An Independent Division of Verizon Business

ICSA Labs
Network IPS Certification Testing Report
Network IPS Enterprise Certification Testing Criteria - Version 1.2

Sourcefire

Sourcefire 3D Sensor Family
Sourcefire 3D3800 Sensor v4.8.0.2
Sourcefire 3D4500 Sensor v4.8.0.2
Sourcefire DC3000 v4.8.0.2 (build 202)

September 21, 2009

Prepared by ICSA Labs
1000 Bent Creek Blvd, Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

NIPS-SOURCEFIRE-2009-0921-01

TABLE OF CONTENTS

Sourcefire Network IPS Certification Testing Report

Network IPS Enterprise Certification Testing Criteria - Version 1.2

Preface

Comprehensive enterprise network security is increasingly important. Savvy network and security professionals realize that a strong defense – that incorporates deep packet inspection with an appropriate real-time action – is no longer optional. These professionals know it is essential to detect and block malicious and other unwanted traffic from entering and damaging the enterprise network, while introducing little latency, and allowing valid business traffic to pass unimpeded. These needs are addressed by a class of security devices known as network intrusion prevention systems (network IPS).

In attempting to make an informed purchasing decision, it is easy to be baffled by the endless array of features, attributes, and performance characteristics claimed by network IPS developers. This is where ICSA Labs adds its value. ICSA Labs has a rich heritage of rigorous security testing. Recognized throughout the world for setting the standard in computer and network security certification testing programs, ICSA Labs has been testing and certifying the world's leading security products against criteria developed with input from key industry stakeholders for more than 15 years. In today's security marketplace, ICSA Labs is recognized as the worldwide de facto standard certification testing body for network security technologies including anti-virus, firewalls, IPsec-VPNs, and SSL-VPNs to name a few.

In late 2005, ICSA Labs began a program to test and certify network IPS devices. Until that time, third-party network IPS testing had lacked a proper combination of rigorous security coverage, network performance, and administrative requirements that were relevant to enterprise end users. In creating a test suite that incorporates all these elements and bringing to bear ICSA Labs' considerable security testing expertise, ICSA Labs has created the most exacting, comprehensive, objective, and worthwhile network IPS testing in existence today on behalf of the community of enterprise end users.

Executive Summary

What follows is a report that presents how a particular candidate fared during ICSA Labs Network IPS Certification Testing. Candidates are measured against version 1.2 of the *Network IPS Enterprise Certification Testing Criteria* and any other additional, optional criteria requirements elected by the candidate's developer. The 50+ requirements in the baseline criteria cover a wide range of functionality that a network IPS must provide in order to achieve ICSA Labs Network IPS Certification.

The test suite contains hundreds of test cases – each developed to ensure that one or more criteria requirements are met. Test candidates are subjected to test cases that combine:

- vulnerability-focused attack testing,
- evasion testing,
- denial-of-service testing,
- network performance/latency testing, and
- administrative function testing.

ICSA Labs understands that ignoring or short-changing one or more of the above areas at best falls short of serving enterprise end users and at worst totally misleads them. Therefore, in addition to comprehensive and relevant testing in the above areas, the test suite tests the listed functions simultaneously, not just in isolation. 3rd-party testing that does anything less is similarly misleading. In sum, the test suite mimics the real world network conditions in which the candidate network IPS might be deployed. As a result of these considerations, an ICSA Labs Certified Network IPS performs its functions well in live networks, not just in the lab.

In this report, the ICSA Labs Network IPS team first identifies the components of the candidate network IPS that together are able to satisfy the *Network IPS Enterprise Certification Testing Criteria*. Afterwards, the high-level procedures used to test the key aspects of a network IPS are presented. The Network IPS team then documents its findings and the results of this iteration of certification testing for the candidate, including any and all the resolved criteria violations. Finally, the report concludes with an analyst notes section, general observations, and a pictorial summary of the functions that were tested.

Product Overview

The primary component of a network IPS is the engine. This is the component that sits inline in the network detecting and preventing attacks per the applied policy. In addition, a network IPS that meets the ICSA Labs criteria may include other important components. Any additional components provide capabilities that are required by the criteria, but not natively or entirely contained in the network IPS engine itself. Typically, multiple hardware and software components comprise the candidate network IPS tested by ICSA Labs.

Hardware

Sourcefire provided ICSA Labs with the following hardware:

- Two models from the Sourcefire 3D Sensors family were tested: the Sourcefire 3D4500 sensor and the Sourcefire 3D3800 sensor. Each network IPS sensor has eight data ports that support up to four in-line segments, a separate data port for a network management from a separate Sourcefire Defense Center device, and a DB-9 console port. Each model has a server listening on TCP port 22 (ssh) for command line driven management. And unlike the 3D3800, the 3D4500 also has a server listening on TCP port 443 (https) for private, web-based management, and this interface was used to gather administrative log events.
- Sourcefire Defense Center 3000 (DC3000) – This is a Jarrell 2U appliance running Sourcefire's Linux-based operating system. The DC3000 enables central management of multiple sensors and contains other capabilities including the ability to schedule automated policy downloads and distribution across sensors. This was the primary mean to access the 3D3800 and 3D4500 for this round of testing.

The following hardware was also used:

- PC running Microsoft Windows 2000 SP4 with Kiwi Syslog Server – This was used because not all required log events included a year in the timestamp.

