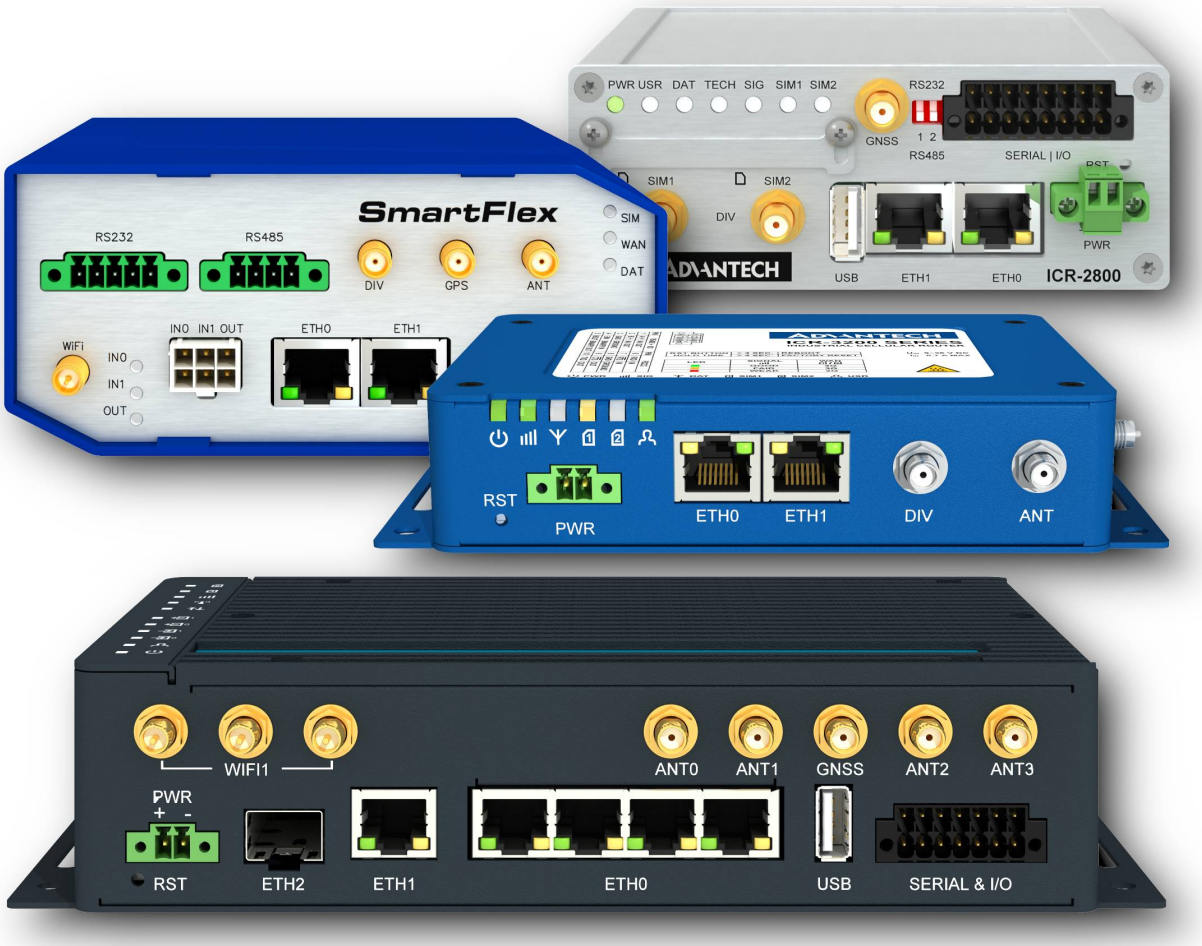
PCI DSS Compliance Considerations

APPLICATION NOTE



Used symbols

Danger – Information regarding user safety or potential damage to the router.

Attention – Problems that can arise in specific situations.

Information, notice – Useful tips or information of special interest.

Example – Example of function, command or script.

Advantech Czech s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic.
Document No. APP-0090-EN, revision from September 1, 2022. Released in the Czech Republic.

Contents

1. Introduction

This Application Note provides guidance for configuration and assessment of Advantech cellular routers within the cardholder data environment for reaching the PCI DSS compliance.

The Payment Card Industry Data Security Standard (PCI DSS) [1] comprises a minimum set of requirements for protecting account data. It applies to merchants and other entities that store, process, and/or transmit cardholder data.

The cardholder data environment is comprised of people, processes, and technology that handle cardholder data or sensitive authentication data. System components include network devices (both wired and wireless), servers, computing devices, and applications. Virtualization components, such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors, are also considered system components within PCI DSS. [2]

The PCI DSS standard comes in multiple versions. This document applies to the PCI DSS Version 3.2.1 (May 2018) and will be updated once a new PCI DSS version is released.

The PCI DSS defines 12 high-level requirements and then numerous sub-requirements. The following sections provide considerations for all first-level sub-requirements (1.1, 1.2, etc.)

2. Requirements Considerations

Requirement 1

Install and maintain a firewall configuration to protect cardholder data

1.1 Establish and implement firewall and router configuration standards.

Inspect the Security Guidelines [3], which include recommendations for secure configuration and operation.

The entire router configuration is in a single file, which enables identification of all configuration changes. For example, integration with the Zabbix monitoring system [5] allows detection of unauthorized configuration changes.

The router provides a stateful firewall functionality. The configuration enables two roles:

- Admin, who can configure the router;
- User, who can review the configuration.

The NetFlow/IPFIX Router App [6] enables you to observe the actual traffic flows and validate network diagrams.

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

The router acts as a conduit between two security zones: WAN (untrusted) and LAN (trusted). The firewall has a specific configuration for each of the zones.

Wi-Fi clients should be authorized using WPA2, possibly using a RADIUS server. The Ethernet devices can be authorized using the 802.1X Authenticator Router App [7].

The firewall filtering is disabled by default. In the router configuration you should:

- *Enable filtering of incoming packets* to deny WAN traffic from entering the LAN;
- *Enable filtering of forwarded packets* to deny traffic routing between WAN, LAN and Wi-Fi networks;
- *Enable filtering of locally destinated packets* to deny traffic towards router services.

Customized configurations can use other defaults. Please consult your dealer if you need the firewall enabled by default, or some other custom settings.

The router configuration is persistent. It can be centrally managed and auto-updated, e.g. using the WA/DMP.

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

The router can be installed on one segment boundary. Through the *filtering of forwarded packets* you can limit the traffic flow to/from specific addresses only. The established connections are then allowed in any direction.

Multiple routers and firewalls are needed to implement a Demilitarized Zone (DMZ).

The Reverse Path Filtering (`/proc/sys/net/ipv4/conf/default/rp_filter`) can be used to prevent IP address spoofing and e.g. block traffic originating from the Internet with an internal source address.

The Network Address Translation (NAT) towards WAN is used by default, so the internal IP addresses are never revealed.

The router itself does not store the payload (i.e. cardholder data), even the NetFlow/IPFIX Router App [6] doesn't store the packet content.

1.4–1.5 are not applicable

These PCI DSS requirements describe documentation or process related requirements that are not relevant to technical equipment such as cellular routers.

Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters

2.1 Always change vendor- supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.

The checklist in the Security Guidelines [3] suggests changes of the default passwords and SNMP community strings. There are no accounts other than “root” and no default secrets in the Wi-Fi configuration.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

The Security Guidelines [3] include a Hardening Guide and recommendations for secure operation that cover known security vulnerabilities. This document is periodically updated and reviewed to meet the industry best practices.

By default no network facing services and protocols are enabled; each has to be explicitly enabled.

The insecure services such as Telnet, FTP and older TLS versions are provided for compatibility with legacy systems only. These must be disabled in the PCI environment.

2.3 Encrypt all non-console administrative access using strong cryptography.

The Telnet and plain HTTP must be disabled and the secure alternatives should be used instead. The SSH and HTTPS is used with minimum TLS 1.2 and strong encryption per NIST SP 800-57.

2.4 Maintain an inventory of system components that are in scope for PCI DSS.

The remote monitoring systems such as Zabbix [5] can help maintaining the system inventory.

2.5–2.6 are not applicable

These PCI DSS requirements describe process related requirements that are not relevant to technical equipment such as cellular routers.

Requirement 3

Protect stored cardholder data

3.1–3.4 are not applicable

These PCI DSS requirements apply to cardholder data storage, whereas the router does not store any cardholder data. Even the NetFlow/IPFIX Router App [6] doesn't store the packet content.

3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.

The router does not store any cardholder data; the cryptographic keys can however be used to protect transmission of cardholder data across unprotected networks (see Requirement 4).

On router platforms without any hardware security module (e.g. TPM) are the private keys stored in the router configuration and protected by the root password only.

When performing the *Configuration Backup*, make sure to specify the *Encryption Password* to protect the keys from disclosure.

Changes to the cryptographic keys will be reported via System Logging (syslog). Remote monitoring such as Zabbix [5] can be also configured to detect modification of the key.

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.

The SCEP Router App [8] enables:

- Automated generation of strong cryptographic keys;
- X.509 certificate enrollment and renewal using a standard Public Key Infrastructure (PKI, e.g. the OpenXPKI [1]);
- Download of a Certificate Revocation List (CRL).

3.7 is not applicable

This PCI DSS requirement describes a documentation related requirement that is not relevant to technical equipment such as cellular routers.

