

## گزارش درباره‌ی نصب و راه‌اندازی OPNsense

تهیه و تنظیم: مبین خیبری

شماره دانشجویی: 994421017

استاد راهنما: دکتر تاجبخش

### چکیده:

در گزارش کار پیش‌رو قصد داریم اقدامات لازم برای نصب و راه‌اندازی اولیه‌ی سرویس OPNsense بر روی یک کامپیوتر شخصی را قدم به قدم دنبال کنیم.

سرویس OPNsense در واقع چرخه‌ی حیات خود را در سال 2015 با انشعاب از Pfsense آغاز کرد. اما در ادامه و با گذر زمان، امروزه به یکی از قابل‌اعتمادترین روش‌های طراحی و پیاده‌سازی فایروال‌ها تبدیل شده‌است.

همانطور که می‌دانید، سرویس OPNsense نیز همچون سرویس Pfsense از ابتدا بر اساس نیازمندی‌ها و ویژگی‌های سیستم عامل Free BSD طراحی و تولید شد. به این دلیل و همچنین به علت وجود اهداف آموزشی در نصب و راه‌اندازی این سیستم، ما نیز مراحل نصب و کانفیگ را در یک محیط مجازی دنبال خواهیم کرد.

حداقل نیازمندی‌های سیستمی و نیز سخت‌افزار پیشنهادی برای نصب و راه‌اندازی این سیستم در زیر آورده شده‌اند. در طول گزارش پیش‌فرض ما این است که دسترسی لازم به منابع کافی در این زمینه وجود دارد.

## Suggested Hardware

- 1GHz CPU
- 1 GB of RAM
- 4GB of storage
- 2 or more PCI-e network interface cards.

### Hardware Minimums

- 500 Mhz CPU
- 1 GB of RAM
- 4GB of storage
- 2 network interface cards

اولین قدم برای نصب و راه اندازی این سرویس آن است که فایل نصبی مربوط به برنامه‌ی آن را از لینک زیر دانلود کنیم:

[/https://opnsense.org/download](https://opnsense.org/download)

برای دانلود این فایل ابتدا لینک مربوط به آن را از صفحه‌ی مذکور یافته و سپس دستور زیر را در کامندلاین اجرا می‌کنیم:

```
wget -c http://mirrors.nycbug.org/pub/opnsense/releases/mirror/OPNsense-18.7-OpenSSL-dvd-amd64.iso.bz2 $
```

بعد از اتمام دانلود فایل، نیاز داریم که آن را به کمک ابزار `bunzip` از حالت فشرده شده خارج کنیم. دستور زیر در این مورد ما را یاری خواهد کرد:

```
bunzip2 OPNsense-18.7-OpenSSL-dvd-amd64.iso.bz2 $
```

در ادامه لازم است که با استفاده از یک USB فضایی برای بوت شدن برنامه بسازیم. ابزار `dd tool` در این زمینه ما را یاری خواهد کرد.

در مرحله‌ی بعدی لازم است که به کمک ابزار `lsblk` در ترمینال، فضایی از دیسک را به این سرویس اختصاص دهیم:

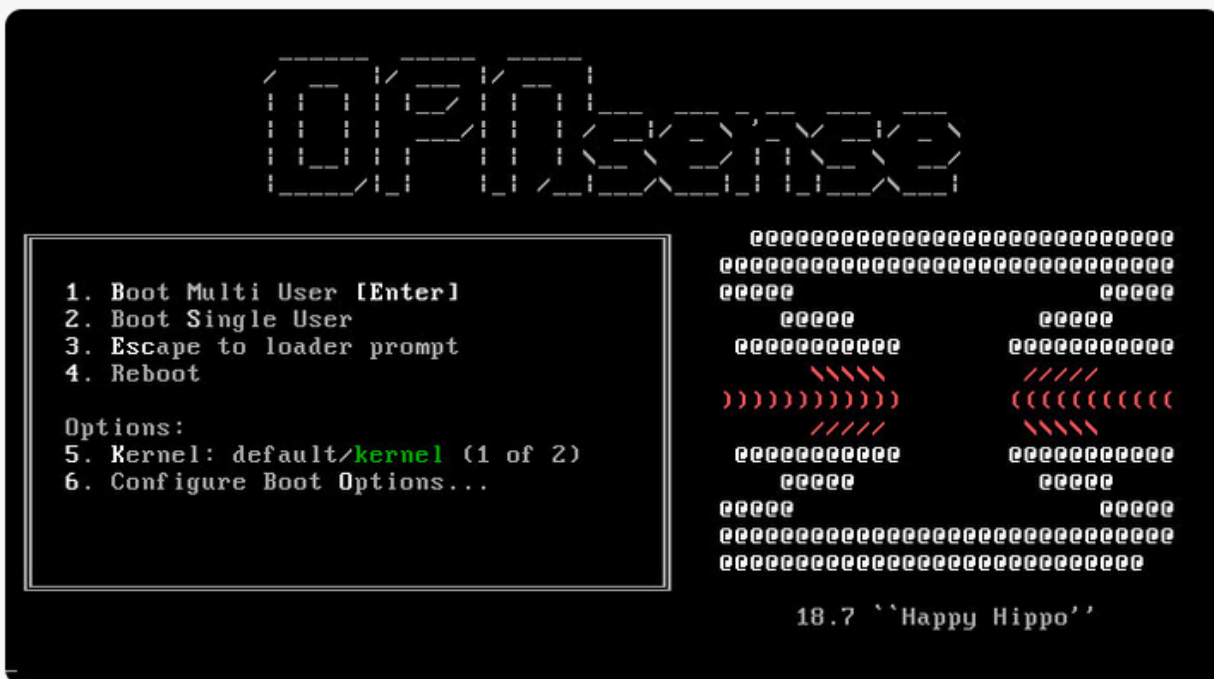
```
h @' | ~ $ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda          8:0    0 465.8G  0 disk
├─sda1       8:1    0   25G  0 part
├─sda2       8:2    0  81.9G  0 part
├─sda3       8:3    0    1K  0 part
├─sda5       8:5    0 351.3G  0 part
├─sda6       8:6    0   7.6G  0 part
sdb          8:16   0 931.5G  0 disk
├─sdb1       8:17   0 931.5G  0 part
sdc          8:32   1   7.4G  0 disk
├─sdc1       8:33   1   1.6G  0 part
└─sdc2       8:34   1    2.3M  0 part
sr0         11:0    1 1024M  0 rom
```

حال با اجرای دستورات زیر، فایل ISO را بر روی حافظه‌ی فلش مموری می‌نویسیم:

```
sudo dd if=~/.Downloads/OPNsense-18.7-OpenSSL-dvd-amd64.iso of=/dev/sdc $
```

توجه: دستور بالا به طور اتوماتیک تمام محتویات حافظه را پیش از انتقال فایل‌های جدید به آن پاک یا فرمت خواهد کرد.

در مرحله‌ی بعدی همزمان که حافظه‌ی فلش مموری به یکی از درگاه‌های کامپیوتر متصل است، آن را ری‌استارت کرده و برنامه‌ی نوشته‌شده روی USB را با بوت‌لودر اجرا می‌کنیم.



همانطور که در تصویر بالا پیداست، هنگام بوت کردن سیستم با این برنامه، می‌توانید به طور زنده و بدون نیاز به نصب از برخی امکانات آن استفاده کنید. اما در اینجا ما گزینه‌ی نصب را انتخاب کرده و به مرحله‌ی بعد می‌رویم.

هنگام نصب این ابزار برای بار نخست، باید یک رمز عبور جهت محرمانه نگه داشتن سطح دسترسی به برنامه تعبیه کرد:

```
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNsense_INSTALL

*** OPNsense.localdomain: OPNsense 18.7 (amd64/OpenSSL) ***

LAN (em0)      -> v4: 192.168.1.1/24

HTTPS: SHA256 05:18:65:7A:6C:E7:4E:61:F8:1B:8A:5E:AA:6B:24:BC:
          B0:BD:AC:8D:0A:0E:50:00:A7:C6:4C:6F:C0:41:29:D0
SSH:      SHA256 pfZaOWiSTsTrv9lsSEPrKoshqaw+DSfUaKEHaHzCucI (ECDSA)
SSH:      SHA256 VdGw3U/TwgeWsJZTQ0fC20vvrSDBZ8kc48WGoAGX8TU (ED25519)
SSH:      SHA256 1hjiSgXCEvp3yeZafJhN2bsoY13oavdyApB9wD6bI10 (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: installer
password:
```

تصویر بعدی یک هشدار است که پیش از ادامه‌ی مراحل نصب و جهت کسب اطمینان از آگاهی کاربر به او نشان داده می‌شود.



