Best Practices
for PCI DSS Version 3.2
Network Security Compliance
Executive Summary

Payment data fraud by cyber criminals is a growing threat not only to financial institutions and retail organizations, but to enterprises everywhere in practically every industry. As a result, the Payment Card Industry Data Security Standard (PCI DSS) is one of the most wide-reaching standards today. The goal of PCI DSS is to encourage and enhance payment data security and facilitate the broad adoption of consistent data security measures globally. It protects against fraud and security threats by providing a baseline of technical and operational requirements designed to protect payment data.

To comply with the PCI DSS, IT managers and PCI internal auditors must perform periodic audits every 6 months. Furthermore, the PCI DSS Council updates the standard periodically to remediate growing threats by cybercriminals. Therefore, complying with the latest PCI DSS standard and ensuring that the enterprise network is audit ready is a pressing concern of many IT managers and PCI internal auditors today.

Yet, according to Dark Reading, “7 out of 10 companies that achieve PCI compliance fail to maintain that status even for a year. Verizon’s research showed that only 28.6% of companies managed to remain compliant for the full year between annual assessments.” So maintaining compliance and audit-readiness is certainly a challenge. Gartner’s recent research, What’s Changing and How to Respond to PCI DSS v.3.2 recommends, “that instead of a goal-led approach to PCI DSS compliance, a systems-led approach is adopted, moving implementation of security controls away from a project-based approach into day-to-day application, systems and security operations.”

This paper provides information to IT managers and PCI internal auditors for understanding network security needs and best practices to mitigate payment data cyber threats as well as the related requirements for PCI DSS version 3.2 audits. Tufin’s network security expertise enables excellent support for PCI internal auditors, IT managers and their network operation teams to design, plan and integrate the changes required for PCI DSS compliance into business-as-usual activities. The Tufin Orchestration Suite™ solution supports IT managers and PCI internal auditors to lessen their compliance headache.

Protecting Payment Data with PCI DSS

The PCI DSS defines 12 high-level requirements, grouped into 6 control objectives. To comply, PCI internal auditors or IT managers perform periodic audits every 6 months (3 months recommended). Audits demonstrate compliance via numerous testing procedures and sub-requirements, as seen in the table:

<table>
<thead>
<tr>
<th>PCI DSS Control Objectives</th>
<th>Requirement Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network and Systems</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Protect all systems against malware and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td></td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
</tbody>
</table>
Implement Strong Access Control Measures
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy
12. Maintain a policy that addresses information security for all personnel

The main PCI DSS principle: Payment data is only as secure as the pathways that provide access to it. On the one hand, PCI DSS requirements are designed to ensure that network security practices eliminate or minimize known risks. On the other hand, they ensure that the organization defines well-structured policies, procedures and practices that can be tracked and audited. To ensure both secure data pathways and adherence to strict network security policies, PCI DSS requires:

- Specific guidelines for processing card payments to help prevent payment data fraud, skimming and other security threats
- Aligning with the industry best practices to increase the trust of both customers and partners
- Limiting external network access to sensitive data, combined with a formal process for monitoring all changes to firewall configuration and cloud security groups
- Tracking and auditing of firewall and cloud operations regularly, including clear definitions of roles and responsibilities
- Strictly limiting internal organizational access to sensitive data
- Documenting, enforcing and auditing all operational procedures and practices

In summary, PCI DSS demands that organizations maintain continuous compliance through an ongoing process of: Assess, RemEDIATE and Report.¹ To comply, your IT organization must have an accurate picture of your compliance posture, the tools to address issues, and the ability to demonstrate compliance through internal and external audits.

Complying with PCI DSS Network Security Challenges

About 40% of PCI DSS is related to network security, but this is really the crux of the headache, pitfalls and disturbance for PCI internal auditors, IT managers and their teams.

For network security teams to integrate a repeatable compliance procedure that doesn’t disrupt business-as-usual, it’s simply not feasible for IT managers and PCI internal auditors to manually manage and test. The many IT tasks involved in documenting, tracking and auditing network security procedures manually can take weeks. The numerous security devices (firewalls, routers and others), with each device managing hundreds to thousands of rules makes for an extremely complex enterprise network environment. To ensure compliance, the team must have a clear visibility to the network topology, the routing flow of data around the network, and the setting of all security devices (as there are many paths to move between network segments, and all paths should be configured based on the desired policy). Therefore, PCI DSS compliance requires the right set of tools and automated solutions for visibility, alerting and quick breach fixes.

¹https://www.pcisecuritystandards.org/security_standards/getting_started.php
Seven PCI DSS Best Practices for Network Security

Since PCI DSS is the de-facto standard that any company processing credit cards must comply to, IT managers and PCI internal auditors continually align their enterprise security program to achieve this goal.

