防火墙在企业网络中的应用

任俊峰 （新疆兵团武警指挥部 乌市南湖路65号 830063）

摘要：在Internet应用迅速普及发展的今天，企业计算机网络接入Internet获取资源、提供信息是广泛的应用模式。此时，如何保护企业计算机网络资源不受外部非法侵袭是一个严肃、重要的课题。本文列举XXX企业计算机网络系统的Internet访问安全核心Cisco公司的PIX 525防火墙，介绍如何利用防火墙提供的安全策略，构筑一般企业计算机网络Internet应用的安全。

关键字：Intranet RIP (Route Information Protocol) PIX (Private Internet Exchange) NAT (Network Address Translation) PAT (Port Address Translation)

1 需求分析

XXX计算机网络是以3Com公司CoreBuilder 9000为企业核心层交换机，以3Com CoreBuilder 7000HD、CoreBulider 3500和Cisco Catalyst 4006为各二级单位分布层交换机，以3Com SSII 1100/3300和Cisco Catalyst 3500为访问层交换机的三层星型网络结构，采用先进的千兆以太网技术，融合历史的ATM网络技术，结合Cisco 2511、1601等提供的DDN链路进行远程局域网络连接和移动用户拨号访问，利用Cisco 3661的2M DDN串型链路连接Internet。

随着XXX应用水平的不断提高，利用Internet与外部交流信息的需求非常迫切，如何既要保证XXX网络不受外部Internet的非法访问和攻击，又能安全快速的访问Internet，是企业网络安全建设的必要条件，而网络防火墙是解决这一问题的最好方法。

经过分析和比较后，XXX计算机网络采用了Cisco PIX 525防火墙作为企业用户Internet访问时的安全保证。下面我们结合PIX 525防火墙的功能谈谈防火墙在企业网络安全中的应用。

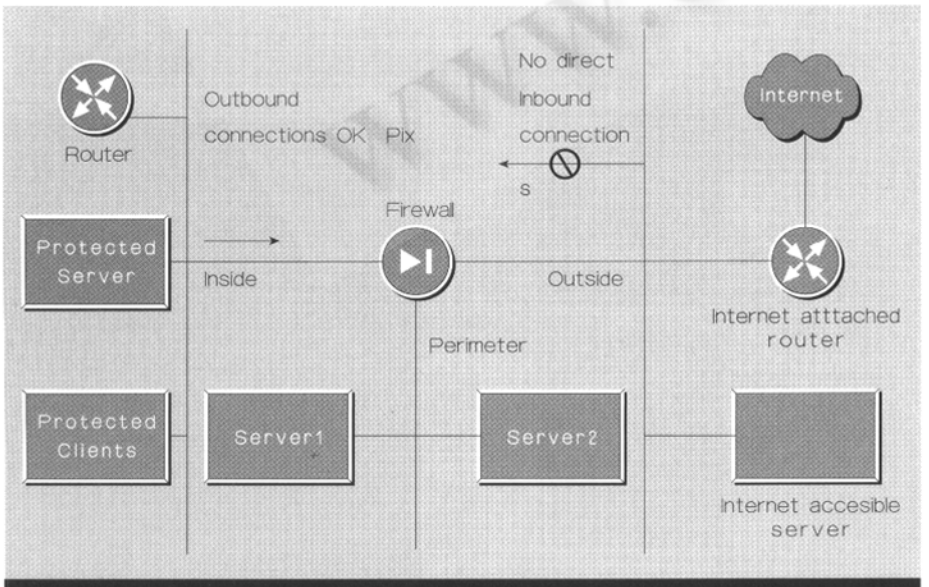

图1

2 防火墙

PIX防火墙能在两个或多个网络之间防止非授权的连接，即PIX防火墙能保护一个或多个网络，与外部的、非保护的网络隔离，防止非授权访问，这些网络间的所有连接都能被PIX防火墙控制。

为了在你的组织中高效使用防火墙，你需要一个安全策略来确认被保护网络的所有数据包只能通过防火墙传递到非保护网络。这样，你就能控制谁能访问网络，访问什么服务，及如何利用PIX防火墙的功能实现你的安全策略。

图1显示了PIX防火墙如何保护内部网络安全地访问Internet

在这个结构中，PIX防火墙在被保护网络和非保护网络之间形成了一个边界。被保护网络和非保护网络之间的所有数据包流量必须经过防火墙以遵循一定的安全策略。被保护网络通常能访问Internet。PIX防火墙让你将诸如Web、SNMP、E-mail等服务放置在被保护网络中，以控制外部用户的对这些服务的访问。

另一方面，服务系统也能放置在Perimeter网络中，见图1。PIX防火墙也能控制和监视Inside网络或Outside网络对这些服务系统的访问。

典型的，Inside网络就是一个组织自己的内部Intranet网络，Outside网络就是Internet。但是，PIX防火墙也能在Intranet网络中使用以隔离或保护一组内部的计算机系统。Perimeter网络能和Inside网络一样进行安全配置。PIX防火墙的Inside、Perimeter和Outside接口能监听RIP路由更新消息，如果需要，所有的接口能广播一个缺省的RIP路由。

