NetCommWireless

# Remote HTTP access from a single IP address

**Note:** This document is subject to change without notice.

This document covers the following products:

NetComm Wireless VDSL/ADSL WiFi Gigabit Modem Router (NF4V)

NetComm Wireless VDSL/ADSL WiFi Modem Router (NF10W)

NetComm Wireless VDSL/ADSL N300 WiFi Modem Router with VoIP (NF10WV)

NetComm Wireless VDSL/ADSL Dual Band AC1600 Gigabit WiFi Modem Router with VoIP (NF17ACV)

NetComm Wireless VDSL/ADSL AC1600 WiFi Gigabit Modem Router (NF8AC)

| DOCUMENT DESCRIPTION | DATE |
|---|---|
| 1.0 - Initial document release | 14 December 2016 |

*Table i - Document revision history*

# Overview

To enhance the security of your router, you can restrict the IP addresses that can access your router remotely via HTTP. This guide explains how to allow one remote IP address to access the router from the WAN interface.

## Setup process variations

On the NF4V you achieve this by setting up a firewall and then making a rule with an exception for the IP address that you want to allow access from.

On the NF10WV and NF17ACV, when a firewall is enabled on a WAN or LAN interface, all incoming IP traffic is blocked by default. You must set up an IP Filter for the IP traffic from your designated IP address to be accepted through the firewall.

# NF4V

## Enable WAN Access

The first step is to enable the WAN Access, in this example: Web and Telnet

1 Select **Management -> Access Control -> Services Control** to open the **Access Control - - Services** page.

2 Check the enable checkbox in the **WAN** column for **HTTP > WAN: ☑ enable**

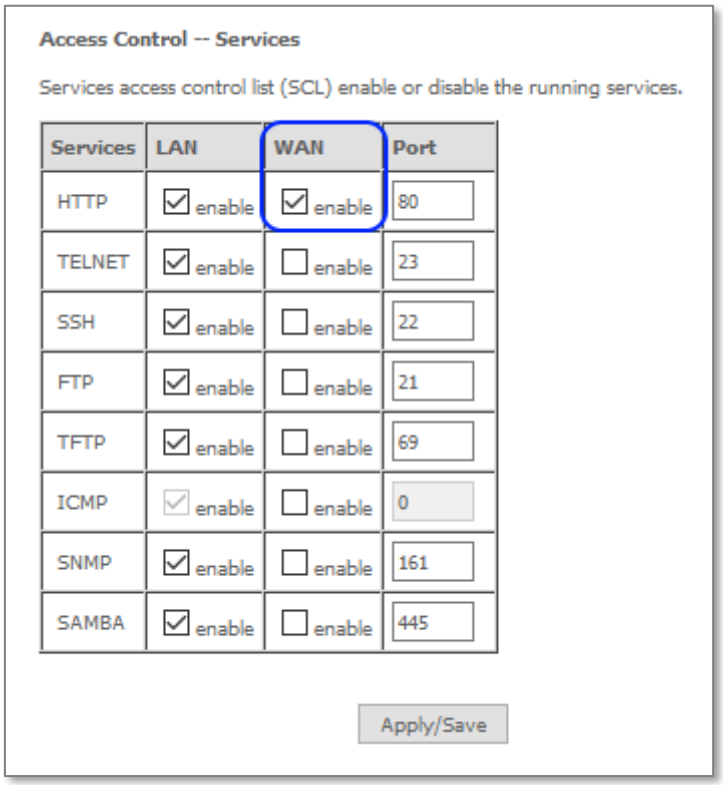


*Figure 1 – Enable WAN service*

3 Click **Apply/Save**.

The next steps are to set up a Firewall and then create a Firewall Rule that restricts access to the single IP address.

