Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Infrastructures Réseaux et Serveurs

(Annexes)

Arno COURTINAT

Préfecture des Bouches-du-Rhône,
Service de l'Innovation Numérique et des Systèmes d'Information et de Communication

Responsable entreprise : Lionel MOURRE

Responsable académique : Éric SOCCORSI

2024

2 Présentation de l'Institution, de ses Services et du SINSIC

2.1 Organigramme et Articulation de ses Services

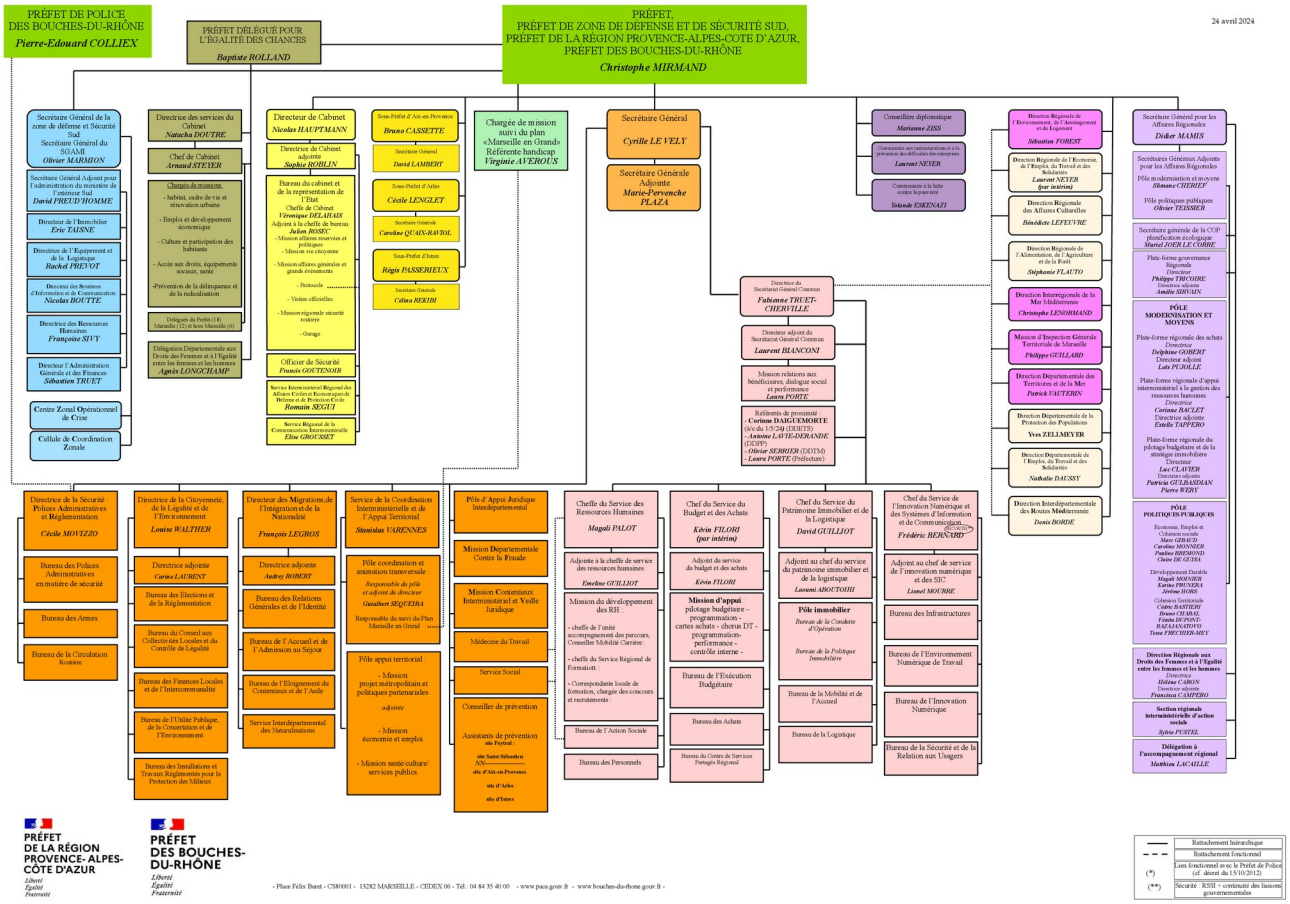


Fig. 1A : Organigramme détaillé de la Préfecture des Bouches-du-Rhône (une version agrandie de celui-ci est présente plus bas sous la forme de la Fig. 1B)

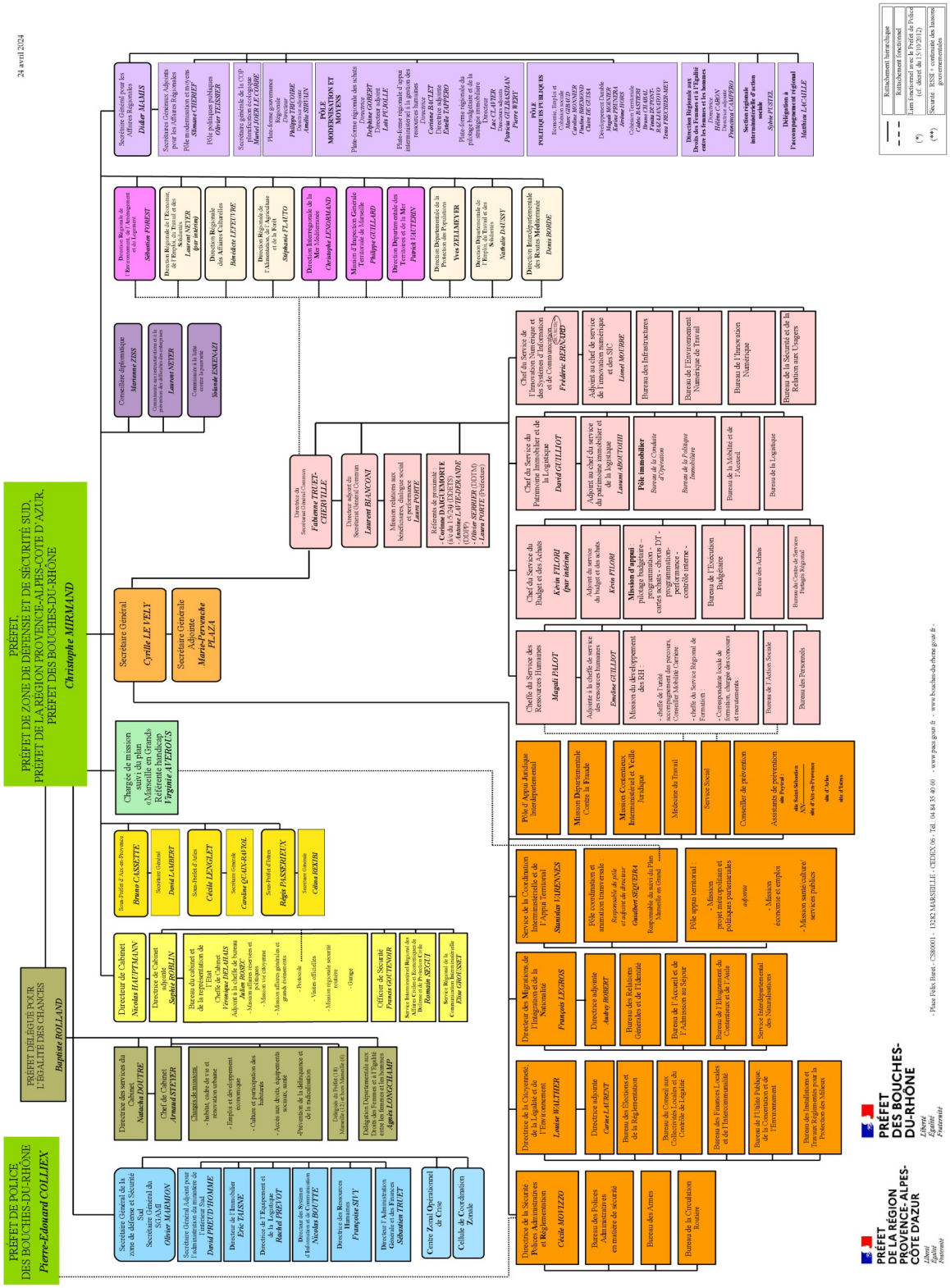


Fig. 1B : Organigramme détaillé de la Préfecture des Bouches-du-Rhône (celui-ci à été agrandi pour une meilleure visibilité, en raison de sa densité et de sa complexité)

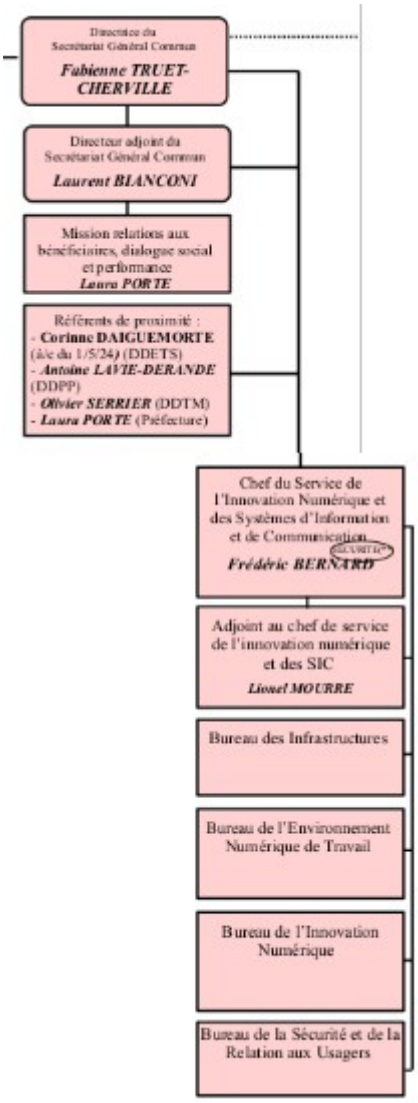


Fig. 2 : Zoom, au sein de l'organigramme des Figs. 1A et 1B, sur le Secrétariat Général Commun (SGC) contenant entre autres le Service de l'Innovation Numérique et des Systèmes d'Information et de Communication (SINSIC)

4 Travail Réalisé dans les Différents Projets

4.1 Projets Secondaires

4.1.1 Étude de l'Infrastructure Réseau en Place, Coordination du «Nettoyage» des Baies de Brassage

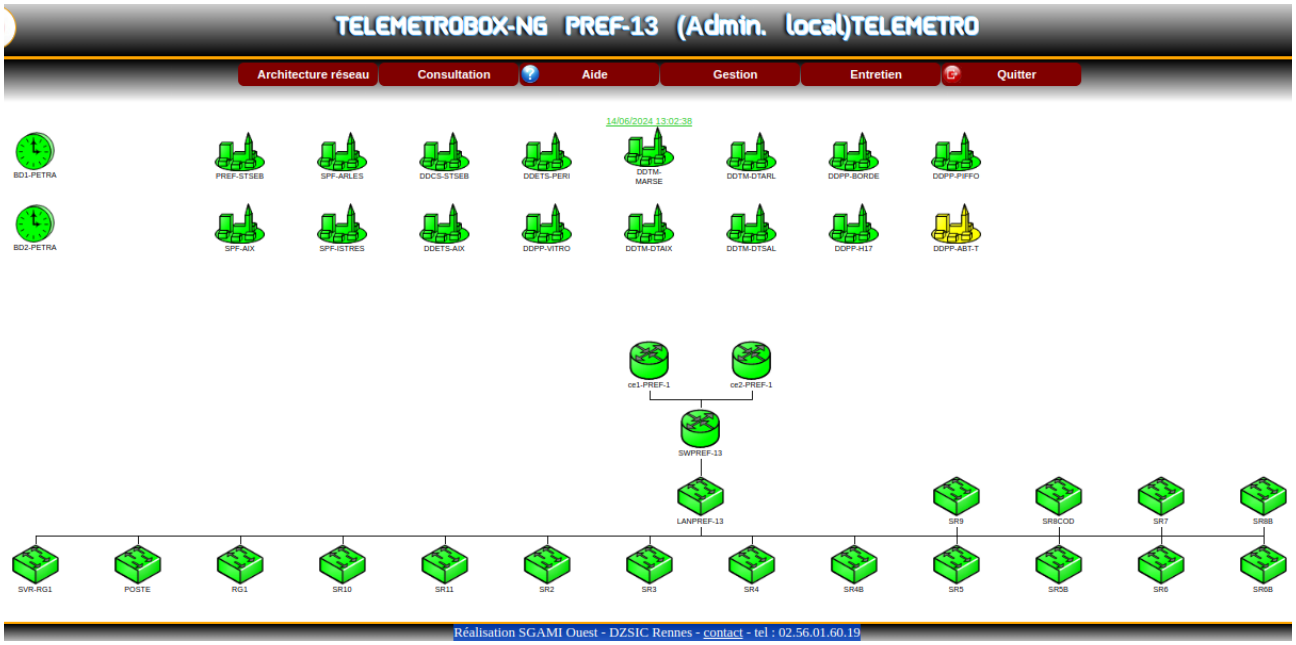


Fig. A1 : Page d'accueil du logiciel en ligne TelemetroBox-NG («monitoring» de l'architecture réseau globale : site principal et connectivité générale à chacun des sites distants)

