Mise en service d’un pare-feu



Table des matières

[1 Analyse préliminaire 4](#_Toc130996332)

[1.1 Introduction 4](#_Toc130996333)

[1.2 Objectifs 4](#_Toc130996334)

[1.3 Planification initiale 5](#_Toc130996335)

[1.4 Cahier des Charges 6](#_Toc130996336)

[1.5 Règles pare-feu CPNV 7](#_Toc130996337)

[2 Analyse / Conception 8](#_Toc130996338)

[2.1 Méthode de travail 8](#_Toc130996339)

[2.2 Informations générales 9](#_Toc130996340)

[2.2.1 Définition 9](#_Toc130996341)

[2.2.2 Fortinet 9](#_Toc130996342)

[2.3 Concept 11](#_Toc130996343)

[2.3.1 Déroulement du projet 11](#_Toc130996344)

[2.4 Stratégie de test 11](#_Toc130996345)

[2.5 Risques techniques 12](#_Toc130996346)

[2.5.1 Manque de compétence 12](#_Toc130996347)

[2.5.2 Risque forfaitaire 12](#_Toc130996348)

[2.5.3 Risque "propriétaire" 12](#_Toc130996349)

[2.6 Planification 13](#_Toc130996350)

[2.7 Dossier de conception 13](#_Toc130996351)

[3 Réalisation 14](#_Toc130996352)

[3.1 Dossier de réalisation 14](#_Toc130996353)

[3.2 Description des tests effectués 20](#_Toc130996354)

[3.3 Erreurs restantes 20](#_Toc130996355)

[3.4 Liste des documents fournis 21](#_Toc130996356)

[4 Conclusions 22](#_Toc130996357)

[5 Remerciements 24](#_Toc130996358)

[Fin du rapport 24](#_Toc130996359)

[6 Annexes 25](#_Toc130996360)

[6.1 Résumé du rapport du pré-TPI 25](#_Toc130996361)

[6.2 Sources 26](#_Toc130996362)

[6.3 Glossaire 27](#_Toc130996363)

[6.4 Journal de travail 28](#_Toc130996364)

[6.5 Manuel d’Installation 32](#_Toc130996365)

[1 Dans la boite 32](#_Toc130996366)

[2 Interfaces physique 33](#_Toc130996367)

[2.1 Front panel 33](#_Toc130996368)

[2.2 Back Panel 33](#_Toc130996369)

[3 Connecter le FG 80F 34](#_Toc130996370)

[4 Première connexion à l'interface graphique du FG 80F 35](#_Toc130996371)

[6.6 Manuel d’Utilisation 36](#_Toc130996372)

[1. Mise à zéro de l'appareil 36](#_Toc130996373)

[a. Physique 36](#_Toc130996374)

[b. Via CLI 36](#_Toc130996375)

[2. Première connexion 36](#_Toc130996376)

[3. Appropriation 38](#_Toc130996377)

[a. Définition 38](#_Toc130996378)

[b. Mise à jour du Firmware 38](#_Toc130996379)

[c. Changement du nom d'hôte & du fuseau horaire de l'appareil 38](#_Toc130996380)

[d. Création d'un administrateur 38](#_Toc130996381)

[e. Commentaire 39](#_Toc130996382)

[4. Networking 40](#_Toc130996383)

[a. Libérations des ports 40](#_Toc130996384)

[b. Création de VLANs 40](#_Toc130996385)

[c. Création de sous-réseaux 41](#_Toc130996386)

[5. Accès à internet 43](#_Toc130996387)

[6. Règles de pare-feu 43](#_Toc130996388)

[a. Création des adresses 43](#_Toc130996389)

[b. Création des règles 44](#_Toc130996390)

[6.7 Manuel de tests 48](#_Toc130996391)

[Fin des annexes 58](#_Toc130996392)

# Analyse préliminaire

## Introduction

Ce pré-TPI est un dérivé de la fiche signalétique qui avait été soumise en décembre 2022 au doyen en fonction à cette date, Mr. Claude Egger, qui avait pour titre : "*Assurer la sécurité d’un réseau informatique*" et pour description générale : "*Assurer la cybersécurité d’une entreprise à l’aide d’une approche sous 3 angles ; matériel (Firewall, IDS, UTM), outils (proxy, vpn) et politique (droits de partage, ntfs, politique mot de passe, subnetting).*"

À la suite d'une discussion avec Mr. Varela, il s'est avéré que ce projet aurait été trop théorique et par conséquent pas adapté à un travail de TPI. Cependant il m'a été proposé par Mr. Varela d'effectuer un travail dans la lignée de ma fiche signalétique ; me permettant de faire mes premières expériences avec un pare-feu physique tout en mettant en pratique une partie des connaissances acquises pendant ma formation FPA, notamment concernant la partie réseau informatique.

Lors d'une seconde discussion avec Mr. Varela, il est ressortit qu'une partie de ce pré-TPI pourrait servir à élargir le cours I-CT 146 intitulé "Relier une entreprise à internet" et qui contient une composante pare-feu, limitée pour le moment à un simple exercice théorique.

## Objectifs

*Tiré du cahier des charges :*

"Le projet utilisera l’infrastructure réseau physique du CPNV comme étant la partie WAN.

La fonction de pare-feu virtuel sera activée sur le Fortinet avec deux réseaux distincts accédant à Internet chacun ayant sa carte réseau physique et chacun son adressage IP.

Des VM clients pourront être utilisées pour tester l’accès à Internet.

Afin de faciliter la sortie sur Internet la MAC adresse de la carte réseau WAN sera transmis au SIp

Les règles de sorties (ports et protocoles) seront les mêmes que celle du CPNV"

Pour résumé en une phrase : il faut, grâce au pare-feu, créer deux sous-réseau ayant accès au WAN, ayant chacun leur règles, comparable à celle du CPNV.

## Planification initiale

**Une image contenant graphique

Description générée automatiquement**

Figure 1 Planification initiale

## Cahier des Charges

*Cahier des charges, envoyée le 01.02.2023 par Mr. Varela :*

TITRE

Mise en service d’un pare-feu Fortinet

MATÉRIEL ET LOGICIEL À DISPOSITION

1 ordinateur type CPNV avec accès Internet

1 Environnement (Windows10, Office, VMware)

Tous les médias d’installation et licence pour Windows et GLPI

Un pare-feu Fortinet entrée de gamme

1 imprimante réseau

PRÉREQUIS

Le candidat possède les bases pour installer et configurer :

Un poste client sous Windows 10

VMware Workstation

Les protocoles réseau nécessaires au projet

Les règles de Pare-feu

DESCRIPTIF DU PROJET

Le projet utilisera l’infrastructure réseau physique du CPNV comme étant la partie WAN.

La fonction de pare-feu virtuel sera activée sur le Fortinet avec deux réseaux distincts accédant à Internet chacun ayant sa carte réseau physique et chacun son adressage IP.

Des VM clients pourront être utilisées pour tester l’accès à Internet.

Afin de faciliter la sortie sur Internet la MAC adresse de la carte réseau WAN sera transmis au SIp

Les règles de sorties (ports et protocoles) seront les mêmes que celle du CPNV

LIVRABLES

Le candidat est responsable de livrer à son chef de projet et à l’expert :

* Une planification initiale
* Un rapport de projet
* Un journal de travail
* Les marches à suivre techniques
* Toutes les sources utilisées

POINTS TECHNIQUES EVALUES SPECIFIQUES AU PROJET

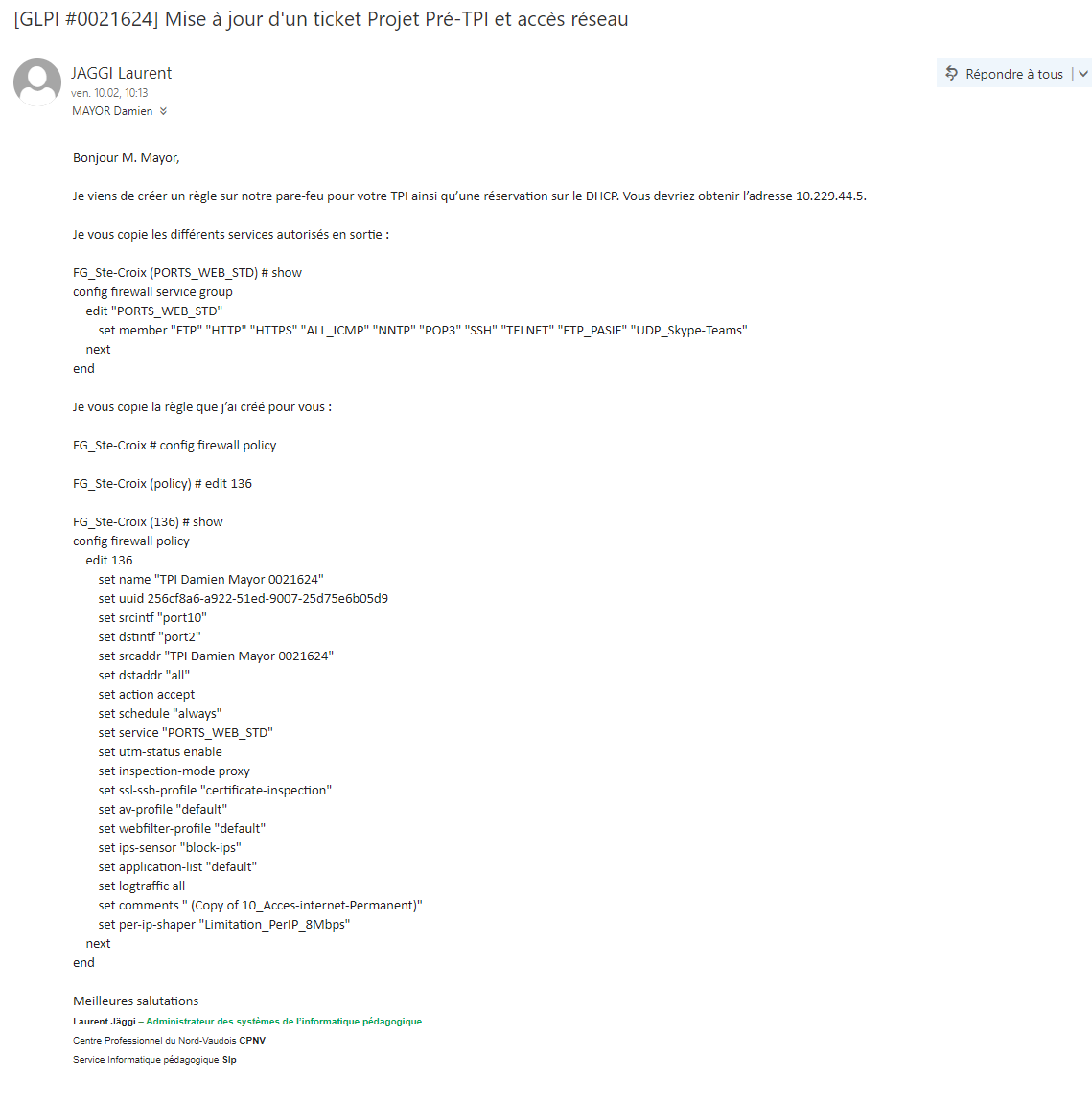
La grille d’évaluation définit les critères généraux selon lesquels le travail du candidat sera évalué (documentation, journal de travail, respect des normes, qualité …).

En plus de cela, le travail sera évalué sur les 7 points spécifiques suivant (Point A14 à A20) :

1. La solution est fonctionnelle
2. Facilité de mise en œuvre
3. Documentation d’installation et de l’utilisation de la solution pour l’IT
4. La solution de pare-feu virtuel proposée peut être reproduite
5. Les règles de pare-feu
6. Les tables de routage
7. Description et qualité des tests effectués

## Règles pare-feu CPNV

*Email concernant règles du pare-feu CPNV, envoyé le 10.02 par Laurent Jaggi*



# Analyse / Conception

## Méthode de travail

Pendant la formation nous avons pu découvrir à travers le module I-CT 431 intitulé "Exécuter des mandats de manière autonome dans un environnement informatique" le framework Scrum, méthode dites agile.

Selon moi cette méthodologie est excellente pour les développeurs qui travaillent en équipe et qui ont un besoin de partage accru par l'interdépendance inhérent au développement informatique mais se prête moins à un projet mené par une unique personne, d'autant plus dans le domaine du réseau informatique, très linaire.

C'est pour cette raison que j'ai choisi la méthodologie "Waterfall" (ou cascade) qui me semble plus appropriée. D'ailleurs, le document de base utilisé pour cette documentation, téléchargée du site [www.tpivd.ch](http://www.tpivd.ch), est bâtie sur ce modèle en cascade.

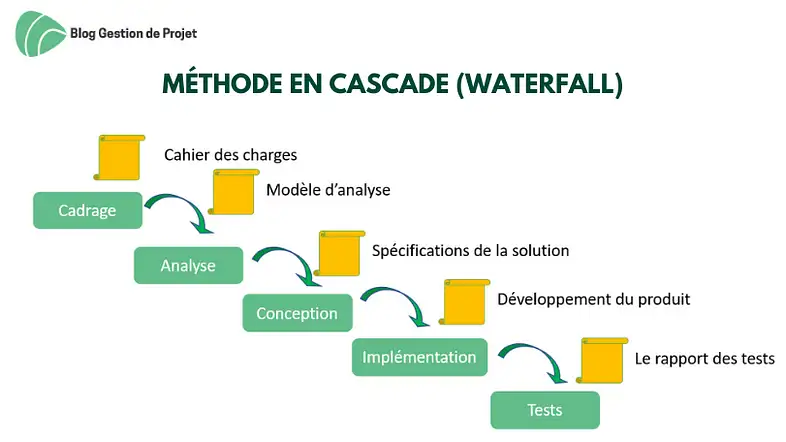


Figure 2 méthode en cascade. Source blog-gestion-de-projet.com

Les avantages de cette méthode sont qu'elle est simple, facile à mettre en place, logique et structurée. Son inconvénient principal et son manque de flexibilité dû à son déroulement séquentiel.

## Informations générales

### Définition

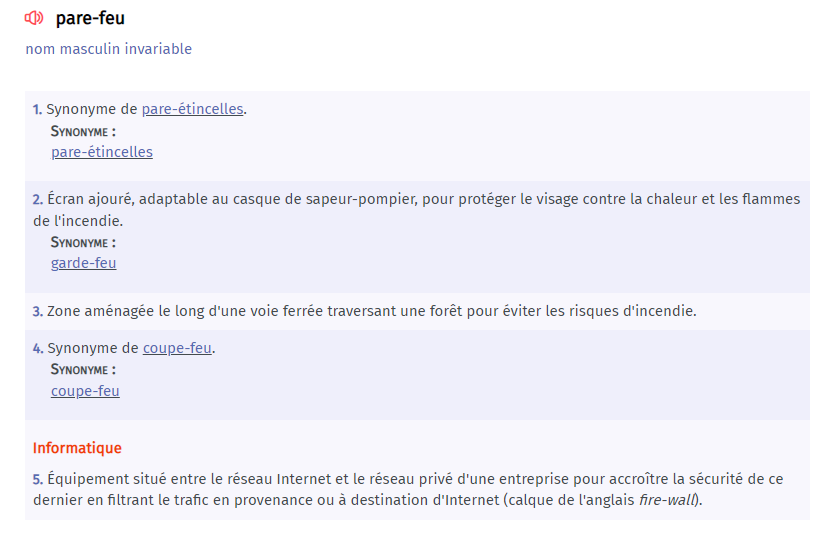


Figure 3 Définition pare-feu. Source www.larousse.fr

### Fortinet

Fortinet, Inc. est une entreprise américaine fondée en 2000, basée à Sunnyvale en Californie et qui compte 13'000 employés. Cette société développe des appareils et des logiciels pour la sécurité de l'information tels que des pare-feu, des programmes antivirus ou encore des systèmes de détection d'intrusion.

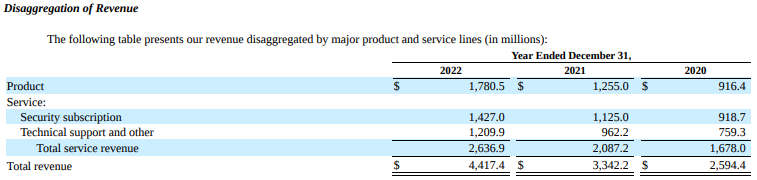


Figure 4 Revenus Fortinet 2022. Source investor.fortinet.com

Avec des revenus supérieurs à 4 milliards de dollars, environ 60% viennent de la vente de services et les 40% restant proviennent de la vente de matériel.

Fortinet tire donc ses revenus majoritairement de la vente de services liés à leurs appareils. Ceci a conduit l’entreprise à réduire fortement les fonctionnalités disponibles sur leurs appareils ne nécessitant pas d’abonnement.

Voici en image ce à quoi donne droit les différents niveau d'abonnements Fortinet : pour référence nous avons droit aux fonctionnalités de base.

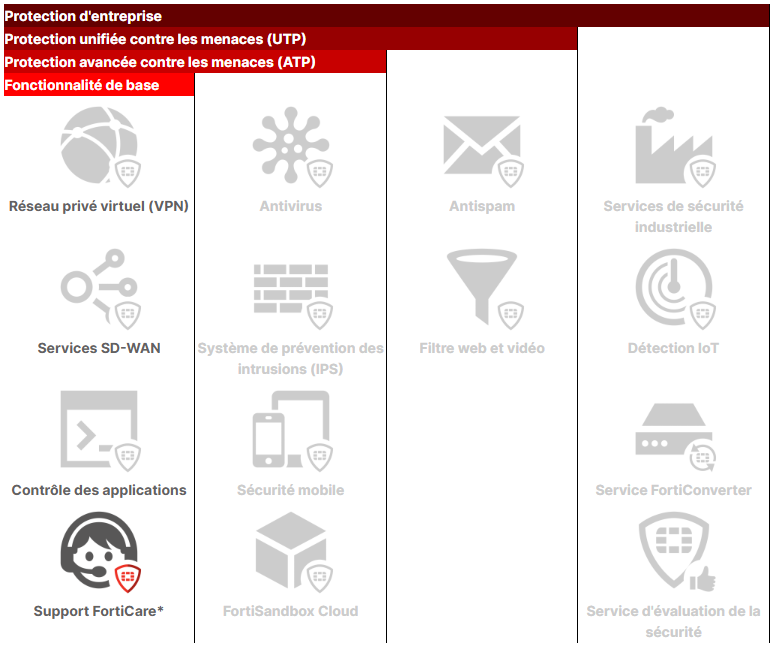


Figure 5 Niveaux d'abonnements. Source [www.enbitcon.ch](http://www.enbitcon.ch)

Ce tableau est confirmé par une capture d'écran de la section FortiGuard du FG-80F :

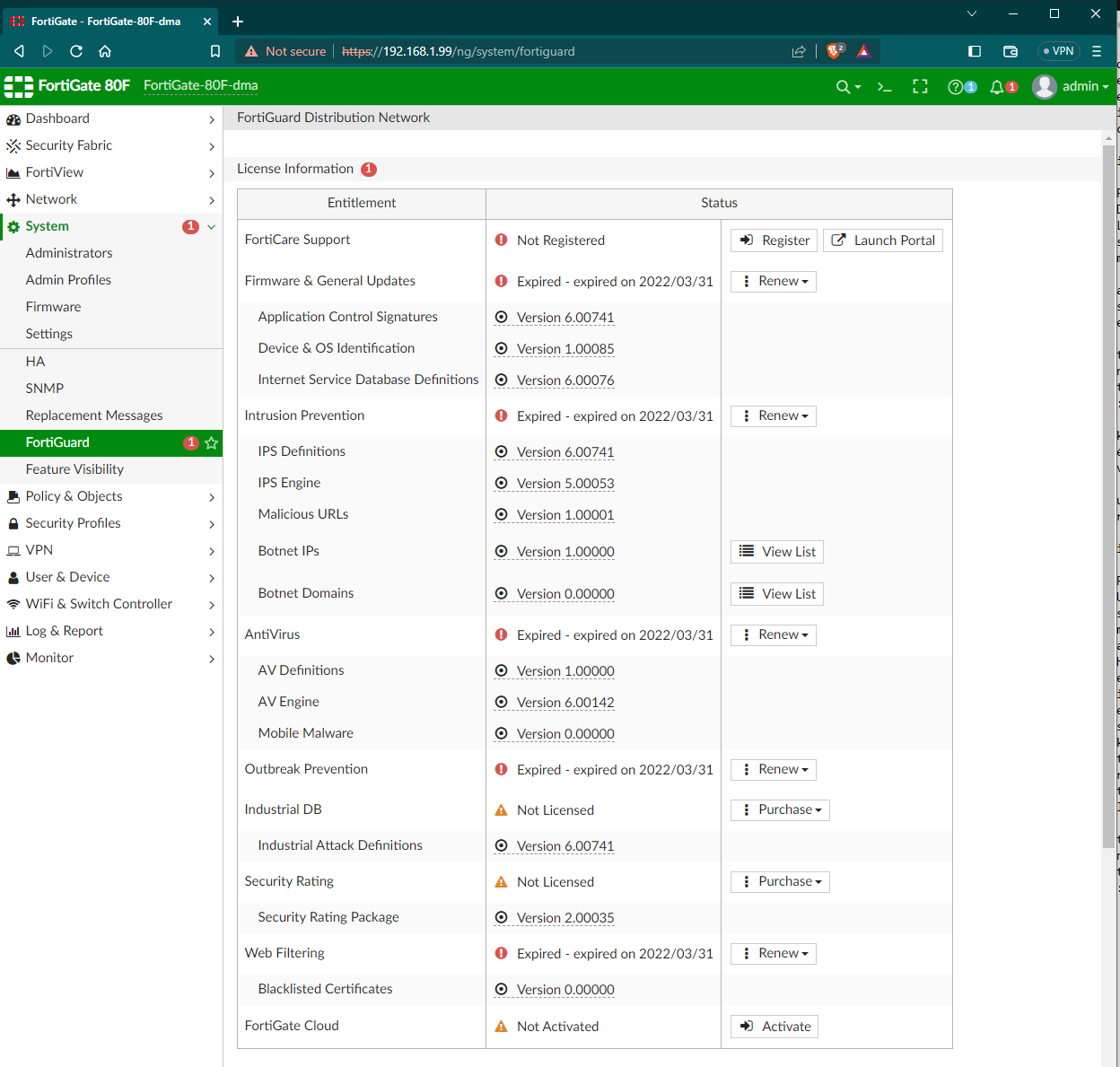


Figure 6 Services disponible sur le FG-80F. Source GUI 192.168.1.99

## Concept

### Déroulement du projet

Je prévois une implémentation du projet en 4 phases :

Installation : mise en place physique du firewall, avec vérification de fonctionnement, branchements et sa reconnaissance par le réseau du CPNV, sensé jouer le rôle de WAN pour le projet. Aussi basique que cela semble, la couche n° du modèle OSI est toujours la première que l'on vérifie car si un problème surgit à ce niveau-là : rien ne pourra fonctionner.