Software

Sourcefire provided ICSA Labs with the following software:

- Security Enhancement Update (SEU) – Software updates for the network IPS engine. SEUs contain new and updated intrusion rules, as well as new and updated preprocessors and protocol decoders.
- ICSA-IPS-Policy-AUG-2009.sfo – Sensor policy file. This policy will detect and prevent all attacks targeting ICSA Labs' April 2008 vulnerability set.
  (Md5sum: fcf7fcd660df48708de1ac437ff8146d)
- ICSA-IDS-Policy-AUG-2009.sfo – Sensor policy file. This policy will detect and permit attacks targeting ICSA Labs' April 2008 vulnerability set.
  (Md5sum: 05e3c562e59afedccd79f8da8b36a09c)

Multiple Network IPS Engine Models

Network IPS developers often provide multiple network IPS engine models to attract and accommodate a broad range of customers. Among other things, each network IPS engine model often has different interface types (e.g., copper versus fiber), a different number of interface segments, and other hardware differences. Also across models the developer may report differing values for maximum throughput, number of new connections, etc. Though these differences exist, the software and/or firmware providing the network IPS engine functionality across a group of related hardware models remains essentially the same.

In an effort to be practical while still providing a meaningful level of assurance to end users, ICSA Labs tests two or more models from a group of related models. Additionally, the developer signs an ICSA Labs attestation form confirming that all the models in the group are indeed the same with respect to the criteria. Therefore the attestation form coupled with the successful testing of at least two models from the group leads to certification for not just the models tested but the entire group.

The following table depicts the entire group of ICSA Labs Network IPS Certified models. The italicized models are the ones that were tested during this and previous iterations of annual and maintenance testing. Models are rotated in-and-out of ICSA Labs such that all models in the group are tested over time. The models listed are subject to change. For the most up-to-date list of certified product models refer to the Network IPS Certified Devices List on the ICSA Labs website at http://www.icsalabs.com/nips/certifiedproducts.html.

Sourcefire Network IPS Model Names
3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, ***3D3800***, ***3D4500***, 3D5800, 3D6500, 3D9800, 3D9900

Table 1 - Group of Sourcefire 3D Sensor Models that are ICSA Labs Network IPS Certified

Testing Methodology Highlights

Background

Developing a comprehensive network IPS test suite that is relevant to enterprise end users is a complex and lengthy undertaking. In fact, ICSA Labs spent more than a year developing the most rigorous network IPS test suite in the industry. And we are continually adding to it. The test suite is comprised of hundreds of individual test cases focused on three main categories: security coverage tests, network performance tests, and administrative tests. This section provides an overview of the key test cases performed by the network IPS team at ICSA Labs in each category.

Security Coverage Tests

There are thousands of known vulnerabilities with more being discovered every day. Since some vulnerabilities are not remotely exploitable and others are only present in obscure software rarely found in enterprise networks, not all vulnerabilities are relevant for network IPS testing. To determine the vulnerabilities that are most relevant for its testing, ICSA Labs performs research[1] on a regular, ongoing basis. Each developer's solution is tested against attacks targeting this evolving set of remotely exploitable, high-severity vulnerabilities spanning the last several years. The vulnerabilities are present in software likely to be found on enterprise networks including Microsoft IIS, Microsoft Exchange Server, and Symantec Backup Exec.

To attain and retain ICSA Labs Network IPS Certification, the candidate being tested must repeatedly prevent any and all attacks targeting the vulnerability set while 80% of the product's bandwidth is consumed by real, background network traffic. In the midst of the network traffic, ICSA Labs injects attacks at pseudo-random intervals. If a replayed attack targeting a vulnerability is either not detected or detected but not prevented, then ICSA Labs verifies the findings by running the actual attack through the candidate against a real vulnerable system. ICSA Labs maintains a collection of vulnerable systems on a network known as "Death Row". This network is comprised of numerous VMware images and physical systems running versions of enterprise software that the Network IPS team built and confirmed to be vulnerable to attacks targeting vulnerability set elements.

In the event that a candidate does not detect and/or prevent an attack targeting a vulnerability set element, ICSA Labs informs the developer that the candidate did not prevent an attack targeting a vulnerability set element. ICSA Labs then provides the CVE ID of the vulnerability for which protection is inadequate. ICSA Labs does not provide the attack, the source of the attack, or a packet capture of the attack to the developer. By placing some constraints on what is provided to the developer to resolve the violation, ICSA Labs helps the industry move toward true vulnerability protection and away from individual attack protection. With testing that is vulnerability focused, the network IPS industry is encouraged to build network intrusion prevention systems that protect against the exploitation of each vulnerability instead of reactionary protection after each new attack is released.

[1] ICSA Labs begins its research to help determine the relevant set of vulnerabilities with a service called Cisco IntelliShield Alert Manager from Cisco Systems. For more on this and other commercial tools used in testing please refer to Appendix 1.

The ICSA Labs Network IPS team also verifies that the network IPS is not easily evaded. To attain and retain ICSA Labs Network IPS Certification, the candidate being tested must not be evaded using common evasion techniques such as those found in the Ptacek/Newsham paper.[2]

ICSA Labs evasion testing combines attacks used in security coverage protection testing with evasions at one or multiple layers in the TCP/IP stack. The evasion testing exploits TCP/IP's natural, built-in flexibility in order to disguise attacks. With attacks disguised in one or more ways, those that would regularly be caught can sometimes evade detection by the candidate network IPS. ICSA Labs Network IPS Certification Testing uses a great deal of this trickery in an attempt to evade the protections provided by the candidate device under test.

Finally, ICSA Labs Network IPS Certification Testing verifies that a candidate network IPS can mitigate the effects of denial of service (DoS) attacks. ICSA Labs does not expect a network IPS to completely neutralize all DoS attacks. Instead, ICSA Labs expects any rate-based and/or resource consumption-based DoS attack launched by a motivated script kiddie to be mitigated to acceptable levels as defined in the *Network IPS Enterprise Certification Testing Criteria*.

