



# Quick Note 13

---

## **Configuring a main mode IPsec VPN between a Digi TransPort and a Netgear DG834G**

**UK Support**

November 2015

## Contents

1	Introduction .....	3
1.1	Outline.....	3
1.2	Assumptions.....	3
1.3	Version.....	3
1.4	Corrections.....	3
2	Configuration & scenario.....	4
3	Netgear configuration .....	5
4	TransPort router configuration .....	8
4.1	Configure IKE .....	8
4.2	Configure IPsec .....	9
4.3	Configure the pre-shared key.....	10
4.4	Save the configuration changes to profile 0 .....	11
5	Check and test the VPN .....	12

# 1 INTRODUCTION

## 1.1 Outline

This document contains configuration instructions for building a main mode IPsec VPN tunnel between a Digi TransPort router and a Netgear DG834G router.

## 1.2 Assumptions

This guide has been written for use by technically competent personnel, with a good understanding of the communications technologies used in the product and of the requirements for their specific application.

**Configuration:** This application note assumes that both routers will be connecting to an ADSL service and that both devices are set to their factory default configurations. Most configuration commands are only shown if they differ from the factory default.

This application note applies to:

**Models shown:** Digi Transport DR64

**Other Compatible Models:** All Digi TransPort routers that include IPsec encryption

**Firmware versions:** 5.123 and above

## 1.3 Version

Version	Status
1.0	Published
1.1	Rebranded and updated
2.0	Updated for new web GUI

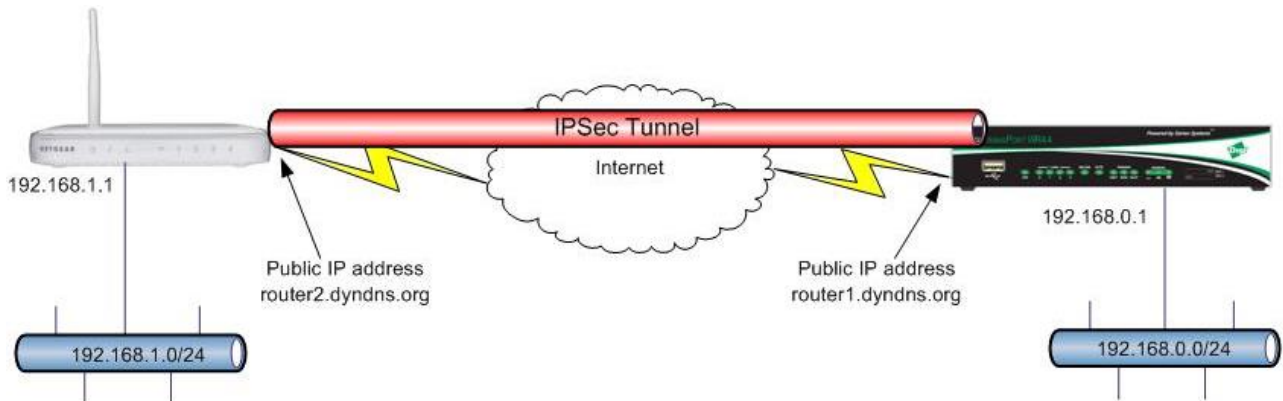
## 1.4 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: [Tech.Support@digicom](mailto:Tech.Support@digicom)

Requests for new application notes can be sent to the same address.

## 2 CONFIGURATION & SCENARIO

An IPsec VPN tunnel is set up to provide secure communications between the remote site Netgear router and the central TransPort router. The Netgear router must be running firmware version V5.01.09 or later.



Both routers have been configured with internet connectivity, they both use ADSL with a dynamic public IP address.

They both use the DynDNS service so that they can always be reached at the hostnames router1.dyndns.org and router2.dyndns.org.

Actual public IP addresses used for testing have been replaced with "xx.xx.xx.xx" where they appear in screenshots.

LAN segments are attached to Eth 0.

The IPsec tunnel will be established using main mode - aggressive mode connections are not accepted by the Netgear router.

