Setting Up Wi-Fi in pfSense

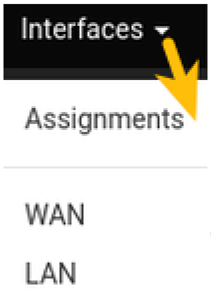
Configuration Guide

Please follow the below mentioned steps to setup wireless interface in pfSense 2.4.X:

1. Add wireless interface
2. Assign newly created wireless interface
3. Configure the interface
4. Configure DHCP for the interface
5. Allow the Wi-Fi interface traffic through the firewall.

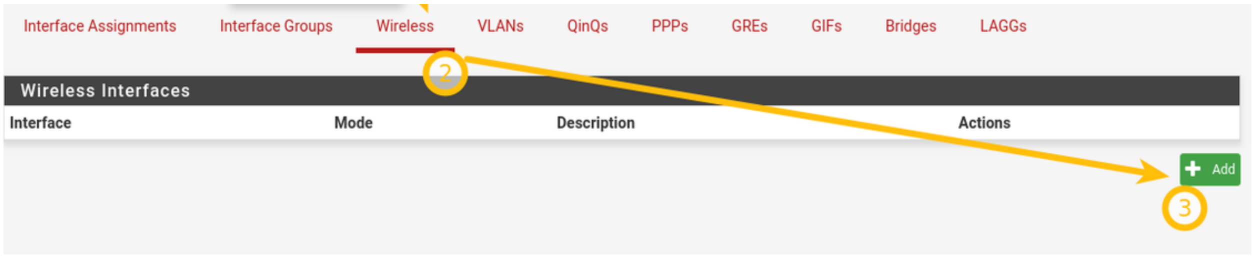
1. Add wireless interface

Select “interfaces” from the top left-hand corner then go for “Assignments”.



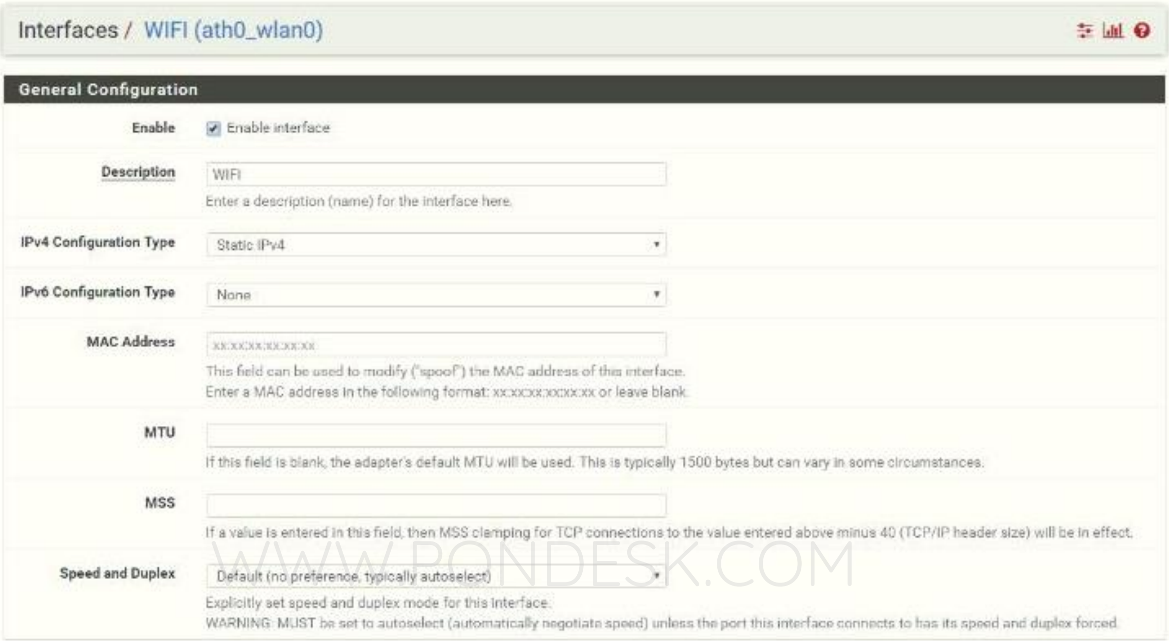
2. Assign newly created wireless interface

Select “wireless” then select “add”.



