algosec

Secure application connectivity.
Anywhere.

Whitepaper

PCI-DSS v4.0

Automating audits and ensuring continuous compliance with AlgoSec

Version 01
January 2026

Revision History

Version	Date	Changes	Author/Editor	Approved By
1	29-Apr-26	Initial document	TD	ES

Contents

1. Simplifying PCI-DSS Audits & Ensuring Continuous Compliance with AlgoSec

PCI-DSS is a multi-faceted security standard created by the Payment Card Industry Data Security Standard (PCI-DSS) Council and designed to help organizations proactively protect customer account data. The PCI Data Security requirements apply to all members, merchants, and service providers that store, process or transmit cardholder data. The requirements also apply to all system components which are defined as any network component, server, or application included in, or connected to, the cardholder data environment. The payment brands may, at their discretion, fine an acquiring bank $5,000 to $500,000 per month for PCI compliance violations.

PCI-DSS directly impacts an organization's network security architecture and policies for firewalls, routers, and related security infrastructure, and validating the compliance of corporate firewalls and routers with PCI-DSS requirements is not an easy task. An audit typically involves a manual process of checking each element against the relevant PCI-DSS requirement and determining if it complies. For items that do not comply with the requirements, the auditor would then suggest a remedy, follow up on the correction process and validate that the fix was implemented according to the requirement. This process requires lengthy manual operations that consume considerable time, costs and resources, and are prone to human error.

AlgoSec provides security teams and auditors with an out-of-the-box PCI-DSS compliance report on firewalls and routers that substantially reduces the time to conduct an audit of the network security policy – by as much as 80%. AlgoSec's PCI-DSS Compliance Report pulls directly from the Payment Card Industry (PCI) Data Security Standard and contains the seven requirements that are relevant to policy management of firewalls and routers. Reports can be automatically generated per device or a specified group of devices in a single report.

AlgoSec provides immediate visibility into the organization's compliance status, highlights gaps and risks and provides recommendations for remediation, which can be automatically implemented directly through the AlgoSec security management solution. Some key benefits include:

- Reduce audit preparation time and costs by as much as 80%: Automatically generate PCI reports with the "push of a button", even across a group of devices to further save time from having to collate reports per device.
- Ensure accuracy of audits: PCI-DSS requirements are systematically compared to the network security infrastructure, providing an accurate picture of your compliance status.
- Quickly address compliance gaps with actionable recommendations: Pinpoint areas of non-compliance with steps for remediation
- Ensure continuous compliance: Automatically run PCI-DSS risk and compliance checks on every change in the security change management workflow before changes are processed.

Requirement 1: Install and maintain Network Security Controls

PCI-DSS Requirement 1 covers many aspects of security policy management. AlgoSec supports this requirement by:

- Identifying all PCI-DSS related risks
- Tracking every security policy change with customizable alerts
- Generating a current and interactive network topology map
- Automatically analyzing firewall configurations at designated intervals
- And much more

