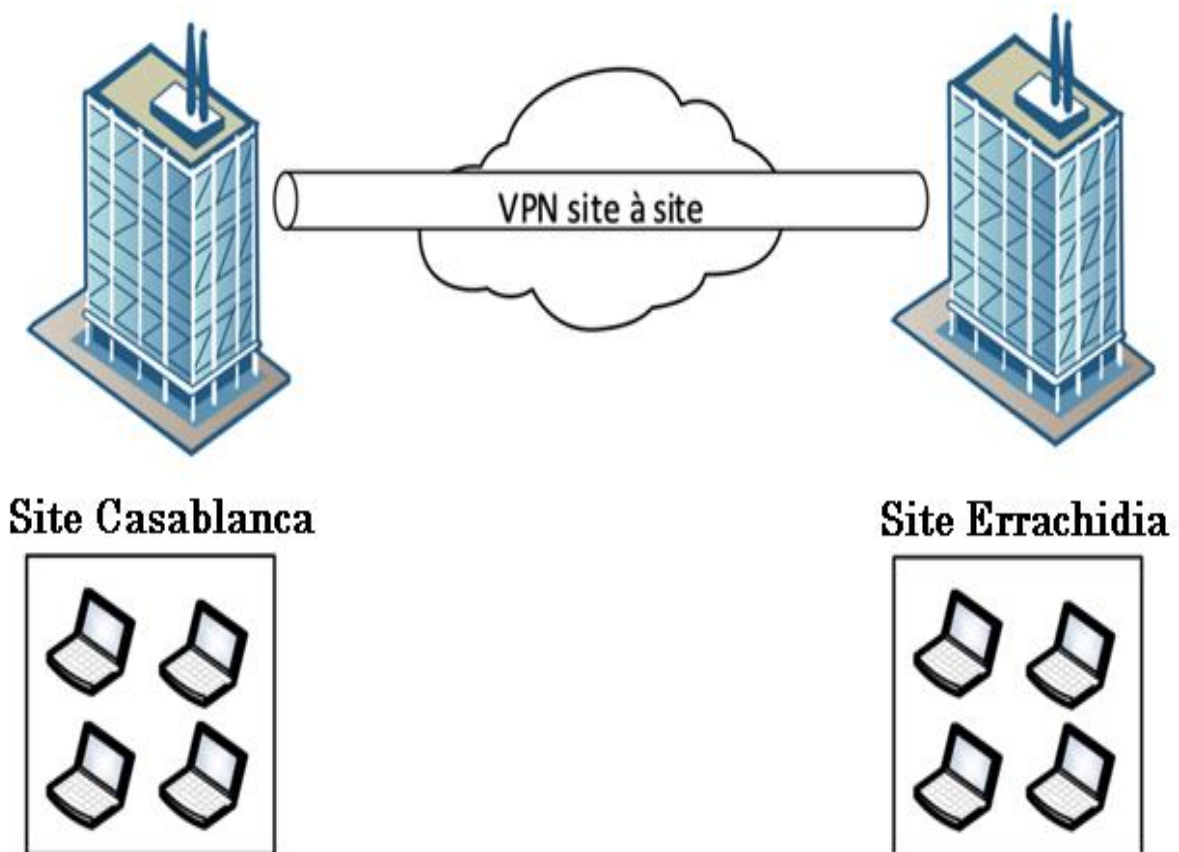




Architecture VPN Site-to-Site : Configuration et Optimisation sous pfSense



Réalisé par : Karim maâli



Introduction

Un VPN site-to-site permet d'établir une connexion sécurisée entre deux réseaux distants via Internet. pfSense, un pare-feu et routeur open-source, offre la possibilité de configurer un VPN site-to-site en utilisant Ipsec.



VPN Site-to-Site

Un VPN (Virtual Private Network) site-to-site est une connexion sécurisée qui permet de relier deux réseaux distincts via Internet comme s'ils étaient sur le même réseau local. Contrairement aux VPN client-à-site, où un utilisateur individuel se connecte à un réseau distant, le VPN site-à-site est conçu pour connecter des infrastructures réseau entières.

Principes de fonctionnement :

Chiffrement : Les données échangées entre les sites sont chiffrées pour garantir leur confidentialité.

Authentification : Les deux passerelles VPN doivent s'authentifier mutuellement avant d'établir la connexion.

