Chapter 9: Infrastructure Security

Security Appliances

Principle	Description
Gap analysis	A comparison of the organization’s current state of information security with recommended controls
Segmentation	Dividing a network into multiple subnets or segments with each acting as its own small network to improve monitoring and enhance security
Isolation	Keeping multiple instances of an attack surface separate so that each instance can only see and affect itself
Least privilege	Granting access that is limited to what is only necessary for a device or user to complete their work
Configuration enforcement	Applying security measures to reduce unnecessary vulnerabilities
Decommissioning	Removing or dismantling a technology or service from a live production
Removal of unnecessary software	Deleting software that is not essential to an operation in order to eliminate an attack vector
Selection of effective controls	Choosing productive safeguards or countermeasures to limit the exposure of an asset to a danger
Device placement	Physically locating important devices in secure locations

Common Network Devices

- A network **switch** is a device that connects network devices
  - A switch can learn which device is connected to each of its ports by examining the media access control (MAC) address of frames it receives
  - Proper hardening of a switch includes implementing port security and configuring other switch defenses
- A common attack against switches is a MAC flooding attack
- Switches that support **port security** can be configured to limit the number of MAC addresses that can be learned on ports

Common Network Devices

Type of attack	Description	Security defense
MAC flooding	An attacker can overflow the switch's address table with fake MAC addresses, forcing it to act like a hub, sending packets to all devices	Use a switch that can close ports with too many MAC addresses
MAC address spoofing	If two devices have the same MAC address, a switch may send frames to each device. An attacker can change the MAC address on their device to match the target device's MAC address	Configure the switch so that only one port can be assigned per MAC address
ARP poisoning	The attacker sends a forged ARP packet to the source device, substituting the attacker's computer MAC address	Use an ARP detection appliance
Port mirroring	An attacker connects their device to the switch's port	Secure the switch in a locked room

Common Network Devices

- A **router** is a network device that can forward frames across different computer networks
- Routers can also perform a security function by using an access control list (ACL)
  - An ACL is a set of permissions or rules that functions as a network filter to permit or restrict data flowing into and out of the router network interfaces
- Routers can protect against devices that imitate another computer’s IP address (this defense is called **antispoofing**)

Common Network Devices

- A **server** distributes resources and services to devices connected to the network
- The basic steps for hardening a server include the following:
  - Apply patches to vulnerabilities
  - Monitor the server
  - Control access permissions
  - Remove unnecessary software
  - Secure the server location

Common Network Devices

- Load balancing is a technology that can help to evenly distribute work across a network
  - It can be performed through software running on a computer or as a dedicated hardware device known as a load balancer
- The use of a load balancer has security advantages:
  - They can detect and stop attacks directed at a server or application
  - They can be used to detect and prevent protocol attacks
  - Some can hide HTTP error pages or remove server identification headers from HTTP responses

