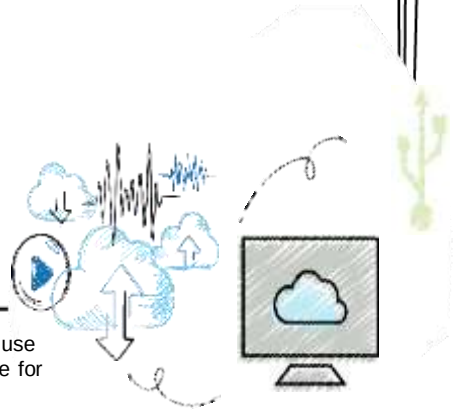
CompTIA Security+ Guide to Network Security Fundamentals, Sixth Edition

Chapter 6

Network Security Devices, Design, and Technology



Objectives

6.1 List the different types of network security devices and how they can be used

6.2 Describe secure network architectures

6.3 Explain how network technologies can enhance security

Security Through Network Devices

- Security can be achieved through using the security features found in standard networking devices
  - As well as hardware designed primarily for security

Standard Network Devices

- Standard network devices can be classified by the OSI layer at which they function
- OSI model breaks networking steps into seven layers
  - Each layer has different networking tasks
  - Each layer cooperates with adjacent layers
- Security functions of network devices can provide a degree of network security
  - Improperly configured standard network devices can introduce vulnerabilities
- Some devices include:
  - Bridges, switches, routers, load balancers, and proxies

Bridges (1 of 2)

- Bridges
  - Hardware device or software that is used to join two separate computer networks to enable communication between them
  - Can connect two local area networks (LANs) or two network segments (subnets)
  - Operate at the Data Link layer (Layer 2) so all networks or segments connected must use the same Layer 2 protocol (such as Ethernet)
  - Most OSs allow for a software bridge to connect two network segments
  - Creating a software bridge could create a security vulnerability

Bridges (2 of 2)

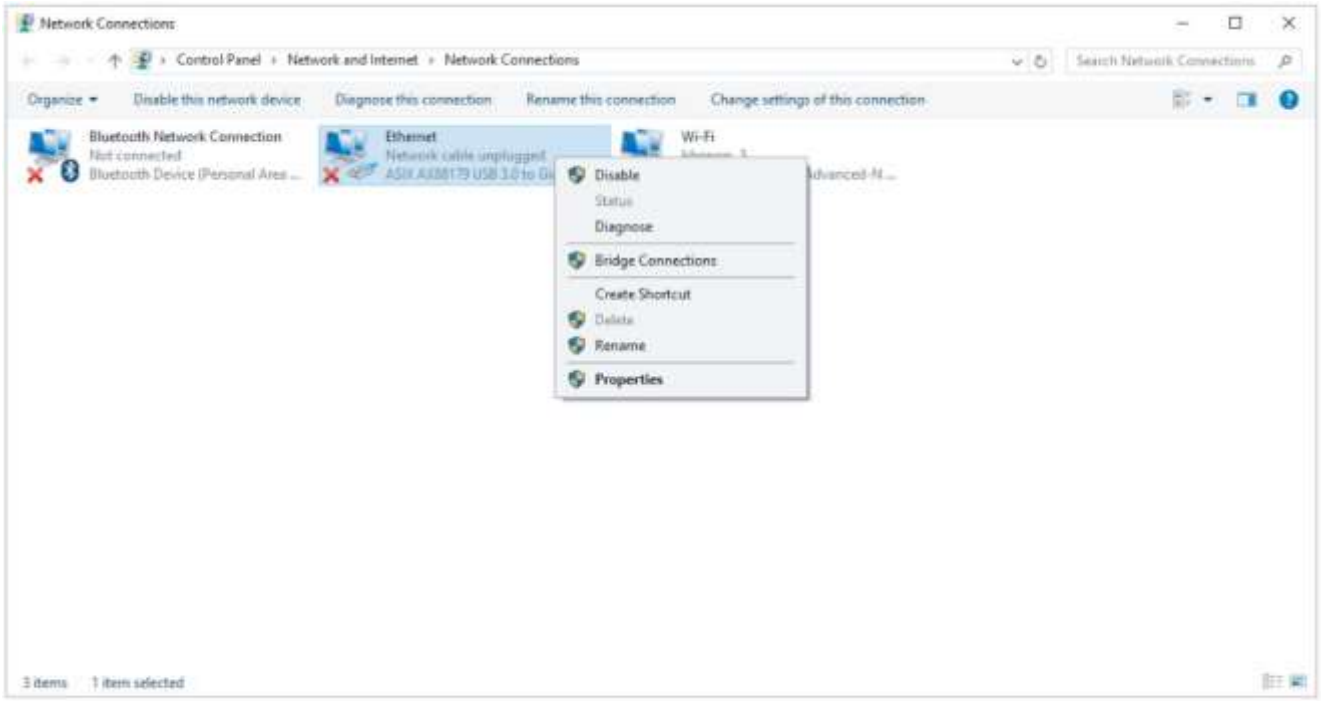


Figure 6-1 Microsoft Windows software network bridge

Switches (1 of 3)

- Switches
  - A device that connects network hosts intelligently
  - Can learn which device is connected to each of its ports
  - Examines the MAC address of frames that it receives and associates its port with the MAC address of the device connected to that port
    - Stores addresses in a MAC address table
  - Forwards frames intended for a specific device (unicast) instead of sending it out all ports (broadcast)
  - Important for switches to be properly configured to provide a high degree of security
  - Proper configuration includes loop prevention, and providing a flood guard

Switches (2 of 3)

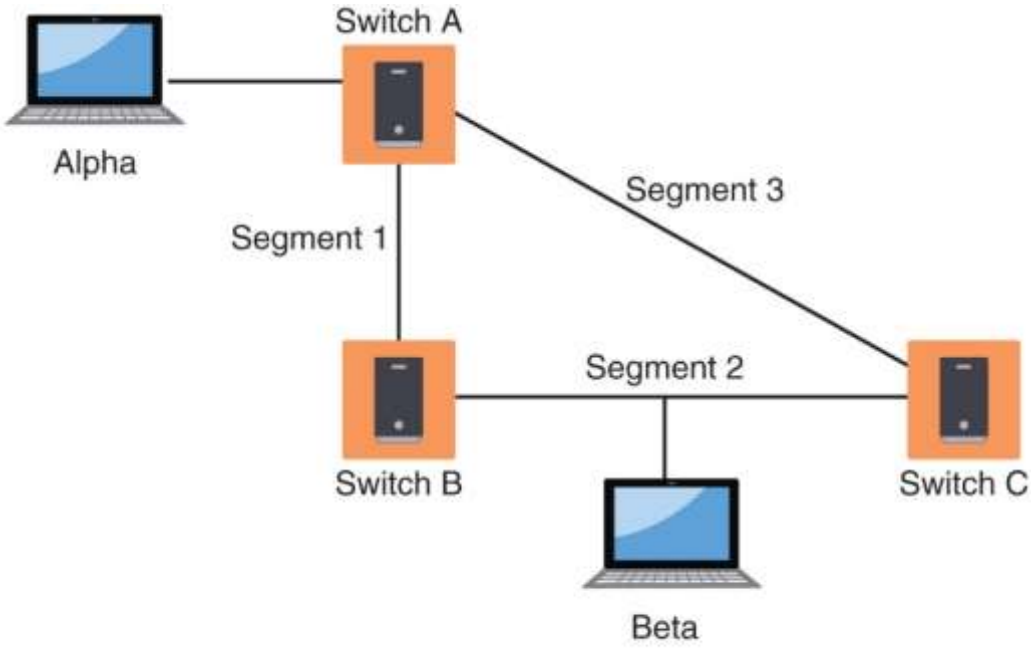


Figure 6-2 Broadcast storm

Switches (3 of 3)

- Flood Guard
  - A threat agent may attempt a MAC flooding attack by overflowing the switch with Ethernet frames that have been spoofed so that each frame contains a different source MAC address
  - The defense against a MAC flooding attack is a flood guard (port security)
  - Switches that support port security can be configured to limit the number of MAC addresses that can be learned on ports

Routers

- Routers
  - Forward packets across different computer networks
  - Operate at Network Layer (Layer 3)
  - Can be set to filter out specific types of network traffic by using an Access Control List (ACL)
  - Can also be used to limit traffic entering the network from unapproved networks
- Load balancers
  - Help evenly distribute work across a network
  - Allocate requests among multiple devices

Load Balancers (1 of 2)

- Load balancers
  - Help evenly distribute work across a network
  - Allocate requests among multiple devices
- Advantages of load-balancing technology
  - Reduces probability of overloading a single server
  - Optimizes bandwidth of network computers

Load Balancers (2 of 2)

- Load balancing is achieved through software or hardware device (load balancer)
- Load balancers are grouped into two categories:
  - **Layer 4 load balancers** - act upon data found in Network and Transport layer protocols
  - **Layer 7 load balancers** - distribute requests based on data found in Application layer protocols
- Different scheduling protocols used in load balancers:
  - Round-robin
  - Affinity
  - Other

Proxies (1 of 3)

