This guide will assist you with securing your Point of Sale network from unwanted external traffic. The implementation of firewalls and strict security policies is critical to ensure the protection of cardholder data. Following these steps will ensure compliance within the PCI DSS.

What is a firewall?

A firewall can be described as a device or service that prevents unauthorized access to a secure network, while still allowing authorized communications. A firewall is the security barrier that separates your POS systems from any unsecured network. Requirement 1 of the PCI DSS states that a firewall must be installed and maintained on any POS network.

Choosing a firewall:

There are many different types of firewalls available, depending on the level of security desired. The varying levels of security and pricing can easily cause confusion, so this document has been addresses a basic low-cost solution that will address the requirements of the PCI DSS. The following settings and configuration examples are taken from a **Netgear RP614** router. This device offers the stateful packet inspection, as required by Section 1.3.6 of the PCI DSS, and is available for under $100.

Installation:

A firewall must exist between the network segment that captures and processes cardholder data and any other segment that provides wireless or internet traffic. A detailed example of this can be found in the **VersiTech Recommended Network Diagram** document.

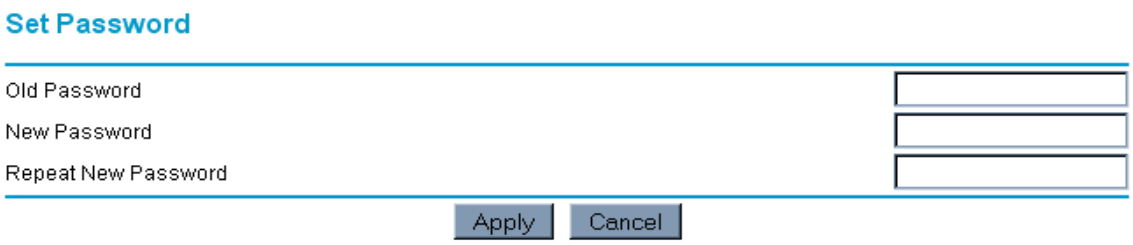
Resetting default account access:

One of the most critical elements to installing a secure firewall solution is to modify the default administrative access to the device. A quick internet search can reveal the default administrative user name and password for most routers and firewalls available on the market today. Adjusting these credentials is the first step in securing your POS network.

A secure administrative access account must include the following restrictions:

- Password must contain at least 7 characters.
- Password must contain both numeric and alphabetic characters.
- Password must be reset after 90 days.
- Password must not be the same as any 4 of the previous used.

Fig 01: Password change screen.



Ensuring upgraded firmware:

A firewall's firmware is the software operating system that controls the functionality of the device. This firmware must be updated with manufacturer's newest revision to ensure that the device is protected from any bugs or potential security exploits. Section 1.1.1 of the PCI DSS requires that a formal process be established to review and approve all changes to router or firewall configuration. This review process should include a maintenance update of the device's current firmware revision.

Fig 02: Router upgrade screen.

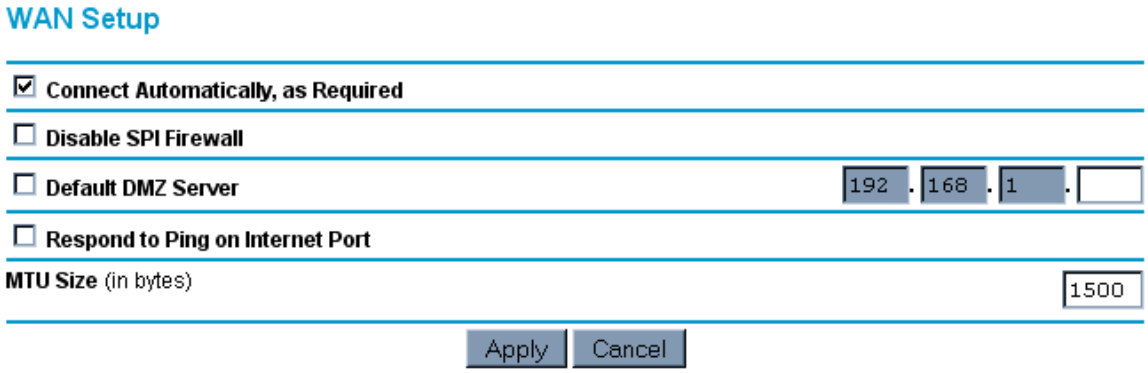
Enabling SPI and establishing a DMZ:

Section 1.3.6. of the PCI DSS requires that stateful packet inspection (SPI) must exist within any firewall solution used. This is a critical element, as it ensures that data packets are thoroughly scanned prior to their leaving your network, while still allowing for a level of performance that suits the needs of your business. Essentially, a SPI firewall will provide the highest level of security while not drastically impeding the communication between your POS clients or server.

