PACKETSLED™

# *Network Visibility* in PCI Regulated Environments

JULY, 2018

# PCI COMPLIANCE

## BACKGROUND

If your business accepts payments via credit, debit, or pre-paid cards, you are required to comply with the security requirements of the Payment Card Industry Security Standards Council (PCI Council)[1]. Looking from the top down, the PCI Data Security Standard (DSS) appears concise and designed to ensure a card-holder data environment (CDE) has proper security controls in place. The current DSS standard is v.3.2.[2] The standard focuses on six key requirements:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

Businesses that must comply with PCI regulations are classified based on the total number of transactions they process in a year.

**Level 1:** 6 million+ transactions per year.
**Level 2:** 1-6 million transactions per year.
**Level 3:** 20,000 to 1 million card transactions per year.
**Level 4**: Fewer than 20,000 transactions per year.

Regardless of what PCI level, every business must attest they comply with the PCI-DSS on an annual basis. Level-1 businesses must complete an *Annual Report on Compliance* (ROC)and perform quarterly vulnerability scans. Level 2-4 businesses are required to complete an *Annual Self-Assessment Questionnaire* (SAQ) and perform quarterly vulnerability scans.

## THE PCI COMPLIANCE BURDEN

When you look at the PCI-DSS from the bottom up, you quickly realize the task of complying with the standard can be a daunting experience. Underneath the six high-level goals of the standard are twelve detailed requirements. The complete standard looks like this:

1. **Build and Maintain a Secure Network**
   Requirement-1: Install and maintain a firewall configuration to protect cardholder data.
   Requirement-2: Do not use vendor-supplied defaults for system passwords and other security parameters.
2. **Protect Cardholder data.**

[1] https://www.pcisecuritystandards.org/

[2] https://www.pcisecuritystandards.org/document_library

Requirement-3: Protect stored cardholder data.
Requirement-4: Encrypt transmission of cardholder data across open, public networks.

3. Maintain a Vulnerability Management Program.
   Requirement-5: Protect all systems against malware and regularly update anti-virus software or programs.
   Requirement-6: Develop and maintain secure systems and applications.
4. Implement Strong Access Control Measures.
   Requirement-7: Restrict access to cardholder data by business need to know.
   Requirement-8: Identify and authenticate access to system components.
   Requirement-9: Restrict physical access to cardholder data.
5. Regularly Monitor and Test Networks.
   Requirement-10: Track and monitor all access to network resources and cardholder data.
   Requirement-11: Regularly test security systems and processes.
6. Maintain an Information Security Policy.
   Requirement-12: Maintain a policy that addresses information security for all personnel.

## NETWORK VISIBILITY IN PCI ENVIORMENTS

PacketSled has deep expertise in monitoring, analyzing and visualizing network traffic. Our network visibility platform is easy to implement, flexible, and scalable from the smallest to the largest enterprises. We strongly believe adding a network visibility capability to PCI regulated environments pays high dividends. While a traditional PCI-DSS assessment clearly has value in identifying gaps in security compliance, it is a labor-intensive and time-consuming process that relies on an organization "*Telling*" an assessor about their security controls protecting the CDE. At PacketSled, we think it is much better to "*Show*" how implemented PCI controls perform.

It is easy to contemplate having a network visibility capability to measure security controls around PCI-DSS goal 1) "Build and maintain a secure network," and 5) "Regularly monitor and test networks" is useful. At PacketSled, we believe our platform provides much more to a PCI merchant or QSA. For example, a PCI assessment requires the assessor select a sample of firewalls in the CDE and review their rules configuration. This can be done manually, or with the assistance of tools that analyze the firewall rules file. Instead of spending hours reviewing a five-thousand-line firewall rule file, why not deploy a *PacketSled* sensor and "***see***" what the firewalls are allowing into your CDE. Simple.

PacketSled sensors deployed in your PCI regulated environment not only provide continuous network visibility and full-packet capture as desired, but they make managing complex PCI networks easier. Upon deep analysis of the ROC reporting template, we identified 100+ use-cases where deployment of the PacketSled platform could assist in the verification and/or testing of PCI-DSS required controls. This is *in addition* to providing continuous monitoring of network traffic. The PCI requirements around securing and monitoring of networks is our sweet-spot. But we can do a lot more. In fact, we cross-referenced the entire ROC report template to PacketSled's platform capabilities. For each item in the ROC template, we classified each requirement under one of three categories: 1) PS-Test, 2) PS-Verify, or 3) PS-NA.

