

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет безопасности информационных технологий

Дисциплина:

«Вычислительные сети и контроль безопасности в компьютерных сетях»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

«Безопасность DNS»

Выполнили:

Чу Ван Доан, студент группы N3347



(подпись)

Чан Бао Линь, студентка группы N3346



(подпись)

Проверил:

Савков Сергей Витальевич, инженер факультета БИТ

(отметка о выполнении)

(подпись)

Санкт-Петербург

2025 г.

СОДЕРЖАНИЕ

Содержание.....	2
Введение.....	3
Задание.....	4
Ход работы.....	5
1. Подготовка практического стенда.....	5
2. Установка BIND на SRV1 и SRV2.....	6
3. Настройка BIND на SRV1.....	7
4. Настройка BIND на SRV2.....	11
5. Тестирование разрешения DNS.....	13
6. Настройка DNSSEC на SRV2.....	16
7. Проведение тестирования.....	19
7.1. Тест-кейс 1: Проверка ping между машинами (SRV1, SRV2, Клиент).....	19
7.2. Тест-кейс 2: Проверка службы BIND на SRV1.....	20
7.3. Тест-кейс 3: Проверка разрешения lab.test с Клиента.....	21
7.4. Тест-кейс 4: Проверка разрешения srv1.lab.test.....	21
7.5. Тест-кейс 5: Проверка разрешения srv2.lab.test.....	22
7.6. Тест-кейс 6: Проверка разрешения my.lab.test через SRV1.....	23
7.7. Тест-кейс 7: Проверка прямого разрешения my.lab.test на SRV2.....	24
7.8. Тест-кейс 8: Проверка разрешения srv2.my.lab.test.....	25
7.9. Тест-кейс 9: Проверка разрешения с использованием DNSSEC.....	26
Заключение.....	28

ВВЕДЕНИЕ

Цель работы - Изучить основные принципы работы системы доменных имен DNS, получить представление об основных угрозах безопасности DNS, изучить основы настройки серверов DNS на примере BIND.

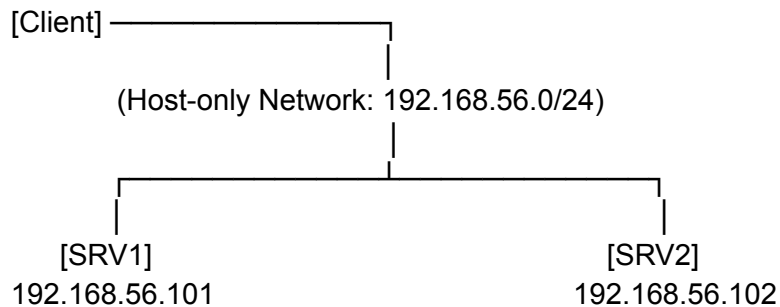
Задание

- Настроить лабораторный стенд согласно сетевой схеме. Для настройки лабораторного стенда можно использовать среду GNS3 либо ПО для работы с виртуальными машинами.
- На сервере SRV1 настроить зону lab.test. С помощью утилит dig/nslookup проверить работоспособность зоны.
- На сервере SRV1 настроить делегирование поддомена my.lab.test на сервер SRV2. На сервере SRV2 настроить зону my.lab.test, проверить ее работоспособность с клиентского устройства.
- Для дочерней зоны my.lab.test настроить механизм DNSSEC для обеспечения защиты от атак типа DNS-spoofing. Убедиться в корректности разрешения имен и проверки цифровой подписи DNS-запросов.

ХОД РАБОТЫ

1. Подготовка практического стенда

Сетевая схема:



- SRV1: основной DNS-сервер для домена lab.test, также имеет сетевую карту NAT для доступа в интернет.
- SRV2: резервный DNS-сервер, обслуживает домен my.lab.test.
- Client: использует команды dig или nslookup для проверки работы DNS.

Машина	Адаптер 1	Адаптер 2
SRV1	NAT	Host-only (имя: vboxnet0)
SRV2	Host-only (vboxnet0)	
CLIENT	Host-only (vboxnet0)	

```
srv1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@srv1:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d3:19:0e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 83700sec preferred_lft 83700sec
    inet6 fd17:625c:f037:2:a00:27ff:fed3:190e/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86036sec preferred_lft 14036sec
    inet6 fe80::a00:27ff:fed3:190e/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:73:ef:2d brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe73:ef2d/64 scope link
        valid_lft forever preferred_lft forever
root@srv1:~# ip route
default via 10.0.2.2 dev enp0s3 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15
10.0.2.2 dev enp0s3 proto dhcp scope link src 10.0.2.15 metric 100
192.168.56.0/24 dev enp0s8 proto kernel scope link src 192.168.56.101
root@srv1:~#
```

Рисунок 1 – Настройка сети на SRV1

```
srv2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@srv2:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c4:a7:c6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec4:a7c6/64 scope link
        valid_lft forever preferred_lft forever
root@srv2:~# ip route
default via 192.168.56.101 dev enp0s3 proto static
192.168.56.0/24 dev enp0s3 proto kernel scope link src 192.168.56.102
root@srv2:~#
```

Рисунок 2 – Настройка сети на SRV2

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5c:92:8c brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.1/24 brd 192.168.56.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe5c:928c/64 scope link
        valid_lft forever preferred_lft forever
root@client:~# ip route
default via 192.168.56.101 dev enp0s3 proto static
192.168.56.0/24 dev enp0s3 proto kernel scope link src 192.168.56.1
root@client:~#
```

Рисунок 3 – Настройка сети на Client

2. Установка BIND на SRV1и SRV2

- Запустите на обоих серверах SRV1 и SRV2:

```
sudo apt update
```

```
sudo apt install bind9 bind9utils bind9-doc -y
```

- быстрая проверка, что BIND9 слушает IPv4:

```
sudo ss -tulpn | grep named
```

```
srv1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
bind9-doc is already the newest version (1:9.18.30-0ubuntu0.20.04.2).
bind9utils is already the newest version (1:9.18.30-0ubuntu0.20.04.2).
0 upgraded, 0 newly installed, 0 to remove and 57 not upgraded.
root@srv1:~# ss -tulnp | grep named
udp UNCONN 0 0 192.168.56.101:53 0.0.0.0:
* users:(("named",pid=2025,fd=21))
udp UNCONN 0 0 10.0.2.15:53 0.0.0.0:
* users:(("named",pid=2025,fd=19))
udp UNCONN 0 0 127.0.0.1:53 0.0.0.0:
* users:(("named",pid=2025,fd=16))
udp UNCONN 0 0 [::1]:53 [::]:
* users:(("named",pid=2025,fd=23))
udp UNCONN 0 0 [fd17:625c:f037:2:a00:27ff:fed3:190e]:53 [::]:
* users:(("named",pid=2025,fd=25))
udp UNCONN 0 0 [fe80::a00:27ff:fed3:190e]%enp0s3:53 [::]:
* users:(("named",pid=2025,fd=27))
udp UNCONN 0 0 [fe80::a00:27ff:fe73:ef2d]%enp0s8:53 [::]:
* users:(("named",pid=2025,fd=29))
tcp LISTEN 0 10 192.168.56.101:53 0.0.0.0:
* users:(("named",pid=2025,fd=22))
tcp LISTEN 0 10 10.0.2.15:53 0.0.0.0:
* users:(("named",pid=2025,fd=20))
tcp LISTEN 0 10 127.0.0.1:53 0.0.0.0:
* users:(("named",pid=2025,fd=17))
tcp LISTEN 0 5 127.0.0.1:953 0.0.0.0:
* users:(("named",pid=2025,fd=24))
```

Рисунок 4 – BIND правильно слушает IPv4 на SRV1

```
srv2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@srv2:~# ss -tulnp | grep named
udp UNCONN 0 0 192.168.56.102:53 0.0.0.0:*
* users:(("named",pid=1973,fd=19))
udp UNCONN 0 0 127.0.0.1:53 0.0.0.0:*
* users:(("named",pid=1973,fd=16))
udp UNCONN 0 0 [::1]:53 [::]:*
* users:(("named",pid=1973,fd=21))
udp UNCONN 0 0 [fe80::a00:27ff:fec4:a7c6]%enp0s3:53 [::]:*
* users:(("named",pid=1973,fd=23))
tcp LISTEN 0 10 192.168.56.102:53 0.0.0.0:*
* users:(("named",pid=1973,fd=20))
tcp LISTEN 0 10 127.0.0.1:53 0.0.0.0:*
* users:(("named",pid=1973,fd=17))
tcp LISTEN 0 5 127.0.0.1:953 0.0.0.0:*
* users:(("named",pid=1973,fd=25))
tcp LISTEN 0 10 [::1]:53 [::]:*
* users:(("named",pid=1973,fd=22))
tcp LISTEN 0 10 [fe80::a00:27ff:fec4:a7c6]%enp0s3:53 [::]:*
* users:(("named",pid=1973,fd=24))
tcp LISTEN 0 5 [::1]:953 [::]:*
* users:(("named",pid=1973,fd=26))
root@srv2:~#
```

Рисунок 5 – BIND правильно слушает IPv4 на SRV2

3. Настройка BIND на SRV1

- Создание каталога zones: `sudo mkdir -p /etc/bind/zones`
- Редактирование файла: `sudo nano /etc/bind/named.conf.options`
- Добавьте ACL для клиентов, которым разрешён доступ:

```
acl "trusted" {  
  192.168.56.101; # SRV1  
  192.168.56.102; # SRV2  
  192.168.56.1; # Client  
};  
  
options {  
  directory "/var/cache/bind";  
  
  recursion yes;  
  allow-recursion { trusted; };  
  listen-on { 192.168.56.101; };  
  allow-transfer { none; };  
  
  forwarders {  
    8.8.8.8;  
    8.8.4.4;  
  };  
  
  dnssec-validation yes;  
};
```



```
srv1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@srv1:~# cat /etc/bind/named.conf.options
acl "trusted" {
    192.168.56.101; # SRV1
    192.168.56.102; # SRV2
    192.168.56.1;  # Client
};

options {
    directory "/var/cache/bind";
    recursion yes;
    allow-recursion { trusted; };
    listen-on { 192.168.56.101; };
    allow-transfer { none; };

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };

    dnssec-validation yes;
};
root@srv1:~#
```

Рисунок 6 – File `named.conf.options`

- Редактирование файла: `sudo nano /etc/bind/named.conf.local`
- Добавьте следующее содержимое:

```
zone "lab.test" {
type master;
file "/etc/bind/zones/db.lab.test";
};
```

```
srv1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@srv1:~# cat /etc/bind/named.conf.local
zone "lab.test" {
    type master;
    file "/etc/bind/zones/db.lab.test";
};
root@srv1:~#
```

Рисунок 7 – File `named.conf.local`

- Создание файла зоны: `sudo nano /etc/bind/zones/db.lab.test`
- Вставьте следующее содержимое:

```
$TTL 604800
```

```
@    IN    SOA    srv1.lab.test. admin.lab.test. (  
        3      ; Serial  
        604800    ; Refresh  
        86400     ; Retry  
        2419200   ; Expire  
        604800 )   ; Negative Cache TTL
```

```
;
```

```
; Name servers
```

```
    IN    NS     srv1.lab.test.
```

```
; A record for lab.test itself
```

```
@    IN    A     192.168.56.101
```

```
; A records for hosts
```

```
srv1  IN    A     192.168.56.101
```

```
srv2  IN    A     192.168.56.102
```

```
; NS record for subdomain
```

```
my    IN    NS     srv2.lab.test.
```

```
srv1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@srv1:~# cat /etc/bind/zones/db.lab.test
$TTL      604800
@         IN      SOA      srv1.lab.test. admin.lab.test. (
                        3      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
; Name server
@         IN      NS       srv1.lab.test.

