

WHITE PAPER | JUNE 2017

# TEMPERED NETWORKS IDENTITY-DEFINED NETWORKING PLATFORM COMPLIANCE WITH PCI DSS V3.2

PRODUCT APPLICABILITY GUIDE TO  
ASSIST IN SUPPORTING PAYMENT CARD  
INDUSTRY DATA SECURITY STANDARD  
V3.2 COMPLIANCE

MARK BEDELL | PCNSE, SECURITY +

COALFIRE OPINION SERIES  
FINAL VERSION 1.0



COALFIRE

North America | Europe

877.224.8077 | [info@coalfire.com](mailto:info@coalfire.com) | [Coalfire.com](http://Coalfire.com)

# TABLE OF CONTENTS

<b>Executive Overview .....</b>	<b>3</b>
<b>Payment Card Industry Data Security Standard Overview (PCI DSS) .....</b>	<b>4</b>
Tempered Networks Identity-Defined Networking (IDN) .....	5
Tempered Networks – Conductor .....	5
Tempered Networks – HIP Services .....	6
Tempered Networks – HIPrelay .....	7
Use case #1: Point-of-Sale(POS) Sim Deployment .....	8
Use Case #1: POS Endpoint – Coalfire Lab Testing .....	9
Use case #2: Micro-segmentation Sim Deployment .....	10
Use Case #2: Micro-segmentation – Coalfire Lab Testing .....	11
Use Case #2: Micro-segmentation – Coalfire Lab Testing (Cont.) .....	12
<b>Tempered Networks IDN - PCI DSS 3.2 Requirements .....</b>	<b>13</b>
Requirement 1: Install and maintain a firewall configuration to protect cardholder data .....	13
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters .....	17
Requirement 4: Encrypt transmission of cardholder data across open, public networks .....	18
Requirement 10: Track and monitor all access to network resources and cardholder data .....	20
<b>Coalfire Opinion .....</b>	<b>22</b>
A Comment Regarding Regulatory Compliance .....	22
<b>References .....</b>	<b>22</b>
<b>Acknowledgements .....</b>	<b>22</b>

## EXECUTIVE OVERVIEW

One of the recommendations for organizations to obtain PCI DSS compliance is to ensure segmentation of the cardholder's data environment from the remainder of the network. This reduces the eventual scope of an assessment, cost of the assessment, and overall risk to an organization. Proper network segmentation will isolate systems that store, process, or transmit cardholder data, thereby restricting access to as few locations as possible.

Tempered Networks, founded in 2012, has introduced a method of securing and micro-segmenting any host or network with an architecture that is based on cryptographic identities rather than IP through their Identity-Defined (IDN) solution. The IDN solution is Tempered Networks' answer to establishing trust using cryptographic overlays.

In this Product Applicability Guide for Tempered Networks, Coalfire Systems (Coalfire) reviewed capability alignment with the Payment Card Industry Data Security Standard (PCI DSS) version 3.2, released in April, 2016. The review followed our standard methodology where we evaluate the specific PCI DSS technical controls that are addressed by Tempered Networks and make a determination of the product's capability to support those requirements. Our methodology is specifically directed by the guidance provided in the [PCI DSS Requirements and Security Assessment Procedures, Version 3.2, April 2016](#) document.

Based upon the findings obtained during our review, Coalfire concluded that the Tempered Networks' IDN solution **is effective** in meeting many of PCI DSS controls under PCI DSS requirements 1,2, 4, and 10.

In the following sections, this paper discusses in more specific detail the particular features of the Tempered Networks IDN solution that can be used to address the PCI DSS requirements for an implementing organization. To assist the Qualified Security Assessor (PCI DSS QSA) with a formal PCI evaluation, we provide detailed mapping of available features within the Tempered Networks' IDN to specific requirements in the PCI DSS framework.

For introductory purposes, a brief overview of the PCI DSS requirements follow in the next section.

# PAYMENT CARD INDUSTRY DATA SECURITY STANDARD OVERVIEW (PCI DSS)

Payment Card Industry Data Security Standard (PCI DSS) is a framework that defines baseline physical, technical, and operational security controls, defined as requirements and sub-requirements, necessary for protecting payment card account data. PCI DSS defines two categories of payment account data: cardholder data (CHD), which includes primary account number (PAN), cardholder name, expiration date, and service code; and Sensitive Authentication Data (SAD), which includes full track data (magnetic-stripe data or equivalent on a chip), Card Security Code (CAV2/CVC2/CVV2/CID), and personal identification numbers (PINs/PIN blocks) entered during the transaction.

PCI DSS applies to any organization that stores, processes, or transmits CHD. These organizations include (but are not limited to): merchants, payment processors, issuers, acquirers, and service providers. The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment (CDE). The CDE is comprised of people, processes, and technologies that store, process, or transmit CHD or SAD. PCI DSS defines 12 requirements designed to address the six PCI DSS objectives, as shown in this high-level overview:

**TABLE 1 - PCI DATA SECURITY STANDARD – HIGH-LEVEL OVERVIEW**

OBJECTIVE	REQUIREMENT
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Protect all systems against malware and regularly update anti-virus software or programs</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need to know</li> <li>8. Identify and authenticate access to system components</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security for all personnel</li> </ol>

## TEMPERED NETWORKS IDENTITY-DEFINED NETWORKING (IDN)

IDN is a unified networking and security architecture based on simple and highly scalable orchestration of cryptographic identities using the Host Identity Protocol (HIP). RFC 5201, which defines Host Identity Protocol, was published in 2008. The result of a Tempered Networks IDN deployment is a significant reduction in the overall network and system attack surface through device cloaking and simple trust-based segmentation, which isolates the reach of an attacker even if a device was compromised. Tempered Networks IDN fabric can be deployed on top of any IP network and requires few, if any, minor changes to the underlying network or security design. In this section, we provide an overview of the IDN architecture.

### Tempered Networks – Conductor

The Conductor is referred to as the orchestration engine and is the intelligence behind the IDN, providing centralized control of a deployment and the ability to instantly connect, secure, move, or disconnect any IP resource. The Conductor provisions encrypted overlay networks between HIPswitches and manages trust policies, statistics, and user accounts. The Conductor provides policy configuration, collects metrics, and enforces explicit trust relationships through device-based whitelisting based on unique cryptographic IDs (CIDs).

