CSE P 590 / CSE M 590 (Spring 2010)

# Computer Security and Privacy

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

# Goals for Today

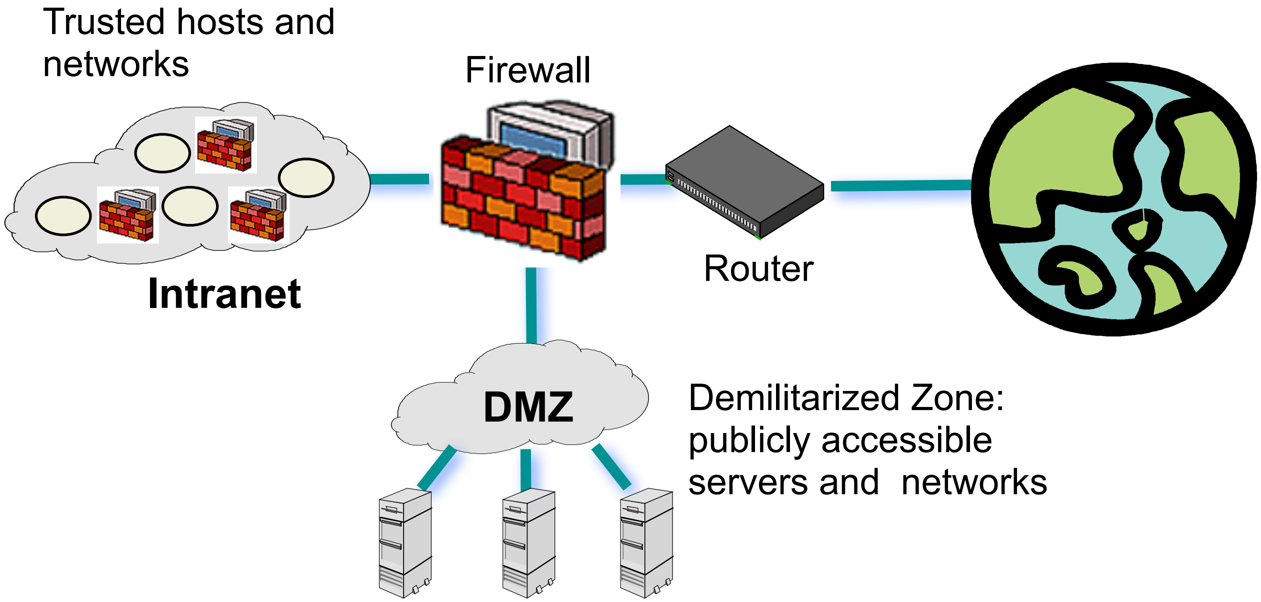
- Lab 2 discussion / HW 3 discussion

- Network security
- Hardware security (based on requests)
- Research reading

# Network Security

# Firewalls

- Idea: separate local network from the Internet

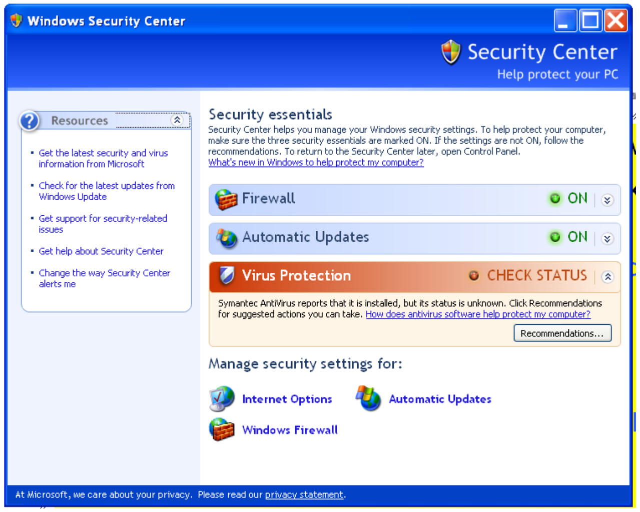

Trusted hosts and networks
Firewall
Intranet
Router
DMZ
Demilitarized Zone: publicly accessible servers and networks

# Castle and Moat Analogy

- More like the moat around a castle than a firewall
  - Restricts access from the outside
  - Restricts outbound connections, too
    - Important: filter out undesirable activity from internal hosts!

# Firewall Locations in the Network

- Between internal LAN and external network
- At the gateways of sensitive subnetworks within the organizational LAN
  - Payroll's network must be protected separately within the corporate network
- On end-user machines
  - "Personal firewall"
  - Microsoft's Internet Connection Firewall (ICF) comes standard with Windows XP


Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me

Security essentials

Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?

Firewall: ON

Automatic Updates: ON

Virus Protection: CHECK STATUS

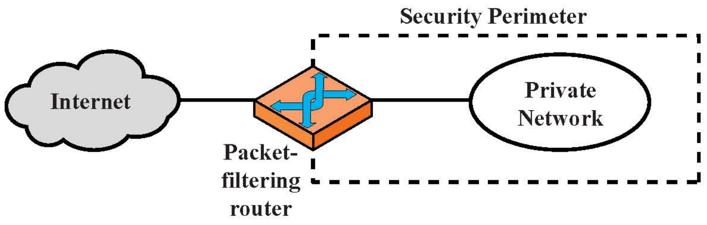
Symantec AntiVirus reports that it is installed, but its status is unknown. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?

At Microsoft, we care about your privacy. Please read our privacy statement.