In DoS testing, the attacking system is connected on one side of the network IPS candidate, and the target system is connected on the other. The ICSA Labs Network IPS team launches a variety of DoS attacks that are publicly known and easily executed by script kiddies. The DoS attacks include – for example – synflood, udpflood, and the whole suite of targa2 DoS attacks. At the same time, real background traffic is filling 80% of the available bandwidth with real network traffic. In order to determine whether or not a candidate can satisfy the DoS attack criteria requirement and successfully mitigate the DoS attack, the Network IPS team measures:

- the rate of DoS attack traffic that leaves the attacking system,
- the rate of DoS attack traffic that arrives at the target system,
- the reduction in capability of the candidate network IPS to pass legitimate background traffic, and
- the manageability of the candidate network IPS via its primary administrative interface.

Network Performance Tests

It is important that while under sufficient load that a network IPS device introduce a minimal amount of latency as it inspects real-world traffic. During testing, ICSA Labs increases the amount real background traffic[3] until one or more of the following occurs: the candidate begins to allow attacks to pass through that it had previously blocked at lower throughput rates, the latency of the candidate increases to such a high level that a further increase in throughput is not possible, administration of the candidate becomes impractical, or the media speed of the mission interfaces becomes the limiting factor.

ICSA Labs employs a combination of mechanisms to fill the pipe with real background network traffic. Both traffic generation tools and the open source packet capture replay tool, Tomahawk,[4] are used.

In order for Tomahawk to be used, ICSA Labs collected packet captures from the networks of existing enterprises so that the background network traffic mix used in testing would be as realistic as possible. Finding a realistic mix of traffic was challenging but necessary to properly test network IPS devices intended for real-world deployments. Before being used in ICSA Labs' network IPS testing, the packet captures went through a thorough, pre-testing cleaning process that involved removing – among other things – all malicious traffic, incomplete sessions, and sessions with incomplete frames. Following cleaning, the primary packet capture used during testing is characterized in Table 2.

[2] Ptacek, Thomas H., and Timothy N. Newsham. "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection." Technical Report. Secure Networks, Inc. January 1998. <http://www.insecure.org/stf/secnet_ids/secnet_ids.pdf>

[3] The hardware in the network IPS lab is presently capable of generating well over 10 Gbps background traffic.

[4] ICSA Labs made over 15 significant modifications to the Tomahawk greatly improving and enhancing the tool. The changes were delivered to the open source Internet community and introduced into version 1.1. Tomahawk is available at http://tomahawk.sourceforge.net.

General	IP breakdown	Application breakdown
Number of frames: 195,072 Average frame size: 462 bytes Unique IP addresses: 2614 TCP Conversations: 6444 UDP Conversations: 4754	Packets: Bytes: tcp - 85% tcp - 96% udp - 15% udp - 4%	Packets: Bytes: http - 38% http - 51% https - 35% https - 35% dns - 13% smtp - 9% smtp - 7% dns - 4% other - 7% other - 1%

Table 2 - Characteristics of Background Traffic Used During Testing

While the candidate is configured to block relevant attacks, one-way latency[5] is measured following guidance provided in RFC 2544. Seven different datagram sizes are used during testing. At each size, 1200 UDP datagrams are sent at a rate of 10 datagrams per second. The reported latency is calculated as the average value measured with the network IPS device inline minus the average value that was separately measured with just a crossover cable in place. The test is conducted first with no background traffic present and subsequently with realistic background traffic filling 80% of the product's available bandwidth. The Network IPS team verifies that the measured average one-way latency is lower than the value permitted by the criteria.

Administrative Tests

Lastly, but importantly, ICSA Labs Network IPS certification testing includes thorough coverage of pertinent administrative functions provided by the candidate network IPS. Among other items, there are stringent logging and reporting requirements. The Network IPS team generates events that must be logged -- including attack attempts, policy modifications, and network link status changes -- and verifies that appropriate information required by the criteria is captured by the candidate.

Another important administrative function that is tested is the capability of the candidate network IPS to automatically acquire and apply the latest set of coverage protection updates. The Network IPS team connects the candidate such that it can access its update server. ICSA Labs then configures the appropriate settings to enable the candidate to automatically update its protection, and verifies that the protection updates are properly received and applied. This important capability helps ensure enterprise end-users remain protected long after the initial deployment of the network IPS engine.

What Triggered Testing?

This testing report serves two purposes. First it marks Sourcefire's having attained certification across its entire product line. For that to happen, the 3D4500 was tested against the complete set of test cases to ensure it, like the 3D3800, satisfied all of ICSA Labs' network IPS criteria in the same way. The second purpose is to show the results of "maintenance testing" that ICSA Labs performed on the 3D3800.

The "maintenance testing" that was performed on the 3D3800 was done to ensure it could provide continued coverage protection since ICSA Labs updated the vulnerability set in April 2008. Typically Sourcefire would have been tested soon after the set was published; however, at that time, the 3D3800 was already in the midst of maintenance testing against the previous vulnerability set. In addition to that, Sourcefire released generally available software version 4.8 that contained all of the fixes required from the initial round of ICSA Labs network IPS testing that concluded in December 2006. ICSA Labs was also in the process of verifying the incorporation of those fixes. Thus their maintenance testing against the April 2008 vulnerability set was pushed back. Finally note that beginning about 30 days from this report's publication date, Sourcefire will be tested to ensure coverage protection for the current vulnerability set that was published in Feb 2009.

[5] This is the time interval between the first data bit out of the transmit port to the first data bit received by the receive port.

Regarding the vulnerability set[6], please note that the set evolves over time. In fact, ICSA Labs regularly performs research on all known remotely-exploitable vulnerabilities. The culmination of the research is an updated vulnerability set comprised of the high severity vulnerabilities that are most relevant to enterprise end users. Each time the vulnerability set is updated, newer vulnerabilities are added to the set, while other vulnerabilities that are older or that are no longer as relevant are removed. And once it is updated, all certified product vendors must be tested against it to demonstrate coverage protection.

