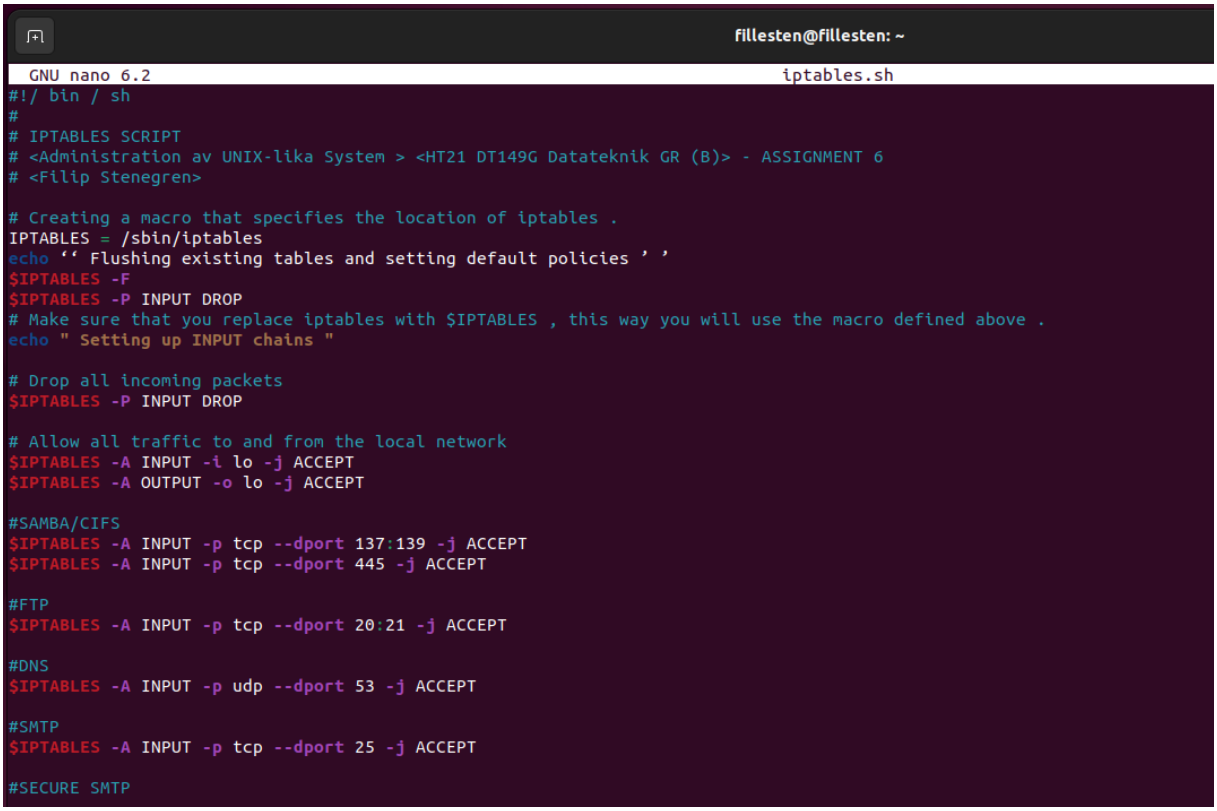
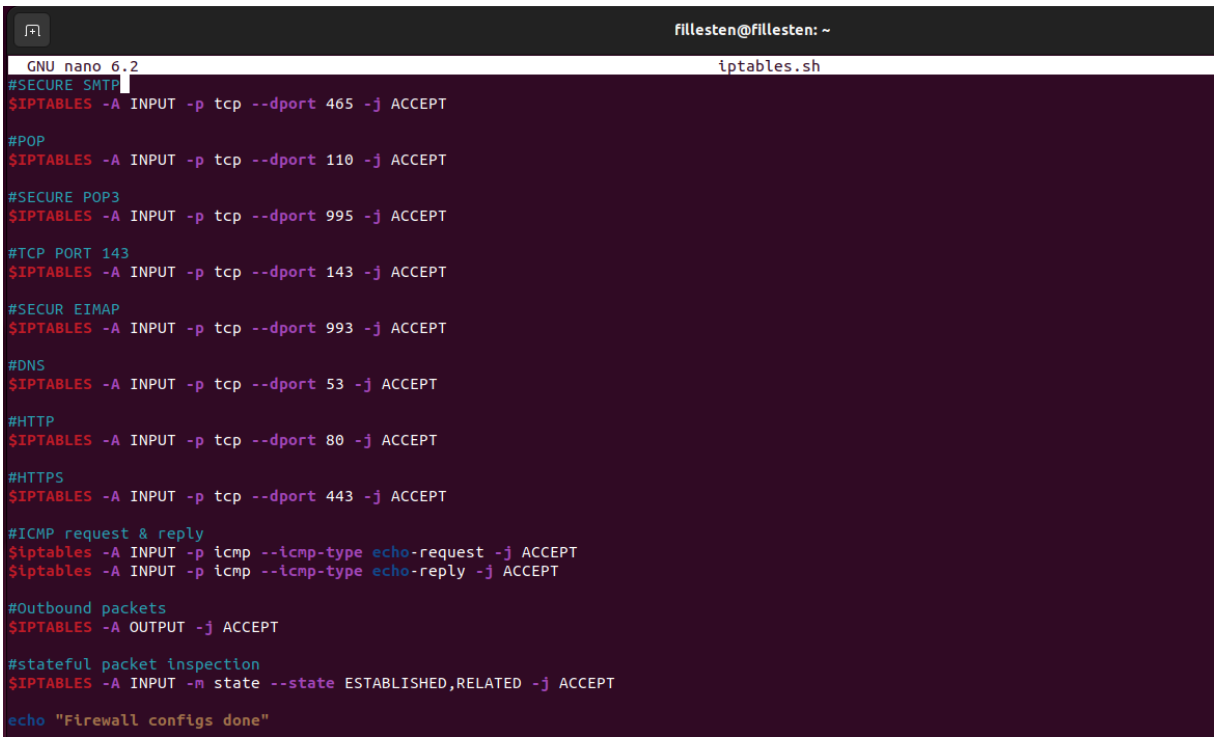
UNIX LAB 6