Below is an example of an IDN encrypted fabric and the connectivity through the Conductor:

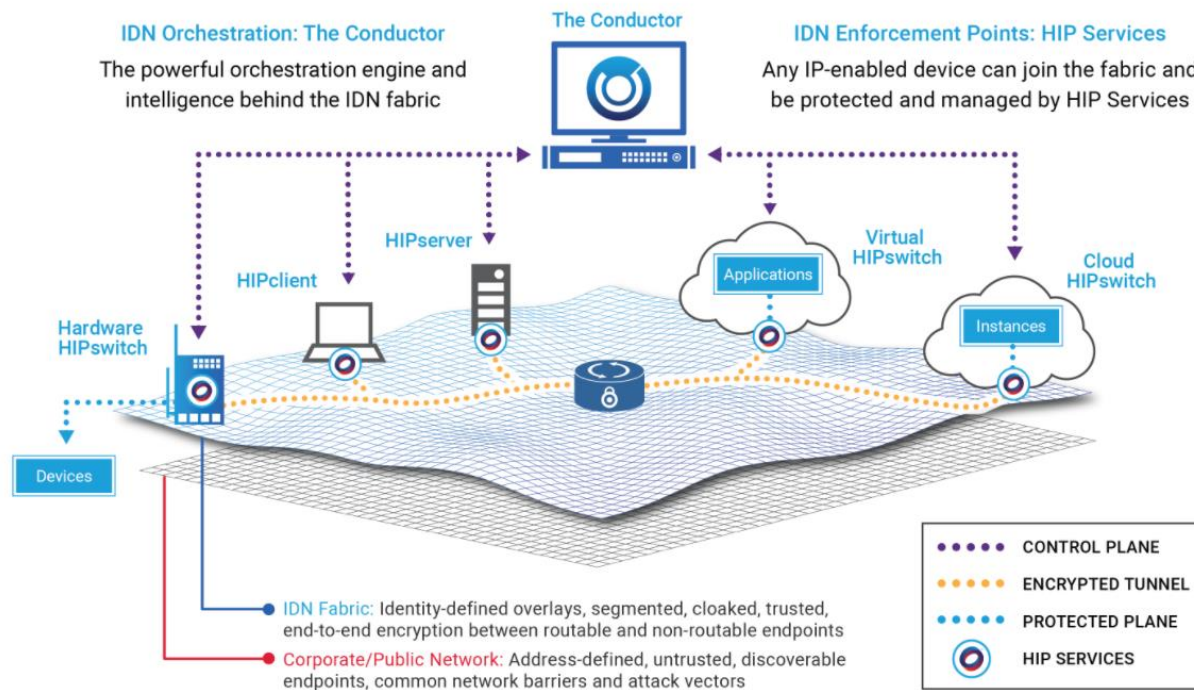


Figure 1 - Example of end-to-end encrypted overlay

Tempered Networks simplifies management of the HIPservices through the use of a RESTful API. Through the secure API, it is possible to also integrate the Conductor with security and network services, such as Active Directory, SIEMs, and monitoring tools. Instant quarantine can be automatically driven by events detected by SIEMs (e.g. Splunk), enabling organizations to build networks that respond to events in real-time. The Conductor's user interface is in a dashboard layout accessible via SSL, which makes for easy administration.

Below is a screen shot of the Conductor dashboard and connected HIPswitches:

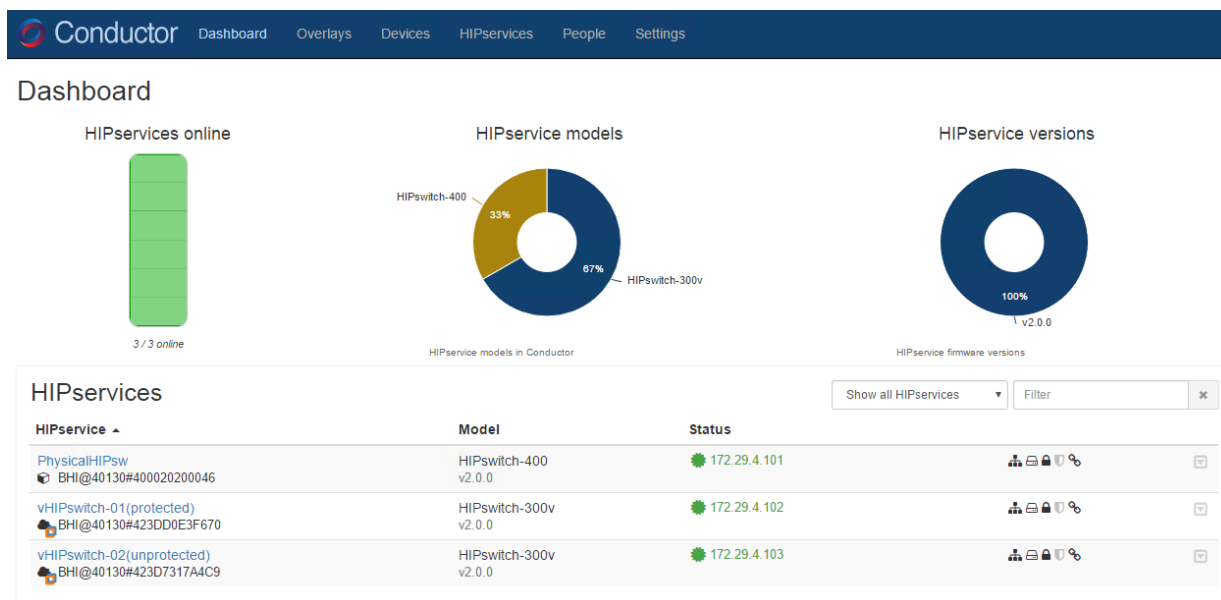


Figure 2 - Conductor dashboard

## Tempered Networks – HIP Services

Tempered Networks' method for protecting and managing devices across a network is binding a provable cryptographic identity to a machine with HIP Services. HIP Services are software products delivered in different form factors that act as IDN enforcement endpoints and support their service principle that they can secure networks for any device at any location. HIP Services can be deployed as physical appliances, virtual instances, cloud workloads, and software installed on a client or server or can be embedded within an application. HIP Services are the mechanism that enforces security policy within the IDN fabric.

Below are some of the deployment options:

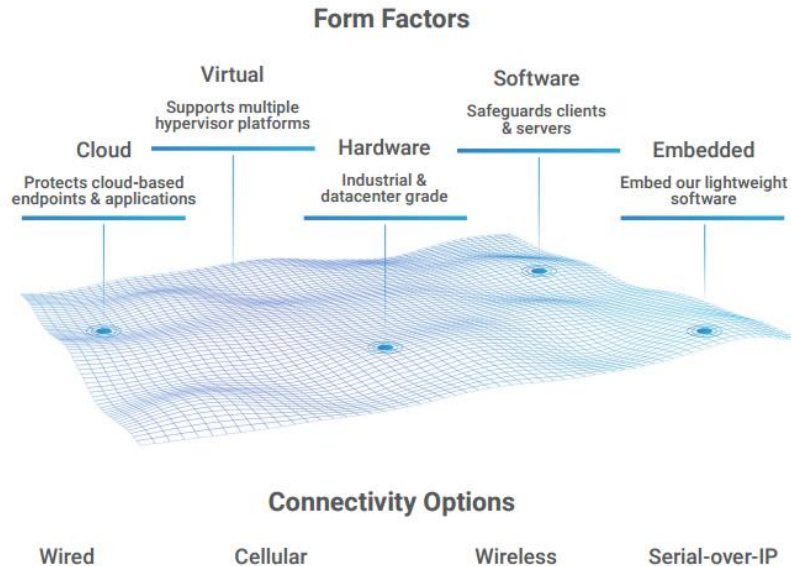


Figure 3 – Tempered Networks – HIP deployment options

HIP Services establish encrypted tunnels to each other using AES-256 encryption over a shared (public) network. Each HIP Service has a unique public/private 2048-bit RSA key pair and a Tempered Networks signed certificate (or customer signed certificate) that establishes a chain of trust between a Conductor and HIP Services to authenticate to each other. Customer signed certificates can be used in place of Tempered Networks signed certificates. HIP Services cache their current policies and configuration to persistent storage, so in the event a Conductor becomes unavailable, they continue to operate using their cached policies and configuration. Local devices connect directly to any HIP Service and can be moved to remote locations regardless of IP addressing.

