IDS
Lecture 15a

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

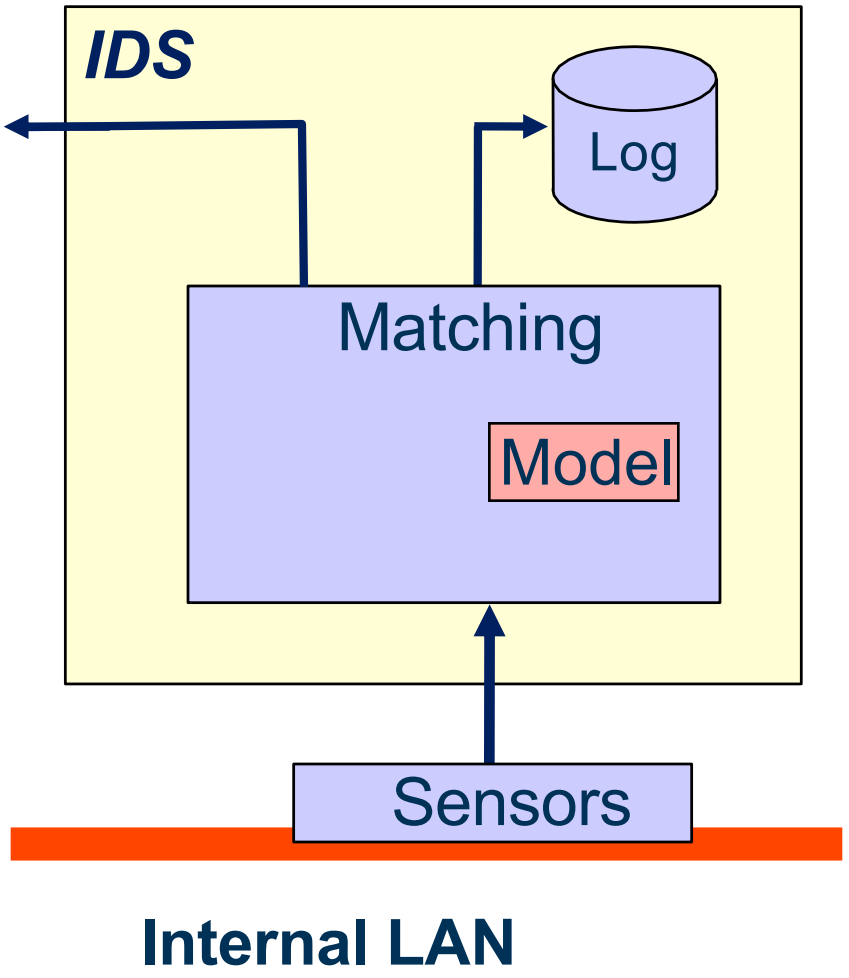
August 19, 2021

Source of some slides: **University of Twente** and **Northwestern University**

INTRUSION DETECTION SYSTEM (IDS)

- Intrusion detection is the process of **identifying** (and responding to) **malicious activities** targeted at computing and network resources

