



Making Intrusion Event Analysis easy

June 3rd, 2009

SOURCE*fire*

ENTERPRISE THREAT MANAGEMENT

Agenda



- ❏ Adaptive IPS Today
- ❏ Adaptive IPS with RNA
- ❏ Competitive Comparisons
- ❏ Adaptive IPS Benefits





Adaptive IPS In-Depth



What is Adaptive IPS?



- ❏ Strategy for making the IPS:
 - Contextual
 - Self-tuning
 - Performance-efficient
 - More accurate and non-evadable
- ❏ Leverages network intelligence provided by RNA
- ❏ Benefits:
 - See only what's relevant
 - Handle more traffic faster
 - Put less effort into tuning
 - Avoid security evasions and detect traffic more accurately

Adaptive IPS Components



1. Impact Analysis
2. Automated IPS Tuning
3. Adaptive Traffic Profiles
4. Non-Standard Port Handling



1. Impact Analysis



📦 We know what this is! Impact Flags!

| Impact Flag Rating | Target Network Monitored by RNA | Target Host Monitored by RNA | Exploit Matches Target OS and/or Service | Exploit Targets a Known Vulnerability |
|--------------------|---------------------------------|------------------------------|--|---------------------------------------|
| 1 | Yes | Yes | Yes | Yes |
| 2 | Yes | Yes | Yes | No |
| 3 | Yes | Yes | No | No |
| 4 | Yes | No | Unknown | Unknown |
| 0 | No | No | Unknown | Unknown |

- 📦 Impact Flag 1 – Act immediately!
- 📦 Impact Flag 2 – Investigate
- 📦 Impact Flags 3, 4 & 0 – Good to know

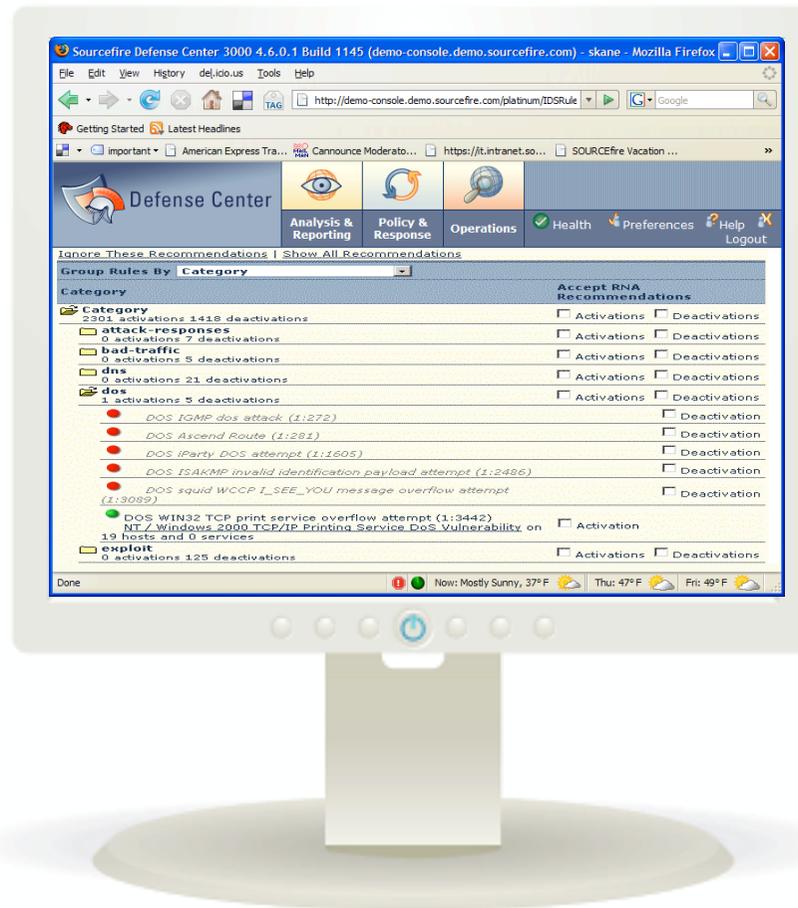
2. Automated IPS Tuning



- We know this one, too!
- RNA Recommended Rules
 - RNA recommends Snort rules to enable based on the assets you're protecting
 - Maximizes network protection
 - Maximizes 3D Sensor resources



Let's See a Demo!



