CSET 150

NETWORK DESIGN AND MANAGEMENT

EVENING MASTERS EDITION

DR. MAHBOOB QAOSAR

ASSOCIATE PROFESSOR, CSE, RU

COURSE CONTENTS

Network Design: Design Principles, Determining Requirements, Analyzing the Existing Network, Preparing the Preliminary Design, Completing the Final Design Development, Deploying the Network, Monitoring and Redesigning, Maintaining, Design Documentation, Modular Network Design, Hierarchical Network Design, The Cisco Enterprise Composite Network Model.

Technologies - Switching Design: Switching Types, Spanning, Tree Protocol, Redundancy in Layer 2 Switched Networks, STP Terminology and Operation, Virtual LANs, Trunks, Inter VLAN Routing, Multilayer Switching, Switching Security and Design Considerations, IPv4 Address Design, Private and Public Addresses, NAT, Subnet Masks, Hierarchical IP Address Design, IPv4 Routing Protocols, Classification, Metrics, Routing Protocol Selection.

Network Security Design: Hacking, Vulnerabilities, Design Issues, Human Issues, Implementation Issues, Threats, Reconnaissance Attacks, Access Attacks, Information Disclosure Attacks, Denial of Service Attacks, Threat Defense, Secure Communication, Network Security Best Practices, SAFE Campus Design.

Wireless LAN Design: Wireless Standards, Wireless Components, Wireless Security, Wireless Security Issues, Wireless Threat Mitigation, Wireless Management, Wireless Design Considerations, Site Survey, WLAN Roaming, Wireless IP Phones, Quality of Service Design, QoS Models, Congestion Avoidance, Congestion Management.

Network Management: ISO Network Management Standard, Protocols and Tools, SNMP, MIB, RMON NetFlow, Syslog, Network Management Strategy, SLCs and SLAs, IP Service-Level Agreements, Content Networking Design, Case Study, Venti Systems.

MITIGATING TECHNOLOGIES

- Known threats can usually be mitigated by security equipment and sound security policies.
- Mitigation techniques which are grouped in these four major categories:
    1. Threat defense
    2. Secure communication
    3. Trust and identity
    4. Network security best practices

THREAT DEFENSE

- … refers to the activities that are necessary to guard against known and unknown attacks, specifically by doing the following:
    1. Defending the edge (border)
    2. Protecting the interior (core)
    3. Guarding the end points

Threat Defense

- To do so, the campus design should include the following:
    1. Virus protection
    2. Traffic filtering
    3. Intrusion detection and prevention
    4. Content filtering

Mitigating Technologies

- Mitigating Technologies
  - Threat Defense
    - Virus protection

VIRUS PROTECTION

- … … **up-to-date virus protection.**
- Virus scanning can be performed at :
  - **Hosts:** Workstations and servers.
  - **E-mail servers:** Incoming messages are scanned prior to being passed to the recipient.
  - **Network:** An intrusion detection system (IDS) or intrusion prevention system (IPS),
- N.B.: recommendation – different brand antivirus @ different junction.

Mitigating Technologies

- Mitigating Technologies
  - Threat Defense
    - ~~Virus protection~~
    - **Traffic filtering**

TRAFFIC FILTERING

- Traffic filtering can be achieved at many layers of the OSI model.
- It can be done at the **data link layer** using the **Media Access Control (MAC) address**
- But is most commonly done at the network layer through packet filtering.
- Packet filtering is further divided into the following areas:
  1. Static packet filtering
  2. Dynamic packet filtering