3. Configure the interface

“Enable the interface” by putting a checkmark. Provide the necessary description. Select the configuration type as “IPv4”. Leave “mac, mtu, mss, speed and duplex” as blank.



Interfaces / WIFI (ath0_wlan0)

General Configuration

Enable: ☑ Enable interface

Description: WIFI
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

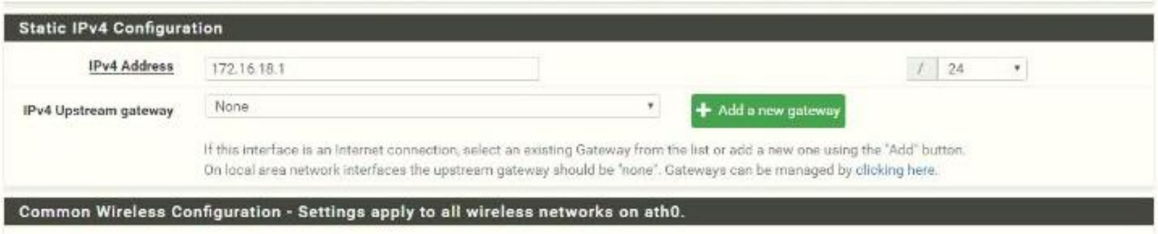
MAC Address: xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Now assign an IP address to the interface.



Static IPv4 Configuration

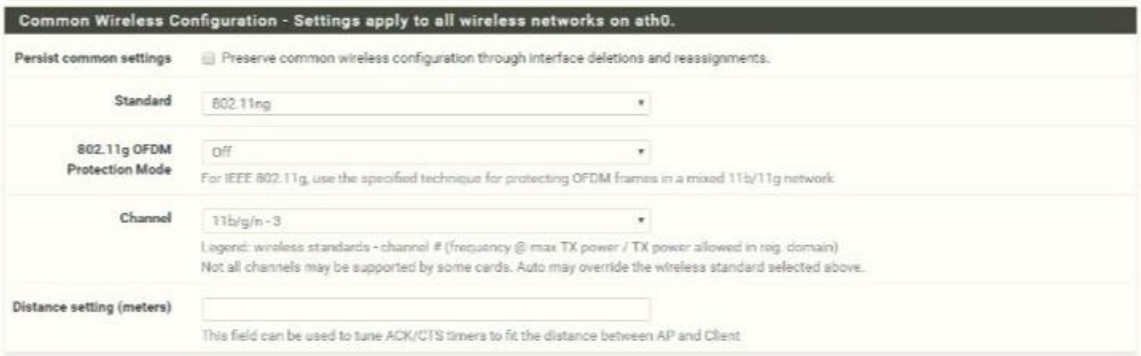
IPv4 Address: 172.16.18.1 / 24

IPv4 Upstream gateway: None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

Common Wireless Configuration - Settings apply to all wireless networks on ath0.