Encapsulation : Le trafic réseau est encapsulé dans des paquets IPsec avant d'être transmis via Internet.

Tunnel sécurisé : Un canal chiffré est établi entre les deux sites, garantissant un échange sécurisé des données.



Protocoles utilisés

IKE (Internet Key Exchange) : Permet la négociation et l'établissement des clés de chiffrement.

IPsec (Internet Protocol Security) : Utilisé pour sécuriser les communications entre les sites.

ESP (Encapsulating Security Payload) : Assure l'intégrité et la confidentialité des données transmises.

Description du projet :

Le projet consiste à établir une connexion sécurisée entre deux sites : **Casablanca** et **Errachidia** en utilisant pfSense. L'objectif est de permettre une communication fluide et sécurisée entre les réseaux des deux sites en utilisant un tunnel IPsec.

Objectifs du projet :

- ⇒ Créez une connexion sécurisée entre les sites de Casablanca et d'Errachidia en utilisant le VPN IPsec.
- ⇒ Sécurité des données via un cryptage fort (AES-256, SHA-256).
- ⇒ Faciliter l'accès aux ressources internes des deux sites.
- ⇒ Performances et stabilité améliorées via le protocole IKEv2.
- ⇒ Implémentez des politiques de sécurité strictes sur pfSense.
- ⇒ Réduisez les coûts en utilisant Internet ordinaire au lieu du MPLS.

Infrastructure réseau :

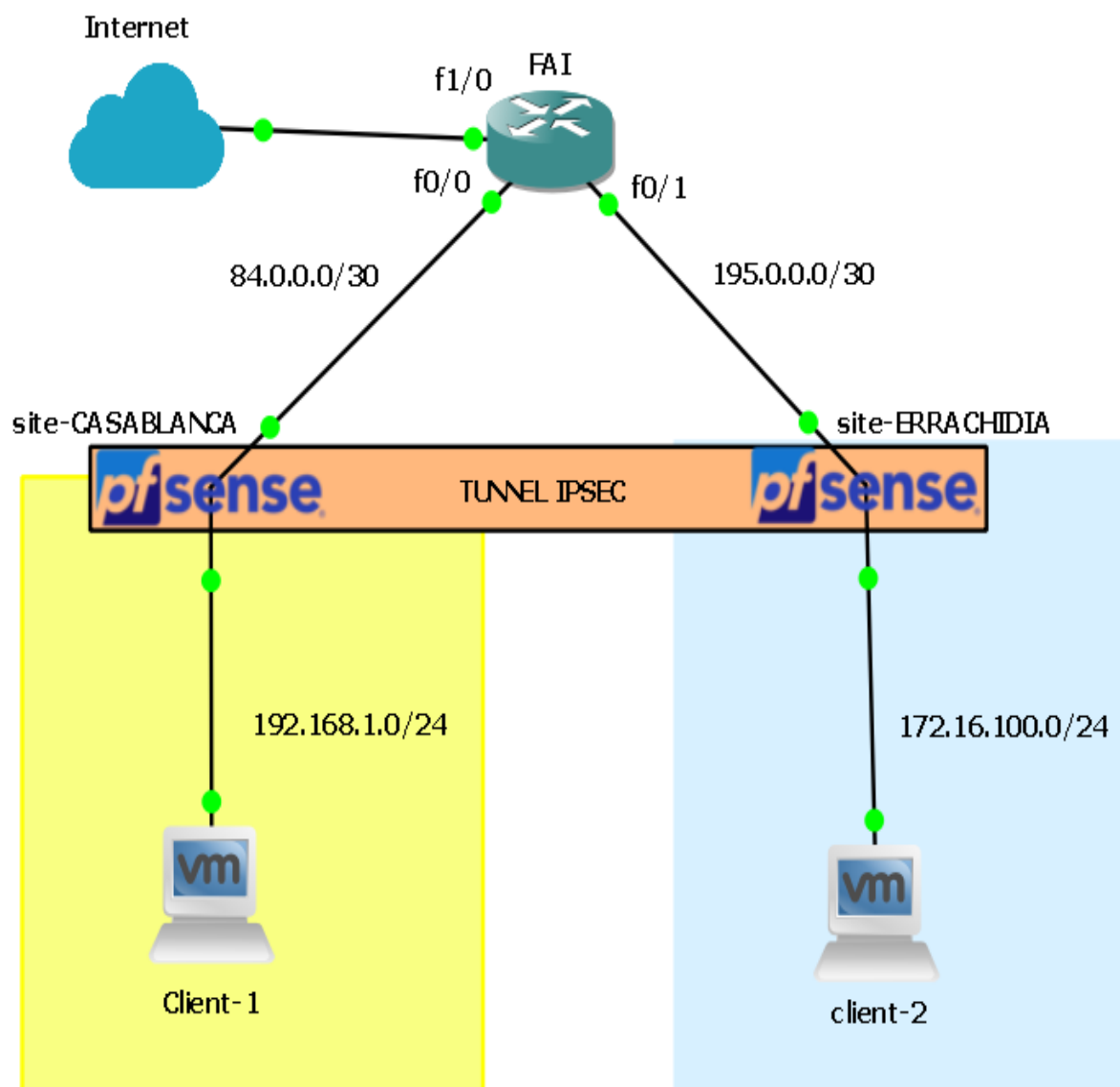
Site Casablanca :

