

Topic / Issue: Bintec X Series IPSEC router configuration with Netgear FVS318

Written By: Scott Young

Guide to configuring X1200 IPSEC VPN to a Netgear FVS318.

The Netgear should be set to the following

Use your own values in Local IPsec Identifier, Remote IPsec Identifier and note these for later use on the x1200.

Ensure that the security association = Main mode

Ensure that Perfect Forward Secrecy = Enabled

Ensure that Encryption protocol = 3DES

Use a new Preshared Key - note this for later use on the X1200

The X1200 should be configured like so:

The first step is to run the IPSEC configuration wizard.

When running this select:

Authentication Method = 'preshared_keys'.

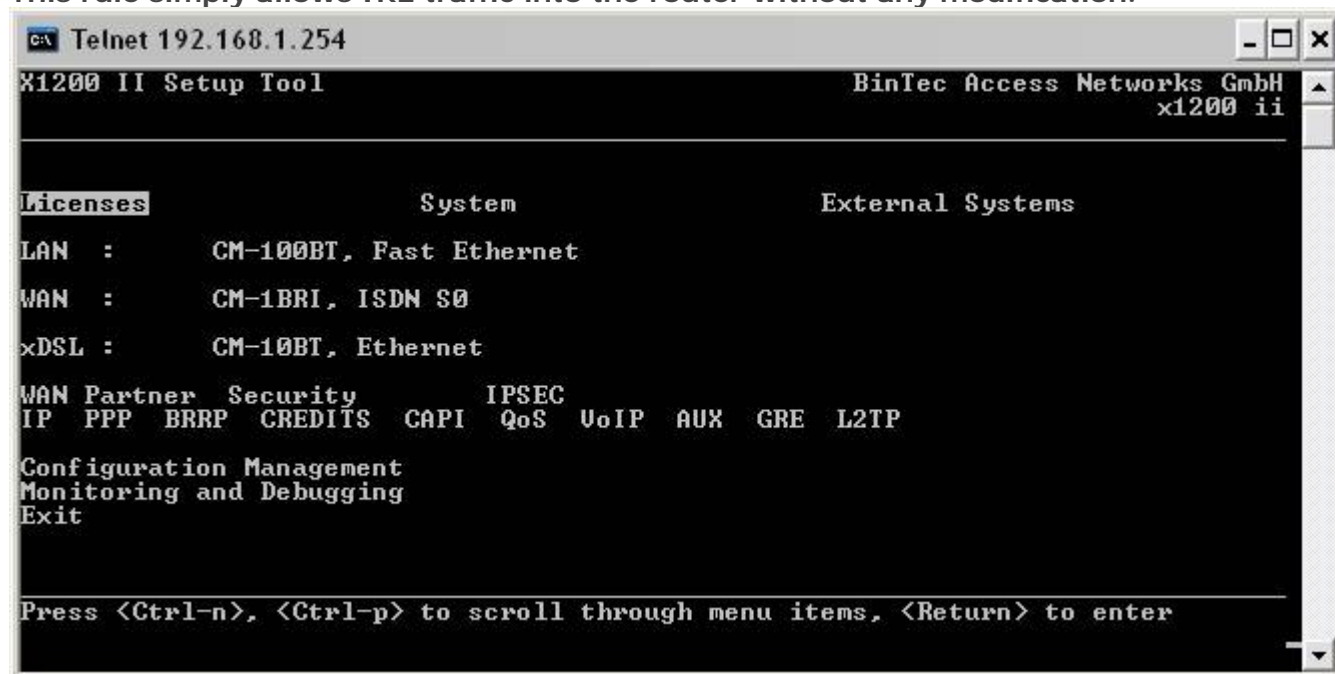
Peer = Peer ID name and IP Address

Peer traffic = 'don't verify' and specify the Local and Remote LAN networks.

The wizard will configure the basic's but you will now need to customise some of the parameters, specifically the Encryption and Hash Algorithms types.

