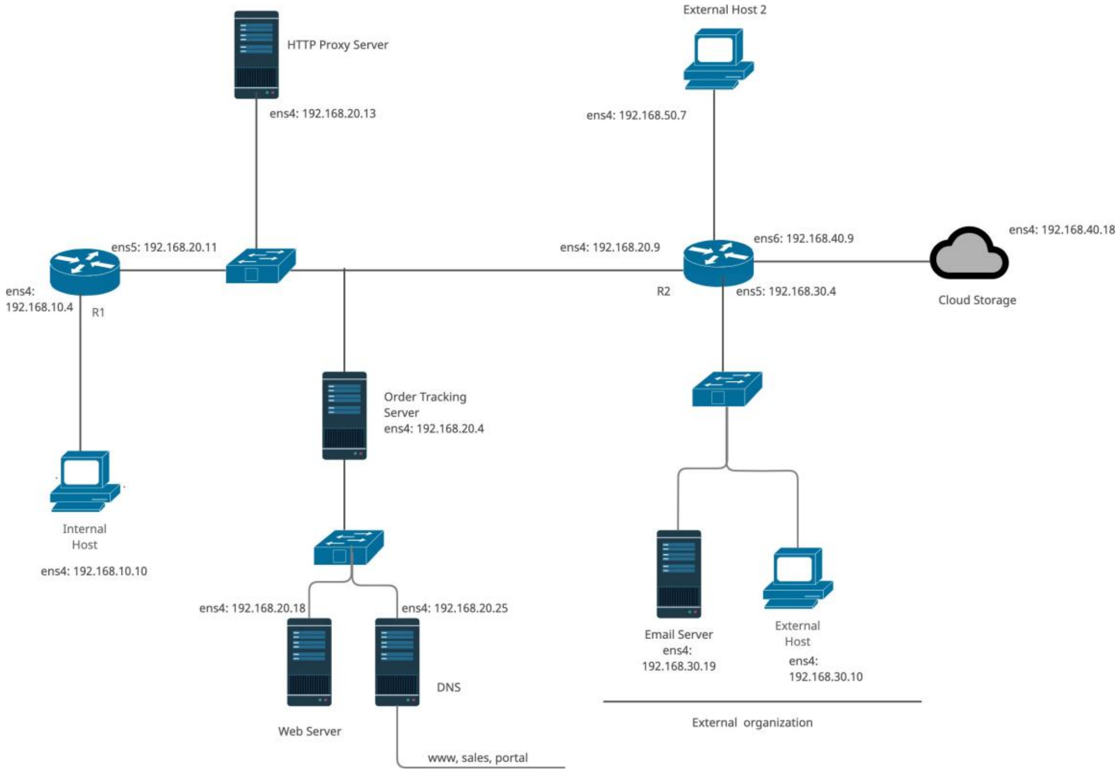
Network Security - A firewall's design and execution

CONTENTS

S.NO	Table of Contents	Pg.No
1	Topology	3
2	Networks and Instances Used	4
3	VPN	5
4	Web Server access using Netcat	9
5	Email Server	11
6	HTTP Proxy Server	17
7	DNS (Domain Name System)	20
8	Order Tracking Server	24
9	Additional Security Mechanism (Zeek IDS)	26

1. TOPOLOGY:



DESIGN RATIONALE :

By implementing this network diagram, the internal organization, which, in this case, the LAN users will be able to browse anything outside the organization and also establish connection to the email server. According to the topology , when LAN access a website it goes through the proxy server and the IP address is resolved into the domain name by the DNS server. Only www, sales and portal will be accessed by the external users and the addresses are resolved to names by Name server. The order tracking server essentially shows the data traffic between internal and external network while blocking few networks and allowing only networks which is required. We have established VPN connection between the internal and external clients. Zeek which is an intrusion Detection System is placed in Router 1 which acts as a firewall and also a network analyzer. This will monitor the network traffic and alerts the user when there is a malicious traffic. This acts as a security mechanism for detecting intrusion .

2. Networks and Instances Used:

Instance	IP address	Networks	Interface
LAN (Internal Host)	192.168.10.10	Network 1	ens4
Router 1	192.168.10.4, 192.168.20.11	Network 1 Network 2	ens4 ens5
HTTP Proxy Server	192.168.20.13	Network 2	ens4
Order Tracking Server	192.168.20.4	Network 2	ens4
Web Server	192.168.20.18	Network 2	ens4
DNS	192.168.30.18	Network 2	ens4
Router 2	192.168.20.9, 192.168.30.4, 192.168.40.9, 192.168.50.15	Network 2, Network 3, Network 4, Network 5	ens4, ens5, ens6, ens7
Email Server	192.168.30.19	Network 3	ens4
External Host	192.168.30.10	Network 3	ens4
Cloud Storage	192.168.40.18	Network 4	ens4
External Host	192.168.50.7	Network 5	ens5

- Number of Networks : 5
- Routers : 2
- Server: 4
- Internal Host: 1
- External Host : 2
- DNS : 1

3. VPN :

- VPN - Virtual Private Network used for tunnelling between Router 1 and Router 2.
- Implementation is done using IPsec-based VPN with Strongswan.
- Strongswan is an open-source, cross-platform.
    - VPN connection process:

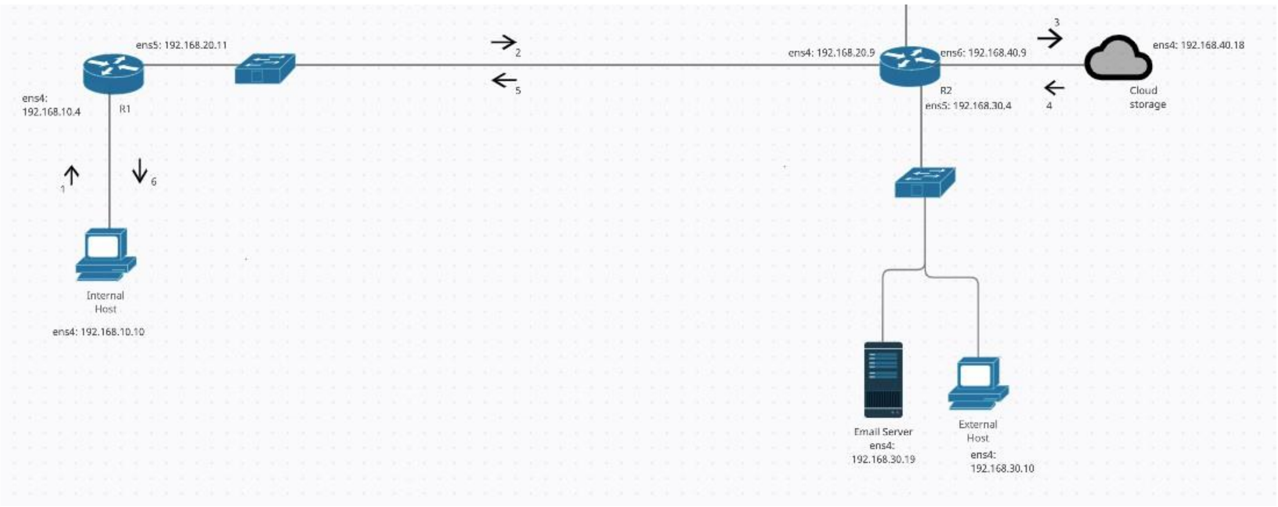


Figure 1 : VPN Flow (Internal to External)

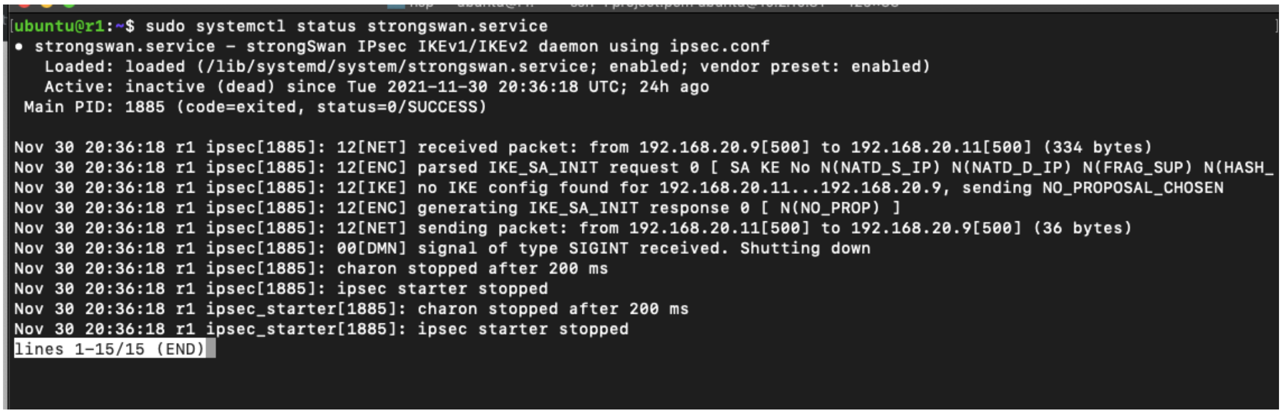
STEPS FOLLOWED:

3.1 Testing Environment :

- Site 1 Router 1 (Internal to External)
    - OS : Ubuntu 18.04
    - Public IP: 192.168.20.11 (ens5)
    - Private IP: 192.168.10.10 (ens4)
    - Private Subnet: 192.168.10.0/24
- Site 2 Router 2 (External to Internal)
    - OS : Ubuntu 18.04
    - Public IP: 192.168.20.9 (ens4)
    - Private IP: 192.168.40.18 (ens4)
    - Private Subnet: 192.168.40.0/24

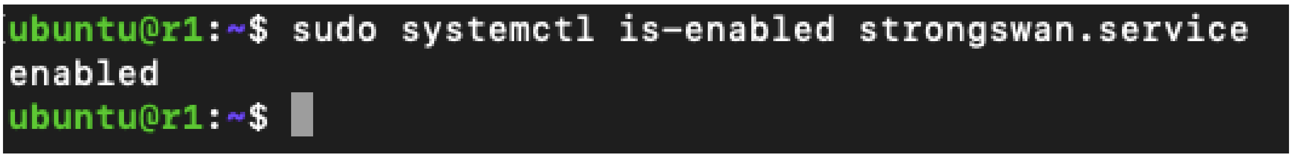
3.2 Installing StrongSwan in Ubuntu:

- Update the packages - $ sudo apt update.
- Install StrongSwan - $ sudo apt install strongswan
- After Installation, checking the status and service
  - $ sudo systemctl status strongswan.service



```
ubuntu@r1:~$ sudo systemctl status strongswan.service
● strongswan.service - strongSwan IPsec IKEv1/IKEv2 daemon using ipsec.conf
   Loaded: loaded (/lib/systemd/system/strongswan.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Tue 2021-11-30 20:36:18 UTC; 24h ago
 Main PID: 1885 (code=exited, status=0/SUCCESS)

Nov 30 20:36:18 r1 ipsec[1885]: 12[NET] received packet: from 192.168.20.9[500] to 192.168.20.11[500] (334 bytes)
Nov 30 20:36:18 r1 ipsec[1885]: 12[ENC] parsed IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP) N(HASH_
Nov 30 20:36:18 r1 ipsec[1885]: 12[IKE] no IKE config found for 192.168.20.11...192.168.20.9, sending NO_PROPOSAL_CHOSEN
Nov 30 20:36:18 r1 ipsec[1885]: 12[ENC] generating IKE_SA_INIT response 0 [ N(NO_PROP) ]
Nov 30 20:36:18 r1 ipsec[1885]: 12[NET] sending packet: from 192.168.20.11[500] to 192.168.20.9[500] (36 bytes)
Nov 30 20:36:18 r1 ipsec[1885]: 00[DMN] signal of type SIGINT received. Shutting down
Nov 30 20:36:18 r1 ipsec[1885]: charon stopped after 200 ms
Nov 30 20:36:18 r1 ipsec[1885]: ipsec starter stopped
Nov 30 20:36:18 r1 ipsec_starter[1885]: charon stopped after 200 ms
Nov 30 20:36:18 r1 ipsec_starter[1885]: ipsec starter stopped
lines 1-15/15 (END)
```

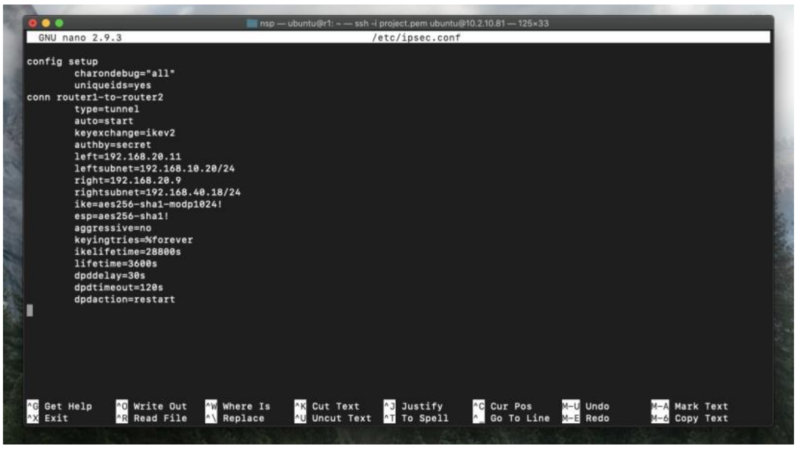
  - $ sudo systemctl is-enabled strongswan.service



```
ubuntu@r1:~$ sudo systemctl is-enabled strongswan.service
enabled
ubuntu@r1:~$ 
```

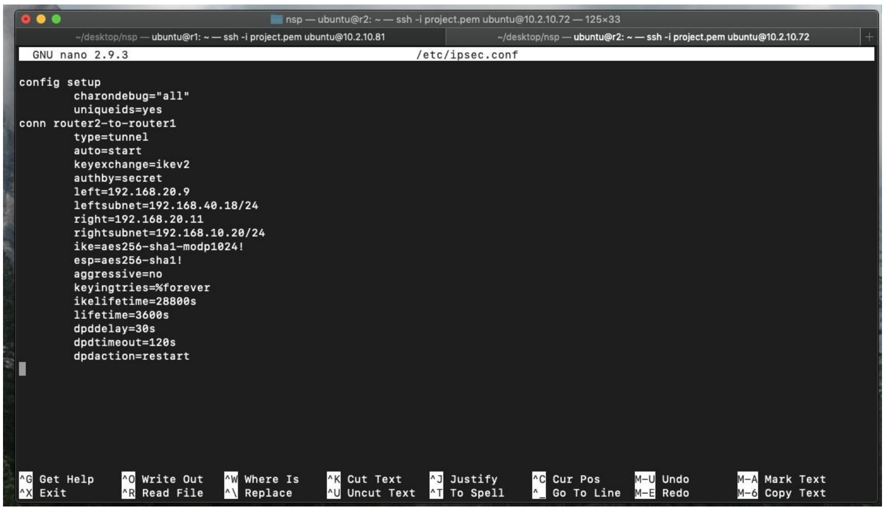
3.3 Configuring Security Gateways:

- Configure the security gateway using the /etc/ipsec.conf configuration file.
- Site 1 Gateway (Router 1 to Router 2)
  - $ sudo cp /etc/ipsec.conf /etc/ipsec.conf.orig
  - $ sudo nano /etc/ipsec.conf
  - Configuration file



```
config setup
        charondebug="all"
        uniqueids=yes
conn router1-to-router2
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left=192.168.20.11
        leftsubnet=192.168.10.20/24
        right=192.168.20.9
        rightsubnet=192.168.40.18/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart
```

- Site 2 Gateway (Router 2 to Router 1)
  - $ sudo cp /etc/ipsec.conf /etc/ipsec.conf.orig
  - $ sudo nano /etc/ipsec.conf
  - Configuration file

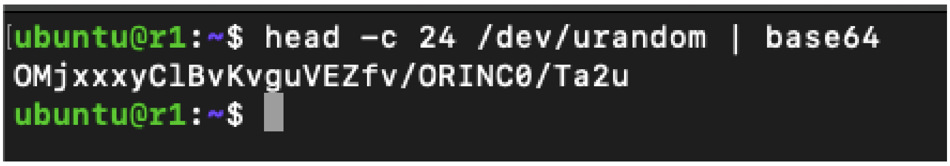


nsp — ubuntu@r2: ~ — ssh -i project.pem ubuntu@10.2.10.72 — 125×33
~/desktop/nsp — ubuntu@r1: ~ — ssh -i project.pem ubuntu@10.2.10.81
~/desktop/nsp — ubuntu@r2: ~ — ssh -i project.pem ubuntu@10.2.10.72
GNU nano 2.9.3
/etc/ipsec.conf

```
config setup
        charondebug="all"
        uniqueids=yes
conn router2-to-router1
        type=tunnel
        auto=start
        keyexchange=ikev2
        authby=secret
        left=192.168.20.9
        leftsubnet=192.168.40.18/24
        right=192.168.20.11
        rightsubnet=192.168.10.20/24
        ike=aes256-sha1-modp1024!
        esp=aes256-sha1!
        aggressive=no
        keyingtries=%forever
        ikelifetime=28800s
        lifetime=3600s
        dpddelay=30s
        dpdtimeout=120s
        dpdaction=restart
```

3.4 Configuring PSK for Peer-to-Peer Authentication

- Generate a secure PSK
  - $head -c 24 /dev/urandom | base 64

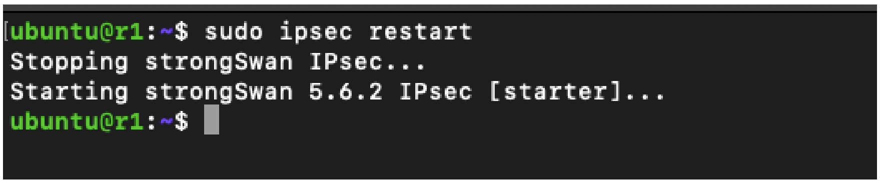


```
ubuntu@r1:~$ head -c 24 /dev/urandom | base64
OMjxxxyClBvKvguVEZfv/ORINC0/Ta2u
ubuntu@r1:~$
```

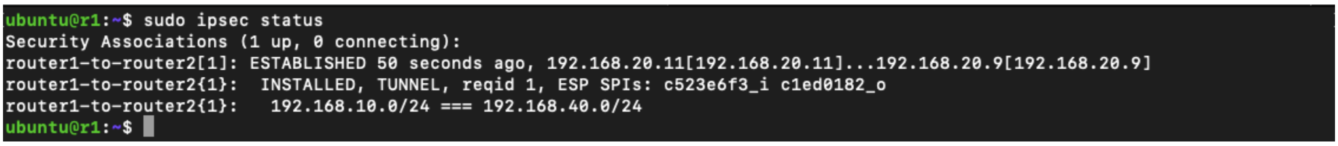
- Adding PSK in /etc/ipsec.secrets file on both gateways.
  - $ sudo vim /etc/ipsec.secrets
- Site 1 Gateway (Router 1 to Router 2) : 192.168.20.11 192.168.20.9 : PSK “OMjxxxyClBvKvguVEZfv/ORINC0/Ta2u”
- Site 2 Gateway (Router 2 to Router 1) : 192.168.20.9 192.168.20.11 : PSK “OMjxxxyClBvKvguVEZfv/ORINC0/Ta2u”

- Restart IPSec program and check its status
  - $ sudo ipsec restart
  - $ sudo ipsec status

- Router 1:

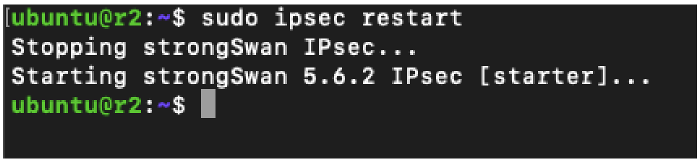


```
ubuntu@r1:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
ubuntu@r1:~$
```

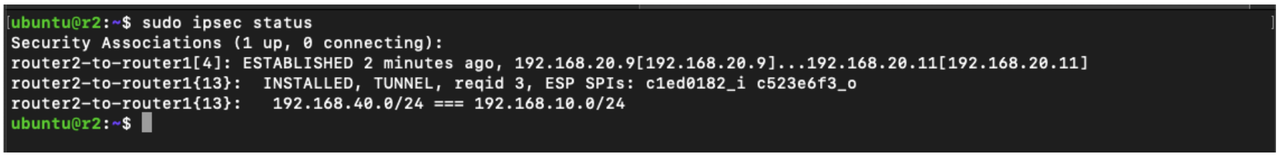


```
ubuntu@r1:~$ sudo ipsec status
Security Associations (1 up, 0 connecting):
router1-to-router2[1]: ESTABLISHED 50 seconds ago, 192.168.20.11[192.168.20.11]...192.168.20.9[192.168.20.9]
router1-to-router2{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c523e6f3_i c1ed0182_o
router1-to-router2{1}:   192.168.10.0/24 === 192.168.40.0/24
ubuntu@r1:~$
```

- Router 2:



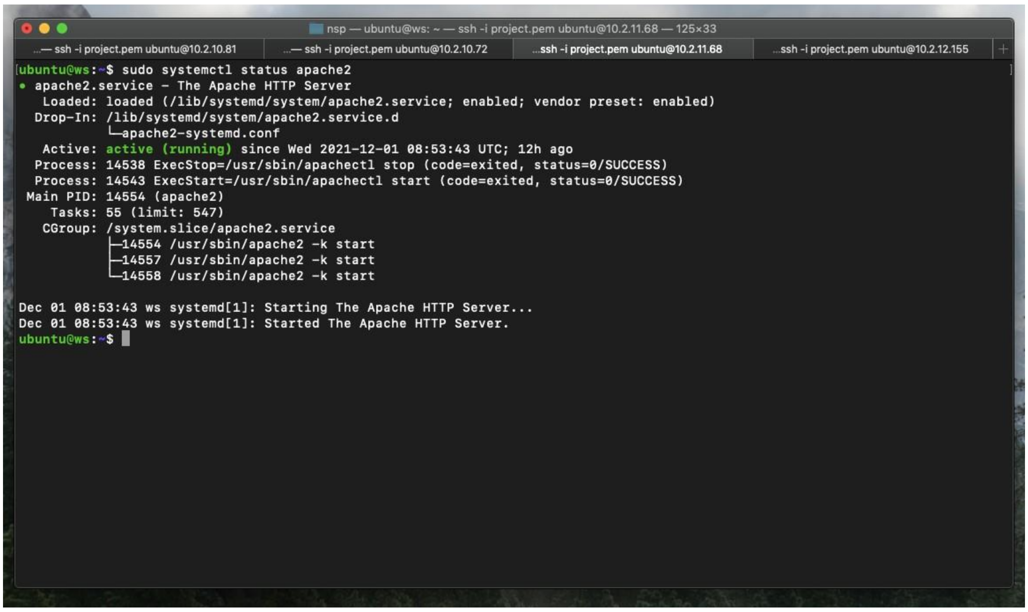
```
ubuntu@r2:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.6.2 IPsec [starter]...
ubuntu@r2:~$
```



```
ubuntu@r2:~$ sudo ipsec status
Security Associations (1 up, 0 connecting):
router2-to-router1[4]: ESTABLISHED 2 minutes ago, 192.168.20.9[192.168.20.9]...192.168.20.11[192.168.20.11]
router2-to-router1{13}:  INSTALLED, TUNNEL, reqid 3, ESP SPIs: c1ed0182_i c523e6f3_o
router2-to-router1{13}:   192.168.40.0/24 === 192.168.10.0/24
ubuntu@r2:~$
```

4. WEB SERVER ACCESS USING NETCAT:

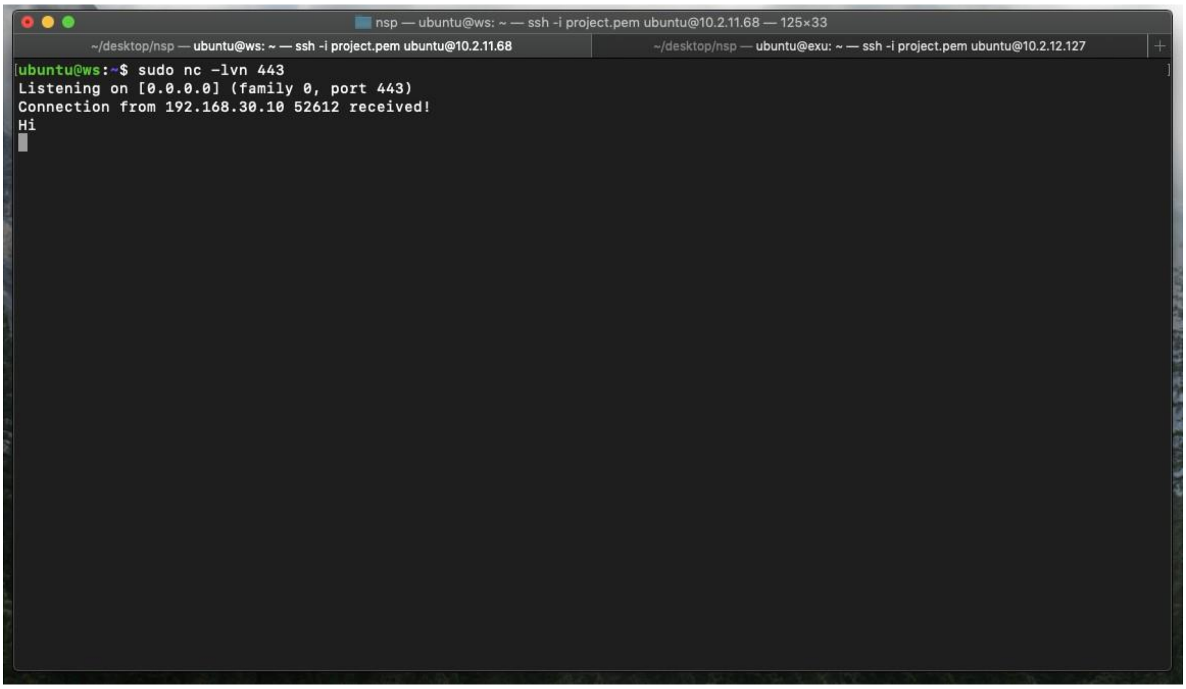
- Install Apache 2 for web server.
- HTTPS uses 443/TCP and HTTP uses 80/TCP
    - Group A -> Web Server - 443
    - Install : $ sudo apt -y install apache2
    - Status : $ sudo systemctl status apache2



nsp — ubuntu@ws: ~ — ssh -i project.pem ubuntu@10.2.11.68 — 125×33
...— ssh -i project.pem ubuntu@10.2.10.81
...— ssh -i project.pem ubuntu@10.2.10.72
...ssh -i project.pem ubuntu@10.2.11.68
...ssh -i project.pem ubuntu@10.2.12.155

```
ubuntu@ws:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Wed 2021-12-01 08:53:43 UTC; 12h ago
  Process: 14538 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
  Process: 14543 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 14554 (apache2)
    Tasks: 55 (limit: 547)
   CGroup: /system.slice/apache2.service
           ├─14554 /usr/sbin/apache2 -k start
           ├─14557 /usr/sbin/apache2 -k start
           └─14558 /usr/sbin/apache2 -k start

Dec 01 08:53:43 ws systemd[1]: Starting The Apache HTTP Server...
Dec 01 08:53:43 ws systemd[1]: Started The Apache HTTP Server.
ubuntu@ws:~$ 
```

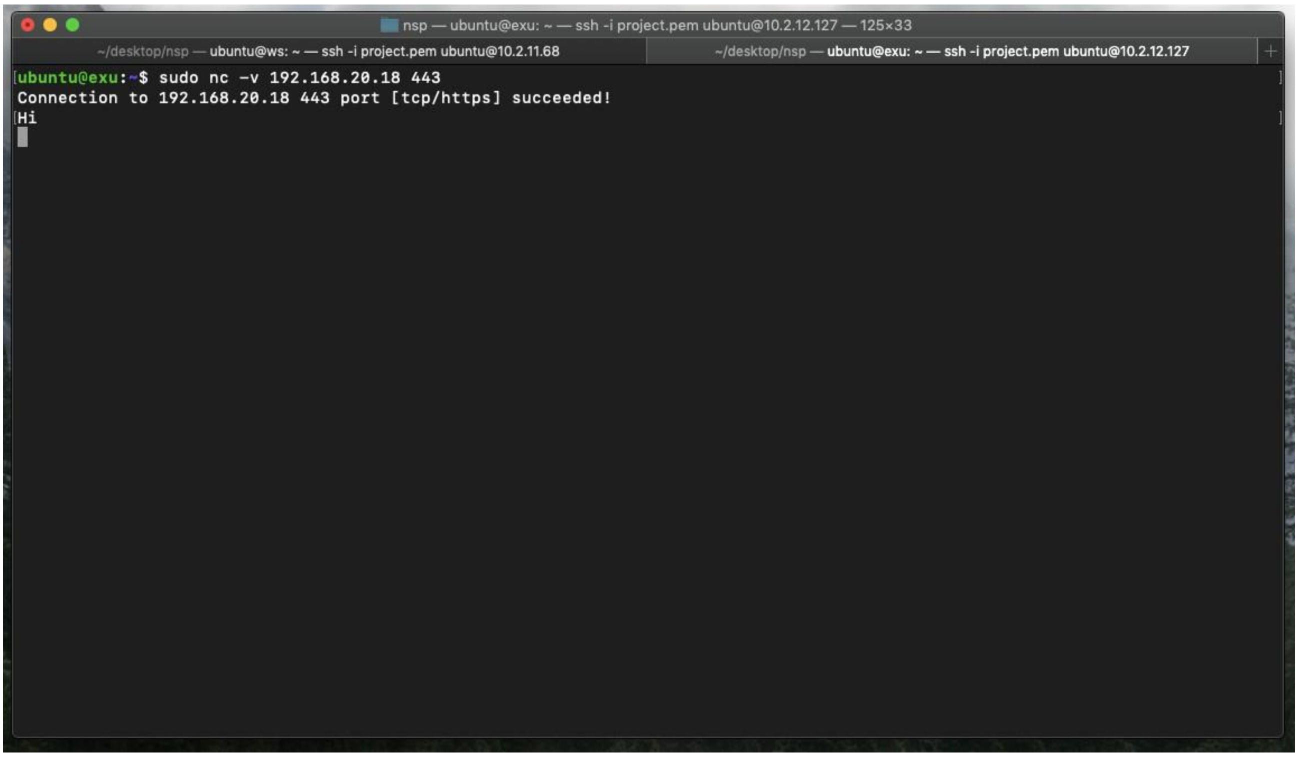
- By using Netcat we listening on port 443/TCP and making connection.
    - Web Server : $ sudo nc -lvn 443



nsp — ubuntu@ws: ~ — ssh -i project.pem ubuntu@10.2.11.68 — 125×33
~/desktop/nsp — ubuntu@ws: ~ — ssh -i project.pem ubuntu@10.2.11.68
~/desktop/nsp — ubuntu@exu: ~ — ssh -i project.pem ubuntu@10.2.12.127

```
ubuntu@ws:~$ sudo nc -lvn 443
Listening on [0.0.0.0] (family 0, port 443)
Connection from 192.168.30.10 52612 received!
Hi
```

- External User : $ sudo nc -v 192.168.30.10 443



nsp — ubuntu@exu: ~ — ssh -i project.pem ubuntu@10.2.12.127 — 125×33
~/desktop/nsp — ubuntu@ws: ~ — ssh -i project.pem ubuntu@10.2.11.68
~/desktop/nsp — ubuntu@exu: ~ — ssh -i project.pem ubuntu@10.2.12.127

```
ubuntu@exu:~$ sudo nc -v 192.168.20.18 443
Connection to 192.168.20.18 443 port [tcp/https] succeeded!
Hi
```

- By using Netcat, IP tables are written such that we can listen only on port 443/ TCP and establish connection and not via any other ports.

<u>IP Tables:</u>

- Allow SSH
  - $ sudo iptables -A INPUT -p tcp --sport 22 -j ACCEPT
  - $ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
- Allow TCP Traffic to particular port
  - $ sudo iptables -A INPUT -p tcp —sport 443 -j ACCEPT
  - $ sudo iptables -A INPUT -p tcp —dport 443 -j ACCEPT
- Allowing ICMP rules
  - $ sudo iptables -A INPUT -p ICMP -j ACCEPT
- Allowing Deny ALL (Default)
  - $ sudo iptables -A INPUT -j DROP

5. EMAIL SERVER:

- Here we install postfix Email Server.
- Install Dovecot for POP/IMAP server. POP uses 110/TCP and IMAP uses 143/ TCP.

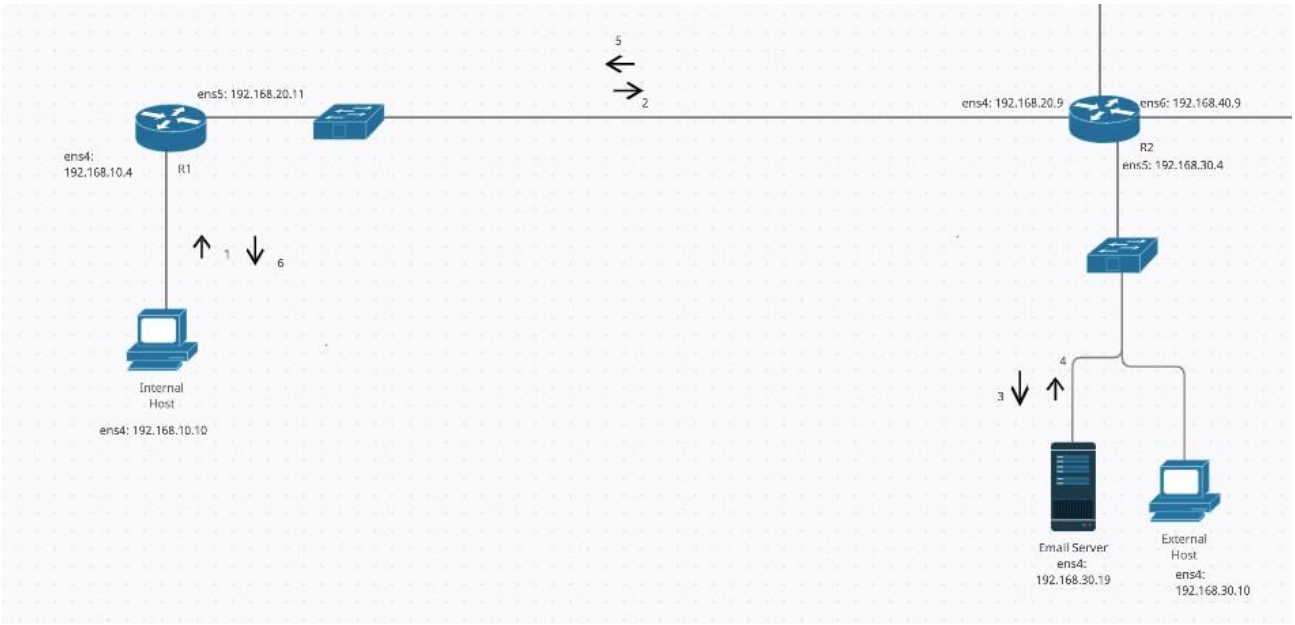


Figure 2 Internal Host to Email Server

Steps Followed on Email Server:

5.1 Get the mail server app in running to make all ports run:

- To on the email domain, (here, myclouda.net is the email domain name)
- Setup email trackers in the public IP: $hostname -f -> email.myclouda.net

5.2 Update Repositories:

Commands:

- $ sudo apt-get update
- $ sudo apt-get upgrade -y
- $ sudo apt-get dist-upgrade -y
- $ sudo apt-get install postfix -y

5.3 Package Reconfigure

- $sudo dpkg-reconfigure postfix
- Local Network:
- [Add LAN IP address – Eg:192.168.30.0/24]
- Mail box size limit (bytes)
- 0
- Local address extension characters:’
- +
- Internet protocols to use:
- Ipv4

5.4 Configure postfix:

$sudo nano /etc/postfix/main.cf

- home_mailbox = Maildir/
- smtpd_sasl_type = dovecot
- smtpd_sasl_path = private/auth
- smtpd_sasl_local_domain = myclouda.com (providing our domain name)
- smtpd_sasl_security_options = noanonymous
- broken_sasl_auth_clients = yes
- smtpd_sasl_auth_enable = yes
- smtpd_recipient_restrictions = permit_networks, permit_sasl_authenticated, reject_unauth_destination
- smtpd_client_restrictions = permit_networks, permit_sasl_authenticated, reject_unknown_clienthostname

  - smtp_tls_security_level = may
  - smtpd_tls_security_level = may
  - smtp_tls_note_stattls_offer = yes
  - smtpd_tls_loglevel = 1
  - smtpd_tls_received_header = yes
- openssl genrsa -des3 -out server.key 4096 (Generating RSA Private key)
- Sopenssl rsa -in server.key -out server.key.insecure
- $mv server.key server.key secure
- $mv server.key.insecure server.key
- $open ssl req -new -key server.key -out server.csr
- Generating the SSL certificates
  - $openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
  - $sudo cp server.crt /etc/ssl/certs
  - $sudo cp server.key /etc/ssl/private
  - $sudo postconf -e ‘smtpd_tls_key_file = /etc/ssl/private/server.key’
  - $sudo postconf -e ‘smtpd_tls_cert_file = /etc/ssl/certs/server.crt’
  - sudo nano /etc/postfix/main.cf

5.5 Installing Dovecot:

- Commands,
  - $sudo apt-get install dovecot-common -y
  - Ask to create self signed certificate –yes

  - Host name: email.myclouda.net(mail server name)
- To modify some files in dovecot,
  - [auth_mechanisms = plain login] #change plain to plain login
- To restart the service
  - $sudo service postfix restart
  - $ sudo service postfix restart(#Restart again)
  - $sudo service dovecot restart (#dovecot restart)
  - $telnet email.myclouda.net smtp

    ehlo email.myclouda.net

    ctrl+x
  - $telnet mail.robert.com. 587

    ehlo email.myclouda.net

    ctrl+x
- Install dovecot pop3:

    $sudo apt-get install dovecot-imapd dovecot-pop3 -y

  - Configure mail box

    $sudo nano /etc/dovecot/conf.d/10-mail.conf

    Mail_location = maildir:~/Maildir

    $ sudo nano /etc/dovecot/conf.d/20-pop3.conf

    (Uncomment pop3_uidl_format = %08Xu%08Xv)

    $sudo nano /etc/dovecot/conf.d/10-ssl.conf

(Uncomment ssl = yes)

- $sudo service dovecot restart

- Connect Mail Server:

  - $telnet mail.robert.com 110

  Ctrl+x

  - $telnet mail.robert.com 995

  Ctrl+x

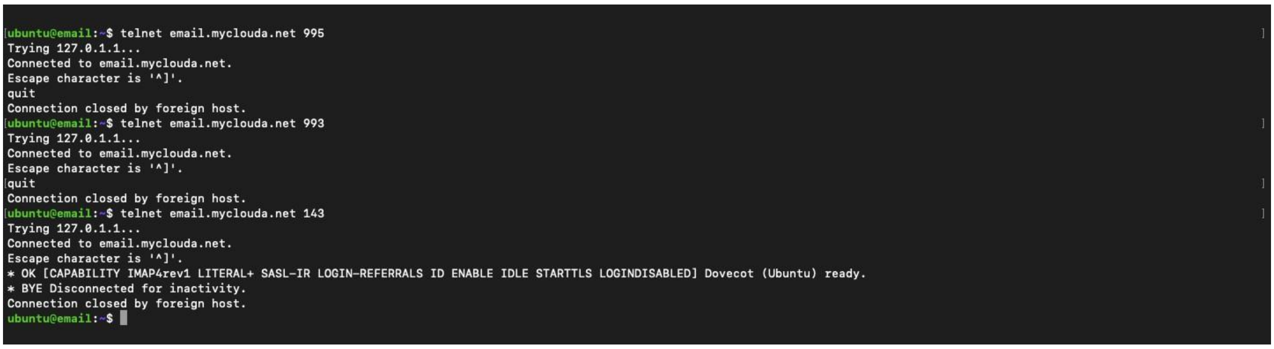
  - $telnet mail.robert.com 993

  Ctrl+x

  - $telnet mail.robert.com 143

  Ctrl+x

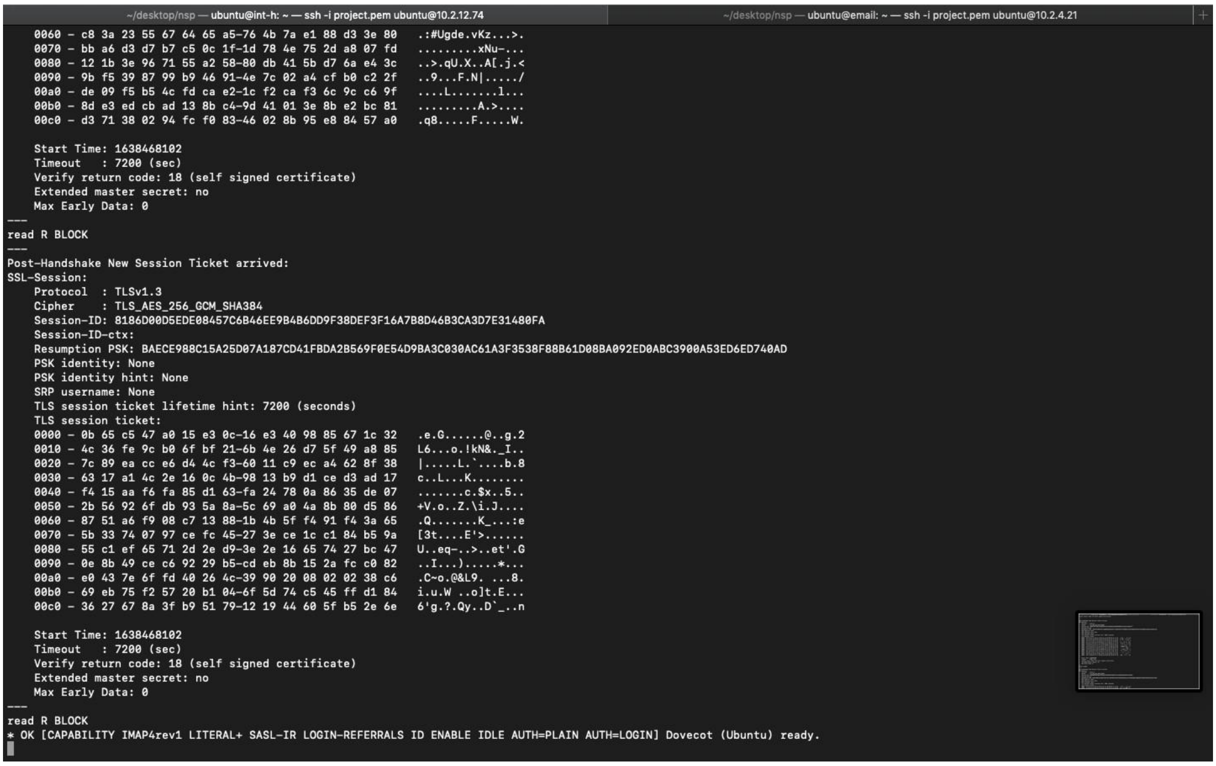
5.6 OUTPUT:



```
ubuntu@email:~$ telnet email.myclouda.net 995
Trying 127.0.1.1...
Connected to email.myclouda.net.
Escape character is '^]'.
quit
Connection closed by foreign host.
ubuntu@email:~$ telnet email.myclouda.net 993
Trying 127.0.1.1...
Connected to email.myclouda.net.
Escape character is '^]'.
quit
Connection closed by foreign host.
ubuntu@email:~$ telnet email.myclouda.net 143
Trying 127.0.1.1...
Connected to email.myclouda.net.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot (Ubuntu) ready.
* BYE Disconnected for inactivity.
Connection closed by foreign host.
ubuntu@email:~$
```

