Firewall - a barrier on the network that prohibits bad behavior, keeps good behavior correct.

What is a firewall? A router

1. Must ship all traffic through it
2. Must be hardened (can't be compromised)
3. Must only allow authorized traffic through (defined by local policy)

Open policy - check list of prohibited actions (default - forward)
Closed policy - check list of approved actions (default - discard)

Types of Firewalls
1) Packet inspection - source IP, dest IP, ports, some activities
   - NAT - as many devices as you want behind the firewall
2) Stateful Connection - keep track of state of TCP connection
3) Application gateway - put proxy in between sender and receiver
   - Proxy system acting on behalf of user
4) Circuit level - doesn't allow point to point connections with TCP connection
   - SSL (secure socket layer) - ability to do encryption at hardware level

The Need of Firewalls
- Internet connectivity is a threat.
- Must protect LANs, so firewalls become the perimeter defense.

Firewall Filtering Characteristics
- IP address and protocol values
- Application protocol
- User identity
- Network activity
Capabilities
- Single network choke point
- Provides location for monitoring security (and non-security internet functions)

Limitations
- Cannot protect if attack bypasses firewall
- Internal threats can't be stopped

Packet Filter
Advantages
- Simple
- Invisible to users

Disadvantages
- Limiting logging
- Cannot support advanced user authentication
- Vulnerable to attacks on TCP/IP protocol bugs
- Useless if there is improper configuration