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.

Review Questions

1. Give examples of applications of IPSec.
2. What is the difference between transport mode and tunnel mode?
3. What is a replay attack and how can IPSec prevent it?
4. Why does ESP include a padding field?
5. What are the distinctions between a Phase 1 and a Phase 2 Security Association?

Lab Tasks

In this lab we are creating an IPSec site-to-site VPN tunnel to connect SecureCorp's Melbourne office and the Sydney office. The perimeter firewall of each site will be configured as the VPN gateways. Both firewalls are running Mikrotik RouterOS.

Open a terminal in your VM and run the following command to download and install the IPSec project.

```
gdown 1Xp20VDmzh2_NvoaP90zRRvoQP5wqAQnZ ; sudo bash ./install_IPSec.sh
```

Or for Apple Silicon VM, run the following command in GNS3 VM Shell. Instructions on how to access the shell is given in the appendix section of the Apple Silicon lab setup document:

```
gdown 1z9_SK__CjRm2UZ6gixTbnGJsATiFZS8A ; sudo bash ./install_IPSec_arm.sh
```

`IPSec` project should now appear in your GNS3 projects library. Open `IPSec` project and start all nodes in the network.

1. **Check connectivity between LANs**
   Start Apache service on the `Web Server` in Melbourne site.

   ```
   service apache2 start
   ```

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

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

   There is no connectivity between the two internal LANs of the as they are in private IP subnets. Private IPs are not routed in the public internet.

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
   ```

   Similarly, login to `SYD-FW` and check the connectivity to `MEL-FW`'s public interface IP.

   ```
   ping 200.99.99.222
   ```

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

(a) **Creating IPSec Profiles:** Profiles defines a set of parameters that will be used for IKE negotiation during Phase 1. Use the following command to create a new Profile in each firewall.

`Configuration required on both firewalls:`

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

(b) **Creating IPSec Proposal:** Proposals contain the information that will be sent by IKE daemons to establish Security Associations(SA) for a certain IPSec policy. Use the following command to create a new Proposal in each firewall.

`Configuration required on both firewalls:`

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

(c) **Adding a Peer:** Peer settings are used to establish connections between IKE daemons. This connection then will be used to negotiate keys and algorithms for SAs. Use the following command to add a new peer for the remote site.

`Configuration required on MEL-FW:`

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

`Configuration required on SYD-FW:`

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

(d) **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. 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"
```

(e) **Adding an IPSec Policy:** Policies are used to determine whether security settings should be applied to a packet. 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:`

```
/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:`

```
/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
```

(f) **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
```

4. **Configure routing for remote LAN**
   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
```

   `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
```

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

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

   (a) Is the inter-site traffic encrypted?

   (b) Now ping `google.com` from `RemoteClient`. Is the traffic encrypted?

   (c) Observe the ESP header. Is it possible to determine if this packet was generated in transport mode or tunnel mode by examining the encrypted data?

   (d) Is the Authentication Header(AH) used? Why? How does IPSec provide integrity without AH?