思科 ASA 防火墙配置

要想配置思科的防火墙得先了解这些命令：
常用命令有：nameif、interface、ip address、nat、global、route、static 等。
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_id ip_address-ip_address [netmark global_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。
[netmark global_mask]：表示全局 ip 地址的网络掩码。
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_id local_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。
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。
0 0 ：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。
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：
asa(config)#static (inside，outside) 133.0.0.1 192.168.0.8
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

****

asa#conf t

asa(config)# hostname asa //设置主机名

asa(config)#enable password cisco //设置密码

配置外网的接口，名字是 outside，安全级别 0，输入 ISP 给您提供的地址就行了。

asa(config)#interface GigabitEthernet0/0

asa(config)#nameif outside //名字是 outside

asa(config)#securit-level 0 //安全级别 0

asa(config)#ip address *.*.*.* 255.255.255.0 //配置公网 IP 地址

asa(config)#duplex full

asa(config)#

asa(config)#no shutdown

配置内网的接口，名字是 inside，安全级别 100

asa(config)#interface GigabitEthernet0/1

asa(config)#nameif inside

asa(config)#securit-level 100

asa(config)#duplex full

asa(config)#speed 100

asa(config)#no shutdown

配置 DMZ 的接口,名字是 dmz，安全级别 50

asa(config)#interface GigabitEthernet0/2

asa(config)#nameif dmz

asa(config)#securit-level 50

asa(config)#duplex full

asa(config)#

asa(config)#no shutdown

网络部分设置

asa(config)#nat(inside) 1 192.168.1.1 255.255.255.0

asa(config)#global(outside) 1 222.240.254.193 255.255.255.248

asa(config)#nat (inside) 0 192.168.1.1 255.255.255.255 //表示 192.168.1.1 这个地址不需要转换。直接转发出去。

asa(config)#global (outside) 1 133.1.0.1-133.1.0.14 //定义的地址池

asa(config)#nat (inside) 1 0 0 //0 0 表示转换网段中的所有地址。定义内部网络地址将要翻译成的全局地址或地址范围

配置静态路由

asa(config)#route outside 0 0 133.0.0.2 //设置默认路由 133.0.0.2 为下一跳

如果内部网段不是直接接在防火墙内口，则需要配置到内部的路由。

asa(config)#Route inside 192.168.10.0 255.255.255.0 192.168.1.1 1

地址转换

asa(config)#static (dmz，outside) 133.1.0.1 10.65.1.101 ;静态 NAT

asa(config)#static (dmz，outside) 133.1.0.2 10.65.1.102 ;静态 NAT

asa(config)#static (inside，dmz) 10.66.1.200 10.66.1.200 ;静态 NAT

如果内部有服务器需要映射到公网地址(外网访问内网)则需要 static

asa(config)#static (inside, outside) 222.240.254.194 192.168.1.240

asa(config)#static (inside, outside) 222.240.254.194 192.168.1.240 10000 10 //后面的 10000 为限制连接数，10 为限制的半开连接数

ACL 实现策略访问

asa(config)#access-list 101 permit ip any host 133.1.0.1 eq www;设置 ACL

asa(config)#access-list 101 permit ip any host 133.1.0.2 eq ftp;设置 ACL

asa(config)#access-list 101 deny ip any any ;设置 ACL

asa(config)#access-group 101 in interface 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。

思科 ASA 和 PIX 防火墙配置手册

 一、 配置基础

1.1 用户接口

思科防火墙支持下列用户配置方式：

Console，Telnet，SSH（1.x 或者 2.0，2.0 为 7.x 新特性，PDM 的 http 方式（7.x 以后称为 ASDM）和 VMS 的 Firewall Management Center。

支持进入 Rom Monitor 模式，权限分为用户模式和特权模式，支持 Help，History 和命令输出的搜索和过滤。

注：Catalyst6500 的 FWSM 没有物理接口接入，通过下面 CLI 命令进入：

Switch# session slot slot[/i] processor 1 （FWSM 所在 slot 号）

用户模式：

Firewall> 为用户模式，输入 enable 进入特权模式 Firewall#。特权模式下可以进入配置模式，在 6.x 所有的配置都在一个全局模式下进行，7.x 以后改成和 IOS 类似的全局配置模式和相应的子模式。通过 exit，ctrl-z 退回上级模式。

配置特性：

在原有命令前加 no 可以取消该命令。Show running-config 或者 write terminal 显示当前配置，7.x 后可以对 show run 的命令输出进行搜索和过滤。Show running-config all 显示所有配置，包含缺省配置。Tab 可以用于命令补全，ctrl-l 可以用于重新显示输入的命令（适用于还没有输入完命令被系统输出打乱的情况），help 和 history 相同于 IOS 命令集。

Show 命令支持 begin，include，exclude，grep 加正则表达式的方式对输出进行过滤和搜索。

Terminal width 命令用于修改终端屏幕显示宽度，缺省为 80 个字符，pager 命令用于修改终端显示屏幕显示行数，缺省为 24 行，pager lines 0 命令什么效果可以自己试试。

1.2 防火墙许可介绍

防火墙具有下列几种许可形式，通过使用 show version 命令可以看设备所支持的特性：

Unrestricted (UR) 所有的限制仅限于设备自身的性能，也支持 Failover

Restricted (R) 防火墙的内存和允许使用的最多端口数有限制，不支持 Failover

Failover (FO) 不能单独使用的防火墙，只能用于 Failover

Failover-Active/Active (FO-AA) 只能和 UR 类型的防火墙一起使用，支持 active/active failover

注：FWSM 内置 UR 许可。

activation-key 命令用于升级设备的许可，该许可和设备的 serial number 有关（show version 输出可以看到），6.x 为 16 字节，7.x 为 20 字节。

1.3 初始配置

跟路由器一样可以使用 setup 进行对话式的基本配置。

 二、 配置连接性

2.1 配置接口

接口基础：

防火墙的接口都必须配置接口名称，接口 IP 地址和掩码（7.x 开始支持 IPv6）和安全等级。接口可以是物理接口也可以是逻辑接口（vlan），从 6.3✡贾 C?lt;/SPAN>trunk，但只支持 802.1Q 封装，不支持 DTP 协商。

接口基本配置：

注：对于 FWSM 所有的接口都为逻辑接口，名字也是 vlan 后面加上 vlanid。例如 FWSM 位于 6500 的第三槽，配置三个接口，分别属于 vlan 100,200,300.

