Quick Note 13

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

UK Support

November 2015

Contents

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

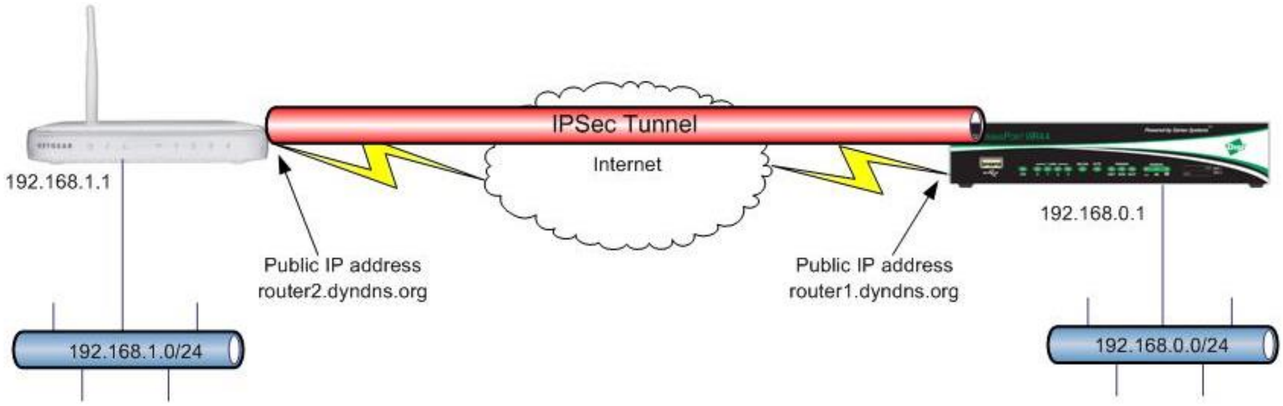
1.4 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: Tech.Support@digi.com

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.

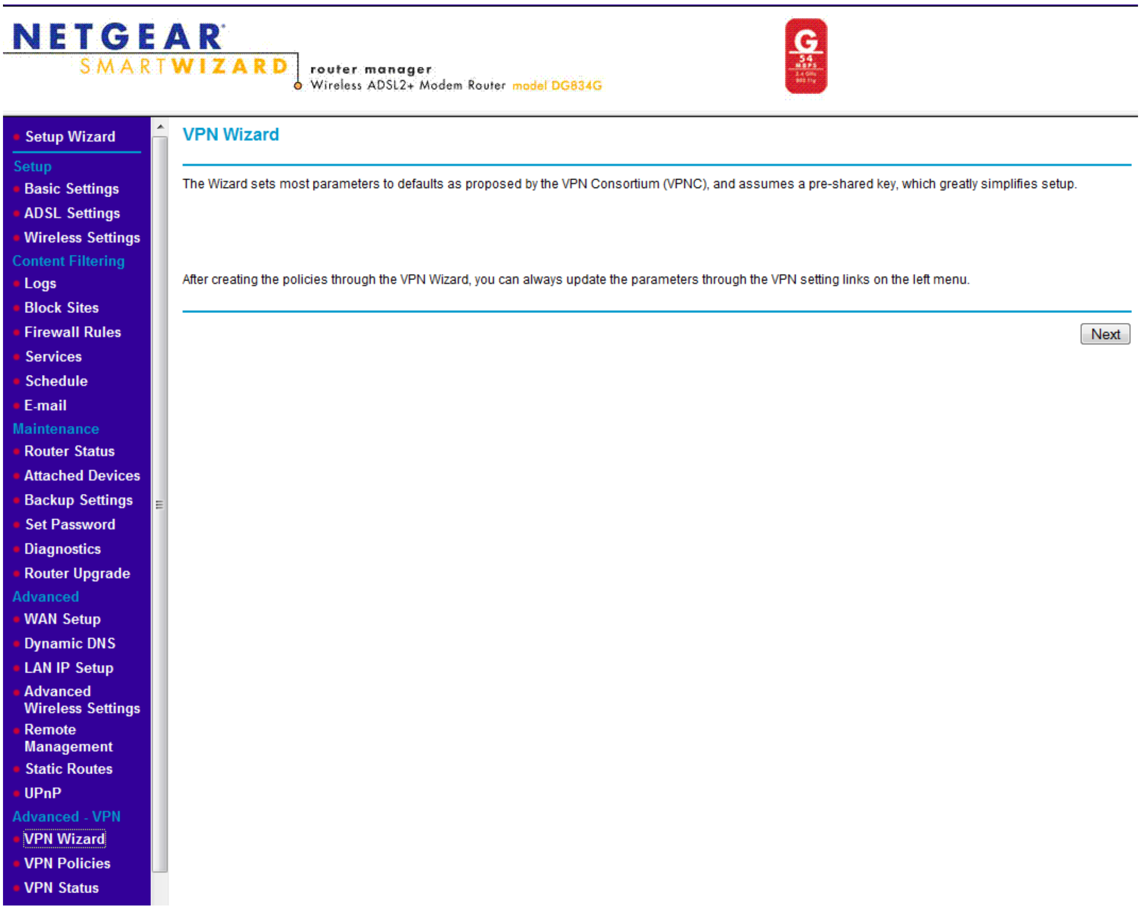
Actual public IP addresses used for testing have been replaced with “xx.xx.xx.xx” where they appear in screenshots.

