# PCI-DSS v3.2:

# AUTOMATING AUDITS AND ENSURING CONTINUOUS COMPLIANCE WITH ALGOSEC

algosec

# Simplifying PCI-DSS Audits and 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.

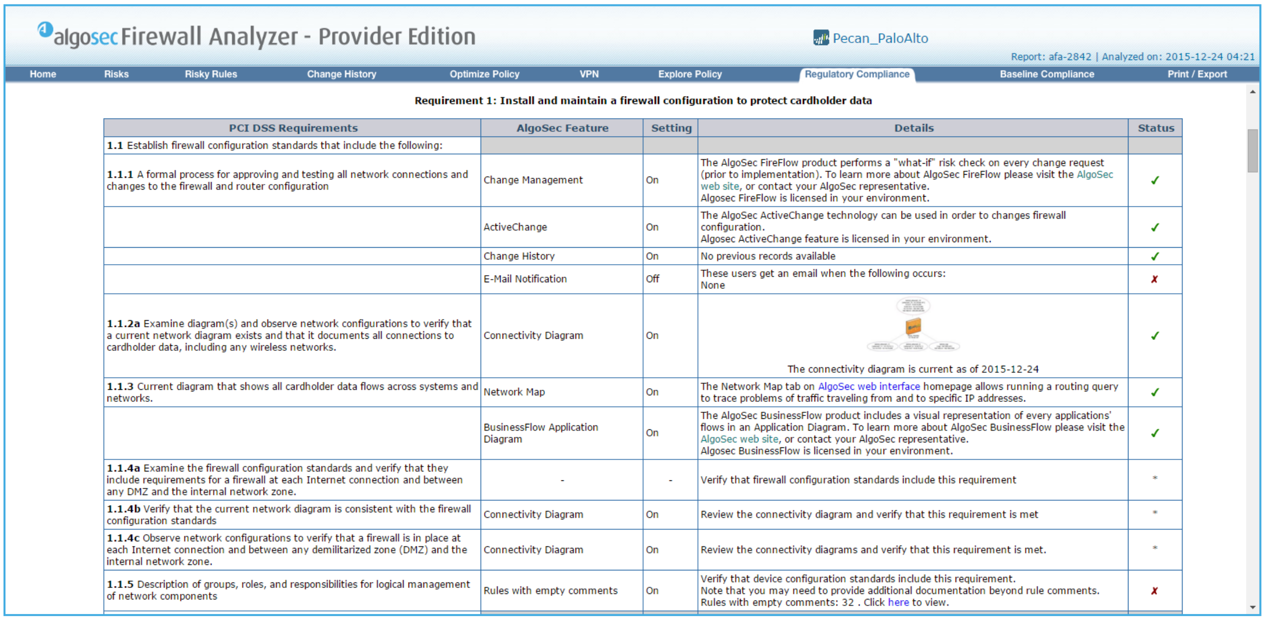
- **Quickly address compliance gaps with actionable recommendations:** Pinpoint areas of non-compliance with steps for remediation.

- **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 a firewall configuration to protect cardholder data

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



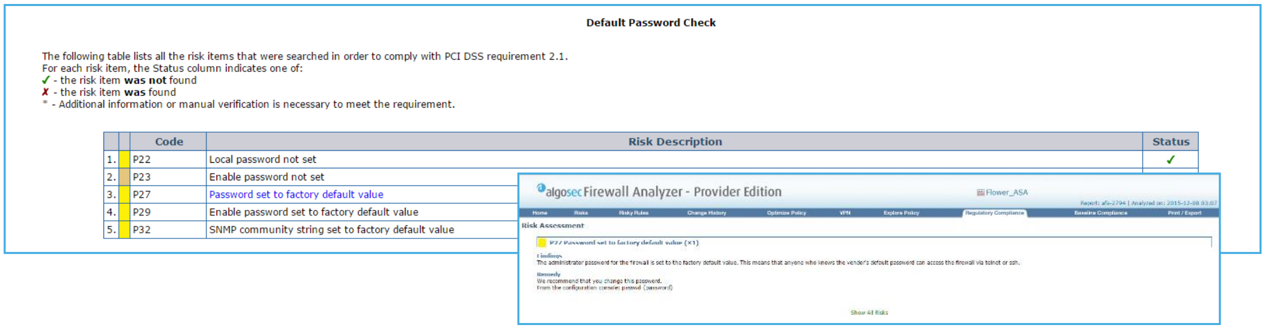
**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

