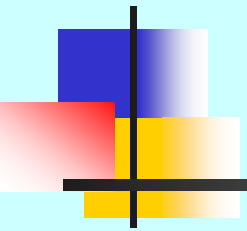
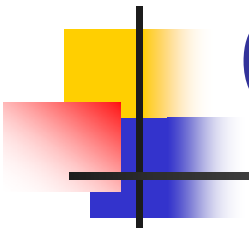


Chapter 7: Securing The INTERNET

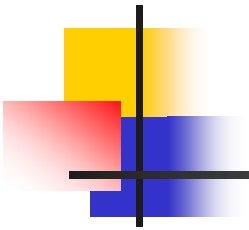


Objectives

- In this chapter we want to show how certain security aspects, particularly privacy and message authentication, can be applied to the network, transport, and application layers of the Internet model.
- We will briefly show how the IPsec protocol can add authentication and confidentiality to the IP protocol.
- How SSL/TLS can do the same for the TCP protocol.
- HTTPs and FTP security protocols are also discussed.

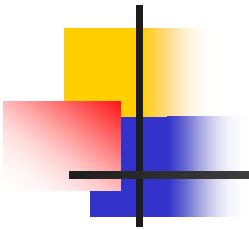
Objectives (cont.)

- Wireless security is also briefly described.
- We also discuss a common protocol, the virtual private network (VPN)
- We also discuss Firewalls, a mechanism for preventing the attack on the network of an organization.
- Also, intrusion-detection systems IDSs and network monitoring and diagnostic devices are discussed.
- Finally, virtual local area networks (VLANs) and Honeypots are discussed



IPSec

- Different security tools function at different layers of the Open System Interconnection (OSI) model
- Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) operate at the Application layer
- Kerberos functions at the Session layer



IPSecurity (IPSec)

- IPsec is a collection of protocols designed to provide security for a packet at the network level.
- Considered to be a transparent security protocol
- Transparent to applications, users, and software
- Provides three areas of protection that correspond to three IPSec protocols:
  - Authentication
  - Confidentiality
  - Key management
- IPSec helps to create authenticated and confidential packets for the IP layer.
- IPsec operates in one of two modes: the transport mode or the tunnel mode.

IP Security (IPSec) (cont.)

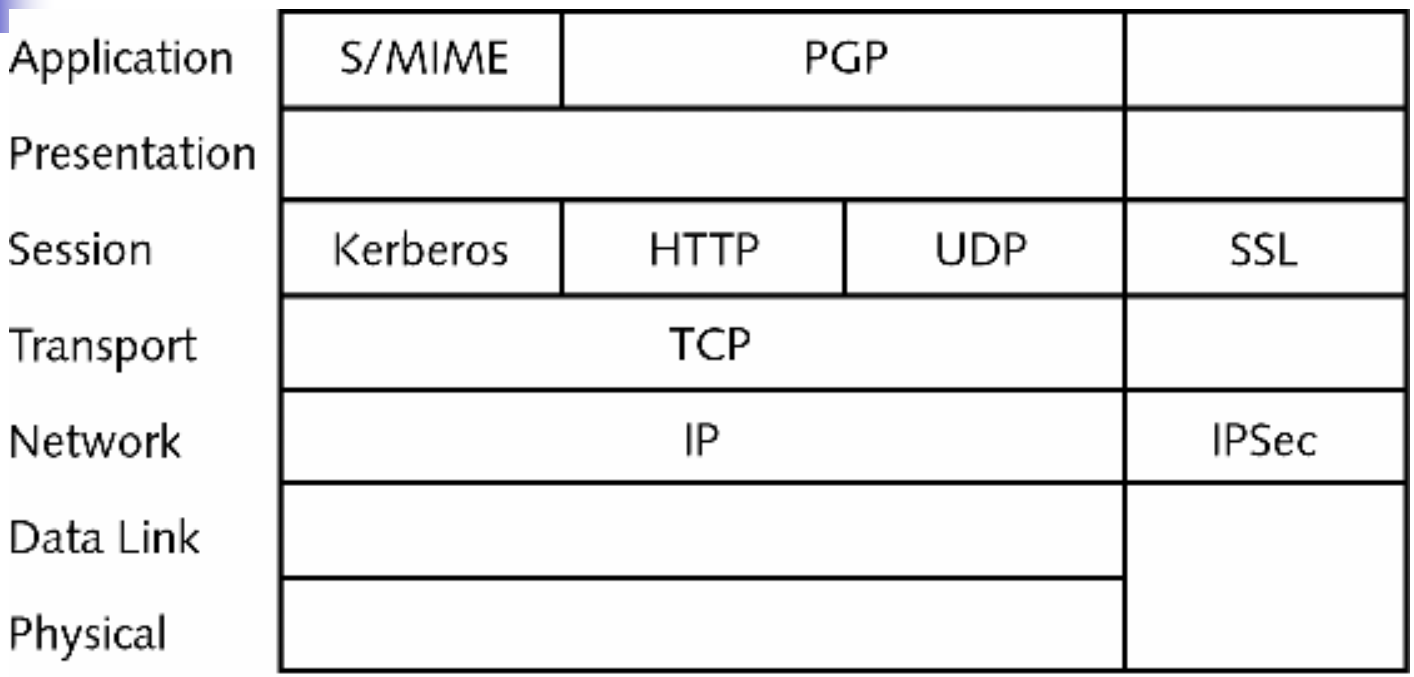


Figure 1 Security tools and the OSI model

IPSec Packet

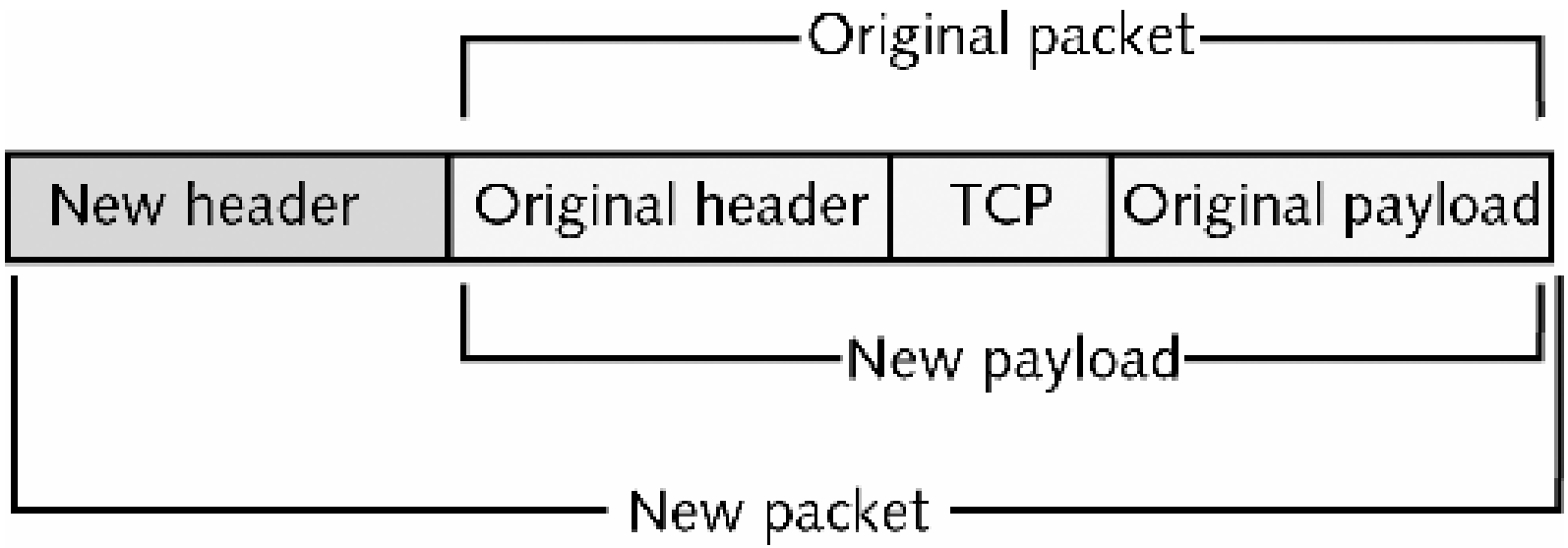
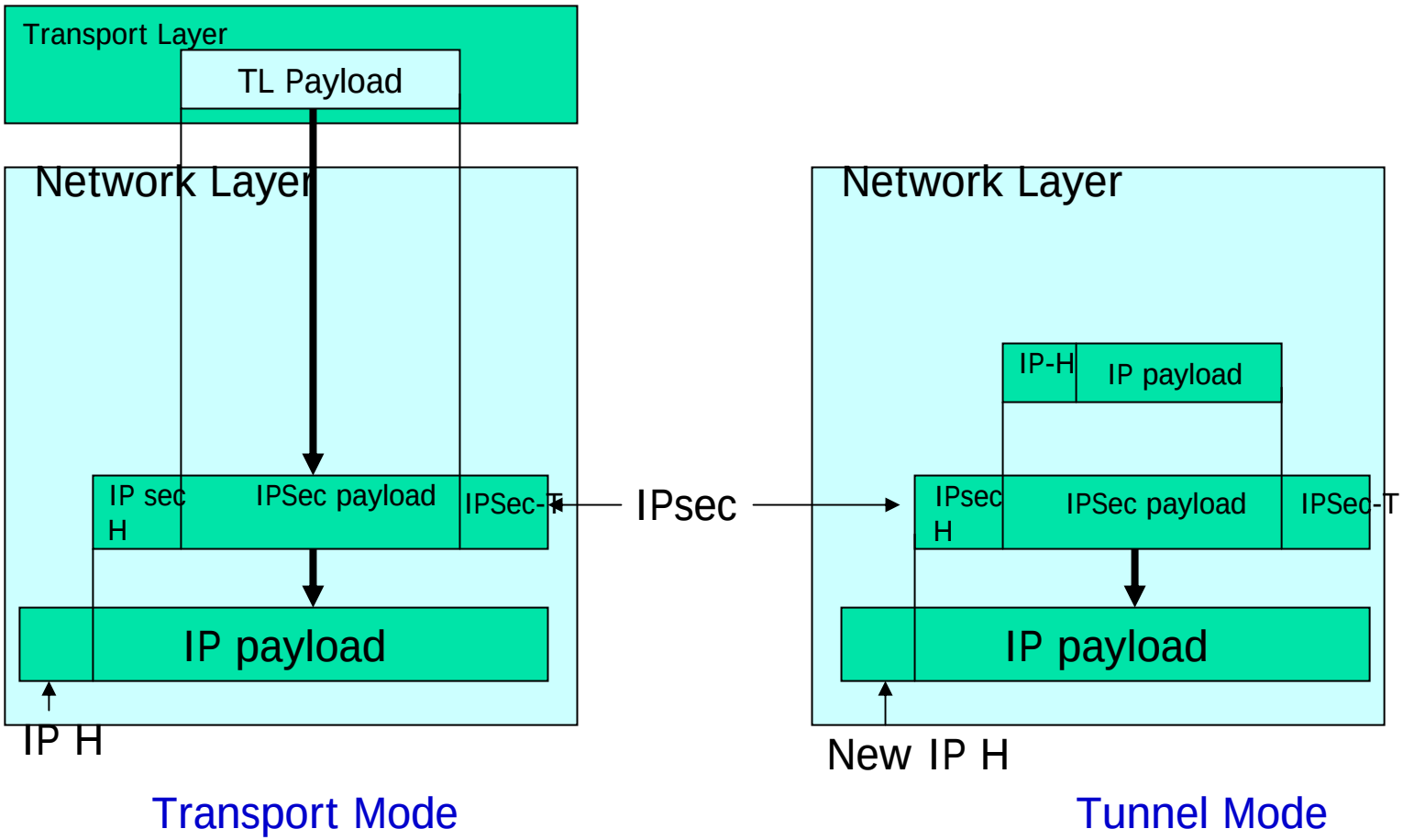


Figure 2 New IPSec packet

Transport Mode and Tunnel Mode



Transport Mode

Tunnel Mode

IPSec Transport Mode

- In this mode ,IPSec protects what is delivered from the transport layer to the network layer i.e. this mode the network layer payload is protected, the payload to be encapsulated in the network layer.
- Note: this mode does not protect the IP header.
- In other words, the transport mode does not protect the whole IP packet; it protects only the packet from the transport layer.
- In this mode, the IPSec header and trailer are added to the information coming from the transport layer. The IP header is added later.
- This mode is normally used when we need host-to-host (end-to-end) protection of data.

