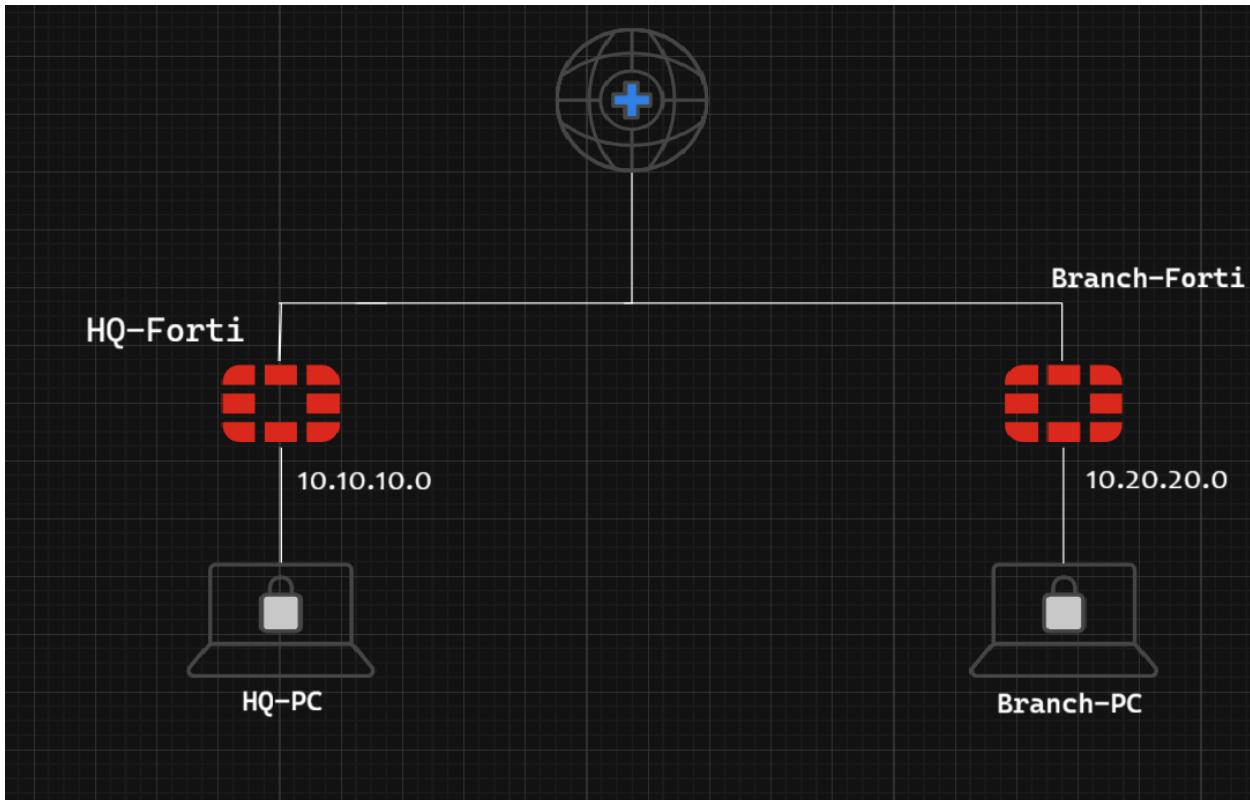

Week 2 – IPsec VPN Configuration Documentation

1. Objective

The main objective of this task is to establish a secure IPsec VPN tunnel between two FortiGate devices to ensure encrypted communication between two remote networks over the internet.

2. Network Topology



Description:

- Two FortiGate firewalls were used to connect two different LAN networks through the internet using an IPsec VPN tunnel.
- Each FortiGate represents a branch office / Headquarter office.

