

APPLICATION NOTE

APNUS032 How to Configure NAT Port Forwarding July 2023

Content

1. Glossary.....	3
2. Introduction.....	3
3. Port Forwarding Configuration architecture	3
4. ACKSYS Router configuration	5
Configuring Network Interfaces	5
CONFIGURING SSID FOR PUBLIC NETWORK.....	5
PUBLIC NETWORK	6
PRIVATE NETWORK.....	7
NETWORK OVEVIEW.....	8
Configuring DHCP Server on WIFI Interface (Public Network).....	8
Configuring Network Zones.....	8
PUBLIC ZONE	8
PRIVATE ZONE	9
Configuring Port Forwarding Rule (on Public Zone)	10
NETWORK ZONE OVERVIEW.....	11
Configuring the WaveManager Server (in the private network)	11
Router: WiFi Status.....	12
6. TESTING	13

1. Glossary

NAT : Network Address Translation

PAT: Port Address Translation

GW: Gateway

DHCP: Dynamic Host Configuration Protocol

TCP:Transmission Control protocol

UDP:User Datagram Protocol

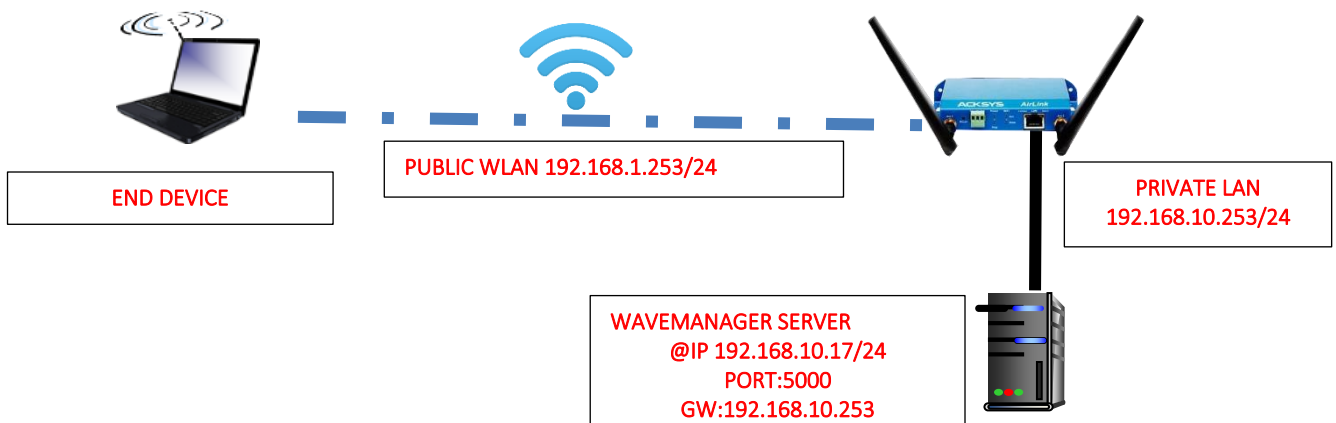
2. Introduction

All IP packets have a source IP address and a destination IP address. Typically, with NAT, packets passing from the private network to the public network will have their source address modified, while packets passing from the public network back to the private network will have their destination address modified.

The aim of this application note is to show in details the configuration steps to configure the NAT port forwarding on ACKSYS router.

3. Port Forwarding Configuration architecture

In this application note, we will explain in detail a practical step-by-step how to configure port forwarding on Acksys Router to reach in a private Network WaveManager Server connected on LAN Interface via Public Network.



