文章编号：1006-4354（2004）01-0033-02

防火墙在陕西气象信息网络中的应用

燕东渭[1]，夏巧利[1]，史海燕[2]

（1. 陕西省气象台，陕西西安 710014；2. 渭南市气象局，陕西渭南 714000）

中图分类号：TP393 **文献标识码**：B

防火墙是设置在不同网络（如 Internet 和内部网）之间的部件，是不同网络之间信息的唯一出入口，能根据设订的安全规则控制出入网络的信息流。它是提供信息安全服务，实现网络和信息安全的基础设施。防火墙能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。以陕西省气象信息网络系统采用的北京天融信公司的网络卫士防火墙为例，介绍防火墙的基本配置。该产品采用了目前流行的多种网络安全机制，如多端口结构、NAT、端口映射和地址映射、安全服务器网络（SSN）、用户鉴别、透明代理、安全套接层（SSL）、支持安全外壳 SSH、抗攻击能力、入侵检测等等。该防火墙的基本配置需要采用两个步骤，即串口管理和 Web 管理，配置过程首先通过串口进行最基本的接口、路由等配置，然后再利用防火墙提供的 WWW 服务方式配置访问规则、安全政策等。

1 串口管理配置

串口管理负责对防火墙的基本配置，并可以设置修改 Web 管理员的口令，并限制 Web 管理员登录的 IP 地址。在防火墙初始配置完成后，只要网络的拓扑结构不再修改，无需再进行串口配置。防火墙安装后，串口管理员必须通过 Console 口配置防火墙的系统，包括设定防火墙的 IP、路由、域名服务器、防火墙接口配置、用户管理、透明配置等。

1.1 配置各个接口的 IP 地址

```
ifconfig eth0 61.134.1.70 255.255.255.255
ifconfig eth1 61.134.1.71 255.255.255.255
ifconfig eth2 10.1.1.42 255.255.255.255
```

1.2 配置接口路由

```
route add 61.134.1.66 255.255.255.255 eth1
route add 10.1.2.0 255.255.255.0 eth2
route add 61.134.1.65 eth0
route add default 61.134.1.65
```

1.3 配置接口的属性，用 eth0 作为外网口，eth1 作为 SSN，eth2 作为内网口。

```
fwip add eth0 61.134.1.70 o
fwip add eth1 61.134.1.71 s
fwip add eth2 10.1.1.42 i
```

还可以指明透明方式，settran eth0 eth1 on，最后保存并重启防火墙。

2 Web 管理配置

Web 管理则负责日常的防火墙管理和配置，如具体的访问控制规则，安全政策等等，根据不同的网络情况，配置相应的规则。Web 管理员可

收稿日期：2003-10-27

作者简介：燕东渭（1975-），男，陕西周至人，气象电子工程师，主要从事计算机网络管理及开发工作。

期为 29 至 58 d 不等。我们向省建六公司、福园时代广场等建设施工单位提供的气象服务中，增加了日平均温度预报和前一日的日平均温度实况，随时提供逐日的平均温度累计值，以便施工单位掌握每批浇筑试件等效养护龄期的截止日期。建议施工单位根据冷空气的强弱不同，采用人工加热等不同措施，在保证混凝土构件的强度增长不受影响的前提下，尽量缩短混凝土构件的养护时间。受到建设施工单位和建设监理部门的高度重视。

以设置将日志传送到哪个日志服务器，并可以打开和关闭计费日志，通过浏览器还可以察看最近的日志。Web 管理有 3 种常用的配置。

2.1 允许内部用户自由访问 Internet

进入 Netguard Manager（该防火墙的管理软件）管理界面，在规则政策→对象管理→IP 对象中，先创建一个内部用户的对象 in _ user，内容为内部各网段的 IP 地址及相应掩码；再在 OUT 服务对象中创建一个适应于内部用户的服务对象 in _ user，为其增加 3 条服务内容，一是方式选 NAT，协议选 TCP，源端口和目的端口都选 0～65535；二是方式选 NAT，协议选 ICMP；三是方式选 NAT，协议选 UDP，源端口和目的端口都选 0～65535。在规则政策→访问规则中增加一条访问规则，即方向选 OUT，源选 IP→in _ user，目的选 OutService →any，时间选 any，动作选允许。最后，在规则政策→地址转换→静态网址转换中，增加几条静态 NAT 规则，转换依据选源，IP 地址填入内部各个网段的地址（如 10.1.1.0）和掩码，NAT IP 填入防火墙外网接口的地址。有了这条规则，内部用户就可以毫无限制的通过防火墙自由访问 Internet。

