Internet Firewalls
-
An Overview

Marcus J. Ranum
Senior Scientist
Trusted Information Systems, Inc.

Why a Firewall?

- To protect one network from another
  - Keep out unauthorized users
  - Keep in private or sensitive data
- To "sell" upper management on the idea of connecting to the Internet
- To audit or log Internet usage
  - Justify connection through usage statistics
  - Pinpoint bottlenecks
- To act as a central point of contact for the organization (ex: *gatekeeper.dec.com*)

Security Paradigms

- **That which is not expressly permitted is prohibited**
  - **Firewall blocks everything**
  - **Administrator must take steps to support each service**
  - **Implicitly “dis-empowers” users**

- **That which is not expressly prohibited is permitted**
  - **Firewall blocks services that are known potential security risks**
  - **Users can potentially introduce security holes in system**

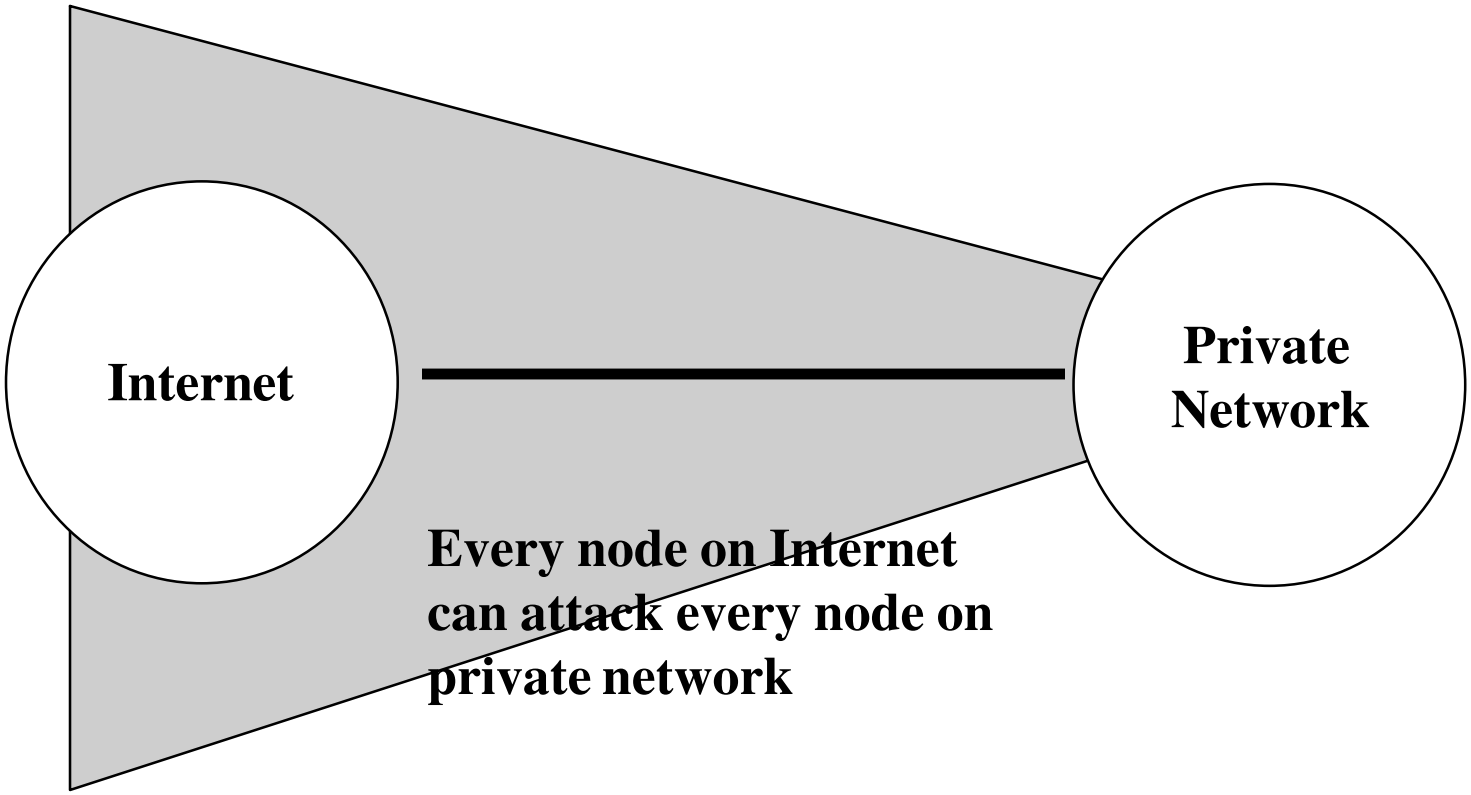
Perimeter Defense
v.s.
Defense In Depth

- **Principles of Perimiter Defense:**
  - **Protect all access paths leading into the network, using internet firewalls, passwords on terminal servers, modem callback, etc.**
  - **Within the network, hosts can trust each other**
  - **Not concerned about ethernet sniffer attacks within the network**
- **Principles of Defense in Depth:**
  - **Protect all access to hosts, enforcing strict security policies on each system that is on network**
  - **Within the network, hosts require strong authentication for trust (e.g.: Kerberos, SecurID, etc)**
  - **Restrict connection to the network - users generally do not manage or install their own systems**