; A records
@         IN      A        192.168.56.101
srv1      IN      A        192.168.56.101
srv2      IN      A        192.168.56.102

my        IN      NS       srv2.lab.test.
root@srv1:~# _
```

Рисунок 8 – File **db.lab.test**

- Проверка и перезапуск BIND:

`sudo named-checkconf`

`sudo named-checkzone lab.test /etc/bind/zones/db.lab.test`

`sudo systemctl restart bind9.service`

```
root@srv1:~# named-checkconf
root@srv1:~# named-checkzone lab.test /etc/bind/zones/db.lab.test
zone lab.test/IN: loaded serial 3
OK
root@srv1:~# systemctl restart bind9.service
root@srv1:~#
```

Рисунок 9 – Проверка и перезапуск BIND

4. Настройка BIND на SRV2

- Редактирование файла: `sudo nano /etc/bind/named.conf.local`
- Добавьте следующее содержимое:

```
zone "my.lab.test" {
    type master;
    file "/etc/bind/zones/db.my.lab.test";
};
```

```

root@srv2:~#
root@srv2:~# cat /etc/bind/named.conf.local
zone "my.lab.test" {
    type master;
    file "/etc/bind/zones/db.my.lab.test";
};
root@srv2:~#

```

Рисунок 10 – File **named.conf.local**

- Создание файла зоны:

sudo mkdir -p /etc/bind/zones

sudo nano /etc/bind/zones/db.my.lab.test

\$TTL 604800

```

@ IN SOA srv2.my.lab.test. admin.my.lab.test. (
    2 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL

```

;

; Name servers

```

IN NS srv2.my.lab.test.

```

; A record for my.lab.test itself

```

@ IN A 192.168.56.102

```

; A record for srv2

```

srv2 IN A 192.168.56.102

```

```

root@srv2:~# cat /etc/bind/zones/db.my.lab.test
$TTL      604800
@         IN      SOA      srv2.my.lab.test. admin.my.lab.test. (
                                4
                                604800
                                86400
                                2419200
                                604800 )
;
@         IN      NS       srv2.my.lab.test.
@         IN      A        192.168.56.102
srv2      IN      A        192.168.56.102

```

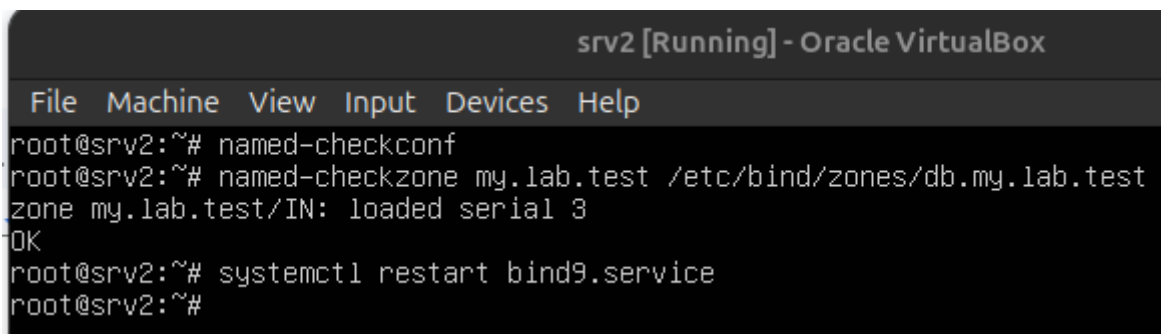
Рисунок 11 – File **db.my.lab.test**

- Проверка и перезапуск BIND:

`sudo named-checkconf`

`sudo named-checkzone my.lab.test /etc/bind/zones/db.my.lab.test`

`sudo systemctl restart bind9.service`



```

srv2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@srv2:~# named-checkconf
root@srv2:~# named-checkzone my.lab.test /etc/bind/zones/db.my.lab.test
zone my.lab.test/IN: loaded serial 3
OK
root@srv2:~# systemctl restart bind9.service
root@srv2:~#

```

Рисунок 12 – Проверка и перезапуск BIND

5. Тестирование разрешения DNS

На CLIENT:

`dig @192.168.56.101 lab.test`

`dig @192.168.56.101 srv1.lab.test`

`dig @192.168.56.101 my.lab.test`

`dig @192.168.56.102 my.lab.test`

```

root@client:~# dig @192.168.56.101 lab.test

; <<> DiG 9.18.30-Ubuntu0.20.04.2-Ubuntu <<> @192.168.56.101 lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1372
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 04a541a2ffbbd3ec01000000680cd34d5f2b7434e3d757a7 (good)
;; QUESTION SECTION:
;lab.test.                IN      A

;; ANSWER SECTION:
lab.test.                  604800  IN      A      192.168.56.101

;; Query time: 7 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sat Apr 26 12:36:29 UTC 2025
;; MSG SIZE rcvd: 81
root@client:~#

```

Рисунок 13 – Тестирование разрешения DNS На CLIENT

```

root@client:~# dig @192.168.56.101 srv1.lab.test

; <<> DiG 9.18.30-Ubuntu0.20.04.2-Ubuntu <<> @192.168.56.101 srv1.lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52167
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 349302681bceea3c01000000680cd5393233ff4236ff10af (good)
;; QUESTION SECTION:
;srv1.lab.test.           IN      A

;; ANSWER SECTION:
srv1.lab.test.            604800  IN      A      192.168.56.101

;; Query time: 4 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sat Apr 26 12:44:41 UTC 2025
;; MSG SIZE rcvd: 86

```

Рисунок 14 – Тестирование разрешения DNS На CLIENT

- добавить содержимое в файл /etc/bind/named.conf.local на SRV1:

```

zone "my.lab.test" {
    type forward;
    forward only;
    forwarders { 192.168.56.102; };
};

```