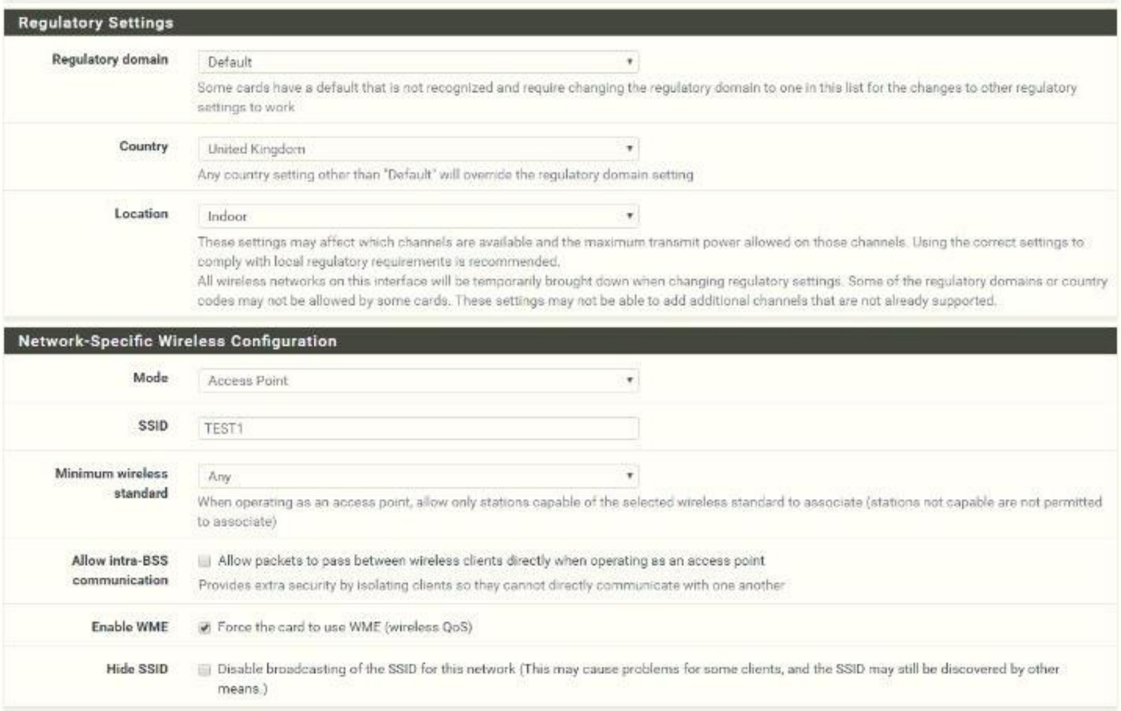
Now we need to configure the Wi-Fi settings for connectivity. Select the standard as "802.11 ng".



Common Wireless Configuration - Settings apply to all wireless networks on ath0.

Persist common settings	□ Preserve common wireless configuration through interface deletions and reassignments.
Standard	802.11ng ▾
802.11g OFDM Protection Mode	Off ▾ For IEEE 802.11g, use the specified technique for protecting OFDM frames in a mixed 11b/11g network
Channel	11b/g/n - 3 ▾ Legend: wireless standards - channel # (frequency @ max TX power / TX power allowed in reg. domain) Not all channels may be supported by some cards. Auto may override the wireless standard selected above.
Distance setting (meters)	 This field can be used to tune ACK/CTS timers to fit the distance between AP and Client

Leave the "802.11 OFDM Protection Mode" off select channel as per your requirement but channels "1, 6 and 11" are non-overlapping channels which are recommended if you are planning to install Access Points in a multi-story building or an apartment and leave the distance setting as blank.