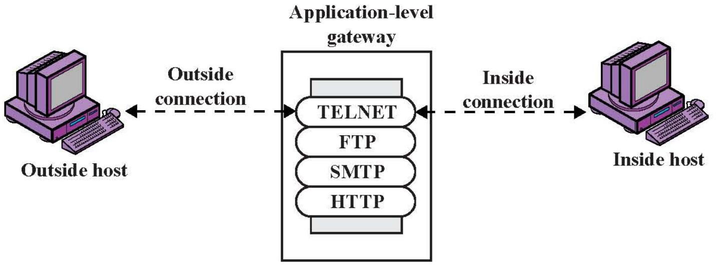
# Firewall Types

- Packet- or session-filtering router (filter)
- Proxy gateway
  - All incoming traffic is directed to firewall, all outgoing traffic appears to come from firewall
  - Application-level: separate proxy for each application
    - Different proxies for SMTP (email), HTTP, FTP, etc.
    - Filtering rules are application-specific
  - Circuit-level: application-independent, “transparent”
    - Only generic IP traffic filtering (example: SOCKS)
- Personal firewall with application-specific rules
  - E.g., no outbound telnet connections from email client

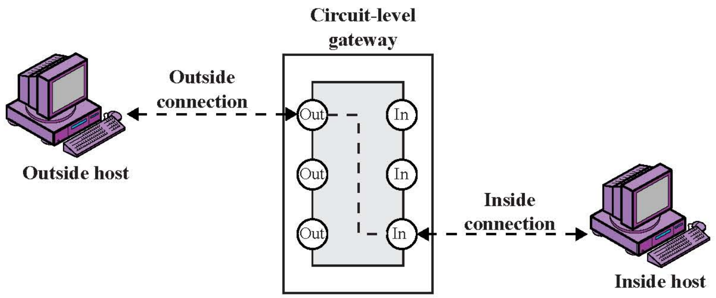
# Firewall Types: Illustration



(a) Packet-filtering router



(b) Application-level gateway

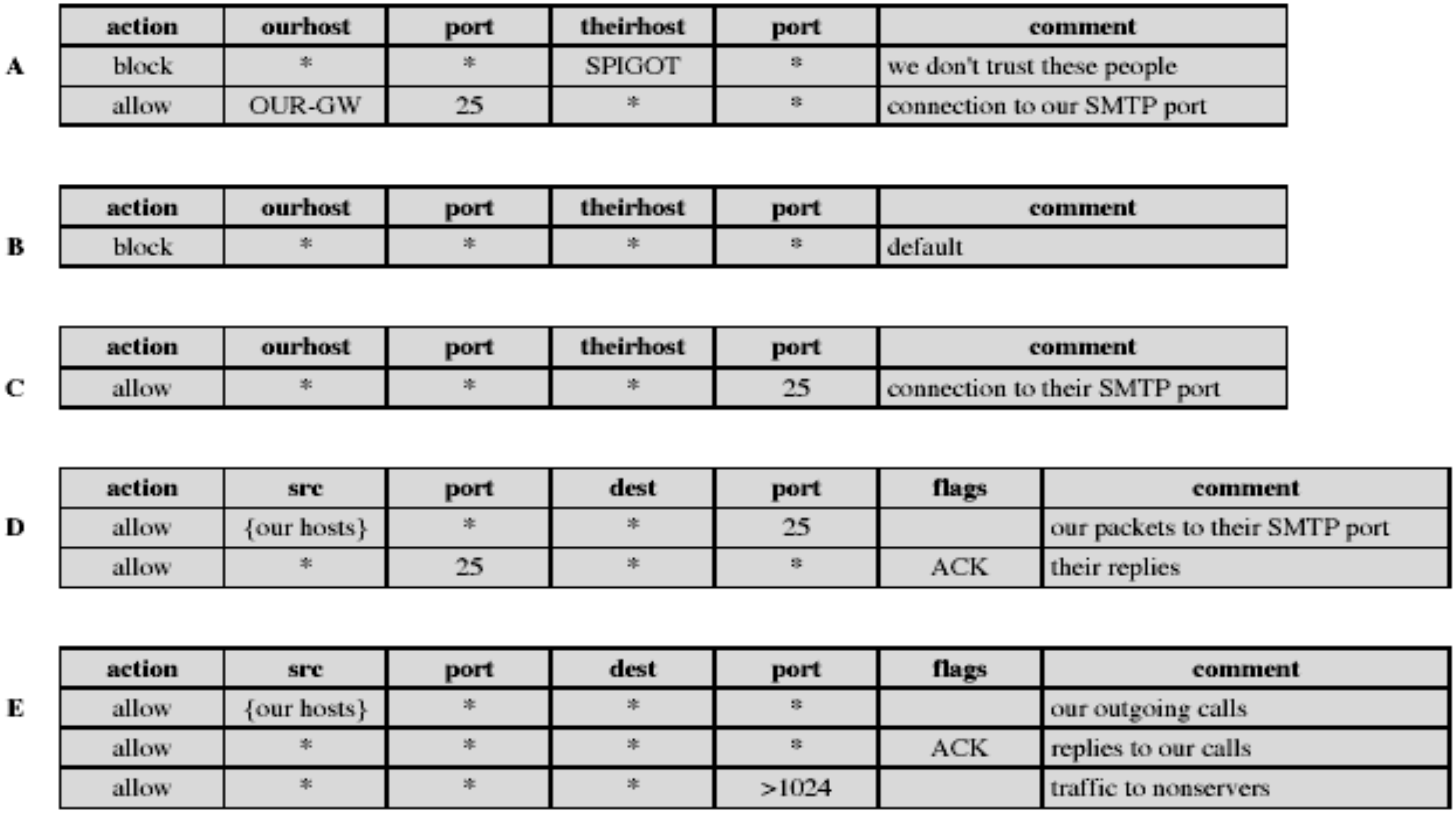


(c) Circuit-level gateway

# Packet Filtering

- For each packet, firewall decides whether to allow it to proceed
  - Decision must be made on per-packet basis
    - Stateless; cannot examine packet's context (TCP connection, application to which it belongs, etc.)
- To decide, use information available in the packet
  - IP source and destination addresses, ports
  - Protocol identifier (TCP, UDP, ICMP, etc.)
  - TCP flags (SYN, ACK, RST, PSH, FIN)
  - ICMP message type
- Filtering rules are based on pattern-matching