Switch(config)# firewall vlan-group 1 100,200,300[/i]

Switch(config)# firewall module 3[/i] vlan-group 1[/i]

Switch(config)# exit

Switch# session slot 3[/i] processor 1

经过此配置后形成三个端口 vlan100.vlan200,vlan300

PIX 6.x

Firewall(config)# interface hardware-id[/i] [hardware-speed] [shutdown] （Hardware-id 可以用 show version 命令看到）

PIX 7.x

Firewall(config)# interface hardware-id[/i]

Firewall(config-if)# speed {auto | 10 | 100 | nonegotiate}

Firewall(config-if)# duplex {auto | full | half}

Firewall(config-if)# [no] shutdown

命名接口

FWSM 2.x

Firewall(config)# nameif vlan-id if_name[/i] securitylevel[/i]

PIX 6.x

Firewall(config)# nameif {hardware-id | vlan-id}[/i] if_name securitylevel [/i]

PIX 7.x

Firewall(config)# interface hardware_id[.subinterface][/i]

Firewall(config-if)# nameif if_name[/i]

Firewall(config-if)# security-level level[/i]

注：Pix 7.x 和 FWSM 2.x 开始支持不同接口有相同的 security level，前提是全局配置模式下使用 same-security-traffic permit inter-interface 命令。

配置 IP 地址

静态地址：Firewall(config)# ip address if_name ip_address [netmask][/i]

动态地址：Firewall(config)# ip address outside dhcp [setroute] [retry retry_cnt[/i]]

注：setroute 参数可以同时获得来自 DHCP 服务器的缺省路由，再次输入此命令可以 renew 地址。

PPPOE：Firewall(config)# vpdn username JohnDoe[/i] password JDsecret[/i]

Firewall(config)# vpdn group ISP1[/i] localname JohnDoe[/i]
Firewall(config)# vpdn group ISP1[/i] ppp authentication chap[/i]
Firewall(config)# vpdn group ISP1[/i] request dialout pppoe
Firewall(config)# ip address outside pppoe setroute
验证接口
Firewall# show ip
IPv6 地址配置（7.x 新特性）
暂略
ARP 配置
配置一个静态的 ARP 条目：Firewall(config)# arp if_name ip_address mac_address[/i] [alias]
配置 timeout 时间：Firewall(config)# arp timeout seconds [/i]缺省为 4 小时
注：一般情况下使用 clear arp 会清除所有的 ARP 缓存，不能针对单个的条目，但是可以通过以下变通方法：配置一个静态的条目，映射有问题的 ip 为一个假的 mac 地址，然后 no 掉该命令就会重新建立一个 arp 条目。
MTU 和分段
配置 MTU：Firewall(config)# mtu if_name bytes 使用 show mtu (6.3) 或者 show running-config mtu (7.x)来验证
分段（fragment）的几个命令：限制等待重组的分段数 Firewall(config)# fragment size database-limit [if_name][/i]
限制每个包的分段数 Firewall(config)# fragment chain chain-limit [if_name][/i][/i]
限制一个数据包分段到达的时间 Firewall(config)# fragment timeout seconds [if_name][/i]
配置接口的优先队列（7.x 新特性）
暂略
2.2 配置路由
启用 PRF 防止地址欺骗 Firewall(config)# ip verify reverse-path interface if_name[/i][/i]
配置静态路由 Firewall(config)# route if_name ip_address netmask gateway_ip [metric][/i]
配置 RIP
被动听 RIP 更新(v1，v2)Firewall(config)# rip if_name[/i] passive [version 1] （Firewall(config)# rip if_name[/i] passive version 2 [authentication [text | md5 key (key_id)[/i]]]）
宣告该接口为缺省路由 Firewall(config)# rip if_name[/i] default version [1 | 2 [authentication [text | md5 key key_id]]
配置 OSPF
定义 OSPF 进程 Firewall(config)# router ospf pid
指定相应网络到 OSPF 区域 Firewall(config-router)# network ip_address netmask area area_id
可选：定义 Router ID Firewall(config-router)# router-id ip_address
记录 OSPF 邻居状态更新 Firewall(config-router)# log-adj-changes [detail]
启用 OSPF 更新认证 Firewall(config-router)# area area_id authentication [message-digest]宣告缺省路由 Firewall(config-router)# default-information originate [always] [metric value] [metric-type {1 | 2}] [route-map name]调节 OSPF 参数 Firewall(config-router)# timers {spf spf_delay spf_holdtime |lsa-group-pacing seconds}
2.3 DHCP
配置成为 DHCP Server：
配置地址池 Firewall(config)# dhcpd address ip1[-ip2] if_name[/i] [/i]（最多 256 个客户端）
配置 DHCP 参数 Firewall(config)# dhcpd dns dns1 [dns2] [/i]Firewall(config)# dhcpd wins wins1

[wins2][/i] Firewall(config)# dhcpd domain domain_name[/i] Firewall(config)# dhcpd lease lease_length[/i] Firewall(config)# dhcpd ping_timeout timeout[/i]

启用 DHCP 服务 Firewall(config)# dhcpd enable if_name[/i]

验证：show dhcdp, show dhcpd bindings, show dhcpd statistics

配置 DHCP 中继：

定义真实 DHCP Server Firewall(config)# dhcprelay server dhcp_server_ip server_ifc[/i](最多 4 个)

中继参数 Firewall(config)# dhcprelay timeout seconds [/i]Firewall(config)# dhcprelay setroute client_ifc[/i]

启用中继 Firewall(config)# dhcprelay enable client_ifc[/i]

验证 show dhcprelay statistics

2.4 组播的支持

暂略

 一、防火墙的管理

3.1 使用 Security Context 建立虚拟防火墙（7.x 特性）

特性介绍：从 PIX7.0 和 FWSM 2.2(1)开始，可以把物理的一个防火墙配置出多个虚拟的防火墙，每个防火墙称为 context，这样一个防火墙就支持两种工作模式：single-context 和 multiple-context，处于后者工作模式的防火墙被分为三个功能模块：system execution space(虽然没有 context 的功能，但是是所有的基础)，administrative context(被用来管理物理的防火墙) 和 user contexts(虚拟出来的防火墙，所有配置防火墙的命令都适用)

配置：首先使用 show activation-key 来验证是否有 multiple-context 的许可，然后通过 mode multiple 和 mode single 命令在这两个模式之间进行切换，当然也可以用 show mode 来验证现在工作在什么模式下。在不同 context 下进行切换使用 Firewall# changeto {system | context name[/i]}，由于所有的 context 的定义都必须在 system execution space 下，所以要首先使用 changeto system 转入该模式，Firewall(config)# context name[/i] 接着要把物理接口映射到 context 中 只要这样才能在相应的 context 下显示出物理接口，从而配置其属性 Firewall(config-ctx)# allocate-interface physical-interface[/i] [map-name[/i]] 最后定义 context 的 startup-config 的存放位置 Firewall(config-ctx)# config-url url[/i]

通过 show context 验证

注：当防火墙工作在 multiple-context 模式下，admin context 就自动生成。(show context 来验证)

由于所有的 context 都共享设备的资源，所以要限制各个 context 的资源分配

首先定义 class Firewall(config)# class name[/i] [/i] 然后 Firewall(config-class)# limit-resource all number%[/i] Firewall(config-class)# limit-resource [rate] resource_name number[%][/i] 最后在相应的 context 配置下 Firewall(config-ctx)# member class[/i]

通过以下命令验证 show class， show resource allocation, show resource usage 等

注：缺省 telnet，ssh，IPsec 5 sessions，MAC address 65535 条目

3.2 管理 Flash 文件系统

6.x 文件系统

只有六种文件可以保存到 Flash，没有文件名只有代号，没有目录结构

0 OS 镜像 1 启动文件 2 VPN 和密匙证书 3 PDM 镜像 4 崩溃信息 5 0 的文件大小

show flashfs 显示 flash 文件

7.x 和 FWSM 文件系统

7.x 和 FWSM 更像 IOS 的文件系统，具有层级目录，要被格式化后才可以使用，7.x 使用 flash:/代表 Flash 文件系统，FWSM 分别使用 flash:/ (系统镜像)和 disk:/(配置文件)

