



TECHNOLOGY BRIEF

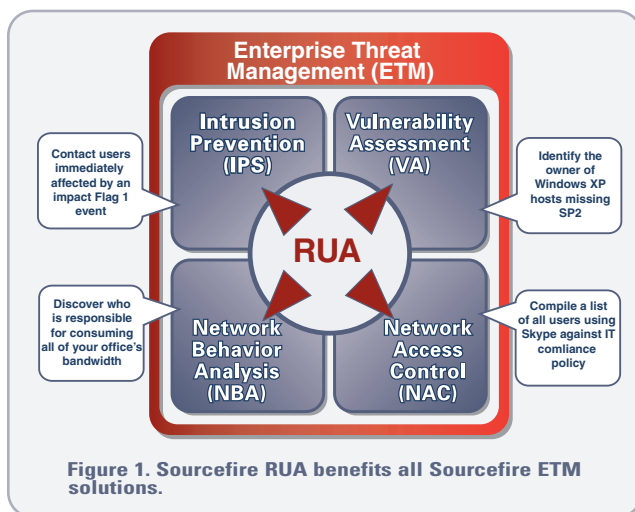
The Power of Sourcefire RUA™



Discover. Determine. Defend.

BRINGING REAL-TIME USER AWARENESS TO ENTERPRISE THREAT MANAGEMENT

For anyone who has used a network management or security incident/event management (SIEM) console, one problem is inevitably familiar. Having an IP address to identify the source and target machines responsible for activities occurring on the network is not nearly as useful as knowing the actual identities of the corresponding users. Sourcefire RUA™ (Real-time User Awareness) is a solution that addresses this situation by maintaining an accurate mapping between IP address and user identity, including not just the user's actual name, but other helpful details as well (e.g., contact information). As depicted in Figure 1, the real-time "user intelligence" supplied by Sourcefire RUA effectively enhances each of the primary components of Sourcefire's Enterprise Threat Management (ETM) solution – intrusion prevention (IPS), network behavior analysis (NBA), network access control (NAC), and vulnerability assessment (VA).



PENETRATING THE VEIL THAT OBSCURES USER IDENTITY

In today's enterprise computing environments, network and security operations personnel are bombarded by a steady and often overwhelming stream of events and alerts. But managing the sheer volume is not their only challenge. They must also contend with the fact that the vast majority of associated data at their disposal includes IP addresses as the only means for identifying the sources and targets of activities occurring in the network. This situation is clearly an issue for large organizations that have thousands of addresses, network nodes, and end

users. However, smaller organizations are not immune, especially given the pervasive use of technology that dynamically assigns addresses and the growing population of devices that frequently connect, disconnect, and reconnect to the network (e.g., laptops, PDAs, smartphones).

During the process of characterizing the nature and scope of a security or compliance event and subsequently taking corrective action, it is important to know more than just the IP addresses of the affected systems. To efficiently and effectively address a given event, network and security administrators will often need to know the identities of the actual users that are either causing or being impacted by it. Typically, though, that level of information is not readily available. To get it, administrators will often resort to consulting static (and therefore highly inaccurate) resources such as spreadsheets listing IP/user pairings, or they will spend precious time sifting through Active Directory or LDAP log files, manually linking usernames to host IP addresses.

The Sourcefire Approach to User Awareness

What organizations ultimately need is a product that automatically tracks user identity and makes the resulting information readily available in a manner that best meets the needs of network and security administrators, architects, and managers. Sourcefire RUA is such a product.