The April 2008 vulnerability set against which both Sourcefire models were tested can be found at:

http://www.icsalabs.com/icsa/docs/html/communities/nips/criteria/VulnerabilitySet_ServerSide_080403.xls

Finally, note that detailed information about how the Sourcefire 3D System 3D3800 fared during previous iterations of ICSA Labs network IPS testing can be found in the certification testing report available from the following URL:

http://www.icsalabs.com/icsa/docs/html/communities/nips/certifiedproducts/Sourcefire_3D3800_NIPS_mtr_081111.pdf

Summary of Findings

There is no such thing as a partial pass in ICSA Labs Network IPS certification testing. In order to attain ICSA Labs Network IPS Certification, the candidate network IPS must meet – in its entirety – the latest version of the ICSA Labs *Network IPS Enterprise Certification Testing Criteria*. The table below documents all the criteria requirements that were tested and satisfied. It begins by identifying the criteria and version and it identifies any optional criteria modules against which the candidate network IPS was measured.

Criteria	*Network IPS Enterprise Certification Testing Criteria*	**Version**	1.2
Optional Modules	None		

Security Testing

Requirement ID	Requirement Summary	Result
ST1	Mission Interfaces Ignore Non-Administrative Traffic	PASS
ST2	Cannot Obtain Unauthorized Access to Administrative Functions	PASS
ST3	Engine Itself is Invulnerable to Attacks Via Mission Interfaces	PASS
ST4.1	Prevents Attacks Targeting the 109 Most Relevant Vulnerabilities[7]	PASS[a]
ST4	Prevents Attacks That Use Evasion Techniques to Escape Detection	PASS
ST5	Mitigates All DoS Attacks Regardless of Origin	PASS
ST6	Repeatedly Provides Protection for ST4 and ST5 Related Attacks	PASS

[6] In this report, the words “vulnerability set” used together refer to a released version of the *Vulnerability Set* referenced by the *Network IPS Enterprise Certification Testing Criteria.*

[7] Though a security bulletin from a 3rd party (e.g., Microsoft) may suggest that a vulnerability has a critical severity, such a vulnerability may or may not be in the vulnerability set. If it is in the set, products tested by ICSA Labs must provide protection but are not required to have protection enabled by default.

ST7	After Tuning, Does Not Detect Attacks in Clean Traffic (i.e., No False Positives)	PASS[b]
Administration		
Requirement ID	Requirement Summary	Result
AD1	Perform Remote Administration of Engine	PASS
IA1	Enforce Identification & Authentication	PASS
IA2	Set Strong Passwords	PASS
Traffic Flow		
Requirement ID	Requirement Summary	Result
TF1	Passes Clean Traffic While Enforcing Policy	PASS
Logging		
Requirement ID	Requirement Summary	Result
LO1.1.a.i	Logs Attacks Targeting Vulnerability Set in Detect & Prevent Mode	PASS
LO1.1.a.ii	Logs Attacks Targeting Vulnerability Set in Detect & Permit Mode	PASS
LO1.2.a	Logs Powering Down Engine	N/A
LO1.2.b	Logs Change to Policy Being Enforced	PASS
LO1.2.c	Logs Changes to Authentication Data	PASS
LO1.2.d	Logs Attempts to Authenticate for Remote Administration	PASS
LO1.3.a	Logs Engine Power On	PASS[c]
LO1.3.b	Logs Mission Interface Link Status Changes	PASS[d]
LO2.1.a	All Required Log Data Includes Timestamp	PASS
LO2.1.b	All Required Log Data Properly Describes the Event	PASS
LO2.2.a	Events Under LO1.1.a Indicate Action Taken	PASS
LO2.2.b	Events Under LO1.1.a Indicate Protocol	PASS
LO2.2.c	Events Under LO1.1.a Indicate Source & Destination IPs	PASS
LO2.2.d	Events Under LO1.1.a that are TCP or UDP Indicate Ports	PASS
LO2.2.e	Events Under LO1.1.a Include Unique Identifier of Engine	PASS
LO2.3.a	Events Under LO1.2.d Indicate Username	PASS

LO2.3.b	Events Under LO1.2.d Indicate Success or Failure	PASS
LO2.4.a	Events Under LO1.3.b Indicate Link Status	PASS
LO3	Log Data Available for Review and Human Readable	PASS
LO4	Correlation Exists Between Split Log Records For Any Single Event	N/A

Reporting

Requirement ID	Requirement Summary	Result
RE1	Reports Top 10 Violations Over Several Periods	PASS
RE2	Reports Top 10 Sources of Violations Over Several Periods	PASS

Administration

Requirement ID	Requirement Summary	Result
AF1	Place interfaces into Transparent or Routing Mode (Transparent was chosen)	PASS
AF2.1	Access Through Remote Administrative Interface	PASS
AF2.2	Configure & Apply Policies	PASS
AF2.3	Configure & Change or Acquire Date & Time	PASS
AF2.4	Enable & Disable Logging of Required Events	PASS
AF2.5	Display Required Log Data	PASS
AF2.6	Generate & Display Required Report Data	PASS
AF2.7	Configure & Change Authentication Data	PASS
AF2.8	Configure & Change Remote Administration Settings	PASS
AF2.9	Enable & Disable Network Acquisition of Protection Updates	PASS

Functional Testing

Requirement ID	Requirement Summary	Result
FT1	Administrative Functions Defined in AF1 & AF2 (See Above) Work Properly	PASS
FT2	Introduces Acceptable Average One-Way Latency	PASS[e],[f]

