硬件防火墙的配置过程讲解

【导读】本篇要为大家介绍一些实用的知识，那就是如何配置防火中的安全策略。但要注意的是，防火墙的具体配置方法也不是千篇一律的，不要说不同品牌，就是同一品

牌的不同型号也不完全一样，所以在此也只能对一些通用防火墙配置方法作一基本介绍。同时，具体的防火墙策略配置会因具体的应用环境不同而有较大区别。

本篇要为大家介绍一些实用的知识，那就是如何配置防火中的安全策略。但要注意的是，防火墙的具体配置方法也不是千篇一律的，不要说不同品牌，就是同一品牌的不同型号也不完全一样，所以在此也只能对一些通用防火墙配置方法作一基本介绍。同时，具体的防火墙策略配置会因具体的应用环境不同而有较大区别。首先介绍一些基本的配置原则。

一. 防火墙的基本配置原则

默认情况下，所有的防火墙都是按以下两种情况配置的：

●拒绝所有的流量，这需要在你的网络中特殊指定能够进入和出去的流量的一些类型。

●允许所有的流量，这种情况需要你特殊指定要拒绝的流量的类型。可论证地，大多数防火墙默认都是拒绝所有的流量作为安全选项。一旦你安装防火墙后，你需要打开一些必要的端口来使防火墙内的用户在通过验证之后可以访问系统。换句话说，如果你想让你的员工们能够发送和接收 Email，你必须在防火墙上设置相应的规则或开启允许 POP3 和 SMTP 的进程。

在防火墙的配置中，我们首先要遵循的原则就是安全实用，从这个角度考虑，在防火墙的配置过程中需坚持以下三个基本原则：

（1）．简单实用：对防火墙环境设计来讲，首要的就是越简单越好。其实这也是任何事物的基本原则。越简单的实现方式，越容易理解和使用。而且是设计越简单，越不容易出错，防火墙的安全功能越容易得到保证，管理也越可靠和简便。

每种产品在开发前都会有其主要功能定位，比如防火墙产品的初衷就是实现网络之间的安全控制，入侵检测产品主要针对网络非法行为进行监控。但是随着技术的成熟和发展，这些产品在原来的主要功能之外或多或少地增加了一些增值功能，比如在防火墙上增加了查杀病毒、入侵检测等功能，在入侵检测上增加了病毒查杀功能。但是这些增值功能并不是所有应用环境都需要，在配置时我们也可针对具体应用环境进行配置，不必要对每一功能都详细配置，这样一则会大大增强配置难度，同时还可能因各方面配置不协调，引起新的安全漏洞，得不偿失。

（2）．全面深入：单一的防御措施是难以保障系统的安全的，只有采用全面的、多层次的深层防御战略体系才能实现系统的真正安全。在防火墙配置中，我们不要停留在几个表面的防火墙语句上，而应系统地看等整个网络的安全防护体系，尽量使各方面的配置相互加强，从深层次上防护整个系统。这方面可以体现在两个方面：一方面体现在防火墙系统的部署上，多层次的防火墙部署体系，即采用集互联网边界防火墙、部门边界防火墙和主机防火墙于一体的层次防御；另一方面将入侵检测、网络加密、病毒查杀等多种安全措施结合在一起的多层安全体系。

（3）．内外兼顾：防火墙的一个特点是防外不防内，其实在现实的网络环境中，80%以上的威胁都来自内部，所以我们要树立防内的观念，从根本上改变过去那种防外不防内的传统观念。对内部威胁可以采取其它安全措施，比如入侵检测、主机防护、漏洞扫描、病毒查杀。这方面体现在防火墙配置方面就是要引入全面防护的观念，最好能部署与上述内部防护手段一起联动的机制。目前来说，要做到这一点比较困难。

二、防火墙的初始配置

像路由器一样，在使用之前，防火墙也需要经过基本的初始配置。但因各种防火墙的初始配置基本类似，所以在此仅以 Cisco PIX 防火墙为例进行介绍。

防火墙的初始配置也是通过控制端口（Console）与 PC 机（通常是便于移动的笔记本电脑）的串口连接，再通过 Windows 系统自带的超级终端（HyperTerminal）程序进行选项配置。防火墙的初始配置物理连接与前面介绍的交换机初始配置连接方法一样，参见图 1 所示。