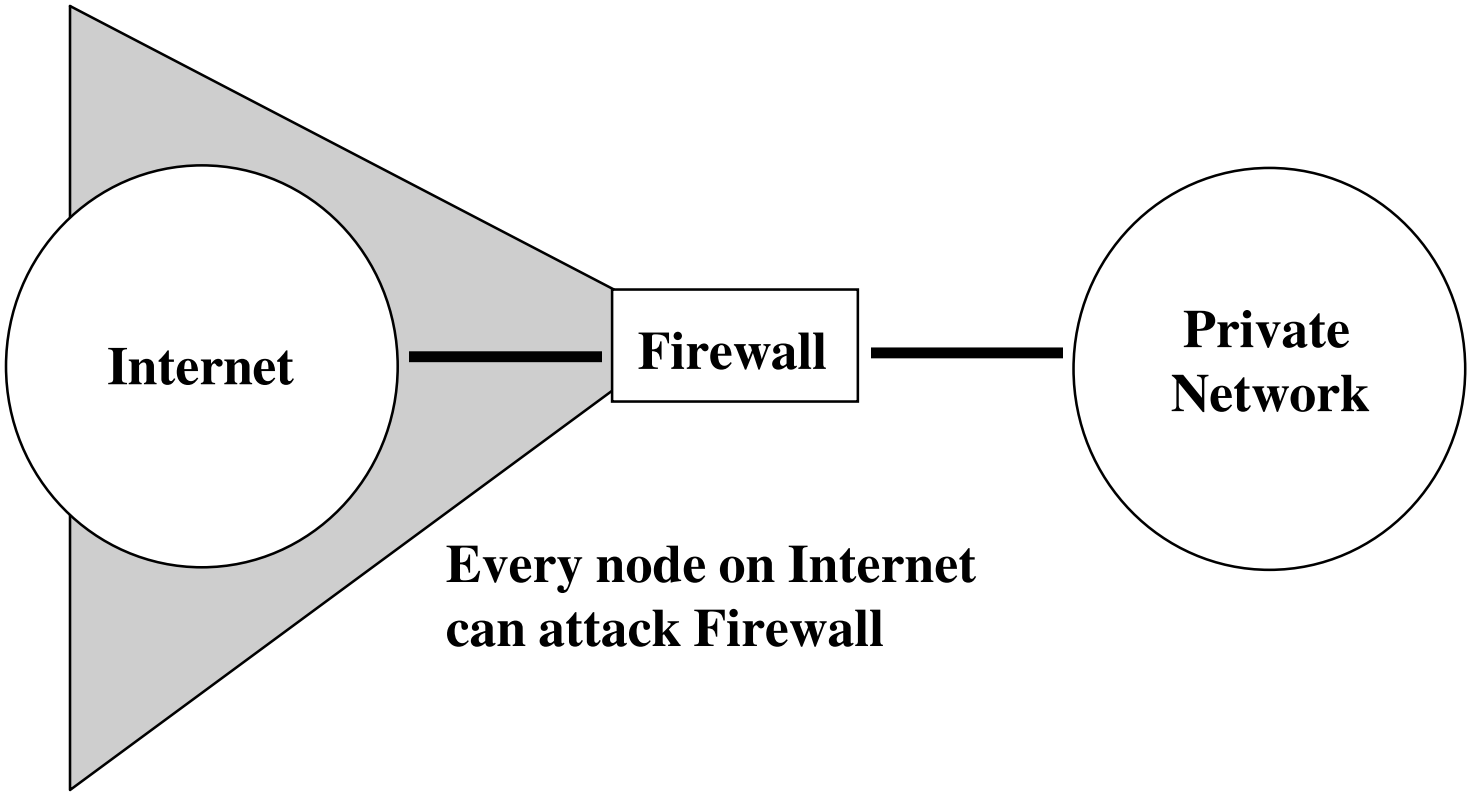
A Threat Model for Firewalls

- **Threat is quantified in terms of "Zones of Risk"**
  - **How many potential angles of attack can the firewall be subjected to?**
  - **What is the progression of attacks if the first one succeeds?**
  - **At what point do an attacker's actions become untraceable?**
