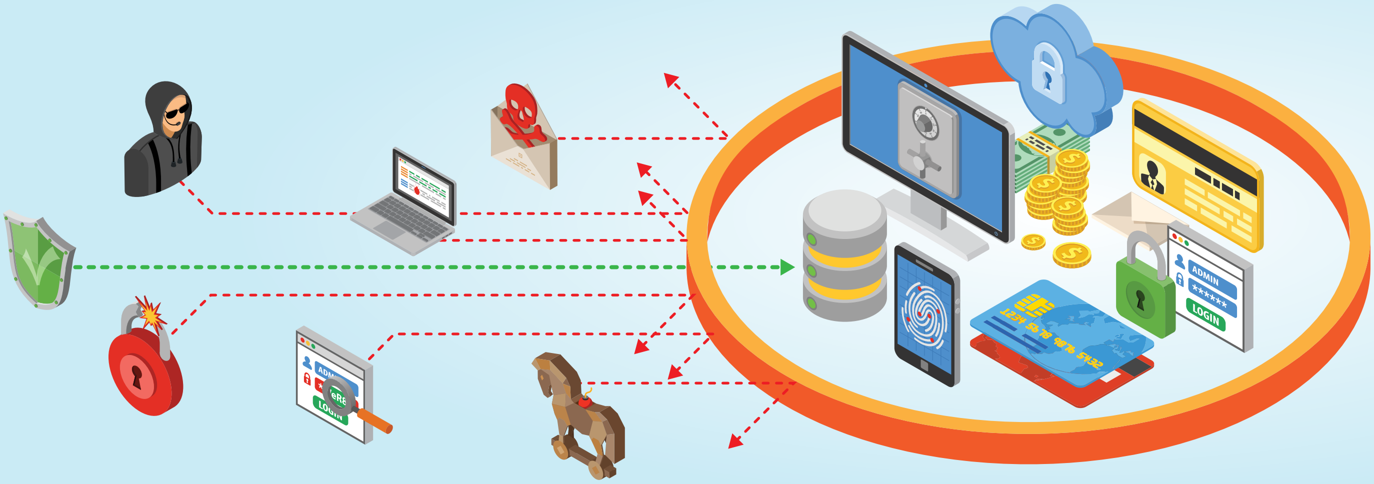
PCI Firewall Basics

PCI Security Standards Council®



A firewall is equipment or software that sits between your payment system and the Internet. It acts as a barrier to keep traffic out of your network and systems that you don't want and didn't authorize. Firewalls are configured (in hardware, software, or both) with specific criteria to block or prevent unauthorized access to a network. Firewalls are often included in the router "box" provided by your Internet provider.

Firewall rules can seem complex, but configuring them properly is vital to security. If you do not understand how to properly configure your firewall, it is wise to seek help from a network professional.

HERE IS THE MINIMUM SUGGESTED CONFIGURATION FOR A FIREWALL:

Change the original password provided by the vendor (the "default password") to a strong password

Restrict both inbound and outbound traffic to your payment systems to only what is necessary

allow ⚠ any

Avoid the use of "Any" in firewall allow rules

STOP

"Deny all" traffic that you don't specifically authorize

Permit only "established" connections into your network (for example, via stateful packet inspection or dynamic packet filtering)

Turn on intrusion detection and intrusion blocking, if available

Turn on notifications

Turn on Network Address Translation (NAT) to hide your internal addresses from the Internet

Check for and install firewall updates (or patches) to address new vulnerabilities, as soon as the patch is available

www.pcisecuritystandards.org/merchants/

© 2018 PCI Security Standards Council LLC.