### 3 NETGEAR CONFIGURATION

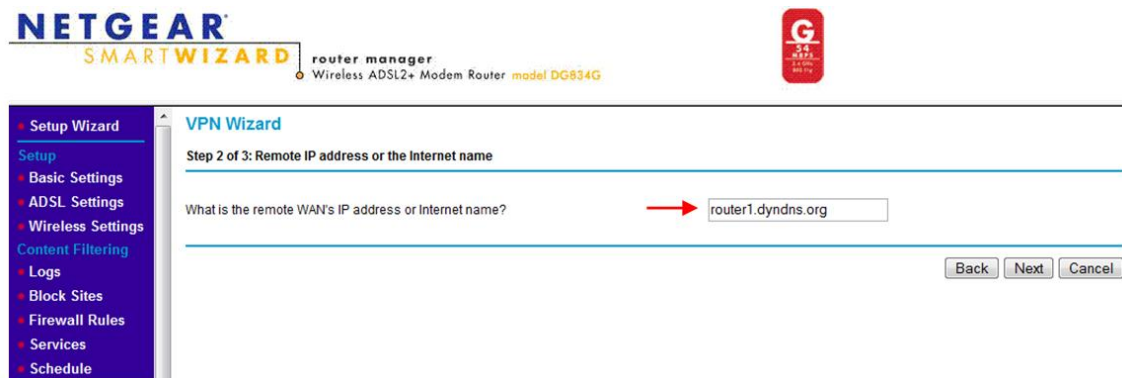
From the menu on the left, choose VPN Wizard, then click Next:

The screenshot shows the Netgear Smart Wizard router manager interface. The left sidebar contains a menu with categories: Setup Wizard, Setup, Content Filtering, Maintenance, Advanced, and Advanced - VPN. The 'VPN Wizard' option is highlighted under the 'Advanced - VPN' category. The main content area is titled 'VPN Wizard' and contains the following text: 'The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup.' and 'After creating the policies through the VPN Wizard, you can always update the parameters through the VPN setting links on the left menu.' A 'Next' button is located at the bottom right of the main content area.

Enter a descriptive name for the connection, the pre-shared key and select VPN Gateway, then click Next:

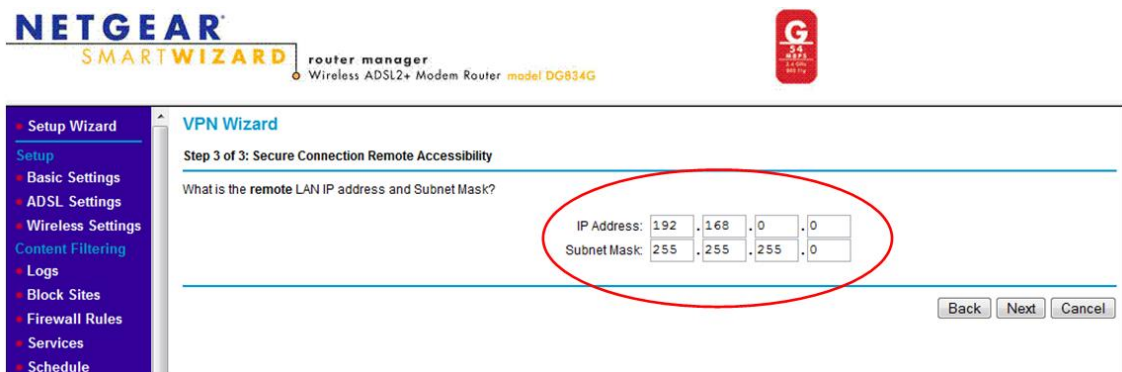
The screenshot shows the Netgear Smart Wizard router manager interface, specifically the 'VPN Wizard' section. The left sidebar is the same as in the previous screenshot. The main content area is titled 'VPN Wizard' and shows 'Step 1 of 3: Connection Name and Remote IP Type'. The form contains the following fields and options: 'What is the new Connection Name?' with a text box containing 'TransPort'; 'What is the pre-shared key?' with a text box containing 'mysharedkey123'; and 'This VPN tunnel will connect to:' with two radio button options: 'A remote VPN Gateway' (selected) and 'A remote VPN client (single PC)'. A red oval highlights the text boxes and the radio button options. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Enter the FQDN of the TransPort router, then click Next:



The screenshot shows the Netgear SmartWizard VPN Wizard interface. The left sidebar contains a menu with options: Setup Wizard, Setup, Basic Settings, ADSL Settings, Wireless Settings, Content Filtering, Logs, Block Sites, Firewall Rules, Services, and Schedule. The main panel is titled 'VPN Wizard' and 'Step 2 of 3: Remote IP address or the Internet name'. It asks 'What is the remote WAN's IP address or Internet name?'. A red arrow points to the input field containing 'router1.dyndns.org'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Enter the remote subnet details, then click Next:



The screenshot shows the Netgear SmartWizard VPN Wizard interface. The left sidebar is the same as in the previous step. The main panel is titled 'VPN Wizard' and 'Step 3 of 3: Secure Connection Remote Accessibility'. It asks 'What is the remote LAN IP address and Subnet Mask?'. A red oval highlights the input fields for IP Address (192, 168, 0, 0) and Subnet Mask (255, 255, 255, 0). At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Review the summary screen, then click Done:

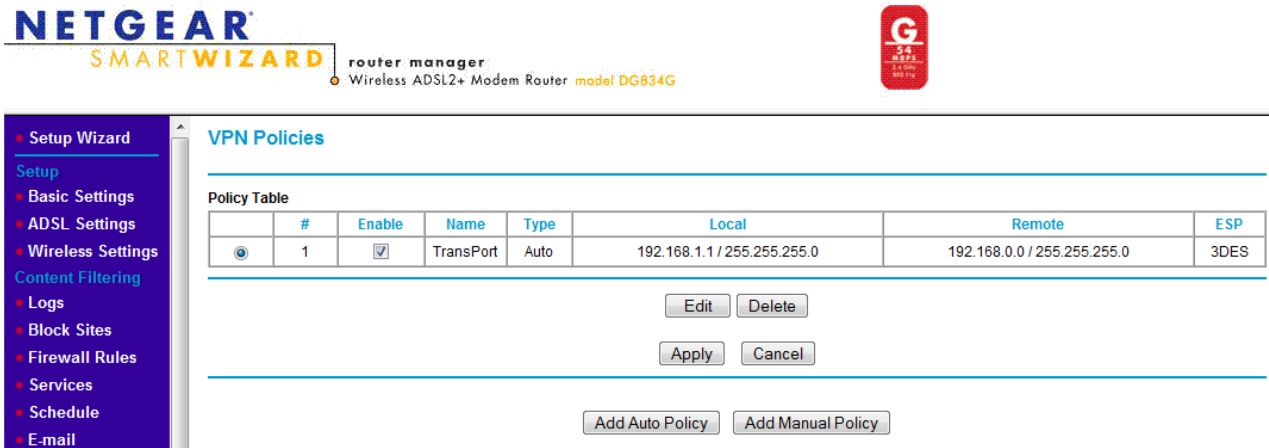


The screenshot shows the Netgear SmartWizard VPN Wizard interface. The left sidebar is the same as in the previous steps. The main panel is titled 'VPN Wizard' and 'Summary'. It says 'Please verify your inputs:'. The summary table is as follows:

Connection Name:	TransPort
Remote VPN Endpoint:	router1.dyndns.org
Remote Client Access:	By Subnet
Remote IP:	192.168.0.0 / 255.255.255.0
Remote ID:	
Local Client Access:	By subnet
Local IP:	192.168.1.1 / 255.255.255.0
Local ID:	

Below the table, it says 'You can click [here](#) to view the VPNC-recommended parameters. Please click "Done" to apply the changes.' At the bottom right are 'Back', 'Done', and 'Cancel' buttons.