Cela va permettre également de vérifier que la mise à zéro du pare-feu c'est bien fait et qu'il est donc possible de commencer le projet sur une base saine.

Appropriation : reproduire sur le pare-feu ce que l'on ferait avec toute installation d'un nouvel ordinateur : mise à jour du système d'exploitation et des drivers, création d'admin local

Network : créer des sous-réseaux indépendants, capable de distribuer des adresses IP propre à leur plage attribuée et à communiquer entre elles selon besoin. Que ces réseaux soient joignables par un ou plusieurs ordinateurs. Ils devront aussi être capable d'accéder au WAN.

Firewall : mettre en place les règles qui permettent aux interfaces d'accéder au WAN ou entre elles si besoin, ou alors dans le cas inverse, de restreindre les accès.

## Stratégie de test

Basé sur mon expérience des tests dans le domaine des réseaux informatique : mes tests vont être très linéaire, chacun étant la suite logique de l'autre. J'ai une liste d'une vingtaine de tests qui va pouvoir, tout au long de l'implémentation du projet, tester le bon déroulement de ladite implémentation. Tous les tests seront de niveau unitaire et de type fonctionnel.

Chaque phase (installation, appropriation, network et firewall) va être testée dans l'ordre de réalisation

Les tests se feront toujours avec le FortiGate 80F fournit ainsi qu'avec le PC05 à ma disposition. En supplément, mon MacBook air personnel pourra être utilisé notamment pour les tests liés au networking et les distributions par les sous-réseaux, d'adresses IP.

Je prévois des tests assez simples : "obtient-on le résultat attendu ?" Si la réponse est oui : on passe à la prochaine implémentation, si la réponse est non : on revient en arrière sur les choses mises en place depuis le dernier test réussi.

Je prévois de faire les tests moi-même dans un premier temps et par la suite de les faire faire par un de mes camarades avec l'aide du guide d'utilisation.

La liste complète des tests, de leurs résultats ainsi que les preuves sont disponible dans les annexes.

**Edit :** Au final, tant mes camardes et moi nous sommes retrouvés à court de temps. Les tests n'ont donc été réalisé que par moi.

## Risques techniques

### Manque de compétence

Avant le début de ce projet mes connaissances en matière de pare-feu se limitaient à deux expériences :

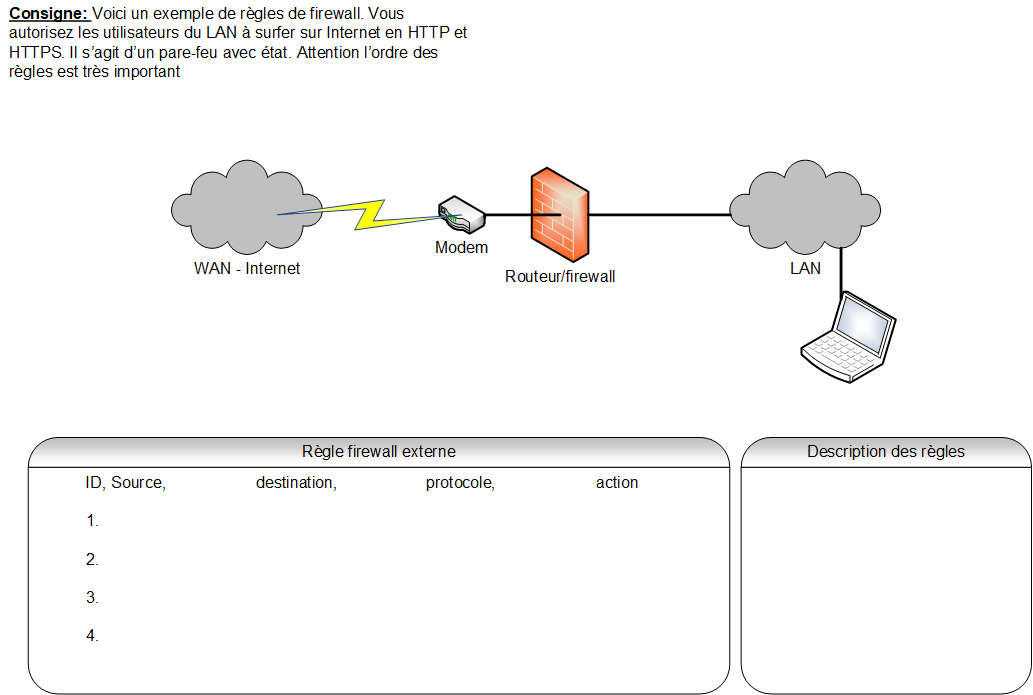
1. I-CT 146 dans lequel nous avons remplis manuellement la feuille suivante :

Figure 7 Exercice règles pare-feu. Sources I-CT146

1. Eteindre le pare-feu logiciel de nos machines virtuelles afin de pouvoir utiliser le protocole ICMP.

Pour combler ce manque de connaissances j’ai passé beaucoup de temps à consulter le document FortiOS-6.2.3-Cookbook.pdf, j’ai lu le livre "UTM For Dummies" et j’ai pris le temps de discuter avec Mr. Laurent Jaggi, enseignant au CPNV et membre de l’équipe du Service Informatique pédagogique du CPNV.

### Risque forfaitaire

Le FG 80F ne comprend pas d’abonnement. Comme expliqué au point 2.2.2 Fortinet tire maintenant la majorité de ses revenus de la vente d’abonnements. Cela limite les fonctionnalités accessibles sans abonnement : par exemple, le filtrage par catégorie, tel qu’utilisé par le CPNV/Etat de Vaud n’est pas possible.

Fortinet ne proposant pas de solution gratuite pour étudiants, rien n’a pu être fait pour remédier à ce problème.

### Risque "propriétaire"

N’étant pas le propriétaire de l’appareil, il m’est impossible de le faire enregistrer. Ceci a pour conséquence de ne pas pouvoir faire de mise à jour du système d’exploitation. Nous sommes donc limités à l’utilisation de FortiOS 6.2.3, sortis en mars 2019. La version la plus récente de FortiOS étant la version 7.2.4.

## Planification

Planification effective du projet. Pour le détail : se référer au journal de travail de l'annexe 6.4

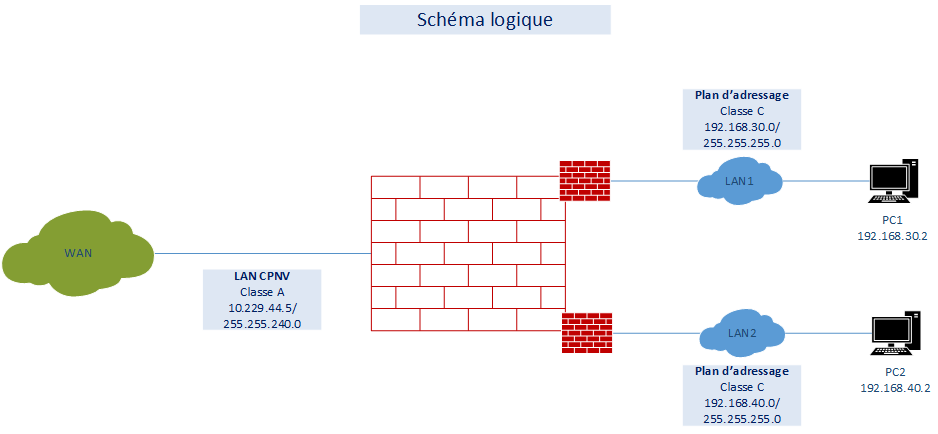
## Dossier de conception

Liste du matériel utilisé :

|  |  |  |  |
| --- | --- | --- | --- |
| PC CPNV | Pare-feu | Switch | PC personnel |
| Dell Optiplex 7070 | FortiGate 80F | Netgear ProSafe 16 | MacBook Air 2020 |
| Windows 10 Edu 21H2 | FortiOS 6.2.3 | - | OSX 13.2.1 |

J'ai fait le choix d'utiliser l'interface graphique proposée par le FortiGate mais il aurait été possible d'utiliser uniquement l'interface de commande de ligne qui est intégrée à FortiOS. Ce choix était possible car le projet se déroulait en classe avec tous les équipements sous la main. En plus de l'interface de ligne de commande, le FortiGate possède un port console pour les situations d'installation/dépannage un peu plus "nomade".

D'un point de vue logiciel, les seuls utilisés ont été des web browsers. Google Chrome pour le Dell et Apple Safari pour le MacBook Air.



Mon projet étant de taille modeste j'ai pu le réaliser physiquement, sans avoir besoin de recourir à des machines virtuelles. Mon schéma logique est donc également mon schéma physique.

La marche à suivre pour l'installation physique du pare-feu se trouve dans l'annexe 6.5 Guide d'installation de ce document.

La marche à suivre pour la création des réseaux et des règles de pare feux se trouve dans l'annexe 6.6 Guide d'utilisation de ce document

Etant resté en mode NAT une table de routage n'a pas été nécessaire.

# Réalisation

## Dossier de réalisation

**Libérations des ports physique**

* Se rendre dans Network -> Interface -> Hardware Switch -> internal -> double-click.
* 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
* Connectez votre câble rj45 de votre ordinateur aux ports restant 5 ou 6 du pare-feu.

**Création du sous-réseau internal3**

* Se rendre dans Network -> Interface -> Physical Interface -> internal3 -> double-click
* *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*

* Cliquer sur OK

**Création du sous-réseau internal4**

* Se rendre dans Network -> Interface -> Physical Interface -> internal4 -> double-click
* *Name: internal4*

*Alias:*

*Type: Physical Interface*

*Role: Undefined*

*Addressing mode: Manual*

*IP/Netmask: 192.168.40.1/255.255.255.0*

*Secondary IP address: off*

*IPv4: HTTPS, HTTP, PING, SSH*

*Receive LLDP: Use VDOM Setting*

*Transmit LLDP: Use VDOM Setting*

*DHCP Server: on*

*Address range: 192.168.40.2-192.168.40.254*

*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*

* Cliquer sur OK

**Création de l'adresse du sous-réseau internal3**

* Policy & Objects -> Addresses -> Create New -> Address
* *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*

* Cliquer sur OK
* 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 internal3

**Création de l'adresse du sous-réseau internal4**

* Policy & Objects -> Addresses -> Create New -> Address
* *Name: Sous-Réseau4*

*Color: orange*

*Type: Subnet*

*IP/Netmask: 192.168.40.0/24*

*Interface: internal3*

*Show in address list: on*

*Static route configuration: off*

*Comments: création addresse Sous-Réseau4 dma*

* Cliquer sur OK

**Création adresse perdu.com**

* Se rendre sur Policy & Objects -> Address -> Create New -> Address
* *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*

* Cliquer sur OK

**Création adresse test loldle**

* Se rendre sur Policy & Objects -> Address -> Create New -> Address
* *Name: test loldle*

*Color: vert*

*Type: FQDN*

*FQDN: www.loldle.net*

*Interface: any*

*Show in address list: on*

*Static route configuration: off*

*Comments: création adresse loldle.net dma*

* Cliquer sur OK

**Création IPv4 Policy DNS internal3**

* Policy & Objects -> IPv4 Policy -> Create New
* *Name: DNS internal3*

*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 internal3 dma*

*Enable this policy: on*

* Cliquer sur OK

**Création IPV4 Policy perdu ?**

* Policy & Objects -> IPv4 Policy -> Create New
* *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*

* Cliquer sur OK

**Création IPv4 Policy DNS internal4**

* Policy & Objects -> IPv4 Policy -> Create New
* *Name: DNS internal4*

*Incoming Interface: internal4*

*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 internal4 dma*

*Enable this policy: on*

* Cliquer sur OK

**Création IPv4 Policy block loldle**

* Policy & Objects -> IPv4 Policy -> Create New
* *Name: block loldle*

*Incoming Interface: internal4*

*Outgoing Interface: wan1*

*Source: all*

*Destination: perdu.com*

*Schedule: always*

*Service: HTTP, HTTPS*

*Action: DENY*

*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*

* Cliquer sur OK

**Création IPv4 Policy Open bar**

* Policy & Objects -> IPv4 Policy -> Create New
* *Name: perdu?*

*Incoming Interface: internal4*

*Outgoing Interface: wan1*

*Source: all*

*Destination: all*

*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*

* Cliquer sur OK

Deux sous-réseaux ont été créé : internal3 et internal4, correspondant aux ports physiques 3 et 4 du pare-feu. Ils distribuent chacun des adresses IP propre à leurs plages respectives. Ces deux sous-réseaux ont des règles de pare-feu propre :

Internal 3 n'accès qu'au site [www.perdu.com](http://www.perdu.com)

Internal 4 a accès à l'entier d'internet sauf au site [www.loldle.net](http://www.loldle.net)

Avec un abonnement FortiGuard il aurait été possible de faire du filtrage web, comme le fait le CPNV, et donc de pouvoir reproduire en grande partie le pare-feu de l'école.

## Description des tests effectués

Voir annexe 6.7 Manuel de test

## Erreurs restantes

J'ai remarqué deux erreurs :

1) Il a été impossible de transmettre à mes deux réseaux les mêmes règles que celles du CPNV. Comme expliqué aux points 2.2.2 et 2.5.2: sans accès à la formule payante, il m'est impossible de répliquer le filtrage web qu'utilise le pare-feu de l'école.

Une réplication manuelle n'est pas envisageable vu la quantité de sites qu'il faudrait bloquer. Une alternative techniquement réalisable serait de bloquer tous les sites et seulement d'en autoriser une sélection. Cependant cette solution n'est pas viable à l'échelle d'une école sur le long terme, les étudiants ayant besoin d'un large accès à internet pour les nombreuses recherches demandées par leurs formations respectives.

Deux solutions : trouver un pare-feu qui ne fait pas payer son service de filtrage ou alors prendre un abonnement à FortiGuard.

2) Je me suis rendu compte trop tard que j'avais mal lu mon cahier des charges et oublié un élément essentiel : *La fonction de pare-feu virtuel sera activée sur le Fortinet avec deux réseaux distincts accédant à Internet chacun ayant sa carte réseau physique et chacun son adressage IP.*

Le pare-feu Fortinet offre deux mode : Transparent et NAT, ce dernier étant le mode de base. Il existe la possibilité de changer de mode, ce qui aurait pu selon permettre de mettre en place cet élément du cahier des charges.

Ayant raté ce point, il ne me reste pas assez de temps pour tenter de le mettre en œuvre.

La conséquence est que les deux réseaux sortent sur internet avec la même adresse IP au lieu d'avoir des adresses IP différentes. Il n'y a pas d'autre moyen de remédiation que de passer en mode transparent. J'aimerai beaucoup voir une correction sur comment arriver à ce résultat.

## Liste des documents fournis

-Rapport de projet pré-TPI DMA.pdf

-Sources (en annexe)

-Glossaire (en annexe)

-Journal de travail (en annexe)

-Manuel d'installation (en annexe)

-Manuel d'utilisation (en annexe)

-Manuel de tests (en annexe)

Disponible sur N:\COMMUN\ELEVE\INFO\SI-CA2a\pré-TPI\Damien Mayor\Sources

-Fiche signalétique SI-CA2a\_Mayor\_Damien.pdf

-CDC Pré-TPI-23-SYS-MAYOR Damien – Fortinet.pdf

-FG-80F-datasheet.pdf

-FG-80F\_quick\_start\_guide.pdf

-Fortinet Annual Report 2022.pdf

-FortiOS-6.2.3-Cookbook.pdf

-FortiOS-6.2.13-CLI\_reference.pdf

-UTM\_For\_Dummies\_r2.pdf

# Conclusions

Objectifs atteints / non-atteints

Au niveau des objectifs atteints : le pare-feu fonctionne, il propose des sous-réseaux chacun ayant sa plage IP et ses règles propre. Les pare-feu virtuels ne reproduisent certes pas les mêmes règles de l'école mais ceci est lié au non-abonnement au service FortiGate et donc hors de portée dans la configuration actuelle.

En ce qui concerne les échecs : dû à mon inattention les deux sous-réseaux sortent en configuration NAT sur le WAN au lieu de sortir chacun de manière indépendante.

Points positifs / négatifs

Le sujet était très intéressant pour moi et mon orientation cybersécurité. Mr. Varela a réussi à transformer ma demande qui était trop théorique en projet pratique. J'ai le sentiment que je ressors de ce projet avec des compétences particulières que j'espère pouvoir utiliser bientôt.

Par contre, se lancer sur un appareil totalement inconnu, limité artificiellement dans ses capacités, sans aucune forme support, c'était difficile, très difficile. Je suis content d'avoir réussi à trouver une solution fonctionnelle, mais ne pouvant pas reproduire exactement ce qu'il m'était demandé, j'ai l'impression de livrer un POC plutôt qu'un projet complet.

Difficultés particulières

J'ai rencontré 3 difficultés: mon manque de connaissance sur le sujet du pare-feu mais surtout la complexité de l'interface graphique de FortiOS, renforcé par. Mon manque de rigueur par rapport au plan que je m'étais fixé dès que j'ai rencontré des difficultés. Et pour finir mon manque de discipline, notamment dans la tenue de la documentation et son journal de travail.

Améliorations

Il y a plusieurs suites possibles pour ce sujet : **la mise en place du mode transparent** que j'ai échoué à mettre en place. Ceci permettrait aux réseaux d'être vraiment indépendants les uns des autres.

**La mise en place de VPN** pourrait également selon moi être une très intéressante évolution, notamment dans un monde post-Covid où le travail à domicile est encore très présent et par conséquent le besoin de connexions sécurisées aux ressources de l'entreprise très important.

**L'achat d'un abonnement FortiGuard** permettrai lui aussi de vraiment pouvoir explorer tout le potentiel du pare-feu FG 80F.

J'ai fait le choix d'utiliser uniquement l'interface graphique proposée mais toute l'installation et documentation relative aurait également pu être fait en ligne de commande. Selon les besoins et le publique cible de la documentation, ce serait bien de proposer les deux variantes.

Pour finir sur une touche plus personnelle, j'anticipais ce pré-TPI qui s'annonçait comme une répétition générale mais qui s'est transformée en Masterclass des choses à ne pas faire : manque de discipline, manque de rigueur, mauvais gestion du temps. Je retire énormément d'enseignement que je mettrai en œuvre pour mon TPI, tant dans la méthodologie de travail que dans le niveau de détail à mettre dans ma documentation, mes tests et tous les documents à fournir.

Je suis fier du travail accompli, tout en étant conscient du travail qu'il faudra produire afin de réussir mon TPI. Je me réjouis d'avoir des retours sur ma documentation mais également d'un point de vue technique sur comment j'aurais pu mettre en œuvre une solution plus efficiente. D'ailleurs, ayant découvert pendant ce pré-TPI que Fortinet a lancé un "training institute" et je vais profiter des vacances de paques pour me faire certifier ; pour mes connaissances personnelles mais également pour élargir mes compétences professionnelles.