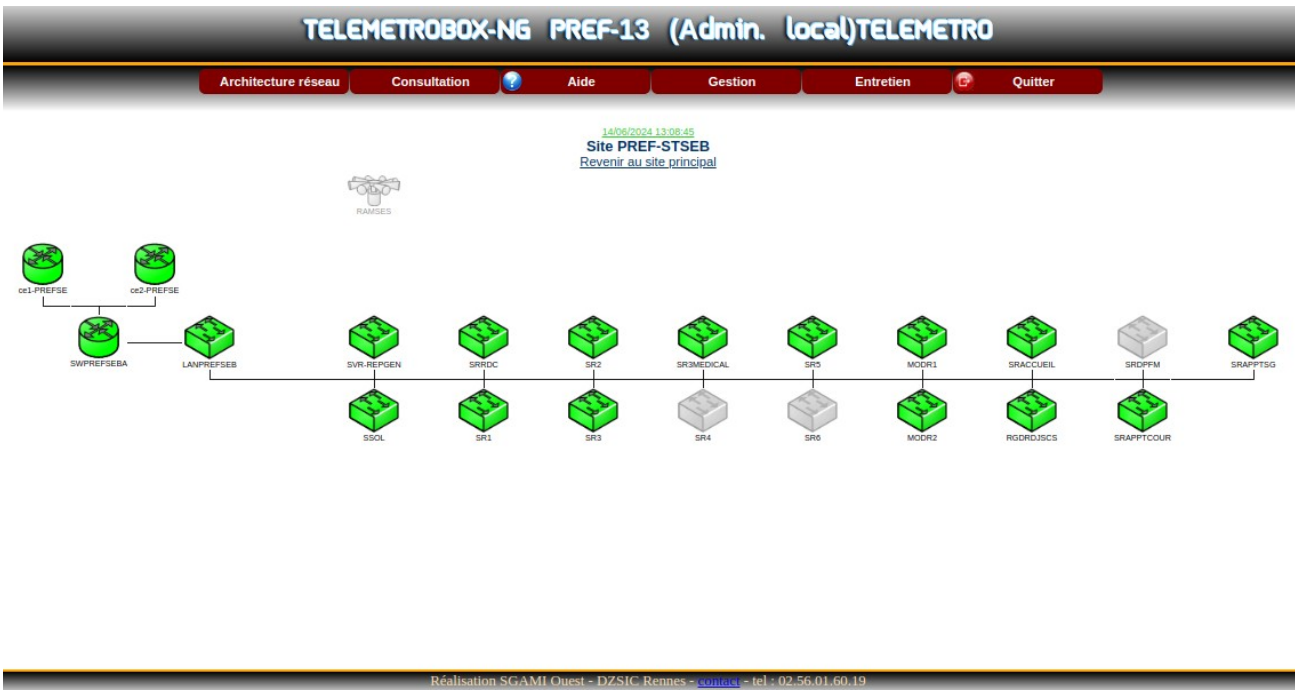


Fig. A2 : Exemple de «monitoring» du réseau de l'un des sites distants (certains équipements sont ici grisés car désactivés en raison des importants travaux ayant lieu au site de Saint Sébastien)

Fig. A3 : Onglet spécifique dans la rubrique spécifique à utiliser de TelemetroBox-NG

Fig. A4 : Exemple de cartographie de l'état des interfaces d'une des baies de brassage à l'aide de TelemetroBox-NG

4.1.2 Diagnostic et Réinitialisation d'Équipements Réseau Inutilisés

Figs. B1, B2 et B3 (ordre respectif descendant) : Modèles de commutateurs 3COM 5500-EI, H3C S5500 et HP A3600 (respectivement) présents en versions 24 et 48 ports, constituant la grande majorité du matériel à diagnostiquer et réinitialiser

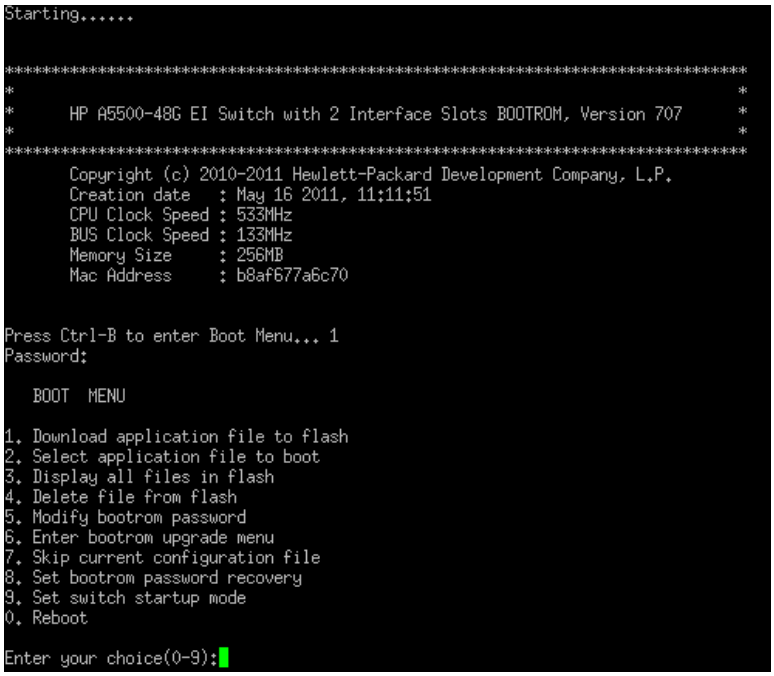


Fig. B4 : Exemple d'entrée dans le «Boot Menu» (accessible sur les commutateurs de la famille HP par la combinaison de touches CTRL+B avant le chargement du système d'exploitation) : celui-ci possède l'option numéro 7 «Ignorer le fichier de configuration actuel», très utile lorsque le mot de passe de connexion console est inconnu (une fois l'appareil démarré, un fichier de configuration d'usine peut remplacer le fichier de configuration actuel grâce à la commande «erase startup-

config», puis le changement peut être écrit en mémoire avec la commande «write memory», avant de redémarrer l'équipement avec la commande «reboot» pour appliquer les modifications)

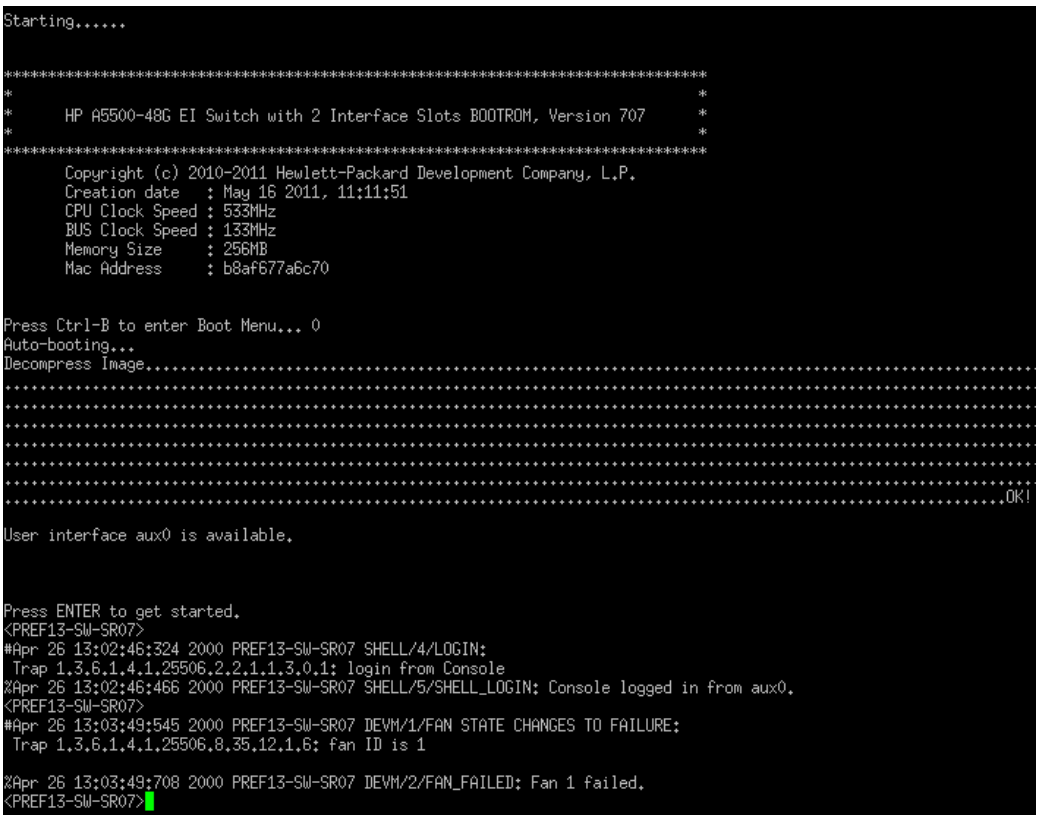
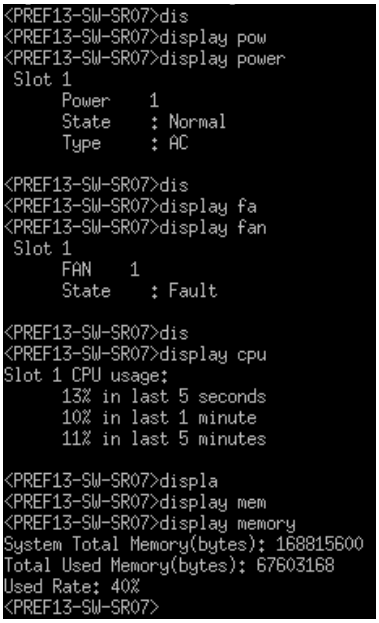


Fig. B5 : Exemple de connexion console sur un commutateur de famille HP, avec son unique mode de configuration : dès le démarrage, le message «Fan 1 failed» («Échec du ventilateur n°1», message répertorié dans les journaux système («logs») de la machine comme nous le verrons ci-dessous) indique à l'opérateur que ce commutateur présente un problème matériel avant même que celui-ci ne vérifie manuellement l'état de santé des composants



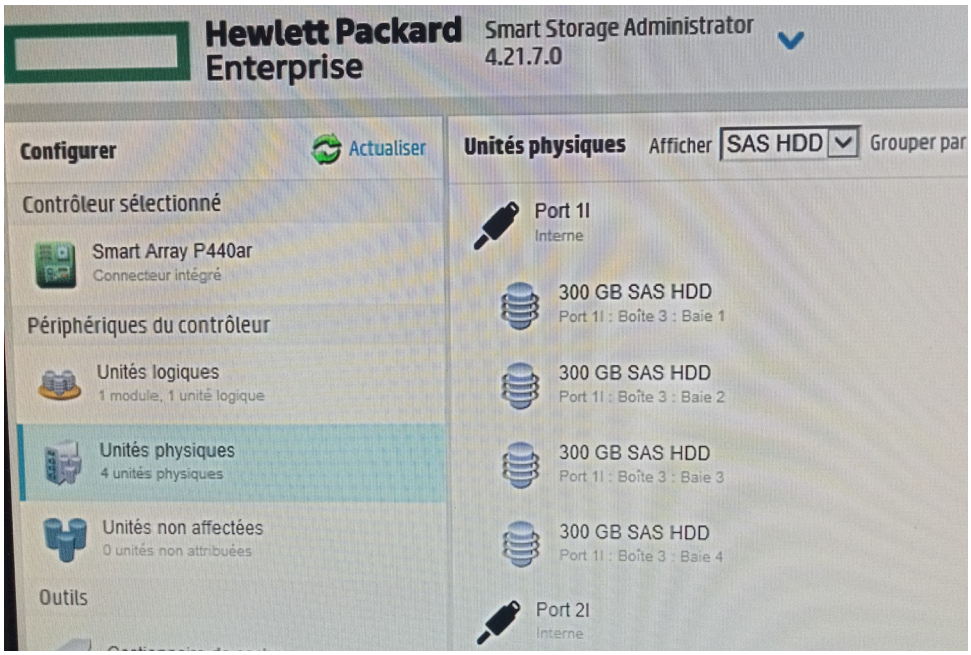
```
<PREF13-SW-SR07>display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 26

%Apr 26 12:00:38:134 2000 PREF13-SW-SR07 IC/6/SYS_RESTART: System restarted --
HP Platform Software.
%Apr 26 12:01:41:498 2000 PREF13-SW-SR07 IFNET/3/LINK_UPDOWN: Aux0/0/0 link status is UP.
%Apr 26 13:01:48:432 2000 PREF13-SW-SR07 MSTP/6/MSTP_ENABLE: STP is now enabled on the device.
%Apr 26 13:02:28:738 2000 PREF13-SW-SR07 DEVM/2/FAN_FAILED: Fan 1 failed.
%Apr 26 13:02:46:578 2000 PREF13-SW-SR07 SHELL/5/SHELL_LOGIN: Console logged in from aux0.
%Apr 26 13:03:49:799 2000 PREF13-SW-SR07 DEVM/2/FAN_FAILED: Fan 1 failed.
%Apr 26 13:05:10:607 2000 PREF13-SW-SR07 DEVM/2/FAN_FAILED: Fan 1 failed.
%Apr 26 13:05:29:040 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display system-failure
%Apr 26 13:05:37:937 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display system
%Apr 26 13:05:52:118 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display power
%Apr 26 13:05:57:373 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display fan
%Apr 26 13:06:10:389 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display cpu
%Apr 26 13:06:15:260 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display memory
%Apr 26 13:06:31:416 2000 PREF13-SW-SR07 DEVM/2/FAN_FAILED: Fan 1 failed.
%Apr 26 13:07:52:224 2000 PREF13-SW-SR07 DEVM/2/FAN_FAILED: Fan 1 failed.
%Apr 26 13:09:13:033 2000 PREF13-SW-SR07 DEVM/2/FAN_FAILED: Fan 1 failed.
%Apr 26 13:09:35:508 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display component
%Apr 26 13:10:13:900 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display device
%Apr 26 13:10:23:004 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display diagnostic-information
%Apr 26 13:10:33:840 2000 PREF13-SW-SR07 DEVM/2/FAN_FAILED: Fan 1 failed.
%Apr 26 13:11:54:709 2000 PREF13-SW-SR07 DEVM/2/FAN_FAILED: Fan 1 failed.
%Apr 26 13:12:02:919 2000 PREF13-SW-SR07 CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=1-CommandSource=2-ConfigSource=4-ConfigDestination=2; Configuration is changed.
%Apr 26 13:12:09:865 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display info-center
%Apr 26 13:12:16:274 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display logbuffer
%Apr 26 13:12:24:240 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display info-center
%Apr 26 13:13:07:529 2000 PREF13-SW-SR07 SHELL/6/SHELL_CMD: -Task=au0-IPAddr=**-User=**; Command is display logbuffer
<PREF13-SW-SR07>
```