PIX防火墙的工作原理如下：

数据包如何通过防火墙

当向外连接的数据包(Outbound Packets)到达PIX防火墙的被保护接口时(Inside Interface)，PIX防火墙检查先前的数据包是否是来自此主机。如果没有，PIX防火墙就在它的状态表为新的连接建立一个转换槽(translation slot)。通过网络地址转换(NAT)或端口地址转换(PAT)的分配，这个槽包括内部IP地址和一个唯一的全局IP地址。PIX防火墙这时转换这个数据包的源IP地址(source IP)为这个唯一的全局IP地址，并按需修改其他字段，然后转发这个数据包到合适的非保护接口。

当向内连接的数据包(Inbound Packets)到达PIX防火墙的非保护接口时(outside Interface)，它必须先经过PIX防火墙的安全检查。如果数据包检查通过，则PIX防火墙移走这个数据包的目的IP地址(destination IP)，插入内部的IP地址，这样，这个数据包被转发到被保护接口。

转换内部地址

动态转换对在Internet上不需要固定地址的桌面计算机是非常有用的。使用非NIC(Network Information Center)注册的IP地址的内部网络主机通过在PIX防火墙中的地址转换能直接访问Internet上的标准TCP/IP程序，而不需要特定的客户程序。PIX防火墙支持能为每个内部主机提供一个全局唯一网络地址的网络地址转换(NAT)，和为许多内部主机提供一个共享的全局唯一网络地址的端口地址转换(PAT)。NAT和PAT能转换为多达64K主机地址。

PIX防火墙中的另一个地址转换是静态转换。静态转换能有效地移动一个内部的、非注册主机到防火墙中的虚网。这对一个需要映射到外部Internet网关的内部主机是非常有用的，如，SMTP服务器。

3 安全策略

PIX防火墙能对诸如Web、FTP、Telnet、和SMTP等网络服务分别提供安全策略，使企业网络安全配置具有灵活性和高性能。为了有效地在企业网络中使用防火墙，需要规划网络安全策略以保护重要的数据资源，通过建立和改进企业网络安全策略，能防止企业外部网络的非法恶意攻击，控制企业网络失效的概率。

网络安全策略必须确保用户只能执行被授权的任务和获取被授权的信息，不能具有对关键数据、应用程序和系统操作环境破坏的能力。为了建立全面的网络安全策略，网络管理员需确定以下作：

(1) 画出企业网络完全示意图，说明系统连接至Internet细节，服务器细节及相应的IP地址。

(2) 标识出应被保护的系统，能被外部网络访问的系统等。PIX防火墙的网络地址转换功能(NAT)能实现这些功能。

(3) 标识出内部网络的么服务能被外部网络访问，并说明外 部用户访问这些服务所需的验证和授权方法、类型。

(4) 标识出与防火墙协调工作的路由器。

需要说明的是，PIX防火墙不能防止来自网络内部的恶意攻击，为了防止这些内部威胁，所有的内部网络用户只需分配与其工作相适应的最小权限。

我们以XXX计算机网络为例，根据PIX防火墙的功能，说明企业网络安全策略的规划和实施。

根据XXX计算机网络Internet访问的系统配置，画出系统示意图2：

在此网络中，PIX防火墙安装了两个接口，一个内部接口Inside (10.124.1.253)和一个外部接口Outside (127.104.10.23)，Inside接口连接企业内部网络10.124.0.0，Outside接口连接外部

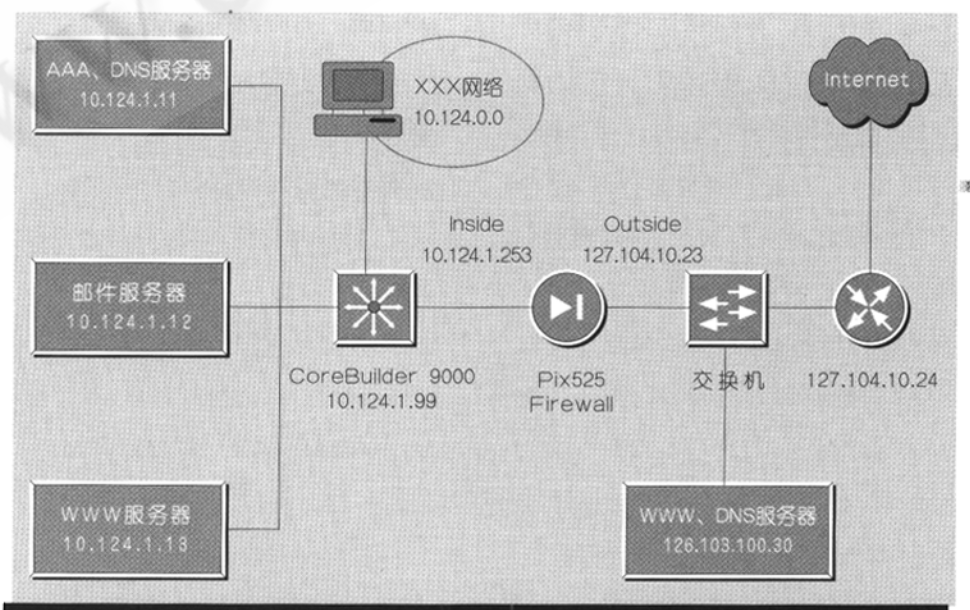

图2

Internet，Inside接口连接的企业内部网络使用私有IP地址，Outside接口连接的外部的网络连接设备使用Internet合法的IP地址，此网络的Internet的访问使用一台Cisco 3600路由器，通过2M DDN数据专线连接至Internet，防火墙外设置的一台服务器主要作为DNS服务，进行Web和电子邮件的域名解析。