# Remerciements

A Monsieur Francis Varela pour avoir réussi à trouver un projet intéressant, dans l'esprit de ma demande et surtout pour un projet qui me sera utile à l'avenir.

A Monsieur Laurent Jaggi pour sa disponibilité, sa patience et son support pendant ce projet.

A Monsieur Sylvain Fasola pour avoir partagé avec nous son expérience du TPI, prouvant que même quelqu'un comme lui, reconnu pour ses compétences, peut échouer la réalisation de son TPI mais qu'en documentant le tout on peut quand même s'en sortir.

# Fin du rapport

# Annexes

## Résumé du rapport du pré-TPI

J'ai reçu comme projet de pré-TPI : "Mise en service d'un pare-feu Fortinet". Ce projet est dérivé de ma fiche signalétique de décembre : "Assurer la sécurité d'un réseau informatique". J'ai reçu un pare-feu Fortinet, modèle FortiGate 80F. Je dois créer des sous-réseaux indépendants ayant chacun leurs règles de pare-feu indépendantes. Les règles de pare-feu doivent être les mêmes que celles de du CPNV

N'ayant jamais approché de pare-feu avant ce projet j'ai rencontré plusieurs challenges : le manque de connaissances, un pare-feu au capacités limitées par le manque d'abonnement payant, et par l'impossibilité de mettre à jour le système d'exploitation. Il a fallu consacrer beaucoup de temps à la recherche d'information pour finalement me concentrer quasiment uniquement sur les documentations issues de Fortinet, plus précisément le FortiOS 6.2.3 Cookbook. Certaines des solutions pour des situations proche (Routeur / Switch manageable) se sont prouvées inefficaces. De plus, une mauvaise gestion du temps m'a fait manquer un point important du projet à savoir : que chaque réseau a sa carte réseau physique. Ceci dit, je ne suis pas sûr à 100% que cela soit faisable. Je me réjouis de voir la correction.

Au final, malgré la non-perfection du travail rendu, j'arrive à proposer une solution fonctionnelle aussi proche que possible de la solution demandée. Il y a eu énormément d'apprentissage pendant ce pré-TPI, qui s'est avéré être pour moi une expérience très enrichissante et surtout une mise à niveau entre ce qu'il nous a été demandé pendant ces deux dernières années. Au final c'était un projet passionnant et j'en retire énormément d'enseignements qui me seront très utile à la réalisation de mon TPI.

## Sources

|  |  |
| --- | --- |
| *Sujet* | *Source* |
| Prix Fortinet | <https://www.avfirewalls.com/FortiGate-80F.asp> |
| Abonnements Fortinet | <https://www.enbitcon.ch/shop/fortinet/fortigate-firewall/end-of-sale/fortigate-90d> |
| Méthodologie Waterfall | <https://blog-gestion-de-projet.com/gestion-de-projet/outils-methodes-gestion-projet/> |
| Méthodologie Waterfall | <https://www.planzone.fr/blog/quest-ce-que-la-methodologie-waterfall> |
| Exécuter des mandats de manière autonome dans un environnement informatique | Cours I-CT 431 |
| Techniques de Présentation | Cours MA-09 |
| Mettre en place l'infrastructure d'une petite entreprise | Cours I-CT 117 |
| Projet en groupe | Cours ProjGrp |
| Mettre en service des composants réseaux | Cours I-CT 129 |
| Pratique réseau | Cours MA-23 |
| Relier une entreprise à internet | Cours I-CT 146 |
| Réaliser la sécurité informatique d'un système | Cours I-CT 182 |
| UTM | FTNT\_UTM\_For\_Dummies\_r2.pdf |
| Cahier des charges pré-TPI | CDC Pré-TPI-23-SYS-Mayor Damien - Fortinet.pdf |
| Commandes CLI FortiOS | FortiOS-6.2.12-CLI-Reference.pdf |
| Quick start guide FG-80F | FG-80G\_quick\_start\_guide.pdf |
| Spécificités Hardware FG-80F | FG-80F\_datasheet.pdf |
| FortiOS 6.2.3 | FortiOS-6.2.3-Cookbook.pdf |
| Détails FortiOS 6.2.3 | <https://endoflife.date/fortios> |
| Rapport annuel Fortinet | <https://investor.fortinet.com/annual-reports-and-proxies> |
| Définition pare-feu | <https://www.larousse.fr/dictionnaires/francais/pare-feu/58122> |
| Dossier TPI | <https://www.tpivd.ch/> |
| VLANs & Règles pare-feu | Laurent Jaggi |

## Glossaire

|  |  |
| --- | --- |
| *Terme* | *Définition* |
| ATP | Advanced Threat Protection : Solution de protection contre les programmes malveillants. |
| CLI | Command Line Interface : En opposition a l'interface graphique. |
| CPNV | Centre Professionnel du Nord Vaudois : Ecole des métiers à Sainte Croix. |
| DNS | Domaine Name System : Système permettant la traduction d'adresses IP en nom de domaine. |
| FG-80f | FortiGate-80F : Modèle de pare-feu Fortinet utilisé dans ce projet. |
| FortiGate | Gamme des pare-feu Fortinet. |
| FortiGuard | Abonnement de sécurité pour pare-feu Fortinet. |
| Fortinet | Société américaine active dans la cybersécurité. |
| FortiOS | Nom du système d'exploitation des équipements Fortinet. |
| GUI | Graphical User Interface : En opposition à l'interface de ligne de commande. |
| ICMP | Internet Control Message Protocol : Aussi connu sous le nom de "ping" |
| IDS | Intrusion Detection System : Solution de détection d'intrusions non autorisée ou malveillante sur un réseau. |
| IP Address | Internet Protocol Address : Elément essentiel pour la création d'un réseau. |
| IPS | Intrusion Prevention System : |
| LAN | Local Area Network : En opposition au Réseau étendu. Exemple votre réseau à la maison. |
| LED | Light-emitting diode : Dispositif opto-électronique capable d'émettre de la lumière. |
| OS | Operating System : Système d'exploitation d'un système informatique |
| Proxy | Machine qui sert d'intermédiaire entre les machines d'un réseau et internet. |
| SIp | Service Informatique Pédagogique : Support informatique du CPNV |
| UTM | Unified Threat Management : Equipement de sécurité unique qui fournit plusieurs fonctions de sécurité en un seul point du réseau. |
| UTP | Unified Threat Prevention : Voir UTM, UTP est la version Fortinet. |
| VLAN | Virtual Local Area Network : Voir le réseau local mais en virtuel. |
| VPN | Virtual Private Network : Service qui achemine le trafic internet |
| WAN | Wide Area Network : En opposition au réseau local. Exemple : internet |

## Journal de travail

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Date** | **Semaine** | **Catégorie** | **Description** | **Remarques/problèmes** | **Début** | **Fin** |
| 31.01.2023 | 1 | Mise en place | Début du Pré-TPI | Lancement du projet de Pré-TPI, téléchargement documents & personnalisation, création des journaux, création Github | 13:30:00 | 16:05:00 |
| 01.02.2023 | 1 | Mise en place | Recherche documentation | Normes ISO:27001 afin de créer un politique de sécurité de l'information pour mon entreprise | 10:40:00 | 12:15:00 |
| 01.02.2023 | 1 | Mise en place | Divers | Calculs moyennes, attente | 15:20:00 | 16:00:00 |
| 01.02.2023 | 1 | Mise en place | Reçu sujet | Prise en main d'un Fortinet: prise en main, comprendre le fonctionnement, implanter un/des firewall virtuels + début recherches Fortinet | 16:00:00 | 16:55:00 |
| 02.02.2023 | 1 | Mise en place | Découverte cahier des charges | Lecture, préparation questions pour Mr. Varela | 09:50:00 | 10:30:00 |
| 02.02.2023 | 1 | Implémentation | Créations de VMs | Machines virtuelles VM1 et VM2 selon schéma. Pas touches aux réglages réseaux, NAT et DHCP reçu de l'école | 10:30:00 | 11:40:00 |
| 02.02.2023 | 1 | Documentation | Schéma logique | Préparation du schéma logique, avec les éléments actuels. | 11:40:00 | 12:00:00 |
| 02.02.2023 | 1 | Documentation | Mis en en place documentation | Création document principal | 12:00:00 | 12:15:00 |
| 02.02.2023 | 1 | Mise en place | Réception Fortinet | Réception, déballage et inventaire du matériel reçu | 13:40:00 | 14:00:00 |
| 02.02.2023 | 1 | Mise en place | Découverte du matériel | Lecture mode d'emploi et recherche documentation supplémentaire | 14:00:00 | 15:05:00 |
| 07.02.2023 | 2 | Mise en place | Prise de contact SIp | Préparation de la communication au SIp pour sortie sur Internet + récupération règles de sorties du CPNV + visite SIp | 13:30:00 | 14:15:00 |
| 07.02.2023 | 2 | Mise en place | Installation | Installation physique du Fortinet sur PC16 + cable management | 14:15:00 | 14:35:00 |
| 07.02.2023 | 2 | Mise en place | Découverte interface | Premiers pas, découverte interface | 14:35:00 | 15:05:00 |
| 07.02.2023 | 2 | Mise en place | Découverte interface | Premiers pas, reset complet du système | 15:20:00 | 15:55:00 |
| 07.02.2023 | 2 | Documentation | Journaux | Mise à jour des journaux | 15:55:00 | 16:05:00 |
| 08.02.2023 | 2 | Documentation | Documentation | Analyse préliminaire: introduction, objectifs | 10:45:00 | 11:15:00 |
| 08.02.2023 | 2 | Documentation | Documentation | Planification initiale | 11:15:00 | 12:15:00 |
| 09.02.2023 | 2 | Documentation | Documentation | Planification initiale | 09:50:00 | 12:15:00 |
| 09.02.2023 | 2 | Documentation | Discussion avec Mr. Varela | Avancée du projet, personne de contact, documentation à rendre. | 13:30:00 | 14:15:00 |
| 21.02.2023 | 3 | Analyse | Recherche documentation | Documentation de FortiOS ainsi que des différentes possibilités du FortiGate 80F | 13:30:00 | 16:05:00 |
| 22.02.2023 | 3 | Mise en place | Branchement et mise en route | Panne du FortiGate, dépannage, cause câble Ethernet RJ45 FG80F - PC05 défectueux, remplacé. | 10:40:00 | 11:20:00 |
| 22.02.2023 | 3 | Implémentation | Découverte | Recherche mode d'emplois et autres guides. | 11:20:00 | 12:15:00 |
| 22.02.2023 | 3 | Implémentation | Découverte | Renommage de l'hôte, création de compte admin Damien et tentatives infructueuses de création de LANs | 13:30:00 | 16:55:00 |
| 23.02.2023 | 3 | Documentation | Réorganisation documentation | Refonte total de la structure de fichier pour le projet, création des documents prévu pour l'entier du projet. Mise à jour du journal de travail | 09:50:00 | 11:00:00 |
| 23.02.2023 | 3 | Mise en place | Visionnage vidéo | Vidéo explicative de la gestion de base du FortiGate | 11:00:00 | 12:15:00 |
| 23.02.2023 | 3 | Documentation | Stratégie de test | Création du document de stratégie de test et définition de cette dernière | 13:30:00 | 15:05:00 |
| 28.02.2023 | 4 | Documentation | Reprise documentation | Tests, création glossaire, création manuel d'installation | 13:30:00 | 15:05:00 |
| 28.02.2023 | 4 | Implémentation | Problème | Impossible de se logger en temps qu'admin, impossible de mettre à zéro l'appareil via le bouton reset…complétement bloqué | 15:20:00 | 15:55:00 |
| 01.03.2023 | 4 | Implémentation | Solution | En branchant le Fortinet sur un autre pc, un des mots de passe essayé auparavant, fonctionne. Login: 'admin' pwd: 'Pa$$w0rd' | 10:40:00 | 11:30:00 |
| 01.03.2023 | 4 | Documentation | Documentation | Manuel d'installation | 11:30:00 | 12:15:00 |
| 01.03.2023 | 4 | Implémentation | Création d'un nouvel admin | Super admin login: 'DMA' pwd: '#1 Turing, Alan' créé | 15:20:00 | 15:40:00 |
| 01.03.2023 | 4 | Implémentation | Connexion via SSH | CMD SSH DMA@192.168.1.99 #1 Turing, Alan: succès! | 15:40:00 | 16:00:00 |
| 01.03.2023 | 4 | Implémentation | Création VLANs | VLAN\_100 (10.1.1.0) et VLAN\_200 (10.1.2.0) ont créés via CLI | 16:00:00 | 16:55:00 |
| 02.03.2023 | 4 | Implémentation | - | - | 09:50:00 | 12:15:00 |
| 02.03.2023 | 4 | Implémentation | - | - | 13:30:00 | 15:05:00 |
| 07.03.2023 | 5 | Absence | Présentation ES | Présentation des filières ES, présence obligatoire | 13:30:00 | 14:30:00 |
| 07.03.2023 | 5 | Documentation | - | Fin du protocole de test, préparation questions pour Mr. Jaggi, documentation | 14:30:00 | 16:05:00 |
| 08.03.2023 | 5 | Absence | Maladie | - | - | - |
| 09.03.2023 | 5 | Absence | Maladie | - | - | - |
| 14.03.2023 | 6 | Implémentation | Réalisation | Libération des ports, créations des sous-réseaux, mise en place DHCP, création adresses | 13:30:00 | 16:05:00 |
| 15.03.2023 | 6 | Implémentation | Règles de firewall | Tentative de création de règle de firewall, sans succès | 15:20:00 | 15:55:00 |
| 15.03.2023 | 6 | Analyse | Meeting avec LJI | Discussion avec Mr. Jaggi concernant sous-réseaux vs VLANs. Discussions sur les règles de firewall. | 15:55:00 | 16:30:00 |
| 15.03.2023 | 6 | Implémentation | Règle de firewall | Après correction d'une erreur grâce à la discussion avec Mr. Jaggi, une règle spécifique à un réseau a été implémentée avec succès | 16:30:00 | 16:55:00 |
| 16.03.2023 | 6 | Documentation | Réorganisation pour fin du projet | La partie conception étant finie, je dois planifier les deux semaines qu'il me reste pour finir le projet. | 09:50:00 | 12:15:00 |
| 16.03.2023 | 6 | Mise en place | Discussion avec Mr. Konutse | Mise au point projet | 13:30:00 | 13:45:00 |
| 16.03.2023 | 6 | Implémentation | Back-up configuration |  | 13:45:00 | 15:05:00 |
| 21.03.2023 | 7 | Implémentation | Maladie | - | - | - |
| 22.03.2023 | 7 | Implémentation | Test | Malade travail depuis la maison: mise à zéro du système + remise en place | 10:40:00 | 12:15:00 |
| 22.03.2023 | 7 | Implémentation | Test | Malade travail depuis la maison: mise à zéro du système + remise en place | 15:20:00 | 16:55:00 |
| 23.03.2023 | 7 | Implémentation | Mise à jour manuel d'installation | Test de toutes les procédures (création sous-réseau, rejoindre réseau, rejoindre internet, règles firewall), mise par écrit précise, et documentation | 09:50:00 | 12:15:00 |
| 23.03.2023 | 7 | Implémentation | Mise à jour manuel d'utilisation | Test de toutes les procédures (création sous-réseau, rejoindre réseau, rejoindre internet, règles firewall), mise par écrit précise, et documentation | 13:30:00 | 15:05:00 |
| 28.03.2023 | 8 | Documentation | Finissions |  | 13:30:00 | 16:05:00 |
| 29.03.2023 | 8 | Documentation | Mise en page |  | 10:40:00 | 12:15:00 |
| 29.03.2023 | 8 | Documentation | Mise en page |  | 13:30:00 | 16:05:00 |
| 30.03.2023 | 8 | Documentation | Présentation |  | 09:50:00 | 12:15:00 |
| 30.03.2023 | 8 | Documentation | Présentation |  | 13:30:00 | 15:05:00 |
|  |  |  |  |  | **Total** | **66:10:00** |

## Manuel d’Installation

1. Dans la boite



*Figure 8 Contenu de la boite*

1 câble alimentation T12 – C5

1 block d’alimentation

1 FortiGate 80F

1 Câble RJ 45

1 QuickStart Guide "FortiGate 80F Series"

1. Interfaces physique
   1. Front panel



*Figure 9 Front panel*

LEDs dans l'ordre de gauche à droite :

ON/OFF (non libellé, sur la gauche de l'inscription FortiGate 80F)

Statuts

HA 1 3 5 A WAN1 SFP1

POWER 2 4 6 B WAN2 SFP2

* 1. Back Panel

Une image contenant intérieur

Description générée automatiquement

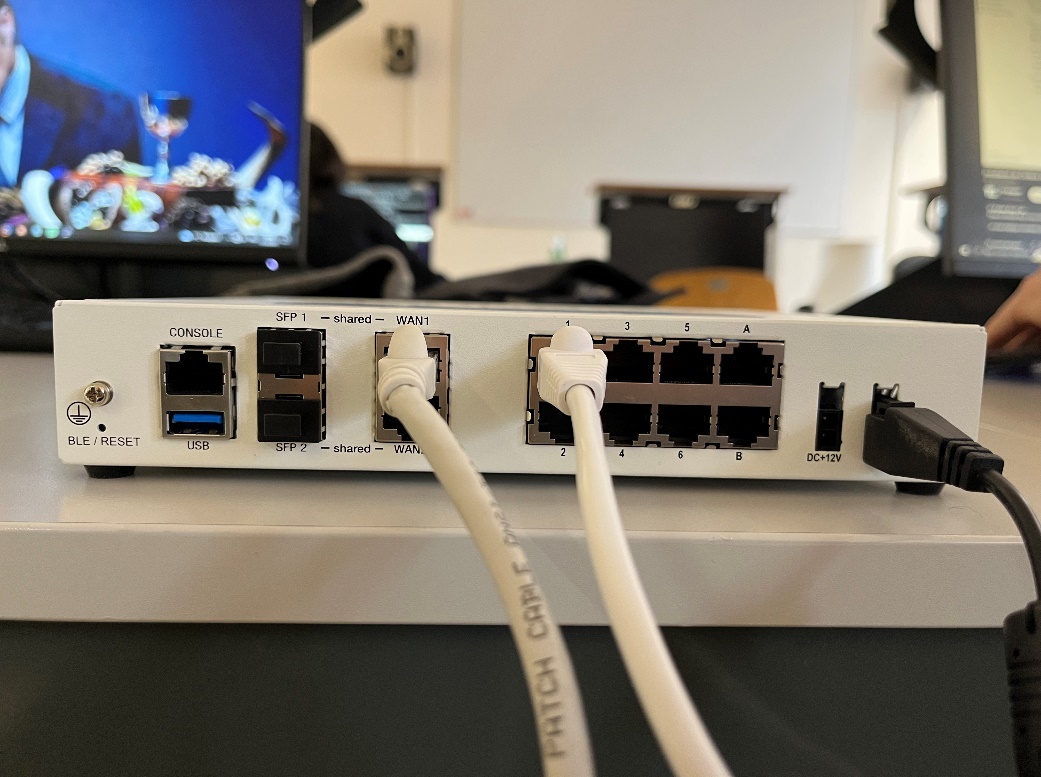
*Figure 10 Back panel*

Ports dans l'ordre de gauche à droite :

CONSOLESFP1 WAN1 1 3 5 A

BLE/RESET USB SFP2 WAN2 2 4 6 B DC+12V DC+12V

1. Connecter le FG 80F
2. Connecter le câble RJ45 de votre WAN dans la prise WAN1 du FG 80F.
3. Connecter un second câble RJ45 : dans un des ports 1-6 du FG 80 F, l'autre dans le port Ethernet de votre ordinateur.
4. Connecter le câble électrique et l’alimentation ensemble.
5. Connecter l’alimentation dans le FG 80F et le câble électrique dans la prise de courant



