Fundamentals of Information & Network Security ECE 471/571

Lecture #40: Firewalls

Instructor: Ming Li

Dept of Electrical and Computer Engineering

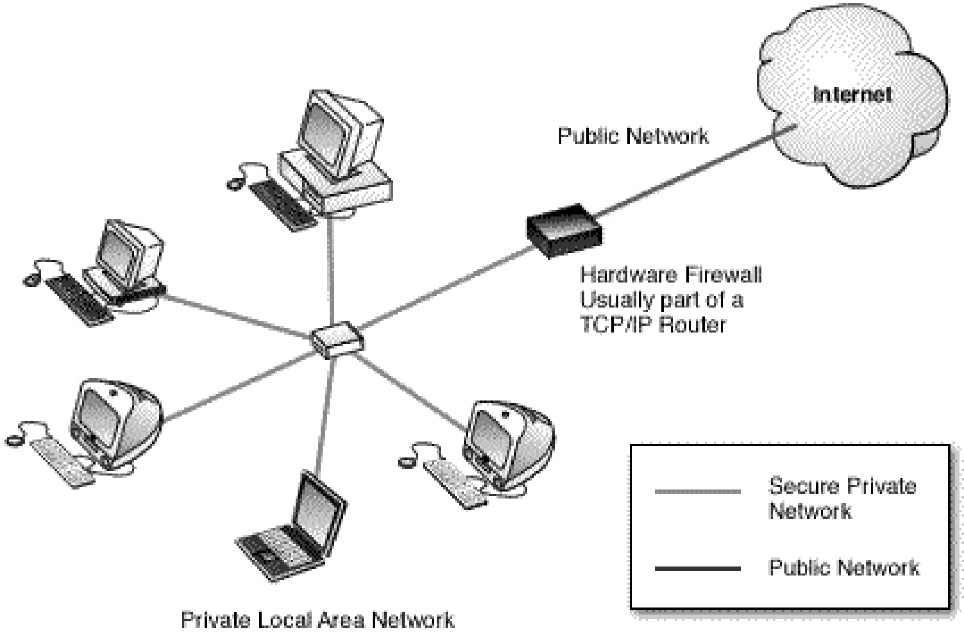
University of Arizona

What is a Firewall?

- Appeared in 90’s, but reflect *reference monitor* concepts from the 70’s.
- A computer system between the internal network and the rest of the Internet
  - Usually runs on a dedicated devices - a single computer or a set of computers - why?
  - Protect the internal network from Internet based attacks
  - A single choke point to impose security and audit

Security Guard for Private Buildings

Firewalls


Internet
Public Network
Hardware Firewall
Usually part of a
TCP/IP Router
Secure Private
Network
Public Network
Private Local Area Network

Design Goals

- All traffic from inside to outside, or outside to inside, must pass through the firewall - Configuration
- Only authorized traffic allowed to pass – Security policy
- The firewall itself is secure.
- Always invoked
- Small and simple enough for rigorous analysis
- Default deny vs. default permit?
  - Specific policy can be defined by an admin.

Types of Firewalls

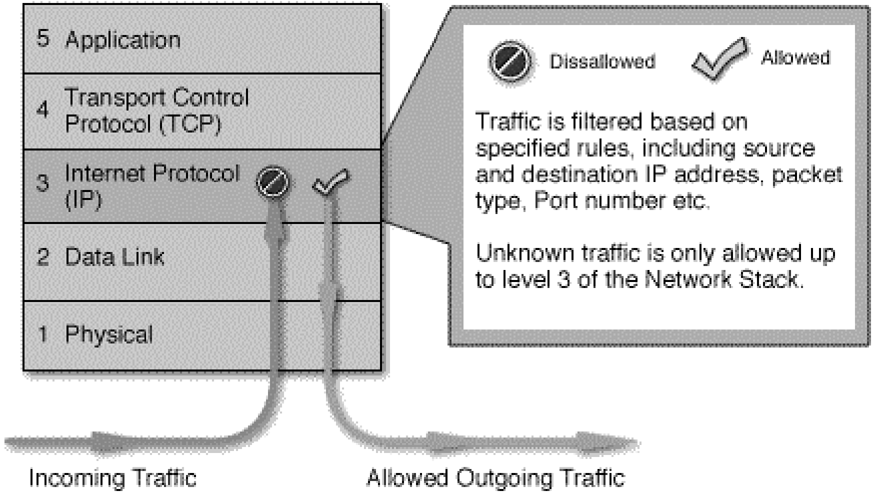
- Packet filtering gateway (screening router).
- Statefull inspection firewall
- Application proxy
- Personal firewall

Packet Filters

- Apply rules to each incoming IP packet and then forward or discard the packet
- Rules based on information contained in the packet
  - Source IP address
  - Destination IP address
  - Source and destination transport level address
  - IP protocol field
  - Interface
- Default policy: discard/forward