- Proxies - there are several types of proxies used in computer networking
  - Forward proxy - a computer or an application program that intercepts user requests from the internal network and processes that request on behalf of the user
  - Application/multipurpose proxy - a special proxy server that “knows” the application protocols that it supports
  - Reverse proxy – routes requests coming from an external network to the correct internal server
  - Transparent proxy – does not require any configuration on the user’s computer

Proxies (2 of 3)

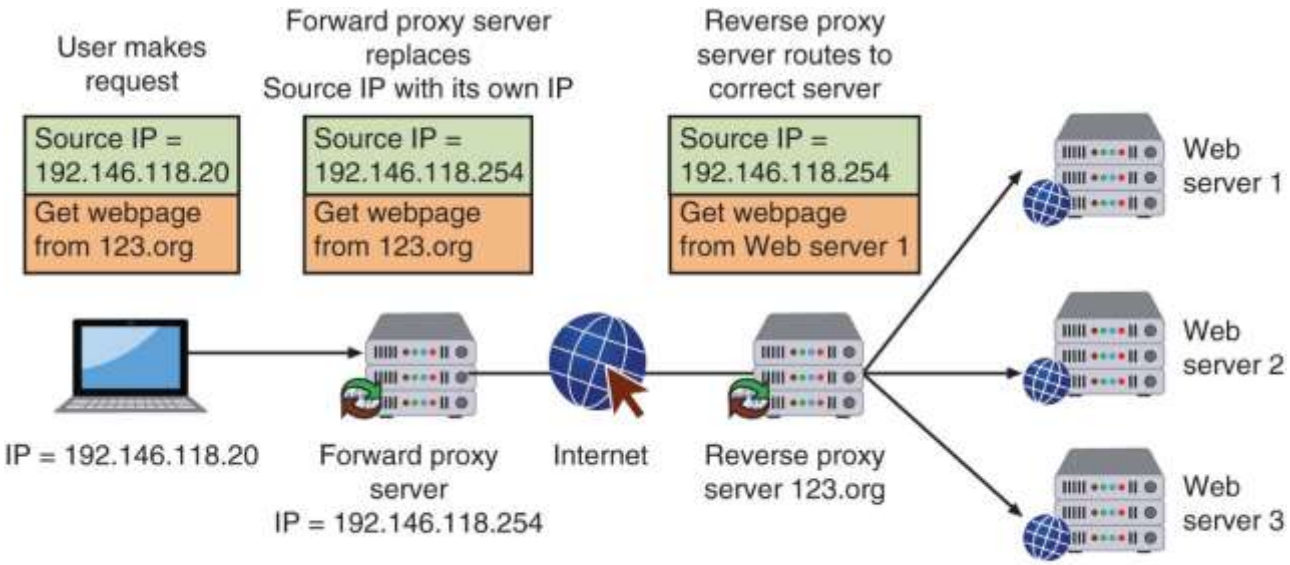


Figure 6-3 Forward and reverse proxy servers

Proxies (3 of 3)

- Advantages of proxy servers:
  - Increased speed
  - Reduced costs
  - Improved management
  - Stronger security

Network Security Hardware

- Specifically designed security hardware devices
  - Provide greater protection than standard networking devices
- Firewalls
  - Can be software-based or hardware-based
  - Both types inspect packets and either accept or deny entry
  - Hardware firewalls tend to be more expensive and more difficult to configure and manage
  - Software firewalls running on a device provide protection to that device only
  - All modern OSs include a software firewall, usually called a host-based firewall

Firewalls (1 of 3)

Figure 6-5 Enterprise hardware firewall

Source: https://www.juniper.net/assets/img/products/image-library/srx-series/srx3400/srx3400-frontwtop-high.

Firewalls (2 of 3)

