Cisco PIX 防火墙的安装流程

1. 将 PIX 安放至机架，经检测电源系统后接上电源，并加电主机。
2. 将 CONSOLE 口连接到 PC 的串口上，运行 HyperTerminal 程序从 CONSOLE 口进入 PIX 系统；此时系统提示 pixfirewall>。
3. 输入命令：enable,进入特权模式，此时系统提示为 pixfirewall#。
4. 输入命令： configure terminal,对系统进行初始化设置。
5. 配置以太口参数：
   interface ethernet0 auto （auto 选项表明系统自适应网卡类型 ）
   interface ethernet1 auto
6. 配置内外网卡的 IP 地址：
   ip address inside ip_address netmask
   ip address outside ip_address netmask
7. 指定外部地址范围：
   global 1 ip_address-ip_address
8. 指定要进行要转换的内部地址：
   nat 1 ip_address netmask
9. 设置指向内部网和外部网的缺省路由
   route inside 0 0 inside_default_router_ip_address
   route outside 0 0 outside_default_router_ip_address
10. 配置静态 IP 地址对映：
    static outside ip_address inside ip_address
11. 设置某些控制选项：
    conduit global_ip port[-port] protocol foreign_ip [netmask]
    global_ip 指的是要控制的地址
    port 指的是所作用的端口，其中 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 global_ip 的外部 ip，其中表示所有的 ip。
12. 设置 telnet 选项：
    telnet local_ip [netmask]
    local_ip 表示被答应通过 telnet 访问到 pix 的 ip 地址（假如不设此项， PIX 的配置只能由 consle 方式进行）。
13. 将配置保存：
    wr mem
14. 几个常用的网络测试命令：
    #ping
    #show interface 查看端口状态
    #show static 查看静态地址映射

Cisco PIX 防火墙配置命令大全

一、PIX 防火墙的熟悉

PIX 是 Cisco 的硬件防火墙，硬件防火墙有工作速度快，使用方便等特点。

PIX 有很多型号，并发连接数是 PIX 防火墙的重要参数。PIX25 是典型的设备。

PIX 防火墙常见接口有：console、Failover、Ethernet、USB。

网络区域：

内部网络：inside

外部网络：outside

中间区域：称 DMZ(停火区)。放置对外开放的服务器。

二、防火墙的配置规则

没有连接的状态(没有握手或握手不成功或非法的数据包)，任何数据包无法穿过防火墙。(内部发起的连接可以回包。通过 ACL 开放的服务器答应外部发起连接)

