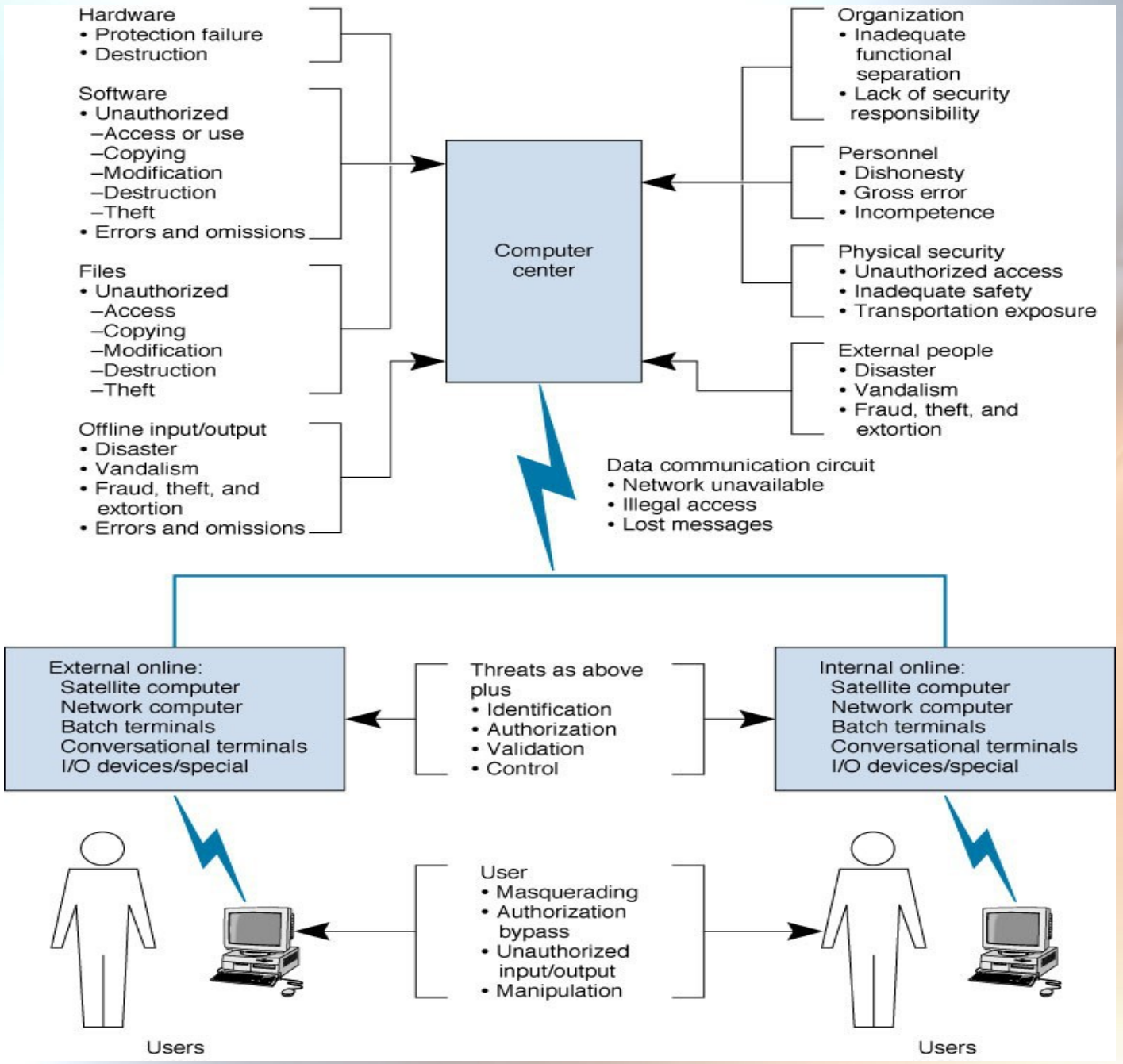
Slide Set 4

Network Security

Introduction

- Security is a major networking concern. 52% of the respondents to the 2006 Computer Security Institute/FBI Computer Crime and Security Survey reported unauthorized use of computer systems in the last 12 months.
- Gartner estimates losses from cyber attacks worldwide at $16.7 billion for year 2007.
- It means more than preventing a hacker from breaking into your computer, it also includes being able to recover from temporary service problems, or from natural disasters.

