



**Payment Card Industry (PCI)
Data Security Standard (DSS)
Product Capability Assurance Report**

**For:
Citrix Systems, Inc.**

Prepared by:

ICSA Labs
1000 Bent Creek Boulevard, Suite 200
Mechanicsburg, PA 17050
USA

<http://www.icsalabs.com>

Executive Summary

This report gives merchants a detailed understanding of how the functionality of a specific product or family of products compares to the Payment Card Industry (PCI) Data Security Standard (DSS) version 1.1. As not all PCI DSS requirements are applicable to products, the comparison is only made for applicable PCI DSS requirements. The table in this report documents whether the product can be configured to satisfy or help satisfy a specific requirement. Requirements not supported by the product are not listed.

PCI DSS and ICSA Labs Testing

The PCI DSS version 1.1, dated September 2006, is a set of twelve requirements grouped into six logical groups called "Control Objectives". Together, these requirements establish minimum information security standards for merchant environments where sensitive payment cardholder data is stored, processed or transmitted.

Within the 12 requirements, there are effectively mandates for a merchant to deploy five computer and network security components that fall within the scope of ICSA Labs' testing and certification programs:

1. Internet Firewalls
2. PC Firewalls
3. Antivirus Products
4. Web Application Firewalls
5. Network and Host IDS / IPS Products

Beyond requiring that certain security components be present in the merchant environment, the PCI DSS imposes implicit, as well as detailed, specific policy and configuration requirements within its sub-paragraphs. Many of these requirements coincide with product capabilities mandated by the certification criteria in one or more of ICSA Labs' product testing and certification programs.

Claims of PCI DSS relevant capabilities within this report are determined by ICSA Labs based on knowledge of the product derived from the ICSA Labs certification testing programs listed in the *ICSA Labs Certifications* section below. The product may have additional capabilities which could be relevant to the PCI DSS which are not currently tested by ICSA Labs. The statements in this report are valid only for the product and version specified. This report makes no claims regarding previous or subsequent versions of this product. Finally note that in order to be eligible to receive this report, the product or family of products had to first be successfully tested in at least one of ICSA Labs' certification testing programs.

Product Description

Hardware

- NetScaler Appliance

Software

- Version 8.0 build 46.14

ICSA Labs Certifications

The products listed above are currently certified in the following ICSA Labs programs:

- Web Application Firewall version 2.0.1

Details on these and other ICSA Labs product certification programs, lists of certified products and product certification lab reports are available at the ICSA Labs web site.

Detailed Findings

The following table lists the specific PCI DSS version 1.1 requirements as they apply to security products, and details either if and how the listed product can be configured to support the requirement.

Note that of the numerous paragraphs and sub-paragraphs contained within the twelve requirements and six logical groups of PCI DSS v1.1, only the subset of requirements capable of being satisfied by a computer or network security component are listed here. Policy requirements are specifically omitted.

An entry of “Y” in the “Compliant” column indicates that based on the knowledge gained through the course of ICSA Labs certification testing, the product or product family is capable of satisfying the PCI DSS requirement in question. An entry of “N” indicates that it is not, and that compliance must be achieved through alternate means, either through the deployment of an additional product, or through the use of a compensating control.

Paragraph Number	Text	Compliant	Note
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	Y	
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	Y	
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.	Y	
6.5	Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:	See Sub-Paragraphs Below	ICSA Labs certified Web Application Firewalls are designed to provide protection against 6.5.1 – 6.5.9 as listed below
6.5.1	Unvalidated input	Y	
6.5.2	Broken access control (for example, malicious use of user IDs)	Y	
6.5.3	Broken authentication and session management (use of account credentials and session cookies)	Y	
6.5.4	Cross-site scripting (XSS) attacks	Y	
6.5.5	Buffer overflows	Y	
6.5.6	Injection flaws (for example, structured query language (SQL) injection)	Y	
6.5.9	Denial of Service	Y	
6.6	Ensure that all web-facing applications are protected against known attacks by applying either of the following methods: <ul style="list-style-type: none"> • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security • Installing an application layer firewall in front of web-facing applications. 	Y	

Paragraph Number	Text	Compliant	Note
7.2	Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.	Y	
8.1	Identify all users with a unique user name before allowing them to access system components or cardholder data.	Y	
8.5.15	If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal	Y	
10.2	Implement automated audit trails for all system components to reconstruct the following events:	See Sub-Paragraphs Below	
10.2.2	All actions taken by any individual with root or administrative privileges	Y	
10.2.3	Access to all audit trails	Y	
10.2.4	Invalid logical access attempts	Y	
10.2.5	Use of identification and authentication mechanisms	Y	
10.2.6	Initialization of the audit logs	Y	
10.2.7	Creation and deletion of system-level objects.	Y	
10.3	Record at least the following audit trail entries for all system components for each event:	See Sub-Paragraphs Below	
10.3.1	User identification	Y	
10.3.2	Type of event	Y	
10.3.3	Date and time	Y	
10.3.4	Success or failure indication	Y	
10.3.5	Origination of event	Y	
10.3.6	Identity or name of affected data, system component, or resource.	Y	
10.4	Synchronize all critical system clocks and times.	Y	
10.5.2	Protect audit trail files from unauthorized modifications	Y	

Contact Information

Test Location

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
USA
<http://www.icsalabs.com>

Vendor Headquarters

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
USA
<http://www.citrix.com>

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, PC firewall, SSL-VPN, application firewall, anti-spam and Wireless LAN. For more information about ICSA Labs, please visit: <http://www.icsalabs.com>.

Copyright

Copyright 2008 Cybertrust. All Rights Reserved. No part of this report may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information or storage retrieval system, without the express permission in writing from ICSA Labs. ICSA Labs is an Independent Division of Verizon Business.