第39章　加强TCP/IP传输安全

作者：Anne Carasik

本章内容包括：

- 定义所需的网络安全
- 加强网络安全
- 应用配置
- 使用端口及可信端口
- 一般安全事务

正如网络必须提供访问一样，网络安全也日益重要。用户必须确定允许哪些应用访问基于TCP端口的网络服务。如果没有安全应用，也可使用虚拟专用网 (VPN)创建安全通道来加强TCP/IP的安全。

39.1　定义所需的网络安全

如果一家很大的公司仅有很小的安全部门，要实现所有的安全策略包括物理安全是一件很困难的事。它必须有较大的部门维护网络的安全。

用户定义网络安全策略时，需要考虑网络流量，确定哪些应用可以出 /入内部网。除非用户非常必要(并且得到很好的控制)，否则不要允许网络报文进入内部网。 Internet上有很多黑客工具可供任何人下载，如果不小心的话，它们很容易对用户的网络造成损害。

如果用户允许报文进入，要非常小心地监视提供服务的软件及端口，并且尽可能快地为应用软件打补丁。

另外，用户可以使用加密应用如Secure Shell、安全套接字层(SSL)或VPN产品，并且使用公钥进行认证和解密以保证进入网络的报文的安全。这一方法也适用于出去的报文。这样用户也可不用担心密钥等信息未经加密就发送到公司站点。

39.1.1　什么是网络安全

简单来说，网络安全就是规定哪些报文允许进入内部网络，哪些报文允许从内部网络流

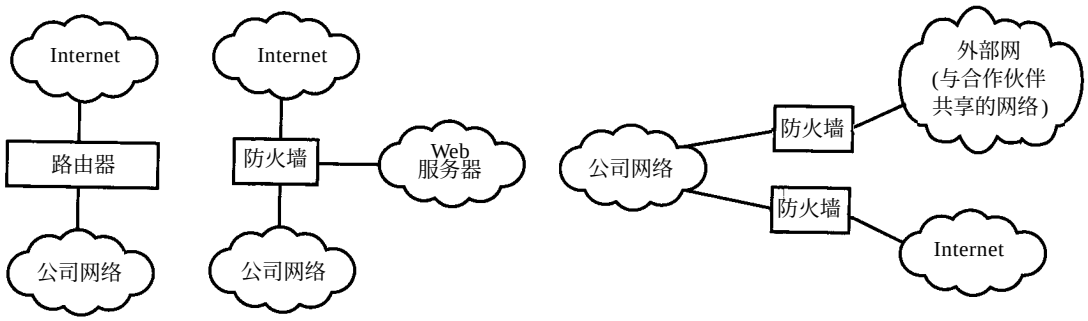

图39-1　控制点如何分隔各种网络

出。内部网可以是局域网(LAN)的子网或广域网(WAN)。

定义网络安全的一种方式是将网络分隔为多个包含控制点如防火墙或路由器的子网。在防火墙或路由器上，用户可以定义允许通过控制点的网络报文类型及网络应用。

控制点类似于过滤器，它仅允许特定的报文通过 (进、出或双向)。例如：电子邮件是商业应用的重要组成部分。在简单的网络安全策略中，邮件允许通过简单邮件传输协议 (SMTP)进出网络，且必须使用25号端口，而所有其他报文都不允许进出网络。

图39-1显示各种控制点的实例。

39.1.2 为什么网络安全非常重要

随着互联网用户人数的膨胀，对安全的需求也日益增加。越来越多的人和公司怀疑遭受过网络攻击。以下是遭受攻击的原因：

- 某些人想获得用户或公司的敏感信息。
- 某些人测试他们的黑客技巧，选中你为他们的目标。
- 某些人仅出于好奇而下载并使用黑客工具。

39.1.3 安全级别

网络安全级别根据访问而定义 —— 允许某些人访问而拒绝另一些人访问。采用网络安全机制，某些用户拥有管理员权限，而另一些仅拥有一般用户的通用权限。

在管理员与一般用户间还包括许多权限等级。某些管理员仅可管理一个系统而另一些可以控制多个系统。例如：某个管理员管理所有服务系统，而另一个管理防火墙。

许多操作系统，如UNIX及Windows NT拥有管理员帐号(UNIX中为根用户帐号)及一般用户帐号，这代表网络安全的两个极端。其他级别的访问权限包括拥有部分管理权限的用户及通用帐号“ guest ”等。