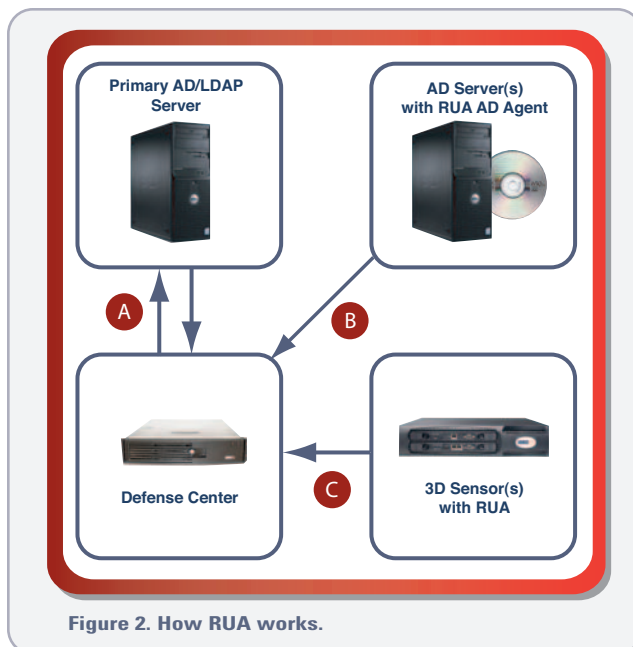
How RUA Works

The options for implementing RUA differ slightly based on the user directory technology an organization employs. But regardless of whether the organization uses Active Directory (AD) or LDAP, the first part of the solution is effectively the same. One of the organization's directory servers is designated as "primary" and is used as the source of information to generate a user database within a designated Sourcefire Defense Center appliance. User accounts are replicated to Defense Center via a synchronization process that occurs every 60 minutes. (See Step A in Figure 2.) The purpose of the user database is to establish and maintain a record of known usernames, along with additional pieces of helpful information, including the user's actual name, email address, phone number, and department.

For Active Directory shops, the second part of the solution entails running Sourcefire RUA Active Directory Agents on each of the organization's AD servers. These agents monitor users as they log into the network or when they are authenticated against the AD credential store for any other reason (e.g., to obtain access to a given service or

host). As a user logs on, the RUA Agent captures the username being submitted and the corresponding IP address that it is being submitted from and forwards this username-IP address pair to Defense Center for incorporation in the user database. (See Step B in Figure 2.)

Alternatively, administrators can run RUA software on Sourcefire 3D Sensors that are deployed in the network. This configuration enables the 3D Sensors to passively detect logon activity in the traffic they observe and to forward username-IP address pairs for incorporation in the Defense Center User Database. (See Step B in Figure 2.) This configuration is intended primarily for LDAP shops not running Active Directory or IT organizations that have an objection to running agents on their AD servers.



Regardless of which approach is used to pair usernames with corresponding host IP addresses, RUA provides powerful user tracking and identification capabilities that enable crucial network and security processes to be conducted more efficiently and effectively. With the user intelligence supplied by RUA:

- administrators can immediately identify actual users, enabling both rapid response to threats and tighter control of the computing environment;
- analysts and architects can make better decisions about changes to security policies, modifications to prioritization and resource allocation schemes, and potential upgrades to network infrastructure; and

- managers can know specifically who is consuming which IT resources to facilitate fair allocation of budgets and to expedite remediation of compliance violations.

With Sourcefire RUA, there is no need for any additional devices to be used beyond Sourcefire 3D Sensors and Defense Center appliances. Although many alternative solutions require IT to deploy one or more dedicated servers or appliances, RUA gets the job done by taking advantage of existing Sourcefire 3D Sensors that may already be running Sourcefire IPS™ and/or Sourcefire RNA™ (Real-time Network Awareness) applications, or through the use of RUA Agents installed on Active Directory servers.

IMPROVING ALL ASPECTS OF ENTERPRISE THREAT MANAGEMENT

The Power of ETM

Over the past few years, it has become glaringly apparent that a point-product approach to information security is incapable of keeping up with prevailing changes to the threat, technology, and regulatory landscapes. In response, Sourcefire has developed Enterprise Threat Management (ETM), an approach based on combining complementary threat and vulnerability management technologies, infusing and enhancing them with “shared intelligence”, and having them be controlled by a central management system.

The goal of ETM is to enable organizations to work smarter, not harder, when it comes to protecting their computing and information assets. One of the most significant keys to meeting this goal is the concept of shared intelligence. Shared intelligence means that each of the ETM technologies has some pieces of information pertaining either to the composition of the environment that is being protected (i.e., the what), or how that environment is being used: IPS has information on actual and possible threats; VA has information on actual and possible vulnerabilities; NAC has information on endpoints; and NBA has information on normal and abnormal network activities. And, although these pieces of information are clearly useful within the domain of each individual technology, very often they are also useful to one or more of the other domains.

