# Complying with PCI DSS

Any merchant who accepts credit cards as payment must abide by the Payment Card Industry Data Security Standard version 2.0. Compliance is crucial to protect both businesses and consumers, and F5 solutions can help organizations gain or maintain compliance.

White Paper

by Peter Silva

# Introduction

According to the nonprofit Privacy Rights Clearinghouse, more than 510 million records with sensitive information have been breached since January 2005.[1]

When the Payment Card Industry Data Security Standard (PCI DSS) was envisioned in 2004, it was actually a number of different procedures from each of the major credit card issuers. The different card programs were comparable in that they all prompted merchants to comply with a minimum set of security requirements when processing, transmitting, and storing cardholder data. The goal was to protect the sensitive information that consumers have to share over the Internet when they use credit cards to make purchases online.

Subsequently, the five major credit card companies (Visa, MasterCard, Discover, American Express, and JCB) came together and formed the PCI Security Standards Council (SSC), a neutral organization that aligned the distinct policies and then released PCI DSS version 1.0. This created one uniform set of requirements with which all parties could easily comply.

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.

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

**Figure 1:** PCI DSS requirements[2]

The PCI DSS is fairly comprehensive and incorporates different compliance tiers based on the annual number of credit card transactions. Merchants who handle more transactions must meet more in-depth requirements. Over the years, the standard has undergone clarifications, revisions, the addition of wireless and virtualization guidelines, the addition of personal identification number (PIN) entry devices, and of course, version updates—1.1, 1.2, 1.2.1, and 2.0, the most recent. PCI DSS version 2.0 was released in October 2010 and went into effect January 1, 2011. Organizations had until December 31, 2011, to implement and comply with the changes.

It's been an interesting ride for the PCI DSS, with supporters hailing its mission and others complaining that it's expensive, confusing, and subjective. If nothing else, it has made businesses focus on, and consumers more aware of, data security. Organizations that want to comply with PCI DSS can protect their web application infrastructures and make significant progress toward compliance by implementing F5 technologies.

## PCI DSS 2.0

PCI DSS 2.0 does not have extensive new requirements, but it does clarify requirements for easier understanding and makes adoption, especially for small merchants, simpler and easier. Some of the important updates include the need for a comprehensive audit prior to assessment to understand where cardholder data resides within the infrastructure. Knowing all the locations and flows of sensitive data can help in protecting them. Data form diagrams and scope reduction are important steps in becoming PCI compliant.

An evolving requirement allows merchants to execute a risk-based approach, based on business circumstances, for ranking, addressing, and prioritizing vulnerabilities. This approach encourages organizations to conduct a risk assessment and focus on areas that are the most vulnerable. This can help smaller merchants target their limited resources to a specific area of concern.

Another evolving requirement addresses the need for more effective and centralized log management. Scouring logs from various systems looking for that one nasty IP address can be cumbersome, and the ability to centralize log management is important, whether an organization is trying to be PCI compliant or not. Cloud computing could be a big beneficiary of centralized management. F5 Networks collaborates with a number of security information and event management partners such as Splunk, ArcSight, and Nitro to ensure product compatibility, provide real-time analysis of security events, aggregate log data, and generate reports for both management and compliance purposes.

Cloud computing will also benefit from the virtualization guidelines of the PCI DSS, since the latest version expands the definition of system components to include virtual components. For instance, organizations can only implement one primary function per server, so functions like web applications, databases, domain name service (DNS), and so forth should be running on separate virtual machines. The PCI SSC wants to avoid situations where different functions that may have different security levels are cohabitating on the same server.

Some other clarifications in version 2.0 include allowing companies to rank and prioritize vulnerabilities according to risk, an evolving requirement about payment applications needed to facilitate central logging, and clarification on the secure boundaries between the Internet and the cardholder data environment, otherwise known as the DMZ.

The full summary of PCI DSS changes can be found in the PCI DSS Summary of Changes Version 1.2.1 to 2.0.

## Achieving PCI Compliance Using F5 Solutions

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.

