Sourcefire 3D System IPv6 Capabilities

SOURCEfire®

Forward Looking Statements

This presentation contains forward-looking statements. These statements relate to future events or to future financial performance and involve known and unknown risks, uncertainties, and other factors that may cause our actual results, levels of activity, performance, or achievements to be materially different from any future results, levels of activity, performance, or achievements expressed or implied by these forward-looking statements. In some cases, you can identify forward-looking statements by the use of words such as “may,” “could,” “expect,” “intend,” “plan,” “seek,” “anticipate,” “believe,” “estimate,” “predict,” “potential,” or “continue” or the negative of these terms or other comparable terminology. You should not place undue reliance on forward-looking statements because they involve known and unknown risks, uncertainties and other factors that are, in some cases, beyond our control and that could materially affect actual results, levels of activity, performance, or achievements.

Other factors that could materially affect actual results, levels of activity, performance or achievements can be found in Sourcefire’s Form 10-Q for the quarter ended March 31, 2010, filed with the Securities and Exchange Commission on May 6, 2010. If any of these risks or uncertainties materialize, or if our underlying assumptions prove to be incorrect, actual results may vary significantly from what we projected. Any forward-looking statement you see or hear during this presentation reflects our current views with respect to future events and is subject to these and other risks, uncertainties, and assumptions relating to our operations, results of operations, growth strategy, and liquidity. We assume no obligation to publicly update or revise these forward-looking statements for any reason, whether as a result of new information, future events, or otherwise.

About Sourcefire

- Sourcefire was founded in January 2001 by Martin Roesch, author of open source Snort®, the world's most downloaded intrusion detection and prevention technology with nearly 4 million downloads to date.
- In response to increased demand for a commercial version of the popular software, the company developed the Sourcefire 3D® System—a systematic network defense system built on Snort and designed to adapt to dynamic networks and threats in real time.
- Leader, Gartner IPS Magic Quadrant, for four consecutive years
- The Sourcefire Web Site: www.sourcefire.com

About Snort

- Snort® is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire.
- Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and approximately 300,000 registered users, Snort has become the de facto standard for IPS.
- The Snort Web Site: www.snort.org
- The Snort Blog: http://blog.snort.org/

