????????? ???????? OPNsense 20.x ??? ??????????? ?????? RackCorp

??????:

Настроить OPNsense достаточно просто, если у вас есть прямой доступ к «голому железу» (bare metal) или есть виртуализация рабочего стола, где можно определить внутренние сетевые адаптеры / сети, которые можно использовать для управления со стороны локальной сети.

Однако, поскольку мы настраиваемся в гибридном публичном/частном облаке, без настройки терминала управления (ВМ) в той же подсети, что и сеть LAN, мы не сможем управлять и настраивать OPNsense, поскольку заблокированный интерфейс WAN является единственным открытым для "внешнего мира". Кроме того, ограниченная конфигурация предоставляется через его шелл.

Мы хотим, чтобы некоторые управляющие порты (должным образом защищенные) были доступны для Интернета.

Для нашего гибридного облака мы поменяем местами публичный и частный интерфейсы в OPNsense.
Это противоположно ожидаемому процессу установки. Мы делаем это, потому что интерфейс LAN имеет предустановленное правило «разрешить все», которое позволяет нам входить в портал управления.

Это позволит нам легко настроить систему удаленно через веб-браузер, а затем мы снова изменим настройки на общедоступный IP-адрес на интерфейсе WAN и частный IP-адрес на интерфейсах LAN.

> Общие шаги по запуску OPNsense 20 на RackCorp Hybrid заключаются в следующем:

> Установить ISO

> Организовать доступ к веб-интерфейсу (Web GUI)

