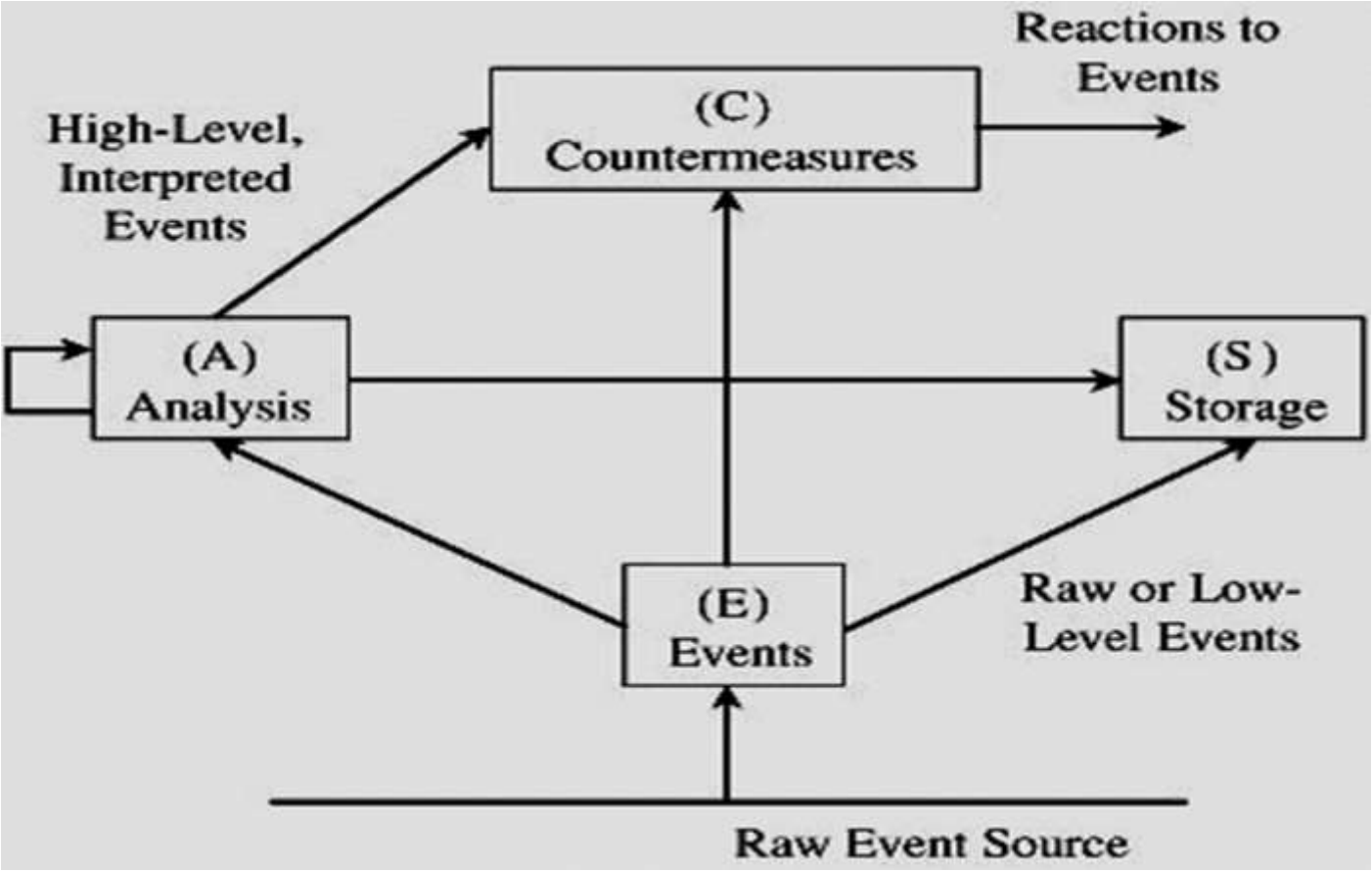
Security Chapter 5 IDS And Firewalls

An **intrusion detection system (IDS)** is a device, typically another separate computer, that monitors activity to identify malicious or suspicious events.
An IDS receives raw inputs from sensors. It saves those inputs, analyzes them, and takes some controlling action.