- Goal: Identify intrusions and report them



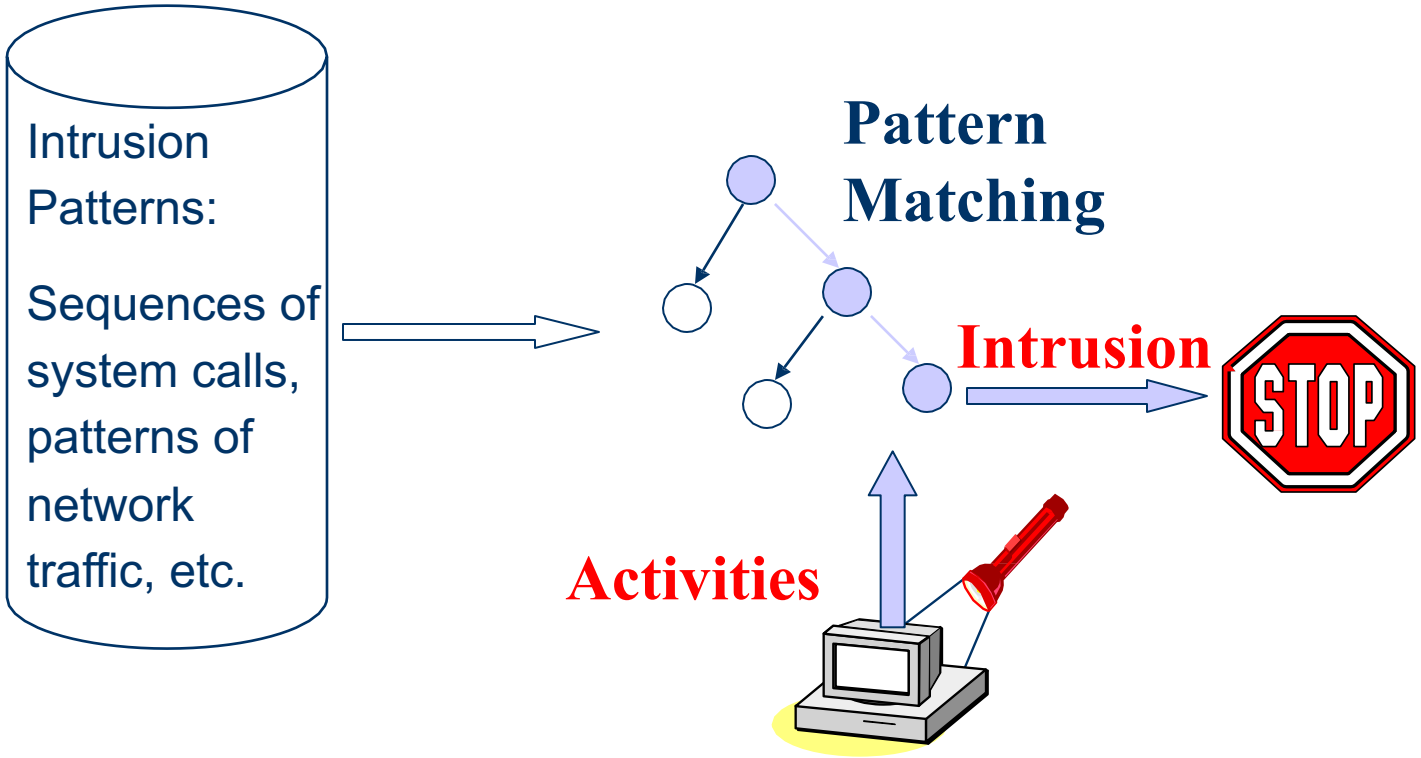
LOGICAL COMPONENTS

- Sensors
  - Collect data
  - Should operate at line speed
  - Based on pcap library
- Analyser
  - Determine if intrusion has occurred
- User interface
  - Manage / direct / view IDS

CLASSES OF IDS

- What type of analysis?
  - Signature-based IDS
  - Anomaly-based IDS

SIGNATURE-BASED DETECTION

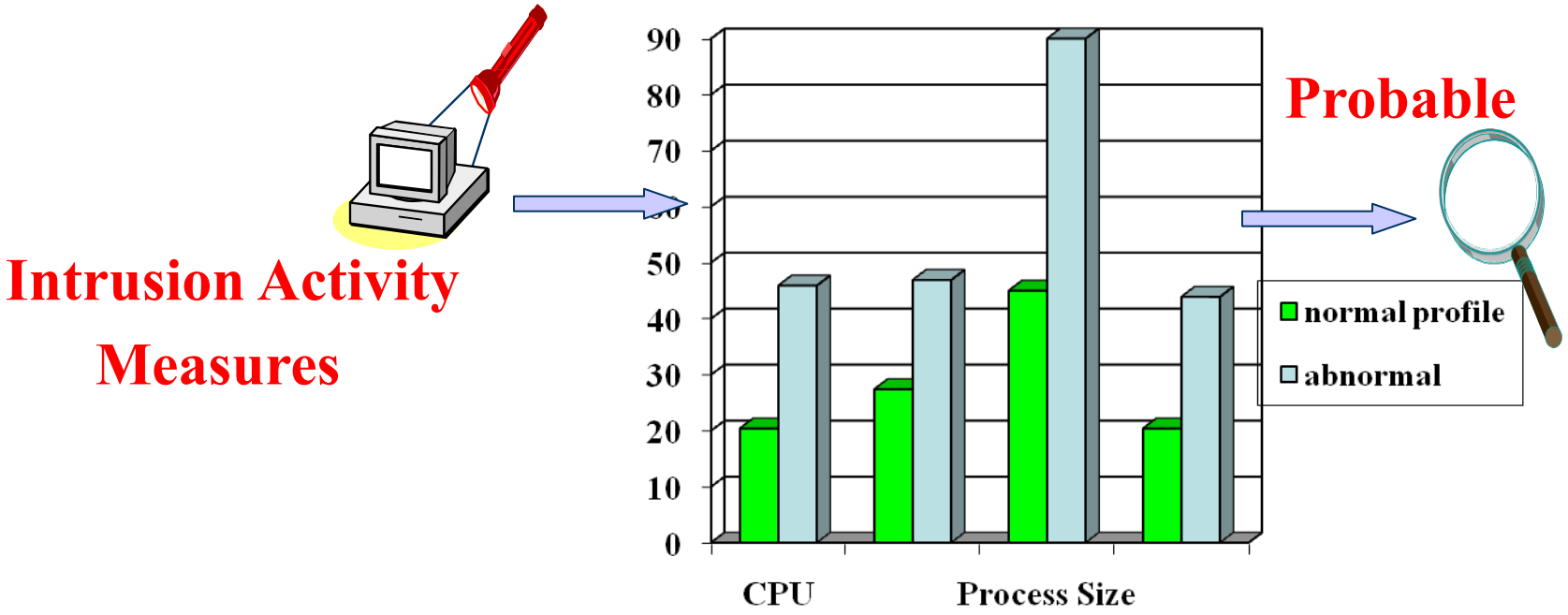


Example: *if* (traffic contains "x90+de[^\r\n]{30}")
then "attack detected"

Advantage: Mostly accurate. But problems?

We cannot detect new attacks

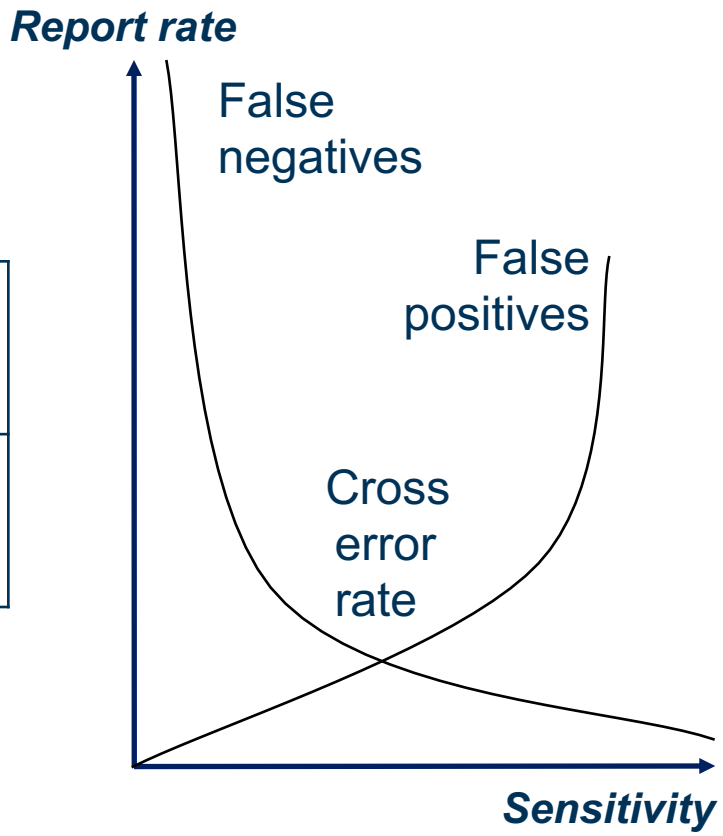
ANOMALY-BASED DETECTION



- Define a profile describing “normal” behaviour
- Then, detect deviations
- It can detect potential new attacks, any problem?
- Anomalies can just be new normal activities
- Relatively high false positive rates