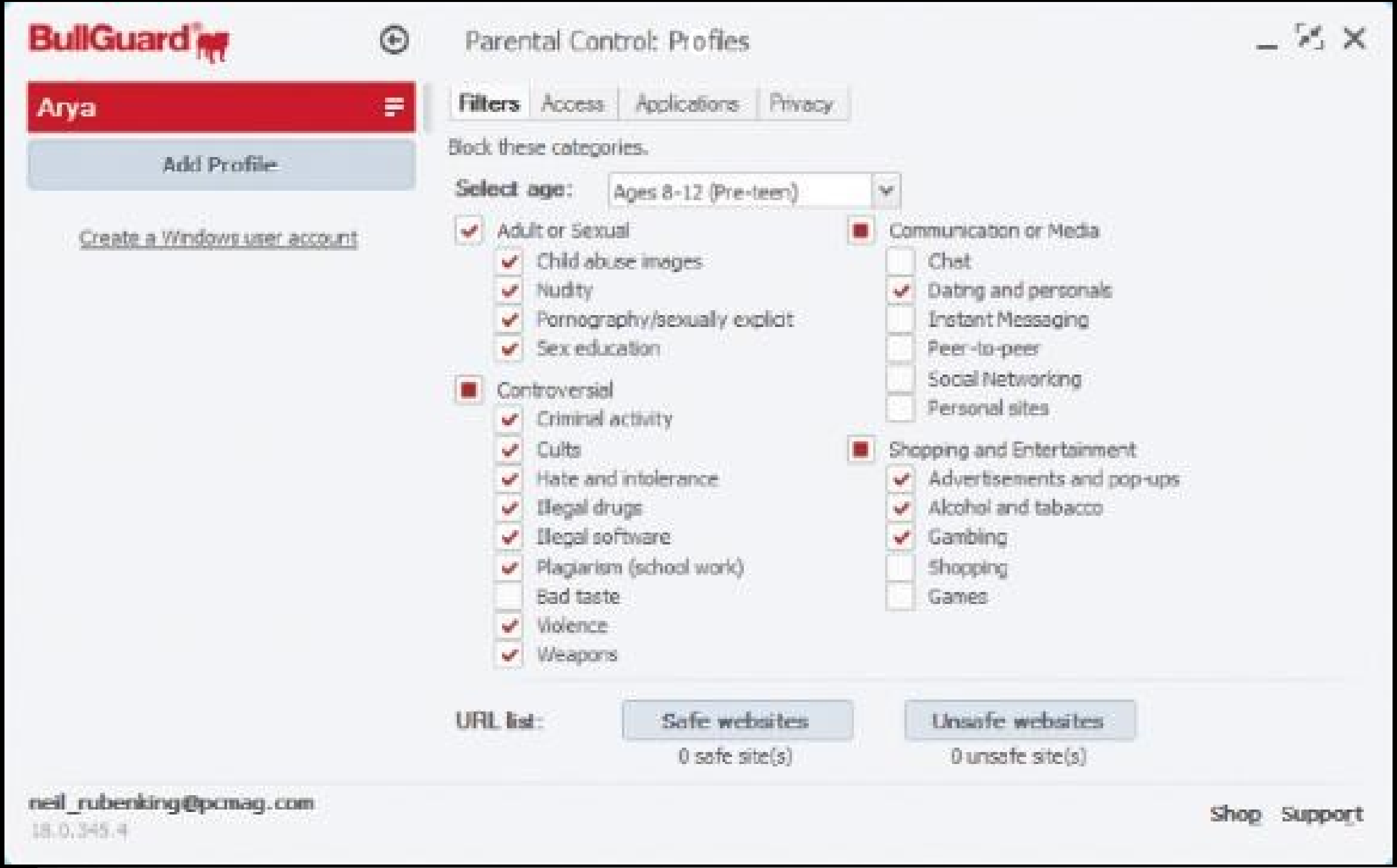
Infrastructure Security Hardware

- A **firewall** uses bidirectional inspection to examine outgoing and incoming packets
  - The actions are based on specific criteria or rules (called **rule-based firewalls**)
  - A more flexible type of firewall is a **policy-based firewall** which allows more generic statements instead of specific rules
  - Firewalls can also apply **content/URL filtering**

Infrastructure Security Hardware

Action	Description	Example	Comments
Allow	Explicitly allows traffic that matches the rule to pass	Permit incoming Address Resolution Protocol (ARP) traffic	Implicitly denies all other traffic unless explicitly allowed
Bypass	Allows traffic to bypass the firewall	Bypass based on IP, port, traffic direction, and protocol	Designed for media-intensive protocols or traffic from a trusted source
Deny	Explicitly blocks all traffic that matches the rule	Deny traffic from IP address	Generally drops the packet with no return message to the sender
Force Allow	Forcibly allows traffic that would normally be denied by other rules	Useful for determining if essential network services are able to communicate	Traffic will still be subject to inspection by other security appliances
Log Only	Traffic is logged but no other action is taken	Bypass rules do not generate log files but Log Only will	Occurs if the packet is not stopped by a Deny rule or an Allow rule that excludes it

Content/URL Filter



Block these categories.

Select age: Ages 8-12 (Pre-teen)

- ☑ Adult or Sexual
  - ☑ Child abuse images
  - ☑ Nudity
  - ☑ Pornography/sexually explicit
  - ☑ Sex education
- ■ Controversial
  - ☑ Criminal activity
  - ☑ Cults
  - ☑ Hate and intolerance
  - ☑ Illegal drugs
  - ☑ Illegal software
  - ☑ Plagiarism (school work)
  - □ Bad taste
  - ☑ Violence
  - ☑ Weapons
- ■ Communication or Media
  - □ Chat
  - ☑ Dating and personals
  - □ Instant Messaging
  - □ Peer-to-peer
  - □ Social Networking
  - □ Personal sites
- ■ Shopping and Entertainment
  - ☑ Advertisements and pop-ups
  - ☑ Alcohol and tabacco
  - ☑ Gambling
  - □ Shopping
  - □ Games

