STORMSHIELD

WHITE PAPER

Stormshield Network Firewall

Stormshield Network Firewall & PCI DSS

Document version: 3.0 (September 2015)

Version of Stormshield firewalls: 1 & 2

Introduction

Are Stormshield Network Security products compatible with PCI DSS?

We have often been asked this question. Unfortunately, even the best firewalls are only part of the PCI DSS certification process.

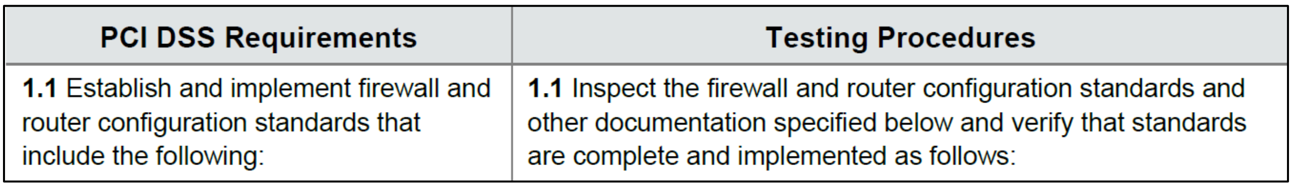
This document lists some of the PCI DSS 3.1 requirements (April 2015) and indicates how Stormshield responds to them in order to help companies that seek to comply with this standard. While this document is probably not exhaustive, it highlights the important role that Stormshield Network Security products may play in a corporation that wishes to obtain PCI DSS certification.

IMPORTANT NOTE

The contents, taken from https://www.pcisecuritystandards.org/ remain the property of their owner.

PCI DSS - Condition 1

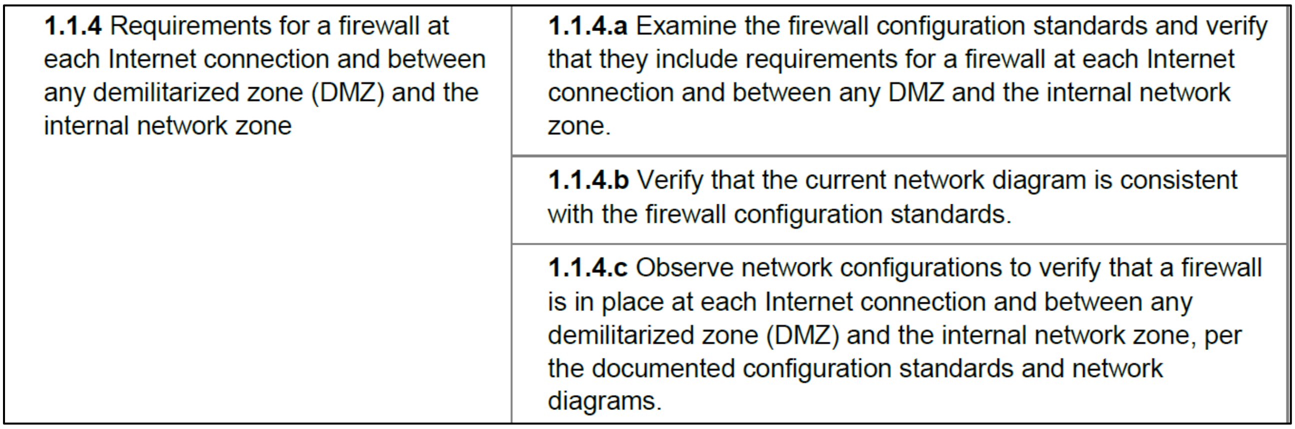
1.1 A firewall is mandatory



PCI DSS Requirements	Testing Procedures
1.1 Establish and implement firewall and router configuration standards that include the following:	**1.1** Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:

Section 1 specifies that the configuration and network architecture have to be documented.

1.1.4 Network segmentation (DMZ)



1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.4.a** Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.
	1.1.4.b Verify that the current network diagram is consistent with the firewall configuration standards.
	1.1.4.c Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams.

Stormshield makes the creation of a DMZ easier and more legible, thanks to the high number of network ports available on its range of firewalls.

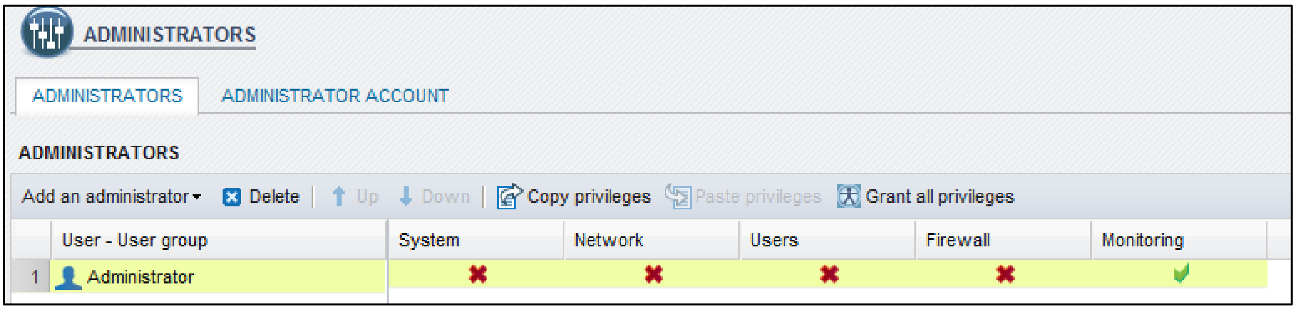
The transparent network bridge feature also allows isolating each of the servers without changing the address range.

The “Internet” network object, only available on Stormshield Network Security appliances, prevents the creation of rules that are too permissive (e.g. destination “all”), which creates unwanted access to the DMZ.

1.1.5 Role-based management

1.1.5 Description of groups, roles, and responsibilities for management of network components	**1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.
	1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.

The Stormshield Network firewall allows the creation of administration profiles, as well as the authentication of users found on the network. It is also possible to create groups, to link the firewall to an external user database, such as an Active Directory and to create a security policy using these users and groups.



	User - User group	System	Network	Users	Firewall	Monitoring
1	Administrator	✗	✗	✗	✗	✓

Defining a Stormshield Network firewall’s administration role

1.1.6 Insecure services

1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.	**1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.
	1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.
	1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.

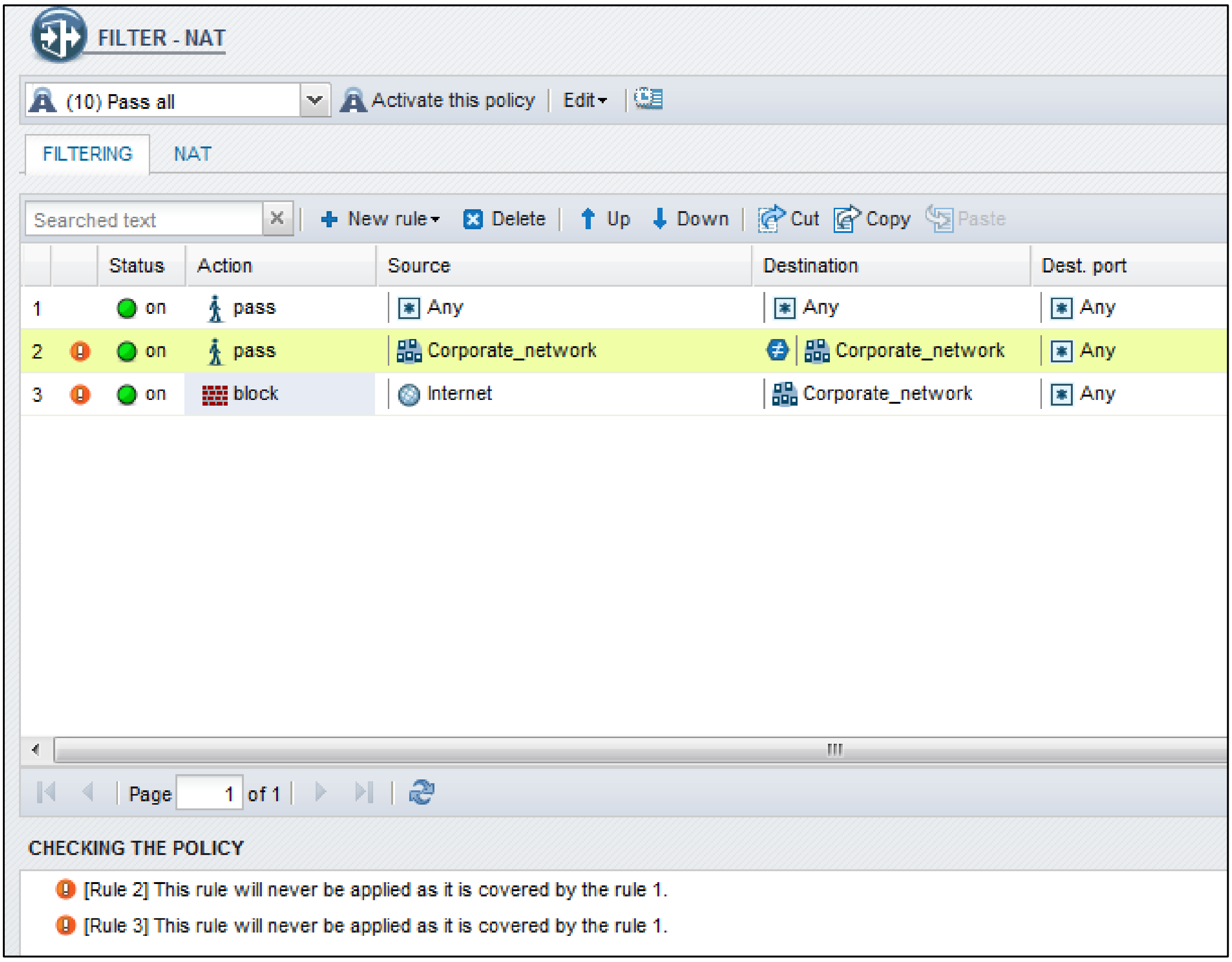
Stormshield Network’s filter policy relies on the use of network objects. Services are therefore defined by using named objects. Insecure services are as such easily identifiable.

1.2 Restriction on connections between zones

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:** An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	**1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment:

Stormshield firewalls use a one-click checkbox to determine if an interface is connected to a protected network or a public network. The security policy is automatically fine-tuned based on this setting.

Stormshield Network Security's real-time filter policy diagnosis tool allows identifying errors in the policy, in particular rules that will never be applied. In this case as well, the Internet object allows defining this zone accurately.



		Status	Action	Source	Destination	Dest. port
1		● on	pass	Any	Any	Any
2	⚠	● on	pass	Corporate_network	Corporate_network	Any
3	⚠	● on	block	Internet	Corporate_network	Any

CHECKING THE POLICY

⚠ [Rule 2] This rule will never be applied as it is covered by the rule 1.

⚠ [Rule 3] This rule will never be applied as it is covered by the rule 1.

Simple example of a real-time diagnosis on a Stormshield Network firewall

1.2.2 Securing the router

1.2.2 Secure and synchronize router configuration files.	**1.2.2.a** Examine router configuration files to verify they are secured from unauthorized access.
	1.2.2.b Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted).

Stormshield firewalls include static and dynamic routing functions. The routing feature is more secure, as it benefits from SNS products' protection methods, unlike an independent router that would be placed in front of the firewall.

1.2.3 Segmenting wireless networks

1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	**1.2.3.a** Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment.
	1.2.3.b Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

Stormshield simplifies the creation of a wireless network, making it more legible thanks to the high number of network ports available on its firewall range.

Likewise, the transparent network port (bridge) feature allows isolating each server without modifying the address range.

The "Internet" network object, available only on Stormshield Network Security appliances, prevents the creation of rules that are too permissive (destination "any") and which enable unwanted access to or from the wireless network.

1.3 – 1.3.5 Securing cardholder data

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment**.**	**1.3** Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment:

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	**1.3.1** Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	**1.3.2** Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.

1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	**1.3.3** Examine firewall and router configurations to verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.

1.3.4 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	**1.3.4** Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ**.**

1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	**1.3.5** Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.

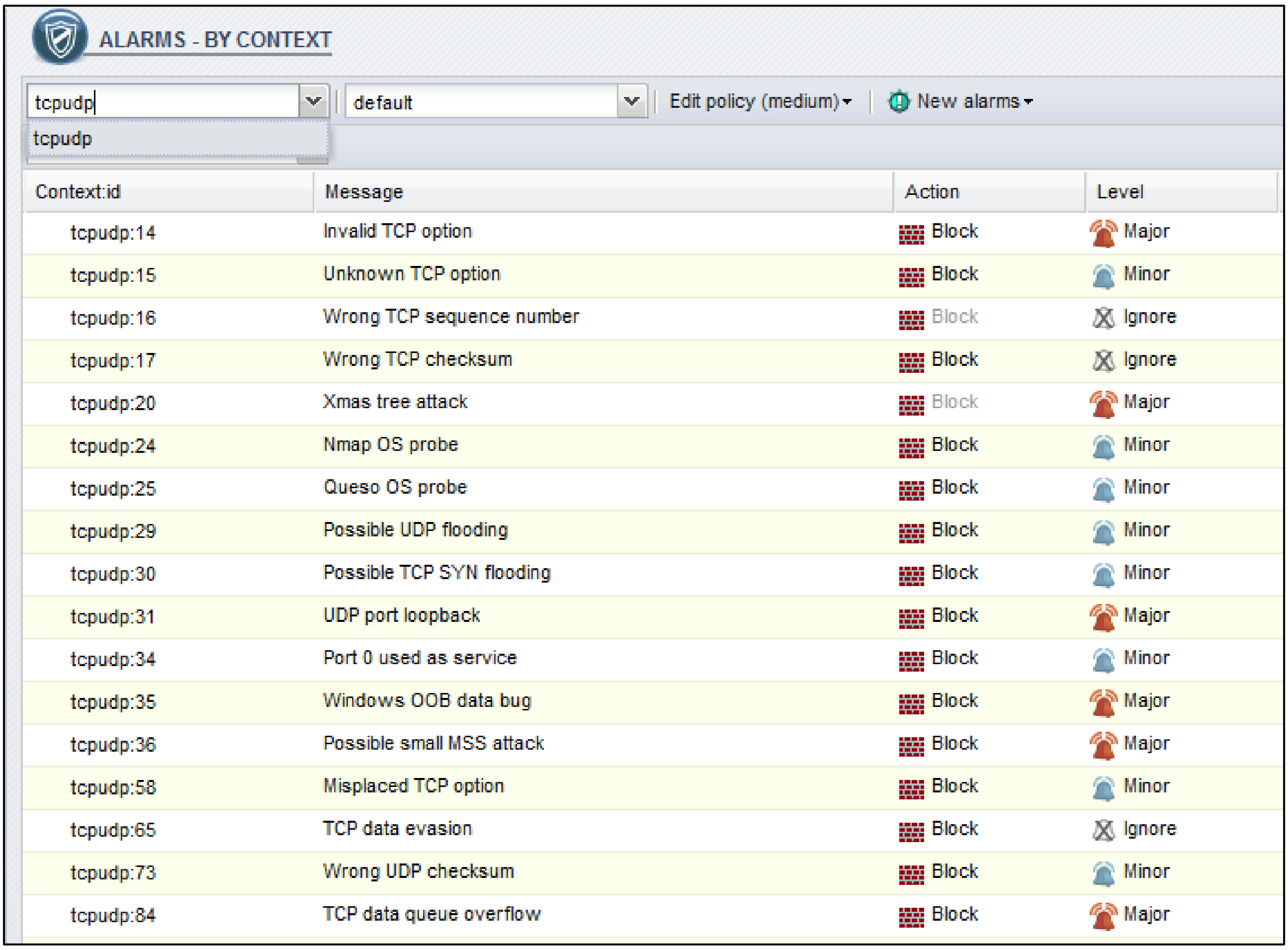
This section sets out the expectations in terms of data security in the DMZ. The SNS firewall can help in several ways:

- **Network segmentation:** the server that holds the data can be on an independent port
- **Filter policy:** access to the data server is restricted
- **Traffic inspection:** Stormshield Network Security's various application traffic inspection technologies guarantee the airtightness of the DMZ. One notable example is protection from IP address spoofing, which is enabled on Stormshield firewalls by default.
- **Intuitive configuration:** Stormshield embeds an Internet object, which conveniently replace the inappropriate use of "any" as a source or a destination for the traffic.

