BUSINESS GATEWAY AR129
PORT FORWARDING INSTRUCTIONS

Toll Fraud Liability

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DOS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. Commander offers no warranties, either express or implied, regarding the prevention, detection, or deterrence of toll fraud, networking attacks, or unauthorized, illegal, or improper use of Commander-supplied equipment or software. Therefore, Commander is not liable for any losses or damages resulting from such fraud, attack, or improper use, including, but not limited to, human and data privacy, intellectual property, material assets, financial resources, labour and legal costs.

Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you and you are encouraged to review documentation regarding available security measures, their configuration and implementation and to test such features as is necessary for your network

Disclaimers

The sample details used in this document are for illustrative purpose only and may vary for each individual customer depending on the customer's requirements. It should not be relied upon by any person as being complete or accurate.

Whilst Commander has made every reasonable effort to ensure that this user guide is accurate, Commander disclaims liability for any inaccuracies or omissions that may have occurred. Information in this user guide is subject to change without notice and does not represent a commitment on the part of Commander. Commander assumes no responsibility for any inaccuracies that may be contained in this User guide. Vocus makes no commitment to update or keep current the information in this user Guide and reserves the right to make improvements to this user Guide and/or to the products or services described in this user guide, at any time without notice.

Port Forwarding instructions

These instructions are to enable you to configure the Port Forwarding for the AR129 Business Gateway. The Firefox Browser was used for this guide, other browsers may differ slightly in the look and feel although similar steps will be required.

We recommend the use of Firefox or Chrome in the configuration of the Business Gateway AR129.

Browse to the device

1. Type the URL into a Browser and press enter.

http://192.168.11.1

Note: If you have changed the IP Address of the gateway, you will need to use the new IP Address.

A security warning will be displayed.

2. Click **Details**.

This site is not secure

This might mean that someone's trying to trick you or steal any information that you send to the server. You should close this site immediately.

Go to your Start page

Details

This site is not secure

This might mean that someone's trying to trick you or steal any information that you send to the server. You should close this site immediately.

Go to your Start page

Details

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

Go on to the webpage (Not recommended)

3. Click Go on to the webpage. (Not recommended)

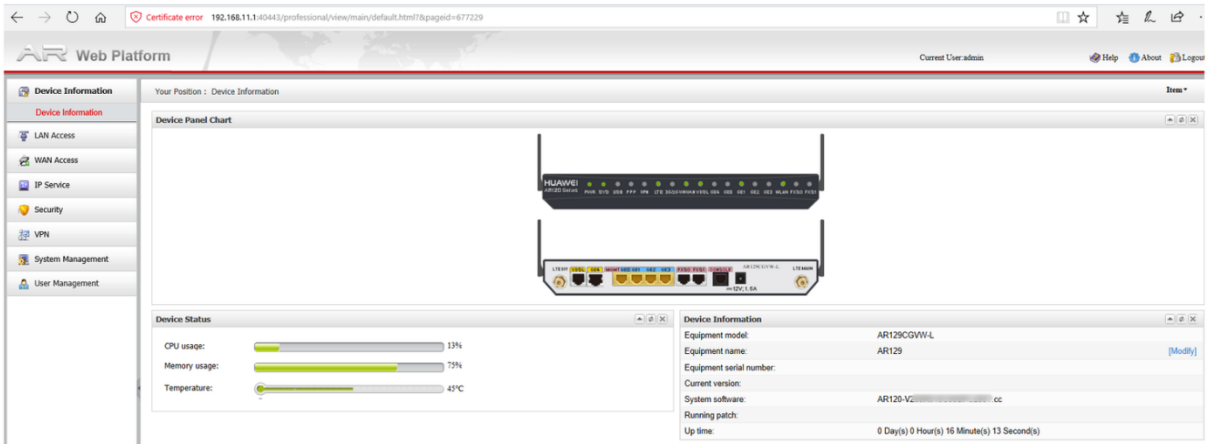
The Router login page will be displayed.

Login to Router

1. Enter the Default username: **admin.**
2. Enter the Default password: **password@admin.**
3. Click Login.

Note: If you have changed the password of the gateway (recommended), you will need to use the new password.

The Device Information page is displayed.

