

Intrusion Detection Systems



Dr. Williams Central Connecticut State University

Definitions

(From Internet Security Glossary)

Security Intrusion: A security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so.

Intrusion Detection: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

Intruder Behavior



- Information gathering
 - Identify vulnerable services, port scans, NMAP, etc
- Initial access
 - Exploit vulnerability, password guessing, spear phishing, etc.
- Privilege escalation
 - Scan local host for vulnerable application, install sniffers, pivot
- Information gathering or exploit
 - Send back target information, exploit further attack
- Maintain access
 - Install backdoor, modify or disable anti-virus or IDS
- Cover tracks
 - Rootkit to hide, remove traces in logfiles

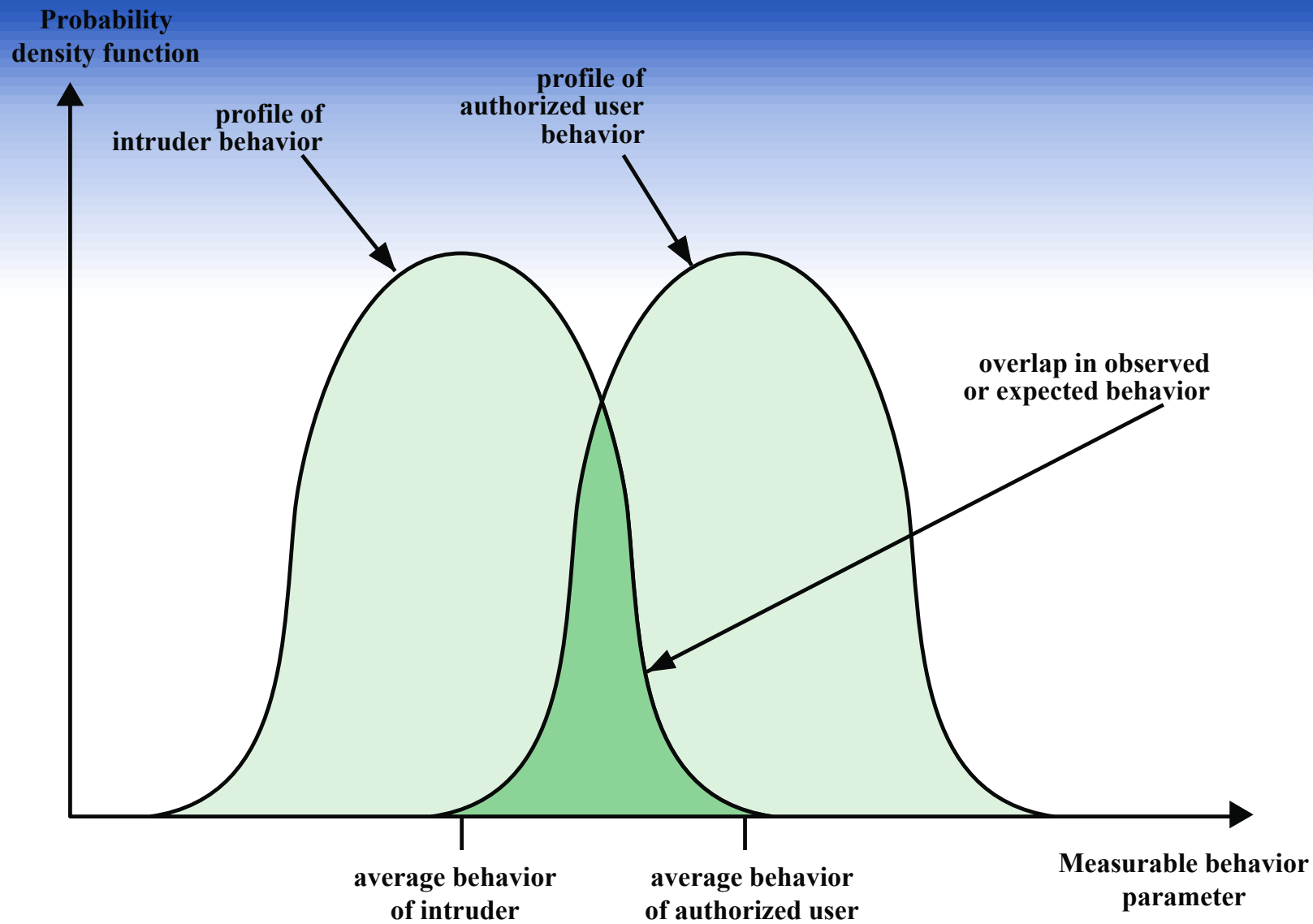


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

INTRUSION DETECTION

VS

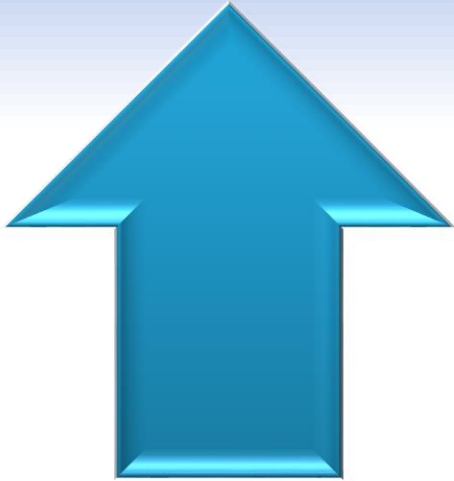
INTRUSION PREVENTION SYSTEMS

The Need For Firewalls



- Internet connectivity is essential
 - However it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
 - Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defense
 - Single choke point to impose security and auditing
 - Insulates the internal systems from external networks

Firewall Capabilities And Limits



Capabilities:

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as the platform for IPSec



Limitations:

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organization
- Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

Intrusion detection vs Intrusion prevention

- Ideally would want to prevent any intrusion
- Not an ideal world...
 - Complexity of processing
 - Amount of processing
 - Nature of detection
- Result since not all can be processed in real-time need/want a mix of both

IDS Requirements

Run continually

Be fault tolerant

Resist subversion

**Impose a minimal
overhead on
system**

**Configured
according to
system security
policies**

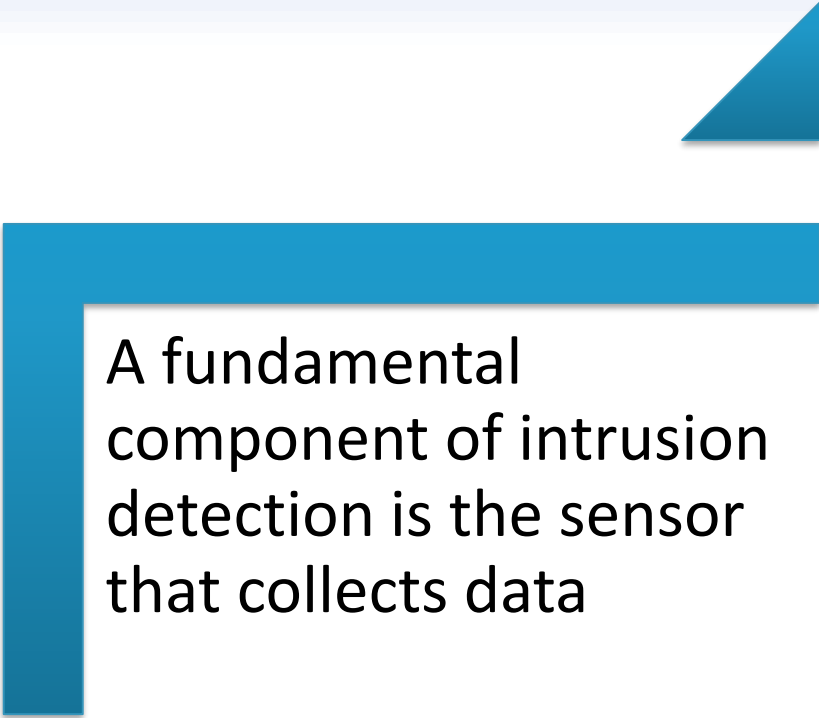
**Adapt to changes
in systems and
users**

**Scale to monitor
large numbers of
systems**

**Provide graceful
degradation of
service**

**Allow dynamic
reconfiguration**

Data Sources and Sensors



A fundamental component of intrusion detection is the sensor that collects data



Common data sources include:

- System call traces
- Audit (log file) records
- File integrity checksums
- Registry access
- Network access
- Protocol use

Intrusion Detection System (IDS)

- Host-based IDS (HIDS)
 - Monitors the characteristics of a single host for suspicious activity
- Network-based IDS (NIDS)
 - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
 - Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity

Comprises three logical components:

- **Sensors - collect data**
- **Analyzers - determine if intrusion has occurred**
- **User interface - view output or control system behavior**