*Figure 11 Back panel branché.*

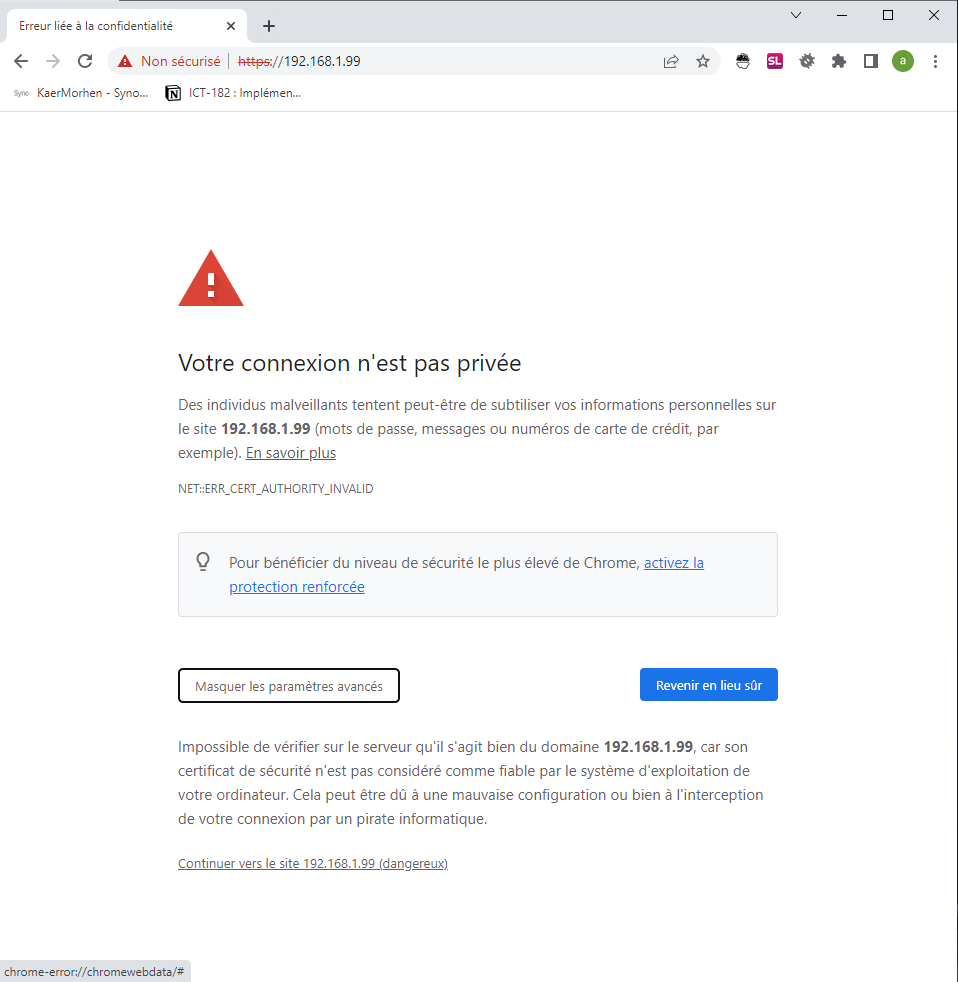
Le FG 80F va commencer sa séquence de boot, une fois qu’il sera accessible ses LEDs seront dans cette configuration suivante :



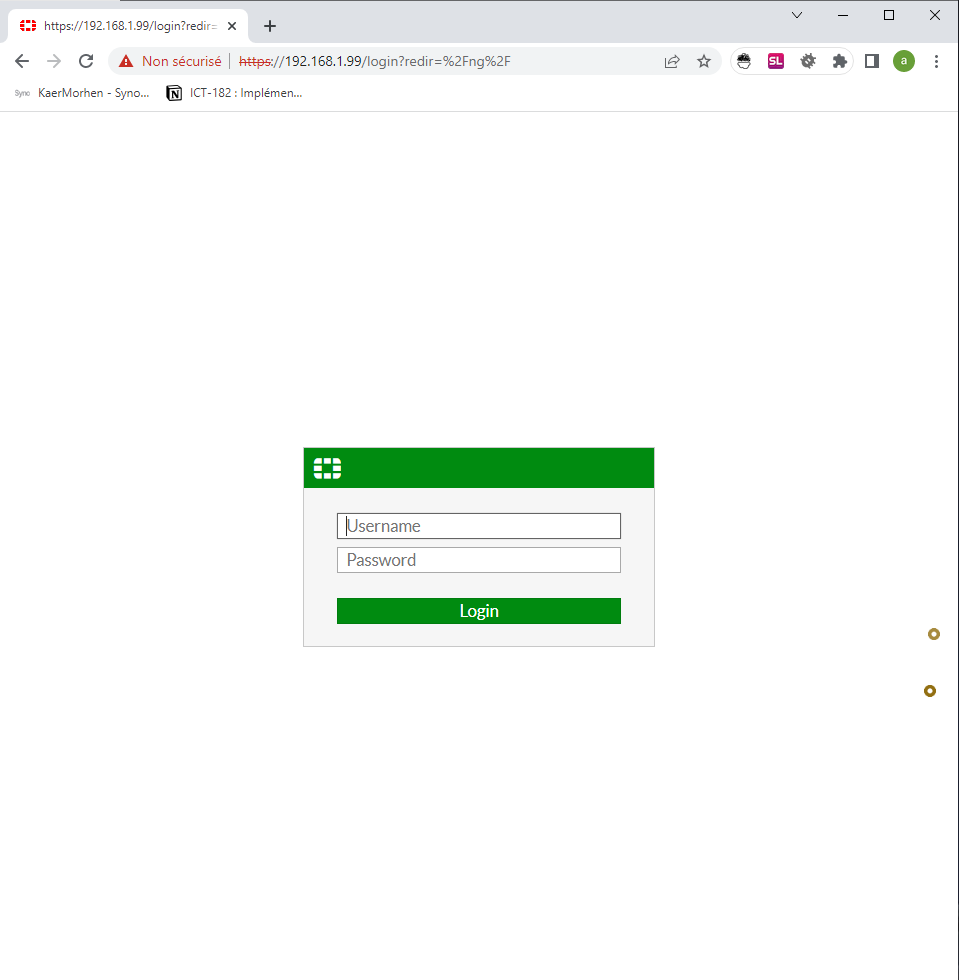
*Figure 12 LEDs de fonctionnement.*

1. Première connexion à l'interface graphique du FG 80F

Rentrer l’adresse 192.168.1.99 dans votre navigateur. Vous allez recevoir un message d’alerte, cliquer sur paramètres avancés et ensuite sur le lien ‘continuer vers le site 192.168.1.99 (dangereux).



*Figure 13 Alerte connexion*

Lorsque votre pare-feu est branché correctement, vous devriez arriver à cette page de connexion.

*Figure 14 Bienvenue dans l'interface graphique de votre pare-feu Fortinet*

## Manuel d’Utilisation

1. Mise à zéro de l'appareil

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

* 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 a une fréquence accélérée puis relâcher le bouton reset

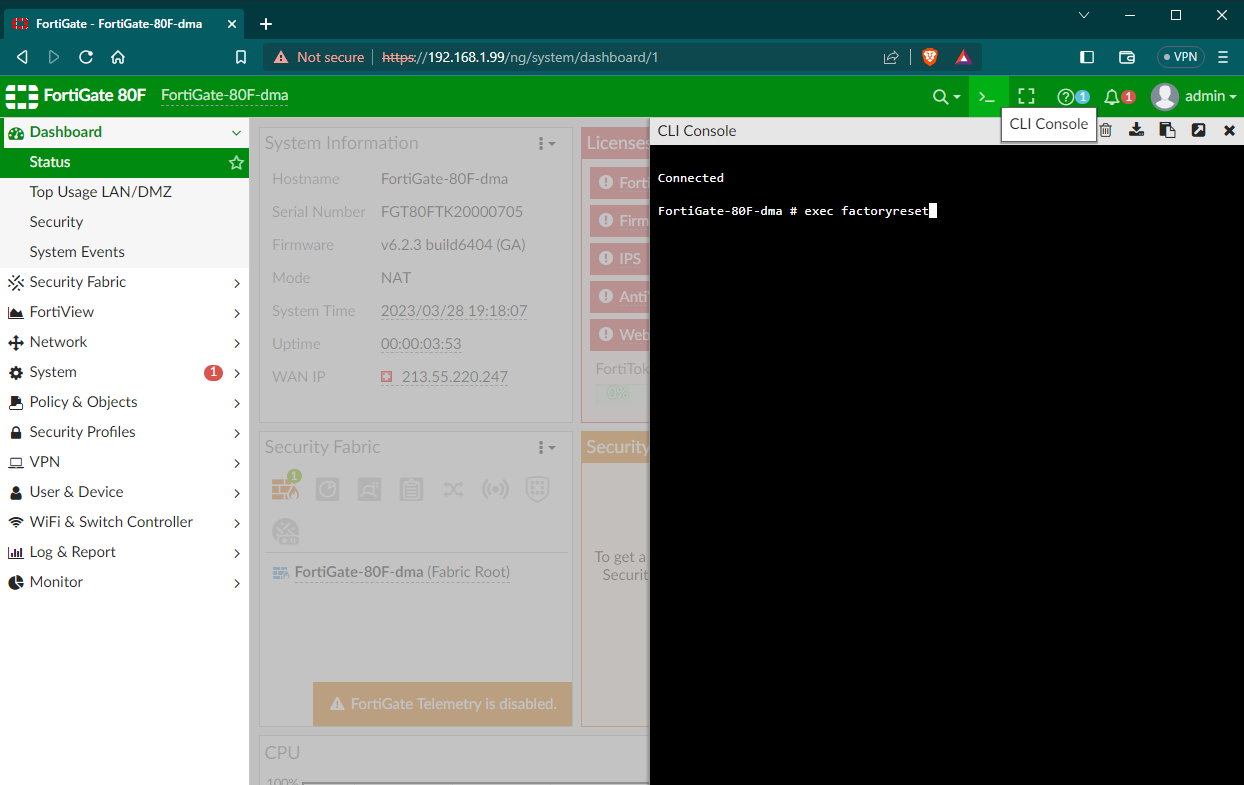
Une image contenant texte, intérieur

Description générée automatiquement

*Figure 15 Bouton reset.*

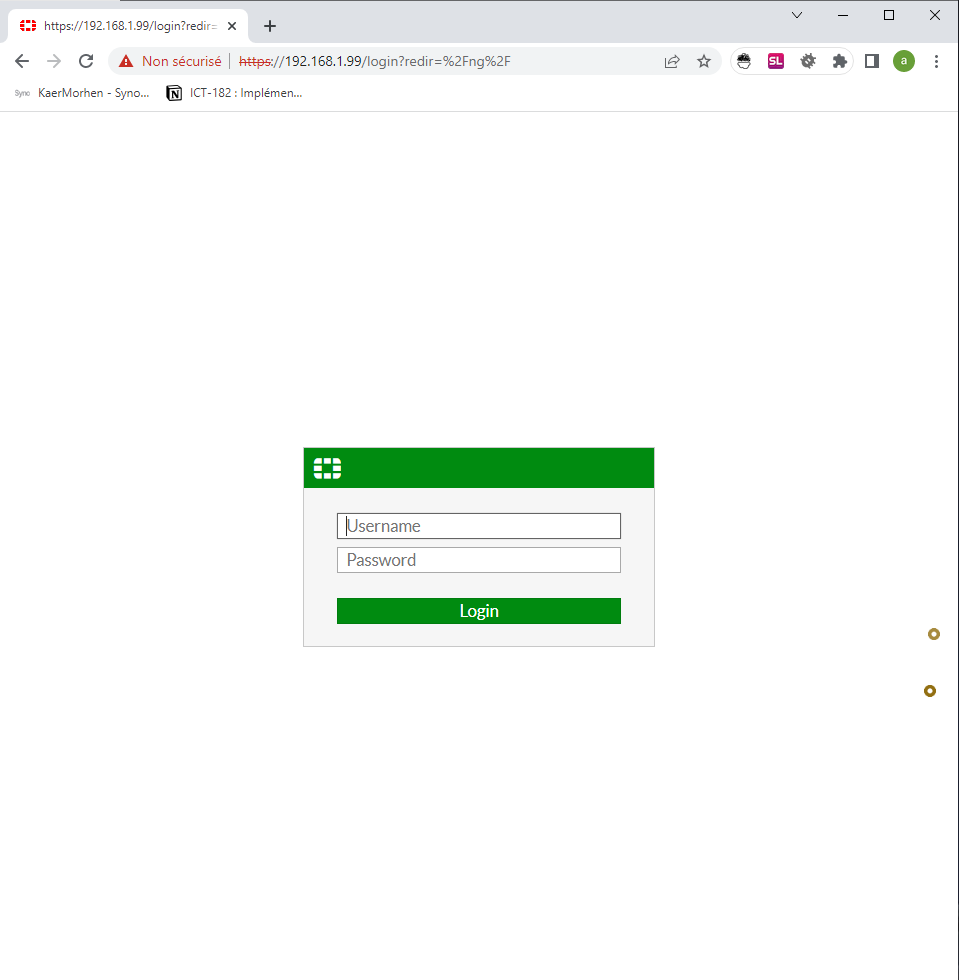
* 1. Via CLI

Ouvrir la ligne de commande

Taper la commande suivante : # exec factoryreset

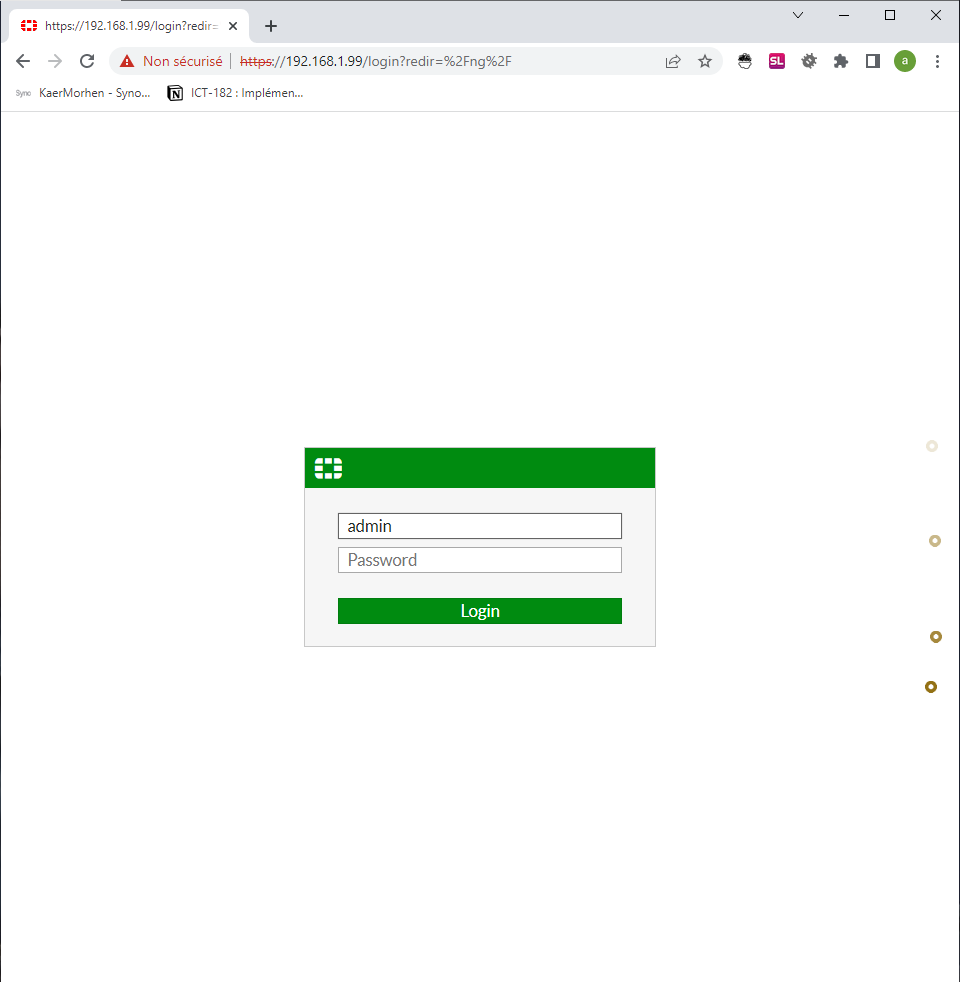
*Figure 16 Ouvrir la console CLI et effectuer le reset.*

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



*Figure 17 Login vide.*

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



*Figure 18 Login pour première connexion.*

1. Changer le mot de passe

Une image contenant table

Description générée automatiquement

*Figure 19 Changement de mot de passe lors de la première connexion.*

1. Vous voilà dans le dashboard

Une image contenant table, calendrier

Description générée automatiquement

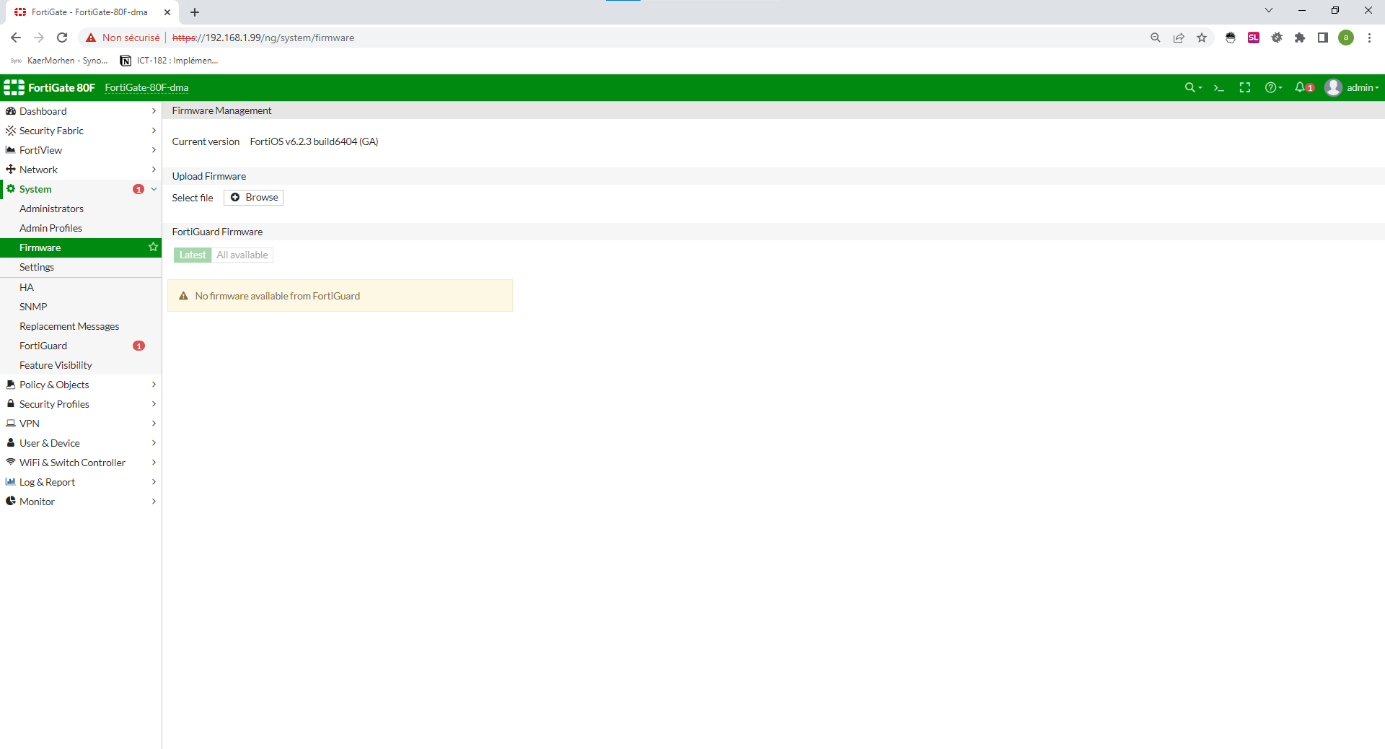
*Figure 20 Dashboard.*

1. Appropriation
   1. Définition

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

* 1. Mise à jour du Firmware

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

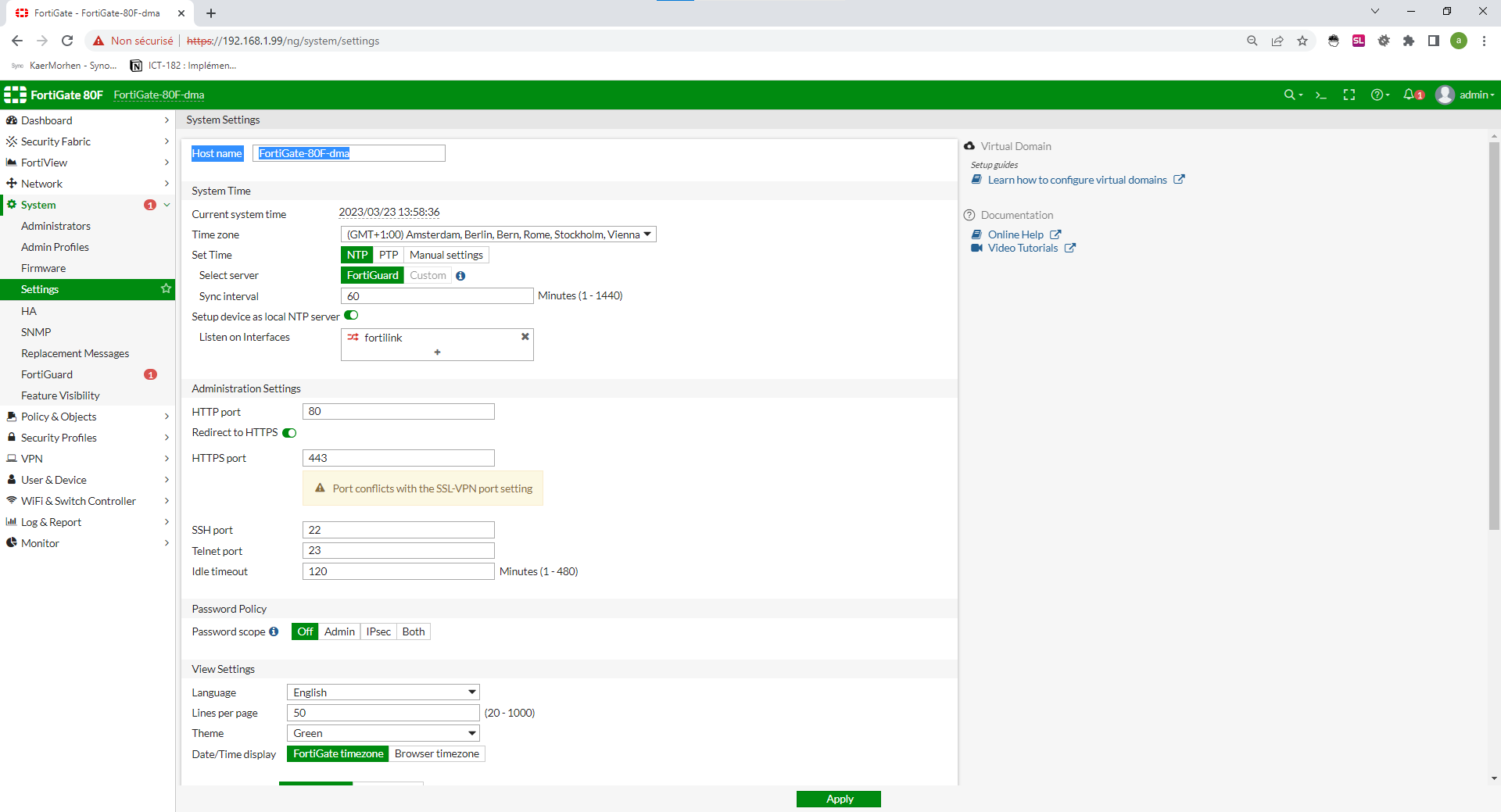


*Figure 21 Mise à jour du firmware.*

* 1. 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 22 Changement host name & fuseau horaire.*

* 1. 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 23 Création nouvel administrateur.*

* 1. 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.

