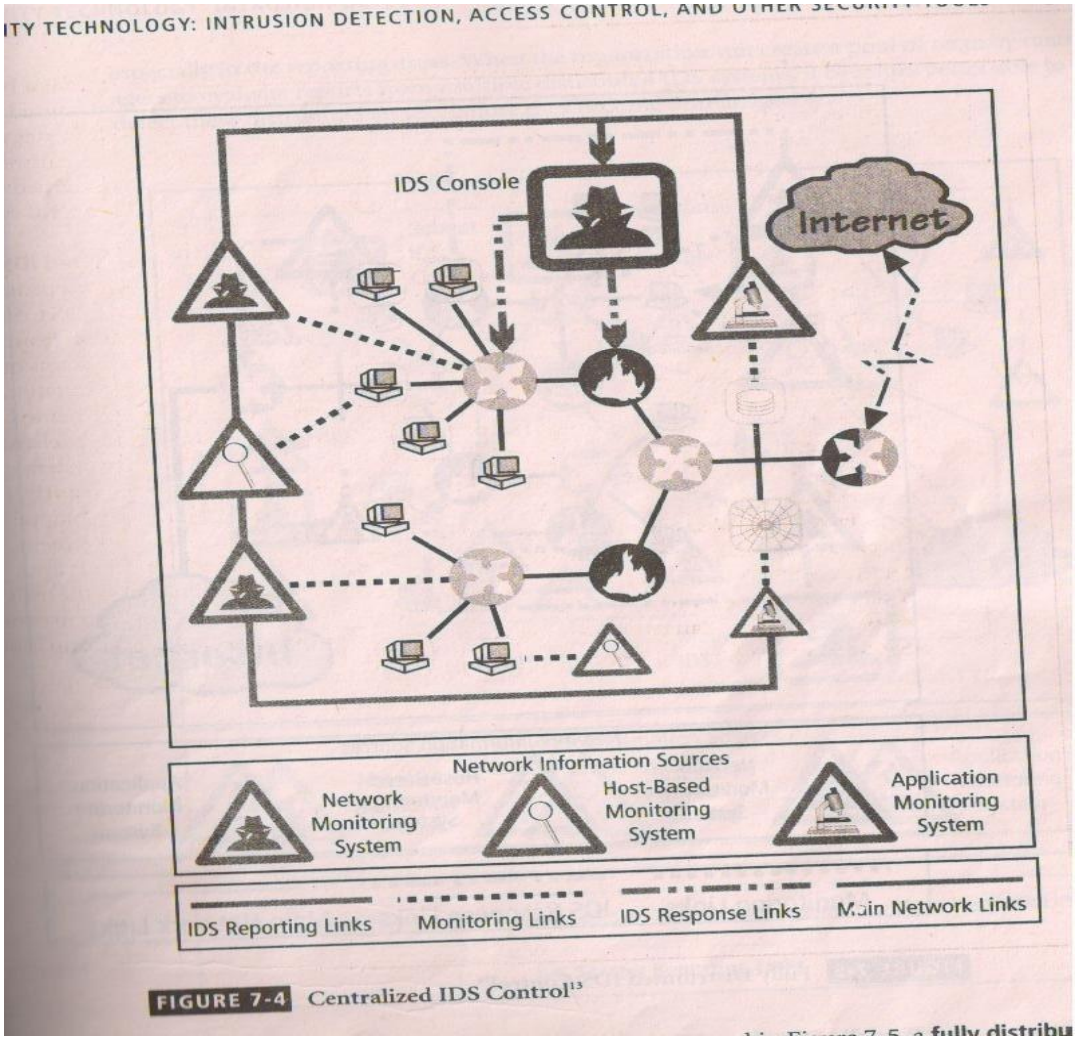
IDS CONTROL STRATEGIES

An IDS can be implemented via one of three basic control strategies. A control strategy determines how an organization exerts influence and maintains the configuration of an IDS. It will also determine how the input and output of the IDS is to be managed. The three commonly utilized control strategies are centralized, partially distributed, and fully distributed. The IT industry has been exploring technologies and practices to enable the distribution of computer processing cycles and data storage for many years. These explorations have long considered the advantages and disadvantages of the centralized strategy versus those of strategies with varying degrees of distribution. In the early days of computing, all systems were fully centralized, resulting in a control strategy that provided high levels of security and control, as well as efficiencies in resource allocation and management. During the '80s and '90s, with the rapid growth in networking and computing capabilities, the IT industry's ideas about how to arrange computing systems swung to the other end of the pendulum-that is, the trend was to implement a fully distributed strategy. In the mid- '90s, however, the high costs of a fully distribute architecture became apparent, and the IT industry shifted toward a mixed strategy of partially distributed control. A strategy of partial distribution, where some features and components are distributed and others are centrally controlled, has now emerged as the recognized recommended practice for IT systems in general and for IDS control systems in particular.

