



Digi Wi-Point 3G Application Guide

How to Create a VPN between Wi-Point 3G and Sonicwall

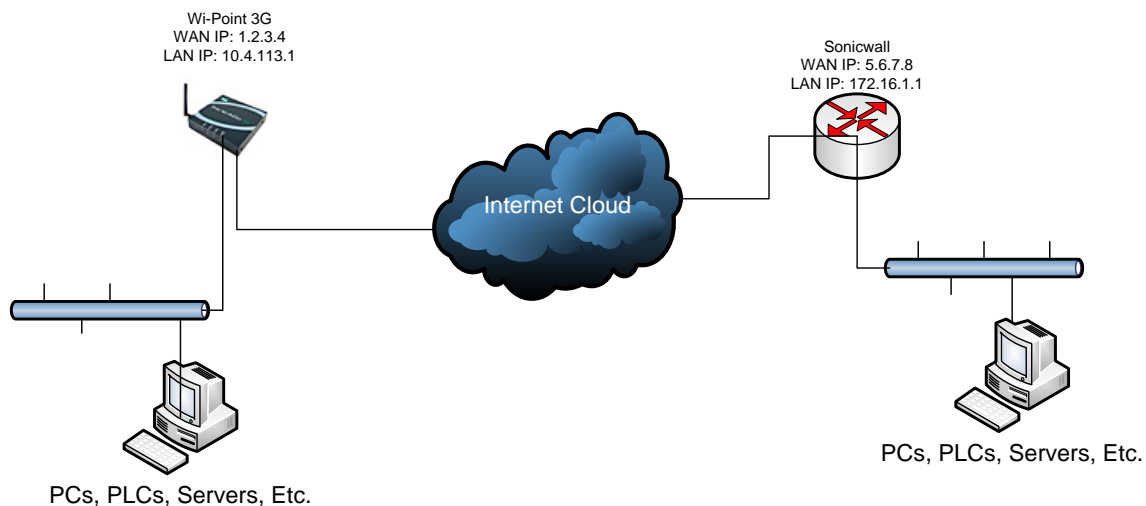
Scenario

Digi Wi-Point 3G 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 Wi-Point 3G gateway to provide primary internet connectivity. The other location is using a Sonicwall VPN appliance 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>.

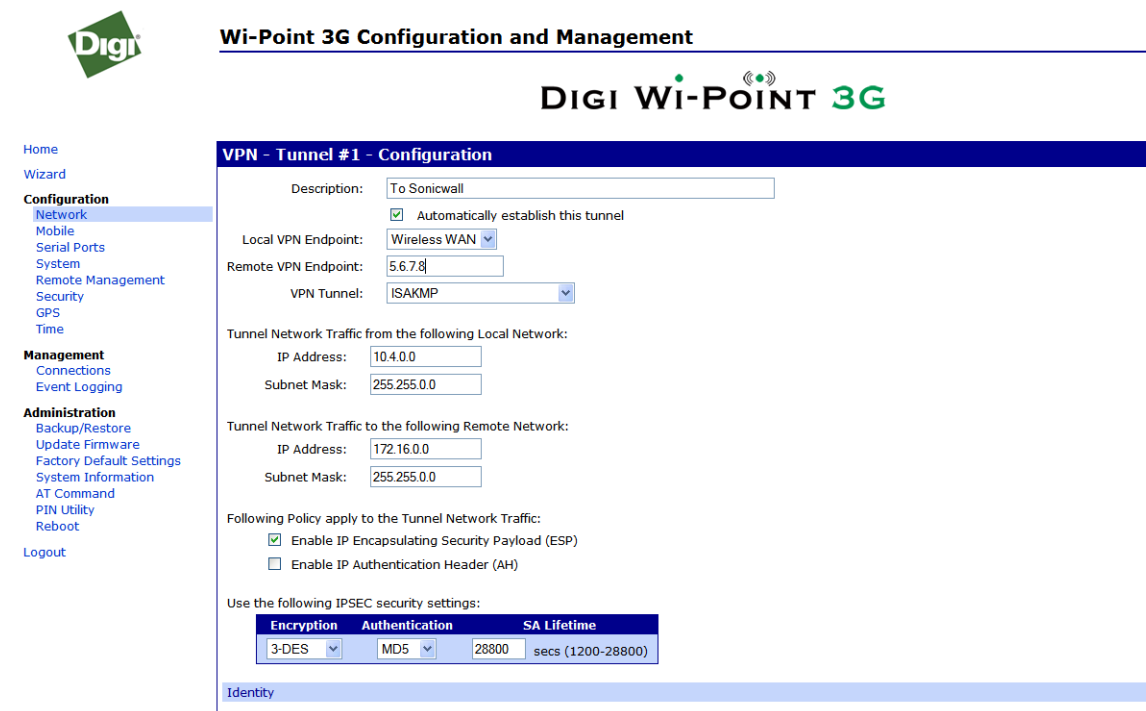
GSM GPRS/EDGE APN Type needed: VPN and GRE end-points usually require static (persistent) IP addresses and must support mobile terminated data connections. If mobile termination is not an option with your current APN, you will need to acquire a new one that does support mobile termination.

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. Open the Web Interface of the device.
 - b. Navigate to **Configuration > Network > VPN Settings**
 - c. Click **VPN Tunnel Settings**
 - d. Click **Add**
 - e. Fill in the appropriate settings below



The screenshot displays the web interface for configuring a VPN tunnel on a Digi Wi-Point 3G device. The page title is "Wi-Point 3G Configuration and Management" and the main heading is "DIGI WI-POINT 3G". The left sidebar contains navigation menus for Home, Wizard, Configuration (with sub-items like Network, Mobile, Serial Ports, System, Remote Management, Security, GPS, Time), Management (Connections, Event Logging), and Administration (Backup/Restore, Update Firmware, Factory Default Settings, System Information, AT Command, PIN Utility, Reboot). The main content area is titled "VPN - Tunnel #1 - Configuration".

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 Sonicwall

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.

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_2.html

General Proposals Advanced

Security Policy

IPsec Keying Mode: IKE using Preshared Secret

Name: To_WiPoint

IPsec Primary Gateway Name or Address: 1.2.3.4

IPsec Secondary Gateway Name or Address: 0.0.0.0

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
10.4.0.0	255.255.0.0

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 top screenshot shows the 'Advanced' tab for the 'IKE (Phase 1) Proposal' and 'Ipssec (Phase 2) Proposal' sections. The bottom screenshot shows the 'Advanced Settings' section.

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

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. 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 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.