1. Networking

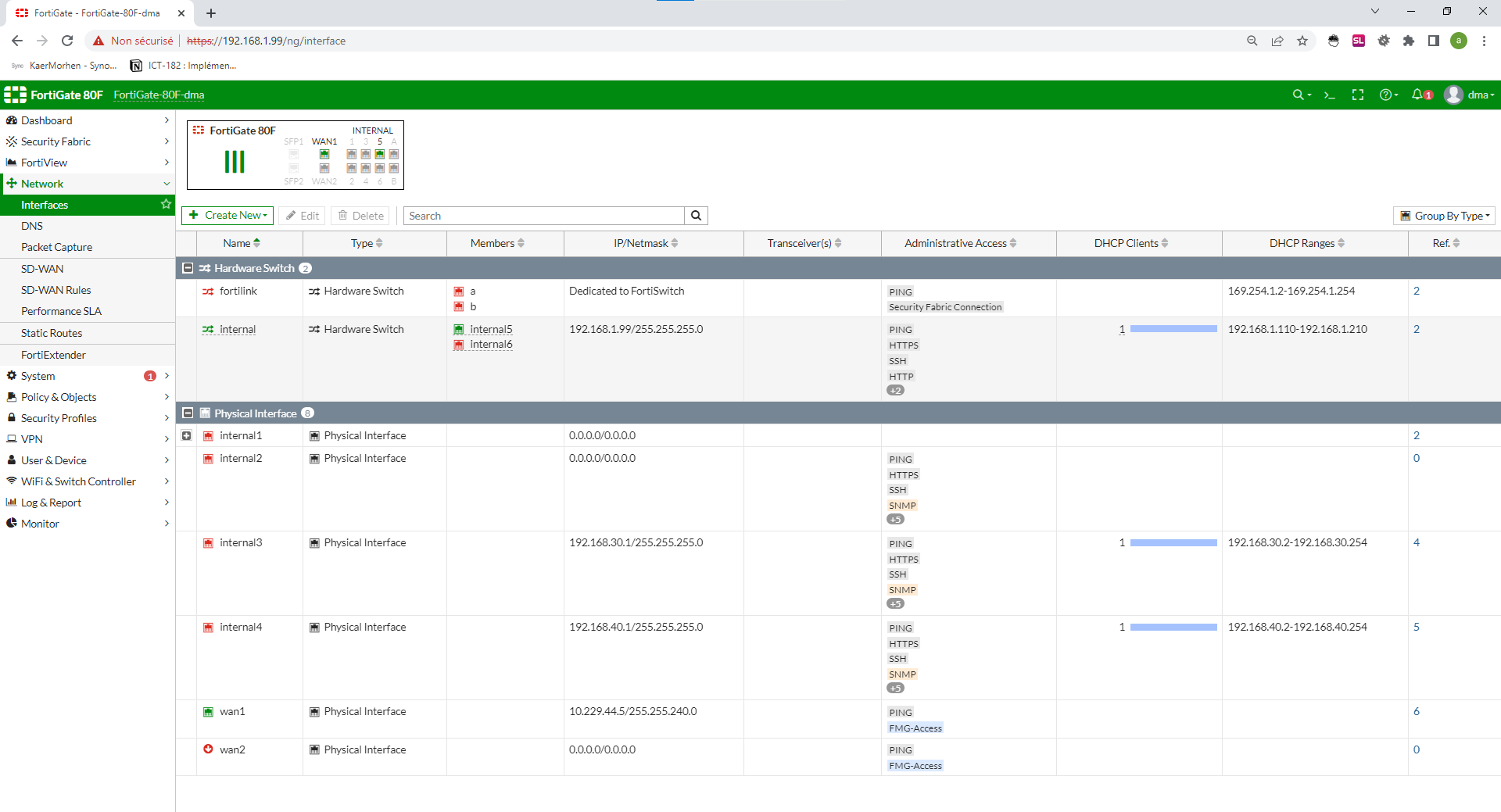
Dans cette partie nous allons créer des VLANs et/ou des sous-réseaux

* 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

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



*Figure 24 Libération des ports.*

* 1. 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 25 Créer une interface VLAN.*

Une image contenant texte

Description générée automatiquement

*Figure 26 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

* 1. 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*

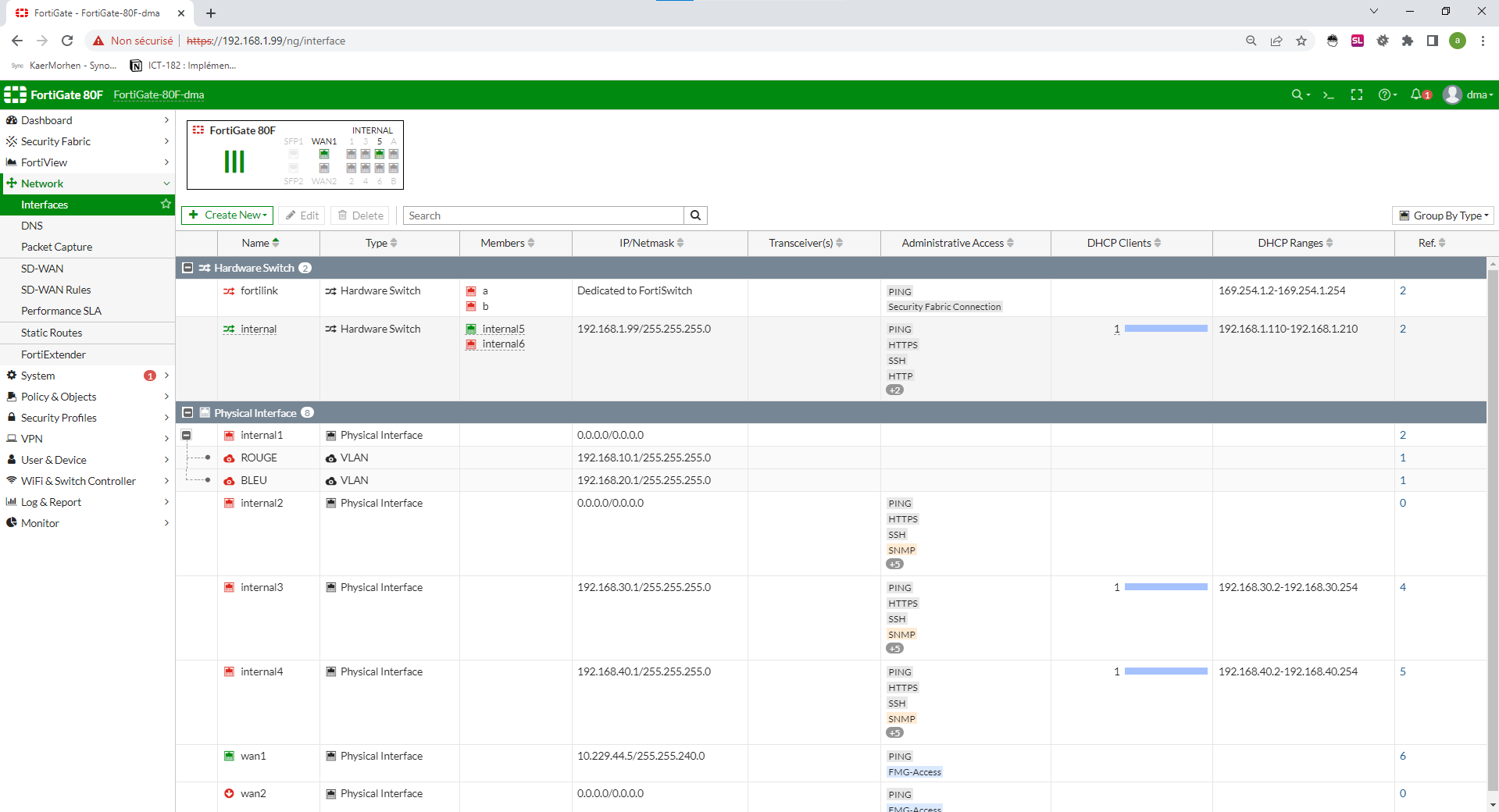
*Outbound shaping profile: off*

*Comments: création sous-réseau sur port3 dma*

*Status: Enabled*

1. Cliquer sur OK

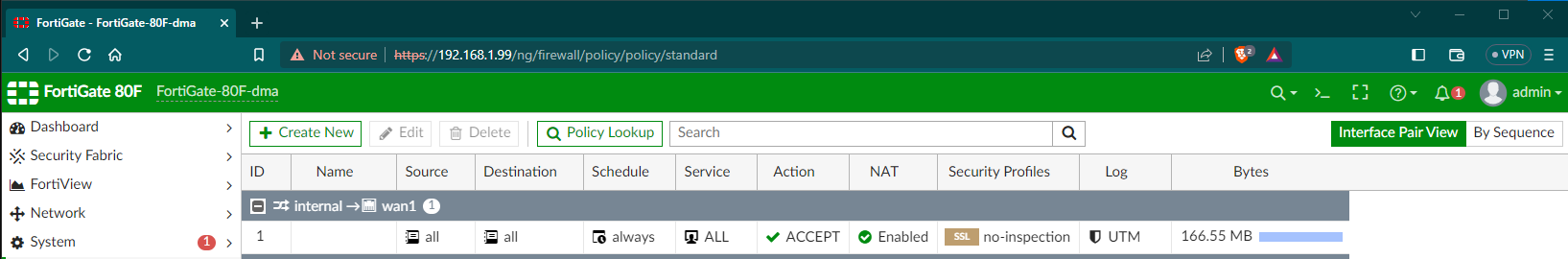
Nous venons de donner à l'interface internal3 une adresse IP et un masque de sous-réseau 192.168.30.1/24, ainsi qu'en activant la fonction DHCP, nous lui donnons la faculté de distribuer des adresses IP aux machines connectées, sur la plage 192.168.30.2-192.168.30.254.



*Figure 27 Création sous-réseau internal3.*

1. 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 28 Les ports sur l'interface internal ont accès au WAN étant donné la configuration de base.*

1. Règles de pare-feu
   1. Création des adresses
2. Policy & Objects -> Addresses -> Create New -> Address
3. *Name: Sous-Réseau3*

*Color: orange*

*Type: Subnet*

*IP/Netmask: 192.168.30.0/24*

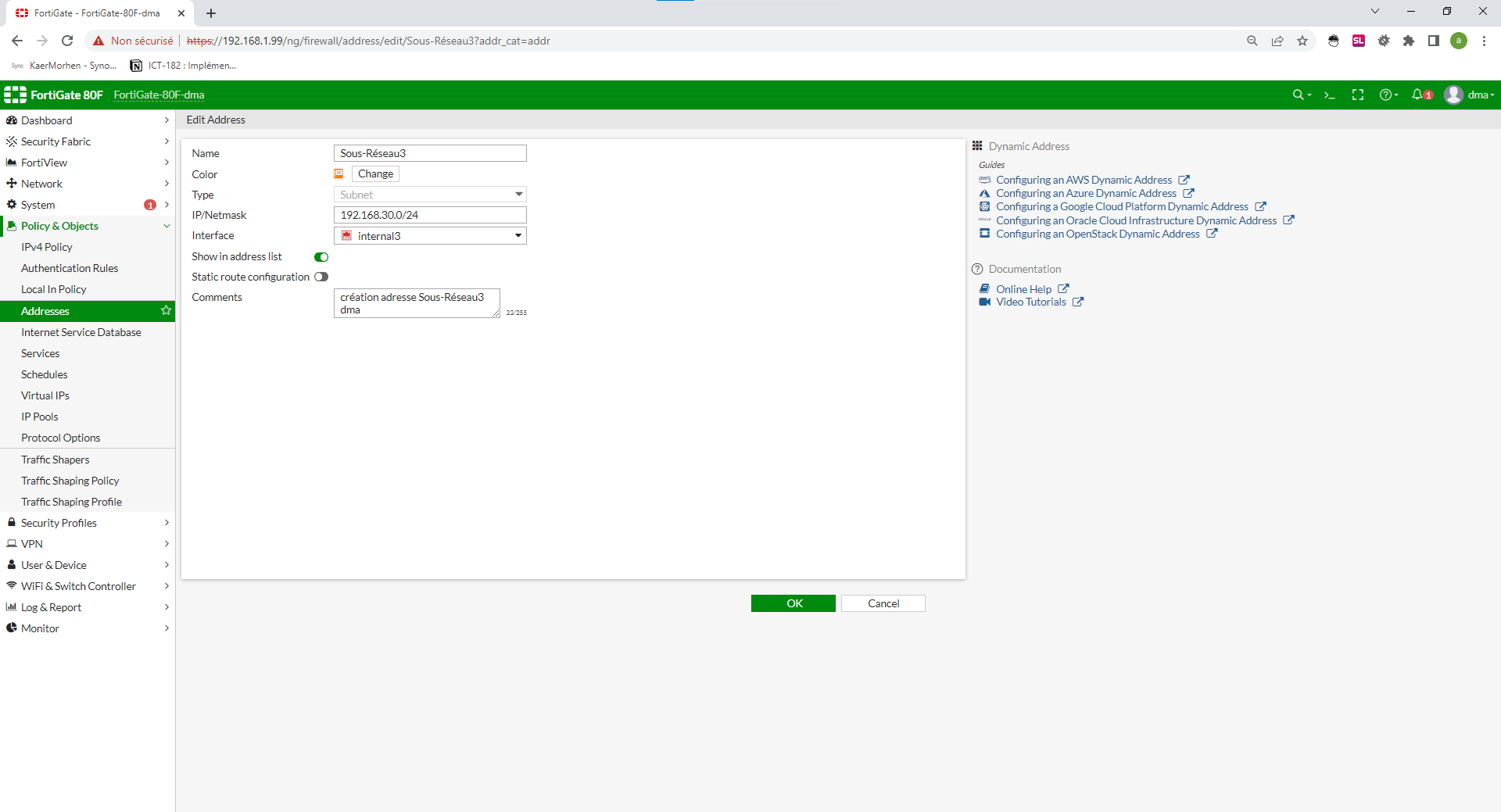
*Interface: internal3*

*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 29 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*

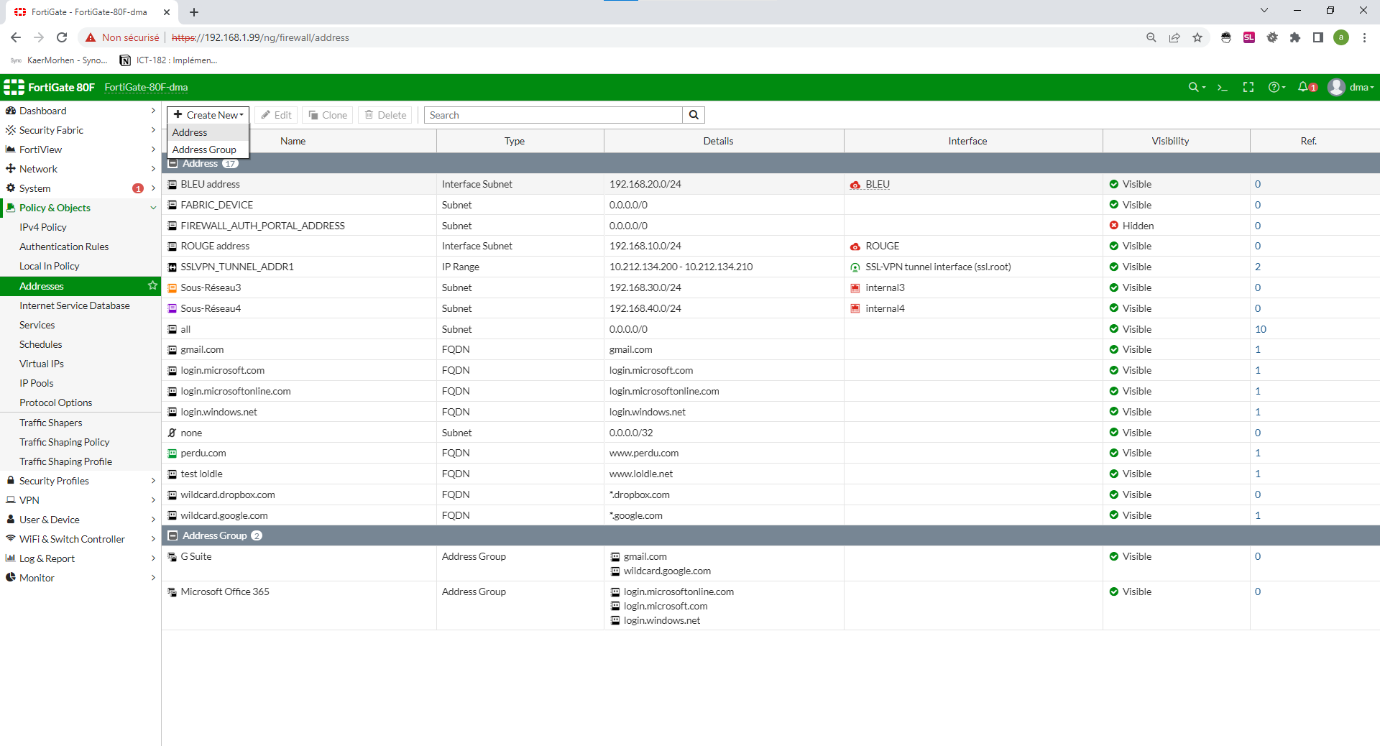
1. Cliquer sur OK

Une image contenant texte

Description générée automatiquement

*Figure 30 Création adresse perdu.com.*

Récapitulatif des adresses crées.



