Project 3 Report: Implementing VPN solutions with FortiGate

BY:

1. Mahmoud Wael Mohammed (Team Leader) | 21056157 | mahmoudwtawfik@gmail.com
2. Mohammed Wael Mohammed | 21056156 | mohammadwtawfik@gmail.com
3. Radwa Amr Ahmed | 21070835 | radwaamora17@gmail.com
4. Rana Mohamed Elsayed | 21028713 | ranam1131@gmail.com
5. Haneen Mohamed Gaber | 21092529 | es-haneen.mohamed2027@alexu.edu.eg
6. Shahd Mahmoud Omar | 21031378 | omarshiko358@gmail.com

Contents

Idea of the project:

The telecommunications companies in Egypt have merged into a single corporation. This corporation operates two branches, and each branch contains two telecommunications companies along with two departments: IT and HR.

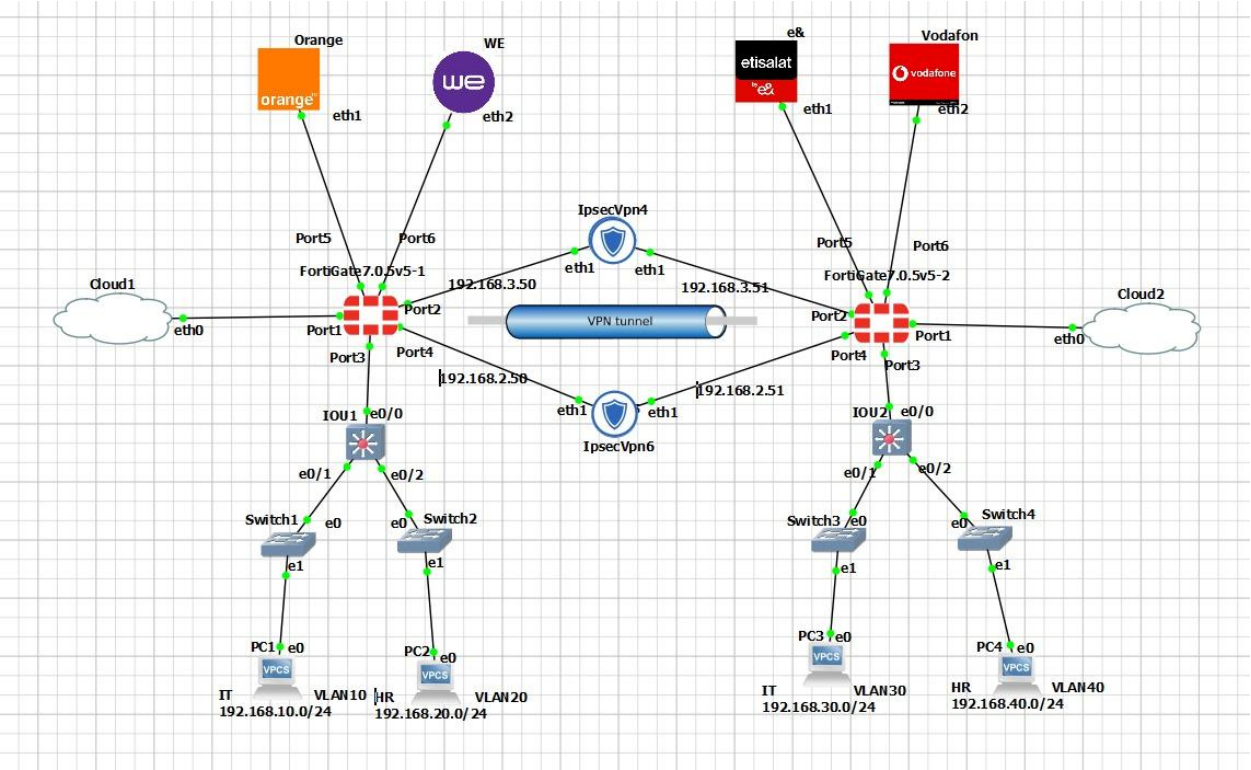
Each telecommunications company is responsible for one of these departments.

