September 24, 2024

“Do You Trust Me?”

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

OU Tulsa
SCHUSTERMAN CENTER

Checking In

- Recently we looked at the question “What Happens During a Hijacking?”
  - DDoS
  - DNS
  - MITM
  - Network and Security Protocols
  - POPS, IMAP, S/MIME
  - SSL/TLS; SSH, FTPS & SFTP

Checking In

- What were the most important concepts that you learned in the last classes?
- What were the muddiest (most unclear) points during the last classes?

Overview of Secure Network Design

- Definition: Secure Network Design involves structuring a network in a way that minimizes vulnerabilities, controls access, and ensures the confidentiality, integrity, and availability of data.

- Importance: As organizations increasingly rely on digital infrastructures, designing secure networks becomes paramount to protect against cyber threats, data breaches, and unauthorized access.

Key Objectives of Secure Network Design

- Confidentiality: Ensuring that sensitive information is accessible only to authorized individuals.
- Integrity: Protecting data from being altered or tampered with by unauthorized parties.
- Availability: Guaranteeing that network resources are accessible to authorized users when needed.

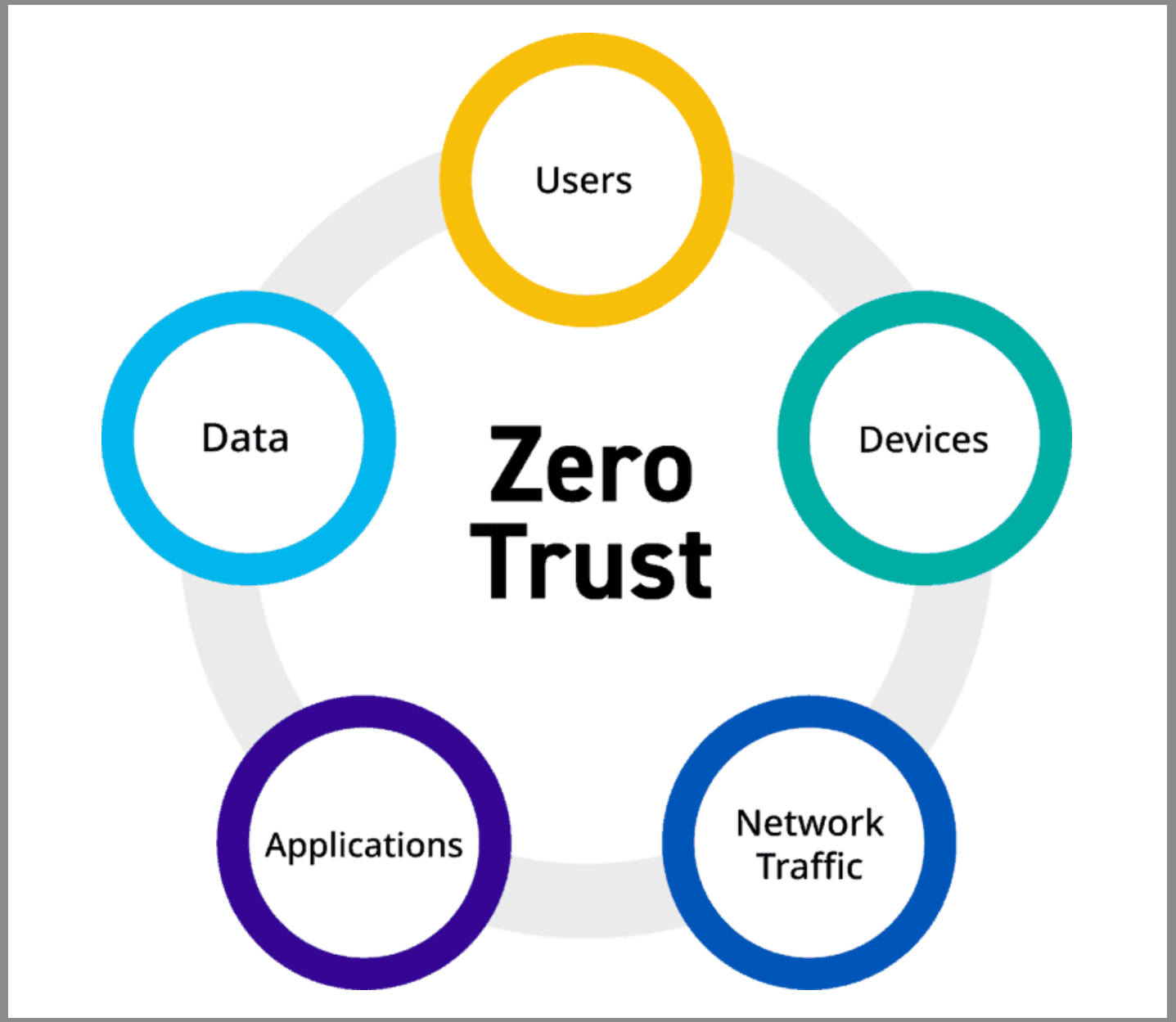
How Do You Define Trust?

"Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another."

-- Denise M. Rousseau

The Academy of Management Review, Vol. 23, No. 3 (Jul, 1998), pp. 393-404


AI
ACCESS
CONTROL


Users
Data
Devices
Zero
Trust
Applications
Network
Traffic

THE TRUST EQUATION

David Maister

Defining Trust in Network Security

- In network security, trust refers to the level of confidence that a system or user is legitimate and authorized to access specific network resources.
- Components of Trust:
  - Identity Verification: Confirming the identity of users and devices through authentication mechanisms.
  - Access Control: Determining what resources a trusted entity can access based on predefined policies.

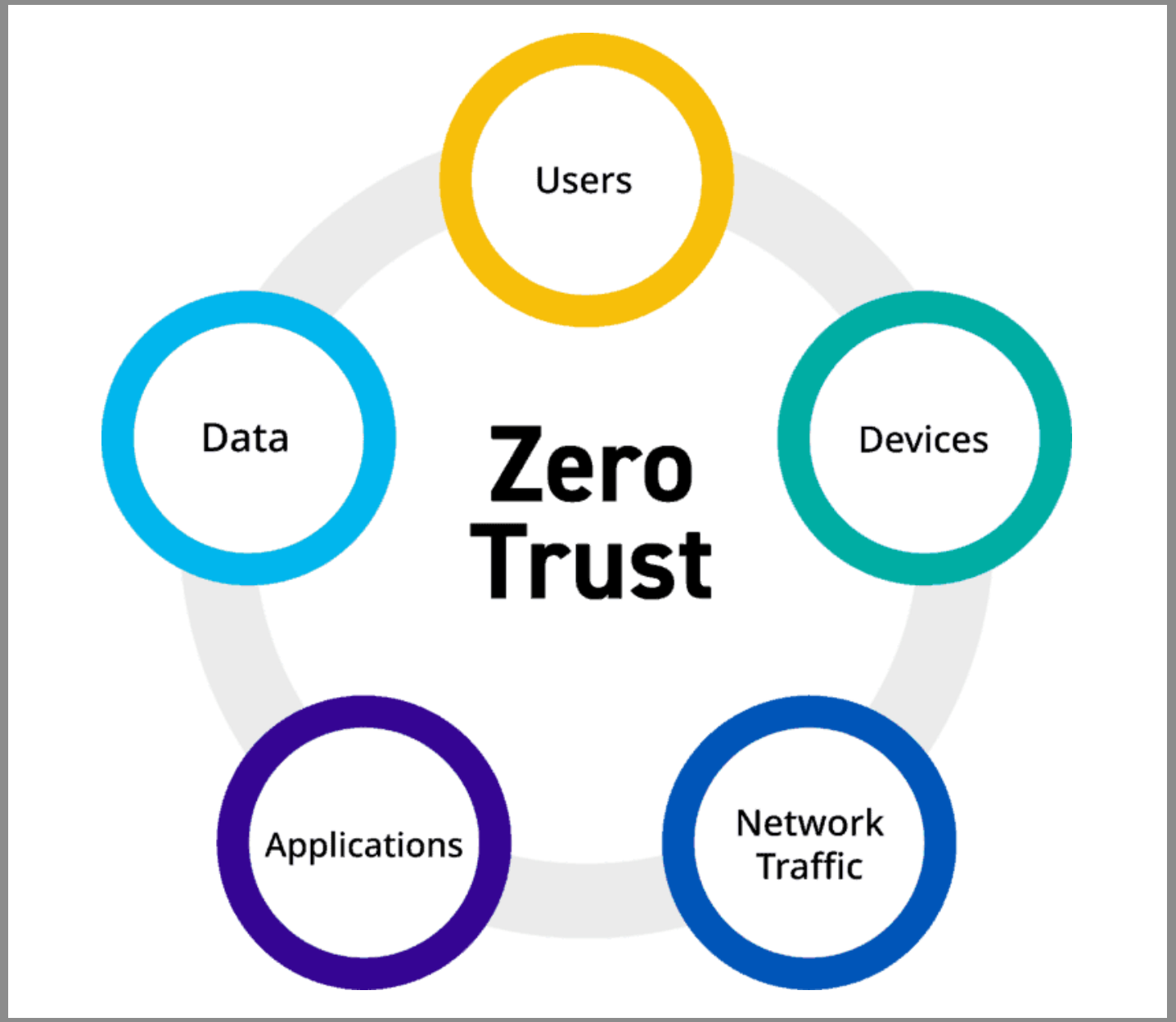
Building Trust in Networks

Credibility: Establishing trust through consistent and accurate identity verification methods (e.g., multi-factor authentication).

Reliability: Ensuring that trusted entities consistently adhere to security protocols and policies.

Integrity: Maintaining secure and tamper-proof systems that trusted entities can rely on.


AI
ACCESS
CONTROL


Users
Data
Devices
Zero
Trust
Applications
Network
Traffic

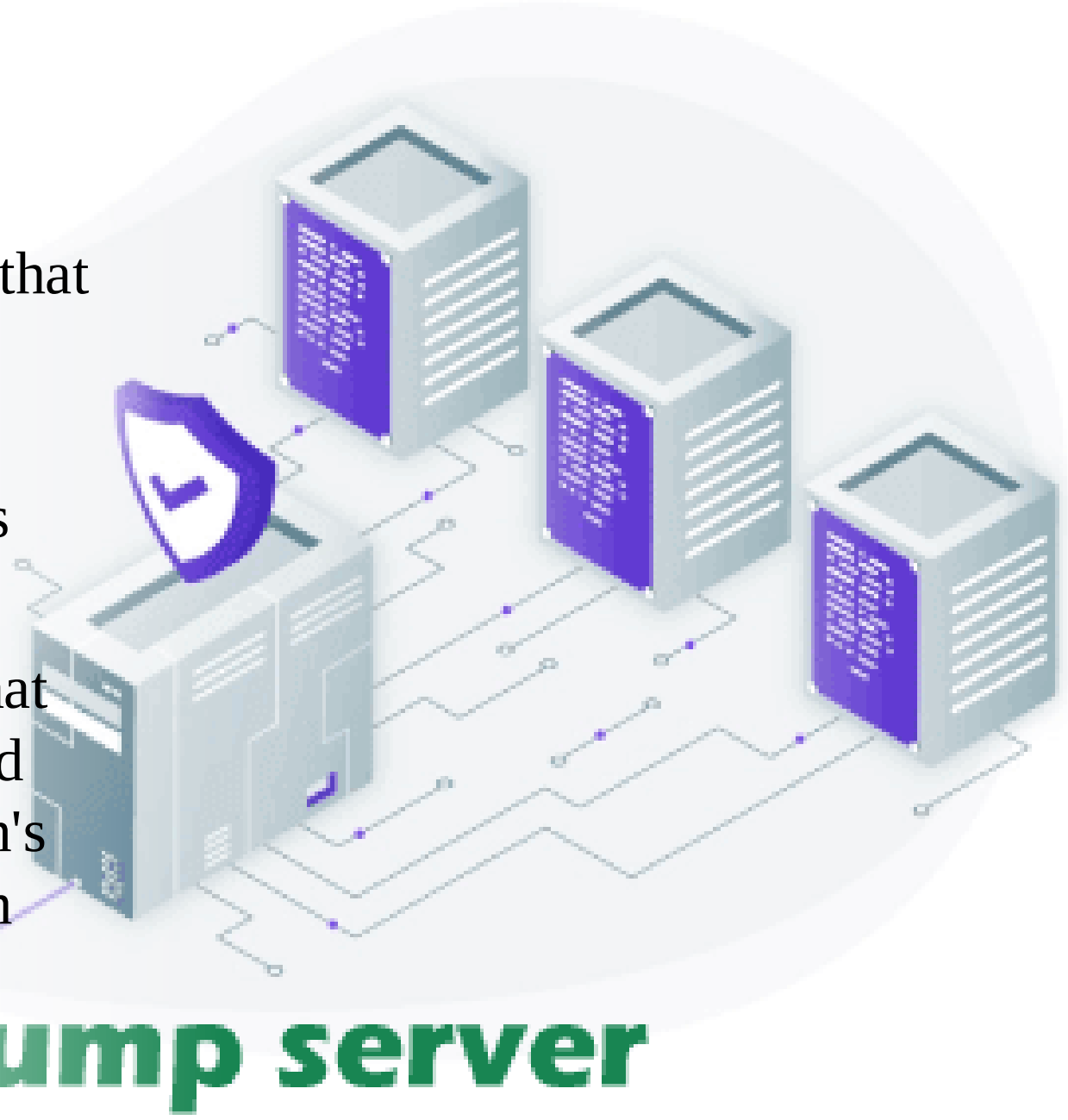
Network Segmentation

- The process of dividing a network into smaller, isolated segments to enhance security, improve performance, and simplify management.
- Organizations use segmentation to improve monitoring, boost performance, localize technical issues and – most importantly – enhance security. Individuals within the perimeter were assumed to be trustworthy and therefore not a threat.
- Limits the spread of malicious activity, reduces broadcast domains (messages), and localizes technical issues.

https://secureteam.co.uk/2020/08/07/what-is-network-segmentation/

Playing Zone Defense

- Trusted zone: a security zone that contains protected network resources that should only be accessible by an authorized user or system.
- Untrusted zone: a security zone that is outside an organization's control.
- Demilitarized zone: a security zone that lies between a trusted and an untrusted zone. A DMZ protects an organization's private network in a trusted zone from untrusted traffic.



Implementing VLANs for Logical Segmentation

Virtual Local Area Networks (VLANs): Logical subdivisions within a physical network, allowing multiple virtual networks to coexist on the same physical infrastructure.

Types of VLANs:

- Port-based VLAN: Assigns VLANs based on switch port configurations (physically located).
- Protocol-based VLAN: Segregates traffic based on network communication protocols.
- MAC-based VLAN: Uses device MAC addresses to assign VLAN memberships.

Best Practices for Network Segmentation

- **Least Privilege**: Grant only the necessary access to resources based on roles and responsibilities. (Which A?)
- **Regular Audits**: Continuously monitor and review segmentation policies to ensure they meet security requirements.
- **Automated Tools**: Utilize network management and security tools to maintain and enforce segmentation policies effectively.

Overview of Firewalls

- Definition: Firewalls are network devices or software applications that control incoming and outgoing traffic based on predefined security rules.

- Function: Act as barriers between trusted and untrusted networks, enforcing access policies to protect network resources.

Firewall Types

- Stateless (aka packet filter)
  - Operation: Inspects each packet independently based on header information (source/destination IP, port numbers, protocols).
  - Advantages: Simple and fast.
  - Limitations: Cannot track connection states, making them less effective against complex attacks.
- Stateful firewall (aka dynamic packet filter)
  - Operation: Monitors active connections and makes decisions based on the state of traffic (established, related, new).
  - Advantages: Provides better security by understanding traffic context.
  - Use Cases: Suitable for environments requiring dynamic and context-aware filtering.

