Manuel d'utilisation d’un pare-feu



Table des matières

[1 Mise à zéro de l'appareil 3](#_Toc130930618)

[1.1 Physique 3](#_Toc130930619)

[1.2 Via CLI 3](#_Toc130930620)

[2 Première connexion 3](#_Toc130930621)

[3 Appropriation 5](#_Toc130930622)

[3.1 Définition 5](#_Toc130930623)

[3.2 Mise à jour du Firmware 5](#_Toc130930624)

[3.3 Changement du nom d'hôte & du fuseau horaire de l'appareil 5](#_Toc130930625)

[3.4 Création d'un administrateur 5](#_Toc130930626)

[3.5 Commentaire 6](#_Toc130930627)

[4 Networking 7](#_Toc130930628)

[4.1 Libérations des ports 7](#_Toc130930629)

[4.2 Création de VLANs 7](#_Toc130930630)

[4.3 Création de sous-réseaux 8](#_Toc130930631)

[5 Accès à internet 10](#_Toc130930632)

[6 Règles de pare-feu 10](#_Toc130930633)

[6.1 Création des adresses 10](#_Toc130930634)

[6.2 Création des règles 11](#_Toc130930635)

[7 Table des illustrations 15](#_Toc130930636)

# Mise à zéro de l'appareil

Il existe deux manière d’effectuer un reset sur votre FortiGate 80F :

## 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 a une fréquence accélérée puis relâcher le bouton reset

Une image contenant texte, intérieur

Description générée automatiquement

Figure Bouton reset.

## Via CLI

Ouvrir la ligne de commande

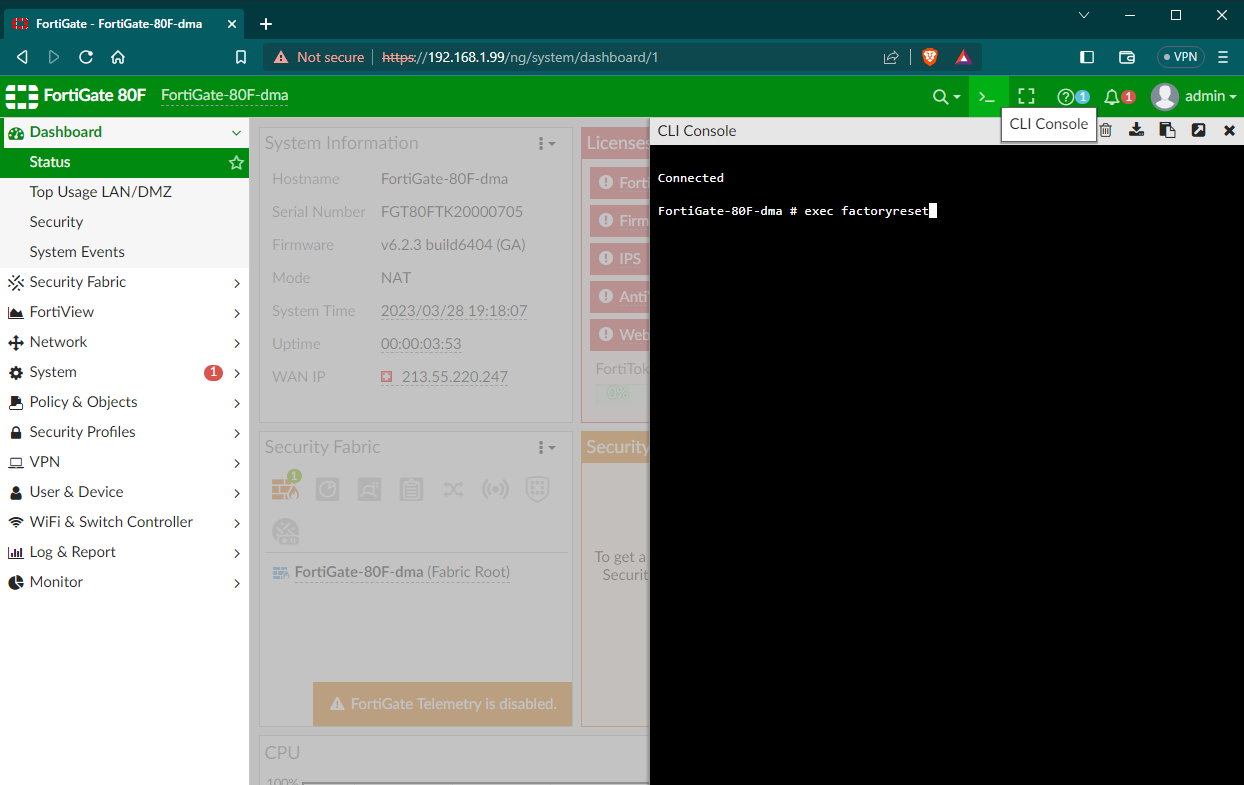
Taper la commande suivante : # exec factoryreset

Figure Ouvrir la console CLI et effectuer le reset.