STATIC PACKET FILTERING

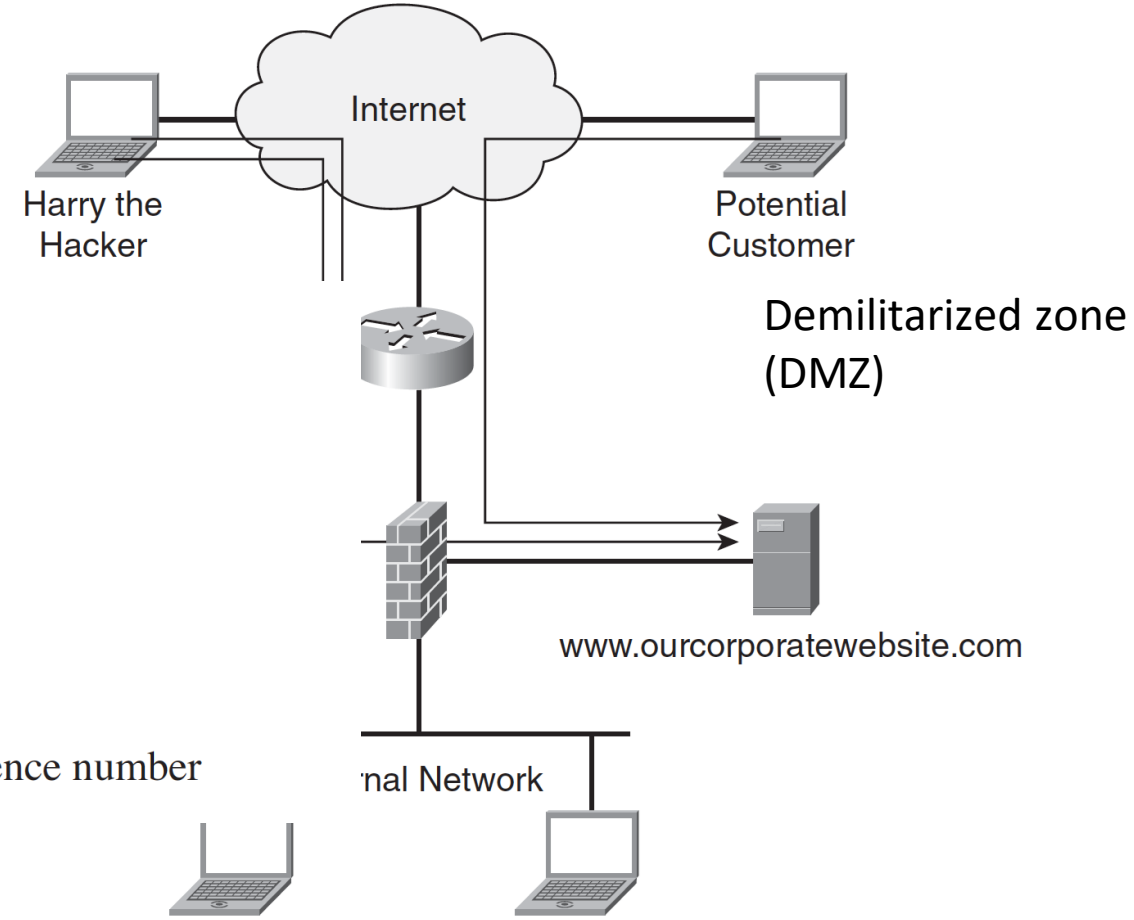
- …also known as stateless packet filtering or stateless firewalling.
- It is often performed at the perimeter router, which acts as the logical point of demarcation between the ISP and the corporate network.
- With stateless firewalling, the router does not track the state of packets and does not know whether a packet is part of the SYN process, the actual transmission, or the FIN process.
- A stateless firewall typically tracks only **IP addresses** and therefore can be tricked by a hacker who spoofs IP addresses.

DYNAMIC PACKET FILTERING

- … also referred to as **Stateful firewalling**.
- It is usually done by a firewall, which is a dedicated appliance that performs packet scans.
- The default behavior of a firewall is that outgoing traffic, traffic that flows from the inside network to the outside network is allowed to leave and its reply traffic is allowed back in.
- However, traffic that originates from the outside network and attempts to come to the inside network is automatically denied.

DYNAMIC PACKET FILTERING

- Source IP address
- Destination IP address
- Source port
- Destination port
- Connection TCP flags
- Randomized TCP sequence number



Mitigating Technologies

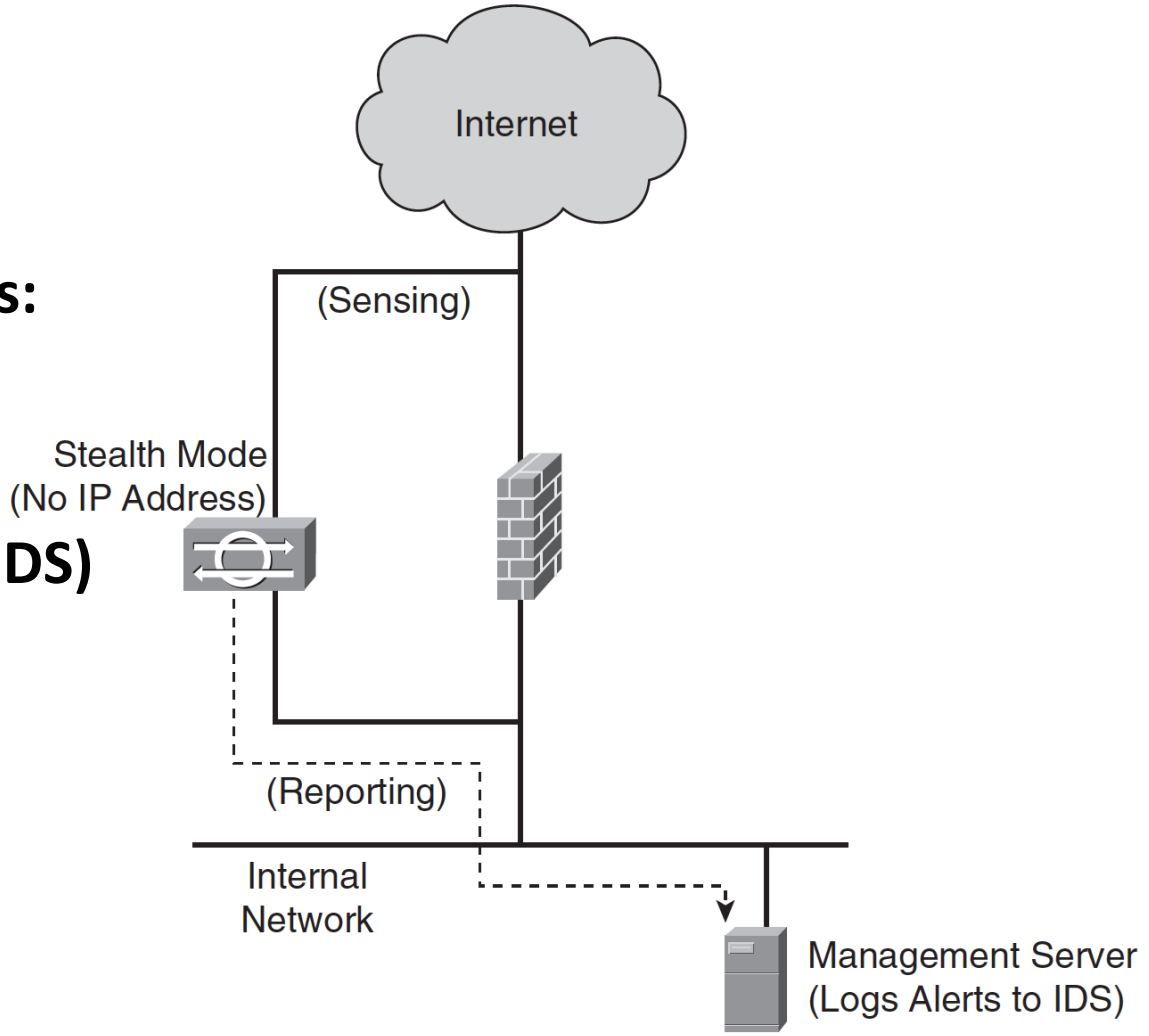
- Mitigating Technologies
  - Threat Defense
    - ~~Virus protection~~
    - ~~Traffic filtering~~
    - **Intrusion detection and prevention**