由于该系统使用类 Unix 的指令，所以可以使用下列常用命令来对该文件系统操作：

dir pwd cd more delete copy rename mkdir rmdir format erase fsck(检查文件系统完整性)
6.x 在 Flash 里面只能保存一个系统镜像，7.x 则废除了此种限制通过使用 Firewall(config)# boot system flash:filename[/i]来选取不同的系统镜像，show bootvar 进行验证
OS 升级 见附录
3.3 管理配置文件
7.0 以后可以使用多个启动配置文件 Firewall(config)# boot config url[/i]
显示启动配置文件 Firewall# show startup-config Firewall# show configuration (6.x 为 show configure)
保存当前配置文件 write memory, copy running-config startup-config, write net [[server-ip-address]:[filename]][/i] [/i](7.x 也支持 copy 至 tftp)
强制 standby 同步当前配置文件 write standby 删除启动配置文件 write erase
合并启动配置文件为当前配置文件 configure memory 从 Web 导入配置文件 configure http[s]://[user:password@]location[:port]/ http-pathname (7.x 支持 copy 自以上源)
合并配置文件自自动更新服务器
Firewall(config)# auto-update device-id {hardware-serial | hostname |
ipaddress [if_name[/i]] | mac-address [if_name[/i]] | string text[/i]}
Firewall(config)# auto-update server http[s]://[username:password@][/i]
AUSserver-IP-address[:port][/i]/autoupdate/AutoUpdateServlet
[verify-certificate]
3.4 管理管理会话
Firewall(config)# console timeout minutes[/i] 配置 console 登录的超时(缺省 0 不超时)
禁止来自 outside 端口的 telnet，启用 telnet Firewall(config)# telnet ip_address netmask if_name [/i]Firewall(config)# telnet timeout minutes [/i] [/i]配置 telnet 超时
启用 SSH 配置
首先生成 RSA 密匙对 Firewall(config)# domain-name name Firewall(config)# ca generate rsa key [modulus] (7.x 使用 crypto key generate rsa general-keys [modulus modulus]) Firewall(config)# ca save all (7.x 自动保存)
使用 show ca mypubkey rsa 来验证(7.x show crypto key mypubkey rsa) ca zeroize rsa 作废原有密匙对(7.x crypto key zeroize rsa default)
最后允许 ssh 会话 Firewall(config)# ssh ip_address netmask if_name
ssh version 命令可以选择 ssh 的版本，ssh timeout 定义超时时间
PDM/ASDM 配置
由于 PDM 存放位置固定，所以不需要指定镜像的位置，ASDM 使用 Firewall(config)# asdm image device:/path 来指定镜像位置，如果没有可以使用 copy 命令来安装。然后配置访问许可 Firewall# http ip_address subnet_mask if_name 启用 HTTP 进程 Firewall# http server enable 使用 https://ip-address/admin 来访问。
Banner 配置 Firewall(config)# banner {exec | login | motd} text 对 banner 不能修改，只能用 no 来删除，或者 clear banner 来清除所有的 banner（7.0 clear configure banner）
监控管理会话 who 监控 telnet 会话 kill telnet-id 来清除会话，show ssh sessions 监控 ssh 会话，ssh disconnect session-id 清除 ssh 会话，show pdm sessions 监控 pdm 会话，pdm disconnect session-id 清除 pdm 会话
3.5 系统重启和崩溃
通常使用 reload 命令重启系统，从 7.0 以后支持在特定的时间重启系统 Firewall# reload at hh:mm [month day | day month] [max-hold-time {minutes | hhh:mm}] [noconfirm] [quick] [save-config] [reason text]或者经过一定的时间间隔后重启 Firewall# reload in {minutes | hh:mm} [max-hold-time

{minutes | hhh:mm}] [noconfirm] [quick] [save-config] [reason text]
启用崩溃信息生成 Firewall(config)# crashinfo save enable (7.0 no crashinfo save disable) show crashinfo 来看崩溃信息 clear crashinfo 删除信息（FWSM 使用 crashdump）
3.6 SNMP 支持
系统 SNMP 信息 Firewall(config)# snmp-server location string (contact string)
SNMP 访问许可 Firewall(config)# snmp-server host if_name ip_addr [poll | trap]
Firewall(config)# snmp-server community key

四、用户管理

4.1 一般用户管理

注：缺省情况下认证用户仅需要 password，这样的一般用户缺省用户名就是 enalbe_1,在 ssh 情况下缺省用户名就是 pix，然后用 password 来认证。

非特权模式密码配置 Firewall(config)# {password | passwd} password [encrypted] (恢复缺省密码 cisco 用 clear {password | passwd})

特权模式密码配置 Firewall(config)# enable password [pw] [level priv_level] [encrypted]

4.2 本地数据库管理用户

定义用户 Firewall(config)# username username [{nopassword | password password}

[encrypted]] privilege level

启用本地认证 Firewall(config)# aaa authentication {serial | telnet | ssh | http} console LOCAL

注：缺省情况特权模式密码使用 enable password 定义，这样用户通过认证后使用 enable 来进入特权模式，而不管用户初始什么等级的权限，所有用户使用相同的密码。这里也可以使用本地 enable 认证(aaa authentication enable console LOCAL)，用户使用 username password 的密码来进入 enable，用户 enable 密码独立从而增加安全性。

本地授权：Firewall(config)# aaa authorization command LOCAL

配置命令的特权等级：Firewall(config)# privilege {show | clear | configure} level level [mode {enable | configure}] command command

使用 show privilege 来看当前命令的特权等级(7.x 使用 show run all privilege)

4.3 使用 AAA 服务器来管理用户

定义 AAA 服务器组和协议 Firewall(config)# aaa-server server_tag protocol {tacacs+ | radius} (7.x 还增加了 kerberos,ldap,nt,sdi 协议的支持)

加入服务器到组 Firewall(config)# aaa-server server_tag [(if_name)] host server_ip [key] [timeout seconds]

可选命令

定义服务器失败阀值 FWSM Firewall(config)# aaa-server server_tag max-attempts number

PIX 6.x Firewall(config)# aaa-server server_tag max-failed-attempts number

PIX 7.x Firewall(config-aaa-server-group)# max-failed-attempts number

定义统计策略(7.x 特性) Firewall(config-aaa-server-group)# accounting-mode {single | simultaneous}

具体各协议参数配置暂略

4.4 配置 AAA 管理用户

启用鉴权 Firewall(config)# aaa authentication {serial | telnet | ssh | http} console

server_tag [LOCAL]

启用授权 Firewall(config)# aaa authorization command server_tag [LOCAL]

启用统计 Firewall(config)# aaa accounting command [privilege level] server_tag

注：AAA 服务器配置略

4.5 配置 AAA 支持用户 Cut-Through 代理

五 防火墙的访问控制

5.1 防火墙的透明模式

特性介绍：从 PIX 7.0 和 FWSM 2.2 开始防火墙可以支持透明的防火墙模式，接口不需要配置地址信息，工作在二层。只支持两个接口 inside 和 outside，当然可以配置一个管理接口，但是管理接口不能用于处理用户流量，在多 context 模式下不能复用物理端口。由于连接的是同一地址段的网络，所以不支持 NAT，虽然没有 IP 地址但是同样可以配置 ACL 来检查流量。

进入透明模式 Firewall(config)# firewall transparent (show firewall 来验证当前的工作模式，由于路由模式和透明模式工作方式不同，所以互相切换的时候会清除当前配置文件)

