PPE3-M5 « SporTif »

Mission :

Créer un système d'authentification pour pouvoir accéder à internet, utilisation de filtrage pour interdire certaines IP de se connecter (niveau 3 & 4), visuels du journal log et sauvegarde sur un ftp (sauvegarde automatique).

Besoins :

- Exploitation : Afficher et gérer l'activité des équipements présents sur le réseau de consultation. (Authentification -> Activité)

- Administration du portail : Connexion sur un serveur d'annuaire, activation du service d'administration à distance SSH. (Interne)

- Consultation des statistiques d'exploitation du réseau de consultation, de la bande passante et du volume des connexions. (Statistiques -> Trafic global)

- Consultation des événements du pare-feu. (Sauvegarde -> Journaux d'imputabilité)

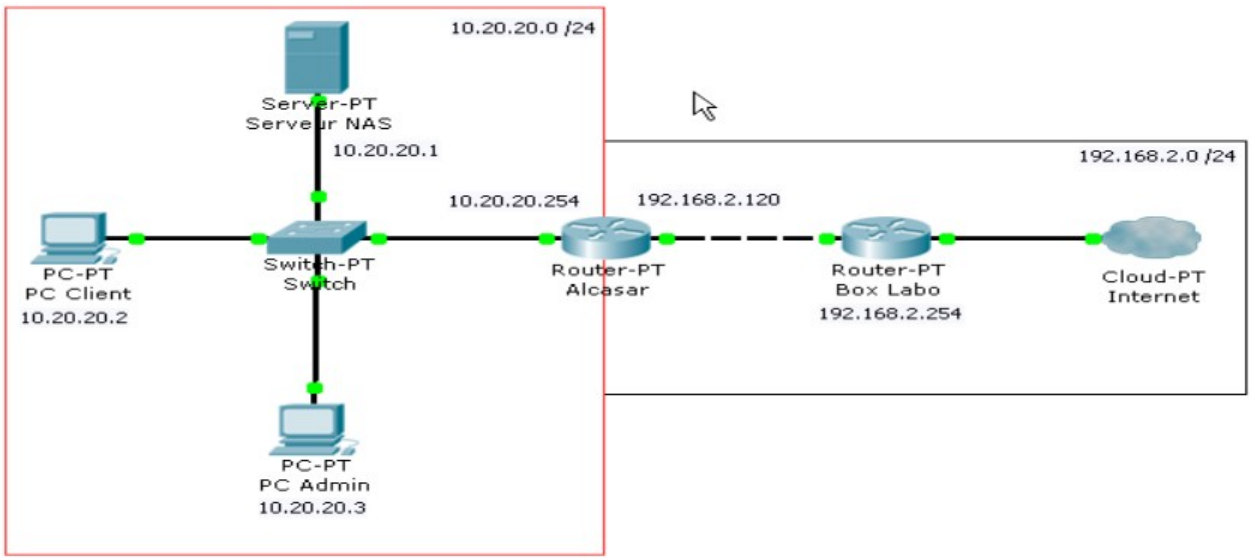
- Récupération des fichiers journaux pour archivage. Ces fichiers : contiennent des traces des connexions. Ils constituent ainsi les preuves de l'activité du réseau de consultation. Ils doivent pouvoir être chiffrés.
  (Sauvegardes -> Journaux d'imputabilité)

- Activation et désactivation de l'antivirus du flux WEB.

- (Dé)Activation ,modification ou mise à jour de "blacklist" de domaines ou d'URL filtrés. (Filtrage -> Liste noire)

- (Dé)Activation ou modification du filtrage réseau (filtrage de protocoles)
  (Filtrage -> Protocoles)

Schéma Réseau :



Besoins matériel :

→ Un PC Admin pour se connecter par interface WEB d'Alcasar.
→ Un PC Client pour se connecter à Internet.
→ Un serveur NAS pour y stocker les logs.
→ Un serveur Linux Mageia Alcasar agissant comme portail captif.
→ La box du labo qui permet la connexion à internet.

