



## Achieving PCI Compliance Using F5 Products

**Overview** In April 2000, Visa launched its Cardholder Information Security Program (CISP) -- a set of mandates designed to protect its cardholders from identity theft and other misuse. Visa outlined key security requirements, along with a program for validation and auditing.

In December of 2004, Visa and MasterCard joined forces to simplify compliance for merchants and payment processors with the jointly-developed, 12-point PCI standard. The scope of these requirements is quite broad, incorporating best practices for perimeter security, data privacy, and layered security. The 6 core areas and 12 requirements are listed below:

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

**Challenge** The primary reasons why PCI was created are to protect cardholder information, reduce fraud and identify common security issues/vulnerabilities which could be then exploited for malicious use if the risk is not managed appropriately. Businesses and merchants that process, store and transmit transaction information must comply with the controls.

PCI ensures that compliance with the following standards is achieved:

- American Express Data Security Operating Policy (DSOP)
- Discover Information Security and Compliance (DISC)
- MasterCard Site Data Protection (SDP) Security Certification
- Visa Account Information Security (AIS)
- Visa Cardholder Information Security Program (CISP)

### Who is Affected by PCI?

Any type of business that processes, stores and transmits cardholder and transaction data must comply to PCI in order maintain membership status. If a business fails to comply with PCI then any breach of cardholder or transaction data may result in substantial fines, resulting in the privilege to accept credit card payments being revoked.



### What is Affected by PCI?

The PCI requirements apply to all “system components” which is 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. Applications include all purchased and custom applications, including internal and external (web) applications. The cardholder data environment is a combination of all of the system components which come together to store and provide access to sensitive user financial information.

## **Solution** F5 – A Key Part Of PCI Compliance

F5 Networks can help with the 6 core areas and 10 of the 12 requirements. The following requirements discussed include only those relevant to F5’s solutions.

### **A: Build and Maintain a Secure Network**

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

**Description from PCI** - Firewalls are computer devices that control computer traffic allowed into and out of a company’s network, as well as traffic into more sensitive areas within a company’s internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees’ Internet-based access through desktop browsers, or employees’ e-mail 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 Networks represents the intelligence in the network to enable truly secure networking across all systems and network and application protocols. The BIG-IP Local Traffic Manager and FirePass SSL VPN allow for configurations that create security layers where traffic flow and application data can be controlled and inspected. By acting as an application-specific firewall (sometimes referred to as a 2<sup>nd</sup> tier firewall in the DMZ), the F5 Application Security Manager adds additional levels of security to HTTP services in the application layer. In addition, the BIG-IP with the TMOS architecture offers a unique Layer 2–7 security architecture and full packet inspection, which allows for identification of malicious activity embedded deep into the payload of both application and networking protocols. These solutions offer market leading virtualization functionality which allows for masking of all internal resources. When combined with the FirePass controller for secure application access, ASM and TMOS for application and network security, and features such as VLAN segmentation between both FirePass and TMOS, the result is a complete and secure application delivery network.

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

**Description from PCI** - Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.



**Solution** - All F5 solutions allow full access for administrators to change all forms of access and service authentication credentials, including admin passwords, application service passwords, and system monitoring passwords (such as SNMP). Appliances such as the FirePass controller limit remote connectivity to only a GUI, allowing tighter control over authenticated entry points. The BIG-IP and TMOS allow the administrator to open up multiple access points for administration to fit into the existing secure network. Both FirePass and the BIG-IP offer secure role-based administration (SSL/TLS & SSH) and virtualization for designated access rights on a per-user/group basis.

## B: Protect Cardholder Data

### Requirement 3: Protect stored data

**Description from PCI** - Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

**Solution** - The BIG-IP and ASM have full control over the data and network path, allowing the devices to secure data both in and out of the application network. With both TMOS and FirePass, data can be encrypted between the end-user and the applications, providing security for data “in the wild”. With ASM and TMOS, data such as the PAN can be masked when delivered and displayed outside of the application network. The FirePass controller can provide a secure access path to and control restricted storage environments where the encryption keys are held (such as connecting a POS device to a secure back-end database, protecting data in transit over networks such as insecure WiFi networks).

### Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

**Description from PCI** - Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

**Solution** - F5 Networks offers an exclusive full-proxy architecture allowing for bi-directional data flow protection and selective SSL encryption. All or selective parts of the data stream can be masked and/or SSL encrypted on all parts of the delivery network. The BIG-IP and TMOS support both SSL Termination, decrypting data traffic between the end-user for clear-text delivery on the application network, and SSL Proxying, decrypting data traffic on BIG-IP and FirePass for content inspection and security and re-encrypting the data back on the wire in both directions. TMOS and iRules support specific data string encryption via publicly tested and secure algorithms as well, allowing the enterprise to selectively encrypt individual data values for delivery on the wire or for secure back-end storage.

