过整个文档，Expressway设备被提到作为ExpresswayE和ExpresswayC。然而，相同的配置适用于视频通信服务器(VCS) Expressway和VCS控制设备。

背景信息

故意地，思科ExpresswayE可以在非敏感区域(DMZ)安置或者或面对公共网络(互联网)和能与在私有网络的思科ExpresswayC。然而，当思科ExpresswayE在DMZ时放置，这些是additional好处。

- 在多数常见情况中，思科ExpresswayE从私有网络管理。通过安置思科ExpresswayE在DMZ，一perimetral (外部)防火墙可以用于阻止对Expressway的不需要的访问例如(安全的超文本传输协议) 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，专用服务器要求处理横断DMZ的流量。思科Expressway能作为会话初始化协议(SIP)的该服务器和H.323语音和视频流量。在这种情况下，您能使用允许思科Expressway有两个不同的IP地址的双重网络接口选项，一个到/从外部防火墙的流量和一个到/从内部防火墙的流量的。
- 此设置防止外部通信连接直接地到内部网络。这改善内部网络安全所有。

提示：为了得到关于网真实施的更多详细信息，[在公共互联网里参考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

此图表显示ExpresswayE的一示例部署与双重网络接口和静态NAT。作为穿越客户端和两防火墙(FW A和FWB)的ExpresswayC。一般，在此非军事区配置，FW A不能路由流量对FW B，并且设备例如双界面ExpresswayE要求验证和转发流量从FW A的子网到FW 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

- FW A内部接口– 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内部接口– 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

- FW A是外部或perimetral防火墙;它配置与静态翻译对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有禁用的静态NAT模式
- ExpresswayE LAN2有静态NAT模式启用与静态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配置与IP地址10.0.20.2

需求/限制

非重复子网

如果ExpresswayE配置使用两个LAN接口，在非重复子网必须查找LAN1和LAN2接口保证流量被派出对正确接口。

集群

当集群的Expressway设备有配置时的**先进的网络选项**，每集群对等体需要其自己的LAN1接口地址

。另外，在没有启用的静态NAT模式的接口必须配置集群。所以，推荐您使用LAN2作为外部接口，并且LAN2使用作为静态NAT接口在可适用地方。

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。在一双重网络接口ExpresswayE配置中，这可能通常设置为ExpresswayE外部LAN接口。

静态路由

必须配置ExpresswayE与10.0.10.1默认网关地址此方案的。这意味着，默认情况下，通过LAN2被派出的所有流量发送对IP地址10.0.10.1。

如果FW B翻译从10.0.30.0/24子网发送的流量到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)，此流量出现，当来自FWB外部接口(10.0.20.1)，到达ExpresswayE LAN1。因为该流量明显的来源在相同子网，查找ExpresswayE然后能应答到此流量通过其LAN1接口。

如果FW B不执行NAT，从ExpresswayC发送的流量到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，发送此流量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)后查找。所以，静态路由需要被添加，使用xCommand RouteAdd CLI命令通过SSH会话到Expressway。

在本例中特定的示例，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。这使用此命令是实现的。

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

注意：静态路由配置可以通过在部分**系统/network >接口/静态路由**的ExpresswayE图形用户界面(GUI)应用。

注意：推荐避免使用在FW-B的NAT ExpresswayC的。这允许ExpresswayE到达与其实际IP地址10.0.30.2的ExpresswayC。这避免某些电话服务问题。被确认ExpresswayC的NAT配置能促成莫比尔和远程访问(MRA)设备不出来。

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FW B不执行NAT和ExpresswayE需要用在FW B后也查找例如SSH和HTTPS连接从此网络工作站或网络服务的类似NTP、DNS、LDAP/AD和Sylog的子网的设备通信除10.0.30.0/24之外，必须为这些设备/子网添加静态路由。

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需要的ExpresswayC和ExpresswayE双重网络接口/双NIC实施的在ASA。其外，处理的SIP/H323流量一些ASA模块化政策架构(MPF)配置推荐通过ASA。

