

Remote HTTP access from a single IP address

Copyright

Copyright© 2016 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless.

Trademarks and registered trademarks are the property of NetComm Wireless Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.



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 1 - 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**

Access Control -- Services

Services access control list (SCL) enable or disable the running services.

Services	LAN	WAN	Port
HTTP	<input checked="" type="checkbox"/> enable	<input checked="" type="checkbox"/> enable	80
TELNET	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	23
SSH	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	22
FTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	21
TFTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	69
ICMP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	0
SNMP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	161
SAMBA	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	445

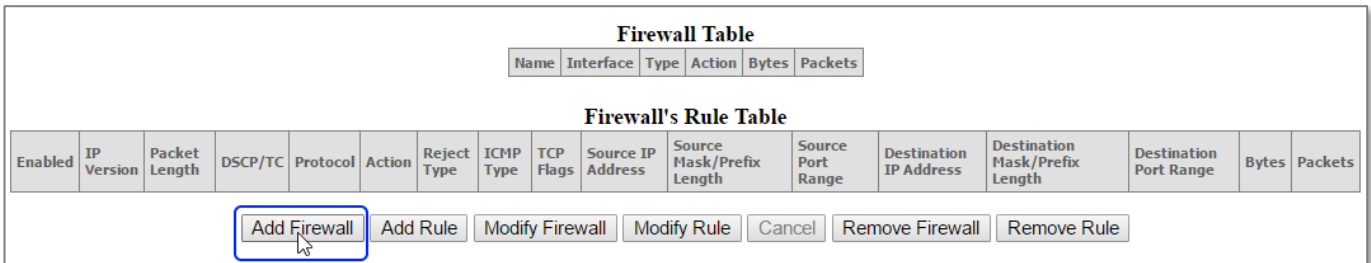
Figure 1 – Enable WAN service

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

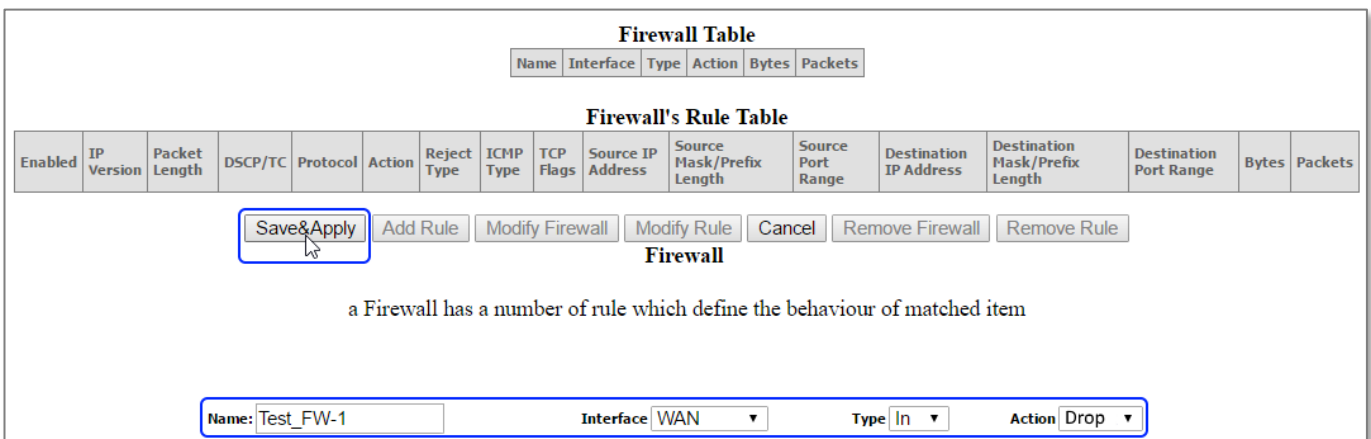
1 Go to **Advanced Setup -> Security -> Firewall** and click the **Add Firewall** button:



The screenshot shows the 'Firewall Table' and 'Firewall's Rule Table' sections. The 'Add Firewall' button is highlighted with a red box. Below the tables are buttons for 'Add Rule', 'Modify Firewall', 'Modify Rule', 'Cancel', 'Remove Firewall', and 'Remove Rule'.

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)**.



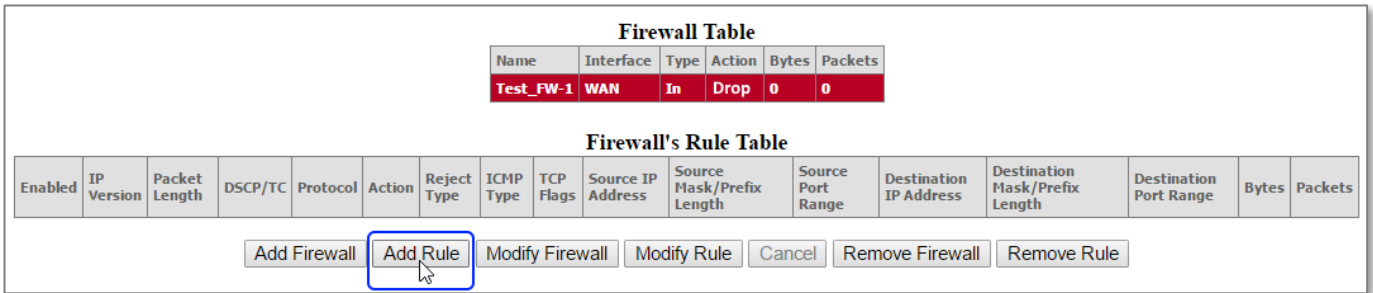
The screenshot shows the 'Add Firewall' page with the 'Save & Apply' button highlighted. The form fields are filled out as follows: Name: Test_FW-1, Interface: WAN, Type: In, Action: Drop. Below the form, there is a note: 'a Firewall has a number of rule which define the behaviour of matched item'.

Figure 3 – Define Firewall

Field name	Value	Description/explanation
Name	<i>Your choice</i>	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:



Firewall Table

Name	Interface	Type	Action	Bytes	Packets
Test_FW-1	WAN	In	Drop	0	0

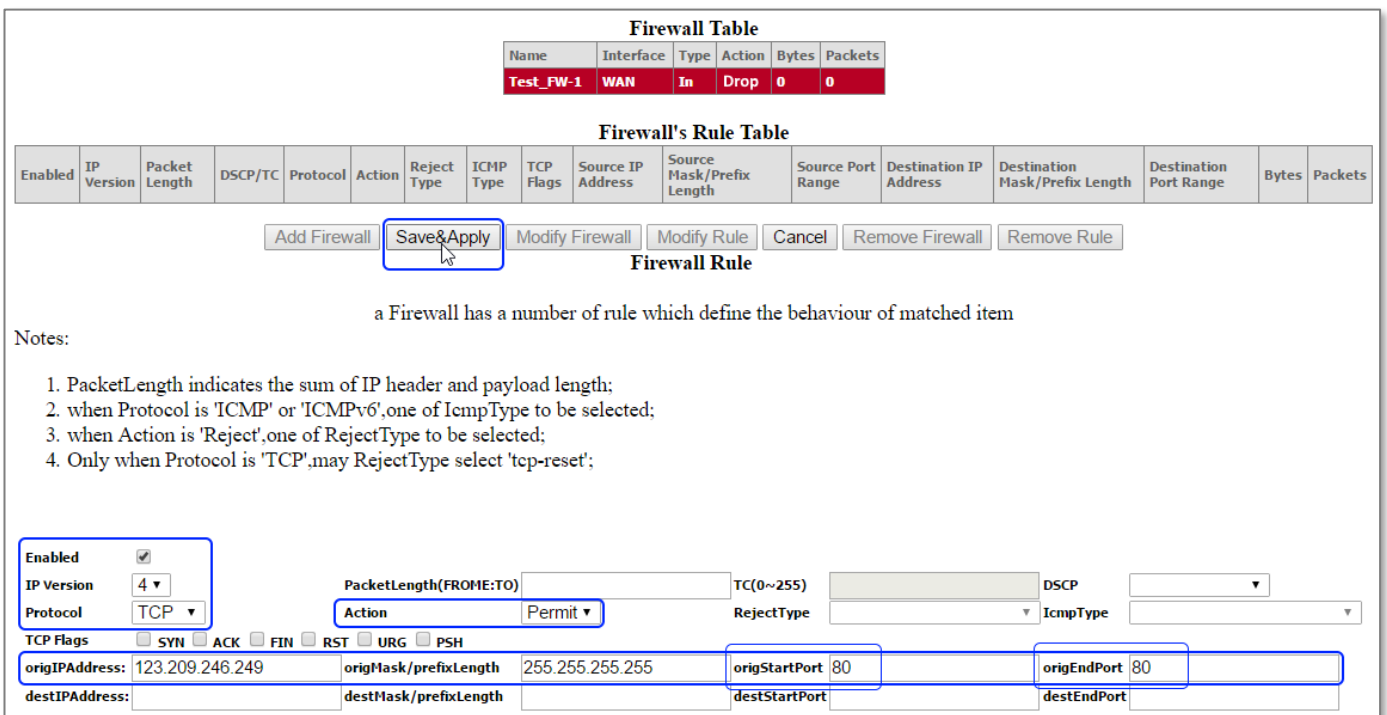
Firewall's Rule Table

Enabled	IP Version	Packet Length	DSCP/TC	Protocol	Action	Reject Type	ICMP Type	TCP Flags	Source IP Address	Source Mask/Prefix Length	Source Port Range	Destination IP Address	Destination Mask/Prefix Length	Destination Port Range	Bytes	Packets
<input type="button" value="Add Firewall"/> <input style="border: 2px solid blue;" type="button" value="Add Rule"/> <input type="button" value="Modify Firewall"/> <input type="button" value="Modify Rule"/> <input type="button" value="Cancel"/> <input type="button" value="Remove Firewall"/> <input type="button" value="Remove Rule"/>																

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):



Firewall Table

Name	Interface	Type	Action	Bytes	Packets
Test_FW-1	WAN	In	Drop	0	0

Firewall's Rule Table

Enabled	IP Version	Packet Length	DSCP/TC	Protocol	Action	Reject Type	ICMP Type	TCP Flags	Source IP Address	Source Mask/Prefix Length	Source Port Range	Destination IP Address	Destination Mask/Prefix Length	Destination Port Range	Bytes	Packets
<input type="button" value="Add Firewall"/> <input style="border: 2px solid blue;" type="button" value="Save&Apply"/> <input type="button" value="Modify Firewall"/> <input type="button" value="Modify Rule"/> <input type="button" value="Cancel"/> <input type="button" value="Remove Firewall"/> <input type="button" value="Remove Rule"/>																

Firewall Rule

a Firewall has a number of rule which define the behaviour of matched item

Notes:

1. PacketLength indicates the sum of IP header and payload length;
2. when Protocol is 'ICMP' or 'ICMPv6', one of IcmpType to be selected;
3. when Action is 'Reject', one of RejectType to be selected;
4. Only when Protocol is 'TCP', may RejectType select 'tcp-reset';

Configuration fields:

- Enabled:
- IP Version: 4
- Protocol: TCP
- Action: Permit
- origIPAddress: 123.209.246.249
- origMask/prefixLength: 255.255.255.255
- origStartPort: 80
- origEndPort: 80

Figure 5 – Define Firewall Rule

Field name	Value	Description/explanation
Enabled	<input checked="" type="checkbox"/> (yes)	The rule is active and will be applied to the firewall. 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. 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".
origEndPort	80	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.

