DESIGN OF SECURITY ARCHITECTURE

- To inform the discussion of information security program architecture and to illustrate industry best practices , the following sections outline a few key security architectural components.
- Many of these components are examined in an overview.
- An overview is provided because being able to assess whether a framework and/or blueprint are on target to meet an organization‘s needs requires a working knowledge of these security architecture components.

Defense in Depth

- One of the basic tenets 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 establishes sufficient security controls and safeguards so that an intruder faces multiple layers of control.
- 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 , it certainly prepares the organization to handle them.
- Coupled with other layers , policy can deter attacks.
- Training and education are similar.
- Technology is also implemented in layers, with detection equipment working in tandem with reaction technology, 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 through the security architecture such as firewalls, proxy servers, and access controls.
- Fig 6.18 illustrates the concept of building controls in multiple, sometimes redundant layers.
- The Fig shows the use of firewalls and intrusion detection systems(IDS) that use both packet –level rules (shown as the header in the diagram) and the data content analysis (shown as 0100101000 in the diagram)

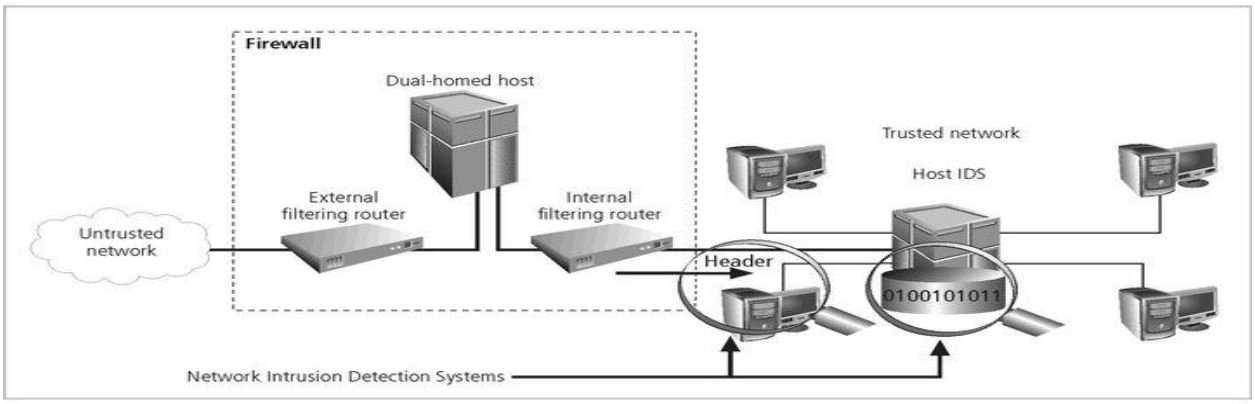

FIGURE 6-18 Defense in Depth

Security Perimeter

- A perimeter is the boundary of an area. A security perimeter defines the edge between the outer limit of an organizations security and the beginning of the outside world.
- A security perimeter is the first level of security that protects all internal systems from outside threats , as pictured in Fig 6.19
- Unfortunately, the perimeter does not protect against internal attacks from employee threats or on-site physical threats.
- There can be both an electronic security perimeter, usually at the organization‘s exterior network or internet connection, and a physical security perimeter, usually at the gate to the organization‘s offices.
- Both require perimeter security.
- Security perimeters can effectively be implemented as multiple technologies that safeguard the protected information from those who would attack it.
- Within security perimeters the organization can establish security domains, or areas of trust within which users can freely communicate.
- The assumption is that if individuals have access to all systems within that particular domain.

- The presence and nature of the security perimeter is an essential element of the overall security framework, and the details of implementing the perimeter make up a great deal of the particulars of the completed security blueprint.
- The key components used for planning the perimeter are with respect to firewalls, DMZs, Proxy servers, and intrusion detection systems.

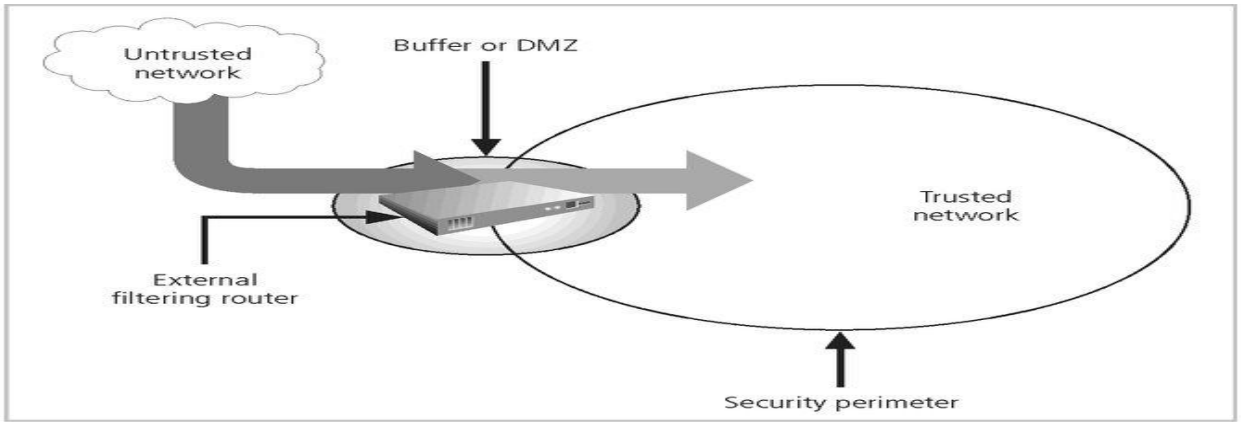

FIGURE 6-19 Security Perimeters and Domains

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf