



# What's New

## Sourcefire 3D™ System 4.7

Sourcefire is pleased to announce general availability of the Sourcefire 3D™ System 4.7 release, including availability of two new Sourcefire products—Sourcefire RUA™ and Sourcefire NetFlow Analysis. The purpose of this document is to describe the new and improved capabilities of Sourcefire 3D System 4.7.

This document is divided into the following sections:

Sourcefire 3D System Enhancements .....	1
Sourcefire RUA .....	7
Sourcefire NetFlow Analysis .....	8
For More Information .....	9

### Sourcefire 3D System™ Enhancements

#### **New!** Default IPS Policies

**Description:** Within the 3D System 4.7 release, Sourcefire provides three Default IPS Policies for users to choose from when seeking guidance on which Snort® rules to enable when initially configuring a Sourcefire IPS™. These default policies take three different security stances:

- **Security over Connectivity** - This policy is built for organizations where security of network infrastructure takes precedence over user convenience. This inline policy enables a far greater number of rules than those enabled in the Connectivity over Security policy.
- **Balanced Security and Connectivity** - This inline policy is built for both speed and detection. It serves as a good starting point for networks with average security requirements. Also, note that this policy is roughly equivalent to the Suggested Inline Rules policy in previous versions of the product.
- **Connectivity over Security** - This inline policy is built for organizations where connectivity (being able to get to all resources and applications) takes precedence over security of network infrastructure. Only the most critical rules that block traffic are enabled.

**Benefit:** This capability speeds the process of initially configuring a Sourcefire IPS while providing guidance on which Snort rules to enable based on the type of traffic that exists on the network and an organization’s overall stance on network security.

#### **New!** RNA-Recommended Rules

**Description:** Sourcefire is pioneering the Enterprise Threat Management (ETM) market with its visionary approach to intrusion prevention called “Adaptive IPS”. The core concept behind Adaptive IPS is using threat and endpoint intelligence to automatically configure and tune Sourcefire IPS software. Sourcefire’s Adaptive IPS approach begins with the Sourcefire RNA™ (Real-time Network Awareness), which enables Sourcefire Defense Center™ to



## What's New

### Sourcefire 3D™ System 4.7

correlate endpoint intelligence against internal and external threats, thus setting Impact Flag priorities and helping the IPS to make better blocking and alerting decisions. With version 4.7 of the 3D System, Sourcefire is taking its Adaptive IPS approach even further by automatically leveraging endpoint intelligence aggregated by Sourcefire RNA™, Nessus, Nmap and other endpoint intelligence solutions (see “Host Input API” feature description) to propose Snort IPS rules, called RNA-Recommended Rules, to be enabled and/or disabled based on the operating systems and services actually in use on the network. RNA-Recommended Rules can be generated on both an ad-hoc or scheduled basis. Customers can determine whether to “manually” or “automatically” enable/disable Snort rules recommended by RNA.

**Benefit:** RNA-Recommended Rules helps take the guess work out of selecting Snort rules that are most applicable to your network environment. By combining threat and endpoint intelligence as part of an Adaptive IPS strategy, 3D System implementations can be highly optimized to provide the best IPS protection possible, while maximizing security and performance of Sourcefire IPS appliances, minimizing false positives and negatives, and ultimately reducing costs.

#### **New! Nmap Integration**

**Description:** Sourcefire is partnering with Insecure.Org to integrate the Nmap active scanning tool as a standard component of the Sourcefire 3D System. Specifically, Sourcefire has integrated Nmap into Sourcefire Defense Center similar to how Nessus has been integrated prior to the 4.7 release. Nmap scans can be initiated ad hoc or through period scheduling using the Defense Center interface. Endpoint intelligence collected by Nmap is fed into existing host profiles initially created by RNA.

**Benefit:** Nmap can benefit Sourcefire 3D System customers in the following ways:

- Nmap can narrow down the list of potential Windows operating systems for a given Windows host, thus honing the list of potential host vulnerabilities and ultimately reducing the quantity of associated Impact Flag 1 events
- Nmap provides deeper endpoint intelligence to assist the 3D System with assessing host policy compliance
- Surgical Nmap scans can be triggered when a new host is detected by RNA on the network and/or when a host is involved in a security or compliance event

#### **New! Host Input API**

**Description:** Sourcefire’s new Host Input API will enable customers to leverage third-party active scanning and vulnerability assessment tools to populate the RNA Host Database with endpoint intelligence. This API can also leverage the “User Defined Host Attributes” section of a host profiles so that endpoint data can be logically placed into custom fields. Host data can also be inserted into the RNA Host Database in bulk through a .CSV import tool, or manually edited on an ad hoc basis.



## What's New

### Sourcefire 3D™ System 4.7

**Benefit:** There are three main benefits of leveraging external endpoint intelligence into the 3D System by using the Host Input API:

- The quantity of actionable Impact Flag 1 events can be reduced by narrowing the list of “potential” and or “actual” vulnerabilities associated with a given host
- Assessing host compliance is improved by providing endpoint intelligence about hosts that RNA has not yet discovered and by providing endpoint intelligence that RNA is unable to detect or has not yet provided
- Custom host attributes within RNA Host Profiles can be populated from third-party systems enabling Sourcefire administrators to identify the port on a switch for a given host, the physical location of a given host, and the IT resource responsible for a given host, just to name a few examples

#### **New! “Set Attribute” Remediation Module**

**Description:** Sourcefire now offers a “Set Attribute” Remediation Module that leverages the new Host Input API. In the event a Policy & Response (P&R) rule is triggered, users can configure RNA to automatically populate a custom field in the RNA Host Database. For example, a user may wish to query new hosts that have been detected on the network (e.g., “New Host = Yes”) or those hosts in violation of a Skype ban policy (e.g., “Skype = Yes”).

**Benefit:** When the Set Attribute Remediation Module is used in conjunction with the Host Input API, users can query the RNA Host Database to discover incremental new hosts added to the network, identify hosts that are in non-compliance of a specific P&R rule, and a myriad of other uses. Users can now evaluate new hosts and resolve compliance violations more quickly and easily than ever before.

#### **Improved! Master Defense Center (MDC) Global Policy Management**

**Description:** Earlier this year, Sourcefire introduced Master Defense Center technology enabling up to ten subordinate Defense Center (DC) appliances to forward intrusion, compliance and health events to an MDC appliance. With version 4.7 of the 3D System, Sourcefire is extending its MDC capabilities to provide for global policy management, enabling Sourcefire administrators to “push” IPS, RNA, system and health policies down to subordinate DCs and/or sensors from one centralized MDC console. Furthermore, an MDC environment can now support high availability (HA) pairs of subordinate DC appliances.

**Benefit:** This is the next logical step in Sourcefire’s quest to provide best-in-class enterprise scalability. Now enterprises of all shapes and sizes can reduce operating costs and achieve economies of scale when multiple DC appliances are spread throughout the organization.

#### **New! IPS Support for IPv6**

**Description:** Sourcefire’s IPS can now detect IPv6 exploits, whether potential exploits exist in native IPv6 traffic or within IPv6 traffic tunneled within IPv4 packets.



## What's New

### Sourcefire 3D™ System 4.7

**Benefit:** This capability enables Sourcefire customers to protect both IPv4 and IPv6 network assets against both internal and external threats.

#### **New! Setup Wizard**

**Description:** A Setup Wizard is now presented during the setup process of Sourcefire Defense Center and Sourcefire 3D Sensor appliances. The Setup Wizard guides users through the process of defining their networks, selecting initial detection policies and configuring detection engines and interface sets.

**Benefit:** Prior to the Setup Wizard, users were required to jump to multiple screens in various parts of the user interface to configure settings. More pre-existing Sourcefire expertise was required before placing a 3D Sensor or Defense Center appliance into production. But now, configuring Sourcefire appliances is easier than ever. Using the Setup Wizard, the time spent configuring base settings on a Sourcefire appliance is significantly reduced, and considerably less prerequisite knowledge in configuring Sourcefire software is required.

#### **New! Latency Thresholding**

**Description:** Sourcefire customers can use packet latency thresholding and rule latency thresholding to balance security with the need to maintain sensor latency at an acceptable level by enabling either or both of the following latency thresholding features:

- **Packet latency thresholding** measures the total elapsed time taken to process a packet by applicable decoders, preprocessors, and rules, and ceases inspection of the packet if the processing time exceeds a configurable threshold.
- **Rule latency thresholding** measures the elapsed time each rule takes to process an individual packet, suspends a rule for a specified time if the processing time exceeds the rule latency threshold a configurable consecutive number of times, and restores the rule when the suspension expires.