  - **At what point do the network's defenses completely come apart?**
- **Minimizing zones of risk entails restricting the "size" of the network connection to be as small as possible**
- **Single point of failure must be avoided if possible**

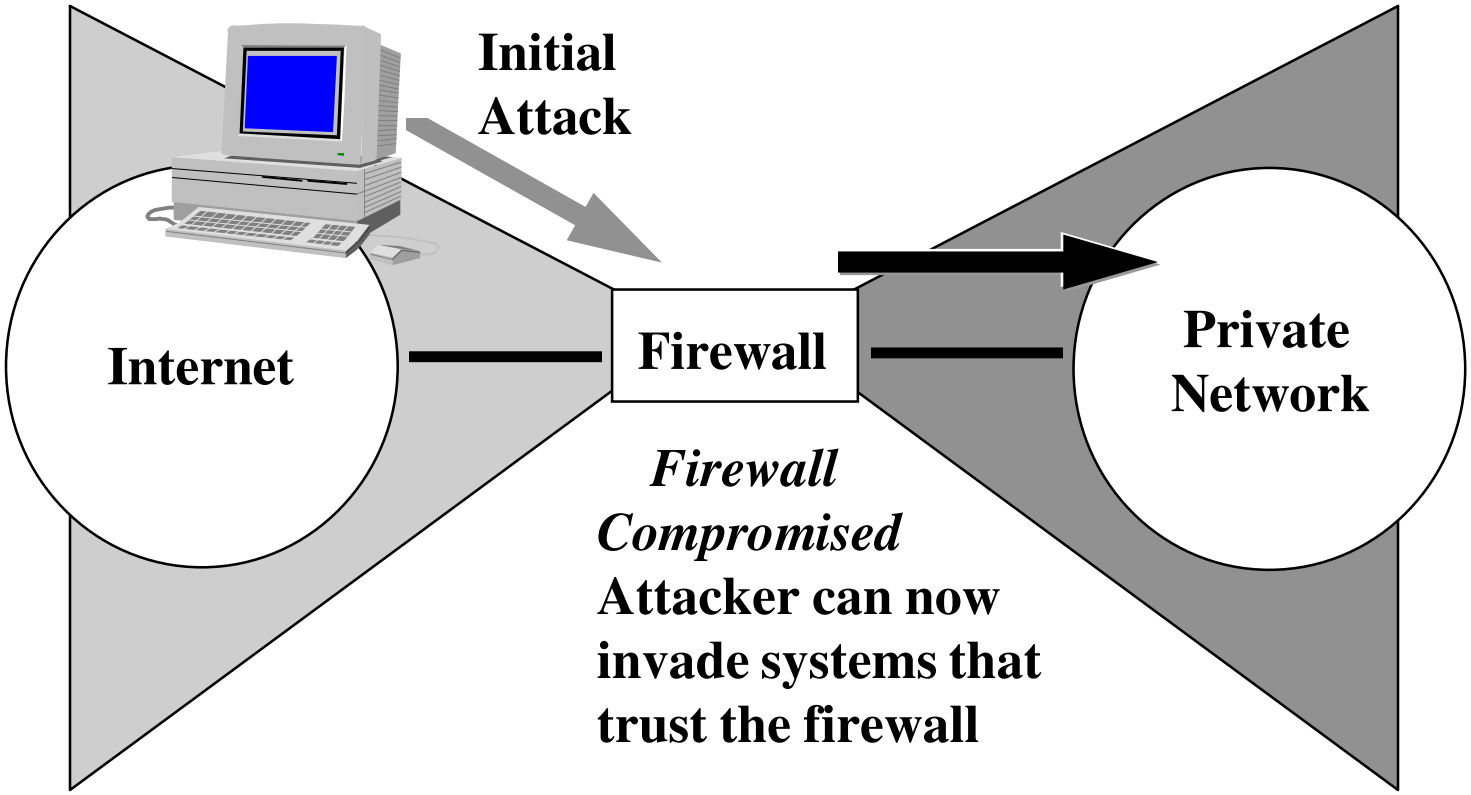
Zones of Risk
Direct Internet Connection



Zones of Risk
With a Firewall



Zones of Risk
Island-Hopping Attacks



The User Problem

- **Most systems break-ins are result of users picking poor passwords, setting bad entries in *.rhosts* or otherwise weakening security**
- **Most system security bugs require a log-in on the system to exploit them fully**

...*So what can you do about it??*

Keep users off the firewall itself!!

- **This means that someone logging into the firewall is a noteworthy security event**

Firewall Components
Screening Routers

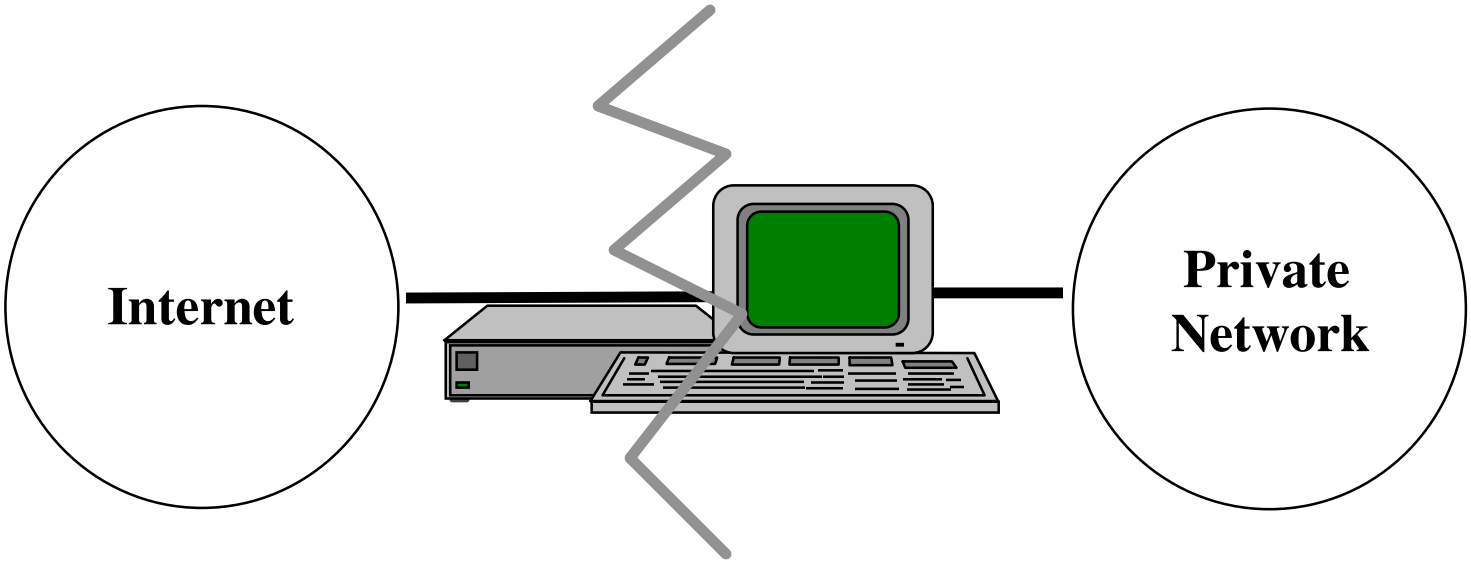
- **Can be a commercial router (e.g.: a Cisco, Wellfleet, Proteon, etc)**
- **Can be a host running an operating system that supports packet screening**
- **Some screening routers permit various levels and types of packet logging**
- **Many firewalls consist of nothing more than a screening router**