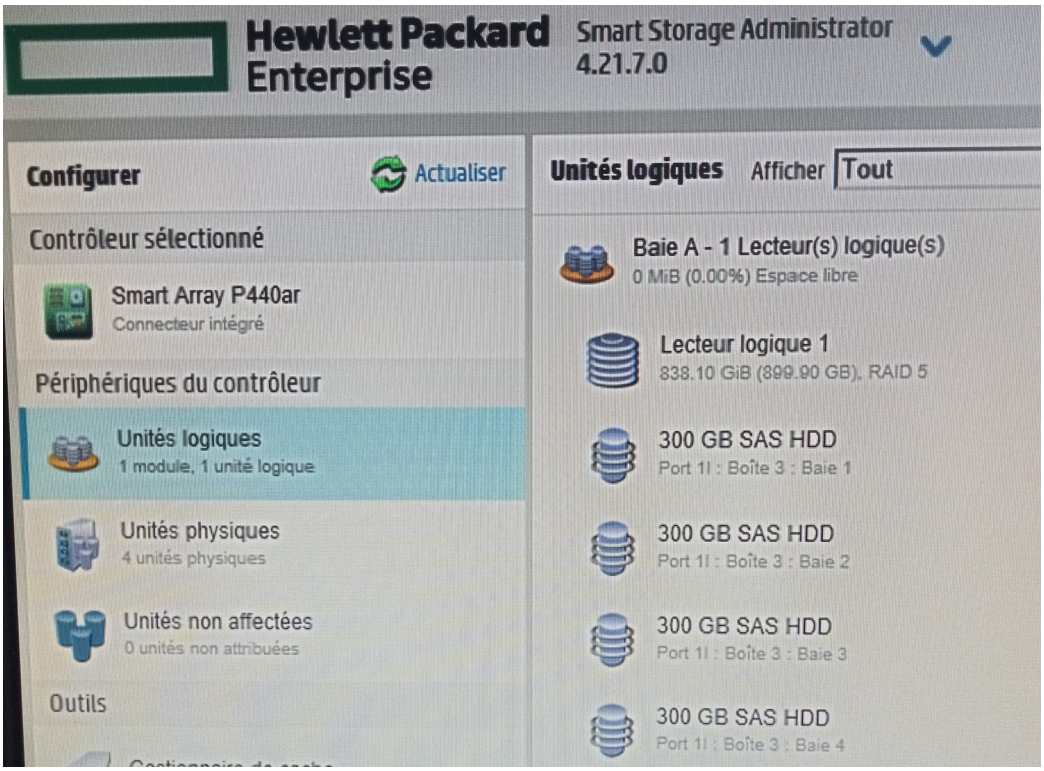
Figs. B6 et B7 (ordre respectif descendant) : Commandes HP utiles au diagnostic de la santé du matériel : tandis que la commande «display power» affiche la présence et l'état des modules d'alimentation (un appareil doté de deux modules d'alimentation pourrait par exemple présenter une panne sur l'un d'entre eux sans pour autant cesser de fonctionner), la commande «display fan» affiche l'état de fonctionnement des ventilateurs (dans l'exemple présent, celle-ci confirme une panne du module de ventilateurs n°1 : problème courant sur les appareils 3COM, il est impossible de déterminer combien de temps un commutateur mis en production avec un problème de ventilateurs mettrait avant de surchauffer (ce qui entraînerait une dégradation des performances, une usure prématurée des composants internes, etc.)), la commande «display cpu» permet d'afficher l'utilisation actuelle de chaque cœur du processeur (et donc le bon fonctionnement de chacun d'entre eux), la commande «display memory» permet d'afficher les informations concernant la mémoire vive de l'appareil, et la commande «display logbuffer» affiche les journaux système récents stockés dans la mémoire-tampon interne (avertissements, erreurs, etc.); à toutes ces commandes doit également être ajoutée la commande «display current-configuration» permettant de visualiser le fichier de configuration en cours (et donc s'assurer qu'il a bien été remis à zéro si cela doit être le cas, s'assurer de l'état de chacune des interfaces de l'appareil, etc.)

4.1.3 Mise à Niveau et Configuration du Futur Serveur Autocom

Fig. C1 : Serveur HP HPE ProLiant DL380 Gen9 ayant été modifié en conséquence


Hewlett Packard Enterprise
Smart Storage Administrator 4.21.7.0
Périphérique(s) disponible(s)
Actualiser
Serveur
Serveur
Phonix
Contrôleurs de réseau intelligent
Smart Array P440ar
Connecteur intégré
Autres périphériques
Périphériques SSD
0 SSD
Bienvenue dans Smart Storage Administrator
Cette application vous permet de configurer, diagnostiquer et gérer des périphériques Smart Storage connectés à votre serveur.
Veuillez commencer par sélectionner un périphérique dans le menu sur la gauche.


Hewlett Packard Enterprise
Smart Storage Administrator 4.21.7.0
Configurer
Actualiser
Unités physiques
Afficher
SAS HDD
Grouper par
Contrôleur sélectionné
Smart Array P440ar
Connecteur intégré
Périphériques du contrôleur
Unités logiques
1 module, 1 unité logique
Unités physiques
4 unités physiques
Unités non affectées
0 unités non attribuées
Outils
Port 1I
Interne
300 GB SAS HDD
Port 1I : Boîte 3 : Baie 1
300 GB SAS HDD
Port 1I : Boîte 3 : Baie 2
300 GB SAS HDD
Port 1I : Boîte 3 : Baie 3
300 GB SAS HDD
Port 1I : Boîte 3 : Baie 4
Port 2I
Interne


Hewlett Packard Enterprise
Smart Storage Administrator 4.21.7.0
Configurer
Actualiser
Unités logiques
Afficher
Tout
Contrôleur sélectionné
Smart Array P440ar
Connecteur intégré
Périphériques du contrôleur
Unités logiques
1 module, 1 unité logique
Unités physiques
4 unités physiques
Unités non affectées
0 unités non attribuées
Outils
Baie A - 1 Lecteur(s) logique(s)
0 MiB (0.00%) Espace libre
Lecteur logique 1
838.10 GiB (899.90 GB), RAID 5
300 GB SAS HDD
Port 1I : Boîte 3 : Baie 1
300 GB SAS HDD
Port 1I : Boîte 3 : Baie 2
300 GB SAS HDD
Port 1I : Boîte 3 : Baie 3
300 GB SAS HDD
Port 1I : Boîte 3 : Baie 4

Figs. C2, C3 et C4 (ordre respectif descendant) : Présentation du logiciel HP Smart Storage Administrator permettant la configuration et la gestion dans une interface graphique simplifiée des périphériques RAID

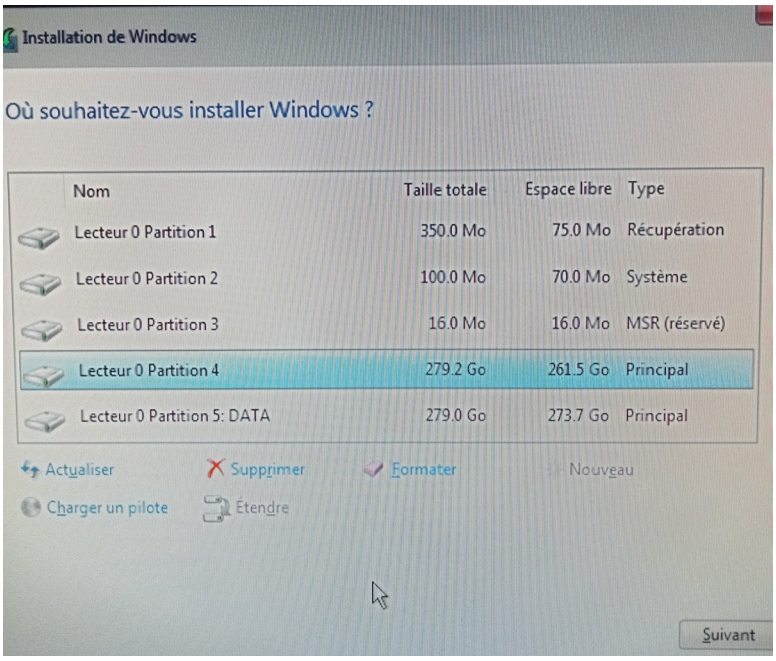


Fig. C5 : Création des partitions sur le disque virtuel créé précédemment (les partitions «Récupération», «Système» et «MSR (réservé)» sont créées automatiquement à la création de la première partition destinée ; de plus, posséder une partition destinée à héberger le système (ici partition 4 future C:\) distincte de la partition de données (ici partition 5 «DATA» future D:\) est une bonne pratique de sécurité : cela permet de protéger les données en cas de corruption du système ou, inversement, de protéger le système en cas de faille de sécurité sur la partition de données (par exemple, un serveur Web hypothétiquement piratable peut être installé comme devant travailler sur la partition D:\))

Fig. C6 : Après l'opération, le résultat obtenu est bien celui escompté : la disque dur virtuel créé précédemment a été partitionné

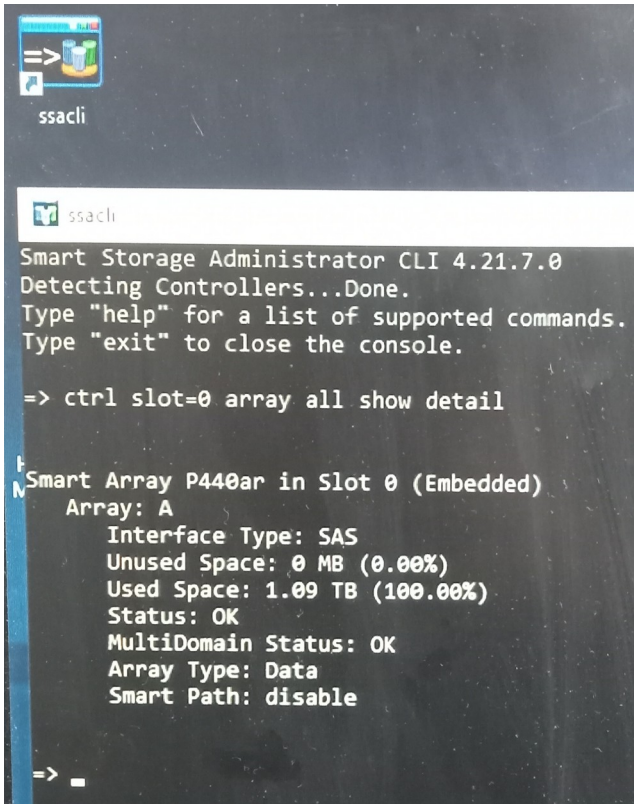
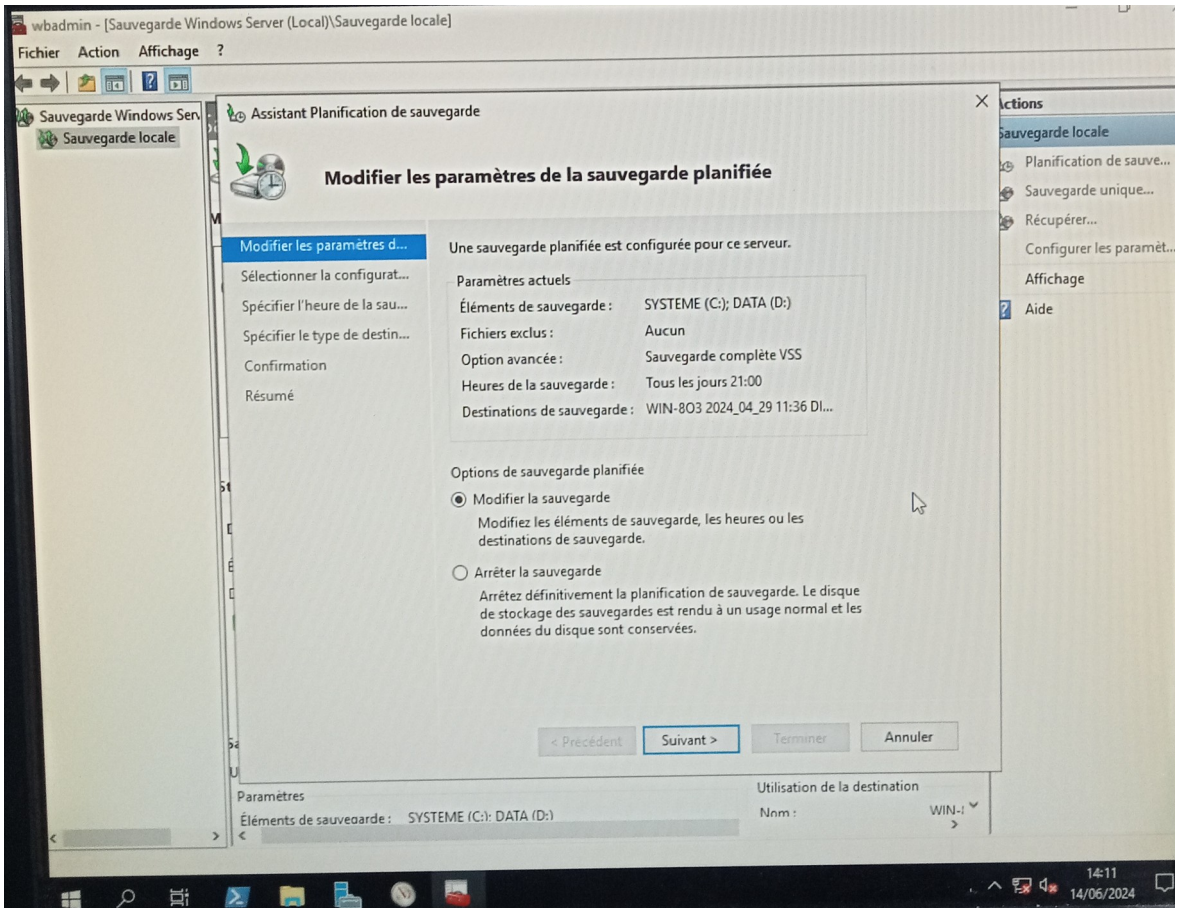
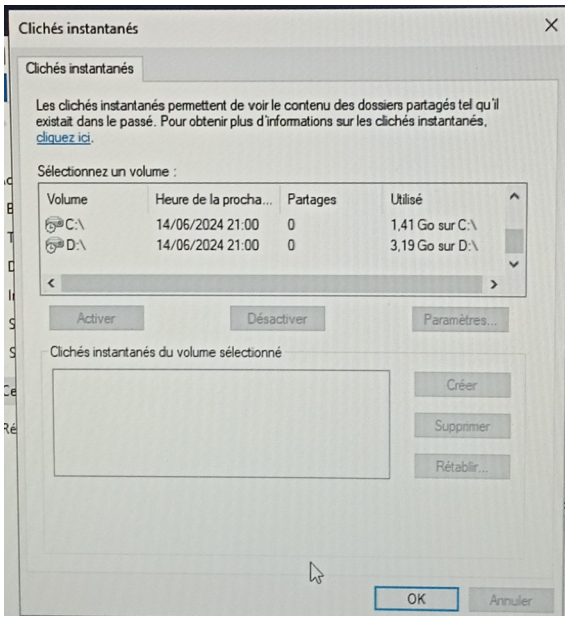


