Infrastructure

Contexte

La SNCF a récemment pris conscience de l'importance de sécuriser son réseau interne et d'optimiser ses performances. Pour répondre à cette exigence, elle a décidé de mettre en place une infrastructure robuste en utilisant pfSense comme pare-feu et du matériel Cisco pour assurer la connectivité réseau.

L'objectif ultime de ce projet est de créer une infrastructure réseau sécurisée et efficace, garantissant une protection maximale des données de l'entreprise tout en assurant une connectivité rapide et fiable entre les différents sites.

Situation professionnelle :

En tant qu'ingénieur réseau chez la SNCF, la mission consiste à mettre en place une infrastructure réseau solide en utilisant pfSense comme pare-feu et du matériel Cisco pour assurer une connectivité optimale entre les différents sites de l'entreprise.

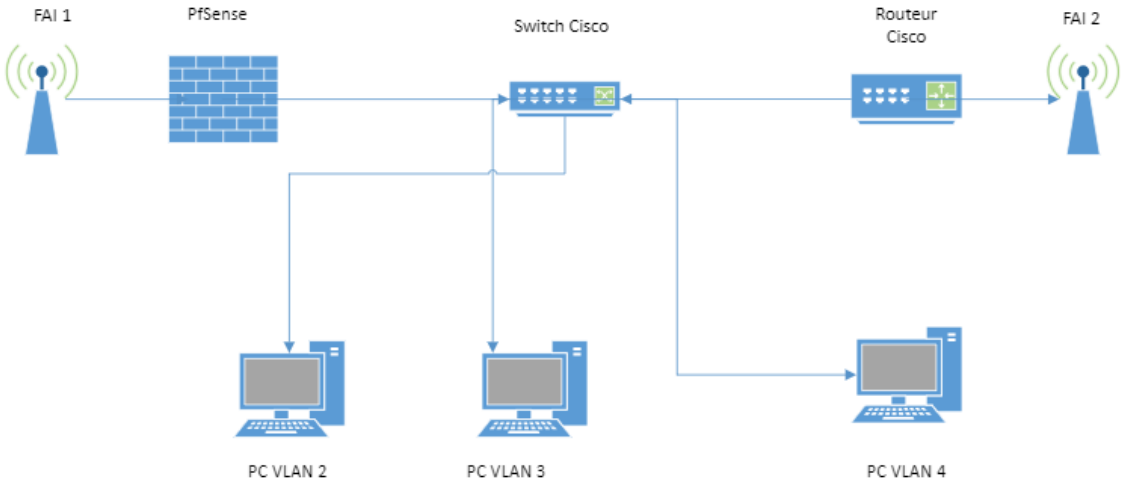
Objectifs de la mission :

1. Mettre en place un pare-feu pfSense pour sécuriser le réseau de l'entreprise et filtrer le trafic réseau entrant et sortant.
2. Configurer les équipements Cisco, y compris les commutateurs et les routeurs, pour assurer une connectivité réseau efficace.
3. Optimiser les performances du réseau en configurant les paramètres appropriés sur les équipements Cisco et pfSense.
4.

Coût de la mission :

- Durée : 3 jours.
- Rémunération : 100 euros net par jour.
- Matériel : Achat si nécessaire.

1 .Schéma Simplifié



Vlan 2 : 192.168.2.0 /24

Vlan 3 : 192.168.3.0 /24

Vlan 4 : 192.168.4.0 /24

IP PfSense : 10.10.2.254

*Nous avons autoriser tous les trafics sur le PfSense pour le test.