警告 用户增加“ guest ”类型的帐号时要谨慎，该类型的账号是一些UNIX及NT系统的缺省设置。当用户机器连入网络，尤其当机器中含有重要信息时，最好禁止这类账号。

一些操作系统如HP-UX CMW(隔离模式的工作站)采用HP-UX的虚拟Vault技术。HP-UX的独立版本包含多个不同的访问级别，并且没有管理员账号。管理员权限被分隔为多个账号，他们对应的四个不同的访问级别分别为：高层系统(system hign)、低层系统(system low)外部系统(system Outside)及内部系统(system inside)，如图39-2所示。

警告 某些操作系统，如Windows NT，自动给“ everyone ”组完全控制(读、写、删除、执行)权限。用户在必要时需要重新定义相应的权限(如删除“ everyone ”访问)。对于关键的系统或网络文件，也应当删去某些管理员的权限。

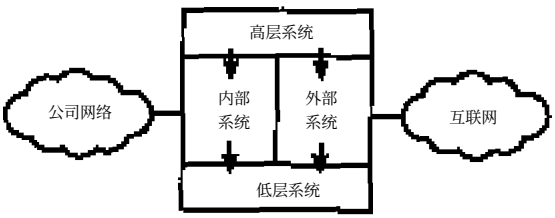

图39-2 HP-UX CMW隔离访问

在四种级别的权限中，用户不能向上写但可向下读。允许同一级别的读写操作。例如，拥有system low权限的管理员帐号不能向system high权限的目录中写。

注意 http://www.hp.com/security/products/virtualvault中包含更多关于Visual Vault的信息。

39.1.4 口令与口令文件

口令是确认用户可对某个帐号访问的通用方式。其他方式如生物认证 (以生物特性进行认证)或公钥系统不如口令认证普遍。目前，大部分网络认证协议及应用仍采用口令方式。

口令认证方式的问题是它很容易被绕过。一些口令体制的加密机制强度有限，另一些机制有绕过口令认证的后门。即使口令体制被正确实施，仍存在其他问题。

不幸的是，绝大多数用户为了便于记忆，采用的口令很容易被破解。大多数用户的口令源于字典中的单词、生日、电话号码或宠物的名字等。

因此，管理员需要提醒用户使用更安全的口令，某些系统强迫用户使用安全性较好的口令。

安全性高的口令包括：

- 字母数字序列
- 大小写混合
- 采用特殊字符(!@#$%^&*_=+\?/><.,"':~、)

这将大大降低口令在短时间内被破解的可能性。

高安全性的口令示例如下：

%Ji928 a*jpeijAjdkljW

然而，此类口令的问题在于用户难于记忆。如果将它写下来，将带来另外的风险。用户可以使用某些常用词的变体建立口令，如：

iLuv2c0mpute Primez!

这类口令既容易记忆也不容易被字典攻击破解。

提示 在口令中增加空隔将有助于口令安全。

同时，用户的口令也需定期更换。许多安全站点的口令需 90天更换一次。出于安全方面的考虑，最好不要重复使用口令。

如果用户想要检查口令是否安全，在测试机器上 (没有任何重要的信息且不与网络相连)创建一些用户帐号，使某些口令易于破解而另一些安全性高。有一些软件可供用户测试口令的安全性，表39-1列出了部分免费破解软件及其站点。

表39-1 口令破解软件

程 序	网 址
Crack	http://www.cs.purdue.edu/COAST
L0phtcrack	http://www.l0pht.com
John the Ripper	http://www.rootshell.com/archive- j457nxi-qi3gq59dv/199812/john-1.6.tgz.html

