# Using Robustel Routers in PCI DSS Compliant Applications

# Preface

## 1) Right of Revision

Robustel reserves the right to revise this publication and to make changes in the content thereof without obligation to notify any person or organization of any revisions or changes.

## 2) Revision Tracking

| Revision | Date | Description | Author |
|---|---|---|---|
| 1.0 | July 5, 2020 | Initial Release | Simon Feng |
| | | | |

## 3) Intellectual Property

Robustel and the Robustel logo are registered trademarks of Guangzhou Robustel LTD in China and other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

# Table of Contents

# Overiew

## 1) Business Drivers

Point-of-Sale (POS) businesses are subject to stringent requirements with regards to protecting sensitive customer and company information. Financial institutions require that any company that stores, processes or transmits credit card information complies with the PCI-DSS (Payment Card Industry, Data Security Standards).

Companies that fail to comply are subject to fines, lawsuits, and can even be banned from processing credit cards. Even worse, companies that are breached can find themselves in the news headlines, significantly impacting goodwill with customers, partners and shareholders.

## 2) Summary

When properly configured, monitored and maintained, Robustel devices meet the requirements of PCI-DSS 3.0. Enabling features include VLAN, stateful firewall, MAC/IP/URL filtering, authentication/encryption, event logging, event alerts, time synchronization, and configuration/upgrade management from the RCMS platform.

## 3) Objective of this

Robustel specializes in network connectivity solutions for the Retail Point-of-Sale market. Our products are deployed broadly in several Retail POS segments that process credit card transactions, including:

- Retail Stores
- Restaurants & Bars
- Convenience Stores
- Coffee Shops
- Kiosks
- ATMs
- Service Locations
- Entertainment & Recreational Venues
- Special Events
- Temporary Vending Locations

# PCI Security Standards

## 1) Overview

The objective of the Payment Card Industry (PCI) Security Standards is to protect cardholder data. The standards are developed and published by the PCI Security Standards Council (SSC), which consists of hundreds of industry participants who have a vested interested in reducing vulnerabilities in the card-processing ecosystem.

The PCI-SSC was founded by the following five global payment brands:

- American Express
- Discovery Financial Services
- JCB International
- MasterCard Worldwide
- Visa, Inc.

## 2) Scope

The PCI SSC publishes the following standards:

**PCI Data Security Standards (DSS):** Applies to any entity that stores, processes, and/or transmits cardholder data. The standard covers technical and operational components include in or connected to cardholder data. If a business accepts or processes payment cards, it must comply with the PCI DSS.

**PIN Transaction Security Requirements (PTS):** Applies to manufacturers who develop PIN (personal identification number) entry terminals used for payment card financial transactions.

Payment Application Data Security Standards (PA-DSS): Applies to software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement.

**Point-to-Point Encryption (P2PE):** Applies to merchants to reduce the scope of their cardholder data environment and annual PCI DSS assessments.

## 3) Compliance

Merchants who process credit card transactions are responsible for complying with the PCI-DSS. “PCI Compliance” is achieved when the merchant successfully demonstrates (via external audits or self-certification) that their entire system and process complies with the 12 requirements of the PCI-DSS.

## 4) Requirements

Version 3.0 of the PCI-DSS was released in November, 2013. The PCI-DSS provides a baseline of technical and operational requirements designed to protect cardholder data. The PCI-DSS is organized around the following high-level goals and requirements:

| Goals | Requirements |
|---|---|
| **Build and Maintain a Secure Network and Systems;** | ·Install and maintain a firewall configuration to protect cardholder data;<br>·Do not use vendor-supplied defaults for system passwords and other security parameters. |
| **Do not use vendor-supplied defaults for system passwords and other security parameters.** | ·Protect stored cardholder data;<br>·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;<br>·Develop and maintain secure systems and applications. |
| **Implement Strong Access Control Measures** | ·Restrict access to cardholder data by business need to know;<br>·Identify and authenticate access to system components;<br>·Restrict Physical access to cardholder data. |
| **Regularly Monitor and Test Networks** | ·Track and monitor all access to network resources and cardholder data;<br>·Regularly test security systems and processes. |
| **Maintain an Information Security Policy** | ·Maintain a policy that addresses information security for all personnel. |

### 5) Certification

While the standards are driven by the PCI SSC, each payment card financial institution has its own program for compliance. In general, compliance can be certified by the merchant through a Self-Assessment Questionnaire (SAQ) or through a Qualified Assessor such as a QSA (Qualified Security Assessor) or ASV (Approved Scanning Vendor).

