1 Network Configuration

1.1 Network Topology

1. The given example network connects the University network with a remote branch (an another faculty) through a Virtual Private Network (VPN) via internet.

2. First, create the given network using the Cisco Packet Tracer. Here, the Layer 3 (L3) switches are used for routing between sub-nets, and Figure 1 shows a network created using the Cisco Packet Tracer v7.2.1.

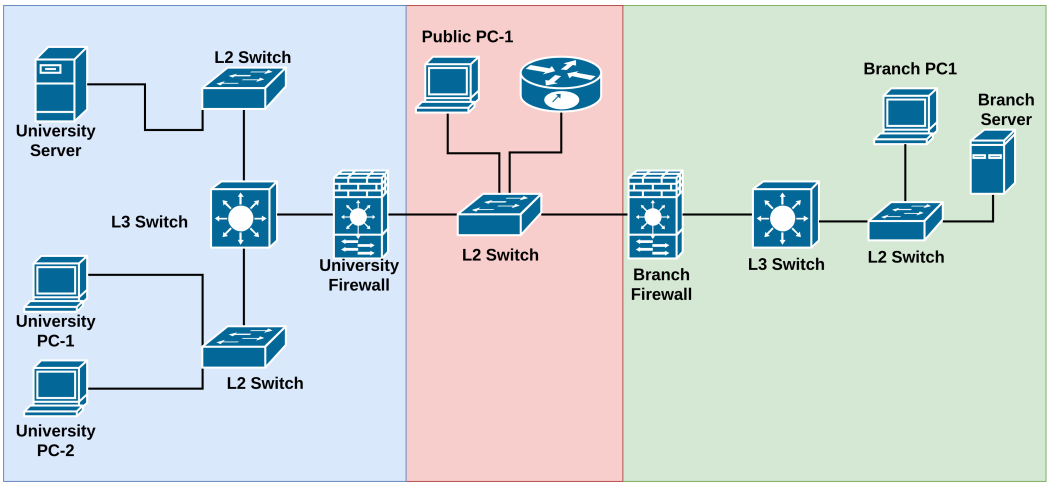

Figure 1: The network topology

3. For the given network setup use the following IP plan.

   - Private network IP addresses: **10.40.0.0/16**
   - University network IP addresses: **10.40.0.0/18**
   - University server sub-net: **10.40.18.0/24**
   - University users sub-net: **10.40.19.0/24**
   - Branch Network IP addresses: **10.40.96.0/19**
   - Internet (Public) IP addresses: **134.95.56.16/28**

4. Configure the inside and outside interfaces of two firewalls. Set the security level of the **inside interface** to 100 and the **outside interface** to 0. (For this task, you have to use above IP ranges.)

5. To complete the next step, you will need some knowledge regarding the Cisco Packet Tracer simulation mode. If you are not familiar with it, please refer **Part 1** in the following link: Packet Tracer Simulation

6. Use the simulation mode in the Packet Tracer to check what happens when you,

   - Try the *ping* command to the outside network and branch network from an University PC.
   - Try the *ping* command to the University or branch network from an outside PC.

1.2 Configuring the University Firewall

1. Configure the interfaces. Set the security level of the inside interface to 100 and the outside interface to 0. Allocate proper IP addresses to the interfaces from the IP pools given above.

2. Create three network objects for the branch network, university network and for the whole private network.

```
# object network private_network
    # subnet 10.40.0.0 255.255.0.0
```

3. Add a static route to the outside interface to direct traffic to the branch network.

```
# route outside <branch network# <mask# <branch firewall IP# 1
```

4. Add a static route to the inside interface to route University traffic to the the main router.

```
# route inside <university network# <mask#  <core router IP# 1
```

5. Create an access list to capture the traffic to the branch network.

```
# access-list branch-traffic extended permit tcp object
# campus_network object branch_network
```

6. Create an access list to capture traffic from the private network to the private network.

```
# access-list private-traffic extended permit ip object
# private_network object private_network
```

7. Apply private-traffic access group to the inside interface.

```
# access-group private-traffic out interface inside
```

8. Configure the Internet Security Association Management Protocol (ISAKMP) policies. For this lab, we are using **IKEv1** connection. Set up the policy according to the following configuration settings,

   - The authentication method as pre-shared key
   - Encryption as AES
   - HMAC method as SHA-1
   - The Diffie-Hellman group as group 2

```
# crypto ikev1 policy 1
    # encr aes
    # authentication pre-share
    # Hash sha
    # group 2
```

9. Enable IKEv1 on the interface outside.

```
# crypto ikev1 enable outside
```

10. Create IKEv1 transform-set with AES as the encryption method and **Sha-Hmac** as the authentication method.

```
# crypto ipsec ikev1 transform-set Lan2Lan esp-aes esp-sha-hmac
```

11. Create a crypto map with the following properties,

    - Assign the branch_traffic ACL
    - Set peer as the branch firewall's outside interface
    - Set the lifetime as 86400 seconds
    - Specify the previously created transform-set as the **IKEv1** transform set of the crypto map

```
# crypto map branch 1 match address branch-traffic
# crypto map branch 1 set peer <branch IP#
# crypto map branch 1 set security-association lifetime seconds 86400
# crypto map branch 1 set ikev1 transform-set Lan2Lan
```

12. Apply the created *crypto* map to the outside interface

```
# crypto map branch interface outside
```

13. Define a tunnel group. Here, we use IPsec Lan-to-Lan connection type. Then, define a pre-shared key for this tunnel group (for this, you can define your own key).

```
# tunnel-group <Branch IP# type ipsec-l2l
# tunnel-group <Branch IP# ipsec-attributes
    # ikev1 pre-shared-key cisco123
```

1.3 Configuring the Branch Firewall

1. Configure the interfaces. Set the security level of the inside interface to 100 and the outside interface to 0. Allocate proper IP's to the interfaces from the IP pools given in section 1.1.

2. Create three network objects for the branch network, university network and for the whole private network.

```
# object network private_network
    # subnet 10.40.0.0 255.255.0.0
```

3. Add a static route to the outside interface to direct traffic to the University network.

```
# route outside <University  network# <mask# <University  firewall IP# 1
```

4. Add a static route to inside interface to route branch traffic to the main router.

```
# route inside <branch network# <mask#  <core router IP# 1
```

5. Create an access list to capture the traffic to the University.

```
# access-list university-traffic extended permit tcp object
# branch_network object campus_network
```

6. Create an access list to the capture traffic from the private network to the private network.

```
# access-list private-traffic extended permit ip object
# private_network object private_network
```

7. Apply private-traffic access group to the inside interface.

```
# access-group private-traffic out interface inside
```

8. Configure **ISAKMP** policies. Here, we are using **IKEv1** connection. Set the,

   - The authentication method as pre-shared key
   - Encryption as AES
   - HMAC method as SHA-1
   - The Diffie-Hellman group as group 2

```
# crypto ikev1 policy 1
    # encr aes
    # authentication pre-share
    # Hash sha
    # group 2
```

9. Enable **IKEv1** on the interface outside.

```
# crypto ikev1 enable outside
```

10. Create ikev1 transform-set with AES as the encryption method and sha-hmac as the authentication method.

```
# crypto ipsec ikev1 transform-set Lan2Lan esp-aes esp-sha-hmac
```

11. Create a crypto map with the following properties,

    - Assign the university_traffic ACL
    - Set peer as the university firewall's outside interface
    - Set the lifetime as 86400 seconds
    - Specify the previously created transform-set as the IKEv1 transform set of the crypto map

```
# crypto map branch 1 match address university-traffic
# crypto map branch 1 set peer <University IP#
# crypto map branch 1 set security-association lifetime seconds 86400
# crypto map branch 1 set ikev1 transform-set Lan2Lan
```

12. Apply the created crypto map to the outside interface

```
# crypto map branch interface outside
```

13. Define a tunnel group. Here, we use IPsec Lan-to-Lan connection type. Then, define a pre-shared key for this tunnel group (for this, you can define your own key).

```
# tunnel-group <University IP# type ipsec-l2l
# tunnel-group <University IP# ipsec-attributes
    # ikev1 pre-shared-key cisco123
```

1.4 Verifying the Virtual Private Network

1. Use the show *crypto isakmp sa* command to show the Internet Security Association Management Protocol (ISAKMP) security associations (SAs) which have been negotiated between the two firewalls.
2. Use the show *crypto ipsec sa* command to check IPSec security associations and monitor encrypted traffic statistics.
3. Then, use the simulation mode to explore how the IPsec works and send packets from the University network to branch network and see whether your network is working as expected.

2 Clientless SSL VPN

Clientless SSL VPN enables end users to securely access resources on the corporate network from anywhere using an SSL-enabled Web browser. The user first authenticates with Clientless SSL VPN gateway, which then allows the user to access pre-configured network resources.

In-class Activity: Implement a Clientless SSL VPN using the same network, and test it using the internet PC. You can find the implementation details on the official CIsco ASA 9.6 documentation.

3 Assignement

Find answers for the following questions.

3.1 Part 1

1. Briefly explain the IPSec protocol and the services it provides.
2. What is the use of step 3 and step 4 of the configuring process?
3. What is the use of step 5 of the configuring process?
4. What will happen if you skipped step 6 and 7 and why?
5. Briefly explain what is **ISAKMP** and why we need **ISAKMP** in this process.
6. What is a transform set?
7. What is a Crypto map? Explain the minimum requirement for compatibility of two crypto maps.
8. Send HTTP request from a branch PC to University server with and without VPN. Capture the packets going through the internet and Identify the difference of the packet structure between two scenarios. If you need you can use diagrams to explain.
9. What do you need to change in this example if you only need your UDP packets to be protected on the internet?
10. Give a summary of the vulnerabilities of technologies you used here that can be used to expose your data and what can you do to improve your system's security.

3.2 Part 2

1. Explain the differences between Clientless SSL VPN and Lan-to-Lan IPSec VPN.