

第9章 配置

通过Cisco PIX防火墙的访问

本章包含下列主题：

- ❖ 通过PIX防火墙进行访问
- ❖ 理解静态翻译和管道
- ❖ 穿过PIX防火墙的其他方法
- ❖ 配置多个接口

配置通过PIX防火墙的访问

只有两种方法可以允许从一台不太被信任的设备通过PIX防火墙，访问一台相对更被信任的设备。

- ❖ 对合法请求的响应——当在内部的用户建立一条到外部设备的连接时，缺省情况下，对那个请求的响应是被允许通过PIX防火墙返回。所有由内向外的连接将向PIX防火墙中的翻译表填充信息。当一台外部设备响应这个请求时，PIX防火墙检查翻译表，看看对于那个请求是否存在一个翻译槽位。如果存在一个翻译槽位，PIX防火墙就允许响应通过。在会话终止后，与该特定翻译槽位相关的空闲定时器开始计数。在PIX OS 5.1版中，缺省值是三个小时。

- ❖ 配置一个管道——用于由外向内的通信。首先配置静态翻译或者global和nat命令（虽然nat/global命令支持源自内部的连接，但如果用户想让回声应答被允许通过PIX防火墙返回，就还必须配置一个管道）。然后配置一个管道，它定义了被允许流过PIX防火墙的地址或地址组、源和/或目的TCP/UDP端口或端口范围。

理解静态翻译和管道命令

虽然大多数的连接时从具有较高安全级别的接口去往具有较低安全级别的接口，但是仍然有一些情况需要允许从具有较低安全级别的接口连接到具有较高安全级别的接口。为了满足这种需要，可以采用conduit命令。

static命令创建了一个本地（内部）IP地址和一个全局（外部）IP地址之间的静态映射。使用static命令可以让我们为一个特定的内部IP 地址设置一个永久的全局IP地址。这样就能够为具有较低安全级别的指定接口创建一个入口，使它们可以进入具有较高安全级别的指定接口。

记住下列要点很重要：

- *conduit命令允许从较低安全级别接口到较高安全级别接口的连接。对于一台给定的主机，在ASA的向内的安全策略中，conduit命令是一个例外。
- *static命令用来在一个本地IP地址和一个全局IP地址之间，创建一个永久映射。

❖ static命令

static命令在一个本地IP地址和一个全局IP地址之间，创建一个永久映射（静态翻译槽位）。当连接到Internet时，全局IP地址必须是一个经过注册的IP地址。static命令语句优先于nat和global命令组。我们可以使用show static命令来显示PIX防火墙配置中的static命令语句。

每个接口的安全级别是由nameif命令设置的。当与static命令一起使用时，conduit命令允许数据流源自一个具有较低安全值得接口，通过PIX防火墙向一个具有较高安全值的接口。例如，必须配置静态和管道，来允许从外部到DMZ接口的入方向会话，或从外部到内部接口的入方向会话。

❖ conduit命令

conduit命令允许或拒绝从PIX防火墙外部的连接访问内部网络主机上的TCP、UDP和其他协议服务。conduit语句可以被以一种非常通用的方式、或一种非常具体的方式使用。例如，可以允许对一台特定主机的HTTP访问。

在下面例子中，首先使用static命令将IP地址10.0.1.10静态翻译成192.168.1.101。conduit命令将只允许对主机10.0.1.10（被翻译成192.168.1.101）进行HTTP访问。

例：如图6-1，联合使用static和conduit命令来只允许HTTP访问

```
static (inside,outside) 192.168.1.101 10.0.1.10  
netmask 255.255.255.255
```

```
conduit permit tcp any eq www host 172.16.1.1
```

conduit命令语法：

```
conduit permit | deny protocol global_ip global_mask  
[operator port [port]] foreign_ip foreign_mask  
[operator port [port]]
```