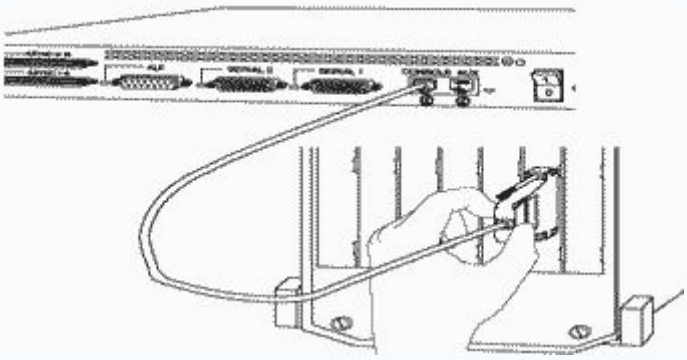


图 1

防火墙除了以上所说的通过控制端口（Console）进行初始配置外，也可以通过 telnet 和 Tffp 配置方式进行高级配置，但 Telnet 配置方式都是在命令方式中配置，难度较大，而 Tffp 方式需要专用的 Tffp 服务器软件，但配置界面比较友好。

防火墙与路由器一样也有四种用户配置模式，即：普通模式（Unprivileged mode）、特权模式（Privileged Mode）、配置模式（Configuration Mode）和端口模式（Interface Mode），进入这四种用户模式的命令也与路由器一样：

普通用户模式无需特别命令，启动后即进入；

进入特权用户模式的命令为"enable"；进入配置模式的命令为"config terminal"；而进入端口模式的命令为"interface ethernet（）"。不过因为防火墙的端口没有路由器那么复杂，所以通常把端口模式归为配置模式，统称为"全局配置模式"。

防火墙的具体配置步骤如下：

1. 将防火墙的 Console 端口用一条防火墙自带的串行电缆连接到笔记本电脑的一个空余串口上，参见图 1。

2. 打开 PIX 防火电源，让系统加电初始化，然后开启与防火墙连接的主机。

3. 运行笔记本电脑 Windows 系统中的超级终端（HyperTerminal）程序（通常在"附件"程序组中）。对超级终端的配置与交换机或路由器的配置一样，参见本教程前面有关介绍。

4. 当 PIX 防火墙进入系统后即显示"pixfirewall>"的提示符，这就证明防火墙已启动成功，所进入的是防火墙用户模式。可以进行进一步的配置了。

5. 输入命令：enable,进入特权用户模式，此时系统提示为：pixfirewall#。

6. 输入命令：configure terminal,进入全局配置模式，对系统进行初始化设置。

（1）. 首先配置防火墙的网卡参数（以只有 1 个 LAN 和 1 个 WAN 接口的防火墙配置为例）

Interface ethernet0 auto　　# 0 号网卡系统自动分配为 WAN 网卡，"auto"选项为系统自适应网卡类型

Interface ethernet1 auto

（2）. 配置防火墙内、外部网卡的 IP 地址

IP address inside ip_address netmask　# Inside 代表内部网卡
IP address outside ip_address netmask　# outside 代表外部网卡

（3）. 指定外部网卡的 IP 地址范围：

global 1 ip_address-ip_address

（4）. 指定要进行转换的内部地址

nat 1 ip_address netmask

（5）. 配置某些控制选项：

conduit global_ip port[-port] protocol foreign_ip [netmask]

其中，global_ip：指的是要控制的地址；port：指的是所作用的端口，0 代表所有端口；protocol：指的是连接协议，比如：TCP、UDP 等；foreign_ip：表示可访问的 global_ip 外部 IP 地址；netmask：为可选项，代表要控制的子网掩码。

7. 配置保存：wr mem

8. 退出当前模式

此命令为 exit，可以任何用户模式下执行，执行的方法也相当简单，只输入命令本身即可。它与 Quit 命令一样。下面三条语句表示了用户从配置模式退到特权模式，再退到普通模式下的操作步骤。

pixfirewall(config)# exit
pixfirewall# exit
pixfirewall>

9. 查看当前用户模式下的所有可用命令：show，在相应用户模式下键入这个命令后，即显示出当前所有可用的命令及简单功能描述。

10. 查看端口状态：show interface，这个命令需在特权用户模式下执行，执行后即显示出防火墙所有接口配置情况。

11. 查看静态地址映射:show static，这个命令也须在特权用户模式下执行，执行后显示防火墙的当前静态地址映射情况。

三、Cisco PIX 防火墙的基本配置

1. 同样是用一条串行电缆从电脑的 COM 口连到 Cisco PIX 525 防火墙的 console 口；

2. 开启所连电脑和防火墙的电源，进入 Windows 系统自带的"超级终端"，通讯参数可按系统默然。进入防火墙初始化配置，在其中主要设置有：Date(日期)、time(时间)、hostname(主机名称)、inside ip address(内部网卡 IP 地址)、domain(主域)等，完成后也就建立了一个初始化设置了。此时的提示符为：pix255>。

3. 输入 enable 命令，进入 Pix 525 特权用户模式,默然密码为空。

如果要修改此特权用户模式密码，则可用 enable password 命令，命令格式为：enable password password [encrypted]，这个密码必须大于 16 位。Encrypted 选项是确定所加密码是否需要加密。

