

Manuel d'utilisation d'un pare-feu



Table des matières

1	Mise à zéro de l'appareil	3
1.1	Physique	3
1.2	Via CLI	3
2	Première connexion	3
3	Appropriation	5
3.1	Définition	5
3.2	Mise à jour du Firmware	5
3.3	Changement du nom d'hôte & du fuseau horaire de l'appareil	5
3.4	Création d'un administrateur	5
3.5	Commentaire.....	6
4	Networking.....	7
4.1	Libérations des ports	7
4.2	Création de VLANs.....	7
4.3	Création de sous-réseaux.....	8
5	Accès à internet.....	10
6	Règles de pare-feu.....	10
6.1	Création des adresses.....	10
6.2	Création des règles.....	11
7	Table des illustrations.....	15

1 Mise à zéro de l'appareil

Il existe deux manières d'effectuer un reset sur votre FortiGate 80F :

1.1 Physique

Débrancher votre FortiGate 80F du secteur.

Insérer de quoi atteindre le bouton reset qui se trouve dans l'orifice nommé BLE / RESET, situé en bas à gauche du Back panel.

Rebrancher le FortiGate 80F sur le secteur, tout en appuyant sur le bouton reset.

Maintenir appuyé jusqu'à ce que la LED STATUS, située sur le front panel, se mette à clignoter à une fréquence accélérée puis relâcher le bouton reset



Figure 1 Bouton reset.

1.2 Via CLI

Ouvrir la ligne de commande

Taper la commande suivante : `# exec factoryreset`

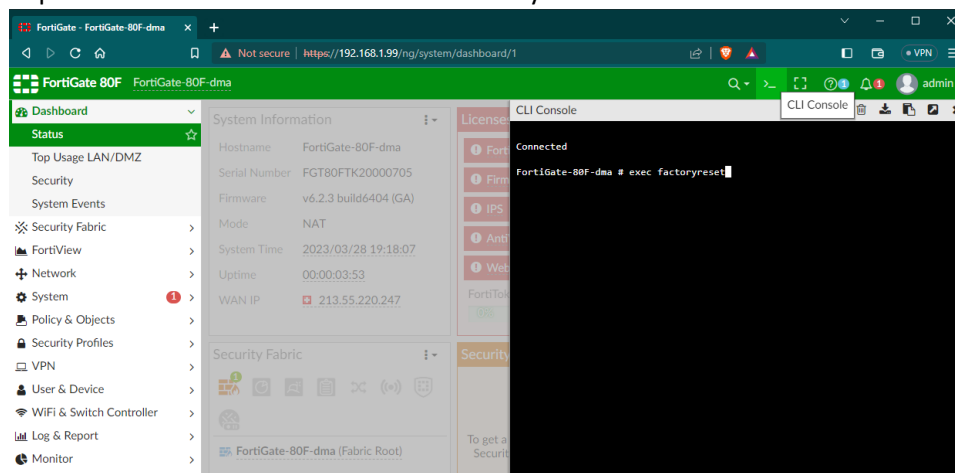


Figure 2 Ouvrir la console CLI et effectuer le reset.

2 Première connexion

1. Connecter le FG 80F, en cas de besoin : se référer au manuel d'installation.
2. Se connecter au GUI via l'adresse IP 192.168.1.99

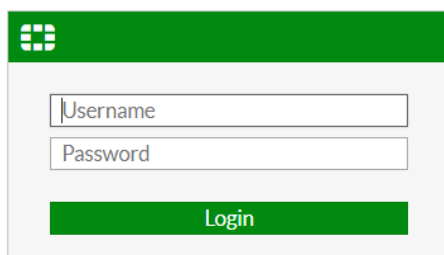
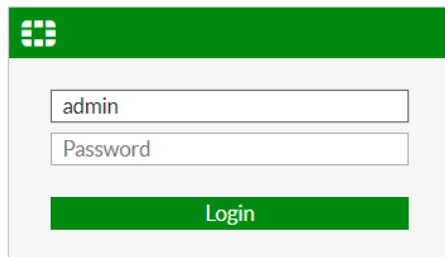


Figure 3 Login vide.

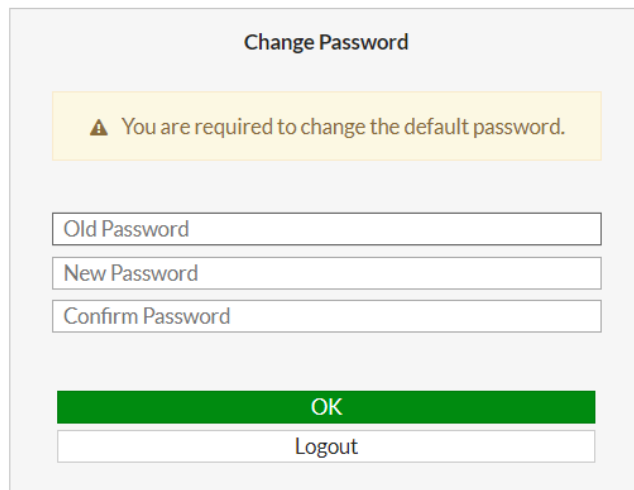
3. Rentrer le login : admin et laisser le mot de passe vide



FortiGate login form. It features a green header with the FortiGate logo. Below the header, there are two input fields: the first is labeled 'admin' and the second is labeled 'Password'. At the bottom, there is a green 'Login' button.

Figure 4 Login pour première connexion.

4. Changer le mot de passe



Change Password form. It has a title 'Change Password' and a yellow warning box that says 'You are required to change the default password.' Below the warning box are three input fields: 'Old Password', 'New Password', and 'Confirm Password'. At the bottom, there are two buttons: a green 'OK' button and a white 'Logout' button.

