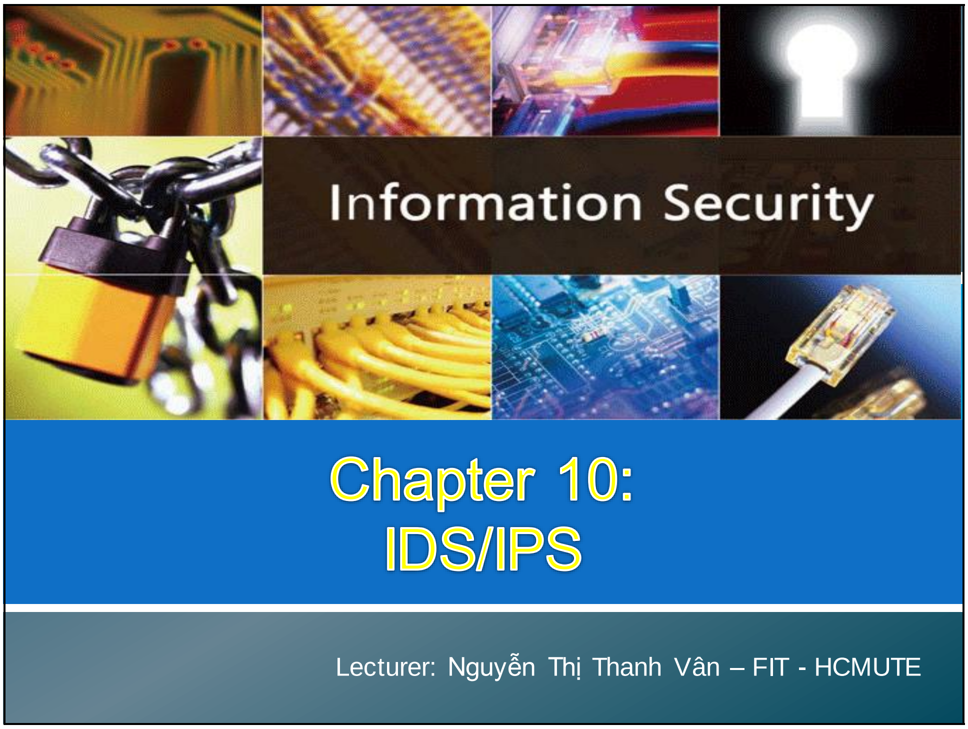
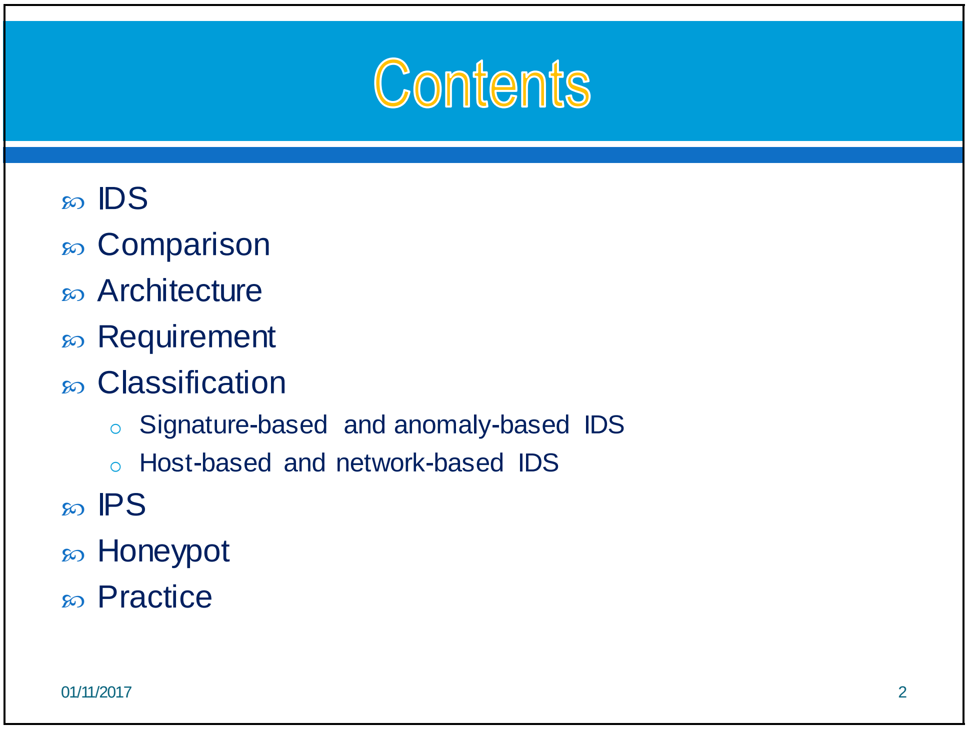


Information Security

Chapter 10: IDS/IPS

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

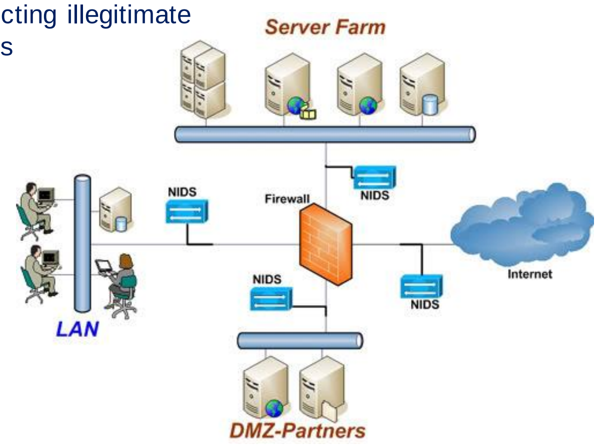


Contents

- IDS
- Comparison
- Architecture
- Requirement
- Classification
  - Signature-based and anomaly-based IDS
  - Host-based and network-based IDS
- IPS
- Honeypot
- Practice

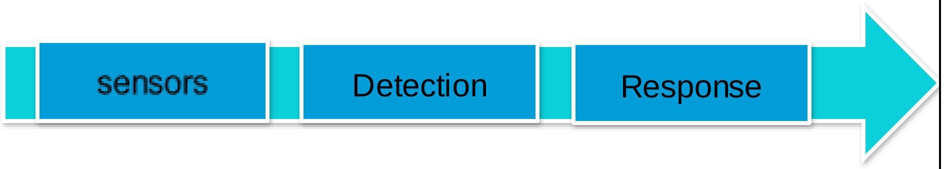
Intrusion Detection Systems

- IDS:
  - is a system of devices or applications
  - has capability of detecting illegitimate intrusions on networks



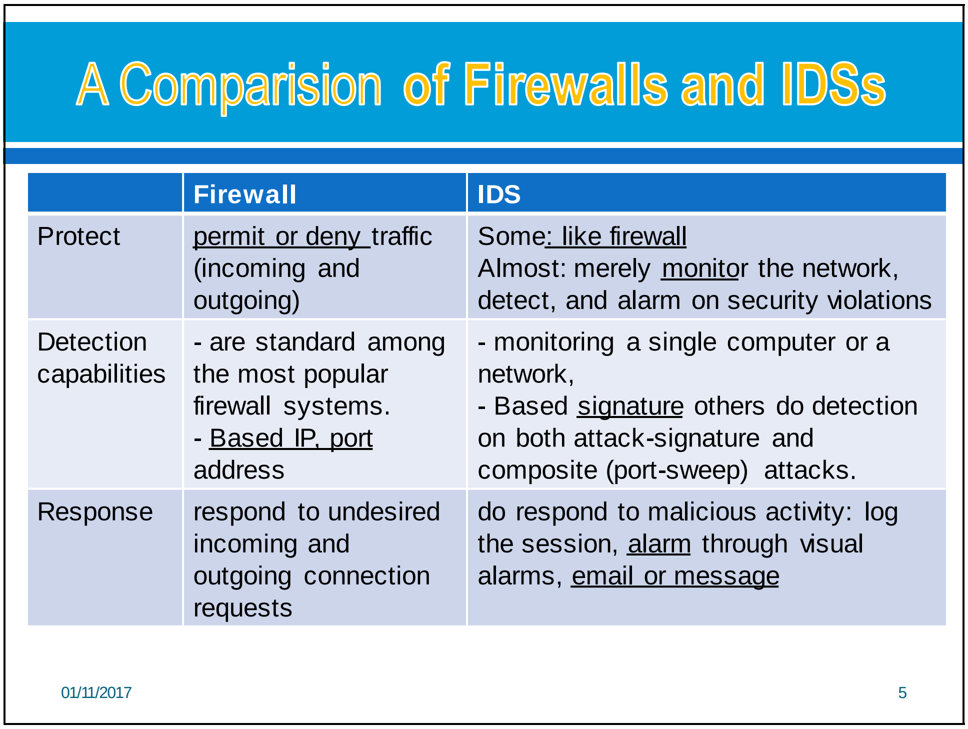
Intrusion Detection Systems

- Logical components:
  - sensors - collect data
  - Detection (Analyzers) - determine if intrusion has occurred
  - Response (user interface) - manage /direct /view IDS


