Firewall User's Overview

Introduction

The network you are using is connected to the Internet, protected with a network "firewall". The firewall blocks all traffic between the Internet and the protected network, but still permits users on the protected network to carry out certain basic operations. These are:

- Sending electronic mail (e-mail)
- File transfer using the FTP program
- Remote terminal sessions using the TELNET program

In order to use these services, you must be logged into a computer that is running TCP/IP on the protected network. Electronic mail requires no extra action on the part of the user other than specifying a proper Internet-style address. For FTP and TELNET, users first connect to a *proxy* server running on the firewall, which will in turn connect them to the destination system.

Using FTP

When connecting to the FTP proxy, you issue the command as if you wished to FTP files with the firewall system itself:

```
host%  ftp gatekeeper.mydomain.domain
```

Once you are connected to the FTP proxy, and you are prompted for your username, give the username and hostname of the system you wish to transder files with, in the form of *username@hostname*. If you don't know the hostname, and only have the TCP/IP network address, you can also use *username@IP-address*. For example, if you wish to log in as "anonymous" on node "Ftp.Uu.Net", give your username as "anonymous@ftp.uu.net."

```
host% ftp gatekeeper.company.com
Connected to gatekeeper.company.com
220 gatekeeper FTP proxy (Version 1.0 stable) ready.
Name (gatekeeper:you): anonymous@ftp.uu.net
331-(----GATEWAY CONNECTED TO ftp.uu.net----)
331-(220 ftp.uu.net FTP server (SunOS 4.1) ready.)
```

```
331 Guest login ok, send ident as password.
Password: ######
230 Guest login ok, access restrictions apply.
ftp> dir
200 PORT command successful.
(...etc.)
```

Once you are connected via the proxy and you see the "GATEWAY CONNECTED TO" message, any subsequent commands you enter are forwarded to the destination system by the proxy. If you type a password incorrectly, after you are connected, you no longer need to use the *user@host* form, just act as if the proxy is not there. After connecting, any normal FTP commands can be issued. For details on the other options to the version of FTP on your system, consult the manual.

If you are using FTP from *outside* of your security perimeter, you may have to authenticate yourself to the proxy before you are allowed to transfer files. To authenticate, the FTP user command is used twice in sequence:

```
outside.host%> ftp gatekeeper.company.com
Connected to gatekeeper.company.com.
220-Before using the proxy you must first authenticate
220 gatekeeper FTP proxy (Version 1.0 stable) ready.
Name (gatekeeper.company.com:you):
331 SNK Challenge "90280":
Password: ##########
230 User authenticated to proxy
ftp> user you@somebox
331-(----GATEWAY CONNECTED TO somebox----)
331-(220 somebox FTP server ready.)
331 Password required for you.
Password: ##########
230 User you logged in.
ftp>
```

The first invocation of the "user" command (done automatically by the FTP client) authenticates you to the proxy. The second is used to initiate the connection to an FTP server within the security perimeter.

Using TELNET

To use the TELNET proxy, simply telnet to the firewall system as if you wished to log into it. There will be a short pause, and you will be prompted with a command prompt for the proxy. At the command prompt, you may specify the host you wish to connect with, by typing "*connect hostname*" or "*c hostname*." If you prefer to give a TCP/IP address instead of a host name, you may do so. Once you have entered the name of the host to connect to, the proxy will connect you to that system, and its login prompt should appear. If the system is down or is unreachable, the proxy will inform you of this fact, and

you may quit using the "*quit*" command. For example, if you wish to login to a system named "Foo.Baz.Com" you might employ the proxy as follows:

```
host% telnet gatekeeper.company.com
Trying 192.33.112.117 ...
Connected to gatekeeper.company.com.
Escape character is '^]'.
gatekeeper telnet proxy (Version V1.0) ready:
tn-gw-> c foo.baz.com

HP-UX foo A.09.01 A 9000/710 (ttys1)

login: you
Password: ######
Please wait...checking for disk quotas
unknown mode: crt
foo->
(...etc.)
```

When you logout from the destination system, the proxy will automatically disconnect you and return to a command prompt on your local system.

Using Rlogin

For communicating with remote systems that support the rlogin protocol, an rlogin proxy is provided. One advantage of the rlogin proxy is that it eliminates the need to authenticate a user twice. In order to use the rlogin proxy, the firewall bastion host must be prepared to accept rlogin connections. If the rlogin proxy is invoked with no user name and destination, it presents the user with a command menu similar to the telnet proxy's:

```
%-> rlogin gatekeeper
rlogin-gw-> ?
Valid commands are: (unique abbreviations may be used)
   connect hostname
   help/?
   quit/exit
   password
rlogin-gw-> c somebox.someplace.org
Trying you@55.55.55.55...
Password:
Last login: Mon Oct 25 21:54:33 from homebox.someplace.else
SomeOS Release 4.1.Wed Apr 14 07:21:50 EDT 1993

you have new mail
somebox%
```

In this example, the rlogin server on "somebox.someplace.org" prompted for a password, since the proxy server "gatekeeper" was not in the user's *.rhosts* file. If a username and hostname is specified, the rlogin proxy will automatically reconnect to the specified remote system. For example:

```
%-> rlogin gatekeeper -l you@somebox.someplace.org
Trying you@55.55.55.55...
Last login: Mon Oct 25 21:54:33 from homebox.someplace.else
SomeOS Release 4.1.Wed Apr 14 07:21:50 EDT 1993

you have new mail
somebox%
```

If using the rlogin proxy from outside the perimeter, it may stop and require authentication before proceeding:

```
%-> rlogin gatekeeper.your.org -l you@homebox
Username: you
SNK Challenge "32015": 32256239
Login Accepted
Trying you@32.33.22.11...
Last login: Mon Oct 25 21:23:53 from some.place
SomeOS Release 4.1.3 (homebox) #3: Mon Jun 21
You have new mail.
homebox->
```

Note that some networks block rlogin protocol traffic in or out in such a manner than the rlogin proxy may not be useable. In such circumstances, rely on the telnet proxy instead.

Changing Passwords via the Proxies

Users who rely on authentication protocols that have passwords or changeable PINs may reset their passwords using built-in capabilities in the proxies. Both the telnet and rlogin proxies support changing passwords at the command line, if connected to from systems within the security perimeter. To change your password, connect to the proxy and issue the "password" command as in this example:

```
%-> telnet gatekeeper.your.org
Trying 192.33.112.117 ...
Connected to gatekeeper.
Escape character is '^]'.
otter telnet proxy (Version V1.0) ready:
tn-gw-> pass
Changing passwords
Enter Username: you
Skey Challenge "s/key 665 ot572005": JAR ADA ANA DRUM GLEN GAUR
New Password: #####
Repeat New Password: #####
ID mjr s/key is 666 ot572006
tn-gw-> quit
Disconnecting...
Connection closed by foreign host.
%->
```

In the example above, the user resets their S/Key secret key using the telnet proxy. It is important to remember ***never*** to reset the password from a system that may be compromised, or a system that is on an untrusted network. The firewall administrator has the ability to limit the hosts from which users may change their passwords. If you attempt to change your password and cannot, contact your administrator to find out from what hosts password changing is permitted.