

## HOWTO setup Proxicast for streaming data from GPS receiver

1. Under “Advanced” -> “NAT” add the NetRS streaming port to the “Port Forwarding” table:

NAT

The screenshot shows the 'Port Forwarding Rules' configuration page in the Proxicast NAT section. The 'WAN Interface' is set to 'Cellular'. The 'Default Server' is '0.0.0.0'. The 'Go To Page' is '1'. The table below lists the port forwarding rules.

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	NetRS HTTP	8080 - 8080	8080 - 8080	192.168.1.2
2	<input checked="" type="checkbox"/>	NetRS HTTP	8443 - 8443	8443 - 8443	192.168.1.2
3	<input checked="" type="checkbox"/>	NetRS FTP	20 - 21	20 - 21	192.168.1.2
4	<input checked="" type="checkbox"/>	NetRS HTTP	80 - 80	80 - 80	192.168.1.2
5	<input checked="" type="checkbox"/>	NetRS HTTP	443 - 443	443 - 443	192.168.1.2
6	<input checked="" type="checkbox"/>	NetRS FTP	8020 - 8021	8020 - 8021	192.168.1.2
7	<input checked="" type="checkbox"/>	NetRS FTP	5001 - 5017	5001 - 5017	192.168.1.2
8	<input type="checkbox"/>		0 - 0	0 - 0	0.0.0.0
9	<input type="checkbox"/>		0 - 0	0 - 0	0.0.0.0
10	<input type="checkbox"/>		0 - 0	0 - 0	0.0.0.0

Note 1: You may also need to create a [Firewall](#) rule.  
Note 2: Port Translation is optional.  
Note 3: You may also need to define rules for [remote management](#) ports if you set a non-zero Default Server address.

Buttons: Apply, Reset

2. Add the new ports to your firewall rules for WAN->LAN and CELL->LAN.

The screenshot shows the 'Default Rule Setup' page in the Proxicast Firewall section. The 'Enable Firewall' checkbox is checked. The 'Allow Asymmetrical Route' checkbox is also checked. The table below shows the default rules for various interfaces.

From	To	LAN	WAN	CELL	DMZ	WLAN	VPN
LAN		0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit
WAN		1 Rules Drop	0 Rules Drop	0 Rules Drop	0 Rules Permit	0 Rules Drop	0 Rules Permit
CELL		2 Rules Drop	0 Rules Drop	2 Rules Drop	0 Rules Permit	0 Rules Drop	0 Rules Permit
DMZ		0 Rules Drop	0 Rules Permit	0 Rules Permit	0 Rules Drop	0 Rules Drop	0 Rules Permit
WLAN		0 Rules Drop	0 Rules Permit	0 Rules Permit	0 Rules Drop	0 Rules Drop	0 Rules Permit
VPN		0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit























Buttons: Apply, Reset

3. Create a new “firewall rule”.

The screenshot shows the 'Rule Summary' page in the Proxicast Firewall section. The 'Packet Direction' is set to 'WAN to LAN'. The table below shows the summary of the rules.

#	Name	Active	Source Address	Destination Address	Service Type	Action	Sch.	Log	Modify
1	NetRS Ports	Y	Any	Any	*NetRS All FTP Port 8021(TCP:8021)	Permit	No	No	

## Custom Service

#	Service Name	Protocol	Attribute*	Modify
1	ECHO REPLY	ICMP	0/0	 
2	ECHO REQUEST	ICMP	8/0	 
3	NetRS All FTP Port 8021	TCP	8021	 
4	NetRS All HTTP Port 8080	TCP	8080	 
5	NetRS All HTTPS Port 8443	TCP	8443	 
6	NetRS streaming	TCP/UDP	5001~5017	 
7	PRX-FTP	TCP	7721	 
8	PRX-HTTP	TCP	7780	 
9	PRX-HTTPS	TCP	7443	 
10	PRX-SSH	TCP	7722	 
11	VPN_NAT_T	UDP	4500	 

\*Attribute: Port Range for TCP/UDP, Type/Code for ICMP.

Add

Rule Name All NetRS Ports

## Edit Source Address

Address Editor

Address Type

Start IP Address

End IP Address

Subnet Mask

Add

Modify

Any Address

0 . 0 . 0 . 0

0 . 0 . 0 . 0

0 . 0 . 0 . 0

Source Address(es)

Any

Delete

## Edit Destination Address

Address Editor

Address Type

Start IP Address

End IP Address

Subnet Mask

Add

Modify

Any Address

0 . 0 . 0 . 0

0 . 0 . 0 . 0

0 . 0 . 0 . 0

Destination Address(es)

Any

Delete

## Edit Service

Available Services (See Service)

\*ECHO REPLY(ICMP Type:0/Code:0)  
\*ECHO REQUEST(ICMP Type:8/Code:0)  
\*NetRS All HTTPS Port 8443(TCP:8443)  
\*PRX-FTP(TCP:7721)  
\*PRX-HTTP(TCP:7780)  
\*PRX-HTTPS(TCP:7443)  
\*PRX-SSH(TCP:7722)  
\*VPN\_NAT\_T(UDP:4500)  
\*AMNEW\_ICM(TCP:5190)  
\*AUTH(TCP:113)  
\*BGP(TCP:179)  
\*BOOTP\_CLIENT(UDP:68)  
\*BOOTP\_SERVER(UDP:67)  
\*CJ-SEMI(TCP/UDP:7648,24032)  
\*DNS(TCP/UDP:53)

&lt;&lt;

&gt;&gt;

Selected Service(s)

\*NetRS All FTP Port 8021(TCP:8021)  
\*NetRS All HTTP Port 8080(TCP:8080)  
\*NetRS streaming(TCP/UDP:5001-5017)

## Edit Schedule

Day to Apply:

☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat

Time of Day to Apply: (24-Hour Format)

☒ All day

Start: 0 (Hour) 0 (Minute) End: 0 (Hour) 0 (Minute)

## Actions When Matched

☐ Log Packet Information When Matched☐ Send Alert Message to Administrator When Matched

Action for Matched Packets

Permit

Apply

Cancel