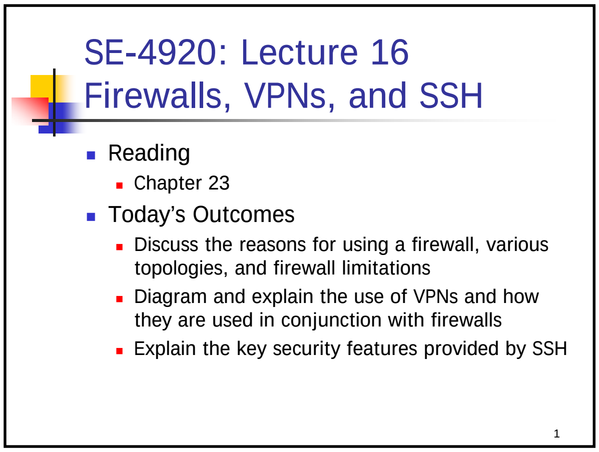
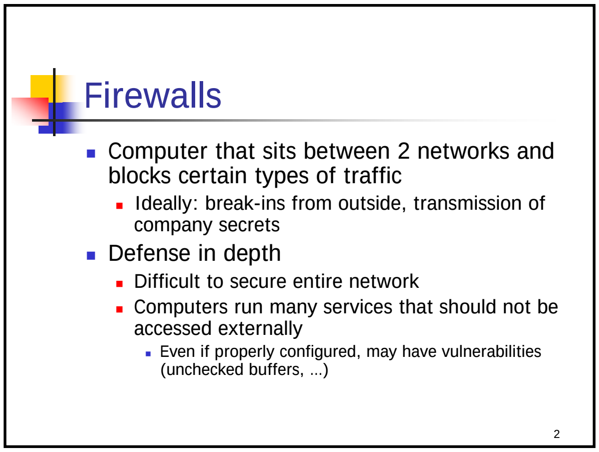


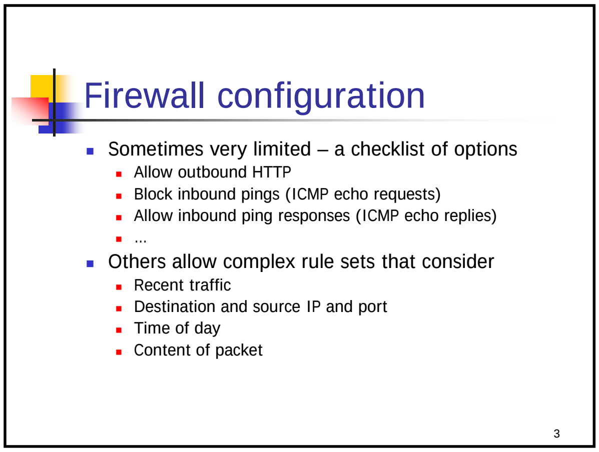
SE-4920: Lecture 16 Firewalls, VPNs, and SSH

- Reading
  - Chapter 23
- Today's Outcomes
  - Discuss the reasons for using a firewall, various topologies, and firewall limitations
  - Diagram and explain the use of VPNs and how they are used in conjunction with firewalls
  - Explain the key security features provided by SSH



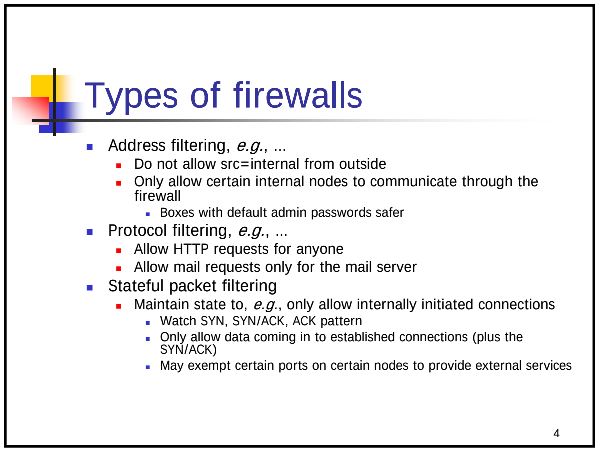
Firewalls

- Computer that sits between 2 networks and blocks certain types of traffic
  - Ideally: break-ins from outside, transmission of company secrets
- Defense in depth
  - Difficult to secure entire network
  - Computers run many services that should not be accessed externally
    - Even if properly configured, may have vulnerabilities (unchecked buffers, ...)



