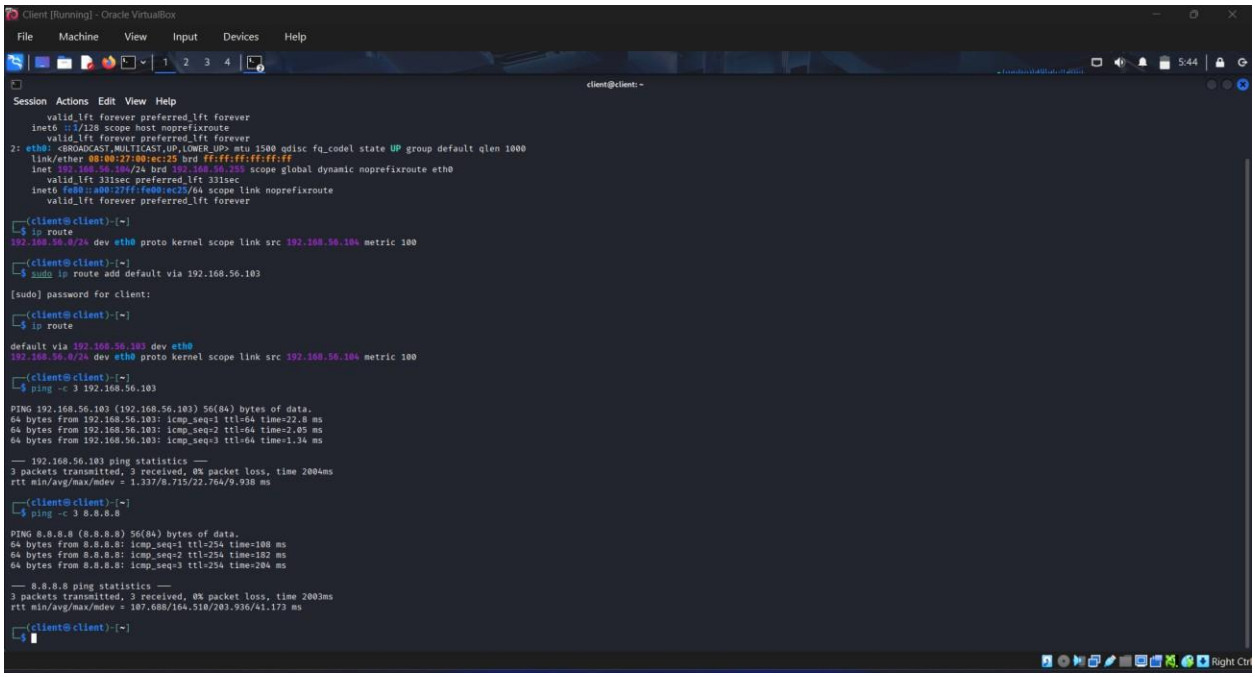
Proxy DNS Service Implementation on Internet Gateway

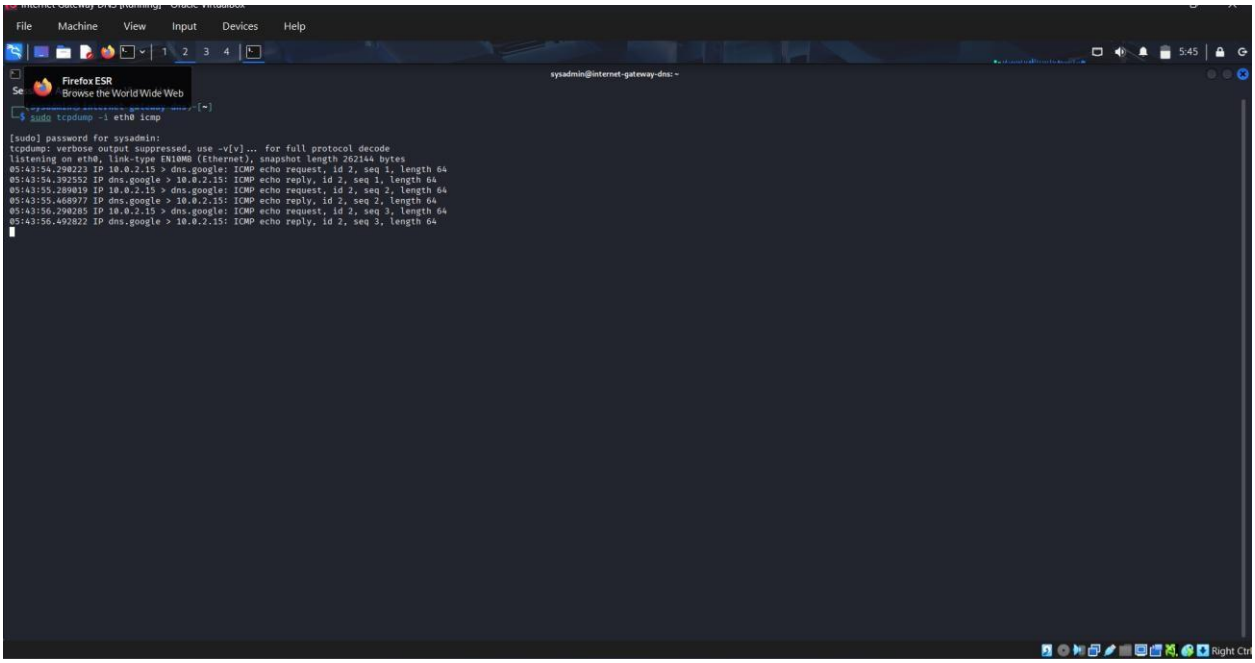
1. Introduction

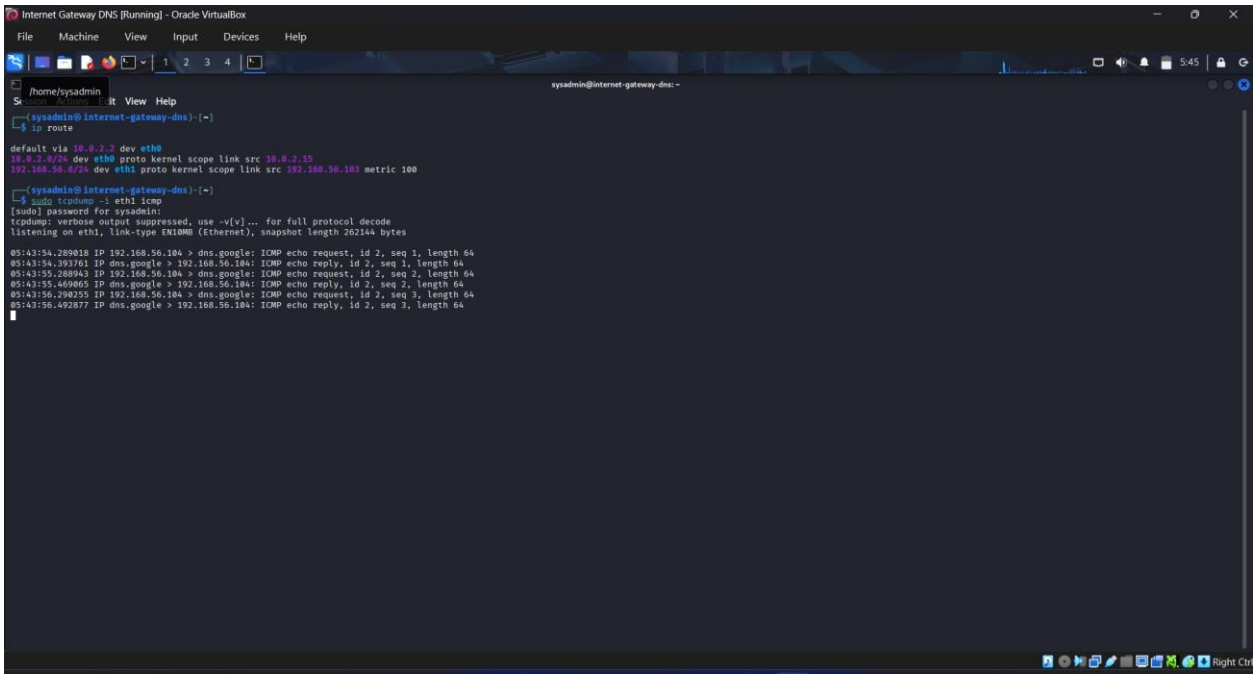
In this assignment, we implemented a Proxy DNS service on a Kali Linux Internet Gateway. The goal was to provide DNS resolution for Client PCs using a secure upstream DNS server. We used:

- Unbound DNS server as the authoritative DNS for the local LAN (Client PCs).
- DNSCrypt-proxy as the upstream server to encrypt DNS queries between the gateway and public DNS servers.

This ensures that the client receives DNS responses while maintaining privacy and integrity of queries on the internet.