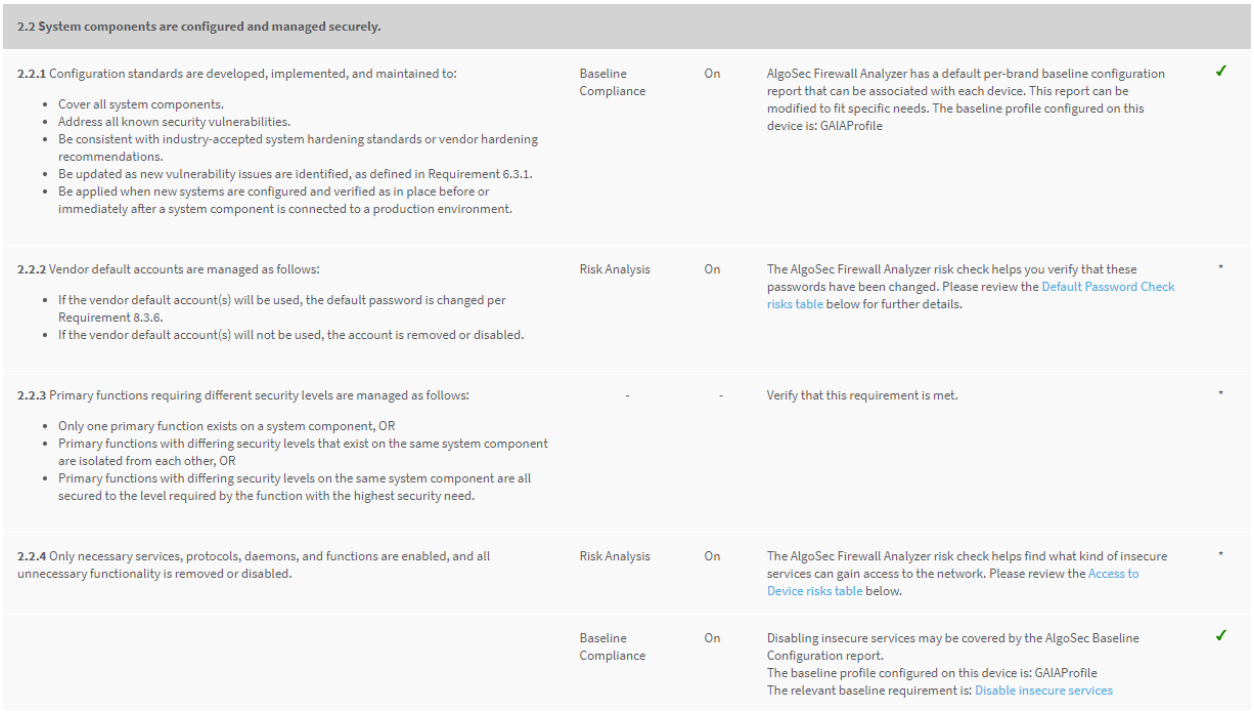
PCI DSS Requirements	AlgoSec Feature	Setting	Details	Status
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.				
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	-	-	Please make sure that all the security polices and procedures are documented, updated, in use and shared with the relevant parties.	
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	AlgoSec Administrators	On	The following users have administration permissions on the AlgoSec Firewall Analyzer: AlgoSec Administrator algobotalgosec demo Ned NetOps	*
	Users	On	The AlgoSec Firewall Analyzer allows user management that specifies access per user and per feature. The following user names are defined on AlgoSec Firewall Analyzer and have access to DaffodilCheckpointGW-2: AlgoSec Administrator (Standard) Sue Security (Standard) algobotalgosec (Standard) demo (Standard) Ned NetOps (Standard) harry helpdesk (Read only)	*
1.2 Network security controls (NSCs) are configured and maintained.				
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	Risk Analysis	On	The AlgoSec Risk Analysis mechanism is the configurations standards for the NSC rulesets.	✓
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	FireFlow	On	The AlgoSec FireFlow product performs a "what-if" risk check on every change request (prior to implementation). To learn more about AlgoSec FireFlow please visit the AlgoSec web site, or contact your AlgoSec representative. Algosec FireFlow is licensed in your environment.	✓
	ActiveChange	On	The AlgoSec ActiveChange technology can be used in order to changes firewall configuration. Algosec ActiveChange feature is licensed in your environment.	✓
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	Connectivity Diagram	On	 The connectivity diagram is current as of 2024-01-25	✓
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.	AppViz	On	AlgoSec AppViz includes a data-flow diagram for all applications under management.	✓
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.	Allowed Services	On	Click here to view the list of open services from Outside and DMZs to Inside, and from Inside and DMZs to Outside.	*
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	Risk Analysis	On	Risks found: 1 high risks, 3 suspected high risks, 10 medium risks, 2 low risks Please review the Offline Security Scan results at the bottom for details. For details regarding the controls used in conjunction with the risk profile see the Risk Assessment Criteria at the bottom.	✗
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	Scheduled Analysis	Off	The AlgoSec Firewall Analyzer conducts analysis that includes testing of different firewall performances. The audit is scheduled	✗
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	Access Control	On	The AlgoSec Firewall Analyzer access controls provide access to the AlgoSec reports only to authorized staff members, at a per-person per-firewall access granularity. Access to the AlgoSec system is only possible over an encrypted HTTPS connection. Administration access to the AlgoSec server is possible only via an encrypted SSH connection. This sensitive information is protected during transit. AlgoSec Uses TLSv1.2 to protect communication in and out of the AlgoSec system. AlgoSec recommends customers install a properly signed certificate on the AlgoSec System to comply with this requirement. The instructions on how to generate CSR and install the certificate are here.	✓

1.3 Network access to and from the cardholder data environment is restricted.				
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	Allowed Services	On	Click here to view the list of open services from Outside to Inside and from Outside to DMZs.	*
	-	-	An implicit final "drop rule" is the default behavior for Check Point R80.40	✓
1.3.2 Outbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	Allowed Services	On	Click here to view the list of open services from Inside to Outside and from DMZs to Outside.	*
	-	-	An implicit final "drop rule" is the default behavior for Check Point R80.40	✓
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • All wireless traffic from wireless networks into the CDE is denied by default.	-	-	Verify that this requirement is met.	*
1.4 Network connections between trusted and untrusted networks are controlled.				
1.4.1 NSCs are implemented between trusted and untrusted networks.	-	DaffodilCheckpointGW-2	Device TrafficLogsGW_2 is a firewall.	✓
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.	Customize Topology	DMZs not marked	-	*
	-	-	Check Point R80.40 is a stateful firewall	✓
	-	-	An implicit final "drop rule" is the default behavior for Check Point R80.40	✓
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	Anti Spoofing	-	Firewalls can provide Anti-Spoofing protection if configured to do so: Anti Spoofing is not configured on TrafficLogsGW_2	✗
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.	PCI Zone	On	Defined PCI Zone: 192.168.11.09-192.168.11.150 64.46.192.1 16.47.71.61-16.47.76.13 100.77.28.115 144.101.125.1-144.101.251.6	✓
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	-	-	Number of routable (non-RFC1918) IP addresses in the Inside: 512 Number of routable (non-RFC1918) IP addresses in the DMZs: 0	*
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.				
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entityâ⊠⊠s network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	-	DaffodilCheckpointGW-2	Device TrafficLogsGW_2 is a firewall. The AlgoSec Firewall Analyzer access controls provide access to the AlgoSec reports only to authorized staff members, at a per-person per-firewall access granularity. Access to the AlgoSec system is only possible over an encrypted HTTPS connection. Administration access to the AlgoSec server is possible only via an encrypted SSH connection. This sensitive information is protected during transit.	✓

Requirement 2: Apply Secure Configurations to All System Components

AlgoSec's PCI-DSS report addresses requirement 2 through risk analysis and baseline compliance checks which provide critical device checks. Specific information contained in the AlgoSec report for this requirement includes:

- Color code of the severity of the risk
- Risk code
- Risk description with a link to the Risk Assessment page of the firewall report that provides a
- detailed explanation of the risk, the rules that contribute to the risk, and the remedy
- Status
- Default password settings



2.2 System components are configured and managed securely.				
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	Baseline Compliance	On	AlgoSec Firewall Analyzer has a default per-brand baseline configuration report that can be associated with each device. This report can be modified to fit specific needs. The baseline profile configured on this device is: GAIAProfile	✓
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	Risk Analysis	On	The AlgoSec Firewall Analyzer risk check helps you verify that these passwords have been changed. Please review the Default Password Check risks table below for further details.	*
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	-	-	Verify that this requirement is met.	*
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	Risk Analysis	On	The AlgoSec Firewall Analyzer risk check helps find what kind of insecure services can gain access to the network. Please review the Access to Device risks table below.	*
	Baseline Compliance	On	Disabling insecure services may be covered by the AlgoSec Baseline Configuration report. The baseline profile configured on this device is: GAIAProfile The relevant baseline requirement is: Disable insecure services	✓

Default Password Risks

The following table lists all the risk items that were searched in order to comply with ASD Security Control 1304 and 1312 .

For each risk item, the Status column indicates one of:
✓ - the risk item **was not** found
✗ - the risk item **was** found
* - Additional information or manual verification is necessary to meet the requirement.

		Code	Risk Description	Status
1.		P22	Local password not set	✓
2.		P23	Enable password not set	✓
3.		P27	Password set to factory default value	✗
4.		P29	Enable password set to factory default value	✓
5.		P32	SNMP community string set to factory default value	✓

Access to Device Risks

The following table lists all the risk items that were searched in order to comply with PCI DSS requirement 2.2.2.
For each risk item, the Status column indicates one of:
✓ - the risk item **was not** found
✗ - the risk item **was** found
* - Additional information or manual verification is necessary to meet the requirement.

		Code	Risk Description	Status
1.		F01	Insecure external access to firewall	✗
2.		F02	Insecure internal access to firewall	✗
3.		F06	Insecure external VPN access to firewall	✓
4.		F07	Insecure internal VPN access to firewall	✓

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

PCI DSS Requirement 4.0 addresses the need to encrypt sensitive information during transmission over networks that are easily accessed by malicious individuals. AlgoSec supports this requirement by performing risk analysis that indicates whether insecure protocols are being used and through VPN analysis to make sure all remote connections are managed correctly. The following table details how AlgoSec assists the organization in meeting this requirement.

4.2 PAN is protected with strong cryptography during transmission.

4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	VPN Analysis	On	See the VPN Analysis report for details regarding remote access rights through firewall DaffodilCheckpointGW-2 ✓

Index

TABLE		DESCRIPTION
VPN Rules	1	VPN rules on firewall Rose_checkpoint
User Groups	0	VPN user groups, linked to their rules
Users	0	VPN user definitions, linked to their groups
Communities	2	VPN communities, linked to member firewalls
Expired Users	0	List of expired users
Users about to expire	0	Users about to expire
Unattached user groups	0	List of user groups which are not contained in any rule
Unattached Users	0	List of users which are not contained in any user group

VPN Rules

RULE	NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION
13	13		Internal_net_10 Internal_Net_233 FW_ILE CheckPoint_R80	FW_ILE GP_ile.vered.net CheckPoint_R80	MyIntranet	http https ftp	Accept

User Groups

GROUP	COMMENTS	USERS	IN GROUPS	VPN RULES

Users

USER	COMMENTS	AUTHENTICATION	GROUPS	EXPIRATION DATE	ENCRYPTION	DATA INTEGRITY

Communities

NAME	COMMENTS	GATEWAYS	IKE ENCRYPTION	IKE INTEGRITY	DATA ENCRYPTION	DATA INTEGRITY	VPN RULES	EXCLUDED SERVICES
MyIntranet			AES-256	SHA1	AES-128	SHA1	13	

Email Configuration Risks

The following table lists all the risk items that were searched in order to comply with PCI DSS requirement 4.2.
For each risk item, the Status column indicates one of:
✓ - the risk item **was not** found
✗ - the risk item **was** found
* - Additional information or manual verification is necessary to meet the requirement.

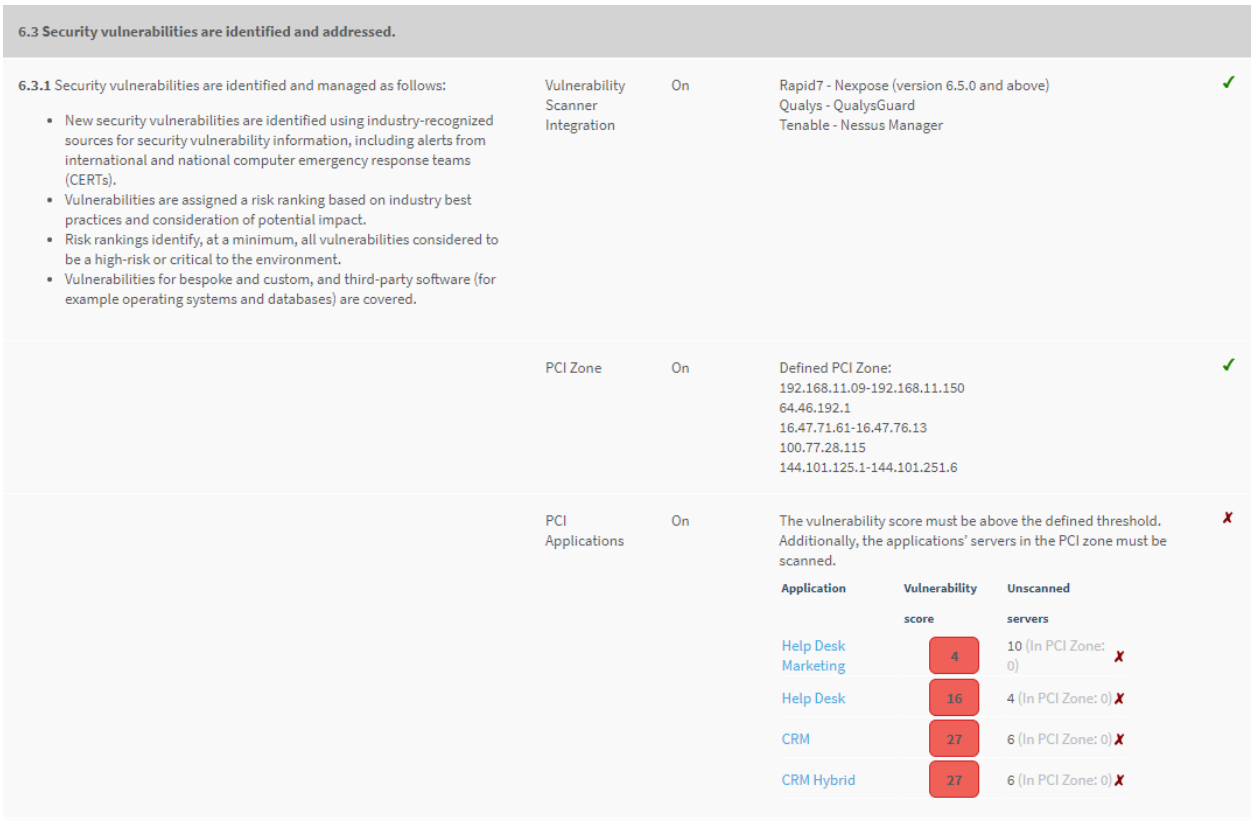
		Code	Risk Description	Status
1.		O01	POP3 can exit your network	✓
2.		P08	Application Intelligence - No POP3/IMAP protection	✓
3.		I09	Over 256 IP addresses can be reached by SMTP	✓

Requirement 6: Develop and maintain secure systems and software.

