

# How NETGEAR® ProSecure™ UTM Helps Small Businesses Meet PCI Requirements

## Introduction

The Payment Card Industry Data Security Standard (PCI DSS) was developed in 2004 by the PCI Security Standards Council to ensure that companies entrusted with credit card data adopt consistent security measures to protect cardholder information when it is processed, stored, and transmitted. Known simply as "PCI", the purpose of the standard was to protect consumers through the prevention of credit card fraud, data theft, and other security threats.

Compliance with PCI DSS is a business essential for any merchant or service provider that transmits, stores, or processes cardholder data related to any of the major credit card companies – American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Covered entities that are found to be non-PCI compliant face fines of \$5,000 to \$25,000 per month. In the event a non-compliant company suffers a data breach, the fines can be as high as \$500,000.

In recent years, hackers and cyber criminals have successfully infiltrated merchants' systems, gaining access to the credit card numbers and other sensitive financial information of millions of consumers. In January 2007, computer systems of the nationwide discount retailer chain T.J. Maxx were hacked and information of at least 45.7 million credit and debit cards were stolen. The compromised data included credit card numbers, transaction information, and customer data. In January 2009, payment processing firm Heartland Payment Systems publicly disclosed that it had suffered a breach of its processing system in 2008. The scope of the damage from that breach could potentially surpass 100 million records.

## PCI Compliance Requires Robust Security Measures

Attacks from cyber criminals have become increasingly sophisticated, enabling them to easily bypass firewalls and other traditional methods of network security. As a result, defending the company's network assets against these threats now requires a multi-layered security solution. The PCI Security Standards Council has outlined the following six security categories for merchant compliance:

### 1. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

### 2. Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

### 3. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

### 4. Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

### 5. Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

### 6. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

The PCI Security Standards Council continually monitors these defenses for compliance, to ensure the highest level of safety against attack.

## Achieving and Maintaining PCI Compliance

PCI compliance is about more than just avoiding fines from the Security Standards Council. It shows consumers the company's commitment to the safety of their sensitive data. Adhering to strong security standards also helps protect the company's reputation and brand image. Suffering a database security breach can cause irreparable damage to customer trust.

With an enterprise-class 2-way firewall, industry-leading antivirus and anti-spam, and strong data encryption at the source, the NETGEAR® ProSecure™ UTM supports the following requirements for PCI compliance:

PCI DSS Requirement	Details	NETGEAR Solution
<b>Build and Maintain a Secure Network</b>		
<b>Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data</b>		
1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment	The NETGEAR ProSecure UTM features a configurable DMZ where traffic to and from the trusted network is restricted unless otherwise specified in the firewall configuration.
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	The NETGEAR ProSecure UTM contains firewall rules that restrict inbound and outbound traffic between LAN, WAN, and DMZ zones unless otherwise defined.
1.2.3	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	Connect a wireless access point into the DMZ port on the NETGEAR ProSecure UTM, effectively separating wireless traffic from the trusted network (cardholder data environment).
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	The NETGEAR ProSecure UTM features a proven firewall, VPN, IPS, and enterprise-class content security filters to prevent unauthorized access to system components inside the company network.
1.3.1	Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	The NETGEAR ProSecure UTM features a configurable DMZ where traffic to and from the trusted network is restricted unless otherwise specified in the firewall configuration.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	The NETGEAR ProSecure UTM can be configured to only allow inbound Internet traffic within the DMZ.
1.3.3	Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	The NETGEAR ProSecure UTM contains firewall rules that restrict inbound and outbound traffic between the LAN (cardholder data environment) and WAN (Internet) zones.
1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ.	The NETGEAR ProSecure UTM does not allow internal addresses to be visible from the Internet.
1.3.5	Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	The NETGEAR ProSecure UTM can be configured to only allow outbound traffic from the LAN zone going to IP addresses within the DMZ.
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	The NETGEAR ProSecure UTM performs stateful packet inspection.

PCI DSS Requirement	Details	NETGEAR Solution
1.3.7	Place the database in an internal network zone, segregated from the DMZ	The NETGEAR ProSecure UTM features a configurable DMZ where traffic to and from the trusted network is restricted unless otherwise specified in the firewall configuration. The database can be placed in the LAN zone, thus segregated from the DMZ.
1.3.8	Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).	Network Address Translation (NAT) and port address translation (PAT) are standard features of the NETGEAR ProSecure UTM.
<b>Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters</b>		
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.	The NETGEAR ProSecure UTM contains a simple 10-step setup wizard where the administrator can change the default admin password before installing the UTM onto the network.
2.2.2	Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	The NETGEAR ProSecure UTM supports firewall and content filter policies that can be configured to provide detailed granular control over which protocols, ports, and content are allowed through the UTM. Additionally, patent-pending Stream Scanning technology, along with enterprise-class anti-virus, anti-spyware, and intrusion detection technologies keep your network safe from threats that take advantage of services and protocols that have been allowed by policy.
2.2.3	Configure system security parameters to prevent misuse	The NETGEAR ProSecure UTM supports firewall and content filter policies that can be configured to provide detailed granular control over which protocols, ports, and content are allowed through the UTM.
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	The NETGEAR ProSecure UTM supports encrypted HTTPS Web-based management.
<b>Protect Cardholder Data</b>		
<b>Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks</b>		
4.1	<p>Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSec) to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p>Examples of open, public networks that are in scope of the PCI DSS are:</p> <ul style="list-style-type: none"> <li>•The Internet</li> <li>•Wireless technologies</li> <li>•Global System for Mobile communications (GSM)</li> <li>•General Packet Radio Service (GPRS)</li> </ul>	The NETGEAR ProSecure UTM support both SSL and IPsec VPN connections for secure data transmission over public networks.