Figure 5 Changement de mot de passe lors de la première connexion.

5. Vous voilà dans le dashboard

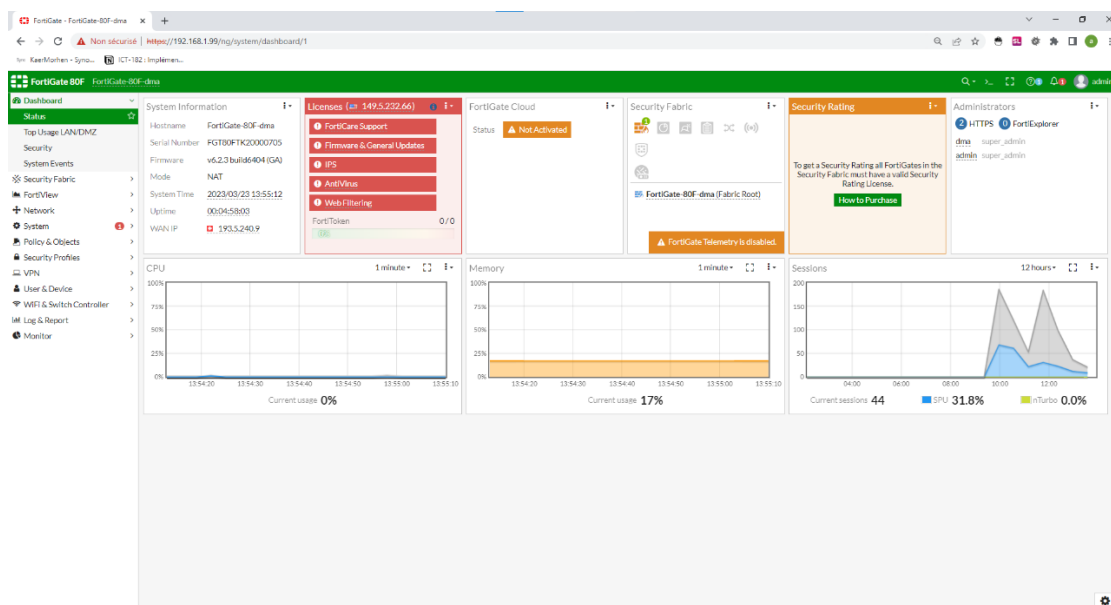


Figure 6 Dashboard.

3 Appropriation

3.1 Définition

J'attends par appropriation certaines actions qui font passer un dispositif de son état "mis à zéro" à "en cours d'utilisation".

3.2 Mise à jour du Firmware

System -> Firmware | impossible vu le non-enregistrement de l'appareil

Page | 5

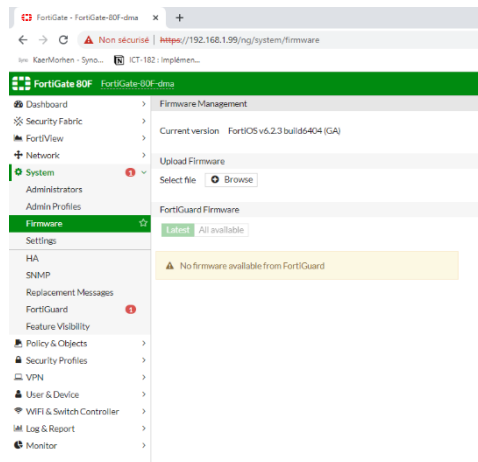


Figure 7 Mise à jour du firmware.

3.3 Changement du nom d'hôte & du fuseau horaire de l'appareil

changer d'host name : System -> Settings -> Host name -> FortiGate-80F-DMA

changer l'heure: System -> Settings -> System time -> GMT+1:00

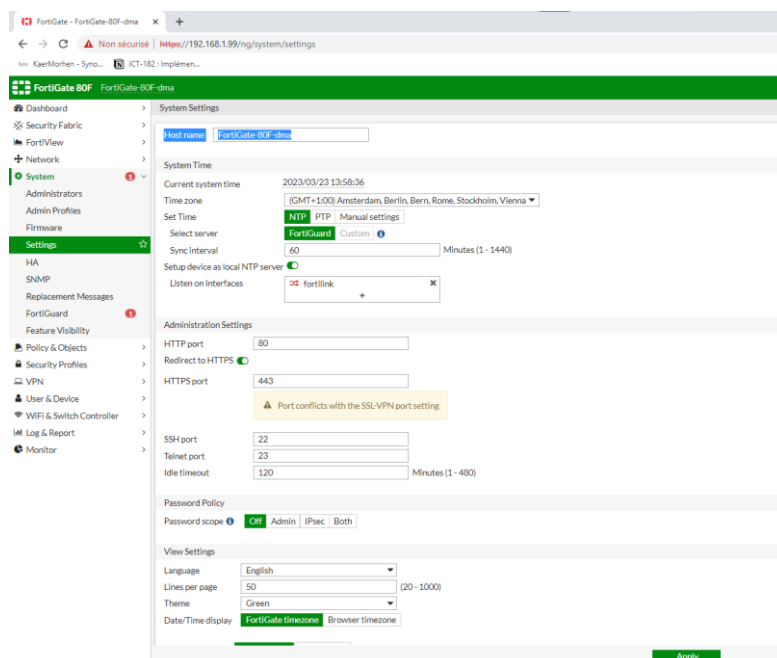


Figure 8 Changement host name & fuseau horaire.