## C: Maintain a Vulnerability Management Program

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

**Description from PCI** - Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

**Solution** – With FirePass, F5 Networks offers the ability to scan any remote or internal system to ensure that an updated anti-virus package is running prior to connecting to the network. Once connected, FirePass continually monitors the user connections for a vulnerable state change, and if detected, can quarantine the user on-the-fly into a safe, secure, and isolated network, using VLAN segmentation in conjunction with BIG-IP and TMOS. For servers in the datacenter, BIG-IP can integrate with existing network security and monitoring tools, and if an application server is determined to be vulnerable or compromised, can automatically take that device out of the service pool or quarantine it as well.

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

**Description from PCI** - Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

**Solution** - F5 Networks offers the ASM (Application Security Manager), which is a market leading web application firewall allowing protection for vulnerable and poorly written web applications. Utilizing both a positive security model for dynamic application protection along with a strong signature-based negative security model, ASM provides application layer protection from both targeted and generalized application attacks and protection against the OWASP Top Ten vulnerabilities and the WebAppSec Threat Classification lists. When implemented in conjunction with a vulnerability scanning application and robust patch management system, ASM and BIG-IP can add additional security support to the application network by protection the applications between scanning and patching cycles and against Zero Day attacks that signature-based scanners won't find. Both of these solutions are critical in creating a secure development environment, especially for applications that developed in-house. ASM and TMOS can also be used to implement, manage, and enforce an application revision control system. ASM's policy approach and the BIG-IP system's management network work together to ensure that applications are secure, available and performing optimally.

### **D: Implement Strong Access Control Measures**

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

**Description from PCI** - This requirement ensures critical data can only be accessed by authorized personnel.

**Solution** – For secure access, the FirePass controls and restricts access to corporate applications and cardholder data using a standard web browser. Access is granted at both user and network levels on an as-needed basis. Delivering outstanding performance, scalability, ease-of-use, and end-point security, the FirePass controller helps increase the productivity of those working from home or on the road, allowing only authorized personnel and keeping corporate data secure. For application services, ASM and TMOS protect data on the application delivery network as it is communicated to the user and other service architectures. ASM and TMOS with iRules can scan, inspect, manage, and control both incoming and outgoing data, in messaging requests such as headers (meta-data), cookies, and POST data, and in message responses in meta-data and in the response payload. FirePass, ASM, and TMOS all work together to create a secure, role-based, data access path, prohibiting malicious users from bypassing role (user, group, and networking) restrictions and accessing unauthorized data.



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

**Description from PCI** - 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.

**Solution** - F5's entire product suite addresses the issue of unique user identification and management. For identification, FirePass, TMOS, and ASM all work on the user session level, managing a single user session throughout the duration of the access session. This is done using various tools, such as secure cookies, session IDs, and flow-based policies. For authentication, the BIG-IP, TMOS, and FirePass integrate 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 (e.g. Siteminder) and Windows Domain Servers, as well as supporting programmatic user authentication via as secure keys, smart cards, and client SSL certificates, allowing near-infinite authentication combinations across public and enterprise credential services. Transport security is accomplished through SSL. The BIG-IP and TMOS can offload SSL from both the FirePass and back-end application servers, providing data security and network flexibility. TMOS is a full SSL proxy, allowing ASM to inspect and protect data passed to the application via SSL, and then re-encrypting the data for secure delivery to the application or back to the end-user.

## **E: Regularly Monitor and Test Networks**

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

**Description from PCI** - Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

**Solution** - F5 Networks offers a suite of products that are session-based, not packet based. With this full reverse proxy architecture, BIG-IP, TMOS, ASM, iRules, and FirePass all have the ability to manage full user sessions, regardless of the transport mechanism or network, and match those user sessions to specific data actions, providing a full audit trail from the user to the data. This allows F5 application security devices to provide data confidentiality, integrity, and availability to all application data on the network. The ability to monitor and log all user sessions and access requests to sensitive information, such as cardholder data and Social Security numbers is critical to any security environment. All F5 products support remote logging, allowing logs to be pushed to secure networks and devices for archiving. In addition, TMOS 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 24x7 without impacting network performance is a core function and the foundation of all of F5's security products.

## **F: Maintain an Information Security Policy**

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

**Description from PCI** - A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.



**Solution** – F5 security appliances are policy-based devices: ASM for application and business logic policies; FirePass for user access and control policies; iRules for applying policies to network traffic and to back-end application services. This policy-based approach provides F5 delivery controllers the means to match applied security policy to a functional business policy. With both a proactive approach (ASM and a positive security policy, iRules for signature- and action-based security, FirePass for secure access) and a re-active approach (ASM and TMOS triggers when a breach is detected, FirePass remediation when a users' secure state changes to an insecure state), F5 can act as an enabler in helping roll out business policies and security policies together. Applications don't have to be built and deployed in a vacuum; F5 Networks technologies can be implemented in conjunction with corporate policies that address information security.

**About F5** F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's extensible architecture intelligently integrates application optimization, protects the application and the network, and delivers application reliability. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to [www.f5.com](http://www.f5.com).