PCI DSS v4.0 Network Security Checklist

Version: 1.0 | **Author:** VarnaAI (varnaai.com) | **License:** Free for commercial use **Scope:** Network and firewall requirements from PCI DSS v4.0 (Requirements 1, 2, 10, 11)

Assessment Information

Field	Value
Assessment Date	//________
Assessor	
Organization	
Scope	
PCI DSS Version	4.0
SAQ Type	[ ] A [ ] A-EP [ ] B [ ] C [ ] D [ ] ROC

Requirement 1: Install and Maintain Network Security Controls

1.1 Processes and Mechanisms

#	Control	Status	Evidence
1.1.1	Security policies for Requirement 1 are documented, kept up to date, and communicated	[ ] In Place [ ] Not In Place	
1.1.2	Roles and responsibilities for Requirement 1 are documented, assigned, and understood	[ ] In Place [ ] Not In Place	

1.2 Network Security Controls (NSC) Configuration

#	Control	Status	Evidence
1.2.1	NSC rulebase reviewed at least every 6 months	[ ] In Place [ ] Not In Place	
1.2.2	All changes to NSC configurations are approved and managed per change control	[ ] In Place [ ] Not In Place	
1.2.3	Accurate network diagram maintained showing all connections to CDE	[ ] In Place [ ] Not In Place	
1.2.4	Accurate data-flow diagram maintained for all cardholder data flows	[ ] In Place [ ] Not In Place	
1.2.5	All services, protocols, and ports allowed are identified, approved, and have business need	[ ] In Place [ ] Not In Place	

1.2.6	Security features defined for all insecure services/protocols in use	[ ] In Place [ ] Not In Place	
1.2.7	NSC configurations reviewed at least every 6 months to confirm relevance	[ ] In Place [ ] Not In Place	
1.2.8	NSC configuration files are secured and synchronized	[ ] In Place [ ] Not In Place	

1.3 Network Access Restrictions

#	Control	Status	Evidence
1.3.1	Inbound traffic to CDE restricted to only what is necessary	[ ] In Place [ ] Not In Place	
1.3.2	Outbound traffic from CDE restricted to only what is necessary	[ ] In Place [ ] Not In Place	
1.3.3	NSC installed between all wireless networks and CDE	[ ] In Place [ ] Not In Place	

1.4 Network Connections Between Trusted and Untrusted

#	Control	Status	Evidence
1.4.1	NSC implemented between trusted and untrusted networks	[ ] In Place [ ] Not In Place	
1.4.2	Inbound traffic from untrusted to trusted is restricted to authorized communications	[ ] In Place [ ] Not In Place	
1.4.3	Anti-spoofing measures implemented to detect forged source IPs	[ ] In Place [ ] Not In Place	
1.4.4	Cardholder data is not directly accessible from untrusted networks	[ ] In Place [ ] Not In Place	
1.4.5	Internal IP addresses are not disclosed to the internet	[ ] In Place [ ] Not In Place	

1.5 Risks to CDE from Computing Devices

#	Control	Status	Evidence
1.5.1	Security controls on devices connecting to both untrusted and CDE networks	[ ] In Place [ ] Not In Place	

Requirement 2: Apply Secure Configurations to All System Components

2.1 Processes and Mechanisms

#	Control	Status	Evidence
2.1.1	Security policies for Requirement 2 are documented and communicated	[ ] In Place [ ] Not In Place	
2.1.2	Roles and responsibilities documented and assigned	[ ] In Place [ ] Not In Place	

2.2 System Components Securely Configured

#	Control	Status	Evidence
2.2.1	Configuration standards developed for all system components	[ ] In Place [ ] Not In Place	
2.2.2	Vendor default accounts managed (changed, disabled, or removed)	[ ] In Place [ ] Not In Place	
2.2.3	Primary functions requiring different security levels are managed on separate instances	[ ] In Place [ ] Not In Place	
2.2.4	Only necessary services, protocols, and ports are enabled	[ ] In Place [ ] Not In Place	
2.2.5	Insecure services secured with additional features if in use	[ ] In Place [ ] Not In Place	
2.2.6	System security parameters configured to prevent misuse	[ ] In Place [ ] Not In Place	
2.2.7	All non-console administrative access encrypted with strong cryptography	[ ] In Place [ ] Not In Place	

Requirement 10: Log and Monitor All Access (Network-Relevant)

#	Control	Status	Evidence
10.2.1	Audit logs enabled on all system components and cardholder data	[ ] In Place [ ] Not In Place	
10.2.2	Logs capture all required details (user ID, event type, date/time, success/fail, data origin, resource affected)	[ ] In Place [ ] Not In Place	
10.3.1	Time-synchronization technology in use and kept current	[ ] In Place [ ] Not In Place	
10.3.3	Time settings received from industry-accepted sources	[ ] In Place [ ] Not In Place	
10.4.1	Audit logs reviewed at least daily for security events	[ ] In Place [ ] Not In Place	
10.5.1	Audit log history retained for at least 12 months (3 months immediately available)	[ ] In Place [ ] Not In Place	
10.6.1	Log harvesting systems protected from tampering	[ ] In Place [ ] Not In Place	

Requirement 11: Test Security Regularly (Network-Relevant)

#	Control	Status	Evidence

11.1.1	All security policies and procedures for Requirement 11 documented	[ ] In Place [ ] Not In Place	
11.2.1	Authorized and unauthorized wireless access points managed quarterly	[ ] In Place [ ] Not In Place	
11.3.1	Internal vulnerability scans performed at least quarterly	[ ] In Place [ ] Not In Place	
11.3.2	External vulnerability scans via ASV at least quarterly	[ ] In Place [ ] Not In Place	
11.4.1	External penetration testing at least annually and after significant changes	[ ] In Place [ ] Not In Place	
11.4.2	Internal penetration testing at least annually and after significant changes	[ ] In Place [ ] Not In Place	
11.5.1	Intrusion-detection/prevention techniques in place at CDE perimeter and critical points	[ ] In Place [ ] Not In Place	
11.5.2	Change-detection mechanism deployed on critical files	[ ] In Place [ ] Not In Place	
11.6.1	Change-and-tamper-detection mechanism on payment page HTTP headers and scripts	[ ] In Place [ ] Not In Place	

Summary

Requirement	In Place	Not In Place	Total
Req 1: Network Security Controls			/22
Req 2: Secure Configurations			/9
Req 10: Logging and Monitoring			/7
Req 11: Security Testing			/9
TOTAL			**/47**

Compliance Status: [ ] Compliant [ ] Non-Compliant [ ] Partially Compliant

Remediation Plan

Finding #	Requirement	Gap Description	Remediation Action	Owner	Target Date
1					
2					
3					

Sign-Off

Role	Name	Signature	Date
Assessor			
IT Security Manager			
CISO			

Free template by VarnaAI — AI-powered firewall change management. Try our free firewall rule scanner at fwchange.com/audit