APPLICATION NOTE

APNUS013 NAT Configuration example

For WaveOS

May 2020 – Rev. A1

CONFIGURING A WAVEOS PRODUCT IN NAT MODE

Desired NAT configuration:

- Private network (LAN): 192.168.100.100/24
- Public network (WLAN): 192.168.1.10/24

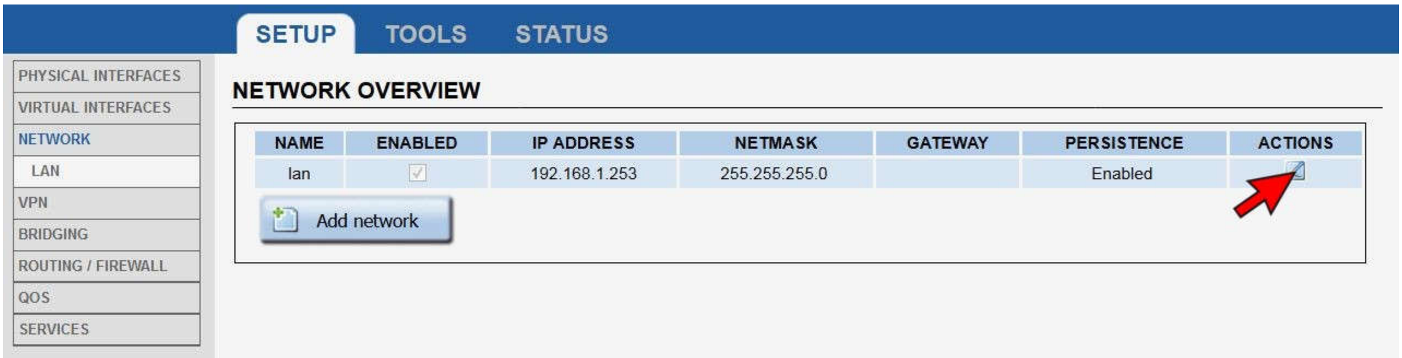
Translation rules:

- PLC_MASTER: TCP 192.168.1.10: 8080 translated to 192.168.100.101: 80
- PLC_IO : UDP 192.168.1.10: 4200 translated to 192.168.100.101: 4200

Private side (LAN):

Default gateway = 192.168.100.100 (or route 192.168.1.0/24 to 192.168.100.100)

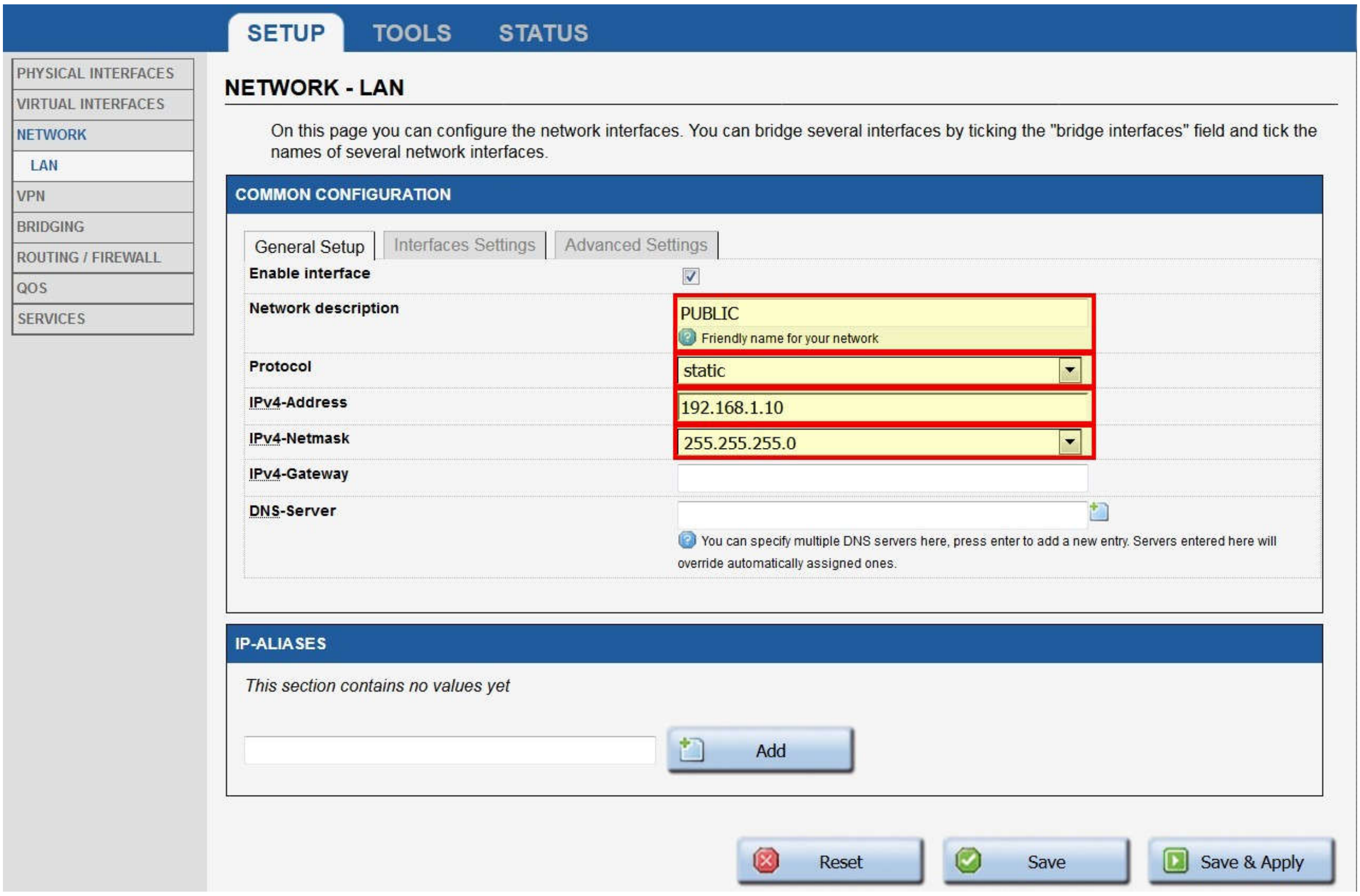
After configuring the WiFi settings, go to **SETUP/NETWORK** and edit the default network (**lan**):



NETWORK OVERVIEW

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY	PERSISTENCE	ACTIONS
lan	☑	192.168.1.253	255.255.255.0		Enabled	✎

Rename the network as **PUBLIC** and fill in the required fields. Then go to the **Interfaces Settings** tab



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.