sensors

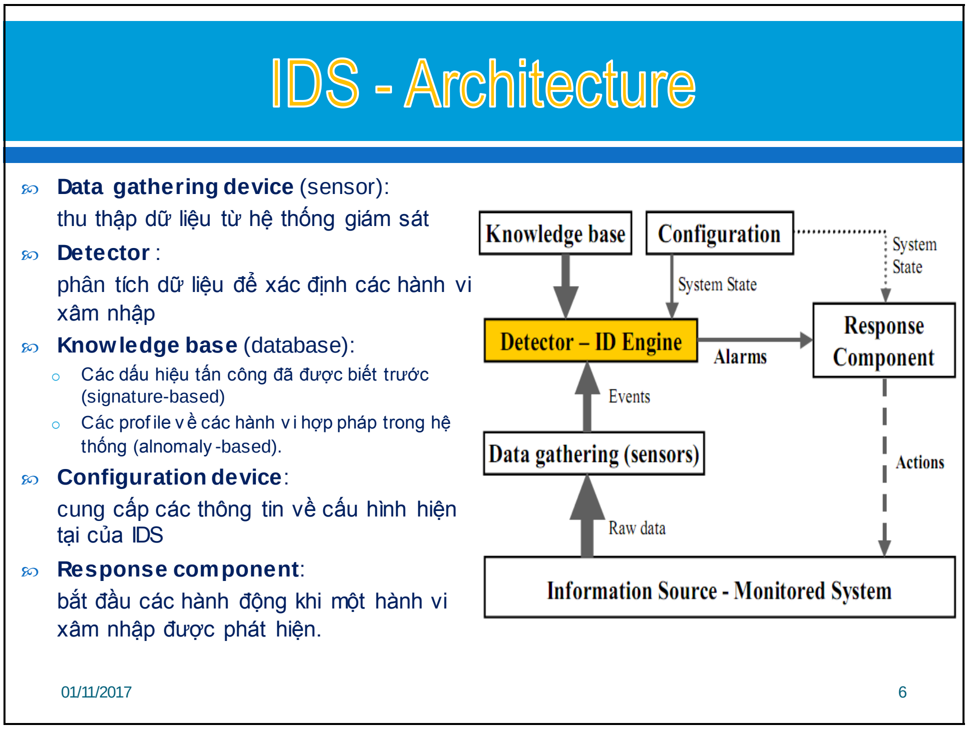
Detection

Response



A Comparision of Firewalls and IDSs

	Firewall	IDS
Protect	permit or deny traffic (incoming and outgoing)	Some: like firewall Almost: merely monitor the network, detect, and alarm on security violations
Detection capabilities	- are standard among the most popular firewall systems. - Based IP, port address	- monitoring a single computer or a network, - Based signature others do detection on both attack-signature and composite (port-sweep) attacks.
Response	respond to undesired incoming and outgoing connection requests	do respond to malicious activity: log the session, alarm through visual alarms, email or message



IDS - Architecture

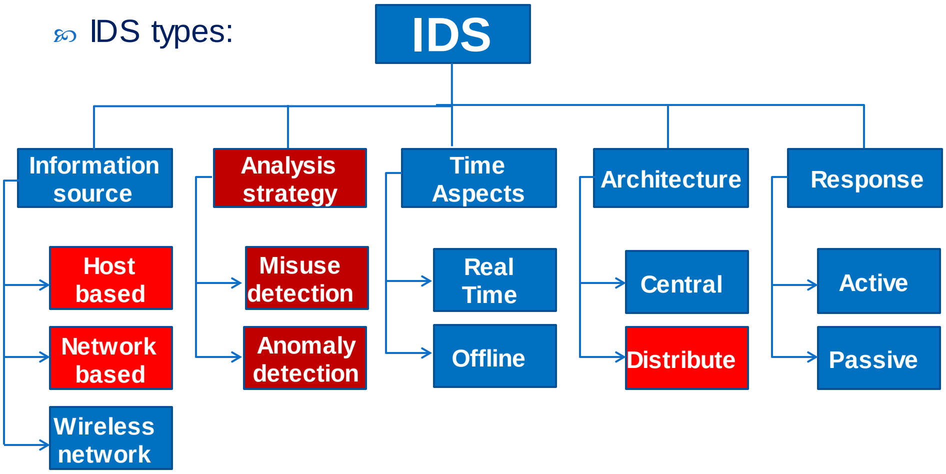
- **Data gathering device** (sensor):
  thu thập dữ liệu từ hệ thống giám sát
- **Detector** :
  phân tích dữ liệu để xác định các hành vi xâm nhập
- **Knowledge base** (database):
  - Các dấu hiệu tấn công đã được biết trước (signature-based)
  - Các profile về các hành vi hợp pháp trong hệ thống (alnomaly-based).
- **Configuration device**:
  cung cấp các thông tin về cấu hình hiện tại của IDS
- **Response component**:
  bắt đầu các hành động khi một hành vi xâm nhập được phát hiện.

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

IDS Classification

- IDS types:



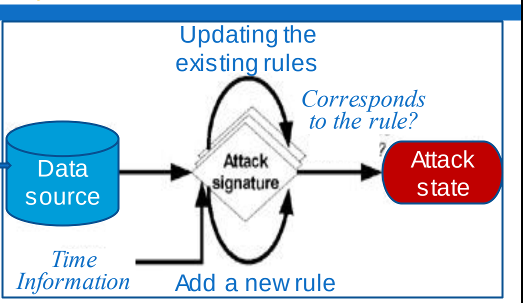
IDS

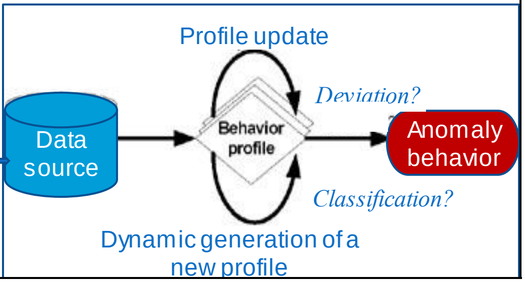
- Information source
  - Host based
  - Network based
  - Wireless network
- Analysis strategy
  - Misuse detection
  - Anomaly detection
- Time Aspects
  - Real Time
  - Offline
- Architecture
  - Central
  - Distribute
- Response
  - Active
  - Passive

Two IDS types – Signature-based IDS and anomaly-based IDS

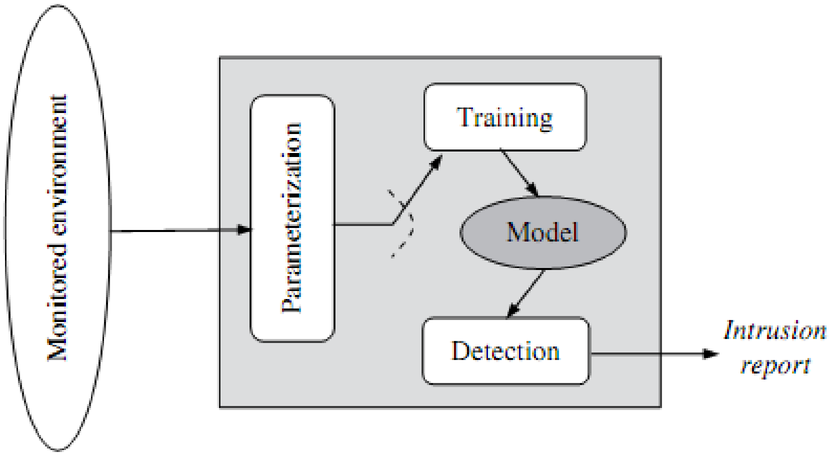
- Signature-based
  - Depend on matching patterns that are collected from known attacks

- Anomaly-based
  - Thru continuous observation and modeling of normal behavior, the system finds possible threats via deviation from the normal model or a classification executed