| PCI DSS Requirements | AlgoSec Feature | Setting | Details | Status |
|---|---|---|---|---|
| **1.1** Establish firewall configuration standards that include the following: | | | | |
| **1.1.1** A formal process for approving and testing all network connections and changes to the firewall and router configuration | Change Management | 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.<br>Algosec FireFlow is licensed in your environment. | ✓ |
| | ActiveChange | On | The AlgoSec ActiveChange technology can be used in order to changes firewall configuration.<br>Algosec ActiveChange feature is licensed in your environment. | ✓ |
| | Change History | On | No previous records available | ✓ |
| | E-Mail Notification | Off | These users get an email when the following occurs:<br>None | ✗ |
| **1.1.2a** Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks. | Connectivity Diagram | On | The connectivity diagram is current as of 2015-12-24 | ✓ |
| **1.1.3** Current diagram that shows all cardholder data flows across systems and networks. | Network Map | On | The Network Map tab on AlgoSec web interface homepage allows running a routing query to trace problems of traffic traveling from and to specific IP addresses. | ✓ |
| | BusinessFlow Application Diagram | On | The AlgoSec BusinessFlow product includes a visual representation of every applications' flows in an Application Diagram. To learn more about AlgoSec BusinessFlow please visit the AlgoSec web site, or contact your AlgoSec representative.<br>Algosec BusinessFlow is licensed in your environment. | ✓ |
| **1.1.4a** 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. | - | - | Verify that firewall configuration standards include this requirement | * |
| **1.1.4b** Verify that the current network diagram is consistent with the firewall configuration standards | Connectivity Diagram | On | Review the connectivity diagram and verify that this requirement is met | * |
| **1.1.4c** 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. | Connectivity Diagram | On | Review the connectivity diagrams and verify that this requirement is met. | * |
| **1.1.5** Description of groups, roles, and responsibilities for logical management of network components | Rules with empty comments | On | Verify that device configuration standards include this requirement.<br>Note that you may need to provide additional documentation beyond rule comments.<br>Rules with empty comments: 32 . Click here to view. | ✗ |

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

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



**Default Password Check**

The following table lists all the risk items that were searched in order to comply with PCI DSS requirement 2.1.
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 | |

Risk Assessment

P27 Password set to factory default value (x1)

Findings
The administrator password for the firewall is set to the factory default value. This means that anyone who knows the vendor's default password can access the firewall via telnet or ssh.

Remedy
We recommend that you change this password.
From the configuration console: passwd {password}

## Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirement 4 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 also through VPN analysis to make sure all remote connections are being managed correctly. The following table details how AlgoSec assists the organization in meeting this requirement.

**Requirement 4: Encrypt transmission of cardholder data across open, public networks**

| PCI DSS Requirements | AlgoSec Feature | Setting | Details | Status |
|---|---|---|---|---|
| **4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.<br>Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016 | VPN Analysis | On | See the VPN Analysis report for details regarding remote access rights through firewall Pecan_PaloAlto | ✓ |
| | Baseline Compliance | On | SSH protocol settings, and replacing SSL by modern TLS in the device's built-in web server, may be covered by the AlgoSec Baseline Configuration report.<br>Also verify that the device's software version is up to date: see Requirement 6.<br>The baseline profile configured on this device is: PaloAltoProfile | * |
| **4.2** Never send unprotected PANs by end-user messaging technologies. | Risk Analysis | On | The AlgoSec Firewall Analyzer risk check helps you check if protocols such as POP, IMAP, and SMTP are allowed through the firewall, please review the Email Configuration risks table below for further details. | * |