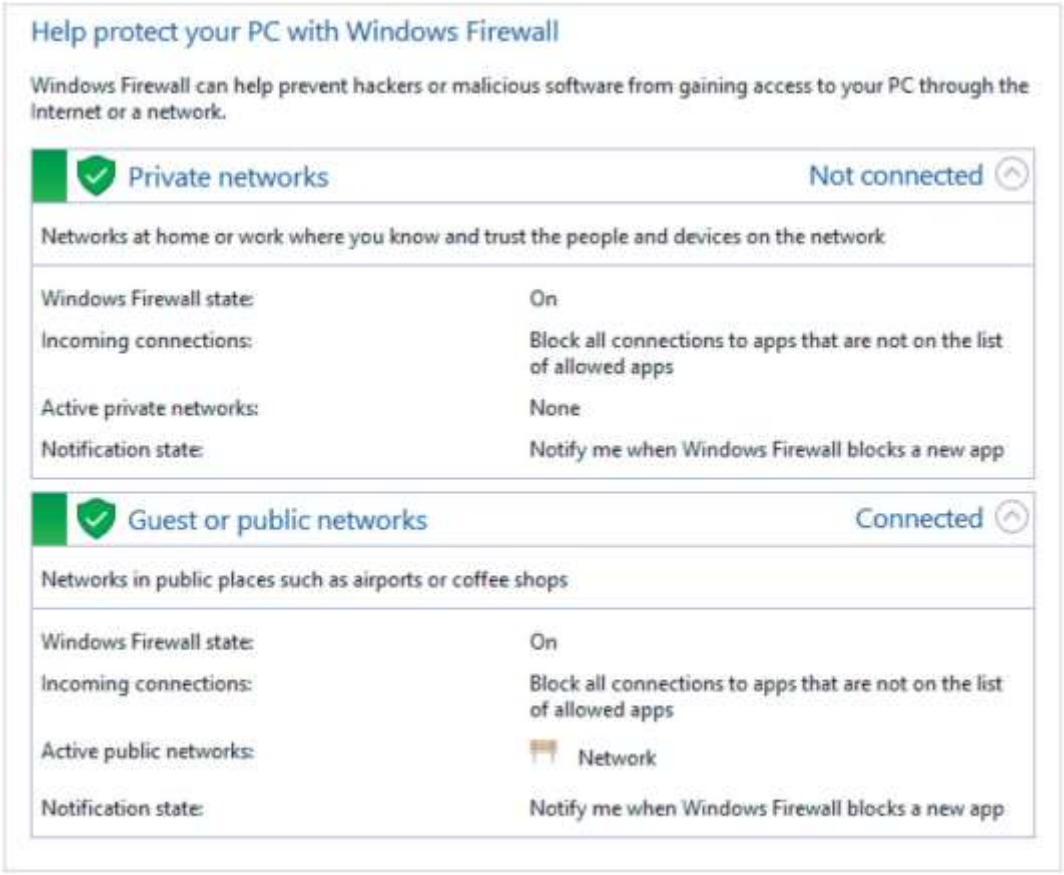


Figure 6-6 Windows personal firewall settings

Firewalls (3 of 3)

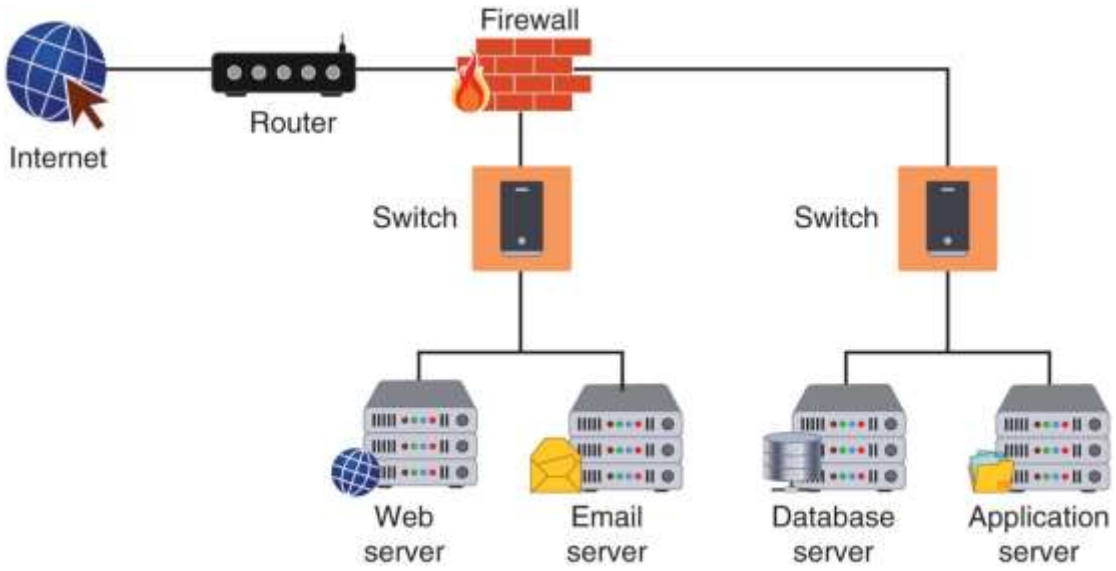


Figure 6-7 Network firewall

Network-Based Firewalls (1 of 2)

- Methods of firewall packet filtering
  - **Stateless packet filtering**
    - Inspects incoming packet and permits or denies based on conditions set by administrator
  - **Stateful packet filtering**
    - Keeps a record of the state of a connection
    - Makes decisions based on the connection and conditions
- Firewall actions on a packet
  - **Allow** (let packet pass through)
  - **Drop** (prevent the packet from passing into the network and send no response to sender)
  - **Reject** (prevent the packet from passing into the network but send a message to the sender)

