



# Digi Connect® Family Application Guide

## How to Create a VPN between Digi and D-Link

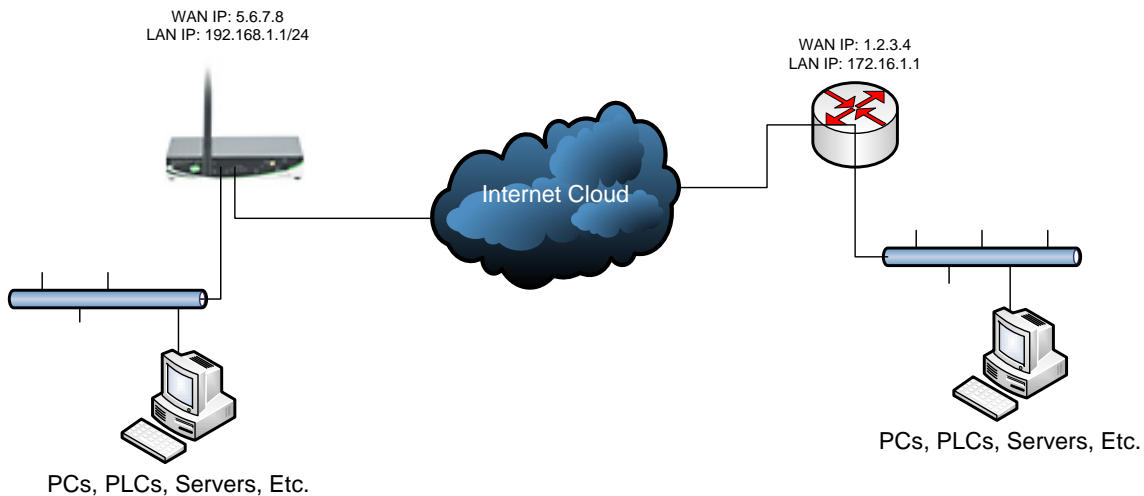
### Scenario

Digi Connect family VPN router (for example ConnectPort WAN or Digi Connect WAN IA) 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 Connect router to provide primary internet connectivity. The location is using a D-Link router for primary site connectivity. A VPN tunnel will be created to the Digi Connect router, creating a secure connection for data to pass through.

### Sample Diagram



### Carrier Plan and PC / VPN Appliance Requirements

**Digi Connect Router 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 Router Configuration

1. Read and follow the quick-start guide for the Digi Connect router and optionally for Digi Connectware® Manager if used.
2. Assign a static IP address to the Ethernet port (the default address is 192.168.1.1). Note the default gateway may show or change to an address such as 10.6.6.6. This is normal as it is the cellular provider's network default gateway.
3. Configure the Digi Connect router settings
  - a. VPN Policy Settings
    - i. Click on **VPN Policy Settings**.
    - ii. Click on the **Add** button to setup the individual tunnel.
    - iii. Fill in the appropriate information, shown in the following screenshots:

Home

Configuration

- Network
- Mobile
- Serial Ports
- Camera
- Alarms
- System
- Remote Management
- Security
- Position

Applications

- Python
- RealPort

Management

- Serial Ports
- Connections
- Event Logging
- Network Services

Administration

- File Management
- X.509 Certificate/Key Management
- Backup/Restore
- Update Firmware
- Factory Default Settings
- System Information
- Reboot

Logout

### VPN - Tunnel #1 - Configuration

Description:

Remote VPN Address:

VPN Tunnel:

Local Endpoint Type:

#### Identity

Network Interface:

Negotiate tunnel as soon as interface comes up

Use the following as the identity:

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:

Subnet Mask:

#### Remote Endpoint

Tunnel Network Traffic to the following Remote Network:

IP Address:

Subnet Mask:

#### Pre-Shared Key Settings

Use the following IP address, FQDN, or username for the remote VPN's ID:

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

Done

Internet

IC

## Digi Connect Family Application Guide – Digi to D-Link

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)	SHA1	28800 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	SHA1	3600 secs	Remove
<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="text" value="28200"/> secs	<input type="button" value="Add"/>

Copyright © 1996-2008 Digi International Inc. All rights reserved.  
[www.digi.com](http://www.digi.com)

- iv. Click **Apply** after filling in the above information to complete the tunnel setup on the Digi Connect router.

## 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

**System Firewall Servers Tools Status Help**

### VPN Tunnels

Edit IPsec tunnel **ToDigi**:

Name:

Local Net:

Authentication:

**PSK - Pre-Shared Key**

PSK:

Retype PSK:

**Certificate-based**

Local Identity:

Certificates:

Use ctrl/shift click to select multiple certificates.  
To use ID lists below, you must select a CA certificate.

Identity List:

Tunnel type:

**Roaming Users** - single-host IPsec clients

IKE XAuth:  Require user authentication via IKE XAuth to open tunnel.

**LAN-to-LAN tunnel**

Remote Net:

Remote Gateway:

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Route:  Automatically add a route for the remote network.

Proxy ARP:  Publish remote network on all interfaces via Proxy ARP.

IKE XAuth client:  Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

Delete this VPN tunnel

**Advanced Apply Cancel Help**

- 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 – Digi to D-Link

**VPN Tunnels**

Edit advanced settings of IPsec tunnel **ToDigi**:

Limit MTU:

IKE Mode:  Main mode IKE  
 Aggressive mode IKE

IKE DH Group:

PFS:  Enable Perfect Forward Secrecy

PFS DH Group:

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:

**IKE Proposal List**

Cipher	Hash	Life KB	Life Sec
#1:			
#2:			
#3:			
#4:			
#5:			
#6:			
#7:			
#8:			

**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

"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.

**Apply** **Cancel** **Help**

- 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, or using the DDNS update feature of Digi Connectware® Manager. 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 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).