Firewall Types - Next-Generation (NGFW)

- **Deep Packet Inspection (DPI)**: Analyzes packet data beyond headers to identify malicious content.
- **Application Awareness**: Recognizes and controls applications regardless of port or protocol.
- **Integrated Intrusion Prevention**: Combines firewall functions with IPS capabilities.
- **Threat Intelligence Integration**: Utilizes real-time data on emerging threats to update security policies.
- **Advantages**: Provides comprehensive protection against modern threats with advanced capabilities.
- **Example Products**: Palo Alto Networks NGFW, Cisco Firepower

Virtual and Host-based Firewalls

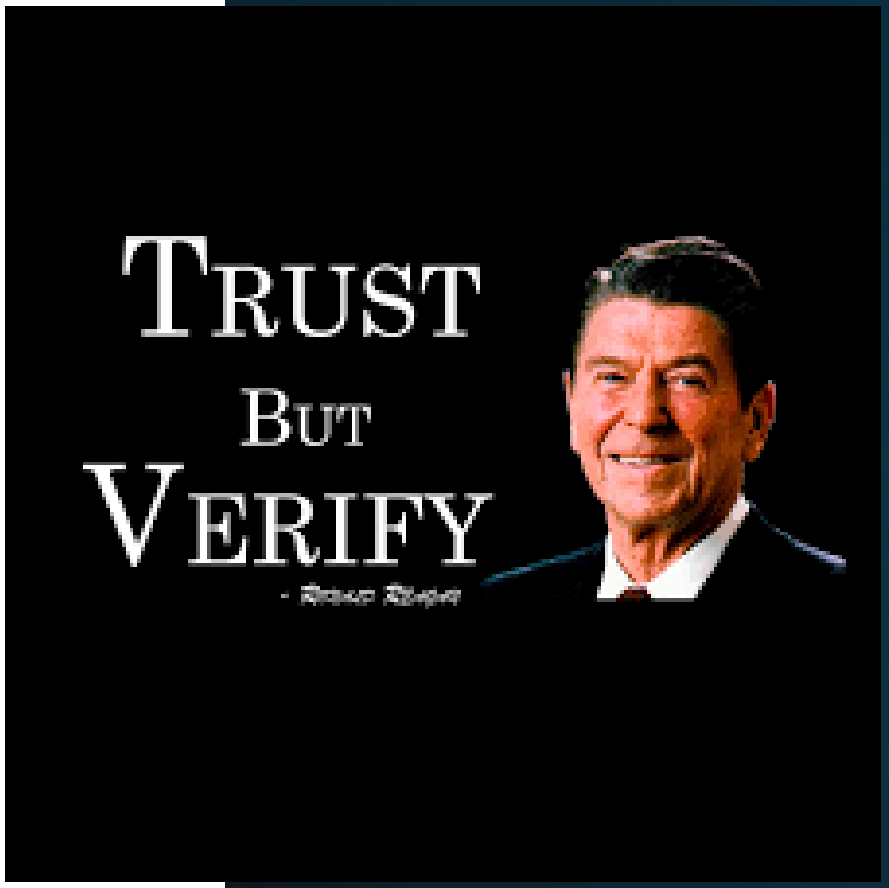
- A virtual firewall, also known as cloud firewalls or virtualized NGFWs (software), grants or rejects network access to traffic flows between untrusted zones and trusted zones in virtual networks.
  - A device that is physically located inside the data center has to perform north-south communication to interact with a device that is physically outside of the data center.
  - East-west traffic is traffic that originates and terminates all within a single data center.
- Host-based firewall is software installed directly on individual networked devices. Filters network traffic on a single device by inspecting both incoming and outgoing data.

Fail-Open vs. Fail-Closed :

Fail-Open Firewall	**Fail-Closed Firewall**
Default action when firewall fails: **Allow all traffic through**	Default action when firewall fails: **Block all traffic**
Pros: Ensures continued availability and prevents network outages.	**Pros**: Maximizes security by blocking all unauthorized or potentially harmful traffic.
Cons: Compromises security while the firewall is down, potentially allowing malicious traffic.	**Cons**: Can cause significant service interruptions, leading to downtime and possible business disruption.
Use Case: Critical applications where uptime is more important than short-term security, such as healthcare, financial trading, or emergency services.	**Use Case**: Security-sensitive environments where it’s critical to prevent unauthorized access, even at the cost of downtime.

Zero Trust Framework

- Zero Trust is a security framework that requires continuous authentication, authorization, and validation of security configurations for every user, device, and network flow, regardless of their location within or outside the network perimeter.
- Core Philosophy: "Never trust, always verify."
  - Is this really where are now?