Before we begin, let's overview the configuration that we are attempting to achieve and the prerequisites that make it possible in this application note :

- AirLink or Any type of Acksys Router
- WaveManager Server connected in AirLink LAN interface
- Laptop to configure the router

Networks	Public IP: 192.168.10.253 SSID=PAT
	Private IP: 192.168.1.253
Zone/Firewall	Public Zone with Masquerade enable
	Private Zone
WLAN DHCP server	Range 192.168.1.100 & .150
WaveManager	IP:192.168.10.17/24 GW:192.168.10.253 Port:5000

4. ACKSYS Router configuration

The first step is configuring the AirBox router. For this, you will need to connect a network cable between your PC and AirBox router, and then open an Internet browser. The default IP address is 192.168.1.253 reason why your PC should be configured using a static IP address in the range 192.168.1.X

Configuring Network Interfaces

If you have familiarized yourself with the configuration scheme and we can start configuring the router using instructions provided. We will create two Network called Public and Private

CONFIGURING SSID FOR PUBLIC NETWORK

By default the WiFi Adaptor is disabled therefore in this application note, we will create an SSID to associate to the WIFI adapter to allow end device connected on its.

In the GUI, go to Setup → Physical Interfaces → Click WiFi Adaptor to On

WI-FI INTERFACE					
Wi-Fi 4 (802.11n) Wireless interface					
	CHANNEL	802.11 MODE	SSID	ROLE	SECURITY
	Automatic	802.11b+g+n	acksys	Access Point (infrastructure)	none
					ACTIONS
					Interface disabled

- Click the "Edit" button located to the right and your SSID configuration page:

WI-FI INTERFACE					
Wi-Fi 4 (802.11n) Wireless interface					
	CHANNEL	802.11 MODE	SSID	ROLE	SECURITY
	Automatic	802.11b+g+n	acksys	Access Point (infrastructure)	none
					ACTIONS

- Role: Access Point
- ESSID: PAT
- Network: PUBLIC
- Click on Save

WIRELESS SETTINGS : WIFI

The Device Configuration section covers physical settings of the radio hardware which is shared among all defined wireless networks. Per network settings like encryption or operation mode are in the Interface Configuration. If SRCC role is selected, most of the Device Configuration is irrelevant (please refer to the product user guide).

DEVICE CONFIGURATION	
General Setup	a/b/g Data Rates 802.11n Mcs Advanced Settings
802.11 mode	802.11b+g+n (2.4 GHz)
HT mode	20MHz
Automatic channel select	<input checked="" type="checkbox"/> Automatic channel select is not compatible with Ad-hoc, Mesh and multi-interfaces

INTERFACE CONFIGURATION	
General Setup	Wireless Security Advanced Settings MAC Filter Frame filters
Role	Access Point (infrastructure)
ESSID	PAT
Maximum simultaneous associations	Max allowed by radio card (see documentation)
Hide ESSID	<input type="checkbox"/> In order to comply with the DFS regulation, clients might not associate if you check this option and select a DFS channel. See the user guide for more details.
Network	<input checked="" type="radio"/> PUBLIC <input type="radio"/> PRIVATE <input type="radio"/> unspecified -or- create:

- Security: No encryption (only in this note but we invite partner to set a strong password)

INTERFACE CONFIGURATION	
General Setup	Wireless Security Advanced Settings MAC Filter Frame filters
Security	No encryption
	<small>WARNING: The WEP encryption is only supported with 11abg mode</small>

PUBLIC NETWORK

In the GUI, go to Setup → Physical Interfaces → Edit LAN Interface

NETWORK OVERVIEW

NAME	ENABLED	IPv6 ADDRESS	IPv6 GATEWAY	IPv4 ADDRESS	NETMASK	IPv4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
lan	<input checked="" type="checkbox"/>			192.168.1.253	255.255.255.0		Default	

[Add network](#)

Click the "Edit" button located to the right and let configure LAN Interface.

- General Setup
 - Network description :PUBLIC (use your custom name)
 - Protocol: Static
 - Select IPv4 Address IP family : 192.168.1.253
 - IPv4-Netmask:255.255.255.0
 - Save

NETWORK - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.

COMMON CONFIGURATION

General Setup | Interfaces Settings | Advanced Settings | IPv6 Setup

Enable interface

Network description: PUBLIC

Protocol: static

IPv4-Address: 192.168.1.253

IPv4-Netmask: 255.255.255.0

- Interface Settings
 - Bridge Interfaces: Click to enable
 - Interface: Unclick Ethernet Adapter to use WIFI adapter for public Network
 - Click Save

NETWORK - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.

