2. What are intrusion detection systems (IDS)? (Nov /Dec 2011, May/June 2015, Nov/Dec 2014, Nov/Dec 2012, May/June 2013)

Intrusion Detection Systems (IDSs)

IDSs work like burglar alarms. IDSs require complex configurations to provide the level of detection and response desired. An IDS operates as either network-based, when the technology is focused on protecting network information assets, or host-based, when the technology is focused on protecting server or host information assets. IDSs use one of two detection methods, signature-based or statistical anomaly-based.

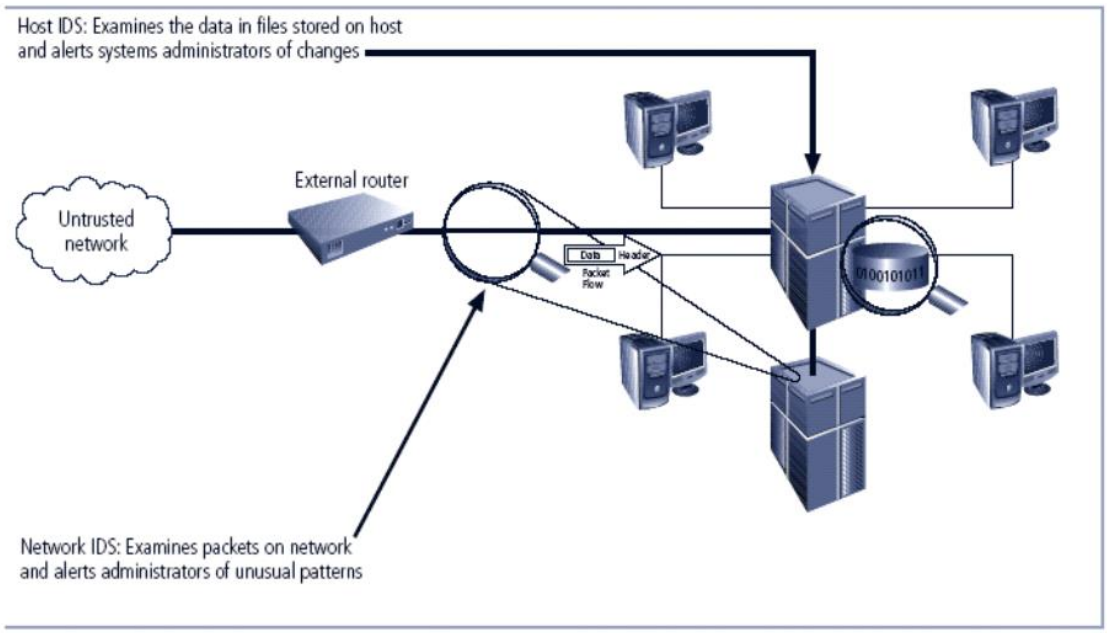
IDS terminology

- Alert or alarm
- False negative - The failure of an IDS system to react to an actual attack event.
- False positive - An alarm or alert that indicates that an attack is in progress or that an attack has successfully occurred when in fact there was no such attack.
- Confidence value
- Alarm filtering

IDSs Classification

- All IDSs use one of two detection methods:
  - Signature-based
  - Statistical anomaly-based
- IDSs operate as:

- When measured activity is outside baseline parameters or clipping level, IDS will trigger an alert
- IDS can detect new types of attacks
- Requires much more overhead and processing capacity than signature-based
- May generate many false positives



- Network-based
- Host-based
- Application-based systems

1. Signature-Based IDS

- Examine data traffic in search of patterns that match known signatures
- Widely used because many attacks have clear and distinct signatures
- Problem with this approach is that as new attack strategies are identified, the IDS's
  Database of signatures must be continually updated

2. Statistical Anomaly-Based IDS

- The statistical anomaly-based IDS (stat IDS) or behavior-based IDS sample network activity to compare to traffic that is known to be normal

3. Network-Based IDS (NIDS)

- Resides on computer or appliance connected to segment of an organization's network;

- When examining packets, a NIDS looks for attack patterns
- Installed at specific place in the network where it can watch traffic going into and out of particular network segment

NIDS Signature Matching

- To detect an attack, NIDSs look for attack patterns
- Done by using special implementation of TCP/IP stack:
  - In process of protocol stack verification, NIDSs look for invalid data packets
  - In application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use

unexpected packet behavior or improper use

4. Host-Based IDS

- Host-based IDS (HIDS) resides on a particular computer or server and monitors activity only on that system
- Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- Most HIDSs work on the principle of configuration or change management
- Advantage over NIDS: can usually be installed so that it can access information encrypted when traveling over network