### Tempered Networks – HIPrelay

HIPrelay, an add-on feature to a HIPswitch, is an identity-based router that controls traffic between HIPswitches, allowing them to securely communicate with each other when direct communication is not possible. It gives the ability to securely move an organizations trust perimeter across any public, private, or hybrid network, with host-to-host encryption. The IP schema used and whether a system is static or dynamically addressed becomes irrelevant. The HIPrelay add-on is available on HIPswitch-400 series hardware, HIPswitch-300 virtual, and cloud platforms.

Below is an example of a typical HIPrelay deployment:

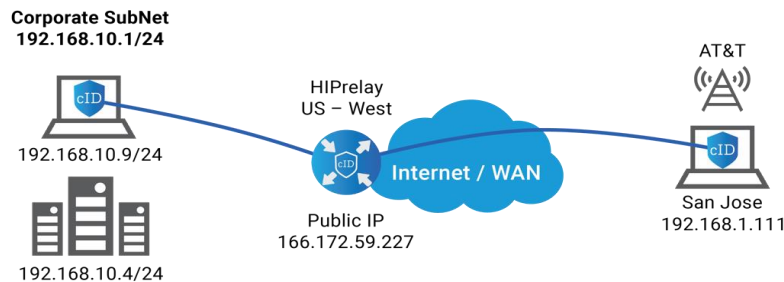


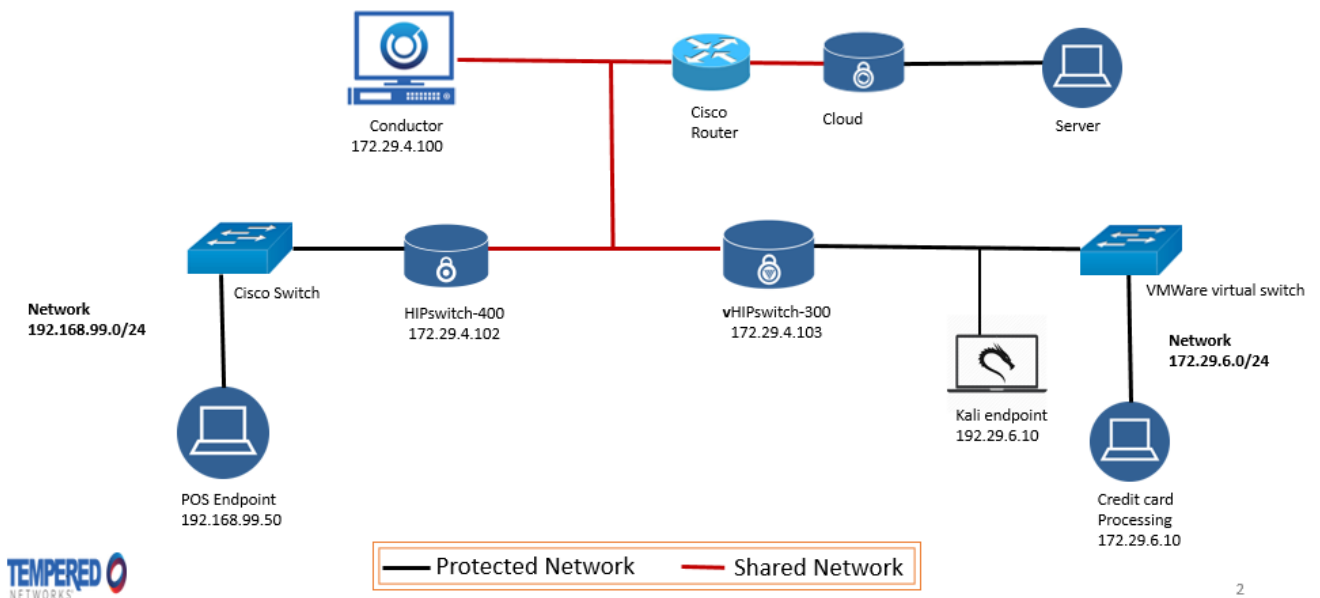
Figure 4 - HIPrelay deployment example



## USE CASE #1: POINT-OF-SALE(POS) SIM DEPLOYMENT

This use case depicts a typical end-to-end POS merchant client-server transaction network, deploying a HIPswitch at the merchant front-end and a virtual HIPswitch in a virtualized enclave at the cloud service providers' CHD processing back-end. In this scenario, a Kali endpoint infiltrated the protected (inside) network and an NMAP scan was the tool utilized for identifying vulnerabilities. The Kali host was also leveraged for demonstrating how trust is established between two local devices on the same network segment. Product applicability was determined by enabling/disabling HIP tunneling.

### Product Applicability – C&V Lab Use Case #1- POS endpoint CDE



2

Figure 5 - Use case #1 - lab design



## Use Case #1: POS Endpoint – Coalfire Lab Testing

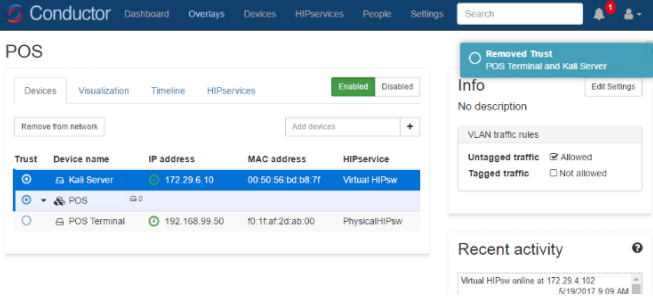
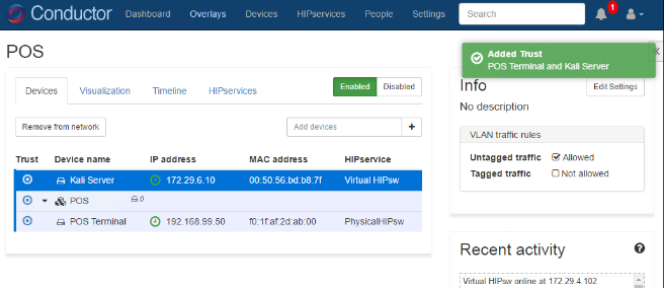
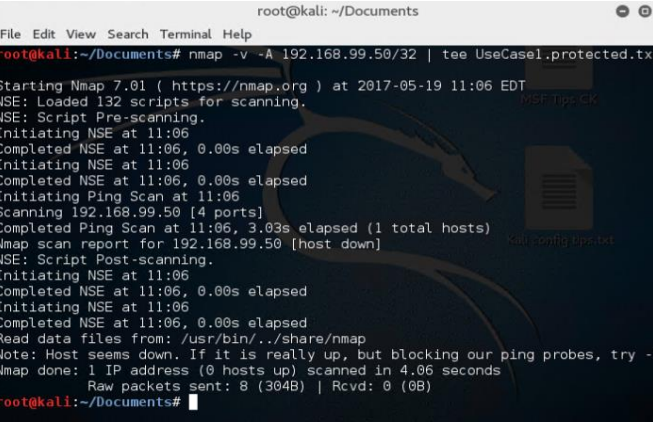
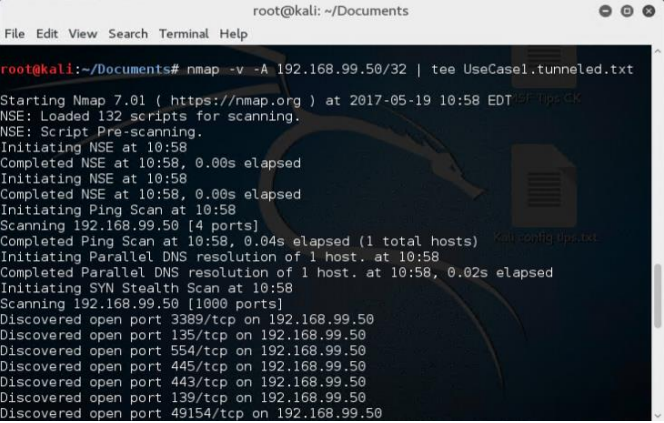
TRUST – DISABLED: KALI SCANNING POS ENDPOINT	TRUST – ENABLED: KALI SCANNING POS ENDPOINT																																								
 <table border="1"> <thead> <tr> <th>Trust</th> <th>Device name</th> <th>IP address</th> <th>MAC address</th> <th>HiPService</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/></td> <td>Kali Server</td> <td>172.29.6.10</td> <td>00:50:56:bd:b8:7f</td> <td>Virtual HiPaw</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td>POS</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="radio"/></td> <td>POS Terminal</td> <td>192.168.99.50</td> <td>10:1f:af:2d:ab:00</td> <td>PhysicalHiPaw</td> </tr> </tbody> </table>	Trust	Device name	IP address	MAC address	HiPService	<input type="radio"/>	Kali Server	172.29.6.10	00:50:56:bd:b8:7f	Virtual HiPaw	<input checked="" type="radio"/>	POS				<input type="radio"/>	POS Terminal	192.168.99.50	10:1f:af:2d:ab:00	PhysicalHiPaw	 <table border="1"> <thead> <tr> <th>Trust</th> <th>Device name</th> <th>IP address</th> <th>MAC address</th> <th>HiPService</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/></td> <td>Kali Server</td> <td>172.29.6.10</td> <td>00:50:56:bd:b8:7f</td> <td>Virtual HiPaw</td> </tr> <tr> <td><input checked="" type="radio"/></td> <td>POS</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="radio"/></td> <td>POS Terminal</td> <td>192.168.99.50</td> <td>10:1f:af:2d:ab:00</td> <td>PhysicalHiPaw</td> </tr> </tbody> </table>	Trust	Device name	IP address	MAC address	HiPService	<input type="radio"/>	Kali Server	172.29.6.10	00:50:56:bd:b8:7f	Virtual HiPaw	<input checked="" type="radio"/>	POS				<input type="radio"/>	POS Terminal	192.168.99.50	10:1f:af:2d:ab:00	PhysicalHiPaw
Trust	Device name	IP address	MAC address	HiPService																																					
<input type="radio"/>	Kali Server	172.29.6.10	00:50:56:bd:b8:7f	Virtual HiPaw																																					
<input checked="" type="radio"/>	POS																																								
<input type="radio"/>	POS Terminal	192.168.99.50	10:1f:af:2d:ab:00	PhysicalHiPaw																																					
Trust	Device name	IP address	MAC address	HiPService																																					
<input type="radio"/>	Kali Server	172.29.6.10	00:50:56:bd:b8:7f	Virtual HiPaw																																					
<input checked="" type="radio"/>	POS																																								
<input type="radio"/>	POS Terminal	192.168.99.50	10:1f:af:2d:ab:00	PhysicalHiPaw																																					
KALI SCAN RESULT: DENIED	KALI SCAN RESULT: PERMITTED																																								
 <pre> root@kali: ~/Documents File Edit View Search Terminal Help root@kali:~/Documents# nmap -v -A 192.168.99.50/32   tee UseCase1.protected.txt Starting Nmap 7.01 ( https://nmap.org ) at 2017-05-19 11:06 EDT NSE: Loaded 132 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 11:06 Completed NSE at 11:06, 0.00s elapsed Initiating NSE at 11:06 Completed NSE at 11:06, 0.00s elapsed Initiating Ping Scan at 11:06 Scanning 192.168.99.50 [4 ports] Completed Ping Scan at 11:06, 3.03s elapsed (1 total hosts) Nmap scan report for 192.168.99.50 [host down] NSE: Script Post-scanning. Initiating NSE at 11:06 Completed NSE at 11:06, 0.00s elapsed Initiating NSE at 11:06 Completed NSE at 11:06, 0.00s elapsed Read data files from: /usr/bin/./share/nmap Note: Host seems down. If it is really up, but blocking our ping probes, try -Ph Nmap done: 1 IP address (0 hosts up) scanned in 4.06 seconds Raw packets sent: 8 (3048)   Rcvd: 0 (0B) root@kali:~/Documents#     </pre>	 <pre> root@kali: ~/Documents File Edit View Search Terminal Help root@kali:~/Documents# nmap -v -A 192.168.99.50/32   tee UseCase1.tunneled.txt Starting Nmap 7.01 ( https://nmap.org ) at 2017-05-19 10:58 EDT NSE: Loaded 132 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 10:58 Completed NSE at 10:58, 0.00s elapsed Initiating NSE at 10:58 Completed NSE at 10:58, 0.00s elapsed Initiating Ping Scan at 10:58 Scanning 192.168.99.50 [4 ports] Completed Ping Scan at 10:58, 0.04s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 10:58 Completed Parallel DNS resolution of 1 host. at 10:58, 0.02s elapsed Initiating SYN Stealth Scan at 10:58 Scanning 192.168.99.50 [1000 ports] Discovered open port 3389/tcp on 192.168.99.50 Discovered open port 135/tcp on 192.168.99.50 Discovered open port 554/tcp on 192.168.99.50 Discovered open port 445/tcp on 192.168.99.50 Discovered open port 443/tcp on 192.168.99.50 Discovered open port 139/tcp on 192.168.99.50 Discovered open port 49154/tcp on 192.168.99.50     </pre>																																								

Figure 6 – Coalfire lab testing (Use case #1)

## USE CASE #2: MICRO-SEGMENTATION SIM DEPLOYMENT

The following lab testing demonstrates a form of micro-segmentation that is achieved through encrypted communication between hosts, residing at different locations, within the same IP subnet. Despite the separate physical locations between these devices, they can be cloaked by the HIPswitch. Trust is enabled by the Conductor when locally connected devices are added to the crypto overlay (HIP tunnel). This use case displays three scenarios utilizing a single architecture – Kali scan from PROTECTED with no HIP tunnel or trust, Kali scan from PROTECTED with HIP tunnel and trust, and Kali scan from SHARED with HIP tunnel enabled/disabled.

### Product Applicability – C&V Lab Use Case #2- Micro-segmentation

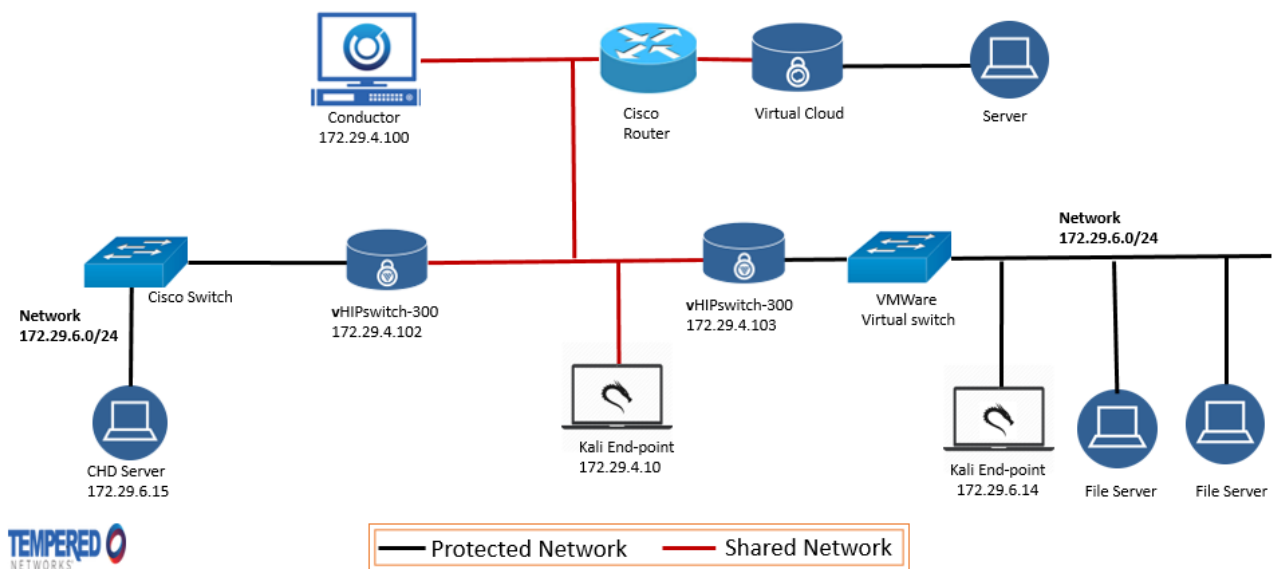


Figure 7 - Use case #2 - lab design

## Use Case #2: Micro-segmentation – Coalfire Lab Testing

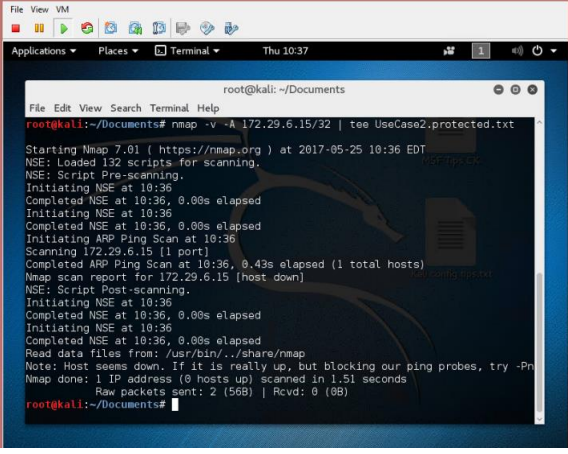
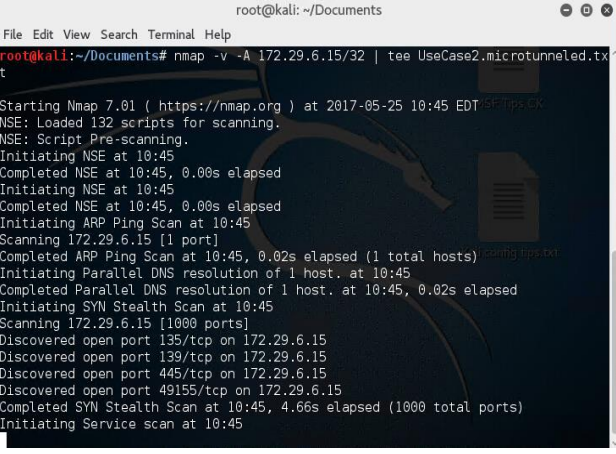
TRUST DISABLED: KALI - NO HIP TUNNEL, NO MICRO-SEGMENTATION	TRUST ENABLED: KALI – HIP TUNNEL, MICRO-SEGMENTATION																																								
<p>Micro-segmentation</p> <p>Devices Visualization Timeline HIPservices <b>Enabled</b> Disabled</p> <p>Remove from network Add devices +</p> <table border="1"> <thead> <tr> <th>Trust</th> <th>Device name</th> <th>IP address</th> <th>MAC address</th> <th>HIPservice</th> </tr> </thead> <tbody> <tr> <td>⊙</td> <td>AD server</td> <td>172.29.6.14</td> <td>00:50:56:bd:ed:65</td> <td>vHIPswitch-02(unprotected)</td> </tr> <tr> <td>⊙</td> <td>CHD server</td> <td>172.29.6.15</td> <td>00:50:56:bd:d8:8c</td> <td>vHIPswitch-01(protected)</td> </tr> <tr> <td>⊙</td> <td>Kali Linux</td> <td>172.29.6.10</td> <td>00:50:56:bd:b6:7f</td> <td>vHIPswitch-02(unprotected)</td> </tr> </tbody> </table>	Trust	Device name	IP address	MAC address	HIPservice	⊙	AD server	172.29.6.14	00:50:56:bd:ed:65	vHIPswitch-02(unprotected)	⊙	CHD server	172.29.6.15	00:50:56:bd:d8:8c	vHIPswitch-01(protected)	⊙	Kali Linux	172.29.6.10	00:50:56:bd:b6:7f	vHIPswitch-02(unprotected)	<p>Micro-segmentation</p> <p>Devices Visualization Timeline HIPservices <b>Enabled</b> Disabled</p> <p>Remove from network Add devices +</p> <table border="1"> <thead> <tr> <th>Trust</th> <th>Device name</th> <th>IP address</th> <th>MAC address</th> <th>HIPservice</th> </tr> </thead> <tbody> <tr> <td>⊙</td> <td>AD server</td> <td>172.29.6.14</td> <td>00:50:56:bd:ed:65</td> <td>vHIPswitch-02(unprotected)</td> </tr> <tr> <td>⊙</td> <td>CHD server</td> <td>172.29.6.15</td> <td>00:50:56:bd:d8:8c</td> <td>vHIPswitch-01(protected)</td> </tr> <tr> <td>⊙</td> <td>Kali Linux</td> <td>172.29.6.10</td> <td>00:50:56:bd:b6:7f</td> <td>vHIPswitch-02(unprotected)</td> </tr> </tbody> </table>	Trust	Device name	IP address	MAC address	HIPservice	⊙	AD server	172.29.6.14	00:50:56:bd:ed:65	vHIPswitch-02(unprotected)	⊙	CHD server	172.29.6.15	00:50:56:bd:d8:8c	vHIPswitch-01(protected)	⊙	Kali Linux	172.29.6.10	00:50:56:bd:b6:7f	vHIPswitch-02(unprotected)
Trust	Device name	IP address	MAC address	HIPservice																																					
⊙	AD server	172.29.6.14	00:50:56:bd:ed:65	vHIPswitch-02(unprotected)																																					
⊙	CHD server	172.29.6.15	00:50:56:bd:d8:8c	vHIPswitch-01(protected)																																					
⊙	Kali Linux	172.29.6.10	00:50:56:bd:b6:7f	vHIPswitch-02(unprotected)																																					
Trust	Device name	IP address	MAC address	HIPservice																																					
⊙	AD server	172.29.6.14	00:50:56:bd:ed:65	vHIPswitch-02(unprotected)																																					
⊙	CHD server	172.29.6.15	00:50:56:bd:d8:8c	vHIPswitch-01(protected)																																					
⊙	Kali Linux	172.29.6.10	00:50:56:bd:b6:7f	vHIPswitch-02(unprotected)																																					
KALI SCAN RESULT: DENIED	KALI SCAN RESULT: PERMITTED																																								
 <pre> root@kali: ~/Documents File Edit View Search Terminal Help root@kali:~/Documents# nmap -v -A 172.29.6.15/32   tee UseCase2.protected.txt Starting Nmap 7.01 ( https://nmap.org ) at 2017-05-25 10:36 EDT NSE: Loaded 132 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 10:36 Completed NSE at 10:36, 0.00s elapsed Initiating NSE at 10:36 Completed NSE at 10:36, 0.00s elapsed Initiating ARP Ping Scan at 10:36 Scanning 172.29.6.15 [1 port] Completed ARP Ping Scan at 10:36, 0.43s elapsed (1 total hosts) Nmap scan report for 172.29.6.15 [host down] NSE: Script Post-scanning. Initiating NSE at 10:36 Completed NSE at 10:36, 0.00s elapsed Initiating NSE at 10:36 Completed NSE at 10:36, 0.00s elapsed Read data files from: /usr/bin/./share/nmap Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn Nmap done: 1 IP address (0 hosts up) scanned in 1.51 seconds Raw packets sent: 2 (56B)   Rcvd: 0 (0B) root@kali:~/Documents#     </pre>	 <pre> root@kali: ~/Documents File Edit View Search Terminal Help root@kali:~/Documents# nmap -v -A 172.29.6.15/32   tee UseCase2.microtunnelled.txt Starting Nmap 7.01 ( https://nmap.org ) at 2017-05-25 10:45 EDT NSE: Loaded 132 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 10:45 Completed NSE at 10:45, 0.00s elapsed Initiating NSE at 10:45 Completed NSE at 10:45, 0.00s elapsed Initiating ARP Ping Scan at 10:45 Scanning 172.29.6.15 [1 port] Completed ARP Ping Scan at 10:45, 0.02s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 10:45 Completed Parallel DNS resolution of 1 host. at 10:45, 0.02s elapsed Initiating SYN Stealth Scan at 10:45 Scanning 172.29.6.15 [1000 ports] Discovered open port 135/tcp on 172.29.6.15 Discovered open port 139/tcp on 172.29.6.15 Discovered open port 445/tcp on 172.29.6.15 Discovered open port 49155/tcp on 172.29.6.15 Completed SYN Stealth Scan at 10:45, 4.66s elapsed (1000 total ports) Initiating Service scan at 10:45     </pre>																																								