### Build and Maintain a Secure Network

#### 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.

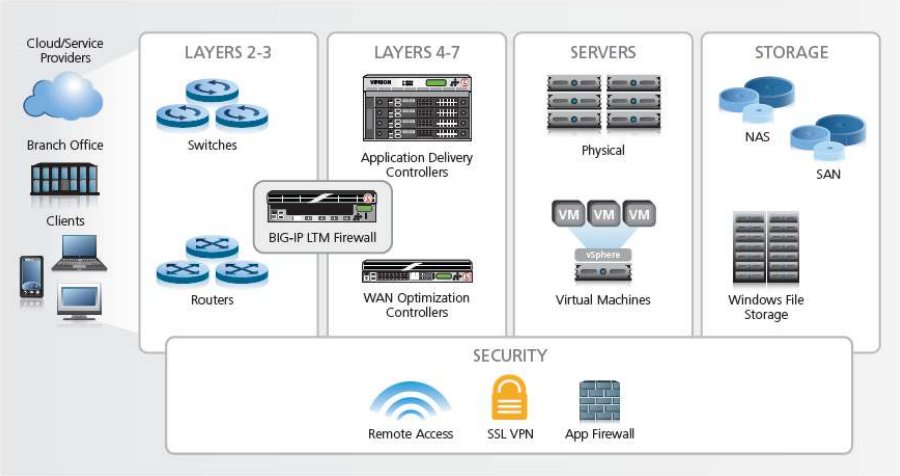


**Figure 2:** Replacing stateful firewall services with BIG-IP LTM in the data center architecture.

## 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 version 11, companies now 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.

## Protect Cardholder Data

### 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.

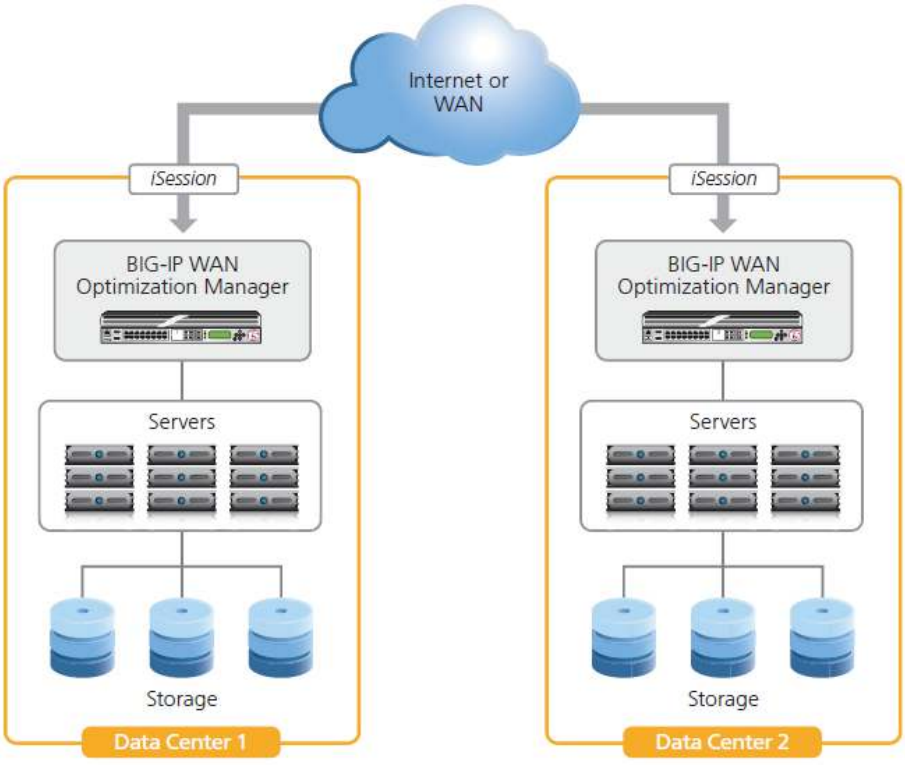


**Figure 3:** iSession tunnels create a site-to-site secure connection to accelerate data transfer over the WAN.

## Maintain a Vulnerability Management Program

### Requirement 5: Use and regularly update antivirus software or programs.

PCI DSS Quick Reference Guide description: Vulnerability management is the process of systematically and continuously finding weaknesses in an entity's payment card infrastructure system. This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