Principles of Zero Trust

- **Assume Breach:** Operate under the assumption that the network is already compromised.
- **Least Privilege Access**: Grant users and devices only the minimum access necessary to perform their functions.
- **Microsegmentation:** Divide the network into smaller segments to limit lateral movement of threats.
- **Continuous Monitoring and Validation**: Regularly assess and revalidate trust levels based on real-time data (e.g. 802.1X working with RADIUS).
- **Dynamic Policy Enforcement**: Adapt security policies based on contextual factors like user behavior, device health, and threat intelligence.

Zero Trust vs. Traditional Perimeter Security

Traditional Perimeter Security: Focuses on securing the boundary between internal and external networks, implicitly trusting internal users and devices.

Zero Trust Security: Removes the implicit trust, requiring verification for every access request, thereby providing enhanced security in dynamic and distributed environments.

Zero Trust vs. Traditional Perimeter Security

Traditional Perimeter Security: Focuses on securing the boundary between internal and external networks, implicitly trusting internal users and devices.

Zero Trust Security: Removes the implicit trust, requiring verification for every access request, thereby providing enhanced security in dynamic and distributed environments.

Example Scenario: Zero Trust Implementation

Implementation Steps:

1. User Authentication: Implement multi-factor authentication (MFA) for all users accessing cloud services.

2. Device Compliance: Ensure all devices meet security standards before granting access.

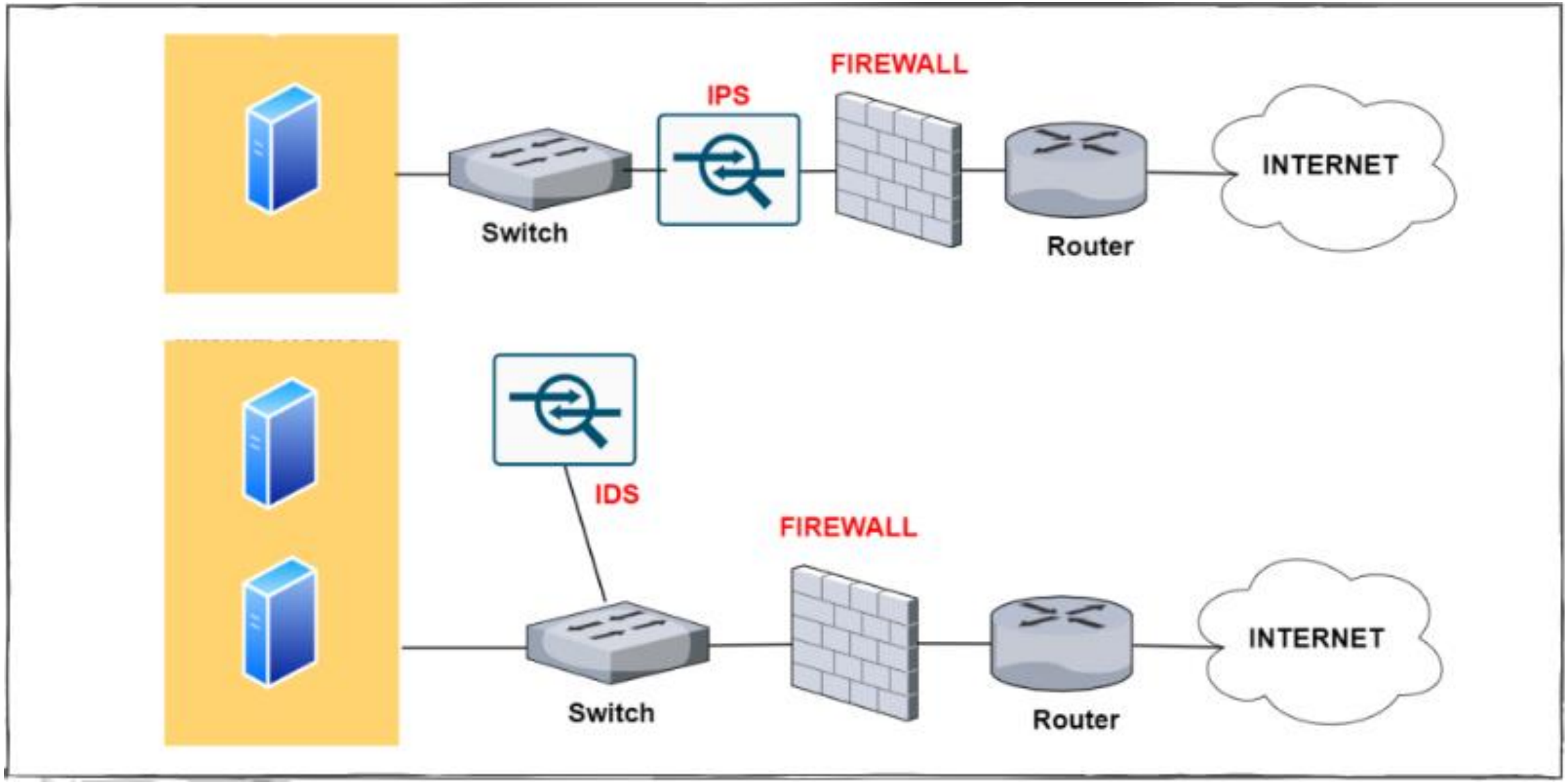
3. Microsegmentation: Divide the network into segments where each application has its own security controls.

