

ICSA LABS NETWORK IPS COVERAGE PROTECTION SUMMARY

STONESOFT

IPS-2000 Intrusion Prevention System

Version 4.3.0 build 4333



www.stonesoft.com



**Attained Certification
December 2007**

What the Test Means?

- *Product Appropriate for SMBs and Enterprises*
- *Blocks High Severity Attacks in Relevant Enterprise Software*
- *No False Positives After Tuning*
- *Low Latency*
- *Mitigates DoS Attacks*
- *Vendor Commitment to Independent Testing*
- *Vendor Resources are in Place to Cover Emerging Threats*

Executive Summary

Stonesoft maintained their ICSA Labs network IPS certification following a 3rd iteration of rigorous network IPS testing. Stonesoft's product was able to demonstrate 100% coverage protection against high-severity vulnerabilities using attacks with and without evasions directed at enterprise software. It did so while under significant load and without false positives. The network traffic into which hundreds of attacks and evasions were randomly and repeatedly injected over the course of the test was a mix of real world traffic taken from an actual enterprise organization's network perimeter. Detailed testing was also performed in the areas of logging, reporting, identification, authentication, remote administration, administrative functions, documentation, denials of service, and latency. Ultimately, the Stonesoft IPS-2000 Intrusion Prevention System again met the 50+ industry-standard network IPS certification testing requirements. It's the perfect fit for many SMB and enterprise organizations. For more information about the criteria requirements completely satisfied through testing, visit: www.icsalabs.com/technology-program/network-ips/testing-requirements

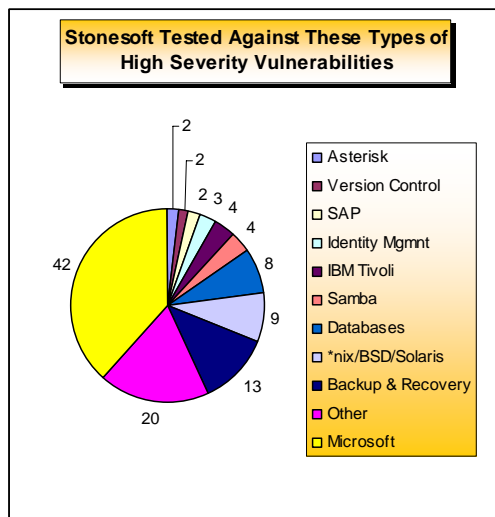


Product Overview

The IPS-2000 sensor version tested was 4.3.0 build 4333 for i386. Also, dynamic update package 161 was employed. Because no enterprise is complete without a management system, the StoneGate Management Center version 4.3.0 build 7891 was also needed for testing.

How ICSA Labs Tests Security Coverage

The test environment is designed to mimic the real world conditions in which a network IPS is deployed. Sandwiched between two heavy-duty Cisco Catalyst switches is the network IPS under test. Feeding these switches are a column of high-end, rack mounted, multi-processor Dell servers each with several GB of memory running Tomahawk. 40% of this free test tool is written by ICSA Labs. It is the Tomahawk server's job to fill the IPS' bandwidth with network traffic. A 3rd interface on each Tomahawk server is connected to a separate management switch. Also connected is a PC that accurately tabulates the throughput output of the Tomahawk boxes. The Tomahawk boxes replay once live traffic taken from actual enterprise networks; so the traffic used by ICSA Labs in testing is neither artificial nor contrived. A Tomahawk server also replays attack packet captures – each meticulously created at ICSA Labs by running real attacks against actual vulnerable systems. When an IPS fails to provide

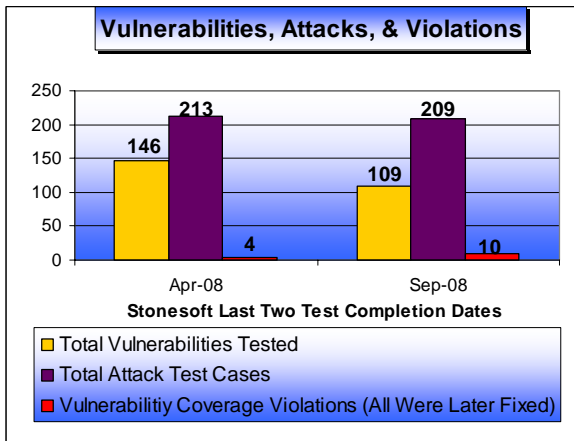


coverage protection, ICSA Labs runs the actual attack against the real vulnerable system through the IPS under test to confirm the results. In that way vendors and end users alike can trust ICSA Labs' findings. The kind of vulnerabilities tested most recently are shown in the chart above right.