PCI-DSS Requirement 6.1 requires a process to identify and rank security vulnerabilities. AlgoSec uniquely maps and correlates security vulnerability data to their respective applications and processes within the scope of the PCI DSS audit. This gives users the information they need to focus and proactively prioritize any necessary remediation efforts based on business priorities and audit requirements. This data is presented in AlgoSec's out-of-the-box PCI DSS report, making it easy for organizations to support requirement 6.1 of the PCI DSS v4.0 regulatory standard.

PCI DSS Requirements	AlgoSec Feature	Setting	Details	Status
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.				
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	-	-	Please make sure that all the security polices and procedures are documented, updated, in use and shared with the relevant parties.	
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	AlgoSec Administrators	On	The following users have administration permissions on the AlgoSec Firewall Analyzer: AlgoSec Administrator algobotalgosec demo Ned NetOps	*
	Users	On	The AlgoSec Firewall Analyzer allows user management that specifies access per user and per feature. The following user names are defined on AlgoSec Firewall Analyzer and have access to DaffodilCheckpointGW-2: AlgoSec Administrator (Standard) Sue Security (Standard) algobotalgosec (Standard) demo (Standard) Ned NetOps (Standard) harry helpdesk (Read only)	*

To comply with PCI-DSS Requirement 6.3 merchants and service providers need to ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. AlgoSec helps organizations comply with this requirement by checking that firewalls and routers are running software versions that are still actively supported and maintained by the vendors.



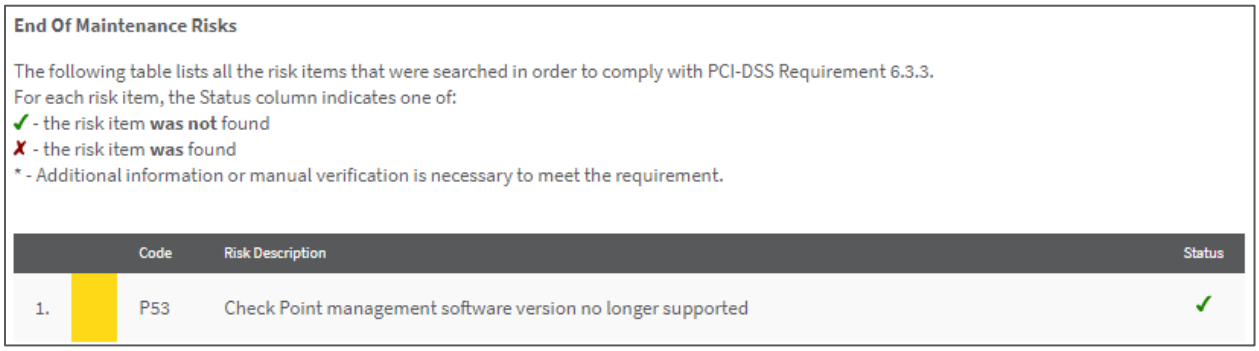
6.3 Security vulnerabilities are identified and addressed.

6.3.1 Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Vulnerability Scanner Integration	On	Rapid7 - Nexpose (version 6.5.0 and above) Qualys - QualysGuard Tenable - Nessus Manager	✓
PCI Zone	On	Defined PCI Zone: 192.168.11.09-192.168.11.150 64.46.192.1 16.47.71.61-16.47.76.13 100.77.28.115 144.101.125.1-144.101.251.6	✓
PCI Applications	On	The vulnerability score must be above the defined threshold. Additionally, the applications' servers in the PCI zone must be scanned.	✗

Application	Vulnerability score	Unscanned servers
Help Desk Marketing	4	10 (In PCI Zone: 0) ✗
Help Desk	16	4 (In PCI Zone: 0) ✗
CRM	27	6 (In PCI Zone: 0) ✗
CRM Hybrid	27	6 (In PCI Zone: 0) ✗



End Of Maintenance Risks

The following table lists all the risk items that were searched in order to comply with PCI-DSS Requirement 6.3.3.
For each risk item, the Status column indicates one of:
✓ - the risk item **was not** found
✗ - the risk item **was** found
* - Additional information or manual verification is necessary to meet the requirement.

		Code	Risk Description	Status
1.		P53	Check Point management software version no longer supported	✓

PCI-DSS 4.0 Section 6.5 focuses on the development and maintenance of secure systems and applications. It mandates Implementation of a robust change management process to ensure any changes to applications do not introduce new vulnerabilities.

AlgoSec aims to ensure that applications are developed and maintained with security as a priority, reducing the risk of vulnerabilities being exploited. AlgoSec achieves this through its FireFlow change management solution and Firewall Analyzer's change history for enhanced visibility.

