Manuel de tests

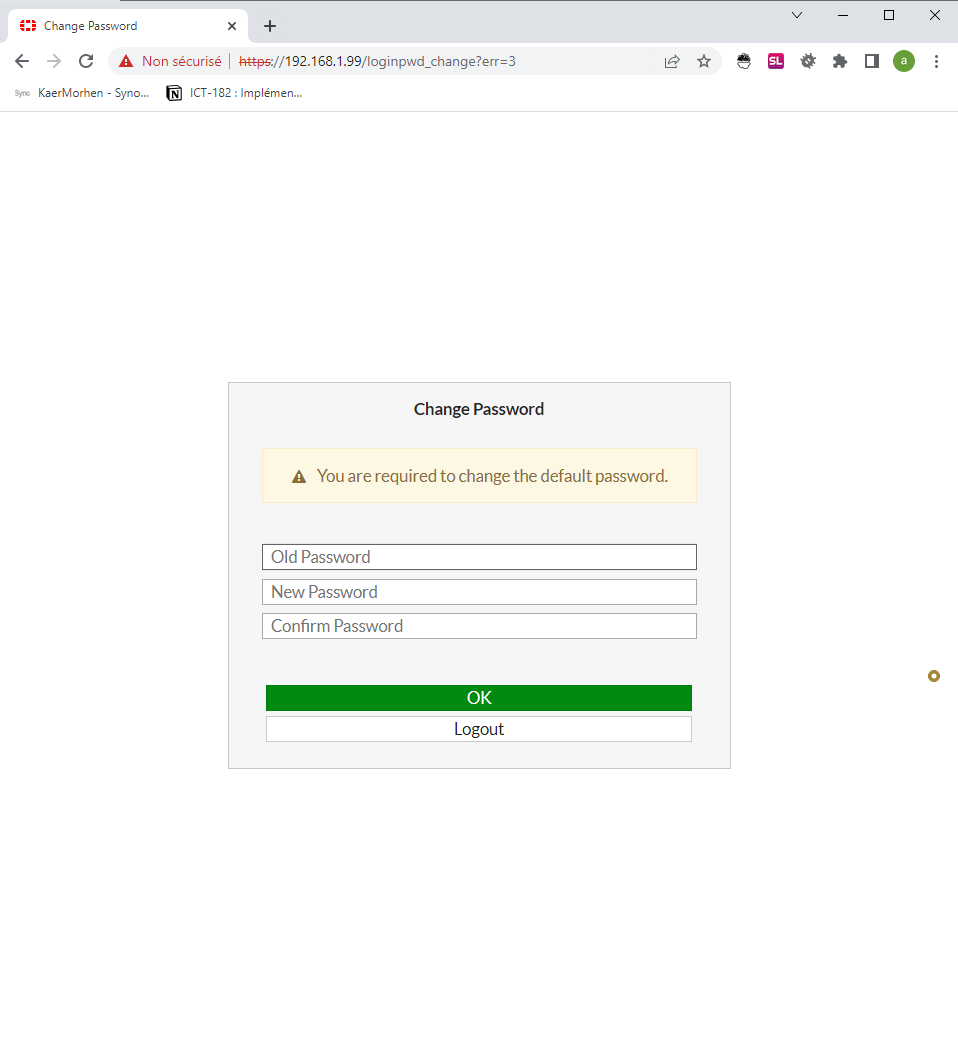


|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **N°** | **Nom du test** | **But du test** | **Description du test** | **Résultat attendu** | **Status** | **Problème possible** |
| 1 | LEDs Party | Vérifier que l'appareil est bien branché | Brancher le FortiG 80F selon manuel d'installation | 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 |  | - |

