Firewalls.com
Get Secure. Stay Secure.™

Architect Solutions

PCI DSS Compliance

PCI Compliance got your head spinning? We've got you covered.

At a Glance

- Certified network engineers ensure you find the most effective firewall appliance to fit your needs
- Configuration service ensures that every aspect of security and compliance are taken into account
- Virtual Private Network allows your organization to transmit payment card data between POS terminal and home office database
- Keep firmware current with frequent updates
- Network monitoring reports provide you with easy-to-understand visualized data to ensure access to cardholder data stays restricted

What's In It For Me?

PCI DSS Compliance can be a confusing process. Luckily, knowing how to configure and maintain a firewall appliance is half the battle. And Firewalls.com knows firewalls. We can help you purchase, configure, and deploy a secure network security infrastructure so that your business can turn your focus from handling payments to collecting them.

The Story

Running a cash-only business in 2017 can evoke the ire of disappointed customers with their credit cards in hand. If you're lagging a bit behind when it comes to payment card compliances, stop worrying! Firewalls.com can make your business PCI DSS compliant in a snap. After all, half of the compliance battle is just having a cyber security infrastructure in place.

If you're confused by the vague and verbose world of PCI standards, give our certified sales team a call. We deal with these security standards on a regular basis. We've perfected this process down to a science. Firewalls.com will walk you through the **12 Steps of PCI DSS** and ensure that your brand has everything you need to keep your revenue flowing securely, easily, and affordably.

12 Steps to PCI DSS

1. Install and maintain a firewall configuration to protect cardholder data -- ***We can do this in our sleep!***

2. Do not use vendor-supplies defaults for system passwords & other security parameters -- ***Duh.***

3. Protect stored cardholder data -- ***That's what we're here for.***

4. Encrypt transmission of cardholder data across open, public networks -- ***Virtual private networks? No problem.***

5. Use and regularly update anti-virus software or programs -- ***You do this anyway, right?***

6. Develop and maintain secure systems and applications -- ***Next-gen firewalls got you covered!***

7. Restrict access to cardholder data by business need-to-know -- ***Segmenting users into User Groups? That's light work.***

8. Assign a unique ID to each person with computer access -- ***Restricting access to User IPs is a breeze.***

9. Restrict physical access to cardholder data -- ***Sorry, this one's up to you..***

10. Track & monitor all access to network resources and cardholder data -- ***WatchGuard Dimension? Sophos Central? SonicWall Analyzer? Got it.***

11. Regularly test security systems and processes -- ***Not rocket science.***

12. Maintain a policy that addresses information security for all personnel -- ***Check our Blog for tips on creating a culture of cyber security.***

Contact Us Today
to Keep Your
Profits Flowing!

866.403.5305

sales@firewalls.com

Firewalls.com