COMMON CONFIGURATION

General Setup | Interfaces Settings | Advanced Settings | IPv6 Setup

Bridge interfaces

Enable STP/RSTP

Enable LLDP forwarding

bridge VLAN

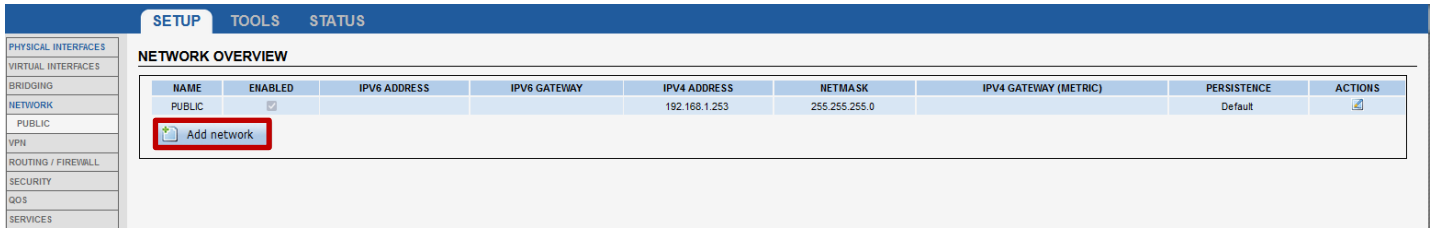
Interface: Ethernet adapter: LAN (network: PUBLIC)

WiFi adapter: WIFI (currently disabled) - acksys (network: PUBLIC)

MTU: 1500

PRIVATE NETWORK

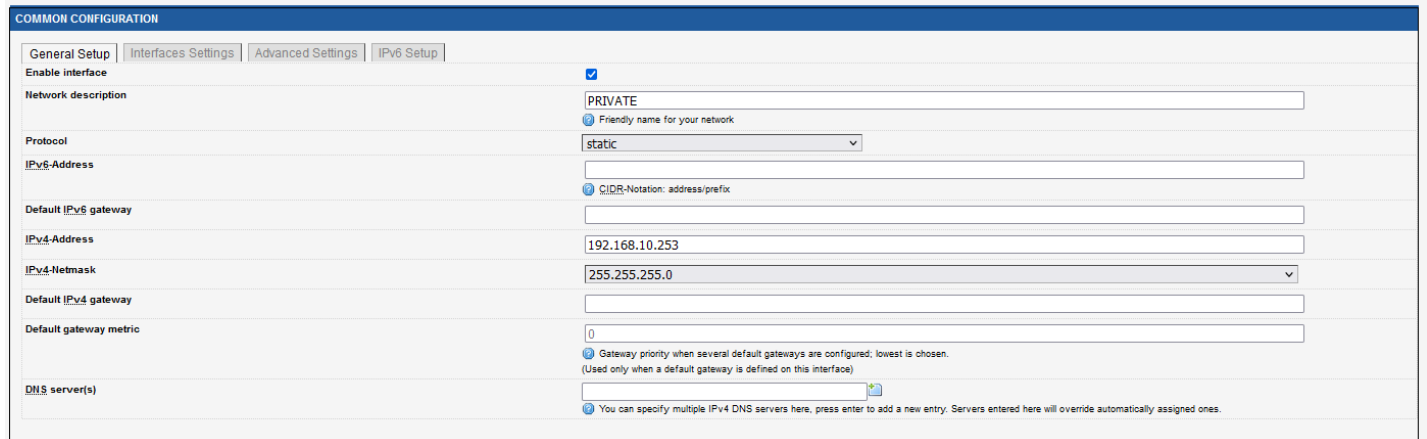
Click the "Add network" button to add the Private Network and let configure its.



- General Setup
 - Network description :PRIVATE (use your custom name)
 - Protocol: Static
 - Select IPv4 Address IP family : 192.168.10.253
 - IPv4-Netmask:255.255.255.0
 - Save

NETWORK - NET2

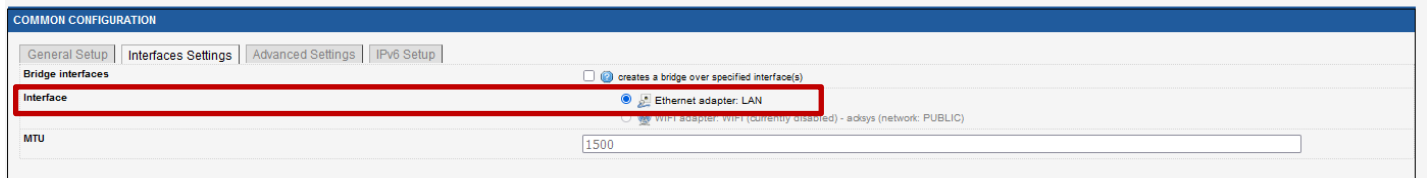
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.



- Interface Settings
 - Bridge Interfaces: unclick to disable
 - Interface: Click Ethernet Adapter to use LAN adapter for private Network
 - Click Save

NETWORK - NET2

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.



NETWORK OVEVIEW

Let have an overview on Network created for Private and Public.

NETWORK OVERVIEW

NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
PUBLIC	<input checked="" type="checkbox"/>			192.168.1.253	255.255.255.0		Default	
PRIVATE	<input checked="" type="checkbox"/>			192.168.10.253	255.255.255.0		Default	

Add network

Configuring DHCP Server on WIFI Interface (Public Network)

By default, the DHCP server is disable and to allow end devices to receive IP address, we will configure the DHCP server with the default following information:

In GUI and go to Setup → Services →DHCP/DNS RELAY

- LAN Interface is enable DHCP
- Select DHCP service: DHCP server
- Save and Apply

DHCP / DNS RELAY

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

INTERFACE SETTINGS: PUBLIC

General Setup | Advanced Settings

Ignore interface Disable DHCP for this interface.

Select DHCP service: **DHCP server**

DHCP pool first address:
Lowest leased address as offset from the network address.

DHCP pool size:
Maximum number of leased addresses.

Lease time:
Expiry time of leased addresses, minimum is 2 Minutes (m).

Configuring Network Zones

In this section, we will create 2 Network Zones (PUBLIC and PRIVATE) mapping the both Networks created already created.

PUBLIC ZONE

In the GUI, go to Setup → Routing /Firewall → Network Zones → click on Add Zone to create the Two Network Zone

NETWORK ZONES OVERVIEW

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	IP MASQUERADING	LOCAL SERVICES	ACTIONS
Add zone					

As soon as clicking in Add zone, we will be redirected to the network zone configuration

- General Setup
 - Name: PUBLIC (use your custom name)
 - IP Masquerading: Enable
 - Covered Networks: PUBLIC
 - Save

NETWORK ZONES - ZONE SETTINGS

ZONE "ZONE_1"

This section defines common properties of "zone_1".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: PUBLIC

Enable IP Masquerading: Only on public zones. Use for NAT/PAT routing
Warning: if using VRRP, the NATed network must be set to protocol NONE

MSS clamping:

Default acceptance policy for local services: All enabled
You can restrict or open the local services in the firewall section below

Covered networks: PUBLIC: PRIVATE:

PRIVATE ZONE

In the GUI, go to Setup → Routing /Firewall → Network Zones → click on Add Zone to create the Private Network Zone

SETUP | TOOLS | STATUS

NETWORK ZONES OVERVIEW

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	IP MASQUERADING	LOCAL SERVICES	ACTIONS
PUBLIC	"PUBLIC"	-	<input checked="" type="checkbox"/>	All enabled	
<input checked="" type="button" value="Add zone"/>					

As soon as clicking in Add zone, we will be redirected to the network zone configuration

- General Setup
 - Name: PRIVATE (use your custom name)
 - IP Masquerading: Disable
 - Covered Networks: PRIVATE
- Inter-Zone Forwarding
 - Allow forwarding to destination zones: PUBLIC
 - Save

