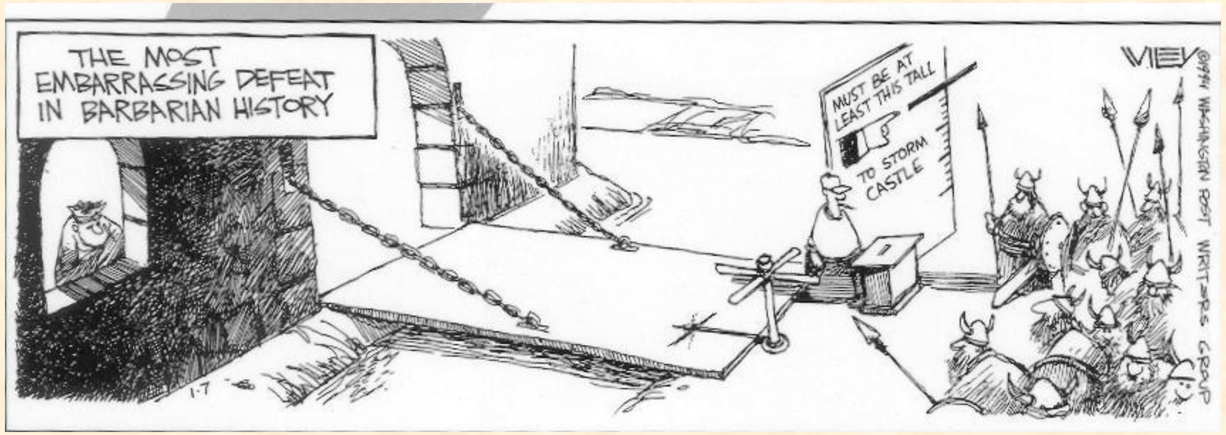
Thanks to Tom Dunigan @ UTK

Network defenses

firewalls


THE MOST EMBARRASSING DEFEAT IN BARBARIAN HISTORY
MUST BE AT LEAST THIS TALL
TO STORM CASTLE
VIEY
©1994 WASHINGTON POST WRITERS GROUP
1-7

In the news

- Man draws 10 yr sentence for sending trojans, blackmailing minors
- Denial of service now punishable by 10 yr sentence in UK
- Phishers spoofing Social Security Administration
- Judge shuts down spyware and malware purveyors

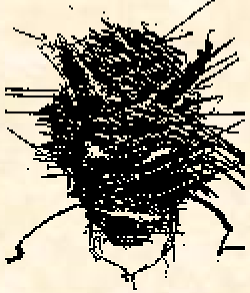
Network defenses

- **disable**
- **configure properly**
- **xinetd, tcpwrappers**
  - filters (allow, deny)
  - audit and alarm
- **filtering portmap**
- **application filtering (securelib)**
- **patches**
- **scanners (Nessus, SATAN, ISS)**
- **firewalls**
- **intusion detection & response**
- **encryption, IPsec, virtual private networks (VPNs)**

Defense in depth

- on a hill
- moat
- outer wall
- archer towers
- inner wall

Assess your attack surface



Scanners

ISS, Nessus,nmap -- probe and report network hosts and services

- point, click, scan a net
- port probes (nmap)
- OS type probes (nmap)
- portmap probes
- X and NFS attempts
- sendmail checks
- NIS probes

Network countermeasures

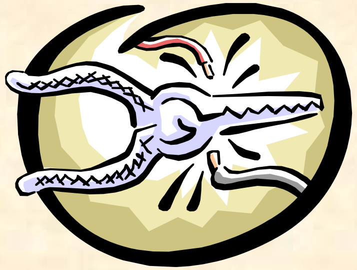
- host-based (wrappers, personal firewalls)
- router based (filters)
- firewalls
- Intrusion Detection Systems (IDS/IPS)
- authentication/encryption (IPsec/VPNs)

Host network services “wrappers”

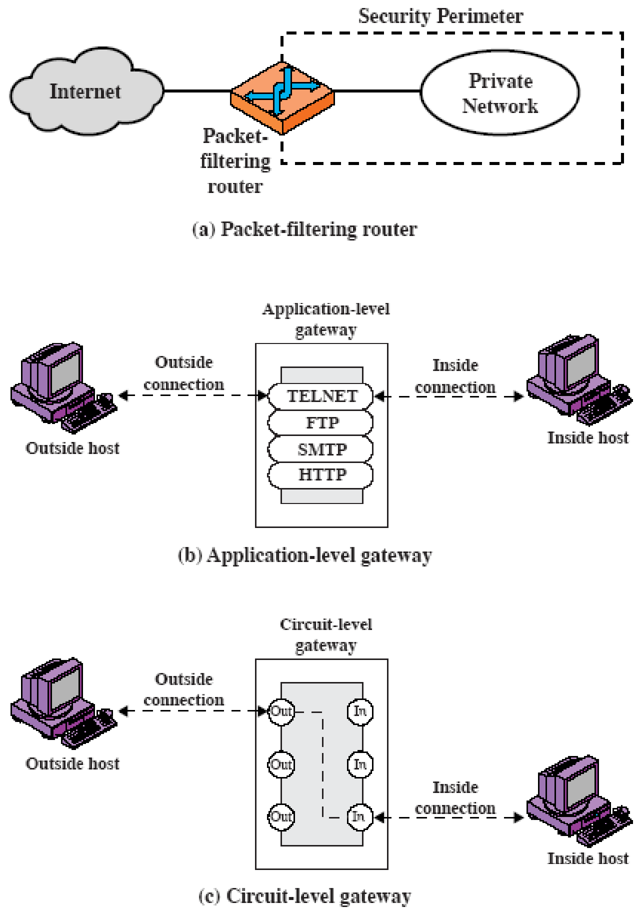
- **network/host access control lists**
- **re-write applications with filters (securelib)**
- **replace inetd with filtering version (xinetd)**
- **use tcp wrappers**
  - free, no changes to application
  - inetd services only
  - allow/deny
  - double DNS lookups
  - audit and alarm
  - API for new app’s

```
/etc/inetd.conf
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  wu.ftpd
telnet  stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
shell   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd -L
login   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind

/etc/hosts.deny
in.rlogind: ALL
in.telnetd: ALL
in.rshd: ALL
wu.ftpd: ALL

/etc/hosts.allow
in.rlogind: 128.219., 134.167., 127.
in.telnetd: 128.219., 134.167., 127.
wu.ftpd: 128.219., 134.167., 127.
in.rshd: 128.219., 134.167.
```

firewalls



- NO connection -- best ☺
- toolkits, personal firewalls (Linux, PC)
- filtering/screening routers
- dual-homed gateways (bastion host)
- screened host gateway
- screened subnet (NAT)
- commercial solutions (enterprise firewalls)