It is the merchant’s responsibility to work with their payment card financial institution to determine what form of certification is required.

## Robustel Recommendations for PCI Compliance

### 1) Overview

The PCI SSC does not publish any certification standards for network equipment other than PIN entry terminals. As a result, there is no such thing as a “PCI Compliant Router”.

To become “PCI Compliant”, the merchant must verify that their entire system (POS devices, network devices, servers, applications, policies, and procedures) complies with the PCI-DSS 3.0. As part of that overall effort, the merchant must verify that their network equipment (including Robustel devices) is properly configured and managed to ensure overall compliance with the PCI-DSS.

Robustel cannot control how an end user configures and manages a Robustel router. Similarly, Robustel does not have any control over the other devices, servers and applications that comprise an end-to-end card payment system. As such, PCI compliance can only be obtained by the merchant in the context of their entire system. The merchant is also responsible for obtaining certification of their end-to-end system from a QSA (Qualified Security Assessor) or ASV (Approved Scanning Vendor).

Robustel devices are utilized in several PCI-compliant systems. This section provides a summary of Robustel features and capabilities that have been used by other customers to help achieve PCI Compliance for their end-to-end systems.

## 2) Reference Implementation

The following reference implementation represents a reasonably complex topology that includes:

- Ethernet access for POS devices
- Ethernet and Wi-Fi access for employee computers and printers
- Ethernet and Wi-Fi access for other devices
- Wi-Fi access for customers.

## 3) Recommendations

Wi-Fi: This interface can be firewalled and segmented just like any Ethernet or PPP interface. WPA/WPA2/WEP security and MAC address filtering are also supported.

Cellular: The cellular PPP instance appears as a WAN interface and can be firewalled and segmented as needed. Interfaces can also be set to not allow management connections.

Step 1: Configure the router with the suitable firmware

Step 2: Change the default passwords

Step 3: Lock down the router entry points

Step 4: Configure the firewall

Step 5: Set up different network segments to different devices by VLANs

Step 6: Set up the segment of Wi-Fi, which is different from POS device

Step 7: Create secure WAN connectivity

Step 8: Configure communication with an external SysLog server

Step 9: Configure communication with an external Time server

Step 10: Monitor device usage with RCMS

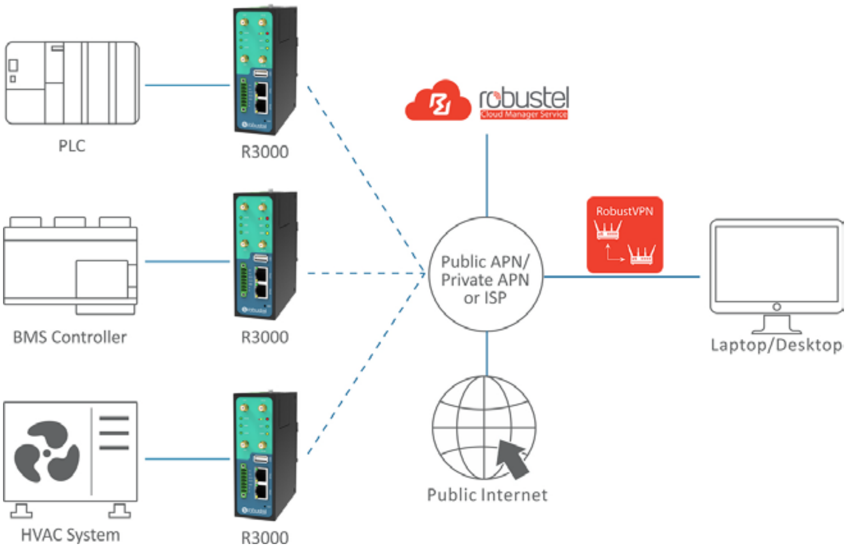
# Recommended Robustel Products for use in PCI DSS Applications

## 1) Industrial Dual SIM Cellular VPN Router R3000

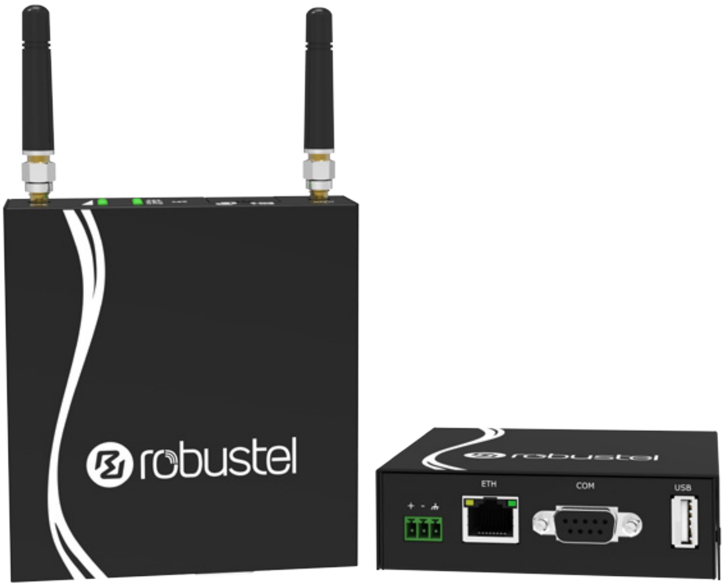
### KEY FEATURES

- The feature Link Manager supporting WWAN1, WWAN2, Ethernet WAN, WLAN WAN link backup and ICMP detection
- he option Backup Mode supporting cold, warm and load balancing
- RobustOS + SDK + App
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Management and maintenance via Web/CLI/SNMP/RobustLink Cloud
- Robust industrial design (9 to 60V DC, desktop or wall mounting or DIN rail mounting)

### TOPOGRAPHY



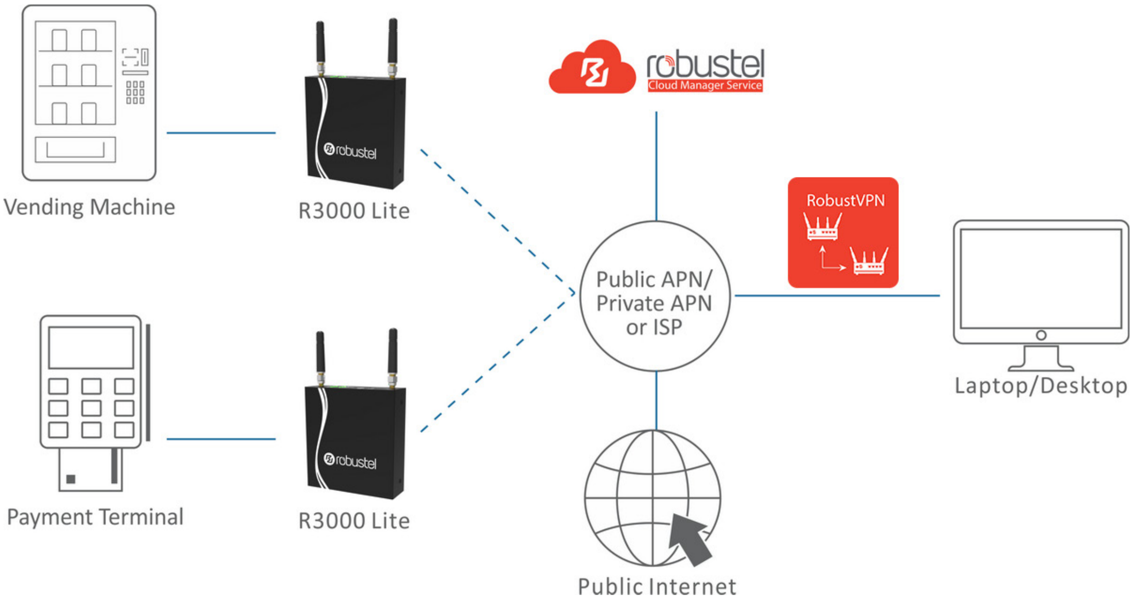
## 2) Industrial Dual SIM Cellular VPN Router R3000 Lite



### KEY FEATURES

- Dual SIM redundancy for persistent 2G/3G/4G cellular network connections
- RobustOS + SDK + App
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Management and maintenance via Web/CLI/SMS/SNMP/RobustLink Cloud
- Robust industrial design (9 to 36V DC, desktop or wall mounting or DIN rail mounting )