39.1.5 控制对口令的访问

口令应当被存为加密文件或加密数据库，以防止某些用户读取其他用户的口令并使用这些口令登录。

不同的操作系统将口令存放在不同的位置。表 39-2显示一些口令文件的位置。

表39-2 不同操作系统本地口令文件的位置

操作系统	口令文件位置
Windows NT	Registry
UNIX	/etc/passwd or /etc/shadow

必须正确设置口令文件的权限和所有者。例如， UNIX系统的口令文件只有根用户可以访问，如果口令文件被存为shadow文件，则只有根用户可读Shadow文件。

UNIX的某些更安全的版本如HP-UX CMW和B1 Solaris的口令文件被存为数据库或多个文件的形式，这样可以防止某个用户一旦读取某个文件即可一次破解所有口令。

39.2 加强网络安全

加强网络安全的最大挑战在于使所有用户同意安全策略并自觉执行。大多数用户如果不从网络安全策略中受益，将不会自觉执行。然而仍然有许多方式可帮助用户加强甚至提高网络的安全性。

39.2.1 攻击种类

在网络安全领域，存在多种类型的攻击。

1. 特洛伊木马

特洛伊木马是一组程序，它将自身伪装成其他程序以便为黑客获取系统信息。例如：黑客伪造网络登录界面，得到用户名及口令后，向用户发送登录错误消息，并将得到的信息以邮件发送给攻击者。

特洛伊木马不仅可收集信息，它们还可能破坏系统。特洛伊木马不能复制自身，因此它不是病毒。例如，特洛伊木马可伪造 UNIX登录界面，当用户试图登录时，打印错误信息。每次用户敲入口令后，它都将口令存储在某处以供攻击者使用。

2. 后门

后门一般隐藏在软件或操作系统中，不为使用者知晓，而它可供某些人绕过系统的安全机制获取访问权限。

3. 拒绝服务攻击/服务质量攻击

拒绝服务及服务质量攻击可彻底停止某种网络服务 (如Web服务)或降低服务的质量，如影响服务响应时间，使访问者难以忍受。

4. 网络攻击

网络攻击包括端口扫描。如 5641号端口为Windows NT的PCAnywhere端口。该端口需要用户名及口令认证，但某些用户可以暴力猜测用户名及口令或通过软件的后门进入系统。

5. 欺骗

欺骗就是伪造为某个用户或主机。这种攻击主要针对伯克利的 r系列应用。主要是因为r系列应用信任主机名，它并不检查主机名是否来自正确的位置及主机。

r系列应用很容易欺骗主要是因为主机名及用户名认证很容易伪造。用户可以在外部系统中设置内部主机信任的用户名。不幸的是，系统从不检测登录的系统是否确实是可信任的系统。任何用户都可使用主机名欺骗 r系列应用。

注意 目前，路由器的IP地址反欺骗机制可以防止某些欺骗，但它不影响主机名欺骗。用户可以定义一些规则禁止r系列应用的报文进入网络。

6. 口令破解

如果某人可获得口令文件或NT的注册表，就可以从互联网上下载某些破解软件对口令进行破解。如果时间允许，破解软件总可以得到用户口令，使破解者进入机器。

7. 软件开采与缓存区溢出

目前，通用的攻击方法是检查软件或程序的漏洞，当程序无法处理大量的输入信息时，可使入侵者获取管理员或根用户的权限。这使程序执行错误，产生内存转储（memory dump)。这种类型的攻击称为缓存区溢出。

许多网络应用，如sendmail和NFS等均有漏洞。因此，它们被认为是不安全的网络应用。然而因为邮件的必要性以及用户对网络文件系统的需求，这些应用仍被广泛采用。

注意 除了sendmail外，还存在多种SMTP应用，如qmail，它是安全邮件服务包，可从http://www.qmail.org/上获得更详细的信息。

虽然NFS有安全风险，但它仍然得到广泛使用， AFS是NFS的同类应用，它比NFS的安全性更高，详细信息见：http://www.faqs.org/faqs/afs-faq/。