>

Создать правило для фаервола на интерфейсе WAN для удаленного управления

Переназначить/поменять местами интерфейсы LAN/WAN

Обновить IP-адрес для интерфейсов LAN/WAN

IP-адрес WAN, включенный в это руководство, приведен только для примера. Пожалуйста, замените его на тот, который Вам предоставили сотрудники RackCorp

```
Starting DHCPv4 service...done.

You can now access the web GUI by opening
the following URL in your web browser:

    http://10.0.0.1

*** OPNsense.localdomain: OPNsense 20.1.6 (amd64/OpenSSL) ***

 LAN (vtnet0)    -> v4: 10.0.0.1/24
 WAN (vtnet1)    -> v4/DHCP4: 116.206.80.210/24

 SSH:   SHA256 sALNA9gQ9chUqK0o0eTjNoYrWIIVbDZhBfmbzYJNO7E (ECDSA)
 SSH:   SHA256 0NKgHOnGIkyarnGc5Vg9196v9i+2qYD2vc1jDKsQ3nY (ED25519)
 SSH:   SHA256 m1KHCBMbD0BjgIdlfaLCfS/pNn4zL1X5GB7Cp/dqopU (RSA)

  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. ?????????? ISO

OPNsense назначает свои интерфейсы сетевым адаптерам (NIC) в том порядке, в котором они назначены на портале RackCorp, начиная с интерфейса LAN.

Итак, давайте «поменяем местами» интерфейсы, чтобы мы могли войти на веб-страницу управления:

1. Начните со следующей конфигурации портала RackCorp и OPNsense на вашей виртуальной машине RackCorp:

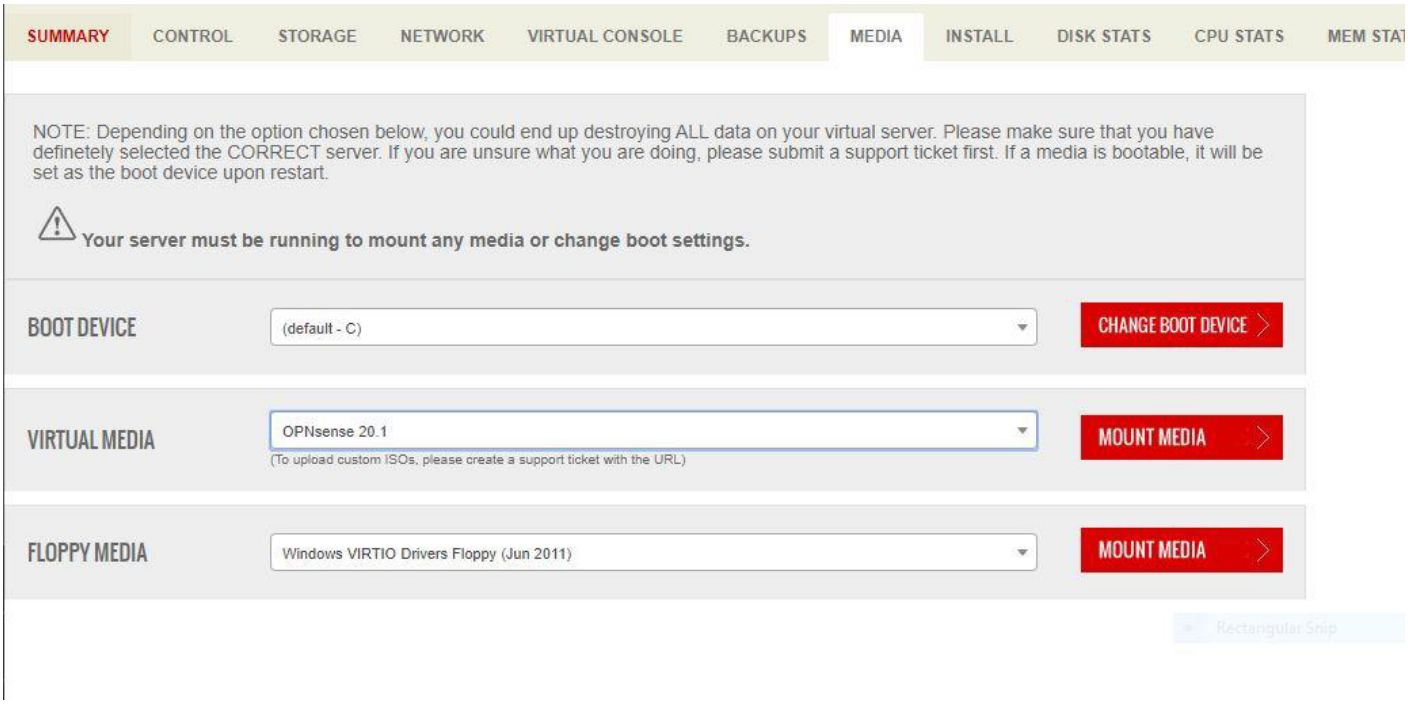
RackCorp vNIC ID	RackCorp vNIC Label	IP	VLAN	OPNsense Interface
NIC 1	Public	116.206.80.210 /27	<your assigned VLAN> Public VLAN1 for Demo	LAN (vtnet0)
NIC 2	Private	10.0.0.1 /24	<your assigned VLAN> Public VLAN1 for Demo	WAN (vtnet1)

Когда конфигурация верна, на портале Rackcorp загорится зеленый свет.

- Не забудьте добавить сети VLAN
- Для демонстрации мы оставили метки vNIC по умолчанию. Если метки vNIC сбивают с толку, вы можете определить их на основе интерфейса, например Частный или общедоступный в сочетании с концом MAC-адреса vNIC, например 33 или 34.

---

2. Следуйте инструкциям по загрузке и установке opnsense 20.x, используя файл образа ISO.
2.1 Смонтируйте ISO-образ установщика OPNsense на портале RackCorp, а затем загрузите виртуальную машину.



2.2 Живая среда загружается при необязательной установке.

> Не запускайте назначение интерфейса во время загрузки, если вы собираетесь установить на HD.

```
Starting PFLOG...done.
Syncing OpenVPN settings...done.
Starting NTP service...deferred.
Starting Unbound DNS...done.
Generating RRD graphs...done.
Configuring system logging...done.
>>> Invoking start script 'newwanip'
>>> Invoking start script 'freebsd'
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs
Fri May 15 01:42:31 UTC 2020

*** OPNsense.localdomain: OPNsense 20.1 (amd64/OpenSSL) ***

 LAN (vtnet0)    -> v4: 192.168.1.1/24

 HTTPS: SHA256 D8 FA 8E 37 F2 3B BB 0D 14 F1 F5 A6 D5 CF DA 99
               4F AE 93 84 93 DD 4B F9 70 B7 6F 41 33 88 FC 2B

