

Распределенные системы

ДЗ 03

Выполнил: Зеленин Е.В.

В качестве домашнего задания требуется создать сертификаты для доменных имен, настроенных в первом занятии, установить и настроить Nginx в Docker контейнере, проверить доступность сервисов через интернет.

Сгенерируем сертификаты через Certbot:

```
Please deploy a DNS TXT record under the name:
_acme-challenge.molnija3d.ru.

with the following value:

j4ebDdtJ8EfQc1T2fwNlmR3rQs0qwBhY5944dHYERwQ

-----
Press Enter to Continue

-----
Please deploy a DNS TXT record under the name:
_acme-challenge.molnija3d.ru.

with the following value:

y3X9KE_NonVlj5XxmOeEJFE0CamKBGnmkH9z2Lr_UaE

(This must be set up in addition to the previous challenges; do not remove,
replace, or undo the previous challenge tasks yet. Note that you might be
asked to create multiple distinct TXT records with the same name. This is
permitted by DNS standards.)

Before continuing, verify the TXT record has been deployed. Depending on the DNS
provider, this may take some time, from a few seconds to multiple minutes. You can
check if it has finished deploying with aid of online tools, such as the Google
Admin Toolbox: https://toolbox.googleapps.com/apps/dig/#TXT/_acme-challenge.molnija3d.ru.
Look for one or more bolded line(s) below the line ';ANSWER'. It should show the
value(s) you've just added.

-----
Press Enter to Continue
```

<input type="text" value="_acme-challenge.molnija3d.ru"/>	<input type="text" value="TXT"/>	<input type="text" value="j4ebDdtJ8EfQc1T2fwNlmR3rQs0qwBhY5944dHYERwQ"/>
<input type="text" value="_acme-challenge.molnija3d.ru"/>	<input type="text" value="TXT"/>	<input type="text" value="y3X9KE_NonVlj5XxmOeEJFE0CamKBGnmkH9z2Lr_UaE"/>

Проверим доменные записи и продолжим генерацию ключей:

Имя

_acme-challenge.molnija3d.ru

A

AAAA

ANY

CAA

CNAME

DNSKEY

DS

MX

NS

PTR

SOA

SRV

TLSA

TSIG

TXT

TTL:

1 hour 3 minutes 20 seconds

VALUE:

"j4ebDdtJ8EfQc1T2fwN1mR3rQs0qwBhY5944dHYERwQ"

TXT

TTL:

1 hour 3 minutes 20 seconds

VALUE:

"y3X9KE_NonV1j5Xxm0eEJFE0CamKBGnmkH9z2Lr_UaE"

Сертификаты сгенерированы успешно:

```
Before continuing, verify the TXT record has been deployed. Depending on the DNS provider, this may take some time, from a few seconds to multiple minutes. You can check if it has finished deploying with aid of online tools, such as the Google Admin Toolbox: https://toolbox.googleapps.com/apps/dig/#TXT/\_acme-challenge.molnija3d.ru. Look for one or more bolded line(s) below the line ';ANSWER'. It should show the value(s) you've just added.
```

```
-- -- -- -- --
Press Enter to Continue
```

```
Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/molnija3d.ru/fullchain.pem
Key is saved at:      /etc/letsencrypt/live/molnija3d.ru/privkey.pem
This certificate expires on 2025-08-24.
These files will be updated when the certificate renews.
```

NEXT STEPS:

```
- This certificate will not be renewed automatically. Autorenewal of --manual certificates requires a cron job as not provided. To renew this certificate, repeat this same certbot command before the certificate expires.
```

```
-- -- -- -- --
If you like Certbot, please consider supporting our work by:
```

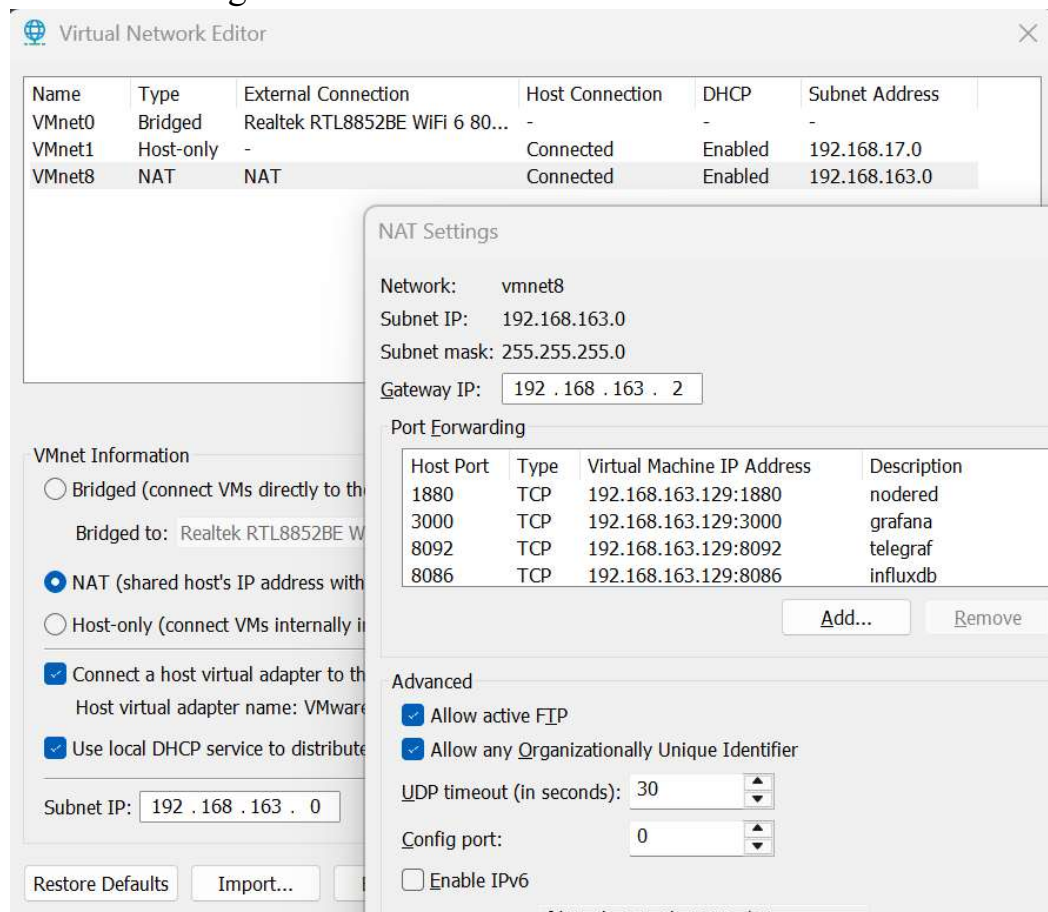
- * Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>
- * Donating to EFF: <https://eff.org/donate-le>

Настроим PortForwarding. В моем случае структура сети имеет несколько более сложную организацию. Интернет подключен через Firewall на FreeBSD, после него подключен WiFi роутер, которому подключен ноутбук. На ноутбуке запущена виртуальная машина через NAT (т.к. Bridge mode не дает выделить второй MAC адрес для виртуальной машины через WiFi, а это необходимо для корректной работы внутреннего DHCP сервера).