Figure 8 – Coalfire lab testing results (Use case #2)

## Use Case #2: Micro-segmentation – Coalfire Lab Testing (Cont.)

**KALI FROM SHARED NET- HIP TUNNEL ENABLED / DISABLED**

**\*\*Previous Conductor screenshots apply\*\***

**KALI SCAN RESULT: DENIED**




```
root@kali: ~/Documents
File Edit View Search Terminal Help
root@kali:~/Documents# nmap -v -A 172.29.6.15/32 | tee UseCase2.fromshared.txt
Starting Nmap 7.01 ( https://nmap.org ) at 2017-06-16 19:05 EDT
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Initiating Ping Scan at 19:05
Scanning 172.29.6.15 [4 ports]
Completed Ping Scan at 19:05, 3.04s elapsed (1 total hosts)
Nmap scan report for 172.29.6.15 [host down]
NSE: Script Post-scanning.
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Initiating NSE at 19:05
Completed NSE at 19:05, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 4.81 seconds
Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
root@kali:~/Documents# nmap -v -A 172.29.6.15/32 | tee UseCase2.fromshared-6.14.txt
```

Figure 9 – Coalfire lab testing results (Use case #2)

## TEMPERED NETWORKS IDN - PCI DSS 3.2 REQUIREMENTS


Although PCI DSS v3.2 requirements define baseline technical, physical, and operational security controls necessary for protecting payment card account data, the Tempered Networks IDN implements only technical controls to collect activity data and ultimately provide detection of, and protection from, threats to the implementing organization. Non-technical controls were not reviewed against Tempered Networks.

Below is a brief description of categories used to identify the coverage status of specific PCI DSS v3.2 requirements:

-  **Available Capability** – The capabilities to satisfy the requirement are available within the Tempered Networks IDN.
-  **Partially Supported Capability** – The features available in the Tempered Networks IDN can be utilized by the implementing organization to partially satisfy the specifications in the requirement.
- [ ] **Not Applicable/Support Not Available** – The requirement is not supported or provided by the Tempered Networks IDN or is a process requirement that is exclusively the responsibility of the implementing organization.
-  **Applicable/Not Supported** – The requirement is not supported or available within the Tempered Networks IDN.

### REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

TABLE 1 - PCI DSS REQUIREMENT 1






PCI DSS REQUIREMENT	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE	SUPPORTED
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	Not Applicable.  This is a process requirement that is the responsibility of the implementing organization.	
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	1.1.4.c 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, per the network diagrams.	Partially Supported Capability.  A HIPswitch has a built-in firewall but is not intended as a perimeter firewall. Implicit deny-all is enforced. Only authenticated and authorized HIP tunnels are allowed.	