- Réseau local : 192.168.1.0/24
- Adresse IP publique : 84.0.0.2
- Pare-feu : pfSense installé sur un serveur dédié

Site Errachidia :

- Réseau local : 172.16.100.0/24
- Adresse IP publique : 195.0.0.2
- Pare-feu : pfSense installé sur un serveur dédié

Topologie réseau simulée avec GNS3 :



Périphérique	Interface	Adresse IP	Masque de sous réseau	passerelle
FAI	F0/0	84.0.0.1	/30	N/A
	F0/1	195.0.0.1	/30	N/A
	F1/0	DHCP		
Site-casablanca	wan	84.0.0.2	/30	84.0.0.1
	lan	192.168.1.1	/24	N/A
Site-errachidia	Wan	195.0.0.2	/30	195.0.0.1
	Lan	172.16.100.1	/24	N/A

Configuration des équipements réseau pour une infrastructure optimale :

1. Configuration des interfaces sur le routeur FAI

```
FAI(config)#interface fastethernet 1/0
FAI(config-if)#ip address dhcp
FAI(config-if)#ip nat outside
FAI(config-if)#no shutdown
```

```
FAI(config)#interface fastethernet 0/0
FAI(config-if)#ip address 84.0.0.1 255.255.255.252
FAI(config-if)#ip nat inside
FAI(config-if)#no shutdown
```

```
FAI(config)#interface fastethernet 0/1
FAI(config-if)#ip address 195.0.0.1 255.255.255.252
FAI(config-if)#ip nat inside
FAI(config-if)#no shutdown
```

Vérification des adressage:

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

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet1/0	<u>192.168.211.156</u>	YES	DHCP	up	up
FastEthernet0/0	<u>84.0.0.1</u>	YES	manual		up
FastEthernet0/1	<u>195.0.0.1</u>	YES	manual	up	up

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

```
FAI(config)#ip access-list standard karim
FAI(config-std-nacl)#permit 84.0.0.0 0.0.0.3
FAI(config-std-nacl)#permit 195.0.0.0 0.0.0.3
FAI(config-std-nacl)#exit
FAI(config)#ip nat inside source list karim interface
f1/0 overload
```

Une fois le processus de configuration terminé, configurez Votre carte réseau doit être sur le même réseau 192.168.100.0/24 pour site **Casablanca** et 172.16.100.0/24 pour site **errachidia** pour configurer notre pare-feu