```

root@srv1:~# cat /etc/bind/named.conf.local
zone "lab.test" {
    type master;
    file "/etc/bind/zones/db.lab.test";
};
zone "my.lab.test" {
    type forward;
    forward only;
    forwarders { 192.168.56.102; };
};
root@srv1:~# _

```

Рисунок 15 – File named.conf.local на SRV1

```

root@client:~# dig @192.168.56.101 my.lab.test

; <<>> DiG 9.18.30-Ubuntu0.20.04.2-Ubuntu <<>> @192.168.56.101 my.lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14869
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4444e947df26719201000000680d19ade1175dd8b2df978a (good)
;; QUESTION SECTION:
;my.lab.test.                IN      A

;; ANSWER SECTION:
my.lab.test.                 604800  IN      A      192.168.56.102

;; Query time: 43 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sat Apr 26 17:36:45 UTC 2025
;; MSG SIZE rcvd: 84

```

Рисунок 16 – Тестирование разрешения DNS На CLIENT

```

root@client:~# dig @192.168.56.102 my.lab.test

; <<>> DiG 9.18.30-Ubuntu0.20.04.2-Ubuntu <<>> @192.168.56.102 my.lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10041
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f7333be32a5b26e601000000680d1b439bedbcc8a8f2dde2 (good)
;; QUESTION SECTION:
;my.lab.test.                IN      A

;; ANSWER SECTION:
my.lab.test.                604800  IN      A      192.168.56.102

;; Query time: 0 msec
;; SERVER: 192.168.56.102#53(192.168.56.102) (UDP)
;; WHEN: Sat Apr 26 17:43:31 UTC 2025
;; MSG SIZE rcvd: 84

```

Рисунок 17 – Тестирование разрешения DNS На CLIENT

6. Настройка DNSSEC на SRV2

- Настройка DNSSEC для зоны my.lab.test на SRV2
- Создание каталога для хранения ключей

```
sudo mkdir /etc/bind/keys
```

```
cd /etc/bind/keys
```

- Создание KSK (Key Signing Key):

```
sudo dnssec-keygen -f KSK -a RSASHA256 -b 2048 -n ZONE my.lab.test
```

-f KSK : тип ключа KSK (ключ подписи)

-a RSASHA256 : алгоритм шифрования лучше, чем RSASHA1

-b 2048 : длина ключа 2048 бит

-n ZONE : используется для зоны my.lab.test

```

root@srv2:/etc/bind/keys# dnssec-keygen -f KSK -a RSASHA256 -b 2048 -n ZONE my.lab.test
Generating key pair.....+++++
.....+++++
(Kmy.lab.test.+008+20836
root@srv2:/etc/bind/keys# ls
Kmy.lab.test.+008+20836.key  Kmy.lab.test.+008+20836.private

```

Рисунок 18 – Создание KSK (Key Signing Key)

- Создание ZSK (Zone Signing Key):

`sudo dnssec-keygen -a RSASHA256 -b 2048 -n ZONE my.lab.test`

```
root@srv2:/etc/bind/keys# dnssec-keygen -a RSASHA256 -b 2048 -n ZONE my.lab.test
Generating key pair.....
.+++++ .....
.....+++++
Kmy.lab.test.+008+48724
root@srv2:/etc/bind/keys# ls
Kmy.lab.test.+008+20836.key      Kmy.lab.test.+008+48724.key
Kmy.lab.test.+008+20836.private  Kmy.lab.test.+008+48724.private
root@srv2:/etc/bind/keys#
```

Рисунок 19 – Создание ZSK (Zone Signing Key)

- Вставка публичных ключей в файл зоны db.my.lab.test:
- На сервере SRV2 выполните:

`sudo cat /etc/bind/keys/Kmy.lab.test.*.key >> /etc/bind/zones/db.my.lab.test`

→ Вставьте оба публичных ключа в файл зоны.

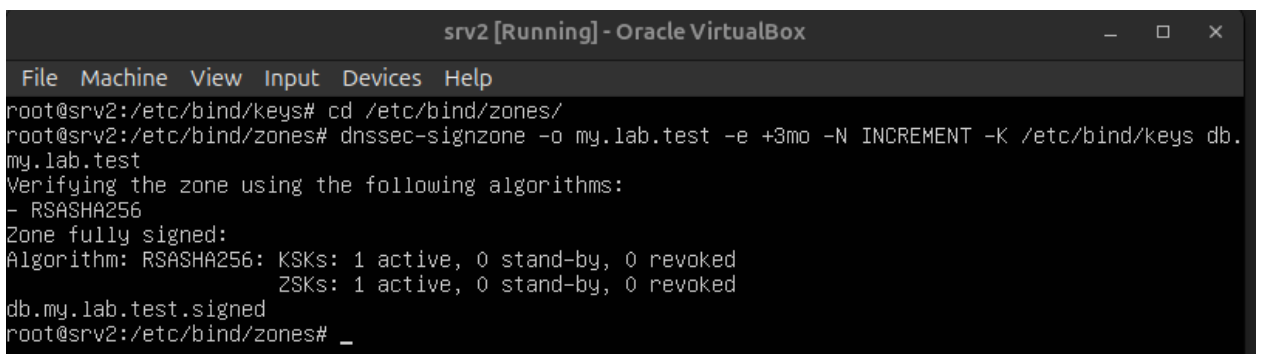
```
root@srv2:/etc/bind/keys# cat /etc/bind/keys/Kmy.lab.test.*.key >> /etc/bind/zones/db.my.lab.test
root@srv2:/etc/bind/keys# cat /etc/bind/zones/db.my.lab.test
$TTL      604800
@         IN      SOA      srv2.my.lab.test. admin.my.lab.test. (
4
604800
86400
2419200
604800 )
;
@         IN      NS       srv2.my.lab.test.
@         IN      A        192.168.56.102
srv2      IN      A        192.168.56.102
; This is a key-signing key, keyid 20836, for my.lab.test.
; Created: 20250426205505 (Sat Apr 26 20:55:05 2025)
; Publish: 20250426205505 (Sat Apr 26 20:55:05 2025)
; Activate: 20250426205505 (Sat Apr 26 20:55:05 2025)
my.lab.test. IN DNSKEY 257 3 8 AwEAAZ6x0wFOXbg1LPAhSWDvmAhwj4xSABw2sWxo50eRycErbrvpH0F0 wa0TidYcuNm8
J0rKtX17xGF2SLAQmZsm/7j40pk5F1NnxIhoHgoU621U K7roJyYVspDEhBtDIKo72mYgluz4PubcfyPfU4Q1V9RNxgkh2Wi+hg1
6 7E6i2UzTPsmZm3RW5E0Mb4fGfVPziHZMT3ogy0Ix0BvhcfjzfmYjUDI1 KyIWbF/Bn503KbKxeBmuTG0cdtp/IwYhsJnF/icXF
YVKQ10VT/6QK4NH DP2VWh7tEjSgU/tBNQp1mUX8RWTin1W1u+XSKuZIRrbY+N+KM0Vy12eb e9SqN2CfM+E=
; This is a zone-signing key, keyid 48724, for my.lab.test.
; Created: 20250426205738 (Sat Apr 26 20:57:38 2025)
; Publish: 20250426205738 (Sat Apr 26 20:57:38 2025)
; Activate: 20250426205738 (Sat Apr 26 20:57:38 2025)
my.lab.test. IN DNSKEY 256 3 8 AwEAAAd4pGFAwb0R3uNJh0d19ydW6XIzEI0t6JAeN7HPiOj12GHoECyeg DFMjWs1oRDDE
E0F+VMjdT23oWig1J5Fp0JvvB1SoRTLcVmlQcJz+Ruwv n9fVUX7Ne6ehESVP1VTuq8gIJEvApd7bdRJ7I4tuTMADkKtSEr1QNj+
s LhIDIJjfmPspjGABQCN221Zg2QrwTHa7N6/Z/bEcudBM1Wb2bXq4nv2r+ gLK4RpkCCoG8c0WpSNy02yNp+3dyfBULwtZem011u
oSFoU1PXkqYViyF Bf1N08gho02y6UNnG36cHCDdAZYangmef7PBhbS86E7/pDk68CdM/EvQ Yj5IWY+Puvs=
root@srv2:/etc/bind/keys#
```

Рисунок 20 – Вставка публичных ключей в файл зоны db.my.lab.test

- Подпись зоны my.lab.test

`cd /etc/bind/zones`

`sudo dnssec-signzone -o my.lab.test -e +3mo -N INCREMENT -K /etc/bind/keys
db.my.lab.test`



```
srv2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@srv2:/etc/bind/keys# cd /etc/bind/zones/
root@srv2:/etc/bind/zones# dnstsec-signzone -o my.lab.test -e +3mo -N INCREMENT -K /etc/bind/keys db.
my.lab.test
Verifying the zone using the following algorithms:
- RSASHA256
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                        ZSKs: 1 active, 0 stand-by, 0 revoked
db.my.lab.test.signed
root@srv2:/etc/bind/zones# _
```

Рисунок 21 – Подпись зоны my.lab.test

- -o my.lab.test : имя зоны
- -e +3mo : подпись действительна в течение 3 месяцев
- -K /etc/bind/keys : каталог, содержащий ключи
- db.my.lab.test : имя файла зоны для подписи

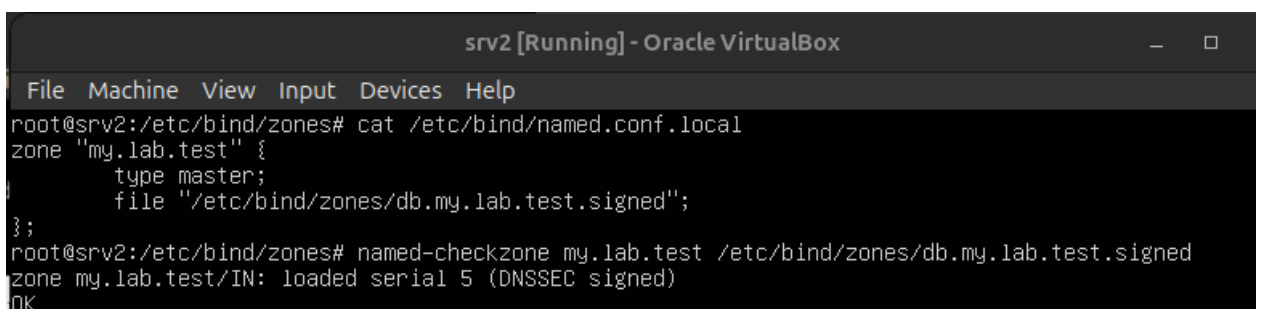
После выполнения этой команды будет создан новый файл: db.my.lab.test.signed

- Изменение named.conf.local на SRV2 для использования файла .signed

`sudo nano /etc/bind/named.conf.local`

- Измените объявление зоны:

```
zone "my.lab.test" {
    type master;
    file "/etc/bind/zones/db.my.lab.test.signed";
};
```



