

PPE3-M5 « SporTif »

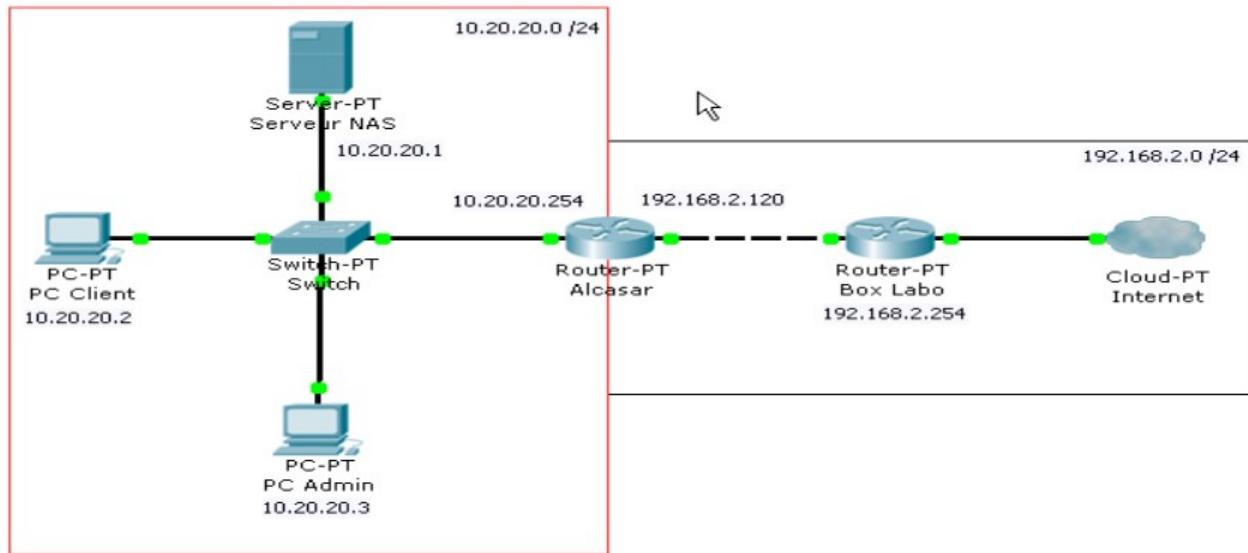
Mission :