During testing the Catalyst switches carry VLAN-tagged network and attack traffic in-and-out of the IPS on enough trunk lines to saturate even the fastest IPS' on the market. It's into that traffic mix that attacks and evasions are injected repeatedly and at random intervals. When using multiple sets of legitimate traffic mixes, commercial traffic generation tools including Ixia and Spirent are at ICSA Labs' disposal. These tools are also used when measuring latency.

For coverage protection testing, IPS vendors submit 2 security policies. ICSA Labs individually deploys and tests each on the network IPS under test. One is an IDS policy with logging turned on and other is an IPS policy with logging turned on. Testing both policies assures end users that an ICSA Labs certified IPS can be either an effective inline IDS or IPS.

The ICSA Labs test environment is capable of testing any IPS – regardless of throughput. It doesn't matter if the IPS is rated at 10Mbps or 10Gbps. ICSA Labs' testing is not intended to confirm vendor throughput claims. Instead, ICSA Labs tests to ensure coverage protection while processing a considerable – but not unreasonable – amount of legitimate TCP and UDP traffic. ICSA Labs' network IPS testing gives end users a good idea about how effective the IPS is in a typical enterprise network.

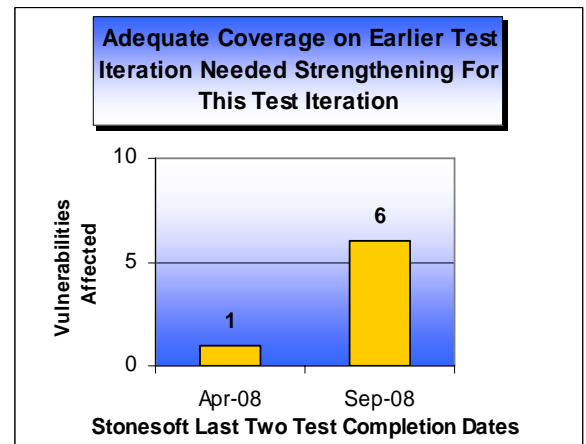


Summary of Coverage Protection Results

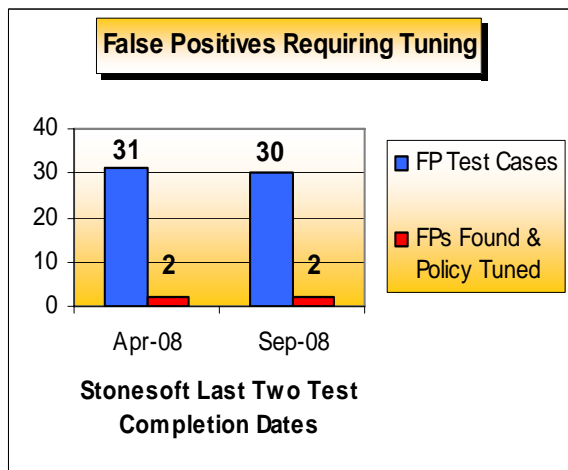
ICSA Labs tests network IPS products to ensure that they block attacks aimed at a set of enterprise vulnerabilities. The chart to the left shows that in the last two test iterations in April 2008 and September 2008 that Stonesoft was tested to ensure coverage protection for 146 and 109 vulnerabilities respectively. Initial tests showed that coverage protection had to be improved for just 3% of the tested vulnerabilities in April (4 of the 146) and 9% in September (10 of the 109). After making the fixes each time, ICSA Labs confirmed through further testing that Stonesoft had full coverage protection for all tested vulnerabilities.

For the last two Stonesoft test iterations, the chart to the right shows the number of vulnerabilities in both the current and earlier test sets for which improved protection was now required. In other words, during the testing that ended in April 2008, 1 vulnerability that had been tested in December 2007 was no longer sufficiently covered. Similarly, during September 2008 testing product protection for 6 vulnerabilities that had been tested in April was no longer sufficient. Though all of these were corrected because of ICSA Labs' testing, it highlights what has become an interesting trend for all products in testing, not just Stonesoft. That is,

For the last two



testing of IPS products reveals that coverage protection from version-to-version tested often requires coverage protection improvements to some subset of vulnerabilities previously tested by ICSA Labs - an excellent reason why network IPS products need regular, repeated third-party testing by a trusted lab.

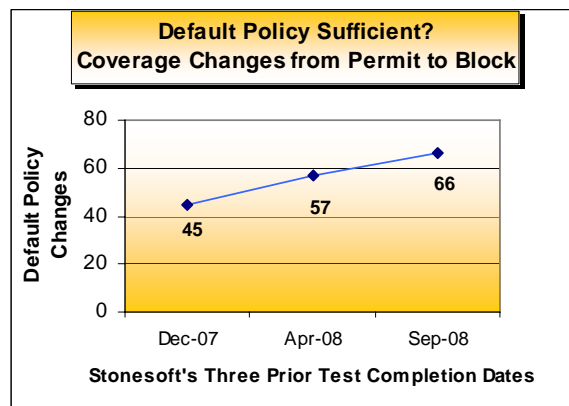


ICSA Labs ran about 30 false positive test cases during each of Stonesoft's last two test iterations. In each test iteration 2 false positives were found. Sometimes this can be tuned away by modifying the policy. Other times the vendor tightens up its protections. In either case the result is that the IPS allows legitimate traffic that it had been blocking and continues to stop malicious traffic. In both test iterations Stonesoft tightened up a couple of existing signatures that had been blocking legitimate traffic. The chart on the left depicts this.

The level of protection out of the box varies dramatically from one IPS to the next. Based on ICSA Labs' experience, end users should tune the policy for their environment rather than rely on the default policy. A separate ICSA Labs testing report provides information about the changes made to the default policy in order to provide the requisite protection needed to pass our network IPS testing. Links to these reports are found at the end of this summary report. Of particular interest is the number of protections that have to be changed from a default permit setting to a block setting. The chart below-right shows the number of these default policy changes made during each of the last three test iterations for Stonesoft. As you can see there has been a mild but steady increase in the number of protections that had to be changed from permit to block. In the most recent test, 66 signatures had to be changed and set to block in order to protect against the tested vulnerabilities.

In terms of being able to protect against new threats, end users in the market for or currently administering an IPS should look for indications about the kind of vulnerability coverage protection staff that the network IPS provider employs. First and foremost, end users can have some confidence in IPS vendors who are able to contend with repeated,

recurring, rigorous testing by an independent, third party with the testing expertise of ICSA Labs. Such IPS vendors are already in extremely good shape. But beyond that, there



During each of the last two test iterations performed by ICSA Labs, Stonesoft had to fix fewer coverage protection issues compared to their first go-round.

are additional indicators that demonstrate vendor expertise. One such indicator is how well the vendor does providing coverage protection for each vulnerability

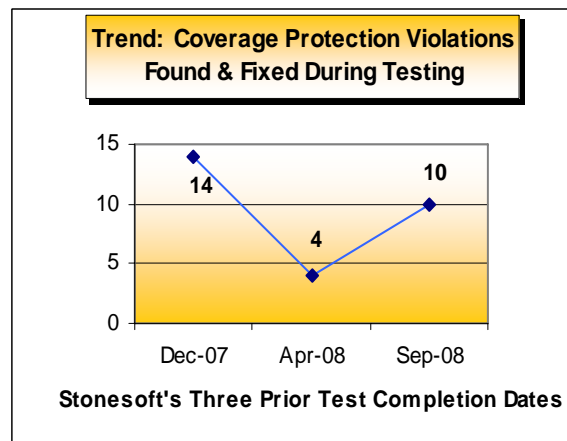
in the set against which ICSA Labs tests. During each of the last two test iterations performed by ICSA Labs, Stonesoft had to fix fewer coverage protection issues compared to their first go-round. The chart below-right depicts this trend.

A final positive note is that the Stonesoft product neutralized all denial of service attacks sent through the IPS destined for servers and systems on the opposite side. Even while under attack these servers continued to operate as expected and the IPS continued to be administrable throughout the attacks.

ICSA Labs Network IPS Test Philosophy

To ensure products are tested uniformly and so a true apples-to-apples comparison of results is possible, all tested products must provide 100% coverage protection for the complete set of vulnerabilities tested. The vulnerability set is chosen by ICSA Labs after research and is updated at least once per year to remain relevant to enterprises. It contains only high-severity vulnerabilities that are likely to be exploited. Also, the set contains only those vulnerabilities found in relevant enterprise-class software.

