Sourcefire IPS™ (Intrusion Prevention System)

Best-in-Class Intrusion Detection and Prevention

Today's networks are highly dynamic. Threats are constantly evolving and becoming more sophisticated. Network security breaches continue to occur because static defenses can't protect today's dynamic networks against dynamic threats. Learn why more organizations depend on Snort® than any other intrusion prevention technology worldwide, and why thousands of enterprises rely on Sourcefire's IPS and real-time adaptive security solution to protect their networks.

SOURCEFIRE IPS—THE FOUNDATION OF THE SOURCEFIRE 3D® SYSTEM

Snort—the De Facto Standard for Intrusion Prevention

Built on Snort, the de facto standard for intrusion detection and prevention (IDS/IPS), Sourcefire IPS™ (Intrusion Prevention System) is the foundation of the award-winning Sourcefire 3D® System. Sourcefire IPS uses a powerful combination of vulnerability- and anomaly-based inspection methods—at line speeds up to 10Gbps—to analyze network traffic and prevent threats from damaging your network. Whether deployed at the perimeter, in the DMZ, in the core, or at critical network segments, Sourcefire's easy-to-use IPS appliances provide comprehensive threat protection.

Sourcefire IPS contains multiple default policies for out-of-the box blocking, drawing from a comprehensive library of open Snort rules. Open rules allow customers to verify that rules address the vulnerabilities for which coverage is claimed and to create new rules or modify existing ones to protect custom applications and systems. Sourcefire's IPS can be deployed in inline blocking and/or passive alerting modes, and can remediate attacks using external devices, such as firewalls, routers, patch management systems, and more.

Snort, created by Sourcefire, has nearly 4 million downloads and approximately 300,000 registered users. More organizations rely on Snort than any other intrusion prevention technology worldwide. Over the past decade, the Snort community has grown to become an entire ecosystem, from user groups, to books, to classes taught at hundreds of colleges and universities. More IT security professionals are familiar with Snort than any other IPS technology in the market. Sourcefire customers benefit from this extensive Snort ecosystem on day one.

Protection Against Known and Unknown Threats

The Sourcefire Vulnerability Research Team™ (VRT) works around the clock to ensure that Sourcefire commercial customers and open source Snort users are protected against both known and unknown threats. The VRT leads the IPS industry in addressing Microsoft Tuesday vulnerabilities on the same day they are announced.

It's often the unknown threat that can be the most damaging. That's why Sourcefire publishes vulnerability-based Snort rules. Unlike an IPS that relies primarily on exploit-based signatures, Snort rules offer protection against any possible exploitation of a vulnerability. This was illustrated when Sourcefire protected its 3D customers and open source Snort users more than two years in advance of the Conficker worm.

Key Sourcefire IPS Capabilities

- Snort IPS detection engine
- Snort ruleset offers protection from constantly evolving vulnerabilities
- Open rules language—view, edit, and create Snort rules
- Operates on physical and virtual Sourcefire 3D Sensors
- Reports, alerts, and dashboards
- Multiple default IPS policies
- Packet-level forensics
- Sophisticated, customizable workflows

Snort—the De Facto IPS Standard

- Invented in 1998 by Martin Roesch, Sourcefire Founder and CTO
- Most widely-deployed IPS technology worldwide
- Used by 80% of Fortune 100
- Used by the 30 largest U.S. government agencies
- Used by 42% of Global 500
- Snort community has become an entire ecosystem:
  - » Approximately 300,000 registered users
  - » Dozens of Snort books published
  - » Classes taught at colleges and universities
  - » User groups
  - » Discussion lists and forums

SOURCEfire®

Sourcefire's IPS appliances provide comprehensive threat protection against:

- Worms
- Trojans
- Backdoor attacks
- Spyware
- Port scans
- VoIP attacks
- IPv6 attacks

- DoS attacks
- Buffer overflows
- P2P attacks
- Statistical anomalies
- Protocol anomalies
- Application anomalies
- Malformed traffic

- Invalid headers
- Blended threats
- Rate-based attacks
- Zero-day threats
- TCP segmentation and IP fragmentation

Protection for Physical and Virtual Environments

Purpose-built, ICSA-certified Sourcefire 3D® Sensors are available with throughputs from 5Mbps up to 10Gbps. By clustering two 10Gbps 3D9900 Sensors, the 3D System can support throughput up to 20Gbps. 3D Sensors are available with fault-tolerant features, such as fail-open copper and fiber ports, dual power supplies, and RAID drives.

