Digi Connect® VPN Application Guide

Configuring IPsec VPN Using Pre-Shared Key for Primary Connectivity

Scenario

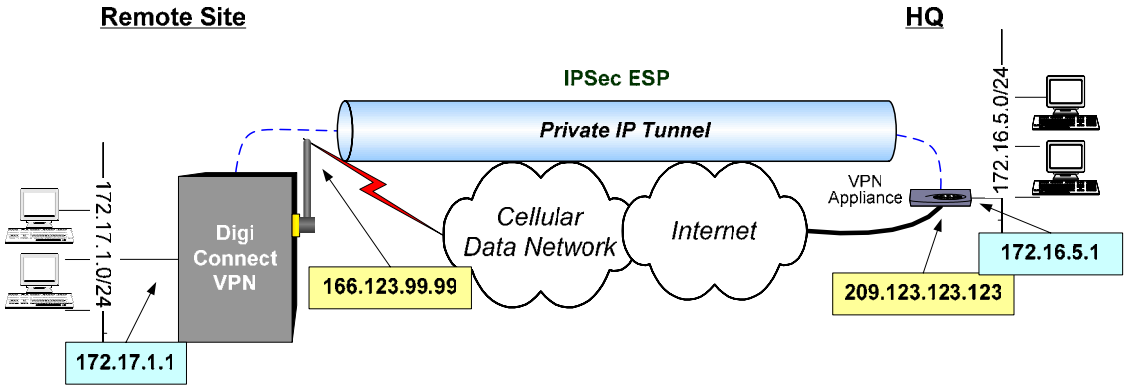
Digi Connect VPN is used for primary or backup remote site connectivity. Secured IPsec VPN traffic is typically routed from the Digi Connect VPN over the cellular IP network and is terminated by a VPN appliance at the host end.

There are several possible scenarios where the Digi Connect VPN can be used:

- As the *primary* remote site router where no other WAN router is used.
- As a *backup* router where the remote site has a primary WAN connection via DSL, Frame Relay, etc. If the primary router provides IPsec termination or origination then a Digi Connect® WAN or Digi Connect VPN can be used to pass VPN traffic through to the router. See the Digi Connect WAN application guide on using the Digi Connect WAN for Backup Connections.
- To provide secure access to remote serial and/or Ethernet *devices*.

This document will focus on using the Digi Connect VPN as a primary remote site router using IPsec ESP and IKE/ISAKMP pre-shared key VPN.

Sample Diagram:



Theory of Operation

The Digi Connect VPN's Ethernet port will typically connect to a switch or hub which then connects to other Ethernet devices.

The wireless carrier provides only one IP address to the mobile interface. The Digi Connect VPN uses Network Address Translation (NAT) where only the mobile IP address is visible to the outside. Private IP addresses are typically used on the remote site LAN connected to the Digi Connect VPN's Ethernet port. All outgoing traffic, except for tunneled VPN traffic, uses the mobile IP address of the Digi Connect VPN.

Digi Connect VPN supports the Encapsulating Security Payload (ESP) version of IPsec. AH is not supported at this time.

Typically a host or device on the remote subnet (in this case 172.17.1.0) will request information from a host on the HQ subnet (172.16.5.0). For example, a computer at 172.17.1.20 needs a file from 172.16.5.100. The Digi Connect VPN sees the request as

being on the HQ subnet and checks to see if a tunnel between the two sites exists. If not, the Digi Connect VPN will initiate a VPN tunnel request to its peer, the VPN concentrator at HQ. Various VPN policy settings are compared and if they match appropriately an IPsec tunnel is created between the Digi Connect VPN and the VPN concentrator. Traffic is encrypted as defined in the VPN policies.