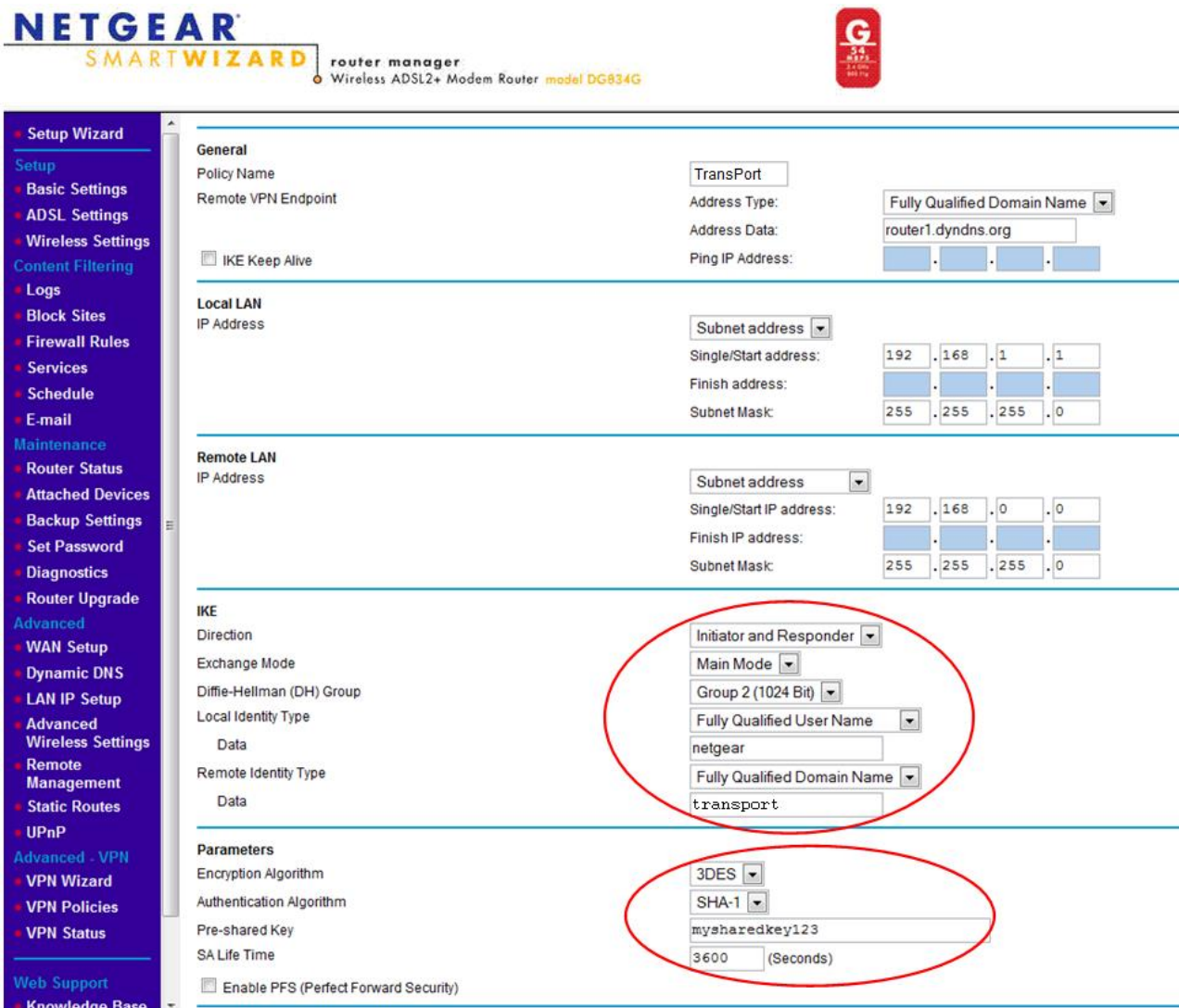
From the menu on the left, choose VPN Policies. The newly created policy is shown - click Edit:



The screenshot shows the Netgear SmartWizard router manager interface for a Wireless ADSL2+ Modem Router model DG834G. The left sidebar contains a menu with options: Setup Wizard, Setup, Basic Settings, ADSL Settings, Wireless Settings, Content Filtering, Logs, Block Sites, Firewall Rules, Services, Schedule, and E-mail. The main area is titled "VPN Policies" and displays a "Policy Table" with one policy. The policy has ID 1, is enabled, named "TransPort", and is of type "Auto". It shows local and remote IP ranges and uses 3DES encryption. Below the table are buttons for "Edit", "Delete", "Apply", and "Cancel". At the bottom, there are buttons for "Add Auto Policy" and "Add Manual Policy".

