Complying with PCI DSS&ndash;Part 2: Protect Cardholder Data

Peter Silva, 2012-18-04

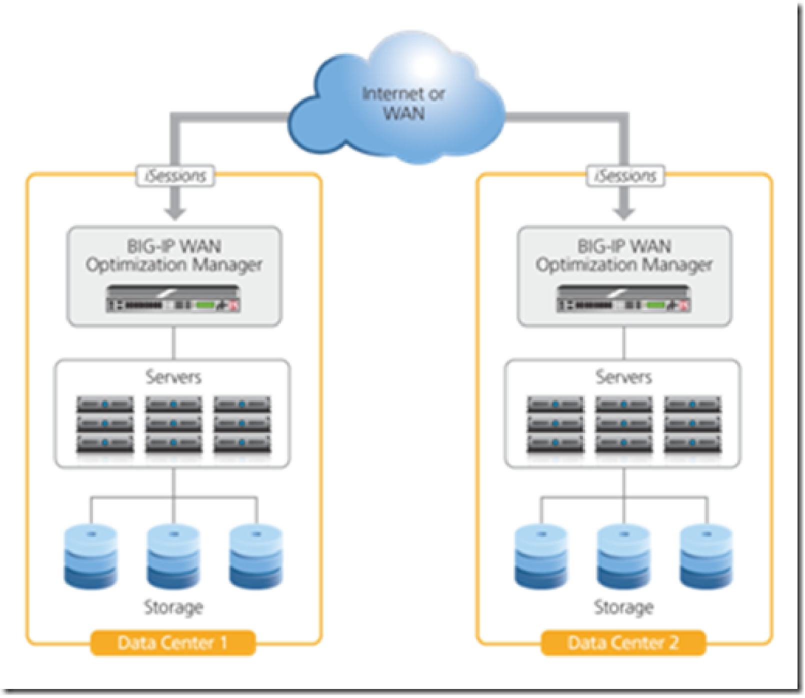
According to the PCI SSC, there are 12 PCI DSS requirements that satisfy a variety of security goals. Areas of focus include building and maintaining a secure network, protecting stored cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining information security policies. The essential framework of the PCI DSS encompasses assessment, remediation, and reporting. We're exploring how F5 can help organizations gain or maintain compliance and today is **Protect Cardholder Data** which includes PCI Requirements 3 and 4. To read Part 1, click: Complying with PCI DSS–Part 1: Build and Maintain a Secure Network

Requirement 3: Protect stored cardholder data.
PCI DSS Quick Reference Guide description: *In general, no cardholder data should ever be stored unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. If your organization stores PAN, it is crucial to render it unreadable, for instance, [by] obfuscation [or] encryption.*

Solution: The spirit of this requirement is encryption-at-rest—protecting stored cardholder data. While F5 products do not encrypt data at rest, the BIG-IP platform has full control over the data and network path, allowing the devices to secure data both in and out of the application network. F5 iSession tunnels create a site-to-site secure connection between two BIG-IP devices to accelerate and encrypt data transfer over the WAN. With BIG-IP APM and BIG-IP Edge Gateway, data can be encrypted between users and applications, providing security for data in transit over the Internet. BIG-IP APM and BIG-IP Edge Gateway can also provide a secure access path to, and control, restricted storage environments where the encryption keys are held (such as connecting a point-of-sale [POS] device to a secure back-end database to protect data in transit over insecure networks such as WiFi or mobile).   With BIG-IP Application Security Manager (ASM), data such as the primary account number (PAN) can be masked when delivered and displayed outside of the secure ADN. BIG-IP ASM also can mask such data within its logs and reporting, ensuring that even the administrator will not be able to see it.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.
PCI DSS Quick Reference Guide description: *Cyber criminals may be able to intercept transmissions of cardholder data over open, public networks, so it is important to prevent their ability to view this data. Encryption is a technology used to render transmitted data unreadable by any unauthorized person*.

Solution: The modular BIG-IP system is built on the F5 TMOS full-proxy operating system, which enables bi-directional data flow protection and selective TLS/SSL encryption. All or selective parts of the data stream can be masked and/or TLS/SSL encrypted on all parts of the delivery network. The BIG-IP platform supports both SSL termination, decrypting data traffic with the user for clear-text delivery on the ADN, and SSL proxying, decrypting data traffic on BIG-IP devices for content inspection and security before re-encrypting the data back on the wire in both directions. The BIG-IP platform, along with the F5 iRules scripting language, also supports specific data string encryption via publicly tested and secure algorithms, allowing the enterprise to selectively encrypt individual data values for delivery on the wire or for secure back-end storage. The BIG-IP® Edge Client software module, offered with BIG-IP APM and BIG-IP Edge Gateway or as a mobile application, can encrypt any and all connections from the client to the BIG-IP device. Customers have customized and installed BIG-IP Edge Client on ATMs and currency or coin counting kiosks to allow those devices to securely connect to a central server. In addition, two BIG-IP devices can create an iSession tunnel to create a site-to-site connection to secure and accelerate data transfer over the WAN.



iSession tunnels create a site-to-site secure connection to accelerate data transfer over the WAN

Next: Maintain a Vulnerability Management Program

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