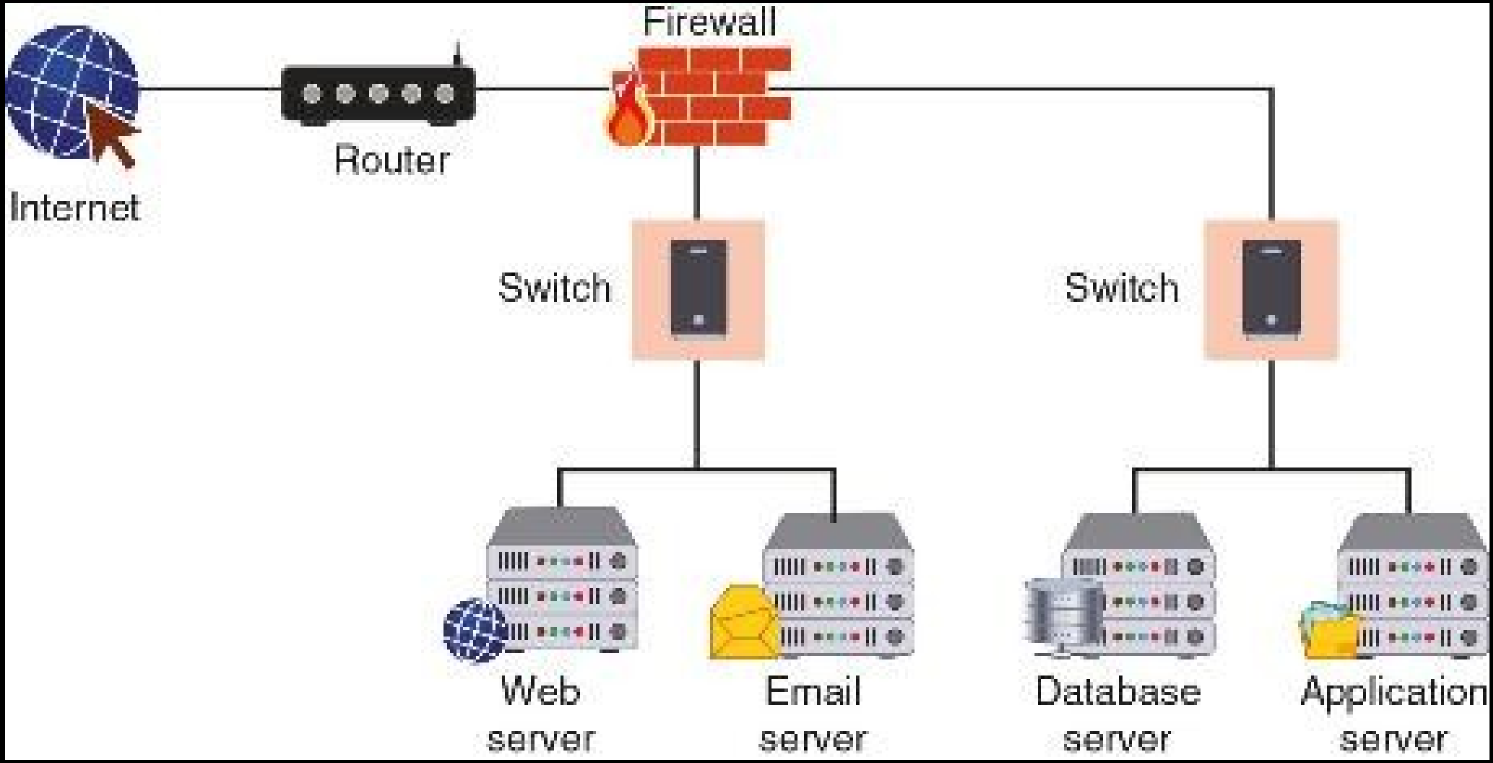
URL list: Safe websites: 0 safe site(s) | Unsafe websites: 0 unsafe site(s)

neil_rubenking@pcmag.com
18.0.345.4

Infrastructure Security Hardware

- The following are different categories of firewalls:
  - Hardware versus software
  - Host versus appliance versus virtual
  - Open source versus proprietary
  - Stateful versus stateless
  - Dedicated firewall versus network access control list (ACL)