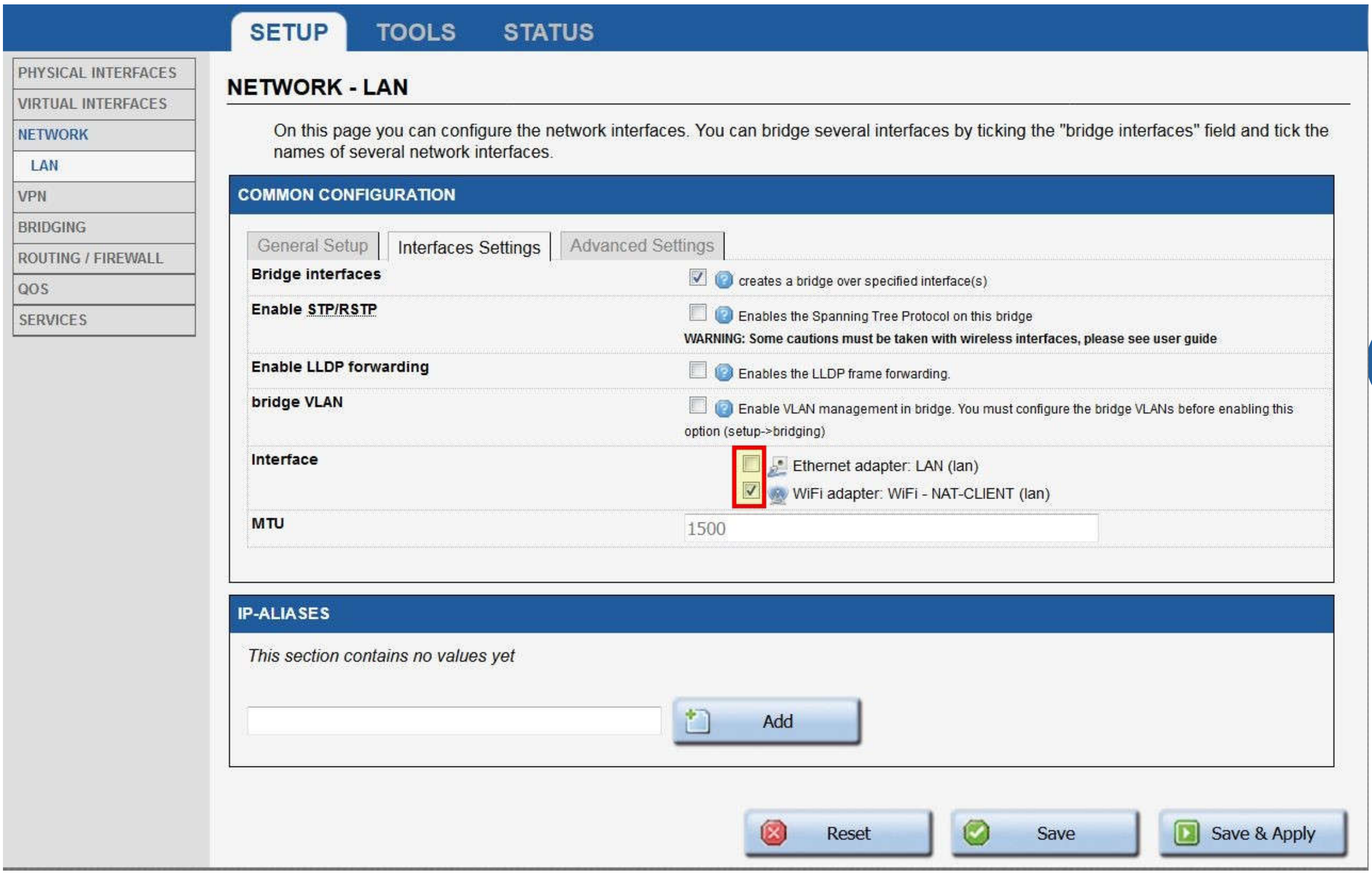
COMMON CONFIGURATION

Enable interface	☑
Network description	PUBLIC Friendly name for your network
Protocol	static
IPv4-Address	192.168.1.10
IPv4-Netmask	255.255.255.0
IPv4-Gateway	
DNS-Server	You can specify multiple DNS servers here, press enter to add a new entry. Servers entered here will override automatically assigned ones.

IP-ALIASES

This section contains no values yet

Uncheck the **Ethernet adapter** checkbox, then **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.

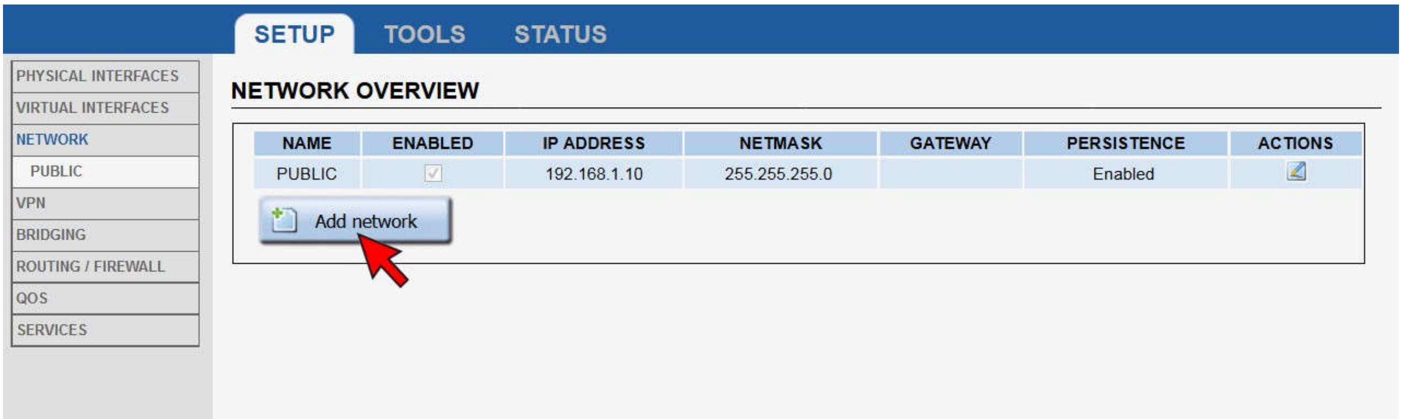
COMMON CONFIGURATION

Bridge interfaces	☑ creates a bridge over specified interface(s)
Enable STP/RSTP	☐ Enables the Spanning Tree Protocol on this bridge WARNING: Some cautions must be taken with wireless interfaces, please see user guide
Enable LLDP forwarding	☐ Enables the LLDP frame forwarding.
bridge VLAN	☐ Enable VLAN management in bridge. You must configure the bridge VLANs before enabling this option (setup->bridging)
Interface	☐ Ethernet adapter: LAN (lan) ☑ WiFi adapter: WiFi - NAT-CLIENT (lan)
MTU	1500

