



# Digi Wi-Point 3G Application Guide

## How to Create a VPN between Wi-Point 3G and D-Link

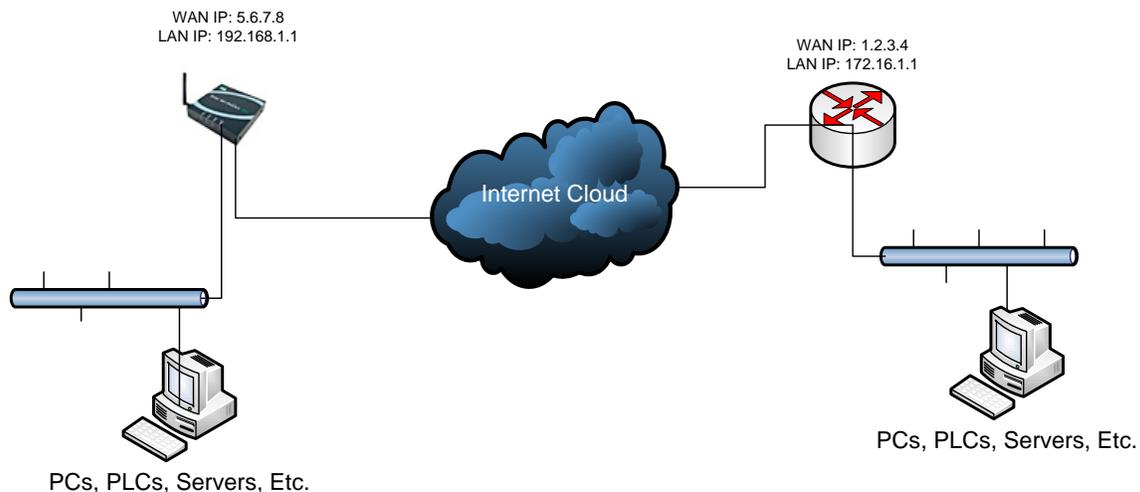
### Scenario

Digi Wi-Point 3G is used for remote site connectivity. The primary site is using a D-Link 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 D-Link router 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



### Wi-Point 3G Configuration and Management

## DIGI WI-POINT 3G

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  
Logout

### VPN - Tunnel #1 - Configuration

Description:

Automatically establish this tunnel

Local VPN Endpoint:

Remote VPN Endpoint:

VPN Tunnel:

Tunnel Network Traffic from the following Local Network:

IP Address:

Subnet Mask:

Tunnel Network Traffic to the following Remote Network:

IP Address:

Subnet Mask:

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
<input type="text" value="3-DES"/>	<input type="text" value="MD5"/>	<input type="text" value="28800"/> secs (1200-28800)

Identity

## Digi Connect Family Application Guide – Wi-Point 3G to D-Link

[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/>

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

## D-Link VPN Configuration

1. Configure the D-Link VPN device
  - a. Log into the Web Interface of the D-Link device.
  - b. Navigate to **Firewall > VPN**.
  - c. Click **Add New** under the section called **IPsec Tunnels**.
  - d. Fill in the appropriate information show in the following screenshots

The screenshot shows the 'VPN Tunnels' configuration page in the D-Link web interface. The 'Firewall' tab is selected, and the 'VPN' sub-tab is active. The form is titled 'Edit IPsec tunnel ToDigi'. The 'Name' field is set to 'ToDigi' and the 'Local Net' is '172.16.0.0/16'. Under the 'Authentication' section, the 'PSK - Pre-Shared Key' option is selected. The 'PSK' and 'Retype PSK' fields are empty. The 'Certificate-based' option is unselected. The 'Local Identity' dropdown is set to 'Admin - CN=0013469C4215'. The 'Certificates' field is empty. Below it, there is a note: 'Use ctrl/shift click to select multiple certificates. To use ID lists below, you must select a CA certificate.' The 'Identity List' dropdown is set to '[no list]'. On the left side of the interface, there is a vertical menu with buttons for 'Policy', 'Port Mapping', 'Users', 'Schedules', 'Services', 'VPN' (highlighted), 'Certificates', and 'Content Filtering'.