PS-Test means the PacketSled platform can be used to *test* whether or not the requirement has been implemented. PS-Verify, means PacketSled can be used to verify the requirement has been implemented *properly*. PS-NA means the PacketSled platform does not provide any additional value for that requirement. For example, requirements around the physical security requirements around a CDE are classified as PS-NA since network visibility cannot help test or verify if these controls are in place. The chart on page 7-9 of this document, contains a summary of the ROC template sections and the relevant PacketSled applicability.

## PACKETSLED'S SOLUTION

When Fluke, the world leader in compact, professional electronic test tools evaluated PacketSled, they realized the potential in the platform's ability to leverage data for reasons beyond security metrics. They could also use PacketSled for network baselining, user-agent types, client distributions, etc. All of which enables Fluke to adhere to government compliance regulations including (but not limited to), PCI, SOX GDPR, DFARS, ITAR, Chinese and Russian data privacy laws. They also appreciated how PacketSled was quick to implement feature requests and integrations and could be deployed on premise or in the cloud, based on the need of each Fluke location. But most importantly, Fluke's security team would be empowered with real-time threat identification and greater network visibility across the expanse of their global operation. Other gained benefits include:

- ✓ Uncovering hidden attack signals that were not previously visible.
- ✓ Improved network context to the threat hunting and anomaly detection processes.
- ✓ Utilization of built-in interactive visualizations and custom detections that provide meaningful situational awareness during IR.
- ✓ PacketSled is also used by Fluke for Merger and Acquisition risk assessment.
- ✓ Improved security monitoring on internal segments.
- ✓ Quickly retrieve historical network data during incident response exercises.
- ✓ Automatically check traffic against built in, open source and custom detection signatures.
- ✓ The ability to add custom detections.
- ✓ The ability to leverage the data for not just security metrics, but network baselining, government regulations, user-agent types and client distributions.
- ✓ The product is Bro-based and is quick to implement detections for new threats or attack vectors globally.
- ✓ Full network telemetry byproduct, which enabled usability outside of the security team.

*"Fluke is accountable to several compliance frameworks and risk associated with our business model. PacketSled provides us a hybrid of deployment solutions and assessment capabilities for a small team to centralize, visualize, detect, report and manage risk. We use PacketSled's full telemetry to evaluate risk either in responding to incidents or as part of our acquisition risk assessment strategy."*

*Brandon Glaze – Information Security Officer*

## ABOUT PACKETSLED

PacketSled is the network analytics platform of choice for security teams globally. Used by enterprises and MSSPs for real-time data analysis, threat hunting and incident response, the platform leverages continuous internal network monitoring and retrospection to provide network forensics and security analytics. Security teams can integrate PacketSled into their orchestration engine, SIEM, or use PacketSled independently to dramatically reduce the resources required to respond to persistent threats, malware, insider attacks, and nation state espionage efforts.

The company has been named an innovator in leading publications and by security analysts, including SC Magazine, earning a finalist award in 2018 for network visibility. For continuous product updates and industry news, please visit us at www.packetsled.com or call us at 1 (858) 225-2352 or follow us @packetsled.

## EXAMPLE OF NETWORK VISIBILITY IMPLEMENTATION

Figure-1 (below) comes from the PCI-Council's, "Guidance-PCI-DSS-Scoping-and-Segmentation_v1" document. It shows the 'CDE' and 'Shared Services' networks are "in-scope" and protected by firewalls as required by the Standard. The 'Corporate Lan' is not in PCI scope because there is no network route to the 'Shared Services' or 'CDE' networks based on router configuration.

To add network visibility to this network is a snap. A PacketSled sensor is deployed in the 'Shared Services' network, and a second sensor would be deployed in the 'CDE' network. This is shown in Figure-2 (below).

With this configuration (Figure -2 below), every network packet moving through these networks is recorded, analyzed, and visualized. This includes more than 63 protocols from network layers 2-7. This simple network addition now provides all of the benefits highlighted in Table-1 (below).

What happens if the 'Corporate Lan' is determined to be in PCI scope? This can happen if there is any route to the Corporate network from any PCI network determined to be 'In-Scope.' Figure-3 shows an example of this scenario.

