

**PARE-FEU FORTIGATE**

# **Configurer une Interface Réseau Physique**



**Maîtrisez la configuration depuis l'interface  
web ou la ligne de commande FortiOS**

**LE GUIDE RAPIDE ET COMPLET  
POUR ADMINISTRATEURS RÉSEAU**



**FORTINET**

### 3- FIREWALL POLICIES

#### Qu'est ce qu'une règle de sécurité ?

Les règles de sécurité ( Policies) permettent de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité.

Les règles de firewall sont exécutées de haut en bas.

Pour créer une règle de sécurité il faut configurer certains éléments essentiels à savoir :

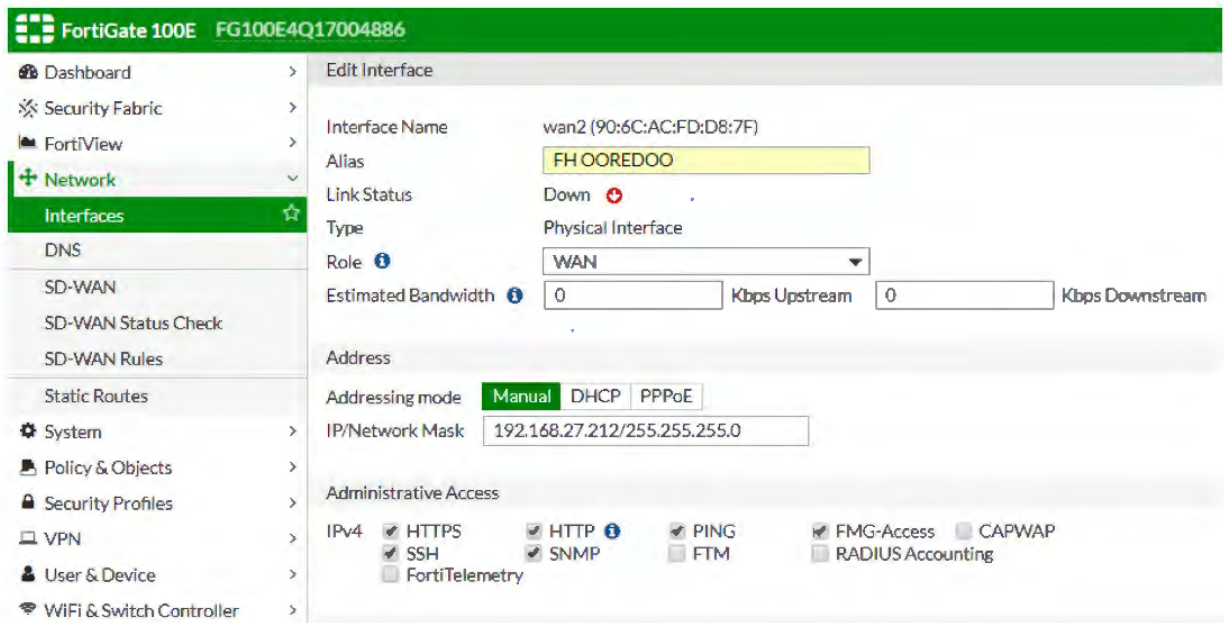
- Interface
- Source et Destination
- Service
- Shedeling
- Profils de sécurité
- Action
- Trafic Shapers

#### Gestion des interfaces

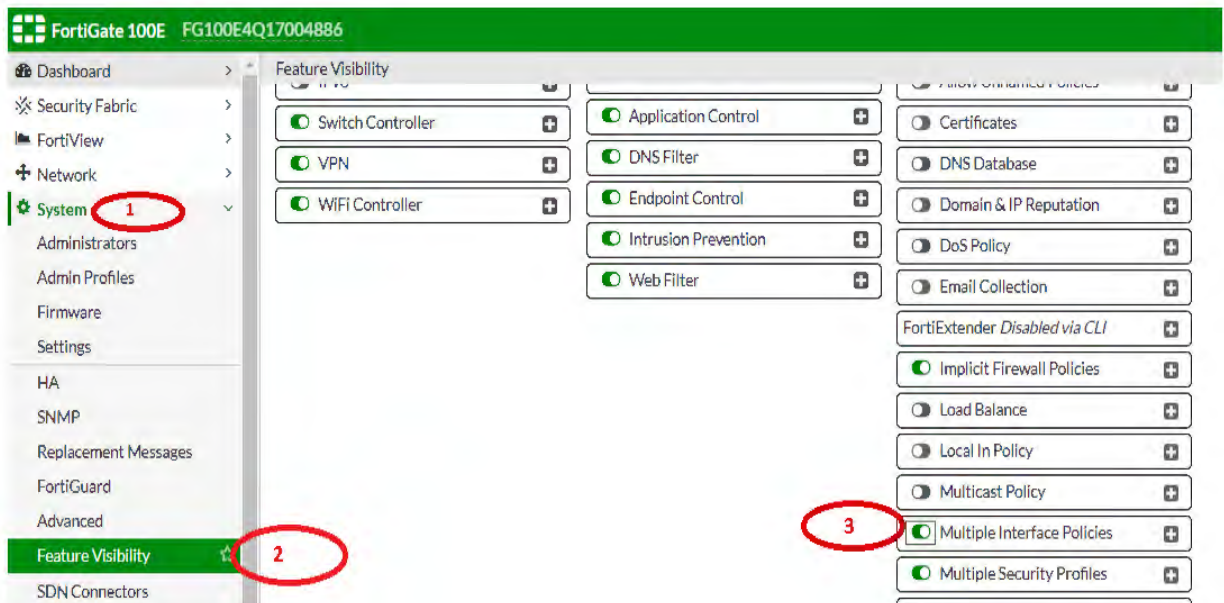
Pour créer une interface il faut l'associer à un port vacant de FortiGate comme suit :

Status	Name	Members	IP/Netmask	Type
Hardware Switch (1)				
	lan		192.168.100.99 255.255.255.0	Hardware Switch (12)
Physical (8)				
+	dmz (Vocalcom-Local-Server)		192.168.26.220 255.255.255.0	Physical Interface
+	ha1		0.0.0.0 0.0.0.0	Physical Interface
+	ha2		0.0.0.0 0.0.0.0	Physical Interface
+	mgmt		192.168.1.99 255.255.255.0	Physical Interface
+	port3 (WIFI-Cisco-AP)		172.17.11.254 255.255.255.0	Physical Interface
+	port5 (Voip-Mgmt)		172.17.5.254 255.255.255.0	Physical Interface
+	wan1 (FO)		41.231.83.46 255.255.255.252	Physical Interface
+	wan2		192.168.27.212 255.255.255.0	Physical Interface
Redundant (7)				
+	LAN	port1, port2	0.0.0.0 0.0.0.0	Redundant Interface (2)

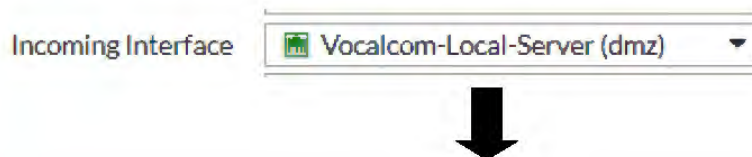
Accéder à l'interface et mettre les paramètres de cette dernière puis valider:



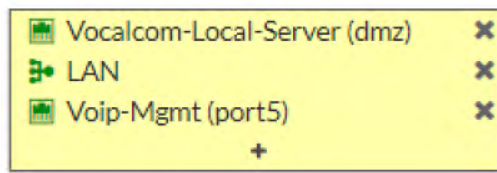
Il est possible de choisir de multiples interface au niveau d'une policy pour celà il faut activer cette fonctionnalité comme suit :