3. Configuration sur pare-feu :

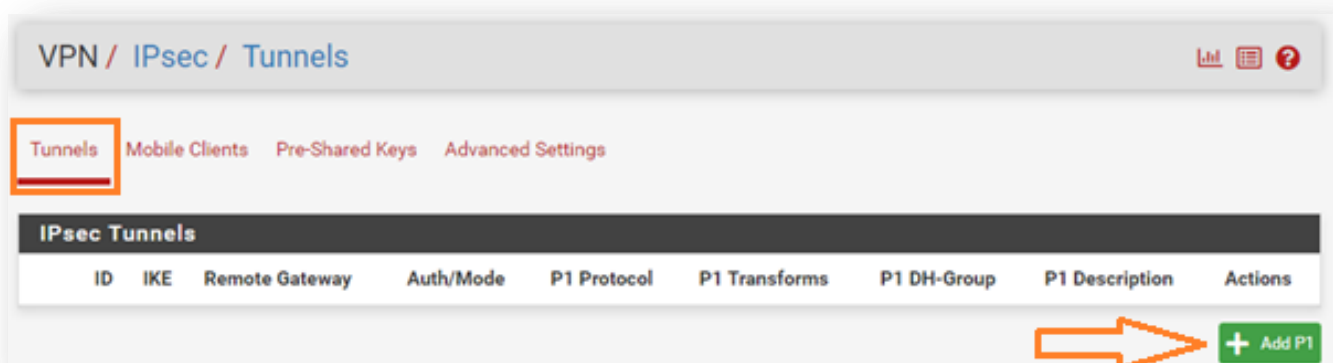
La création du VPN site à site :

✚ Au niveau de parefeu **site-casablanca** :

Étape 1 : Configuration du premier site (Site-casablanca)

Connectez-vous à l'interface web de pfSense (<https://192.168.1.1>).

- ⇒ Allez dans **VPN > IPsec** et cliquez sur l'onglet **Tunnels**.
- ⇒ Cliquez sur **Ajouter un tunnel**.



⇒ Remplissez les paramètres suivants :


Key Exchange Version : IKEv2 .

Interface : WAN.

Remote Gateway : 195.0.0.2


Description	<input type="text" value="phase-1-site-casablanca"/>
A description may be entered here for administrative reference (not parsed).	
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration

Key Exchange version	<input type="text" value="IKEv2"/>
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.	
Internet Protocol	<input type="text" value="IPv4"/>
Select the Internet Protocol family.	
Interface	<input type="text" value="WAN"/>
Select the interface for the local endpoint of this phase1 entry.	
Remote Gateway	<input type="text" value="195.0.0.2"/>
Enter the public IP address or host name of the remote gateway. 	

Pre-Shared Key (PSK) : Définissez une clé partagée (identique sur les deux sites).(karim@maali1978)

Phase 1 Proposal (Authentication)

Authentication Method	<input type="text" value="Mutual PSK"/>
Must match the setting chosen on the remote side.	
My identifier	<input type="text" value="My IP address"/>
Peer identifier	<input type="text" value="Peer IP address"/>
Pre-Shared Key	<input type="text" value="karim@maali1978"/>
Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.	
 Generate new Pre-Shared Key	

Phase 1 (IKE) :

- **Encryption Algorithm** : AES 256.
- **Hash Algorithm** : SHA-256.
- **DH Group** : 14 (2048 bits).

Phase 1 Proposal (Encryption Algorithm)


Encryption Algorithm

AES

256 bits

SHA256

14 (2048)

 Delete

Algorithm


Key length

Hash

DH Group

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.





Add Algorithm

 Add Algorithm




Cliquez sur **Save**, puis **Apply Changes**.



Phase 2 (IPsec SA)

1. Allez dans l'onglet **Phase 2** et cliquez sur **Ajouter**.

IPsec Tunnels										
		ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	Disable	1	V2	WAN 195.0.0.2	Mutual PSK -	AES (256 bits)	SHA256	14 (2048 bit)	phase-1-site-casablanca	  
<div> Show Phase 2 Entries (0)</div>										

IPsec Tunnels

	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Action
<input type="checkbox"/> Disable 	1	V2	WAN 195.0.0.2	Mutual PSK -	AES (256 bits)	SHA256	14 (2048 bit)	phase-1-site-casablanca	 

	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 action
<div> </div>									

- Remplissez les informations :

- **Mode** : Tunnel IPv4.
- **Local Network** : Réseau local du Site casablanca (local subnet).
- **Remote Network** : Réseau local du Site errachidia (172.16.100.0/24).
- **Encryption Algorithm** : AES 256.
- **Hash Algorithm** : SHA-256.
- **PFS Key Group** : 14 (2048 bits).