2.Configuration des équipements Cisco

Switch :

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		notconnect	2	auto	auto	10/100BaseTX
Fa0/2		notconnect	2	auto	auto	10/100BaseTX
Fa0/3		connected	2	a-full	a-100	10/100BaseTX
Fa0/4		notconnect	2	auto	auto	10/100BaseTX
Fa0/5		notconnect	3	auto	auto	10/100BaseTX
Fa0/6		notconnect	3	auto	auto	10/100BaseTX
Fa0/7		notconnect	3	auto	auto	10/100BaseTX
Fa0/8		notconnect	3	auto	auto	10/100BaseTX
Fa0/9		notconnect	4	auto	auto	10/100BaseTX
Fa0/10		notconnect	4	auto	auto	10/100BaseTX
Fa0/11		notconnect	4	auto	auto	10/100BaseTX
Fa0/12		notconnect	4	auto	auto	10/100BaseTX
Fa0/13		notconnect	1	auto	auto	10/100BaseTX
Fa0/14		notconnect	1	auto	auto	10/100BaseTX
Fa0/15		notconnect	1	auto	auto	10/100BaseTX
Fa0/16		notconnect	1	auto	auto	10/100BaseTX
Fa0/17		notconnect	1	auto	auto	10/100BaseTX
Fa0/18		notconnect	1	auto	auto	10/100BaseTX
Fa0/19		notconnect	1	auto	auto	10/100BaseTX
Fa0/20		notconnect	1	auto	auto	10/100BaseTX
Fa0/21		connected	trunk	a-full	a-100	10/100BaseTX

Routeur :

```
!
interface GigabitEthernet0/1
 ip address 10.10.2.253 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.4
 encapsulation dot1Q 4
 ip address 192.168.4.254 255.255.255.0
!
```

```
router ospf 2
 network 10.10.0.0 0.0.255.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
!
```

3.Configuration PfSense

Dans un premier temps nous allons paramétrer les vlan 2 et 3

VLAN Interfaces

Interface	VLAN tag	Priority	Description	Actions
igc1 (lan)	2		vlan 2	
igc1 (lan)	3		vlan 3	

Interface	Network port	
WAN	igc0 (28:b1:33:00:5a:7d)	
LAN	igc1 (28:b1:33:00:5a:7e)	Delete
OPT1	VLAN 2 on igc1 - lan (vlan 2)	Delete
OPT2	VLAN 3 on igc1 - lan (vlan 3)	Delete

Ensuite nous allons paramétrer l'OSPF dans l'ordre ci-dessous

Services / FRR / Global Settings

Global Settings | Access Lists | Prefix Lists | Route Maps | Raw Config | [BFD] | [BGP] | [OSPF]

General Options

Enable ☑ Enable FRR

Default Router ID

Specify the default Router ID. RID is the highest logical (loopback) IP address configured on a router.
For more information on router identifiers see wikipedia.
Per-daemon configuration will take precedence over this setting.

Master Password 123456789

Password to access the management daemons. Required.

Encrypt Password ☐ Enable password encryption service.

Ignore IPsec Restart ☐ Ignore IPsec restart events. When unchecked, IPsec VTI interfaces will be reset in FRR when IPse becoming inactive in the routing table after interface events.

CARP Status IP None

Used to determine the CARP status. When the CARP vhid is in BACKUP status, FRR will not be starte

Route Handling

Networks marked **Do Not Accept** will be prevented from having exact-matching routes accepted from routing protocols
Networks marked **Null Route** will never be routed, and traffic destined for these networks will be dropped.
Networks with a selected **Static Route Target** will have a route entered into the FRR/Zebra static route table, which can be used by other protocols for route redistribution. The **Null Route** option takes precedence and will cause this option to be ignored. These routes are also added to the operating system routing table.

Routes	☐	☐	10.10.0.0/16	Interface: LAN	Delete
	☐	☐	192.168.0.0/16	Interface: OPT1	Delete
	☐ Do Not Accept	☐ Null Route	192.168.0.0/16 Subnet	Interface: OPT2 Static Route Target	Delete
Add	+ Add				

OSPF Networks

DEPRECATED: Define areas and use areas on interfaces instead. Use route-maps and distribute lists to limit distributed networks.
The networks listed below define valid connected networks to redistribute to OSPF neighbors.
The exact networks specified will not be distributed, but instead determine which interfaces will be active in OSPF.
To advertise an interface network without activating it for OSPF, define it on the Interfaces tab and mark it as a Passive Interface.
Interfaces must have link and be up or their networks will not be advertised.
These rules take precedence over any redistribute options specified above.
Networks listed here will conflict with overlapping interface networks and may prevent ospfd from starting.