```
srv2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@srv2:/etc/bind/zones# cat /etc/bind/named.conf.local
zone "my.lab.test" {
    type master;
    file "/etc/bind/zones/db.my.lab.test.signed";
};
root@srv2:/etc/bind/zones# named-checkzone my.lab.test /etc/bind/zones/db.my.lab.test.signed
zone my.lab.test/IN: loaded serial 5 (DNSSEC signed)
OK
```

Рисунок 22 – Изменение file named.conf.local

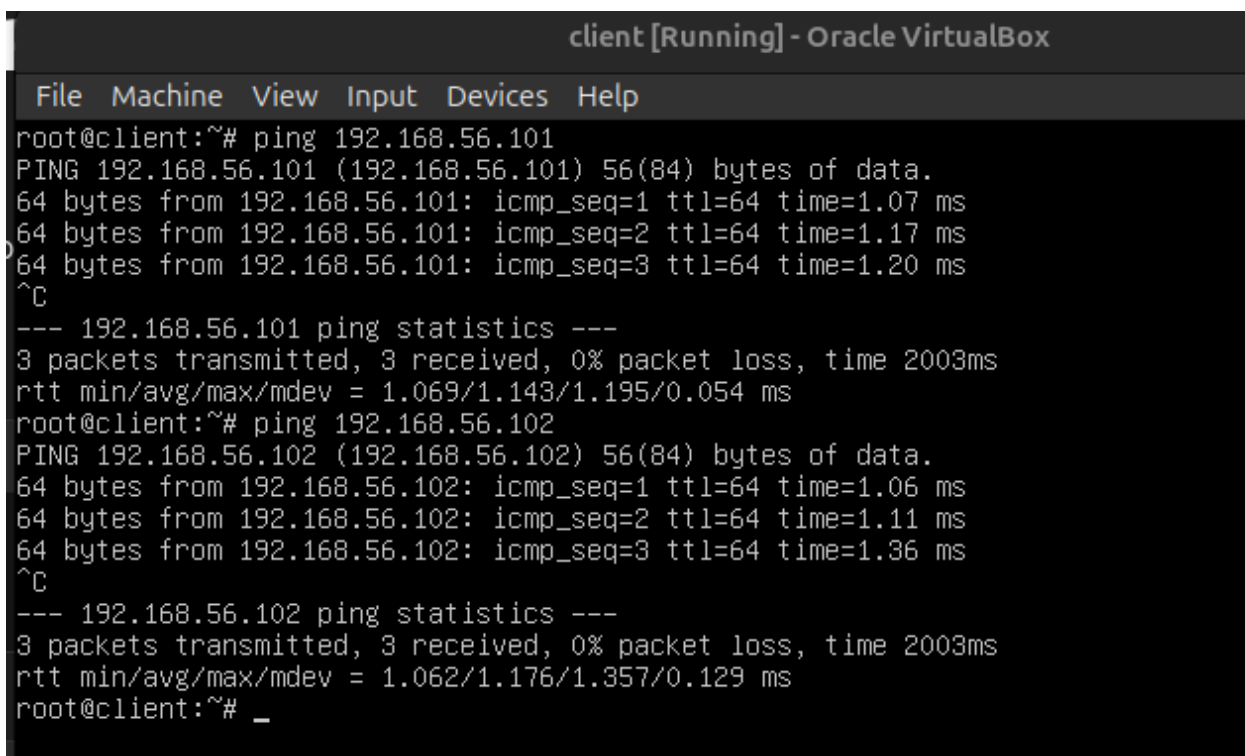
7. Проведение тестирования

7.1. Тест-кейс 1: Проверка ping между машинами (SRV1, SRV2, Клиент)

- На каждой машине (SRV1, SRV2, Клиент) поочерёдно отправляйте ping на IP-адреса двух других машин.

ping 192.168.56.101 # Ping SRV1

ping 192.168.56.102 # Ping SRV2



```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=1.17 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=1.20 ms
^C
--- 192.168.56.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.069/1.143/1.195/0.054 ms
root@client:~# ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.36 ms
^C
--- 192.168.56.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.062/1.176/1.357/0.129 ms
root@client:~# _
```

Рисунок 23 – Client

ping 192.168.56.102 # Ping SRV2

ping 192.168.56.1 # Ping Client

```
srv1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@srv1:~# ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.28 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.665 ms
^C
--- 192.168.56.102 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.665/0.973/1.281/0.308 ms
root@srv1:~# ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
64 bytes from 192.168.56.1: icmp_seq=1 ttl=64 time=1.20 ms
64 bytes from 192.168.56.1: icmp_seq=2 ttl=64 time=1.25 ms
^C
--- 192.168.56.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.196/1.221/1.247/0.025 ms
root@srv1:~# _
```

Рисунок 24 – SRV1

7.2. Тест-кейс 2: Проверка службы BIND на SRV1

`sudo systemctl status bind9.service`