در مرحله‌ی بعدی نیاز داریم که Keymap مناسب را از میان لیست ارائه‌شده انتخاب کنیم. انتخاب پیشنهادشده توسط خود برنامه، معمولاً بهترین انتخاب ممکن است:

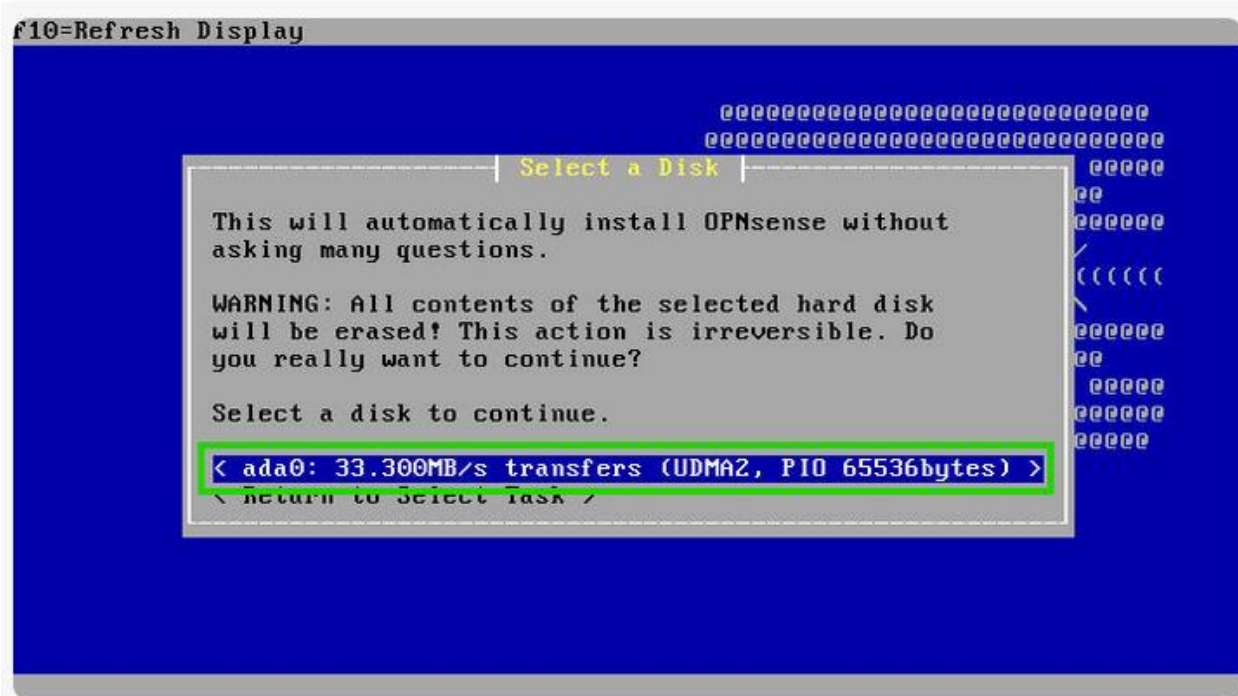


سپس از میان گزینه‌های موجود در مرحله‌ی بعد، گزینه‌ی Guided Installation را انتخاب می‌کنیم:

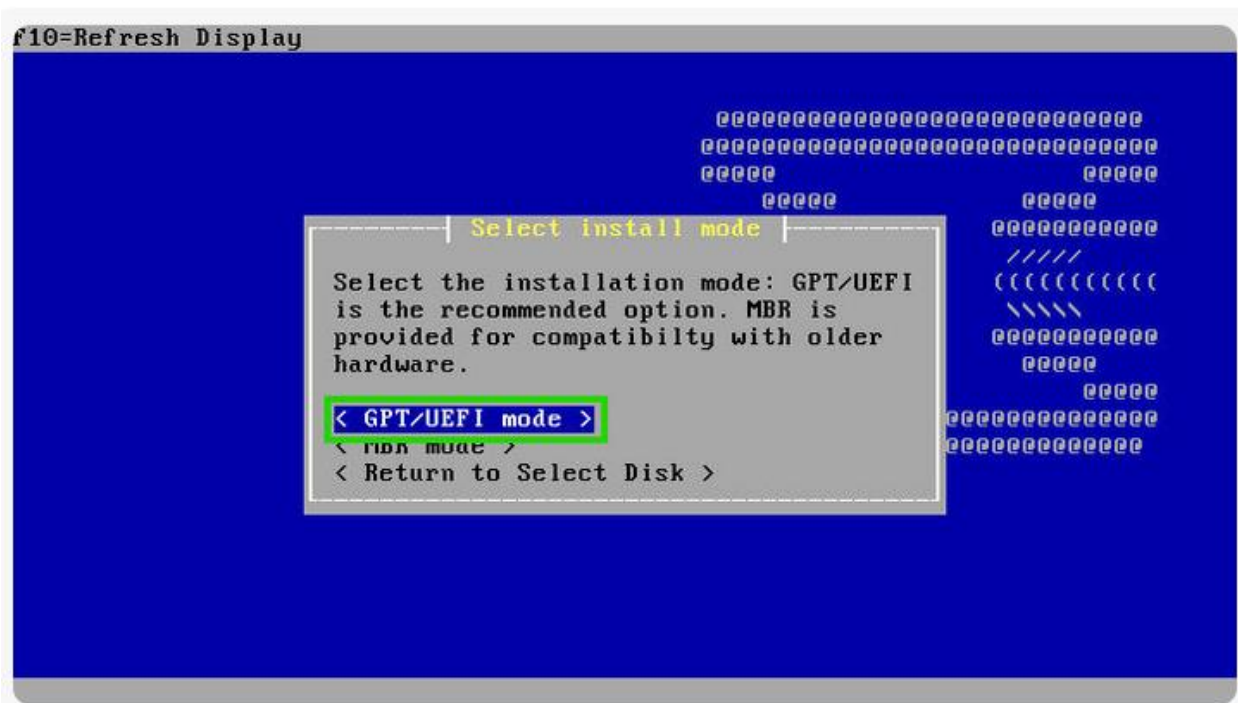




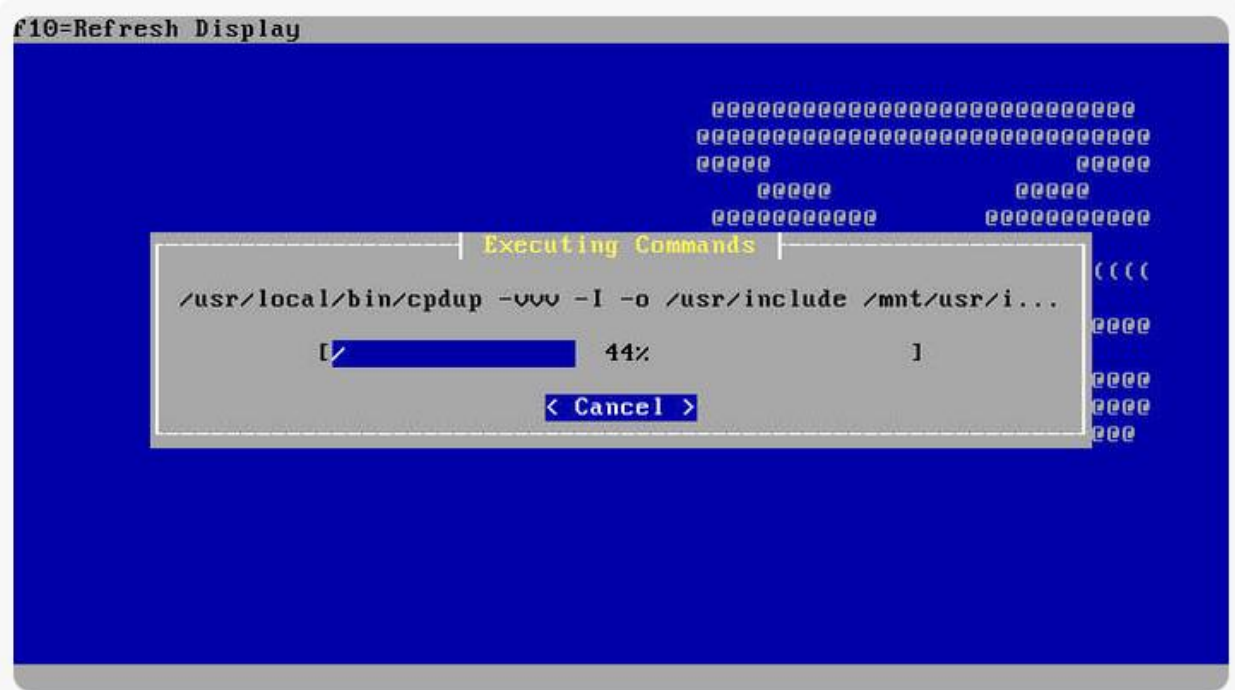
در مرحله‌ی بعد، محل نصب برنامه روی دیسک را مشخص می‌کنیم:



و بعد از آن، نوبت به انتخابِ مود نصب می‌رسد:



در آخر، لازم است کمی صبر کنیم تا فرآیند نصب برنامه به پایان برسد:



بعد از پایان مراحل نصب، یک رمزعبور مخصوص دسترسی به بخش‌های روت برنامه انتخاب کرده و آن را به سیستم اطلاع می‌دهیم:



حال بعد از ری استارت کردن سیستم، نام کاربری و رمز عبور را تایپ کرده و وارد محیط برنامه می شویم:

```
Starting DHCPv4 service...done.
Generating /etc/hosts...done.
Configuring firewall.....done.
Starting NTP service...deferred.
Generating RRD graphs...done.
Configuring system logging...done.
>>> Invoking start script 'newwanip'
>>> Invoking start script 'freebsd'
Configuring additional services: OK
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs

*** OPNsense.localdomain: OPNsense 18.7 (amd64/OpenSSL) ***

LAN (em0)      -> v4: 192.168.1.1/24

HTTPS: SHA256 05:18:65:7A:6C:E7:4E:61:F8:1B:8A:5E:AA:6B:24:BC:
              B0:BD:AC:8D:0A:0E:50:00:A7:C6:4C:6F:C0:41:29:D0

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █
```

تصاویر زیر آدرس های پیش فرض در نظر گرفته شده برای برنامه شبکه های موجود را نشان می دهند:

```
Hello, this is OPNsense 18.7
Website:      https://opnsense.org/
Handbook:     https://docs.opnsense.org/
Forums:       https://forum.opnsense.org/
Lists:        https://lists.opnsense.org/
Code:         https://github.com/opnsense

*** OPNsense.localdomain: OPNsense 18.7 (amd64/OpenSSL) ***

LAN (em0)      -> v4: 192.168.1.1/24

HTTPS: SHA256 05:18:65:7A:6C:E7:4E:61:F8:1B:8A:5E:AA:6B:24:BC:
              B0:BD:AC:8D:0A:0E:50:00:A7:C6:4C:6F:C0:41:29:D0

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option: █
```



```
HTTPS: SHA256 05:18:65:7A:6C:E7:4E:61:F8:1B:8A:5E:AA:6B:24:BC:
          B0:BD:AC:8D:0A:0E:50:00:A7:C6:4C:6F:C0:41:29:D0
```

- |                              |                         |
|------------------------------|-------------------------|
| 0) Logout                    | 7) Ping host            |
| 1) Assign interfaces         | 8) Shell                |
| 2) Set interface IP address  | 9) pfTop                |
| 3) Reset the root password   | 10) Firewall log        |
| 4) Reset to factory defaults | 11) Reload all services |
| 5) Power off system          | 12) Update from console |
| 6) Reboot system             | 13) Restore a backup    |

Enter an option: 1

Valid interfaces are:

```
em0      08:00:27:71:4b:0b Intel(R) PRO/1000 Legacy Network Connection 1
.1.0
em1      08:00:27:59:d1:0a Intel(R) PRO/1000 Legacy Network Connection 1
.1.0
```

You now have the opportunity to configure VLANs. If you don't require VLANs for initial connectivity, say no here and use the GUI to configure VLANs later.

Do you want to configure VLANs now? [y/N]:

You now have the opportunity to configure VLANs. If you don't require VLANs for initial connectivity, say no here and use the GUI to configure VLANs later.

Do you want to configure VLANs now? [y/N]: n

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection

NOTE: this enables full Firewalling/NAT mode.

