

# Établissement d'une connexion VPN sécurisée entre les sites de Casablanca et Rabat via Fortigate



Réalisé par:

WAFAA EL MAIFI

## ***I. Description du projet*** :

Le projet vise à établir une connexion sécurisée entre deux sites distincts, le premier à **Casablanca** et le second à **Rabat** en utilisant la technologie VPN via les pare-feu Fortigate. La connexion entre les deux sites sera configurée pour garantir un échange de données sécurisé et fiable, permettant aux utilisateurs des deux sites d'accéder aux ressources partagées comme s'ils étaient sur le même réseau local.

## ***II. Étapes de base du projet*** :

**Configurer les appliances Fortigate sur chaque site :** les appliances Fortigate seront configurées pour agir comme des pare-feu et fournir une connexion sécurisée entre les deux sites.

**Configuration VPN site à site :** une connexion VPN sera établie entre les deux sites pour garantir que les données sont cryptées et protégées lors de la transmission sur Internet.

**Paramètres de sécurité :** des politiques de sécurité seront définies pour garantir que l'accès au réseau interne se fait uniquement via des canaux cryptés et fiables.

**Test de connexion :** la stabilité de la connexion VPN entre les deux sites sera vérifiée et des tests seront effectués pour garantir un transfert de données sans problème.

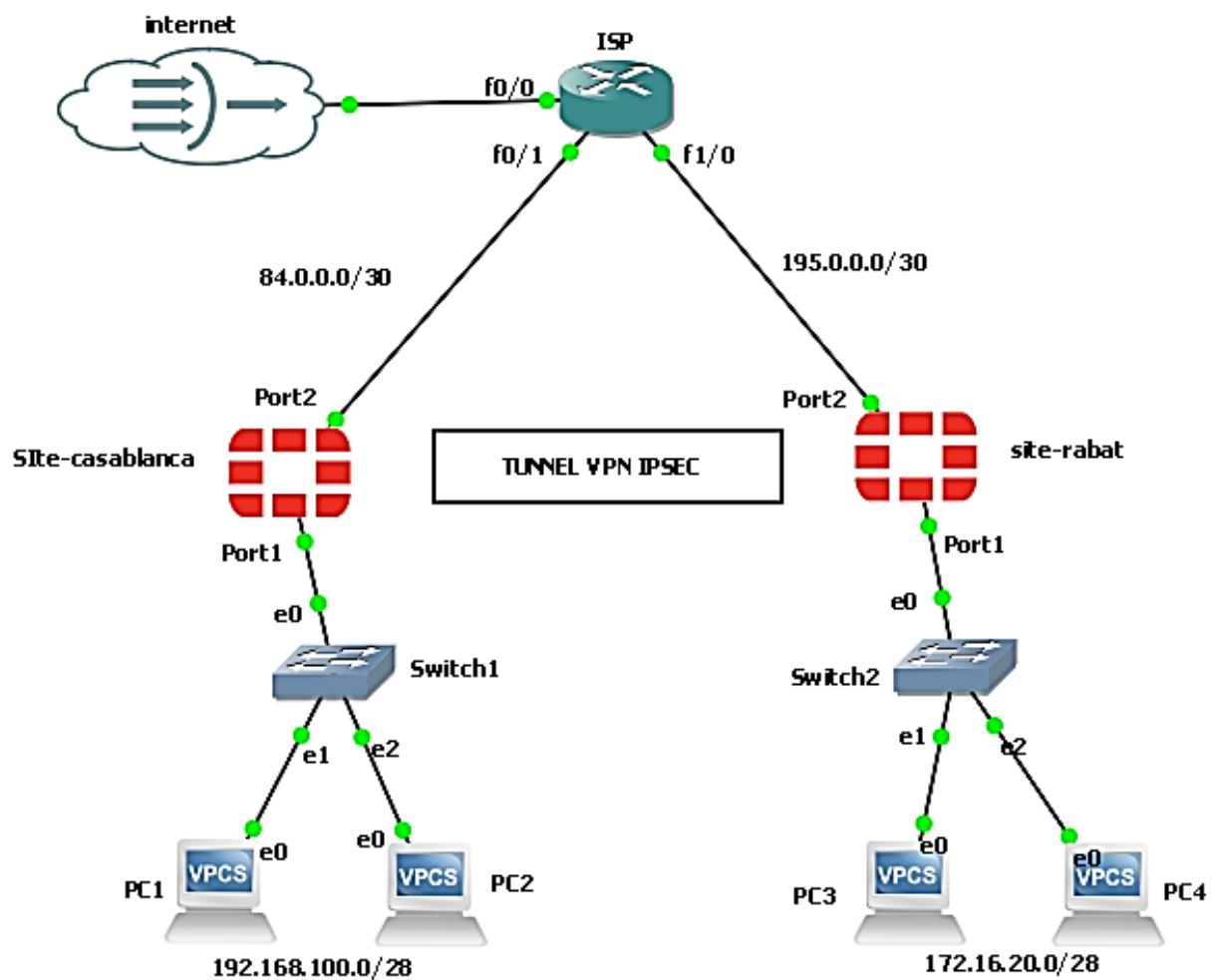
## ***III. Objectifs du projet*** :

