

LAB 1 – Networking & Interface Configuration

The screenshot shows two windows of a web browser displaying the pfSense interface configuration. Both windows are titled "Interfaces / WAN (em1)".

Top Window (Configuration View):

- General Configuration:**
 - Enable:
 - Description: WAN
 - IPv4 Configuration Type: DHCP
 - IPv6 Configuration Type: DHCP6
 - MAC Address: XX:XX:XX:XX:XX:XX
 - MTU: (Blank)
 - MSS: (Blank)
 - Speed and Duplex: Default (no preference, typically autoselect)
- DHCP Client Configuration:**
 - Options: Advanced Configuration Configuration Override

Bottom Window (Confirmation Message):

- A red box highlights a "WARNING" message:

The password for this account is insecure. Password is currently set to the default value (pfSense).
Change the password as soon as possible.
- The title bar shows the URL: 192.168.56.101/interfaces.php?if=wan
- The main content area displays the same WAN configuration settings as the top window, with a green "Apply Changes" button.

LAB 2 – Firewall Rule Logic & Policy Enforcement

hh

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	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 159.153.226.105	ICMP
▶	Oct 19 01:51:45	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 159.153.225.30	ICMP
▶	Oct 19 01:51:43	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 159.153.93.2	ICMP
▶	Oct 19 01:51:42	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 64.125.199.186	ICMP
▶	Oct 19 01:51:40	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 64.125.31.206	ICMP
▶	Oct 19 01:51:39	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 64.125.25.113	ICMP
▶	Oct 19 01:51:37	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 64.125.25.46	ICMP
▶	Oct 19 01:51:36	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 64.125.30.233	ICMP
▶	Oct 19 01:51:34	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 64.125.31.234	ICMP
▶	Oct 19 01:51:33	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 64.125.24.5	ICMP
▶	Oct 19 01:51:32	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 75.149.228.134	ICMP
▶	Oct 19 01:51:30	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 68.86.87.18	ICMP
▶	Oct 19 01:51:29	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 68.86.91.229	ICMP
▶	Oct 19 01:51:27	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 68.85.155.14	ICMP
▶	Oct 19 01:51:26	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 68.85.154.10	ICMP
▶	Oct 19 01:51:24	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 162.151.1.141	ICMP
▶	Oct 19 01:51:23	LAN	❶ ❷ ❸ 192.168.1.10	❶ ❷ ❸ 67.160.236.1	ICMP

The screenshot shows the pfSense Firewall Rules list. A specific rule has been selected, and its details are displayed in a modal window.

Selected 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" identifier 1757202313

Logs:

Time	Source	Destination	Protocol
Sep 7 10:17:10	❶ ❷ ❸ 192.168.1.45	❶ ❷ ❸ 239.255.255.250	IGMP
Sep 7 10:17:05	❶ ❷ ❸ 192.168.1.45	❶ ❷ ❸ 239.255.255.250	IGMP
Sep 7 10:17:05	❶ ❷ ❸ 192.168.1.70	❶ ❷ ❸ 239.255.255.250	IGMP
Sep 7 10:16:03	❶ ❷ ❸ 192.168.1.155	❶ ❷ ❸ 239.255.255.250	IGMP
Sep 7 10:16:02	❶ ❷ ❸ 192.168.1.45	❶ ❷ ❸ 239.255.255.250	IGMP
Sep 7 10:15:07	❶ ❷ ❸ 192.168.1.45	❶ ❷ ❸ 239.255.255.250	IGMP
Sep 7 10:15:06	❶ ❷ ❸ 192.168.1.155	❶ ❷ ❸ 239.255.255.250	IGMP
Sep 7 10:15:01	❶ ❷ ❸ 192.168.1.45	❶ ❷ ❸ 239.255.255.250	IGMP

Schedule Information

Schedule Name	BusinessHours																																										
Description	Normal Business Hours																																										
Month	August_16																																										
Date	August_2016 <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Mon</th> <th>Tue</th> <th>Wed</th> <th>Thu</th> <th>Fri</th> <th>Sat</th> <th>Sun</th> </tr> </thead> <tbody> <tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr> <tr><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td></tr> <tr><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td></tr> <tr><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td></tr> <tr><td>29</td><td>30</td><td>31</td><td></td><td></td><td></td><td></td></tr> </tbody> </table>	Mon	Tue	Wed	Thu	Fri	Sat	Sun	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
Mon	Tue	Wed	Thu	Fri	Sat	Sun																																					
1	2	3	4	5	6	7																																					
8	9	10	11	12	13	14																																					
15	16	17	18	19	20	21																																					
22	23	24	25	26	27	28																																					
29	30	31																																									

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

Time	9	00	17	00
------	---	----	----	----

Time range description Work Week

Add Time **Clear selection**

Log	Action	Reason	IP Address 1	IP Address 2	Protocol
Sep 7 10:17:10 LAN	Passed via EasyRule (1757202313)	Tracker ID: 1757202313	192.168.1.45	239.255.255.250	IGMP
Sep 7 10:17:05 LAN	Passed via EasyRule (1757202313)	Matched Rule: unavailable	192.168.1.45	239.255.255.250	IGMP
Sep 7 10:17:05 LAN	Passed via EasyRule (1757202313)	Associated Rules:	192.168.1.70	239.255.255.250	IGMP
Sep 7 10:16:03 LAN	Passed via EasyRule (1757202313)	@#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" identifier 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

LAB 3 – NAT & Port Forwarding

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
										 Add  Add  Delete  Toggle  Save

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)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input checked="" type="checkbox"/>	0 /0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN OpenVPN Server wizard	
<input checked="" 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

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
										Add Add Delete Toggle Save

Automatic Rules

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description		
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8 ::1/128	10.1.1.0/24	172.16.10.0/24	*	*	500	WAN address	*	<input checked="" type="checkbox"/> Auto created rule for ISAKMP
<input checked="" type="checkbox"/>	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

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