2. System Architecture Gateway VM:

- eth0 → Internet-facing interface
- eth1 → LAN interface, connected to Client PC

Client VM: - Single interface connected to the LAN - Uses Gateway VM for DNS resolution and internet access

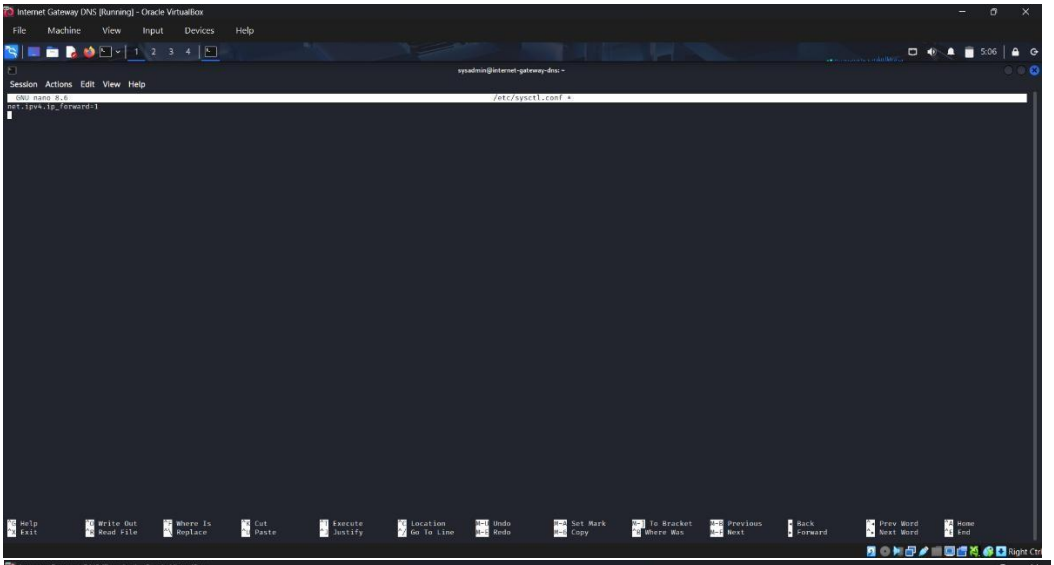
DNS Flow: Client PC –> Gateway (Unbound) –> DNSCrypt Proxy –> Internet DNS

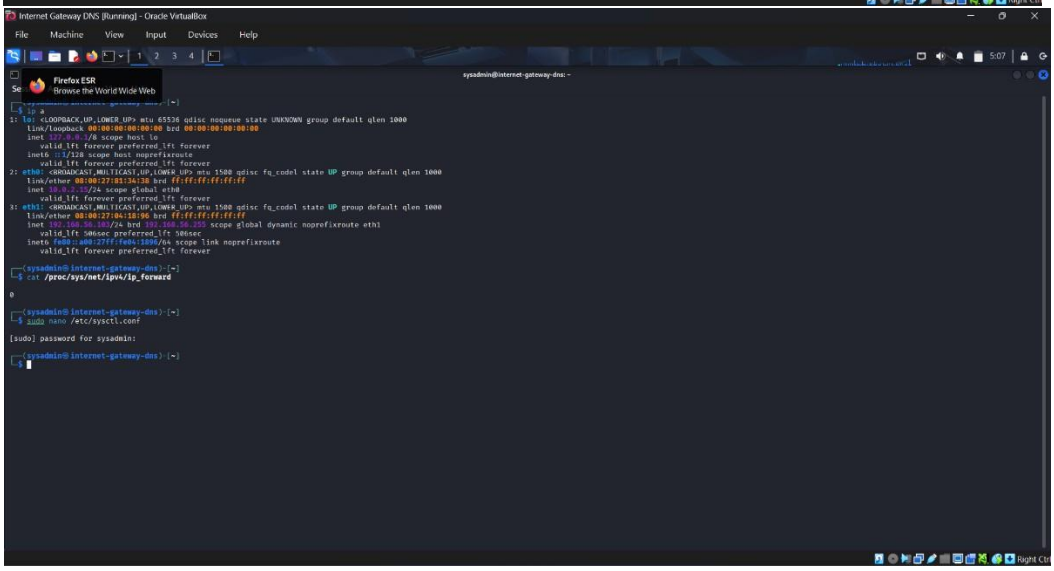
3. Implementation Steps

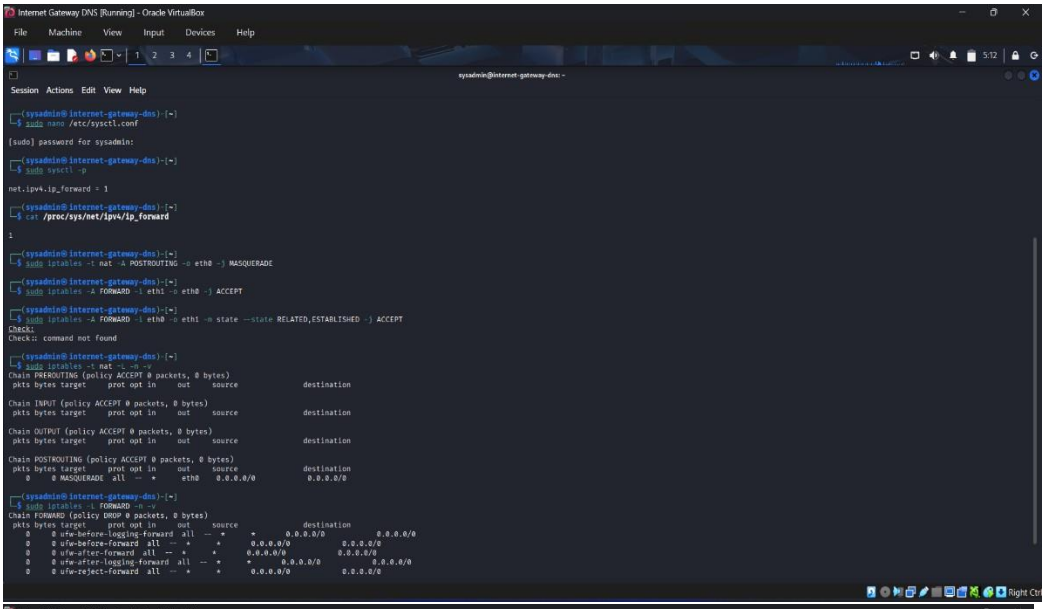
Step 1: Network Setup Gateway VM:

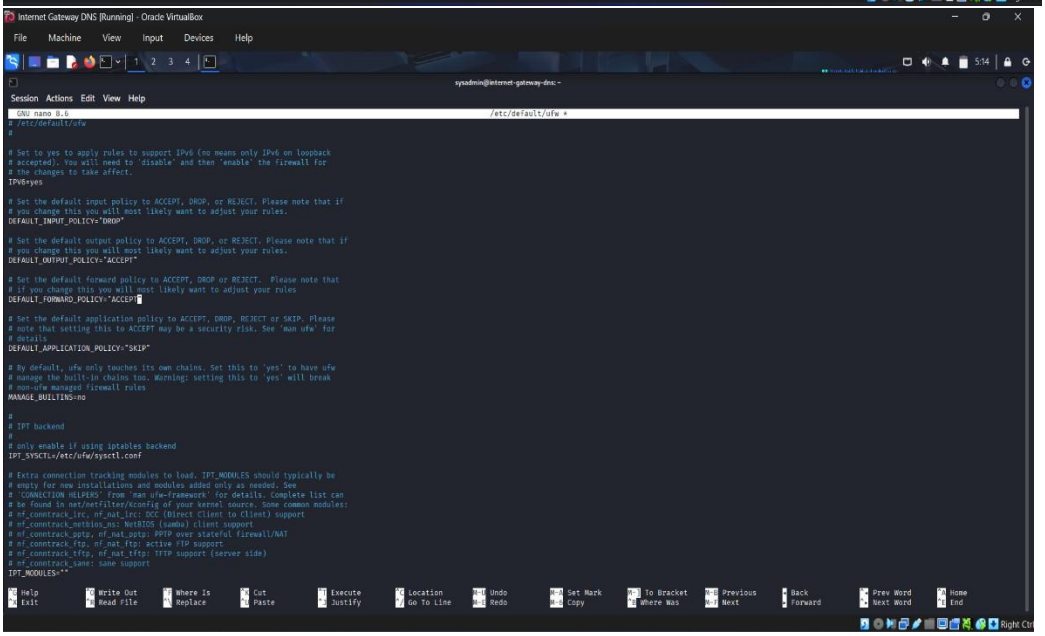
sudo sysctl -w net.ipv4.ip_forward=1
echo "net.ipv4.ip_forward = 1" | sudo tee -a /etc/sysctl.conf
sudo sysctl -p

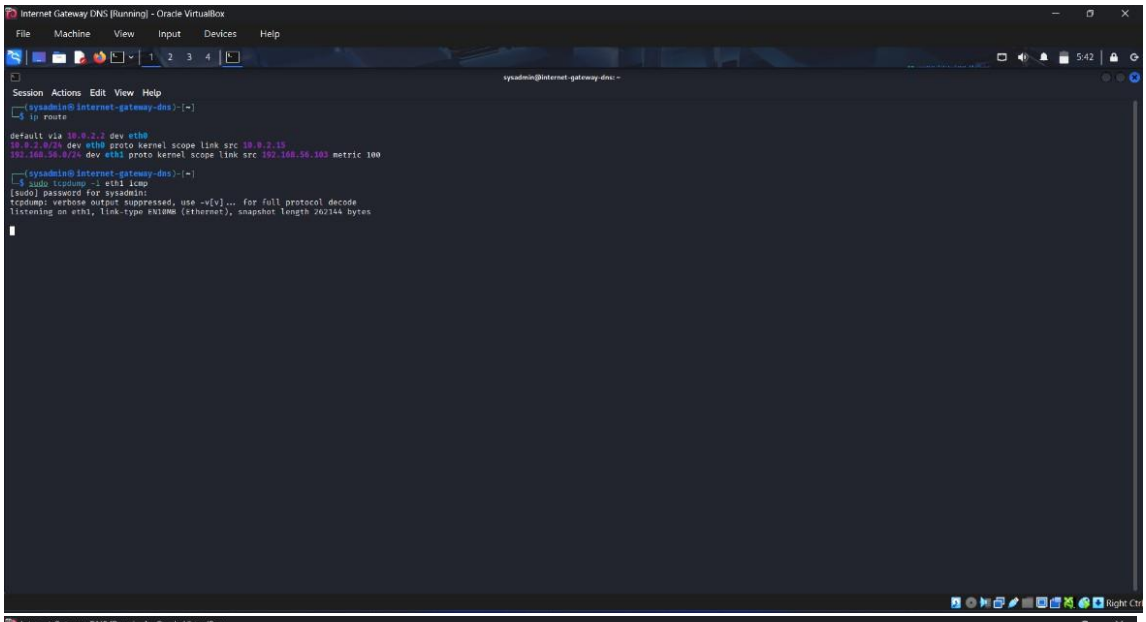
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
sudo iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT

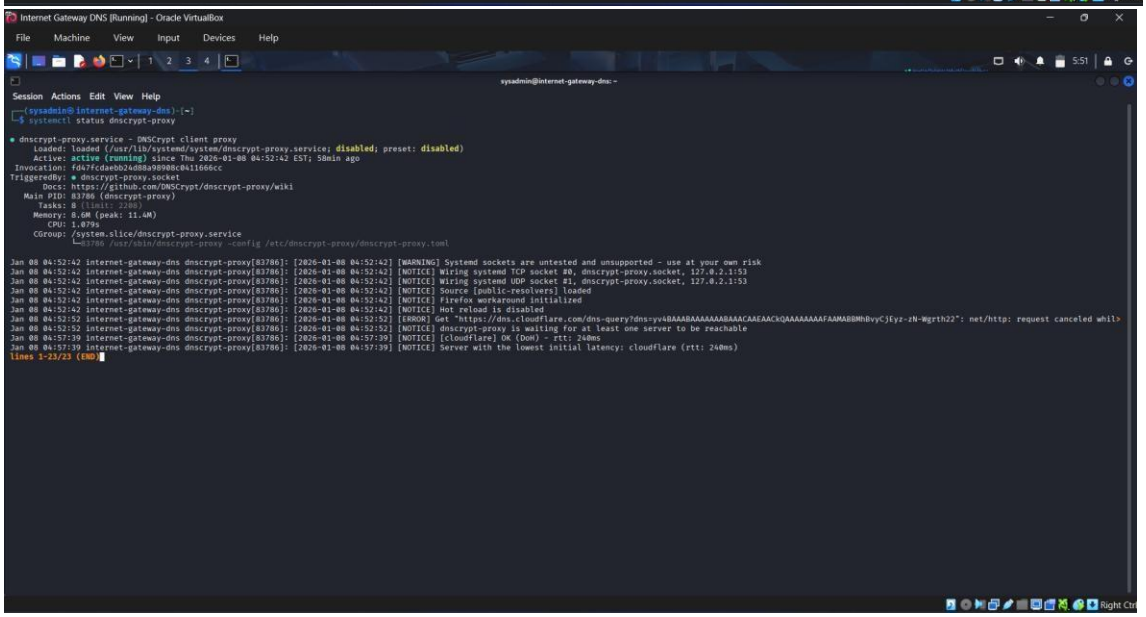


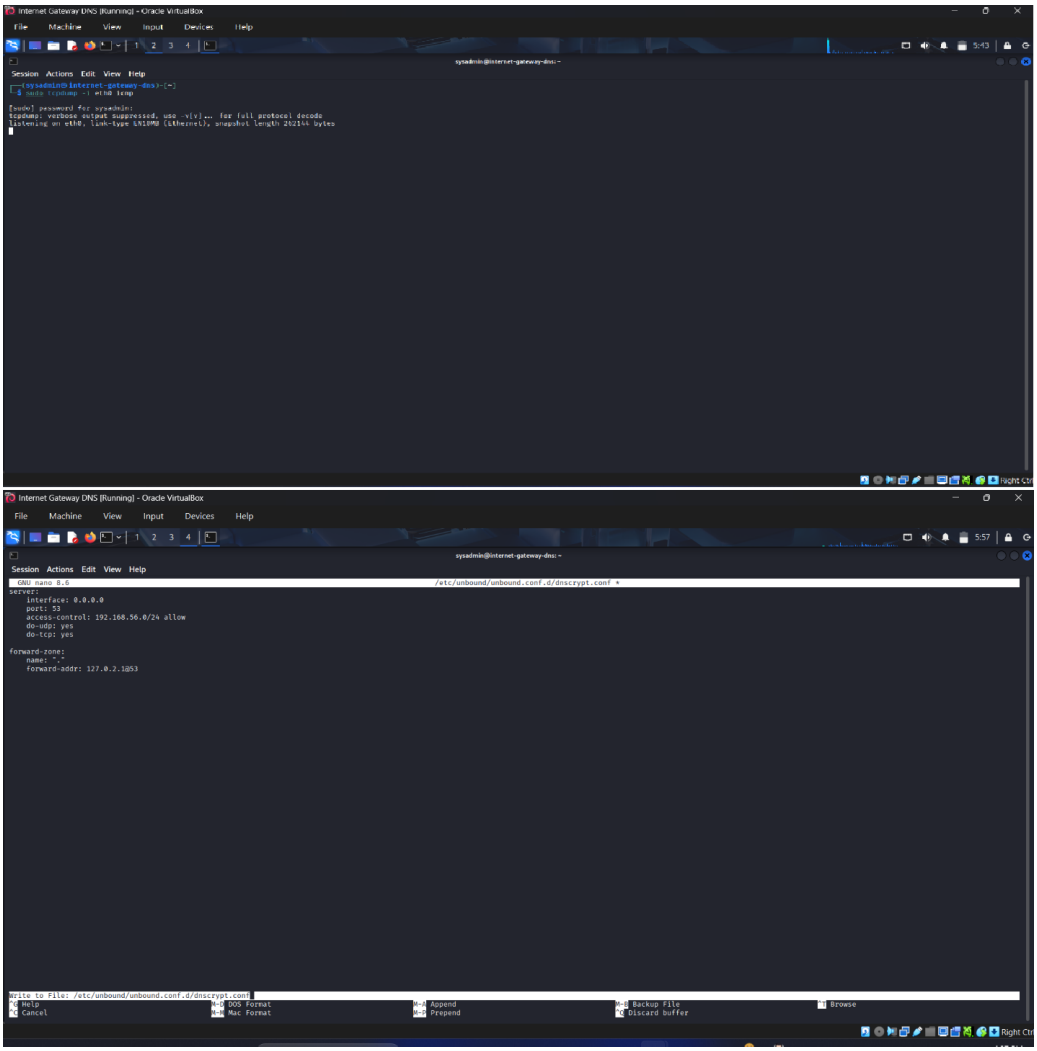



Internet Gateway DNS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
sysadmin@internet-gateway-dns: ~
Session Actions Edit View Help
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo nano /etc/sysctl.conf
[sudo] password for sysadmin:
$ sudo sysctl -p
net.ipv4.ip_forward = 1
$ cat /proc/sys/net/ipv4/ip_forward
1
$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
$ sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
$ sudo iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
Check:
Check:: command not found
$ sudo iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 MASQUERADE all -- * eth0 0.0.0.0/0 0.0.0.0/0
$ sudo iptables -L FORWARD -n -v
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ufw-before-logging-forward all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 ufw-before-forward all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 ufw-after-forward all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 ufw-after-logging-forward all -- * * 0.0.0.0/0 0.0.0.0/0
0 0 ufw-reject-forward all -- * * 0.0.0.0/0 0.0.0.0/0
Right Ctrl