```
srv1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

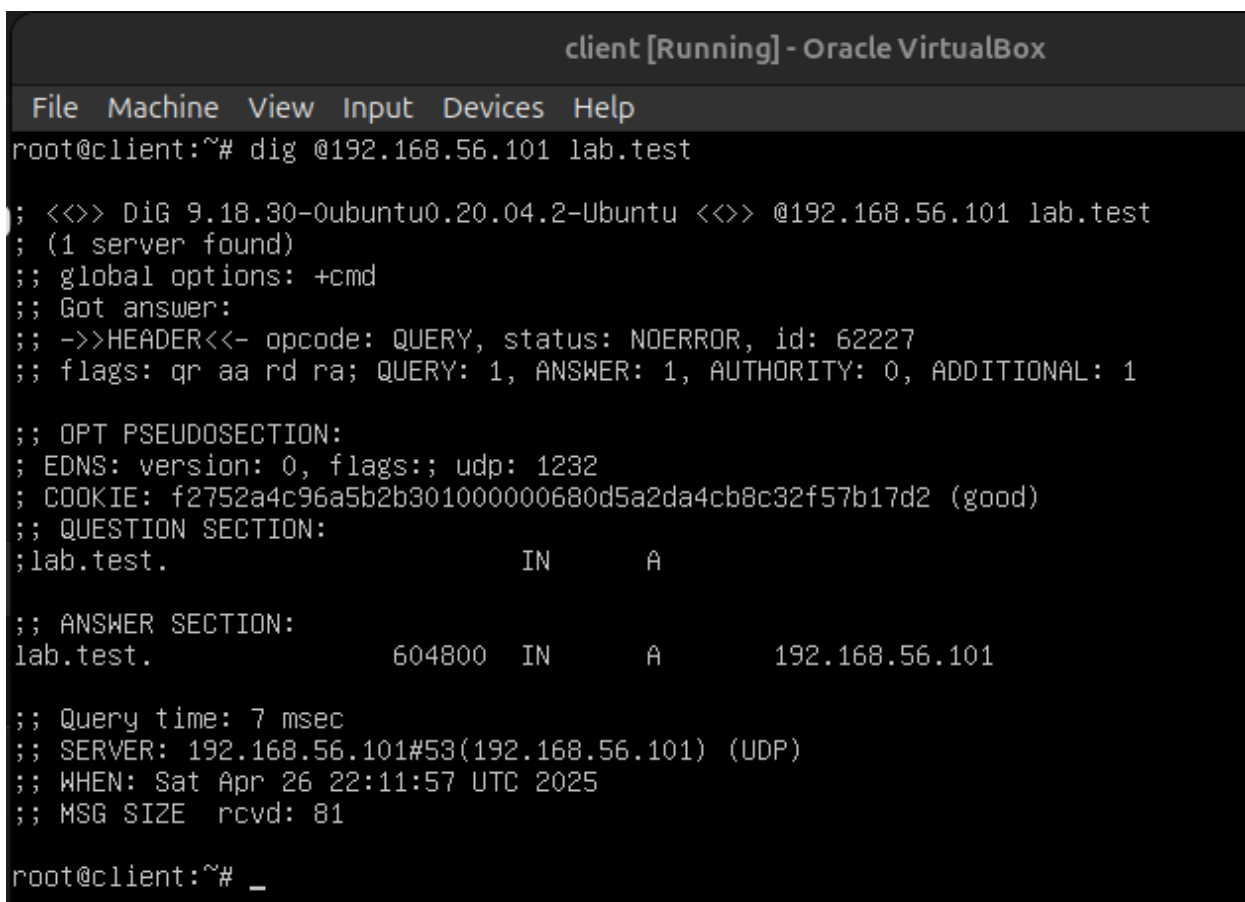
root@srv1:~# systemctl status bind9.service
• named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2025-04-26 17:36:35 UTC; 4h 32min ago
     Docs: man:named(8)
   Main PID: 3916 (named)
    Tasks: 4 (limit: 1046)
   Memory: 6.5M
   CGroup: /system.slice/named.service
           └─3916 /usr/sbin/named -f -u bind

Apr 26 17:36:35 srv1 named[3916]: managed-keys-zone: loaded serial 4
Apr 26 17:36:35 srv1 named[3916]: zone 0.in-addr.arpa/IN: loaded serial 1
Apr 26 17:36:35 srv1 named[3916]: zone 255.in-addr.arpa/IN: loaded serial 1
Apr 26 17:36:35 srv1 named[3916]: zone lab.test/IN: loaded serial 4
Apr 26 17:36:35 srv1 named[3916]: zone localhost/IN: loaded serial 2
Apr 26 17:36:35 srv1 named[3916]: zone 127.in-addr.arpa/IN: loaded serial 1
Apr 26 17:36:35 srv1 named[3916]: all zones loaded
Apr 26 17:36:35 srv1 named[3916]: running
Apr 26 20:43:10 srv1 named[3916]: resolver priming query complete: timed out
Apr 26 21:25:12 srv1 named[3916]: resolver priming query complete: timed out
root@srv1:~#
```

Рисунок 25 – Проверка службы BIND на SRV1

7.3. Тест-кейс 3: Проверка разрешения lab.test с Клиента

На Client выполните: `dig @192.168.56.101 lab.test`



```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# dig @192.168.56.101 lab.test

; <<>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <<>> @192.168.56.101 lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62227
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f2752a4c96a5b2b301000000680d5a2da4cb8c32f57b17d2 (good)
;; QUESTION SECTION:
;lab.test.                                IN      A

;; ANSWER SECTION:
lab.test.                                604800  IN      A      192.168.56.101

;; Query time: 7 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sat Apr 26 22:11:57 UTC 2025
;; MSG SIZE rcvd: 81

root@client:~# _
```

Рисунок 26 – Проверка разрешения lab.test с Клиента

-> В ответе есть раздел **ANSWER SECTION** с IP-адресом.

7.4. Тест-кейс 4: Проверка разрешения srv1.lab.test

На Клиенте выполните: `dig @192.168.56.101 srv1.lab.test`

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# dig @192.168.56.101 srv1.lab.test

; <<>> DiG 9.18.30-Oubuntu0.20.04.2-Ubuntu <<>> @192.168.56.101 srv1.lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23825
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: edf2bbe4878d320801000000680d5ac237c07b95d2d7d85d (good)
;; QUESTION SECTION:
;srv1.lab.test.                IN      A

;; ANSWER SECTION:
srv1.lab.test.                604800  IN      A      192.168.56.101

;; Query time: 0 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sat Apr 26 22:14:26 UTC 2025
;; MSG SIZE rcvd: 86
```

Рисунок 27 – Проверка разрешения srv1.lab.test

-> В ответе в разделе ANSWER домен srv1.lab.test имеет IP-адрес 192.168.56.101.

7.5. Тест-кейс 5: Проверка разрешения srv2.lab.test

На Клиенте выполните: `dig @192.168.56.101 srv2.lab.test`

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# dig @192.168.56.101 srv2.lab.test

; <>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <>> @192.168.56.101 srv2.lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4703
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e81da6b067bbabaf01000000680d5b69a77ff2f6efc44586 (good)
;; QUESTION SECTION:
;srv2.lab.test.                IN      A

;; ANSWER SECTION:
srv2.lab.test.                604800  IN      A      192.168.56.102

;; Query time: 0 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sat Apr 26 22:17:12 UTC 2025
;; MSG SIZE rcvd: 86
```

Рисунок 28 – Проверка разрешения srv2.lab.test

-> В ответе в разделе ANSWER домен srv2.lab.test имеет IP-адрес 192.168.56.102.

7.6. Тест-кейс 6: Проверка разрешения my.lab.test через SRV1

На Клиенте выполните: `dig @192.168.56.101 my.lab.test`

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# dig @192.168.56.101 my.lab.test

; <<>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <<>> @192.168.56.101 my.lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9235
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3bf0d2142a45ddb701000000680d5bfb2f1641f5f1203ff8 (good)
;; QUESTION SECTION:
;my.lab.test.                IN      A

;; ANSWER SECTION:
my.lab.test.                587826  IN      A      192.168.56.102

;; Query time: 11 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sat Apr 26 22:19:39 UTC 2025
;; MSG SIZE rcvd: 84
```

Рисунок 29 – Проверка разрешения my.lab.test

-> SRV1 пересылает запрос на SRV2 и получает в ответ IP-адрес **192.168.56.102**.

