opengear

Best Practices for PCI DSS Compliance with Opengear Products

A Technical Whitepaper

May, 2016

What is PCI DSS and who needs it?

The Payment Card Industry Data Security Standards (PCI-DSS) are a set of baseline technical and operation standards created and maintained by the payment card industry (PCI) Security Standards Council (SSC) to verify that merchants and service providers appropriately protect cardholder data. This means that any organization that has any contact with card data is required to be PCI DSS compliant. The core PCI DSS standard currently at Version 3.0 has been around for nearly a decade.

PCI compliance is vital for any company which processes, accepts or stores payment cards (credit, debit or charge cards) online or offline: from the world's largest corporations to small Internet stores: from local service providers in the Pacific to global financial companies. For more details visit the official PCI website.

Recently PCI DSS Version 3.2 was introduced with additional and expanded requirements. Multi-factor authentication is now required for all personal with non-console administration access and all personal with remote access to card-holder data environment (CDE). Opengear devices have 2 factor authentication when configured and we are fully compliant with PCI DSS Version 3.2.

The intended audience for this white paper included network administrators, security architects, and PCI DSS compliance auditors who wish to enhance the security of corporate networks and ensure that payment information is well protected.

PCI Best Practices with Opengear Products

The PCI DSS encompasses 6 primary areas of focus, which are divided into 12 major requirements, shown below:

PCI Data Security Standard - High Level Overview	
Build and Maintain a Secure Network and Systems	• Install and maintain a firewall to protect cardholder data • Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	• Protect stored cardholder data • Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	• Protect all systems against malware and regularly update anti-virus software or programs • Develop and maintain secure systems and applications

PCI Data Security Standard - High Level Overview	
Implement Strong Access Control Measures	• Restrict access to cardholder data by business need to know • Identify and authenticate access to system components • Restrict physical access to cardholder data
Regularly Monitor and Test Networks	• Track and monitor all access to network resources and cardholder data • Regularly test security systems and processes
Maintain an Information Security Policy	• Maintain a policy that addresses information security for all personnel

The major PCI requirements contain approximately 242 sub-requirements, making a PCI DSS audit a major undertaking for any organization. This security best practices guide provides a number of recommendations designed to assist Opengear customers in improving their PCI DSS compliance status.

1.1 Regularly review and apply security updates

Regular patching is one of the cornerstones of a secure computing environment. PCI DSS specifically prescribes this process in requirement 6.2, which states "Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches.".

Why is regular patching so important?

The majority of successful attacks against organizations are perpetrated using well known, commonly found exploits. A simple Google search will return copious lists of vulnerabilities for practically any software or hardware IT product on the market. Detailed instructions on how to exploit these vulnerabilities and even pre-written exploit code is readily available on the Internet. The infamous, zero-day exploits are quite rare in comparison.

Opengear regularly monitors the IT security landscape for emerging threats and promptly reviews and updates product firmware and software to ensure customer products are provided the maximum protection available. Customers of Opengear are also provided with access to Zendesk forums, which provide notifications on recent security issues as well as information on the latest firmware release. Security notifications can be viewed at **https://opengear.zendesk.com/forums/22980218-Security-Notifications**

Firmware update notifications can be viewed at **https://opengear.zendesk.com/forums/21504458-Firmware-Update-Notifications**

The latest product firmware and software can be downloaded at **http://opengear.com/downloads/**

Opengear customers can create a Zendesk account by browsing to the following URL: **https://opengear.zendesk.com/access/unauthenticated#register**

Once the account is active, customers are advised to subscribe to the email and RSS notifications for security and firmware updates. This will ensure that customers are promptly informed of any current security issues, which should be addressed.

Opengear recommends that customers make use of these forums and apply security patches and firmware updates regularly.

1.2 Change default passwords

A common, often overlooked security issue in many organizations is the use of default passwords. In most instances IT devices are shipped with a default administrator-level credential, which is used by IT staff to initially configure the device. In general, these default credentials are well known and widely documented on the Internet. A Google search, using a device's model number, will often return pages containing the default/factory username and password used to access the device.

Attackers, when attempting to exploit a system, will initially try the device’s default administrator username and password in the hopes of gaining easy access to the system. After obtaining administrative access, the attacker will then be able to capture and control any data traversing the device. Captured data may include card-holder data or possibly authentication credentials for other systems on the network.

The PCI DSS addresses this issue explicitly in requirement 2.1, which states “Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.”.