Packet filters

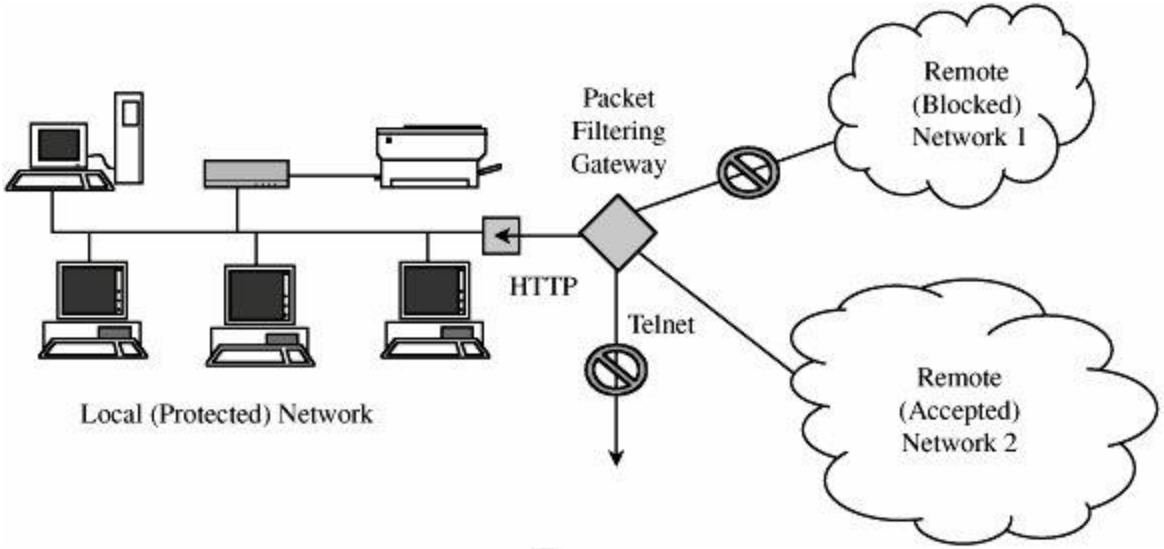
- A packet conveys the following information
  - Source IP address and port
  - Destination IP address and port
  - Information about the protocol
  - Error checking information

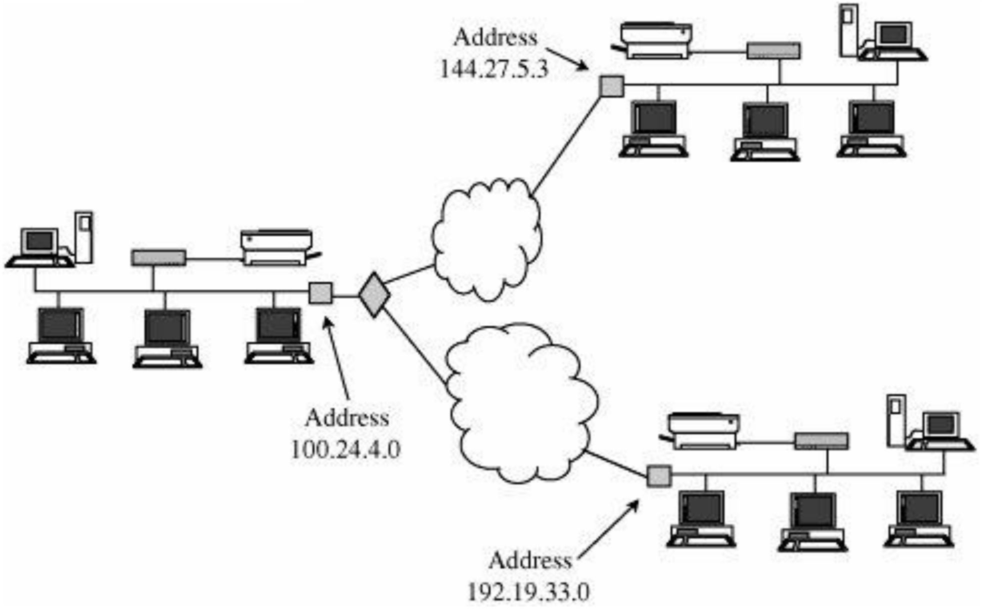


Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.