Network-Based Firewalls (2 of 2)

- Rule-based firewalls
  - Use a set of individual instructions to control actions
- Each rule is a separate instruction processed in sequence telling the firewall what action to take
- Rules are stored together in one or more text file(s) that are read when the firewall starts
- Rule-based systems are static in nature
  - Cannot do anything other than what they have been configured to do

Application-Based Firewalls

- Application-Aware Firewalls
  - Operate at a higher level by identifying applications that send packets through the firewall and make decisions about actions to take
- Applications can be identified by application-based firewalls through:
  - Predefined application signatures
  - Header inspection
  - Payload analysis
- Web application firewall
  - Special type of application-aware firewall that looks deeply into packets that carry HTTP traffic
  - Can block specific sites or specific types of HTTP traffic

Virtual Private Network (VPN) Concentrator (1 of 2)

- **Virtual private network (VPN)** - enables authorized users to use an unsecured public network as if it were a secure private network
  - All data transmitted between remote device and network is encrypted
- Types of VPNs
  - **Remote-access VPN** - a user-to-LAN connection
  - **Site-to-site** - multiple sites can connect to other sites over the Internet
  - **Always-on VPNs** – allow the user to always stay connected
- Endpoints
  - The end of the tunnel between VPN devices
  - May be software on local computer or a VPN concentrator

Virtual Private Network (VPN) Concentrator (2 of 2)

- **VPN concentrator** - a dedicated hardware device that aggregates hundreds or thousands of VPN connections
- When using a VPN, there are two options:
  - All traffic is sent to the VPN concentrator and protected (called a full tunnel)
  - Only some traffic is routed over the secure VPN, while other traffic directly accesses the Internet (called split tunneling)

Mail Gateway

- There are two different email systems in use:
  - One system uses two TCP/IP protocols to send and receive messages: Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP/POP3)
  - IMAP (Internet Mail Access Protocol) is a more recent and advanced email system
    - With IMAP, email remains on the email server and is not downloaded to a user's computer
- Mail gateway
  - Monitors emails for unwanted content and prevents these messages from being delivered
- For inbound emails, a mail gateway can search for various types of:
  - Malware, spam, and phishing attacks
- For outbound email, a mail gateway can detect and block the transmission of sensitive data

CENGAGE

Network Intrusion Detection and Prevention (1 of 5)

- Intrusion detection system (IDS)
  - Can detect attack as it occurs
- Inline IDS
  - Connected directly to the network and monitors the flow of data as it occurs
- Passive IDS
  - Connected to a port on a switch, which receives a copy of network traffic
- IDS systems can be managed:
  - In-band – through the network itself by using network protocols and tools
  - Out-of-band – using an independent and dedicated channel to reach the device

Network Intrusion Detection and Prevention (2 of 5)

Function	Inline	Passive
Connection	Directly to network	Connected to port on switch
Traffic flow	Routed through the device	Receives copy of traffic
Blocking	Can block attacks	Cannot block attacks
Detection error	May disrupt service	May cause false alarm

Network Intrusion Detection and Prevention (3 of 5)

- Monitoring methodologies
  - Anomaly-based monitoring
    - Compares current detected behavior with baseline
  - Signature-based monitoring
    - Looks for well-known attack signature patterns
  - Behavior-based monitoring
    - Detects abnormal actions by processes or programs
    - Alerts user who decides whether to allow or block activity
  - Heuristic monitoring
    - Uses experience-based techniques

Network Intrusion Detection and Prevention (4 of 5)

- Types of IDS - two basic types if IDS exist
- Host intrusion detection system (HIDS)
  - A software-based application that can detect an attack as it occurs
  - Installed on each system needing protection
  - Monitors:
    - System calls and file system access
    - Can recognize unauthorized Registry modification
    - Host input and output communications
      - Detects anomalous activity
- Disadvantages of HIDS
  - Cannot monitor network traffic that does not reach local system
  - All log data is stored locally
  - Resource-intensive and can slow system

Network Intrusion Detection and Prevention (5 of 5)

- Network intrusion detection system (NIDS)
  - Watches for attacks on the network
  - NIDS sensors installed on firewalls and routers:
    - Gather information and report back to central device
  - NIDS can sound an alarm and log events
- Application-aware IDS
  - A specialized IDS
  - Uses “contextual knowledge” in real time
  - It can know the version of the OS or which application is running
    - As well as what vulnerabilities are present in the systems being protected

Intrusion Prevention Systems (IPSs)