Informations complémentaire :

Alcasar : Admin Admin

IP extérieure : 192.168.2.120

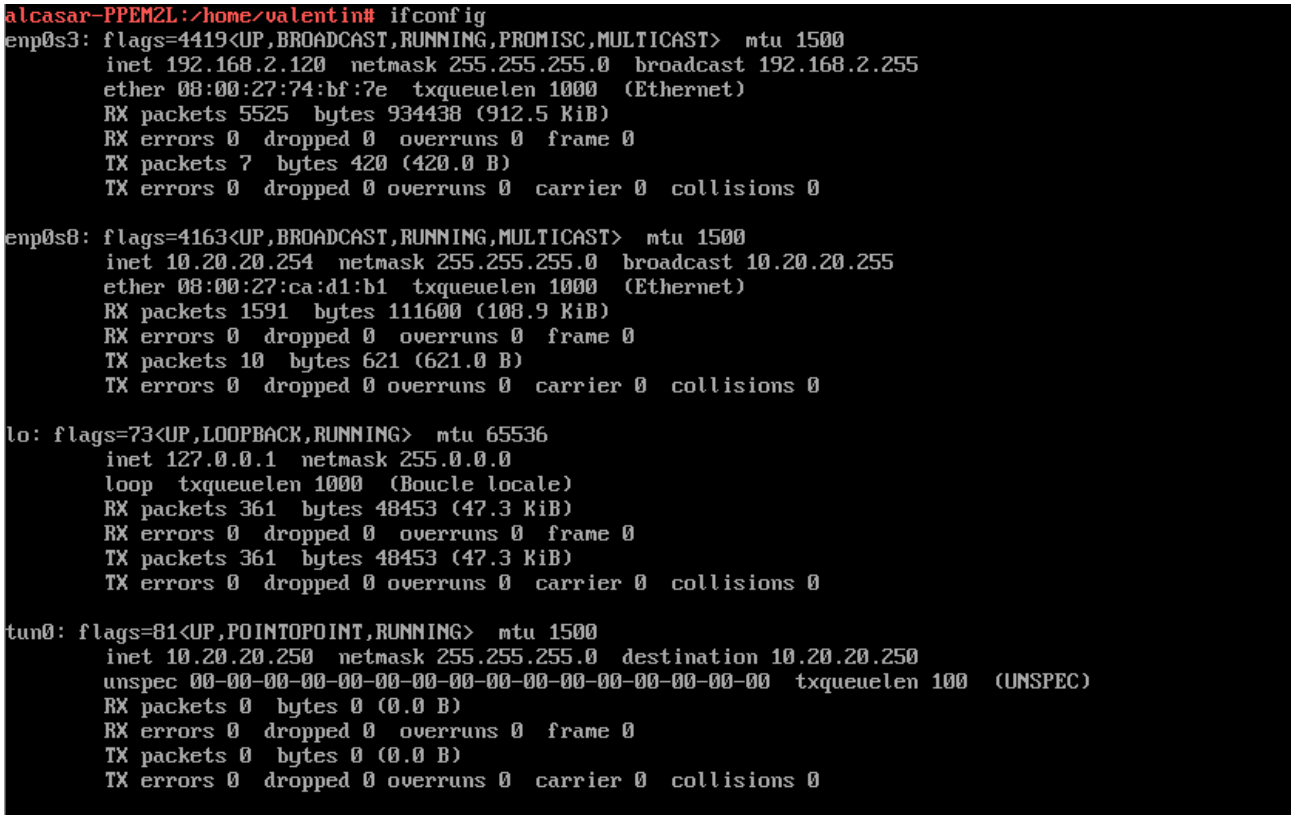
IP de consultation : 10.20.20.254

DNS : 8.8.8.8

DNS SECONDAIRE : 1.1.1.1

Après avoir téléchargé, décompressé puis installé Alcasar (mageia) sur un serveur Linux, ce dernier doit être administré en lui mettant deux adresses ip :