(a) Packet-filtering router

(b) Application-level gateway

(c) Circuit-level gateway

Figure 20.1 Firewall Types

Personal (host) firewalls

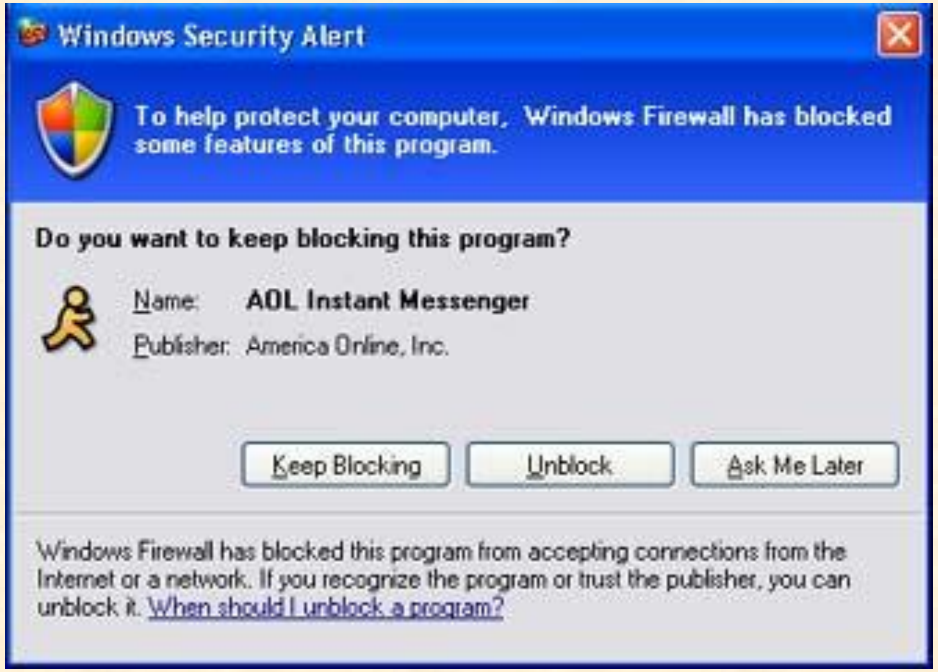
- **Network access control lists**
  - Which hosts/nets you permit/deny
  - Which services you permit/deny
  - Make your host invisible to net (ping/port scans)
- **PC/Windows – XP firewall (ICF), ZoneAlarm, NetIce**
- **Linux – iptables**
- **MAC – ipfw**

Difficult to configure and EVERY host needs to do it.

If bad guy gets in to your host, he’ll disable your host’s firewall.

Windows firewall

- **Security Center (firewall, auto updates, viruses)**
  - Blocks outside requests
  - Alerts if program attempts to use Internet
  - Add exceptions (program or port)
  - Keeps a log



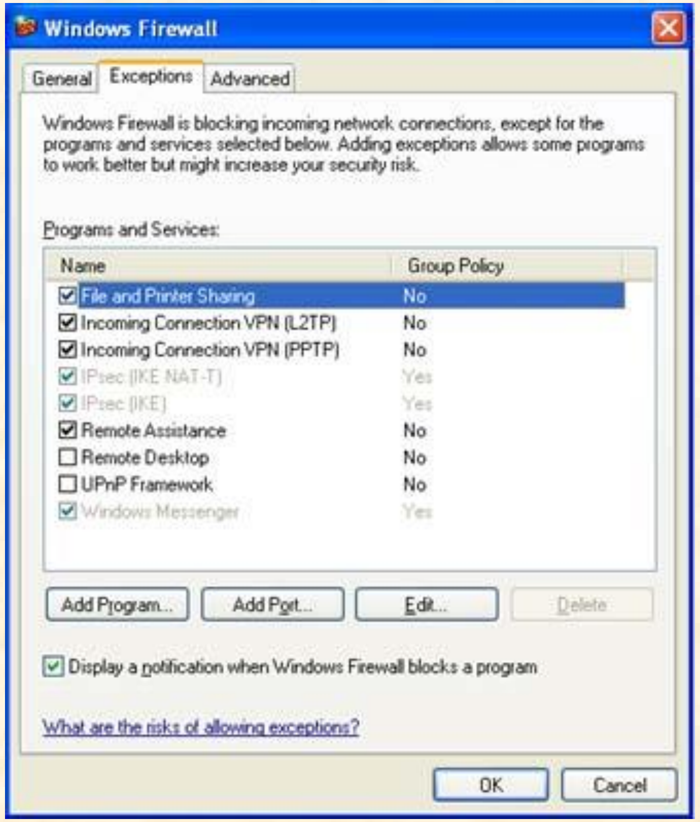
To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: AOL Instant Messenger

Publisher: America Online, Inc.