**Réaliser la connectivité entre les deux sites :** permettre aux deux sites d'interagir efficacement sur un réseau sécurisé.

**Sécurité améliorée :** assurez la sécurité des données grâce à l'utilisation de techniques de cryptage avancées.

**Assurer la continuité des activités :** Assurer que la communication entre les sites est toujours disponible, ce qui contribue à la continuité des activités entre Casablanca et Rabat.

Topologie réseau simulée avec GNS3 :



Gestion de l'adressage IP sur les équipements réseau :

Périphérique	Interface	Adresse IP	Masque de sousréseau
ISP	F0/1	84.0.0.2	255.255.255.252
	F1/0	195.0.0.2	255.255.255.252
	F0/0	DHCP	
Site-casablanca	Port2	84.0.0.1	255.255.255.252
	Port1	192.168.100.1	255.255.255.240
Site-Rabat	Port2	195.0.0.1	255.255.255.252
	Port1	172.16.20.1	255.255.255.240

Configuration des équipements réseau pour une infrastructure optimale :

## 1. Configuration des interfaces sur le routeur ISP:

```
ISP(config)#interface fastethernet 0/0
ISP(config-if)#ip address dhcp
ISP(config-if)#ip nat outside
ISP(config-if)#no shutdown
```

```
ISP(config)#interface fastethernet 0/1
ISP(config-if)#ip address 84.0.0.2 255.255.255.252
ISP(config-if)#ip nat inside
ISP(config-if)#no shutdown
```

```
ISP(config)#interface fastethernet 1/0
ISP(config-if)#ip address 195.0.0.2 255.255.255.252
ISP(config-if)#ip nat inside
ISP(config-if)#no shutdown
```

### • Vérification des adressage:

```
ISP(config)#do show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.122.235	YES	DHCP	up	up
FastEthernet0/1	84.0.0.2	YES	manual	up	up
FastEthernet1/0	195.0.0.2	YES	manual	up	up

- Configuration du NAT sur le routeur pour l'accès à Internet :

```
ISP(config)#ip access-list standard karim
ISP(config-std-nacl)#permit 84.0.0.0 0.0.0.3
ISP(config-std-nacl)#permit 195.0.0.0 0.0.0.3
ISP(config-std-nacl)#exit
ISP(config)#ip nat inside source list karim interface f0/0
overload
```

## 2. Configuration sur pare-feu :

- Sur le pare-feu sur le site-Casablanca :

Le premier nom d'utilisateur est « **admin** », qui est le nom par défaut **et ne contient aucun mot de passe**. Vous devez définir un mot de passe avant de commencer.

Configuration du port 1 pour la gestion via l'interface web graphique :