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

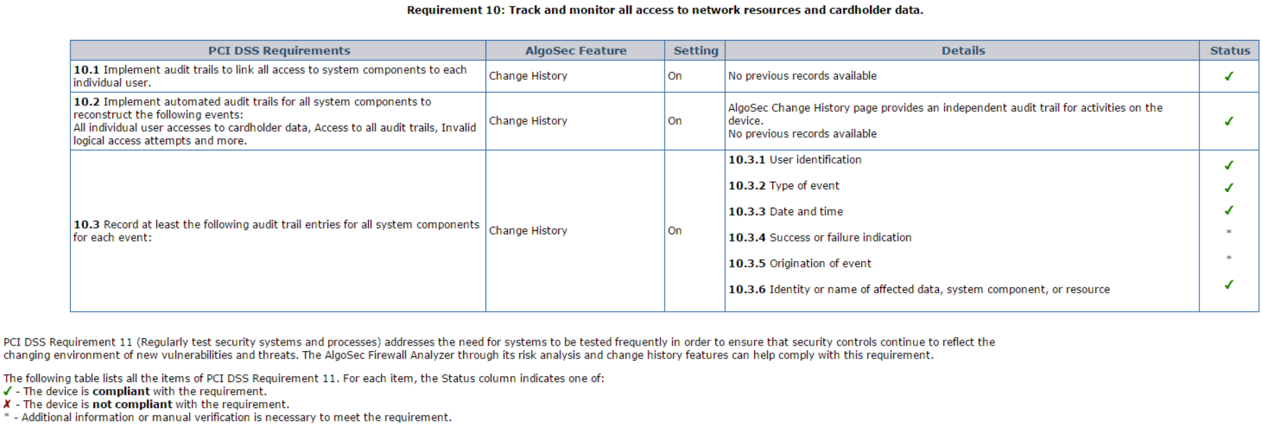
PCI-DSS Requirement 6.1 requires a process to identify and rank security vulnerabilities. AlgoSec uniquely maps and correlates security vulnerability data to their respective applications and processes within the scope of the PCI DSS audit. This gives users the information they need to focus and proactively 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 v3.2 regulatory standard.

To comply with PCI-DSS Requirement 6.2 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.

| | | Code | Risk Description | Status |
|---|---|---|---|---|
| 1. | 🟨 | P47 | Palo Alto software version no longer supported | ✗ |

## Requirement 10: Regularly test security systems and processes

AlgoSec provides an immediate view of compliance with PCI-DSS 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 following table details how AlgoSec assists the organization in meeting this requirement.



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

| PCI DSS Requirements | AlgoSec Feature | Setting | Details | Status |
|---|---|---|---|---|
| **10.1** Implement audit trails to link all access to system components to each individual user. | Change History | On | No previous records available | ✓ |
| **10.2** Implement automated audit trails for all system components to reconstruct the following events:<br>All individual user accesses to cardholder data, Access to all audit trails, Invalid logical access attempts and more. | Change History | On | AlgoSec Change History page provides an independent audit trail for activities on the device.<br>No previous records available | ✓ |
| **10.3** Record at least the following audit trail entries for all system components for each event: | Change History | On | **10.3.1** User identification | ✓ |
| | | | **10.3.2** Type of event | ✓ |
| | | | **10.3.3** Date and time | ✓ |
| | | | **10.3.4** Success or failure indication | * |
| | | | **10.3.5** Origination of event | * |
| | | | **10.3.6** Identity or name of affected data, system component, or resource | ✓ |

PCI DSS Requirement 11 (Regularly test security systems and processes) addresses the need for systems to be tested frequently in order to ensure that security controls continue to reflect the changing environment of new vulnerabilities and threats. The AlgoSec Firewall Analyzer through its risk analysis and change history features can help comply with this requirement.