*Figure 31 Récapitulatif des adresses crées.*

* 1. 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*

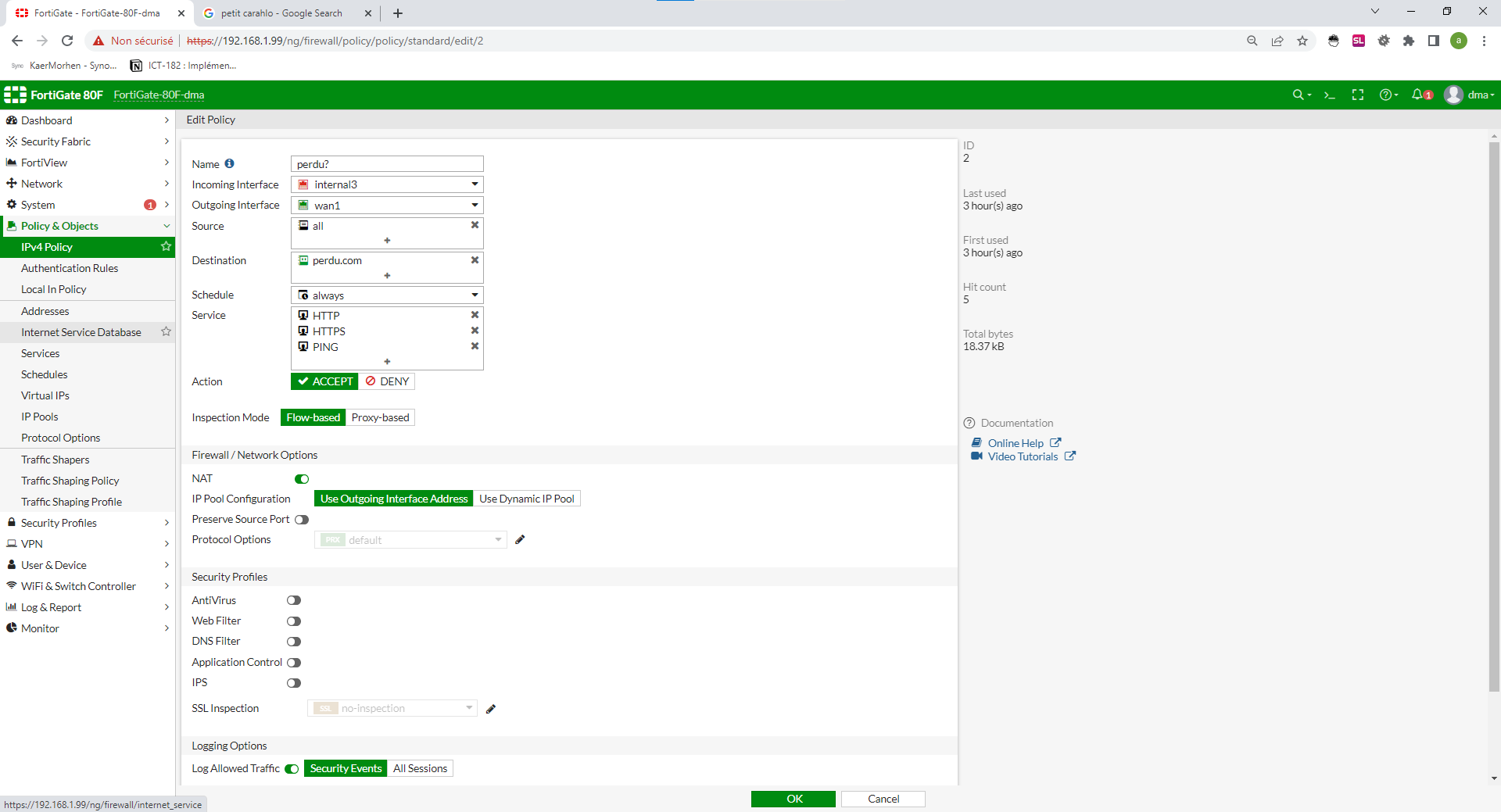
*SSL Inspection: no-inspection*

*Log Allowed Traffic: Security Events*

*Comments: création règle perdu.com dma*

*Enable this policy: on*

1. Cliquer sur OK



*Figure 32 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*

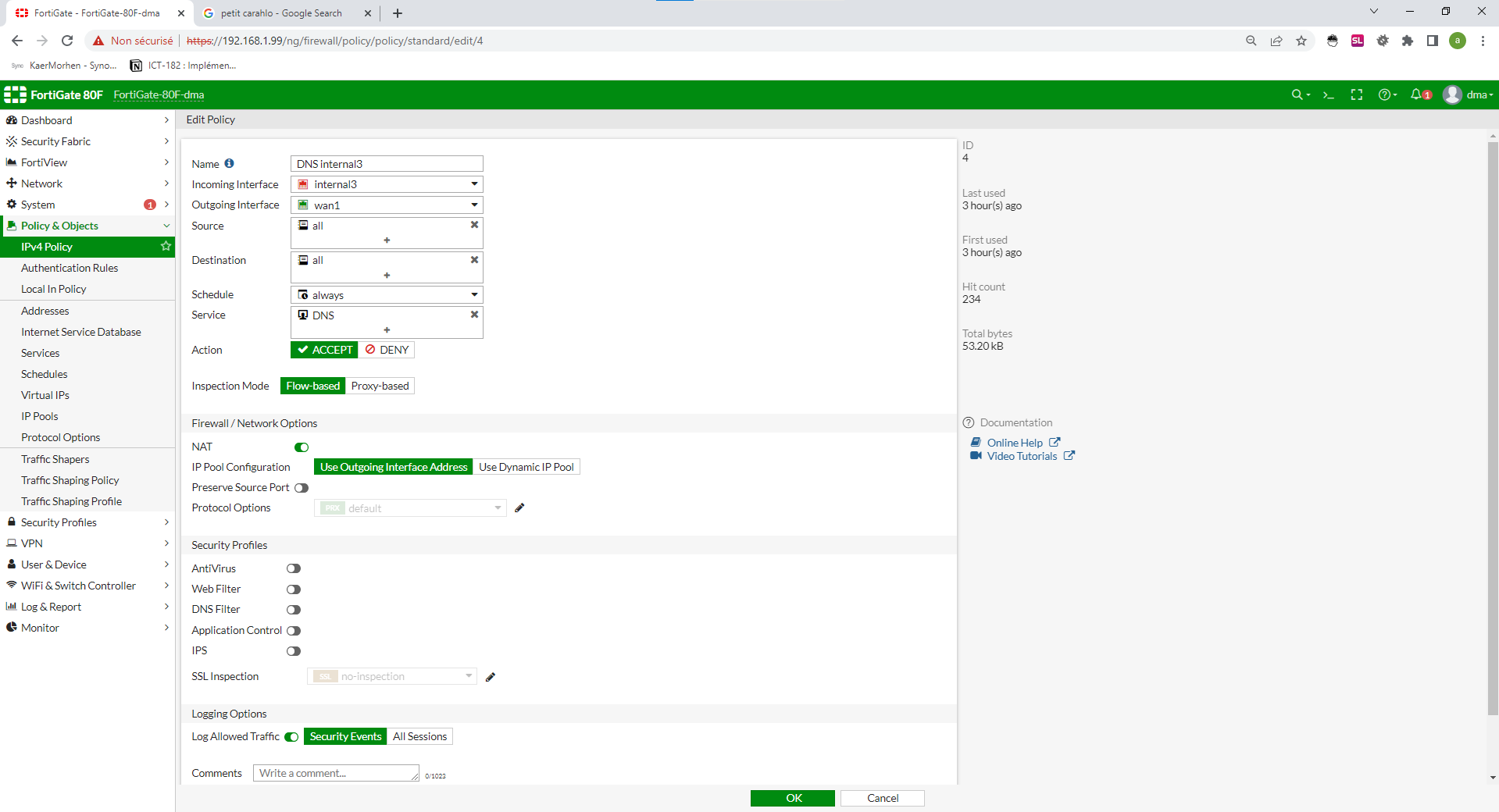
*SSL Inspection: no-inspection*

*Log Allowed Traffic: Security Events*

*Comments: création règle dns dma*

*Enable this policy: on*

1. Cliquer sur OK



*Figure 33 Règle accès DNS sur interface internal3.*

Récapitulatif des règles:

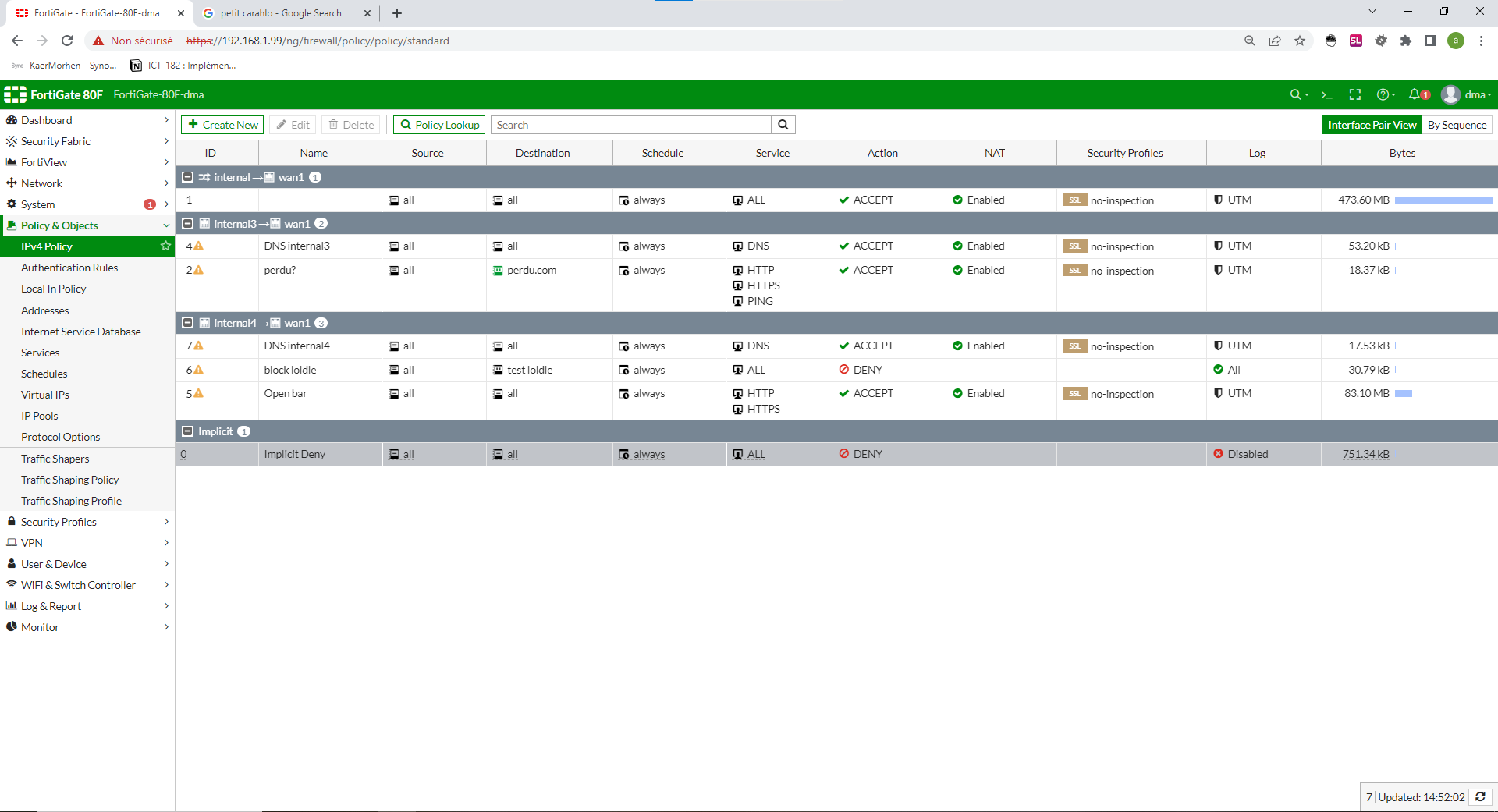


Figure 34 Ensemble des règles crées pour différents tests.

## Manuel de tests

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **N°** | **Nom du test** | **But du test** | **Description du test** | **Résultat attendu** | **Status** | **Problème possible** |
| 1 | LEDs Party | Vérifier que l'appareil est bien branché | Brancher le FortiG 80F selon manuel d'installation | LEDs ON/OFF, STATUS, POWER, WAN1 et les ports allumés |  | - |
| 2 | Mise à zéro de l'appareil | Vérifier que l'appareil a bien été mis à zéro | Au login, entrer "admin" et " " | Demande du système d'un changement de mot de passe |  | - |
| 3 | Adresse IP venant de pare-feu | Vérifier que le PC recoive bien une adresse ip du pare-feu | Faire un ip config et recevoir une adresse du pare-feu | Adresse IP en 192.168.1.XX |  | - |
| 4 | Atteindre le GUI | Vérifier la connexion au GUI du pare-feu | Se logger en tant qu'admin avec le mdp mis lors du test 2 | Login réussi, accès au dashboard |  | - |
| 5 | Mise à jour du Firmware | Mettre à jour FortiOS | Dans System -> Firmware: Update Firmware | Changement d'OS pour une version plus récente |  | Abonnement nécessaire |
| 6 | Changement hostname - date | Vérifier que les changements effectués sont pris en compte | Se logger au GUI et vérifier sur la page Dashboard -> Status | Les deux changements sont visible |  | - |
| 7 | Nouvel administrateur | Vérifier que le nouvel admin peut se logger | Se logger au GUI avec les infos de l'admin créé | Login réussi |  | - |
| 8 | Accès à internet | Vérifier que l'on a une connexion au WAN | Ouvrir un browser et tester www.lematin.ch | On réussi à atteindre le site |  | - |
| 9 | Libération des interfaces | Vérifier que les interfaces physique choisi sont disponibles. | Aller dans Network Interfaces et controller le contenu de Physical Interfaces | On doit y trouver les internal1-4 libéré |  | - |
| 10 | Création de VLAN | Vérifier que la VLAN a bien été créé | Aller dans Network Interfaces Internal1 et vérifier si un VLAN s'y trouve | Le VLAN ROUGE est visible |  | - |
| 11 | VLAN utilisable | Vérifier que le VLAN créé peut se faire attribuer un port physique | - | - |  | Switch manageable nécessaire |
| 12 | Création de sous-réseaux | Vérifier que le sous-réseaux a bien été créé | Aller dans Network Interfaces et vérifier si internal3 s'y trouve | internal3 possède IP/netmask, Admin Access et DHCP Range |  | - |
| 13 | Attribution d'interface | Vérifier que l'interface libérée au test 9 est disponible | Créer une nouvelle adresse et pouvoir lui attribuer l'interface3 | Internal3 est disponible dans le menu déroulant d'Interface |  | - |
| 14 | Connexion à internet sur internal3 | Tester si il est possible de se connecter sur ce port | Ouvrir un browser et tester www.lematin.ch | Connexion doit échouer |  | - |
| 15 | Création d'adresse pour internet | Vérifier qu'il est possible d'accéder au site dont l'adresse a été crée | Ouvrir un browser et tester www.perdu.com | On doit pouvoir se connecter au site perdu.com |  | Pas de DNS |
| 16 | DNS? | Vérifier que le problème du test 15 est bien lié au DNS | Ouvrir un browser et tester de ping 104.21.5.178 | Pinger doit réussir |  | - |
| 17 | Création DNS | Vérifier que la règle DNS permettent d'atteindre www.perdu.com | Ouvrir un browser et tester www.perdu.com | On doit pouvoir se connecter au site perdu.com |  | - |
| 18 | Uniquement perdu.com | Vérifer que seul l'accès à perdu.com est possible | Ouvrir un browser et tester www.lematin.ch | On ne doit pas pouvoir se connecter au matin.ch |  | - |
| 19 | Règle Open bar | Tester l'inverse qu'internal3: accès à tous les sites | Ouvrir un browser et tester un site internet au hasard | On doit pouvoir se connecter à n'importe quel site |  | - |
| 20 | Règle block loldle | Tester qu'il est possible de bloquer un site bien précis | Ouvrir un browser et tester l'accès à loldle.net | On ne doit pas pouvoir se connecter se connecter à loldle.net |  | - |
| 21 | Règles similaire CPNV | Tester si il est possible d'utiliser un filtre web | Essayer d'aller sur www.jeuxvideo.com | On ne doit pas pouvoir s'y connecter |  | Pas de FortiGuard |
| 22 | Switch | Vérifier la bonne connexion entre le pare-feu et un switch | Brancher un PC non sur le pare-feu directement mais sur le switch | On doit être connecté au réseau correspondant |  | - |
| 23 | DHCP | Vérifier que toutes les machines sur le réseau recoivent une adresse IP | Brancher deux pc sur le switch du test 23 | Les deux PCs doivent recevoir des adresses IP |  | - |