Anomaly Detection



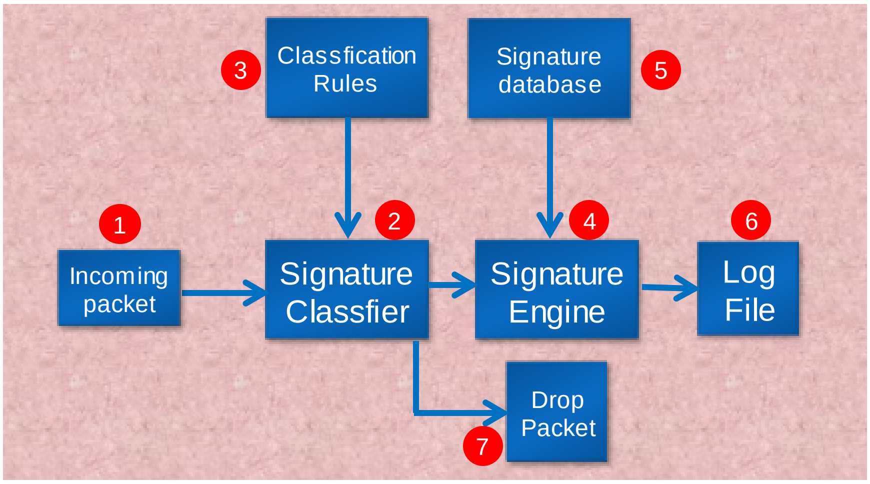
Anomaly Detection

- threshold detection
  - checks excessive event occurrences over time
  - alone a crude and ineffective intruder detector
  - must determine both thresholds and time intervals
- profile based
  - characterize past behavior of users / groups
  - then detect significant deviations
  - based on analysis of audit records
    - gather metrics: counter, guage, interval timer, resource utilization
    - analyze: mean and standard deviation, multivariate, markov process, time series

Anomaly Detection

- Advantage:
  - detect insider attacks based on collected normal activities in the system;
  - ability to detect previously unknown attacks; and
  - it is very difficult for an attacker to know which certainty activity can be executed without generate an alarm.
- Limits:
  - the system must go through a training period in which appropriate user profiles are created by defining normal traffic profiles, that is a difficult task and consumes a lot time.
  - Because it is looking for anomalous events rather than attacks, so they will generate false alarms when there is an anomalous behavior but not an attack

Signature-based: basic Architecture



1 Incoming packet

2 Signature Classfier

3 Classfication Rules

4 Signature Engine

5 Signature database

6 Log File

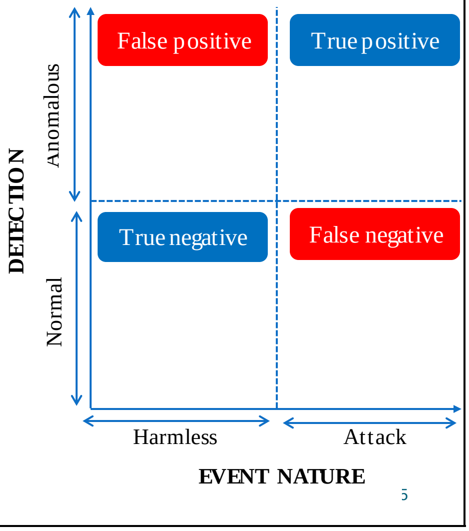
7 Drop Packet

Signature Detection

- observe events on system and applying a set of rules to decide if intruder
- approaches:
  - rule-based anomaly detection
    - analyze historical audit records for expected behavior, then match with current behavior
  - rule-based penetration identification
    - rules identify known penetrations / weaknesses
    - often by analyzing attack scripts from Internet
    - supplemented with rules from security experts

Two IDS types – Pos & cons

- Signature-based
  - (+) Detect known attacks
  - (-) False negative alarm
  - (-) Can penetrate to know signatures, then another method is used to attack
- Anomaly-based
  - (+) Detect unknown attacks
  - (-) False positive alarm
  - (+) Can't penetrate to know certainty activity can be executed without generate an alarm.



DETECTION	Harmless	Attack
Anomalous	False positive	True positive
Normal	True negative	False negative

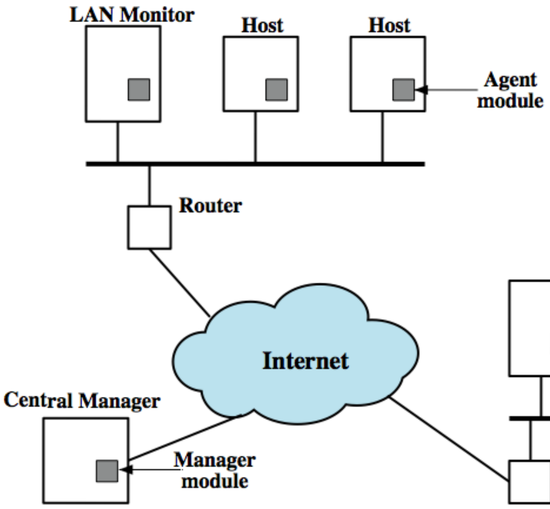
EVENT NATURE

01/11/2017 5

Host-Based IDS

- specialized software to monitor system activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions
- two approaches, often used in combination:
  - anomaly detection - defines normal/expected behavior
    - threshold detection
    - profile based
  - signature detection - defines proper behavior

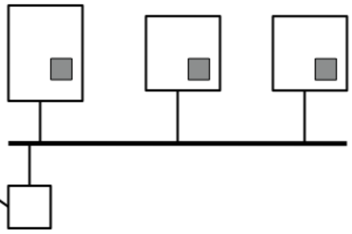
Distributed Host-Based IDS



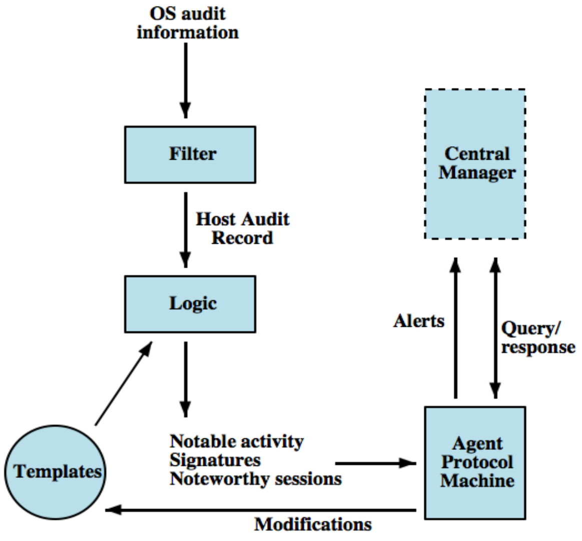
Host AM: collect data on security-related events on the host and transmit these to the central manager

LAN Monitor: + analyzes LAN traffic and reports the results to the central manager.

Central manager module: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion.



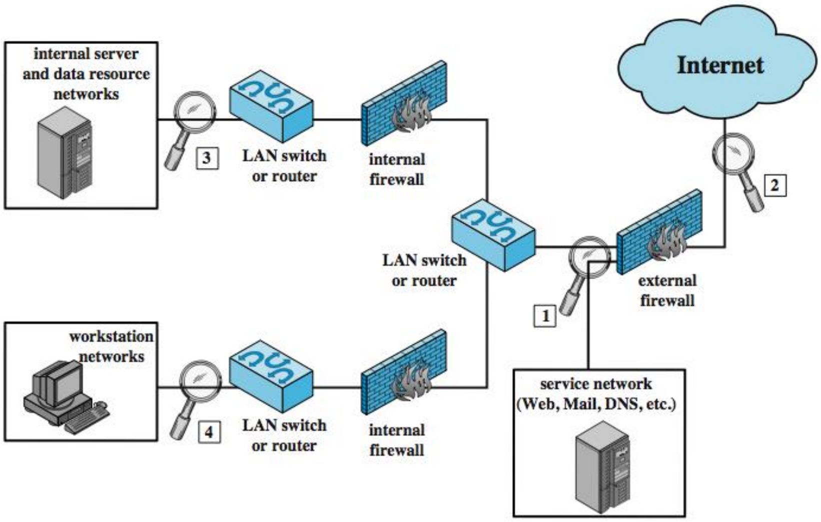
Distributed Host-Based IDS



Network-Based IDS

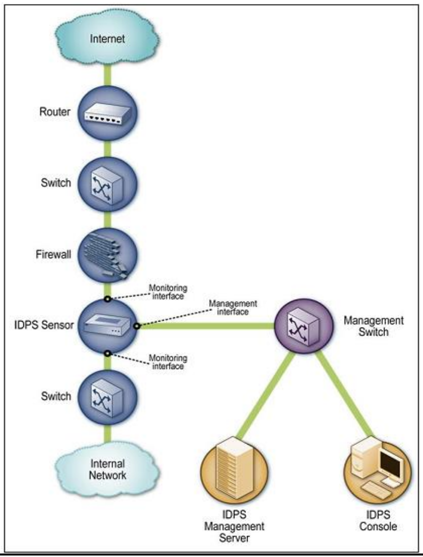
- network-based IDS (NIDS)
  - monitor traffic at selected points on a network
  - in (near) real time to detect intrusion patterns
  - may examine network, transport and/or application level protocol activity directed toward systems
- comprises a number of sensors
  - inline (possibly as part of other net device)
  - passive (monitors copy of traffic)