4、 定义以太端口：先必须用 enable 命令进入特权用户模式，然后输入 configure terminal（可简称为 config t），进入全局配置模式模式。具体配置

pix525>enable
Password:
pix525#config t
pix525 (config)#interface ethernet0 auto
pix525 (config)#interface ethernet1 auto

在默然情况下 ethernet0 是属外部网卡 outside, ethernet1 是属内部网卡 inside, inside 在初始化配置成功的情况下已经被激活生效了, 但是 outside 必须命令配置激活。

5. clock

配置时钟, 这也非常重要, 这主要是为防火墙的日志记录而资金积累的, 如果日志记录时间和日期都不准确, 也就无法正确分析记录中的信息。这须在全局配置模式下进行。

时钟设置命令格式有两种, 主要是日期格式不同, 分别为:

clock set hh:mm:ss month day month year 和 clock set hh:mm:ss day month year

前一种格式为:小时:分钟:秒 月 日 年;而后一种格式为:小时:分钟:秒 日 月 年, 主要在日、月份的前后顺序不同。在时间上如果为 0, 可以为一位, 如:21:0:0。

6. 指定接口的安全级别

指定接口安全级别的命令为 nameif, 分别为内、外部网络接口指定一个适当的安全级别。在此要注意, 防火墙是用来保护内部网络的, 外部网络是通过外部接口对内部网络构成威胁的, 所以要从根本上保障内部网络的安全, 需要对外部网络接口指定较高的安全级别, 而内部网络接口的安全级别稍低, 这主要是因为内部网络通信频繁、可信度高。在 Cisco PIX 系列防火墙中, 安全级别的定义是由 security () 这个参数决定的, 数字越小安全级别越高, 所以 security0 是最高的, 随后通常是以 10 的倍数递增, 安全级别也相应降低。如下例:

pix525(config)#nameif ethernet0 outside security0 # outside 是指外部接口

pix525(config)#nameif ethernet1 inside security100 # inside 是指内部接口

7. 配置以太网接口 IP 地址

所用命令为 :ip address, 如要配置防火墙上的内部网接口 IP 地址为 :192.168.1.0 255.255.255.0;外部网接口 IP 地址为:220.154.20.0 255.255.255.0。

配置方法如下:

pix525(config)#ip address inside 192.168.1.0 255.255.255.0

pix525(config)#ip address outside 220.154.20.0 255.255.255.0

8. access-group

这个命令是把访问控制列表绑定在特定的接口上。须在配置模式下进行配置。命令格式为:access-group acl_ID in interface interface_name, 其中的"acl_ID"是指访问控制列表名称, interface_name 为网络接口名称。如:

access-group acl_out in interface outside, 在外部网络接口上绑定名称为"acl_out"的访问控制列表。

clear access-group:清除所有绑定的访问控制绑定设置。

no access-group acl_ID in interface interface_name:清除指定的访问控制绑定设置。

show access-group acl_ID in interface interface_name:显示指定的访问控制绑定设置。

9. 配置访问列表

所用配置命令为:access-list, 合格格式比较复杂, 如下:

标准规则的创建命令:access-list [normal | special] listnumber1 { permit | deny } source-addr [source-mask]

扩展规则的创建命令:access-list [normal | special] listnumber2 { permit |

deny } protocol source-addr source-mask [operator port1 [port2]] dest-addr dest-mask [operator port1 [port2] | icmp-type [icmp-code]] [log]

它是防火墙的主要配置部分，上述格式中带"[]"部分是可选项，listnumber 参数是规则号，标准规则号（listnumber1）是 1~99 之间的整数，而扩展规则号（listnumber2）是 100~199 之间的整数。它主要是通过访问权限"permit"和"deny"来指定的，网络协议一般有 IP|TCP|UDP|ICMP 等等。如只允许访问通过防火墙对主机:220.154.20.254 进行 www 访问，则可按以下配置：

pix525(config)#access-list 100 permit 220.154.20.254 eq www

其中的 100 表示访问规则号，根据当前已配置的规则条数来确定，不能与原来规则的重复，也必须是正整数。关于这个命令还将在下面的高级配置命令中详细介绍。

10. 地址转换（NAT）

防火墙的 NAT 配置与路由器的 NAT 配置基本一样，首先也必须定义供 NAT 转换的内部 IP 地址组，接着定义内部网段。

定义供 NAT 转换的内部地址组的命令是 nat，它的格式为：nat [(if_name)] nat_id local_ip [netmask [max_conns [em_limit]]]，其中 if_name 为接口名；nat_id 参数代表内部地址组号；而 local_ip 为本地网络地址；netmask 为子网掩码；max_conns 为此接口上所允许的最大 TCP 连接数，默认为"0"，表示不限制连接；em_limit 为允许从此端口发出的连接数，默认也为"0"，即不限制。如：

