

# IT 4823

## Information Security Administration

### Firewalls and Intrusion Defense



Notice: This session is  
being recorded.

Some lecture slides prepared by Dr Lawrie Brown for “*Computer Security: Principles and Practice*”, 1/e, by William Stallings and Lawrie Brown,

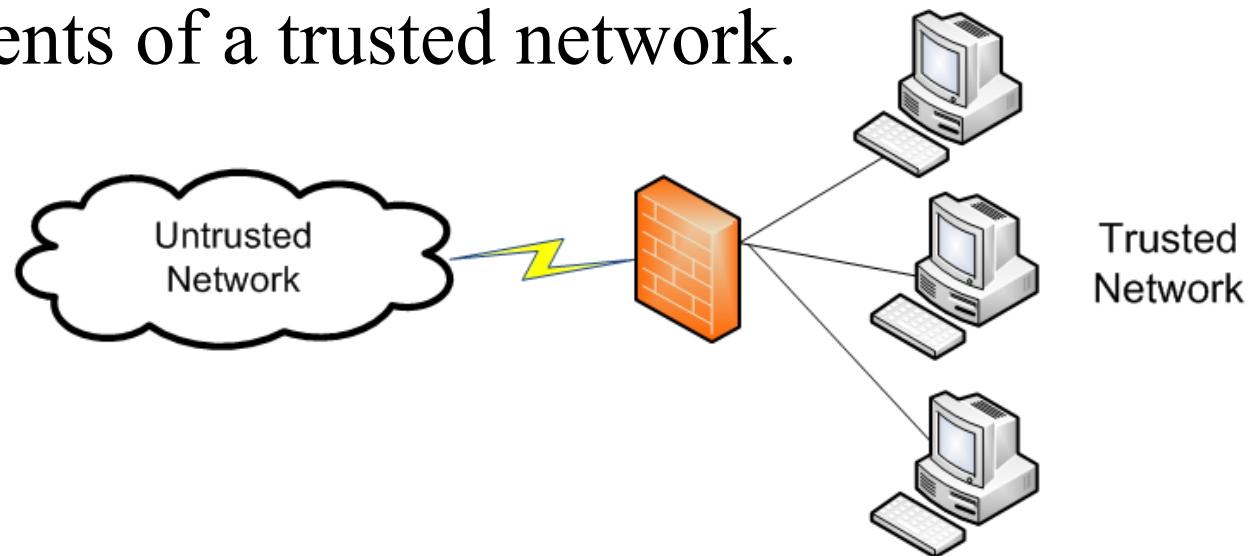


Copyright © 2016 by Bob Brown



# Firewall

- Router, general-purpose computer, or appliance...
- That controls the flow of packets between a trusted and an untrusted network, or between segments of a trusted network.



# Firewall Capabilities and Limits

- Capabilities:
  - defines a choke point
  - provides a location for monitoring security events
  - convenient platform for some Internet functions such as NAT, usage monitoring, IPSEC VPNs
- Limitations:
  - cannot protect against attacks bypassing firewall
  - may not protect against internal threats
  - improperly secure wireless LAN
  - laptop, phones, portable storage device infected outside then used inside

# Firewalls and Intrusion Prevention Systems

- Internet connectivity is essential
  - for organizations and individuals
  - but creates opportunities for threats
- Firewalls are an effective means of protecting LANs
- Can also secure workstation and server subnets
- Use firewall as perimeter defense: a choke point to impose security

# Firewalls

- Hosts that mediate access to a network
  - Allows, disallows accesses based on configuration and type of access
- Example: block Back Orifice
  - BO allows external users to control systems
    - Requires commands to be sent to a particular port
  - Firewall can block traffic to or from that port
    - So even if BO installed, outsiders can't use it
    - **Principle of least privilege (default deny):** block *all* ports that are not specifically needed. (How do I know that BO isn't using a "needed" port?)

# Types of Firewalls/Filters

- Packet filtering: Rules operate on information in the packet headers.
- Stateful inspection:
  - Filters on packet headers, but also
  - Keeps information about outgoing connections; incoming packets are allowed on high ports only if there is a corresponding outgoing connection.
  - Can inspect “data;” really protocol parameters for higher-level protocols, *e.g.* HTTP,FTP, SIP...
- Proxy firewalls.

