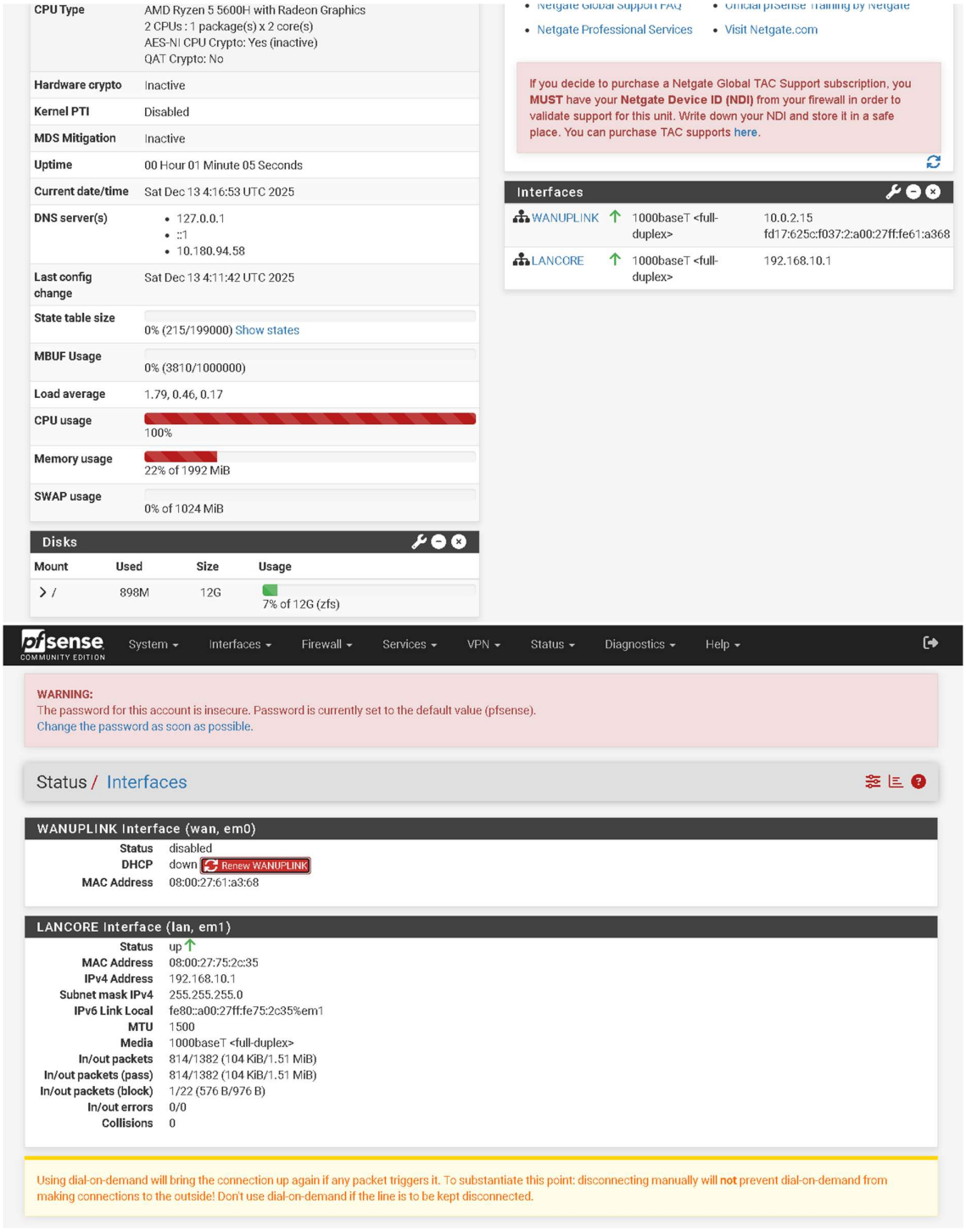
LAB – 1



CPU Type	AMD Ryzen 5 5600H with Radeon Graphics 2 CPUs : 1 package(s) x 2 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 01 Minute 05 Seconds
Current date/time	Sat Dec 13 4:16:53 UTC 2025
DNS server(s)	• 127.0.0.1 • ::1 • 10.180.94.58
Last config change	Sat Dec 13 4:11:42 UTC 2025
State table size	0% (215/199000) Show states
MBUF Usage	0% (3810/1000000)
Load average	1.79, 0.46, 0.17
CPU usage	100%
Memory usage	22% of 1992 MiB
SWAP usage	0% of 1024 MiB

Disks

Mount	Used	Size	Usage
/	898M	12G	7% of 12G (zfs)

• Netgate Professional Services • Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC supports here.

Interfaces

WANUPLINK	↑	1000baseT <full-duplex>	10.0.2.15 fd17:625c:f037:2:a00:27ff:fe61:a368
LANCORE	↑	1000baseT <full-duplex>	192.168.10.1

pfsense COMMUNITY EDITION — System — Interfaces — Firewall — Services — VPN — Status — Diagnostics — Help

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Status / Interfaces

WANUPLINK Interface (wan, em0)

Status	disabled
DHCP	down Renew WANUPLINK
MAC Address	08:00:27:61:a3:68

LANCORE Interface (lan, em1)

Status	up ↑
MAC Address	08:00:27:75:2c:35
IPv4 Address	192.168.10.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe75:2c35%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	814/1382 (104 KiB/1.51 MiB)
In/out packets (pass)	814/1382 (104 KiB/1.51 MiB)
In/out packets (block)	1/22 (576 B/976 B)
In/out errors	0/0
Collisions	0

Using dial-on-demand will bring the connection up again if any packet triggers it. To substantiate this point: disconnecting manually will **not** prevent dial-on-demand from making connections to the outside! Don't use dial-on-demand if the line is to be kept disconnected.

