Network Security Management with Firewalls

Stephen P. Cooper
Advanced Security Projects
Computer Security Technology Center
Lawrence Livermore National Laboratory
Email: SPCooper@LLNL.GOV

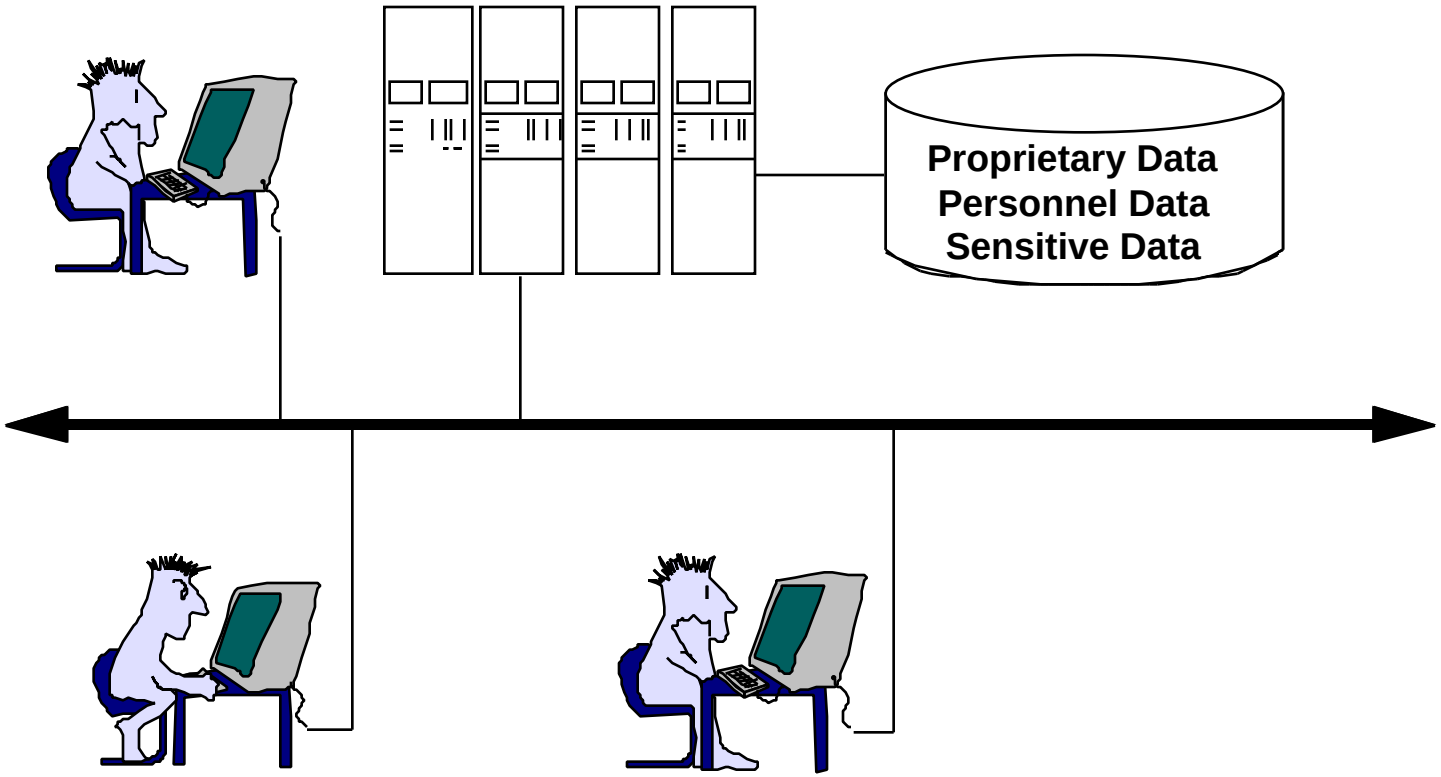
Computer Security Practitioners Conference