# 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

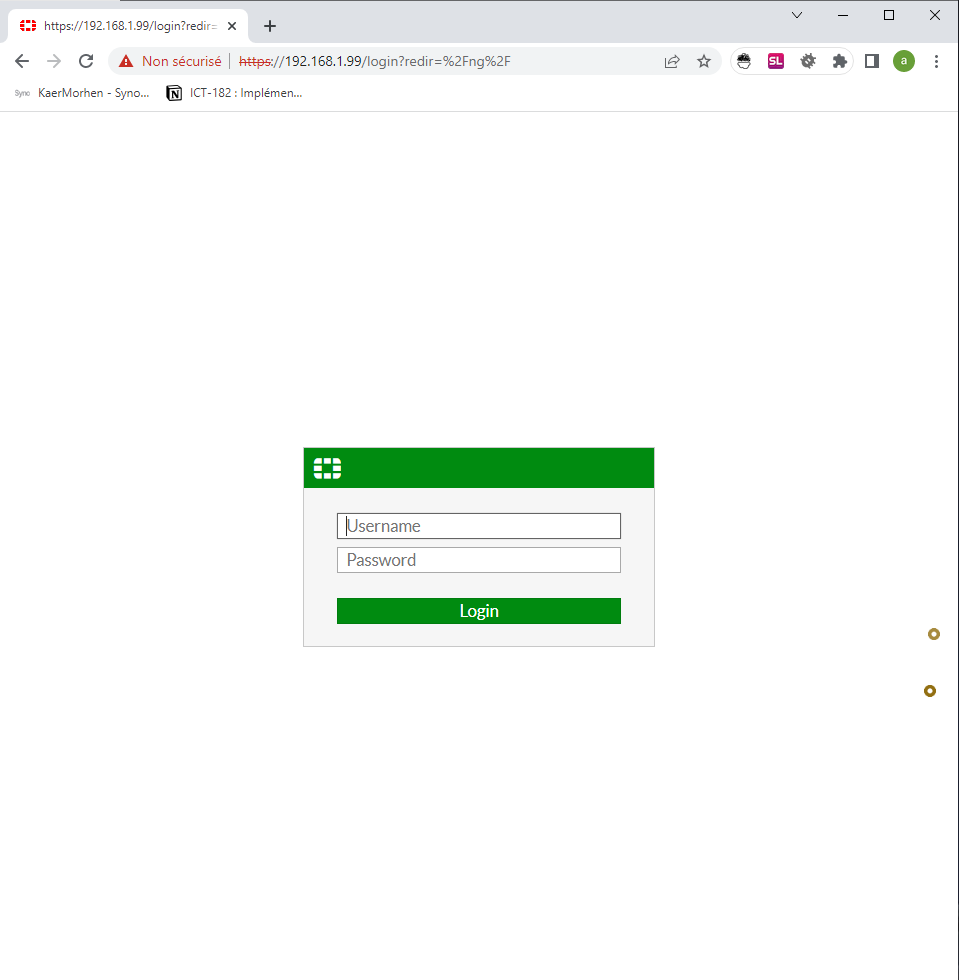


Figure Login vide.

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

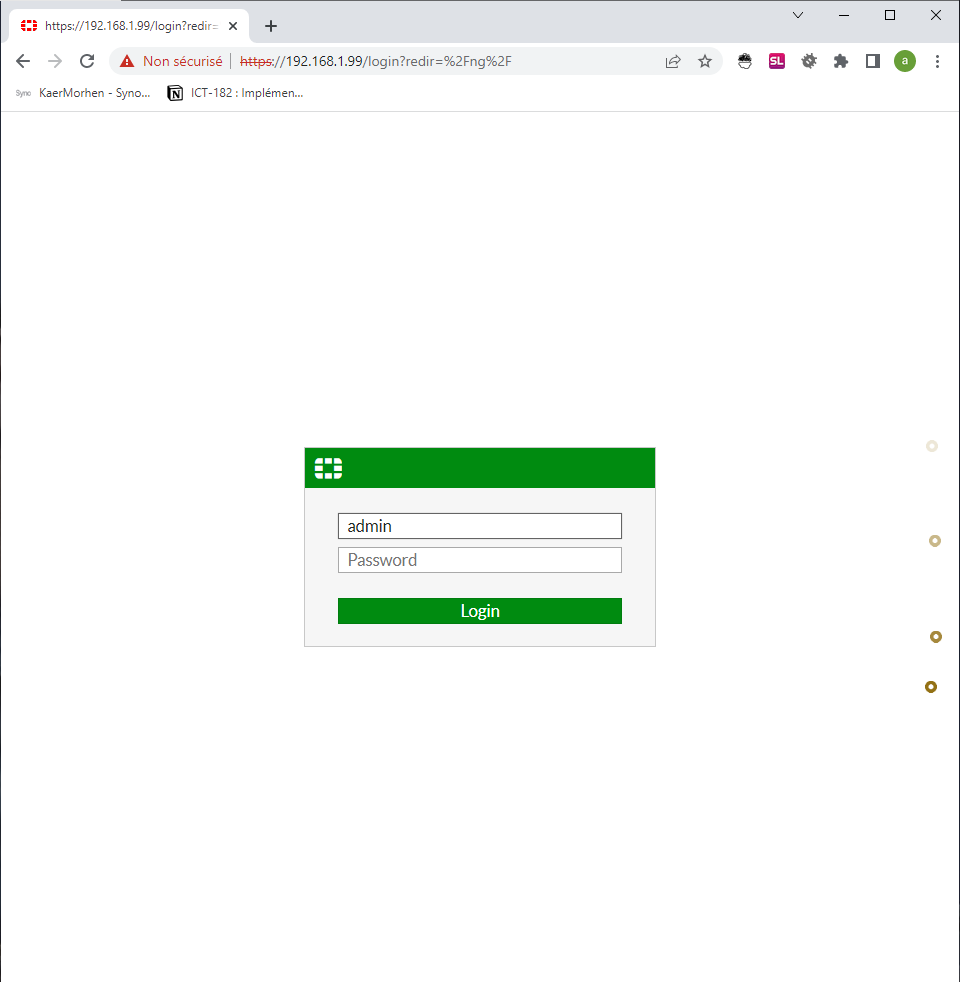


Figure Login pour première connexion.

1. Changer le mot de passe

Une image contenant table

Description générée automatiquement

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

1. Vous voilà dans le dashboard

Une image contenant table, calendrier

Description générée automatiquement

Figure Dashboard.