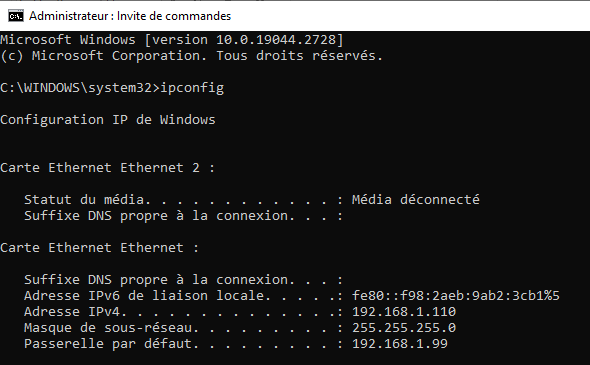
1 LEDs Party



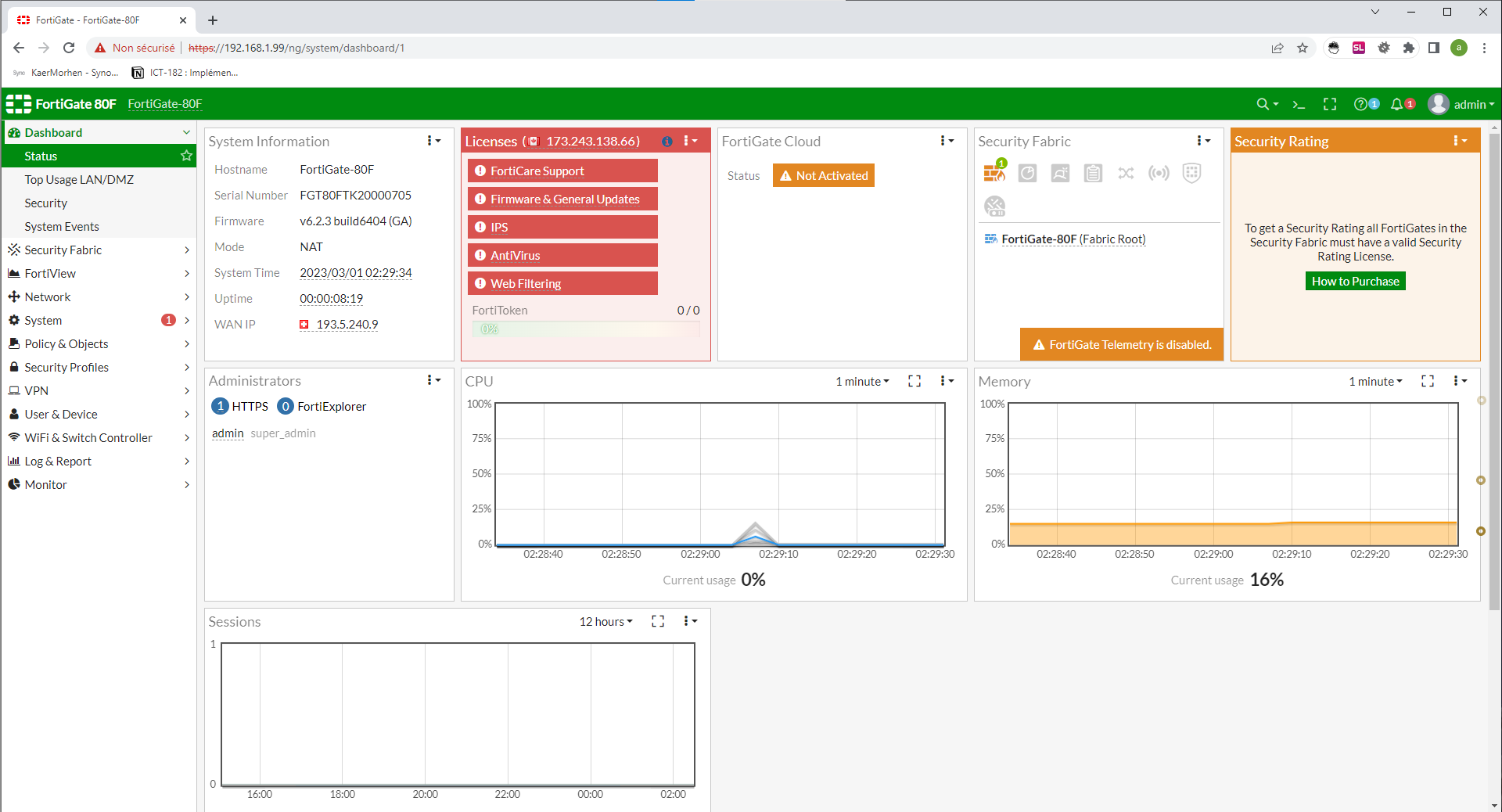
2 Mise à zéro de l'appareil



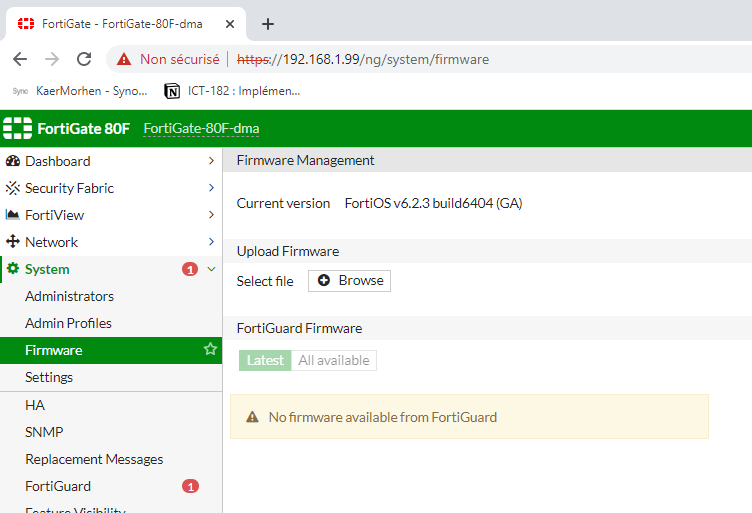
3 Adresse IP venant de pare-feu