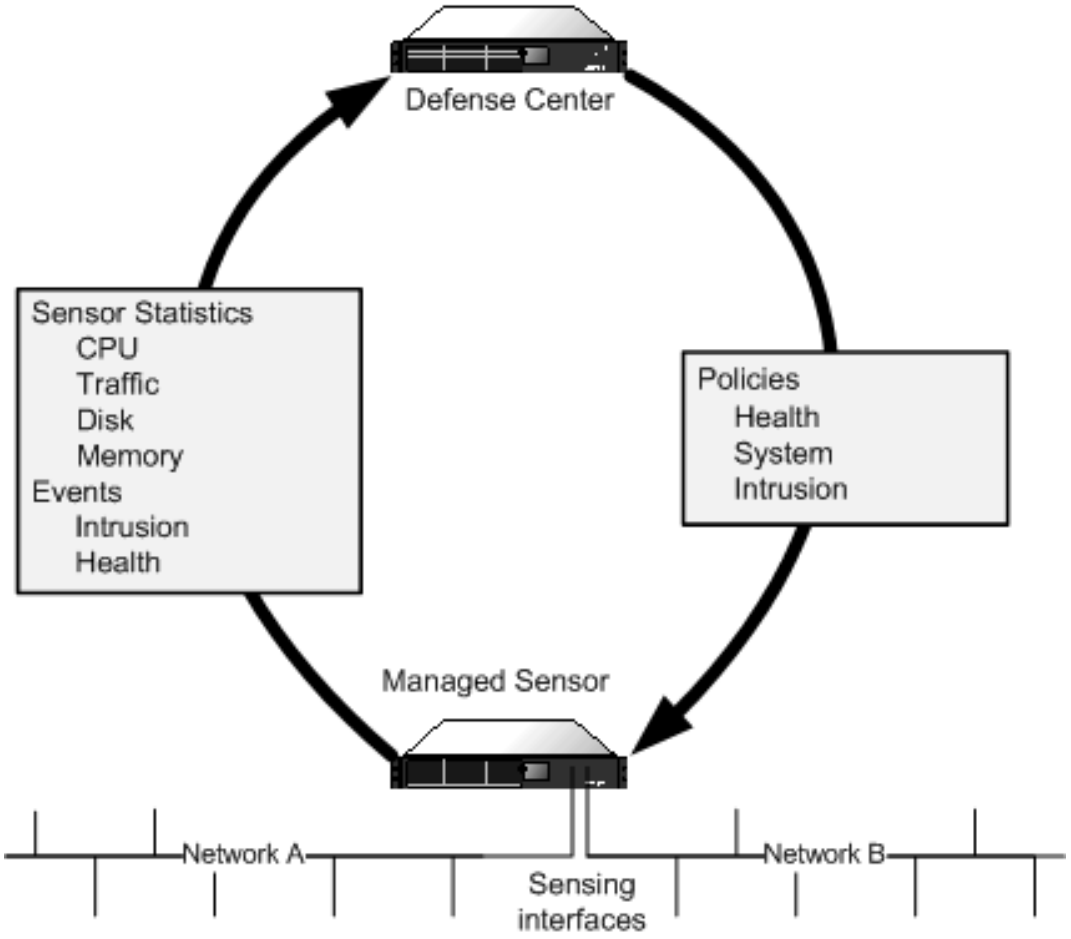
About the Sourcefire VRT

- The **Sourcefire Vulnerability Research Team (VRT)** is a group of leading-edge network security experts working around the clock to proactively discover, assess, and respond to the latest trends in hacking activities, intrusion attempts, malware and vulnerabilities. Some of the most renowned security professionals in the industry are members of the Sourcefire VRT. This team is supported by the vast resources of the open source Snort and ClamAV communities, making it the largest group dedicated to advances in the network security industry.
- The VRT develops and maintains the official rule set of Snort.org. Each rule is developed and tested using the same rigorous standards VRT uses for Sourcefire customers. The VRT also maintains shared object rules that are distributed for many platforms in binary format.
- The VRT blog: http://vrt-blog.snort.org/
- The VRT advisory RSS feed: http://www.snort.org/vrt/advisories.xml/

About the Sourcefire 3D System

- 3D Sensors:
  - 3D500
  - 3D1000
  - 3D2000
  - 3D2100
  - 3D2500
  - 3D3500
  - 3D4500
  - 3D6500
  - 3D9800
  - 3D9900
  - Sourcefire Virtual Sensor
- Defense Centers:
  - DC500
  - DC1000
  - DC3000
  - Sourcefire Virtual Defense Center
- Master Defense Center: MDC3000
- ICSA Labs Network IPS Certification (requires 100% detection of tested threats)
- NSS Labs, Inc. highest rating of “Recommend”, two consecutive years

Sourcefire 3D System



Sourcefire Product Support for IPv6

- Sourcefire 3D System currently meets the requirements in the IPv6 protection profile for hosts and for IDS/IPS network protection devices
- Sourcefire 3D System in USGv6 testing at ICSA:
  - Host testing successfully completed, waiting for report to create Supplier Declaration of Conformance
  - NPD testing in process, expect to be able to create declaration of conformance in 2011

Support for Basic IPv6 Network Protection Device Requirements

- Allows dual-stack, IPv4 only, and IPv6 only
- Provides a full UI for configuration of protection functionality, logging and alerting, and administrative functions
- Provides an administrator role, as well as a variety of other user roles, to control access to all functionality
- Retains device settings if appliance loses and regains power
- Meets all auditing and logging requirements for an IDS/IPS

Support for IPv6 connectivity

- IPv6 connections between management console and sensor
- IPv6 connections to auxiliary servers such as LDAP, email, syslog, SNMP, SSHFS (backup), and NTP (time server)
- Access control for connections from IPv6 addresses
- HTTP, peer, and SSH IPv6 client connections
- IPv6 connection to proprietary Sourcefire 3D System clients such as our host input and eStreamer clients

Assignment and Resolution of IPv6 addresses

- Resolution of IPv6 addresses via DNS
- Support for automatic assignment via DHCPv6 server or via IPv6 network router
- Manual assignment of IPv6 addresses also supported

IPv6 Operating System Support

- All Sourcefire 3D System appliances use the same operating system and IP stack
- The IP stack complies with the mandatory IPv6 host requirements in the USGv6 protection profile

IPv6 Sensing: Performance Under Load

- Health Monitoring facility provides alerts on process health, event rates, and traffic status
- Rule keywords that require established TCP sessions and rate-based detection options prevent SYN floods and other connection-intensive attacks