# Packet Filtering Examples



**A**

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

**B**

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

**C**

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

**D**

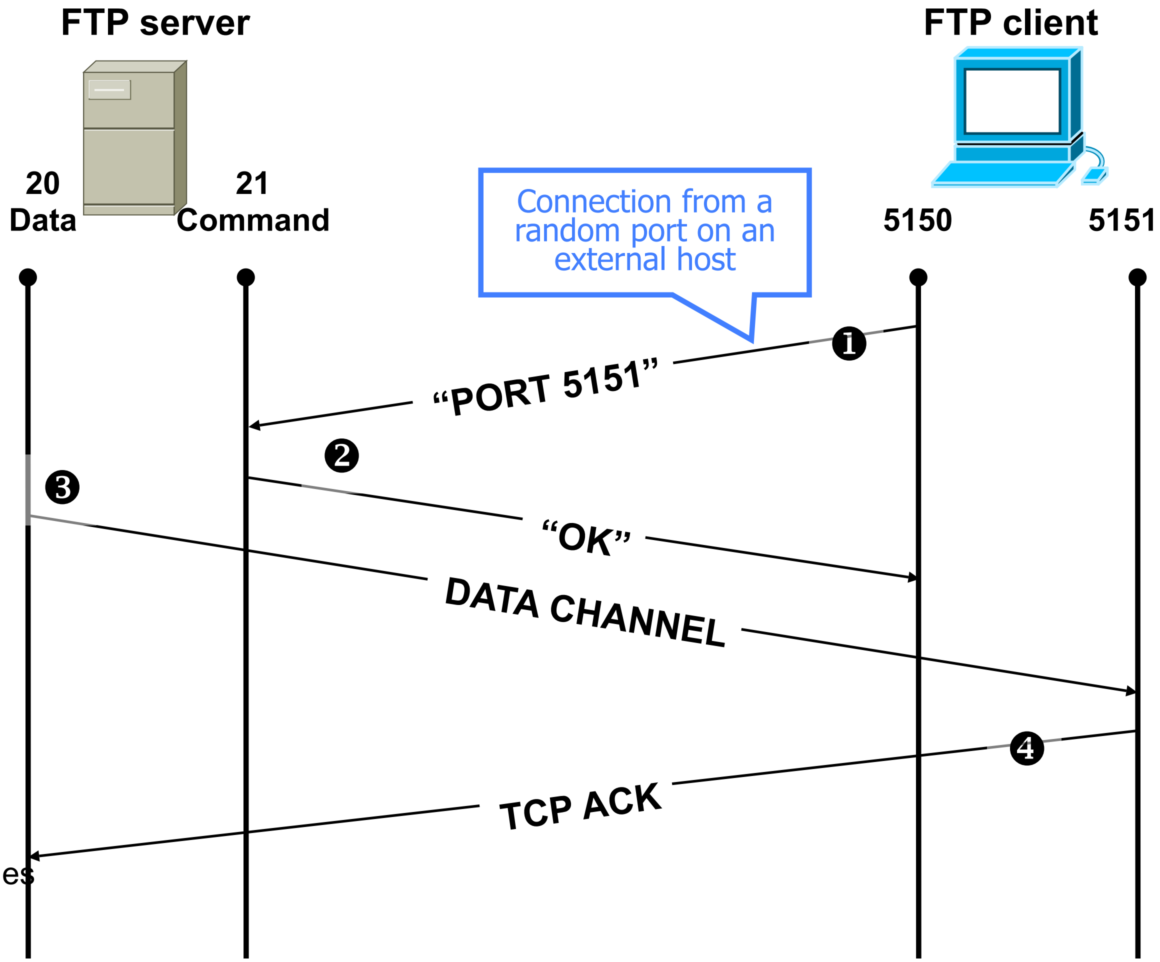
| action | src | port | dest | port | flags | comment |
|---|---|---|---|---|---|---|
| allow | {our hosts} | * | * | 25 | | our packets to their SMTP port |
| allow | * | 25 | * | * | ACK | their replies |