IPSec Tunnel Mode

- In this mode, IPSec protects the entire IP packet.
- It takes an entire IP packet, including the header, applies IPSec methods to the entire packet, and then adds a new IP header which has different information than the original IP header.
- The tunnel mode is normally used between two routers, between a host and a router, or between a router and a host.
- The entire packet is protected from intrusion between the sender and the receiver.
- It is as though the whole packet goes through an imaginary tunnel.

IPSec Protocols : AH and ESP

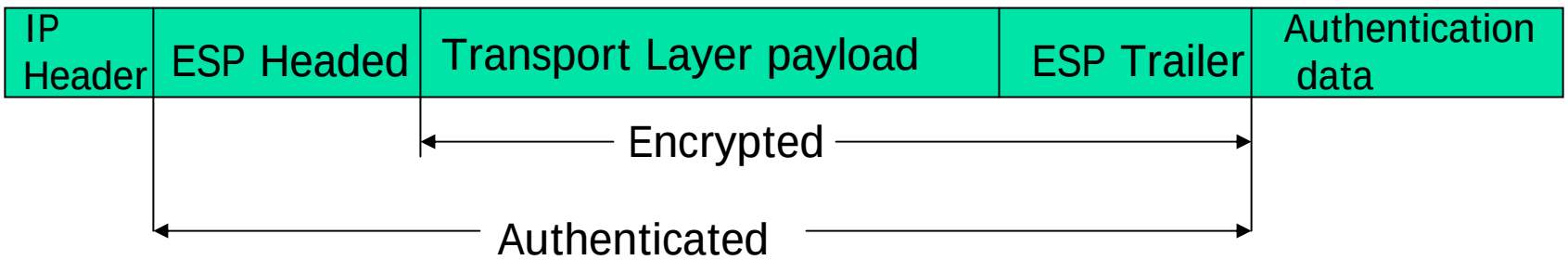
- Authentication Header protocol (AH) is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet.
- The protocol uses a hash function and a symmetric key to create a message digest; the digest is inserted in the authentication header.
- The AH is then placed in the appropriate location based on the mode (transport or tunnel mode)

Authentication Header Protocol in Transport Mode

Note : The AH protocol provides source authentication and data integrity, but not privacy

IPSec Encapsulating Security Payload (ESP)

- IPSEC defined an alternative protocol that provides source authentication, integrity, and privacy called ESP.
- ESP adds a header and trailer.



Services Provided by IPSec

Services	AH	ESP
Access Control	Yes	Yes
Message authentication (and integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

Secure Socket Layer SSL and Transport Layer Security TLS

- SSL is a general purpose protocol developed by Netscape for managing the encryption of information being transmitted over the Internet.
- Today, SSL is almost ubiquitous with respect to e-commerce – all browsers support it do web servers.
- Virtually all sensitive financial traffic from

  e-commerce web sites use this method to protect information in transit between servers and browsers.

SSL / TLS (cont.)

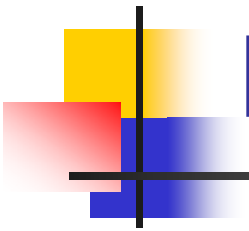
- The Internet Engineering Task Force (IETF) embraced SSL in 1996 through a series of RFCs and the group Transport Layer Security (TLS)
- Starting with SSL 3.0 in 1999 the IETF issued RFC 2246, “TLS Protocol Version 1.0”
- Followed by RFC 2712 ,which added Kerberos authentication
- Then RFCs 2817 and 2818 which extended TLS to HTTP version 1.1
- Today, TLS and SSL are essentially the same protocol although not interchangeable.

SSL / TLS (cont.)

- SSL/TLS is a series of functions that exist in the OSI model between the application layer and the TCP/IP implementation in the transport and network layers.
- The goal of TCP is to send an unauthorized error-free stream of information between two computers.
- SSL/TLS adds message integrity and authentication functionality to TCP through the use of cryptographic methods.

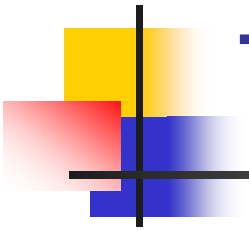
SSL / TLS Initiation

- When two programs initiate an SSL/TLS connection, one of the first tasks is to compare available protocols and agree on an appropriate common cryptographic protocol to use in this particular communication.
- As SSL/TLS can use separate algorithms and methods for encryption, authentication, and data integrity, each of these is negotiated and determined depending upon need at the beginning of a communication.



How SSL/TLS Works

- SSL/TLS uses a wide range of cryptographic protocols.
- An agreement between the client and server must be reached on which protocols to use.
- The SSL handshake process is used to accomplish this task.

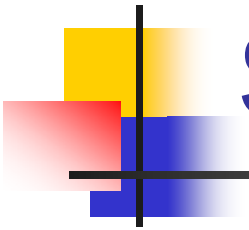


The SSL Handshake Process

- The handshake process begins with a client request for a secure connection, and a server's response.
- The questions to be answered are which protocol and which cryptographic algorithm will be used.
- For client and server to communicate, both sides have to agree on a commonly held protocol (SSL v1, v2, v3, or TLS v1)
- Commonly available cryptographic algorithms include Diffie Hellman and RSA.

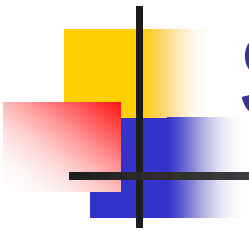
The SSL Handshake Process (cont.)

- The next step is to exchange certificates and keys as necessary to enable authentication
- Authentication was a one-way process for SSL v1 and v2, with only the server providing authentication.
- In SSL v3/TLS, mutual authentication of both client and server is possible.
- The certificate exchange is via X.509 certificates, and public key cryptography is used to establish authentication.
- Once authentication is established, the channel is secured with symmetric key cryptographic methods and hashes , typically RC4 or 3DES for symmetric key and MD5 or SHA-1 for the hash functions.



SSL and Certificates

- The use of certificates could present a lot of data and complication to a user.
- Fortunately, browsers have incorporated much of this desired functionality into a seamless operation.
- Once you have decided to always accept code from XYZ Corp., subsequent certificate checks are handled by the browser .
- The ability to manipulate certificate settings is through the OPTIONS menu in Internet Explorer.



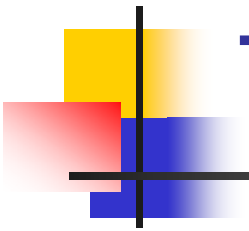
SSL and Security

- SSL/TLS is specifically designed to provide protection from man-in-the-middle attacks.
- By authenticating the server end of the connection, SSL/TLS prevents the initial hijacking of a session.
- By encrypting all the conversations between the client and the server, SSL prevents eavesdropping.

SSL and Trojan Attacks

- Once a communication is in the SSL/TLS channel, it is very difficult to defeat the protocol.
- Before data enters the secured channel, however, defeat is possible.
- A Trojan program that copies keystrokes and echoes them to another TCP/IP address in parallel with the intended communication can defeat SSL/TLS, provided that the Trojan program copies the data prior to SSL/TLS encapsulation.
- This type of attack has occurred and has been used to steal passwords and other sensitive material from users, performing the theft as the user actually types in the data.

The Web (HTTP and HTTPS)

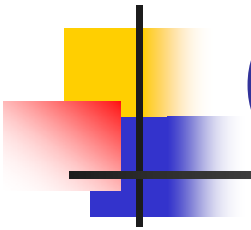


- HTTP is the protocol designated for the transfer of hypertext-linked data over the Internet, from web servers to browsers.
- HTTP traffic takes place over TCP port 80 by default, and this port is typically left open on firewalls because of this protocol.
- One of the primary drivers behind the development of SSL/TLS was the desire to hide the complexities of cryptography from end users.
- To request a secure connection use HTTPS:// in place of HTTP://

File Transfer Protocol (FTP)

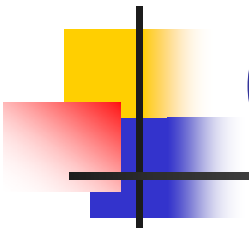
- FTP protocol is used for transferring files between computers .
- FTP is an application level protocol.
- Clients for FTP on a PC can range from an application program to the command line ftp program in Windows/DOS in most browsers
- FTP servers can be configured to allow unauthenticated users to transfer files (called anonymous FTP or blind FTP)

File Transfer Protocol (FTP) (cont.)



- Vulnerabilities associated with using FTP
  - FTP does not use encryption
  - Files being transferred by FTP are vulnerable to man-in-the-middle attacks
- Use secure FTP (SFTP) to reduce risk of attack
  - Secure FTP is a term used by vendors to describe encrypting FTP transmissions
- Most secure FTP products use Secure Socket Layers (SSL) to perform the encryption

File Transfer Protocol (FTP) (cont.)



- FTP active mode
  - Client connects from any random port >1,024 (PORT N) to FTP server's command port, port 21 (Step 1)
  - Client starts listening to PORT N+1 and sends the FTP command PORT N+1 to the FTP server
- FTP passive mode
  - Client initiates both connections to server
  - When opening an FTP connection, client opens two local random unprivileged ports >1,024

Securing File Transfer Protocol (FTP) (cont.)

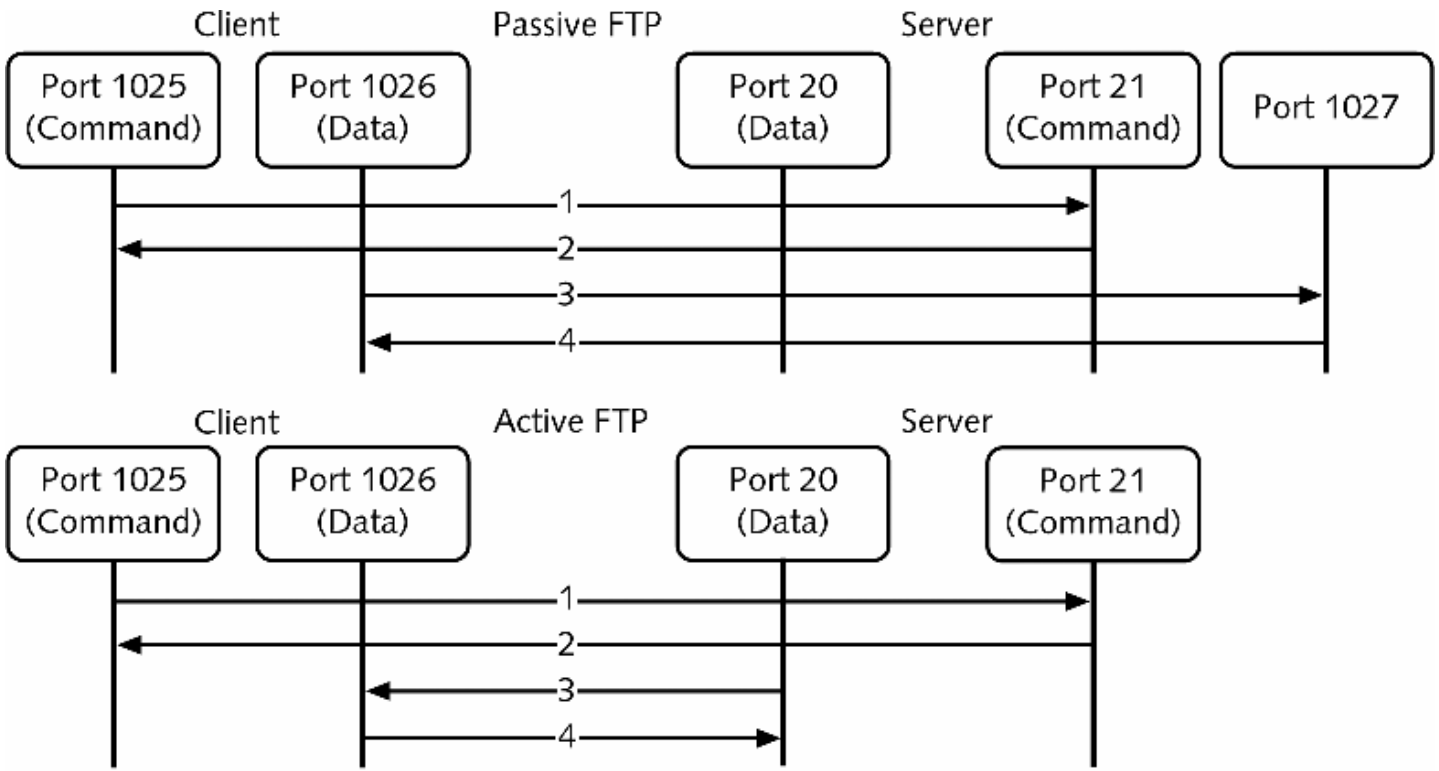
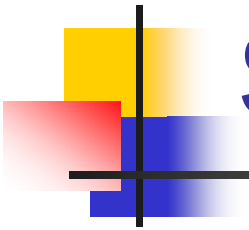
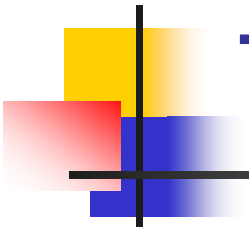