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:

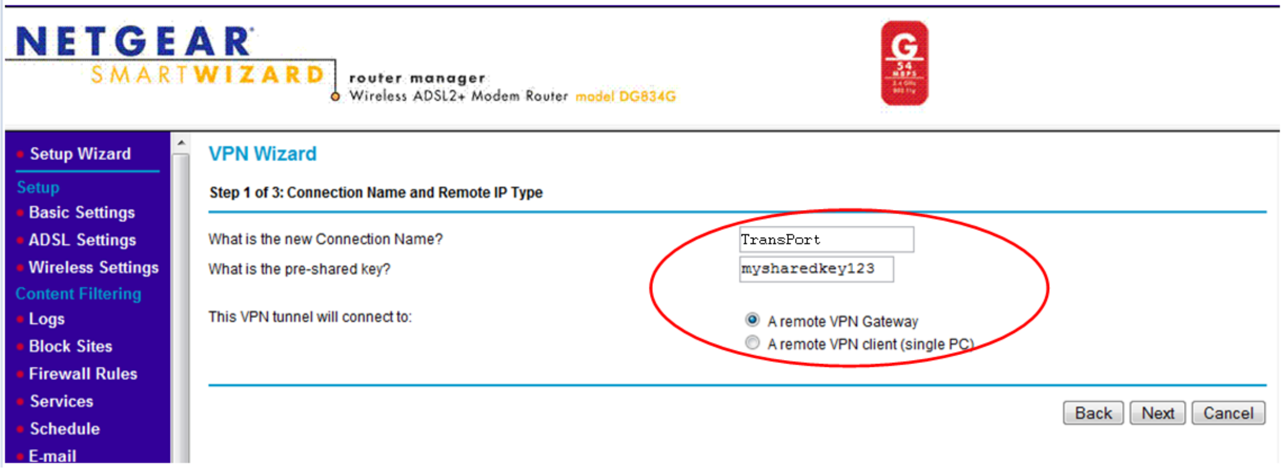


VPN Wizard

The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup.

After creating the policies through the VPN Wizard, you can always update the parameters through the VPN setting links on the left menu.

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



VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

What is the new Connection Name? TransPort

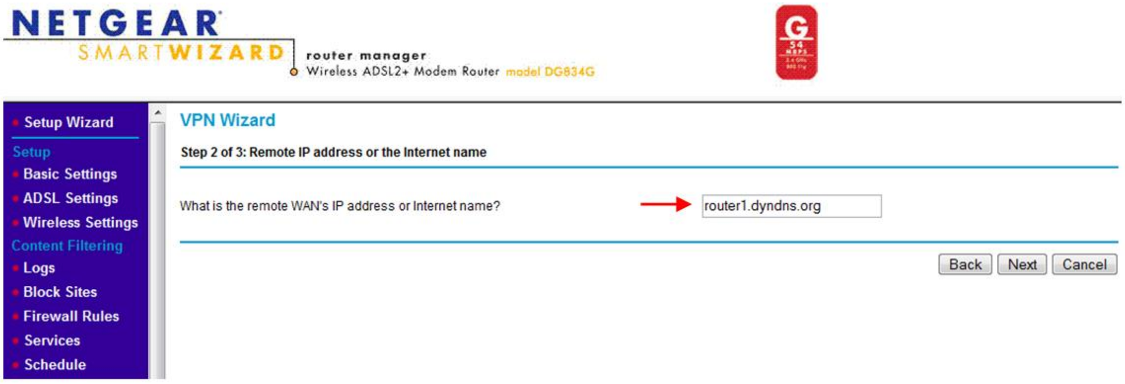
What is the pre-shared key? mysharedkey123

This VPN tunnel will connect to:

● A remote VPN Gateway

○ A remote VPN client (single PC)

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

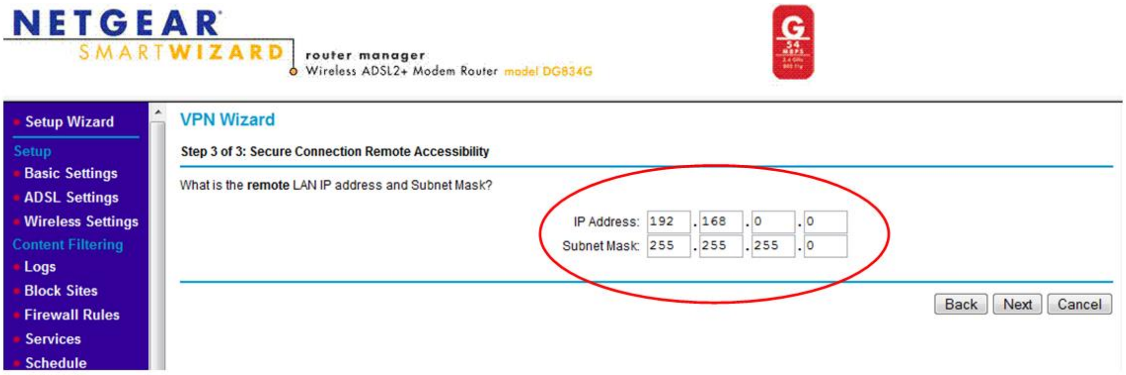


VPN Wizard

Step 2 of 3: Remote IP address or the Internet name

What is the remote WAN's IP address or Internet name? router1.dyndns.org

Enter the remote subnet details, then click Next:



VPN Wizard

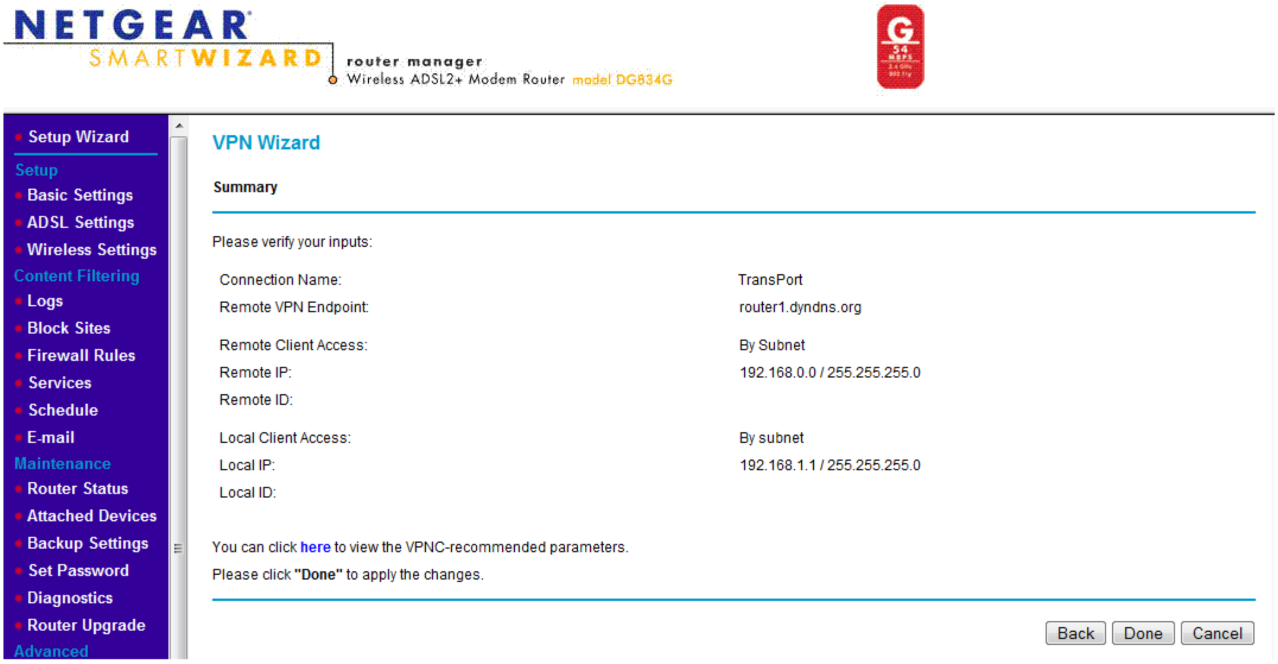
Step 3 of 3: Secure Connection Remote Accessibility

What is the **remote** LAN IP address and Subnet Mask?

IP Address: 192 . 168 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Review the summary screen, then click Done:



VPN Wizard

Summary

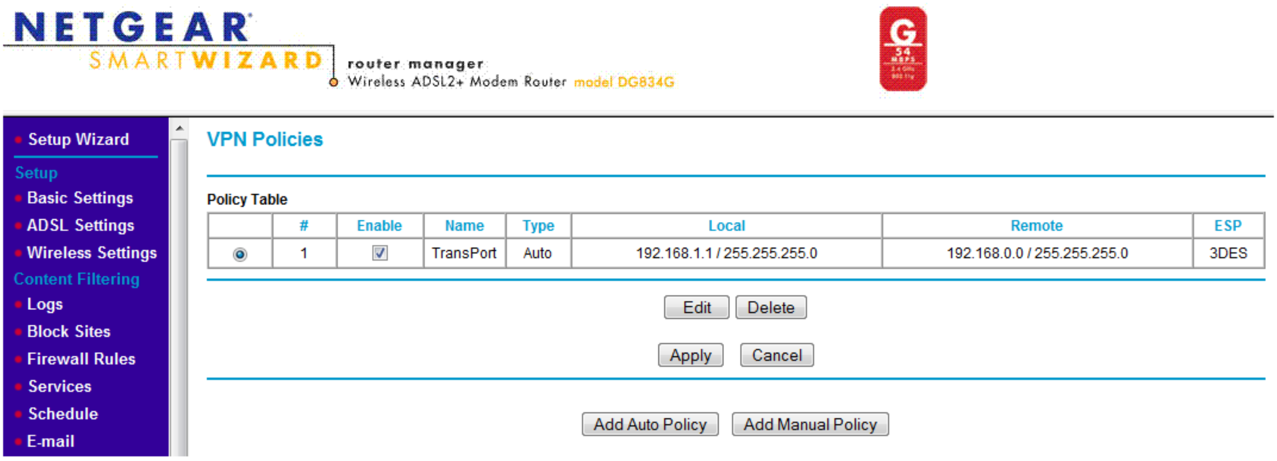
Please verify your inputs:

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:	

You can click here to view the VPNC-recommended parameters.

