PCI DSS 3.0 Compliance Guide

August 2015

Document Information

Version	Notes	Author
1.0	Released.	Martin Langmaid (mlangmaid@peplink.com)
1.0.1	Minor changes and clarifications.	Peplink Team

Table of Contents

PCI DSS 3.0 and Peplink/Pepwave Routers **2**

Introduction 2

PCI Data Security Standard - High Level Overview **3**

How does this apply to your Peplink router? 3

The DSS requirements for your firewall **4**

Configuration Example **5**

Configuration Recommendations **6**

How does this apply to your Peplink router? 3

1. Upgrade Router to latest Firmware 6
2. Change the Default Admin Username & Password 6
3. Secure the WAN Configuration 6
4. Configure the Firewall 7
5. Segment the network using VLANs 8
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. InControl 2 Configuration 15

Summary **16**

Disclaimer **16**

PCI DSS 3.0 and Peplink/Pepwave Routers

Introduction

The Payment Card Industry Data Security Standard v3 ("PCI 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.

PCI Data Security Standard - High Level Overview

Build and maintain a secure network	• 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	• Protect stored cardholder data • Encrypt transmission of cardholder data across open and public networks.
Maintain a Vulnerability Management program	• Use and regularly update anti-virus software or programs • Develop and maintain secure systems and applications
Implement Strong Access Control measures	• 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	• 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.

How does this apply to your Peplink/Pepwave 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.

We used the MAX BR1 in this document as an example and the same principles can be applied to other Peplink/Pepwave routers to attain PCI DSS compliance.

For the simplicity of this document, the terminology "Peplink routers" shall refer to both "Peplink and Pepwave" routers.

The DSS Requirements for your firewall

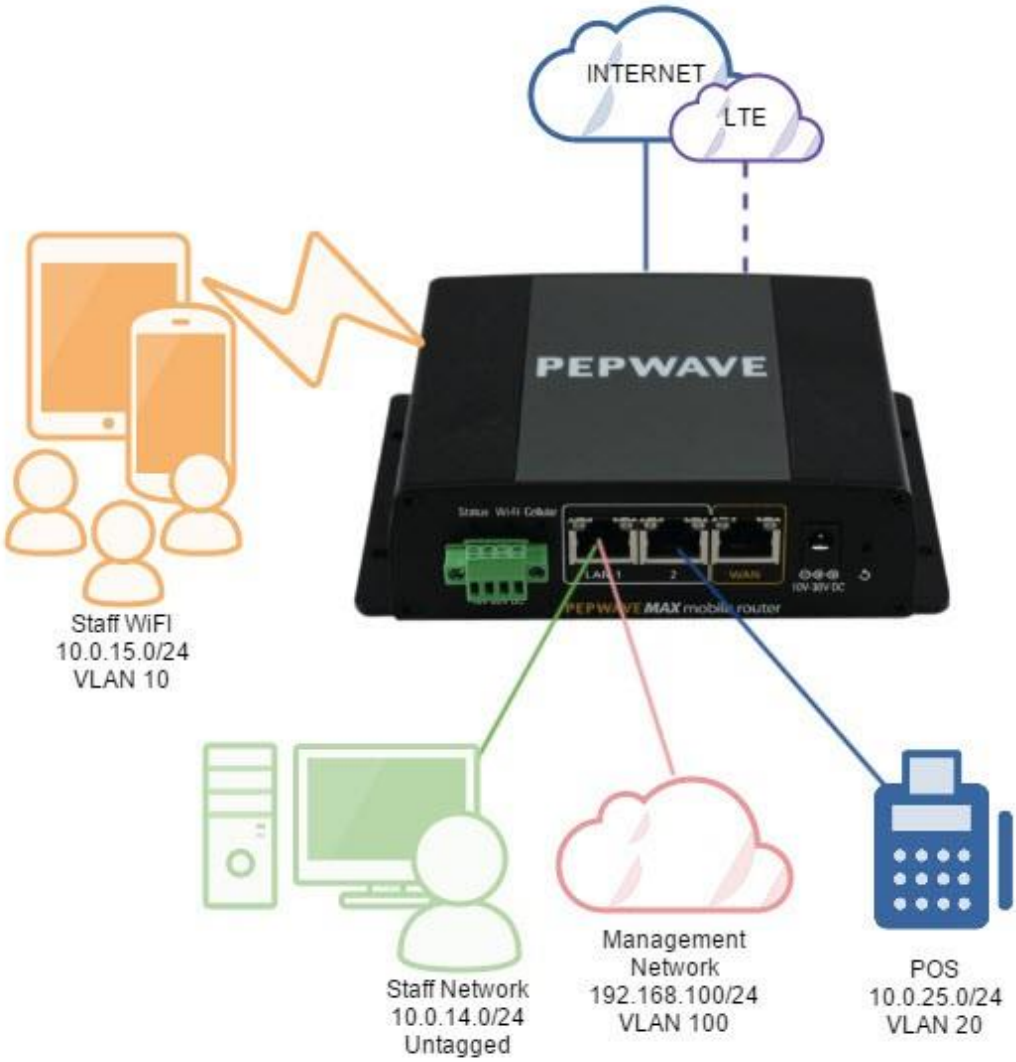
1. Install and maintain a firewall on any network which processes card data
2. The firewall must only permit services/traffic which is necessary to that Cardholder Data Environment (CDE).
3. Document your network fully (with diagrams and inventory) and justify all enabled services.
4. Only authorized 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.
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.