(or nothing if finished): em1

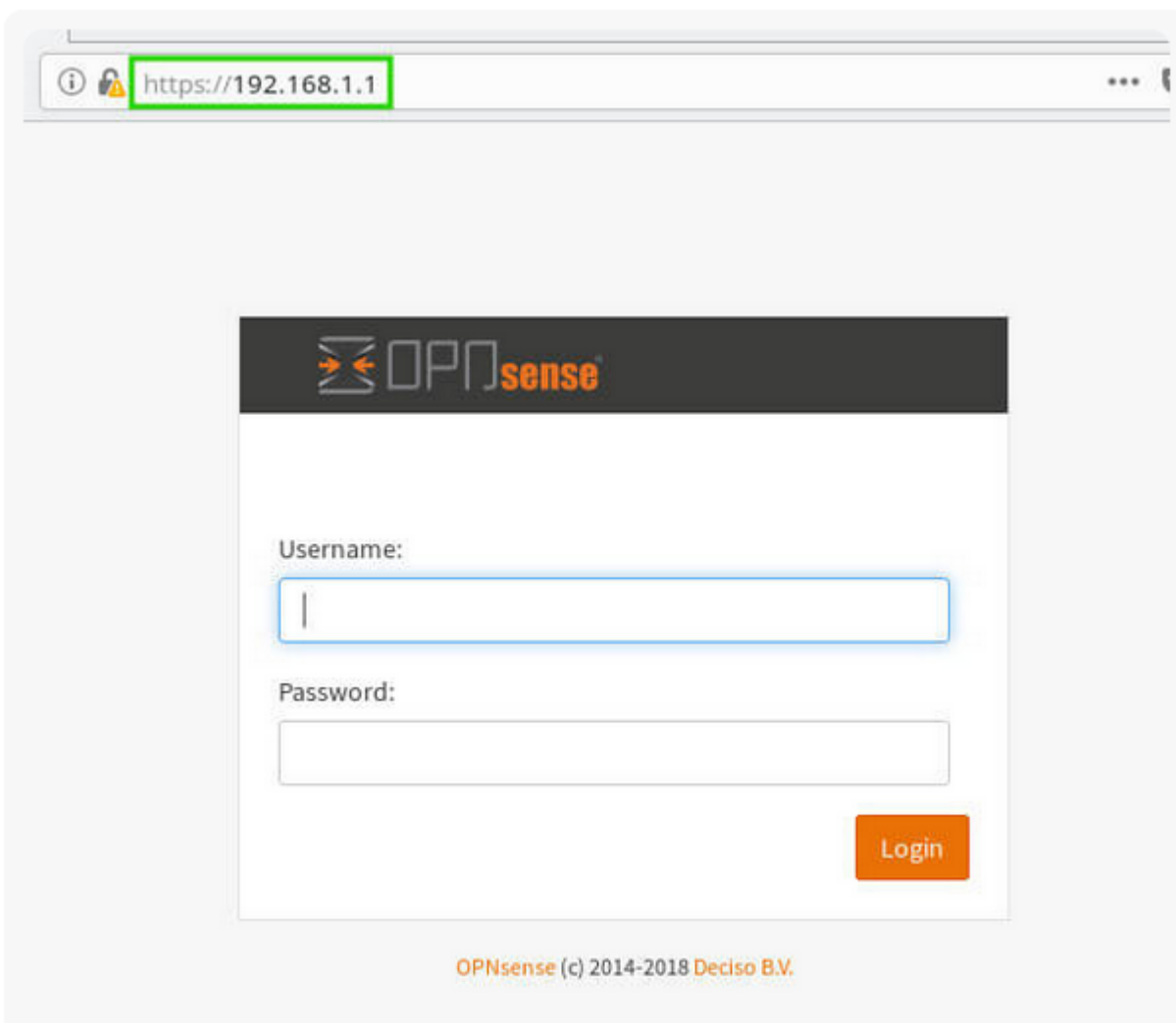
Enter the Optional 1 interface name or 'a' for auto-detection  
(or nothing if finished):

The interfaces will be assigned as follows:

```
WAN -> em0
LAN -> em1
```

Do you want to proceed? [y/N]:

حال برای اعمال تغییرات و مشاهده‌ی پارامترهای تعریف‌شده برای فایروال می‌توانیم به کمک یک مرورگر وارد آدرس زیر شده و از رابط کاربری گرافیکی آن بهره‌مند شویم:



The image shows a web browser window with the address bar displaying `https://192.168.1.1`. The page features the OPNsense logo at the top. Below the logo, there is a login form with two input fields: "Username:" and "Password:". To the right of the password field is an orange "Login" button. At the bottom of the page, the text "OPNsense (c) 2014-2018 Deciso B.V." is visible.

به کمک این سیستم می‌توانیم فایروال را روی انواع مختلف شبکه‌ها و بر اساس مفاهیم و پروتکل‌های متنوعی فعال کنیم.

تصاویر صفحات بعدی مراحل انجام این کار را برای DNS Overriding، NTP، LAN و WAN نشان می‌دهند:

OPNsense

root@OPNsense.localdomain

Lobby

Reporting

System

Access

Configuration

Firmware

Gateways

High Availability

Routes

Settings

Trust

Wizard

Log Files

Diagnostics

Interfaces

Firewall

## System: Wizard: General Information

General Information

Hostname:

OPNsense

Domain:

localdomain

Language:

English

Primary DNS Server:

Secondary DNS Server:

Override DNS:

☐ Allow DNS servers to be overridden by DHCP/PPP on WAN

Unbound DNS

OPNsense

root@OPNsense.localdomain

Lobby

Reporting

System

Access

Configuration

Firmware

Gateways

High Availability

Routes

## System: Wizard: Time Server Information

Time server hostname:

0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2....