5.7 Internal Host:

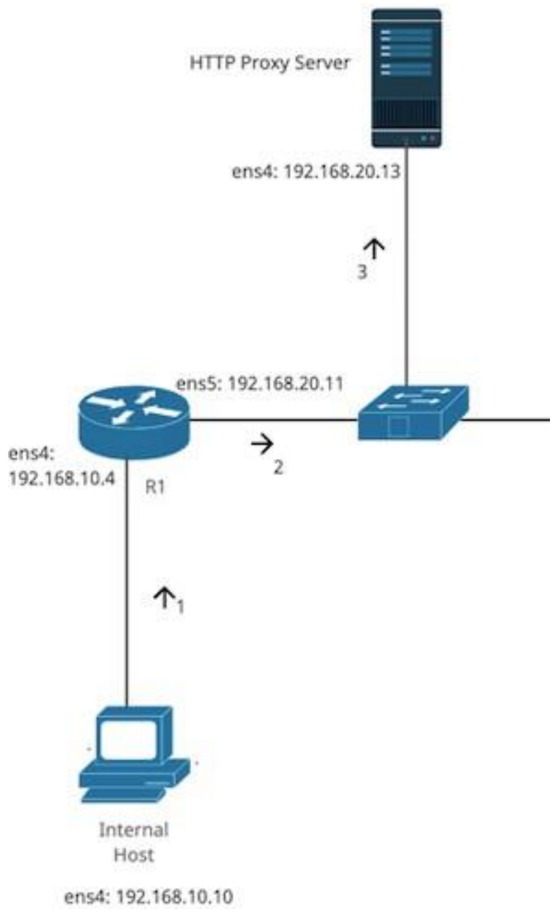
- IP Address : 192.168.10.10
- OS : Ubuntu 18.04
- Interface: ens4 (connected with router 1)
- Command : $ sudo openssl s_client -connect 192.168.30.19:993
- Internal Host to Email Server


~/desktop/nsp — ubuntu@int-h: ~ — ssh -i project.pem ubuntu@10.2.12.74
~/desktop/nsp — ubuntu@email: ~ — ssh -i project.pem ubuntu@10.2.4.21

```
    0060 - c8 3a 23 55 67 64 65 a5-76 4b 7a e1 88 d3 3e 80   .:#Ugde.vKz...>.
    0070 - bb a6 d3 d7 b7 c5 0c 1f-1d 78 4e 75 2d a8 07 fd   .........xNu-...
    0080 - 12 1b 3e 96 71 55 a2 58-80 db 41 5b d7 6a e4 3c   ..>.qU.X..A[.j.<
    0090 - 9b f5 39 87 99 b9 46 91-4e 7c 02 a4 cf b0 c2 2f   ..9...F.N|...../
    00a0 - de 09 f5 b5 4c fd ca e2-1c f2 ca f3 6c 9c c6 9f   ....L.......l...
    00b0 - 8d e3 ed cb ad 13 8b c4-9d 41 01 3e 8b e2 bc 81   .........A.>....
    00c0 - d3 71 38 02 94 fc f0 83-46 02 8b 95 e8 84 57 a0   .q8.....F.....W.

    Start Time: 1638468102
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 8186D00D5EDE08457C6B46EE9B4B6DD9F38DEF3F16A7B8D46B3CA3D7E31480FA
    Session-ID-ctx:
    Resumption PSK: BAECE988C15A25D07A187CD41FBDA2B569F0E54D9BA3C030AC61A3F3538F88B61D08BA092ED0ABC3900A53ED6ED740AD
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 0b 65 c5 47 a0 15 e3 0c-16 e3 40 98 85 67 1c 32   .e.G......@..g.2
    0010 - 4c 36 fe 9c b0 6f bf 21-6b 4e 26 d7 5f 49 a8 85   L6...o.!kN&._I..
    0020 - 7c 89 ea cc e6 d4 4c f3-60 11 c9 ec a4 62 8f 38   |.....L.`....b.8
    0030 - 63 17 a1 4c 2e 16 0c 4b-98 13 b9 d1 ce d3 ad 17   c..L...K........
    0040 - f4 15 aa f6 fa 85 d1 63-fa 24 78 0a 86 35 de 07   .......c.$x..5..
    0050 - 2b 56 92 6f db 93 5a 8a-5c 69 a0 4a 8b 80 d5 86   +V.o..Z.\i.J....
    0060 - 87 51 a6 f9 08 c7 13 88-1b 4b 5f f4 91 f4 3a 65   .Q.......K_....:e
    0070 - 5b 33 74 07 97 ce fc 45-27 3e ce 1c c1 84 b5 9a   [3t....E'>......
    0080 - 55 c1 ef 65 71 2d 2e d9-3e 2e 16 65 74 27 bc 47   U..eq-..>..et'.G
    0090 - 0e 8b 49 ce c6 92 29 b5-cd eb 8b 15 2a fc c0 82   ..I...).....*...
    00a0 - e0 43 7e 6f fd 40 26 4c-39 90 20 08 02 02 38 c6   .C~o.@&L9. ...8.
    00b0 - 69 eb 75 f2 57 20 b1 04-6f 5d 74 c5 45 ff d1 84   i.u.W ..o]t.E...
    00c0 - 36 27 67 8a 3f b9 51 79-12 19 44 60 5f b5 2e 6e   6'g.?.Qy..D`_..n

    Start Time: 1638468102
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu) ready.
```

6. HTTP PROXY SERVER:

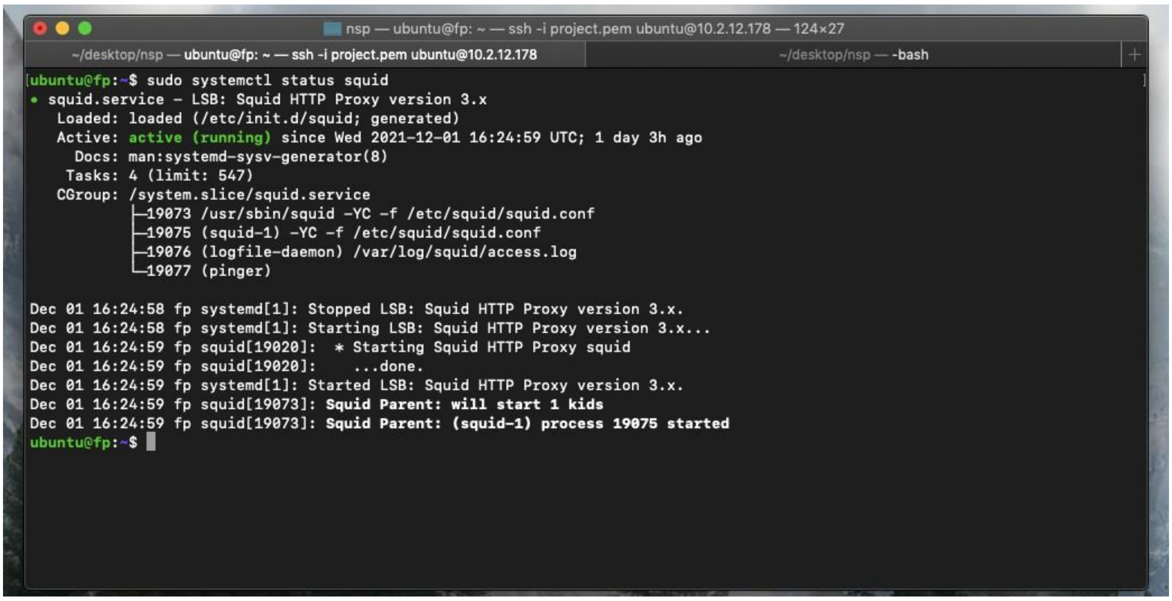
- Install Squid and configure Proxy Server.
- Squid is a web proxy cache server application which provides proxy services for HTTP and popular network protocols.
    - Internal Host connect to Proxy server to browse websites



Internal host to proxy server:

- Internal Host : ens4 -> 192.168.10.10
- Router 1 : ens5 -> 192.168.20.11
- Proxy server : ens4 -> 192.168.20.12

- $ sudo systemctl status squid.



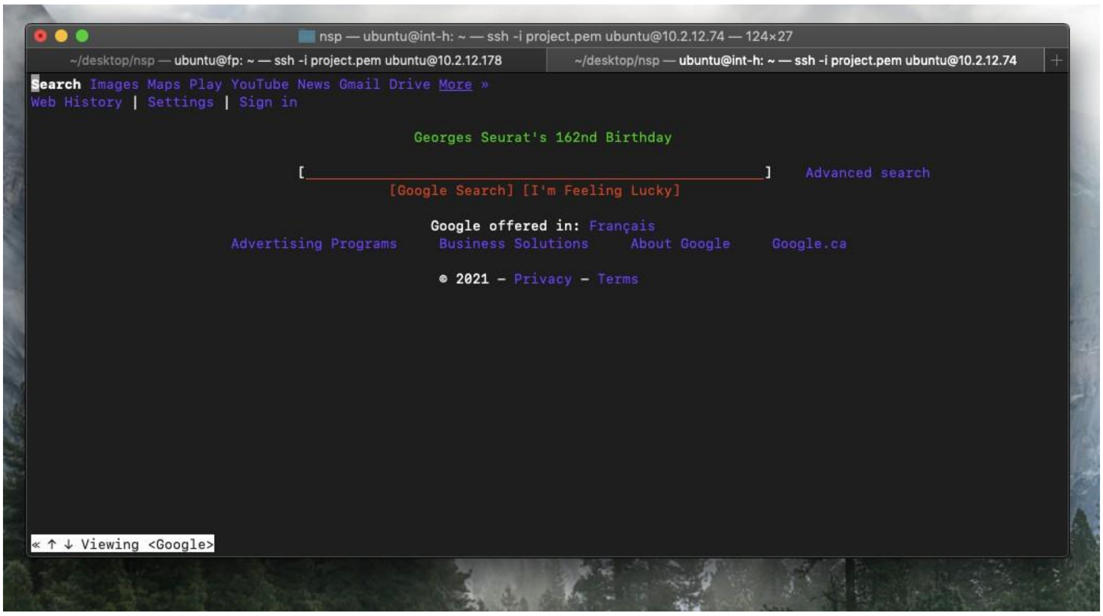
nsp — ubuntu@fp: ~ — ssh -i project.pem ubuntu@10.2.12.178 — 124×27
~/desktop/nsp — ubuntu@fp: ~ — ssh -i project.pem ubuntu@10.2.12.178
~/desktop/nsp — -bash

```
ubuntu@fp:~$ sudo systemctl status squid
● squid.service - LSB: Squid HTTP Proxy version 3.x
   Loaded: loaded (/etc/init.d/squid; generated)
   Active: active (running) since Wed 2021-12-01 16:24:59 UTC; 1 day 3h ago
     Docs: man:systemd-sysv-generator(8)
    Tasks: 4 (limit: 547)
   CGroup: /system.slice/squid.service
           ├─19073 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           ├─19075 (squid-1) -YC -f /etc/squid/squid.conf
           ├─19076 (logfile-daemon) /var/log/squid/access.log
           └─19077 (pinger)

Dec 01 16:24:58 fp systemd[1]: Stopped LSB: Squid HTTP Proxy version 3.x.
Dec 01 16:24:58 fp systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Dec 01 16:24:59 fp squid[19020]:  * Starting Squid HTTP Proxy squid
Dec 01 16:24:59 fp squid[19020]:    ...done.
Dec 01 16:24:59 fp systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
Dec 01 16:24:59 fp squid[19073]: Squid Parent: will start 1 kids
Dec 01 16:24:59 fp squid[19073]: Squid Parent: (squid-1) process 19075 started
ubuntu@fp:~$
```

- Adding source network network (LAN networks) and all necessary commands
  - acl lan src 192.168.10.0/24
  - http_access allow lan
  - request_header_access Referer deny all
  - request_header_access X-Forwarded-For deny all
  - request_header_access Via deny all
  - request_header_access Cache-Control deny all

6.1 Internal Host:

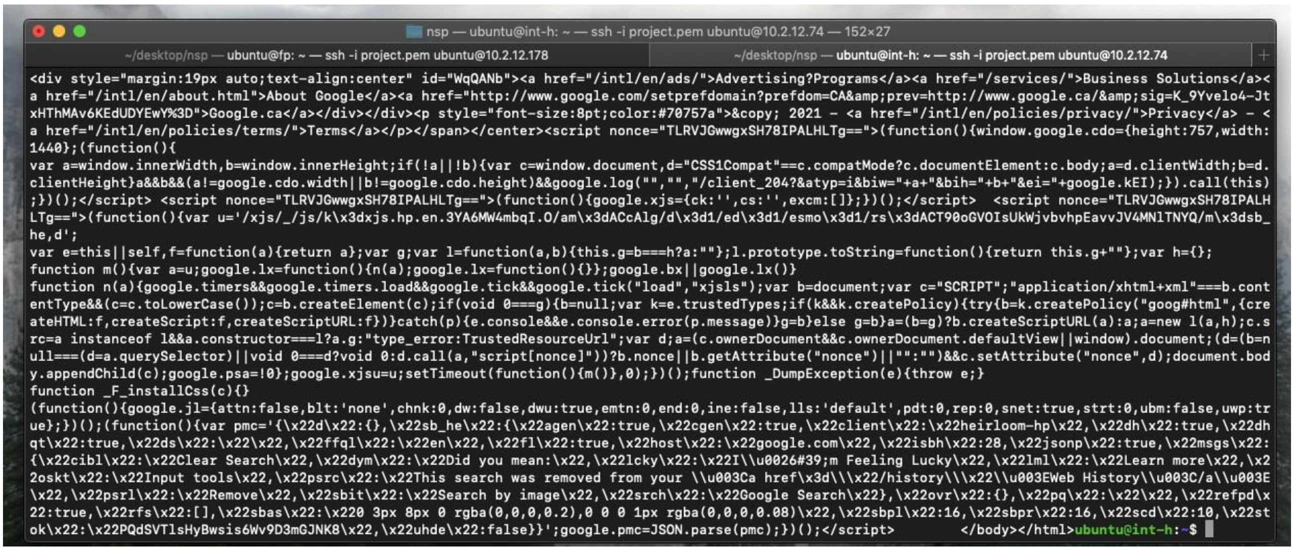
- Browsing the website in LAN using Proxy Server using w3m.



nsp — ubuntu@int-h: ~ — ssh -i project.pem ubuntu@10.2.12.74 — 124×27
~/desktop/nsp — ubuntu@fp: ~ — ssh -i project.pem ubuntu@10.2.12.178
~/desktop/nsp — ubuntu@int-h: ~ — ssh -i project.pem ubuntu@10.2.12.74

```
Search Images Maps Play YouTube News Gmail Drive More »
Web History | Settings | Sign in

                              Georges Seurat's 162nd Birthday

                 [_____________________________________________]   Advanced search
                              [Google Search] [I'm Feeling Lucky]

                              Google offered in: Français
             Advertising Programs    Business Solutions    About Google    Google.ca

                                  © 2021 - Privacy - Terms

« ↑ ↓ Viewing <Google>
```