3. Adaptive Traffic Profiles

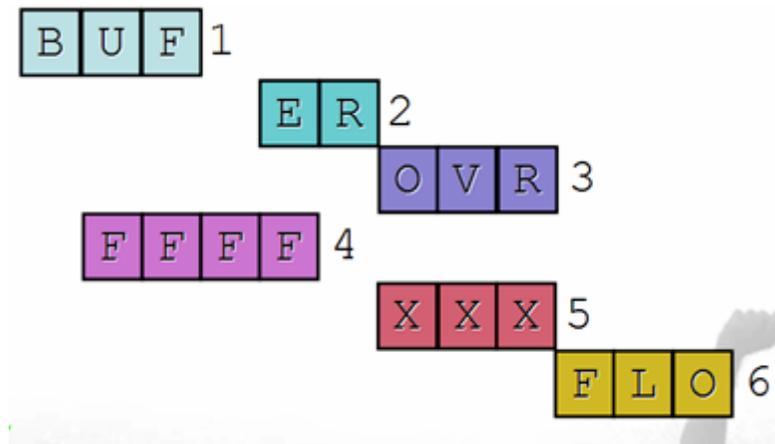


- ❏ Uses RNA network intelligence about the target host's operating system
- ❏ Models traffic the way that operating system would see it
- ❏ Other IPS products need to make assumptions about how to model traffic that are often wrong
- ❏ Avoids evasions

3. Adaptive Traffic Profiles, cont.



- Different operating systems sometimes “see” the same traffic differently
- If IPS and target see traffic differently, this can cause evasions
- Danger: IPS misses the attack but the target sees it



| | | | | | | | | | | | | |
|----------|---|---|---|---|---|---|---|---|---|---|---|---|
| Win32 | B | U | F | F | E | R | O | V | R | F | L | O |
| FreeBSD | B | U | F | F | F | R | O | V | R | F | L | O |
| LaçerJet | B | F | F | F | E | R | X | X | X | F | L | O |

4. Non-Standard Port Handling



- ❏ IPS automatically applies appropriate rules to traffic on non-standard ports
- ❏ If HTTP is running on port 8080, RNA knows this. The Defense Center will instruct the IPS to apply HTTP rules to port 8080.
- ❏ Benefits:
 - Reduced manual administrator tuning
 - Maximized network protection

Adaptive IPS – Industry Comparison



| Capability |  |  |  |  |  |  |
|----------------------------|---|--|---|---|---|---|
| Impact Analysis | ✓ | | Limited | Limited | | |
| Automated IPS Tuning | ✓ | | | | | |
| Adaptive Traffic Profiles | ✓ | | | | | |
| Non-Standard Port Handling | ✓ | | ✓ | Limited | | |

Summary of Benefits



- ❏ Maximizes network protection
- ❏ Maximizes IPS performance
- ❏ Minimizes the quantity of actionable events
- ❏ Minimizes the need for manual IPS tuning
- ❏ Minimizes false positives
- ❏ Minimizes network security risks



Adaptive IPS Technology Brief



Available now!

http://www.sourcefire.com/resources/downloads/public/techbrief/SF_TB_AdaptiveIPS.pdf

SOURCEfire
Security for the real world.