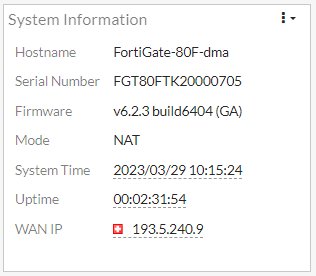
4 Atteindre le GUI



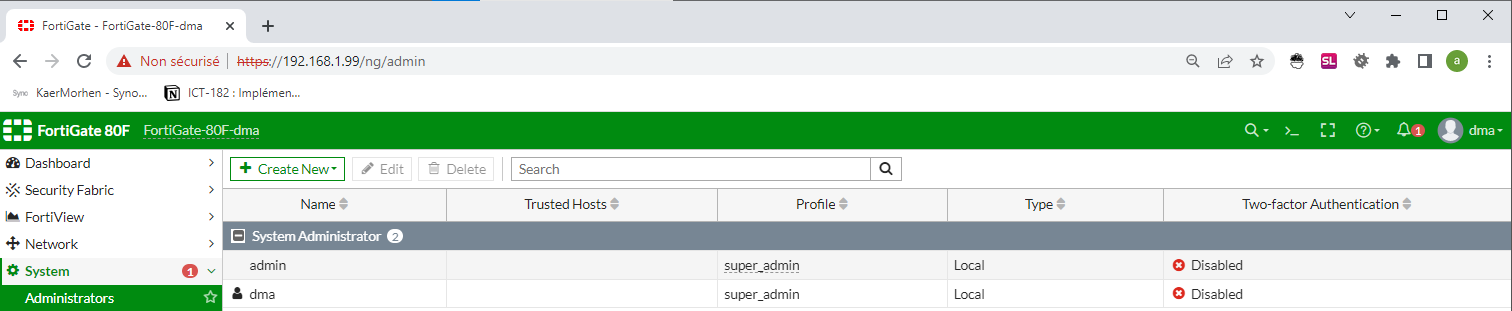
5 Mise à jour du Firmware



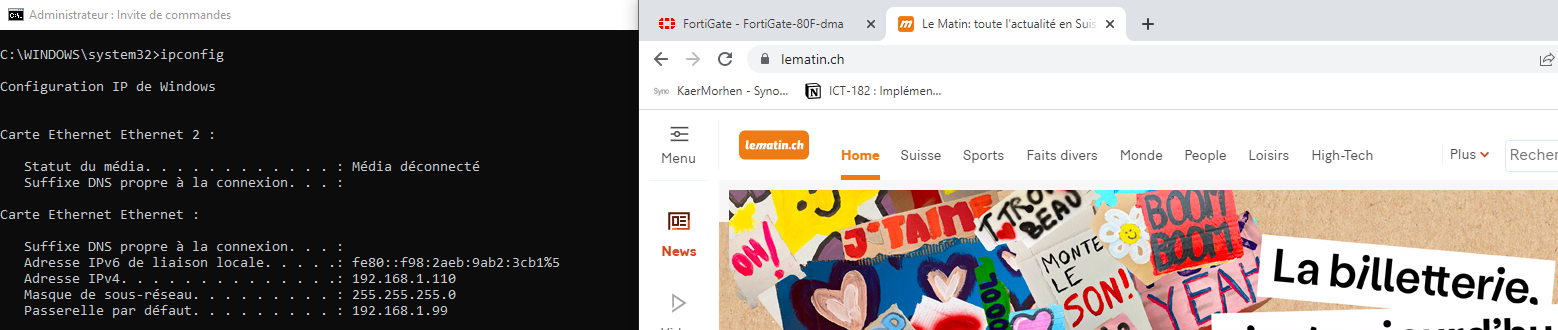
