



**Product Capability Assurance Report
Payment Card Industry
Data Security Standard v.1.2**

Stonesoft

IPS-2000 Intrusion Prevention System

6/25/2009

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

PCAR-STONESOFTX-2009-0625-01



Table of Contents

EXECUTIVE SUMMARY 1
PCI DSS AND ICSA LABS TESTING 1
PRODUCT DESCRIPTION..... 2
 Hardware..... 2
 Software..... 2
ICSA LABS CERTIFICATIONS 2
SUMMARY OF FINDINGS 2
TESTING INFORMATION 5
 Test Location..... 5
 Product Developer's Headquarter Location..... 5
ABOUT ICSA LABS 5

Executive Summary

The Payment Card Industry (PCI) Data Security Standard (DSS) was written by the payment card industry to help merchants worldwide to better safeguard cardholder data. Its requirements apply to merchant environments and any third-party service providers where cardholder data is processed, stored, or transmitted.

Merchants and service providers must comply with the PCI DSS standard. They are faced with purchasing and deploying computer and network security products that help them achieve and demonstrate compliance with PCI DSS requirements, or to develop and document appropriate compensating controls. Qualified Security Assessors (QSAs) likewise need assistance in understanding whether or not products in the cardholder data environment have the capacity to assist the merchant in achieving compliance with the PCI DSS.

This report helps both merchants and QSAs by identifying where a specific product or family of products has the capability to satisfy or help to satisfy one or more of the individual PCI DSS requirements. Armed with this information, merchants and QSAs can better determine where additional products or compensatory controls may be required.

PCI DSS and ICSA Labs Testing

The PCI DSS version 1.2, dated October 2008, is a set of 12 groups of requirements. These groups of requirements establish minimum security standards for merchant and service provider environments where sensitive payment cardholder data is processed, stored, or transmitted.

Within the 12 requirements there are mandates that merchants deploy several computer and network security components. There is a corresponding certification testing program at ICSA Labs for each of the five security components below which are mandated by the PCI DSS:

1. Firewalls (PCI DSS also refers to these as “network firewalls” or “perimeter firewalls”)
2. PC Firewalls (PCI DSS refers to these as “personal firewalls”)
3. Web Application Firewalls
4. Anti-virus Products
5. Network Intrusion Prevention Systems (IPS)

Beyond requiring that the security components above be present in the merchant environment, the PCI DSS imposes policy and configuration requirements as well. Policy requirements cannot be met by a product.

Statements of a product’s capability to satisfy individual PCI DSS requirements as made in this report are based on ICSA Labs’ knowledge of the product or product family. Product knowledge comes from successful certification testing in the program(s) identified in the *ICSA Labs Certifications* section below. The product may employ additional capabilities that could be relevant to PCI DSS, but these may not have been tested by ICSA Labs.

Product Description

This report is valid only for the product and version specified below. The report makes no claims regarding previous or subsequent versions of this product or product family.

Hardware

Stonesoft provided ICSA Labs with the following hardware listed below:

- StoneGate™ IPS-2000 Intrusion Prevention System (IPS-2000C), which includes both the StoneGate™ Sensor and StoneGate™ Analyzer software components.
- Intel-based PC - For the management server and client

Software

Stonesoft provided ICSA Labs with the following software and/or firmware:

- StoneGate™ Management Center (SMC)
- StoneGate™ Management Client

ICSA Labs Certifications

The product or product family listed above is currently certified in the following ICSA Labs certification testing program(s):

- Network Intrusion Prevention Systems Certification Testing Program

Details on ICSA Labs certification testing programs, including lists of certified products and certification testing reports are available on the ICSA Labs web site:

<http://www.icsalabs.com>

Summary of Findings

The PCI DSS is comprised of requirements that may be met by one or more products as well as requirements that are purely policy oriented (i.e., requirements to maintain a policy, often with specific required elements). Of those PCI DSS requirements that are product related, no single product can meet them all. However, a product can satisfy or help satisfy one or more of them. Only a subset of the product-related requirements were tested and reported on below.

