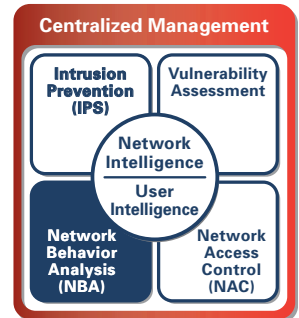


Sourcefire Network Behavior Analysis

The best approach to network security is one of layered defenses, commonly referred to as “Defense in Depth”. Relying on perimeter-based firewalls and IPSes alone does nothing to guard against attacks that originate from the inside—whether an attack is initiated by a malicious insider or a worm is unknowingly propagated by a trusted employee.

Fortunately, a new approach to defending the internal network has emerged. An approach that not only augments existing Information Security defenses, but also offers collateral benefits to solving everyday Network Operations challenges. Introducing Sourcefire Network Behavior Analysis (NBA), a key component of Sourcefire’s Enterprise Threat Management (ETM) solution.



Sourcefire NBA at a glance:

- Detect and contain worm propagation
- Establish and enforce IT compliance policies
- Monitor contractors and guests
- Harden network assets before the attack
- Improve IPS efficiency and effectiveness
- Evaluate network bandwidth utilization
- Troubleshoot network performance issues
- Monitor network resource usage
- Detect network changes in real-time

“Sourcefire’s RNA is like a magic eye that watches everything happening on your network.”

NetworkWorld

BRIDGING THE GAP BETWEEN INFORMATION SECURITY AND NETWORK OPERATIONS

NBA is one of the fastest-growing segments in network security today. Originally fueled by rampant outbreaks of computer-based worms (e.g., Zotob, AnnaKournikova, Mydoom, Sasser), NBA technology has evolved over time to augment a company’s IT compliance enforcement capabilities, while providing new capabilities for monitoring bandwidth utilization and troubleshooting network outages and performance degradations. As a result, NBA technology is bridging the gap between Information Security and Network Operations by providing a unified framework for solving daily challenges faced by both organizations.

SOURCEFIRE NBA BENEFITS FOR INFORMATION SECURITY

Sourcefire’s NBA solution offers numerous benefits for Information Security professionals, including:

- ▶ **Detect and quarantine internal threats** – Establish “normal” traffic baselines and detect network anomalies. Security analysts can receive real-time alerts via e-mail, SNMP or through a third-party SIEM using Sourcefire’s eStreamer capability. Endpoints accessing unauthorized resources or propagating worms can be quarantined at the router or firewall using Sourcefire’s Remediation API.
- ▶ **Establish and enforce IT compliance policies** – Create, monitor and enforce customized IT compliance policies, through whitelists and/or customized rules, and detect violations of those policies in real time. Achieving compliance not only helps to harden assets and prevent unauthorized data leakage, but also helps to achieve government (e.g., SOX, HIPAA, FISMA) and/or industry (e.g., PCI) compliance.
- ▶ **Monitor contractors and guests** – IT has enough challenges securing “managed” devices, much less “unmanaged” devices used by contractors and guests that may appear on any given day. By leveraging RNA’s real-time, passive network discovery, IT can be alerted instantly when a new host appears. Surgical host scans can be automatically triggered using Nessus or other vulnerability scanners, and IT can be alerted any time the new host attempts to access an unauthorized network resource.
- ▶ **Harden network assets before the attack** – Sourcefire RNA™ (Real-time Network Awareness) passively detects hosts as they appear on the network, inventories their assets (e.g., OS, services, ports, protocols) and detects potential vulnerabilities. Information Security professionals can harden assets before the attack by applying key patches and shutting down unnecessary ports, services and unauthorized applications.
- ▶ **Improve IPS efficiency and effectiveness** – Endpoint intelligence collected by Sourcefire’s NBA solution is correlated against Sourcefire IPS™ intrusion events. Impact Flag severity ratings are assigned to each intrusion event, enabling security analysts to focus their attention on those events that matter most. Sourcefire RNA can also recommend Snort® rules to enable and disable based on actual assets protected—a key component of Sourcefire’s Adaptive IPS strategy.

SOURCEFIRE NBA BENEFITS FOR NETWORK OPERATIONS

Sourcefire’s NBA solution also offers significant benefits for Network Operations professionals, including:

- ▶ **Evaluate network bandwidth utilization** – By leveraging flow data generated by Sourcefire RNA and/or NetFlow-enabled routers and switches, network analysts can monitor bandwidth consumption on all corners of the network, ensuring that ample bandwidth is provisioned across the entire organization.