nat (inside) 1 10.1.6.0 255.255.255.0

表示把所有网络地址为 10.1.6.0，子网掩码为 255.255.255.0 的主机地址定义为 1 号 NAT 地址组。

随后再定义内部地址转换后可用的外部地址池，它所用的命令为 global,基本命令格式为：

global [(if_name)] nat_id global_ip [netmask [max_conns [em_limit]]]，各参数解释同上。如：

global (outside) 1 175.1.1.3-175.1.1.64 netmask 255.255.255.0

将上述 nat 命令所定的内部 IP 地址组转换成 175.1.1.3~175.1.1.64 的外部地址池中的外部 IP 地址，其子网掩耳盗铃码为 255.255.255.0。

11. Port Redirection with Statics

这是静态端口重定向命令。在 Cisco PIX 版本 6.0 以上，增加了端口重定向的功能，允许外部用户通过一个特殊的 IP 地址/端口通过防火墙传输到内部指定的内部服务器。其中重定向后的地址可以是单一外部地址、共享的外部地址转换端口（PAT），或者是共享的外部端口。这种功能也就是可以发布内部 WWW、FTP、Mail 等服务器，这种方式并不是直接与内部服务器连接，而是通过端口重定向连接的，所以可使内部服务器很安全。

命令格式有两种，分别适用于 TCP/UDP 通信和非 TCP/UDP 通信：

（1）． static[(internal_if_name, external_if_name)]{global_ip|interface}local_ip[netmask mask] max_conns [emb_limit[norandomseq]]]

（2）. static [(internal_if_name, external_if_name)] {tcp|udp}{global_ip|interface} global_port local_ip local_port [netmask mask] [max_conns [emb_limit [norandomseq]]]

此命令中的以上各参数解释如下：

internal_if_name :内部接口名称 ;external_if_name :外部接口名称 ;{tcp|udp}：选择通信协议类型；{global_ip|interface}：重定向后的外部 IP 地址或共享端口；local_ip：本地 IP 地址；[netmask mask]：本地子网掩码；max_conns：允许的最大 TCP 连接数，默认为"0"，即不限制；emb_limit：允许从此端口发起的连接数，默认也为"0"，即不限制；norandomseq：不对数据包排序，此参数通常不用选。

现在我们举一个实例，实例要求如下

●外部用户向 172.18.124.99 的主机发出 Telnet 请求时，重定向到 10.1.1.6。

●外部用户向 172.18.124.99 的主机发出 FTP 请求时，重定向到 10.1.1.3。

●外部用户向 172.18.124.208 的端口发出 Telnet 请求时，重定向到 10.1.1.4。

●外部用户向防火墙的外部地址 172.18.124.216 发出 Telnet 请求时，重定向到 10.1.1.5。

●外部用户向防火墙的外部地址 172.18.124.216 发出 HTTP 请求时，重定向到 10.1.1.5。

●外部用户向防火墙的外部地址 172.18.124.208 的 8080 端口发出 HTTP 请求时，重定向到 10.1.1.7 的 80 号端口。

以上重写向过程要求如图 2 所示，防火墙的内部端口IP地址为 10.1.1.2，外部端口地址为 172.18.124.216。

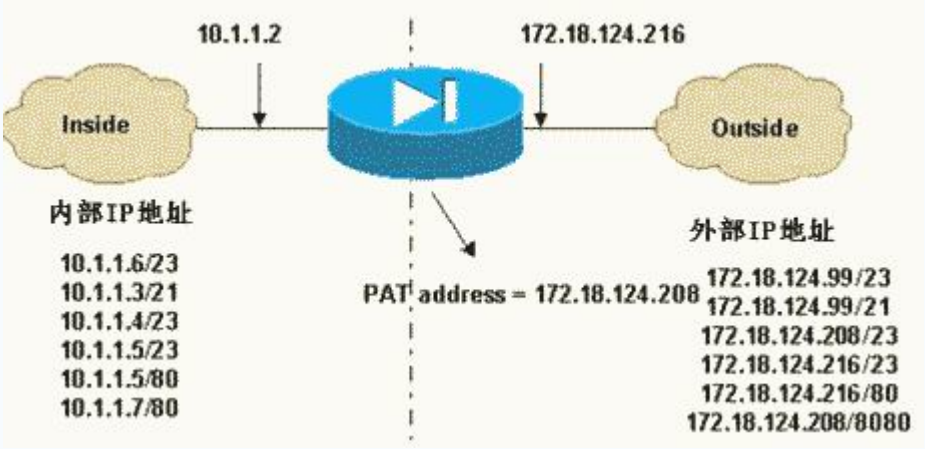


图 2

以上各项重定向要求对应的配置语句如下：

```
static (inside,outside) tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.99 ftp 10.1.1.3 ftp netmask
255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 telnet 10.1.1.4 telnet netmask
255.255.255.255 0 0
static (inside,outside) tcp interface telnet 10.1.1.5 telnet netmask
255.255.255.255 0 0
static (inside,outside) tcp interface www 10.1.1.5   www netmask
255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7 www netmask
255.255.255.255 0 0
```