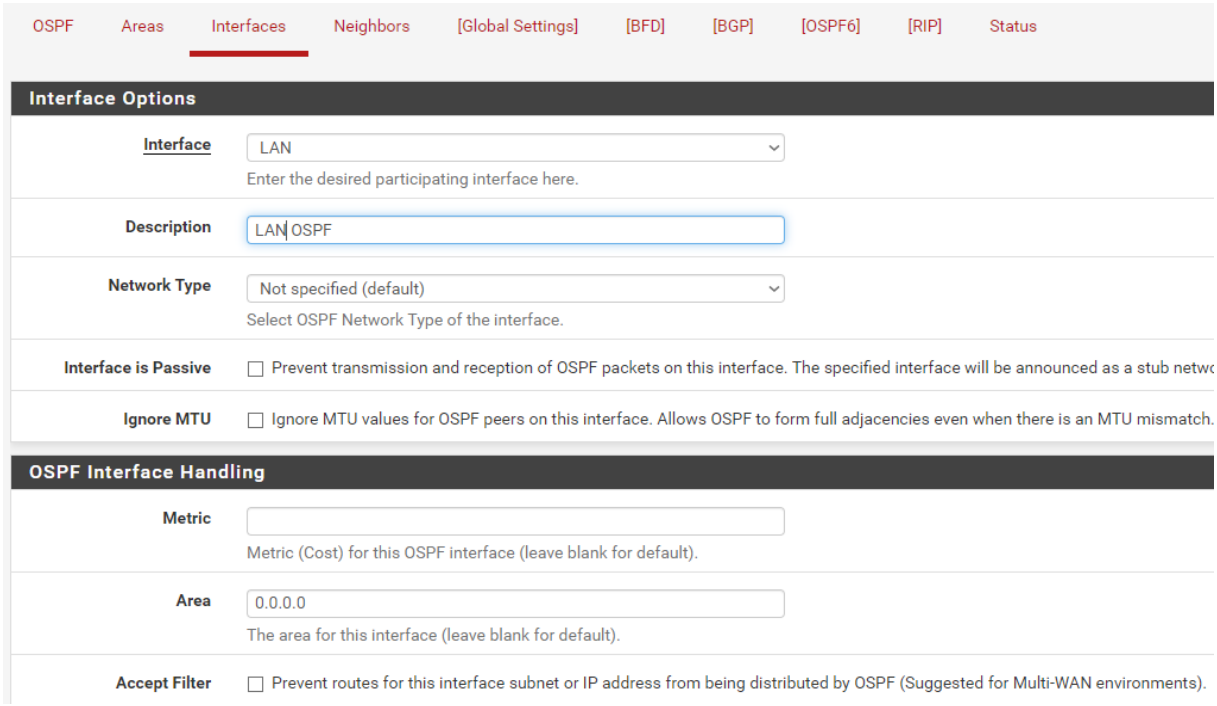
OSPF Networks	10.10.0.0/16	0.0.0.0	Delete
	192.168.0.0/16 OSPF Subnet	0.0.0.0 Area ID	Delete

