



PCI Compliance Guide

June 2017

Document Information

Version	Notes	Author
1.0 Jul 2015	Initial Release.	Martin Langmaid (<i>mlangmaid@peplink.com</i>)
1.1 Jun 2017	Updated to reflect the release of PCI DSS 3.2 (June 2017)	Martin Langmaid (<i>martin@slingshot6.com</i>)

Table of Contents

PCI Compliance Guide.....	1
Document Information	2
Table of Contents.....	2
PCI DSS and Peplink Routers	3
Introduction	3
The New PCI DSS V3.2	3
PCI Data Security Standard – A High Level Overview	5
How does this apply to your Peplink router?.....	5
The DSS Requirements for your firewall	6
Configuration Example	7
Configuration Recommendations	8
1. Upgrade Router to latest Firmware	8
2. Change the Default Admin Username & Password	8
3. Secure the Wan Configuration	9
4. Initial Firewall Configuration	9
5. Segment the network using VLANs	10
6. Setup the Wireless Network.....	11
7. Setup Syslog Server	12
8. Setup Email Alerts	13
9. Configure 4G/LTE for Failover	13
10. Create a VPN to Head Office for Card Data Transmission.....	14
11. Secure and Restrict CDE VPN Network Traffic	15
12. InControl 2 Configuration	17
Summary	19
Disclaimer	19

PCI DSS and Peplink Routers

Introduction

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.

PCI DSS applies to any company which processes, accepts or stores payment card data (credit, debit or charge cards). The need for DSS is clear in light of the many high-profile thefts of credit card data from major retailers in recent years together with the exponential growth of e-commerce. Since the introduction of the DSS in 2004, the rules have evolved to reduce the risk from new risks and technology.

The New PCI DSS V3.2

The new and always evolving requirements make up the greatest changes – most of which do not go into effect until February 1, 2018

- **Section 3.3** is an updated requirement that clarifies that any displays of a primary account number (PAN) greater than the first six/last four digits of the PAN requires a legitimate business need.
- **Section 3.5.1** is a new requirement for service providers only to maintain a documented description of the cryptographic architecture (algorithms, protocols, and keys) involved in their cardholder data environment (CDE).
- **Section 6.4.6** is a new requirement for change control processes to incorporate verification of other PCI DSS requirements that are impacted by a change such as network diagrams, endpoint controls, and the inclusion of new systems into the quarterly vulnerability scan process.
- **Section 8.3** has been expanded into sub-requirements to require multi-factor authentication for all personnel with non-console administrative access and all personnel with remote access to the CDE. This includes a new requirement, 3.2, that addresses multi-factor authentication for all personnel with remote access

to the CDE and a new requirement 8.3.1 that addresses multi-factor authentication for all personnel with non-console administrative access to the CDE.

- **Sections 10.8 & 10.8.1** are new requirements for service providers to detect and report on failures of critical security control systems such as firewalls, anti-virus, and audit logging mechanisms.
- **Section 11.3.4.1** is a new requirement for service providers to perform penetration testing on segmentation controls at least every six months.
- **Section 12.4.1** is a new requirement for service providers whereby executive management must establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include accountability and a charter to ensure the program is communicated to management.
- **Sections 12.11 & 12.11.1** are new requirement for service providers to perform quarterly security program reviews and maintaining documentation and sign-off of those reviews.
- **New Appendix A2** that outlines additional requirements for SSL/TLS, namely:
 - After June 30, 2018, stop using SSL/early TLS as a security control and use only secure versions of the protocol (i.e. TLS v1.2).
 - Prior to June 30, 2018, existing implementations that use SSL and/or TLS 1.0 and 1.1 must have a formal Risk Mitigation and Migration Plan in place.

A complete summary of all changes can be found in the document [Summary of Changes from PCI DSS Version 3.1 to 3.2.](#)

PCI Data Security Standard – A High Level Overview

Build and maintain a secure network	<ul style="list-style-type: none">• Install and maintain a firewall configuration to protect cardholder data• Do not use vendor supplied defaults for system passwords and other security parameters.
Protect Cardholder data	<ul style="list-style-type: none">• Protect stored cardholder data (One Way Encryption, Store Keys offsite, separation of privileges, segregation of data)• Encrypt transmission of cardholder data across open and public networks.
Maintain a Vulnerability Management program	<ul style="list-style-type: none">• Use and regularly update anti-virus software or programs• Develop and maintain secure systems and applications
Implement Strong Access Control measures	<ul style="list-style-type: none">• Restrict Access to cardholder data by business need to know• Assign unique IDs to each person with computer access• Restrict Physical access to cardholder data
Regularly Monitor and Test Networks	<ul style="list-style-type: none">• Track and monitor all access to network resources and cardholder data• Regularly test security systems and processes
Maintain an information security policy	<ul style="list-style-type: none">• Maintain a policy that addresses information security for all personnel.

How does this apply to your Peplink router?

In the context of your Internet connectivity and your router/firewalls, DSS imposes specific requirements so it's important that you select a product which can be PCI/DSS compliant. Importantly we say 'can be' because a product itself cannot be universally 'compliant', only its configuration can be. Any product capable of PCI DSS compliance can also be set up in such a way that it is not compliant, so correct configuration and usage is vital.

The DSS Requirements for your firewall

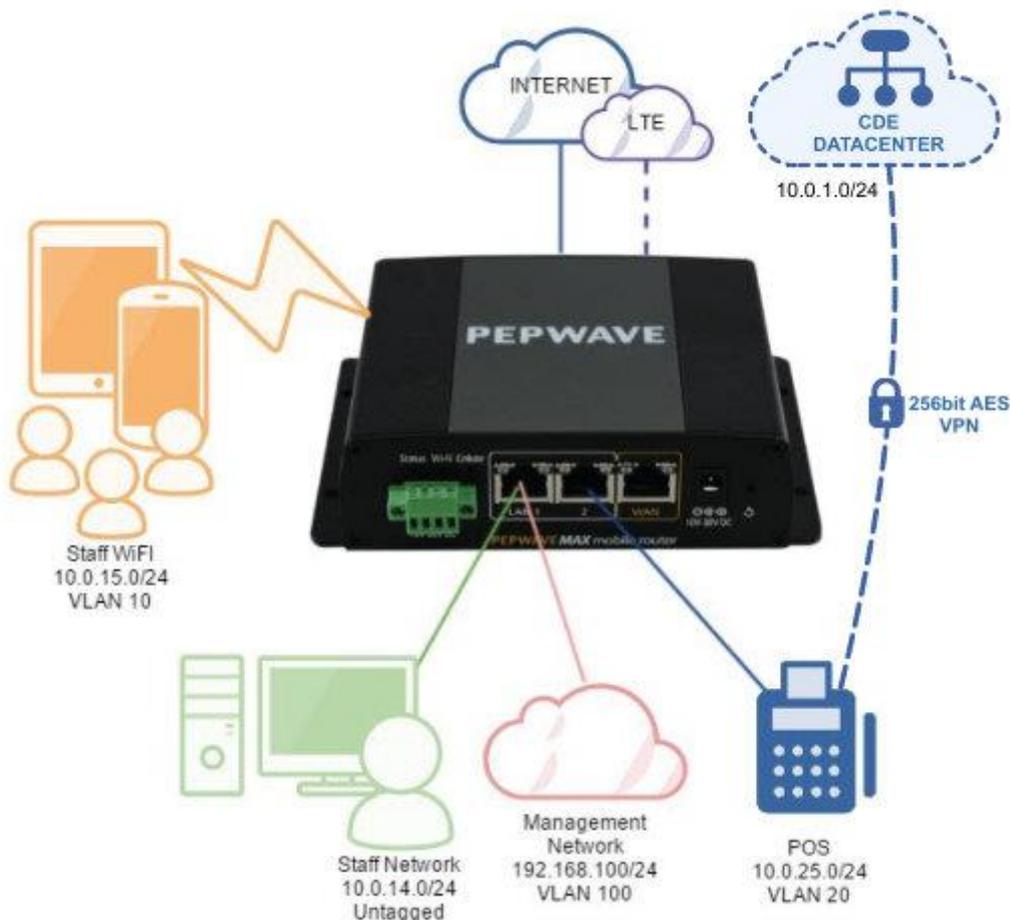
1. Install and maintain a firewall on any network which processes card data
2. The firewall must only permit services/traffic which is necessary to that Cardholder Data Environment (CDE). *(in 3.2 there is a clarification in section 1.2.1.b that specifies that both inbound and outbound rules must be in place)*
3. Document your network fully (with diagrams and inventory) and justify all enabled services.
4. Only authorized people may make changes to the firewall configuration; there must be a log of anyone making changes to the firewall configuration (an audit trail).
5. Assign a unique user ID (login) to each person with firewall administrator access. *(New in 3.2 is the requirement for multi-factor authentication for all personnel with non-console administrative access and all personnel with remote access to the CDE.)*
6. You should also have an up to date network diagram and document and justify all enabled services (such as VPNs).
7. Any wireless networks must be additionally firewalled or separated from the CDE.
8. Direct public access to the CDE must be blocked. A DMZ, logically separated from the CDE, must be used for any systems which provide public services.
9. Enable anti-spoofing measures to block and detect forged source IP addresses on incoming connections.
10. Operate Stateful Packet Inspection (SPI). This allows only established connections to have access into the CDE.
11. Disable any features that you do not need to use.
12. Use encryption for all firewall administrative access (e.g. SSH, HTTPS, SSL etc.).
13. Keep private IP addresses secret. The use of NAT is one way to obfuscate private/internal IP addresses, but block route advertisements (RIP)
14. Do not use vendor default passwords for any devices. Change the passwords when installing any product as your first step, including wireless and admin passwords. Passwords should be 'strong' (sufficiently complex).
15. Encrypt transmission of cardholder data across open, public networks. The use of VPN with encryption is essential if you need to pass data between secure networks over the public Internet.