12. 显示与保存结果

显示结果所用命令为：show config；保存结果所用命令为：write memory。

四、包过滤型防火墙的访问控制表（ACL）配置

除了以上介绍的基本配置外，在防火墙的安全策略中最重要还是对访问控制列表（ACL）进行配有关置。下面介绍一些用于此方面配置的基本命令。

1. access-list：用于创建访问规则

这一访问规则配置命令要在防火墙的全局配置模式中进行。同一个序号的规则可以看作一类规则，同一个序号之间的规则按照一定的原则进行排列和选择，这个顺序可以通过 show access-list 命令看到。在这个命令中，又有几种命令格式，分别执行不同的命令。

（1）创建标准访问列表

命令格式：access-list [normal | special] listnumber1 { permit | deny } source-addr [source-mask]

（2）创建扩展访问列表

命令格式：access-list [normal | special] listnumber2 { permit | deny } protocol source-addr source-mask [operator port1 [port2]] dest-addr dest-mask [operator port1 [port2] | icmp-type [icmp-code]] [log]

（3）删除访问列表

命令格式：no access-list { normal | special } { all | listnumber [subitem] }

上述命令参数说明如下：

●normal：指定规则加入普通时间段。

●special：指定规则加入特殊时间段。

●listnumber1：是 1 到 99 之间的一个数值，表示规则是标准访问列表规则。

●listnumber2：是 100 到 199 之间的一个数值，表示规则是扩展访问列表规则。

●permit：表明允许满足条件的报文通过。

●deny：表明禁止满足条件的报文通过。

●protocol：为协议类型，支持 ICMP、TCP、UDP 等，其它的协议也支持，此时没有端口比较的概念；为 IP 时有特殊含义，代表所有的 IP 协议。

●source-addr：为源 IP 地址。

●source-mask：为源 IP 地址的子网掩码，在标准访问列表中是可选项，不输入则代表通配位为 0.0.0.0。

●dest-addr：为目的 IP 地址。

●dest-mask：为目的地址的子网掩码。

●operator：端口操作符，在协议类型为 TCP 或 UDP 时支持端口比较，支持的比较操作有：等于（eq）、大于（gt）、小于（lt）、不等于（neq）或介于（range）；如果操作符为 range，则后面需要跟两个端口。

port1 在协议类型为 TCP 或 UDP 时出现，可以为关键字所设定的预设值（如 telnet）或 0~65535 之间的一个数值。port2 在协议类型为 TCP 或 UDP 且操作类型为 range 时出现；可以为关键字所设定的预设值（如 telnet）或 0~65535 之间的一个数值。

●icmp-type：在协议为 ICMP 时出现，代表 ICMP 报文类型；可以是关键字所设定的预设值（如 echo-reply）或者是 0~255 之间的一个数值。

●icmp-code：在协议为 ICMP，且没有选择所设定的预设值时出现；代表 ICMP 码，是 0~255 之间的一个数值。

●log：表示如果报文符合条件，需要做日志。

●listnumber：为删除的规则序号，是 1~199 之间的一个数值。

●subitem：指定删除序号为 listnumber 的访问列表中规则的序号。

例如，现要在华为的一款防火墙上配置一个"允许源地址为 10.20.10.0 网络、目的地址为 10.20.30.0 网络的 WWW 访问，但不允许使用 FTP"的访问规则。相应配置语句只需两行即可，如下：

Quidway (config)#access-list 100 permit tcp
10.20.10.0 255.0.0.0 10.20.30.0 255.0.0.0 eq www
Quidway (config)#access-list 100 deny tcp
10.20.10.0 255.0.0.0 10.20.30.0 255.0.0.0 eq ftp

2. clear access-list counters：清除访问列表规则的统计信息

命令格式：clear access-list counters [listnumber]

