Web Security

CS 161/194-1
Anthony D. Joseph
November 21, 2005

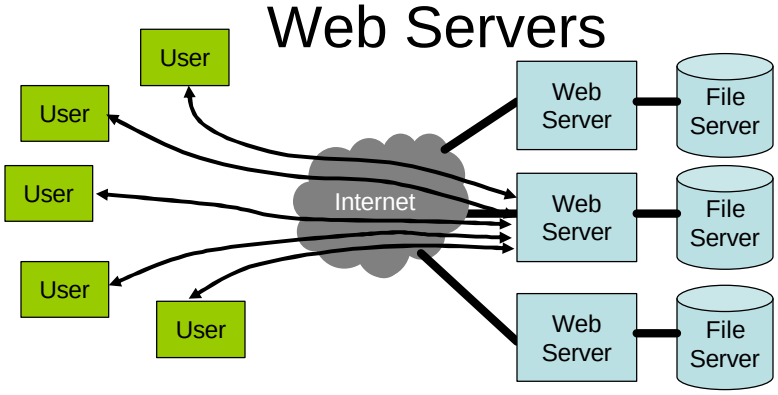
Outline

- Web Servers
  - Static and Dynamic Content
- Firewall review
  - Adding a DMZ
- Secure Topologies

Polls

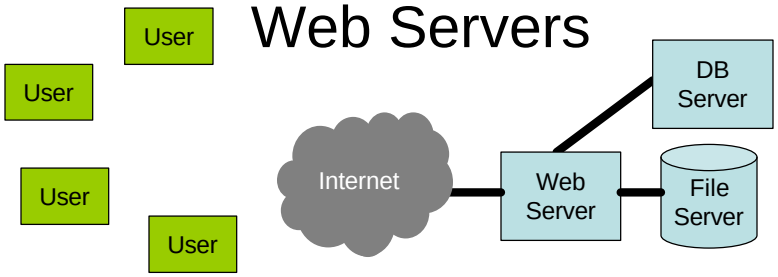
- How many people have set up a personal web server?
- How many people have set up a business web server?

Web Servers



- Web server serves up static, read-only content from file server
- Scales up by replicating web servers
  - Can use DNS round-robin or load balancer

Web Servers



- Add a database server for dynamic content
  - DB used to store per-user info or site content
  - Also, used for authentication, read/write actions, e-commerce, …
- Software connector to DB server
  - Object/Java DataBase Connectivity

Web Servers

- Static content model:
  - Web server uses file server for static content, templates, …
- Dynamic content model:
  - Web server uses database server to retrieve/store dynamic content
- Can have mixtures
  - Ex: Storing dynamic content in FS
  - Ex: Storing static content in DB
- What are the security issues?

Some Web Server Threats and Attacks

- Replace static content ("defacement")
  - Exploit vulnerability to access Web or File servers
- (Distributed) Denial of Service attack
  - Request large image or emulate complex transaction
- Unauthorized database access
  - Exploit vulnerability (e.g., SQL injection) to read/write database
- Attack server OS or other services
  - Exploit vulnerability to disable server

Replace Static Content ("Defacement")

- Cracker exploits a vulnerability to gain access to Web or File Servers
- Examples:
  - Flaws in CGI programs
  - Flaws in URL processing
  - Buffer overflows
- Replaces web pages with their own
- May also access protected content

(Distributed) Denial of Service Attack

- Cracker performs resource exhaustion attack
  - Overwhelm network, CPU, disk bandwidth, …
- Examples
  - Request large image or file
  - POST large image or file (requires many zombies)
  - Emulate complex transaction
- Typically use large number of zombies (1,000's to 100,000's)

Unauthorized Database Access

- Cracker exploits vulnerability in Web server to DB server connection to read/write database
- Example:
  - Use URL or POST attack to inject SQL code
  - Gain access to Web server, then connect to DB
- Attacks can compromise DB integrity

Attack Server OS or Other Services

- Cracker exploits vulnerability to gain access to server
  - Many OS and service vulnerabilities…
- Can be a stepping stone to attacking web service or accessing database