Solution: With BIG-IP APM and BIG-IP Edge Gateway, F5 provides the ability to scan any remote device or internal system to ensure that an updated antivirus package is running prior to permitting a connection to the network. Once connections are made, BIG-IP APM and BIG-IP Edge Gateway continually monitor the user connections for a vulnerable state change, and if one is detected, can quarantine the user on the fly into a safe, secure, and isolated network. Remediation services can include a URL redirect to an antivirus update server. For application servers in the data center, BIG-IP products can communicate with existing network security and monitoring tools. If an application server is found to be vulnerable or compromised, that device can be automatically quarantined or removed from the service pool.

With BIG-IP ASM, file uploads can be extracted from requests and transferred over iCAP to a central antivirus (AV) scanner. If a file infection is detected, BIG-IP ASM will drop that request, making sure the file doesn't reach the web server.

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

PCI DSS Quick Reference Guide description: Security vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures, and other secure software development practices should always be followed.

Solution: Requirements 6.1 through 6.5 deal with secure coding and application development; risk analysis, assessment, and mitigation; patching; and change control. Requirement 6.6 states: “Ensure all public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.” This requirement can be easily met with BIG-IP ASM, which is a leading web application firewall (WAF) offering protection for vulnerable web applications. Using both a positive security model for dynamic application protection and a strong, signature-based negative security model, BIG-IP ASM provides application-layer protection against both targeted and generalized application attacks. It also protects against the Open Web Application Security Project (OWASP) Top Ten vulnerabilities and threats on the Web Application Security Consortium's (WASC) Threat Classification lists.

To assess a web application's vulnerability, most organizations turn to a vulnerability scanner. The scanning schedule might depend on a change in control, as when an application is initially being deployed, or other triggers such as a quarterly report. The vulnerability scanner scours the web application, and in some cases actually attempts potential attacks, to generate a report indicating all possible vulnerabilities. This gives the administrator managing the web security devices a clear view of all exposed areas and potential threats to the website. Such a report is a moment-in-time assessment and might not result in full application coverage, but should give administrators a clear picture of their web application security posture. It includes information about coding errors, weak authentication mechanisms, fields or parameters that query the database directly, or other vulnerabilities that provide unauthorized access to information, sensitive or not. Otherwise, many of these vulnerabilities would need to be manually re-coded or manually added to the WAF policy—both expensive undertakings.

Simply having the vulnerability report, while beneficial, doesn't make a web application secure. The real value of the report lies in how it enables an organization to determine the risk level and how best to mitigate the risk. Since recoding an application is expensive and time-consuming and may generate even more errors, many organizations deploy a WAF like BIG-IP ASM. A WAF enables an organization to protect its web applications by virtually patching the open vulnerabilities until developers have an opportunity to properly close the hole. Often, organizations use the vulnerability scanner report to either tighten or initially generate a WAF policy.

While finding vulnerabilities helps organizations understand their exposure, they must also have the ability to quickly mitigate those vulnerabilities to greatly reduce the risk of application exploits. The longer an application remains vulnerable, the more likely it is to be compromised. For cloud deployments, BIG-IP ASM Virtual Edition (VE) delivers the same functionality as the physical edition and helps companies maintain compliance, including compliance with PCI DSS, when they deploy applications in the cloud. If an application vulnerability is discovered, BIG-IP ASM VE can quickly be deployed in a cloud environment, enabling organizations to immediately patch vulnerabilities virtually until the development team can permanently fix the application. Additionally, organizations are often unable to fix applications developed by third parties, and this lack of control prevents many of them from considering cloud deployments. But with BIG-IP ASM VE, organizations have full control over securing their cloud infrastructure.

