



Topic / Issue: Bintec Series II, X1200_II and X1000_II IPSEC Configuration

Written By: Scott Young

Configuration Guide for Bintec Series II IPSEC tunnels (Bintec router to Bintec router)

The Bintec Series II routers include a free IPSEC (limited) License.
This is implemented through a IPSEC enabled firmware - Download from www.bintec.net

Default "setup" screen

```
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

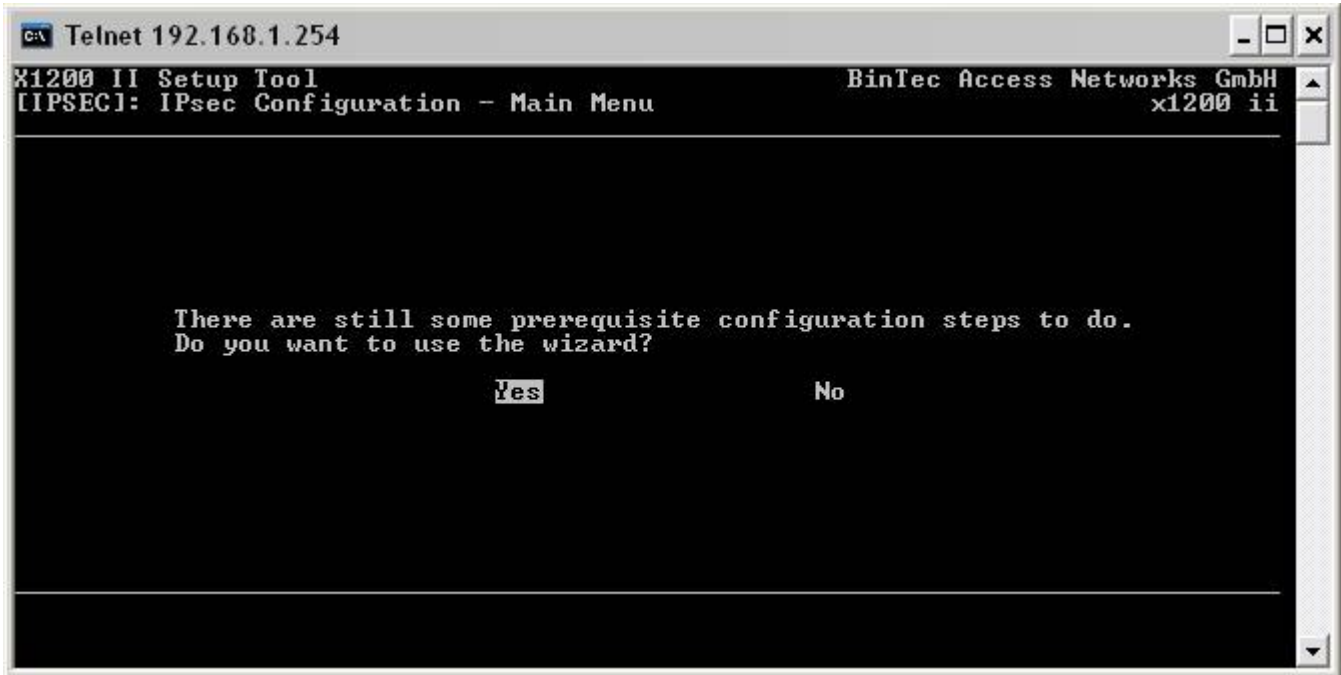
Configuration Management
Monitoring and Debugging
Exit

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

Once your 2 end points are connected to the internet.

You need to configure the IPSEC tunnel

Use the Wizard to default all settings and Open NAT for IPSEC

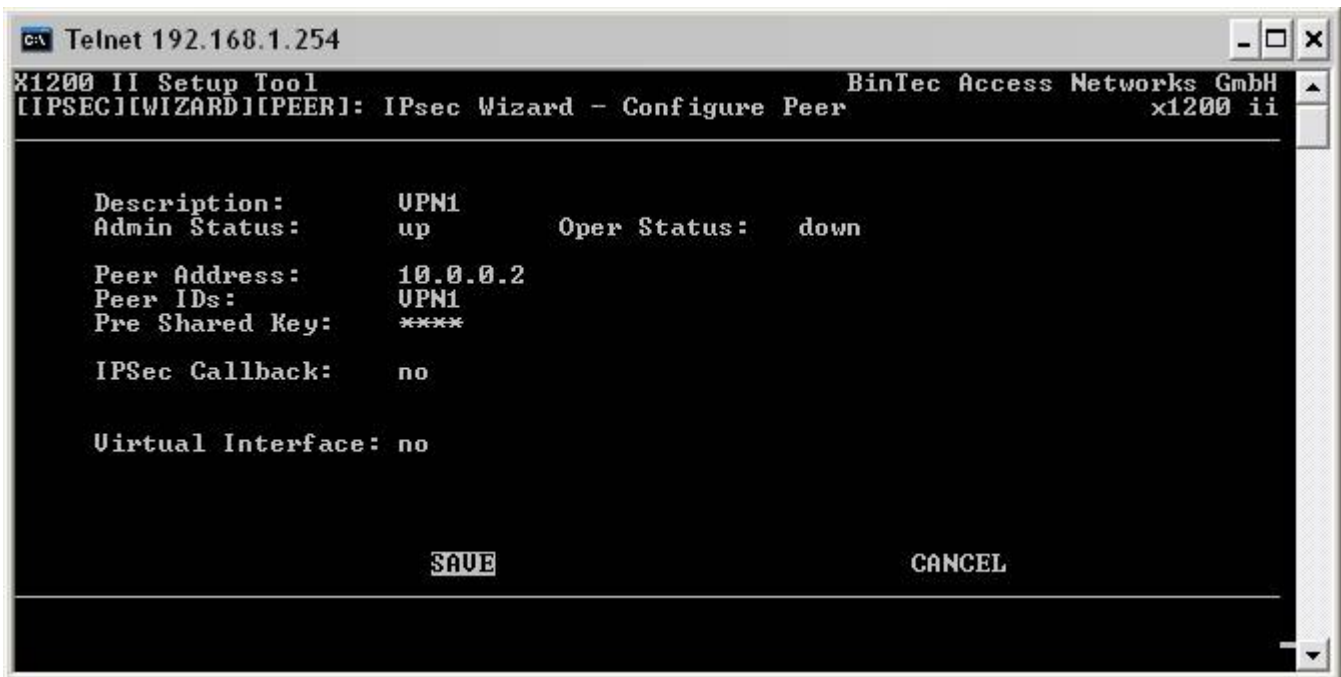


Use which Default IPSEC Authentication Method ? Select PSK

Which Local ID should be used for IPsec ? VPN1

(to keep the configuration simple we will use the same ID, Password and Local

Configure Peers ? Start



Description = VPN1

Peer Address = the WAN IP of the Remote VPN end Point

(if the remote end point is Dynamic, leave this blank)

Peer ID = VPN1

Pre Shared Key = VPN1

Configure Peer Traffic ? Start



Description = VPN1

Protocol = "dont-verify"

This instructs the Bintec router to IPSEC encrypt all traffic types between the local LAN and the remote network LAN.

Define the Local LAN IP range and Remote LAN IP range.

The "/ 24" is the mask applied to the addresses, 24 = 255.255.255.0, 16 = 255.255.255.0 etc...