		It is the host networks' responsibility to secure the Internet perimeter.	
<b>1.1.5</b> Description of groups, roles, and responsibilities for management of network components	<b>1.1.5.a</b> Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.	Not Applicable.  This is a process requirement that is the responsibility of the implementing organization.	
<b>1.2</b> Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	<b>1.2</b> Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment:	Available Capability.  Deny-by-default policy is applied, unless a machine is explicitly authorized to communicate within a trust network.	✓
<b>1.2.1</b> Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	<b>1.2.1.a</b> Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.	Available Capability.  A deny-by-default policy is applied after the SPI firewall is enabled until a trust relationship is established between host devices across a shared network.	✓
	<b>1.2.1.b</b> Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.	Available Capability.  A deny-by-default policy is applied after the SPI firewall is enabled until a trust relationship is established between host devices across a shared network.	✓
	<b>1.2.1.c</b> Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	Available Capability.  A deny-by-default policy is applied after the SPI firewall is enabled until a trust relationship is established between host devices across a shared network.	✓

1.2.2 Secure and synchronize router configuration files.	1.2.2.a Examine router configuration files to verify they are secured from unauthorized access.	Available Capability.	✓
	1.2.2.b Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted).	Available Capability. All HIP Services are synchronized immediately with the Conductor at start-up with policy changes. The policy on each HIPswitch is static until it receives a policy change from the conductor.	✓
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	1.2.3.a Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the CDE.	Not Applicable.  This is the responsibility of the implementing organization, which provides boundary protection.	
	1.2.3.b Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Available Capability. Deny-by-default policy is applied, unless a machine is explicitly authorized to communicate within a trust network.	✓
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	1.3 Examine firewall and router configurations—including, but not limited to, the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment.	Not Applicable.  Best practices for restricting inbound network access is a primary responsibility of the implementing organization who manages the ports, protocols, and services for network security at the perimeter.	
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	1.3.1 Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Partially Supported Capability.  Each HIPswitch has a SPI firewall that can be configured with a whitelist using custom rules to allow incoming connections to a local server. However, these incoming	✓








		connections are within encrypted overlay.	
<b>1.3.2</b> Limit inbound Internet traffic to IP addresses within the DMZ.	<b>1.3.2</b> Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.	Partially Supported Capability.  Each HIPswitch has a SPI firewall that can be configured with a whitelist using custom rules to allow incoming connections to a local server. However, these incoming connections are within encrypted overlay.	
<b>1.3.3</b> Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	<b>1.3.3</b> Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ.	Available Capability.  The IDN architecture is based on crypto IDs and not IP addresses to identify local devices. The Conductor can also apply a feature to prevent MAC spoofing.	
<b>1.3.4</b> Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	<b>1.3.4</b> Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	Available Capability.  An encrypted overlay provides explicit trust for devices behind HIPswitches. If required, a HIPswitch SPI firewall can also filter connections.	
<b>1.3.5</b> Permit only "established" connections into the network.	<b>1.3.5</b> Examine firewall and router configurations to verify that the firewall permits only established connections into the internal network and denies any inbound connections not associated with a previously established session.	Available Capability.  HIPswitches enforce a deny-by-default inbound policy.	
<b>1.3.6</b> Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	<b>1.3.6</b> Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	Available Capability.  CHD system access can be restricted to only machines across the crypto overlay and isolated from hosts in untrusted networks.	

<p><b>1.3.7</b> Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: Network Address Translation (NAT) Placing servers containing cardholder data behind proxy servers/firewalls, Removal or filtering of route advertisements for private networks that employ registered addressing, Internal use of RFC1918 address space instead of registered addresses.</p>	<p><b>1.3.7.a</b> Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.</p>	<p>Available Capability.</p> <p>HIPswitches have an external IP address to mask the real IP address of a local device. NAT is used in conjunction with HIPswitch subnet routing to route between different subnets over the shared network.</p>	
	<p><b>1.3.7.b</b> Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized.</p>	<p>Available Capability</p> <p>CHD system access can be restricted to only machines across the crypto overlay and isolated from hosts in untrusted networks.</p>	

**REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS**


TABLE 2 - PCI DSS REQUIREMENT 2

PCI DSS REQUIREMENT	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE	SUPPORTED
<p><b>2.1</b> Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol</p>	<p><b>2.1a</b> Choose a system sample of components and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed.</p>	<p>Available Capability.</p> <p>The local admin account can have password changed from default. Confirmed in lab.</p>	
<p><b>2.3</b> Encrypt all non-console administrative access using strong cryptography. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.</p>	<p><b>2.3.a</b> Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.</p>	<p>Available Capability.</p> <p>SSL access is the primary form of management access to the Conductor appliance which is the single point of access for all connected HIPswitches.</p>	

	<p><b>2.3.b</b> Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access.</p>	<p>Available Capability.</p> <p>Only secure methods are available for remote administrative access.</p>	
	<p><b>2.3.c</b> Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.</p>	<p>Available Capability.</p> <p>Confirmed. Each system admin can use SSL for the conductor's web-based user interface.</p>	
<p><b>2.5</b> Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties</p>	<p><b>2.5</b> Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are:</p> <ul style="list-style-type: none"> <li>• Documented,</li> <li>• In use, and</li> <li>• Known to all affected parties</li> </ul>	<p>Partially Supported Capability.</p> <p>The vendor provides default credentials in the admin guide. The implementing organization has the responsibility to manage the Conductor account.</p>	
<p><b>2.6</b> Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers</p>	<p><b>2.6</b> Perform testing procedures A1.1 through A1.4 detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.</p>	<p>Not Applicable.</p> <p>This is the responsibility of the hosting cloud service provider.</p>	

**REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS**

TABLE 3 - PCI DSS REQUIREMENT 4

PCI DSS REQUIREMENT	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE	SUPPORTED
<p><b>4.1</b> Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open,</p>	<p><b>4.1.a</b> Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify</p>	<p>Available Capability.</p> <p>The basis of the IDN crypto overlay is 2048-bit encryption.</p>	

<p>public networks, including the following:</p> <ul style="list-style-type: none"> <li>• Only trusted keys and certificates are accepted.</li> <li>• The protocol in use only supports secure versions or configurations.</li> <li>• The encryption strength is appropriate for the encryption methodology in use.</li> </ul>	<p>the use of security protocols and strong cryptography for all locations.</p>		
	<p><b>4.1.b</b> Review documented policies and procedures to verify processes are specified for the following:</p> <ul style="list-style-type: none"> <li>• For acceptance of only trusted keys and/or certificates</li> <li>• For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported)</li> <li>• For implementation of proper encryption strength per the encryption methodology in use</li> </ul>	<p>Available Capability.</p> <p>End-to-end encryption for the IDN fabric is not optional for the system/user. Default settings are AES 256 SHA2.</p>	✓
	<p><b>4.1.d</b> Examine keys and certificates to verify that only trusted keys and/or certificates are accepted.</p>	<p>Available Capability.</p> <p>The HIPswitches employ self-signed public certificates.</p>	✓
	<p><b>4.1.e</b> Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.</p>	<p>Available Capability.</p> <p>The encryption key size applied, by default, already meets NIST recommend guidelines. Default - AES 256.</p>	✓
	<p><b>4.1.f</b> Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use.</p>	<p>Available Capability.</p> <p>The encryption key size applied, by default, already meets NIST recommend guidelines. Default is 256</p>	✓
<p><b>4.1.1</b> Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.</p>	<p><b>4.1.1</b> Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment.</p>	<p>Not Applicable.</p> <p>Although the HIPswitches do not provide wireless encryption for authentication, once a wireless session is initiated, the data will be encrypted over a HIP tunnel between two HIPswitches.</p>	