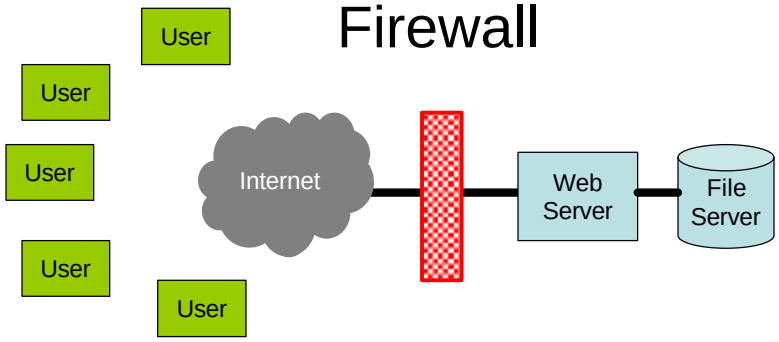
Stopping *Some* Attacks

- Replace static content ("defacement")
  - Harden server (latest patch levels, minimum services)
  - Limit data on file server
- (Distributed) Denial of Service attack
  - Add load balancer, DNS round-robin, replicated clusters, …
- Unauthorized database access
  - Harden server (latest patch levels, minimum services)
  - Sanity check all arguments
- Attack server OS or other services
  - Harden servers (latest patch levels, minimum services)

Problems

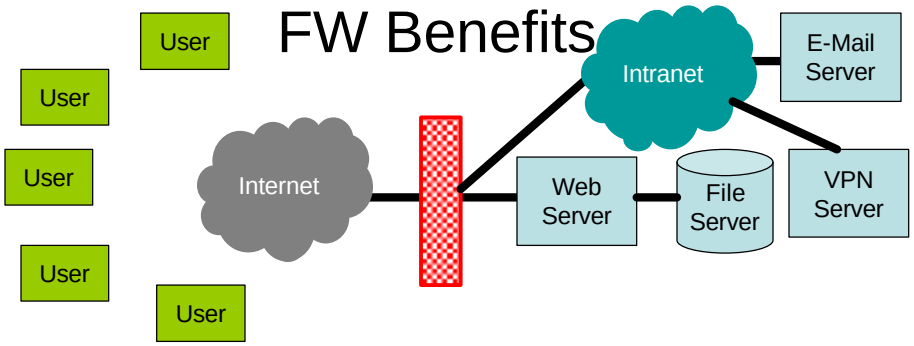
- Hard to keep servers up-to-date with patches
  - Zero-day exploits
  - Delays in releasing, retrieving, testing, installing patches
- DDoS attacks still impose load on servers
- Add layered defense
  - Place firewall between Internet and Web server

Firewall



- Default firewall rule: `deny all`
- Other firewall rules:
  - `allow *,*,TCP -> <web server IP>,80`
  - `allow *,*,TCP -> <web server IP>,443`
  - Add stateful inspection rules for known attacks: Code Red, Nimda, …

FW Benefits

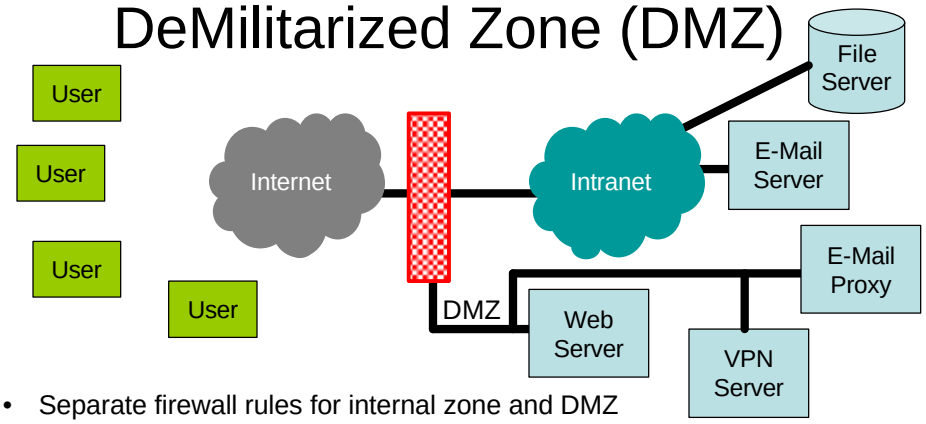


- Helps harden servers by blocking all but web traffic
- Can help with DDoS attacks by adding stateful rules (examining content) or blocking zombie IP subnets
  - Doesn't work for all content attacks
- Problems?
  - How to access Intranet (Internal LAN) and e-mail server?