Analysis Approaches

Signature/Heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Can only identify known attacks for which it has patterns or rules
- Easier to act on resulting data

Anomaly detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Key IDS research topic – intersection of these:

- Ways to combine approaches for benefits of both
- Detect unknown attacks more effectively AND given more meaningful alert data

Anomaly Detection

A variety of classification approaches are used:

Statistical

- Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics

Knowledge based

- Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior

Machine-learning

- Approaches automatically determine a suitable classification model from the training data using data mining techniques

Signature or Heuristic Detection

Signature approaches

Match a large collection of known patterns of malicious data against data stored on a system or in transit over a network

The signatures need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data

Widely used in anti-virus products, network traffic scanning proxies, and in NIDS

Rule-based heuristic identification

Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage

Typically rules used are specific

SNORT is an example of a rule-based NIDS

Host-Based Intrusion Detection (HIDS)

- Adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- Monitors activity to detect suspicious behavior
 - Primary purpose is to detect intrusions, log suspicious events, and send alerts
 - Can detect both external and internal intrusions

Network-Based IDS (NIDS)

Monitors traffic at selected points on a network

Examines traffic packet by packet in real or close to real time

May examine network, transport, and/or application-level protocol activity

Comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface

Analysis of traffic patterns may be done at the sensor, the management server or a combination of the two