Firewall Components
Bastion Hosts

- **Bastion Hosts are systems identified as network "strong points"**
- **Often act in capacity of Email relays, name servers, FTP servers, USENET News servers, etc.**
- **Generally, a Bastion Host is one that is recognized as a potential point of attack (E.g.: *gatekeeper.dec.com* or *dockmaster.ncsc.mil*)**

Firewall Components
Dual Homed Gateway

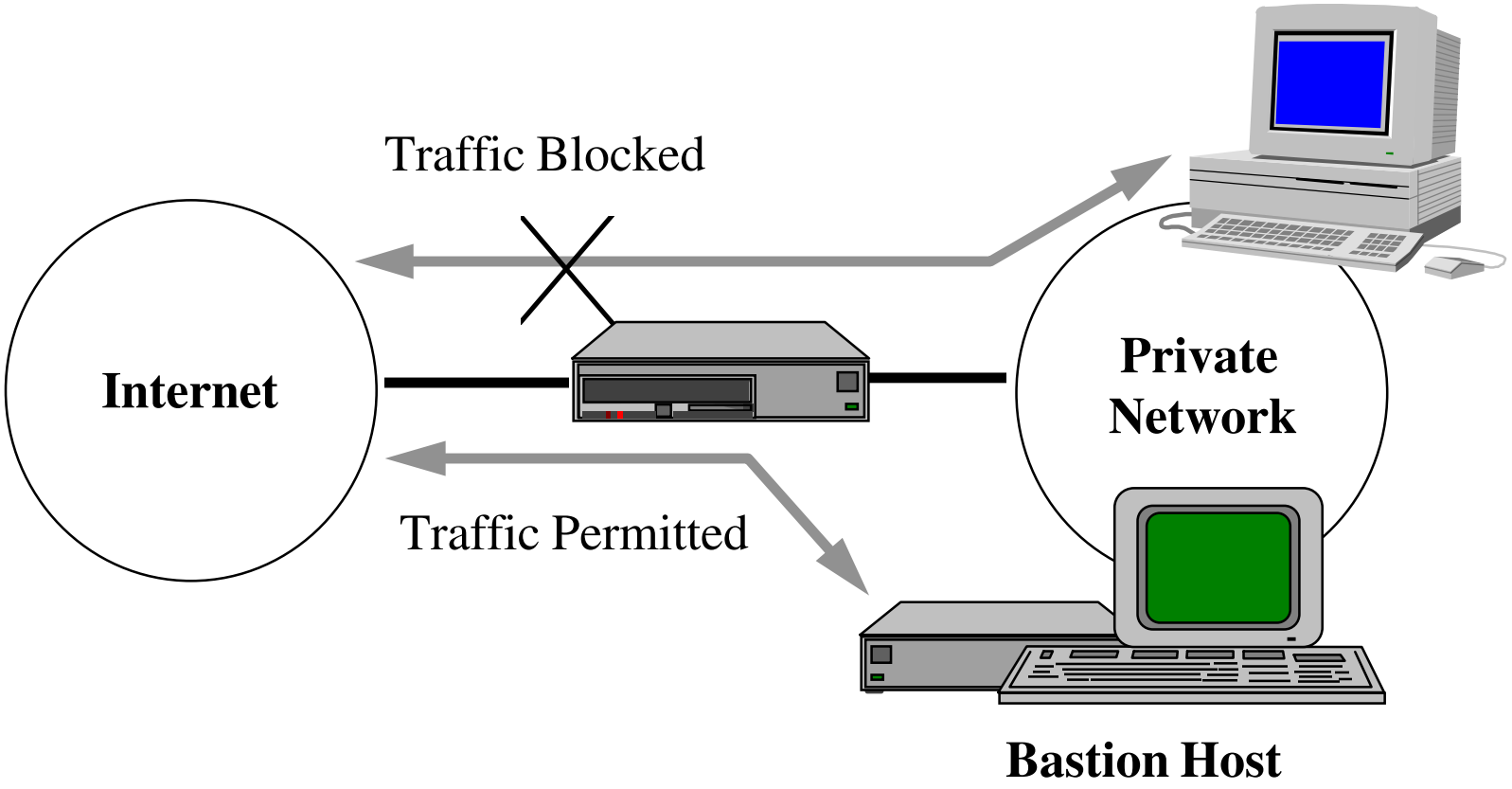
- **Dual Homed Gateways are based on a system with two network connections, with routing between them disabled**