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

Requirement 4

Encrypt transmission of cardholder data across open, public networks

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

The router supports the following cryptographic protections against unauthorized disclosure of cardholder data:

- Private APN (Access Point Name) in the cellular operator's network, authenticated by the SIM (Subscriber Identity Module) Card;,
- WPA2–AES encryption protecting the Wi-Fi communication;
- VPN (IPsec, OpenVPN) based on pre-shared secrets or X.509 certificates protecting network traffic;
- TLS 1.2 protecting the SSH and HTTPS communication for router administration.

The cipher suites supported meet the NIST SP 800-57 requirements for the cryptographic strength in 2030.

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

No user data are sent over messaging technologies. The SMS is used for status reporting and limited remote control such as reboot and WAN connection/disconnection.

4.3 is not applicable

This PCI DSS requirement describes a documentation related requirement that is not relevant to technical equipment such as cellular routers.

Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs

5.1 - 5.4 are not applicable

The router runs a custom distribution of a Linux operating system, which is not accessible for regular users. Only administrator (root) can login and perform configuration changes.

The remote monitoring systems such as Zabbix [5] can monitor system integrity and trigger a warning when the router configuration is modified.

Requirement 6

Develop and maintain secure systems and applications

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

We proactively search for security deficiencies in our products. We monitor public vulnerability databases such as NVD and perform thorough penetration testing. The PSIRT (Product Security Incident Response Team) is fully compliant with FIRST (Forum of Incident Response and Security Teams) recommendations for Level 1.

List of vulnerabilities in our products is available through the Engineering Portal [2].

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches.

The firmware updates with security patches is released at least 4 times a year. This includes fixes of known vulnerabilities in system components, which has CVSS > 6.5. Fixes to critical vulnerabilities are released on an ad-hoc basis.

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely.

The firmware is developed based on the best industry practices. Every code contribution undergoes a peer review according to internal coding standards, including a check that no test provisions are included in the firmware.

6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following: [. . .]

The firmware development is under a strict version control. Before releasing a new firmware, the following actions are performed:

- The new release undergoes a thorough function and performance test;
- Release Notes are provided that describe all changes made, including a list of fixed security vulnerabilities;
- The product documentation is updated after each firmware release.

The v3 routers can recover from a failed upgrade: when the new firmware fails to boot, the previous version is restored.

[2] https://icr.advantech.cz/download/security-notifications

6.5 Address common coding vulnerabilities in software-development processes.

Every release undergoes an automated penetration test for known vulnerabilities and manual penetration tests are made at least once a year by an independent organization.

The internal coding standards include the SEI CERT C Coding Standard. The developers have every year a security training that cover the most relevant security flaws discovered.

6.6–6.7 are not applicable

These PCI DSS requirements are related to public-facing websites and operational procedures and thus not relevant to technical equipment such as cellular routers.

Requirement 7

Restrict access to cardholder data by business need to know

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

Access to the router is limited to authorized persons only. The router configuration enables two roles:

- Admin, who can configure the router;
- User, who can review the configuration.

When connecting devices over LAN or Wi Fi it is also possible to use 802.1X or WPA2-Enterprise authentication to restrict access of the individual devices.

The MAC address filtering provided by the Layer 2 Firewall (L2FW) Router App [9] may also be used.

7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Without an explicit authorization nobody can login. Access to the router can be controlled by a TACACS+ or a RADIUS server. The user role can be selected based on the RADIUS *Service-Type* attribute.

7.3 is not applicable

This PCI DSS requirement describes a documentation related requirement that is not relevant to technical equipment such as cellular routers.

Requirement 8

Identify and authenticate access to system components

8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components

Users connect to the router with unique username and a password.

All administration actions are logged to syslog. Integrity checks performed by remote monitoring machines can detect unauthorized changes.

After 3 unsuccessful login attempts the Web admin access gets locked for 60 minutes.

Established SSH, Web (HTTP), Telnet and FTP sessions (if enabled) get closed after a defined period of inactivity.

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users.

The user password or a passphrase is used. Empty password is not allowed. The `/etc/settings.policy` file defines a password complexity policy, including:

- Minimal length;
- Minimal number of uppercase, lowercase characters and digits.

Users are reminded to change the default password with a red highlighted text. Without changing the default password it is not possible to enable remote access in the NAT configuration.

The user passwords are not stored in the router; only SHA-1 hashes are used. The TLS 1.2 (HTTPS, SSH) is used to protect the password during authentication exchange.

8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (Old definition from DSS 1.2.)

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

The router is not intended as an entry point for network-level access originating from outside the network. Hence, the two-factor authentication is not needed and not supported.