5. Application-Based IDS

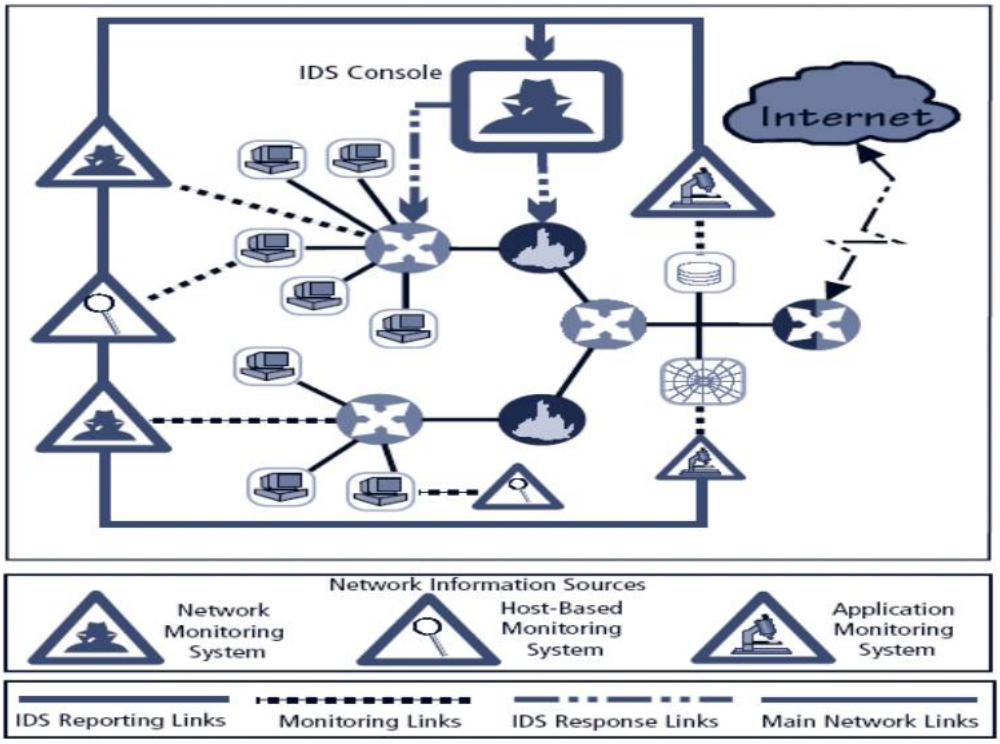
- Application-based IDS (AppIDS) examines application for abnormal events
- AppIDS may be configured to intercept requests:
  - File System
  - Network
  - Configuration
  - Execution Space

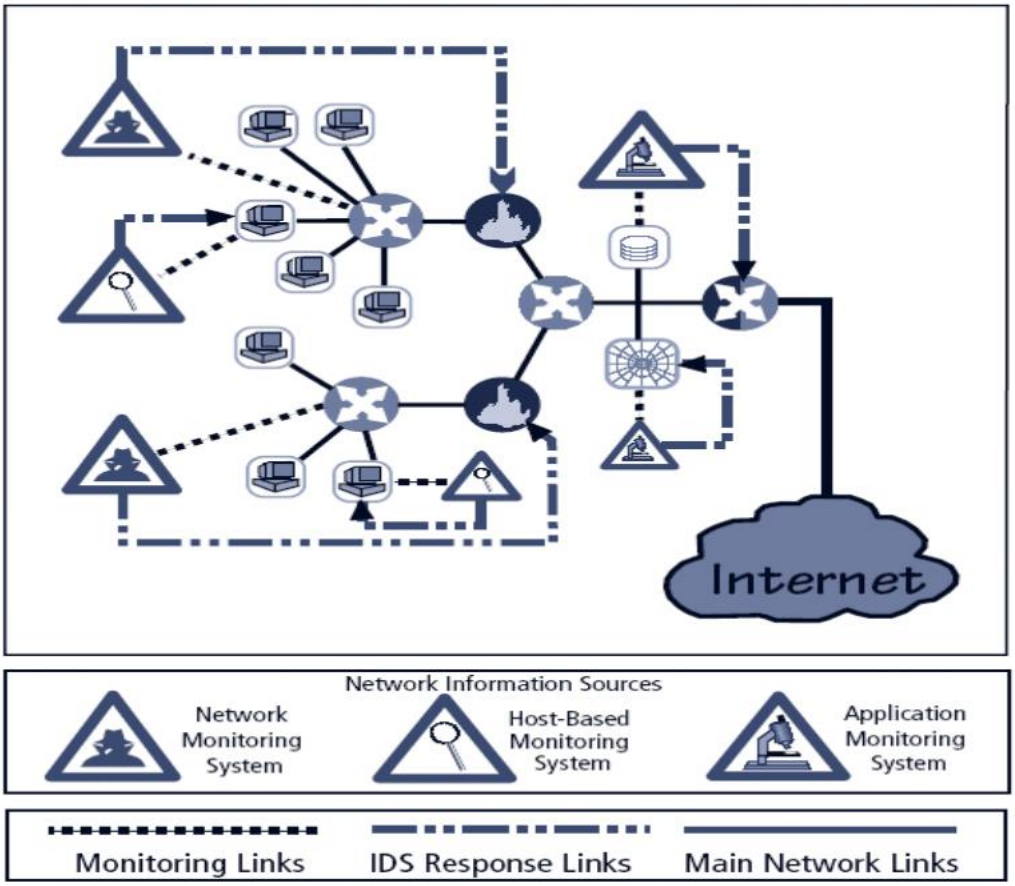
6. Log File Monitors (LFM)