- 192.168.2.120 pour le réseau extérieur
- 10.20.20.254 pour le réseau de consultation
-



Nous avons alors fais un test des ping :

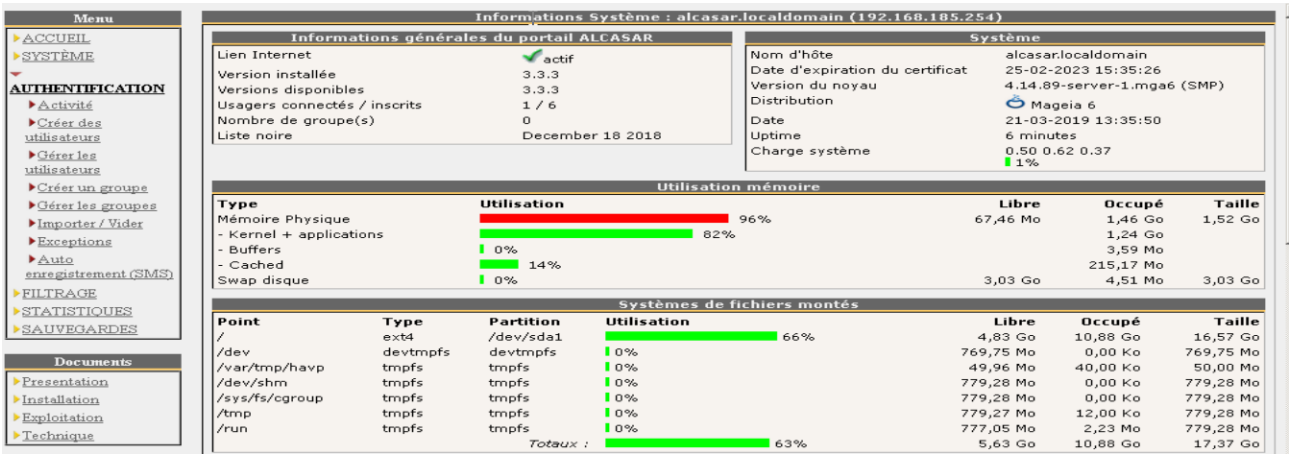
TABLEAU DE TEST DES PING

	PC ADMIN	PC CLIENT	NAS QNAP	ALCASAR	INTERNET
PC ADMIN	OK	OK	OK	OK	OK
PC CLIENT	OK	OK	OK	OK	OK
NAS QNAP	OK	OK	OK	OK	OK
ALCASAR	OK	OK	OK	OK	OK
INTERNET	OK	OK	OK	OK	OK

Ensuite, il faut se connecter au serveur via un navigateur web en tapant l'adresse ip du serveur /acc :

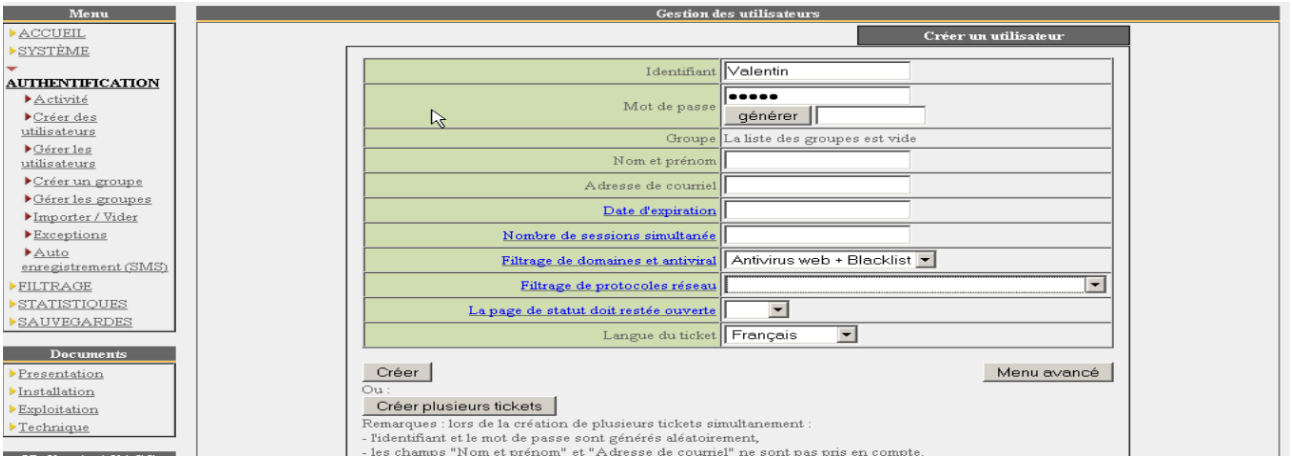
On arrive alors sur une page d'accueil :