- Intrusion Prevention System (IPS)
  - Monitors network traffic to immediately block a malicious attack
  - Similar to NIDS
  - NIPS is located “in line” on the firewall
  - Allows the NIPS to more quickly take action to block an attack
- Application-aware IPS
  - Knows which applications are running as well as the underlying OS

Security and Information Event Management (SIEM) (1 of 3)

- Security and Information Event Management (SIEM) product
  - A SIEM consolidates real-time monitoring and management of security information
  - Analyzes and reports on security events
- A SIEM product can be:
  - A separate device
  - Software that runs on a computer
  - A service that is provided by a third party

Security and Information Event Management (SIEM) (2 of 3)

Figure 6-8 SIEM dashboard

https://cdn.alienvault.com/images/uploads/home/screen1

Security and Information Event Management (SIEM) (3 of 3)

- A SIEM typically has the following features:
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event duplication
  - SIEM logs

Other Network Security Hardware Devices (1 of 2)

Name	Description	Comments
Hardware security module	A dedicated cryptographic processor that provides protection for cryptographic keys	A tamper-resistant device that can securely manage, process, and store cryptographic keys
SSL decryptor	A separate device that decrypts SSL traffic	Helps reduce performance degradation and eliminates the need to have multiple decryption licenses spread across multiple devices
SSL/TLS accelerator	A separate hardware card that inserts into a web server that contains one or more co-processors to handle SSL/TLS processing	Used to accelerate the computationally intensive initial SSL connection handshake, during which keys are generated for symmetric encryption using 3 DES or AES
Media gateway	A device that converts media data from one format to another	Sometimes called a **softswitch**, converts data in audio or video format

Other Network Security Hardware Devices (2 of 2)

Name	Description	Comments
Unified Threat Management (UTM)	Integrated device that combines several security functions	Multipurpose security appliance that provides an array of security functions, such as antispam, antiphishing, antispyware, encryption, intrusion protection, and web filtering
Internet content filter	Monitors Internet traffic and block access to preselected websites and files	Restricts unapproved websites based on URL or by searching for and matching keywords such as **sex** or **hate** as well as looking for malware
Web security gateway	Blocks malicious content in real time as it appears without first knowing the URL of a dangerous site	Enables a higher level of defense by examining the content through application-level filtering

Security Through Network Architecture

- The design of a network can provide a secure foundation for resisting attackers
- Elements of a secure network architectural design include:
  - Creating security zones
  - Using network segregation

Security Zones

- A secure approach is to create zones to partition the network
  - So that certain users may enter one zone while access is prohibited to other users
- The most common security zones:
  - Demilitarized zones
  - Using network address translation to create zones

Demilitarized Zone (DMZ)

- DMZ - a separate network located outside secure network perimeter
- Untrusted outside users can access DMZ but not secure network

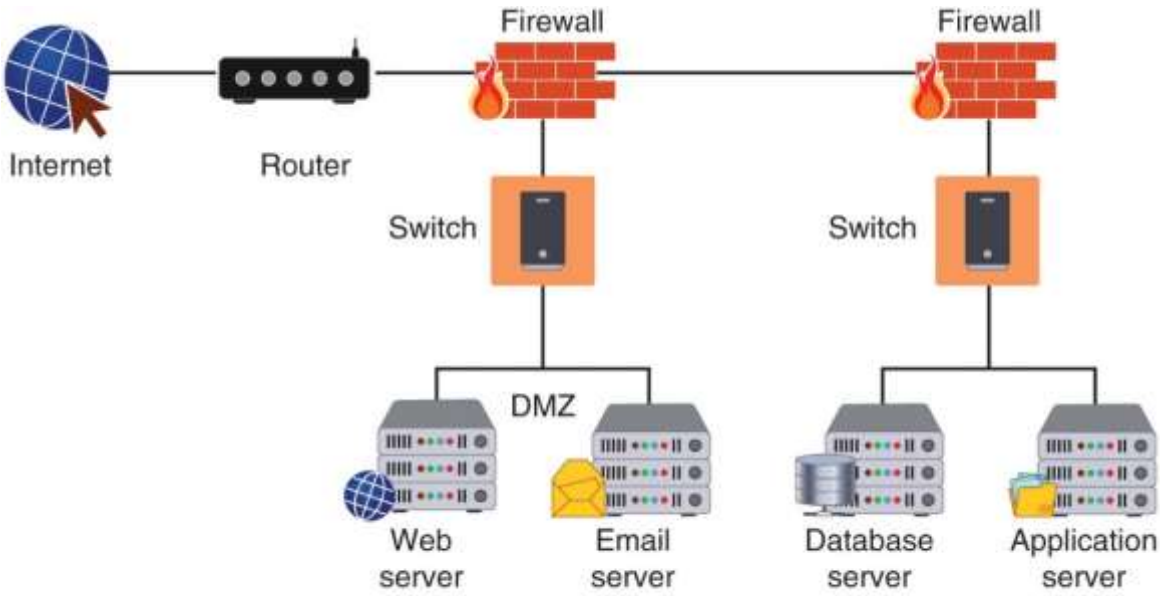


Figure 6-9 DMZ with two firewalls

Network Address Translation (NAT) (1 of 2)