1.3.6 Stateful inspection

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	**1.3.6** Examine firewall and router configurations to verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)

The stateful inspection of TCP/IP connections is a basic function on Stormshield firewalls. Indeed, it is an integral part of the application inspection, up to layer 7 of the OSI model.



Context:id	Message	Action	Level
tcpudp:14	Invalid TCP option	Block	Major
tcpudp:15	Unknown TCP option	Block	Minor
tcpudp:16	Wrong TCP sequence number	Block	Ignore
tcpudp:17	Wrong TCP checksum	Block	Ignore
tcpudp:20	Xmas tree attack	Block	Major
tcpudp:24	Nmap OS probe	Block	Minor
tcpudp:25	Queso OS probe	Block	Minor
tcpudp:29	Possible UDP flooding	Block	Minor
tcpudp:30	Possible TCP SYN flooding	Block	Minor
tcpudp:31	UDP port loopback	Block	Major
tcpudp:34	Port 0 used as service	Block	Minor
tcpudp:35	Windows OOB data bug	Block	Major
tcpudp:36	Possible small MSS attack	Block	Major
tcpudp:58	Misplaced TCP option	Block	Minor
tcpudp:65	TCP data evasion	Block	Ignore
tcpudp:73	Wrong UDP checksum	Block	Minor
tcpudp:84	TCP data queue overflow	Block	Major

Examples of alarms in the TCP/IP connection tracking module

1.3.8 Confidentiality of private IP addresses

1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	**1.3.8.a** Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.
	1.3.8.b Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized.

Stormshield firewalls embed a full IP address translation engine. The translation engine (NAT) is embedded in the traffic inspection engine, which guarantees that traffic is scanned, regardless of the translation operation performed.

PCI DSS – Condition 2

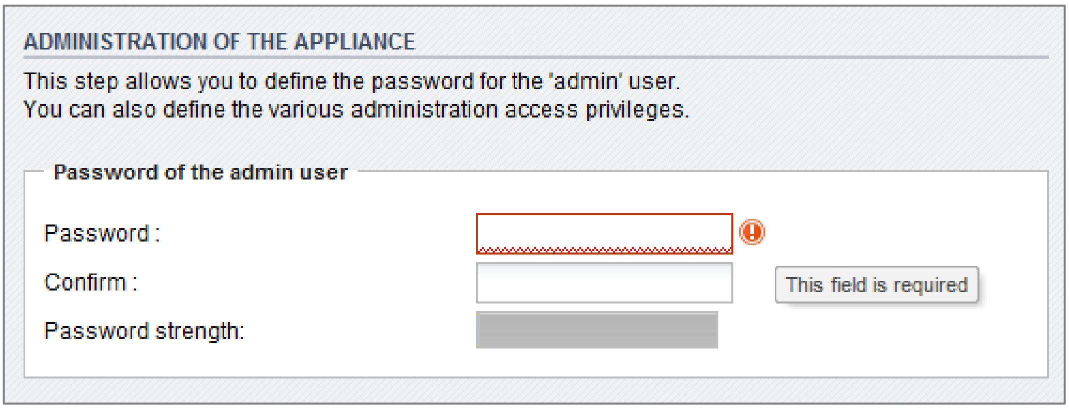
2.1 Default passwords

1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)	**1.3.6** Examine firewall and router configurations to verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)

2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, *point-of-sale (POS)* terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	**2.1.a** Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)

Stormshield firewalls embed several authentication methods, including the certificate method, in order to offer alternatives to the default password.

The wizard in the initial installation of a Stormshield Network Security firewall contains a step in which the default password is changed. This step is mandatory.



ADMINISTRATION OF THE APPLIANCE

This step allows you to define the password for the 'admin' user.
You can also define the various administration access privileges.

Password of the admin user

Password :

Confirm :

Password strength:

This field is required

Stormshield Network Security installation wizard: mandatory modification of the password

2.2.1 DMZ and virtual servers

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:** Where virtualization technologies are in use, implement only one primary function per virtual system component.*	**2.2.1.a** Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server.
	2.2.1.b If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device.

The Stormshield firewall range exists in virtual image format. Even though it cannot replace the step above, it can complement it. A virtual Stormshield firewall allows going one step further by segmenting virtual servers within the same physical server.

2.2.2 Services open on servers

2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	**2.2.2.a** Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled.
	2.2.2.b Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards.

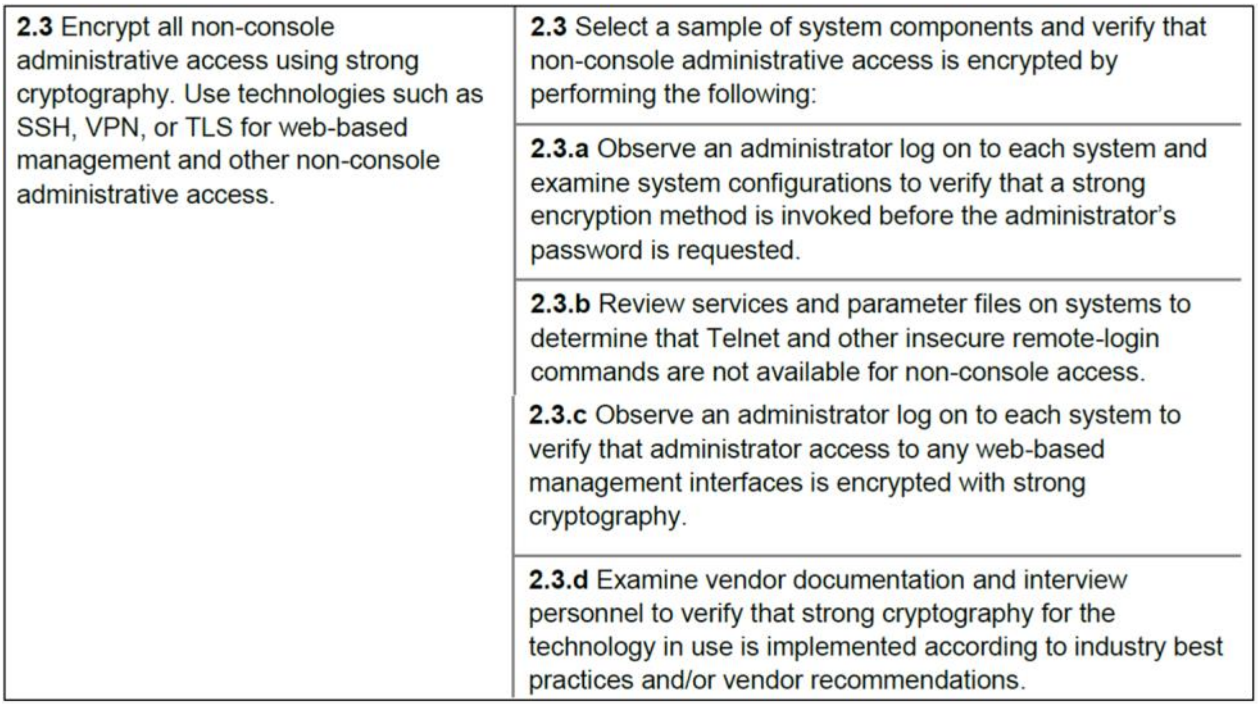
Stormshield firewalls allow identifying insecure services used by sensitive servers. The product Stormshield Network Vulnerability Manager helps the security manager to keep track of unwanted services.

2.2.4 Enable security parameters

2.2.4 Configure system security parameters to prevent misuse.	**2.2.4.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.
	2.2.4.b Examine the system configuration standards to verify that common security parameter settings are included.
	2.2.4.c Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.