En ouvrant une session internet et en se connectant, on arrive alors sur la page d'administration d'Alcasar :



On y voit alors certaines informations telles que l'utilisation de la mémoire, des informations systèmes et d'autres plus générales comme l'état de la liaison internet.

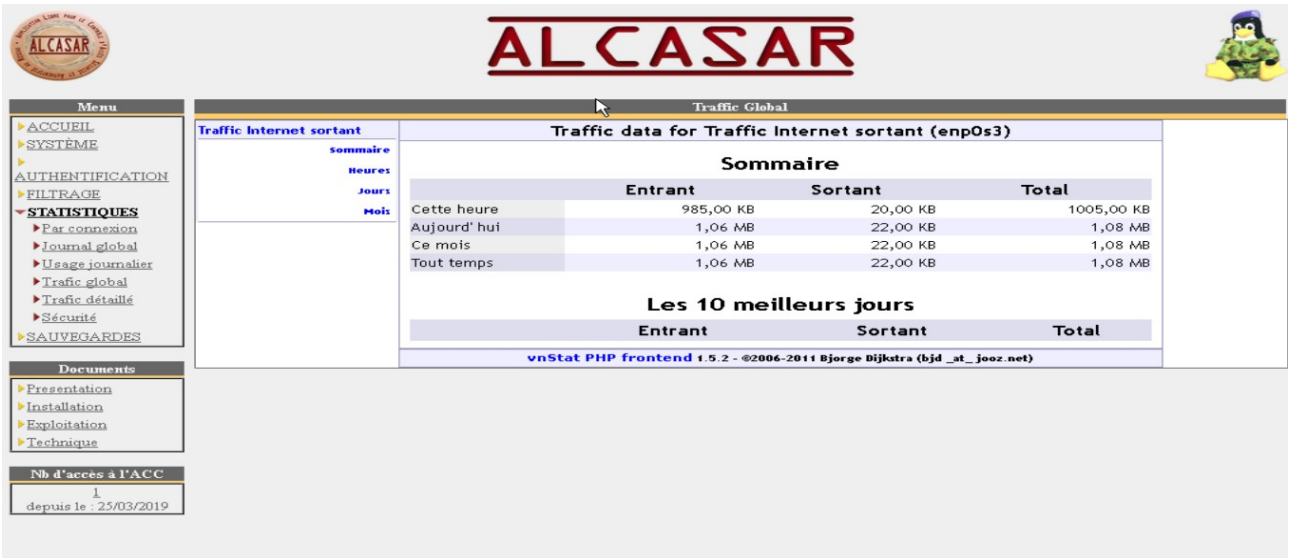
Pour la gestion des utilisateurs, nous pouvions simplement les créer un par un directement depuis l'administration d'Alcasar en nous rendant dans l'onglet " Authentification > Créer des utilisateurs ", il n'y a alors pas besoin d'utiliser un service d'annuaire comme LDAP ou AD voire Radius ou encore un fichier CSV :