Check 'Pre IPSEC Rule' You should have one rule entry in here that is automatically generated.

This rule simply allows IKE traffic into the router without any modification.



```
C:\> Telnet 192.168.1.254
X1200 II Setup Tool                                     BinTec Access Networks GmbH
                                                         x1200 ii

Licenses          System          External Systems
LAN :             CM-100BT, Fast Ethernet
WAN :             CM-1BRI, ISDN S0
xDSL :           CM-10BT, Ethernet

WAN Partner Security  IPSEC
IP PPP BRRP CREDITS  CAPI QoS UoIP AUX GRE L2TP

Configuration Management
Monitoring and Debugging
Exit

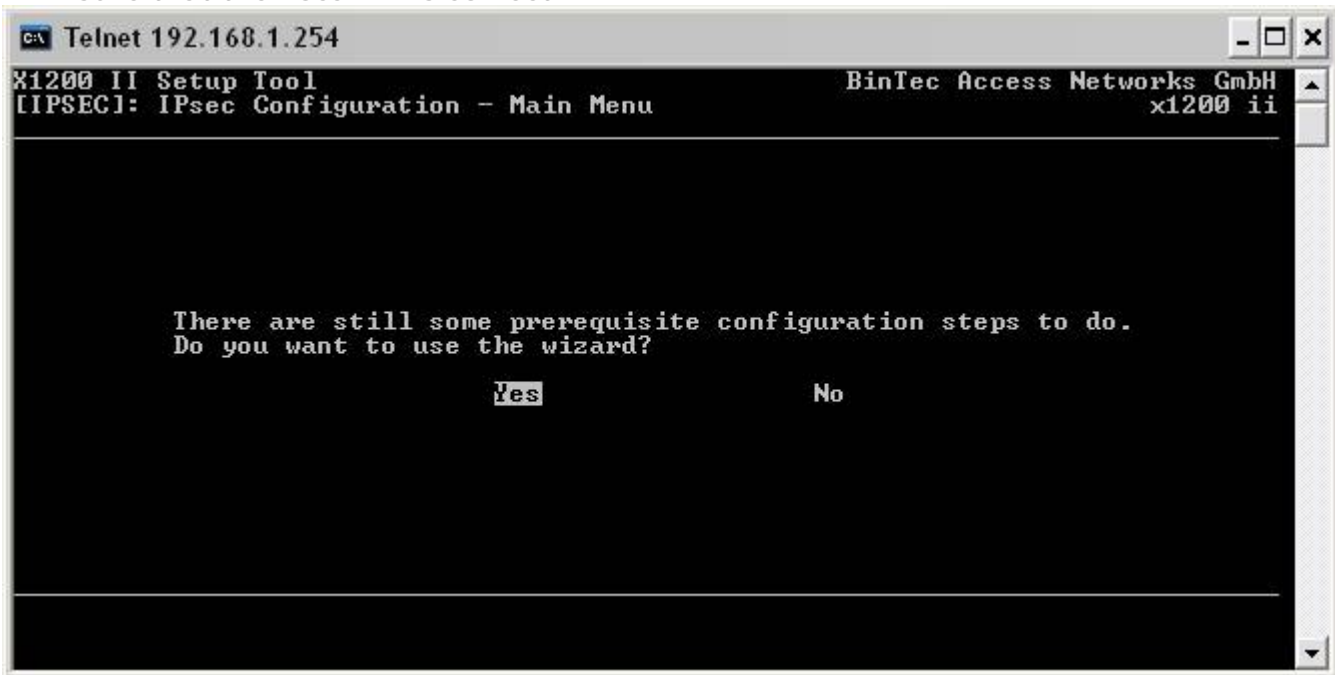
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to enter
```


Check the 'Phase 1' settings.