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login:
```

2.3 После загрузки установите систему на диск, используя следующие учетные данные:

Login: **installer**
password: **opnsense**

Следуйте инструкциям по установке на жесткий диск. Значения по умолчанию подходят для установки на один диск. После завершения следуйте инструкциям, чтобы перезагрузить установку opnsense и ИЗВЛЕЧЬТЕ ISO-образ с портала RackCorp.

2. ??????????? ?????? ? ???-?????????? (Web GUI)

3. После установки, Opnsense загрузится в меню консоли, которая имеет встроенный мастер установки. Он помогает пользователю настроить свою сетевую карту LAN, сетевую карту WAN, любую третичную сетевую карту, например DMZ или управляющую сетевую карту, а также адресацию IPv4 / 6 и DHCP.

3.1 **УСТАНОВИТЕ IP-ИНТЕРФЕЙС** для **WAN**
Выберите **NONE**, это очистит интерфейс и позволит нам переназначить.

3.2 **УСТАНОВИТЕ IP-ИНТЕРФЕЙС** для **LAN**
Выберите **116.206.80.210/27** согласно таблице.

Поскольку в этом примере используется 27-битная подсеть, наш шлюз - .193, наш максимальный хост - .223.

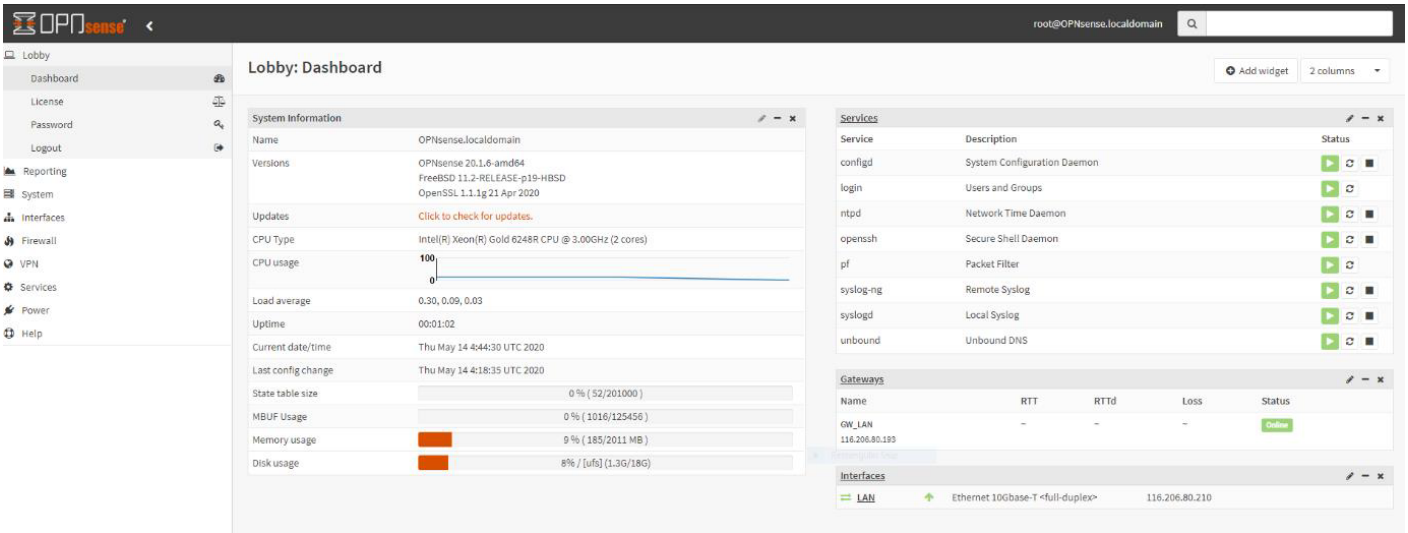
Для DNS используйте RackCorp NS1 110.232.116.249 или Google DNS 8.8.8.8

Interface	**LAN**
DHCP	No
New LAN IP	116.206.80.210
Subnet	27

Gateway	116.206.80.193
Gateway as name server	No
IPv4 Name server	8.8.88
IPv6 LAN Interface via WAN Tracking:	No
IPv6 LAN Interface via DHCP:	No
IPv6 Address:	<enter> for none
LAN DHCP Server:	n
HTTP fallback for web GUI	n

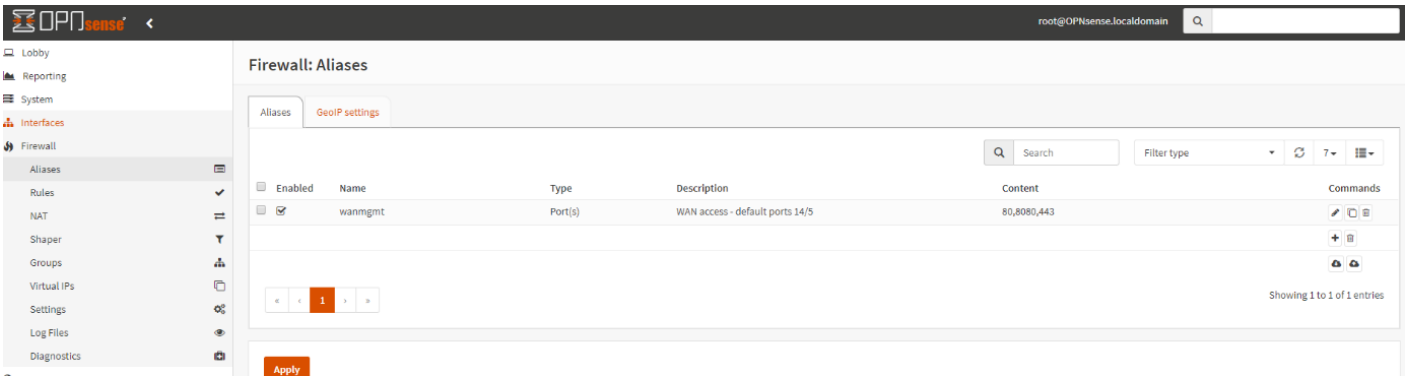
4. После ввода IP-адреса LAN вы сможете получить доступ через веб-браузер. Вы увидите вводный мастер установки, но не забудьте пропустить страницу настройки WAN. Тспользуя учетные данные, войдите на веб-страницу OPNsense. Щелкните логотип вверху слева, чтобы пропустить мастер настройки.

После того, как мы вошли на страницу управления OPNsense, это подтверждение того, что мы можем получить доступ к системе.



3. ??????? ??????? ??? ???????? ?? ?????????? WAN ??? ????????? ?????????

5. Добавьте псевдоним для определения портов управления. **Брандмауэр (Firewall)-> Псевдонимы (Aliases)**. В этом примере мы используем порты **80, 443, 8080**. **[Сохранить]. [Применить]**