General Information	
Description	<input type="text" value="phase2-site-casablanca"/> <small>A description may be entered here for administrative reference (not parsed).</small>
Disabled	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
Mode	<input type="text" value="Tunnel IPv4"/>
Phase 1	phase-1-site-casablanca (IKE ID 1)

Networks	
Local Network	<input type="text" value="LAN subnet"/> / <input type="text" value="0"/> <small>Type Address</small> <small>Local network component of this IPsec security association.</small>
NAT/BINAT translation	<input type="text" value="None"/> / <input type="text" value="0"/> <small>Type Address</small> <small>If NAT/BINAT is required on this network specify the address to be translated</small>
Remote Network	<input type="text" value="Network"/> / <input type="text" value="172.16.100.0"/> / <input type="text" value="24"/> <small>Type Address</small> <small>Remote network component of this IPsec security association.</small>

Phase 2 Proposal (SA/Key Exchange)	
Protocol	<input type="text" value="ESP"/> <small>Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.</small>
Encryption Algorithms	<input checked="" type="checkbox"/> AES <input type="text" value="128 bits"/> <input type="checkbox"/> AES128-GCM <input type="text" value="128 bits"/> <input type="checkbox"/> AES192-GCM <input type="text" value="Auto"/> <input checked="" type="checkbox"/> AES256-GCM <input type="text" value="Auto"/> <input type="checkbox"/> CHACHA20-POLY1305
Hash Algorithms	<input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC <small>Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.</small>
PFS key group	<input type="text" value="14 (2048 bit)"/> <small>Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.</small>

Cliquez sur **Save**, puis **Apply Changes**.

Étape 2 : Configuration des règles de pare-feu

Allez dans **Firewall > Rules > wan**

Ajouter une règle autorisant le protocole isakamp



Action : Pass.

Interface : Wan

Address family : ipv4

Protocol : udp

Edit Firewall Rule

Action Pass ▼
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface WAN ▼
Choose the interface from which packets must come to match this rule.

Address Family IPv4 ▼
Select the Internet Protocol version this rule applies to.

Protocol UDP ▼
Choose which IP protocol this rule should match.

Source : address or alias (195.0.0.2)

Destination : address or alias (84.0.0.2)

Detination port : isakmp (500)

Source

Source ☐ Invert match Address or Alias 195.0.0.2 /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Address or Alias 84.0.0.2 /

Destination Port Range

From ISAKMP (500) Custom To ISAKMP (500) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Cliquez sur **Save**, puis **Apply Changes**.

Ajouter une other règle autorisant tout le trafic entre les réseaux locaux des deux sites.

Allez dans **Firewall > Rules > IPsec**.

Floating WAN LAN **IPsec**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
--------	----------	--------	------	-------------	------	---------	-------	----------	-------------	---------

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Action : Pass.

Interface : ipsec

Address family : ipv4

Protocol : any

Edit Firewall Rule

Action Pass
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface IPsec
 Choose the interface from which packets must come to match this rule.

Address Family IPv4
 Select the Internet Protocol version this rule applies to.

Protocol Any
 Choose which IP protocol this rule should match.

Source : any

Destination : any

Source

Source ☐ Invert match Any Source Address /

Destination

Destination ☐ Invert match Any Destination Address /

Cliquez sur **Save**, puis **Apply Changes**.

Au niveau de parefeu **site-errachidia**:

Connectez-vous à l'interface web de pfSense (<https://172.16.100.1>).

Répétez les mêmes étapes sur le second pfSense en inversant les paramètres


⇒ : Allez dans **VPN > IPsec** et cliquez sur l'onglet **Tunnels**.

⇒ Cliquez sur **Ajouter un tunnel**.

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

IPsec Tunnels


ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
 + Add P1								

⇒ Remplissez les paramètres suivants :


Key Exchange Version : IKEv2 .

Interface : WAN.

Remote Gateway : 84.0.0.2

Description	<input type="text" value="phase1-site-errachidia"/>
A description may be entered here for administrative reference (not parsed).	
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE Endpoint Configuration	
Key Exchange version	<input type="text" value="IKEv2"/> Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.
Internet Protocol	<input type="text" value="IPv4"/> Select the Internet Protocol family.
Interface	<input type="text" value="WAN"/> Select the interface for the local endpoint of this phase1 entry.
Remote Gateway	<input type="text" value="84.0.0.2"/> Enter the public IP address or host name of the remote gateway. 