Internet Gateway DNS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
sysadmin@internet-gateway-dns: ~
Session Actions Edit View Help
GNU nano 8.6 /etc/default/ufw *
/etc/default/ufw
#
# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=yes
# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="DROP"
# Set the default output policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_OUTPUT_POLICY="ACCEPT"
# Set the default forward policy to ACCEPT, DROP or REJECT. Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="ACCEPT"
# Set the default application policy to ACCEPT, DROP, REJECT or SKIP. Please
# note that setting this to ACCEPT may be a security risk. See 'man ufw' for
# details
DEFAULT_APPLICATION_POLICY="SKIP"
# By default, ufw only touches its own chains. Set this to 'yes' to have ufw
# manage the built-in chains too. Warning: setting this to 'yes' will break
# non-ufw managed firewall rules
MANAGE_BUILTINS=no
#
IPT backend
#
# only enable if using iptables backend
IPT_SYSCTL=/etc/ufw/sysctl.conf
# Extra connection tracking modules to load. IPT_MODULES should typically be
# empty for new installations and modules added only as needed. See
# 'CONNECTION HELPERS' from 'man ufw-framework' for details. Complete list can
# be found in net/netfilter/Kconfig of your kernel source. Some common modules:
# nf_conntrack_irc, nf_nat_irc: DCC (Direct Client to Client) support
# nf_conntrack_netbios_ns: NetBIOS (samba) client support
# nf_conntrack_pptp, nf_nat_pptp: PPTP over stateful firewall/NAT
# nf_conntrack_ftp, nf_nat_ftp: active FTP support
# nf_conntrack_tftp, nf_nat_tftp: TFTP support (server side)
# nf_conntrack_sane: sane support
IPT_MODULES=""
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-P Previous M-B Back ^← Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-N Next ^→ Forward ^Y Next Word ^E End
Right Ctrl


Internet Gateway DNS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
sysadmin@internet-gateway-dns: ~
Session Actions Edit View Help
(sysadmin㉿internet-gateway-dns)-[~]
$ ip route
default via 10.0.2.2 dev eth0
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15
192.168.56.0/24 dev eth1 proto kernel scope link src 192.168.56.103 metric 100
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo tcpdump -i eth1 icmp
[sudo] password for sysadmin:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes


Internet Gateway DNS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
sysadmin@internet-gateway-dns: ~
Session Actions Edit View Help
(sysadmin㉿internet-gateway-dns)-[~]
$ systemctl status dnscrypt-proxy
● dnscrypt-proxy.service - DNSCrypt client proxy
Loaded: loaded (/usr/lib/systemd/system/dnscrypt-proxy.service; disabled; preset: disabled)
Active: active (running) since Thu 2026-01-08 04:52:42 EST; 58min ago
Invocation: fdc7fcdaebb24d88a98908c041166cc
TriggeredBy: ● dnscrypt-proxy.socket
Docs: https://github.com/DNSCrypt/dnscrypt-proxy/wiki
Main PID: 83786 (dnscrypt-proxy)
Tasks: 8 (limit: 2288)
Memory: 8.6M (peak: 11.4M)
CPU: 1.879s
CGroup: /system.slice/dnscrypt-proxy.service
└─83786 /usr/sbin/dnscrypt-proxy -config /etc/dnscrypt-proxy/dnscrypt-proxy.toml
Jan 08 04:52:42 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:52:42] [WARNING] Systemd sockets are untested and unsupported - use at your own risk
Jan 08 04:52:42 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:52:42] [NOTICE] Wiring systemd TCP socket #0, dnscrypt-proxy.socket, 127.0.2.1:53
Jan 08 04:52:42 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:52:42] [NOTICE] Wiring systemd UDP socket #1, dnscrypt-proxy.socket, 127.0.2.1:53
Jan 08 04:52:42 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:52:42] [NOTICE] Source [public-resolvers] loaded
Jan 08 04:52:42 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:52:42] [NOTICE] Firefox workaround initialized
Jan 08 04:52:42 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:52:42] [NOTICE] Hot reload is disabled
Jan 08 04:52:52 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:52:52] [ERROR] Get "https://dns.cloudflare.com/dns-query?dns=yv4BAAABAAAAAAABAAACAAEAACkQAAAAAAAAFAAMAABBMhBvyCjEyz-zN-Wgrth22": net/http: request canceled whil>
Jan 08 04:52:52 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:52:52] [NOTICE] dnscrypt-proxy is waiting for at least one server to be reachable
Jan 08 04:57:39 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:57:39] [NOTICE] [cloudflare] OK (DoH) - rtt: 240ms
Jan 08 04:57:39 internet-gateway-dns dnscrypt-proxy[83786]: [2026-01-08 04:57:39] [NOTICE] Server with the lowest initial latency: cloudflare (rtt: 240ms)
lines 1-23/23 (END)



Step 2: DNS Service Setup on Gateway Install Unbound and DNSCrypt-proxy:

sudo apt update && sudo apt install unbound dnscrypt-proxy -y

Unbound Configuration (/etc/unbound/unbound.conf):

server:
    interface: 0.0.0.0
    port: 53
    access-control: 192.168.56.0/24 allow
    do-udp: yes
    do-tcp: yes
    do-not-query-localhost: no
    username: "root"

forward-zone:

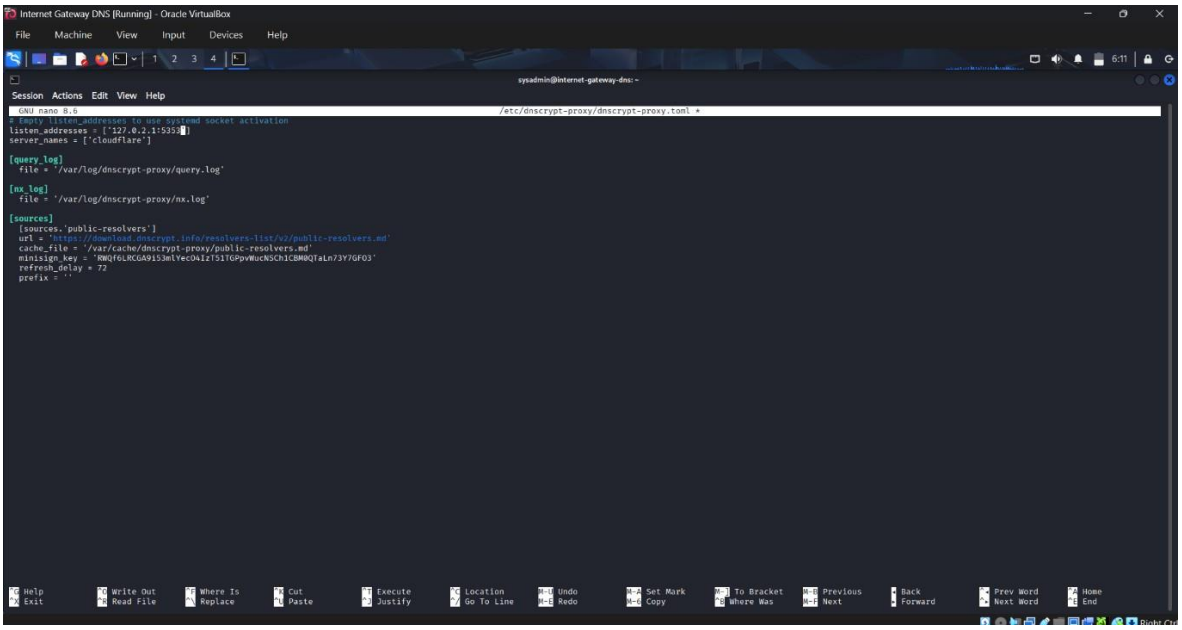
name: "."
forward-addr: 127.0.2.1@5353

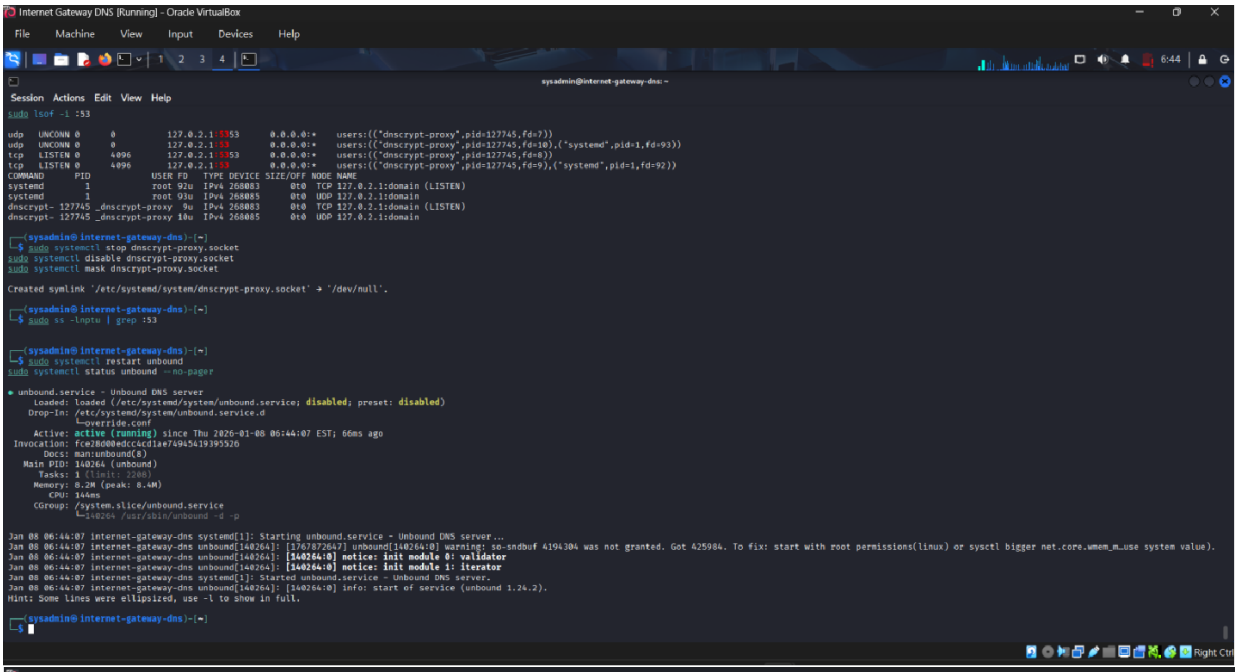
DNSCrypt Proxy Configuration (/etc/dnscrypt-proxy/dnscrypt-proxy.toml): - Listening port: 5353 on 127.0.2.1 - Use public resolvers (Cloudflare, Quad9)