3.4 Création d'un administrateur

créer un administrateur: System -> Administrators -> Create New -> Administrator:

Username: dma
Type: Local User
Password: Pa\$\$word
Confirm Password: Pa\$\$word
Comments: compte admin damien mayor
Administrator Profile: super_admin
Email Address: damien.mayor@cpnv.ch
SMS: off
Two-factor Authentication: off
Restrict login to trusted hosts: off
Restrict admin to guest account provisioning only: off

Cliquer sur ok

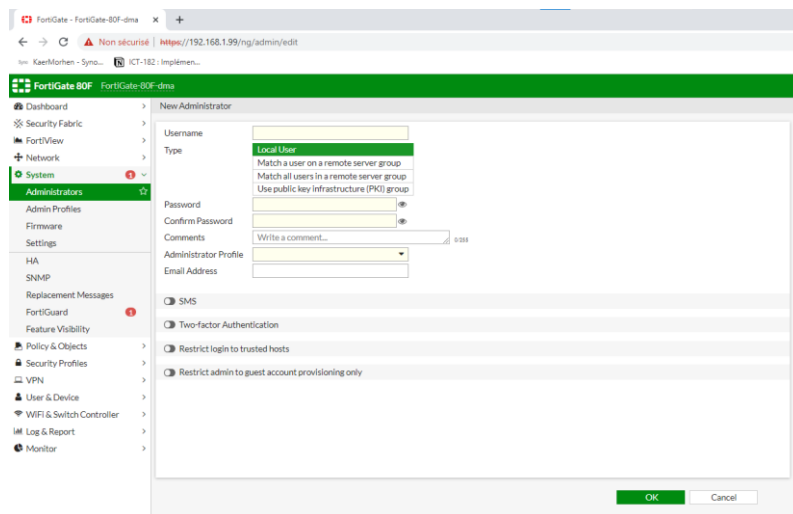


Figure 9 Création nouvel administrateur.

3.5 Commentaire

Dans sa configuration initiale, le niveau d'exigence des mots de passe est très bas, FortiOS offre la possibilité d'augmenter ce niveau d'exigence. Ceci est recommandé pour une utilisation professionnelle du pare-feu.

4 Networking

Dans cette partie nous allons créer des VLANs et/ou des sous-réseaux

4.1 Libérations des ports

1. Se rendre dans Network -> Interface -> Hardware Switch -> internal -> double-click.
2. Interface members : sortir les ports à qui l'on souhaite utiliser pour des vlans/sous-réseaux : dans mon cas internal1 à internal4, laissant internal5 & internal6
Attention, ceci va rendre vos ports physique 1 à 4 momentanément inutilisable, il vous sera même impossible de se connecter au GUI sur ces ports
3. Connectez votre câble rj45 de votre ordinateur aux ports restant 5 ou 6 du pare-feu.

Page | 7

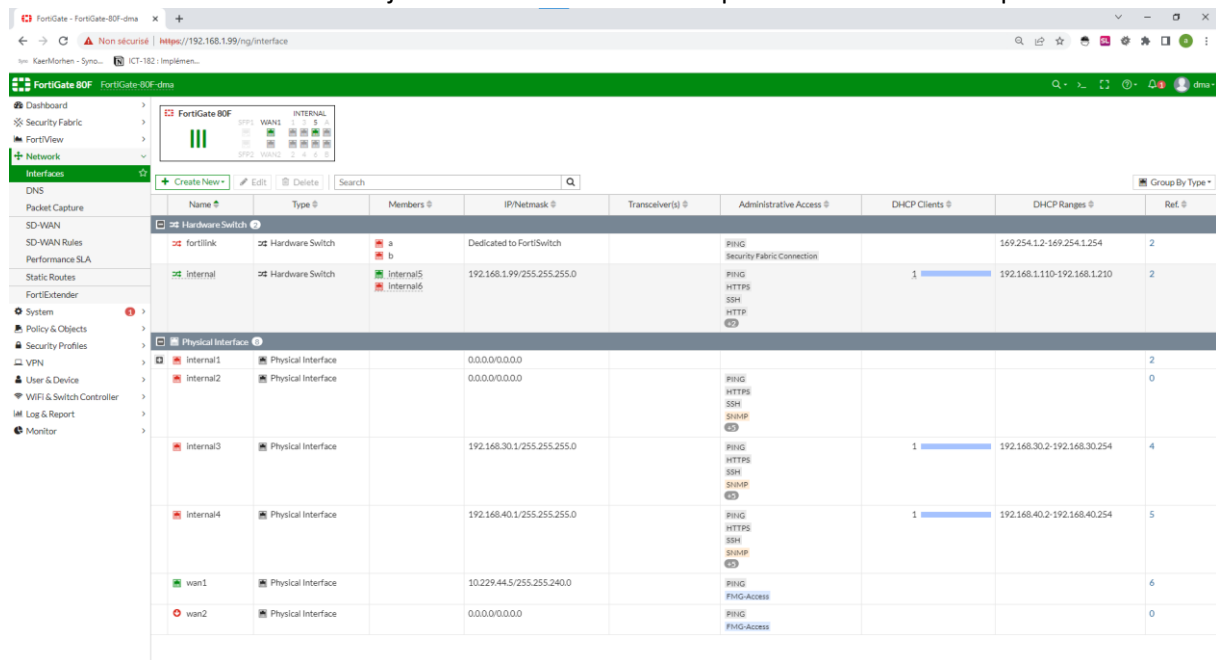


Figure 10 Libération des ports.