Sourcefire NBA Flow Data:

- Flow type (RNA or NetFlow)
- First and last packet timestamps
- Total bytes transferred
- Total packets transferred
- Source and destination IP addresses
- Source and destination ports
- Source and destination protocols*
- Source and destination operating systems*
- Source and destination services*
- Source and destination usernames**
- Source and destination client applications and URLs used within the transaction*

* Sourcefire RNA required
** Sourcefire RUA required

- ▶ **Troubleshoot network performance issues** – Analyze NBA flow data to uncover root causes to network outages and performance degradations. Receive alerts and investigate network performance events before users even pick up the phone.
- ▶ **Monitor network resource usage** – Sourcefire's NBA solution can help to determine which network resources are actually used and which aren't, providing hard data for IT to reference in defending recommendations for retiring legacy applications and services.
- ▶ **Detect network changes in real-time** – Leveraging RNA's real-time, passive network discovery, Network Operations can be notified the moment a new host appears on the network and/or when an existing host has changed its approved configuration (e.g., OS upgrade, new service, new port).

EXTENDING THE REACH WITH NETFLOW ANALYSIS

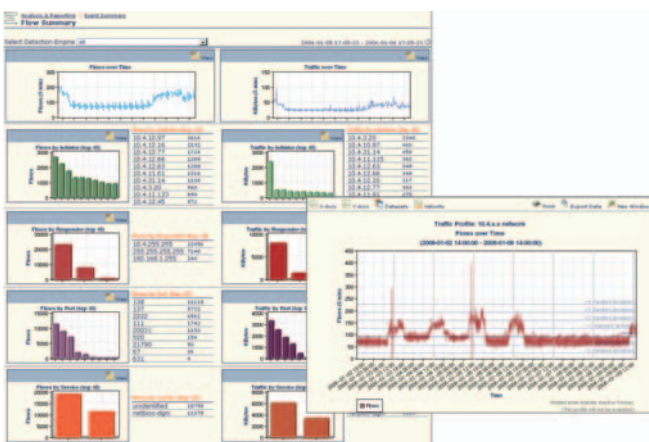
Sourcefire RNA generates rich flow data by passively detecting traffic segments monitored by Sourcefire 3D Sensors and creating proprietary flow records of host-to-host communications. RNA Flows capture traditional NetFlow metrics, such as source/destination IP, timestamps, quantity of packets/bytes transmitted, and ports. But RNA Flow goes beyond traditional NetFlow data by also inferring Layer 7 attributes, such as operating systems, services, select applications and potential host vulnerabilities. However, in the event there are network segments not covered by RNA, Sourcefire offers a full-featured NetFlow Analysis capability to extend the reach if its NBA solution to corners of the network where 3D Sensors don't yet exist.

LINKING USERS TO SECURITY AND COMPLIANCE EVENTS

Sourcefire RUA™ (Real-time User Awareness) is an important component of the Sourcefire 3D System, responsible for linking Active Directory and LDAP usernames to security and compliance events. With RUA, Information Security and Network Operations professionals can resolve incidents and troubleshoot problems more quickly and easily—when time is of the essence. No longer do analysts have to manually sift through Active Directory or LDAP log files. User identity is right at your fingertips, including username, full name, phone, email and department.

THE POWER OF INTEGRATION

There are many NBA solutions on the market today. But when selecting the NBA solution that's right for you, it's important not only to evaluate the base functionality of the solution, but also how it integrates within your existing network security and systems management infrastructure. According to a major IT research analyst firm, Sourcefire offers the best IPS/NBA integration on the market. Using the Sourcefire 3D System, one integrated console is used to manage all Sourcefire Enterprise Threat Management (ETM) solutions, including IPS, NBA, NAC and Vulnerability Assessment. Furthermore, using Sourcefire's series of APIs (e.g., Remediation API, Host Input API) and other interfaces (e.g., eStreamer, SNMP), the 3D System can integrate into a variety of network infrastructure, SIEM, Vulnerability Management, Patch Management, Help Desk and Systems Management solutions.



Sourcefire's NBA solution offers significant benefits for Information Security and Network Operations professionals alike. Using the Sourcefire 3D System, Information Security personnel can establish "normal" traffic baselines and detect anomalies (e.g., worm propagation), while Network Operations personnel can evaluate bandwidth consumption and troubleshoot root causes for network outages and performance degradations.

CONTACT SOURCEFIRE TODAY!

For more information about the Sourcefire 3D System, including Sourcefire's Network Behavior Analysis solution, contact your Sourcefire sales representative or call 1.800.501.6008.

www.sourcefire.com

Copyright ©2007, Sourcefire, Inc. All rights reserved. SOURCEFIRE®, SNORT®, the Sourcefire logo, the Snort and Pig logo, SECURITY FOR THE REAL WORLD™, SOURCEFIRE 3D™, SOURCEFIRE DEFENSE CENTER™, SOURCEFIRE IPS™, SOURCEFIRE MASTER DEFENSE CENTER™, ESTREAMER™, SOURCEFIRE RNA™, SOURCEFIRE RUA™, DAEMONLOGGER™, OFFICECAT™ NETWORK USAGE CONTROL™ (NUC) and certain other trademarks and logos are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries.