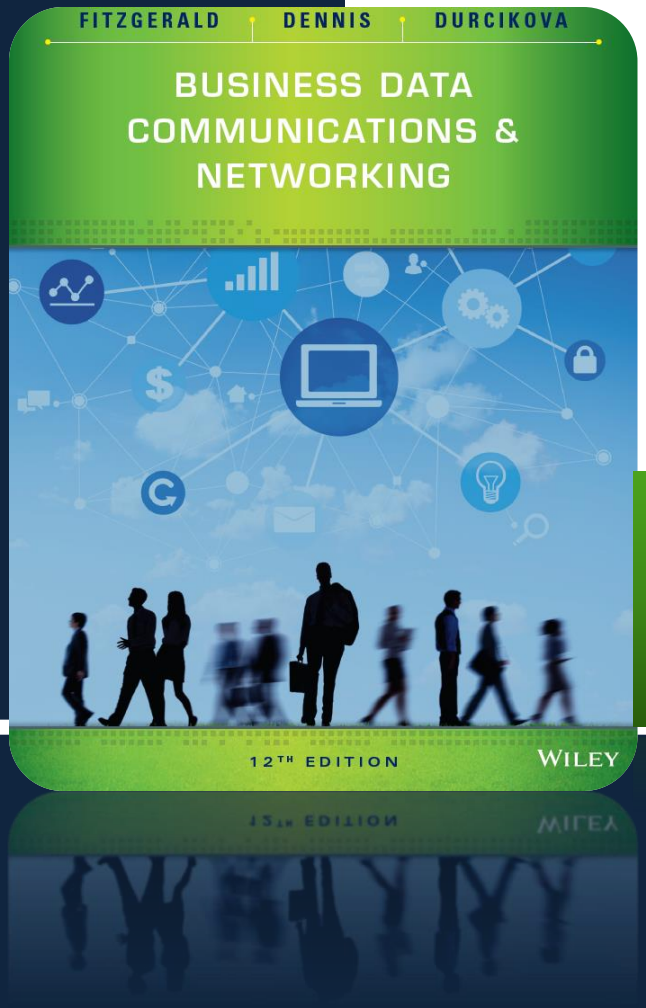


BUSINESS DATA COMMUNICATIONS & NETWORKING

Chapter 11
Network Security

FitzGerald ● Dennis ● Durcikova

Prepared by Taylor M. Wells: College of Business Administration, California State University, Sacramento

Outline

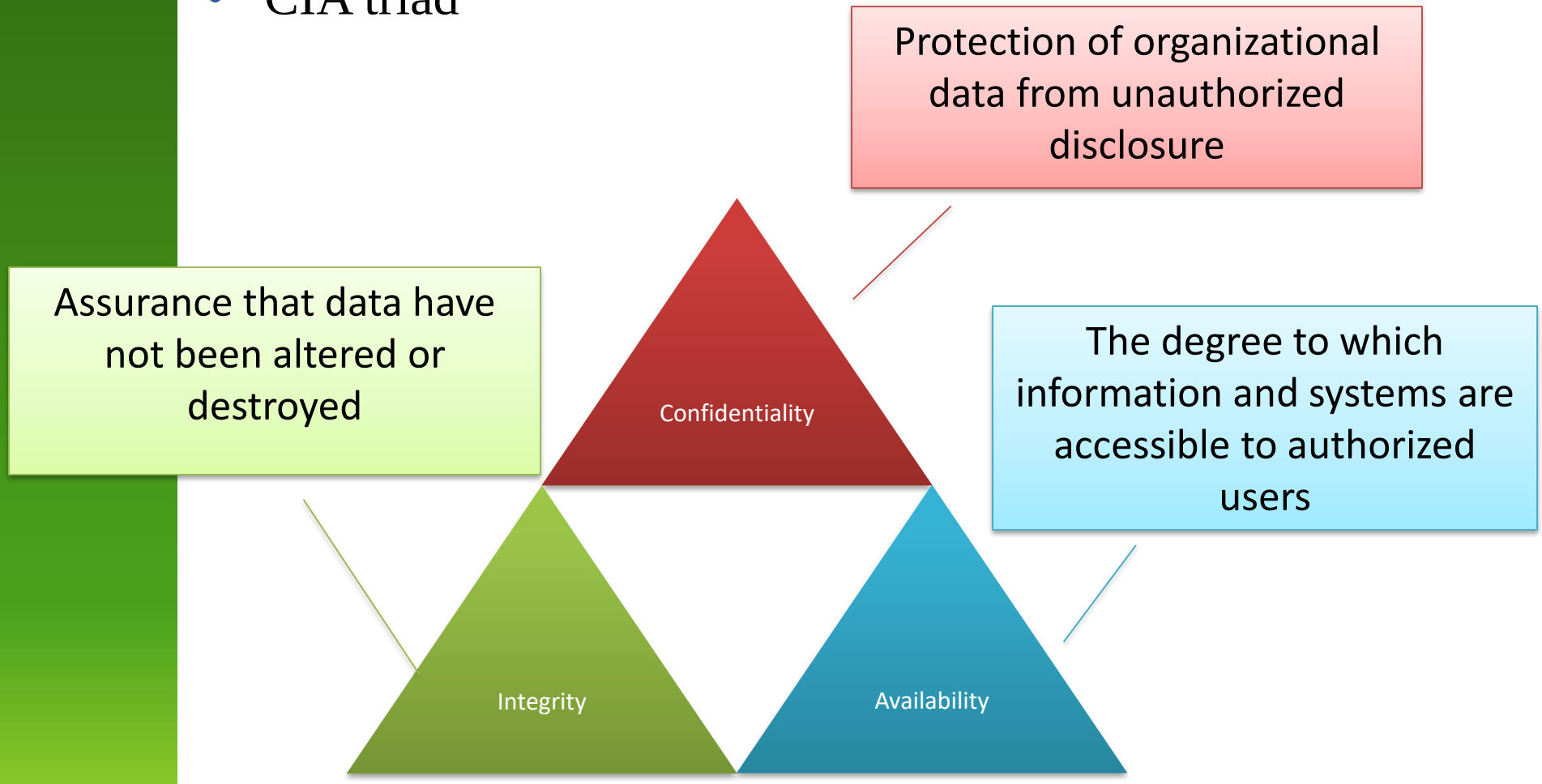
- Importance of Network Security
- Security Goals
- Network Controls
- Risk Assessment
- Ensuring Business Continuity
- Intrusion Prevention
- Recommended Practices
- Implications for Management