Appliance Firewall



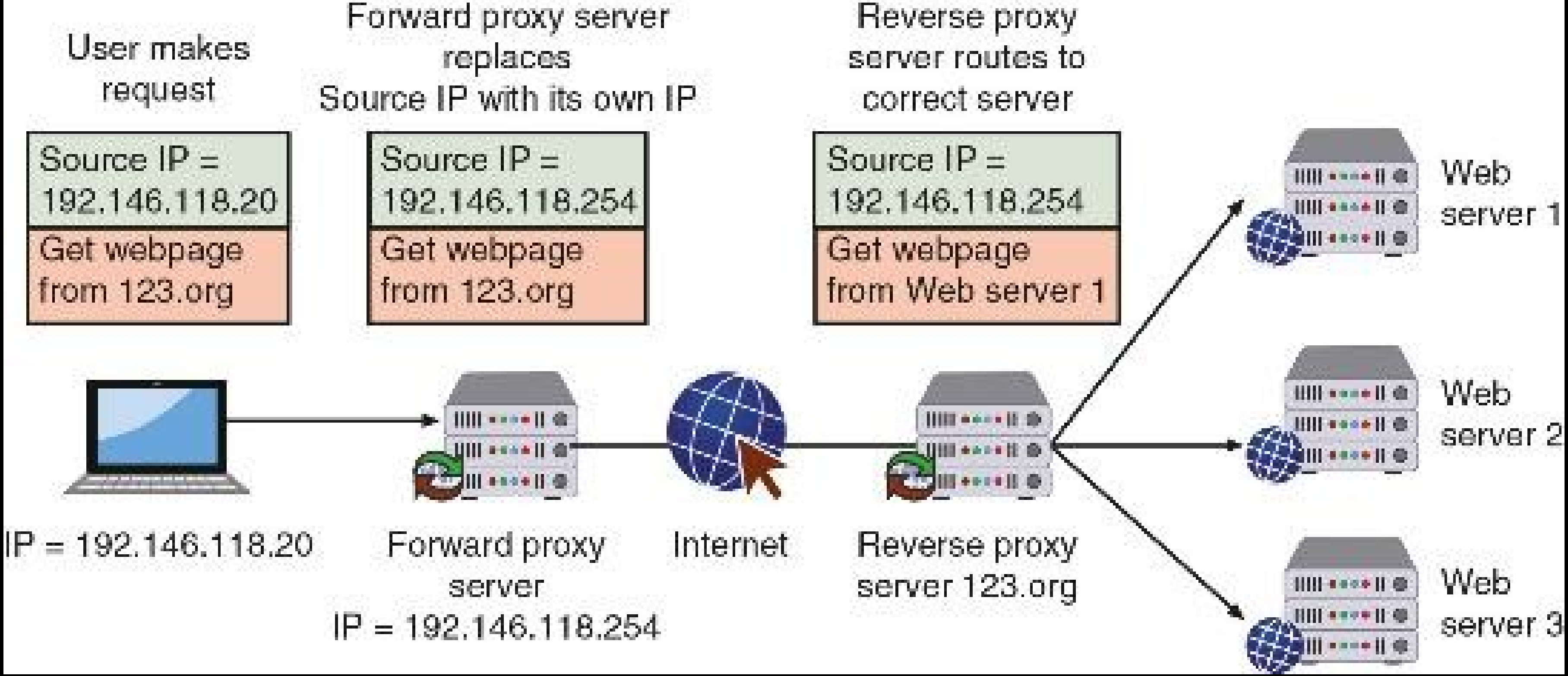
Infrastructure Security Hardware

- Several specialized firewall appliances include the following:
  - Web application firewall
  - Next-generation firewall
  - Unified threat management
  - Layer 7 firewall
  - Network address translation gateway

Infrastructure Security Hardware

- Proxy servers are devices that act as substitutes on behalf of the primary device
- A **forward proxy** is a computer or an application that intercepts user requests from the internal secure network and processes the requests on behalf of the user
- A **reverse proxy** routes requests coming from an external network to the correct internal server

Forward and Reverse Proxy Servers


User makes request
Forward proxy server replaces Source IP with its own IP
Reverse proxy server routes to correct server
Source IP = 192.146.118.20
Get webpage from 123.org
Source IP = 192.146.118.254
Get webpage from 123.org
Source IP = 192.146.118.254
Get webpage from Web server 1
Web server 1
Web server 2
Web server 3
IP = 192.146.118.20
Forward proxy server
IP = 192.146.118.254
Internet
Reverse proxy server 123.org

Infrastructure Security Hardware

- Deception can be used as a security defense: by directing threat actors away from a valuable asset to something that has little or no value
- A technology lure can serve as bait to threat actors
- A **honeypot** is a computer located in an area with limited security that serves as “bait” to threat actors
- Two goals of using a honeypot include the following:
  - *Deflect*
  - *Discover*

Infrastructure Security Hardware

- A **low-interaction honeypot** may only contain a login prompt
- A **high-interaction honeypot** is designed for capturing more information from the threat actor
- A **honeynet** is a network of honeypots set up with intentional vulnerabilities
- A **sinkhole** is a “bottomless pit” designed to steer unwanted traffic away from its intended destination to another device
  - The goal is to deceive the threat actor into thinking the attack was successful

Infrastructure Security Hardware

- An **intrusion detection system** (**IDS**) can detect an attack as it occurs
- An **intrusion prevention system** (**IPS**) attempts to block the attack
- An inline system is connected directly to the network and monitors the flow of data as it occurs
- A **passive system** is connected to a port on a switch, which receives a copy of network traffic
- The network-based systems are known as network intrusion detection systems (NIDS) and network intrusion prevention system (NIPS)

Question?

- Maya is researching information on firewalls. She needs a firewall that allows for more generic statements instead of creating specific rules. What type of firewall should Maya consider purchasing that supports her need?