IP-ALIASES

This section contains no values yet

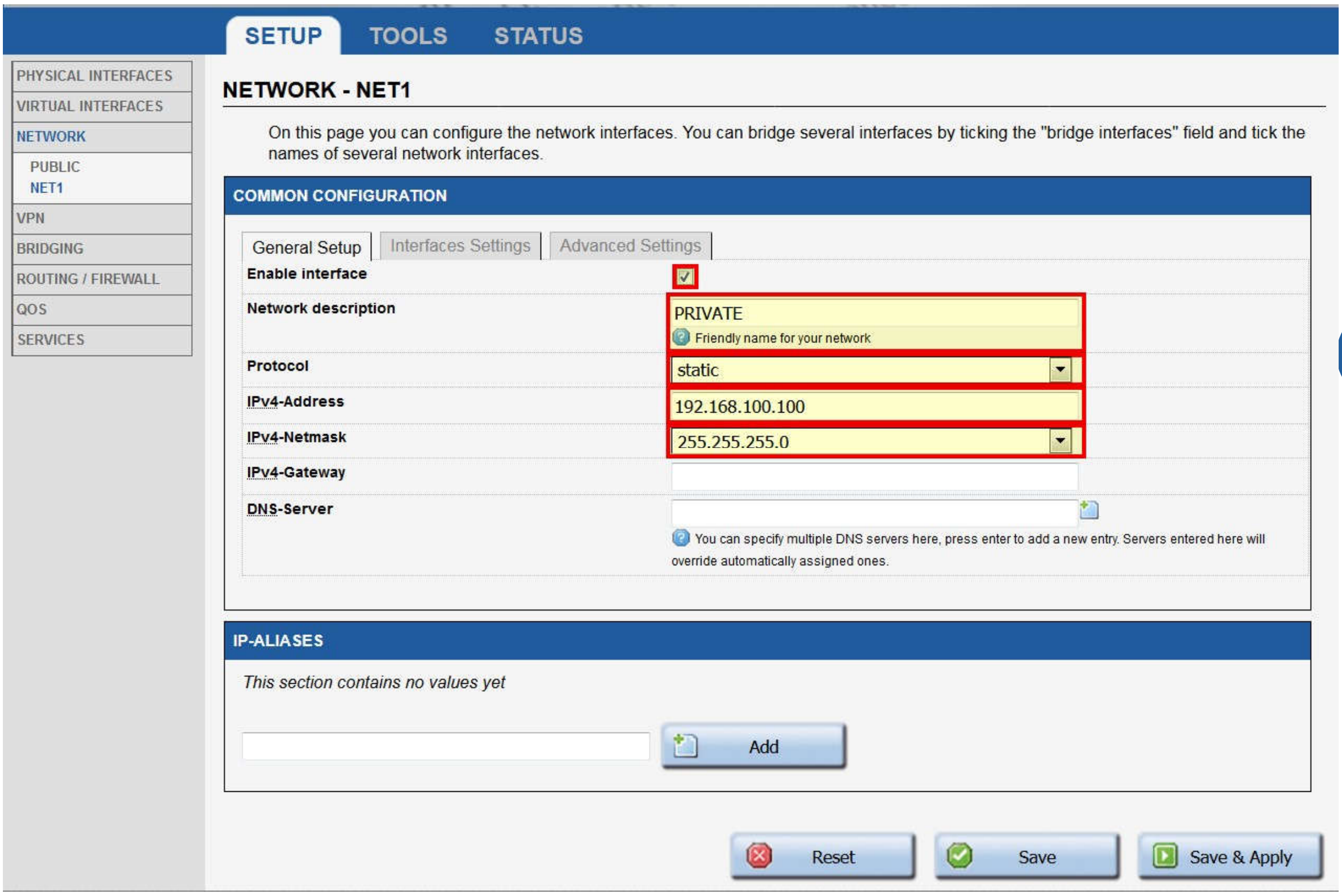
Click **NETWORK** on the left to return to **NETWORK OVERVIEW**. Click on **Add Network**



NETWORK OVERVIEW

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY	PERSISTENCE	ACTIONS
PUBLIC	☑	192.168.1.10	255.255.255.0		Enabled	✎

Name the network **PRIVATE** and fill in the required fields, then switch to the **Interfaces Settings** tab



NETWORK - NET1

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.

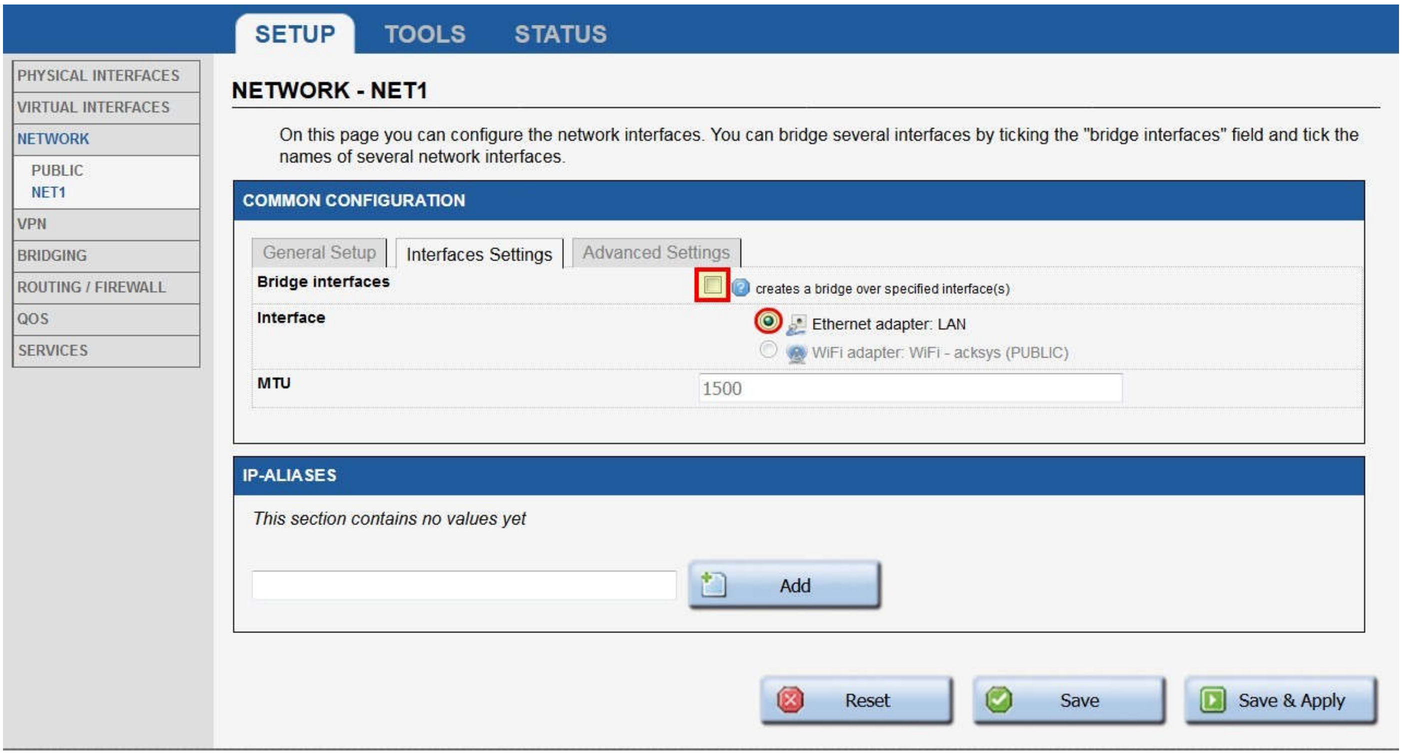
COMMON CONFIGURATION

Enable interface	☑
Network description	PRIVATE Friendly name for your network
Protocol	static
IPv4-Address	192.168.100.100
IPv4-Netmask	255.255.255.0
IPv4-Gateway	
DNS-Server	You can specify multiple DNS servers here, press enter to add a new entry. Servers entered here will override automatically assigned ones.

IP-ALIASES

This section contains no values yet

Uncheck the **Bridge interfaces** box and select **Ethernet adapter LAN**



NETWORK - NET1

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.

