

---

**Topic / Issue:** Configuration of VPN Tunnel using 2 IP470VPN's with 1 dynamic IP address

---

**Written By:** Scott Young

**Public Directory:** [www.alloy.com.au](http://www.alloy.com.au)

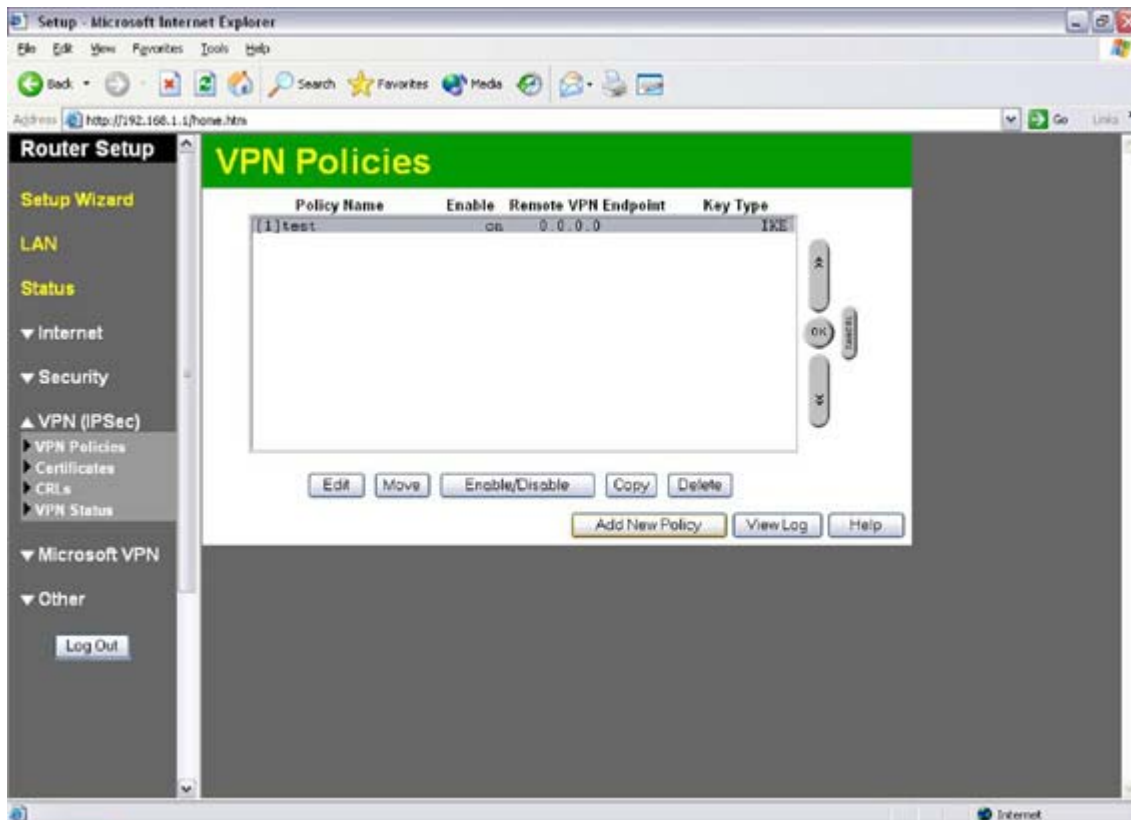
---

To configure a VPN Tunnel using 2 IP470VPN's with 1 dynamic IP address you must upgrade the IP470VPN to firmware version 1.0 release 0E or later.

The following configuration is a guide for creating an IPSec Based VPN Tunnel across the internet using two IP470VPN's with only one static IP Address. The instructions below are assuming that you have pre-configured the IP470VPN's Internet Connection.

Firstly you will need to create a VPN Policy at each end to allow a connection to be made between the two IP470VPN's.

-Click on VPN Policies and then select Add to create a new policy.  
You can either work your way through the Policy wizard or click on Setup Screen to configure policy manually.



---

Here we will create a VPN Policy for the remote network to connect to the local network with a static IP Address.

Click on Setup Screen to Configure Policy manually.

-Enter a Policy name where specified.

-The Remote VPN Endpoint will be the static WAN IP Address of the IP470VPN on the local network.

