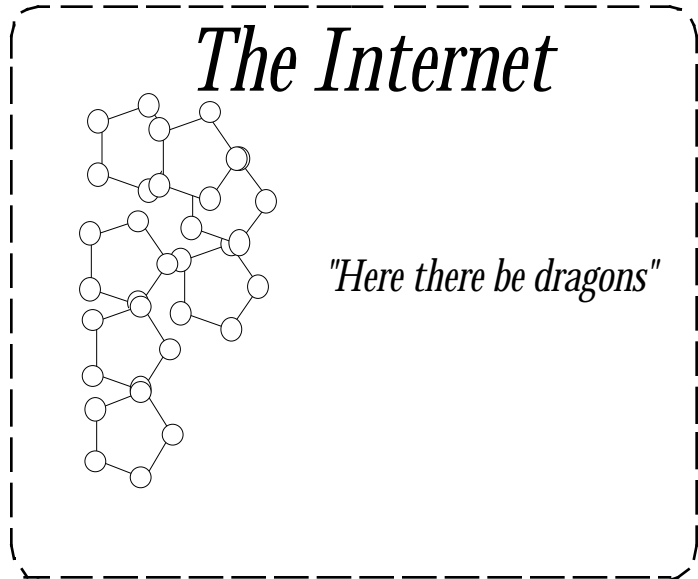
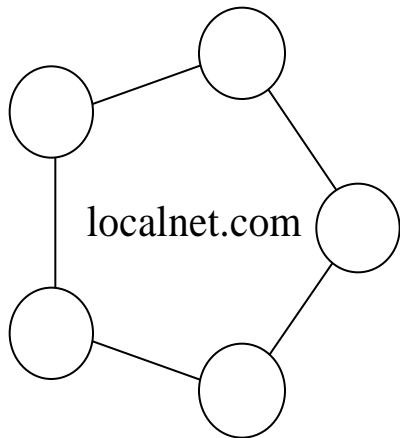


Constructing Firewalls

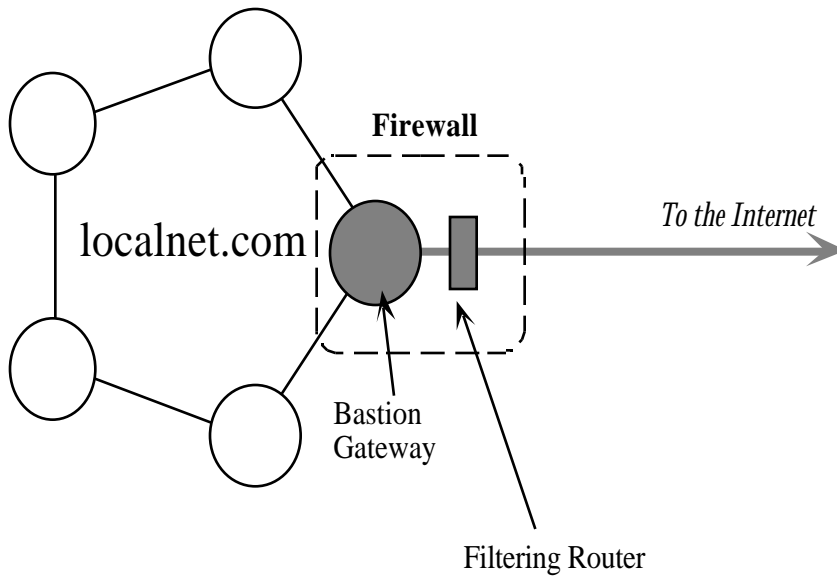
By Micah Altman
Last Revision: May 19, 1998
Copyright 1993-8

Constructing Firewalls



- Security issues
- Types of Firewalls
- Implementation
- Special issues
- Limitations
- References

Firewalls and Security



- Security scenario
 - protect internal network from outside attacks
 - prevent information leaks from inside
 - allow increased level of service on internal hosts
- What is a firewall?
 - combination of gateway and routers
 - all traffic goes through firewall
 - firewall permits only services consistent with company's security policy
 - firewall itself is heavily protected against attacks
- Advantages of firewall
 - much easier to secure one machine (the firewall), than all machines on the network
 - allows "risky" but useful services to run on internal network while preventing attacks from outside
 - hides information about internal network from outside world
 - provides additional authentication and logging