IPv6 Sensing: Fragmentation Handling

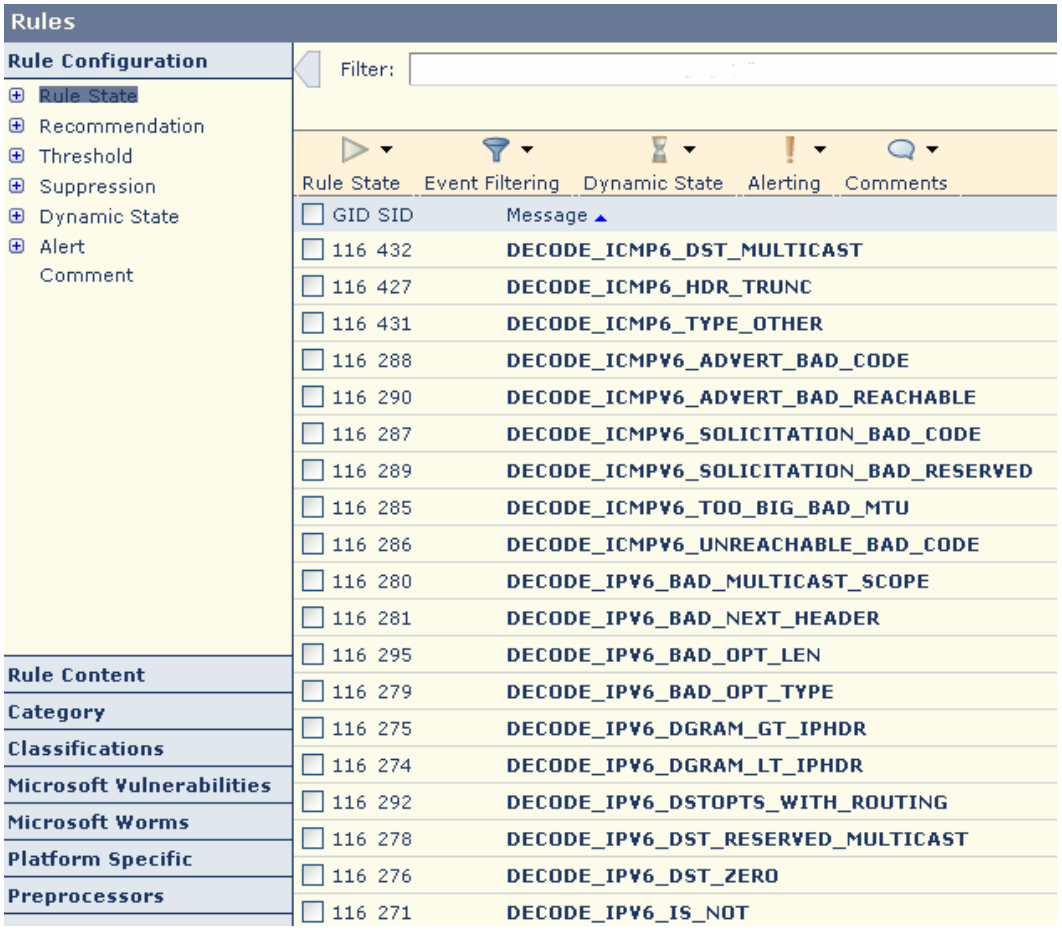
- For both IPv4 and IPv6 traffic, several preprocessors defragment traffic, perform stateful analysis of packets, and normalize traffic to allow analysis of different kinds of traffic as it will be received by the target host
- Inline normalization of IPv6 and ICMPv6 packets removes anomalies and prepares traffic for analysis
- IP Defragmentation preprocessor supports both IPv4 and IPv6 traffic

IPv6 Sensing: Fragmentation Handling

- IPS always inspects IPv6 traffic when it is present
- By default, IPS IPv6 inspection includes the following tunneling schemes:
  - 4in6
  - 6in4
  - 6to4
  - When the UDP header specifies port 3544, Teredo tunneling
- You can enable inspection of all UDP payloads for Teredo tunneling

IPv6 Sensing: Malformed Packet Detection

- Alerts Based on Address or Encapsulation
- Alerts Based on Header Values
- Alerts for ICMPv6 packets



SOURCEfire®

IPv6 Sensing: Known Attack Detection

- Detects suspicious IPv6 traffic based on known attack patterns
- Offers over 10000 rules, combined, for detection of IPv4 and IPv6 attacks
- VRT responds to new threats by creating additional rules or updating existing ones
- Detects the following types of portscans in either IPv4 and IPv6 traffic:
  - Portscans
  - Port sweeps
  - Decoy portscans
  - Distributed scans

Example: Detecting a Packet Anomaly in Teredo Traffic on a Non-Standard Port

- An IPv6 packet with an anomalous TTL value, encapsulated within an IPv4 UDP datagram, arrives via a non-standard port
- Detect Teredo on Non-Standard Ports and Detect Invalid IP Options are enabled
- All UDP payloads are checked for IPv6 traffic, regardless of port
- Decoder rule 116:270 is set to drop traffic and generate an event, detecting that the TTL value for the packet exceeds the limit
- The anomaly is detected, an alert is generated, and the traffic is dropped

Example: Detecting a Port Sweep in 6in4 Traffic

- A IPv6 host outside of your network performs TCP port scans on several hosts in your network via an IPv4 router
- The packet decoder detects the 6in4 pattern and analyzes the traffic in the encapsulated IPv6 packet
- The portscan detector is enabled and Rule 122:3 is set to drop and generate events
- The port sweep pattern is detected, alerts are generated, and the packets are dropped
- The attacker fails to obtain the reconnaissance information he was seeking

Summary

- The Sourcefire 3D System is currently IPv6 capable
- The Sourcefire 3D System Defense Center has passed host testing at ICSA
- The Sourcefire 3D System IPS is currently in Network Protection Device testing at ICSA
- Sourcefire provides comprehensive detection coverage for both IPv4 and IPv6 traffic