BIG-IP ASM version 11.1 includes integration with IBM Rational AppScan, Cenzic Hailstorm, QualysGuard WAS, and WhiteHat Sentinel, making BIG-IP ASM the most advanced vulnerability assessment and application protection on the market. In addition, administrators can better create and enforce policies with information about attack patterns from a grouping of violations or otherwise correlated incidents. In this way, BIG-IP ASM protects the applications between scanning and patching cycles and against zero-day attacks that signature-based scanners won't find. Both are critical in creating a secure Application Delivery Network.

BIG-IP ASM also makes it easy to understand where organizations stand relative to PCI DSS compliance. With the BIG-IP ASM PCI Compliance Report, organizations can quickly see each security measure required to comply with PCI DSS 2.0 and understand which measures are or are not relevant to BIG-IP ASM functions. For relevant security measures, the report indicates whether the organization's BIG-IP ASM appliance complies with PCI DSS 2.0. For security measures that are not relevant to BIG-IP ASM, the report explains what action to take to achieve PCI DSS 2.0 compliance.

**Executive Summary**

| # | Requirement | Compliance State |
|---|---|---|
| 1 | Install and maintain a firewall configuration to protect cardholder data | N/A |
| 2 | Do not use vendor-supplied defaults for system passwords and other security parameters | ✔ |
| 3 | Protect stored cardholder data | ✘ |
| 4 | Encrypt transmission of cardholder data across open, public networks | ✔ |
| 5 | Use and regularly update anti-virus software | N/A |
| 6 | Develop and maintain secure systems and applications | ✔ |
| 7 | Restrict access to cardholder data by business need-to-know | N/A |
| 8 | Assign a unique ID to each person with computer access | ✔ |
| 9 | Restrict physical access to cardholder data | N/A |
| 10 | Track and monitor all access to network resources and cardholder data | ✔ |
| 11 | Regularly test security systems and processes | N/A |
| 12 | Maintain a policy that addresses information security | N/A |

**Figure 4:** A BIG-IP ASM PCI Compliance Report

In addition, with the unique F5 iHealth™ system, organizations can analyze the configuration of their BIG-IP products to identify any critical patches or security updates that may be necessary.

