Communications between the ILL and the outside Internet

Based on documentation from F. Pinet
Last modification 24th March 2006, (R. Ghosh)

The ILL/ESRF/EMBL joint site network is protected from access from the Internet by a "firewall" computer managed by the ESRF which filters communications in both directions. Most internal communications pass via proxies which can either be configured automatically on systems using DHCP (visitor network/wireless network), ticking automatic proxy configuration in the network connections, or, for fixed IP addresses using the proxy configuration file http://proxy.ill.fr/proxy.pac The default port number for proxies at the ILL is 8888.
The following procedures for connecting with or exchanging data between the ILL and a computer connected outside the site are:

1. Mail
2. Telnet
3. SSH, Xwindow, and sftp
4. FTP
5. WWW
6. Private access: Callback and VPN

---

1. Mail

1.1. Sending Mail

Your addressee in the ILL has an Email address in the form: *username@ill.fr*
The username is usually the person's name. Most of the users also have an alias like: *forename.surname@ill.fr*
The ILL staff phone book including email addresses is available on our website: http://www.ill.fr.

Mail is subject to the following filters (both to and from the site):

- **Anti-spam** (Unsolicited Commercial Email)
  Mail sent from known spam-sites or with a badly formed "from" field are rejected.
- **Antivirus**
  All mail is checked by an antivirus program. If a virus is found, the addressee receives the original mail with a warning message and, if possible, the "disinfected" attachment. If decontamination is impossible, the attachment is removed from the mail. The sender is also warned of the presence of the virus in the mail.
- **Size limited to 10 Mb**
  Note:
  . An attached file occupies about 110% of its nominal size.
  . Mail passes through several relays outside our site; some relays may have a lower limit than ours.

1.2. Receiving Mail

Web Mail Server mailout.ill.fr
Users with ILL accounts may log on this machine and receive their mail and send replies over an encrypted https web-browser interface from inside or outside the ILL. The home page http://mailout.ill.fr has full information.
An alternative when on-site is that you activate a *forward* to an external computer, then consult your copied Emails off-site.
To do this, direct your web browser to http://mail.ill.fr from the ILL, then click on the "MailMaster" button.
Note: You are advised against permanently keeping this forward active. Your mailbox risks being blocked or being intercepted.

---

2. Telnet

Access using the telnet protocol was closed at the end of February 2003.
Ssh offers the same possibilities (and more) with distinctly better security.
Only use of ssh is described here.

---

3. ssh, Xwindow, and sftp

- ssh: secure-shell connection in terminal mode (as a telnet replacement).
- Xwindow: interactive graphical windows are carried (encrypted) across the network.
- sftp: secure ftp allows file transfer with an ssh connection.
  Usage is similar to ftp though it does not use the ftp protocol.

3.1. Basic functions

To connect with ssh to the ILL, you must have:
- An account on our site entry computer: *grill.ill.fr*.
  (The "Local Contact's signature is required when visitors ask to be registered.)
- A recent ssh program, because only version 2 of the protocol is accepted.

Connection parameters (for ssh and sftp):

- Host : *firewall.ill.fr*
- Port : **5023** Note: This is NOT the default port (22)
- Login : Your account name on ***grill***
- Password : Your password on ***grill***

!! Warning !! : There is an automatic proxy between the firewall port number 5023 and *grill* hence your login is effectively directly on *grill*
At the first connection, the ssh/sftp program will ask you to validate the server's key, please answer yes.

Once connected to *grill*:
- With ssh: you can connect other systems at the ILL with telnet (or sometimes with ssh).
- With sftp: you can exchange files with *grill* but not necessarily with other workstations unless the sftpd client program is running. To transfer your files between *grill* and another ILL workstation, please connect to *grill* with ssh then use the ftp command. NOTE: your data should not remain on *grill*; old data will be deleted without notice.

Xwindow programs
It is possible to run Xwindow programs on a system inside the ILL from an external system, providing that external system has an Xwindow server to treat the graphics messages. Unix workstations have an ssh and X compatible with this; the public CYGWIN package, providing a unix environment on PCs also provides ssh and an Xwindow server. Commercial communications packages like Hummingbird Exceed, StarNet Xwin-32, etc., also provide an Xserver linked to ssh.
The external machine is logged into the ILL in two stages, transferring its DISPLAY identity with the command:
$ ssh -X -p 5023 extenal_user@firewall.ill.fr
Password (on grill) :
.. logs into grill, and then, for example, to chania
ssh -X illusername@chania
Password (on chania)

Then standard programs (xclock etc) should bring up a window on the external system.

Note If the user logs in to one of the shared visitor accounts, e.g. d22, which ask for his name to switch to his own directory, it is necessary to issue the following **additional** command before running Xwindow applications:

$ setenv XAUTHORITY ../../.Xauthority

to ensure that the X-authorisation, established on login, in the initial "home" directory, is correctly invoked after changing to the user's own directory.

3.2. ssh clients tested and validated

The following program list is limited. Any ssh programs which use the protocol version 2 should work. These programs were selected because they all implement some advanced ssh features (port selection and X11 tunnelling).

3.2.1. PC under Windows (any version)

Two programs are proposed. Their respective advantages are:
- Putty is free and does not need to be installed, so you can easily take it around with you on a floppy disk or usb disk.
- SSH WinSecureShell is somewhat more complete and the use of sftp is easier.

*** Putty**

Free executables: http://www.chiark.greenend.org.uk/~sgtatham/putty/
Download putty.exe (Ssh client) and psftp.exe (sftp client).

Simple connection in terminal mode:
- Run the downloaded program : putty.exe (No installation is needed)
- Check the protocol option : SSH (NOTE you must do this at the first use)
  . Host name : *firewall.ill.fr*
  . Port : 5023
- Click on: Open
- then logon to *grill*

Connection with sftp:
The psftp program works in a DOS window like the basic ftp Windows command. Type:
psftp -P 5023 *your_username_on_grill@firewall.ill.fr*

*** SSH WinSecure Shell**

Download: http://www.ssh.com (free for "non-profit users")

Simple connection in terminal mode:
- Install the program with all parameters set to defaults
- Run the installed program: SSH Secure Shell Client
- Click on: Quick Connect
  . Host Name : *firewall.ill.fr*
  . User Name : your username on *grill*
  . Port Number : 5023
- Click on: Connect

Transfers with sftp:
- Please connect in terminal mode, then go to the menu: Windows->New File Transfer.
- Alternatively: connect directly with the program "SSH Secure File Transfer Client".

3.2.2. Unix, Linux, and Mac OS X

* **OpenSSH** (from release 2.9)

Source: http://www.openssh.org (free, often supplied with your OS though package may require selective installation)

This package contains several client programs and a sshd server, which allows remote clients to connect. These commands have no graphic interface, they should be executed from a terminal window like xterm.

Simple connection in terminal mode:
ssh -p 5023 *your_username_on_grill@firewall.ill.fr*

See above for example of passing the Xwindow identification ssh -X

File transfers with Sftp:
sftp -oPort=5023 *your_username_on_grill@firewall.ill.fr*

3.2.3. Mac OS 9 and older

*** MacSSH**

Download: http://www.macssh.com (free)

Simple connection in terminal mode:
- Run the MacSSH program
- Go to the menu: Favorites - > Edit Favorites
- Click on: New
  . Alias: Grill thru out (you can put what you want here)
  . Host name: *firewall.ill.fr*
  . Port: 5023
- Click on: OK, several times to close all windows
- Go to the menu: Favorites - > Grill thru out (previously created alias)

File Transfers with sftp:
Not possible: unfortunately this program does not include an sftp client.

---

4. FTP

The FTP protocol is blocked for outside requests to the site; it is open for any operations initiated within the site. File transfers with sftp are possible with the same conditions as Ssh (See previous paragraph).

NOTE: to exchange files with an ILL computer from outside our site, You MUST have:
- either an account on *grill* (for all methods);
- or a contact in the ILL who will do the transfer for you (excluding 4.3.).

4.1. The easiest way, if you have a local ftp server, and no home firewall

1/ If you have an account on *grill*, please connect to the ILL using ssh, then to the internal computer
2/ Do your ftp transfer from the internal computer to your own local FTP server.

4.2. The easiest way, if you have a local ssh server

1/ If you have an account on Grill, please connect with ssh to the ILL
2/ Do an sftp transfer from the internal computer to your external ssh server.

4.3. sftp with *grill*

This method is possible only if you have an account on *grill*. You will have to connect with Ssh and use Sftp on this computer.

Please transfer yout files in two steps :
- between your computer and *grill* : transfer using sftp from your computer;
- between *grill* and another ILL workstation : then use the ftp command on *grill*.

NOTE: your data should not remain on *grill*; old data will be deleted without warning.

4.4. Ftp on ftp.ill.fr

We provide a temporary storage area on a FTP server with general access:
Host : *ftp.ill.fr*
Login : *transit*
Password: *<A demander au HelpDesk>*

ftp is directed to a 'transit' directory which is not protected. If you connect to this server as *'anonymous'* (without password) you will have only have read-access to this area.

Method to exchange files with the ILL with this server:
- Ask your contact (or yourself using ssh) to put or get your files in the 'transit' area of ftp.ill.fr.
- logout and locally fetch your files with a ftp connection to ftp.ill.fr.

N.B.: files in the 'transit' area are automatically deleted after a short period.

---

5. WWW

It is NOT possible to access the ILL internal web servers from the outside.

External web servers:

http://www.ill.fr	ILL official web site
http://barns.ill.fr	Experiment-data treatment/Access to Archived data
http://mailout.ill.fr	Accessing mail forwarded with mailmaster
http://vitraill.ill.fr	Proposal and report submission

Definition of Network Proxy Server within the ILL

To allow internal WWW requests to transit the firewall, proxy names allow requests to be automatically redirected. Proxies are set up for each type of service, http (normal web browsing), gopher, wais etc. To simplify configuration of these proxies, and allow changes to be managed centrally, web browsers should have their network configurations modified to "automatic proxy configuration" and the configuration then identified as http://proxy.ill.fr/proxy.pac This is usually found under Network Preferences, or Internet Options.

If this is not defined then access to the external Internet is blocked.

The proxies so defined include a cache web server to hold temporary copies of files retrieved from Internet for a set time, A second request returns this shared temporary copy rather than fetching the original again. This reduces the network load, and gives a much more rapid response.

The actual external Internet access is made by the proxy server, but routed avoiding the firewall.

Note: Remote websites often interrogate the user's computer for its network identification. Local Internet addresses cannot be seen from outside. The proxy intercepts these requests and hence allows our internal systems to be represented as itself, satisfying the remote site.

A description of the methods of configuring browsers to access the WWW from ILL is given in the ESRF Firewall Manager's Document.

---

6. Access for ILL Staff

The following means allow a more general access to the ILL, requiring specific authorisation.

6.1 Callback

A system of connection by modem is available.
A complete documentation (on-site) is available from the Computer Service.

6.2 VPN - Virtual Private Network

A connection system by VPN, which will allow a full access to the site from a secure computer on Internet, is now operational. Registered users who wish to use this new service should contact the Helpdesk.

Last Modified: Thu Aug 2 14:28:21 2007