Configuration Example

For the purposes of this document, below is a configuration example that you might see in a typical small retail environment.

In this example, we have:

- A Peplink BR1 single cellular Router with two possible WAN connections - a fixed line WAN service (e.g. DSL/Fiber) and a 4G cellular WAN for failover in the event the fixed line service is unavailable.
- Portable Staff devices connected to it over Wi-Fi
- Fixed Staff PCs connected via wired Ethernet using a switch (the switch is not shown in the diagram below for the sake of simplicity)
- A management network used by visiting IT support engineers to locally manage the BR1
- A VLAN network for the Point of Sale (PoS) machines / credit card readers.
- A VPN Connecting the POS VLAN to the Card Holder Data Environment in the Datacenter.



Configuration Recommendations

1. Upgrade Router to latest Firmware

Either use InControl 2 to automatically manage the firmware on your device, or login locally via the administration web interface and upload the latest firmware. The latest firmware release for your device can be downloaded from <http://www.peplink.com/support/downloads/>

2. Change the Default Admin Username & Password

The default admin username and password on a factory fresh Peplink product is admin/admin. This should be changed on in the **System -> Admin Security** page in the webui to something other than admin for the username and a complex password.

Admin User Name	<input type="text" value="StoreAdmin"/>
Admin Password	<input type="password" value="....."/>
Confirm Admin Password	<input type="password" value="....."/>

Of note here is that in under PCI DSS 3.2 (8.3.1) all 'non console' based user access to the device must use multi-factor authentication.

There are two suggested approaches to this. The first is to enable Authentication by RADIUS on the device (in **System > Admin Security**) to authenticate all web admin access using an external radius server (hosted in the CDE datacenter/network accessible over secure VPN) which in turn incorporates MFA.

When enabled, the *Authentication by RADIUS* feature disables the local user accounts of the device (unless the RADIUS server is unreachable – in which case local user account access is enabled to allow for emergency access to the device).

The second is to enforce the use of multi-factor authentication for InControl 2 user accounts and only allow access to the web ui via its [Remote Web Admin tool](#).

In either case, it is important to set a long and complex admin password on the device itself – likely one designed not to be shared with or used by a local administrator. InControl 2 makes admin password management easy by centrally managing & enforcing the use of complex passwords across all your devices.

3. Secure the Wan Configuration

Disable UPnP & NAT-PMP

Turn off UPnP and NAT PMP features in **Advanced -> Port Forwarding**

UPnP / NAT-PMP Settings	
UPnP	<input type="checkbox"/> Enable
NAT-PMP	<input type="checkbox"/> Enable

Disable WAN Ping Response

Make the WAN interface harder to discover using network ping scans by setting 'Reply to ICMP Ping' to 'No' in the WAN Connection Settings.

Reply to ICMP PING	<input type="radio"/> Yes <input checked="" type="radio"/> No
--------------------	---

Disable Web Administration from the WAN

Make sure that the administration web interface of the device is not accessible from the WAN interfaces by setting 'Web Admin Access' to 'LAN Only', and change the security to HTTPS and limit access to the Management VLAN only in **System -> Admin Security**

Security	HTTPS
Web Admin Port	443 <input type="button" value="Default"/>
Web Admin Access	LAN Only

LAN Connection Access Settings	
Allowed LAN Networks	<input type="radio"/> Any <input checked="" type="radio"/> Allow this network only Management Network (100)

4. Initial Firewall Configuration

IP Spoofing Protection

[IP Spoofing Protection](#) is enabled by default on WAN links in NAT Mode.

Enable Intrusion Detection

Turn on Intrusion Detection and DoS Prevention in **Advanced -> Firewall | Access Rules**

Intrusion Detection and DoS Prevention	
Intrusion Detection and DoS Prevention	<input checked="" type="checkbox"/> Enable

5. Segment the network using VLANs

Management Network

1. The management network (192.168.100.0/24 in the example above) is the only network that the BR1s web administration interface is available from. Devices connected to other networks on the BR1 (such as those on the staff Wi-Fi network) can not access the routers Web UI.
2. Both the IP range and the VLAN ID have been intentionally chosen to be outside of expected ranges compared to the staff networks. This makes them harder to guess.
3. Remote Web Admin access is still possible by device administrators using InControl 2.
4. Inter VLAN routing is disabled on this network segment so that if a malicious user could physically connect to the BR1 and set their VLAN ID to 100 they would not immediately have access to the rest of the network (in particular the PoS Network).
5. The Management VLAN is designed to only ever be used by an authorized IT engineer.

The screenshot shows a configuration window titled "LAN" with a close button (X) in the top right corner. The window is divided into three main sections: "IP Settings", "Network Settings", and "DHCP Server Settings".

IP Settings: IP Address is set to 192.168.100.1, and the network is 255.255.255.0 (/24).

Network Settings: Name is "Management Network", VLAN ID is 100, Inter-VLAN routing is disabled, Admin Access is checked, and Captive Portal is disabled.

DHCP Server Settings: DHCP Server is enabled, IP Range is 192.168.100.10 - 192.168.100.15, Lease Time is 1 Day, 0 Hours, 0 Mins, DNS Servers are assigned automatically, BOOTP is disabled, and there are no extended DHCP options. A DHCP Reservation table is empty.

At the bottom right, there are "Save" and "Cancel" buttons.

LAN			
IP Settings			
IP Address	192.168.100.1	255.255.255.0 (/24)	
Network Settings			
Name	Management Network		
VLAN ID	100		
Inter-VLAN routing	<input type="checkbox"/>		
Admin Access	<input checked="" type="checkbox"/>		
Captive Portal	<input type="checkbox"/>		
DHCP Server Settings			
DHCP Server	<input checked="" type="checkbox"/> Enable		
IP Range	192.168.100.10	-	192.168.100.15
Lease Time	1	Days	0
		Hours	0
		Mins	
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically		
BOOTP	<input type="checkbox"/>		
Extended DHCP Option	No Extended DHCP Option		
	Add		
DHCP Reservation			
	Name	MAC Address	Static IP

Staff Network

1. The staff network is for in store employee devices that are physically wired to the network. This would include shared printers, servers, and computers.
2. Inter VLAN routing is enabled for this network as Staff devices connected via Wi-Fi will need to be able to access these physically connected resources.
3. Devices on the Staff Network cannot communicate with devices on the POS network (as inter VLAN routing is disabled on the POS network).
4. The BR1 Admin Access is disabled as local staff should not manage the BR1 themselves - this is the responsibility of their IT department.

LAN

IP Settings

IP Address	10.0.14.1	255.255.255.0 (/24)
------------	-----------	---------------------

Network Settings

Name	Staff Network
Inter-VLAN routing	<input checked="" type="checkbox"/>
Admin Access	<input type="checkbox"/>
Captive Portal	<input type="checkbox"/>

DHCP Server Settings

DHCP Server	<input checked="" type="checkbox"/> Enable						
IP Range	10.0.14.10 - 10.0.14.200	255.255.255.0 (/24)					
Lease Time	1 Days 0 Hours 0 Mins						
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically						
BOOTP	<input type="checkbox"/>						
Extended DHCP Option	<table><thead><tr><th>Option</th><th>Value</th></tr></thead><tbody><tr><td colspan="2">No Extended DHCP Option</td></tr><tr><td colspan="2"><input type="button" value="Add"/></td></tr></tbody></table>	Option	Value	No Extended DHCP Option		<input type="button" value="Add"/>	
Option	Value						
No Extended DHCP Option							
<input type="button" value="Add"/>							
DHCP Reservation	<table><thead><tr><th>Name</th><th>MAC Address</th><th>Static IP</th></tr></thead><tbody><tr><td></td><td></td><td></td></tr></tbody></table> <input type="button" value="+"/>	Name	MAC Address	Static IP			
Name	MAC Address	Static IP					

PoS Network

1. The Point of Sale network has all of the Card terminals physically connected to it (via a switch - not shown in the diagram above).
2. It has inter VLAN routing disabled to block communications with other devices on other network segments.

LAN

IP Settings

IP Address: 255.255.255.0 (/24) ▼

Network Settings

Name:

VLAN ID:

Inter-VLAN routing:

Admin Access:

Captive Portal:

DHCP Server Settings

DHCP Server: Enable

IP Range: - 255.255.255.0 (/24) ▼

Lease Time: Days Hours Mins

DNS Servers: Assign DNS server automatically

BOOTP:

Extended DHCP Option

Option	Value
No Extended DHCP Option	
<input type="button" value="Add"/>	

DHCP Reservation

Name	MAC Address	Static IP	
			<input type="button" value="+"/>

6. Setup the Wireless Network

Staff Wi-Fi LAN Segment

1. Create a VLAN LAN segment to be used for staff Wi-Fi devices
2. Set VLAN ID and enable Inter-VLAN routing (to enable access to shared printers and servers connected directly to the LAN of the BR1)

LAN

IP Settings

IP Address: 10.0.15.1 | 255.255.255.0 (/24)

Network Settings

Name: Staff-WiFi

VLAN ID: 10

Inter-VLAN routing:

Admin Access:

Captive Portal:

DHCP Server Settings

DHCP Server: Enable

IP Range: 10.0.15.10 - 10.0.15.100 | 255.255.255.0 (/24)

Lease Time: 1 Days 0 Hours 0 Mins

DNS Servers: Assign DNS server automatically

BOOTP:

Extended DHCP Option

Option	Value
No Extended DHCP Option	
Add	

DHCP Reservation

Name	MAC Address	Static IP	
			+

Save Cancel

Wireless Network Settings

1. Create and configure SSID as hidden and secured with WPA2/Enterprise
2. Use MAC address whitelists for authorized Staff devices where possible (strongly recommended).

SSID Settings	
SSID	Staff WiFi
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
VLAN	Staff-WiFi (10)
Broadcast SSID	<input type="checkbox"/> Enable
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Multicast Filter	<input checked="" type="checkbox"/> Enable
Multicast Rate	MCS0/6M
IGMP Snooping	<input checked="" type="checkbox"/>
Layer 2 Isolation	<input checked="" type="checkbox"/>

Security Settings	
Security Policy	WPA2 - Enterprise
Encryption	AES:CCMP

RADIUS Server Settings	Primary Server	Secondary Server
Host	radius.mystore.com	
Secret	5tr0ng&C0mplic4tedPwd	
Authentication Port	1812 <input type="button" value="Default"/>	1812 <input type="button" value="Default"/>
Accounting Port	1813 <input type="button" value="Default"/>	1813 <input type="button" value="Default"/>

Access Control Settings	
Restriction Mode	Deny all except listed
MAC Address List	AC:22:0B:DA:95:D0 4C:80:93:41:01:B3

7. Setup Syslog Server

A remote syslog server should be configured for centralized logging of all router activity for auditing purposes.

Send Events to Remote Syslog Server	
Remote Syslog	<input checked="" type="checkbox"/>
Remote Syslog Host	syslog.mystore.com

8. Setup Email Alerts

Email alerts can be configured to notify on key system events

Email Notification Setup	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	smtp.mystore.com <input type="button" value="🔒"/> <input checked="" type="checkbox"/> Require authentication
SSL Encryption	<input checked="" type="checkbox"/> (Note: any server certificate will be accepted)
SMTP Port	465 <input type="button" value="Default"/>
SMTP User Name	notifications
SMTP Password <input type="button" value="🔒"/>
Confirm SMTP Password <input type="button" value="🔒"/>
Sender's Email Address	store01@mystore.com
Recipient's Email Address	notifications@store01.com

9. Configure 4G/LTE for Failover

On the dashboard drag the WAN connections so that the wired WAN (DSL in this example) is priority 1 and the cellular WAN is priority 2. This means that the cellular WAN will be automatically used for failover in the event the DSL is unavailable.