Types of IDSs

- **Signature-based intrusion detection systems** perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type.
- **Heuristic intrusion detection systems**, " **anomaly based"** build a model of acceptable behavior and flag exceptions to that model; for the future, the administrator can mark a flagged behavior as acceptable or not so that the heuristic IDS will now treat that previously unclassified behavior as how it was classified.

-A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network.

-A host-based IDS runs on a single workstation or client or host, to protect that one host.

A firewall is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network.
It needs a security policy.

Packet Filtering	Stateful Inspection	Application Proxy	Guard	Personal Firewall
Simplest	More complex	Even more complex	Most complex	Similar to packet filtering firewall
Sees only addresses and service protocol type	Can see either addresses or data	Sees full data portion of packet	Sees full text of communication	Can see full data portion of packet
Auditing difficult	Auditing possible	Can audit activity	Can audit activity	Canand usually doesaudit activity
Screens based on connection rules	Screens based on information across packetsin either header or data field	Screens based on behavior of proxies	Screens based on interpretation of message content	Typically, screens based on information in a single packet, using header or data
Complex addressing rules can make configuration tricky	Usually preconfigured to detect certain attack signatures	Simple proxies can substitute for complex addressing rules	Complex guard functionality can limit assurance	Usually starts in "deny all inbound" mode, to which user adds trusted addresses as they appear

Proxy gateway examples

- **A company** wants to set up an **online price list** so that outsiders can **see** the products and prices offered. It wants to be sure that (a) no outsider can change the prices or product list and (b) outsiders can access only the price list, not any of the more sensitive files stored inside.
- **A school** wants to allow its students to retrieve any information from World Wide Web resources on the Internet. To help provide efficient service, the school wants to know what **sites have been visited** and what files from those sites have been fetched; particularly popular files will be cached locally.
- **A government** agency wants to respond to queries through a **database management** system. However, because of inference attacks against databases, the agency wants to **restrict queries** that return the mean of a set of fewer than five values.
- **A company** with multiple offices wants to **encrypt the data** portion of all e-mail to addresses at its other offices. (A corresponding proxy at the remote end will remove the encryption.)
- **A company** wants to allow **dial-in access** by its employees, without exposing its company resources to login attacks from remote nonemployees.

Guard examples:

- **A university** wants to allow its students to use **e-mail up to a limit** of so many messages or so many characters of e-mail in the last so many days. Although this result could be achieved by modifying e-mail handlers, it is more easily done by monitoring the common point through which all e-mail flows, the mail transfer protocol.
- **A school** wants its students to be able to access the World Wide Web but, because of the **slow speed** of its connection to the web, it will allow only so many characters per downloaded image (allowing text mode and simple graphics, but disallowing complex graphics, animation, music, or the like).
- **A library** wants to make available certain documents but, to support fair use of copyrighted matter, it will allow a user to retrieve only the first so many characters of a document. After that amount, the library will require the user to **pay a fee** that will be forwarded to the author.
- **A company** wants to allow its employees to fetch files via ftp. However, to prevent introduction of viruses, it will first pass all incoming files through a **virus scanner**. Even though many of these files will be nonexecutable text or graphics, the company administrator thinks that the expense of scanning them (which should pass) will be negligible.

What Firewalls Can and Cannot Block

firewalls are not complete solutions to all computer security problems.
A firewall protects only the perimeter of its environment against attacks from outsiders who want to execute code or access data on the machines in the protected environment.

Keep in mind these points about firewalls.

- Firewalls can protect an environment only if the firewalls control the entire **perimeter**.
- Firewalls do **not protect** data **outside** the perimeter
- Firewalls are the **most visible** part of an installation to the outside, so they are the most attractive target for attack. ➔ several different layers of protection, called **defense in depth**, are better than relying on the just a single firewall.
- Firewalls must be correctly **configured**, that configuration must be updated as the internal and external environment changes, and firewall activity reports must be reviewed periodically.
- Firewalls are targets for **penetrators**. While a firewall is designed to withstand attack, it is not impenetrable.
- Firewalls exercise **only minor control** over the content admitted to the inside.