

Class Nine – Network Security

Topics (security by OSI layer):

- **Layer 1 - Physical:**
 - Modems
 - Wireless
- **Layer 2 – Data Link:**
 - Switches and Virtual Local Area Network (VLAN)
 - Wireless
- **Layer 3 - Network:**
 - Network Address Translation (NAT)
 - Virtual Private Networks (VPNs)
- **Layer 4 – Transport/session layers**
 - Secure Sockets (SSL)
- **Firewalls (all layers)**

8/24/2007

Class 9

1

Layer 1 - Dial-In Connections

- **Vulnerabilities:**
 - Unauthorized use by authorized parties
 - War games dialers (Toneloc, etc.)
 - Session hi-jacking
 - Call forwarding, or re-programming of numbers (a type of routing attack)
- **Counter-measures:**
 - Control dial-in access points
 - Dial-back modems
 - Modem passwords
 - One-time authentication

8/24/2007

Class 9

2

Layer 1 - Wireless

- Vulnerabilities:
 - Eavesdropping
 - Theft of network services
 - Access point impersonation
 - Illicit entry to internal networks
 - Denial of service (jamming)
- Physical Layer Counter-measures:
 - Use lower power
 - Directional antennas
 - Shield physical perimeter from RF
- Note that wireless physical layer measures tend to be either very costly, annoying to legitimate users, or ineffective against determined attackers

8/24/2007

Class 9

3

Layer 2 - Switched Network Security

- Switches vs. hubs
 - Hubs – all traffic mirrored on all physical ports
 - Switches –only send traffic on port having destination device
- Security features of a switched backbone
 - Deters sniffing traffic not specifically designated for segment
 - Can be broken – do not rely on this as your sole security measure for sensitive traffic
- What's a Virtual Local Area Network (VLAN)
 - Groups users together based on common communication needs
 - Group may extend across WAN (VLAN identity preserved across switches)
 - Broadcast traffic restricted to within a VLAN group
 - Stronger security than simple switching

8/24/2007

Class 9

4

Layer 2 - Wireless Security

- Link encryption from client to the access point
 - WEP – Wired Equivalent Privacy
 - WPA – WiFi Protected Access
 - WPA2 - WiFi Protected Access 2
- WEP has been broken
 - Cryptographic keys can be figured out given enough traffic
 - Poorly chosen checksum algorithm allows modifying messages without detection
 - Weak vendor implementations compound these failings and others
- WPA2 with Temporal Key Integrity Protocol (TKIP) is current recommendation
 - Uses best currently know cryptographic algorithms
 - Keys are changed very frequently via TKIP
 - Access point must authenticate itself to clients (much harder for attacker to insert bogus access point)

8/24/2007

Class 9

5

Layer 3 – Network Layer Security

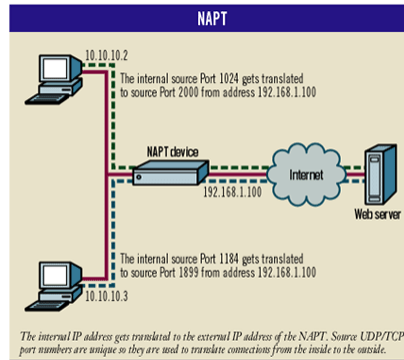
- Firewalls (secure Internet gateways)
 - Filter traffic based on Layer 3 criteria
 - More on this later
- IP- Layer Encryption (IPSec)
 - Encryption, authentication at network layer
 - A different protocol from IP
 - A true network layer Virtual Private Network
- Network Address Translation
 - Masks internal addresses from unauthorized outside nodes
 - Single (or small number of) external addresses map to much larger pool of internal addresses
 - RFC 1631, use of private addresses while connecting to the public Internet

8/24/2007

Class 9

6

Network Address (Port) Translation



From Network Computing, November 27 2000,
<http://www.networkcomputing.com/1123/1123ws2.html>

8/24/2007

Class 9

7

Virtual Private Networks

- How used
 - Mobile users
 - Branch office to corporate
 - Other point-to-point
- Protocols:
 - Level 2 Transport Protocol (L2TP), RFC 2341 & RFC 2661
 - Layer 2, hence independent of network layer
 - Point to Point Tunneling Protocol (PPTP) RFC 2637
 - Microsoft supported
 - PPP based, designed for dial-in remote access
 - IPSec
 - Currently accepted standard
 - True Layer 3 VPN

8/24/2007

Class 9

8

IPSec

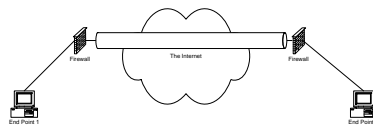
- Described in IETF RFCs 1825 and 2401
- Works with both IP version 4 (current) and IP version 6 (proposed)
- IPSec Components
 - Authentication Header (AH): Provides authenticity guarantee for packets
 - Encapsulating Security Payload (ESP): Provides confidentiality guarantee for packets, by encrypting packets
 - IP payload compression (IPcomp): provides a way to compress packet before encryption by ESP (Of course, you can use IPcomp alone if you wish to)
 - Internet Key Exchange (IKE): Secure key negotiation between partners.
- Transport and Tunnel mode
 - Transport – client-to-client
 - Tunnel – gateway-to-gateway
- Policy management (which packets must be secured)
 - IP Address for host or subnet
 - Socket from which packet originates

8/24/2007

Class 9

9

IPSec Tunnel Mode



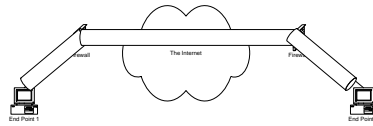
- Gateway to Gateway
- Entire IP packet encrypted
 - New header wraps existing packet
 - New source and destination addresses are that of gateways
 - Gateways wrap and unwrap
- Provides some protection against traffic analysis
 - Outsider doesn't know which host in a network is talking to which other host
- Using NAT is feasible, if gateways translate after unwrapping packet

8/24/2007

Class 9

10

IPSec Transport Mode



- Endpoint to Endpoint
- Only IP payload encrypted (plus a few other things like ports)
- Original source and destination remains
- Using NAT is infeasible
 - Translating address causes packet authentication to fail

8/24/2007

Class 9

11

Layer 4 – Session Layer Security

- Firewalls (secure Internet gateways)
 - Filter traffic based on Layer 4 criteria
 - More on this later
- Session-Level Encryption (SSL)/Transport Layer Security (TLS)
 - SSL was Netscape's original version, the current IETF standard is called TLS
 - Generally used for secure Web access, but any TCP-based application can use for SSL security
 - Can even be used as a "layer 4 VPN", for example the OpenVPN product
 - Server must authenticate to client, client may optionally authenticate to server
 - Protocol involves three basic phases:
 - Client/server negotiate which cryptographic algorithms preferred/supported
 - Public key exchange to authenticate and securely pass the private session key
 - Encrypted session using the negotiated private session key

8/24/2007

Class 9

12

Layer 3, 4 and above - Firewalls

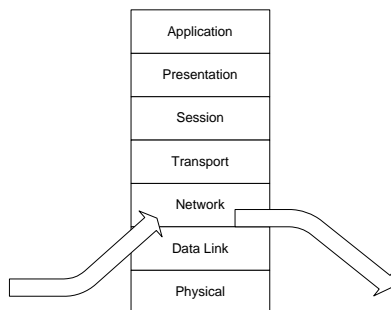
- Separate networks having different security policies and different threat levels:
 - Internal network vs. public Internet vs. publicly accessible servers
 - Internal sub-networks having different sensitivity levels
 - Remote access to internal networks
- Firewall types based on layers of OSI model:
 - Packet filters
 - Stateful Packet inspection
 - Circuit Gateways
 - Application Gateways or Proxy Servers

8/24/2007

Class 9

13

Internet Security – Packet Filter Firewalls



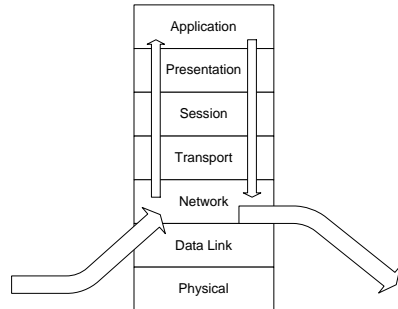
- Filter traffic based on IP-level information
 - From/To IP address
 - Port requested
 - Protocol (TCP, UDP, ICMP)
 - Physical interface
- Packet-by-Packet control
- No knowledge of session status (stateless)
- Typical example a router configured to filter traffic

