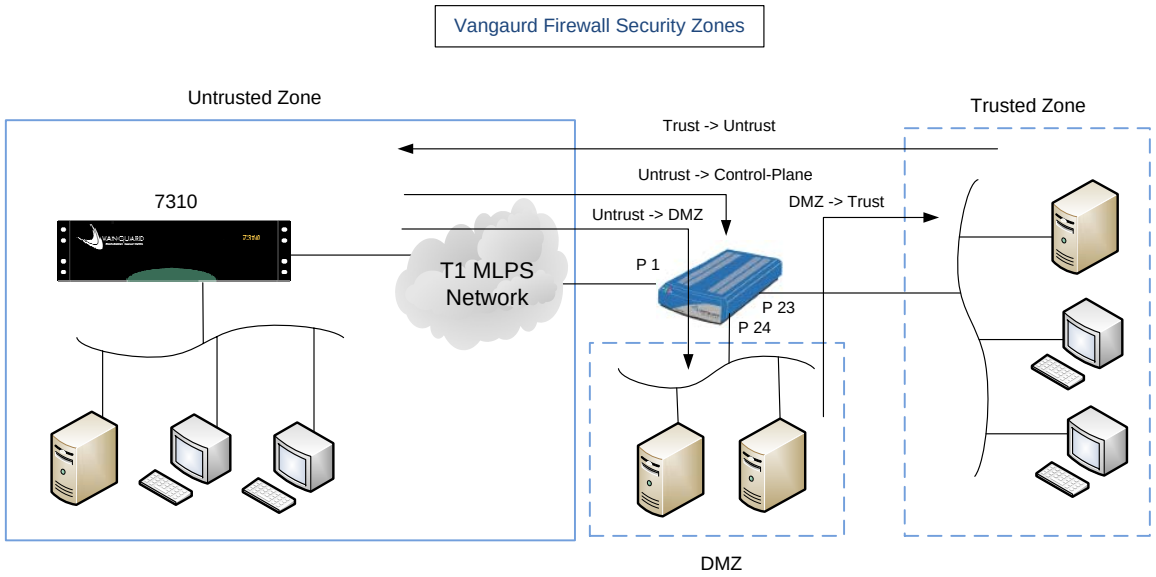
Retail Stores Networks and PCI compliance

Executive Summary:
Given the increasing reliance on public networks (Wired and Wireless) and the large potential for brand damage and loss of customer trust, retail stores must secure customer credit card information and take measures to protect this data from unauthorized access and other security threats. Adhering to PCI DSS requirements is one first step, but a comprehensive security posture is needed there where customer credit card information is acquired, transmitted or stored. Vanguard Networks and its Resellers Partners offer a comprehensive set of products and services (See Addendum A for a detailed compliance matrix) to ensure this goal fulfillment.

Firewall at the Store:
There is a trend to use public broadband IP networks to connect stores to the network. In this scenario, the store is more likely to become victim of security breaches.
Vanguard Networks' Firewall feature set provides an intermediate Security Zone that can be accessible from both external and internal users if allowed by the configured policies.
The Vanguard Networks Router provides four types of security zones:

- Trust
- Untrusted
- DMZ
- Control-Plane



The Demilitarized Zone (DMZ) provides external users a controlled access to resources. The Control-Plane controls any incoming data directed to internal interfaces in the Vanguard Networks Router itself.

Router Interfaces are assigned to Trust and/or DMZ. Unassigned interfaces, by default, belong to Untrusted zones.
Firewall Policies are configured between Zones, not Interfaces, based on Policy Action (Permit or Deny), Source Subnet, Source Mask, Destination Subnet, Destination Mask, Protocol (TCP, UDP, ICMP, or ANY), Source/Destination Port Range.

Firewall Monitoring: Firewall traffic logs can be generated by configuring Traffic Logging as Start, End, or Start+End. "Start" allows the node to generate an event log when a flow matching this configured policy is created. "End" generates an event log when a flow matching the policy closes. START+END covers both Start and End.
These Firewall traffic logs can be passed to the SYSLOG Server feature, which requires configuring SYSLOG Type with TRAFFIC and SYSLOG Severity with NOTICE. With these SYSLOG Server configurations, when incoming and/or outgoing flows match the configured Firewall policies, Firewall traffic logs will be generated and sent to the configured SYSLOG server.

