

The Sourcefire logo features the word "SOURCE" in a bold, dark blue, sans-serif font, followed by "fire" in a lowercase, orange, script font.

REAL-TIME NETWORK AWARENESS™
Enabling Intelligent Network Security

For more information on Sourcefire solutions in the UK: contact Phoenix Datacom
Phoenix House, Smeaton Close, Rabans Lane, Aylesbury, Bucks, HP19 8UW
T: 01296 397711 E: info@phoenixdatacom.com W: www.phoenixdatacom.com/security

P H O E N I X
D A T A C O M

www.sourcefire.com

Sourcefire, Inc.
9212 Berger Road
Suite 200
Columbia, MD 21046

August 2004

TABLE OF CONTENTS

Table of Contents	2
Introduction	3
Sourcefire Intrusion Management System – Redefining the Industry	3
Real-time Network Awareness	3
Passive Network Discovery	4
Continuous Change and Vulnerability Monitoring/Management	4
Elimination of False Positives and Negatives	5
figure 1. Policy Optimization	5
Intelligent Intrusion Detection and Response	6
Security Monitoring and Threat Detection.....	6
Threat Mitigation	7
Integrated High Performance System Management.....	7
Meaningful Correlation.....	8
figure 2. Meaningful Correlation	8
Ultra High Performance Data Aggregation	8
Conclusion.....	9

INTRODUCTION

Today, networks are becoming increasingly complex and traditional security devices are failing to meet the needs of enterprises. False positives continue to plague intrusion detection systems (IDS), costing time and money to investigate and often causing real attacks to go unnoticed. The tremendous amounts of information generated by today's IDS are becoming increasingly difficult to manage while making sense of the information requires greater skill on the part of the administrator.

Since the inception of the concept in 1980 by James Anderson, intrusion detection systems have tried to solve the critical function of identifying network threats and misuse. Early intrusion detection systems (IDS) promised to reveal what was happening on networks but overwhelming amounts of false positives and inflexible detection techniques quickly overshadowed any benefits. Users couldn't make sense of the data, which led to reduced usability. While detection methodologies have improved to detect known and unknown threats, it is still up to the administrator/analyst to sort through a tremendous amount of data in order to determine if an actual attack occurred, what happened, and what should be done about it. The focus of most vendors has been to increase the accuracy of detection and reduce the risk of potentially evading the sensor. But improved detection and traffic analysis alone can never truly solve the problems of false positives, false negatives and evasion. The problem has remained the same over the years. Attacks are occurring on the network and enterprises need to know when and how to best respond.

SOURCEFIRE INTRUSION MANAGEMENT SYSTEM – REDEFINING THE INDUSTRY

Today, Sourcefire offers revolutionary new technologies that create a fully integrated security monitoring infrastructure for identifying and protecting against network threats. These systems include **Sourcefire Real-time Network Awareness™** for proactive passive network discovery and analysis; **Sourcefire Network Sensors** for state-of-the-art network monitoring with the industry's most accurate threat detection and prevention; and **Sourcefire Management Console** for integrated, high performance system management and threat response.

REAL-TIME NETWORK AWARENESS

One of the inherent issues with traditional intrusion detection systems is that a fundamental lack of information leads to a great deal of ambiguity – sensors operate with virtually no compositional knowledge of the network components they are defending. Sourcefire Real-time Network Awareness™ (RNA) solves this problem by providing continuously updated, persistent information about all of the active components of a network. This provides the contextual data required to disambiguate the environment in which the IDS operates, allowing the IDS to start protecting assets, not protocols or traffic.

Passive Network Discovery

Sourcefire RNA utilizes a combination of passive network discovery, behavioral profiling and vulnerability analysis techniques to provide unprecedented visibility of the network environment. This combination offers a complete and accurate profile of the hosts and services that are being monitored, enabling administrators to confidently manage the configuration of their security infrastructure.

This unique approach delivers the benefits of network discovery, mapping, and vulnerability analysis without the drawbacks of traditional host-based or active scanning approaches. Unlike active network scanners, RNA consumes no network bandwidth and is not disruptive to network assets. By remaining an 'observer' on the network, RNA is capable of evaluating the potential threat a given host poses to your organization without causing the potential downtime or service impact associated with traditional vulnerability scanning or tipping off the potential attacker to its presence.

