Livermore Software Laboratories, Inc. (LSLI™)

P.O. Box 73228 Houston, TX 77273-3228
Phone: 1-800-240-LSLI (5754), or 1-713-379-5754; FAX: 1-713-379-5225;
e-mail: portusinfo@gw.lsli.com

PORTUS™ Announcement Letter

Introduction: LSLI's PORTUS secure firewall system was developed at the IBM Thomas J. Watson Research Center (WRC) to secure its private network when connected to Internet. This firewall has been in production since 1988 and has received multiple enhancements over the years. PORTUS is based on the current version of the WRC secure firewall and represents the state of the art in securing a network from unauthorized intrusions.

PORTUS was named after the ancient Roman deity, Portunus, who protected doors, gateways and harbors from intruders. Portunus was often portrayed holding a key by a gateway, just as our product requires an external user to hold a key to enter the network gateway.

Objectives: PORTUS is designed to repel the most sophisticated attacks of determined super crackers residing on the Internet. For example, on February 4, 1994, the Computer Emergency Response Team (CERT) alerted Internet users to a Trojan Horse that had compromised tens of thousands of user accounts and passwords. PORTUS can defend against such sophisticated attacks, and many others.

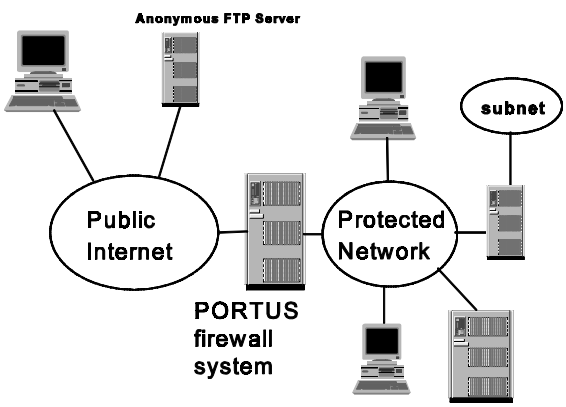

Figure 1. Connecting Public Internet to Private Network

The PORTUS firewall system provides access from a secure internal network to an unsecured external network without undue hassle. It provides Telnet and File Transfer Protocol (FTP) services to and from the outside world for authorized individuals without compromising network security(Figure 1). Authorized users can telnet from the unsecured external network to systems on the secure network. PORTUS uses a smart card to positively identify users coming from the unsecured network. PORTUS supports electronic mail without exposing an organization to potential security loopholes. With PORTUS an organization can gain all the benefits of a connection to Internet without undue risk.

PORTUS can also be used to protect portions of an organization's internal network from their general network. For example, a research department may want to limit access to their confidential data within their company (Figure 2).

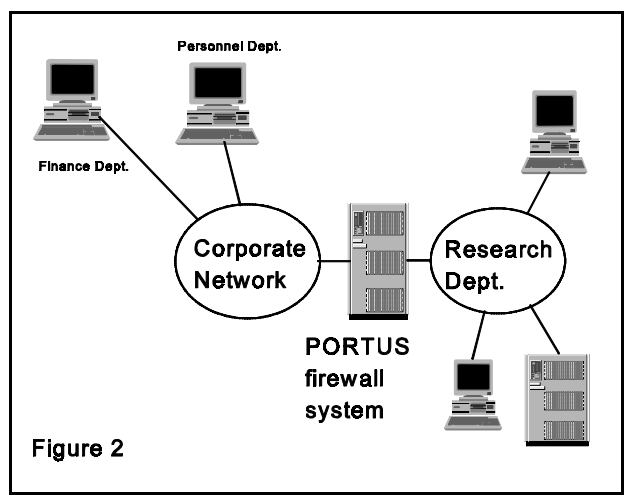

Figure 2

Functions: PORTUS provides a **secure gateway** to a heterogeneous private network with the following functions:

© LSLI 1994

1. PORTUS turns off IP packet forwarding.

This greatly enhances security by controlling use of protocols and hiding internal network structure.

2. PORTUS uses static routing instead of dynamic routing.

This defeats routing attacks and keeps the firewall system from advertising internal node names.