NETWORK ZONES - ZONE SETTINGS

ZONE "PRIVATE"

This section defines common properties of "PRIVATE".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: PRIVATE

Enable IP Masquerading: Only on public zones. Use for NAT/PAT routing
Warning: if using VRRP, the NATed network must be set to protocol NONE

MSS clamping:

Default acceptance policy for local services: All enabled
You can restrict or open the local services in the firewall section below

Covered networks: PUBLIC: PRIVATE:

INTER-ZONE FORWARDING

Use this section only if IP Masquerading is disabled on this zone.
The options below control the forwarding policies between this zone (%s) and other zones. Destination zones cover forwarded traffic **originating from %q**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forwarding to destination zones: PUBLIC: PUBLIC:

Configuring Port Forwarding Rule (on Public Zone)

In the GUI, go to Setup → Routing /Firewall → Network Zones → Edit Public Zone et create the new rule below:

SOURCE ZONE	NAME	SOURCE IP	FRAME PROTOCOL	PUBLIC PORT	PRIVATE PORT	DESTINATION IP	SORT
PUBLIC	WaveManager_Access	any	tcp & udp	5000	5000	192.168.10.17	

Use this section only if IP Masquerading is enabled on this zone.
This section allow to redirect the input traffic on this zone to a device on other zone

Blank any ip source Blank, all ports Blank, all ports

Add

The rule above redirects all PUBLIC tcp/udp incoming traffic from the router on port 5000 via WIFI connection to private port 5000 on the IP 192.168.10.17, i.e. port 5000 on the WaveManager Server.

Field Name	Value	Description
Source Zone	Public	Your custom zone name covered the network
Name	WaveManager Access	Name of your custom
Source IP	Any	The network/mask or the source IP address
Frame Protocol	TCP&UDP	Type of protocol of incoming packet
Public port (destination port)	5000	Traffic will be forwarded from this port on the Public Network
Private port (destination port)	5000	The rule will redirect the traffic to this port on the internal machine
Destination IP	192.168.10.17	The IP address of the WaveManager that hosts want to access from the Public Zone

NETWORK ZONE OVERVIEW

We have now created the two network zones , private and Public to manage network traffic through the router.

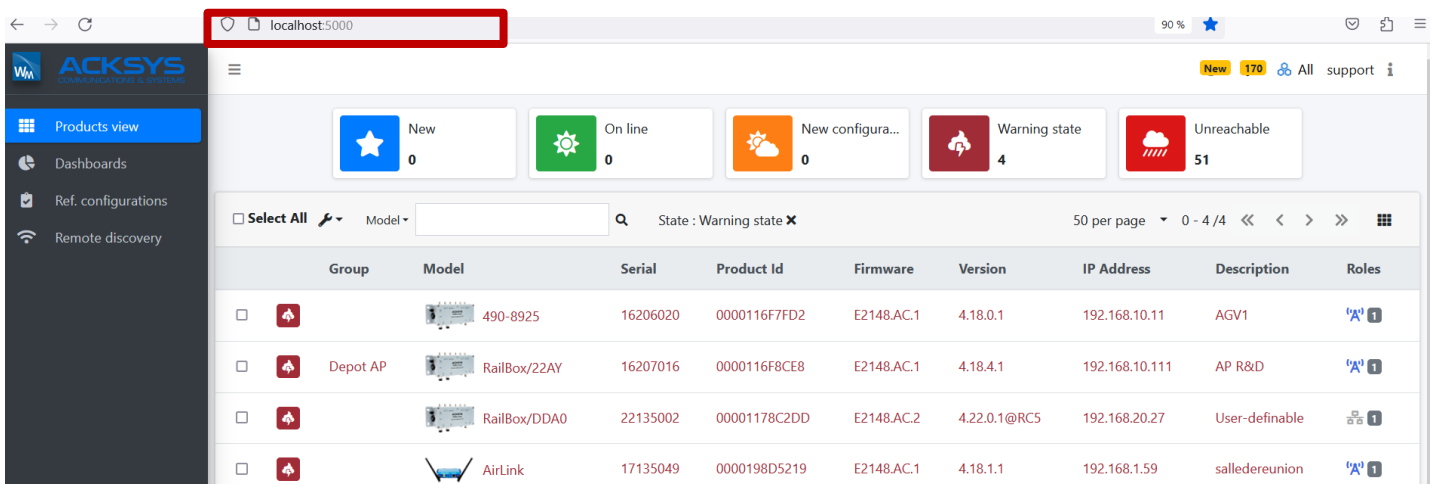
NETWORK ZONES OVERVIEW					
NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	IP MASQUERADING	LOCAL SERVICES	ACTIONS
PUBLIC	"PUBLIC"	-	<input checked="" type="checkbox"/>	All enabled	
PRIVATE	"PRIVATE"	PUBLIC	<input type="checkbox"/>	All enabled	

