<CTAINASL>

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

ADVANCED INFORMATION ASSURANCE & SECURITY

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

Intrusion Detection, Honeypots, Honeynets

LEARNING OUTCOMES

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

01

Identify and describe the operating models for intrusion and detection systems

02

Define and describe honeypots, honeynets and padded cell systems

03

List and define the major categories of scanning and analytics tools

Intrusion Detection

Intrusion Detection

An Intrusion Detection System (IDS) is a cybersecurity tool that monitors network traffic and detects suspicious activities that may indicate a cyber attack.

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

Why is IDS Important?

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

Key Features of IDS

Real-Time Monitoring

IDS continuously monitor network traffic and system activities in realtime, looking for any abnormal behavior or known attack patterns.

Alert Generation

When suspicious activity is detected, IDS generates alerts or notifications to inform administrators or security personnel about a potential security breach.

Severity Levels

Informational Alerts

Informational alerts are the lowest level of alerts and typically don't indicate a security threat. They provide details about normal system activities, configuration changes, or network events.

Severity Levels

Low-level Alerts

Low-level alerts may indicate suspicious activities that could be early indicators of an attack. They don't necessarily confirm an intrusion but warrant investigation to rule out potential threats.

Severity Levels

Medium-level Alerts

Medium-level alerts signify more suspicious activities that may require immediate attention. They are often generated for events that have a moderate likelihood of indicating an intrusion.

Severity Levels

High-level Alerts

High-level alerts are raised for events that are highly indicative of a security breach. These events require immediate action, such as isolating affected systems, blocking traffic, or launching a deeper investigation into the incident.

Severity Levels

Critical-level Alerts

Critical-level alerts are the highest level of alerts and signify a confirmed security breach or a severe threat. Immediate and decisive action is necessary to contain the intrusion, mitigate damages, and restore security.

Severity Levels

User-Defined Alerts

User-Defined Alerts allow organizations to define custom alert levels based on their specific needs and risk profiles. These user-defined levels enable organizations to tailor alert classifications to their unique security requirements.

Log Analysis

IDS analyze system logs, including event logs, firewall logs, and application logs, to detect unusual or potentially harmful activities. It involves the examination of log files generated by various network and system components to identify potential security issues or signs of intrusion.

Scalability

IDS can be scaled to meet the needs of various network sizes and configurations, from small local networks to large enterprise-level systems.

- One key process for achieving scalability is load balancing.
- Distributed architectures are another important aspect of scalability, especially for large-scale networks

Automated Response Capabilities

Some IDS are capable of taking automated responses when suspicious activity is detected.

Centralized Management

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

Centralized management capabilities are integral to effective IDS implementations as they allow organizations to efficiently monitor, configure, and maintain their security infrastructure from a single, unified interface.

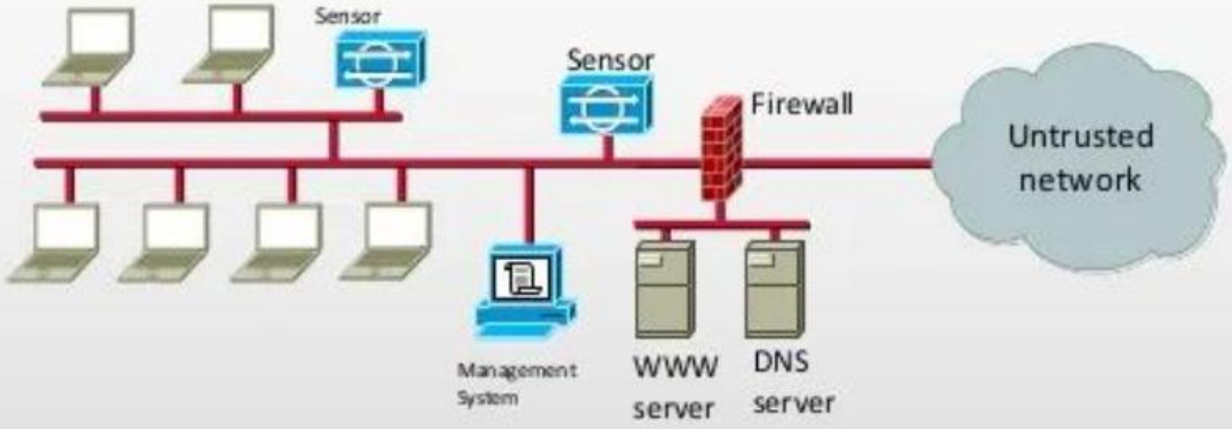

1900
INTEGRITY • COMPASSION • RESILIENCE • INNOVATION • PATRIOTISM
124
NATIONAL UNIVERSITY
HONORING YEARS OF Education that works.