Figure 1 Active FTP and passive FTP



Secure Remote Access

- Windows NT includes User Manager to allow dial-in access, while Windows 2003 uses Computer Management for Workgroup access and Active Directory for configuring access to the domain
- Windows 2003 Remote Access Policies can lock down a remote access system to ensure that only those intended to have access are actually granted it



Tunneling Protocols

- Tunneling: technique of encapsulating one packet of data within another type to create a secure link of transportation

Tunneling Protocols (continued)

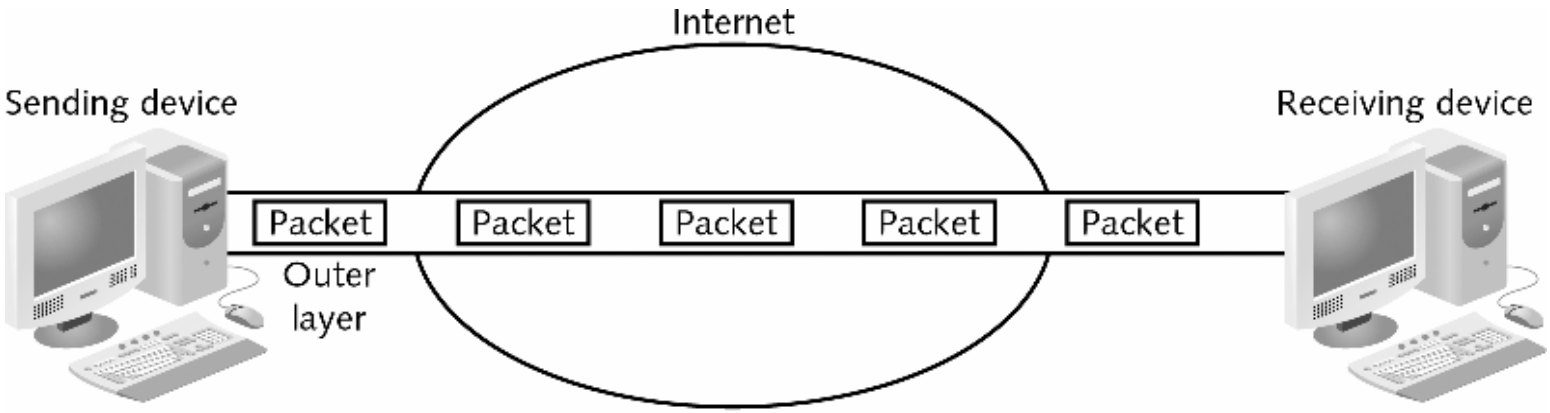


Figure 2 Tunneling

Point-to-Point Tunneling Protocol (PPTP)

- Most widely deployed tunneling protocol
- Connection is based on the Point-to-Point Protocol (PPP), widely used protocol for establishing connections over a serial line or dial-up connection between two points
- Client connects to a network access server (NAS) to initiate connection
- Extension to PPTP is Link Control Protocol (LCP), which establishes, configures, and tests the connection

Point-to-Point Tunneling Protocol (PPTP) (continued)

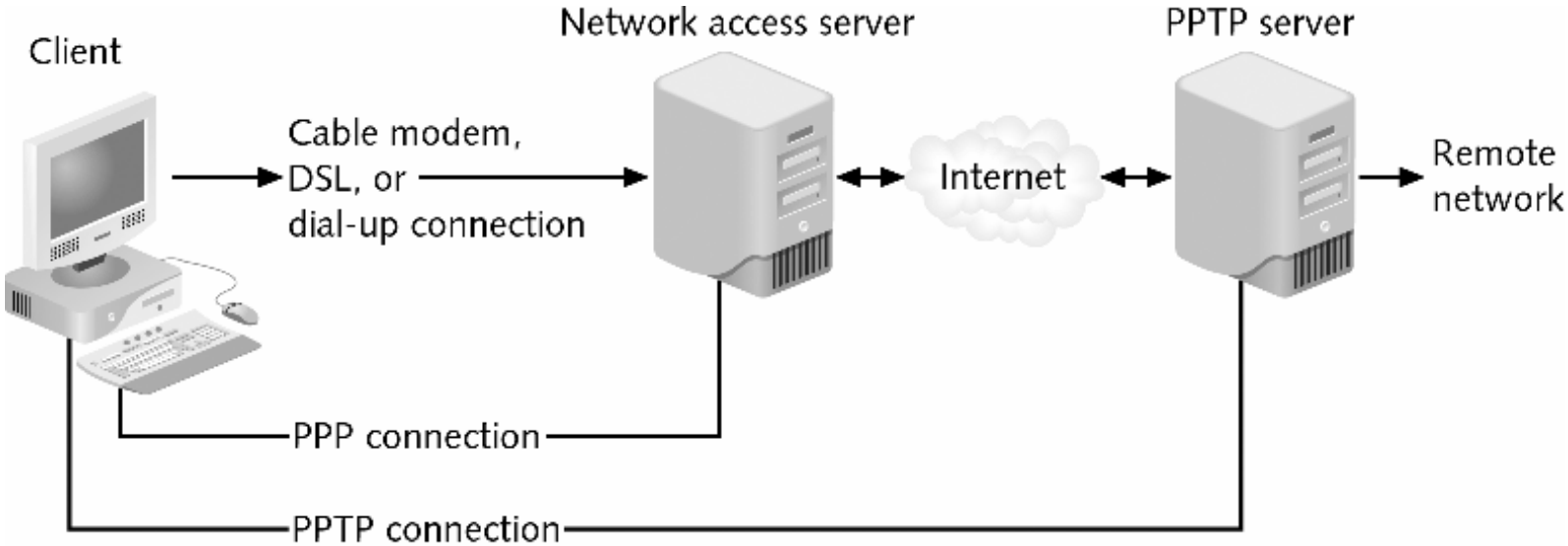
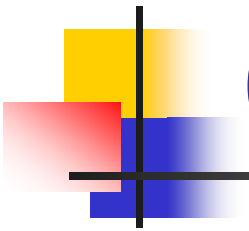


Figure 3 Point-to-Point Tunneling Protocol (PPTP)

Layer 2 Tunneling Protocol (L2TP)



- Represents a merging of features of PPTP with Cisco's Layer 2 Forwarding Protocol (L2F), which itself was originally designed to address some of the weaknesses of PPTP

- Unlike PPTP, which is primarily implemented as software on a client computer, L2TP can also be found on devices such as routers

Authentication Technologies

- Authenticating a transmission to ensure that it comes from an approved sender can provide an increased level of security for remote access users

IEEE 802.1x

- Based on a standard established by the Institute for Electrical and Electronic Engineers (IEEE)
- Gaining wide-spread popularity
- Provides an authentication framework for 802-based LANs (Ethernet, Token Ring, wireless LANs)
- Uses port-based authentication mechanisms
  - Switch denies access to anyone other than an authorized user attempting to connect to the network through that port

IEEE 802.1x (continued)

- Network supporting the 802.1x protocol consists of three elements:
  - Supplicant: client device, such as a desktop computer or personal digital assistant (PDA), which requires secure network access
  - Authenticator: serves as an intermediary device between supplicant and authentication server
  - Authentication server: receives request from supplicant through authenticator

IEEE 802.1x (cont.)

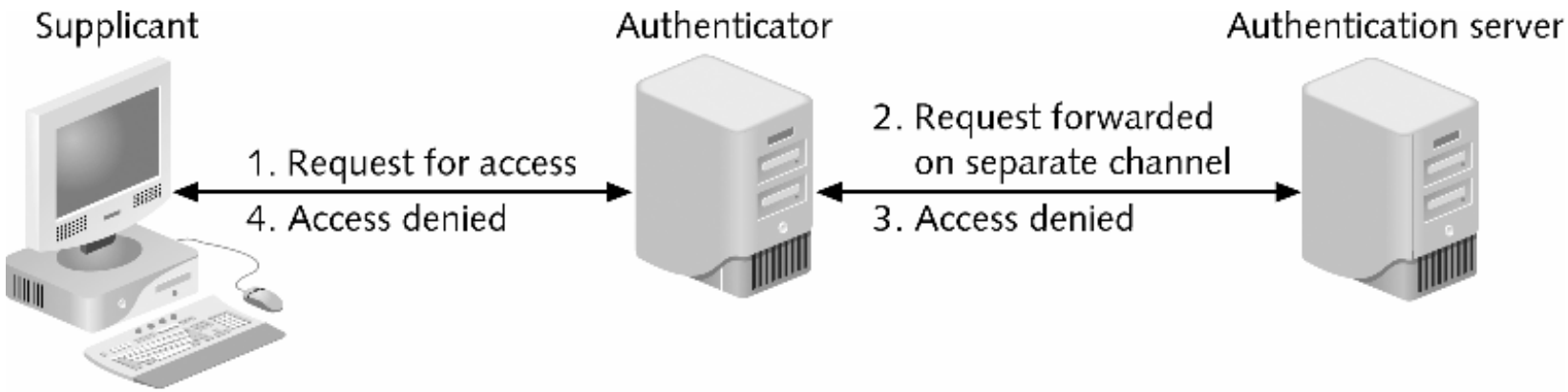


Figure 4 802.1x protocol

IEEE 802.1x (cont.)

