DSR to DSR VPN Tunnel

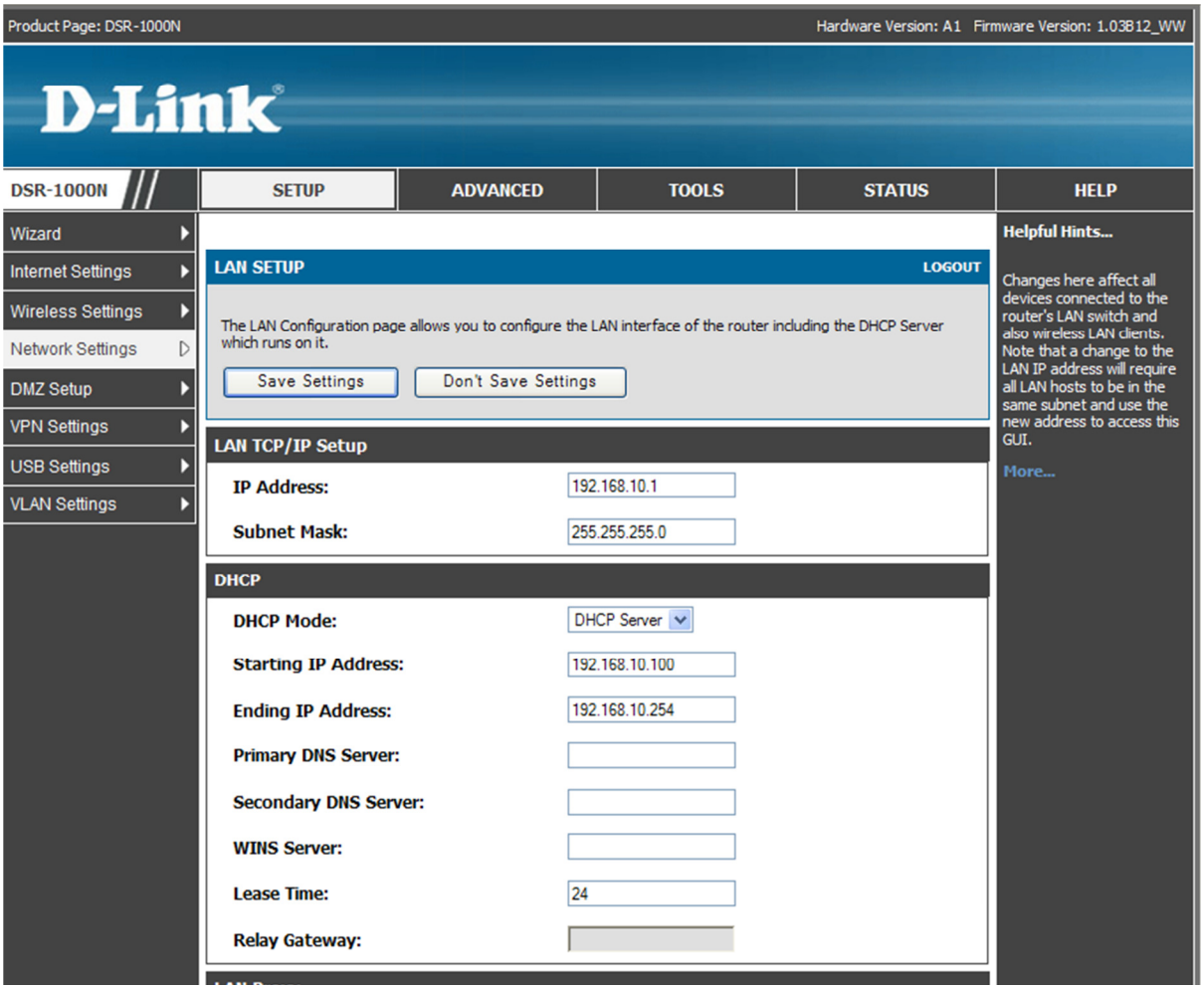
(LAN:192.168.10.1)DSR-1000N (WAN) - - -  - - - - (WAN) DSR-1000N (LAN: 192.168.30.1)

Here we're trying to build a VPN tunnel between two DSR units.

