UMP OPEN COURSEWARE

Universiti Malaysia PAHANG
Engineering • Technology • Creativity

CHAPTER 9

DEVELOPING NETWORK SECURITY STRATEGIES

Expected Outcomes

Able to design the network security for the entire network
Able to develop and suggest the security plan and policy

Network Security Design
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

A Security Policy

- 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 (IDSs)

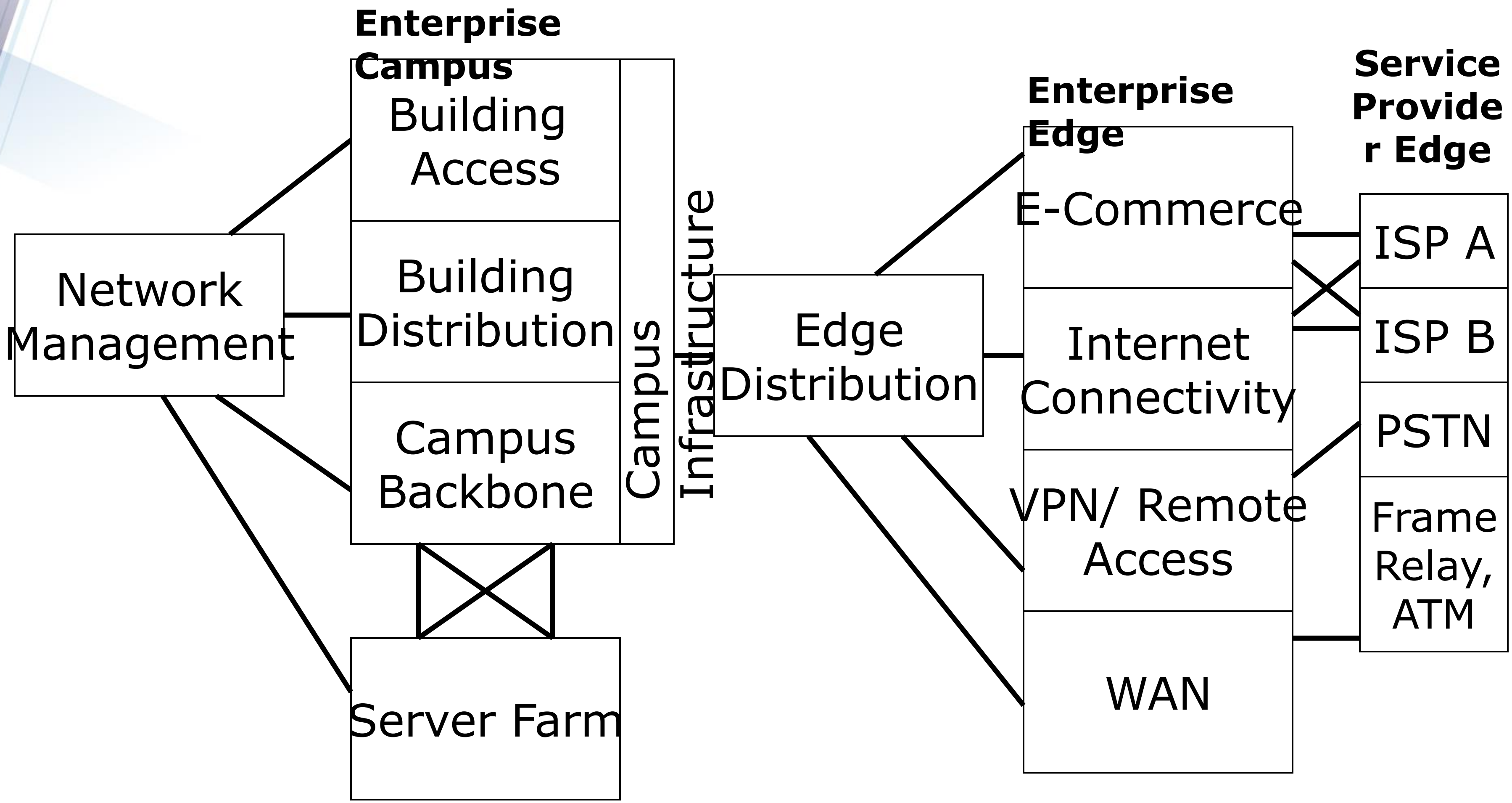
Modularizing Security Design

- 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

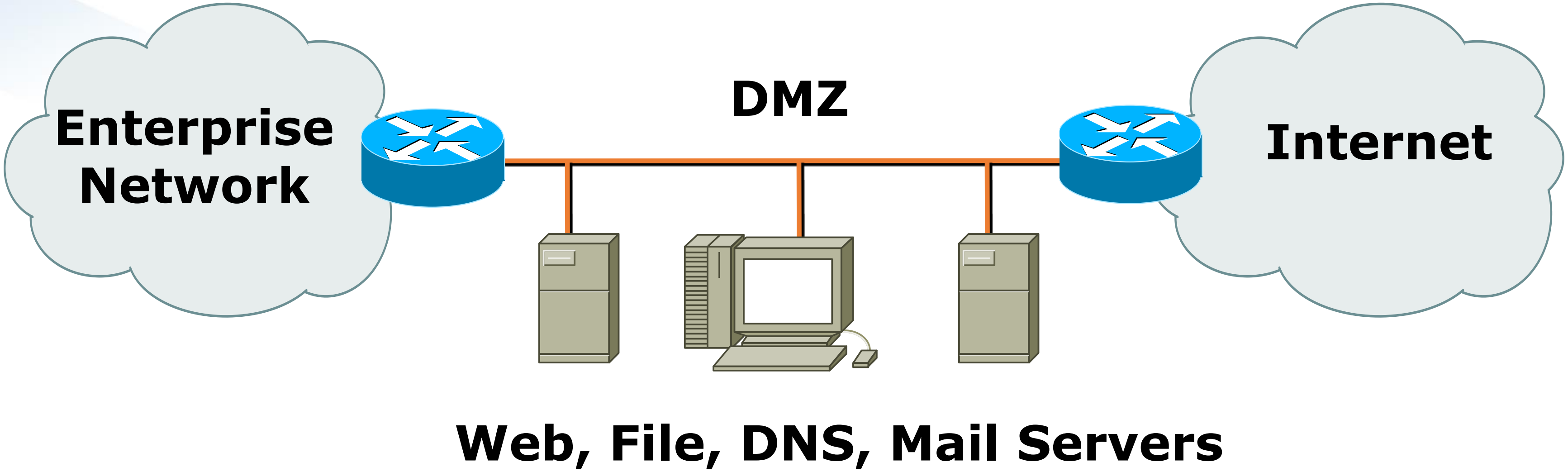
Cisco’s Enterprise Composite Network Model



