

#### Scenario

Digi Connect family VPN router (for example ConnectPort WAN or Digi Connect WAN IA) is used for primary remote site connectivity. A remote user needs to be able to VPN into the Digi Connect router for network access to devices behind the Digi.

### Theory of Operation

The remote user needs a way of connecting to devices on the LAN side of the Digi Connect router. They will have TheGreenBow VPN client installed on their PC to accommodate this function. TheGreenBow VPN client will initialize the connection to the Digi Connect router on demand.

The Digi Connect router is setup to accept incoming VPN connections from a VPN client using IPSec as the transport protocol.

#### 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 <u>http://www.digi.com/support</u>.

**PC Requirements:** TheGreenBow VPN client will need to be installed on the PC. This setup may work with other VPN clients that support IPSec tunnels, but have not been tested by Digi International.

**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 Global Settings
    - i. Navigate to **Configuration > Network > VPN Settings** in the web interface of the unit.
    - ii. Click on VPN Global Settings.
    - iii. Click the check box for **Enable Antireplay**.
    - iv. Click **Apply** to save the changes.

nome	Network Configuration
Configuration	Ethernet IP Settings
Mobile	DHCP Server Settings
Serial Ports	Network Services Settings
Alarms	Dynamic DNS Update Settings
System	IP Filtering Settings
Security	▶ IP Forwarding Settings
Position	IP Network Failover Settings
Applications	Socket Tunnel Settings
Python RealPort	▼ Virtual Private Network (VPN) Settings
Management	▼ VPN Global Settings
Serial Ports	General Security Settings
Event Logging	
Network Services	🔛 Enable Antrice)ay
Administration	Miscellaneous Settings
File Management X.509 Certificate/Kev	Suppress SA lifetime during IKE phase 1
Management	Suppress Delete Phase 1 SA Message For PFS
Update Firmware	Draddresses of remote VPN peers may change on the fly (Dynamic DNS)
Factory Default Settings	
Reboot	Apply
Logout	▶ VPN Policy Settings
	IP Pass-through Settings
	Host List Settings
	Control Device De doue Device Device 100000 Deble de

- b. 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	🕜 Hel	р
Configuration Network	VPN - Tunnel #2 - Configuration	l
Mobile Serial Ports Camera Alarms System iDiai	Description:     TheGreenBow       VPN Tunnel:     ISAYMP       Local Endpoint Type:     Local endpoint is a subnet	
Security	VPN Mode	I.
Position	Initiate client connections to and accept connections from the remote VPN device at:	
Applications Python RealPort	0.0.0	
Management Serial Ports	Accept connections from any VPN device	
Connections	Identity	4
Event Logging Network Services	Network Interface: mobile0 •	
Administration File Management X.509 Certificate/Key Management Backup/Restore Update Firmware	Use the following as the identity: bill@digi.com     Use the interface IP address     Use the identity certificate X.S09 distinguished name (DN)	
Factory Default Settings System Information	Local Endpoint	1
Reboot Logout	Tunnel Network Traffic from the following Local Network:       IP Address:     104.116.0       Subnet Mask:     255 255.55 0	