#	Enable	Name	Type	Local	Remote	ESP
1	<input checked="" type="checkbox"/>	TransPort	Auto	192.168.1.1 / 255.255.255.0	192.168.0.0 / 255.255.255.0	3DES

Review the configuration, change the IKE and Parameters sections as shown below, then click Apply:



The screenshot shows the Netgear SmartWizard router manager interface for a Wireless ADSL2+ Modem Router model DG834G. The left sidebar contains a menu with options: Setup Wizard, Setup, Basic Settings, ADSL Settings, Wireless Settings, Content Filtering, Logs, Block Sites, Firewall Rules, Services, Schedule, E-mail, Maintenance, Router Status, Attached Devices, Backup Settings, Set Password, Diagnostics, Router Upgrade, Advanced, WAN Setup, Dynamic DNS, LAN IP Setup, Advanced Wireless Settings, Remote Management, Static Routes, UPnP, Advanced - VPN, VPN Wizard, VPN Policies, and VPN Status. The main area is titled "VPN Policies" and displays the configuration for the "TransPort" policy. The "General" section shows the policy name, remote VPN endpoint, and IKE Keep Alive checkbox. The "Local LAN" section shows the IP address and subnet mask. The "Remote LAN" section shows the IP address and subnet mask. The "IKE" section shows the direction, exchange mode, Diffie-Hellman (DH) group, local identity type, and remote identity type. The "Parameters" section shows the encryption algorithm, authentication algorithm, pre-shared key, and SA life time. The "Advanced - VPN" section shows the VPN Wizard, VPN Policies, and VPN Status. The "Web Support" section shows the Knowledge Base. The "IKE" and "Parameters" sections are circled in red.

**General**

Policy Name: TransPort

Remote VPN Endpoint: Address Type: Fully Qualified Domain Name, Address Data: router1.dyndns.org, Ping IP Address: . . .

☐ IKE Keep Alive

**Local LAN**

IP Address: Subnet address, Single/Start address: 192.168.1.1, Finish address: . . ., Subnet Mask: 255.255.255.0

**Remote LAN**

IP Address: Subnet address, Single/Start IP address: 192.168.0.0, Finish IP address: . . ., Subnet Mask: 255.255.255.0

**IKE**

Direction: Initiator and Responder

Exchange Mode: Main Mode

Diffie-Hellman (DH) Group: Group 2 (1024 Bit)

Local Identity Type: Fully Qualified User Name: netgear, Fully Qualified Domain Name: transport

**Parameters**

Encryption Algorithm: 3DES

Authentication Algorithm: SHA-1

Pre-shared Key: mysharedkey123

SA Life Time: 3600 (Seconds)

☐ Enable PFS (Perfect Forward Security)

## 4 TRANSPORT ROUTER CONFIGURATION

### 4.1 Configure IKE

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0

Configure as follows:

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE > IKE 0

▼ IKE 0

Use the following settings for negotiation

Encryption: ☐ None ☐ DES ☒ 3DES ☐ AES (128 bit) ☐ AES (192 bit) ☐ AES (256 bit)

Authentication: ☐ None ☐ MD5 ☒ SHA1

Mode: ☒ Main ☐ Aggressive

MODP Group for Phase 1: 2 (1024) ▼

MODP Group for Phase 2: No PFS ▼

Renegotiate after 0 hrs 20 mins 0 secs

▼ Advanced

Retransmit a frame if no response after 10 seconds

Stop IKE negotiation after 2 retransmissions

Stop IKE negotiation if no packet received for 30 seconds

☒ Enable Dead Peer Detection

☒ Enable NAT-Traversal

☒ Send INITIAL-CONTACT notifications

☐ Retain phase 1 SA after failed phase 2 negotiation

RSA private key file:

SA Removal Mode: Normal ▼

☐ Delete SAs when invalid SPI notifications are received

Apply



## 4.2 Configure IPsec

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0

Configure as follows:

**Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0 - 9 > IPsec 0**

**IPsec 0**

Description:

The IP address or hostname of the remote unit

Use  as a backup unit

Local LAN	Remote LAN
<input checked="" type="radio"/> Use these settings for the local LAN	<input checked="" type="radio"/> Use these settings for the remote LAN
IP Address: <input type="text" value="192.168.0.0"/>	IP Address: <input type="text" value="192.168.1.0"/>
Mask: <input type="text" value="255.255.255.0"/>	Mask: <input type="text" value="255.255.255.0"/>
<input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/>	<input type="radio"/> Remote Subnet ID: <input type="text"/>

Use the following security on this tunnel

☐ Off ☒ Preshared Keys ☐ XAUTH Init Preshared Keys ☐ RSA Signatures ☐ XAUTH Init RSA

Our ID:

Our ID type: ☒ IKE ID ☐ FQDN ☐ User FQDN ☐ IPv4 Address

Remote ID:

Use  encryption on this tunnel

Use  authentication on this tunnel

Use Diffie Hellman group

Use IKE  to negotiate this tunnel

Use IKE configuration:

Bring this tunnel up

☐ All the time

☒ Whenever a route to the destination is available

☐ On demand

If the tunnel is down and a packet is ready to be sent

Bring this tunnel down if it is idle for  hrs  mins  secs

Renew the tunnel after

hrs  mins  secs

KBytes of traffic

**Tunnel Negotiation**

**Advanced**

## 4.3 Configure the pre-shared key

### Configuration - Security > Users > User 20 - 29 > User 29

Enter \* for the username and use the same pre-shared key as configured on the Netgear router.

Using \* as the username creates a wildcard entry, so this MUST be the last user in the TransPort router's configuration – in this example it is User 29:

**Configuration - Security > Users > User 20 - 29 > User 29**

- System
  - Users
    - User 0 - 9
    - User 10 - 19
    - User 20 - 29
      - User 20
      - User 21
      - User 22
      - User 23
      - User 24
      - User 25
      - User 26
      - User 27
      - User 28
      - User 29 - \*

Username: \*

Password: ••••••

Confirm Password: ••••••

Access Level: None

Advanced

Apply

## 4.4 Save the configuration changes to profile 0

### Administration - Save configuration

**Administration - Save configuration**

Save current configuration to Config 0 (power up) ▼

Save all configuration. This includes the following

- Save the current configuration to config 0
- Save the current firewall
- Save all registers on all ports to profile 0
- Save all PAD parameters on all PADs to profile 0

## 5 CHECK AND TEST THE VPN

On the TransPort router, browse to: **Management - Connections > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec Tunnels 0 - 9 > IPsec Tunnels 0 - 9**

The SAs will be shown:

▼ IPsec Tunnels 0 - 9

Outbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface
0	xx.xx.xx.xx	192.168.0.0/24	192.168.1.0/24	N/A	SHA1	3DES	N/A	0	0	3120	PPP 1
<div>Remove All</div>											

Inbound V1 SAs

#	Peer IP Addr	Local Network	Remote Network	AH	ESP Auth	ESP Enc	IP Comp	KBytes Delivered	KBytes Left	Time Left (secs)	Interface
0	xx.xx.xx.xx	192.168.0.0/24	192.168.1.0/24	N/A	SHA1	3DES	N/A	0	0	3120	PPP 1
<div>Remove All</div>											

Browse to: **Administration - Execute a command** then enter a ping command to ping a device on the remote (Netgear) subnet.

Be sure to use the argument `-e0` (or `-e1`, `-e2` etc.) to specify the Ethernet source port so that the ping traverses the VPN tunnel. For example, if the LAN subnet is configured on Eth 0 then use `-e0`.

Enter the command then click Execute:

**Administration - Execute a command**

Command:

The ping results are shown a moment later:

```
Command: ping 192.168.1.1 -e0
Command result

Pinging Addr [192.168.1.1]

sent PING # 1
PING receipt # 1 : response time 0.06 seconds
Iface: PPP 1
Ping Statistics
Sent      : 1
Received  : 1
Success   : 100 %
Average RTT : 0.06 seconds

OK
```

On the Netgear router, from the menu on the left choose VPN Status. Scroll to the bottom of the log and look for “IPsec SA established”. Click on the VPN Status button and the tunnel show as connected:

**NETGEAR SMARTWIZARD** router manager  
Wireless ADSL2+ Modem Router model DG834G

**VPN Status/Log**

```

Sun, 2002-09-08 12:01:30 - added connection description "TransPort"
Sun, 2002-09-08 12:01:30 - adding interface ipsec0/ppp0 xx.xx.xx.xx
Mon, 2012-09-03 10:32:33 - [TransPort] initiating Main Mode
Mon, 2012-09-03 10:32:34 - [TransPort] ISAKMP SA established
Mon, 2012-09-03 10:32:34 - [TransPort] sent QI2, IPsec SA established
  