其中，permit：如果条件匹配，就允许访问。

deny：如果条件匹配，就拒绝访问。

protocol：为连接指定传输协议。

global_ip：先前由global或static命令定义的一个全局IP地址。

global_mask：global_ip的网络掩码。

foreign_ip：可以访问global_ip的一个外部IP地址（主机或网络）。

foreign_mask：foreign_ip的网络掩码。

operator：一个比较运算符，让我们指定一个端口或端口范围。

- *不使用运算符和端口就相当于指定了所有的端口。如：conduit permit tcp any any

- *使用eq和一个端口来允许或拒绝对这个端口的访问。如（使用eq ftp来允许或拒绝只对FTP的访问）：conduit deny tcp host 192.168.1.1 eq ftp 209.165.201.1

- *使用lt和一个端口来允许或拒绝对小于我们指定端口的所有端口的访问。如（使用lt 1025来允许或拒绝对众所周知端口（1到1024）的访问）：conduit permit tcp host 192.168.1.1 lt 1025 any

- *使用gt和一个端口来允许或拒绝对大于我们指定端口的所有端口的访问。如（使用gt 42来允许或拒绝对端口43到65535的访问）：conduit deny udp host 192.168.1.1 gt 42 host 209.165.201.2

- *使用“neq”和一个端口来允许或拒绝对除了我们指定端口之外的所有端口的访问。如（使用neq 10来允许或拒绝对端口1到9和11到65535的访问）：conduit deny tcp host 192.168.1.1 neq 10 host 209.165.201.2 neq 42

- *使用“range”和一个端口范围来允许或拒绝只对那些在范围内的端口的访问。如（使用“range 10 1024”来允许或拒绝只对端口10到1024的访问，所有的其他端口不受影响）：conduit deny tcp any range 10 1024 any

port：在访问global_ip或foreign_ip时，我们允许使用的服务。

icmp_type：ICMP消息的类型。如0表示echo-reply，3表示unreachable，4表示source-quench等。省略这个选项就意味着全部ICMP类型。这条命令的一个实例如下，它允许全部ICMP类型：conduit permit icmp any any 这条命令允许向内和向外的ICMP消息通过。

在使用conduit命令时，最好是尽可能地具体。允许在外部的所有用户telnet到内部的一台主机可能会违背安全策略。

例：如图6-2，只允许一台特定的外部主机访问一台特定的本地主机。在这个例子中还包含static命令，以完成配置。

```
static (inside,outside) 192.168.1.101 10.0.1.10 netmask  
255.255.255.255
```

```
conduit permit tcp host 192.168.1.101 eq www telnet host  
172.16.1.1
```

外部的用户具有IP地址172.16.1.1，它使用的目标IP地址是192.168.1.101。PIX防火墙对那个地址进行翻译，并根据所配置的静态翻译，将对内部的请求发送给IP地址10.0.1.10。

穿过PIX进行访问的其他方法

从内部到外部通过PIX进行访问的最常用的方法是使用global和nat命令组。这也被称为网络地址翻译。这在访问外部的设备时，允许将内部的一段地址范围翻译成一段全局地址范围。还可以将一段内部地址范围翻译成单个全局地址。这被称为端口地址翻译。

PAT用一个IP地址和一个源端口号的组合来唯一性地标识一个会话。PIX防火墙将每个本地地址翻译成相同的全局地址，但是给它们分配一个大于1024的、唯一的源端口号。如图6-3。

❖ 配置PAT

配置PAT类似于配置NAT，但是有一个不同——在global语句中使用单个IP地址，而不是一段地址范围。例如，在10.0.0.0网络上的所有本地主机都将被翻译成全局地址192.168.0.15。所有的源端口将被改成一个大于1024的、唯一的端口号。如图6-4，部分配置如下：

```
ip address (inside) 10.0.0.1 255.255.255.0
ip address (outside) 192.168.0.2 255.255.255.0
route (outside) 0.0.0.0 0.0.0.0 192.168.0.1
global (outside) 1 192.168.0.15 netmask
    255.255.255.0
nat (inside) 1 10.0.0.0 255.0.0.0
```


