

Scenario

Digi Connect family VPN router (for example ConnectPort WAN or Digi Connect WAN IA) is used for remote site connectivity. Juniper Netscreen is used at the local site for connectivity. The connection between the two networks needs to be secure for data transmission.

Theory of Operation

A location needs to be able to build a secure tunnel between the main site and a remote branch. One location has a Digi Connect router to provide primary internet connectivity. The other location uses a Juniper Netscreen for primary internet connectivity. The Digi Connect router will create a VPN tunnel to the Juniper Netscreen, creating a secure connection.

Sample Diagram



Carrier Plan and 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>.

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.

Home	Network Configuration
Configuration	Ethernet IP Settings
Mobile	DHCP Server Settings
Serial Ports	Network Services Settings
Alarms	Dynamic DNS Update Settings
System Romoto Managoment	IP Filtering Settings
Security	IP Forwarding Settings
Position	IP Network Failover Settings
Applications	Socket Tunnel Settings
RealPort	▼ Virtual Private Network (VPN) Settings
Management	▼ VPN Global Settings
Serial Ports Connections	General Security Settings
Event Logging Network Services	🗹 Enable Antireplay
Administration	Miscellaneous Settings
File Management X 509 Certificate/Key	Cuproce SA lifetime during IVE phase 1
Management	Suppress Delete Diace 1 SA Messare En PES
Update Firmware	
Factory Default Settings	Apply
Reboot	VDN Policy Settinge
Logout	V Pri Policy Securitys
-	IP Pass-through Settings
	Host List Settings
	Virtual Kouter Redundancy Protocol (VRKP) Settings
	Advanced Network Settings
Done	Q Internet

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:

	VPN = Lunnel # L - Contiguration
Configuration	
Network Mobile	Description: Lunne I
Serial Ports	Remote VPN Address: 70.57.159.140
Alarms	VPN Tunnel: ISAKMP
System Remote Management	Local Endpoint Type: Local endpoint is a subnet
Position	Identity
Applications	Network Interface: mobile0 💌
Python RealPort	☑ Negotiate tunnel as soon as interface comes up
Management	
Serial Ports	• Use the following as the identity: Dob@digl.com
Event Logging	Use the interface IP address
Network Services	Obe the identity certificate X.509 distinguished name (DN)
Administration File Management	Local Endpoint
X.509 Certificate/Key Management	Tunnel Network Traffic from the following Local Network:
Backup/Restore	IP Address: 192.168.1.0
Update Firmware Factory Default Settings	Subnet Mask: 255 255 255 0
System Information	
Reboot	Remote Endpoint
Logoul	Tunnel Network Traffic to the following Remote Network:
	IP Address: 172.16.0.0
	Subnet Mask: 255.255.0.0
	Pre-Shared Key Settings
	Use the following IP address, FQDN, or username for the remote VPN's ID:
	bill@digi.com
	Use the following pre-shared key to negotiate INE security settings:
Use the f	ollowing pre-shared key to negotiate IKE security settings:
12	3456
	×
ISAKMP	Phase 1 Settings
General S	jecurity Settings for Phase 1
Co	
0	nnection Mode: Main Y
	nnection Mode: Main Y Enable Perfect Forward Secrecy (PFS)
VAT-T Set	Innection Mode: Main Finable Perfect Forward Secrecy (PFS)
NAT-T Set	Innection Mode: Main Enable Perfect Forward Secrecy (PFS) tings Enable Mit Tenered (MIT T)
NAT-T Set	Innection Mode: Main Enable Perfect Forward Secrecy (PFS) tings Enable NAT Traversal (NAT-T) Keen Alive Internal: 20
NAT-T Se	Innection Mode: Main Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20
ISAKMP P	Innection Mode: Main Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies
ISAKMP P	Innection Mode: Main Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman
	Innection Mode: Main Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove
	Innection Mode: Main Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove 7re-Shared Key V DES (64-bit) V MD5 86400 secs Group 2 Add
ISAKMP	nnecton Mode: Man ♥ Enable Perfet Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove 7re-Shared Key ♥ DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings
ISAKMP General S	Intection Mode: Main Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key DES (64-bit) W MD5 86400 secs Group 2 Add Phase 2 Settings ecurity Settings for Phase 2
ISAKMP General S Diff	nnection Mode: Main ♥ Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key ♥ DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings ecurity Settings for Phase 2 ie-Hellman: Group 2 ♥
ISAKMP General S Diff	nnection Mode: Main ♥ Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key ♥ DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings ecurity Settings for Phase 2 ie-Hellman: Group 2 ♥
ISAKMP General S Diff	nnecton Mode: Main ♥ Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings iecurity Settings for Phase 2 ie-Hellman: Group 2 ♥ hase 2 Policies
ISAKMP P Use the f	nnecton Mode: Man ♥ Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key ♥ JES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key ♥ JES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings iecurity Settings for Phase 2 ie-Hellman: Group 2 ♥ hase 2 Policies Jlowing policies to negotiate security settingsHighest priority listed last: Encryption Authentication SA Lifetime
ISAKMP P Use the f	nnecton Mode: Main ♥ Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key ♥ DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings iecurity Settings for Phase 2 ie-Hellman: Group 2 ♥ hase 2 Policies slowing policies to negotate security settingsHighest priority listed last: Encryption Authentication SA Lifetime 3-DES SHA1 28200 secs Remove
ISAKMP P Use the f	nnecton Mode: Main ♥ Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key ♥ DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings iecurity Settings for Phase 2 ie-Hellman: Group 2 ♥ hase 2 Policies slowing policies to negotiate security settingsHighest priority listed last: Encryption Authentication SA Lifetime None ♥ None ♥ 28200 secs Remove
ISAKMP P Use the f	nnecton Mode: Main ♥ Enable Perfect Forward Secrecy (PFS) titings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key ♥ DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings iecurity Settings for Phase 2 ie-Hellman: Group 2 ♥ hase 2 Policies Blowing policies to negotiate security settingsHighest priority listed last: Encryption Authentication SA Lifetime None ♥ None ♥ 28200 secs Remove
ISAKMP P Use the f	nnecton Mode: Main ♥ Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key ♥ DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings iecurity Settings for Phase 2 ie-Hellman: Group 2 ♥ hase 2 Policies allowing policies to negotiate security settingsHighest priority listed last: Encryption Authentication SA Lifetime 3-DES SHA1 28200 secs Remove None ♥ None ♥ 28200 secs Add
ISAKMP P Use the f	Innection Mode: Main Enable Perfect Forward Secrecy (PFS) Enable Perfect Forward Secrecy (PFS) Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key DES (64-bit) MD5 86400 secs Group 2 Remove Pre-Shared Key DES (64-bit) MD5 86400 secs Group 2 Add Phase 2 Settings iecurity Settings for Phase 2 ie-Hellman: Group 2 hase 2 Policies allowing policies to negotiate security settingsHighest priority listed last: Encryption Authentication SA Lifetime 3-DES SHA1 28200 secs Remove None None None Authentication SA Lifetime 2ancel
ISAKMP P ISAKMP P General S Diff ISAKMP P Use the f	nnecton Mode: Man ♥ Enable Perfect Forward Secrecy (PFS) ttings Enable NAT Traversal (NAT-T) Keep Alive Interval: 20 hase 1 Policies Authentication Encryption Integrity SA Lifetime Diffie-Hellman Pre-Shared Key 3-DES (192-bit) SHA1 86400 secs Group 2 Remove Pre-Shared Key DES (64-bit) ♥ MD5 ♥ 86400 secs Group 2 ♥ Add Phase 2 Settings iecurity Settings for Phase 2 ie-Hellman: Group 2 ♥ hase 2 Policies ollowing policies to negotiate security settingsHighest priority listed last: Encryption Authentication SA Lifetime 3-DES SHA1 28200 secs Remove None ♥ None ♥ 28200 secs Add

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

Juniper Netscreen Configuration

- 1. Log into the Juniper Netscreen through its web interface.
- 2. Navigate to **Objects > Addresses > List** in the web interface. Select **Untrust** in the upper left hand corner, and click **New** in the upper right hand corner.
- 3. Fill in your Remote Site information, as shown in the screenshot below:

🖉 Juniper-ScreenOS Administration Tools (ns5gt) - Windows Internet Explorer			- 2 🛛
S 😒 🖝 http://172.16.1.90/rswebui.html	Google 🖌 🖌		P -
Google 🛛 👻 👽 Search 🖗 🖉 • 🕅 • 🏙 🖉 🚯 • 🔛 • 🏠 Boolimarks • 🔀 Find • 🖑 Check •		S -	🔵 filpdo *
😭 🏟 🔝 Junper-StreenOS Administration Tools (rs5gt)	👌 • 🔊 -	🖶 🔹 🔂 Bage 🤹	💮 Tools 🔹 🎽
Objects > Addresses > Configuration		ns5gt	?
Dipersonation Dipersonation Dipersonation Network Oconfiguration Network Screening Policies VPNa Objects Addresses List Groups Summary Serveesing Policies Uses Pools Schedules Comp Expressions Centificates Natacks Reports Vitizates Oktoria Output Introduction		ns5gt	2

4. Once this has been completed, click **Ok** to save the setting. You will then need to switch the **Untrust** option to **Trust** and perform the same settings for the Local Site information, as shown in the following screenshot:

C Juniper-ScreenOS Administr	ation Tools (ns5gt) - Windows Internet Explorer			
	3/nswebui.html		Google 😽 🗙 Google	P -
Google 8 -	Search 🛛 🖉 • 🕅 • 🎆 🧟 🕑 • 🔤 • 🏠 Bookmarks• 🔍 Find • ỡ Che	:k •		🔦 🔹 🔵 flipdo •
🚖 🔅 🎦 Juniper-ScreenOS Adm	inistration Tools (ns5gt)		🙆 • 🖻 👘	🖶 🔹 🔂 Page 🔹 🍈 Tgols 🔹
	Objects > Addresses > Configuration			ns5gt ?
Version of the second s	Address Name Comment P Address / Domain Name Domain Name Zone	VPNIocal		

5. Navigate to **VPNs > AutoKey Advanced > Gateway:**

🖉 Juniper-ScreenOS Administratio	on Tools (ns5gt) -	Windows Interne	et Explorer				_ 7 🗙
C					✓ 47 × 60	ogle	P •
Google 8 -	Search 👳	🧭 • 🕅 • 🎆	🧟 🕒 - 🔤 - 🔕 - 🛠 Bookmarks - 🗟 Find - 🛠 Chec	k -		ې • 📢	🕽 flipdo 🔹
🚖 🔅 🔝 Juniper-Screen OS Administr	ration Tools (ns5gt)				🖄 •	🔊 - 🖶 - 🕞 Bage - 🏈	Tgols + "
	VPNs > AutoKey	/ Advanced > G	ateway			ns5gt	?
	List 20 🔽 per	page					
Juniper *						N	lew
E Z NETWORKS							
NetScreen-5GT	Name	Туре	Address/ID/User Group	Local ID	Security Level	Configure	
- Home	test	Static	166.130.108.93	bill@digi.com	Custom	Edit -	
Configuration Addition							
Screening							
Policies VPNs							
AutoKey IKE							
- Gateway							
- P1 Proposal - P2 Proposal							
- XAuth Settings							
– VPN Groups – Manual Key							
L2TP Manifes Status							
Objects							
Reports Wizards							
+ Help							
- Logout							
Toggle Menu							
Done					u 😜 😱	iternet 🔍	. • .:

- 6. Click **New** in the upper right hand corner and fill in the following information (shown in the following screenshot):
 - a. Security Level Custom
 - b. Remote Gateway Type Can be static or dynamic. This example will use static.
 - c. IP Address/Hostname The mobile IP or hostname of the Digi gateway.
 - d. Peer ID The ID that the Digi gateway is using.
 - e. Preshared Key
 - f. Local ID The ID that the Juniper unit is using.