4.2 Création de VLANs

1. Se connecter à l'interface physique internal1: Network -> Interfaces -> Physical Interface -> internal1 -> double-click
2. **Name :** internal1
Alias : -
Type : Physical Interface1
VLAN ID : 10
Role : LAN
Addressing mode : Manual
IP/Netmask : IP et masque selon vos besoins. 192.168.10.1/255.255.255.0 (vous pouvez également écrire /24)
Create address object matching subnet: on
Secondary IP address: off
Administrative access: off
DHCP Server: off
Device detection: on
Security mode: off
Outbound shaping profile: off
Comments : création vlan ROUGE dma

Status : Enabled

3. Cliquer sur OK
4. Network -> Interfaces - Physical Interface -> internal1 -> ouvrir : vous devriez voir votre VLAN ROUGE
5. Répéter la procédure pour la création du vlan BLEU, en adaptant l'alias, le vlan id ainsi que la plage d'adresse IP et son masque.

Page | 8

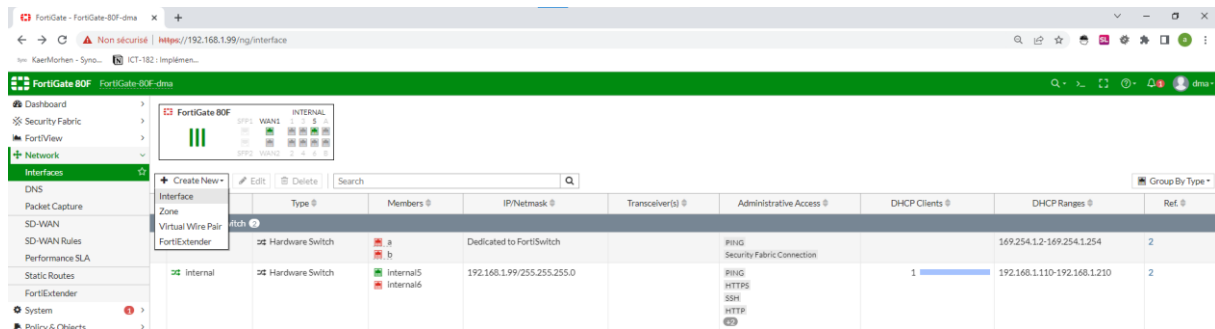


Figure 11 Créer une interface VLAN.

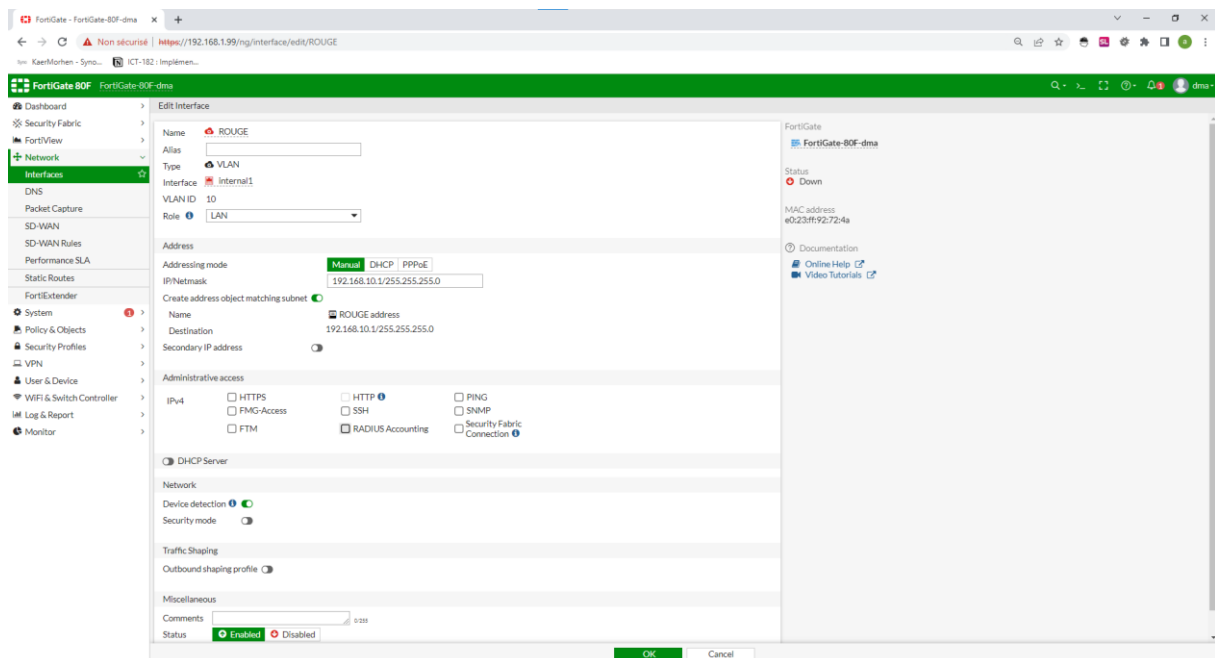


Figure 12 Nouveau VLAN ROUGE.

Il n'est pas possible d'attribuer un port physique à un VLAN, il faudrait pour ceci utiliser un switch manageable. Si vous n'en n'avez pas à disposition, vous pouvez arriver à un résultat similaire en créant des sous-réseaux comme expliqué au point 4.3