Digi Connect VPN IPsec Features / Specifications:

- Max number of tunnels supported: two
- Global VPN Settings (see Digi Connect VPN help screens for details):
  - Identity**: (***Default: mac-address@digi.com*)
    - Fully Qualified Domain Name (FQDN)
    - User FQDN
    - Network Address (IPv4)
  - Connection Modes: **(***Default: Main Mode*)
    - Main Mode
    - Aggressive Mode.
  - Diffie-Hellman (DH) Groups: (*Default: Group 2 1024-bit*)
    - Group 1 (768-bit)
    - Group 2 (1024-bit)
    - Group 5 (1536-bit)
  - Perfect Forward Secrecy (PFS) (*Default: Enabled*)
  - Anti-replay (*Default: Disabled*)
- IKE/ISAKMP key exchange/authentication:
  - Pre-Shared Key (PSK) only
- IPsec Tunnel Settings:
  - ESP Only
  - Multiple proposals
  - Manual Key Optional
- Encryption:
  - DES: 64 bit; 3DES: 192bit (DES and 3DES are fixed key lengths)
  - AES 128/192/256 bit keys
  - MD5 and SH1 Hash algorithms
- Plus full Digi Connect® RG serial port functionality including RealPort® support

IP Address Requirements

GSM GPRS/EDGE APN Type needed: A *Custom APN* may be required if the VPN end-points require static (persistent) IP addresses. An *Internet APN* may work if the main site (HQ) VPN appliance can support Dynamic DNS names or if another form of authentication is used (e.g.,, FQDN). Note these APNs are based on Cingular Blue; other carrier APNs may have similar requirements.

CDMA carrier requirements are similar in that static IP addresses may be required depending on the host site concentrator VPN implementation.

In both cases, the Digi Connect VPN Mobile IP address will likely need to support mobile terminated data (i.e.,, the ability to accept incoming data connections).

HQ Router / VPN Appliance Configuration

Refer to the Digi Connect VPN IPsec specifications for supported protocols. Security policies on the HQ VPN device must match those on the Digi Connect VPN.

The HQ VPN appliance's peer address will be the Connect VPN's Mobile IP address.

Console Port: As a side benefit, the Digi Connect WAN console port can configured for "Console Management" to provide SSH or telnet access. It can be cabled to the router or VPN appliance's console port to provide true diverse out-of-band console access.

Digi Connect Typical WAN Configuration

1. Read and follow the quick-start guide for the Digi Connect WAN 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 GSM provider's network default gateway.
3. Using a Browser, Configure IPsec via **Network > VPN Settings.** Refer to the WebUI *Help* screens and the example setup below for details.
    a. **VPN Settings** defines the main IKE/ISAKMP parameters to authenticate and protect phase 1 IKE negotiations:
        i. Identity – how the Digi Connect VPN is identified its VPN peer
        ii. General Settings for Connection Mode (main or aggressive) and DH Group (1, 2, 5)
        iii. Enable/Disable PFS and Anti-replay
        iv. IKE Security Settings. Chose the appropriate settings for encryption, hash and SA life-time. Either choose the default (3-DES, SHA1, 86400 secs.) or add other entries.
    b. **VPN Tunnel Settings** define the actual tunnels that exist between two private networks. Up to two tunnels can be defined.
        i. Description: Provides entry of a more descriptive name.
        ii. Remote VPN Endpoint: The IP address (or host-name) of the remote VPN peer, typically a VPN concentrator or appliance at the host site.
        iii. VPN Tunnel: The type of policy to be used; either manual keyed IPsec (i.e., no IKE) or IKE/ISAKMP with Pre-shared Keys (PSK).
        iv. Tunnel Network Traffic *From*…: Defines the *local* subnet attached to the Digi Connect VPN Ethernet port.
        v. Tunnel Network Traffic *To*…: Defines the *remote* subnet attached host site VPN device.
            - NOTE: These two settings must complement each other. I.e., my remote subnet must match your local subnet and vice-versa.
        vi. Security Settings: Based using ISAKMP/PSK vs. Manual Key select
            1. Manual Key IPsec
                a. SPI values must be defined for incoming and outgoing traffic. My outgoing SPI must be your incoming SPI and vice-versa.

b. Optional encryption and/or authentication. The key length is based on the encryption and/or authentication hash algorithms used:

		ASCII Key Length	Hexadecimal Key Length
DES	64-bit	8	16
3-DES	192-bit	24	48
AES	128-bit	16	32
	192-bit	24	48
	256-bit	32	64
MD5	128-bit	16	32
SHA1	160-bit	20	40

Hex key values must be prefixed by "0x". For example a hex key of “1AB3” is entered as “0x10xA0xB0x3”.

