

How to Meet PCI DSS Requirements with WatchGuard® XTM

This document is a brief summary of the white paper *Meeting PCI DSS Merchant Requirements with WatchGuard® XTM*, available at no charge on the WatchGuard web site at www.watchguard.com/infocenter/whitepapers.asp.

Introduction

Companies accepting credit or debit cards in exchange for goods or services must already be compliant with the PCI DSS requirements, and as of June 30, 2008 all web-facing applications must also be protected by a web application firewall. This document contains a high-level overview of the PCI DSS requirements affected by a firewall or unified threat management (UTM) deployment, focusing on how WatchGuard® XTM appliances help to meet the standard.

No firewall product is going to be “certified PCI DSS compliant.” This is just a myth. Any network firewall, and by extension a unified threat management appliance that combines a network firewall with other features (such as anti-virus and intrusion prevention services), can be a part of *becoming* compliant, but it’s only going to cover a certain portion of the requirements.

Requirements

Note: PCI DSS Requirement sections 3, 7, 9 and 12 do not affect a network firewall deployment and are not included.

1. Install and maintain a firewall configuration to protect cardholder data

Essential to meeting the first requirement and central to protecting a PCI DSS environment is the use of a zoned network, including a Demilitarized Zone (DMZ), with strict controls over what network traffic has access to the Trusted network zone, including wireless networks.

- XTM proxy firewall architecture, incorporating Network Address Translation, provides detailed granular control over which protocols, ports, and content are allowed through the firewall. This is achieved by blocking all traffic by default and defining a proxy policy that allows only approved traffic (i.e., specific protocols and IP addresses) to pass into the PCI DSS operating environment.
- With detailed network traffic awareness (e.g., protocol anomaly detection) and control, the XTM proxy architecture exceeds the stateful inspection portion of this requirement section. At the same time, XTM IPS and AV services can also be used to scan the allowed traffic to monitor for threats from malware or unauthorized intrusion attempts.

2. Do not use vendor-supplied defaults for system passwords & other security parameters

This requirement is intended to ensure that the system cannot be compromised by anyone who is able to identify the system components (e.g., databases, endpoints, network infrastructure) and try default passwords for the devices used.

In addition, all unnecessary and unsecure services and protocols must be disabled and non-console administrative access must be encrypted.

- Password management for XTM appliances is easily achieved via the intuitive management interface.
- The proxy architecture of the WatchGuard XTM can be used to block all traffic by default, providing access only to those specific protocols that are allowed.
- XTM’s IPS and AV services provide additional layers of security for those allowed protocols. All management communications with XTM appliances are done via a secure encryption-based protocol.

4. Encrypt transmission of cardholder data across open, public networks

Standard encryption mechanisms, such as IPSec or SSL VPN tunnels, must be used on all communications channels, including wireless communications, to protect cardholder data in transit.

- XTM appliances support both IPSec and SSL VPN secure communication.
- For Wi-Fi communications, the standard requires that the wireless operating environment be physically segregated from the wired environment and appropriately firewalled. WatchGuard XTM 2 Series models support WPA2 and can be combined with either IPSec or SSL VPN tunnels to achieve the objectives of this requirement.

5. Use and regularly update anti-virus software or programs

This requirement states that anti-virus software must be deployed and regularly, automatically updated. While the focus is on endpoint anti-virus solutions, the layered approach of using Gateway Antivirus products also helps to meet or exceed this requirement's objectives.

- All XTM appliances provide Gateway AntiVirus support, which serves to reduce the ingress of malware into the network and includes automatic updates of the virus signature database. In addition, the XTM logs are updated whenever traffic is denied by the Gateway AntiVirus and whenever the signature sets are updated.

6. Develop and maintain secure systems and applications

To protect against current and evolving threats, there must be regular system updates and an awareness process for newly discovered security vulnerabilities. All web-facing applications must also be protected via a web application firewall by June 30, 2008.

- WatchGuard LiveSecurity® Service provides updates and enhancements for XTM products, including software patches and new software versions. In addition, the WatchGuard LiveSecurity Service Rapid Response Team, a dedicated group of network security experts, monitors the Internet to identify emerging threats, delivering alerts that concisely describe what can be done to address each new menace.
- In combination with a web application firewall, XTM devices provide an additional layer of protection. The HTTP proxy is a high-performance content filter that examines web traffic to identify suspicious content, which can be a virus, spyware, or other type of intrusion. It can also protect your web server from attacks from the external network.

8. Assign a unique ID to each person with computer access

Each user accessing cardholder data in the PCI DSS environment must be uniquely identifiable and this requirement addresses the ways by which this is attained, including the transmission and storage of password information.

- XTM appliances support user authentication via Active Directory and two-factor authentication, including RADIUS, SecurID, and individual VPN certificates. All management communications with XTM appliances are done via a secure encryption-based protocol, with password information stored in an encrypted format.

10. Track and monitor all access to network resources and cardholder data

The basic objective here is to ensure that all access to stored cardholder data is logged and that network component configuration changes are also logged. All log data must be stored and periodically monitored to identify any potential or actual security breach. In the case of a compromise, this data is essential for tracing the cause and identifying the network vulnerability so that it may be remedied.

Practical network monitoring for all but the smallest organization is best done using something like a Security Information Management (SIM) solution that continually analyzes log data from network components and then uses data correlation techniques to attempt to identify and alert the system administrator of any security breaches.

- Audit trails can be secured by either configuring the XTM to send log data to a SIM via SNMP, or by using XTM logs in their raw form. If XTM logs are used, then the Log server must be on a secure machine (interaction with the XTM is secure).
- For tracking identity and logging access, it is best to use an Active Directory-type solution. All XTM appliances support authentication via Active Directory. All XTM appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated.

11. Regularly test security systems and processes

Included in this requirement is the need to use an Intrusion Prevention Service in the network. In addition to the intrusion prevention capabilities of their proxy architecture, XTM appliances have a fully integrated Intrusion Prevention Service (IPS) security subscription that is a powerful complement to its built-in intrusion prevention defenses.

For more information on WatchGuard network security solutions, visit us at www.watchguard.com, or call us at 1.800.734.9905 (U.S. and Canada) or +1.206.613.0895 (International).

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis. ©2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and LiveSecurity are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66527_072210