Answer

- Maya is researching information on firewalls. She needs a firewall that allows for more generic statements instead of creating specific rules. What type of firewall should Maya consider purchasing that supports her need?
- Policy-based Firewall; A more flexible type of firewall than a rule-based firewall is a policy-based firewall. This type of firewall allows for more generic statements to be used instead of specific rules.
-

Software Security Protections

- **Web filtering** monitors the websites users are browsing so that the organization can either allow or block web traffic to protect against potential threats and enforce corporate policies
- The different types of web filtering software are based on the location of the filtering engine:
  - Browser scanning
  - Agent-based scanning
  - Centralized proxy scanning
  - Cloud scanning

Software Security Protections

- There are different methods that web filtering uses to identify malicious websites to create block rules, or criteria for which a website is inaccessible to users
    - Content categorization
    - Universal Resource Locator (URL) scanning
    - Reputation score

DNS Filtering

- **DNS filtering** blocks harmful or inappropriate content
  - Web filtering blocks webpages, DNS filtering blocks entire domains
- DNS resolvers can act as filters by refusing to resolve queries for certain domains
  - These malicious domains are found in a list of unapproved sites that a DNS can access

File Integrity Monitoring (FIM)

- File integrity monitoring (FIM) is a technology designed to “keep an eye on” files to detect any changes within the files that may indicate a cyberattack
- A problem with FIM is the high volume of “noise,” or too much unhelpful information

Extended Detection & Response

- Endpoint detection and response (EDR) tools monitor endpoint events by aggregating data from multiple endpoint computers to a centralized database
- **Extended detection and response** (**XDR**) collects and correlates data across various network appliances, including servers, email systems, cloud repositories, as well as endpoints

What is Secure Infrastructure Design?

- A network infrastructure should be designed with some areas for general access while other parts of the network having successively tighter restrictions
  - The most restricted level of all can be a network that has physical isolation from all other networks or the Internet (called an **air-gapped network**)
- Infrastructure separation can be achieved through **physical segmentation** and **logical segmentation**
  - Logical segmentation creates subnets via “virtual networks” or through network addressing schemes

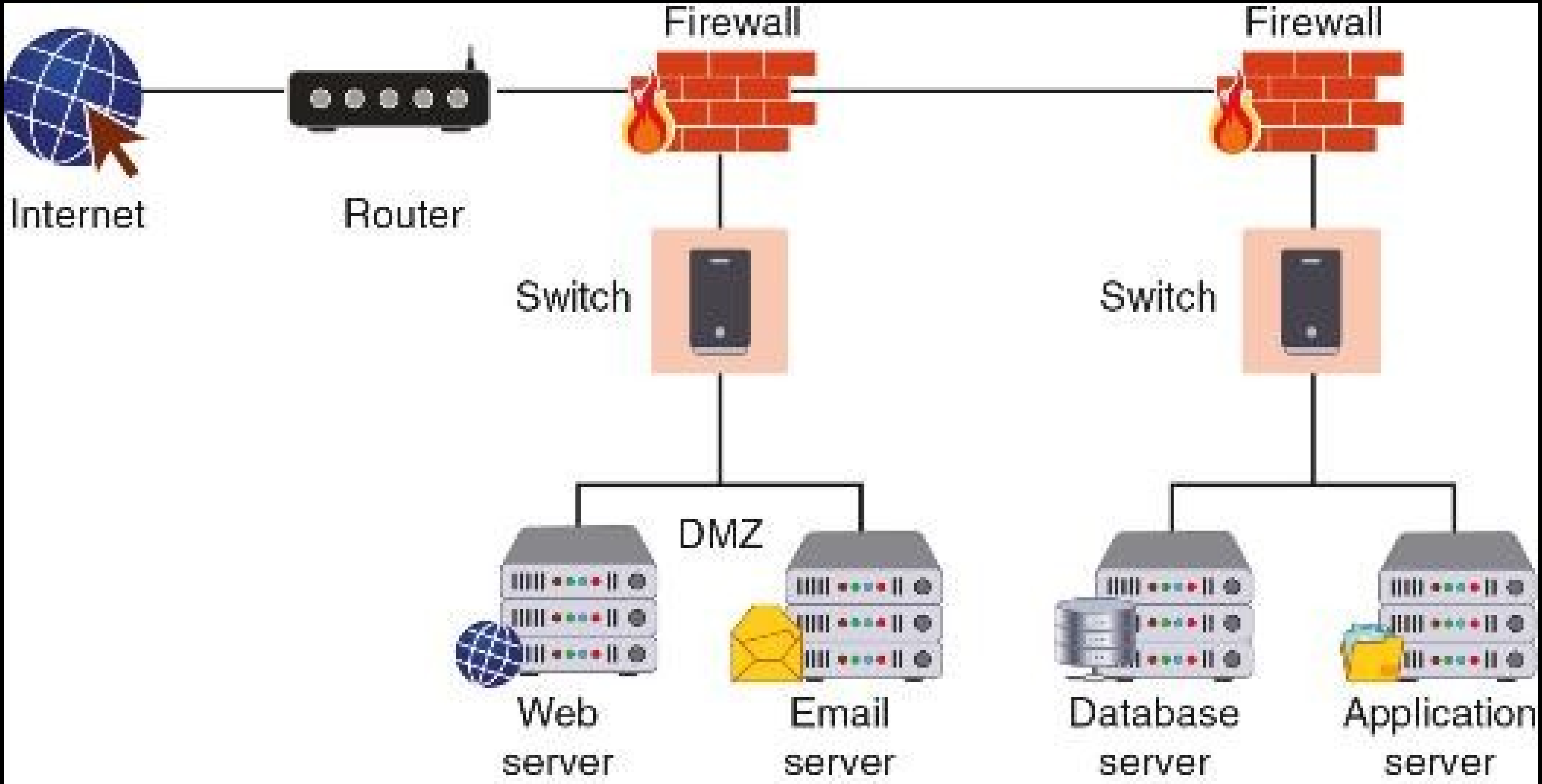
Virtual LANs (VLANs)