Pre-Shared Key : Identique à celle du Site-casablanca (**karim@maali1978**)

Phase 1 Proposal (Authentication)	
Authentication Method	<input type="text" value="Mutual PSK"/> Must match the setting chosen on the remote side.
My identifier	<input type="text" value="My IP address"/>
Peer identifier	<input type="text" value="Peer IP address"/>
Pre-Shared Key	<input type="text" value="karim@maali1978"/> Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.  Generate new Pre-Shared Key

Phase 1 (IKE) :

- **Encryption Algorithm** : AES 256.
- **Hash Algorithm** : SHA-256.
- **DH Group** : 14 (2048 bits).

Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm

Algorithm

AES

▼

256 bits

▼

Key length

SHA256


▼

Hash

14 (2048)


▼

DH Group

 Delete

Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.





Add Algorithm




 Add Algorithm



Cliquez sur **Save**, puis **Apply Changes**.

Phase 2 (IPsec SA)

1. Allez dans l'onglet **Phase 2** et cliquez sur **Ajouter**.


IPsec Tunnels										
		ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/>	Disable	1	V2	WAN 84.0.0.2	Mutual PSK -	AES (256 bits)	SHA256	14 (2048 bit)	phase1-site-errachidia	  
<div>  Show Phase 2 Entries (0) </div>										

IPsec Tunnels										
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Action	
<input type="checkbox"/> Disable 	1	V2	WAN 84.0.0.2	Mutual PSK -	AES (256 bits)	SHA256	14 (2048 bit)	phase1-site-errachidia	 	

	ID	Local Mode	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 Description	P2 Action
<div>   </div>								

Remplissez les informations :

- **Mode** : Tunnel IPv4.
- **Local Network** : Réseau local du Site errachidia (local subnet).
- **Remote Network** : Réseau local du Site casablanca (192.168.1.0/24).
- **Encryption Algorithm** : AES 256.
- **Hash Algorithm** : SHA-256.
- **PFS Key Group** : 14 (2048 bits).

Description	phase2-site-errachidia		
	A description may be entered here for administrative reference (not parsed).		
Disabled	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.		
Mode	Tunnel IPv4		
Phase 1	phase1-site-errachidia (IKE ID 1) 		
Networks			
Local Network	LAN subnet		/ 0
	Type	Address	
	Local network component of this IPsec security association.		
NAT/BINAT translation	None		/ 0
	Type	Address	
	If NAT/BINAT is required on this network specify the address to be translated		
Remote Network	Network	192.168.1.0	/ 24
	Type	Address	

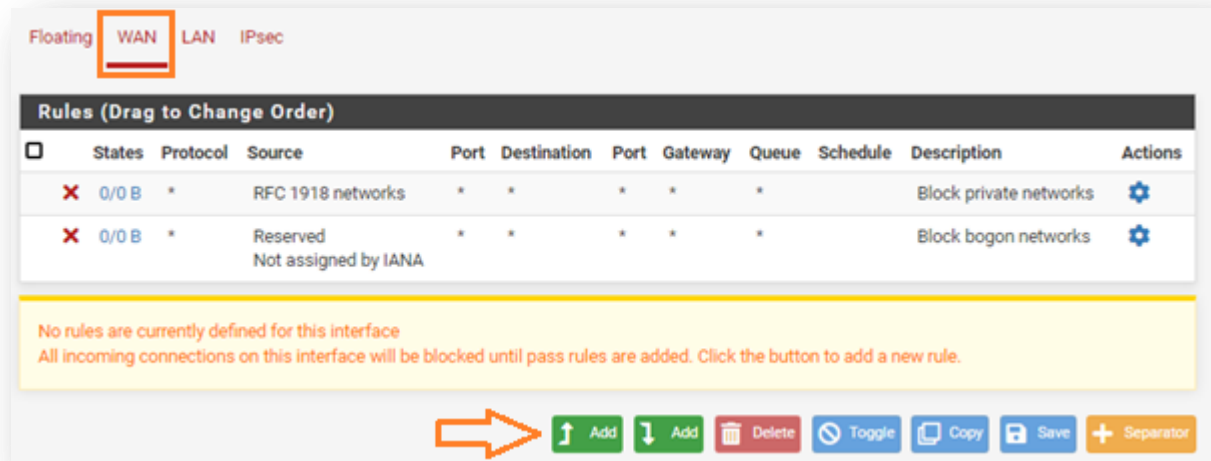
Phase 2 Proposal (SA/Key Exchange)	
Protocol	ESP
	Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.
Encryption Algorithms	<input checked="" type="checkbox"/> AES 128 bits
	<input type="checkbox"/> AES128-GCM 128 bits
	<input type="checkbox"/> AES192-GCM Auto
	<input checked="" type="checkbox"/> AES256-GCM Auto
	<input type="checkbox"/> CHACHA20-POLY1305
Hash Algorithms	<input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC
	Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.
PFS key group	14 (2048 bit)
	Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Cliquez sur **Save**, puis **Apply Changes**.