2. ISAKMP Pre-shared key:
   a. Pre-shared Secret key is a fixed-length string shared by the two VPN peers. As with the manual key the value can be ASCII or hex. The key lengths may be:

Size	Key Length	
	ASCII	Hexidecimal
128-bit	16	32
192-bit	24	48
256-bit	32	64

   b. Policies (proposals): Chose the appropriate settings for encryption, hash and SA life-time.

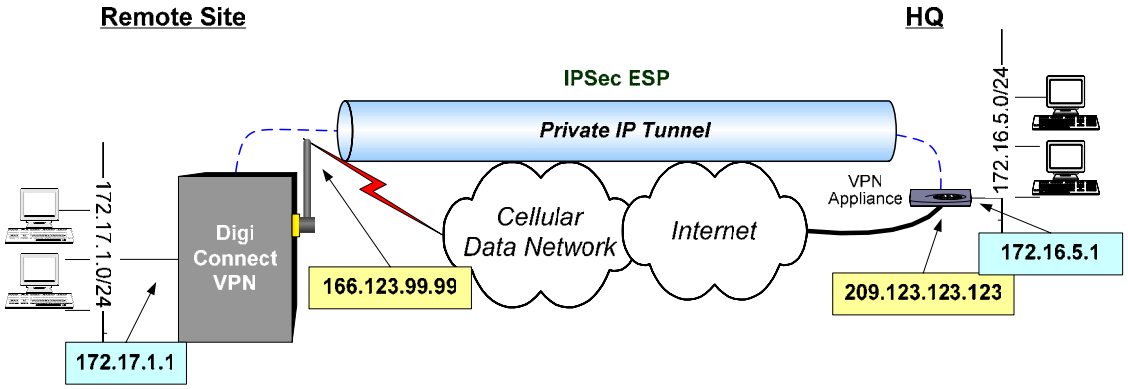
c. Be sure to always:
   i. Click ADD when necessary to add new entries
   ii. Click APPLY to save changes.

4. Bring up the VPN tunnel by generating traffic (e.g., ping) from the remote site to the host subnet.

Refer to the Digi Connect VPN’s built-in help for more details.

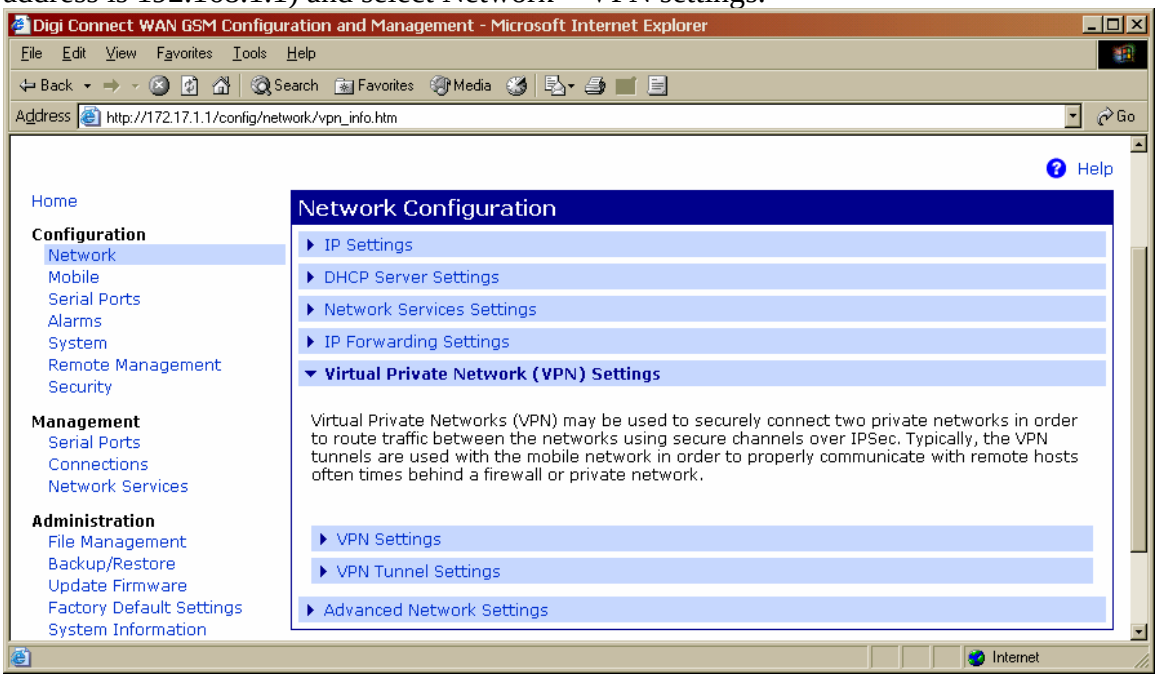
Example IPsec ESP Using IKE/ISAKMP Pre-Shared Key VPN Setup