Communication between the two companies is allowed, but only under strict conditions:

A department may only communicate with the corresponding department in the other branch.

For example, the IT department may communicate only with the IT department in the other branch, and the HR department may communicate only with HR in the other branch.

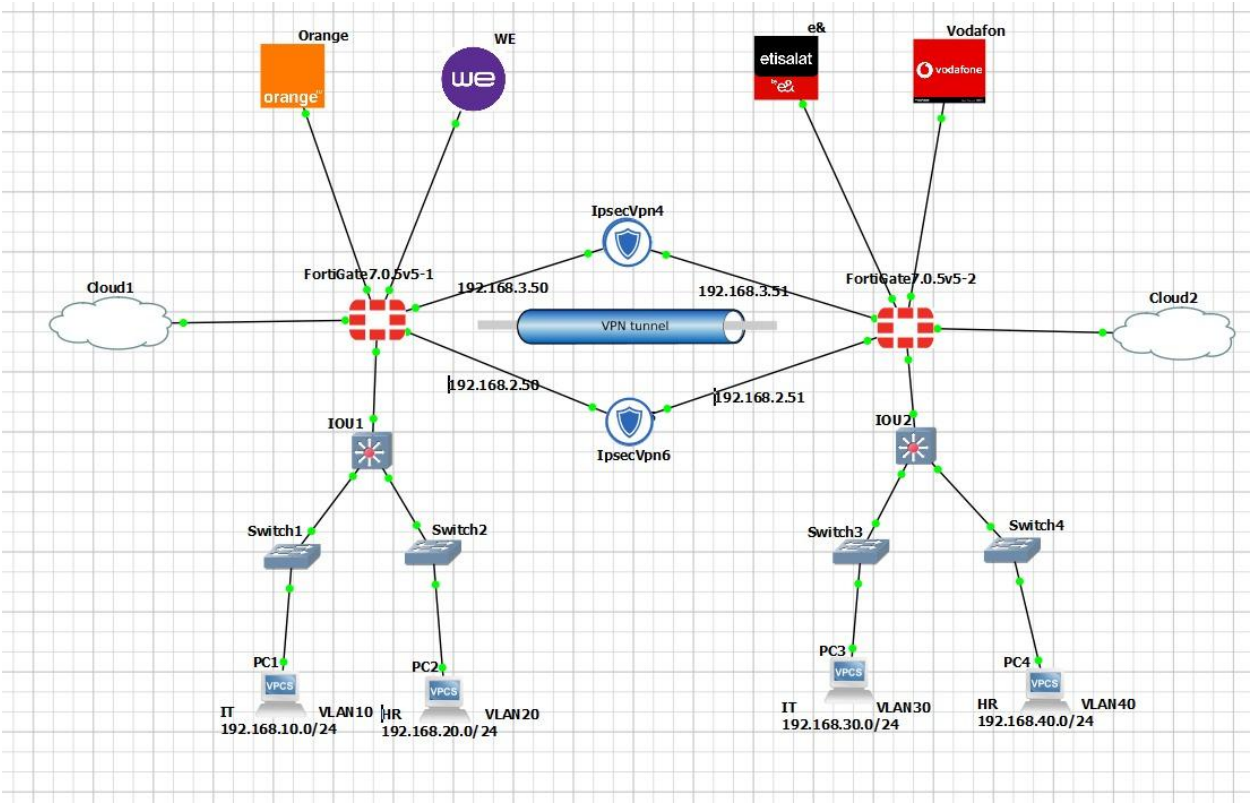
No cross-department communication is permitted — i.e., HR cannot communicate with IT, and vice versa.



1st: Creating VLANs:

We configured VLANs for both the **IT** and **HR** departments in each branch.

- **Branch 1** includes **VLAN 10 (IT)** and **VLAN 20 (HR)**.
- **Branch 2** includes **VLAN 30 (IT)** and **VLAN 40 (HR)**.