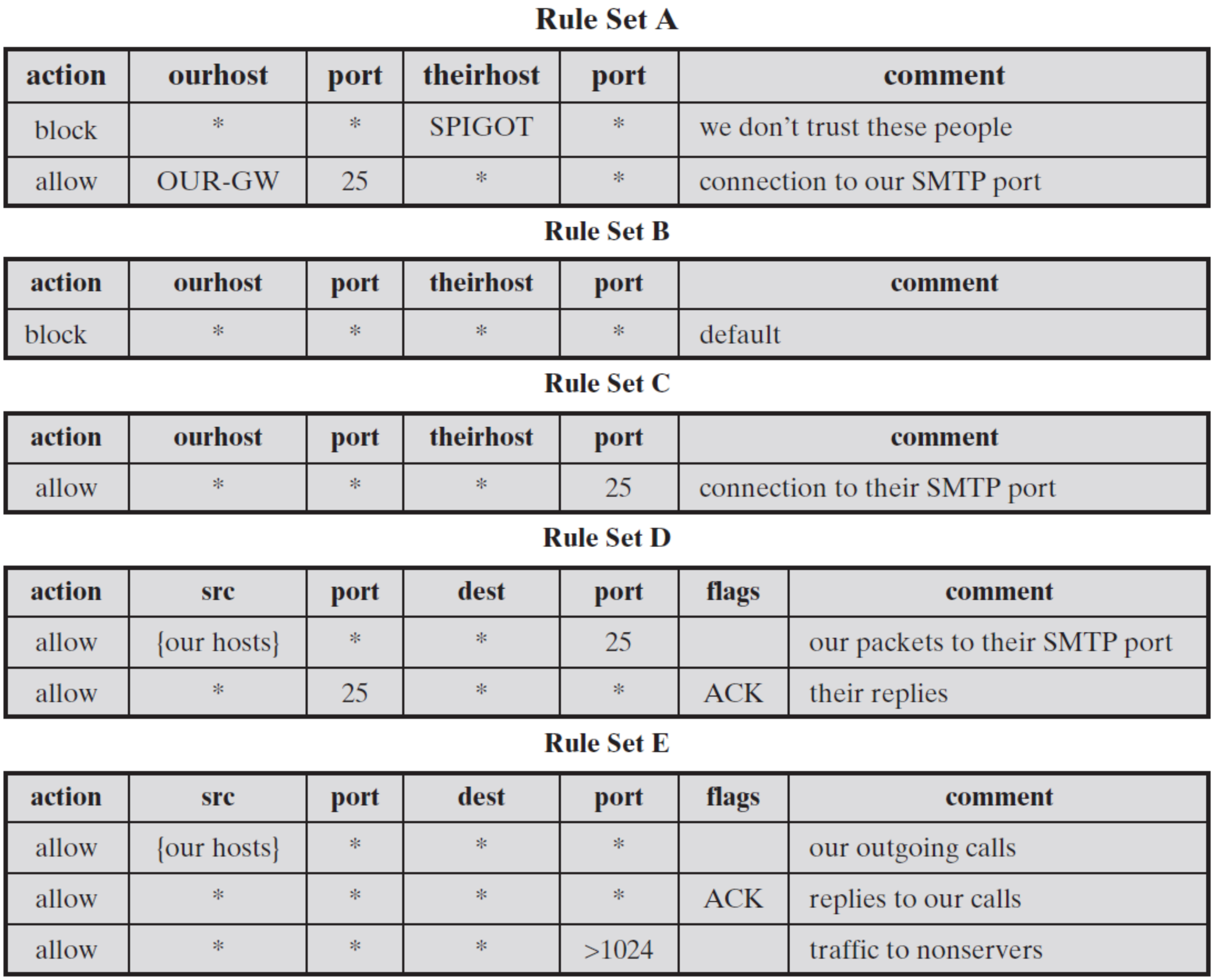
Unknown traffic is only allowed up to level 3 of the Network Stack.

Packet filters





Packet Filtering Examples



Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

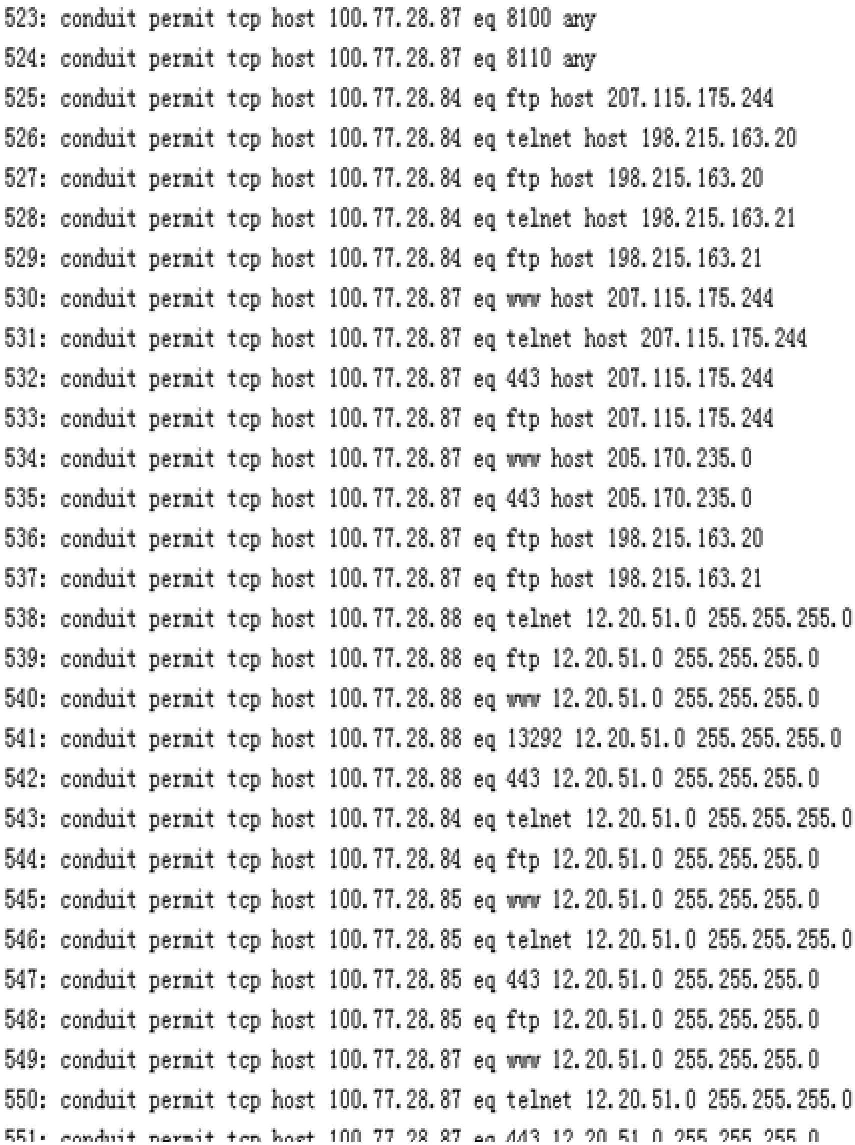
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Real-life Firewalls are Complex