February 7, 1996

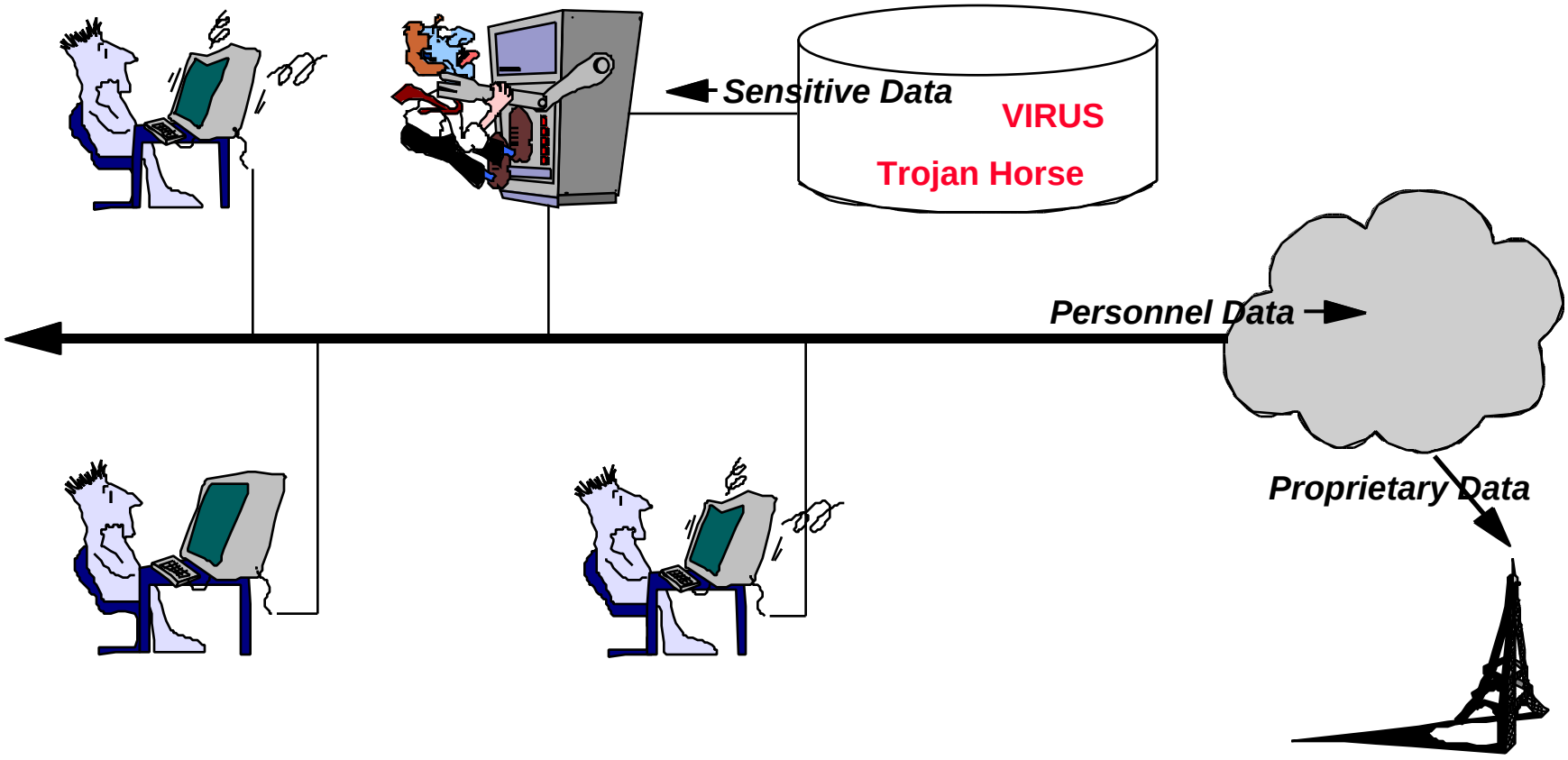
UCRL-MI-123352

Work performed under the auspices of the U.S. Department of Energy by
Lawrence Livermore National Laboratory under Contract W-7405-ENG-48.

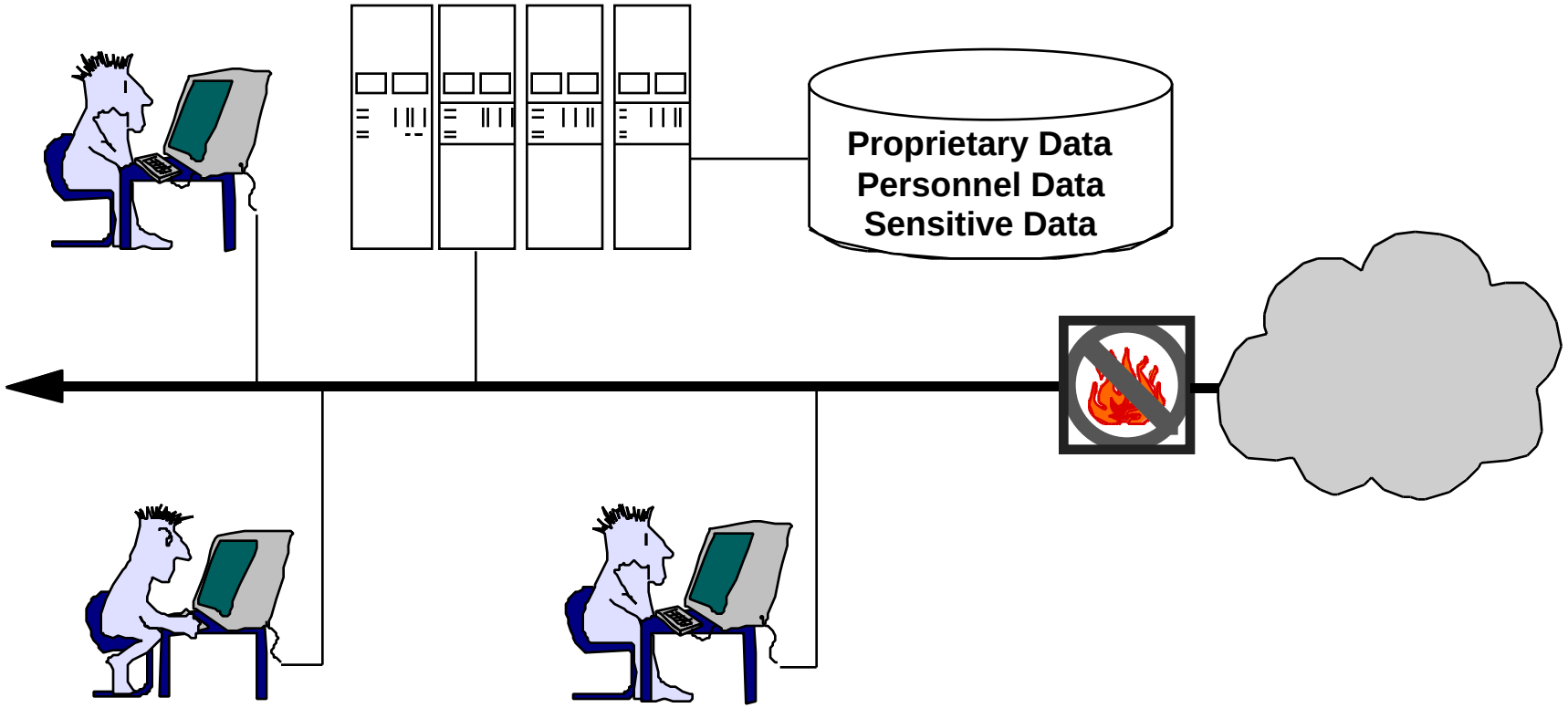
This is your network...