- Network address translation (NAT)
  - Allows private IP addresses to be used on the public Internet
  - Replaces private IP address with public address
- Advantage of NAT
  - Masks IP addresses of internal devices
  - An attacker who captures the packet on the Internet cannot determine the actual IP address of sender

Network Address Translation (NAT) (2 of 2)

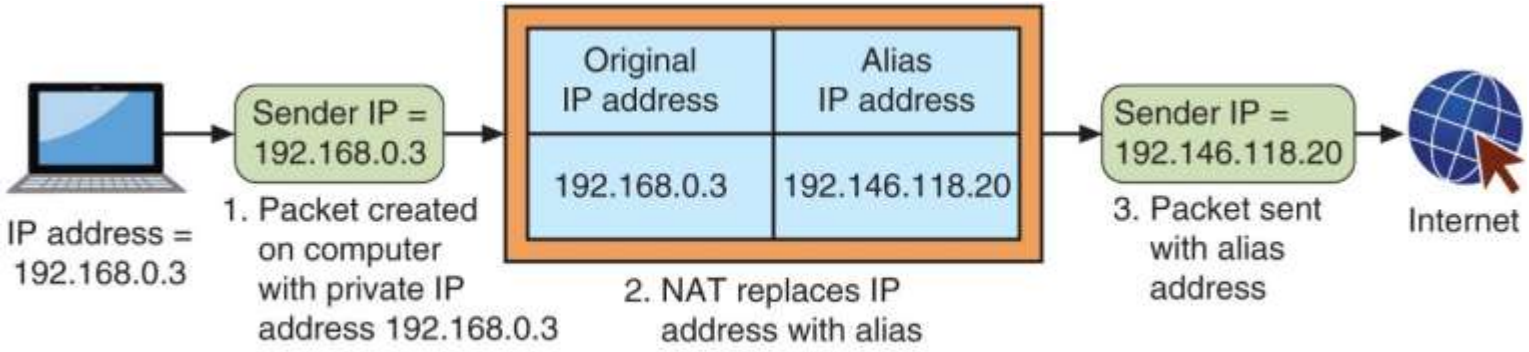


Figure 6-10 Network address translation (NAT)

Other Zones

Name	Description	Security benefits
Intranet	A private network that belongs to an organization that can only be accessed by approved internal users	Closed to the outside public, thus data is less vulnerable to external threat actors
Extranet	A private network that can be access by authorized external customers, vendors, and partners	Can provide enhanced security for outside users compared to a publicly accessible website
Guest network	A separate open network that anyone can access without prior authorization	Permits access to general network resources like web surfing without using the secure network

Network Segregation (1 of 2)

- Physical network segregation
  - Isolates the network so that it is not accessible by outsiders
- Air gap
  - The absence of any type of connection between devices
  - In this case the secure network and another network
- Networks can be segmented using switches to divide the network into a hierarchy
  - Core switches reside at the top of the hierarchy and carry traffic between switches
  - Workgroup switches are connected directly to the devices on the network

Network Segregation (2 of 2)

- Virtual LAN (VLAN)
  - Allow scattered users to be logically grouped together
  - Even if attached to different switches
- Can isolate sensitive data to VLAN members
- Communication on a VLAN
  - If connected to same switch, switch handles packet transfer
  - A special “tagging” protocol is used for communicating between switches

Security Through Network Technologies

- Two technologies that can help secure a network:
  - Network access control
  - Data loss prevention

Network Access Control (NAC) (1 of 3)

- NAC
  - Examines the current state of a system or network device before it can connect to the network
  - Any device that does not meet a specified set of criteria can connect only to a “quarantine” network where the security deficiencies are corrected
- Goal of NAC
  - To prevent computers with suboptimal security from potentially infecting other computers through the network

Network Access Control (NAC) (2 of 3)

- NAC uses software “agents” to gather information and report back (host agent health checks)
- An agent may be a:
  - Permanent NAC agent
  - Dissolvable NAC agent – disappears after reporting information to the NAC
- NAC technology can be embedded within a Microsoft Windows Active Directory domain controller
  - NAC uses AD to scan the device (called agentless NAC)