Number of rules can be large

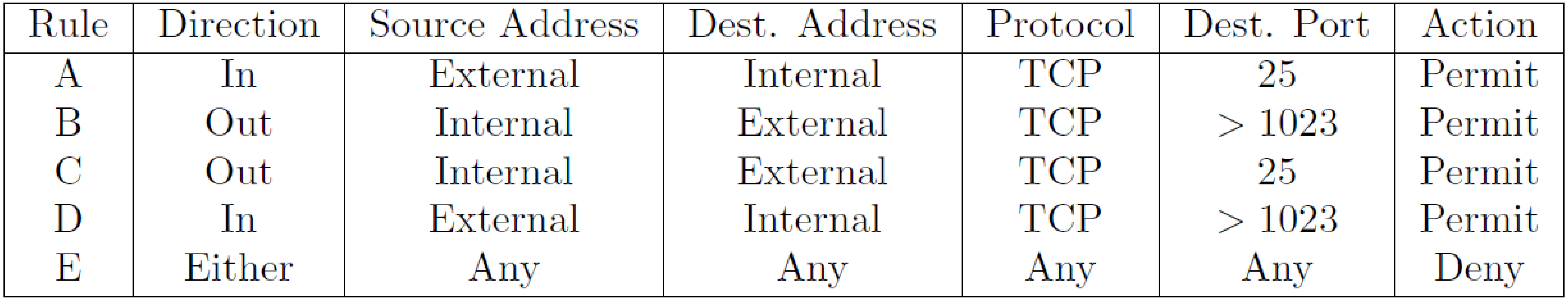
Legacy rules

Cascade impact of change



```
523: conduit permit tcp host 100.77.28.87 eq 8100 any
524: conduit permit tcp host 100.77.28.87 eq 8110 any
525: conduit permit tcp host 100.77.28.84 eq ftp host 207.115.175.244
526: conduit permit tcp host 100.77.28.84 eq telnet host 198.215.163.20
527: conduit permit tcp host 100.77.28.84 eq ftp host 198.215.163.20
528: conduit permit tcp host 100.77.28.84 eq telnet host 198.215.163.21
529: conduit permit tcp host 100.77.28.84 eq ftp host 198.215.163.21
530: conduit permit tcp host 100.77.28.87 eq www host 207.115.175.244
531: conduit permit tcp host 100.77.28.87 eq telnet host 207.115.175.244
532: conduit permit tcp host 100.77.28.87 eq 443 host 207.115.175.244
533: conduit permit tcp host 100.77.28.87 eq ftp host 207.115.175.244
534: conduit permit tcp host 100.77.28.87 eq www host 205.170.235.0
535: conduit permit tcp host 100.77.28.87 eq 443 host 205.170.235.0
536: conduit permit tcp host 100.77.28.87 eq ftp host 198.215.163.20
537: conduit permit tcp host 100.77.28.87 eq ftp host 198.215.163.21
538: conduit permit tcp host 100.77.28.88 eq telnet 12.20.51.0 255.255.255.0
539: conduit permit tcp host 100.77.28.88 eq ftp 12.20.51.0 255.255.255.0
540: conduit permit tcp host 100.77.28.88 eq www 12.20.51.0 255.255.255.0
541: conduit permit tcp host 100.77.28.88 eq 13292 12.20.51.0 255.255.255.0
542: conduit permit tcp host 100.77.28.88 eq 443 12.20.51.0 255.255.255.0
543: conduit permit tcp host 100.77.28.84 eq telnet 12.20.51.0 255.255.255.0
544: conduit permit tcp host 100.77.28.84 eq ftp 12.20.51.0 255.255.255.0
545: conduit permit tcp host 100.77.28.85 eq www 12.20.51.0 255.255.255.0
546: conduit permit tcp host 100.77.28.85 eq telnet 12.20.51.0 255.255.255.0
547: conduit permit tcp host 100.77.28.85 eq 443 12.20.51.0 255.255.255.0
548: conduit permit tcp host 100.77.28.85 eq ftp 12.20.51.0 255.255.255.0
549: conduit permit tcp host 100.77.28.87 eq www 12.20.51.0 255.255.255.0
550: conduit permit tcp host 100.77.28.87 eq telnet 12.20.51.0 255.255.255.0
551: conduit permit tcp host 100.77.28.87 eq 443 12.20.51.0 255.255.255.0
```

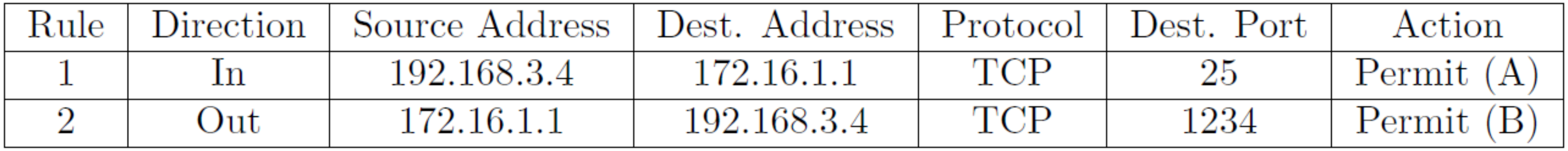
An Example



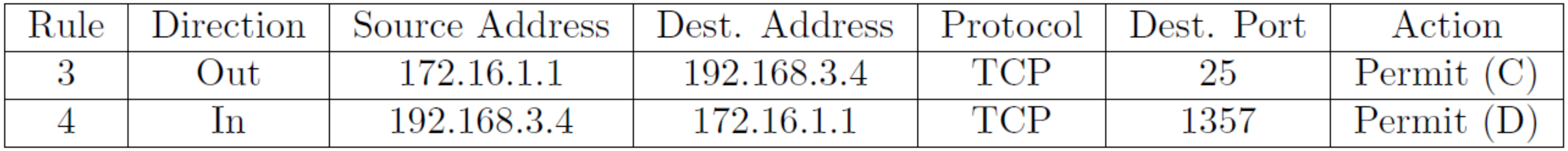
Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	> 1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	> 1023	Permit
E	Either	Any	Any	Any	Any	Deny

Table 1: Packet Filter 1

- 192.168.3.4 (remote host), 172.16.1.1 (local host)



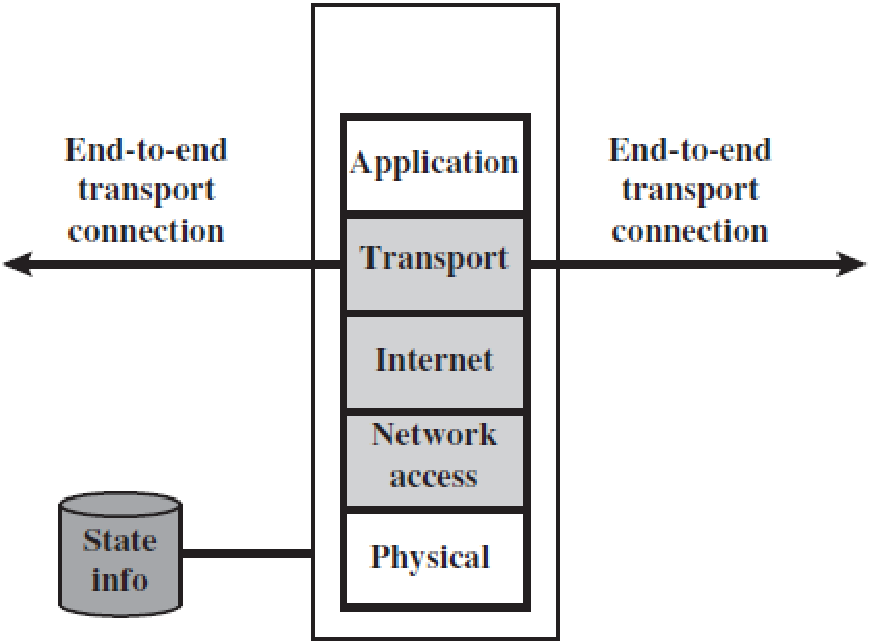
Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	Permit (A)
2	Out	172.16.1.1	192.168.3.4	TCP	1234	Permit (B)



Rule	Direction	Source Address	Dest. Address	Protocol	Dest. Port	Action
3	Out	172.16.1.1	192.168.3.4	TCP	25	Permit (C)
4	In	192.168.3.4	172.16.1.1	TCP	1357	Permit (D)

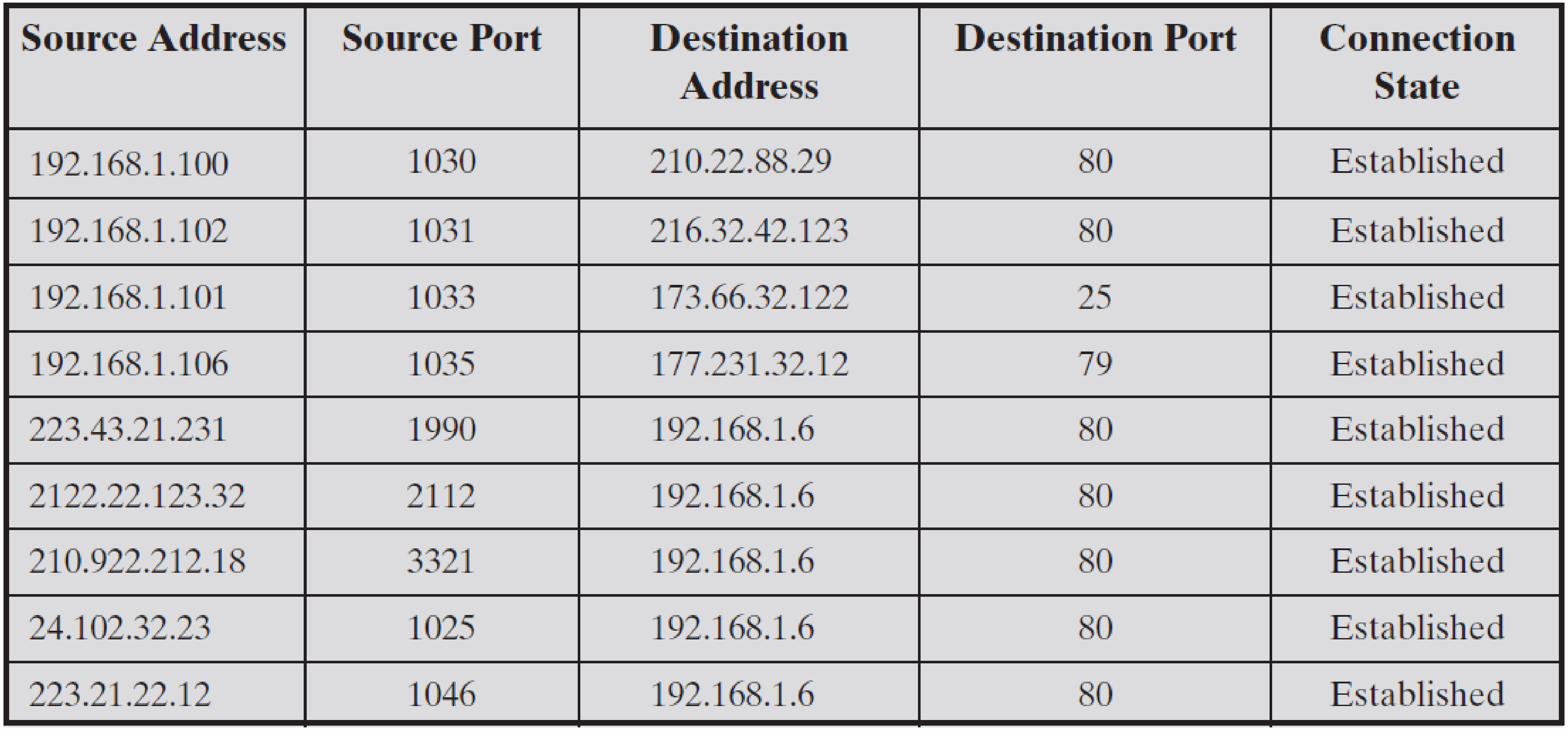
Stateful Packet Filter

- Problem: high-numbered port numbers are dynamic, could be exploited
- Solution: Remember the established connections


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

(c) Stateful inspection firewall

Stateful Packet Filter



Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Example connection state table

Application Level Gateway

- Bastion host, Proxy server
- Simulates application behavior to the outside world
- Support specific applications, and specific features

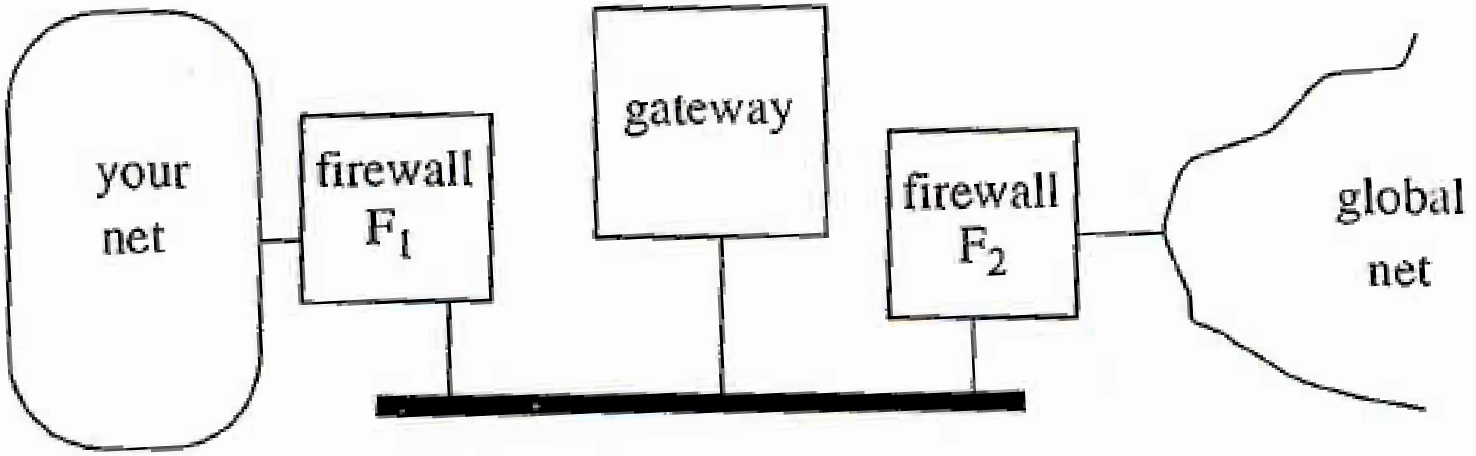
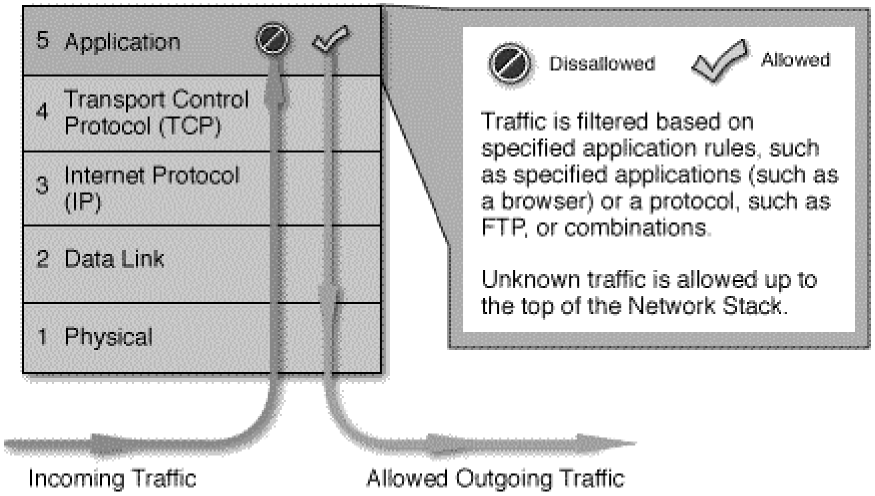