NIDS Sensor Deployment



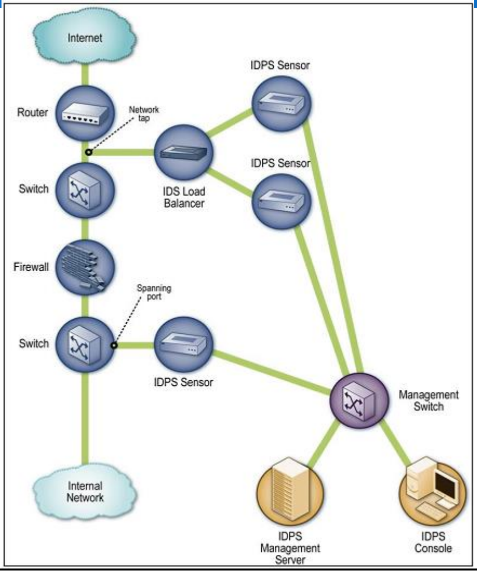
Network-Based IDS

- Sensor Inline



Network-Based IDS

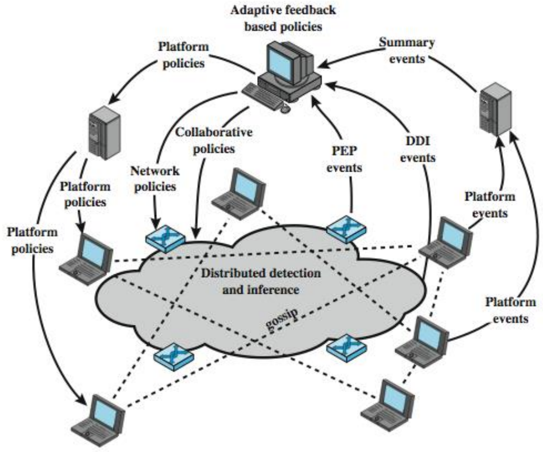
- Sensor **Passive**



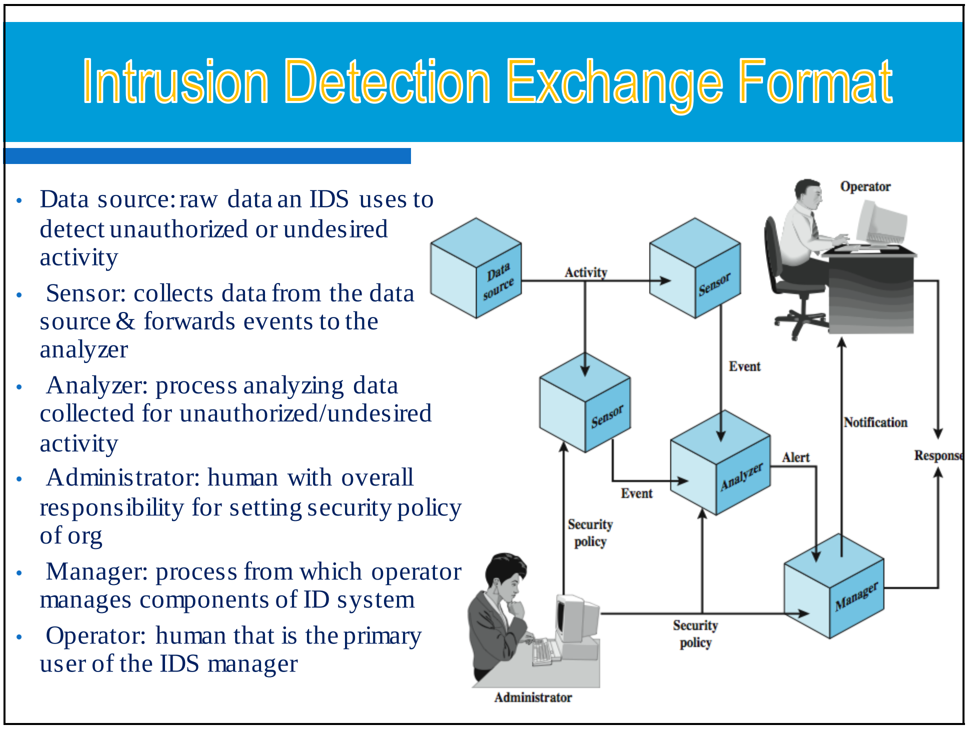
Intrusion Detection Techniques in NIDS

- signature detection
  - at application, transport, network layers; unexpected application services, policy violations
- anomaly detection
  - of denial of service attacks, scanning, worms
- when potential violation detected sensor sends an alert and logs information
  - used by analysis module to refine intrusion detection parameters and algorithms
  - by security admin to improve protection

Distributed Adaptive Intrusion Detection



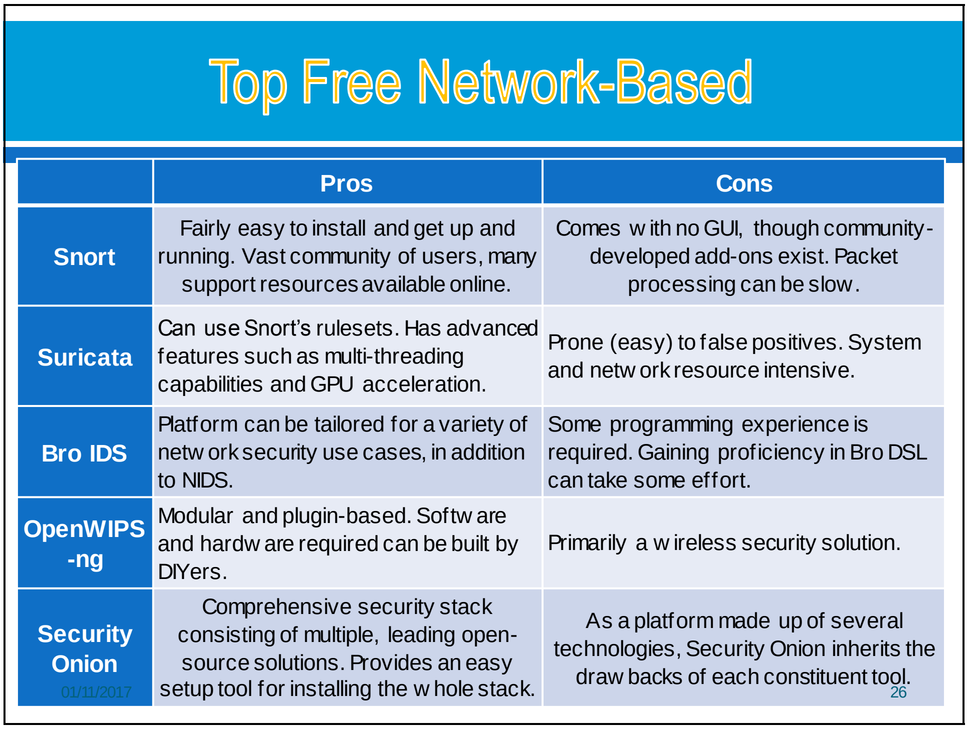
PEP = policy enforcement point
DDI = distributed detection and inference



Intrusion Detection Exchange Format

- Data source: raw data an IDS uses to detect unauthorized or undesired activity
- Sensor: collects data from the data source & forwards events to the analyzer
- Analyzer: process analyzing data collected for unauthorized/undesired activity
- Administrator: human with overall responsibility for setting security policy of org
- Manager: process from which operator manages components of ID system
- Operator: human that is the primary user of the IDS manager

Operator
Data source
Activity
Sensor
Event
Sensor
Notification
Analyzer
Alert
Response
Event
Security policy
Manager
Security policy
Administrator