Packet Based Firewalls

- Non-forwarding gateway
 - no packets or connections are forwarded
 - all traffic must originate on firewall gateway
 - to contact external network, must run on firewall
- Packet filtering router
 - filters traffic on the basis of packet header information
 - typically uses source & destination addresses, header flags, protocol types and port numbers
 - dangerous services are not permitted through firewall

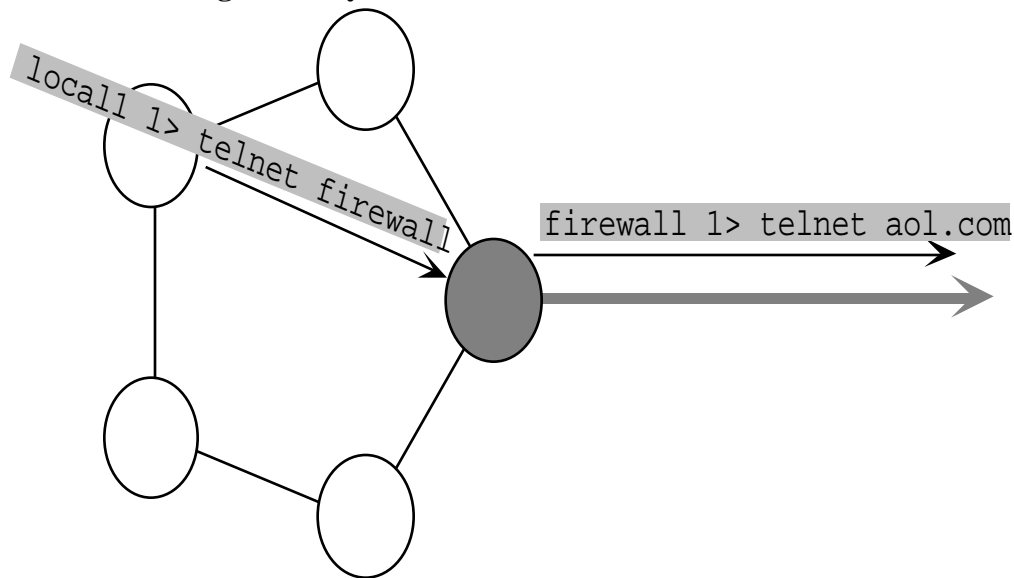
Application Based Firewalls

- Circuit level firewall
 - only tcp services are supported through firewall
 - all tcp services connect to proxy program on firewall
 - firewall creates a separate connection to the outside, and copies the data stream to its internal connection
 - usually combined with packet filtering
- Application level firewall
 - only specific services are supported
 - each service is rewritten to connect only to a special proxy server on the firewall
 - firewall reconnects to the outside, forwards information
 - usually combined with packet filtering

General Firewall Setup

- Keep things simple
 - have as few accounts as possible
 - eliminate unnecessary services and software (such as compilers, PERL, etc.)
 - eliminate as much system software as feasible
- Test firewall
 - interactions between different services can create unexpected holes
 - always test for correct operation
 - public auditing software available for testing common problems
 - COPS, TripWire: system security auditing
 - ISS, SATAN: network security auditing
- Configure firewall to fail-safe — block traffic if system crashes

Non-Forwarding Gateway



- Design
 - turn off forwarding on gateway host,
 - often a Unix platform
 - all internal users must login (or rsh) to gateway to access external network
- Advantages
 - simple to set up
 - simplicity can increase security
 - monitoring is easier: if you see a direct connection from internal to external network, something is wrong
 - mistakes in configuration less likely: no complicated interaction of filtering rules to be considered
- Limitations
 - gateway host must run all application services
 - administrative complexity: users must be able to log on to the gateway and run services from there
 - centralization: in this configuration, gateway must run as DNS server, network news hub, mail relay, etc.
 - security issues: complexity increases probability of possible configuration error, or buggy service
 - single point of failure
 - penetration of the gateway leads to total failure of security
 - not designed to prevent deliberate internal information leaks