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

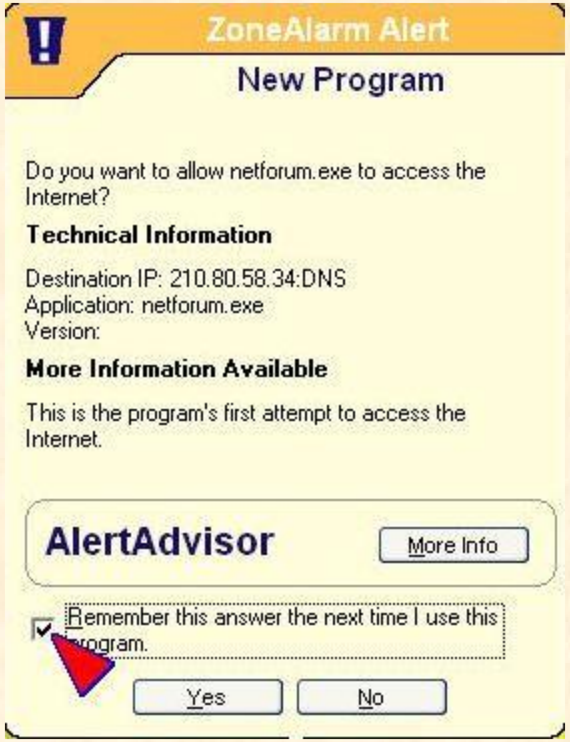
Programs and Services:

Name	Group Policy
☑ File and Printer Sharing	No
☑ Incoming Connection VPN (L2TP)	No
☑ Incoming Connection VPN (PPTP)	No
☑ IPsec (IKE NAT-T)	Yes
☑ IPsec (IKE)	Yes
☑ Remote Assistance	No
☐ Remote Desktop	No
☐ UPnP Framework	No
☑ Windows Messenger	Yes

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

zonealarm



ZoneAlarm Alert

New Program

Do you want to allow netforum.exe to access the Internet?

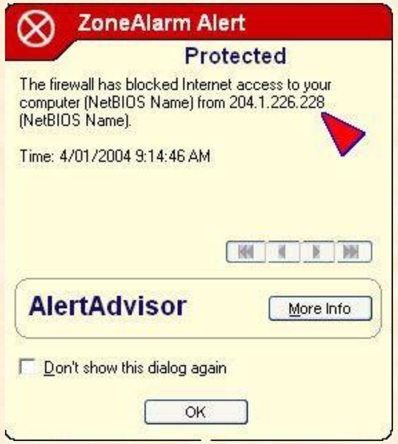
Technical Information

Destination IP: 210.80.58.34:DNS
Application: netforum.exe
Version:

More Information Available

This is the program's first attempt to access the Internet.

☑ Remember this answer the next time I use this program.



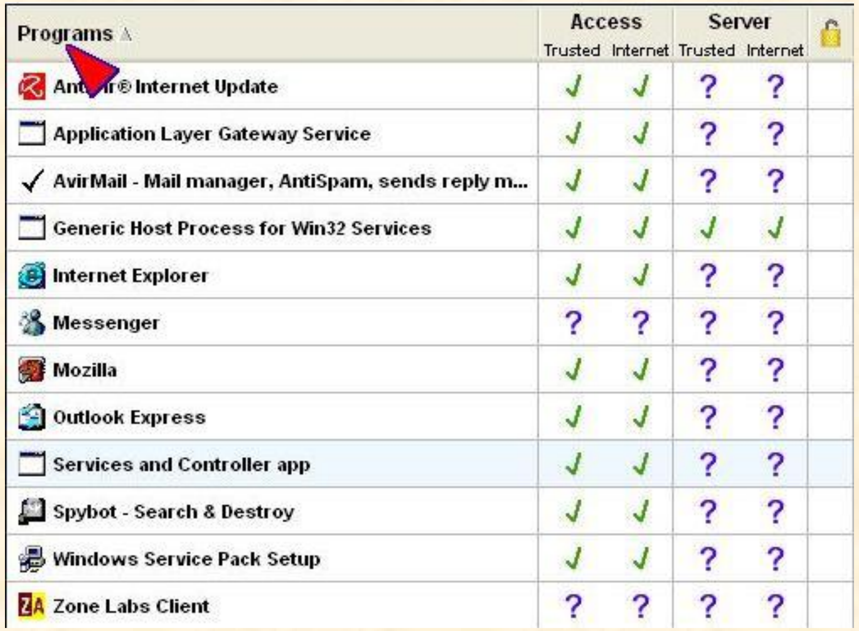
ZoneAlarm Alert

Protected

The firewall has blocked Internet access to your computer (NetBIOS Name) from 204.1.226.228 (NetBIOS Name).

Time: 4/01/2004 9:14:46 AM

□ Don't show this dialog again



Programs	Access		Server		
	Trusted	Internet	Trusted	Internet	
Ant ir® Internet Update	✓	✓	?	?	
Application Layer Gateway Service	✓	✓	?	?	
AvirMail - Mail manager, AntiSpam, sends reply m...	✓	✓	?	?	
Generic Host Process for Win32 Services	✓	✓	✓	✓	
Internet Explorer	✓	✓	?	?	
Messenger	?	?	?	?	
Mozilla	✓	✓	?	?	
Outlook Express	✓	✓	?	?	
Services and Controller app	✓	✓	?	?	
Spybot - Search & Destroy	✓	✓	?	?	
Windows Service Pack Setup	✓	✓	?	?	
Zone Labs Client	?	?	?	?	