Use of DMZ: Using Demilitarized Zone (DMZ), Vanguard routers can limit inbound and outbound traffic to only the necessary protocols for specific data environments. Vanguard Router's Firewall-DMZ feature provides the functionality to control any types of traffic as required in the PCI standard.

Securing the Store Router: To protect from security breaches, Vanguard Router supports 7 different security access privileges for username and password access, which are applied to SSH version 2.0, Radius Authentication, and X.509 Digital Certificate. It also supports a required minimum password length which must be at least 7 characters and include both alpha and numeric characters, eliminating prevalent passwords such as "lab" and "network."
Vanguard Router can also eliminate Denial of Service (DoS) attacks such as bad packets, bad TCO flags, and fake requests to enhance network security and ensure PCI compliance.

NAT: IP masquerading, Network Address Translation (NAT), can translate an internal or private IP address to a global IP address to enable devices in a private network access to external or global domains.
Using PPP, PPPoE, or DHCP, Vanguard Networks Router can assign a learned or pre-configured external IP address to the internal or private IP address statically or dynamically.
And Network Address Port Translation (NAPT) extends the capability of NAT by allowing Many-to-One address mapping, which allows multiple hosts to access the external domain simultaneously using a single external address.

Encryption: Vanguard Networks Router's data protection is provided by either software or hardware based encryption engines. DES_CBC and 3DES_CBC are available with the software encryption. The optional hardware engine on the motherboard can also perform

AES encryption (128, 192 and 256 bit key lengths), and provides faster encryption, stronger security, and higher performance.
For Encapsulating Security Payload (ESP) with Authentication, HMAC-MD5-96 and HMAC-SHA1-96 encryption algorithms are available.

Vanguard Networks router can function as the hub of an enterprise network. It is capable of terminating up to 1,000 encrypted tunnels and provides an integrated stateful Firewall at the hub site. The Firewall feature can also be configured on any Vanguard router at any remote site as required.

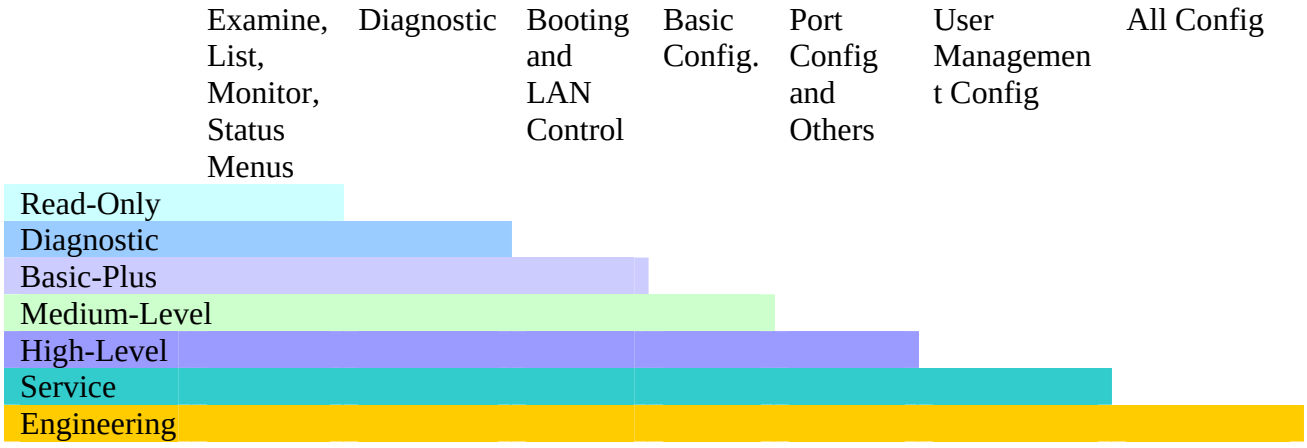
Vanguard Networks Firewall and ICSA Compliance:

Vanguard Networks Routers´ Firewall is ICSA certifiable.