Importance of Network Security

- Security has always been a major business concern
- Computers and the Internet have redefined the nature of information security
- Average value of organizational data and applications far exceeds cost of networks
- Losses associated with security failures can be large
  - Financial loss due to theft and from system downtime
  - Loss of consumer confidence
  - Fines

Security Goals

- CIA triad



Security Threats

- Threats to Business Continuity
  - Disruptions – A loss or reduction in network service
  - Destruction of data
  - Disasters
- Threat of Unauthorized Access (Intrusion)
  - External attackers exist, but most unauthorized access incidents involve employees

Network Controls

- **Network controls** are safeguards that reduce or eliminate threats to network security
- **Preventative controls**
  - Mitigate or stop a person from acting or an event from occurring
  - Act as a deterrent by discouraging or restraining
- **Detective controls**
  - Reveal or discover unwanted events (e.g., auditing)
  - Documenting events for potential evidence
- **Corrective controls**
  - Remedy an unwanted event or intrusion

Risk Assessment

- A key step in developing a secure network
- Assigns level of risks to various threats
- Risk assessment frameworks
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - Control Objectives for Information and Related Technology (COBIT)
  - Risk Management Guide for Information Technology Systems (NIST guide)

Risk Assessment

- Risk Assessment Steps

1. Develop risk measurement criteria
2. Inventory IT assets
3. Identify threats
4. Document existing controls
5. Identify improvements

Risk Assessment

1. Develop risk measurement criteria
   - The measures used to examine how threats impact the organization
   - Prioritize and evaluate each measure

Impact Area	Priority	Low Impact	Medium Impact	High Impact
Financial	High	Sales drop by less than 2%	Sales drop 2-10%	Sales drop by more than 10%
Productivity	Medium	Increase in operating expenses by less than 3%	Increase in operating expenses between 3-6%	Increase in operating expenses by more than 6%
Reputation	High	Decrease in number of customers by less than 2%	Decrease in number of customers by 2-15%	Decrease in number of customers by more than 15%
Legal	Medium	Incurring fines or fees less than $10,000	Incurring fines or fees between $10,000 and $60,000	Incurring fines or fees exceeding $60,000

Risk Assessment

2. Inventory IT assets
   - Mission-critical applications and data are the most important
   - Document and evaluate why each asset is important to the organization

Asset Type	Examples
Hardware	• Servers (e.g., mail, web, and file servers) • Client computers (e.g., desktops, laptops, tablets, phones, etc.) • Networking devices (e.g., switches and routers)
Circuits	• LANs, Backbone networks, WANs, Internet access circuits
Software	• Operating systems (servers, clients, and networking devices) • Application software ○ Some applications may be mission-critical and warrant special attention
Organizational data	• Databases

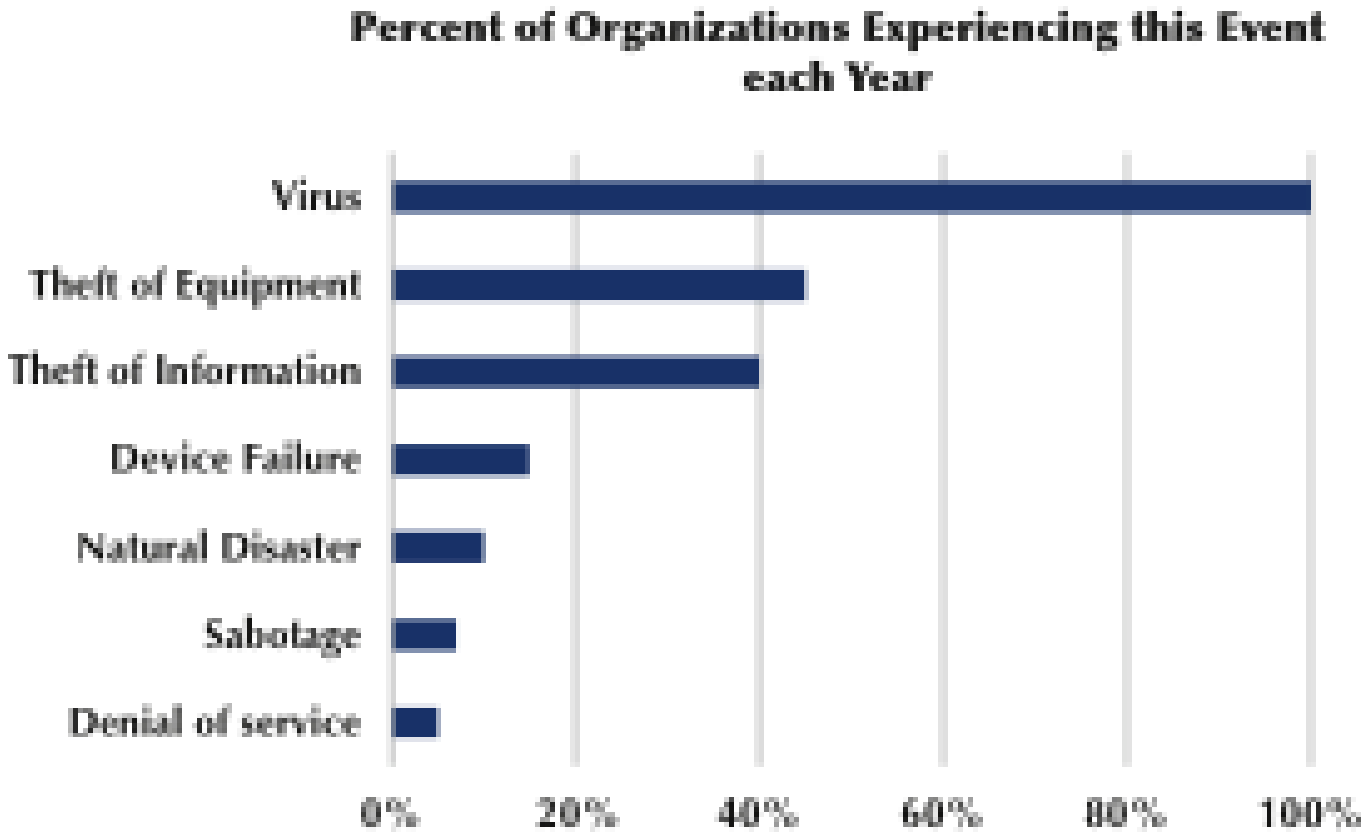
Risk Assessment

3. Identify threats
   - Any potential occurrence that can do harm, interrupt the systems using the network, or cause a monetary loss to the organization
   - Create **threat scenarios** that describe how an asset can be compromised by a threat
     - Likelihood of occurrence
     - Potential consequences of threat
     - **Risk Scores** can be used to quantify the impact and likelihood of occurrence