**Figure 1**
(right)

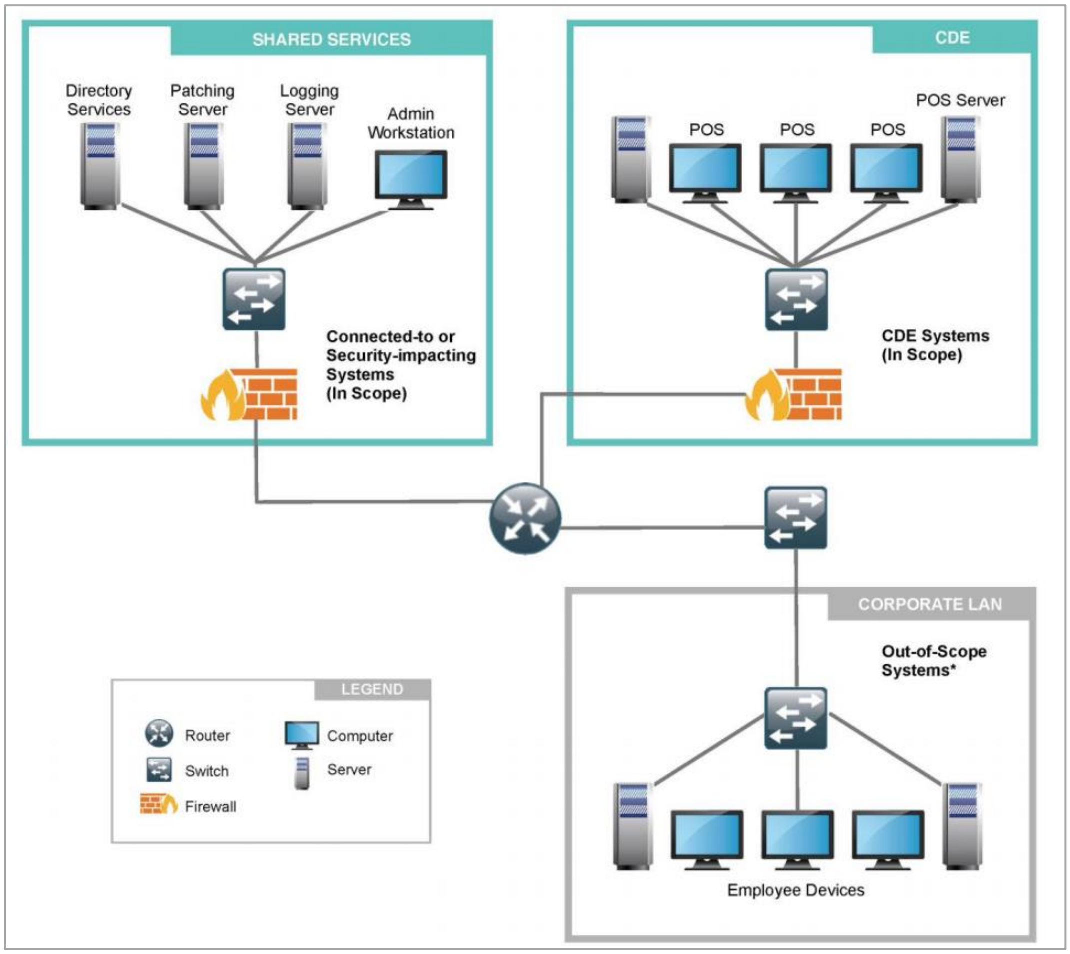
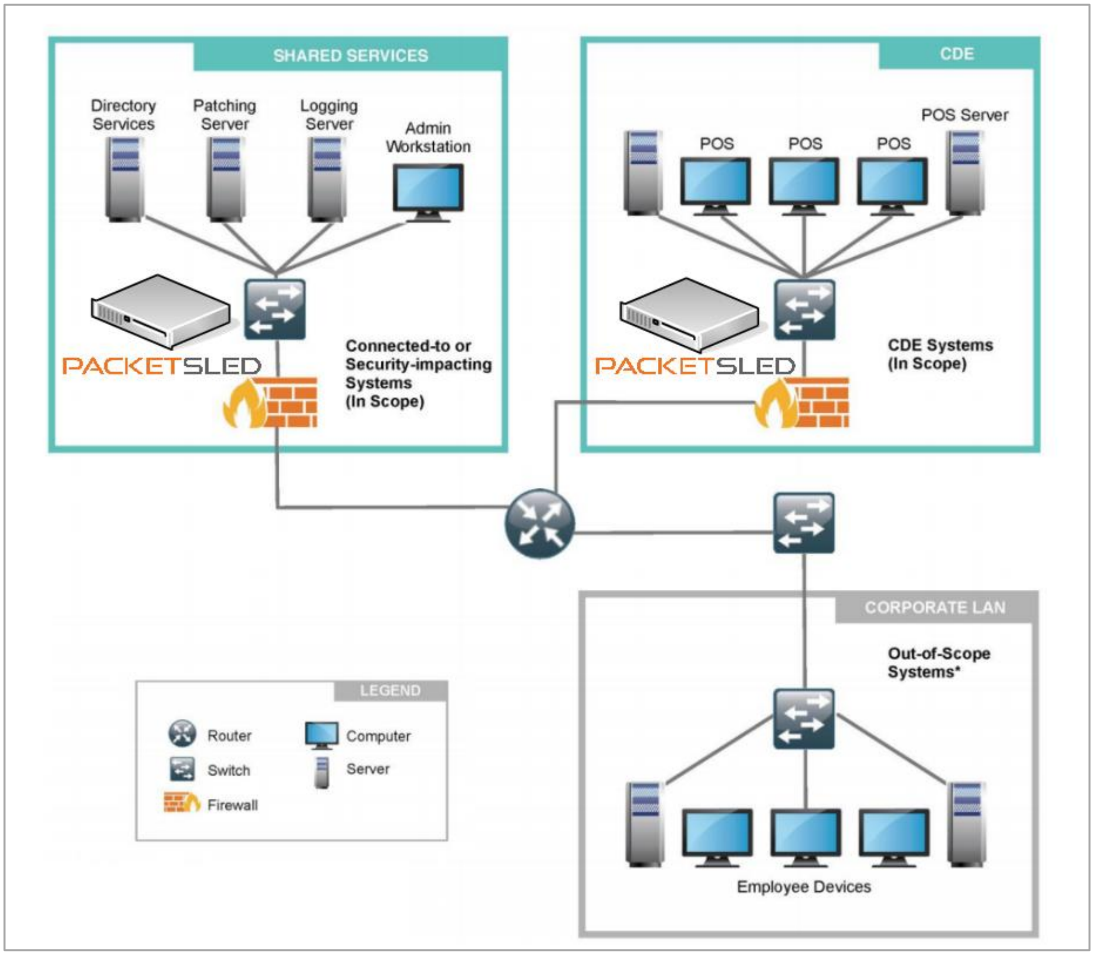