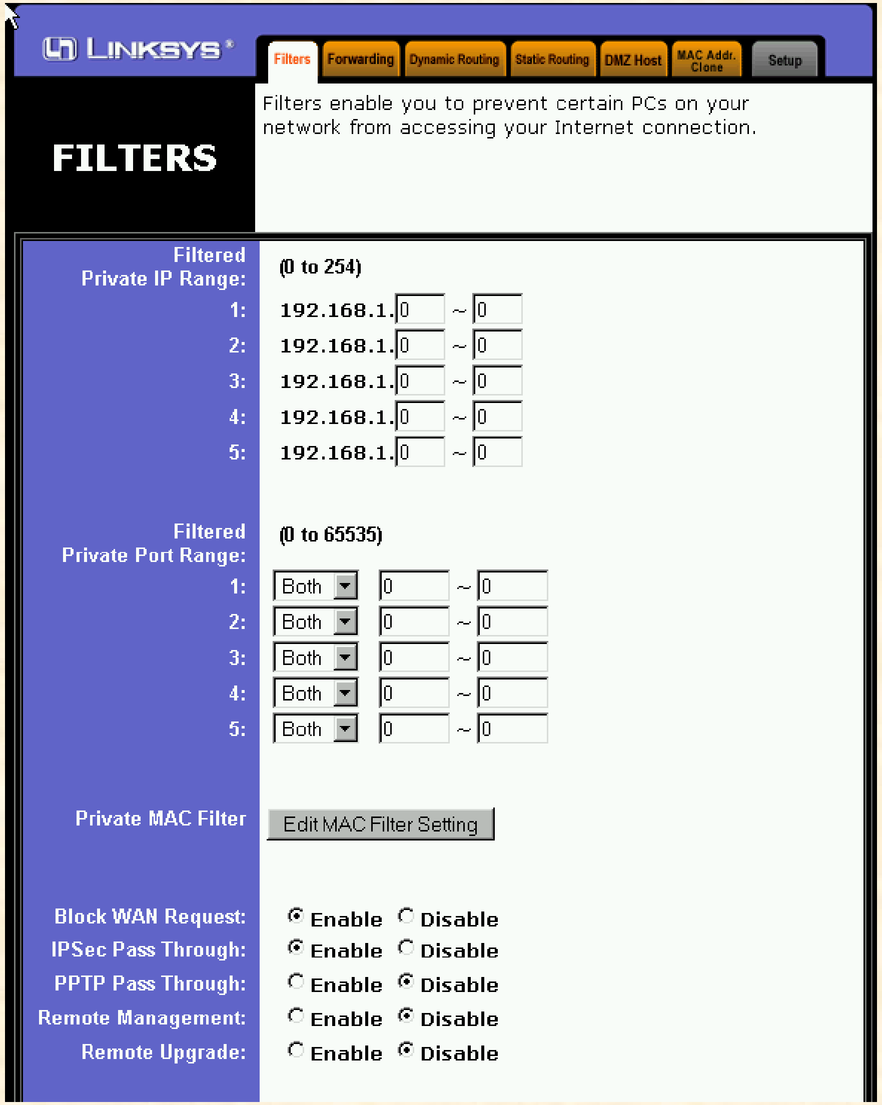
Linux firewalls

- **ipfwadm begat ipchains begat iptables**
- **accept/reject rules (tables) + logging**
- **RedHat select security (high, medium, none)**
- **provides Network Address Translation (NAT), masquerading**
  - IPforwarding (private nets 10.0.0.0, 172.16.0.0,192.168.0.0)

```
iptables -F iptables -A INPUT -i lo -p all -j ACCEPT - Allow self access by loopback interface

iptables -A OUTPUT -o lo -p all -j ACCEPT

iptables -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT - Accept established connections

iptables -A INPUT -p tcp --tcp-option ! 2 -j REJECT --reject-with tcp-reset iptables -A INPUT -p tcp -i eth0 --
dport 21 -j ACCEPT - Open ftp port

iptables -A INPUT -p udp -i eth0 --dport 21 -j ACCEPT

iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT - Open secure shell port

iptables -A INPUT -p udp -i eth0 --dport 22 -j ACCEPT

iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT - Open HTTP port

iptables -A INPUT -p udp -i eth0 --dport 80 -j ACCEPT

iptables -A INPUT -p tcp --syn -s 192.168.10.0/24 --destination-port 139 -j ACCEPT - Accept local network Samba
connection

iptables -A INPUT -p tcp --syn -s trancas --destination-port 139 -j ACCEPT

iptables -P INPUT DROP - Drop all other connection attempts. Only connections defined above are allowed.
```

Home protection

- **Personal PC firewalls (ZoneAlarm, iptables)**
- **DSL/Cable**
  - Inexpensive router, NAT, firewall
  - Home network with perimeter protection
- **Wireless**
  - Enable WPA key
  - Accept only designated ether addresses (MAC filter)
  - Disable SSID broadcast
  - Use ssh or VPN
- **Review logs**



FILTERS

Filters enable you to prevent certain PCs on your network from accessing your Internet connection.

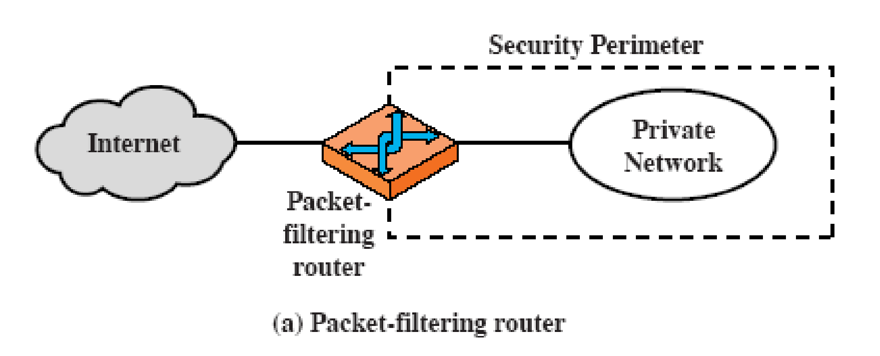
Filtered Private IP Range:	(0 to 254)
1:	192.168.1.0 ~ 0
2:	192.168.1.0 ~ 0
3:	192.168.1.0 ~ 0
4:	192.168.1.0 ~ 0
5:	192.168.1.0 ~ 0

Filtered Private Port Range:	(0 to 65535)	
1:	Both	0 ~ 0
2:	Both	0 ~ 0
3:	Both	0 ~ 0
4:	Both	0 ~ 0
5:	Both	0 ~ 0