Please click **"Done"** to apply the changes.

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

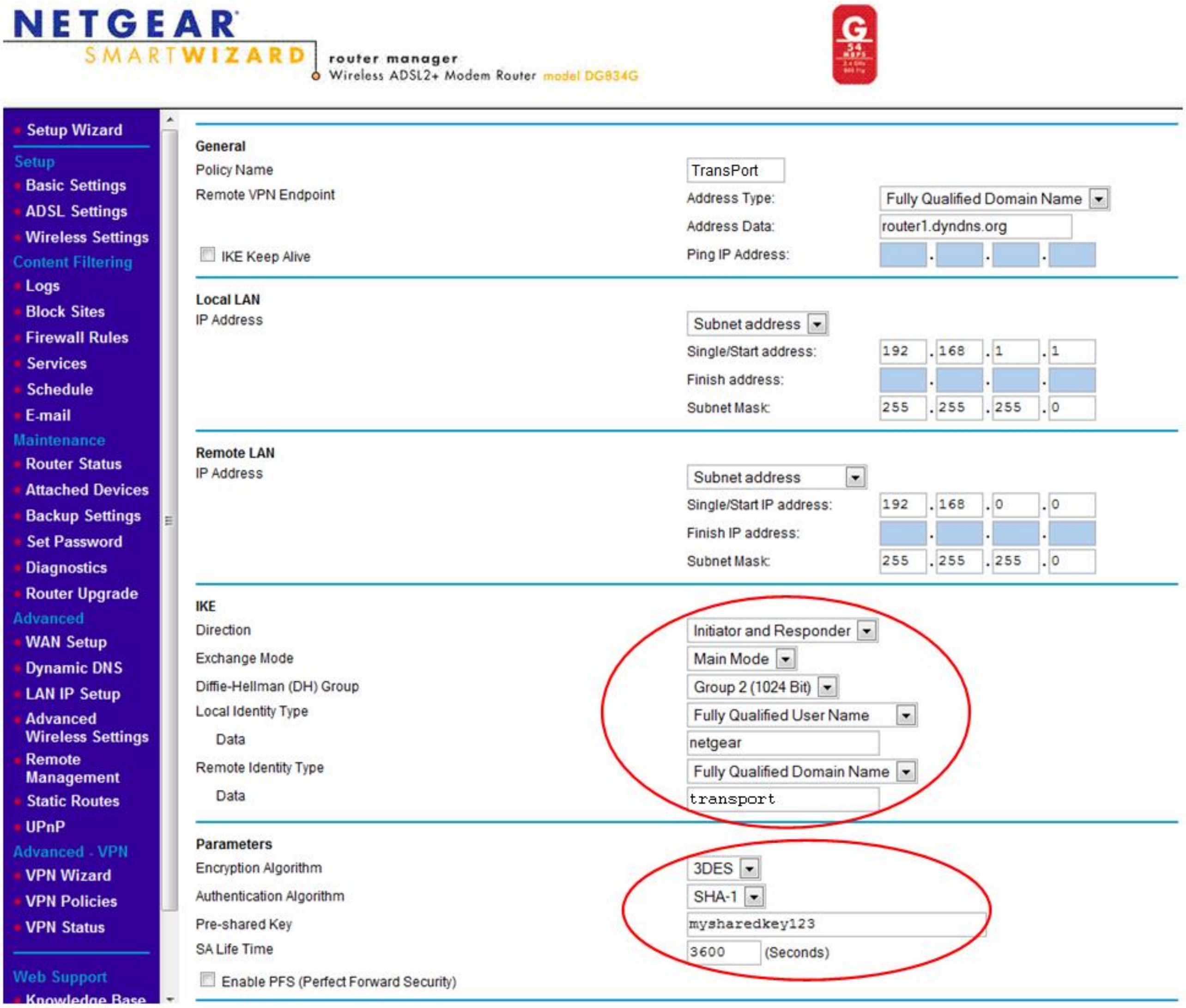


VPN Policies

Policy Table

	#	Enable	Name	Type	Local	Remote	ESP
●	1	☑	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:



General

Policy Name: TransPort

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

□ IKE Keep Alive
Ping IP Address: . . .

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
Data: netgear
Remote Identity Type: Fully Qualified Domain Name
Data: transport