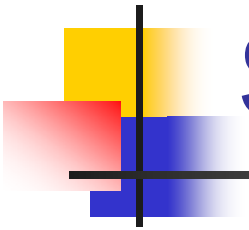
- Several variations of EAP can be used with 802.1x:
  - EAP-Transport Layer Security (EAP-TLS)
  - Lightweight EAP (LEAP)
  - EAP-Tunneled TLS (EAP-TTLS)
  - Protected EAP (PEAP)
  - Flexible Authentication via Secure Tunneling (FAST)

Remote Authentication Dial-In User Service (RADIUS)

- Originally defined to enable centralized authentication and access control and PPP sessions
- Requests are forwarded to a single RADIUS server
- Supports authentication, authorization, and auditing functions
- After connection is made, RADIUS server adds an accounting record to its log and acknowledges the request
- Allows company to maintain user profiles in a central database that all remote servers can share

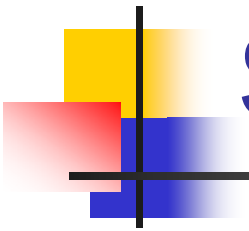
Terminal Access Control Access Control System (TACACS+)

- Industry standard protocol specification that forwards username and password information to a centralized server
- Whereas communication between a NAS and a TACACS+ server is encrypted, communication between a client and a NAS is not



Secure Transmission Protocols

- PPTP and L2TP provide a secure mechanism for preventing eavesdroppers from viewing transmissions



Secure Shell (SSH)

- One of the primary goals of the ARPANET (which became today's Internet) was remote access
- SSH is a UNIX-based command interface and protocol for securely accessing a remote computer
- Suite of three utilities—slogin, ssh, and scp
- Can protect against:
  - IP spoofing
  - DNS spoofing
  - Intercepting information

Secure Shell (SSH) (continued)

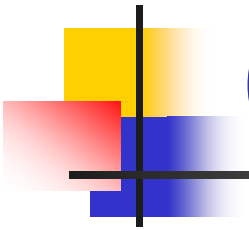
Table 1 UNIX commands

UNIX Command Name	Description	Syntax	Secure Command Replacement
rlogin	Log on to remote computer	rlogin *remotecomputer*	slogin
rcp	Copy files between remote computers	rcp [*options*] *localfile remotecomputer: filename*	scp
rsh	Executing commands on a remote host without logging on	rsh *remotecomputer command*	ssh

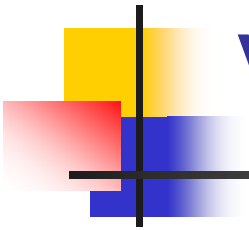
Virtual Private Networks (VPN)

- Is a technology that is gaining popularity among large organizations that use the global Internet for bot intra- and interorganization communication, but require privacy in their internal communications.

Virtual Private Networks (VPNs)

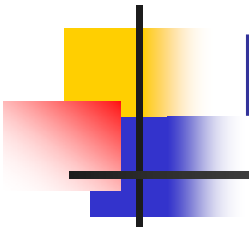


- Takes advantage of using the public Internet as if it were a private network
- Allow the public Internet to be used privately
- Prior to VPNs, organizations were forced to lease expensive data connections from private carriers so employees could remotely connect to the organization's network



Virtual Private Networks

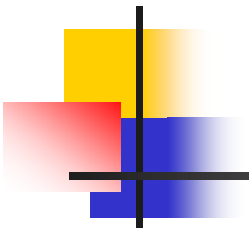
- What if a company has more than one office?
- And they are far apart?
  - Like on the opposite coasts of the US
- How can you have a secure cooperation between them?



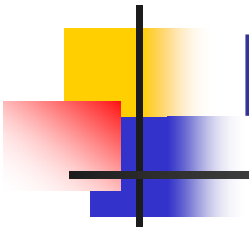
Leased Line Solution

- Lease private lines from some telephone company
- The phone company ensures that your lines cannot be tapped
  - To the extent you trust in phone company security
- Can be expensive and limiting

Another Solution via the Internet



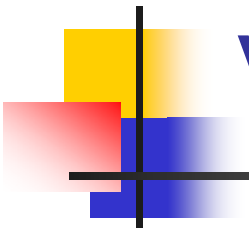
- Communicate via the Internet
  - Getting full connectivity, bandwidth, reliability, etc..
  - At a lower price, too
- But how do you keep the traffic secure?
- Encrypt everything!



Encryption and VPNs

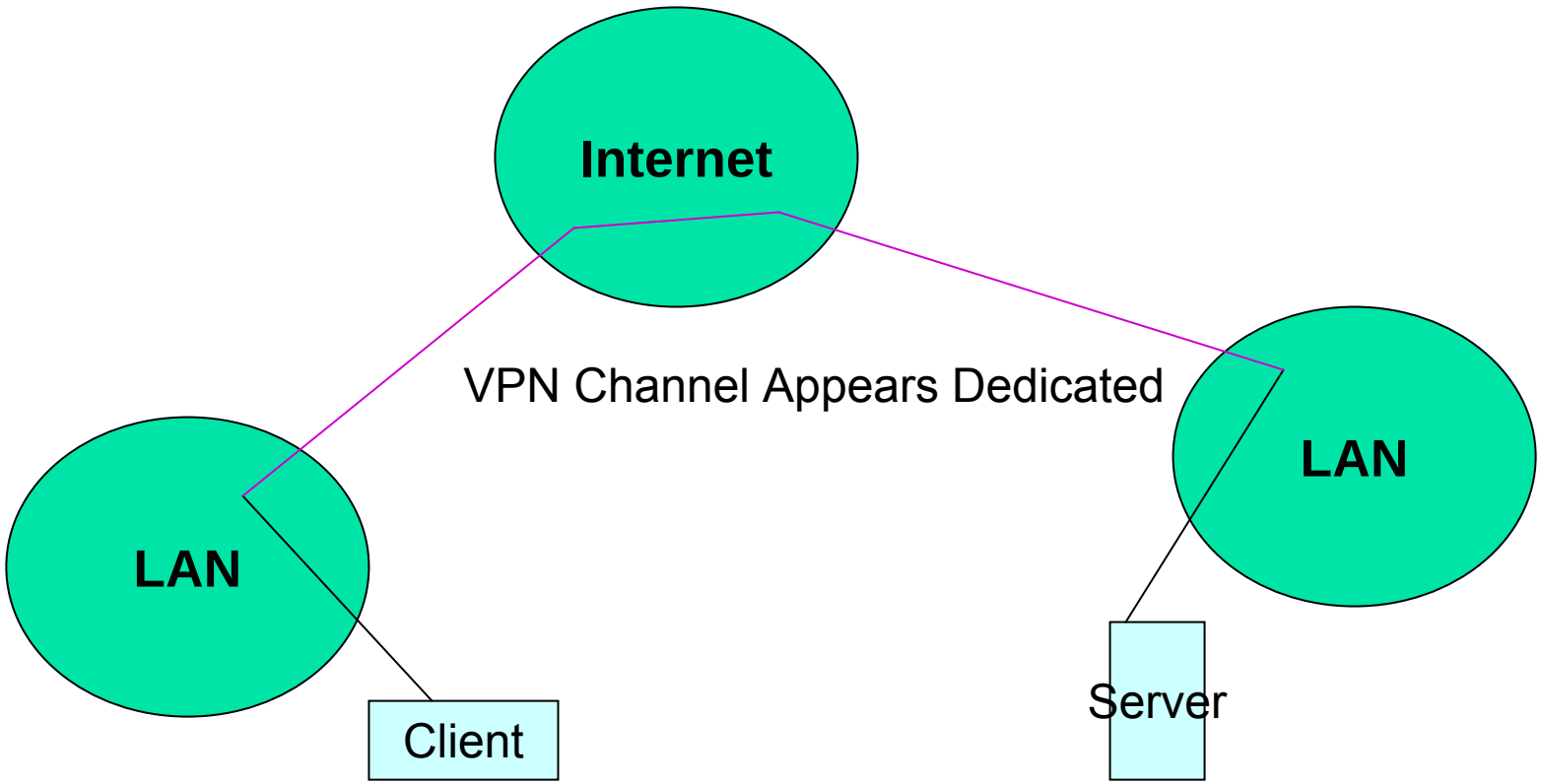
- Use encryption to convert a shared line to a private line
- Set up a firewall at each installation's network
- Set up shared encryption keys between the firewalls
- Encrypt all traffic using those keys

Actual Use of Encryption in VPNs



- VPNs run over the Internet
- Internet routers can't handle fully encrypted packets
- Obviously VPN packets aren't entirely encrypted
- They are encrypted in a tunnel mode
- VPNs typically use a tunneling protocol such as Layer2 Tunneling Protocol (L2TP), IPsec, or Point-to-Point Tunneling Protocol (PPTP)

Two LANs Being Connected Using VPN Across the Internet



Virtual Private Networks (VPNs) (cont.)

- Two common types of VPNs include:
  - Remote-access VPN or virtual private dial-up network (VPDN): user-to-LAN connection used by remote users
  - Site-to-site VPN: multiple sites can connect to other sites over the Internet
- VPN transmissions achieved through communicating with endpoints
  - An endpoint can be software on a local computer, a dedicated hardware device such as a VPN concentrator, or even a firewall

Virtual Private Networks (VPNs) (cont.)

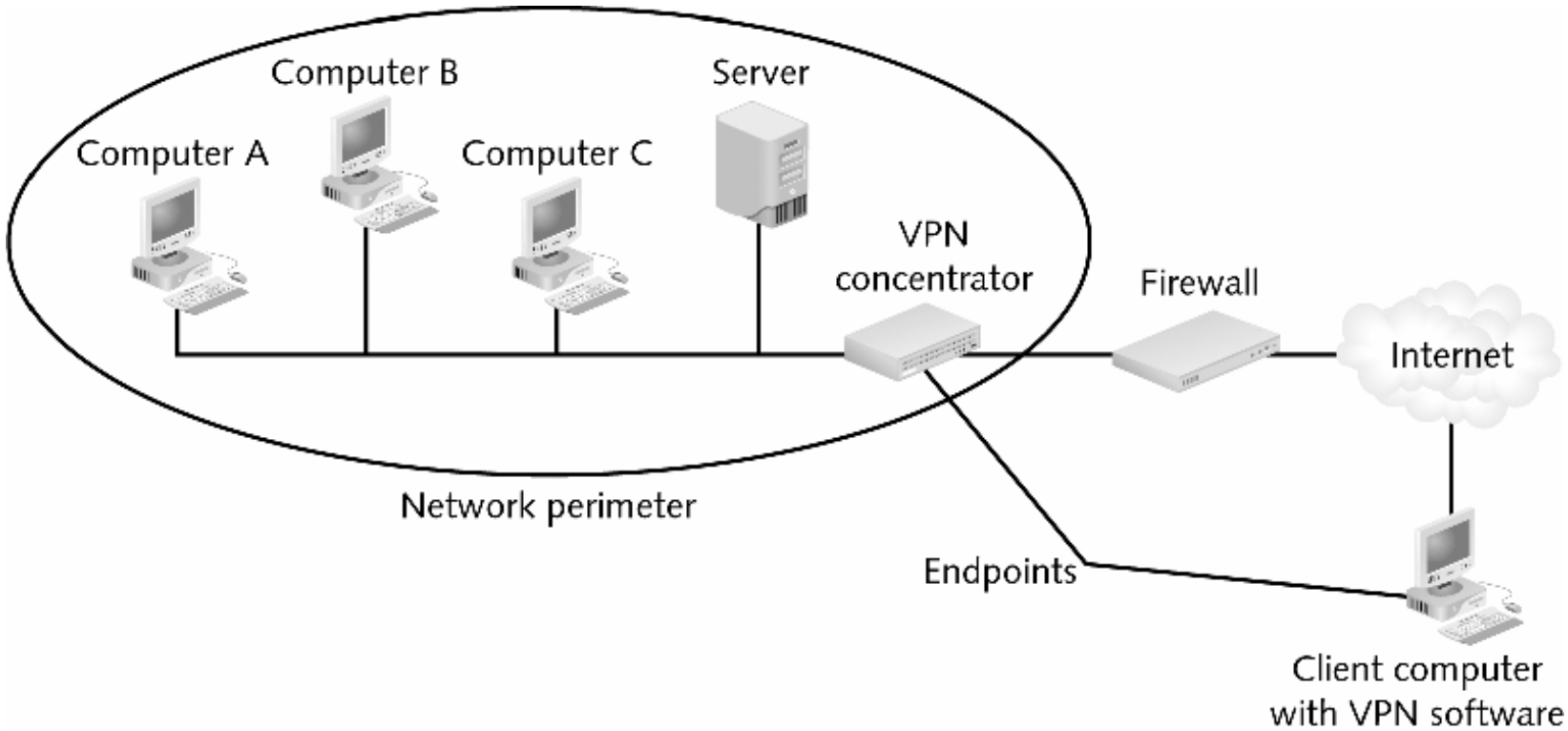
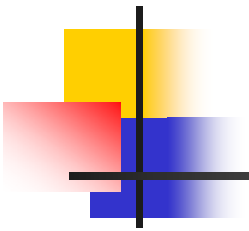


