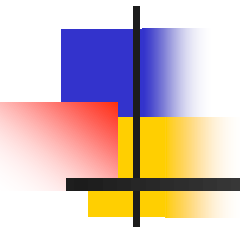
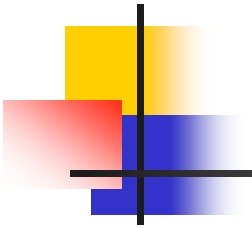


# *Firewalls and VPN*

***Professor Stephen S. Yau***



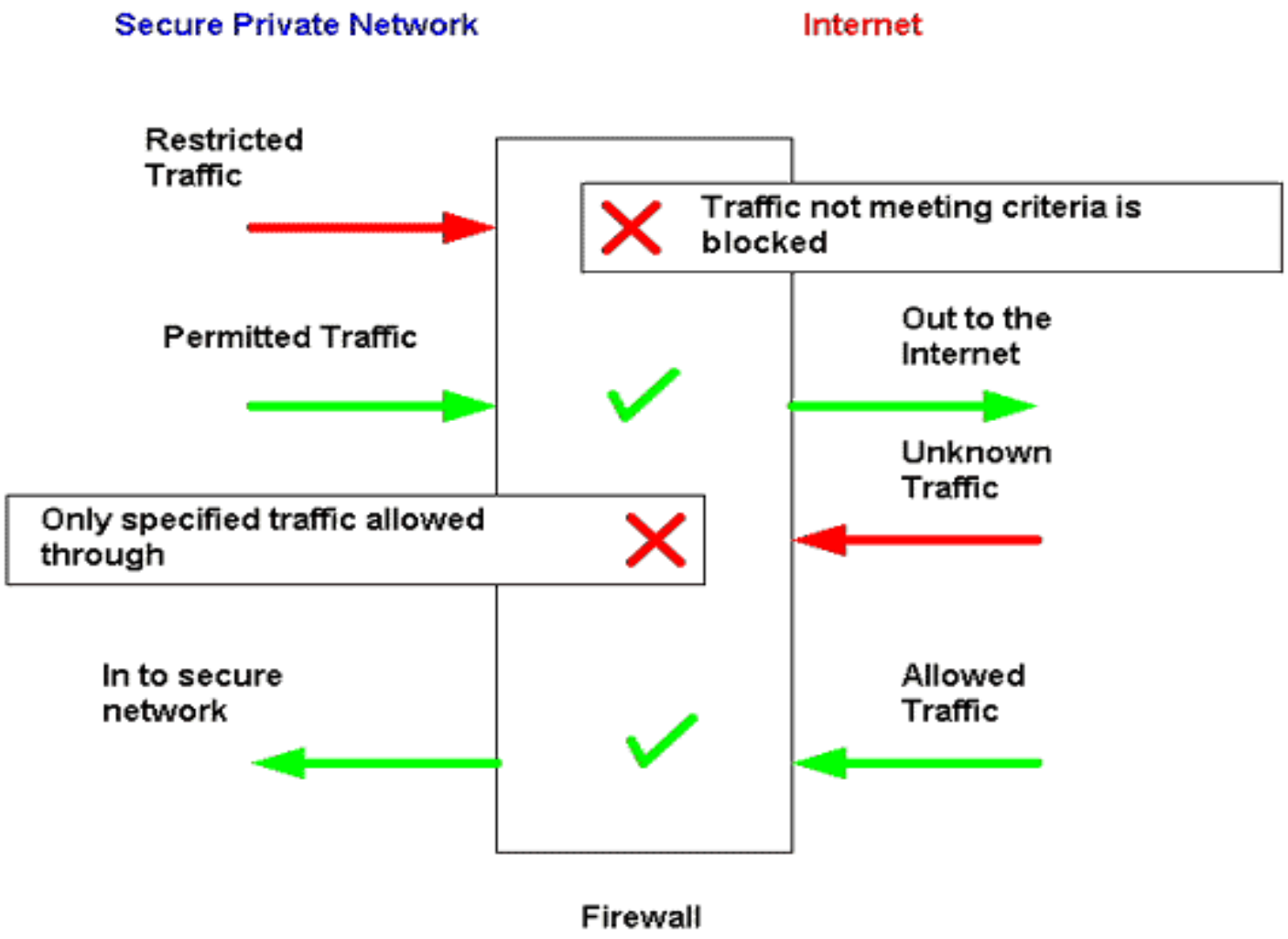
# *DMZ*

- The ***DMZ*** *(Demilitarized Zone)* is a portion of a network that separates a purely internal network from an external network.
- DMZ is where public servers and proxies should be located
  - ***Proxy*** is an intermediate agent or server that acts on behalf of an endpoint without allowing a direct connection between the two endpoints

# *Firewalls*

- A ***firewall*** is a host that mediates access to a network, allowing or disallowing certain types of access on the basis of a configured security policy.
- Protect a network from external networks
- Block unwanted traffic and pass desirable traffic to and from both sides of the network
  - Examples:
    - Allows: http, mails
    - Keeps out: suspected users, denial of services attacks, spam, viruses

# Operations of Firewall



# *Firewalls in Different Layers*

- **Network layer: *Packet-Filtering Firewalls***
  - Concerned with ***routing*** of packets to their destinations.
- **Transport layer: *Circuit-Level Firewalls***
  - Concerned with ***session*** of packets
- **Application layer: *Application-Level Firewalls***
  - Concerned with ***contents*** of packets

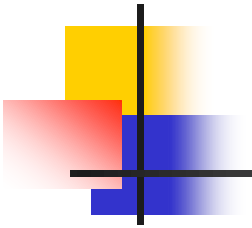
# *Packet Filtering Firewalls*

- A ***packet filtering firewall*** performs access control on basis of attributes of packet headers, such as destination addresses, source address, and options.
- Whenever a network receives a packet, three possible actions: ***forward*** to destination, ***block***, or ***return*** to sender
- One of these actions is chosen according to a set of rules usually in a form of "access control lists".

| Rule | Source Address | Destination Address | Action |
|---|---|---|---|
| 1 | 149.59.0.0/16 | 123.45.6.0/24 | permit |
| 2 | 149.59.34.0/24 | 123.45.0.0/16 | deny |
| 3 | 0.0.0.0/0 | 0.0.0.0/0 | deny (default) |

# *Packet Filtering Firewalls (cont.)*

- Factors determining the actions:
  - Source address
  - Destination address
  - Direction of traffic
- Rules applied top to bottom
  - Ordered from least restrictive to most restrictive
- Packets are not scrutinized



# *Circuit-Level Firewalls*

- Validates sessions before opening connections (handshakes)
- Once a connection is made, all packets related to that connection pass
- Packets not scrutinized
- No direct connections with other networks without validation

# *Circuit-Level Firewalls (cont.)*

- Establishes two connections:
  - Between client and firewall
  - Between firewall and server
- Implemented using sockets ( which is IP address + Port number)
- Manipulating established connection is easy
- Packets are not scrutinized

# *Application-Level Firewalls*

- ***Application-level firewall*** (also called ***Proxy firewall***) uses proxies to perform access control.
- Acts as a proxy server, evaluates requests and decides "accept" or "deny" according to security concerns
- All packets are scrutinized

# *Choosing a Firewall*

- What OS required and other OSs supported?
- How much CPU/RAM/disk space it needs?
- What is the authentication scheme?
- Does it support logging?
- What hardware is provided?
- What software is provided?
- What is the cost for installing and operating the firewall?
- What are other features?

# *Firewall Configuration Criteria*

- Analyze their ***security needs***. Potential risks and threats must be contemplated.
- Considerations affecting configuration of firewalls:
  - Organizational ***policies***
    - What ***level of access control*** does management want?
    - The desired ***level of monitoring and access*** must be determined.
    - What ***level of risk*** is organization willing to accept?
  - What ***types of messages*** should be monitored, permitted and denied?

# *Firewall Configuration Criteria (cont.)*

- Considerations affecting configuration of firewalls *(cont.):*
  - ***Cost***, including maintenance, must be considered against the potential threat. What would be the potential ***cost/damage*** of attacks to the system from outside?
  - The ***number, placement, and types*** of firewalls to be used must be determined.
  - What is the estimated ***overhead*** in using the selected firewalls?

# *Some Commercially Available Firewalls*

- Hardware
  - Linksys Etherfast Cable/DSL Firewall Router, Microsoft MN-100, D-Link Express EtherNetwork
- Mac OS X servers
  - DoorStop Server Firewall, Firewall X2, Impasse, IPNetSentry, Net Barrier
- Linux
  - IP tables, SINUS, ipchains
- Windows
  - BlackICE, Kerio, McAfee, Norton Personal Firewall, Outpost, Sygate, Terminet, and ZoneAlarm

# *VPN*

# *Virtual Private Networks (VPNs)*

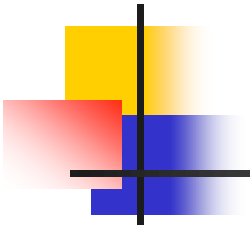
- ***Private and secure network connection*** between systems; uses data communication capability of ***unsecured public networks***
- Extends organization's internal network connections securely to remote locations beyond trusted networks

# *Virtual Private Networks (VPNs) (cont.)*

- Three types of VPN technologies
  - ***Trusted VPN*** (or simply ***VPN***): uses ***leased circuits (trusted) from a service provider*** and conducts ***packet switching*** over these (trusted) leased circuits
  - ***Secure VPN***: uses ***security protocols and encrypt traffic*** transmitted across unsecured public networks, like the Internet
  - ***Hybrid VPN***: combines trusted and secure

# *Virtual Private Networks (VPNs) (cont.)*

- VPN must accomplish
  - ***Encapsulation*** of incoming and outgoing data
  - ***Encryption*** of incoming and outgoing data
  - ***Authentication*** of remote computers and (perhaps) remote users as well
- Two modes of operations: transport and tunneling



# *Transport Mode*

- Data within IP packets is encrypted, but header information is not
- Allows user to establish secure links directly with remote hosts, encrypting only data contents of packets
- Two popular uses:
  - End-to-end transport of encrypted data
  - Example: A remote access worker or a teleworker connects to office network over Internet by connecting to a VPN server on the perimeter of internal networks

# *Tunnel Mode*

- Organization establishes two perimeter tunnel servers
- These servers act as encryption points, encrypting all traffic that will traverse unsecured network between these two servers.
- Primary benefit of this mode: an intercepted packet reveals nothing about true destination
- Example: Microsoft's Internet Security and Acceleration (ISA) Server

# *References*


- Michael E. Whitman, and Herbert J. Mattord , *Principles of Information Security*, *4th edition*, Course Technology, 2011
- Mark Stamp, *Information Security: Principles and Practice*, Wiley, May 2011, 606 pages, ISBN-10 0470626399
- Matt Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2002, ISBN: 0201440997
- M. Merkow, and J. Breithaupt, *Information Security: Principles and Practices*, Prentice Hall, August 2005, 448 pages, ISBN 0131547291
- J. G. Boyce, and D. W. Jennings, *Information Assurance*: *Managing Organizational IT Security Risks*. Butterworth Heineman, 2002, ISBN 0-7506-7327-3