



# Firewalls

**Tom Longstaff**

**Institute of Internal Auditors**

**Advanced Technology Conference and InfoExpo**

**September 21, 1994**

CERT<sup>SM</sup> Coordination Center  
Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh PA 1521

The CERT Coordination Center is sponsored by the Advanced Research Projects Agency (ARPA). The Software Engineering Institute is sponsored by the U.S. Department of Defense.

1



## Definition

**“A fireproof wall used in buildings and machinery to prevent the spread of fire”**

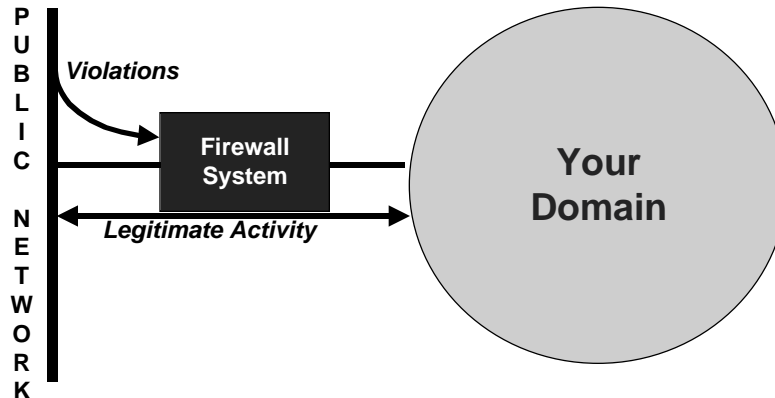
***The American Heritage Desk Dictionary***

**In an automobile, a firewall prevents the spread of fire while allowing control and monitoring connections to pass through**

2



## Network Firewall Concept



3



## Legitimate Activity

**Regulated by *policy***

**Defined by type of service (application),  
source, and destination  
allow electronic mail to  
and from anyone**

- allow news reading but not news posting
- allow login from inside to outside but not vice versa
- allow file transfer to a single system in your domain only
- do not give out the names of any systems in the environment

4



## Violations

**Violations are activities or behaviors not permitted in the policy**

- these can be either explicit or implied

**Firewall technology may help with the detection and prevention of violations from outsiders are intrusions**

5



## Firewalls and Policy

**Firewalls automate the enforcement of a network access policy**

**Some firewall architectures may also provide**

- additional functionality
- monitoring
- public services

**Firewalls cannot**

- determine intent
- prevent abuse of allowed services
- provide host security
- protect against violations through other pathways

6



## Firewall Types

### Filters

- Restrict traffic based on packet header information
- Most common fields are type (tcp, udp, etc), src, dst, port/service
- Advanced filters may restrict traffic based on traffic patterns or other aggregate information

### Proxies (or Application Gateways)

- Restrict traffic based on packet content
- Is application specific

### VPN/IPSec Gateways

- Supports tunneling between networks
- Can support tunneling to mobile nodes

7



## Filter Rules

### Two philosophies

- Allow all except those packet types that carry known vulnerabilities
- Deny all except those packet types that are required by users

### Some rules carry context

- Connection-oriented
- Based on SYN/ACK protocol

### Filters have problems with:

- Malformed packets/fragmented packets
- Out-of-sequence protocols
- Backward client-server protocols (X11, FTP)

8



## Gateways and Proxies

**These are paths through your firewall to allow services**

**Proxies are intermediaries that regulate service through the firewall**

**Application gateways and proxies allow specific application interfaces through the firewall**

**Encryption is the bane of gateways and proxies**

9



## Firewall Architectures

### Where to position firewalls?

- between your domain and every access to the outside
- between administrative domains of dissimilar policy
- between networks where the boundary much be controlled