*Note: Although HIPswitches do not provide wireless encryption for client authentication, once a wireless session is initiated, HIP tunnels can employ strong encryption (AES 256) within the CDE. HIP Services encryption cannot be disabled.*

## REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

TABLE 4 - PCI DSS REQUIREMENT 10

PCI DSS REQUIREMENT	TESTING PROCEDURES	COMPLIANCE AND GUIDANCE	SUPPORTED
<b>10.1</b> Implement audit trails to link all access to system components to each individual user.	<b>10.1</b> Verify, through observation and interviewing the system administrator, that: <ul style="list-style-type: none"> <li>• Audit trails are enabled and active for system components.</li> <li>• Access to system components is linked to individual users.</li> </ul>	Available Capability.  Internal logging for changes was verified.	✓
<b>10.2</b> Implement automated audit trails for all system components to reconstruct the following events:	<b>10.2</b> Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	See sub-controls below.	
<b>10.2.2</b> All actions taken by any individual with root or administrative privileges	<b>10.2.2</b> Verify all actions taken by any individual with root or administrative privileges are logged.	Available Capability.  Internal logging for changes was verified.	✓
<b>10.2.4</b> Invalid logical access attempts	<b>10.2.4</b> Verify invalid logical access attempts are logged.	Available Capability.  Internal logging for changes was verified.	✓
<b>10.2.5</b> Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	<b>10.2.5.a</b> Verify use of identification and authentication mechanisms is logged.	Available Capability.  Internal logging for changes was verified.	✓
	<b>10.2.5.b</b> Verify all elevation of privileges is logged.	Available Capability  Internal logging for changes was verified.	✓
	<b>10.2.5.c</b> Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	Available Capability.  Internal logging for changes was verified.	✓
<b>10.3</b> Record at least the following audit trail entries for all system components for each event:	<b>10.3</b> Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:	See sub-controls below.	

<b>10.3.1</b> User identification	<b>10.3.1</b> Verify user identification is included in log entries.	Available Capability This capability was confirmed in IDN admin guide.	✓
<b>10.3.2</b> Type of event	<b>10.3.2</b> Verify type of event is included in log entries.	Available Capability This was verified after reviewing system log .	✓
<b>10.3.3</b> Date and time	<b>10.3.3</b> Verify date and time stamp is included in log entries.	Available Capability. This was verified after reviewing system log.	✓
<b>10.3.4</b> Success or failure indication	<b>10.3.4</b> Verify success or failure indication is included in log entries.	Available Capability. This was verified after reviewing system log.	✓
<b>10.3.5</b> Origination of event	<b>10.3.5</b> Verify origination of event is included in log entries.	Not Applicable.	
<b>10.3.6</b> Identity or name of affected data, system component, or resource.	<b>10.3.6</b> Verify identity or name of affected data, system component, or resources is included in log entries.	Available Capability. This was verified after reviewing system log	✓
<b>10.4.3</b> Time settings are received from industry-accepted time sources	<b>10.4.3</b> Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock)	Not Supported.  Only a time-zone is an available option for NTP reference. HIPswitches synchronize time directly with Conductor.	X
<b>10.8</b> Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: <ul style="list-style-type: none"><li>• Firewalls</li><li>• IDS/IPS</li><li>• FIM</li><li>• Anti-virus</li><li>• Physical access controls</li><li>• Logical access controls</li><li>• Audit logging mechanism</li><li>• Segmentation controls (if used)</li></ul>	<b>10.8.a</b> Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: <ul style="list-style-type: none"><li>• Firewalls</li><li>• IDS/IPS</li><li>• FIM</li><li>• Anti-virus</li><li>• Physical access controls</li><li>• Logical access controls</li><li>• Audit logging mechanisms</li><li>• Segmentation controls</li></ul>	Not Applicable.  This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	



## COALFIRE OPINION

The Payment Card Industry Data Security Standard version 3.2 (PCI DSS v3.2) was developed to protect cardholder data (CHD) and sensitive authentication data (SAD) from loss, theft, and exploitation and has been mandated by the Card Brands since introduction in 2005. Technical product is used in conjunction with other measures to address information system security controls enumerated within the specific requirements of the standard.

In Coalfire's opinion, Tempered Networks Identity-Defined Networking (IDN) is effective in providing significant support for the key requirements and controls of PCI DSS and can assist in a comprehensive program of cyber-security for merchants, issuing banks, processors, services providers, and other entities required to comply with PCI DSS 3.2.

Coalfire's opinion is dependent on a number underlying presumptions, which are enumerated here:

- The implementing organization follows best practices when designing network perimeter protection.
- The implementing organization has resources properly trained to configure and deploy.
- Alignment of technical controls with actual PCI entity missions, roles, responsibilities, policies, procedures, baselines, mandates, etc.
- All type 1 (direct CHD storage, processing and transmission) and type 2 (supporting CHD systems) have anti-malware software installed and centrally managed.
- The installation of server and PC client operating systems following vendor best practices and recommended hardening after deployment.
- The presence and/or availability of IT staff at the payment card entity and any service providers as well.
- Although not required in PCI DSS, scope reduction by segmentation is a recommended method and supported by the product.

## A COMMENT REGARDING REGULATORY COMPLIANCE

Coalfire disclaims generic suitability of any product to cause a customer using that product to achieve regulatory compliance. ***Customers attain compliance through a Governance, Risk Management, and Compliance (GRC) program, not via the use of a specific product. This is true for PCI DSS compliance required entities as well as for customers targeting compliance with other regulations.***

## REFERENCES

1. PCI Security Standards Council, LLC. (April 2016). [Payment Card Industry Data Security Standard version 3.2, Requirements and Security Assessment Guidelines](#)
2. Tempered Networks (2017). [IDN Administrator Guide](#)
3. Tempered Networks (2017). [www.temperednetworks.com](http://www.temperednetworks.com) Product Brochures

## ACKNOWLEDGEMENTS

The author would like to acknowledge the following individuals from Tempered Networks for this PCI DSS Product Applicability Guide: Amruta Dhotre and Lucas Messenger for their technical contributions and timely support. The author is also thankful to Abdul Mahmood for managing the project.



## ABOUT THE AUTHORS

**Mark Bedell** | Senior Consultant, Cyber Engineering, Coalfire Systems

Mr. Bedell authored this product applicability guide and regularly contributes on network and security architecture assessments.

**Chris Krueger** | Managing Principal, Cyber Engineering, Coalfire Systems

Mr. Krueger contributes as an author and thought leader on information security and regulatory compliance topics for Coalfire's clientele in the "new and emerging" technical areas.

**Marc Kaplan** | Vice President, Systems Engineering, Tempered Networks

Mr. Kaplan contributed to the network design, providing product expertise in authoring this paper.

**Erik Glesa** | Vice President, Product Management, Tempered Networks

Mr. Glesa provided the test scenarios and PCI control focus areas for this paper.

Published June 2017

## ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. [Coalfire.com](http://Coalfire.com)

Copyright © 2014-2017 Coalfire Systems, Inc. All Rights Reserved. Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI-DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.

TEMPERED NETWORKS IDENTITY-DEFINED NETWORKING PLATFORM COMPLIANCE WITH PCI DSS V3.2 - JUNE 2017