

Why can't I use an inexpensive firewall purchased from a "big box" store or off the Internet to secure the data at my site? This question is one asked by many small business owners. And the Payment Card Industry – Data Security Standards (PCI-DSS) definitively answers it. It's crucial that, as a business owner, you are aware of how PCI-DSS and the use of the right firewall can impact your business.

First, let's define what a firewall is. Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and un-trusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.. Firewalls permits or restricts traffic based on a prescribed set of rules, known as policies.

There are 2 basic categories of firewalls:

- ☛ Consumer-grade firewalls that are inexpensive and can be purchased from a "big box" store or off the Internet that provide a base level of protection but do not thoroughly secure your environment and do not allow you to meet the PCI-DSS requirement #1.
- ☛ Commercial-grade firewalls that are more expensive but provide advanced security capabilities required per the PCI-DSS and require significantly more processing power and memory.

Having a consumer-grade firewall on the network is certainly better than having nothing at all. However, many small businesses have installed these systems in the mistaken belief that their networks are now immune from attacks by hackers and malicious code (malware), which could lead to the theft of credit card data. A commercial-grade firewall is one of the most important layers of protection to keep your consumer credit card data secure.

Some of the advanced security requirements that are not available in consumer-grade firewalls include:

- ☛ Intrusion Prevention— your network security must include an intrusion prevention system (IPS), along with the ability to perform regular updates to its IPS signatures (i.e., software that can detect a specific threat or group of threats). These features are, without argument, the most important ones needed to meet PCI-DSS compliance using firewalls. And, along with IPS, your business firewall should include gateway anti-virus and web access control technologies. Respectively, these services protect against viruses coming from the web and allow you to control who inside your business gets web access and to what sites. These services simply aren't available on consumer-grade firewalls.
- ☛ Filtering — to more securely protect your network, a full-featured, or commercial-grade, firewall employs built-in technology to filter incoming data traffic in search of exploits. An exploit is malware created by hackers with the specific intent to steal information or to take control of network resources (i.e., computers, data storage, etc.) without your knowing it. Intrusion prevention systems (IPS) rely on this filtering capability to identify and block malicious activity. A consumer-grade firewall just doesn't have the resources to provide this feature.
- ☛ Network Segmentation — finally, the network on which you transmit credit card data must implement access controls, and these controls must be regularly monitored and maintained. Furthermore, a commercial-grade firewall allows you to segregate your networks, allowing your credit card information to be securely transmitted on one network, while at the same time, enabling a second network (for example, to run your internal mail, applications, web access, etc.) on the same firewall. This feature significantly reduces the amount of testing and validation required to meet PCI DSS requirements and saves you the expense of purchasing a secondary firewall and DSL connection.

PCI-DSS provides very specific requirements related to the implementation of firewalls. For businesses that allow their customers to purchase products or services using credit or debit cards, compliance is not optional. A commercial-grade firewall is a must to secure your network and to meet the requirements of PCI-DSS.

	PCI Requirements	Comments	WatchGuard XTM	Consumer Firewall
1.x	Firewall must control access to and from PCI environment	WatchGuard provides full access controls that allow you to configure access to and from the payment card environment. Consumer firewalls do not provide these full access controls.	✓	✗
1.3	Implement stateful-packet inspection (SPI)	WatchGuard uses SPI to keep track of the state of network connections travelling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected. WatchGuard also uses tools that allow servers behind the firewall to remain anonymous. Consumer firewalls generally use network address translation (NAT), which provides no packet inspection.	✓	✗
4.1	Use strong cryptography and security protocols to safeguard cardholder data transmission	WatchGuard supports IPS and SSL-VPN security protocols to help protect cardholder data during transmissions. Most consumer firewalls do not provide these security protocols.	✓	?
5.x	Use and regularly update anti-virus software	WatchGuard provides a gateway anti-virus that allows the firewall to check files for viruses. This does not preclude the need for antivirus to be implemented on your BOH server. The firewall also provides regular updates to the anti-virus software. Most consumer firewalls do not provide AV services	✓	?
8.3	Implement 2-factor authentication for remote access	WatchGuard can be configured to interface to most popular two-factor authentication systems that have to be implemented with remote access applications. Consumer firewalls generally do not have the capability to work with two-factor remote access applications.	✓	✗
10.x	Track and monitor access to network resources	WatchGuard comes with a full-featured, secure logging and reporting capability that allows you to track and monitor activity in your payment card environment. File logging capabilities are not available on most consumer devices.	✓	✗
11.x	Use network intrusion prevention system (IPS)	WatchGuard includes advanced and up-to-date IPS capabilities and signatures that identify malicious activity, log information about the activity, attempt to block/stop the activity, and report the activity. Many consumer firewalls promote having an IPS, but with limited capability and no, or infrequent, updates.	✓	✗