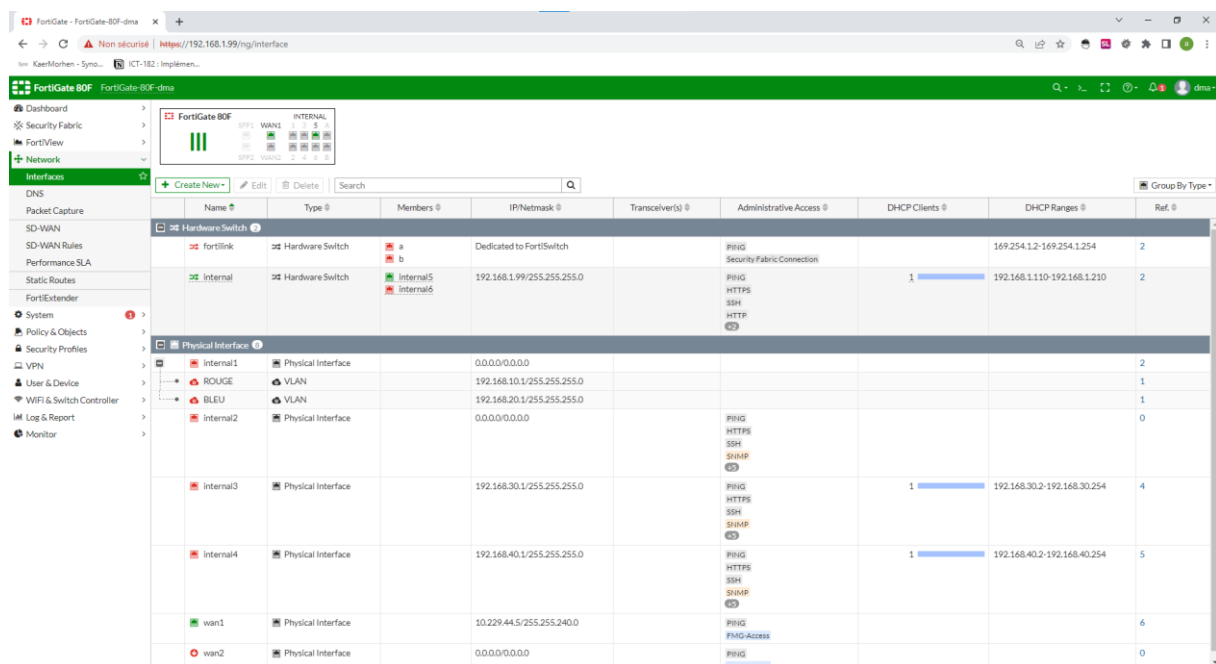
4.3 Création de sous-réseaux

1. Se rendre dans Network -> Interface -> Physical Interface -> internal3 -> double-click
2. Name: internal3
Alias:
Type: Physical Interface
Role: Undefined
Addressing mode: Manual

IP/Netmask: 192.168.30.1/255.255.255.0
 Secondary IP address: off
 IPv4: HTTPS, HTTP, PING, SSH
 Receive LLDP: Use VDOM Setting
 Transmit LLDP: Use VDOM Setting
 DHCP Server: on
 Address range: 192.168.30.2-192.168.30.254
 Netmask: 255.255.255.0
 Default gateway: Same as Interface IP
 DNS server: Same as System DNS
 Lease time:604800
 FortiClient On-Net Status: on
 Device detection: off
 Security mode: off
 Outbound shaping profile: off
 Comments: création sous-réseau sur port3 dma
 Status: Enabled

3. Cliquer sur OK

Nous venons de donner à l'interface internal3 une adresse IP et un masque de sous-réseau 192.168.30.1/24, ainsi qu'en activant la fonction DHCP, nous lui donnons la faculté de distribuer des adresses IP aux machines connectées, sur la plage 192.168.30.2-192.168.30.254.

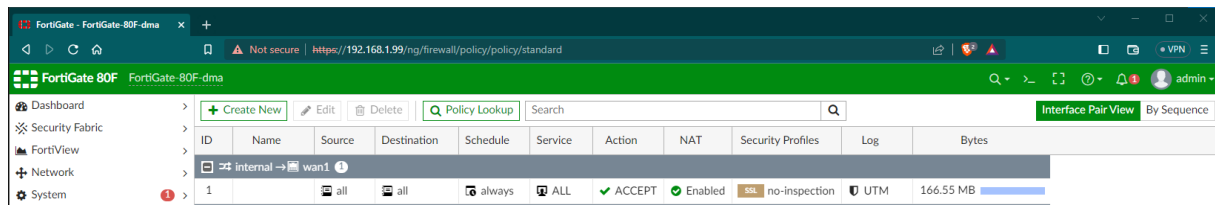


Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
fortilink	Hardware Switch	a, b	Dedicated to FortiSwitch		PING, Security Fabric Connection		169.254.1.2-169.254.1.254	2
Internal	Hardware Switch	Internal5, Internal6	192.168.1.99/255.255.255.0		PING, HTTPS, SSH, HTTP	1	192.168.1.110-192.168.1.210	2
Internal1	Physical Interface		0.0.0.0/0.0.0.0					2
ROUGE	VLAN		192.168.10.1/255.255.255.0					1
BLEU	VLAN		192.168.20.1/255.255.255.0					1
Internal2	Physical Interface		0.0.0.0/0.0.0.0		PING, HTTPS, SSH, SNMP			0
Internal3	Physical Interface		192.168.30.1/255.255.255.0		PING, HTTPS, SSH, SNMP	1	192.168.30.2-192.168.30.254	4
Internal4	Physical Interface		192.168.40.1/255.255.255.0		PING, HTTPS, SSH, SNMP	1	192.168.40.2-192.168.40.254	5
wan1	Physical Interface		10.229.44.5/255.255.240.0		PING, Ping Access			6
wan2	Physical Interface		0.0.0.0/0.0.0.0		PING, Ping Access			0

Figure 13 Création sous-réseau internal3.

5 Accès à internet

La configuration de base du pare-feu inclut une règle qui permet d'accéder à internet, rien à faire de ce côté-là.



Page | 10

Figure 14 Les ports sur l'interface internal ont accès au WAN étant donné la configuration de base.