配置接口 Firewall(config)# interface hardware-id

Firewall(config-if)# speed {auto | 10 | 100 |nonegotiate}

Firewall(config-if)# duplex {auto | full | half}

Firewall(config-if)# [no] shutdown

Firewall(config-if)# nameif if_name

Firewall(config-if)# security-level level

注：不用配置 IP 地址信息，但是其它的属性还是要配置的，接口的安全等级一般要不一样， same-security-traffic permit inter-interface 命令可以免除此限制。

配置管理地址 Firewall(config)# ip address ip_address subnet_mask

Firewall(config)# route if_name foreign_network foreign_mask gateway [metric]

MAC 地址表的配置 Firewall# show mac-address-table 显示 MAC 地址表

Firewall(config)# mac-address-table aging-time minutes 设置 MAC 地址表过期时间

Firewall(config)# mac-address-table static if_name mac_address 设置静态 MAC 条目

Firewall(config)# mac-learn if_name disable 禁止特定接口地址学习(show mac-learn 验证)

ARP 检查 Firewall(config)# arp if_name ip_address mac_address 静态 ARP 条目

Firewall(config)# arp-inspection if_name enable [flood | no-flood] 端口启用 ARP 检查

为非 IP 协议配置转发策略 Firewall(config)# access-list acl_id ethertype {permit | deny} {any | bpdu | ipx | mpls-unicast | mpls-multicast | ethertype}

Firewall(config)# access-group acl_id {in | out} interface if_name

5.2 防火墙的路由模式和地址翻译

特性介绍：从高安全等级到低安全等级的访问称为 outbound 访问，需要配置地址翻译和 outbound 访问控制，PIX 缺省情况下不用配置 ACL 就允许此类访问，FWSM 则需要配置 ACL 来允许此类型的访问。而从低安全等级到高安全等级的访问称为 inboud 访问，也需要配置地址翻译和 inboud 访问控制，此类型必须配置 ACL.同一安全等级的访问也可以配置地址翻译。

支持下列几种 NAT 类型

Translation Type
Application
Basic Command
Direction in Which Connections Can Be Initiated

Static NAT
Real source addresses (and ports) are translated to mapped addresses (and ports)
static
Inbound or outbound

Policy NAT
Conditionally translates real source addresses (and ports) to mapped addresses
static access-list
Inbound or outbound

Identity NAT
No translation of real source addresses
nat 0
Outbound only

NAT exemption
No translation of real source addresses matched by the access list
nat 0 access-list
Inbound or outbound

Dynamic NAT
Translates real source addresses to a pool of mapped addresses
nat id

global id address-range
Outbound only

PAT
Translates real source addresses to a single mapped address with dynamic port numbers
nat id

global id address
Outbound only

配置

对于连接数的控制 PIX 6.x ... [norandomseq] [max_conns [emb_limit]]

PIX 7.x ... [norandomseq] [[tcp] max_conns [emb_limit]] [udp udp_max_conns]

连接超时控制 Firewall(config)# timeout [conn hh:mm:ss] [udp hh:mm:ss]

静态 NAT

基于地址的静态翻译 Firewall(config)# static (real_ifc,mapped_ifc) {mapped_ip | interface} {real_ip [netmask mask]} [dns] [norandomseq] [max_conns [emb_limit]]

基于端口的静态翻译 Firewall(config)# static (real_ifc,mapped_ifc) {tcp | udp} {mapped_ip | interface} mapped_port {real_ip real_port [netmask mask]} [dns] [norandomseq] [max_conns [emb_limit]]

策略 NAT

定义翻译策略 Firewall(config)# access-list acl_name permit ip real_ip real_mask foreign_ip foreign_mask

静态的 Firewall(config)# static (real_ifc,mapped_ifc) mapped_ip access-list acl_name [dns] [norandomseq] [max_conns [emb_limit]]

NAT 的 Firewall(config)# global (mapped_ifc) nat_id {global_ip [-global_ip] [netmask global_mask]} | interface

Firewall(config)# nat (real_ifc) nat_id access-list acl_name [dns] [outside][norandomseq] [max_conns [emb_limit]]

Identify NAT Firewall(config)# nat (real_ifc) 0 real_ip real_mask [dns] [norandomseq] [max_conns [emb_limit]]

注：nat 0 和 static 相同地址的区别在于：nat 0 只能用于 outbound 访问，static 两种访问都可以，对同一地址不建议同时配置此两类命令。

NAT Exemption

Firewall(config)# access-list acl_name permit ip local_ip local_mask foreign_ip foreign_mask

Firewall(config)# nat (real_ifc) 0 access-list acl_name [dns] [outside] [max_conns [emb_limit] [norandomseq]]

注：此类型 NAT 策略只能根据源和目的地址不能根据协议类型或者端口

动态地址翻译

定义 NAT 的映射地址 Firewall(config)# global (mapped_ifc) nat_id global_ip[-global_ip] [netmask global_mask]

定义 PAT 的映射地址 Firewall(config)# global (mapped_ifc) nat_id {global_ip | interface}

定义翻译策略 Firewall(config)# nat (real_ifc) nat_id real_ip [mask [dns] [outside] [[norandomseq] [max_conns [emb_limit]]]

注：也可以使用 ACL 来做类似的策略 NAT。

5.3 使用 ACL 进行访问控制

特性介绍：防火墙的 ACL 配置跟 IOS 不同，子网掩码部分为正常的子网掩码不需要使用反转的子网掩码。还支持 Object group，包含 IP 地址组，ICMP 类型组，IP 协议或者端口组，并且支持组嵌套。access-list acl_name compiled 配置 Turbo ACL，7.x 自动 turbo。防火墙的 ACL 缺省是扩展模式的，7.x 后也支持标准模式了尽管只用于路由协议的配置上，并且加上了 extend 的参数，虽然配置的时候可以不必强制用这个参数但是当你需要移除该条目的时候要记得把 extend 这个参数加上。

配置

定义 Object Group

网络对象组 Firewall(config)# object-group network group_id

Firewall(config-network)# description text

Firewall(config-network)# network-object ip_addr mask (或者 host ip_addr)

Firewall(config-network)# group-object group_id

ICMP 对象组 Firewall(config)# object-group icmp-type group_id

Firewall(config-icmp-type)# description text

Firewall(config-icmp-type)# icmp-object icmp_type

Firewall(config-icmp-type)# group-object group_id

协议对象组 Firewall(config)# object-group protocol group_id

Firewall(config-protocol)# description text

Firewall(config-protocol)# protocol-object protocol

Firewall(config-protocol)# group-object group_id

服务对象组 Firewall(config)# object-group service group_id {tcp | udp | tcp-udp}

Firewall(config-service)# description text

Firewall(config-service)# port-object range begin_port end_port (或者 eq port)