This is your network on the Internet



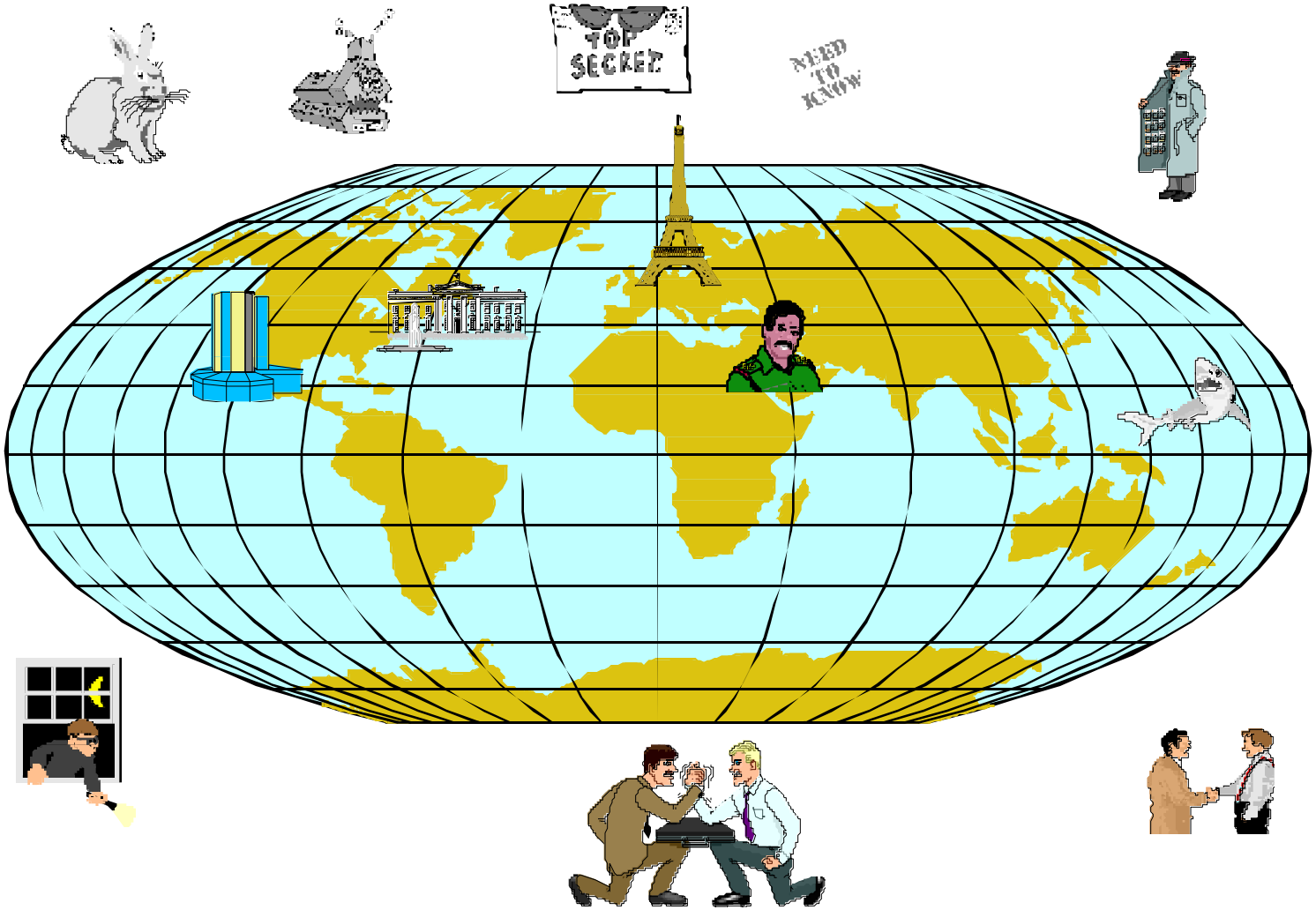
Unless you have a Firewall



Why a firewall?

- **You have information and resources that need protection.**
- **You have a need to connect to a network that has a different view of the world.**
- **Strong host-based security is too costly or difficult.**