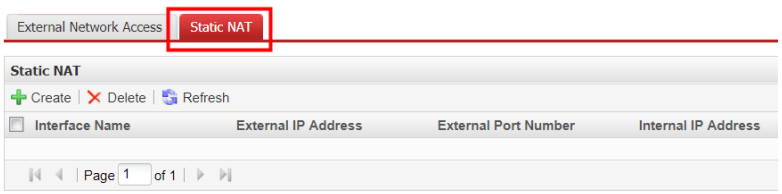


4. Click **IP service** from the left pane.

The DHCP item is selected by default.

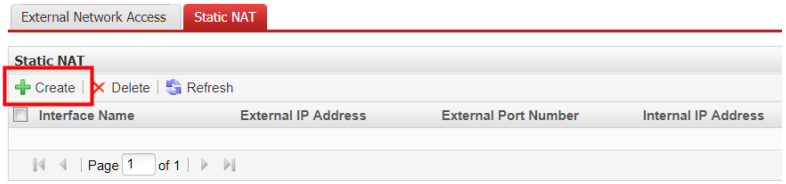
From here, select NAT.

5. Select the **Static NAT** tab.

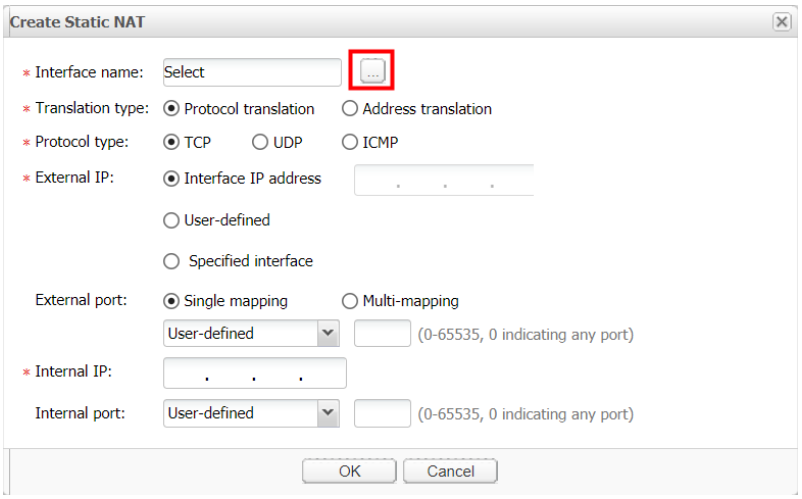


Configure Port Forwarding

1. Click Create .



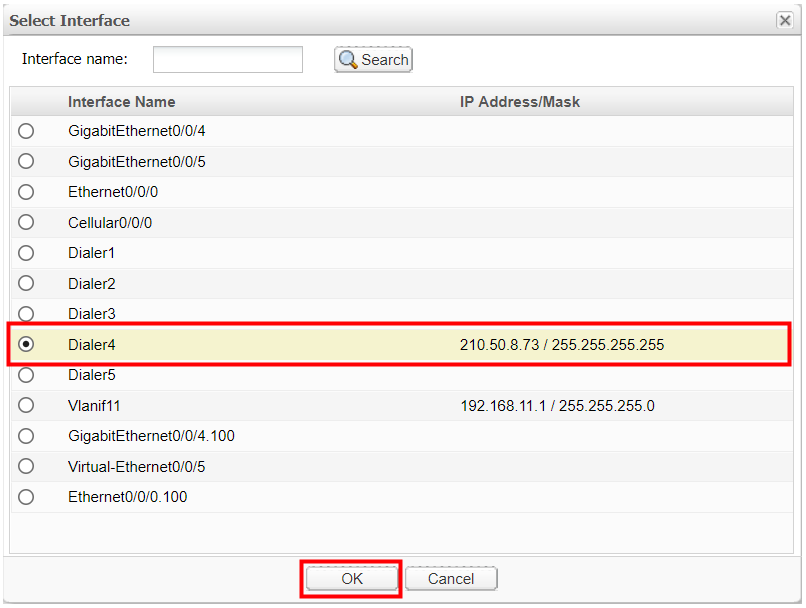
2. Click the ellipses button next to **Interface name**.



3. Select **Interface name**.

Note: This must be the Dialer with a WAN IP.