6 Changement hostname – date



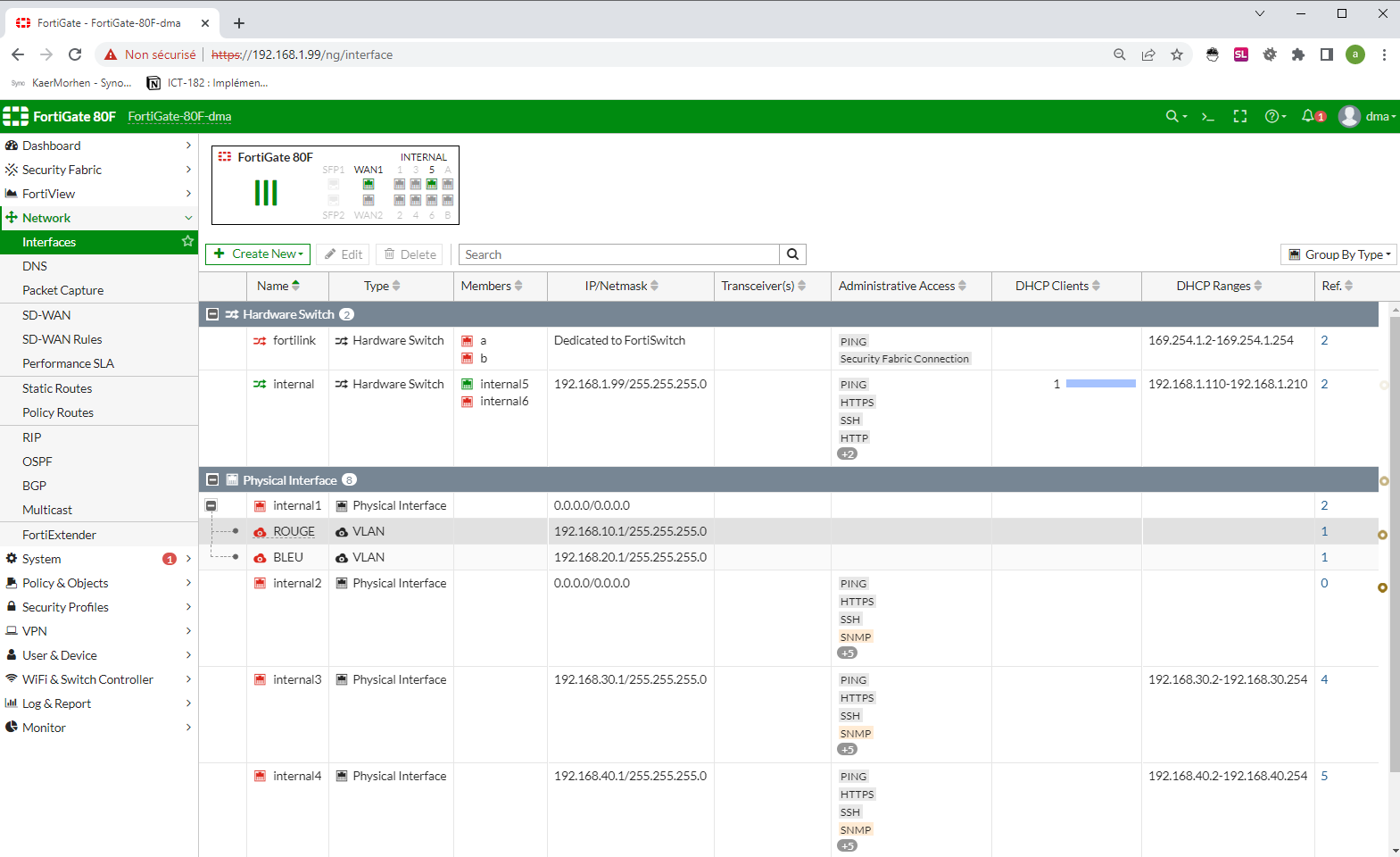
7 Nouvel administrateur



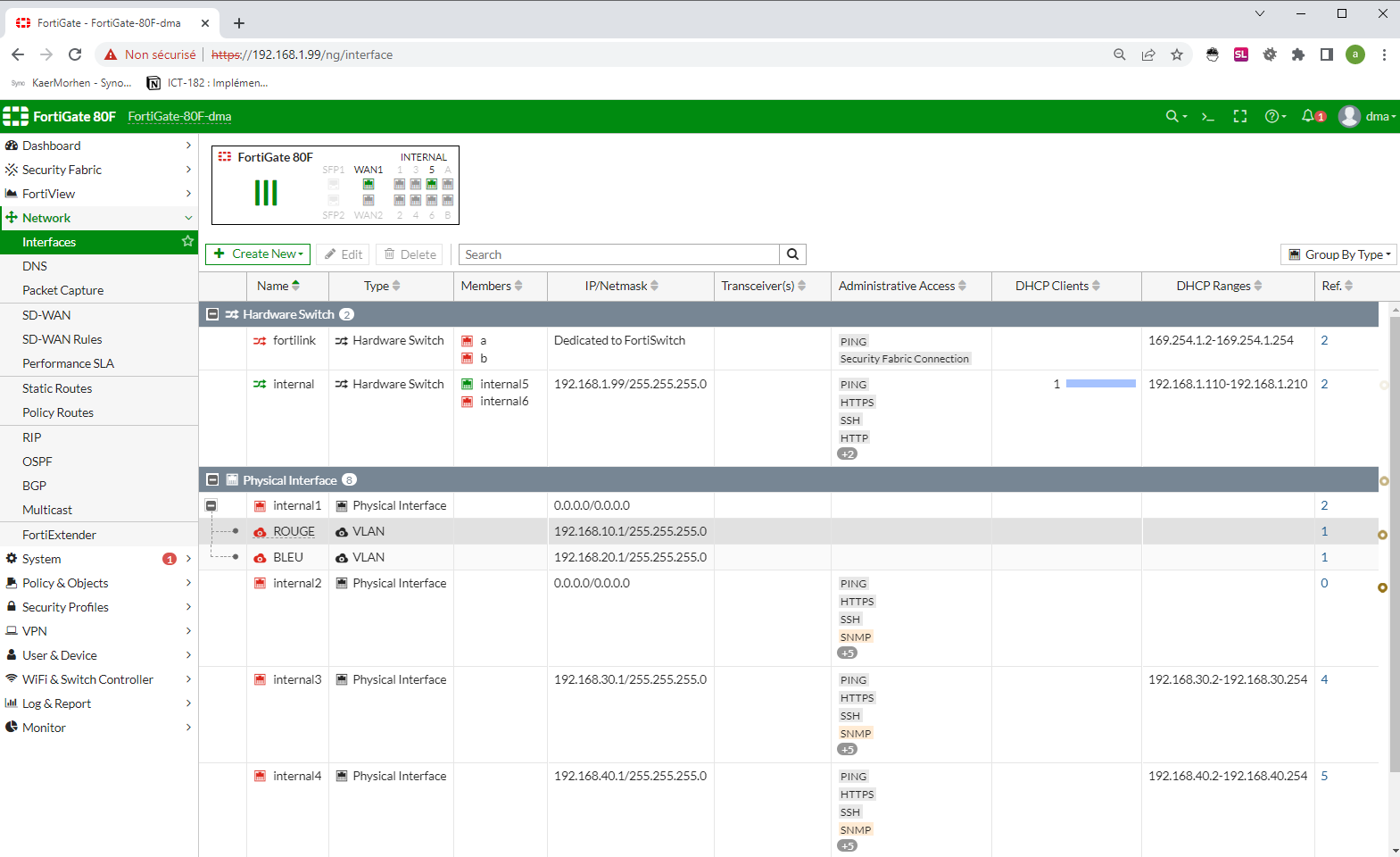
8 Accès à internet



9 Libération des interfaces