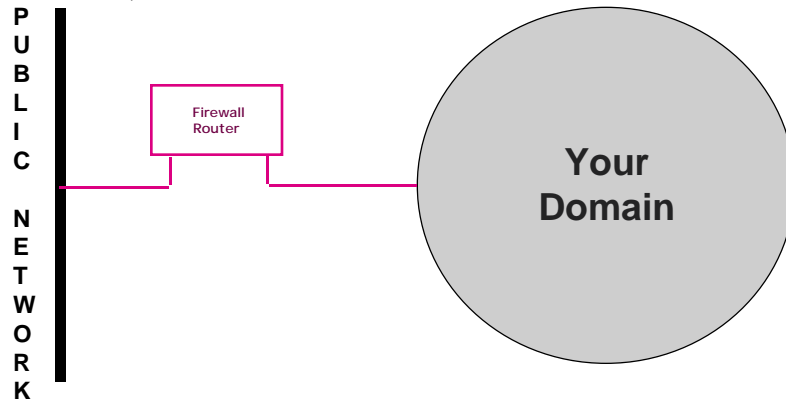
### What architecture to use?

- simple router
- router with multiple interfaces
- gateway/proxy services between dual routers
- a gateway separating dual routers

10



## The Simple Router (packet filter) -1



11



## The Simple Router (packet filter) -2

### Advantages

- cheap - usually a must-have anyway
- simple - only one configuration file to contend with
- verifiable - packet monitoring at the site will assure filtering is working

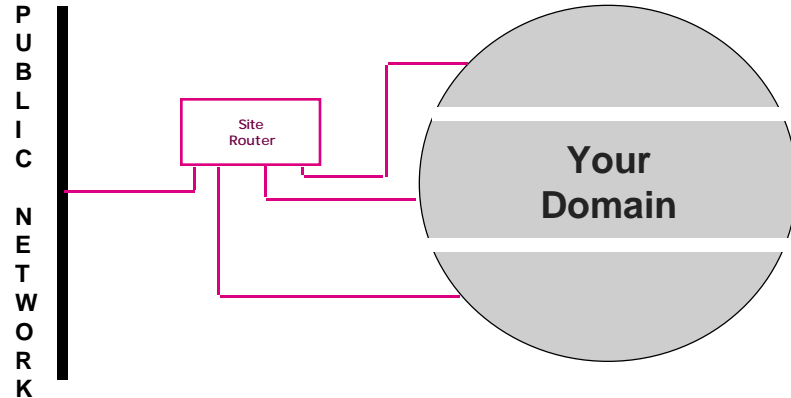
### Disadvantages

- no flexibility with applications - packet filter only
- only extreme for security
- limited logging capability

12



## A Router with Multiple Interfaces -1



13



## A Router with Multiple Interfaces -2

### Advantages

- ability to segment a site into distinct domains
- flexibility to create logical architectures
- single configuration file to maintain

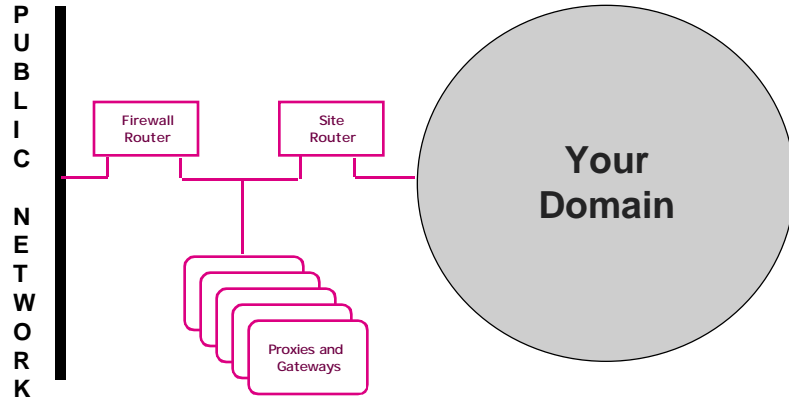
### Disadvantages

- single point of failure
- convoluted configuration file
- possible confusion over interfaces
- vulnerabilities associated with the router

14



## Gateway/Proxy Services Between Dual Routers -1



15



## Gateway/Proxy Services Between Dual Routers -2

### Advantages

- ability to provide risky services
- application filtering possible
- allows you to hide many hosts behind the second router
- provides a good auditing point