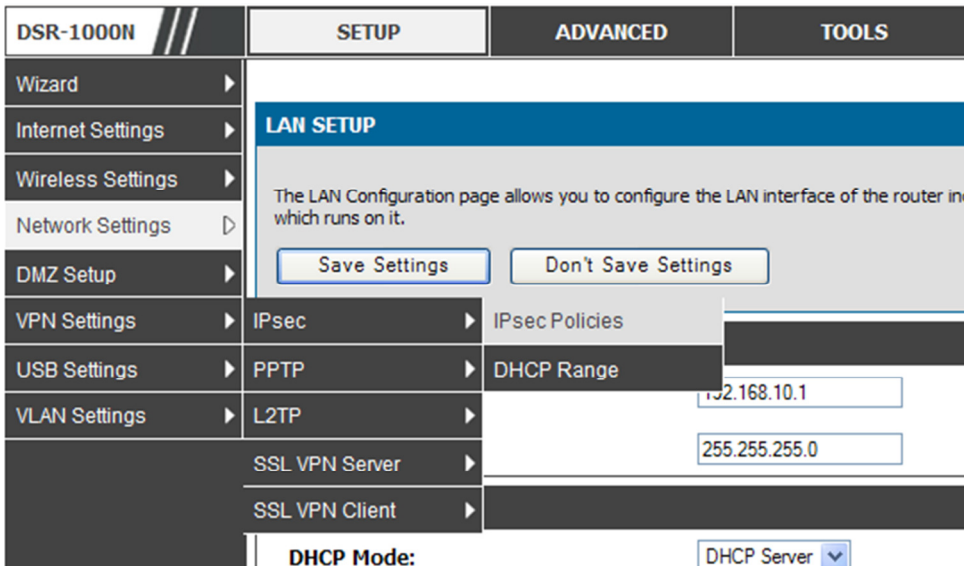
DSR-1000N Setup

Step 1) Go to SETUP > Network Settings.
Set the LAN IP of the product, this will need to be in a different subnet on each side.

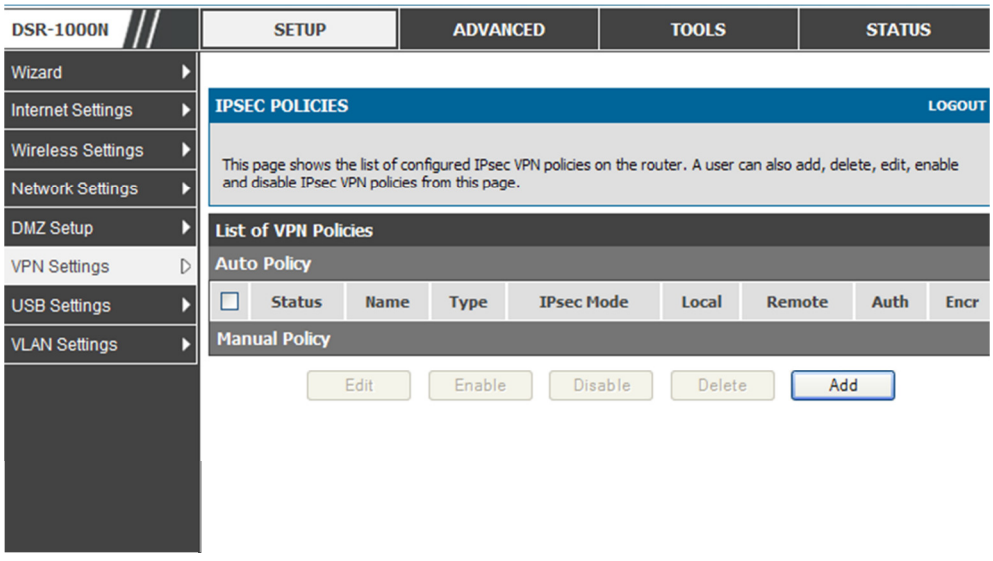
Once done clink **"Save Settings"**



Step 2) Go to SETUP > VPN Settings > SSL VPN server > Portal Layouts.

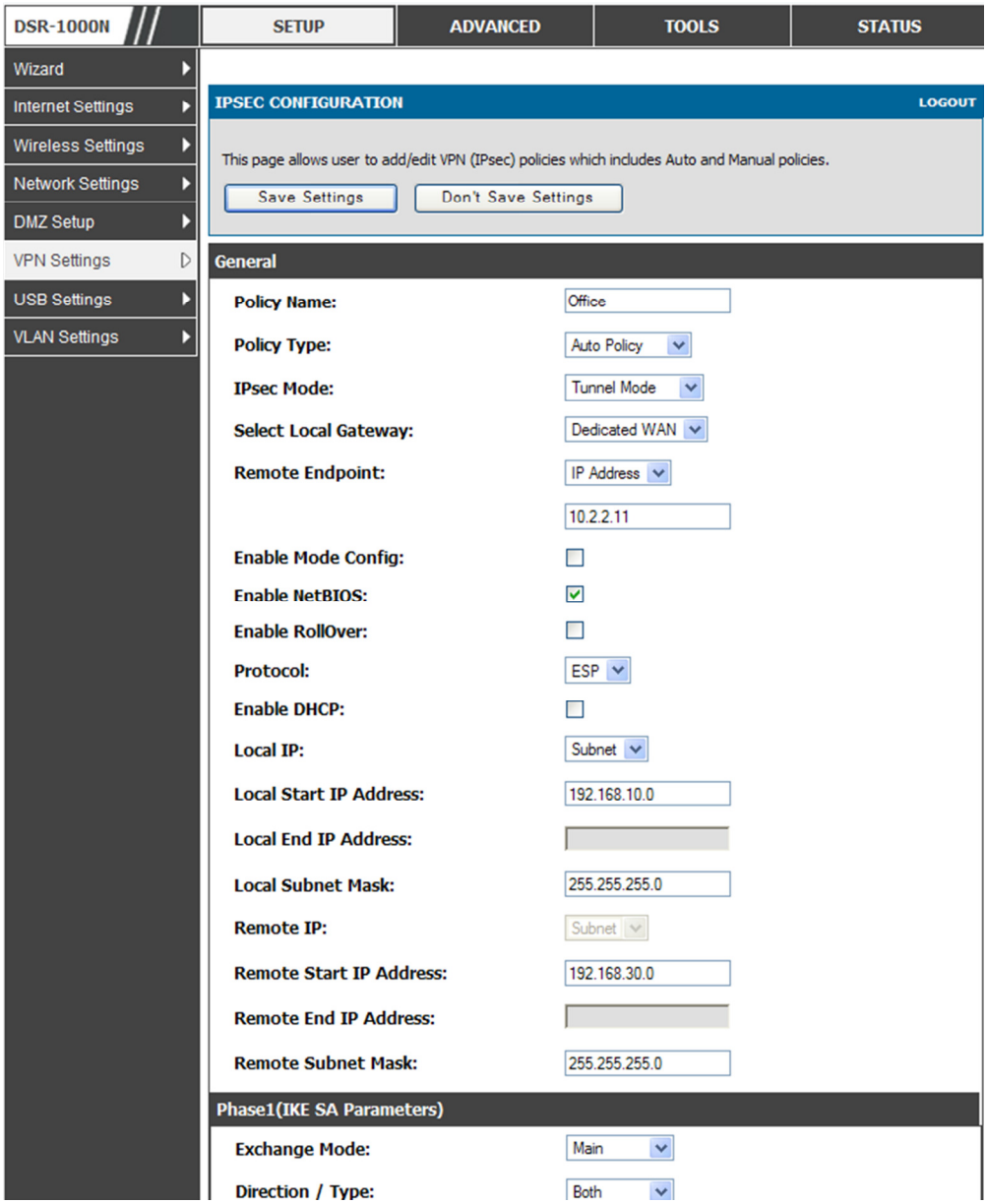


Click on **"Add"**



Under IPsec Configuration enter in the below;

