



# Digi Connect Port WAN VPN

## Configuration of a VPN tunnel between the Digi Connect Port WAN and a Checkpoint Firewall

### 1. Configuring the Digi Connect Port WAN VPN with firmware 2.6 and earlier

**VPN Settings**

**Identity**

Use the following as the identity:  
Identity string:

Use the Mobile IP address as the identity

**General Security Settings**

Connection Mode:

Diffie-Hellman:

Enable Perfect Forward Secrecy (PFS)

Enable Antireplay

**Internet Key Exchange (IKE) Security Settings**

Use the default policies to negotiate Internet Key Exchange (IKE) security settings

Use the following policies to negotiate Internet Key Exchange (IKE) security settings

Encryption	Authentication	SA Lifetime	
3-DES (192-bit)	SHA1	86400 secs	<a href="#">Remove</a>
<input type="text" value="DES (64-bit)"/>	<input type="text" value="MD5"/>	<input type="text" value="86400"/> secs	<input type="button" value="Add"/>

**VPN - Tunnel #1 - Configuration**

Description:

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:

**Security Settings**

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

Use the following policies to negotiate security settings --Highest priority listed last:

Encryption	Authentication	SA Lifetime	
3-DES	SHA1	86400 secs	<a href="#">Remove</a>
<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="text" value="28200"/> secs	<input type="button" value="Add"/>



## Configuration of a VPN tunnel between the Digi Connect Port WAN and a Checkpoint Firewall

### 2. Configuring the Digi Connect Port WAN VPN with firmware 2.7 and later

Virtual Private Network (VPN) Settings

VPN Global Settings

General Security Settings

Enable Antireplay

Miscellaneous Settings

Suppress SA lifetime during IKE phase 1

Suppress Delete Phase 1 SA Message For PFS

**VPN - Tunnel #1 - Configuration**

Description: Tunnel 1

Remote VPN Address: 62.189.60.194

VPN Tunnel: ISAKMP

Local Endpoint Type: Local endpoint is a subnet

**Identity**

Network Interface: mobile0

Negotiate tunnel as soon as interface comes up

Use the following as the identity: VPNUSER@DIGI.COM

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: 192.168.220.0

Subnet Mask: 255.255.255.0

**Remote Endpoint**

Tunnel Network Traffic to the following Remote Network:

IP Address: 172.16.192.0

Subnet Mask: 255.255.248.0

**Pre-Shared Key Settings**

Use the following IP address, FQDN, or username for the remote VPN's ID:

62.189.60.194

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

geheim1234



## Configuration of a VPN tunnel between the Digi Connect Port WAN and a Checkpoint Firewall

**ISAKMP Phase 1 Settings**

General Security Settings for Phase 1

Connection Mode:    
 Enable Perfect Forward Secrecy (PFS)

**NAT-T Settings**

Enable NAT Traversal (NAT-T)  
Keep Alive Interval:

**ISAKMP Phase 1 Policies**

Authentication	Encryption	Integrity	SA Lifetime	Diffie-Hellman	
Pre-Shared Key	3-DES (192-bit)	SHA1	86400 secs	Group 2	<input type="button" value="Remove"/>
<input type="text" value="Pre-Shared Key"/> <input type="button" value="v"/>	<input type="text" value="3-DES (192-bit)"/> <input type="button" value="v"/>	<input type="text" value="SHA1"/> <input type="button" value="v"/>	<input type="text" value="86400"/> secs	<input type="text" value="Group 2"/> <input type="button" value="v"/>	<input type="button" value="Add"/>

**ISAKMP Phase 2 Settings**

General Security Settings for Phase 2

Diffie-Hellman:

**ISAKMP Phase 2 Policies**

Use the following policies to negotiate security settings --Highest priority listed last:

Encryption	Authentication	SA Lifetime	
3-DES	SHA1	86400 secs	<input type="button" value="Remove"/>
<input type="text" value="3-DES"/> <input type="button" value="v"/>	<input type="text" value="SHA1"/> <input type="button" value="v"/>	<input type="text" value="86400"/> secs	<input type="button" value="Add"/>

### 3. Configuring the Checkpoint Firewall

Firstly define the remote network 'behind' the Digi unit:

Network Properties - WirelessLogic\_Test\_Network-192.168.220.0-24

General | NAT

Name:

Network Address:

Net Mask:

Comment:

Color:

Broadcast address:  
 Included  Not included

Define any specific hosts on the network as required.  
Add a New Externally Managed Checkpoint Gateway:



## Configuration of a VPN tunnel between the Digi Connect Port WAN and a Checkpoint Firewall

Externally Managed Check Point Gateway - WirelessLogic\_Test\_VPN

Externally Managed Check Point Gateway - General Properties

Name:

IP Address:

Comment:

Color:

Check Point Products

Version:

Type:

Firewall  
 VPN  
 QoS  
 SecureClient Policy Server  
 SecureClient Software Distribution Server  
 Management Station

Additional Products:

Web Server

Enter a name for the gateway and enter the Internet-facing IP address of the Digi unit. Under Topology, select the network you defined above:

Externally Managed Check Point Gateway - WirelessLogic\_Test\_VPN

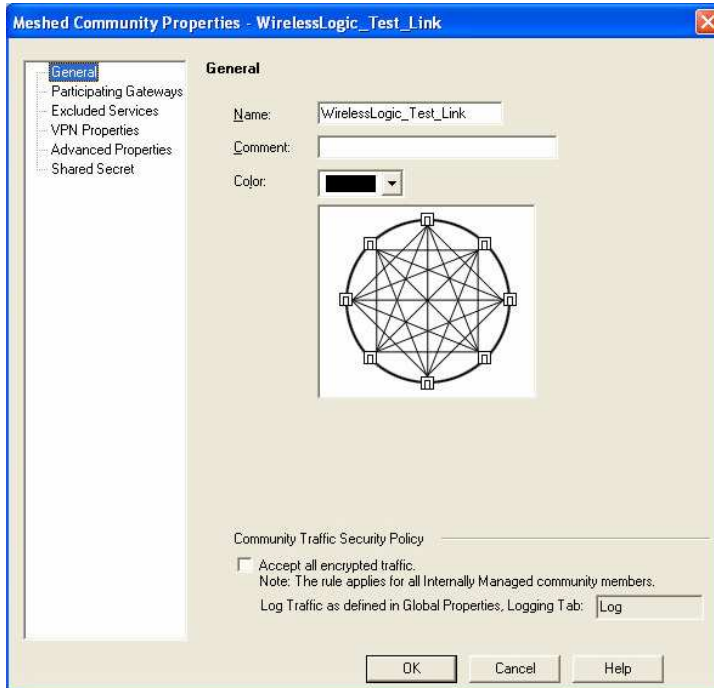
Topology

Name	IP Address	Network Mask	IP Addresses behind interface

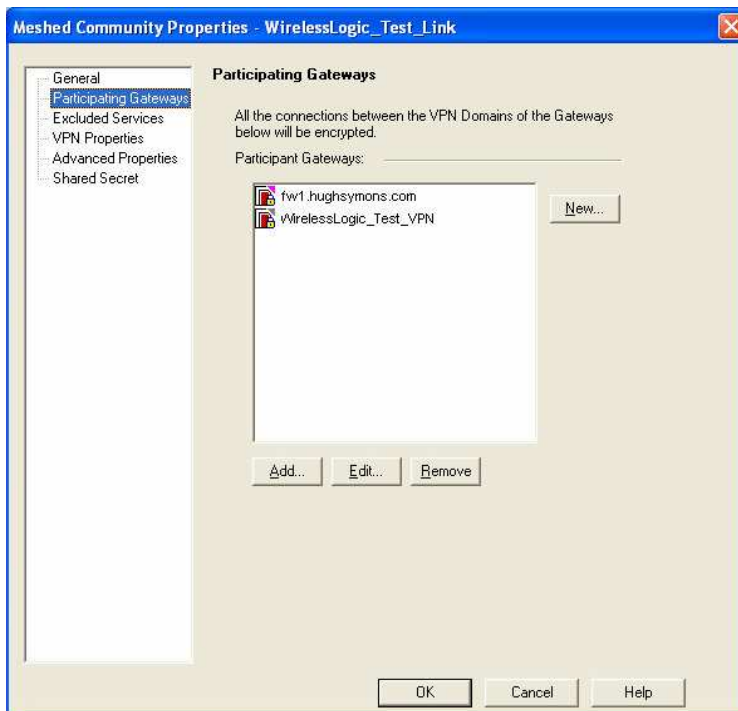
VPN Domain

All IP Addresses behind Gateway based on Topology information.  
 Manually defined