IDS DECISIONS

True Positive This is really an attack	**False Negative** IDS fails to report a malicious activity
False Positive IDS reports legitimate activity as malicious	**True Negative** This is safe traffic



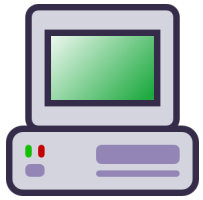
SIGNATURE-BASED VS ANOMALY-BASED DETECTION

Types	Advantage	Disadvantage
Signature-based detection	More accurate and easy to manage	Cannot detect novel/unknown attacks
Anomaly-based detection	Can detect novel/unknown attacks	High false alarm, more complex, and limited by training data

CLASSES OF IDS

- What type of analysis?
  - Signature-based IDS
  - Anomaly-based IDS
- Where is it operating?
  - Host-based IDS
  - Network-based IDS

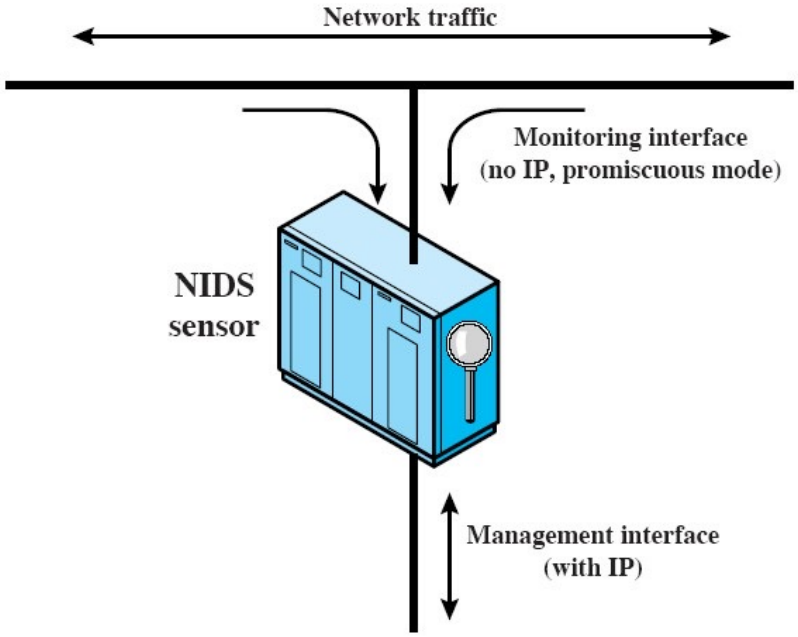
HOST-BASED IDS (HIDS)



- Uses **OS auditing and monitoring/analysis mechanisms** to find malware
  - Can execute full static and dynamic analysis of a program
    - Monitors shell **commands and system calls**
  - Has the most **comprehensive program info** for detection, thus **accurate**