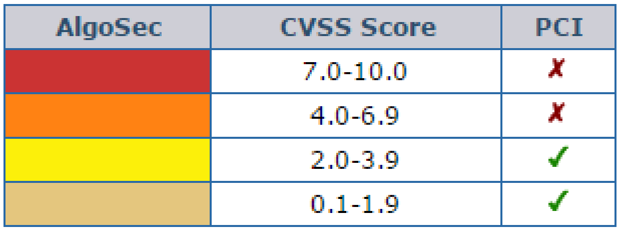
The following table lists all the items of PCI DSS Requirement 11. For each item, the Status column indicates one of:
✓ - The device is **compliant** with the requirement.
✗ - The device is **not compliant** with the requirement.
* - Additional information or manual verification is necessary to meet the requirement.

## Requirement 11: Regularly test security systems and processes

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:

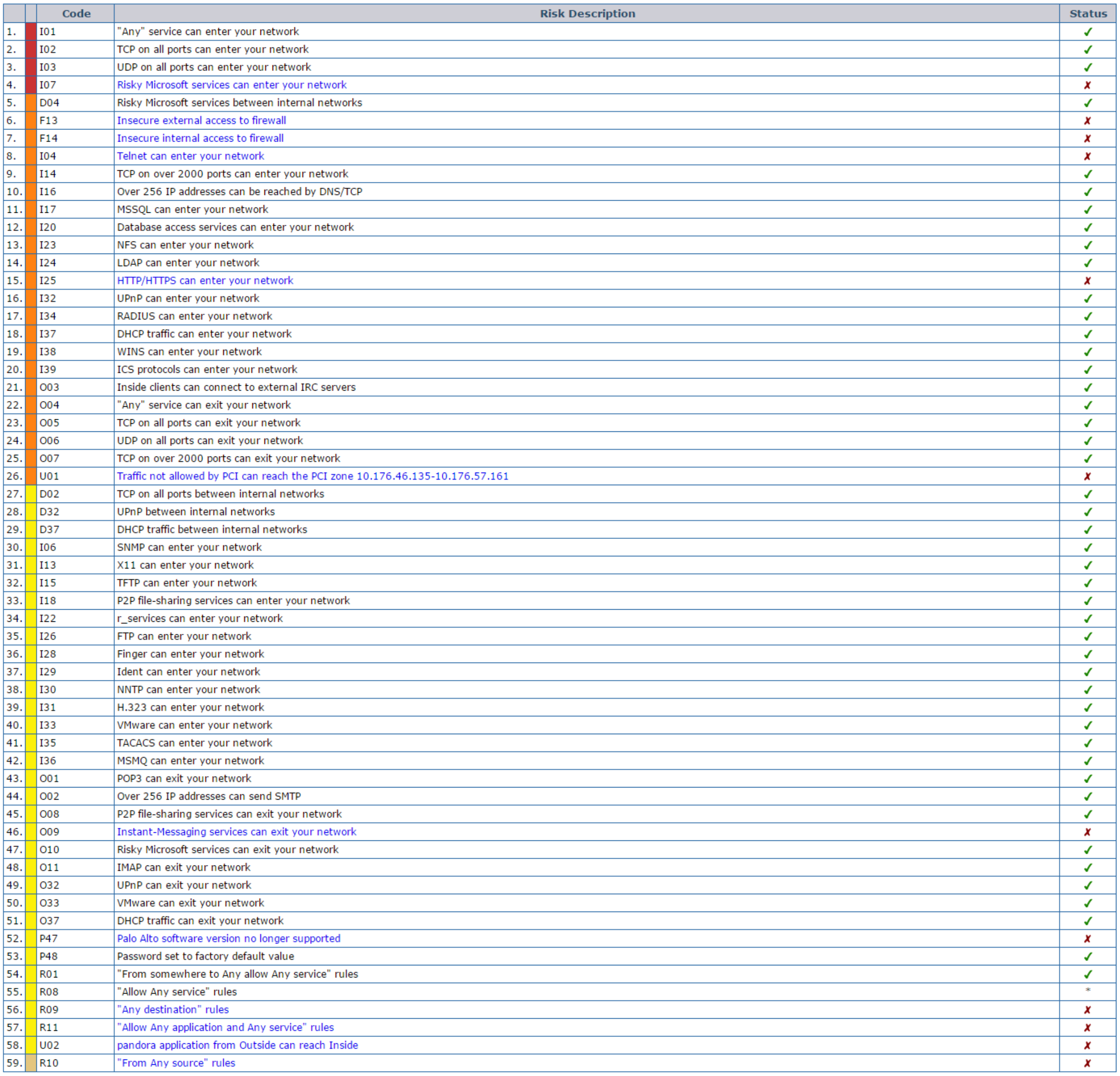
- The findings of the AlgoSec scan indicate inherent risks in the firewall configurations
- The findings can be used by the ASV to focus the scan precisely on those networks and hosts that are inadequately protected by the firewall