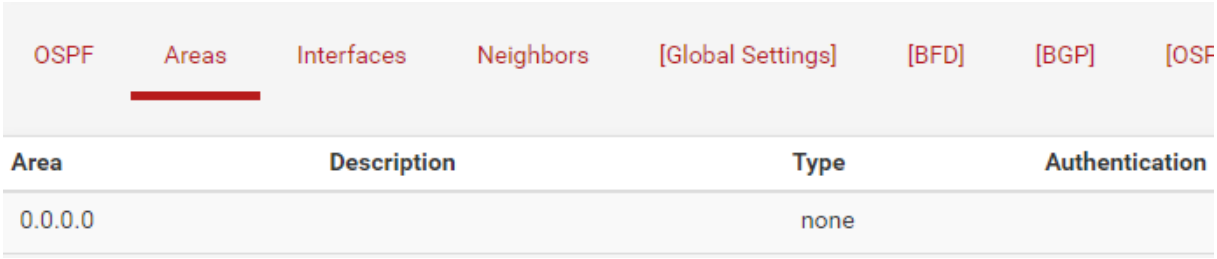
Services / FRR / OSPF / OSPF

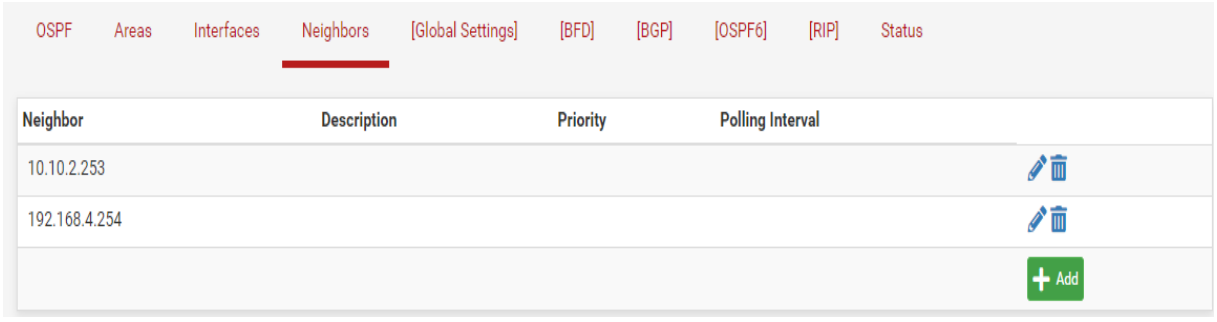
OSPF | Areas | Interfaces | Neighbors | [Global Settings] | [BFD] | [BGP] | [OSPF6] | [RIP] | Status

General Options

Enable	☑ Enable OSPF Routing
Log Adjacency Changes	☐ If set to yes, adjacency changes will be written via syslog.
Router ID	10.10.2.254 Override the default Router ID. RID is the highest logical (loopback) IP address configured on a router. For more information on router identifiers see wikipedia.


OSPF
Areas
Interfaces
Neighbors
[Global Settings]
[BFD]
[BGP]
[OSPF6]
[RIP]
Status
Interface Options
Interface
LAN
Enter the desired participating interface here.
Description
LAN OSPF
Network Type
Not specified (default)
Select OSPF Network Type of the interface.
Interface is Passive
Prevent transmission and reception of OSPF packets on this interface. The specified interface will be announced as a stub netwo
Ignore MTU
Ignore MTU values for OSPF peers on this interface. Allows OSPF to form full adjacencies even when there is an MTU mismatch.
OSPF Interface Handling
Metric
Metric (Cost) for this OSPF interface (leave blank for default).
Area
0.0.0.0
The area for this interface (leave blank for default).
Accept Filter
Prevent routes for this interface subnet or IP address from being distributed by OSPF (Suggested for Multi-WAN environments).


OSPF
Areas
Interfaces
Neighbors
[Global Settings]
[BFD]
[BGP]
[OSF
Area
Description
Type
Authentication
0.0.0.0
none


OSPF
Areas
Interfaces
Neighbors
[Global Settings]
[BFD]
[BGP]
[OSPF6]
[RIP]
Status
Neighbor
Description
Priority
Polling Interval
10.10.2.253
192.168.4.254
Add

4.Résultat :

On constate que le PfSense et le routeur communique