Table 2 – Add Firewall Rule fields

3 Click **Apply/Save**.

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

Firewall Table															
Name	Interface	Type	Action	Bytes	Packets										
Test_FW-1	WAN	In	Drop	775	11										

Firewall's Rule Table																
Enabled	IP Version	Packet Length	DSCP/TC	Protocol	Action	Reject Type	ICMP Type	TCP Flags	Source IP Address	Source Mask/Prefix Length	Source Port Range	Destination IP Address	Destination Mask/Prefix Length	Destination Port Range	Bytes	Packets
enabled	4			TCP	Permit				123.209.246.249	255.255.255.255	80:80				0	0

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.

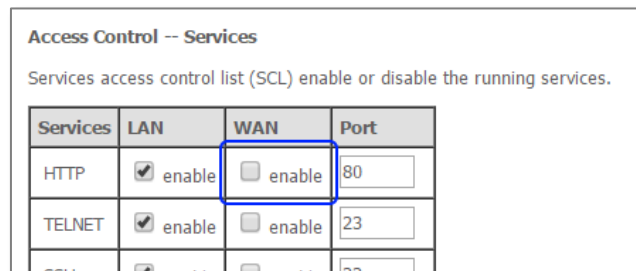
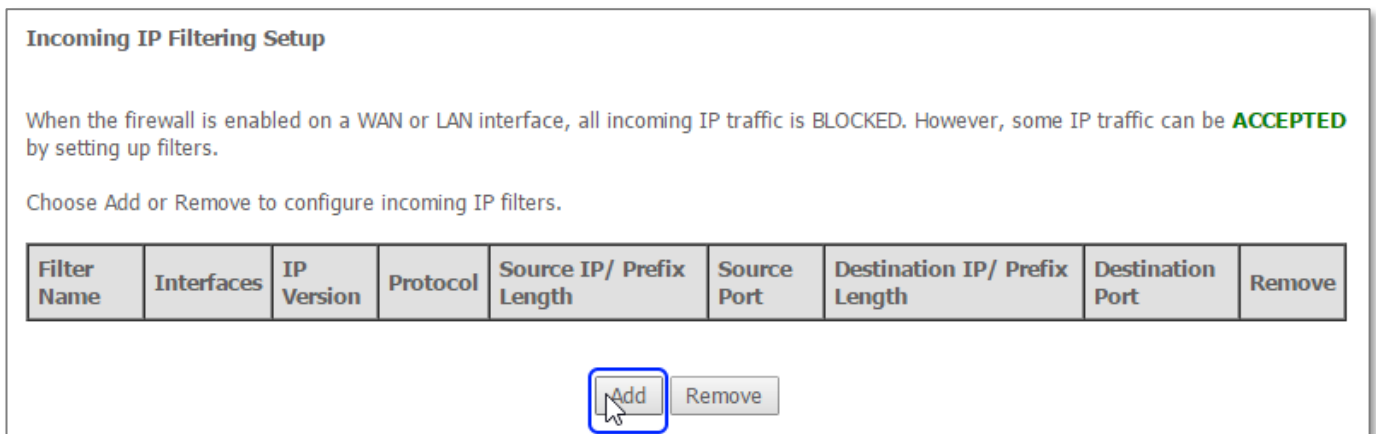


Figure 7 - Disabling WAN access control

- 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:

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces
 Select one or more WAN/LAN interfaces displayed below to apply this rule.

Select All br0/br0

Figure 8 – Add IP Filter – Incoming settings

Enter the details as described in the table below.

Field name	Value	Description/explanation
Filter Name	<i>Your choice</i>	We recommend that you use a name that indicates that it is a filter.
IP Version	Options: IPv4 IPv6	Select IPv4
Protocol	Options: TCP/UDP TCP UDP 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	<input checked="" type="checkbox"/> (yes)	Use Select All , this will check all three checkboxes.
br0/br0	<input checked="" type="checkbox"/> (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:

Incoming IP Filtering Setup

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	Interfaces	IP Version	Protocol	Source IP/ Prefix Length	Source Port	Destination IP/ Prefix Length	Destination Port	Remove
testFILTER01	br0	4	TCP	12.34.56.78			80	<input type="checkbox"/>

Figure 9 – Add IP Filter – Incoming settings

The router is now accessible from the Source IP address.