IK2206 – Internet Security and Privacy
Chapter 23 – Firewalls

23.1 Packet Filters (READ)

- What are the basic functions of a firewall?

  The basic function of a firewall is to manage access from/to internal/external networks at a central point. It enforces security policies about how to handle traffic.

- How can a firewall help bolster the protection of our hosts?

  Each system provides several services, many by default. Most were designed for environments where no bad guys were expected. It is difficult – if not impossible – to harden all systems in order to reduce the risk of an external attack.

  Firewalls attempt to protect systems inside from attacks from outside without requiring the administrator to know about each and every service.

23.2 Application Level Gateway (READ)

- What protection can an application level gateway offer?

  Application level gateways are much more powerful than packet filter firewalls, since they're able to look inside application protocols. Application level gateways protect applications hosted in the trusted network without having to know much about the application itself.

- What are its limitations?

  Most application level gateways are not transparent for users. So, they mostly have to provide credentials to pass messages through.

  There are always tricks to go around limitations set by application level gateways. (Large email message limitation can be bypassed using message split mechanisms,…).

23.3 Encrypted Tunnels (READ)

- What benefit do you get from using encrypted tunnels over the Internet?

  Encrypted tunnels allow to interconnect multiple trusted sites. If all "inside" sides are securely connected together, we only have to have one point (=one firewall) that connects the "outside" world. This avoids enormous administrative effort and is considered as a best practice.

23.4 Comparisons (READ)

23.5 Why Firewalls Don't Work (READ)

- What kind of attacks and attackers won't a firewall protect against?

  Attacks from the inside network.

- Are firewall friendly protocols really friendly?

  It depends on who we ask. One of these firewall friendly protocols is http. This protocol is in most configurations allowed to pass the firewall. Many other applications, others than web browsing, adapted their protocols to run over http. Packet filter firewalls cannot distinguish between normal web browsing traffic and other applications, e.g. Skype calls. This is where content filtering comes into play…

23.6 Denial-of-Service Attacks (READ)

- What is a DoS-attack?

  Denial-of-Service attacks try to make a certain resource unavailable. Availability is (besides confidentiality, integrity, authenticity, and non-repudiation) one of the key parts of IT security. http://en.wikipedia.org/wiki/Information_security#Availability

- Can we protect against them, and if so, how?

  Firewalls can be configured to drop packets that come from untrusted IP ranges. This is, of course, a very unpractical approach. Now, each DoS attacks follows some – more or less – strict patterns. There are sophisticated application level firewalls that are able to recognize certain patterns in the traffic and thereby reveal DoS attacks.