8. 不正确的权限

UNIX或Windows NT上文件权限的不当设置，可使一般用户以管理员权限运行某些程序或摧毁整个系统，当某个应用的权限设置不正确，就有可能遭受缓存区溢出攻击。

如果根用户或管理员拥有其他用户可写的文件，其他用户就可能修改文件的内容或应用，在管理员不知道的情况下给本地用户或远程用户分配管理员权限。

9. 病毒

病毒是将自身依附于其他软件的一组程序。病毒的目的是破坏计算机系统如重映射键盘、破坏硬盘中的内容或删除某种类型的文件。

有许多公司开发反病毒软件。反病毒软件的关键是找出病毒的特征码，并且每月更新病毒数据库。

在互联网上，最令人惊奇的是将任何问题都称为病毒。许多程序如 Netbus或Back Orifice实际上是特洛伊木马或后门，但有人也认为是病毒。虽然从技术上说，这些程序不属于病毒，但反病毒公司仍检查它们并将它们从系统中清除，以避免对系统造成损害。

10. 社会工程攻击

某些人随意传播它们的网络口令，使其他人可以访问网络服务。这是网络安全最难于克服的问题。

社会工程攻击也包括贿赂或欺骗以获取网络口令或重要信息。其他一些方法如伪装递送人员并试图访问网络等也属于该攻击范围。

39.2.2 加强网络安全

本节列出了一些用户可以加强其网络安全的方法。在考虑网络安全时，也需要将时间、人员等信息考虑在内。

1. 用户教育与再教育

无论你相不相信，用户的教育与再教育是加强网络安全的最重要措施。网络安全员需要确认所有雇员，无论新雇员还是老雇员，都必须熟悉网络安全策略并且信任它。如果每个雇员都能做到这一点并作为企业文化的一部分，安全管理员就可以实施安全口令、智能卡或利用密钥等安全措施，并要求雇员不共享关键的文件。

2. 入侵检测系统

这些系统检查不正常地导致系统崩溃的网络报文(如拒绝服务攻击)及使用特殊报文(如Windows OOB(Out of Bound，带外)报文等。它使用户可以跟踪可能对系统造成破坏的攻击。表39-3列出了部分可用的入侵检测系统。

表39-3 入侵检测系统

系 统	网 址
Network Flight Recorder	http://www.nfr.com
RealSecure	http://www.iss.net
NetProwler	http://www.axent.com

3. 入侵测试

入侵测试是通过已知的安全漏洞入侵自己的系统。这是确定系统安全性最有效的方式之一。然而这也是最有争议的方式，因为许多黑客也因受到许多公司的咨询而倍受推崇。即使用户不愿意使用推荐的软件，也应该运行一些测试工具以断定用户的网络没有明显的安全漏洞。

大量的软件支持入侵测试。许多站点还提供源代码供用户编译使用。也有部分软件来自商业安全公司。表39-4列出了部分可用的入侵测试软件。

表39-4 入侵测试软件

软 件	网 址
Internet Security Scanner	http://www.iss.net
SATAN	http://www.fish.com/SATAN
Nessus	http://www.nessus.org
Cybercop	http://www.nai.com

4. 文件完整性检查

判断系统是否受到攻击的基本方式之一是进行文件完整性检查。许多程序可以检查文件系统是否被修改或某些文件是否被改动。这可以帮助安全管理员发现什么文件被修改，是谁进行的修改，以判断系统是否遭受攻击。表 39-5列出了一些可用的完整性检查工具。

表39-5 文件完整性检查工具

软 件	网 址
Tripwire	http://www.tripwiresecurity.com
COPS	http://www.cs.purdue.edu/COAST
Tiger	http://www.cs.purdue.edu/COAST
System Scanner	http://www.iss.net

5. 日志审计

这是一种既简单又省事的检查攻击的方式，用户可以查看日志以发现奇怪的活动。不幸

的是这既耗时又枯燥，而且检查日志并不能证明系统的安全性。当入侵者获得了管理员权限后，他们可以对日志进行修改以隐藏踪迹。

39.3 应用配置

为了确保网络安全，用户必须正确配置网络应用。正确配置网络应用是保证网络安全的关键。配置网络时有以下几条准则：

- 只打开绝对必要的应用。
- 关闭所有不需要的应用。
- 尽可能加强应用的安全性。
- 网络是提供访问的。任何时候都必须开启一定的网络服务，一旦打开服务，就必然存在一定的风险。