这一命令必须在特权用户模式下进行配置。listnumber 参数是用指定要清除统计信息的规则号，如不指定，则清除所有的规则的统计信息。

如要在华为的一款包过滤路由器上清除当前所使用的规则号为 100 的访问规则统计信息。访问配置语句为：

clear access-list counters 100

如有清除当前所使用的所有规则的统计信息，则以上语句需改为：Quidway#clear access-list counters

3. ip access-group

使用此命令将访问规则应用到相应接口上。使用此命令的 no 形式来删除相应的设置，对应格式为：

ip access-group listnumber { in | out }

此命令须在端口用户模式下配置，进入端口用户模式的命令为 :interface ethernet （），括号中为相应的端口号，通常 0 为外部接口，而 1 为内部接口。进入后再用 ip access-group 命令来配置访问规则。listnumber 参数为访问规则号，是 1~199 之间的一个数值（包括标准访问规则和扩展访问规则两类）；in 表示规则应用于过滤从接口接收到的报文；而 out 表示规则用于过滤从接口转发出去的报文。一个接口的一个方向上最多可以应用 20 类不同的规则；这些规则之间按照规则序号的大小进行排列，序号大的排在前面，也就是优先级高。对报文进行过滤时，将采用发现符合的规则即得出过滤结果的方法来加快过滤速度。所以，建议在配置规则时，尽量将对同一个网络配置的规则放在同一个序号的访问列表中；在同一个序号的访问列表中，规则之间的排列和选择顺序可以用 show access-list 命令来查看。

例如将规则 100 应用于过滤从外部网络接口上接收到的报文，配置语句为（同样为在倾为包过滤路由器上）：

ip access-group 100 in

如果要删除某个访问控制表列绑定设置，则可用 no ip access-group listnumber { in | out } 命令。

4. show access-list

此配置命令用于显示包过滤规则在接口上的应用情况。命令格式为：show access-list [all | listnumber | interface interface-name]

这一命令须在特权用户模式下进行配置，其中 all 参数表示显示所有规则的应用情况，包括普通时间段内及特殊时间段内的规则；如果选择 listnumber 参数，则仅需显示指定规则号的过滤规则；interface 表示要显示在指定接口上应用的所有规则序号；interface-name 参数为接口的名称。

使用此命令来显示所指定的规则，同时查看规则过滤报文的情况。每个规则都有一个相应的计数器，如果用此规则过滤了一个报文，则计数器加 1；通过对计数器的观察

可以看出所配置的规则中，哪些规则是比较有效，而哪些基本无效。例如，现在要显示当前所使用序号为 100 的规则的使用情况，可执行 Quidway#show access-list 100 语句即可，随即系统即显示这条规则的使用情况，格式如下：

Using normal packet-filtering access rules now.

100 deny icmp 10.1.0.0 0.0.255.255 any host-redirect (3 matches,252 bytes -- rule 1)

100 permit icmp 10.1.0.0 0.0.255.255 any echo (no matches -- rule 2)

100 deny udp any any eq rip (no matches -- rule 3)

5. show firewall

此命令须在特权用户模式下执行，它显示当前防火墙状态。命令格式非常简单，也为：show firewall。这里所说的防火墙状态，包括防火墙是否被启用，启用防火墙时是否采用了时间段包过滤及防火墙的一些统计信息。

6. Telnet

这是用于定义能过防火配置控制端口进行远程登录的有关参数选项，也须在全局配置用户模式下进行配置。

命令格式为：telnet ip_address [netmask] [if_name]

其中的 ip_address 参数是用来指定用于 Telnet 登录的 IP 地址，netmask 为子网掩码，if_name 用于指定用于 Telnet 登录的接口，通常不用指定，则表示此 IP 地址适用于所有端口。如：

telnet 192.168.1.1

如果要清除防火墙上某个端口的 Telnet 参数配置，则须用 clear telnet 命令，其格式为：clear telnet [ip_address [netmask] [if_name]]，其中各选项说明同上。它与另一个命令 no telnet 功能基本一样，不过它是用来删除某接口上的 Telnet 配置，命令格式为：no telnet [ip_address [netmask] [if_name]]。

如果要显示当前所有的 Telnet 配置，则可用 show telnet 命令。

思科 PIX 防火墙

【导读】思科 PIX 防火墙可以保护各种网络。有用于小型家庭网络的 PIX 防火墙，也有用于大型园区或者企业网络的 PIX 防火墙。在本文的例子中，我们将设置一种 PIX 501 型防火墙。PIX 501 是用于小型家庭网络或者小企业的防火墙。

在本期应用指南中，管理员可以学到如何设置一个新的 PIX 防火墙。你将设置口令、IP 地址、网络地址解析和基本的防火墙规则。

假如你的老板交给你一个新的 PIX 防火墙。这个防火墙是从来没有设置过的。他说，这个防火墙需要设置一些基本的 IP 地址、安全和一些基本的防火墙规则。你以前从来没有使用过 PIX 防火墙。你如何进行这种设置?在阅读完这篇文章之后，这个设置就很容易了。 下面，让我们看看如何进行设置。

思科 PIX 防火墙的基础

思科 PIX 防火墙可以保护各种网络。有用于小型家庭网络的 PIX 防火墙，也有用于大型园区或者企业网络的 PIX 防火墙。在本文的例子中，我们将设置一种 PIX 501 型防火墙。PIX 501 是用于小型家庭网络或者小企业的防火墙。

