A. Where do firewalls live?
   a. Networks gateway
      i. External firewall; filters through packets.
   b. Host
      i. Teach it about applications on it
      ii. Filter and restrict packet flows
      iii. Can be implemented as a Bastion server
   c. Personal Machine
      i. Allows a black list
      ii. Usually a software module

B. *Bastion server (Critical strong point)
   a. Stand alone machine that is hardened
      i. Hardened: only necessary programs are uploaded onto there.
   b. Routers and switches can be inserted into it.
   c. Characteristics:
      i. Each proxy is small, simple, secure.
      ii. Each proxy is independent.

C. We cannot protect out-to-out (That’s the entire Internet)
   a. So we protect in-to-in; protect clusters of networks.
      i. ex: each CSU department has a firewall.

D. Firewall Configurations
   a. VPN
      i. Sets us an end-to-end connection.
         1. Then encrypts the connection.
   b. Topologies
i. How many firewalls are being set up? In what order?

ii. Can be as simple as firewall connected to system or a firewall on every system in network.

E. Intrusion Detection Systems
   a. When intruders are detected, activity should be dropped.
      i. Uses anomaly and signature detection
   b. Buffer overflow exploit can be used to escalate permissions
      i. Store a variable on the stack, overwrite with longer variable and overwrite 'return address' for the destination you want.
   c. HIPS (Host-based IPS)
      i. Capability tailored to the host it is on
      ii. Role: Main target is desktop and laptops so this is an endpoint security product.
   d. NIPS look fors packets (Network-Based IPS)
      i. Keeps statistics on normal traffic and alerts if traffic exceeds normal benchmarks.
      ii. NIPS is an inline NIDS that can tear down TCP connections.
   e. Digital Immune System
      i. Comprehensive defense against malware
         1. Motivation for creation includes the rising threat of malware.