WAN Connection Status	
Priority 1 (Highest)	
<input checked="" type="checkbox"/> WAN	<input checked="" type="checkbox"/> Connected <input type="button" value="Details"/>
Priority 2	
<input type="checkbox"/> Cellular	<input type="checkbox"/> Standby 3G <input type="button" value="Details"/>
Priority 3	

10. Create a VPN to Head Office for Card Data Transmission

1. Create a VPN profile with 256bit AES encryption for transmitting card data to head office (use a long Pre-shared Key).
2. Optionally send all outbound traffic from the BR1 (including general internet access) via the head office VPN connection. This allows all web access to be filtered at the head office location as well as antivirus scanning using 3rd party tools.

PepVPN Profile					
Name	HeadOffice *				
Active	<input checked="" type="checkbox"/>				
SpeedFusion	Supported				
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF				
Authentication	<input checked="" type="radio"/> Remote ID / Pre-shared Key				
Remote ID / Pre-shared Key	<table border="1"><thead><tr><th>Remote ID</th><th>Pre-shared Key</th></tr></thead><tbody><tr><td>HeadOffice *</td><td>*</td></tr></tbody></table>	Remote ID	Pre-shared Key	HeadOffice *	*
Remote ID	Pre-shared Key				
HeadOffice *	*				
NAT Mode	<input type="checkbox"/>				
Remote IP Address / Host Names (Optional)	1.1.1.1 <small>If this field is empty, this field on the remote unit must be filled</small>				
Data Port	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="text"/>				
Bandwidth Limit	<input type="checkbox"/>				

Some incompatible options are disabled. To enable them, please make sure this profile is not being used by "Outbound Policy Rules", "DNS Proxy Settings" and "Send All Traffic To".

Save Cancel

3. Disable PepVPN backwards compatibility settings (in **Network > Speedfusion**)
This forces PepVPN to use TLS V1.2 (a requirement since PCI DSS V 3.1)

PepVPN Settings	
Backward Compatibility	<input type="radio"/> High (firmware 6.1+) <input checked="" type="radio"/> Restricted (firmware 6.2+)
Link Failure Detection Time	<input checked="" type="radio"/> Recommended (Approx. 15 secs) <input type="radio"/> Fast (Approx. 6 secs) <input type="radio"/> Faster (Approx. 2 secs) <input type="radio"/> Extreme (Under 1 sec)

