TECHNOLOGY BRIEF

SOURCEFIRE ADAPTIVE IPS

KNOW MORE NETWORK RISKS
NO MORE GUESSING

SOURCEfire®

TODAY'S THREAT MANAGEMENT CHALLENGES

Today's threat and regulatory landscapes are causing organizations to increasingly require more from their security solutions. Many IT security departments are finding that they need to achieve significantly greater degrees of efficiency just to keep pace as:

- The diversity and sophistication of threats to their critical information resources continue to increase.
- The proliferation of new applications ensures a growing population of vulnerabilities that are ripe for exploitation.
- Technologies facilitating greater degrees of user mobility, interconnectivity with remote offices, and third-party access to networked resources introduce more entry points for threats.
- A plethora of regulatory compliance requirements consumes an increasing percentage of available IT resources.

To improve the effectiveness of their security infrastructure, many organizations have deployed a network intrusion prevention system (IPS). Historically, however, this technology has been somewhat of a paradox. Although it can reliably detect and prevent a wide range of network-borne threats, it has been criticized for the "noise" or false positives it creates and the corresponding effort required to separate significant events from the potentially overwhelming amount of insignificant events. Furthermore, even though security administrators understand the recommendation to tune their detection systems for the actual computing environment that is being protected, this is viewed as a significant operational burden. The result is that organizations typically accept a compromise, settling for an alternative that is less effective from a security perspective in exchange for reduced administrative effort—such as operating with a vastly reduced, generic set of inspection rules.

THE ADAPTIVE IPS FEATURE SET

Sourcefire's Adaptive IPS solution addresses an organization's need for better efficiency and effectiveness by significantly reducing the number of actionable security events and sharply reducing or eliminating the manual effort required to tune Sourcefire's IPS. The Adaptive IPS feature set consists of several components, including impact flags, RNA-Recommended Rules, adaptive traffic profiles, non-standard port handling, and contextually aware engine—all of which work together to ensure that the Sourcefire IPS™ prioritizes and processes traffic without introducing noise, without blocking legitimate traffic, and without missing critical attacks.

Impact Flags

Sourcefire RNA™ (Real-time Network Awareness) leverages a vulnerability database to generate a list of an asset's potential vulnerabilities. RNA uses this vulnerability data to make its impact analysis more accurate. The Sourcefire Defense Center™, a highly customizable central management console that provides event aggregation, asset monitoring, and Sourcefire 3D™ Sensor management, can correlate security event data with a target's operating system, services, applications, and potential vulnerabilities in real time. By comparing attacks to the assets of the hosts under attack, the Sourcefire 3D System can assign an "impact" value to the attack and visually represent this impact with a prioritized impact flag on the Defense Center dashboard. By determining the relevance and impact of each intrusion attack on your network, actionable events are typically reduced by 99% or more, and security analysts can focus their attention only on those events that matter most.

RNA-Recommended Rules

The RNA-Recommended Rules (RRR) feature leverages the power of Sourcefire RNA to recommend a set of IPS rules for a user's particular network environment. From a functional perspective, RRR involves three steps. First, RNA establishes a profile for a given network, identifying all hosts, the operating systems (OSes) and services they are running, the ports they are using to communicate, and the vulnerabilities to which they are potentially susceptible. Next, this inventory is compared to the rule set for the 3D Sensor(s) with IPS protecting the profiled network. The result is a set of recommendations for rules that should be added or removed from this rule set. For example, a profile indicating the presence of Linux-based hosts would result in the recommendation to add "missing" Linux-oriented rules to a 3D Sensor configuration that did not already have some (or all) of them in place. Finally, security administrators can choose to accept the recommendations as is or modify them as desired. To aid this step, recommended rules are conveniently organized by category (e.g., OS, service, threat type), and can be selected individually, by category, or all at once. Furthermore, exceptions can be configured to suppress unwanted recommendations from recurring in the future.

RNA-Recommended Rules can provide semi-automated IPS tuning as users have the opportunity to review changes and intervene in the tuning process. An additional mode allows RRR to make fully automated tuning decisions at scheduled intervals without human intervention.

The balance of the Adaptive IPS features typically impact only certain portions of the 3D Sensor configuration (e.g., the subset of rules that deal with host OSes). Administrators have complete control of whether, and to a certain extent how, these features are implemented.

Adaptive Traffic Profiles
Most IPSes are configured to inspect segmented and fragmented traffic from the viewpoint of a single operating system type. Given this limitation, the potential exists for a clever hacker to circumvent an IPS' detection engine. But by modeling segmented and fragmented traffic in the same manner in which the host operating system would see it, the potential for circumventing a Sourcefire IPS is greatly reduced.

Non-Standard Port Handling
The relationship between certain services and ports is based on convention. Nothing precludes the use of non-standard ports (e.g., running HTTP on TCP 8080 instead of TCP 80). In fact, some organizations purposely take advantage of non-standard ports for management or security reasons. Alternately, hackers and various user-centric applications (e.g., file sharing, IM) will often use non-standard ports to hide their activities.

Sourcefire's non-standard port handling capability automatically accounts for such scenarios. This is accomplished by dynamically applying the appropriate rules for a given session based on input from RNA that identifies the actual relationship between ports and services for the associated hosts. The net result is that administrators do not need to manually configure rules for known cases where services are running on non-standard ports.

Contextually Aware Engine
Sourcefire is moving toward allowing RNA-Recommended Rules to operate fully dynamically. Sensor rule sets will be dynamically modified in real time to correspond to the network and host profiles that are seen in a customer's environment. The contextually aware engine feature will include:

- The RNA-driven automated population/definition of variables (e.g., $HTTP_SERVERS) that control the invocation of various 3D Sensor pre-processors.
- The ability to recommend rules and dynamically adjust 3D Sensor configurations based on data and attributes obtained from external tools (e.g., vulnerability scanners, patch management systems) via the Sourcefire Host Input API.

THE BENEFITS OF ADAPTIVE IPS

Organizations can derive the following benefits from implementing Sourcefire's Adaptive IPS solution:

- **Operational efficiency is improved.** Real-time, automated intrusion event impact assessment through impact flags typically reduces the number of actionable events by 99% or more. In addition, whether semi-automatic or fully automated, the tuning options afforded by Adaptive IPS can significantly reduce the effort required to establish and maintain ideal configurations for 3D Sensors, especially in highly dynamic computing environments. These capabilities also have the side benefit of freeing security administrators and analysts to spend cycles tackling other challenges, such as securing a new VoIP implementation or addressing the ever-growing population of compliance requirements.
- **Security effectiveness is improved.** Adjusting packet processing techniques, inspection rules, and other aspects of 3D Sensor configuration to correspond to the relevant characteristics of the actual systems that are being protected is certain to reduce false positives and false negatives, thereby enabling security administrators to identify and respond more quickly to those events that matter most, and ensuring that attacks are properly blocked. Making these adjustments in a fully dynamic manner only serves to multiply the advantage.
- **System performance is improved.** Both individual 3D Sensors and the Defense Center management infrastructure benefit from the elimination of unnecessary rules and the corresponding stream of events that they would inevitably generate.

For more information about Adaptive IPS, visit Sourcefire's web site at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Solutions Network™ today.