Risk Assessment

3. Identify threats

FIGURE 11-5
Likelihood of a threat



Risk Assessment

4. Document existing controls
   - Identify controls and determine how they will be used in the **risk control strategy**
   - Risk acceptance
     - Organizations may choose to take no actions for risks that have low impacts
   - Risk mitigation
     - Use of control to remove or reduce impact of threat
   - Risk sharing
     - Transferring all or part of impact (e.g., insurance)
   - Risk deferring
     - For non-imminent risks

Risk Assessment

5. Identify improvements
   - It is infeasible to mitigate all risks
   - Evaluate adequacy of the controls and degree of risk associated with each threat
   - Establish priorities for dealing with threats to network security

Ensuring Business Continuity

- Making certain that organization's data and applications will continue to operate even in the face of disruption, destruction, or disaster
  - Virus Protection
  - Denial of Service Protection
  - Theft Protection
  - Device Failure Protection
  - Disaster Protection

Ensuring Business Continuity

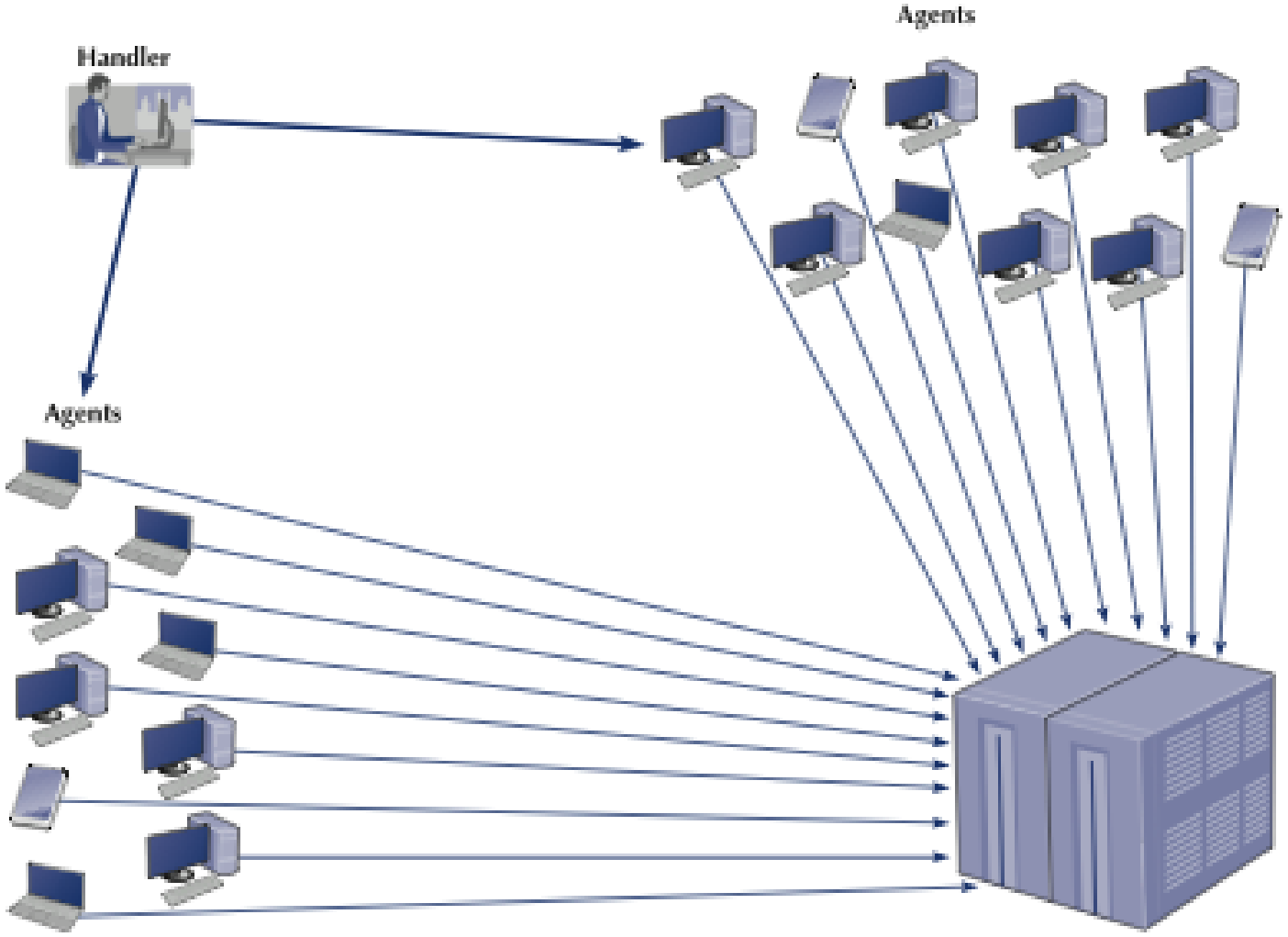
- Virus Protection
  - Nearly all organizations experience computer viruses
  - Widespread infection is less common
  - Viruses, worms, and Trojan horses
  - Malware, spyware, adware, and rootkits
  - Threat mitigated using antivirus software and training

Ensuring Business Continuity

- Denial of Service Protection
  - **Denial of Service (DoS) attacks** flood a network with messages that prevent normal access
    - A **Distributed DoS (DDoS)** attack uses multiple devices to perform the attack
    - DDoS attacks are often performed using a network of compromised devices (called agents, bots, or zombies)