Firewall Components
Dual Homed Gateways

- **Reachable from both Internet and private network, but traffic cannot flow across it directly**
- **Some sites use a Dual Homed Gateway as a user "base of operations" for access to Internet**
  - **Users must first log in to Gateway, then can log in to hosts on Internet, or do FTP, etc.**
- **Dual Homed Gateway system is, by definition, a Bastion Host**

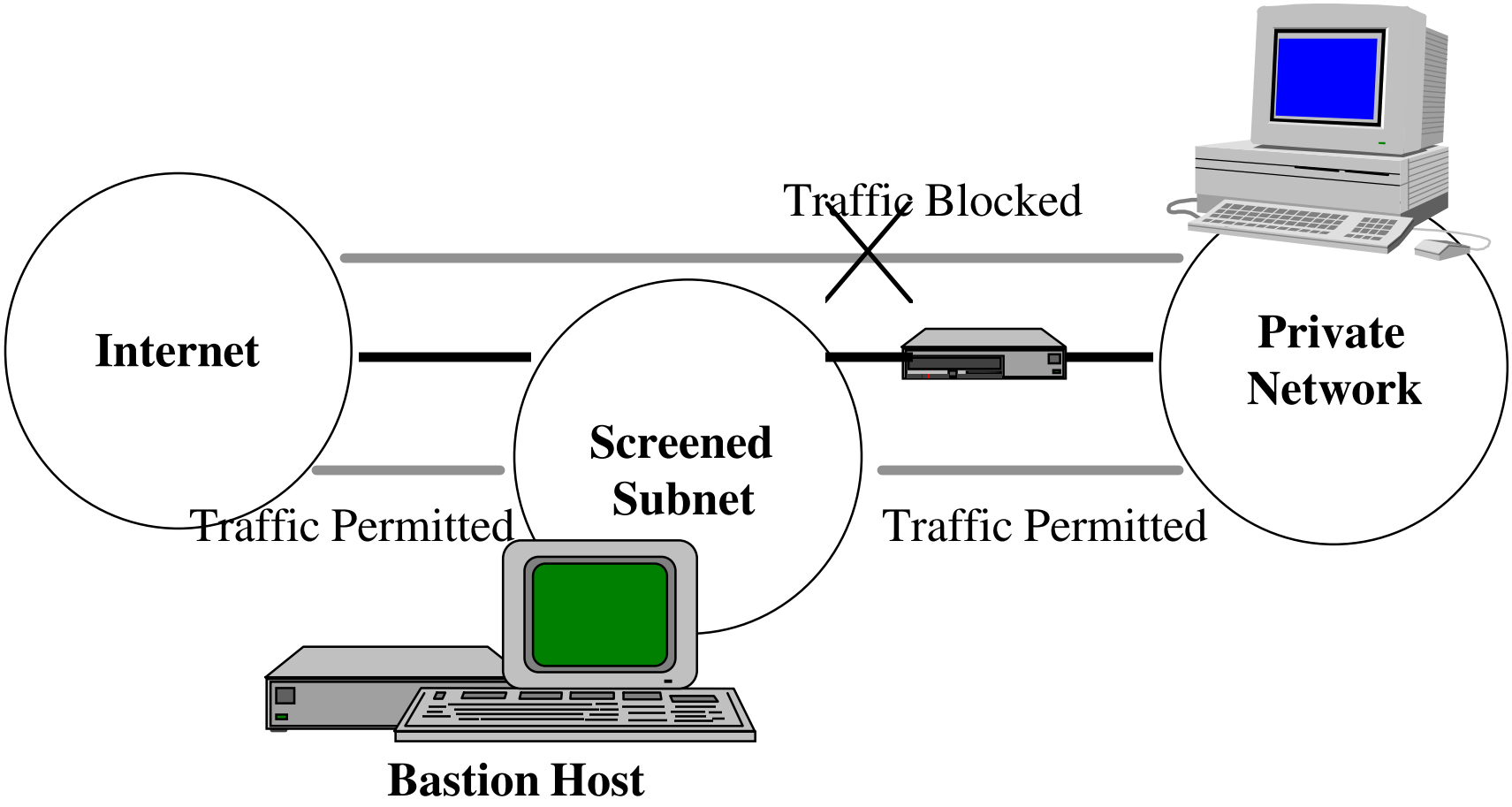
Firewall Components
Screened Host Gateway