# Appropriation

## Définition

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

## Mise à jour du Firmware

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

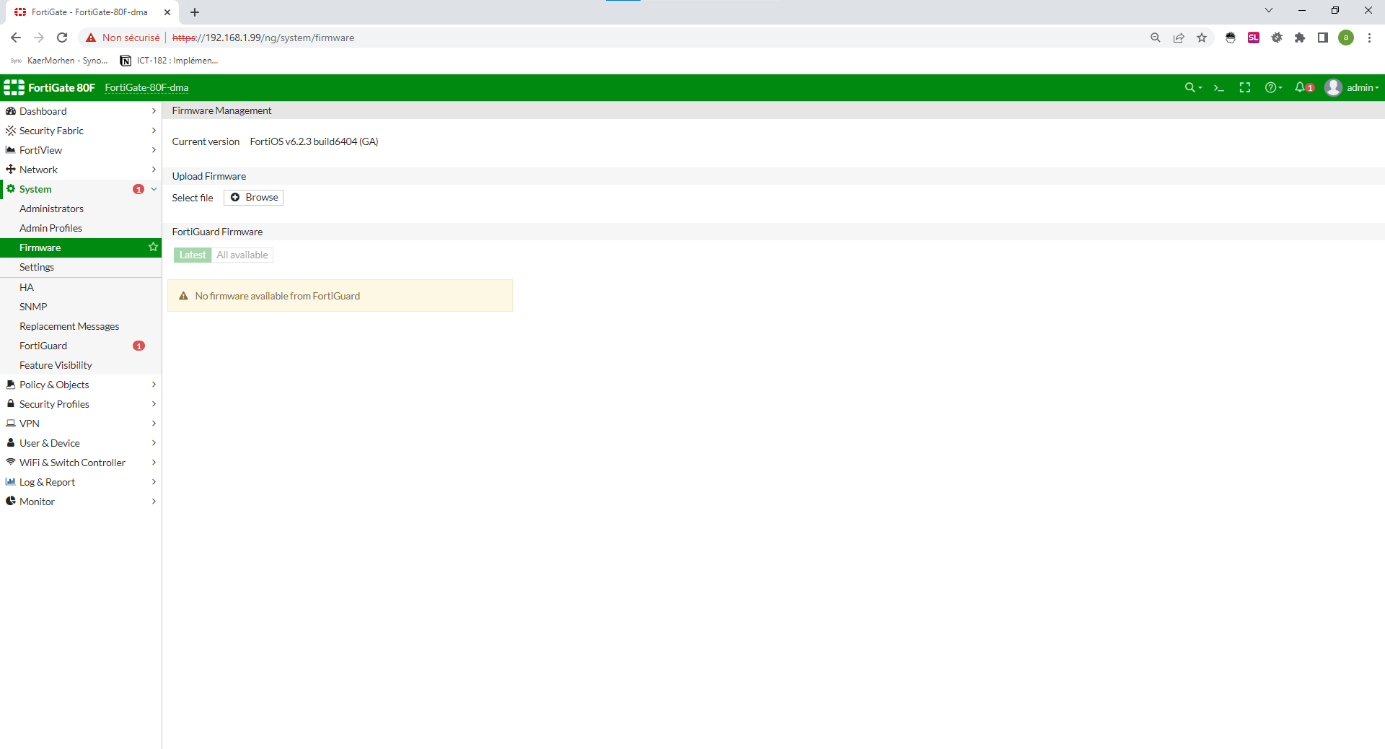


Figure Mise à jour du firmware.

## 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

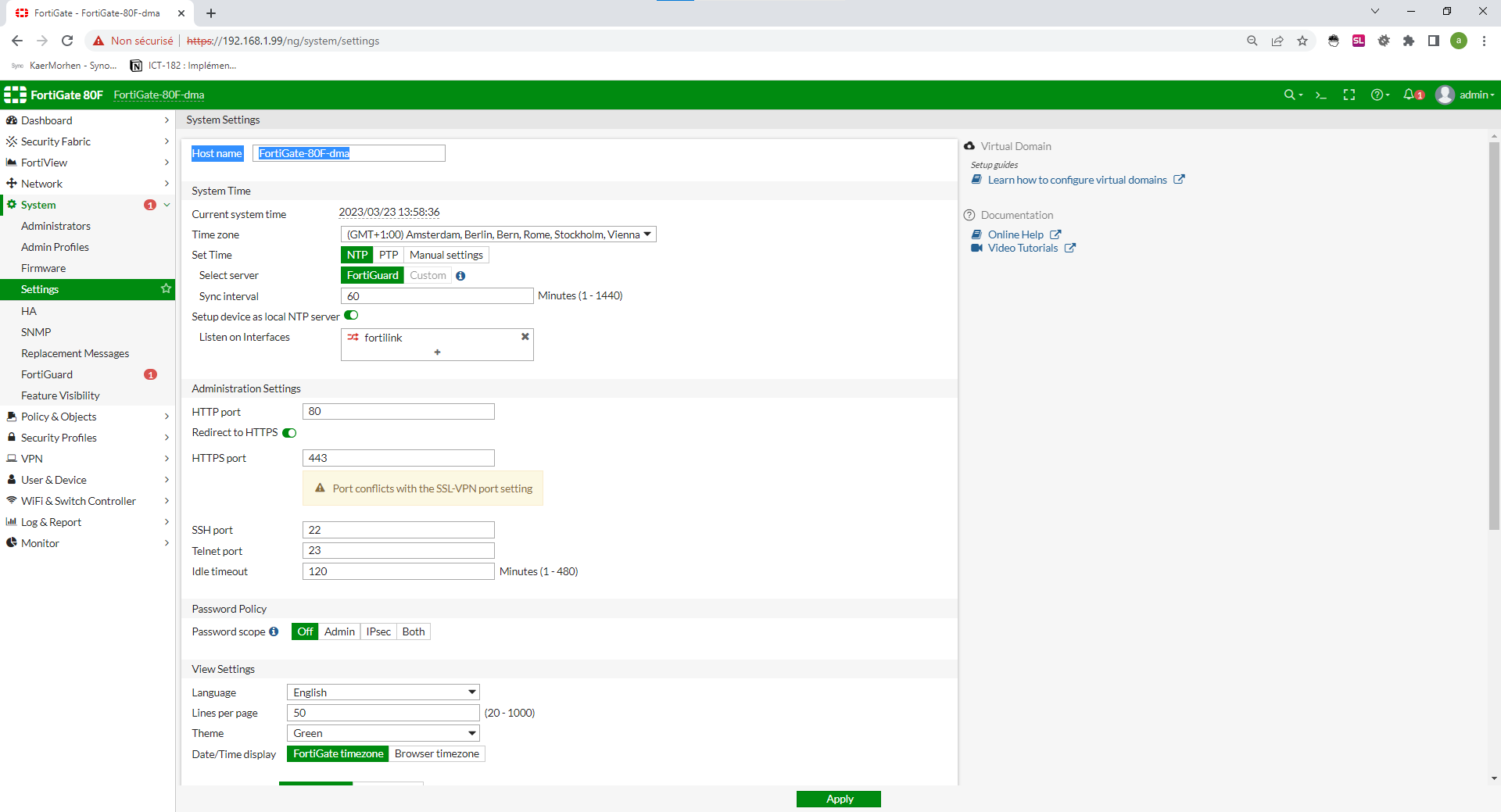


Figure Changement host name & fuseau horaire.

## 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

Une image contenant texte

Description générée automatiquement

Figure Création nouvel administrateur.