inside 可以访问任何 outside 和 dmz 区域。

dmz 可以访问 outside 区域。

inside 访问 dmz 需要配合 static(静态地址转换)。

outside 访问 dmz 需要配合 acl(访问控制列表)。

三、PIX 防火墙的配置模式

PIX 防火墙的配置模式与路由器类似，有 4 种治理模式：

PIXfirewall>：用户模式

PIXfirewall#：特权模式

PIXfirewall(config)#：配置模式

monitor>：ROM 监视模式，开机按住[Esc]键或发送一个“Break”字符，进入监视模式。

四、PIX 基本配置命令

常用命令有：nameif、interface、ipaddress、nat、global、route、static 等。

1、nameif

设置接口名称，并指定安全级别，安全级别取值范围为 1～100，数字越大安全级别越高。

例如要求设置：

ethernet0 命名为外部接口 outside，安全级别是 0。

ethernet1 命名为内部接口 inside，安全级别是 100。

ethernet2 命名为中间接口 dmz,安装级别为 50。

使用命令：

PIX525(config)#nameif ethernet0 outside security 0

PIX525(config)#nameif ethernet1 inside security 100

PIX525(config)#nameif ethernet2 dmz security 50

2、interface

配置以太口工作状态，常见状态有：auto、100full、shutdown。

auto：设置网卡工作在自适应状态。

100full：设置网卡工作在 100Mbit/s，全双工状态。

shutdown：设置网卡接口关闭，否则为激活。

命令：

PIX525(config)#interface ethernet0 auto

PIX525(config)#interface ethernet1 100full

PIX525(config)#interface ethernet1 100fullshutdown

3、ipaddress

配置网络接口的 IP 地址，例如：

PIX525(config)#ip address outside 133.0.0.1 255.255.255.252

PIX525(config)#ip address inside 192.168.0.1 255.255.255.0

内网 inside 接口使用私有地址 192.168.0.1，外网 outside 接口使用公网地址 133.0.0.1。

4、global

指定公网地址范围：定义地址池。

Global 命令的配置语法：

global(if_name) nat_idip_address-ip_address[netmarkglobal_mask]

其中：

(if_name)：表示外网接口名称，一般为 outside。

nat_id：建立的地址池标识(nat 要引用)。

ip_address-ip_address：表示一段 ip 地址范围。

[netmarkglobal_mask]：表示全局 ip 地址的网络掩码。

例如：

PIX525(config)#global(outside) 1 133.0.0.1-133.0.0.15

地址池 1 对应的 IP 是：133.0.0.1-133.0.0.15

PIX525(config)#global(outside) 1 133.0.0.1

地址池 1 只有一个 IP 地址 133.0.0.1。

PIX525(config)#noglobal(outside) 1 133.0.0.1

表示删除这个全局表项。

5、nat

地址转换命令，将内网的私有 ip 转换为外网公网 ip。

nat 命令配置语法：nat(if_name) nat_idlocal_ip[netmark]

其中：

(if_name)：表示接口名称，一般为 inside.

nat_id：表示地址池，由 global 命令定义。

local_ip：表示内网的 ip 地址。对于 0.0.0.0 表示内网所有主机。

[netmark]：表示内网 ip 地址的子网掩码。

在实际配置中 nat 命令总是与 global 命令配合使用。

一个指定外部网络，一个指定内部网络，通过 net_id 联系在一起。

例如：

PIX525(config)#nat(inside) 1 0 0

表示内网的所有主机(00)都可以访问由 global 指定的外网。

PIX525(config)#nat(inside) 1 172.16.5.0 255.255.0.0

表示只有 172.16.5.0/16 网段的主机可以访问 global 指定的外网。

6、route

route 命令定义静态路由。

语法：

route(if_name) 0 0 gateway_ip[metric]

其中：

(if_name)：表示接口名称。

00：表示所有主机

Gateway_ip：表示网关路由器的 ip 地址或下一跳。

[metric]：路由花费。缺省值是 1。

例如：

PIX525(config)#routeoutside 0 0 133.0.0.11

设置缺省路由从 outside 口送出，下一跳是 133.0.0.1。

00 代表 0.0.0.0 0.0.0.0，表示任意网络。

PIX525(config)#routeinside 10.1.0.0 255.255.0.0 10.8.0.11

设置到 10.1.0.0 网络下一跳是 10.8.0.1。最后的“1”是花费。

7、static

配置静态 IP 地址翻译，使内部地址与外部地址一一对应。

语法：

static(internal_if_name,external_if_name) outside_ip_addr inside_ip_address

其中：

internal_if_name 表示内部网络接口，安全级别较高，如 inside。

external_if_name 表示外部网络接口，安全级别较低，如 outside。

outside_ip_address 表示外部网络的公有 ip 地址。

inside_ip_address 表示内部网络的本地 ip 地址。

(括号内序顺是先内后外，外边的顺序是先外后内)

例如：

PIX525(config)#static(inside，outside)133.0.0.1192.168.0.8

表示内部 ip 地址 192.168.0.8，访问外部时被翻译成 133.0.0.1 全局地址。

PIX525(config)#static(dmz，outside)133.0.0.1172.16.0.2

中间区域 ip 地址 172.16.0.2，访问外部时被翻译成 133.0.0.1 全局地址。

8、conduit

管道 conduit 命令用来设置答应数据从低安全级别的接口流向具有较高安全级别的接口。

例如答应从 outside 到 DMZ 或 inside 方向的会话(作用同访问控制列表)。

语法：

conduit permit|deny protocol global_ipport[-port]foreign_ip[netmask]