Firewall Components
Screened Host Gateway

- **Screened Host Gateways are the most common form of firewall, also the most flexible**
- **Screening Router blocks traffic between Internet and all hosts on private network *except* for a single Bastion Host**
- **Screening Router can be configured to permit nodes on private network to directly access Internet via TELNET or FTP**

Firewall Components
Screened Subnet

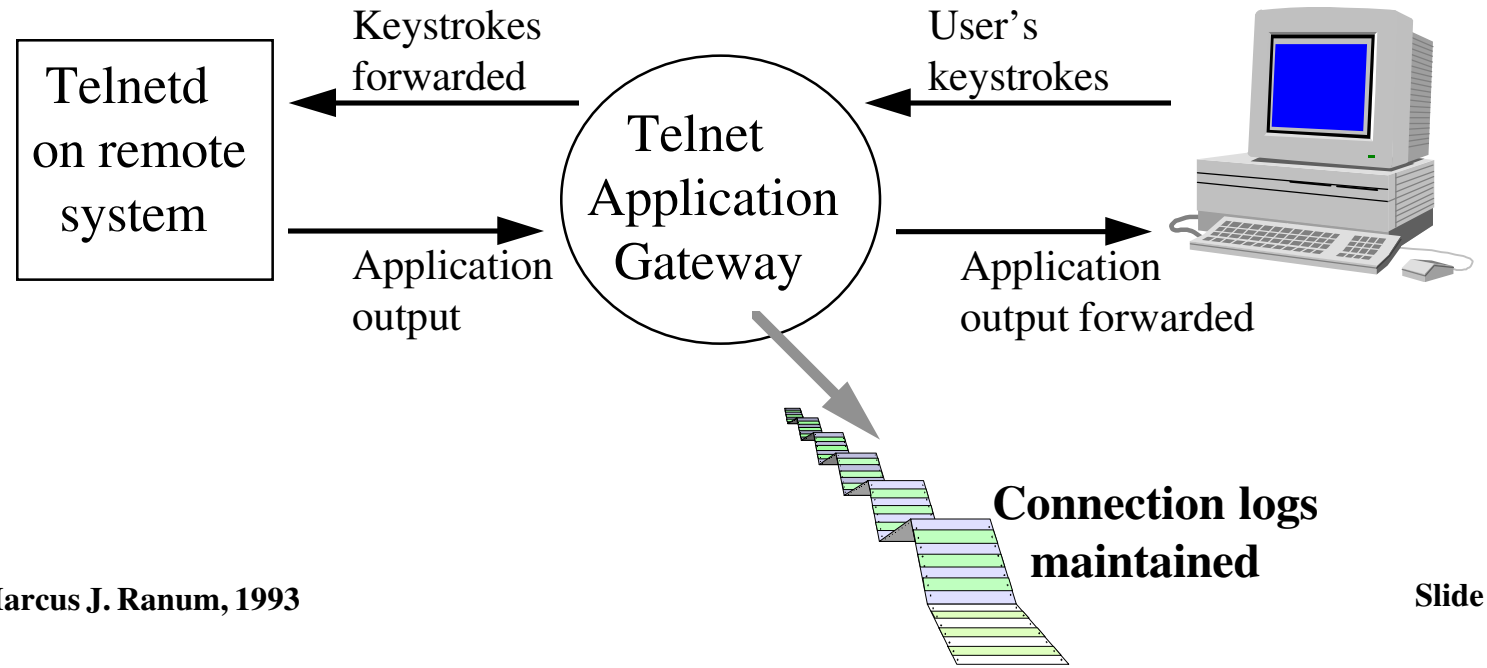


Firewall Components
Screened Subnets

- **Screened Subnet approach places a "sandbox" network between the Internet and the private network**
- **Internet can only communicate with nodes on the Screened Subnet**
- **Private network nodes can only communicate with nodes on the Screened Subnet**
- **Permits the private network to be effectively "invisible" to the Internet**

Application Gateways

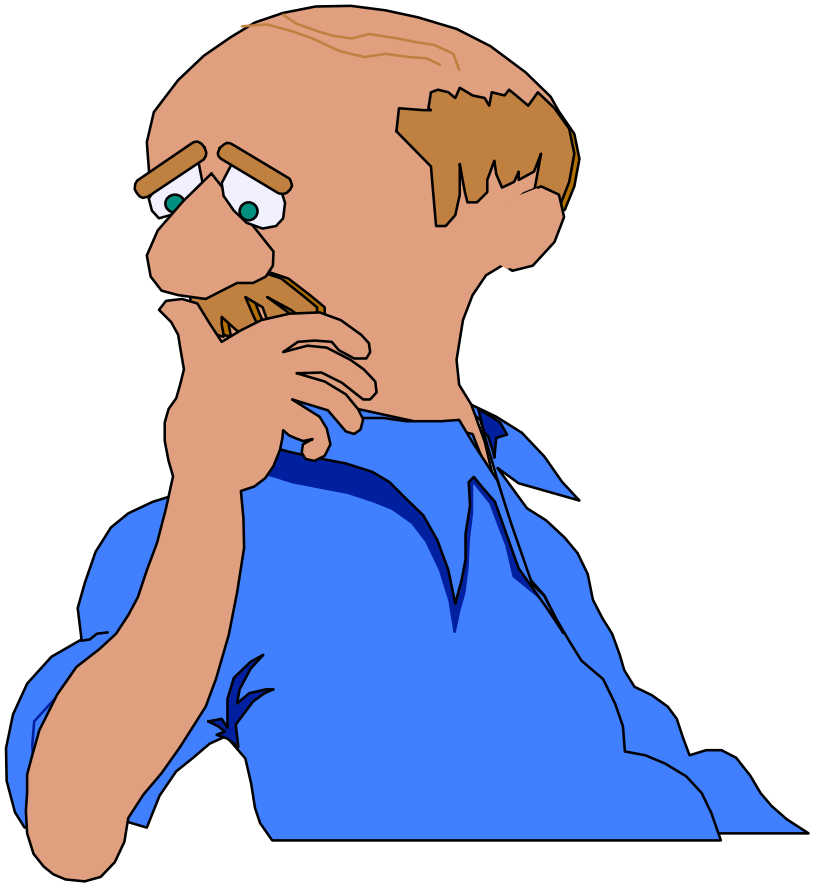
- **Application Gateways handle store and forward traffic and some types of interactive traffic**



Application Gateways

- **Since Application Gateways handle traffic at an application level, they understand the protocol of that application, and can log/audit traffic**
- **Application Gateways can have extra security/Authorization built into them as needed**
- **Examples:**
  - **Sendmail (arguably)**
  - **Telnet gateway (telnetxd)**
  - **FTP gateway (ftpxd)**
  - **X11 protocol forwarder**

Conclusions and Observations

- **Don't be scared of the Internet**
- **Build on past experience - there are many examples of good firewalls out there**
  - **Firewalls mailing list on Internet (firewalls@greatcircle.com, send mail to majordomo@greatcircle.com to get on it)**
  - **Papers by AT&T Research on *research.att.com* in *dist/internet_security***
  - **Papers on *decuac.dec.com* in *pub/docs/firewall***
- **Commercial and consulting offerings for firewalls are plentiful**

Sure, I'm paranoid.
But am I paranoid *enough*?