



Digi Wi-Point 3G Application Guide

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

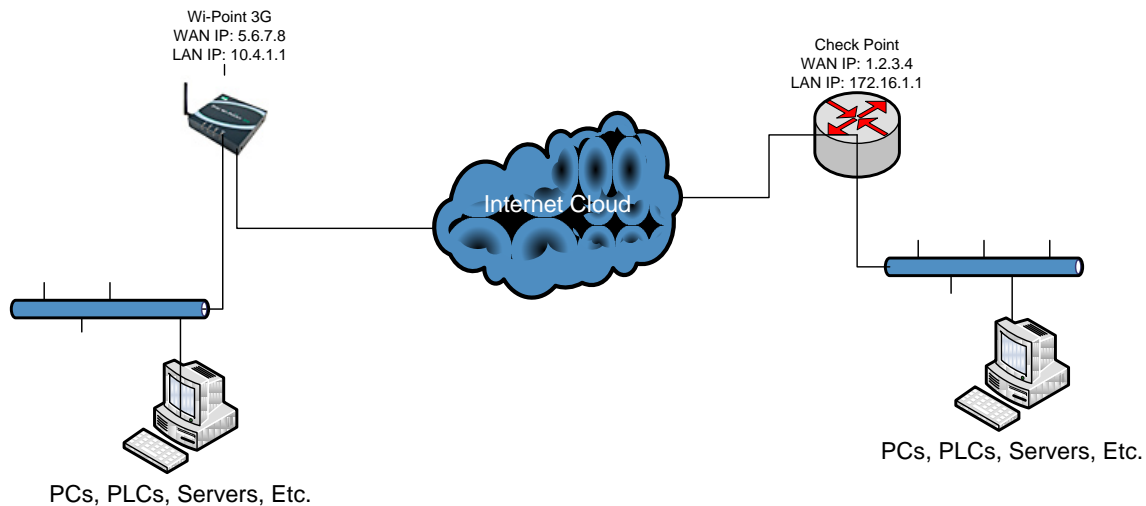
Scenario

Digi Wi-Point 3G is used for remote site connectivity. The primary site is using a Check Point VPN appliance for connectivity. 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 Check Point 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>.

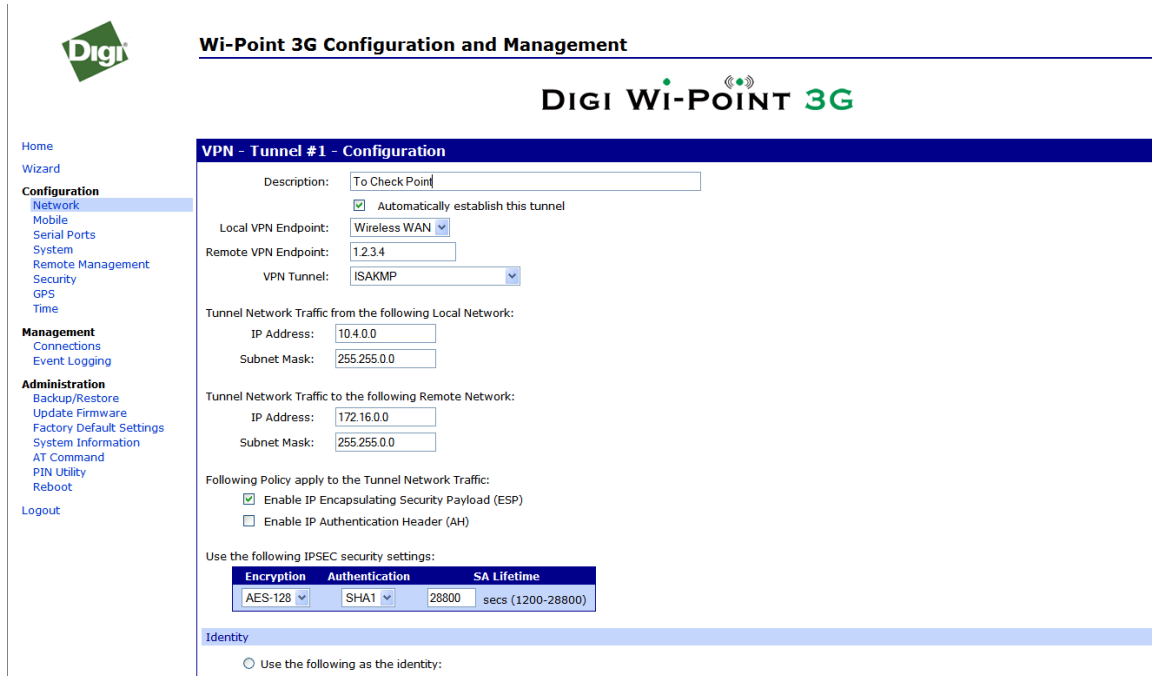
GSM GPRS/EDGE APN Type needed: VPN and GRE end-points usually require static (persistent) IP addresses and must support mobile terminated data connections. If mobile termination is not an option with your current APN, you will need to acquire a new one that does support mobile termination.