### TOPOGRAPHY

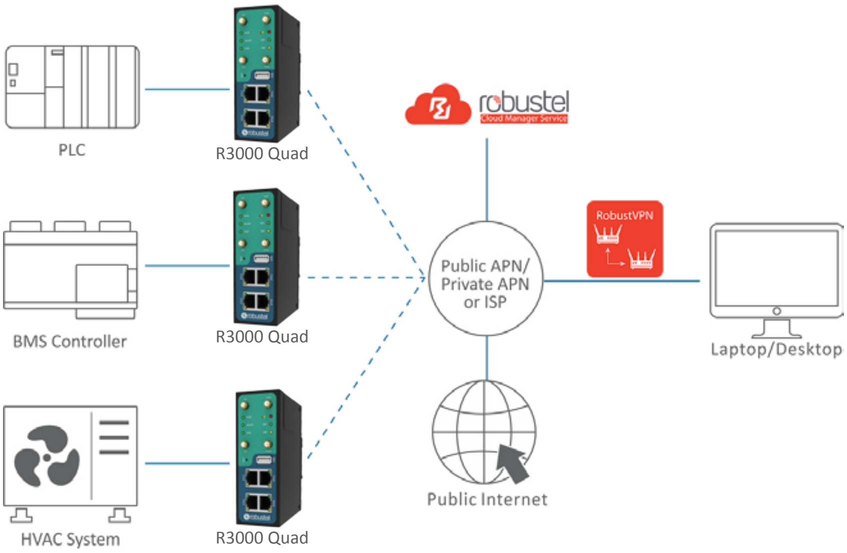


## 3) Industrial Cellular VPN Router R3000 Quad

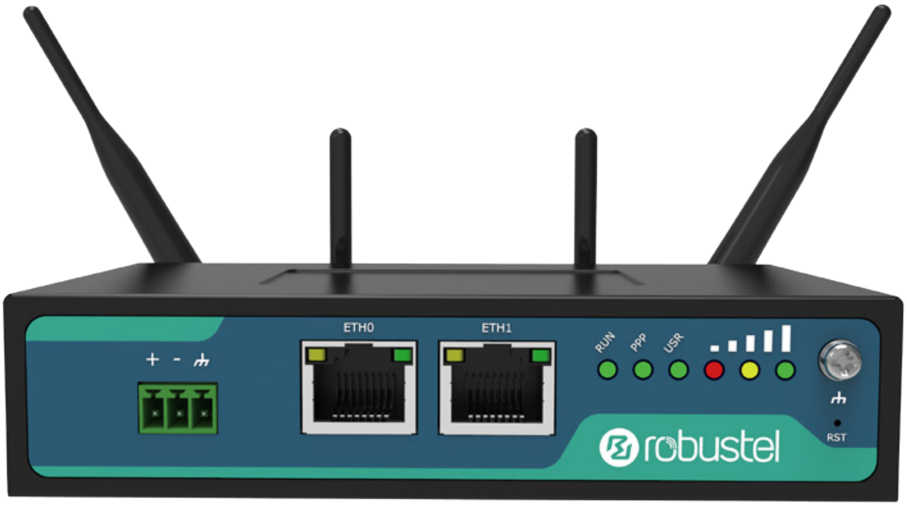
### KEY FEATURES

- The feature Link Manager supporting WWAN1, WWAN2, Ethernet WAN, WLAN WAN link backup and ICMP detection
- The option Backup Mode supporting cold, warm and load balancing
- RobustOS + SDK + App
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Management and maintenance via Web/CLI/SNMP/RCMS Cloud
- Robust industrial design (9 to 36V DC, desktop or wall mounting or DIN rail mounting )

### TOPOGRAPHY



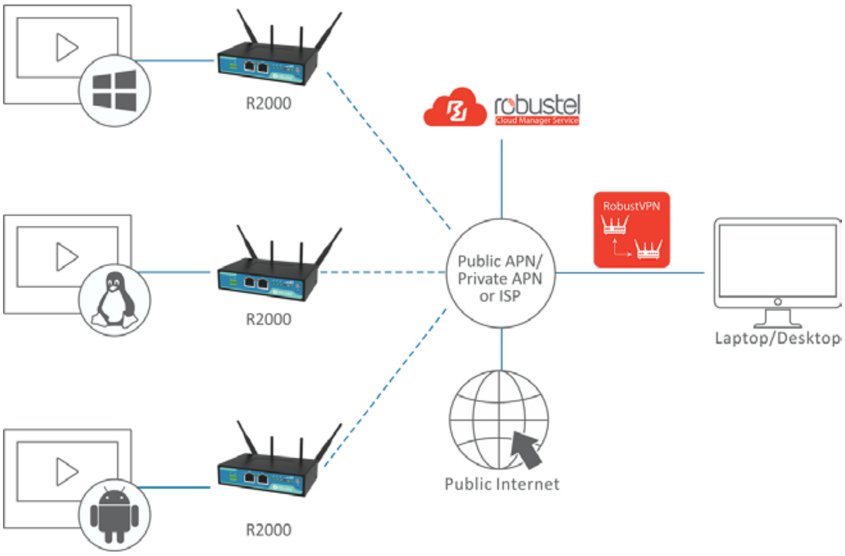
## 4) Industrial Dual SIM Cellular VPN Router R2000