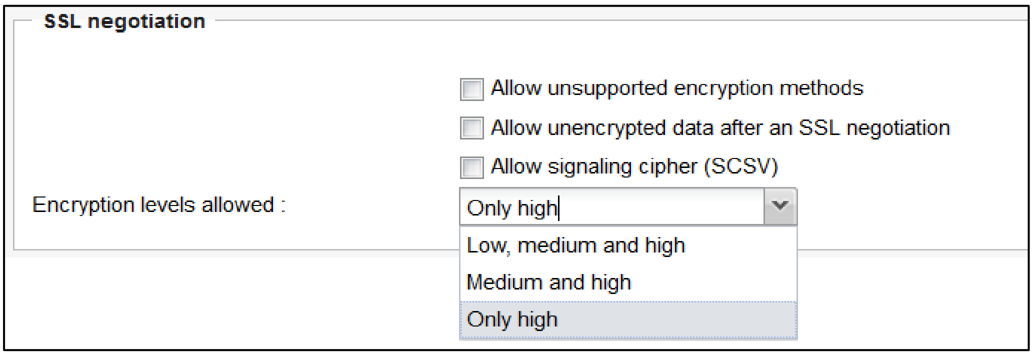
All Stormshield Network Security products include a system that protects against malicious acts. These components are enabled by default to guarantee an optimum level of security.

2.3 Encryption of administrative access



2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.	**2.3** Select a sample of system components and verify that non-console administrative access is encrypted by performing the following:
	2.3.a Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.
	2.3.b Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.
	2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.
	2.3.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.

The Stormshield Network Security application protection engine allows guaranteeing a minimum encryption level for an SSL connection. It also allows preventing any interactive connections on unencrypted protocols.



SSL negotiation

□ Allow unsupported encryption methods

□ Allow unencrypted data after an SSL negotiation

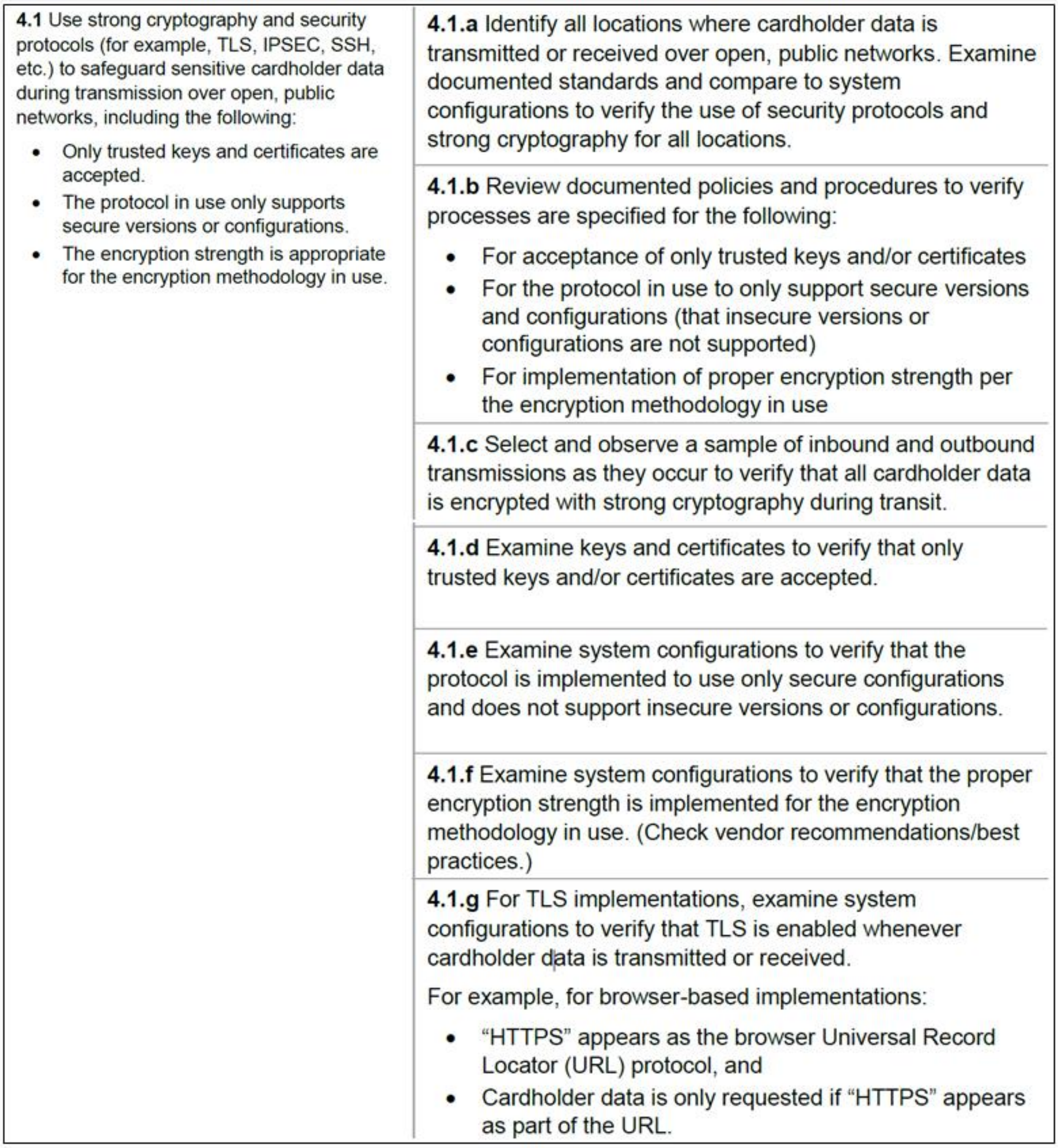
□ Allow signaling cipher (SCSV)

Encryption levels allowed : Only high

SSL protocol: allowing only strong encryption

PCI DSS – Condition 4

4.1 Encrypt the transmission of sensitive data



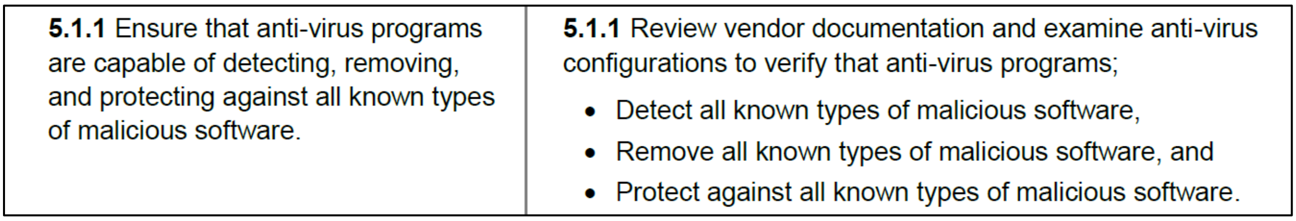
4.1 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	**4.1.a** Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.
	4.1.b Review documented policies and procedures to verify processes are specified for the following: • For acceptance of only trusted keys and/or certificates • For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported) • For implementation of proper encryption strength per the encryption methodology in use
	4.1.c Select and observe a sample of inbound and outbound transmissions as they occur to verify that all cardholder data is encrypted with strong cryptography during transit.
	4.1.d Examine keys and certificates to verify that only trusted keys and/or certificates are accepted.
	4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.
	4.1.f Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)
	4.1.g For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received. For example, for browser-based implementations: • "HTTPS" appears as the browser Universal Record Locator (URL) protocol, and • Cardholder data is only requested if "HTTPS" appears as part of the URL.

In addition to the restrictive function of strong encryption in SSL (cf. 4.1.d), Stormshield firewalls have an SSL traffic inspection feature in order to guarantee security. For example, it is possible to set up an alarm that would be triggered in case of clear text SSL traffic (sort of debug mode for SSL traffic). The Stormshield firewall can also play the role of an IPSec VPN tunnel endpoint, and of a PKI for certificates.