Status / Interfaces

WANUPLINK Interface (wan, em0)

Status	up
DHCP	up Release WANUPLINK Relinquish Lease
MAC Address	08:00:27:61:a3:68
IPv4 Address	10.0.2.15
Subnet mask IPv4	255.255.255.0
Gateway IPv4	10.0.2.2
IPv6 Link Local	fe80::a00:27ff:fe61:a368%em0
DNS servers	10.180.94.58
MTU	1200
Media	1000baseT <full-duplex>
In/out packets	9369/9614 (614 KiB/410 KiB)
In/out packets (pass)	9369/9614 (614 KiB/410 KiB)
In/out packets (block)	0/1 (0 B/40 B)
In/out errors	0/0
Collisions	0

LANCORE Interface (lan, em1)

Status	up
MAC Address	08:00:27:75:2c:35
IPv4 Address	192.168.10.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe75:2c35%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	732/1262 (87 KiB/1.40 MiB)
In/out packets (pass)	732/1262 (87 KiB/1.40 MiB)
In/out packets (block)	1/22 (576 B/976 B)
In/out errors	0/0
Collisions	0

Using dial-on-demand will bring the connection up again if any packet triggers it. To substantiate this point: disconnecting manually will **not** prevent dial-on-demand from making connections to the outside! Don't use dial-on-demand if the line is to be kept disconnected.

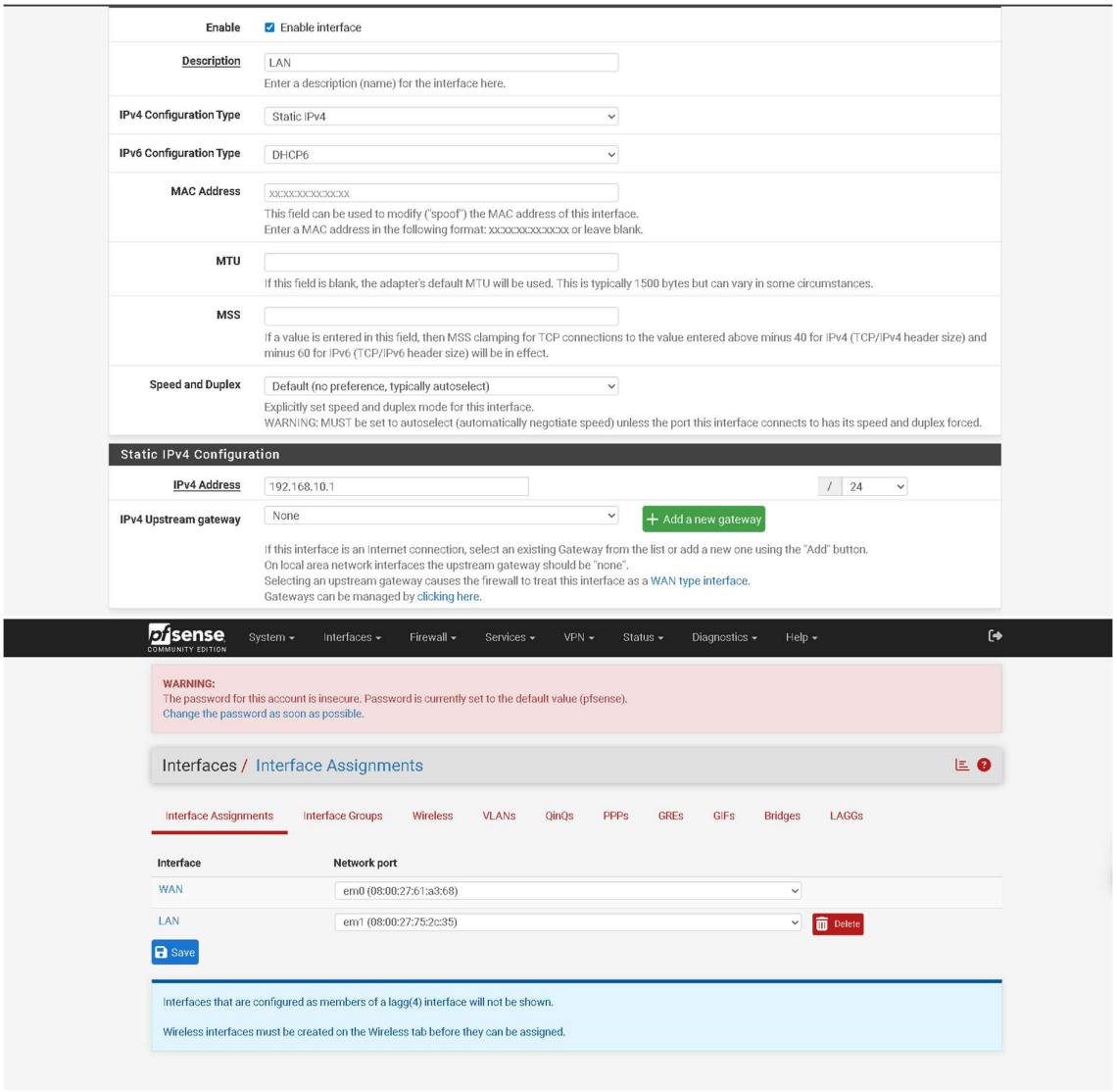
Status / Interfaces

WANUPLINK Interface (wan, em0)

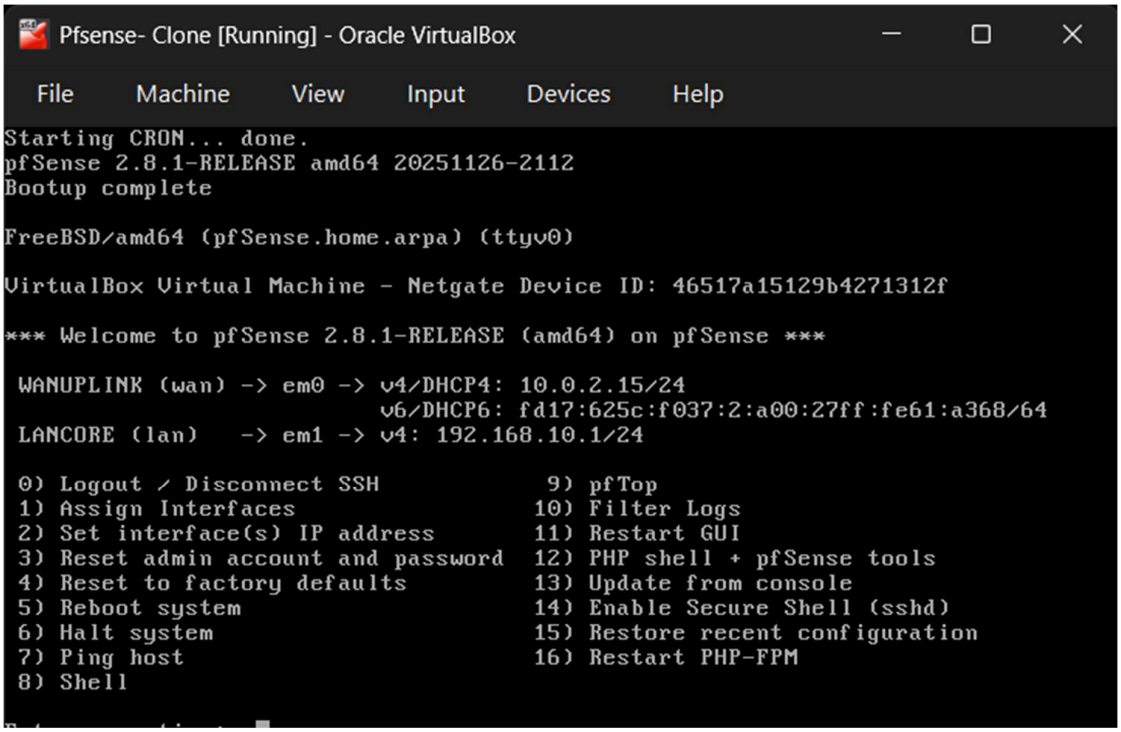
Status	up
DHCP	up Release WANUPLINK Relinquish Lease
MAC Address	08:00:27:61:a3:68
IPv4 Address	10.0.2.15
Subnet mask IPv4	255.255.255.0
Gateway IPv4	10.0.2.2
IPv6 Link Local	fe80::a00:27ff:fe61:a368%em0
IPv6 Address	fd17:625c:f037:2:a00:27ff:fe61:a368
Subnet mask IPv6	64
Gateway IPv6	fe80::2%em0
DNS servers	10.180.94.58
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	9078/9303 (581 KiB/397 KiB)
In/out packets (pass)	9078/9303 (581 KiB/397 KiB)
In/out packets (block)	0/1 (0 B/40 B)
In/out errors	0/0
Collisions	0

LANCORE Interface (lan, em1)

Status	up
MAC Address	08:00:27:75:2c:35
IPv4 Address	192.168.10.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe75:2c35%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	686/1181 (80 KiB/1.32 MiB)
In/out packets (pass)	686/1181 (80 KiB/1.32 MiB)
In/out packets (block)	1/22 (576 B/976 B)
In/out errors	0/0
Collisions	0


Enable
Enable interface
Description
LAN
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: xxxxxxxxxxxx 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
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.

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.
Interfaces / Interface Assignments
Interface Assignments
Interface Groups
Wireless
VLANs
QinQs
PPPs
GREs
GIFs
Bridges
LAGGs
Interface
Network port
WAN
em0 (08:00:27:61:a3:68)
LAN
em1 (08:00:27:75:2c:35)
Delete
Save
Interfaces that are configured as members of a lagg(4) interface will not be shown.
Wireless interfaces must be created on the Wireless tab before they can be assigned.



Before disabling the interface, ICMP ping requests received a valid reply, indicating the interface was active and processing traffic. After unchecking 'Enable Interface', the interface state changed to 'down'. Subsequent ping attempts resulted in a 'Request Timed Out' because the operating system stopped listening on that port and logically disconnected it from the network stack.

LAB – 2

Action	Time	Interface	Rule	Source	Destination	Protocol
✕	Dec 13 04:02:08	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:64562	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:08	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:64562	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:09	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:64562	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:10	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:64562	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:12	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:64562	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:16	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:16	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:16	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:16	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:16	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:16	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:16	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:17	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:64562	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:17	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:18	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:20	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:25	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:26	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:64562	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:32	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:43	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:64562	192.168.10.106:80	TCP:A
✕	Dec 13 04:02:46	LANCORE	Default deny rule IPv4 (1000000104)	192.168.10.103:51581	192.168.10.106:80	TCP:A
✕	Dec 13 04:07:00	WANUPLINK	Default deny rule IPv4 (1000000104)	10.0.2.15:48451	192.168.10.103:51581	TCP:RA
✕	Dec 13 04:11:51	WANUPLINK	Default deny rule IPv4 (1000000103)	10.0.2.2:67	255.255.255.255:68	UDP

pfsense COMMUNITY EDITION   System   Interfaces   Firewall   Services   VPN   Status   Diagnostics   Help

