Packet Filtering Setup Guide

(3GM1WN)

Packet Filtering

The Packet Filter enables you to control what packets are allowed to pass through the router. There are two types of packet filter, the "Outbound Packet Filter" which applies to all outbound packets and the "Inbound Packet Filter" which only applies to packets that are destined for a Virtual Server or DMZ host only.

There are two types of filtering policies:

1. Allow all data through the router except data that matches the specified rules.
2. Deny all data through the router except data that matches the specified rules.

For each direction, you can specify up to 48 rules. For each rule you will need to define the following:

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol: TCP or UDP or both.
- Use Schedule Rule#

For source or destination IP address, you can define a single IP address (192.168.1.1) or a range of IP addresses (192.168.1.100-192.168.1.200). Empty fields imply all IP addresses.

For source or destination port, you can also define a single port (80) or a range of ports (1000-1999). Use the prefix "T" or "U" to specify either the TCP or UDP protocol e.g. T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty field implies all ports.

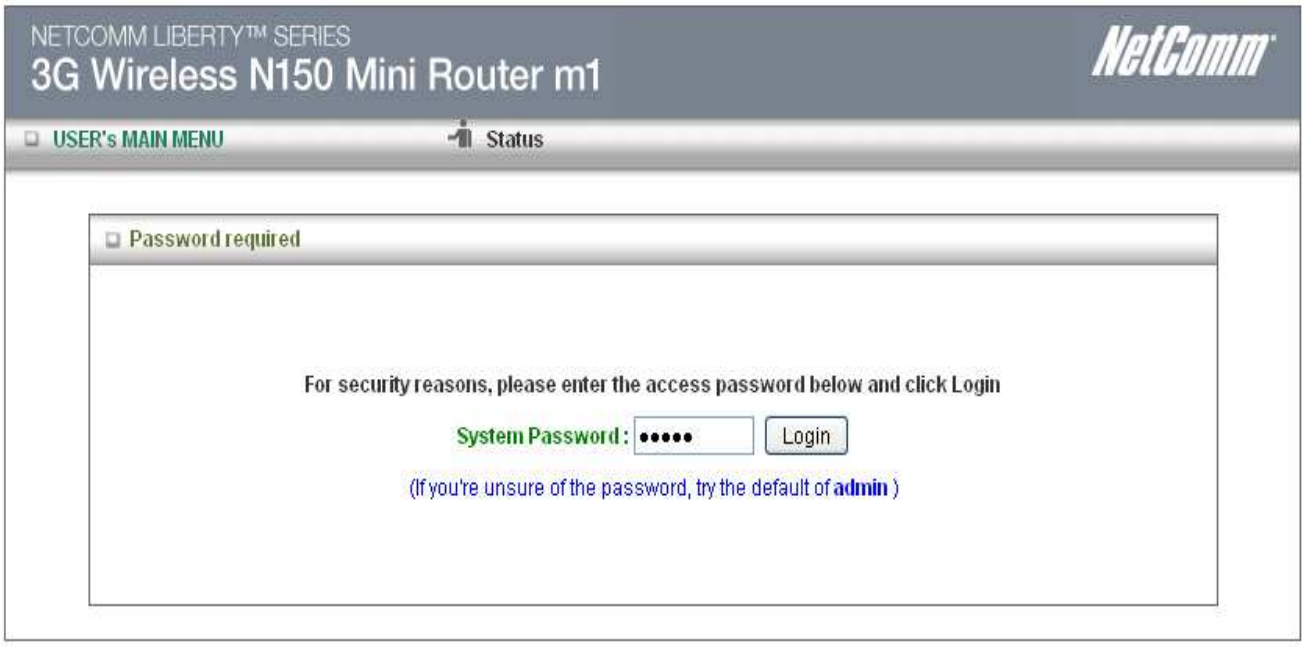
Adding a Packet Filter Rule

This guide will take you through the steps required to add a packet filter rule to your modem / router.