Types of IDS

Network-based IDS (NIDS)

- Monitors all traffic passing through a network.
- Placed at key points, such as routers, gateways, or data centers.
- Ideal for detecting large-scale attacks like Distributed Denial of Service (DDoS) attacks.

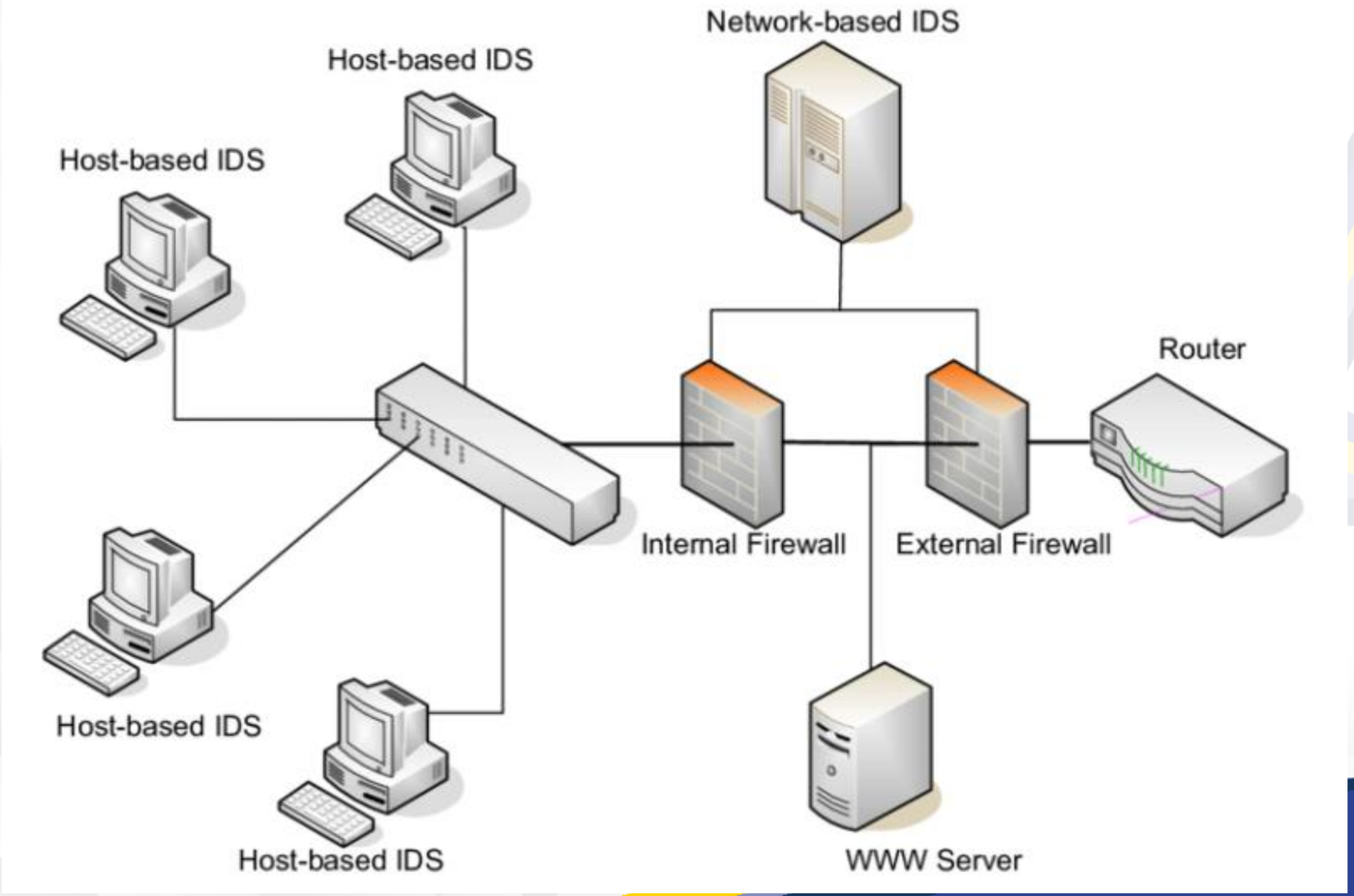
Network Based IDS



Host-based IDS (HIDS):

- Installed on individual computers or servers.
- Monitors activities inside a device, such as unauthorized file modifications, software installations, or changes to system settings.
- Useful for detecting insider threats and attacks that bypass firewalls.

