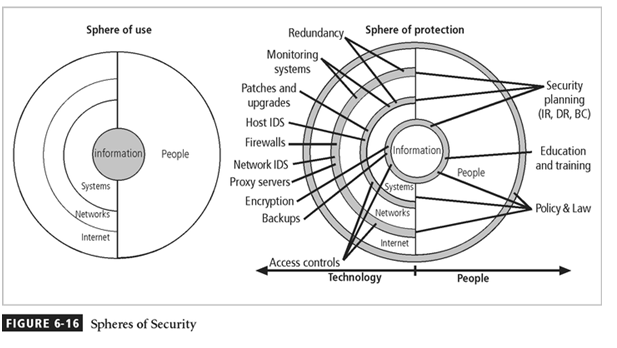
**14 a) What is Sphere of protection, Defense in Depth and Security perimeter? What are the**

**key technological components used for security implementation?**

**Explain in detail about design of security architecture. (Nov /Dec 2011, May/June 2015)**

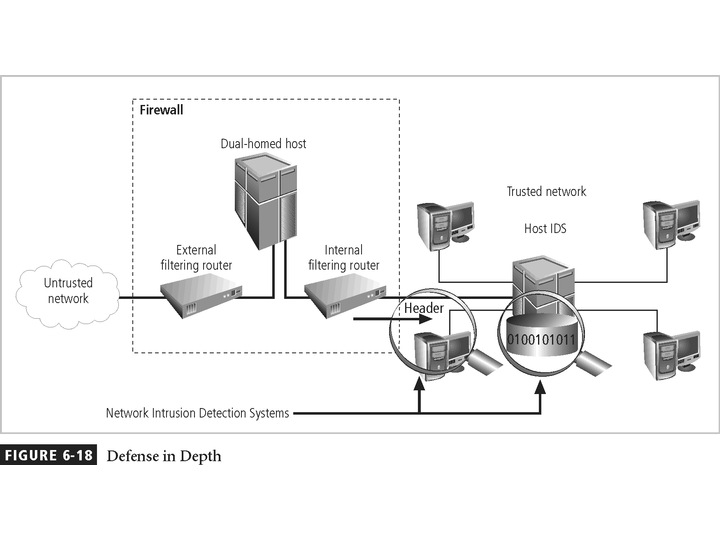
**Sphere of Protection**

* The “sphere of protection” overlays each of the levels of the “sphere of use” with a layer of security, protecting that layer from direct or indirect use through the next layer
* The people must become a layer of security, a human firewall that protects the information from unauthorized access and use
* Information security is therefore designed and implemented in three layers
  + policies
  + people (education, training, and awareness programs)
  + technology

****

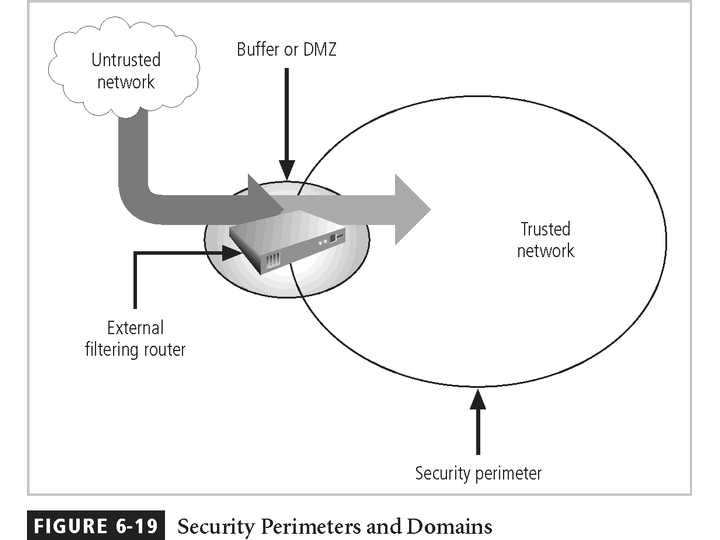
**Defense in Depth**

* One of the basic foundations of security architectures is the implementation of security in layers. This layered approach is called **defense in depth**.
* Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls.
* These layers of control can be organized into policy, training and education and technology as per the NSTISSC model.
* While policy itself may not prevent attacks, they coupled with other layers and deter attacks.
* Training and Education are similar.
* Technology is also implemented in layers, with detection equipment, all operating behind access control mechanisms.
* Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of the information is referred to as **redundancy**.
* Redundancy can be implemented at a number of points throughout the security architecture, such as firewalls, proxy servers, and access controls.
* The figure shows the use of firewalls and intrusion detection systems (IDS) that use both packet-level rules and data content analysis.