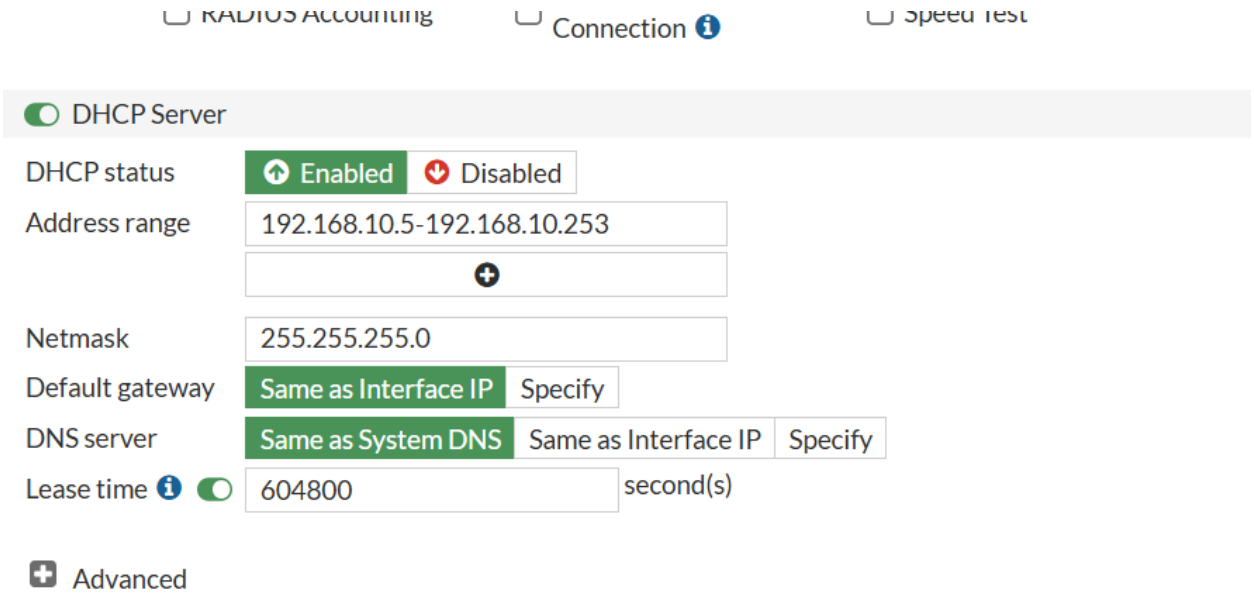


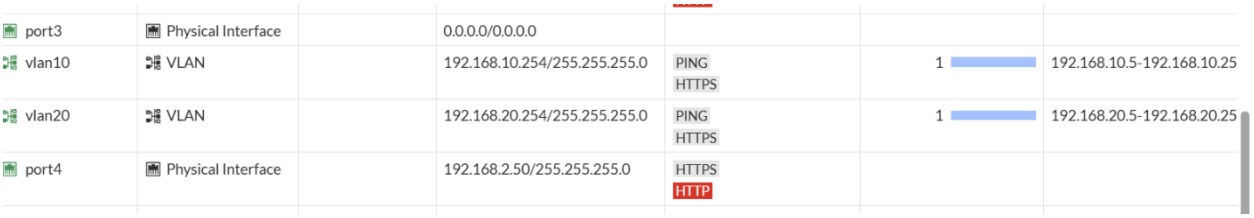

PC1
PC3
PC2
PC4
IOU2
nterface Ethernet0/0
switchport trunk allowed vlan 1,30,40
switchport trunk encapsulation dot1q
switchport mode trunk
nterface Ethernet0/1
switchport access vlan 30
switchport mode access
nterface Ethernet0/2
switchport access vlan 40
switchport mode access
nterface Ethernet0/3
nterface Ethernet1/0
nterface Ethernet1/1
nterface Ethernet1/2
nterface Ethernet1/3
nterface Ethernet2/0
nterface Ethernet2/1


PC1
PC3
PC2
PC4
IOU2
IOU1
!
!
!
!
interface Ethernet0/0
switchport trunk allowed vlan 1,10,20
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access vlan 10
switchport mode access
!
interface Ethernet0/2
switchport access vlan 20
switchport mode access
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
--More--

2nd: Distributing DHCP:

The **firewall** is responsible for distributing **DHCP** across the network.