**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 |

slide

# Example: FTP (borrowed from Wenke Lee)



❶ Client opens command channel to server; tells server second port number

❷ Server acknowledges

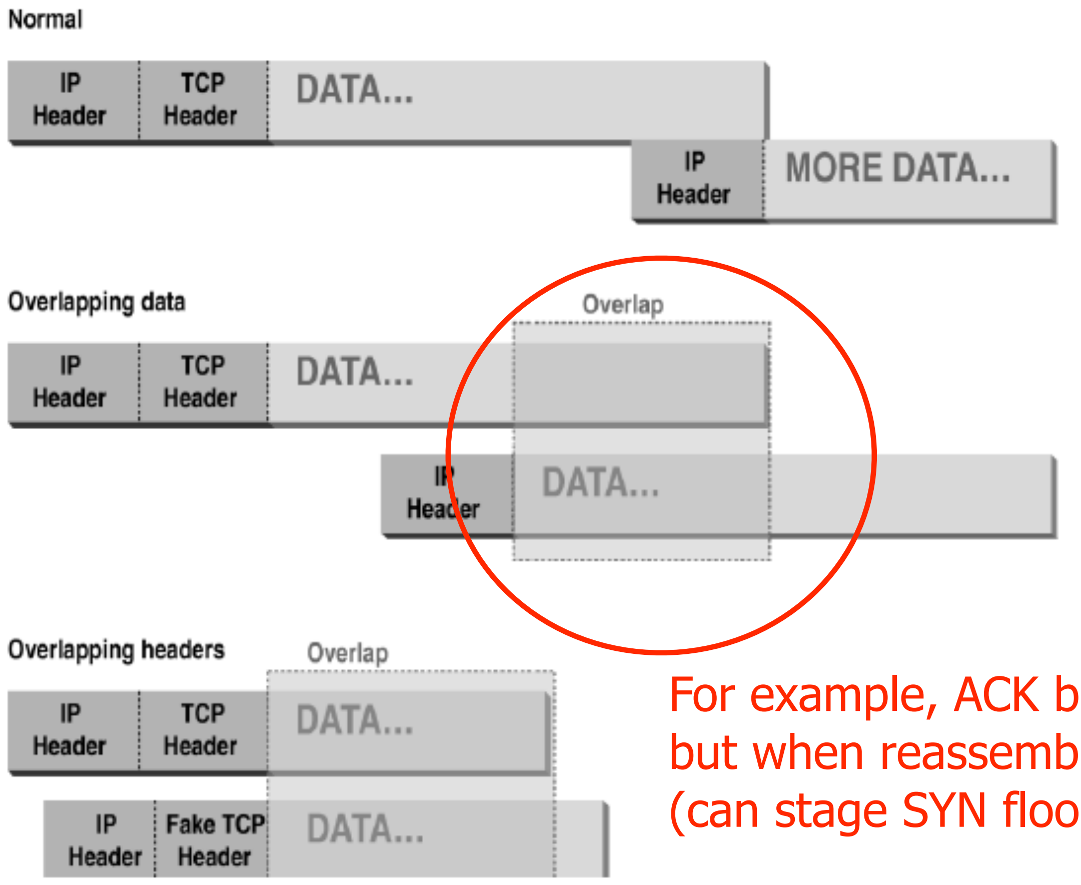
❸ Server opens data channel to client’s second port

❹ Client acknowledges

# Weaknesses of Packet Filters

- Do not prevent application-specific attacks
  - For example, if there is a buffer overflow in URL decoding routine, firewall will not block an attack string
- No user authentication mechanisms
  - … except (spoofable) address-based authentication
  - Firewalls don't have any upper-level functionality
- Vulnerable to TCP/IP attacks such as spoofing
  - Solution: list of addresses for each interface (packets with internal addresses shouldn't come from outside)
- Security breaches due to misconfiguration

# Abnormal Fragmentation

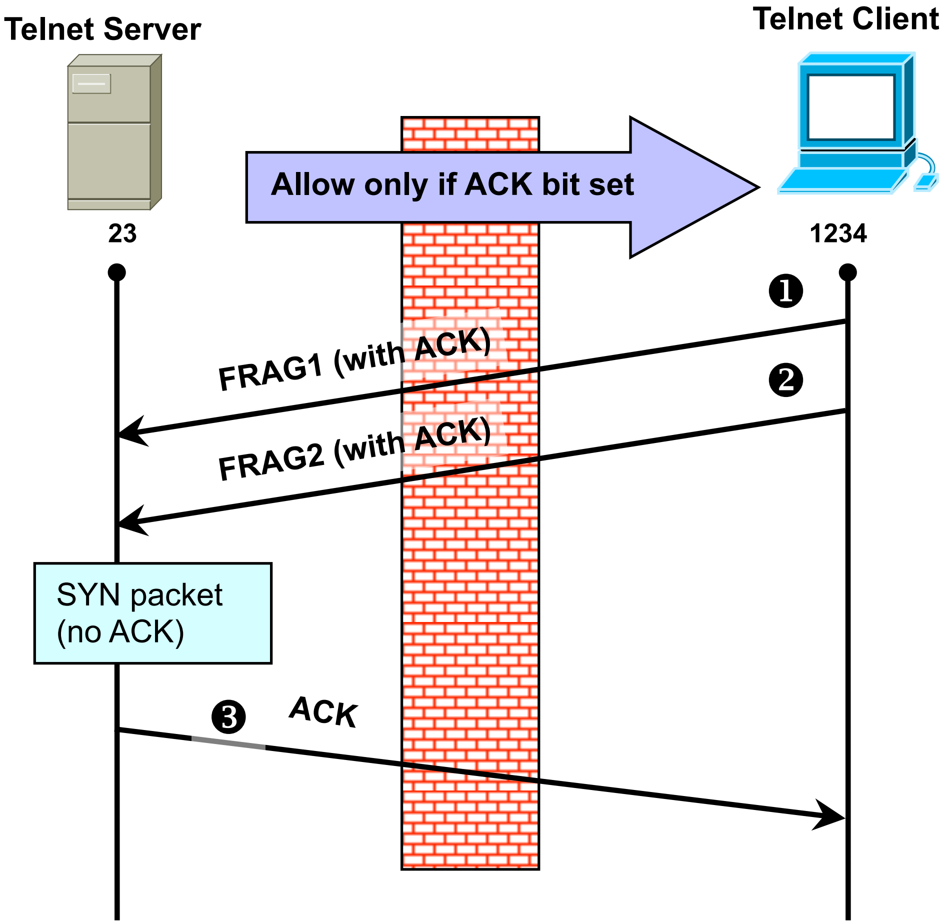


For example, ACK bit is set in both fragments, but when reassembled, SYN bit is set (can stage SYN flooding through firewall)