其中：

global_ip 是一台主机时前面加 host 参数，所有主机时用 any 表示。

foreign_ip 表示外部 ip。

[netmask]表示可以是一台主机或一个网络。

例如：

PIX525(config)#static(inside，outside)133.0.0.1192.168.0.3

PIX525(config)#conduit permit tcp host 133.0.0.1 eq www any

这个例子说明 static 和 conduit 的关系。192.168.0.3 是内网一台 web 服务器，

现在希望外网的用户能够通过 PIX 防火墙访问 web 服务。

所以先做 static 静态映射：192.168.0.3－>133.0.0.1

然后利用 conduit 命令答应任何外部主机对全局地址 133.0.0.1 进行 http 访问。

9、访问控制列表 ACL

访问控制列表的命令与 couduit 命令类似，

例：

PIX525(config)#Access-list 100 permit ip anyhost 133.0.0.1 eq www

PIX525(config)#access-list 100 deny ip any any

PIX525(config)#access-group 100 ininterface outside

10、侦听命令 fixup

作用是启用或禁止一个服务或协议，

通过指定端口设置 PIX 防火墙要侦听 listen 服务的端口。

例：

PIX525(config)#fixup protocol ftp 21

启用 ftp 协议，并指定 ftp 的端口号为 21

PIX525(config)#fixup protocol http 8080

PIX525(config)#nofixup protocol http 80

启用 http 协议 8080 端口，禁止 80 端口。

11、telnet

当从外部接口要 telnet 到 PIX 防火墙时，telnet 数据流需要用 vpn 隧道 ipsec 提供保护或在 PIX 上配置 SSH，然后用 SSHclient 从外部到 PIX 防火墙。

例：

telnetlocal_ip[netmask]