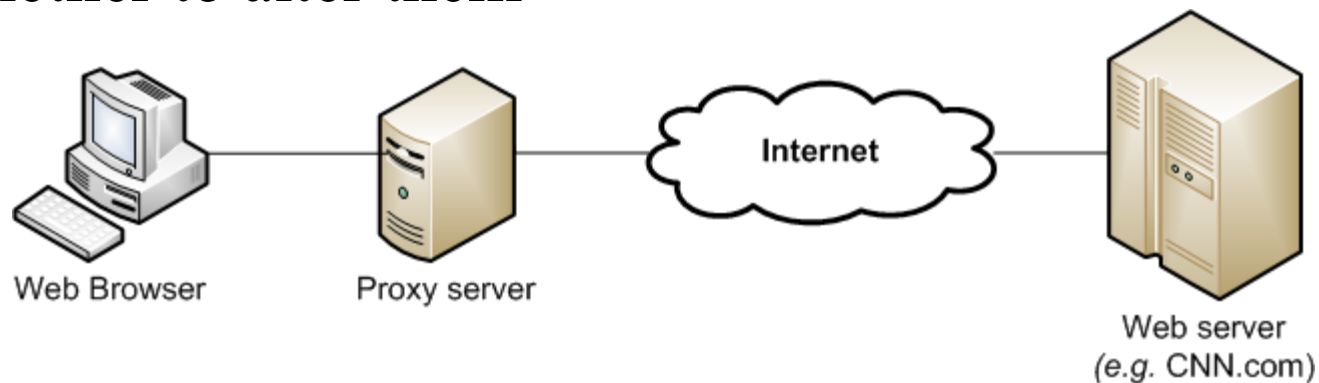
# Filtering Firewalls

- Access control based on attributes of packets and packet headers
  - Such as destination address, port numbers, options, etc.
  - Also called a *packet filtering firewall*
  - Does not control access based on content
  - Examples: routers, other infrastructure systems

# Proxy

An intermediate agent or server acting on behalf of endpoint without allowing a direct connection between the two endpoints

- So, each endpoint talks to proxy, thinking it is talking to other endpoint
- Proxy decides whether to forward messages, and whether to alter them





# Proxy Firewall

Access control done with proxies

- Usually bases access control on content as well as source, destination addresses, etc.
- Also called an *applications level* or *application level firewall*
- Example: virus checking in electronic mail
  - Incoming mail goes to proxy firewall
  - Proxy firewall receives mail, scans it
  - If no virus, mail forwarded to destination
  - If virus, mail rejected or disinfected before forwarding