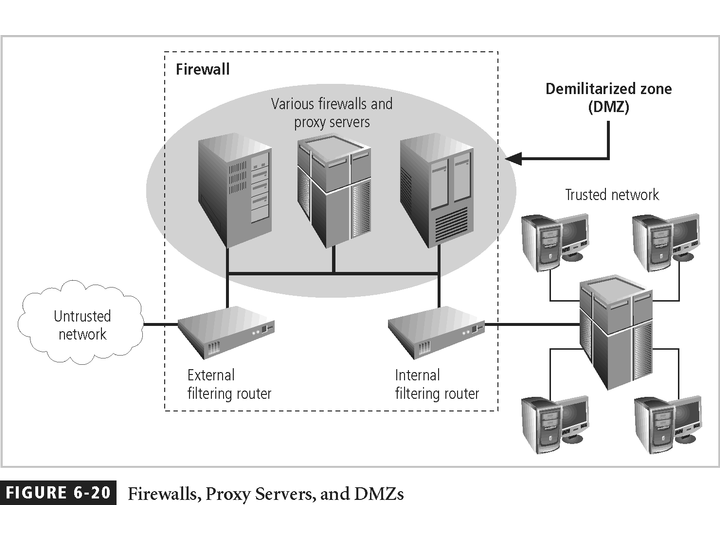
**Security Perimeter**

* + The point at which an organization’s security protection ends, and the outside world begins
  + Referred to as the security perimeter
  + Unfortunately the perimeter does not apply to internal attacks from employee threats, or on-site physical threats

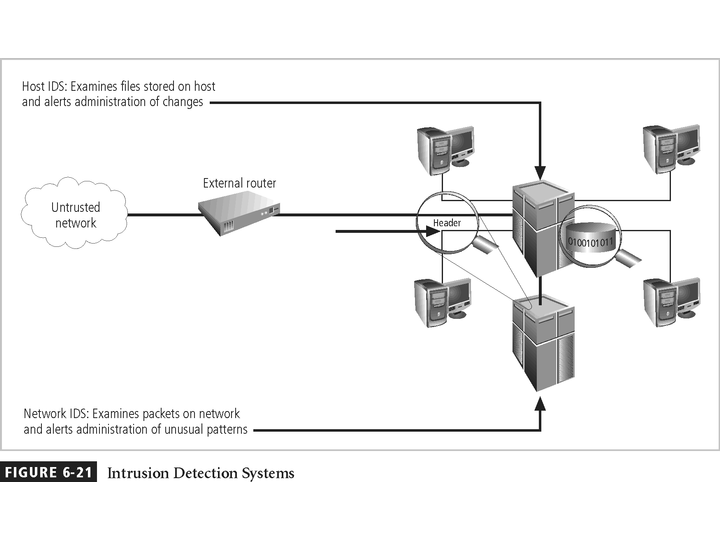
****

**Key Technology Components**

* Other key technology components
  + A **firewall** is a device that selectively discriminates against information flowing into or out of the organization.
  + Firewalls are usually placed on the security perimeter, just behind or as part of a **gateway router**.
  + Firewalls can be packet filtering, stateful packet filtering, proxy, or application level.
  + A Firewall can be a single device or a **firewall subnet**, which consists of multiple firewalls creating a buffer between the outside and inside networks.
  + The **DMZ** (demilitarized zone) is a no-man’s land, between the inside and outside networks, where some organizations place Web servers
  + These servers provide access to organizational web pages, without allowing Web requests to enter the interior networks.
  + **Proxy server-** An alternative approach to the strategies of using a firewall subnet or a DMZ is to use a **proxy server**, or **proxy firewall**.
  + For more frequently accessed Web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called **cache servers.**

****

* + **Intrusion Detection Systems (IDSs).** In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement **Intrusion Detection Systems or IDS**.
  + **IDs** come in two versions. Host-based & Network-based IDSs.
    - **Host-based IDSs** are usually installed on the machines they protect to monitor the status of various files stored on those machines.
    - **Network-based IDSs** look at patterns of network traffic and attempt to detect unusual activity based on previous baselines.
  + This could include packets coming into the organization’s networks with addresses from machines already within the organization (IP spoofing).
  + It could also include high volumes of traffic going to outside addresses (as in cases of data theft) or coming into the network (as in a denial of service attack).
  + Both host-and network based IDSs require a database of previous activity.

****