## Set up Firewall

1 Go to **Advanced Setup -> Security -> Firewall** and click the **Add Firewall** button:

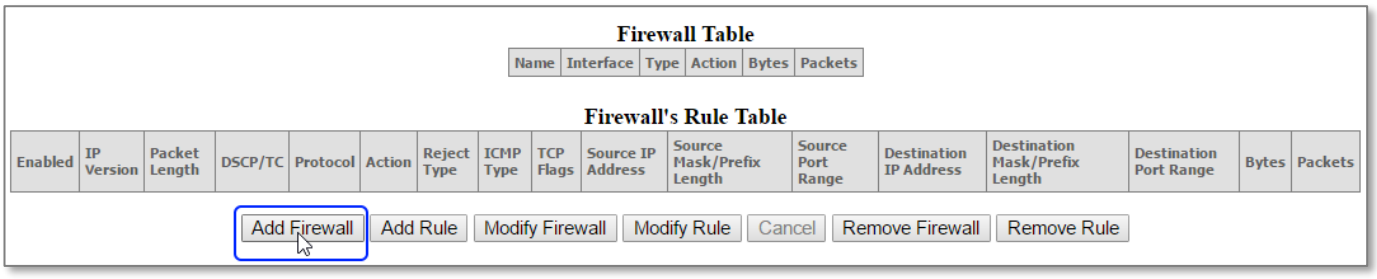


*Figure 2 – Add Firewall button*

2 In the **Add Firewall** page, enter a unique **Name** and accept the default settings for **Interface (WAN)**, **Type (In)** and **Action (Drop)**.

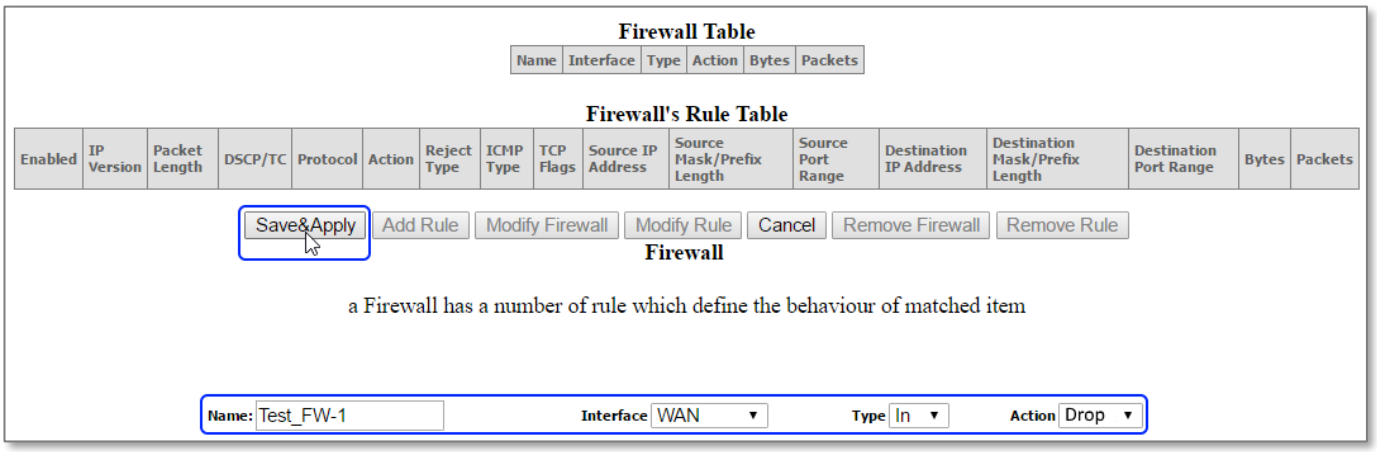


*Figure 3 – Define Firewall*

| Field name | Value | Description/explanation |
|---|---|---|
| **Name** | *Your choice* | We recommend that you use a name that indicates that it is a firewall. |
| **Interface** | WAN | Set the interface type to WAN. |
| **Type** | In | Set the firewall to block all inward messages. |
| **Action** | Drop | Set the firewall's Action to "Drop", meaning all incoming messages will be ignored, unless a rule allowing a specific IP Address is created. See the next section. |