Logging: All inbound and outbound access requests from private or public network clients through and/or into Vanguard Router will generate Firewall traffic logs for both permitted and denied policies. These traffic logs include Policy, Date and Time, Action (Permitted or Denied), Source/Destination IP Address, Port Number, Protocol Type, Packets Sent/Received and Current Access Status (Create, Ageout, FIN, Reset, etc). The logs can be seen in the CTP's Firewall Stats Menu, Firewall Traffic Log. Also, they can be sent to a Syslog Server by configuring both SYSLOG Type to TRAFFIC and SYSLOG Severity to NOTICE in a SYSLOG Server configuration.

[Note: Vanguard Networks Router does not support, at the moment, event correlation or event sequence number.]

Administrative Functions: Vanguard Networks Router provides security access privileges, which can configure 7 different access levels (Read-Only, Diagnostic, Basic-Plus, Medium-Level, High-Level, Service, and Engineering).



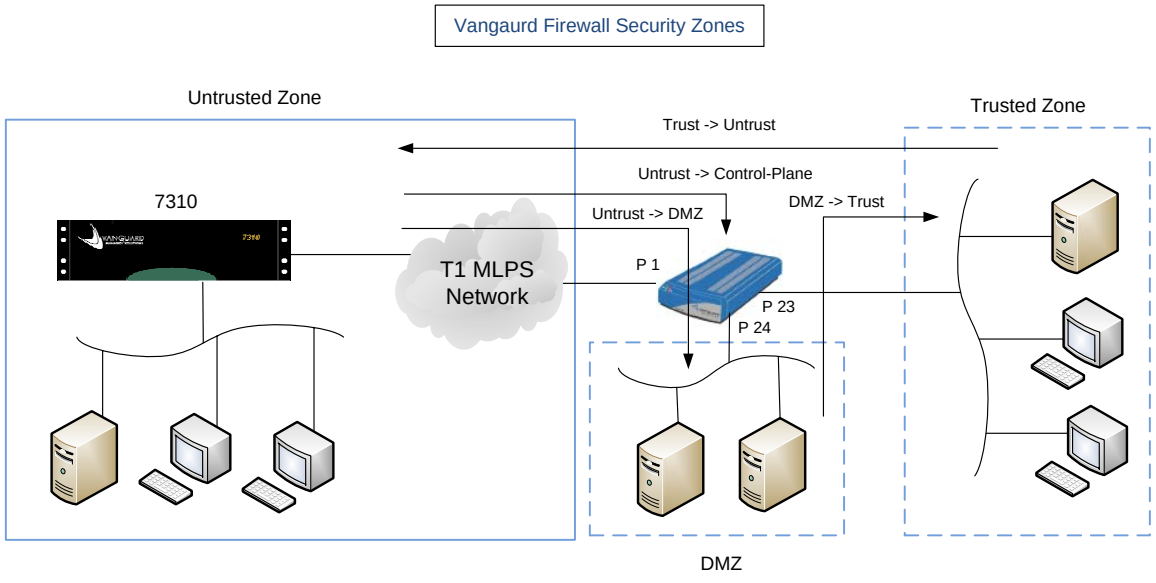
For example, the Read-Only access privilege can check the configuration and monitor the status. But it cannot create or modify the configuration nor boot the node. On the other hand, the Engineering level provides a root access to control and manage all the functions

running on the node, setting time and date, creating, modifying and/or deleting configurations, checking logged alarms, and so forth.

For network security access, Interface Services can filter what types of services should be allowed to each router interface. By configuring protocol types, the interface will accept the configured service. The options available are:
TELNET+HTTP+SSH+PING+SNMP+TFTP+SoTCP
As for Telnet access, Vanguard Router can deny all Telnet access easily by configuring Node Record's Enable/Disable Telnet Server as DISABLE. Or not including TELNET in Interface will deny all Telnet accesses to that configured router interface.

Persistence: The software image and the saved configuration are stored on onboard Flash and a lithium battery on the motherboard is used to maintain the node's real-time clock. Thus, Vanguard Router will not lose the software image, the saved configuration, and Date and Time because of the loss or removal of power. When electrical power is reapplied, the exactly same software/ Firewall configuration and real Date and Time will be back on the node.