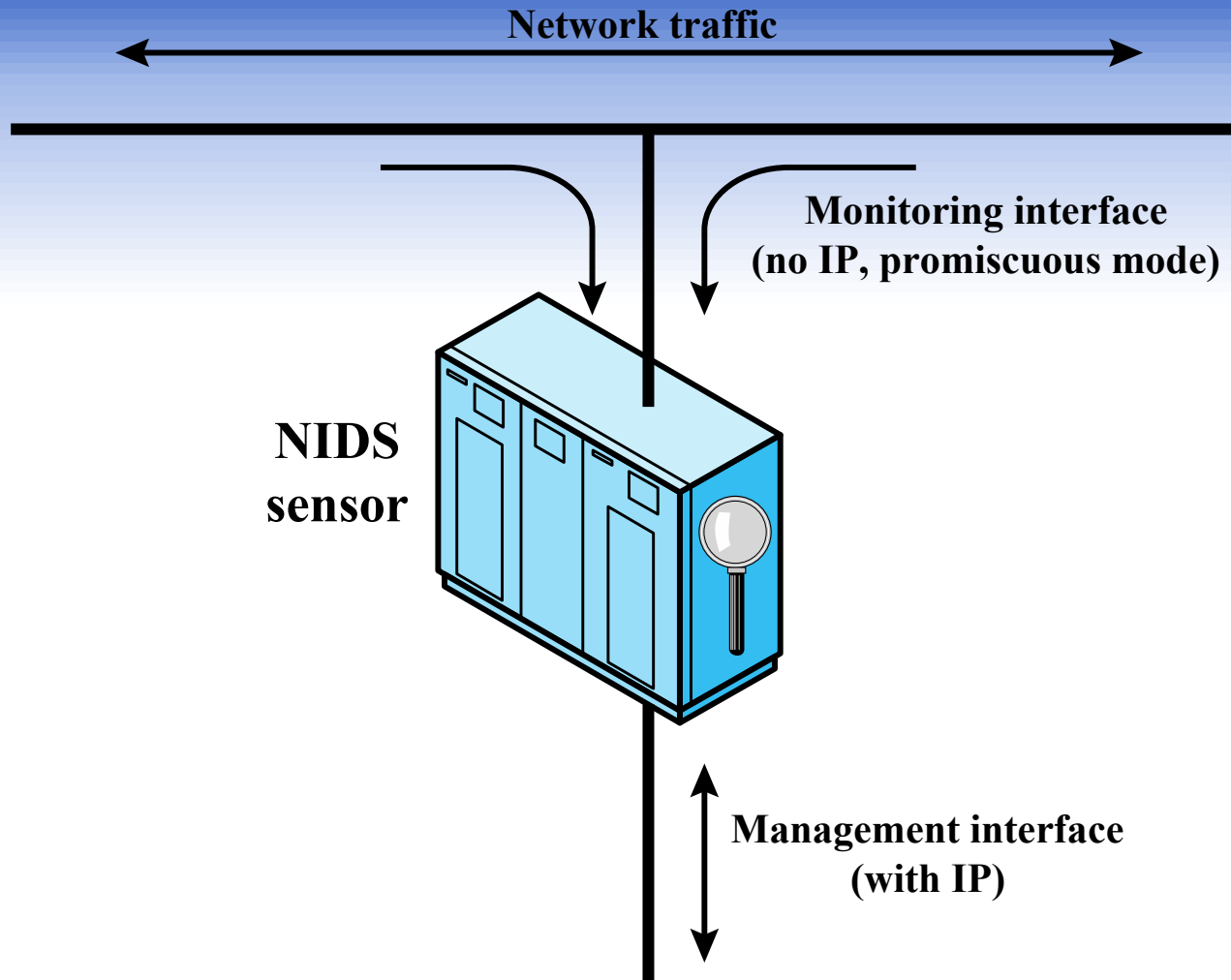


Figure 8.4 Passive NIDS Sensor

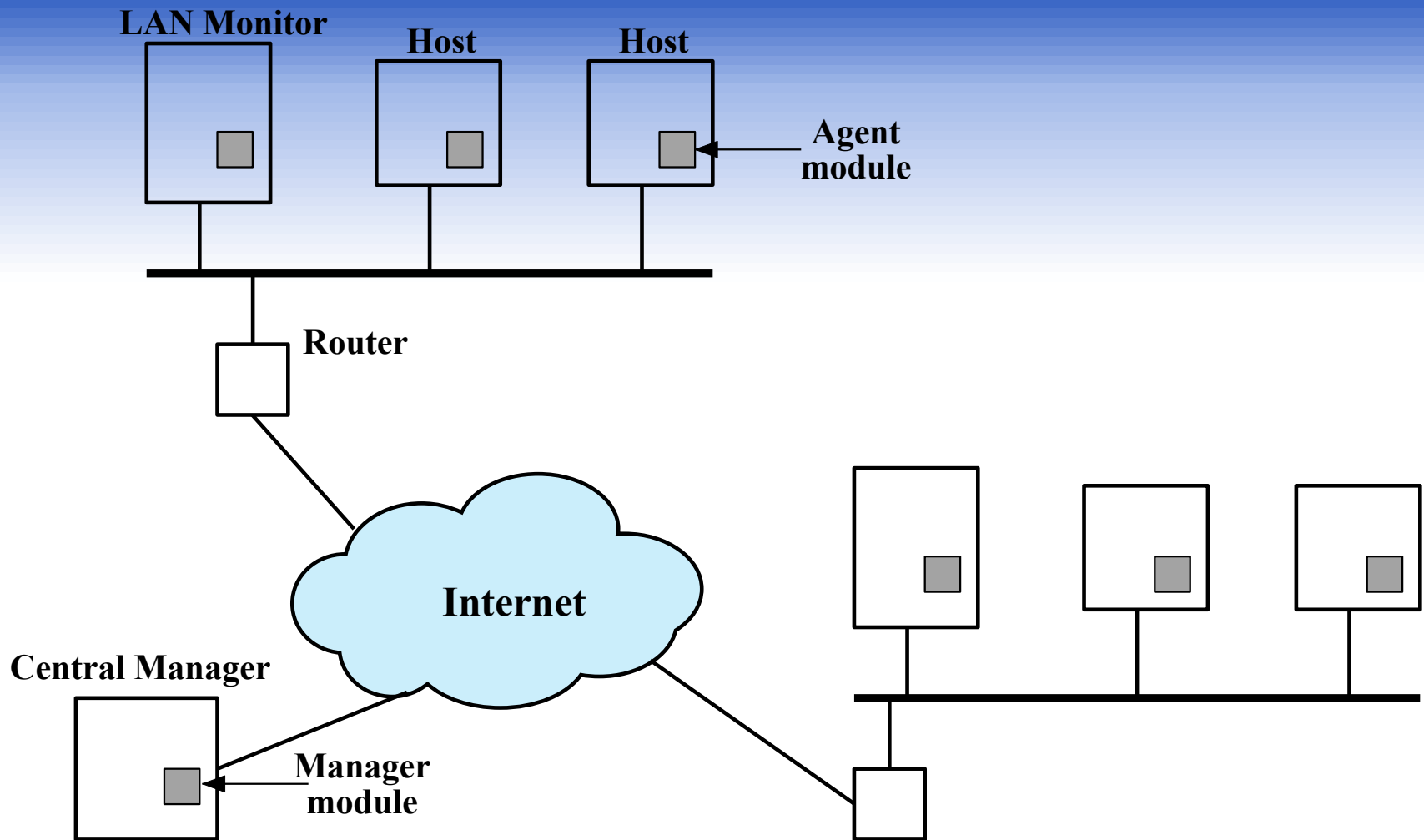


Figure 8.2 Architecture for Distributed Intrusion Detection

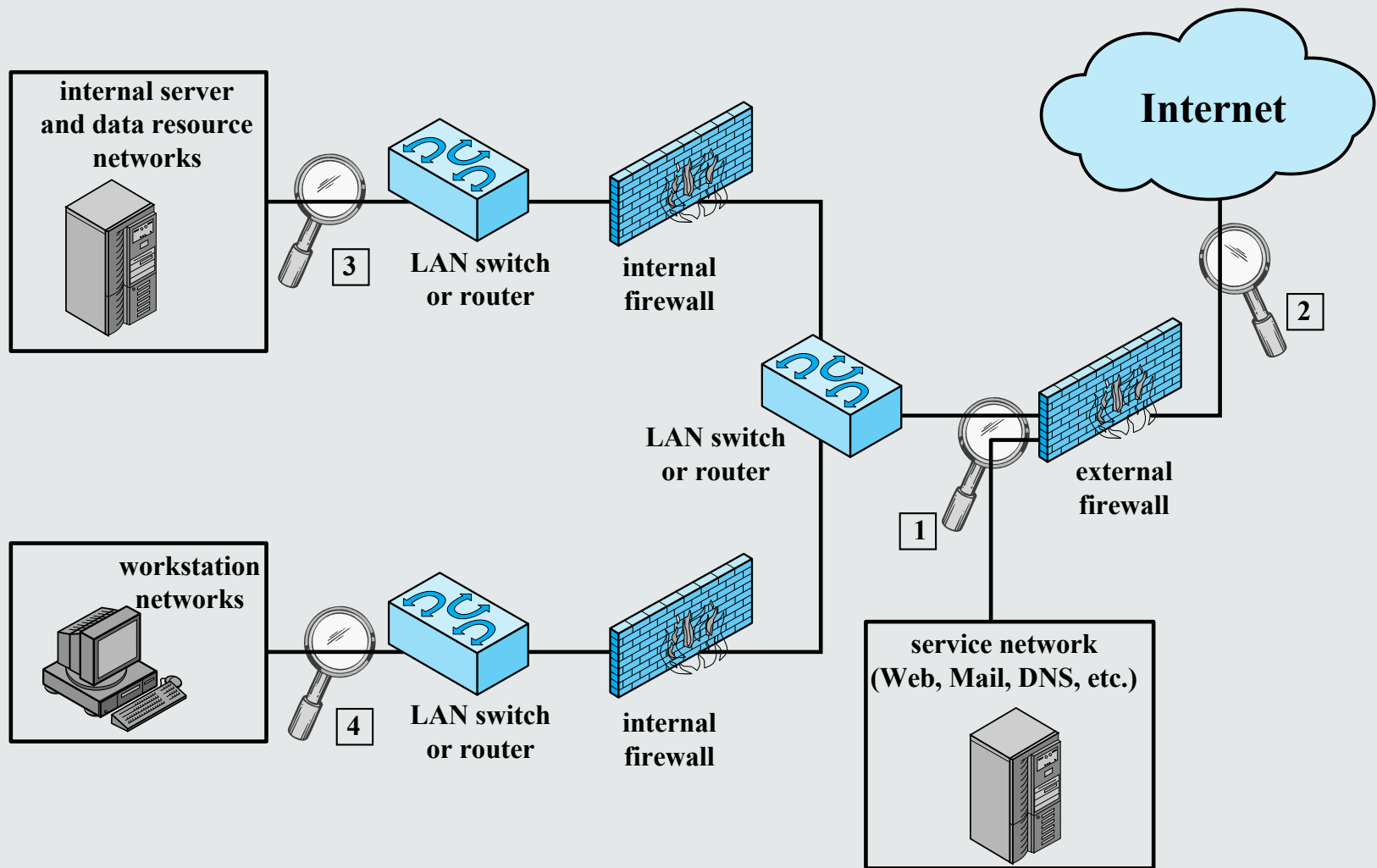


Figure 8.5 Example of NIDS Sensor Deployment

Intrusion Detection Techniques

Attacks suitable for Signature detection

- Application layer reconnaissance and attacks
- Transport layer reconnaissance and attacks
- Network layer reconnaissance and attacks
- Unexpected application services
- Policy violations

Attacks suitable for Anomaly detection

- Denial-of-service (DoS) attacks
- Scanning
- Worms

Honeypots



- Decoy systems designed to:
 - Lure a potential attacker away from critical systems
 - Collect information about the attacker's activity
 - Encourage the attacker to stay on the system long enough for administrators to respond
- Systems are filled with fabricated information that a legitimate user of the system wouldn't access
- Resources that have no production value
 - Therefore incoming communication is most likely a probe, scan, or attack
 - Initiated outbound communication suggests that the system has probably been compromised

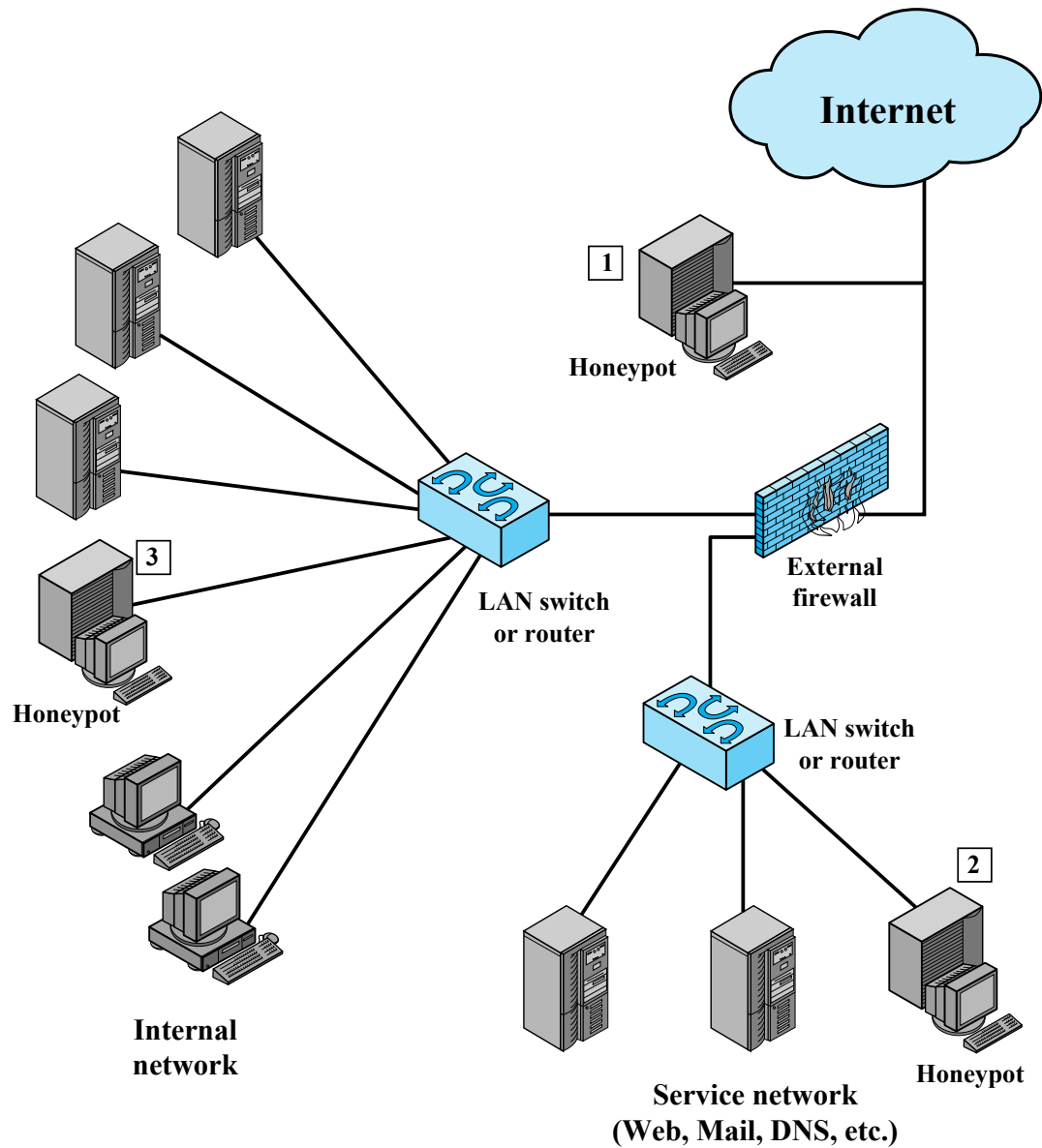


Figure 8.8 Example of Honeypot Deployment

Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

Host-Based IPS (HIPS)

- Can make use of either signature/heuristic or anomaly detection techniques to identify attacks
 - Signature: focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious
 - Anomaly: IPS is looking for behavior patterns that indicate malware
- Examples of the types of malicious behavior addressed by a HIPS include:
 - Modification of system resources
 - Privilege-escalation exploits
 - Buffer-overflow exploits
 - Access to e-mail contact list
 - Directory traversal
- In general extremely difficult to have successful anomaly based HIPS based on single host sensors alone – distributed sensors key

Network-Based IPS (NIPS)

- Inline NIDS with the authority to modify or discard packets and tear down TCP connections
- Makes use of signature/heuristic detection and anomaly detection
- May provide flow data protection
 - Requires that the application payload in a sequence of packets be reassembled
- Methods used to identify malicious packets:



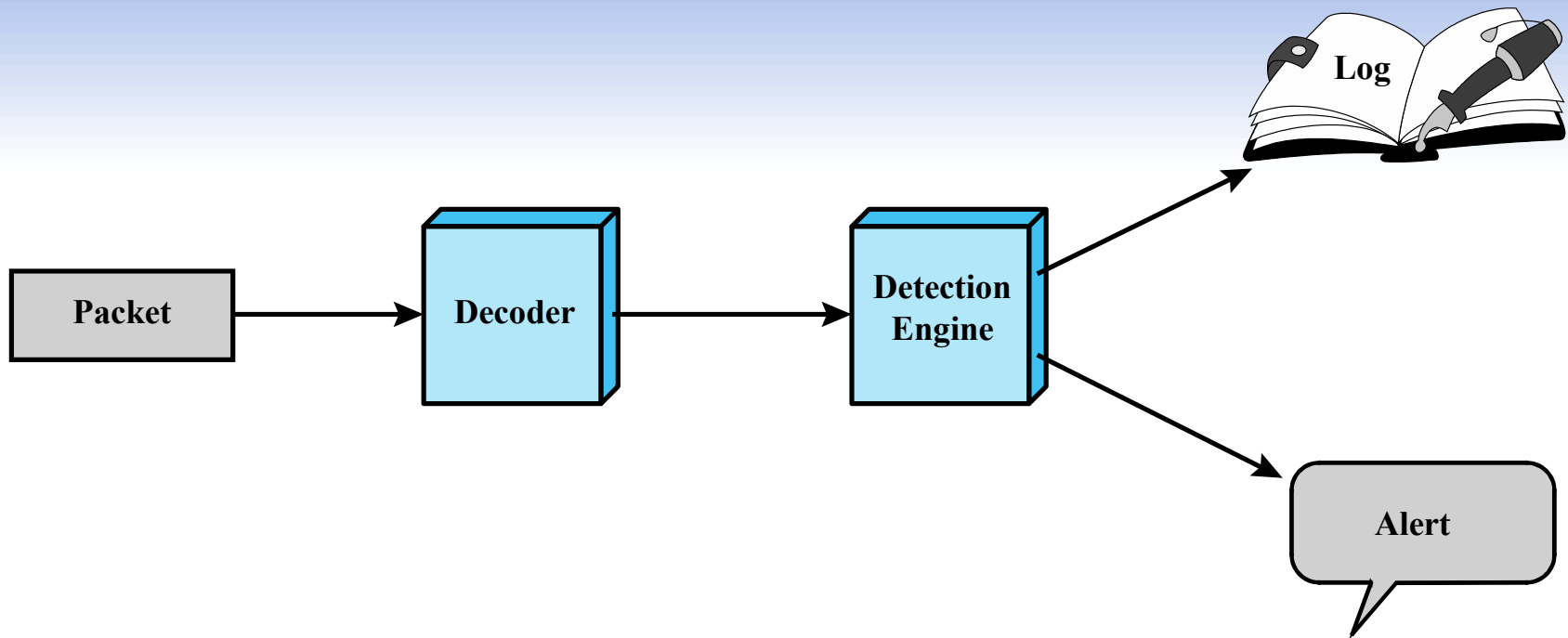
Pattern
matching

Stateful
matching

Protocol
anomaly

Traffic
anomaly

Statistical
anomaly



Snort Architecture

Snort Inline

- Enables Snort to function as an intrusion prevention system
- Includes a replace option which allows the Snort user to modify packets rather than drop them
 - Useful for a honeypot implementation
 - Attackers see the failure but cannot figure out why it occurred