- A **virtual LAN** (**VLAN**) allows scattered users to be logically grouped together even though they are physically attached to different switches
- VLAN communication takes place in the following ways:
  - When devices in the same VLAN are connected to the same switch, the switch can handle the transfer of packets to the members of the VLAN group
  - When VLAN members on one switch need to communicate with members connected to another switch, a special “tagging” protocol must be used

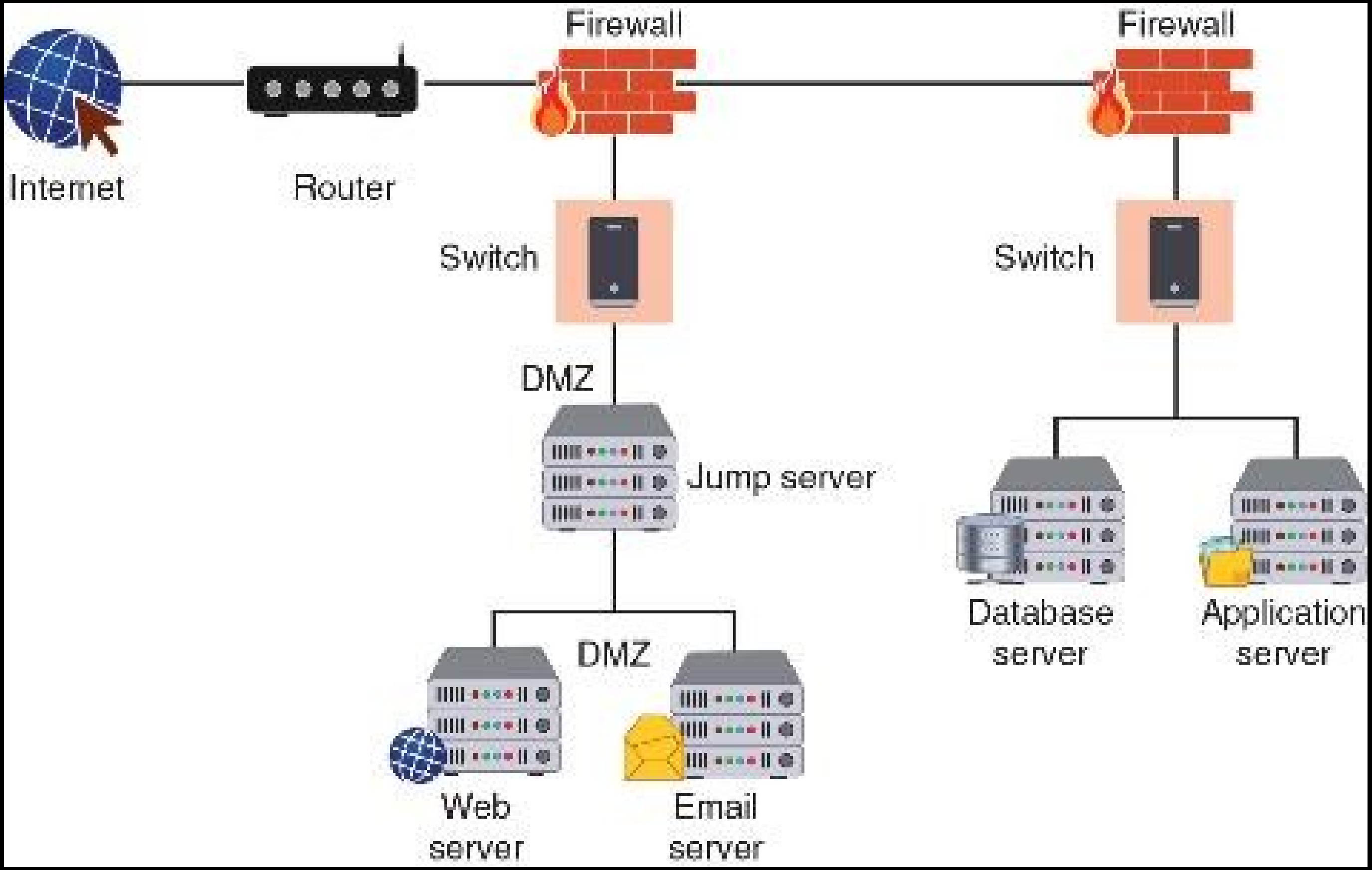
Demilitarized Zone (DMZ)

