## 4.4 HYBRID OR DISTRIBUTED INTRUSION DETECTION

The idea of communicating IDSs has developed in recent years to involve dispersed systems working together to detect intrusions and adjust to shifting attack characteristics. To monitor and coordinate intrusion detection and response in an organization's IT infrastructure, HIDS and NIDS combine their complementary information sources-host-based process and data details and network events and data-into a central IDS.

systems like IDS, Firewalls, virus and worm detectors, and so on have always had two main issues.

- First off, these techniques might not detect brand new risks of significant changes to known threats
- Second, it is challenging to update strategies quickly enough to counter attacks that spread swiftly.

The fact that hosts can typically move in and out of modern enterprises loosely defined boundaries presents a different challenge for perimeter defences like firewalls. Hosts that internet wirelessly and workstation laptops that can plug inte network ports are two examples Attackers have used a variety of techniques to exploit these issues. The more conventional attack strategy involves creating worms and other malicious software that spreads quickly as well as other attacks like Dos attacks) that launch a powerful attack before a defence can be set up. This kind of attack is still common. However, more recently, attackers have added a very different strategy: slow the attack's propagation so that it will be harder to spot by traditional algorithms.

Creating cooperative systems that can identify attacks based on shadier cues and then quickly react is one strategy to defend against such attacks. In this method, local nodes with anomaly detectors search for signs of anomalous activity. For instance, if a computer is abruptly ordered to increase the rate at which it establishes connections to the network, it may assume that an attack is underway.

If the local system reacts to the suspected attack (for example, by disconnecting from the network and issuing an alert), it runs the danger of a false positive, but if it ignores the attack or waits for more proof, it runs the risk of a false negative. Instead, the local node in an adaptive, cooperative system employs a peer-to-peer "gossip" protocol to alert other computers of its suspicions, expressed as a probability that the network is being attacked.

A machine assumes an attack is underway and reacts if enough of these messages are received for a threshold to be surpassed. The machine has the Ability to protect itself locally while also alerting a centralized system. Autonomic enterprise security [AG0806], a plan created by Intel, is an illustration of this strategy. The strategy is demonstrated in Figure.

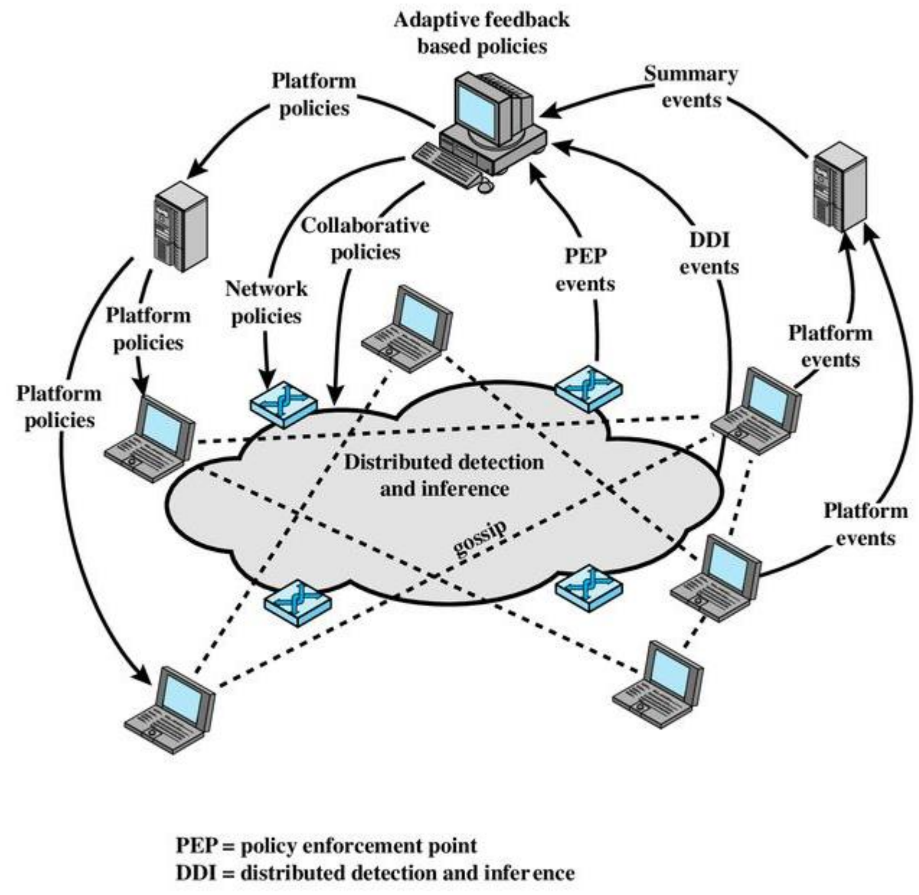

**Figure 8.6 Overall Architecture of an Autonomic Enterprise Security System**

This method does not rely exclusively on individual host-based defenses or perimeter defenses like firewalls. Instead, every network equipment (such as routers) and end host are thought of as possible sensors, and they might even have the sensor software module installed. In this dispersed architecture, the sensors can communicate to confirm the network's condition.

The following justifications are offered for this strategy by the Intel designers:

1. IDSs that are selectively installed could fail to detect a network-based attack or take too long to do so. It has been demonstrated that using numerous IDSs that exchange information increases coverage and speeds up response to attacks, particularly those that spread slowly (such as [BAIL05], [RAJA05]).

2. Network traffic analysis at the host level creates an environment with far less network traffic than that of a network device like a router. As a result, attack patterns will be more noticeable, increasing the signal to noise ratio.

3. Host-based detectors can access a wider variety of data, including application data from the host, which could be used as an input

**Distributed or Hybrid IDS**

Multiple solutions from a same vendor can be combined to create a distributed or hybrid IDS that is intended to share and exchange data. This is undoubtedly a simpler approach, but it might not be the most economical or complete one. It is also possible to ingest and analyze data from a number of sources, sensors, and devices using specialized security information and event management (SIEM) software. Such software might very well be dependent on standardized protocols, such the intrusion detection exchange format that will be covered in the following section.

An analogy might make the benefit of this dispersed strategy more clear. Let's say a single host is the target of a protracted attack, and the host is set up to reduce false positives. No notice is issued in the early stages of the attack due to the high likelihood of a false positive. As long as the attack continues, there is better proof that it is occurring, and the possibility of false positives in reduced.

But a lot of time has passed. Now imagine a large number of local sensors working together to detect the beginning of an attack Multiple systems are detecting the same data, thus there is little chance of a false positive when an alarm is sent. Therefore, to decrease false positives and yet identify attacks, we employ a high number of sensors rather than a lengthy amount of time. This kind of product is now available from numerous manufacturers

The key components of this strategy are now summarized and are shows in Figure. A default set of security policies is set up on a central system. These policies are modified based on feedback from networked sensors, and specific actions are conveyed to the various platforms in the distributed system.

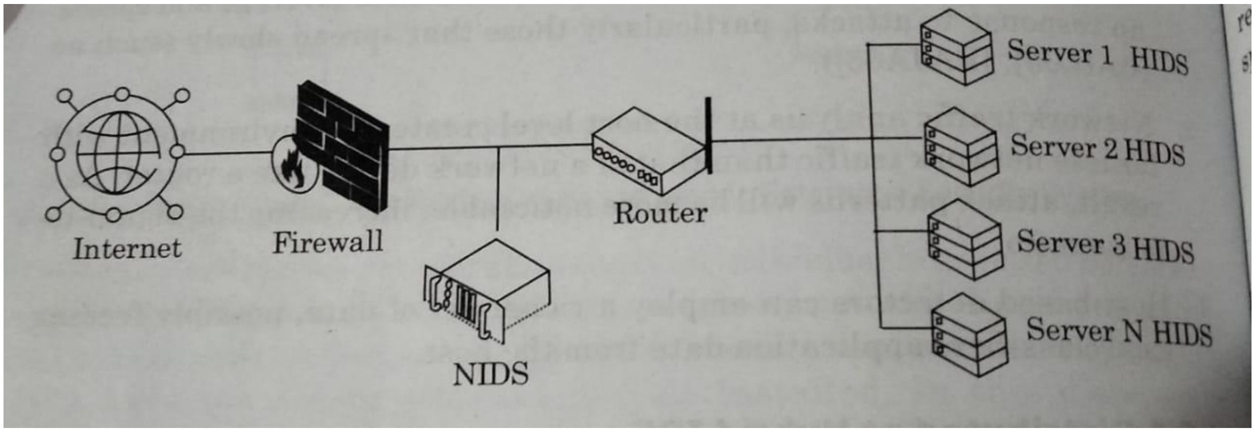

**Figure Distributed or Hybrid IDS architecture diagram**

The device-specific policies could specify immediate actions to be taken or changes to be made to parameter values. Additionally, the central system transmits to all platforms collaborative policies that modify the frequency and substance of collaborative gossip messages. The central system's activities are guided by three different types of input:

**Summary Events**: Servers that cater to a particular area of the company network act as intermediate collection points that gather events from numerous sources. For distribution to the main policy system, these events are condensed.

**Distributed Detection and Inference (DDI) Events**: These warnings are sent when a platform can infer an attack is happening from the gossip traffic.

**PEP Events:** Intelligent IDSs and trusted, self-defending platforms house Policy Enforcement Points (PEPs), which enforce policies. These systems use local judgements, distributed data, and specific device behaviors to identify intrusions that may not be immediately apparent at the host level