TECHNOLOGY BRIEF

Sourcefire Adaptive IPS

MANAGEMENT

Regulatory landscapes are increasingly look for more solutions. Many IT security teams that need to achieve degrees of efficiency just to keep up with the sophistication of threats to their resources continue to find new applications ensures a new level of security that are ripe for exploitation. Increasing the degree of user activity with remote offices, access to networked resources by mobile devices, and regulatory compliance increases the number of IT resources. Organizations have pursued to increase their security through the employment of a network system (IPS). Historically, IPS technology has been somewhat of a niche product that is not as reliable as other network-based security solutions. The "noise" it creates and the effort required to separate the signal from the noise (i.e., insignificant events) from a potentially large volume of events is often a significant barrier to the adoption of systems for the actual protection that is being provided. Organizations typically accept a significant operational burden for an alternative that is less effective in exchange for a reduced, generic set of features.

IPS FEATURE SET

Adaptive IPS addresses organizations' need for efficiency and effectiveness by minimizing the effort required to manage IPS sensors. The Adaptive IPS consists of several components, including Recommended Rules, IPS evasion and port handling, and Windows, then a subtly crafted threat will be detected. The IPS Evasion is achieved by eliminating the question. This is accomplished by adjusting the input from RNA that system of the destination figure exceptions is also addressing the feature for matching that corresponding sampled in a particular way. The relationship between the ports is based on the use of non-standard ports. In fact, some organizations will use non-standard ports for such scenarios. This is typically applying the given session based on the actual ports and services for the net result is that save to manually configure where services are running.

Sourcefire is moving recommended Rules to real time to correspond to profiles that are seen in a Advanced self-tuning will protect population/definition of IP_SERVERS that control sensor pre-processors. Send rules and dynamically based on data and external tools (e.g., patch management input API).

RNA-Recommended Rules. The RNA-Recommended Rules feature leverages the power of RNA (Real-time Network Awareness) to recommend a set of IPS rules for a user's particular environment. From a functional perspective, RNA-Recommended Rules involves three steps. First, RNA establishes a profile for a given network, identifying all hosts, the operating systems 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 IPS sensor(s) protecting the profiled network. The result is a set of recommendations for rules that should be added or removed from this ruleset. For example, a profile indicating the presence of Linux-based hosts would result in the recommendation to add "missing" Linux-oriented rules to a sensor configuration that did not already have some (or all) of them in place. Finally, security administrators can choose to accept the recommendations wholesale or modify them as desired. To aid this step, recommended rules are conveniently organized by category (e.g., operating system, service, threat type), and can be selected either 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, or facilitated, IPS tuning as users have the opportunity to review changes and intervene in the tuning process. An additional mode allows RNA-Recommended Rules 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 sensor configuration (e.g., the subset of rules that deal with host operating systems). Administrators have complete control of whether, and to a certain extent, how these features are implemented.

IPS Evasion Avoidance. Different operating systems handle the reassembly of fragmented traffic differently. Unfortunately, this provides the opportunity for hackers to take advantage of a technique known as evasion. In an IPS evasion, threats are crafted and fragmented in very specific ways that enable them to appear benign to an IPS while still having the desired, negative effect on the targeted host. For example, if the target host is a BSD box but the inspection engine is reassembling traffic in the same manner as

THE BENEFITS OF ADAPTIVE IPS

Organizations can derive the following benefits from Adaptive IPS:

- Operational efficiency is improved. Whether semi-automatic or fully dynamic, the tuning options afforded by Adaptive IPS can significantly reduce the effort required to establish and maintain ideal configurations for IPS sensors, especially in computing environments that are subject to continuous change. This also has 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 sensor configuration 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 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.

Finally, Adaptive IPS is an integral part of the Sourcefire 3D System. The same infrastructure that enables the Adaptive IPS feature set also provides the full range of capabilities and benefits that are associated with a complete Enterprise Threat Management (ETM) solution—including network behavior analysis (NBA), network access control (NAC), and vulnerability assessment (VA) from a technical perspective, as well as vastly improved efficiency and effectiveness from an operational perspective.

For more information about Adaptive IPS, Enterprise Threat Management, or the Sourcefire 3D System, visit Sourcefire's web site at www.sourcefire.com or contact Sourcefire today.

SOURCEfire 2

Questions?