IPTABLES





Iptables.sh with the required policies.

4.2 securing dns

1. See 2.
2. Appending the following lines into named.conf.options (i initially had it in named.conf which meant I couldn't run the bind9-server later on)

```
dnssec-enable yes;
dnssec-validation yes;
```

3. Generating zsk and ksk

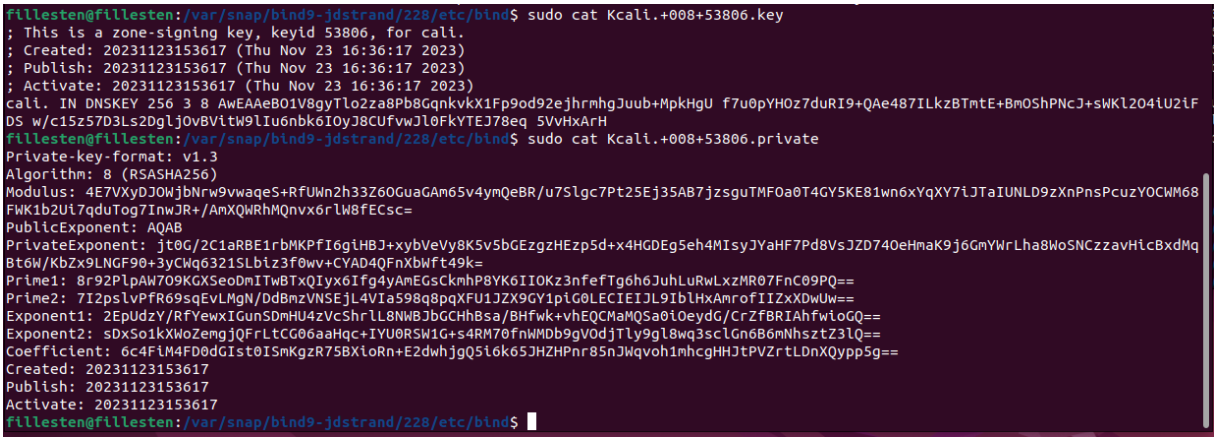
According to https://linux.die.net/man/8/dnssec-keygen RSA keys must be between 512 and 2048. And it also mentions that the default bit size for ZSK is 1024 and KSK 2048, which I picked. Seeing as it is the standard it probably is the ideal size for getting sufficient security with low resources needed.

4. Dnssec-keygen generates two pairs:

.key contains public key and a DNS KEY record.

.private contains the private key and data regarding algorithm.

ZSK pair:

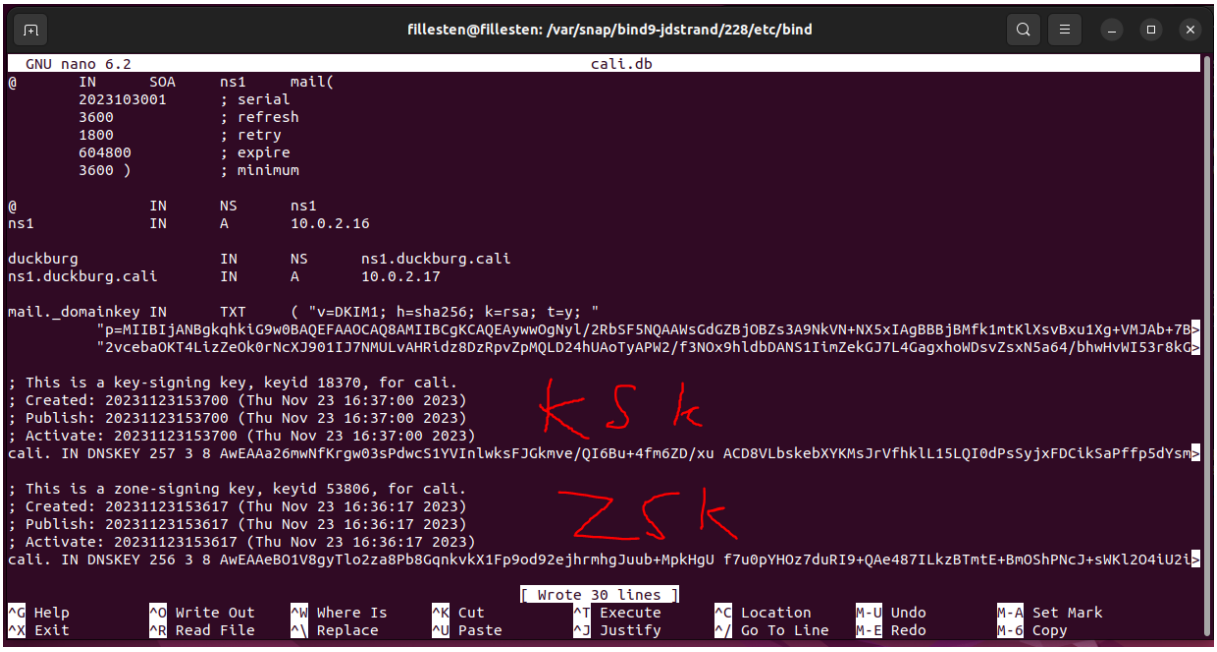


KSK pair:

```
fillesten@fillesten:/var/snap/bind9-jdstrand/228/etc/bind$ sudo cat Kcali.+008+18370.private
Private-key-format: v1.3
Algorithm: 8 (RSASHA256)
Modulus: rbqbA18quDDTew93BxLVhUieXCSwUkaSa979AjoG77h+bpkP/G4AIPxUtuyR5tdgoywmtV+GSUvXktAjR0+xLKPEUMKKRJo99+nl1iyZ7nJoKNhfV3amSktvoA+9WC
3fbCg476/xxAK1s5Ps6x+r2VBZiPNRCJIbiYpR/RWHesMYs0+vUUh9rUvkkuYimSpsAUPPHVaqoF9D+9UulLesFQ95baDDVp5gaNuMf0bRiUP0y8KH2D4zwwk0pZDhsd+iTkLPm
KrrmHBWynrxqtdgn1yPV9uCyoCCinTHVW31dQMudSY897Iew73OW8eftsW86RaeSVnp3mt++j79bZIJ/w==
PublicExponent: AQAB
PrivateExponent: MITADBYE+UHxnhm4lUomRb39NCCu+ZtqAyRYpsmL7GErNjobI9WYxZ2TDy9MpBqci5WmDdtqxoee4gqs/5p7Ect+5UsfkH8/NUCmhsUYDGb5PgcHwYaKdI
9S0nHy4HCXSD6HgDE0JRjYpBl4/kVvGhb9mmjRxcIAXM47jaH4n0jtZ39ALmFRQa3MDd44io/4feBFysgfWU2PpHwqiT7Ho8dNjHSXbwDYT1LmgwRe4Rx8O+Bl4FS3+J8Wbo/B6
LNm6UJveRCOC7WGIC+F0gbuva1lq7JJd6AsRHULLr22kD+y14Luh/f/r39u4uDlkP56UTnM1b8RLOfkk8ePjO5gaQ==