Private MAC Filter: Edit MAC Filter Setting

Block WAN Request: ● Enable ○ Disable
IPSec Pass Through: ● Enable ○ Disable
PPTP Pass Through: ○ Enable ● Disable
Remote Management: ○ Enable ● Disable
Remote Upgrade: ○ Enable ● Disable

Screening routers



(a) Packet-filtering router

- **router's job is to forward packets (fast)**
- **add filters (ACL's) for each interface**
- **can block IP address spoofing of internal addresses**
- **should permit out only legit. local addresses**
- **may deny/restrict specific services (ports)**
- **weaknesses**
  - complicated filter expressions
  - may fail to the open mode
  - limited logging
  - no authentication
  - DNS spoofing

Port deny list:

portmap, tftp, snmp, syslog, telnet

Restrict http to designated servers

Screening routers -- rules

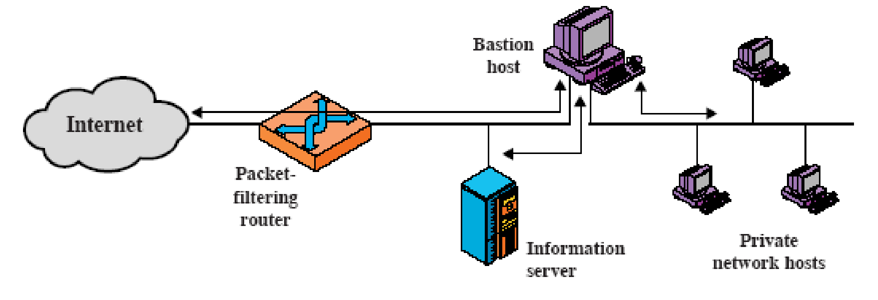
```
! access list  102 specifies what addresses are allowed out
access-list 102 deny   ip 128.219.250.0 0.0.1.255 0.0.0.0 255.255.255.255
! no snmp out
access-list 102 deny   udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 162
access-list 102 permit ip 128.219.0.0 0.0.255.255 0.0.0.0 255.255.255.255
access-list 102 permit ip 134.167.0.0 0.0.255.255 0.0.0.0 255.255.255.255
access-list 102 permit ip 192.12.68.0 0.0.0.255 0.0.0.0 255.255.255.255

! access list  112 denies local addresses from the outside
access-list 112 deny ip 128.219.0.0   0.0.255.255 0.0.0.0 255.255.255.255
access-list 112 deny ip 134.167.0.0   0.0.255.255 0.0.0.0 255.255.255.255
access-list 112 deny ip 192.12.68.0   0.0.0.255   0.0.0.0 255.255.255.255
! block a known bad guy
access-list 112 deny ip 130.225.220.16 0.0.0.0 0.0.0.0 255.255.255.255
! deny remote SNMP's and tftp's
access-list 112 deny   udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 161
access-list 112 deny   udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 69
! special internal hosts
access-list 112 deny   ip 0.0.0.0 255.255.255.255 128.219.250.0 0.0.1.255
```

other rules for what routes are advertised

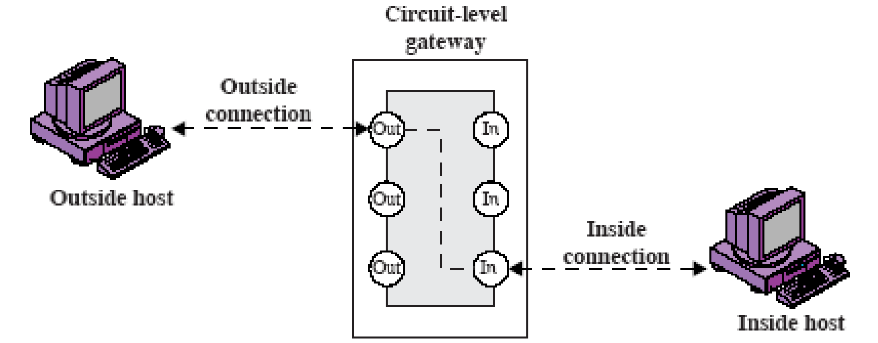
Bastion host

dual-homed (hardened) gateway

- host with two network interfaces
- IP forwarding disabled
- reachable from either side, but packets do not flow from one side to the other
- user must login to bastion host, then to other side
- supplement with application gateway software (email, ssh)
- strong authentication (Securid), logging (hardened host)
- limited services (restricted shell), wrappers
- custom mail programs
- hides enterprise network (private IP addresses)



(b) Screened host firewall system (dual-homed bastion host)

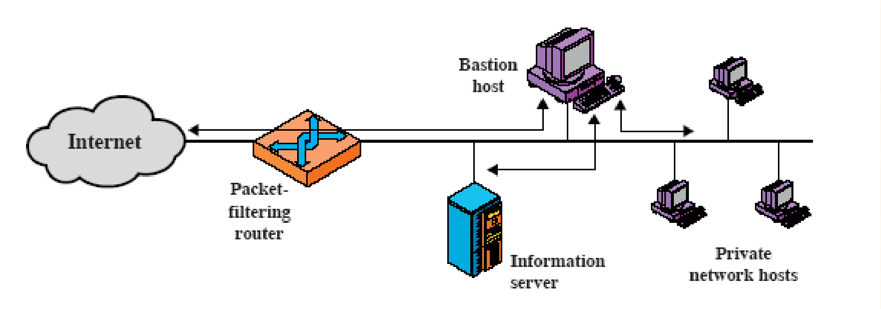


(c) Circuit-level gateway

Screened host/net

Screened host

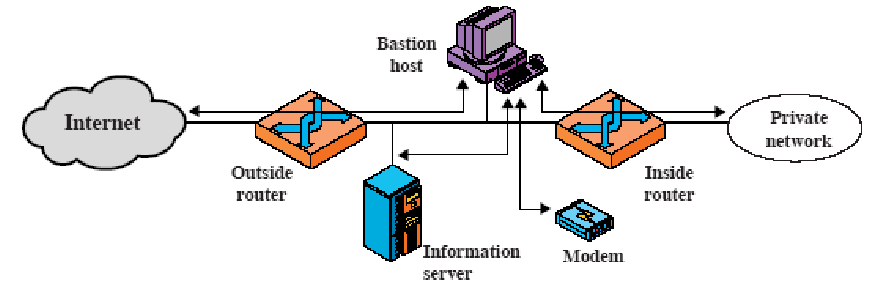
- common implementation
- traffic to/from Internet allowed only to bastion host, though can let internal hosts access some Internet services (ssh, ftp, www)
- bastion host acts as application gateway