Policy Name: A name that describes the tunnel
Policy Type: Auto Policy
IPSec Mode: Tunnel Mode
Local Gateway: Dedicated WAN
Remote Endpoint: This is the Public IP of the remote unit
Local IP set to **"Subnet"** and enter in the start IP of the local network
Local Subnet mask: enter in the local subnet
Remote Start IP: same as above but the remote start IP
Remote Subnet mask: The remote subnetmask



Under Phase1 enter in the below:

Exchange Mode: Main

Direction / Type: Both

Nat Transversal: If modem has NAT enabled set NAT Transversal to “ON”, otherwise set to “Off”

Local Identifier Type: Local Wan IP

Remote Identifier Type: Remote Wan IP

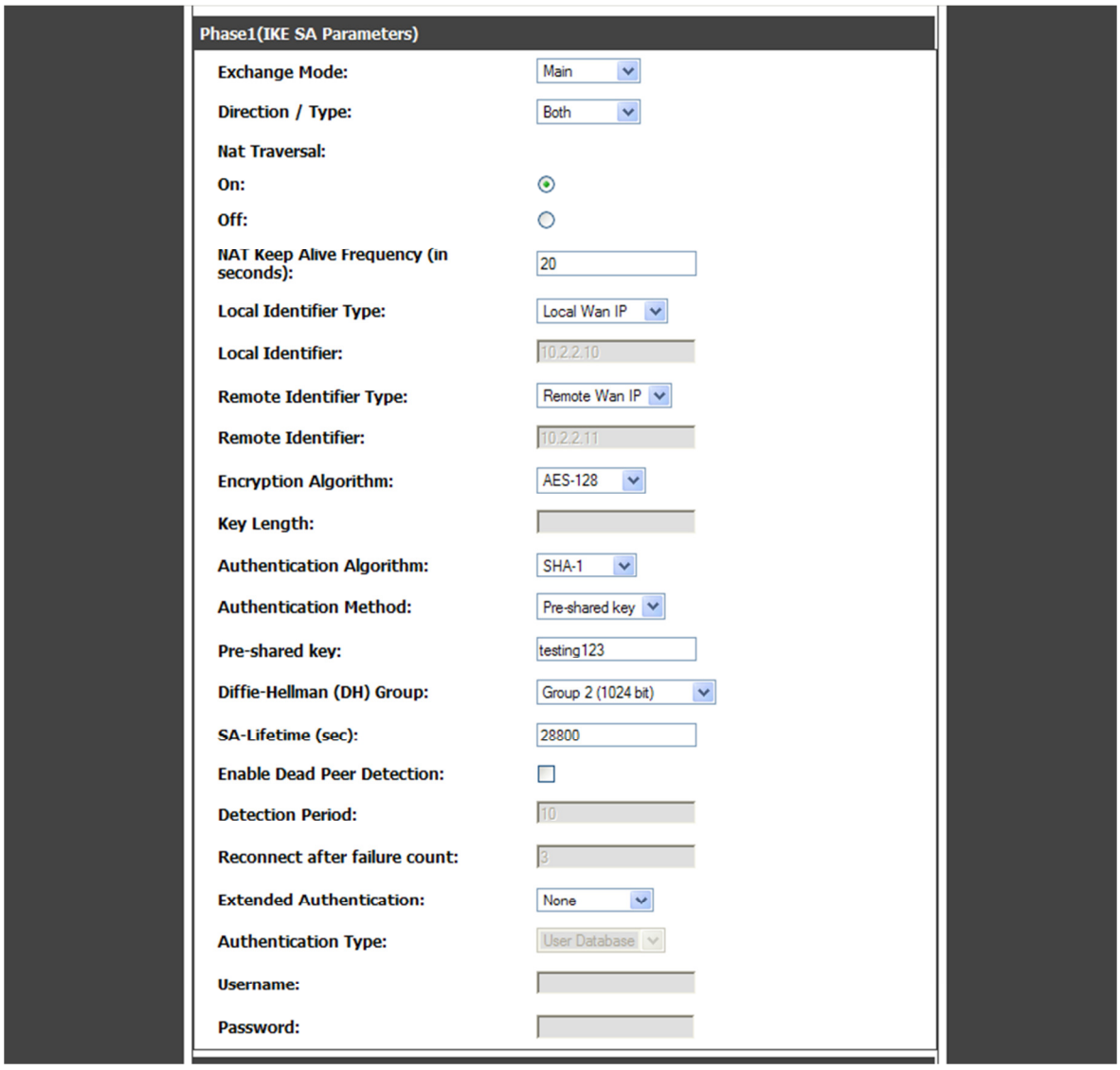
Encryption Algorithm: AES-128

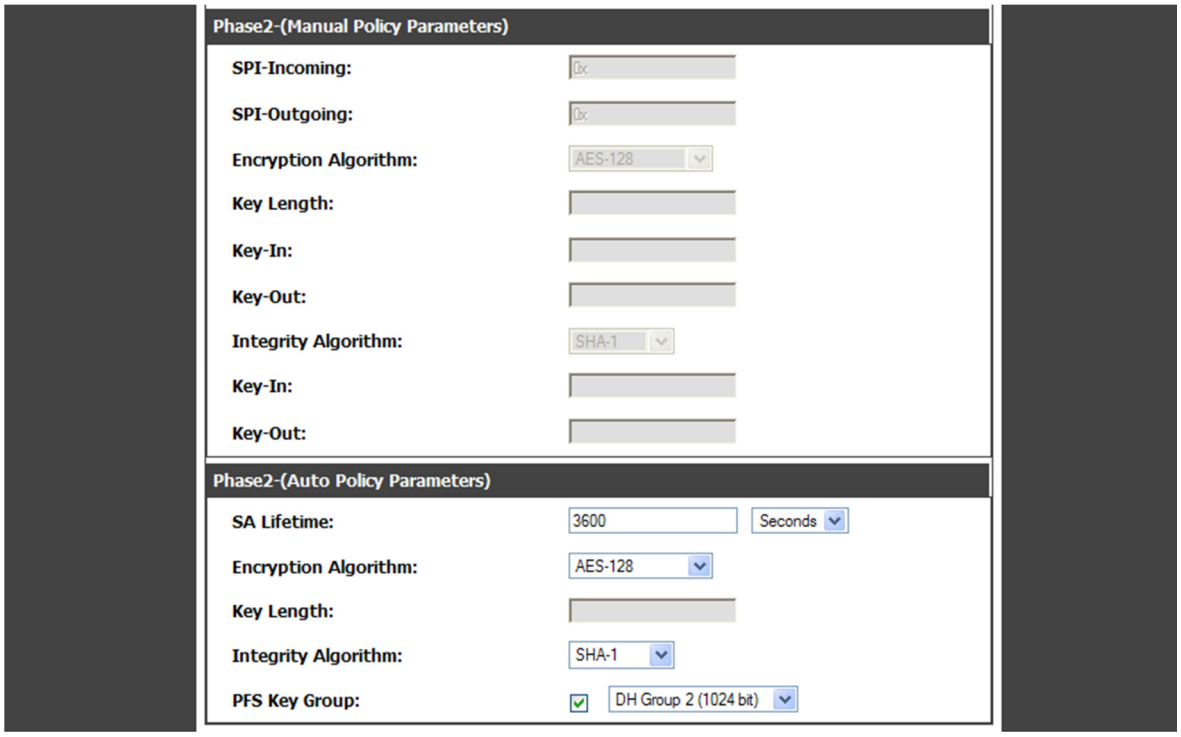
Authentication Algorithm: SHA-1

Authentication Method: Pre-shared key

Pre-shared key: Enter in a password

All other settings below Pre-shared key leave as default.