Par la suite l'affichage changera comme suit au niveau de la règle :



Incoming Interface



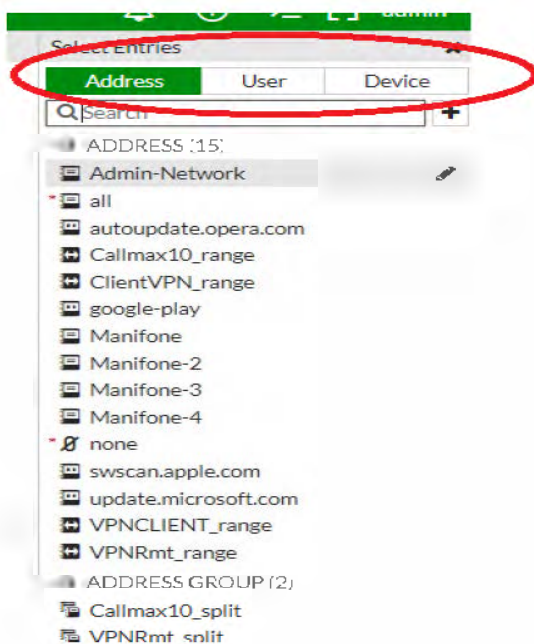
Idem pour Outging Interface.

## Gestion d'une Policy (règle)

Les sources et les destinations d'une Policy peuvent être :

- Adresse ou un regroupement d'adresse
- utilisateur ou un groupe d'utilisateur
- Dispositif (exemple ; Iphone, PC Windows, Imprimante...)

Ils sont déterminés comme suit:



## Création d'adresse

Il existe plusieurs types d'adresses

- FQDN: un site ou un domaine
- Geography : par pays
- IP Range : une plage d'adresse IP
- Subnet: une adresse IP



Type

Subnet
FQDN
Geography
IP Range
Subnet

**FortiGate 100E FG100E4Q17004886**

Dashboard > New Address

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

IPv4 Policy >

**Addresses** ☆

Internet Service Database

Services

Schedules

Virtual IPs

Name callmax

Color [Change]

Type Subnet

Subnet / IP Range 41.231.83.46

Interface any

Show in Address List ☒

Static Route Configuration ☐

Comments 0/255

## Création d'utilisateur ou groupe d'utilisateur

**FortiGate 100E FG100E4Q17004886**

Dashboard > Edit User

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

**User & Device** >

**User Definition** ☆

User Name Callmax2

User Account Status ☒ Enabled ☐ Disabled

User Type Local User

Password .....

Email Address

User Group ☒ SSLVPN-FrGrp

☐ SMS

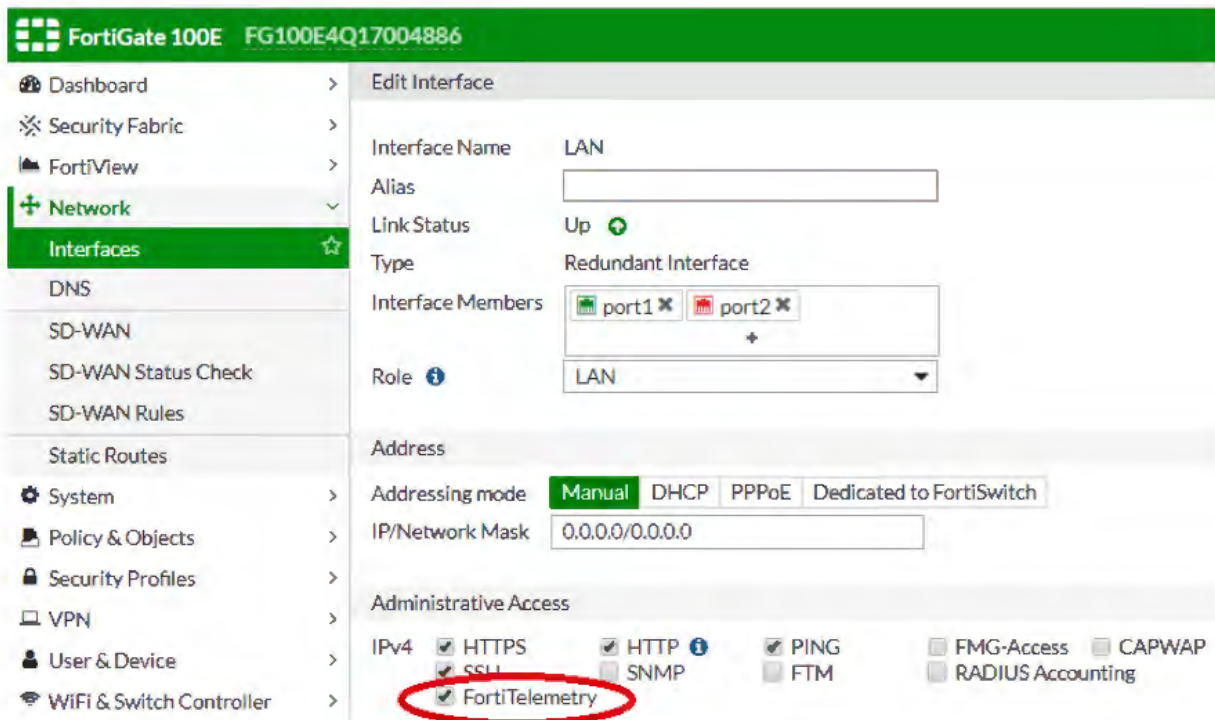
## Identification de dispositif ( Devices)

L'accès au Firewall peut se faire par 2 méthodes :

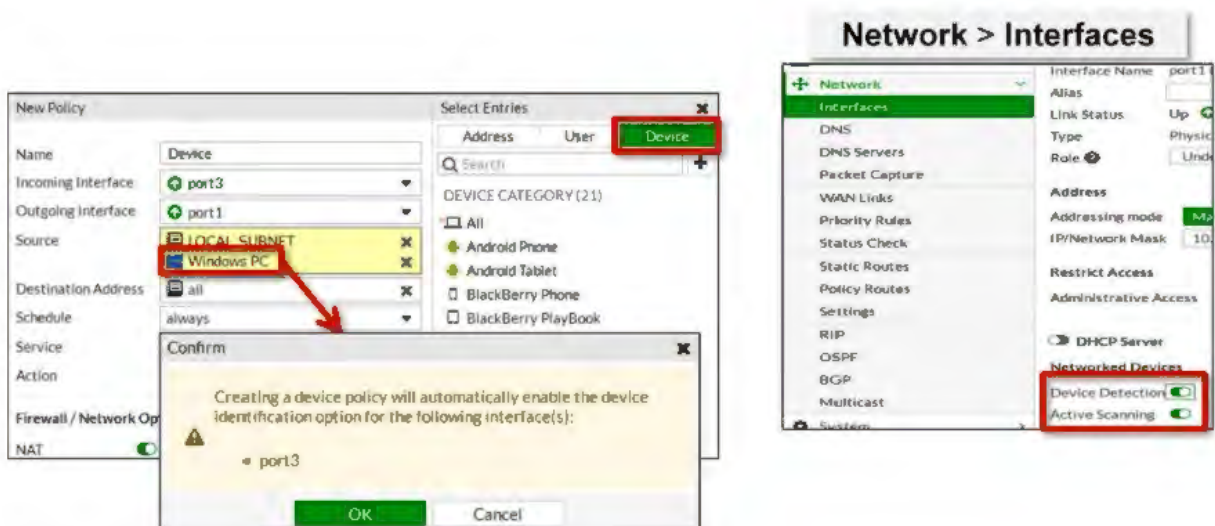
- Accès local

- Accès distant : VPN via Forticlient





Il est recommandé également d'activer l'option détection des périphériques au niveau des interfaces comme suit pour avoir le log en cas de besoin :