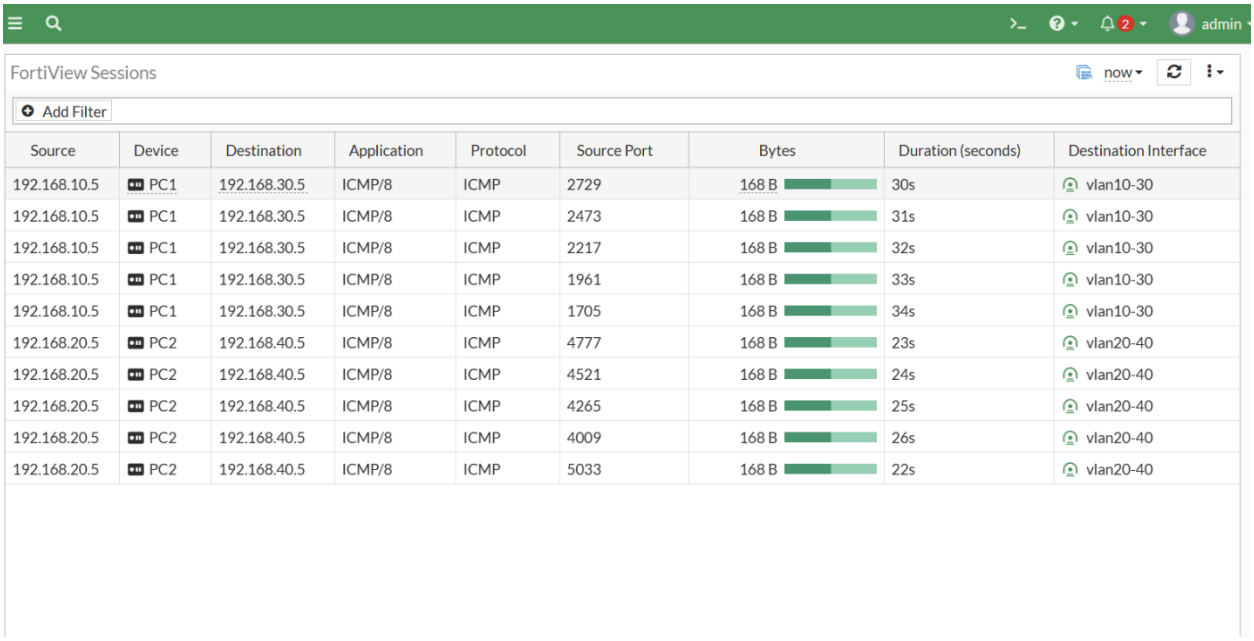


3rd: VPNs:

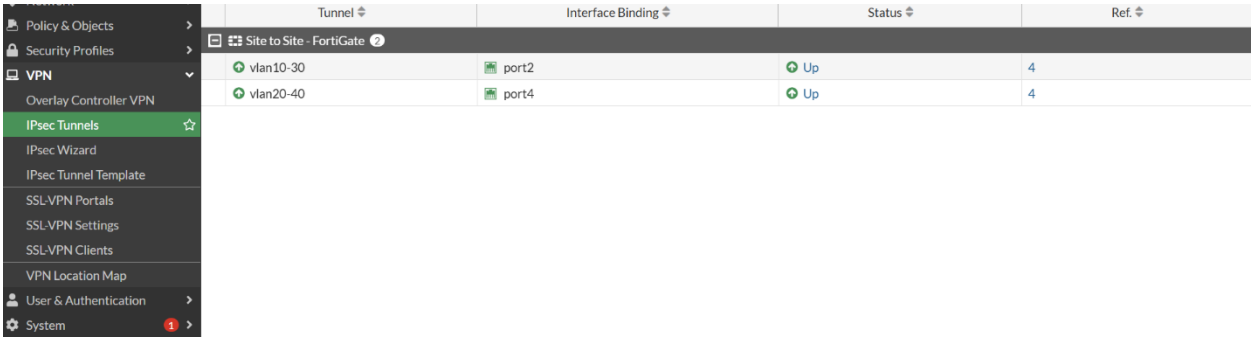
We utilized **IPsec VPNs** to enforce secure inter-branch communication.
A specific policy was configured to ensure that the **IT department** communicates only with the IT department in the other branch through a dedicated VPN tunnel (**IPsec VPN 4**), which uses the IP addresses **192.168.3.50** and **192.168.3.51**.

Similarly, another policy was implemented to allow the **HR department** to communicate exclusively with its corresponding department in the other branch via a separate VPN tunnel (**IPsec VPN 6**), associated with the IP addresses **192.168.2.50** and **192.168.2.51**.

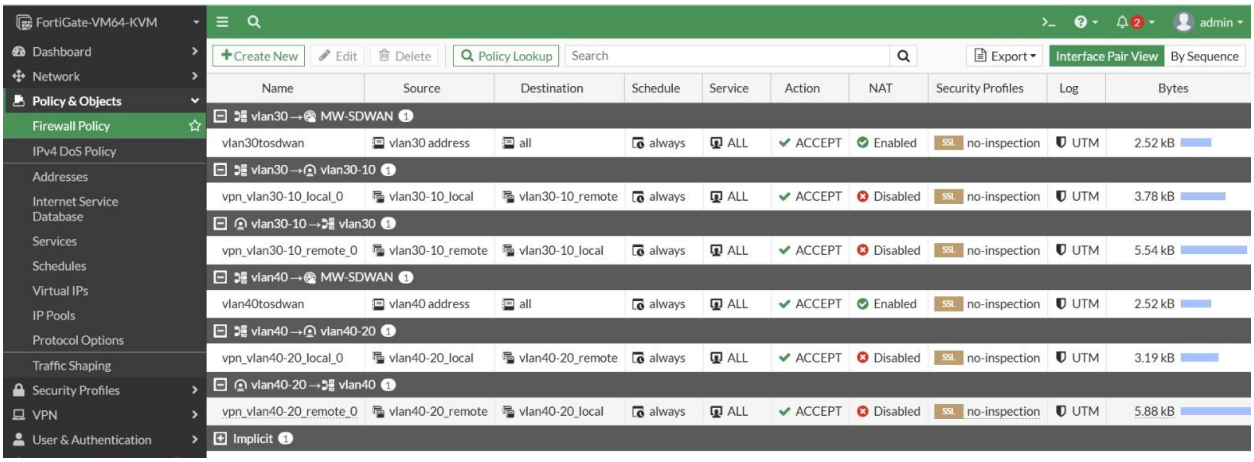
VPN 1st branch:



Source	Device	Destination	Application	Protocol	Source Port	Bytes	Duration (seconds)	Destination Interface
192.168.10.5	PC1	192.168.30.5	ICMP/8	ICMP	2729	168 B	30s	vlan10-30
192.168.10.5	PC1	192.168.30.5	ICMP/8	ICMP	2473	168 B	31s	vlan10-30
192.168.10.5	PC1	192.168.30.5	ICMP/8	ICMP	2217	168 B	32s	vlan10-30
192.168.10.5	PC1	192.168.30.5	ICMP/8	ICMP	1961	168 B	33s	vlan10-30
192.168.10.5	PC1	192.168.30.5	ICMP/8	ICMP	1705	168 B	34s	vlan10-30
192.168.20.5	PC2	192.168.40.5	ICMP/8	ICMP	4777	168 B	23s	vlan20-40
192.168.20.5	PC2	192.168.40.5	ICMP/8	ICMP	4521	168 B	24s	vlan20-40
192.168.20.5	PC2	192.168.40.5	ICMP/8	ICMP	4265	168 B	25s	vlan20-40
192.168.20.5	PC2	192.168.40.5	ICMP/8	ICMP	4009	168 B	26s	vlan20-40
192.168.20.5	PC2	192.168.40.5	ICMP/8	ICMP	5033	168 B	22s	vlan20-40