ICSA Labs does not focus vendor resources on protecting against attacks aimed at lower-severity vulnerabilities or vulnerabilities that are unlikely to be exploited. Also, because testing is aimed at protecting enterprise customers, ICSA Labs avoids testing vulnerabilities not found in enterprise-class software. ICSA Labs understands that end users want assurance that they will be protected against the threats that might actually happen and cause them harm as opposed to against questionable things that are unlikely to occur.



In ICSA Labs testing, the majority of vulnerabilities are server-side – i.e., the bad guy initiates the attack without user action. In addition, there are a handful of client-side vulnerabilities in the set - e.g., a user clicks on a link in an e-mail and is taken to a site that downloads and runs malicious code taking advantage of some flaw in their browser. While client-side vulnerabilities have been on the rise, they are less likely to be exploited than server-side vulnerabilities. That is because they typically require user action to be successful. Many vendors and experts alike believe that client-side vulnerabilities are best handled at the endpoint as opposed to in the network. Even so, ICSA Labs tests against an optional set of high-severity, client side vulnerabilities in relevant enterprise software when requested by vendors.

In all cases, ICSA Labs takes pains to ensure that vendors do not “have the answers to the test”. ICSA Labs does not disclose any attacks or attack packet captures. If an attack is missed, ICSA Labs tells the vendor that coverage protection for such-n-such vulnerability was not sufficient. It is then incumbent upon the vendor to remedy the situation in order to attain or maintain certification. 75% protection and 90% protection aren’t “good enough” to pass. No end user would want a product that permitted 99% coverage - if among the 1% getting through was the next slammer-like worm. Only products that protect against all of the attacks can claim certification – as long as they also pass the hundreds of tests associated with the other approximately 50 testing requirements. Thus a true apples-to-apples product comparison can be made, as all ICSA Labs certified products have passed the same set of tests.



For More Information

This report, issued by the authority of the Managing Director of ICSA Labs, summarizes how the Stonesoft IPS performs in terms of coverage protection testing – against attacks, evasions, false positives, and denials of service. More exhaustive, free testing reports indicating how the IPS performed in all aspects of ICSA Labs network IPS testing are available for this and all prior iterations of testing. Refer to the table below for prior IPS testing reports:

Sep 2008	www.icsalabs.com/sites/default/files/Stonesoft_IPS2000_NIPS_mtr_080915.pdf
Apr 2008	www.icsalabs.com/sites/default/files/Stonesoft_IPS2000_NIPS_mtr_080418.pdf
Dec 2007	www.icsalabs.com/sites/default/files/Stonesoft_IPS2000_NIPS_report_071221.pdf

Need to know more about how the Stonesoft IPS helps your organization be PCI DSS compliant? If so refer to the following report produced by ICSA Labs:

Jun 2009	www.icsalabs.com/sites/default/files/Stonesoft_NIPS_20090625_01_0.pdf
----------	--

Finally, please visit the address below to find out more about this and any other Stonesoft products that have been tested by ICSA Labs:

<http://www.icsalabs.com/vendor/stonesoft-corporation>.

About ICSA Labs

ICSA Labs, an independent division of Verizon Business, offers vendor-neutral testing and certification of security products. Many of the world's top security vendors submit their products for testing and certification at ICSA Labs. Businesses rely on ICSA Labs to authoritatively set and apply objective testing and certification criteria for measuring product compliance and reliability. ICSA Labs was the first security-product testing organization to earn ISO/IEC 17025 accreditation, validating the laboratory's world-class capabilities. For more information about ICSA Labs, visit: <http://www.icsalabs.com>.

About Stonesoft Corporation

Stonesoft Corporation (NASDAQ OMX: SFT1V) delivers proven, innovative solutions that simplify network security management for even the most complex network environments. The StoneGate Platform unifies management of entire networks - including StoneGate and third-party devices – blending integrated threat management, end-to-end high availability and network optimization into a centrally controlled system. As a result, Stonesoft provides the highest levels of proactive control, always-on connectivity and compliance at one of the lowest total cost of ownership (TCO) on the market today. Founded in 1990, the company is an established leader in network security innovation with corporate headquarters in Helsinki, Finland and Americas headquarters in Atlanta, Georgia.