Ensuring Business Continuity

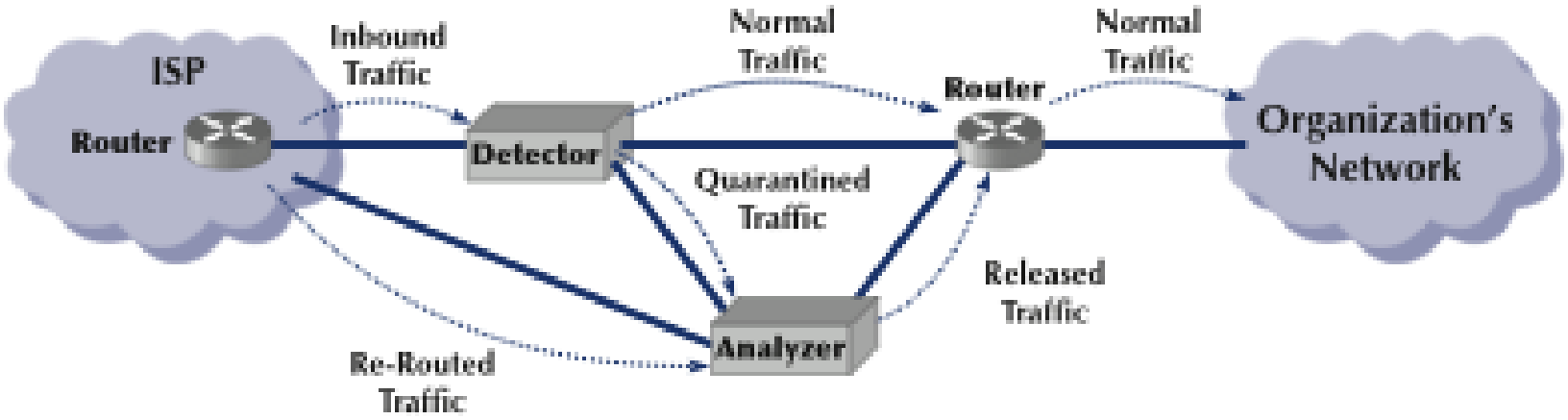
FIGURE 11-8 A distributed denial-of-service attack



Ensuring Business Continuity

- Denial of Service Protection
  - Traffic filtering
  - Traffic limiting
  - Traffic analysis
    - Using traffic anomaly analyzer

FIGURE 11-9 Traffic analysis reduces the impact of denial of service attacks



Ensuring Business Continuity

- Theft Protection
  - Mitigated using physical security and training
- Device Failure Protection
  - All devices fail eventually
  - Methods of reducing failures or their impacts
    - Redundancy in devices and circuits
      - e.g., redundant array of independent disks (RAID)
    - Uninterruptible power supplies (UPS)
    - Failover server clusters (or high-availability clusters)

Ensuring Business Continuity

- Disaster Protection
  - Avoidance
    - e.g., storing data in multiple locations and avoiding locations prone to natural disasters
  - Disaster Recovery
    - Organizations should have a clear **disaster recovery plan (DRP)**
      - Identify responses to different types of disasters
      - Provide recovery of data, applications and network
      - Specify the backup and recovery controls
    - Some organizations outsource to **disaster recovery firms**

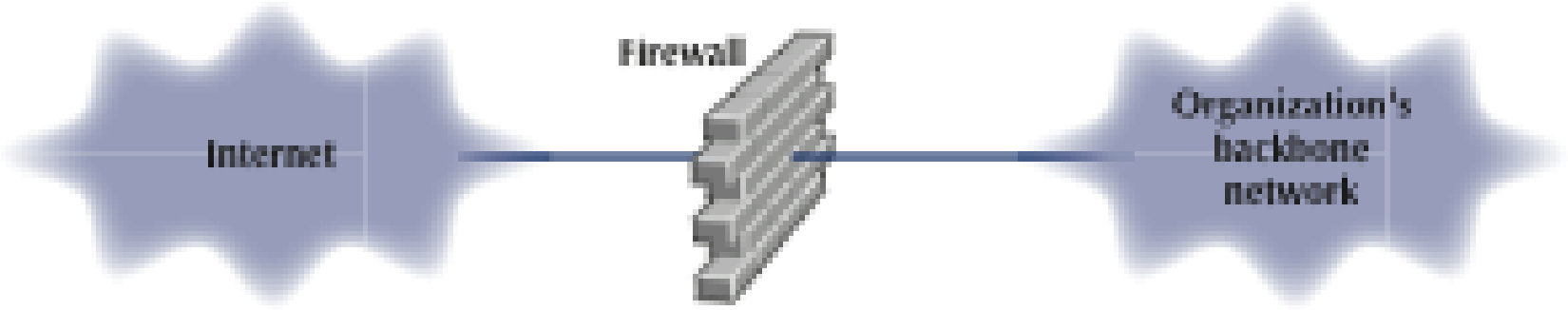
Intrusion Prevention

- Security Policy
- Physical Security
- Types of intruders
  - "Script kiddies" – novices using software created by others
  - Recreational hackers motivated by philosophy or entertainment
  - Professional hackers performing espionage or fraud
  - Organizational employees

Intrusion Prevention

- **Firewalls** restrict access to the network
- **Packet-level firewalls**
  - Examine the source/destination address of every packet
  - Using access control list (ACL) rules, decides which packets are allowed or denied

