



Digi Wi-Point 3G Application Guide

How to Create a VPN between Wi-Point 3G and WatchGuard

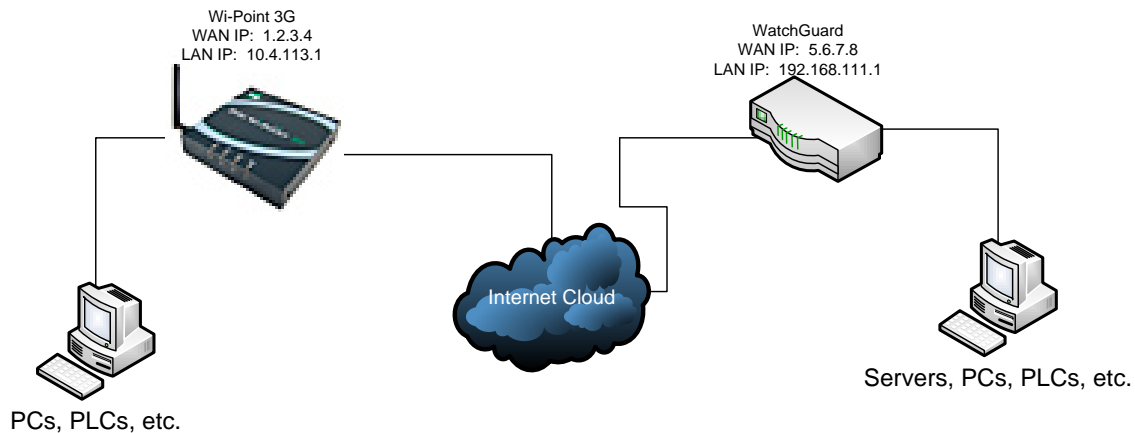
Scenario

Digi Wi-Point 3G is used for remote site connectivity. The primary site is using a WatchGuard VPN appliance. The two networks need to be connected, and the data needs to be encrypted between them.

Theory of Operation

A remote location needs to be able to build a secure tunnel between the main site and a remote branch. One location is using a Digi Wi-Point 3G gateway to provide primary internet connectivity. The other location is using a WatchGuard VPN appliance for primary site connectivity. A VPN tunnel will be created to the Digi Wi-Point 3G gateway, creating a secure connection for data to pass through.

Sample Diagram



Carrier Plan and PC / VPN Appliance Requirements

Digi Wi-Point 3G Requirements: Firmware version must be 1.1.34-8 or later. To download the latest firmware, go to <http://www.digi.com/support>.

GSM GPRS/EDGE APN Type needed: VPN and GRE end-points usually require static (persistent) IP addresses and must support mobile terminated data connections. If mobile termination is not an option with your current APN, you will need to acquire a new one that does support mobile termination.

CDMA networks may also require special plans to provide static IP addresses and support mobile terminated data connections.

Check with your wireless provider on the available plan types.

Digi Wi-Point 3G Configuration

1. Read and follow the quick-start guide for the Digi Wi-Point 3G.
2. Assign a static IP address to the Ethernet port (the default address is 192.168.1.1).
3. Configure the Digi Wi-Point 3G settings
 - a. Navigate to **Configuration > Network > VPN Settings**.
 - b. Click **VPN Tunnel Settings**.
 - c. Click **Add**.
 - d. Fill in the appropriate settings below:

The screenshot shows the 'VPN - Tunnel #1 - Configuration' page in the Digi Wi-Point 3G management interface. The page has a blue header with the Digi logo and the title 'Wi-Point 3G Configuration and Management'. Below the header is the 'DIGI WI-POINT 3G' logo. On the left is a navigation menu with categories: Home, Wizard, Configuration (Network, Mobile, Serial Ports, System, Remote Management, Security, GPS, Time), Management (Connections, Event Logging), Administration (Backup/Restore, Update Firmware, Factory Default Settings, System Information, AT Command, PIN Utility, Reboot), and Logout. The main content area is titled 'VPN - Tunnel #1 - Configuration' and contains the following settings:

- Description: To WatchGuard
- Automatically establish this tunnel
- Local VPN Endpoint: Wireless WAN
- Remote VPN Endpoint: 5.6.7.8
- VPN Tunnel: ISAKMP
- Tunnel Network Traffic from the following Local Network:
 - IP Address: 10.4.0.0
 - Subnet Mask: 255.255.0.0
- Tunnel Network Traffic to the following Remote Network:
 - IP Address: 192.168.111.0
 - Subnet Mask: 255.255.255.0
- Following Policy apply to the Tunnel Network Traffic:
 - Enable IP Encapsulating Security Payload (ESP)
 - Enable IP Authentication Header (AH)
- Use the following IPSEC security settings:

Encryption	Authentication	SA Lifetime
3-DES	MD5	28800 secs (1200-28800)

The 'Identity' section is partially visible at the bottom of the page.

Digi Connect Family Application Guide – Wi-Point 3G to WatchGuard

PIN Utility
Reboot
Logout

Following Policy apply to the Tunnel Network Traffic:

- Enable IP Encapsulating Security Payload (ESP)
- Enable IP Authentication Header (AH)

Use the following IPSEC security settings:

Encryption	Authentication	SA Lifetime
3-DES	MD5	28800 secs (1200-28800)

Identity

Use the following as the identity:
Identity string:

Use the Mobile IP address as the identity

Security Settings

Connection Mode:

Diffie-Hellman:

Enable Perfect Forward Secrecy (PFS)

Use the following pre-shared key to negotiate IKE security settings:

Use the following policy to negotiate IKE security settings:

Authentication	Encryption	Integrity	SA Lifetime
Pre-Shared Key	3-DES (192-bit)	MD5	86400 secs (1200-86400)

Copyright © 1996-2008 Digi International Inc. All rights reserved.
<http://www.digi.com/>

- e. Click **Apply** to save the changes.
- f. A reboot is required for the settings to take effect. **Reboot** the unit.

WatchGuard VPN Configuration

1. Configure the WatchGuard VPN device
 - a. Log into the Web Interface of the WatchGuard device.
 - b. Navigate to **VPN** in the left hand panel.
 - c. Under the section titled 'Manual VPN Gateways', click **Configure**.
 - d. Click **Add** to add a new VPN policy.
 - e. Fill in the appropriate information shown in the screenshots below

The screenshots show the WatchGuard Firebox X Edge VPN configuration interface. The top screenshot displays the 'Phase 1 Settings' section, and the bottom screenshot displays the 'Phase 2 Settings' section.

Phase 1 Settings

- Name: To_WiPoint
- Shared Key: 123456
- Mode: Main Mode
- Remote IP Address: Local ID 5.6.7.8, Remote ID 1.2.3.4 (both Type IP Address)
- Authentication Algorithm: MD5-HMAC
- Encryption Algorithm: 3DES-CBC
- Negotiation expires in: 0 kilobytes
- Negotiation expires in: 24 hours
- Diffie-Helman Group: 2
- Send IKE Keep Alive Messages

Phase 2 Settings

- Authentication Algorithm: MD5-HMAC
- Encryption Algorithm: 3DES-CBC
- Enable Perfect Forward Security
- Key expires in: 8192 kilobytes
- Key expires in: 24 hours

The Firebox X Edge creates a tunnel for each remote network you define. To operate correctly, you must configure the remote peer the same way.

Local Network	Remote Network
192.168.111.0/24	10.4.0.0/16

Local Network: 0.0.0.0/0
Remote Network: 0.0.0.0/0

Buttons: Submit, Reset, Remove, Add

- f. Click **Submit** to save the changes.

ADDITIONAL NOTES

1. This configuration will work with Dynamic IP addresses, using hostnames established with DynDNS.org. When using a Dynamic IP address, you will need to set the VPN tunnel to use **Aggressive Mode** to make the connection work.
2. This configuration will work with other VPN parameters than what is listed in the screenshots. i.e. – DES, 3DES, AES 192-bit, AES 256-bit, etc.

Where to Get More Information

Refer to the Digi Wi-Point 3G user documentation and Digi technical support website at www.digi.com/support for more information. Technical assistance is available at <http://www.digi.com/support/eservice/eservicelogin.jsp>.

For sales and product information, please contact Digi International at 952-912-3444 or refer to the Digi Cellular pages at www.digi.com.