The screenshot shows the 'Tunnel type' section of the VPN configuration page. The 'LAN-to-LAN tunnel' option is selected. The 'Remote Net' field is '192.168.1.0/24' and the 'Remote Gateway' is '5.6.7.8'. Below these fields, there is a note: 'The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.' The 'Route' checkbox is checked with the label 'Automatically add a route for the remote network.' The 'Proxy ARP' checkbox is unchecked with the label 'Publish remote network on all interfaces via Proxy ARP.' The 'IKE XAuth client' checkbox is unchecked with the label 'Pass username and password to peer via IKE XAuth, if the remote gateway requires it.' Below this, there are 'XAuth Username' and 'XAuth Password' input fields. At the bottom, there is a checkbox for 'Delete this VPN tunnel'. At the bottom right, there are four buttons: 'Advanced' (with a purple icon), 'Apply' (with a green checkmark icon), 'Cancel' (with an orange X icon), and 'Help' (with a red plus icon).

- e. Click **Apply** to save the changes.
- f. Click **Edit** on the newly created item on the VPN page under the **IPsec Tunnels** heading.
- g. Click **Advanced** to configure additional parameters, as shown in the following screenshots:

## Digi Connect Family Application Guide – Wi-Point 3G to D-Link

The screenshot displays the 'VPN Tunnels' configuration page in the Digi Connect Family web interface. The left sidebar contains navigation buttons for Policy, Port Mapping, Users, Schedules, Services, VPN (highlighted), Certificates, and Content Filtering. The main content area is titled 'VPN Tunnels' and shows the configuration for an IPsec tunnel named 'ToDigi'. The configuration includes:

- Limit MTU: 1424
- IKE Mode:  Main mode IKE,  Aggressive mode IKE
- IKE DH Group: 2 - modp 1024-bit
- PFS:  Enable Perfect Forward Secrecy
- PFS DH Group: 2 - modp 1024-bit
- NAT Traversal:  Disabled,  On if supported and needed (NAT detected between gateways),  On if supported
- Keepalives:  No keepalives,  Automatic keepalives (works with other DFL-200/700/1100 units),  Manually configured keepalives
- Source IP: [ ]
- Destination IP: [ ]

Below the configuration are two tables:

**IKE Proposal List**

Cipher	Hash	Life KB	Life Sec
#1: AES-128 Allowed:128-256	SHA-1	0	28800
#2: AES-128 Allowed:128-256	MD5	0	28800
#3: 3DES	SHA-1	0	28800
#4: 3DES	MD5	0	28800
#5: DES	SHA-1	0	28800
#6: DES	MD5	0	28800
#7: -	MD5	0	0
#8: -	MD5	0	0

**IPsec Proposal List**

Cipher	HMAC	Life KB	Life Sec
#1: AES-128 Allowed:128-256	SHA-1	0	3600
#2: AES-128 Allowed:128-256	MD5	0	3600
#3: 3DES	SHA-1	0	3600
#4: 3DES	MD5	0	3600
#5: DES	SHA-1	0	3600
#6: DES	MD5	0	3600
#7: -	MD5	0	0
#8: -	MD5	0	0

A note at the bottom explains the 'AES-128 Allowed:128-256' cipher: "AES-128 Allowed:128-256" means that this unit will propose 128 bit encryption to the remote end when establishing an outbound tunnel, and will accept any cipher key sizes between 128 and 256 (inclusive) when receiving inbound tunnels.

At the bottom right, there are three buttons: **Apply** (with a green checkmark icon), **Cancel** (with a red X icon), and **Help** (with a red plus icon).

- h. Click **Apply** to save the changes.
- i. Click **Activate** on the left hand side to commit the changes that were done to the running configuration of the device.

### 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 Connect router user documentation and Digi technical support website at [www.digi.com/support](http://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 Connect wireless pages at [www.digi.com](http://www.digi.com).