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.

3. Secure the WAN Configuration

Disable UPnP & NAT-PMP

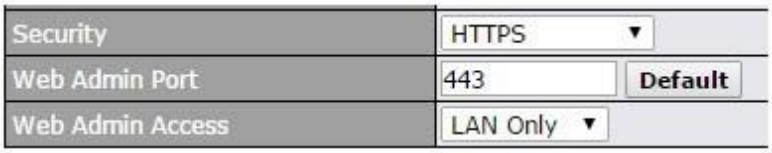
Turn off UPnP and NAT PMP features in **Advanced -> Port Forwarding**

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.

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' in ***System -> Admin Security***



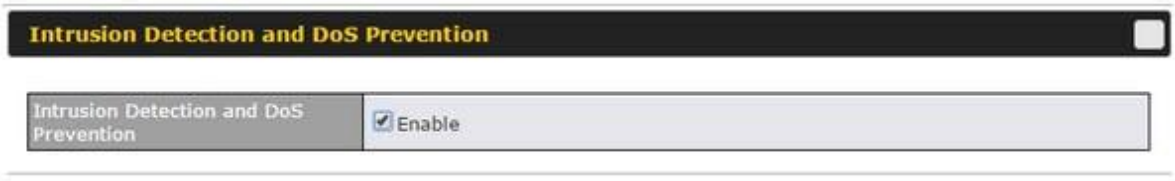
4. Configure the Firewall

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***



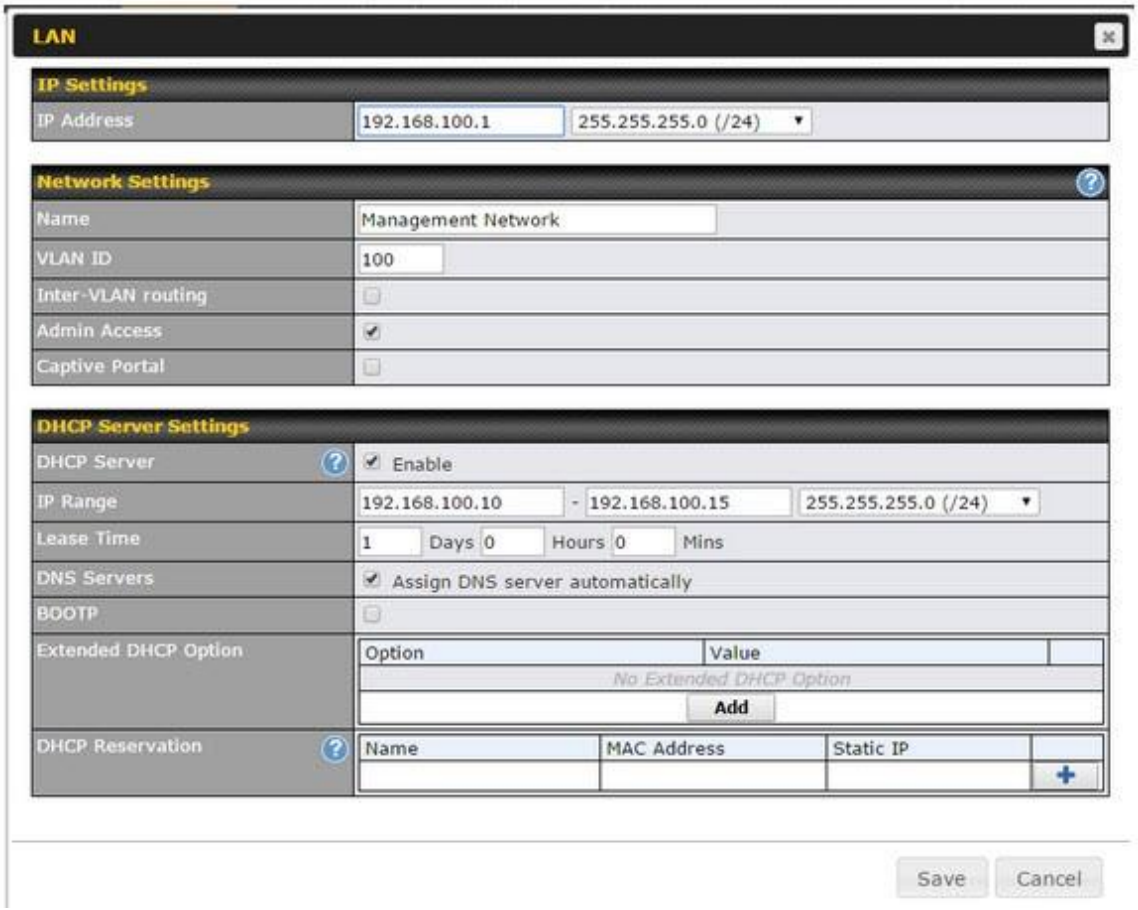
Use MAC Filtering to Whitelist devices on PoS VLAN

One method to restrict unauthorized activity on a LAN segment is to only allow communication out of the network by known devices. To do this add a deny all rules for that particular network segment and add a rule per device.