Configuration des règles de pare-feu

Allez dans **Firewall > Rules > wan**

Ajouter une règle autorisant le protocole isakamp



Action : Pass.

Interface : Wan

Address family : ipv4

Protocol : udp

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

WAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

UDP

Choose which IP protocol this rule should match.

Source : address or alias (84.0.0.2)

Destination : address or alias (195.0.0.2)

Detination port : isakmp (500)

Source

Source ☐ Invert match Address or Alias 84.0.0.2 /

[Display Advanced](#)

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match Address or Alias 195.0.0.2 /

Destination Port Range

From ISAKMP (500) Custom To ISAKMP (500) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Cliquez sur **Save**, puis **Apply Changes**.

Ajouter une other règle autorisant tout le trafic entre les réseaux locaux des deux sites.

Allez dans **Firewall > Rules > IPsec**.

Floating WAN LAN **IPsec**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
--------	----------	--------	------	-------------	------	---------	-------	----------	-------------	---------

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add Add Delete Toggle Copy Save Separator

Action : Pass.

Interface : ipsec

Address family : ipv4

Protocol : any

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	IPsec
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	Any
Choose which IP protocol this rule should match.	

Source : any

Destination : any




Source

Source	<input type="checkbox"/> Invert match	Any	Source Address	/	
---------------	---------------------------------------	-----	----------------	---	--

Destination

Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	
--------------------	---------------------------------------	-----	---------------------	---	--

Cliquez sur **Save**, puis **Apply Changes**.

IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #1	phase1-site- errachidia 	ID: 195.0.0.2 Host: 195.0.0.2:500 SPI: f56ca8781ca5a23f	ID: 84.0.0.2 Host: 84.0.0.2:500 SPI: 4827d028db0e042a	IKEv2 Initiator	Rekey: 14000s (03:53:20) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 9372 seconds (02:36:12) ago  Disconnect P1
 Show child SA entries (1 Connected)							

Tester la communication entre les des sites :

⇒ Client 1 (Site-casablanca) → client 2 (Site-errachidia)

```
C:\Users\karim>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : maroc.ma
    Link-local IPv6 Address . . . . . : fe80::f4e9:5fc2:b850:4059%11
    IPv4 Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::e80:6bff:fe1f:1%11
                                192.168.1.1

Tunnel adapter isatap.maroc.ma:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : maroc.ma

C:\Users\karim>ping 172.16.100.10

Pinging 172.16.100.10 with 32 bytes of data:
Reply from 172.16.100.10: bytes=32 time=44ms TTL=126
Reply from 172.16.100.10: bytes=32 time=22ms TTL=126
Reply from 172.16.100.10: bytes=32 time=33ms TTL=126
Reply from 172.16.100.10: bytes=32 time=30ms TTL=126

Ping statistics for 172.16.100.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 44ms, Average = 32ms
```

⇒ Client 2 (Site-errachidia) → client 1(Site-casablanca)

```
C:\Users\karim>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : maroc.ma
    Link-local IPv6 Address . . . . . : fe80::e476:3b9d:ba09:b72a%11
    IPv4 Address. . . . . : 172.16.100.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.100.1

Tunnel adapter isatap.maroc.ma:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : maroc.ma

C:\Users\karim>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=92ms TTL=126
Reply from 192.168.1.100: bytes=32 time=32ms TTL=126
Reply from 192.168.1.100: bytes=32 time=30ms TTL=126
Reply from 192.168.1.100: bytes=32 time=29ms TTL=126

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 29ms, Maximum = 92ms, Average = 45ms

C:\Users\karim>█
```

Tester la connexion entre le site et Internet :