Ensure that Proposal = DES3/MD5

Ensure that Mode = id_protect (Note: 'id_protect' is another name for 'Main Mode')

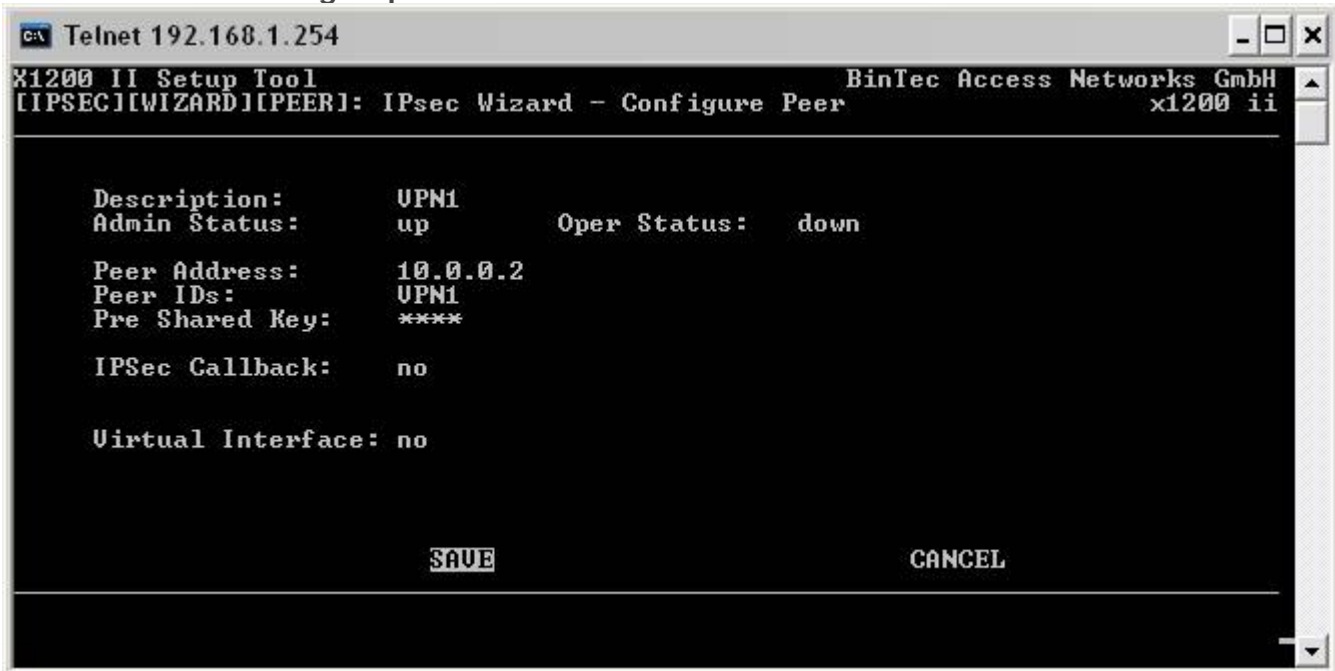
Ensure that the Local ID is correct



Check the 'Phase 2' settings.

Ensure that Proposal = ESP(DES3/MD5) no Comp


Ensure that PFS = group 1



Once the above has been configured you should be able to initiate a VPN from a ping packet.

Do not perform the ping from the X1200 itself, as this will originate the ping from the WAN, and not trigger a IPSEC connection.

Then check the status of the IPSEC VPN within the 'IP SEC security associations' monitoring page.



```
C:\> Telnet 192.168.1.254
X1200 II Setup Tool                               BinTec Access Networks GmbH
[WIZARD][ADD]: Traffic Entry <UPN1>                x1200 ii

Description:   UPN1
Protocol:      dont-verify
Local:
  Type: net    Ip: 192.168.1.0    / 24
Remote:
  Type: net    Ip: 192.168.0.0    / 24
Action:        protect

                SAVE                                CANCEL
```

Summary:
(If required)