Enter the hostname (FQDN) of the time server.

Timezone:

Etc/UTC

Next

OPNsense

root@OPNsense.localdomain

Lobby

Reporting

System

Access

Configuration

Firmware

Gateways

System: Wizard: Configure WAN Interface

SelectedType: DHCP

General configuration

MAC Address:

OPNsense

root@OPNsense.localdomain

Lobby

Reporting

System

Access

Configuration

Firmware

Gateways

High Availability

Routes

System: Wizard: Configure LAN Interface

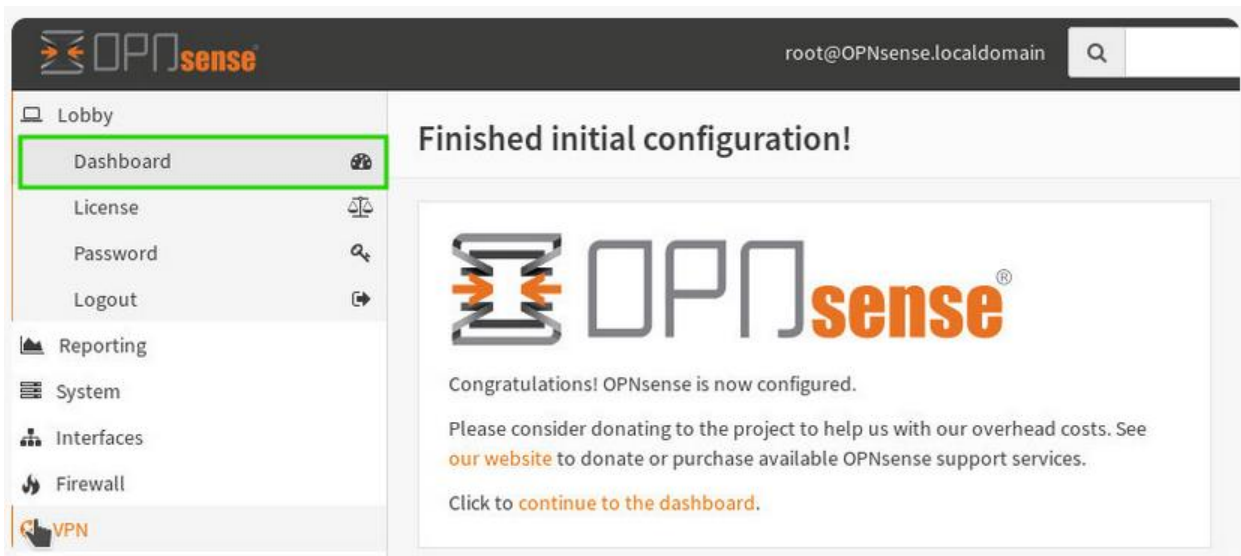
LAN IP Address: 192.168.1.1

(leave empty for none)

Subnet Mask: 24

Next

در نهایت پس از انجام فرآیند Config مطابق میلان، می‌توانیم از اطلاعات موجود در داشبورد استفاده کرده و شیوه‌های فایروال بر اعضای مختلف شبکه را رصد کنیم:



OPNsense

root@OPNsense.localdomain

Lobby

Dashboard

License

Password

Logout

Reporting


System

Interfaces

Firewall

VPN

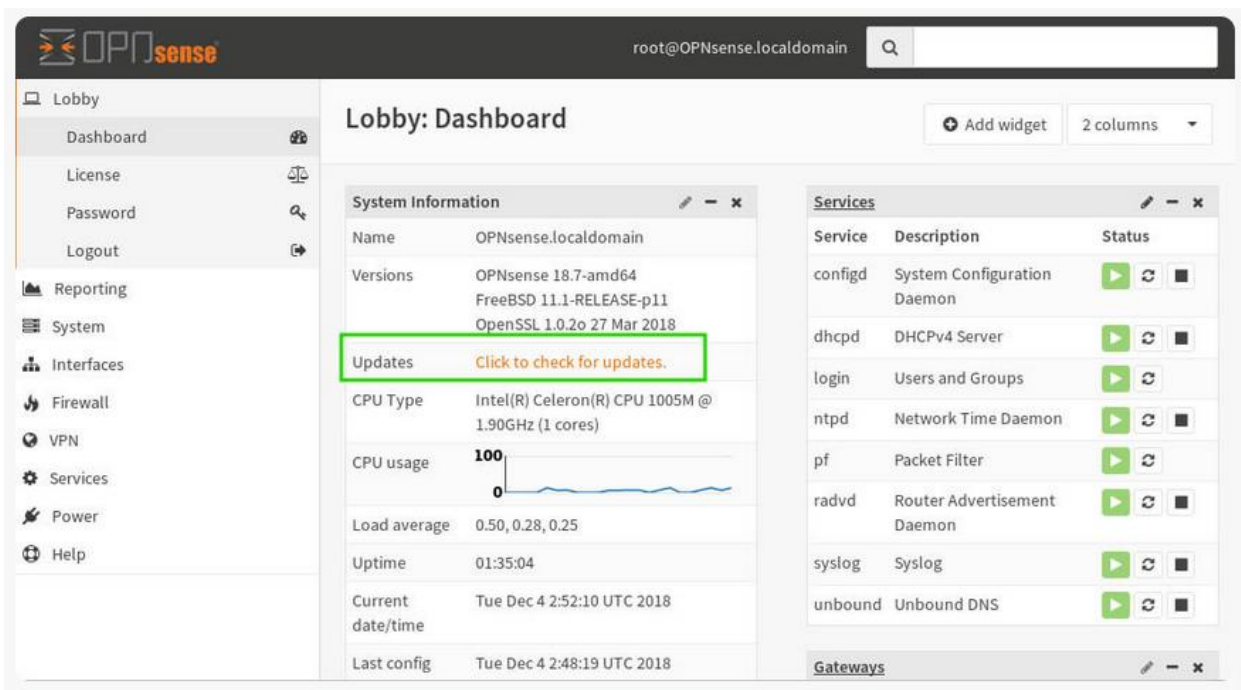
### Finished initial configuration!



Congratulations! OPNsense is now configured.

Please consider donating to the project to help us with our overhead costs. See [our website](#) to donate or purchase available OPNsense support services.

Click to [continue to the dashboard](#).



OPNsense

root@OPNsense.localdomain

Lobby

Dashboard

License

Password

Logout

Reporting

System

Interfaces

Firewall

VPN

Services























Power

Help

### Lobby: Dashboard

Add widget 2 columns

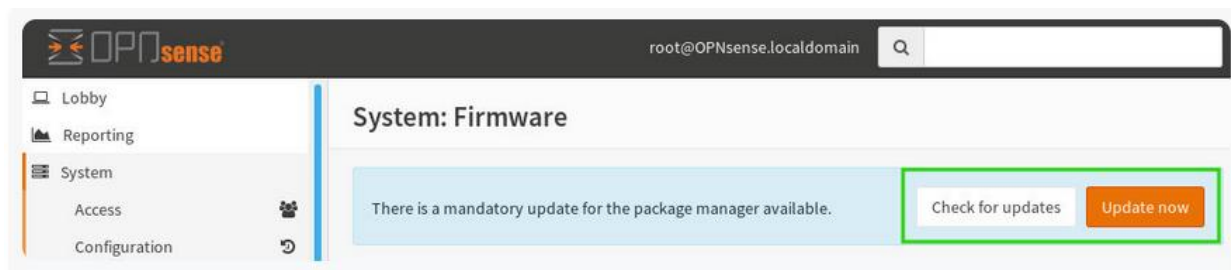
System Information	
Name	OPNsense.localdomain
Versions	OPNsense 18.7-amd64 FreeBSD 11.1-RELEASE-p11 OpenSSL 1.0.2o 27 Mar 2018
Updates	<a href="#">Click to check for updates.</a>
CPU Type	Intel(R) Celeron(R) CPU 1005M @ 1.90GHz (1 cores)
CPU usage	100
Load average	0.50, 0.28, 0.25
Uptime	01:35:04
Current date/time	Tue Dec 4 2:52:10 UTC 2018
Last config	Tue Dec 4 2:48:19 UTC 2018

Services		
Service	Description	Status
configd	System Configuration Daemon	  
dhcpcd	DHCPv4 Server	  
login	Users and Groups	 
ntpd	Network Time Daemon	  
pf	Packet Filter	 
radvd	Router Advertisement Daemon	  
syslog	Syslog	  
unbound	Unbound DNS	  

Gateways	
----------	--



در آخر، اگر تغییرات اعمال شده در شبکه با خواسته‌ها و اهدافمان همخوانی داشت، برنامه را یک بار آپدیت می‌کنیم تا تغییرات در کل شبکه‌ی انتخابی پیاده‌سازی شوند.



نصب و راه‌اندازی برنامه در این نقطه به انتها رسیده و در صورت لزوم می‌توانیم از قسمت Dashboard فایروال را در سطح شبکه غیرفعال کنیم.

پایان.