A large percentage of the systems on the network can go unknown or can be poorly maintained at the time of compromise. Since RNA provides a persistent understanding of the network, the 'point in time' problem associated with traditional network scanners is eliminated. The immediate availability of critical and relevant information finally enables proactive response to potential threats and significantly reduces time to resolution for security related incidents. With RNA as a constant observer analyzing the information available, hosts cannot be 'hidden' like they can from active scanners; any active elements on the network are discovered and analyzed as they produce traffic.

In addition, since RNA does not rely on host-based technologies, discovery of 'unknown' assets is possible. This pervasive awareness provides constant protection for the ever-evolving networks that organizations are forced to maintain. Any system introduced into the network, authorized or not, is immediately analyzed and its threat potential made known to the security staff. Centralizing this discovery and analysis of threat at the network layer eliminates the traditional overhead costs and maintenance required for host-based software.

Continuous Change and Vulnerability Monitoring/Management

Sourcefire RNA continuously discovers and monitors network assets and provides notifications of any observed changes, including the introduction of new network assets, services, behaviors, or anomalous traffic patterns and policy violations.

For example, network environments usually have a set of servers that are statically configured, such as a web server. In the event that the web server is compromised and an attacker establishes a new service on the host like IRC or SSH, use of that service would be noticed and analyzed by the RNA system, initiating a change notification to administrators.

This benefit can also be seen any time a system is rebuilt without the administrator's knowledge, which potentially exposes new vulnerabilities or avenues for intellectual property theft. Because RNA is constantly discovering the network, it will notice the system's new configuration and service offerings and automatically associate these changes in network assets with potential vulnerabilities and exploits that may target those vulnerabilities.

For example, when a developer is tasked with creating a new service offering for a business partner, a production environment outside of the normal asset deployment process may be built. This method of ad-hoc development enables rapid development and deployment of new services, but also introduces otherwise unknown security risks. If Sourcefire's Real-time Network Awareness™ technology were deployed, the security team would immediately be made aware of these new systems and associated vulnerabilities. Since RNA is constantly evaluating the threat potential of all systems on the network, a threat profile is developed and readily available even before new services are moved into production. This results in increased security and reduced deployment costs.

Elimination of False Positives and Negatives

Network intrusion detection systems operate by analyzing traffic on the network and applying various types of analysis to the protocols and packets that they observe. Most of this analysis is done without one key piece of information: the composition of the actual assets being targeted by attackers. Without this information, the IDS is at a disadvantage against the advanced attacker, who can exploit these ambiguities to cause the IDS to miss an attack. This phenomenon, known as 'false negatives,' can be eliminated with the knowledge RNA provides to the IDS.

Another classic problem with NIDS is false positives. False positives occur for a number of reasons, but one of the primary reasons is because the IDS lacks the contextual information surrounding the data that it collects. A classic example would be an intrusion detection system alerting a "Code Red" attack against a Linux web server that cannot possibly be vulnerable to that exploit. If the IDS merely knew what operating system the target host was running, it would know that the attack could be de-prioritized to an "informational" level instead of being prioritized as a critical security event.

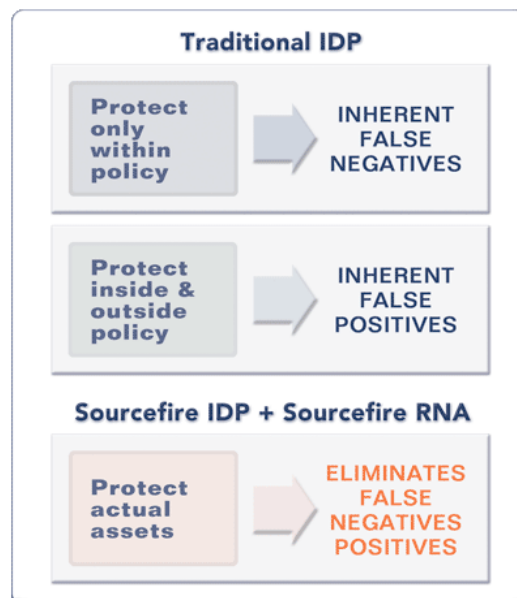


figure 1. Policy Optimization

Unless an intrusion detection system is aware of the targets it is monitoring, it will inevitably produce false positives or false negatives. Sourcefire RNA enables users to know exactly what the sensor is monitoring and specifically tune the ruleset to protect actual assets, eliminating both false positives and false negatives. Now administrators can optimize their intrusion detection and prevention policies to include asset-specific rule sets and anomaly parameters effortlessly.