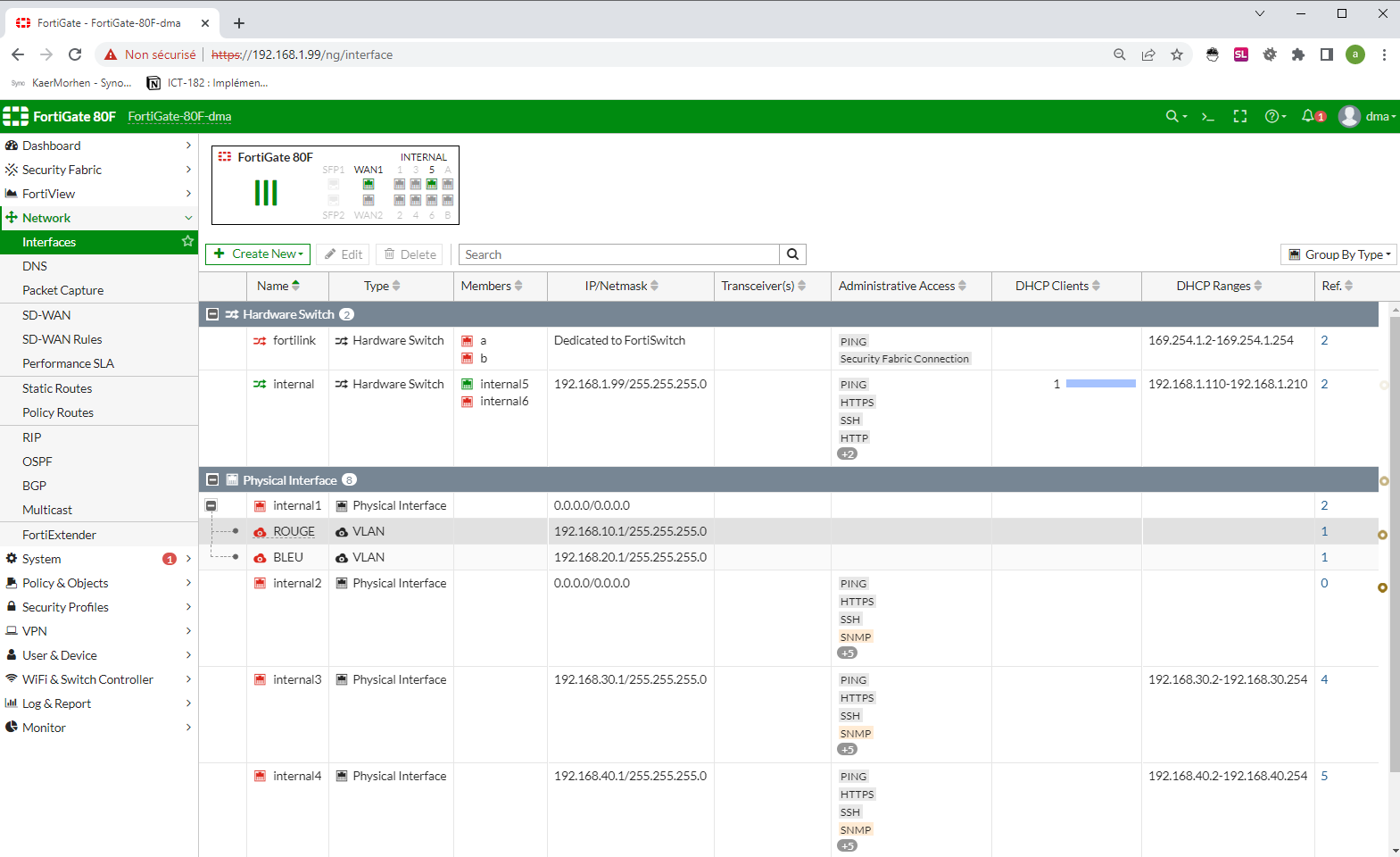
10 Création de VLAN



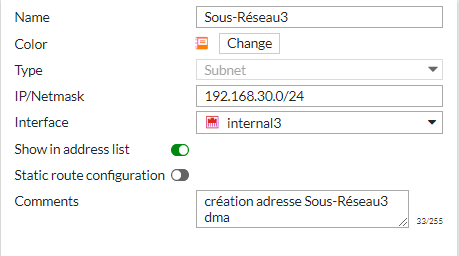
11 VLAN utilisable

Pas d'illustration

12 Création de sous-réseaux



13 Attribution d'interface