La liste des dispositifs détectés par le firewall est accessible via l'onglet User & Device

--> Device Inventory comme suit :

FortiGate 100E FG100E4Q17004886					
Dashboard	Refresh	Edit	Delete	Search	
Security Fabric	Status	Device	Address	Interfaces	OS
FortiView	IP Phone (2)				
Network	Online	SEPC4B9CD807AA1	172.17.10.154	Admin	Cisco / 1
System	Offline	SEPC4B9CD807B4E	172.17.10.155	Admin	Cisco / 1
Policy & Objects	iPhone (1)				
Security Profiles	Offline	iPhone-X	172.17.10.150	Admin	iPhone / IOS
VPN	Other Network Device (1)				
User & Device	Online	Switch1	172.16.200.101	LAN	Cisco SG500-28
User Definition	Router/NAT Device (13)				
User Groups	Windows PC (33)				
Guest Management	Online	ADMIN-PC	172.17.30.22	Agents	Windows 7 / 2008 R2
Device Inventory	Online	CALLMAX-PC	172.17.30.9	Agents	Windows / 7
Custom Devices & Groups	Online	CALLMAX-PC	172.17.10.67	Admin	Windows 7 / 2008 R2
Single Sign-On	Online	CALLMAX-PC	172.17.10.88	Admin	Windows 7 / 2008 R2
LDAP Servers	Online	DESKTOP-L60N5KU	172.17.10.72	Admin	Windows / NT 10.0
RADIUS Servers	Online	HP-PC	172.17.10.166	Admin	Windows 7 / 2008 R2
	Online	HP-PC	172.17.30.29	Agents	Windows / 7
	Online	pc-PC	172.17.30.15	Agents	Windows / 7
	Online	PCCALLMAX	172.17.10.53	Admin	Windows 7 / 2008 R2

## Shedeling

Cette option permet d'exécuter la policy selon les jours et le temps programmé.

FortiGate 100E FG100E4Q17004886		
Dashboard	Edit Policy	
Security Fabric	Incoming Interface	Admin
FortiView	Outgoing Interface	Servers
Network	Source	all
System	Destination	all
Policy & Objects	Schedule	always
IPv4 Policy	Service	Search
Addresses	Action	RECURRING SCHEDULE (3)
Internet Service Database	Firewall / Network O	always
Services	NAT	none
Schedules		PAUSE DEJEUNER
Virtual IPs		ONETIME SCHEDULE (1)
IP Pools		FACEBOOK
Traffic Shapers		

Pour créer un shedling il faut procéder comme suit :



**FortiGate 100E** FG100E4Q17004886

**Dashboard** > **Edit Schedule**

**Security Fabric** >

**FortiView** >

**Network** >

**System** >

**Policy & Objects** >

IPv4 Policy

Addresses

Internet Service Database

Services

**Schedules** ☆

Type: **Recurring** One-time

Name: PAUSE DEJEUNER

Color: [Change]

Days: ☐ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday

All Day: ☐

Start Time: Hour 13 Minute 0

Stop Time: Hour 14 Minute 0

**OK** Cancel

Un shedule peut être :

- Récursive ; come l'exemple ci-dessous ou
- pour une seule utilisation occasionnelle comme ci-dessous :

Type: Recurring **One-time**

Name: FACEBOOK

Color: [Change]

Start Date: 2018/03/08

Start Time: Hour 19 Minute 0

End Date: 2018/03/14

Stop Time: Hour 0 Minute 0

Pre-expiration event log: ☒ Number of days before: 3

## Profils de sécurité:

L'une des importantes fonctionnalités de FortiGate est le profil de sécurité qui regroupe plusieurs points et qui peuvent être personnalisés selon le besoin.