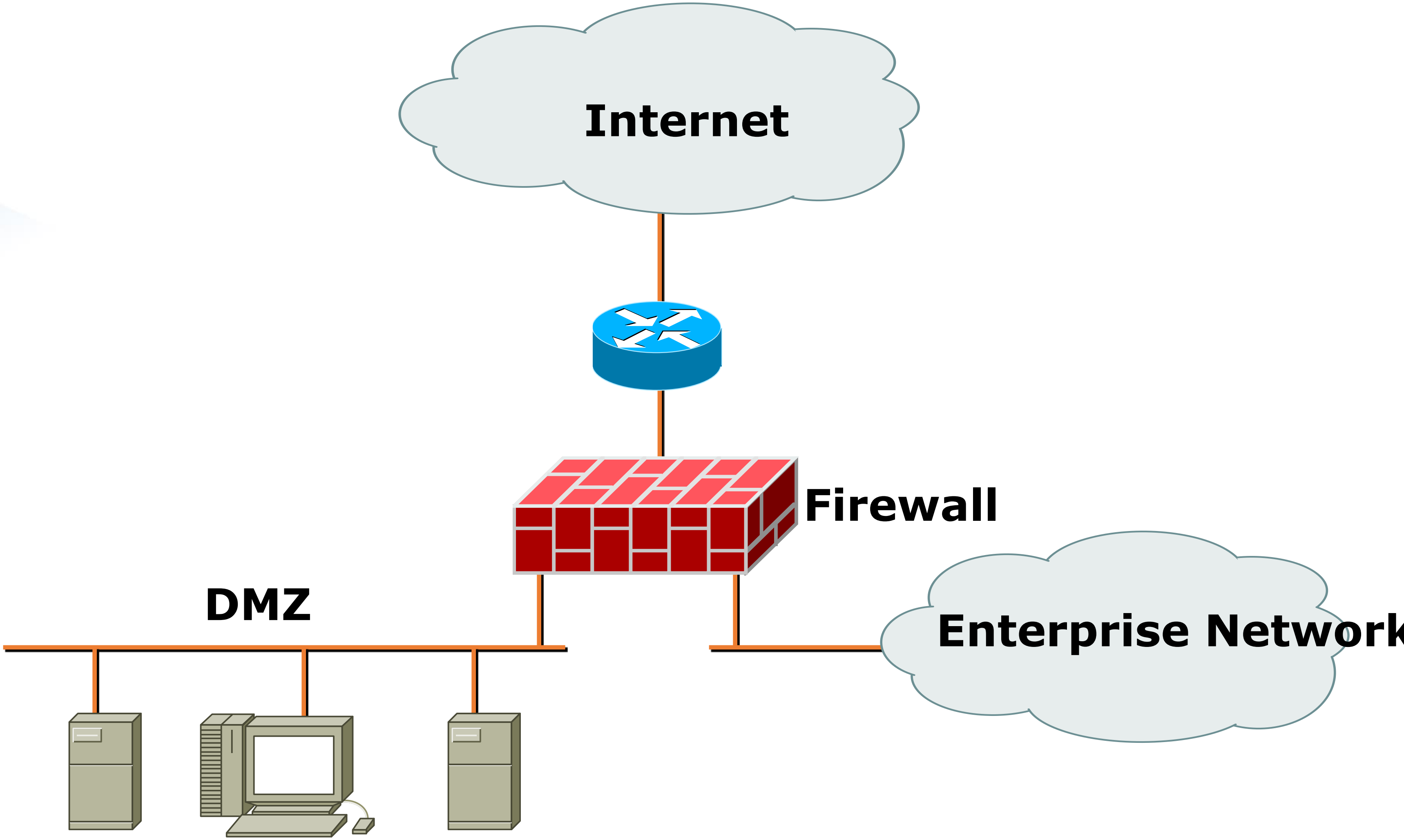
Securing Internet Connections

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

Security Topologies



Security Topologies



Internet

Firewall

DMZ

Enterprise Network

Web, File, DNS, Mail Servers

Securing Remote-Access and Virtual Private Networks

- 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

Securing Wireless Networks

- Place wireless LANs (WLANs) in their own subnet or VLAN
  - Simplifies addressing and makes it easier to configure packet filters
- Require all wireless (and wired) laptops to run personal firewall and antivirus software
- Disable beacons that broadcast the SSID, and require MAC address authentication
  - Except in cases where the WLAN is used by visitors

WLAN Security Options

- Wired Equivalent Privacy (WEP)
- IEEE 802.11i
- Wi-Fi Protected Access (WPA)
- IEEE 802.1X Extensible Authentication Protocol (EAP)
  - Lightweight EAP or LEAP (Cisco)
  - Protected EAP (PEAP)
- Virtual Private Networks (VPNs)
- Any other acronyms we can think of? :-)

Wired Equivalent Privacy (WEP)

- Defined by IEEE 802.11
- Users must possess the appropriate WEP key that is also configured on the access point
  - 64 or 128-bit key (or passphrase)
- WEP encrypts the data using the RC4 stream cipher method
- Infamous for being crackable

WEP Alternatives

- Vendor enhancements to WEP
- Temporal Key Integrity Protocol (TKIP)
  - Every frame has a new and unique WEP key
- Advanced Encryption Standard (AES)
- IEEE 802.11i
- Wi-Fi Protected Access (WPA) from the Wi-Fi Alliance
  - Realistic parts of IEEE 802.11i now!

Cisco’s Lightweight EAP (LEAP)

- Standard EAP plus mutual authentication
  - The user and the access point must authenticate
- Used on Cisco and other vendors’ products

VPN Software on Wireless Clients

- Safest way to do wireless networking for corporations
- Wireless client requires VPN software
- Connects to VPN concentrator at HQ
- Creates a tunnel for sending all traffic
- VPN security provides:
  - User authentication
  - Strong encryption of data
  - Data integrity

Summary

- Use a top-down approach
  - Chapter 2 talks about identifying assets and risks and developing security requirements
  - Chapter 5 talks about logical design for security (secure topologies)
  - Chapter 8 talks about the security plan, policy, and procedures
  - Chapter 8 also covers security mechanisms and selecting the right mechanisms for the different components of a modular network design

Review Questions

- How does a security plan differ from a security policy?
- Why is it important to achieve buy-in from users, managers, and technical staff for the security policy?
- What are some methods for keeping hackers from viewing and changing router and switch configuration information?
- How can a network manager secure a wireless network?