Figure 23-2. Application Level Gateway

Application proxy (2)

- More secure, easy to log and audit
- Additional processing overhead

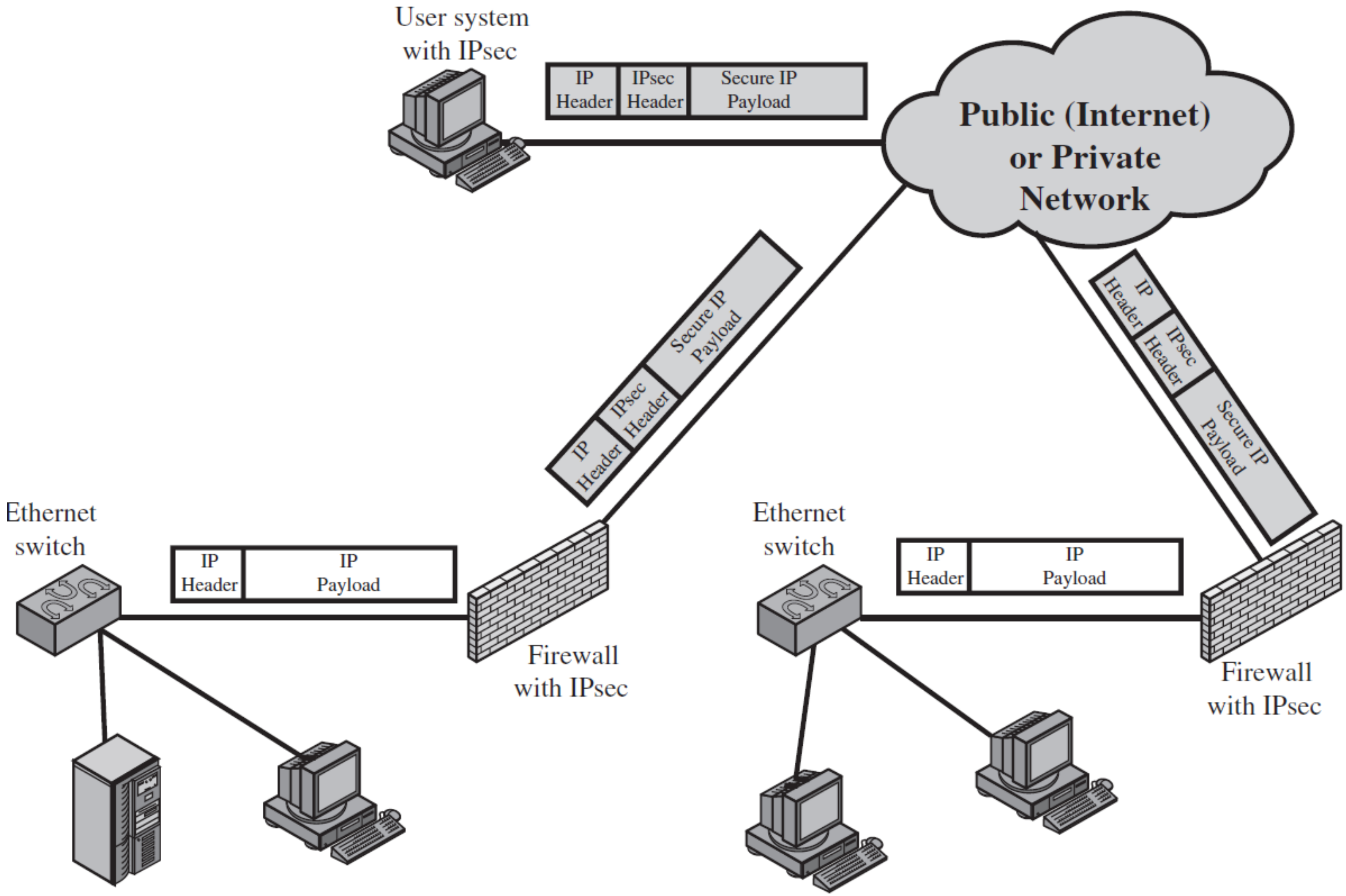


Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

Unknown traffic is allowed up to the top of the Network Stack.

Advantage? Disadvantage?