```

c:\ Telnet 192.168.1.254
x1200 II Setup Tool                               BinTec Access Networks GmbH
IPsec Configuration - Wizard Menu                 x1200 ii

IPsec 1st step configurations wizard

Configuration History:
+ Check for Peer ...
  IPSEC already enabled
  Pre Shared Key now set
  IPSEC already enabled
+ Check for ISDN Callback configuration ...
+ Check for Peer Virtual interface ...
+ Check for Peer Traffic ...
  Peer Traffic now configured (Index 2)
= IPsec Wizard finished =

What to do?
<create syslog messages for configuration history>
                                                    clear config
                                                    <<Space> to choose)
                                                    <<Return> to select)

                                Exit

Use <Space> to choose <Return> to select

```

The configuration is completed.

Select Exit, and then Save the Config.

(not at this point also do master "Configuraiton management Save Option"

Now Verify the confing.

Select Pre-IPSEC rules:

```
c:\ Telnet 192.168.1.254
X1200 II Setup Tool BinTec Access Networks GmbH
[PRE IPSEC TRAFFIC]: IPsec Configuration - Configure Traffic List x1200 ii

Highlight an entry and type 'i' to insert new entry below,
'u'/'d' to move up/down, 'a' to select as active traffic list

Local Address M/R Port Proto Remote Address M/R Port A Proposal
*0.0.0.0 M0 500 udp 0.0.0.0 M0 500 PA

APPEND DELETE EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit
```

(your config should be like above)

Select Configure Peers:

```
c:\ Telnet 192.168.1.254
X1200 II Setup Tool BinTec Access Networks GmbH
[PEERS]: IPsec Configuration - Configure Peer List x1200 ii

Highlight an entry and type 'I' to insert new entry below,
'U'/'D' to move up/down, 'M' to monitor, 'PSCEAFT' to change sorting.

State desCription pEerid peerAddress proFile Traffic
dorm UPN1 UPN1 10.0.0.2 d 3 2

APPEND DELETE REORG EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return> to edit
```

(your config should be like above)

The above procedure needs to be repeated on the remote Bintec Router.

(Note: some of the IP settings need to be reversed - Local IP will now be the Remote IP etc..)

After saving the configuration go to the command prompt in the Bintec router (Exit setup menu) and test the IPSEC connection via pinging the remote network.

Go back into the Setup menu

Select Monitoring

Select IPSEC monitor

Select Global Statistics

```
C:\> Telnet 192.168.1.254
X1200 II Setup Tool BinTec Access Networks GmbH
[MONITOR][IPSEC][STATS]: IPsec Monitoring - Global Statistics x1200 ii

Peers Up : 1 /1 Dormant: 0 Blocked: 0

SAs Phase 1: 1 /1 Phase 2: 1 /1

Packets In Out
Total : 180699 174355
Passed : 86801 92289
Dropped: 3 0
Protect: 82336 82081
Errors : 0 0

EXIT
```

You should see Peers Up 1 / 1 (0 / 1 indicates the connection did not establish)

Note: Dynamic End Points.

To support one end being Dynamic, you need to change the IKE Phase 1 mode.

Select Edit IKE Phase 1:

Change the mode section to aggressive (from id_protect)

This will enable a Dynamic to Statis IPSEC connection.



```
C:\> Telnet 192.168.1.254
X1200 II Setup Tool                               BinTec Access Networks GmbH
[IPSEC][PHASE1][EDIT]                             x1200 ii

Description (Idx 3) : *autogenerated*
Proposal           : 1 (Blowfish/MD5)
Lifetime           : use default
Group              : 2 (1024 bit MODP)
Authentication Method : Pre Shared Keys
Mode              : aggressive
Heartbeats         : none
Block Time         : 0
Local ID           : UPN1
Local Certificate  : none
CA Certificates    :
Nat-Traversal      : enabled

View Proposals >
Edit Lifetimes >

SAVE                                CANCEL

Use <Space> to select
```

Summary:
(If required)