3. PORTUS only allows FTP from inside the protected network.

Use of FTP from the outside network is considered too dangerous so it is restricted to users coming from a protected system. FTP was modified to listen to a single port, and will only accept requests from the protected network.

4. PORTUS allows outbound telnet.

Internal users first login to the firewall system then telnet to their intended destination.

5. PORTUS uses a strong authentication process for incoming users to control access to the internal network.

It is clear that use of a user id and a password does not provide sufficient protection for users coming from unsecured networks. Therefore, authentication is provided with the SecureNet Key[1] authentication system, or the Kripto Card. This challenge-response system defeats eavesdroppers who might have picked up valid user ids and passwords from the network. Challenges and valid responses change with every login attempt. Without access to the key it's virtually impossible to break in.

6. PORTUS assigns different shells for a user depending on whether the user is coming from the outside network or from the protected network.

PORTUS automatically determines if the user is coming from the protected or public network and assigns the appropriate shell. External users are assigned restricted shells. This prevents the use of functions which are too dangerous to use when coming from the outside. If the user is coming from the protected network then they can safely be given access to standard shells.

Restricted shells are preassigned by the administrator to allow functions such as telnet, passwd, finger and exit. All other commands are rejected. Use of commands and protocols that are unsafe when coming from the outside are not permitted.

7. Restricted shells can be assigned to each user, or group of users, to provide different levels of control for incoming and outgoing traffic.

The system administrator has nearly infinite variability to configure user shells on the PORTUS firewall system.

8. Incoming users can be directed to a specific node.

The system administrator can hard code command arguments in a user's restricted shell. This can be used to direct an external user to a specific system when they enter the telnet command.

9. PORTUS has eliminated the "open" sub command of telnet.

This prevents outside telnet users from escaping to the command level and gaining access to unauthorized nodes.

10. PORTUS uses a new telnet daemon.

The new telnet daemon prevents a cracker from forging a reverse address lookup thus fooling the system into sending packets to the wrong node.

11. Access to the firewall gateway can be controlled to limit exposure.

---

[1] The SecureNet Keys are available from Digital Pathways, 201 Ravendale Dr., Mt. View, CA. 94043. The cost per card in January 1994 was $60.

© LSLI 1994

Only internal users who need to access the outside network and external users who need access to the internal network need user id and passwords on the PORTUS firewall system. Some users can be given access from the protected network, but no access from the external network. Access is controlled on a need to use basis.

12. PORTUS supports the Simple Mail Transfer Protocol (SMTP) used on the Internet.

PORTUS runs sendmail, which provides a flexible mechanism for configuring electronic mail.

The PORTUS firewall system can be configured so that all outgoing mail appears to come from the firewall machine. Sendmail can modify out-bound header records to conceal internal system names. This serves to hide the structure of the internal network. It also provides a consistent external e-mail address if the user moves to another system.

All incoming mail can be routed to an internal mail hub. An aliases file combined with Mail Exchange (MX) records can be used to automatically route in-bound mail to the appropriate user id on the desired system. Thus, external users do not need to know the name of internal systems to send mail to a user.

The system controls who can receive external mail through the use of aliases and MX records.

13. On the PORTUS firewall system:

- The protected ***network administrator*** maintains control of **root** access;
- The **root** user can only login at the console and it is impossible to login as root from the unprotected network;
- Will not allow the "r" commands (rsh, rlogin, rexecd, rwho);
- **X-Window** applications that access systems on the unprotected network must run on the PORTUS firewall to avoid a major security exposure (applications such as xarchie, xgopher or xmosaic can be run on the gateway with output displayed on the user's workstation).
- The encrypted passwords are stored in a directory accessible only by root. This defeats password cracking programs.

14. The PORTUS firewall system provides separate domain name servers for the unprotected and protected networks.

PORTUS provides Internet Name Services (DNS) to the outside network for systems on the protected network.

PORTUS provides a separate internal name server to further enhance security. This prevents a DNS attacker from using the zone transfer command (AXFR) to obtain a list of every host name and address in the domain of the protected network.