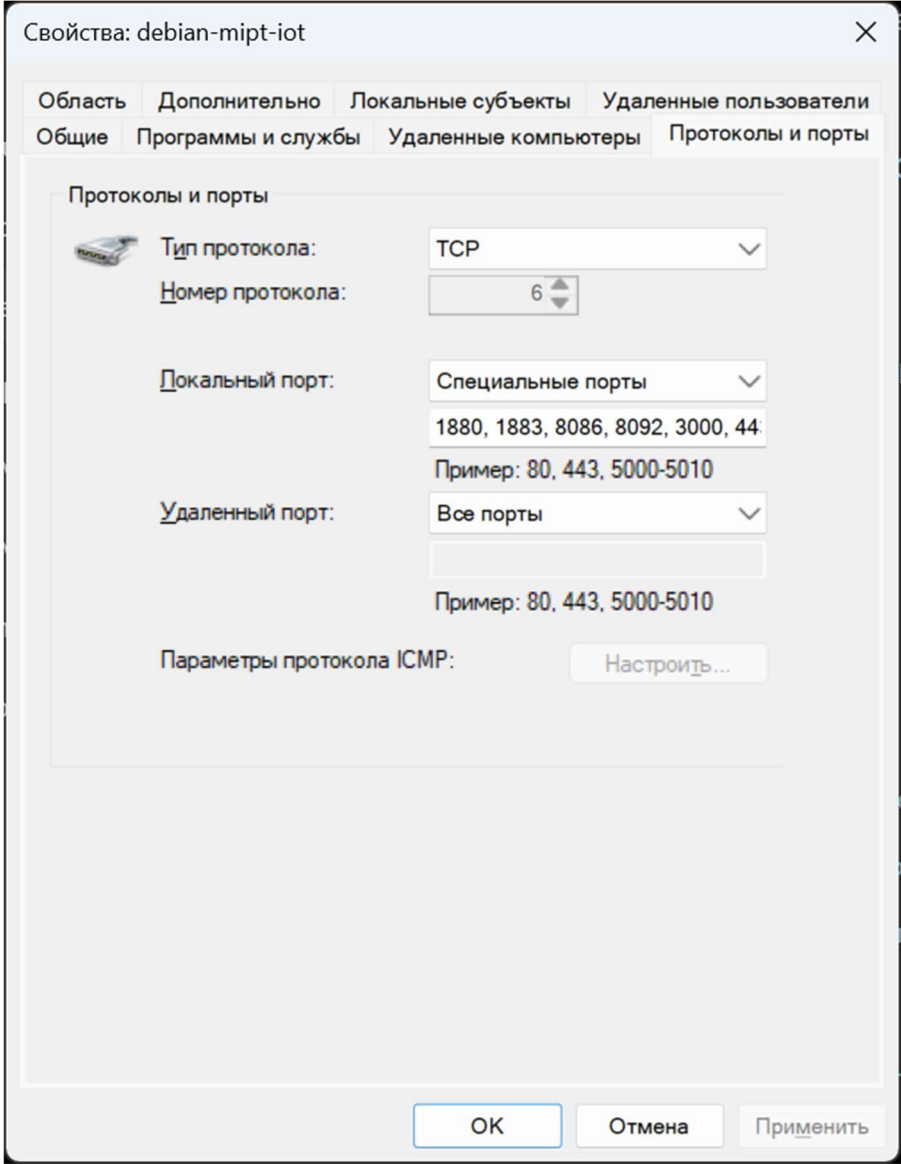
Таким образом, настройки выглядят следующим образом:

- 1) Пробросить порт через Nat виртуальной машины на IP ноутбука, сделать настройки Firewall windows и открыть необходимые порты.
- 2) На WiFi роутере настроить PortForwarding с IP ноутбука на WAN IP роутера
- 3) На FreeBSD настроить portforwarding с IP WiFi роутера на внешний IP адрес, полученный от провайдера.

PortForwarding на VMWare:



Правило на Windows Firewall:



Настройка портов на Wi-Fi роутере:

SSH	****	2244	192.169.5.180	2244	TCP/UDP	<input type="checkbox"/>
nodored	****	1880	192.169.5.180	1880	TCP	<input type="checkbox"/>
graphana	****	3000	192.169.5.180	3000	TCP	<input type="checkbox"/>
telegraf	****	8092	192.169.5.180	8092	TCP	<input type="checkbox"/>
influx	****	8086	192.169.5.180	8086	TCP	<input type="checkbox"/>
mosquitto	****	1883	192.169.5.180	1883	TCP	<input type="checkbox"/>
nginx	****	443	192.169.5.180	443	TCP	<input type="checkbox"/>

Настройка портов на pfSense:

pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

Firewall

NAT

Port Forward

The NAT configuration has been changed.

The changes must be applied for them to take effect.

Apply Changes

Port Forward

1:1

Outbound

NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN_PPPOE	TCP	*	*	WAN_PPPOE address	443 (HTTPS)	192.169.7.2	443 (HTTPS)	nginx	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN_PPPOE	TCP	*	*	WAN_PPPOE address	1883	192.169.7.2	1883	mosquitto	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN_PPPOE	TCP	*	*	WAN_PPPOE address	8086	192.169.7.2	8086	influxdb	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN_PPPOE	TCP	*	*	WAN_PPPOE address	8092	192.169.7.2	8092	telegraf	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN_PPPOE	TCP	*	*	WAN_PPPOE address	3000 (HBCI)	192.169.7.2	3000 (HBCI)	graphana	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN_PPPOE	TCP	*	*	WAN_PPPOE address	1880	192.169.7.2	1880	nodered	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN_PPPOE	TCP/UDP	*	*	WAN_PPPOE address	2244	192.169.7.2	2244	ssh-virtual	<div><div></div><div></div><div></div></div>