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

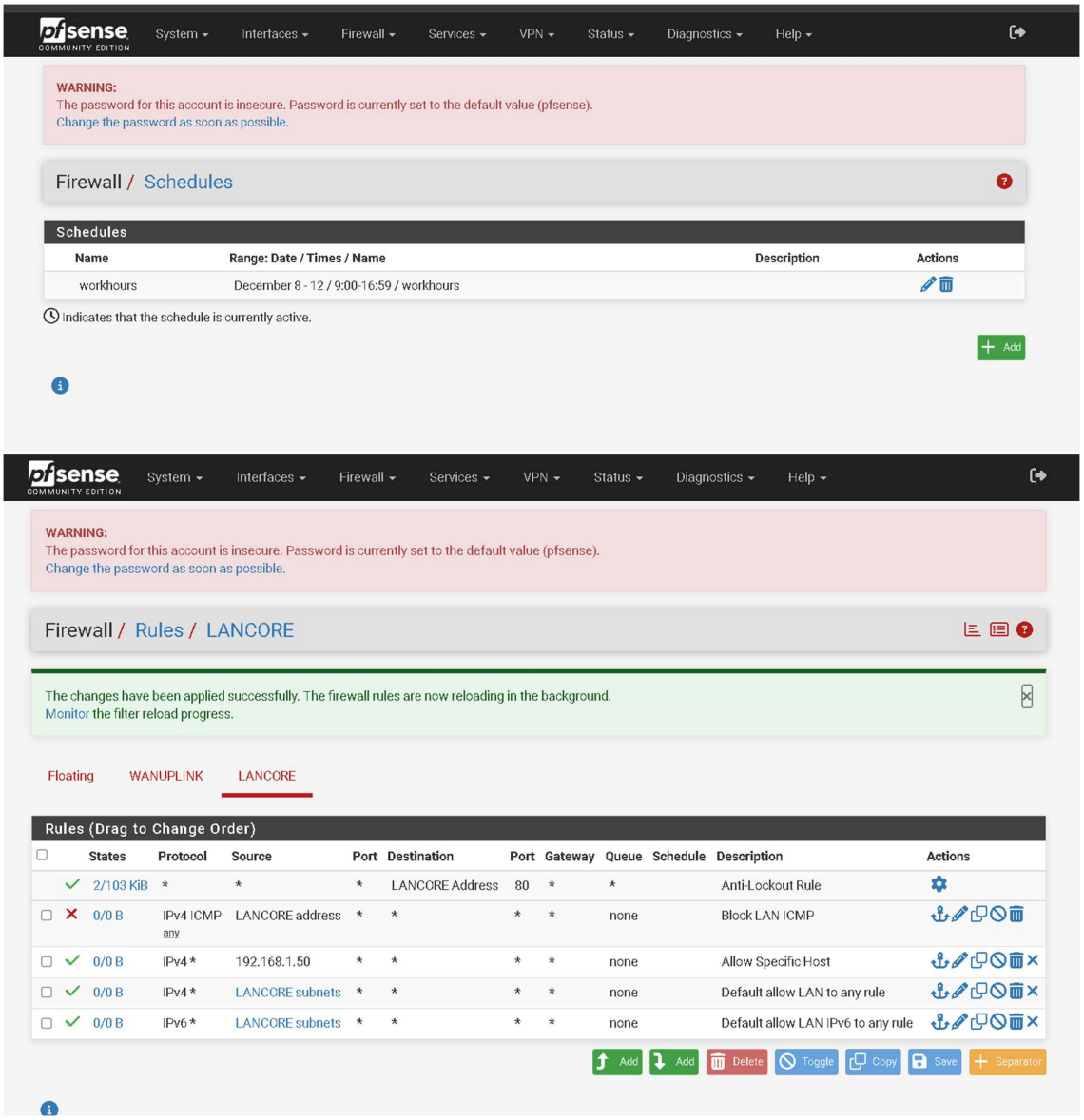
Firewall / Rules / LANCORE

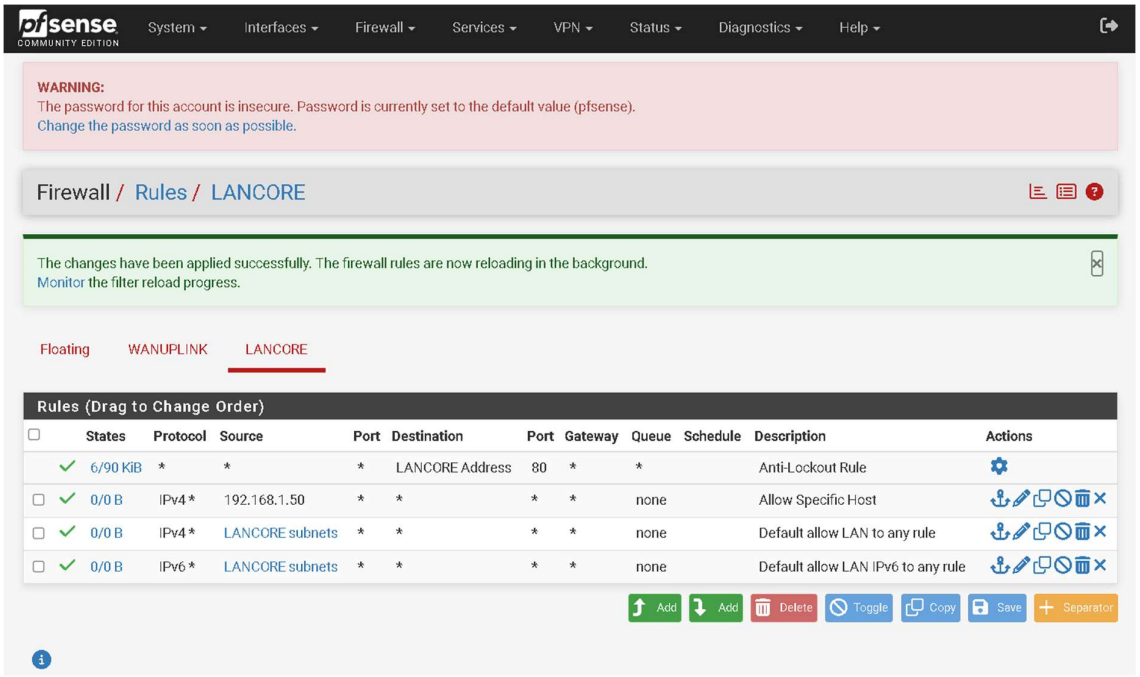
Floating   WANUPLINK   LANCORE

Rules (Drag to Change Order)