## 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.

# Networking

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

## 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

1. Connectez votre câble rj45 de votre ordinateur aux ports restant 5 ou 6 du pare-feu.

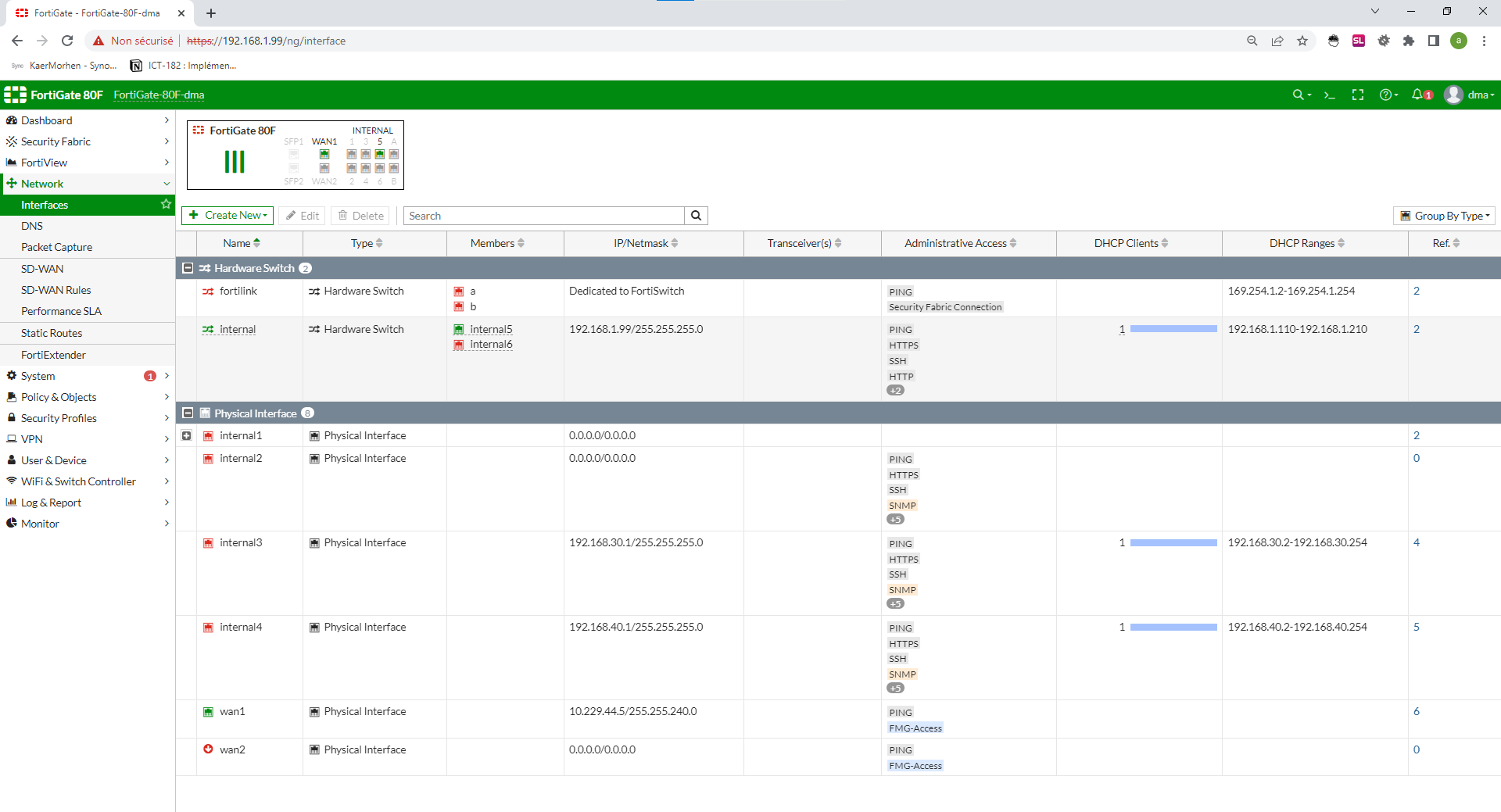


Figure Libération des ports.

## 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*

1. Cliquer sur OK
2. Network -> Interfaces - Physical Interface -> internal1 -> ouvrir : vous devriez voir votre VLAN ROUGE
3. 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.

Une image contenant texte, capture d’écran, intérieur

Description générée automatiquement

Figure Créer une interface VLAN.

Une image contenant texte

Description générée automatiquement

Figure 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

## 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*

1. 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.

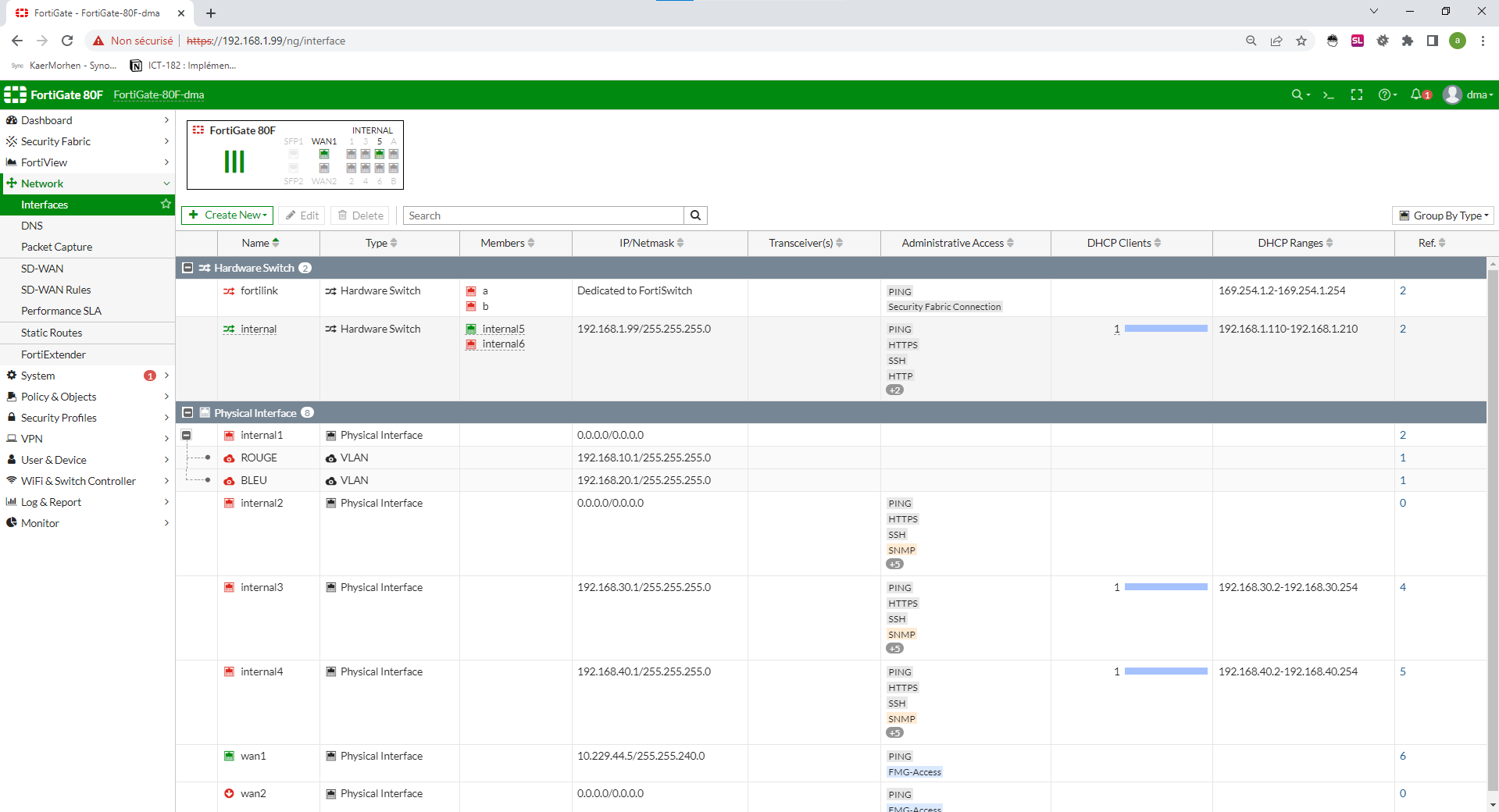


Figure Création sous-réseau internal3.

# Accès à internet

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

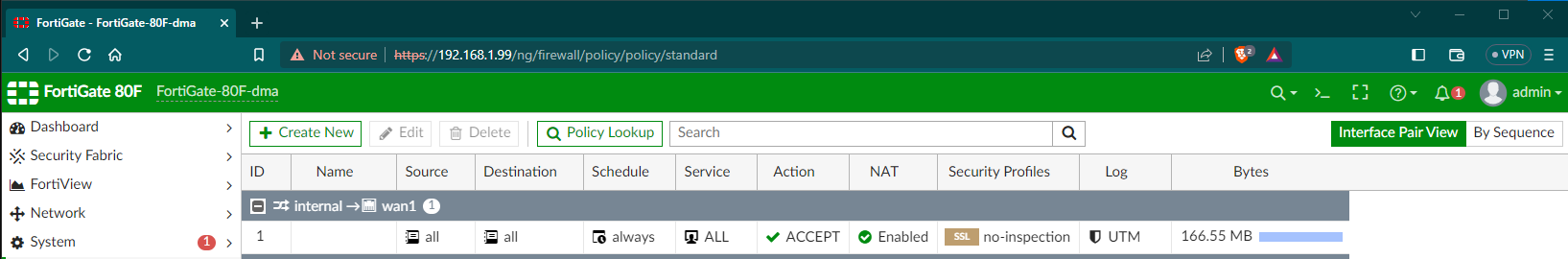


Figure Les ports sur l'interface internal ont accès au WAN étant donné la configuration de base.

# Règles de pare-feu

## 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 addresse Sous-Réseau3 dma*

1. Cliquer sur OK
2. 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
3. Suivre la même procédure pour les autres sous-réseaux.