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. Navigate to Configuration > Network > VPN Settings
 - b. Click **VPN Tunnel Settings**
 - c. Click **Add**
 - d. Fill in the appropriate settings below



The screenshot displays the 'VPN - Tunnel #1 - Configuration' page in the Digi Wi-Point 3G web interface. The interface includes a navigation menu on the left and a main configuration area on the right. The configuration area is titled 'VPN - Tunnel #1 - Configuration' and contains the following fields and options:

- Description:** To Check Point
- Automatically establish this tunnel
- Local VPN Endpoint:** Wireless WAN
- Remote VPN Endpoint:** 1.2.3.4
- VPN Tunnel:** ISAKMP
- Tunnel Network Traffic from the following Local Network:**
 - IP Address:** 10.4.0.0
 - Subnet Mask:** 255.255.0.0
- Tunnel Network Traffic to the following Remote Network:**
 - IP Address:** 172.16.0.0
 - Subnet Mask:** 255.255.0.0
- 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
AES-128	SHA1	28800 secs (1200-28800)
- Identity:**
 - Use the following as the identity:

Wi-Point 3G Application Guide – Wi-Point 3G to Check Point

System Information
AT Command
PIN Utility
Reboot
Logout

Subject Mask: [XXXXXXXXXX]

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
AES-128	SHA1	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: Main

Diffie-Hellman: Group 2

Enable Perfect Forward Secrecy (PFS)

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

123456

Use the following policy to negotiate IKE security settings:

Authentication	Encryption	Integrity	SA Lifetime
Pre-Shared Key	AES (128-bit)	SHA1	86400 secs (1200-86400)

Apply

Copyright © 1996-2008 Digi International Inc. All rights reserved.
<http://www.digi.com/>

- e. Click **Apply** to save the changes
- f. A reboot is required for the settings to take effect. **Reboot** the unit.

Check Point VPN Configuration

1. Configure the Check Point VPN device
 - a. Log into the Web Interface of the Check Point device.
 - b. Navigate to **VPN** on the left hand panel.
 - c. Click the **VPN Sites** tab at the top of the page.
 - d. Click **New Site** to add the VPN tunnel.
 - e. Choose the options, shown in the following screenshots, that reflect **your** configuration:

VPN-1 Edge VPN Site Wizard

Welcome to the VPN Site Wizard

Using this Wizard, you can create a connection to a VPN (Virtual Private Network) site.
Select the type of site to establish:

- Remote Access VPN:**
Allow a user to establish remote access sessions to another network.
- Site-to-Site VPN:**
Establishes a permanent secure link between your network and a remote network.

To continue, click **Next**.