INTRUSION DETECTION & PREVENTION

- **INTRUSION – interruption**
- An IDS watches for:
  - **Attack signatures**, such as DoS and virus patterns
  - **Traffic anomalies**, such as the same source sending countless requests to SYN on a specific target
  - **Protocol anomalies**, such as a malformed packet
- An IDS can be one of the following:
  - **Network-based IDS (NIDS)** A dedicated appliance installed on the network
  - **Host-based IDS (HIDS)** Integrated software on a mission-critical system

Intrusion Detection & Prevention

- **Network-Based IDSs:**
- **NIDS**
- **Host-Based IDSs (HIDS)**
  - Mission critical stage



Intrusion Detection & Prevention

- **Intrusion Prevention Systems**
- Upon discovering malicious activity, the IPS can take at least one of the following actions:
  1. Alert the management console server
  2. Send a TCP reset (RST) to the source
  3. Shun the source of the attack by sending a command to the firewall requesting it to temporarily block the suspect IP address.
- Currently, only subtle differences exist between IDSs and IPSs; therefore, many vendors interchange the terms.

Mitigating Technologies

- Mitigating Technologies
  - Threat Defense
    - ~~Virus protection~~
    - ~~Traffic filtering~~
    - ~~Intrusion detection and prevention~~
    - **Content filtering**

CONTENT FILTERING

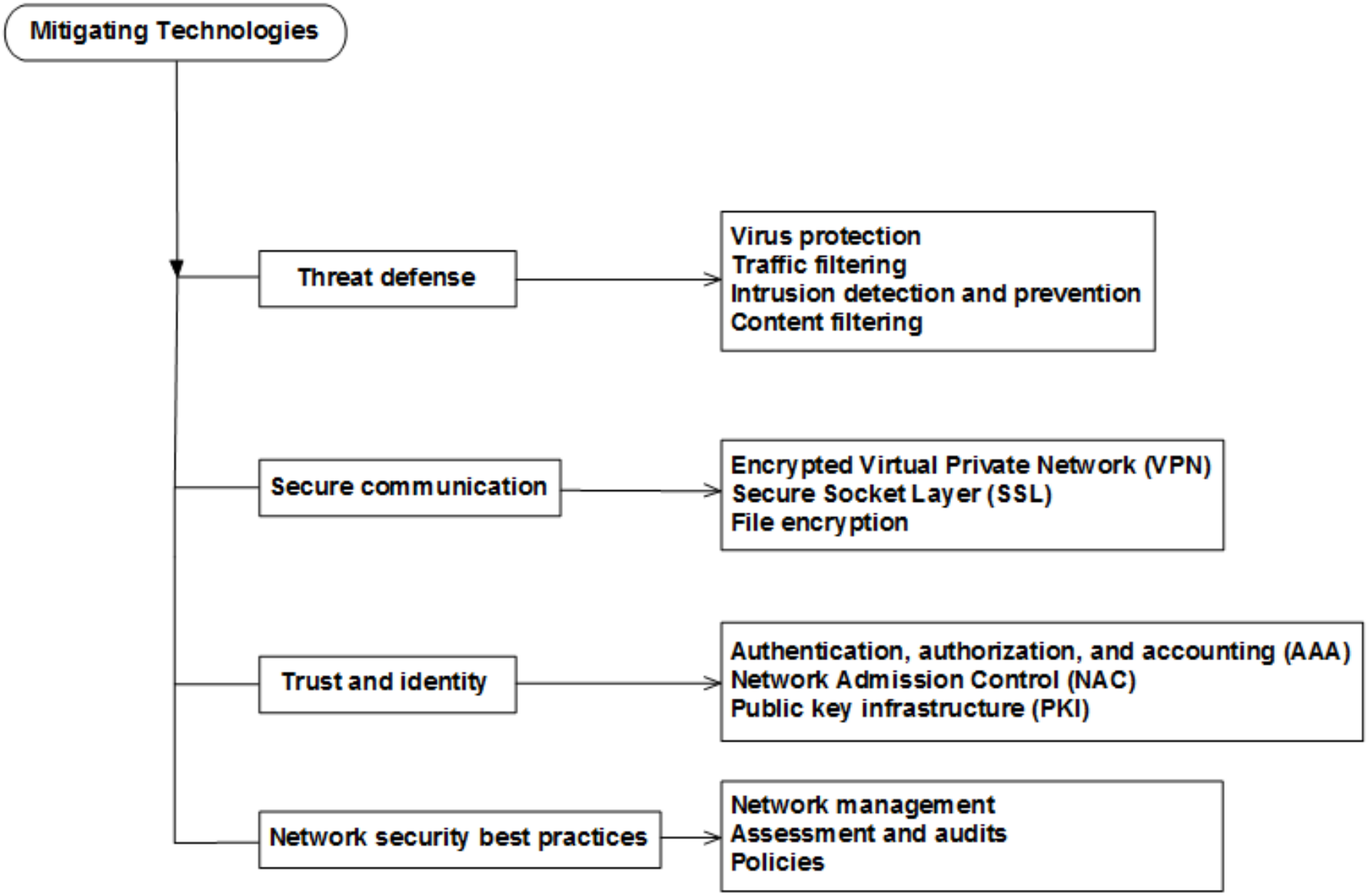
- **Uniform resource locator (URL) filtering**
  - Corporations use content filtering to enforce their Internet usage policies, hoping to protect themselves from possible legal implications should their employees visit objectionable websites
- **E-mail filtering**
  - When designing your corporate e-mail services, consider including an e-mail filtering service. That service, installed on the same network segment as your mail server (usually in a DMZ), sanitizes the e-mail from malware and some executable attachments prior to delivery of the messages to the end user