1 LEDs Party

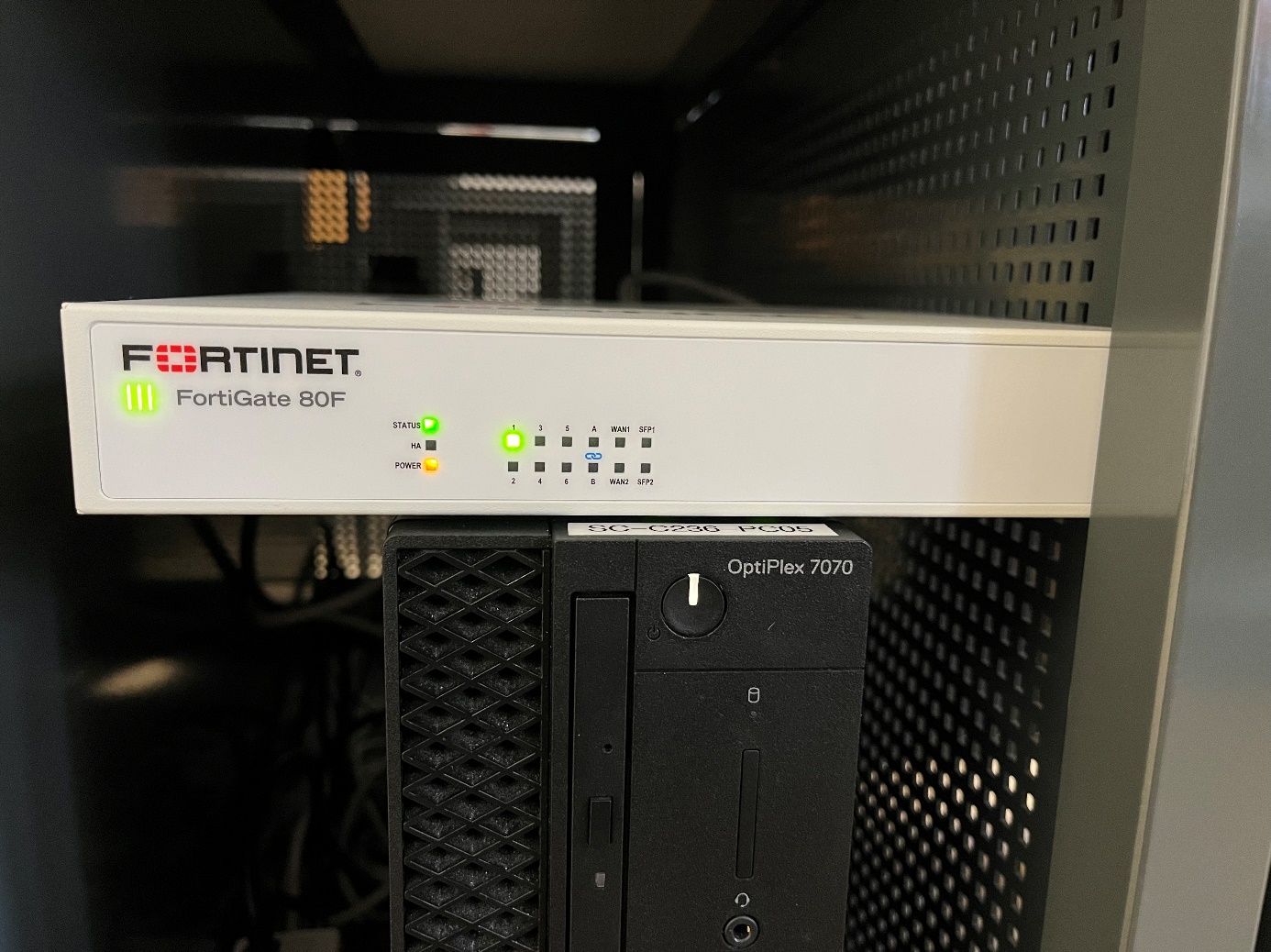


Figure 35 LEDs du FG 80F fonctionel

2 Mise à zéro de l'appareil

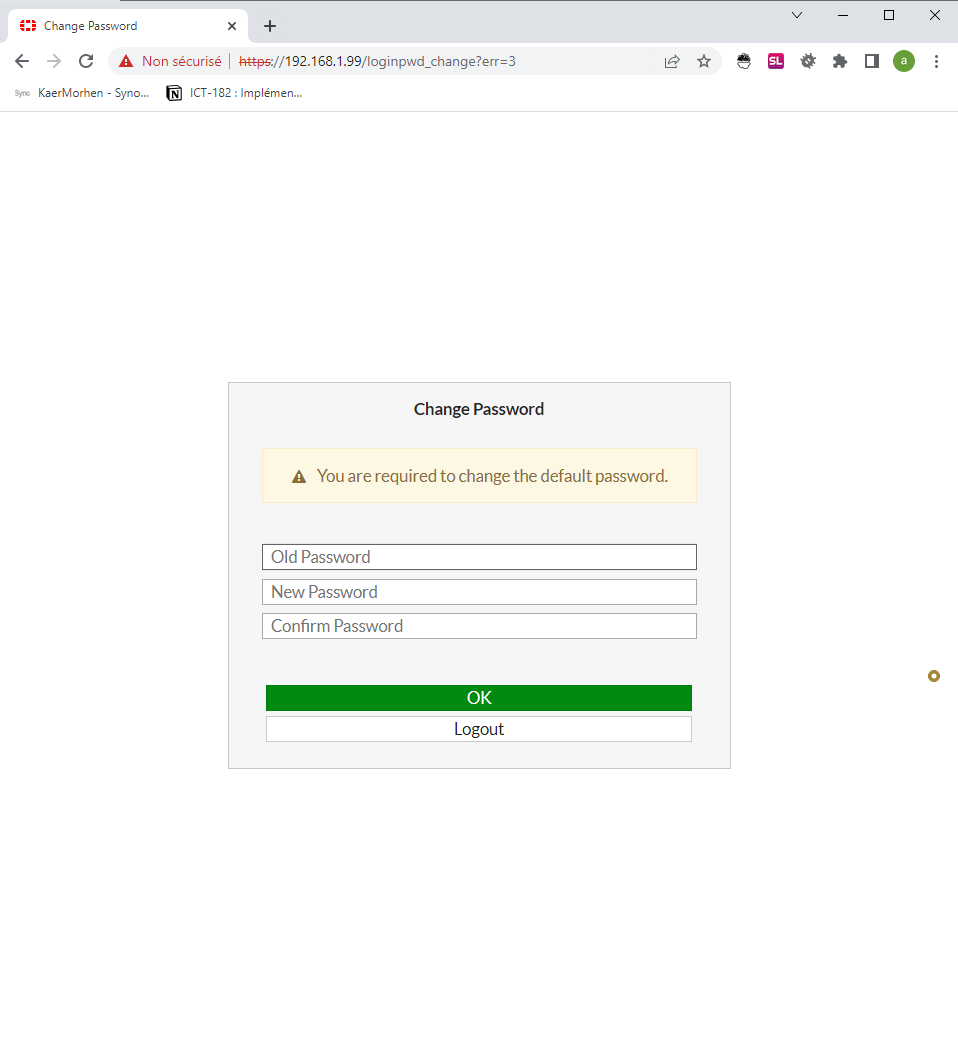


Figure 36 Changement de mot de passe obligatoire

3 Adresse IP venant de pare-feu

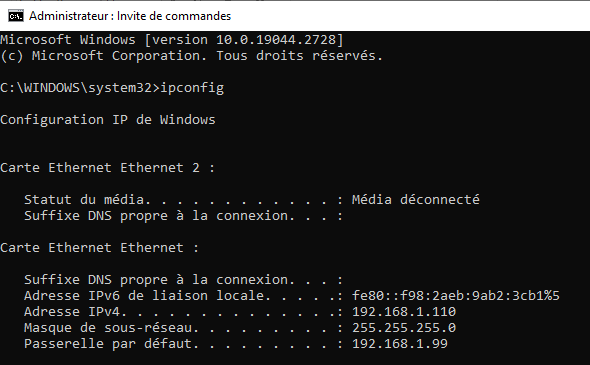


Figure 37 ipconfig

4 Atteindre le GUI

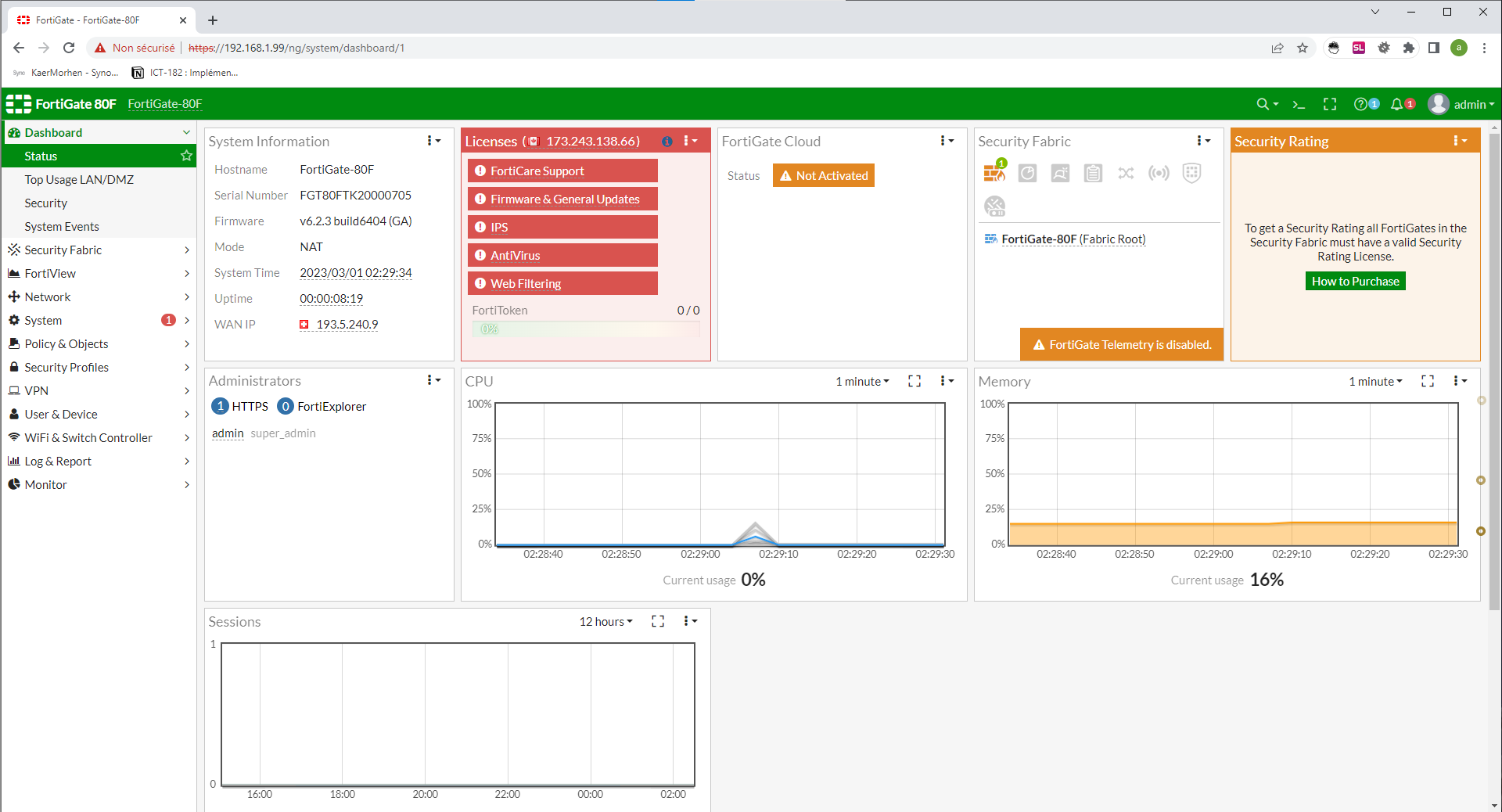


Figure 38 GUI FortiOS

5 Mise à jour du Firmware

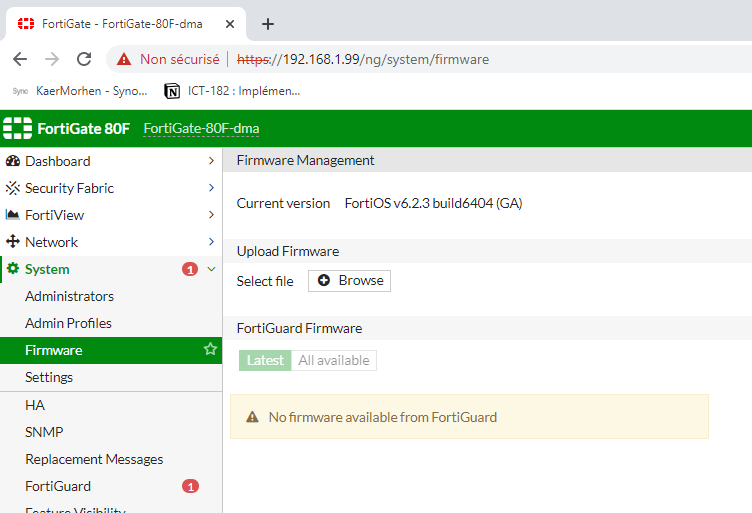


Figure 39 Mise à jour Firmware

6 Changement hostname – date



Figure 40 Dashboard FortiOS System Information

7 Nouvel administrateur

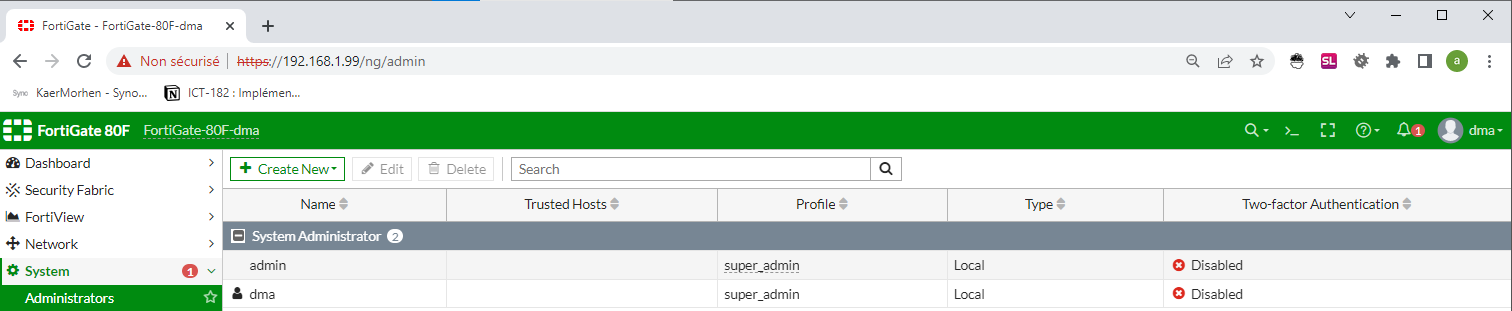


Figure 41 Nouvel administrateur

8 Accès à internet

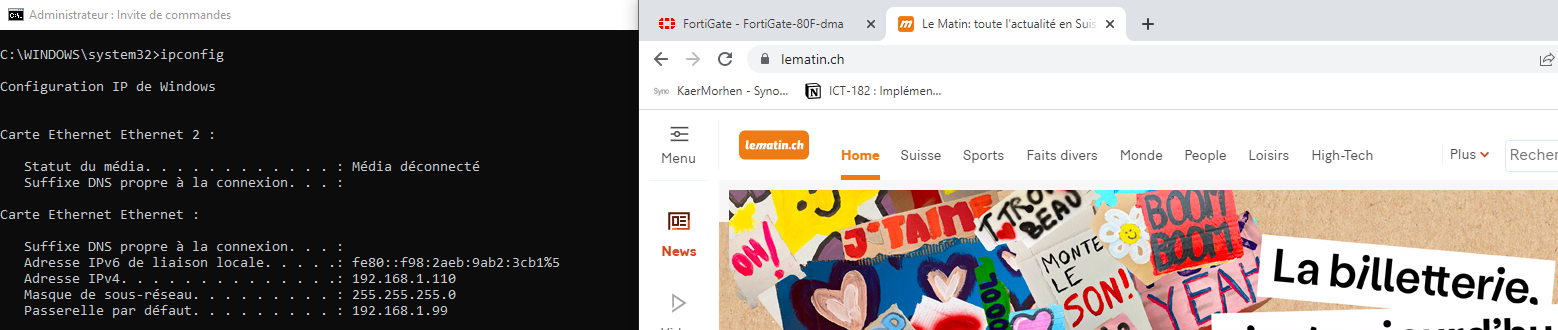


Figure 42 Accès à internet

9 Libération des interfaces

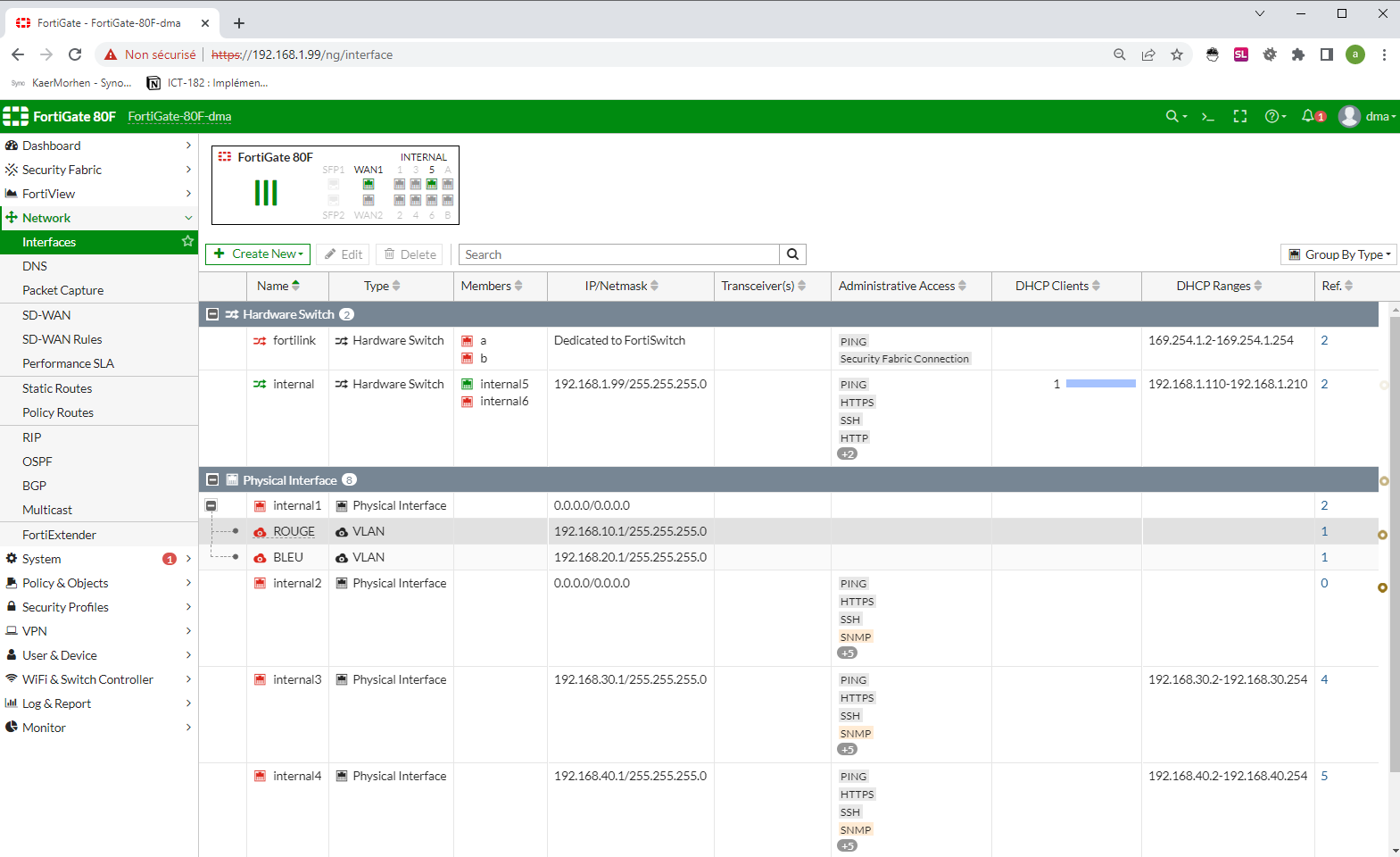


Figure 43 Libération des interfaces

10 Création de VLAN

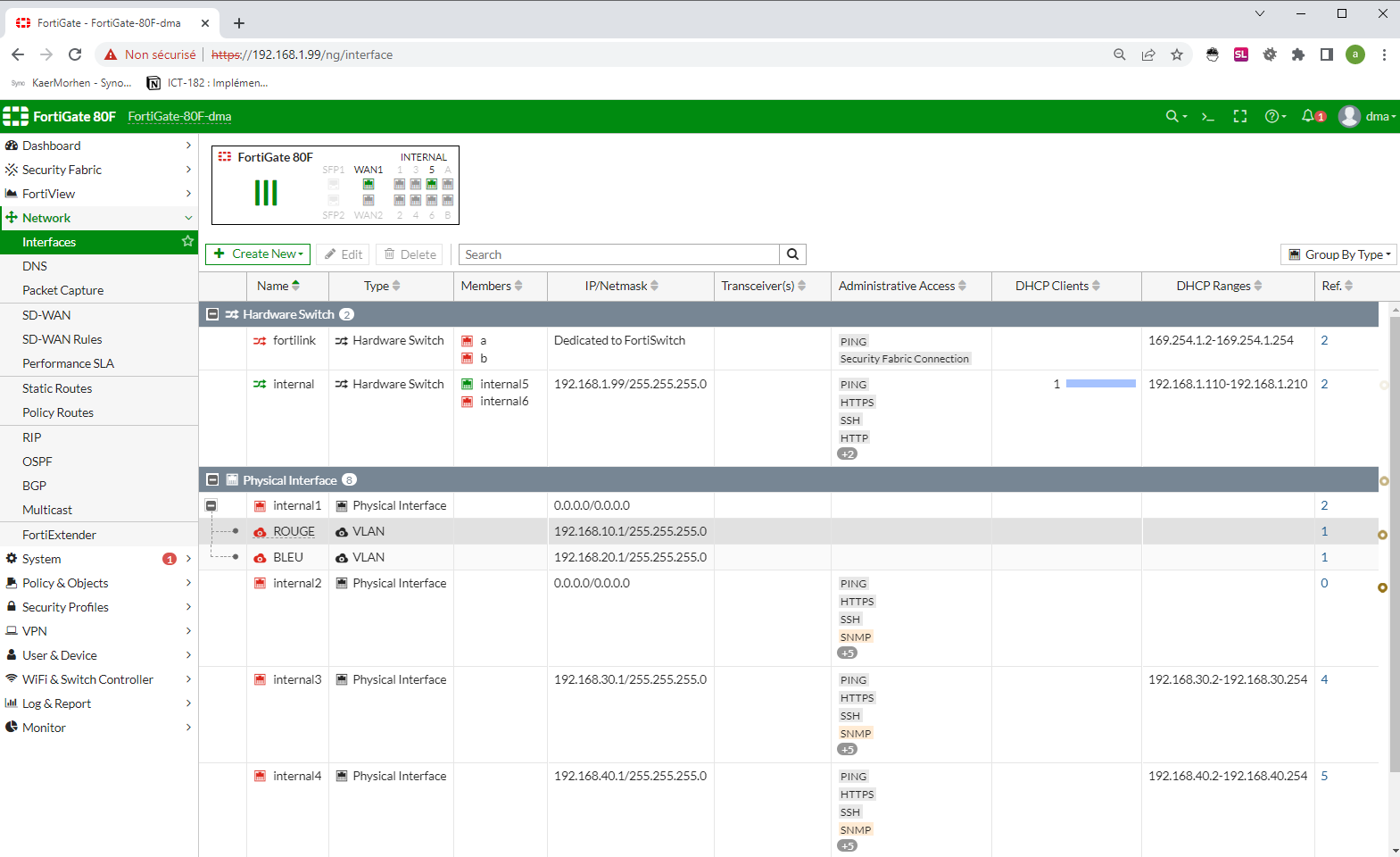


Figure 44 Création de VLAN

11 VLAN utilisable