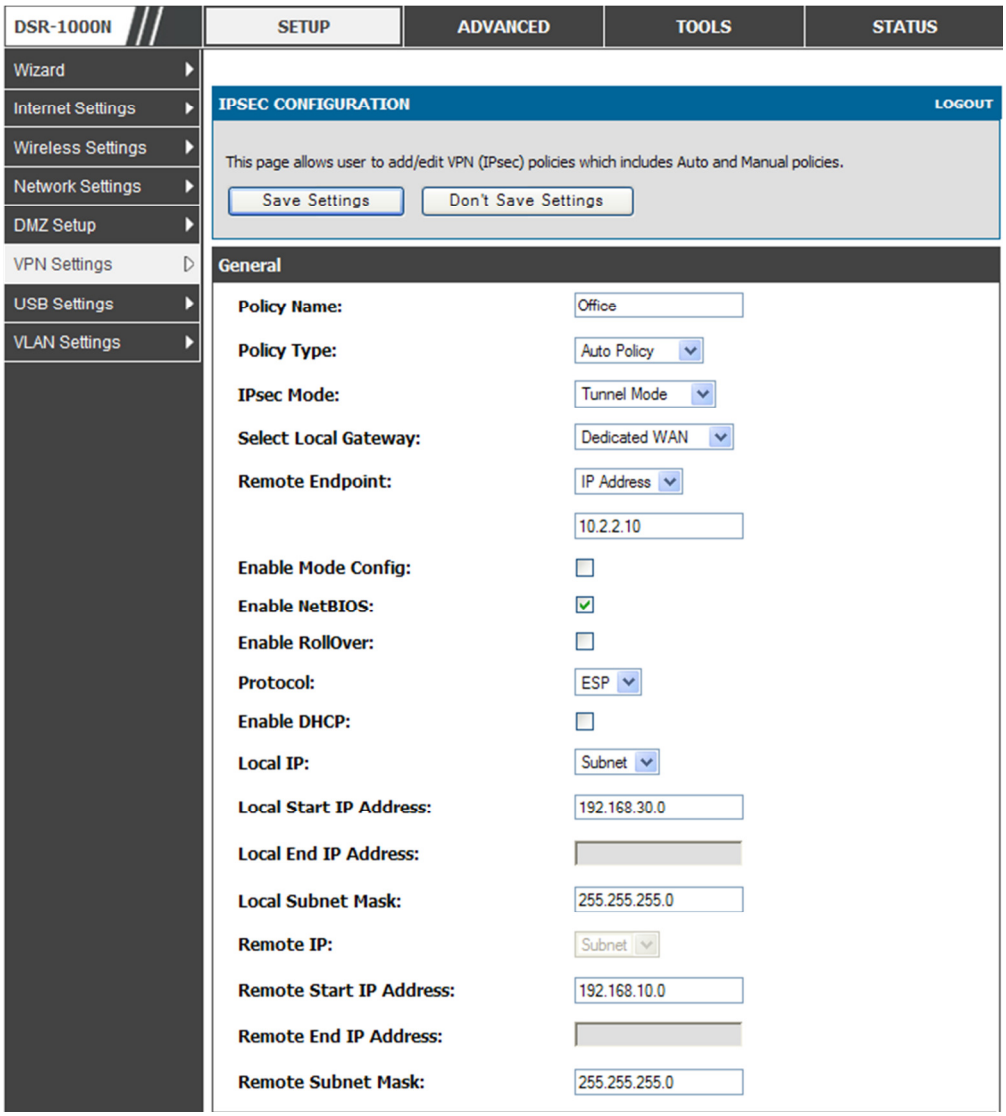


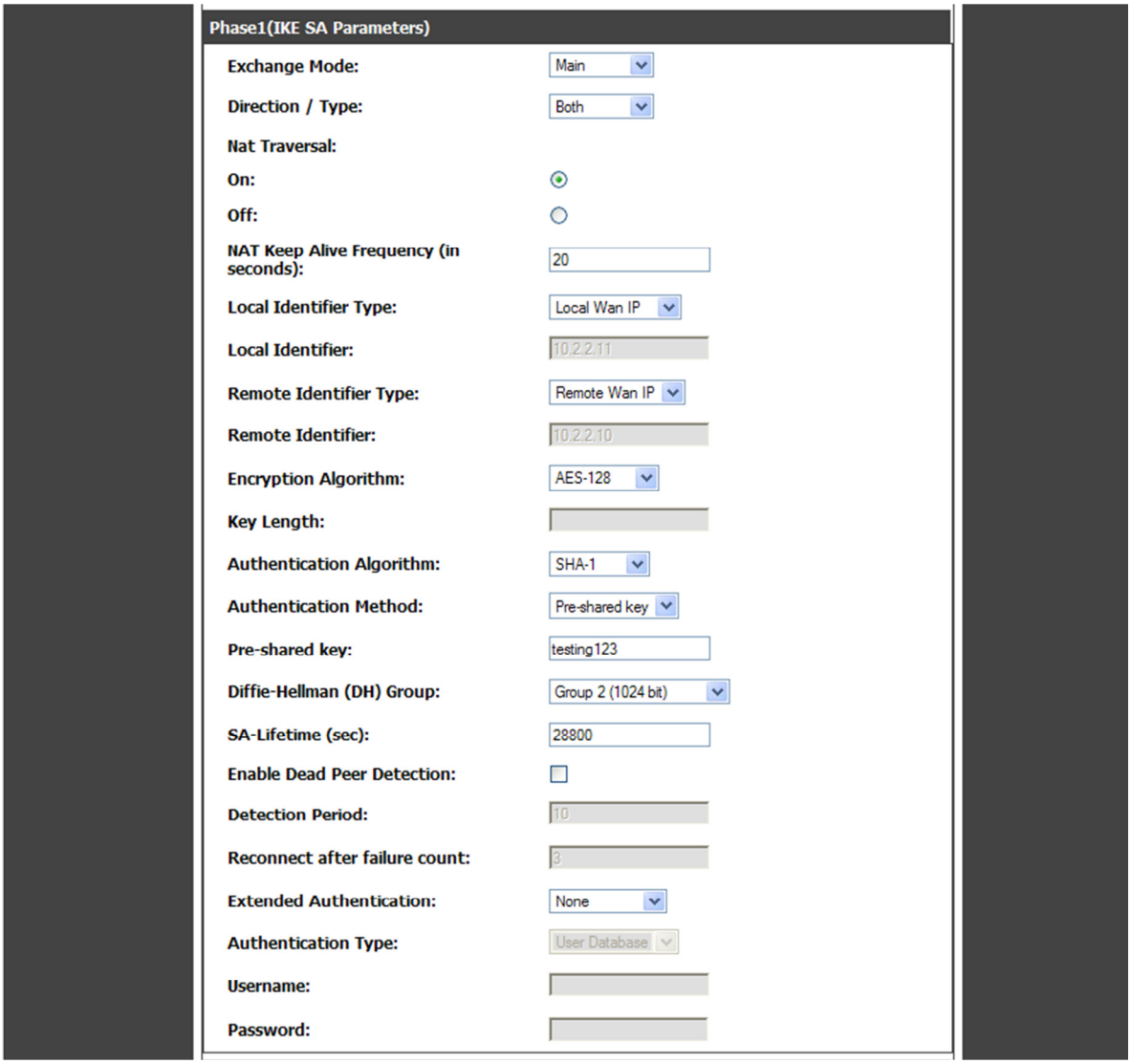

Phase2-(Manual Policy Parameters)
SPI-Incoming:
0x
SPI-Outgoing:
0x
Encryption Algorithm:
AES-128
Key Length:
Key-In:
Key-Out:
Integrity Algorithm:
SHA-1
Key-In:
Key-Out:
Phase2-(Auto Policy Parameters)
SA Lifetime:
3600
Seconds
Encryption Algorithm:
AES-128
Key Length:
Integrity Algorithm:
SHA-1
PFS Key Group:
DH Group 2 (1024 bit)