5. Segment the network using VLANs

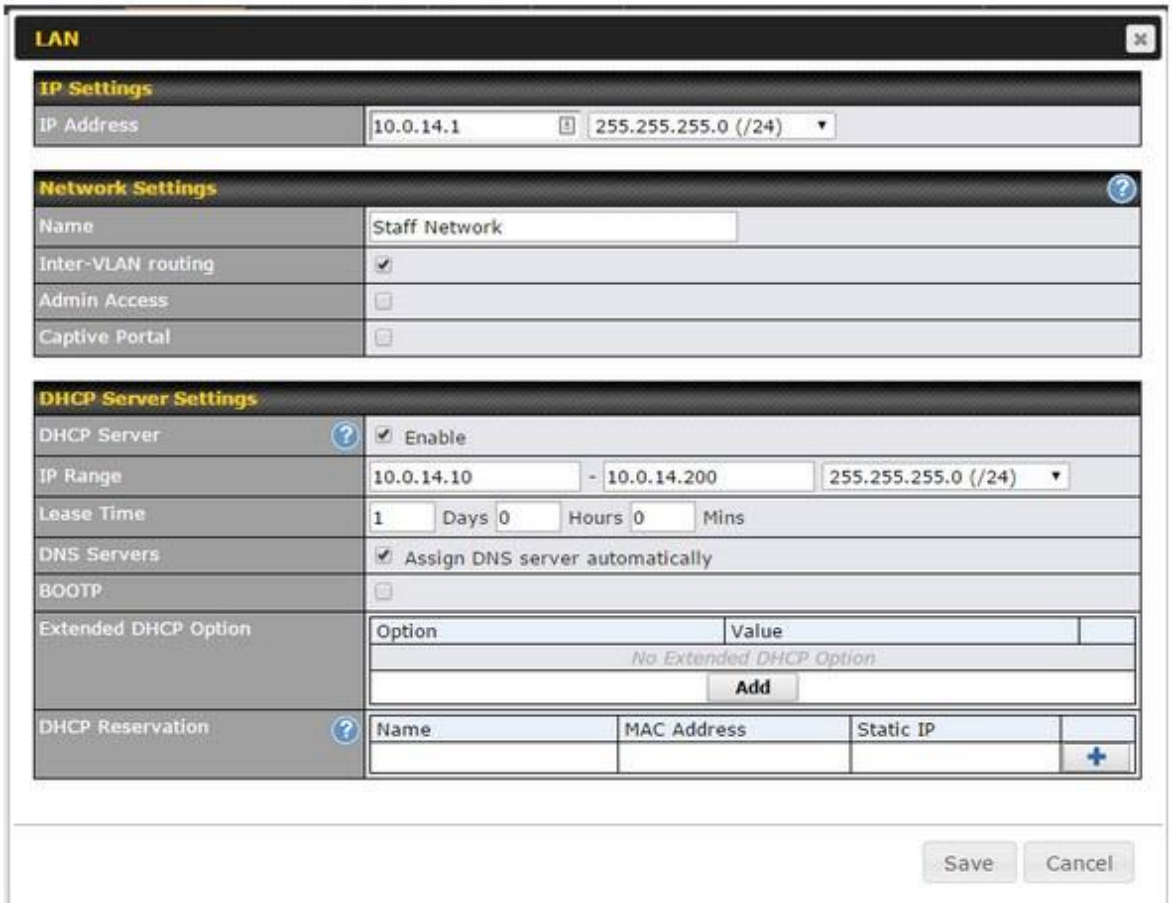
Management Network

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 an intruder was able to 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 be used by an authorized IT engineer who knows the BR1 password.