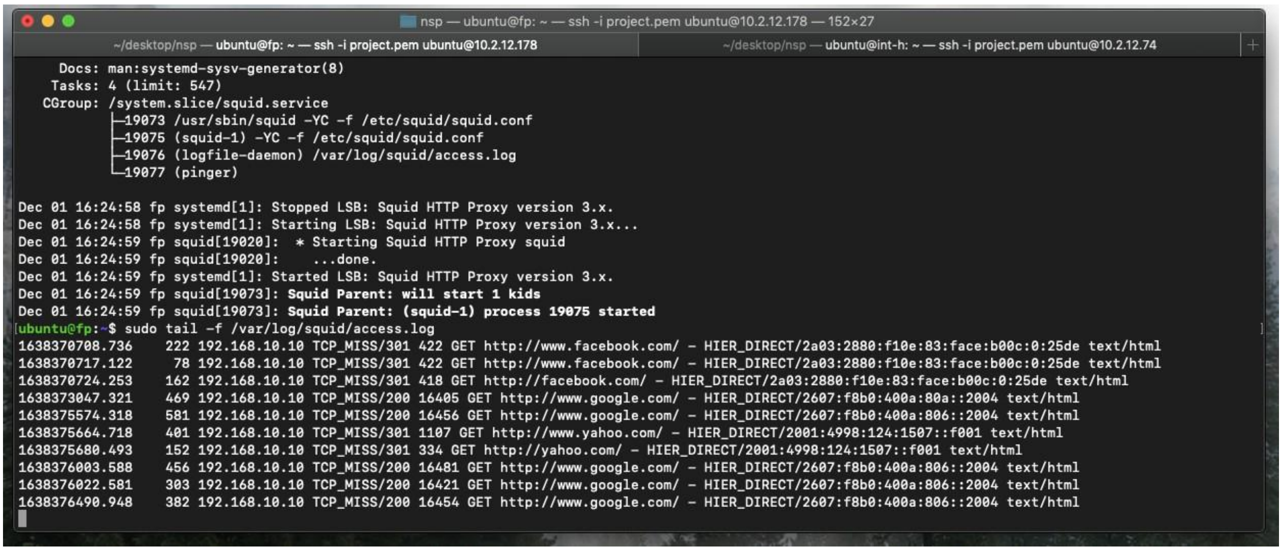
- Using : curl http://www.google.com


nsp — ubuntu@int-h: ~ — ssh -i project.pem ubuntu@10.2.12.74 — 152×27
~/desktop/nsp — ubuntu@fp: ~ — ssh -i project.pem ubuntu@10.2.12.178
~/desktop/nsp — ubuntu@int-h: ~ — ssh -i project.pem ubuntu@10.2.12.74

```
<div style="margin:19px auto;text-align:center" id="WqQANb"><a href="/intl/en/ads/">Advertising?Programs</a><a href="/services/">Business Solutions</a><
a href="/intl/en/about.html">About Google</a><a href="http://www.google.com/setprefdomain?prefdom=CA&amp;prev=http://www.google.ca/&amp;sig=K_9Yvelo4-Jt
xHThMAv6KEdUDYEwY%3D">Google.ca</a></div></div><p style="font-size:8pt;color:#70757a">&copy; 2021 - <a href="/intl/en/policies/privacy/">Privacy</a> - <
a href="/intl/en/policies/terms/">Terms</a></p></span></center><script nonce="TLRVJGwwgxSH78IPALHLTg==">(function(){window.google.cdo={height:757,width:
1440};(function(){
var a=window.innerWidth,b=window.innerHeight;if(!a||!b){var c=window.document,d="CSS1Compat"==c.compatMode?c.documentElement:c.body;a=d.clientWidth;b=d.
clientHeight}a&&b&&(a!=google.cdo.width||b!=google.cdo.height)&&google.log("","","/client_204?&atyp=i&biw="+a+"&bih="+b+"&ei="+google.kEI);}).call(this)
;})();</script> <script nonce="TLRVJGwwgxSH78IPALHLTg==">(function(){google.xjs={ck:'',cs:'',excm:[]};})();</script>  <script nonce="TLRVJGwwgxSH78IPALH
LTg==">(function(){var u='/xjs/_/js/k\x3dxjs.hp.en.3YA6MW4mbqI.O/am\x3dACcAlg/d\x3d1/ed\x3d1/esmo\x3d1/rs\x3dACT90oGVOIsUkWjvbvhpEavvJV4MNlTNYQ/m\x3dsb_
he,d';
var e=this||self,f=function(a){return a};var g;var l=function(a,b){this.g=b===h?a:""};l.prototype.toString=function(){return this.g+""};var h={};
function m(){var a=u;google.lx=function(){n(a);google.lx=function(){}};google.bx||google.lx()}
function n(a){google.timers&&google.timers.load&&google.tick&&google.tick("load","xjsls");var b=document;var c="SCRIPT";"application/xhtml+xml"===b.cont
entType&&(c=c.toLowerCase());c=b.createElement(c);if(void 0===g){b=null;var k=e.trustedTypes;if(k&&k.createPolicy){try{b=k.createPolicy("goog#html",{cre
ateHTML:f,createScript:f,createScriptURL:f})}catch(p){e.console&&e.console.error(p.message)}g=b}else g=b}a=(b=g)?b.createScriptURL(a):a;a=new l(a,h);c.s
rc=a instanceof l&&a.constructor===l?a.g:"type_error:TrustedResourceUrl";var d;a=(c.ownerDocument&&c.ownerDocument.defaultView||window).document;(d=(b=n
ull===(d=a.querySelector)||void 0===d?void 0:d.call(a,"script[nonce]"))?b.nonce||b.getAttribute("nonce")||"":"")&&c.setAttribute("nonce",d);document.bod
y.appendChild(c);google.psa=!0};google.xjsu=u;setTimeout(function(){m()},0);})();function _DumpException(e){throw e;}
function _F_installCss(c){}
(function(){google.jl={attn:false,blt:'none',chnk:0,dw:false,dwu:true,emtn:0,end:0,ine:false,lls:'default',pdt:0,rep:0,snet:true,strt:0,ubm:false,uwp:tr
ue};})();(function(){var pmc='{\x22d\x22:{},\x22sb_he\x22:{\x22agen\x22:true,\x22cgen\x22:true,\x22client\x22:\x22heirloom-hp\x22,\x22dh\x22:true,\x22dh
qt\x22:true,\x22ds\x22:\x22\x22,\x22ffql\x22:\x22en\x22,\x22fl\x22:true,\x22host\x22:\x22google.com\x22,\x22isbh\x22:28,\x22jsonp\x22:true,\x22msgs\x22:
{\x22cibl\x22:\x22Clear Search\x22,\x22dym\x22:\x22Did you mean:\x22,\x22lcky\x22:\x22I\\u0026#39;m Feeling Lucky\x22,\x22lml\x22:\x22Learn more\x22,\x2
2oskt\x22:\x22Input tools\x22,\x22psrc\x22:\x22This search was removed from your \\u003Ca href\x3d\\\x22/history\\\x22\\u003EWeb History\\u003C/a\\u003E
\x22,\x22psrl\x22:\x22Remove\x22,\x22sbit\x22:\x22Search by image\x22,\x22srch\x22:\x22Google Search\x22},\x22ovr\x22:{},\x22pq\x22:\x22\x22,\x22refpd\x
22:true,\x22rfs\x22:[],\x22sbas\x22:\x220 3px 8px 0 rgba(0,0,0,0.2),0 0 0 1px rgba(0,0,0,0.08)\x22,\x22sbpl\x22:16,\x22sbpr\x22:16,\x22scd\x22:10,\x22st
ok\x22:\x22PQdSVTlsHyBwsis6Wv9D3mGJNK8\x22,\x22uhde\x22:false}}';google.pmc=JSON.parse(pmc);})();</script>       </body></html>ubuntu@int-h:~$ 
```

6.2 Access Log in Proxy Server:

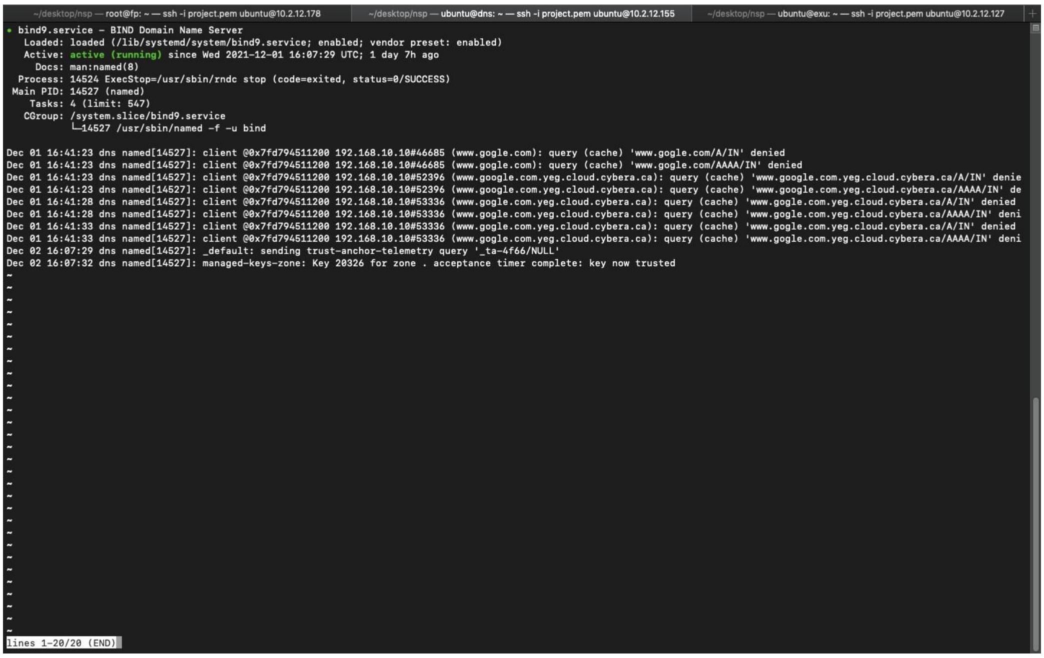
- Provides the details about the access of the website accessed by the Internal host.
- It will provide history of the Internal user’s browse history.


nsp — ubuntu@fp: ~ — ssh -i project.pem ubuntu@10.2.12.178 — 152×27
~/desktop/nsp — ubuntu@fp: ~ — ssh -i project.pem ubuntu@10.2.12.178
~/desktop/nsp — ubuntu@int-h: ~ — ssh -i project.pem ubuntu@10.2.12.74

```
     Docs: man:systemd-sysv-generator(8)
    Tasks: 4 (limit: 547)
   CGroup: /system.slice/squid.service
           ├─19073 /usr/sbin/squid -YC -f /etc/squid/squid.conf
           ├─19075 (squid-1) -YC -f /etc/squid/squid.conf
           ├─19076 (logfile-daemon) /var/log/squid/access.log
           └─19077 (pinger)

Dec 01 16:24:58 fp systemd[1]: Stopped LSB: Squid HTTP Proxy version 3.x.
Dec 01 16:24:58 fp systemd[1]: Starting LSB: Squid HTTP Proxy version 3.x...
Dec 01 16:24:59 fp squid[19020]:  * Starting Squid HTTP Proxy squid
Dec 01 16:24:59 fp squid[19020]:    ...done.
Dec 01 16:24:59 fp systemd[1]: Started LSB: Squid HTTP Proxy version 3.x.
Dec 01 16:24:59 fp squid[19073]: Squid Parent: will start 1 kids
Dec 01 16:24:59 fp squid[19073]: Squid Parent: (squid-1) process 19075 started
ubuntu@fp:~$ sudo tail -f /var/log/squid/access.log
1638370708.736    222 192.168.10.10 TCP_MISS/301 422 GET http://www.facebook.com/ - HIER_DIRECT/2a03:2880:f10e:83:face:b00c:0:25de text/html
1638370717.122     78 192.168.10.10 TCP_MISS/301 422 GET http://www.facebook.com/ - HIER_DIRECT/2a03:2880:f10e:83:face:b00c:0:25de text/html
1638370724.253    162 192.168.10.10 TCP_MISS/301 418 GET http://facebook.com/ - HIER_DIRECT/2a03:2880:f10e:83:face:b00c:0:25de text/html
1638373047.321    469 192.168.10.10 TCP_MISS/200 16405 GET http://www.google.com/ - HIER_DIRECT/2607:f8b0:400a:80a::2004 text/html
1638375574.318    581 192.168.10.10 TCP_MISS/200 16456 GET http://www.google.com/ - HIER_DIRECT/2607:f8b0:400a:806::2004 text/html
1638375664.718    401 192.168.10.10 TCP_MISS/301 1107 GET http://www.yahoo.com/ - HIER_DIRECT/2001:4998:124:1507::f001 text/html
1638375680.493    152 192.168.10.10 TCP_MISS/301 334 GET http://yahoo.com/ - HIER_DIRECT/2001:4998:124:1507::f001 text/html
1638376003.588    456 192.168.10.10 TCP_MISS/200 16481 GET http://www.google.com/ - HIER_DIRECT/2607:f8b0:400a:806::2004 text/html
1638376022.581    303 192.168.10.10 TCP_MISS/200 16421 GET http://www.google.com/ - HIER_DIRECT/2607:f8b0:400a:806::2004 text/html
1638376490.948    382 192.168.10.10 TCP_MISS/200 16454 GET http://www.google.com/ - HIER_DIRECT/2607:f8b0:400a:806::2004 text/html
```

7. DNS (Domain Name System):

- BIND is used to configure DNS server which resolved domain name or IP address.
- Command: $ sudo apt -y install bind9 bind9utils