Fig. C7 : Version en ligne de commande de l'utilitaire Smart Storage Administrator vu précédemment : celui-ci permet de modifier et/ou obtenir des informations sur l'architecture RAID mise en place via des commandes intégrables dans des scripts pour une surveillance automatisée





Figs. C8 et C9 (ordre respectif descendant) : Après avoir installé l'utilitaire Sauvegarde Windows Server et branché le disque dur externe qui va accueillir la sauvegarde, une nouvelle tâche peut être programmée simplement en cliquant sur Planification de sauvegarde et en renseignant les champs demandés de la même façon que sur l'image C8 ; enfin, après avoir accédé au gestionnaire de clichés instantanés, ceux-ci sont activables pour les deux partitions utiles créées précédemment (une petite partie d'espace disque sur celles-ci est alors allouée au stockage des clichés instantanés) en sélectionnant l'une après l'autre lesdites partitions puis en sélectionnant Activer, et en renseignant la fréquence ainsi que l'heure auxquelles les clichés instantanés doivent avoir lieu

4.1.4 Choix et Mise en Œuvre d'un Outil d'Administration Système

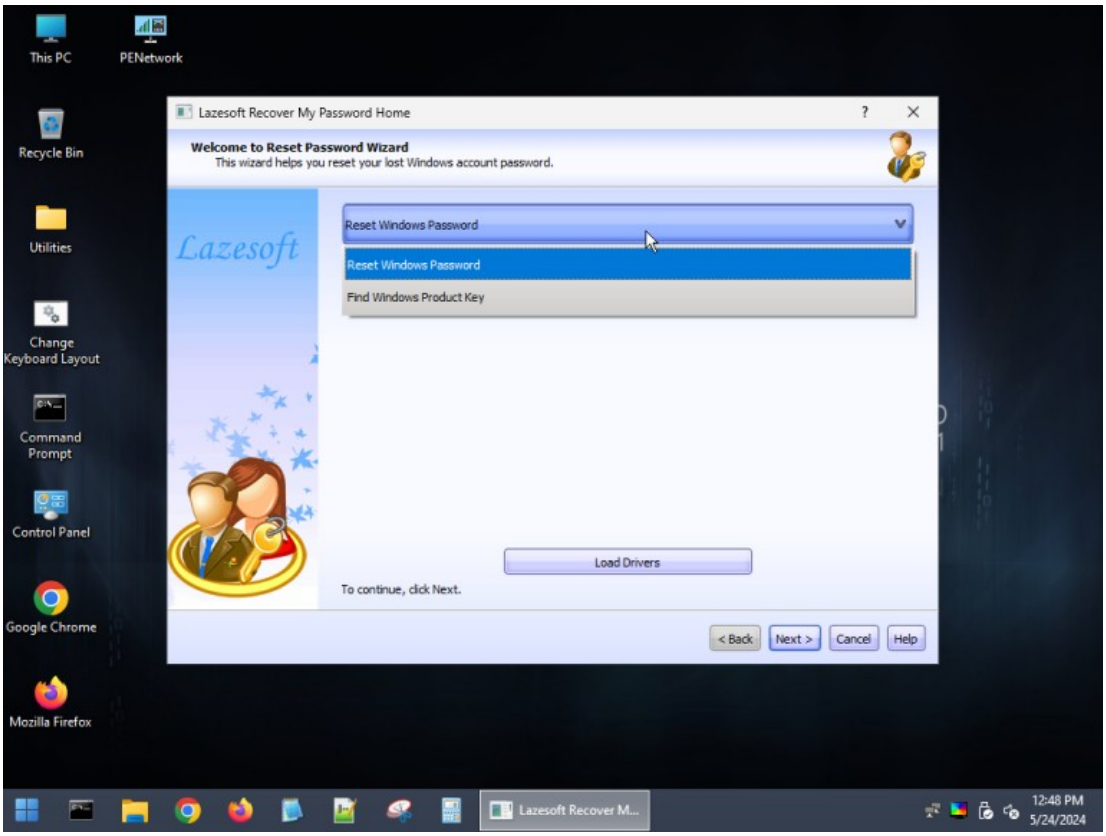
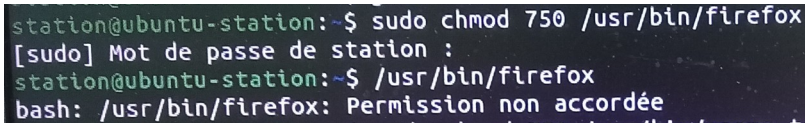


Fig. D1 : Constituant un véritable système d'exploitation Windows 11 de petite taille pleinement fonctionnel, Hiren's Boot CD PE intègre toutefois de nombreux outils de dépannage système qui

peuvent s'avérer utiles en cas de perte de données sur disque, d'infection de la machine par des logiciels malveillants, etc. (outils parmi lesquels l'utilitaire Lazesoft Password Recovery : celui-ci, en agissant sur le fichier de mots de passe locaux Windows «gestionnaire des comptes de sécurité» («Security Account Manager» ou «fichier SAM» situé à «C:\Windows\system32\config\SAM»), permet de supprimer le mot de passe de n'importe quel compte utilisateur local de façon à permettre la connexion sans qu'aucun mot de passe ne soit donné : toutes les versions de Windows fonctionnant à l'aide de cette base de données de comptes locaux, cet outil est également en théorie utilisable en ciblant les comptes de toutes les versions de Windows)

4.1.5 Sécurisation de Station Blanche



Figs. E1, E2, E3, E4, E5, E6, E7 et E8 (ordre respectif descendant) : Jeu de commandes utilisé afin de sécuriser la station blanche de Maël LESAICHERRE sans entraver le bon fonctionnement de son programme (il convient de noter qu'à travers ces commandes, le droit d'ouvrir un terminal est retiré à l'utilisateur «station» : ces commandes doivent donc être entrées avec attention et l'absence d'erreurs doit être vérifiée minutieusement avant de fermer le terminal utilisé, car un nouveau terminal ne pourra pas être ouvert une fois celui-ci fermé !) : les exécutables «/usr/bin/firefox», «/usr/bin/gnome-terminal» et «/usr/bin/nautilus», par défaut, appartiennent à l'utilisateur «root» ainsi qu'au groupe «root» mais incluent des droits d'exécution pour la catégorie «autres [utilisateurs]» (qui inclue l'utilisateur «station» : il suffit de retirer ces droits pour la catégorie «autres [utilisateurs]» afin que l'opérateur de la station blanche ne puisse plus ouvrir Firefox (ce qui permettrait par exemple de télécharger n'importe quel logiciel sur la station), ne puisse plus ouvrir de Terminal (dans les mains d'un opérateur mal intentionné, celui-ci pourrait permettre de lancer sur la machine une bombe à processus («fork bomb») (ce qui consiste par exemple en une commande pas plus difficile que «:(){ :|:& };:» trouvable rapidement sur Internet) ou bien un script s'attaquant aux performances du réseau (par exemple, sur le même principe que celui de «fork bomb», en lançant indéfiniment de nouvelles requêtes «ping» sur l'adresse de diffusion ou «broadcast») et ne puisse plus ouvrir l'explorateur de fichiers (nommé «Nautilus» sur Ubuntu) (ce qui permettrait par exemple d'identifier et de déplacer les fichiers utiles au bon fonctionnement du programme de la station blanche, par exemple les images évoquées plus bas permettant de changer le fond d'écran du Bureau de la machine selon le résultat de l'analyse) ; une fois les droits d'exécution desdits exécutables retirés pour l'utilisateur «station», l'arborescence entière à l'intérieur du répertoire «/home/station» peut être déclarée comme appartenant à l'utilisateur «root» afin qu'aucun nouveau fichier ou répertoire ne puisse plus y être créé par l'opérateur de la

station (à l'exception toutefois du répertoire «/home/station/Images» ainsi que de ses contenus «green.png», «red.png» et «test.jpg» (correspondant aux arrières-plans de Bureau selon le résultat de l'analyse ou en l'absence d'analyse) nécessaires au bon fonctionnement du programme réalisé par Maël LESAICHERRE et devant demeurer comme appartenant à l'utilisateur «station» ainsi qu'au groupe «station»)

4.2 Projet Principal

4.2.1 Élaboration d'un Équipement Réseau sous pfSense et de son Écosystème de Production