Common Threats to Network Security



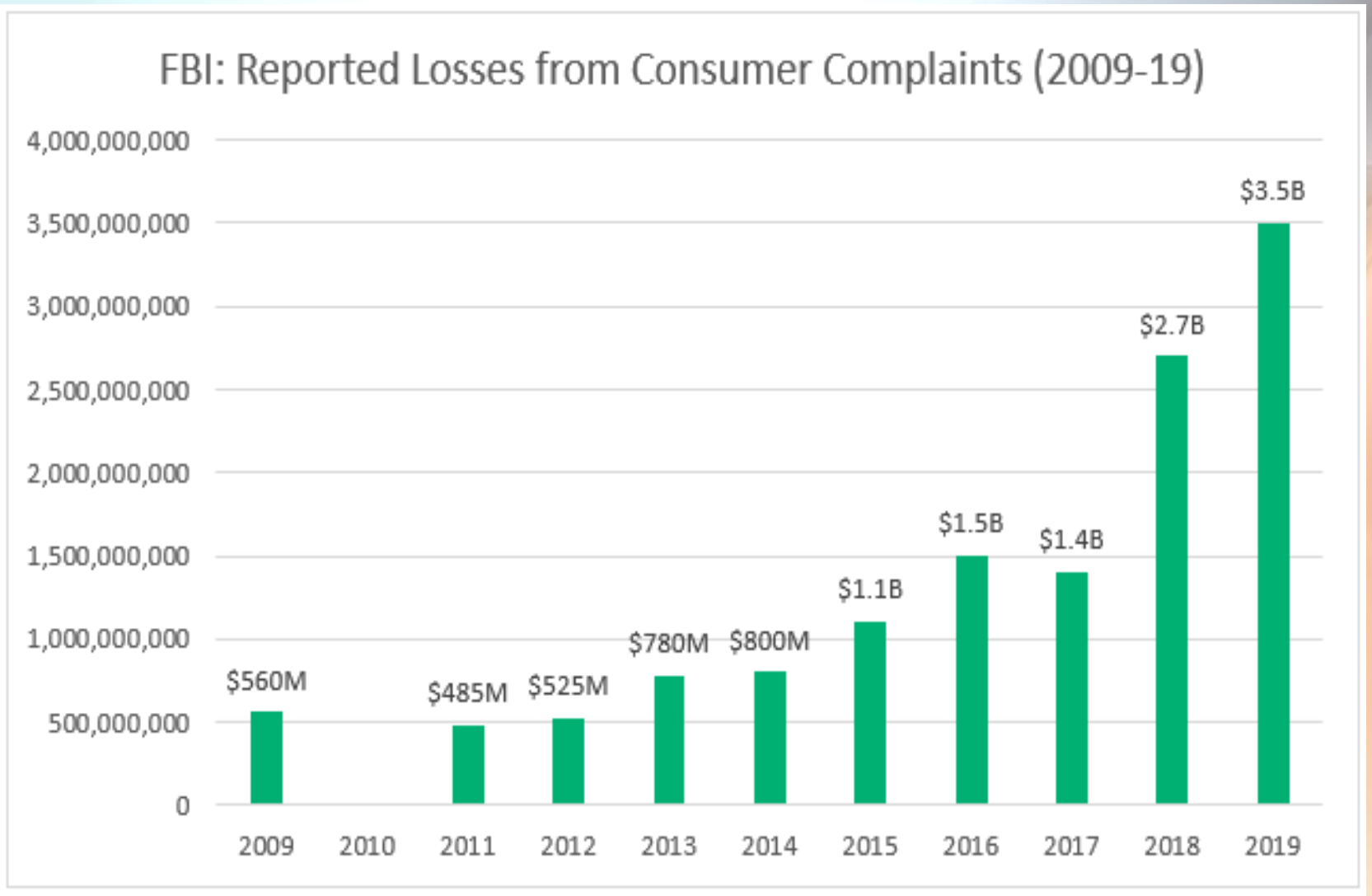
Types of Security Threats

- Disruptions are the loss or reduction in network service.
- Some disruptions may also be caused by or result in the destruction of data.
- Natural (or man-made) disasters may occur that destroy host computers or large sections of the network.
- Unauthorised access is often viewed as hackers gaining access to organizational data files and resources. However, most unauthorized access incidents involve employees.

Security Problems Are Growing

- The Computer Emergency Response Team (CERT) at Carnegie Mellon University was established with US DoD support in 1988 after a computer virus shut down 10% of the computers on the Internet
- In 1989, CERT responded to 137 incidents.
- In 2000, CERT responded to 21,756 incidents.
- By this count, security incidents are growing at a rate of 100% per year.
- In Mauritius, Computer Misuse and Cybercrime Act 2003, Data Protection Act 2017,

Number of Incidents and Losses reported in the USA



Network Controls

- Developing a secure network means developing mechanisms that reduce or eliminate the threats to network security, called controls.
- There are three types of controls:
  - Preventative controls - mitigate or stop a person from acting or an event from occurring (e.g. passwords).
  - Detective controls - reveal or discover unwanted events (e.g. auditing software, Intrusion Detection System IDS).
  - Corrective controls - rectify an unwanted event or a trespass (e.g. reinitiating a network circuit).

Network Controls

- It is not enough to just establish a series of controls; personnel need to be designated as responsible for network control and security.
- This includes developing controls, ensuring that they are operating effectively, and updating or replacing controls.
- Controls must also be periodically reviewed to:
  - ensure that the control is still present (verification)
  - determine if the control is working as specified (testing)

Security Threats

- A network security threat is any potentially adverse occurrence that can harm or interrupt the systems using the network, or cause a monetary loss to an organization.
- Once the threats are identified they are then ranked according to their occurrence.
- The next slide summarizes the most common cyber threats worldwide.

Top 15 Cyber Threats Worldwide

Evaluate the Network's Security

- The last step in designing a control spreadsheet is evaluating the adequacy of the controls and the degree of risk associated with each threat.
- Based on this, priorities can be decided on for dealing with threats to network security.
- The assessment can be done by the network manager, but it is better done by a team of experts chosen for their in-depth knowledge about the network and environment being reviewed.

Preventing Disruption, Destruction and Disaster

- Preventing disruptions, destructions and disasters mean addressing a variety of threats including:
  - Creating redundancy
  - Preventing natural disasters impact
  - Preventing theft
  - Preventing computer malware attacks
  - Preventing denial-of-service attacks

Network Redundancy

- The key to in preventing or reducing disruption, destruction and disaster - is **redundancy**
- Examples of components that provide redundancy include:
  - Uninterruptible Power Supplies (UPS)
  - Disk redundancy (RAID & Backup)
  - Network link redundancy (Spanning Tree Protocol)
  - Network topology (Mesh or Hybrid)
- Redundancy can be built into other network components as well.

Preventing Impact of Natural Disasters

- Disasters are different from disruptions since the entire site can be destroyed.
- The best solution is to have a completely redundant network that duplicates every network component, but in a different location.
- Generally speaking, preventing disasters is difficult. The most fundamental principle is to decentralize the network resources.
- Other steps depend on the type of disaster to be prevented.

Preventing Theft

- Equipment theft can also be a problem if precautions against it are not taken.
- Industry sources indicate that about $1 billion is lost each year to theft of computers and related equipment (USA statistic).
- For this reason, security plans should include an evaluation of ways to prevent equipment theft.

Preventing Computer Malware

- Special attention must be paid to preventing viruses that attach themselves to other programs and spread when the programs are executed.
- Macroviruses attach themselves to documents and become active when the files are opened are also common. Anti-malware software packages are available to check disks and files to ensure that they are virus-free.
- Incoming e-mail messages are the most common source of viruses. Attachments to incoming e-mail should be routinely checked for viruses.
- The use of filtering programs that 'clean' incoming e-mail is also becoming common.

Detecting Disruption, Destruction & Disaster

- One function of network monitoring software is to alert network managers to problems so that these can be corrected.
- Detecting minor disruptions can be more difficult.
- The network should also routinely log fault information to enable network managers to recognize minor service problems.
- In addition, there should be a clear procedure by which network users can report problems.