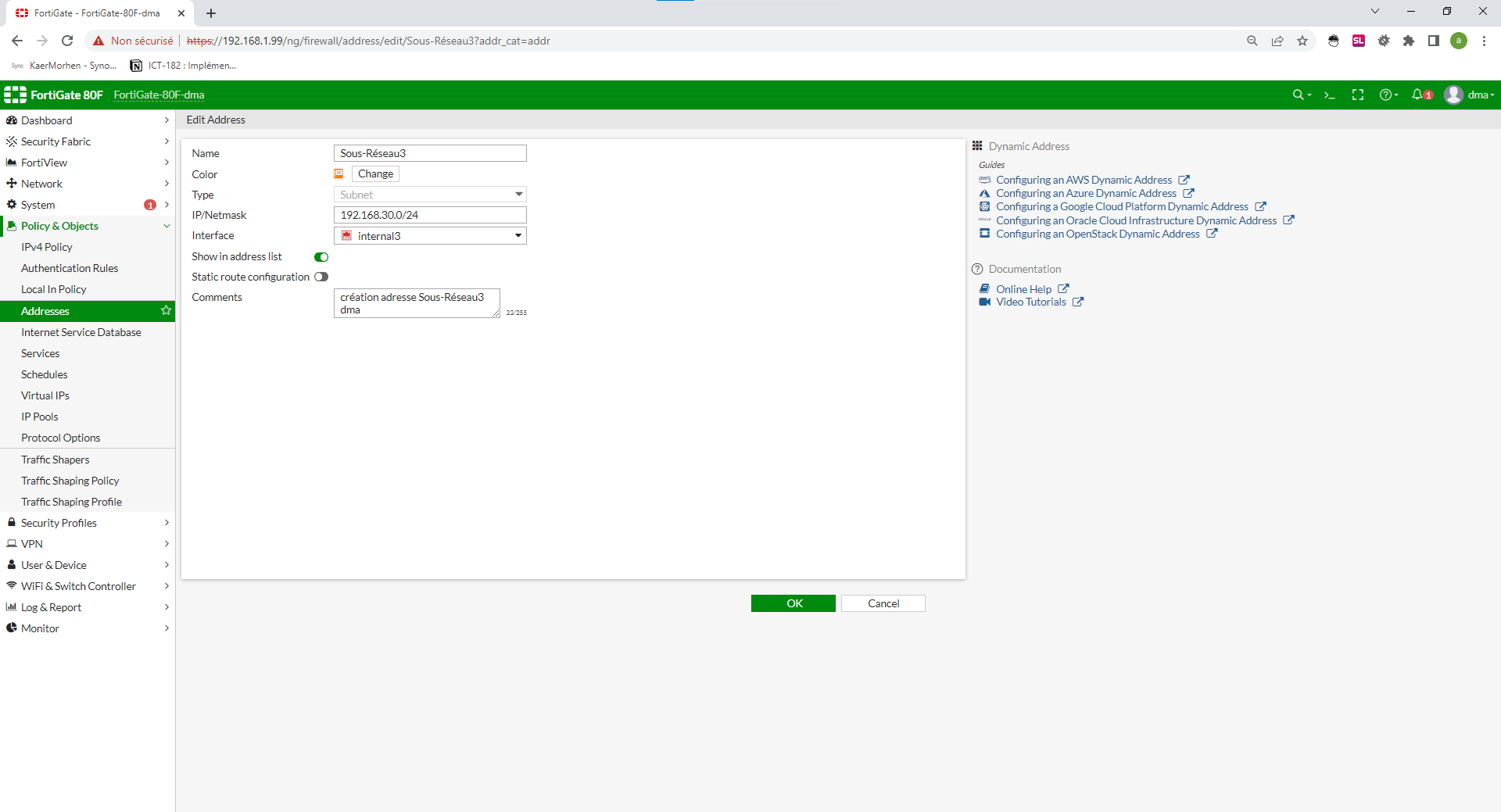


Figure création de l'adresse du sous-réseau 3.

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*

1. Cliquer sur OK

Une image contenant texte

Description générée automatiquement

Figure Création adresse perdu.com.

Récapitulatif des adresses crées.

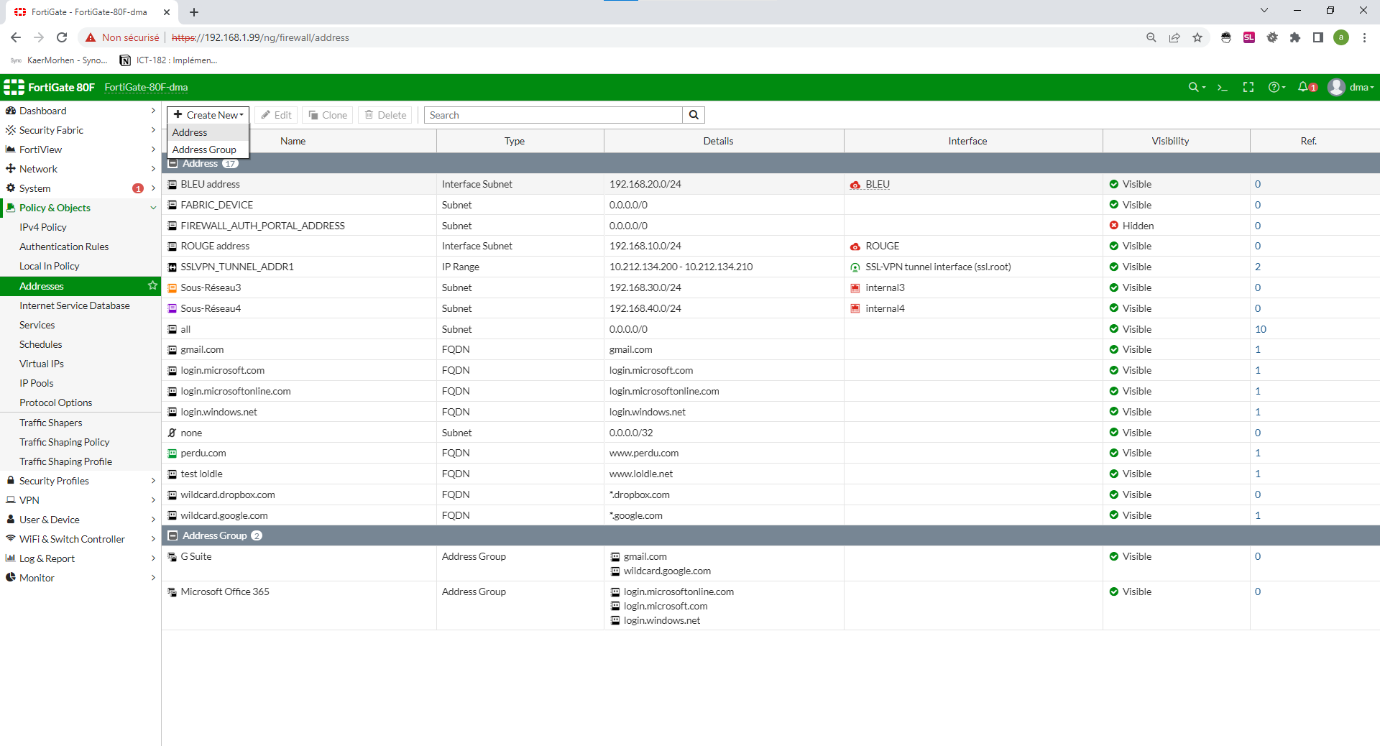


Figure Récapitulatif des adresses crées.

## 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 :

1. Création de la règle de firewall Policy & Objects -> IPv4 Policy -> Create New
2. *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*