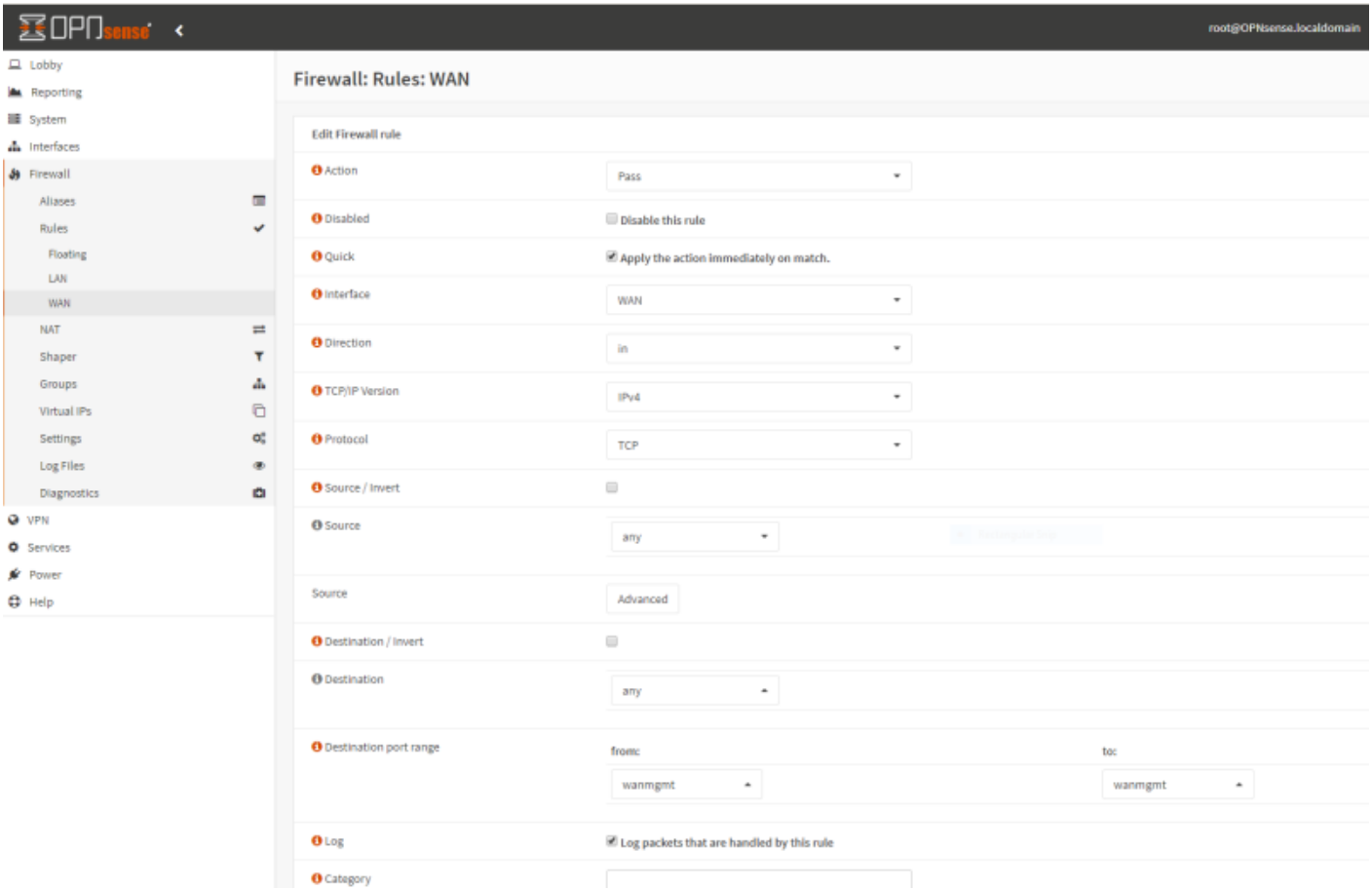


---

6. Добавьте правило переадресации порта WAN в **Firewall -> Rules -> WAN**.

Protocol:	TCP
Source Port:	Any
Destination port range Start:	<Your alias name> Scroll UP in the list to find it.
Destination port range End:	<Your alias name> Scroll UP in the list to find it.
Log Packets:	Enabled

[Save]. [Apply].



---

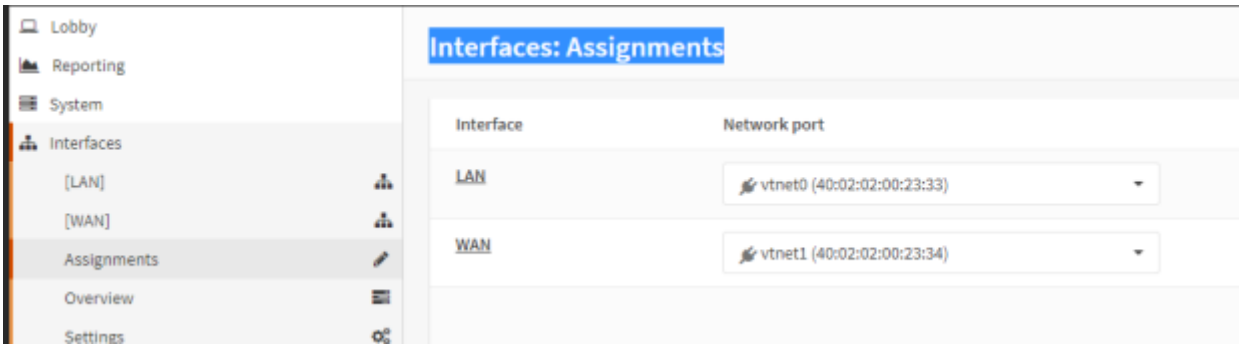
4. ??????????????/???????? ??????? ??????????? LAN/WAN

7. **Интерфейсы (Interfaces)-> Назначения (Assignments)**. Сравните настройки здесь с данными на портале Rackcorp.

На данный момент мы должны находится: LAN-интерфейс с публичным IP-адресом, установленным в OPNsense, и WAN-интерфейс без WAN-IP (a LAN Interface with public IP set in OPNsense and WAN interface with no WAN IP set).

Поскольку наш Port Forward, который позволит нам получить доступ к интерфейсу управления извне, теперь определен, мы можем поменять местами интерфейсы. Вам необходимо поменять местами оба интерфейса на портале OPNsense .