local_ip 表示被授权可以通过 telnet 访问到 PIX 的 ip 地址。

假如不设此项，PIX 的配置方式只能用 console 口接超级终端进行。

12、显示命令：

show interface；查看端口状态。

show static；查看静态地址映射。

show ip；查看接口 ip 地址。

show config；查看配置信息。

show run；显示当前配置信息。

write terminal；将当前配置信息写到终端。

show cpu usage；显示 CPU 利用率，排查故障时常用。

show traffic；查看流量。

show blocks；显示拦截的数据包。

show mem；显示内存

13、DHCP 服务

PIX 具有 DHCP 服务功能。

例：

PIX525(config)#ip address dhcp

PIX525(config)#dhcp daddress 192.168.1.100-192.168.1.200 inside

PIX525(config)#dhcp dns 202.96.128.68 202.96.144.47

PIX525(config)#dhcp domain abc.com.cn

五、PIX 防火墙举例

设：

ethernet0 命名为外部接口 outside，安全级别是 0。

ethernet1 被命名为内部接口 inside，安全级别 100。

ethernet2 被命名为中间接口 dmz，安全级别 50。

PIX525#conft

PIX525(config)#nameif ethernet0 outside security0

PIX525(config)#nameif ethernet1 inside security100

PIX525(config)#nameif ethernet2 dmz security50

PIX525(config)#interface ethernet0 auto

PIX525(config)#interface ethernet1 100 full

PIX525(config)#interface ethernet2 100 full

PIX525(config)#ip address outside 133.0.0.12 255.255.255.252;设置接口 IP
PIX525(config)#ip address inside 10.66.1.200 255.255.0.0;设置接口 IP
PIX525(config)#ip address dmz 10.65.1.200 255.255.0.0;设置接口 IP
PIX525(config)#global(outside) 1 133.1.0.1-133.1.0.14;定义的地址池
PIX525(config)#nat(inside) 1 0 0;00 表示所有
PIX525(config)#route outside 0 0 133.0.0.2;设置默认路由
PIX525(config)#static(dmz，outside)133.1.0.1 10.65.1.101;静态 NAT
PIX525(config)#static(dmz，outside)133.1.0.2 10.65.1.102;静态 NAT
PIX525(config)#static(inside，dmz)10.66.1.200 10.66.1.200;静态 NAT
PIX525(config)#access-list 101 permit ip anyhost 133.1.0.1 eq www;设置 ACL
PIX525(config)#access-list 101 permit ip anyhost 133.1.0.2 eq ftp;设置 ACL
PIX525(config)#access-list 101 deny ip any any;设置 ACL
PIX525(config)#access-group 101 ininterface outside;将 ACL 应用在 outside 端口
当内部主机访问外部主机时，通过 nat 转换成公网 IP，访问 internet。
当内部主机访问中间区域 dmz 时，将自己映射成自己访问服务器，否则内部主机将会映射成地址池的 IP，到外部去找。
当外部主机访问中间区域 dmz 时，对 133.0.0.1 映射成 10.65.1.101，static 是双向的。
PIX 的所有端口默认是关闭的，进入 PIX 要经过 acl 入口过滤。
静态路由指示内部的主机和 dmz 的数据包从 outside 口出去。

Cisco PIX 的基本配置

Cisco PIX 520 是一款性能良好的网络安全产品，假如再加上 Check Point 的软件防火墙组成两道防护，可以得到更加完善的安全防范。

主要用于局域网的外连设备（如路由器、拨号访问服务器等）与内部网络之间，实现内部网络的安全防范，避免来自外部的恶意攻击。

Cisco PIX 520 的默认配置答应从内到外的所有信息请求，拒绝一切外来的主动访问，只答应内部信息的反馈信息进入。当然也可以通过某些设置，例如：访问表等，答应外部的访问。 因为，远程用户的访问需要从外到内的访问。另外，可以通过 NAT 地址转换，实现公有地址和私有地址的转换。

简单地讲，PIX 520 的主要功能有两点：1.实现网络安全，2.实现地址转换

下面简单列出 PIX 520 的基本配置

1.Configure without NAT

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
interface ethernet0 auto
interface ethernet1 auto
ip address outside 202.109.77.1 255.255.255.0 (假设对外端口地址)
ip address inside 10.1.0.9 255.255.255.0(假设内部网络为:10.1.0.0)
hostname bluegarden
arp timeout 14400
no failover
names
pager lines 24
logging buffered debugging
nat (inside) 0 0 0
rip inside default
no rip inside passive
no rip outside default
rip outside passive
route outside 0.0.0.0 0.0.0.0 202.109.77.2 1(外连设备的内部端口地址)
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server community public
mtu outside 1500
mtu inside 1500
```

2.Configure with NAT

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
interface ethernet0 auto
interface ethernet1 auto
ip address outside 202.109.77.1 255.255.255.0 (假设对外端口地址)
ip address inside 10.1.0.9 255.255.255.0(假设内部网络为:10.1.0.0)
hostname bluegarden
arp timeout 14400
no failover
names
pager lines 24
logging buffered debugging
nat (inside) 1 0 0
global (outside) 1 202.109.77.10-202.109.77.20
global (outside) 1 202.109.22.21
no rip inside default
no rip inside passive
no rip outside default
no rip outside passive
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 202.109.77.2 1(外连设备的内部端口地址)
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server community public
mtu outside 1500
mtu inside 1500
```

Cisco 公司对 BT 封锁的方法

用户疯狂 BT(p2p 软件)对网络的使用造成了极大危害，目前常用的办法是:

方法 1、采用 Cisco 公司的 nbar 来限制;

配置步骤如下:

----------定义 Class-map----------;

!

class-map match-all bittorrent

match protocol bittorrent

class-map match-all edonkey

match protocol edonkey

!