7.7. Тест-кейс 7: Проверка прямого разрешения my.lab.test на SRV2

На Клиенте выполните: **dig @192.168.56.102 my.lab.test**


```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# dig @192.168.56.102 my.lab.test

; <<>> DiG 9.18.30-Ubuntu0.20.04.2-Ubuntu <<>> @192.168.56.102 my.lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52747
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ffae9683cbd249ec01000000680df45820666607f00d99c3 (good)
;; QUESTION SECTION:
;my.lab.test.                IN      A

;; ANSWER SECTION:
my.lab.test.                604800  IN      A      192.168.56.102

;; Query time: 8 msec
;; SERVER: 192.168.56.102#53(192.168.56.102) (UDP)
;; WHEN: Sun Apr 27 09:09:44 UTC 2025
;; MSG SIZE rcvd: 84
```

Рисунок 30 – Проверка прямого разрешения my.lab.test на SRV2

-> SRV2 напрямую возвращает IP-адрес 192.168.56.102.

7.8. Тест-кейс 8: Проверка разрешения srv2.my.lab.test

На Клиенте выполните:

`dig @192.168.56.101 srv2.my.lab.test`

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# dig @192.168.56.101 srv2.my.lab.test

; <>> DiG 9.18.30-Ubuntu0.20.04.2-Ubuntu <>> @192.168.56.101 srv2.my.lab.test
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62640
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1232
; COOKIE: 05b28803d3bf8b5801000000680df528c0cf97024d7e7b3a (good)
;; QUESTION SECTION:
;srv2.my.lab.test.                IN      A

;; ANSWER SECTION:
srv2.my.lab.test.                604800  IN      A      192.168.56.102

;; Query time: 28 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sun Apr 27 09:13:12 UTC 2025
;; MSG SIZE rcvd: 89
```

Рисунок 31 – Проверка разрешения srv2.my.lab.test

В разделе ANSWER есть IP-адрес для srv2.my.lab.test.

7.9. Тест-кейс 9: Проверка разрешения с использованием DNSSEC

- На Клиенте выполните:

`dig @192.168.56.101 my.lab.test +dnssec`

`dig @192.168.56.102 my.lab.test +dnssec`

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# dig @192.168.56.101 my.lab.test +dnssec

; <<>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <<>> @192.168.56.101 my.lab.test +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6780
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: a330c641dda9438001000000680dfe644bb861e06aa8b38d (good)
;; QUESTION SECTION:
;my.lab.test.                IN      A

;; ANSWER SECTION:
my.lab.test.                546249  IN      A      192.168.56.102

;; Query time: 0 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Sun Apr 27 09:52:36 UTC 2025
;; MSG SIZE rcvd: 84
```

Рисунок 32 – Проверка разрешения с использованием DNSSEC

```
client [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@client:~# dig @192.168.56.102 my.lab.test +dnssec

; <<>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <<>> @192.168.56.102 my.lab.test +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25117
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: 6060da2ec098b68701000000680dfe9415cd94e7ee363563 (good)
;; QUESTION SECTION:
;my.lab.test.                IN      A

;; ANSWER SECTION:
my.lab.test.                604800  IN      A      192.168.56.102
my.lab.test.                604800  IN      RRSIG  A 8 3 604800 20250725200651 20250426200651 48724 my.
lab.test. PGY1TLE41Wx+NukBGH1fcmitpGhSiImCiXGiGSa/i+XNyoBN9GL67et0 15FoT04QdKef/o/COmhF9ONk4NhpiqNjQ
ulW6yjQBBsKZNi921CjtLit zhrG4fAM5pgTJvEmXXRSmtYHGgHodEOVAkyi40CPqgmKTbnf11o/AZE6 WxbgTdr2fAh/OVSkhtj
VpXVwe11iJuZcH0IPessubUGz24DPyqP/CoVtu 1Np8KziaaG47RrAlX4R1kyuIfU9gLR3qavXR/Zik3FhhQdEQTMeLv4Yp L+Tqs
8o0Mo0Y2Mvqmcvvs3BwLuYx1jsV4txPLIf0V05mxPMrdXTenK3/ zs0wLw==

;; Query time: 8 msec
;; SERVER: 192.168.56.102#53(192.168.56.102) (UDP)
;; WHEN: Sun Apr 27 09:53:24 UTC 2025
;; MSG SIZE rcvd: 383
```

Рисунок 33 – Проверка разрешения с использованием DNSSEC

ЗАКЛЮЧЕНИЕ

В ходе выполнения лабораторной работы была произведена настройка системы доменных имен DNS в тестовой среде с использованием виртуальных машин.

Было настроено доменное пространство lab.test на сервере SRV1, реализовано делегирование поддомена my.lab.test на сервер SRV2. Осуществлена проверка корректности разрешения имен с помощью утилит dig и nslookup.

На сервере SRV2 была проведена настройка механизма DNSSEC для зоны my.lab.test, включая генерацию ключей KSK и ZSK, подписание зоны и проверку цифровой подписи запросов DNS.

Результаты тестирования показали успешную работу механизма защиты DNS: имена разрешались корректно, а подписи RRSIG присутствовали в ответах сервера SRV2 при включении запроса DNSSEC.

Таким образом, были достигнуты все цели лабораторной работы: изучены принципы работы DNS, механизм делегирования поддоменов, а также способы защиты зоны с помощью технологии DNSSEC.