Before getting into the PCI DSS requirement details, it’s good to look at what’s worked at many enterprises to enforce and remediate PCI network security compliance. Tufin networking experts gathered valuable learning and best practices from their PCI implementation experience. If IT managers and PCI internal auditors do it right, their work on PCI compliance can also be a springboard for their organization into continuous network security and more effective work processes.

Tufin’s 7 best practices for network security compliance are:

1) **Create a clear separation** with proper network segmentation of PCI data, PCI application, and PCI web within the network (DMZ, Internal and Internet)

2) **Ensure that you have an enterprise-wide network change workflow process** in place that meets PCI requirements

3) **Ensure that every network change has a complete audit trail** with the who, what, when, and why

4) **Validate every network change** with the following:
   a. Analyze the change for risks as defined in your security policy
   b. Get approval by the business owner
   c. Ensure the changes are implemented according to the PCI-compatible network change workflow

5) **Ensure that firewalls protecting PCI zones work** with the following guidelines:
   a. Every rule has a comment
   b. Every rule has a log
   c. No rules with “Any” in the Src, Dest, and Srv
   d. No rules with risky services (un-encrypted)
   e. Delete unused rules

6) **Ensure every firewall rule and cloud security groups is documented properly** with the following info:
   a. Business justification
   b. Business owner
   c. Application name

7) **Ensure that you keep firewall and cloud security groups logs** for at least 12 months
Audit Readiness Through Continuous Compliance

PCI DSS v3.2 compliance can be a great opportunity to get the buy-in and budgets to ensure network security is geared for ongoing success... For IT managers and PCI internal auditors to set high, sustainable security standards, Tufin experts suggest paying special attention to sub-requirements within PCI DSS requirement 1.

When IT managers take a broader look at PCI requirement 1, not just with an eye on getting PCI compliance, these requirements open the door for implementing ongoing network security solutions. Otherwise, they tend to be problematic since they rely on manual processes that no longer scale to meet the needs of the business — an increasingly common scenario.

In any case, enterprises with large firewall estates need to automate firewall operations to meet business reality. While large-scale deployments are always intense, introducing some long-term improvements that align PCI compliance efforts with your organization’s specific security needs can be a good way to make the effort even more worthwhile and have long-term effect on the enterprise.

To overcome the common network security and PCI DSS compliance challenges, IT managers and PCI internal auditors can gain insights by drilling down into 5 requirements. Additional best practices for focusing efforts on achieving both compliance and ongoing success are revealed:

1.1.1 Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.

PCI internal auditors need to show that a clearly defined, enforceable change process for firewall policies exists. The PCI external auditor will ask to see a change report with a full audit trail, and then select some random changes and request to see the sign off.

**The Challenge:** Many organizations still don’t have a change process in place or, if they do, it’s too loose or relies on good will rather than formal procedures.

**Best Practice:** The best way to implement formal, auditable change processes is to by using an adequate tool for the task.

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.

This sub-requirement is concerned with three main risks:

1. Are the connections required for business known?
2. Are firewalls and cloud security groups implementing the Principle of Least Privilege? Allowing only connections that are required for business?
3. Are any of these connections insecure? Do compensating controls for them exist?

**The Challenge:** Most organizations don’t have an up-to-date list of services that are required for business. In the best case, documentation per firewall rule/cloud security group exists. Most likely some connections contain insecure services (NOTE: For PCI, the list is open to interpretation by the auditor).

**Best Practice:** IT managers need to make sure they know about each of these services in advance with relevant justifications from a security perspective.

1.1.7 Requirement to review rule sets for firewalls, routers and cloud security groups at least every six months
IT managers and PCI internal auditors need to have proof that a process exists and working to meet this requirement. Complying with this requirement usually entails having a report to show rule sets were in fact reviewed, and that any questionable rules from the last audit were addressed, and that any changes to rules since the last audit were dealt with properly (i.e. old or non-compliant rules/objects were dealt with).

**Best Practice:** Around one third of companies fail to provide the required documentation to satisfy the PCI external auditor on this point because of poor processes. Therefore, ensure your processes are up to date and functioning.

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the payment data environment

Usually the PCI external auditor is looking for a set of rules that permit specific PCI services (approved known protocols used by the PCI servers) followed by an explicit drop rule for all other traffic. Exceptions must include proper documentation (such as rule comments) that makes sense to the auditor.

**Best Practice:** Around one quarter of businesses find it difficult to correctly restrict inbound access; setting explicit drop rules is much easier. Proper definition of PCI services and PCI zones make compliance much simpler. So it’s important to ensure that the PCI external auditor agrees to the contents of PCI services and PCI zones.

If IT managers and PCI internal auditors can prove that an active alerting mechanism to prevent non-compliant changes exists, the enterprise is audit ready.