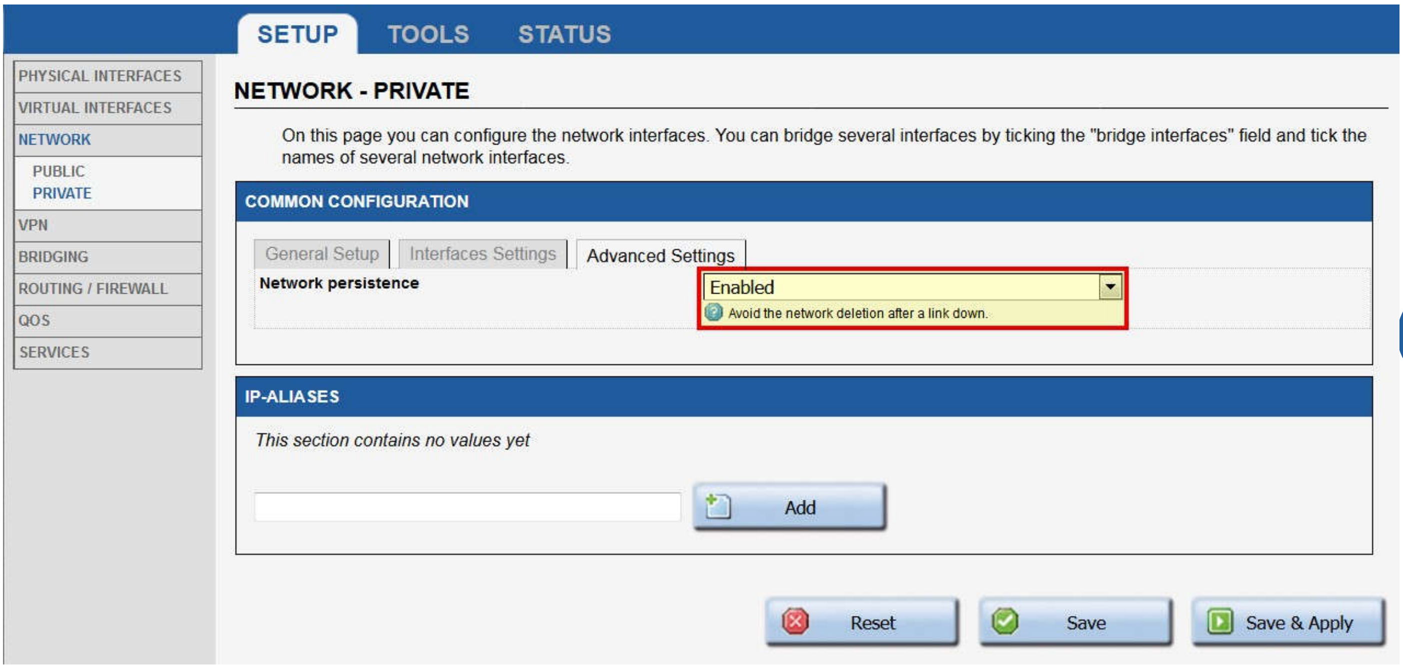
COMMON CONFIGURATION

Bridge interfaces	□ creates a bridge over specified interface(s)
Interface	● Ethernet adapter: LAN ○ WiFi adapter: WiFi - acksys (PUBLIC)
MTU	1500

IP-ALIASES

This section contains no values yet

In the **Advanced settings** tab, check that the network persistence is **Enabled** then **Save**



NETWORK - PRIVATE

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

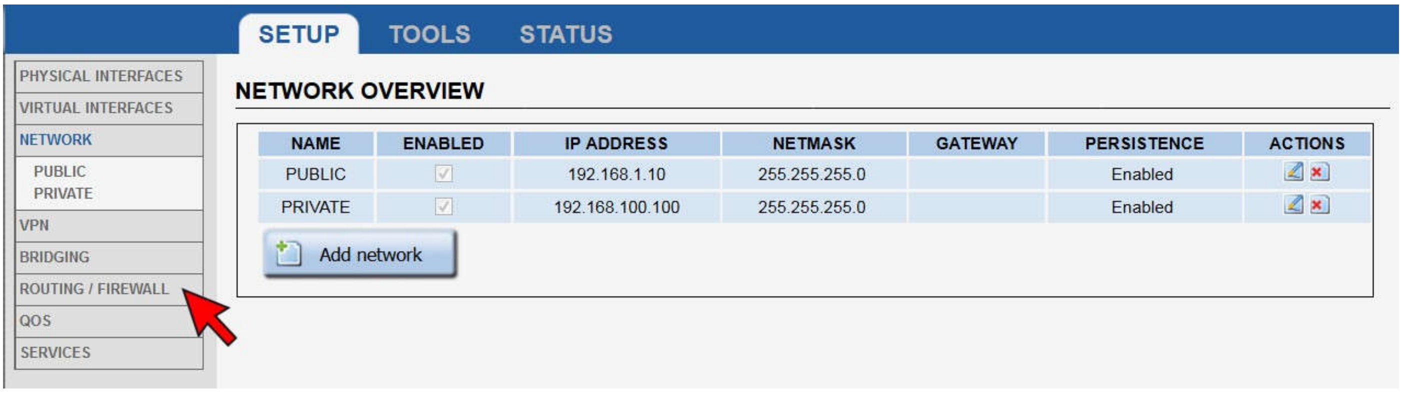
Network persistence: Enabled

Avoid the network deletion after a link down.

IP-ALIASES

This section contains no values yet

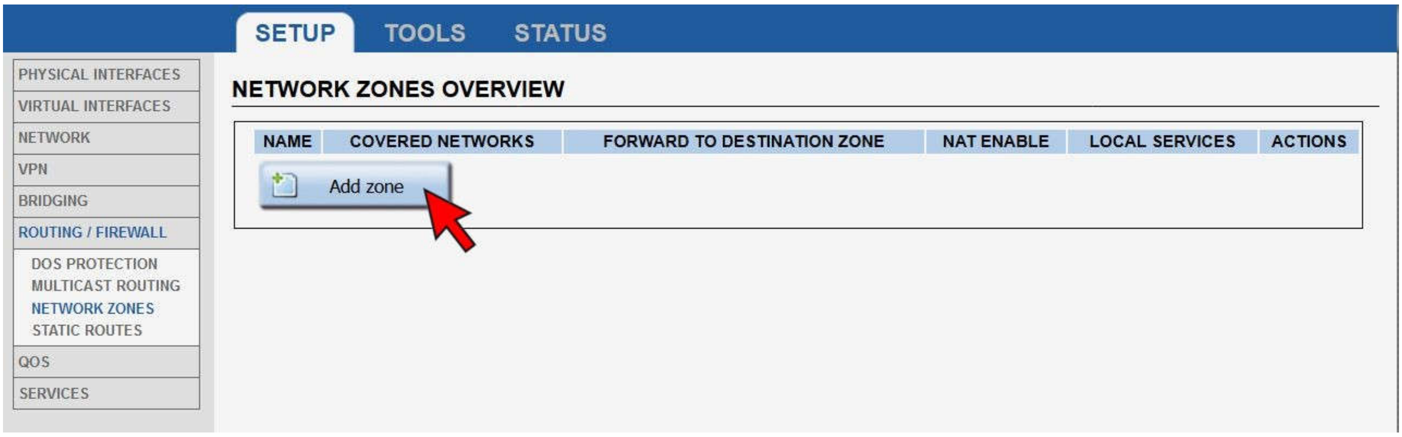
Click on **Routing/Firewall**



NETWORK OVERVIEW

NAME	ENABLED	IP ADDRESS	NETMASK	GATEWAY	PERSISTENCE	ACTIONS
PUBLIC	☑	192.168.1.10	255.255.255.0		Enabled	
PRIVATE	☑	192.168.100.100	255.255.255.0		Enabled	