6.5 Changes to all system components are managed securely.				
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security.	FireFlow	On	The AlgoSec FireFlow product includes change approval steps, validation process and roll back instructions to allow returning to a secure state. To learn more about AlgoSec FireFlow please visit the AlgoSec web site, or contact your AlgoSec representative. Algosec FireFlow is licensed in your environment.	✓
	Change History	On	AlgoSec Change History page provides an independent audit trail for activities on the device. Records available since 2020-08-26	✓
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	FireFlow	On	The AlgoSec FireFlow product includes validation that the requested changes are implemented correctly. To learn more about AlgoSec FireFlow please visit the AlgoSec web site, or contact your AlgoSec representative. Algosec FireFlow is licensed in your environment.	✓

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

AlgoSec provides an immediate view of compliance with PCI-DSS 4.0 Requirement 10 by incorporating the audit logs from the organization's firewalls inside the AlgoSec reports, and by providing an additional annotated log of the changes to the firewalls. The Compliance Report details how AlgoSec assists the organization in meeting this requirement.

PCI DSS Requirements	AlgoSec Feature	Setting	Details	Status
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.				
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	-	-	Please make sure that all the security polices and procedures are documented, updated, in use and shared with the relevant parties.	
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	AlgoSec Administrators	On	The following users have administration permissions on the AlgoSec Firewall Analyzer: AlgoSec Administrator algobotalgosec demo Ned NetOps	*
	Users	On	The AlgoSec Firewall Analyzer allows user management that specifies access per user and per feature. The following user names are defined on AlgoSec Firewall Analyzer and have access to DaffodilCheckpointGW-2: AlgoSec Administrator (Standard) Sue Security (Standard) algobotalgosec (Standard) demo (Standard) Ned NetOps (Standard) harry helpdesk (Read only)	*
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.				
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	Log Collection	Off	Continuous log collection is disabled	✗
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	Change History	On	AlgoSec Change History page provides an independent audit trail for activities on the device. Records available since 2024-01-21	✓
10.3 Audit logs are protected from destruction and unauthorized modifications.				
10.3.1 Read access to audit logs files is limited to those with a job-related need.	AlgoSec Administrators	On	The following users have administration permissions on the AlgoSec Firewall Analyzer: AlgoSec Administrator algobotalgosec demo Ned NetOps	*
	Users	On	The AlgoSec Firewall Analyzer allows user management that specifies access per user and per feature. The following user names are defined on AlgoSec Firewall Analyzer and have access to DaffodilCheckpointGW-2: AlgoSec Administrator (Standard) Sue Security (Standard) algobotalgosec (Standard) demo (Standard) Ned NetOps (Standard) harry helpdesk (Read only)	*
10.3.2 Audit log files are protected to prevent modifications by individuals.	-	-	Accss to AlgoSec system and console is restricted to authorised subjects only.	✓
10.6 Time-synchronization mechanisms support consistent time settings across all systems.				
10.6.1 System clocks and time are synchronized using time-synchronization technology.	Baseline Compliance	Off	NTP server settings may be covered by the AlgoSec Baseline Configuration report. The baseline profile configured on this device is: None	*

Requirement 11: Test Security of Systems and Networks Regularly

To comply with PCI-DSS requirement 11.2, merchants and service providers must have their web sites or IT infrastructures with Internet-facing IP addresses scanned at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). PCI Security Scans are scans conducted over the Internet by an Approved Scanning Vendor (ASV) and AlgoSec provides an offline security scan that supports and complements the ASV's online scan in two ways:

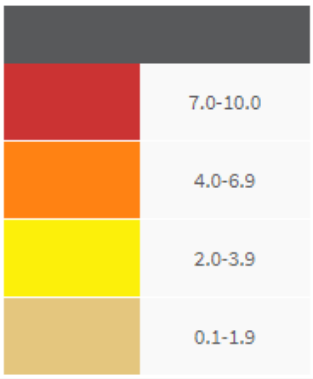
- The findings of the AlgoSec scan indicate inherent risks in the firewall configurations.
- The findings can be used by the ASV to focus the scan precisely on those networks and hosts that are inadequately protected by the firewall.
-

To be considered PCI-DSS compliant, the PCI-DSS Requirements and Security Assessment Procedures require that a scan must not contain any vulnerability that has been assigned a Common Vulnerability Scoring System (CVSS) base score equal to or higher than 4.0.