```
site-casablanca #config system interface
site-casablanca (interface)#edit port1
site-casablanca (port1) # set mode static
site-casablanca (port1) #set ip address 192.168.100.1 255.255.255.240
site-casablanca (port1) #set alias lan
site-casablanca (port1) #set role lan
site-casablanca (port1) #set allowaccess ping http https snmp ssh
```

Après avoir terminé le processus de configuration, configurez votre carte réseau pour qu'elle appartienne au même réseau 192.168.100.0/28.

Accédez à votre navigateur et saisissez 192.168.100.1



Après avoir entré votre nom d'utilisateur "admin "avec votre mot de passe

A login form with a green header bar containing a white grid icon. Below the header, there are two input fields: 'Username' and 'Password'. At the bottom, there is a green 'Login' button.

### 3. Configuration des ports

Configurer le **port1** pour le réseau interne et activer-le dhcp pour attribuer les adress automatiquement.

A configuration page for a network interface. The 'Name' field is 'lan (port1)'. The 'Alias' field is 'lan'. The 'Type' is 'Physical Interface'. The 'VRF ID' is '0'. The 'Role' is 'LAN'. Below these fields, there is a section for 'Address' configuration. The 'Addressing mode' is set to 'Manual' (highlighted in green), with 'DHCP' and 'Auto-managed by IPAM' as options. The 'IP/Netmask' field is '192.168.100.1/255.255.255.240'. There are two toggle switches: 'Create address object matching subnet' and 'Secondary IP address', both currently turned off.

☒ DHCP Server

DHCP status

Address range

Netmask

Default gateway

DNS server

Lease time ⓘ ☒  second(s)

- Test des périphériques clients du réseau (Site – Casablanca) :

PC1 :

```
PC1>
PC1> ip dhcp
DORA IP 192.168.100.2/28 GW 192.168.100.1
```

PC2 :