Documentation

Requirement ID	Requirement Summary	Result
DO1	Provides Enough Accurate Guidance to Set Up Candidate	PASS

DO2	Provides Enough Accurate Guidance to Perform Administrative Functions	PASS

Table 3 - Criteria Requirements Tested and Satisfied

---

[a] **Resolved Criteria Violation**: When no background network traffic or evasion techniques were included, the 3D Series models tested provided proper coverage protection for the majority of the 109 vulnerabilities in the April 2008 *vulnerability set* (see vulnerability set). However, attack attempts targeting the following vulnerabilities were initially not detected:

	CODE		
CVE ID	**α**	**γ**	**Brief Description**
2003-0605	●	●	Microsoft Windows RPCSS DCOM Interface Denial of Service Vulnerability
2004-0397	●	●	Subversion Date Parsing Overflow
2006-0150	●	●	Linux/Unix: Apache auth_ldap Module Format String Vulnerability
2006-3439	●	●	Microsoft Windows Server Service Buffer Overflow Vulnerability
2007-1675	●	●	IBM Lotus Domino nimap.exe CRAM-MD5 Buffer Overflow
2007-2446	●	●	Samba NDR Parsing MS-RPC Request Handling Buffer Overflow Vulnerability
2007-2881	●	●	Sun Java System Web Proxy Server SOCKS Module Buffer Overflow Vulnerability

CODE values:

α	-	Not logged with *Detect and Permit* or *Detect and Prevent* policy
γ	-	Not blocked with *Detect and Prevent* policy

Note on the above security coverage results:
Before proceeding, ICSA Labs verified the fixes provided by Sourcefire, including new or modified signatures and signature settings, and confirmed that the fixes resolved all of the security coverage criteria violations listed above.

[b] **Resolved Criteria Violation**: Previously, when the Sourcefire 3D Sensor Family was configured with a “detect and prevent” policy, a false positive was found during testing when clean traffic (similar to the attack traffic targeting CVE-2004-0397) was improperly blocked. The legitimate traffic was blocked by SID (1:14601) EXPLOIT Subversion 1.0.2 get-dated-rev buffer overflow attempt. As this SID was not blocking any testing-related attacks Sourcefire disabled this SID for the policy listed in this report and the legitimate traffic was no longer blocked.

[c] **Resolved Criteria Violation**: When the sensor is powered on, a log message is generated and sent to the sensor’s internal syslog server. On all models in the Sourcefire 3D Sensor Family (refer to Table 1 above), with the exception of the 3D3800, the internal syslog server does not include a year in the timestamp. Previous Sourcefire testing had been performed against the 3D3800 alone. At that time, this criteria violation was found, reported and corrected. Sourcefire will be fixing this behavior on all models in the Sourcefire 3D Sensor Family such that the year may be added to the timestamp if desired. The interim workaround for testing on the 3D4500 was to add an external Kiwi Syslog Server to the collection of hardware comprising the subject under test. Events like this one that are normally logged to the local syslog server were redirected instead to the external Kiwi Syslog Server which includes the year in all timestamps for logged events.

[d] **Resolved Criteria Violation**: In terms of logging changes to the mission interface link status, the products behave as described in the previous end note. The fix and workaround are the same as well.

[e] In real enterprise networks, the throughput of a network IPS varies depending on a number of factors. For example, these factors include the security policy being enforced and all the many properties of the traffic passing through the network IPS (refer back to Table 2 for a partial list). And when it comes to certification testing, device throughput is not only affected by those factors but is also impacted by the test tools and test procedures used to generate or reproduce the network traffic.

Given that many factors affect device throughput, ICSA Labs network IPS testing is not intended to measure the maximum amount of throughput that a network IPS can withstand. Instead, the purpose is to ensure that the network IPS satisfies all the criteria requirements while under load.

To determine an appropriate load, ICSA Labs observes the network IPS' top level of sustainable throughput. After settling on the top level, which is impacted by the performance-related factors mentioned above, the Network IPS team further reduces the throughput by at least 20% – i.e., so the load is heavy but not overwhelming. Then while passing and inspecting that amount of network traffic, the device is thoroughly load tested.

Presented in the table below are the throughput loads under which each model was tested. Note that as stated in the preceding paragraphs, the table is not intended to indicate the maximum throughput of the sensors listed. Instead the table reflects the throughput at which the models were tested along with the number of interface sets, detection engines, and detection resources used.

Presented in the table below are the throughput loads under which each model was tested. The throughput load for the 3D4500 depicted below correspond to one interface set, one detection engine (DE) and one detection resource (DR) and does not reflect the maximum throughput of the sensor itself.

Network IPS Model	Tested at
3D3800	535 Mbps
3D4500	500 Mbps

Table 4 – Throughput Used to Test Under Load

[f] The results of latency testing are shown in Table 5 below.

	UDP Frame Size in Bytes						
	64	**128**	**256**	**512**	**1024**	**1280**	**1518**
No traffic	87.0	83.5	87.2	101.6	123.4	108.4	120.5
400 Mbps	255.1	258.7	249.9	242.9	248.6	246.9	255.3

Table 5 – Average One-Way Latency Introduced by 3D4500 (in microseconds)

The highest incremental latency introduced by the 3D4500 in testing was 255 μs for UDP frame size of 1518 bytes. To put that value into perspective, the maximum latency measured on the ICSA Labs network IPS test jig with a cross-over cable inline instead of the network IPS and 400 Mbps of background traffic (80% of 500 Mbps) and 1518 UDP frame size was 376 μs. In that case, the only pieces of hardware in the path of the packets were two enterprise-class switches. This data and data from previous testing of the 3D3800 suggests that the 3D Series introduces only slightly more latency than one of these switches.