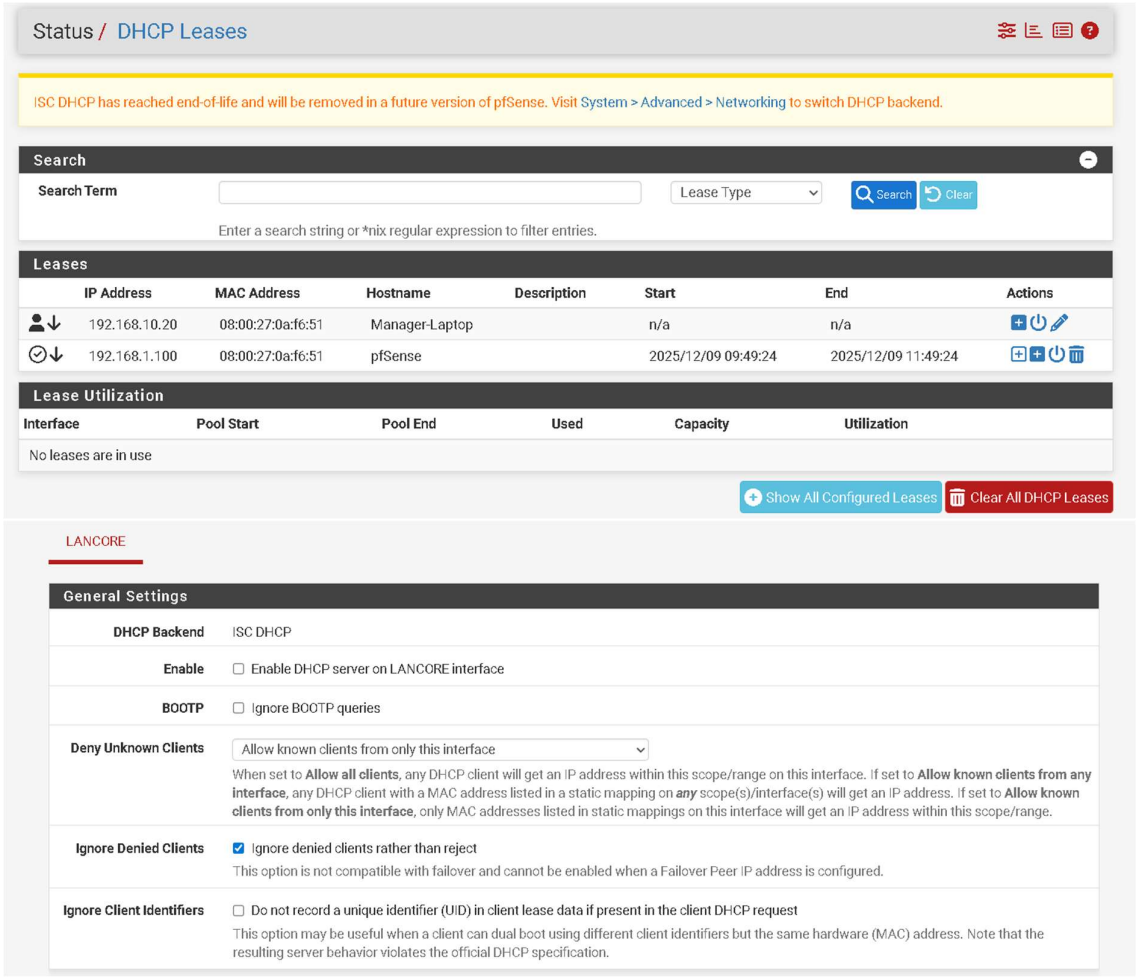
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓	1/105 KiB	*	*	*	LANCORE Address	80	*	*		Anti-Lockout Rule
✕	0/0 B	IPv4 ICMP any	LANCORE address	*	*	*	*	none		Block LAN ICMP
✓	0/0 B	IPv4 *	192.168.1.50	*	*	*	*	none	workhours	Allow Specific Host
✓	0/0 B	IPv4 *	LANCORE subnets	*	*	*	*	none		Default allow LAN to any rule
✓	0/0 B	IPv6 *	LANCORE subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule

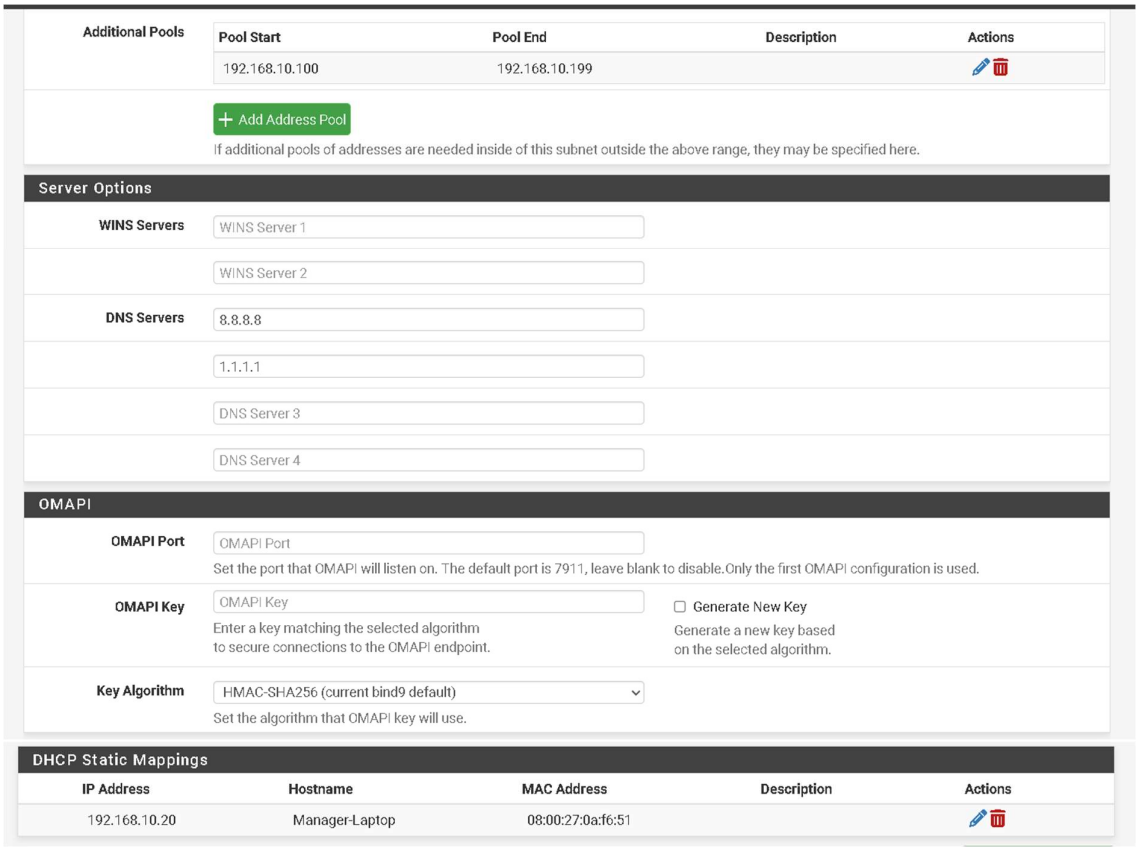
Add   Add   Delete   Toggle   Copy   Save   Separator


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.
Firewall / Schedules
Schedules
Name
Range: Date / Times / Name
Description
Actions
workhours
December 8 - 12 / 9:00-16:59 / workhours
Indicates that the schedule is currently active.
Add
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.
Firewall / Rules / LANCORE
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WANUPLINK
LANCORE
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
2/103 KiB
*
*
*
LANCORE Address
80
*
*
Anti-Lockout Rule
0/0 B
IPv4 ICMP any
LANCORE address
*
*
*
*
none
Block LAN ICMP
0/0 B
IPv4 *
192.168.1.50
*
*
*
*
none
Allow Specific Host
0/0 B
IPv4 *
LANCORE subnets
*
*
*
*
none
Default allow LAN to any rule
0/0 B
IPv6 *
LANCORE subnets
*
*
*
*
none
Default allow LAN IPv6 to any rule
Add
Add
Delete
Toggle
Copy
Save
Separator


pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.
Firewall / Rules / LANCORE
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating
WANUPLINK
LANCORE
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
6/90 KiB * * * LANCORE Address 80 * * Anti-Lockout Rule
0/0 B IPv4 * 192.168.1.50 * * * * none Allow Specific Host
0/0 B IPv4 * LANCORE subnets * * * * none Default allow LAN to any rule
0/0 B IPv6 * LANCORE subnets * * * * none Default allow LAN IPv6 to any rule
Add
Add
Delete
Toggle
Copy
Save
Separator