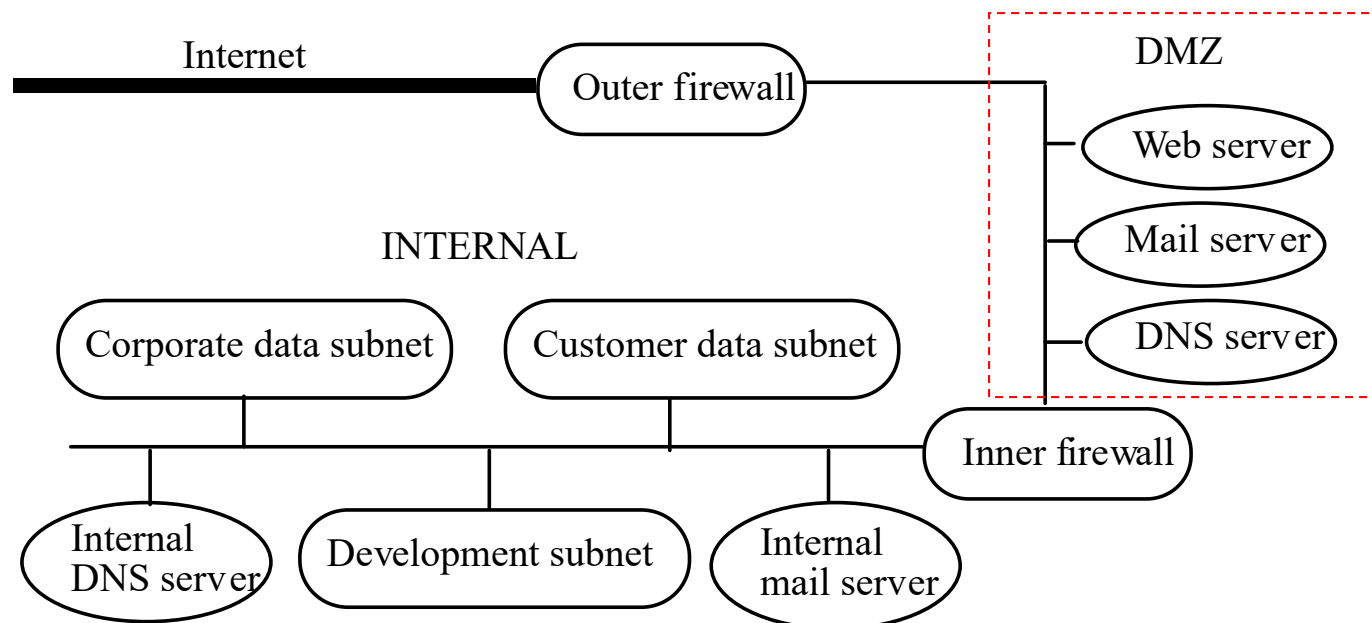
# Views of a Firewall

- Access control mechanism
  - Determines which traffic goes into, out of network
- Audit mechanism
  - Analyzes packets that enter and leave protected net
  - Takes action based upon the analysis
  - Leads to traffic shaping, intrusion response, etc.

# Case Study: Hypothetical Organization

Partition network into several subnets

Place firewalls between them prevent leakage



# DMZ

- DMZ: “demilitarized zone”
- Portion of network separating purely internal network from external network
  - Allows control of accesses to some trusted systems inside the corporate perimeter
  - If DMZ systems breached, internal systems are still safe
  - Can perform different types of checks at boundary of internal, DMZ networks and DMZ, Internet network

# Application of Principles

- Least privilege
  - Containment of internal addresses
  - Limit access
- Complete mediation
  - Inner firewall mediates every access to DMZ
- Separation of privilege
  - Going to Internet must pass through inner, outer firewalls and DMZ servers

# Application of Principles

- Least common mechanism
  - Inner, outer firewalls distinct; DMZ servers separate from inner servers
  - DMZ DNS *violates* this principle
    - If it fails, multiple systems affected
    - Inner, outer firewall addresses fixed, so they do not depend on DMZ DNS

# Outer Firewall Configuration

- Goals: restrict public access to trusted network; restrict trusted net access to Internet
- Required: public needs to send, receive email; access web services
  - So outer firewall allows SMTP, HTTP, HTTPS
  - Outer firewall uses its address for those of mail, web servers

# Details

- Proxy firewall
- SMTP: mail assembled on firewall
  - Scanned for malicious logic; rejected or “cleaned” if found
  - Otherwise forwarded to DMZ mail server
- HTTP, HTTPS: messages checked
  - Checked for suspicious components; dropped if found
  - Otherwise, forwarded to DMZ web server
- Note: web, mail servers are *different physical systems*; neither is the same as firewall



# Attack Analysis

Three points of entry for attackers:

- Web server ports: proxy checks for invalid, illegal HTTP, HTTPS requests, rejects them
- Mail server port: proxy checks email for invalid, illegal SMTP requests, rejects them
- An attacker might bypass low-level firewall checks by exploiting vulnerabilities in software, hardware
  - Firewall designed to be as simple as possible
  - Defense in depth