Expressway C和E -双重网络接口/双NIC实施



在本例中IP地址assignment是下部分。

ExpresswayC IP address: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是可达的从互联网使用公网IP地址64.100.0.10。最后一个NAT对ExpresswayE LAN2 IP地址10.0.10.2/24，说的该，这是需要的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
```

注意：如果，当尝试应用静态PAT时发出命令您收到错误消息‘ERROR:无法的NAT保留ASA命令行界面的端口的，然后，清除与x.x.x.x对应于ASA外部IP地址的clear xlate命令本地x.x.x.x的xlate条目。此命令清除在生产环境关联的对此IP，因此所有转换，小心地运行它。

ASA版本8.2和以下：

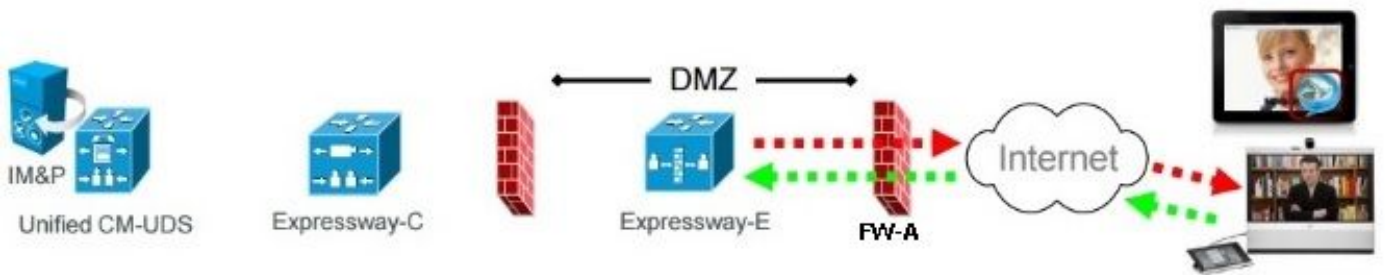
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port. This esample shows only when Static one-to-one NAT is used.

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

步骤2.允许端口的访问控制表(ACL)配置要求从互联网到ExpresswayE

根据Unified通信：Expressway (DMZ)对公共互联网文档，这是的TCP & UDP端口列表ExpresswayE在FW-A要求允许：

Unified Communications: Expressway (DMZ) to public internet



| | | 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).

这是如入站要求的ACL配置在FW A外部接口。

ASA版本8.3和以上。

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

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

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 esample shows only when Static one-to-one NAT is used.

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

注意：它是高度推荐的禁用SIP和H.323检验在防火墙运载的网络流量到/从ExpresswayE，和，当启用，频繁地发现这负影响ExpresswayE内置的firewall/NAT穿越功能。

FW-B配置。

按照本文的**Background Information**部分说明，当出去对FW B的外部接口时，FW B要求一动态NAT或PAT配置允许将翻译的内部子网10.0.30.0/24对IP地址10.0.20.1。

ASA版本8.3和以上。

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

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

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 esample shows only when Static one-to-one NAT is used.
```

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

注意：它是高度推荐的禁用SIP和H.323检验在防火墙运载的网络流量到/从ExpresswayE，as，当启用这频繁地被发现负影响ExpresswayE内置的firewall/NAT穿越功能。

提示：在此Cisco文档上指定请务必所有ExpresswayC的需要的TCP & UDP端口能适当地工作在FW B打开，：[思科Expressway防火墙穿越的IP波尔特使用情况](#)

验证

数据包跟踪程序在ASA可以用于确认ExpresswayE静态NAT转换运转如所需求。

测试64.100.0.10的数据包跟踪程序在TCP/5222。

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

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

测试64.100.0.10的数据包跟踪程序在TCP/8443。

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

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

测试64.100.0.10的数据包跟踪程序在TCP/5061。

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

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

测试64.100.0.10的数据包跟踪程序在UDP/24000：

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

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

测试64.100.0.10的数据包跟踪程序在UDP/36002。

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

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

故障排除

步骤1.数据包捕获。

数据包捕获可以被采取在ASA入口和出口接口

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

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

64.100.0.10的数据包捕获在TCP/5222 :

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

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

64.100.0.10的数据包捕获在TCP/5061 :

! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This esample 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.加速的安全路径(ASP)丢弃数据包捕获。

ASA ASP丢弃捕获使用ASA决定丢弃的数据包。选项**全部**捕获所有可能的来源ASA为什么丢弃了数据包。如果有任何supected原因，这可以缩小。对于ASA使用分类此丢包原因的列表，show命令asp丢弃能使用。

每个ASA捕获的默认缓冲区是512 KB。如果有很多拒绝的数据包由此ASA，此缓冲区被充满的非常快。使用选项**缓冲区**，此缓冲区可以被增加。

```
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：此ASA ASP捕获是否是非常有用的在此方案确认ASA丢包数据包由于打开丢失的ACL或的NAT特定TCP或ExpresswayE的UDP端口。

建议

保证SIP/H.323检验完全禁用在介入的防火墙

它是高度推荐的禁用SIP和H.323检验在处理网络流量到/从ExpresswayE，as，当启用这频繁地被发现负影响Expressway内置的firewall/NAT穿越功能的防火墙。

这是示例如何禁用SIP和H.323检验在ASA。

```
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
```

其它方案

—其它方案而不是实现ExpresswayE使用双重网络接口/双NIC，将实现ExpresswayE使用在防火墙的一NAT反射配置，此链路显示关于此方案的更详细的资料。

[ASA : NAT VCS Expressway实施的反射配置。](#)

然而，因为在本文初被提及了，双重网络设置在NAT反射推荐。

相关链接

[思科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](#)

[思科Expressway防火墙穿越的IP波尔特使用情况](#)