Disaster Recovery Plans (DRP)

- The goal of the disaster recovery plan (DRP) is to plan responses to possible disasters, providing for partial or complete recovery of all data, application software, network components, and physical facilities.
- Critical to the DRP are backup and recovery controls that enable an organization to recover its data and restart its application software should some part of the network fail.
- The DRP should also address what to do in a variety of situations, such as, if the main database is destroyed or if the data center is destroyed.

Preventing Intruder Access

- Four types of intruders attempt to gain unauthorized access to computer networks.
  1. Casual hackers who only have limited knowledge of computer security.
  2. Security experts whose motivation is the thrill of the hunt.
  3. Professional hackers who break into corporate or government computers for specific purposes.
  4. Organization employees who have legitimate access to the network but who gain access to information they are not authorized to use or view.

Preventing Unauthorized Access

- A proactive approach that includes routinely testing your security systems is key to preventing unauthorized access.
- Access related security issues include:
  - Security policies
  - User profiles
  - Physical security
  - Firewalls
  - Network address translation
  - Encryption

Developing a Security Policy

- The security policy should clearly define the important network components to be safeguarded along with controls needed to do that.
- The most common way for a hacker to break into a system is through “social engineering” (breaking security simply by asking how).

Elements of a Security Policy

- Names of responsible individuals.
- Incident reporting system and response team.
- Risk assessment with priorities.
- Controls on access points to prevent or deter unauthorized external access.
- Controls within the network to ensure internal users cannot exceed their authorized access.
- An acceptable use policy.
- User training plan on security.
- Testing and updating plans.

User Profiles and Forms of Access

- The limits of what users have access to on a network are determined by user profiles assigned to each user account by the network manager.
- The profile specifies access details such as which data and network resources a user can access and the type of access (e.g., read, write, create, delete).
- Most access is still password based, that is, users gain access based on something they know.
- Many systems require users to enter a password in conjunction with something they have, such as a smart card. ATM cards work in this way.
- In high-security applications, users may be required to present something they are, such as a finger, hand or the retina of their eye for scanning by a biometric system.

User Profiles: Managing User Access

- User profiles can limit the allowable log-in days, time of day, physical locations, and the allowable number of incorrect log-in attempts.
- Creating accounts and profiles is simple, as they are created when new personnel arrive.
- One security problem is often created because network managers forget to remove user accounts when someone leaves an organization.

Managing Users

- It is important to screen and classify both users and data (need to know).
- The effect of any security software packages that restrict or control access to files, records, or data items should also be reviewed.
- Adequate user training on network security should be provided through self-teaching manuals, newsletters, policy statements, and short courses.
- A well publicized security campaign can also help deter potential intruders.

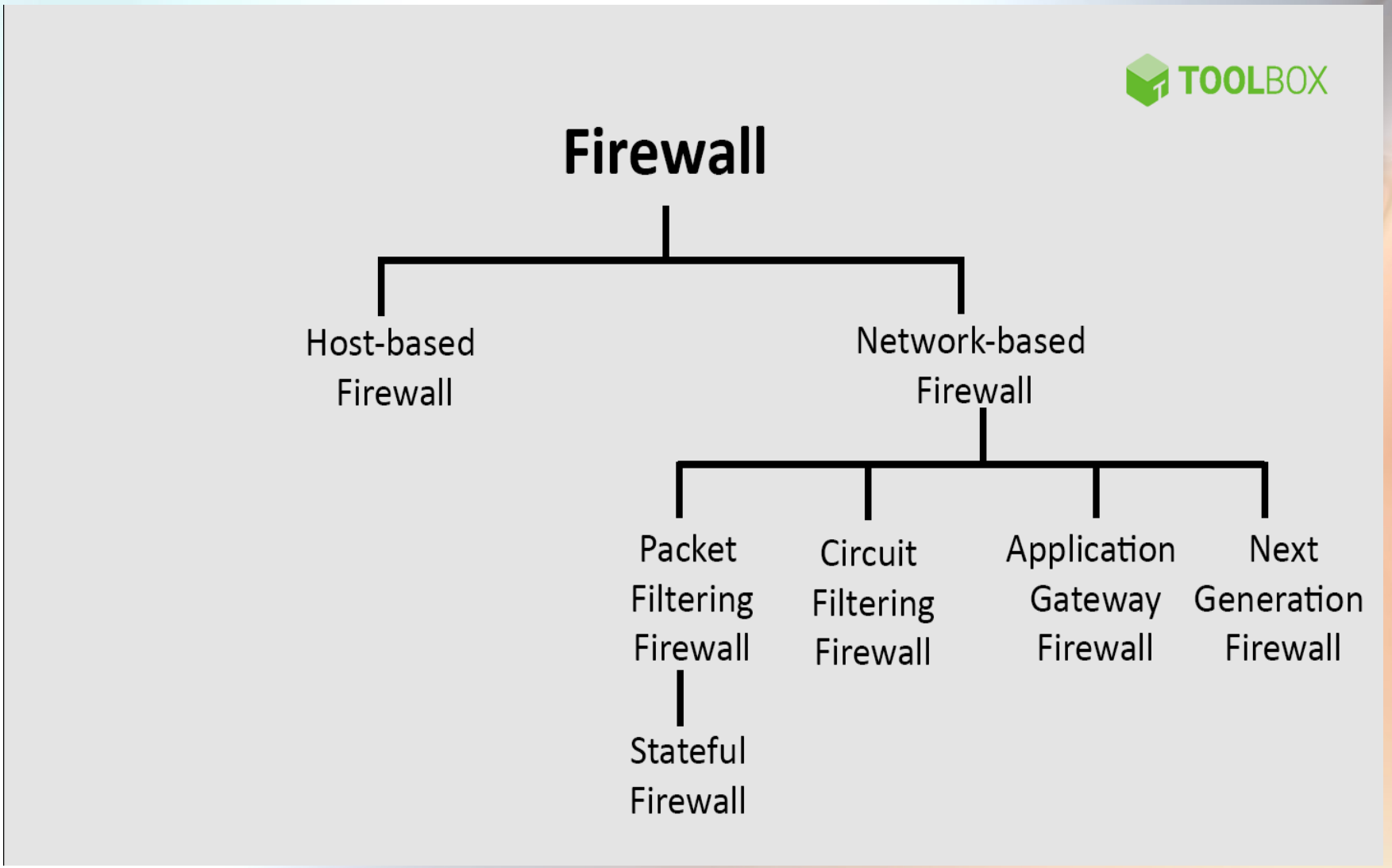
Physical Security

- Physical security means implementing access controls so only authorized personnel have access to areas where network equipment is located.
- Each network component should have its own level of physical security.
- Two important areas of concern are network cabling and network devices.
- Network cables should be secured behind walls.
- Network devices such as hubs and switches should be secured in locked wiring closets.