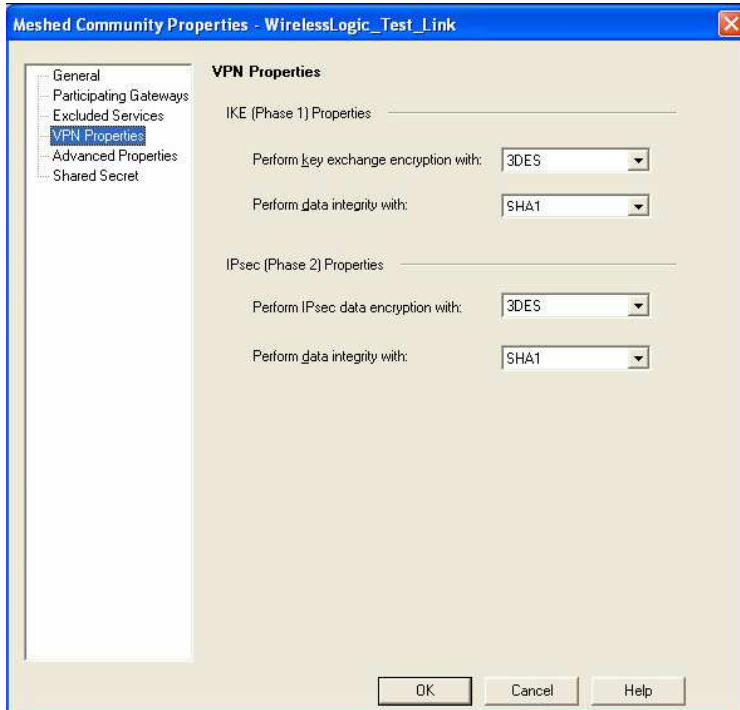
Configure a new Site-to-Site Meshed VPN:



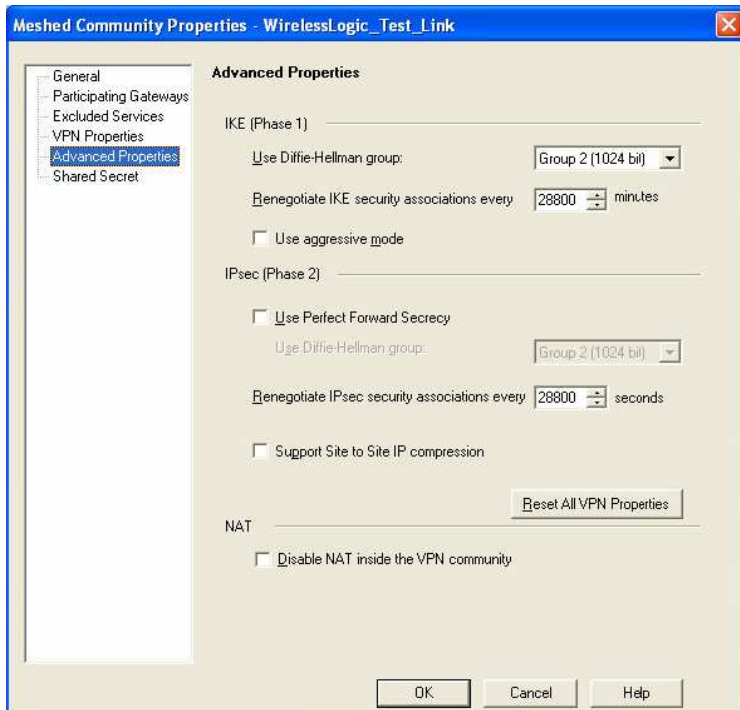
Add the gateway you defined above, as well as the Checkpoint gateway:



Configure the VPN properties as shown below:



Configure the Advanced VPN Properties as shown below:



Enter the same shared secret that you entered previously on the Digi unit. Now allow the required services on the firewall:



## Configuration of a VPN tunnel between the Digi Connect Port WAN and a Checkpoint Firewall

---

65	WirelessLogic_T1 James_PC-172	WirelessLogic_T1 WirelessLogic_T1	WirelessLogic_T1	TCP vWinVNC icmp-requests	accept	Log	fw1.hughsymon	Any
----	----------------------------------	--------------------------------------	------------------	------------------------------	--------	-----	---------------	-----