Host-based IDS (HIDS):



NATIONAL UNIVERSITY

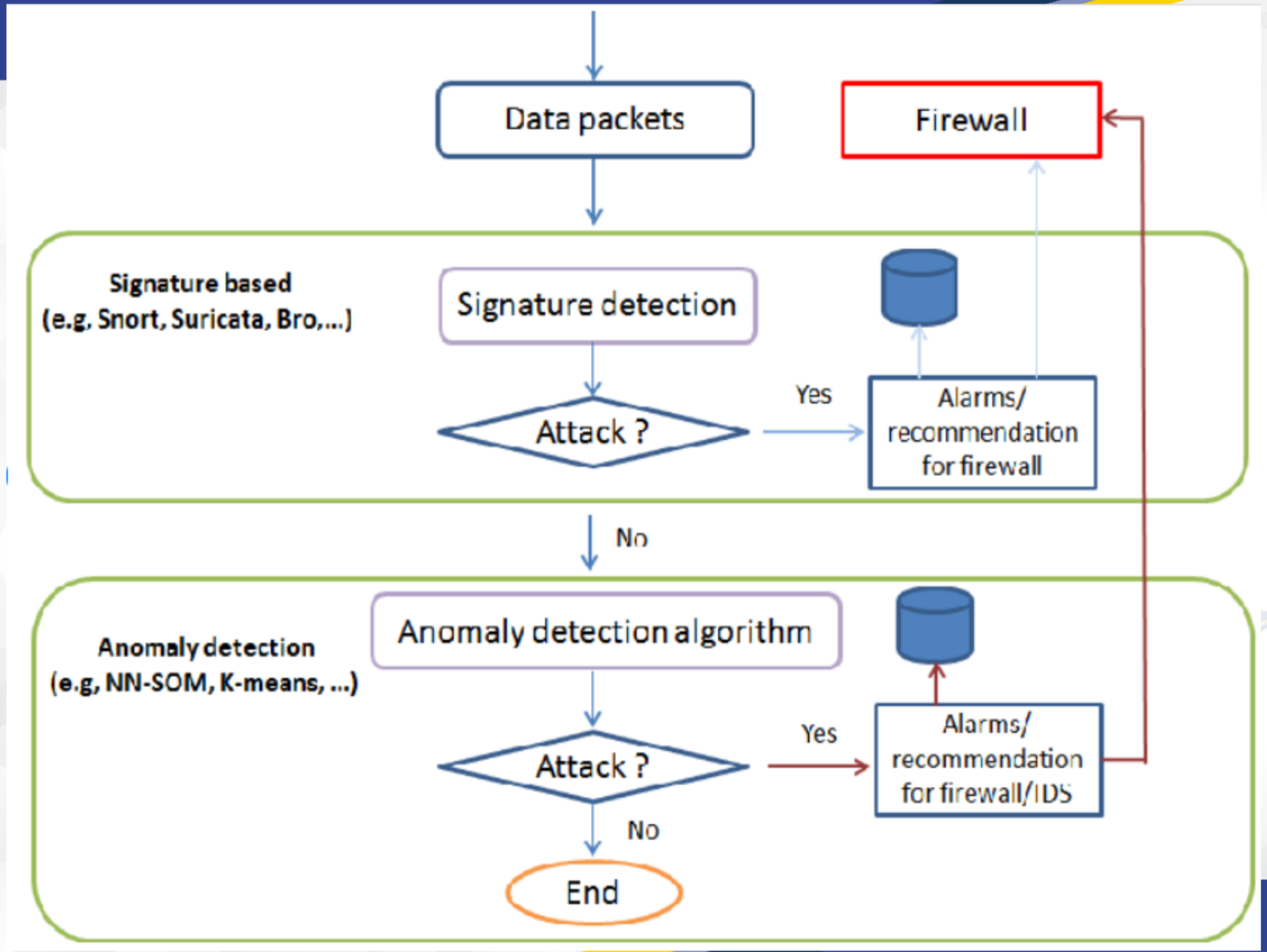
HONORING YEARS OF *Education that works.*

Signature-based IDS

- Works like an antivirus program—it detects known attack patterns (signatures).
- Very effective against known threats but fails to detect new, unknown attacks.

Anomaly-based IDS

- Uses machine learning or statistical models to detect abnormal behavior.
- Can detect zero-day attacks (new, previously unknown threats).
- Prone to false positives because not all unusual activities are malicious.



NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

How IDS Works

NATIONAL UNIVERSITY

...that works.

Packet Sniffing and Traffic Analysis

Log Monitoring and Behavioral Analysis

Threat Intelligence Integration

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

Common IDS Tools and Technologies

Popular IDS Tools

- ✓ Snort – Open-source, widely used for network monitoring.
- ✓ Suricata – High-performance IDS with deep packet inspection.
- ✓ Zeek (Bro) – IDS that also helps with network forensics.
- ✓ OSSEC – Host-based IDS that monitors system logs.

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

IDS Deployment Strategies

Perimeter IDS

Placed at the network entry points (e.g., firewalls, gateways).

Detects threats before they reach internal systems.

Internal IDS

- Placed inside a network, monitoring activities among devices.
- Useful for detecting insider threats and lateral movement attacks.