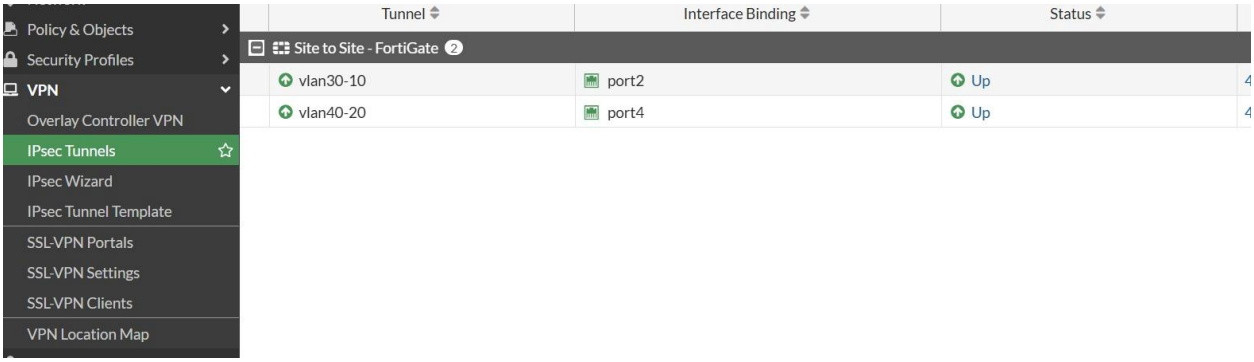


Policy of 1st branch:

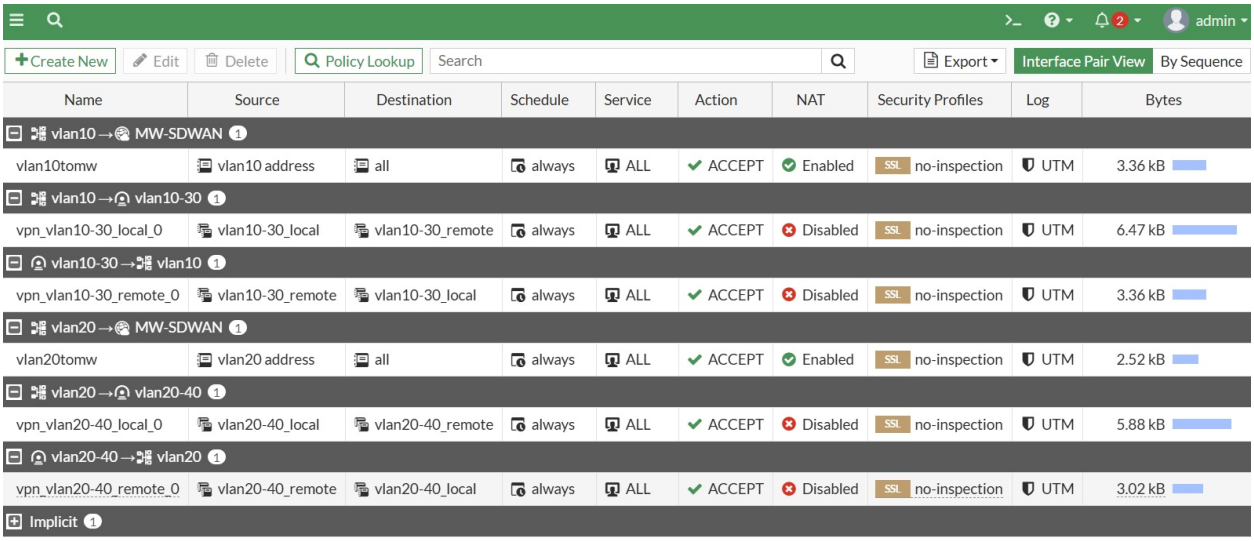


VPN 2nd branch:

Source	Device	Destination	Application	Protocol	Source Port	Bytes	Packets	Duration (seconds)	Destination Int
192.168.30.5	PC3	192.168.10.5	ICMP/8	ICMP	11690	168 B	2	25s	vlan30-10
192.168.40.5	PC4	192.168.20.5	ICMP/8	ICMP	14250	168 B	2	15s	vlan40-20
192.168.30.5	PC3	192.168.10.5	ICMP/8	ICMP	11946	168 B	2	24s	vlan30-10
192.168.40.5	PC4	192.168.20.5	ICMP/8	ICMP	13482	168 B	2	18s	vlan40-20
192.168.40.5	PC4	192.168.20.5	ICMP/8	ICMP	13226	168 B	2	19s	vlan40-20
192.168.40.5	PC4	192.168.20.5	ICMP/8	ICMP	13994	168 B	2	16s	vlan40-20



Policy of 2nd branch:



admin

Create New | Edit | Delete | Policy Lookup | Search | Export | Interface Pair View | By Sequence

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
vlan10 → MW-SDWAN 1									
vlan10tomw	vlan10 address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	3.36 kB
vlan10 → vlan10-30 1									
vpn_vlan10-30_local_0	vlan10-30_local	vlan10-30_remote	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	6.47 kB
vlan10-30 → vlan10 1									
vpn_vlan10-30_remote_0	vlan10-30_remote	vlan10-30_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	3.36 kB
vlan20 → MW-SDWAN 1									
vlan20tomw	vlan20 address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	2.52 kB
vlan20 → vlan20-40 1									
vpn_vlan20-40_local_0	vlan20-40_local	vlan20-40_remote	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	5.88 kB
vlan20-40 → vlan20 1									
vpn_vlan20-40_remote_0	vlan20-40_remote	vlan20-40_local	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	3.02 kB
Implicit 1									

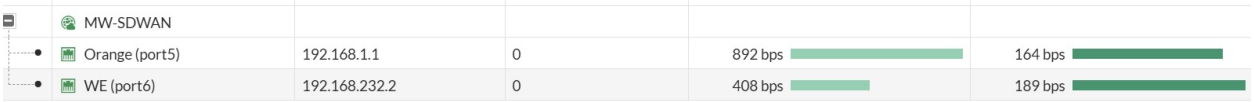
4th: SD-WANs:

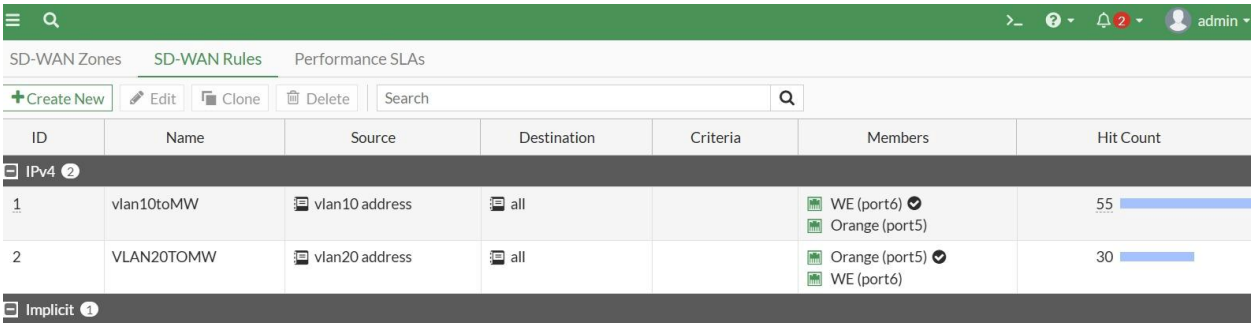
We applied **SD-WAN** configurations on the **WE** and **Orange** links in **Branch 1**, and on the **Vodafone** and **Etisalat** links in **Branch 2**.

In **Branch 1**, the **IT department's traffic** is routed through the **WE** connection, while the **HR department's traffic** is routed through **Orange**.
This behavior is enforced through the **SD-WAN policy**.
The configuration also includes an automatic failover mechanism: if the Orange connection goes down, HR traffic is automatically redirected to the WE link.

In **Branch 2**, the **IT department** is routed through **Etisalat**, and the **HR department** is routed through **Vodafone**, also controlled by the SD-WAN policy.
Similarly, a failover rule is implemented: if the Vodafone link fails, HR traffic is automatically switched to the Etisalat connection.

SD-WAN branch 1:

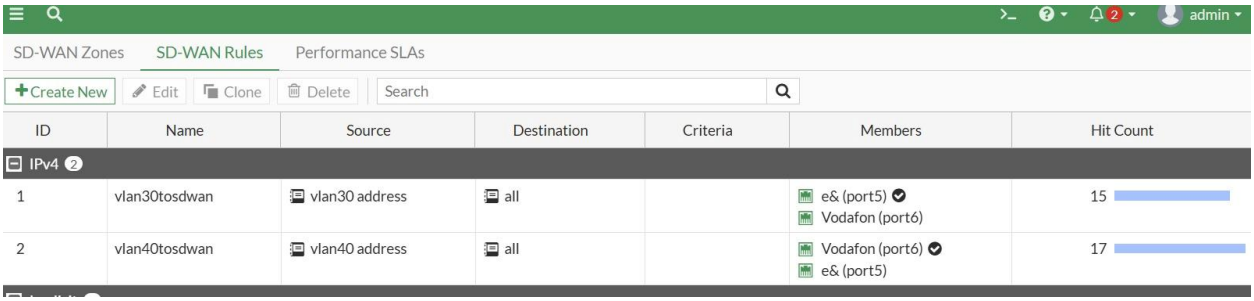




Source	Device	Destination	Application	Protocol	Source Port	Bytes	Duration (seconds)	Destination Interface
192.168.20.5	PC2	8.8.8.8	ICMP/8	ICMP	44457	168 B	45s	Orange (port5)
192.168.20.5	PC2	8.8.8.8	ICMP/8	ICMP	44713	168 B	44s	Orange (port5)
192.168.20.5	PC2	8.8.8.8	ICMP/8	ICMP	43945	168 B	47s	Orange (port5)
192.168.20.5	PC2	8.8.8.8	ICMP/8	ICMP	44201	168 B	46s	Orange (port5)
192.168.10.5	PC1	8.8.8.8	ICMP/8	ICMP	45225	168 B	41s	WE (port6)
192.168.10.5	PC1	8.8.8.8	ICMP/8	ICMP	44969	168 B	43s	WE (port6)
192.168.10.5	PC1	8.8.8.8	ICMP/8	ICMP	45737	168 B	39s	WE (port6)

SD-WAN branch 2:

	MW-SDWAN				
	e& (port5)	192.168.1.1	0	41.65 kbps	5.12 kbps
	Vodafon (port6)	192.168.232.2	0	298 bps	12 bps



Source	Device	Destination	Application	Protocol	Source Port	Bytes	Packets	Duration (seconds)	Destination Int
192.168.30.5	PC3	8.8.8.8	ICMP/8	ICMP	33194	168 B	2	1s	e& (port5)
192.168.30.5	PC3	8.8.8.8	ICMP/8	ICMP	32938	168 B	2	2s	e& (port5)
192.168.30.5	PC3	8.8.8.8	ICMP/8	ICMP	32682	168 B	2	3s	e& (port5)
192.168.40.5	PC4	8.8.8.8	ICMP/8	ICMP	31658	168 B	2	7s	Vodafon (p
192.168.40.5	PC4	8.8.8.8	ICMP/8	ICMP	32426	168 B	2	4s	Vodafon (p
192.168.40.5	PC4	8.8.8.8	ICMP/8	ICMP	32170	168 B	2	6s	Vodafon (p

Conclusion:

In this project, we successfully implemented a secure and structured network solution using FortiGate technologies to support the operational requirements of the merged telecommunications corporation. By segmenting the network through VLANs, assigning DHCP distribution to the firewall, and configuring department-specific IPsec VPN tunnels, we ensured that communication remains strictly controlled and limited to corresponding departments across branches.

Additionally, the application of SD-WAN policies provided intelligent traffic routing and reliable failover capabilities, guaranteeing continuous connectivity and optimal link utilization for both IT and HR departments. These configurations collectively enhanced network security, efficiency, and resilience, delivering a fully functional architecture that meets the organization's communication and performance needs.