Functional Testing: Once Vanguard Router's Firewall is enabled, associated policies must be configured, especially to permit data flows.
Otherwise, all the incoming and outgoing data will be denied by default.
Firewall Policies must be configured for each data flow direction if needed:
Trust -> Untrust
Untrust -> Trust
Trust -> DMZ
DMZ -> Trust
DMZ -> Untrust
Trust -> Control-Plane
Untrust -> Control-Plane
DMZ -> Control-Plane



The newly implemented Control-Plane parameter can control incoming data to Vanguard Router itself, especially managing access protocols such as Telnet, SSH, and TFTP.

Security Testing: Vanguard Router correctly reassembles fragmented IP packets and then passes the reassembled IP packets towards destinations as long as these packets meet the configured policies. If the packets violate the security policy, they will be denied and discarded.

Documentation: The Firewall user manual shows how the feature works and how each parameter should be configured in a user-friendly manner.
It is available at http://www.vanguardnetworks.com/support-manuals.htm.

Addendum A

The PCI Security Standard and Vanguard Networks Solutions
Vanguard Networks and its Reseller Partners provide the features and services needed to make a network PCI compliant.

PCI DSS Requirements	Vanguard Networks solution
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.	
1.1 Establish firewall and router configuration standards.	**As of Vanguard Networks ApplicationsWare release 7.2, Firewall functionality is included which supports Trust, Untrust, DMZ (demilitarized) as well as the internal Network Zone. What data may pass between these zones can be modified through configuration to protect cardholder data from other portions of the network. Vanguard Networks Services can assist in the configuration, documentation and process requirements.**
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	**Only traffic that is specifically configured to pass between zones will be passed. By default, data from untrusted zones will not be permitted pass.**
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	**Our Firewall policies provide the functionality to prohibit public access to card holder data via the use of the Firewall DMZ zone policies. ApplicationsWare software also provides NAT functionality which will provide IP address masquerading to prevent internal addresses from being translated and revealed on the Internet**
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	**Vanguard Networks do not provide mobile devices as such.**
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	
2.1 Always change vendor-supplied defaults **before** installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	**Vanguard Networks routers supports password changes, updating and removal of user accounts. Backdoor passwords can be disabled by an access key.**
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.	**Vanguard Networks is working to become fully compliant with SANS, NIST and CIS standards. Unprotected features such as Telnet, TFTP, HTTP and SNMPv1 should be omitted from the software upon creation.**

2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	**Vanguard Networks routers support SSH for administrative access. Vanguard Network Services can assist in support of security policies and procedures.**
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*	**Vanguard Networks Services can aid with network design and configuration to ensure that cardholder data which transverses through our equipment is isolated.**
Requirement 3: Protect stored cardholder data	
Requirements 3.1 to 3.6 refer to storing of cardholder data.	**Vanguard Networks router's do not store any data, therefore these requirements are not applicable.**
Requirement 4: Encrypt transmission of cardholder data across open, public networks	
4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.	**Vanguard Networks Routers can be configured for MD5 and 3DES, as well as SHA-1 and AES which is recommended by PCI.**
4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	**Vanguard Networks Services can aid with network design and configuration to ensure compliance**
Requirement 5: Use and regularly update anti-virus software or programs	
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**Requirements 5.1 to 5.2 refer to the use of anti-virus protection for PC's and servers which is non-applicable to our routers.**
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	
Requirement 6: Develop and maintain secure systems and applications	
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	**Requirements 6.1 to 6.4 refer to requirements for secure software development and testing. We are working to ensure that our current security procedures adhere to the specific requirements. Be aware that Vanguard Networks is ISO9000 certified which addresses many of these requirements.**
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	
6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices and incorporate information security throughout the software development life cycle. These processes must include the following:	

