1) Review of Firewalls
   a. Looking at packets
   b. State full Firewall
      i. Keeping track of TCP Connections
   c. Proxy Based Firewalls.

2) Where do Firewalls live?
   a. At network’s gateway? (Inside boundary.)
      i. Bastion Hosts
         1. Identified a critical strong point.
         2. Standalone Machine
         3. Hardened, with only needed services installed
         4. Not a part of Authentication system
   b. Putting them in the existing devices (Routers, computers...)
      i. Software based.
      ii. Performance issue.
      iii. Prone to all the vulnerabilities of the device it resides on.
   c. Host Based Firewalls
      i. Protects individual host
      ii. Filter and restrict packet flows
      iii. Common location is a server

3) How do we configure them?
   a. Establish DMZ
      i. Segregate services that must be exposed to outside world from those that can reside only inside.
      ii. External DMZ vs Internal DMZ
   b. External Firewall
      i. Faces outside to protect from outside coming in.
   c. Internal Firewall
      i. Protects from an attack from a misfeasor toward the DMZ
      ii. Protects from In-In attacks, protecting cluster of systems.
   d. Firewall Topologies
      i. Can be as complex or as simple as you want.

4) Remote Users
   a. VPNs
      i. Create a secure Point to Point connection
         1. Using Encryption/Session Key
         2. Best place is within the Firewalls themselves
            a. Network Layer Protocols
            3. IPSec

5) Best Solution
   a. Combination of all of the above
   b. Ideally talking to each other.
      i. Still not there.
c. Performance and Money are the hindrances

6) Intrusion Prevention Systems (IPS)
   a. Host Based IPS (HIPS)
      i. Signature or Anomaly Based
   b. Network Based IPS (NIPS)
      i. Looking for patterns in the traffic.
      ii. Taking actions to prevent unauthorized access.
   c. Distributed or Hybrid IPS

7) Digital Immune System
   a. Defense against malicious behavior