The exercises are designed for students to finish in an individual capacity. The exercises are not designed to be completed in tutorial sessions but rather to give you some tasks and a starting point to continue and complete on your own.

---

1 Lab Setup

1.1 Installing Project

To complete this week's lab tasks, we will be using a new network topology. Run the command below on the GNS3 VM shell to download the IPSec project. If you SSH into the VM from your host OS terminal, you can simply copy and paste the command instead of typing it manually.

```
gdown 1UxInN_231qiX__UzfIT7g_vr5LJ2yA2Y ; sudo bash ./install_IPSec.sh
```

Alternatively, you can use the link below to download the same project. However, if you are connected to the **Monash Wi-Fi**, this method may not work. In that case, please use a mobile hotspot. (Download size: 1.5MB. Single command.)

```
wget https://sniffnrun.com/install_IPSec.sh --no-check-certificate ; \
sudo bash ./install_IPSec.sh
```

1.2 Topology

Open the IPSec project in GNS3 and start all nodes. The topology represents the Wide Area Network (WAN) of SecureCorp's Melbourne and Sydney offices. In addition, a remote client will connect to the Melbourne site in order to access selected internal services which the public internet should not have access to.

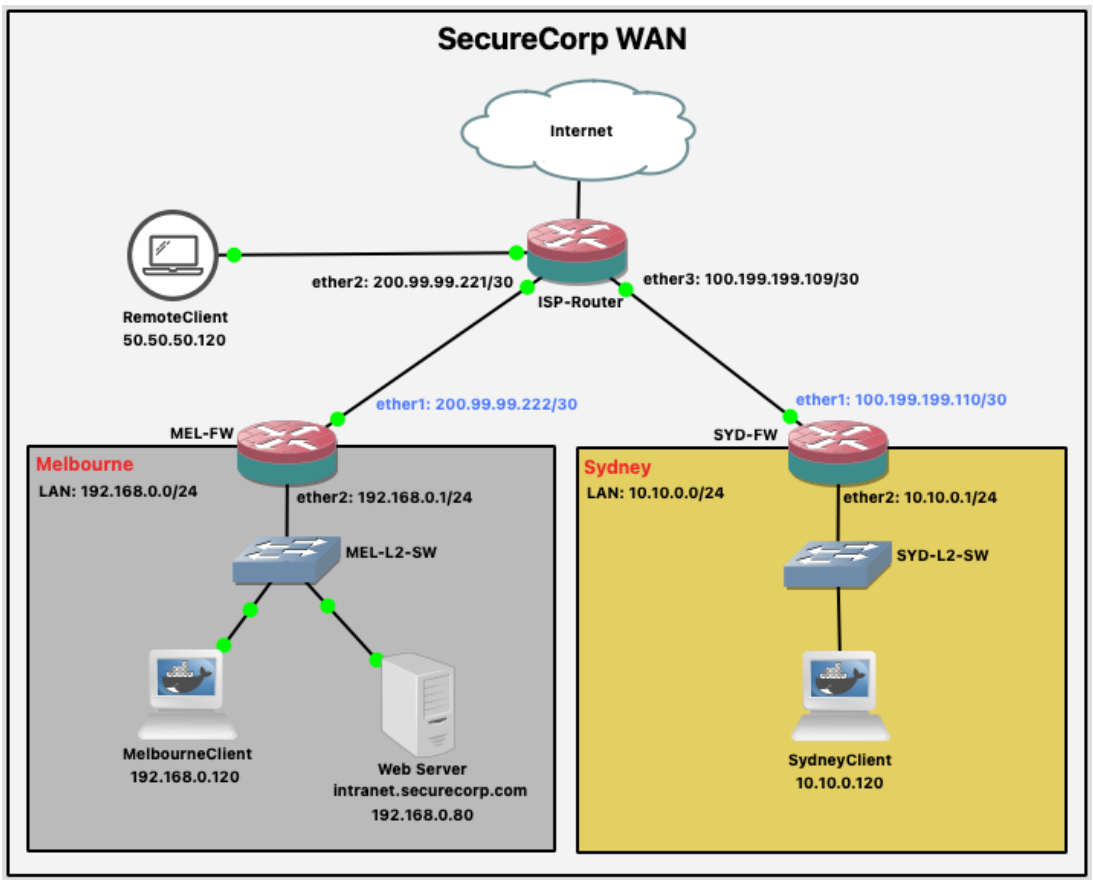

Figure 1: Topology

2 Site-to-Site VPNs

SecureCorp's head office and main datacenter are located in Melbourne, where all internal services are hosted. One such service is the SecureCorp Intranet web server, which should only be accessible by internal employees and must not be exposed to the Internet. However, since the Intranet server is not externally accessible, employees in the Sydney branch are also unable to reach it.

In this task, we will create a site-to-site IPsec VPN that allows the Sydney office to securely access the internal services hosted in the Melbourne datacenter, without exposing them to the Internet.

2.1 Checking Connectivity

2.1.1 Check connectivity between LANs

Access the Intranet server from `MelbourneClient`.

```
lynx intranet.securecorp.com
```

Open the console of `SydneyClient` and use the following command to check connectivity to Melbourne web server.

```
lynx intranet.securecorp.com
ping intranet.securecorp.com
```

As expected, there is no connectivity between the two internal LANs, since they are in private IP subnets. Private IP addresses are not routed on the public Internet.

2.1.2 Check connectivity between firewalls

