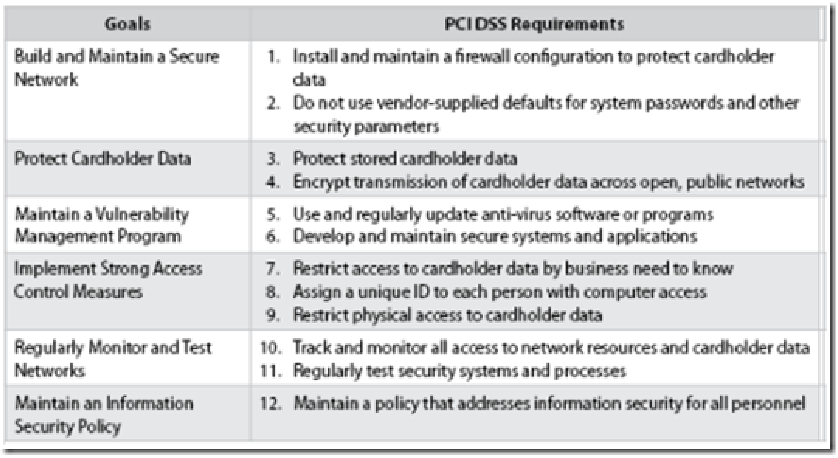
# Complying with PCI DSS&ndash;Part 1: Build and Maintain a Secure Network

**Peter Silva, 2012-17-04**

According to the PCI SSC, there are 12 PCI DSS requirements that satisfy a variety of security goals.  Areas of focus include building and maintaining a secure network, protecting stored cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining information security policies.  The essential framework of the PCI DSS encompasses assessment, remediation, and reporting.  Over the next several blogs, we'll explore how F5 can help organizations gain or maintain compliance.   Today is **Build and Maintain a Secure Network** which includes PCI Requirements 1 and 2.



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

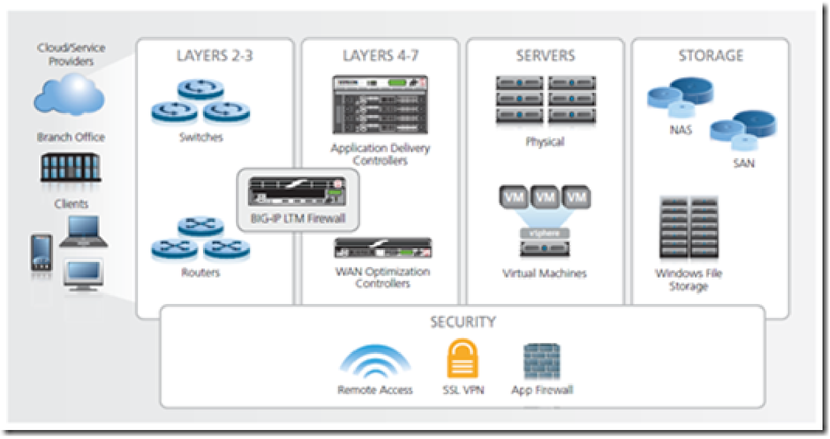
*PCI DSS Quick Reference Guide, October 2010*

The PCI DSS requirements apply to all "system components," which are defined as any network component, server, or application included in, or connected to, the cardholder data environment.  Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP servers.  Applications include all purchased  and custom applications, including internal and external web applications.  The cardholder data environment is a combination of all the system components that come together to store and provide access to sensitive user financial information.  F5 can help with all of the core PCI DSS areas and 10 of its 12 requirements.

**Requirement 1: Install and maintain a firewall and router configuration to protect cardholder data.**
**PCI DSS Quick Reference Guide description**: *Firewalls are devices that control computer traffic allowed into and out of an organization's network, and into sensitive areas within its internal network.  Firewall functionality may also appear in other system components. Routers are hardware or software that connects two or more networks. All such devices are in scope for assessment of Requirement 1 if used within the cardholder data environment.  All systems must be protected from unauthorized access from the Internet, whether via e-commerce, employees' remote desktop browsers, or employee email 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.*

**Solution:** F5 BIG-IP products provide strategic points of control within the Application Delivery Network (ADN) to enable truly secure networking across all systems and network and application protocols.  The BIG-IP platform provides a unified view of layers 3 through 7 for both general reporting and alerts and those required by ICSA Labs, as well as for integration with products from security information and event management (SIEM) vendors.  BIG-IP Local Traffic Manager (LTM) offers native, high-performance firewall services to protect the entire infrastructure.  BIG-IP LTM is a purpose-built, high-performance Application Delivery Controller (ADC) designed to protect Internet data centers. In many instances, BIG-IP LTM can replace an existing firewall while also offering scalability, performance, and persistence. Running on an F5 VIPRION chassis, BIG-IP LTM can manage up to 48 million concurrent connections and 72 Gbps of throughput with various timeout behaviors and buffer sizes when under attack. It protects UDP, TCP, SIP, DNS, HTTP, SSL, and other network attack targets while delivering uninterrupted service for legitimate  connections.  The BIG-IP platform, which offers a unique Layer 2–7 security architecture and full packet inspection, is an ICSA Labs Certified Network Firewall.



*Replacing stateful firewall services with BIG-IP LTM in the data center architecture*

**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters. PCI DSS Quick Reference Guide description:** *The easiest way for a hacker to access your internal network is to try default passwords or exploits based on the default system software settings in your payment card infrastructure.  Far too often, merchants do not change default passwords or settings upon deployment.  This is akin to leaving your store physically unlocked when you go home for the night.  Default passwords and settings for most network devices are widely known.  This information, combined with hacker tools that show what devices are on your network, can make unauthorized entry a simple task if you have failed to change the defaults.*

**Solution**: All F5 products allow full access for administrators to change all forms of access and service authentication credentials, including administrator passwords, application service passwords, and system monitoring passwords (such as SNMP).  Products such as BIG-IP Access Policy Manager (APM) and BIG-IP Edge Gateway limit remote connectivity to only a GUI and can enforce two-factor authentication, allowing tighter control over authenticated entry points.  The BIG-IP platform allows the administrator to open up specific access points to be fitted into an existing secure network. BIG-IP APM and BIG-IP Edge Gateway offer secure,  role-based administration (SSL/TLS and SSH protocols) and virtualization for designated access rights on a per-user or per-group basis.  Secure Vault, a hardware-secured encrypted storage system introduced in BIG-IP
version 9.4.5, protects critical data using a hardware-based key that does not reside on the appliance's file system.  In BIG-IP v11, companies have the option of securing their cryptographic keys in hardware, such as a FIPS card, rather than encrypted on the BIG-IP hard drive.  The Secure Vault feature can also encrypt certificate passwords for enhanced certificate and key protection in environments where FIPS 140-2 hardware support is not required, but additional physical and role-based protection is preferred. Secure Vault encryption may also be desirable when deploying the virtual editions of BIG-IP products, which do not support key encryption on hardware.

**Next**: Protect Cardholder Data

ps

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com