AlgoSec	CVSS Score	PCI
	7.0-10.0	✗
	4.0-6.9	✗
	2.0-3.9	✓
	0.1-1.9	✓

Offline Security Scan Results

The AlgoSec Firewall Analyzer provides an **Offline** Security Scan of the organization's devices.
The risks that the AlgoSec Firewall Analyzer flags are coordinated with the Common Vulnerability Scoring System (CVSS), as follows:



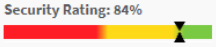
			algobotalgosec (Standard) demo (Standard) Ned NetOps (Standard) harry helpdesk (Read only)	
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.				
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entityâ⊠⊠s vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.	Risk Analysis	On	The AlgoSec Firewall Analyzer check for risks that can be mitigated within the network. Risks found: 1 high risks, 3 suspected high risks, 10 medium risks, 2 low risks See the Offline Security Scan results below for details.	✗
	Scheduled Analysis	Off	The AlgoSec Firewall Analyzer conducts analysis that includes reporting of the devices. The audit is scheduled	✗
11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	Risk Analysis	On	The AlgoSec Firewall Analyzer provides an Offline Security Scan, that supports and complements the ASV's online scan: First, the findings of the AlgoSec scan indicate inherent risks in the firewall configurations; and Second, the findings can be used by the ASV to focus the scan precisely to those networks and hosts that are inadequately protected by the firewall.	✗
11.6 Unauthorized changes on payment pages are detected and responded to.				
11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: ◦ At least once every seven days **OR** ◦ Periodically (at the frequency defined in the entityâ⊠⊠s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	Monitoring	On	All the changes made to device DaffodilCheckpointGW-2 are accessible on-line via the Monitoring tab in theÂ AlgoSec web interface.	✓
	Real-Time Alerting	On	The following users get alerts: Sue Security AlgoSec Administrator algobotalgosec demo Ned NetOps	✓

Below are the risks that AlgoSec flags, coordinated with PCI-DSS vulnerability levels:

		Code	Risk Description	Status
1.		C00014	Unauthorized traffic from Other to PCIzone	✗
2.		I01	"Any" service can enter your network	✓
3.		I02	TCP on all ports can enter your network	✓
4.		I03	UDP on all ports can enter your network	✓
5.		I07	Risky Microsoft services can enter your network	✓
6.		D01	"Any" service between internal networks	✗
7.		F01	Insecure external access to firewall	✗
8.		F02	Insecure internal access to firewall	✗
9.		I04	Telnet can enter your network	✓
10.		I09	Over 256 IP addresses can be reached by SMTP	✓
11.		I10	Over 256 IP addresses can be reached by DNS/UDP	✓
12.		I14	TCP on over 2000 ports can enter your network	✓
13.		I16	Over 256 IP addresses can be reached by DNS/TCP	✓
14.		I17	MSSQL can enter your network	✓
15.		I20	Database access services can enter your network	✓
16.		I23	NFS can enter your network	✓
17.		I24	LDAP can enter your network	✓
18.		I25	HTTP/HTTPS can enter your network	✓
19.		I32	UPnP can enter your network	✓
20.		I34	RADIUS can enter your network	✓
21.		I37	DHCP traffic can enter your network	✓
22.		I38	WINS can enter your network	✓
23.		I39	ICS protocols can enter your network	✓
24.		O03	Inside clients can connect to external IRC servers	✓
25.		O04	"Any" service can exit your network	✓
26.		O05	TCP on all ports can exit your network	✓
27.		O06	UDP on all ports can exit your network	✓
28.		O07	TCP on over 2000 ports can exit your network	✓
29.		R02	Implicit Check Point Rules (DNS/TCP)	✓
30.		R03	Implicit Check Point Rules (DNS/UDP)	✓
31.		C00001	Unauthorized service from Net1 to Net3,PCIzone	✓
32.		C00002	Unauthorized traffic from Net1 to Net1	✓
33.		C00003	forbiddenSvc from Net1 can reach Net2	✓
34.		C00004	Unauthorized service from Net2 to PCIzone	✓
35.		C00005	Unauthorized traffic from Net2 to Net2	✓
36.		C00006	Unauthorized service from Net3 to PCIzone	✓
37.		C00007	OnlySrvX from Net3 can reach Net2	✓
38.		C00008	Unauthorized traffic from Net3 to Net3	✓
39.		C00009	Unauthorized service from Net3 to Net1	✓
40.		C00010	Unauthorized service from PartnerNet to PCIzone	✓
41.		C00011	Unauthorized service from PartnerNet to Net1,Net2,Net3	✓
42.		C00012	Unauthorized service from PCIzone to Net1,Net2,Net3,PartnerNet	✓
43.		C00013	Unauthorized traffic from PCIzone to PCIzone,Other	✗
44.		C00015	Unauthorized traffic from Other to Net1,Net2,PartnerNet	✗
45.		C00016	Unauthorized service from Other to Net3	✗
46.		D02	TCP on all ports between internal networks	-
47.		D03	UDP on all ports between internal networks	-
48.		D04	Risky Microsoft services between internal networks	-
49.		D32	UPnP between internal networks	-
50.		D37	DHCP traffic between internal networks	-
51.		H03	External machines can manage your firewall	✓
52.		I05	RPC can enter your network	✓
53.		I06	SNMP can enter your network	✓
54.		I12	Over 256 IP addresses can be scanned by ICMP	✓
55.		I13	X11 can enter your network	✓
56.		I15	TFTP can enter your network	✓
57.		I18	P2P file-sharing services can enter your network	✓
58.		I19	Obsolete Instant-Messaging services can enter your network	✓
59.		I22	r_services can enter your network	✓
60.		I26	FTP can enter your network	✓
61.		I28	Finger can enter your network	✓
62.		I29	Ident can enter your network	✓
63.		I30	NNTP can enter your network	✓
64.		I31	H.323 can enter your network	✓
65.		I33	VMware can enter your network	✓
66.		I35	TACACS can enter your network	✓
67.		I36	MSMQ can enter your network	✓
68.		O01	POP3 can exit your network	✓
69.		O02	Over 256 IP addresses can send SMTP	✓
70.		O08	P2P file-sharing services can exit your network	✓
71.		O09	Obsolete Instant-Messaging services can exit your network	✓
72.		O10	Risky Microsoft services can exit your network	✓
73.		O11	IMAP can exit your network	✓
74.		O32	UPnP can exit your network	✓
75.		O33	VMware can exit your network	✓
76.		O37	DHCP traffic can exit your network	✓
77.		P04	Web Intelligence - No HTTP protocol inspection	✓
78.		P06	Web Intelligence - No Injection protection	✓
79.		P07	Application Intelligence - No P2P enforcements	✓
80.		P08	Application Intelligence - No POP3/IMAP protection	✓
81.		P09	Application Intelligence - No Microsoft NetBios protection	✓
82.		P11	Policy saved but not installed	✓
83.		P34	Password set to factory default value	✓
84.		P38	No anti-spoofing on any of the interfaces	✗
85.		P51	Missing Application Control ###Block### rules	✗
86.		P53	Check Point management software version no longer supported	✓
87.		R01	"From somewhere to Any allow Any service" rules	✗
88.		R05	Implicit Check Point Rules (RIP)	✓
89.		R06	Missing "Stealth" rule	✗
90.		R07	Implicit Check Point Rules (packets originating from Gateway)	✗
91.		R08	"Allow Any service" rules	✗
92.		R09	"Any destination" rules	✗
93.		F06	Insecure external VPN access to firewall	✓
94.		F07	Insecure internal VPN access to firewall	✓
95.		H01	Over 10 machines can manage your firewall	✓
96.		H02	Over 20 machines can manage your firewall	✓
97.		H04	Zone-spanning object definitions	✗
98.		I21	Version control services can enter your network	✓
99.		P01	IPS configuration - No denial of service protection	✓
100.		P02	IPS configuration - No flood protection	✓
101.		P03	IPS configuration - No check for out of sequence TCP packets	✓
102.		P10	Application Intelligence - No IP and ICMP checking	✓
103.		R04	Implicit Check Point Rules (ICMP)	✓
104.		R10	"From Any source" rules	✗

