1. CDNs & DoS Attacks
   a. **DoS** – attacker launches a large scale distributed attack from a number of servers (compromise).
      i. CDNs protect against this by running tight systems and never publishing the IP Address of the actual website. The IP Address is completely hidden.
      ii. CDN machines are arranged in a hierarchy where only a very secure core of CDN machines know about a websites IP address and all of the other CDN machines access those core machines to get content.
      iii. No IP Address. Website operators simply publish their data to the CDN machines; therefore there is no centralized website for anybody to attack.
   b. What happens if you attack the CDN?
      i. A CDN has something of the order of 16,000 machines. In order to launch a DoS attack you need at least 10 attackers to each machine you want to attack. Can’t take down all of the CDNs machines at once.
      ii. CDNs use a very short TTL. They will also balance their loads across one another. If you attack a few of the CDN machines those machines will have very high loads and legitimate traffic will be directed to other CDN machines with less of a load on them (load-balancing). If the attacker then switches to other CDN machines, the first set of attacked machines come back to life and the load of traffic is transferred back to the original machines.
      iii. The only way to launch a DoS attack against a CDN is to have on the order of 100,000 attacker machines in order to attack all CDN machines at once.
   c. Technique for isolating attack traffic
      i. Advertise a large IP space in which your website lives in. Then when you suspect that there are name servers which are being used to attack you, hand half of your IPs to some of these name servers, and half to the other. By repeating this process and monitoring traffic from each half of the IPs you give, you can then determine which name servers are being used to launch attacks on you.

2. Firewalls
   a. A firewall is either a machine or software that “protects” (A CDN can be seen as a big firewall for any website that it hosts).
   b. They are typically placed at a trust boundary. (For example between a company’s LAN and their central connection to the Internet).
   c. Benefits of Firewalls:
      i. Provide Authentication services to keep harmful traffic out.
ii. Helps to detect harmful traffic that may come from within your network to protect a company for liability reasons. (Easy point to monitor all incoming and outgoing traffic).

iii. Allows for a collection of traffic statistics and audit trails.

iv. Allows you to relax internal patch procedures because your machines are protected by the firewall.

d. Drawbacks to running a Firewall:
   i. Single point of failure or slowdown for all traffic.
   ii. Firewalls block many ports inconvenience users who want to run services on their machines.
   iii. False sense of security. (You still need antivirus anti-spy ware software).

e. Stateless and Stateful Firewalls
   i. Stateless Firewalls – Firewalls that simply act as packet filters. Simply based on rules. E.g.: To block the Finger command you would implement a rule saying to block all TCP packets to port 79. To block all connections you can simply block all packets with the ‘ack’ bit not set.
   ii. Stateful Firewalls – Will inspect packets deeply and is aware of certain protocols. It will temporarily change state when it realizes there is a callback.
      1. How FTP Works:
         a. Client logs onto Server via port 21
         b. For transfer client asks OS for port and sends that port to server
         c. Server calls back to the sent port
         d. Data is transferred over the data line.

3. Virtual Private Networks (VPNs)

![Diagram of a VPN setup]

4. Problems
   • You can punch holes in a firewall (port knocking).
     o Port knocking - Set up a sequence of ports to contact and when a client contacts those ports in the correct order, the firewall will open up the port for a certain period of time.
     o Connection Welding – Two machines that need to exchange information both contact a coordinator (welder) machine which will put the information together and forward it between the two. Later the
welder machine can remove himself from the connection by telling the other two machines to spoof his IP.

- You can tunnel things over port 80 because most firewalls allow port 80 incoming/outgoing.