Network Firewalls

- Firewalls are used to prevent intruders on the Internet from making unauthorized access and denial of service attacks to your network.
- A firewall is a router/gateway, or special purpose computer that examines packets flowing into and out of the organization's network (usually via the Internet or corporate Intranet), restricting access to that network.
- The two main types of network firewalls are packet-level firewalls and application-level firewalls.

Firewall Classification



Packet-Level Firewalls

A packet-level firewall (or packet filter) examines the source and destination address of packets that pass through it, only allowing packets that have acceptable addresses to pass.

Packet filtering firewall advantages

- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive
- Minimal effect on resources, network performance and end-user experience

Packet filtering firewall disadvantages

- Because traffic filtering is based entirely on IP address, packet filtering lacks broader context that informs other types of firewalls
- Doesn't check the payload and can be spoofed (unless it performs SPI as well)
- Not an ideal option for every network
- Access control lists can be difficult to set up and manage

Circuit-Level Firewalls

A packet-level firewall (or packet filter) examines the source and destination address of packets that pass through it, only allowing packets that have acceptable addresses to pass.

Packet filtering firewall advantages

- A single device can filter traffic for the entire network
- Extremely fast and efficient in scanning traffic
- Inexpensive
- Minimal effect on resources, network performance and end-user experience

Packet filtering firewall disadvantages

- Because traffic filtering is based entirely on IP address, packet filtering lacks broader context that informs other types of firewalls
- Doesn't check the payload and can be spoofed (unless it performs SPI as well)
- Not an ideal option for every network
- Access control lists can be difficult to set up and manage

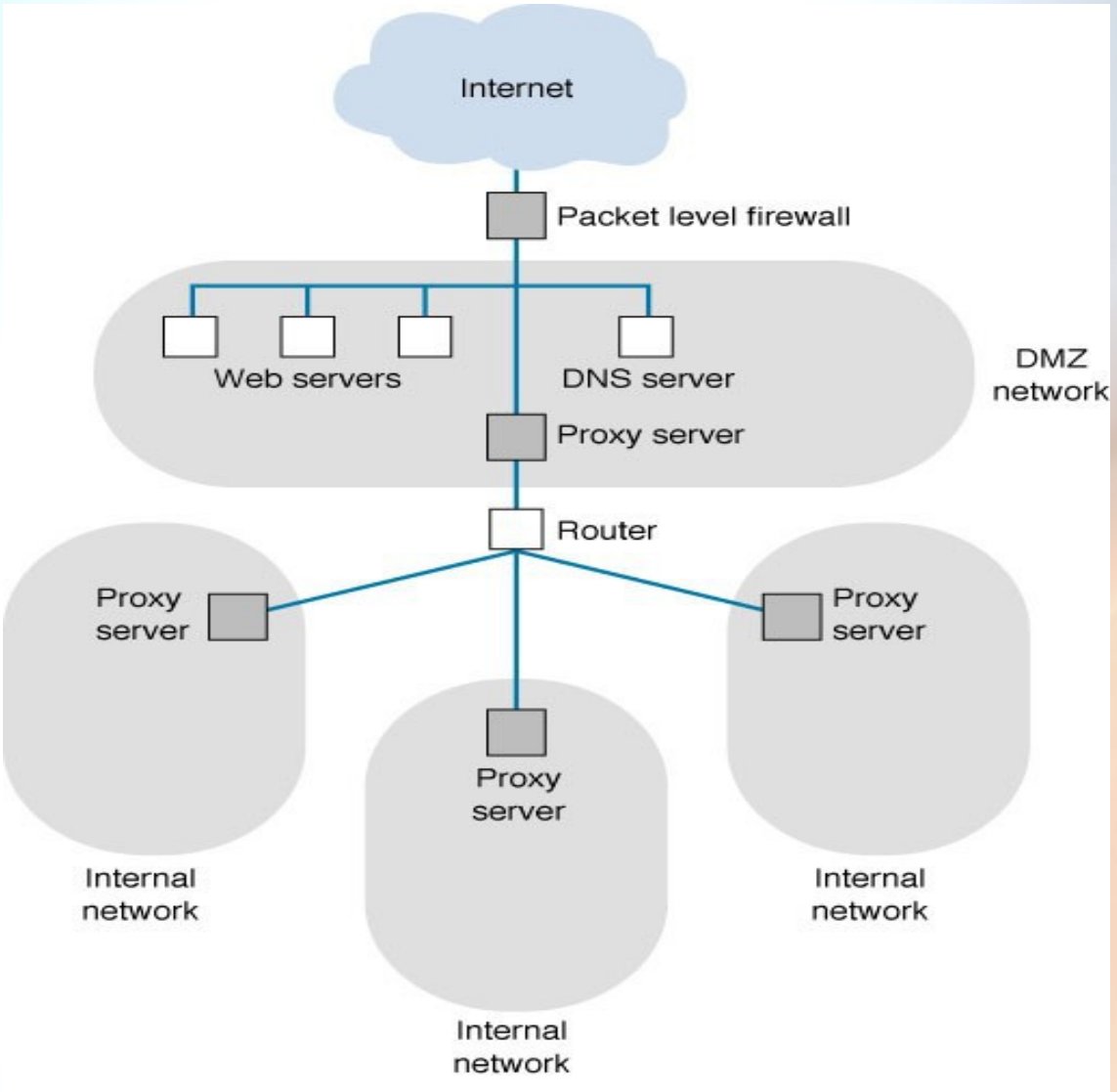
Application-Level Firewalls

- An application-level firewall or application gateway acts as an intermediate host computer, separating a private network from the rest of the Internet, but it works on specific applications, such as Web site access.
- The application gateway acts as an intermediary between the outside client making the request and the destination server responding to that request, hiding individual computers on the network behind the firewall.
- Because of the increased complexity of what they do, application level firewalls require more processing power than packet filters which can impact network performance.