Firewall(config-service)# group-object group_id

定义时间范围 7.0 特性

Firewall(config)# time-range name

Firewall(config-time-range)# periodic start-day hh:mm to end-day hh:mm

Firewall(config-time-range)# periodic days-of-the-week hh:mm to hh:mm

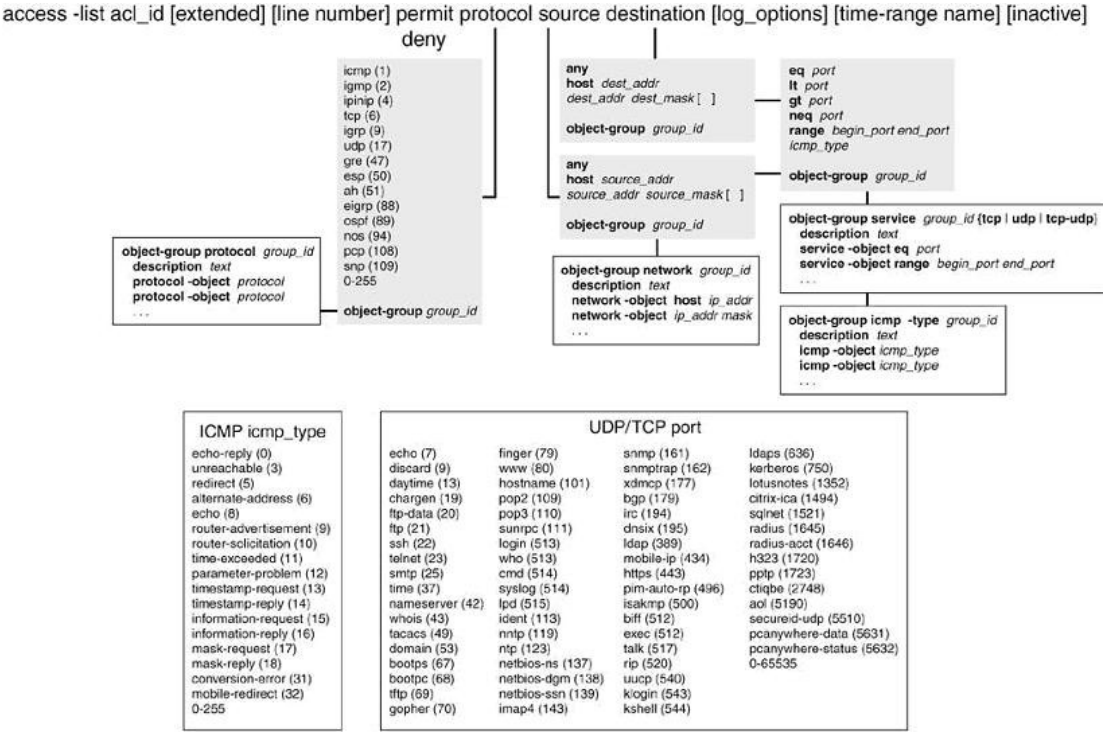
Firewall(config-time-range)# absolute [start hh:mm day month year] [end hh:mm day month year]

配置 ACL Firewall(config)# access-list acl_id [line line-num] [extended] {permit | deny}

{protocol | object-group protocol_obj_group} {source_addr source_mask | object-group network_obj_group} [operator sport | object-group service_obj_group]

{destination_addr destination_mask |object-group network_obj_group}

[operator dport | object-group service_obj_group] [log [[disable | default] | [level]]] [interval secs]] [time-range name] [inactive]



show access-list 来验证， clear access-list acl_id counters 重置 ACL 计数器

在配置 PIX 防火墙之前，先来介绍一下防火墙的物理特性。防火墙通常具有至少 3 个接口，但许多早期的防火墙只具有 2 个接口；当使用具有 3 个接口的防火墙时，就至少产生了 3 个网络，描述如下：

内部区域（内网）：内部区域通常就是指企业内部网络或者是企业内部网络的一部分。它是互连网络的信任区域，即受到了防火墙的保护。

外部区域（外网）：外部区域通常指 Internet 或者非企业内部网络。它是互连网络中不被信任的区域，当外部区域想要访问内部区域的主机和服务，通过防火墙，就可以实现有限制的访问。

停火区（DMZ）：停火区是一个隔离的网络，或几个网络。位于停火区中的主机或服务器被称为堡垒主机。一般在停火区内可以放置 Web 服务器，Mail 服务器等。停火区对于外部用户通常是可以访问的，这种方式让外部用户可以访问企业的公开信息，但却不允许他们访问企业内部网络。

注意：2 个接口的防火墙是没有停火区的。

由于 PIX535 在企业级别不具有普遍性，因此下面主要说明 PIX525 在企业网络中的应用。

PIX 防火墙提供 4 种管理访问模式：

非特权模式。 PIX 防火墙开机自检后，就是处于这种模式。系统显示为 pixfirewall>

特权模式。 输入 enable 进入特权模式，可以改变当前配置。显示为 pixfirewall#

配置模式。 输入 configure terminal 进入此模式，绝大部分的系统配置都在这里进行。显示为 pixfirewall(config)#

监视模式。 PIX 防火墙在开机或重启过程中，按住 Escape 键或发送一个"Break"字符，进入监视模式。这里可以更新*作系统映象和口令恢复。显示为 monitor>

配置 PIX 防火墙有 6 个基本命令：nameif，interface，ip address，nat，global，route.

这些命令在配置 PIX 时是必须的。以下是配置的基本步骤：

1. 配置防火墙接口的名字，并指定安全级别（nameif）。
Pix525(config)#nameif ethernet0 outside security0
Pix525(config)#nameif ethernet1 inside security100
Pix525(config)#nameif dmz security50
提示：在缺省配置中，以太网 0 被命名为外部接口（outside），安全级别是 0；以太网 1 被命名为内部接口（inside），安全级别是 100.安全级别取值范围为 1～99，数字越大安全级别越高。若添加新的接口，语句可以这样写：
Pix525(config)#nameif pix/intf3 security40 （安全级别任取）

2. 配置以太口参数（interface）
Pix525(config)#interface ethernet0 auto （auto 选项表明系统自适应网卡类型 ）
Pix525(config)#interface ethernet1 100full （100full 选项表示 100Mbit/s 以太网全双工通信 ）
Pix525(config)#interface ethernet1 100full shutdown （shutdown 选项表示关闭这个接口，若启用接口去掉 shutdown ）

3. 配置内外网卡的 IP 地址（ip address）
Pix525(config)#ip address outside 61.144.51.42 255.255.255.248
Pix525(config)#ip address inside 192.168.0.1 255.255.255.0
很明显，Pix525 防火墙在外网的 ip 地址是 61.144.51.42，内网 ip 地址是 192.168.0.1

例 1. Pix525(config)#conduit permit tcp host 192.168.0.8 eq www any
这个例子表示允许任何外部主机对全局地址 192.168.0.8 的这台主机进行 http 访问。其中使用 eq 和一个端口来允许或拒绝对这个端口的访问。Eq ftp 就是指允许或拒绝只对 ftp 的访问。

例 2. Pix525(config)#conduit deny tcp any eq ftp host 61.144.51.89
表示不允许外部主机 61.144.51.89 对任何全局地址进行 ftp 访问。

例 3. Pix525(config)#conduit permit icmp any any
表示允许 icmp 消息向内部和外部通过。

例 4. Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.3
Pix525(config)#conduit permit tcp host 61.144.51.62 eq www any
这个例子说明 static 和 conduit 的关系。192.168.0.3 在内网是一台 web 服务器，现在希望外网的用户能够通过 pix 防火墙得到 web 服务。所以先做 static 静态映射：192.168.0.3－>61.144.51.62（全局），然后利用 conduit 命令允许任何外部主机对全局地址 61.144.51.62 进行 http 访问。

C. 配置 fixup 协议

fixup 命令作用是启用，禁止，改变一个服务或协议通过 pix 防火墙，由 fixup 命令指定的端口是 pix 防火墙要侦听的服务。见下面例子：
例 1． Pix525(config)#fixup protocol ftp 21 启用 ftp 协议，并指定 ftp 的端口号为 21
例 2． Pix525(config)#fixup protocol http 80
Pix525(config)#fixup protocol http 1080 为 http 协议指定 80 和 1080 两个端口。
例 3． Pix525(config)#no fixup protocol smtp 80 禁用 smtp 协议。