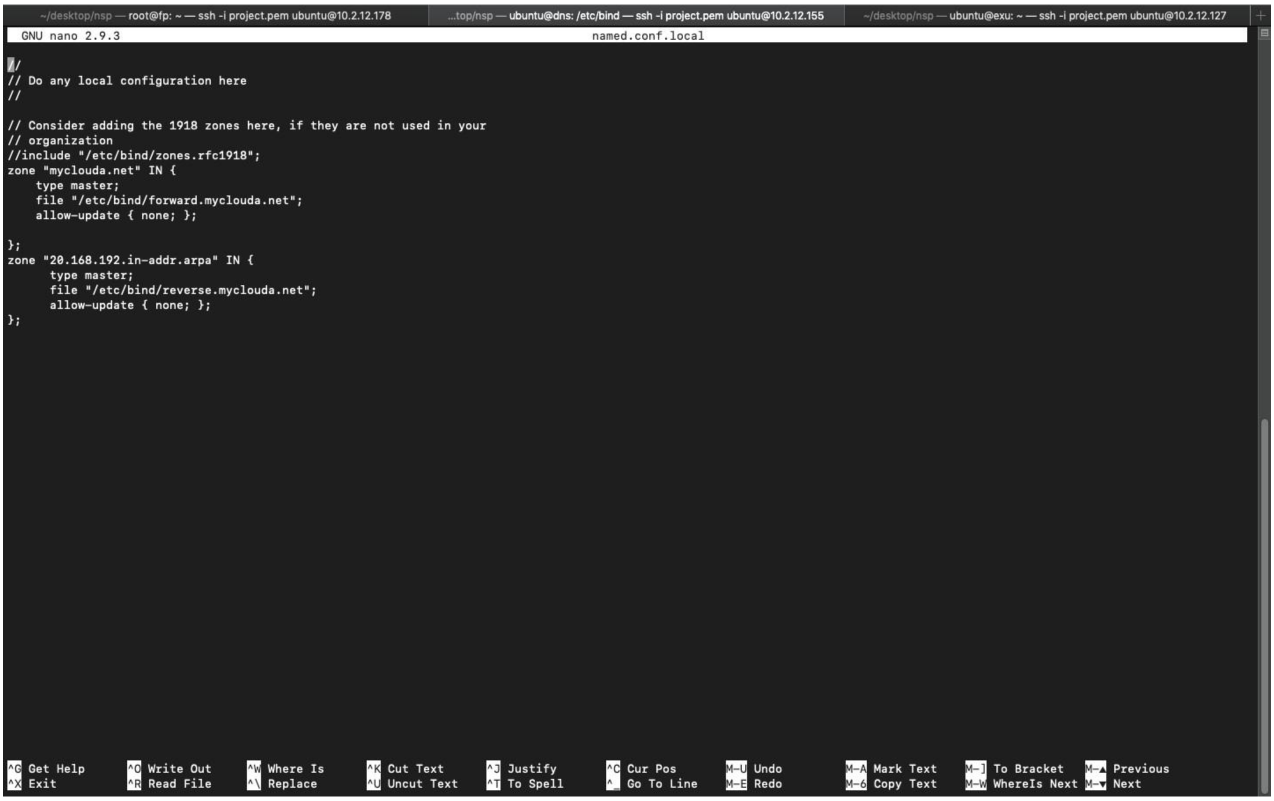


~/desktop/nsp — root@fp: ~ — ssh -i project.pem ubuntu@10.2.12.178
~/desktop/nsp — ubuntu@dns: ~ — ssh -i project.pem ubuntu@10.2.12.155
~/desktop/nsp — ubuntu@exu: ~ — ssh -i project.pem ubuntu@10.2.12.127

```
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2021-12-01 16:07:29 UTC; 1 day 7h ago
     Docs: man:named(8)
  Process: 14524 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 14527 (named)
    Tasks: 4 (limit: 547)
   CGroup: /system.slice/bind9.service
           └─14527 /usr/sbin/named -f -u bind

Dec 01 16:41:23 dns named[14527]: client @0x7fd794511200 192.168.10.10#46685 (www.gogle.com): query (cache) 'www.gogle.com/A/IN' denied
Dec 01 16:41:23 dns named[14527]: client @0x7fd794511200 192.168.10.10#46685 (www.gogle.com): query (cache) 'www.gogle.com/AAAA/IN' denied
Dec 01 16:41:23 dns named[14527]: client @0x7fd794511200 192.168.10.10#52396 (www.google.com.yeg.cloud.cybera.ca): query (cache) 'www.google.com.yeg.cloud.cybera.ca/A/IN' denie
Dec 01 16:41:23 dns named[14527]: client @0x7fd794511200 192.168.10.10#52396 (www.google.com.yeg.cloud.cybera.ca): query (cache) 'www.google.com.yeg.cloud.cybera.ca/AAAA/IN' de
Dec 01 16:41:28 dns named[14527]: client @0x7fd794511200 192.168.10.10#53336 (www.gogle.com.yeg.cloud.cybera.ca): query (cache) 'www.gogle.com.yeg.cloud.cybera.ca/A/IN' denied
Dec 01 16:41:28 dns named[14527]: client @0x7fd794511200 192.168.10.10#53336 (www.gogle.com.yeg.cloud.cybera.ca): query (cache) 'www.gogle.com.yeg.cloud.cybera.ca/AAAA/IN' deni
Dec 01 16:41:33 dns named[14527]: client @0x7fd794511200 192.168.10.10#53336 (www.gogle.com.yeg.cloud.cybera.ca): query (cache) 'www.gogle.com.yeg.cloud.cybera.ca/A/IN' denied
Dec 01 16:41:33 dns named[14527]: client @0x7fd794511200 192.168.10.10#53336 (www.gogle.com.yeg.cloud.cybera.ca): query (cache) 'www.gogle.com.yeg.cloud.cybera.ca/AAAA/IN' deni
Dec 02 16:07:29 dns named[14527]: _default: sending trust-anchor-telemetry query '_ta-4f66/NULL'
Dec 02 16:07:32 dns named[14527]: managed-keys-zone: Key 20326 for zone . acceptance timer complete: key now trusted
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
lines 1-20/20 (END)
```

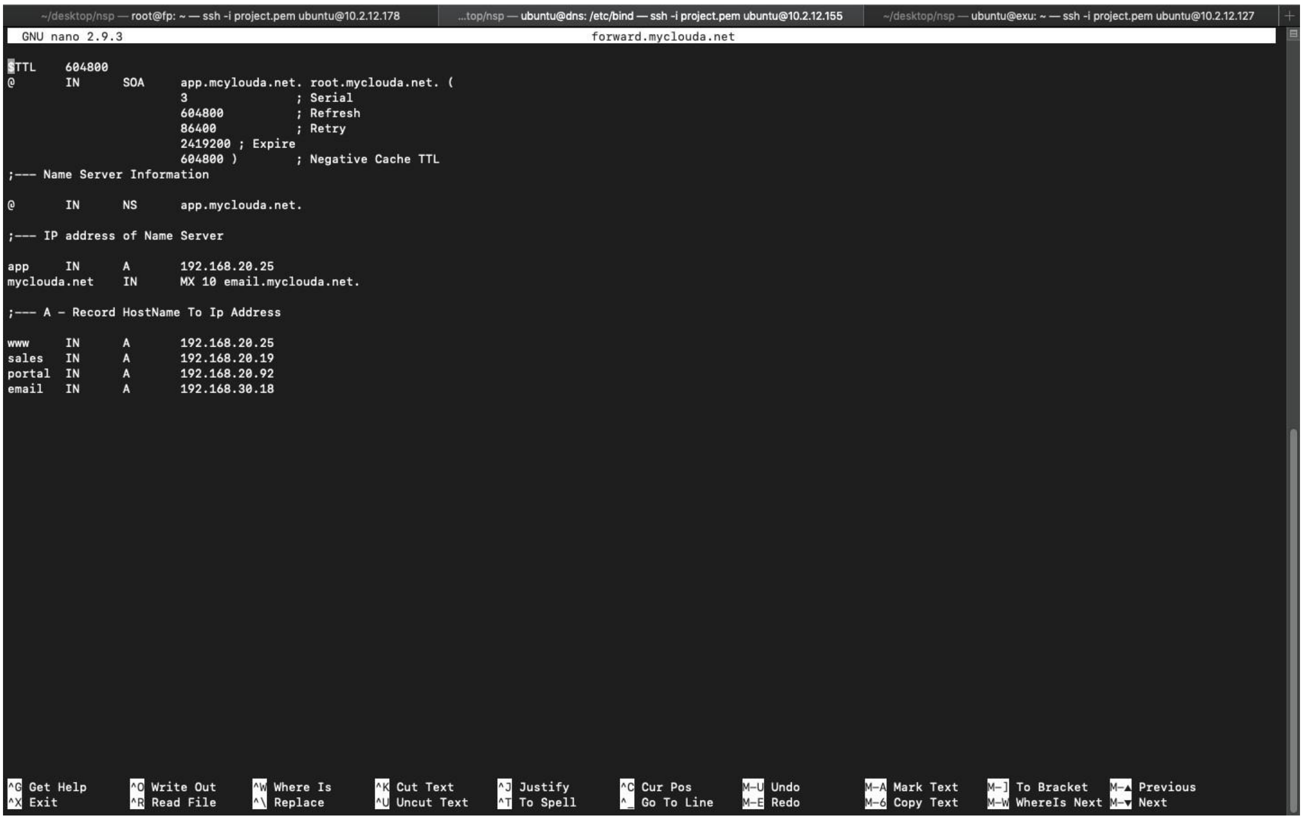
- Configuration on /etc/bind/named.conf.local.

7.1 Configure Zone Files:



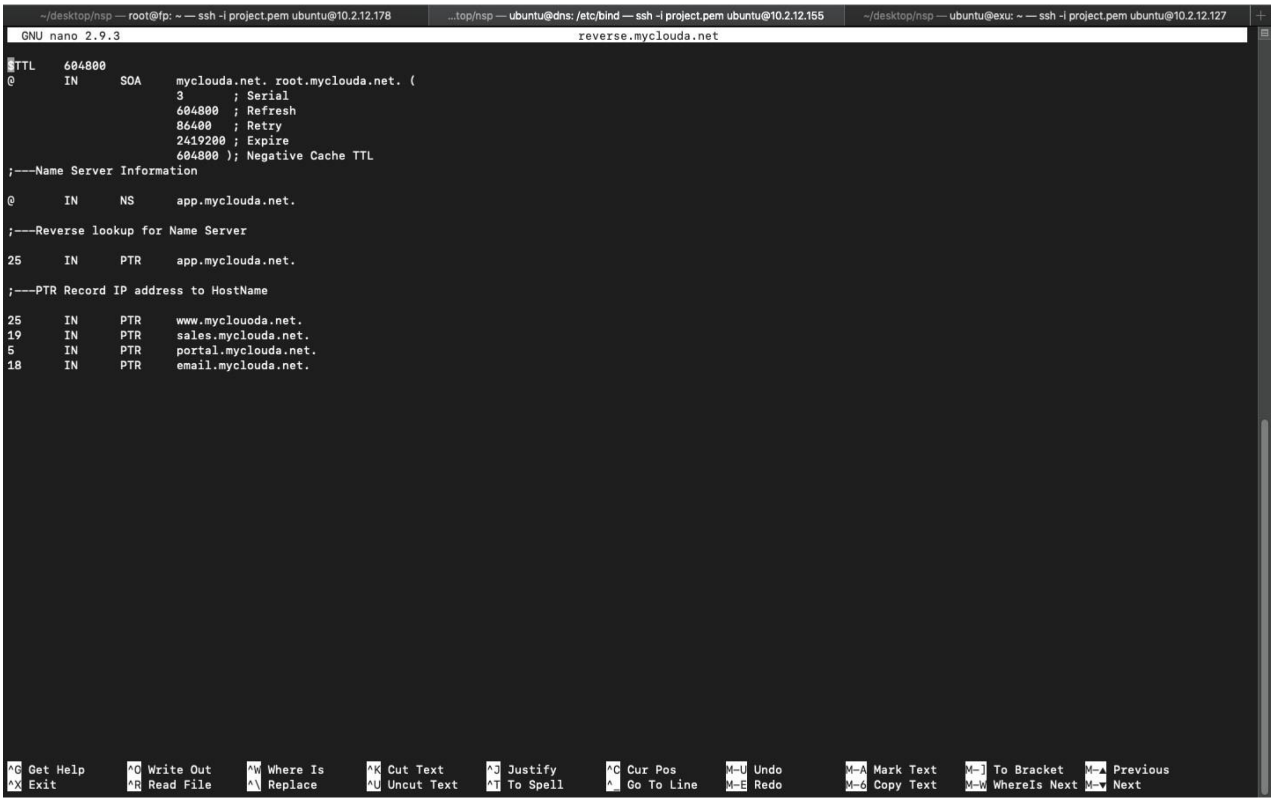
```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "myclouda.net" IN {
    type master;
    file "/etc/bind/forward.myclouda.net";
    allow-update { none; };

};
zone "20.168.192.in-addr.arpa" IN {
      type master;
      file "/etc/bind/reverse.myclouda.net";
      allow-update { none; };
};
```

- For Internal Zone,



```
$TTL    604800
@       IN      SOA     app.mcylouda.net. root.myclouda.net. (
                        3               ; Serial
                        604800          ; Refresh
                        86400           ; Retry
                        2419200 ; Expire
                        604800 )        ; Negative Cache TTL
;--- Name Server Information

@       IN      NS      app.myclouda.net.

;--- IP address of Name Server

app     IN      A       192.168.20.25
myclouda.net    IN      MX 10 email.myclouda.net.

;--- A - Record HostName To Ip Address

www     IN      A       192.168.20.25
sales   IN      A       192.168.20.19
portal  IN      A       192.168.20.92
email   IN      A       192.168.30.18
```

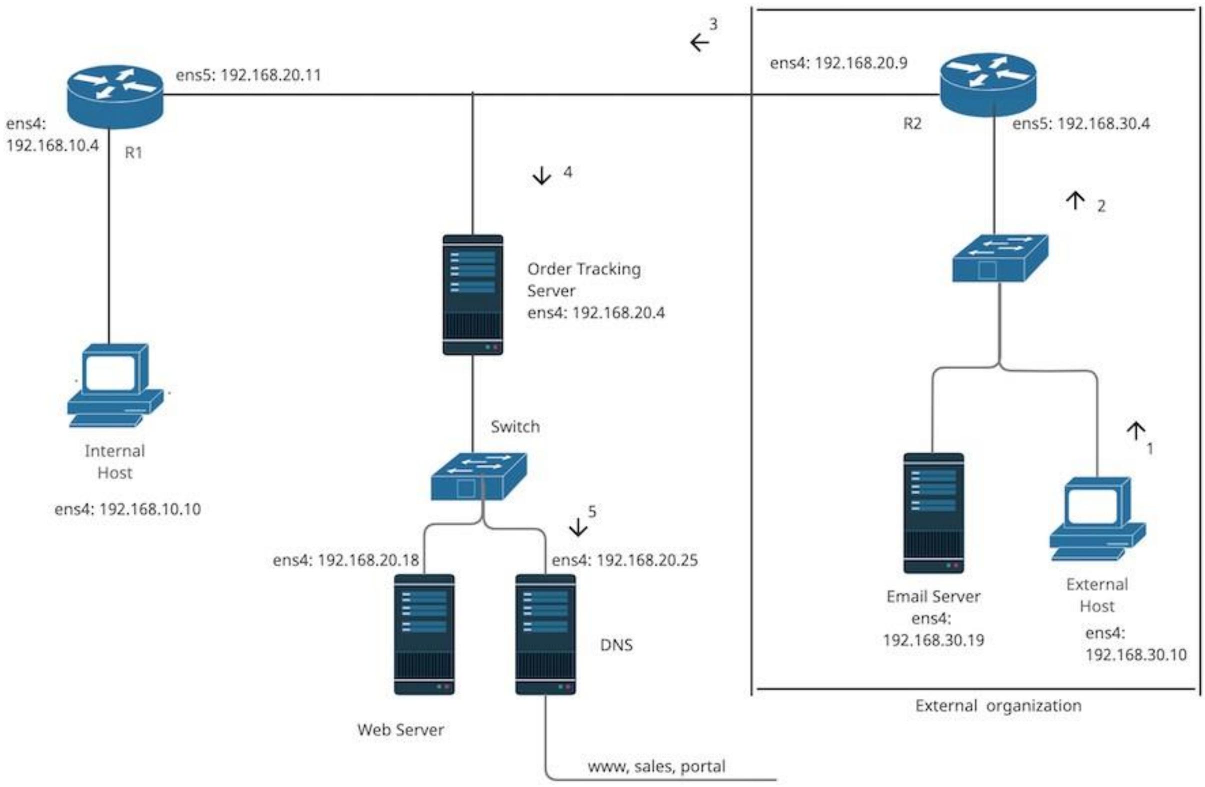
- For External Zone,



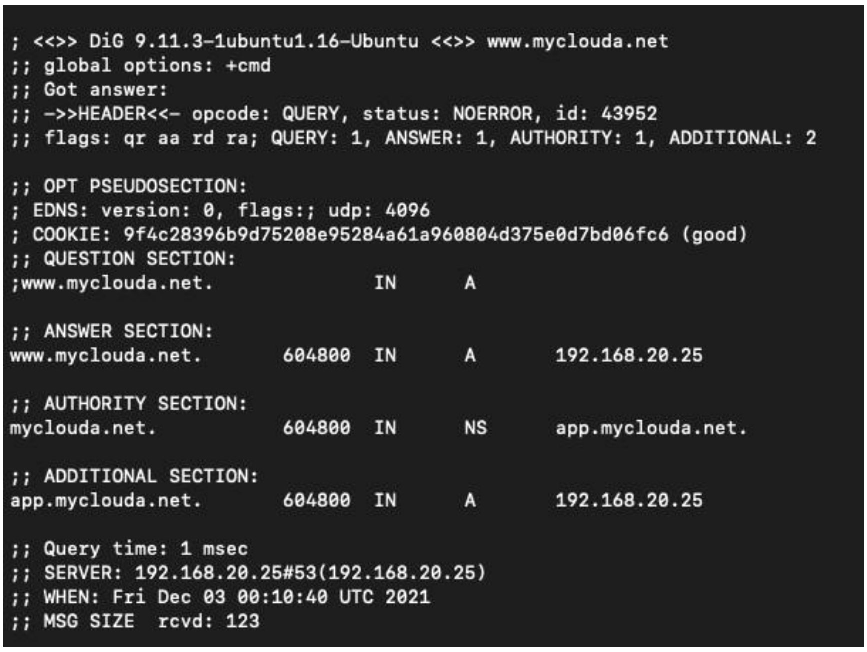
```
$TTL    604800
@       IN      SOA     myclouda.net. root.myclouda.net. (
                        3       ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ); Negative Cache TTL
;---Name Server Information

@       IN      NS      app.myclouda.net.

;---Reverse lookup for Name Server

25      IN      PTR     app.myclouda.net.

;---PTR Record IP address to HostName

25      IN      PTR     www.myclouoda.net.
19      IN      PTR     sales.myclouda.net.
5       IN      PTR     portal.myclouda.net.
18      IN      PTR     email.myclouda.net.
```

7.2 External User to DNS access:

- External user able to resolve the three hosts know as www, sales, portal.
- External User -> Router 2 -> Order tracking server -> DNS

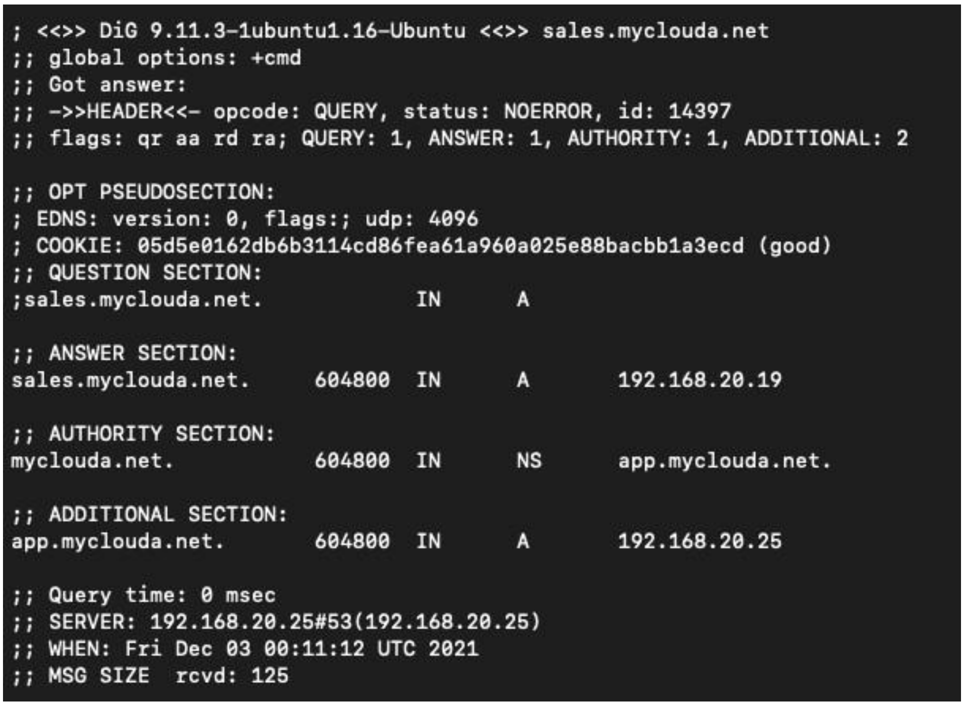


- Resolve the hosts:
    - www



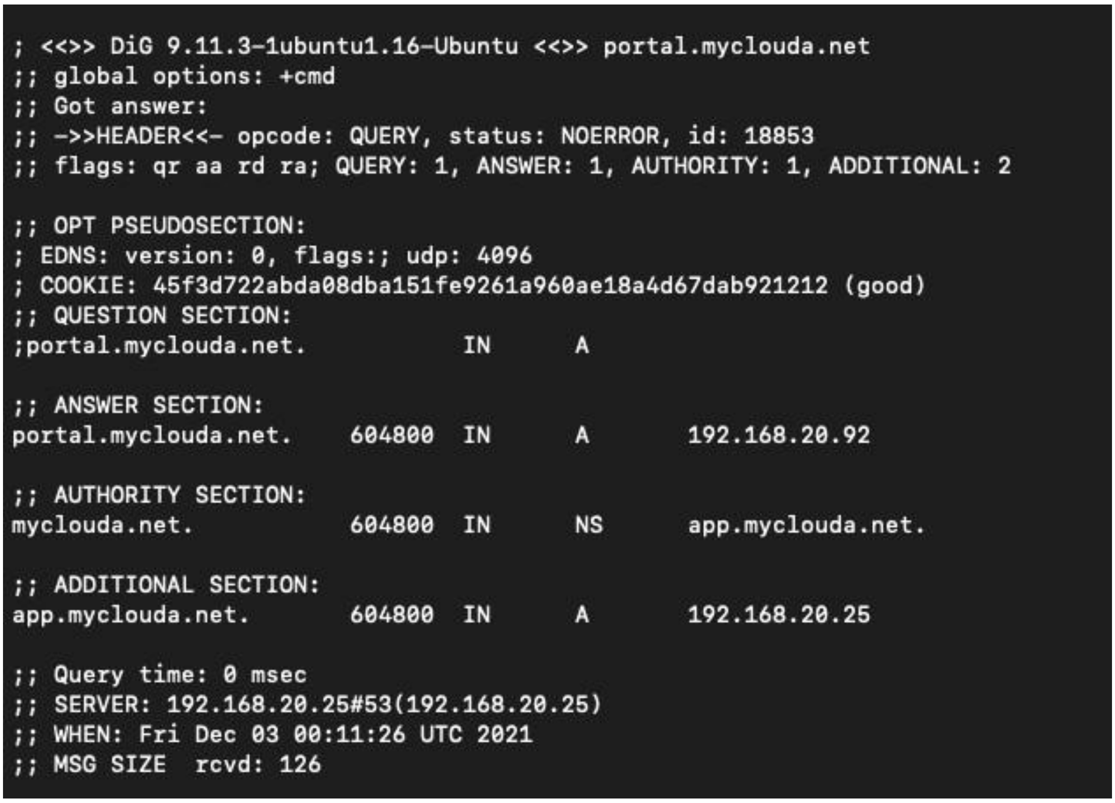
```
; <<>> DiG 9.11.3-1ubuntu1.16-Ubuntu <<>> www.myclouda.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43952
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9f4c28396b9d75208e95284a61a960804d375e0d7bd06fc6 (good)
;; QUESTION SECTION:
;www.myclouda.net.              IN      A

;; ANSWER SECTION:
www.myclouda.net.       604800  IN      A       192.168.20.25

;; AUTHORITY SECTION:
myclouda.net.           604800  IN      NS      app.myclouda.net.

;; ADDITIONAL SECTION:
app.myclouda.net.       604800  IN      A       192.168.20.25

;; Query time: 1 msec
;; SERVER: 192.168.20.25#53(192.168.20.25)
;; WHEN: Fri Dec 03 00:10:40 UTC 2021
;; MSG SIZE  rcvd: 123
```

- Sales



```
; <<>> DiG 9.11.3-1ubuntu1.16-Ubuntu <<>> sales.myclouda.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14397
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 05d5e0162db6b3114cd86fea61a960a025e88bacbb1a3ecd (good)
;; QUESTION SECTION:
;sales.myclouda.net.            IN      A

;; ANSWER SECTION:
sales.myclouda.net.     604800  IN      A       192.168.20.19

;; AUTHORITY SECTION:
myclouda.net.           604800  IN      NS      app.myclouda.net.

;; ADDITIONAL SECTION:
app.myclouda.net.       604800  IN      A       192.168.20.25

;; Query time: 0 msec
;; SERVER: 192.168.20.25#53(192.168.20.25)
;; WHEN: Fri Dec 03 00:11:12 UTC 2021
;; MSG SIZE  rcvd: 125
```

- Portal

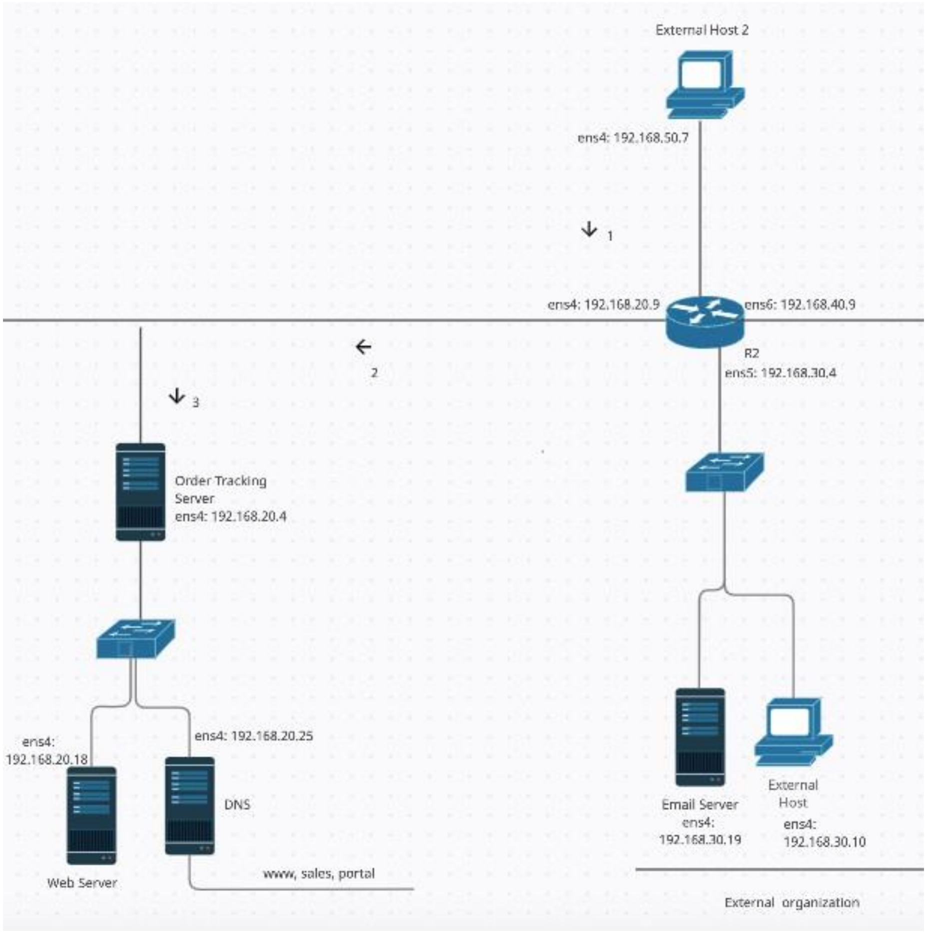


```
; <<>> DiG 9.11.3-1ubuntu1.16-Ubuntu <<>> portal.myclouda.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18853
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 45f3d722abda08dba151fe9261a960ae18a4d67dab921212 (good)
;; QUESTION SECTION:
;portal.myclouda.net.           IN      A

;; ANSWER SECTION:
portal.myclouda.net.    604800  IN      A       192.168.20.92

;; AUTHORITY SECTION:
myclouda.net.           604800  IN      NS      app.myclouda.net.

;; ADDITIONAL SECTION:
app.myclouda.net.       604800  IN      A       192.168.20.25

;; Query time: 0 msec
;; SERVER: 192.168.20.25#53(192.168.20.25)
;; WHEN: Fri Dec 03 00:11:26 UTC 2021
;; MSG SIZE  rcvd: 126
```

- Domain name : myclouda.net ; Host names : www, sales, portal.

8. <u>ORDER TRACKING SERVER:</u>

- Order tracking server monitors the network traffic between only selected list of clients. We have done the IP whitelisting allowing few networks to access the internal organization and blocked (Network 5 - 192.168.50.0/24) so that it will not be able to access. The order tracking server shows only the network traffic between the allowed IP address .



- External Host 1 - Allowing only selected clients from the Network 5 to DNS server.

