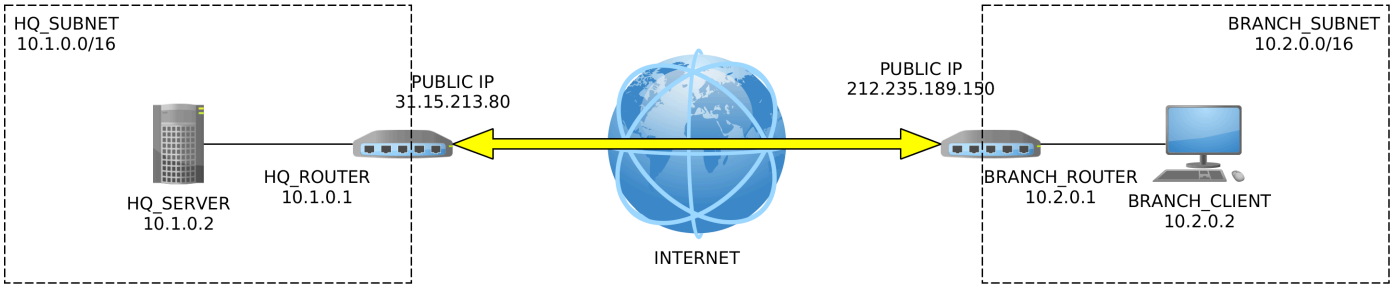
Introduction

As part of setting up a company network infrastructure, we shall set up a tunneled VPN between the headquarters and its remote branch. The following diagram illustrates the network topology:



Prerequisites

To set up the VPN, we will be using StrongSwan, which is an open-source implementation of IKE. StrongSwan is an IKE keying daemon - a program running in the background that sets up ISAKMP and IKE associations between various network points.

We will need four virtual machines:

- Two routers
- Two hosts

The routers shall have two network interfaces, while the hosts shall have a single network interface each.

Initial Setup

Preparing the ISP Machine

First, install all required software on the ISP machine, which will serve as a template. During the lab session, the ISP machine will not be running.

```
sudo apt update
sudo apt install strongswan strongswan-pki libcharon-extra-plugins apache2
wireshark
```

Note: strongswan-pki and libcharon-extra-plugins are needed for optional assignments

During Wireshark installation when asked "Should non-superusers be able to capture packets?", select yes. If you make a mistake and select no, you can change your selection by running:

```
sudo dpkg-reconfigure wireshark-common
```

Then add your user to the group wireshark:

```
sudo usermod -a -G wireshark $USER
```

Network Configuration

1. Shut down the ISP machine
2. Configure it to have 2 NICs:
    - Go to Machine > Settings > Network
    - Set Adapter 1 to NAT Network
    - Set Adapter 2 to Internal-Network

Creating Virtual Machines

Clone the ISP machine four times creating:

- hq_router
- branch_router
- hq_server
- branch_client

Note: You may create linked clones. Do not forget to reinitialize the MAC addresses.

Network Settings Configuration

HQ Router

- Adapter 1: NAT Network
- Adapter 2: Internal-Network (hq_subnet)

Branch Router

- Adapter 1: NAT Network
- Adapter 2: Internal-Network (branch_subnet)

HQ Server

- Disable Adapter 2
- Adapter 1: Internal-Network (hq_subnet)

Branch Client

- Disable Adapter 2
- Adapter 1: Internal-Network (branch_subnet)

Setting Up the Headquarters

HQ Router Configuration

1. Start hq_router
2. Edit network configuration:

```
# /etc/netplan/01-network-manager-all.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
      dhcp-identifier: mac
    enp0s8:
      addresses: [10.1.0.1/16]
```

3. Apply changes:

```
sudo netplan apply
```

4. Enable packet forwarding:

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

HQ Server Configuration

1. Start hq_server
2. Edit network configuration:

```
# /etc/netplan/01-network-manager-all.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      addresses: [10.1.0.2/16]
      routes:
        - to: default
          via: 10.1.0.1
      nameservers:
        addresses: [8.8.8.8]
```

Setting Up the Branch

Branch Router Configuration

1. Start branch_router
2. Edit network configuration:

```
# /etc/netplan/01-network-manager-all.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: true
      dhcp-identifier: mac
    enp0s8:
      addresses: [10.2.0.1/16]
```

Branch Client Configuration

1. Start branch_client
2. Edit network configuration:

```
# /etc/netplan/01-network-manager-all.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      addresses: [10.2.0.2/16]
      routes:
        - to: default
          via: 10.2.0.1
      nameservers:
        addresses: [8.8.8.8]
```

Checkpoint Verification

Verify the following connectivity:

1. Ping between hq_router and hq_server (network 10.1.0.0/16)
2. Ping between branch_router and branch_client (network 10.2.0.0/16)
3. Ping between hq_router and branch_router (using public addresses)

Creating the VPN IPsec Tunnel

HQ Router VPN Configuration

1. Configure IPsec:

```
# /etc/ipsec.conf
config setup

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        keyexchange=ikev2
```

```
        authby=secret

conn net-net
        leftsubnet=10.1.0.0/16
        leftfirewall=yes
        leftid=@hq
        right=$BRANCH_IP
        rightsubnet=10.2.0.0/16
        rightid=@branch
        auto=add
```

2. Set up pre-shared key:

```
# /etc/ipsec.secrets
@hq @branch : PSK "secret"
```

3. Restart IPsec:

```
sudo ipsec restart
```

Branch Router VPN Configuration

1. Configure IPsec:

```
# /etc/ipsec.conf
config setup

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        keyexchange=ikev2
        authby=secret

conn net-net
        leftsubnet=10.2.0.0/16
        leftid=@branch
        leftfirewall=yes
        right=$HQ_IP
        rightsubnet=10.1.0.0/16
        rightid=@hq
        auto=add
```

2. Set up pre-shared key:

```
# /etc/ipsec.secrets
@hq @branch : PSK "secret"
```

Establishing the VPN Link

1. Check IPsec status:

```
sudo ipsec status[all]
```

2. Establish tunnel (on either router):

```
sudo ipsec up net-net
```

Debugging Tips

- Run StrongSwan in foreground with debug output:

```
sudo ipsec start --nofork
```

- For ping tests with specific source IP:

```
ping -I 10.1.0.1 10.2.0.1
```

Lab Exercises

1. Monitor traffic using Wireshark:
    - Filter: `isakmp || esp || icmp`
    - Observe ISAKMP, ICMP and ESP traffic

2. Monitor SA establishment:
    - Via Wireshark
    - Via auth.log: `tail -f -n 0 /var/log/auth.log`
3. Check Security Policy Database:

```
sudo ip xfrm policy
```

Exercise Questions

1. **Question 1**: Examine SPIs using `sudo ip xfrm state`. Why are there two SPIs?
2. **Question 2**: Why can't hq_server and branch_client access the Internet? How to fix this?
3. **Question 3**: Analyze `mtr 10.2.0.2` output from hq_server. How would it change with 10 network hops?

Optional Assignments

Certificate-Based Authentication

1. Install additional tools:

```
sudo apt install strongswan-pki
```

2. Create CA and client certificates
3. Configure certificate locations in `/etc/ipsec.d/`
4. Update configurations in `/etc/ipsec.conf` and `/etc/ipsec.secrets`

Road Warrior Configuration

Configure HQ router for remote access:

- Assign virtual IPs from 10.3.0.0/16
- Enable access to both networks (10.1.0.0/16 and 10.2.0.0/16)
- Configure for multiple road warriors