Add zone

Now, we must Apply and Save button to restart the router for the configuration to be effective. The final step is to connect WaveManager Server to the Acksys Router using an Ethernet cable.

Configuring the WaveManager Server (in the private network)

The last step is to configure the WaveManager Server. This application note will not enter in detail regarding the steps to be installed and configure WaveManager server. However, below is a screenshot of the configuration of the WaveManager in local address: <http://localhost:5000>



In summary, the WaveManager Server listened by default on port 5000 and it is installed on a Windows 10 Laptop with the below network parameters:

- IP Address: Fixed IP address (DHCP disabled) 192.168.10.17
- Netmask 255.255.255.0.
- Gateway: The Acksys LAN IP address 192.168.10.253
- WaveManager Listen Port: 5000

Finally, the web port has been chosen as TCP 5000 for simplicity (this way, via port 80 the Acksys Router configuration can be accessed remotely, and via port 5000 the IP WaveManager can be accessed).

Router: WiFi Status

First of all let test a wireless connection with an end device to the AP with the SSID named PAT before checking the redirection rule. Windows In GUI and go to **Status** → **Wireless** to verify if WIFI clients is connected to the routeur.

The screenshot shows the ACKSYS router's web interface. The browser address bar indicates the URL: 192.168.1.253/cgi-bin/guiweb/stok=af0649db9ef532404da0c363c67d7538/status/wireless/. The page header includes the ACKSYS logo and the text 'Wireless just became easier AirLink series' with an image of a blue wireless router. The navigation menu shows 'SETUP', 'TOOLS', and 'STATUS' (selected). On the left, a sidebar menu lists various status pages, with 'WIRELESS' selected. The main content area is titled 'ASSOCIATED STATIONS' and shows 'ASSOCIATED STATIONS RESULTS : 1'. Below this is a table with the following data:

GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	WIFI	PAT	Infrastructure	28:6B:35:92:66:39	11	-58 dBm	-95 dBm	37 dB