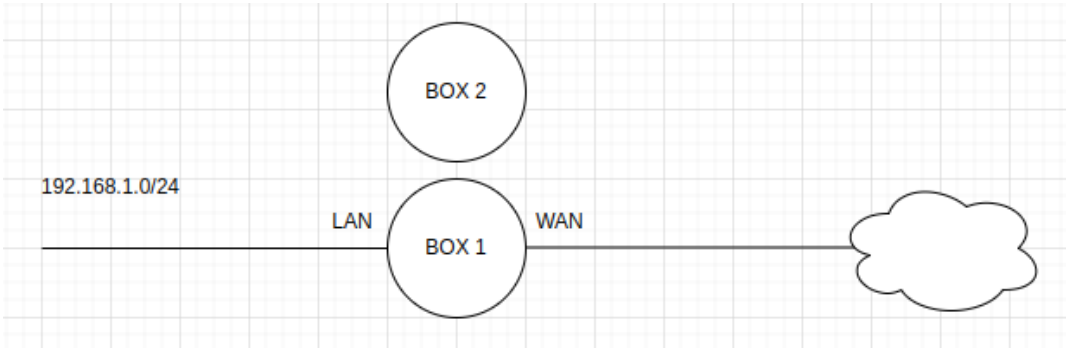
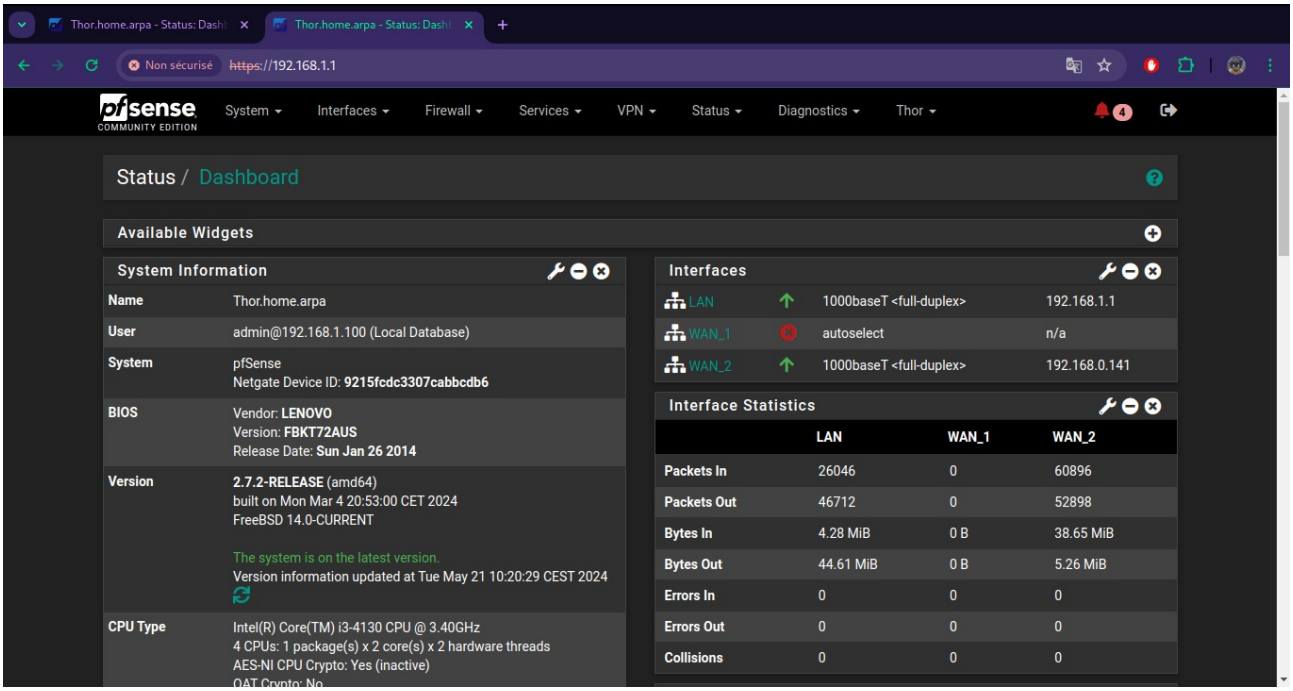
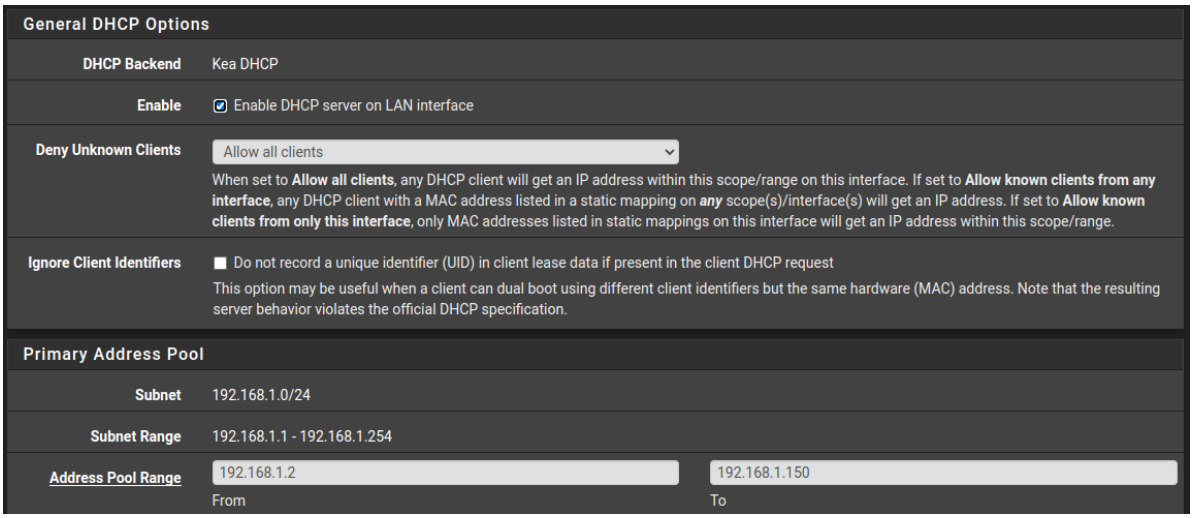


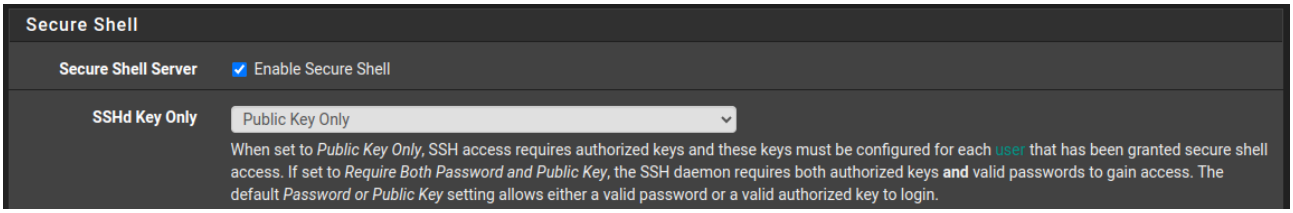
Fig. F1 : Topologie réseau avant modification : l'entièreté du réseau dépend de deux Box Internet Orange Pro v3 identiques au modèle présenté ci-dessous (une seule d'entre elles peut être raccordée au réseau et, en cas de panne de la première, la seconde doit impérativement être branchée manuellement à la place de celle-ci)

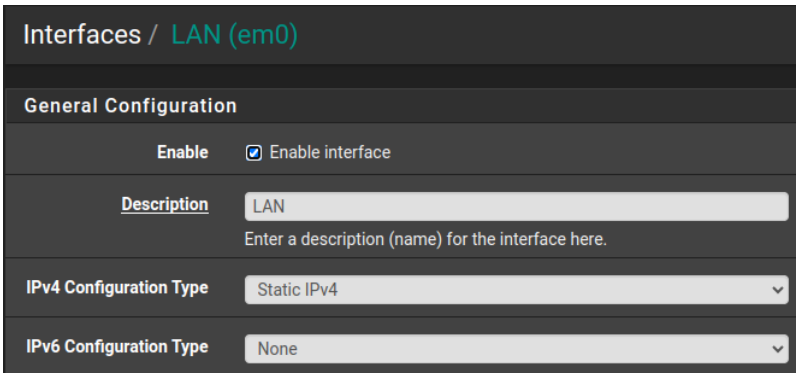
Fig. F2 : Modèle de Box Internet professionnelle Orange Pro v3

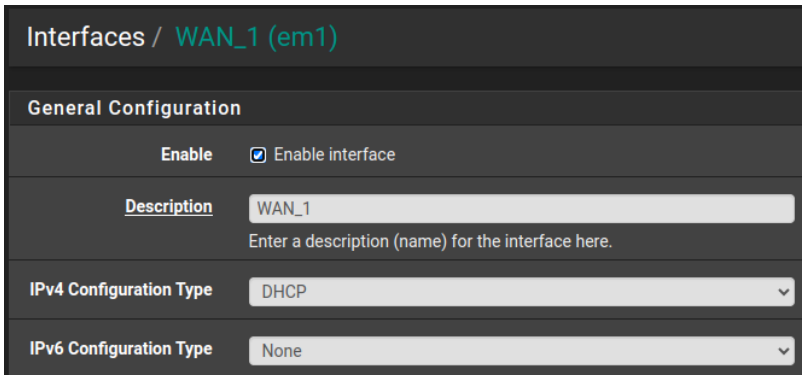
Figs. F3 et F4 (ordre respectif descendant) : Matériel utilisé pour la création d'un routeur pare-feu et de son écosystème de production : offrant une plate-forme polyvalente pouvant être transformée en équipement réseau comme en serveur de stockage (quatre ports «Serial Advanced Technology Attachment» (SATA) permettant de connecter entre autres divers supports de stockage ainsi que quatre ports de Mémoire Vive («Random Access Memory» ou RAM) disponibles, ports de ventilateurs additionnels disponibles (rappelons qu'un équipement réseau est prévu pour fonctionner 24h/24 et 7j/7, et qu'une surchauffe d'une machine entraîne une dégradation des performances, une usure prématurée des composants internes, etc.), quatre emplacements d'extensions PCI ou PCI Express («Peripheral Component Interconnect» ou «Peripheral Component Interconnect Express») utiles afin d'ajouter des interfaces réseau), deux Lenovo ThinkCentre M93 retirés du service ont été utilisés (le premier afin de créer l'équipement réseau en lui-même, et le second afin de créer un Serveur de Protocole Trivial de Transfert de Fichiers («Trivial File Transfer Protocol» ou TFTP) de sauvegarde de configuration destiné à maximiser la robustesse et la durée de vie de l'appareil réseau tout en facilitant une éventuelle reprise d'activité après sinistre) (toujours dans l'objectif de créer les équipements les plus résilients possibles, deux disques de capacité égale ont été inclus dans l'équipement réseau et quatre dans le serveur TFTP (nous étudierons ces points plus en détail plus bas)), ainsi qu'une carte réseau double Intel D33682 préférée aux multiples cartes réseau simples pour son intégration directe de deux interfaces et pour ses meilleures capacités en termes de vitesse de transfert de paquets

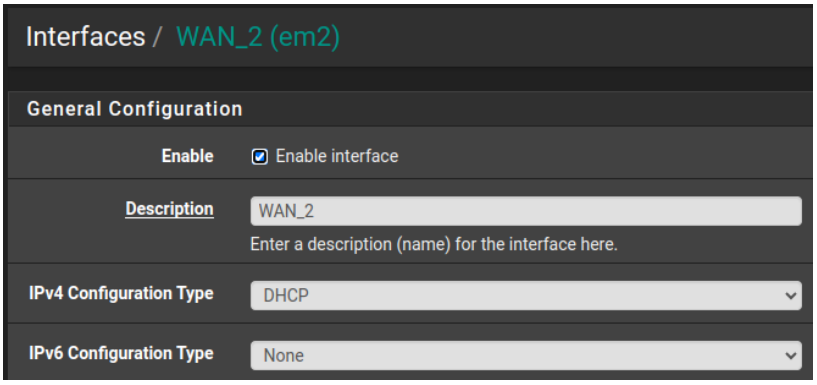


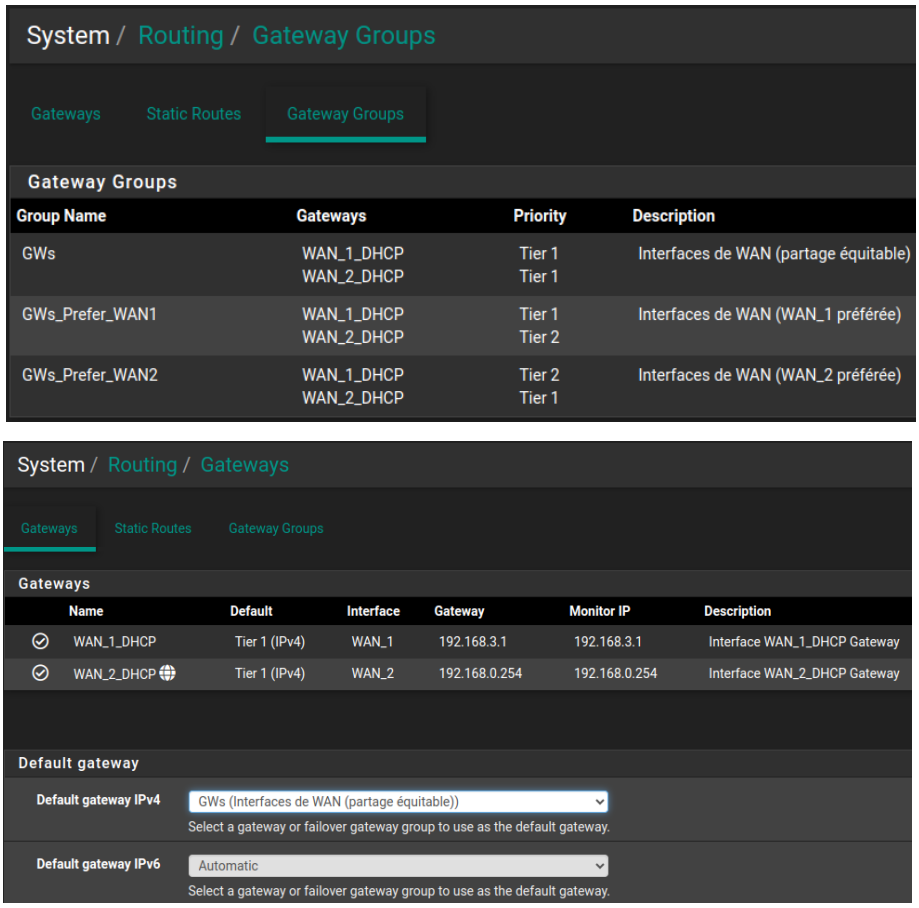

General DHCP Options
DHCP Backend
Kea DHCP
Enable
Enable DHCP server on LAN interface
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Client Identifiers
Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
Primary Address Pool
Subnet
192.168.1.0/24
Subnet Range
192.168.1.1 - 192.168.1.254
Address Pool Range
192.168.1.2
From
192.168.1.150
To


Secure Shell
Secure Shell Server
Enable Secure Shell
SSHd Key Only
Public Key Only
When set to Public Key Only, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to Require Both Password and Public Key, the SSH daemon requires both authorized keys and valid passwords to gain access. The default Password or Public Key setting allows either a valid password or a valid authorized key to login.