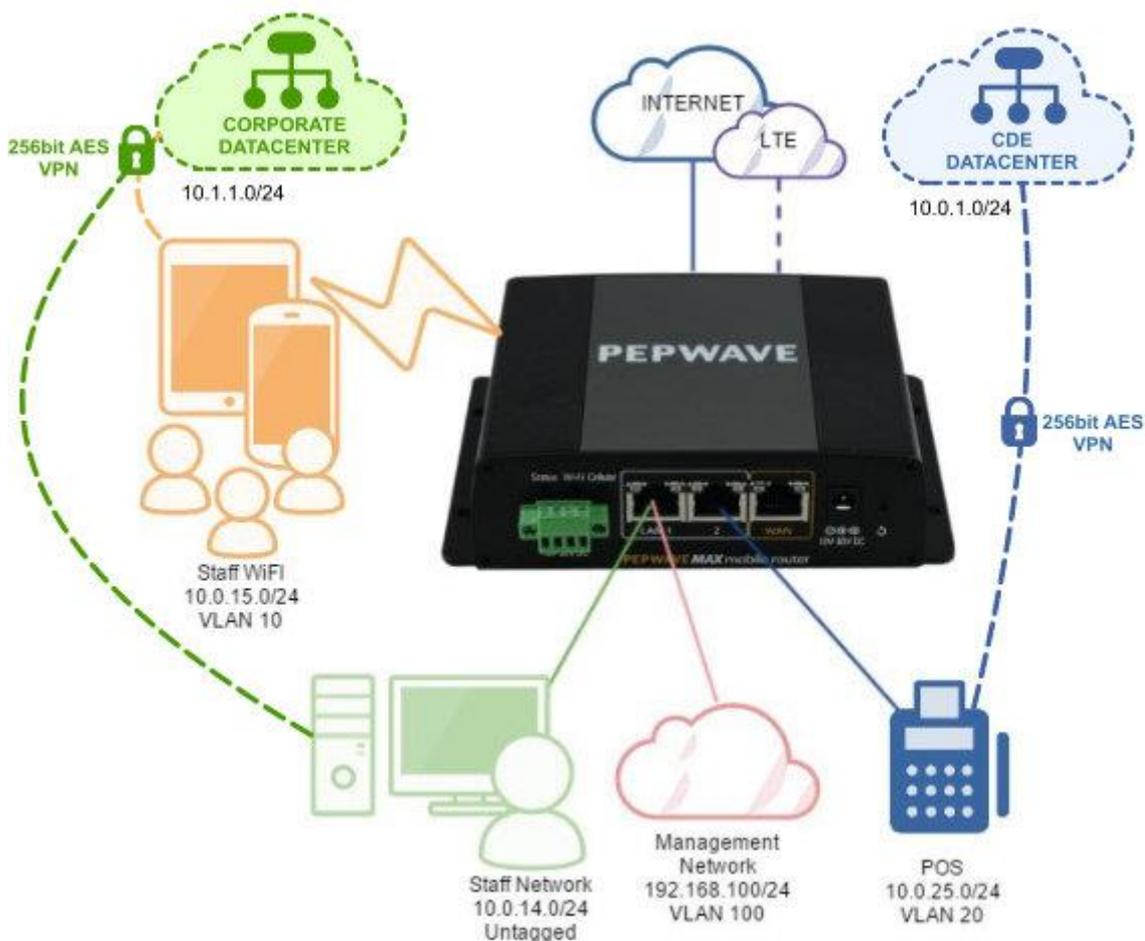
Help [Close](#)
To customize handshake port (TCP), please click [here](#).
To change backward compatibility option, please click [here](#).

11. Secure and Restrict CDE VPN Network Traffic

Once the VPN to the CDE datacenter is in place, by default any device on the LAN of the BR1 (Staff network, Management Network or POS network) can now route traffic to the CDE datacenter over that VPN connection.

This might be a desired configuration if the VPN connection terminates in a DMZ at the CDE datacenter as you could have web filtering appliances and proxies in place (so that all outbound user/web traffic is checked and filtered for compliance purposes) and additional firewalls protecting the servers deeper within the datacenter that contain card holder data, however you might want to segregate CDE and web/user VPN traffic completely.

Since the BR1 supports up to 2 PepVPN connections, one way to configure this would be to have a dedicated VPN connection for the CDE traffic, and another for the corporate user/web traffic (with the target datacenters potentially separate / geographically isolated from each other) – isolating the POS/CDE VPN network traffic completely.



To achieve this, we would do the following:

1. Create a New additional VPN connection to the corporate datacenter.

2. Create Two New Outbound Policies (**Advanced > Outbound Policy**)
 - a. Send All Outbound Traffic from the POS network (10.0.25.0/24) via the CDE Datacenter VPN (enforced).
 - b. Send All Other Outbound Traffic Via the Corporate Datacenter VPN (enforced).

Rules (Drag and drop rows to change rule order)					
Service	Algorithm	Source	Destination	Protocol / Port	
Send POS Via CDE DC	Enforced VPN: CDE-Datace...	IP Network 10.0.25.0/24	Any	Any	
Send all Via Corp DC	Enforced VPN: Corporate HQ	Any	Any	Any	
PepVPN Routes					
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	
Default	(Auto)				
<input type="button" value="Add Rule"/>					

3. Add Firewall Rules (**Advanced > Firewall | Access Rules**) to:
 - a. Block inbound and outbound traffic to and from the POS network over the WAN connections. This stops a malicious user who might have gained access to the POS network from being able to send data (like captured credit card information) out directly to the internet. It also blocks any inbound traffic from the WAN connections from reaching the POS network.

