

第9章 配置Cisco PIX防火墙

本章包含下列主题：

- ❖ ASA安全级别
- ❖ Cisco PIX防火墙配置的6个基本命令

ASA安全级别

安全级别的范围是从0到100(见图4-1)：

- ❖ 安全级别100——对于一个接口来说，这是最高的安全级别。它被用于PIX防火墙的内部接口。这是PIX防火墙的缺省参数，不能被修改。
- ❖ 安全级别0——这是最低的安全级别。这种安全级别被用于PIX防火墙的外部接口。这是PIX防火墙的缺省参数，不能被修改。
- ❖ 安全级别1~99——这些安全级别可以被分配给连接PIX防火墙的边界接口。通常，将这些边界接口中的一个连接到作为停火区（DMZ）的一个网络。DMZ是一台设备或网络，对于来自不被信任环境中的用户来说，DMZ通常是可以被访问的。DMZ是一个隔离的区域，是从内部被信任的环境中隔离出来的。

下面是在PIX防火墙和其他边界设备之间不同接口连接的几个实例，可以通过一些配置来实现。

- ❖ 从一个相对安全（高安全级别）的接口流向一个不太安全（低安全级别）接口的数据。
- ❖ 从一个不太安全（低安全级别）的接口流向一个相对安全（高安全级别）接口的数据。
- ❖ 在两个具有相同安全级别的接口之间流动的数据

配置Cisco PIX防火墙的6个基本命令

有6个基本配置命令被认为是PIX防火墙的基础。nameif、interface和ip address命令对于PIX的运行是必要的。nat、global和route命令虽然不是必需的，但是也经常会被使用。为了让数据流通过PIX防火墙，必须对它进行配置。nat和global命令通常用于提供从一个相对可信的网络（高安全级别接口）的访问。

❖ nameif命令

命令nameif为PIX防火墙上的每个接口分配一个名字，并指定它的安全级别（PIX防火墙的内部接口和外部接口除外，它们的名字是缺省的）。

语法：nameif hardware_id if_name security_level

其中：

hardware_id：指定一个边界接口，以及它在PIX防火墙上的物理位置。PIX防火墙可以支持三种类型的接口：以太网、FDDI和令牌环接口。例如，以太网接口可以被标识为ethernet1、ethernet2、ethernet3等；

if_name：为物理边界接口指定一个名字。这个名字是由用户指定的，而且必须被用于所有未来的配置中，以提供对边界接口的引用。缺省情况下，接口e1的名字是inside（内部接口），接口e0的名字是outside（外部接口）。

security_level：为边界接口指定安全级别。输入取值范围为1~99的安全级别。

❖ interface命令

interface命令用以确定硬件类型，设置硬件速度，并启用接口。当在PIX防火墙上安装一块附加的以太网接口卡时，PIX防火墙可以自动识别这块附加的卡。

语法：interface hardware_id hardware_speed [shutdown]

例如：

```
interface ethernet0 10baset shutdown
```

```
interface ethernet1 10baset shutdown
```

```
interface ethernet0 10baset
```

```
interface ethernet1 10baset
```

其中：

`hardware_id`：指定一个接口，以及它在PIX防火墙上的物理位置。用法与`nameif`命令中相同。

`hardware_speed`：确定连接速度。输入“auto”，这样PIX防火墙就可以自动感知设备所需的速度。对于网络接口速度，以太网可能的值是：10baset—10Mbit/s以太网半双工通信；10full—10Mbit/s以太网全双工通信。

`shutdown`：管理性的关闭这个窗口。

❖ ip address命令

PIX防火墙上的每个接口都必须用一个IP地址进行配置。

语法：ip address if_name ip_address [netmask]

其中，

ip_name：描述了这个接口。这个名字是由用户指定的，而且必须被用于所有未来的配置中，以提供对这个接口的引用。

ip_address：为接口分配的IP地址。

netmask：如果没有指定网络掩码，将采用“有类别（classful）”的网络掩码——A类255.0.0.0
B类255.255.0.0 C类255.255.255.0

❖ nat命令

网络地址翻译（NAT）让用户能够保持内部IP地址对于外部网络是未知的。nat命令需要完成的工作是，在数据包被转发到外部网络之前，将内部未经注册的IP地址（这些地址不具有全球唯一性）翻译成经过注册的、全球接受的IP地址。除了nat 0以外，nat命令总是与global命令一起使用。

语法：nat (if_name) nat_id local_ip [netmask]