Remote Endpoint								
Tunnel Network Traffic	to the following Remote N	etwork:						
IP Address:	192.168.1.0							
Subnet Mask:	255.255.255.0							
Pre-Shared Key Setting	s							
Use the following IP ad	dress, FQDN, or username	for the remote VF	PN's ID:					
bob@digi.com								
Use the following pre-s	hared key to negotiate IK	E security settings						
123456789					*			
					*			
ISAKMP Phase 1 Sett	ngs							
General Security Settin	gs for Phase 1							
Connection Mc	de: Main 💌							
Enable Perfe	t Forward Secrecy (PES)							
Lo chabic Pere								
NAT-T Settings								
🗹 Enable NAT T	raversal (NAT-T)							
Keep Alive	Interval: 20							
ISAKMP Phase 1 Policia	0							
ISAKAP PHase I Police	•				_			
Authenticatio	on Encryption	Integrity S/	A Lifetime	Diffie-Hellman	Romovo			
Fre-Sitaleu K	ey AES (120-bic)	JIMI 00	0400 secs	Group 2	Keniove			
🗹 Enable Perfe	t Forward Secrecy (PFS)							
☑ Enable Perfe	tt Forward Secrecy (PFS)							
Enable Perfe  NAT-T Settings	tt Forward Secrecy (PFS)							
Enable Perfe  NAT-T Settings      Enable NAT T  Koon Alive	tt Forward Secrecy (PFS)							
Enable Perfe  NAT-T Settings      Enable NAT T      Keep Alive	raversal (NAT-T) Interval: 20							
Enable Perfe  NAT-T Settings      Enable NAT T      Keep Alive  ISAKMP Phase 1 Policie	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20							
Enable Perfe     Art-T Settings     Enable NAT T     Keep Alive     ISAKMP Phase 1 Policie     Authenticati	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s pn Encryption	Integrity S/	A Lifetime	Diffie-Hellman				
Enable Perfe     AT-T Settings     Enable NAT T     Enable NAT T     Keep Alive     ISAKMP Phase 1 Policie     Authenticali     Pre-Shared k	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s on <u>Ettcryption</u> ey AES (128-bit)	Integrity S/ SHA1 86	A Lifetime 6400 secs	Diffic-Hellman Group 2	Remove			
<ul> <li>Enable Perfe</li> <li>NAT-T Settings</li> <li>Enable NAT T</li> <li>Keep Alive</li> <li>ISAKMP Phase 1 Policie</li> <li>Pre-Shared K</li> <li>Pre-Shared Ke</li> </ul>	autor         Intervent Secrecy (PFS)           raversal (NAT-T)         Interval:           n         Encryption           s         Encryption           n         Encryption           y         AES (128-bit)	Integrity SX SHA1 88 SHA1 86	A Lifetime 6400 secs 400 secs	Diffie-Hellman Group 2 Group 2	Remove Add			
Enable Perfe     Enable Perfe NAT-T Settings     Enable NAT T     Keep Alive ISAKMP Phase 1 Policie     Pre-Shared K     Pre-Shared K     ISAKMP Phase 2 Setti	tt Forward Serrecy (PFS) raversal (NAT-T) Interval: 20 s pn Encryption ey AES (128-bit) y AES (128-bit) mps	Integrity SJ SHA1 86 SHA1 86	A Lifetime 6400 secs 400 secs	Diffie-Hellman Group 2 Group 2	Remove Add			
Enable Perfe     MAT-T Settings     Enable NAT T     Keep Alive     ISAKMP Phase 1 Policie     Pre-Shared K     Pre-Shared K     ISAKMP Phase 2 Sett     General Security Settin	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s bn Encryption AES (128-bit) Encryption ags for Phase 2	Integrity S/ SHA1 80 SHA1 86	A Lifetime 6400 secs 400 secs	Diffie-Hellman Group 2 Group 2	Remove Add			
Rable Perfe     AT-T Settings     Enable NAT T     Keep Alive     ISAKMP Phase 1 Policie     Pre-Shared K     Pre-Shared K     Pre-Shared K     General Security Settin     Diffie-Hellman:	aut	Integrity S/ SHA1 80 SHA1 86	A Lifetime 6400 secs 400 secs	Diffie-Hellman Group 2 Group 2 💌	Remove Add			
Enable Perfe     AT-T Settings     Enable NAT T     Keep Alive     ISAKMP Phase 1 Policie     Pre-Shared Ke     Pre-Shared Ke     ISAKMP Phase 2 Setti     General Security Settin     Diffie-Hellman:	autor         Interval         Strong           raversal (NAT-T)         Interval:         20           s         Strong         Strong           on         Encryption         Encryption           y         AES (128-bit)         *           ngs         gs for Phase 2         Group 2         *	Integrity S/ SHA1 84 SHA1 96	A Lifetime 6400 secs 400 secs	Diffie-Hellman Group 2 Group 2 💌	Remove Add			
Enable Perfe     AT-T Settings     Enable NAT T     Keep Alive     SAUMP Phase 1 Policie     Pre-Shared K     Pre-Shared K     Pre-Shared K     General Security Settin     Diffie-Hellman:     ISAMP Phase 2 Policie	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s bn Encryption x AES (128-bit) x AES (128-bit)	Integrity S/ SHA1 86 SHA1 96	A Lifetime 6400 secs 400 secs	Diffic-Heliman Group 2 Group 2	Remove Add			
Rable Perfe     AT-T Settings     Enable NAT T     Keep Alive     SAKOMP Phase 1 Policic     Pre-Shared K     Pre-Shared K     Pre-Shared K     Pre-Shared K     Drifie-Hellman:     Difie-Hellman:     Difie-Hellman:	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s n Encryption y AES (128-bit) y AES (128-bit) y Group 2 Group 2 s s s	Integrity SJ SHA1 86 SHA1 = 864 SHA1 = 864 stingsHiphest pr	A Lifetime 6400 secs 400 secs	Diffie-Hellman Group 2 Group 2	Remove Add			
Enable Perfe     AT-T Settings     Control Contro	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s n Encryption s s AES (128-bit) v AES (128-bit) v AES (128-bit) s gs for Phase 2 Group 2 s s to negotiate security ss Authentication S	Integrity Sr SHA1 86 SHA1 66 SHA1 66 SHA1 A 66	A Lifetime 6400 secs 400 secs	Diffre-Hollman Group 2 Group 2 •	Remove Add			
Enable Perfe     An-T Settings     Enable NAT T     Keep Alive     SALVP Phase 1 Policie     Authenticali     Pre-Shared K     Pre-Shared	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s pn Encryption v AES (128-bit) v AES (128-bit) v AES (128-bit) s g for Phase 2 Group 2 • s Authentication S y SHAL 2	Integrity S/ SHA1 8 SHA1 8 SHA1 8 86 SHA1 8 86 SHA1 8 86 SHA1 8 SHA1 8 S	A Lifetime 6400 secs 400 secs riority listed la:	Diffie-Hellman Group 2 Group 2 •	Remove Add			
Inable Perfe     AT-T Settings     Inable Parfe     AT-T Settings     Inable NAT 1     Keep Alive     Stat/MP Phase 1 Policie     Pre-Shared K     Pre-Shared K     Pre-Shared K     Pre-Shared K     Drifie-Hellman:     Dfie-Hellman:     ISA/MP Phase 2 Policie     Use the following polici     Lister S (128-bit)     AES (128-bit)	att         Forward Secrecy (PFS)           raversal (NAT-T)         Interval:           n         Encryption           ex         AES (128-bit)           y         AES (128-bit)           y         AES (128-bit)           gs for Phase 2         Group 2           s         s           attention as your of the security is some	Integrity 55 SHA1 80 SHA1 ₹ 86 SHA1 \$ 86 SHA1	A Lifetime 6400 secs 400 secs riority listed la:	Diffie-Hellman Group 2 Group 2	Remove Add			
Enable Perfe     AT-T Settings     Enable NAT 1     Keep Alive     StAVOP Phase 1 Policie     Pre-Shared K     Pre-Shared K     Pre-Shared K     Pre-Shared K     StAKMP Phase 2 Setti     StAKMP Phase 2 Policie     Use the following polic     Encryption     AES (128-b);     AES (128-b);     AES (128-b);	aux         intervent           raversal (NAT-T)         Interval:           Interval:         20           s         S           on         Encryption           y=         AES (128-bit)           y=         S           gs         Group 2           s         S           y=         SHA1	Integrity SF SHA1 & R SHA1 • 86 SHA1	A Lifetime 6400 secs 400 secs secs riority listed la:	Diffle-Hellman Group 2 Group 2 • st:	Remove Add			
Charles Perference Constraints Constraint	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s proversal (NAT-T) reversal (NAT-T) reversal (NAT-T) s s s s s s s s s s s s s	Integrity S/ SHA1 8 SHA1 8 SHA1 8 8 SHA1 8 8 SHA1 8 8 SHA1 8 SHA1	A Lifetime 6400 secs 400 secs riority listed la: nove add	Diffie-Hellman Group 2 Group 2 •	Remove Add			
Canable Perfe     AT-T Settings     Canable Parfe     Arthenicati     Canable NAT 1     Keep Alive     Statume Content of the Content of	tt Forward Secrecy (PFS) raversal (NAT-T) Interval: 20 s on Encryption ev AES (128-bit) v AES (128-bit) v AES (128-bit) s g for Phase 2 Group 2 s s s to negotiate security s AES to negotiate security s AES ANT 2 a SHA1 2 a	Integrity 55 SHA1 & R SHA1 = 86 SHA1	A Lifetime 6400 secs 400 secs 400 secs 400 secs 400 secs 400 secs 400 secs 400 secs	Diffie-Hellman Group 2 Group 2 •	Remove Add			