6.4 Follow change control procedures for all changes to system components. The procedures must include the following:	
6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the *Open Web Application Security Project Guide.* Cover prevention of common coding vulnerabilities in software development processes, to include the following:	**Vanguard Networks routers software may contain an HTTP module which allows access from a web browser. Currently this application is not secure and needs to be omitted from the build in order to comply with this requirement. Secure access to the node should be done using SSH. Vanguard Networks is working to provide secure file transfers via SSH.**
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 limitations must include the following:	**Vanguard Networks routers supports multiple usernames with specific privileges and access rights. This is also available when using Radius for verification.**
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**Vanguard Networks routers supports multiple usernames with specific privileges and access rights. This is also available when using RADIUS for authentication. Note that our current default setting allows connections, this must be changed to comply.**
Requirement 8: Assign a unique ID to each person with computer access.	
8.1 Assign all users a unique username before allowing them to access system components or cardholder data.	**This is a procedure not directly related to Vanguard Networks Routers operation.**
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: ▪ Password or passphrase ▪ Two-factor authentication (e.g., token devices, smart cards, biometrics, or public keys)	**Vanguard Networks routers supports multiple usernames and passwords.**
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. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	**Vanguard Network routers Support RADIUS authentication for SSH. Certificates are supported for IPSEC VPNs and SSH.**
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography based on approved standards (defined in *PCI DSS Glossary, Abbreviations, and Acronyms*).	**The passwords for RADIUS and SSH are encrypted for the entire session.**

8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components.	**Most of these requirements are procedures not directly related to Vanguard Networks Routers operation. No automatic first time passwords are provided. Currently users must have already been authenticated before being allowed to menus that allows the changing\resetting of passwords. We do not currently perform another verification before allowing a password change\reset. Vanguard Networks are currently working to fully comply with other specific password requirements (minimum length and content, not allowing previous entries. limiting access attempts etc). SSH does comply with the timeout requirements.**
Requirement 9: Restrict physical access to cardholder data.	
All requirements in section 9 relate to physical access security.	**These requirements are not directly related to Vanguard Networks Routers operation.**
Requirement 10: Track and monitor all access to network resources and cardholder data.	
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	**Individual user accounts can be set up within the router configuration.**
10.2 Implement automated audit trails for all system components to reconstruct the following events: All individual accesses to cardholder data. All actions taken by any individual with root or administrative privileges. Access to all audit trails. Invalid logical access attempts. Use of identification and authentication mechanisms. Use of identification and authentication mechanisms. Initialization of the audit logs. Creation and deletion of system-level objects	**Vanguard networks Routers currently supports RADIUS logging which addresses many of these requirements. Syslog and the refinement of audit trails of configuration changes and logins is currently in development.**
10.3 Record at least the following audit trail entries for all system components for each event: Type of event, date and time, success or failure indication, origination of event and identity or name of affected data, system component, or resource.	**The alarm logs in Vanguard Networks routers log events which include date\time, node name, event description and menu path(for configuration changes). Currently the username is not logged with each event.**
10.4 Synchronize all critical system clocks and times.	**Vanguard Networks routers support SNTP which can synchronize all connected routers with one clock\time source.**
10.5 Secure audit trails so they cannot be altered	**Permission control of viewing alarm\traffic logs are set up in the username configuration so only authorized users can view. Currently the Alarm log and Syslog is not normally transmitted securely. SYSLOG SSL/TLS with certificates is being developed. Vanguard Networks services can assist in assuring that the data is transmitted only over secure links.**

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).	**Vanguard Networks routers have the ability to view the logs locally at any given time. Procedures outside the operation of the router must also be implemented.**
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	**Syslogg is currently in development, procedures outside the operation of the router must also be implemented.**
Requirement 11: Regularly test security systems and processes.	
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use	**Vanguard Networks do not have wireless devices.**
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).	**Although Vanguard Networks is ISO9000 certified, procedures and routine vulnerability testing must be implemented to be fully compliant.**
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include network-layer and application-layer penetration tests.	**Although Vanguard Networks is ISO9000 certified, procedures and routine vulnerability testing must be implemented to be fully compliant.**
11.4 Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	**This functionality is external to the router, although Vanguard Networks routers support traffic logging and IPFLOW which are necessary to correlate intrusions.**
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly.	**This requirement is not directly related to Vanguard Networks routers operation.**
Requirement 12: Maintain a policy that addresses information security for employees and contractors.	
The requirements in section 12 mostly relate to administrative policy making. Automatic disconnect of sessions for remote access technologies after a specific period of inactivity is required.	**Vanguard Networks implementation of SSH incorporates an inactivity timer.**
Requirement A.1: Shared hosting providers must protect the cardholder data environment	
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data. Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.t.	**Most of these requirements are procedures not directly related to Vanguard Networks routers operation. Logs are unique with node name, domain name and IP address.**