↑ Add

↓ Add

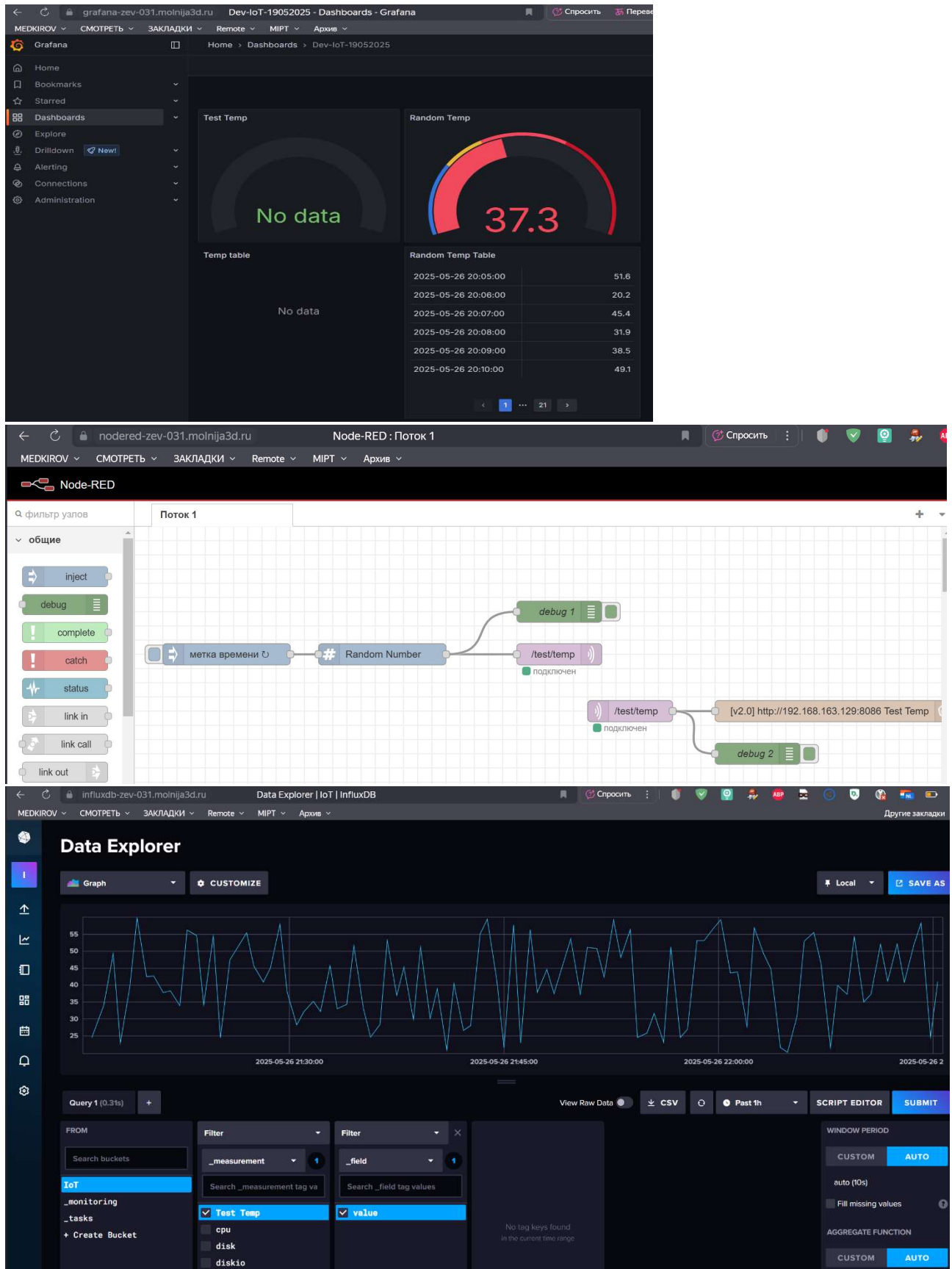
Delete

Toggle

Save

+ Separator

Проверим доступность сервисов из вне:



Как видно из скриншотов, сервисы работают, доступ обеспечен.

Можно проверить доступность сервисов по следующим ссылкам:

1) <https://grafana-zev-031.molnija3d.ru>

login: admin

password: myIOT25*

2) <https://nodered-zev-031.molnija3d.ru>

3) <https://telegraf-zev-031.molnija3d.ru>

4) <https://influxdb-zev-031.molnija3d.ru>

login: iotuser1

password: myIOT25*

Виртуальную машину сначала сделал на VMware на ноутбуке, потом перенес на домашний гипервизор Proxmox.