On the WWW, everyone is a neighbor

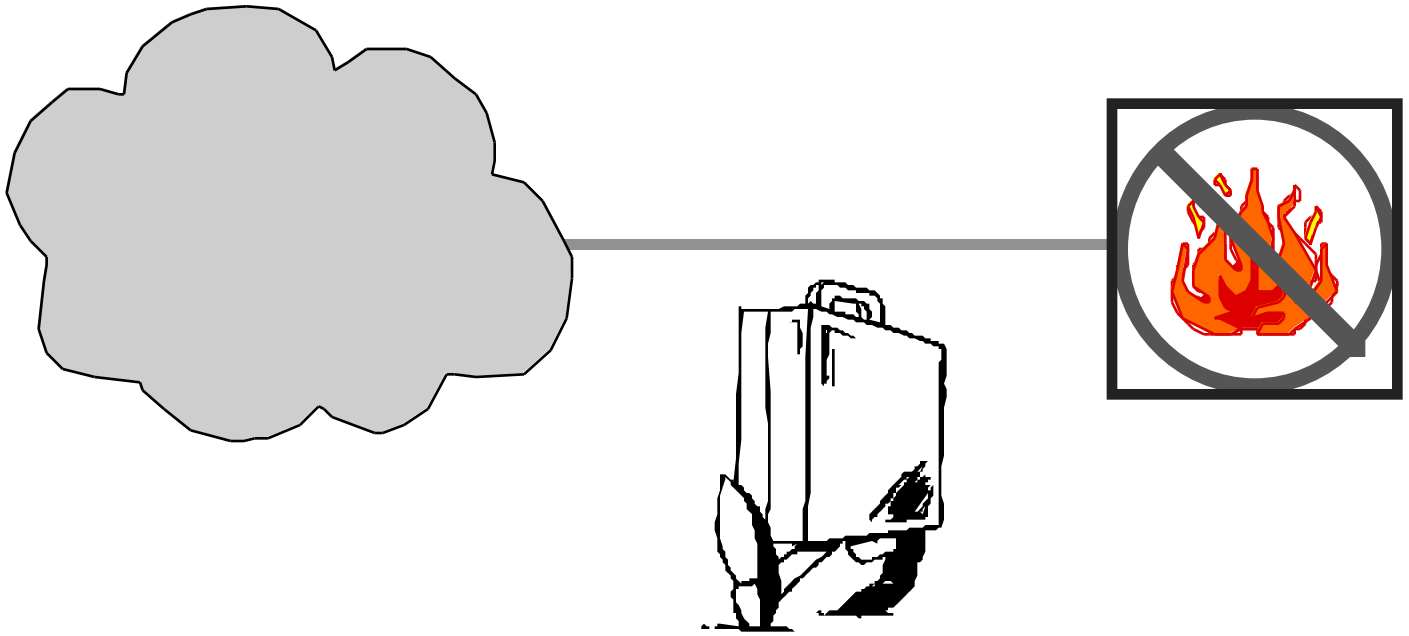


A Firewall is...

- **A gateway between a trusted network and a less trusted one.**
- **An enforcer of security policy.**
- **A system designed to:**
  - **Control external access to company data and resources.**
  - **Control internal access to Internet systems and services.**
  - **Provide a security and monitoring choke point.**

... or in a nutshell

- **A firewall is a tool for managing and controlling traffic that crosses a network "boundary."**

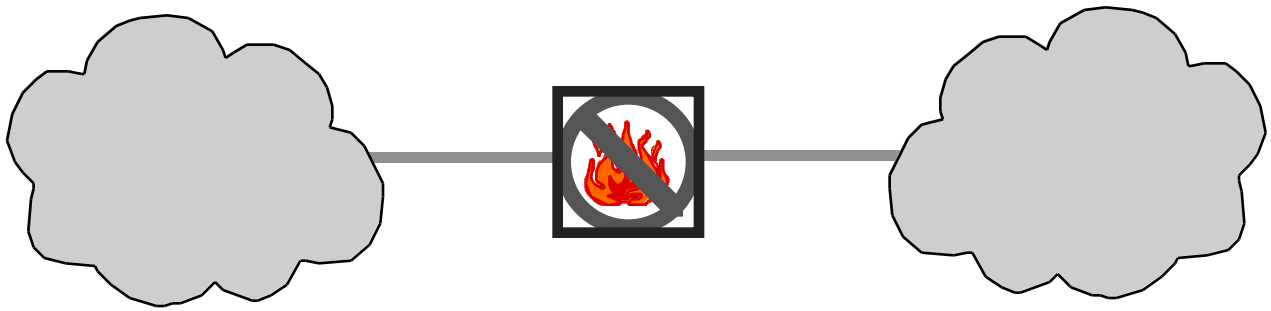


Reality Check!

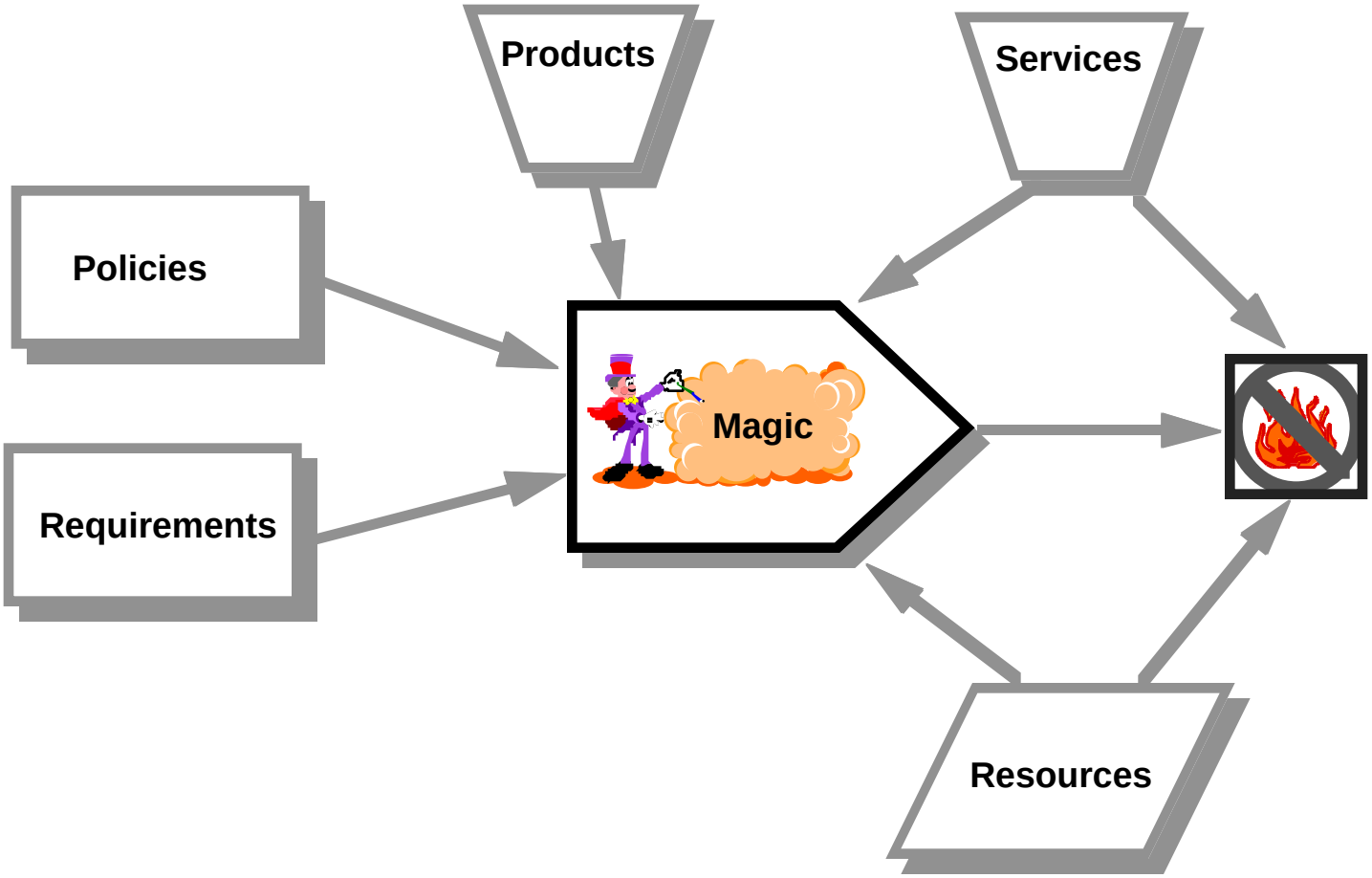
- **The purpose of a business is to provide some product or service.**
- **The purpose of security is to reduce some of the risks associated with operating and maintaining a business.**
- **The purpose of a firewall is to support some aspects of the security policy.**