Requirement 12: Support Information Security with Organizational Policies and Programs

PCI DSS Requirement 12 addresses the need to have a strong security policy that sets the security tone for the whole entity and informs personnel what is expected of them. AlgoSec supports this requirement by providing detailed Risk Analysis that can help create an effective and strong security policy. The following table lists the items of PCI DSS Requirement 12 that AlgoSec supports:

PCI DSS Requirements	AlgoSec Feature	Setting	Details	Status
12.1 A comprehensive information security policy that governs and provides direction for protection of the entityâ€™s information assets is known and current.				
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	Risk profile	On	The AlgoSec Standard Risk Profile is a knowledge base of risk items that is included with the AlgoSec Firewall Analyzer, for details regarding the controls used in conjunction with the risk profile see the Risk Assessment Criteria.	✓
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.				
12.3.2 targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, including: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Maintained. • Performance of the targeted analysis of risk at least once every 12 months.	Risk Analysis	On	The AlgoSec Firewall Analyzer check for risks that can be mitigated within the network. Risks found: 1 high risks, 3 suspected high risks, 10 medium risks, 2 low risks See the Offline Security Scan results below for details.	✗
	Security Rating	On	**Security Rating: 84%** 	✓

2. About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity by automating connectivity flows and security policy, anywhere.

The AlgoSec platform enables the world's most complex organizations to gain visibility, reduce risk, achieve compliance at the application-level and process changes at zero-touch across the hybrid network.

Over 1,800 of the world's leading organizations trust AlgoSec to help secure their most critical workloads across public cloud, private cloud, containers, and on-premises networks.