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ

IT managers need to allow traffic from the Internet to specific servers (IP Addresses) in the DMZ — everything else should be dropped. Proper definition of traffic that is Internet (i.e. all non-local IP addresses) and proper definition of the accessible IPs within the DMZ are critical for compliance. Plus, the PCI external auditor must agree that definitions are correct.

**Best Practice:** If definitions are in place, an active alert mechanism for unauthorized traffic is what’s needed for IT managers to ensure network security.

1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet

To do this, network operation teams need to properly define the 'Internet' and 'cardholder data' environments, or in other words, create network segmentations that can be isolated. The PCI external auditor wants to see that there is no direct access between these entities, and that there is proper evidence for this.

**Best Practice:** If IT managers document and manage access with the right tools, PCI DSS auditing becomes part of the everyday IT and business activities:

1) Ensure documentation is ready
2) Prove serious about maintaining compliance
Quick PCI DSS v3.2 Network Security Checklist

IT managers and PCI internal auditors can use the PCI DSS Network Security Checklist for preparing for audits. The checklist summarizes the key PCI DSS Requirements and Testing Procedures related to network security. If best practices for network security have been implemented in the organization, the PCI DSS audit becomes a healthy routine versus a compliance headache.

To meet the requirements related to network security in an efficient, quick and manageable way, Tufin’s PCI DSS solution helps organizations with tools for compliance with version 3.2:

<table>
<thead>
<tr>
<th>PCI DSS Requirements &amp; Testing Procedures</th>
<th>Tufin’s PCI DSS 3.2 Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and maintain a secure network and systems</td>
<td>1.1 Establish and implement firewall and router configuration standards that include the following: Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:</td>
</tr>
<tr>
<td>1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations</td>
<td>Automation and documentation of all firewall and router configuration changes, PCI firewall and router checks, PCI requirements deviation detection and reporting</td>
</tr>
<tr>
<td>1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks</td>
<td>PCI zone mapping and network topology map</td>
</tr>
<tr>
<td>1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone</td>
<td>PCI firewall and router checks, PCI requirements deviation detection and reporting</td>
</tr>
<tr>
<td>1.1.6 Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each.</td>
<td>USP, policy browser, rule properties and documentation</td>
</tr>
<tr>
<td>1.1.7 Requirement to review firewall and router rule sets at least every six months</td>
<td>PCI compliance report, USP and violations dashboard</td>
</tr>
<tr>
<td>1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. (1.2.1a, 1.2.1b, 1.2.1c)</td>
<td>PCI firewall and router connection checks, USP, violations dashboard and reporting</td>
</tr>
<tr>
<td>1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment (1.3.1,1.3.2,1.3.4,1.3.6)</td>
<td>Central network management for firewall and router to restrict traffic between Internet and PCI zone via the USP</td>
</tr>
<tr>
<td>Develop configuration standards for all system components. Assume that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards</td>
<td>2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.</td>
</tr>
<tr>
<td>2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure</td>
<td>USP, rule documentation and policy browser</td>
</tr>
<tr>
<td>2.2.4 Configure system security parameters to prevent misuse</td>
<td>Tufin Orchestration Suite support of TLS v1.2 for encrypting communications between internal processes. Note: Users must ensure that other devices, daemons, and services use secure encryption for any communications.</td>
</tr>
<tr>
<td>2.3.1 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.</td>
<td>USP, configuration of rule properties to identify unused rules</td>
</tr>
</tbody>
</table>
As most enterprises are adopting public and/or private cloud platforms, it is important to note that although the PCI DSS standard relates predominantly to firewall environments, the Tufin Orchestration Suite solution for network security policy management supports all leading network security platforms, including hybrid cloud.

To summarize, the Tufin Orchestration Suite solution provides the following benefits for PCI DSS 3.2 compliance needs:

- Reduced time and effort required for audit readiness through continuous compliance, including automated audit trail of full accountability with documentation
- Proactive risk analysis to avoid security and compliance violations
- Implementation of network changes in minutes instead of days
- Increased control with a unified console supporting all leading enterprise network security platforms (traditional networks and firewalls, SDN and cloud platforms)
- Automated provisioning and end-to-end orchestration for multi-vendor environments to reduce complexity and human error
- Flexible, customizable workflows for full integration into enterprise ITSM processes

For more information on using the Tufin Orchestration Suite for PCI DSS v3.2 compliance, please refer to the Tufin Knowledge Center Technical Notes on Security and Compliance, “Implement PCI DSS v3 Using Unified Security Policy.”

About Tufin

Tufin® is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 1,800 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries.

Copyright © 2016 Tufin
Tufin logo, Tufin and SecureChange are registered trademarks of Tufin. Unified Security Policy, Tufin Orchestration Suite, SecureTrack and SecureApp are trademarks of Tufin. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.