



Digi Connect® Family Application Guide

How to Create a VPN between a Connect Gateway and WatchGuard

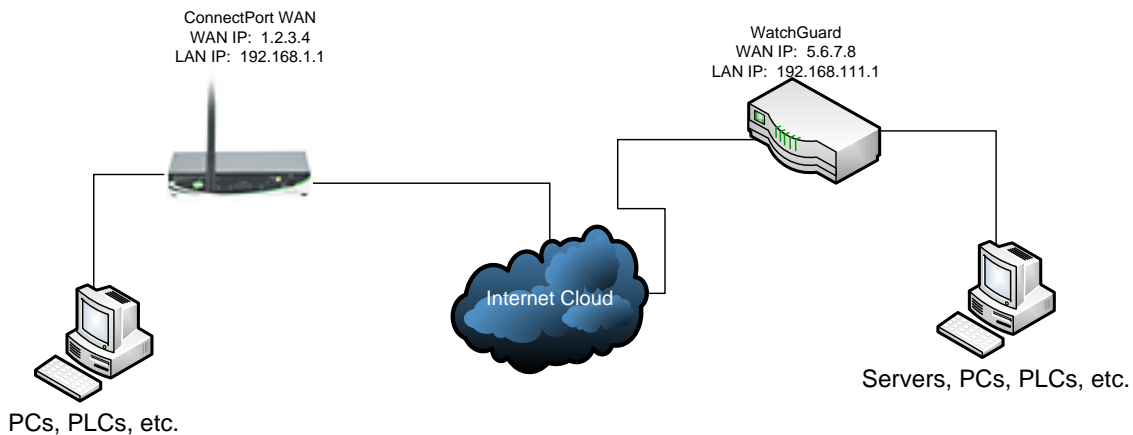
Scenario

Digi Connect WAN 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 Connect 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 Connect gateway, creating a secure connection for data to pass through.

Sample Diagram



Carrier Plan and PC / VPN Appliance Requirements

Digi Connect Requirements: Firmware version must be 2.8 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 Connect Gateway Configuration

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

The screenshot displays the 'VPN - Tunnel #1 - Configuration' page. On the left is a navigation menu with categories: Home, Configuration (Network, Mobile, Serial Ports, Camera, Alarms, System, Remote Management, Security, Position), Applications (Python, RealPort), Management (Serial Ports, Connections, Event Logging, Network Services), and Administration (File Management, X.509 Certificate/Key Management, Backup/Restore, Update Firmware, Factory Default Settings, System Information, Reboot), and Logout.

The main configuration area includes the following sections:

- VPN - Tunnel #1 - Configuration**
 - Description: To WatchGuard
 - Remote VPN Address: 5.6.7.8
 - VPN Tunnel: ISAKMP
 - Local Endpoint Type: Local endpoint is a subnet
- Identity**
 - Network Interface: mobile0
 - Negotiate tunnel as soon as interface comes up
 - Use the following as the identity: 00:40:9D:33:87:73@digi.com
 - Use the interface IP address
 - Use the identity certificate X.509 distinguished name (DN)
- Local Endpoint**
 - Tunnel Network Traffic from the following Local Network:
 - IP Address: 192.168.1.0
 - Subnet Mask: 255.255.255.0
- Remote Endpoint**
 - Tunnel Network Traffic to the following Remote Network:
 - IP Address: 192.168.111.0
 - Subnet Mask: 255.255.255.0
- Pre-Shared Key Settings**
 - Use the following IP address, FQDN, or username for the remote VPN's ID: 5.6.7.8
 - Use the following pre-shared key to negotiate IKE security settings: _____

Digi Connect Family Application Guide – Connect Gateway to WatchGuard

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

123456

ISAKMP Phase 1 Settings

General Security Settings for Phase 1

Connection Mode:

Enable Perfect Forward Secrecy (PFS)

NAT-T Settings

Enable NAT Traversal (NAT-T)

Keep Alive Interval:

ISAKMP Phase 1 Policies

Authentication	Encryption	Integrity	SA Lifetime	Diffie-Hellman	
Pre-Shared Key	3-DES (192-bit)	MD5	86400 secs	Group 2	Remove
<input type="text" value="Pre-Shared Key"/>	<input type="text" value="DES (64-bit)"/>	<input type="text" value="MD5"/>	<input type="text" value="86400"/> secs	<input type="text" value="Group 2"/>	<input type="button" value="Add"/>

ISAKMP Phase 2 Settings

General Security Settings for Phase 2

Diffie-Hellman:

ISAKMP Phase 2 Policies

Use the following policies to negotiate security settings --Highest priority listed last:

Encryption	Authentication	SA Lifetime	
3-DES	MD5	28200 secs	Remove
<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="text" value="28200"/> secs	<input type="button" value="Add"/>

Copyright © 1996-2009 Digi International Inc. All rights reserved.
www.digi.com

- e. Click **Apply** to save the changes.

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 top screenshot shows the WatchGuard Firebox X Edge configuration page for a VPN gateway. The left sidebar shows the navigation menu with 'VPN' selected. The main content area is titled 'VPN > Manual VPN Edit Gateway'. It includes fields for 'Name' (To_Digi_Connect) and 'Shared Key' (123456). Below are 'Phase 1 Settings' and 'Phase 2 Settings' sections with various dropdown menus and input fields for IP addresses, algorithms, and negotiation parameters.

The bottom screenshot shows the 'Local Network' and 'Remote Network' configuration section. It features a table with the following data:

Local Network	Remote Network
192.168.111.0/24	192.168.1.0/24

Below the table are input fields for 'Local Network' (0.0.0.0/0) and 'Remote Network' (0.0.0.0/0) with an 'Add' button. At the bottom are 'Submit' and 'Reset' buttons.

- 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.
3. This configuration will work with other Digi Cellular products, such as the Connect WAN, Connect WAN 3G, and ConnectPort WAN VPN series of products that support VPN connections.

Where to Get More Information

Refer to the Digi Connect gateway 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.