Intelligent Intrusion Detection and Response

Sourcefire RNA can generate asset, change and vulnerability reports that in turn give the security administrator complete knowledge of the assets requiring protection. From the Sourcefire Management Console, users can translate this information into proper configuration documentation and confidently perform rapid rule tuning for their Sourcefire Network Sensors. This level of network intelligence greatly improves the performance of the sensors and accuracy of the detection methodologies. Administrators can now unquestionably configure sensors for the environment it monitors, enabling it to make more advanced and relevant decisions about potential threats. This intelligence in detection, coupled with the performance and flexibility of Sourcefire Network Sensors, ultimately enables administrators to configure automatic response mechanisms to close potential attack vectors immediately.

SECURITY MONITORING AND THREAT DETECTION

The contextual knowledge provided by Sourcefire RNA is specifically designed to complement the precision and flexibility inherent in Sourcefire Network Sensors (NS). Every network is different and not all alerts are important to all organizations. Often alerts are raised for behavior that is actually legitimate or benign within a certain environment, resulting in loss of time and resources by administrators needing to investigate each event. Sourcefire eliminates this problem by allowing users to enable, disable or modify individual rules that are not applicable to the environment being monitored. In addition, custom rules can be created to define known valid traffic without reducing the threat coverage provided to the rest of the network or that specific host.

For example, access to the default 'scripts' folder of an IIS web server is considered a potential threat to the organization. This is because there are sample applications shipped with IIS that are known to be vulnerable to attack. In most cases the scripts folder is removed or otherwise rendered benign. Should there be a specific application that is configured to run under the scripts folder, a rule could be written to allow access to this known, good application without raising an alert and without reducing coverage for that web server or any other unknown entities in the network that may not be configured properly.

Sourcefire Network Sensors offer the industry's most accurate network monitoring and detection capabilities. This precision is achieved through an advanced combination of rule-based and protocol anomaly detection methods. In addition, Sourcefire provides users the ability to edit existing and write new rules to suit their specific environment, ensuring the detection of both known and unknown threats.

Sourcefire Network Sensors enhance the defense in depth concept by monitoring and analyzing network traffic and alerting when suspicious activity is detected.

THREAT MITIGATION

Understanding that controlling access to the network assets and services is the first line of defense for your network, Sourcefire Intrusion Management System is designed with the flexibility to work with traditional access control devices, providing users with the most effective strategy for threat mitigation at both the perimeter and deep within the core.

Sourcefire Intrusion Management System provides the ability to completely model organizational policies; not only mitigating, but often eliminating threats against an organization's network assets.

For example, Sourcefire Network Sensors can be configured to audit traffic originating from your network to the Internet for interesting activity. The flexibility of the rules language makes it possible to write rules that will alert on or block traffic if a database server connects to the Internet, potentially preventing the theft of confidential information in the case of compromise. Sourcefire Network Sensors can also be configured to mirror the firewall policies currently in place and respond appropriately if a discrepancy is found. This brings a check and balance to your control systems and significantly reduces the potential for human error to go unnoticed until it is too late.

If the corporate policy does not allow access to web based email systems, rules can be written to detect the transmission of email over http or another protocol and then instruct the firewall to prevent any further activity for the parties involved. While instructing the firewall to prevent this activity, an alert is raised to the security staff so that they can investigate and respond appropriately.

This integration ultimately enables traditional firewall devices to perform tasks similar to next generation firewalls and emerging 'intrusion prevention' devices without requiring a replacement or overhaul of the current architecture.

In addition, through strategic partnerships like Check Point's OPSEC program, Sourcefire's products can trigger firewall responses to stop malicious traffic from entering a corporate network. This solution is easily implemented without requiring additional capital investment or introducing additional points of failure.

