Network Security

Introduction

Three Laws of Secure Computing

1. Don't buy a computer.

2. If you do buy a computer, don't plug it in.

3. If you do plug it in, sell it and return to step 1

The 12 Step Program

1. Identify network assets
2. Analyze security risks
3. Analyze security requirements and tradeoffs
4. Develop a security plan
5. Define a security policy
6. Develop procedures for applying security policies

The 12 Step Program (continued

7. Develop a technical implementation strategy
8. Achieve buy-in from users, managers, and technical staff
9. Train users, managers, and technical staff
10. Implement the technical strategy and security procedures
11. Test the security and update it if any problems are found
12. Maintain security

Network Assets

- Hardware
- Software
- Applications
- Data
- Intellectual property
- Trade secrets
- Company's reputation

Security Risks

- Hacked network devices
  - Data can be intercepted, analyzed, altered, or deleted
  - User passwords can be compromised
  - Device configurations can be changed
- Reconnaissance attacks
- Denial-of-service attacks

Security Tradeoffs

- Tradeoffs must be made between security goals and other goals:
  - Affordability
  - Usability
  - Performance
  - Availability
  - Manageability

A Security Plan

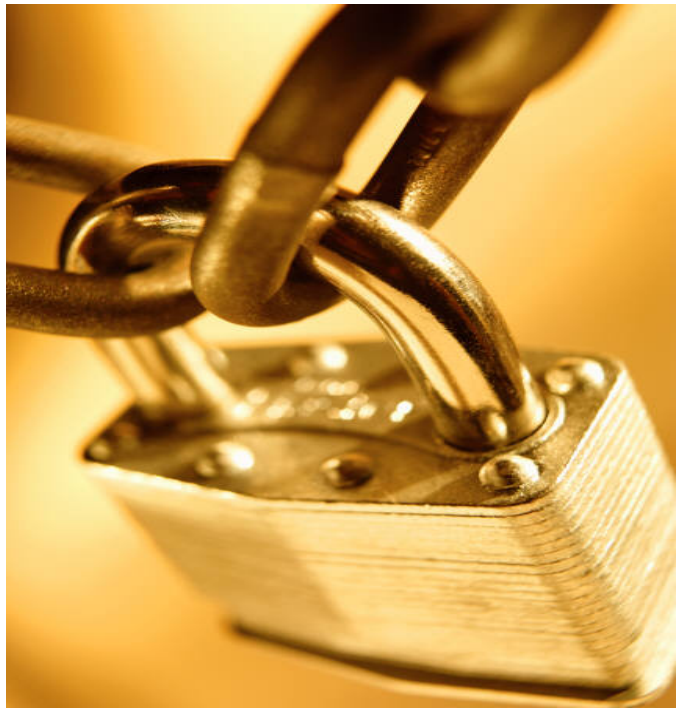
- High-level document that proposes what an organization is going to do to meet security requirements
- Specifies time, people, and other resources that will be required to develop a security policy and achieve implementation of the policy

Security

- Per RFC 2196, "The Site Security Handbook," a security policy is a
  - "Formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."
- The policy should address
  - Access, accountability, authentication, privacy, and computer technology purchasing guidelines

Security Mechanisms

- Physical security
- Authentication
- Authorization
- Accounting (Auditing)
- Data encryption
- Packet filters
- Firewalls
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)



THE CIA

Modularizing Security Design

- Security defense in depth
  - Network security should be multilayered with many different techniques used to protect the network
- Belt-and-suspenders approach
  - Don’t get caught with your pants down

Modularizing Security Design

- Secure all components of a modular design:
  - Internet connections
  - Public servers and e-commerce servers
  - Remote access networks and VPNs
  - Network services and network management
  - Server farms
  - User services
  - Wireless networks

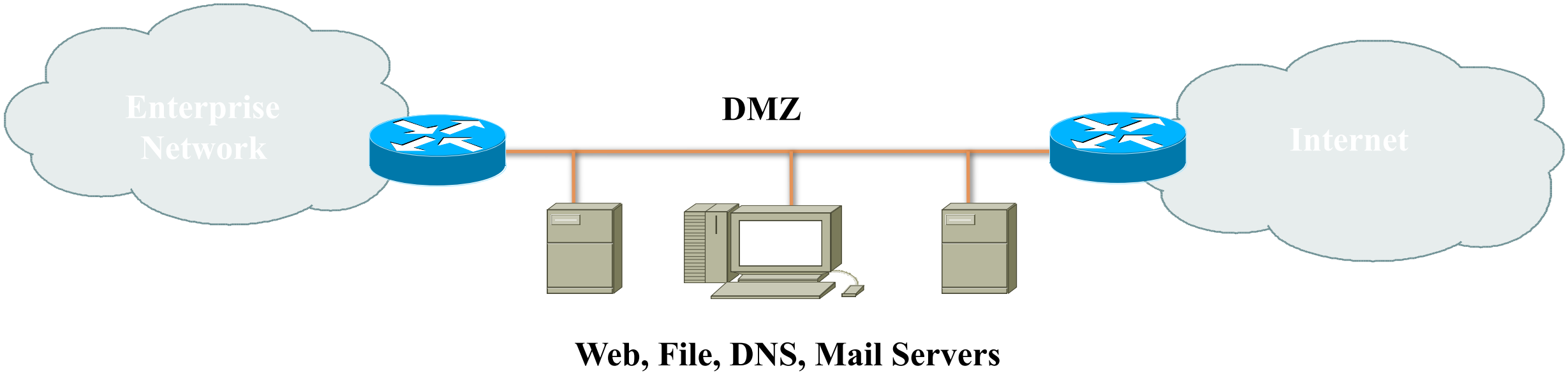
Securing Internet Connections

- Physical security
- Firewalls and packet filters
- Audit logs, authentication, authorization
- Well-defined exit and entry points
- Routing protocols that support authentication

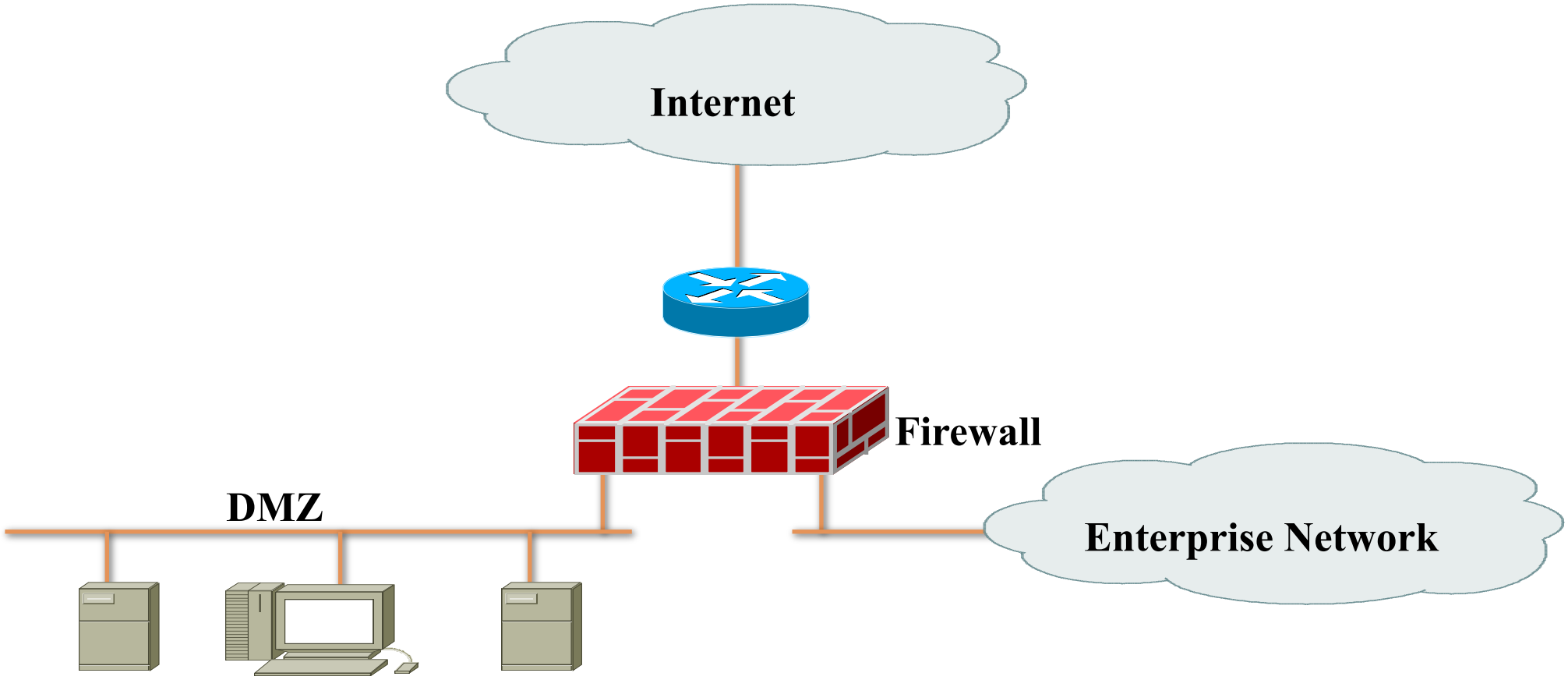
Securing Public Servers

- Place servers in a DMZ that is protected via firewalls
- Run a firewall on the server itself
- Enable DoS protection
  - Limit the number of connections per timeframe
- Use reliable operating systems with the latest security patches
- Maintain modularity
  - Front-end Web server doesn't also run other services

Security Topologies



Security Topologies



Securing Remote-Access & VPN's

- Physical security
- Firewalls
- Authentication, authorization, and auditing
- Encryption
- One-time passwords
- Security protocols
  - CHAP
  - RADIUS
  - IPSec

Securing Network Services

- Treat each network device (routers, switches, and so on) as a high-value host and harden it against possible intrusions
- Require login IDs and passwords for accessing devices
  - Require extra authorization for risky configuration commands
- Use SSH rather than Telnet
- Change the welcome banner to be less welcoming

Securing Server Farms

- Deploy network and host IDSs to monitor server subnets and individual servers
- Configure filters that limit connectivity from the server in case the server is compromised
- Fix known security bugs in server operating systems
- Require authentication and authorization for server access and management
- Limit root password to a few people
- Avoid guest accounts

Securing User Services

- Specify which applications are allowed to run on networked PCs in the security policy
- Require personal firewalls and antivirus software on networked PCs
  - Implement written procedures that specify how the software is installed and kept current
- Encourage users to log out when leaving their desks
- Consider using 802.1X port-based security on switches

Vulnerability Scanners - Nessus

- Pros
  - Large plugin or signature base
  - You can customize and create new plugins
- Cons
  - Taken over by Tenable no longer free
  - Purchasing plans for new plugins
  - Shareware plug-ins are seven days behind

Vulnerability Scanners - GFI LANguard

- Pros
  - Port Scanner, Enumeration, and Vulnerability Scanner
  - Many features such as SNMP and SQL brute force
  - Great for Windows networks
- Cons
  - Lacks extensive signatures for other operating systems
  - Look to Nessus for scanning heterogeneous networks