*Table 1 – Add Firewall parameter fields*

3 Click **Save&Apply** and the new firewall will be added to the Firewall Table:

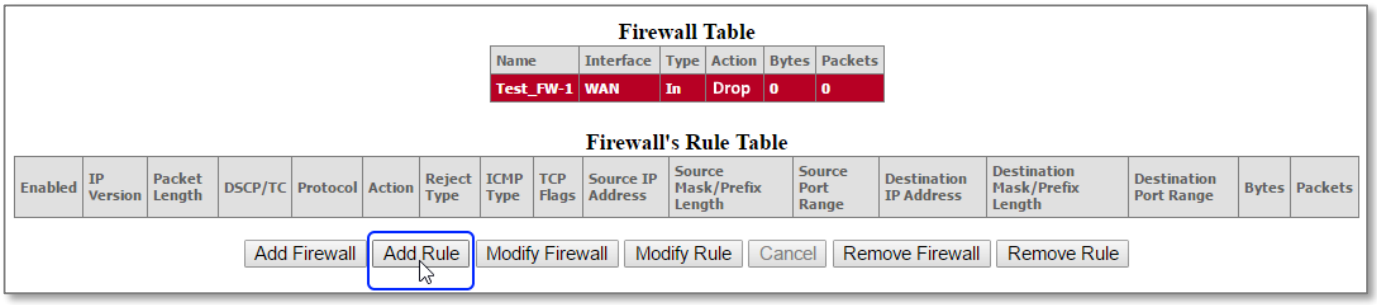


*Figure 4 – All Firewall Rule button*

## Set up Firewall Rule

1 Click the **Add Rule** button.

2 In the **Add Firewall Rule** page, set up the firewall rule as follows (regardless of the port number on Step 1):

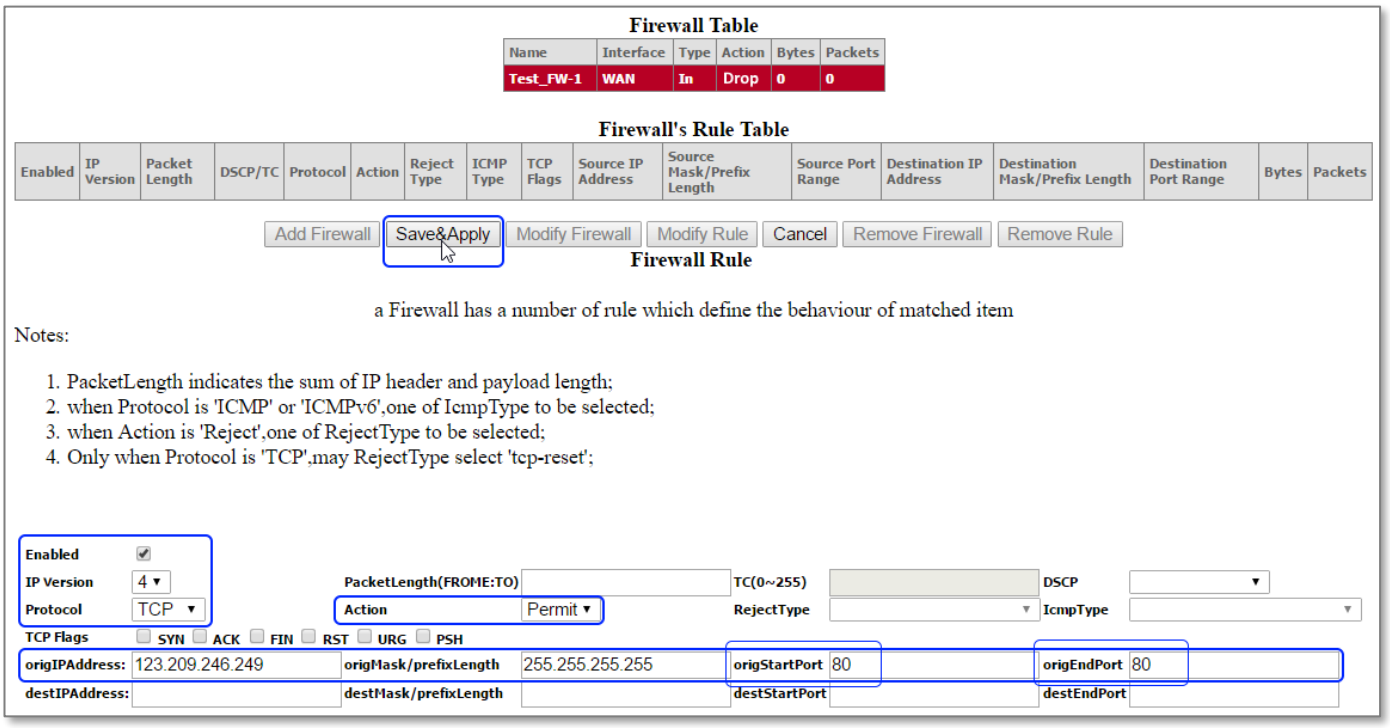


*Figure 5 – Define Firewall Rule*

| Field name | Value | Description/explanation |
|---|---|---|
| **Enabled** | ☑ (yes) | The rule is active and will be applied to the firewall.<br>Note that rather than using the **Remove Rule** button which will delete the rule, you can disable it. Disabled rules can be used again by enabling them. |
| **IP Version** | 4 | Select "4" to use IPv4. |
| **Protocol** | TCP or UDP | Select "TCP" or "UDP" |
| **Action** | Permit | Select Action = "Permit", this allows the rule to have an exception to the Firewall setting of Action = "Drop" |
| **origIPAddress** | 123.209.246.249 | This is the "originating IP Address" that a request for entry comes from, that is the remote WAN IP address that you want this rule to allow through the firewall so that only it can connect to the router.<br>You can change it at any time. |
| **origMask/ prefix Length** | 255.255.255.255 | Leave as "255.255.255.255" |
| **origStartPort** | 80 | These two settings are used to define the "Source Port Range".<br>When the start (80) and end (80) of the range are the same, access is limited to a single port only, in this example Port 80. |
| **origEndPort** | 80 | |

*Table 2 – Add Firewall Rule fields*

3 Click **Apply/Save**.

The Rule will now be listed in the **Firewall's Rule Table**:

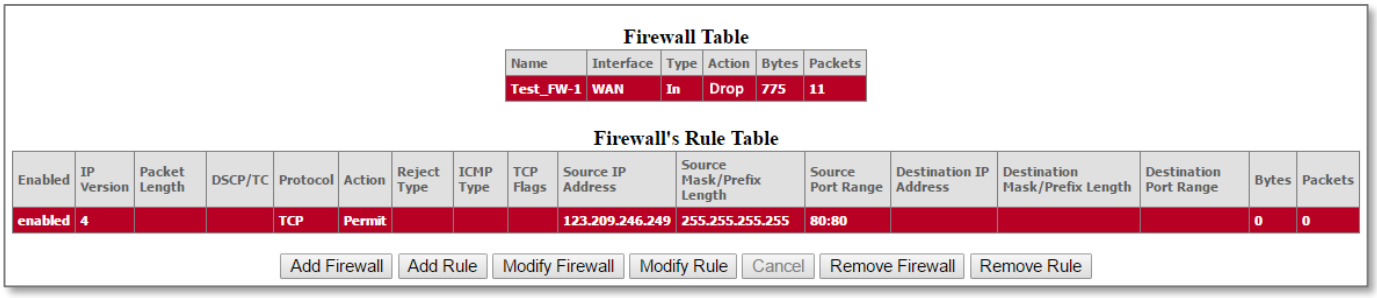


*Figure 6 – Firewall Rule Table*

To change the **Source IP Address** click the **Modify Rule** button?

# NF10W, NF10WV, NF17ACV and NF8AC

To allow only one remote IP address to access the NF10WV and NF17ACV, do the following:

## Disable WAN access

The first step is to disable global WAN access via HTTP. To disable global WAN access via HTTP:

1 Go to **Management > Access Control > Services Control** and make sure that WAN access is disabled by unchecking the HTTP / WAN checkbox.

