Port Forwarding Overview

Port forwarding enables programs or devices running on your LAN to communicate with the internet as if they were directly connected. This is most commonly used for remotely accessing DVR/NVR Controller, IP Cameras, Web Server or online gaming (via game console or computer).

Port forwarding works by "forwarding" a specific TCP or UDP port from the NF18ACV to the computer or device you are using.

This guide has been revised to include the latest changes and updates from the NF18ACV's new NC2 web user interface.

Prerequisite

Prior to setting the port forwarding function you must know which ports need to be opened. If you are not sure, contact the application vendor or developer.

Add a Port Forwarding Rule

Login to Web User Interface

Connect a computer and theNF18ACV using an Ethernet cable. (A yellow Ethernet cable was provided with your NF18ACV).

1   Open a web browser (such as Google Chrome or Mozilla Firefox), type following address into the address bar and press **Enter**.

   http://192.168.20.1

2   Enter the following credentials in the **User Name** and **Password** fields:

   User Name: **admin**

   Password: **admin**

3   Click the **Login** button.
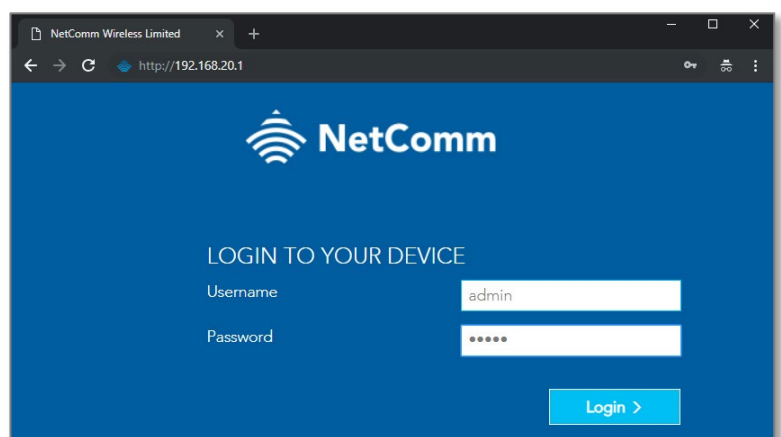

Note – If no authentication prompt is displayed or you see a request time out message, refer to the *What if I cannot access Web User Interface guide* from FAQs section.

![NetComm logo]

Set up Port forwarding (a.k.a. Virtual Server)

