

## NQG\_050: Creating an IPSec Tunnel Between a Netopia R-Series Router and a WatchGuard FireBox

Notice: Netopia Technical Support provides this document to you as an added service. Although the configurations described below have proven successful in many instances, Netopia support cannot be responsible for issues with the installation and configuration of non-Netopia products. If the following suggestions do not provide the results you desire, please contact WatchGuard Technical Support directly.

### Assumptions:

- The Netopia router must be running 4.8 or later firmware. If not, you must upgrade your firmware (see our firmware download page) before attempting to follow this Quick Guide.
- No server list entries for port 500 exist in your router, and any active filter sets do not block protocols 50 and 51.
- The WatchGuard FireBox and the Netopia router are both already correctly configured for Internet access, and are not behind a firewall, proxy server or other NAT-enabled router that may block IPSec access.
- You are running the latest version of the WatchGuard configuration software. At the time this technote was written this was version 4.10 with security pack A.

### 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\\_021](#).

### 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.

### Example Configuration:

For this example, the Netopia was set up as follows.

<b>Local WAN IP Address:</b>	163.176.56.154
<b>Local WAN IP Mask:</b>	255.255.255.0
<b>Default IP Gateway:</b>	163.176.56.1
<b>Ethernet IP Address:</b>	11.0.0.1
<b>Ethernet Subnet Mask:</b>	255.255.255.0

The WatchGuard was set up using these values:

<b>External Interface:</b>	163.176.56.181 /24*
<b>Internal Interface:</b>	192.168.1.1 /24*
<b>Default Gateway:</b>	163.176.56.1

The Optional Interface was not used.

\*The WatchGuard uses "slash notation" to reference subnet mask values. The number after the slash refers to the number of bits in the subnet mask. A /24 notation indicates a subnet mask that is 24 bits in length, which equates to 255.255.255.0 in the more traditional "dotted quad" notation. Some common values are referenced below:

255.255.255.0	= /24
255.255.255.128	= /25
255.255.255.192	= /26
255.255.255.224	= /27
255.255.255.240	= /28
255.255.255.248	= /29
255.255.255.252	= /30

Consult the WatchGuard help system for more information on slash notation.

The example configuration below uses the above values for reference. When configuring your Netopia router and WatchGuard firewall, substitute the values in your router or firewall for these numbers wherever appropriate.

### **Netopia Step-By-Step Configuration:**

1. From the **Main Menu**, go to **Quick Menus** and select **Add Connection Profile**.
2. Give the profile a descriptive name and set the **Data Link Encapsulation** to **IPSec**.
3. Arrow down to **Data Link options** and hit **ENTER**.
4. Set **Encryption Transform** to **Null** or **DES** (Null is not recommended as it offers no security). If you have 4.82 or better firmware and the optional Mezzanine VPN Accelerator card installed, you will also have an option for 3DES.
5. Enter a **16-digit hexadecimal key** in the **Encryption Key** field. For example, 1234567890ABCDEF. If you are using 3DES, you will

need to enter three keys. All three keys **MUST** be different for 3DES to work correctly.

6. For **Authentication Type**, select **Null** or **ESP**. Do not select AH (AH cannot be used because the Netopia will ALWAYS do ESP; if AH is selected in the Netopia, the Netopia will use both ESP and AH. This is not supported in the WatchGuard).
7. For **Authentication Transform**, choose **HMAC-MD5-96** or **HMAC-SHA1-96**.
8. For **Authentication Key**, enter a **32-digit hexadecimal value** (if using MD5) or a **40-digit hexadecimal value** (if using SHA1). For example, 1234567890ABCDEF1234567890ABCDEF or 1234567890123456789012345678901234567890.
9. If you have an option for **Compression** type, leave it as **None**. The WatchGuard doesn't support compression.
10. Hit **ENTER** on **COMMIT** to confirm your settings.
11. Arrow down to **IP Profile Parameters** and hit **ENTER**.
12. Set the **SPI** to a value between **257** and **1023** (the range supported by the WatchGuard).
13. **Remote Tunnel Endpoint Address** is the **External Interface** address of the WatchGuard device (163.176.56.181 in the example).
14. **Remote Members Network** is the **Internal Interface** address of the WatchGuard device (192.168.1.1 in the example). Remote members mask corresponds to the mask in use on the Internal Interface of the WatchGuard (/24 or 255.255.255.0 in the example).
15. Leave **Address Translation Enabled** to **NO** and **Filter Set** to **NONE**. Leave the Advanced IP Profile Options alone.
16. Hit **ENTER** on **COMMIT** to set the **IP Profile parameters**, then **ENTER** on **COMMIT** again to complete the setup of the IPSec profile.