Analyst Notes

Included below are factual observations, general notes, specific comments, and/or opinions collected during testing by the Network IPS team. This information did not directly relate to satisfying a criteria element. Nonetheless, the information is presented as it may be useful to enterprise end users.

Developer Philosophy

When developers build a network IPS they have a very good idea about the kind of end user customer networks for which their product is best suited. End users could benefit from knowing this information as well. There are a number of places in a network where one might deploy a network IPS and there are organizations of all different sizes with all kinds of different needs in terms or protection, latency, etcetera. ICSA Labs believes it is important for the end user to be able to marry their own needs to those of developers attempting to satisfy those needs. Below is a brief overview of what the Sourcefire says about its group of devices – for what purpose they should be used, where they should be deployed, and by whom.

> *Sourcefire IPS provides vulnerability-based intrusion prevention built on the foundation of Snort. Sourcefire IPS uses a rules-based language—combining signature, protocol, and anomaly-based inspection methods—to examine packets for attacks. Attacks protected against include worms, Trojans, port scans, buffer overflow attacks, spyware, Voice Over IP (VoIP) attacks, IPv6 attacks, protocol anomalies, malformed traffic, invalid headers, denial of service attacks, and zero-day attacks. The Snort rules language is well-known by security industry practitioners. Sourcefire IPS allows users to create, edit, and view detection rules. Also, full packet payloads are logged for every event so users can see exactly what threatening traffic has been detected. Sourcefire IPS can block threats directly and stop attackers by integrating with access control devices such as firewalls, routers, and switches. With inline or passive deployment options, at line speeds and fully redundant configurations, Sourcefire IPS appliances are architected to meet your network's needs.*

Tolerance for Anomalous TCP Packets

Network IPS devices tested exhibited a different level of tolerance for handling anomalous TCP packets – including those that arrived out-of-sequence, arrived outside the current window for the session, or did not strictly adhere to some other aspect of the TCP protocol. As an example, suppose a network IPS keeps a state table to track currently open TCP connections.[8] When a TCP packet arrives that does not begin a new connection (SYN packet) and does not belong to a currently open connection, the network IPS has several options for handling the anomalous packet. A more tolerant network IPS would allow the packet to pass through without logging the event. A less tolerant network IPS would block and log it.

In some cases, it may be irrelevant whether the packet is allowed to pass or whether the network IPS logs the event. For example, it is unlikely that neglecting to block a TCP RST packet would be harmful after the corresponding connection had timed out in the network IPS' connection table. However, in other cases, anomalous packets may be an indication of foul play and should not be ignored. For example, some attempts to evade network IPS devices involve sending packets with bad TCP checksums.

For most Network IPS devices, the response to anomalous packets of the type discussed in this section is configurable either by enabling or disabling certain signatures or modifying appropriate tuning parameters. Therefore, what is worth noting is the default configuration for each device. Out-of-the box, the 3D Series models required a policy to be installed before any passing of traffic could occur. With the IPS policy provided the sensors tested blocked and logged many types of anomalous TCP packets.

Other Notes

During testing of DoS attacks, the 3D4500 did not generate any alerts concerning the actual DoS attack. Other logging functionality did operate as expected.

[8] Open connections are connections for which the Network IPS has observed the 3-way handshake but has not yet observed a proper closing sequence (initiated by a FIN-ACK or RST) or the connection has not yet timed out from lack of activity.

From Patched to Generally Available

ICSA Labs requires developers to migrate any and all fixes that result from our testing into the main trunk of their network IPS' code base, making it generally available to their customers in each subsequent release. Due to developer release schedules and the need for developers to perform quality assurance testing on code fixed as a result of our testing, the release of generally available code may not be possible immediately upon the completion of annual or maintenance testing.

For this testing iteration, Sourcefire only needed to provide ICSA Labs with new policy files and updated Snort engines, which they did. Therefore, no non-coverage related changes were made to either the sensor or management appliance in the ICSA Labs network IPS test bed before or as a result of this round of maintenance testing.

Conclusion

The Sourcefire 3D Sensor Family defined in Table 1, including all necessary component parts, meets the requirements set forth in version 1.2 of the *Network IPS Enterprise Certification Testing Criteria.* Therefore, in addition to the 3D3800 which retained certification, the remainder of the Sourcefire 3D Sensor Family has successfully attained and can now likewise claim ICSA Labs Network IPS Certification.

The 3D3800 and 3D4500 remain continuously deployed in the ICSA Labs network IPS testing laboratory. This affords ICSA Labs the ability to test the network IPS devices whenever relevant vulnerabilities, attacks, and evasions emerge. Like this report, the criteria document is freely available on the ICSA Labs website at http://www.icsalabs.com/icsa/nips.

Testing Information

Lab Report
September 4, 2009[9]