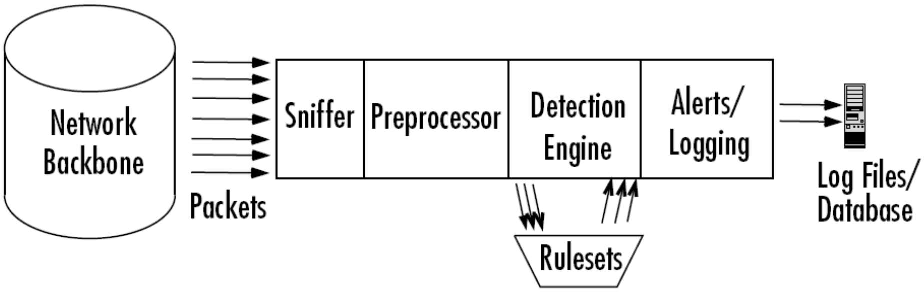


Top Free Network-Based

	Pros	Cons
Snort	Fairly easy to install and get up and running. Vast community of users, many support resources available online.	Comes with no GUI, though community-developed add-ons exist. Packet processing can be slow.
Suricata	Can use Snort's rulesets. Has advanced features such as multi-threading capabilities and GPU acceleration.	Prone (easy) to false positives. System and network resource intensive.
Bro IDS	Platform can be tailored for a variety of network security use cases, in addition to NIDS.	Some programming experience is required. Gaining proficiency in Bro DSL can take some effort.
OpenWIPS-ng	Modular and plugin-based. Software and hardware required can be built by DIYers.	Primarily a wireless security solution.
Security Onion	Comprehensive security stack consisting of multiple, leading open-source solutions. Provides an easy setup tool for installing the whole stack.	As a platform made up of several technologies, Security Onion inherits the drawbacks of each constituent tool.

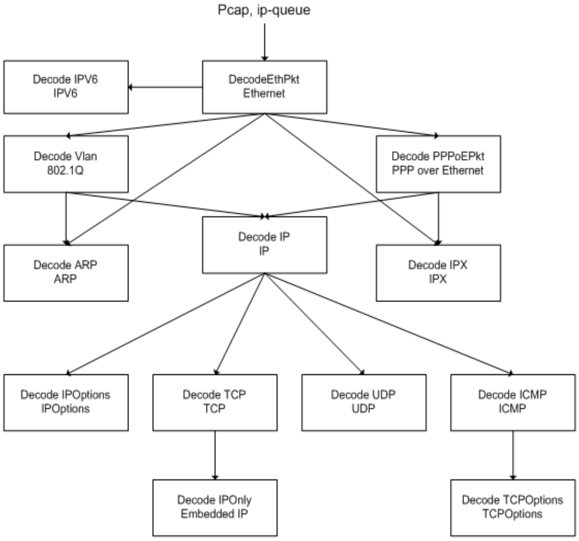
SNORT

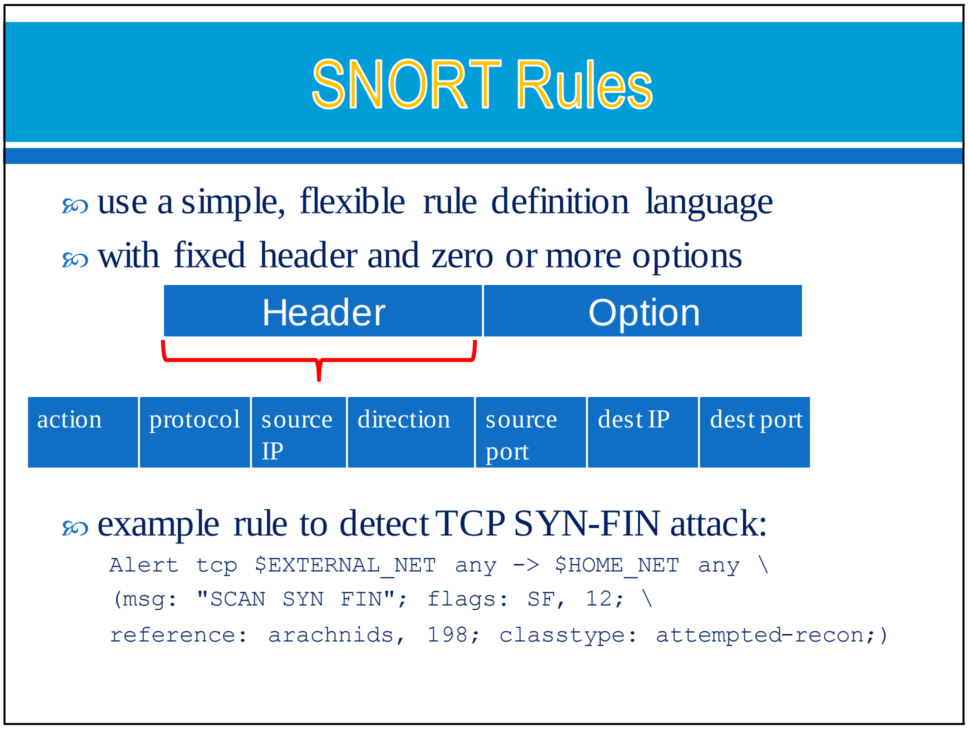
- lightweight IDS
  - real-time packet capture and rule analysis
  - passive or inline



SNORT

- **Packet Decoder**





SNORT Rules

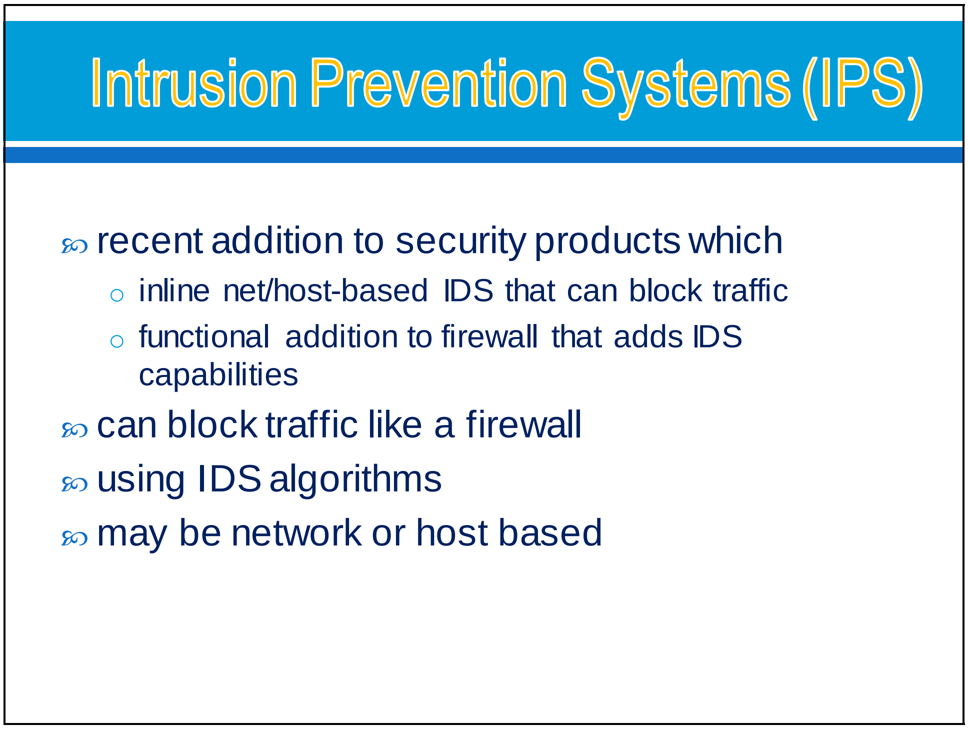
- use a simple, flexible rule definition language
- with fixed header and zero or more options