(a) Screened host firewall system (single-homed bastion host)

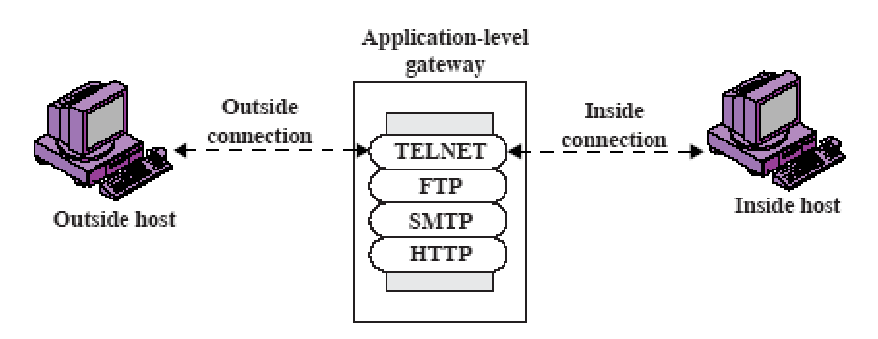
Screened subnet (DMZ)

- two screening routers
- one or more bastion hosts on subnet
- internal net can be private (invisible), network
- address translation (NAT)
- place some servers on DMZ (www, anon ftp)
- place intrusion detectors, traps on DMZ
- place external DNS on DMZ



(c) Screened-subnet firewall system

Application gateways

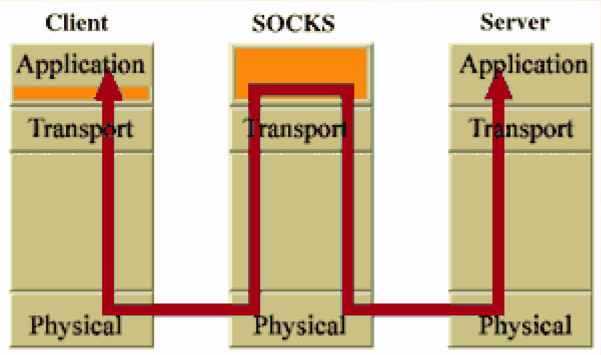


(b) Application-level gateway

proxy services on the bastion host

- **run minimal services (trusted OS?)**
- **no compilers, linkers**
- **use wrappers**
- **no local logins**
- **custom servers (minimal pkt forwarders, logging, ACLs)**
- **connections from outside**
  - strong authentication (skey, securID)
  - encrypted (ssh, stel)
  - user then connects to internal host and logs in again
- **2-part mail forwarder/scanner (IPS)**
  - Remove evil attachments
  - Block spam

Proxy servers

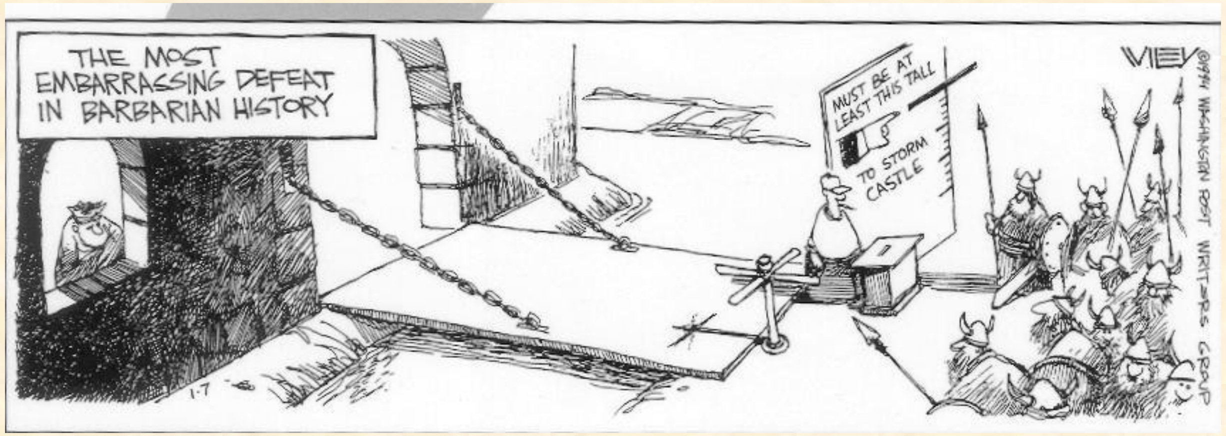


internal hosts accessing the outside (“relay”)

- need socks-ified local applications

  #define connect Sconnect
- proxy on bastion host (tn-gw, rlogin-gw, ftp-gw, x-gw, http-gw)
- servers are simple packet forwarders with ACL, e.g., telnet and an itelnet
- some services support proxies (netscape, gopher)
- socks library for building your own local apps

Enterprise firewalls


THE MOST EMBARRASSING DEFEAT IN BARBARIAN HISTORY
MUST BE AT LEAST THIS TALL TO STORM CASTLE
WIEV
©1994 WASHINGTON POST WRITERS GROUP
1-7

router with an attitude

- **establish a perimeter**
- **single point of protection (rather than host by host)**
  - Controls inbound and outbound network flows (by hosts/service)
  - logs
- **principle of layering, reference monitor**
  - always invoked
  - tamper resistant
  - small and simple (understandable)