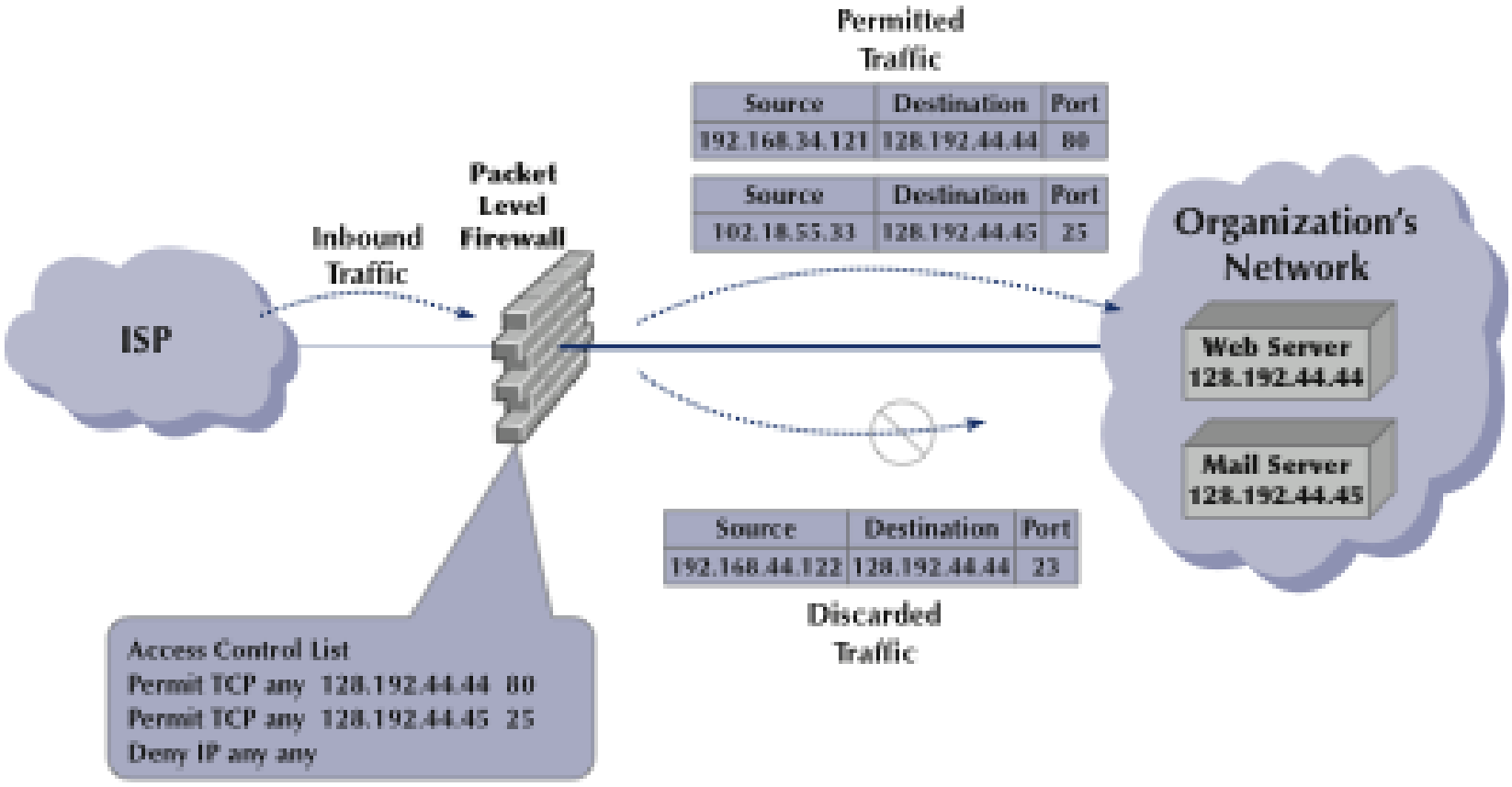
FIGURE 11-12
Using a firewall to protect networks