4. Continuous Monitoring: Use monitoring tools to detect and respond to suspicious activities in real-time.

Network Intrusion Detection and Prevention Systems

IDS monitors network traffic and devices for known malicious activity, suspicious activity or security policy violations.

IPS stops the intrusion before it gets on your network. The IPS is placed inline, directly in the flow of network traffic between the source and destination.



https://www.networkstraining.com/firewall-vs-ips-vs-ids-vs-waf/

Types of IDS/IPS (1 of 2)

- Network Intrusion Detection System (NIDS):
  - Function: Monitors and analyzes network traffic for signs of malicious activity.
  - Deployment: Positioned at strategic points within the network (e.g., behind firewalls).
- Host-based Intrusion Detection System (HIDS):
  - Function: Monitors activities on individual hosts (e.g., processes, logs).
  - Deployment: Installed directly on endpoints like servers or workstations.
- NIDS monitors all network traffic passing through a specific point on the network, while HIDS monitors activity happening directly on a host system, like system calls (e.g, open a file, run a program), file access, and running processes (e.g., manage CPU time).

Types of IDS/IPS (2 of 2)

- Network Intrusion Prevention System (NIPS)
  - Function: Detects and prevents identified threats by taking immediate action (e.g., blocking traffic).
- Differences Between IDS and IPS:
  - IDS
    - Role: Passive monitoring and alerting.
    - Action: Sends alerts for detected threats but does not take action to block them.
  - IPS
    - Role: Active prevention and mitigation.
    - Action: Automatically blocks or mitigates threats upon detection

Detection Methods Used by IDS/IPS

- Signature-based Detection: Identifies threats by matching patterns against a database of known attack signatures.
- Anomaly-based Detection: Detects deviations from established normal behavior patterns.
- Behavior-based Detection: Monitors and analyzes behaviors or actions that are indicative of malicious intent.
- Heuristic-based Detection: Uses algorithms and machine learning to identify potential threats based on unusual characteristics or behaviors.

How Can a Criminal Evade IDS Security?

- DDoS – flood the system, take IDS offline.
- DNS Spoofing – fake a trusted source.
- Fragmentation – split malware into small packets
- Encryption – Manipulate decryption key.
- Operator error – Weakest link.

https://www.mfellattorneyatlaw.com/learn-about-your-options-for-a-strong-defense-against-evading-police/

Load Balancing

Definition: The practice of distributing network or application traffic across multiple servers to ensure no single server becomes overwhelmed, enhancing performance and reliability.

Load balancers based on algorithms: static and dynamic.

- A static load balancer will not be aware of which servers are performing slowly or underutilized.
- Dynamic load balancing algorithms take the current availability, workload, and health of each server into account.

September 26, 2024

Presentations

Foundations of Cybersecurity - CYBS 3213

Christopher Freeze, Ph.D.
Assistant Professor, Cybersecurity
OU Polytechnic Institute

OU Tulsa
SCHUSTERMAN CENTER