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

Challenges and Limitations of IDS

False Positives

IDS sometimes alerts on harmless activity, like a legitimate user accessing the system from a new location.

False Negatives

IDS might miss a threat if the attack is sophisticated.

Performance Impact

IDS can slow down networks if not configured properly.

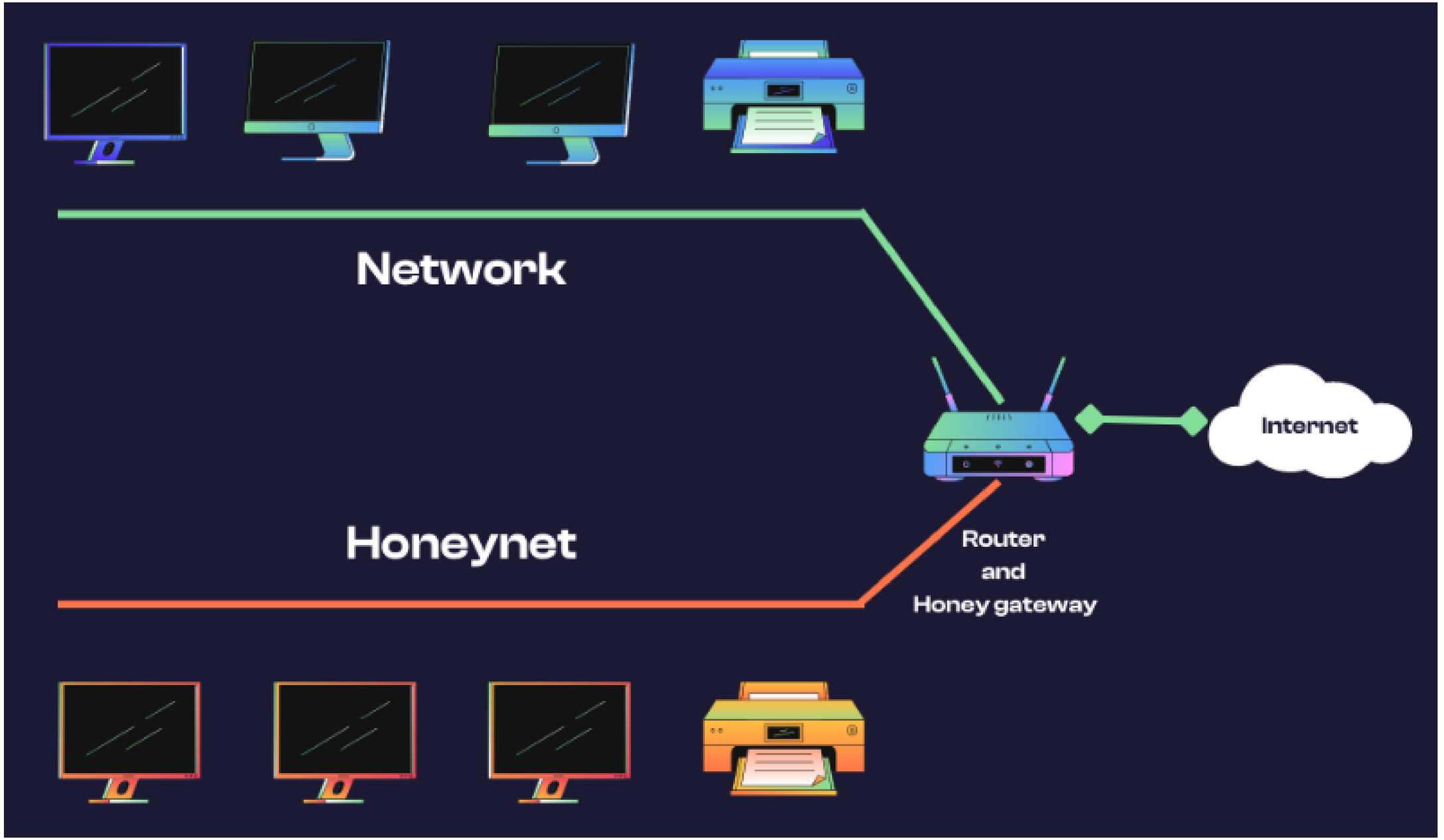
Honeypots and Honeynets

Honeypots

Honeypots are decoy systems or network devices designed to attract and detect unauthorized access or cyberattacks by imitating vulnerable targets.

Honeynets

Honeynets are network security systems that consist of multiple interconnected honeypots, designed to collectively monitor and analyze network traffic, detect and track cyber threats, and gain insights into attack patterns and behaviors.


Network
Honeynet
Router
and
Honey gateway
Internet


TechTarget

NATIONAL UNIVERSITY

HONORING YEARS OF *Education that works.*

THANK YOU