Mitigating Technologies

- Mitigating Technologies
  - Threat Defense
    - ~~Virus protection~~
    - ~~Traffic filtering~~
    - ~~Intrusion detection and prevention~~
    - ~~Content filtering~~

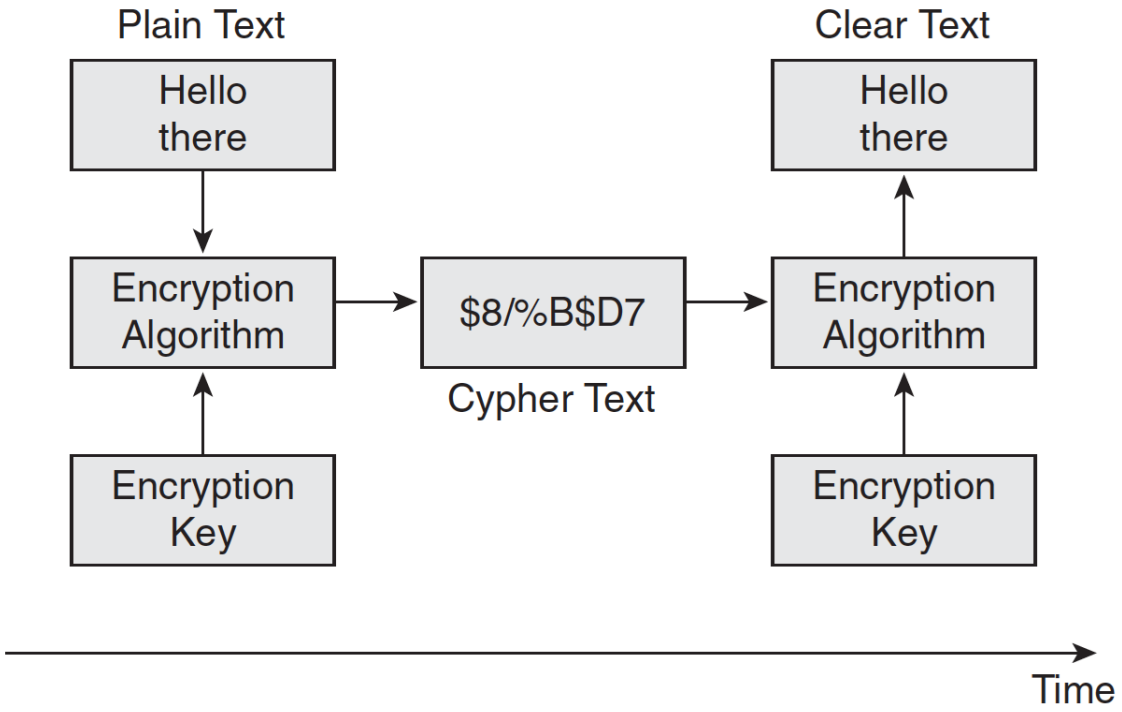
Mitigating Technologies

- Mitigating Technologies
  - ~~Threat Defense~~
  - Secure communication
  - Trust and identity
  - Network security best practices


Mitigating Technologies
Threat defense
Virus protection
Traffic filtering
Intrusion detection and prevention
Content filtering
Secure communication
Encrypted Virtual Private Network (VPN)