This completes the configuration of the Netopia router.

### WatchGuard Step-by-Step Configuration:

1. Open the **WatchGuard Policy Manager**.
2. Select the **Network** menu, **Branch Office VPN** -> **IPSec** selection.
3. Click on **Gateways**. The **IPSec Gateway** window will appear. Click **Add**.
4. Supply a descriptive name. Set **key negotiation type** to **Manual**.
5. Set **Remote IP Gateway** to the **Local WAN Address** of the Netopia (163.176.56.154 in the example). Click **OK**.
6. Click on **Tunnels**. The **Configure Tunnels** window will appear. Click **Add**.
7. Select the **Gateway** representing the Netopia router. Click **OK**.
8. Supply a **Name** for the tunnel in the Identity tab then click on **Manual Security**.
9. Click on **Settings**. For **Incoming**, select Use **ESP**.
10. Set the **SPI** to the *exact same* value as was used in **Step 12** of the Netopia Configuration above. Both the Netopia and the WatchGuard store their SPI's in binary format, so no conversion is required.
11. Set **Encryption** to match the **Encryption Transform** setting specified in **Step 4** of the Netopia configuration above. Set the

- Encryption Key** to be identical to that entered in **Step 5** of the Netopia Configuration above. If 3DES is used, note that the WatchGuard stores all three keys on a single line.
12. Set **Authentication** to match the **Authentication Transform** setting specified in **Step 7** of the Netopia configuration above.
  13. Set the **Authentication Key** to the identical key used in **Step 8** of the Netopia configuration above.
  14. Do **NOT** select Use **AH**.
  15. Make sure that **Use Incoming Settings for Outgoing** is selected, and leave the Outgoing tab alone.
  16. Click **OK** to all the open windows until you are back at the **Policy Manger**.
  17. Click on the **Add Service** button. The Services window appears. Open the **Packet Filters** folder and select **ANY**.
  18. Click **OK** to the **Add Service Dialog**. The **ANY** properties dialog appears.
  19. In the **Incoming Tab**, set **Incoming Connections are...** to **Enabled and Allowed**.
  20. In the **From** window, click **Add**. The Add Address dialog appears. Select **Add Other**.
  21. Set **Choose Type** to **Network IP Address**. For **Value**, enter the **Ethernet IP Address** of the Netopia, with the appropriate slash-notation value for the Ethernet Subnet Mask of the Netopia. In the example, this is 11.0.0.0 (this is technically the network number; if you attempt to enter 11.0.0.1, the WatchGuard will give you an error message) /24. Click OK.
  22. Click **OK** in the **Add Address** dialog window.
  23. In the **To** window, click **add**. Select **Trusted from the Members** window and click on **OK**.
  24. Click on the **Outgoing Tab**. Set the **Outgoing Connections are** setting to **Enabled and Allowed**. In the From window, click on **Add**. The Add Address dialog appears.
  25. In the **Members section**, select **Trusted**. Click on **Add** then click on **OK**.
  26. In the **To** window, click on **Add**. The Add Address dialog appears.
  27. Select **Add Other**. Set the **Type and Value** to be identical to **Step 21** in this section. Click **OK**. Click **OK** to the ANY Properties screen.
  28. Close the **Services** dialog. The **ANY** service, with the network settings you specified should appear at the top of the **Policy Manager** list.
  29. Click on the **Save to FireBox** icon. Follow the prompts, entering your **write access password** to the WatchGuard when prompted, and follow all prompts until it has rebooted.

This completes the configuration of the WatchGuard FireBox.

The IPSec tunnel between your Netopia router and WatchGuard FireBox is now complete. You can verify the connection by looking in the Netopia's Quick View -> VPN Quick View screen. If you intend to use Windows Networking (Network Neighborhood, File & Printer Sharing, etc), please see the following technotes for issues regarding Windows Networking across a WAN connection:

[NIR\\_028: Windows Peer to Peer Networking](#)

[NIR\\_030: Windows to NT Networking](#)