### Security Profiles

AntiVirus	<input checked="" type="checkbox"/>	AV	default	
Web Filter	<input checked="" type="checkbox"/>	WEB	default	
DNS Filter	<input checked="" type="checkbox"/>	DNS	default	
Application Control	<input checked="" type="checkbox"/>	APP	default	
IPS	<input checked="" type="checkbox"/>	IPS	default	
SSL/SSH Inspection	<input type="checkbox"/>	SSL	certificate-inspection	

### Actions de filtrage:

3 actions de filtrage sont possibles :

- **Accept** : Laisser passer le trafic  
Il est conseillé d'activer l'option de log correspondante

#### Logging Options

Log Allowed Traffic ☒ Security Events All Sessions

- **Deny** : Bloquer le trafic .  
Il est conseillé d'activer le log de tentatives d'accès.

☒ Log Violation Traffic

- **Learning** : Cette option permet d'autoriser tout le trafic et applique tout les profils de sécurité statique en activons le log pour chaque comportement.

FortiGate 100E FG100E4Q17004886

Dashboard > Edit Policy

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

IPv4 Policy ☆

Addresses

Internet Service Database

Services

Outgoing Interface Servers

Source all

Destination all

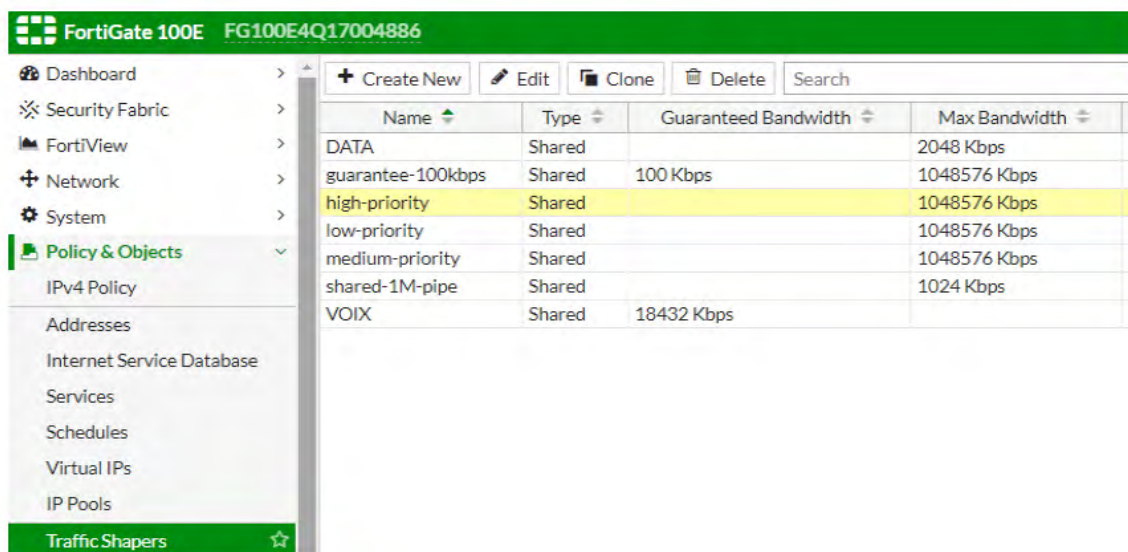
Schedule always

Service ALL

Action ☒ ACCEPT ☐ DENY ☐ LEARN

### Traffic Shapers

Cette option permet de réserver ou de garantir des bandes passantes bien déterminées à des interfaces.



Name	Type	Guaranteed Bandwidth	Max Bandwidth
DATA	Shared		2048 Kbps
guarantee-100kbps	Shared	100 Kbps	1048576 Kbps
high-priority	Shared		1048576 Kbps
low-priority	Shared		1048576 Kbps
medium-priority	Shared		1048576 Kbps
shared-1M-pipe	Shared		1024 Kbps
VOIX	Shared	18432 Kbps	