

## NQG\_053: Configuring the Netopia router for IPsec with IKE

This Quick Guide covers the configuration of an **IPsec profile** using the **Internet Key Exchange (IKE)** protocol for a Netopia R-Series router.

### Assumptions:

This guide assumes that you are running Netopia router firmware version **4.10** or later, and have read the firmware documentation. To update your router firmware, go to our [firmware update page](#).

*Note: IPsec tunneling supports IP routing only. IPX, AppleTalk or any protocol other than IP will not be routed across an IPsec tunnel.*

### Before you start:

- **PLEASE READ** our [Notice on Configuring VPN Tunnels with Netopia Routers](#).
- Establish a serial connection to the Netopia router's console using a communications program such as HyperTerminal or Z-Term. The settings should be 9600 Baud, 8 Data Bits, and 1 Stop Bit. Disable flow control.
- Alternatively, you can use Telnet over your LAN to get to the console screens.
- For detailed instructions on using HyperTerminal, Z-Term, or Telnet, please see [Netopia Quick Guide NQG\\_100](#).

### Tips:

- Do not change any settings other than the ones referred to below.
- Pressing Return takes you into a page; pressing Escape takes you out.
- Press Return after entering each setting to save it.

**Note:** This quick guide covers the creation of the phase1 (IKE) profile and the phase2 (IPsec) profile in the Netopia. In the Netopia, all connections are managed in a connection profile that contains all the pertinent information and options for that connection. To change an IPsec profile that has already been created, go to WAN Configuration -> Change Connection Profile, and select the appropriate profile. To change an IKE profile that has already been created, go to WAN Configuration -> IPsec configuration. Do not make changes to settings unless referenced in this configuration guide. Unlike other connection types, there is no need to establish an IPsec connection; once the profile is configured, the tunnel is automatically and transparently active. However, depending on hardware configuration, encryption options and etc. it can take up to two minutes for the tunnel to complete authentication and begin relaying traffic. Please bear this fact in mind when testing the tunnel connectivity with ping and other diagnostic tools. This configuration assumes that both sides of the VPN have static, valid Internet IP address on their WAN interfaces, and that NAT is not used in the VPN tunnel itself, though it may be used on the Internet connection.

### Router Step-by-step Configuration

The following example configuration is based on two R-Series routers with connections to the Internet using NAT (Network Address Translation). It is not necessary for you to have NAT enabled on your Internet connection profile for this to work. The **Local WAN IP addresses** used in the configuration are only an example. This configuration will also cover a Netopia connecting to most other IPsec security gateway products. While this Quick Guide does not cover all possible configuration options, the configuration detailed should work well in most situations.

*Note:* The **Ethernet IP Addresses** used in this example can be implemented in other similar configurations. However, the **Local WAN IP Addresses** will change per individual configuration. The following router configurations are based on the following example configurations. Please substitute your own IP information when configuring your routers. In any case, both routers must be configured for

different Ethernet IP subnets, as the example configuration illustrates.

#### Example Netopia Configuration:

WAN IP Address:	172.16.0.2
WAN Subnet Mask:	255.255.0.0
Ethernet IP Address:	192.168.2.1
Ethernet Subnet Mask:	255.255.255.0

#### Example Remote System Configuration:

WAN IP Address:	172.16.0.1
WAN Subnet Mask:	255.255.0.0
Ethernet IP Address:	192.168.1.254
Ethernet Subnet Mask:	255.255.255.0

Note that this makes the Network Address of the Netopia's Ethernet interface 192.168.2.0 and the Network Address of the LAN interface of remote system 192.168.1.0. These addresses will be used throughout the creation of the tunnel.

#### Netopia Step-by-Step Configuration:

1. Telnet or Console into the Netopia.
2. Go to **Quick Menus, Add Connection Profile**.
3. Supply a descriptive **Profile Name** and set the **Encapsulation Type** to **IPsec**.
4. Select **Encapsulation Options**
5. Set **Key Management** to **IKE**
6. Select **IKE Phase 1 Profile, ADD PH1 PROFILE**
7. Supply a descriptive name for the IKE profile
8. Leave **Mode** at **Main Mode**.
9. Leave **Authentication Method** at **Shared Secret**
10. Set the **Shared Secret** to an agreed upon password - this can be any alphanumeric string, 'Netopia1234' for example.
11. Select either **DES** or **3DES** for the **Encryption Algorithm**. Note: it is **strongly** recommended that you have the optional **VPN accelerator card** if you intend to use 3DES.
12. Select either **MD5** or **SHA1** for the **Hash Algorithm**
13. **Diffie-Hellman Group** defaults to **Group 2**; to interoperate with other vendors' equipment, you may sometimes need to specify Group 1.
14. Leave the **Advanced IKE Phase 1 Options** alone.
15. Select **ADD IKE PHASE 1 PROFILE**
16. Make Sure that **IKE Phase 1 Profile** lists the IKE profile you just created.
17. Leave **Encapsulation** set to **ESP**
18. Set **ESP Encryption Transform** to either **DES** or **3DES**. Note that it is **strongly** recommended that you have installed the optional **VPN Accelerator card** if you intend to use **3DES**. Null is not recommended; it offers no data security.
19. Set **ESP Authentication Transform** to either **HMAC-MD5-96** or **HMAC-SHA1-96**
20. If you have the VPN accelerator card, you will have an option for **Compression Type**; if your remote system supports **LZS compression**, you can specify **LZS compression** here. Otherwise, set compression to **None**.
21. Leave the **Advanced IKE Options** alone.
22. Hit enter on **COMMIT**
23. Arrow down to **IP Profile Parameters** and hit **ENTER**
24. Set **Remote Tunnel Endpoint** to the WAN Interface address of the remote system. This is the same value used in step #11 above (172.16.0.1 in the example).
25. Leave **Remote Member Format** at **Subnet**
26. Set **Remote Member Address** to the LAN interface network address of the remote system

- (192.168.1.0 in the example).
27. Set **Remote Member Mask** to the subnet mask used on the LAN interface of the Nortel switch (255.255.255.0 in the example)
  28. Leave **Local Member Format** as **Subnet**
  29. Set **Local Member Address** to the network address associated with the Ethernet IP of the Netopia (192.168.2.0 in the example).
  30. Set the **Local Member Mask** to the Ethernet IP Subnet Mask of the Netopia (255.255.255.0 in the example).
  31. Leave **Address Translation Enabled** set to **No**
  32. Leave **Filter Set** set to **None**, and leave the **Advanced IP Profile Options** alone.
  33. Arrow down to **COMMIT** and hit **ENTER**. Repeat this for the **Add Connection Profile** screen.

This completes the Netopia portion of the configuration. If your remote system is another Netopia router, simply repeat the above procedure, reversing all the IP addresses for the various fields.

At this point, you are ready to test the configuration. Bear in mind that the tunnel can take upwards of 120 seconds to authenticate, so if you are testing using ping, send at least 120 packets.