1. Cliquer sur OK

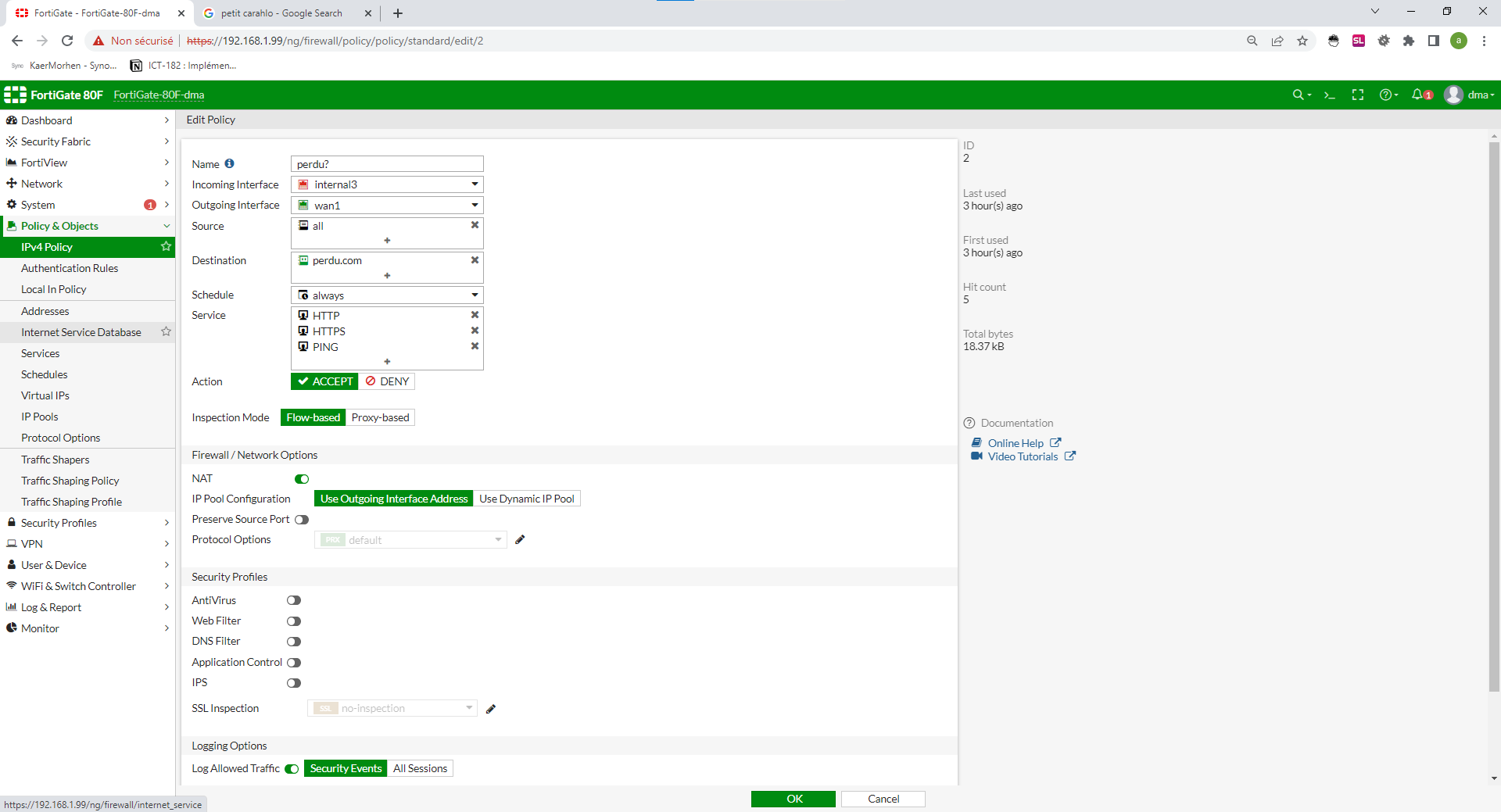


Figure Règle accès à perdu.com sur interface internal3.

1. Création de la règle de firewall Policy & Objects -> IPv4 Policy -> Create New
2. *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*

1. Cliquer sur OK

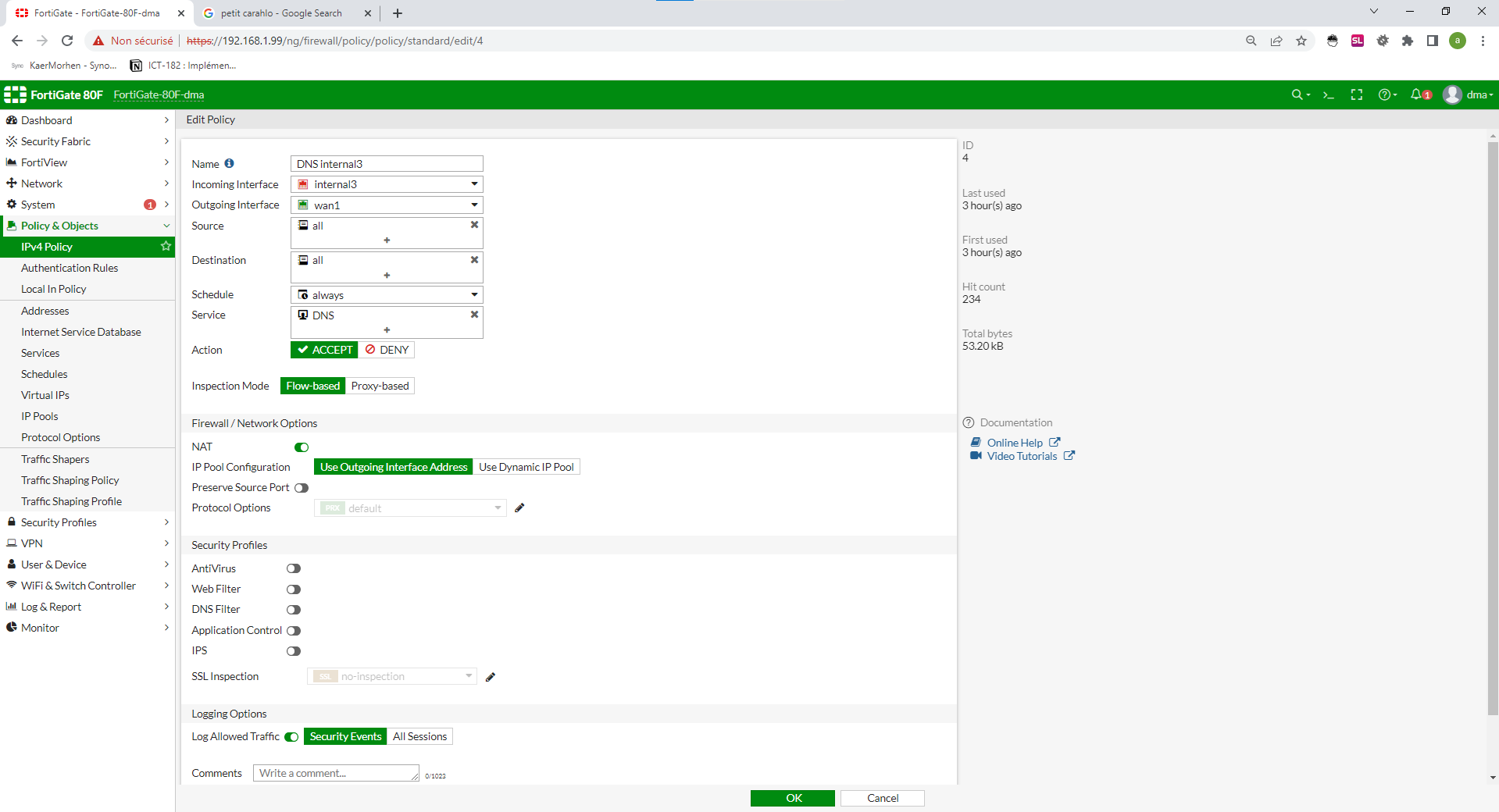


Figure Règle accès DNS sur interface internal3.