Firewall Issues

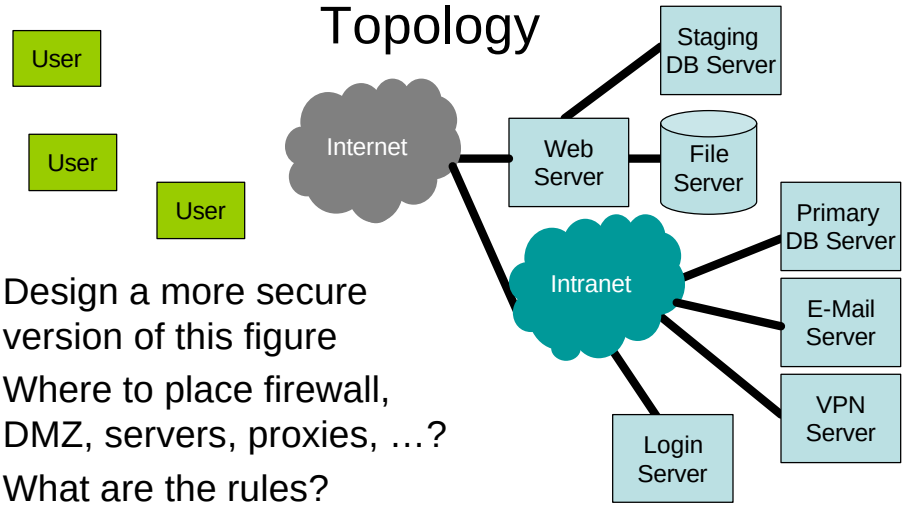
- We can add more rules
  - For access to Intranet, E-mail server, and other "public" servers
- But, what happens if one server or Intranet machine is compromised?
- This is the classic firewall problem:
  - All our machines are now vulnerable!
- Real issue:
  - We need to both protect public servers and Intranet
- Solution: Place public servers in a DMZ

DeMilitarized Zone (DMZ)



- Separate firewall rules for internal zone and DMZ
  - Internet-DMZ rules only allow web, e-mail traffic
  - DMZ-Intranet rules only allow access to file, e-mail, remote login *from DMZ*
  - No Internet-Intranet access
- Should e-mail server be in intranet or DMZ?
  - Add proxy to isolate e-mail access/storage from e-mail forwarding

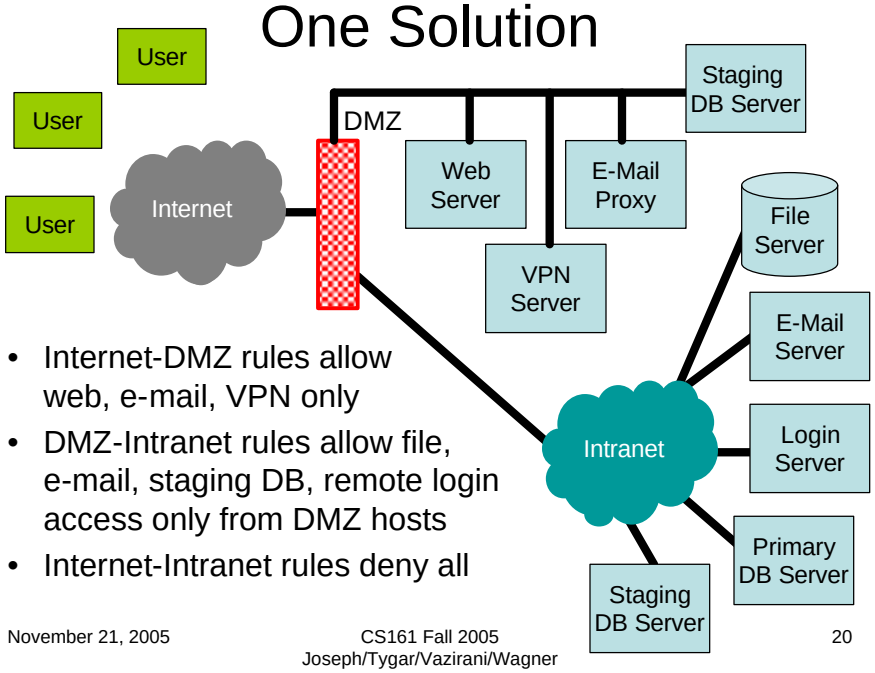
Designing a More "Secure" Topology



- Design a more secure version of this figure
- Where to place firewall, DMZ, servers, proxies, …?
- What are the rules?

Design

One Solution



- Internet-DMZ rules allow web, e-mail, VPN only
- DMZ-Intranet rules allow file, e-mail, staging DB, remote login access only from DMZ hosts
- Internet-Intranet rules deny all

Summary

- Public servers are vulnerable to attack
  - OS and services
- Eliminate unnecessary services
- Apply all patches
- Use a DMZ to provide layered defense
  - Place server/proxy in DMZ
  - Place database/file/“real” servers in Intranet
  - Deny all default for Internet-Intranet traffic