# Defense in Depth

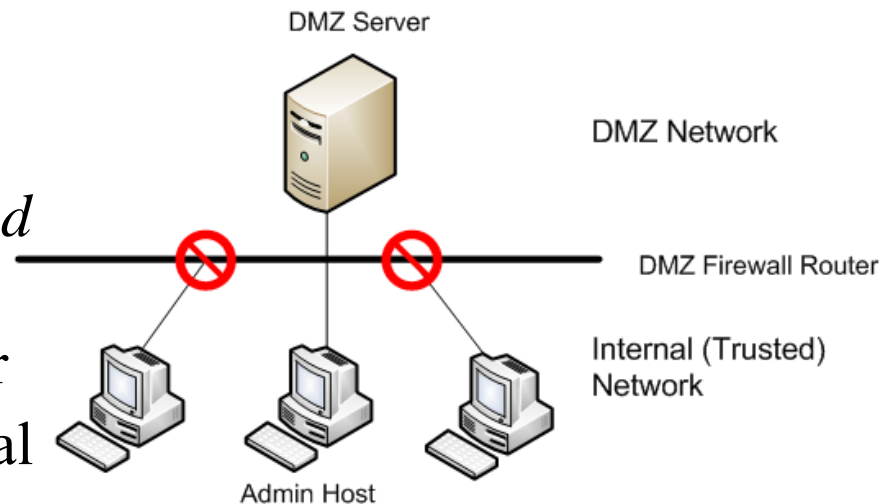
- A form of separation of privilege
- To attack system in DMZ by bypassing firewall checks, attacker must know internal addresses
  - Then can try to piggyback unauthorized messages onto authorized packets
- But the rewriting of DMZ addresses prevents this

# Inner Firewall Configuration

- Goals: restrict access to internal network
- Rule: block *all* traffic except for that *specifically* authorized to enter. Default deny principle.
- Example: Hypothetical organization uses NFS on some internal systems
  - Outer firewall disallows NFS packets crossing
  - Inner firewall disallows NFS packets crossing, too
  - DMZ does not need access to this information (least privilege)
  - If inner firewall fails, outer one will stop leaks, and vice versa (separation of privilege)

# More Configuration

- Internal folks require email; SMTP proxy required
- Administrators for DMZ need login access
  - So, allow SSH through *if and only if*:
  - Destination is a DMZ server
  - Originates at specific internal host (administrative host)



# DMZ

Look at servers separately:

- Web server: handles web requests with Internet
  - May have to send information to internal network
- Email server: handles email with Internet
  - Must forward email to internal mail server
- DNS
  - Used to provide addresses for systems DMZ servers talk to
- Log server
  - DMZ systems log info here

# DMZ Mail Server

- Performs address, content checking on *all* email
- Goal is to hide internal information from outside, but be transparent to inside
- Receives email from Internet, forwards it to internal network
- Receives email from internal network, forwards it to Internet

# Mail from Internet

- Reassemble messages into header, letter, attachments as files
- Scan header, letter, attachments looking for “bad” content
  - “Bad” = known malicious logic
  - If none, scan original letter (including attachments and header) for violation of SMTP spec
- Scan recipient address lines
  - Address rewritten to direct mail to internal mail server
  - Forward letter there

# Mail to Internet

- Like mail from Internet with 2 changes:
  - Step 2: also scan for sensitive data (like proprietary markings or content, etc.)
  - Step 3: changed to rewrite all header lines containing host names, email addresses, and IP addresses of internal network
    - All are replaced by “example.com” or IP address of external firewall



# Administrative Support

- Runs SSH server
  - Configured to accept connections *only* from trusted administrative host in internal network
  - All public keys for that host fixed; no negotiation to obtain those keys allowed
  - Allows administrators to configure, maintain DMZ mail host remotely while minimizing exposure of host to compromise

# DMZ Web Server

- Accepts, services requests from Internet
- Never contacts servers, information sources in internal network
- CGI scripts checked for potential attacks
  - Hardened to prevent attacks from succeeding
  - Server itself contains no confidential data
- Server is `www.example.com` and uses IP address of outer firewall when it must supply one

# Updating DMZ Web Server

- Clone of web server kept on internal network
  - Called “WWW-clone”
- All updates done to WWW-clone
  - Periodically admin copies contents of WWW-clone to DMZ web server
- DMZ web server runs SSH server
  - Used to do updates as well as maintenance, configuration
  - Secured like that of DMZ mail server

# Internet Ordering

## Orders for merchandise from Internet

- Customer enters data, which is saved to file
- After user confirms order, web server checks format, content of file and then uses public key of system on internal customer subnet to encipher it. This file is placed in a spool area not accessible to web server program
- Original file deleted
- Periodically, internal trusted administrative host uploads these files, and forwards them to internal customer subnet system

# Analysis

- If attacker breaks into web server, cannot get order information
  - There is a slight window where the information of customers still on system can be obtained
- Attacker can get enciphered files, public key used to encipher them
  - Use of public key cryptography means it is computationally infeasible for attacker to determine private key from public key

# DMZ Log Server

- DMZ systems all log information
  - Useful in case of problems, attempted compromise
- Problem: attacker will delete or alter them if successful
  - So log them off-line to this server
- Log server saves logs to file, also to write-once media
  - Latter just in case log server compromised
- Runs SSH server
  - Constrained in same way server on DMZ mail server is

# Summary

- Each server knows only what is needed to do its task
  - Compromise will restrict flow of information but not reveal info on internal network
- Operating systems and software:
  - All unnecessary features, servers disabled
  - Better: create custom systems
- Proxies prevent direct connection to systems
  - For all services except SSH from internal network to DMZ, which is itself constrained by source, destination

# Internal Mail Server

- Can communicate with hosts on subnets
- Subnet may allow mail to go directly to destination host
- Internal DNS needs to know addresses of all destination hosts



# WWW-clone

- Provides staging area for web updates
- All internal firewalls allow access to this
  - WWW-clone controls who can put and get what files and where they can be put
- Synchronized with web pages on server
  - Done via internal trusted administrative host
- Used as testbed for changes in pages
  - Allows corporate review before anything goes public
  - If DMZ web server trashed or compromised, all web pages can be restored quickly

# Trusted Administrative Host

- Access tightly controlled
  - Only system administrators authorized to administer DMZ systems have access
- All connections to DMZ through inner firewall must use these hosts
  - Exceptions: internal mail server, possibly DNS
- All connections use SSH
  - DMZ SSH servers accept connections from this host only

# Analysis

- DMZ servers never communicate with internal servers
  - All communications done via inner firewall
- Only client to DMZ that can come from internal network is SSH client from trusted administrative host. Authenticity established by public key authentication
- Only data non-administrative staff can alter are web pages. Even then, they do not access DMZ

# Analysis

- Only data from DMZ is customer orders and email
  - Customer orders already checked for potential errors, enciphered, and transferred in such a way that it cannot be executed
  - Email thoroughly checked before it is sent to internal mail server

# Assumptions

- Software, hardware does what it is supposed to
  - If software compromised, or hardware does not work right, defensive mechanisms fail
  - For this reason separation of privilege is *critical*
    - If a component fails, other components provide additional defenses
- Assurance is vital!

# Availability

- Access over Internet must be unimpeded
  - Context: flooding attacks, in which attackers try to overwhelm system resources
- Example: SYN flood
  - Problem: server cannot distinguish legitimate handshake from one that is part of this attack
  - Flood can overwhelm communication medium. Can't do anything about this (except buy a bigger pipe or filter upstream)
  - Flood can overwhelm resources on our system

# Intermediate Hosts

Use routers to eliminate non-legitimate traffic

- Goal: only legitimate traffic reaches firewall
- Example: Cisco routers try to establish connection with source (TCP intercept mode)
  - On success, router does same with intended destination, merges the two
  - On failure, short time-out protects router resources and target never sees flood

# Attacks Against Outer Firewall

- Unsuccessful attacks
  - Logged, then ignored
  - Security folks use these to justify budget, train new personnel
- Successful attack against SMTP proxy
  - Proxy will start non-standard programs
  - Anomaly detection component of IDS on log server will report unusual behavior
    - Security officers monitor this around the clock



# In the DMZ

- Very interested in attacks, successful or not
- Means someone who has obtained access to DMZ launched attack
  - Some trusted administrator shouldn't be trusted
  - Some service on outer firewall is compromised
  - Software on DMZ system not restrictive enough
- IDS system on DMZ log server looks for misuse (known attacks) to detect this

# Ignoring Failed Attacks

- Sounds dangerous
  - Successful attacker probably tried and failed earlier
- “So what?”
  - Not sufficient personnel to handle all alerts
  - Focus is on what we care most about: Successful attacks, or failed attacks where there should be none

# Key Points

- Begin with policy
- Craft network architecture and security measures from it
- Assume failure will occur
  - Try to minimize it
  - Defend in depth
  - Have plan to handle failures

# Questions