14 Connexion à internet sur internal3

Pas d'illustration

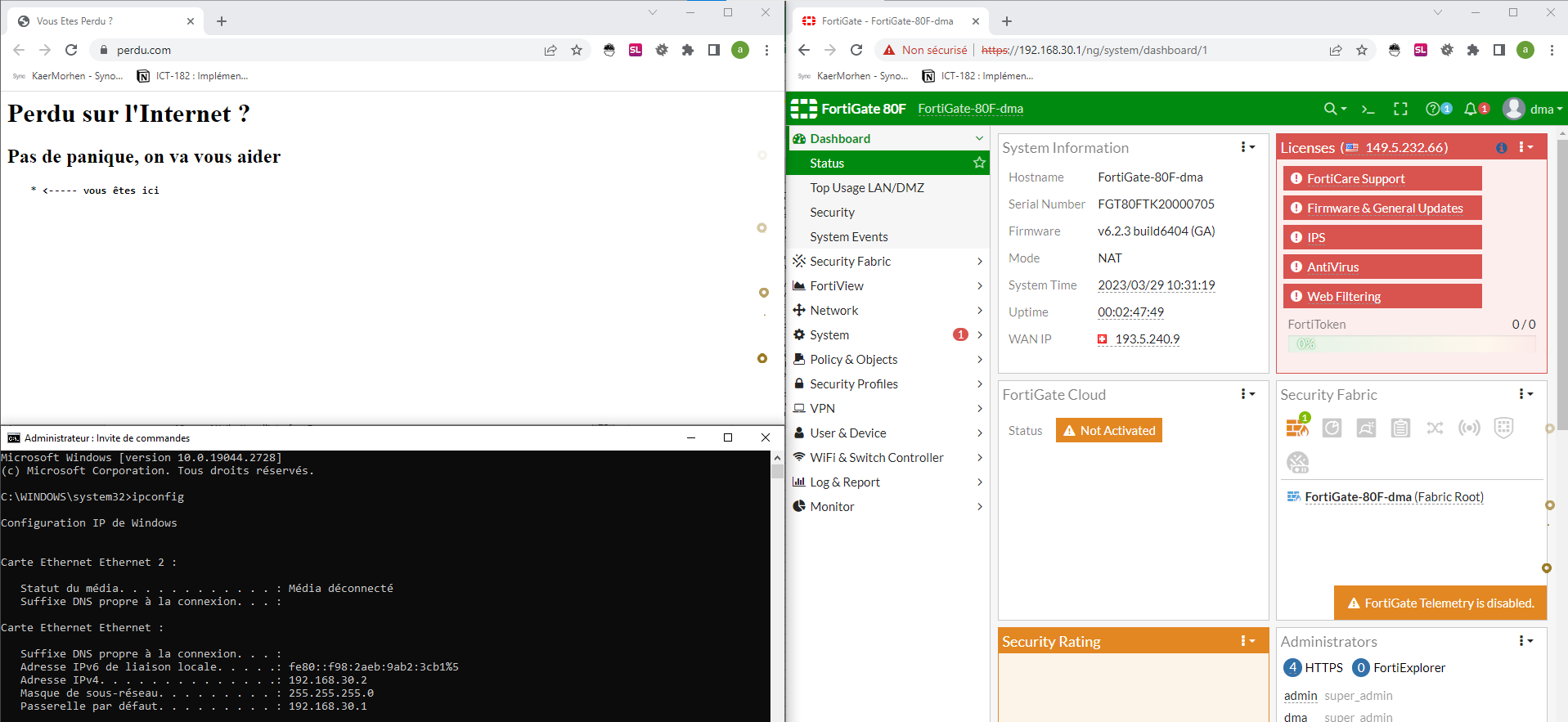
15 Création d'adresse pour internet

Pas d'illustration

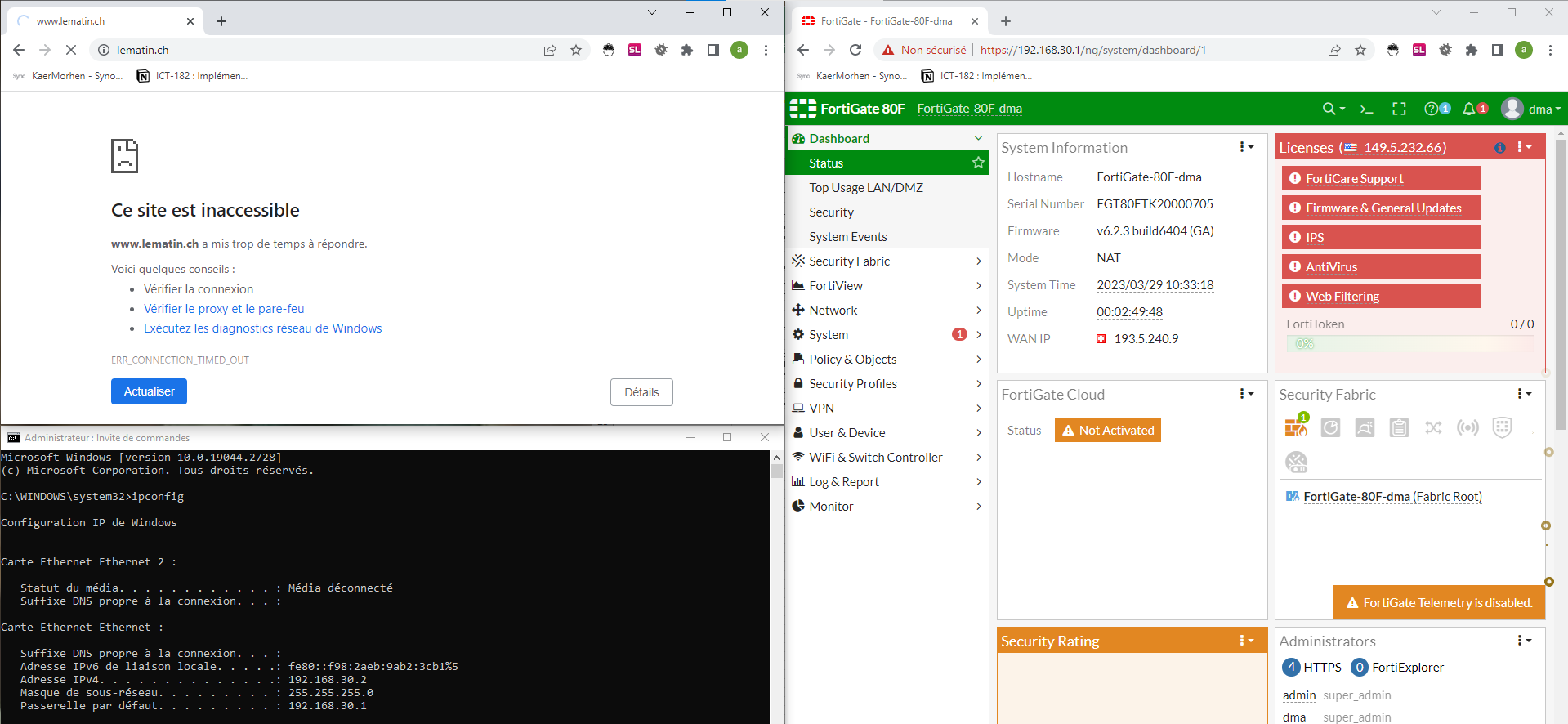
16 DNS?