Figure 7 Virtual private network

Protecting Directory Services

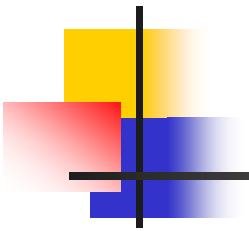
- A directory service is a database stored on the network itself and contains all information about users and network devices
- A directory service contains information such as the user's name, telephone extension, e-mail address, and logon name
- The International Standards Organization (ISO) created a standard for directory services known as X.500

Protecting Directory Services (continued)



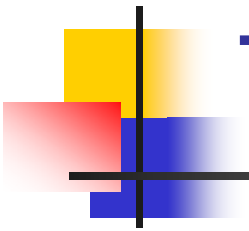
- Purpose of X.500 was to standardize how data was stored so any computer system could access these directories
- Information is held in a directory information base (DIB)
- Entries in the DIB are arranged in a directory information tree (DIT)

Protecting Directory Services (continued)



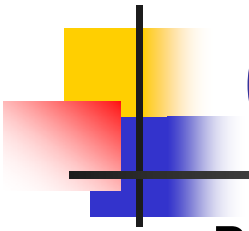
- The X.500 standard defines a protocol for a client application to access the X.500 directory called the Directory Access Protocol (DAP)
- The DAP is too large to run on a personal computer
- The Lightweight Directory Access Protocol (LDAP), or X.500 Lite, is a simpler subset of DAP

Securing Digital Cellular Telephony



- The early use of wireless cellular technology is known as First Generation (1G)
- 1G is characterized by analog radio frequency (RF) signals transmitting at a top speed of 96 Kbps
- 1G networks use circuit-switching technology
- Digital cellular technology, which started in the early 1990s, uses digital instead of analog transmissions
- Digital cellular uses packet switching instead of circuit-switching technology

Wireless Application Protocol (WAP)



- Provides standard way to transmit, format, and display Internet data for devices such as cell phones
- A WAP cell phone runs a microbrowser that uses Wireless Markup Language (WML) instead of HTML
  - WML is designed to display text-based Web content on the small screen of a cell phone
  - Because the Internet standard is HTML, a WAP Gateway (or WAP Proxy) must translate between WML and HTML

Wireless Application Protocol (WAP) (cont.)

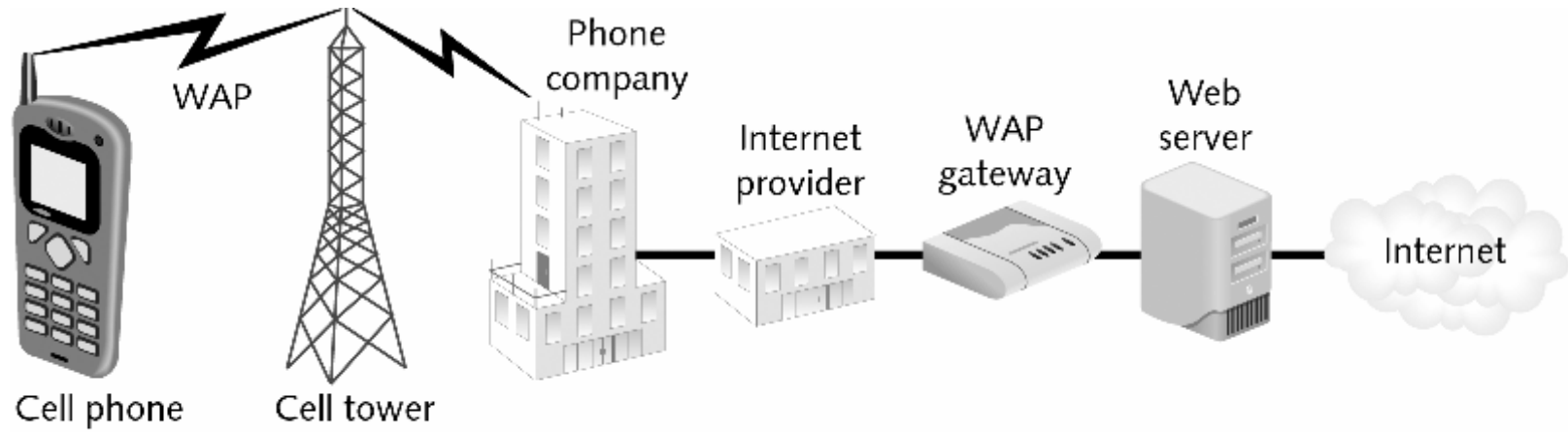
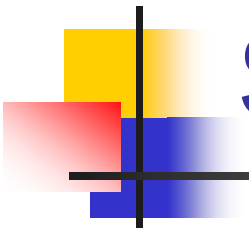


Figure 8 WAP transmission

Wireless Transport Layer Security (WTLS)



- Security layer of the WAP
- Provides privacy, data integrity, and authentication for WAP services
- Designed specifically for wireless cellular telephony
- Based on the TLS security layer used on the Internet
- Replaced by TLS in WAP 20

Securing Wireless Local Area Networks (WLAN)

- By 2007, >98% of all notebooks will be wireless-enabled
- Serious security vulnerabilities have also been created by wireless data technology:
  - Unauthorized users can access the wireless signal from outside a building and connect to the network
  - Attackers can capture and view transmitted data
  - Employees in the office can install personal wireless equipment and defeat perimeter security measures
  - Attackers can crack wireless security with kiddie scripts

IEEE 802.11 Standards

- A WLAN shares same characteristics as a standard data-based LAN with the exception that network devices do not use cables to connect to the network
- RF is used to send and receive packets
- Sometimes called Wi-Fi for Wireless Fidelity, network devices can transmit 11 to 108 Mbps at a range of 150 to 375 feet
- 802.11a has a maximum rated speed of 54 Mbps and also supports 48, 36, 24, 18, 12, 9, and 6 Mbps transmissions at 5 GHz

IEEE 802.11 Standards (cont.)

- In September 1999, a new 802.11b High Rate was amended to the 802.11 standard
- 802.11b added two higher speeds, 55 and 11 Mbps
- With faster data rates, 802.11b quickly became the standard for WLANs
- At same time, the 802.11a standard was released

WLAN Components

- Each network device must have a wireless network interface card installed
- Wireless NICs are available in a variety of formats:
  - Type II PC card
  - Mini PCI
  - CompactFlash (CF) card
  - USB device
  - USB stick

WLAN Components (cont.)

- An access point (AP) consists of three major parts:
  - An antenna and a radio transmitter/receiver to send and receive signals
  - An RJ-45 wired network interface that allows it to connect by cable to a standard wired network
  - Special bridging software

Basic WLAN Security

- Two areas:
  - Basic WLAN security
  - Enterprise WLAN security
- Basic WLAN security uses two new wireless tools and one tool from the wired world:
  - Service Set Identifier (SSID) beaconing
  - MAC address filtering
  - Wired Equivalent Privacy (WEP)

Service Set Identifier (SSID) Beaconing

- A service set is a technical term used to describe a WLAN network
- Three types of service sets:
  - Independent Basic Service Set (IBSS)
  - Basic Service Set (BSS)
  - Extended Service Set (ESS)
- Each WLAN is given a unique SSID

MAC Address Filtering

- Another way to harden a WLAN is to filter MAC addresses
- The MAC address of approved wireless devices is entered on the AP
- A MAC address can be spoofed
- When wireless device and AP first exchange packets, the MAC address of the wireless device is sent in plaintext, allowing an attacker with a sniffer to see the MAC address of an approved device

Wired Equivalent Privacy (WEP)

- Optional configuration for WLANs that encrypts packets during transmission to prevent attackers from viewing their contents
- Uses shared keys—the same key for encryption and decryption must be installed on the AP, as well as each wireless device
- A serious vulnerability in WEP is that the IV is not properly implemented
- Every time a packet is encrypted it should be given a unique IV

Wired Equivalent Privacy (WEP) (cont.)

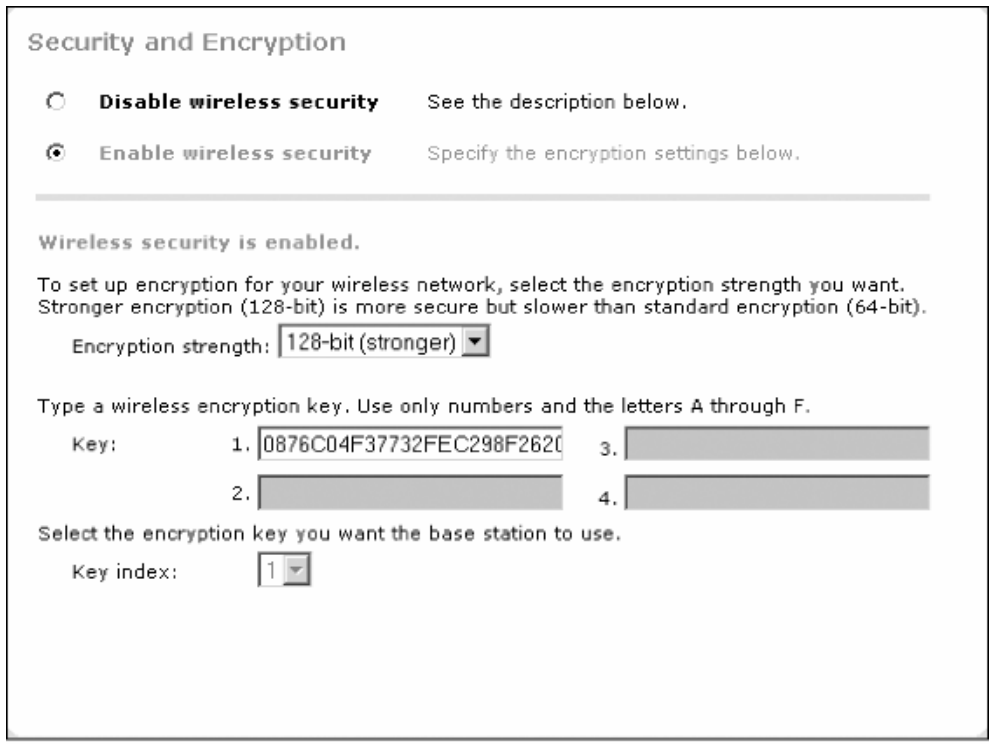


Figure 9 WEP configuration

Untrusted Network

- The basic WLAN security of SSID beaconing, MAC address filtering, and WEP encryption is not secure enough for an organization to use
- One approach to securing a WLAN is to treat it as an untrusted and unsecure network
- Requires that the WLAN be placed outside the secure perimeter of the trusted network

Untrusted Network (cont.)