Network Access Control (NAC) (3 of 3)

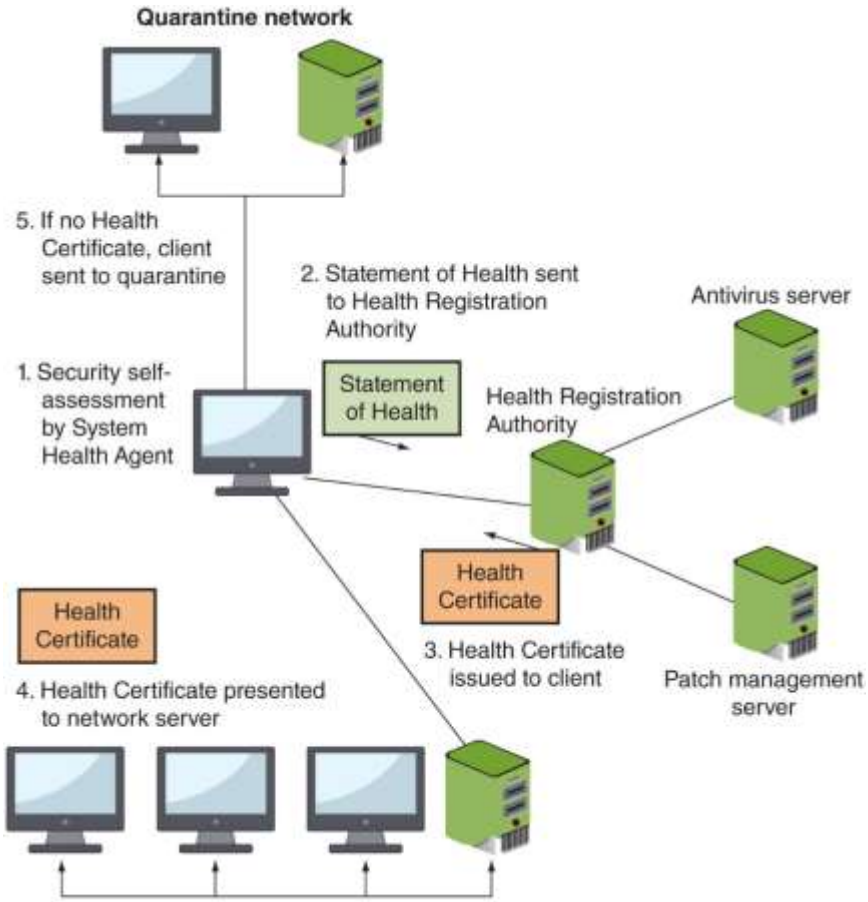


Figure 6-11 Network access control (NAC) framework

Data Loss Prevention (DLP) (1 of 3)

- DLP
  - A system of security tools that is used to recognize and identify data that is critical to the organization
  - Ensures that it is protected
- Two common uses of DLP
  - Monitoring emails through a mail gateway
  - Blocking the copying of files to a USB flash drive (USB blocking)
- Most DLP systems use **content inspection**
  - Defined as a security analysis of the transaction within its approved context

Data Loss Prevention (DLP) (2 of 3)

- Content inspection looks at not only the security level of data, but also:
  - Who is requesting it
  - Where the data is stored
  - When it was requested
  - Where it is going
- Three types of DLP sensors:
  - DLP network sensors
  - DLP storage sensors
  - DLP agent sensors

Data Loss Prevention (DLP) (3 of 3)

- When a policy violation is detected by the DLP agent
  - It is reported back to the DLP server
- Different actions can be taken:
  - Block the data
  - Redirect it to an individual who can examine the request
  - Quarantine the data until later
  - Alert a supervisor of the request

Chapter Summary (1 of 2)

- Standard network security devices provide a degree of security
  - Switches, router, load balancer, and proxies
- Hardware devices specifically designed for security give higher protection level
  - Hardware-based firewall, Web application firewall
- Virtual private networks (VPNs) use an unsecured public network and encryption to provide security
- A mail gateway monitors emails for unwanted content and prevents these messages from being delivered
- An intrusion detection system (IDS) is designed to detect an attack as it occurs

Chapter Summary (2 of 2)

- A Security and Information Event Management (SIEM) product consolidates real-time monitoring and management of security information along with an analysis and reporting of security events
- Other network security hardware devices include:
  - Hardware security modules, SSL decryptors, SSL/TLS accelerators, media gateways, UTM products, Internet content filters, and web security gateways
- Methods for designing a secure network
  - Demilitarized zones
  - Virtual LANs
- Network technologies can help secure a network
  - Network access control (NAC)