PIX 防火墙有内部和外部接口的概念。内部接口是内部的，通常是专用的网络。外部接口是外部的，通常是公共的网络。你要设法保护内部网络不受外部网络的影响。

PIX 防火墙还使用自适应性安全算法(ASA)。这种算法为接口分配安全等级，并且声称如果没有规则许可，任何通信都不得从低等级接口(如外部接口)流向高等级接口(如内部接口)。这个外部接口的安全等级是“0”，这个内部接口的安全等级是“100”。

下面是显示“nameif”命令的输出情况：

```
pixfirewall# show nameif
nameif ethernet0 outside security0
nameif ethernet1 inside security100
pixfirewall#
```

请注意，ethernet0(以太网 0)接口是外部接口(它的默认名字)，安全等级是 0。另一方面，ethernet1(以太网 1)接口是内部接口的名字(默认的)，安全等级是 100。

指南

在开始设置之前，你的老板已经给了你一些需要遵守的指南。这些指南是：

·所有的口令应该设置为“思科”(实际上，除了思科之外，你可设置为任意的口令)。

·内部网络是 10.0.0.0，拥有一个 255.0.0.0 的子网掩码。这个 PIX 防火墙的内部 IP 地址应该是 10.1.1.1。

·外部网络是 1.1.1.0，拥有一个 255.0.0.0 的子网掩码。这个 PIX 防火墙的外部 IP 地址应该是 1.1.1.1。

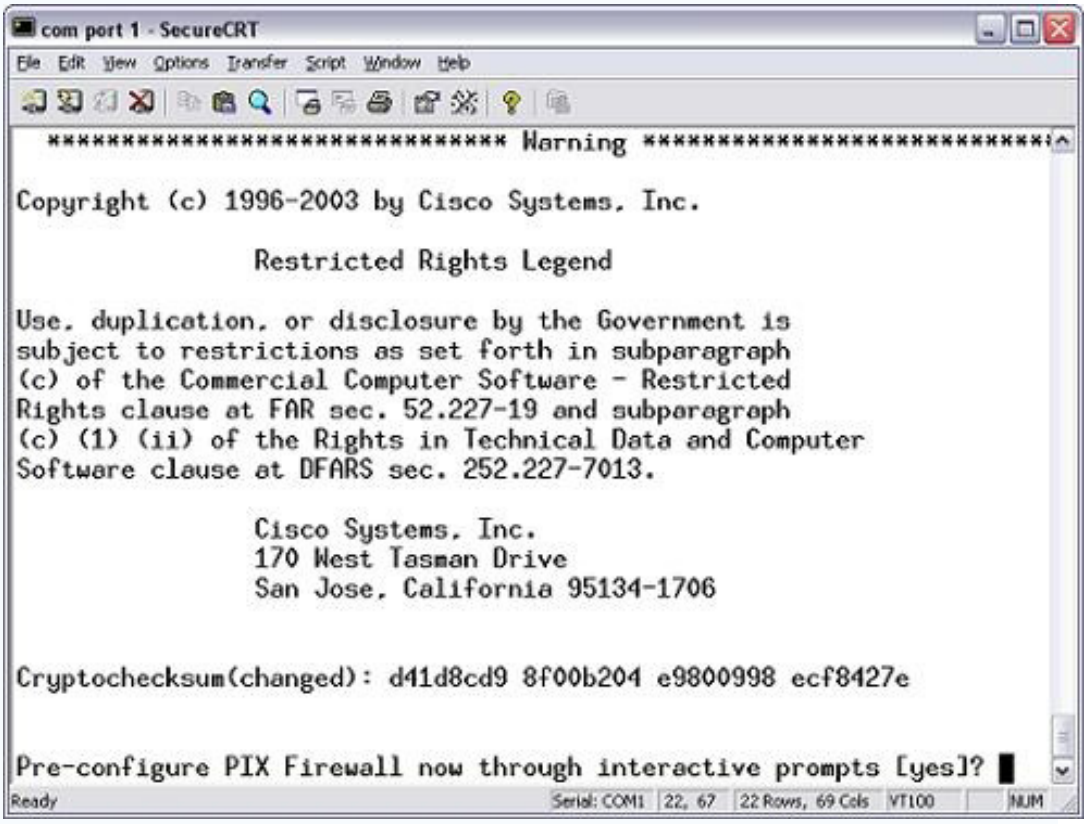
·你要创建一个规则允许所有在 10.0.0.0 网络上的客户做端口地址解析并且连接到外部网络。他们将全部共享全球 IP 地址 1.1.1.2。