39.3.1 Internet守护进程与/etc/inetd.conf

大多数UNIX系统上的应用都可在/etc/inetd.conf文件中关闭。/etc/inetd.conf文件控制所有由Internet超级守护进程启动的网络应用守护进程。

注意 第35章中包含inetd与/etc/inetd.conf文件的详细信息。

/etc/inetd.conf文件未经修改和配置时，如下所示：

```
# Version:      @(#)/etc/inetd.conf      3.10      05/27/93
#
# Authors:      Original taken from BSD UNIX 4.3/TAHOE.
#             Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org>
#
echo       stream       tcp       nowait       root       internal
echo       dgram       udp       wait       root       internal
discard       stream       tcp       nowait       root       internal
discard       dgram       udp       wait       root       internal
daytime       stream       tcp       nowait       root       internal
daytime       dgram       udp       wait       root       internal
chargen       stream       tcp       nowait       root       internal
chargen       dgram       udp       wait       root       internal
time       stream       tcp       nowait       root       internal
time       dgram       udp       wait       root       internal

# These are standard services.
#
ftp     stream   tcp    nowait root  /usr/sbin/tcpd   in.ftpd -l -a
telnet stream   tcp    nowait root  /usr/sbin/tcpd   in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
shell  stream   tcp    nowait    root    /usr/sbin/tcpd    in.rshd
login  stream   tcp    nowait    root    /usr/sbin/tcpd    in.rlogind
#exec    stream    tcp    nowait    root    /usr/sbin/tcpd    in.rexecd
#comsat dgram   udp    wait    root    /usr/sbin/tcpd    in.comsat
```

```
talk    dgram   udp   wait   root   /usr/sbin/tcpd      in.talkd
ntalk   dgram   udp   wait   root   /usr/sbin/tcpd      in.ntalkd
#dtalk   stream  tcp   waut   nobody   /usr/sbin/tcpd      in.dtalkd
#
# Pop and imap mail services et al
#
#pop-2   stream  tcp     nowait  root    /usr/sbin/tcpd      ipop2d
pop-3   stream  tcp     nowait  root    /usr/sbin/tcpd      ipop3d
imap    stream  tcp     nowait  root    /usr/sbin/tcpd      imapd
#
```

在上例中，任何没有注释符(#)的服务均由inetd启动。如果仅允许系统运行FTP及Telnet服务，新的/etc/inetd.conf文件如下：

```
# Version:      @(#)/etc/inetd.conf      3.10      05/27/93
#
# Authors:      Original taken from BSD UNIX 4.3/TAHOE.
#         Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org>
#
#echo          streamtcp   nowait   root   internal
#echo          dgramudp   wait          root   internal
#discard   streamtcp   nowait   root   internal
#discard   dgramudp   wait           root   internal
#daytime   streamtcp   nowait   root   internal
#daytime   dgramudp   wait           root   internal
#chargen   streamtcp   nowait   root   internal
#chargen   dgramudp   wait          root   internal
#time          streamtcp   nowait   root   internal
#time          dgramudp   wait          root   internal

# These are standard services.
#
ftp   stream   tcp   nowait   root   /usr/sbin/tcpd   in.ftpd -l -a
telnet   stream  tcp    nowait  root    /usr/sbin/tcpd   in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
#shell   stream   tcp   nowait   root   /usr/sbin/tcpd   in.rshd
#login   stream   tcp   nowait   root   /usr/sbin/tcpd   in.rlogind
#exec   stream   tcp   nowait   root   /usr/sbin/tcpd   in.rexecd
#comsat   dgram   udp   wait   root   /usr/sbin/tcpd   in.comsat
#talk   dgram   udp   wait   root   /usr/sbin/tcpd   in.talkd
#ntalk   dgram   udp   wait   root   /usr/sbin/tcpd   in.ntalkd
#dtalk   stream   tcp   waut   nobody   /usr/sbin/tcpd   in.dtalkd
#
# Pop and imap mail services et al
#
#pop-2   stream  tcp     nowait  root    /usr/sbin/tcpd   ipop2d
#pop-3   stream  tcp     nowait  root    /usr/sbin/tcpd   ipop3d
#imap    stream  tcp     nowait  root    /usr/sbin/tcpd   imapd
#
```