# Fragmentation Attack (borrowed from Wenke Lee)

❶,❷ Send 2 fragments with the ACK bit set; fragment offsets are chosen so that the full datagram re-assembled by server forms a packet with the SYN bit set (the fragment offset of the second packet overlaps into the space of the first packet)

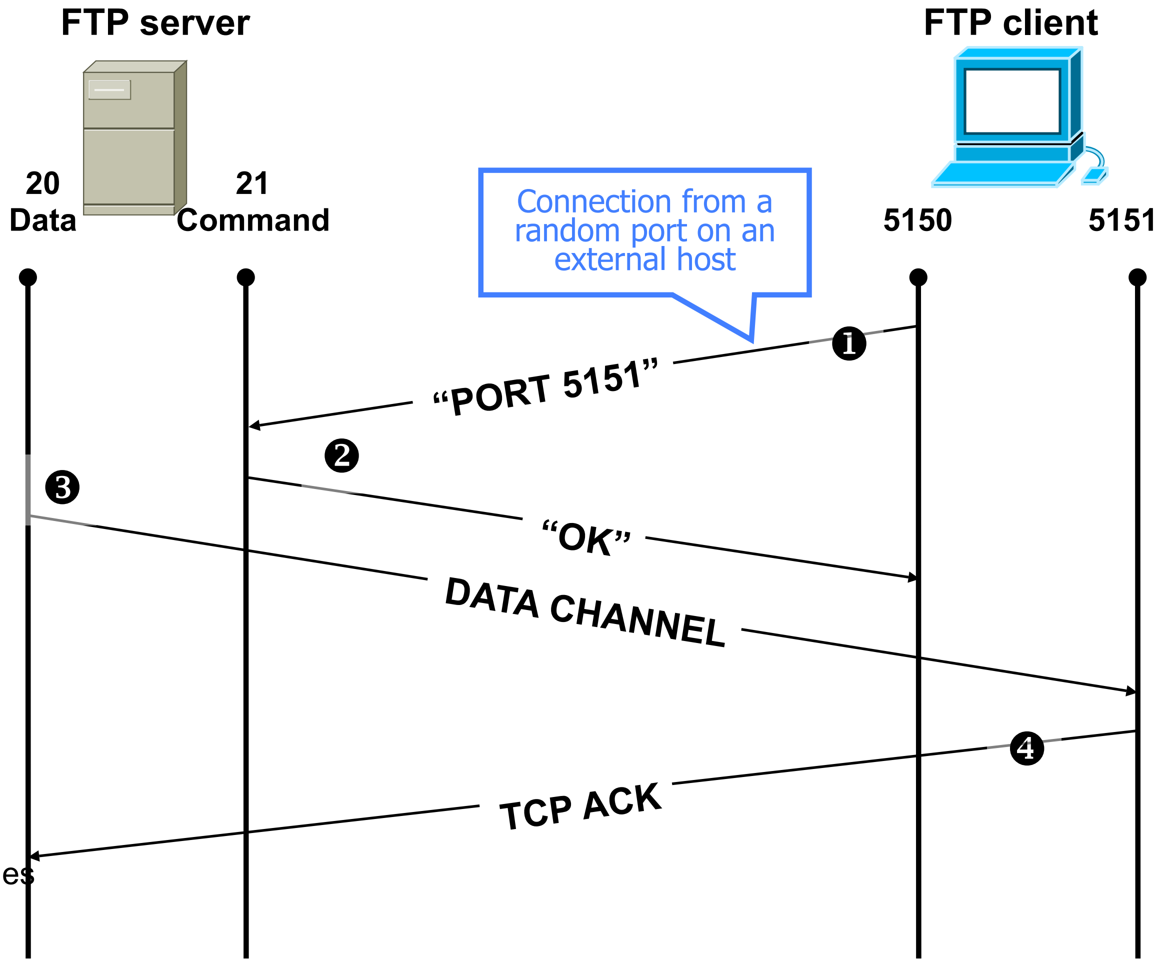
❸ All following packets will have the ACK bit set



# Stateless Filtering Is Not Enough

- In TCP connections, ports with numbers less than 1024 are permanently assigned to servers
  - 20,21 for FTP, 23 for telnet, 25 for SMTP, 80 for HTTP…
- Clients use ports numbered from 1024 to 16383
  - They must be available for clients to receive responses
- What should a firewall do if it sees, say, an incoming request to some client's port 5612?
  - It must allow it: this could be a server's response in a previously established connection…
  - …OR it could be malicious traffic
  - Can't tell without keeping state for each connection