Pas d'illustration

12 Création de sous-réseaux

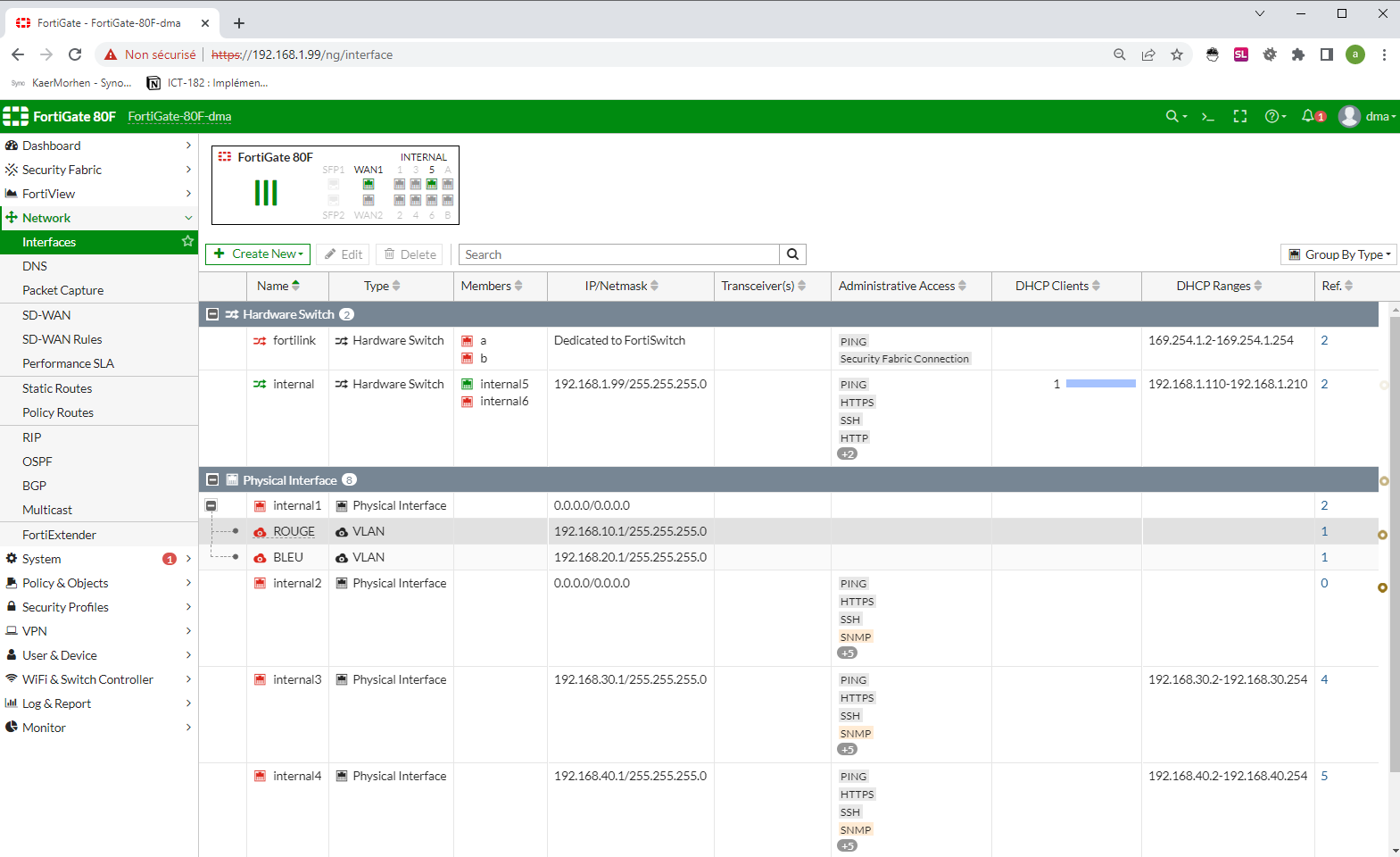


Figure 45 Création de sous-réseaux

13 Attribution d'interface

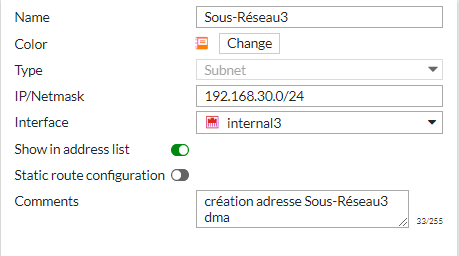


Figure 46 Attribution d'interface

14 Connexion à internet sur internal3

Pas d'illustration

15 Création d'adresse pour internet

Pas d'illustration

16 DNS?

Pas d'illustration

17 Création DNS

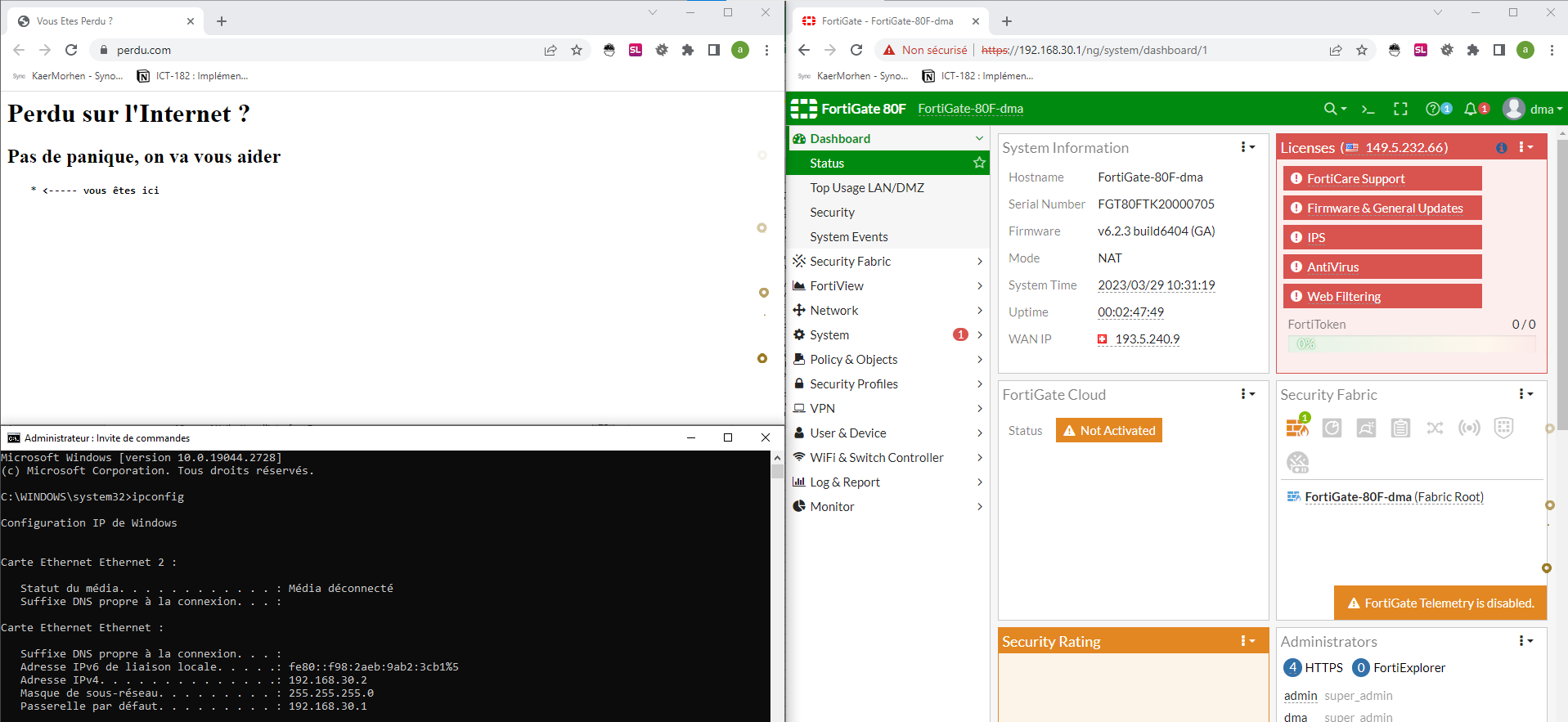


Figure 47 Création règle DNS

18 Uniquement perdu.com

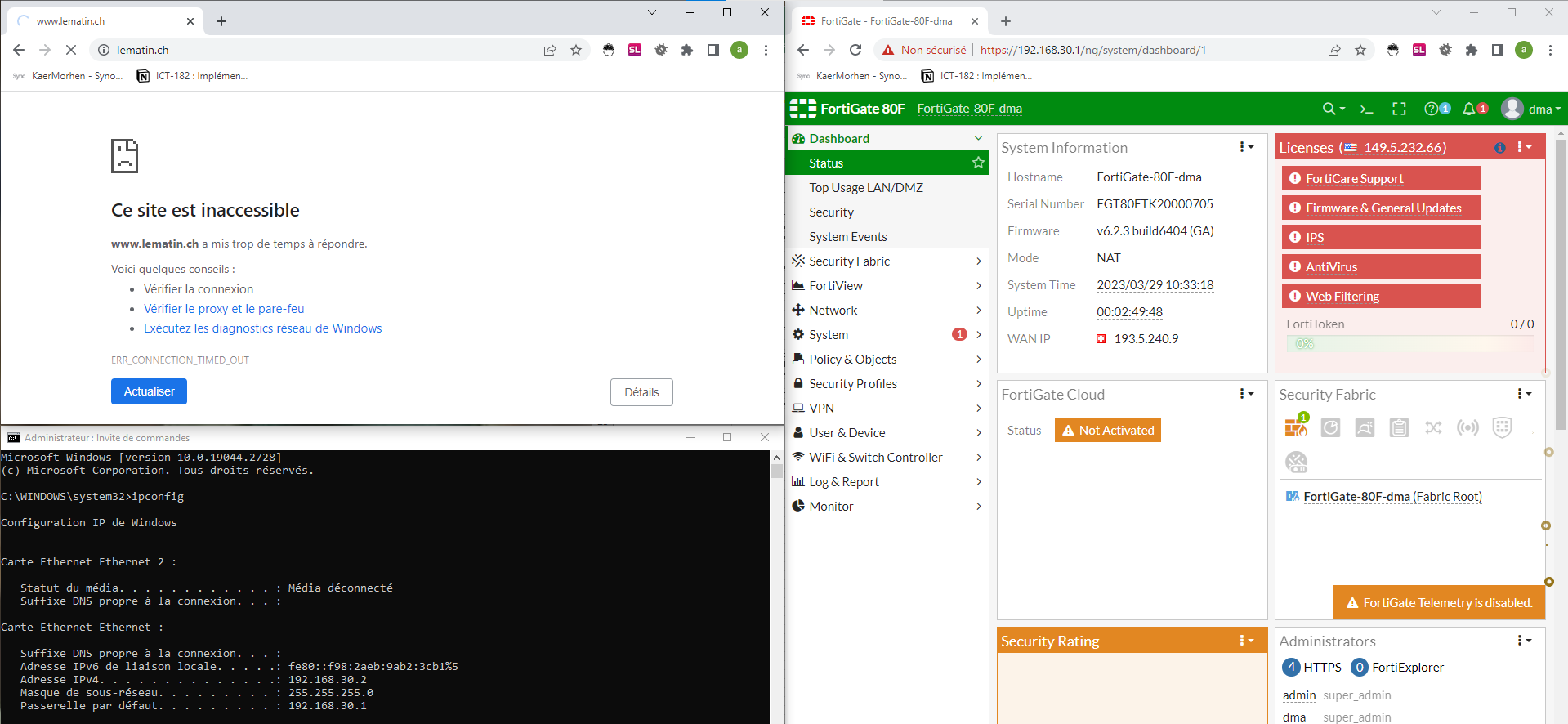


Figure 48 Accès uniquement à perdu.com

19 Règle Open bar

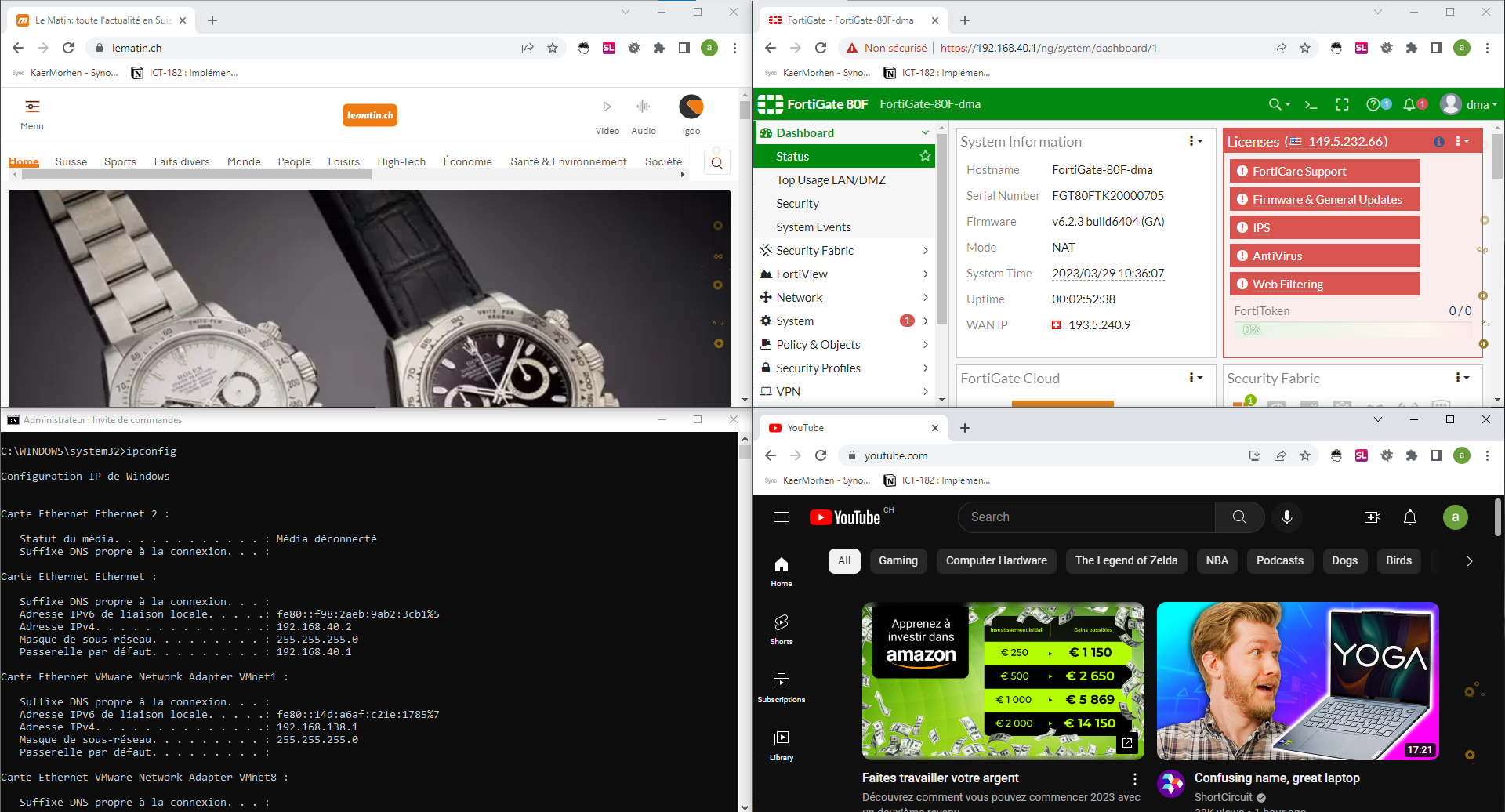


Figure 49 Règle Open bar

20 Règle block loldle

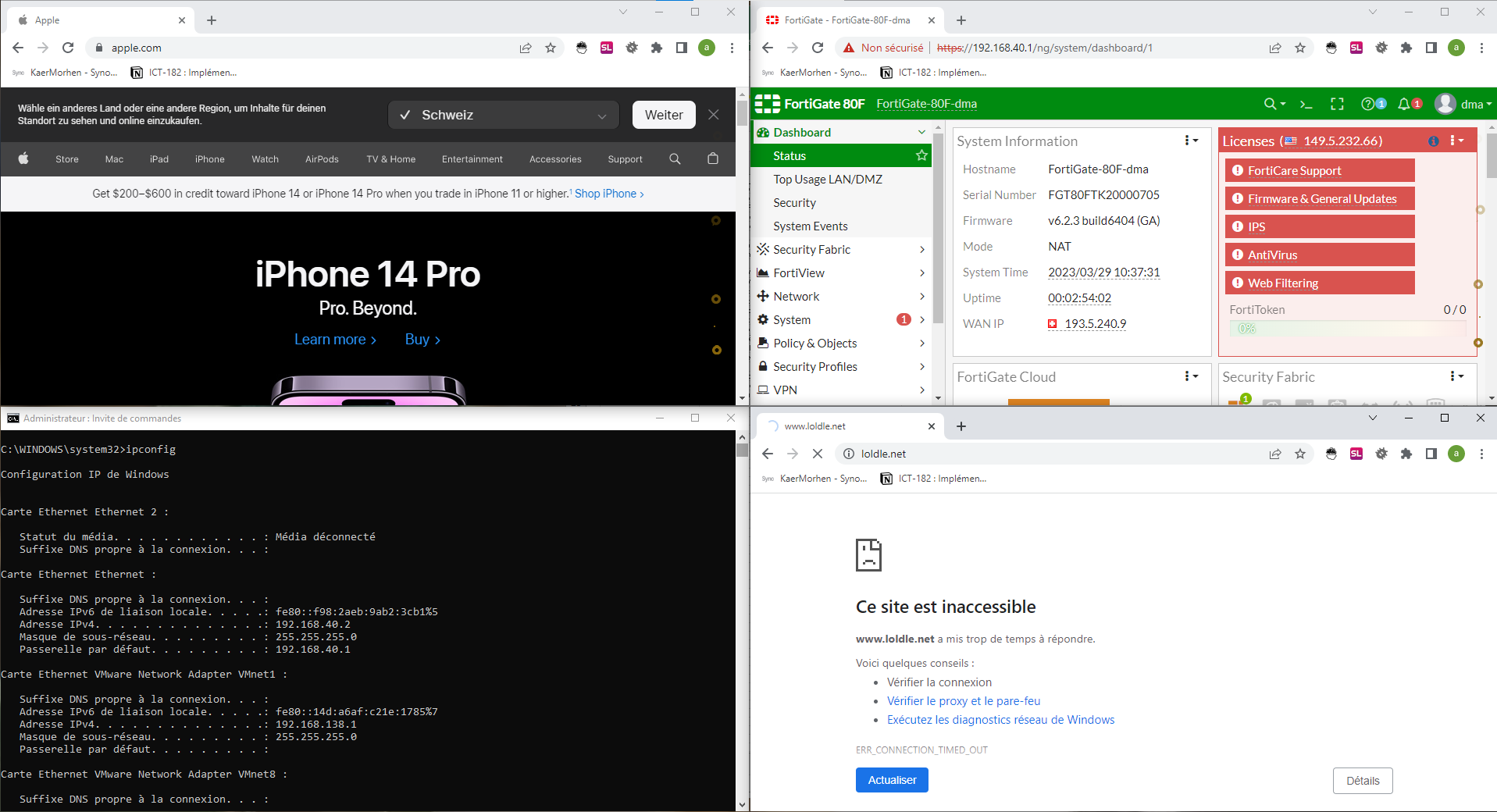


Figure 50 règle de blocage de loldle.net

21 Règles similaire CPNV

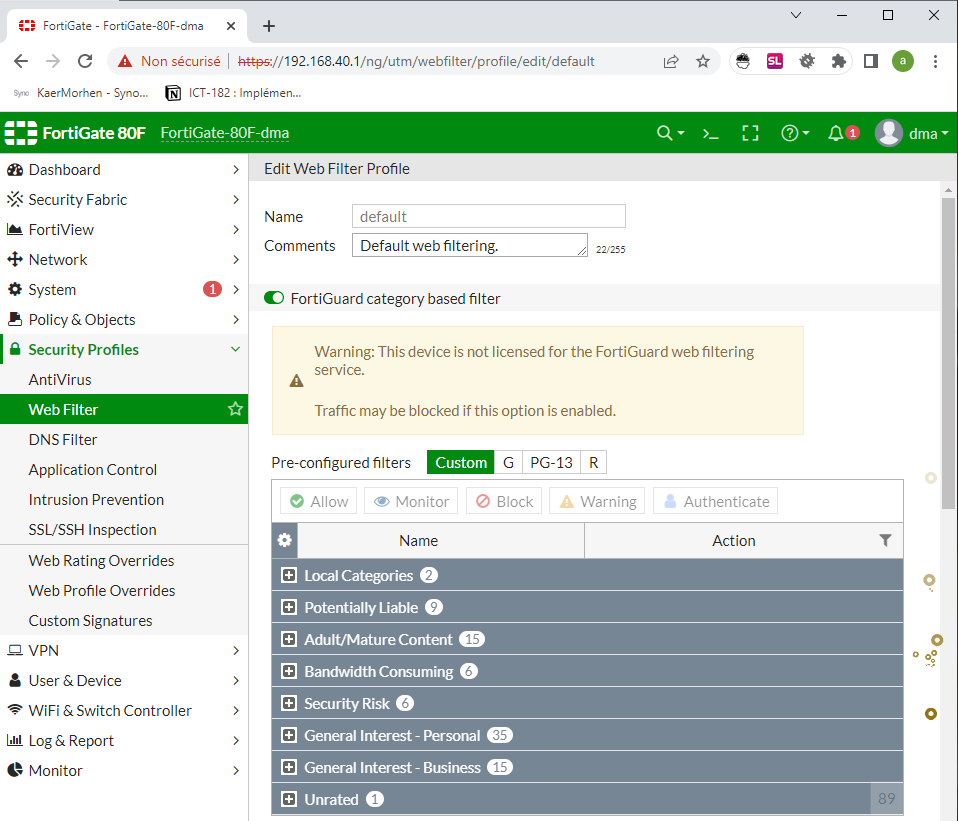


Figure 51 Impossibilité d'implémenter les mêmes règles que le CPNV

22 Switch

Pas d'illustration

23 DHCP

Pas d'illustration

# Fin des annexes