·然而，客户只能访问端口 80(网络浏览)。

·用于外部(互联网)网络的默认路由是 1.1.1.254。

设置

当你第一次启动 PIX 防火墙的时候，你应该看到一个这样的屏幕显示：



你将根据提示回答“是”或者“否”来决定是否根据这个互动提示来设置 PIX 防火墙。对这个问题回答“否”，因为你要学习如何真正地设置防火墙，而不仅仅是回答一系列问题。

然后，你将看到这样一个提示符:pixfirewall>

在提示符的后面有一个大于号“>”，你处在 PIX 用户模式。使用 en 或者 enable 命令修改权限模式。在口令提示符下按下“enter”键。下面是一个例子:

pixfirewall> en

Password:

pixfirewall#

你现在拥有管理员模式，可以显示内容，但是，你必须进入通用设置模式来设置这个 PIX 防火墙。

现在让我们学习 PIX 防火墙的基本设置:

PIX 防火墙的基本设置

我所说的基本设置包括三样事情:

·设置主机名

·设置口令(登录和启动)

·设置接口的 IP 地址

·启动接口

·设置一个默认的路由

在你做上述任何事情之前，你需要进入通用设置模式。要进入这种模式，你要键入:

pixfirewall# config t

pixfirewall(config)#

要设置主机名，使用主机名命令，像这样:

pixfirewall(config)# hostname PIX1

PIX1(config)#

注意，提示符转变到你设置的名字。

下一步，把登录口令设置为“cisco”(思科)，像这样:

PIX1(config)# password cisco

PIX1(config)#

这是除了管理员之外获得访问 PIX 防火墙权限所需要的口令。

现在，设置启动模式口令，用于获得管理员模式访问。

PIX1(config)# enable password cisco

PIX1(config)#

现在，我们需要设置接口的 IP 地址和启动这些接口。同路由器一样，PIX 没有接口设置模式的概念。要设置内部接口的 IP 地址，使用如下命令:

PIX1(config)# ip address inside 10.1.1.1 255.0.0.0

PIX1(config)#

现在，设置外部接口的 IP 地址:

PIX1(config)# ip address outside 1.1.1.1 255.255.255.0

PIX1(config)#

下一步，启动内部和外部接口。确认每一个接口的以太网电缆线连接到一台交换机。注意，ethernet0 接口是外部接口，它在 PIX 501 防火墙中只是一个 10base-T 接口。ethernet1 接口是内部接口，是一个 100Base-T 接口。下面是启动这些接口的方法:

PIX1(config)# interface ethernet0 10baset

```
PIX1(config)# interface ethernet1 100full
PIX1(config)#
```

注意，你可以使用一个显示接口的命令，就在通用设置提示符命令行使用这个命令。

最后，让我们设置一个默认的路由，这样，发送到 PIX 防火墙的所有的通讯都会流向下一个上行路由器(我们被分配的 IP 地址是 1.1.1.254)。你可以这样做:

```
PIX1(config)# route outside 0 0 1.1.1.254
PIX1(config)#
```

当然，PIX 防火墙也支持动态路由协议(如 RIP 和 OSPF 协议)。

现在，我们接着介绍一些更高级的设置。

网络地址解析

由于我们有 IP 地址连接，我们需要使用网络地址解析让内部用户连接到外部网络。我们将使用一种称作“PAT”或者“NAT Overload”的网络地址解析。这样，所有内部设备都可以共享一个公共的 IP 地址(PIX 防火墙的外部 IP 地址)。要做到这一点，请输入这些命令:

```
PIX1(config)# nat (inside) 1 10.0.0.0 255.0.0.0
PIX1(config)# global (outside) 1 1.1.1.2
Global 1.1.1.2 will be Port Address Translated
PIX1(config)#
```

使用这些命令之后，全部内部客户机都可以连接到公共网络的设备和共享 IP 地址 1.1.1.2。然而，客户机到目前为止还没有任何规则允许他们这样做。

防火墙规则

这些在内部网络的客户机有一个网络地址解析。但是，这并不意味着允许他们访问。他们现在需要一个允许他们访问外部网络(互连网)的规则。这个规则还将允许返回的通信。

要制定一个允许这些客户机访问端口 80 的规则，你可以输入如下命令:

```
PIX1(config)# access-list outbound permit tcp
10.0.0.0 255.0.0.0 any eq 80
PIX1(config)# access-group outbound in interface
inside
PIX1(config)#
```

注意:与路由器访问列表不同，PIX 访问列表使用一种正常的子网掩码，而不是一种通配符的子网掩码。

使用这个访问列表，你就限制了内部主机访问仅在外部网络的 Web 服务器(路由器)。

显示和存储设置结果

现在你已经完成了 PIX 防火墙的设置。你可以使用显示命令显示你的设置。

确认你使用写入内存或者“wr m”命令存储你的设置。如果你没有使用这个命令，当关闭 PIX 防火墙电源的时候，你的设置就会丢失。