The PCI DSS also contains requirements related to acceptable password strength. In particular, requirement 8.2.3 states that passwords should have the following minimum characteristics:

- Passwords must have a minimum length of seven characters.
- Passwords must contain both numeric and alphabetic characters.

Opengear strongly recommends that:

- Customers should change default credentials prior to installing any device into production network.
- Customers should choose strong, complex passwords, which meet or exceed the PCI DSS requirements, to ensure device management accounts are adequately protected.

1.3 Create named accounts for device administrators and configuring 2-factor authentication

Access controls are a critical component in a secure computing environment. A well designed access control system will permit access to systems and devices based on an individual's role or job function and deny all other access. The PCI DSS devotes the whole of major requirement 8 to this topic, which states *“Identify and authenticate access to system components.”.*

Opengear devices provide the capability to manage local users and groups as well as providing support for remote authentication mechanisms including TACACS, RADIUS, LDAP and Kerberos.

The factory-set configuration for Opengear devices provide IT staff with a single administrator account called 'root'. This account has permissions to control all aspects of the device and is designed to be used during the device's initial configuration.

One of the first configuration tasks which should be performed is to create named accounts for each IT administrator who is responsible for device management. PCI DSS sub-requirement 8.1.1 explicitly states “*Assign all users a unique ID before allowing them to access system components or card-holder data.*”. In addition requirement 8.5 states “*Do not use group, shared or generic IDs, passwords, or other authentication methods.*”.

The primary purpose of creating named accounts is to make it possible to trace system access and activities to an individual. This process provides valuable information to investigators when reconstructing security events and may also engender a sense of personal responsibility in administrators who are aware that their actions are logged and can be traced back to them.

Opengear recommends that personal, named accounts are created for each administrator who is responsible for managing and maintaining Opengear devices.

Under the latest PCI DSS 3.2 ALL users with access to the company’s card-holder data must go through multi-factor authentication process. To be compliant to PCI DSS 3.2 Opengear devices should be configured with RADIUS security protocol. The device can support RSA SecurID over RADIUS AAA, however any multi-factor authentication that utilizes RADIUS can be used to be in compliance.

Opengear provide a knowledge base article on how to accomplish this, at the following URL: https://opengear.zendesk.com/entries/23224052-RSA-SecurID-support

1.4 Configure devices to regularly ship logs

Logging and monitoring are important components in an organization’s security defense strategy. PCI DSS devotes a whole major requirement to these topics. Requirement 10 states “*Track and monitor all access to network resources and card-holder data.*”.

To be effective, logging needs to be informative, ubiquitous, constantly monitored and protected from tampering.

When correctly implemented, a logging and monitoring solution will:

- Alert the organization when their systems are under attack. This assists the company in promptly responding to security events and, in doing so, minimizes the affects of or possibly completely halt an attack in progress.
- Provide information and evidence to assist the organization, forensic analysts and police in reconstructing a systems breach so that the extent of an incursion can be measured and so that any identified security holes or issues can be mitigated.

Opengear devices provide extensive logging functionality, which can be accessed by the web management, SSH and console interfaces. The devices also support log shipping through a number of well known mechanisms including SYSLOG, CIFS, NFS and USB flash.

There are two primary advantages of log shipping:

1. Device log files are protected from tampering. When an attacker gains access to a device or system one of their priority tasks is to remove evidence of the incursion by deleting or modifying log files. If the logs are regularly shipped, or backed up to a secure location, then the content of those files is protected from tampering.
2. Centrally storing log files eases the administrative overhead of monitoring security related activity within the computing environment. IT staff can review all log events without having to individually log on to every system in the environment.

Two sub-requirements of PCI DSS requirement 10, specifically deal with log file shipping. Requirement 10.5.3 states “Promptly back up audit trail files to a centralized log server or media that is difficult to alter.” and requirement 10.5.4 states “Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.”.

Opengear recommends that customers configure their devices to regularly ship logs to a secure location so that log data can be protected.

1.5 Configure the device to use a central time server

Time synchronization is an important service within an organization's computing environment. Many common authentication schemes make use of time data to process requests and protect themselves against replay attacks. Kerberos, for example, is the primary authentication scheme used by Windows systems. To function correctly, Kerberos relies on the clocks on client and server computers to be synchronized. Some One-Time-Password (OTP) authentication schemes are also time based.

In addition to its role in authentication, time is important for logging. Event reconstruction, in the case of a network or systems breach, often relies on matching time-stamp values of log entries in disparate systems. If system times vary, then it is difficult to fully reconstruct an event.