As for the vulnerability management feature, it indicates possible flaws in public servers, especially in the case of a flaw during the implementation of the encrypted protocol.

PCI DSS – Condition 5

5.1.1 Guarantee the detection of malicious software



5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	**5.1.1** Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs; • Detect all known types of malicious software, • Remove all known types of malicious software, and • Protect against all known types of malicious software.

This condition targets the antivirus module on client workstations. However, in the way the condition has been phrased, the network antivirus found on Stormshield firewalls may apply. It complements a desktop antivirus and increases the probability of detection of malicious software.

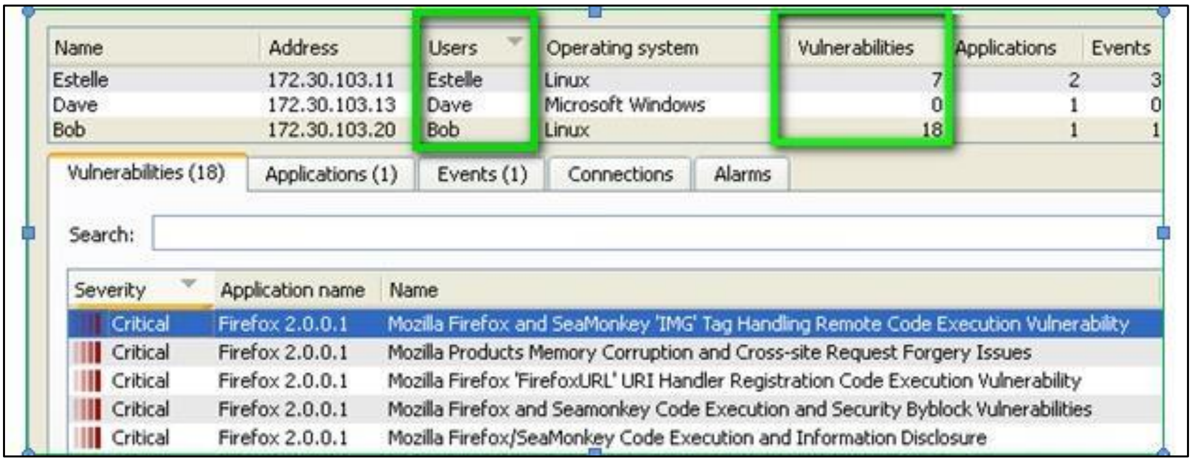
The product Stormshield Network Vulnerability Manager detects attempts to update certain antivirus brands in order to target obsolete installations.

PCI DSS – Condition 6

6.1 Identification of vulnerabilities

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.* *Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*	**6.1.a** Examine policies and procedures to verify that processes are defined for the following: • To identify new security vulnerabilities • To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. • To use reputable outside sources for security vulnerability information.
	6.1.b Interview responsible personnel and observe processes to verify that: • New security vulnerabilities are identified. • A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities. • Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.

The product Stormshield Network Vulnerability Manager helps to automatically and more quickly detect the appearance of new vulnerabilities.



Name	Address	Users	Operating system	Vulnerabilities	Applications	Events
Estelle	172.30.103.11	Estelle	Linux	7	2	3
Dave	172.30.103.13	Dave	Microsoft Windows	0	1	0
Bob	172.30.103.20	Bob	Linux	18	1	1

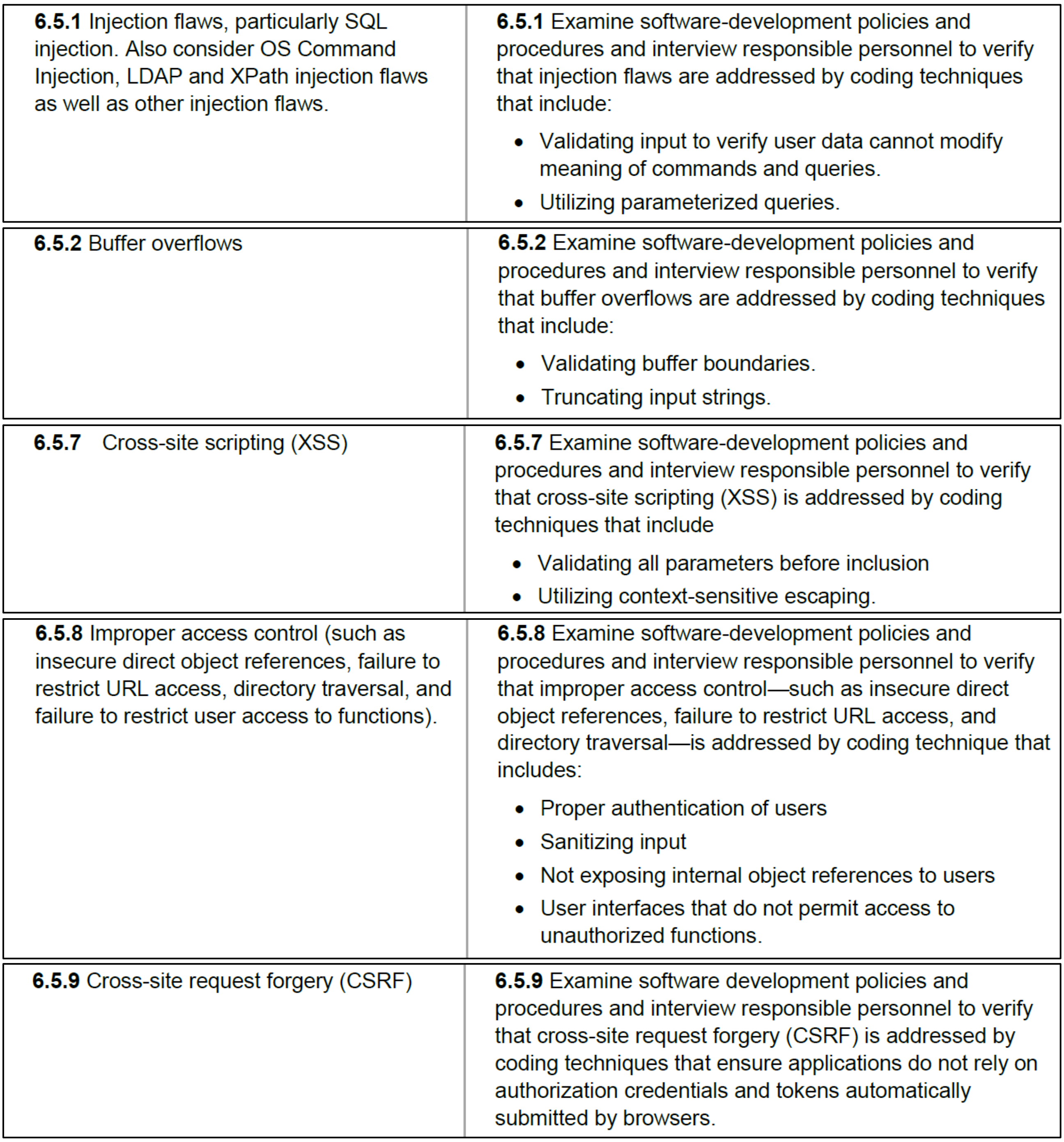
Severity	Application name	Name
Critical	Firefox 2.0.0.1	Mozilla Firefox and SeaMonkey 'IMG' Tag Handling Remote Code Execution Vulnerability
Critical	Firefox 2.0.0.1	Mozilla Products Memory Corruption and Cross-site Request Forgery Issues
Critical	Firefox 2.0.0.1	Mozilla Firefox 'FirefoxURL' URI Handler Registration Code Execution Vulnerability
Critical	Firefox 2.0.0.1	Mozilla Firefox and Seamonkey Code Execution and Security Byblock Vulnerabilities
Critical	Firefox 2.0.0.1	Mozilla Firefox/SeaMonkey Code Execution and Information Disclosure