The screenshot shows the 'VPN Policy Definition' window with the following configuration:

- Name:** Test
- Enable Policy
- Allow NetBIOS traffic
- Remote VPN endpoint:**
  - Dynamic IP
  - Fixed IP: 10 . 0 . 0 . 1
  - Domain Name: [ ]
- Local IP addresses:**
  - Type: Subnet address
  - IP address: 192 . 168 . 0 . 0 ~ 0
  - Subnet Mask: 255 . 255 . 255 . 0
- Remote IP addresses:**
  - Type: Subnet address
  - IP address: 192 . 168 . 1 . 0 ~ 0
  - Subnet Mask: 255 . 255 . 255 . 0
- Authentication & Encryption:**
  - AH Authentication: MD5
  - ESP Encryption: 3DES, Key Size: n/a (AES only)
  - ESP Authentication: MD5
  - Manual Key Exchange
  - IKE (Internet Key Exchange)
    - Direction: Both Directions
    - Local Identity Type: WAN IP Address
    - Local Identity Data: [ ]

When using a Dynamic IP Address at one end you need to use the Internet Key Exchange (IKE)

Under the IKE option you must select the Direction as Both Directions, the Local Identity Type as WAN IP address and the Remote Identity Type as Remote WAN IP

Also you will need to enter a Pre Shared Key and change the Exchange Mode to Aggressive Mode.

When using IKE you have to make sure that you use the same Pre Shared Key at both ends. You will also have to make your Keys a certain length, the wizard will prompt you if your key is not the appropriate length.

---

ESP Authentication MD5

Manual Key Exchange

IKE (Internet Key Exchange)

Direction: Both Directions

Local Identity Type: WAN IP Address

Local Identity Data: 10.0.0.2

Remote Identity Type: Remote WAN IP

Remote Identity Data: 10.0.0.1

Authentication:  RSA Signature (requires certificate)  
 Pre-shared Key  
 test1234

Authentication Algorithm: MD5

Encryption: 3DES Key Size: n/a (AES only)

Exchange Mode: Aggressive Mode

IKE SA Life Time: 180 (secs)

IKE Keep Alive Ping IP Address: 0.0.0.0

IPSec SA Life Time: 300 (secs)

DH Group: Group 2 (1024 Bit)

IKE PFS: Group 2 (1024 Bit)

IPSec PFS: Group 2 (1024 Bit)

Save Cancel Back Help

Now we need to create a VPN Policy for the Local network to connect to the Remote network with the Dynamic IP Address.  
 Click on Setup Screen to Configure Policy manually.  
 -Enter a Policy name where specified.  
 -The Remote VPN Endpoint will be Dynamic IP.

### VPN Policy Definition

Name: test  Enable Policy  
 Allow NetBIOS traffic

Remote VPN endpoint:  Dynamic IP  
 Fixed IP: 0.0.0.0  
 Domain Name:

Local IP addresses  
 Type: Subnet address IP address: 192.168.1.0 ~ 0  
 Subnet Mask: 255.255.255.0

Remote IP addresses  
 Type: Single address IP address: 0.0.0.0 ~ 0  
 Subnet Mask: 255.255.255.0

Authentication & Encryption  
 AH Authentication MD5  
 ESP Encryption 3DES Key Size: n/a (AES only)  
 ESP Authentication MD5

Manual Key Exchange

IKE (Internet Key Exchange)

Direction: Responder

Local Identity Type: WAN IP Address

Local Identity Data: 10.0.0.1

---

Under the IKE option the Direction will be automatically set as Responder, select the Local Identity Type as WAN IP address and the Remote Identity Type as Remote WAN IP. Also you will need to enter a Pre Shared Key and change the Exchange Mode to Aggressive Mode.

When using IKE you have to make sure that you use the same Pre Shared Key at both ends. You will also have to make your Keys a certain length, the wizard will prompt you if your key is not the appropriate length.

The screenshot shows a configuration window for IKE (Internet Key Exchange). The 'Manual Key Exchange' option is unselected, and 'IKE (Internet Key Exchange)' is selected. The 'Direction' is set to 'Responder'. The 'Local Identity Type' is 'WAN IP Address' with 'Local Identity Data' set to '10.0.0.1'. The 'Remote Identity Type' is 'Remote WAN IP' with 'Remote Identity Data' set to '0.0.0.0'. Under 'Authentication', 'Pre-shared Key' is selected with the key 'test1234' and 'Authentication Algorithm' set to 'MD5'. Under 'Encryption', '3DES' is selected with 'Key Size' set to 'n/a'. The 'Exchange Mode' is 'Aggressive Mode'. The 'IKE SA Life Time' is '180 (secs)'. The 'IKE Keep Alive' checkbox is unchecked, and the 'Ping IP Address' is '0.0.0.0'. The 'IPSec SA Life Time' is '300 (secs)'. The 'DH Group', 'IKE PFS', and 'IPSec PFS' are all set to 'Group 2 (1024 Bit)'. At the bottom, there are 'Save', 'Cancel', 'Back', and 'Help' buttons.

You should now be able to initiate your VPN connection from pinging from the remote network to any IP address on the local network.

*Please note, that you can only initiate the VPN connection by pinging from the Network that has a dynamic WAN IP Address to the network that has the Static WAN IP Address.*

---

**Summary:**  
**(If required)**