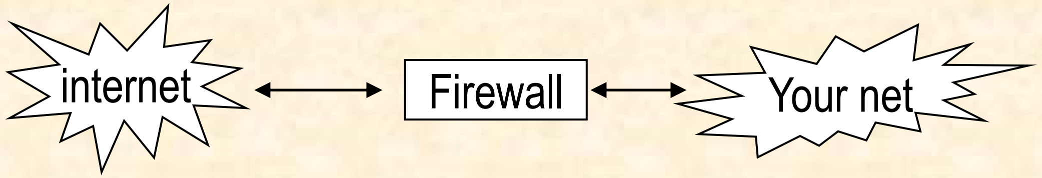
establish a policy

- **What's not denied is allowed**
- **What's not allowed is denied -- best**
- **Complicated rules**

security vs convenience

Enclaves

use firewalls and VLANs to create internal protected subnets (e.g., business subnet, medical subnet,)



internet ↔ Firewall ↔ Your net

Firewall limitations

What they don't do?

- **don't do UDP very well**
- **don't prevent session hijacking**
- **don't provide privacy**
- **don't protect against viruses**
- **don't protect against insider (need internal firewalls/enclaves)**
- **don't prevent backdoors (modems, VPNs/tunnels)**
- **don't log/alarm like an IDS – some do**
- **don't improve throughput!**

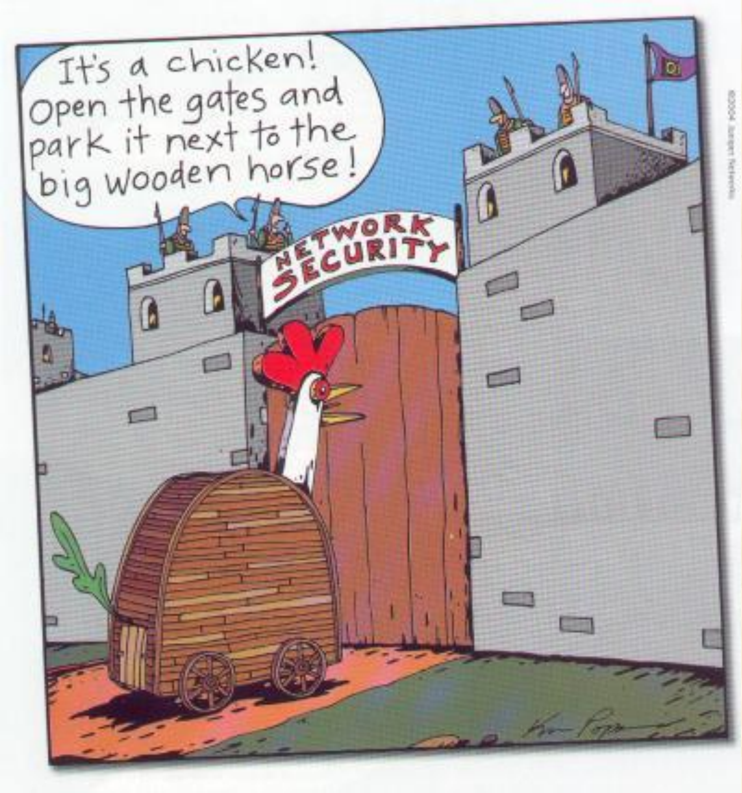
Watch out for tunneling through “permitted” ports (trojan horse)

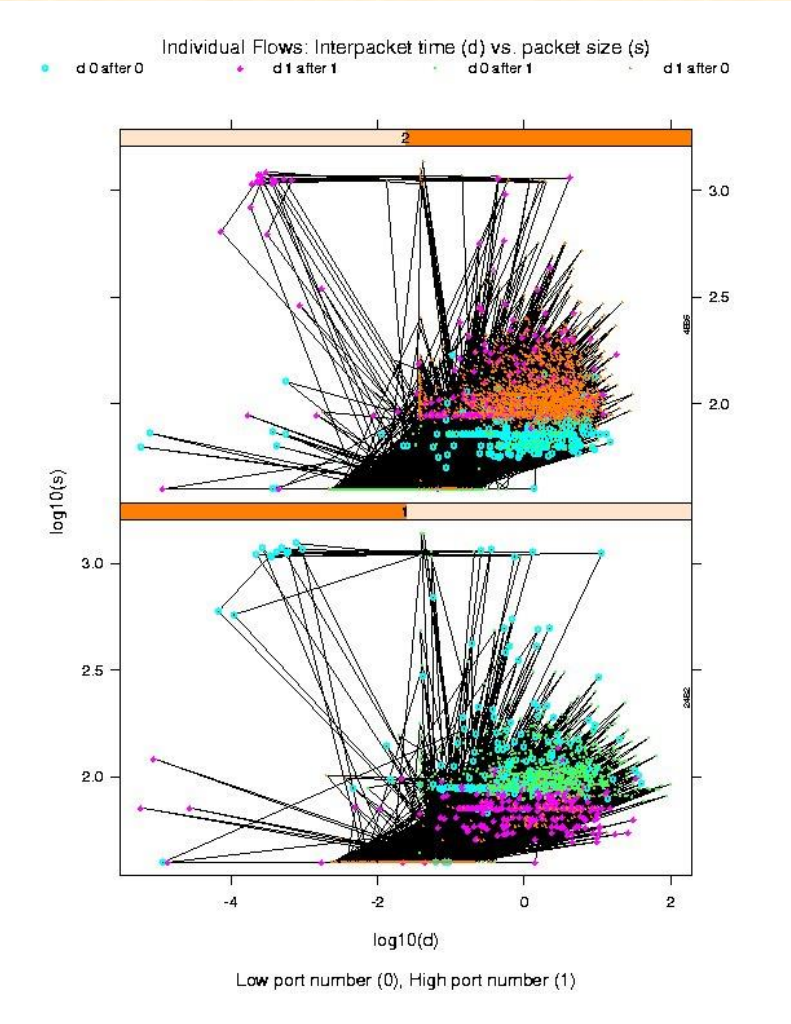
Selecting an enterprise firewall

- commercial, consultant, kit
- filters for both in and out
- filter granularity (stateful, ftp support)
- IP fragment management
- filter language and user interface
- proxy applications, clients, extensible
- authentication mechanisms
- network address translation (NAT) and VPN
- integration with intrusion detection (IPS)
- IPv6
- logging and audit tools
- ease of install and use
- performance
- cost