Example Topology:

Site A LAN (10.10.10.0/24) --- FortiGate A ---- Internet ---- FortiGate B ---- Site B LAN (10.20.20.0/24)

3. IPsec VPN Configuration Steps (HQ – Configuration)

Step 1: Phase 1 Configuration

- Go to **VPN** → **IPsec Tunnels** → **Create New** → **Custom**.
- **Name:** HQ-to-Branch
- **Remote Gateway:** Static IP Address (192.168.1.5) (**HQ WAN IP**)
- **Interface:** WAN (port1)
- **Authentication Method:** Pre-shared Key
- **IKE Version:** IKEv2
- **Encryption:** DES
- **Authentication:** SHA384
- **DH Group:** 14,5
- **Key Lifetime:** 86400

Network

IP Version	IPv4
Remote Gateway	<input type="button" value="Static IP Address"/>
IP Address	192.168.1.5
Interface	<input type="button" value="WAN (port1)"/>
Local Gateway	<input checked="" type="checkbox"/>
Mode Config	<input type="checkbox"/>
NAT Traversal	<input type="button" value="Enable"/> <input checked="" type="button" value="Disable"/> <input type="button" value="Forced"/>
Dead Peer Detection	<input type="button" value="Disable"/> <input type="button" value="On Idle"/> <input checked="" type="button" value="On Demand"/>
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress <input type="checkbox"/> Ingress <input type="checkbox"/>
Advanced...	

Authentication

Method: Pre-shared Key

Pre-shared Key:

IKE

Version: 2

Phase 1 Proposal + Add

Encryption: DES

Authentication: SHA384

Diffie-Hellman Groups:

32 31 30 29 28 27
 21 20 19 18 17 16
 15 14 5 2 1

Key Lifetime (seconds): 86400

Local ID:

Step 2: Phase 2 Configuration

- **Local Subnet:** 10.10.10.0/255.255.255.0
- **Remote Subnet:** 10.20.20.0/255.255.255.0
- **Encryption:** DES
- **Authentication:** SHA256
- **Enable Replay Detection**

Comments	Comments 	
Local Address	Subnet	10.10.10.0/255.255.255
Remote Address	Subnet	10.20.20.0/255.255.255
<input type="checkbox"/> Advanced...		
Phase 2 Proposal	<input type="button" value="Add"/>	
Encryption	DES	Authentication
Enable Replay Detection <input checked="" type="checkbox"/>		
Enable Perfect Forward Secrecy (PFS) <input checked="" type="checkbox"/>		
Diffie-Hellman Group	<input type="checkbox"/> 32 <input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 2 <input type="checkbox"/> 1	
Local Port	All <input checked="" type="checkbox"/>	
Remote Port	All <input checked="" type="checkbox"/>	
Protocol	All <input checked="" type="checkbox"/>	
Auto-negotiate	<input type="checkbox"/>	
Autokey Keep Alive	<input type="checkbox"/>	
Key Lifetime	Seconds	
Seconds	43200	

Step 3: Firewall Policies

- Create policies to allow traffic from LAN → VPN and VPN → LAN on both FortiGates.

1- LAN-To-VPN

- **Incoming Interface:** LAN (port2)
- **Outgoing Interface:** HQ-to-Branch
- **Action:** Accept
- **NAT:** Disabled

- **Source :** HQ Subnet (10.10.10.0/24)
- **Destination :** HQ Subnet (10.20.20.0/24)

Name LAN-To-VPN

Incoming Interface LAN (port2)

Outgoing Interface HQ-to-Branch

Source HQ_Subnet

Destination Branch_Subnet

Schedule always

Service ALL

Action ACCEPT DENY

Statistics (since last reset)

ID	2
Last used	2 day(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	6
Total bytes	7.14 kB
Current bandwidth	0 bps

Clear Counters

Last 7 Days Bytes ▾

Category	Oct 21	Oct 22	Oct 23	Oct 24	Oct 25	Oct 26	Oct 27	Oct 28
SPU	0 B	0 B	0 B	0 B	0 B	0 B	0 B	~8 kB
Software	0 B	0 B	0 B	0 B	0 B	0 B	0 B	~7 kB

2- VPN-to-LAN

- **Incoming Interface:** HQ-to-Branch
- **Outgoing Interface:** LAN (port2)
- **Action:** Accept
- **NAT:** Disabled
- **Source :** Branch Subnet (10.20.20.0/24)
- **Destination :** HQ Subnet (10.10.10.0/24)

Name	VPN-To-LAN
Incoming Interface	HQ-to-Branch
Outgoing Interface	LAN (port2)
Source	Branch_Subnet
Destination	HQ_Subnet
Schedule	always
Service	All
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

Statistics (since last reset)

ID	3
Last used	2 day(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	20
Total bytes	17.06 kB
Current bandwidth	0 bps

Last 7 Days Bytes ▾

Oct 21	Oct 22	Oct 23	Oct 24	Oct 25	Oct 26	Oct 27	Oct 28
0 kB	~18 kB						

Step 4: Static Routes

- Add static routes to reach the remote subnet through the VPN tunnel.
- Destination : Subnet (10.20.20.0 / 255.255.255.0)
- Interface : HQ-to-Branch

Destination i

Subnet	Internet Service
10.20.20.0/255.255.255.0	
Interface	HQ-to-Branch
Administrative Distance i	10
Comments	Write a comment... 0/255
Status	Enabled Disabled

+ Advanced Options

4. Branch FortiGate Configuration

Step 1: Phase 1 Configuration

- Go to VPN → IPsec Tunnels → Create New → Custom.
- Name: Branch-to-HQ
- Remote Gateway: Static IP Address (192.168.1.8) (HQ WAN IP)
- Interface: WAN (port1)
- Authentication Method: Pre-shared Key
- IKE Version: IKEv2
- Encryption: DES
- Authentication: SHA384
- DH Group: 14,5
- Key Lifetime: 86400

Network

IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	192.168.1.8
Interface	WAN (port1)
Local Gateway	<input checked="" type="checkbox"/>
Mode Config	<input type="checkbox"/>
NAT Traversal	Enable Disable Forced
Dead Peer Detection	Disable On Idle On Demand
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress <input type="checkbox"/> Ingress <input type="checkbox"/>
Advanced...	

Authentication

Method

Pre-shared Key

••••••••

IKE

Version

1
2

Phase 1 Proposal

Add

EncryptionAuthentication

Diffie-Hellman Groups

32
 31
 30
 29
 28
 27

21
 20
 19
 18
 17
 16

15
 14
 5
 2
 1

Key Lifetime (seconds)

Local ID

Note:

Make sure the Pre-shared Key matches exactly with the one configured on HQ.

Step 2: Phase 2 Configuration

- **Local Subnet: 10.20.20.0 / 255.255.255.0**
- **Remote Subnet: 10.10.10.0 / 255.255.255.0**
- **Encryption: DES**
- **Authentication: SHA256**

- **Enable Replay Detection:** Enabled

Comments	Comments					
Local Address	Subnet	10.20.20.0/255.255.255				
Remote Address	Subnet	10.10.10.0/255.255.255				
[+] Advanced...						
Phase 2 Proposal	+ Add					
Encryption	DES	Authentication				
SHA256						
Enable Replay Detection <input checked="" type="checkbox"/>						
Enable Perfect Forward Secrecy (PFS) <input checked="" type="checkbox"/>						
Diffie-Hellman Group	<input type="checkbox"/> 32	<input type="checkbox"/> 31	<input type="checkbox"/> 30	<input type="checkbox"/> 29	<input type="checkbox"/> 28	<input type="checkbox"/> 27
	<input type="checkbox"/> 21	<input type="checkbox"/> 20	<input type="checkbox"/> 19	<input type="checkbox"/> 18	<input type="checkbox"/> 17	<input type="checkbox"/> 16
	<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	
Local Port	All <input checked="" type="checkbox"/>					
Remote Port	All <input checked="" type="checkbox"/>					
Protocol	All <input checked="" type="checkbox"/>					
Auto-negotiate	<input type="checkbox"/>					
Autokey Keep Alive	<input type="checkbox"/>					
Key Lifetime	Seconds					
Seconds	43200					

Step 3: Firewall Policies

1- LAN-To-VPN

- **Incoming Interface:** LAN (port2)
- **Outgoing Interface:** Branch-to-HQ
- **Action:** Accept
- **NAT:** Disabled

- **Source: Branch Subnet (10.20.20.0/24)**
- **Destination: HQ Subnet (10.10.10.0/24)**

Name LAN-To-VPN
 Incoming Interface: LAN (port2)
 Outgoing Interface: Branch-to-HQ
 Source: Branch_Subnet
 Destination: HQ_Subnet
 Schedule: always
 Service: ALL
 Action: ✓ ACCEPT ✗ DENY

Statistics (since last reset)

ID	2
Last used	2 day(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	20
Total bytes	17.06 kB
Current bandwidth	0 bps

✗ Clear Counters

Firewall/Network Options
 NAT:
 Protocol Options: PROT default

Security Profiles
 AntiVirus:
 Web Filter:
 DNS Filter:
 Application Control:

Last 7 Days Bytes

Date	Bytes
Oct 21	0 kB
Oct 22	0 kB
Oct 23	0 kB
Oct 24	0 kB
Oct 25	0 kB
Oct 26	0 kB
Oct 27	0 kB
Oct 28	~18 kB

SPU Software

OK Cancel

2- VPN-To-LAN

- **Incoming Interface: Branch-to-HQ**
- **Outgoing Interface: LAN (port2)**
- **Action: Accept**
- **NAT: Disabled**
- **Source: HQ Subnet (10.10.10.0/24)**
- **Destination: Branch Subnet (10.20.20.0/24)**

Name	VPN-To-LAN
Incoming Interface	Branch-to-HQ
Outgoing Interface	LAN (port2)
Source	HQ_Subnet
Destination	Branch_Subnet
Schedule	always
Service	ALL
Action	<input checked="" type="radio"/> ACCEPT <input type="radio"/> DENY

Firewall/Network Options

NAT

Protocol Options PROT default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

OK Cancel

Statistics (since last reset)

ID	3
Last used	2 day(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	7
Total bytes	7.98 kB
Current bandwidth	0 bps

Last 7 Days Bytes ▾

12500 B
10 kB
8 kB
5 kB
3 kB
0 B

.J. SPU .I. Software

Oct 21 Oct 22 Oct 23 Oct 24 Oct 25 Oct 26 Oct 27 Oct 28

Step 4: Static Routes

- **Destination: 10.10.10.0 / 255.255.255.0**
- **Interface: Branch-to-HQ**

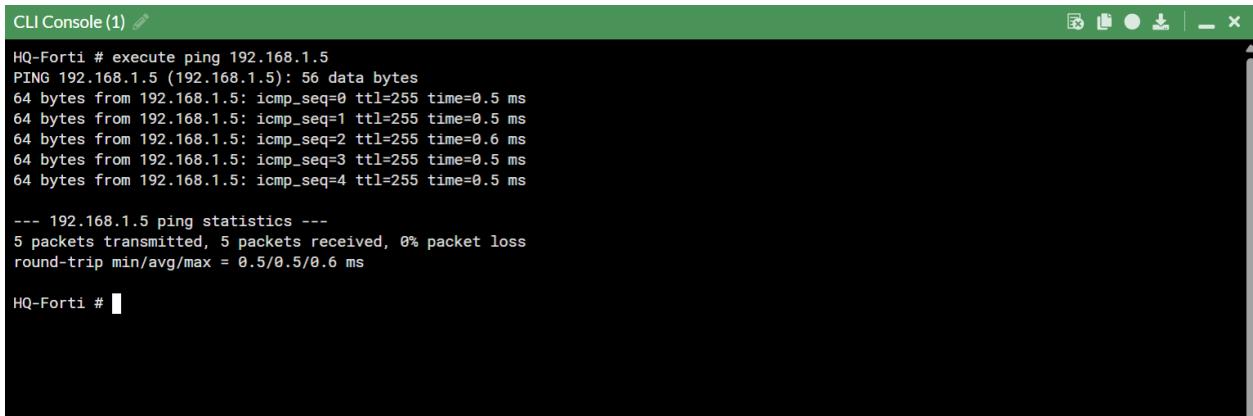
Destination	<input checked="" type="radio"/> Subnet <input type="radio"/> Internet Service
Subnet	10.10.10.0/255.255.255.0
Interface	Branch-to-HQ <input type="button" value="Edit"/>
+	
Administrative Distance	10
Comments	Write a comment... 0/255
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<input type="button" value="Advanced Options"/>	

5. Connectivity Test Results

Test 1: Ping Test Between Branches

- From: HQ Forti 192.168.1.8
- To: Branch Forti 192.168.1.5

 **Result:** Successful ping replies received, indicating that both LAN networks are reachable through the IPsec VPN tunnel.



```
CLI Console(1) 
HQ-Forti # execute ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5): 56 data bytes
64 bytes from 192.168.1.5: icmp_seq=0 ttl=255 time=0.5 ms
64 bytes from 192.168.1.5: icmp_seq=1 ttl=255 time=0.5 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=255 time=0.6 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=255 time=0.5 ms
64 bytes from 192.168.1.5: icmp_seq=4 ttl=255 time=0.5 ms

--- 192.168.1.5 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.6 ms

HQ-Forti #
```

Tunnel	Interface Binding	Status
Custom 1		
 Branch-to-HQ	 WAN (port1)	 Up

Create New	Edit	Delete	Show Matching Logs	Search	Q
Tunnel	Interface Binding	Status			
Custom 1					
 HQ-to-Branch	 WAN (port1)	 Up			

Test 2: File Transfer Test (SCP Protocol)

- **Objective:** Verify real data transfer through the IPsec tunnel.
- **Setup:**
 - A Windows machine connected to HQ LAN (10.10.10.50).
(From DHCP Of LAN)
 - A Kali Linux machine connected to Branch LAN (10.20.20.50).
(From DHCP Of LAN)

- **Method:**
 - From the Windows PC, access the Kali shared folder using SSH protocol (\\\10.20.20.50\share).
 - Attempt to copy a test file (e.g., test.txt) between both devices.
- **Command:**
 - From Windows PC Open The PowerShell and Type :
 - `scp C:\Share\DEPI.txt muhabz@10.10.10.50:/home/muhabz`
- **Result:**

File transfer completed successfully with stable throughput and no packet loss.
This confirms that the IPsec tunnel securely transmits not only ICMP packets but also application-layer data traffic.

```
Windows PowerShell
PS C:\Users\Mohab-Branch> scp C:\Share\DEPI.txt muhabz@10.10.10.50:/home/muhabz
muhabz@10.10.10.50's password:
DEPI.txt                                                 100%   33    6.4KB/s  00:00
PS C:\Users\Mohab-Branch>
```

```
muhabz@muhabz-VMware-Virtual-Platform:~$ ls
DEPI.txt  Documents  Music  Public  Templates
Desktop  Downloads  Pictures  snap  Videos
muhabz@muhabz-VMware-Virtual-Platform:~$ cat DEPI.txt
Here's Our IPsec Configuration <3

muhabz@muhabz-VMware-Virtual-Platform:~$
```

6. Conclusion

The IPsec VPN tunnel between the HQ FortiGate and the Branch FortiGate was successfully established and tested.

Connectivity between the two LANs was confirmed through ICMP ping tests and SSH file transfer verification.

This demonstrates that encrypted communication and secure data exchange between both networks are fully operational.

The configuration followed standard security best practices, ensuring data integrity and confidentiality across the VPN connection.