Reviewing the example diagram:

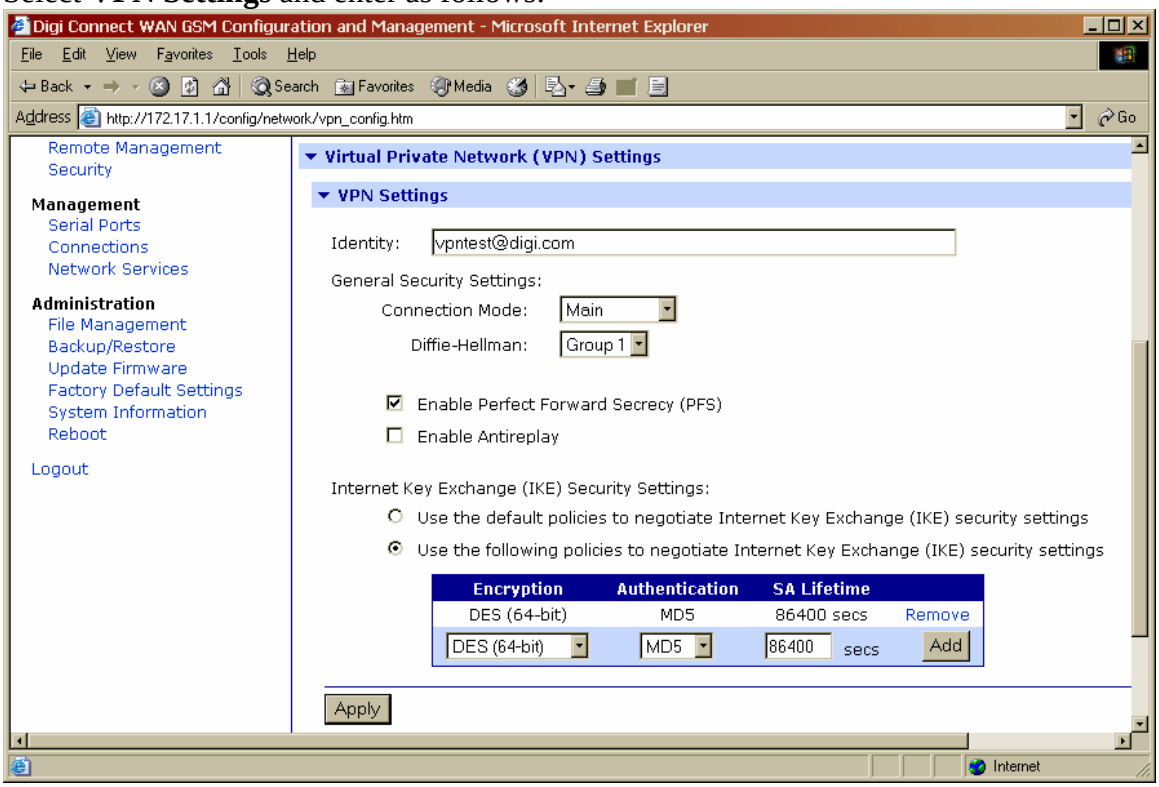


	Remote Site (Digi Connect VPN)	HQ (VPN Concentrator)
Local Interface IP Address	172.17.1.1	172.16.5.1
Local Subnet	172.17.1.0/24	172.16.5.0/24
External/Mobile IP Address	166.213.99.99	209.123.123.123
Remote Subnet	172.16.5.0/24	172.17.1.0/24
Remote VPN Endpoint	209.123.123.123	166.123.99.99
ISAKMP Shared Secret	sixteencharacter	sixteencharacter
Identity: User FQDN	vpntest@digi.com	vpntest@digi.com
IKE Parameters	DES / MD5 / 86400 sec.	DES / MD5 / 86400 sec.
IPsec Parameters	3DES / MD5 / 86400 sec.	3DES / MD5 / 86400 sec.