D. 设置 telnet

telnet 有一个版本的变化。在 pix OS 5.0（pix*作系统的版本号）之前，只能从内部网络上的主机通过 telnet 访问 pix。在 pix OS 5.0 及后续版本中，可以在所有的接口上启用 telnet 到 pix 的访问。当从外部接口要 telnet 到 pix 防火墙时，telnet 数据流需要用 ipsec 提供保护，也就是说用户必须配置 pix 来建立一条到另外一台 pix，路由器或 vpn 客户端的 ipsec 隧道。另外就是在 PIX 上配置 SSH，然后用 SSH client 从外部 telnet 到 PIX 防火墙，PIX 支持 SSH1 和 SSH2，不过 SSH1 是免费软件，SSH2 是商业软件。相比之下 cisco 路由器的 telnet 就做得不怎么样了。
telnet 配置语法：telnet local_ip [netmask] local_ip
表示被授权通过 telnet 访问到 pix 的 ip 地址。如果不设此项，pix 的配置方式只能由 console 进行。

说了这么多，下面给出一个配置实例供大家参考。

Welcome to the PIX firewall

Type help or '?' for a list of available commands.
PIX525> en
Password:
PIX525#sh config :
Saved :
PIX Version 6.0(1) ------ PIX 当前的*作系统版本为 6.0
Nameif ethernet0 outside security0
Nameif ethernet1 inside security100 ------ 显示目前 pix 只有 2 个接口
Enable password 7Y051HhCcoiRTSQZ encrypted
Passed 7Y051HhCcoiRTSQZ encrypted ------ pix 防火墙密码在默认状态下已被加密，在配置文件中不会以明文显示，telnet 密码缺省为 cisco
Hostname PIX525 ------ 主机名称为 PIX525
Domain-name 123.com ------ 本地的一个域名服务器 123.com，通常用作为外部访问
Fixup protocol ftp 21
Fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060 ------ 当前启用的一些服务或协议，注意 rsh 服务是不能改变端口号的
names ------ 解析本地主机名到 ip 地址，在配置中可以用名字代替 ip 地址，当前没有设置，所以列表为

空
pager lines 24 ------ 每 24 行一分页
interface ethernet0 auto
interface ethernet1 auto ------ 设置两个网卡的类型为自适应
mtu outside 1500
mtu inside 1500 ------ 以太网标准的 MTU 长度为 1500 字节
ip address outside 61.144.51.42 255.255.255.248
ip address inside 192.168.0.1 255.255.255.0 ------ pix 外网的 ip 地址 61.144.51.42，内网的 ip 地址 192.168.0.1
ip audit info action alarm
ip audit attack action alarm ------ pix 入侵检测的 2 个命令。当有数据包具有攻击或报告型特征码时，pix 将采取报警动作（缺省动作），向指定的日志记录主机产生系统日志消息；此外还可以作出丢弃数据包和发出 tcp 连接复位信号等动作，需另外配置。
pdm history enable ------ PIX 设备管理器可以图形化的监视
PIX arp timeout 14400 ------ arp 表的超时时间
global (outside) 1 61.144.51.46 ------ 如果你访问外部论坛或用 QQ 聊天等等，上面显示的 ip 就是这个
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside, outside) 61.144.51.43 192.168.0.8 netmask 255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 61.144.51.43 eq www any
conduit permit udp host 61.144.51.43 eq domain any ------ 用 61.144.51.43 这个 ip 地址提供 domain-name 服务，而且只允许外部用户访问 domain 的 udp 端口
route outside 0.0.0.0 0.0.0.0 61.144.51.61 1 ------ 外部网关 61.144.51.61
timeout xlate 3:00:00 ------ 某个内部设备向外部发出的 ip 包经过翻译(global)后，在缺省 3 个小时之后此数据包若没有活动，此前创建的表项将从翻译表中删除，释放该设备占用的全局地址
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute ------ AAA 认证的超时时间，absolute 表示连续运行 uauth 定时器，用户超时后，将强制重新认证
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius ------ AAA 服务器的两种协议。AAA 是指认证，授权，审计。Pix 防火墙可以通过 AAA 服务器增加内部网络的安全
no snmp-server location no snmp-server contact snmp-server community public ------ 由于没有设置 snmp 工作站，也就没有 snmp 工作站的位置和联系人
no snmp-server enable traps ------ 发送 snmp 陷阱 floodguard enable ------ 防止有人伪造大量认证请求，将 pix 的 AAA 资源用完
no sysopt route dnat telnet timeout 5 ssh timeout 5 ------ 使用 ssh 访问 pix 的超时时间
terminal width 80 Cryptochecksum:a9f03ba4ddb72e1ae6a543292dd4f5e7
PIX525#
PIX525#write memory ------ 将配置保存
上面这个配置实例需要说明一下，pix 防火墙直接摆在了与 internet 接口处，此处网络环境有十几个公有 ip,可能会有朋友问如果我的公有 ip 很有限怎么办？你可以添加 router 放在 pix 的前面，或者 global 使用单一 ip 地址，和外部接口的 ip 地址相同即可。另外有几个维护命令也很有用，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，ping outside | inside ip_address 确定连

通性。

PIX 上实现 VPN 步骤
在 PIX 上防火墙用预共享密钥配置 IPSec 加密主要涉及到 4 个关键任务：

一、为 IPSec 做准备

为 IPSec 做准备涉及到确定详细的加密策略，包括确定我们要保护的主机和网络，选择一种认证方法，确定有关 IPSec 对等体的详细信息，确定我们所需的 IPSec 特性，并确认现有的访问控制列表允许 IPSec 数据流通过；
步骤 1：根据对等体的数量和位置在 IPSec 对等体间确定一个 IKE（IKE 阶段 1，或者主模式）策略；
步骤 2：确定 IPSec（IKE 阶段 2，或快捷模式）策略，包括 IPSec 对等体的细节信息，例如 IP 地址及 IPSec 变换集和模式；
步骤 3：用"write terminal"、"show isakmp"、"show isakmp policy"、"show crypto map "命令及其他"show"命令来检查当前的配置；
步骤 4：确认在没有使用加密前网络能够正常工作，用"ping"命令并在加密前运行测试数据流来排除基本的路由故障；
步骤 5：确认在边界路由器和 PIX 防火墙中已有的访问控制列表允许 IPSec 数据流通过，或者想要的数据流将可以被过滤出来。

二、配置 IKE 配置 IKE 涉及到启用 IKE（和 isakmp 是同义词），创建 IKE 策略，和验证我们的配置；
步骤 1：用"isakmp enable"命令来启用或关闭 IKE；
步骤 2：用"isakmp policy"命令创建 IKE 策略；
步骤 3：用"isakmp key"命令和相关命令来配置预共享密钥；
步骤 4：用"show isakmp [policy]"命令来验证 IKE 的配置。

三、配置 IPSec

IPSec 配置包括创建加密用访问控制列表，定义变换集，创建加密图条目，并将加密集应用到接口上去；

步骤 1：用 access-list 命令来配置加密用访问控制列表； 例如： access-list acl-name {permit|deny} protocol src_addr src_mask [operator port [port]]dest_addr dest_mask [operator prot [port]]
步骤 2：用 crypto ipsec transform-set 命令配置变换集； 例如： crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]] 3. 步骤 3：（任选）用 crypto ipsec security-association lifetime 命令来配置全局性的 IPSec 安全关联的生存期；
步骤 4：用 crypto map 命令来配置加密图；
步骤 5：用 interface 命令和 crypto map map-name interface 应用到接口上； 6. 步骤 6：用各种可用的 show 命令来验证 IPSec 的配置。

