



Digi Connect[®] Application Guide

How to create a VPN tunnel between 2 Digi Connect devices

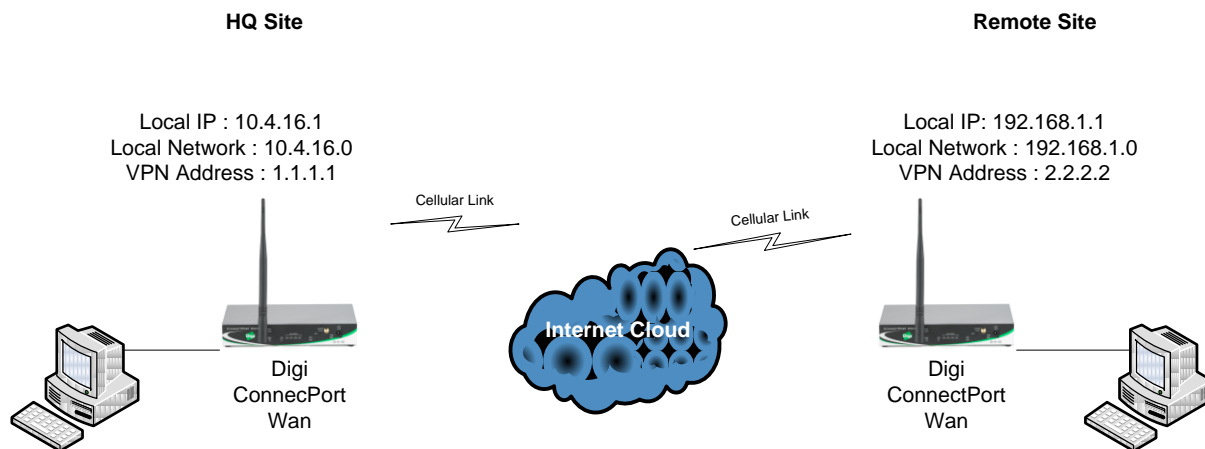
Scenario

Digi Connect family VPN router (for example Digi Connect WAN 3G) is used for primary and remote site connectivity. The data needs to be encrypted between the two devices.

Theory of Operation

A location needs to be able to build a secure tunnel between the main site and a remote branch. Both locations have Digi Connect routers to provide primary internet connectivity. The Digi Connect router will create a VPN tunnel to the opposite Digi Connect router, creating a secure connection

Sample Diagram



Carrier Plan and VPN Appliance Requirements

Digi Connect Router Requirements: This document assumes that Firmware version 2.14 or later is installed. 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. The connection must also support Mobile-to-Mobile communication, as not all APNs allow for this.

CDMA networks may also require special plans to provide static IP addresses and support mobile terminated data connections. The connection must also support Mobile-to-Mobile communication, as not all service plans allow for this.

Check with your wireless provider on the available plan types.



Digi Connect® Application Guide

How to create a VPN tunnel between 2 Digi Connect devices

Digi Connect Router Configuration

1. Read and follow the quick-start guide for the Digi Connect router and optionally visit <http://www.idigi.com> if the device is connected to the iDigi device cloud.
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 (HQ Location) settings:
 - a. Navigate to **Configuration > Network > VPN Settings** in the web interface of the unit.
 - b. Click on **VPN Policy Settings**.
 - c. Click on the **Add** button to setup the individual tunnel.
 - d. Fill in the appropriate information, shown in the following screenshots
 - e. The remote VPN device is the IP address of the mobile interface of the Digi router



Connect WAN 3G Configuration and Management

Home

Configuration

Network
Mobile
Serial Ports
Camera
Alarms
System
iDigi
Users
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

Press **Apply** for changes to take effect.

Help

VPN - Tunnel #2 - Configuration

Description:	To Remote Site
VPN Tunnel:	ISAKMP
Local Endpoint Type:	Local endpoint is a subnet

VPN Mode

Initiate client connections to and accept connections from the remote VPN device at:
2.2.2.2

Accept connections from any VPN device

Identity

Network Interface: mobile0

Negotiate tunnel as soon as interface comes up
 Keep tunnel up by periodically sending pings
Minutes Between Pings: 0

Use the following as the identity: hq@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:	10.4.16.0
Subnet Mask:	255.255.255.0



Digi Connect[®] Application Guide

How to create a VPN tunnel between 2 Digi Connect devices

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:

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	AES (256-bit)	MD5	86400 secs	Group 2	Remove
<input type="text" value="Pre-Shared Key"/>	<input type="text" value="AES (256-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	
AES (256-bit)	MD5	28200 secs	Remove
<input type="text" value="AES (256-bit)"/>	<input type="text" value="MD5"/>	<input type="text" value="28200"/> secs	<input type="button" value="Add"/>

e. Click **Apply** after filling in the above information to complete the tunnel setup on the Digi Connect router (HQ location).

4. Configure the Digi Connect router (Remote Location) settings:

- Navigate to **Configuration > Network > VPN Settings** in the web interface of the unit.
- Click on **VPN Policy Settings**.
- Click on the **Add** button to setup the individual tunnel.
- Fill in the appropriate information, shown in the following screenshots:



Digi Connect® Application Guide

How to create a VPN tunnel between 2 Digi Connect devices

Connect WAN 3G Configuration and Management

Home

Configuration

- Network
- Mobile
- Serial Ports
- Camera
- Alarms
- System
- IDigi
- Users
- 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

Press **Apply** for changes to take effect.

Help

VPN - Tunnel #2 - Configuration

Description:

VPN Tunnel:

Local Endpoint Type:

VPN Mode

Initiate client connections to and accept connections from the remote VPN device at:

Accept connections from any VPN device

Identity

Network Interface:

Negotiate tunnel as soon as interface comes up

Keep tunnel up by periodically sending pings

Minutes Between Pings:

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:

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	AES (256-bit)	MD5	86400 secs	Group 2	Remove
Pre-Shared Key	AES (256-bit)	MD5	86400 secs	Group 2	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	
AES (256-bit)	MD5	28200 secs	Remove
AES (256-bit)	MD5	28200 secs	Add

e. Click **Apply** after filling in the above information to complete the tunnel setup on the Digi Connect router (HQ location).



Digi Connect® Application Guide

How to create a VPN tunnel between 2 Digi Connect devices

ADDITIONAL NOTES

1. This configuration will work with Dynamic IP addresses or 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 128-bit, AES 192-bit, etc.
3. This configuration will work with most Digi Cellular products, such as the Connect WAN, Connect WAN VPN, and ConnectPort WAN VPN series of products that support VPN connections.
4. This configuration will also work with older versions of Digi firmware. The preceding screenshots will not match the web interface of older firmware.
5. When using two Cellular devices to create a VPN tunnel, you are creating a larger than normal amount of overhead over the cellular connection. In doing so, your data charges may be higher than normal for each device.
6. Latency will be doubled (or higher) when using two Cellular devices to create a VPN tunnel. Throughput is also reduced to the lowest common denominator – typically the upload speed.

Where to Get More Information

Refer to the Digi Connect router 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 Connect wireless pages at www.digi.com.