Interfaces / LAN (em0)
General Configuration
Enable
Enable interface
Description
LAN
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None


Interfaces / WAN_1 (em1)
General Configuration
Enable
Enable interface
Description
WAN_1
Enter a description (name) for the interface here.
IPv4 Configuration Type
DHCP
IPv6 Configuration Type
None


Interfaces / WAN_2 (em2)
General Configuration
Enable
Enable interface
Description
WAN_2
Enter a description (name) for the interface here.
IPv4 Configuration Type
DHCP
IPv6 Configuration Type
None



Figs. F5, F6, F7, F8, F9, F10, F11 et F12 (ordre respectif descendant) : Suite à la sécurisation du Firmware BIOS de la machine (mot de passe administrateur afin d'y accéder, etc.) et à la familiarisation avec la logique pfSense (rappelant énormément les Travaux Pratiques réalisés sur matériel STORMSHIELD, tant du point de vue de la construction de l'interface Web que des pratiques appliquées par défaut (interface d'administration Web joignable uniquement sur l'interface LAN par défaut, etc.)), à la sécurisation de ses accès d'administration (SSH par clé publique uniquement en écoute sur l'interface LAN exclusivement, augmentation du temps de verrouillage de l'interface d'administration Web en cas de répétition de tentatives de connexion erronées et déconnexion automatique au bout de 60 minutes, etc.) et à sa configuration de base (création et affectation des interfaces, service DHCP en écoute sur l'interface LAN selon les critères donnés, etc.), sa configuration en matière de routage doit être réalisée afin de remplir le premier point du cahier des charges : différents groupes de passerelles («gateways») peuvent être programmés (pour une répartition différente au besoin : cela passe par l'utilisation de «niveaux» («tier») supérieurs, inférieurs ou égaux selon si le trafic doit emprunter préférablement une passerelle plutôt qu'une autre) et le principal groupe répartissant équitablement entre les deux passerelles disponibles peut être utilisé d'office comme passerelle par défaut IPv4 (toute configuration IPv6 ayant été désactivée car non abordée dans le cahier des charges)

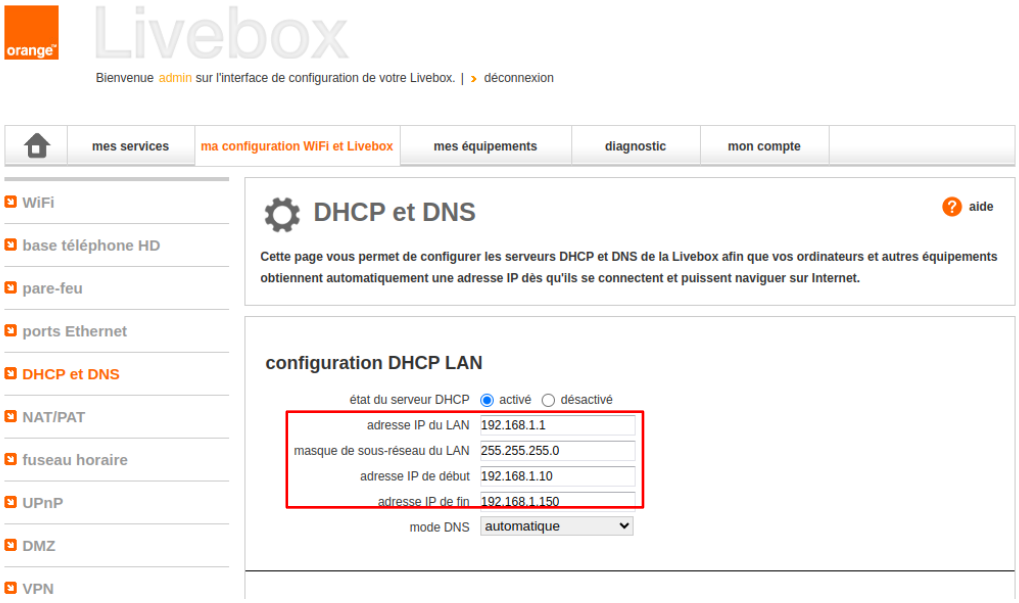
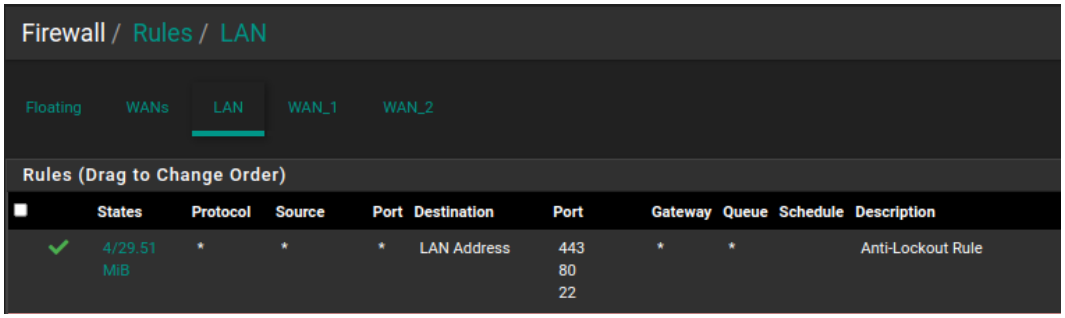
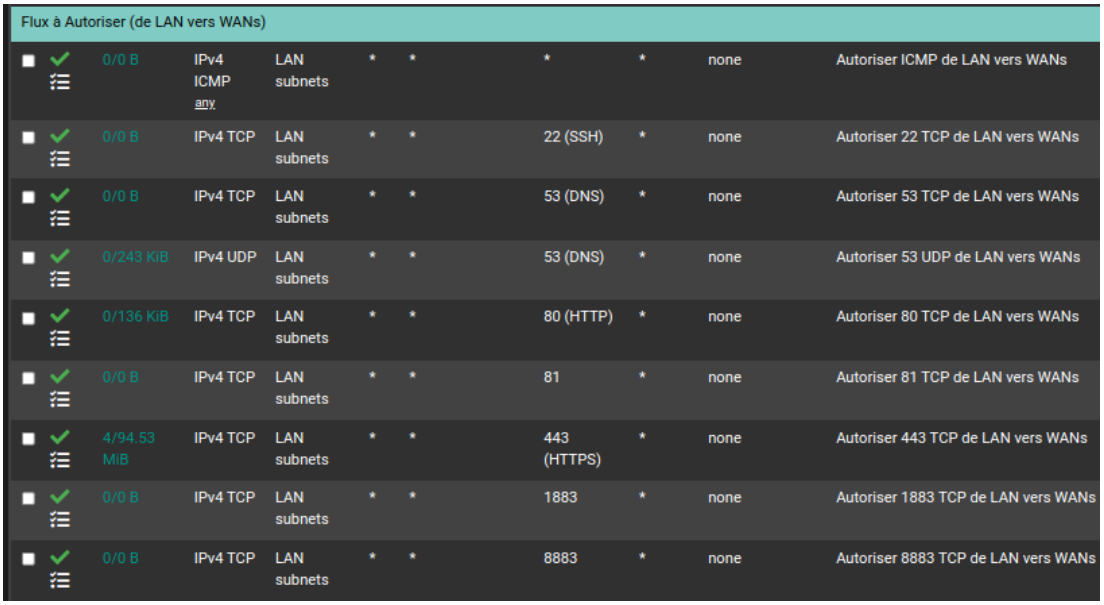
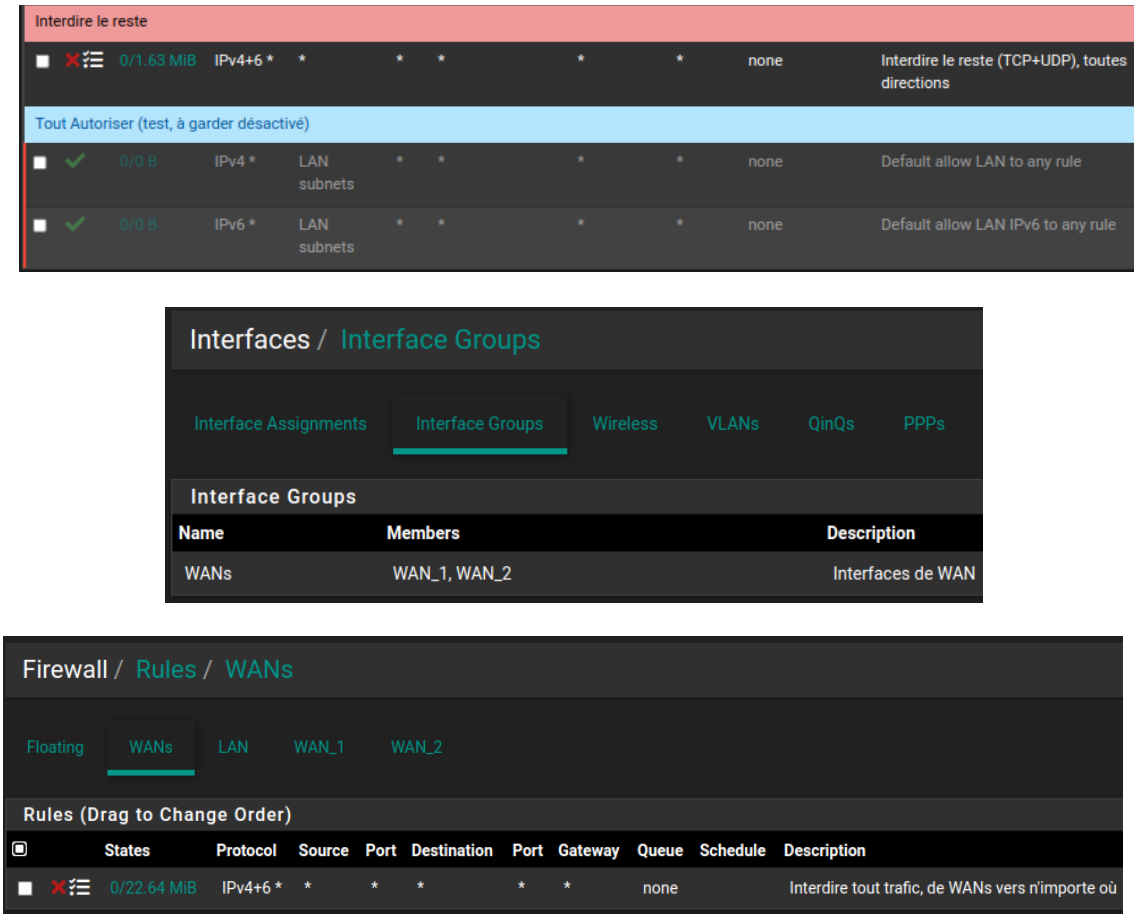


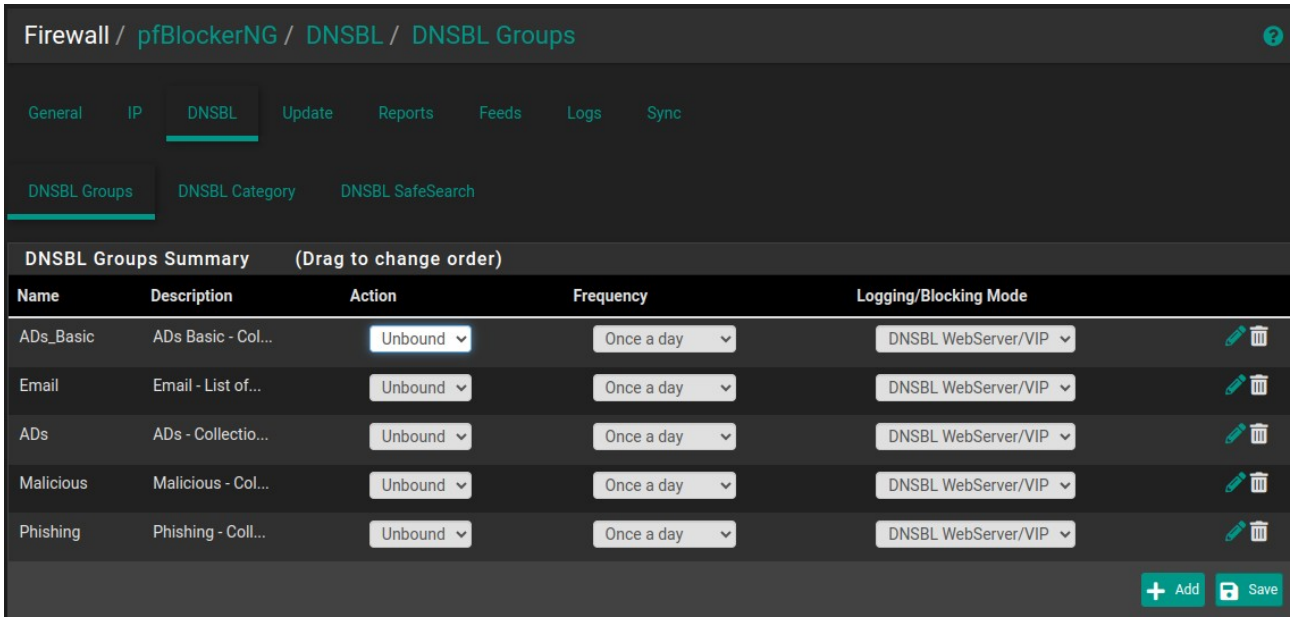
Fig. F13 : Interface d'administration Web d'une Box Internet Orange Pro v3, et sa rubrique permettant de changer le réseau IP distribué en DHCP (et donc récupéré sur les interfaces WAN du nouvel équipement réseau) sur l'interface LAN de la Box : à titre d'exemple, les réseaux 192.168.10.0/24 et 192.168.11.0/24 peuvent être distribués par les deux Box afin de conserver le réseau 192.168.1.0/24 sur l'interface LAN du nouvel équipement réseau