Outbound Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
Block POS Network	Any	10.0.25.0/24	Any		
Default	Any	Any	Any		
<input type="button" value="Add Rule"/>					

Inbound Firewall Rules (Drag and drop rows to change rule order)						
Rule	Protocol	WAN	Source IP Port	Destination IP Port	Policy	
Block POS Network	Any	Any	Any	10.0.25.0/24		
Default	Any	Any	Any	Any		
<input type="button" value="Add Rule"/>						

When the rest of the configuration detailed in this document has been completed these rules are redundant since all outbound traffic from the POS network is forced over the CDE VPN in outbound policies and all inbound ports should be closed on the WAN ports.

- b. Only Allow CDE traffic restricted by application port / destination IP to flow outbound from the POS network.

- c. Block all Other outbound traffic from the POS network destined for the CDE datacenter.

Internal Network Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
Only Allow POS Traffic	TCP	10.0.25.0/24	10.0.1.0/24 443	✓	✗
Block Other Traffic	Any	10.0.25.0/24	10.0.1.0/24	⊘	✗
Default	Any	Any	Any	✓	

In the example above, the POS machines (10.0.25.0/24) connect to servers in the CDE datacenter (10.0.1.0/24) over https (port TCP/443) – so this specific traffic is allowed. All other traffic from the POS network to the remote CDE Datacenter is blocked.

We would configure this to restrict the actions of any malicious user / device that forces their way onto the POS network (ie by plugging into the POS LAN physically or by hacking a POS machine itself and gaining admin privileges). By restricting the allowed outbound traffic to a single destination port, a malicious individual would be limited in the actions they can perform and the protocols they can use.

We don't need to add additional rules to block outbound traffic from the staff networks/VLANs to the CDE datacenter as the previous outbound policy configuration already forces all outbound traffic from these networks out over the corporate VPN.

12. InControl 2 Configuration

InControl 2 is a publicly accessible cloud based monitoring and management service provided by Peplink free of charge for in warranty devices.

Using InControl you can:

- Centrally monitor and manage your entire device estate.
- Confirm the availability of your devices and be alerted when a remote device goes offline or when a WAN link fails on a remote device.
- Centrally manage and deploy new firmware updates across all devices.
- Access the WebUI of remote devices easily for configuration changes.
- Get automatic configuration backups of all devices.
- Centrally manage WiFi configurations, WPA2 passwords and monitor wireless device bandwidth usage.
- Centrally manage automatic VPN configurations for all devices

- Centrally Manage User level permissions for remote device access using MFA

Multi-level security models have been baked into InControl 2 from its inception with the intention of providing granular access control to its features and capabilities throughout the service management and support chain. This enables organization admins to restrict who has access to manage and monitor remote devices connected to InControl 2.

Check with your PCI provider if they will accept the use of a public cloud management service.

Some providers will insist that any network device management tool be hosted internally, that the service should only be privately accessible (not shared with other organizations), and fully secured before it can be considered fully compliant.

If that is the case, Peplink can provide an InControl 2 appliance (either virtual or physical) that can be hosted internally on your corporate network to fulfill your management needs.

InControl 2 configuration

Whether you are using the publically accessible or privately hosted InControl 2 service the following should be considered for compliance.

- Multi Factor Authentication - all access to InControl 2 should be by named accounts using multi factor authentications.
- Access should be strictly limited to authorized internal support staff.
- Account usage should be regularly audited to spot any anomalies (e.g. external source IPs for user logon, extra ordinary use outside of office hours)

Summary

This guide has shown how a Peplink BR1 might be deployed in a retail environment in a way that isolates and secures any credit card processing device from all other devices that are directly or indirectly connected to the router.

At the same time, the PoS devices can communicate securely with the CDE datacenter over a 256bit AES encrypted VPN connection that has resilience due to the potential use of a cellular connection in the event the primary fixed line internet service was to fail.

Obviously, this is only one possible configuration, using only one device model from the Peplink range, other deployments and devices will need differing configurations to maintain compliance.

Our final recommendation is that any network deployment that needs to be fully PCI/DSS compliant should undertake regular security drills and evaluations - including 3rd party penetration testing by registered approved Pentest & network security companies.

Disclaimer

The contents of this guide should be taken as the current configuration recommendation for Peplink & Pepwave devices at the time of writing.

However, PCI DSS standards are continuously evolving, and your specific requirement and your provider's interpretation of that may vary. This guide is just a basic overview to introduce the concepts and should not be relied upon to assume or confirm compliance or considered in any way exhaustive of the requirements.