Centralized Control Strategy. As illustrated in Figure 7-4, with a centralized IDS control strategy all IDS control functions are implemented and managed in a central location. This is indicated, in the figure with the large square symbol labeled "IDS Console." The IDS

console includes the management software; which collects information from the remote sensors

(appearing in the figure as triangular symbols), analyzes the systems or networks monitored, and makes the determination as to whether the current situation has deviated from the preconfigured baseline. All reporting features are also implemented and managed from this central location. The primary advantages of this strategy are related to cost and control. With" one central implementation, there is one management system, one place to go to monitor the status of the systems or networks, one location for reports, and one set of administrative management. This centralization of IDS management supports specialization in tasks, since all managers are either located near the IDS management console or can acquire an authenticated remote connection to it, and technicians are located near the remote sensors. This means that each person can focus specifically on the assigned task at hand. In addition, the central control group can evaluate the systems and networks as a whole, and since it can compare pieces of information from all sensors, the group is better positioned to recognize a large-scale attack.



Fully Distributed Control Strategy. As presented in Figure 7-5, a **fully distributed IDS control strategy** is the opposite of the centralized strategy. Note in the figure that all control functions (which appear as small square symbols enclosing a computer icon) are applied at the physical location of each IDS component. Each monitoring site uses its own paired sensors to perform its own control functions to achieve the necessary detection, reaction, and response functions. Thus, each sensor/agent is best configured to deal with its own environment. Since the IDSs do not have to wait for a response from a centralized control facility, their reaction to individual attacks is greatly speeded up.

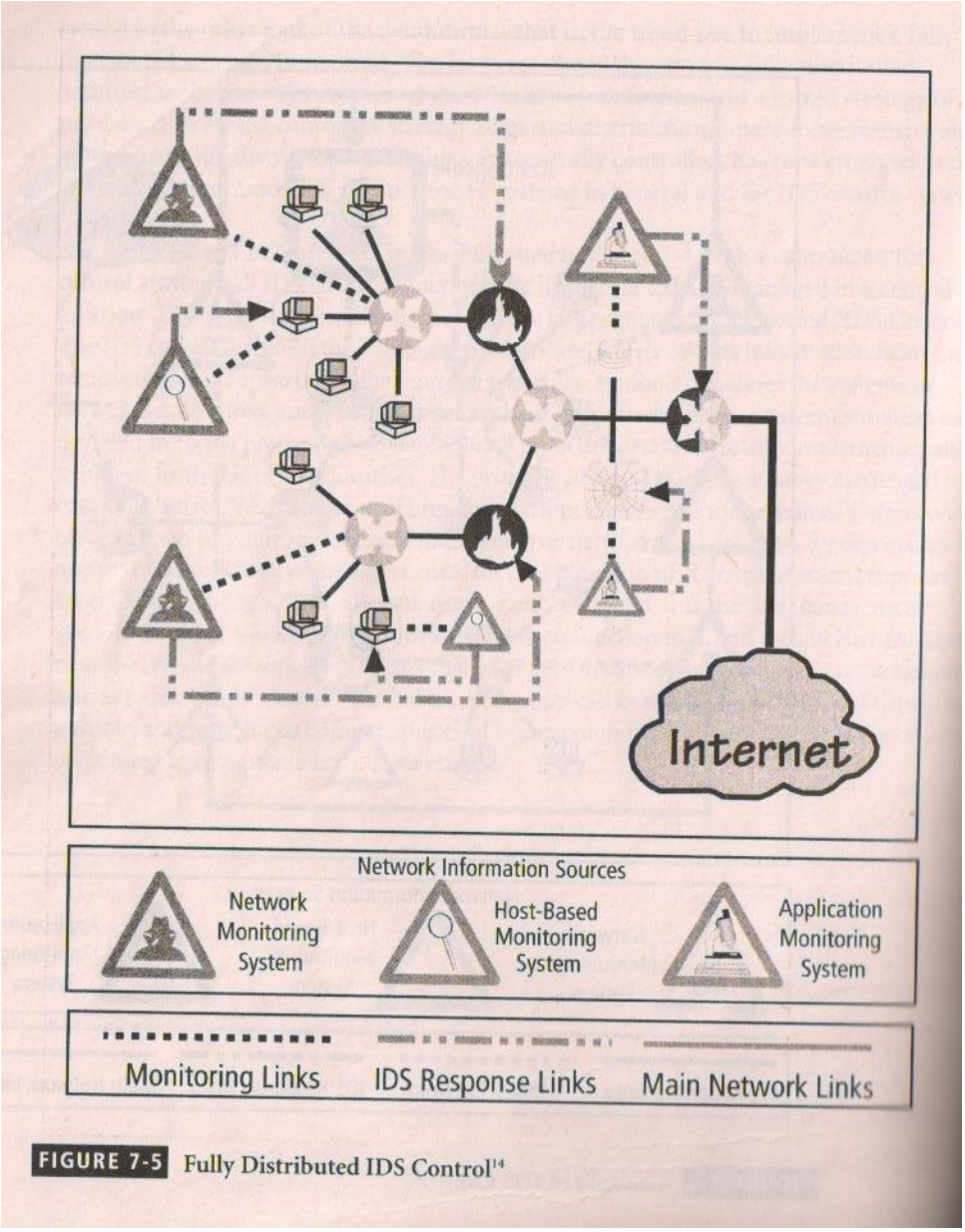


FIGURE 7-5 Fully Distributed IDS Control[14]