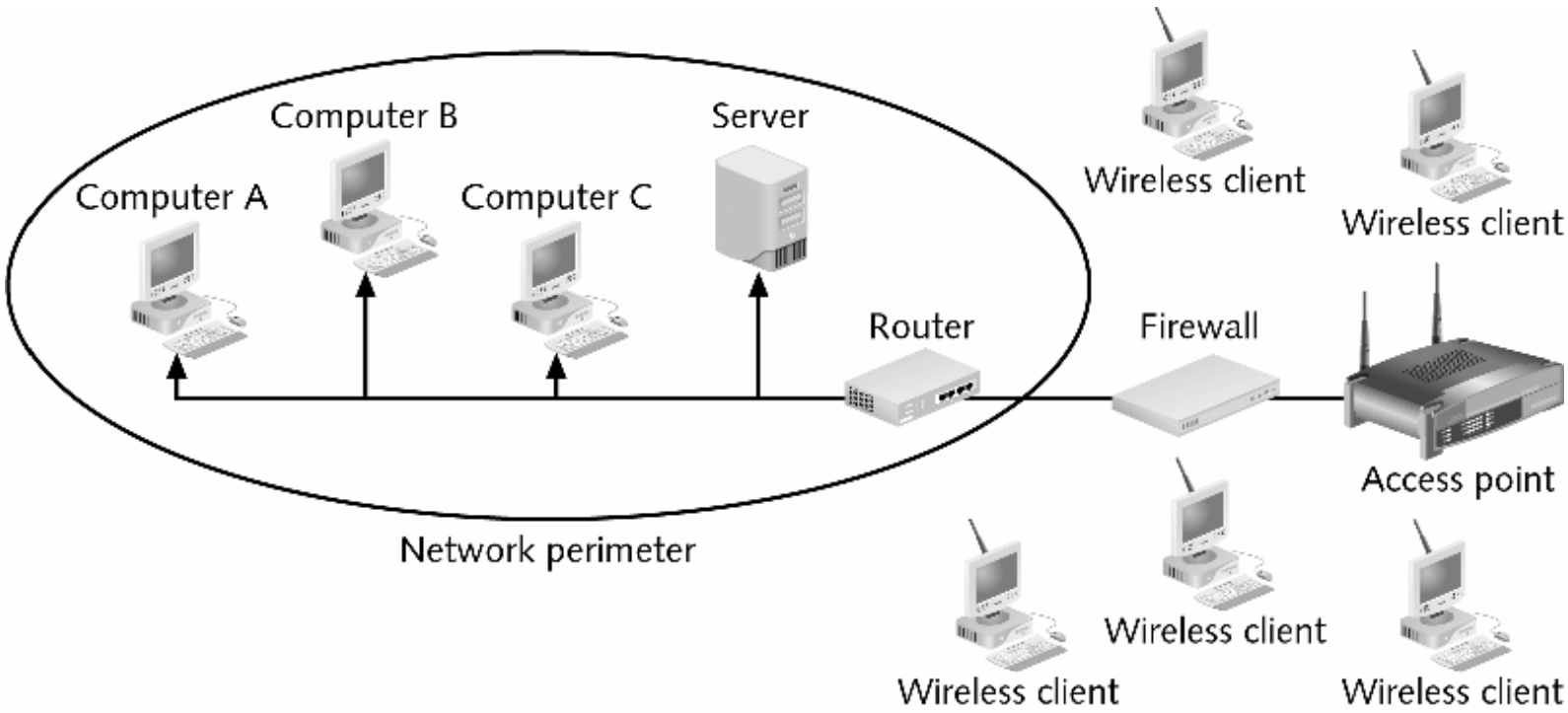
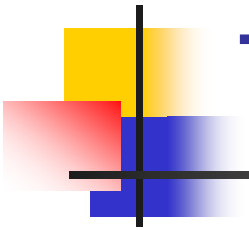


Figure 10 Untrusted WLAN



Trusted Network

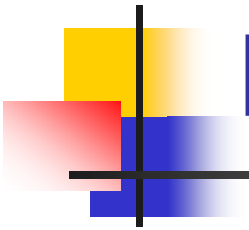
- It is still possible to provide security for a WLAN and treat it as a trusted network
- Wi-Fi Protected Access (WPA) was crafted by the WECA in 2002 as an interim solution until a permanent wireless security standard could be implemented
- Has two components:
  - WPA encryption
  - WPA access control

Trusted Network (continued)

- WPA encryption addresses the weaknesses of WEP by using the Temporal Key Integrity Protocol (TKIP)
- TKIP mixes keys on a per-packet basis to improve security
- Although WPA provides enhanced security, the IEEE 80211i solution is even more secure
- 80211i is expected to be released sometime in 2004

Network Security Devices

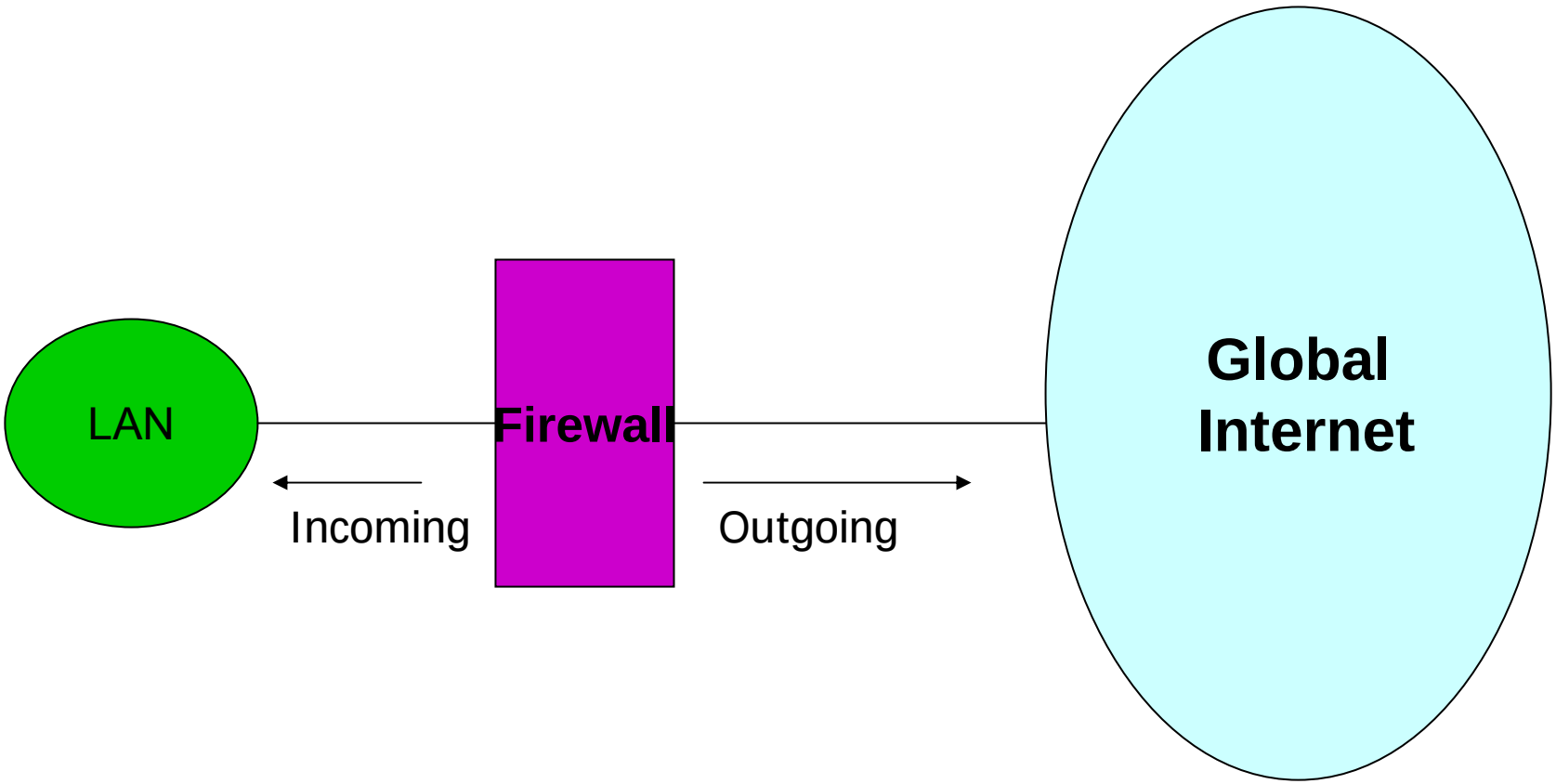
- Network devices designed and used strictly to protect the network
- Include:
  - Firewalls
  - Intrusion-detection systems IDSs
  - Network monitoring and diagnostic devices

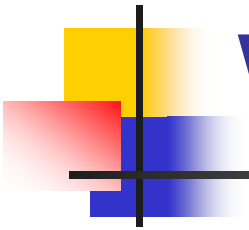


Firewalls

- Typically used to filter packets
- Designed to prevent malicious packets from entering the network or its computers (sometimes called a packet filter)
- Typically located outside the network security perimeter as first line of defense
- The network administrator has the heavy responsibility of configuring the firewalls.

Typical Use of a Firewall



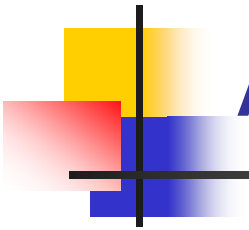


What is a Firewall?

- To control access to a system, we need firewalls.
- A firewall is a device (usually a router or computer running special software)

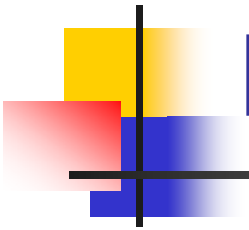
  installed between the internal network of an organization and the rest of the Internet.
- It is designed to forward some packets and filter (not forward) others.
- That somehow regulates traffic between LAN/WAN and the Internet
- For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP.

What can a Firewall Protect Against?



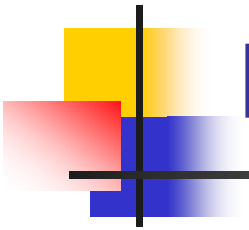
- Generally , firewalls are configured to protect against unauthenticated interactive logins from the “outside” world.
- More elaborate firewalls block traffic from the outside world to the inside, but permit users on the inside to communicate freely with the outside.
- Firewalls provide an important logging and auditing function.
- Often they provide summaries to the administrator about what kinds and amount of traffic passed through it, and how many attempts were made to break in.

Firewalls and Perimeter Defense

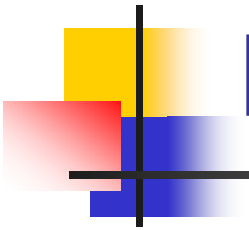


- Firewalls implement a form of security called *perimeter defense*
- Protect the inside of something by defending the outside strongly
  - The firewall machine is often called the *Bastion Horse*
- Control the entry and exit points

Weakness of Perimeter Defense Models

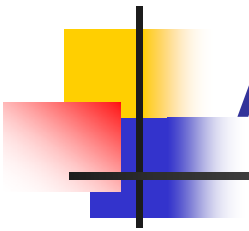


- Breaching the perimeter compromises all security
- Windows passwords are a form of perimeter defense
  - If you get past the password, you can do anything
- Perimeter defense is part of the solution, not the entire solution



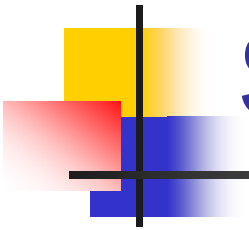
Defense in Depth

- Don’t rely on a single defensive mechanism or defense at a single point
- Combine different defenses
- Defeating one defense doesn’t defeat your entire plan



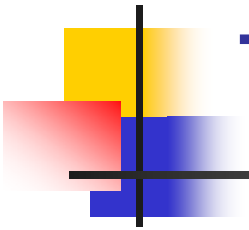
Are Firewalls Useful?

- Definitely !
- They are not the full solution, but they are absolutely part of it
- Anyone who cares about security needs to run a decent firewall
- They just have to do other stuff, too.