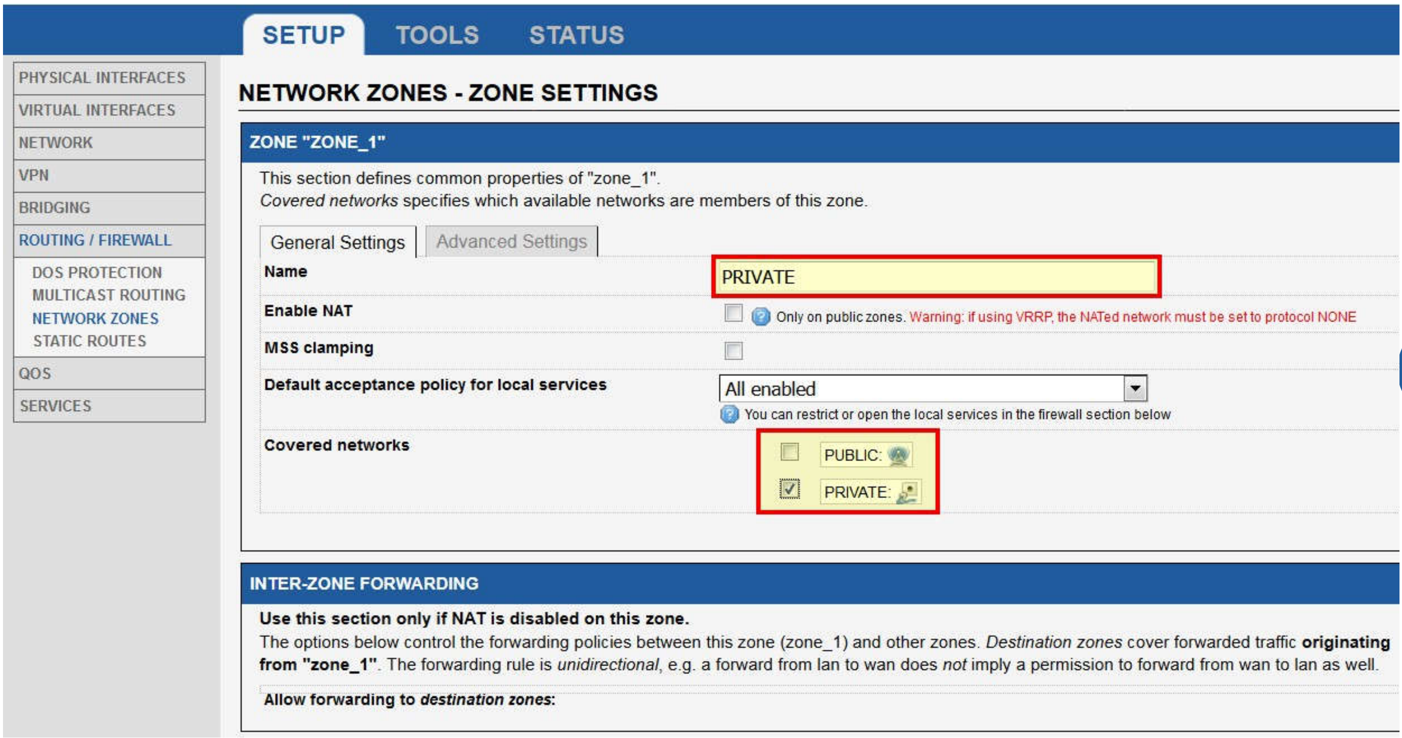
Click on **NETWORK ZONES** then **Add zone**



NETWORK ZONES OVERVIEW

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	NAT ENABLE	LOCAL SERVICES	ACTIONS

Name the zone **PRIVATE** then select **PRIVATE network**



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: PRIVATE

Enable NAT: □ Only on public zones. 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

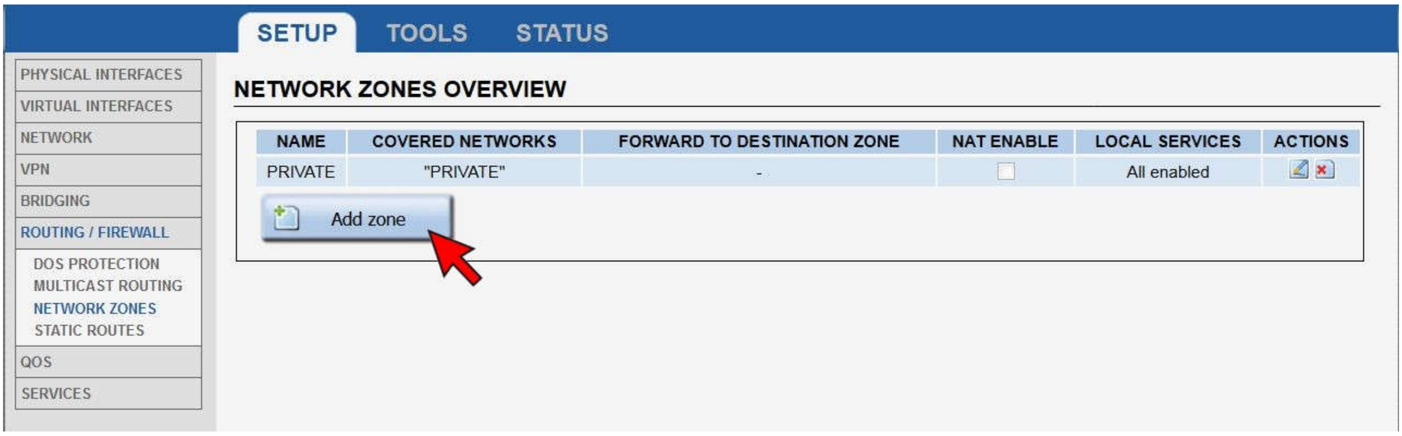
Covered networks: □ PUBLIC: ☑ PRIVATE:

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (zone_1) and other zones. *Destination zones* cover forwarded traffic **originating from "zone_1"**. 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*:

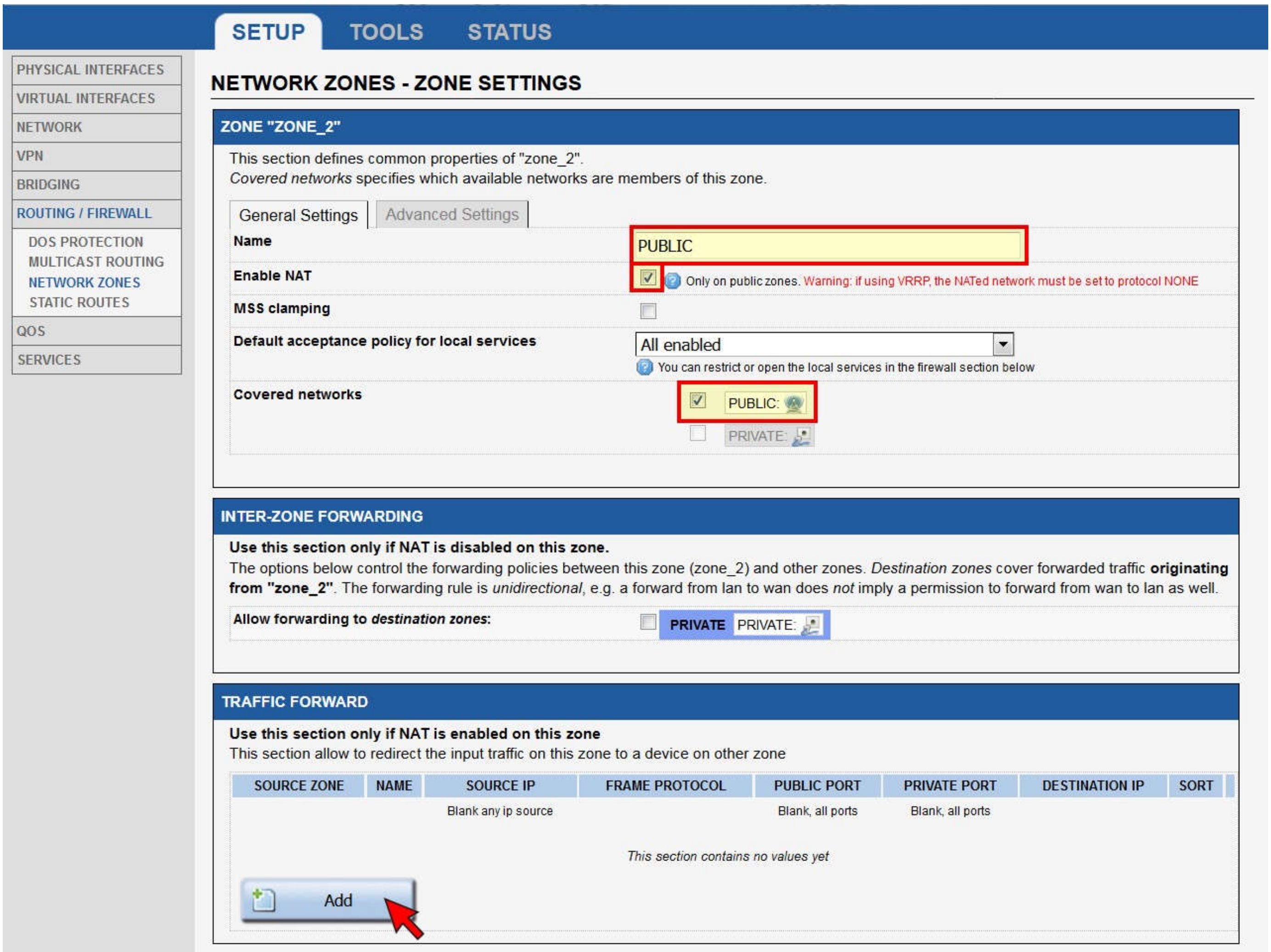
Save and add a new zone from **NETWORK ZONE**



NETWORK ZONES OVERVIEW

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	NAT ENABLE	LOCAL SERVICES	ACTIONS
PRIVATE	"PRIVATE"	-	□	All enabled	

Name the new area **PUBLIC**, check **NAT** and select the **PUBLIC** network, then **Add** in **TRAFFIC FORWARD**.



NETWORK ZONES - ZONE SETTINGS

ZONE "ZONE_2"

This section defines common properties of "zone_2".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name	PUBLIC
Enable NAT	☑ Only on public zones. 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 NAT is disabled on this zone.
The options below control the forwarding policies between this zone (zone_2) and other zones. *Destination zones* cover forwarded traffic **originating from "zone_2"**. 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*: □ PRIVATE PRIVATE:

TRAFFIC FORWARD

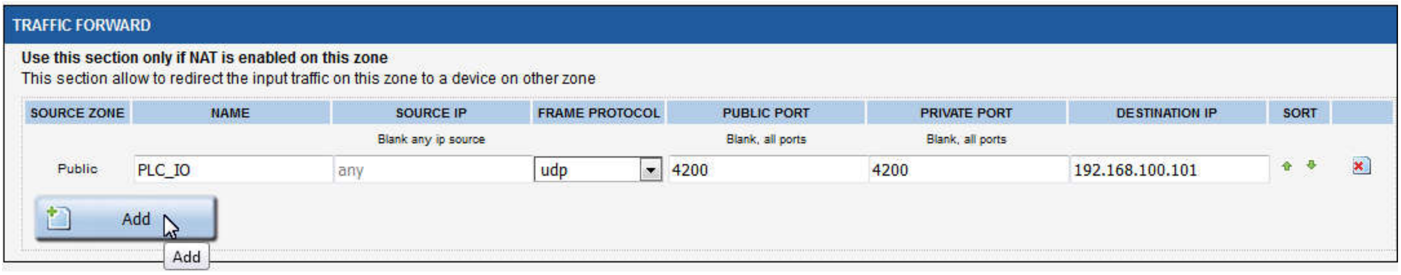
Use this section only if NAT is enabled on this zone
This section allow to redirect the input traffic on this zone to a device on other zone

SOURCE ZONE	NAME	SOURCE IP	FRAME PROTOCOL	PUBLIC PORT	PRIVATE PORT	DESTINATION IP	SORT
		Blank any ip source		Blank, all ports	Blank, all ports		

This section contains no values yet

Add

Fill in the required fields for the first translation rule, then add the second rule

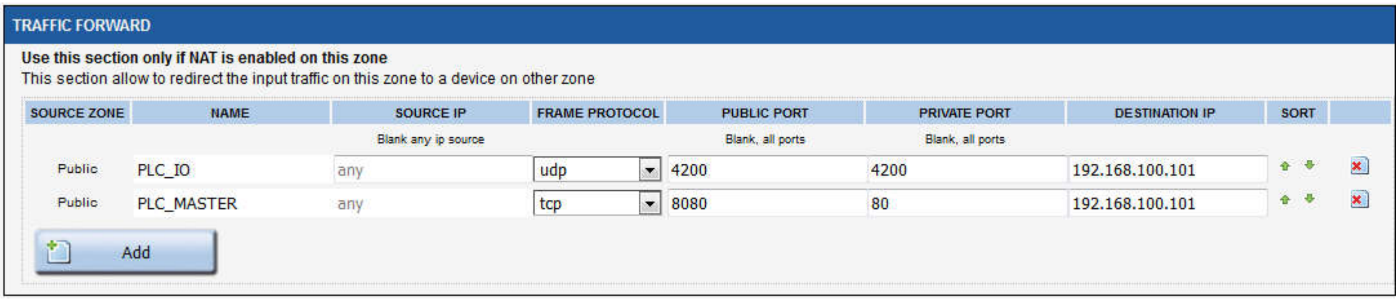


TRAFFIC FORWARD

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

SOURCE ZONE	NAME	SOURCE IP	FRAME PROTOCOL	PUBLIC PORT	PRIVATE PORT	DESTINATION IP	SORT
		Blank any ip source		Blank, all ports	Blank, all ports		
Public	PLC_IO	any	udp	4200	4200	192.168.100.101	