🤗 Juniper-ScreenOS Administration Tools (ns5gt) - Windows Internet Explorer 📃 🖻 🔀						
🚱 🗸 🔺 http://172.16.1.9	18/nswebui.html	Soogle	P -			
Google 8 -	💌 Search 🖗 🖉 • 🕅 • 🏙 🙋 🕑 • 🔤 • 🏠 Bookmarks • 🖳 Find • 🖑 Check •	ی ج 🌒 ا	flipdo*			
🚖 🏘 🔝 Juniper-ScreenOS Adr	ministration Tools (ns5gt)	🚵 🔹 🔝 🕤 🖶 🖬 Bage 🕶 🎯 T	gols - »			
	VPNs > AutoKey Advanced > Gateway > Edit	ns5gt	?			
Description Descr	Gateway Name test Security Level Standard Compatible Basic Custom Static IP Address Dialup User Dialup User Group Preshared Key Local ID bil@digi.com (optional) Outgoing Interface Untust OK Advanced	IP Address/Hostname 156.130.108.93 Peer ID bob@digi.com User None ♥ Group None ♥				

- 7. Click **Advanced** and fill in the following information (shown in the following screenshot):
 - a. Phase 1 Proposal pre-g2-3des-sha
 - b. Mode (Initiator) Main

A http://172.16.1.9	8/novebui.htm	V 4 X Goode	ام
Consta II	warden and a Mar III O A a Mar III a A Budantar A Cata State		A
	Search V (2) · M · M · M · M · M · Doormarks · M ring · V theor ·		N T T T T
💢 🕸 🎦 Juniper-ScreenOS Adi	ninistration Tools (ns5gt)		🖶 * 🔂 Bage • 🕥 Tgols •
	VPNs > AutoKey Advanced > Gateway > Edit		ns5gt ?
Juniper			
A NETWORKS			
NetScreen-5GT	Security Level		
	Predefined O Standard O Compatible O Basic		
- Home Configuration	Phase 1 Proposal		
Network	pre-o2-3des-sha		
Screening Delision	None V None V		
- VPNs			
- AutoKey IKE	Mode (Initiator) Main (ID Protection) Aggressive		
 AutoKey Advanced Gateway 	Enable NAT-Traversal		
- P1 Proposal	UDP Checksum		
- P2 Proposal	Keepalive Frequency 0 Seconds (0~300 Sec)		
- VPN Groups	Louthout		
- Manual Key	Hello 0 Seconds (0~3600 Sec)		
Monitor Status	Reconnect 0 Seconds (60~9999 Sec)		
 Objects 	Threshold 5		
Reports Wizards			
 Help 	None Xauth Server		
– Logout	• Use Default		
Toggle Menu	O Local Authentication		
	O Allow Any		
	Olicer Croup		
	Allowed Authentication Type CHAP Only		
	○ External Authentication None ✓ □ Query Remote Setting		
	 Allow Any 		
	OUser Name		
	OUser Group Name		
	Allowed Authentication		
	O XAuth Client		
	User Name		
	Password		
	Allowed Authentication Type CHAP Only		

- 8. Click **Return.**
- 9. Click Ok.
- 10. Navigate to **VPNs > AutoKey IKE** and click **New** in the upper right hand corner to get to the following screen:

Very Ut2 L1 L1 Very Web Mile Very Mile	🖉 Juniper-ScreenOS Administ	stration Tools (ns5gt) - Windows Internet Explorer		- 7 🛛
Congle g · wonh · · · · · · · · · · · · · · · · · · ·	🕒 🕞 👻 🚹 http://172.16.1.9	.98(nswebul.html	🖌 🍫 🗙 Google	P •
Control delange delange Control delan	Google 8 -	🛩 Search 🗄 🖉 - 🕅 - 🏙 🧭 🚱 - 🔤 - 🧏 Eockmarks - 🖳 Find - 💝 Check -		🔦 🔹 🔵 flipdo •
VPILe > Attrickey IKE > Edit nt5gt 2	🚖 🔅 🔝 Juniper-ScreenOS Ad	dministration Tools (ns5gt)	🚹 • 🖻 ·	🖶 🔹 🔂 Page 🔹 🎯 Tools 🔹 🎽
Configuration New Configuration </th <th></th> <th>VPNs > AutoKey IKE > Edit</th> <th></th> <th>ns5gt ?</th>		VPNs > AutoKey IKE > Edit		ns5gt ?
	Autokey KE Autokey Autokey KE Autokey KE Autokey Autokey KE Autokey KE Autokey Autokey KE Autokey KE Autokey KE Autokey KE Autokey Autokey Autokey Autokey Autokey Autokey Autokey Autokey Autokey Autokey	VPNs > AutoKey KE > Edit VPN Name Test VPN Security Level OStandard OCompatible Basic OCustom Remote Gateway OPredefined Gateway Oreate a Simple Gateway Gateway Name Upe OStatic IP Add ODynamic IP Dialup User Dialup Group Local ID Coptional) Preshared Key Use As Seed Security Level OStandard Ocompatible OBasic Outgoing Interface Unitual V OK Cancel Advanced	at V dress/Hostname Peer ID User None V Group None V	nsēgt ?
	Toggle Manu			
internet T /	DOUR		Lø 🥣 Internet	-100-36-1 •

