

## PCI standard

The PCI DSS is a security standard that includes requirements for all parties that store, process or transmit cardholder data, and affects all payment channels, including retail, mail/telephone order and e-commerce. It defines requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Every Internet Merchant, Payment Service Provider or other organisation participating in the transaction process and/or saving confidential credit card information is required to meet the PCI compliance. Penalties for non-compliance include big fines and withdrawal of payment card services.

To comply PCI standards firms must scan networks four times a year and carry out an annual audit to ensure that the way they work is as safe as the standards demand. Without proper security solutions with comprehensive management this can create a true predicament.

## Meeting the compliance requirements with StoneGate security solution

For most organizations PCI DSS security standards may seem as challenging task to fulfil. However with well defined security processes and modern network security solution meeting the PCI DSS security standard can be easy. Here you can see what articles you can resolve with StoneGate and how.

### Building and Maintaining a Secure Network

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

Firewall configuration controls the access to cardholder data. A modern firewall solution combined with IPS detection can effectively prevent unwanted access and hostile attacks against customer data. Firewall provides the perimeter defence and IPS detects abnormal traffic within internal networks.

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

It is always advisable to change all default passwords and other security parameters.

### **Protect Cardholder Data**

*Requirement 3: Protect stored cardholder data.*

Cardholder data can be easily protected by implementing StoneGate IPS solution in front of servers containing stored data. IPS solution enables you to easily separate these services to a dedicated network segment isolating cardholder data to the dedicated security zone. A modern StoneGate IPS with transparent firewall functionality both prevents unauthorised access and prohibits abnormal or hostile traffic accessing the critical servers.

*Requirement 4: Encrypt transmission of cardholder data across open, public networks*

StoneGate firewall with VPN functionality is the easy way to protect the cardholder data. Integrated VPN functionality enables easy and flexible data tunnelling with secure encrypted traffic over the Internet. With StoneGate security solutions setting up VPN is easy and fast and connection can be done either with IP Sec VPN or SSL VPN according to case specific needs. For guaranteed connectivity top breed firewall solutions contain inbuilt firewall clustering and multi-link enabling multiple parallel internet connections.

### **Maintain a Vulnerability Management Program**

*Requirement 5: Use and regularly update anti-virus software*

In today's organizations the use of anti-virus engines is essential and using out of date versions is as hazardous as being without the firewall at all. With flexible StoneGate security solutions the integration of firewalls and dedicated anti-virus engines is easy. StoneGate firewall can redirect all arriving traffic to the antivirus engine that then blocks the contaminated traffic.

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

With complete security solution; StoneGate Firewall, IPS and comprehensive management it is possible to create such network structure that security flaws are easily discovered and even zero day attacks become detected. With automatic updates and upgrades administrators can be certain that they always have the latest software updates/versions

installed.

### **Implement Strong Access Control Measures**

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

StoneGate IPS solution enables you to easily create a separate these services to a different network segment isolating cardholder data to the dedicated security zone. StoneGate IPS with transparent firewall functionality both prevents unauthorized access and prohibits abnormal or hostile traffic accessing the critical servers.

*Requirement 8: Assign a unique ID to each person with computer access*

With advanced StoneGate security solution a strong authentication is easily organized. Using StoneGate SSL VPN connection it is also very easy to verify later who has accessed and what application.

*Requirement 9: Restrict physical access to cardholder data*

Fulfilling this requirement demands physical security means and does not apply to network security solution.

### **Regularly Monitor and Test Networks**

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

With StoneGate management system it is easy to meet this requirement. With SMCt it is easy to get all the needed information for audits and reports. With sophisticated tools you can collect all the needed information from one source.

*Requirement 11: Regularly test security systems and processes*

When communicating with firewalls StoneGate Intrusion Prevention System gives comprehensive protection from attacks passing firewalls. Added to regular security systems tests, it gives comprehensive protection for networks.

### **Maintain an Information Security Policy**

*Requirement 12: Maintain a policy that addresses information security*

Comprehensive security management, SMC gives you the tools to keep your policy up to date. If there seems to be any misuse in the network, management notifies you and enables you to alter the policy and policies implementing it.