Intrusion Prevention

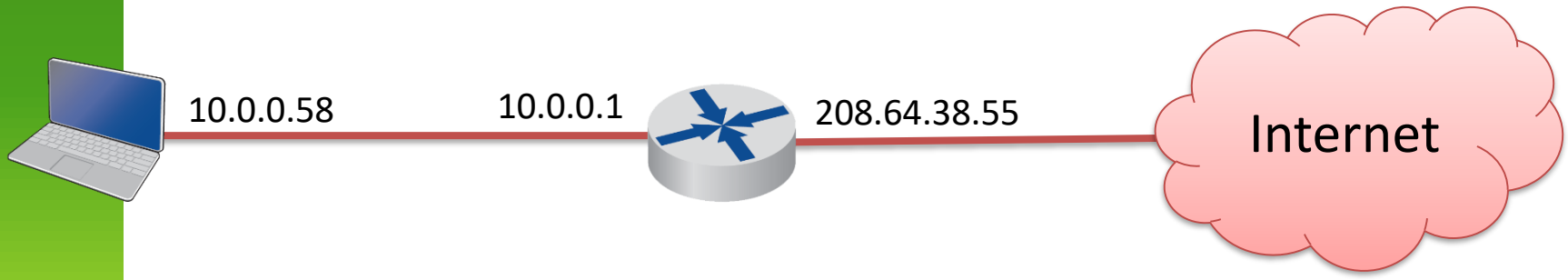
- Packet-level firewall

FIGURE 11-13 How packet-level firewalls work



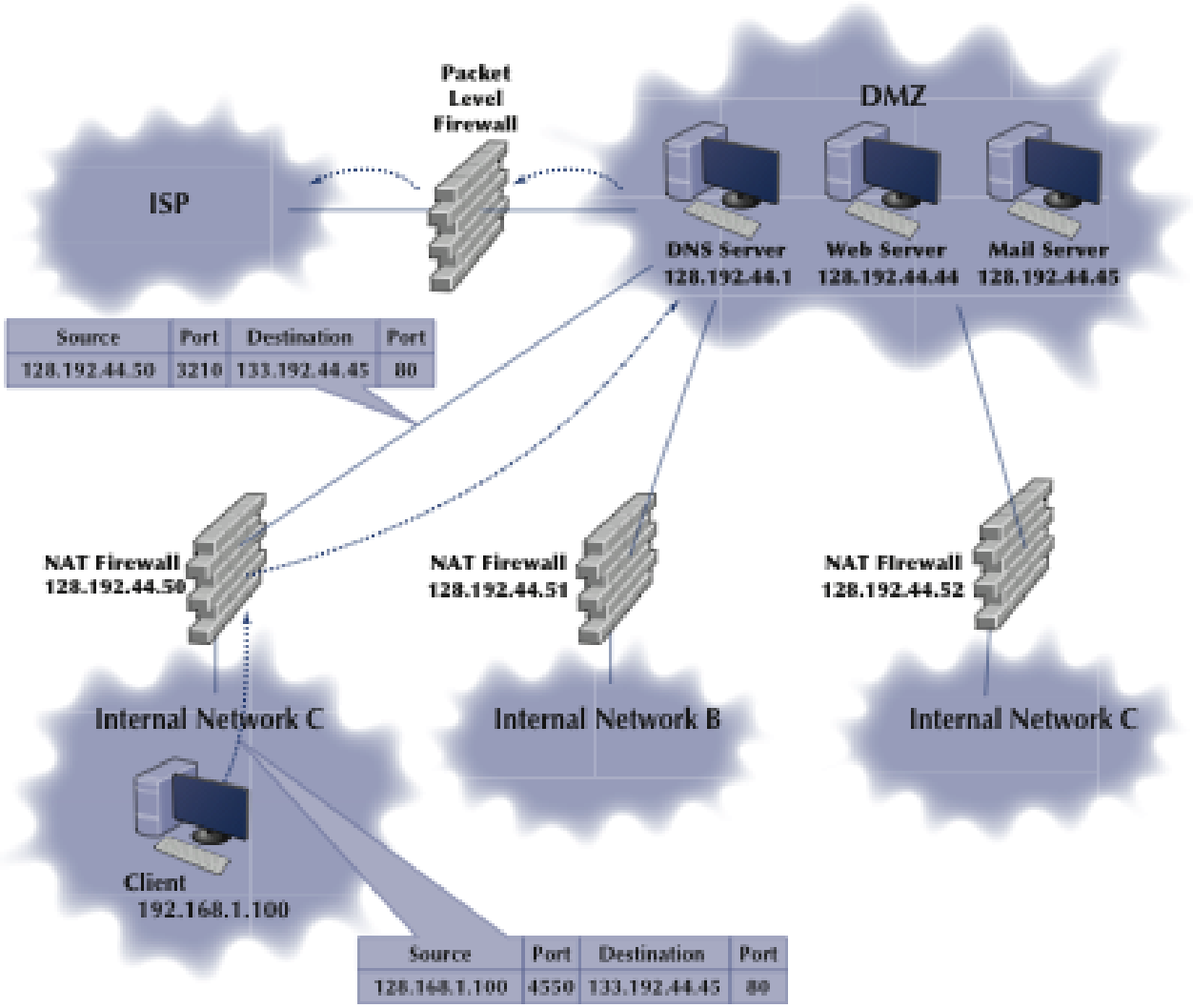
Intrusion Prevention

- **Application-level firewalls**
  - Use stateful inspection to examine traffic at layer 5 for anomalous behavior
- **Network address translation (NAT)**
  - Converts one IP address to another
  - Often from a publicly routable address to a private address



Intrusion Prevention

FIGURE 11-14 A typical network design using firewalls



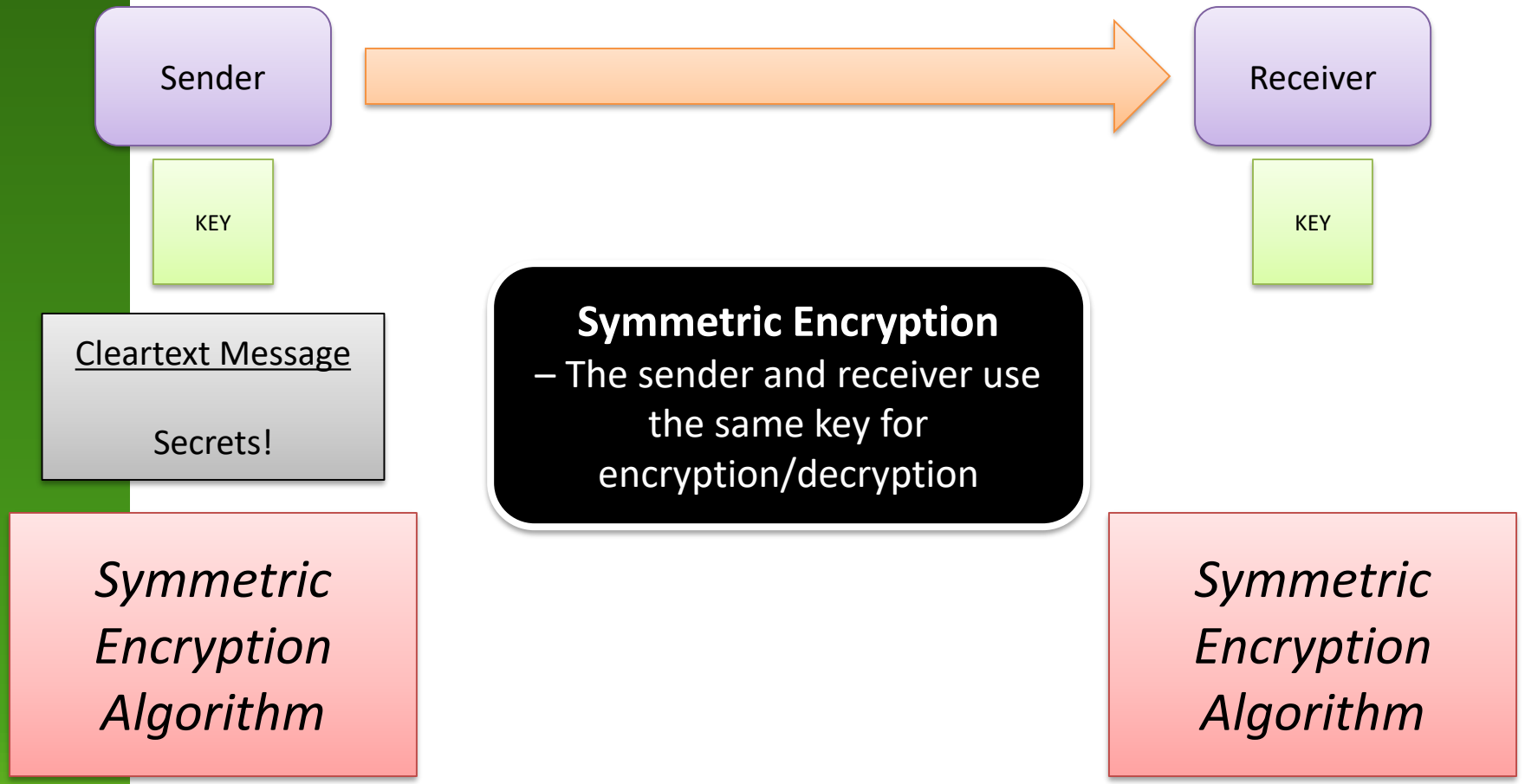
Intrusion Prevention

- **Encryption** is disguising information using mathematical rules, providing confidentiality
- The strength of the encryption is based on
  - The strength of the algorithm
  - The strength of the key
- Often the algorithm is widely known
- A **brute-force attack** on encryption means to try every possible key

Intrusion Prevention

- **Symmetric encryption**
  - Uses a single key for encrypting and decrypting
  - Challenge in sharing key
  - Used for bulk encryption because the algorithms are usually fast
  - Stream Ciphers
    - Encrypt one bit at a time
    - e.g., RC4
  - Block Ciphers
    - Encrypt a group of bits at a time
    - e.g., advanced encryption standard (AES)