基本的Internet访问安全策略是内部网络授权用户可以访问外部Internet，而外部Internet用户不能访问内部网络，E-mail服务实现内外部网络电子邮件的相互访问，允许外部Internet电子邮件进入内部网络，即内部网络用户只需设置一个邮件账号，即可实现内部网络和外部Internet网络电子邮件的收发，实现企业信息的对外发布。

根据上述安全策略的要求，内部网络需设置一台使用Cisco ACS 2.3软件的AAA验证服务器以适合PIX 525防火墙实现Internet访问的授权，只有授权用户才能进行相应服务类型的Internet访问。为了实现内部网络用户访问Internet，利用PIX防火墙的网络地址转换(NAT)功能，将内部网络地址转换为外部合法IP地址。为了允许外部网络访问内部E-mail服务资源，利用PIX防火墙的静态地址映射(Static)功能，将外部虚拟邮件服务器地址127.104.10.25和内部网络邮件服务器地址10.124.1.12映射捆绑而实现内外部网络电子邮件的收发。例如，当内部用户向外部网络发送E-mail时，PIX防火墙将10.124.1.12地址转换为127.104.10.25；当外部用户向内部网络发送E-mail时，PIX防火墙将127.104.10.25地址转换为10.124.1.12，从而实现内外部邮件的收发。为了实现企业信息的对外发布，即可使外部用户访问内部WWW服务器，也可在防火墙外部Outside网络端或Perimeter网络端设置WWW服务器，我们在此选择了在防火墙外部Outside网络端设置了一台WWW服务器用于企业信息的对外发布，此服务器也可进行外部合法IP地址的解析。

通过对网络安全策略的分析，总结具体的实现方法，就可利用防火墙相应的功能进行适当的配置以实现Internet访问的安全。

4 配置

防火墙可以针对不同的企业网络安全策略需求，进行相应 的配置以实现网络安全。各种类型防火墙的主要功能基本一致，只是系统软件的操作环境不一致。我们现以Cisco PIX 525防火墙为例，依据上述XXX计算机网络安全策略，简述利用防火墙的一般功能实现网络安全，对其他类型防火墙的配置有一定的参考。

PIX防火墙缺省的安全策略是允许从被保护网络(Inside)到非保护网络(Outside)的向外连接，拒绝任何从非保护网络(Outside)到被保护网络(Inside)的向内连接。可以对缺省策略进行修改以适合企业自身网络安全策略的需求。

第一步：防火墙端口设置

```
nameif ethernet0 outside security0
; 命名ethernet0端口为外部端口outside，且安全级别最低
nameif ethernet1 inside security100
; 命名ethernet1端口为内部端口inside，且安全级别最高
ip address outside 127.104.10.23 255.255.255.248
; 指定外部端口地址为外部合法IP地址
ip address inside 10.124.1.253 255.255.255.0
; 指定内部端口地址为内部保留IP地址
```

第二步：全局地址指定

```
global (outside) 1 127.104.10.26-127.104.10.27
netmask 255.0.0.0
```

第三步：转换内部地址为全局地址池中合法IP地址

```
nat (inside) 1 10.124.0.0 255.255.0.0 0 0
```

第四步：内外部地址静态映射

```
static (inside,outside) 127.104.10.25 10.124.1.12
netmask 255.255.255.255 255 0
```

第五步：允许指定外部主机访问内部smtp邮件服务，拒绝其他所有主机访问内部所有服务。

```
conduit permit tcp host 127.104.10.25 eq smtp any
conduit deny tcp any any
```

第六步：设置路由协议

```
rip outside passive
; 外部端口不进行rip协议广播
rip inside default
; 内部端口网络协议缺省为rip
route outside 0.0.0.0 0.0.0.0 127.104.10.28 1
; 指定外部网络缺省路由网关
route inside 0.0.0.0 0.0.0.0 10.124.1.254 1
; 指定内部网络缺省路由网关
```

5 结束语

XXX计算机网络利用Cisco Pix 525防火墙非常有效地实 现了对Internet访问的网络安全，有力地促进了XXX计算机应用水平的发展，保证了XXX安全快捷地与外部世界交流信息的能力。当然，有效实现网络安全的方法手段很多，我们以Cisco PIX 525防火墙为例介绍企业组织Internet访问的安全实现，希望能与同行进行经验交流。

参考文献

[1]《Configuration Guide for the PIX Firewall》Cisco System，Inc.