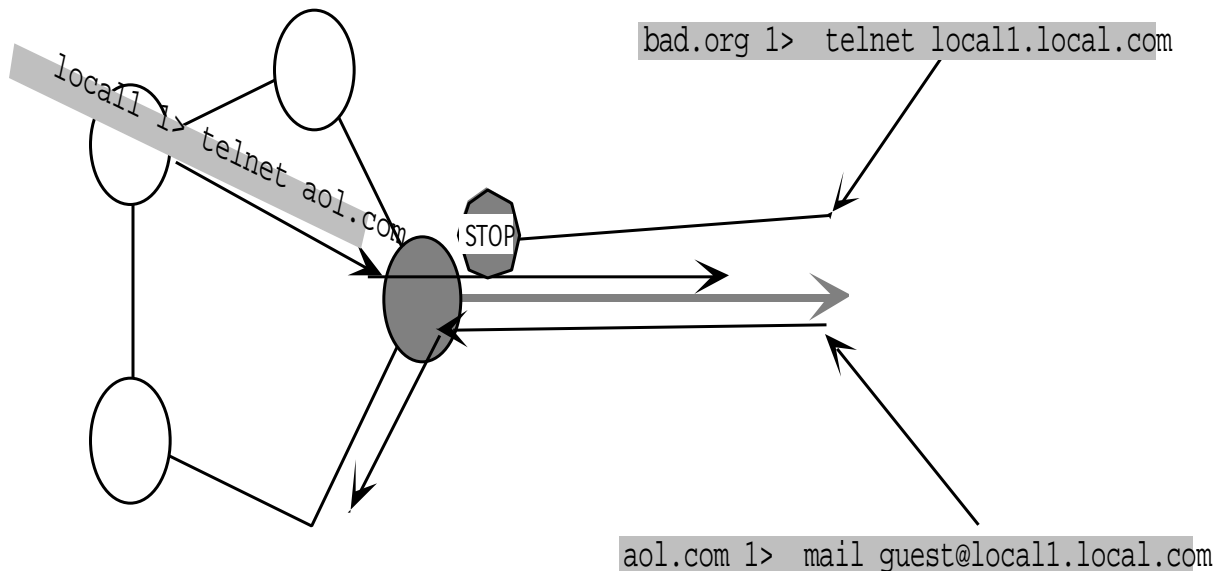
Implementing a Non-Forwarding Gateway

- Basic gateway setup
 - deactivate ip (or other network level) packet forwarding on gateway
 - IRIX setup*
 - ```
set ipforward=0 with systune
(old versions of IRIX rebuild kernel using lboot , edit
 /var/sysgen/master.d/bsd)
```
  - turn off route advertising on gateway
    - On Silicon Graphics platforms:  
edit /var/config/routed.options  
add -q flag to put routing daemon in "quiet" mode  
(Similar setup for gated , check the man pages)
- Client setup
  - no special client setup needed
  - all users must log in to gateway to access external network
- Testing
  - test normal services to ensure that they cannot pass through
  - check blocking of multicast, broadcast and loose-source-route packets as well, some software is not thorough
    - multicasts: in IRIX turn off mouted ("chkconfig mouted off")
    - broadcasts in IRIX: broadcast forwarding controlled by kernel variable  
ipdirected\_broadcasts in /var/sysgen/master.d/bsd or  
systune

## Securing Logins on a Non-Forwarding Gateway

- Failure of gateway can cause total security failure
- Options for securing outside logins
  - option 1: use one-time passwords for all logins
    - if one-time passwords are not used, they may be snooped if logins occur from the external net to the gateway
    - see description of *s/key* below for one-time password support
  - option 2: only console logins are allowed
    - set up in `login.options`
  - option 3: trust internal hosts
    - secure all accounts by putting "\*" in password field
    - use `/etc/host.equiv` to allow unpassworded login as guest from internal machines only
    - deactivate use of `.rhosts` with option to "rlogin" in `inetd.conf`
    - Note: need to filter outside packets to prevent ip address spoofs for full security
  - option 4: use filtering to prevent any logins from external net

## Packet Filtering Router



- Design
  - packet filter prevents all unwanted traffic
  - packet filter may allow services through to all machines, or only to special servers (e.g. for mail, news, dns)
  - often used in combination with non-forwarding approach
    - e.g. mail permitted through gateway, but ftp connections are only allowed to and from gateway.
- Advantages
  - internal users can access outside network transparently
  - no changes necessary for client software