# Example: FTP (borrowed from Wenke Lee)



Connection from a random port on an external host

❶ Client opens command channel to server; tells server second port number

❷ Server acknowledges

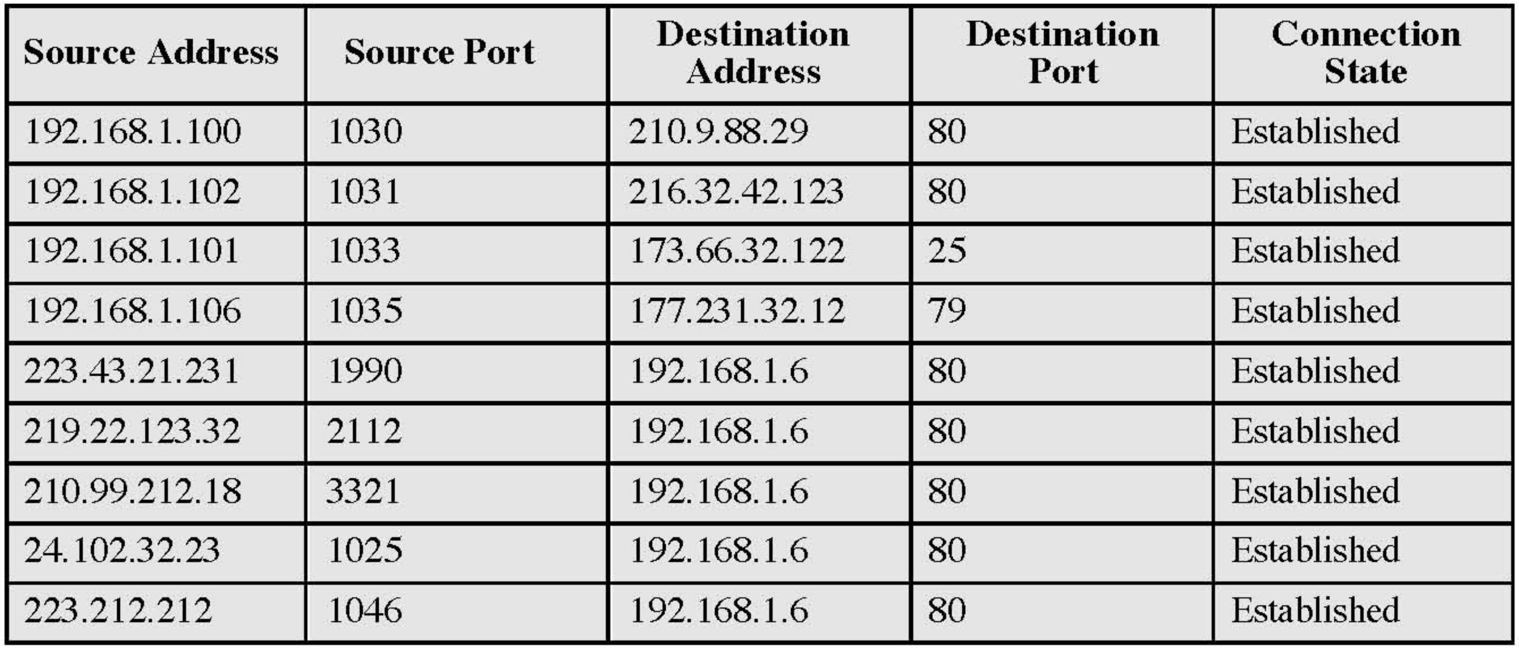
❸ Server opens data channel to client's second port

❹ Client acknowledges

# Session Filtering

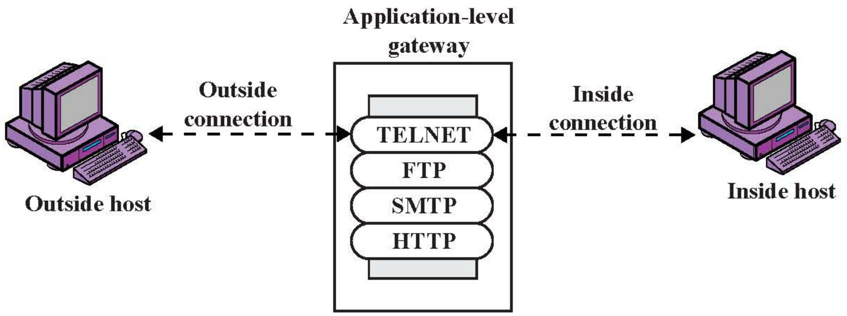
- Decision is still made separately for each packet, but in the context of a connection
  - If new connection, then check against security policy
  - If existing connection, then look it up in the table and update the table, if necessary
    - Only allow incoming traffic to a high-numbered port if there is an established connection to that port
- Hard to filter stateless protocols (UDP) and ICMP
- Typical filter: deny everything that's not allowed
  - Must be careful filtering out service traffic such as ICMP
- Filters can be bypassed with IP tunneling

# Example: Connection State Table



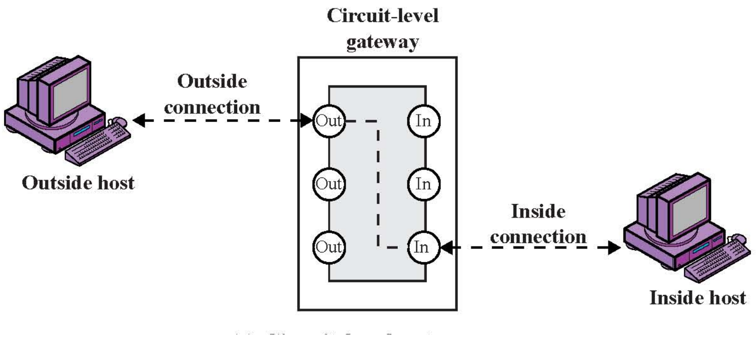
| Source Address | Source Port | Destination Address | Destination Port | Connection State |
|---|---|---|---|---|
| 192.168.1.100 | 1030 | 210.9.88.29 | 80 | Established |
| 192.168.1.102 | 1031 | 216.32.42.123 | 80 | Established |
| 192.168.1.101 | 1033 | 173.66.32.122 | 25 | Established |
| 192.168.1.106 | 1035 | 177.231.32.12 | 79 | Established |
| 223.43.21.231 | 1990 | 192.168.1.6 | 80 | Established |
| 219.22.123.32 | 2112 | 192.168.1.6 | 80 | Established |
| 210.99.212.18 | 3321 | 192.168.1.6 | 80 | Established |
| 24.102.32.23 | 1025 | 192.168.1.6 | 80 | Established |
| 223.212.212 | 1046 | 192.168.1.6 | 80 | Established |