PAT可以提供下列附加的特性和优点：

*PAT和NAT可以被同时使用——可能要被翻译的本地地址数量超出了全局地址的数量。在这种情况下，可以同时使用PAT和NAT。但采用下面的配置时，每个本地IP地址在全局地址范围（从192.168.0.1到192.168.0.9）被完全用尽前将使用NAT方式进行地址翻译。此后，PIX防火墙将开始使用PAT方式，将随后到来的、通过它的任何本地地址翻译成192.168.0.10。

```
global (outside) 1 192.168.0.1-192.168.0.9 netmask  
255.255.255.0
```

```
global (outside) 1 192.168.0.10 netmask  
255.255.255.0
```

```
nat (inside) 1 0.0.0.0 0.0.0.0
```

- *一个全局IP地址可能被用于最多64000台内部主机——这是受端口字段内部尺寸的限制。
- *将多个端口号映射为单个IP地址——将一个全局地址用于所有的内部诸暨，这意味着可以从服务提供商那里租用更少的IP地址。
- *通过使用单个IP地址来隐藏网络内部源地址——当连接到Internet或其他不被信任的环境时，通过NAT或PAT，隐藏内部地址是一项非常安全的措施。

❖ 配置nat 0

连接Internet的一个常见目的是，允许从外部对HTTP服务器或SMTP服务器的访问。这些被访问的设备为了能够与Internet上的其他设备进行通信，必须要拥有经过注册的合法地址。我们可以对PIX防火墙进行配置，使得内部设备的实际分配的IP地址被用作当从外部对它进行访问时的目标IP地址。

nat 0命令让我们可以禁止地址翻译，使得内部IP地址不经过地址翻译，而对于外部是可见的。当内部网络中的、经InterNIC注册过的IP地址对于外部网络应能够访问时，可以使用这个特性。nat 0的使用取决于当前采用的安全策略。如果策略允许内部客户机拥有可以暴露给Internet的IP地址，那么就可以为其使用nat 0命令。单独使用nat 0命令不能允许从外向内的访问，如果策略允许从外向内的访问，那么还应该同时使用conduit命令。

例如：如图6-5，不对IP地址192.168.1.9进行翻译。为DMZ中的HTTP服务器分配此IP地址。应用nat (DMZ) 0命令后，PIX防火墙将不再对HTTP服务器的IP地址进行翻译。应用conduit命令后，PIX防火墙将允许对IP地址192.168.1.9的端口80的任何访问请求。配置如下：

```
conduit permit tcp host 192.168.1.9 eq www any  
nat (DMZ) 0 192.168.1.9 255.255.255.255
```

这个例子中，nat命令确保IP地址192.168.1.9不会被翻译。PIX防火墙的所有安全特性仍然在被继续使用。随后的conduit命令将允许对192.168.1.9的WWW访问。

❖ 配置FIXUP协议

fixup命令允许用户查看、改变、启用或禁止一个服务或协议通过PIX防火墙。由fixup命令指定的端口是PIX防火墙侦听的服务。我们可以对每项服务改变其端口号码，但RSH服务除外。

PIX防火墙根据包含在IP数据包中的TCP或UDP端口号来识别应用（由RFC 1700定义）。例如，它通过端口号21来识别FTP，端口号25来识别SMTP，端口号80来识别HTTP。

为了启用fixup命令，输入下列语句：

```
fixup protocol ftp [port]
```

```
fixup protocol http [port [-port]]
```

```
fixup protocol h323 [port [-port]]
```

```
fixup protocol rsh [514]
```

```
fixup protocol smtp [port [-port]]
```

```
fixup protocol sqlnet [port [-port]]
```

❖ 多媒体支持

对于一个防火墙来说，对多媒体应用的处理可能会非常麻烦，因为多媒体协议常会为连接动态地打开不同的端口。

对于多媒体应用，PIX防火墙提供了下列优点：

- *为安全的多媒体连接动态地开放和关闭UDP端口。其他防火墙可能要求配置开放一个很大的UDP端口范围，这样会带来安全风险；或者他们必须为入方向的多媒体数据配置一个端口，这样会要求客户端重新进行配置。
- *在使用或不使用NAT时都能支持多媒体应用。一些防火墙不能同时支持NAT和多媒体应用，这样就只能允许拥有注册IP地址的用户使用多媒体应用，并且需要向Internet暴露内部网络地址。



当前支持的多媒体应用如下所示：

- *Inter Internet Video Phone;
- *Microsoft Netmeeting(基于H.323标准);
- *RealNetworks RealAudio和RealVideo;
- *Xing Stream Works;
- *VDOnet VDOLive;
- *White Pines Meeting Point

配置多个接口

作为一种为网络提供安全保护的设备，具有两个接口的防火墙通常就足够了。在这种情况下，防火器只是为流入和流出网络的数据流担当一个安全网关。但是，只有两个接口常常是不够的。

如果用户曾经配置过两个接口，那么在PIX上配置附加的接口就会是一个相对简单的事情。只需要为附加的接口增加nameif、interface和ip address命令。

例：如图6-6，在PIX防火墙上配置多个接口

```
nameif ethernet0 outside sec0
```

```
nameif ethernet1 inside sec100
```

```
nameif ethernet2 dmz sec50
```

```
nameif ethernet3 partnernet sec20
```

```
interface ethernet0 auto
```

```
interface ethernet1 auto
```

```
interface ethernet2 auto
```

```
interface ethernet3 auto
```

```
ip address outside 192.168.0.2 255.255.255.0
```

```
ip address inside 10.0.0.1 255.255.255.0
```

```
ip address dmz 172.16.0.1 255.255.255.0
```

```
ip address partnernet 172.26.26.1 255.255.255.0
```



```
nat (inside) 1 10.0.0.0 255.255.255.0
global (outside)1 192.168.0.15-192.168.0.254
    netmask 255.255.255.0
global (dmz)1 172.16.0.10-172.16.0.254
    netmask 255.255.255.0
static (dmz,outside)192.168.0.11 172.16.0.2
conduit permit tcp host 192.168.0.11 eq http
any
```

如果我们的防火墙装备有三个或更多的接口，在使用NAT时，应遵循下列原则对它进行配置：

- *从PIX OS版本5.2X开始，外部接口可以被重新命名，但是缺省是outside。这个接口不能被赋予一个不同的安全级别（必须是最高安全级别）。
- *如果一个接口拥有较低的安全级别，那么它相对其他接口总是“外部的”。在没有适当的static和conduit或access-list命令的情况下，数据包不能在具有相同安全级别的接口之间流动。
- *只使用一条到外部接口缺省路由语句。用route命令设置缺省路由。
- *使用nat命令来让用户从相应的接口上发起向外的连接。在global语句之后，应保存配置，并输入clear xlate命令，这样在翻译表中的IP地址将会被更新（在建立一条新的连接时）。
- *允许访问受保护网络zhoong的服务器的一个方法是，使用static和conduit命令。

使用name命令

name命令让PIX防火墙能够在本地解析主机名与IP地址映射的一个列表。这就允许在配置中可以替代IP地址而使用名字。

names命令用以启用name命令。如：

```
names
```

```
name ip_address name
```

在定义了一个名字之后，它就可以替代IP地址，用于任何PIX防火墙命令中。可以通过输入命令no names，清除PIX防火墙配置中的名字。

name命令描述

ip_address：被命名的主机的IP地址。

name：分配给IP地址的名字。允许的字符是a到z、A到Z、0到9、破折号和下划线。name不能用数字开头。如果名字的长度超过16个字符，“name”命令将失败，名字是区分大小写的，而且必须含有字母数字型的字符，还支持使用下划线，但是名字的长度不能超过16个字符。