IP Tables:

- Allow SSH:

```
$ sudo iptables -A INPUT -p tcp --sport 22 -j ACCEPT
$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

- Blacklist - IP Tables:

```
$ iptables -A INPUT -m iprange --src-range 192.168.50.2-192.168.50.254 -j
      DROP
```

- Whitelist - IP Tables:

```
$ iptables -A INPUT -s 192.168.50.7 -p tcp --dport 443 -i ens4 -j ACCEPT
$ iptables -A INPUT -i lo -m comment --comment "Allow loopback
      connections" -j ACCEPT
$ iptables -A INPUT -s 192.168.50.0/24 -j ACCEPT
$ iptables -A INPUT -s 192.168.50.7 -j ACCEPT
$ iptables -A INPUT -m iprange --src-range 192.168.50.2-192.168.50.100 -j
  ACCEPT
```

9. Additional Security Mechanism :

- **ZEEK IDS:**

  - Zeek is an open-source network traffic analyzer. Incident detection and response is done by giving the transaction data and extracted content data in the form of logs. It also provides alert data and customizes alert when required by the end-user. It can help to look back at the logs what has happened during an incident and after an incident. It would be able to provide all types of logs like DNS logs, SSL and also HTTP sessions.

Steps to Install and configure demonstrate the working of ZEEK IDS in our network

Step 1: Install Zeek

- Instance: Router 1
- Network : 2
- Subnet: 192.168.20.0/24
- Interface: ens5

Adding the Zeek repository to the system

- apt-get install curl gnupg2 wget -y

Step 2: Install and update

- apt-get update -y
- apt-get install zeek -y

Step 3: Add Zeek to the system path and activate ~./.bashrc file and check the version

- echo "export PATH=$PATH:/opt/zeek/bin" >> ~/.bashrc
- source ~/.bashrc

Step 4: Define the network to be monitored

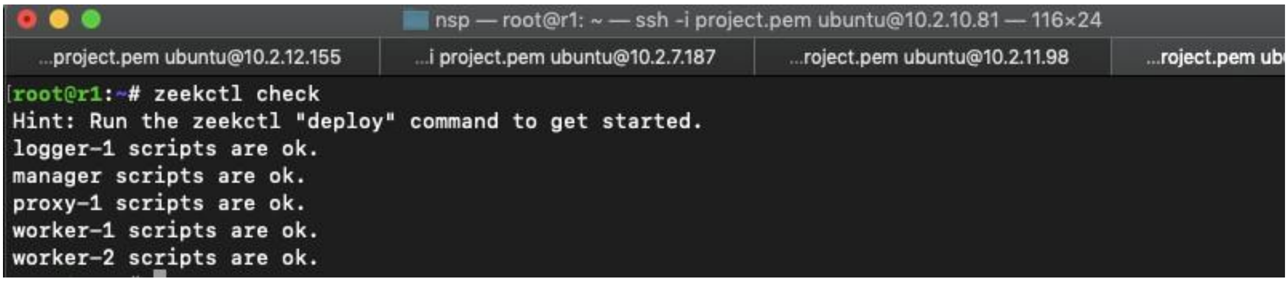
- nano /opt/zeek/etc/networks.cfg
- 192.168.20.0/24

Step 5: Edit the zeek config file

- $ sudo nano /opt/zeek/etc/node.cfg

Step 6 : comment some lines of the file and check using the file using command

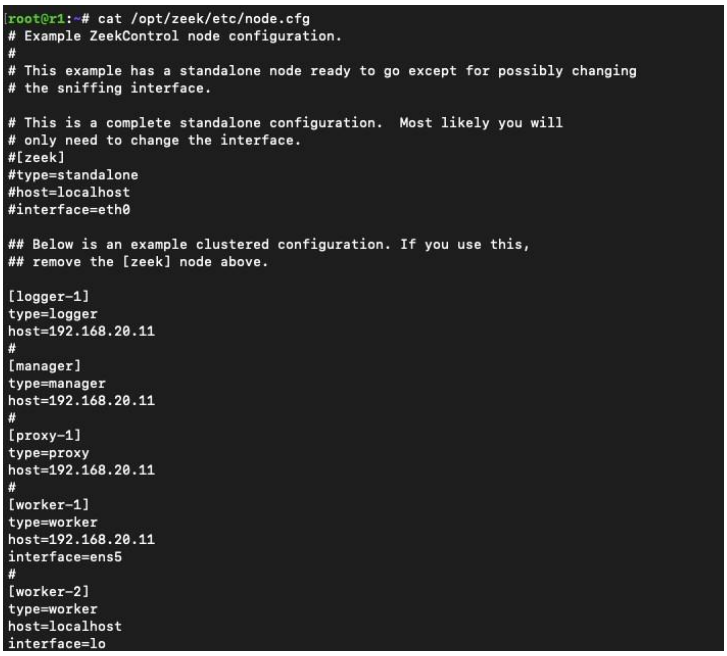
- zeekctl check


nsp — root@r1: ~ — ssh -i project.pem ubuntu@10.2.10.81 — 116×24
...project.pem ubuntu@10.2.12.155
...i project.pem ubuntu@10.2.7.187
...roject.pem ubuntu@10.2.11.98
...roject.pem ub

```
root@r1:~# zeekctl check
Hint: Run the zeekctl "deploy" command to get started.
logger-1 scripts are ok.
manager scripts are ok.
proxy-1 scripts are ok.
worker-1 scripts are ok.
worker-2 scripts are ok.
```

Step 7 : Configure Seek Cluster

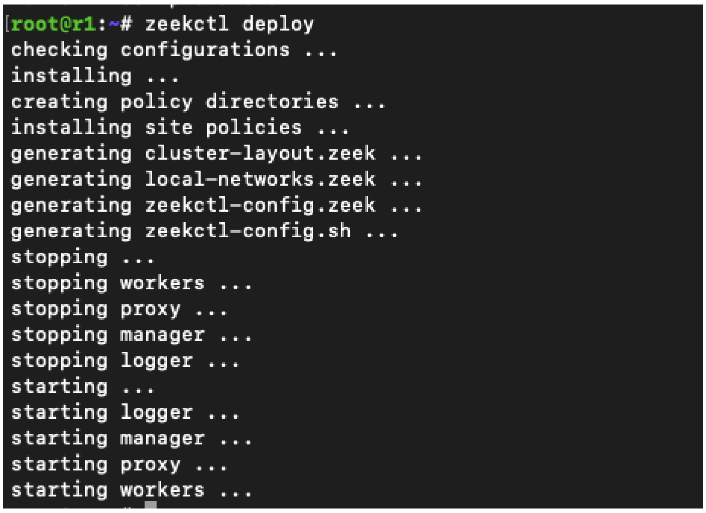
- Sudo /opt/zeek/etc/node.cfg



```
root@r1:~# cat /opt/zeek/etc/node.cfg
# Example ZeekControl node configuration.
#
# This example has a standalone node ready to go except for possibly changing
# the sniffing interface.

# This is a complete standalone configuration.  Most likely you will
# only need to change the interface.
#[zeek]
#type=standalone
#host=localhost
#interface=eth0

## Below is an example clustered configuration. If you use this,
## remove the [zeek] node above.

[logger-1]
type=logger
host=192.168.20.11
#
[manager]
type=manager
host=192.168.20.11
#
[proxy-1]
type=proxy
host=192.168.20.11
#
[worker-1]
type=worker
host=192.168.20.11
interface=ens5
#
[worker-2]
type=worker
host=localhost
interface=lo
```

Step 8 : Deploy ZeekControl Configurations

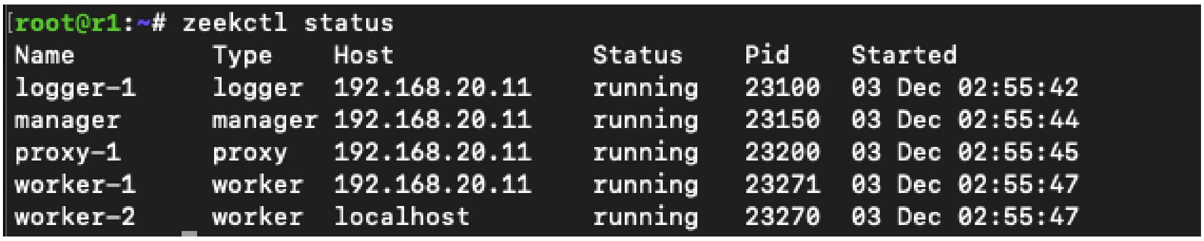
- Zeekctl Deploy



```
root@r1:~# zeekctl deploy
checking configurations ...
installing ...
creating policy directories ...
installing site policies ...
generating cluster-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping workers ...
stopping proxy ...
stopping manager ...
stopping logger ...
starting ...
starting logger ...
starting manager ...
starting proxy ...
starting workers ...
```

Step 9: Check the status of Zeek Instance

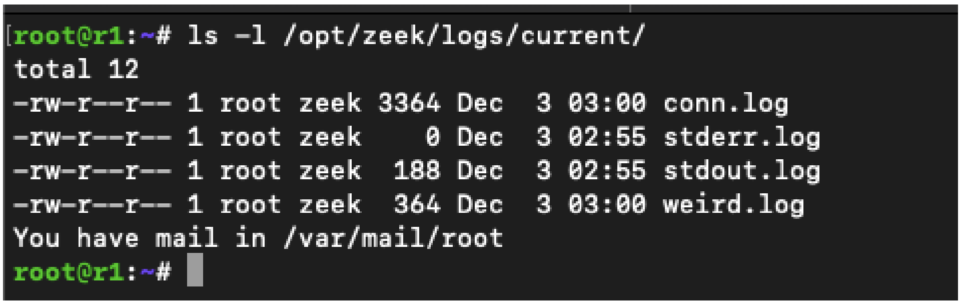
- Zeekctl status



```
root@r1:~# zeekctl status
Name         Type    Host            Status    Pid    Started
logger-1     logger  192.168.20.11   running   23100  03 Dec 02:55:42
manager      manager 192.168.20.11   running   23150  03 Dec 02:55:44
proxy-1      proxy   192.168.20.11   running   23200  03 Dec 02:55:45
worker-1     worker  192.168.20.11   running   23271  03 Dec 02:55:47
worker-2     worker  localhost       running   23270  03 Dec 02:55:47
```

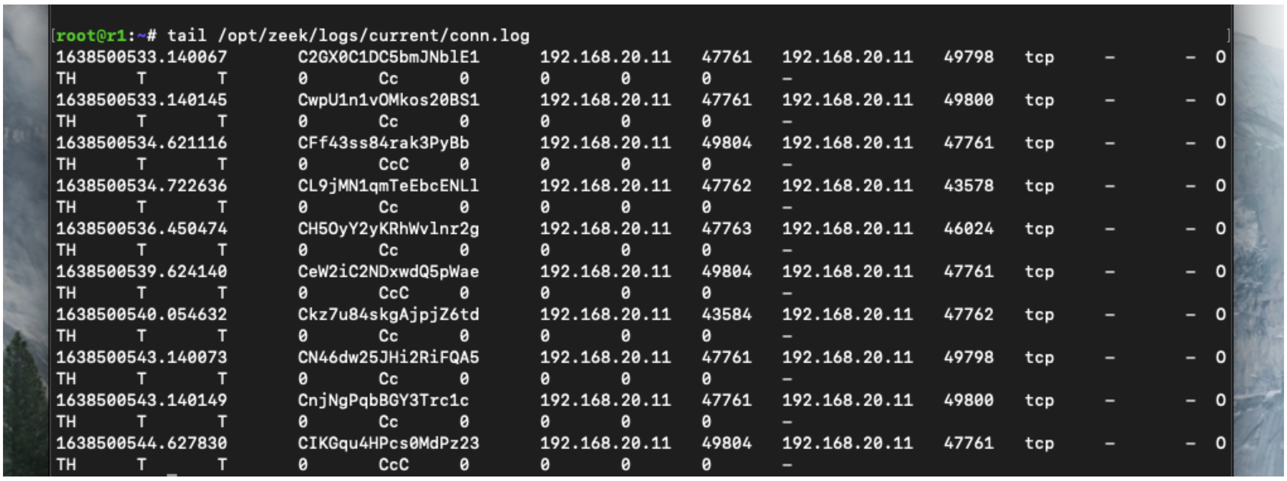
Step 10: Checking Zeek Logs

- Ls -l /opt/zeek/logs/current/



```
root@r1:~# ls -l /opt/zeek/logs/current/
total 12
-rw-r--r-- 1 root zeek 3364 Dec  3 03:00 conn.log
-rw-r--r-- 1 root zeek    0 Dec  3 02:55 stderr.log
-rw-r--r-- 1 root zeek  188 Dec  3 02:55 stdout.log
-rw-r--r-- 1 root zeek  364 Dec  3 03:00 weird.log
You have mail in /var/mail/root
root@r1:~#
```

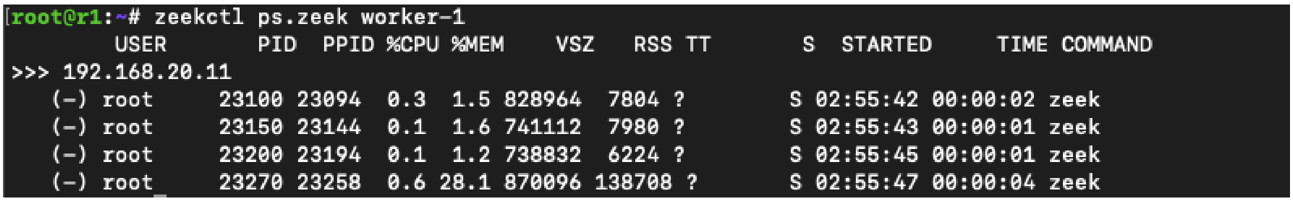
- Sample conn.log
    - tail /opt/zeek/logs/current/conn.log



```
[root@r1:~# tail /opt/zeek/logs/current/conn.log
1638500533.140067       C2GX0C1DC5bmJNblE1      192.168.20.11   47761   192.168.20.11   49798   tcp     -       -  0
TH      T       T       0       Cc      0       0       0       0       -
1638500533.140145       CwpU1n1vOMkos20BS1      192.168.20.11   47761   192.168.20.11   49800   tcp     -       -  0
TH      T       T       0       Cc      0       0       0       0       -
1638500534.621116       CFf43ss84rak3PyBb       192.168.20.11   49804   192.168.20.11   47761   tcp     -       -  0
TH      T       T       0       CcC     0       0       0       0       -
1638500534.722636       CL9jMN1qmTeEbcENLl      192.168.20.11   47762   192.168.20.11   43578   tcp     -       -  0
TH      T       T       0       Cc      0       0       0       0       -
1638500536.450474       CH5OyY2yKRhWvlnr2g      192.168.20.11   47763   192.168.20.11   46024   tcp     -       -  0
TH      T       T       0       Cc      0       0       0       0       -
1638500539.624140       CeW2iC2NDxwdQ5pWae      192.168.20.11   49804   192.168.20.11   47761   tcp     -       -  0
TH      T       T       0       CcC     0       0       0       0       -
1638500540.054632       Ckz7u84skgAjpjZ6td      192.168.20.11   43584   192.168.20.11   47762   tcp     -       -  0
TH      T       T       0       Cc      0       0       0       0       -
1638500543.140073       CN46dw25JHi2RiFQA5      192.168.20.11   47761   192.168.20.11   49798   tcp     -       -  0
TH      T       T       0       Cc      0       0       0       0       -
1638500543.140149       CnjNgPqbBGY3Trc1c       192.168.20.11   47761   192.168.20.11   49800   tcp     -       -  0
TH      T       T       0       Cc      0       0       0       0       -
1638500544.627830       CIKGqu4HPcs0MdPz23      192.168.20.11   49804   192.168.20.11   47761   tcp     -       -  0
TH      T       T       0       CcC     0       0       0       0       -
```

Step 11: Checking Zeek Node Process

- zeekctl ps.zeek < node > ; here worker-1



```
[root@r1:~# zeekctl ps.zeek worker-1
        USER        PID   PPID %CPU %MEM    VSZ    RSS TT       S  STARTED      TIME COMMAND
>>> 192.168.20.11
   (-) root      23100 23094  0.3  1.5 828964   7804 ?        S 02:55:42 00:00:02 zeek
   (-) root      23150 23144  0.1  1.6 741112   7980 ?        S 02:55:43 00:00:01 zeek
   (-) root      23200 23194  0.1  1.2 738832   6224 ?        S 02:55:45 00:00:01 zeek
   (-) root      23270 23258  0.6 28.1 870096 138708 ?        S 02:55:47 00:00:04 zeek
```

- Therefore, in this topology IDS is placed in Router 1 and its helps and monitors the incoming traffic and notifies the user incase of attack.