注重:假如 match protocol 命令里没有 bittorrent、edonkey 选项，那么说明你的 IOS 版本还没有包括此协议，此时你需要到 Cisco 网站上下载 bittorrent.pdlm、edonkey.pdlm 文件，上传到路由器上，然后定义这种协议:

ip nbar pdlm bittorrent.pdlm

ip nbar pdlm edonkey.pdlm)

----------定义 policy-map----------;

!

policy-map limit-bt

class bittorrent

drop

class edonkey

drop

!

----------应用到接口上----------;

!

interface f0/0

service-policy input limit-bt

service-policy output limit-bt

!

说明:这种方法使用后对一些 p2p 软件确实起作用，但目前 Cisco 只定义了少数几个协议(bittorrent、edonkey、kazaa2、gnutella、napster、winmx、fasttrack 等)，不能覆盖所有的此类软件，这有待于 Cisco 的继续努力;

方法 2、采用 ACL 方法;

我们可以采用以下方式来配置 ACL，一种是开放所有端口，只限制 bt 的端口，配置如下；！

Access-list 101 deny tcp any any range 6881 6890 access-list 101 deny tcp any range 6881

6890 any access-list 101 permit ip any any！

说明：这种方法有其局限性，因为现在有的 p2p 软件，端口可以改变，封锁后会自动改端口，甚至可以该到 80 端口，假如连这个也封，那网络使用就无法正常工作了；

另外一种方式是只开放有用的端口，封闭其他所有端口；！

access-list 101 permit tcp any any eq 80 access-list 101 permit tcp any any eq 25 access-list 101 permit tcp any any eq 110 access-list 101 permit tcp any any eq 53 access-list 101 deny ip any any！

说明：此方法是对网络进行严格的控制，对简单的小型网络还可行，而假如是大型网络，数据流量又很复杂那么治理的难度将非常大；

还有一种方式是对端口是 3000 以上的流量进行限速；因为多数蠕虫病毒和 p2p 的端口都是大于 3000 的，当然也有正常的应用是采用 3000 以上的端口，假如我们将 3000 以上的端口封闭，这样正常的应用也无法开展，所以折中的方法是对端口 3000 以上的数据流进行限速，例如：

----------定义 Class-map----------；

！

class-map match-all xs match access-group 101！

----------定义 policy-map----------；

policy-map xs class xs police cir 1000000 bc 1000 be 1000 conform-action transmit exceed-action drop violate-action drop！

----------定义 ACL----------；！

access-list 101 permit tcp any any gt 3000 access-list 101 permit udp any any gt 3000！

----------应用到接口上----------；

interface f0/0 service-policy input xs！

方法 3、采用 NAT 的单用户连接数限制；

在 Cisco IOS 12.3（4）T 后的 IOS 软件上支持 NAT 的单用户限制，即可以对做地址转换的单个 IP 限制其 NAT 的表项数，因为 p2p 类软件如 bt 的一大特点就是同时会有很多的连接数，从而占用了大量的 NAT 表项，因此应用该方法可有效限制 bt 的使用，比如我们为 IP 10.1.1.1 设置最大的 NAT 表项数为 200；正常的网络访问肯定够用了，但假如使用 bt，那么很快此 IP 的 NAT 表项数达到 200，一旦达到峰值，该 IP 的其他访问就无法再进行 NAT 转换，必须等待到 NAT 表项失效后，才能再次使用，这样有效的保护了网络的带宽，同时也达到了警示的作用。

例如限制 IP 地址为 10.1.1.1 的主机 NAT 的条目为 200 条，配置如下：ip nat translation max-entries host 10.1.1.1 200 假如想限制所有主机，使每台主机的 NAT 条目为 200，可进行如下配置：ip nat translation max-entries all-host 200

以上我们总结了目前可用的限制 bt（p2p 软件）的一些方法，具体采用哪种方法只能您根据自己网络的状况来定，当然也可以将几种方法结合起来使用。