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
-

```
alcasar-PPEM2L:/home/valentin# ifconfig
enp0s3: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
        inet 192.168.2.120 netmask 255.255.255.0 broadcast 192.168.2.255
          ether 08:00:27:74:bf:7e txqueuelen 1000 (Ethernet)
            RX packets 5525 bytes 934438 (912.5 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 7 bytes 420 (420.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.20.20.254 netmask 255.255.255.0 broadcast 10.20.20.255
          ether 08:00:27:ca:d1:b1 txqueuelen 1000 (Ethernet)
            RX packets 1591 bytes 111600 (108.9 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 10 bytes 621 (621.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
          loop txqueuelen 1000 (Boucle locale)
            RX packets 361 bytes 48453 (47.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 361 bytes 48453 (47.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=81<UP,POINTOPOINT,RUNNING> mtu 1500
        inet 10.20.20.250 netmask 255.255.255.0 destination 10.20.20.250
          unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
            RX packets 0 bytes 0 (0.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 0 bytes 0 (0.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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 :

10.20.20.254/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 :

The screenshot shows the Alcasar administration interface. On the left is a sidebar with a 'Menu' section containing links like ACCUEIL, SYSTEME, AUTHENTICATION, FILTRAGE, STATISTIQUES, and SAUVEGARDES. Below it is a 'Documents' section with links to Presentation, Installation, Exploitation, and Technique.

The main content area is titled 'Informations Système : alcasar.localdomain (192.168.185.254)'. It has three main sections:

- Informations générales du portail ALCASAR:**
 - Lien Internet: actif
 - Version installée: 3.3.3
 - Versions disponibles: 3.3.3
 - Usagers connectés / inscrits: 1 / 6
 - Nombre de groupe(s): 0
 - Dernière mise à jour: December 18 2018
- Système:**
 - Nom d'hôte: alcasar.localdomain
 - Date d'expiration du certificat: 25-02-2023 15:35:26
 - Version du noyau: 4.14.89-server-1.mga6 (SMP)
 - Distribution: Mageia 6
 - Date: 21-03-2019 13:35:50
 - Uptime: 6 minutes
 - Charge système: 0.50 0.62 0.37 (1%)
- Utilisation mémoire:**

Type	Utilisation	Libre	Occupé	Taille
Mémoire Physique	96%	67,46 Mo	1,46 Go	1,52 Go
- Kernel + applications	82%		1,24 Go	
- Buffers	0%		3,59 Mo	
- Cached	14%		215,17 Mo	
Swap disque	0%	3,03 Go	4,51 Mo	3,03 Go
- Systèmes de fichiers montés:**

Point	Type	Partition	Utilisation	Libre	Occupé	Taille
/	ext4	/dev/sda1	66%	4,83 Go	10,88 Go	16,57 Go
/dev	devtmpfs	devtmpfs	0%	769,75 Mo	0,00 Ko	769,75 Mo
/var/tmp/havp	tmpfs	tmpfs	0%	49,96 Mo	40,00 Ko	50,00 Mo
/dev/shm	tmpfs	tmpfs	0%	779,28 Mo	0,00 Ko	779,28 Mo
/sys/fs/cgroup	tmpfs	tmpfs	0%	779,28 Mo	0,00 Ko	779,28 Mo
/tmp	tmpfs	tmpfs	0%	779,27 Mo	12,00 Ko	779,28 Mo
/run	tmpfs	tmpfs	0%	777,05 Mo	2,23 Mo	779,28 Mo
Totaux :				5,63 Go	10,88 Go	17,37 Go

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 "AUTHENTICATION > 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 :

The screenshot shows the 'Créer un utilisateur' (Create user) form. The sidebar on the left is identical to the previous one. The main form fields are:

- Identifiant: Valentin
- Mot de passe: (redacted)
- Groupe: La liste des groupes est vide
- Nom et prénom: (redacted)
- Adresse de courriel: (redacted)
- Date d'expiration: (redacted)
- Nombre de sessions simultanées: (redacted)
- Filtrage de domaines et antivirus: Antivirus web + Blacklist
- Filtrage de protocoles réseau: (redacted)
- La page de statut doit restée ouverte: (redacted)
- Langue du ticket: Français

At the bottom, there are buttons for 'Créer' (Create), 'Ou:' (Or), and 'Créer plusieurs tickets' (Create multiple tickets). A note at the bottom states: "Remarques : lors de la création de plusieurs tickets simultanément : - l'identifiant et le mot de passe sont générés aléatoirement, - les champs "Nom et prénom" et "Adresse de courriel" ne sont pas pris en compte."

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

Activité sur le réseau de consultation				
Cette page est rafraîchie toutes les 30 secondes				
#	Adresse IP	Adresse MAC	Usager	Action
1	10.20.20.30	C8-D3-FF-E2-19-17 (Unknown)		Dissocier @IP Autoriser temporairement
2	10.20.20.32	08-00-27-F6-57-7A (CADMUS COMPUTER SYSTEMS)		Dissocier @IP Autoriser temporairement
3	10.20.20.10	08-00-27-D1-BC-43 (CADMUS COMPUTER SYSTEMS)		Dissocier @IP Autoriser temporairement
4	10.20.20.6	08-00-27-D1-94-6F (CADMUS COMPUTER SYSTEMS)		Dissocier @IP Autoriser temporairement
5	10.20.20.34	08-00-27-B9-F7-E2 (CADMUS COMPUTER SYSTEMS)		Dissocier @IP Autoriser temporairement
6	10.20.20.1	08-00-27-7A-CD-53 (CADMUS COMPUTER SYSTEMS)	ALCASAR system	
7	10.20.20.11	08-00-27-38-58-87 (CADMUS COMPUTER SYSTEMS)		Dissocier @IP Autoriser temporairement
8	10.20.20.20	F4-30-B9-70-1C-D0 (Unknown)		Dissocier @IP Autoriser temporairement

→ 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 » :

Traffic data for Traffic Internet sortant (enp0s3)			
Sommaire			
	Entrant	Sortant	Total
Cette heure	985,00 KB	20,00 KB	1005,00 KB
Aujourd' hui	1,06 MB	22,00 KB	1,08 MB
Ce mois	1,06 MB	22,00 KB	1,08 MB
Tout temps	1,06 MB	22,00 KB	1,08 MB

Les 10 meilleurs jours			
	Entrant	Sortant	Total
1	Depuis le : 25/03/2019		

→ 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 » :

Numéro de port	Nom du protocole	Autorisé	Retirer de la liste
-	icmp	<input type="checkbox"/>	<input type="checkbox"/>
22	ssh	<input type="checkbox"/>	<input type="checkbox"/>
25	smtpt	<input type="checkbox"/>	<input type="checkbox"/>
80	http	<input type="checkbox"/>	<input type="checkbox"/>
110	pop	<input type="checkbox"/>	<input type="checkbox"/>
143	imap2	<input type="checkbox"/>	<input type="checkbox"/>
220	imap3	<input type="checkbox"/>	<input type="checkbox"/>
443	https	<input type="checkbox"/>	<input type="checkbox"/>
631	ipp	<input type="checkbox"/>	<input type="checkbox"/>
995	pop3s	<input type="checkbox"/>	<input type="checkbox"/>
993	imap s	<input type="checkbox"/>	<input type="checkbox"/>

→ 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 » :

The screenshot shows the ALCASAR software interface. At the top left is the ALCASAR logo. In the center is the large red ALCASAR logo. At the top right is a small cartoon penguin icon. The main window title is "ALCASAR Report".

Génération des journaux d'imputabilité

You allez générer un document réservé aux autorités dans le cadre d'une requête judiciaire ou administrative. Tout les utilisateurs seront avertis de la génération de ce document.

Que désirez vous?

Tous les journaux
 Selectionnez un intervalle ...
 Selectionnez depuis une date ...

Entrez votre mot de passe afin de protéger l'archive contenant le document générée

Information du demandeur :

Nom du demandeur : [Text input field]

Raison : [Text input field]

On the left sidebar, under "Menu", the "SAUVEGARDES" section is expanded, showing "Archives", "Journaux d'imputabilité", "Documents", "Présentation", "Installation", "Exploitation", and "Technique". Under "Nb d'accès à l'ACC", it says "1 depuis le : 25/03/2019".

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