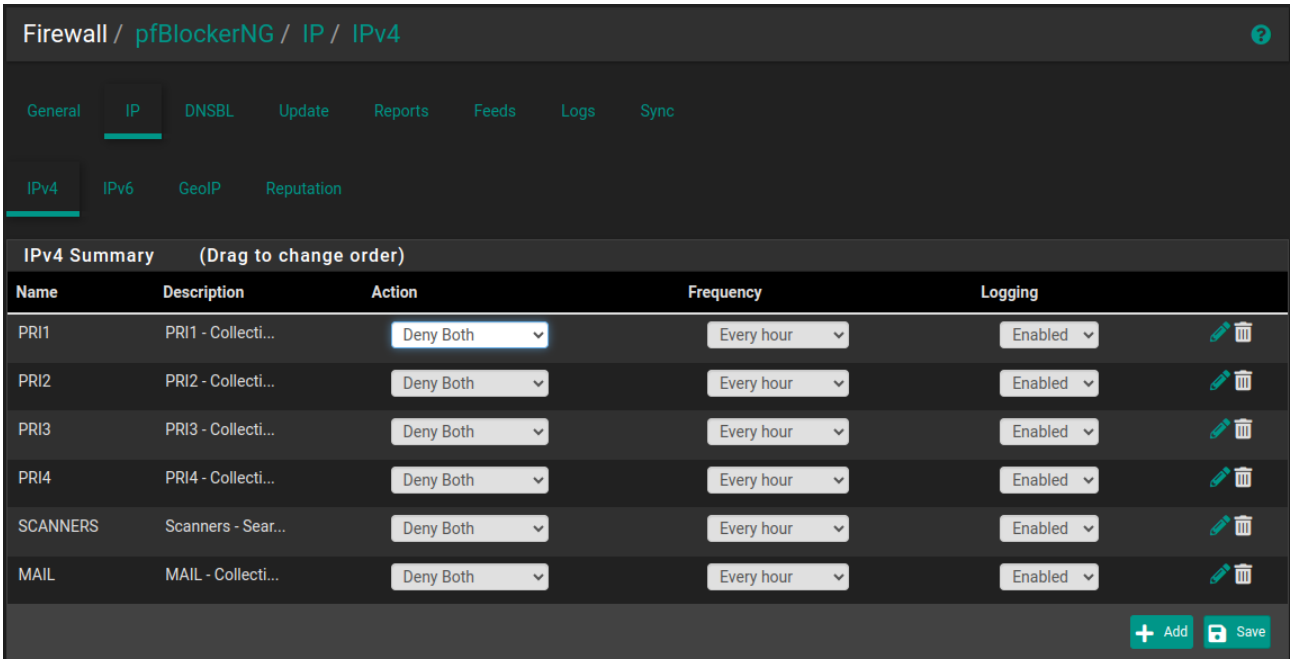


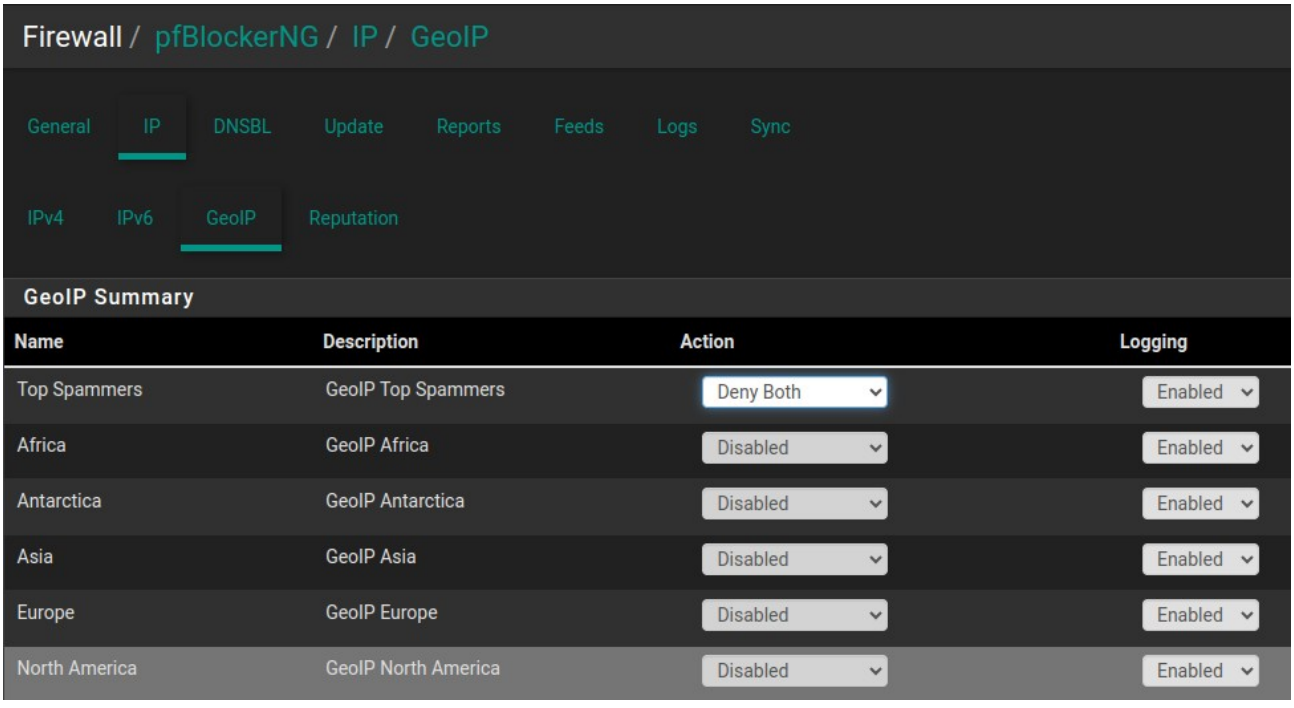


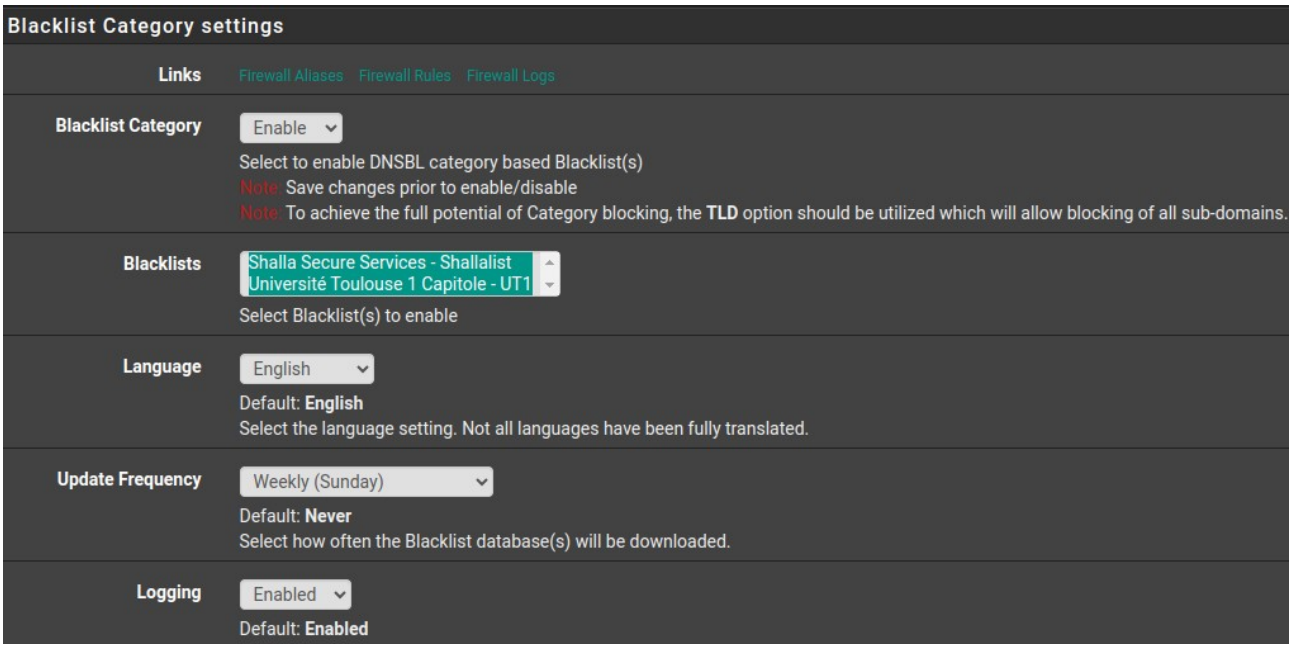


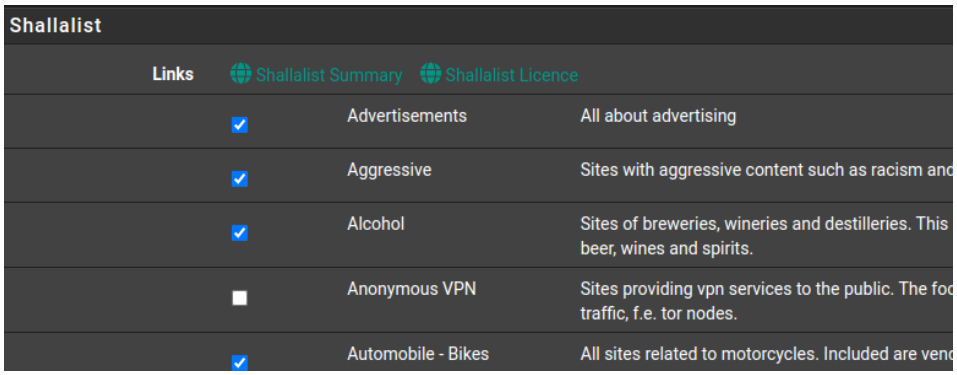
Figs. F14, F15, F16, F17 et F18 (ordre respectif descendant) : Jeu de règles de filtrage (parcourues séquentiellement de haut en bas jusqu'à ce qu'une règle corresponde, selon les pratiques habituelles du «Firewalling») mis en place dans les différentes rubriques afin d'appliquer la matrice de flux indiquée dans le cahier des charges (avec création du groupe d'interfaces «WANs» et application de la règle de filtrage requise directement sur celui-ci) ; point assez déconcertant dans la logique de configuration de pfSense en comparaison avec la logique de configuration STORMSHIELD : là où toutes les règles de filtrage sont dans une seule table (les critères d'interface d'entrée y étant alors explicitement définis) sur STORMSHIELD, sur pfSense une table de filtrage est associée à chaque interface ou groupe d'interface (chaque table concernant le trafic entrant sur l'interface correspondante) (la rubrique «Floating» comporte certes quant à elle une table de filtrage multi-interfaces comparable à celle de STORMSHIELD où chaque règle définit alors ses critères en termes d'interface d'entrée explicitement, mais cette rubrique «Floating» est décrite dans la documentation officielle pfSense comme «Réservée aux utilisateurs aguerris [...] car beaucoup plus sujette à des erreurs difficiles à déceler» et toute tentative de configuration de règles dans cette rubrique s'est effectivement avérée infructueuse pour des raisons inconnues (les règles définies y étaient pourtant logiques et sans erreurs apparentes))

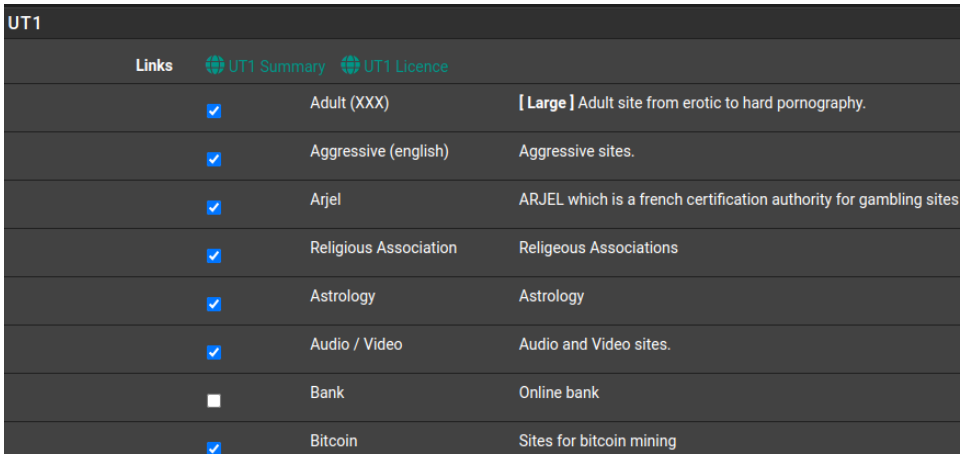

Firewall / pfBlockerNG / DNSBL / DNSBL Groups
General IP DNSBL Update Reports Feeds Logs Sync
DNSBL Groups DNSBL Category DNSBL SafeSearch
DNSBL Groups Summary (Drag to change order)
Name Description Action Frequency Logging/Blocking Mode
ADs_Basic ADs Basic - Col... Unbound Once a day DNSBL WebServer/VIP
Email Email - List of... Unbound Once a day DNSBL WebServer/VIP
ADs ADs - Collectio... Unbound Once a day DNSBL WebServer/VIP
Malicious Malicious - Col... Unbound Once a day DNSBL WebServer/VIP
Phishing Phishing - Coll... Unbound Once a day DNSBL WebServer/VIP
Add Save


Firewall / pfBlockerNG / IP / IPv4
General IP DNSBL Update Reports Feeds Logs Sync
IPv4 IPv6 GeoIP Reputation
IPv4 Summary (Drag to change order)
Name Description Action Frequency Logging
PRI1 PRI1 - Collecti... Deny Both Every hour Enabled
PRI2 PRI2 - Collecti... Deny Both Every hour Enabled
PRI3 PRI3 - Collecti... Deny Both Every hour Enabled
PRI4 PRI4 - Collecti... Deny Both Every hour Enabled
SCANNERS Scanners - Sear... Deny Both Every hour Enabled
MAIL MAIL - Collecti... Deny Both Every hour Enabled
Add Save


Firewall / pfBlockerNG / IP / GeoIP
General IP DNSBL Update Reports Feeds Logs Sync
IPv4 IPv6 GeoIP Reputation
GeoIP Summary
Name Description Action Logging
Top Spammers GeoIP Top Spammers Deny Both Enabled
Africa GeoIP Africa Disabled Enabled
Antarctica GeoIP Antarctica Disabled Enabled
Asia GeoIP Asia Disabled Enabled
Europe GeoIP Europe Disabled Enabled
North America GeoIP North America Disabled Enabled