Example of detected vulnerabilities, sorted by host

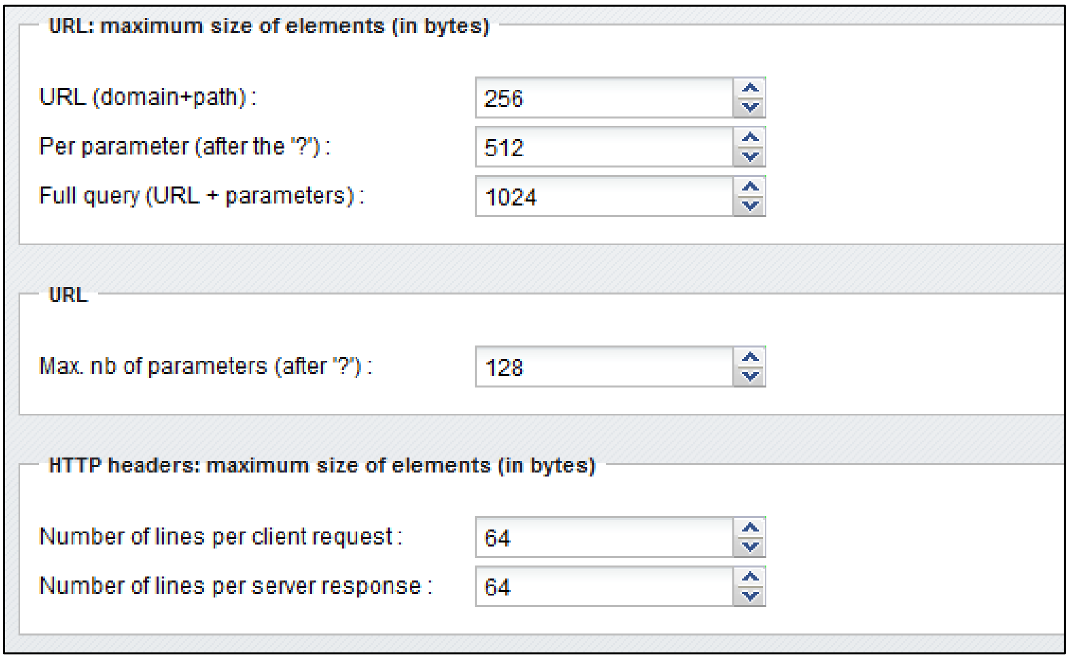
6.5.1 – 6.5.9 Prevent vulnerabilities in applications

This section sets out known vulnerabilities and indicates that the applications developed within the company have to follow development practices in order to prevent the presence of these flaws.

The Stormshield firewall contributes to Condition 6 of “maintaining a secure environment”. For points 6.5.1 to 6.5.9, the firewall can prevent the application attacks mentioned from the network. Here are some of them:



6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	**6.5.1** Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include: • Validating input to verify user data cannot modify meaning of commands and queries. • Utilizing parameterized queries.
6.5.2 Buffer overflows	**6.5.2** Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include: • Validating buffer boundaries. • Truncating input strings.
6.5.7 Cross-site scripting (XSS)	**6.5.7** Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include • Validating all parameters before inclusion • Utilizing context-sensitive escaping.
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	**6.5.8** Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that includes: • Proper authentication of users • Sanitizing input • Not exposing internal object references to users • User interfaces that do not permit access to unauthorized functions.
6.5.9 Cross-site request forgery (CSRF)	**6.5.9** Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.



URL: maximum size of elements (in bytes)

URL (domain+path) : 256

Per parameter (after the '?') : 512

Full query (URL + parameters) : 1024

URL

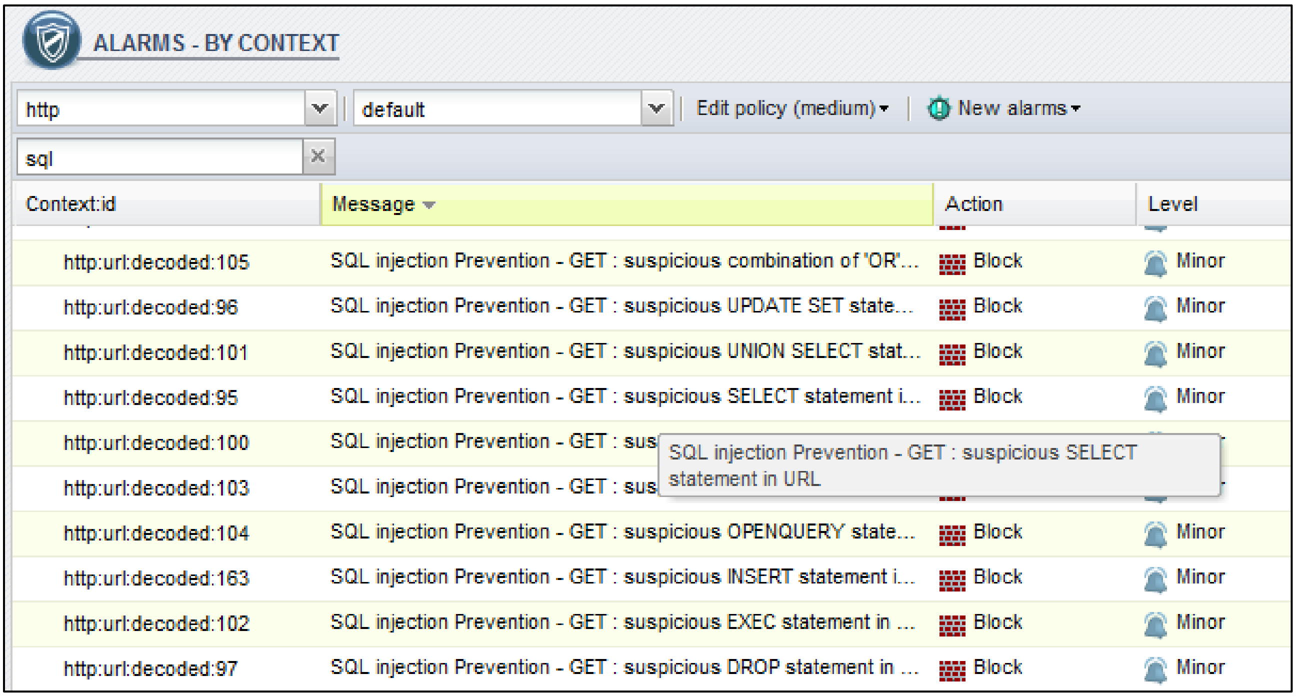
Max. nb of parameters (after '?') : 128

HTTP headers: maximum size of elements (in bytes)

Number of lines per client request : 64

Number of lines per server response : 64

6.5.2: Example of protection from buffer overflow

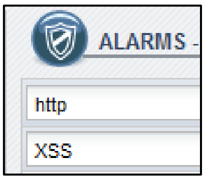


sql

Context:id	Message	Action	Level
http:url:decoded:105	SQL injection Prevention - GET : suspicious combination of 'OR'...	Block	Minor
http:url:decoded:96	SQL injection Prevention - GET : suspicious UPDATE SET state...	Block	Minor
http:url:decoded:101	SQL injection Prevention - GET : suspicious UNION SELECT stat...	Block	Minor
http:url:decoded:95	SQL injection Prevention - GET : suspicious SELECT statement i...	Block	Minor
http:url:decoded:100	SQL injection Prevention - GET : sus		
http:url:decoded:103	SQL injection Prevention - GET : sus		
http:url:decoded:104	SQL injection Prevention - GET : suspicious OPENQUERY state...	Block	Minor
http:url:decoded:163	SQL injection Prevention - GET : suspicious INSERT statement i...	Block	Minor
http:url:decoded:102	SQL injection Prevention - GET : suspicious EXEC statement in ...	Block	Minor
http:url:decoded:97	SQL injection Prevention - GET : suspicious DROP statement in ...	Block	Minor