四、测试和验证 IPSec
该任务涉及到使用"show " 、"debug"和相关的命令来测试和验证 IPSec 加密工作是否正常，并为之排除故障。
样例：

PIX 1 的配置：
!configure the IP address for each PIX Firewall interface
ip address outside 192.168.1.1 255.255.255.0
ip address inside 10.1.1.3 255.255.255.0
ip address dmz 192.168.11.1 255.255.255.0
global (outside) 1 192.168.1.10-192.168.1.254 netmask 255.255.255.0
!creates a global pooll on the outside interface,enables NAT.
!windows NT server
static (inside,outside) 192.168.1.10 10.1.1.4 netmask 255.255.255.0
!Crypto access list specifiles between the global and the inside server beind PIX Firewalls is encrypted ,The source and destination IP address are the global IP addresses of the statics.
Access-list 101 permit ip host 192.168.1.10 host 192.168.2.10
!The conduit permit ICMP and web access for testing.
Conduit permit icmp any any Conduit permit tcp host 192.168.1.10 eq www any
route outside 0.0.0.0 0.0.0.0 192.168.1.2 1
!Enable IPSec to bypass access litst,access ,and confuit restrictions
syspot connnection permit ipsec
!Defines a crypto map transform set to user esp-des
crypto ipsec transform-set pix2 esp-des
crypto map peer2 10 ipsec-isakmp!

完全配置： ip address outside 202.105.113.194 255.255.255.0 /*看电信给你的 IP
ip address inside 192.168.1.1 255.255.255.0
!
global (outside) 1 202.105.113.195-202.105.113.200
global (outside) 1 202.105.113.201
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 202.105.113.203 192.168.1.10 netmask 255.255.255.255 0 0
static (inside,outside) 202.105.113.205 192.168.1.11netmask 255.255.255.255 0 0
conduit permit icmp any any conduit permit tcp host 202.105.113.203 eq www any
conduit permit tcp host 202.105.113.203 eq ftp any
conduit permit tcp host 202.105.113.205 eq smtp any
conduit permit tcp host 202.105.113.205 eq pop3 any
!
route outside 0.0.0.0 0.0.0.0 202.105.113.193 1
route inside 0.0.0.0 0.0.0.0 192.168.1.1

4. 指定要进行转换的内部地址（nat）
网络地址翻译（nat）作用是将内网的私有 ip 转换为外网的公有 ip.Nat 命令总是与 global 命令一起使用，这是因为 nat 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。

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

其中（if_name）表示内网接口名字，例如 inside。Nat_id 用来标识全局地址池，使它与其相应的 global 命令相匹配，local_ip 表示内网被分配的 ip 地址。例如 0.0.0.0 表示内网所有主机可以对外访问。[netmark]表示内网 ip 地址的子网掩码。

例 1．Pix525(config)#nat (inside) 1 0 0
表示启用 nat,内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0

例 2．Pix525(config)#nat (inside) 1 172.16.5.0 255.255.0.0
表示只有 172.16.5.0 这个网段内的主机可以访问外网。

5. 指定外部地址范围（global） global 命令把内网的 ip 地址翻译成外网的 ip 地址或一段地址范围。
Global 命令的配置语法：global (if_name) nat_id ip_address-ip_address [netmark global_mask]
其中（if_name）表示外网接口名字，例如 outside.。Nat_id 用来标识全局地址池，使它与其相应的 nat 命令相匹配，ip_address-ip_address 表示翻译后的单个 ip 地址或一段 ip 地址范围。[netmark global_mask]表救□谜 p 地址的网络掩码。

例 1．Pix525(config)#global (outside) 1 61.144.51.42-61.144.51.48
表示内网的主机通过 pix 防火墙要访问外网时，pix 防火墙将使用 61.144.51.42-61.144.51.48 这段 ip 地址池为要访问外网的主机分配一个全局 ip 地址。

例 2．Pix525(config)#global (outside) 1 61.144.51.42 表示内网要访问外网时，pix 防火墙将为访问外网的所有主机统一使用 61.144.51.42 这个单一 ip 地址。

例 3. Pix525(config)#no global (outside) 1 61.144.51.42 表示删除这个全局表项。

6. 设置指向内网和外网的静态路由（route） 定义一条静态路由。
route 命令配置语法：route (if_name) 0 0 gateway_ip [metric]
其中（if_name）表示接口名字，例如 inside，outside。Gateway_ip 表示网关路由器的 ip 地址。[metric]表示到 gateway_ip 的跳数。通常缺省是 1。

例 1． Pix525(config)#route outside 0 0 61.144.51.168 1
表示一条指向边界路由器（ip 地址 61.144.51.168）的缺省路由。

例 2． Pix525(config)#route inside 10.1.1.0 255.255.255.0 172.16.0.1 1
Pix525(config)#route inside 10.2.0.0 255.255.0.0 172.16.0.1 1
如果内部网络只有一个网段，按照例 1 那样设置一条缺省路由即可；如果内部存在多个网络，需要配置一条以上的静态路由。上面那条命令表示创建了一条到网络 10.1.1.0 的静态路由，静态路由的下一条路由器 ip 地址是 172.16.0.1。

OK，这 6 个基本命令若理解了，就可以进入到 pix 防火墙的一些高级配置了。

A. 配置静态 IP 地址翻译（static）
如果从外网发起一个会话，会话的目的地址是一个内网的 ip 地址，static 就把内部地址翻译成一个指定的全局地址，允许这个会话建立。

static 命令配置语法：
static (internal_if_name，external_if_name) outside_ip_address 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 为外部网络接口，安全级别较低，如 outside 等。outside_ip_address 为正在访问的较低安全级别的接口上的 ip 地址 。inside_ ip_address 为内部网络的本地 ip 地址。

例 1.　Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.8
表示 ip 地址为 192.168.0.8 的主机，对于通过 pix 防火墙建立的每个会话，都被翻译成 61.144.51.62 这个全局地址，也可以理解成 static 命令创建了内部 ip 地址 192.168.0.8 和外部 ip 地址 61.144.51.62 之间的静态映射。

例 2．　Pix525(config)#static (inside, outside) 192.168.0.2 10.0.1.3

例 3.　Pix525(config)#static (dmz, outside) 211.48.16.2 172.16.10.8
注释同例 1。
通过以上几个例子说明使用 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，使它们可以进入到具有较高安全级别的指定接口。

B. 管道命令（conduit）
前面讲过使用 static 命令可以在一个本地 ip 地址和一个全局 ip 地址之间创建了一个静态映射，但从外部到内部接口的连接仍然会被 pix 防火墙的自适应安全算法(ASA)阻挡。
conduit 命令用来允许数据流从具有较低安全级别的接口流向具有较高安全级别的接口，例如允许从外部到 DMZ 或内部接口的入方向的会话。对于向内部接口的连接，static 和 conduit 命令将一起使用，来指定会话的建立。
conduit 命令配置语法：
conduit permit | deny global_ip port[-port] protocol foreign_ip [netmask]
permit | deny 允许 ｜拒绝访问 global_ip 指的是先前由 global 或 static 命令定义的全局 ip 地址，如果 global_ip 为 0，就用 any 代替 0；如果 global_ip 是一台主机，就用 host 命令参数。
port 指的是服务所作用的端口，例如 www 使用 80，smtp 使用 25 等等，我们可以通过服务名称或端口数字来指定端口。
protocol 指的是连接协议，比如：TCP、UDP、ICMP 等。
foreign_ip 表示可访问 global_ip 的外部 ip。对于任意主机，可以用 any 表示。如果 foreign_ip 是一台主机，就用 host 命令参数。