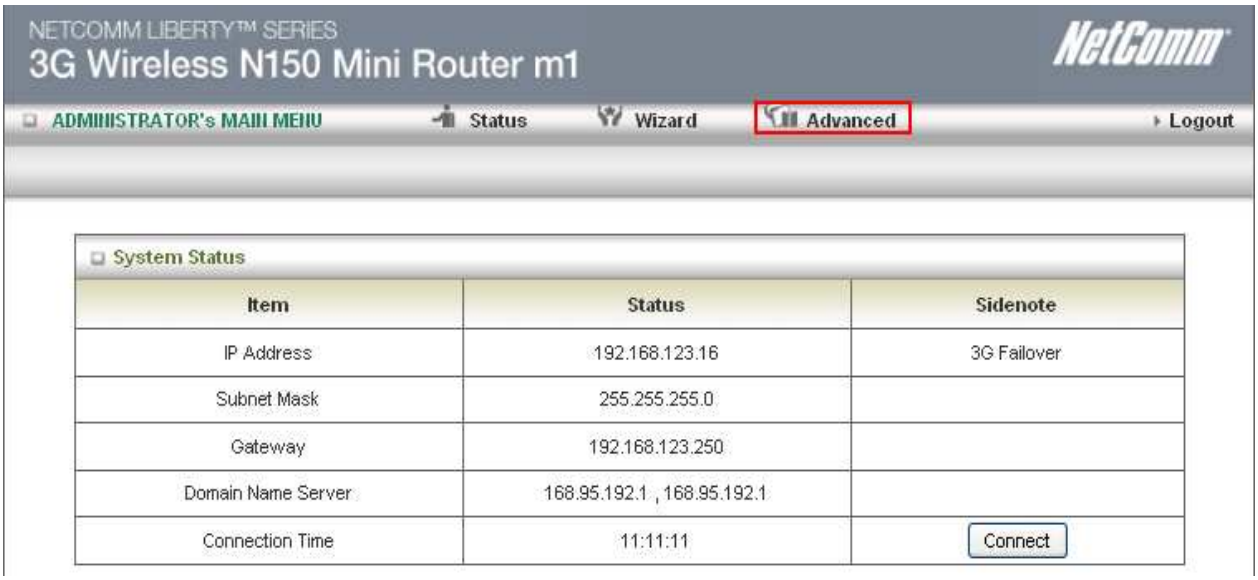
1. Before you can set up port forwarding rules with the 3GM1WN you will need to be connected to the 3GM1WN via wireless connection. Please see the 3GM1WN Wireless Setup Guide for instructions on connecting via wireless to the 3GM1WN.

2. Once you are connected to the 3GM1WN navigate to http://192.168.1.1 in a web browser.

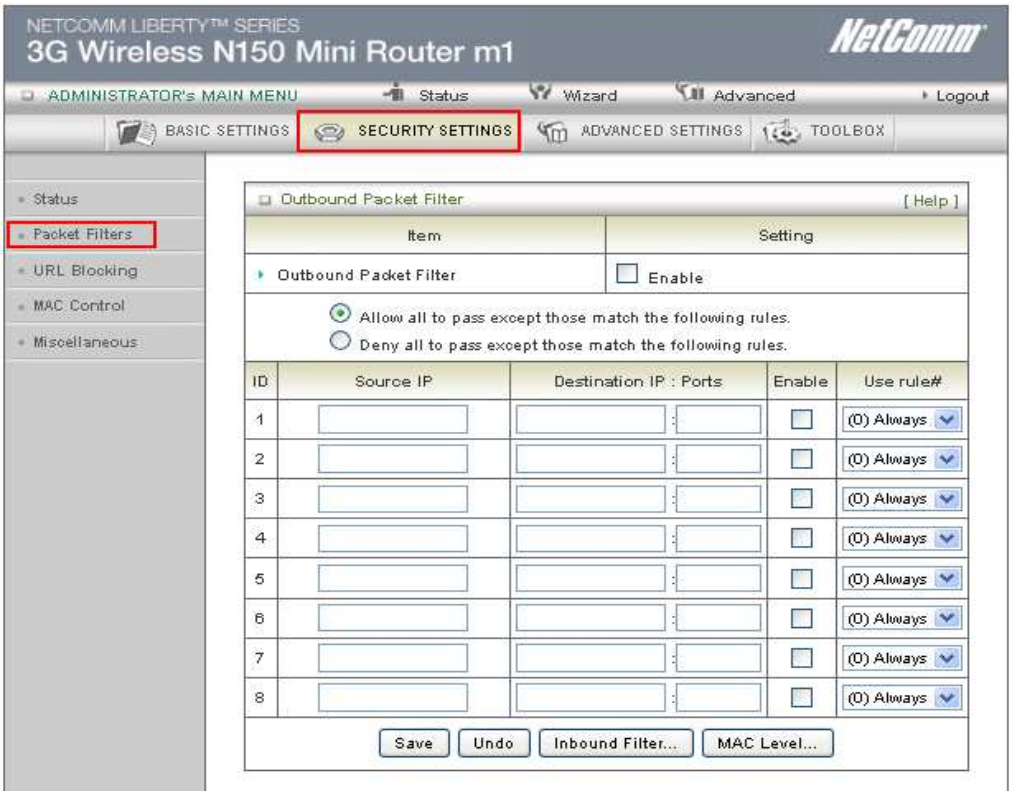
3. Enter '**admin**' as the system password and press the '**Login**' button.



4. Select the '**Advanced**' option from the Administrator's Main Menu.

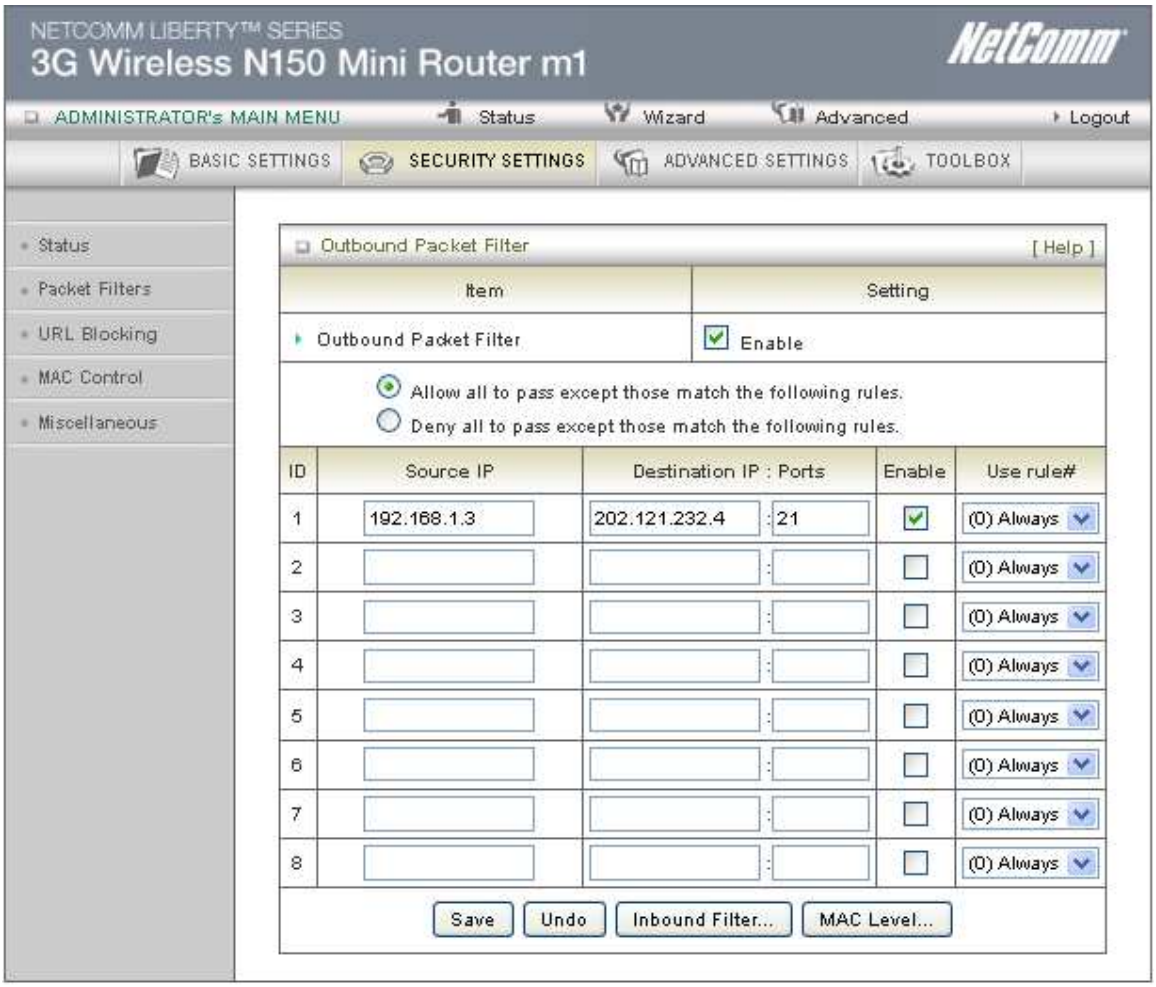


5. Select '**Security Settings**', then '**Packet Filters**' from the left hand side menu.



6. The outbound packet filter screen as shown above will be displayed. If you wish to create an inbound packet filter, that is inbound from the internet, press the Inbound Filter button.

7. Tick the **Enable** checkbox for either the Inbound or Outbound Packet filter.



8. Select **Allow all** or **Deny all** to allow or deny data packets access through the router for a given packet filter rule you are to create.

9. Enter the **Source IP** Address. For an Outbound Packet Filter rule this will be a local address in the range of 192.168.1.2 to 192.168.1.254, for those devices connected to the 3GMiWn. For an Inbound Packet Filter rule this will be a WAN IP address (an internet address) from where the packets are to originate.

10. Enter the destination IP address and associated port(s). For an Outbound Packet Filter rule this will be a a WAN IP address (an internet address) from where the packets are to originate. For an Inbound Packet Filter rule this will be a local IP address, in the range of 192.168.1.2 to 192.168.1.254, for those IP addresses in use by the devices

connected to the 3GM1WN. The example above shows an outbound packet filter rule for a local device using 192.168.1.3 connecting to a server over the internet at 202.121.232.4 using port 21, commonly used by the FTP protocol.

11. Tick the Enable checkbox to enable the packet filtr rule. Alternatively you can untick the Enable checkbox to disable the rule.

12. Set the condition for using the rule, by default set to Always.

13. Press Save to save the packet filter (port forwarding) rule(s).