Secure Socket Layer (SSL)
File encryption
Trust and identity
Authentication, authorization, and accounting (AAA)
Network Admission Control (NAC)
Public key infrastructure (PKI)
Network security best practices
Network management
Assessment and audits
Policies

SECURE COMMUNICATION

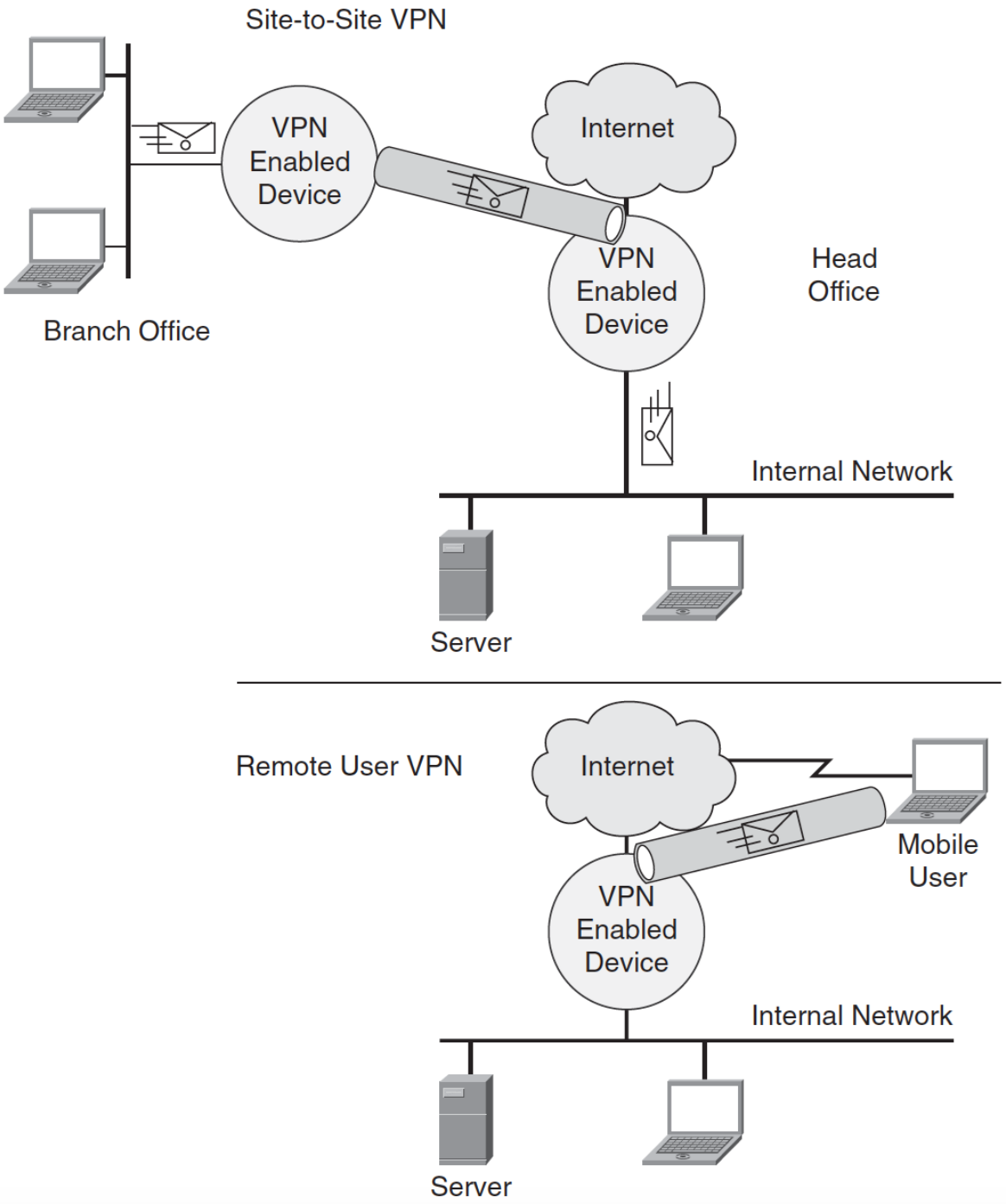
- The following are the two types of encryption keys:
  - **Symmetrical** keys The same key encrypts and decrypts a message.
  - **Asymmetrical keys** A different key decrypts a message from the key that encrypted the message. This is the case with public and private keys.



SECURE COMMUNICATION

- As part of network design activities, you might consider using one of the following common encryption scenarios:
  1. Encrypted VPN
  2. SSL
  3. File encryption

ENCRYPTED VPN



SSL & File Encryption

- **SSL**
  - SSL provides encryption of data to and from a web browser and could be included in a network design if a point-to-point encryption is needed for a service.

- **File Encryption**
  - In the case where a document requires confidentiality but the communication might be in clear text, a person can use file-encryption software such as Pretty Good Privacy (PGP) to encrypt the file. The encrypted file must be unencrypted by the reader after it is received.

Mitigating Technologies

- Mitigating Technologies
  - ~~Threat Defense~~
  - ~~Secure communication~~
  - Trust and identity
  - Network security best practices

TRUST AND IDENTITY

- Trust and identity management includes the following:
  1. Authentication, authorization, and accounting capabilities (AAA)
  2. Network Admission Control (NAC)

- **Authentication**—***Who?*** Checks the identity of the user, typically through a username and password combination.
- **Authorization**—***What?*** After the user is validated, the AAA server dictates what activity the user is allowed to perform on the network.
- **Accounting**—***When?*** The AAA server can record the length of the session, the services accessed during the session, and so forth.

TRUST AND IDENTITY

- Strong authentication refers to the two-factor authentication method. The users are authenticated using two of the following factors:

- **Something you know**—Such as a password or personal identification number (PIN)
- **Something you have**—Such as an access card, bank card, or token*
- **Something you are**—For example, some biometrics, such as a retina print or a fingerprint
- **Something you do**—Such as your handwriting, including the style, pressure applied, and so forth

NETWORK ADMISSION CONTROL

- **Network Admission Control ⇨ NAC**
- NAC ensures that users and their computers comply with corporate network policies.

Figure 4-8. Network Admission Control