```
PC2> ip dhcp
DORA IP 192.168.100.4/28 GW 192.168.100.1
```

- Configurer une route par défaut sur Internet :

Automatic gateway retrieval ⓘ ☐

Destination

Gateway Address

Interface

Administrative Distance ⓘ

Comments  0/255

Status

Advanced Options

- Ajouter une règle pour autoriser les utilisateurs locaux à accéder à Internet

**Edit Policy**

Name	lan-to-wan		
Incoming Interface	lan (port1)		
Outgoing Interface	wan (port2)		
Source	all	+	×
Destination	all	+	×
Schedule	always		
Service	ALL	+	×
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY		
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based		
<b>Firewall / Network Options</b>			
NAT	<input checked="" type="checkbox"/>		
IP Pool Configuration	<input checked="" type="checkbox"/> Use Outgoing Interface Address <input type="checkbox"/> Use Dynamic IP Pool		
Preserve Source Port	<input type="checkbox"/>		
Protocol Options	<input checked="" type="checkbox"/> default <input type="checkbox"/> [edit icon]		
		OK	Cancel



### Notez :

les mêmes configuration que vous ferez pour le pare-feu Site-rabat , changez simplement les address ip.



#### 4. La création du VPN site à site :

##### → Au niveau de parefeu site-casablanca :

Dans cette partie, nous allons créer un tunnel VPN site à site entre deux sites distants, Casablanca et Rabat, en suivant quatre étapes de base :

→ Configurer le VPN : Dans cette étape, nous définissons un nom pour le réseau VPN, le type est VPN Emplacement à emplacement, ainsi que le type d'appareil distant

VPN Creation Wizard

1 VPN Setup

2 Authentication

3 Policy & Routing

4 Review Settings

Name

site\_casablanca

Template type

Site to Site

Hub-and-Spoke

Remote Access

Custom

NAT configuration

No NAT between sites

This site is behind NAT

The remote site is behind NAT

Remote device type

FortiGate

Cisco

Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

< Back

Next >

Cancel

Authentication : L'authentification est une étape cruciale dans la mise en place d'un VPN

Les deux extrémités du tunnel doivent s'authentifier mutuellement pour garantir l'intégrité du lien. ce


Une fois l'appareil distant, l'adresse IP distante, l'interface de sortie et

La méthode d'authentification est une clé pré-partagée. Nous avons choisi **karim@maali** comme clé pré-partagée.


VPN Setup > **2 Authentication** > 3 Policy & Routing > 4 Review Settings

Remote device IP Address Dynamic DNS

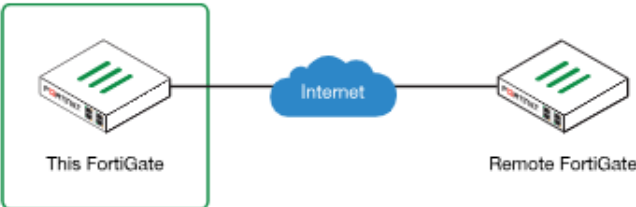
Remote IP address

Outgoing Interface  wan (port2)

Authentication method Pre-shared Key Signature

Pre-shared key  

Site to Site - FortiGate



This FortiGate Remote FortiGate

< Back Next > Cancel

Politiques et conseils : une fois le tunnel VPN établi et l'authentification réussie, nous...

Configurez les politiques de sécurité et les règles de routage pour déterminer quel trafic est autorisé

Via le tunnel VPN et comment il doit être acheminé entre les deux emplacements.

VPN Creation Wizard

☒ VPN Setup > 
 ☒ Authentication > 
 **3 Policy & Routing** > 
 4 Review Settings

Local interface: lan (port1) ✕  
 Local subnets: 192.168.100.0/28  
 Remote Subnets: 172.16.20.0/255.255.255.240  
 Internet Access: None Share Local Use Remote

Site to Site - FortiGate

< Back    Next >    Cancel

Révision des paramètres : Enfin, nous passons en revue tous les paramètres configurés pour le tunnel

VPN, nous assurant que chaque étape a été correctement mise en place et que le tunnel fonctionne

comme prévu. Cette étape de révision garantit la sécurité et l'efficacité du VPN site à site.

VPN Creation Wizard

☒ VPN Setup > 
 ☒ Authentication > 
 ☒ Policy & Routing > 
 **✓ Review Settings**

✓ The VPN has been set up

Object Summary

Phase 1 interface	✓ <span>site-casablanca</span> <span>Edit</span>
Local address group	✓ <span>site-casablanca_local</span> <span>Edit</span>
Remote address group	✓ <span>site-casablanca_remote</span> <span>Edit</span>
Phase 2 interface	✓ <span>site-casablanca</span>
Static route	✓ 2 <span>Edit</span>
Blackhole route	✓ 3 <span>Edit</span>
Local to remote policies	✓ <span>vpn_site-casablanca_local_0 (1)</span>
Remote to local policies	✓ <span>vpn_site-casablanca_remote_0 (2)</span>

Add Another    Show Tunnel List    Active Windows

## ➔ Au niveau du firewall site-Rabat :

### Configuration du VPN :

1 VPN Setup

2 Authentication

3 Policy & Routing

4 Review Settings

Name

site-rabat

Template type

Site to Site

Hub-and-Spoke

Remote Access

Custom

NAT configuration

No NAT between sites

This site is behind NAT

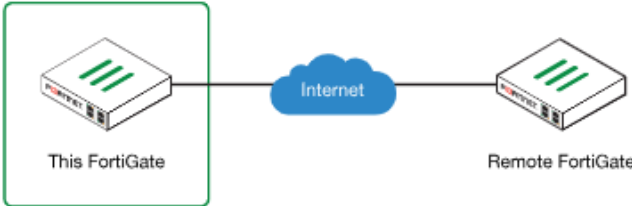
The remote site is behind NAT

Remote device type

FortiGate

Cisco

Site to Site - FortiGate



< Back

Next >

Cancel

### Authentication VPN :

✓ VPN Setup

2 Authentication

3 Policy & Routing

4 Review Settings

Remote device

IP Address

Dynamic DNS

Remote IP address

84.0.0.1

Outgoing Interface

wan (port2)

Authentication method

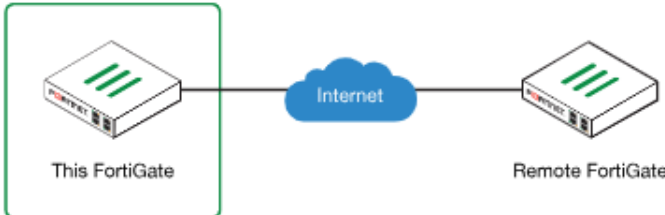
Pre-shared Key

Signature

Pre-shared key

karim@maali

Site to Site - FortiGate



< Back

Next >

Cancel

Politiques et routage :

VPN Creation Wizard

✓ VPN Setup

✓ Authentication

**3 Policy & Routing**

4 Review Settings

Local interface

lan (port1)

+

Local subnets

172.16.20.0/28

+

Remote Subnets

192.168.100.0/255.255.255.240

+

Internet Access

None

Share Local

Use Remote

Site to Site - FortiGate

This FortiGate

Internet

Remote FortiGate

Tests et Vérification du Fonctionnement :

Une fois le tunnel VPN configuré et toutes les politiques de sécurité définies, il est

Il est nécessaire de s'assurer que le réseau fonctionne comme prévu et que toutes les connexions fonctionnent Sûr et efficace :

Vérifier la création du tunnel : les deux tunnels sont créés et activés :

Site to Site - FortiGate 1			
site-casablanca	wan (port2)	Up	4

Site to Site - FortiGate 1			
site-rabat	wan (port2)	Up	4

## Tester la communication entre les des site :

- PC1(Site-casablanca) →→ Pc3(Site-Rabat)