### Disadvantages

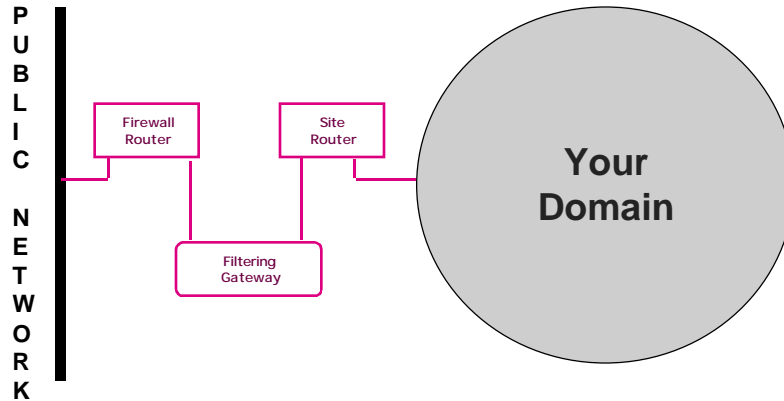
- still a physical connection between routers
- may allow unprotected services and tunnelling through to “slip by” the proxy
- multiple configuration files to maintain

16





## A Gateway Separating Dual Routers (“belt and suspenders”) -1



17



## Gateway Separating Dual Routers -2

### Advantages

- provides both logical and physical separation
- restricts services not addressed by the proxy or gateway system
- provides controlled functionality through the firewall
- supports a limited access policy (e.g., email only)
- excellent central point for accounting/monitoring

### Disadvantages

- limits functionality to available gateway/proxy software
- causes a bottleneck for traffic
- difficult to setup and maintain

18



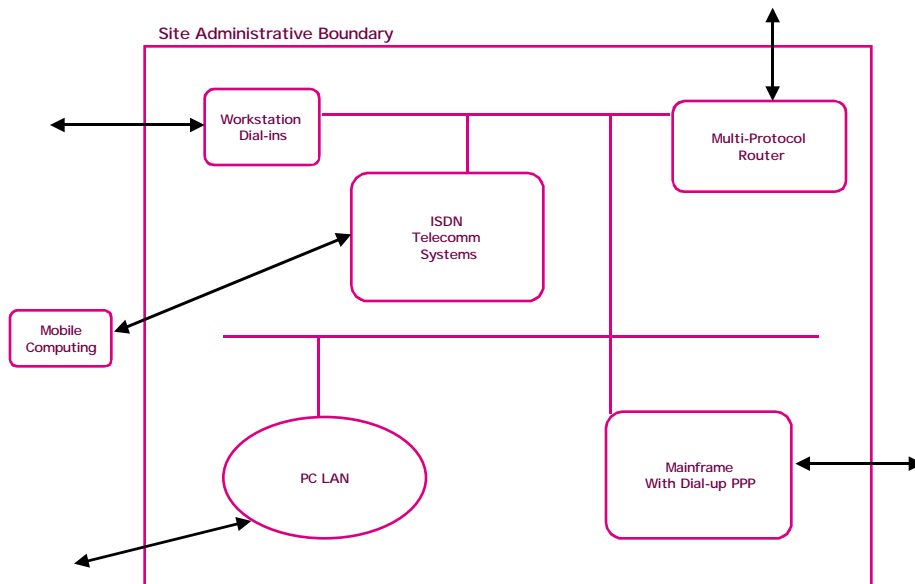
# The Future of Firewalls

**Firewall technology relies on controlling access points to the network**

**When access to the network becomes more distributed and ubiquitous, control becomes difficult**

**Restrictive firewalls discourage network growth and development**

**Trust in firewalls may cause a false sense of security**





## Discussion

If your security policy does not allow Java applets to be run on an internal network, is a proxy or filter more appropriate? Why?

What are some of the issues involved in attempting to use a proxy to disallow Java applets?

Presentation Opportunity: CERT report on State of the Art for Intrusion Detection Systems

Firewall papers (many)

Research CISCO PIX firewall product family and describe the features, performance, and reliability. Also describe how the PIX is configured and determine how easy this would fit into a complex architecture