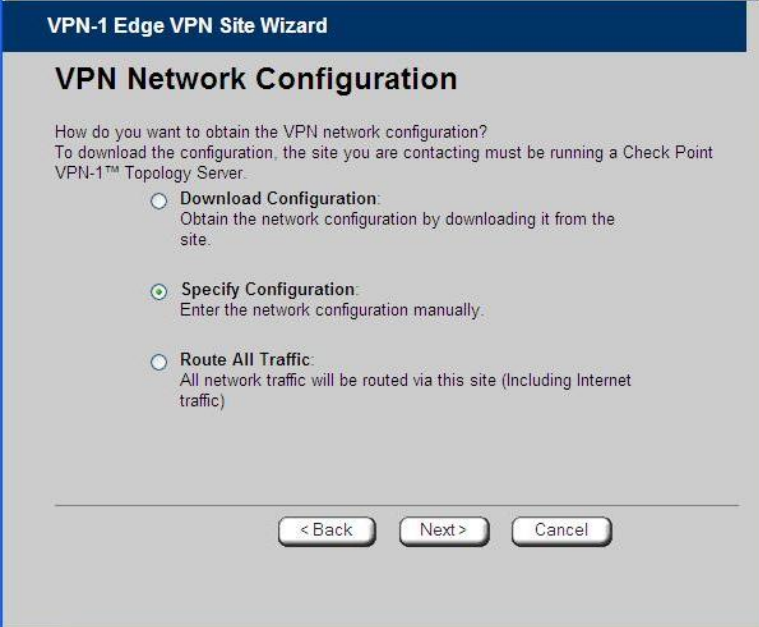
VPN-1 Edge VPN Site Wizard

VPN Gateway Address

Enter the IP address of the VPN gateway to which you want to connect.

VPN Gateway:

- Bypass NAT:**
Don't perform Network Address Translation (NAT) between this site and the internal network
- Bypass the firewall:**
Bypass the firewall between this site and the internal network



VPN-1 Edge VPN Site Wizard

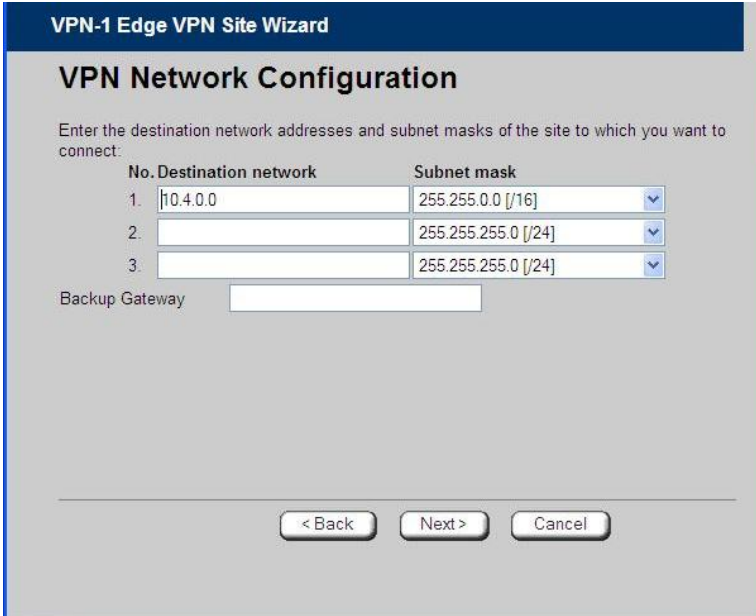
VPN Network Configuration

How do you want to obtain the VPN network configuration?
To download the configuration, the site you are contacting must be running a Check Point VPN-1™ Topology Server.

- Download Configuration:**
Obtain the network configuration by downloading it from the site.
- Specify Configuration:**
Enter the network configuration manually.
- Route All Traffic:**
All network traffic will be routed via this site (Including Internet traffic)

< Back Next > Cancel

NOTE: Your version of Check Point firmware may have additional options at this point in the setup. Newer firmware allows you to specify which type of authentication and encryption to use for Phase 1 and 2 settings. Older firmware will automatically detect what authentication and encryption to use.



VPN-1 Edge VPN Site Wizard

VPN Network Configuration

Enter the destination network addresses and subnet masks of the site to which you want to connect:

No.	Destination network	Subnet mask
1.	<input type="text" value="10.4.0.0"/>	<input type="text" value="255.255.0.0 [/16]"/>
2.	<input type="text"/>	<input type="text" value="255.255.255.0 [/24]"/>
3.	<input type="text"/>	<input type="text" value="255.255.255.0 [/24]"/>

Backup Gateway

< Back Next > Cancel

VPN-1 Edge VPN Site Wizard

Authentication Method

Select the authentication method used by this VPN site.

