



## PCI Compliance with **REFLEXVSA** VIRTUAL SECURITY APPLIANCE

- Overview** This document outlines the features and functions of the Reflex Virtual Security Appliance (VSA) that can enable enterprises to successfully certify their virtualized Payment Card Industry (PCI) infrastructure. The information is based on the PCI Data Security Standard (DSS) version 1.1, released in September of 2006. A complete copy of the standard can be found at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).
- Summary** The following section highlights the portions of the PCI DSS where the Reflex VSA is a compliance enabler.

Physical and Virtual Security Requirements	Reflex
<b>Build and Maintain a Secure Network</b>	
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	YES
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	YES
<b>Protect Cardholder Data</b>	
Requirement 3: Protect stored cardholder data	
Requirement 4: Encrypt transmission of cardholder data across open, public networks	
<b>Maintain a Vulnerability Management Program</b>	
Requirement 5: Use and regularly update anti-virus software	
Requirement 6: Develop and maintain secure systems and applications	YES
<b>Implement Strong Access Control Measures</b>	
Requirement 7: Restrict access to cardholder data by business need-to-know	YES
Requirement 8: Assign a unique ID to each person with computer access	
Requirement 9: Restrict physical access to cardholder data	
<b>Regularly Monitor and Test Networks</b>	
Requirement 10: Track and monitor all access to network resources and cardholder data	YES
Requirement 11: Regularly test security systems and processes	YES
<b>Maintain an Information Security Policy</b>	
Requirement 12: Maintain a policy that addresses information security	YES

# PCI Requirements/Reflex VSA Features Matrix

## Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

- 1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.
- 1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks...
- 1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment
- 1.3.7 Denying all other inbound and outbound traffic not specifically allowed
- 1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).
- 1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.

The layer two firewall module of Reflex VSA provides access list and port/protocol based policy control to support these requirements.

## Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

- 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.

All Reflex VSA sensor communications and system management is provided over a secure channel that is based on the SSH protocol.

## Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

- 6.6 Ensure that all web-facing applications are protected against known attacks by installing an application layer firewall in front of web-facing applications.  
Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.

The IPS engine of Reflex VSA has many application specific signatures designed to protect web and database applications. These signatures are continually updated to counter the latest threats.

## Requirement 7: Restrict access to cardholder data by business need-to-know

This requirement ensures critical data can only be accessed by authorized personnel.

- 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.

The Identity base NAC module in Reflex VSA can limit access to key resources based on user identification.

## Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

- 10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Reflex VSA can export security events into a SIM product and can also be configured to generate daily PCI specific reports that are delivered via E-mail.

## Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

- 11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

Reflex VSA contains a signature based intrusion prevention engine. The system can be configured to automatically update.

## Requirement 12: Maintain a policy that addresses information security for employees and contractors

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

- 12.5.2 Assign to an individual or team to Monitor and analyze security alerts and information, and distribute to appropriate personnel

Reflex VSA management client provides a real time dashboard for monitoring and analyzing security alerts.