⇒ Client 1 (site-casablanca) → (Internet)

```
C:\Users\karim>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : maroc.ma
    Link-local IPv6 Address . . . . . : fe80::f4e9:5fc2:b850:4059%11
    IPv4 Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::e80:6bff:fe1f:1%11
                                192.168.1.1

Tunnel adapter isatap.maroc.ma:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : maroc.ma

C:\Users\karim>ping google.com

Pinging google.com [172.217.168.174] with 32 bytes of data:
Reply from 172.217.168.174: bytes=32 time=101ms TTL=126
Reply from 172.217.168.174: bytes=32 time=85ms TTL=126
Reply from 172.217.168.174: bytes=32 time=84ms TTL=126
Reply from 172.217.168.174: bytes=32 time=83ms TTL=126

Ping statistics for 172.217.168.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 83ms, Maximum = 101ms, Average = 88ms
```

⇒ Client 2 (site-errachidia) → (Internet)

```
C:\Users\karim>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : maroc.ma
    Link-local IPv6 Address . . . . . : fe80::e476:3b9d:ba09:b72a%11
    IPv4 Address. . . . . : 172.16.100.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.100.1

Tunnel adapter isatap.maroc.ma:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : maroc.ma

C:\Users\karim>ping google.com

Pinging google.com [142.250.184.174] with 32 bytes of data:
Reply from 142.250.184.174: bytes=32 time=90ms TTL=126
Reply from 142.250.184.174: bytes=32 time=87ms TTL=126
Reply from 142.250.184.174: bytes=32 time=86ms TTL=126
Reply from 142.250.184.174: bytes=32 time=84ms TTL=126

Ping statistics for 142.250.184.174:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 84ms, Maximum = 90ms, Average = 86ms

C:\Users\karim>
```

Inspection du Trafic VPN Site-to-Site sur pfSense à l'aide de Wireshark :

No.	Time	Source	Destination	Protocol	Length	Info
149	32.606992	84.0.0.2	195.0.0.2	ESP	130	ESP (SPI=0xcd8e4244)
150	32.627327	195.0.0.2	84.0.0.2	ESP	130	ESP (SPI=0xc24ae012)
155	33.622818	84.0.0.2	195.0.0.2	ESP	130	ESP (SPI=0xcd8e4244)
156	33.657546	195.0.0.2	84.0.0.2	ESP	130	ESP (SPI=0xc24ae012)
161	34.626700	84.0.0.2	195.0.0.2	ESP	130	ESP (SPI=0xcd8e4244)
162	34.656958	195.0.0.2	84.0.0.2	ESP	130	ESP (SPI=0xc24ae012)
167	35.618724	84.0.0.2	195.0.0.2	ESP	130	ESP (SPI=0xcd8e4244)
168	35.641020	195.0.0.2	84.0.0.2	ESP	130	ESP (SPI=0xc24ae012)

> Frame 161: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface	0000	c2 01 32 e0 00 00 0c
> Ethernet II, Src: 0c:80:6b:1f:00:00 (0c:80:6b:1f:00:00), Dst: 14:00:00:00:00:00	0010	00 74 27 5d 00 00 40
> Internet Protocol Version 4, Src: 84.0.0.2, Dst: 195.0.0.2	0020	00 02 cd 8e 42 44 00
> Encapsulating Security Payload	0030	00 0e e5 46 4f 87 e4
ESP SPI: 0xcd8e4244 (3448652356)	0040	0d e5 b9 55 1b c5 a9
ESP Sequence: 15	0050	3a 0e d1 29 ba 45 29
	0060	23 d5 a0 b7 4e 6c 15
	0070	d8 14 7a de 2f e8 d8
	0080	ab 6f

Type de protocole : les paquets semblent être du protocole **ESP (Encapsulating Security Payload)**, qui fait partie du VPN IPsec, indiquant que la connexion utilise le cryptage pour protéger les données.

Instructions:

Source : 84.0.0.2

Destination : 195.0.0.2

Cela indique qu'il existe une connexion VPN site à site entre les deux réseaux, où les paquets sont échangés entre les deux appareils via l'ESP.

Cryptage : Grâce à l'utilisation d'ESP, le contenu à l'intérieur des paquets est crypté et ne peut pas être visualisé directement sans décryptage à l'aide de clés VPN.

La connexion entre les deux sites s'effectue correctement via un VPN site à site utilisant IPsec.