Test Location

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

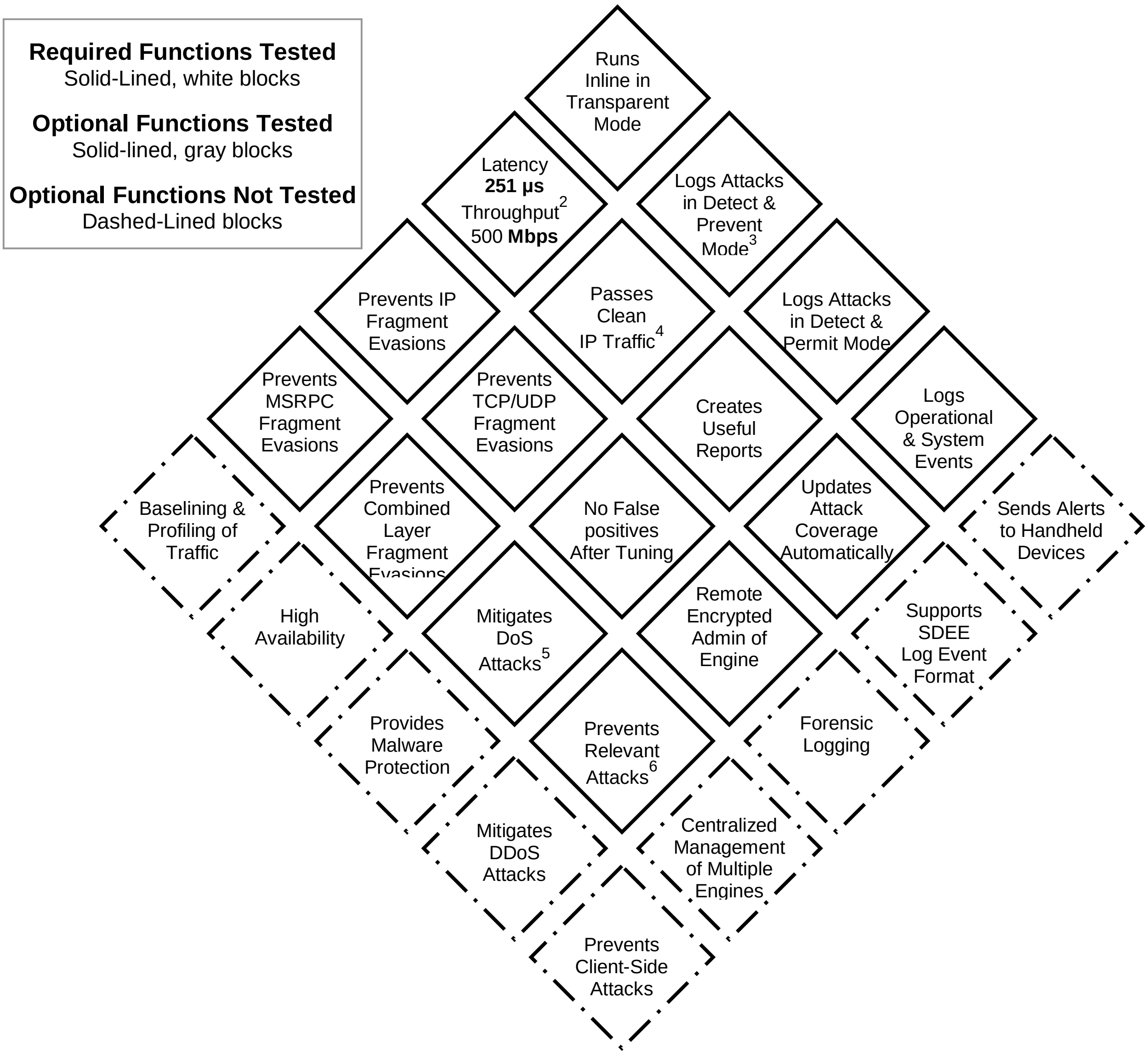
Product Developer's Headquarter Location

Sourcefire, Inc.
9770 Patuxent Woods Drive
Columbia, MD 21046
USA

[9] ***Please visit www.icsalabs.com for possible updates to this and all other reports.***

Summary of Functions Tested

Below is a high-level, pictorial representation of the key features that were and were not examined during testing.[1]


Required Functions Tested
Solid-Lined, white blocks
Optional Functions Tested
Solid-lined, gray blocks
Optional Functions Not Tested
Dashed-Lined blocks
Runs Inline in Transparent Mode
Latency 251 µs Throughput[2] 500 Mbps
Logs Attacks in Detect & Prevent Mode[3]
Prevents IP Fragment Evasions
Passes Clean IP Traffic[4]
Logs Attacks in Detect & Permit Mode
Prevents MSRPC Fragment Evasions
Prevents TCP/UDP Fragment Evasions
Creates Useful Reports
Logs Operational & System Events
Baselining & Profiling of Traffic
Prevents Combined Layer Fragment Evasions
No False positives After Tuning
Updates Attack Coverage Automatically
Sends Alerts to Handheld Devices
High Availability
Mitigates DoS Attacks[5]
Remote Encrypted Admin of Engine
Supports SDEE Log Event Format
Provides Malware Protection
Prevents Relevant Attacks[6]
Forensic Logging
Mitigates DDoS Attacks
Centralized Management of Multiple Engines
Prevents Client-Side Attacks

[1] Please refer to the *Summary of Findings* section earlier in the report for a summarization of the requirements that were tested and satisfied. For specific information about requirements refer to the criteria document itself.

[2] The maximum average latency a network IPS is permitted to introduce is often a function of the throughput at which it was tested.

[3] Logging of attacks is tested on a quiet network with no background traffic. And logging is disabled when possible while testing DoS attack coverage.

[4] To facilitate testing, the traffic was passed through the candidate with 802.1Q VLAN tags.

[5] With DoS attacks rate-limited to 10% of the rated throughput, no more than 20% of rate-based DoS attack traffic passes through the candidate, and throughput for traffic unrelated to the DoS attack is not degraded by more than 30%.

[6] These are attacks targeting a dynamic set currently comprised of 109 remotely exploitable, high severity vulnerabilities. In nearly all cases nothing needs to occur or be known in order for one of these vulnerabilities to be exploited (e.g., no valid account information is required on a vulnerable system).

APPENDIX 1: Tools Provided

A multitude of tools are used during ICSA Labs Network IPS Certification Testing. Many are open source and freely available. Of those that are open source, some were greatly modified and improved to suit our purposes (e.g., Tomahawk). Still other tools that were used are commercially available.

