

# NETGEAR<sup>®</sup> Application Note

## A brief on Two-Factor Authentication

### Summary

This document provides a technology brief on two-factor authentication and how it is used on Netgear SSL312, VPN Firewall, and other UTM products.

### Why do I need Two-Factor Authentication?

Online identity theft and fraud have become common in today's society. Unethical hackers and cyber criminals use various methods to hack and steal personal information for financial gain. Many corporations are losing millions of dollars and running the risk of revealing trade secrets and other proprietary information as the results of these cybercrime activities. Security threats and hackers have become more sophisticated. Therefore, usernames, encrypted passwords, and the presence of firewalls are no longer able to protect networks from being compromised. IT professionals and security organization such as the Payment Card Industry (PCI) Security Standards Council have recognized the necessity to go beyond the traditional authentication processes. They introduced additional guidelines that are required to ensure the security of networks. As a result, PCI 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 3<sup>rd</sup> 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.

### What is 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
- 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.

## What are the benefits of Two-Factor Authentication?

- **Industry approved PCI regulatory compliance** – Two-factor authentication has been recognized and used worldwide to satisfy the security requirements for many businesses, merchants, and service providers who do online transactions.
- **Stronger security.** Passwords alone cannot effectively protect corporate networks because attackers can easily guess simple passwords or users cannot remember complex and unique passwords. A one-time passcode (OTP) replaces the need to remember a complex password, and provides stronger security.
- **No need to replace existing hardware.** Two-factor authentication can be added to existing NETGEAR products via a firmware upgrade.
- **Quick to deploy and manage.** The WiKID solution integrates seamlessly with the NETGEAR SSL, VPN firewall and UTM products.

## NETGEAR Two-Factor Authentication Solution

NETGEAR has implemented a two-factor authentication solution from WiKID ([www.wikidsystems.com](http://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 one-time passcode (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 one-time passcode (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.

## Setting up the WiKID Authentication Server (WAS)

The instructions below provide an example of how to configure the WiKID authentication server and how to deploy the two-factor authentication on a NETGEAR product. This portion of the article assumes that users have installed the WiKID authentication server software and the server is accessible by remote users for authentication. For more information on the WiKID software and installation instruction, please visit <http://www.wikidsystems.com>.

- 1) Download and install the appropriate WiKID Server package that suites your network. You can find the different software packages from WiKID website:  
<http://www.wikidsystems.com/downloads>

- 2) Log into the WiKID server



- 3) Verify that the WiKID server recognized that you have done the following task on the "WiKID Administration Setup Page"
  - "Create an Intermediate CA"
  - "Install the Intermediate CA"
  - "Create a LocalHost Certificate"

WiKID Administration Set-up Page	
Done!	-- Create an Intermediate CA --
Done!	-- Install the Intermediate CA --
Done!	-- Create a LocalHost Certificate --
Optional:	-- Enable Protocol Modules --
Optional:	-- Set Parameters --
Optional:	-- Manage Administrators --
3.0 build 1-b1186	-- Update the WiKID Server --

- 4) Create a new domain or a device that will the WiKID server for its authentication purpose. It is here that you can define the lifetime of the OTP and the maximum number of attempts allows for bad PIN or passcode. Ideally, this domain or device should be accessible via Internet routable IP or domain name.

To create a domain, click on "Domains" tab, then click "Create a New Domain".

Home Users **Domains** Network Clients Configuration

labwikid.wtest.com

**Domain Management Page**

-- Create A New Domain --

Domain Name ▲	Device Name	Domain Identifier	Minimum PIN	Passcode Lifetime
wtest.com	wikid_test	172016000246	6	60

WIKID Systems, Inc.

**NOTE:** The “Domain Identifier” is the 12-digit code that is equivalent of a zero-padded IP address that is Internet accessible. For example, a device is an IP address of 172.16.0.246 will have a 12-digit identifier as 172016000246.

- 5) Select the “Protocol Module” that you will be using to authenticate the users. “Protocol Module” is the authentication protocol/method such as RADIUS, LDAP, or wAuth. The wAuth protocol is the native interface to the WIKID server. This protocol uses SSL and certificate authentication to allow distributed (or local) clients to communicate authentication data over an insecure network.

In our example, we will be using RADIUS protocol:

**RADIUS Configuration**

RADIUS is ENABLED [ DISABLE ]

Host Name:

IP Address:

Port:  (Default is 1812)

Multihomed?:  (Default is on)

Debug Level:  Normal  High  Debug

Use Accounting?:

Accounting Port:  (Default is 1813)

Restrict Network Clients?:

Password Encoding:  (Default is UTF8)

Secret Encoding:  (Default is UTF8)

- 6) Add the NETGEAR device (SSL312, FVX538, FVS336G, etc...) as the Network Client to allow it to validate the user authentication from the WIKID server. The Network Client acts in a proxy capacity, accepting questionable information from users and communicating with the WIKID server for validation.

**NOTE:** Since we are using RADIUS, do not forget to configure the “Shared Secret”

- 7) Now that you have created a Domain and a Network Client, you will need to setup Users so that they can connect and get validated by the WikID server. For our example, we will manually configure a user for this testing purpose. WikID server has the ability to automate the validation process between the users and the server, please contact WikID for additional information on how to setup WikID so that users can easily validate with the server.

**NOTE:** Manually validating a user requires that user first submit a registration request to WikID server using Token client software.