SQL injection Prevention - GET : suspicious SELECT statement in URL

6.5.1: Example of protection from SQL injections

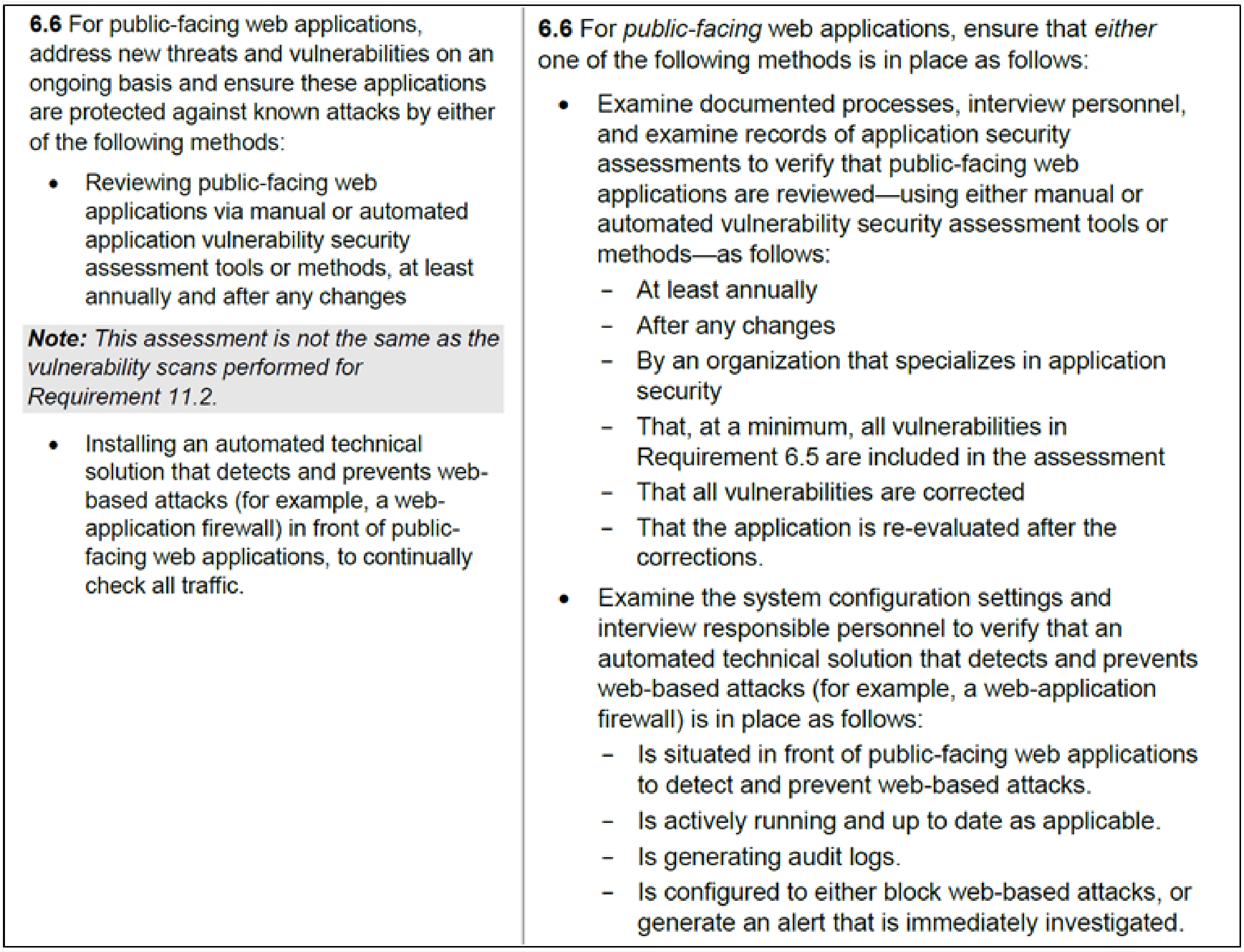


http

XSS

6.5.7: Example of protection from XSS attacks

6.6 Protection of public websites



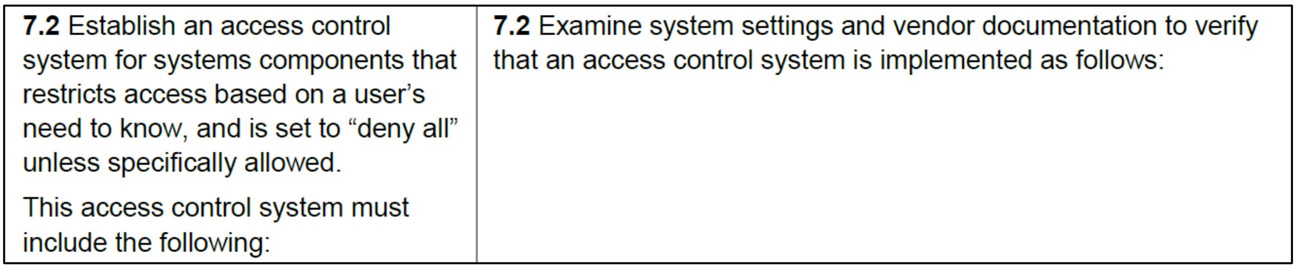
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	**6.6** For *public-facing* web applications, ensure that *either* one of the following methods is in place as follows: • Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: – At least annually – After any changes – By an organization that specializes in application security – That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment – That all vulnerabilities are corrected – That the application is re-evaluated after the corrections. • Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: – Is situated in front of public-facing web applications to detect and prevent web-based attacks. – Is actively running and up to date as applicable. – Is generating audit logs. – Is configured to either block web-based attacks, or generate an alert that is immediately investigated.

The Stormshield firewall has many web traffic scans, in particular a unique web application inspection engine. It can therefore act as a web firewall to protect public websites.

As a complement, vulnerabilities on these web servers are detected by the vulnerability management module.

PCI DSS – Condition 7

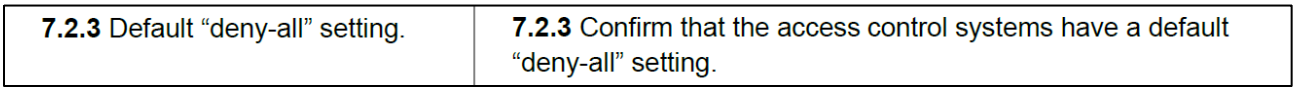
7.2 Control user access



7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented as follows:

The Stormshield firewall allows creating access rules according to users and user groups.

7.2.3 Block by default



7.2.3 Default "deny-all" setting.	**7.2.3** Confirm that the access control systems have a default "deny-all" setting.

Without an explicit "pass" rule, the Stormshield firewall operates in "block" mode. Furthermore, unlike many other solutions, the traffic inspection engine (IPS) is enabled by default on Stormshield Network firewalls.

PCI DSS – Condition 8

8.1.1 Authenticate users

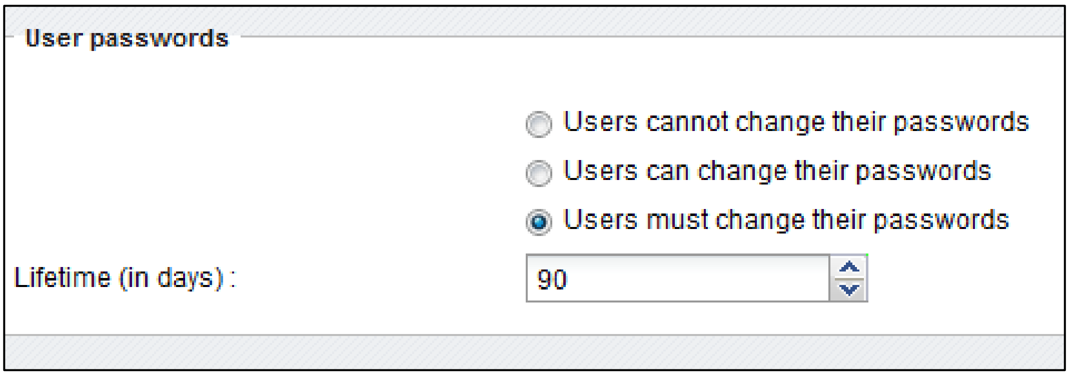
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**8.1.1** Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data.

The Stormshield firewall allows creating access rules according to users and user groups.

8.2.4 User passwords

8.2.4 Change user passwords/passphrases at least once every 90 days.	**8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least once every 90 days.
	8.2.4.b ***Additional testing procedure for service provider assessments only****: Review internal* processes and customer/user documentation to verify that: • Non-consumer customer user passwords are required to change periodically; and • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change.