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

#### NOTE FOR CUSTOMERS RUNNING FIRMWARE VERSION 2.13.x OR LATER

If running firmware version 2.13.x or later, there is a few additional steps to make TheGreenBow work with the Digi Connect device:

- 1) Telnet into the CLI of the Digi Connect device.
- 2) Enter in the folloiwng 3 commands, pressing Enter after each one:

set vpn global send\_natt\_draft\_01\_id=off set vpn global send\_natt\_draft\_02\_id=off set vpn global send\_natt\_draft\_03\_id=off

3) This will now allow TheGreenBow to build a connection to the Digi Connect product.

#### **TheGreenBow VPN Client Configuration**

- 1. Configure TheGreenBow VPN Client
  - a. Install TheGreenBow VPN Client. A free trial version can be downloaded here: <u>http://www.thegreenbow.com/</u>.
  - b. Right click **Configuration** in the left hand pannel, and click **New Phase 1**.
  - c. Fill in the appropriate fields shown in the screenshot below:

	IPSec VPN Clie
🚇 Console	Phase1 (Authentication)
🚱 Parameters	Name To_Digi
S Connections	Interface Any
Root ⊟STO_Dig G Tunnel1	Remote Gateway 166.125.123.25         Preshared Key       ************************************
	IKE     P1 Advanced       Authentication     SHA-1       Key Group     DH2 (1024)

- d. Click the **P1** Advanced button.
- e. Fill in the appropriate fields show in the following screenshot:

Phase1 Advance	1	X
		S
Advanced featur	es	
📃 Config Mod	e Redund.GV	/
Aggressive	Mode NAT-	f Automatic 🔽
X-Auth		
📃 X-Auth Pop	JP Logi	n 🗌
🔄 Hybrid Mod	e Passwor	± t
	- 15	
Local and Remo	Choose the tupe of ID:	Set the value for the ID:
Local ID	Email	bob@digi.com
Remote ID	Email 🗸	bill@digi.com
		Ok Cancel

- f. Click Save & Apply to save the settings.
- g. Right click the Phase 1 policy that was added in the left hand pannel, and click **Add Phase 2**
- h. Fill in the appropriate fields for the Phase 2 settings, shown in the following screenshot:

ile <u>V</u> PN Configuration Vi	e <u>w T</u> ools <u>?</u>
HEGREENBO	IPSec VPN Client
🔑 Console	Phase2 (IPSec Configuration)
🙀 Parameters	Name Tunnel1
S Connections	VPN Client address 192 . 168 . 1 . 100
GRoot ⊡STo_Digi ⊛Tunnel1	Address type Subnet address Remote LAN address 10 , 4 , 116 , 0 Subnet Mask 255 , 255 , 0
	ESP Encryption AES 128  P2 Advanced Authentication SHA-1  Scripts
	Mode Tunnel   PFS Group DH2 (1024)   Open Tunnel
	Save & Apply

**NOTE**: The **VPN Client address** field above needs to match the subnet of the **Remote Endpoint** section of the Digi setup. This IP can be any IP that falls within the subnet specified on the Digi, regardless of what the actual IP of the PC running TheGreenBow is currently using. This is the IP address your PC will show up with on the other side of the VPN tunnel.

- i. Click Save & Apply to save the configuration.
- j. Click **Open Tunnel** to establish the VPN connection to the ConnectPort WAN VPN.

# ADDITIONAL NOTES

- 1. The preceding configuration will also work for the ZyXEL VPN Client. It may also work for other VPN clients that have not been tested by Digi.
- 2. 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.
- 3. 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.
- 4. 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 <u>www.digi.com/support</u> for more information. Technical assistance is available at <u>http://www.digi.com/support/eservice/eservicelogin.jsp</u>.

For sales and product information, please contact Digi International at 952-912-3444 or refer to the Digi Connect wireless pages at <u>www.digi.com</u>.