Reality Check, Part 2!

- **A firewall, as a chokepoint, may also be a single point-of-failure.**
  - **Reliability, performance become issues.**
- **Therefore, the firewall's status may quickly be elevated to a mission critical one.**



How do you set up a firewall?



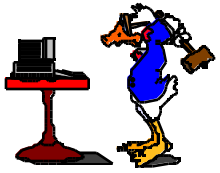
Our goal is to try and reduce the magic.

Develop a policy and requirements

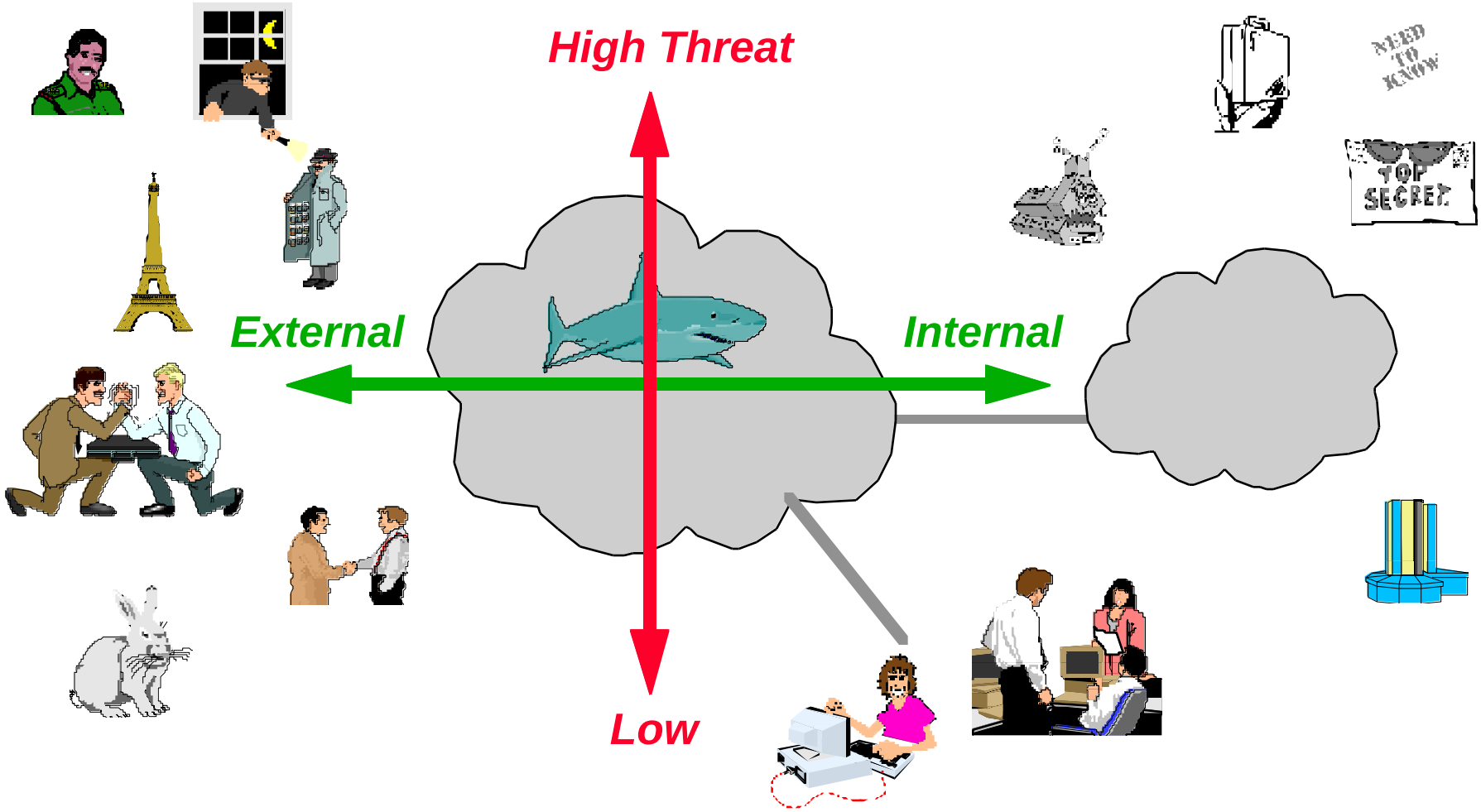
- **Need to understand the assets to be protected and the threats to those assets.**
- **Need to understand the user requirements.**
- **The target is probably somewhere between the two.**

Security

Too Weak **Too Strong**



Assess the threats vs. assets



What about protocols?