**Figure 2**
(right)



## SUMMARY

PacketSled sensors deployed in your PCI regulated environment not only provide continuous network visibility and full-packet capture as desired, but they make managing your complex PCI networks easier. Managing a PCI regulated environment is a tough task. Adding network visibility to the mix is a high-leverage action that can dramatically change the way you manage your PCI security controls.

| ROC Requirement | PacketSled Capabilities |
|---|---|
| **1. Install and maintain a firewall configuration to protect cardholder data** | |
| 1.1 - All | PS-Test, PS-Verify |
| 1.1.2 - 1.1.2a | PS-Verify |
| 1.1.3.a | PS-Verify |
| 1.1.4, 1.1.4.a, 1.1.4.c | PS-Verify |
| 1.1.6 - All | PS-Test, PS-Verify |
| 1.2 – 1.2.1 | PS-Test, PS-Verify |
| 1.2.1.a – 1.2.1.c | PS-Verify |
| 1.3 – 1.3.4 | PS-Test, PS-Verify |
| 1.3.5 | PS-Verify |
| 1.3.6 | PS-Verify |
| 1.3.7 | PS-Test, PS-Verify |
| 1.3.7a – 1.3.7.b | PS-Verify |
| 1.4 – All | PS-NA |
| **2. Do not use vendor defaults for system passwords and other security parameters.** | |
| 2.1 | PS-NA |
| 2.1.1.a | PS-NA |
| 2.2.1.b – 2.2.1.c | PS-Verify |
| 2.2.1.d – 2.2.1.e | PS-NA |
| 2.2 -2.2.c | PS-NA |
| 2.2.d – 2.2.3 | PS-Test, PS-Verify |
| 2.2.3.a | PS-NA |
| 2.2.3.b | PS-Test, PS-Verify |
| 2.2.4 – 2.2.4.c | PS-NA |
| 2.2.5 | PS-Test, PS-Verify |
| 2.3 – 2.3.c | PS-Test, PS-Verify |
| 2.3.d | PS-NA |
| 2.5 – 2.6 | PS-NA |
| **3. Protect stored cardholder data** | |
| 3.1 – 3.7 (CDE storage and encryption key storage and handling.) | PS-NA |
| **4. Encrypt transmission of cardholder data across open, public networks** | |