- 11. Choose the Security Level of **Custom**.
- 12. Under Remote Gateway, choose the option of Predefined, and select the gateway that was just setup. Click **Advanced** and fill in the following:
 - a. Phase 2 Proposal g2-esp-3des-sha
 - b. Enable Replay Protection
 - c. Enable Proxy-ID
 - i. Local IP/Netmask Local Subnet
 - ii. Remote IP/Netmask Remote Subnet

🖉 Juniper-ScreenOS Administra	tion Tools (ns5gt) - Windows Internet Explorer			
🚱 🗸 🔊 http://172.16.1.98/	Inswebui.html		Soogle	<u>- م</u>
Google 8 -	🚽 Search 🗄 💋 + 🔀 + 🏙 🙋 🕒 - 🔤 - 💈	🔹 🏠 Bookmarks • 🛛 🗔 Find • 🖑 Check •		🔦 🔹 🔵 flipdo •
🔆 🏟 🔝 Juniper-Screen OS Admir	ristration Tools (ns5at)		h • N -	🚔 🔹 🔂 Page 🔹 🎯 Tgols 🔹 🎇
	VPNs > AutoKey IKE > Edit		. — —	ns5gt ?
A Constant Sector 2 Adverses A Constant Sector 2 Adverses Active Sector 2 Adverses Adverses Active Sector 2 Adverses Adverses Active Sector 2 Adverses Adver	VPNs > AutoKey IKE > Edit Security Level Predefined User Defined User Defined Bind to Proxy-ID Local IP / Netmask Remote IP / Netmask Remote IP / Netmask Service VPN Group VPN Monitor Source Interface Destination IP Optimized	D Standard O Compatible O Basic O Custom Phase 2 Proposal g2esp-3des-sha V None D For L2TP-over-IPSec only ONone D Turnel Interface D Turnel Interface D Turnel 200 T122.16.0.0 / 15 T122.16.0.0 / 15 T122.16.0.0 / 24 ANY V V Tone V Idefault V 0.0.0.0	none V Unrust-Tun V weight 0	emi + 1 200 + 1 1000 + 1
	Rekey	,		
		Return Cancel		
Done			📑 😜 Interne	c 🔍 100% 🔹 🛒

- 13. Click Return.
- 14. Click **Ok**.
- 15. Navigate to **Policies.**
- 16. At the top of the page, under the **From** drop down box, select **Trust.** Under the **To** drop down box, select **Untrust**. Add the following:
 - a. Source Address Choose Address Book Entry and choose the local subnet that was previously setup from the drop down list.
 - b. Destination Address Choose **Address Book Entry** and choose the remote subnet that was previously setup from the drop down list.
 - c. Action Tunnel
 - d. Tunnel Choose your VPN from the list
 - e. Check the box for "Modify matching bidirectional VPN policy" to automatically setup the permissions for the opposite direction.

17. Click Ok.

18. Move the newly created policy under the "From Trust To Untrust" section above the policy that permits any traffic. If the VPN policy is below the 'any' rule, it will not pass traffic through the tunnel in that direction. You may need to move the same rule under the "From Untrust To Trust" section, also.

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.
- 4. The Juniper screenshots may not reflect your specific model of Juniper VPN appliance. You may need to adjust your settings to reflect newer Juniper firmware.

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>.