- To allow untrusted outside users access to resources such as web servers, most networks employ a **demilitarized zone** (**DMZ**)
  - The DMZ functions as a separate network that rests outside the secure network perimeter
  - Untrusted users can access the DMZ but cannot enter the secure network
- A **jump server** is a minimally configured server within the DMZ that runs only essential protocols and ports
  - It connects two dissimilar security zones while providing restricted access between them

DMZ with Two Firewalls



Jump Server


Firewall
Firewall
Internet
Router
Switch
Switch
DMZ
Jump server
DMZ
Web server
Email server
Database server
Application server

Demilitarized Zone (DMZ)

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 also be accessed 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

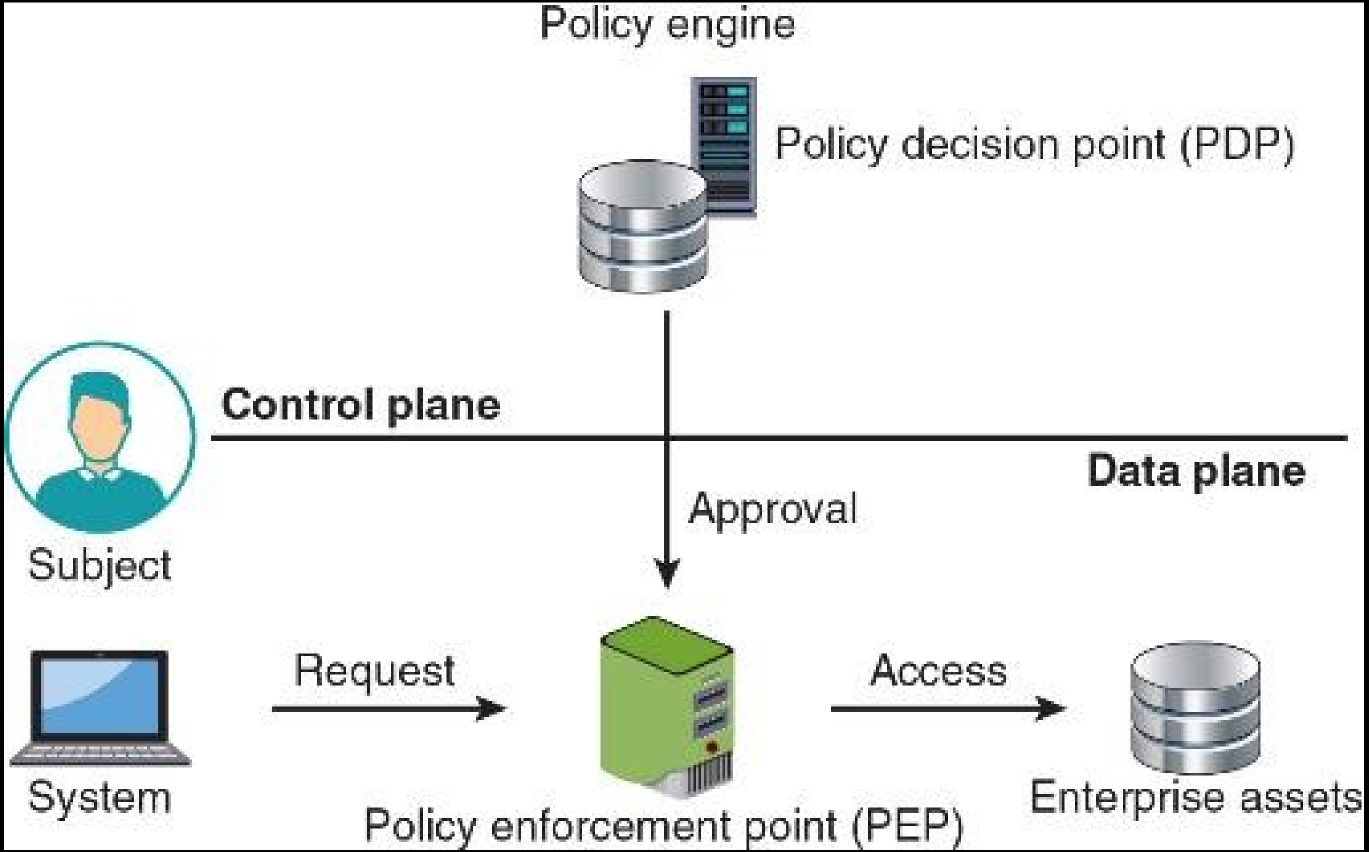
Zero Trust

- **Zero trust** is a strategic initiative that is designed to prevent successful attacks by threat actors who are already within a network
  - Zero trust acknowledges that trusting everyone within a network is a vulnerability
- A zero-trust architecture (ZTA) is a framework for implementing zero trust
  - It focuses on authentication and authorization to shrink implicit trust while still maintaining availability
- ZTA minimizes threats against assets (**threat scope reduction**)