### KEY FEATURES

- The feature Link Manager supporting WWAN1, WWAN2, Ethernet WAN, WLAN WAN link backup and ICMP detection
- The option Backup Mode supporting cold, warm and load balancing
- RobustOS + SDK + App
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Management and maintenance via Web/CLI/SNMP/RCMS Cloud
- Robust industrial design (9 to 36V DC, desktop or wall mounting or DIN rail mounting )

### TOPOGRAPHY

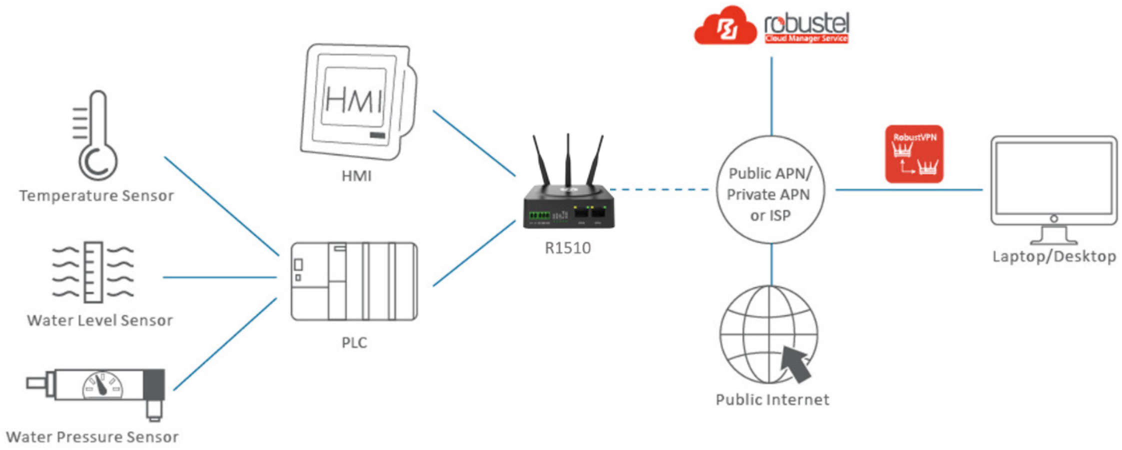


## 4) Industrial Dual SIM Cellular VPN Router R1510

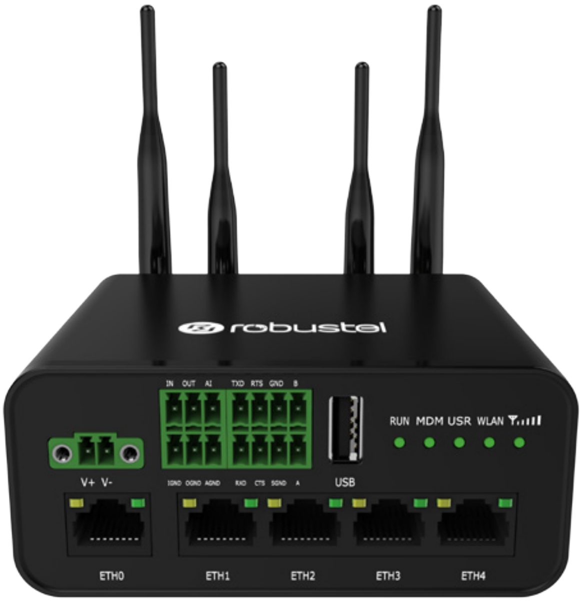
### KEY FEATURES

- Support continuous 2G/3G/4G cellular network connections
- The feature Link Manager supports Cellular WAN, Ethernet WAN, WLAN WAN link backup and ICMP detection
- WAN – Static/PPPoE/DHCP Client
- RobustOS + SDK + App
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Management and maintenance via Web/CLI/SMS/RCMS Cloud
- Auto reboot via SMS/Timing
- Robust industrial design (9 to 26V DC, desktop or wall mounting or DIN rail mounting)