Pas d'illustration

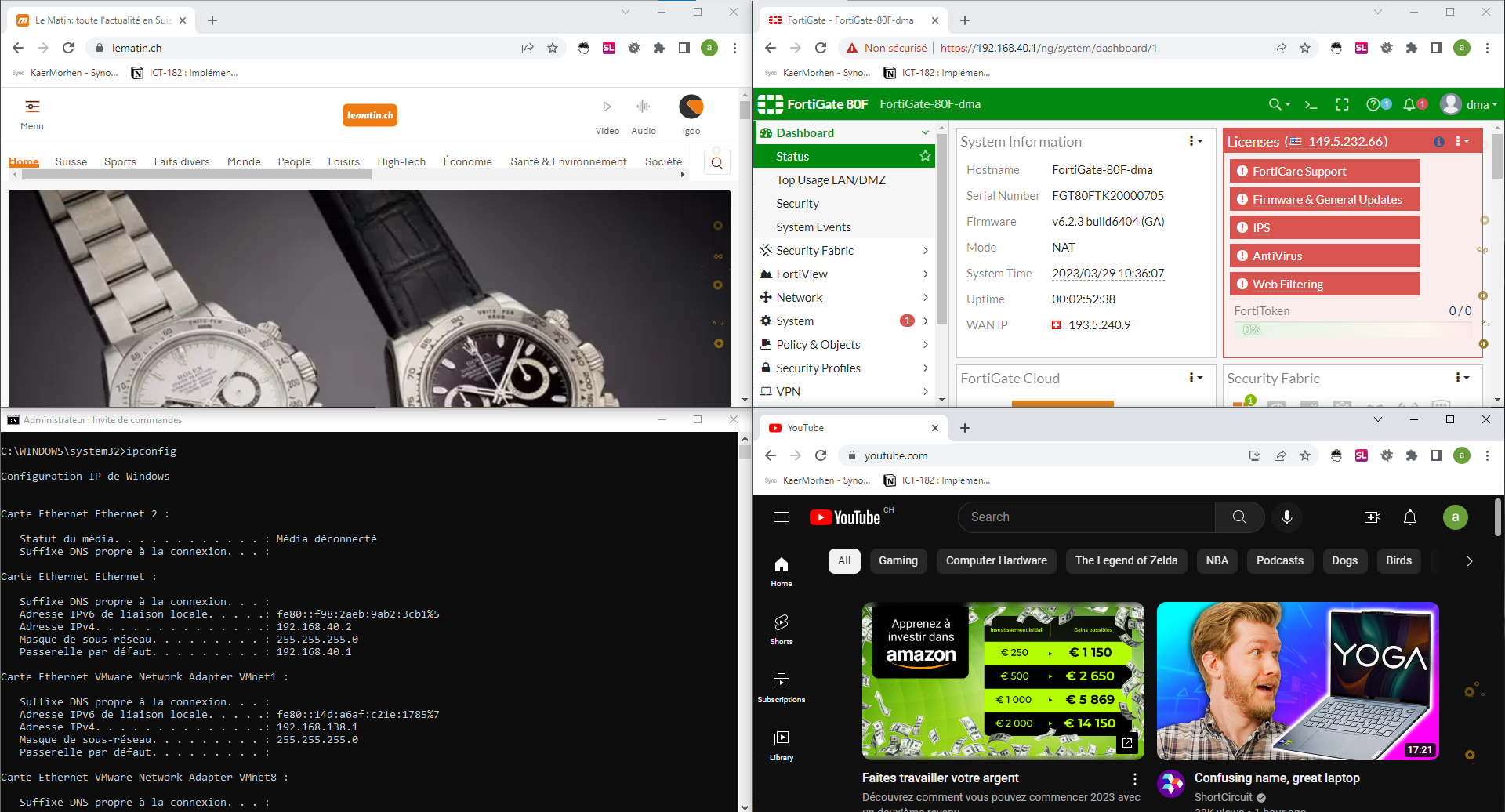
17 Création DNS



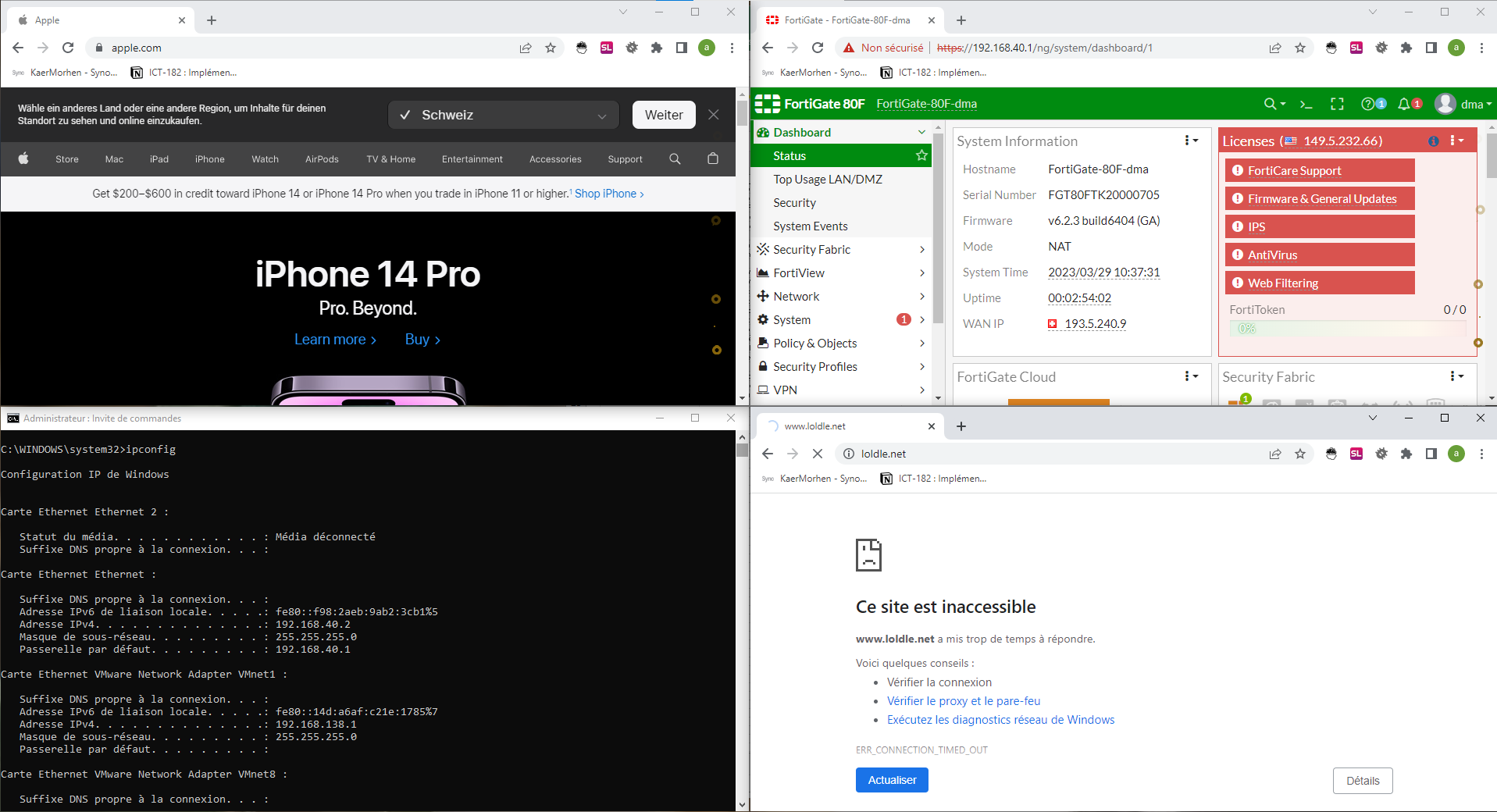
18 Uniquement perdu.com



