

VPN Tunnels with Routers

Notice on Configuring VPN Tunnels with Netopia Routers

Before you attempt to make a VPN connection, confirm your Netopia router configuration conforms to these guidelines:

- A. If you plan to do Windows networking across your VPN, you should have the **Netbios Filter** DISABLED in your Internet **Connection Profile**. To check what **Filter Set** you have enabled, follow these steps from the Main Menu:
 1. Go to **WAN Configuration**
 2. Select **Display/Change Connection Profile**
 3. Select your Internet profile
 4. Select **IP Profile Parameters**
 5. For **Filter Set**, the name listed is the name of the **Filter Set** enabled.
 6. To remove the **Filter Set**, simply select **Remove Filter Set**, and you will see the **Filter Set** name disappear.

(*Note:* For R9100 routers, ignore steps 2 and 3 and select **WAN Setup** instead.)

- G. You should have NO PPTP or IPSec (port 500)**Servers** added to your enabled **NAT Server List**. To check what **NAT Server List** you have enabled, follow these steps from the Main Menu:
 1. Go to **WAN Configuration**
 2. Select **Display/Change Connection Profile**
 3. Select your Internet profile
 4. Select **IP Profile Parameters**
 5. For **NAT Server List...**, the name listed is the name of the **NAT Server List** enabled.

(*Note:* Again, for R9100 routers, ignore steps 2 and 3 and select **WAN Setup** instead.)

To check what **Servers** you have added to your enabled **NAT Server List**, follow these steps from the Main Menu:

1. Go to **Quick Menus**
2. Select **Network Address Translation**
3. Select **Show/Change Server List...**
4. Select your enabled **NAT Server List** (the name from the previous step 4).
5. Select **Show/Change Server...** and your list of active **Servers** will appear. (*Note! If you do not have a **Show/Change Server** option and only see **Add Servers**, you should be fine and do not have any PPTP or IPSec Servers and can move on to the next step*)
6. Once again, confirm there are NO PPTP servers or servers encompassing port 500 (for IPSec) listed. If so, remove the **Server** by hitting your escape key once, select **Delete Server**, and select the **PPTP Server**.

- G. If you have **Input Filters** added to an enabled **Filter Set** (see A above to find out what **Filter Set** you have enabled), you need to include input rules to allow the protocols used by your VPN tunnel. For PPTP tunnels, you will need to allow both TCP port 1723 and GRE, as show below in Figure A. For ATMP tunnels, you will need to allow UDP port 5150 and GRE, shown in Figure B. For IPSec VPN connections you will need to allow UDP 500 as well as protocols 50 and 51 as shown in Figure C.

Figure A - PPTP Filter

#	Source IP Addr	Dest IP Addr	Proto	Src Port	D Port	On?	Fwd?
1	0.0.0.0	0.0.0.0	TCP	NC	=1723	Yes	Yes
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes

Figure B - ATMP Filter

#	Source IP Addr	Dest IP Addr	Proto	Src,Port	D,Port	On?	Fwd?
1	0.0.0.0	0.0.0.0	UDP	NC	=5150	Yes	Yes
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes

Figure C - IPsec Filter

#	Source IP Addr	Dest IP Addr	Proto	Src,Port	D,Port	On?	Fwd?
1	0.0.0.0	0.0.0.0	UDP	NC	=500	Yes	Yes
2	0.0.0.0	0.0.0.0	50	--	--	Yes	Yes
3	0.0.0.0	0.0.0.0	51	--	--	Yes	Yes

Now that you know what **Filter Set** you have enabled (see the first bullet), you can add input rules to the **Input Filter** of your enabled **Filter Set** by following these steps from the Main Menu:

1. Go to **Quick Menus**
2. Select **IP Filter Sets**
3. Select **Display/Change IP Filter Set**
4. Select your enabled **Filter Set**
5. Select **Add Input Filter to Filter Set...**
6. To configure an **Input Filter** for PPTP, enter the following parameters:

```

Change Input Filter 1

Enabled:                Yes
Forward:                Yes

Source IP Address:      0.0.0.0
Source IP Address Mask: 0.0.0.0

Dest. IP Address:       0.0.0.0
Dest. IP Address Mask: 0.0.0.0

Protocol Type:          TCP
Source Port Compare...  No Compare
Source Port ID:         0
Dest. Port Compare...   Equal
Dest. Port ID:          1723
Established TCP Conns. Only: No

Return/Enter accepts * Tab toggles * ESC cancels.
Enter the packet specific information for this filter.
    
```

To configure an **Input Filter** for ATMP, enter the following parameters:

```

                                Add Input Filter

Enabled;                          Yes
Forward;                           Yes

Source IP Address;                 0.0.0.0
Source IP Address Mask;            0.0.0.0

Dest. IP Address;                  0.0.0.0
Dest. IP Address Mask;             0.0.0.0

Protocol Type;                     UDP
Source Port Compare...             No Compare
Source Port ID;                    0
Dest. Port Compare...              Equal
Dest. Port ID;                     5150

ADD THIS FILTER NOW                CANCEL

Return/Enter accepts * Tab toggles * ESC cancels.
Enter the packet specific information for this filter.

```

To configure an **Input Filter** for GRE (for both ATMP and PPTP filter sets), enter the following parameters:

```

                                Add Input Filter

Enabled;                          Yes
Forward;                           Yes

Source IP Address;                 0.0.0.0
Source IP Address Mask;            0.0.0.0

Dest. IP Address;                  0.0.0.0
Dest. IP Address Mask;             0.0.0.0

Protocol Type;                     GRE

ADD THIS FILTER NOW                CANCEL

Return/Enter accepts * Tab toggles * ESC cancels.
Enter the packet specific information for this filter.

```

To configure an **Input Filter** for IKE (for an IPSEC filter set) enter the following parameters:

```

                                Change Input Filter 1

Enabled;                          Yes
Forward;                           Yes

Source IP Address;                 0.0.0.0
Source IP Address Mask;            0.0.0.0

Dest. IP Address;                  0.0.0.0
Dest. IP Address Mask;             0.0.0.0

Protocol Type;                     UDP
Source Port Compare...             No Compare
Source Port ID;                    0
Dest. Port Compare...              Equal
Dest. Port ID;                     500

Return/Enter accepts * Tab toggles * ESC cancels.
Enter the packet specific information for this filter.

```

To configure an **Input Filter** for ESP (for an IPSEC filter set) enter the following parameters:

```

                                Change Input Filter 2

Enabled;                          Yes
Forward;                           Yes

Source IP Address;                 0.0.0.0

```

```
Source IP Address Mask:      0,0,0,0
Dest. IP Address:           0,0,0,0
Dest. IP Address Mask:      0,0,0,0

Protocol Type:              50
```

Return/Enter accepts * Tab toggles * ESC cancels.
Enter the packet specific information for this filter.

To configure an **Input Filter** for AH (for an IPSEC filter set) enter the following parameters:

Change Input Filter 3

```
Enabled:                    Yes
Forward:                    Yes

Source IP Address:          0,0,0,0
Source IP Address Mask:     0,0,0,0

Dest. IP Address:           0,0,0,0
Dest. IP Address Mask:      0,0,0,0

Protocol Type:              51
```

Return/Enter accepts * Tab toggles * ESC cancels.
Enter the packet specific information for this filter.