### TOPOGRAPHY



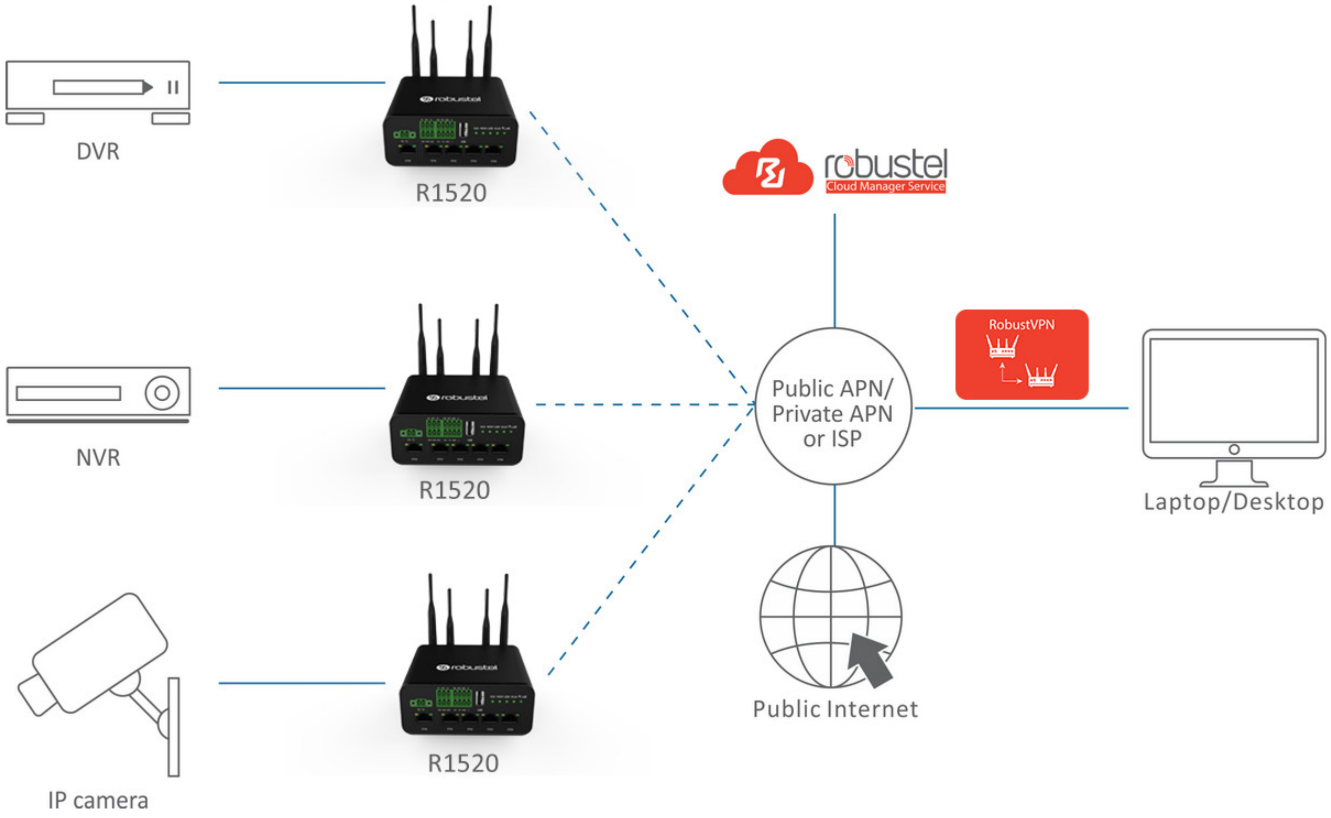
## 5) Industrial Dual SIM Cellular VPN Router R1520



### KEY FEATURES

- Cost-effective & high performance 3G/4G router
- Rugged design with 9 to 36Vdc power
- “Global” 4G version available
- E-mark certification for in vehicle use
- Optically isolated digital IO
- 10-bit Analogue interface for direct sensor connections
- Supports Dual SIMs & Wifi/Ethernet as WAN
- Cellular keep-alive and fast failover
- Extensive range of software “apps” for enhanced functionality
- RobustVPN – hosted service providing a “fixed IP” router
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN supported
- Extensive global certifications

## TOPOGRAPHY



# Additional Information

For additional information about how Robustel can help enable PCI-Compliant card payment systems, please contact Robustel directly. Our Professional Services organization can provide consulting services and best practices that can help guide you towards PCI Compliance.