# Application-Level Gateway



- Splices and relays two application-specific connections
  - Example: Web browser proxy
  - Daemon spawns proxy process when communication is detected
  - Big processing overhead, but can log and audit all activity
- Can support high-level user-to-gateway authentication
  - Log into the proxy server with name, password, etc
- Simpler filtering rules than for arbitrary TCP/IP traffic
- Each application requires implementing its own proxy

# Circuit-Level Gateway



- Splices two TCP connections, relays TCP segments
- Less control over data than application-level gateway
  - Does not examine the contents of TCP segment
- Client's TCP stack must be aware of the gateway
  - Client applications are often adapted to support SOCKS
- Often used when internal users are trusted
  - Application-level proxy on inbound connections, circuit-level proxy on outbound connections (lower overhead)

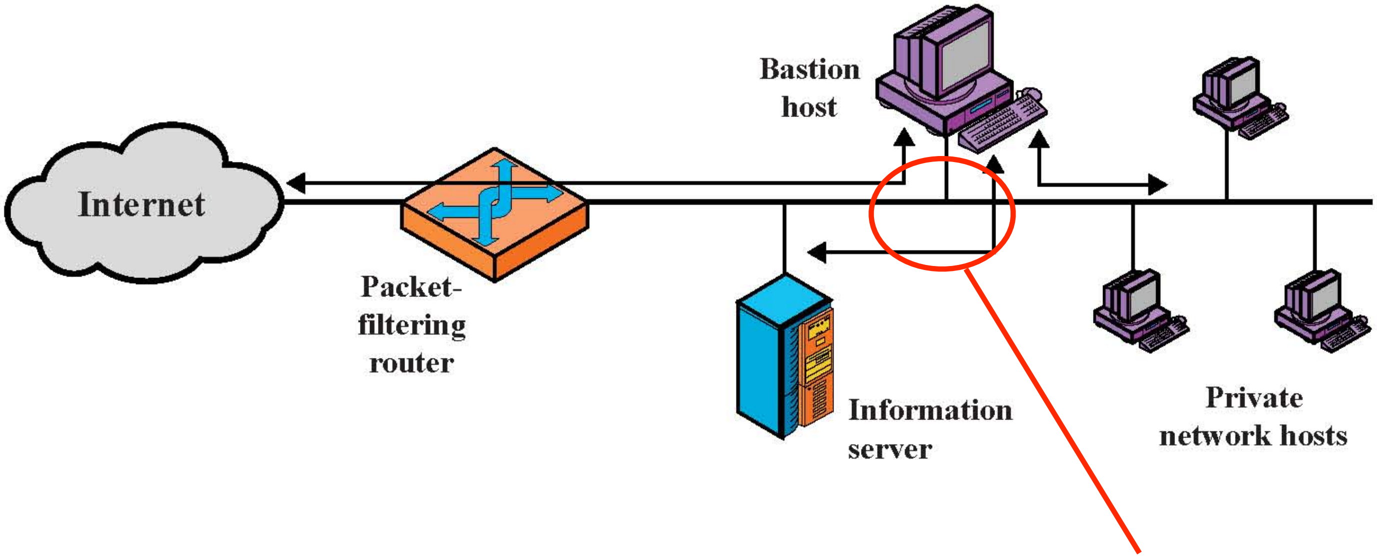
# Comparison

| | Performance | Modify client application | Defends against fragm. attacks |
|---|---|---|---|
| Packet filter | Best | No | No |
| Session filter | ↓ | No | Maybe |
| Circuit-level gateway | | Yes (SOCKS) | Yes |
| Application-level gateway | Worst | Yes | Yes |

# Bastion Host

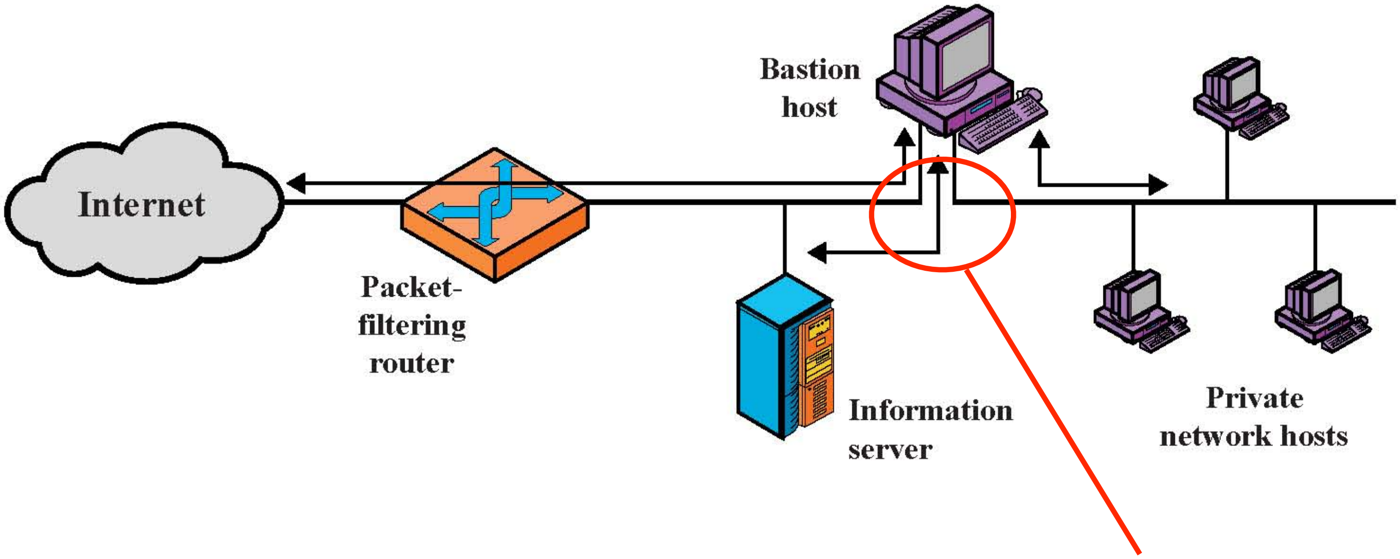
- Bastion host is a hardened system implementing application-level gateway behind packet filter
  - All non-essential services are turned off
  - Application-specific proxies for supported services
    - Each proxy supports only a subset of application’s commands, is logged and audited, disk access restricted, runs as a non-privileged user in a separate directory (independent of others)
  - Support for user authentication
- All traffic flows through bastion host
  - Packet router allows external packets to enter only if their destination is bastion host, and internal packets to leave only if their origin is bastion host