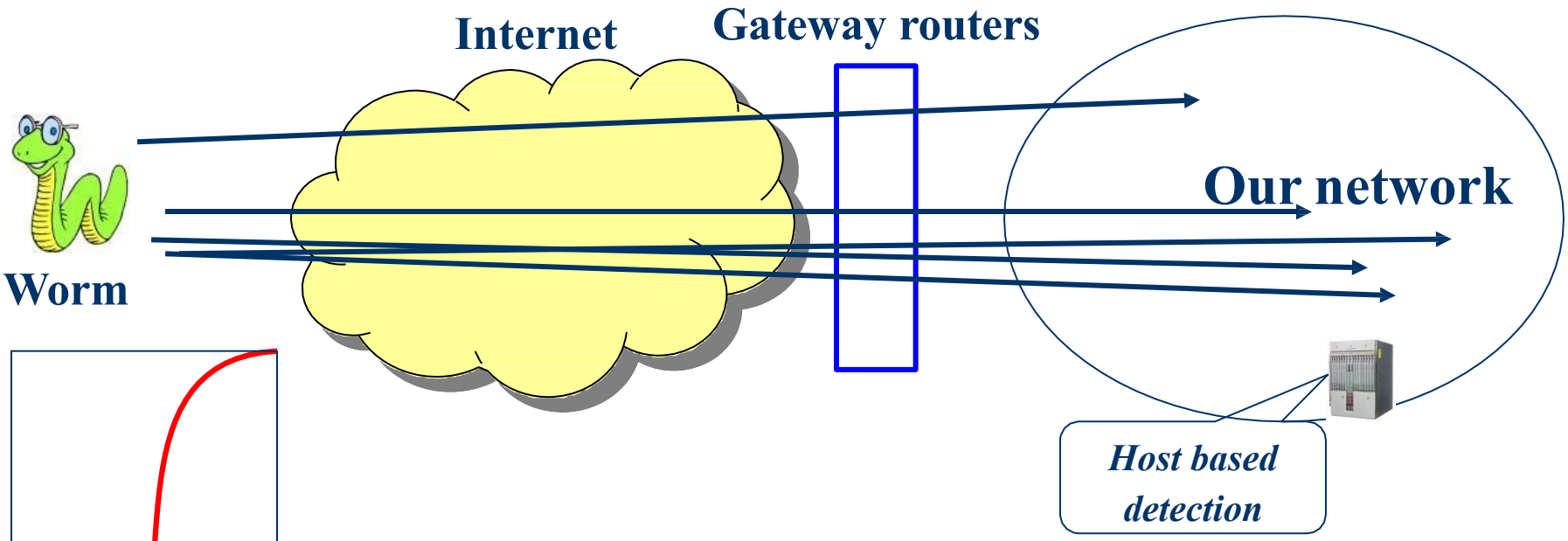
- Problems
  - User **dependent**: Install/update IDS on **all** user machines!
  - If an **attacker** takes over the machine, can tamper with IDS binaries and modify audit logs
  - Only **local view** of the attack

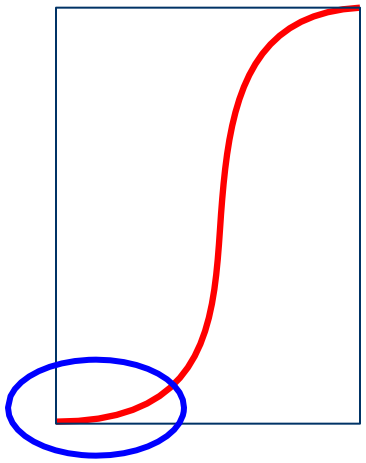
NETWORK-BASED IDS (NIDS)



- Monitors traffic at **selected points on a network**
- In (or near) **real-time** to detect intrusion patterns
- May **examine network**, transport, and/or application-level protocol activity directed toward systems
- Comprises a number of sensors
  - **Inline** (possibly as part of other network device)
  - **Passive** (monitors copy of traffic)