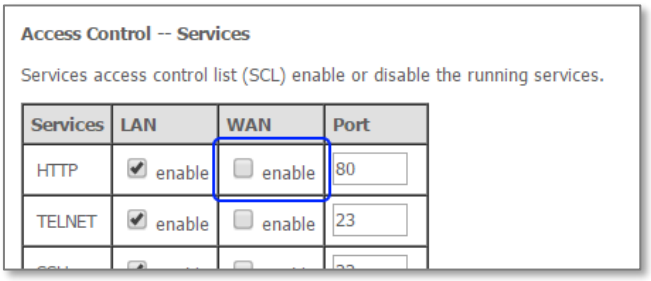


*Figure 7 - Disabling WAN access control*

2 Click **Apply/Save**.

## Add an Incoming IP Filter

3 Go to **Advanced Setup > Security > IP Filtering > Incoming** to create a filter:

4 Click the **Add** button to open the **Add IP Filter – Incoming** page:

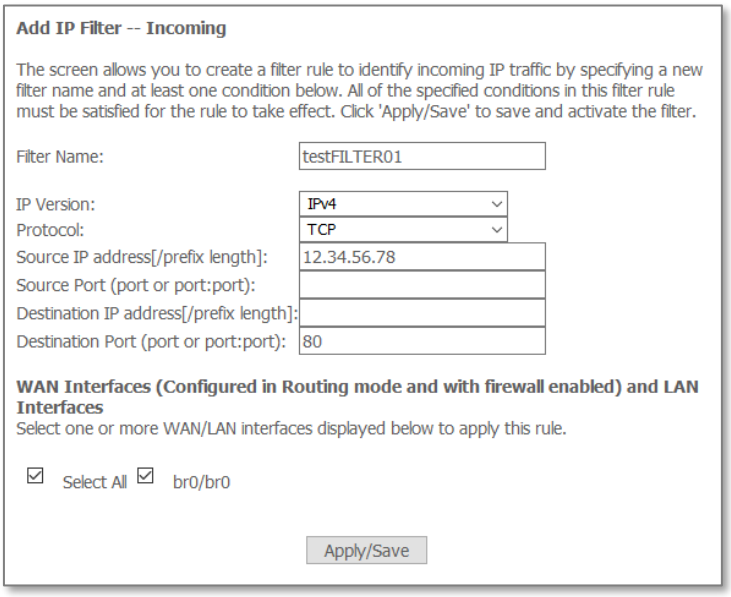


*Figure 8 – Add IP Filter – Incoming settings*

Enter the details as described in the table below.

| Field name | Value | Description/explanation |
|---|---|---|
| **Filter Name** | *Your choice* | We recommend that you use a name that indicates that it is a filter. |
| **IP Version** | Options:<br>IPv4<br>IPv6 | Select IPv4 |
| **Protocol** | Options:<br>TCP/UDP<br>TCP<br>UDP<br>ICMP | Select TCP |
| **Source IP address** [/prefix length] | For example: 12.34.56.78 | This is the "originating IP Address" that a request for entry comes from, that is, the remote WAN IP address that you want to allow through the firewall so that only it can connect to the router. |
| **Source Port** [port or port:port] | | Leave empty. |
| **Destination IP address** [/prefix length] | | Leave empty. |
| **Destination Port** [port or port:port] | 80 | The port that messages are allowed through to access the router. |

| Field name | Value | Description/explanation |
|---|---|---|
| **WAN/LAN Interfaces that this rule applies to** | | |
| **Select All** | ☑ (yes) | Use **Select All**, this will check all three checkboxes. |
| **br0/br0** | ☑ (yes) | See above. |

*Table 3 – Add Firewall Rule fields*

5 Click **Apply/Save**.

The new filter will now be listed in the **Incoming IP Filtering Setup** table:

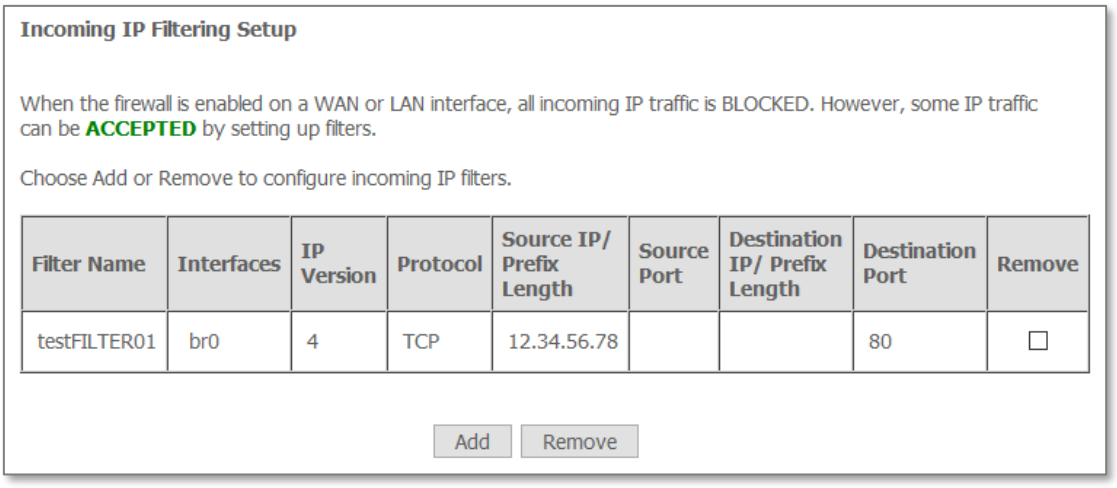


*Figure 9 – Add IP Filter – Incoming settings*

The router is now accessible from the Source IP address.