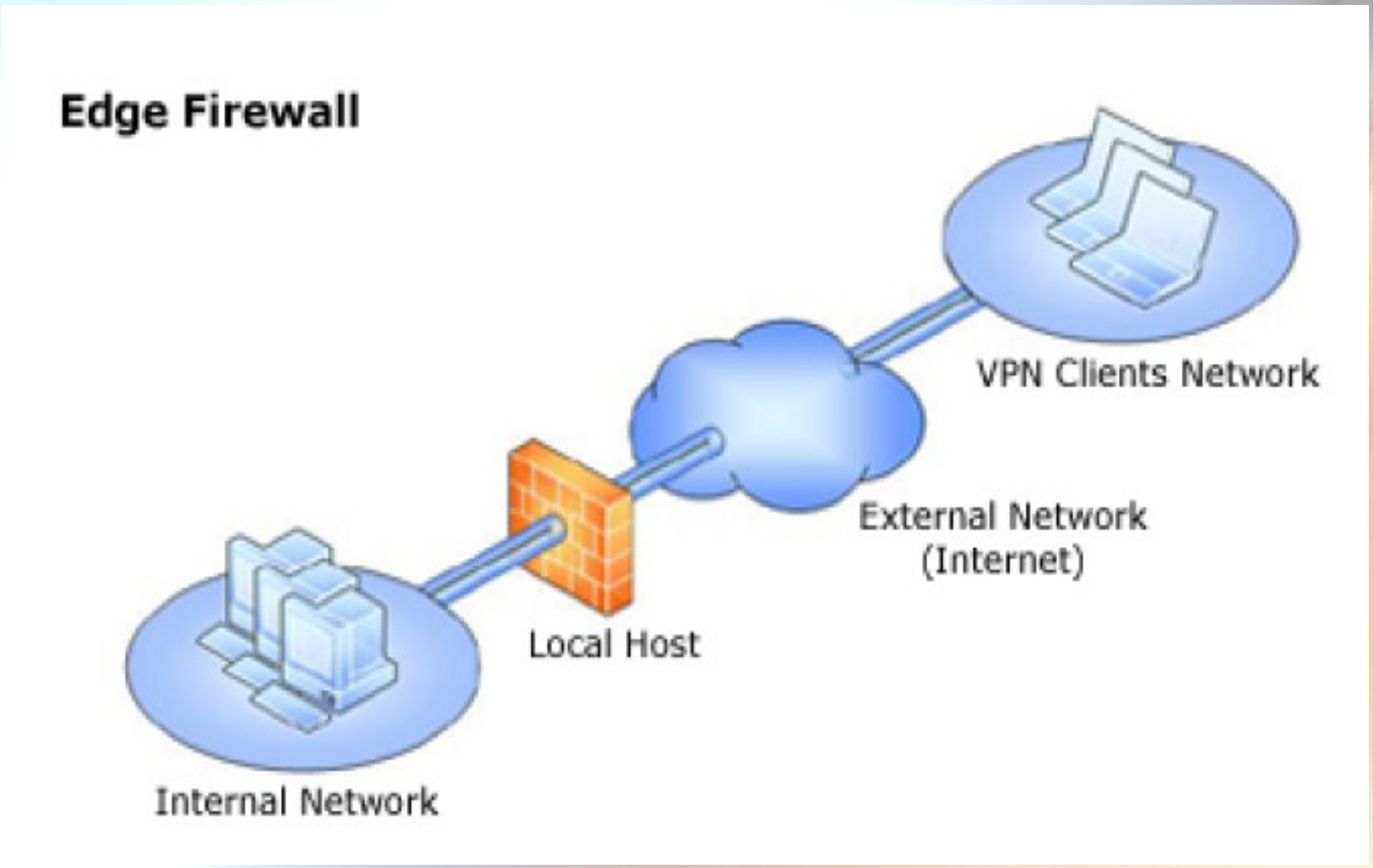
Network Address Translation

- Network address translation (NAT) is used to shield a private network from outside interference.
- An NAT uses an address table, translating network addresses inside the organization into aliases for use on the Internet. So, internal IP addresses remain hidden.
- Many organizations combine NAT servers, packet filters and application gateways, maintaining their online resources in a "DMZ network" between the two.