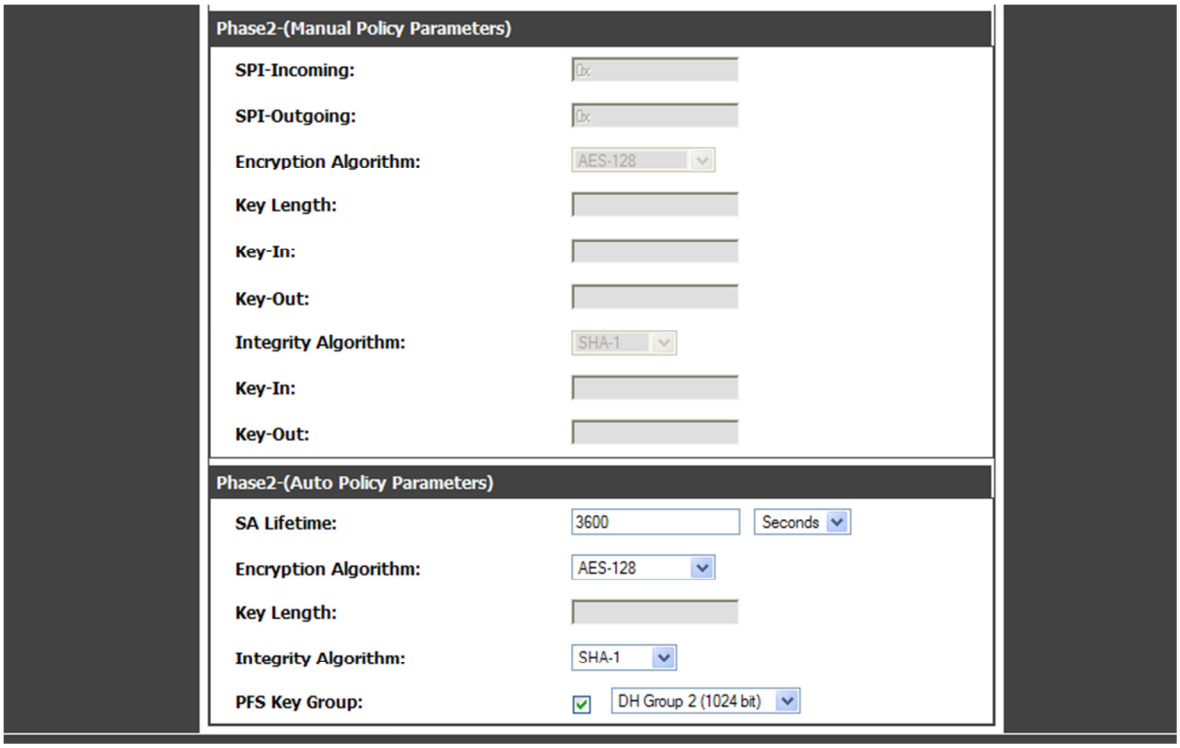
Step 3) Remote unit setup.
The remote unit will be setup with mirror setings to the first.

E.G. The local subnet on the first unit will become the remote subnet on the second unit.

See below for screen shots with the mirror settings.




Phase1(IKE SA Parameters)
Exchange Mode:
Main
Direction / Type:
Both
Nat Traversal:
On:
Off:
NAT Keep Alive Frequency (in seconds):
20
Local Identifier Type:
Local Wan IP
Local Identifier:
10.2.2.11
Remote Identifier Type:
Remote Wan IP
Remote Identifier:
10.2.2.10
Encryption Algorithm:
AES-128
Key Length:
Authentication Algorithm:
SHA-1
Authentication Method:
Pre-shared key
Pre-shared key:
testing123
Diffie-Hellman (DH) Group:
Group 2 (1024 bit)
SA-Lifetime (sec):
28800
Enable Dead Peer Detection:
Detection Period:
10
Reconnect after failure count:
3
Extended Authentication:
None
Authentication Type:
User Database
Username:
Password:



Once finished try to ping a device on the remote side. If the device has a firewall installed (E.G. windows 7 firewall) please disable this as it will block the ping.

Also some AV software can also block ping, if you have a print server or non PC device try to ping this as its less likely to block ping.