Add



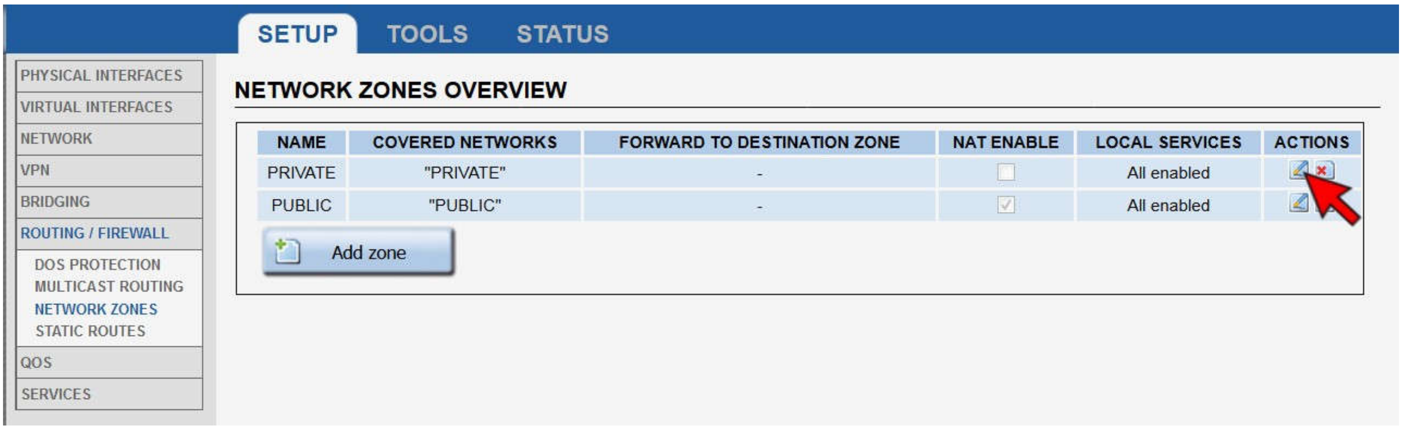
TRAFFIC FORWARD

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

SOURCE ZONE	NAME	SOURCE IP	FRAME PROTOCOL	PUBLIC PORT	PRIVATE PORT	DESTINATION IP	SORT
		Blank any ip source		Blank, all ports	Blank, all ports		
Public	PLC_IO	any	udp	4200	4200	192.168.100.101	
Public	PLC_MASTER	any	tcp	8080	80	192.168.100.101	

Add

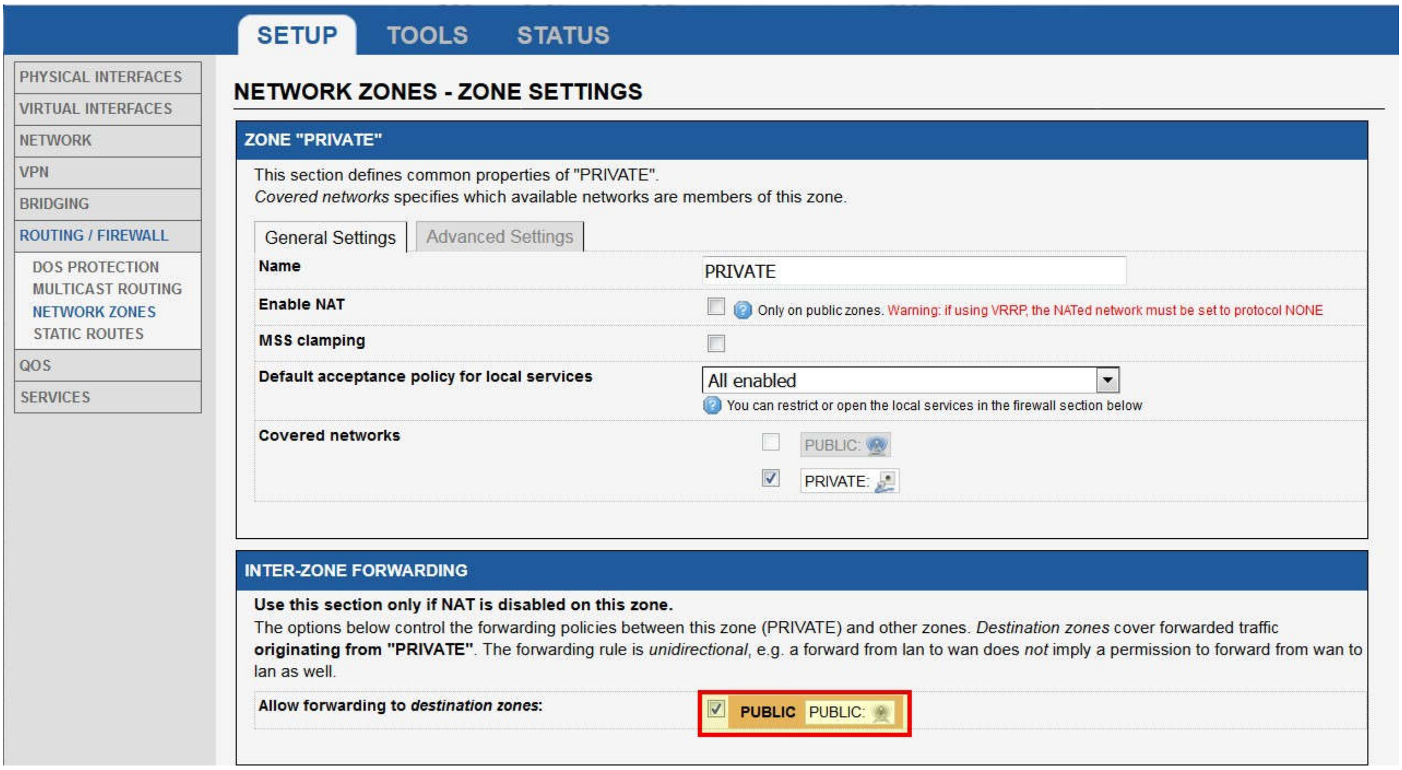
Save and return to **NETWORK ZONE** to edit the **PRIVATE** area



NETWORK ZONES OVERVIEW

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	NAT ENABLE	LOCAL SERVICES	ACTIONS
PRIVATE	"PRIVATE"	-	□	All enabled	
PUBLIC	"PUBLIC"	-	☑	All enabled	

In **INTER-ZONE FORWARDING**, allow routing to the **PUBLIC** area, then **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.

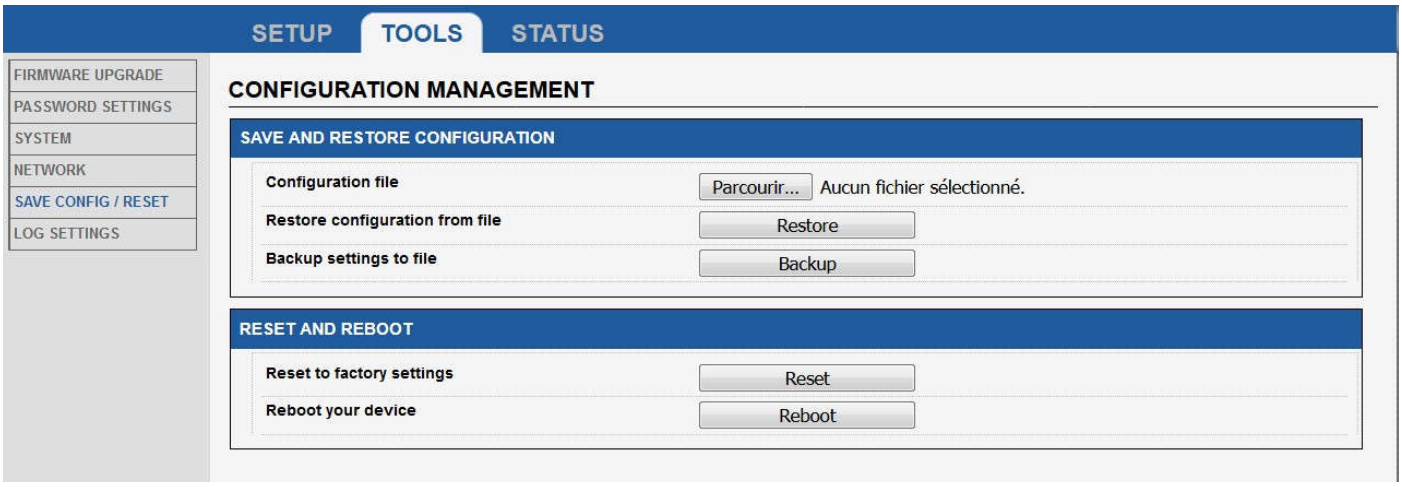
Name	PRIVATE
Enable NAT	□ Only on public zones. Warning: if using VRRP, the NATed network must be set to protocol NONE
MSS clamping	□
Default acceptance policy for local services	All enabled You can restrict or open the local services in the firewall section below
Covered networks	□ PUBLIC: ☑ PRIVATE:

INTER-ZONE FORWARDING

Use this section only if NAT is disabled on this zone.
The options below control the forwarding policies between this zone (PRIVATE) and other zones. *Destination zones* cover forwarded traffic **originating from "PRIVATE"**. 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:

You will now be able to reboot to activate the new configuration. In **TOOLS/SAVE CONFIG**, click **REBOOT**. At this point, make sure your PC is configured on the **PRIVATE** network subnet of the product (192.168.100.0/24) to return to the administration.