Table 1 below lists the specific version 1.2 requirements which the product is capable of satisfying. PCI DSS 1.2 policy-only requirements and requirements the product cannot satisfy are omitted.

**Stonesoft
IPS-2000 Intrusion Prevention System
Product Capability Assurance Report
PCI DSS version 1.2**



The “ID” identifies the requirement number as referenced from the PCI DSS version 1.2. A “Yes” in the “Compliant?” column indicates that based on knowledge gained through the course of ICSA Labs certification testing, the product is capable in whole or in part of satisfying the PCI DSS requirement in question. The “Notes” column includes any additional information that may be of interest.

ID	PCI DSS Requirement Text	Compliant?	Notes
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	Yes	ICSA Labs verified that one can configure the network IPS with various policies that block or allow attack traffic inbound and outbound thereby allowing administrators tighter controls on the traffic into and out of the cardholder data environment.
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non-console administrative access.	Yes	All remote, non-local administration is encrypted.
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Yes	The network IPS requires all administrators to identify themselves before access is granted.
8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: <ul style="list-style-type: none"> • Password or passphrase • Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys) 	Yes	Following user identification, the network IPS requires all administrators to authenticate that they are indeed the administrator identified. Passwords were tested.
8.5.10	Require a minimum password length of at least seven characters.	Yes	Passwords were tested to at least eight characters.
8.5.11	Use passwords containing both numeric and alphabetic characters.	Yes	Passwords were tested not just with letters and numbers but with many special characters as well.
10.2	Implement automated audit trails for all system components to reconstruct the following events:	See below	
10.2.2	All actions taken by any individual with root or administrative privileges	Yes	Actions taken by an administrator can be properly logged and include: security policy changes and changes to authentication data (e.g., password changes).

**Stonesoft
IPS-2000 Intrusion Prevention System
Product Capability Assurance Report
PCI DSS version 1.2**



ID	PCI DSS Requirement Text	Compliant?	Notes
10.2.4	Invalid logical access attempts	Yes	Failures to authenticate can be logged.
10.3	Record at least the following audit trail entries for all system components for each event:	See below	The network IPS can be configured to log the data in 10.3.2, 10.3.3, and 10.3.4 (enumerated below) for all logged events.
10.3.2	Type of event	Yes	
10.3.3	Date and time	Yes	
10.3.4	Success or failure indication	Yes	
10.3.5	Origination of event	Yes	For logged events, the network IPS can label where the logged event came from. This is particularly useful when multiple devices send logged events to the same logging server.
11.4	Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.	Yes	Not every product calling itself an IPS can perform the necessary functions in and implicit to meeting PCI DSS requirement 11.4. ICSA Labs certified network IPS devices like this one are tested on a recurring basis to ensure that it can continually block the high severity attacks most relevant to enterprise end users and that it can be configured to alert personnel of suspected compromises (11.4.b). Also, the network IPS was tested to confirm that it can update itself to the latest set of protections (11.4.c).

Table 1 – The Product Helps Satisfy these v.1.2 PCI DSS Requirements

**Stonesoft
IPS-2000 Intrusion Prevention System
Product Capability Assurance Report
PCI DSS version 1.2**



Testing Information

Test Location

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

Product Developer's Headquarter Location

Stonesoft
Itälahdenkatu 22 A
Helsinki 00210
Finland

About ICSA Labs

ICSA Labs offers vendor-neutral testing and certification of security products. Hundreds of the world's top security vendors submit their products for testing and certification at ICSA Labs. The end-users of security technologies rely on ICSA Labs to authoritatively set and apply objective testing and certification criteria for measuring product compliance and reliability. The organization tests products in key technology categories such as anti-virus, anti-spyware, firewall, IPsec VPN, cryptography, network intrusion prevention, SSL-VPN, web application firewall, anti-spam and also performs custom testing engagements for products that do not fall into any of these named technology areas. For more information about ICSA Labs, please visit: <http://www.icsalabs.com>.