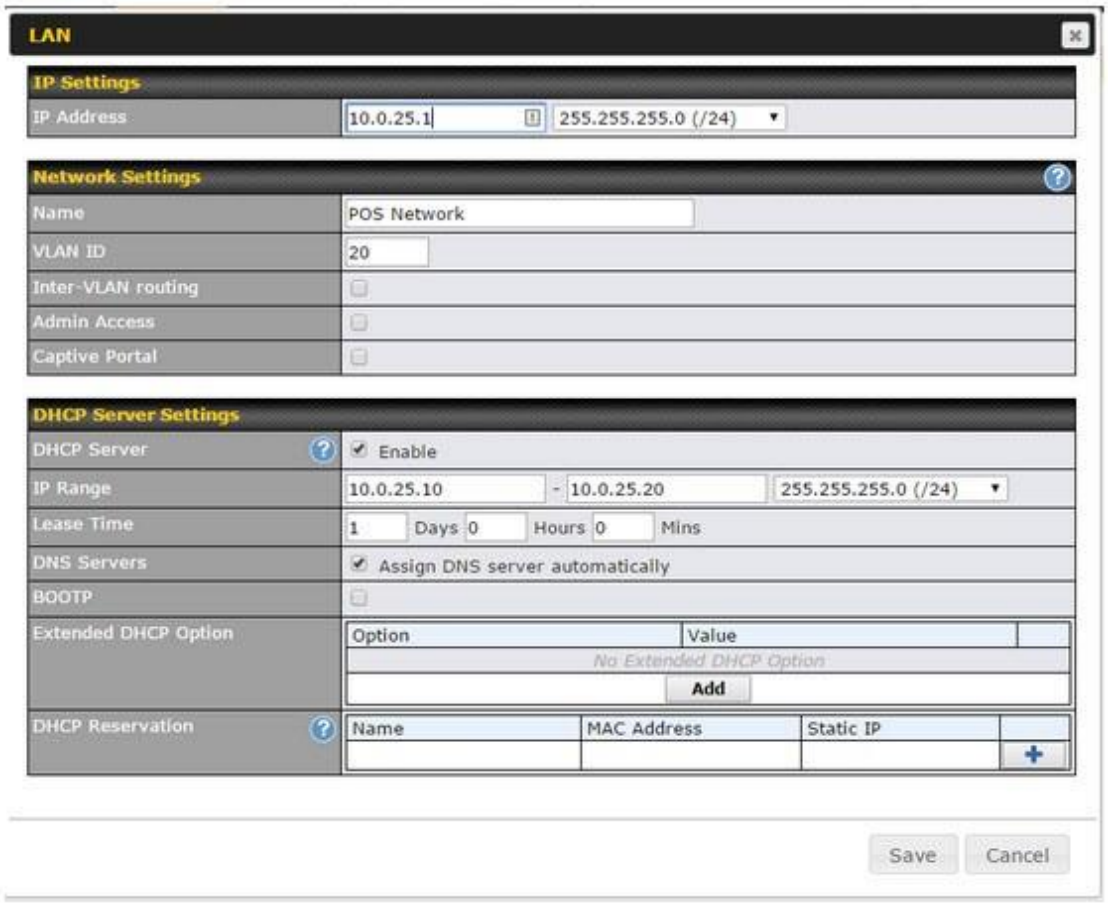
Staff Network

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 can not 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.



POS Network

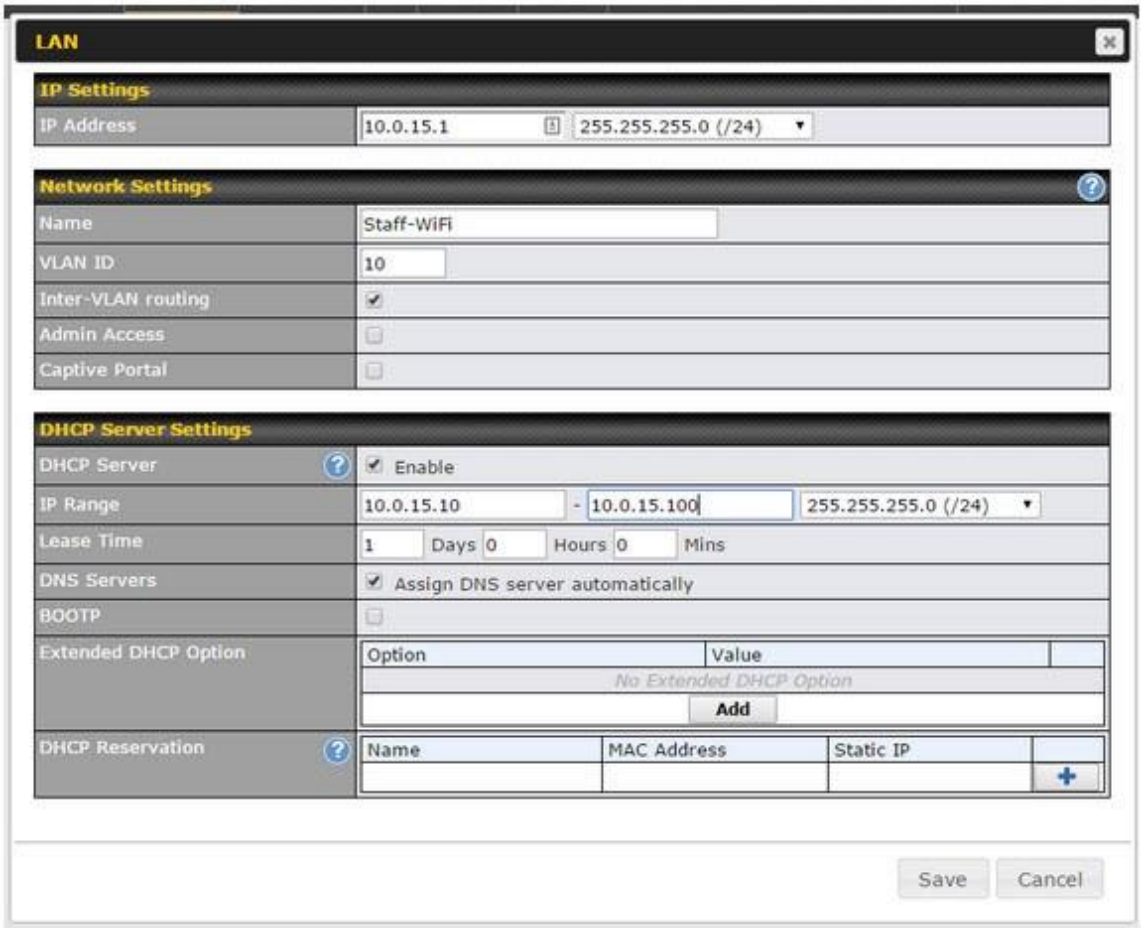
1. The Point of Sale network has all of the Card terminals physically connected to it (via a switch - not shown in the diagram above).
2. It has inter VLAN routing disabled to block communications with other devices on other network segments.