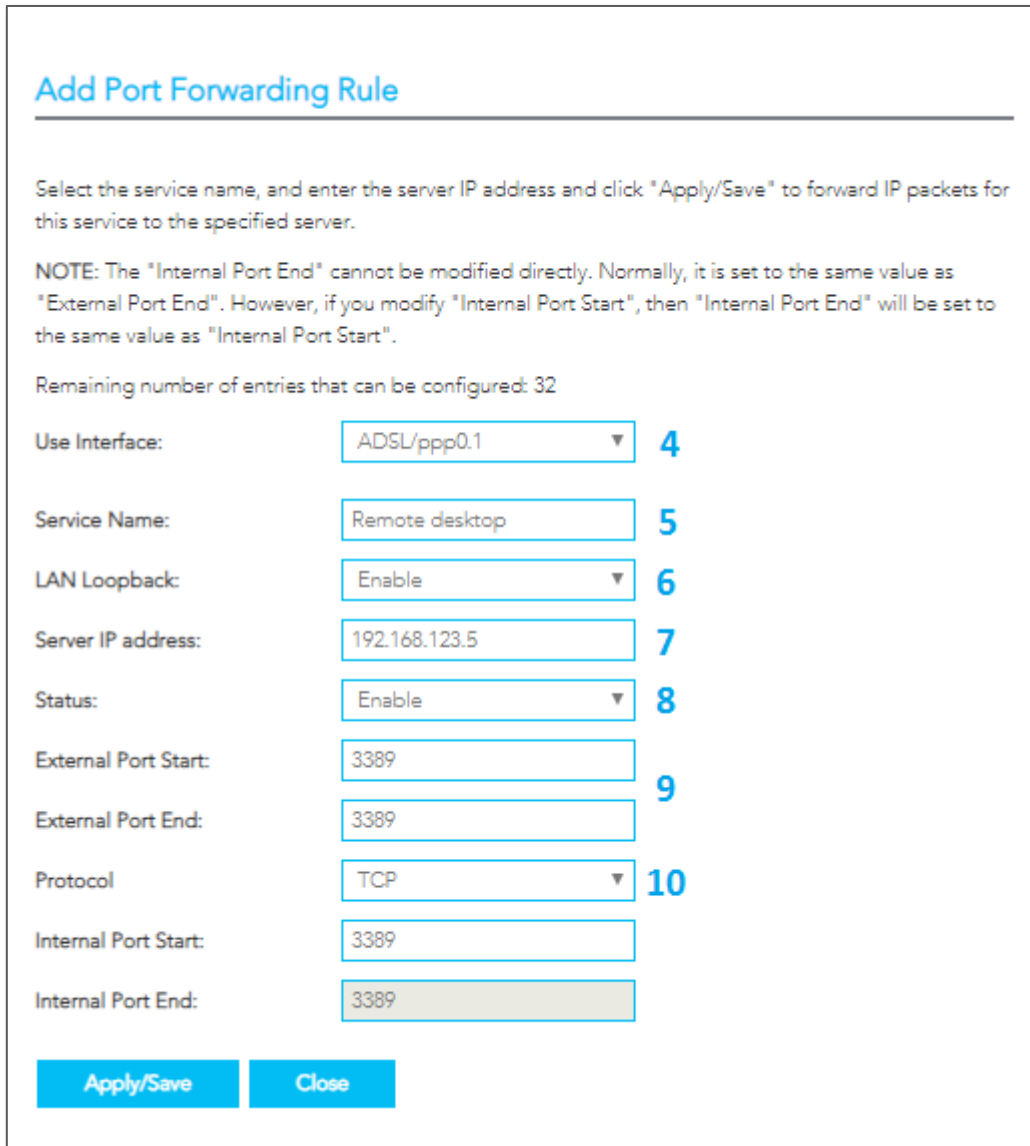1   From the **Advanced** menu, select **NAT** from the **Routing** group.
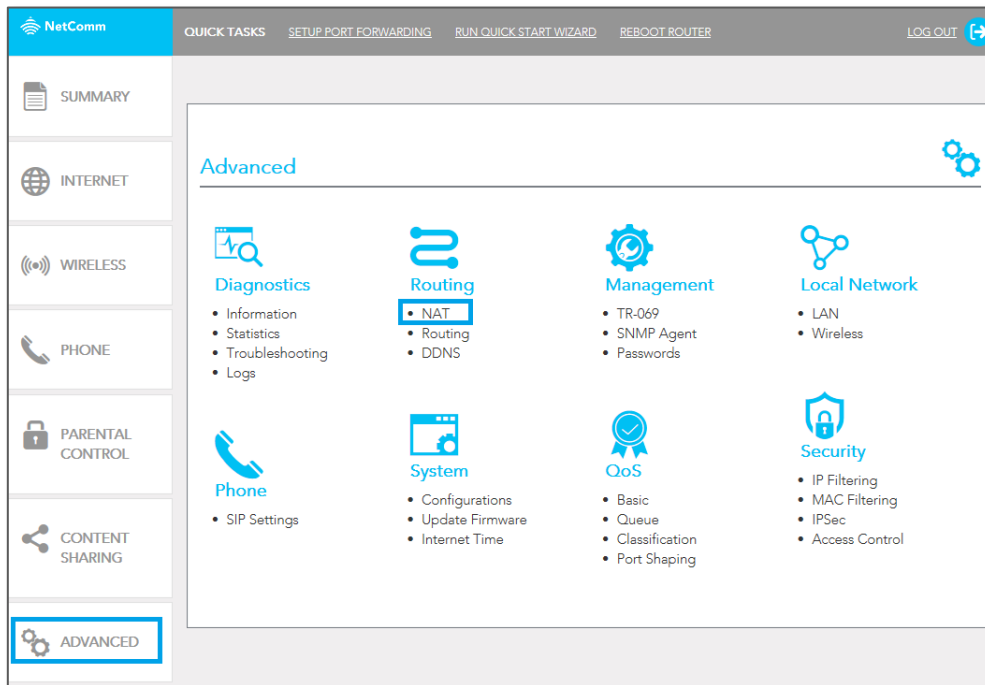
2   Then under the **Port forwarding** section of the **Routing – NAT** page, click the **Add** button to add a new port forwarding rule.
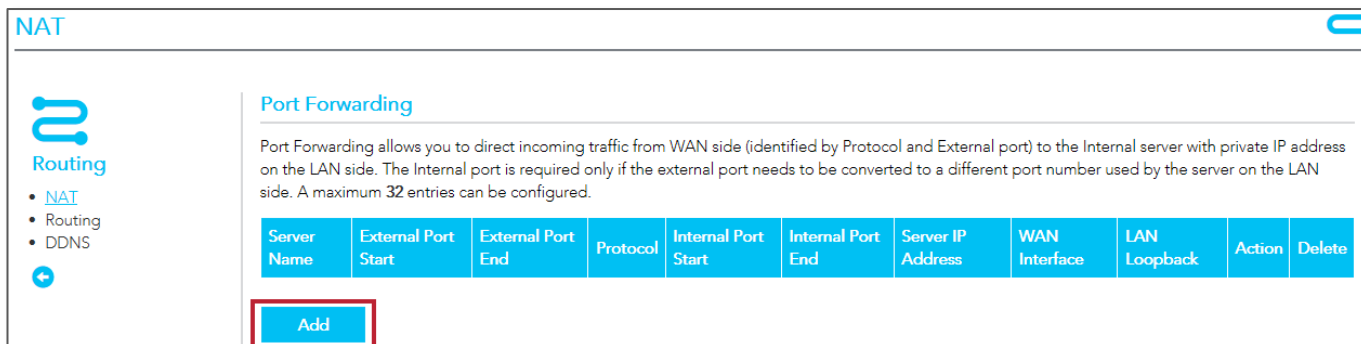
3   The **Add Port Forwarding Rule** pop up window will appear.