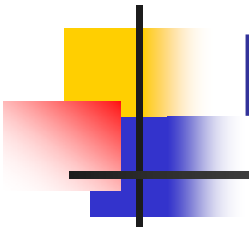
Software Firewalls

- Software firewall runs as a program on a local computer (sometimes known as a personal firewall)
  - Enterprise firewalls are software firewalls designed to run on a dedicated device and protect a network instead of only one computer
  - One disadvantage is that it is only as strong as the operating system of the computer



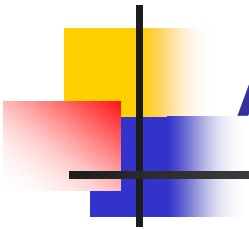
Types of Firewalls

- Filtering gateways
  - AKA screening routers
- Circuit gateways
  - Also a kind of screening router
- Application Level gateways
  - AKA proxy gateways
- Hybrid (complex) gateways



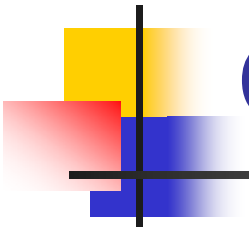
Filtering Firewalls

- Based on packet routing information
- Look at information in the incoming packet's header
- Filter packets in one of two ways:
  - Stateless packet filtering: permits or denies each packet based strictly on the rule base
  - Stateful packet filtering: records state of a connection between an internal computer and an external server; makes decisions based on connection and rule base
- Can perform content filtering to block access to undesirable Web sites



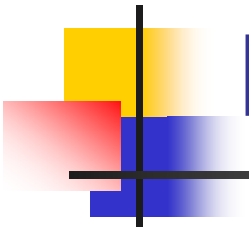
A Fundamental Problem

- Today's packet headers aren't authenticated
  - And are pretty easy to forge
- If the filtering firewall trusts packet headers, it offers little protection
- Situation may be improved by IPsec



One exception To This Problem

- Checking internal addresses
- Safety procedures inside the security perimeter may limit some services to LAN members
- The firewall can check that incoming packets don’t claim to be internal the LAN

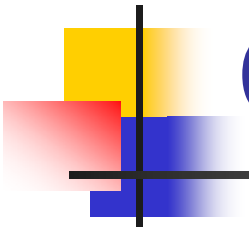


Filtering Based on Ports

- Most incoming traffic is destined for a particular machine and port
  - Which can be derived from the IP and TCP headers
- Only let through packets to select machines at specific ports
- This type of filtering is included in many routers
- E.g. a packet filter man allow web traffic on port 80 and block Telnet traffic on port 23.
- Makes it impossible to externally exploit flaws in little-used ports
  - If you configure the firewall right..

Pros and Cons of Filtering Firewalls

- + Fast
- + Cheap
- + Flexible
- + Transparent
- - Limited Capabilities
- -Dependent on header authentication
- -Generally poor logging
- - May rely on router security

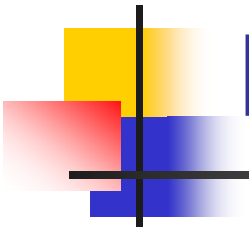


Circuit Gateways

- Another kind of filtering firewall
- Used when internal machines request service from machines outside the firewall
- Makes it look like the request came from the firewall
  - Concealing internal system details

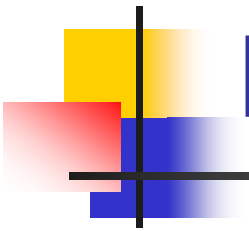
Stateful Inspection Firewalls

- Also referred to as *stateful packet filtering*
- Records are kept using a state table that tracks every communication channel
- Stateful inspections occur at all levels of the network and provide additional security, especially in connectionless protocols such as UDP and ICMP
- DoS attacks present a challenge because flooding techniques are used to overload the state table and effectively cause the firewall to shut down or reboot



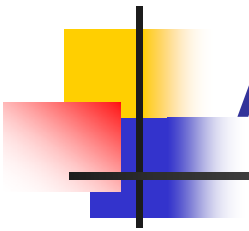
Firewalls and Encryption

- Firewalls provide no confidentiality for data they pass back and forth
- Unless the data is encrypted
- But if the data is encrypted, the firewall can't examine it
- So typically the firewall must be able to decrypt
  - Or only work on unencrypted parts of packets



Firewalls and Viruses

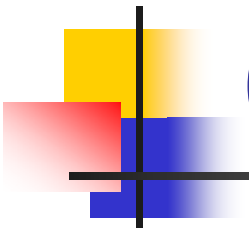
- Firewalls are an excellent place to check for viruses
- Virus detection software can be run on incoming executables
- Requires that firewall knows when executables come in
- And must be reasonably fast
- Again, might be issues with encryption



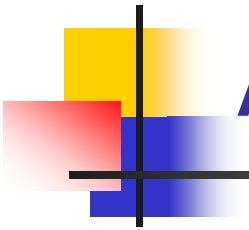
Application Level Firewalls

- Also known as Proxy gateways and stateful firewalls
- Firewalls that understand the application-level details of network traffic
  - To some degree
- The proxy firewall processes requests from an outside network, and examines the data and makes rule-based decisions about whether the request should be forwarded or refused
- The proxy intercepts all the packets and reprocesses them for use internally(this includes hiding IP addresses (NAT))

Application Level Firewalls (cont.)

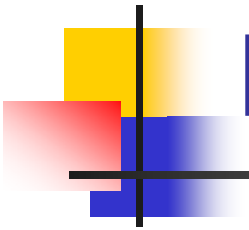


- The firewall serves as a general framework
- Various proxies are plugged into the framework
- Incoming packets are examined
  - And handled by the appropriate proxy
- Programs capable of deep understanding particular kinds of traffic : e.g. HTTP, FTP, etc
- Proxies are specialized



An Example Proxy

- A proxy to audit e-mail
- What might such a proxy do?
  - Allow only e-mail from particular users through
  - Or refuse e-mail from known SPAM sites
  - Or filter e-mail with unsafe inclusions (like executables)

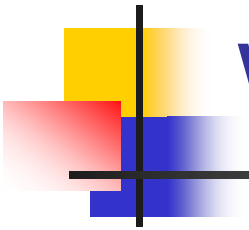


Proxy Firewalls

- An application layer firewall can defend against worms better than other kinds of firewalls
  - Reassembles and analyzes packet streams instead of examining individual packets
- Provides better security than packet filtering because of the increased intelligence that a proxy firewall offers
- Requests from internal network users are routed through the proxy
- The proxy, in turn, repackages the request and sends it along, thereby isolating the user from the external network
- The proxy can also offer caching, should the same request be made again, and can increase the efficiency of data delivery

Proxy Firewalls (DUAL - HOMED)

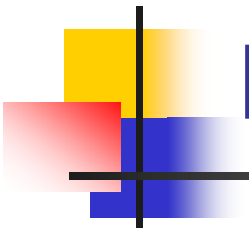
- A proxy firewall with two NICS
- One NIC is connected to the outside network
- The other is connected to the internal network
- The proxy software manages the connection between the two NIC cards
- The setup segregates the two networks from each other and offers increased security
- The proxy function can occur at either the application level or the circuit level
- The circuit level proxy creates a circuit between the client and the server and doesn't deal with the contents of the packets that are being processed



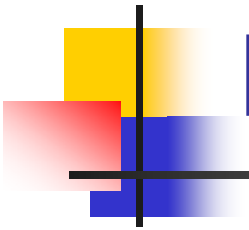
What are the Limits of Proxies?

- Proxies can only test for threats they understand
- Either they must permit a very limited set of operations
- Or they must have deep understanding of the program they protect
  - If too deep, they may share the flaw

Pros and Cons of Application Level Gateways



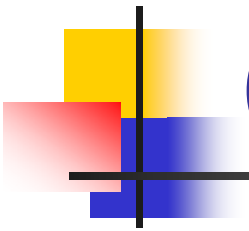
- +Highly flexible
- +Good logging
- +Content-based filtering
- +Potentially transparent
- - Slower
- - More complex and expensive
- - A good proxy is hard to find



Hybrid Gateways

- A combination of two or more other types
  - Typically filtering gateways and proxy gateways
- Are they better?
  - If in parallel, no
  - If in series, maybe

Intrusion-Detection Systems (IDSs)



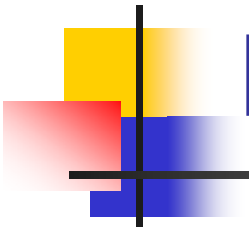
- Devices that establish and maintain network security
- Active IDS (or reactive IDS) performs a specific function when it senses an attack, such as dropping packets or tracing the attack back to a source
  - Installed on the server or, in some instances, on all computers on the network
- Passive IDS sends information about what happened, but does not take action

Intrusion-Detection Systems (IDSs) (continued)

- Host-based IDS monitors critical operating system files and computer's processor activity and memory; scans event logs for signs of suspicious activity
- Network-based IDS monitors all network traffic instead of only the activity on a computer
  - Typically located just behind the firewall
- Other IDS systems are based on behavior:
  - Watch network activity and report abnormal behavior
  - Result in many false alarms

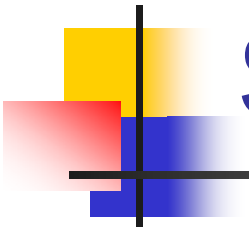
Network Monitoring and Diagnostic Devices

- SNMP enables network administrators to:
  - Monitor network performance
  - Find and solve network problems
  - Plan for network growth
- Managed device:
  - Network device that contains an SNMP agent
  - Collects and stores management information and makes it available to SNMP



Designing Network Topologies

- Topology: physical layout of the network devices, how they are interconnected, and how they communicate
- Essential to establishing its security
- Although network topologies can be modified for security reasons, the network still must reflect the needs of the organization and users



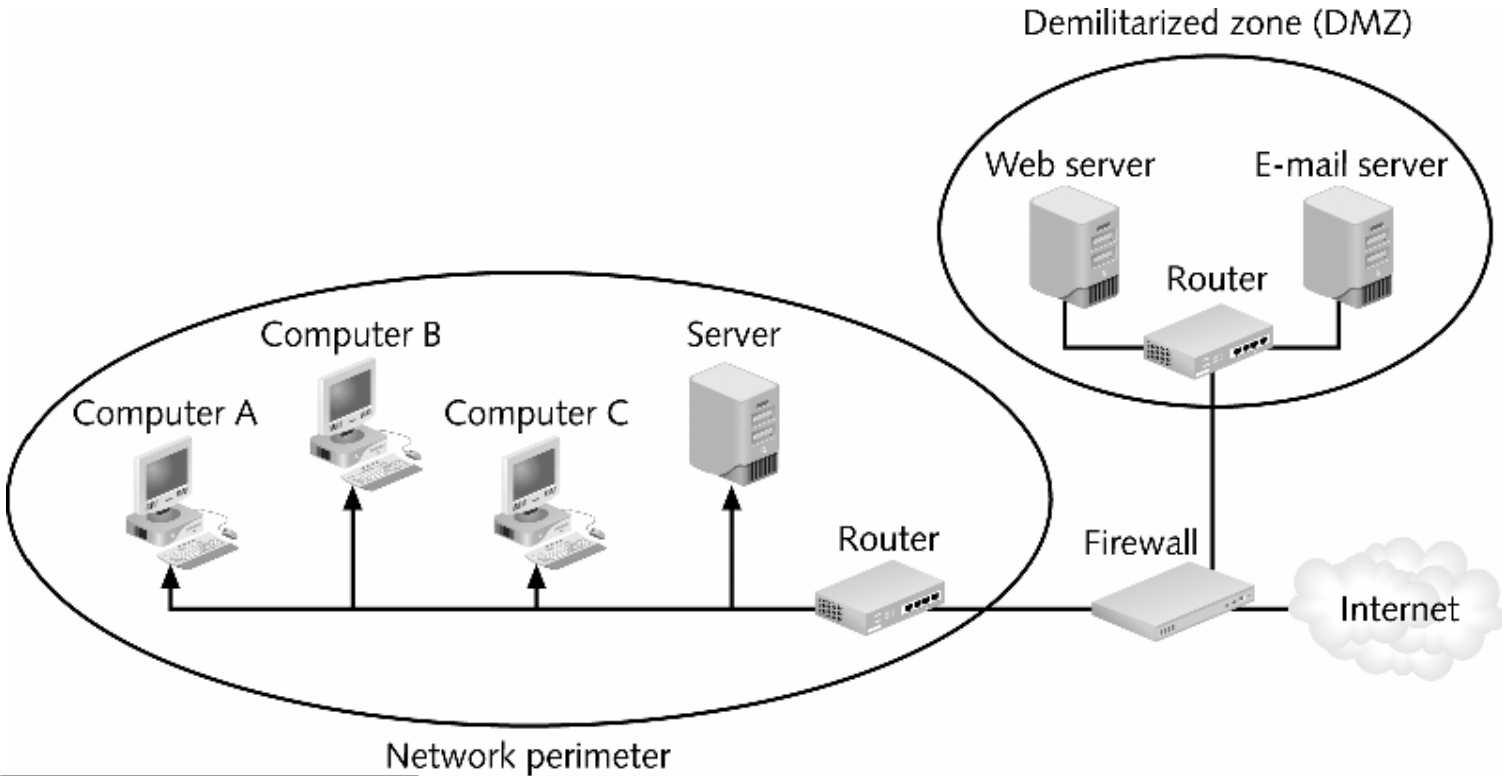
Security Zones

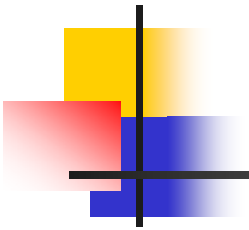
- One of the keys to mapping the topology of a network is to separate secure users from outsiders through:
  - Demilitarized Zones (DMZs)
  - Intranets
  - Extranets