For example, an IPS that has access to endpoint and vulnerability details can automatically deprioritize threats that are irrelevant due to the absence of systems that are actually susceptible to them. In this case, shared intelligence helps

eliminate ambiguity and dangerous assumptions, enabling a better real-time decision to be made. Similarly, available contextual information could be used to proactively or reactively configure NAC to disallow communications that are considered unproductive or risky.

The Power of ETM with User Intelligence

User awareness also plays a major role in an ETM solution. Identity data brings an entirely new set of intelligence into the picture, yielding insight into the who aspect of what is occurring on the network. This insight helps administrators, analysts, and managers to improve operational efficiency and enable better decisions to be made.

In the 3D System, identity data is automatically correlated with network intelligence and is available as an integral element of all types of event records, such as those pertaining to intrusions, traffic flows, and compliance violations generated with the Policy & Response subsystem. Identity data is also available within the host profiles gathered and maintained by Sourcefire RNA to characterize all of the endpoints on the network. Moreover, distinct benefits are derived for each of the primary technologies that comprise Sourcefire's ETM solution.

For IPS:

- Security administrators can rapidly identify specific users that are being targeted by an attack and notify them to take immediate action, such as disconnecting from the network, to minimize the impact.
- The source can be identified for internally initiated attacks, enabling the issue to quickly be resolved at the root and allowing administrative measures to be taken in the event of a malicious user.

For NBA:

- Identity data can reveal the specific consumers of IT resources (e.g., bandwidth) to support network planning and expense allocation.
- The parties responsible for propagating unknown threats can quickly be identified and quarantined.

For NAC:

- Lists indicating who is violating IT policies (e.g., banning the use of Skype) can be compiled and then distributed to the appropriate managers for further action.
- Identity can be used as a constraint in formulating and enforcing network usage rules (e.g., only users in the finance department may access the company's payroll application).

For VA:

- Specific users can be contacted directly and instructed on what to do when a passive or active scan reveals their computers are susceptible to one or more known vulnerabilities.
- Identity data can be used as factor for prioritizing remediation efforts.

WORK SMARTER WITH SOURCEFIRE RUA

With Sourcefire RUA, administrators no longer need to perform time-consuming, manual look-ups to establish the identity of the actual user that lies behind a given IP address. IT architects no longer need to guess at who is using which resources when planning infrastructure changes and upgrades. And managers no longer need to stare at cryptic strings of numbers when reviewing reports that illustrate security events or summarize network usage and specific types of activities. Whether an organization is using all or just select parts of the Sourcefire 3D System, the automated user intelligence capabilities of RUA will enable greater efficiency and effectiveness. IT and security personnel will be able to quickly resolve network events, more tightly control the computing environment, and, in general, make better decisions. In short, RUA enables them to work smarter, not harder.

For more information about the Sourcefire 3D System, including RUA, visit Sourcefire's web site at www.sourcefire.com or contact Sourcefire today.

About Sourcefire

Sourcefire, Inc., a world leader in intrusion prevention, is transforming the way organizations manage and minimize network security risks with its 3D Approach - Discover, Determine, Defend - to securing real networks in real-time. The company's ground-breaking network defense system unifies intrusion and vulnerability management technologies to provide customers with superior network security. Founded in 2001 by the creator of Snort®, Sourcefire is headquartered in Columbia, MD and has been consistently recognized for its innovation and industry leadership by customers, media, and industry analysts alike - with more than 18 awards and accolades since January 2005 alone. Recently, the company was positioned in the Leaders Quadrant of Gartner's "Magic Quadrant for Network Intrusion Prevention System Appliances" report and the Sourcefire 3D System was named "Best Security Solution," at the 2006 SC Magazine Awards. At work in leading Fortune 1000 and government agencies, the names Sourcefire and founder Martin Roesch have grown synonymous with innovation and intelligence in network security.

©2007 Sourcefire, Inc. Sourcefire 3D System, Sourcefire RNA, Intrusion Sensor, RNA Sensor, Defense Center, Sourcefire Success Pack, Sourcefire VRT and Snort are trademarks or registered trademarks of Sourcefire. All rights reserved.