其中，(if_name)：描述将使用全局地址的内部网络接口名字。数据将通过在global命令中指定的接口，离开PIX。

nat_id : 标识全局地址池，并使它与其相应
global命令相匹配。

local_ip : 在内部网络上，分配给设备的IP地址。可以使用0.0.0.0，来允许所有的向外连接使用来自全局池中IP地址进行翻译。

netmask : 本地IP地址的网络掩码。

在刚开始配置PIX防火墙时，可以用

nat 1 0.0.0.0 0.0.0.0命令，允许所有的内部主机向外进行连接访问，并由相应的global命令所指定的全局地址对外进行访问。nat命令可以指定一台主机或一段范围内的主机，这样使访问更具有选择性。

在配置该命令的时候，可以用0代替0.0.0.0。
用0代表0.0.0.0的例子如下：

```
pixfirewall#(config) nat (inside) 1 0 0
```

在任何需要指定0.0.0.0的PIX命令中，都可以使用这种简写方式。

❖ global命令

当从一个被信任的网络向一个不被信任的网络发送数据时，通常需要翻译源IP地址。PIX采用两个命令来进行这项工作。第一个命令是nat，它定义了将要被翻译的、被信任的源地址。用来定义源地址将要翻译成的地址或地址范围的命令是global。

语法：pixfirewall#(config) nat (inside) 1 0 0

其中，

if_name：描述我们将要为之使用全局地址的外部网络接口名字。

nat_id：指示全局地址池，并使它与其相应的nat命令相匹配。

interface：让PIX防火墙将由nat命令所指定的所有IP地址翻译到该指定的接口。这被称为接口PAT。

global_ip：单个IP地址，或一段全局IP地址范围的起始IP地址。

-global_ip：一段全局IP地址范围。

netmask global_mask：全局IP地址的网络掩码。如果子网是有效的，就使用子网掩码（例如，255.255.255.128）。如果我们指定的地址范围与用netmask命令选项指定的子网相交迭，这个命令将不使用全局地址池中的广播或网段地址。例如：如果我们使用网络掩码255.255.255.128，与地址范围192.150.50.20—192.128.50.140，那么广播地址192.128.50.127和网段地址192.128.50.128将不被包括在全局地址池中。

当从内部网络中的一台设备上发出的外出IP包到达PIX防火墙时，源地址被提取出来，并于内部的一张现有翻译表进行比较。如果该设备的地址不在这个表中，就对它进行翻译。为那台设备产生一个新的表项，并从全局IP地址池中为它分配一个全局IP地址。这被称为翻译槽位（translation slot）。翻译后，翻译表被更新，并转发经过翻译的IP包。

在用户配置的时间限制后，或者缺省的三个小时后，如果在这段时间内没有那个特定IP地址的翻译数据包，那么，这个表项就被从表中删除，并释放全局地址，使它可以用于其他的内部设备。

图4-2显示了NAT。如果用nat命令，必须对伴随的global命令进行配置，来定义翻译IP地址池。为了删除一个全局表项，可以使用命令no global。例如：

```
no global [outside]1 192.168.1.10-  
192.168.1.254 netmask 255.255.0.0
```

❖ route命令

route命令为接口定义一条静态路由。route命令语句可以具有一个具有的目的地址，或者可以产生一条缺省的静态路由。

语法：route if_name ip_address netmask gateway_ip [metric]

其中，if_name：描述内部或外部网络接口的名字。数据将通过这个接口离开PIX。

ip_address：描述目的地（内部或外部）网络IP地址。用0.0.0.0指定缺省路由（所有的目标网络）。可以将IP地址0.0.0.0简写为0。

netmask：指定应用于ip_address的网络掩码。用0.0.0.0指定一条缺省路由。可以将网络掩码0.0.0.0简写为0。设置一条路由是一种比较常见的情况。

gateway_ip：指定网关路由器的IP地址（这条路由的下一跳地址）。

metric：制定到gateway_ip的跳数。如果我们不能确定，就输入1。我们的WAN管理员可以提供这项信息，或者我们可以用traceroute命令得到跳数。如果不指定度量值（metric），缺省是1。

例：用六个基本命令配置PIX防火墙

```
nameif ethernet0 outside security0
```

```
nameif ethernet1 inside security100
```

```
nameif ethernet2 dmz security50
```

```
nameif ethernet3 pix/intf3 security15
```

```
nameif ethernet4 pix/intf4 security20
```

```
nameif ethernet5 pix/intf5 security25
```

```
interface ethernet0 100full
```

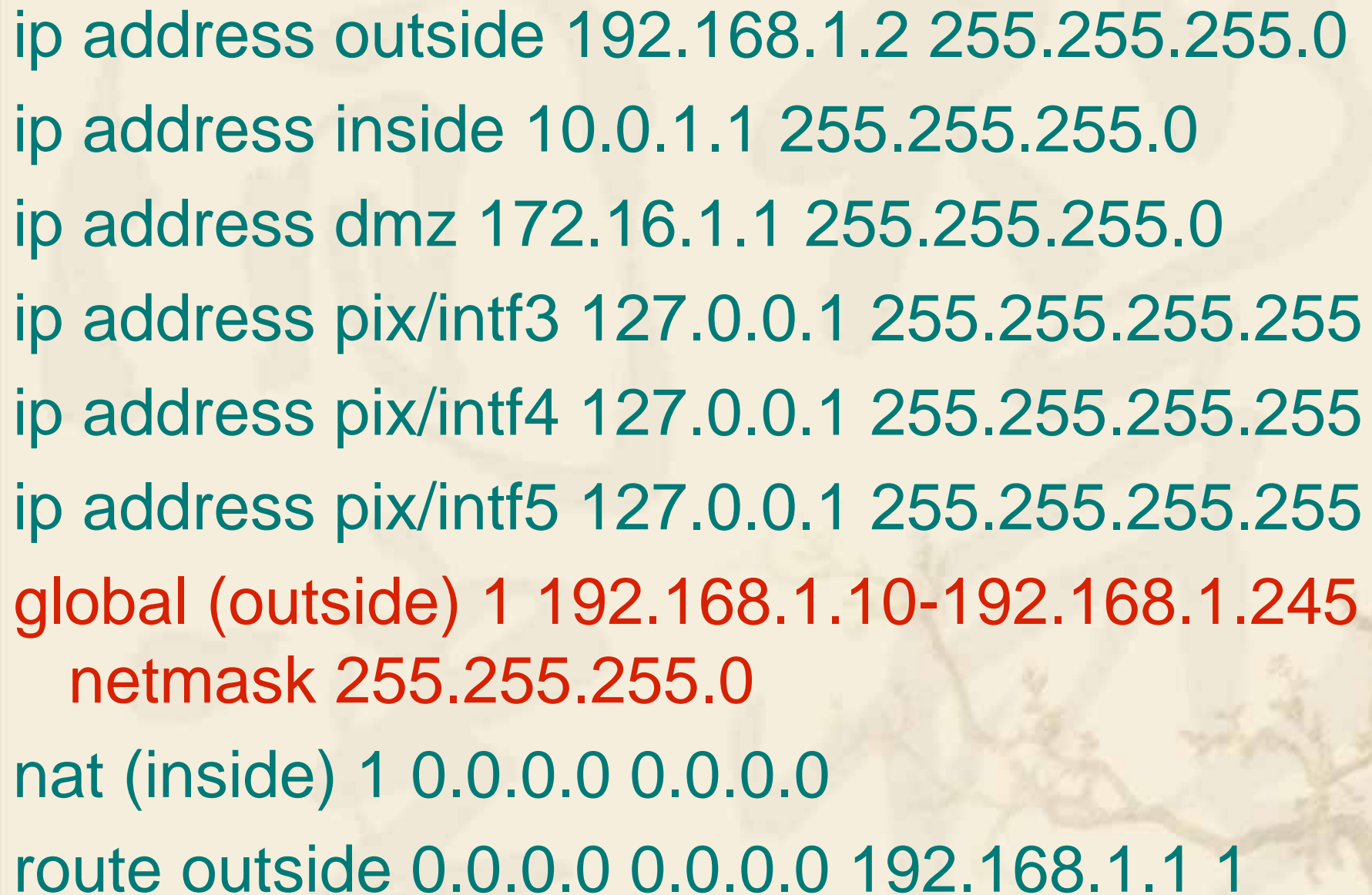

```
interface ethernet1 100full
```

```
interface ethernet2 100full
```

```
interface ethernet3 auto shutdown
```

```
interface ethernet4 auto shutdown
```

```
interface ethernet5 auto shutdown
```

```
ip address outside 192.168.1.2 255.255.255.0
ip address inside 10.0.1.1 255.255.255.0
ip address dmz 172.16.1.1 255.255.255.0
ip address pix/intf3 127.0.0.1 255.255.255.255
ip address pix/intf4 127.0.0.1 255.255.255.255
ip address pix/intf5 127.0.0.1 255.255.255.255
global (outside) 1 192.168.1.10-192.168.1.245
    netmask 255.255.255.0
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
```