If your network includes any public-facing services, such as a web or FTP server, these must be included into a perimeter network segment, also known as a DMZ. The DMZ isolates any network services or devices to an area that does not share resources with your POS systems and database. This removes these high-risk machines from transferring any potential exploits or attacks to an area of your network that contains cardholder data. A firewall must be implemented between

any existing DMZ and the POS network. See the **VersiTech Recommended Network Diagram** document for a visual depiction of how to integrate a DMZ into your network. It is not necessary to implement a DMZ if your network includes only private services.

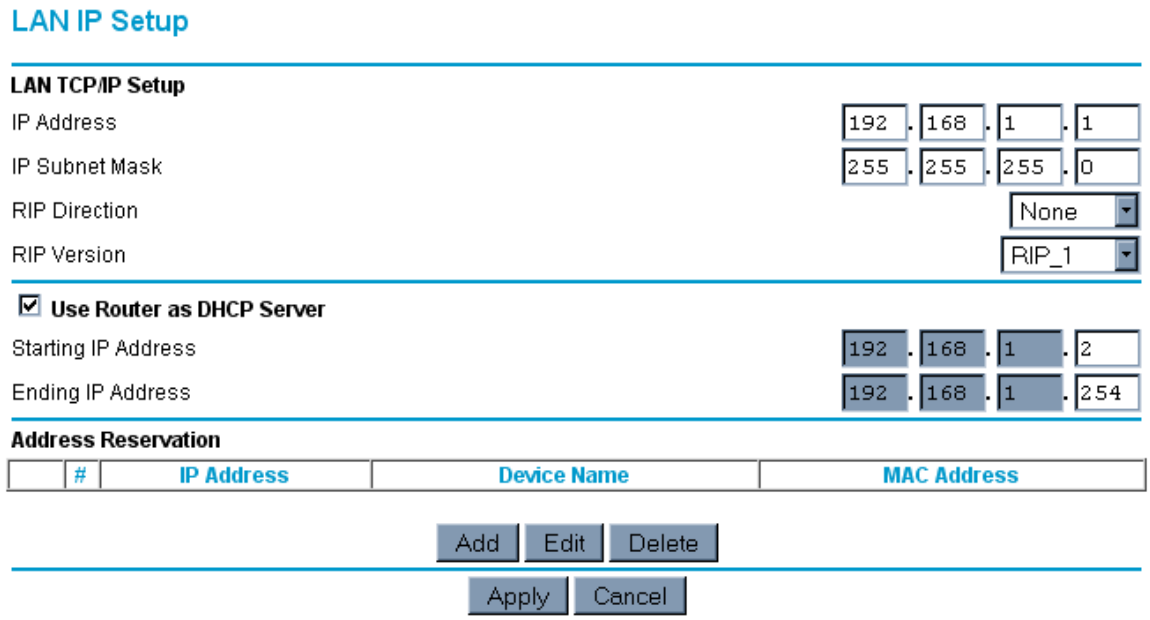
Fig 03: Advanced router configuration.



Creating a subnet:

A device that operates both as a router and a firewall (e.g. Netgear RP614) will include the ability to create a separate subnet for all connected machines. A subnet is a separate segment within your network that isolates machines based on their IP address range. In the example below, the subnet provided by the router is 192.168.1.x. The last number in the IP address is assigned uniquely to each device connected. The service that provides this automatic address assignment is called DHCP, and should be enabled unless you wish to configure each device manually. Creating a separate subnet for your POS machines will help to ensure that they reside in a secured segment of your network.

Fig 04: Advanced router configuration.



Remote Management and Access:

Section 1.4.2 of the PCI DSS states that implementation of a firewall must include rules that prevent public access to cardholder data. This protection is paramount, as cardholder data must reside at all times in an area of your network that is 100% secure from external access. Many routers and firewalls include the ability to be remotely managed. This feature must be disabled. Additionally, any public-facing servers or services within your network must reside within the DMZ. At no time can cardholder data be transmitted from the secure POS network to the DMZ. Essentially, this data must always reside in an area where remote access to it, or any device within its segment, remains completely restricted.

Fig 05: Disabling remote management.