- **The good...**
  - **Telnet**
- **...the bad...**
  - **Any UDP, finger**
- **...and the ugly.**
  - **FTP, X11**
- **Actually depends on your point of view.**

Understand your resources

- **Financial.**
- **Time.**
- **Technical expertise.**
- **Systems used.**

To build your own...

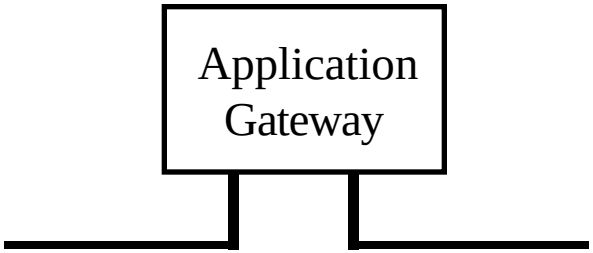
- **It takes a certain level of expertise in computer network security, UNIX system administration, and programming.**
- **"The FWTK is meant for individuals who:**
  - **know C**
  - **know TCP/IP**
  - **know UNIX as a system manager**
  - **have built C software packages on UNIX systems."**

— Frederick Avolio, Trusted Information Systems

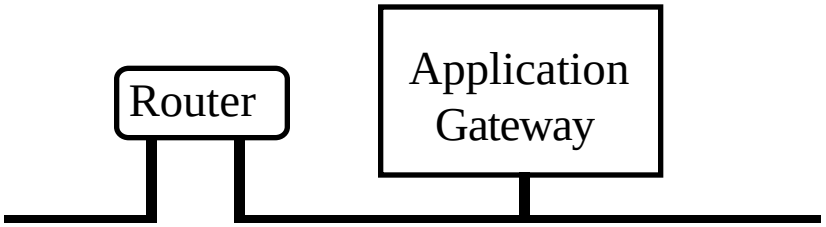
Products and Services

- **There are over 40 commercial firewalls offering a wide range of configurations and capabilities.**
- **There is a wide range of services available.**

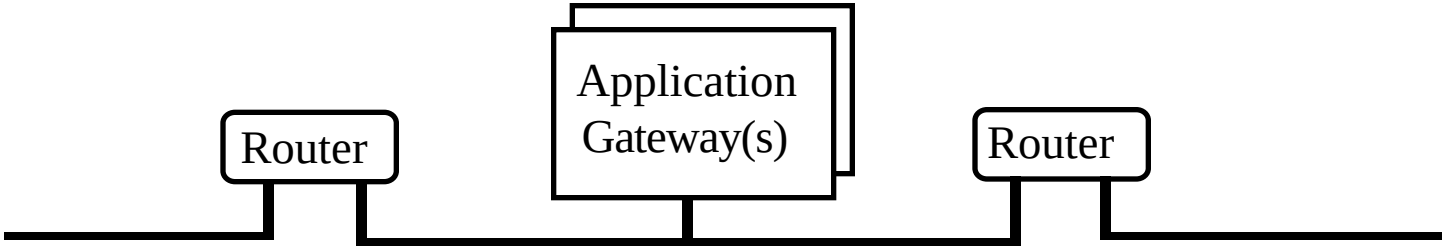
Configurations range from simple to complex