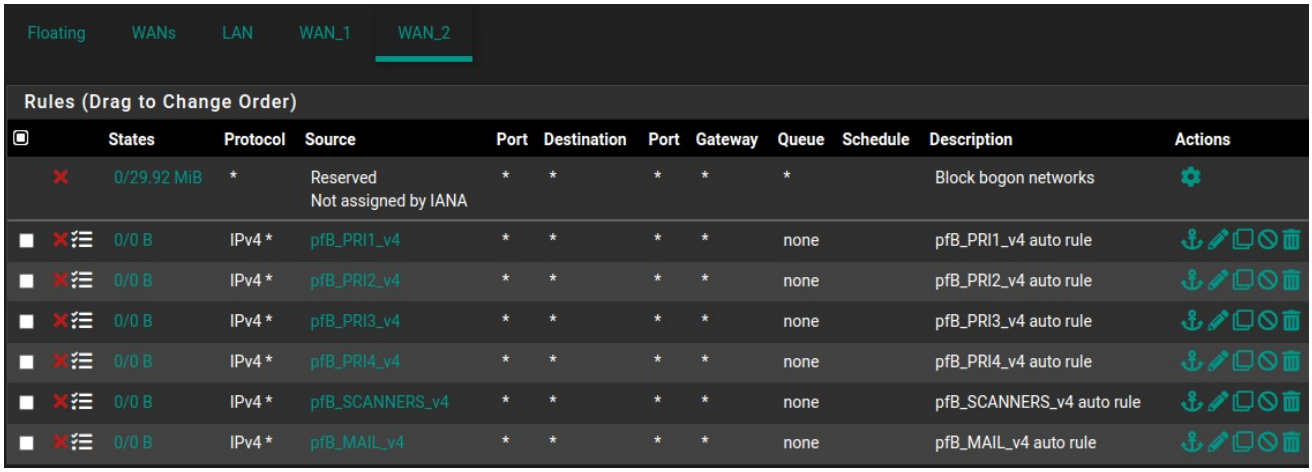






Figs. F19, F20, F21, F22, F23 et F24 (ordre respectif descendant) : Configuration suite à son installation du paquet «pfBlockerNG» permettant de réaliser le filtrage d'adresse IP de destination, de pays de destination et de nom de domaine de destination via l'ajout de listes («feeds») IP et/ou DNSBL prédéfinies et mises à jour périodiquement, tout en réglant les zones géographiques à interdire dans la catégorie «GoIP» (plutôt que d'interdire un ensemble fixe de pays tel que l'Asie (la Russie et/ou la Chine étant des pays très actifs en matière de cyberguerre mais d'autres pays de la même région tels que le Japon ou la Corée du Sud, assez pacifistes en matière de cyberguerre, ne devant pas être interdits de communication au passage), l'ensemble de pays «Top Spammers» mis à jour périodiquement peut être utilisé) et en réglant les catégories de liste noire DNSBL (plusieurs dizaines de catégories disponibles à travers deux listes possibles, mais certaines (telles que «sites gouvernementaux», cela peut être utile pour un réseau ministériel) pouvant s'avérer utiles et ne

devant pas être cochées) : en somme, cet outil crée automatiquement des règles de filtrage à part entière dans les rubriques de chacune des interfaces physiques, comme décrit ci-dessous :

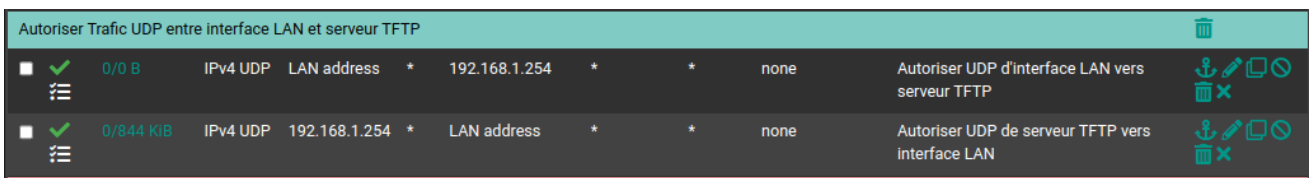


Figs. F25 et F26 (ordre respectif descendant) : Règles de filtrage automatiquement créées par l'outil «pfBlockerNG» (le jeu de règles de l'image F25, ajouté dans la table de l'interface LAN, devant être placé entre la première règle «Anti-lockout rule» (créée d'office sur pfSense afin d'éviter de bloquer malencontreusement les flux d'administration tels que Web et/ou SSH) et l'ensemble de règles «Flux à Autoriser (de LANs vers WANs)» sur les images F14 et F15 ; et le jeu de règles de l'image F26 étant quant à lui ajouté automatiquement de la même façon sur les interfaces «WAN_1» et «WAN_2» (faisant de toutes façons partie du groupe «WANs» stipulant qu'aucune connexion n'est autorisée en entrée des interfaces faisant partie de ce groupe))

30	3	*	*	*	root	sh -c '(/usr/local/sbin/pfSense-upgrade -y) > /var/log/auto_update_pfsense_cron.log 2> /var/log/auto_update_pfsense_cron.err'
0	4	*	*	*	root	sh -c '(/usr/local/sbin/pkg update -f && /usr/local/sbin/pkg upgrade -y) > /var/log/auto_update_packages_cron.log 2> /var/log/auto_update_packages_cron.err'
31	4	*	*	*	root	sh -c '(echo "put /conf/config.xml config-Thor-$(date +\%d\%m\%Y).xml" | tftp 192.168.1.254) > /var/log/auto_tftp_config_cron.log 2> /var/log/auto_tftp_config_cron.err'

```
0 4 * * * (/usr/bin/apt-get update && /usr/bin/apt-get full-upgrade -y --ignore-missing) > /var/log/auto_update_cron.log 2> /var/log/auto_update_cron.err
29 4 * * * /root/commande_creation_tftp.sh
30 4 * * * /usr/bin/systemctl restart tftpd-hpa.service
```

```
root@Odin:~# cat /root/commande_creation_tftp.sh
(/usr/bin/touch /mnt/raid/tftp/config-Thor-$(date +%d%m%Y).xml && /usr/bin/chown tftp:tftp /mnt/raid/tftp/config-Thor-$(date +%d%m%Y).xml && /usr/bin/chmod 777 /mnt/raid/tftp/config-Thor-$(date +%d%m%Y).xml) > /var/log/auto_creation_tftp_cron.log 2> /var/log/auto_creation_tftp_cron.err
root@Odin:~#
```



Figs. F27, F28, F29 et F30 (ordre respectif descendant) : Tâches quotidiennes «Cron» programmées sur le nouvel équipement réseau afin de parfaire sa configuration (chacune des commandes redirige ses sorties standard et d'erreur vers de nouveaux fichiers de journaux système personnalisés, raison pour laquelle celles-ci sont longues et complexes, mais le contenu utile de la commande (c'est-à-dire la commande utilisée dans sa plus simple expression) est facilement repérable entre parenthèses) : après une mise à jour de son système d'exploitation à 3:30 du matin (cette opération, si une nouvelle version du système d'exploitation est trouvée, aura pour effet de redémarrer l'appareil, raison pour laquelle une heure creuse à laquelle le réseau n'est normalement pas sollicité a été sélectionnée ; ce comportement est toutefois préférable à un équipement réseau ne mettant tout simplement pas à jour son système d'exploitation et ne bénéficiant pas des derniers correctifs de sécurité) et une mise à jour des paquets installés (c'est-à-dire le paquet «ShellCMD» permettant d'exécuter automatiquement des commandes au démarrage de la machine (celui-ci a été utilisé afin de s'assurer qu'une connexion console à l'appareil bénéficiera toujours d'un clavier AZERTY), ledit paquet «pfBlockerNG» ainsi que le paquet «Cron» permettant de régler lesdites tâches quotidiennes) à 4:00 du matin ne nécessitant aucun redémarrage, l'appareil envoie à 4:31 du matin une copie de son fichier de configuration au serveur TFTP (celui-ci bénéficiera toujours de la même IP, une entrée DHCP statique ayant été ajoutée sur l'appareil réseau avec l'adresse MAC du serveur afin d'assurer ce comportement), qui, de son côté, après avoir mis à jour ses paquets à 4:00 du matin, crée un fichier vide sur le point de montage Linux du RAID 5 («/mnt/raid/tftp/») nommé comme le fichier de configuration qu'il va recevoir (une mécanique de sécurité intrinsèque à TFTP est qu'un fichier ne peut être envoyé sur le serveur que si un fichier portant le même nom existe déjà : raison pour laquelle une tâche «Cron» sur le serveur crée un fichier vide que la tâche «Cron» de l'équipement réseau va donc venir remplacer par un fichier rempli) et lui applique les bons droits (appartenance à l'utilisateur et au groupe «tftp» avec tous les droits pour tous les utilisateurs) avant de redémarrer le service TFTP ; ce serveur TFTP a été créé en installant le paquet «tftpd-hpa» et a nécessité l'ajout de deux nouvelles règles de filtrage dans la table LAN (image F29) placées entre la rubrique «Flux à Autoriser (de LANs vers WANs)» et la rubrique «Interdire le Reste» (images F15 et F16) destinées à accepter tout trafic UDP entre l'interface LAN et le serveur TFTP (en effet, le fonctionnement intrinsèque de TFTP implique que la connexion pour le transfert de données se fasse entre deux ports UDP aléatoires, or, les bonnes pratiques du «Firewalling» ayant été mises en place sur l'interface LAN de l'équipement réseau, tout trafic entrant sur l'interface LAN n'ayant pas explicitement été déclaré comme devant être autorisé est interdit : ces deux règles sont donc impératives à la communication entre l'équipement réseau et le serveur TFTP, et particulièrement la deuxième) ; il convient de noter que ce serveur TFTP est donc destiné à héberger une grande quantité de fichiers de configuration datés afin de pouvoir, comme indiqué dans la documentation utilisateur, revenir à n'importe quelle configuration précédente en cas d'erreur d'un administrateur local, en cas de besoin de duplication de la machine, etc. (une quantité si prodigieuse de mémoire a été prévue sur ce serveur car l'idée initiale était que l'équipement réseau envoie, en plus de son fichier de configuration, une image disque complète directement utilisable ; néanmoins, réaliser une copie d'un disque en cours d'utilisation (qui plus est, un disque devant se cloner lui-même : le disque devant dans l'idéal être cloné n'étant autre que celui hébergeant pfSense) est non seulement difficile mais surtout dangereux pour le disque source : cette partie du projet a donc été abandonnée au profit de la récupération quotidienne des fichiers de configuration)

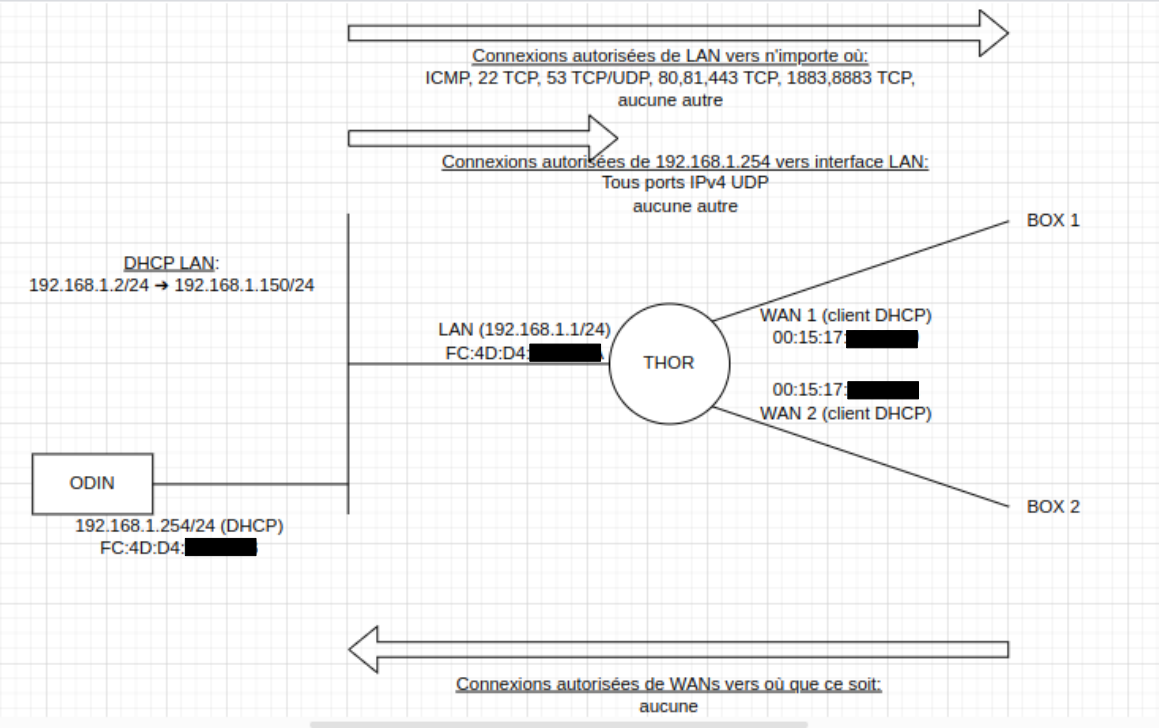


Fig. F31 : Topologie finalement obtenue post-modification avec matrice de flux («Thor» et «Odin» étant les noms de code donnés respectivement à l'équipement réseau et au serveur de sauvegarde TFTP)