6. Setup the Wireless Network

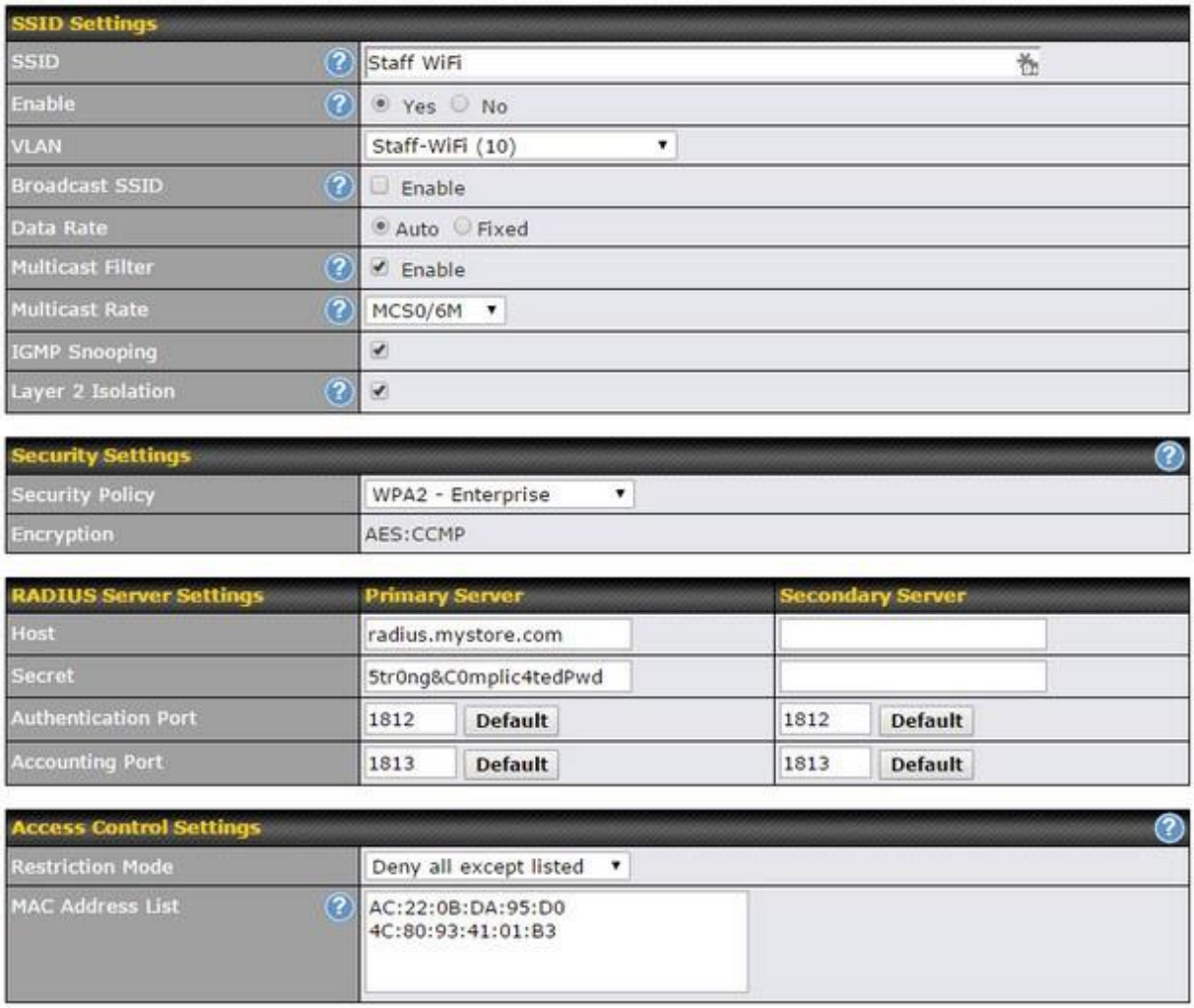
Staff Wi-Fi LAN Segment

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)



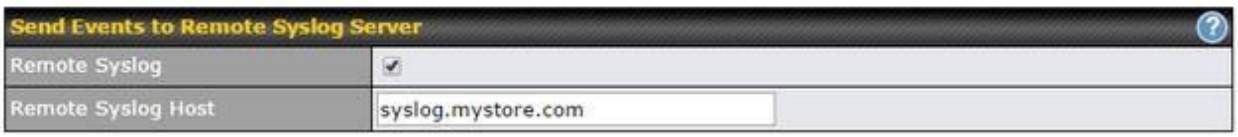
Wireless Network Settings

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).