Regulatory Settings

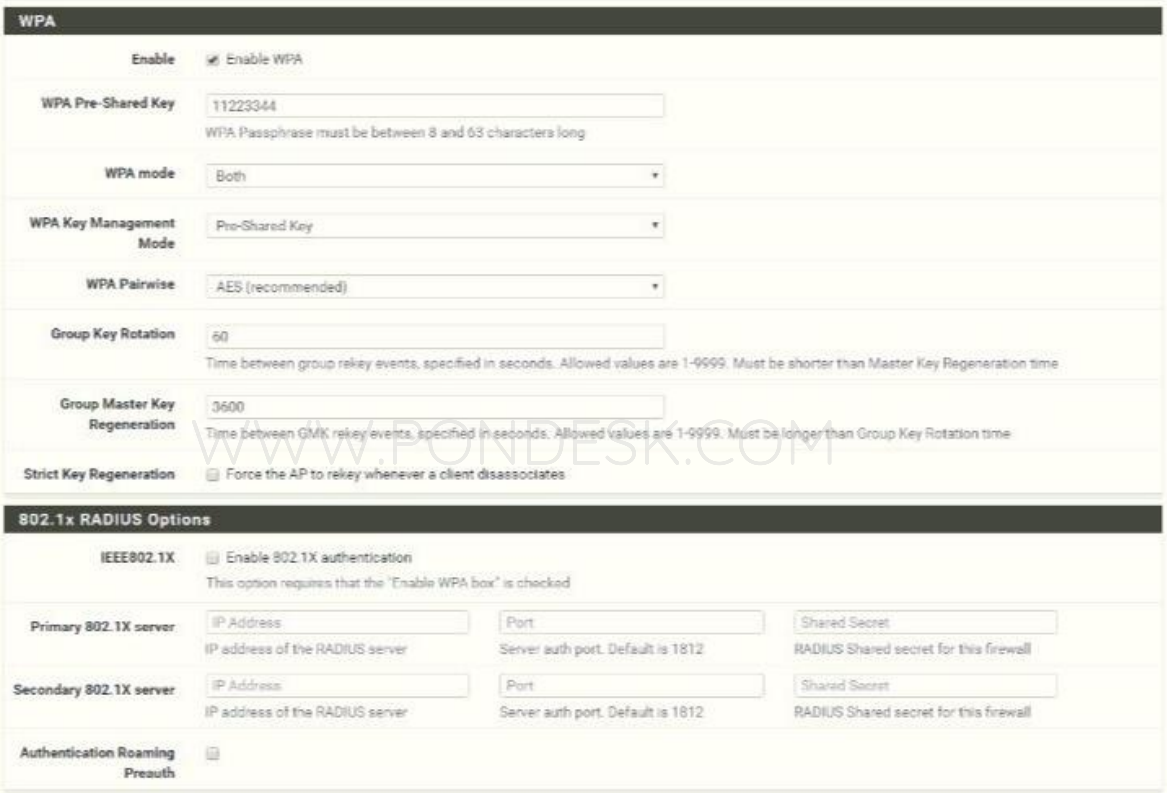
Regulatory domain	Default ▾ Some cards have a default that is not recognized and require changing the regulatory domain to one in this list for the changes to other regulatory settings to work
Country	United Kingdom ▾ Any country setting other than "Default" will override the regulatory domain setting
Location	Indoor ▾ These settings may affect which channels are available and the maximum transmit power allowed on those channels. Using the correct settings to comply with local regulatory requirements is recommended. All wireless networks on this interface will be temporarily brought down when changing regulatory settings. Some of the regulatory domains or country codes may not be allowed by some cards. These settings may not be able to add additional channels that are not already supported.

Network-Specific Wireless Configuration

Mode	Access Point ▾
SSID	TEST1
Minimum wireless standard	Any ▾ When operating as an access point, allow only stations capable of the selected wireless standard to associate (stations not capable are not permitted to associate)
Allow intra-BSS communication	□ Allow packets to pass between wireless clients directly when operating as an access point Provides extra security by isolating clients so they cannot directly communicate with one another
Enable WME	☑ Force the card to use WME (wireless QoS)
Hide SSID	□ Disable broadcasting of the SSID for this network (This may cause problems for some clients, and the SSID may still be discovered by other means.)

Keep the regulatory domain as “default”. Select the appropriate “country” and location as “indoor”. Select the “Mode” as “Access Point”. Choose an appropriate SSID for broadcast. Set the “minimum wireless standard to “Any”. Allow intra-BSS communication unchecked and enable “WME”.

Now for the wireless security enable “WPA”, set the “WPA Pre-Shared Key”, mode as “both”, WPA Key Management Mode as “Pre-Shared Key”, WPA Pairwise “AES (recommended)”.



WPA

Enable	☑ Enable WPA		
WPA Pre-Shared Key	11223344 WPA Passphrase must be between 8 and 63 characters long		
WPA mode	Both ▾		
WPA Key Management Mode	Pre-Shared Key ▾		
WPA Pairwise	AES (recommended) ▾		
Group Key Rotation	60 Time between group rekey events, specified in seconds. Allowed values are 1-9999. Must be shorter than Master Key Regeneration time		
Group Master Key Regeneration	3600 Time between GMK rekey events, specified in seconds. Allowed values are 1-9999. Must be longer than Group Key Rotation time		
Strict Key Regeneration	□ Force the AP to rekey whenever a client disassociates		