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 | ✓ |

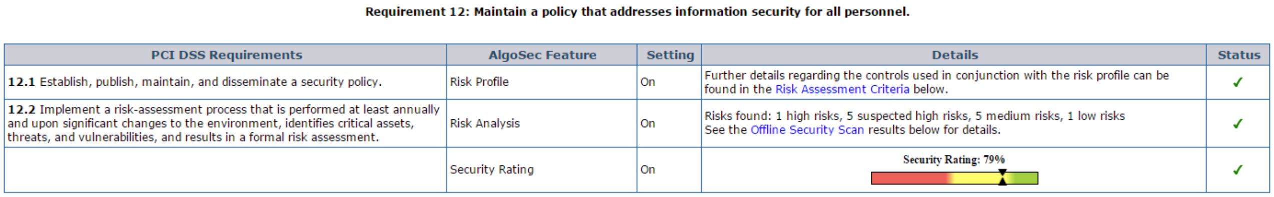
Below are the risks that AlgoSec flags, coordinated with PCI-DSS vulnerability levels:



| | | Code | Risk Description | Status |
|---|---|---|---|---|
| 1. | 🟥 | I01 | "Any" service can enter your network | ✓ |
| 2. | 🟥 | I02 | TCP on all ports can enter your network | ✓ |
| 3. | 🟥 | I03 | UDP on all ports can enter your network | ✓ |
| 4. | 🟥 | I07 | Risky Microsoft services can enter your network | ✗ |
| 5. | 🟧 | D04 | Risky Microsoft services between internal networks | ✓ |
| 6. | 🟧 | F13 | Insecure external access to firewall | ✗ |
| 7. | 🟧 | F14 | Insecure internal access to firewall | ✗ |
| 8. | 🟧 | I04 | Telnet can enter your network | ✗ |
| 9. | 🟧 | I14 | TCP on over 2000 ports can enter your network | ✓ |
| 10. | 🟧 | I16 | Over 256 IP addresses can be reached by DNS/TCP | ✓ |
| 11. | 🟧 | I17 | MSSQL can enter your network | ✓ |
| 12. | 🟧 | I20 | Database access services can enter your network | ✓ |
| 13. | 🟧 | I23 | NFS can enter your network | ✓ |
| 14. | 🟧 | I24 | LDAP can enter your network | ✓ |
| 15. | 🟧 | I25 | HTTP/HTTPS can enter your network | ✗ |
| 16. | 🟧 | I32 | UPnP can enter your network | ✓ |
| 17. | 🟧 | I34 | RADIUS can enter your network | ✓ |
| 18. | 🟧 | I37 | DHCP traffic can enter your network | ✓ |
| 19. | 🟧 | I38 | WINS can enter your network | ✓ |
| 20. | 🟧 | I39 | ICS protocols can enter your network | ✓ |
| 21. | 🟧 | O03 | Inside clients can connect to external IRC servers | ✓ |
| 22. | 🟧 | O04 | "Any" service can exit your network | ✓ |
| 23. | 🟧 | O05 | TCP on all ports can exit your network | ✓ |
| 24. | 🟧 | O06 | UDP on all ports can exit your network | ✓ |
| 25. | 🟧 | O07 | TCP on over 2000 ports can exit your network | ✓ |
| 26. | 🟧 | U01 | Traffic not allowed by PCI can reach the PCI zone 10.176.46.135-10.176.57.161 | ✗ |
| 27. | 🟨 | D02 | TCP on all ports between internal networks | ✓ |
| 28. | 🟨 | D32 | UPnP between internal networks | ✓ |
| 29. | 🟨 | D37 | DHCP traffic between internal networks | ✓ |
| 30. | 🟨 | I06 | SNMP can enter your network | ✓ |
| 31. | 🟨 | I13 | X11 can enter your network | ✓ |
| 32. | 🟨 | I15 | TFTP can enter your network | ✓ |
| 33. | 🟨 | I18 | P2P file-sharing services can enter your network | ✓ |
| 34. | 🟨 | I22 | r_services can enter your network | ✓ |
| 35. | 🟨 | I26 | FTP can enter your network | ✓ |
| 36. | 🟨 | I28 | Finger can enter your network | ✓ |
| 37. | 🟨 | I29 | Ident can enter your network | ✓ |
| 38. | 🟨 | I30 | NNTP can enter your network | ✓ |
| 39. | 🟨 | I31 | H.323 can enter your network | ✓ |
| 40. | 🟨 | I33 | VMware can enter your network | ✓ |
| 41. | 🟨 | I35 | TACACS can enter your network | ✓ |