1. Via web browser open Digi Connect VPN using IP 172.17.1.1 (note the default address is 192.168.1.1) and select Network > VPN settings:

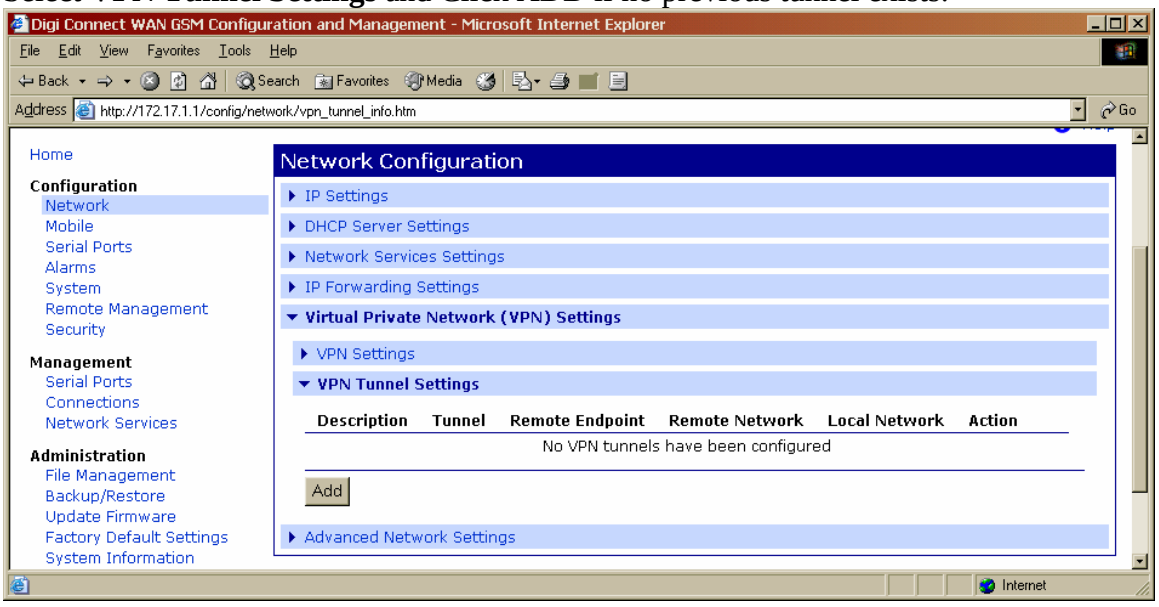


2. Select **VPN Settings** and enter as follows:

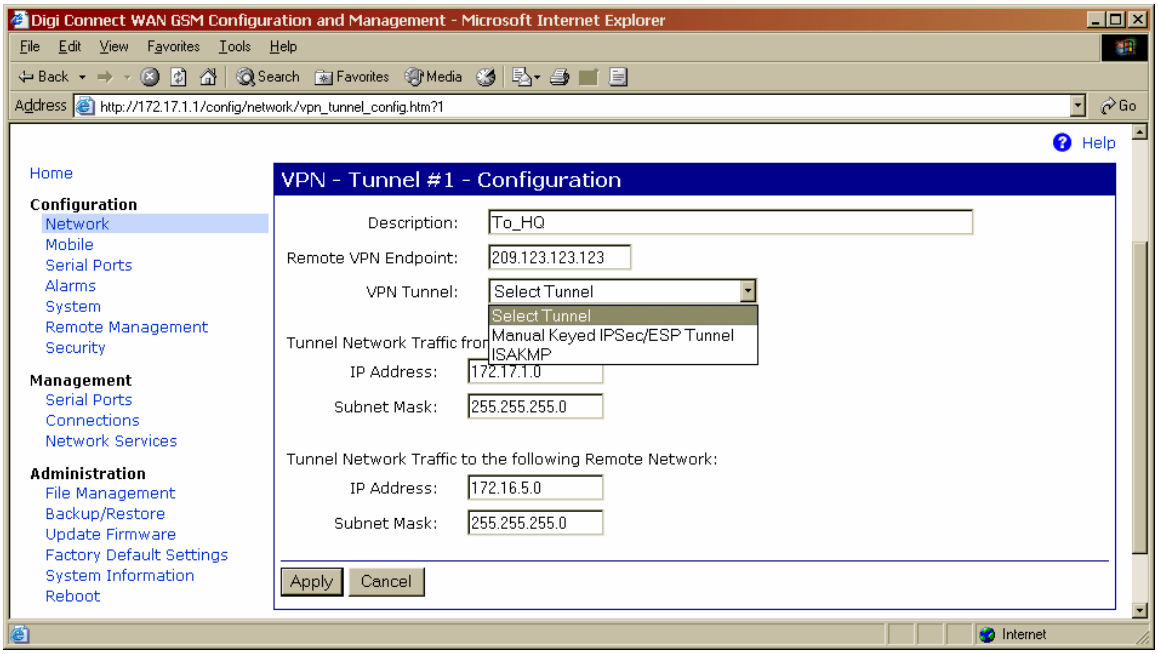


Remember to press APPLY!

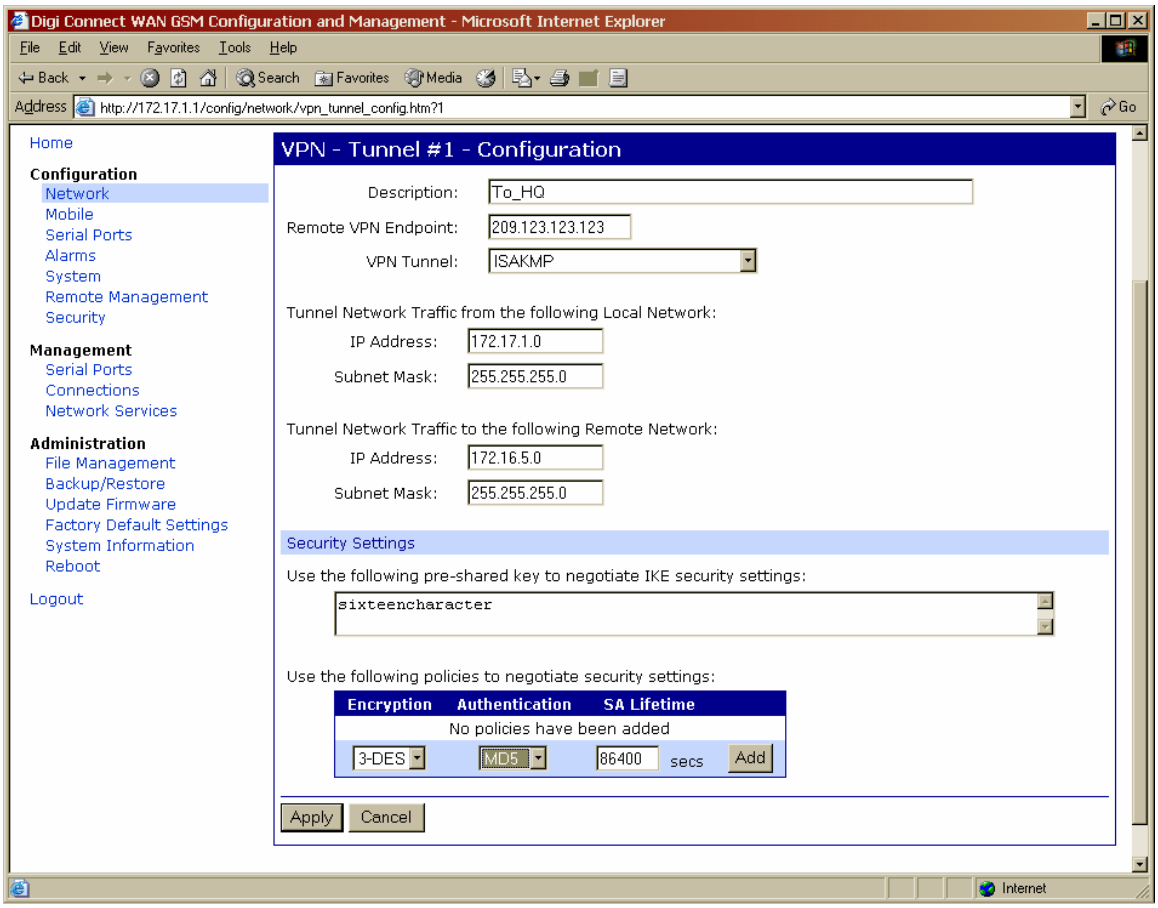
3. Select **VPN Tunnel Settings** and Click ADD if no previous tunnel exists:



Then, add the tunnel:

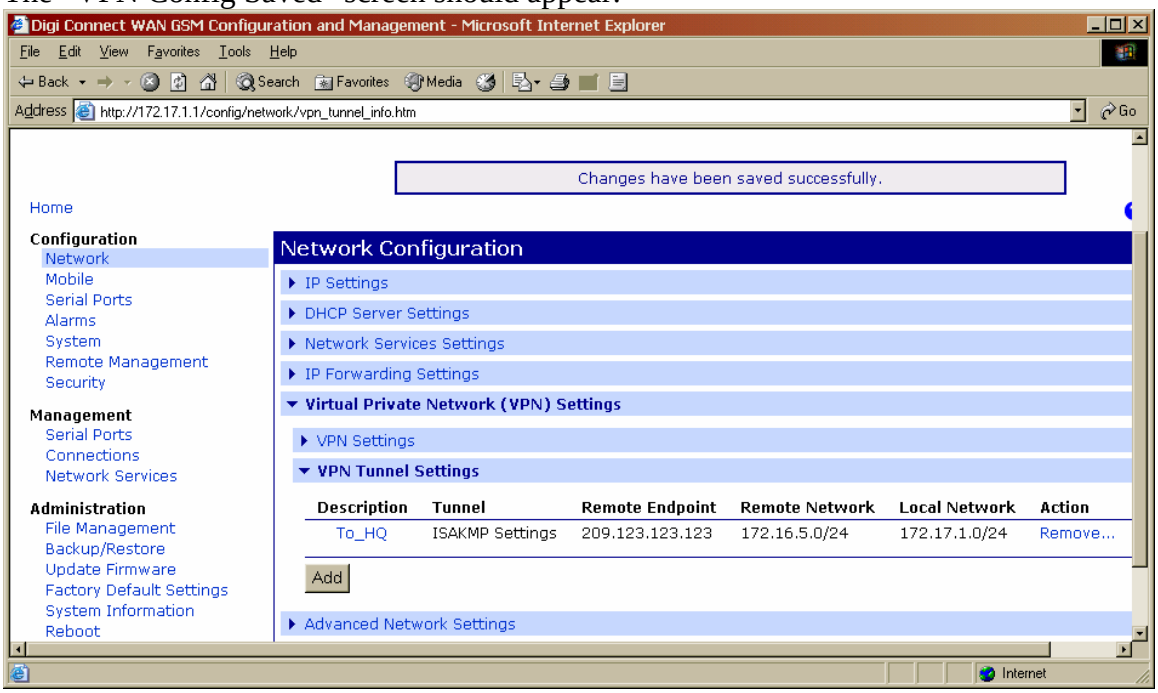


Select ISAKMP and enter the PSK information:



Click APPLY.

4. The "VPN Config Saved" screen should appear:



5. Configure the remote VPN concentrator with the same settings noting to reverse the peer endpoint and remote/local subnet settings.
6. Generate traffic from the remote subnet to the HQ subnet. For example from 172.17.1.100 try pinging 172.16.5.1. The first few pings will say "Destination Host Unreachable" as 172.17.1.100 does not know the route to the remote site. After the VPN tunnel is established, the ping should respond or timeout.
7. To monitor the VPN connection from the Digi Connect VPN:
    a. Via WebUI:
        i. Go to Management > Connections
        ii. The VPN settings should be shown. Note with PSK VPN the "connect" and "disconnect" do not function.
    b. Via Telnet:
        i. Telnet to the Digi Connect VPN IP address, e.g., "telnet 172.17.1.1"
        ii. Enter "display vpn". The current VPN SA information should be listed.

Where to Get More Information

Refer to the Digi Connect WAN 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 via www.digi.com.