Dual-homed Gateway

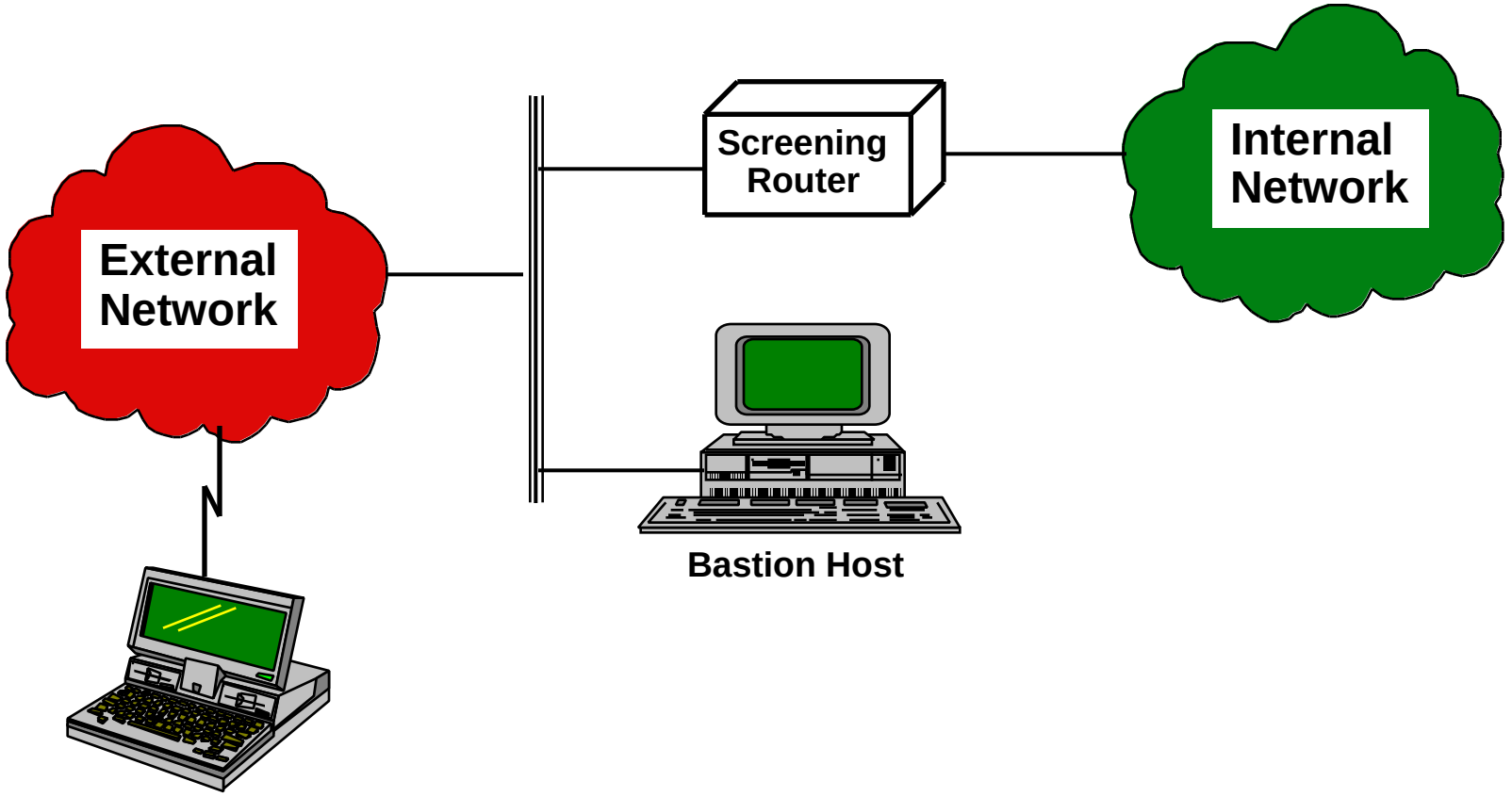


Screened Host Gateway

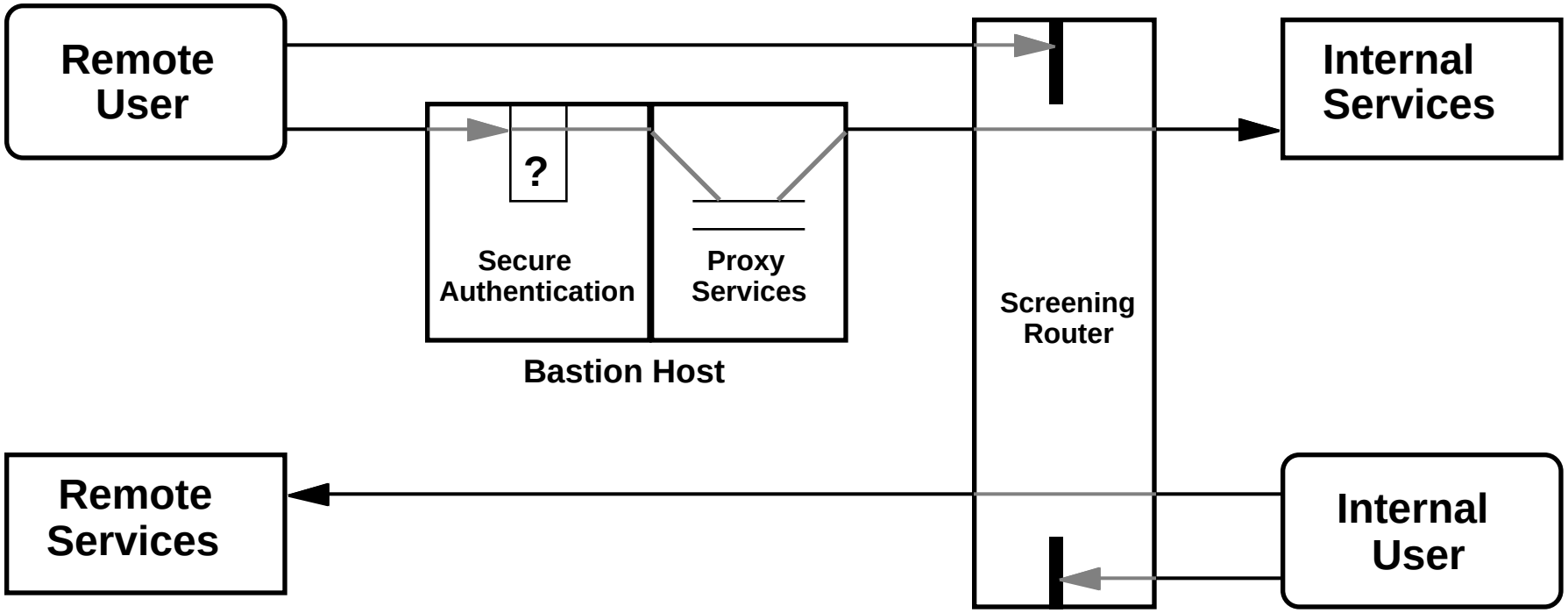


Screened Subnet Gateway

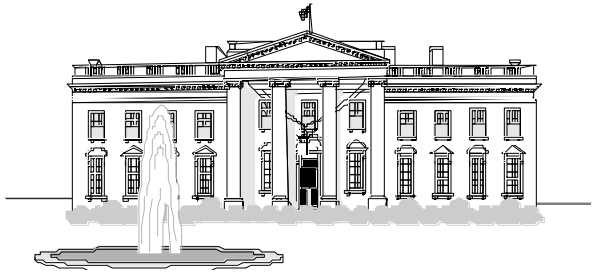
Here is a physical sample...



...and here is the logical view



*White House Firewall**



- **DEC SEAL, Gauntlet based.**
- **9 months and $275K.**
- **2 full-time Secret Service agents for administration.**
- **25-30K mail messages per day, filtered for content.**

**** From a presentation by Bill Hancock to the DECUS Bay LUG, 7/10/95.***

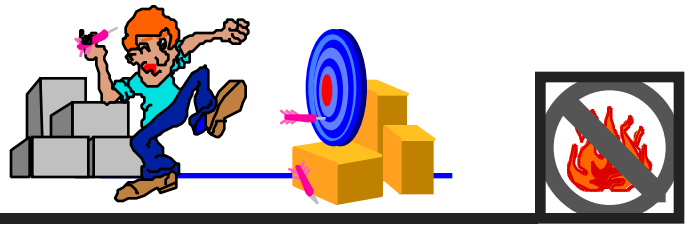
Build your own?

- **There is ample software available:**
  - **TIS Firewall Toolkit (FWTK)**
  - **Freestone from SOS Corp.**
  - **Socks**
  - **Screend**
  - **KarlBridge (demo and commercial), DrawBridge**
  - **S/Key**
  - **Others**

Other Sources:

- **Commercial Services**
  - **Internet Providers**
  - **Consultants**
- **Commercial Products**
  - **Screening Routers**
  - **Software**
  - **Operating Systems**
  - **Hardware**
  - **Services**

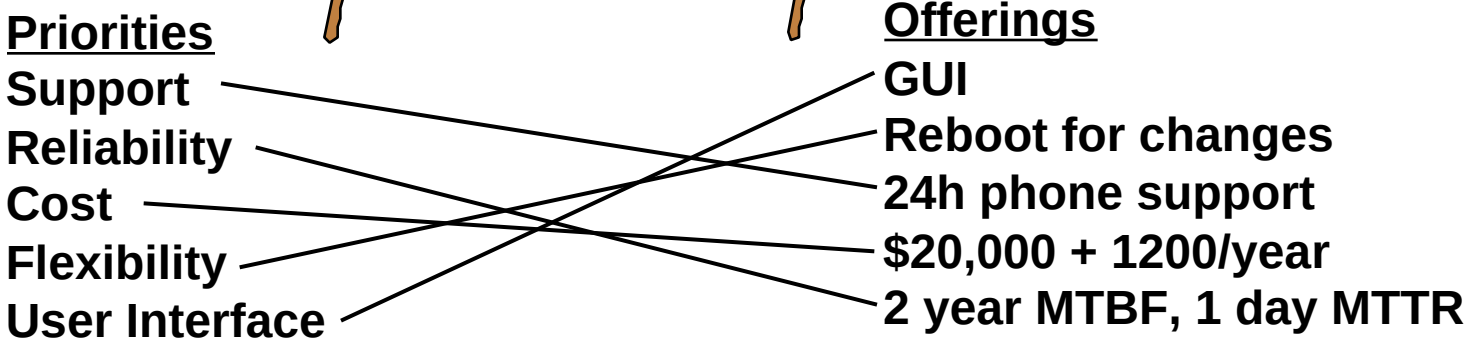
How to select



- **Start with the go/no-go decisions:**
  - **Will a particular product or service support your security policy?**
  - **Do you have the necessary resources?**
  - **Are there other show stoppers?**
    - **Performance (T1, Ethernet, FDDI, etc.)**
    - **Protocols supported (Appletalk, DECnet)**
    - **Encryption**

How to select (cont.)

- For the rest, balance your priorities against the offerings of the target products.



Some Selection Criteria

- **Protocols**
- **Hardware and Operating Systems**
- **Management Interfaces**
- **User Authentication**
- **Encryption**
- **Firewall Validation**
- **Services**

A Sampling of Products

- **Sidewinder**
- **Gauntlet**
- **Digital's Firewall Service (formerly SEAL)**
- **Firewall-1**
- **Internet Site Patrol**
- **Firewall-Plus**
- **SunScreen**

Future directions

- **Better integration of security components.**
  - **Management, host-based security, intrusion detection.**
  - **CSTC and partners have several research projects on the table.**
- **Standards**
  - **Firewall management, cooperative firewalls.**
- **Performance**

References:

- **Cheswick, William R. and Steven M. Bellovin. Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley, 1994.**

- **Chapman, Brent and Elizabeth Zwicky. Building Internet Firewalls, O'Reilly & Associates, 1995.**

- **Hare, R. Christopher and Karanjit Siyan. Internet Firewalls and Network Security, New Riders Publishing, 1995.**

On the WWW:

- **The Firewall Report, by Outlink Market Research (http://www.outlink.com), contains over 600 pages reviewing over 40 firewall products.**
- **Catherine Fulmer maintains a list of firewall products at:**
  - **http://www.waterw.com/~manowar/vendor.html.**
- **The Firewalls Mailing List:**
  - **Send E-Mail to firewalls-request@greatcircle.com with "subscribe firewalls" as the message body.**

Crossing the finish line

- **There are many good products out there, with more emerging.**
- **Avoid “analysis paralysis.”**
- **Don’t fall into a false sense of security.**

We (the CSTC) are here to help you reach your security goals through our various services and projects, but...

...We need your help!

- **Feedback on commercial products and services.**
- **Information on what products and services you are using so that we may serve as an information broker.**

Visit:
http://ciac.llnl.gov/
cstc/CSTCHome.html

CONTACTS
SPCooper@LLNL.GOV
CIAC@LLNL.GOV