Prime1: 3eHSNttKOXXtTwux3kg9RX2Vv1Fr6ND2W9DUAas6z7eXpQKTEq3Og+xMXLdmjonb3uP/5jXyM0AHDysEIDO2wtHiy9gcBZaIBcrvZXBsoxPFD3syrspGg94WHWZFCAt
HpKV8tqpqP+79zTPQbrDAQKzdtBVPbFmKjuZaCIjajF0=
Prime2: yHFHp2fcD1UTnmLuvzFoMP4cB8gHpuTIaM3B5iIaD0+mYx1a3uQyJ+3LGCTuhAP2D36K+0BE66ODSRuiBex4ElGK7gmnGBOQl/igZudd7ohNj3vfH1zk29n2Wv7wPBb
USyzqS/p4uyhnPTJuRMnSW/jN7dw0k97Md+hr6RFV6gs=
Exponent1: RXV//TRA1CQamfgrQk6S/8IEstOmWEeyF6QT+kHEM2phyoI30E0grSO38/5l2JFHh0sQvNx+aZTNoO3yaLJHsE1MFkwc2ZL6GfYhYzwChjqWIfaLMzSXRoirm6B8
U7xUPTKhC/3lLQZ/5VEnGr+yL4zuCoXxSxXszjdGUA2nfPE=
Exponent2: elkC9sEjhsxUbFJRDq0WvwjsjSdg3FM7rRUi7NkV9RCWLFunsvOxVcQFOtiYKkbMtAp2xQQmzXqCUWankFwVsoDJf6CuuLiAgvLE3esN3+KdDR78Q4WNQFEb2dFR
TCxXKwfgf74EYaE42xbkTeKvH2qQMEdAZJ4TSoG5FIt7WJ8=
Coefficient: iqn8Fns7iX/Cf3EVdE+ll1cvaSpTC1U5vX5KBxY337sg1ulFZhfuZW/aI/BFWLCMSb/Y850MfAhSEpOn1ICbRVv4wuf1V3kYjdDTg0rvtVY3hqCWD5TH7wvvkk
+MDrC6k94RH5F30CRBFXGdEypNFwa3Kp3sFfTRwxuqGeTf1ik=
Created: 20231123153700
Publish: 20231123153700
Activate: 20231123153700
fillesten@fillesten:/var/snap/bind9-jdstrand/228/etc/bind$
```

5. Include KSK AND ZSK. HOWEVER I used cat instead.

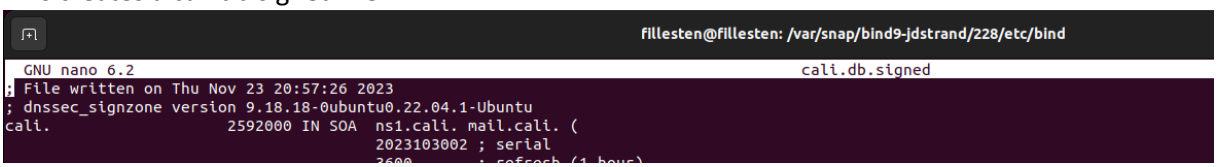
cat Kcali.+008+18370.key >> cali.db
cat Kcali.+008+53806.key >> cali.db



6. Signing the zone following using commands from this guide (https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server-2)

```
fillesten@fillesten:/var/snap/bind9-jdstrand/228/etc/bind$ sudo dnssec-signzone -A -3 $(head -c 1000 /dev/random | sha1sum | cut -b 1-16) -N INCREMENT -o cali. -t cali.db
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
cali.db.signed
Signatures generated:                       15
Signatures retained:                         0
Signatures dropped:                          0
Signatures successfully verified:            0
Signatures unsuccessfully verified:          0
Signing time in seconds:                 0.020
Signatures per second:                 749.662
Runtime in seconds:                      0.032
```

This creates a cali.db.signed file



7. What must be added to parent zone to ensure a chain of trust?

To make sure that the chain of trust is validated the parent zone needs to acquire a DS record. DNSSEC has a DS record which transfers the trust from the parent zone to the child zone. The DS record is a hashed DNSKEY record which contains the KSK. This continues until the root parent has received a DS from their child zone.

8. When is it necessary to enable the the dnssec-lookaside option?

if the parent is not signed or doesn't publis DS's unlike the child zone the lookaside option is enabled to still validate the child.

"DNSSEC Lookaside Validation (DLV) is a mechanism for publishing DNS Security (DNSSEC) trust anchors outside of the DNS delegation chain. It allows validating resolvers to validate DNSSEC-signed data from zones whose ancestors either aren't signed or don't publish Delegation Signer (DS) records for their children." - https://www.rfc-editor.org/rfc/rfc5074

9. present key rollover for ZSK and KSK and how to achieve it in a secure manner for both.

ZSK rollover is relatively straightforward and does not involve your parent zone or any trust anchor issues. The only tricky part is the timing. Keys have an expiration time, so rollover must occur well before that time. However, keys also have a TTL, defined in the zone file. To illustrate, assume that the TTL is one day and that keys don't expire for another week." (Unix and Linux System Administration handbook 5th edition, page 565)

It also describes the steps to solve it, these are the steps:

- Generate a new ZSK.
- Include it in the zone file.
- Sign or re-sign the zone with the KSK and the *old* ZSK.
- Signal the name server to reload the zone; the new key is now there.
- Wait 24 hours (the TTL); now everyone has both the old and new keys.
- Sign the zone again with the KSK and the *new* ZSK.
- Signal the name server to reload the zone.
- Wait another 24 hours; now everyone has the new signed zone.
- Remove the old ZSK at your leisure, e.g., the next time the zone changes.

However, regarding KSK it utilizes a mechanism called double signing. It includes communicating the DS record to the parent, with a positive acknowledgement from the parent beforehand.
the steps for KSK rollover are

- Create a new KSK.
- Include it in the zone file.
- Sign the zone with both old and new KSKs and the ZSK.
- Signal the name server to reload the zone.
- Wait 24 hours (the TTL); now everyone has the new key.
- After confirmation, delete the old KSK record from the zone.
- Re-sign the zone with the new KSK and ZSK.