

LAB 1 – Networking & Interface Configuration

The image displays two screenshots of the pfSense web interface, specifically the 'Interfaces / WAN (em1)' configuration page. The browser address bar shows the URL `192.168.56.101/interfaces.php?if=wlan`.

Top Screenshot: The 'General Configuration' tab is active. The 'Enable' section has the 'Enable interface' checkbox checked. The 'Description' field contains 'WAN'. The 'IPv4 Configuration Type' is set to 'DHCP'. The 'IPv6 Configuration Type' is set to 'DHCP6'. The 'MAC Address' field contains 'xxxxxxxxxxxx'. The 'MTU' and 'MSS' fields are empty. The 'Speed and Duplex' dropdown is set to 'Default (no preference, typically autoselect)'. Below the configuration fields, the 'DHCP Client Configuration' section is visible, with 'Options' checked and 'Advanced Configuration' and 'Configuration Override' unchecked.

Bottom Screenshot: The 'General Configuration' tab is still active. A red warning message at the top states: 'WARNING: The password for this account is insecure. Password is currently set to the default value (pfsense). Change the password as soon as possible.' Below this, a yellow message box indicates: 'The WAN configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying.' A green 'Apply Changes' button is present. In the configuration fields, the 'IPv4 Configuration Type' has been changed to 'Static IPv4', while all other settings remain the same as in the top screenshot.

The WAN configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

General Configuration

Enable ☒ Enable interface

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

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type DHCP6

MAC Address xxxxxxxxxxxx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxx: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 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 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.

Static IPv4 Configuration

LAB 2 – Firewall Rule Logic & Policy Enforcement

hhh

WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address 192.168.10.1 / 24

IPv4 Upstream gateway None [+ Add a new gateway](#)
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".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by [clicking here](#).

DHCPv6 Client Configuration

Options ☐ Advanced Configuration ☐ Configuration Override
Use advanced DHCPv6 configuration options. Override the configuration from this file.

Use IPv4 connectivity as parent interface ☐ Request a IPv6 prefix/information through the IPv4 connectivity link

Request only an IPv6 prefix ☐ Only request an IPv6 prefix, do not request an IPv6 address

DHCPv6 Prefix Delegation size 64
The value in this field is the delegated prefix length provided by the DHCPv6 server. Normally specified by the ISP.

Send IPv6 prefix hint ☐ Send an IPv6 prefix hint to indicate the desired prefix size for delegation

Do not wait for a RA ☐ Required by some ISPs, especially those not using PPPoE

Reserved Networks

Block private networks and loopback addresses ☐
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7), as well as loopback addresses (127.0.0.0/8). This notice should remain, but need not contain this network interface resides in such a

LAB 2 – Firewall Rule Logic & Policy Enforcement

17 matched log entries.Max(50)					
Act	Time	If	Source	Destination	Proto
	Oct 19 01:51:46	LAN	192.168.1.10	159.153.226.105	ICMP
	Oct 19 01:51:45	LAN	192.168.1.10	159.153.225.30	ICMP
	Oct 19 01:51:43	LAN	192.168.1.10	159.153.93.2	ICMP
	Oct 19 01:51:42	LAN	192.168.1.10	64.125.199.186	ICMP
	Oct 19 01:51:40	LAN	192.168.1.10	64.125.31.206	ICMP
	Oct 19 01:51:39	LAN	192.168.1.10	64.125.25.113	ICMP
	Oct 19 01:51:37	LAN	192.168.1.10	64.125.25.46	ICMP
	Oct 19 01:51:36	LAN	192.168.1.10	64.125.30.233	ICMP
	Oct 19 01:51:34	LAN	192.168.1.10	64.125.31.234	ICMP
	Oct 19 01:51:33	LAN	192.168.1.10	64.125.24.5	ICMP
	Oct 19 01:51:32	LAN	192.168.1.10	75.149.228.134	ICMP
	Oct 19 01:51:30	LAN	192.168.1.10	68.86.87.18	ICMP
	Oct 19 01:51:29	LAN	192.168.1.10	68.86.91.229	ICMP
	Oct 19 01:51:27	LAN	192.168.1.10	68.85.155.14	ICMP
	Oct 19 01:51:26	LAN	192.168.1.10	68.85.154.10	ICMP
	Oct 19 01:51:24	LAN	192.168.1.10	162.151.1.141	ICMP
	Oct 19 01:51:23	LAN	192.168.1.10	67.160.236.1	ICMP

sense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

La: Rule details

Action: block

Reason: ip-option

Tracker ID: 1757202313

Matched Rule: unavailable

Associated Rules:

@70 pass in quick on vmx1 inet proto igmp from <LAN__NETWORK:1> to 239.255.255.250 keep state (if-bound) label "USER_RULE: Passed via EasyRule" label "id:1757202313" ridentifier 1757202313

×	Sep 7 10:17:10	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP
×	Sep 7 10:17:05	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP
×	Sep 7 10:17:05	LAN	Passed via EasyRule (1757202313)	192.168.1.70	239.255.255.250	IGMP
×	Sep 7 10:16:03	LAN	Passed via EasyRule (1757202313)	192.168.1.155	239.255.255.250	IGMP
×	Sep 7 10:16:02	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP
×	Sep 7 10:15:07	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP
×	Sep 7 10:15:06	LAN	Passed via EasyRule (1757202313)	192.168.1.155	239.255.255.250	IGMP
×	Sep 7 10:15:01	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP

Sense System Interfaces Firewall Services VPN Status Diagnostics Help

Status / System Logs / Firewall / Normal View

System **Firewall** DHCP Authentication IPsec PPP PPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Rule details

- Action: block
- Reason: ip-option
- Tracker ID: 1757202313
- Matched Rule: unavailable
- Associated Rules:
- @70 pass in quick on vxm1 inet proto igmp from <LAN__NETWORK:1> to 239.255.255.250 keep state (if-bound) label "USER_RULE: Passed via EasyRule" label "id:1757202313" identifier 1757202313

	Time	Direction	Source	Destination	Protocol	Port	Service	State	Label	Identifier
×	Sep 7 10:17:10	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP				
×	Sep 7 10:17:05	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP				
×	Sep 7 10:17:05	LAN	Passed via EasyRule (1757202313)	192.168.1.70	239.255.255.250	IGMP				
×	Sep 7 10:16:03	LAN	Passed via EasyRule (1757202313)	192.168.1.155	239.255.255.250	IGMP				
×	Sep 7 10:16:02	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP				
×	Sep 7 10:15:07	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP				
×	Sep 7 10:15:06	LAN	Passed via EasyRule (1757202313)	192.168.1.155	239.255.255.250	IGMP				
×	Sep 7 10:15:01	LAN	Passed via EasyRule (1757202313)	192.168.1.45	239.255.255.250	IGMP				



Port Forward 1:1 Outbound NPt

Outbound NAT Mode

Mode



Automatic outbound NAT rule generation. (IPsec passthrough included)



Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)



Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)



Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<div><div>↑ Add</div><div>↓ Add</div><div>🗑 Delete</div><div>🔌 Toggle</div><div>💾 Save</div></div>										

Automatic Rules

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 10.1.1.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 10.1.1.0/24	*	*	*	WAN address	*	✗	Auto created rule

Floating

WAN

LAN

IOT

GUEST

OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	*		Reserved Not assigned by IANA	*	*	*	*	Block bogus networks	
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none	OpenVPN OpenVPN Server wizard	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.100.200	5001	*	none	NAT NAS	

↑ Add

↓ Add

Delete

Save

Separator

Firewall / NAT / Outbound

Port Forward

1:1

Outbound

NPt

Outbound NAT Mode

Mode

☒ Automatic outbound NAT rule generation.
(IPsec passthrough included)

☐ Hybrid Outbound NAT rule generation.
(Automatic Outbound NAT + rules below)

☐ Manual Outbound NAT rule generation.
(AON - Advanced Outbound NAT)

☐ Disable Outbound NAT rule generation.
(No Outbound NAT rules)

Save

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<div>↑ Add</div> <div>↓ Add</div> <div> Delete</div> <div> Toggle</div> <div> Save</div>										

Automatic Rules

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description		
✓	WAN	127.0.0.0/8 ::1/128	10.1.1.0/24	172.16.10.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128	10.1.1.0/24	172.16.10.0/24	*	*	*	WAN address	*		Auto created rule

Firewall / NAT / Port Forward

Port Forward

1:1

Outbound

NPt

Rules

<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	
<input type="checkbox"/>	✓	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.1.1.13	443 (HTTPS)	Allow HTTPS access to Webserver_10.1.1.13	
<input type="checkbox"/>	✓	WAN	TCP	*	*	WAN address	80 (HTTP)	10.1.1.13	80 (HTTP)	Allow HTTP access to Webserver_10.1.1.13	
<input type="checkbox"/>	✓	WAN	TCP	*	*	WAN address	81	10.1.1.14	80 (HTTP)	Allow HTTP access to Webserver_10.1.1.14	
<input type="checkbox"/>	✓	WAN	TCP	*	*	WAN address	8443	10.1.1.14	443 (HTTPS)	Allow HTTPS access to Webserver_10.1.1.14	

↑ Add

↓ Add

Delete

Toggle

Save

Separator

Legend

Pass

Linked rule