INTEGRATED HIGH PERFORMANCE SYSTEM MANAGEMENT

The value of these technologies is exponentially increased with the addition of a Sourcefire Management Console (MC), which tightly integrates the information from Sourcefire RNA™ with Sourcefire Network Sensors, providing a level of contextual intelligence that finally enables users to protect the real targets on their networks instead of merely attempting to assess the hostility of the packets traversing the network.

Sourcefire Management Console (MC) is the industry's highest performance management tool for intrusion detection deployments, specifically designed for large distributed enterprise networks. Sourcefire MC simplifies the complicated issues usually associated with intrusion detection system (IDS) deployments by incorporating an ultra high-performance database and enabling grouped sensor management, data aggregation, policy management and configuration

control. All this is available through an easy-to-use interface that facilitates the industry's fastest and easiest installation process.

Meaningful Correlation

Sourcefire Management Console tightly integrates information on network changes produced by Sourcefire RNA and Network Sensors with the latest vulnerability information to determine why the change has occurred and whether or not an attack poses an actual threat. This information allows users to quickly and accurately prioritize the responses.

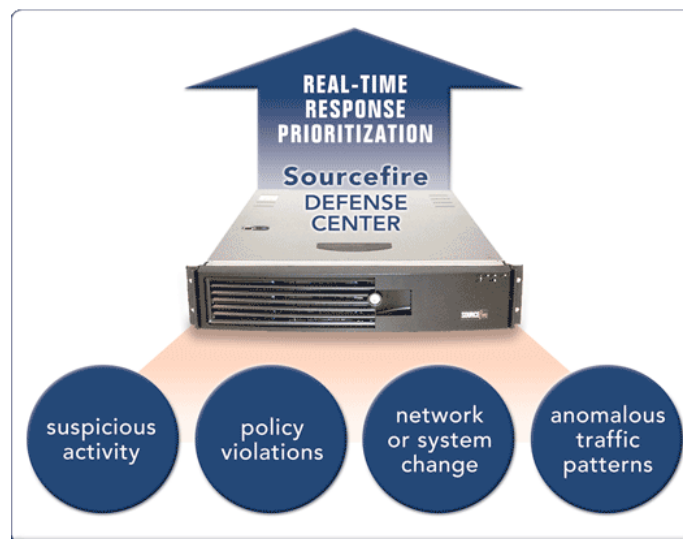


figure 2. Meaningful Correlation

Ultra High Performance Data Aggregation

Sourcefire MC is delivered with a built-in high performance database capable of handling tens of millions of events for identification of long-term security trends while also allowing in-depth forensic analysis down to the individual packet level. The database is preinstalled, preconfigured and self-maintaining, allowing administrators to focus on what is important - gaining an unprecedented level of network security awareness through real time consolidation and analysis of every event identified within the IMS network grid over a time horizon limited only by the amount of disk space on the Management Console.

From a single interface, event information from various Network Sensors can be aggregated into a holistic view of the network sensor grid, providing analysts with the ability to correlate highly granular event data with the most up to date vulnerability information available. For the first time, security administrators are provided with the information they need to reduce threats, prevent attacks and respond to compromises.

CONCLUSION

Network intrusion detection continues to be a field of evolving technology that to date, has offered great promise while delivering solutions that have been somewhat less than satisfying. In order for IDS to reach its full potential, a significant amount of context is required to help validate the output of systems as well as properly prioritizing the data.

The Sourcefire IMS is specifically designed to address these needs. The Sourcefire RNA™ appliance is architected to generate the underlying information infrastructure required to perform effective intrusion detection, as well as serving other critical security needs such as asset identification and vulnerability analysis. Sourcefire's MC brings the data from the RNA™ appliance together with the output from Sourcefire Network Sensors to correlate attacks with vulnerabilities and change data providing validation and appropriate prioritization of security events.

This Security Monitoring Infrastructure will finally let intrusion detection technology achieve its full potential. Integrating network discovery, vulnerability analysis, integrity assurance, intrusion detection and event correlation together, Sourcefire is producing a full end-to-end network security solution that allows users to leverage essential security data more effectively, reducing security costs and improving the effectiveness of security administrators.