lecture #17

- The Need of Firewall
  - Internet connectivity is essential (however it creates a threat)
  - effective means of protecting LANs
  - Inserted between the premises network and the Internet to establish a controlled link
    - Can be a single computer system or a set of two or more systems working together
  - Used as a perimeter defense
    - Single choke point to impose security and auditing
    - Insulates the internal systems from external networks
- Firewall Access Policy
  - A critical component in the planning and implementation of a firewall is specifying a suitable access policy
    - this lists the types of traffic authorized
- Firewall Filter characteristics
  - IP addr and protocol values
    - ~~this~~ used by pkt filter and stateful inspection firewalls
    - used to limit access to specific services
  - Application Protocol
    - used by app-level gateway that relays and monitors the exchange of info for ~~specific~~ app protocol
  - User identity
    - for inside users with some form of secure auth technology
  - Network activity
    - controls access based on time/rate of requests or other activity pattern

Firewall Capabilities and Limits

- Capabilities
  - Defines a single choke point
  - Provides a location for monitoring security events
  - Convenient platform for several Internet functions that are not security related
  - Can serve as the platform for IPSec
- Limitations
  - Cannot protect against attacks bypassing firewall
  - May not protect fully against internal threats
  - Improperly secured wireless LAN can be accessed from outside the organization
  - Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

Packet Filtering Firewall (stateless)

- Based on
  - Src IP addr
  - Dest IP addr
  - Src / Dest transport-level addr
  - IP protocol field
  - Interface
- Two default policies
  - Discard (more conservative; controlled; visible to users)
  - Forward (easier to manage ss use; less secure)
- Advantages
  - Simplicity
  - transparent to users ss very fast
- Disadvantages
  - Cannot prevent attacks that employ app specific vulner/fun
  - Limited logging functionality
  - Do not support advanced user auth
  - Vulnerable to attacks on TCP/IP protocol bugs
  - Improper configuration can lead to breaches

Stateful Inspection Firewall

- Creates directory of outbound TCP connections
  - entry for each currently established connection
  - port filter allows incoming traffic to high ports only if port is ass with one of entries
- Records info about TCP connections
  - keeps track of TCP seq num to prevent such attacks
  - inspect data for protocols like FTP, IM ss SIPS commands

App-level gateway (app proxy)

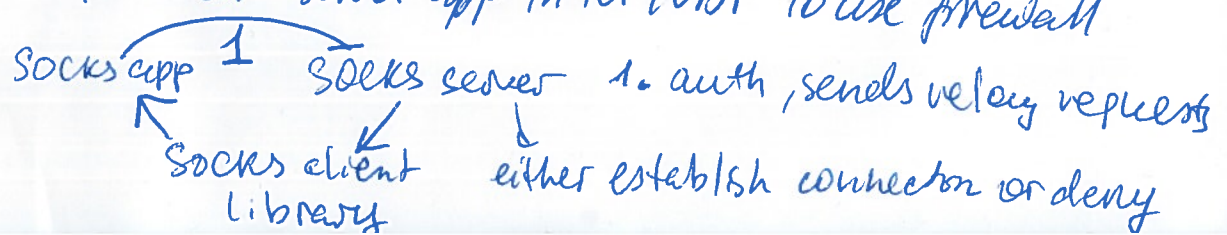
- acts as relay of app-level traffic
  - user contacts gateway using a TCP/IP app
  - user is auth
  - gateway contacts app on remote host and relays TCP segments between server and user
- proxy code for each app (may restrict features)
- more secure than pkt filters
- Disadvantage: additional processing overhead on each connection

Circuit-level gateway (proxy)

- 2 TCP connection: proxy ss TCP user; proxy ss TCP user
  - inner host
  - outside host
- relays TCP segments within connections
- no examine of contents
- used when inside users are trusted
- lower overheads
- may use app-level gateway inbound and CLG outbound

SOCKS:

- framework for client-server app in TCP/UDP to use firewall



- Bastion Hosts
  - critical strong point in the network's security
  - Platform for app-level / circuit-level gateway
  - Common characteristics:
    - only essential services
    - may require user auth to access proxy and host
    - each proxy can restrict features, hosts accessed
    - each proxy is independent, non-privileged
    - limited disk use, hence read-only code
- Host-based Firewalls
  - Used to secure an individual host
  - Available in OS or as add-on package
  - Filter and restrict pkt flows
  - Common loc is a server
  - Advantages:
    - filtering rules can be tailored to host environment
    - Protection is provided independent of topology
    - Provides an additional layer of protection
- Personal Firewall
  - Controls traffic between a personal computer or workstation and the Internet / enterprise network
  - both home and corporate use
  - software module on PC
  - can be in router for home network to DSL, modem, cable
  - less complex than server-based or stand-alone firewalls
  - Primary role is to deny unauthorized remote access
  - monitor outgoing traffic to detect and block worms and malware activity