

1. Add port forwarding for this PC. Open Firewall → Port Forwards like this:

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
This section contains no values yet				

New port forward:

Name	Protocol	External port	Internal IP address	Internal port
DNP_PF	TCP	20000	192.168.8.100	20000

Buttons: Save & Apply, Save, Reset

2. Add a new port forward rule, external port 20000(can be changed), Internal IP address is the IP address of PC. Then click button “Add”, then click Save&Apply.

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
DNP_PF	IPv4-TCP From any host in wan Via any router IP at port 20000	IP 192.168.8.100, port 20000 in lan	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

New port forward:

Name	Protocol	External port	Internal IP address	Internal port
	TCP+UDP			

Buttons: Save & Apply, Save, Reset

3. Add 2 Traffic Rules. Open Firewall → Traffic Rules, and scroll down.

Open ports on router:

Name	Protocol	External port
	TCP+UDP	

Buttons: Add

New forward rule:

Name	Source zone	Destination zone
	lan	wan

Buttons: Add and edit...

Buttons: Save & Apply, Save, Reset

4. Add new forward rule, input the name then click button “Add and edit ...”

Open ports on router:

Name	Protocol	External port
<input type="text"/>	TCP+UDP <input type="button" value="v"/>	<input type="text"/>

New forward rule:

Name	Source zone	Destination zone
ACCEPT_DNP3	lan <input type="button" value="v"/>	wan <input type="button" value="v"/>

- Change Protocol from TCP+UDP to TCP if UDP is not used.

Firewall - Traffic Rules - ACCEPT_DNP3

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled





Name

Restrict to address family

Protocol

Match ICMP type

Source zone

- Any zone
- lan: lan: 
- openvpn: (empty)
- vpnzone: (empty)
- wan: wan:  wan6:  ifmobile: 

- Configure source port to 20000, then click Save & Apply.

Source MAC address

Source address

Source port

Destination zone

- Device (input)
- Any zone (forward)
- lan: lan:
- openvpn: (empty)
- vpnzone: (empty)
- wan: wan: wan6: ifmobile:

Destination address

Destination port

Action

7. Create a new rule to block all traffic from LAN to WAN BLOCK_ALL. Click button “Add and edit...”

second

ACCEPT_DNP3	Any TCP From <i>any host</i> in <i>lan</i> with source port 20000 To <i>any host</i> in <i>wan</i>	Accept forward	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
-------------	--	----------------	-------------------------------------	-------------------------------------	---------------------------------------

Open ports on router:

Name	Protocol	External port
<input type="text"/>	TCP+UDP <input type="text"/>	<input type="text"/>

New forward rule:

Name	Source zone	Destination zone
BLOCK_ALL	lan	wan

8. Change protocol from TCP+UDP to any.

Firewall - Traffic Rules - BLOCK_ALL

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled

Name

Restrict to address family

Protocol

Match ICMP type

Source zone

- Any zone
- lan: lan:
- openvpn: (empty)
- vpnzone: (empty)
- wan: wan: wan6: ifmobile:

9. Scroll down, change Action from accept to drop. Then click Save& Apply.

Destination zone

- Device (input)
- Any zone (forward)
- lan: lan:
- openvpn: (empty)
- vpnzone: (empty)
- wan: wan: wan6: ifmobile:

Destination address

Destination port

Action

Extra arguments

[Back to Overview](#)

[Save & Apply](#)

[Save](#)

[Reset](#)

10. Go back to Traffic Rules list page, make sure that BLOCL_ALL rule is at the end of list.

To any router IP on this device

Allow-ICMPv6-Input	IPv6-ICMP with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement</i> From any host in wan To any router IP on this device	Accept input and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Allow-ICMPv6-Forward	IPv6-ICMP with types <i>echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type</i> From any host in wan To any host in any zone	Accept forward and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
ACCEPT_DNP3	Any TCP From any host in lan with source port 20000 To any host in wan	Accept forward	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
BLOCK_ALL	Any traffic From any host in lan To any host in wan	Discard forward	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Open ports on router:

Name	Protocol	External port
<input type="text"/>	TCP+UDP <input type="button" value="v"/>	<input type="text"/>
<input type="button" value="Add"/>		

New forward rule:

Name	Source zone	Destination zone
------	-------------	------------------