Complying with PCI DSS–Part 4: Implement Strong Access Control Measures

Peter Silva, 2012-23-04

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 **Implement Strong Access Control Measures** which includes PCI Requirements 7, 8 and 9. To read Part 1, click: Complying with PCI DSS–Part 1: Build and Maintain a Secure Network, Part 2: Complying with PCI DSS–Part 2: Protect Cardholder Data and Part 3: Complying with PCI DSS–Part 3: Maintain a Vulnerability Management Program.

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

PCI DSS Quick Reference Guide description: *To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on a need to know and according to job responsibilities. Need to know is when access rights are granted to only the least amount of data and privileges needed to perform a job.*

Solution: BIG-IP APM and BIG-IP Edge Gateway control and restrict access to corporate applications and cardholder data. Secure access is granted at both user and
network levels on an as-needed basis. Delivering outstanding performance, scalability, ease of use, and endpoint security, BIG-IP APM and BIG-IP Edge Gateway help increase the productivity of those working from home or on the road, allowing only authorized personnel access while keeping corporate and cardholder data secure. For application services, the BIG-IP platform protects data on the ADN as it is communicated to the user and other service architectures. The BIG-IP platform can scan, inspect, manage, and control both incoming and outgoing data—in messaging requests such as headers (metadata), cookies, and POST data, and in message responses in metadata and in the response payload. BIG-IP APM, BIG-IP Edge Gateway, and BIG-IP ASM, along with the TMOS operating system, all work together to create a secure, role-based data access path, prohibiting malicious users from bypassing role restrictions and accessing unauthorized data. Lastly, BIG-IP ASM can help make sure web pages that should only be accessed after user login/authentication are only accessible to users who have been properly authenticated.

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

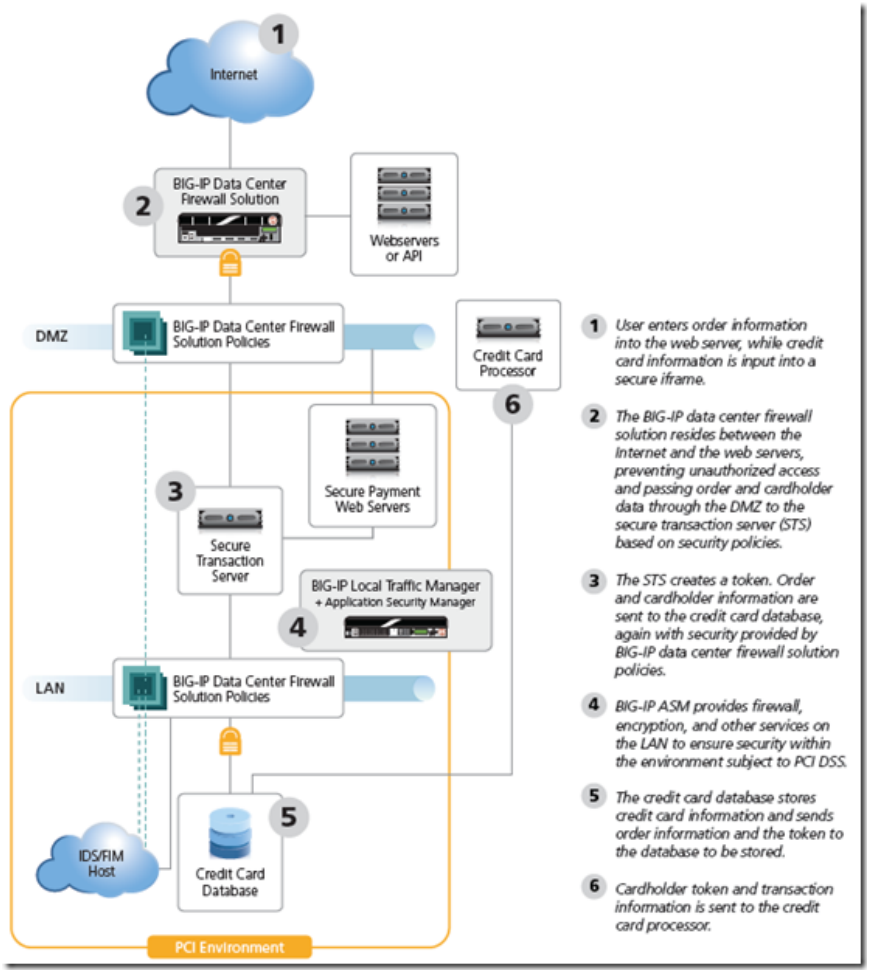
PCI DSS Quick Reference Guide description: *Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Requirements apply to all accounts, including point of sale accounts, with administrative capabilities and all accounts with access to stored cardholder data.*

Solution: The entire F5 product suite addresses the issue of unique user identification and management and acts as an enforcement mechanism. For identification, BIG-IP APM, BIG-IP Edge Gateway, and BIG-IP ASM all work on the user session level, managing a single user session throughout its duration. This is accomplished using various tools, such as secure cookies, session IDs, and flow based policies. For authentication, BIG-IP APM and BIG-IP Edge Gateway communicate with nearly all user ID and authentication systems via RADIUS, Active Directory, RSA-native, Two-Factor, LDAP authentication methods, basic and forms-based HTTP authentication, SSO Identity Management Servers such as Siteminder, and Windows Domain Servers. They also support programmatic user authentication via secure keys, smart cards, and client SSL certificates, allowing near-infinite authentication combinations across public and enterprise credential services. Transport security is accomplished through TLS/SSL. The BIG-IP platform can offload SSL computations from the back-end application servers, providing data security and network flexibility. A BIG-IP ADC is a full SSL proxy, allowing it to inspect and protect data passed to the application over SSL before re-encrypting the data for secure delivery to the application or back to the user. In addition, BIG-IP APM's detailed reporting gives organizations the answers to questions such as "Who accessed the application or network, and when?" and "From what geolocations are users accessing the network?" Reporting capabilities include custom reports on numerous user metrics, with statistics grouped by application and user.

Requirement 9: Restrict physical access to cardholder data.

PCI DSS Quick Reference Guide description: *Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems, or hardcopies, and should be appropriately restricted. "Onsite personnel" are full-and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity's premises. "Visitors" are vendors and guests that enter the facility for a short duration, usually up to one day. "Media" is all paper and electronic media containing cardholder data.*

Solution: A hardware security module (HSM) is a secure physical device designed to generate, store, and protect digital, high-value cryptographic keys. It is a secure crypto-processor that often comes in the form of a plug-in card (or other hardware) with tamper protection built in. HSMs also provide the infrastructure for finance, government, healthcare, and others to conform to industry-specific regulatory standards. Many BIG-IP devices are FIPS 140-2 Level 2 compliant. This security rating indicates that once sensitive data is imported into the HSM, it incorporates cryptographic techniques to ensure the data is not extractable in a plain-text format. It provides tamper-evident seals to deter physical tampering. In fact, the HSM in BIG-IP is certified at 140-2 level 3. By being certified at level 3, the HSM has a covering of hardened epoxy which, if removed, will render the card useless. The BIG-IP system includes the option to install a FIPS HSM (on BIG-IP 6900, 8900, 11000, and 11050 devices). Additionally, the FIPS cryptographic/SSL accelerator uses smart cards to authenticate administrators, grant access rights, and share administrative responsibilities to provide a flexible and secure means for enforcing key management security.



PCI Cardholder Data Environment with F5 Technologies

Next: Regularly Monitor and Test Networks

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