Shared Secret
 Certificate

< Back Next > Cancel

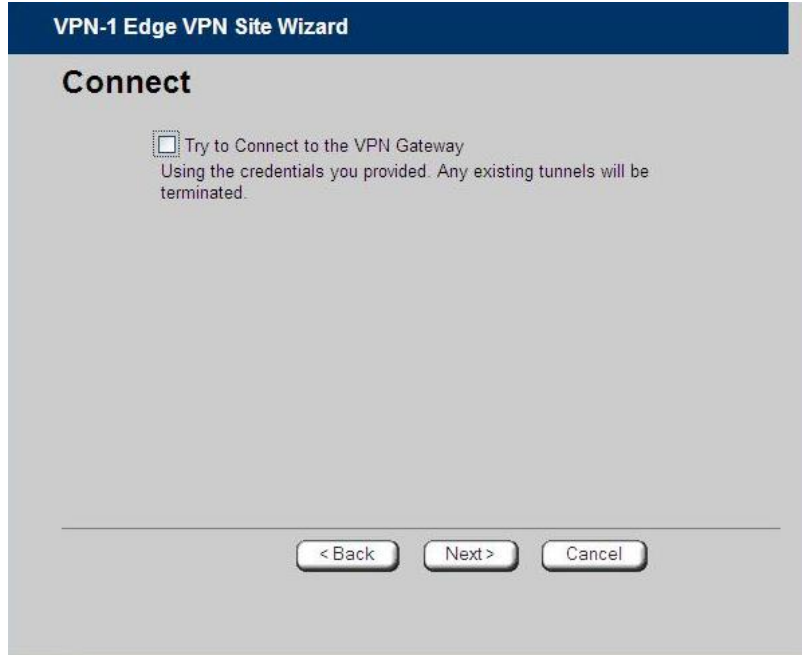
VPN-1 Edge VPN Site Wizard

Authentication

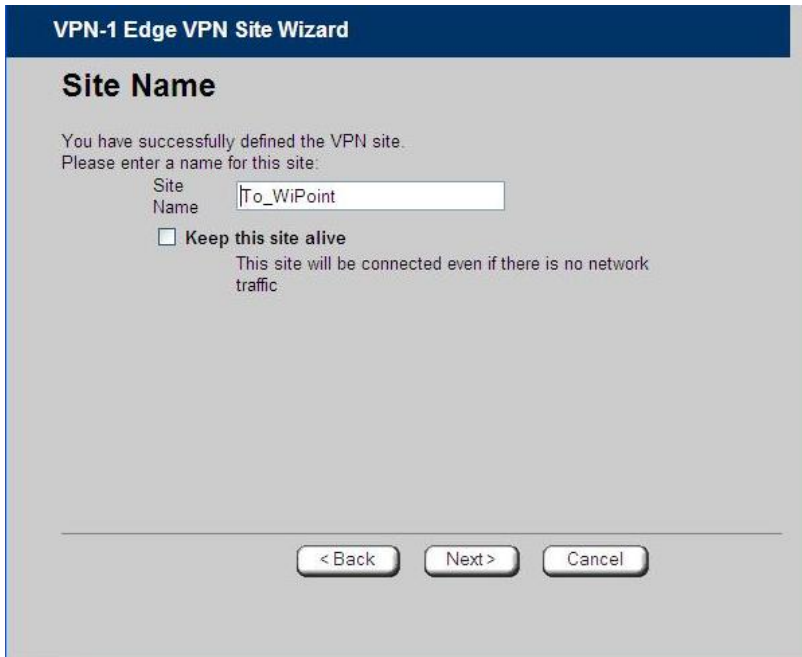
Please enter the credentials for the topology download:

Use Shared Secret

< Back Next > Cancel



The screenshot shows the 'Connect' step of the VPN-1 Edge VPN Site Wizard. The title bar reads 'VPN-1 Edge VPN Site Wizard'. Below the title, the word 'Connect' is displayed in a large, bold font. A checkbox is present with the text 'Try to Connect to the VPN Gateway Using the credentials you provided. Any existing tunnels will be terminated.' At the bottom of the screen, there are three buttons: '< Back', 'Next >', and 'Cancel'.



The screenshot shows the 'Site Name' step of the VPN-1 Edge VPN Site Wizard. The title bar reads 'VPN-1 Edge VPN Site Wizard'. Below the title, the word 'Site Name' is displayed in a large, bold font. The text reads: 'You have successfully defined the VPN site. Please enter a name for this site:'. Below this, there is a text input field labeled 'Site Name' containing the text 'To_WiPoint'. A checkbox is present with the text 'Keep this site alive' and a sub-note: 'This site will be connected even if there is no network traffic'. At the bottom of the screen, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- f. Click **Finish** to complete the VPN setup.

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 Connect router 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 Connect wireless pages at www.digi.com.