NIDS



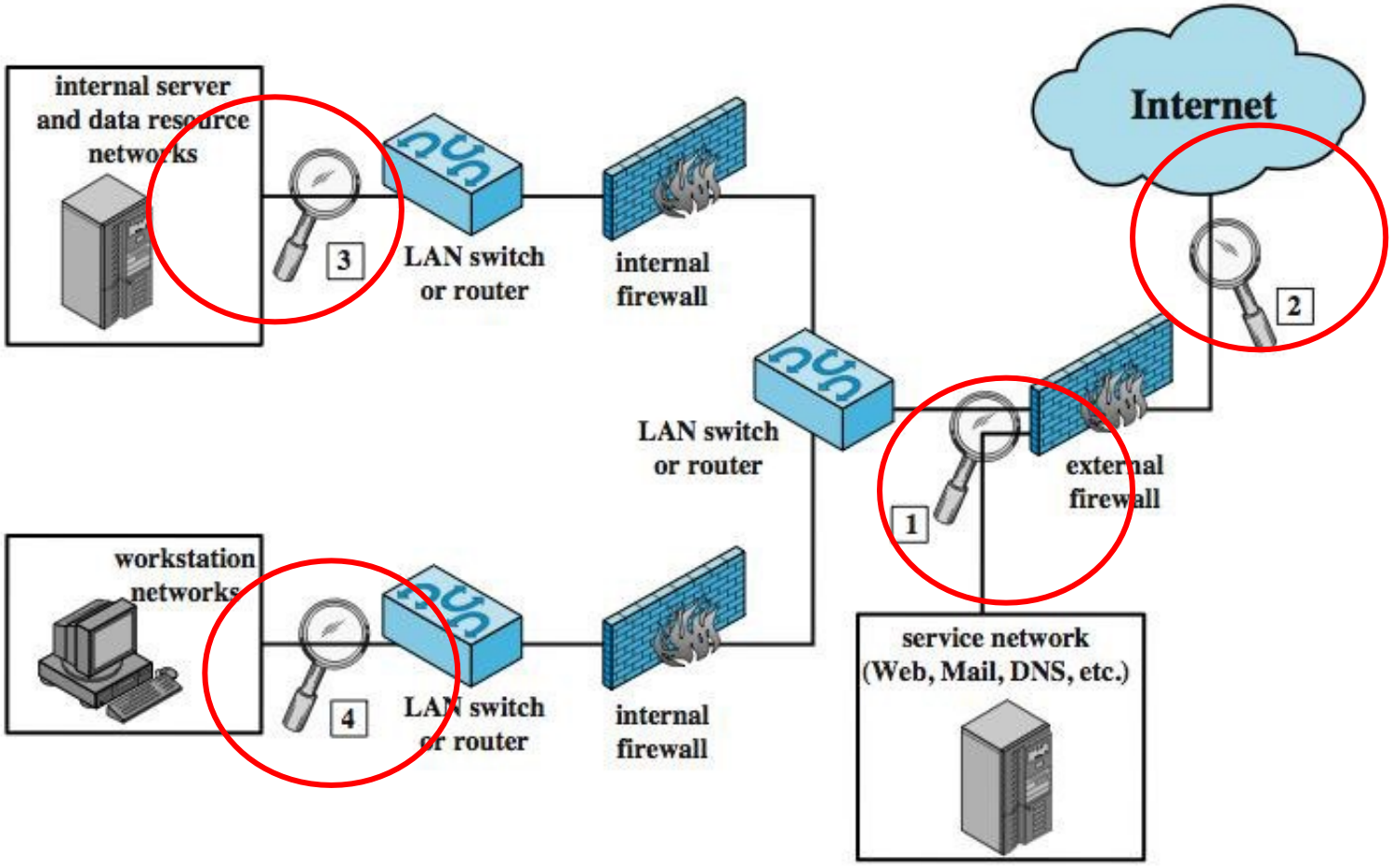


- At the early stage of the worm, only limited worm samples
- Host-based sensors can only cover limited IP space, which has scalability issues
- Thus, they might not be able to detect the worm in its early stage