Header	Option

action	protocol	source IP	direction	source port	dest IP	dest port

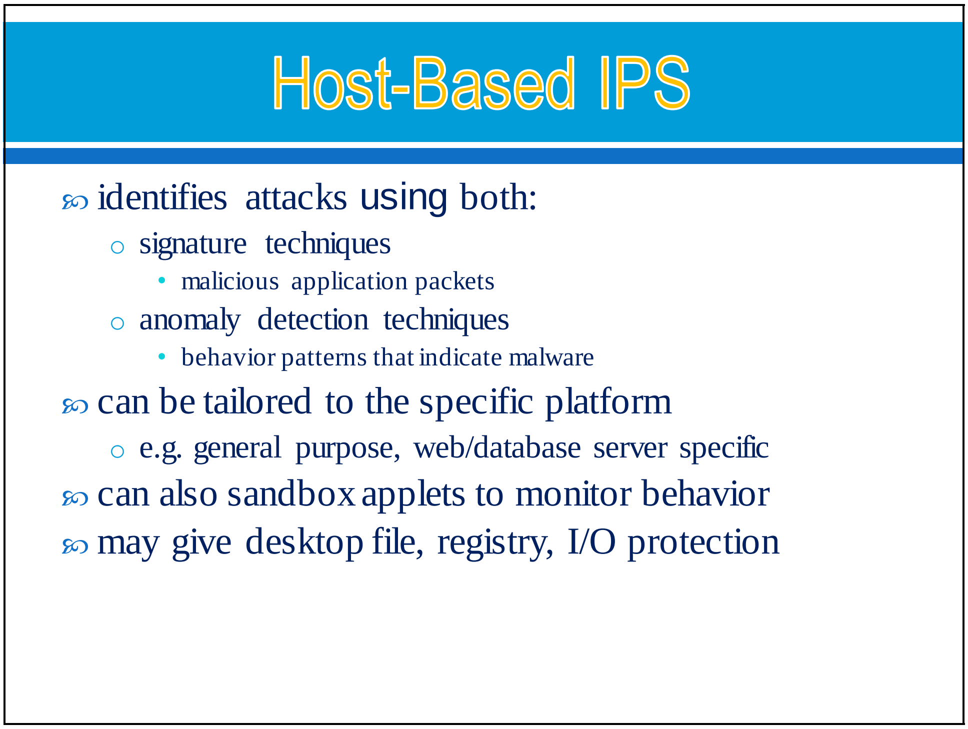
- example rule to detect TCP SYN-FIN attack:

```
Alert tcp $EXTERNAL_NET any -> $HOME_NET any \
(msg: "SCAN SYN FIN"; flags: SF, 12; \
reference: arachnids, 198; classtype: attempted-recon;)
```



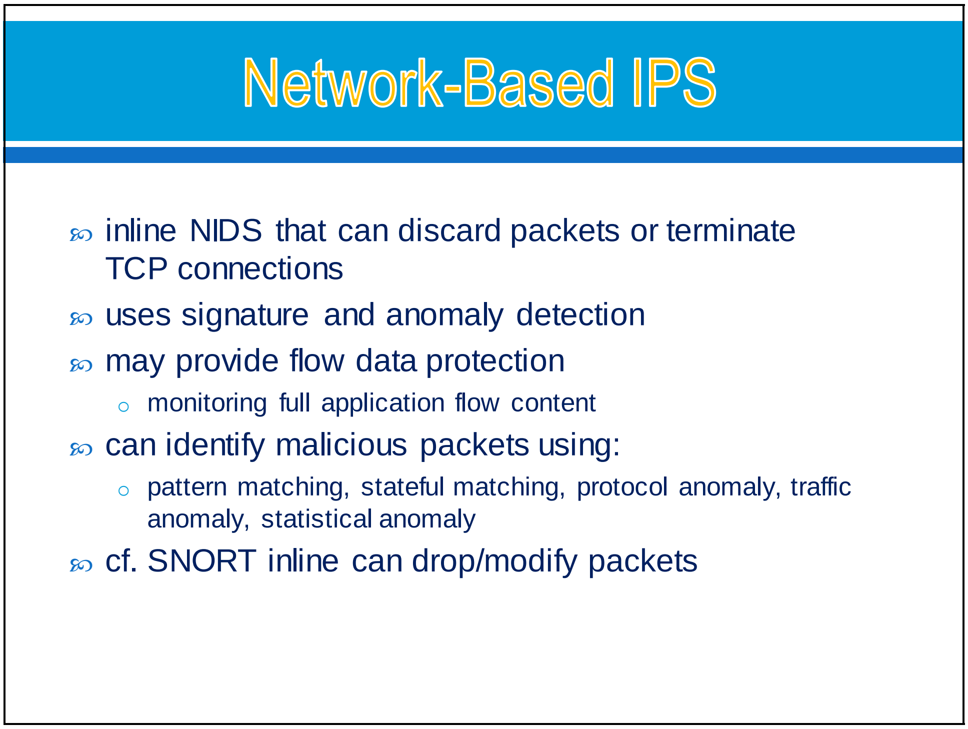
Intrusion Prevention Systems (IPS)

- recent addition to security products which
  - inline net/host-based IDS that can block traffic
  - functional addition to firewall that adds IDS capabilities
- can block traffic like a firewall
- using IDS algorithms
- may be network or host based



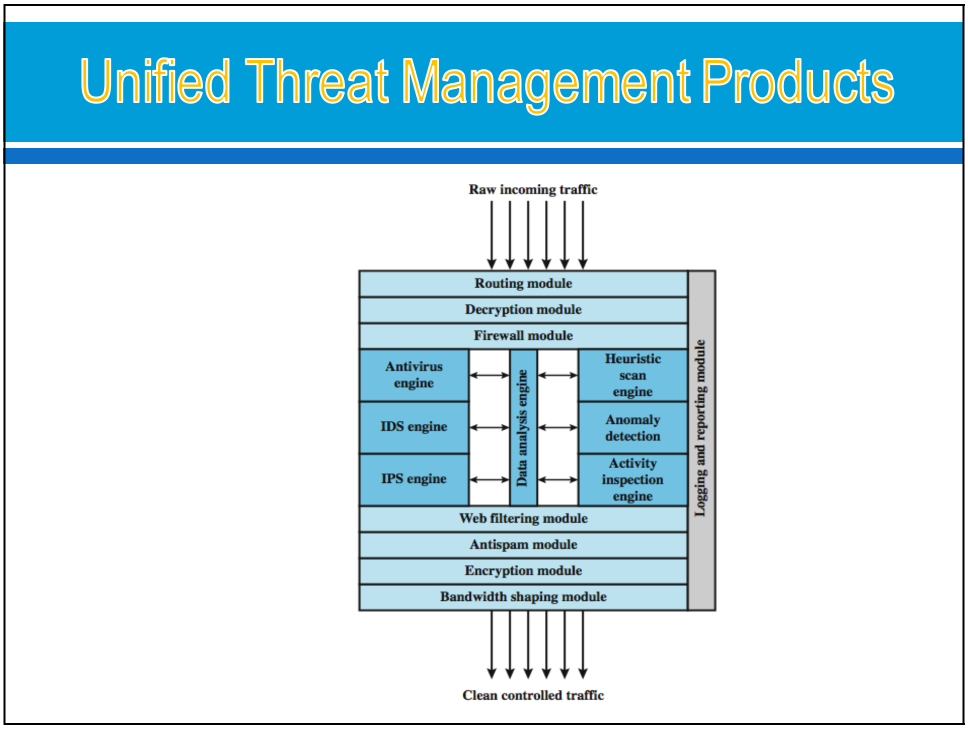
Host-Based IPS

- identifies attacks using both:
  - signature techniques
    - malicious application packets
  - anomaly detection techniques
    - behavior patterns that indicate malware
- can be tailored to the specific platform
  - e.g. general purpose, web/database server specific
- can also sandbox applets to monitor behavior
- may give desktop file, registry, I/O protection



Network-Based IPS

- inline NIDS that can discard packets or terminate TCP connections
- uses signature and anomaly detection
- may provide flow data protection
  - monitoring full application flow content
- can identify malicious packets using:
  - pattern matching, stateful matching, protocol anomaly, traffic anomaly, statistical anomaly
- cf. SNORT inline can drop/modify packets