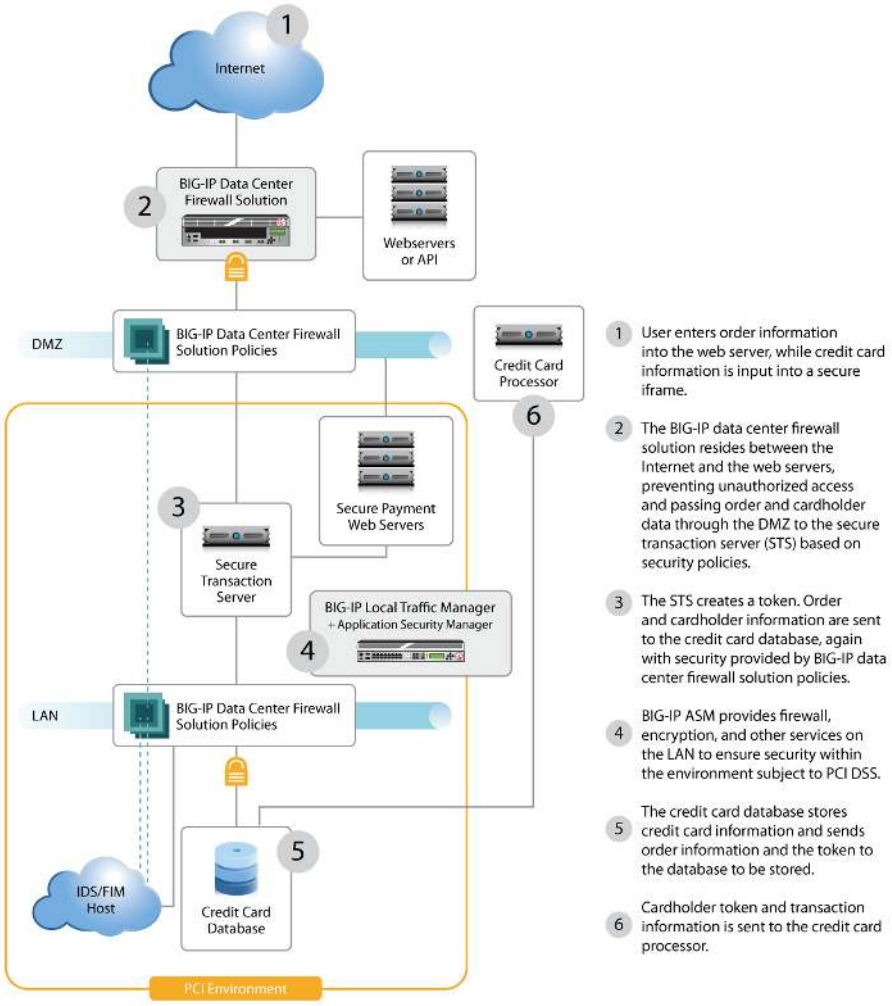


**Figure 5:** The PCI cardholder data environment with F5 technologies

## Implement Strong Access Control Measures

### 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-resistant coatings or seals to deter physical tampering. 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.

## Regularly Monitor and Test Networks

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

PCI DSS Quick Reference Guide description: Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is very difficult without system activity logs.

Solution: The spirit of this requirement is to ensure appropriate systems generate logs, with implementation and monitoring of log aggregation and correlation systems. The ability to monitor and log all user sessions and requests for access to sensitive information, such as cardholder data and Social Security numbers, is critical to any security environment. F5 offers a suite of solutions that are session-based, not packet-based. With this full reverse proxy architecture, the BIG-IP platform has the ability to manage full user sessions, regardless of the transport mechanism or network, and match those user sessions to specific data actions, supplying log data and a full audit trail from the user to the data. This allows F5 application security devices to ensure the confidentiality, integrity, and availability of all application data on the network.

All F5 products support remote logging, allowing logs to be pushed to secure networks and devices for archiving. In addition, the TMOS architecture can manage isolated, secure logging networks in conjunction with the application networks, using features such as mirrored ports, VLANs, and virtualized administrative access. Protecting network resources and application data 24 hours a day, seven days a week, without affecting network performance, is a core function and the foundation of all F5 security products.

### Requirement 11: Regularly test security systems and processes.

PCI DSS Quick Reference Guide description: Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configuration.

Solution: The spirit of this requirement is to ensure that the complying organization itself tests its security system and processes. Since F5 does not offer a penetration testing service, this is one of just two PCI DSS requirements that F5 products cannot significantly address.

### Maintain an Information Security Policy

#### Requirement 12: Maintain a policy that addresses information security for all personnel.

PCI DDS Quick Reference Guide description: A strong security policy sets the security tone for an entire organization, and it informs employees of their expected duties related to security. All employees should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

Solution: The spirit of this requirement is to ensure the adoption of a Corporate Information Security Policy (CISP). Although policy-based, F5 solutions don't, by themselves, meet this requirement in context. F5 products facilitate adherence to the CISP, but they do not actually comprise a CISP.

That said, F5 products can help organizations roll out business policies and security policies together. Applications needn't be built and deployed in a vacuum; F5 technologies can be implemented in conjunction with corporate policies that address information security.

## Conclusion

Since the inception of the PCI DSS, organizations have been laboring to understand, implement, and comply with its guidelines. Often, achieving that goal requires deploying and managing several different types of devices. The BIG-IP platform enables organizations to understand inherent threats and take specific measures to protect their web application infrastructures and to satisfy many PCI DSS requirements.

Built on the TMOS full-proxy operating system, the modular components of the BIG-IP product family can be deployed as virtual solutions or on a series of purpose-built ADCs that offer tremendous performance, scalability, and customization. Application, security, and network teams can use event-driven iRules to quickly build new services that inspect, transform, and direct application traffic.

By delivering a network firewall, distributed denial-of-service (DDoS) protection, SSL offloading, DNS security, application security, access security, traffic management, application acceleration, and much more, the BIG-IP system becomes a strategic point of control that ensures applications are always fast, secure, available, and PCI DSS compliant.

---

[1] Privacy Rights Clearinghouse, August 26, 2010.

[2] PCI DSS Quick Reference Guide, October 2010.

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

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com