Récapitulatif des règles:

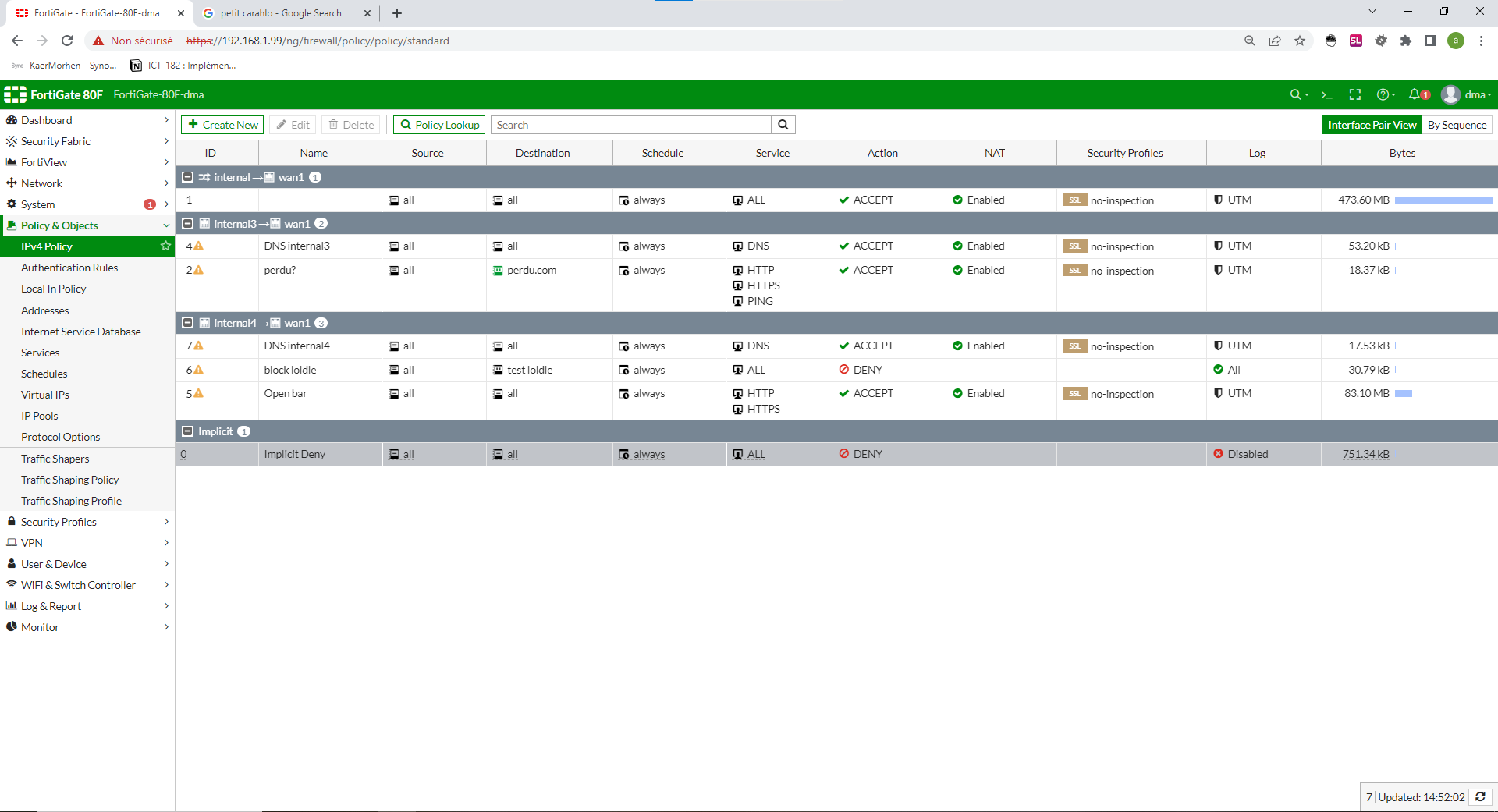


Figure Ensemble des règles crées pour différents tests.

# Table des illustrations

[Figure 1 Bouton reset. 3](#_Toc130930590)

[Figure 2 Ouvrir la console CLI et effectuer le reset. 3](#_Toc130930591)

[Figure 3 Login vide. 3](#_Toc130930592)

[Figure 4 Login pour première connexion. 4](#_Toc130930593)

[Figure 5 Changement de mot de passe lors de la première connexion. 4](#_Toc130930594)

[Figure 6 Dashboard. 4](#_Toc130930595)

[Figure 7 Mise à jour du firmware. 5](#_Toc130930596)

[Figure 8 Changement host name & fuseau horaire. 5](#_Toc130930597)

[Figure 9 Création nouvel administrateur. 6](#_Toc130930598)

[Figure 10 Libération des ports. 7](#_Toc130930599)

[Figure 11 Créer une interface VLAN. 8](#_Toc130930600)

[Figure 12 Nouveau VLAN ROUGE. 8](#_Toc130930601)

[Figure 13 Création sous-réseau internal3. 9](#_Toc130930602)

[Figure 14 Les ports sur l'interface internal ont accès au WAN étant donné la configuration de base. 10](#_Toc130930603)

[Figure 15 création de l'adresse du sous-réseau 3. 10](#_Toc130930604)

[Figure 16 Création adresse perdu.com. 11](#_Toc130930605)

[Figure 17 Récapitulatif des adresses crées. 11](#_Toc130930606)

[Figure 18 Règle accès à perdu.com sur interface internal3. 12](#_Toc130930607)

[Figure 19 Règle accès DNS sur interface internal3. 13](#_Toc130930608)

[Figure 20 Ensemble des règles crées pour différents tests. 14](#_Toc130930609)