8/24/2007

Class 9

14

Internet Security – Stateful Inspection Firewalls



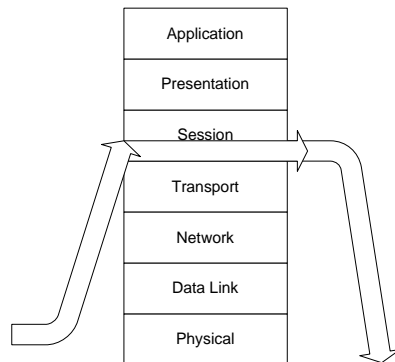
- Start with a packet filter, then add:
 - Ability to maintain state, by “remembering” earlier packets in session
 - Selective analysis of packet data contents (higher level protocol information)
- Can be very fast
- Examples:
 - Checkpoint Firewall-1
 - Cisco PIX

8/24/2007

Class 9

15

Internet Security – Circuit Gateway Firewalls



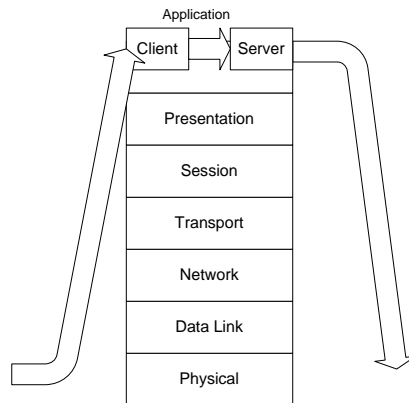
- Proxies session between end points
- Defeats attacks based on confounding session-level logic
 - out-of-sequence packets
 - packet fragments
- Generic
- No awareness of application level logic
- Difficult to use for sessionless UDP-based services
- SOCKS is primary example
- Other firewall products support session level proxies as a “generic proxy”

8/24/2007

Class 9

16

Internet Security – Application Gateway Firewalls



- Proxies application-level service
- Acts as both client and server
- Fine granularity of control (i.e., FTP GET vs. PUT)
- Defends against application-layer attacks
- Slower than other models
- Proprietary protocols “problematic”
- “Behind the curve” for new services
- Examples:
 - Raptor
 - Gauntlet

8/24/2007

Class 9

17

Firewall Topologies (“Architectures”)

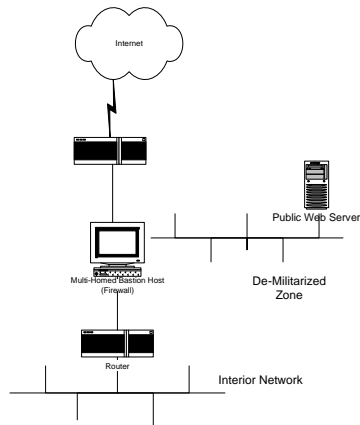
- Placement of firewall with respect to outside and inside networks
- Arrangement of supporting network devices (routers, etc.) with respect to firewall
- Components
 - Redundant firewall devices for continuity of operations
 - Multiple subnets with different screening criteria for different purposes
 - Bastion Host (host publicly visible, hence must be highly fortified)
 - Exterior or Border Router
 - Interior Router

8/24/2007

Class 9

18

Firewall Topologies - Screened Subnet (for almost all shops)



8/24/2007

Class 9

19

Advanced Firewall Capabilities

- Authentication
- Access Control
- Content Filtering
- Network Address Translation
- Load Balancing (among Internet servers)
- Redundancy for fail over
- Virtual Private Networks
 - Uses traffic encryption to obtain services equivalent to a dedicated link over the Internet
 - Requires high levels of confidentiality, integrity, and authentication of communicating parties
 - May use IPSec, PPTP, L2TP or other methods

8/24/2007

Class 9

20