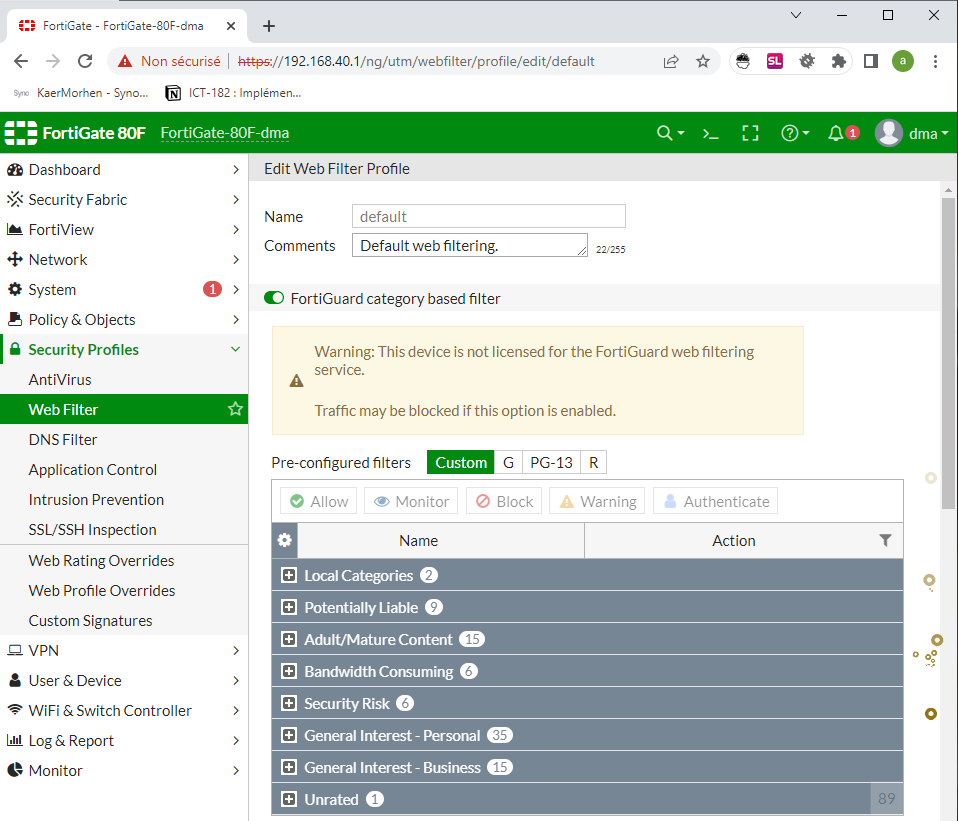
19 Règle Open bar



20 Règle block loldle



21 Règles similaire CPNV



22 Switch

Pas d'illustration

23 DHCP

Pas d'illustration