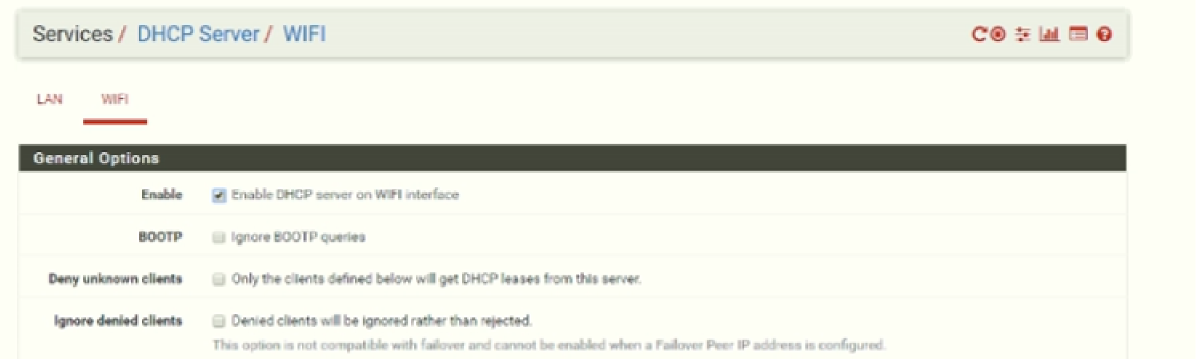
802.1x RADIUS Options

IEEE802.1X	□ Enable 802.1X authentication This option requires that the "Enable WPA box" is checked		
Primary 802.1X server	IP Address IP address of the RADIUS server	Port Server auth port. Default is 1812	Shared Secret RADIUS Shared secret for this firewall
Secondary 802.1X server	IP Address IP address of the RADIUS server	Port Server auth port. Default is 1812	Shared Secret RADIUS Shared secret for this firewall
Authentication Roaming Preauth	□		

Now save the configuration.

4. Configure DHCP Server

Go to “services” then select “DHCP Server”. Here you will find your newly created interface. Select it and click on the check box “Enabled DHCP Server” on the new interface.

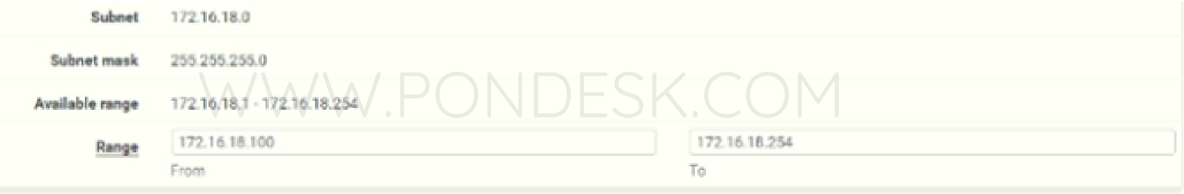


Services / DHCP Server / WIFI

General Options

Enable	☑ Enable DHCP server on WIFI interface
BOOTP	□ Ignore BOOTP queries
Deny unknown clients	□ Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	□ Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Scroll down and specify the IP address range for wireless clients.