| 42. | 🟨 | I36 | MSMQ can enter your network | ✓ |
| 43. | 🟨 | O01 | POP3 can exit your network | ✓ |
| 44. | 🟨 | O02 | Over 256 IP addresses can send SMTP | ✓ |
| 45. | 🟨 | O08 | P2P file-sharing services can exit your network | ✓ |
| 46. | 🟨 | O09 | Instant-Messaging services can exit your network | ✗ |
| 47. | 🟨 | O10 | Risky Microsoft services can exit your network | ✓ |
| 48. | 🟨 | O11 | IMAP can exit your network | ✓ |
| 49. | 🟨 | O32 | UPnP can exit your network | ✓ |
| 50. | 🟨 | O33 | VMware can exit your network | ✓ |
| 51. | 🟨 | O37 | DHCP traffic can exit your network | ✓ |
| 52. | 🟨 | P47 | Palo Alto software version no longer supported | ✗ |
| 53. | 🟨 | P48 | Password set to factory default value | ✓ |
| 54. | 🟨 | R01 | "From somewhere to Any allow Any service" rules | ✓ |
| 55. | 🟨 | R08 | "Allow Any service" rules | * |
| 56. | 🟨 | R09 | "Any destination" rules | ✗ |
| 57. | 🟨 | R11 | "Allow Any application and Any service" rules | ✗ |
| 58. | 🟨 | U02 | pandora application from Outside can reach Inside | ✗ |
| 59. | 🟫 | R10 | "From Any source" rules | ✗ |

## Requirement 12: Maintain a policy that addresses information security for employees and contractors

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:



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

| PCI DSS Requirements | AlgoSec Feature | Setting | Details | Status |
|---|---|---|---|---|
| **12.1** Establish, publish, maintain, and disseminate a security policy. | Risk Profile | On | Further details regarding the controls used in conjunction with the risk profile can be found in the Risk Assessment Criteria below. | ✓ |
| **12.2** Implement a risk-assessment process that is performed at least annually and upon significant changes to the environment, identifies critical assets, threats, and vulnerabilities, and results in a formal risk assessment. | Risk Analysis | On | Risks found: 1 high risks, 5 suspected high risks, 5 medium risks, 1 low risks<br>See the Offline Security Scan results below for details. | ✓ |
| | Security Rating | On | Security Rating: 79% | ✓ |

## About AlgoSec

The leading provider of business-driven security management solutions, AlgoSec helps the world's largest organizations align security with their business processes. With AlgoSec, users can discover, map and migrate business application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate network security changes with zero touch - across their cloud, SDN and on-premise networks. Over 1,800 enterprises, including 20 of the Fortune 50, have utilized AlgoSec's solutions to make their organizations more agile, more secure and more compliant - all the time. AlgoSec is ISO 27001 certified, and since its inception, AlgoSec has provided the industry's only money-back guarantee.