Pour afficher et gérer l'activité des équipements présents sur le réseau de consultation, il faut se rendre dans l'onglet " Authentification > Activité " :

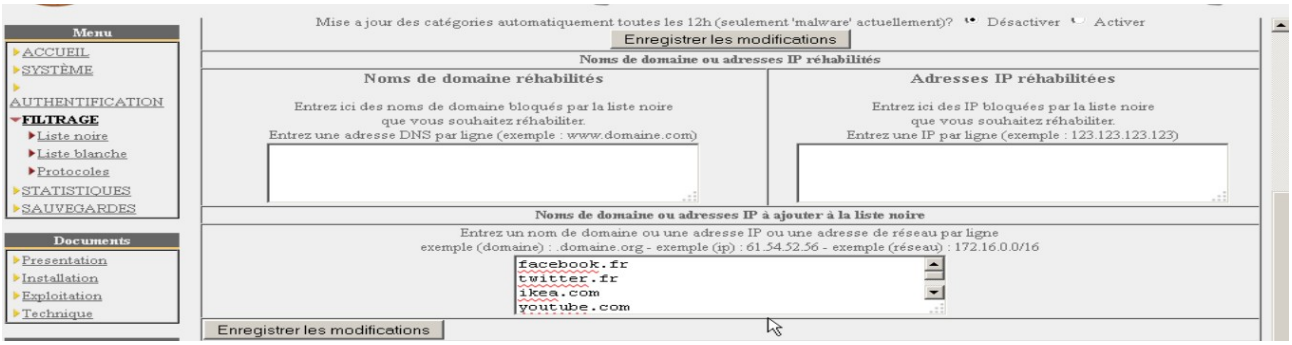
→ Cette page permet de voir toutes les adresses ip et mac qui ont essayé d'accéder à internet depuis le réseau de consultation.

Pour la consultation des statistiques d'exploitation du réseau de consultation, de la bande passante et du volume des connexions, il faut se rendre dans l'onglet « Statistiques → Trafic global » :

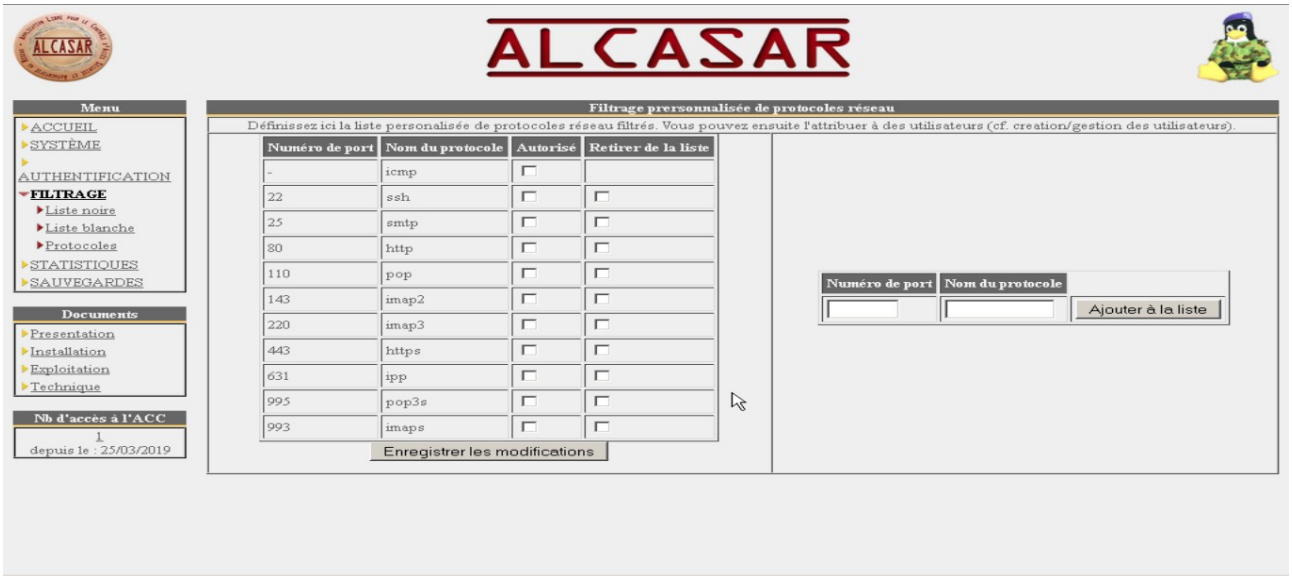


→ Depuis cette page, on peut ainsi voir le débit utilisé sur le trafic sortant (vers Internet) des utilisateurs.

En matière de filtrage, une liste noir est intégrée directement au système d'Alcasar, pour l'utiliser, il faut se rendre dans l'onglet "Filtrage > Liste noire", on peut alors y définir des adresses ip ou des noms de domaines auxquels les utilisateurs ne pourront pas se connecter :

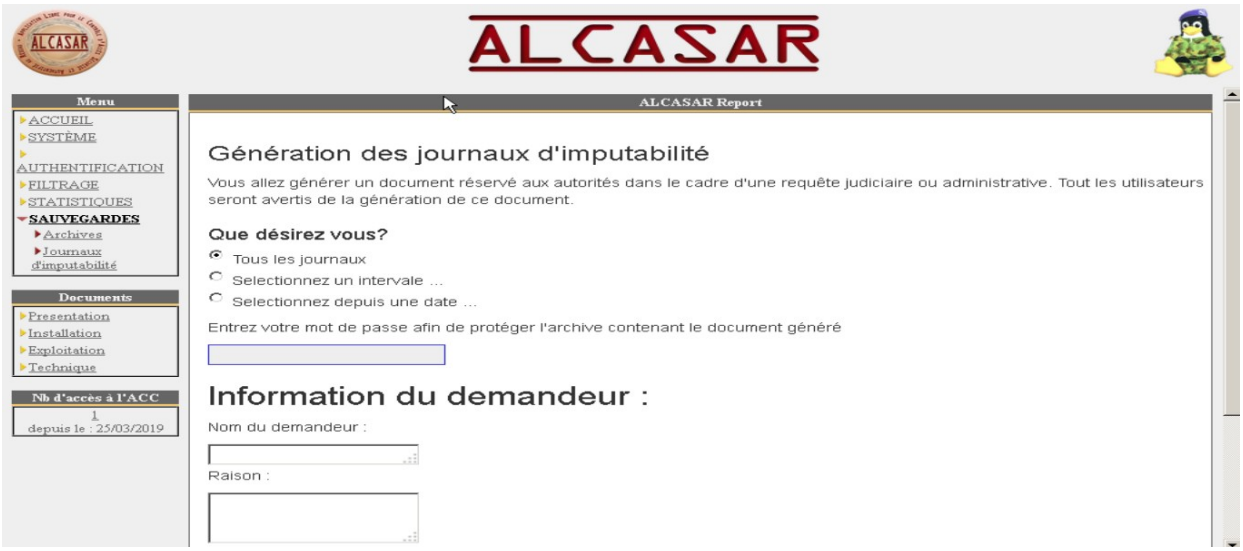


De plus, il est également possible de réaliser un filtrage par protocoles dans l'onglet « Filtrage > Protocoles » :



→ Il suffit alors de cocher « Autorisé » ou « Retirer de la liste » pour définir les protocoles autorisés ou non.

Pour la consultation des événements du pare-feu ou la récupération des fichiers journaux pour archivage, il faut se rendre dans l'onglet « Sauvegarde → Journaux d'imputabilité » :



Il faut alors remplir un formulaire pour récupérer les logs. On peut alors aller les sauvegarder sur le NAS manuellement.