



Digi Connect® Family Application Guide

How to Create a VPN between Digi Connect and Sonicwall

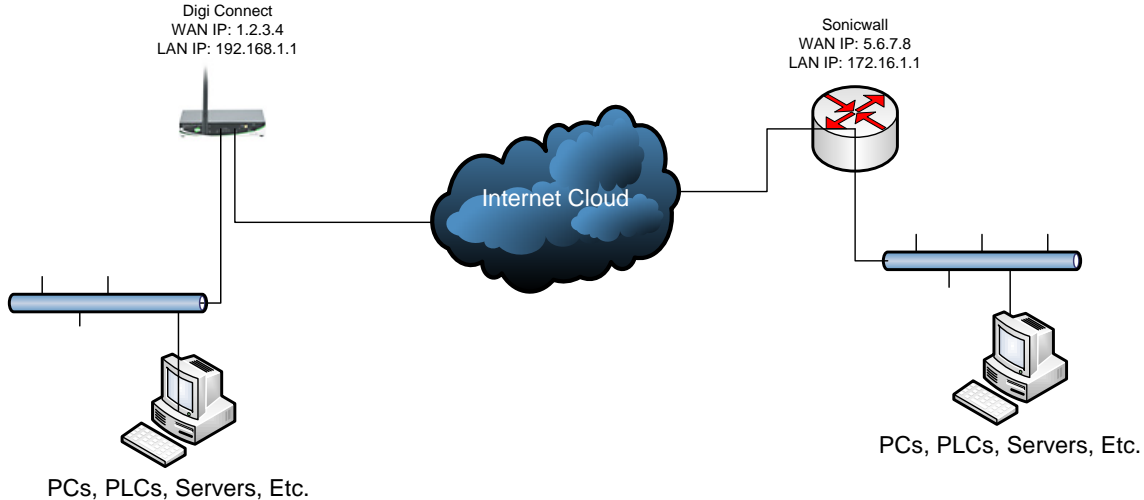
Scenario

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 Sonicwall 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 Sonicwall 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:

Digi Connect Family Application Guide – Connect WAN to Sonicwall

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

123456

ISAKMP Phase 1 Settings

General Security Settings for Phase 1

Connection Mode: Main

Enable Perfect Forward Secrecy (PFS)

NAT-T Settings

Enable NAT Traversal (NAT-T)

Keep Alive Interval: 20

ISAKMP Phase 1 Policies

Authentication	Encryption	Integrity	SA Lifetime	Diffie-Hellman	
Pre-Shared Key	3-DES (192-bit)	MD5	86400 secs	Group 2	Remove
Pre-Shared Key	DES (64-bit)	MD5	86400 secs	Group 2	Add

ISAKMP Phase 2 Settings

General Security Settings for Phase 2

Diffie-Hellman: Group 2

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
None	None	28200 secs	Add

Apply Cancel

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

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

Sonicwall VPN Configuration

1. Configure the Sonicwall VPN device
 - a. Log into the Web Interface of the Sonicwall device.
 - b. Navigate to **VPN** on the left hand panel.
 - c. Under the section titled VPN Policies, click the **Add** button.
 - d. Fill in the appropriate information, shown in the screenshots below

VPN Policy - Mozilla Firefox 3 Beta 2

http://172.16.1.102/vpnConfig_0.html

General Proposals Advanced

Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: To_Digi

IPSec Primary Gateway Name or Address: 1.2.3.4

IPSec Secondary Gateway Name or Address:

Shared Secret: 123456

Destination Networks

Use this VPN Tunnel as default route for all Internet traffic

Destination network obtains IP addresses using DHCP through this VPN Tunnel

Specify destination networks below

Network	Subnet Mask
192.168.1.0	255.255.255.0

Add... Edit... Delete

Ready

OK Cancel Help

Done

The image displays two screenshots of the Sonicwall VPN Policy configuration interface, accessed via Mozilla Firefox 3 Beta 2. The browser address bar shows `http://172.16.1.102/vpnConfig_2.html#`.

Top Screenshot: IKE (Phase 1) Proposal and Ipssec (Phase 2) Proposal

IKE (Phase 1) Proposal:

- Exchange: Main Mode
- DH Group: Group 2
- Encryption: 3DES
- Authentication: MD5
- Life Time (seconds): 28800

Ipssec (Phase 2) Proposal:

- Protocol: ESP
- Encryption: 3DES
- Authentication: MD5
- Enable Perfect Forward Secrecy
- DH Group: Group 2
- Life Time (seconds): 28800

Bottom Screenshot: Advanced Settings

- Enable Keep Alive
 - Try to bring up all possible Tunnels
- Require authentication of local users
- Require authentication of remote users
 - Remote users behind VPN gateway
 - Remote VPN clients with XAUTH
- Enable Windows Networking (NetBIOS) Broadcast
- Apply NAT and Firewall Rules
- Forward packets to remote VPNs
- Default LAN Gateway: 0.0.0.0
- VPN Terminated at:
 - LAN
 - OPT
 - LANOPT

- e. Click **OK** to save the settings.
- f. Click **Apply** in the upper right hand corner to apply the settings to the device. You may have to reboot the device for these changes to take effect, depending on your model of Sonicwall.

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 Wi-Point 3G 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 wireless pages at www.digi.com.