PCI DSS Requirement	Details	NETGEAR Solution
<b>Maintain a Vulnerability Management Program</b>		
<b>Requirement 5: Use and Regularly Update Anti-Virus Software or Programs</b>		
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	The NETGEAR ProSecure UTM features a best-of-breed anti-virus/anti-malware scan engine, which is an essential compliment to the anti-virus software installed on individual computers.
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	The NETGEAR ProSecure UTM employs a comprehensive, best-of-breed security solution, including proactive, "zero-hour" detection and patent-pending Stream Scanning technology to proactively protect business networks from over 13 million types of viruses, worms, spyware, trojans, rootkits, keyloggers, and other Internet-based threats.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	The NETGEAR ProSecure UTM signature database is automatically updated around the clock to meet the objectives of this requirement. Malware detections are logged by the UTM.
<b>Requirement 6: Develop and Maintain Secure Systems and Applications</b>		
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.	The NETGEAR ProSecure UTM automatically checks and downloads the latest firmware version to the appliance. The administrator can then install it from the Web-based management interface.
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.	NETGEAR provides comprehensive online resources for information on the latest threats and vulnerabilities, updated around the clock by NETGEAR security experts to keep you continuously informed about threats as they emerge.
6.6	<p>For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:</p> <ul style="list-style-type: none"> <li>• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes</li> <li>• Installing a web-application firewall in front of public-facing web applications</li> </ul>	The NETGEAR ProSecure UTM's IPS, Web anti-malware scanning, URL filtering capabilities can be used in conjunction with its firewall policies to protect public facing web-applications/servers.

PCI DSS Requirement	Details	NETGEAR Solution
<b>Implement Strong Access Control Measures</b>		
<b>Requirement 8: Assign a Unique ID to Each Person with Computer Access</b>		
8.2	<p>In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> <li>• Password or passphrase</li> <li>• Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)</li> </ul>	The NETGEAR ProSecure UTM supports two-factor authentication.
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.	The NETGEAR ProSecure UTM supports two-factor authentication, including WIKID, Radius, LDAP, and individual VPN certificates.
8.4	Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	All data and passwords used to communicate with NETGEAR ProSecure UTM Web-based management interface are SSL encrypted. All file systems on the UTM are encrypted.
<b>Regularly Monitor and Test Networks</b>		
<b>Requirement 10: Track and Monitor all Access to Network Resources and Cardholder Data</b>		
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.	Actions performed by users in the UTM Web-based management interface are logged by the UTM.
10.2.1	All individual user accesses to cardholder data	Actions performed by users in the UTM Web-based management interface are logged by the UTM.
10.2.2	All actions taken by any individual with root or administrative privileges	
10.2.3	Access to all audit trails	
10.2.4	Invalid logical access attempts	
10.2.5	Use of identification and authentication mechanisms	
10.2.6	Initialization of the audit logs	
10.2.7	Creation and deletion of system-level objects	

PCI DSS Requirement	Details	NETGEAR Solution
10.3	Record at least the following audit trail entries for all system components for each event:	Actions performed by users in the UTM Web-based management interface are logged by the UTM.
10.3.1	User identification	
10.3.2	Type of event	
10.3.3	Date and time	
10.3.4	Success or failure indication	
10.3.5	Origination of event	
10.3.6	Identity or name of affected data, system component, or resource	
10.4	Synchronize all critical system clocks and times.	The NETGEAR ProSecure UTM supports NTP synchronization.
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).  Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.	The NETGEAR ProSecure UTM keeps the following logs: Traffic, Malware, Spam, Content Filter, Email Filter, System, Service, IPS, Port Scan, IM, P2P, Firewall, IPsec VPN, SSL VPN
<b>Requirement 11: Regularly Test Security Systems and Processes</b>		
11.4	Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.  Keep all intrusion detection and prevention engines up-to-date.	The Netgear ProSecure UTM's network intrusion prevention and detection system utilizes a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods, preventing hackers from penetrating the network perimeter.

## Going Beyond PCI Compliance

PCI compliance is an important start to securing the company's network. However, it is important to note that in addition to being PCI compliant, there are other important aspects of the network not covered by the PCI DSS. Business-critical company information and other network assets are still at risk from hackers, malicious programs, and other Internet-based threats. Security experts receive approximately 15 million unique malware samples each year and new threat types and attack vectors are continuously emerging. To effectively combat these continuously emerging threats, IT managers must develop comprehensive security measures that include a robust firewall and a comprehensive suite of Internet security solutions.

As illustrated in the table above, the NETGEAR ProSecure UTM is a comprehensive security solution to help you achieve and maintain PCI compliance. Additionally, the ProSecure UTM provides additional security benefits to help you protect your network from an array of Internet-based threats.

---

## NETGEAR® ProSecure™ Gateway Security Appliance Solutions

*The ProSecure STM and UTM Gateway Security Appliances feature a proven firewall, SSL and IPsec VPN support, IPS, and enterprise-class content security filters to prevent unauthorized access to system components inside the company network.*

*The ProSecure STM and UTM Gateway Security Appliances feature patent pending Stream Scanning technology that is designed to scan data streams as they enter the network. With Stream Scanning technology, the NETGEAR STM and UTM are able to process large amounts of data in real-time, using a single scan to identify spam, malware, security breaches, or unnecessary applications. This ensures that users on the network receive their email and Web content clean and without delay.*

*The ProSecure STM and UTM Gateway Security Appliances offer straight forward installation and maintenance. The STM is a transparent bridge that seamlessly integrates into existing network architectures. The UTM is an all-in-one network security solution that replaces any existing firewall or router. Each solution comes equipped with all the security software needed for your business with no per user licenses required.*

NETGEAR, the NETGEAR logo, Connect with Innovation and ProSecure are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2009 NETGEAR, Inc. All rights reserved.