由于增加了注释符 (#)，仅有FTP和Telnet服务的守护进程被启动。所有不安全的服务如：echo、login、shell及finger等都被禁止，没有人可以使用这些服务连入用户主机。

警告 FTP及Telnet本身也不安全，它们使用明文传输口令，因此很容易被报文嗅探程序(sniffer)获得口令。

39.3.2 网络加密软件

确保TCP/IP传输安全的最有效方式是使用加密软件，其中包括安全套接字层 (SSL) —— 它加密http传输；Secure Shell(SSH) —— 它加密终端及X传输；虚拟私用网 (VPN) —— 它用于在Internet上建立两台远程主机的通道。

SSL与SSH可以用来为其他应用创建安全通道，如 POP3、IMAP及FTP。当用户使用SSL或SSH时，可使用公钥 (如RSA或DSA)进行认证，使用对称密钥 (DES、tDES或IDEA)进行加密。

VPN适用于在任何不安全的网络上建立安全传输。例如：文件共享可使用 VPN加强安全性，而不需从底层重新建立网络应用。

注意 SSH的更详细的信息在站点http://www.employees.org/~satch/ssh/faq。SSL的更多信息也在站点http://www.psych.psy.uq.oz.au/~ftp/Crypto/。上可找到。VPN的详细信息在站点：http://www.vpnc.org。

39.3.3 TCP Wrapper

大多数网络应用可使用TCP Wrapper加强其安全性。它跟踪及限制对 inetd运行的网络服务进行的访问。同时它可以审计跟踪和控制对特定网络服务如 finger、rsh和FTP等的访问。

为了使网络应用守护进程与 TCP Wrapper协同工作，用户必须正确安装和配置 TCP Wrapper。当通过TCP Wrapper运行TCP应用时，服务被TCP Wrapper隐藏。

安装TCP Wrapper时，先解压缩相应的压缩文件，然后运行 make命令：

```
# gzip -dc tcp_wrappers-7.6.tar.gz ¦ tar -xvf
# cd tcp_wrappers-7.6
# make
```

然后根据提示在系统环境下安装 TCP Wrapper。

安装完成后，用户需要配置 /etc/inetd.conf、/etc/hosts.deny及/etc/hosts.allow。TCP Wrapper用于访问控制的文件为 /etc/hosts.allow及/etc/hosts.deny。为使用TCP Wrapper，网络应用守护进程需要由tcpd运行。

为了增加一项隐藏的网络应用，可在 /etc/inetd.conf中增加一行，基本格式如下：

```
netappd     stream  tcp     nowait  root    /usr/sbin/tcpd  netappd
```

TCP Wrapper为每一个对netappd的请求创建一个Secure Shell(SH)。

假设仍采用前一个例子，仅运行FTP及Telnet服务。运行隐藏FTP守护进程，其格式由：

```
ftp   stream   tcp   nowait   root   /usr/sbin/in.ftpd   in.ftpd -l -a
```

改为：

```
ftp   stream   tcp   nowait   root   /usr/sbin/tcpd   in.ftpd -l -a
```

用户首先要确定/etc/hosts.deny设置为任何人都不能通过 TCP Wrappers应用访问系统。这样设置可以防止未经/etc/hosts.allow设置的主机访问用户的系统。为了防止除指定主机外的其余主机访问系统，可在/etc/hosts.deny中加入以下行：

```
ALL : ALL
```

在创建了/etc/hosts.deny后，用户需在/etc/hosts.allow中增加允许使用FTP服务的主机。在/etc/hosts.allow文件中添加访问FTP及Telnet服务的主机示例如下：

```
in.ftpd: example.com: allow
in.telnetd: example.com : allow
```

它将允许example.com访问这两项服务， /etc/hosts.allow及/etc/hosts.deny文件的基本格式如下：

```
deamons: clients: allow/deny
```

