IDS DEPLOYMENT OVERVIEW

Like the decision regarding control strategies, the decisions about where to locate the elements of the intrusion detection systems can be an art in itself. Given the highly technical skills required to implement and configure IDSs and the imperfection of the technology, great care must be made in the decisions about where to locate the components, both in their physical connection to the network and host devices and in how they will be logically connected to each other and the IDS administration team. Since IDSs are designed to detect, report, and even react to anomalous stimuli, placing IDSs in an area where such traffic is common can result in excessive reporting. Moreover, the administrators monitoring systems located in such areas can become desensitized to the high level of information flow and may fail to detect actual attacks in progress.

As an organization selects an IDS and prepares for implementation, planners must select a deployment strategy that is based on a careful analysis of the organization's information security requirements and that integrates with the organization's existing IT infrastructure but, at the same time, causes minimal impact. After all, the purpose of the IDS is to detect anomalous situations-not create them. One consideration for implementation is the skill level of the personnel required to install, configure, and maintain the systems. An IDS is a complex system in that it involves numerous remote monitoring agents (on both individual systems and networks) that require proper configuration to gain the proper authentication and authorization. As the IDS is deployed, each component should be installed, configured, fine-tuned, tested, and monitored. A problem in any step of the deployment process may produce a range of problems-from a minor inconvenience to a network-wide disaster. Thus, both the individuals installing the IDS and the individuals using and managing the system require proper training.

NIDS and HIDS can be used in tandem to cover both the individual systems that connect to an organization's networks and the networks themselves. To do this, it is important for an organization to use a phased implementation strategy so as not to impact the entire organization all at once. A phased implementation strategy also allows security technicians to resolve the problems that do arise without compromising the very information security the IDS is installed to protect. In terms of sequencing the implementation, first the organization should implement the network-based IDS, as they are less problematic and easier to configure than their host -based counterparts. After the NIDSs are configured and running without issue, the HIDSs can be installed to protect the critical systems on the host server. Next, after both are considered operational, it would be advantageous to scan the network with a vulnerability scanner like Nmap or Nessus to determine if a) the scanners pick up anything new or unusual, and b) if the IDS can detect the scans.

Deploying Network-Based IDSs. As discussed above, the placement of the sensor agents is critical to the operation of all IDSs, but this is especially critical in the case of Network IDSs. NIST recommends four locations for NIDS sensors:

Location 1: Behind each external firewall, in the network DMZ (See Figure 7-7, location 1)

Advantages:

- IDS sees attacks that originate from the outside world and may penetrate the network's perimeter defenses.
- IDS can identify problems with the network firewall policy or performance.
- IDS sees attacks that might target the Web server or fip server, both of which commonly reside in this DMZ.

Even if the incoming attack is not detected, the IDS can sometimes recognize, in the outgoing traffic, patterns that suggest that the server has been compromised.

Location 2: Outside an external firewall (See Figure 7-7, location 2)

Advantages:

- IDS documents the number of attacks originating on the Internet that target the network.
- IDS documents the types of attacks originating on the Internet that target the network.

Location 3: On major network backbones (See Figure 7-7, location 3)

Advantages:

- IDS monitors a large amount of a network's traffic, thus increasing its chances of spotting attacks.

- IDS detects unauthorized activity by authorized users within the organization's security perimeter.

Location: On critical subnets (See Figure 7-7, location 4)

Advantages:

- IDS detects attacks targeting critical systems and resources.
- Location allows organizations with limited resources to focus these resources on the network assets considered of greatest value[16].

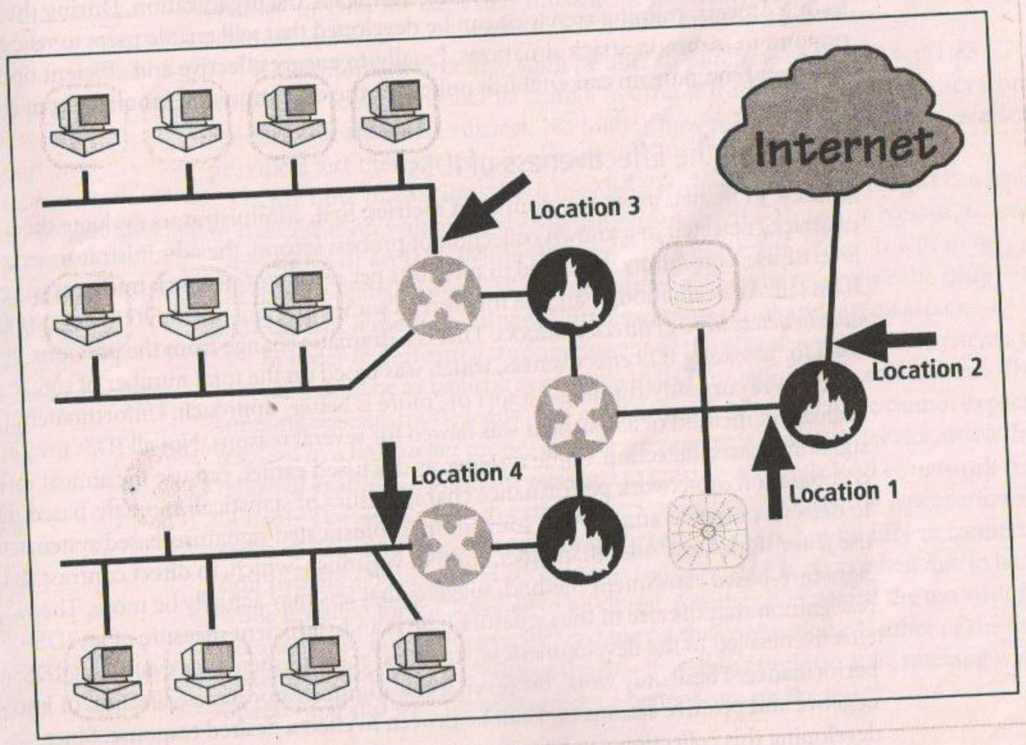

FIGURE 7-7 Network IDS Sensor Locations[17]

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