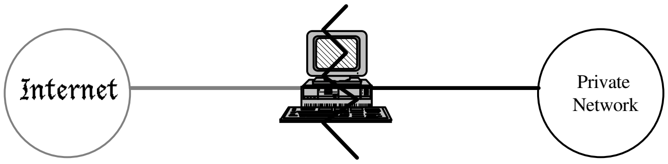
TIS Firewall Toolkit

Building Blocks for Secure Internetwork Connectivity



Three Methods

1. **Roll your own.** A talented network security consultant uses her or his own bag of tricks as well as well-tested publicly available software and methods to build a firewall. If you have the in-house talent, and like to do your own engineering and maintenance, this is a good way to go.

2. **Black Box.** This is often purchased from a firewall vendor or a consultant. Components are pre-built and then customized for your network. The components are easy to understand, upgrade, put together, and take apart. The methods and mechanisms are often proprietary and not available for public examination. If you want to put your trust completely in the experts, and in one company, this is a good path to take. There is comfort in numbers.

3. **Crystal Box.** Source code of components, security analysis, documentation, and testing available for examination, addition, enhancement, all without compromising security. Not "security through obscurity," but, rather, "security through strong practices and expert testing." This method allows you to use in-house experts, or to develop them with the help of someone outside. It also allows you to test and analyze the software and hardware components independently, using your own experts, or those you hire independently. With a crystal box, you get the best of both of the other methods.

Two Philosophies

1. **"That which is not expressly prohibited is permitted."** Least intrusive to the user. This method requires that the security manager anticipate possible attacks and prevent them ahead of time. It is usually implemented with rules in routers. As new attack methods are uncovered, the Site Security Policy implementation is modified along with the firewall to protect against these attacks. This is the classic arms race approach.

2. **"That which is not expressly permitted is prohibited."** Presents the minimum zone of attack to "the outside." Requires that the security manager specifically add services through protected means, based on user business requirements in conjunction with the Site Security Policy. This can also be implemented using rules in routers, but often employs a "Bastion Host" to provide secure access to Internet services. This is the conservative approach. Some call it paranoid. We call it smart.

One Solution

The TIS Firewall Toolkit. A crystal box. Conservative. Minimalist. Documented and tested. Expandable. Available as a kit in source code form. Configuration and installation support available. For further information please send electronic mail to *netsec@TIS.COM*, call (301) 854–6889, Fax to (301) 854–5363, or send postal mail to Trusted Information Systems, Inc., ATTN: Network Security, 3060 Washington Road, Glenwood, MD 21738.

Trusted Information Systems, Inc., 09/17/93