**Benefit:** This optional setting prevents custom and third-party Snort rules from unduly impacting the latency (in inline IPS mode) and detection performance of 3D sensors.

#### **New! Custom Service Detection**

**Description:** Sourcefire RNA can detect dozens of pre-defined services, such as FTP, HTTP, POP3, Telnet and more. With version 4.7, customers can now create their own custom service detection profiles, enabling users to customize RNA to monitor usage of virtually any service deployed within a corporate network.

**Benefit:** Sourcefire RNA can now detect custom network services. Customers can define any service they wish—whether related to “home grown” applications or commercial applications—to further the cause of network policy compliance.



## What's New

Sourcefire 3D™ System 4.7



### Improved! Policy Compliance Status Identification & Reporting

**Description:** In version 4.6 of the 3D System, Sourcefire introduced its “One-Click Compliance” capability, enabling customers to quickly configure network compliance “white lists” based on collected endpoint intelligence. In version 4.7, Sourcefire is extending its compliance capabilities even further, by providing:

- The ability to “reset” a host’s compliance state by deleting only those host attributes that triggered non-compliance status. The host will then be able to return to a compliant state and generate alerts upon subsequent changes.
- A graph of user compliance events over time, allowing users to track and demonstrate progress towards compliance goals.
- Pie charts showing the percent of hosts in compliance for a specific white list or collectively across all white lists within a given 3D System environment.
- The ability to view a list of specific non-compliant attributes for a given host.

**Benefit:** Sourcefire’s extensive compliance capabilities enable customers to quickly and easily deploy network usage policies, helping organizations to achieve government and industry compliance. By extending Sourcefire’s compliance capabilities, customers are able to more easily configure policies and demonstrate enterprise-wide policy compliance.

### New! RNA Support for 3D3800 & 3D5800 Sensors

**Description:** The 3D3800 and 3D5800 models of Sourcefire’s 3D Sensors now support Sourcefire RNA in addition to Sourcefire IPS software.

**Benefit:** Sourcefire customers with high-bandwidth intrusion prevention requirements no longer need to purchase separate appliances to use RNA on the same protected network segment(s).

### New! Flow Summarization

**Description:** Processing RNA flow data can consume significant Defense Center processing resources and disk space. Now, with RNA’s Flow Summarization capability, multiple flow records can be summarized at the 3D Sensor into a single export for more efficient transport to a Defense Center appliance. This option is selectable by the user. When enabled, flow summaries are created every five minutes. As flow summaries arrive at the Defense Center in summarized form, fewer DC processing resources are required and users are now able to store a longer flow data history on the DC’s hard disk. The amount of compression will vary depending on the nature of the flows on a given network, but may result in compression of 50-80% or more.

**Benefit:** This new capability will significantly reduce Defense Center processing and storage requirements for storing flow data. It will also cut down on bandwidth consumed between a Defense Center and its corresponding 3D Sensors.