7.1 На портале OPNense (**Интерфейсы (Interfaces)-> Назначения (Assignments)**) поменяйте местами настройки
(LAN) -> VTNET1 RackCorp NIC 2
(WAN) -> VTNET0 RackCorp NIC 1



[SAVE]

5. ???????? IP-????? ??? ??????????? LAN/WAN

8. После того, как вы поменяли местами порты, OPNense может забыть об IP-подсетях, и нам нужно повторно ввести их в консоли.

Повторно введите IP / подсети, используя опцию 2. Удалите их, если необходимо, с помощью <ENTER NONE>.

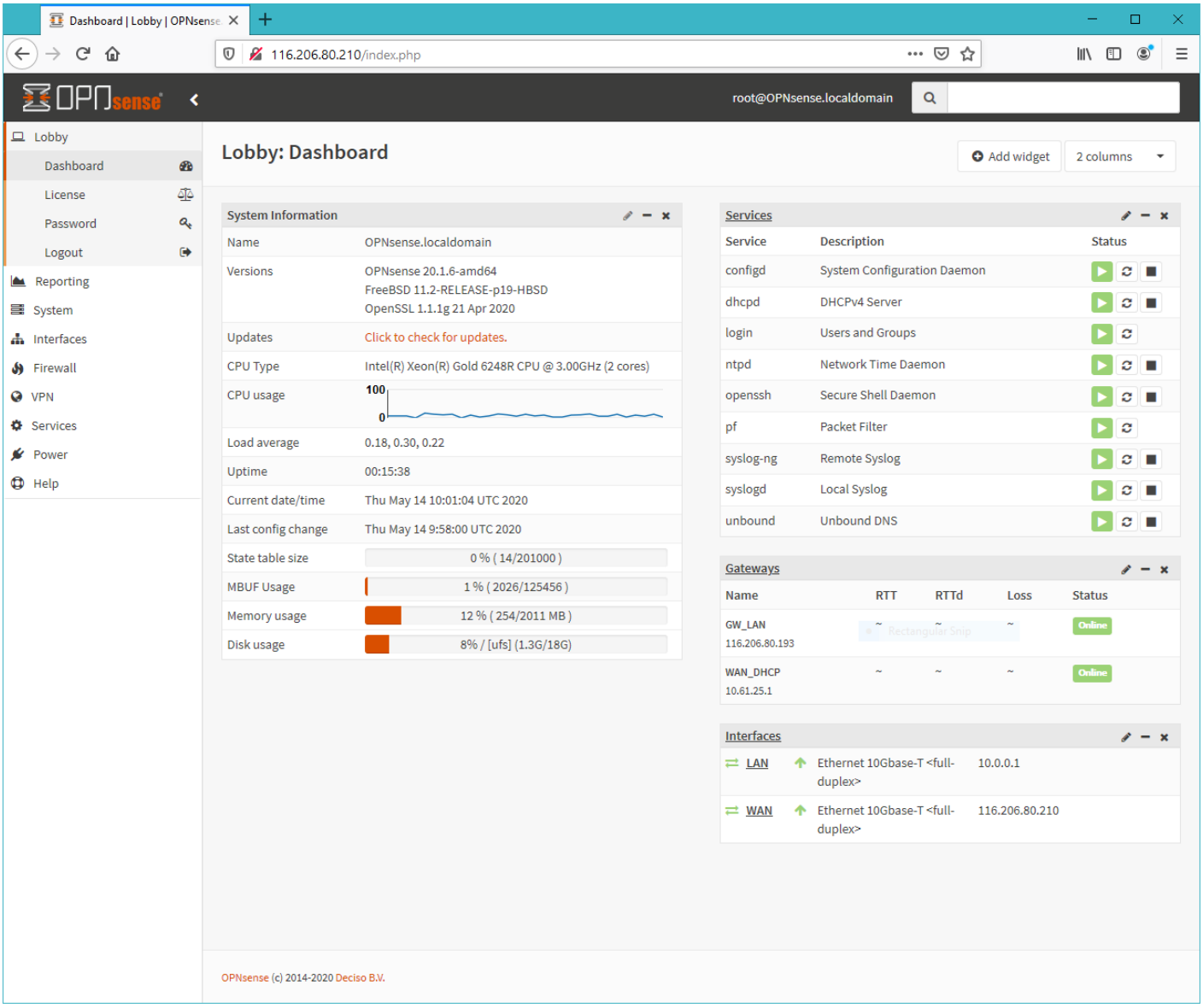
Interface	**LAN**
Configure via DHCP	No
New LAN IP	10.0.0.1
Subnet	24
Gateway	<enter> for none
IPv6 LAN Interface via WAN Tracking:	N
IPv6 LAN Interface via DHCP6:	N
IPv6 Address:	<enter for none
LAN DHCP Server:	Y
SDHCP End Address:	10.0.0.20
Revert to HTTP as web GUI protocol	N

Interface	**WAN**
Configure via DHCP	N
New WAN IP	116.206.80.210

Subnet	27
Gateway	116.206.0.193
Gateway as name server	no
IPv4 Name server	8.8.8.8
IPv6 WAN Interface via DHCP6:	N
IPv6 Address:	<enter> for none
Revert to HTTP as web GUI protocol	N

```
> 10.0.0.1


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] y

Enter the start address of the IPv4 client address range: 10.0.0.10
Enter the end address of the IPv4 client address range:
```

9. После изменения ключей LAN и WAN вы сможете войти в портал управления OPNsense через его адрес WAN, а индикаторы состояния RackCorp vNIC загорятся зеленым.



10. Следуйте далее для дальнейшей настройки по мере необходимости.

11. Если у вас возникли проблемы с этой процедурой, выберите **(4) Reset Factory Settings** в меню консоли. OPNsense перезагрузится, а затем выключится. Перезагрузите виртуальную машину из RackCorp и повторите попытку. **Перезагрузка всех сервисов тоже может помочь.**

```
Starting DHCPv4 service...done.
Starting Unbound DNS...done.
Setting up gateway monitors...done.
Configuring firewall.......done.
Starting PFLOG...done.
Starting DHCPv4 service...done.


*** OPNsense.localdomain: OPNsense 20.1 (amd64/OpenSSL) ***

 LAN (vtnet1)    -> v4: 10.0.0.1/24
 WAN (vtnet0)    -> v4: 116.206.80.210/27

 HTTPS: SHA256 EA 6C C7 4F A1 4E CE 5D E4 2F 2F FA 80 52 21 DB
               E7 A7 50 1A 6B 18 27 F1 9C 77 7E 79 5D 78 3E 62

  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:
```

?????????????? ?????????

После того, как ваша базовая установка будет запущена, ее можно будет дополнительно настроить в соответствии с вашими требованиями.

Ознакомьтесь с политикой безопасности вашей компании а именно, о том, как обращаться с управлением устройством (appliance management).

Также для размышления, многие из которых являются лучшими отраслевыми практиками.

- Рассмотрение вопроса о добавлении сети управления или одной или нескольких сетей DMZ к фаерволу для дополнительной функциональности
- Используйте функцию VPN для входа в систему управления вместо портов HTTP / S
- Используйте функции VPN для удаленных сотрудников, чтобы иметь доступ к корпоративному контенту
- Если порты HTTP / S требуются для управления через WAN / Интернет, рассмотрите возможность изменения номеров портов и / или внесения в белый список OPNSense IP / URL для определенных авторизованных систем управления
- При необходимости настройте и протестируйте доступ по SSH с помощью разрешенного списка, интерфейса управления или VPN-туннеля
- Установите дополнительные плагины, такие как Wireguard VPN или другие утилиты, через страницу плагинов, чтобы расширить функциональность фаервола

Revision #9
Created 24 November 2021 06:45:03 by KonS
Updated 30 May 2022 05:24:30 by KonS