Unified Threat Management Products

Raw incoming traffic

Routing module

Decryption module

Firewall module

Antivirus engine

IDS engine

IPS engine

Data analysis engine

Heuristic scan engine

Anomaly detection

Activity inspection engine

Web filtering module

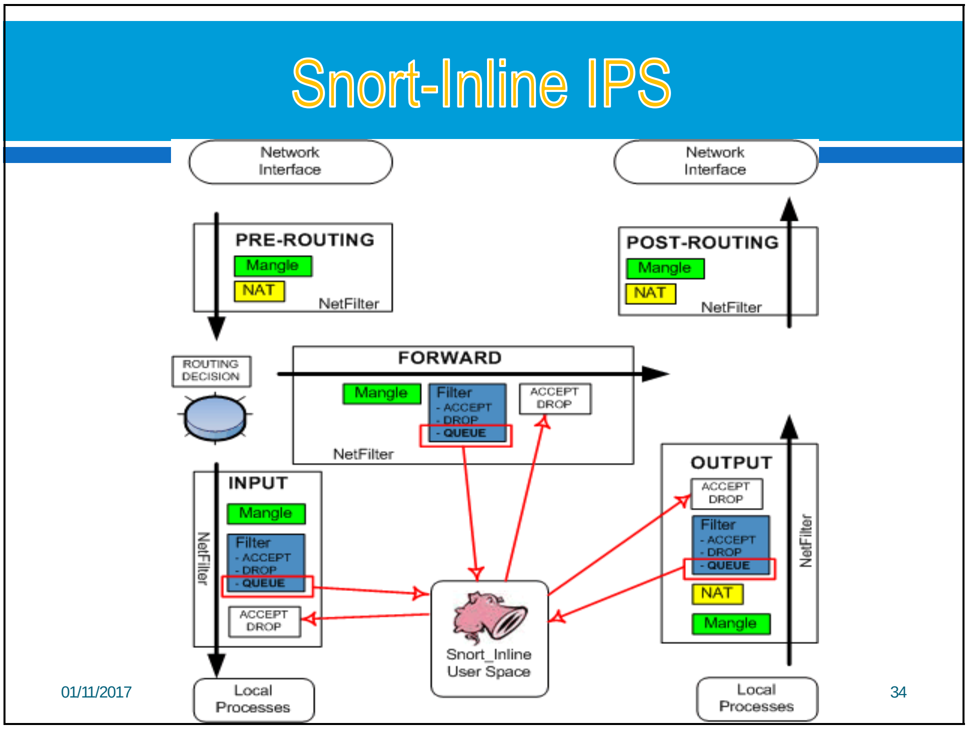
Antispam module

Encryption module

Bandwidth shaping module

Logging and reporting module

Clean controlled traffic



Snort-Inline IPS

Network Interface

Network Interface

PRE-ROUTING

Mangle

NAT

NetFilter

POST-ROUTING

Mangle

NAT

NetFilter

ROUTING DECISION

FORWARD

Mangle

Filter
- ACCEPT
- DROP
- QUEUE

ACCEPT DROP

NetFilter

INPUT

Mangle

Filter
- ACCEPT
- DROP
- QUEUE

ACCEPT DROP

NetFilter

OUTPUT

ACCEPT DROP

Filter
- ACCEPT
- DROP
- QUEUE

NAT

Mangle

NetFilter

Snort_Inline User Space

Local Processes

Local Processes

01/11/2017 34

Snort-Inline modes

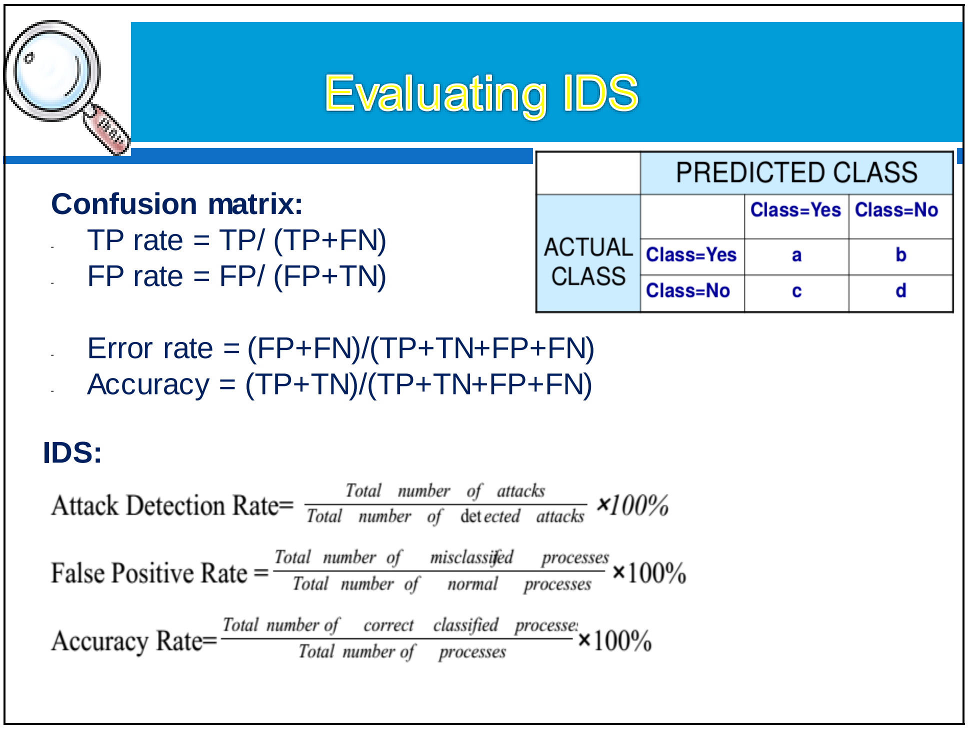
- Drop Mode
  A packet is dropped if it matches an attack signature.
  Three options are available in this mode:
  - Drop: Drops a packet, sends a reset back to the host, logs the event.
  - Sdrop: Drops a packet without sending a reset back to he host.
  - Ignore: Drops a packet, sends a reset back to the host, does not log the event
- Replace Mode
  A packet is modified if it matches an attack signature.

Evaluating IDS

Confusion matrix:

	PREDICTED CLASS		
		Class=Yes	**Class=No**
ACTUAL CLASS	**Class=Yes**	**a**	**b**
	Class=No	**c**	**d**

Parameter	Definition
True Positive Rate (TP)	Attack occur and alarm raised
False Positive Rate (FP)	No attack but alarm raised
True Negative Rate (TN)	No attack and no alarm
False Negative Rate (FN)	Attack occur but no alarm



Evaluating IDS

Confusion matrix:

- TP rate = TP/ (TP+FN)
- FP rate = FP/ (FP+TN)

	PREDICTED CLASS		
		Class=Yes	Class=No
ACTUAL CLASS	Class=Yes	a	b
	Class=No	c	d

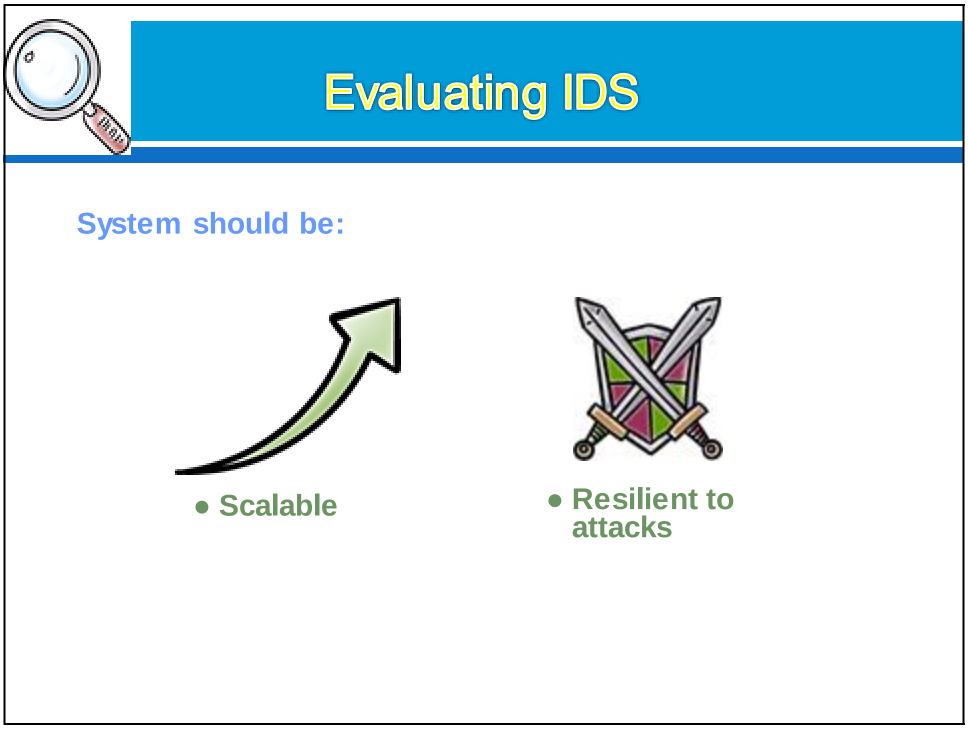
- Error rate = (FP+FN)/(TP+TN+FP+FN)
- Accuracy = (TP+TN)/(TP+TN+FP+FN)

IDS:

$$\text{Attack Detection Rate}=\frac{\textit{Total number of attacks}}{\textit{Total number of detected attacks}}\times 100\%$$

$$\text{False Positive Rate}=\frac{\textit{Total number of misclassified processes}}{\textit{Total number of normal processes}}\times 100\%$$