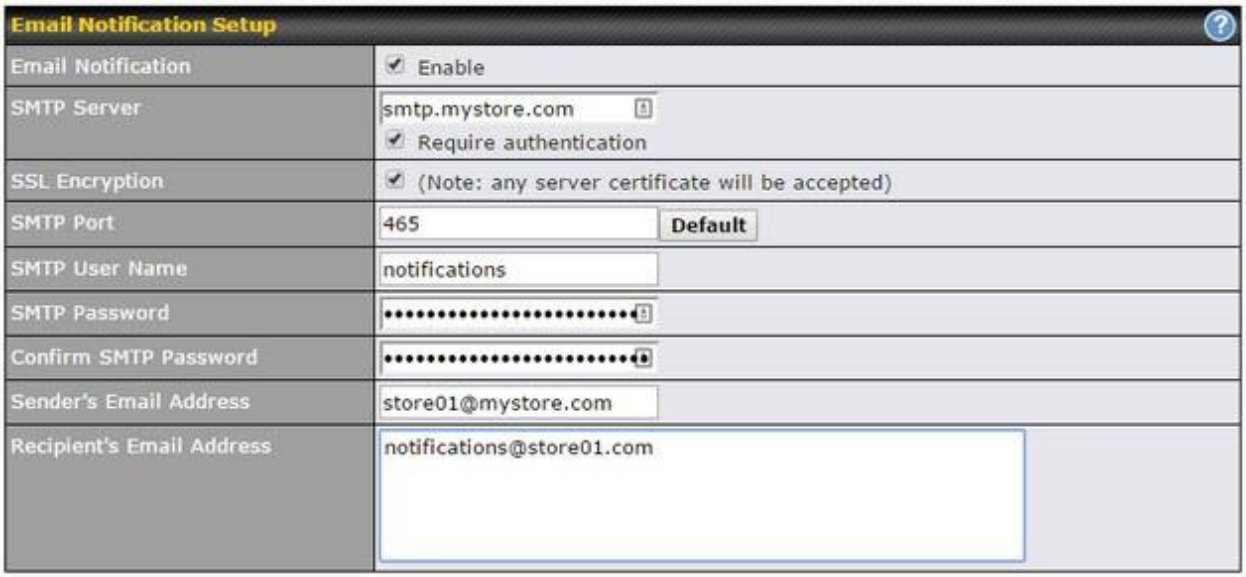
7. Setup Syslog Server

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



8. Setup Email Alerts

Email alerts can be configured to notify on key system events

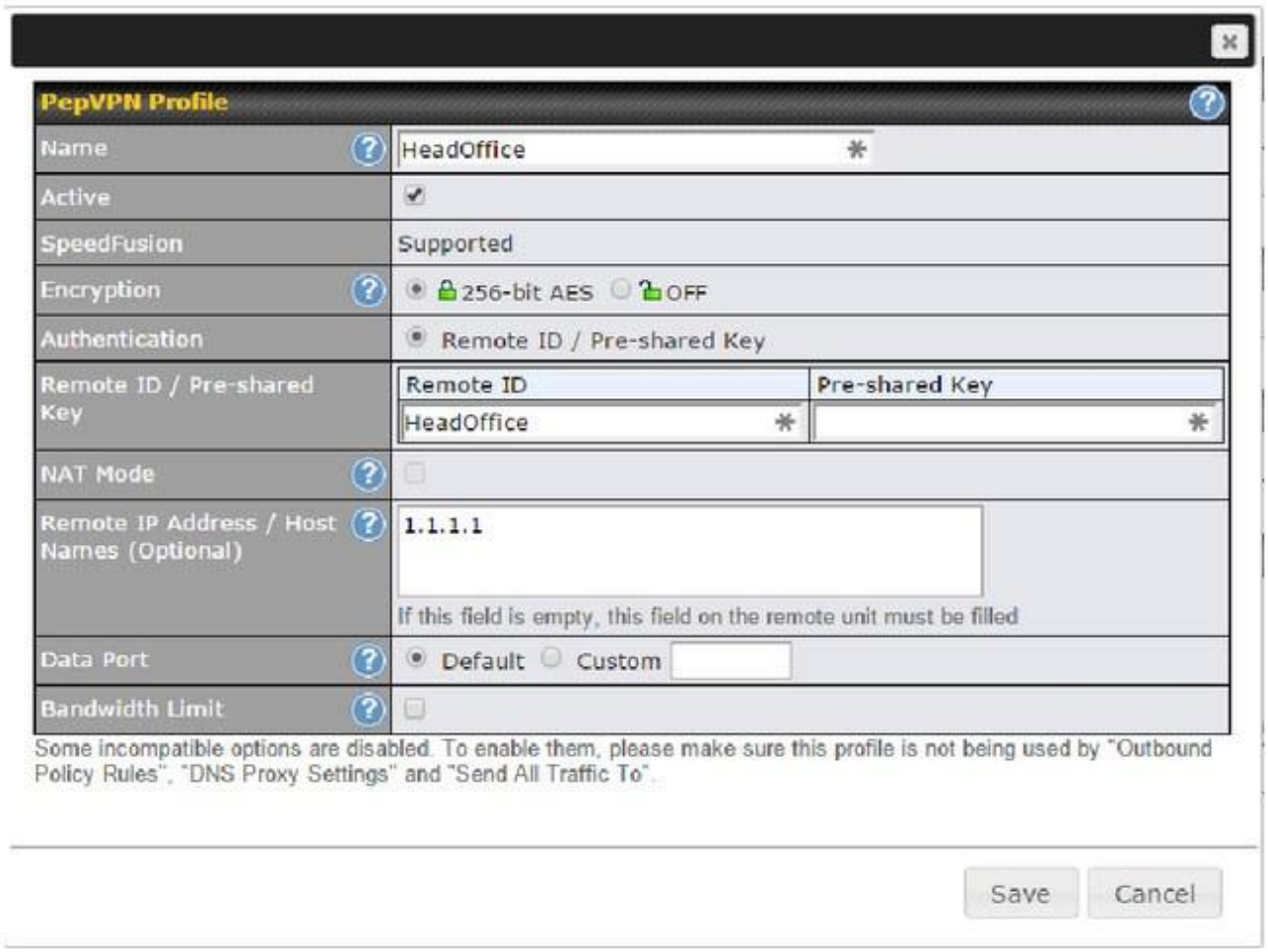


9. Configure 4G/LTE for Failover

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.

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 PSK for additional security).
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.



11. InControl 2 Configuration

InControl 2 is a publically 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

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.

- Two Factor Authentication - all access to InControl 2 should be by named accounts using two factor authentication.
- 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 MAX BR1 router 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 head office 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 were 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 but with the same principles.

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.