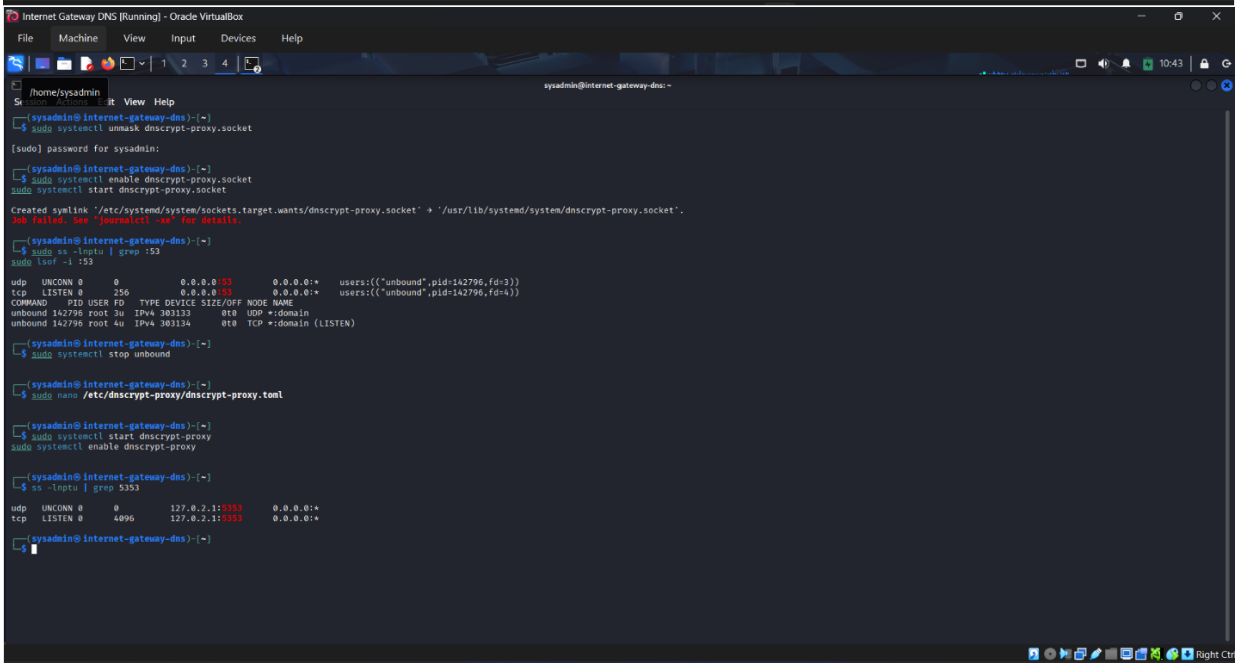
Step 3: Start and Enable Services

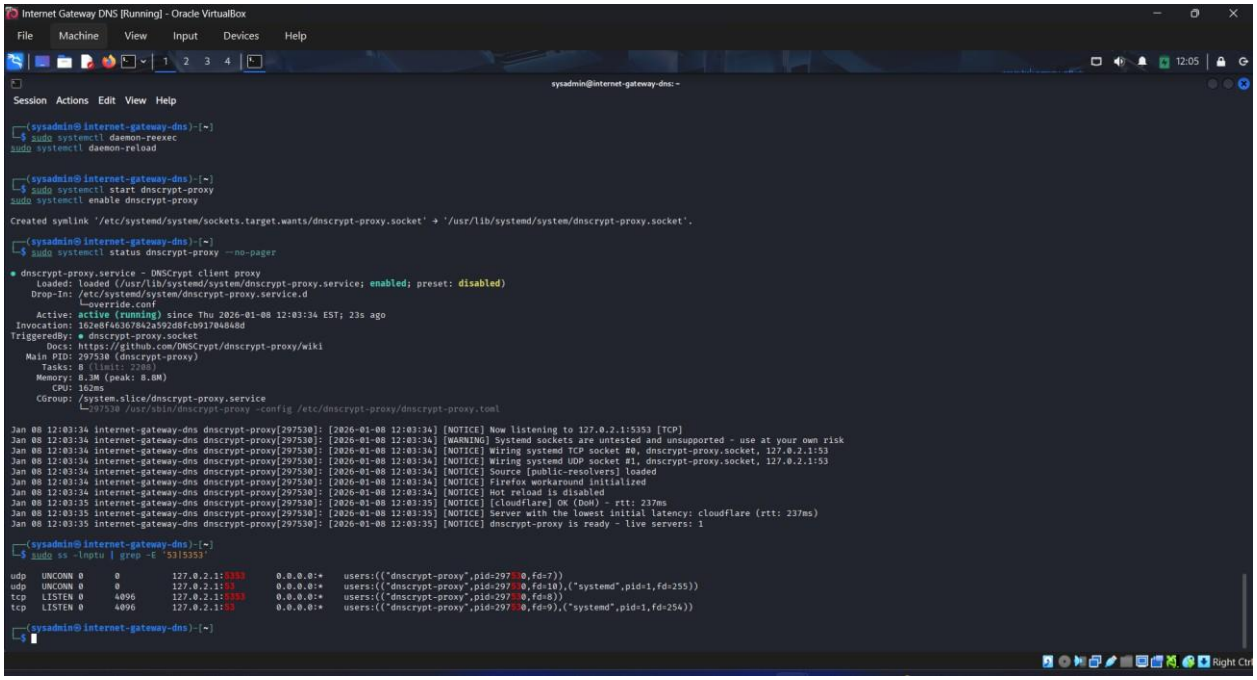
sudo systemctl restart unbound
sudo systemctl enable unbound

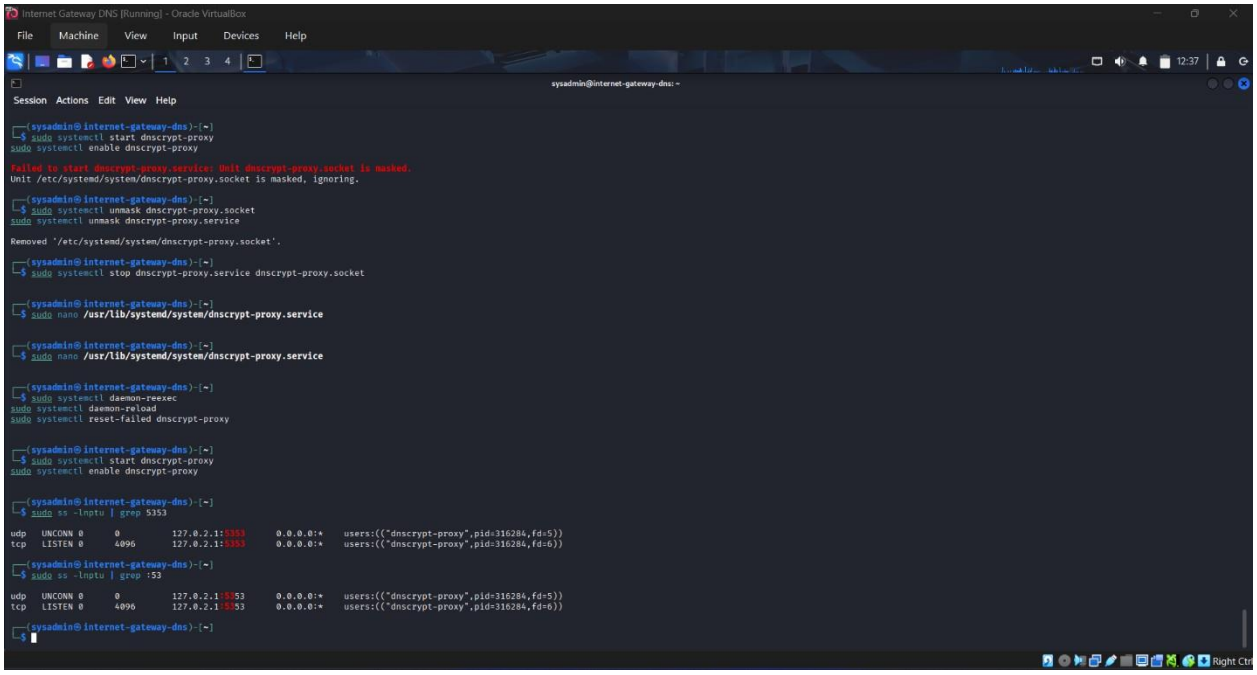
sudo systemctl start dnscrypt-proxy
sudo systemctl enable dnscrypt-proxy




Internet Gateway DNS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
sysadmin@internet-gateway-dns: ~
Session Actions Edit View Help
sudo lsof -i :53
udp UNCONN 0 0 127.0.2.1:5353 0.0.0.0:* users:(("dnscrypt-proxy",pid=127745,fd=7))
udp UNCONN 0 0 127.0.2.1:53 0.0.0.0:* users:(("dnscrypt-proxy",pid=127745,fd=10),("systemd",pid=1,fd=93))
tcp LISTEN 0 4096 127.0.2.1:5353 0.0.0.0:* users:(("dnscrypt-proxy",pid=127745,fd=8))
tcp LISTEN 0 4096 127.0.2.1:53 0.0.0.0:* users:(("dnscrypt-proxy",pid=127745,fd=9),("systemd",pid=1,fd=92))
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
systemd 1 root 92u IPv4 268083 0t0 TCP 127.0.2.1:domain (LISTEN)
systemd 1 root 93u IPv4 268085 0t0 UDP 127.0.2.1:domain
dnscrypt- 127745 _dnscrypt-proxy 9u IPv4 268083 0t0 TCP 127.0.2.1:domain (LISTEN)
dnscrypt- 127745 _dnscrypt-proxy 10u IPv4 268085 0t0 UDP 127.0.2.1:domain
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl stop dnscrypt-proxy.socket
sudo systemctl disable dnscrypt-proxy.socket
sudo systemctl mask dnscrypt-proxy.socket
Created symlink '/etc/systemd/system/dnscrypt-proxy.socket' → '/dev/null'.
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo ss -lnptu | grep :53
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl restart unbound
sudo systemctl status unbound --no-pager
● unbound.service - Unbound DNS server
Loaded: loaded (/etc/systemd/system/unbound.service; disabled; preset: disabled)
Drop-In: /etc/systemd/system/unbound.service.d
└override.conf
Active: active (running) since Thu 2026-01-08 06:44:07 EST; 66ms ago
Invocation: fce28600edcc4cd1ae74945419395526
Docs: man:unbound(8)
Main PID: 140264 (unbound)
Tasks: 1 (limit: 2268)
Memory: 8.2M (peak: 8.4M)
CPU: 144ms
CGroup: /system.slice/unbound.service
└140264 /usr/sbin/unbound -d -p
Jan 08 06:44:07 internet-gateway-dns systemd[1]: Starting unbound.service - Unbound DNS server...
Jan 08 06:44:07 internet-gateway-dns unbound[140264]: [1767872647] unbound[140264:0] warning: so-sndbuf 4194304 was not granted. Got 425984. To fix: start with root permissions(linux) or sysctl bigger net.core.wmem_m…use system value).
Jan 08 06:44:07 internet-gateway-dns unbound[140264]: [140264:0] notice: init module 0: validator
Jan 08 06:44:07 internet-gateway-dns unbound[140264]: [140264:0] notice: init module 1: iterator
Jan 08 06:44:07 internet-gateway-dns systemd[1]: Started unbound.service - Unbound DNS server.
Jan 08 06:44:07 internet-gateway-dns unbound[140264]: [140264:0] info: start of service (unbound 1.24.2).
Hint: Some lines were ellipsized, use -l to show in full.
(sysadmin㉿internet-gateway-dns)-[~]
$
Right Ctrl

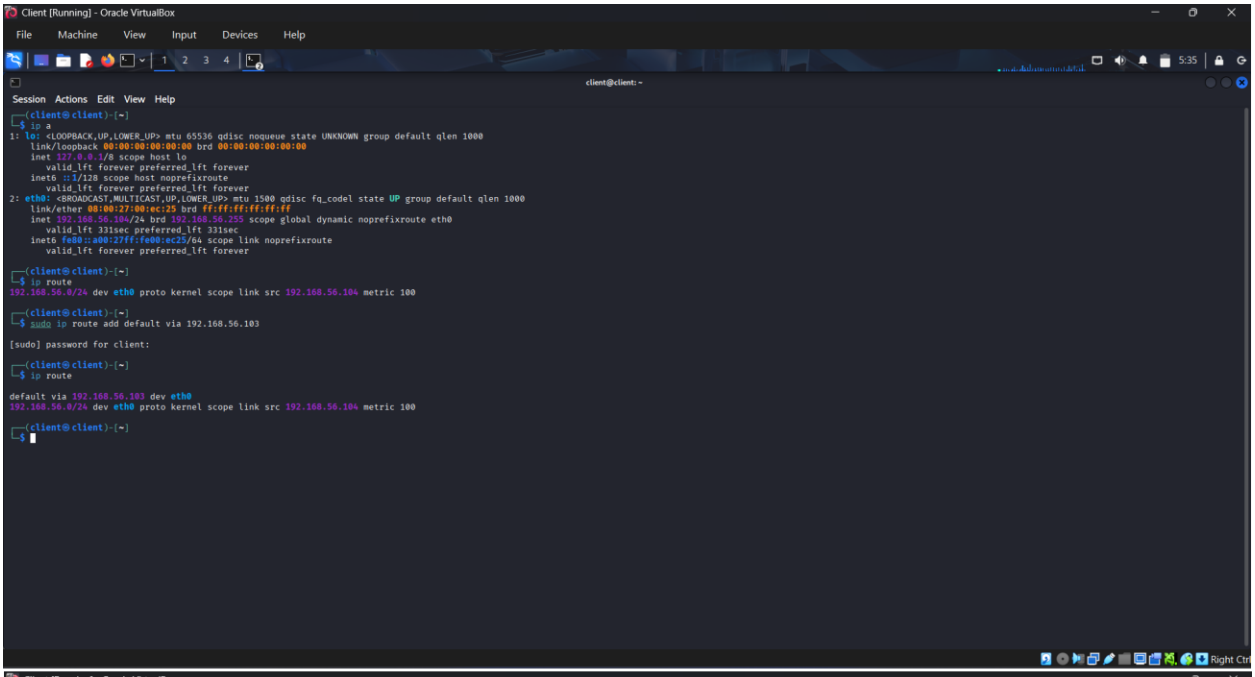

Internet Gateway DNS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
/home/sysadmin
sysadmin@internet-gateway-dns: ~
View Help
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl unmask dnscrypt-proxy.socket
[sudo] password for sysadmin:
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl enable dnscrypt-proxy.socket
sudo systemctl start dnscrypt-proxy.socket
Created symlink '/etc/systemd/system/sockets.target.wants/dnscrypt-proxy.socket' → '/usr/lib/systemd/system/dnscrypt-proxy.socket'.
Job failed. See "journalctl -xe" for details.
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo ss -lnptu | grep :53
sudo lsof -i :53
udp UNCONN 0 0 0.0.0.0:53 0.0.0.0:* users:(("unbound",pid=142796,fd=3))
tcp LISTEN 0 256 0.0.0.0:53 0.0.0.0:* users:(("unbound",pid=142796,fd=4))
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
unbound 142796 root 3u IPv4 303133 0t0 UDP *:domain
unbound 142796 root 4u IPv4 303134 0t0 TCP *:domain (LISTEN)
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl stop unbound
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo nano /etc/dnscrypt-proxy/dnscrypt-proxy.toml
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl start dnscrypt-proxy
sudo systemctl enable dnscrypt-proxy
(sysadmin㉿internet-gateway-dns)-[~]
$ ss -lnptu | grep 5353
udp UNCONN 0 0 127.0.2.1:5353 0.0.0.0:*
tcp LISTEN 0 4096 127.0.2.1:5353 0.0.0.0:*
(sysadmin㉿internet-gateway-dns)-[~]
$
Right Ctrl

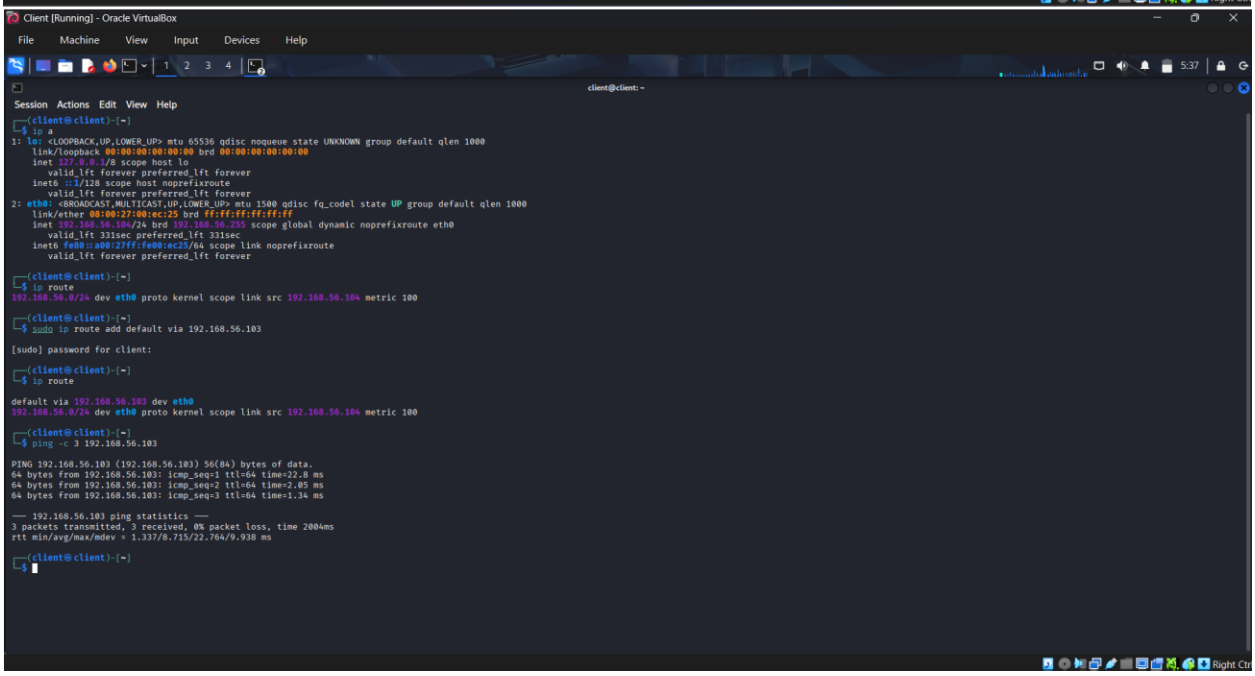

Internet Gateway DNS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
sysadmin@internet-gateway-dns: ~
Session Actions Edit View Help
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl daemon-reexec
sudo systemctl daemon-reload
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl start dnscrypt-proxy
sudo systemctl enable dnscrypt-proxy
Created symlink '/etc/systemd/system/sockets.target.wants/dnscrypt-proxy.socket' → '/usr/lib/systemd/system/dnscrypt-proxy.socket'.
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl status dnscrypt-proxy --no-pager
● dnscrypt-proxy.service - DNSCrypt client proxy
Loaded: loaded (/usr/lib/systemd/system/dnscrypt-proxy.service; enabled; preset: disabled)
Drop-In: /etc/systemd/system/dnscrypt-proxy.service.d
└─override.conf
Active: active (running) since Thu 2026-01-08 12:03:34 EST; 23s ago
Invocation: 162e8f46367842a592d8fcb91704848d
TriggeredBy: ● dnscrypt-proxy.socket
Docs: https://github.com/DNSCrypt/dnscrypt-proxy/wiki
Main PID: 297530 (dnscrypt-proxy)
Tasks: 8 (limit: 2208)
Memory: 8.3M (peak: 8.8M)
CPU: 162ms
CGroup: /system.slice/dnscrypt-proxy.service
└─297530 /usr/sbin/dnscrypt-proxy -config /etc/dnscrypt-proxy/dnscrypt-proxy.toml
Jan 08 12:03:34 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:34] [NOTICE] Now listening to 127.0.2.1:5353 [TCP]
Jan 08 12:03:34 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:34] [WARNING] Systemd sockets are untested and unsupported - use at your own risk
Jan 08 12:03:34 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:34] [NOTICE] Wiring systemd TCP socket #0, dnscrypt-proxy.socket, 127.0.2.1:53
Jan 08 12:03:34 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:34] [NOTICE] Wiring systemd UDP socket #1, dnscrypt-proxy.socket, 127.0.2.1:53
Jan 08 12:03:34 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:34] [NOTICE] Source [public-resolvers] loaded
Jan 08 12:03:34 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:34] [NOTICE] Firefox workaround initialized
Jan 08 12:03:34 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:34] [NOTICE] Hot reload is disabled
Jan 08 12:03:35 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:35] [NOTICE] [cloudflare] OK (DoH) - rtt: 237ms
Jan 08 12:03:35 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:35] [NOTICE] Server with the lowest initial latency: cloudflare (rtt: 237ms)
Jan 08 12:03:35 internet-gateway-dns dnscrypt-proxy[297530]: [2026-01-08 12:03:35] [NOTICE] dnscrypt-proxy is ready - live servers: 1
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo ss -lnptu | grep -E ':53|5353'
udp UNCONN 0 0 127.0.2.1:5353 0.0.0.0:* users:(("dnscrypt-proxy",pid=297530,fd=7))
udp UNCONN 0 0 127.0.2.1:53 0.0.0.0:* users:(("dnscrypt-proxy",pid=297530,fd=10),("systemd",pid=1,fd=255))
tcp LISTEN 0 4096 127.0.2.1:5353 0.0.0.0:* users:(("dnscrypt-proxy",pid=297530,fd=8))
tcp LISTEN 0 4096 127.0.2.1:53 0.0.0.0:* users:(("dnscrypt-proxy",pid=297530,fd=9),("systemd",pid=1,fd=254))
(sysadmin㉿internet-gateway-dns)-[~]
$
Right Ctrl

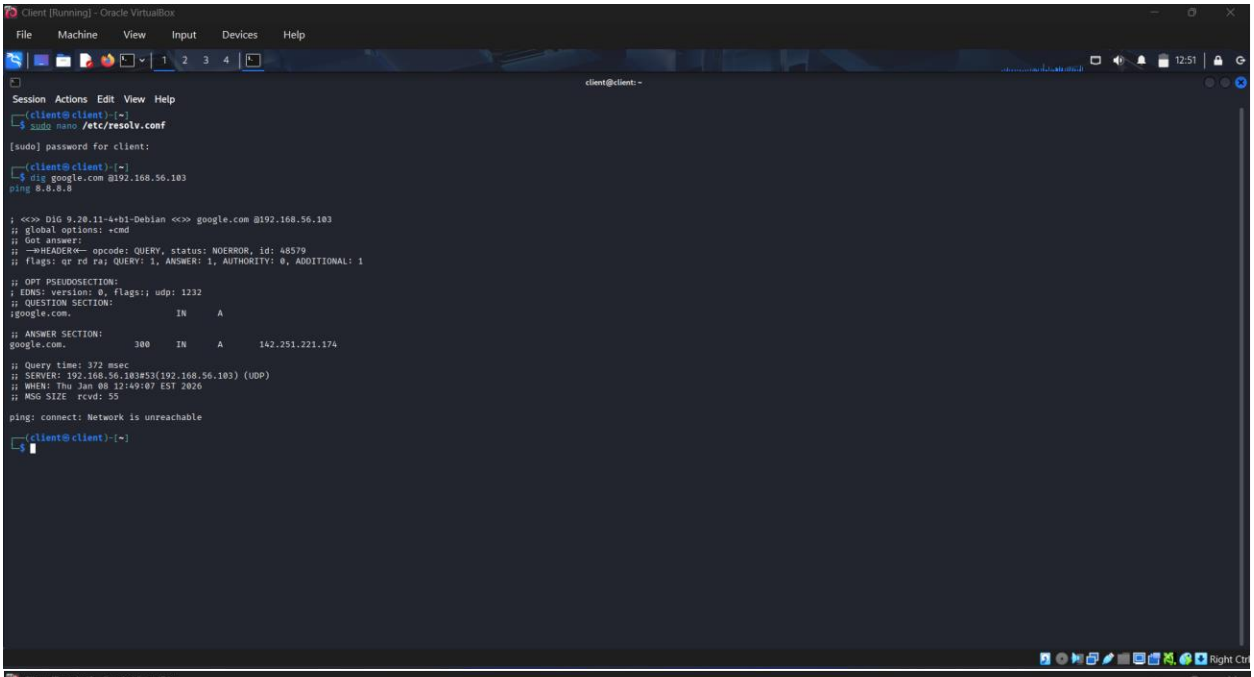

Internet Gateway DNS [Running] - Oracle VirtualBox
File Machine View Input Devices Help
sysadmin@internet-gateway-dns: ~
Session Actions Edit View Help
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl start dnscrypt-proxy
sudo systemctl enable dnscrypt-proxy
Failed to start dnscrypt-proxy.service: Unit dnscrypt-proxy.socket is masked.
Unit /etc/systemd/system/dnscrypt-proxy.socket is masked, ignoring.
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl unmask dnscrypt-proxy.socket
sudo systemctl unmask dnscrypt-proxy.service
Removed '/etc/systemd/system/dnscrypt-proxy.socket'.
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl stop dnscrypt-proxy.service dnscrypt-proxy.socket
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo nano /usr/lib/systemd/system/dnscrypt-proxy.service
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo nano /usr/lib/systemd/system/dnscrypt-proxy.service
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl daemon-reexec
sudo systemctl daemon-reload
sudo systemctl reset-failed dnscrypt-proxy
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo systemctl start dnscrypt-proxy
sudo systemctl enable dnscrypt-proxy
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo ss -lnptu | grep 5353
udp UNCONN 0 0 127.0.2.1:5353 0.0.0.0:* users:(("dnscrypt-proxy",pid=316284,fd=5))
tcp LISTEN 0 4096 127.0.2.1:5353 0.0.0.0:* users:(("dnscrypt-proxy",pid=316284,fd=6))
(sysadmin㉿internet-gateway-dns)-[~]
$ sudo ss -lnptu | grep :53
udp UNCONN 0 0 127.0.2.1:5353 0.0.0.0:* users:(("dnscrypt-proxy",pid=316284,fd=5))
tcp LISTEN 0 4096 127.0.2.1:5353 0.0.0.0:* users:(("dnscrypt-proxy",pid=316284,fd=6))
(sysadmin㉿internet-gateway-dns)-[~]
$
Right Ctrl

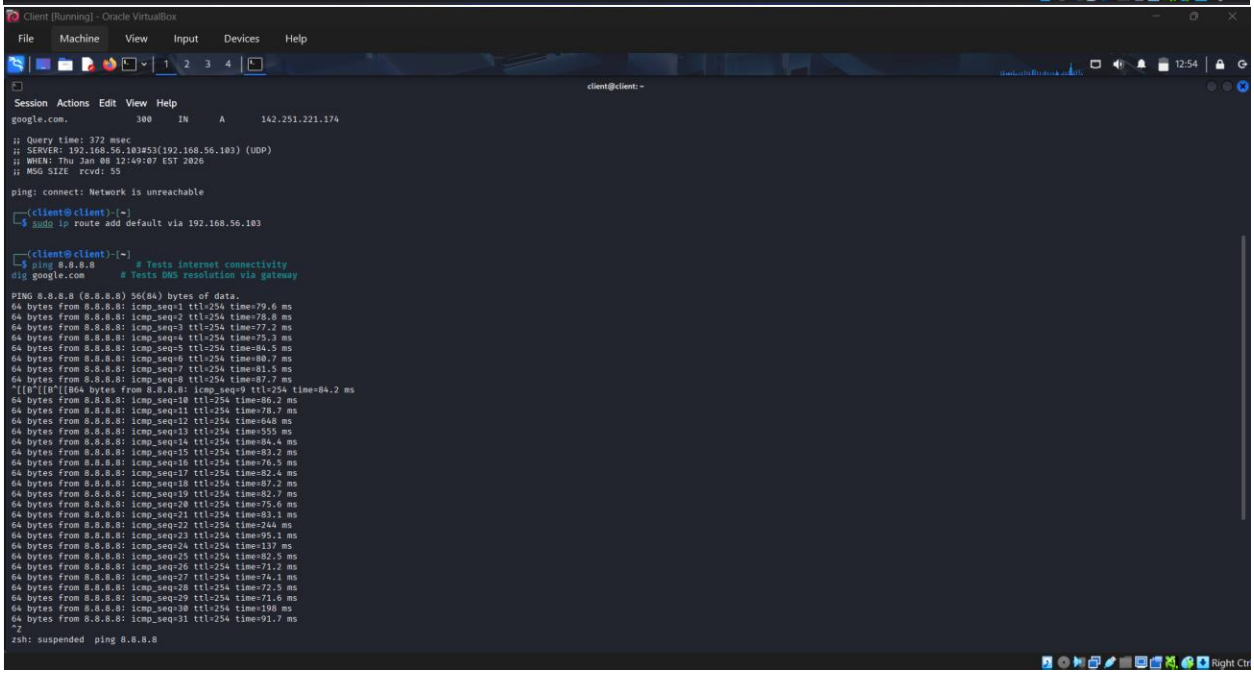
Step 4: Client Configuration

dig google.com @192.168.56.103
ping 8.8.8.8









4. Verification and Testing Gateway:

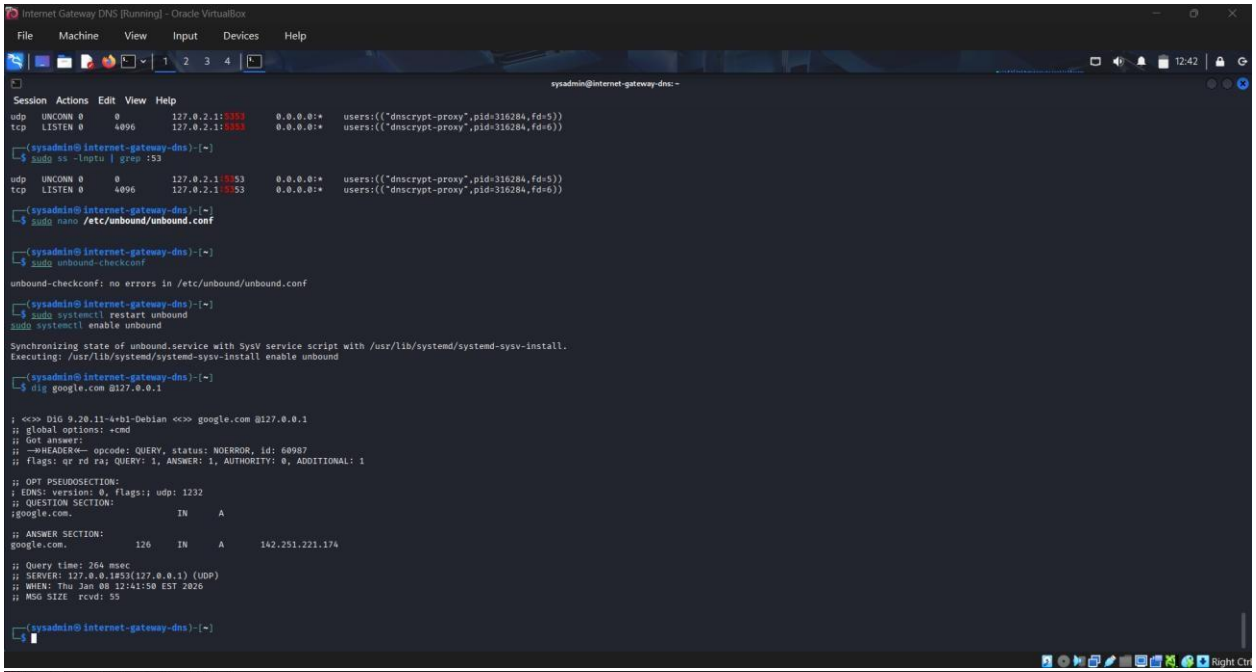
dig google.com @127.0.0.1

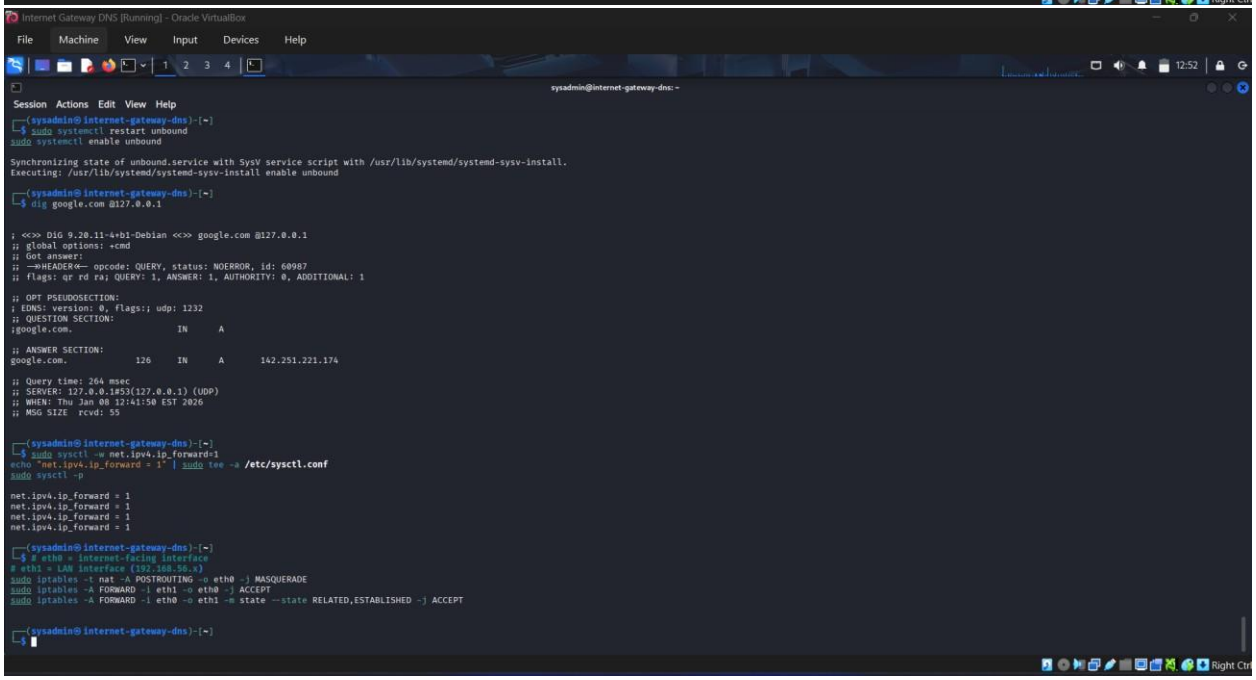
Output shows valid IP, e.g., 142.251.221.174

Client:

dig google.com @192.168.56.103
ping 8.8.8.8

- DNS resolution: Success
- Internet access: Success





5. Conclusion

- Proxy DNS service successfully implemented using Unbound and DNSCrypt-proxy.
- Client PCs can resolve DNS securely through the gateway.
- NAT and IP forwarding ensure full internet access while protecting DNS traffic.