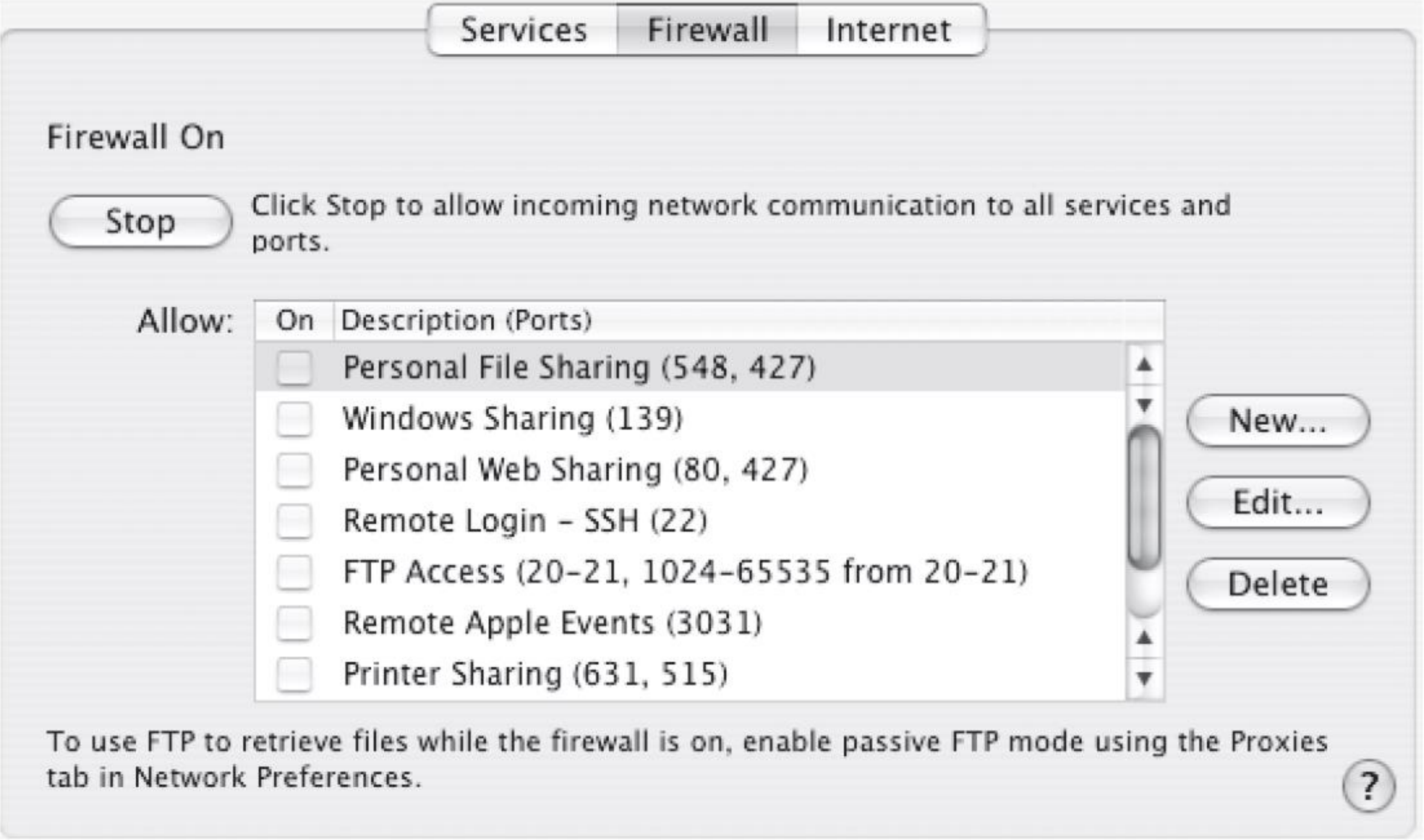
Encrypted Tunnels (VPN)



Personal firewalls

- Suitable for broadband home users.
  - Protecting single workstation or small networks.
  - Runs on the workstation itself (not in isolation).
- Blocks unwanted network traffic.
  - Java applets, Active X, leakage of personal data, closes ports.
- Usually generate activity and access logs.
- May be combined with virus scanners.
- Provide reasonable protection.

Example Interface



Firewall On

Click Stop to allow incoming network communication to all services and ports.

Allow:

On	Description (Ports)
□	Personal File Sharing (548, 427)
□	Windows Sharing (139)
□	Personal Web Sharing (80, 427)
□	Remote Login – SSH (22)
□	FTP Access (20-21, 1024-65535 from 20-21)
□	Remote Apple Events (3031)
□	Printer Sharing (631, 515)

To use FTP to retrieve files while the firewall is on, enable passive FTP mode using the Proxies tab in Network Preferences.

Comparison of Firewall Types

Packet Filtering	Stateful Inspection	Application Proxy	Guard	Personal Firewall
Simplest	More complex	Even more complex	Most complex	Similar to packet filtering firewall
Sees only addresses and service protocol type	Can see either addresses or data	Sees full data portion of packet	Sees full text of communication	Can see full data portion of packet
Auditing difficult	Auditing possible	Can audit activity	Can audit activity	Can and usually does audit activity
Screens based on connection rules	Screens based on information across packetsin either header or data field	Screens based on behavior of proxies	Screens based on interpretation of message content	Typically, screens based on information in a single packet, using header or data
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex addressing rules	Complex guard functionality can limit assurance	Usually starts in "deny all inbound" mode, to which user adds trusted addresses as they appear

What a Firewall can and can’t do

- Can do list:
  - …

- Cannot prevent:
  - Internal threats
  - Attacks that bypass the firewall
  - IP-spoofing?
  - Transfer of virus-infected programs or files

An example when firewalls fail