CONFIGURATION MANAGEMENT

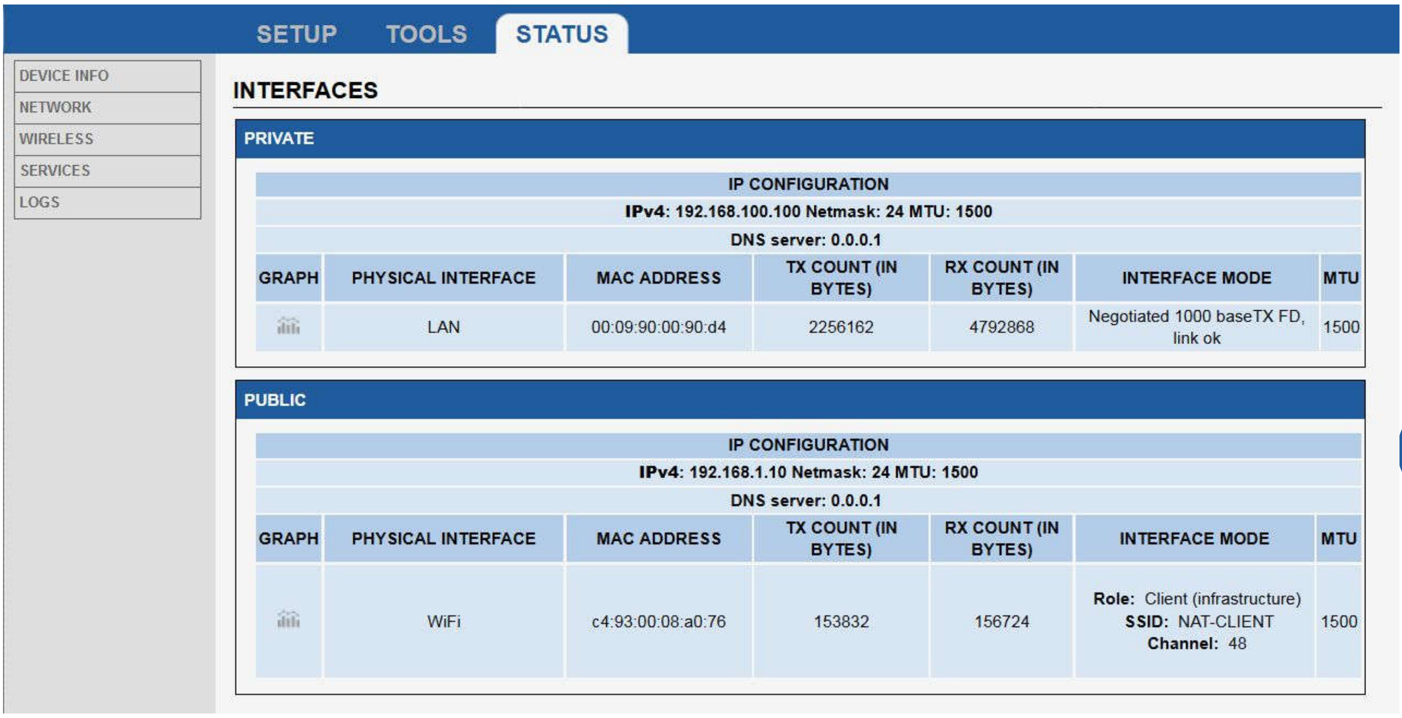
SAVE AND RESTORE CONFIGURATION

Configuration file	Parcourir... Aucun fichier sélectionné.
Restore configuration from file	Restore
Backup settings to file	Backup

RESET AND REBOOT

Reset to factory settings	Reset
Reboot your device	Reboot

After reboot, you can check that the physical interfaces are functional in the **STATUS/NETWORK** page



INTERFACES

PRIVATE

IP CONFIGURATION

IPv4: 192.168.100.100 Netmask: 24 MTU: 1500

DNS server: 0.0.0.1

GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	LAN	00:09:90:00:90:d4	2256162	4792868	Negotiated 1000 baseTX FD, link ok	1500

PUBLIC

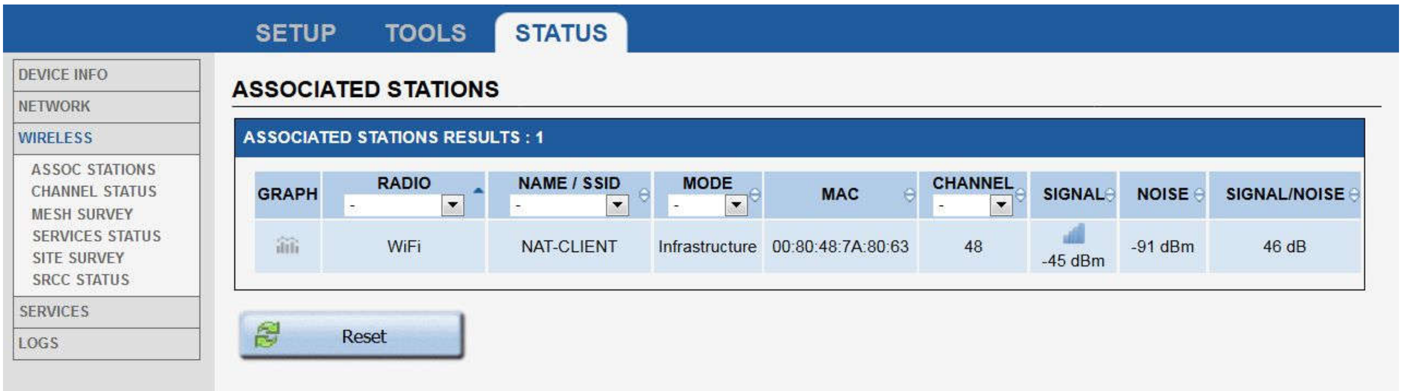
IP CONFIGURATION

IPv4: 192.168.1.10 Netmask: 24 MTU: 1500

DNS server: 0.0.0.1

GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	WiFi	c4:93:00:08:a0:76	153832	156724	**Role:** Client (infrastructure) **SSID:** NAT-CLIENT **Channel:** 48	1500

If the access point is within range, you can check in **STATUS/WIRELESS/ASSOC STATIONS** that the product is correctly associated



ASSOCIATED STATIONS

ASSOCIATED STATIONS RESULTS : 1

GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	-	-	-		-			
	WiFi	NAT-CLIENT	Infrastructure	00:80:48:7A:80:63	48	-45 dBm	-91 dBm	46 dB