例如，如果用户不相信来自于 evil.org域中的主机，可在 /etc/hosts.deny文件中添加如下行：

```
in.fingerd: evil.org: deny
```

注意 TCP Wrapper的更详细信息在站点ftp://ftp.porcupine.org/pub/security 。

39.4 使用端口及可信端口

端口定义了UNIX和Windows NT的服务，用户必须确定端口定义的正确性。如果某人运行端口扫描及检查工具搜索打开的端口，通常会检查端口提供的服务类型。端口可能是后门或易遭受报文风暴的攻击，从而使系统可能遭到破坏。

NT及UNIX都定义了端口，这些端口需要仔细分析，并且可以在 /etc/inetd.conf文件中被注释符(#)取消定义。

39.4.1 防火墙

防火墙是网络的控制点，它决定何种类型的网络应用可以通过。大多数防火墙产品运行于TCP/IP网络，仅有少量产品运行于其他网络(如 IPX)。

防火墙同样提供日志功能，用户可通过日志查看哪些应用程序正在运行，哪些应用程序禁止通过网络。大多数防火墙可灵活定义出入防火墙的应用程序。

警告 即使防火墙允许不安全的连接如NFS或伯克利r系列的命令通过，并不表示用户应该使用这些服务。

防火墙的安全性取决于用户的使用。即使使用了防火墙，用户仍必须确定关闭所有不安全的应用程序，否则违背了使用防火墙的初衷。

39.4.2 包过滤

包过滤检查报文以确信报文的端口是否合法，对报文的内容不做检查。例如，路由器可使用包过滤功能仅允许特定端口的报文进出，而不检查报文的内容。因为报文过滤不检查报文的内容，因而其性能较高。

39.4.3 应用层网关

除了检查报文的端口外，还对报文的内容进行合法性检查，以判断它是否符合其连接的应用的要求。应用层网关检查报文中的所有部分，包括它连接的应用类型。因为应用层网关必须检查每个报文的所有信息，因而性能较包过滤低，这也是应用层网关未得到广泛应用的原因。

大多数应用层网关还提供别的功能，如支持 VPN、与入侵检测系统集成以及可对路由器进行管理等。

当应用层网关对加密报文如SSH或SSL应用的报文进行检查时，对其内容不做检查，此时，它与包过滤的功能类似。

39.4.4 其他应用的过滤

Checkpoint和Cisco PIX使用状态检测，它是包过滤与应用层网关的综合。也对报文的内容作检查，但不像应用层网关那样仔细。

注意 关于防火墙更详细的信息参见第18章。

39.5 一般安全事务

一旦用户建立了安全体系，必须注意以下几种经常发生的安全事务：用户帐号维护、审计和正确的系统配置。

39.5.1 用户帐号维护

网络的使用者具有流动性。因此，很容易忽略帐号与使用者的对应关系，即谁拥有系统的帐号以及帐号口令何时发生了变化。对于较大的公司，用户帐号的管理和维护是一项十分复杂的事务，用户的帐号必须定期更换 (尤其对于通用帐号)。

39.5.2 审计

审计是一项非常耗时而又重要的工作。它包括入侵测试用户的系统、检查系统和路由器的日志(如何人登录，或进行口令尝试 —— 无论成功或失败)。

39.5.3 正确的系统配置

另一项重要的任务是正确地配置系统。当网络中添加了许多系统时，需保证所有系统都添加了最新的补丁或升级到了最新的版本，以保证避免系统的安全隐患。

39.6 小结

当用户加强TCP/IP传输的安全性时，定义所需的 TCP/IP服务是非常重要的步骤。同时，用户也需定义控制点，在控制点上监视进 /出网络的报文，拒绝不符合要求的报文类型。

用户可以定义所需运行的网络服务。在定义网络服务时，必须配置正确，以确保系统的安全。

虽然大多数网络应用都不安全，但用户可以使用加密来保证其安全性：如 SSH(Secure Shell)、SSL(Secure Socket Layer)及VPN(虚拟私用网)，它可以防止某人窃听用户的会话，保证传输的安全性。