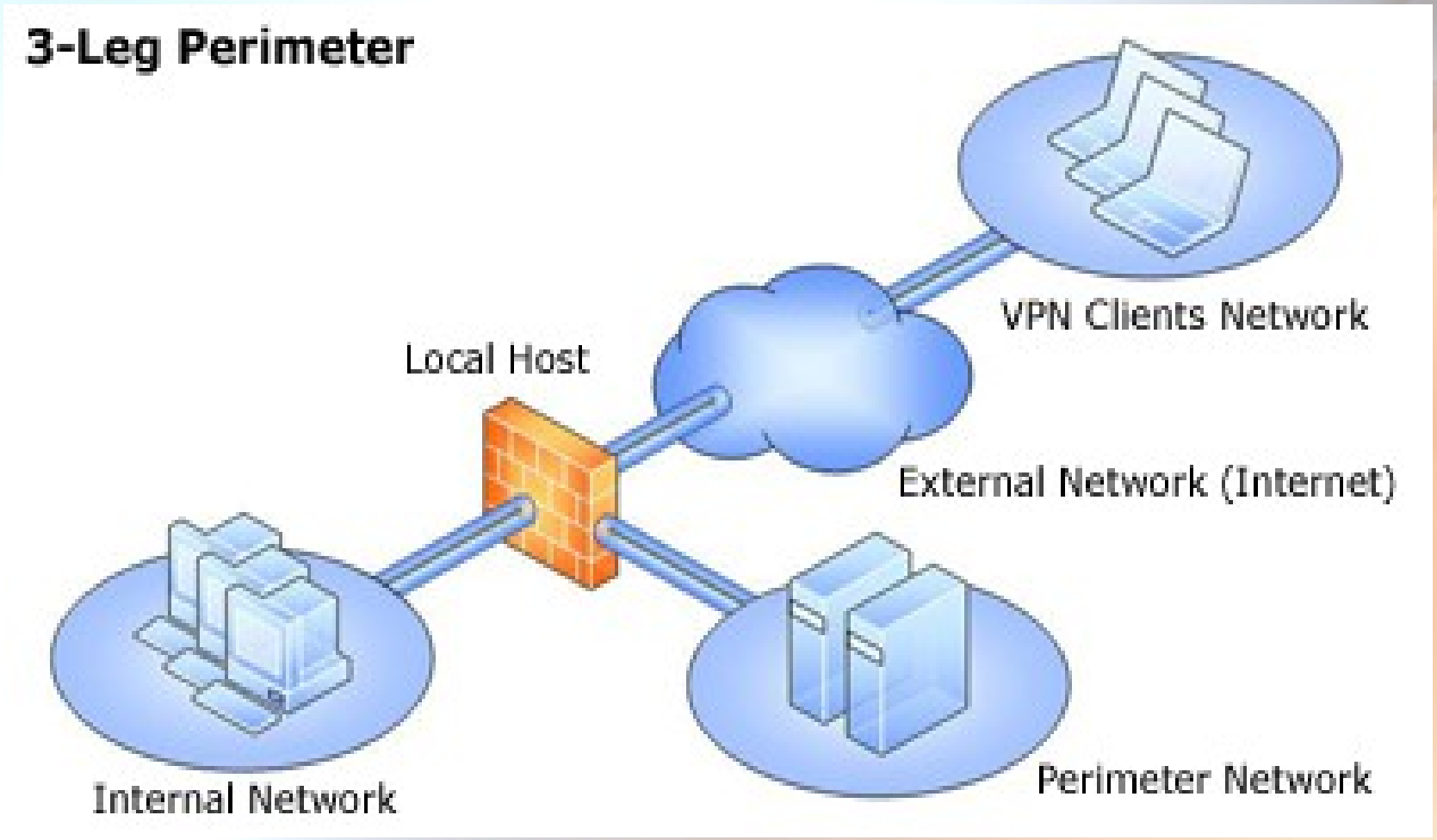
Typical network layout



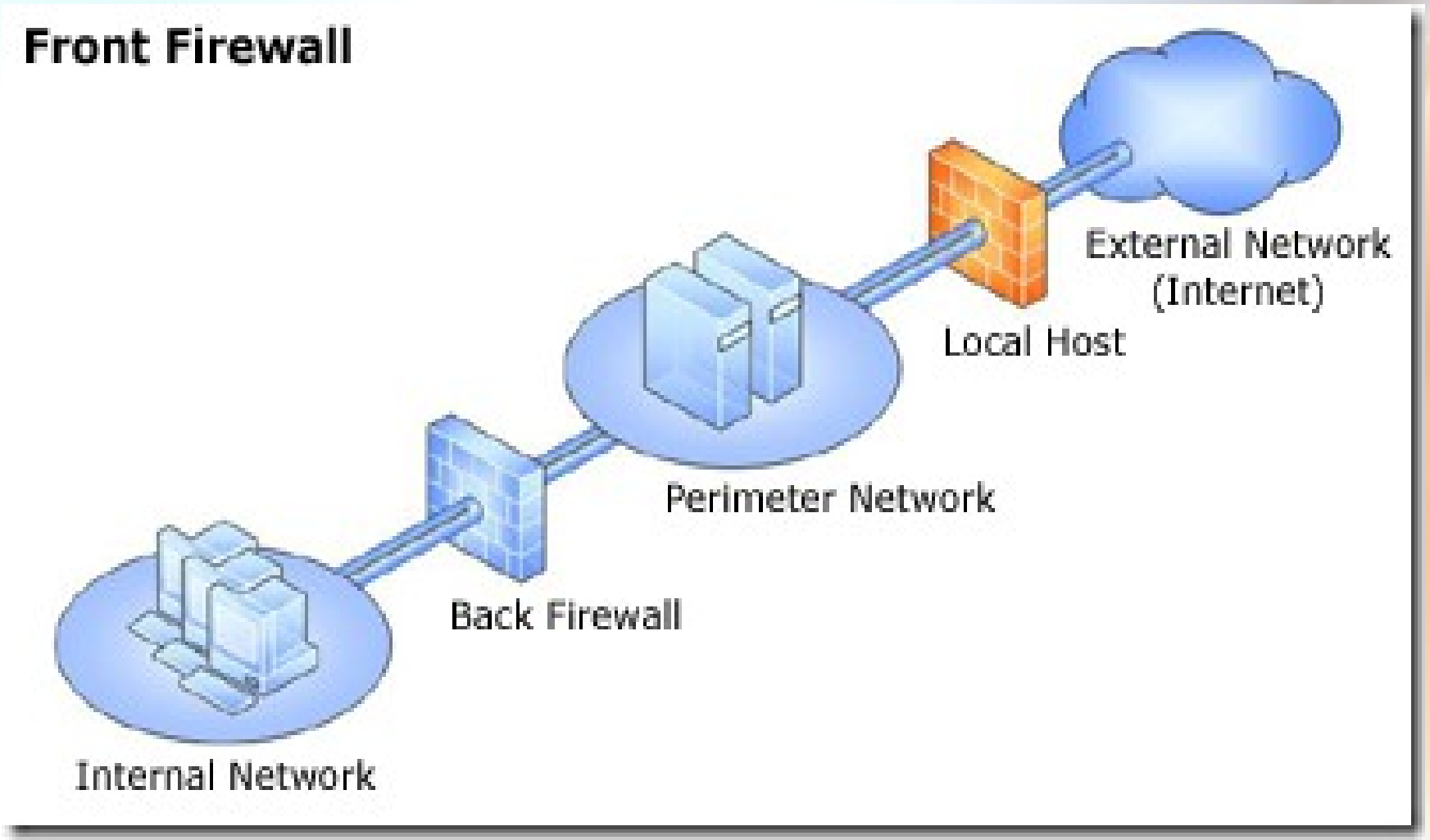
Network Template 1



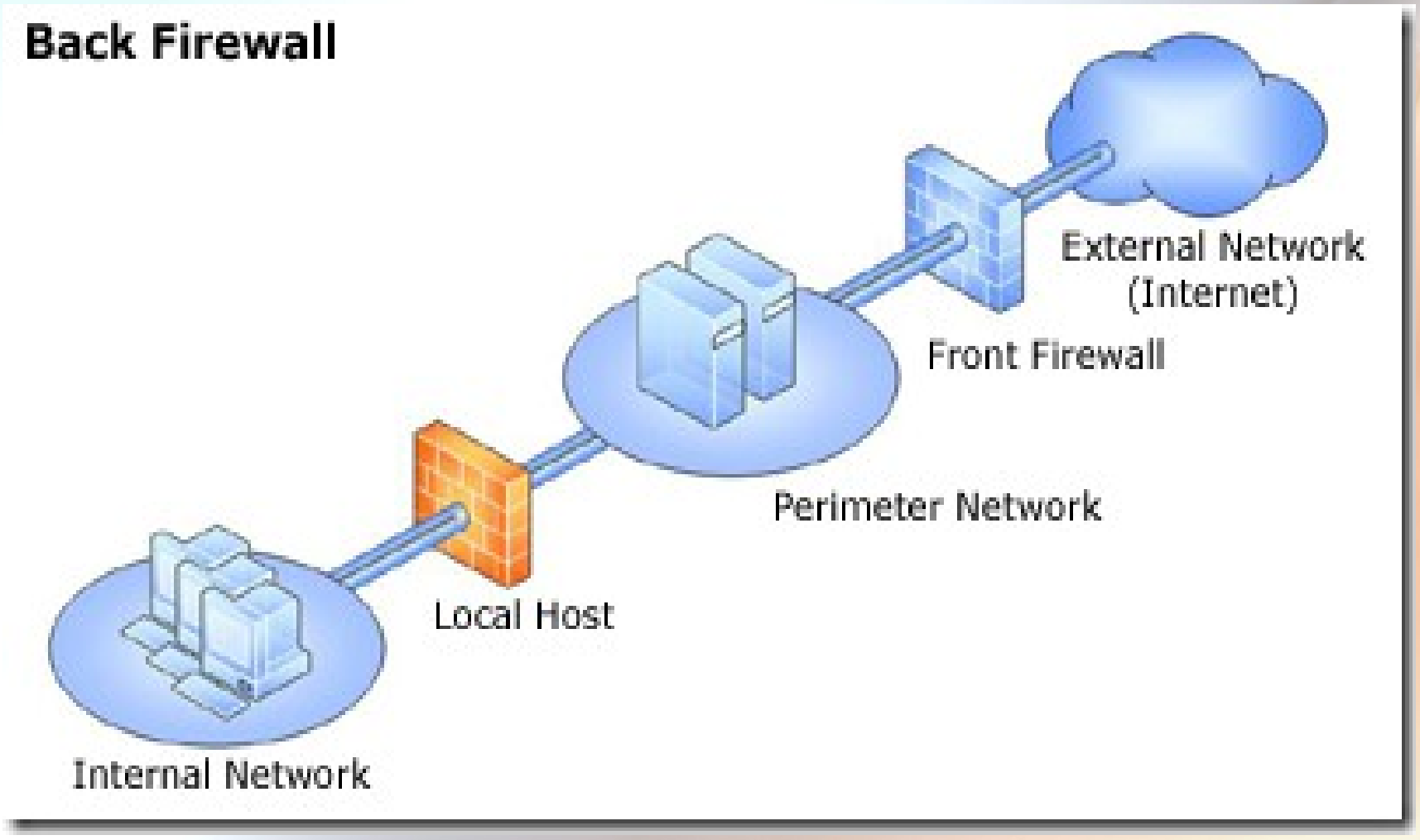
Network Template 2



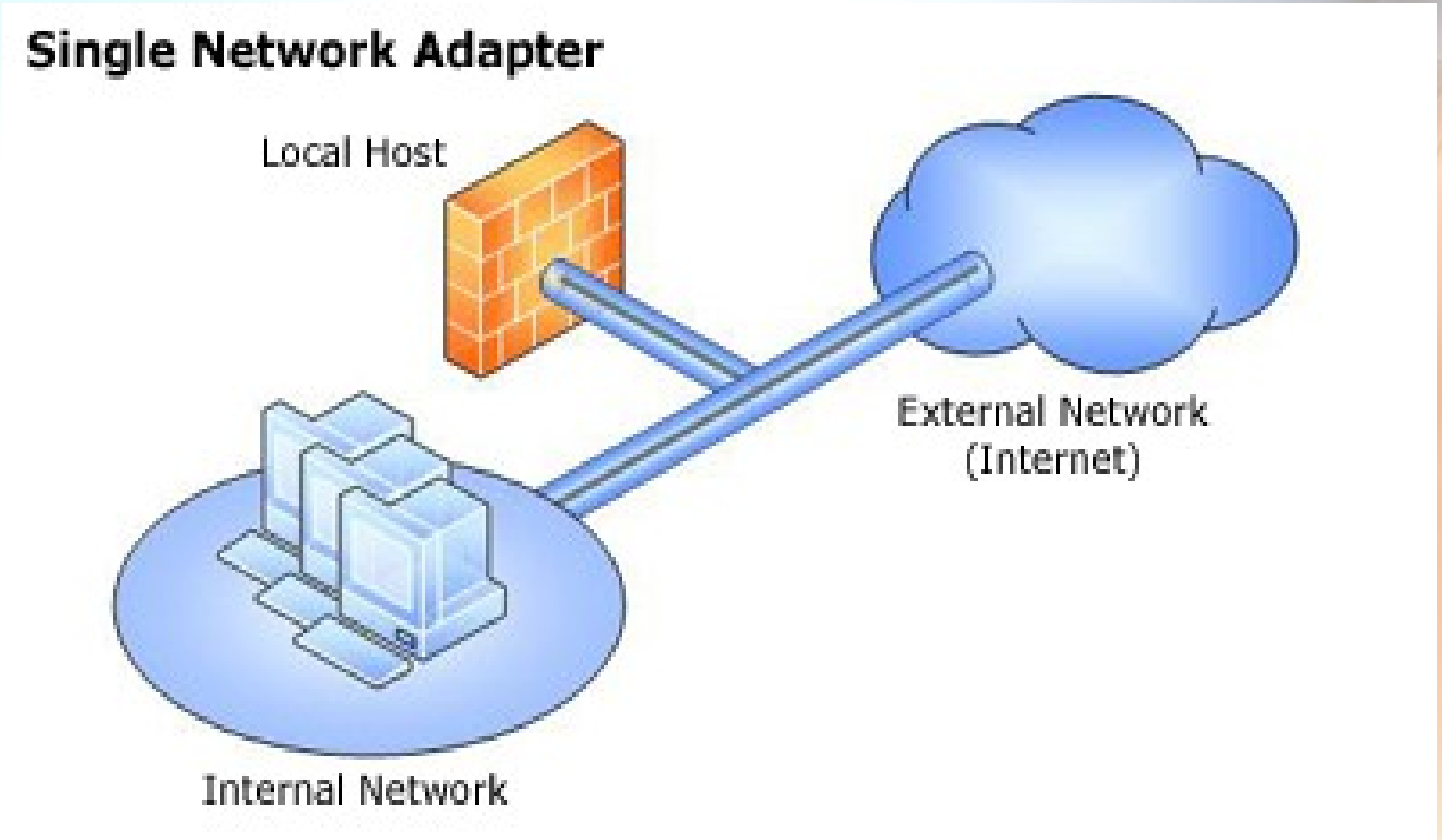
Network Template 3



Network Template 4



Network Template 5



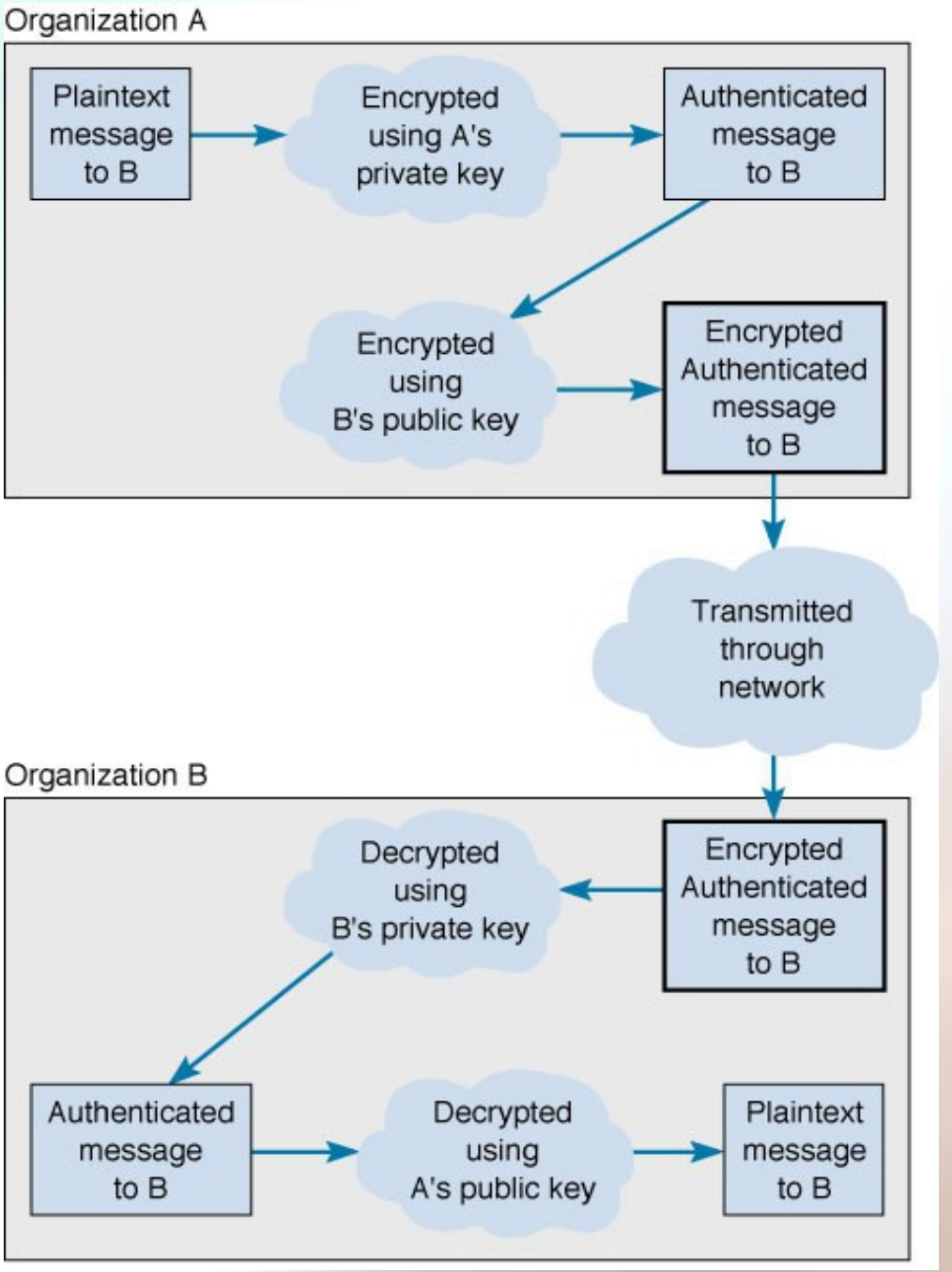
Security Holes

- Security holes are made by flaws in network software that permit unintended access to the network. Operating systems often contain security holes, the details of which can be highly technical.
- Once discovered, knowledge about the security hole may be quickly circulated on the Internet.
- A race can then begin between hackers attempting to break into networks through the security hole and security teams working to produce a patch to eliminate the security hole.

Digital Signatures

- PKE also permits authentication (digital signatures), which essentially uses PKE in reverse. The digital signature, is a small part of the message, and includes the name of the sender and other key contents.
- The digital signature in the outgoing message is encrypted using the sender's private key
- The digital signature is then decrypted using the sender's public key thus providing evidence that the message originated from the sender.
- Digital signatures and public key encryption combine to provide secure and authenticated message transmission

Digital Signatures



Certificate Authorities (CA)

- One problem with digital signatures involves verifying that the person sending the message is really who he or she says they are.
- A **certificate authority (CA)** is a trusted organization that can vouch for the authenticity of the person of organization using authentication.
- The CA sends out a digital certificate verifying the identity of a digital signature's source.
- For higher level security certification, the CA requires that a unique "fingerprint" (key) be issued by the CA for every message sent by the user.