Stormshield firewalls allow imposing the change of passwords for network users.



User passwords

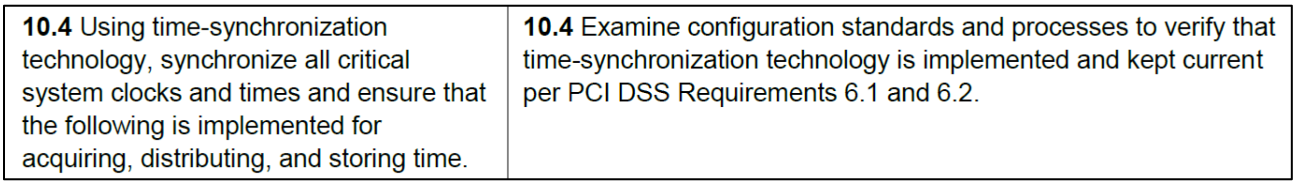
○ Users cannot change their passwords
○ Users can change their passwords
● Users must change their passwords

Lifetime (in days) : 90

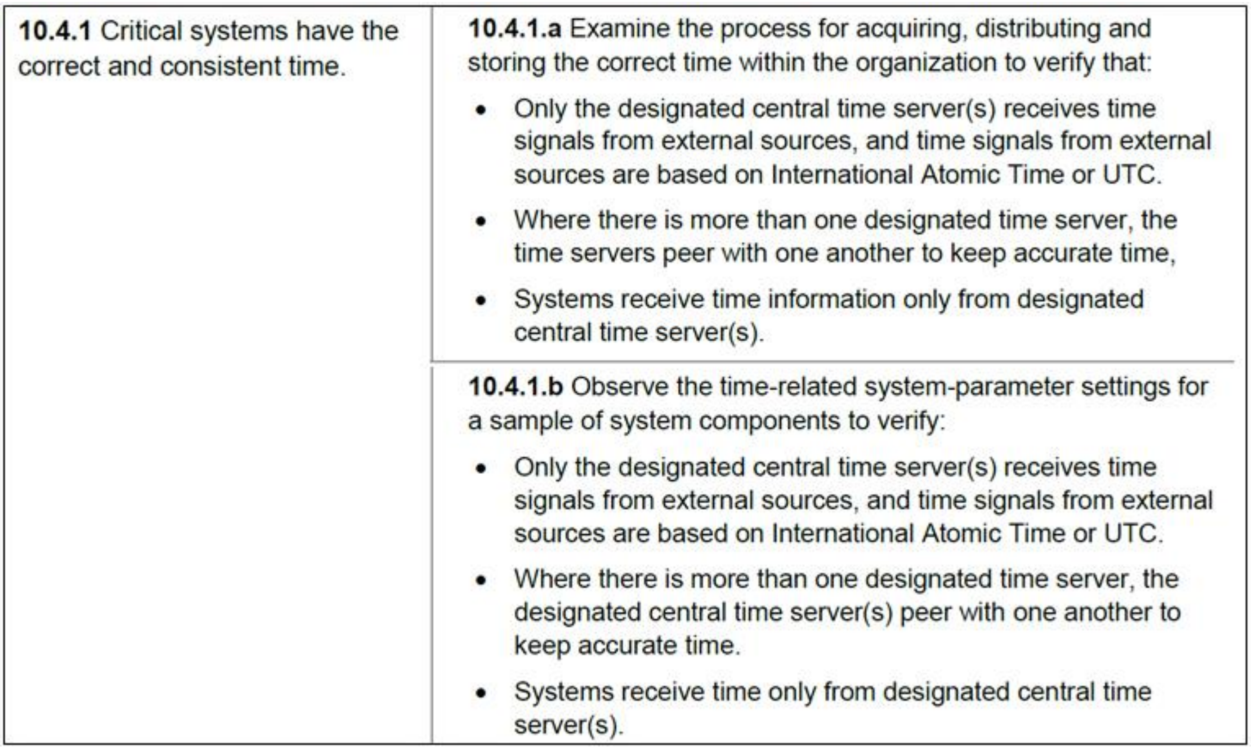
Imposing a change of passwords every 90 days

PCI DSS – Condition 10

10.4 Synchronize clocks



10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	**10.4** Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.

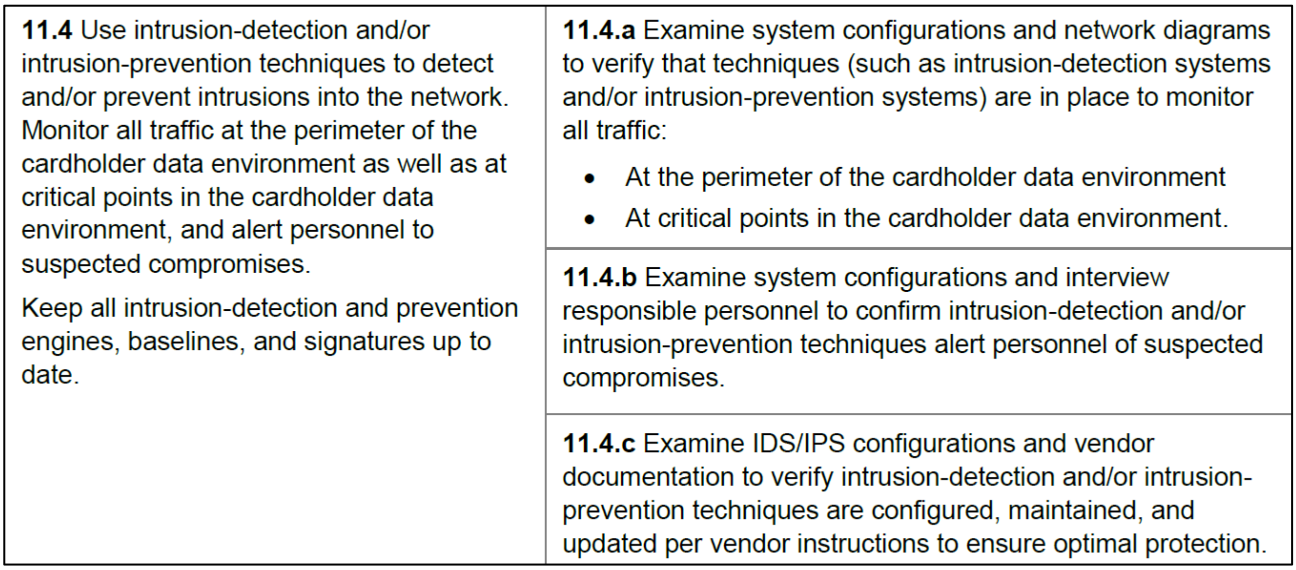


10.4.1 Critical systems have the correct and consistent time.	**10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that: • Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time, • Systems receive time information only from designated central time server(s).
	10.4.1.b Observe the time-related system-parameter settings for a sample of system components to verify: • Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. • Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. • Systems receive time only from designated central time server(s).

Stormshield firewalls embed an NTP client that allows synchronizing the firewall's clock in order to guarantee the validity of dates, especially those in log files.

PCI DSS – Condition 11

11.4 Use an intrusion prevention system (IPS)



11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	**11.4.a** Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic: • At the perimeter of the cardholder data environment • At critical points in the cardholder data environment.
	11.4.b Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.
	11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.

The intrusion prevention engine is at the core of the system on Stormshield Network Security products. It is embedded in the operating system and combines several cutting-edge technologies. The intrusion prevention engine is enabled in factory settings, unlike on many other solutions. This automatic configuration, adapted to the nature of the traffic (outgoing and incoming profiles), significantly increases the chances of the IPS' operation.

The IPS engine is automatically updated from dynamic Stormshield update servers.

Conclusion

All throughout this document, we covered features on Stormshield firewalls that make it easier to obtain PCI DSS certification. This list is not exhaustive, but is a good indicator of the immediate benefits of using a Stormshield Network Security firewall for companies that wish to commence steps to obtaining PCI DSS certification.