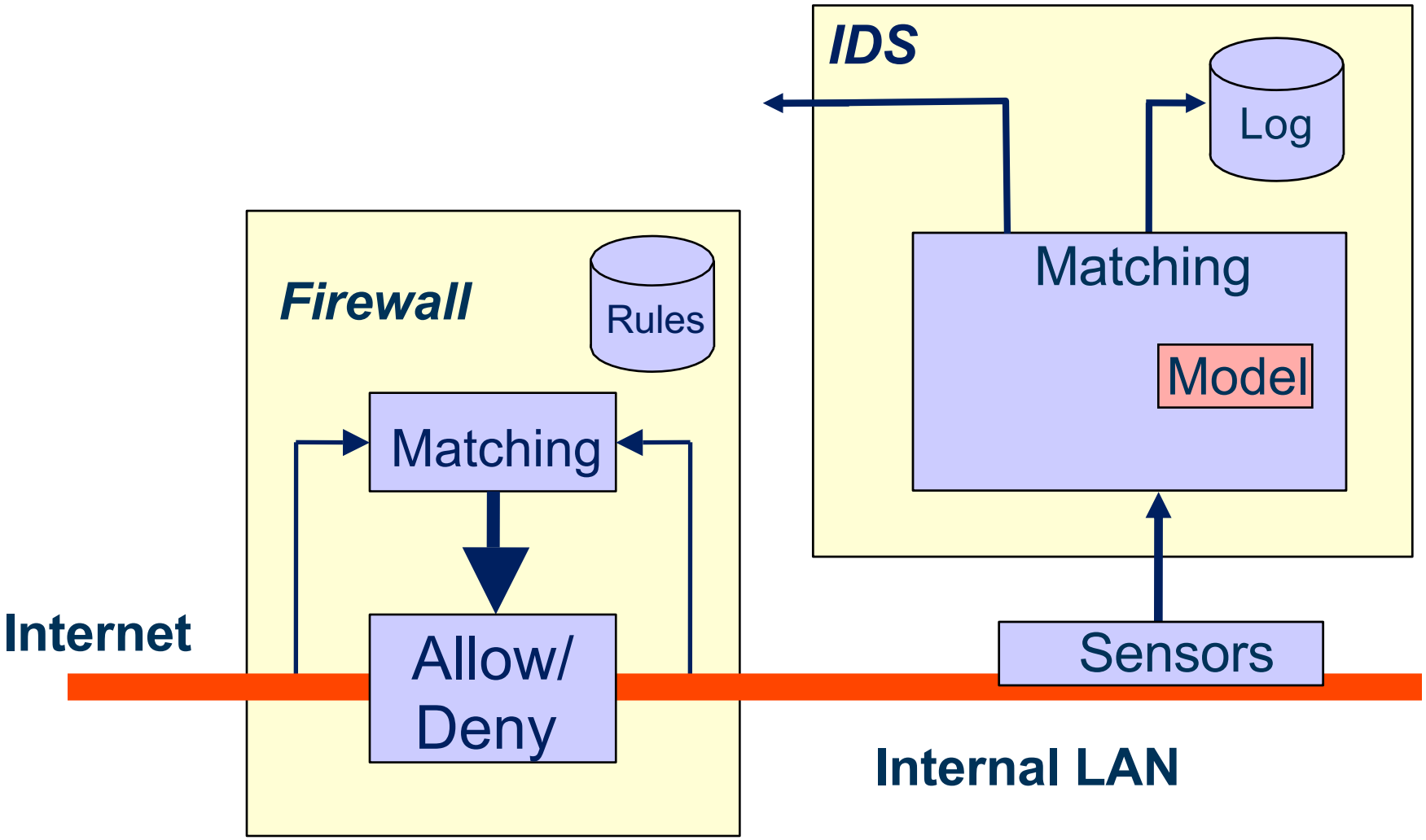
NIDS

- Deploying sensors at strategic locations
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
  - Look into the packet payload for malicious code
- Limitations
  - Cannot execute the payload or do any **code analysis**
  - Even Deep Packet Inspection (**DPI**) gives limited application-level semantic information
  - Record and process **huge amounts** of traffic
  - May be easily **defeated by encryption**, but can be mitigated with encryption only at the gateway/proxy