MODEL	3D500	3D1000	3D2000
Supported Line Speed (IDS/IPS)	5Mbps	45Mbps	100Mbps

MODEL	3D2100	3D2500	3D3500
Supported Line Speed (IDS/IPS)	250Mbps	500Mbps	1Gbps

MODEL	3D4500	3D6500	3D9900
Supported Line Speed (IDS/IPS)	2Gbps	4Gbps	up to 10Gbps*

*Clustering two 3D9900 Sensors provides throughput up to 20Gbps.

Table 1. Sourcefire 3D Sensor Product Family

The Sourcefire Virtual 3D Sensor™ extends the 3D System to far corners of the network where IT security resources don't exist or the deployment of physical 3D Sensors is impractical. Virtual 3D Sensors also provide the capability to inspect VM-to-VM communications, providing the same protection as their physical sensor counterparts. The Virtual 3D Sensor offers support for inspection of network traffic at speeds up to 500Mbps.

Centralized Event Aggregation and Analysis

Using the feature-rich, yet easy-to-use, Sourcefire Defense Center® (DC) or Sourcefire Virtual Defense Center™ management console, customers can analyze events, configure and push IPS policies, automatically download and apply Snort rule updates, and more. Powered by the Snort detection engine, Sourcefire IPS excels with detailed packet-level forensics and sophisticated, customizable workflows for investigating security events as they occur. For larger deployments, customers can leverage Sourcefire's Master Defense Center (MDC) technology to manage multiple DCs and hundreds of physical and/or virtual 3D Sensors across their entire organization.
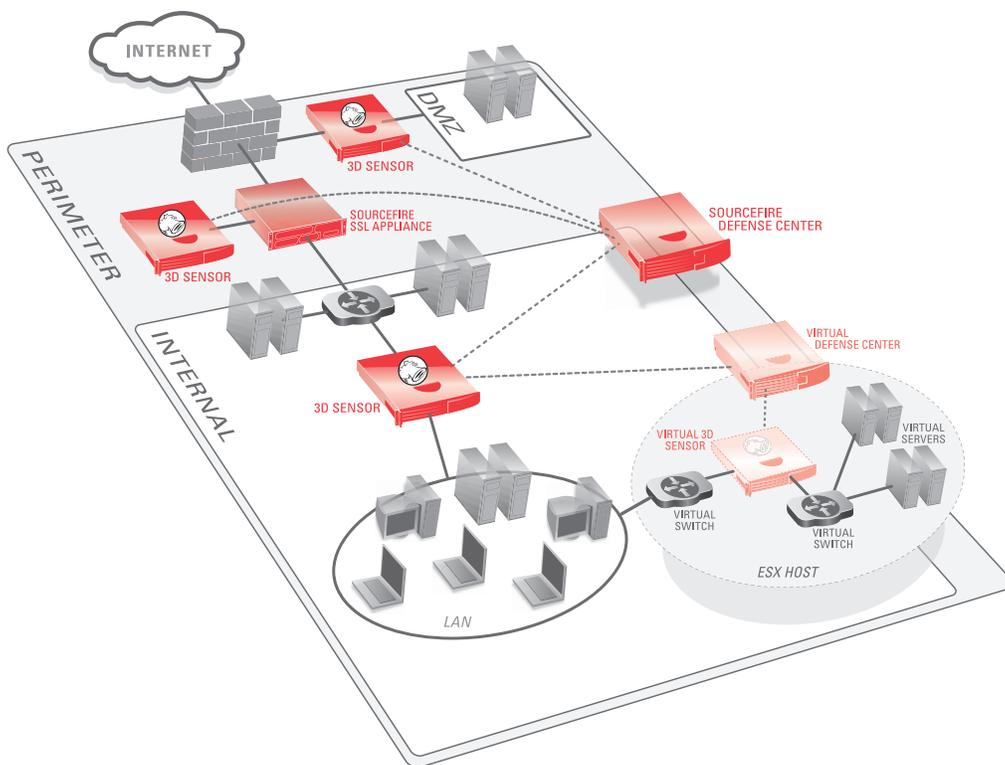
Figure 1. Sourcefire supports a Defense-in-Depth intrusion prevention strategy by allowing physical or virtual Sourcefire 3D Sensors to be positioned in all areas of the network. Sourcefire Defense Center orchestrates all event aggregation, analysis, and IPS policy management.

