INTRUSION DETECTION SYSTEMS

Description of the Application

Intrusion Detection Systems (IDS) are used by organizations to extend their security infrastructure by detecting and responding to unauthorized access of resources in real time. These systems are made up of host based agents and network based devices installed at a variety of key access points throughout a network. From this vantage point, they analyze and assess the integrity of traffic to identify known attack patterns, abnormal activities and unauthorized use. When a threat is detected, these systems alert an organization's security engineers so further action can be taken.

Challenges to the Application Type

While Intrusion Detection Systems enhance network protection, they should not be considered the complete solution for any network security policy. For example, Intrusion Detection Systems cannot compensate for weak identification and authentication mechanisms, or analyze all traffic on busy networks. The challenge is to build a security infrastructure to provide the following business requirements:

Providing high availability - An organization should never deploy a single IDS; this introduces a single point of failure and exposes the organization to down time and security risks. Some Intrusion Detection Systems provide clustering capability, but this creates poor economies of scale. As you add more systems to the cluster, you use more resources in the clustering application and communications, and this reduces the resources needed for detecting intrusions.

Increasing scalability - Few Intrusion Detection Systems have the performance characteristics to meet the growing demands of enterprise application traffic. Although some IDS's are claiming better performance in future platforms, IP application deployments are growing at an equal or greater rate. And the rate of new attacks is growing exponentially, so new filtering rules need to be applied dynamically. An organization should build an infrastructure that allows easy scalability as traffic increases and as more security rules are applied.

Improving inspection efficiency - Traditional IDS devices do not have the ability to decrypt encrypted packets that they intercept. When an encrypted packet is intercepted, it is discarded by the IDS solution, greatly limiting the amount of traffic it is capable of inspecting.

Ease of management - Intrusion Detection Systems typically require one full time dedicated resource to engineer, monitor and maintain the system. System signatures must be constantly updated, reconfigured to align with new threats and security policies, and monitored to assess alerts and take appropriate actions.

F5 Solution Overview

F5 Network's BIG-IP® product combines the expertise of IDS, intrusion protection systems, and other application level scanning devices, and acts on their behalf to automatically respond to, act upon and prevent against changing application level security threats. Using VLAN mirroring or cloned pools, the BIG-IP product directs traffic to the appropriate security device without disrupting the flow of traffic for Intrusion Detection Systems. By using the BIG-IP client-side SSL proxy feature, in combination with VLAN mirroring or cloned pools, you extend the scope of your IDS device. Without this feature, most IDS systems are not able to process encrypted data, greatly compromising their effectiveness.

Enterprises can also use the BIG-IP product to set up and enforce common application level security policies using the product's Universal Inspection Engine (UIE) and iRules to filter and block application level attacks and threats. The BIG-IP product, through the iControl™ API, is the unifying prevention point. Specialized devices can inject their knowledge by creating, deleting or editing iRules, which are then enforced by the UIE. This functionality can be used to secure Web services, mobile applications and nearly any IP-based enterprise application. The result is an automated response, action, and prevention architecture to address continuous security threats.