```
PC1> ip dhcp
DORA IP 192.168.100.2/28 GW 192.168.100.1

PC1> ping 172.16.20.3
84 bytes from 172.16.20.3 icmp_seq=1 ttl=62 time=16.579 ms
84 bytes from 172.16.20.3 icmp_seq=2 ttl=62 time=31.582 ms
84 bytes from 172.16.20.3 icmp_seq=3 ttl=62 time=31.945 ms
84 bytes from 172.16.20.3 icmp_seq=4 ttl=62 time=31.560 ms
84 bytes from 172.16.20.3 icmp_seq=5 ttl=62 time=31.515 ms

PC1> █
```

- PC4(Site-Rabat)→→PC2(Site-casablanca)

```
PC4> ip dhcp
DDORA IP 172.16.20.2/28 GW 172.16.20.1

PC4> ping 192.168.100.4
84 bytes from 192.168.100.4 icmp_seq=1 ttl=62 time=32.160 ms
84 bytes from 192.168.100.4 icmp_seq=2 ttl=62 time=31.695 ms
84 bytes from 192.168.100.4 icmp_seq=3 ttl=62 time=31.839 ms
84 bytes from 192.168.100.4 icmp_seq=4 ttl=62 time=31.639 ms
84 bytes from 192.168.100.4 icmp_seq=5 ttl=62 time=31.608 ms

PC4> █
```

## Tester la connexion entre le site et Internet :

- PC1 (site-casablanca)→→(Internet)

```
PC1> ip dhcp
DORA IP 192.168.100.2/28 GW 192.168.100.1

PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=125 time=108.544 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=125 time=93.103 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=125 time=93.222 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=125 time=93.071 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=125 time=93.007 ms

PC1> █
```

- PC4 (site-Rabat)→→(Internet)

```
PC4> ip dhcp
DORA IP 172.16.20.2/28 GW 172.16.20.1

PC4> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=125 time=93.280 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=125 time=93.093 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=125 time=93.146 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=125 time=93.217 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=125 time=93.226 ms

PC4> █
```

**Le tunnel VPN a fonctionné et toutes les données passent par le tunnel et tout est crypté** 

Ce projet a permis de mettre en place une solution de connectivité sécurisée entre deux sites distants à travers un VPN site-à-site, en utilisant des pare-feu Fortigate. L'objectif était de permettre aux ressources des deux sites de communiquer de manière sécurisée via un tunnel crypté, en assurant la confidentialité et l'intégrité des données échangées.