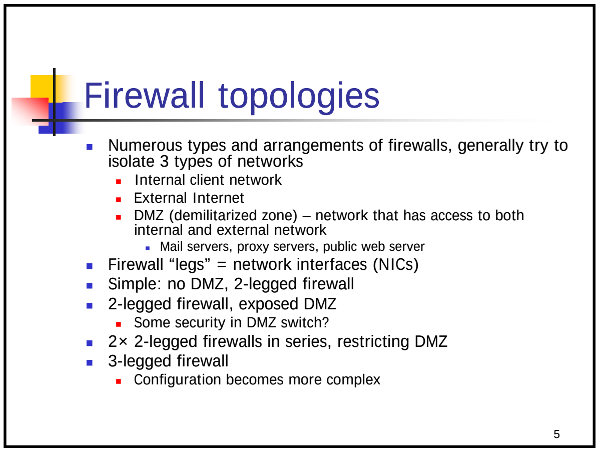
Firewall configuration

- Sometimes very limited – a checklist of options
  - Allow outbound HTTP
  - Block inbound pings (ICMP echo requests)
  - Allow inbound ping responses (ICMP echo replies)
  - ...
- Others allow complex rule sets that consider
  - Recent traffic
  - Destination and source IP and port
  - Time of day
  - Content of packet



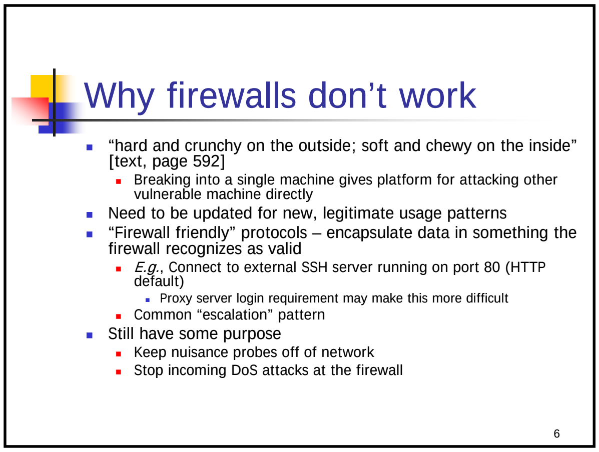
Types of firewalls

- Address filtering, *e.g.*, …
  - Do not allow src=internal from outside
  - Only allow certain internal nodes to communicate through the firewall
    - Boxes with default admin passwords safer
- Protocol filtering, *e.g.*, …
  - Allow HTTP requests for anyone
  - Allow mail requests only for the mail server
- Stateful packet filtering
  - Maintain state to, *e.g.*, only allow internally initiated connections
    - Watch SYN, SYN/ACK, ACK pattern
    - Only allow data coming in to established connections (plus the SYN/ACK)
    - May exempt certain ports on certain nodes to provide external services



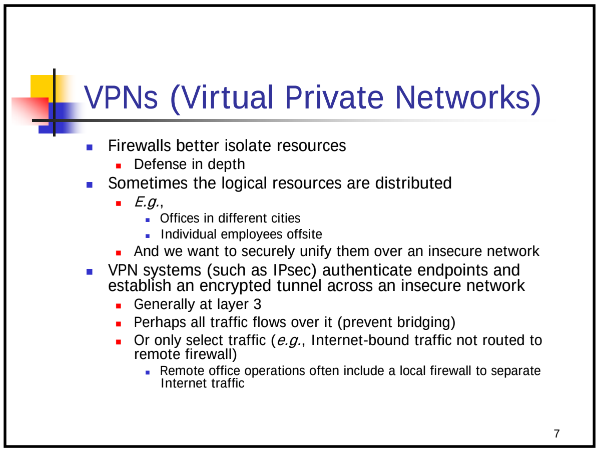
Firewall topologies

- Numerous types and arrangements of firewalls, generally try to isolate 3 types of networks
  - Internal client network
  - External Internet
  - DMZ (demilitarized zone) – network that has access to both internal and external network
    - Mail servers, proxy servers, public web server
- Firewall “legs” = network interfaces (NICs)
- Simple: no DMZ, 2-legged firewall
- 2-legged firewall, exposed DMZ
  - Some security in DMZ switch?
- 2× 2-legged firewalls in series, restricting DMZ
- 3-legged firewall
  - Configuration becomes more complex



Why firewalls don’t work

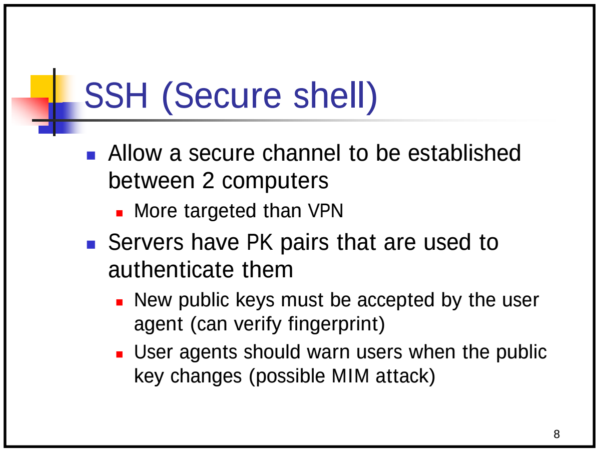
- “hard and crunchy on the outside; soft and chewy on the inside” [text, page 592]
  - Breaking into a single machine gives platform for attacking other vulnerable machine directly
- Need to be updated for new, legitimate usage patterns
- “Firewall friendly” protocols – encapsulate data in something the firewall recognizes as valid
  - *E.g.*, Connect to external SSH server running on port 80 (HTTP default)
    - Proxy server login requirement may make this more difficult
  - Common “escalation” pattern
- Still have some purpose
  - Keep nuisance probes off of network
  - Stop incoming DoS attacks at the firewall