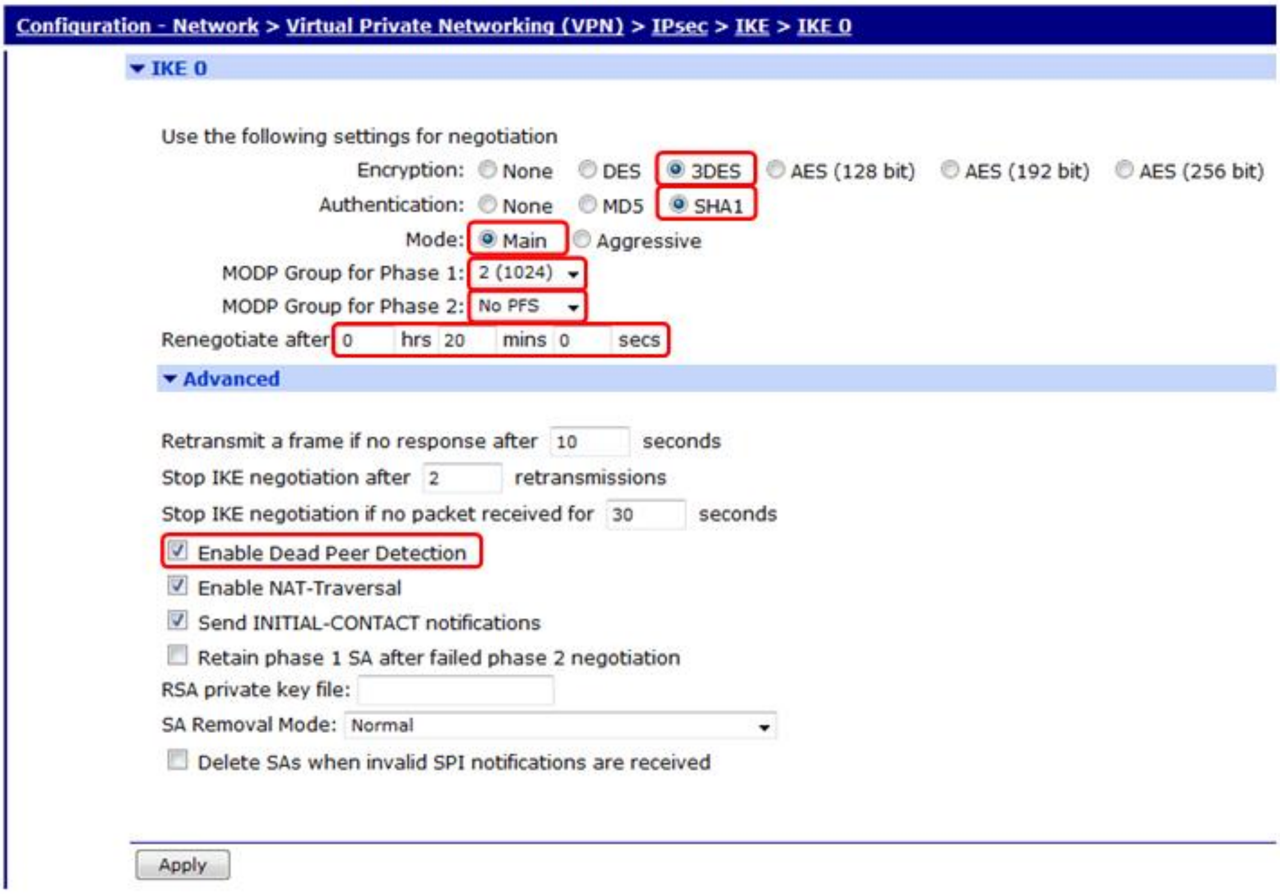
Parameters
Encryption Algorithm: 3DES
Authentication Algorithm: SHA-1
Pre-shared Key: mysharedkey123
SA Life Time: 3600 (Seconds)
□ Enable PFS (Perfect Forward Security)

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:

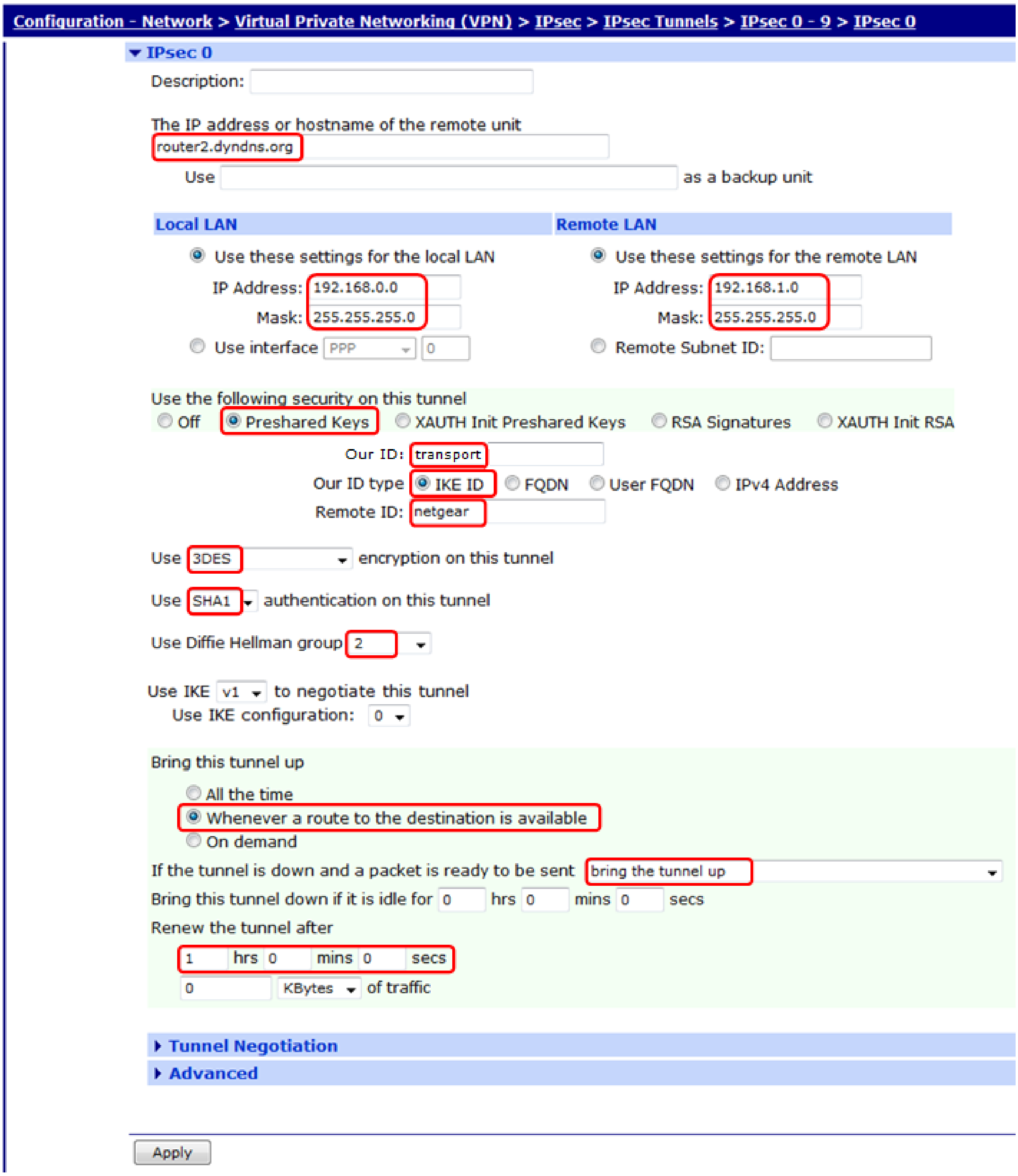
SA Removal Mode: Normal

☐ Delete SAs when invalid SPI notifications are received

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: router2.dyndns.org

Use as a backup unit

Local LAN	Remote LAN
● Use these settings for the local LAN	● Use these settings for the remote LAN
IP Address: 192.168.0.0	IP Address: 192.168.1.0
Mask: 255.255.255.0	Mask: 255.255.255.0
○ Use interface PPP 0	○ Remote Subnet ID:

Use the following security on this tunnel

○ Off ● Preshared Keys ○ XAUTH Init Preshared Keys ○ RSA Signatures ○ XAUTH Init RSA

Our ID: transport

Our ID type ● IKE ID ○ FQDN ○ User FQDN ○ IPv4 Address

Remote ID: netgear

Use 3DES encryption on this tunnel

Use SHA1 authentication on this tunnel

Use Diffie Hellman group 2

Use IKE v1 to negotiate this tunnel

Use IKE configuration: 0

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 the tunnel up

Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs

Renew the tunnel after

1 hrs 0 mins 0 secs

0 KBytes of traffic

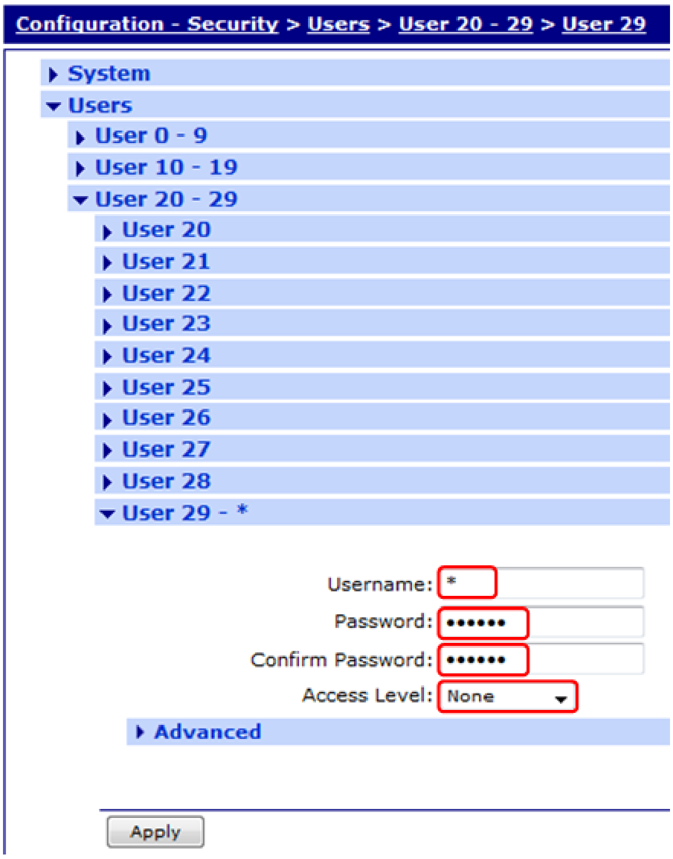
▸ Tunnel Negotiation

▸ 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:



Username: *

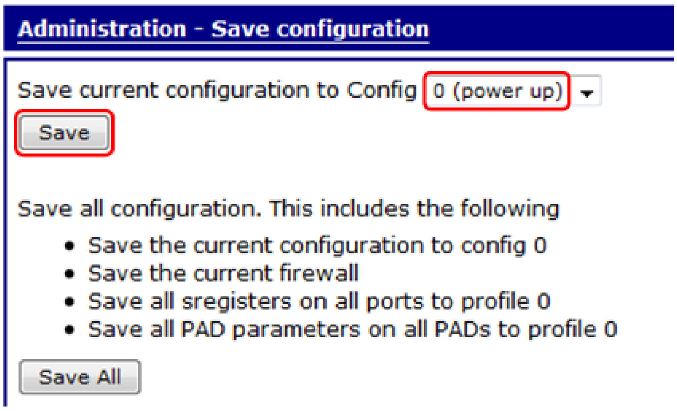
Password: ••••••

Confirm Password: ••••••

Access Level: None

4.4 Save the configuration changes to profile 0

Administration - Save configuration



Administration - Save configuration

Save current configuration to Config 0 (power up)

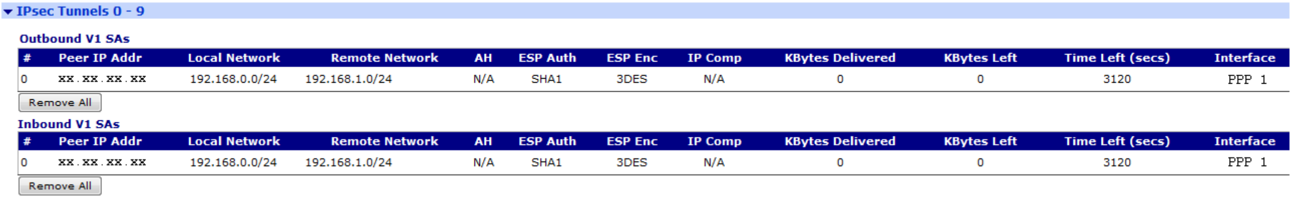
Save all configuration. This includes the following

- Save the current configuration to config 0
- Save the current firewall
- Save all sregisters 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

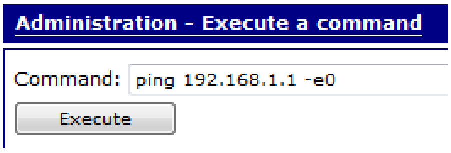
Inbound V1 SAs

#	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

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.

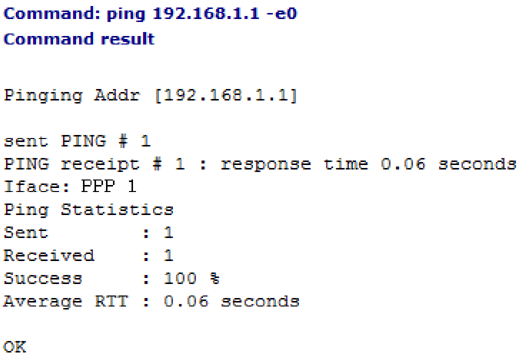
Enter the command then click Execute:



Administration - Execute a command

Command: ping 192.168.1.1 -e0

The ping results are shown a moment later:



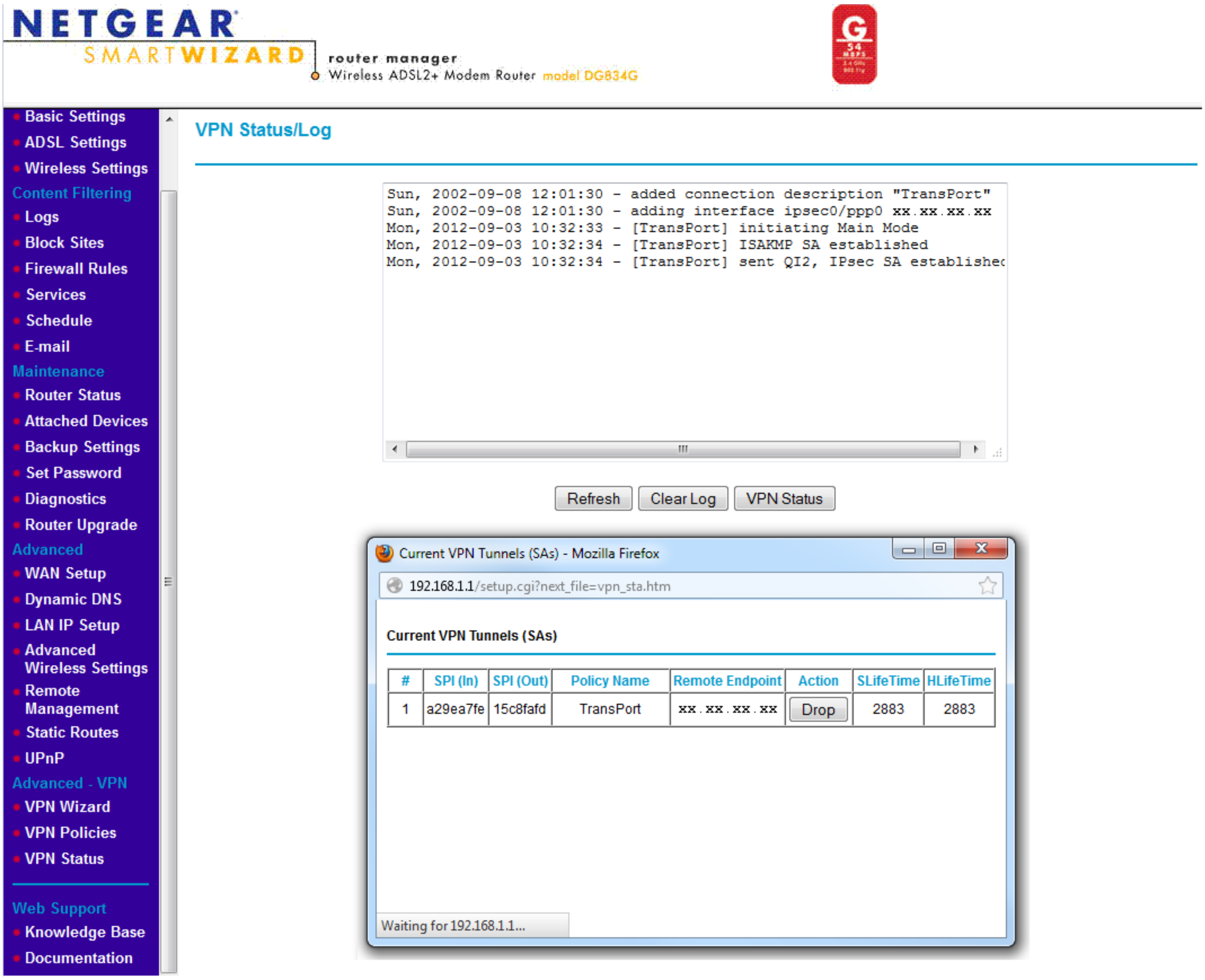
Command: ping 192.168.1.1 -e0
Command result

```
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:

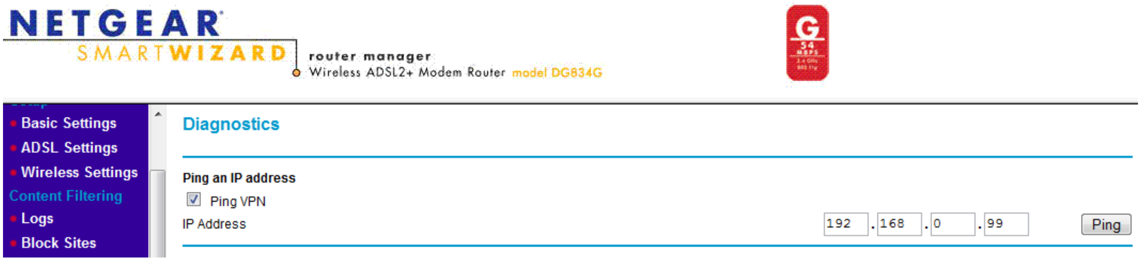


```
Sun, 2002-09-08 12:01:30 - added connection description "TransPort"
Sun, 2002-09-08 12:01:30 - adding interface ipsec0/ppp0 xx.xx.xx.xx
Mon, 2012-09-03 10:32:33 - [TransPort] initiating Main Mode
Mon, 2012-09-03 10:32:34 - [TransPort] ISAKMP SA established
Mon, 2012-09-03 10:32:34 - [TransPort] sent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

Current VPN Tunnels (SAs)

#	SPI (In)	SPI (Out)	Policy Name	Remote Endpoint	Action	SLifeTime	HLifeTime
1	a29ea7fe	15c8fafd	TransPort	xx.xx.xx.xx	Drop	2883	2883

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:



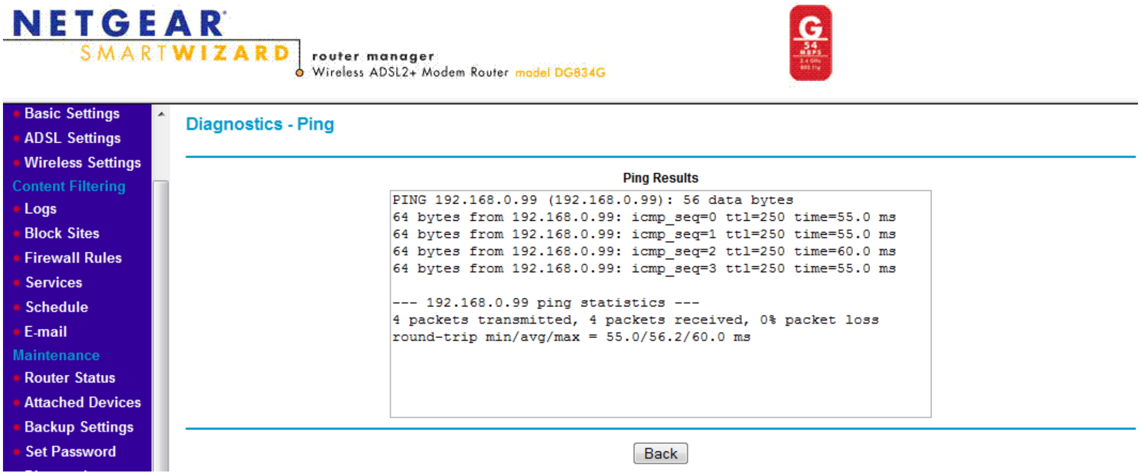
Diagnostics

Ping an IP address

☑ Ping VPN

IP Address 192 . 168 . 0 . 99

The results will be shown a couple of seconds later:



Diagnostics - Ping

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
```