6 Règles de pare-feu

6.1 Création des adresses

1. Policy & Objects -> Addresses -> Create New -> Address
2. *Name: Sous-Réseau3*
Color: orange
Type: Subnet
IP/Netmask: 192.168.30.0/24
Interface: internal3
Show in address list: on
Static route configuration: off
Comments: création adresse Sous-Réseau3 dma
3. Cliquer sur OK
4. Si vous vous débranchez du port physique sur lequel vous êtes actuellement et vous vous branchez sur le port 3, vous arriverez au GUI, et un cmd ipconfig vous donnera une adresse appartenant au sous-réseau 3
5. Suivre la même procédure pour les autres sous-réseaux.

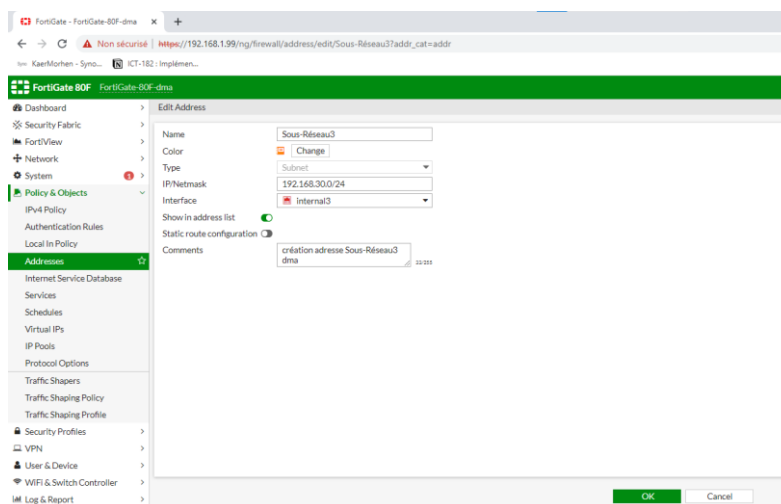


Figure 15 création de l'adresse du sous-réseau 3.

Il va falloir créer des adresses non seulement pour les réseaux mais également pour les sites internet que l'on souhaite visiter.

1. Se rendre sur Policy & Objects -> Address -> Create New -> Address
2. *Name: perdu.com*

Color: vert

Type: FQDN

FQDN: www.perdu.com

Interface: any

Show in address list: on

Static route configuration: off

Comments: création adresse perdu.com dma

3. Cliquer sur OK

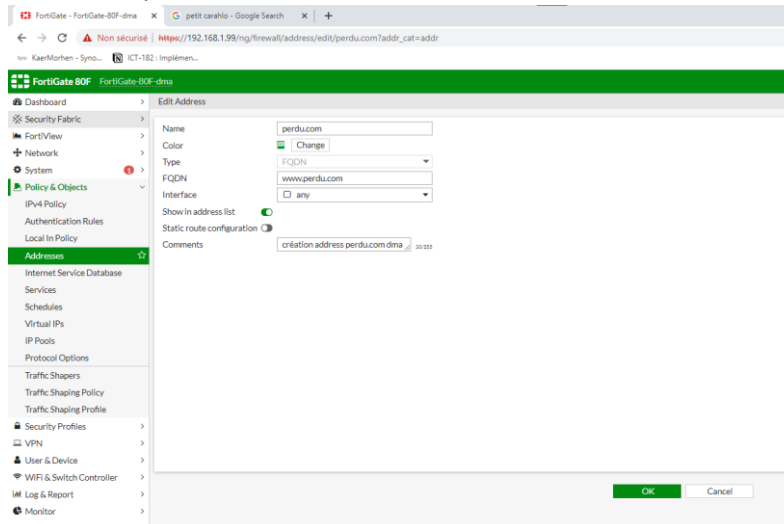
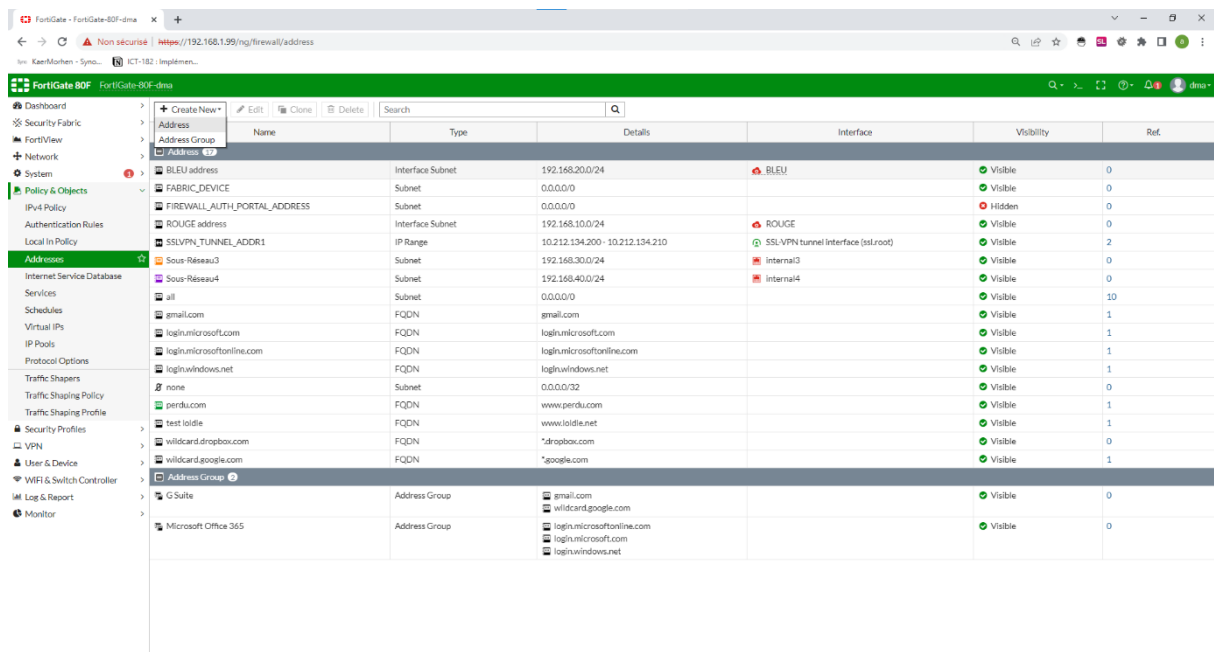


Figure 16 Création adresse perdu.com.