The PCI DSS also discusses time synchronization in requirement 10.4, which states “*Using time-synchronization technology, synchronize all critical system clocks and times*”.

Opengear devices provide the capability to configure external time sources using the Network Time Protocol (NTP).

Customers are advised to configure their devices to synchronize time against the organization's central time servers.

This is particularly important if the device is also configured to use one of the organization's authentication mechanisms, such as Windows domain authentication.

If the device is segregated from the rest of the company's computing environment, then it should be configured to synchronize with a trusted Internet-based time source instead.

1.6 Enable email and/or SMS alerts

Alerting systems are a natural addition to a robust logging and monitoring solution. Such systems promptly inform IT staff of critical security events occurring within the organization's computing environment and thus facilitate a timely activation of response processes.

Opengear products provide alerting capabilities natively using ‘Auto-Responses'. Auto-Responses are constructed by first configuring an alert condition, such as a failed authentication event. When an alert condition occurs, a pre-configured set of actions can be triggered. The actions can include:

- Sending an email or SMS
- Switch DIO line
- Perform RPC Action
- Run a custom script
- Send SNMP trap
- Send Nagios event
- Perform interface action

The PCI DSS deals with logging, monitoring and alerting in requirement 10. In particular, sub-requirement 10.6.1 dictates that logs of all critical system components, including components that perform security functions such as firewalls, are reviewed at least daily. Configuring alerts can help the customer meet this requirement.

Opengear recommends that customers configure a set of Auto-Responses to send email and/or SMS alerts for the following events:

- Success and failed login attempts.
- Addition of users and groups.
- Modification of time settings.

1.7 Secure SNMP

Simple Network Management Protocol (SNMP) is a standards based protocol used to monitor and manage devices on an IP network. Almost all network level devices support this protocol and Opengear devices are no exception.

SNMP is a powerful tool and must be protected from misuse. If the service is configured incorrectly, an attacker may be able to:

- Access useful device and network information such as IP addresses, routing and ARP tables.
- Modify device settings, allowing an attacker to set up a man-in-the-middle scenario.

SNMP is disabled by default on Opengear devices and Opengear recommends that the service remain disabled if it is not actively used in the customer computing environment. One of the enduring recommendations promoted by PCI DSS assessors, in relation to running services, is that “*if it isn't used, disable it*”. This is particularly relevant for SNMP due to the serious consequences of misconfiguration.

If SNMP is required, then the PCI DSS makes a number of recommendations related to secure use of the service.

- Use SNMP v3: Opengear devices support SNMP versions 1, 2c and 3 to promote maximum interoperability with a wide variety of customer network configurations. The PCI DSS describes SNMP v1 and v2c as insecure protocols in requirement 1.1.6. These versions are not strictly prohibited however they do add unnecessary risk, as the control data travels in plain text and could possibly be intercepted and modified by an knowledgeable attacker. For this reason Opengear recommends that customers undergoing a PCI DSS assessment use version 3 of the protocol.
- Set SNMP community strings to unique, long and complex values: If SNMP v3 is not a viable option in the computing environment, then PCI DSS requirement 2.1 dictates that the device's default SNMP community strings are changed before the device is installed in a production network. Community strings are essentially passwords used in versions 1 and 2c to access the SNMP service. PCI DSS requirement 8.2.3 dictates that passwords must be a minimum of 7 characters in length and contain both numeric and alphabetic characters. Opengear recommends that the read-only and read-write community values are modified to contain unique, long and complex values.

1.8 Disable unused services

Systems and devices often ship with a variety of active, remote listening services. Manufacturers determine what services most of their customers are likely to require from the product and activate those services by default. Obviously, each customer environment is different and so some of those active services will not be required by every customer.

Remote compromise of a system or device is usually accomplished by exploiting a weakness in a listening service. For example, an exploitable weakness may be caused by poorly managed configuration settings, such as leaving the administrator's password set to the default value. This type of weakness is more likely to occur in a service that is not actually used by the customer. Weaknesses may also be caused by coding flaws in the service itself. Buffer overflows and SQL injections are good examples of this type of weakness. Whatever the flaw, it cannot be exploited if the service is disabled and that is the premise of this recommendation.

Opengear devices ship with a minimal set of pre-enabled listening services. Over time, however, it is not uncommon for various services to be activated by IT staff for legitimate reasons but then which remain active after those services are not longer required.

Opengear recommends that customers regularly review services actively running on their devices and disable those which are no longer used.