## What's New

Sourcefire 3D™ System 4.7

### Improved! Performance & Usability Improvements

**Description:** The following is a list of usability enhancements related to the Sourcefire 3D System 4.7 release:

- **Exclusion of IP-Port Pairs from RNA Detection Policies.** RNA previously allowed users to exclude one or more IP addresses from the range of IP addresses it passively monitors in its RNA Detection Policy. Version 4.7 is extending this capability by not only allowing users to exclude one or more IP addresses, but also specific ports running on those IP addresses.
- **Support for Internet Explorer 7.0.** Sourcefire now supports the most recent version of Microsoft's Internet Explorer browser.
- **Elimination of Dual Red Impact Flags.** Prior to version 4.7, two different red Impact Flags were presented to users in the dashboard and event summary views due to different underlying methodologies for calculating impact values. Now, these have been consolidated into a single red Impact Flag grouping.
- **Separate Indication of Blocked Events.** Prior to version 4.7, the Impact Flag in inline IPS mode was used to display whether an event had been blocked. Now the blocking status of events is shown separately, allowing administrators to see what impact level an event would have had if it had not been blocked.
- **SIDs in Vulnerability Database Table View.** When reviewing lists of vulnerabilities within the Sourcefire Vulnerability Database, users can now see which SIDs (Snort IDs / rules) are associated with each listed vulnerability.
- **Right-Click Actions from Event View.** Sourcefire is making it easier to navigate to and from frequently used screens within Sourcefire user interfaces by allowing users to deactivate, block, suppress and threshold rules at any level in the event view through a right-click menu.
- **Edit User Configuration File Within GUI.** Some 3D System customers take advantage of functionality only available in the user.conf file on each 3D Sensor. Now this file can be edited from within the Defense Center GUI, rather than from a text editor used locally on each sensor.
- **Prohibit Packet Feature Enabled Within GUI.** Prior to version 4.7, if a user wished to suppress packet data from being sent along with intrusion events to a Defense Center appliance, that setting was required to be enabled in user.conf. Now, with version 4.7, that setting can be enabled as an option in the GUI.
- **Sensor Monitoring Exclusion.** Users can temporarily silence 3D Sensor health monitoring alerts for one or more sensors from the Defense Center console. This is helpful in the event it is necessary to take a 3D Sensor off line for maintenance.
- **Improved Network Map.** Sourcefire RNA users will enjoy a much more responsive rendering of the Network Map when a particular segment of the Network Map is expanded. Also, users can now organize the Network Map and its hierarchy in a way that reflects their actual network construction. Users can group any assortment of networks and subnets into a customizable group.
- **Persistent Manual Host Attributes.** Users can now manually edit operating system and service attributes for a given host within the RNA Host Database. These manually configured attributes will remain persistent and will not be over-written.



## What's New

### Sourcefire 3D™ System 4.7

- **Links to Rule Documentation.** When intrusion events are triggered by Snort rules, it is not always easy to understand the purpose of a given Snort rule and what exploits that rule is designed to protect against. Now, links to Snort rule documentation are available wherever events are referenced.
- **SEU Import History.** When importing a new SEU (Security Enhancement Update), users can now see which Snort rules are new and updated and which rules are being deleted. Equivalent information related to prior-installed SEUs is also maintained.
- **Port Lists.** Prior to 3D System 4.7, Snort rules could be configured to trigger based on an individual port or a range of ports. Now with version 4.7, a list of ports and/or port ranges can be configured within any given Snort rule.
- **Delete Local Rules.** Users now have the ability to delete custom and imported Snort rules. Unneeded rules no longer cause “clutter”.

**Benefit:** These enhancements improve the overall performance and usability of the entire Sourcefire 3D System, saving customers both time, effort and money when installing, configuring and using Sourcefire Enterprise Threat Management (ETM) solutions.

## Sourcefire RUA™

### **New!** User Identity Tracking

**Description:** Sourcefire RUA (Real-time User Awareness) is the newest addition to the Sourcefire 3D System and benefits all four Sourcefire Enterprise Threat Management (ETM) solutions, including IPS, NBA, NAC and VA. Sourcefire RUA streamlines the process of associating a host IP address related to security and policy events with Active Directory / LDAP usernames. Other user attributes, including first name, last name, department, phone number and email address, are obtained through a direct connection to a Primary Active Directory or LDAP Server, and are updated every 60 minutes.

Sourcefire RUA can tell you the “who” behind the “what”. In other words, RUA can tell you:

- **Who** owns the host targeted by a given Impact Flag 1 event
- **Who** just initiated an internal attack
- **Who** just launched an internal port scan
- **Who** just attempted to access the payroll server
- **Who** is consuming the most bandwidth in our office
- **Who** is missing Service Pack 2 for Windows XP
- **Who** is using Skype in violation of company IT policy

**Benefit:** Prior to RUA, customers either didn't associate usernames with events, or they were forced to manually review Active Directory / LDAP log files, or they attempted to correlate user and security intelligence using a SIEM. By implementing RUA, the process of resolving a username to a host IP address associated with security and compliance events is completely streamlined, enabling customers to respond to events more quickly than ever before.