Récapitulatif des adresses créées.



Name	Type	Details	Interface	Visibility	Ref.
BLEU address	Interface Subnet	192.168.20.0/24	BLEU	Visible	0
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
ROUGE address	Interface Subnet	192.168.10.0/24	ROUGE	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSLVPN tunnel interface (sslroot)	Visible	2
Sous-Réseau3	Subnet	192.168.30.0/24	Internal3	Visible	0
Sous-Réseau4	Subnet	192.168.40.0/24	Internal4	Visible	0
all	Subnet	0.0.0.0/0		Visible	10
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
perdu.com	FQDN	www.perdu.com		Visible	1
test.tldie	FQDN	www.tldie.net		Visible	1
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1
Address Group	Address Group	gmail.com, wildcard.google.com		Visible	0
G Suite	Address Group	login.microsoftonline.com, login.microsoft.com, login.windows.net		Visible	0
Microsoft Office 365	Address Group			Visible	0

Figure 17 Récapitulatif des adresses créées.

6.2 Création des règles

Pour le moment si vous êtes connecté sur port3 ou 4 vous n'avez pas accès à internet. Afin de pouvoir y accéder, il va falloir créer des règles :

4. Création de la règle de firewall Policy & Objects -> IPv4 Policy -> Create New
5. *Name: perdu?*
Incoming Interface: internal3
Outgoing Interface: wan1
Source: all
Destination: perdu.com
Schedule: always
Service: HTTP, HTTPS
Action: ACCEPT
Inspection Mode: Flow-based
NAT: on
IP Pool Configuration: Use Outgoing Interface Address
Preserve Source Port: off
Protocol Options: default
AntiVirus: off
Web Filter: off
DNS Filter: off
Application control: off
IPS: off
SSL Inspection: no-inspection
Log Allowed Traffic: Security Events
Comments: création règle perdu.com dma
Enable this policy: on
6. Cliquer sur OK

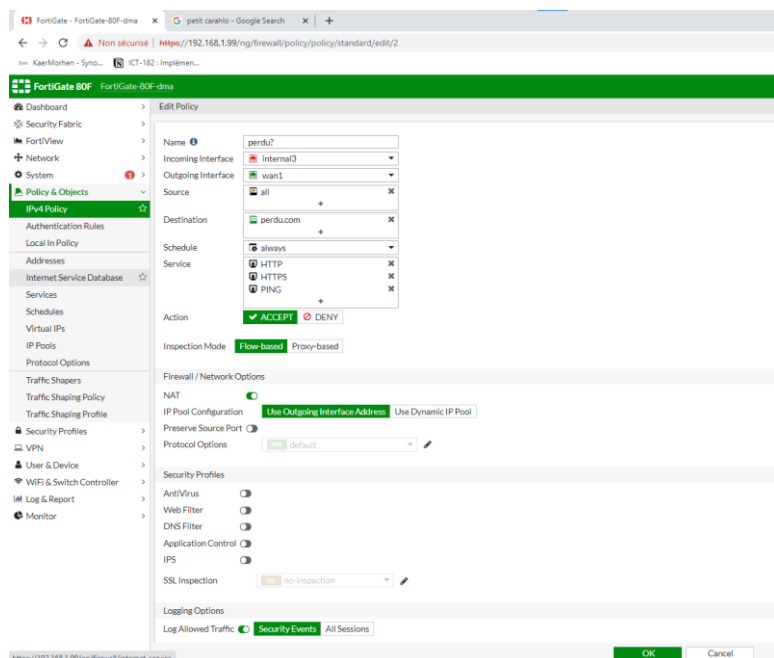


Figure 18 Règle accès à perdu.com sur interface internal3.

7. Création de la règle de firewall Policy & Objects -> IPv4 Policy -> Create New
8. *Name: dns*
Incoming Interface: internal3
Outgoing Interface: wan1

Source: all
Destination: all
Schedule: always
Service: DNS
Action: ACCEPT
Inspection Mode: Flow-based
NAT: on
IP Pool Configuration: Use Outgoing Interface Address
Preserve Source Port: off
Protocol Options: default
AntiVirus: off
Web Filter: off
DNS Filter: off
Application control: off
IPS: off
SSL Inspection: no-inspection
Log Allowed Traffic: Security Events
Comments: création règle dns dma
Enable this policy: on