```

Refresh Clear Log VPN Status

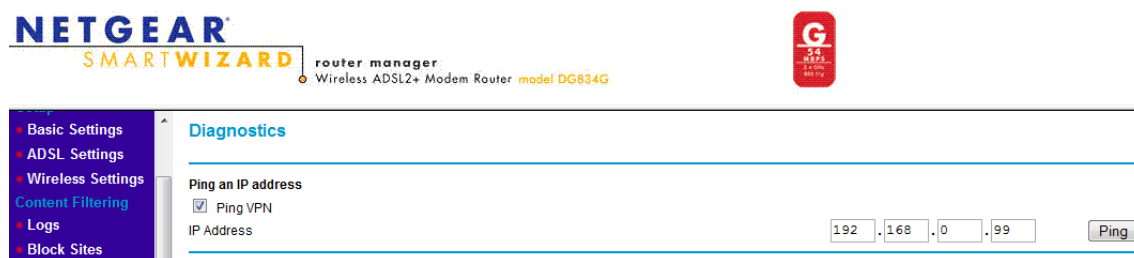
**Current VPN Tunnels (SAs) - Mozilla Firefox**  
192.168.1.1/setup.cgi?next\_file=vpn\_sta.htm

**Current VPN Tunnels (SAs)**

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	a29ea7fe	15c8fefd	TransPort	xx.xx.xx.xx	Drop	2883	2883

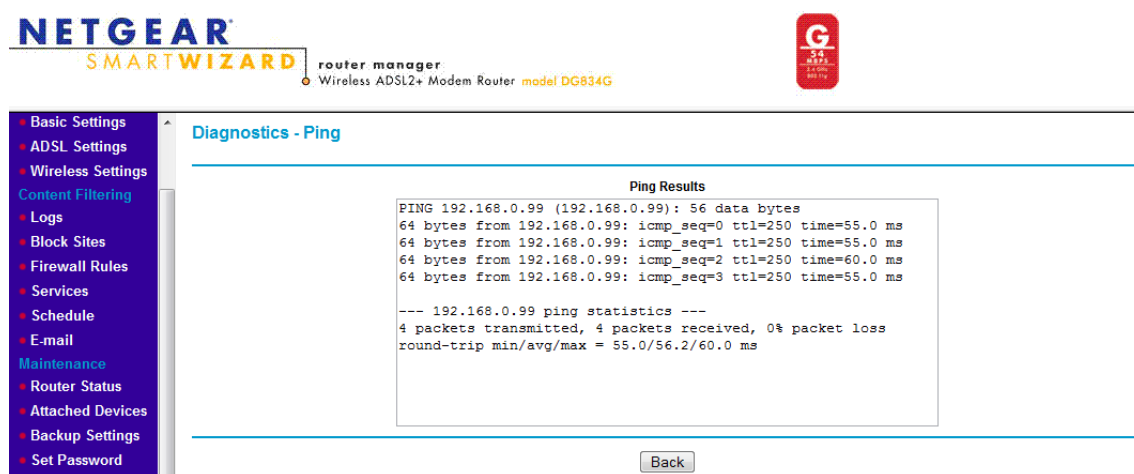
Waiting for 192.168.1.1...

From the menu on the left choose Diagnostics, enter the IP address of a device on the remote LAN, tick “Ping VPN” then click Ping:



The screenshot shows the Netgear Smart Wizard router manager interface. The left sidebar contains a menu with options: Basic Settings, ADSL Settings, Wireless Settings, Content Filtering, Logs, and Block Sites. The main area is titled "Diagnostics". Under "Ping an IP address", the "Ping VPN" checkbox is checked. The "IP Address" field is populated with "192.168.0.99". A "Ping" button is located to the right of the IP address field.

The results will be shown a couple of seconds later:



The screenshot shows the Netgear Smart Wizard router manager interface with the "Diagnostics - Ping" page. The left sidebar menu is the same as in the previous screenshot. The main area displays the "Ping Results" for the IP address 192.168.0.99. The results show four successful ping attempts with 0% packet loss. A "Back" button is located at the bottom of the results area.

```
Ping Results
PING 192.168.0.99 (192.168.0.99): 56 data bytes
64 bytes from 192.168.0.99: icmp_seq=0 ttl=250 time=55.0 ms
64 bytes from 192.168.0.99: icmp_seq=1 ttl=250 time=55.0 ms
64 bytes from 192.168.0.99: icmp_seq=2 ttl=250 time=60.0 ms
64 bytes from 192.168.0.99: icmp_seq=3 ttl=250 time=55.0 ms

--- 192.168.0.99 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 55.0/56.2/60.0 ms
```