partially Distributed Control Strategy. Finally, a partially distributed IDS control strategy, as depicted in Figure 7 -6, combines the best of the other two strategies. While the individual agents can still analyze and respond to local threats, their reporting to a hierarchical central facility enables the organization to detect widespread attacks. This blended approach to reporting is one of the more effective methods of detecting intelligent attackers, especially those who probe an organization through multiple points of entry, trying to scope out the systems' configurations and weaknesses, before they launch a concerted attack. The partially distributed control strategy also allows the organization to optimize for economy of scale in the implementation of key management software and personnel, especially in the reporting areas. When the organization can create a pool of security managers to evaluate reports from multiple distributed IDS systems, it becomes better able to detect these distributed attacks before they become unmanageable.

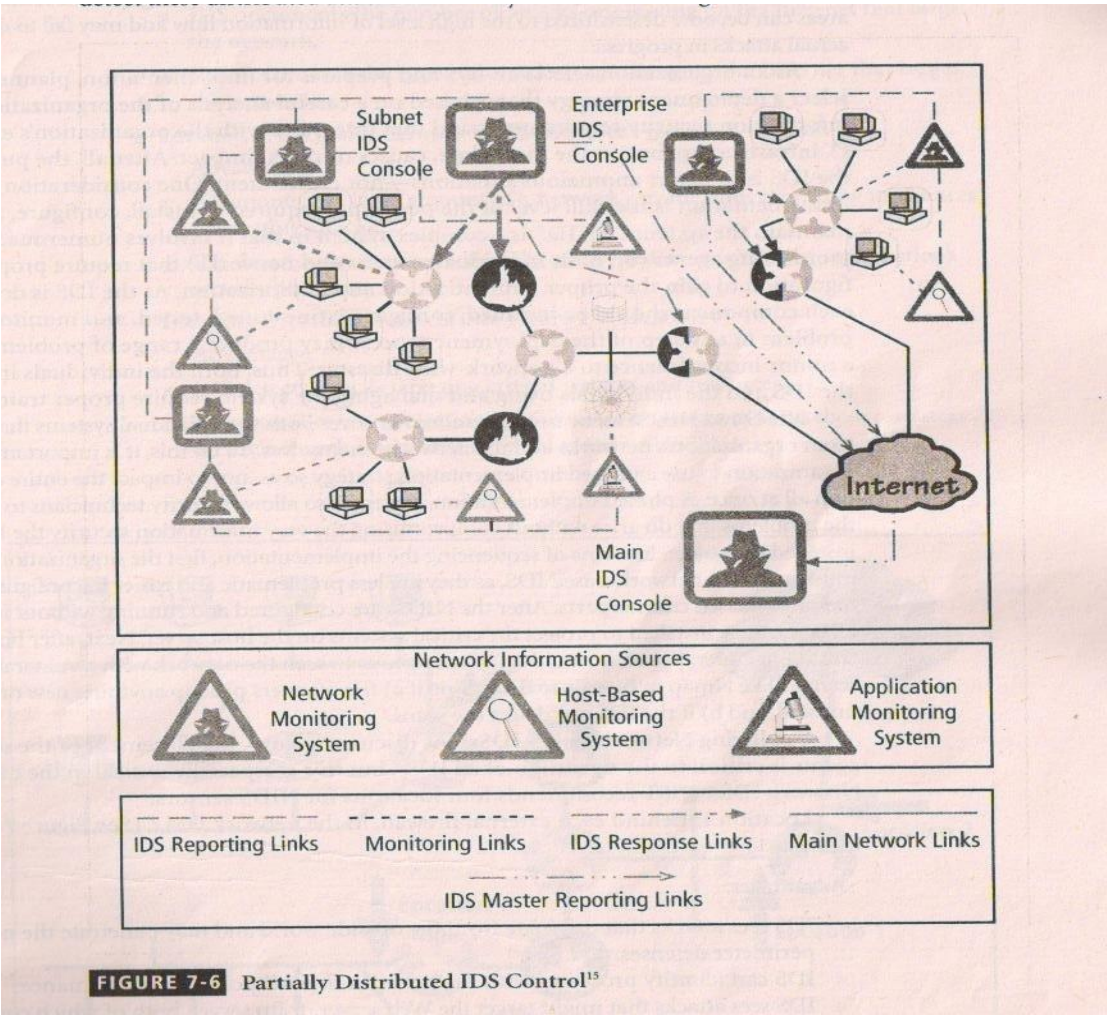


FIGURE 7-6 Partially Distributed IDS Control[15]

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