An example configuration for allowing Remote desktop toward a LAN side device is provided below.

4   Select the correct Interface in the **Use Interface** field.

A misconfiguration will result in the failure to forward anything.

The correct interface can be checked from the **Internet** page.

5   The **Service Name** needs to be unique but also descriptive, so provide a meaningful name suitable for future reference.

6   **LAN Loopback** must be enabled. This is important if you want to access resources using public IP address even when you are connected to the same network.

A good example is a DVR security system. You may watch your camera feed from anywhere in the world using the public IP address. Now if you are in the local network, with this option enabled, you do not need to change DVR IP address.

7   Configure the Private IP address of the device (e.g. Computer, DVR, Gaming Console) you wish to port forward to in the **Server IP Address** field.

This will be a local IP address in the subnet 192.168.20.xx (by default); where xx can be equal to 2 to 254.

8   Open the **Status** drop down list and select **Enable**.

9   Enter the port number or port range into the **External Port Start** and **External Port End** fields.

If you only want to open one port, then enter the same number in **Start** and **End** port fields, but if you want to open range of ports, then enter the start number in **Port Start** field and end number in **Port End** field.

Note that the **Internal Port Start** *and* **Internal Port End** *fields will automatically populate with the same port numbers.*

10   Select the **Protocol** to be used for the port forwarding rule: **TCP**, **UDP** or **TCP/UDP both**.

11   Click the **Apply/Save** button.

12   The port forwarding rule will now be added to the list.

The example Remote desktop access rule created in this section is displayed below.

Port Forwarding

Port Forwarding allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	LAN Loopback	Action	Delete
Remote Desktop	3389	3389	TCP	3389	3389	192.168.123.5	undefined	Enabled	Disable	Delete

Add

Port forwarding is now configured.

You may also **Enable/Disable**, **Delete** any rule existing rule from this window.

Please note

⏚   We recommend that you **set a Static IP address** on the end device, **instead of obtaining one automatically**, to make sure that the request is forwarded to the appropriate machine every individual time.

⏚   You **can only forward a port to one location** (IP address). In some cases, this may cause issues when multiple LAN devices (computers, game consoles, or VOIP ATAs) attempt to use online gaming at the same time or make multiple VOIP service connections. In these cases, you will need to use an alternate port for any subsequent connections after the first device. Please consult your VOIP provider or game manufacturer for assistance with this.

⏚   Similarly, **remote access and the webserver must have unique port numbers**.

For example, you cannot host a web server accessible through port 80 of your public IP and enable remote http administration of the NF18ACV through port 80, you must provide both with unique port numbers.

⏚   Note also that **ports 22456 to 32456 are reserved for RTP protocol in VOIP services**.

Do not use any of these ports for any other service.