Reports, Alerts, and Dashboards

Defense Center provides customers with numerous reports, alerts, and dashboards. Customers can leverage a variety of pre-defined report templates or create custom reports to meet the needs of any organization. They can receive alerts in the form of syslog entries, email messages, or SNMP alerts. Customers can also create fully customized dashboards with dozens of drag-and-drop "widgets" that display critical information in the form of tables and graphs.

SOURCEFIRE'S REAL-TIME ADAPTIVE SECURITY SOLUTION

Real-Time Network Intelligence

Sourcefire RNA® (Real-time Network Awareness) provides 24x7, passive network intelligence, storing a real-time inventory of operating systems, services, applications, protocols, and potential vulnerabilities that exist on the network. RNA collects this intelligence in a completely passive manner, while seamlessly integrating the intelligence with the 3D System. RNA's host database can also be augmented with information gathered by active discovery tools to further expand the store of network intelligence. Combine RNA's real-time network visibility with Sourcefire RUA® (Real-time User Awareness), a technology that links user identity to security and compliance events, and organizations have enterprise-wide intelligence on their dynamic networks and users.

Sourcefire Defense Center Key Capabilities

- Centralized event monitoring
- Manages physical and virtual Sourcefire 3D Sensors
- Customizable dashboards with numerous widgets
- Syslog, email, and SNMP alerts
- Sophisticated and customizable reporting
- Third-party integration APIs
- LDAP and RADIUS support
- Automated VRT rules updates
- Master Defense Center (MDC) scalability

Real-time Adaptive Security Solution Key Benefits

- Know what's on your network in real time
- Save time by significantly reducing quantity of actionable security events
- Reduce risk by ensuring IPS is optimized to protect your dynamically changing network
- Enables organizations with small network security staffs to effectively protect their networks

SOURCEfire®

Automated Impact Assessment

IT security professionals don't have time to sift through hundreds or thousands of security events each day to try to figure out which events matter most. By leveraging Sourcefire RNA's real-time network intelligence, customers can take their Sourcefire IPS to the next level. Threat intelligence is automatically correlated against RNA's real-time target host intelligence to determine the relevance and impact of an attack. With automated impact assessment, events are typically reduced by up to 99%, allowing administrators to focus on the events that can actually affect their networks.

Automated IPS Tuning

IT security professionals don't have time to constantly "tune" their IPSes as their networks change. By incorporating RNA's real-time network intelligence into the Sourcefire IPS, the ongoing process of IPS tuning can also be automated. As your network evolves, RNA-Recommended Rules takes the guesswork out of determining which Snort rules to enable and disable. RNA recommends relevant Snort rules based on the network it's protecting, and Snort rules can be enabled with or without human intervention.

The use of Sourcefire's real-time adaptive security solution results in less manual event investigation and IPS tuning by your IT security staff, lower potential for network downtime, and lower cost of operations. By having real-time knowledge of what's running on your network, the 3D System saves you time and effort and maximizes protection of your ever-changing network.

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK

Sourcefire is the only IPS provider offering dynamic defenses against the threats aimed at your constantly changing network. Sourcefire's key capabilities include:

- Superior attack protection:
  » Snort IPS detection engine
  » Vulnerability-based Snort rules
  » Open rules language—view, edit, and create Snort rules
  » Multiple default IPS policies
  » ICSA Labs certified and NSS Labs tested
- Most contextual information about threats:
  » 24x7, passive network intelligence
  » User identity tracking
- Only network security provider to offer a real-time adaptive security solution:
  » Real-time, automated intrusion event impact assessment
  » Automated IPS tuning based on actual network assets
- Integrated system managed from a single, easy-to-use management console
  » "Manager of managers" enterprise-class scalability through MDC technology
- Excellent forensics and event analysis:
  » Powerful event viewing system
  » Full packet logging

To learn more about Sourcefire's award-winning IPS solutions, visit us at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Global Security Alliance today.