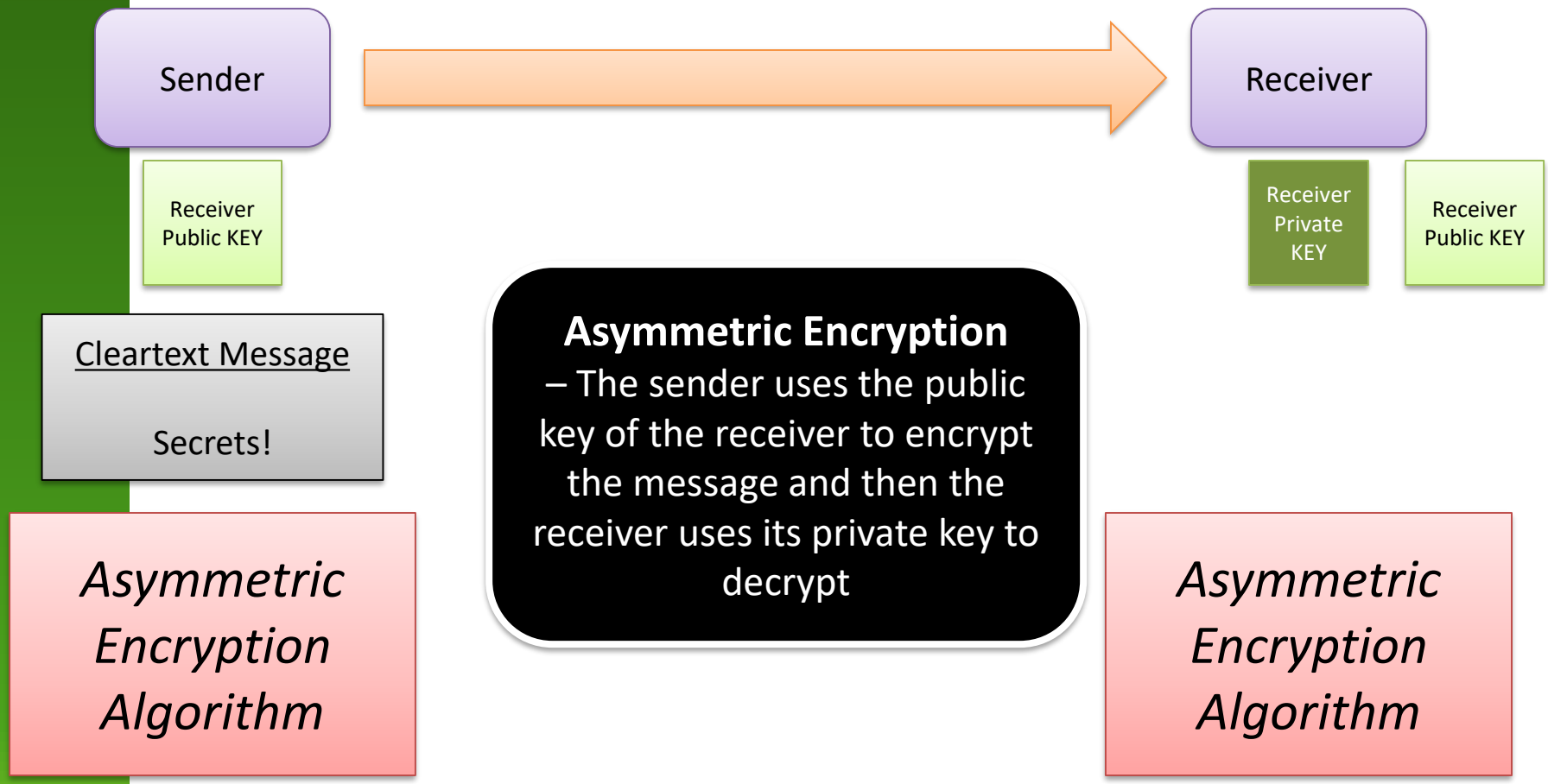
Intrusion Prevention



Intrusion Prevention

- **Asymmetric (public-key) encryption**
  - A pair of keys are used
  - One key is designated the public key and can be freely shared
  - The other key is designated the secret private key
  - When a message is encrypted using one key, it can only be decrypted with the other
  - Based on mathematical calculations that are easy in one direction but difficult in reverse
  - e.g., RSA

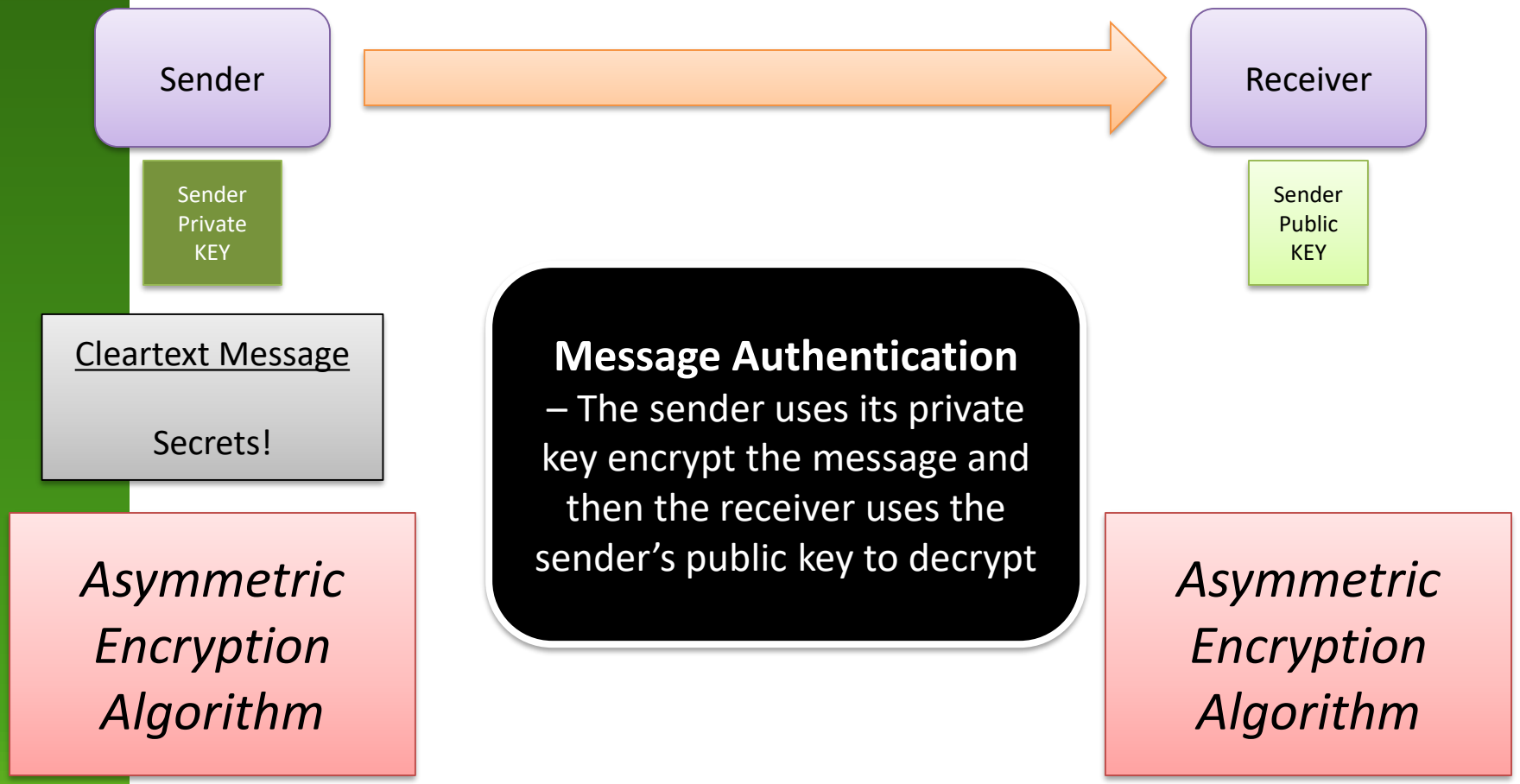
Intrusion Prevention



Intrusion Prevention

- **Asymmetric (public-key encryption)**
  - The **public key infrastructure (PKI)** is a set of hardware, software, organizations, and policies to associate a set of keys with an individual or organization
  - **Certificate authorities (CAs)** are trusted organizations that issue **digital certificates** proving that an individual or organization owns a public key
  - Digital certificates can be used to authenticate messages

Intrusion Prevention



Intrusion Prevention

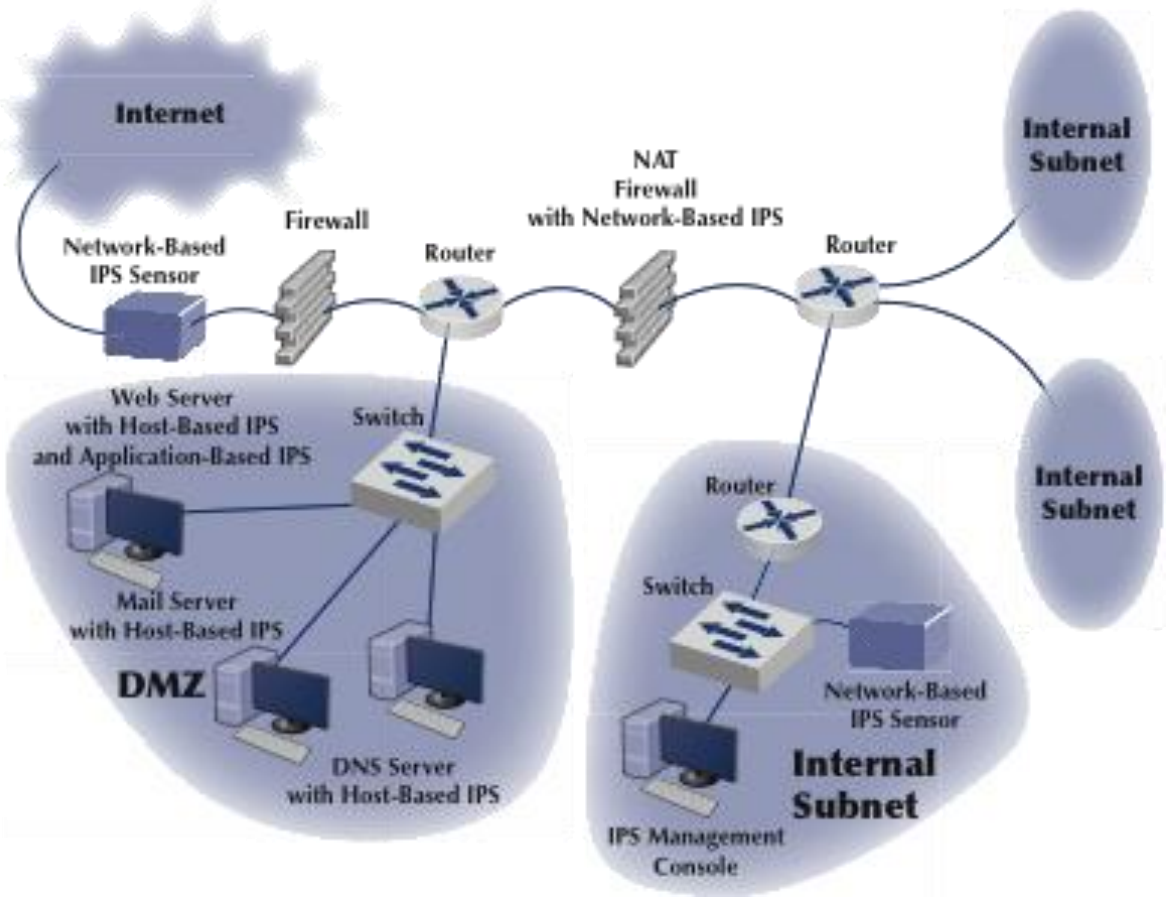
- Applications of encryption
  - **Pretty good privacy (PGP)** is used for encrypting email and some files
  - **Transport layer security (TLS)** succeeds **secure sockets layer (SSL)** as the primary encryption protocol on the Internet
  - **IP security protocol (IPSec)** is a network layer encryption protocol

Intrusion Prevention

- User authentication
  - **User profiles** are used to manage access to resources
  - Types of authentication
    - Something you know
      - e.g., passwords, passphrases, and pin numbers
    - Something you have
      - e.g., access cards, smart cards, tokens, phones
    - Something you are
      - Biometrics like fingerprints, handprints, retina
  - Using multiple types of authentication provides increased security (multi-factor authentication)
  - Most organizations moving to centralized authentication

Intrusion Prevention

FIGURE 11-18 Intrusion prevention system (IPS)
DMZ = demilitarized zone; DNS = Domain Name Service; NAT = network address translation



Recommended Practices

- Clear disaster recovery plan
- Strong security policy
  - Rigorously enforced
  - User training
- Use of security controls
- Content filtering

Implications for Management

- Fastest growing area of networking
- Cost of security expected to increase
  - More sophisticated controls
  - More sophisticated attacks
- Network becoming mission critical