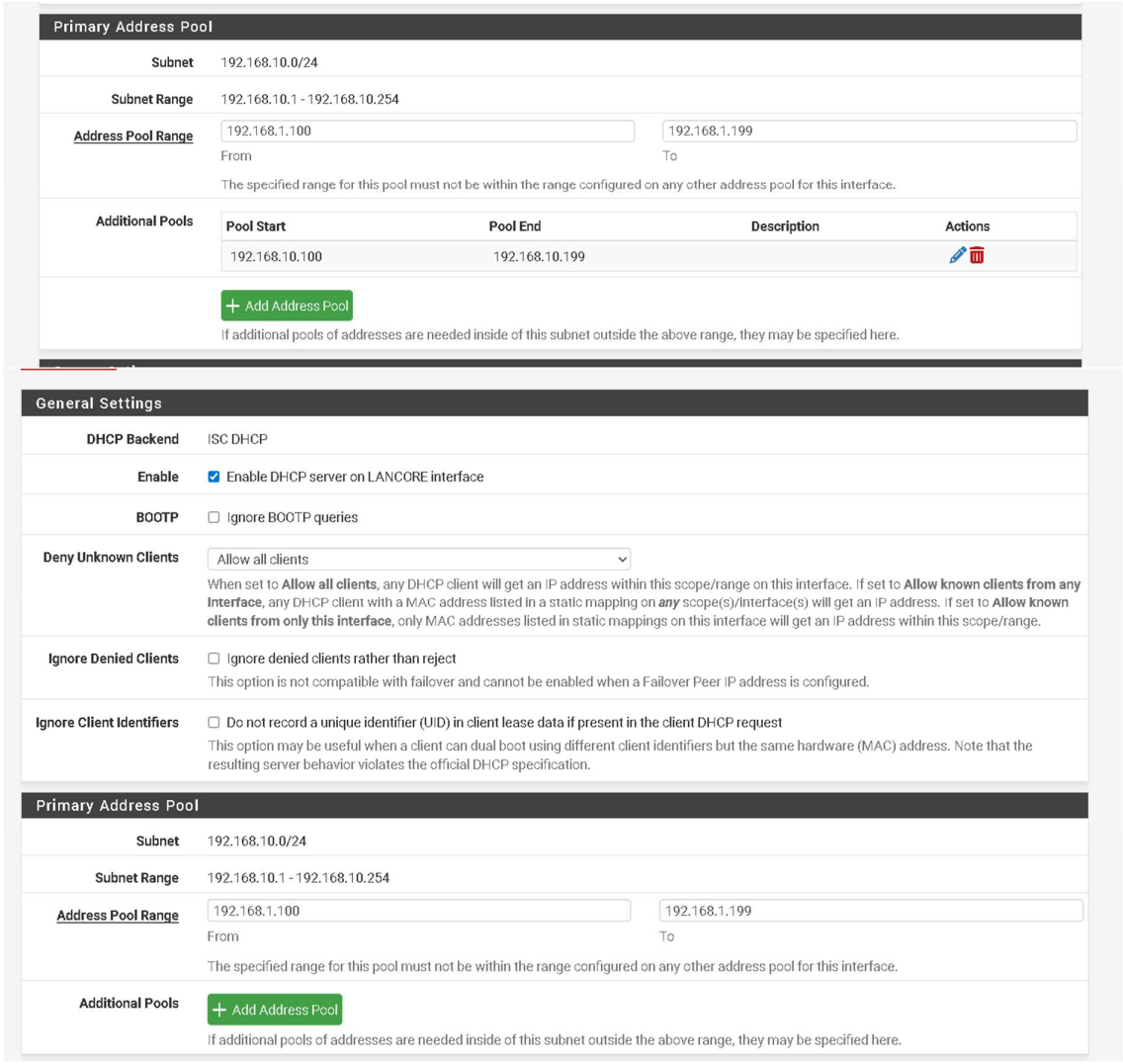
LAB – 4


Status / DHCP Leases
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
Search
Search Term
Lease Type
Search
Clear
Enter a search string or *nix regular expression to filter entries.
Leases
IP Address
MAC Address
Hostname
Description
Start
End
Actions
192.168.10.20
08:00:27:0a:f6:51
Manager-Laptop
n/a
n/a
192.168.1.100
08:00:27:0a:f6:51
pfSense
2025/12/09 09:49:24
2025/12/09 11:49:24
Lease Utilization
Interface
Pool Start
Pool End
Used
Capacity
Utilization
No leases are in use
Show All Configured Leases
Clear All DHCP Leases
LANCORE
General Settings
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on LANCORE interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow known clients from only this interface
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