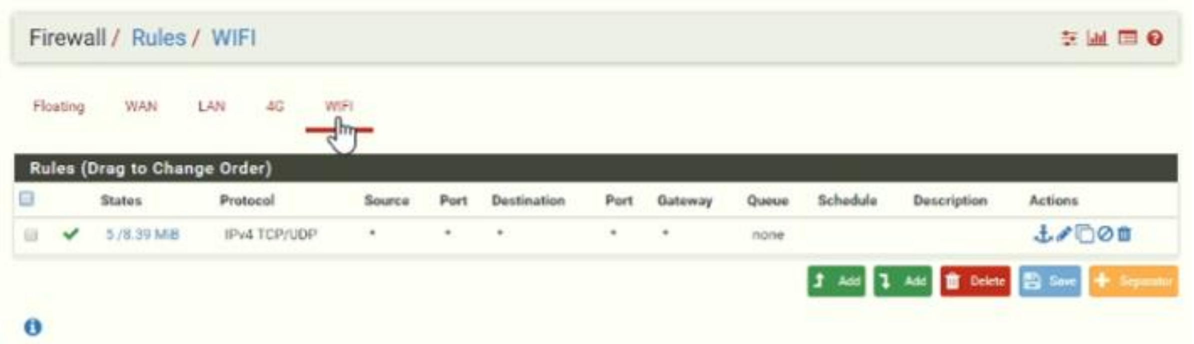


Subnet	172.16.18.0	
Subnet mask	255.255.255.0	
Available range	172.16.18.1 - 172.16.18.254	
Range	172.16.18.100 From	172.16.18.254 To

Now save the configuration.

5. Allow the Wi-Fi interface traffic through firewall

Go to “Firewall” then select “Rules”.

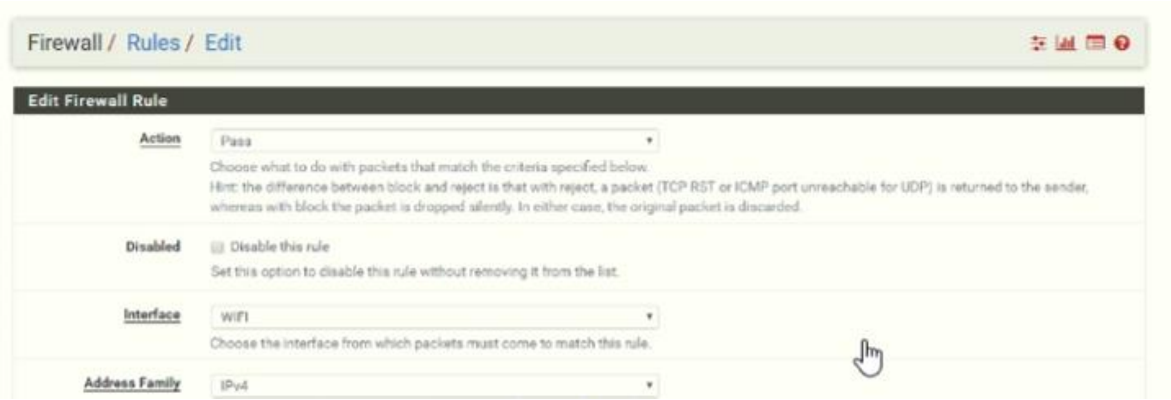


Firewall / Rules / WIFI

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	5 /8.39 MiB	IPv4 TCP/UDP	*	*	*	*	*	none			

Now select the newly created interface and select “Add”.



Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule

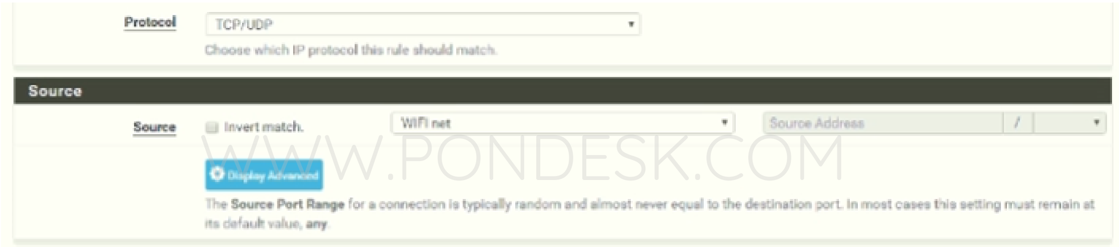
Set this option to disable this rule without removing it from the list.

Interface: WiFI

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Set the action to “Pass”, interface should be “wifi or wireless”, address family “IPv4” and protocol should be “TCP/UDP”. Source should be “Wifi or wireless net”.



Protocol: TCP/UDP

Choose which IP protocol this rule should match.

Source

Source: □ Invert match. WiFI net Source Address /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination should be “Any” as we wish to let the traffic go to the Internet. Provide a description as per your requirement while creating the rule in the “description” section then save the rule. You are good to go now.

THANK YOU

--

PONDESK SUPPORT TEAM

https://www.pondesk.com