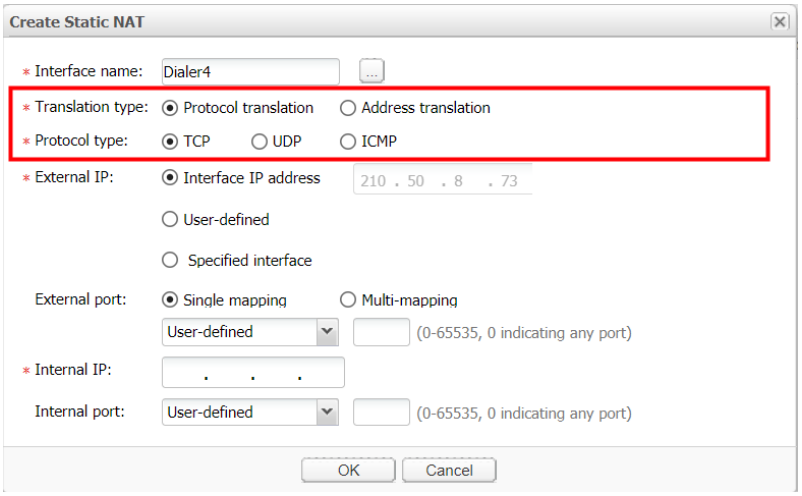
4. Click OK.



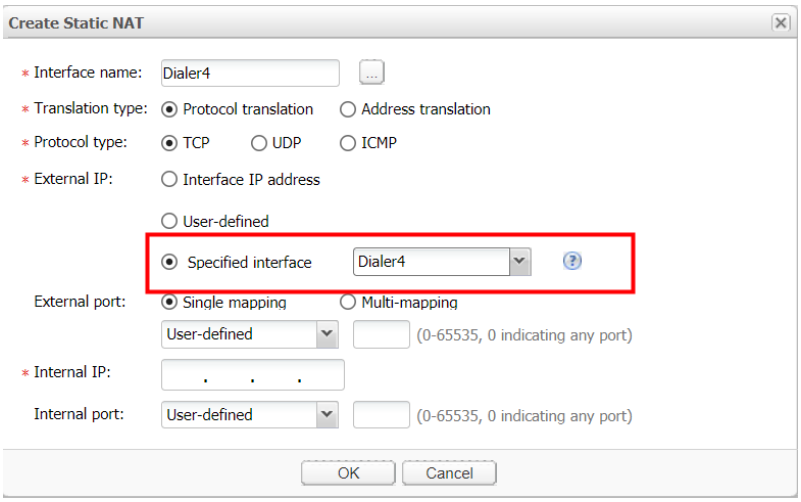
5. Select **Translation Type** of **Protocol translation**.

6. Select required **Protocol Type**. (TCP or UDP)

Note: If you want the rule to apply to both TCP and UDP you will need to create two rules.



7. Select the same Dialer from the drop-down list as the Interface name.



8. Enter **External Port** details.

This is the port that will be accessed from the "outside world".

Select 'Single mapping'.

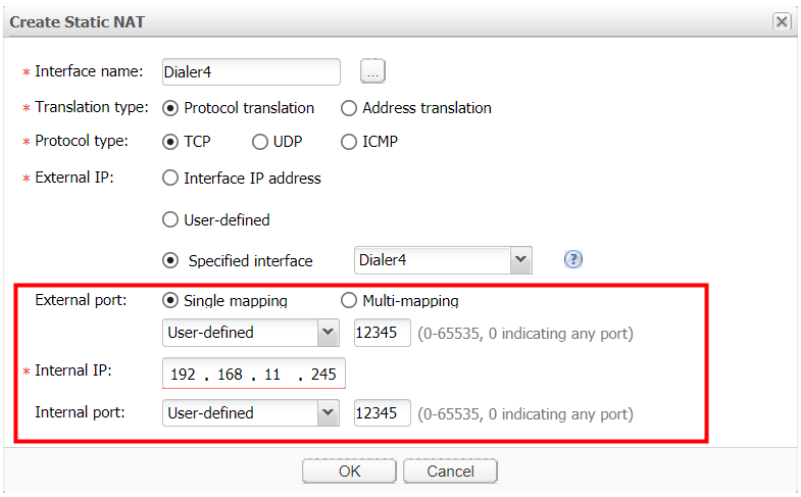
9. Enter **Internal IP**.

This is the IP of the computer needing the port open.

10. Enter **Internal Port** details.

This is the port wanted on the computer. (These can be different)

11. Click OK.



The Static NAT page is redisplayed. With the rule you have created displayed.
Click on Refresh

The device is setup to automatically create a second rule displaying VLAN.

Repeat as necessary for each port that needs forwarding.