The following set of commercial tools is invaluable in ICSA Labs Network IPS Certification Testing. Therefore, ICSA Labs highly recommends them for use. And ICSA Labs both acknowledges and gratefully appreciates the developers of these tools permitting their use free of charge.

Note that none of the tools used – commercial or otherwise – are limited in scope to Network IPS testing. Check out the links associated with each tool to learn more about the myriad of capabilities that each possesses.

Cisco Intellishield Alert Manager Service, Cisco Systems

This is how Cisco Systems describes the IntelliShield Alert Manager Service: “Cisco IntelliShield Alert Manager is a comprehensive threat-monitoring service that provides customized information about current product vulnerabilities and security threats across the enterprise IT domain. The Cisco Adaptive Intelligence Management System, the engine at the core of the service, collects data from thousands of sources daily. The Cisco Security IntelliShield Alert Manager expert team rates each threat on type, urgency, and severity and produces actionable and customized reports that businesses can use to manage security risks.”

“The Cisco Security IntelliShield Alert Manager Service is available worldwide and will be sold primarily through Cisco channel partners with a security specialization. For pricing and additional information, please contact your Cisco sales representative or Cisco channel partner.”

ICSA Labs used the IntelliShield Alert Manager differently than a normal subscriber to the service. A normal subscriber to the service receives alerts about vulnerabilities as they come out and then uses the front end of the database to review details about these vulnerabilities. Instead, ICSA Labs performed queries on the back end of the Alert Manager database to retrieve information about a whole set of vulnerabilities that met our particular specifications.

For more information on the Cisco Security IntelliShield Alert Manager Service refer to the following web page:

http://www.cisco.com/en/US/products/ps6834/serv_home.html

CORE IMPACT, Core Security Technologies

This is how Core Security Technologies describes the CORE IMPACT tool: “CORE IMPACT(™) is the first automated, comprehensive penetration testing product for assessing specific information security threats to an organization. With CORE IMPACT, any network administrator can now safely and efficiently determine exactly how an attacker can get control of their valuable information assets. You no longer have to be an expert, or even a security specialist to perform this critical type of assessment which tests the security of your network, identifies what resources are exposed, and determines if your current security investments are actually detecting and preventing attacks.”

Using this powerful and easy-to-use tool, ICSA Labs aims relevant CORE IMPACT attacks often combined with its evasion techniques against vulnerable systems on our “Death Row” network. Death Row contains a multitude of unpatched machines, VMWare, and Qemu images – all with varying operating systems and other software that are vulnerable to a host of different, relevant vulnerabilities. Using CORE IMPACT, ICSA Labs attacks these vulnerable machines, generating “exploit packet captures”. These exploit packet captures are later replayed through the candidate Network IPS to ensure the attacks are detected and prevented.

In addition to replaying exploit packet captures, ICSA Labs also launches live exploits from CORE IMPACT through the candidate Network IPS to confirm when a exploit packet capture is missed by the candidate Network IPS. Note that other attack tools and individual attacks from other sources are used when possible in addition to CORE IMPACT. The same basic steps are followed to test the candidate Network IPS regardless of the source of the exploit.

For more information on CORE IMPACT refer to the following web page:

http://www.coresecurity.com/products/coreimpact/index.php

IXIA 400T & IxExplorer Application, IXIA

This is how Ixia describes the 400T chassis: "[The IXIA 400T is a] 4 slot chassis including integrated PC controller, IxOS operating system, IxExplorer client application, and IxScriptMate…The…IXIA 400T chassis provide[s] a platform on which an Ixia test system can be built. Each chassis supports an integrated test controller that manages all chassis and testing resources. A wide array of interface Load Modules for the chassis is available, providing the network interfaces and distributed processing resources for customizing and analyzing network traffic flows"

This is how Ixia describes the IxExplorer application: "IxExplorer™ provides a powerful and interactive Graphical User Interface (GUI) for managing Ixia test hardware resources. Complete control is provided for generation and analysis of Layer 2-4 traffic streams on an array of network interface technologies, including Ethernet,10 Gigabit Ethernet, Packet over SONET (POS), ATM, Frame Relay, etc. Ixia test ports can be independently configured to define traffic, filtering, and capture capabilities. Comprehensive statistics and graphical views enable in-depth analysis of the performance and functionality of the Device Under Test (DUT)."

ICSA Labs used the IXIA 400T and IxExplorer application to measure latency according to the methodology described in RFC 2544. For more information on the IXIA 400T refer to the following web page:

http://www.ixiacom.com/products/display?skey=ch_1600t_400t

SmartBits 600B Performance Analysis System with SmartWindow, Spirent Communications

This is how Spirent Communications describes the SmartBits 600B chassis: "The SmartBits 600B is…portable and compact, [and is a] highport-density-for-its-size network performance testing system. Compatible with all of the SmartBits 600x/6000x family of chassis, the SmartBits 600B holds up to two modules that can support up to 16 10/100 Mbps Ethernet ports, 8 Gigabit Ethernet ports, 1 10GbE port, 4 Packet over SONET (POS) ports, 4 Fibre Channel ports, or a mixture of these port types...[The SmartBits 600B] Supports sophisticated automated industry standard performance tests defined in RFC 1242 and RFC 2544."

This is how Spirent Communications describes the SmartWindow tool: "SmartWindow is a graphical user interface that provides an interactive test and measurement environment for SmartBits test modules… You can use SmartWindow to confirm proper handling of VLAN tags, as well as to test a device's throughput and latency."

ICSA Labs used the SmartBits 600B and corresponding SmartWindow software to measure latency according to the methodology described in RFC 2544. For more information on the SmartBits 600B refer to the following web page:

http://www.spirentcom.com/documents/1374.pdf