例 1. Pix525(config)#conduit permit tcp host 192.168.0.8 eq www any
这个例子表示允许任何外部主机对全局地址 192.168.0.8 的这台主机进行 http 访问。其中使用 eq 和一个端口来允许或拒绝对这个端口的访问。Eq ftp 就是指允许或拒绝只对 ftp 的访问。

例 2. Pix525(config)#conduit deny tcp any eq ftp host 61.144.51.89
表示不允许外部主机 61.144.51.89 对任何全局地址进行 ftp 访问。

例 3. Pix525(config)#conduit permit icmp any any
表示允许 icmp 消息向内部和外部通过。

例 4. Pix525(config)#static (inside, outside) 61.144.51.62 192.168.0.3
Pix525(config)#conduit permit tcp host 61.144.51.62 eq www any
这个例子说明 static 和 conduit 的关系。192.168.0.3 在内网是一台 web 服务器，现在希望外网的用户能够通过 pix 防火墙得到 web 服务。所以先做 static 静态映射：192.168.0.3－>61.144.51.62（全局），然后利用 conduit 命令允许任何外部主机对全局地址 61.144.51.62 进行 http 访问。

C. 配置 fixup 协议
fixup 命令作用是启用，禁止，改变一个服务或协议通过 pix 防火墙，由 fixup 命令指定的端口是 pix 防火墙要侦听的服务。见下面例子：
例 1. Pix525(config)#fixup protocol ftp 21 启用 ftp 协议，并指定 ftp 的端口号为 21
例 2. Pix525(config)#fixup protocol http 80
Pix525(config)#fixup protocol http 1080 为 http 协议指定 80 和 1080 两个端口。
例 3. Pix525(config)#no fixup protocol smtp 80 禁用 smtp 协议。

D. 设置 telnet

telnet 有一个版本的变化。在 pix OS 5.0（pix*作系统的版本号）之前，只能从内部网络上的主机通过 telnet 访问 pix。在 pix OS 5.0 及后续版本中，可以在所有的接口上启用 telnet 到 pix 的访问。当从外部接口要 telnet 到 pix 防火墙时，telnet 数据流需要用 ipsec 提供保护，也就是说用户必须配置 pix 来建立一条到另外一台 pix，路由器或 vpn 客户端的 ipsec 隧道。另外就是在 PIX 上配置 SSH，然后用 SSH client 从外部 telnet 到 PIX 防火墙，PIX 支持 SSH1 和 SSH2，不过 SSH1 是免费软件，SSH2 是商业软件。相比之下 cisco 路由器的 telnet 就做得不怎么样了。
telnet 配置语法：telnet local_ip [netmask] local_ip
表示被授权通过 telnet 访问到 pix 的 ip 地址。如果不设此项，pix 的配置方式只能由 console 进行。

说了这么多，下面给出一个配置实例供大家参考。

Welcome to the PIX firewall

Type help or '?' for a list of available commands.
PIX525> en
Password:
PIX525#sh config :
Saved :
PIX Version 6.0(1) ------ PIX 当前的*作系统版本为 6.0
Nameif ethernet0 outside security0
Nameif ethernet1 inside security100 ------ 显示目前 pix 只有 2 个接口
Enable password 7Y051HhCcoiRTSQZ encrypted
Passed 7Y051HhCcoiRTSQZ encrypted ------ pix 防火墙密码在默认状态下已被加密，在配置文件中不会以明文显示，telnet 密码缺省为 cisco
Hostname PIX525 ------ 主机名称为 PIX525
Domain-name 123.com ------ 本地的一个域名服务器 123.com，通常用作为外部访问

Fixup protocol ftp 21
Fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060 ------ 当前启用的一些服务或协议，注意 rsh 服务是不能改变端口号的
names ------ 解析本地主机名到 ip 地址，在配置中可以用名字代替 ip 地址，当前没有设置，所以列表为空
pager lines 24 ------ 每 24 行一分页
interface ethernet0 auto
interface ethernet1 auto ------ 设置两个网卡的类型为自适应
mtu outside 1500
mtu inside 1500 ------ 以太网标准的 MTU 长度为 1500 字节
ip address outside 61.144.51.42 255.255.255.248
ip address inside 192.168.0.1 255.255.255.0 ------ pix 外网的 ip 地址 61.144.51.42，内网的 ip 地址 192.168.0.1
ip audit info action alarm
ip audit attack action alarm ------ pix 入侵检测的 2 个命令。当有数据包具有攻击或报告型特征码时，pix 将采取报警动作（缺省动作），向指定的日志记录主机产生系统日志消息；此外还可以作出丢弃数据包和发出 tcp 连接复位信号等动作，需另外配置。
pdm history enable ------ PIX 设备管理器可以图形化的监视
PIX arp timeout 14400 ------ arp 表的超时时间
global (outside) 1 61.144.51.46 ------ 如果你访问外部论坛或用 QQ 聊天等等，上面显示的 ip 就是这个
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside, outside) 61.144.51.43 192.168.0.8 netmask 255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 61.144.51.43 eq www any
conduit permit udp host 61.144.51.43 eq domain any ------ 用 61.144.51.43 这个 ip 地址提供 domain-name 服务，而且只允许外部用户访问 domain 的 udp 端口
route outside 0.0.0.0 0.0.0.0 61.144.51.61 1 ------ 外部网关 61.144.51.61
timeout xlate 3:00:00 ------ 某个内部设备向外部发出的 ip 包经过翻译(global)后，在缺省 3 个小时之后此数据包若没有活动，此前创建的表项将从翻译表中删除，释放该设备占用的全局地址
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute ------ AAA 认证的超时时间，absolute 表示连续运行 uauth 定时器，用户超时后，将强制重新认证
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius ------ AAA 服务器的两种协议。AAA 是指认证，授权，审计。Pix 防火墙可以通过 AAA 服务器增加内部网络的安全
no snmp-server location no snmp-server contact snmp-server community public ------ 由于没有设置 snmp 工作站，也就没有 snmp 工作站的位置和联系人
no snmp-server enable traps ------ 发送 snmp 陷阱 floodguard enable ------ 防止有人伪造大量认证请求，将 pix 的 AAA 资源用完

no sysopt route dnat telnet timeout 5 ssh timeout 5 ------ 使用 ssh 访问 pix 的超时时间
terminal width 80 Cryptochecksum:a9f03ba4ddb72e1ae6a543292dd4f5e7
PIX525#
PIX525#write memory ------ 将配置保存
上面这个配置实例需要说明一下，pix 防火墙直接摆在了与 internet 接口处，此处网络环境有十几个公有 ip,可能会有朋友问如果我的公有 ip 很有限怎么办？你可以添加 router 放在 pix 的前面，或者 global 使用单一 ip 地址，和外部接口的 ip 地址相同即可。另外有几个维护命令也很有用，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，ping outside | inside ip_address 确定连通性。