特别的，该防火墙本来带有 DNS 功能，即通过在串口配置模式下，在防火墙上指明外部 DNS 的 IP 地址，就可以在内部机器上将 DNS 设置成防火墙的内部地址。但实际上经过多次实验，发现该防火墙的 DNS 功能并不能正常工作，只能在内部机器上直接指外部公网上的 DNS。

2.2 允许内部和外部有限访问 SSN 区域的主机

内部用户访问 SSN，其条件符合上面的规则，可以自由访问 SSN 的主机。外部用户要访问 SSN，先定义一个 IP 对象 web，例如 IP 为 61.134.1.75，掩码 255.255.255.240。再定义一个 In 服务对象 web，为其添加几条服务内容，一是方式选 NONE，协议选 TCP，应用协议选 HTTP；二是方式选 NONE，协议选 TCP，应用协议选 FTP；三是方式选 NONE，协议选 TCP，应用协议选 SMTP；四是方式选 NONE，协议选 TCP，应用协议选 POP－3。增加 1 条访问规则：方向选 IN，源选 IP→any，目的选 IP→web，服务选 web，动作选允许。经过这样的设置，外部用户就可以自由的访问 WWW 和 FTP 服务器，SSN 区的邮件服务器也可以和外部网络的其他邮件服务器交换邮件信息。

2.3 允许外部通过 Internet 访问内部局域网的 FTP 服务器

第一步通过串口连接到防火墙，为防火墙的外网接口增加 FTP 服务器的外部 IP 地址，并指定为 MAP 类型。

ifconfig eth0：0 61. 134. 1. 73 255. 255. 255. 255；为外部接口 eth0 增加 IP 别名 route add 61.134.1.73 255.255.255.255 eth0：0；添加到 61.134.1.73 的单机路由 fwip add eth0：0 61.134.1.73 m；指定 eth0：0 的接口属性为 MAP。

第二步通过 Netguard Manager 的管理界面配置防火墙的访问规则。

先建立 IP 对象 ftp _ map，填入内部 FTP 服务器的外部 IP 地址，例如 61.134.1.73，掩码为 255.255.255.255。再建立一个 IN 服务对象 ftp _ map，增加 2 条内容，一是方式选“地址映射”，协议选 ICMP；二是方式选地址映射，协议选 TCP，源端口 0～65535，目的端口选 20～21。再增加 1 条访问规则，即方向选 IN，源选 IP→any，目的选 IP→ftp _ map，服务选 InService→ftp _ map，动作选允许，在地址转换→IP 映射中，增加 1 条内容，防火墙 IP 选择一个外部 IP，内部服务器 IP 填入内部网络中 FTP 服务器的真实 IP。这样，在 Internet 上的任何一个主机，就可以通过访问前面提到的外部 IP 来达到访问内部 FTP 服务器的目的。由于该防火墙没有提供对于外部地址向内部的反向 NAT，所以真正到达内部 FTP 服务器的 IP 数据包，源 IP 可能五花八门，为了保证网络的连接建立，必须将此 FTP 服务器的默认路由指向防火墙的内部接口地址。虽然此防火墙也提供了端口映射的方式，通过这种方式也可以实现上述要求，但经过多次实验发现，用端口映射并没有用 IP 地址映射稳定，一般防火墙正常 10 min 后再通过它接内部 FTP 服务器，就会出现“连接被拒绝”的情况。所以最好选择 IP 地址映射的方式来完成此功能。