Demilitarized Zones (DMZs)

- Separate networks that sit outside the secure network perimeter
- Outside users can access the DMZ, but cannot enter the secure network
- For extra security, some networks use a DMZ with two firewalls
- The types of servers that should be located in the DMZ include:
  - Web servers
  - Remote access servers
  - E-mail servers
  - FTP servers

Demilitarized Zones (DMZs) (cont.)





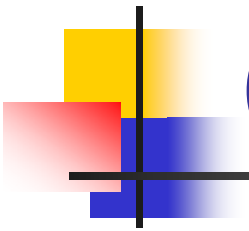
Intranets

- Networks that use the same protocols as the public Internet, but are only accessible to trusted inside users
- Disadvantage is that it does not allow remote trusted users access to information

Extranets

- Sometimes called a cross between the Internet and an intranet
- Accessible to users that are not trusted internal users, but trusted external users
- Not accessible to the general public, but allows vendors and business partners to access a company Web site

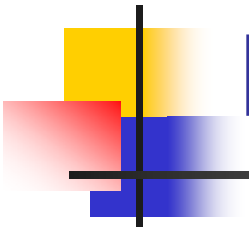
Network Address Translation (NAT)



- “You cannot attack what you do not see” is the philosophy behind Network Address Translation (NAT) systems
- Hides the IP addresses of network devices from attackers
- Computers are assigned special IP addresses (known as private addresses)

Network Address Translation (NAT) (cont.)

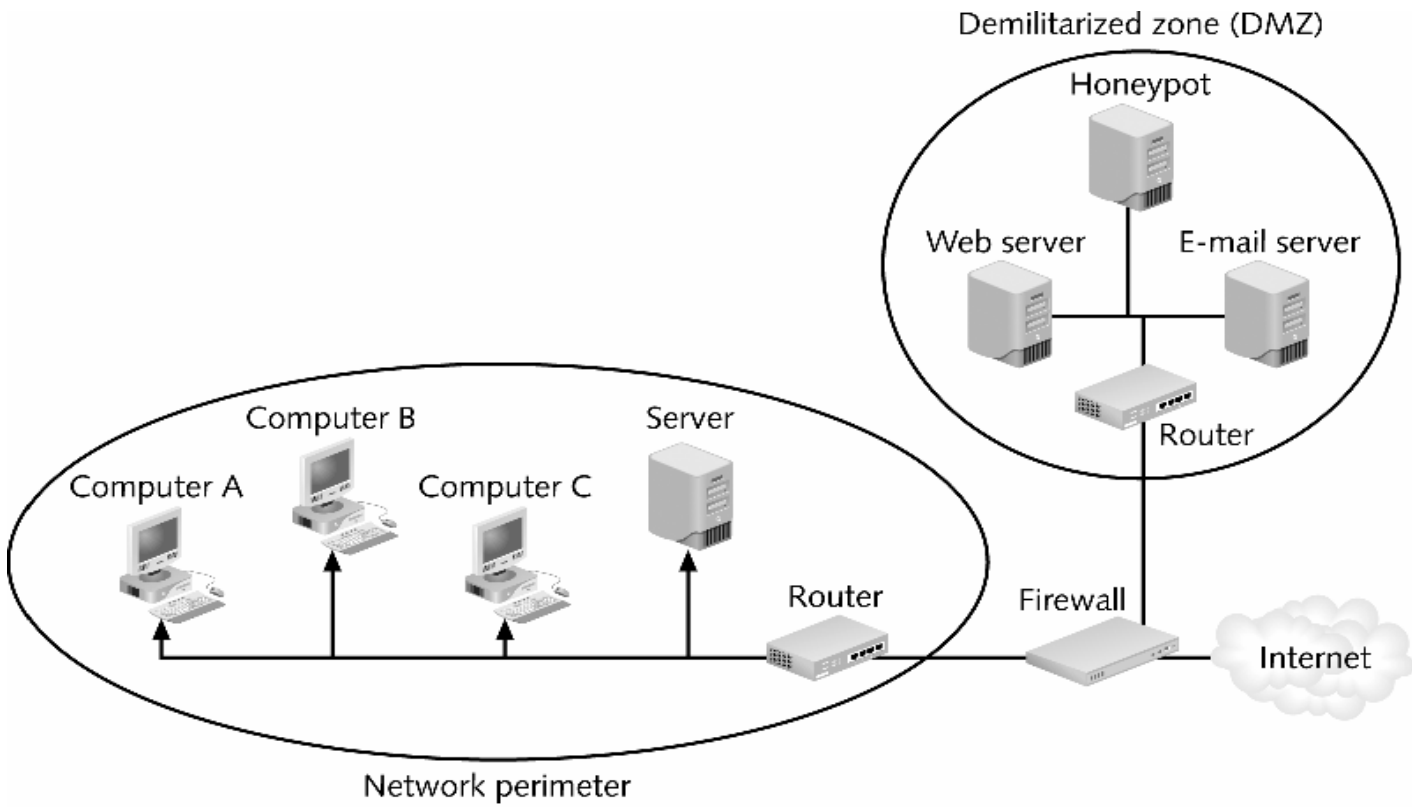
- These IP addresses are not assigned to any specific user or organization; anyone can use them on their own private internal network
- Port address translation (PAT) is a variation of NAT
- Each packet is given the same IP address, but a different TCP port number



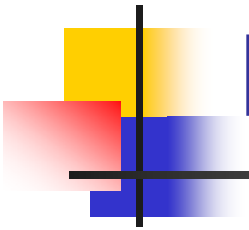
Honeypots

- Computers located in a DMZ loaded with software and data files that appear to be authentic
- Usually a machine dedicated to this purpose
- Intended to trap or trick attackers
- Provides early warning of attacks
- Two-fold purpose:
  - To direct attacker's attention away from real servers on the network
  - To examine techniques used by attackers

Honeypots (cont.)



Honeypots



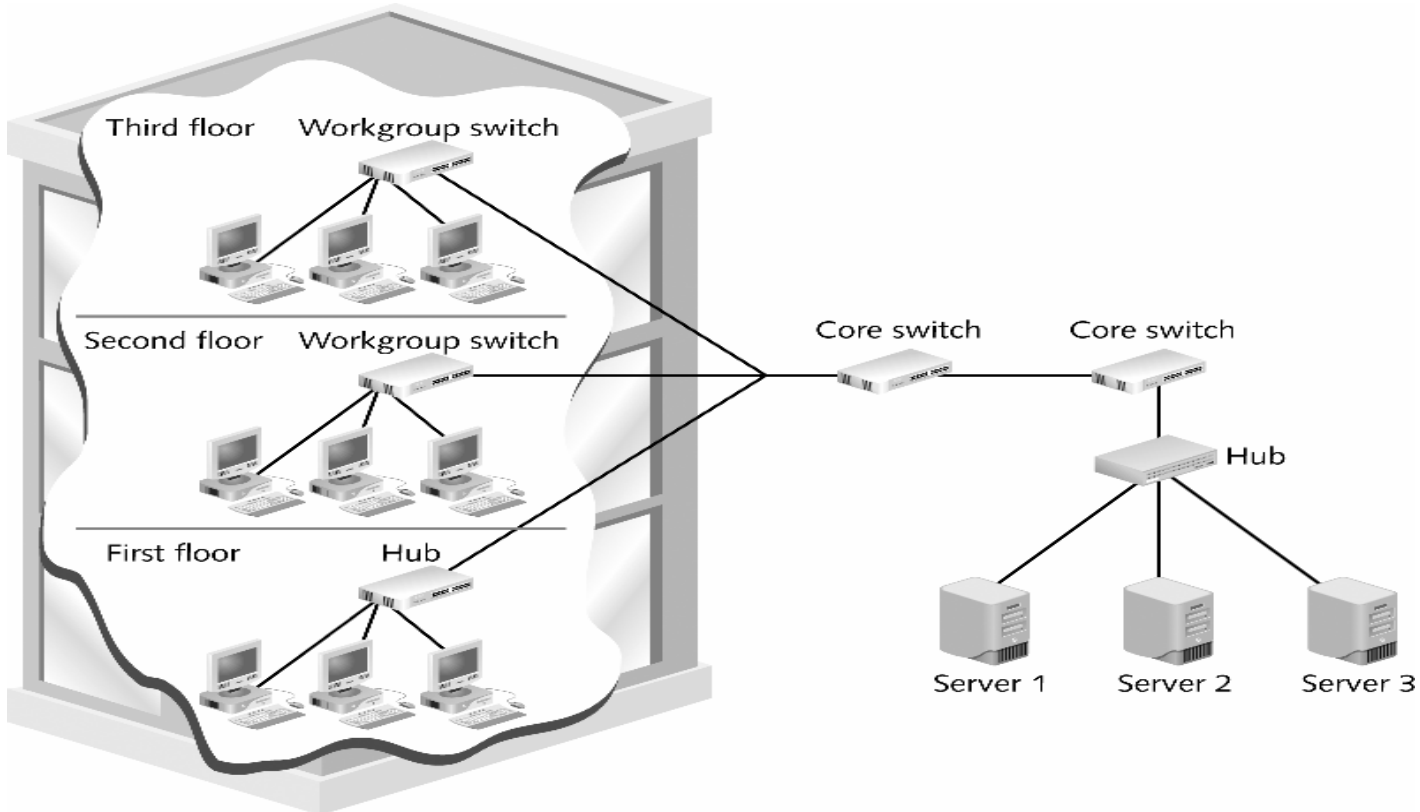
Honeynets

- A collection of honeypots on a single network
- Typically, no other machines are on the network
- Since whole network is phony, all incoming traffic is probably attack traffic
- Good for tracking the spread of worms
- Has given evidence on prevalence of DDos attacks

Virtual LANs (VLANs)

- Segment a network with switches to divide the network into a hierarchy
- Core switches reside at the top of the hierarchy and carry traffic between switches
- Workgroup switches are connected directly to the devices on the network
- Core switches must work faster than workgroup switches because core switches must handle the traffic of several workgroup switches

Virtual LANs (VLANs) (cont.)



VLAN

Virtual LANs (VLANs) (cont.)

- Segment a network by grouping similar users together
- Instead of segmenting by user, you can segment a network by separating devices into logical groups (known as creating a VLAN)