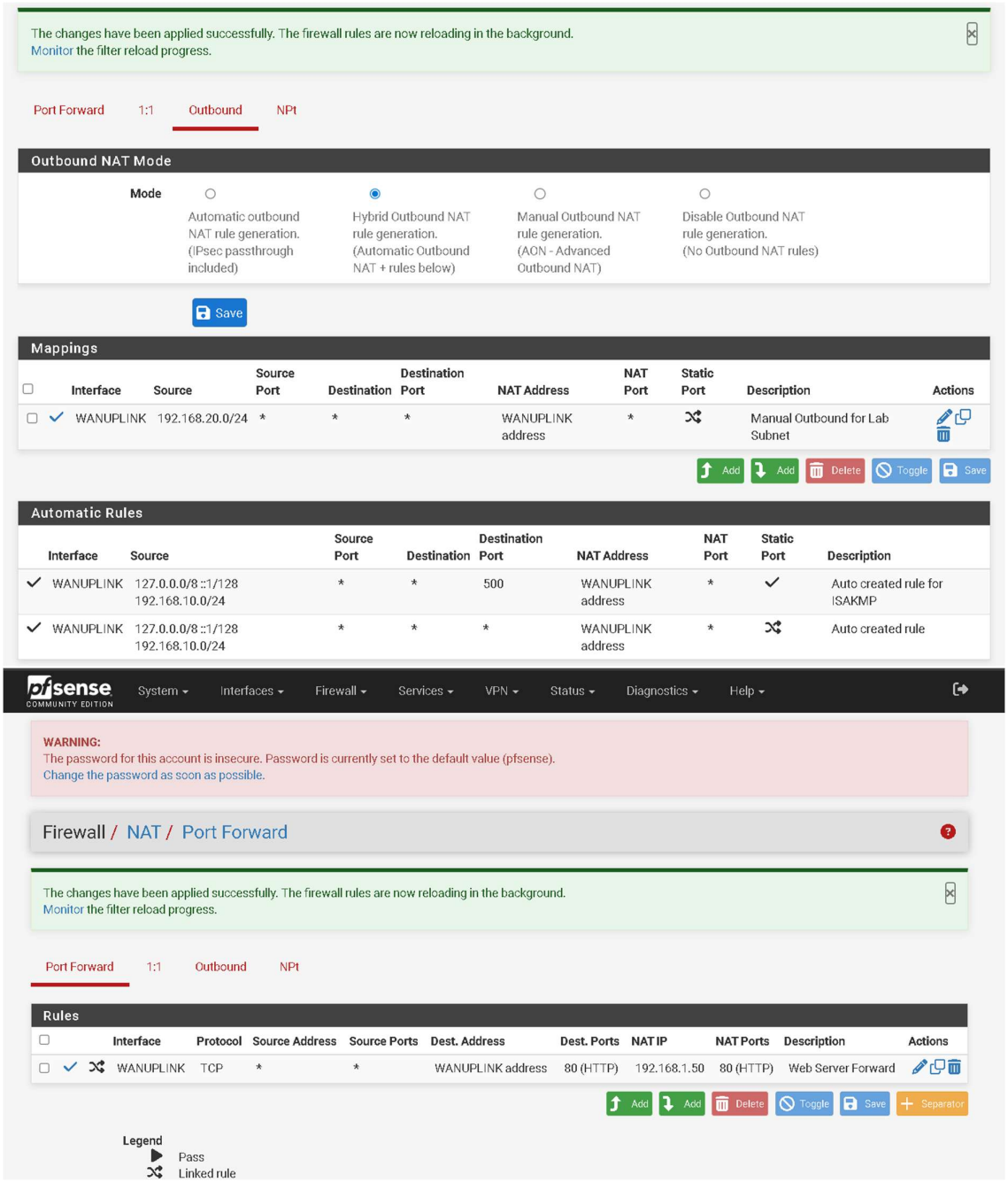


DHCP Static Mappings

IP Address	Hostname	MAC Address	Description	Actions
192.168.10.20	Manager-Laptop	08:00:27:0a:f6:51		


Primary Address Pool
Subnet
192.168.10.0/24
Subnet Range
192.168.10.1 - 192.168.10.254
Address Pool Range
192.168.1.100
From
192.168.1.199
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Pool Start
Pool End
Description
Actions
192.168.10.100
192.168.10.199
Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.
General Settings
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on LANCORE interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients
Ignore denied clients rather than reject
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.10.0/24
Subnet Range
192.168.10.1 - 192.168.10.254
Address Pool Range
192.168.1.100
From
192.168.1.199
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

LAB – 3



The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

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
WANUPLINK	192.168.20.0/24	*	*	*	WANUPLINK address	*		Manual Outbound for Lab Subnet	

Add | Add | Delete | Toggle | Save

Automatic Rules

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WANUPLINK	127.0.0.0/8 ::1/128 192.168.10.0/24	*	*	500	WANUPLINK address	*	✓	Auto created rule for ISAKMP
WANUPLINK	127.0.0.0/8 ::1/128 192.168.10.0/24	*	*	*	WANUPLINK address	*		Auto created rule

pfSense COMMUNITY EDITION — System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Help

WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.

Firewall / NAT / Port Forward

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

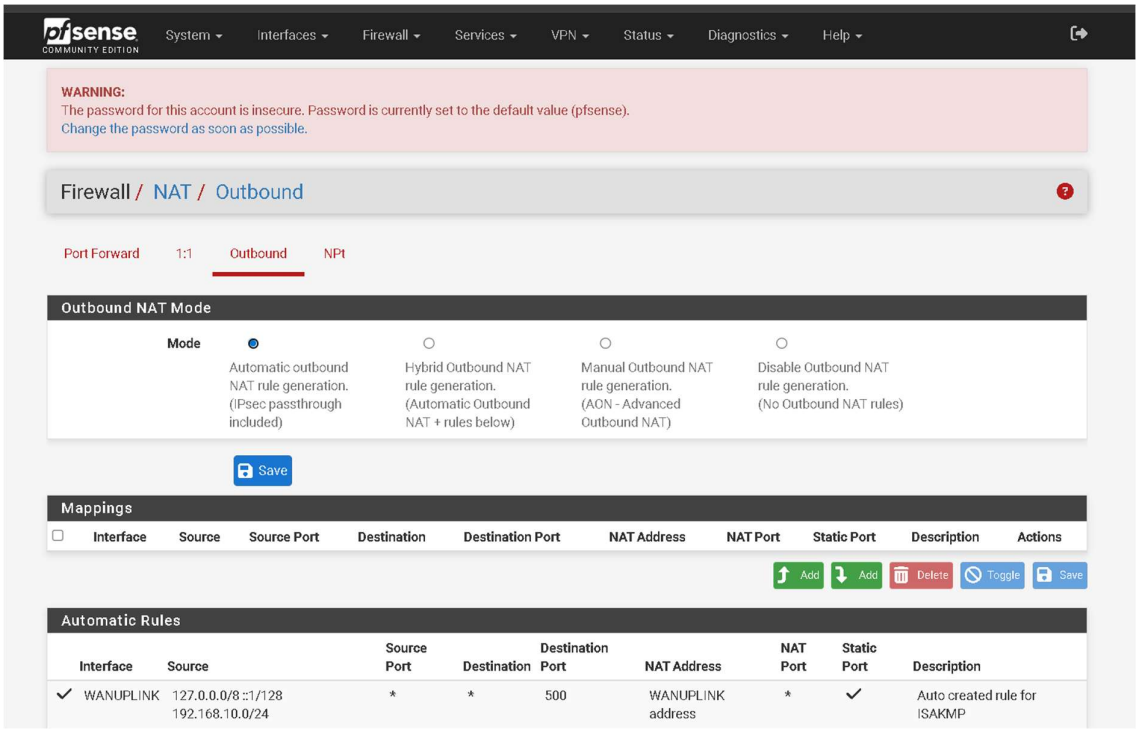
Port Forward | 1:1 | Outbound | NPt

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
WANUPLINK	TCP	*	*	WANUPLINK address	80 (HTTP)	192.168.1.50	80 (HTTP)	Web Server Forward	

Add | Add | Delete | Toggle | Save | Separator

Legend
Pass
Linked rule


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING:
The password for this account is insecure. Password is currently set to the default value (pfsense).
Change the password as soon as possible.
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
WANUPLINK
127.0.0.0/8 ::1/128 192.168.10.0/24
*
*
500
WANUPLINK address
*
Auto created rule for ISAKMP