- firewall machine does not need to run many services itself, increasing security
- Implementation
  - `ipfilterd` - for SGI, part of gateway system software, no additional charge
  - `screend` - for BSDI
  - `ipfwadm` - Linux
  - Karlbridge - freeware converts PC into filtering router
  - Many routers support some filtering

### Packet Filter Design (Continued)

- Limitations
  - only limited information is available from packet headers
    - typically source, destination, protocol type, port #, some flags
  - difficult to deal with services that use callbacks or dynamic server ports
    - callback services - remote machine initiates connection to internal machine. Includes ftp, X11
    - dynamic server ports - many RPC services dynamically allocate ports
    - caveat - these services probably should not be allowed through the router anyway.
    - Use a non-forwarding approach for crucial services such as ftp.
  - vulnerable to deliberate internal information leaks
    - impossible to control meaning of port id on remote host: outgoing information could be to any service, if user wishes
    - vulnerable to "tunneling": illegal service is deliberately piggybacked on permitted service
  - interactions among filter rules can occur with unanticipated results, always test the filtering mechanism

### Implementing Packet-Filtering

- Basic router setup
  - filtering router : set up filter list according to router instructions
  - p.c. or equivalent: use the freely available Karlbridge (`kbridge`) package
  - IRIX system: use the ip filtering daemon, `ipfilterd`
    - to activate: `chkconfig ipfilterd on`, will trigger startup when running network script
    - running: `ipfilterd` should be listed as an active process
    - configuration: `/var/config/ipfilterd.options` contains accept/reject rules for filtering
    - kernel configuration: `/var/sysgen/master.d/ipfilter` sets fail-safe mode, kernel table size for filtering rules
- Service control
  - completely block unneeded or dangerous services
    - some examples: `rexec`, `NFS`, `NIS`
    - don't forget to block informational services: `rwho`, `finger`
  - prevent forwarding of needed but dangerous services
    - incoming services offered to external net: `login`, `ftp`
    - outgoing services: `login`
  - forward most services only to relays
    - host/ip address resolution: DNS should only be allowed between company DNS server and outside world

- mail and news: mail and news should only be sent directly to dedicated mail and news forwarders
- allow safer services transparent access

### Packet Filter - Special Configuration Issues

- Addresses and routing
  - use filtering to prevent address spoofing
    - filter address spoofs: all packets received on the external interface should have source addresses from external nets
    - avoid loose source routing: block all packets with loose source routing
  - control routing updates
    - routing information packets (rip): block from going in or out
    - gateway routing: use gated on the gateway, accept only information about external routes from the external net
    - redirect messages: block icmp redirect packets, or only process them on gateways
- Testing: be especially wary of interactions between filter rules
- No special client setup needed

### Circuit Level Firewall

- Design
  - for TCP services only
  - all client applications connect only to firewall
  - firewall connects to outside network, copies data between connections
- Advantages
  - more information than is normally available from packet filters can be used to determine nature of connection
  - can prevent sequence number attacks and other more complex attacks
  - easier to log TCP connections and analyze logs
  - can be used in conjunction with authentication services to increase security
  - can be used to hide internal network topology (masquerading)
- Limitations
  - requires all TCP based services on clients to be modified, or new services to be used explicitly for outside connections
  - only feasible for TCP (connection based) services

### Implementing a Circuit-Level Firewall

- Firewall Setup
  - configure third-party proxy software to run on firewall
  - deactivate all network services on gateway which are not run through proxy software
  - block or filter packets going through gateway
  - Some available packages
    - TIS toolkit: includes common proxies for HTTP (Web), FTP, Telnet, as well as other protocols
    - socks: a library package for building your own proxies, xforward - proxy X11 for firewalls,

- Client setup
  - option 1: recompile existing client applications (e.g. telnet, ftp,) to use proxy gateway
  - option 2: create "remote" versions of client applications, explicitly for use in contacting the proxy firewall
  - option 3 (advanced): create "transparent" firewalls, with `ipfilterd`'s packet grabbing, and a proxy application
- Caveats
  - "free" software must be tested on your machine to ensure correct operation
  - third party vendor software - may have e more bugs than "free" software, make sure vendors test and certify their software
  - original vendor may not support your changes to the standard operating system, be careful to re-secure system after OS upgrades