Log File Monitor (LFM) is an approach to IDS that is similar to NIDS. The system reviews the log files generated by servers, network devices These systems look for patterns and signatures in the log files that may indicate an attack or intrusion is in process or has already succeeded.

IDS Control Strategies

- An IDS can be implemented via one of three basic control strategies
  - Centralized: all IDS control functions are implemented and managed in a central location
  - Fully distributed: all control functions are applied at the physical location of each IDS component
  - Partially distributed: combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks

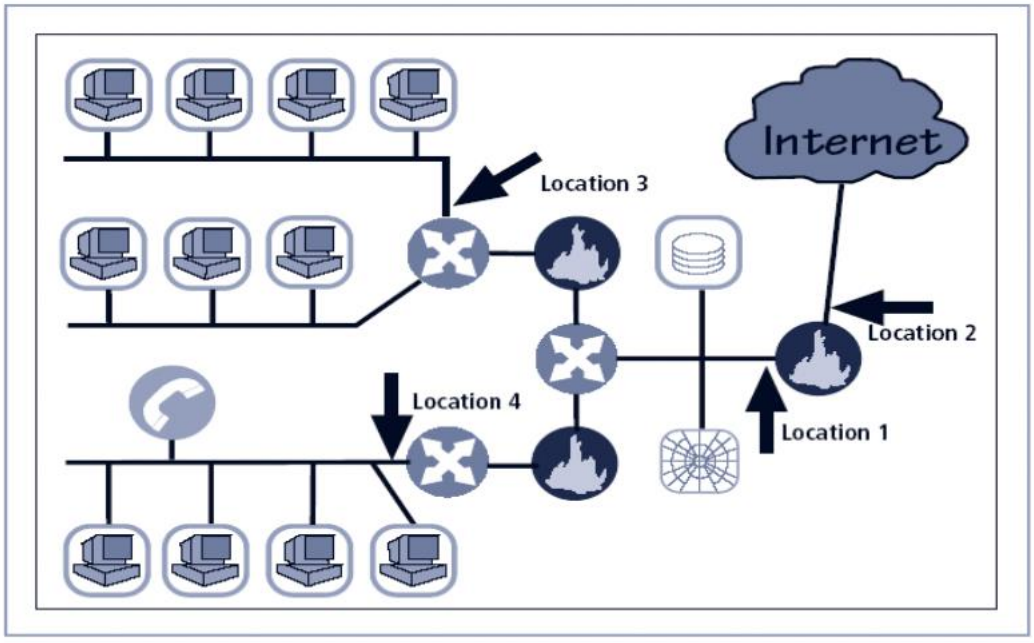

IDS Console
Internet
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
IDS Reporting Links
Monitoring Links
IDS Response Links
Main Network Links


Internet
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
Monitoring Links
IDS Response Links
Main Network Links

Deploying Network-Based IDSs

NIST recommends four locations for NIDS sensors

- Location 1: behind each external firewall, in the network DMZ
- Location 2: outside an external firewall
- Location 3: On major network backbones
- Location 4: On critical subnets



Network IDS Sensor Locations

Honey Pots, Honey Nets, and Padded Cell Systems

- Honey pots: decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves
- Honey nets: collection of honey pots connecting several honey pot systems on a subnet
- Honey pots designed to:
  - Divert attacker from accessing critical systems
  - Collect information about attacker's activity
  - Encourage attacker to stay on system long enough for administrators to document event and, perhaps, respond

Trap and Trace Systems

- Use combination of techniques to detect an intrusion and trace it back to its source
- Trap usually consists of honey pot or padded cell and alarm
- Legal drawbacks to trap and trace
  - Enticement: process of attracting attention to system by placing tantalizing bits of information in key locations
  - Entrapment: action of luring an individual into committing a crime to get a conviction.