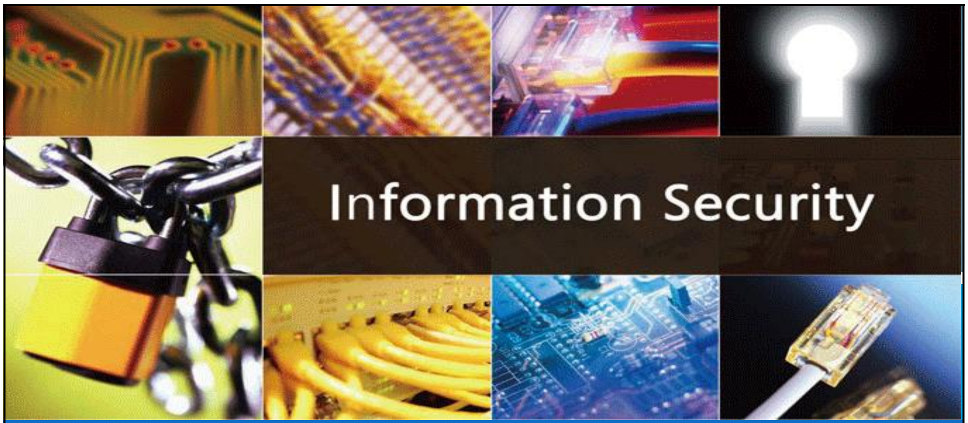
$$\text{Accuracy Rate}=\frac{\textit{Total number of correct classified processe:}}{\textit{Total number of processes}}\times 100\%$$



Evaluating IDS

System should be:

- Scalable
- Resilient to attacks



Chapter 10: Honeypot

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

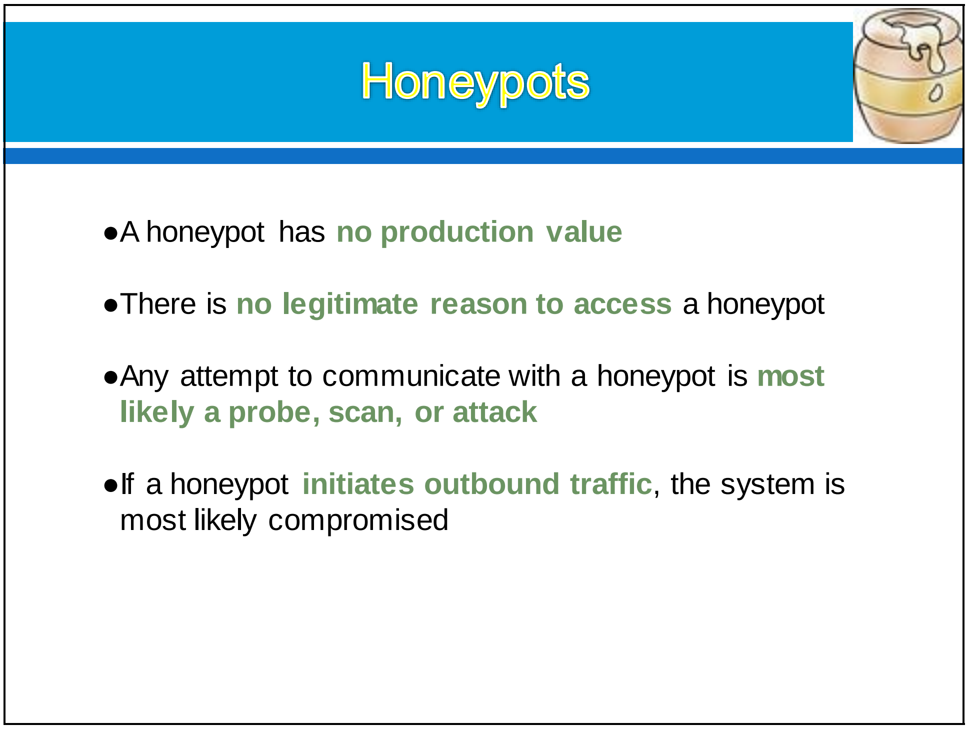
Honeypots

Honeypots are **decoy systems designed to lure attackers** away from critical systems.

- filled with fabricated info
- instrumented with monitors / event loggers

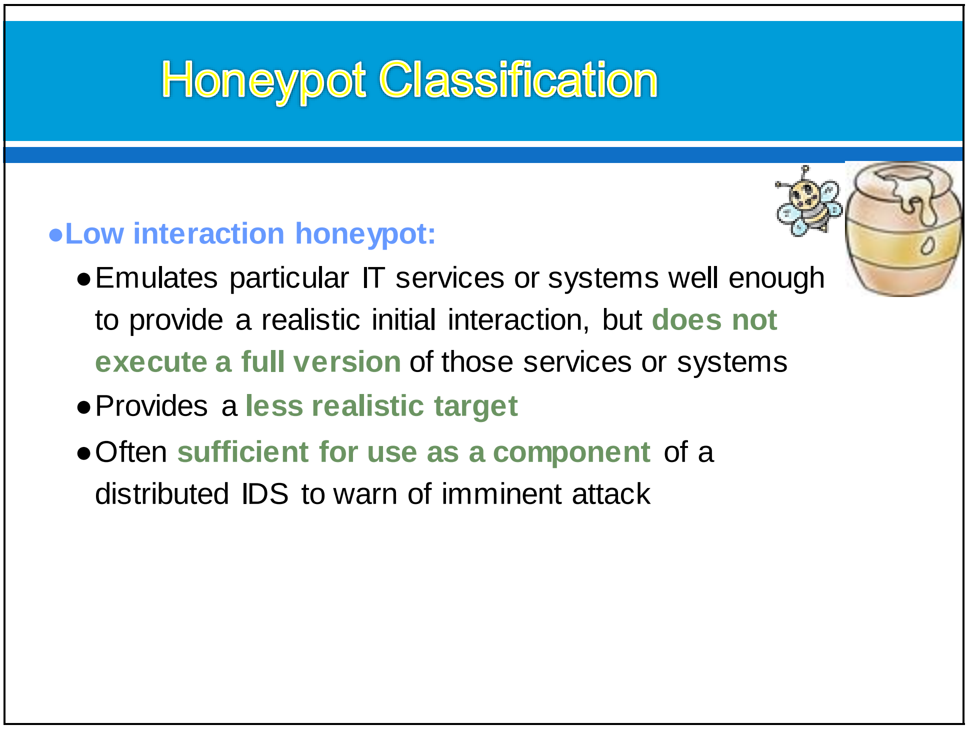
Honeypots are designed to:

- divert an attacker
- collect information about an attacker
- encourage an attacker to stay long enough for administrators to respond



Honeypots

- A honeypot has **no production value**
- There is **no legitimate reason to access** a honeypot
- Any attempt to communicate with a honeypot is **most likely a probe, scan, or attack**
- If a honeypot **initiates outbound traffic**, the system is most likely compromised



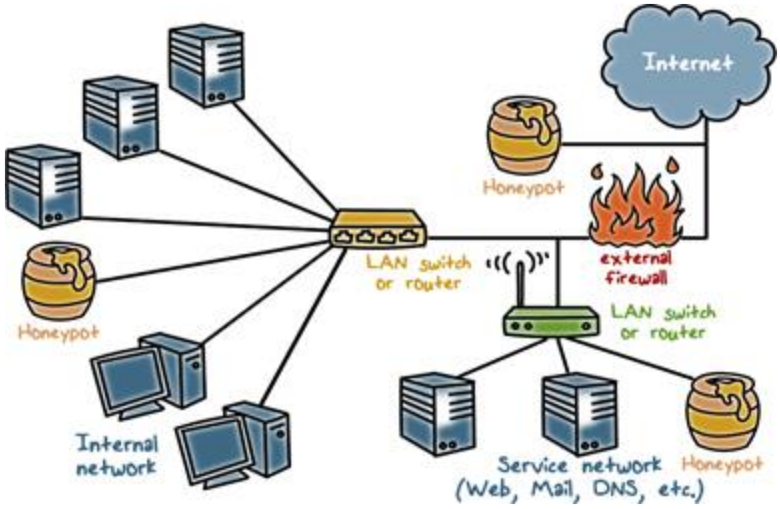
Honeypot Classification

- **Low interaction honeypot:**
  - Emulates particular IT services or systems well enough to provide a realistic initial interaction, but **does not execute a full version** of those services or systems
  - Provides a **less realistic target**
  - Often **sufficient for use as a component** of a distributed IDS to warn of imminent attack

Honeypot Classification

- **High interaction honeypot**
  - A **real system, with a full operating system**, services and applications, which are instrumented and deployed where they can be accessed by attackers
  - **More realistic target** that may occupy an attacker for an extended period
  - However, it **requires significantly more resources**

Honeypot Deployment



Summary

- IDS
- Comparison
- Architecture
- Requirement
- Classification
- Signature-based and anomaly-based IDS
- Host-based and network-based IDS
- IPS
- Honeypot

Practice

- Set up an IDS with one of the following:
  - **Snort**
  - **Suricata**
  - **Bro IDS**
  - **OpenWIPS-ng**
  - **Security Onion**
- Simulate attacks and use IDS above to detect
  - DOS, probe
- Honeypot