# Single-Homed Bastion Host



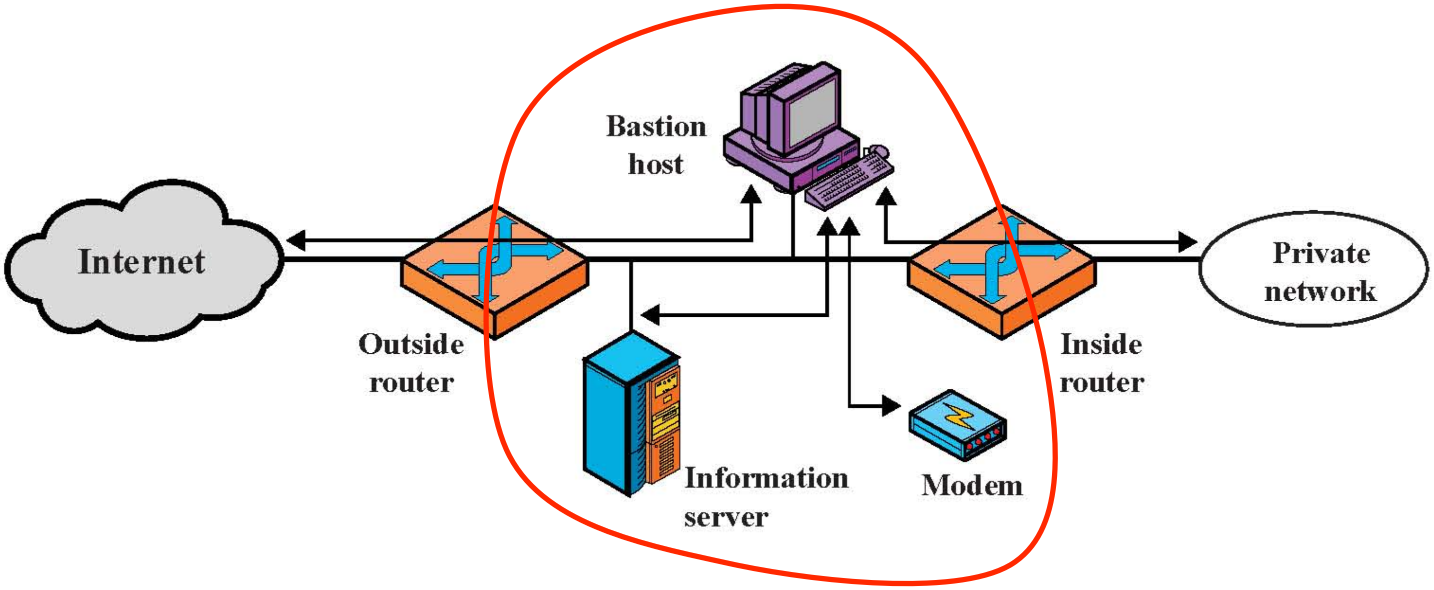
If packet filter is compromised, traffic can flow to internal network

# Dual-Homed Bastion Host



No physical connection between internal and external networks

# Screened Subnet



Only the screened subnet is visible
to the external network;
internal network is invisible

# Protecting Addresses and Routes

- Hide IP addresses of hosts on internal network
  - Only services that are intended to be accessed from outside need to reveal their IP addresses
  - Keep other addresses secret to make spoofing harder
- Use NAT (network address translation) to map addresses in packet headers to internal addresses
  - 1-to-1 or N-to-1 mapping
- Filter route announcements
  - No need to advertise routes to internal hosts
  - Prevent attacker from advertising that the shortest route to an internal host lies through him

# General Problems with Firewalls

- Interfere with networked applications
- Doesn't solve all the problems
  - Buggy software (e.g., buffer overflow exploits)
  - Bad protocol design (e.g., WEP in 802.11b)
- Generally don't prevent denial of service
- Don't prevent insider attacks
- Increasing complexity and potential for misconfiguration

# Cold Boot Attacks

http://citp.princeton.edu/memory/

# Power Analysis

http://www.cc.gatech.edu/~traynor/f08/slides/lecture11-dpa.pdf

# More Hardware Security (Not Covered)

http://www.slideshare.net/guest3bd2a12/advanced-hardware-hacking-techniques-presentation