9. Cliquer sur OK

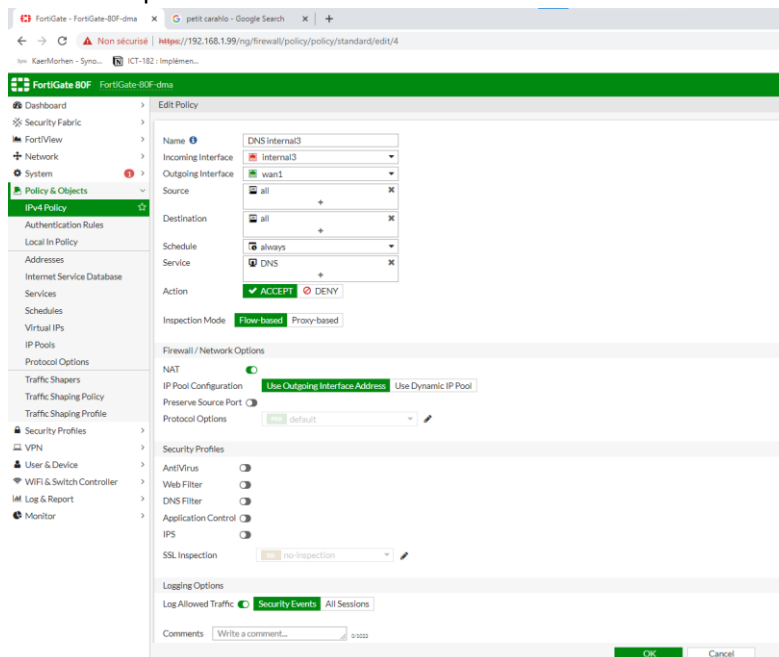
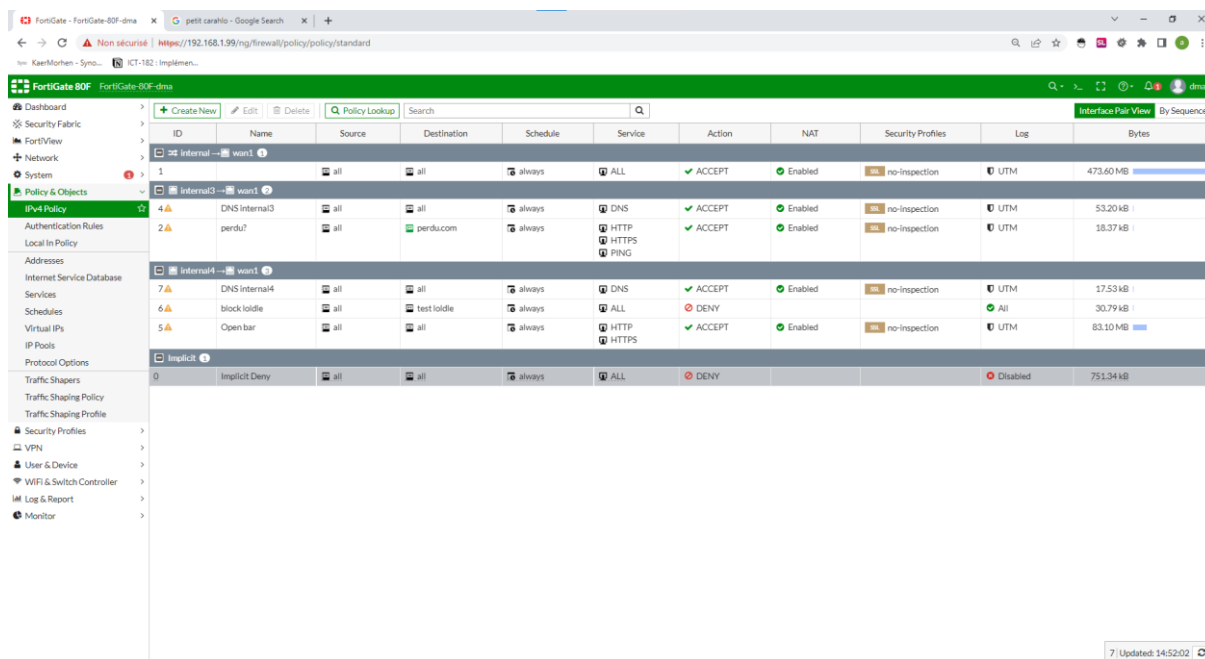


Figure 19 Règle accès DNS sur interface internal3.

Récapitulatif des règles:



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Internal3 wan1	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	473.60 MB
2	Internal3 wan1	all	perdu.com	always	HTTP, HTTPS, PING	ACCEPT	Enabled	no-inspection	UTM	18.37 kB
4	DNS internal3	all	all	always	DNS	ACCEPT	Enabled	no-inspection	UTM	53.20 kB
7	DNS internal4	all	all	always	DNS	ACCEPT	Enabled	no-inspection	UTM	17.53 kB
6	block lolidie	all	test.lolidie	always	ALL	DENY			All	30.79 kB
5	Open bar	all	all	always	HTTP, HTTPS	ACCEPT	Enabled	no-inspection	UTM	83.10 MB
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	751.34 kB

Figure 20 Ensemble des règles créées pour différents tests.

7 Table des illustrations

Figure 1 Bouton reset.	3
Figure 2 Ouvrir la console CLI et effectuer le reset.	3
Figure 3 Login vide.	3
Figure 4 Login pour première connexion.	4
Figure 5 Changement de mot de passe lors de la première connexion.	4
Figure 6 Dashboard.	4
Figure 7 Mise à jour du firmware.	5
Figure 8 Changement host name & fuseau horaire.	5
Figure 9 Création nouvel administrateur.	6
Figure 10 Libération des ports.	7
Figure 11 Créer une interface VLAN.	8
Figure 12 Nouveau VLAN ROUGE.	8
Figure 13 Création sous-réseau internal3.	9
Figure 14 Les ports sur l'interface internal ont accès au WAN étant donné la configuration de base.	10
Figure 15 création de l'adresse du sous-réseau 3.	10
Figure 16 Création adresse perdu.com.	11
Figure 17 Récapitulatif des adresses créées.	11
Figure 18 Règle accès à perdu.com sur interface internal3.	12
Figure 19 Règle accès DNS sur interface internal3.	13
Figure 20 Ensemble des règles créées pour différents tests.	14