8.4 Document and communicate authentication policies and procedures to all users.

Guidelines on selecting secure passwords are provided in the Security Guidelines [3], based on the NIST SP 800-63B.

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows.

The use of group credentials is discouraged in the Security Guidelines. [3]

8.6–8.8 are not applicable

These PCI DSS requirements describe requirements for authentication using security tokens, requirements for a database and documentation related requirements that are not relevant to cellular routers.

Requirement 9

Restrict physical access to cardholder data

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

The router must be placed in a physically secured environment.

As an additional protection measure, a remote monitoring system such as Zabbix [5] can be used to detect additional devices connected to a USB port, and the Ethernet Port Detector Router App [10] can be used to detect and report disconnection of a LAN cable.

9.2–9.9 are not applicable

These PCI DSS requirements describe requirements for onsite personnel security that are not relevant to cellular routers.

Requirement 10

Track and monitor all access to network resources and cardholder data

10.1 Implement audit trails to link all access to system components to each individual user.

The System Log (syslog) includes records of login events, including username and source IP address.

10.2 Implement automated audit trails for all system components to reconstruct the following events: [. . .]

The System Log includes information about all significant events, including:

- Modifications to router configuration;
- Unsuccessful login attempts;
- User administration actions;
- Enabling / disabling of router services, including the syslog service itself;
- Installation and removal of router apps.

10.3 Record at least the following audit trail entries for all system components for each event: [. . .]

Each syslog record includes:

- Software type (called facility) that generated the message;
- Severity level, such as Error(3), Warning(4) or Notice(5);
- Timestamp;
- Originating process;
- Textual message.

10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

The router provides an NTP client, which can use one or two arbitrary NTP servers (primary and secondary).

The NTP client settings can be modified by the Admin (root) only.

Remote monitoring systems such as Zabbix [5] can detect time drift and trigger a warning when the delta gets too large.

10.5 Secure audit trails so they cannot be altered.

Any authenticated user or admin can view the syslog information. The syslog information should be thus sent to a secure, centralized log server for further analysis and storage.

Sensitive information such as passwords are not logged.

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

The Security Guidelines [3] provide some recommendations on security relevant events that should be identifies in system logs.

10.7–10.9 are not applicable

These PCI DSS requirements describe process related requirements that are not relevant to technical equipment such as cellular routers.

Requirement 11

Regularly test security systems and processes

11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

The remote monitoring system such as Zabbix [5] can help maintaining an inventory of Wi-Fi AP.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
11.3 Implement a methodology for penetration testing that includes the following: [. . .]

We perform penetration tests and vulnerability scans also in production to make sure the default configuration is safe.

11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network.

As described in the Remote Monitoring Application Note [4], the router provides NetFlow/IPFIX, SNMP, syslog and other data that can be fed into a network Intrusion Detection System (IDS) for detection of security incidents.

11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files [. . .].

Remote monitoring tools such as Zabbix [5] can be used to detect unauthorized changes to router configuration.

11.6 is not applicable

This PCI DSS requirement describes a documentation related requirement that is not relevant to technical equipment such as cellular routers.

Requirement 12

Maintain a policy that addresses information security for all personnel

12.1 Establish, publish, maintain, and disseminate a security policy.

As a guidance for securing the router we provide the Security Guidelines. [3] These guidelines are reviewed at least once a year by an independent reviewer to make sure these are in line with industry best practices.

12.2 is not applicable

This PCI DSS requirement describes a process related requirement that is not relevant to technical equipment such as cellular routers.

12.3 Develop usage policies for critical technologies and define proper use of these technologies.

The Security Guidelines [3] include instructions for a secure router operation.

12.4–12.11 are not applicable

These PCI DSS requirements describe documentation related requirements that is not relevant to technical equipment such as cellular routers.

3. Related Documents

[1]	PCI Security Standards Council:	**Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.2.1 (May 2018)**
[2]	PCI Security Standards Council:	**PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1**
[3]	Advantech Czech:	**Security Guidelines Application Note** (APP-0078-EN)
[4]	Advantech Czech:	**Remote Monitoring Application Note** (APP-0091-EN)
[5]	Advantech Czech:	**Zabbix Integration Guide Application Note** (APP-0089-EN)
[6]	Advantech Czech:	**NetFlow/IPFIX Router App** (APP-0085-EN)
[7]	Advantech Czech:	**802.1X Authenticator Router App** (APP-0084-EN)
[8]	Advantech Czech:	**SCEP Router App** (APP-0062-EN)
[9]	Advantech Czech:	**Layer 2 Firewall (L2FW) Router App** (APP-0017-EN)
[10]	Advantech Czech:	**Ethernet Port Detector Router App** (APP-0035-EN)

Product-related documents can be obtained on *Engineering Portal* at icr.advantech.cz address.