1.9 Configure the local firewall and optionally a VPN

Firewalls generally represent the first line of defense that networks and systems use to protect against remote attacks. The PCI DSS devotes requirement 1 to this topic, which states “*Install and maintain a firewall configuration to protect card-holder data*”. Some Opengear devices provide a cellular interface, allowing them to act as an external entry point into the network. As such, it is very important to set strict firewall rules on these devices to protect the network from external attackers.

Firewall rules restricting internal access are just as important. Access to management services on a device, such as the web interface, SSH and SNMP should be restricted so that only specific, trusted hosts or networks are permitted to connect to them. Opengear provides a knowledge base article on how to accomplish this, at the following URL: **https://opengear.zendesk.com/entries/56164405-How-do-I-restrict-service-access-to-connections-from-a-trusted-source-network-only**

VPNs are a form of transport layer security, which are generally used to protect traffic traversing untrusted networks. Commonly, VPNs are used to secure an employee's 'work-from-home' connection. Opengear devices support a number of VPN protocols including IPsec, OpenVPN and PPTP. The following knowledge base article discusses the pros and cons of using VPNs with OpenGearOpengear devices and customers are encouraged to review the article to discover how configuring a VPN can improve the organization's network security: **https://opengear.zendesk.com/entries/81208579-Should-I-use-VPN-to-secure-my-connection**

PCI DSS requirement 1.1.6 states "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.". During an audit, a PCI DSS assessor will examine the firewall rules configured on critical system components and compare those rules with the permitted services and ports listed in this document.

Customers undergoing a PCI DSS assessment are advised to keep the service list document up to date and ensure that firewall rule sets on Opengear devices are configured to enforce the restrictions set forth in that document.

1.10 Configure SSH to use key-based authentication

Secure shell (SSH) is a remote management protocol used to provide a console-like interface to administrators for securely managing a device or system. It has become the de-facto standard for remotely managing network level devices and replaces its insecure predecessor Telnet.

Opengear devices have the SSH service enabled by default and, though the devices support Telnet for clients with legacy systems, Telnet is disabled by default. The PCI DSS discusses remote management access in requirement 2.3, which states "*Encrypt all non-console administrative access using strong cryptography.*". Telnet is specifically mentioned in the testing procedures for this requirement "*..determine that Telnet and other insecure remote-login commands are not available for non-console access*".

Opengear recommends that customers undergoing a PCI DSS audit ensure that the Telnet service is disabled on all their devices and that SSH is used instead.

SSH supports a number of authentication mechanisms, with password authentication being the most commonly used. According to the PCI DSS, password-based authentication is considered adequately secure in most instances, provided that passwords meet the minimum standards set in requirement 8.2.3.

Customers wishing to add an extra level of security to their devices should consider configuring the key-based authentication mechanism for SSH and disabling password authentication. Key-based authentication mechanisms use trusted certificates to authenticate to the SSH service rather than relying on passwords. Certificates are more secure than passwords primarily due to their improved resistance to brute-force attacks and for the fact that they are unlikely to be reused in other environments, as passwords often are.

To further secure the device, customers may remove access to any password-based authentication mechanism, for external management interfaces, by disabling the HTTP interface. This configuration ensures that external access to the device is restricted to accept only key-based authentication, effectively mitigating the weaknesses inherent in password based schemes.

Opengear recommends that, for all devices, customers:
- Enable key-based authentication for SSH.
- Disable password authentication for SSH.
- Disable the HTTP web management interface.

1.11 Protect device configuration backups

Configuration backups of all critical system components are a vital part of any organization's disaster recovery and business continuity processes.

All Opengear products provide the capability to backup and restore configuration settings. IT administrators can use the device's web interface to export backups, via the browser, to an external location. The PCI DSS is primarily focused on protecting backup data containing card-holder information, however it is also concerned with protecting authentication credentials during storage as it states in requirement 8.2.1 "*Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.*".

Local authentication credentials on Opengear devices are protected by industry-accepted hashing mechanisms, however some extra mechanisms which the devices support, such as using PAP authentication with the RADIUS service, store passwords in plain-text. If these services are enabled, then configuration backup files may contain the associated passwords.

In this case, Opengear advises that configuration backup files are stored securely in an encrypted form or on an encrypted medium, using industry-accepted cryptographic processes.

Conclusion

By following the recommendations in this white paper, Opengear customers can enhance the security of their networks while making them more compliant with a PCI Architecture. For additional information, please contact Opengear Technical Support at **support@opengear.com**