Login to the `RouterOS` CLI of `MEL-FW` and run the following command to check the connectivity to the public interface IP of `SYD-FW`. `[Login:admin, Password:admin]`

```
ping 100.199.199.110
```

2.2 IPSec Configurations

In this task we are creating a site-to-site IPSec VPN between the public IP addresses of the two firewalls.

Note: Start capturing traffic on the link between `MEL-FW` and the `ISP-Router`.

2.2.1 Creating IPSec Profiles

An IPsec Profile defines the set of parameters used for IKE negotiation during Phase 1. Use the following command to create a new Profile in each firewall.

Configuration required on **BOTH** firewalls [single command]:

```
/ip ipsec profile add name="securecorp-intersite" hash-algorithm=sha256 \
enc-algorithm=aes-256 dh-group=modp2048 lifetime=1d
```

2.2.2 Creating IPSec Proposal

Proposals define the algorithms and parameters used during Phase 2 (the ESP/Child SA) to establish SAs for a given IPsec policy. Use the following command to create a new Proposal in each firewall.

Configuration required on **BOTH** firewalls [single command]:

```
/ip ipsec proposal add name="securecorp-intersite" auth-algorithms=sha256 \
enc-algorithms=aes-256-gcm lifetime=8h
```

2.2.3 Adding a Peer

An IPsec Peer is a configuration object that specifies the remote endpoint and the parameters for IKE negotiation. The peer settings determine how connections are established between IKE endpoints, which are then used to negotiate keys and algorithms for building SAs. Use the following command to add a new peer for the remote site.

Configuration required on **MEL-FW** [single command]:

```
/ip ipsec peer add name="SYD" address=100.199.199.110 profile=securecorp-intersite \
exchange-mode=ike2
```

Configuration required on **SYD-FW** [single command]:

```
/ip ipsec peer add name="MEL" address=200.99.99.222 profile=securecorp-intersite \
exchange-mode=ike2
```

2.2.4 Adding an Identity

Identities are configuration parameters that are specific to the remote peer. Main purpose of an identity is to handle authentication and verify peer's integrity. We are using Pre-Shared Keys (PSK) to authenticate the remote peer. Use the following command to add an identity for the remote peer.

Configuration required on **MEL-FW**:

```
/ip ipsec identity add peer=SYD auth-method=pre-shared-key secret="securecorp"
```

Configuration required on **SYD-FW:**

```
/ip ipsec identity add peer=MEL auth-method=pre-shared-key secret="securecorp"
```

2.2.5 Adding an IPSec Policy

An IPsec Policy is a set of rules that tells the router which traffic should be protected by IPsec and how.

Start packet capturing between any of the firewalls and ISP router before using the following commands to policies to the Security Policy Database (SPD).

You should see Internet Security Association and Key Management Protocol (ISAKMP) traffic establishing the SAs as soon as you create the policies. Examine the details in the ISAKMP header.

Configuration required on **MEL-FW** [single command]:

```
/ip ipsec policy add src-address=192.168.0.0/24 dst-address=10.10.0.0/24 \
peer=SYD action=encrypt level=require ipsec-protocols=esp tunnel=yes \
sa-src-address=200.99.99.222 sa-dst-address=100.199.199.110 \
proposal=securecorp-intersite
```

Configuration required on **SYD-FW** [single command]:

```
/ip ipsec policy add src-address=10.10.0.0/24 dst-address=192.168.0.0/24 \
peer=MEL action=encrypt level=require ipsec-protocols=esp tunnel=yes \
sa-src-address=100.199.199.110 sa-dst-address=200.99.99.222 \
proposal=securecorp-intersite
```

2.2.6 View Established SAs

Try the following command on the firewalls to check if the security associations are established. Examine the parameters of SAs.

```
/ip ipsec installed-sa print
```

2.3 Configuring NAT

Use the following command to view the NAT configurations on the firewall.

```
/ip firewall nat print
```

The existing Source NAT configuration on the firewalls are used to provide internet access to the local LAN. All source addresses are translated to the public IP of the firewall and are thereby kept private. For inter-site network traffic to go through the IPSec tunnel, we should create a new rule to bypass the existing NAT rule. Use the

following commands to add the bypass rule and to move it to the top.
Configuration required on **MEL-FW**:

```
/ip firewall nat add chain=srcnat src-address=192.168.0.0/24 dst-address=10.10.0.1/24 \
action=accept
/ip firewall nat print
/ip firewall nat move 1 0
/ip firewall nat print
```

Output of the final print command should look like this:

```
[[admin@MEL-FW] /ip firewall nat> /ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=accept src-address=192.168.0.0/24
      dst-address=10.10.0.0/24

 1    chain=srcnat action=masquerade
```

Figure 2: MEL-FW NAT Config

Configuration required on **SYD-FW**:

```
/ip firewall nat add chain=srcnat src-address=10.10.0.0/24 dst-address=192.168.0.0/24 \
action=accept
/ip firewall nat print
/ip firewall nat move 1 0
/ip firewall nat print
```

Output of the final print command should look like this:

```
[[admin@SYD-FW] > /ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=accept src-address=10.10.0.0/24
      dst-address=192.168.0.0/24

 1    chain=srcnat action=masquerade
```

Figure 3: SYD-FW NAT Config

2.4 Check Connectivity

Right-click on the link connecting `SYD-FW` and ISP and start capturing traffic. Open the console of `SydneyClient` and use the following command to browse the website hosted in Melbourne LAN via the IPSec tunnel.

```
lynx intranet.securecorp.com
```

1. Is the inter-site traffic encrypted?
2. Now ping `google.com` from the `SydneyClient`. Is the traffic encrypted?

3 Remote Access VPNs

SecureCorp offers flexible work arrangements that allow employees to work from home when needed. While working remotely, users must access the Intranet server hosted in the Melbourne datacenter. To enable this, we will create a Remote Access VPN for remote clients so they can securely reach internal services in the MEL datacenter, which are not exposed to the public Internet.

First, run the following command on the `RemoteClient` to confirm that it cannot currently access the Intranet server.

```
lynx intranet.securecorp.com
```

3.1 Configuring the VPN gateway

Follow the below steps to configure the Remote Access VPN on the **MEL-FW**.

3.1.1 Remote user IP pool

When remote users connect to the firewall via a remote access VPN, they must be assigned an internal IP address in order to access internal resources. To achieve this, we first need to define the IP address pool.

```
/ip pool add name=remote-access-vpn-pool ranges=172.16.10.10-172.16.10.50
```

3.1.2 IPSec Profile

Next step is to create an IPSec Profile for the Remote Access VPN [single command].

```
/ip ipsec profile add name=securecorp-ra-profile dh-group=modp2048 enc-algorithm=aes-256 \
    hash-algorithm=sha256
```

3.1.3 IPSec Peers

Create an IPSec Peer to tell the router who to accept connections from and under what conditions [single command].

```
/ip ipsec peer add name=securecorp-ra-peer address=0.0.0.0/0 exchange-mode=ike2 \
profile=securecorp-ra-profile
```

3.1.4 Mode Config

Mode Config is the mechanism used to assign network configuration settings to VPN clients after authentication. In this setup, we will configure remote clients to route all their traffic through the Remote Access VPN when connected [single command]:

```
/ip ipsec mode-config add address-pool=remote-access-vpn-pool address-prefix-length=32 \
name=securecorp-ra-conf split-include=0.0.0.0/0
```

3.1.5 Configuring Identities

For simplicity in this lab we will assign one PSK for all remote users [single command]:

```
/ip ipsec identity add generate-policy=port-strict mode-config=securecorp-ra-conf \
peer=securecorp-ra-peer secret=SuperSecret
```

3.1.6 IPSec Proposal

Let's create an IPsec Proposal to define the encryption and authentication algorithms that will be used to protect the data traffic [single command]:

```
/ip ipsec proposal add auth-algorithms=sha256 enc-algorithms=aes-256-cbc \
name=securecorp-ra-proposal pfs-group=modp2048
```

3.1.7 IPSec Policy

Finally, create a IPsec Policy to define which traffic should be encrypted between the VPN client and the firewall.

```
/ip ipsec policy add template=yes group=default proposal=securecorp-ra-proposal
```

3.2 Configuring the VPN Client

We use a CLI-based open-source VPN client called **strongSwan** on the remote user's laptop to connect to the SecureCorp Remote Access VPN. **strongSwan** is already installed on the client, but it still needs to be configured with the necessary information to establish the connection.

Add the below lines of configurations to the `/etc/ipsec.conf` file:

Note: Indentation should be followed as shown below.

```
conn securecorp-mel
    keyexchange=ikev2
    ike=aes256-sha256-modp2048!
    esp=aes256-sha256-modp2048!
    left=%defaultroute
    leftsourceip=%config
    leftauth=psk
    right=200.99.99.222
    rightauth=psk
    rightsubnet=0.0.0.0/0
    auto=start
```

Now let's provide the Pre-Shared Key to connect to the SecureCorp Remote Access VPN.

Add the below lines of configurations to the `/etc/ipsec.secrets` file:

```
%any 200.99.99.222 : PSK "SuperSecret"
```

Restart the IPSec service to apply the configurations.

```
ipsec restart
```

3.3 Connecting to the Remote Access VPN

Start packet capturing on the the link connecting the `MEL-FW` to the `IPS-Router` and observe the traffic on Wireshark.

Connect to the SecureCrop Remote Access VPN using the below command.

```
ipsec up securecorp-mel
```

Check your IP configurations. Do you see an internal IP assigned to remote client?

```
ip address
```

Can you access the Intranet now? Observe the traffic in Wireshark.

```
lynx intranet.securecorp.com
```

1. In step `3.1.5` we configured a single PSK for all remote users? In which ways is this a security risk?
2. Which authentication mechanisms can you use to ensure that each user has their own identity?
3. Ping Google DNS server `8.8.8.8` from the RemoteClient. Does the Internet traffic get routed via `MEL-FW` as configure in step `3.1.4`.
4. Discuss the pros and cons of using `split-tunneling` in Remote Access VPNs.

Note: To disconnect the VPN, you can use the below command.

```
ipsec down securecorp-mel
```