NETGEAR®
Connect with Innovation™

# NETGEAR UTM and VPN Firewalls Help Small/Medium Businesses Meet PCI Compliance Standards for 2009

## Introduction

Business communications have become increasingly dependent on the Internet. Online identity theft and fraud have also become more and more rampant. Unethical hackers and cyber criminals use various methods to hack and steal personal information for financial gain. Many specifically target online merchants and payment processing firms. As a result, millions of credit card numbers have gotten into the hands of hackers and cyber criminals over the past few years. In January 2007, computer systems of the nationwide discount retailer chain T.J. Maxx were hacked into and information of at least 45.7 million credit and debit cards were stolen by hackers[1]. The compromised data included credit card numbers, transaction information, and customer data. In January 2009, payment processing firm Heartland Payment Systems issued a press release indicating that a keylogger had infiltrated its processing system in 2008[2]. Heartland Payment Systems processes credit/debit card and other payment-related transactions for over 250,000 business locations nationwide with over 100 million transactions monthly. The scope of the damage is still unknown. Cases such as the ones mentioned above have caused insurmountable damage to many businesses and have put sensitive financial information of the general public at risk.

## PCI Compliance

As security threats and hackers have become more sophisticated, usernames, encrypted passwords, and the presence of firewalls are no longer sufficient to protect networks from being compromised. IT professionals and security organizations have recognized the necessity to go beyond the traditional security processes. And thus the Payment Card Industry Data Security Standard (PCI DSS) was formed. PCI DSS defines 12 baseline requirements on how credit cardholder data access is monitored, logged, controlled, and audited.

PCI DSS is a standard any SMB or enterprise that accepts, and handles credit card data must meet. Becoming "PCI compliant" is now a must or the business will face strict fines — ranging from $5000–$25000 each month they are not compliant. That is nothing compared to the financial penalties merchants will face if credit card data is lost or stolen — up to $500,000 including the risk of losing credit card processing rights.

Since its introduction, the PCI Security Standards Council has been requiring all businesses, merchants, and service providers that process or transmit payment account information to have two-factor authentication for remote access to a network by employees, administrators, and third parties. NETGEAR® has recognized and responded to this new requirement by adding a more robust authentication system known as two-factor authentication (2FA or T-FA) on its SSL and IPSec VPN firewall product line to help companies comply with the new PCI standards.

### PCI Requirement for Two-Factor Authentication

**8.3** Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSec) with individual certificates.

## Two-Factor Authentication

Two-factor authentication is a new security solution that enhances and strengthens security by implementing multiple factors to the authentication process that challenge and confirm the users' identities before they can gain access to the network. There are several factors that are used to validate the users to make sure that they are who they said they are. These factors are:

1. **Something you know** — for example, your password or your PIN or example, your password or your PIN
2. **Something you have** — for example, a token or a Java-enabled mobile phone with generated passcode that is either 6 or 8 digits in length.
3. **Who you are** — for example, username or biometrics such as fingerprints or retinal.

For the purpose of this paper, we will only focus and discuss on the first two factors — *something you know and something you have*. This new security method can be viewed as a two-tiered authentication approach because it typically relies on what you know and what you have. A common example of two-factor authentication is a bank (ATM) card that has been issued by a bank institute:

1. The PIN to access your account is *"something you know"*
2. The ATM card is *"something you have"*

A person must have both of these factors to gain access to his/her bank account. Similar to the ATM card, access to corporate networks and data can also be strengthened using a combination of factors such as a PIN and a token (hardware or software) to validate the user and reduce the incidence of online identity theft.

## The NETGEAR Two-Factor Authentication Implementation

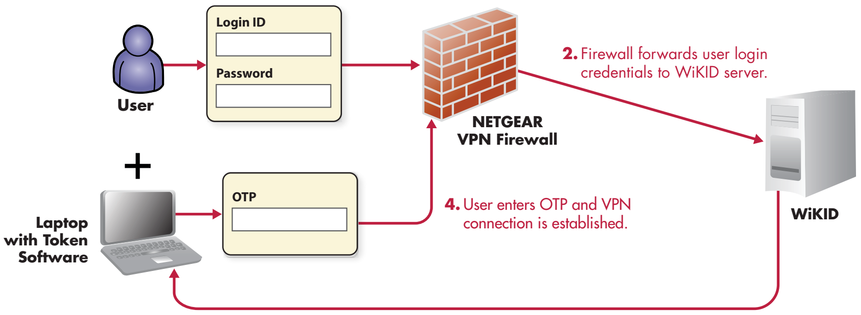
NETGEAR has implemented a two-factor authentication solution from WiKID (www.wikidsystems.com). WiKID is a software-based token solution. Instead of using Windows Active Directory or LDAP as the authentication server, administrators now have the option to use the WiKID authentication server to provide more robust authentication on NETGEAR SSL, VPN, and UTM firewall products.

The WiKID solution is based on a request-response architecture where a one-time passcode (OTP), that is time synchronized with the authentication server, is generated and sent to the user once the server has confirmed the validity of the user. The request-response architecture is capable of self-service initialization by end-users, dramatically reducing implementation and maintenance costs.

Traditionally, a user would log onto the network simply using a username and password and then would have full access to the network. With the WiKID solution, a user would launch the token software to obtain a OTP and must use this time-limited passcode along with the username to log into the network. If the users did not use the OTP in a given time, they would have to request for a new OTP again before they can log into the network.

Let's break it down to explain how this works. Every user knows their username and password (*something you know*). The username and password are stored or linked to the WiKID authentication server. As the second factor of the authentication process, the users would need to use the token software (*something you have*) to validate who they are. The token software talks to the WiKID authentication server to validate the username and password. Once the username and password have been validated, a OTP will be provided for that user. The user would then enter their username (*something they know*) and this OTP (*something they have*) to log onto the network. Combining the username, password, and the OTP from the WiKID authentication server, two-factor authentication ensures the security of the network.

**1.** User attempts to establish VPN connection with firewall.



**2.** Firewall forwards user login credentials to WiKID server.

**4.** User enters OTP and VPN connection is established.

**3.** If the login credentials are valid, the WiKID server sends a one time password (OTP) to the token software located on the user's laptop. The user must enter the OTP before it expires.

PROSAFE®

The NETGEAR two-factor authentication implementation solution has been added at no additional charge via a firmware upgrade to the following VPN firewalls:

- FVS336G
- FVS338
- FVX538
- DGFV338

PROSECURE™

The NETGEAR two-factor authentication solution comes standard on all ProSecure UTMs.

## Conclusion

NETGEAR understands the importance of being PCI compliant. While many businesses are still working to become PCI compliant, NETGEAR has already implemented the new two-factor authentication solution for all of its SSL, VPN, and UTM firewall products. Two-factor authentication is another step in enhancing networking security and at the same time meet PCI standards without having to replace the existing hardware. To obtain and try the new two-factor authentication solution on your products, visit the NETGEAR Product Support website at http://kbserver.netgear.com.

[1] http://www.msnbc.msn.com/id/17871485/
[2] http://www.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach_N.htm