eEye Digital Security

COMPARISON OF SecureIIS™ AND INTRUSION DETECTION SYSTEMS

The following comparison addresses the functionality and capability of **SecureIIS™** - The IIS Application Firewall and **Intrusion Detection Systems** (IDS) as they relate to securing Microsoft's IIS Web server application. This comparison only addresses each product's effectiveness in securing Microsoft's Internet Information Servers (IIS) Web server application.

SecureIIS is an application firewall designed specifically to secure IIS. The product functions as an ISAPI filter loaded onto IIS, and working within it to monitor all incoming and outgoing traffic to IIS. SecureIIS protects IIS from all "Classes" of attack utilized by hackers to break into IIS based servers. SecureIIS does not rely on a database of known vulnerabilities in IIS to provide that protection. As such, SecureIIS is able to protect against attacks *before* they are discovered and attack signatures are developed and disseminated to users. Case in point, SecureIIS protected IIS from the Code Red and Nimda Worms before the Worms were discovered by security research companies.

Intrusion Detection Systems are network or host based systems that are used to monitor network level traffic to block against undesirable traffic. These systems rely on databases of attack signatures that are maintained by product manufacturers and must be regularly updated by the user. In the case of the Code Red and Nimda Worms, IDS systems only started to protect systems against these worms after the worms were discovered and the IDS attack signature database was updated. SecureIIS protected against those worms before they were even discovered.

Intrusion Detection Systems may be credible and effective tools for detecting and blocking a wide range of undesirable network traffic. However, clients should be aware that IDS systems rely on databases of known attack signatures that are maintained by the manufacturer and must be updated by the user. For that reason, IDS systems are not enough to protect networks given that hackers are able to modify attack signatures to penetrate such systems or circumvent them all together. See eEye's white paper about this topic at http://www.eeye.com/html/Research/Papers/DS20010322.html.

Intrusion Detection Systems do not directly address the security of Microsoft's IIS Web application. The Web server tends to be the most vulnerable part of a network given that it needs to accessible by the Internet public. As such, IIS requires very focused and robust security.

SecureIIS is by far the most powerful protection for IIS given the fact that it is:

- designed specifically and exclusively for IIS;
- integrates with IIS (acting as an ISAPI filter) and wraps around IIS;
- looks for classes of attack and not attack signatures;
- does not require database updates;
- protects against attacks prior to their discovery;
- ease of implementation;
- low price point

	SecureIIS™ Application Firewall	Intrusion Detection Systems
Description	Application firewall designed specifically to secure Microsoft's Internet Information Servers (IIS) Web server application. Protects from all "Classes" of hack attacks that leverage Vulnerabilities in IIS. Product loads on the IIS server and works "within" IIS, examining all incoming and outgoing traffic to the Web server	IDS operate by detecting attacks occurring on a host on which it is installed. It works by intercepting OS and application calls, securing the OS and application configurations, validating incoming service requests, and analyzing local log files for after-the-fact suspicious activity.
Focus	Designed specifically to secure IIS against known *and* yet unknown security vulnerabilities and hack attacks	Provides intrusion detection protection for several host based applications – not specific to IIS and is independent of IIS.
Key Protection Approach	SecureIIS is designed to block general "classes" of hack attacks specifically targeting IIS. The product does not rely on attack signatures or a database of known vulnerabilities. In this manner, SecureIIS is able to protect not only against known vulnerabilities with identified and updated attack signatures. It can also protect against attacks that are yet undiscovered. Case in point, SecureIIS was protecting its users from the Code Red and Nimda Worms *prior* to their discovery.	IDS are intended to detect network intrusions based on a database of known attack signatures. Such databases must be maintained by the manufacturer and regularly updated by the user. IDS are intended to protect against such known attacks and rely on prompt updates by the user. While such systems would be able to protect against the Code Red and Nimda Worms after discovery and update, they was not able to protect against the Worms' IIS attack *prior* to the discovery of the Worms and the update to the product.
Types of Attack Protected in IIS	**CLASSES OF ATTACK** (Not relying on attack signatures) • Buffer Overflow Attacks • Parser Evasion Attacks • Directory Traversal Attacks • General Exploitation **ADDITIONAL PROTECTIONS** • HTTPS/SSL Protection • High Bit Shellcode Protection • Third Party Application Protection • Logging of Failed Requests **ADDITIONAL CHECKS** Additional checks are in place for attacks that do not follow recognized patterns. This approach provides extra security and protects against various attacks that involve data conversion problems. Limitations are also placed on the size of Uniform Resource Locators (URL/URI), HTTP variables, Request methods, Request Header Size, and other HTTP related content.	**CLASSES OF ATTACK** (Relying on attack signatures) • Directory Traversal • Remote Code Execution • Unauthorized Changes to Web Content **ADDITIONAL PROTECTIONS** • Analyze incoming HTTP traffic and via the use of generic rules and known attack signatures, determines if it is an attack. • Analyzes the HTTP server's actions to determine if they reflect its normal mode of operations. • General OS protection including buffer overflow prevention and binary modification
Ease of Implementation	Product can be downloaded and installed by client with minimal configuration and customization.	System involves network level installation, typically support by an installation services contract and significant customization.