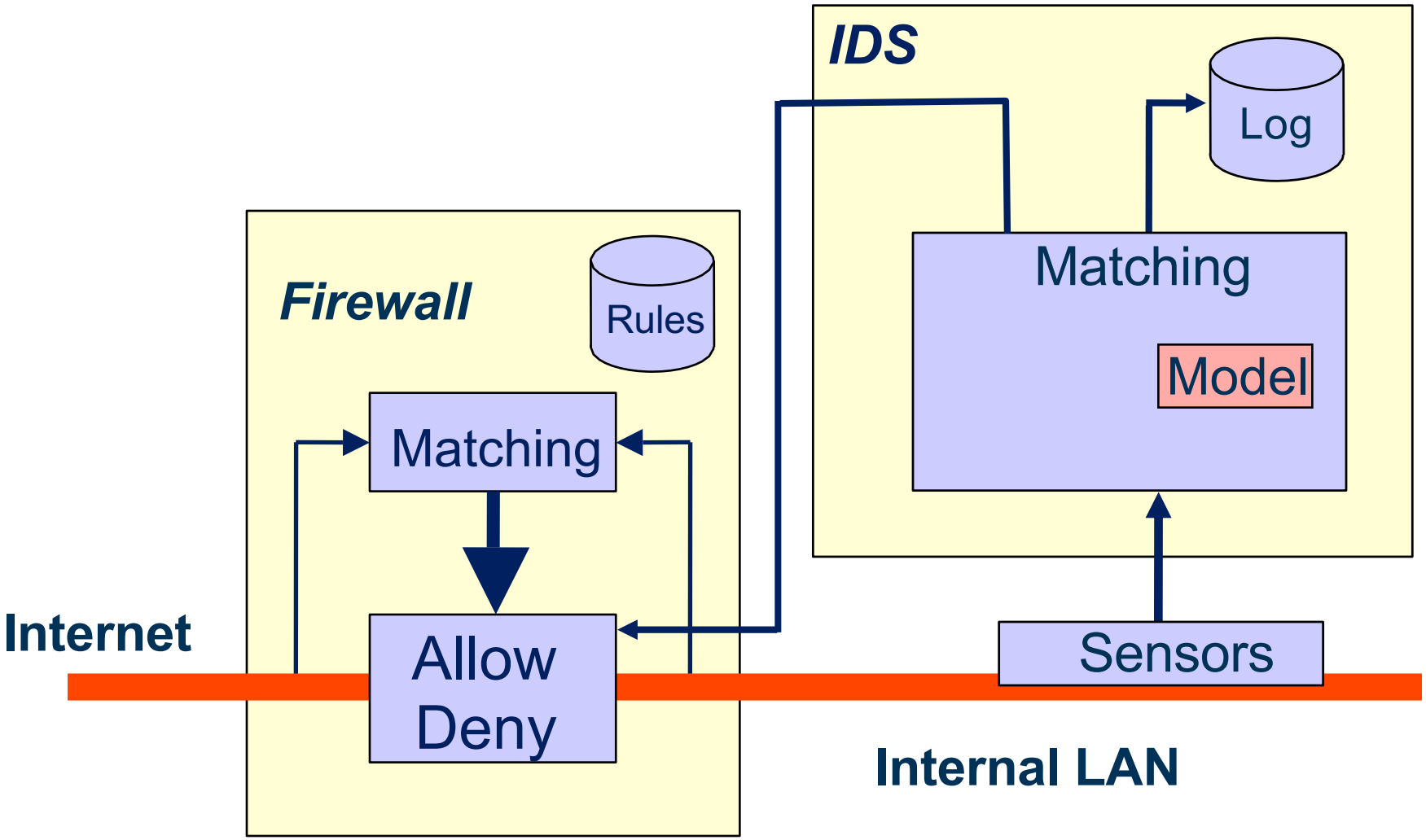
NIDS SENSOR DEPLOYMENT



PASSIVE IDS


IDS
Log
Matching
Model
Firewall
Rules
Matching
Allow/
Deny
Internet
Sensors
Internal LAN

REACTIVE IDS



HIDS VS NIDS

Types	Advantage	Disadvantage
HIDS	Less traffic volume and more accurate	More expensive
NIDS	Easy to deploy but difficult to bypass	Need to have the complete network topology

COMMERCIAL IDS

- Snort
  - Signature-based IDS
- Bro
  - NIDS
- Both are open-source systems

SUMMARY

- IDS aims at identifying malicious activities
- IDS components include sensors, analyser, and user interface
- IDS can be signature-based or anomaly-based
- Signature-based IDS is more accurate but cannot detect new attacks
- Anomaly-based IDS can detect new attacks but depends on training data
- Based on its operating, IDS can be host-based or network-based

RESOURCES

- Read Chapter 9 of
  Network Security Essentials – Applications and Standards
  Fourth Edition
  William Stallings
  Prentice Hall
  ISBN 0-13-706792-5

Questions?

Thanks for your attention!