| **ROC Requirement** | **PacketSled Capabilities** |
|---|---|
| 4.1 – 4.2.a | PS-Test, PS-Verify |
| 4.2.b – 4.3 | PS-NA |
| **5. Protect all systems against malware, regularly update anti-virus software programs** | |
| 5.1 – 5.4 (Anti-Virus implementation) | PS-NA |
| **6. Develop and maintain secure systems and applications** | |
| 6.1 – 6.1.b | PS-NA |
| 6.2 | PS-Test, PS-Verify |
| 6.2.a | PS-NA |
| 6.2.b | PS-Test, PS-Verify |
| 6.2.3 – 6.2.3.d | PS-NA |
| 6.3.1 | PS-Test, PS-Verify |
| 6.3.1 – 6.4 | PS-NA |
| 6.4.1 – 6.4.1.b | PS-Test, PS-Verify |
| 6.4.2 – 6.4.3.b | PS-NA |
| 6.4.4 | PS-Test, PS-Verify |
| 6.4.4.a | PS-NA |
| 6.4.4.b | PS-Test, PS-Verify |
| 6.4.5 – 6.5.c | PS-NA |
| 6.5.1 – 6.5.2 | PS-Test, PS-Verify |
| 6.5.3 | PS-NA |
| 6.5.4 | PS-Test, PS-Verify |
| 6.5.5 | PS-NA |
| 6.5.6 – 6.5.9 | PS-Test, PS-Verify |
| 6.5.10 | PS-NA |
| 6.6 | PS-Test, PS-Verify |
| 6.7 | PS-NA |
| **7. Restrict access to cardholder data by business need to know** | |
| 7.1.A – 7.1.4 | PS-NA |
| 7.2 – 7.2.3 | PS-Test, PS-Verify |
| 7.3 | PS-NA |
| **8. Identify and authenticate access to system components** | |
| 8.1 – 8.1.b | PS-NA |

| ROC Requirement | PacketSled Capabilities |
|---|---|
| 8.1.1 | PS-Test |
| 8.1.2 | PS-NA |
| 8.1.3 – 8.1.3.a | PS-Test |
| 8.1.4 | PS-NA |
| 8.1.5 | PS-Test |
| 8.5.1.a – 8.5.1.b | PS-NA |
| 8.1.6 | PS-Test |
| 8.1.6.a – 8.1.7 | PS-NA |
| 8.1.8 | PS-Test |
| 8.2 – 8.2.1.b | PS-NA |
| 8.2.1.c | PS-Test |
| 8.2.1.d | PS-NA |
| 8.2.1.e | PS-Test |
| 8.2.2 – 8.2.3.1 | PS-NA |
| 8.3.1.a – 8.3.2.a | PS-Test |
| 8.4 – 8.6.c | PS-NA |
| 8.7 – 8.7.b | PS-Test, PS-Verify |
| 8.7.c – 8.8 | PS-NA |
| **9. Restrict physical access to cardholder data** | |
| 9.1 – 9.10 | PS-NA |
| **10. Track and monitor all access to network resources and cardholder data** | |
| 10.1 | PS-Test, PS-Verify |
| 10.2 – 10.2.2 | PS-NA |
| 10.2.3 – 10.2.7 | PS-Test, PS-Verify |
| 10.3 – 10.3.6 | PS-NA |
| 10.4 – 10.4.3 | PS-Test, PS-Verify |
| 10.5 – 10.9 | PS-NA |
| **11. Regularly test security systems and processes** | |
| 11.1 – 11.1.c | PS-Test, PS-Verify |
| 11.1.d – 11.6 | PS-NA |
| **12. Maintain a policy that addresses information security for all personnel** | |