- 8) Install and launch the WikID Token Client software. When you run the Token Client software for the first time, it will ask you to generate a Passphrase. Users must provide this Passphrase each time to access the Token Client software to generate an OTP for the NETGEAR device.

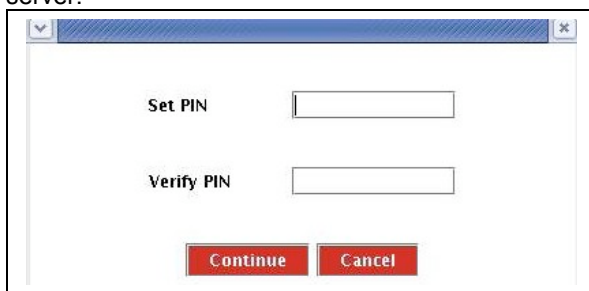
- 9) Click “Action”, then select “Create New Domain” to add the domain that you want to use to validate your login.



- 10) Enter the 12-digit Server Code for the Domain. This is the zero-padded "Domain Identifier" or IP address that you have entered when you created the domain on the WiKID server (step #4).



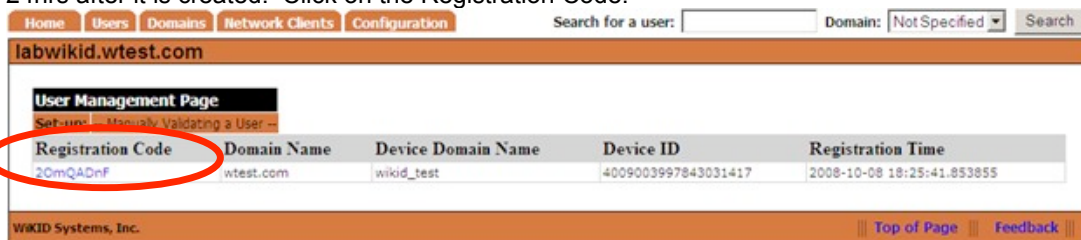
- 11) You will be asked to set a PIN that this Token Client will use to authenticate with the WiKID server.



- 12) Once the Token Client software communicated with the WiKID server, the server will return the initial validation "Registration Code". The users must have their Token Client validated before they can generate a one-time passcode.



- 13) On the WiKID User Management screen, click on Manually Validate a User and you will see the registration code listed. By default a registration code can be validated anytime within 24hrs after it is created. Click on the Registration Code.



- 14) Once you have selected the Registration Code, enter the appropriate user name then click "Register" to validate and allow this user to make request with the chosen Domain.



- 15) Return to the main User Management screen, you will see the validated user listed.



- 16) After a user has been validated by the WiKID server, the user can use the Token Client software to request and generate a one-time passcode (OTP) to log into the network/domain that they have access to.

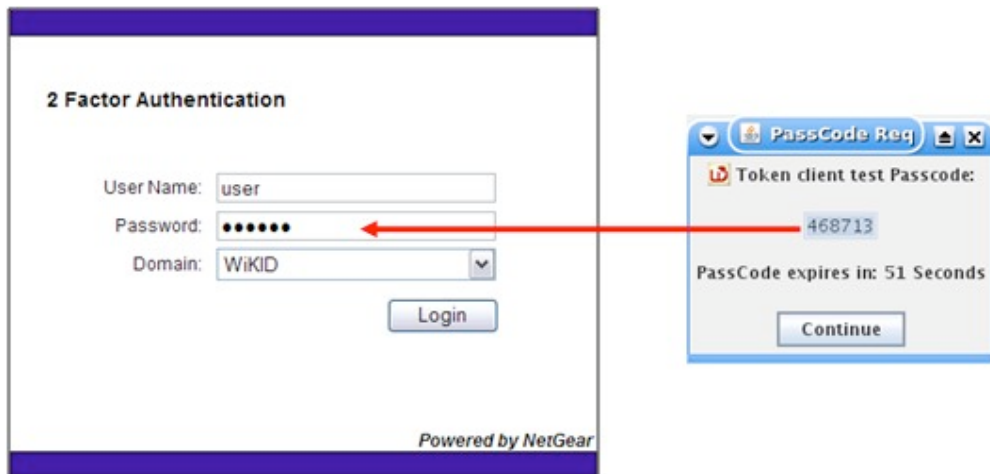
- 17) In the example below, we are showing a user using a WiKID Token Client to gain access to the SSL312 network. The user launches the WiKID token software, enter the PIN that has been given to them (*something they know*) and then press "continue" to receive the one-time passcode (OTP) from the WiKID authentication server:



- 18) A one-time passcode (*something they have*) is generated for this user:  
**NOTE:** The one-time passcode is time synchronized to the authentication server so that the OTP can only be used once and must be used before the expiration time. If a user does not use this passcode before it is expired, the user will need to go through the request process again to generate a new OTP.



- 19) The user then goes to the SSL312 login page and enters the generated one-time passcode as the login password on the SSL312.



- 20) Once the username and the OTP have been entered within the time limit, the user will have access to the network; otherwise the user would have to go through the process to obtain a new OTP to log into the network.

## Conclusion

While many IT professionals are still looking for new ways to protect their networks, NETGEAR has already implemented the new two-factor authentication solution for all of its SSL, VPN, and UTM firewall products. Two-factor authentication is a new and easy way to enhance networking security products without having to replace the existing hardware. To obtain and try the new two-factor authentication solution on your products, visit NETGEAR Support website at <http://kbserver.netgear.com>.

**November 25, 2008**

**Copyright © 2008 NETGEAR®**