VPNs (Virtual Private Networks)

- Firewalls better isolate resources
  - Defense in depth
- Sometimes the logical resources are distributed
  - *E.g.*,
    - Offices in different cities
    - Individual employees offsite
  - And we want to securely unify them over an insecure network
- VPN systems (such as IPsec) authenticate endpoints and establish an encrypted tunnel across an insecure network
  - Generally at layer 3
  - Perhaps all traffic flows over it (prevent bridging)
  - Or only select traffic (*e.g.*, Internet-bound traffic not routed to remote firewall)
    - Remote office operations often include a local firewall to separate Internet traffic

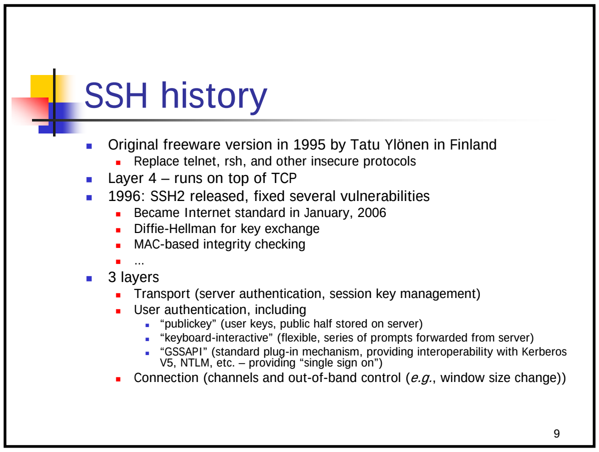
7



SSH (Secure shell)

- Allow a secure channel to be established between 2 computers
  - More targeted than VPN
- Servers have PK pairs that are used to authenticate them
  - New public keys must be accepted by the user agent (can verify fingerprint)
  - User agents should warn users when the public key changes (possible MIM attack)

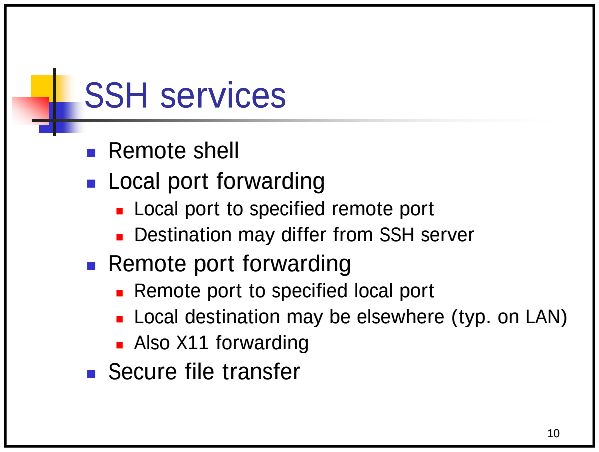
8



SSH history

- Original freeware version in 1995 by Tatu Ylönen in Finland
  - Replace telnet, rsh, and other insecure protocols
- Layer 4 – runs on top of TCP
- 1996: SSH2 released, fixed several vulnerabilities
  - Became Internet standard in January, 2006
  - Diffie-Hellman for key exchange
  - MAC-based integrity checking
  - ...
- 3 layers
  - Transport (server authentication, session key management)
  - User authentication, including
    - “publickey” (user keys, public half stored on server)
    - “keyboard-interactive” (flexible, series of prompts forwarded from server)
    - “GSSAPI” (standard plug-in mechanism, providing interoperability with Kerberos V5, NTLM, etc. – providing “single sign on”)
  - Connection (channels and out-of-band control (*e.g.*, window size change))

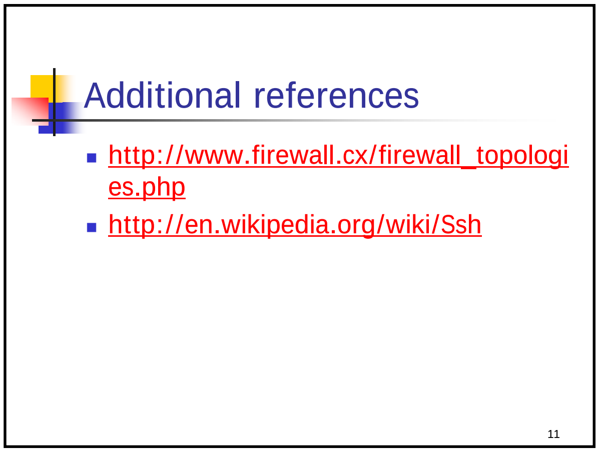
9



SSH services

- Remote shell
- Local port forwarding
  - Local port to specified remote port
  - Destination may differ from SSH server
- Remote port forwarding
  - Remote port to specified local port
  - Local destination may be elsewhere (typ. on LAN)
  - Also X11 forwarding
- Secure file transfer

10



Additional references

- http://www.firewall.cx/firewall_topologies.php
- http://en.wikipedia.org/wiki/Ssh

11