Flow characterization

Firewalls allow only certain services to flow. Hackers often will trojan an allowed service, e.g., use port 80 to carry ssh traffic


It's a chicken! Open the gates and park it next to the big wooden horse!
NETWORK SECURITY



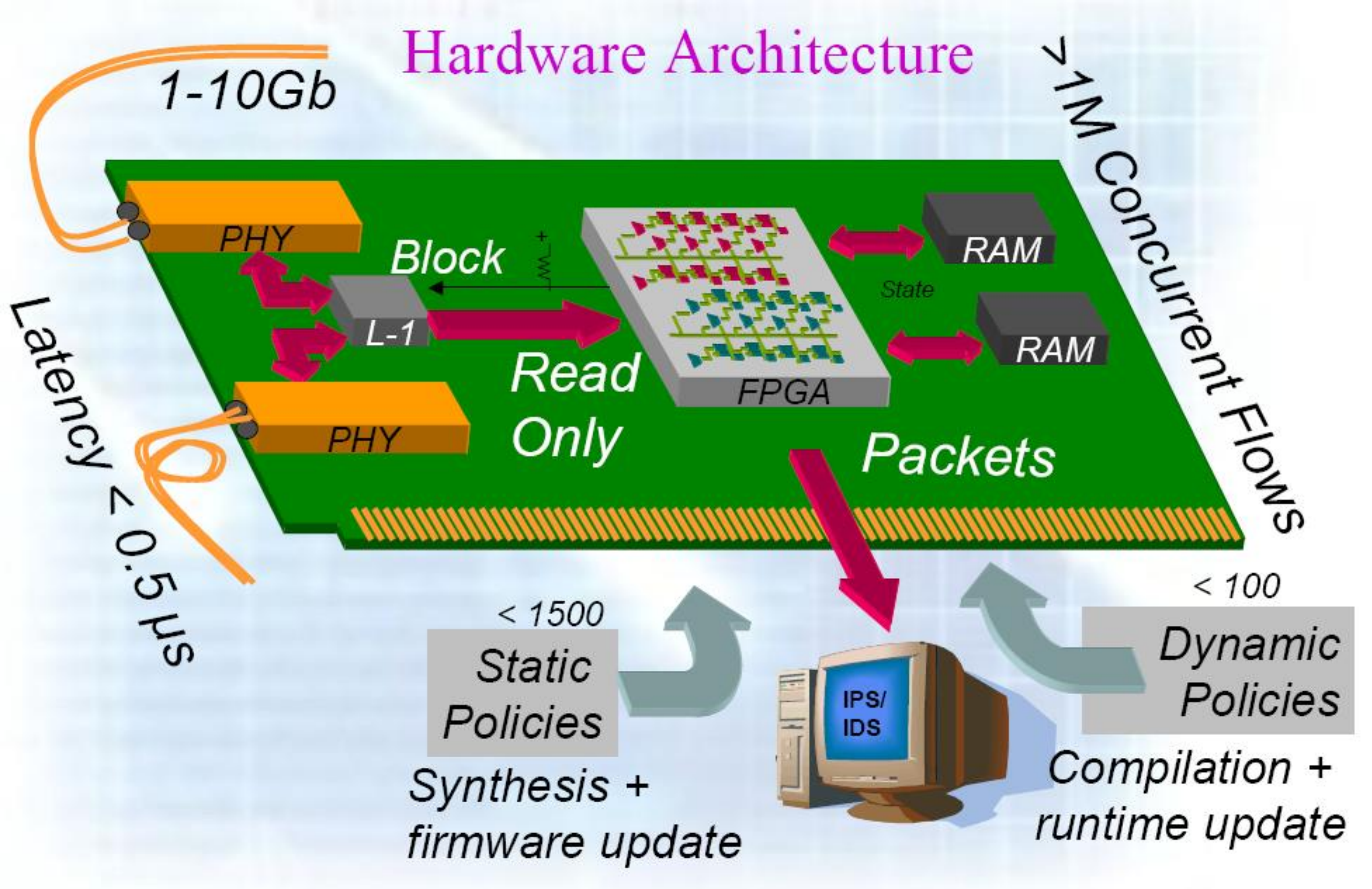
Two flows from a compromised host

Can you characterize a flow (mail, telnet/ssh, www, chat) based on flow stats (interarrival rate, packet size, volume, duration)?

Backtracking spoofed IP address flows

- **Spoofed IP source addresses used by Denial of Service and session hijacking**
- **Perimeter routers SHOULD block spoofed addresses**
  - Don’t allow internal addresses as source address from external interfaces
  - Only allow packets with valid source addresses out
- **For an active attack that is using spoofed IP source addresses**
  - Manually check each router along the flow, backtracking
  - Automated program to access routers and backtrack flow and setting filter to block
  - Hard: crosses administrative domains
- **Other approaches, marking packets, new ICMP … open research**

High speed IDS (10-100gbs)


Hardware Architecture
1-10Gb
>1M Concurrent Flows
PHY
Block
RAM
State
L-1
RAM
Read Only
FPGA
PHY
Latency < 0.5 μs
Packets
< 1500
< 100
Static Policies
IPS/ IDS
Dynamic Policies
Synthesis + firmware update
Compilation + runtime update