Drop

Snort rejects a packet based on the options defined in the rule and logs the result

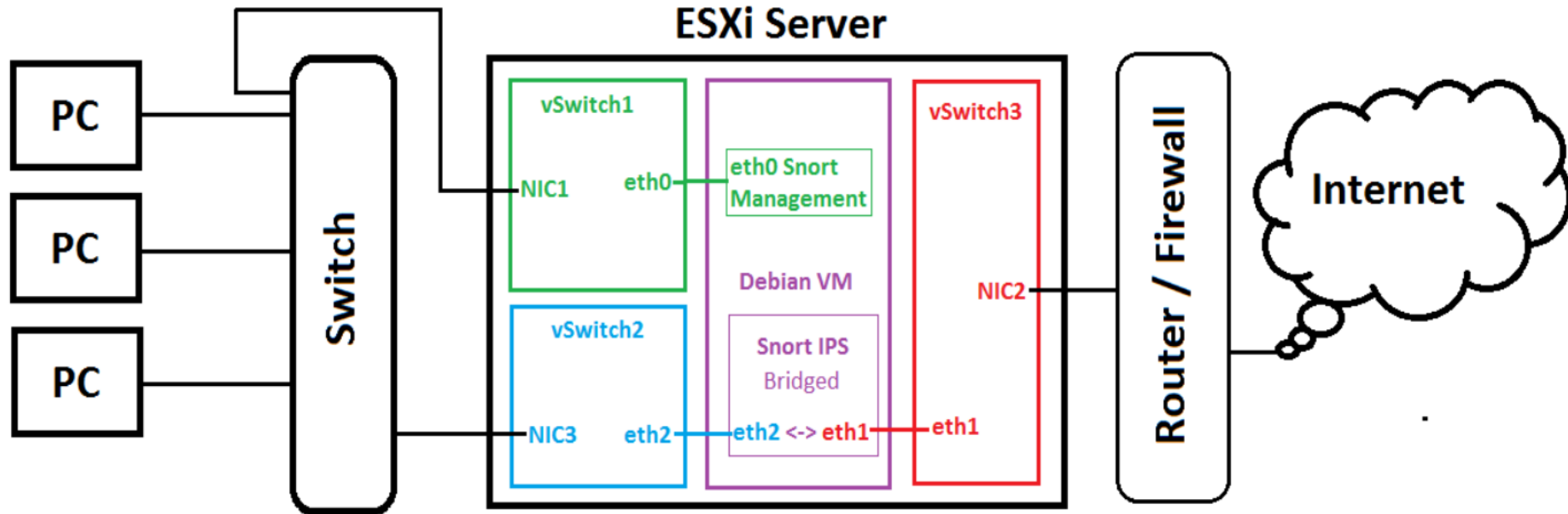
Reject

Packet is rejected and result is logged and an error message is returned

Sdrop

Packet is rejected but not logged

Snort Inline technical implementation



Digital Immune System

- Comprehensive defense against malicious behavior caused by malware
- Developed by IBM and refined by Symantec
- Motivation for this development includes the rising threat of Internet-based malware, the increasing speed of its propagation provided by the Internet, and the need to acquire a global view of the situation
- Success depends on the ability of the malware analysis system to detect new and innovative malware strains

Machine Learning in Intrusion Detection

- Anomaly detection – compare current trends and baselines
- Evolutionary algorithms – model application path of normal behavior identify error paths, and intrusion behavior
- Protocol verification – detect standard protocol interactions follow known paths
- Rule based and fuzzy rule based

Machine Learning in Intrusion Detection

- Artificial Neural Networks
 - Supervised learning – give it known attacks to learn what attacks look like in general or specific attack patterns
 - Unsupervised learning - Apply to complex event streams to model/learn what is normal and classify as normal or compromised.

Example success given sample attack training data

SENSITIVITY AND SPECIFICITY OF GP WITH HOMOLOGOUS CROSSOVER

Type of Attack	Sensitivity	Specificity
Smurf	99.93	99.95
Satan	100.00	99.64
IP Sweep	88.89	100.00
Port Sweep	86.36	100.00
Back	100.00	100.00
Normal	100.00	100.00
Buffer Overflow	100.00	100.00
WarezClient	66.67	99.97
Neptune	100.00	99.56