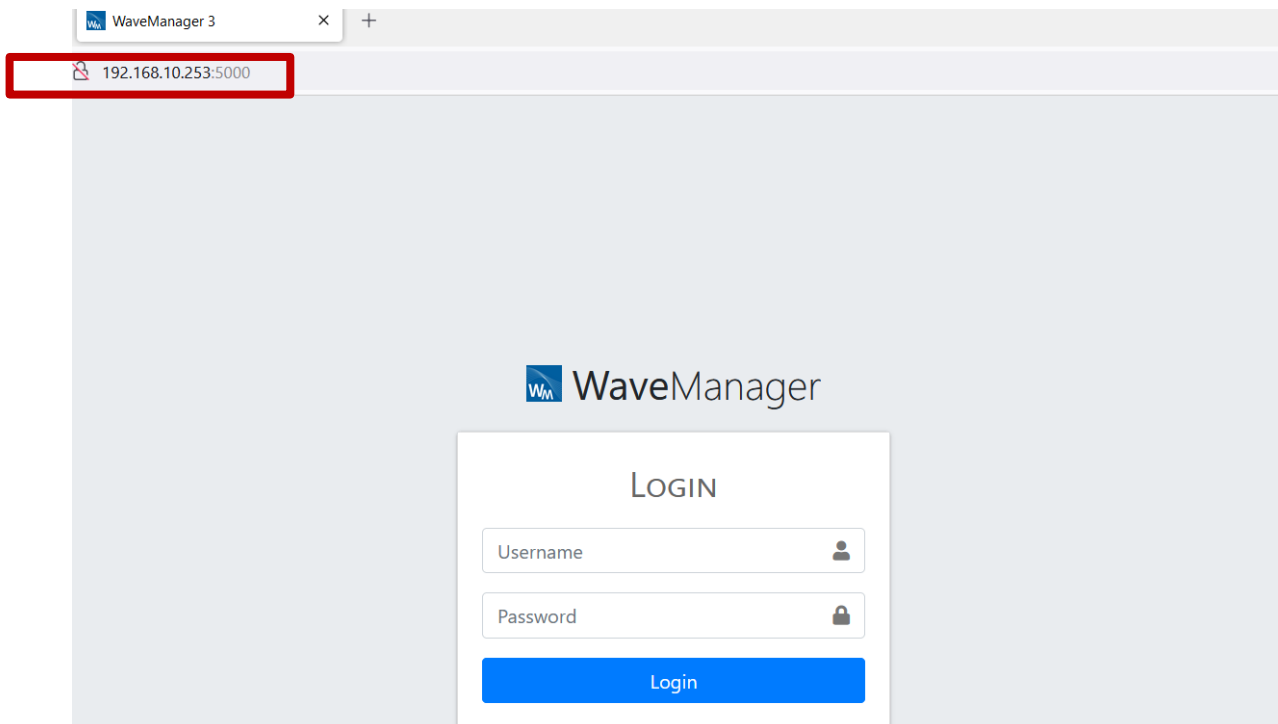
6. TESTING

The final step is to connect the laptop end device on the public zone to the WaveManager Server which is installed on the private zone.

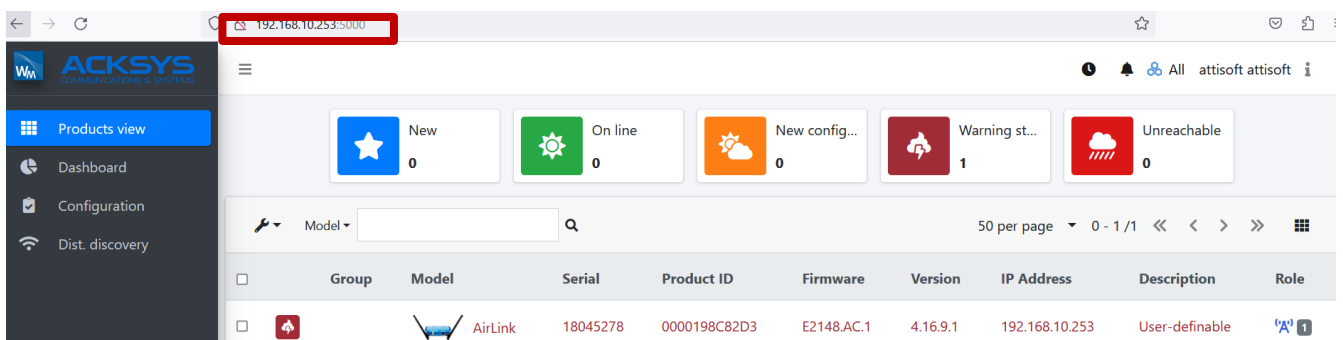
If you've followed all the steps presented above, your configuration should be finished. But as with any other configuration, it is always wise to test the setup in order to make sure that it works properly. In order to check that we have correctly configured everything.

To confirm that port forwarding is working properly, we should be able to access the Wavemanager through the router **public IP: public port:**

We will then be redirected to WaveManager login page with <http://192.168.1.253:5000>. (192.168.1.253 is the Router public IP).



As seen the port forwarding works as expected with the public IP with the public port configured in Routing/Firewall section.



Support : <https://support.acksys.fr>