15. The PORTUS firewall system automatically logs successful logins, and failed login attempts for Telnet and FTP.

Since PORTUS deals with security, it is important to know who is logging in, who is using FTP, and who is trying to get in without permission. The system can tell you who logged in, from what IP address, and how long they were on. You can also see failed login attempts via telnet and FTP. This is useful for determining if someone is attacking your system.

Additional login information can be collected by running the syslog daemon (syslogd). This facility can be used to capture the date and time of unauthorized penetration attempts including the IP address of the node which initiated the attack.

PORTUS can also log events on another system, and send messages to the system administrator.

16. The PORTUS system exceeds the requirements for Class C2 Security.

The National Computer Security Center (NCSC) , a branch of the National Security Agency (NSA), has

developed stringent criteria for evaluating computer systems. The current version of AIX exceeds the requirements for a class C2 system. PORTUS builds upon AIX and further improves its security.

17. PORTUS allows special applications to be developed which provide external users access to protected systems.

Applications that run on protected systems need special modifications to allow authorized external users. These modifications allow the application to use the internal nameserver provided with PORTUS. Source code is available to assist with the modifications.

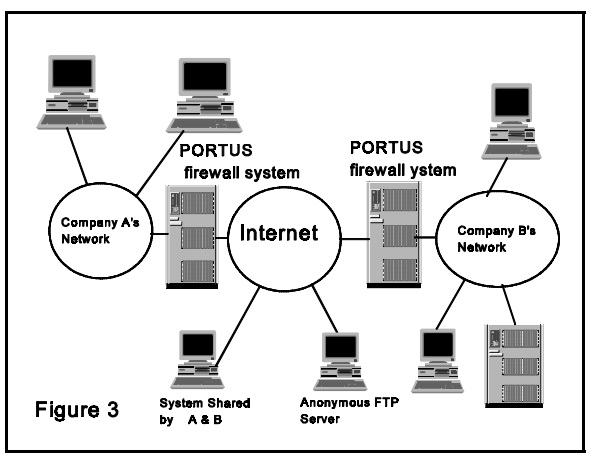

Figure 3

For reasons of security, PORTUS does not allow FTP to access a secured network from the outside. For example, if company A and company B want to use FTP to send files between their respective secure networks they must use a system external to both networks to act as a store and forward system (Figure 3). This can be done using either an "Anonymous FTP server" or by using a system that has User ids and passwords shared by the two companies. The use of **"Anonymous FTP" servers** to share proprietary data between two or more companies, is **unsafe**. The second solution, because it relies on using shared id's and passwords, is significantly more secure than an anonymous FTP server. Data on the store and forward system can be removed as soon as the protected system has received the file. Thus, the data will reside on the external system for only a short time.

Hardware Requirements:
The PORTUS firewall system requires a **dedicated** IBM RS/6000 with: two network adapters, a minimum of 16 MB of RAM and a minimum 540 MB disk drive. The size of the RS/6000 required to support PORTUS depends on the expected number of concurrent users logged in, FTP traffic, and the volume of electronic mail handled by the system, and the requirements of other applications such as xmosaic.

PORTUS requires a dual-homed system with one network interface connected to the unprotected network and the second interface connected to the protected network. Currently supported network interfaces include **any combination** of those supported by TCP/IP and available on an RS/6000 (eg. Token Ring, Ethernet, FDDI, etc.)

Software Requirements: PORTUS runs on the current version of AIX, (AIX 3.2.5). The system can be configured with the AIX feature to support a maximum of 8, 16, 32, 64, and more users. The system should also have AIX/Windows installed if motif based applications such as: IBM's SMIT, xarchie, xgopher, or xmosiac are to be run.

Documentation: Three documents are shipped with the PORTUS system; a PORTUS General Information Manual, a PORTUS User's Guide, and a PORTUS Installation and Administration Guide.

Product Support: PORTUS is backed by a system designed to provide fast and courteous service. Support personnel are available Monday through Friday from 8:00 am to 5:00 pm Central Time.

AIX and IBM are registered trademarks of International Business Machines Corporation. LSLI and PORTUS are trademarks of Livermore Software Laboratories, Inc.