## Application Level Firewall

- Design
    - create separate proxy/forwarder program for each service
    - run proxy server on firewall
    - internal hosts run modified clients that connect to firewall
    - firewall then connects to outside networks, forwards information
  - Advantages
    - maximum control over traffic in and out of the network
  - Limitations
    - more administrative work, a proxy has to be designed for each application service
    - potential for bugs in proxy program to threaten security
  - Implementation
    - essentially the same as circuit level firewall, with multiple proxy programs rather than a single proxy
- Gauntlet
- based on TIS toolkit
  - transparent proxies
  - SGI gui for configuration
  - easy setup of DNS hiding, mail proxies, other common services
  - allows IP encryption (SWIPE) to peers

## Special Issues

- Identification Server
- Common attacks
- Monitoring and logging
- Traps and lures

- Encryption
- Firewalls and performance

### Identification server

- Freeware identd server provides user level identification with each network connection
- Only useful for trusted internal systems
- Provides additional logging information, ability to screen outgoing connections

### Common attacks

- Passwords
  - guessing, cracking and spoofs
  - testing your password files
  - proactive password checkers
  - shadow password files
  - NIS password maps
- Impersonating trusted hosts
  - impersonation through loose source routing
  - impersonation through normal routing
  - impersonation through DNS & NIS
- Trojan horses, etc.
  - login spoofs
  - integrity checks
    - TRIPWIRE: package for monitoring system file integrity
- Bugs in services

### Monitoring and logging

- Obtaining more information
  - resource accounting
  - process accounting
  - keystroke monitoring
  - network connection monitoring
    - login monitoring
    - identification wrappers
- Protecting logs

### Supplementing The Firewall

- Encryption
  - passwords
    - Kerberos
    - OPIE (formerly S/Key) - one time passwords
  - mail
    - PGP - public key encryption and authentication

- documents
- http connections (SSL, SET)
- filesystems: TCFS/CFS
- sessions
  - SSH - secure shell, logins and copies, secure X-windows
  - Gauntlet - can provide encrypted end-to-end sessions

- Traps and lures
  - accounts
  - files
  - hosts

### Limitations of a Firewall

- Firewalls and performance
- Types of attacks
  - easiest to protect against attacks from outside
  - can limit deliberate information leakage
  - those determined to leak information from the inside will be able to do so
- Trojans Horses, Worms, Viruses
  - downloaded by users inside the firewall
  - triggered by users browsing web pages and using Java, JavaScript, VisualBasic, Plug-ins and especially Activex
  - mailed to users
  - use Tripwire/auditing to detect changes to your system
- Physical security
  - security has many components, overall security only as strong as weakest component
  - information leaks may occur by "sneakernet"
  - attacks on network may occur by modem

### More Limitations of Firewalls

- Information in transit
  - even if you are using a firewall, once information leaves your network it is visible
  - passwords, mail, telnet sessions are all clear-text
  - use mail encryption, one-time passwords
    - s/key : software one-time password generating mechanism
    - PEM, RIPEM, PGP: some mail-encryption/digital signature packages
- Continuous monitoring

### References and Further Information

- Books
  - Chapman, Brett and Elizabeth Zwicky 1994. *Building Internet Firewalls*, O'Reilly & Associates, Inc.: California

Constructing Firewalls (Lecture Notes), by Micah Altman

Cheswick, William R. and Steven M. Bellovin 1998. *Firewalls and Internet Security* (2nd edition),  
Addison-Wesley Publishing Co.: U.S.A.

Garfinkel, Simson and Gene Spafford 1997. *Practical Unix and Internet Security*,  
O'Reilly & Associates, Inc.: California

Hunt, Craig, 1992. *TCP/IP Network Administration*,  
O'Reilly & Associates, Inc.: California

Stoll, Clifford 1990., *The Cuckoo's Egg*,  
Shimon and Schuster: New York

- Newsgroups

- comp.security.misc, comp.security.unix, comp.answers and  
news.answers

- FAQ's

- Secure Shell FAQ

- <http://www.uni-karlsruhe.de/~ig25/ssh-faq/ssh-faq.sgml>

- Firewall FAQ

- <http://www.v-one.com>

- Unix Security FAQ's

- <http://www.iss.net/ftp> ftp.iss.net/pub/

- Linux Firewall FAQ and Software

- <http://www.xos.nl/linux/ipfwadm>