Zero Trust

- The policy engine is a component of the **policy decision point** (**PDP**) that provides input into the **policy enforcement point** (**PEP**) to make the decision whether to grant access for a request
- The policy engine relies on **policy automation** that uses automated processes for referring to policies for approval
- The **control plane** is used for communication while the **data plane** is used for the transfer of the resource if approved

Conceptual ZTA



Access Technologies

- Accessing a network infrastructure from a location other than the campus on which the organization is located is called **remote access**
- Remote access always requires the connection be secure (**secure communication**)
  - This involves selecting the best protocol to use (**protocol selection**) and opening the right ports on devices so communication can occur (**port selection**)
- Two of the most common access technologies are virtual private network (VPN) and network access control (NAC)

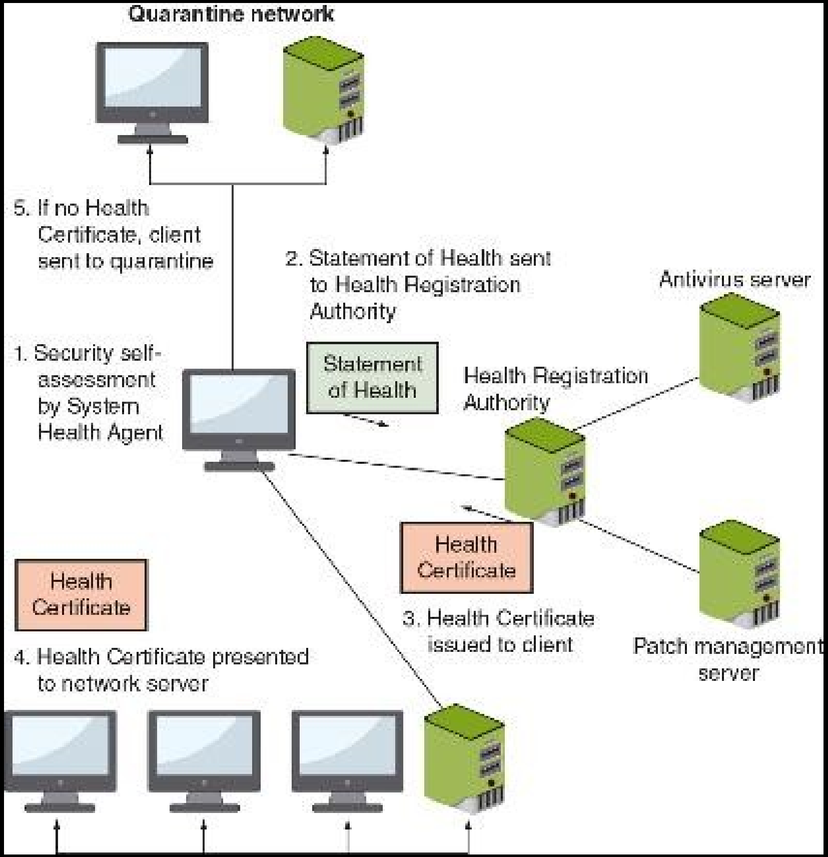
Virtual Private Network (VPN)

- A **virtual private network** (**VPN**) is a security technology that enables authorized users to use an unsecured public network (the Internet) as if it were a secure private network
- There are two common types of VPNs: a remote access VPN and a site-to-site VPN
- The most common protocol used for VPNs are IPsec and SSL
  - The Layer 2 Tunneling Protocol (L2TP) is a VPN protocol that does not offer any encryption or protection, so it is usually paired with IPsec (L2TP/IPsec)

Network Access Control (NAC)

- **Network access control** (**NAC**) examines the current state of an endpoint before it can connect to the network
  - Devices that do not meet a specified set of criteria are denied access to the network, or given restricted access to computing resources, or connected to a “quarantine” network
- Some NAC systems use software agents installed on endpoints to gather information
  - Another alternative is when the NAC technology is embedded within a Microsoft Windows Active Directory domain controller

NAC Process


Quarantine network
5. If no Health Certificate, client sent to quarantine
2. Statement of Health sent to Health Registration Authority
Antivirus server
1. Security self-assessment by System Health Agent
Statement of Health
Health Registration Authority
Health Certificate
Health Certificate
3. Health Certificate issued to client
Patch management server
4. Health Certificate presented to network server