## What's New

Sourcefire 3D™ System 4.7



### **New!** RUA Active Directory Agent

**Description:** For Active Directory customers, Sourcefire provides software to be installed directly on Active Directory servers, called RUA Active Directory Agents. These agents detect each time a user logs onto Active Directory and couples each username with its associated host IP address. By using RUA Active Directory Agents, RUA software running on Sourcefire 3D Sensors is not required.

**Benefit:** This capability leverages customers' existing investments in Active Directory technology to provide user identity information to the Sourcefire 3D System. This additional information can help security analysts to resolve security and compliance events more quickly and easily—when time is of the essence.

### **New!** LDAP Integration

**Description:** Sourcefire 3D Sensors with RUA software can passively detect LDAP usernames (using Kerberos authentication) and pair them with associated host IP addresses. Advanced user attributes, including first name, last name, department, phone number and email address, are obtained directly from a primary LDAP server and are updated every 60 minutes.

**Benefit:** This capability allows the customer to leverage its existing LDAP environment, enabling RUA to be used in non-Active Directory environments.

## Sourcefire NetFlow Analysis

### **New!** NetFlow Integration

**Description:** NetFlow enables administrators to gain insight into network traffic patterns deep within a corporate network—communicating with NetFlow-enabled Cisco routers and switches. Sourcefire now aggregates NetFlow (v5) flow data, providing detailed and statistical flow visibility throughout customer networks.

**Benefit:** This capability strengthens Sourcefire's position as a leading Network Behavior Analysis (NBA) provider and enables Sourcefire customers to extend Sourcefire's NBA solution to areas of the network where Sourcefire RNA Sensors don't yet exist. Sourcefire's NBA capabilities benefit both security analysts and network administrators alike.

### **New!** NetFlow-based Anomaly Detection

**Description:** Sourcefire RNA customers can utilize Sourcefire's proprietary RNA Flow to establish "normal" traffic baselines and detect anomalies (i.e., worm propagation) from those baselines. Now, with Sourcefire's new NetFlow Integration capability, NetFlow can be used as a secondary source for establishing network baselines.



## What's New

### Sourcefire 3D™ System 4.7



**Benefit:** Now Sourcefire customers can establish traffic baselines and detect anomalies from all corners of the network, whether covered by RNA Sensors or NetFlow-enabled routers and switches.

#### **New! NetFlow-based Host Access Compliance**

**Description:** Sourcefire RNA customers can create and enforce host access compliance policies to prevent unauthorized hosts from accessing strategic and/or sensitive company resources. Now, unauthorized host access attempts can be detected by analyzing NetFlow in addition to RNA flow data.

**Benefit:** Now Sourcefire customers can monitor and enforce host access compliance policies across the organization, even to corners of the network where RNA Sensors don't yet exist due to budgetary and/or logistical reasons.

#### **For More Information**

The following materials are available now on the Sourcefire Customer Support web site. They provide additional information about what's new in the Sourcefire 3D System 4.7 release, including Sourcefire RUA and Sourcefire NetFlow Analysis:

- Sourcefire 3D System 4.7 FAQ
- What's New in Sourcefire 3D System 4.7 Webinar
- Sourcefire 3D System 4.7 User Guide
- Sourcefire 3D System 4.7 Installation Guide

To learn more about the Sourcefire 3D System 4.7 release, or to get answers to related technical questions, please select from the following options:

- Visit the Sourcefire Support Site at <https://support.sourcefire.com>
- Email Sourcefire Support at [support@sourcefire.com](mailto:support@sourcefire.com).
- Call Sourcefire Support at 1-800-917-4134 or +1-410-423-1901

For information on Sourcefire's training and certification programs, please select from the following options:

- Visit the Sourcefire Education Site at <http://www.sourcefire.com/services/education>
- E-mail Sourcefire Education Services at [training@sourcefire.com](mailto:training@sourcefire.com)
- Call Sourcefire Education Services at 1-866-505-9113 or +1-734-743-6550

Copyright © 2007, Sourcefire, Inc. All rights reserved. Sourcefire®, Snort®, Sourcefire 3D™, Sourcefire IPS™, Sourcefire RNA™, Sourcefire RUA™, and Sourcefire Defense Center™ are trademarks or registered trademarks of Sourcefire, Inc. in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.