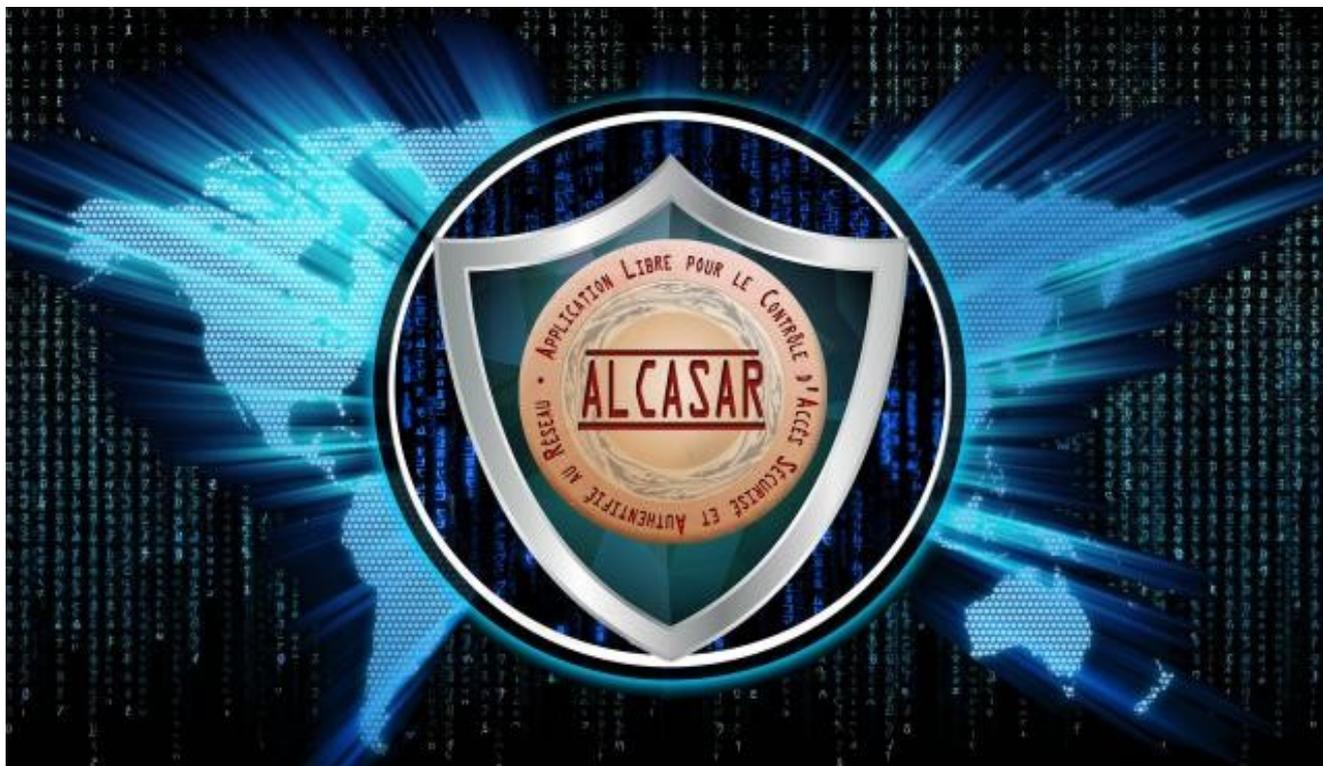


ALCASAR : projet libre et gratuit de gestion des accès à Internet
ALCASAR : a free and open source Internet access management project



www.alcasar.net



Documentation technique

| | |
|---|--|
| Projet : Gestionnaire d'accès à Internet | Auteur : Rexy with helps by alcasar team |
| Objet : Documentation technique du projet | Version : 3.6.1 |
| Mots clés : Contrôleur d'accès au réseau, Network Access Control (NAC), portail captif, captive portal, coovachilli | Date : mars 2024 |

Table des matières

| | |
|--|----|
| 1 - Rappel de l'architecture..... | 3 |
| 2 - Choix des constituants..... | 3 |
| 2.1 - La passerelle d'interception..... | 3 |
| 2.2 - Les autres constituants..... | 4 |
| 3 - Architecture :..... | 5 |
| 4 - Fonction « interception / authentification / autorisation »..... | 7 |
| 4.1 - Le portail captif et client radius..... | 8 |
| 4.2 - Base de données des utilisateurs..... | 10 |
| 4.3 - Le serveur Radius..... | 15 |
| 5 - Fonction « traçabilité et imputabilité »..... | 19 |
| 5.1 - Journalisation principale..... | 19 |
| 5.2 - journalisation accessoire..... | 20 |
| 5.3 - Constitution de l'archive de traçabilité..... | 20 |
| 6 - Fonction « filtrage »..... | 21 |
| 6.1 - Filtrage de protocoles réseau..... | 21 |
| 6.2 - Filtrage de noms de domaines, d'URLs et d'adresses IP..... | 21 |
| 7 - Fonction « Interface de gestion »..... | 27 |
| 8 - Fonction « modules complémentaires »..... | 27 |
| 8.1 - Import de comptes..... | 27 |
| 8.2 - Inscription par SMS..... | 28 |
| 8.3 - Inscription par adresse électronique..... | 31 |
| 8.4 - Watchdog..... | 31 |
| 8.5 - Statistiques réseau..... | 32 |
| 8.6 - Contournement (by-pass)..... | 33 |
| 8.7 - Équilibrage de charge en sortie (load balancing)..... | 33 |
| 8.8 - Sauvegardes..... | 34 |
| 8.9 - WIFI4EU..... | 35 |
| 9 - Annexes..... | 36 |
| 9.1 - CoovaChilli..... | 36 |
| 9.2 - Freeradius..... | 36 |
| 9.3 - Unbound..... | 37 |
| 9.4 - Parefeu..... | 37 |
| 9.5 - E ² Guardian..... | 37 |
| 9.6 - Ulogd..... | 37 |
| 9.7 - Distribution Mageia et ses dépôts..... | 37 |
| 9.8 - Étude du remplacement de DNSMasq par Unbound..... | 37 |
| 10 - Test plan..... | 39 |
| 11 - Security tests..... | 42 |
| 12 - Tests de débit..... | 43 |
| 13 - Arbre de dépendance JS et CSS..... | 44 |
| 13.1 - JS..... | 44 |
| 13.2 - CSS..... | 46 |
| 14 - TODO..... | 49 |

1 - Rappel de l'architecture

ALCASAR est positionné en coupure entre l'accès Internet et un réseau de consultation. Il permet d'authentifier les utilisateurs, de contrôler et filtrer les accès, de tracer les connexions effectuées, de protéger le réseau de consultation. Le cœur d'ALCASAR est constitué des éléments traditionnels d'un contrôleur d'accès au réseau (NAC = Network Access Control) :

- un serveur d'authentification (freeradius),
- une passerelle d'interconnexion universelle (portail captif) et un client radius (coovachilli)
- une base de données d'utilisateurs (mariadb)
- un pare-feu dynamique (netfilter + ipset)
- un système de filtrage (E²Guardian + 4 instances de unbound)

2 - Choix des constituants

2.1 - La passerelle d'interception

Avec le pare-feu, la « passerelle d'interception » (ou portail captif) constitue le chef d'orchestre de cet ensemble. Pour choisir celle qui serait intégrée dans ALCASAR, les passerelles libres suivantes ont été évaluées au lancement du projet :

| | NoCat  | Talweg | Wifidog  | Chillispot/  |
|-------------|---|--|--|--|
| Site WEB | nocat.net | talweg.univ-metz.fr | dev.wifidog.org | www.chillispot.org www.coovachilli.org |
| Langage | C | C# sous mono | - C pour le programme principal - module PHP pour le serveur WEB | - C pour le programme principal - module CGI-BIN pour le serveur WEB (PERL ou C) |
| Description | NoCat est constitué de plusieurs éléments : « NoCatSplash » est le portail, « NoCatAuth » est utilisé pour l'authentification et « Splash Server » est le service permettant de générer les formulaires de connexion des utilisateurs. Le suivi de ce produit a été arrêté en 2005. | Talweg est un portail dont le contrôle d'accès au réseau est géré protocole par protocole. Tous les protocoles utilisables sur Internet ne sont pas encore intégrés. | WifiDog est composé de 2 modules : « Authentification Server » et « WifiDog Gateway ». Le serveur d'authentification doit être installé sur un serveur fixe alors que la passerelle peut être embarquée dans certains équipements réseau compatibles (routeur, passerelle ADSL, etc.). | Chillispot ne constitue que la partie centrale d'une architecture de type portail captif. Il implémente les 2 méthodes d'authentification (UAM et WPA). Il nécessite la connaissance et l'installation des autres services constitutifs du portail captif. Il est compatible radius. |

| | NoCat | Talweg | Wifidog | Chillispot |
|--|-------|--------|---------|------------|
| Simplicité d'installation | | | | |
| Infrastructure nécessaire | | | | |
| Performances & consommation réseau | | | | |
| Gestion utilisateurs | | | | |
| Sécurité authentification | | | | |
| Sécurité communications | | | | |
| Protocoles supportés | | | | |
| Crédit temps | | | | |
| Interface d'administration / Statistiques | | | | |

Légende:
 : Non Disponible.
 : Plus ou moins.

Bien que cette liste ne soit pas exhaustive, la passerelle « Chillispot » a été choisie. Depuis, elle a été remplacée par le clone (fork) « CoovaChilli » (<http://coova.org/CoovaChilli>). Avant chaque nouvelle version d'ALCASAR, le code source du projet « coova-chilli » est récupéré, compilé spécifiquement pour ALCASAR et empaqueté (RPM) pour être intégré à la distribution Linux exploitée par ALCASAR.

2.2 - Les autres constituants

Pour couvrir l'ensemble des besoins d'ALCASAR, les produits libres suivants ont été intégrés. Leur choix est principalement dicté par leur niveau de sécurité et leur reconnaissance au sein de la communauté du logiciel libre.

| Versions majeures d'ALCASAR | | <1.7 | 1.7 | 1.8 | 1.9 | 2.0 | 2.1-2.2 | 2.3-2.5 | 2.6 | 2.7 | 2.8 | 2.9 | 3.0 | 3.1 | 3.2 | 3.3-3.4 | 3.5 | 3.6.1 | |
|---|----------------|--------|--------|--------|--------|---------|---------|---------|---------|---------|----------|----------|----------|---------|----------|----------------|----------|--------|-------|
| Constituants | | | | | | | | | | | | | | | | | | | |
| Système d'exploitation | Linux Mandriva | 2007 | 2009 | 2010.0 | 2010 | 2010 | 2010 | 2010 | | | | | | | | | | | |
| | Mageia | | | | | | | | 2 | 2 | 4.1 | 5.0 | 5.1 | 6 | 6 | 7.1 | 8 | | |
| noyau Linux | | 2.6.1 | 2.6.2 | 2.6.31 | 2.6.33 | | | | 3.4.4 | 3.4.5 | 3.14.4 | 4.4.13 | 4.4.74 | 4.9.5 | 4.14.89 | 5.10.46 | 5.15.126 | | |
| Trace des connexions (sonde noyau NetFlow + collecteur) | IPT_Netflow | 1.8 | | | | | | | | | | | 2.0 | 2.2 | 2.3 | | 2.6 | 2.6.1 | |
| | Nfdump | | | | | | | | | | | | 1.6.13 | 1.6.15 | 1.6.19 | | 1.6.23 | 1.7.3 | |
| Passerelle d'interception | CoovaChilli | 1.0 | 1.0.12 | 1.2.2 | 1.2.5 | 1.2.8 | 1.2.9 | 1.3.0 | | | 1.3.2 | 1.4.3 | | | | 1.6 | 1.6.2 | | |
| DNS | Unbound | | | | | | | | | | | | | | | | 1.10.1 | 1.17.1 | |
| | Dnsmasq | | | | | 2.52-1 | | | | 2.63 | 2.66 | 2.75 | 2.77 | 2.77-1 | | | | | |
| Serveur DHCP (mode bypass) | dhcpd server | 3.0.4 | 3.0.7 | 4.1.0 | | | | | | | | | | | | | | 4.4.1 | 4.4.2 |
| Serveur Web | Apache | 2.2.3 | 2.2.9 | 2.2.14 | 2.2.15 | | | 2.2.2 | 2.2.2 | 2.2.2 | 2.4.7 | 2.4.10 | 2.4.27 | | | | | | |
| | Lighttpd | | | | | | | | | | | | 1.4.51 | | 1.4.53 | 1.4.59 | | | |
| PKI locale (chiffrement des flux) | OpenSSL | | | | | 1.0.0.a | | | | 1.0.0.k | 1.0.1p | 1.0.2h | 1.0.2k | 1.0.2n | 1.0.2q | 1.1.0l | 1.1.1v | | |
| Middleware | PHP | 5.1.6 | 5.2.6 | 5.3.1 | 5.3.4 | 5.3.6 | | 5.3.1 | 5.3.1 | 5.3.2 | 5.5.22 | 5.6.22 | 5.6.30 | 5.6.32 | 5.6.38 | 7.3.29 | 8.0.30 | | |
| Serveur d'authentification | FreeRadius | 1.1.2 | 2.1.0 | 2.1.7 | 2.1.8 | | 2.1.8.6 | | 2.1.12 | 2.2.0 | 2.2.9 | 2.2.10 | 3.0.15 | | | 3.0.22 | | | |
| Serveur de base de données utilisateurs | Mysql | 5.0.2 | 5.0.6 | 5.1.4 | 5.1.4 | 5.1.5 | 5.1.5 | 5.1.6 | | | | | | | | | | | |
| | MariaDB | | | | | | | | 5.5.25 | 5.5.41 | 10.0.2.4 | 10.0.3.1 | 10.1.2.9 | 10.1.35 | 10.3.29 | 10.5.22 | | | |
| Cache WEB (proxy) | Squid | 2.6 | 3.0.8 | 3.0.22 | 3.1.14 | | | | 3.1.19 | | | | | | | cf. e2guardian | | | |
| | tinyproxy | | | | | | | | | | | | 1.8.3 | | | | | | |
| Serveur de temps | ntpd | 4.2 | 4.2.4 | | | | | 4.2.6 | 4.2.6p5 | | | 4.2.8 | | | | | | | |
| Journalisation | Ulogd | 1.24 | | | | | | | | | | 2.0.2 | 2.0.4 | 2.0.5 | | 2.0.7 | | | |
| Filtrage d'URL WEB + Proxy | SquidGuard | 1.2.0 | | | | | | | | | | | | | | | | | |
| | Dansguardian | | 2.9.9 | 2.10.1 | | | | | | 2.12.0 | | | | | | | | | |
| | E2Guardian | | | | | | | | | | | | 3.5.0 | | 5.3.2 | 5.3.4 | | | |
| Statistiques de consultation | Awstat | 2.5 | 2.5.3 | 6.9 | 6.95 | | | | 7.0 | | | | | | | | | | |
| | Nfsen | | | | | | | | 1.3.7 | | 1.3.8 | | | | | | | | |
| Détection d'intrusion | Fail2ban | | | | | | | | | 0.8.6 | 0.8.13 | | 0.9.5 | | | 0.10.4 | 1.0.2 | | |
| Info système | Phpsysinfo | 2.5.3 | | | | | | | | | | | | | | | 3.4.1 | | |
| Chiffrement des fichiers journaux | Gnupg | 1.4.5 | 1.4.9 | 1.4.10 | | | | | 1.4.12 | 1.4.16 | 1.4.19 | 1.4.22 | 1.4.23 | | | 2.2.19 | 2.2.36 | | |
| Connexion distante sécurisée | openssh-server | 4.3-P2 | 5.1-P1 | 5.3-P1 | 5.5p1 | | | | 5.9p1 | 6.2p2 | 6.6-p1 | 7.5p1 | | | | 8.0p1 | 8.4p1 | | |
| Antimalware | LibClamav | | | | 0.96 | 0.96-1 | 0.97-0 | 0.97-3 | 0.97-5 | 0.97-7 | 0.97-8 | 0.98-7 | 0.99-1 | 0.99-2 | 0.100.2 | | | | |
| | clamd | | | | | | | | | | | | | | | | 0.103.2 | | |
| Serveur de courrier | Postfix | | | | | | | | | 2.8.8 | 2.10.2 | 2.10.3 | 3.1.6 | | | 3.4.5 | 3.5.9 | | |
| Couche d'authentification Email | Cyrus SASL | | | | | | | | | | | | | | | | 2.1.27 | | |
| Gestionnaire de SMS | Gammu-smsd | | | | | | | | | | | 1.32 | 1.34 | 1.35 | 1.39 | | 1.42 | | |
| Générateur de fichiers PDF | wkhtmltopdf | | | | | | | | | | | | | | | | 0.12.3 | | |
| Intégration Let's Encrypt | Acme.sh | | | | | | | | | | | | 2.8.6 | | 3.0.4 | 3.0.7 | | | |
| Front-end (Framework) | Bootstrap | | | | | | | | | | | | 3.3.7 | | 4.6.1 | | | | |
| Front-end (Librairie JS) | Jquery / ui | | | | | | | | | | | | 3.2/1.10 | | 3.6/1.12 | | | | |

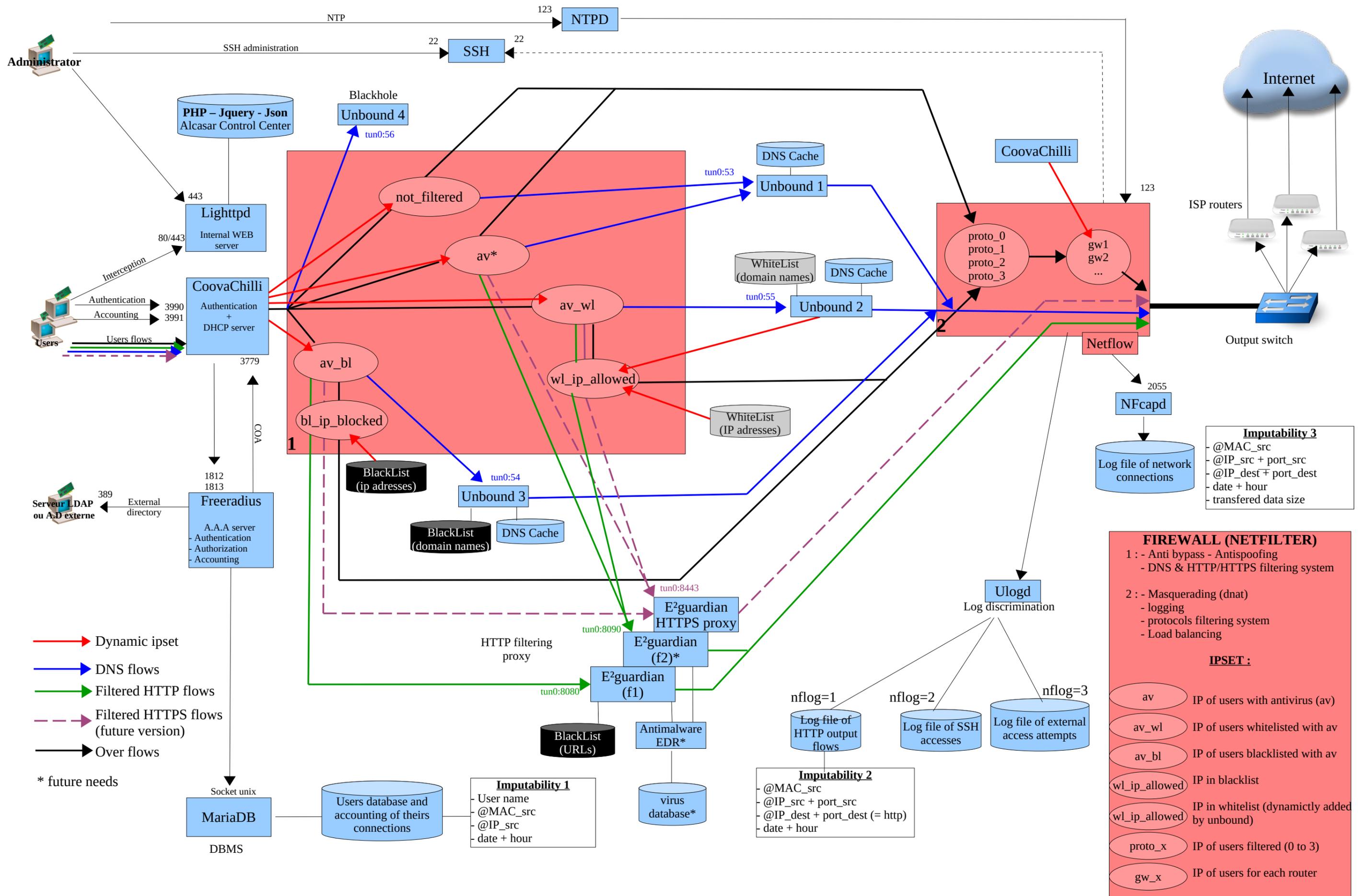
3 - Architecture :

ALCASAR peut être décomposé en cinq fonctions qui sont détaillées dans la suite du document :

- La fonction « interception / authentification / autorisation » est réalisée par CoovaChilli, Unbound, Lighttpd et le couple (Freeradius, MariaDB). Pour l'authentification, la connexion à un annuaire externe (LDAP/A.D.) est possible ;
- La fonction « traçabilité / imputabilité des connexions » est constituée d'une sonde Netflow, des journaux du pare-feu géré par le daemon de journalisation Ulog et du couple (Freeradius, MariaDB) ;
- La fonction de « filtrage » (de domaine, d'URL, d'adresses IP et de protocoles réseau) est réalisé par le pare-feu (Netfilter) associé à des ipset dynamiques, 4 instances de Unbound et le proxy HTTP/HTTPS « E2Guardian » ;
- La fonction « interface de gestion » appelée ALCASAR Control Center (ACC) est réalisée en PHP / HTML4 & 5/ JQuery. Elle est servie par Lighttpd ;
- Les fonctions « modules complémentaires » ont pour objectif d'améliorer la sécurité globale du portail (anti-contournement, anti-usurpation MAC/IP, chiffrement des fichiers journaux, gestion des certificats, IDS, etc.) ou d'enrichir les possibilités du portail (installation, mise à jour, by-pass, archivage, accélération de la consultation, etc.).

Le schéma d'architecture suivant présente les processus principaux d'ALCASAR et les flux de données transitant entre ceux-ci.

ALCASAR – ARCHITECTURE



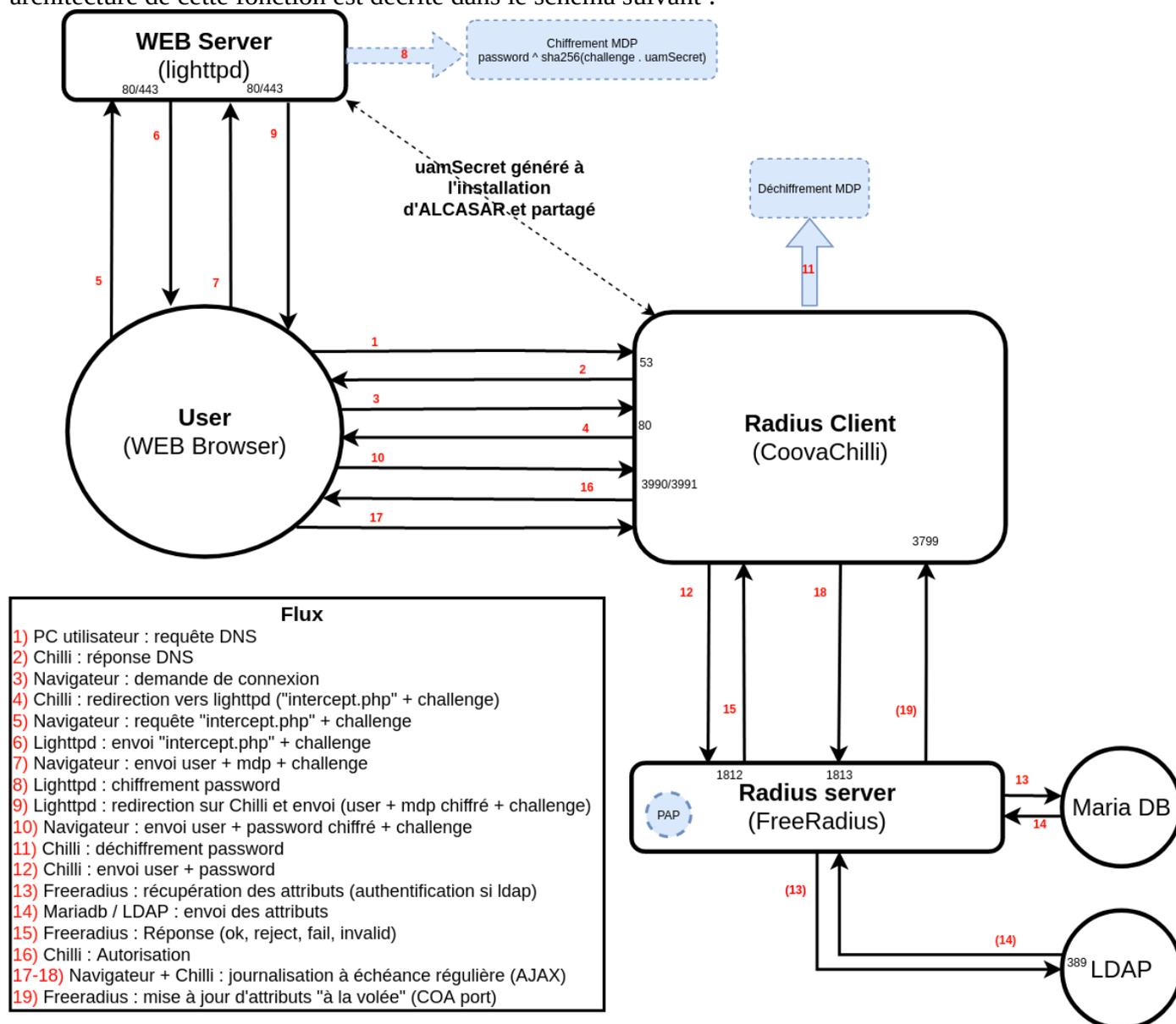
4 - Fonction « interception / authentification / autorisation »

Afin d'être le plus universel possible, ALCASAR s'appuie sur l'« UAM » (Universal Access Method). Cette méthode n'utilise que des protocoles standards ne nécessitant qu'un navigateur WEB pour authentifier un utilisateur. Parmi les autres méthodes, on peut citer celle nécessitant que des agents soient installés sur les équipements des utilisateurs ou celle reposant sur des protocoles réseau dédiés (802.1X par exemple).

La fonction « interception / authentification » s'appuie sur les 4 briques logicielles suivantes :

- « CoovaChilli » (processus « chilli ») gère les fonctions de « portail captif », « client radius » et « serveur DHCP » ;
- « Lighttpd » (processus « lighttpd ») est le serveur WEB présentant les pages web aux utilisateurs (et l'ACC aux administrateurs) ;
- « FreeRadius » (processus « radiusd ») est le serveur d'authentification, d'autorisation et de journalisation (Authentication, Authorisation & Accounting - AAA) de type radius ;
- « Mariadb » (processus « mysqld ») est le système de gestion de bases de données stockant la base des utilisateurs (base « radius »). Mariadb gère aussi la base de données liée à la gestion des SMS (base « gammu »).

L'architecture de cette fonction est décrite dans le schéma suivant :



4.1 - Le portail captif et client radius

« CoovaChilli » est lancé via son unité de démarrage (*/etc/systemd/system/chilli.service*) qui est adapté par le script d'installation (« *alcasar.sh* »). Son fichier de configuration est « */etc/chilli.conf* ». Le processus « chilli » est lancé en mode « daemon ». Ce dernier crée l'interface virtuelle « tun0 »¹ liée en « point à point » à l'interface physique connectée au réseau de consultation (\$INTIF). Cette configuration permet de gérer le cache ARP en espace utilisateur autorisant ainsi le verrouillage des couples (@MAC, @IP) acquis en écoutant le réseau de consultation. Un empoisonnement du cache ARP par le réseau est alors impossible (« cache poisoning »). Dans certains cas, ce comportement peut être bloquant. Exemple : lorsqu'on reparamètre l'@IP d'un équipement qui a déjà été enregistré. La commande « *chilli-query list* » permet d'afficher et de contrôler le cache ARP de « chilli ». Cette commande est utilisée par le centre de contrôle d'ALCASAR – ACC (menu « ACTIVITÉ ») pour gérer ces cas. Complémentaire à cette fonction d'anti-« cache poisoning », ALCASAR utilise un module spécifique de sécurité (*alcasar-watchdog.sh*) qui permet d'éviter l'usurpation d'adresses MAC et d'adresses IP sur le réseau de consultation (cf. fonctions de sécurité).

4.1.1 - Fonctionnement de l'interception/authentification

La capture suivante montre les différentes étapes constitutives de l'interception/authentification de type « UAM » implémenté dans ALCASAR :

| No. - | Time | Source | Destination | Protocol | Info |
|-------|----------|-----------------|-----------------|----------|---|
| 1 | 0.000000 | 192.168.182.129 | 192.168.182.1 | DNS | Standard query A www.free.fr |
| 2 | 0.007977 | 192.168.182.1 | 192.168.182.129 | DNS | Standard query response A 212.27.48.10 |
| 3 | 0.013100 | 192.168.182.129 | 212.27.48.10 | TCP | iclv-nlc > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=1 |
| 4 | 0.018826 | 212.27.48.10 | 192.168.182.129 | TCP | http > iclv-nlc [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS= |
| 5 | 0.022528 | 192.168.182.129 | 212.27.48.10 | TCP | iclv-nlc > http [ACK] Seq=1 Ack=1 win=96768 Len=0 |
| 6 | 0.095262 | 192.168.182.129 | 212.27.48.10 | HTTP | GET / HTTP/1.1 |
| 7 | 0.112659 | 212.27.48.10 | 192.168.182.129 | TCP | http > iclv-nlc [ACK] Seq=1 Ack=384 win=6912 Len=0 |
| 8 | 0.119483 | 212.27.48.10 | 192.168.182.129 | TCP | [TCP segment of a reassembled PDU] |
| 9 | 0.122574 | 212.27.48.10 | 192.168.182.129 | HTTP | HTTP/1.1 302 Moved temporarily (text/html) |
| 10 | 0.126880 | 212.27.48.10 | 192.168.182.129 | TCP | http > iclv-nlc [FIN, ACK] Seq=1511 Ack=384 win=6912 Len=0 |
| 11 | 0.131796 | 192.168.182.129 | 212.27.48.10 | TCP | iclv-nlc > http [ACK] Seq=384 Ack=1512 win=96768 Len=0 |
| 12 | 0.135296 | 192.168.182.129 | 212.27.48.10 | TCP | iclv-nlc > http [FIN, ACK] Seq=384 Ack=1512 win=96768 Len=0 |
| 13 | 0.142579 | 212.27.48.10 | 192.168.182.129 | TCP | http > iclv-nlc [ACK] Seq=1512 Ack=385 win=6912 Len=0 |
| 14 | 0.173829 | 192.168.182.129 | 192.168.182.1 | TCP | iclv-wsm > https [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=1 |
| 15 | 0.182402 | 192.168.182.1 | 192.168.182.129 | TCP | https > iclv-wsm [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0 MSS= |
| 16 | 0.182724 | 192.168.182.129 | 192.168.182.1 | TCP | iclv-wsm > https [ACK] Seq=1 Ack=1 win=96768 Len=0 |
| 17 | 0.259992 | 192.168.182.129 | 192.168.182.1 | SSL | Client Hello |
| 18 | 0.266048 | 192.168.182.1 | 192.168.182.129 | TCP | https > iclv-wsm [ACK] Seq=1 Ack=367 win=6912 Len=0 |
| 19 | 0.268301 | 192.168.182.1 | 192.168.182.129 | TLSv1 | server Hello, change cipher spec, Encrypted Handshake Mess: |

Transmission Control Protocol, Src Port: http (80), Dst Port: iclv-nlc (1594), Seq: 1491, Ack: 384, Len: 0
[Reassembled TCP Segments (1510 bytes): #8(1460), #9(50)]
Hypertext Transfer Protocol
HTTP/1.1 302 Moved temporarily
Connection: close
Cache-Control: no-cache, must-revalidate
P3P: CP="IDC DSP COR ADM DEVI TAII PSA PSD IVAI IVDI CONI HIS OUR IND CNT"
[truncated] Location: https://192.168.182.1/intercept.php?res=notyet&uamip=192.168.182.1&uamport=3990&challenge=6595f6
Content-Type: text/html; charset=UTF-8

Lorsqu'un équipement de consultation tente de se connecter sur Internet (www.free.fr dans la capture ci-dessus) :

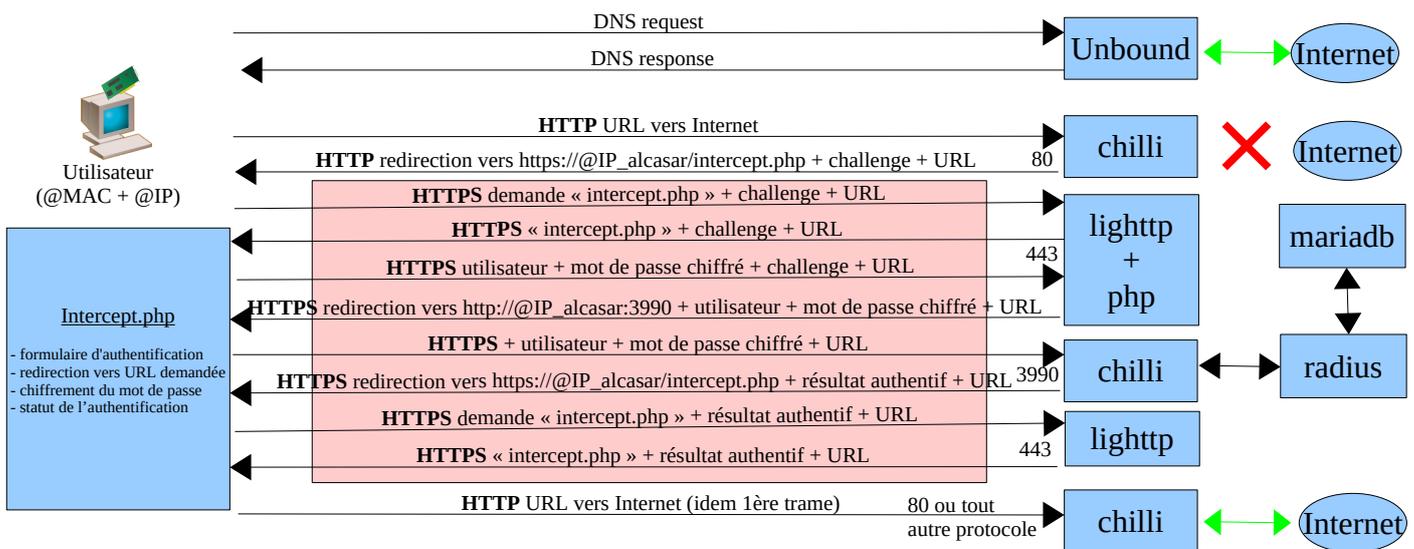
- **1)** [trame 1] La requête DNS de l'équipement est reçue par le serveur DNS principal d'ALCASAR (unbound). Les tentatives de connexion vers d'autres serveurs DNS sont bloquées par le pare-feu interne. Cela permet de prévenir le contournement du DNS d'ALCASAR ainsi que les tunnels DNS.
- **2)** Unbound résout le domaine localement s'il est dans son cache, sinon il transfère la requête vers les serveurs DNS Internet définis lors de l'installation d'ALCASAR. Les réponses sont retournées par unbound à l'équipement de consultation [trame 2].
- **3)** Quand une requête WEB (80 ou 443) est envoyée [trame 3] par l'équipement de consultation, elle est interceptée par « chilli » qui vérifie si un utilisateur n'est pas déjà « autorisé » sur cet équipement :
 - Si tel est le cas, « chilli » laisse transiter toutes les trames de l'équipement quel que soit le protocole. Le pare-feu dynamique prend alors le relais. Il oriente les flux de l'utilisateur (DNS, WEB, etc.) vers les chaînes de traitement associées à son profil (cf. fonction de filtrage).
 - **4)** Si tel n'est pas le cas, « chilli » simule une connexion WEB standard [trames 4 à 6] et répond à la requête de l'équipement [trames 7 à 9] par une trame HTTP de redirection de service (« *HTTP/1.0 302*

1 - Les périphériques « Tap » et « Tun » des noyaux Linux sont des interfaces réseau virtuelles de niveau 2 (Ethernet) pour « Tap » ou 3 (IP) pour « Tun » permettant à des processus exécutés en espace utilisateur d'envoyer ou de recevoir des trames/paquets sur ces interfaces via les fichiers spéciaux (/dev/tapX ou /dev/tunX). Ces interfaces virtuelles peuvent être exploitées exactement comme des interfaces physiques qui fonctionnent en mode « noyau » (configuration, émission/réception, routage). Ainsi, ces interfaces virtuelles autorisent un traitement sur les trames à la réception ou avant l'émission de celles-ci. L'interface Tap est souvent utilisée dans la création de tunnels RVP/VPN afin d'encapsuler un flux dans un autre (cf. projet « OpenVPN »).

Moved Temporarily») contenant l'URL de la page d'authentification définie par la primitive « uamserver » du fichier « /etc/chilli.conf » (« https://@ip_alcasar/intercept.php ») [cf. détail de la trame 9]. Cette session TCP se termine [trames 10 à 13]. Tant que l'utilisateur n'est pas authentifié, aucun flux réseau ne peut sortir de son équipement vers Internet.

- **5) & 6)** Le navigateur initie alors une connexion avec le serveur WEB d'ALCASAR (Lighttpd) afin de récupérer la page « intercept.php » [trame 14 et suivantes].
- **7)** L'utilisateur renseigne les champs d'authentification (identifiant + mot de passe) qui sont envoyés de manière chiffrée à Lighttpd pour être traités **8)**.
- **9)** Lighttpd retourne le résultat au navigateur afin que ce dernier redirige ces informations au processus « chilli » (port 3990²).
- **10)** « chilli » les récupère afin de requêter le serveur radius **11) & 12) & 13) & 14) & 15)**. La communication entre « chilli » et « freeradius » exploite le protocole « radius ». Les paramètres de cette communication sont définis à la fois dans le fichier « /etc/raddb/client.conf » et via les directives « hs_radius », « hs_radius2 » et « hs_radsecret » du fichier « /etc/chilli.conf ».
- **16)** Le résultat de cette requête est retourné au navigateur afin d'être traité par les scripts javascript de la page « intercept.php » (échec ou réussite de la connexion).
- Dans son rôle de client radius, « chilli » gère les compteurs liés aux attributs d'autorisation de l'utilisateur (temps de connexion, débit, volume, etc.). Il les affiche sur la page de connexion de l'utilisateur (requêtes « ajax ») **17)**. Il les enregistre régulièrement pour la journalisation **18)**.
- Pour la déconnexion, les navigateurs Web génèrent une requête adéquate sur le port d'écoute de « chilli » (3990).

Cette phase d'interception peut être schématisée comme suit :



Cette double redirection (chilli → lighttpd → chilli) a été maintenue dans ALCASAR afin de rester conforme au principe de l'UAM où les 3 services en charge de l'authentification/autorisation à savoir le client radius (« chilli »), le serveur radius et le service WEB peuvent être hébergés sur des serveurs différents.

Exception à l'authentification

« chilli » a la possibilité de laisser transiter des trames spécifiques vers Internet sans authentification préalable. Cette possibilité est exploitée dans ALCASAR pour permettre la mise à jour automatique. Les paramètres « uamallowed » et « uamdomain » pointent vers deux fichiers contenant la liste des adresses IP (ou adresse IP de réseaux) ou des noms de domaine joignables sans authentification (« /usr/local/etc/alcasar-uamallow » et « /usr/local/etc/alcasar-uamdomain »).

2 - « chilli » écoute sur un port défini par la primitive « uamport » de son fichier de configuration « /etc/chilli.conf » (3990 par défaut). Le format des requêtes envoyées sur ce port détermine l'action demandée (ex. « @IP:3990/prelogin » pour une demande de connexion, « @IP:3990/logout » pour une demande de déconnexion. La requête contient bien entendu l'ensemble des paramètres nécessaires au traitement de la demande (@MAC, challenge, identifiant, etc.).

4.1.2 - Action lors des connexions / déconnexions

« Chilli » possède la capacité d'exécuter un programme, déclenché par un évènement interne (hook). ALCASAR exploite cette capacité sur les évènements suivants :

- « nouvel utilisateur authentifié » → alcasar-conup.sh ;
- « déconnexion d'un utilisateur » → alcasar-condown.sh
- « nouvelle @MAC détectée » → alcasar-macup.sh

Ces scripts permettent notamment de rediriger les flux des utilisateurs vers les processus de traitement adéquats en fonction de leurs attributs (filtrages DNS, URL, protocoles, etc.). À cet effet, plusieurs « ipset » ont été créés (cf. §6.2.2) pour que le parefeu puisse gérer de manière dynamique les @ip et @MAC des utilisateurs (cf. schéma des flux au §3). La commande « ipset -L -t » permet de lister tous les « ipset » :

- ipset contenant les utilisateurs en fonction de leurs attributs : « not_filtered », « av », « av_bl », « av_wl »
- ipset contenant les @IP de la blacklist : « bl_ip_blocked », « wl_ip_allowed »
- ipset contenant les protocoles réseau filtrés : « proto_0 », « proto_1 », « proto_2 », « proto_3 »
- ipset contenant les sites autorisés sans authentification : « site_direct »

4.1.3 - Protection contre l'écoute

4.2 - Base de données des utilisateurs

Le SGBD « mariaDB » est exploité pour gérer les bases de données d'ALCASAR. Deux bases de données ont été créées : la base « gammu » pour l'exploitation du module d'auto-inscription par SMS et la base « radius » pour la gestion des utilisateurs. Le modèle conceptuel de données (MCD) de cette base est entièrement compatible avec le service d'authentification Radius. Sa structure est mise en place lors de l'installation d'ALCASAR en exploitant un script SQL (« radius-db-vierge.sql »).

```
# Ajout d'une base vierge
mysql -u$DB_USER -p$radiuspwd $DB_RADIUS < $DIR_CONF/radiusd-db-vierge.sql
```

Les deux Modèles Conceptuels de Données (MCD) de ces deux bases sont les suivants :

BASE DE DONNÉES RADIUS V3.x
(gestion des utilisateurs)

Légende

En rouge : Clé Primaire. AI : Auto-Increment
* : Clé secondaire

Tables normalisées Radius

Tables complémentaires ALCASAR

Tables inexploitées actuellement

1. badusers

id int(10)
UserName * varchar(30)
Date * datetime
Reason varchar(200)
Admin varchar(30)

12. userinfo

id int(10) - AI
username * varchar(64)
name varchar(200)
mail varchar(200)
department * varchar(200)
workphone varchar(200)
homphone varchar(200)
mobile varchar(200)

2. mtotacct

mtotacctid bigint(21) - AI
username * varchar(64)
acctdate * date
connnum bigint(12)
conntotduration bigint(12)
connmaxduration bigint(12)
connminduration bigint(12)
inputoctets bigint(12)
outputoctets bigint(12)
nasipaddress * varchar(15)

10. totacct

totacctid bigint(21) - AI
username * varchar(64)
acctdate * date
connnum bigint(12)
conntotduration bigint(12)
connmaxduration bigint(12)
connminduration bigint(12)
inputoctets bigint(12)
outputoctets bigint(12)
nasipaddress * varchar(15)

4. radacct

radacctid bigint(21) - AI
acctsessionid * varchar(32)
acctuniqueid * varchar(64)
username * varchar(64)
groupname varchar(64)
realm varchar(64)
nasipaddress * varchar(15)
nasportid varchar(15)
nasporttype varchar(32)
acctstarttime * datetime
acctstoptime * datetime
Acctsessiontime * int(12)
acctauthentic varchar(32)
connectinfo_start varchar(50)
connectinfo_stop varchar(50)
acctinputoctets bigint(20)
acctoutputoctets bigint(20)
calledstationid varchar(50)
callingstationid varchar(50)
acctterminatecause varchar(32)
servicetype varchar(32)
framedprotocol varchar(32)
framedipaddress * varchar(15)
acctstartdelay int(12)
acctstpsdelay int(12)
xascendsessionsvrkey varchar(10)

8. radpostauth

id int(11) - AI
user varchar(64)
pass varchar(64)
reply varchar(32)
date timestamp(14)

5. radcheck

id int(11) - AI
username * varchar(64)
attribute varchar(64)
op char(2)
value varchar(253)

9. radreply

id int(11) - AI
username * varchar(64)
attribute varchar(64)
op char(2)
value varchar(253)

11. radusergroup

username * varchar(64)
groupname varchar(64)
priority int(11)

7. radgroupreply

id int(11) - AI
groupname * varchar(64)
attribute varchar(64)
op char(2)
value varchar(253)

6. radgroupcheck

id int(11) - AI
groupname * varchar(64)
attribute varchar(64)
op char(2)
value varchar(253)

3. nas

id int(10)
nasname * varchar(128)
shortname varchar(32)
type varchar(30)
ports int(5)
secret varchar(60)
community varchar(50)
description varchar(200)

* dans les version < 2.0 : la table « radusergroup » s'appelait « usergroup » et le champs « groupname » de la table « radacct » n'existait pas
* à partir de la version 2.6, le champs 'username' de la table 'userinfo' change de type pour être compatible avec les autres tables (bascule de varchar(30) en varchar(64))

BASE DE DONNÉES GAMMU V1.39
(gestion des SMS)
Version du schéma : 17

| inbox | |
|-------------------|--|
| UpdateInDB | timestamp |
| ReceivingDateTime | timestamp |
| Text | text |
| SenderNumber | ° varchar(20) |
| Coding | enum('Default_No_Compression', 'Unicode_No_Compression', '8bit', 'Default_Compression', 'Unicode_Compression') |
| UDH | text |
| SMSCNumber | varchar(20) |
| Class | int |
| TextDecoded | ° text |
| ID | ° int |
| RecipientID | text |
| Processed | enum('false', 'true') |
| Status | int |

| SMS_ban_perm | |
|--------------|----------------|
| SenderNumber | ° varchar(20) |
| Expiration | ° varchar(255) |
| Perm | ° int |
| date_add | ° timestamp |

| SMS_ban_temp | |
|--------------|---------------|
| ID | ° int |
| SenderNumber | ° varchar(20) |

| SMS_country | |
|-------------|-------------|
| name | varchar(50) |
| id | varchar(20) |
| status | int |

| gammu | |
|---------|-----|
| Version | int |

| phones | |
|--------------|------------------|
| ID | text |
| UpdateInDB | timestamp |
| InsertIntoDB | timestamp |
| TimeOut | timestamp |
| Send | enum('yes','no') |
| Receive | enum('yes','no') |
| IMEI | varchar(35) |
| IMSI | varchar(35) |
| NetCode | varchar(10) |
| NetName | varchar(35) |
| Client | text |
| Battery | int(11) |
| Signal | int(11) |
| Sent | int(11) |
| Received | int(11) |

| sentitems | |
|-------------------|---|
| UpdateInDB | timestamp |
| InsertIntoDB | timestamp |
| SendingDateTime | timestamp |
| DeliveryDateTime | timestamp |
| Text | text |
| DestinationNumber | varchar(20) |
| Coding | enum('Default_No_Compression', 'Unicode_No_Compression', '8bit', 'Default_Compression', 'Unicode_Compression') |
| UDH | text |
| SMSCNumber | varchar(20) |
| Class | int(11) |
| TextDecoded | text |
| ID | unsigned int |
| SenderID | varchar(255) |
| SequencePosition | int |
| Status | enum('SendingOK', 'SendingOKNoReport', 'SendingError', 'DeliveryOK', 'DeliveryFailed', 'DeliveryPending', 'DeliveryUnknown', 'Error') |
| StatusError | int |
| TPMR | int |
| RelativeValidity | int |
| CreatorID | text |
| StatusCode | int |

| outbox | |
|-------------------|---|
| UpdateInDB | timestamp |
| InsertIntoDB | timestamp |
| SendingDateTime | timestamp |
| SendBefore | time |
| SendAfter | time |
| Text | text |
| DestinationNumber | varchar(20) |
| Coding | enum('Default_No_Compression', 'Unicode_No_Compression', '8bit', 'Default_Compression', 'Unicode_Compression') |
| UDH | text |
| Class | int |
| TextDecoded | text |
| ID | unsigned int |
| MultiPart | enum('false','true') |
| RelativeValidity | int |
| SenderID | varchar(255) |
| SendingTimeOut | timestamp |
| DeliveryReport | enum('default','yes','no') |
| CreatorID | text |
| Retries | int(3) |
| Priority | int |
| Status | enum('SendingOK', 'SendingOKNoReport', 'SendingError', 'DeliveryOK', 'DeliveryFailed', 'DeliveryPending', 'DeliveryUnknown', 'Error', 'Reserved') |
| StatusCode | int |

Légende

- En rouge : Index – Clé Primaire
- Table créée par Gammu-smsd
- Table ajoutée pour gérer les SMS
- Table inexploitée par ALCASAR
- ° : Colonne exploitée

4.2.1 - Débogage

En mode texte

Utilisez les login/mot_de_passe de votre fichier « [/root/ALCASAR-password.txt](#) »

Accès à l'administration globale

```
mysql -uroot -p$(grep '^db_root=' /root/ALCASAR-passwords.txt | cut -d '=' -f2-)
```

ex : pour afficher la liste des bases de données : « SHOW DATABASES ; »

« exit » pour quitter ; « help » pour voir les autres commandes.

Accès aux bases (ex : avec la base « radius »)

```
mysql -uradius -p$(grep '^db_password=' /root/ALCASAR-passwords.txt | cut -d '=' -f2-) radius
```

Entrez le mot de passe associé à l'utilisateur « radius ».

ex : Voir les tables : « SHOW TABLES ; »

ex : Voir le contenu : « SELECT * FROM <tables_name> ; »

Journalisation des événements

Il est possible d'activer la journalisation afin d'afficher toutes les requêtes reçues par le serveur « mysqld ». Pour cela, ajoutez les lignes « [general_log_file=/var/log/mysqld/mariadb.log](#) » et « [general_log=1](#) » dans la section [mysqld] du fichier de conf « [/etc/my.cnf](#) ». relancez le serveur : [systemctl restart mysqld](#). Affichez les log : [tail -f /var/log/mysqld/mariadb.log](#)

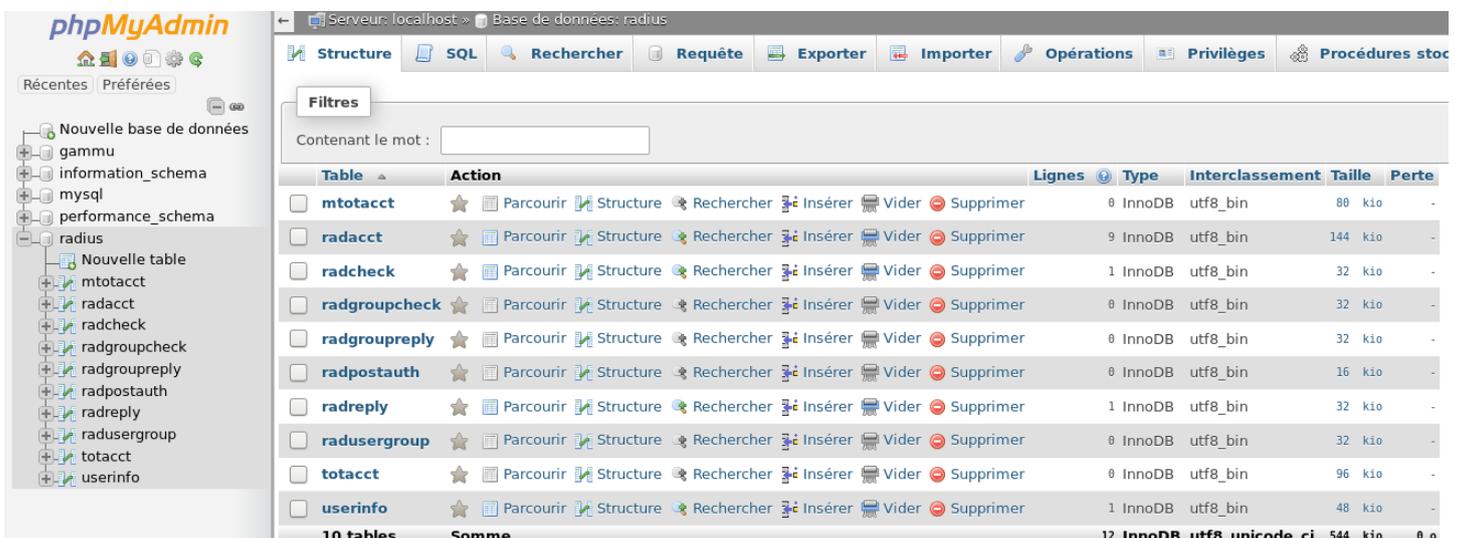
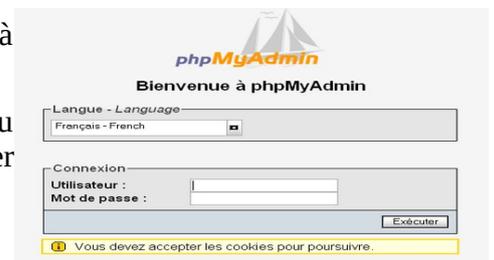
En mode graphique

Il est possible d'afficher de manière graphique (et pédagogique) le contenu des bases exploitées par ALCASAR. Voici la procédure exploitant l'interface WEB « phpmyadmin » (à supprimer après avoir été exploité).

- Récupérez la dernière archive de « phpmyadmin » et copiez-la dans le répertoire [/var/www/html/](#). Installez « unzip » (urpmi « unzip ») et décompressez « phpmyadmin » (unzip nom_de_l'archive). Renommez le nom du répertoire de l'archive en « phpmyadmin » (mv nom_répertoire phpmyadmin) ;
- connectez-vous à la base à partir de votre station de consultation à l'URL : « [https://alcasar.localdomain/phpmyadmin](#) » ;
- récupérez les mots de passe du compte d'administration (root) ou du compte gestionnaire de la base « radius » dans le fichier « [/root/ALCASAR-passwords.txt](#) » ;
- identifiez-vous sur le SGBD soit en « root » soit en « radius » ;
- Vous pouvez maintenant accéder aux bases (« gammu » ou « radius ») ainsi qu'aux contenus des tables.

```
MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| gammu    |
| information_schema |
| mysql    |
| performance_schema |
| radius   |
+-----+
5 rows in set (0.01 sec)

MariaDB [(none)]> USE radius;
MariaDB [(none)]> SHOW TABLES;
+-----+
| Tables_in_radius |
+-----+
| mtotacct         |
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radpostauth      |
| radreply         |
| radusergroup     |
| totacct          |
| userinfo         |
+-----+
10 rows in set (0.01 sec)
```



Quand vous avez terminé avec « phpmyadmin », désinstallez-le (rm -rf phpmyadmin »).

Exemple de mouvement (base « radius »)

```
SET NAMES utf8
```

Ajout d'un groupe (group-test)

Vérification de doublon

```
SELECT DISTINCT groupname FROM radusergroup WHERE username = 'group-test'  
SELECT attribute,value ,op FROM radgroupcheck WHERE groupname = 'group-test'  
SELECT attribute,value ,op FROM radgroupreply WHERE groupname = 'group-test'  
SELECT username FROM radusergroup WHERE groupname = 'group-test' ORDER BY username
```

Insertion

```
INSERT INTO radusergroup (username,groupname) VALUES ('group-test','group-test')
```

Ajout d'attributs

```
INSERT INTO radgroupcheck (attribute,value,groupname ,op) VALUES ('Simultaneous-Use','2','group-test' ,':=')  
INSERT INTO radgroupcheck (attribute,value,groupname ,op) VALUES ('Login-Time','Mo0800-1900,Tu0800-1900,We0800-1900,Th0800-1900,Fr0800-1900','group-test' ,':=')
```

Ajout d'un utilisateur ("rexy") + affectation d'un groupe + ajout d'attribut

Vérification de doublon

```
SELECT attribute,value ,op FROM radcheck WHERE username = 'rexy'  
SELECT attribute,value ,op FROM radreply WHERE username = 'rexy'  
SELECT DISTINCT groupname FROM radusergroup WHERE username = 'rexy'  
SELECT username FROM userinfo WHERE username = 'rexy'
```

Insertion

```
INSERT INTO radcheck (attribute,value,username ,op) VALUES ('Crypt-Password','$5$fdzkw8g$e21ZDZ/OHV2B6iqseee5B/XJ5vzOBk5j/HjQ7eK.ayB','rexy' ,':=')  
INSERT INTO userinfo (username,name,mail,department,homephone,workphone,mobile) VALUES ('rexy',' ',' ',' ',' ',' ')
```

Affectation du groupe

```
INSERT INTO radusergroup (username,groupname) VALUES ('rexy','group-test')
```

Ajout d'un attribut particulier

```
INSERT INTO radcheck (attribute,value,username ,op) VALUES ('Expiration','27 November 2020','rexy' ,':=')
```

Suppression d'un utilisateur ("rexy")

```
DELETE FROM radreply WHERE username = 'rexy'  
DELETE FROM radcheck WHERE username = 'rexy'  
DELETE FROM radusergroup WHERE username = 'rexy'  
DELETE FROM userinfo WHERE username = 'rexy'
```

Ajout d'une adresse MAC

Vérification de doublon

```
SELECT attribute,value ,op FROM radcheck WHERE username = '08-00-27-39-30-92'  
SELECT attribute,value ,op FROM radreply WHERE username = '08-00-27-39-30-92'  
SELECT DISTINCT groupname FROM radusergroup WHERE username = '08-00-27-39-30-92'  
SELECT * FROM userinfo WHERE username = '08-00-27-39-30-92'
```

Insertion

```
INSERT INTO radcheck (attribute,value,username ,op) VALUES ('Crypt-Password','$5$351gtzc$NkEvQ39XIUBclsRu98zSEhQfyoWV0FtugsVFPWINS7','08-00-27-39-30-92' ,':=')  
INSERT INTO userinfo (username,name,mail,department,homephone,workphone,mobile) VALUES ('08-00-27-39-30-92',' ',' ',' ',' ',' ')
```

Ajout d'attributs

```
INSERT INTO radreply (attribute,value,username ,op) VALUES ('Alcasar-Filter','3','08-00-27-39-30-92' ,':=')  
INSERT INTO radreply (attribute,value,username ,op) VALUES ('Alcasar-Protocols-Filter','2','08-00-27-39-30-92' ,':=')  
INSERT INTO radreply (attribute,value,username ,op) VALUES ('Alcasar-Status-Page-Must-Stay-Open','1','08-00-27-39-30-92' ,':=')
```

4.3 - Le serveur Radius

Le service « freeradius » (radiusd) est utilisé comme unité d'authentification, d'autorisation et de journalisation (Authentication Authorization Accounting - AAA).

L'authentification exploite par défaut la base de données locale (mariadb). Un module LDAP additionnel a été intégré afin de pouvoir valider le couple login/MDP avec celui d'un annuaire externe compatible LDAP (Active Directory®, OpenLDAP, etc.).

L'autorisation et la journalisation exploitent uniquement la base de données local.

Les fichiers de configuration du serveur sont dans le répertoire « /etc/raddb ». La configuration de ce serveur est définie dans le fichier « radiusd.conf ». Le fichier « client.conf » contient les paramètres du seul client radius configuré par défaut (« chilli »). Deux fichiers de configuration spécifiques pour ALCASAR sont situés dans le répertoire « sites-available » (« alcasar » et « alcasar-with-ldap »). En fonction de la configuration, l'un ou l'autre est lié symboliquement au fichier « alcasar » situé dans le répertoire « sites-enabled ». Les modules radius (rlm : Radius Loadable Modules) exploités par ALCASAR sont situés dans le répertoire « mods-enabled ». Ce sont des liens symboliques pointant vers des fichiers du répertoire « mods-available ». Les modules suivants sont exploités pour ALCASAR :

- « sql » : définit les paramètres de connexion à la base de données des utilisateurs (mariadb) ;
- « pap » : permet de valider le mot de passe chiffré de l'utilisateur (Password Authentication Protocol) ;
- « attr_filter » : permet de filtrer (mise en forme) certains attributs avant de les traiter ;
- « expr » : utiliser pour effectuer des calculs numériques (*, /, +, sha256, etc.) et pour convertir des caractères (ex : « toupper » et « tolower ») ;
- « expiration » : permet de gérer la date d'expiration d'un compte (attribut : « Expiration ») ;
- « logintime » : permet de gérer le « temps de session max » (attribut : « Session-Timeout ») ;
- « sqlcounter » : permet de calculer les notions de temps ou de volume cumulé. Ils sont définis plus loin dans ce chapitre ;
- « ldap » : permet la connexion vers un annuaire externe (chargé uniquement si configuré)

4.3.1 - Débogage

Il est possible de tester l'authentification et l'autorisation d'un utilisateur sur le serveur radius en ligne de commande :

```
echo "User-Name = test,User-Password=test" | radclient -x localhost:1812 auth $(grep '^secret_radius=' /root/ALCASAR-passwords.txt | cut -d=' ' -f2-)
```

ou

```
radtest 'USERNAME' 'PASSWORD' 127.0.0.1 0 $(grep '^secret_radius=' /root/ALCASAR-passwords.txt | cut -d=' ' -f2-)
```

```
# radtest 'test' 'test' 127.0.0.1 0 $(grep '^secret_radius=' /root/ALCASAR-passwords.txt | cut -d=' ' -f2-)
Sent Access-Request Id 135 from 0.0.0.0:39859 to 127.0.0.1:1812 length 74
  User-Name = "test"
  User-Password = "test"
  Cleartext-Password = "test"
Received Access-Accept Id 129 from 127.0.0.1:1812 to 127.0.0.1:39123 length 38
  Alcasar-Filter = HAVP
  Alcasar-Protocols-Filter = Web
  Session-Timeout = 555222
```

Il est possible d'analyser le fonctionnement du serveur radius. Pour cela, arrêtez le DAEMON (systemctl stop radiusd) et relancez-le en mode « debug » (radiusd -X). Vous pouvez alors analyser les requêtes SQL lorsque des utilisateurs se connectent, se déconnectent, échouent à la connexion, etc.

```
Sent Access-Request Id 130 from 0.0.0.0:40775 to 127.0.0.1:1812 length 74
  User-Name = "test"
  User-Password = ██████████
  NAS-IP-Address = 172.16.0.1
  NAS-Port = 0
  Message-Authenticator = 0x00
  Cleartext-Password = ██████████
Received Access-Accept Id 130 from 127.0.0.1:1812 to 0.0.0.0:0 length 36
  Filter-Id = "00000000"
  Session-Timeout = 7200
```

4.3.2 - Les attributs Radius exploités par ALCASAR

ALCASAR exploite plusieurs attributs standards radius (Crypt_Password, Simultaneous-Use, Wispr-Redirection-URL, Login-Time, Expiration, etc.). De plus, pour ses besoins spécifiques, les 6 attributs dédiés suivants ont été créés (cf. [/etc/raddb/conf/radiusd/dictionary.alcasar](#)) :

- Alcasar-Filter (integer) : 1=None, 2=HAVP, 3=BL, 4=WL
- Alcasar-Protocols-Filter (integer) : 1=None, 2=Web, 3=Commons, 4=Custom
- Alcasar-Imputability-Warning (integer) : 1=Yes
- Alcasar-Status-Page-Must-Stay-Open (integer) : 1=Yes, 2=No
- Alcasar-Expire-After (integer) : Temps de connexion autorisé après le premier login (en seconde)
- Alcasar-Reconnect-Timeout (integer) : Usage futur

4.3.3 - Compteurs SQL exploités par ALCASAR

Ces compteurs permettent de calculer des valeurs cumulatives. Ils sont lancés au moment de la connexion des utilisateurs pour valider leur autorisation.

Déclaration des compteurs (section « authorize » de [« /etc/raddb/sites-enabled/alcasar »](#))

```
authorize {
    sql
    noresetcounter
    dailycounter
    monthlycounter
    expiration
    logintime
    pap
}
```

Définition des compteurs SQL (fichier [« /etc/raddb/mods-enabled/sqlcounter »](#)).

Temps de connexion déjà effectué sur la journée (attribut « Max-Daily-Session »)

```
sqlcounter dailycounter {
    sql_module_instance = sql
    counter_name = Daily-Session-Time
    check_name = Max-Daily-Session
    reply_name = Session-Timeout
    key = User-Name
    reset = daily
    query = "SELECT IFNULL((SELECT SUM(acctsessiontime - GREATEST((%%b - UNIX_TIMESTAMP(acctstarttime)), 0)) FROM radacct WHERE username='%${key})' AND UNIX_TIMESTAMP(acctstarttime) + acctsessiontime > '%%b'), 0)"
}
```

Temps de connexion effectué sur le mois en cours (« monthlycounter » = attribut « Max-Monthly-Session »)

```
sqlcounter monthlycounter {
    sql_module_instance = sql
    counter_name = Monthly-Session-Time
    check_name = Max-Monthly-Session
    reply_name = Session-Timeout
    key = User-Name
    reset = monthly
    query = "SELECT IFNULL((SELECT SUM(acctsessiontime - GREATEST((%%b - UNIX_TIMESTAMP(acctstarttime)), 0)) FROM radacct WHERE username='%${key})' AND UNIX_TIMESTAMP(acctstarttime) + acctsessiontime > '%%b'), 0)"
}
```

Temps autorisé cumulé après le premier login » (attribut « Max-All-Session »)

```
sqlcounter noresetcounter {
    sql_module_instance = sql
    counter_name = Max-All-Session-Time
    check_name = Max-All-Session
    key = User-Name
    reset = never
    query = "SELECT IFNULL(SUM(AcctSessionTime), 0) FROM radacct WHERE username='%${key})'"
}
```

Temps autorisé pour une session (attribut « Alcasar-Expire-after »)

```
sqlcounter expire_on_login {
    sql_module_instance = sql
    counter_name = Alcasar-Expire-After-Initial-Login
    check_name = Alcasar-Expire-After
    key = User-Name
    reset = never
    query = "SELECT IFNULL((SELECT TIME_TO_SEC(TIMEDIFF(NOW(), acctstarttime)) FROM radacct WHERE username='%${key})' ORDER BY acctstarttime LIMIT 1), 0)"
}
```

Volume de données autorisé pour une journée (attribut « CoovaChilli-Max-Total-Octets-Daily »)

```
sqlcounter counterCoovaChilliMaxTotalOctetsDaily {
  sql_module_instance = sql
  counter_name = CoovaChilli-Max-Total-Octets-Daily
  check_name = CoovaChilli-Max-Total-Octets-Daily
  counter_type = data
  reply_name = CoovaChilli-Max-Total-Octets
  key = User-Name
  reset = daily
  query = "SELECT IFNULL((SUM(AcctInputOctets + AcctOutputOctets)), 0) FROM radacct WHERE username=%${key}' AND UNIX_TIMESTAMP(AcctStartTime) + AcctSessionTime > %%b"
```

Volume de données autorisé pour un mois (attribut « CoovaChilli-Max-Total-Octets-Monthly »)

```
sqlcounter counterCoovaChilliMaxTotalOctetsMonthly {
  sql_module_instance = sql
  counter_name = CoovaChilli-Max-Total-Octets-Monthly
  check_name = CoovaChilli-Max-Total-Octets-Monthly
  counter_type = data
  reply_name = CoovaChilli-Max-Total-Octets
  key = User-Name
  reset = monthly
  query = "SELECT IFNULL((SUM(AcctInputOctets + AcctOutputOctets)),0) FROM radacct WHERE username=%${key}' AND UNIX_TIMESTAMP(AcctStartTime) + AcctSessionTime > %%b"
```

Volume max de données autorisé (attribut « CoovaChilli-Max-Total-Octets »)

```
sqlcounter counterCoovaChilliMaxAllTotalOctets {
  sql_module_instance = sql
  counter_name = CoovaChilli-Max-All-Total-Octets
  check_name = CoovaChilli-Max-Total-Octets
  counter_type = data
  reply_name = CoovaChilli-Max-Total-Octets
  key = User-Name
  reset = never
  query = "SELECT IFNULL((SUM(AcctInputOctets + AcctOutputOctets)),0) FROM radacct WHERE username=%${key}'"
```

4.3.4 - Module A.D./LDAP externe

Freeradius peut interroger une base externe via le protocole LDAP. Les paramètres de connexion sont renseignés dans le fichier de configuration central d'ALCASAR (/usr/local/etc/alcasar.conf). Le script « alcasar-ldap.sh » se charge de configurer les modules LDAP de freeradius (« /etc/raddb/mods-available/ldap-alcasar »). Un lien symbolique lie le fichier « /etc/raddb/mods-enabled/ldap » vers ce fichier quand « ldap » est activé. Dans le même ordre d'idée, un lien symbolique lie le fichier « /etc/raddb/sites-available/alcasar-with-ldap » vers le fichier « /etc/raddb/sites-enabled/alcasar ». Les paramètres du fichier sont les suivants :

| Paramètres | Définition | Remarques |
|-------------|--|--|
| server | Nom du serveur LDAP (server = "ldap.example.com" ou server = "@IP") | Le port de connexion par défaut est 389. Pour le changer : @serveur:port |
| basedn | Base de recherche des utilisateurs à authentifier | Voir l'exemple ci-dessous dans le cas d'Active Directory. |
| filter | Recherche de l'identifiant ou attribut pour l'authentification | <u>Pour un ldap standard</u> : filter = "(uid=%{Stripped-User-Name:-%{User-Name}})" <u>Pour Active Directory</u> : filter = "(samAccountName=%{Stripped-User-Name:-%{User-Name}})" |
| base_filter | Filtre de recherche ldap complémentaire | Exemples : <ul style="list-style-type: none">- par défaut, vide- base_filter="(objectclass=radiusprofile)"- base_filter="(memberof=groupe_alcasar)" |
| identity | Compte possédant des droits en lecture sur l'annuaire. | Vide = connexion anonyme (LDAP) <u>Obligatoire pour Active Directory</u> (sur le serveur AD, créer un compte standard avec délégation de qui sera utilisé par ALCASAR pour l'interroger l'annuaire à distance). |
| password | Mot de passe associé au compte avec des droits de lecture sur l'annuaire ldap. | Vide = connexion anonyme (LDAP). <u>Obligatoire pour Active Directory</u> . |

Par rapport à l'exemple d'annuaire présenté dans le document d'exploitation, les paramètres de ce fichier seraient les suivants :

```
basedn = "cn=Users,dc=serverad,dc=com"
filter = "(samAccountName=%{Stripped-User-Name:-%{User-Name}})"
identity= "cn=superman,dc=serverad,dc=com"
password = "*****"
```

Il est possible d'analyser la connexion avec le serveur d'annuaire externe à partir du système ALCASAR après avoir installé le paquetage « `openldap-clients` » (*urpmi openldap-clients*).

La commande « `ldapsearch -vWx -h @ip_A.D -b "cn=Users,dc=serverad,dc=com" -D "superman@serverad.com"` » permet de lister l'ensemble des utilisateurs contenu dans « User ».

Les options utilisées dans cette commande sont les suivantes : -v : verbeux, -b : la base recherchée, -D : le dn de l'utilisateur autorisé à lancer une requête sur la base, -W : demande le mot de passe de manière interactive, -x : exploite l'authentification simple plutôt que SASL.

Sur ALCASAR, les utilisateurs authentifiés de cette manière sont affectés dans le groupe d'utilisateurs nommé « ldap ». Il est ainsi possible de leur affecter des attributs particuliers. Pour modifier ce nom de groupe, il suffit d'éditer le fichier « `/etc/raddb/sql/mysql/dialup.conf` » et modifier la valeur « `default_user_profile = "<nouveau groupe>"` ». Relancer le service « `radiusd` » pour la prise en compte de la modification.

Il est aussi possible d'affecter des attributs ALCASAR à un seul utilisateur authentifié A.D/LDAP. Pour cela il faut créer un utilisateur ALCASAR ayant le même nom que celui qui est dans l'annuaire externe. Exemple d'utilisation : tous les élèves d'une école sont gérés dans un annuaire. Il est possible de limiter la bande passante ou les créneaux de connexion pour l'élève ayant abusé de téléchargements. Il suffit de créer un compte sur ALCASAR avec le nom de cet élève et de lui affecter des attributs particuliers.

5 - Fonction « traçabilité et imputabilité »

Plusieurs systèmes de traçabilité-imputabilité ont été évalués afin de définir celui qui serait exploité dans ALCASAR. Le tableau suivant résume le résultat de cette évaluation :

| | NAGIOS | MRTG | CACTI | MUNIN | NETFLOW |
|---|--------|------|-------|-------|---------|
| Licence GPL | | | | | |
| Compatible <u>Mageia</u> | | | | | |
| Charge supplémentaire sur le système | | | | | |
| Espace de stockage nécessaire | | | | | |
| Facilité d'utilisation | | | | | |
| Interface d'administration | | | | | |
| Représentation des données sous forme de graphes | | | | | |
| Accessibilité aux données antérieures | | | | | |
| Contenu des fichiers journaux pour l'imputabilité | | | | | |
| Affichage de la charge par ports | | | | | |

Satisfait :

Convenable :

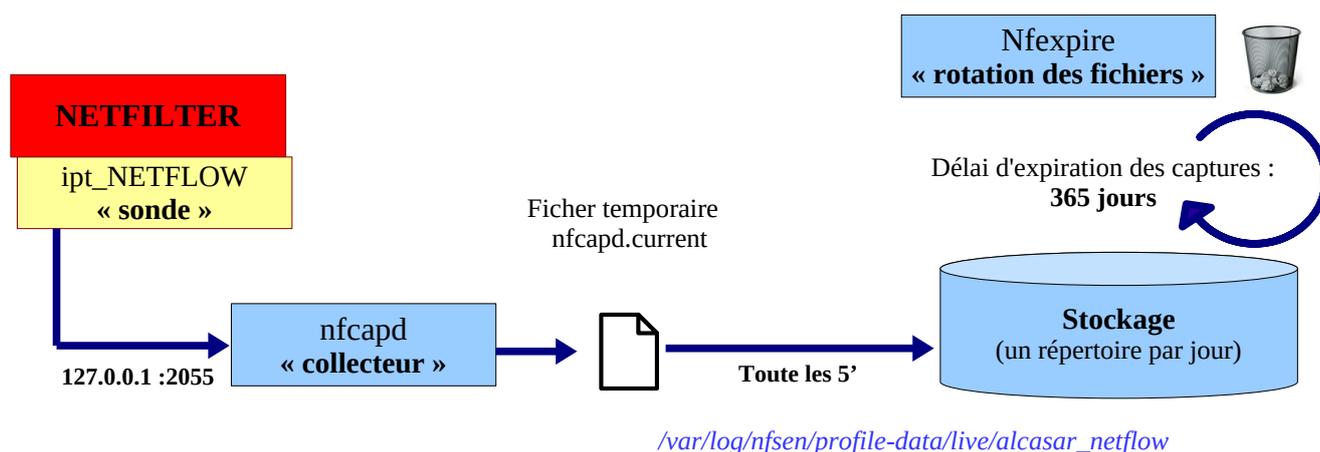
Non satisfait :

5.1 - Journalisation principale

La traçabilité des connexions est gérée par deux canaux de journalisation d'évènements.

1. Le canal général concerne tous les flux des utilisateurs à l'exception des flux HTTP des utilisateurs avec attribut de filtrage (cf. 2^e canal). Les traces sont générées par une sonde NetFlow qui est spécifiquement compilé pour le noyau Linux exploité par ALCASAR (projet « ipt_netflow »). Les flux netflow générés par cette sonde sont manipulés (collecte, interprétation, suppression, etc.) par les outils du projet libre « nfdump ».

Le schéma de fonctionnement de cette sonde est le suivant :



Les flux NetFlow sont générés par la sonde noyau (ipt_NETFLOW) via des règles du parefeu Netfilter (cible « -j Netflow »). Ces flux sont envoyés sur la socket 127.0.0.1:2055 où ils sont récupérés par le collecteur nfcapd qui génère un fichier toutes les 5' dans le répertoire « [/var/log/nfsen/profile_data/live/alcasar_netflow/date_du_jour/](#) » (un répertoire par jour). La commande « nfexpire » est lancée par « crontab » tous les jours à minuit afin de supprimer les fichiers de plus d'un an :

```
Remove netflow files older than one year (daily --> see "cron.daily")
@daily root /usr/bin/nfexpire -e /var/log/nfsen/profiles-data/live/alcasar_netflow -t 365d
```

Chaque semaine, une archive est constituée dans le répertoire « `/var/SAVE` » sous le nom « `traceability-ALL-<date><heure>.tar.gz` » (cf. §5.3).

Les fichiers Netflow ne sont pas directement lisibles. Pour cela, il faut exploiter un **interpréteur Netflow** (ex. : « `Nfdump` ») comme suit : « `nfdump -R <fichier_au_format_netflow> -o extended -a` ». Une fois interprétée, chaque ligne est composée des champs suivants :

| Date first seen | Duration | Proto | Src IP Addr:Port | Dst IP Addr:Port | Flags | Tos | Packets | Bytes | pps | bps | Bpp | Flows |
|-------------------------|----------|-------|----------------------|-----------------------|---------|-----|---------|-------|-----|-----|-----|-------|
| 2020-05-19 23:03:02.978 | 0.000 | TCP | 192.168.182.24:53955 | → 216.239.38.120:443 |S. | 0 | 1 | 60 | 0 | 0 | 60 | 1 |
| 2020-05-19 23:15:10.898 | 133.038 | TCP | 192.168.182.24:49570 | → 216.239.38.120:5228 |S. | 0 | 5 | 300 | 0 | 18 | 60 | 3 |
| 2020-07-04 14:45:29.870 | 0.000 | TCP | 192.168.182.7:48399 | → 104.85.39.74:80 |S. | 0 | 1 | 60 | 0 | 0 | 60 | 1 |

2. Le deuxième canal contient les traces des **flux HTTP** des utilisateurs possédant un attribut de filtrage (blacklist ou whitelist). Ces traces sont générées par une règle « `Ulog` » du pare-feu sur le flux transitant dans le système de filtrage D'ALCASAR (E²Guardian). Ces traces sont écrites dans le fichier « `/var/log/firewall/traceability.log` ». Chaque semaine, ce fichier est copié dans l'archive de traçabilité sous le nom « `traceability-HTTP-<date><heure>.tar.gz` » (cf. §5.3) avant d'être purgé. Dans ce fichier chaque ligne est composée des champs principaux suivants :

Oct 28 03:44:06 alcasar RULE F_http - ACCEPT IN=tun0 OUT= MAC= SRC=192.168.182.2 DST=77.67.27.11 LEN=52 TOS=00 PREC=0x00 TTL=128 ID=19347 DF PROTO=TCP SPT=62934 DPT=80 SEQ=161741080 ACK=0 WINDOW=8192 SYN URG=0

- date**: Oct 28 03:44:06
- Nom de la règle (rule) du pare-feu ayant générée cette ligne**: F_http
- Carte rso par laquelle est entrée la trame**: tun0
- @IP de la station de consultation**: SRC=192.168.182.2
- @IP du serveur destinaire**: DST=77.67.27.11
- Port source**: SPT=62934
- Port destination (forcément 80)**: DPT=80

Legende des actions de filtrage :

- ACCEPT : la trame est sortie sur Internet
- DROP : la trame est restée bloquée

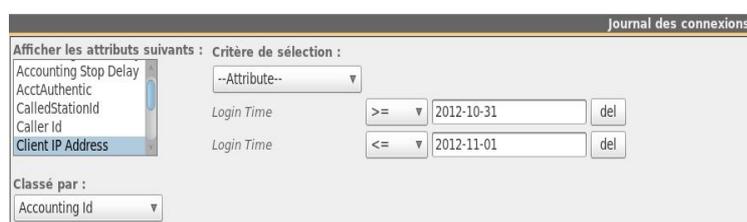
5.2 - journalisation accessoire

- Un canal Ulog génère les fichiers « `/var/log/firewall/ssh.log` » liés aux flux d'administration à distance via le protocole ssh.
- Un canal Ulog génère les fichiers « `/var/log/firewall/ext-access.log` » liés aux tentatives de connexions depuis Internet (fonction « bastion »). Pour ce canal, une protection est mise en place afin de ne pas charger trop le système en cas d'attaque par saturation (flooding).
- Le proxy de filtrage d'URL « E²Gurdian » génère des logs dans le répertoire « `/var/log/e2guardian` » sous le nom : « `access.log` ». Ils présentent les URL ayant été bloquées.
- Le détecteur d'intrusion (IDS) « fail2ban » génère des logs dans « `/var/log/fail2ban` ».

5.3 - Constitution de l'archive de traçabilité

Tous les lundis à 5h35, le gestionnaire de tâche « cron » lance le script « `alcasar-archive.sh` ». Ce script crée un fichier contenant une archive pour chaque canal de journalisation (cf. §5.1) et la base des utilisateurs. Il copie ce fichier sous le nom « `traceability-<date>-<heure>.tar.gz` » dans le répertoire « `/var/Save/archive/` » afin d'être visible dans l'interface de gestion (ACC).

Pour imputer chaque trame, il faut extraire à partir du fichier de la base de données « `radius.sql` » (de la même semaine) le nom de l'utilisateur connecté sur la station de consultation possédant l'adresse IP source. Cette dernière information peut être récupérée directement à partir de l'interface graphique d'ALCASAR (menu « statistique » + « connexions »). Exemple pour chercher les utilisateurs connectés dans la journée du 31/10/2012 :



6 - Fonction « filtrage »

6.1 - Filtrage de protocoles réseau

Cette couche est gérée à l'aide du pare-feu intégré (NetFilter).

Le portail est configuré en mode 'bastion' vis-à-vis d'Internet. Il aiguille et contrôle les flux en provenance du réseau de consultation. Lors de l'installation, les règles du pare-feu sont mises en place.

Le fichier de configuration principal qui conditionne le fonctionnement d'ALCASAR est « [/usr/local/bin/alcasar-iptables.sh](#) ». Il est déconseillé de le modifier afin d'éviter des effets de bords sur le fonctionnement global du portail.

Toutefois, des règles de pare-feu peuvent être surchargées pour autoriser certaines situations particulières (comme l'accès SSH à un équipement de votre LAN depuis Internet par exemple).

Ces règles particulières sont définies dans le fichier « [/usr/local/etc/alcasar-iptables-local.sh](#) » qui est appelé par le fichier de configuration principal du pare-feu. Ce fichier comporte plusieurs ensembles de règles d'exemple qui correspondent à des configurations que des utilisateurs d'ALCASAR ont eu besoin. Il est possible d'activer ces ensembles de règles en les adaptant et en les dé-commentant.

Pour forcer les utilisateurs à passer par le service DNS du portail, le pare-feu effectue une redirection du port 53 vers [l'@IP](#) locale. Cela permet de couper court aux éventuels tunnels DNS (sur le port 53 uniquement).

6.2 - Filtrage de noms de domaines, d'URLs et d'adresses IP

Ce filtrage s'appuie sur l'excellente liste de l'Université de Toulouse qui est organisée en répertoires. Chaque répertoire porte le nom d'une catégorie (adulte, secte, shopping, etc.). Chaque répertoire peut contenir 1 à 3 fichiers contenant la liste des « noms de domaine », des « URLs » et des « @IP » de cette catégorie. Un quatrième fichier permet de savoir si la catégorie est « noire » (blacklist) ou blanche (whitelist) ou les deux. ALCASAR traite cette liste afin de l'exploiter selon 3 techniques différentes :

1. filtrage de noms de domaine : ALCASAR s'appuie sur ses serveurs de DNS internes (« unbound ») ;
2. filtrage d'URLs : ALCASAR s'appuie sur le proxy HTTP « E²Guardian » ;
3. filtrage d'adresses IP : C'est le pare-feu d'ALCASAR qui traite les @IP de la liste.

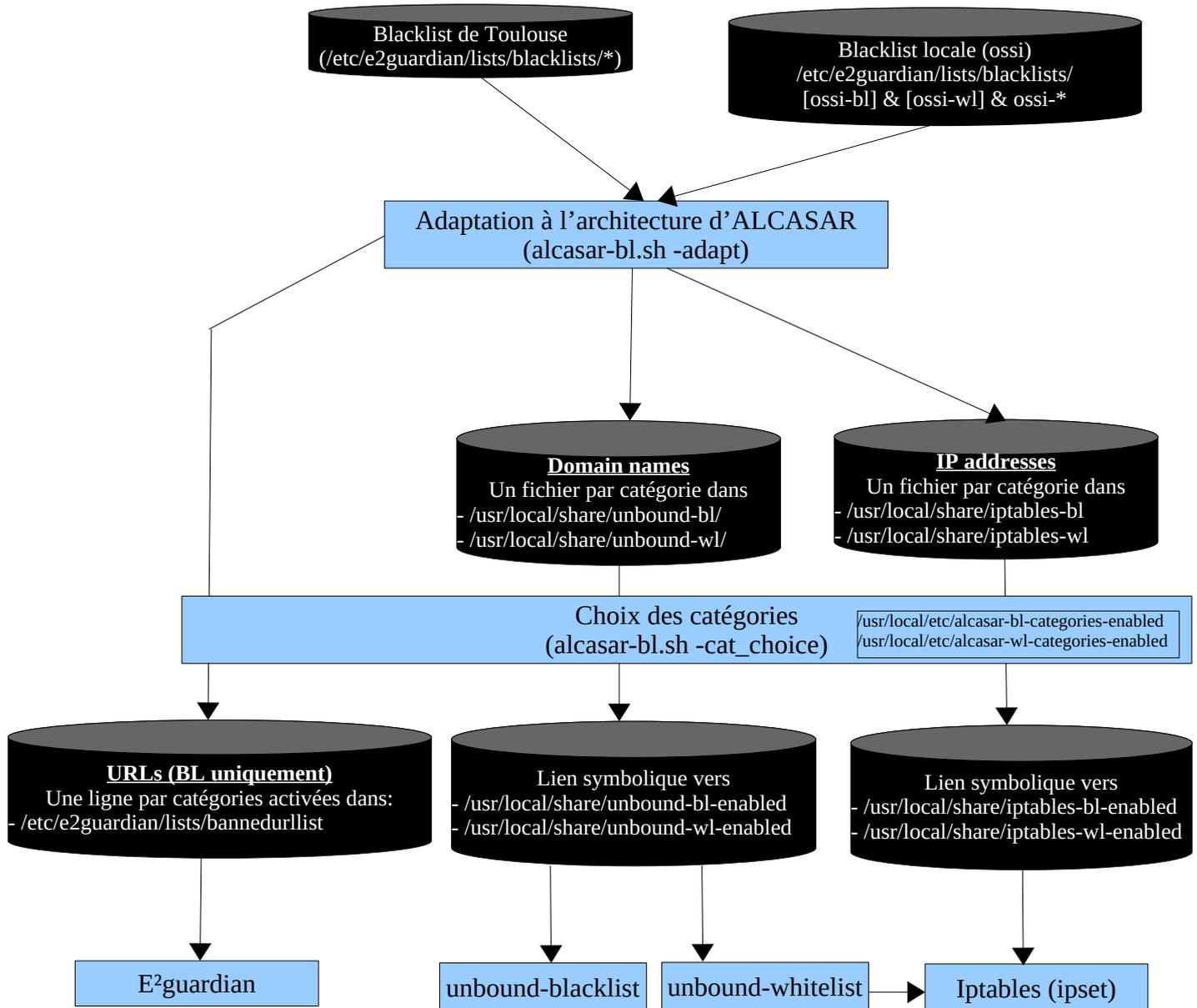
L'architecture d'ALCASAR rend le contournement du filtrage très compliqué. Celui-ci est toujours possible par l'ouverture d'un tunnel (VPN) à destination d'un équipement maîtrisé situé sur Internet dont l'internaute connaît l'adresse IP. Pour fonctionner, ce tunnel doit faire transiter l'ensemble des protocoles de la station de consultation (dont le DNS).

Quoi qu'il en soit, ce type de tunnel ne permet pas de contourner l'authentification. Ainsi, ALCASAR trace et impute les trames de ce tunnel. En cas de problème, et si l'enquête détermine que la sortie du tunnel est impliquée, le portail pourra être sollicité pour déterminer quel utilisateur a créé ce tunnel.

Dans le cas de la WhiteList, ce contournement par VPN n'est pas possible. En effet, ALCASAR tient à jour de manière dynamique les @IP autorisées en fonction des appels DNS réalisés par l'internaute.

6.2.1 - Traitement de la liste de Toulouse

Afin de permettre cette triple exploitation, le script « `alcasar-bl.sh` » effectue le traitement suivant lors de l'installation, de la mise à jour ou du choix des catégories de la Blacklist :



6.2.2 - Filtrage par utilisateur/groupe

Quand un utilisateur réussi sont processus d'authentification, le daemon 'chilli' lance le script « `/usr/local/bin/alcasar-conup.sh` ». Ce script récupère l'ensemble des attributs de l'utilisateur. En fonction de l'attribut de filtrage « `Filter_Id` », le script positionne l'adresse IP de l'utilisateur dans l'IPSET correspondant.

Quand l'utilisateur se déconnecte, le daemon 'chilli' lance le script « `/usr/local/bin/alcasar-condown.sh` » qui retire l'adresse IP de l'utilisateur de l'IPSET correspondant.

Quatre IP_SET ont été créés pour gérer les différentes possibilités de filtrage. Le filtrage affecté à un utilisateur est défini par l'attribut radius « `Filter_Id` ». La liste suivante résume les valeurs des IPSET et de l'attribut « `Filter_Id` » :

- IPSET=« `not_filtered` » pour les utilisateurs sans filtrage. « `Filter_Id` » : `Filter_Id=00000000`
- IPSET=« `av` » pour les utilisateurs filtrés avec un antimalware (réservé pour un usage futur). `Filter_Id=00000001`
- IPSET=« `av_bl` » pour les utilisateurs filtrés par la liste noire. `Filter_Id=00000011`
- IPSET= « `av_wl` » pour les utilisateurs filtrés par la liste blanche. `Filter_Id=00000101`

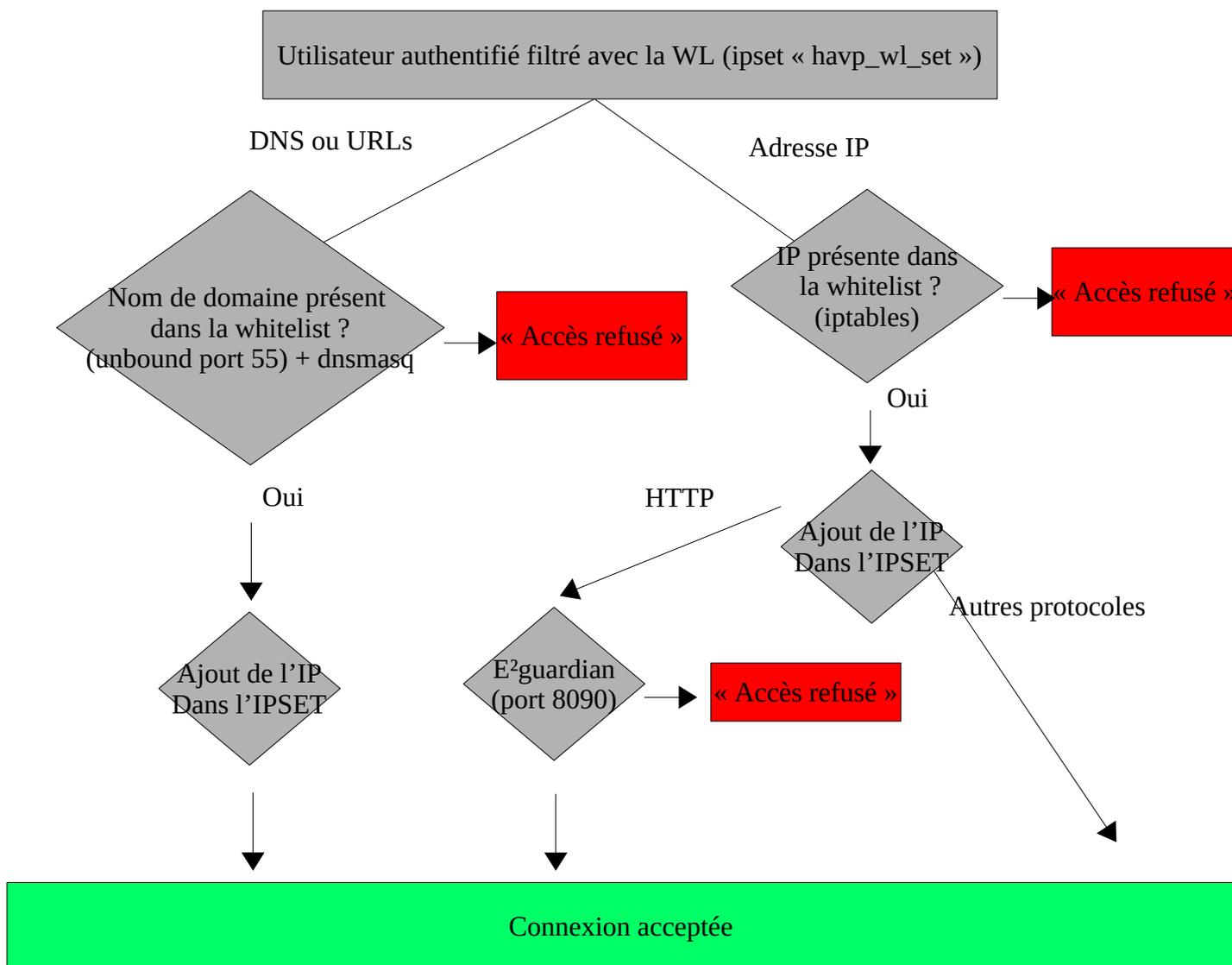
6.2.3 - Double filtrage de la WhiteList (WL)

Un utilisateur filtré avec la WL ne peut consulter que des sites ou des IP définis préalablement. La WL se décompose en plusieurs catégories de noms de domaine pouvant être sélectionnées et mises à jour dans l'ACC. La liste complète des noms de catégorie est située dans [« /usr/local/etc/alcasar-wl-categories »](#). La liste des seules catégories activées est située dans [« /usr/local/etc/alcasar-wl-categories-enabled »](#). Ce sont des liens symboliques pointant vers la liste complète.

Les adresses IP des utilisateurs « whitelists » connectés (authentifiés) sont stockées dans l'IPSET « av_wl ». Lorsqu'un utilisateur se connecte au portail avec cet ipset, ALCASAR va résoudre les requêtes de cet utilisateur via le daemon « unbound-whitelist » (port UDP 55). Si le site en question est présent dans la liste des sites [« /usr/local/share/unbound-wl/*.conf »](#), le daemon peut résoudre le nom de domaine et récupérer l'@IP du site qui est retourné à l'utilisateur. Cette @IP est ajoutée simultanément à l'IPSET « whitelist_ip_allowed » afin d'autoriser l'utilisateur à l'atteindre.

Cette méthode permet d'éviter qu'un utilisateur « whitelisted » puisse contourner le filtrage en se connectant sur un site directement au moyen de son adresse IP (sans résolution de domaine).

Il est possible via l'ACC d'ajouter manuellement de nouveau [site/@IP](#). Les sites seront ajoutés dans le fichier [« /usr/local/share/unbound-wl/ossi-wl.conf »](#). Un lien symbolique sera alors créé pour que ces ajouts soient pris en compte ici [« /usr/local/share/unbound-wl-enabled/ossi-wl »](#). Les adresses IP seront ajoutées dans le fichier [« /usr/local/share/ossi-ip-wl »](#). Le script permettant cet ajout se trouve dans [« /usr/local/bin/alcasar-bl.sh »](#). Voici un schéma récapitulatif du fonctionnement du double filtrage de la WL :



6.2.4 - Filtrage avec la BlackList (BL)

En utilisant ses serveurs DNS, ALCASAR va pouvoir déterminer si le site demandé par l'utilisateur est interdit. Si tel est le cas, l'utilisateur sera renvoyé vers l'[@IP](#) du portail (page de filtrage). Ce filtrage offre l'avantage de pouvoir interdire un nom de domaine, quel que soit le protocole demandé (HTTP, HTTPS, FTP, etc.).

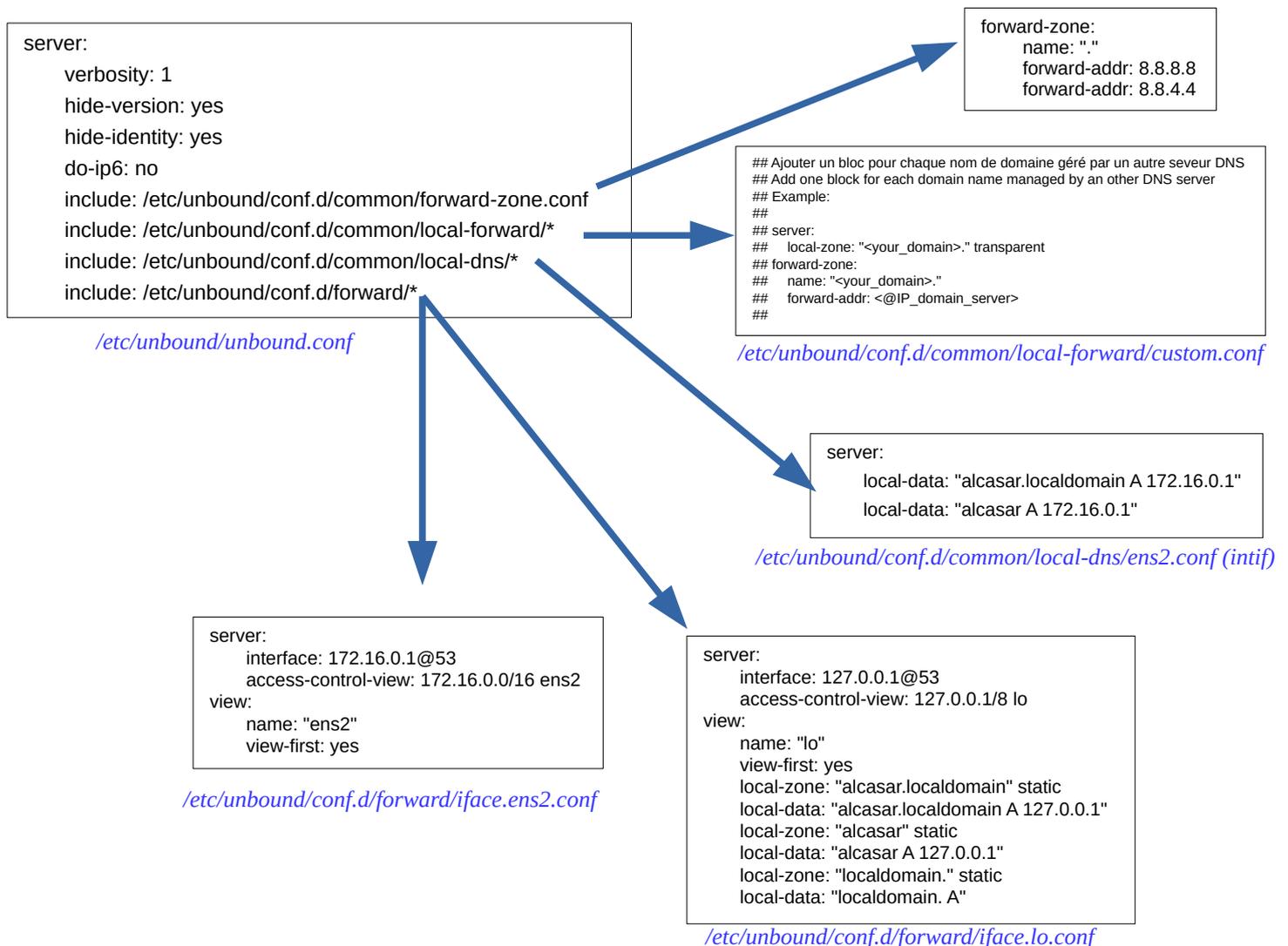
Tout comme la WL, la BL est organisée en catégories. ALCASAR permet de sélectionner ces catégories via l'interface de gestion (ACC). La liste des noms de catégorie ([/usr/local/etc/alcasar-bl-categories](#)) et la liste des catégories activées sont situées dans le répertoire de configuration d'ALCASAR ([/usr/local/etc/alcasar-bl-categories-enabled](#)).

6.2.5 - Configuration DNS

Dans cette fonction de filtrage, le serveur DNS joue un rôle principal. Ainsi, en fonction de son Ipset (cf. §2.2.2), l'utilisateur est redirigé sur un serveur DNS lié à son attribut de filtrage. 4 serveurs DNS (unbound) reçoivent ainsi les requêtes DNS des utilisateurs en fonction de leur redirection. Les schémas suivants montrent l'architecture de ces 4 serveurs DNS. Ces schémas s'appuient sur la configuration d'un ALCASAR d'exemple ayant les paramètres suivants : DNS=8.8.8.8 et 4.4.4.4 ; @IP_LAN=172.16.0.1/24 ; INTIF=ens2 ; nom de domaine par défaut (alcasar.localdomain).

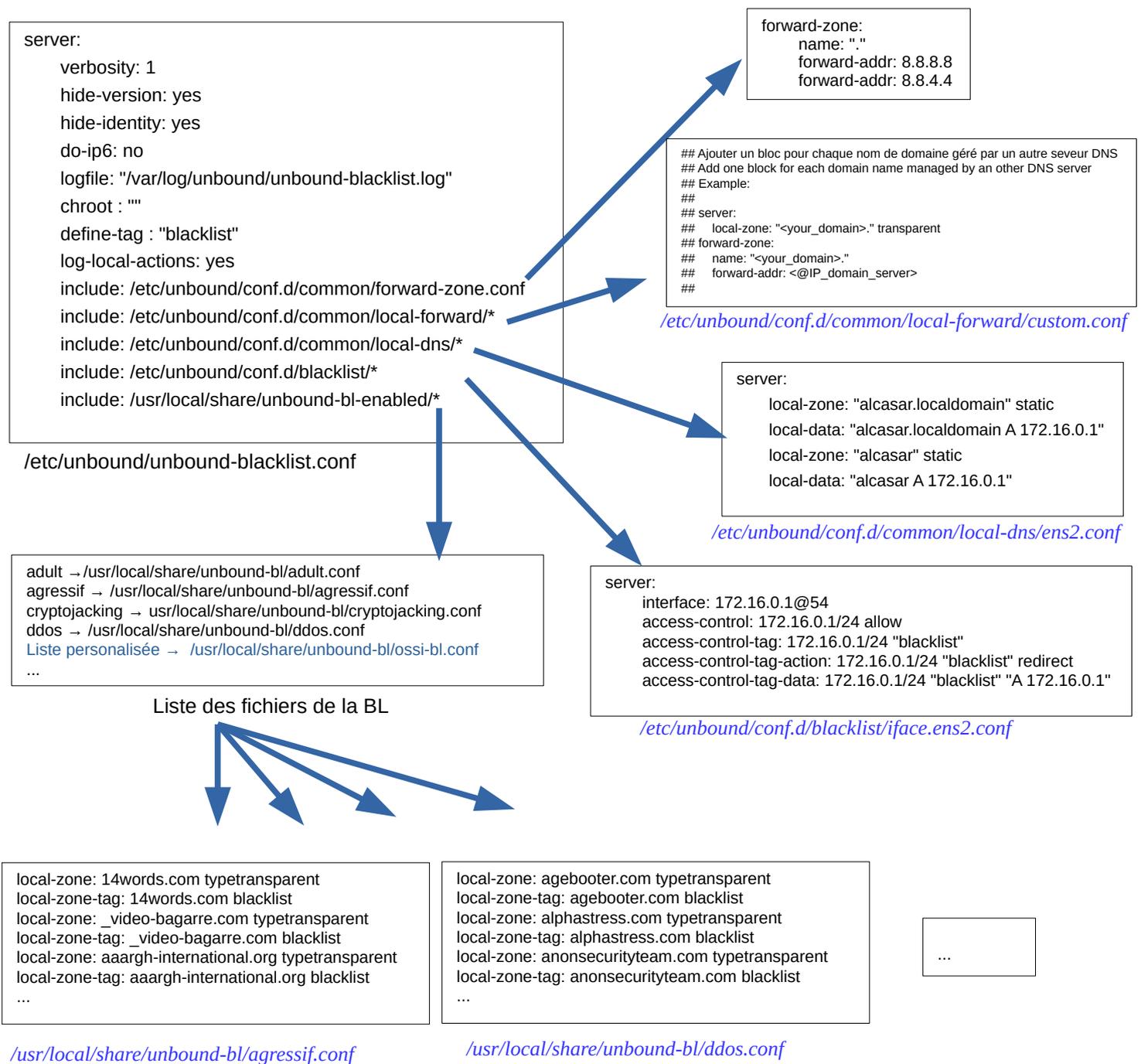
Unbound forward (port 53)

Cette instance de DNS reçoit les requêtes des utilisateurs sans filtrage.



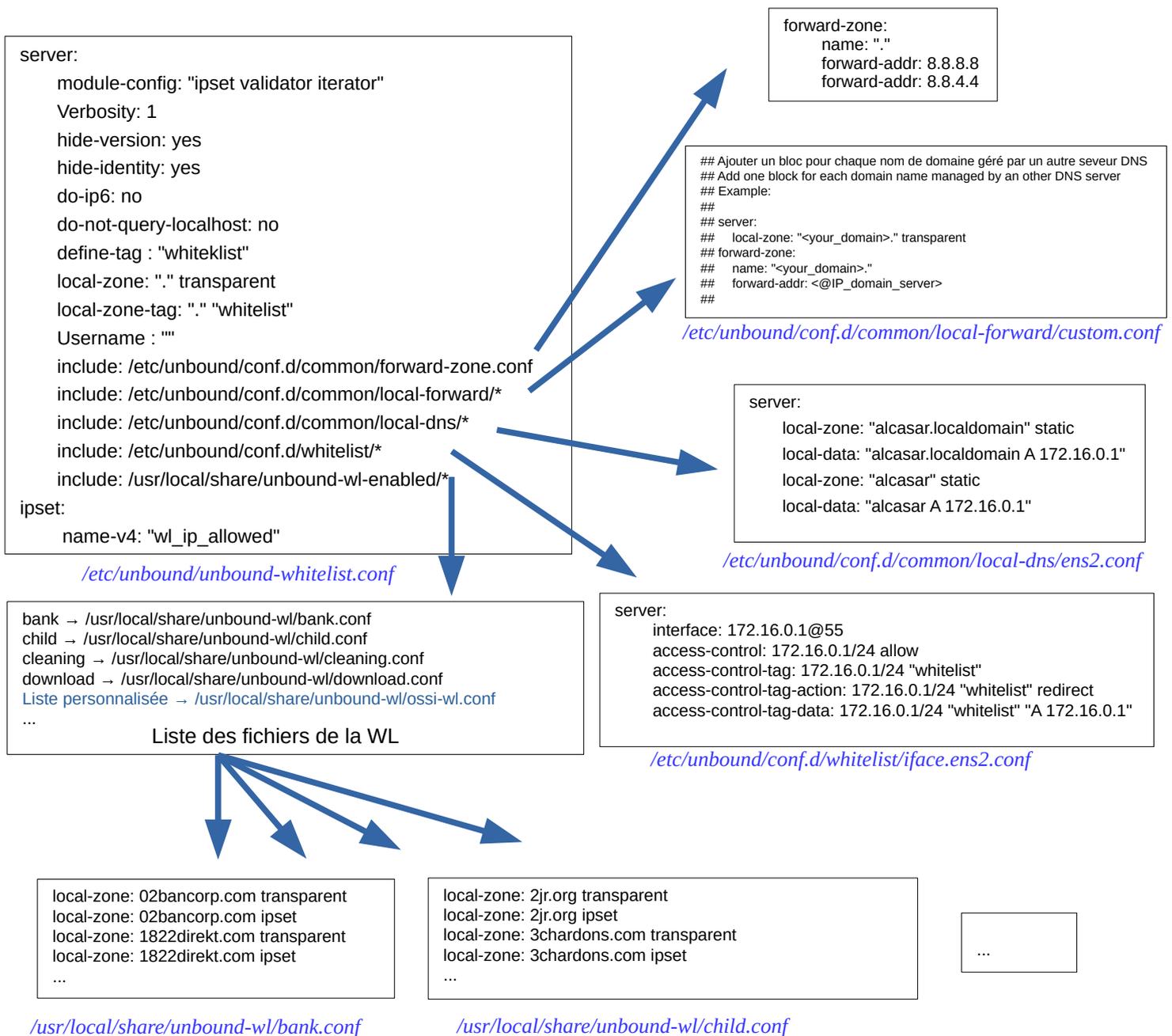
Unbound blacklist (port 54)

Cette instance de DNS reçoit les requêtes des utilisateurs « blacklistés ».



Unbound whitelist (port 55)

Cette instance de DNS reçoit les requêtes des utilisateurs « whitelistés ». Le module « ipset » est exploité pour alimenter dynamiquement netfilter (ipset : « wl_ip_allowed »). Pour cela, l'instance doit être lancée avec les droits « root ».

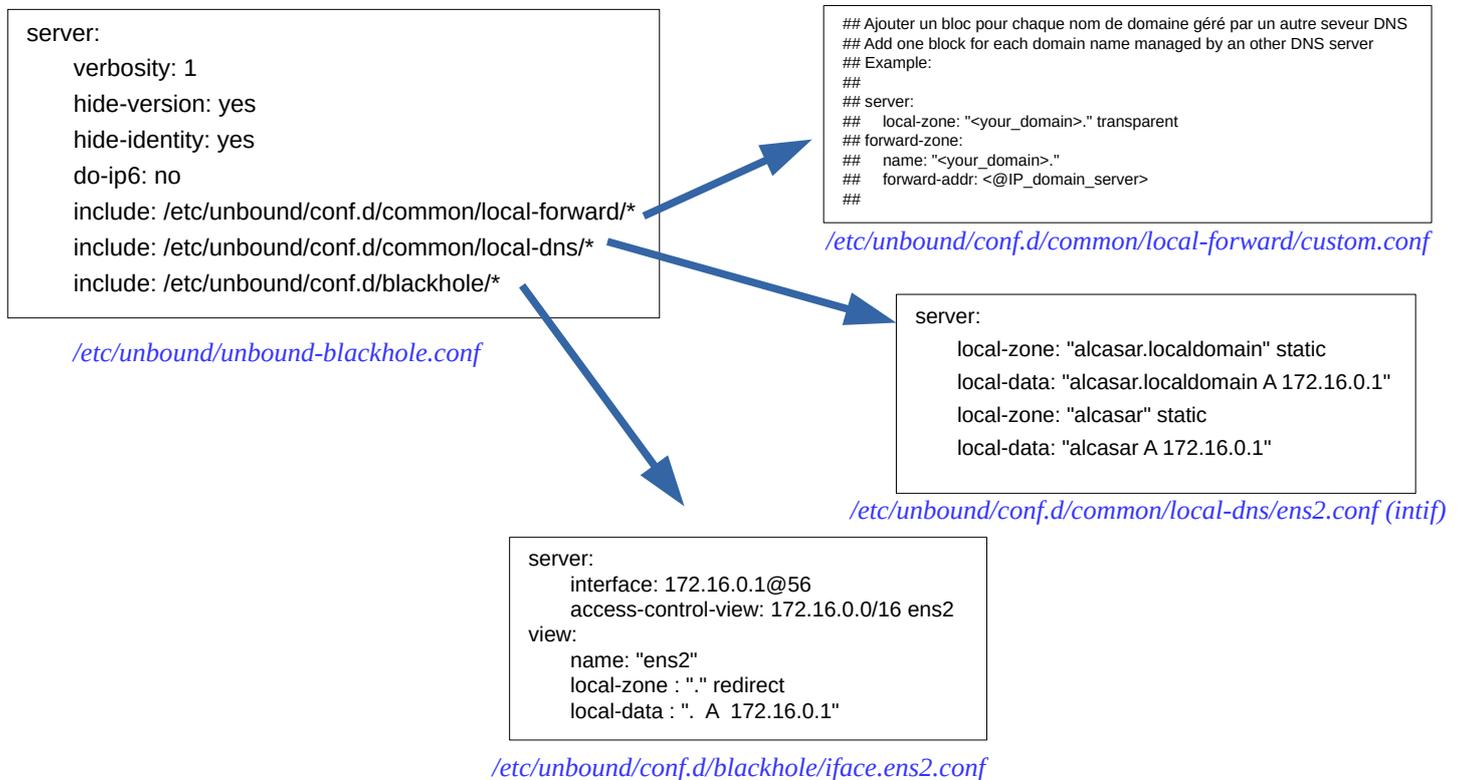


Particularité : Afin de supprimer les fenêtres de détection des portails captifs intégrées aux navigateurs, les domaines suivants doivent être whitelistés :

- Firefox : detectportal.firefox.com → déjà dans la liste « liste_bu »
- Chrome/Chromium : gstatic.com → déjà dans la liste « liste_bu »
- Edge : www.msftconnecttest.com (www.msftconnecttest.com/connecttest.txt)

Unbound blackhole (port 56)

Cette instance de DNS sert à rediriger toutes les requêtes des utilisateurs vers l'@IP d'ALCASAR. Cela n'arrive que quand le watchdog (alcasar-watchdog.sh) détecte que l'accès WAN est hors de service.



7 - Fonction « Interface de gestion »

Cette fonction (ALCASAR Control Center) est réalisée en PHP. Les possibilités de cette interface sont décrites dans la documentation d'exploitation. L'ACC est située dans le répertoire « [/var/www/html/acc](#) ».

Elle est protégée en accès par le module d'authentification « htdigest » de Lighttpd dont le fichier de configuration est « [/etc/httpd/conf/webapps.d/alcasar.conf](#) »

Le répertoire « [/usr/local/etc/digest/](#) » contient les fichiers des identifiants et des mots de passe des administrateurs en fonction de leur profil :

- key_all
- key_admin
- key_manager
- key_backup

8 - Fonction « modules complémentaires »

8.1 - Import de comptes

Dans le cadre de la gestion des comptes d'authentifications, il est possible d'importer une liste de comptes attachés à un groupe prédéfini. Cette fonctionnalité accessible depuis l'interface de gestion génère un fichier <import-user>.pwd pour chaque importation et ajoute les utilisateurs dans le groupe (optionnel) de la base de données. Pour l'instant, seul le groupe peut-être attaché aux identifiants ; c'est-à-dire qu'aucun renseignement supplémentaire n'est importable pour le moment.

Le script « *import_user.php* » du répertoire « */var/www/html/acc/manager/htdocs* » permet d'importer le fichier au format csv ou txt et le script « *import_file.php* » permet de ...

L'importation d'un fichier génère un fichier associé comportant les mots de passe en clair des utilisateurs importés. Ce dernier est téléchargeable pour être distribué aux utilisateurs. Afin de les supprimer périodiquement, une tâche, planifiée toutes les 30min lance le script « *alcasar-import-clean.sh* » qui cherche et supprime les fichiers datant de plus de 24h00.

8.2 - Inscription par SMS

8.2.1 - Fonctionnement global

Ce module permet aux utilisateurs de s'auto-inscrire sur ALCASAR en envoyant un mot de passe par SMS sur à ALCASAR. Un compte est alors créé dont le nom de login est le Nro de GSM de l'utilisateur. Ce module fonctionne grâce au projet « Gammu » (plus précisément Gammu_smsd) qui permet de stocker en base de données (cf. schéma de cette base en P11) les SMS reçus par un MODEM-GSM (ou clé-3G) connecté sur le port USB. Pour un bon fonctionnement, le code PIN de la carte SIM doit être renseigné dans le fichier de configuration de Gammu-smsd : « */etc/gammu_smsd_conf* ».

Fonctionnement :

L'administrateur peut lancer *gammu-smsd* à partir de l'ACC (menu « Authentification/Inscription par SMS ». Il est possible de suivre le journal d'évènements : « *tail -f /var/log/gammu-smsd/gammu-smsd.log* »

À chaque lancement, le script « */usr/local/bin/alcasar-sms.sh --start* » vérifie que le groupe « sms » est bien créé. Il le crée le cas échéant.

En fonctionnement, gammu-smsd dialogue avec le modem-GSM. Les SMS reçus par le modem-GSM sont alors récupérés puis stockés dans la table « inbox » de la base de données « gammu ».

Sur chaque réception de SMS, gammu-smsd, lance le script « /usr/local/bin/alcasar-sms.sh --new_sms ». Ce script permet de traiter le SMS selon le schéma de la page suivante.

Actuellement, l'administrateur à la possibilité :

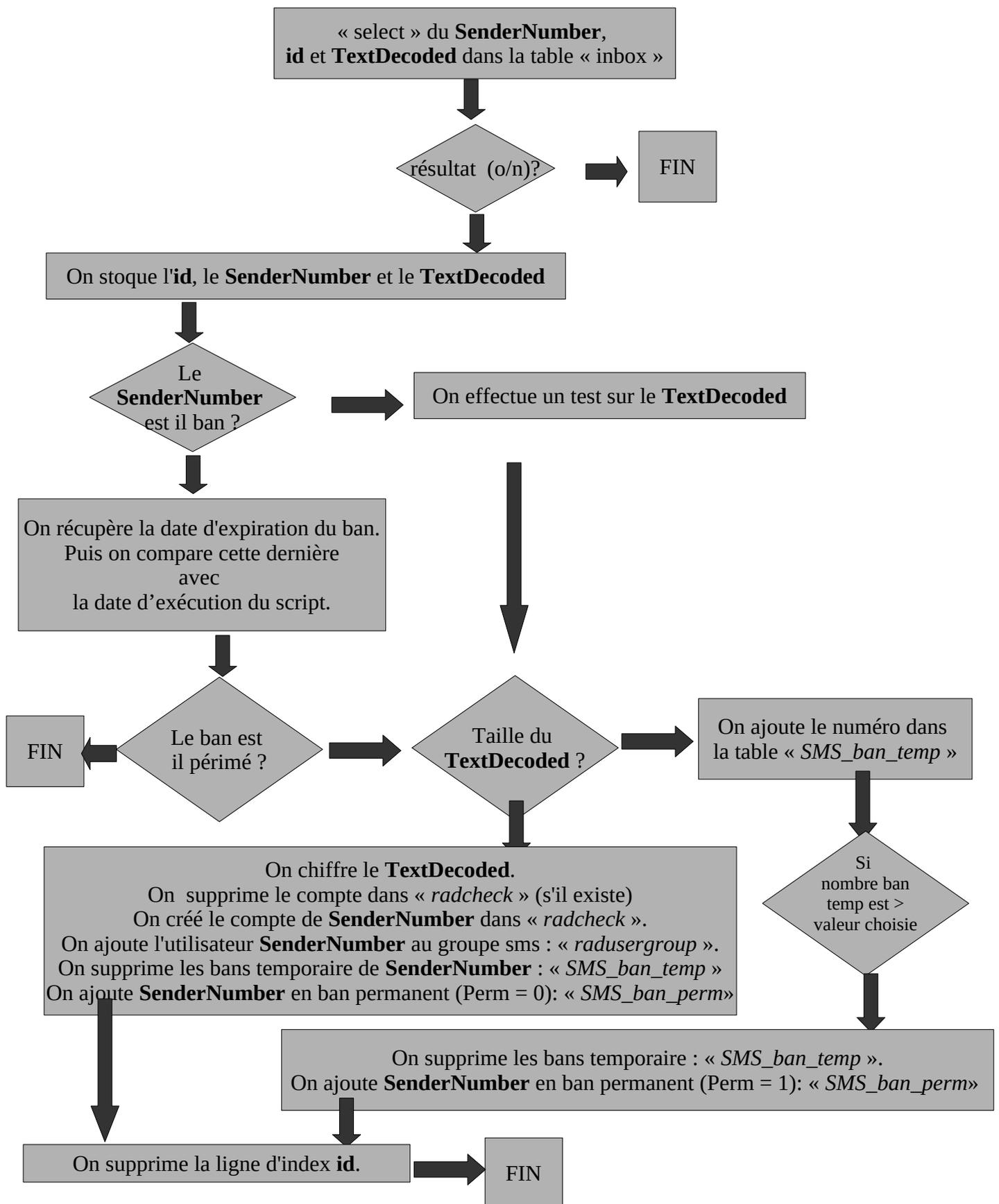
- *Lancer et arrêter gammu-smsd*
- *Renseigner le code PIN de la carte SIM présente dans le modem-GSM.*
- *Renseigner la durée d'une session pour les comptes auto enregistrés.*
- *Renseigner le nombre de bannissements temporaire permis avant le bannissement permanent.*
- *Renseigner la durée d'un bannissement permanent (en jours).*

On retrouve aussi sur cette page d'administration un tableau récapitulatif des comptes bannis :

- *soit pour une raison de Compte existant*
- *soit pour une raison d'excès d'envois de SMS au serveur (Flood).*

L'administrateur peut alors supprimer les numéros bannis. Cette action :

- *supprime le numéro de l'expéditeur du SMS de la table des bannissements permanents (« SMS_ban_perm »),*
- *supprime le numéro de la table du groupe « SMS » (« radusergroup »)*
- *supprime le numéro de la table des comptes radius (« radcheck »).*



8.2.2 - Dialogue avec le modem-GSM – déblocage avec le code PUK

« gammu-smsd » dialogue avec le modem-GSM au moyen de commandes « AT ». Ces commandes permettent de faire un grand nombre d'actions, de la composition d'un numéro de téléphone à l'envoi de SMS, en passant par la récupération de l'état du modem. La syntaxe de ces commandes suit le schéma suivant : « AT+commande ». Les deux premiers caractères (AT) sont l'abréviation du mot 'ATTention'. Ils permettent d'avertir le modem, afin qu'il prenne en compte la commande qui suit. La syntaxe « AT^commande » correspond aux commandes « étendues » pour les modem-GSM de type 3G.

- Liste de commandes AT: <http://www.activexperts.com/sms-component/at/etsi/>
- Liste de commandes AT spécifique Huawei : rechercher « HUAWEI UMTS Datacard Modem AT Command Interface Specification » dans un moteur de recherche.

Une fois « gammu-smsd » lancé, il vérifie l'état de la carte SIM en envoyant la commande : « AT+CPIN? ». Le modem-GSM répond en demandant le code PIN de la carte SIM. Gammu-smsd utilise alors le code PIN écrit dans le fichier de configuration « /etc/gammu_smsd_conf ».

Si ce code PIN est erroné, la carte SIM sera bloquée. Il faudra alors exploiter le code PUK pour la débloquent. La manipulation suivante permet de débloquent la carte SIM à l'aide d'un terminal et de commandes AT.

Arrêtez le service gammu via l'ACC ou via la commande « *alcasar-sms.sh --stop* »

Dans un premier temps, installez « Minicom » sur votre système Linux : « *urpmi minicom* ». Modifiez la configuration de Minicom en lançant la commande « *minicom -s* ». Sélectionnez la 3e entrée (Serial port setup // Configuration du port série). Configurez le port série avec les paramètres suivants (cf. copie d'écran ci-dessous). Une fois les configurations effectuées, appuyer sur « échap » puis déplacer vous dans le menu pour enregistrer les modifications (Save setup as dfl // Enregistrer config. sous dfl). Vous pouvez alors quitter le menu (Exit from Minicom // Sortir de Minicom).

```
+-----+
| A - Serial Device       : /dev/ttyUSB0
| B - LockFile Location  : /var/lock
| C - Callin Program     :
| D - Callout Program    :
| E - Bps/Par/Bits       : 115200 8N1
| F - Hardware Flow Control : Yes
| G - Software Flow Control : No
+-----+
Change which setting?
+-----+
| Screen and keyboard
| Save setup as dfl
| Save setup as..
| Exit
| Exit from Minicom
+-----+
```

```
+-----[configuration]-----+
| Filenames and paths
| File transfer protocols
| Serial port setup
| Modem and dialing
| Screen and keyboard
| Save setup as dfl
| Save setup as..
| Exit
| Exit from Minicom
+-----+
```

Pour se connecter au modem-gsm, lancez la commande : « *minicom -c on* ». Vérifier la connexion au modem avec la commande suivante : « AT ». Si la configuration est correcte, le modem devrait renvoyer « OK ».

La commande « AT+CPIN? » permet de connaître l'état de la carte SIM. La copie d'écran ci-contre, montre la demande de code PIN de la carte SIM afin de pouvoir être exploitée : « +CPIN : SIM PIN ». La commande « AT+CPIN="xxxx" » (où xxxx correspond à votre code PIN), permet de renseigner le code PIN de la carte. Testez alors à nouveau l'état de la carte SIM.

Dans le cas où la carte SIM est bloquée, le modem retourne « +CPIN : SIM PUK ». Récupérez le code PUK (disponible généralement en ligne sur le compte d'abonnement, ou fourni avec la carte SIM). Exécutez alors la commande « AT+CPIN="yyyyyyyy","zzzz" » (où yyyyyyyy correspond à votre code PUK et zzzz correspond à votre nouveau code PIN).

Remarque :

- Vous pouvez accéder au menu de Minicom via la combinaison de touche : « Ctrl+a » puis « z »
- Le modem vous retourne « OK » si la commande envoyée est correcte (syntactiquement) et reconnue.

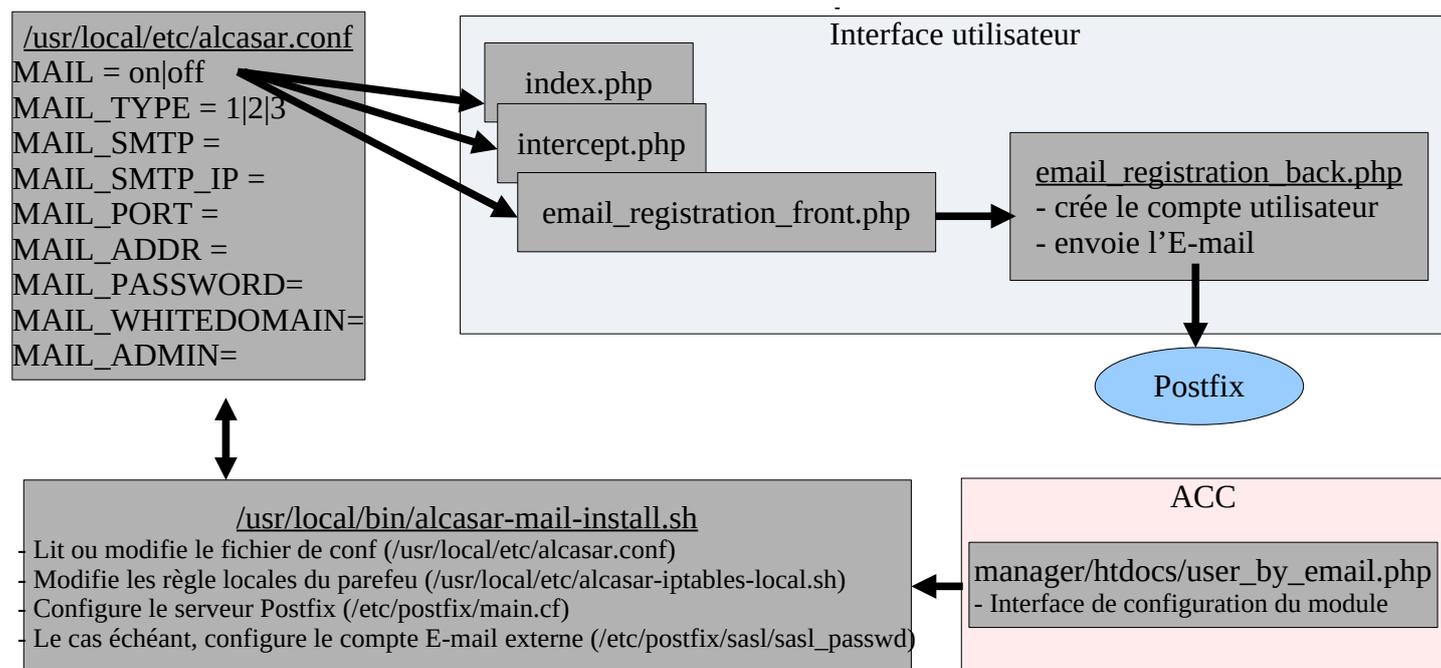
```
AT+CPIN?
+CPIN: SIM PIN
OK
AT+CPIN="1234"
OK
AT+CPIN?
+CPIN: READY
OK
```

8.3 - Inscription par adresse électronique

L'objectif de ce module est de permettre aux utilisateurs de s'auto-inscrire en renseignant leur adresse e-mail. ALCASAR crée alors un nouvel utilisateur donc le login est l'adresse e-mail. Un mot de passe aléatoire est envoyé à cette adresse. Comme ce type d'inscription ne permet pas systématiquement d'imputer les traces de connexion (cas des adresses e-mail à usage unique par exemple), l'administrateur doit configurer les noms de domaine qui seront les seuls autorisés (ex : airbus.com, sncf.fr, etc.). Ce module a été initialement imaginé et développé par K@M3L & T3RRY (LaPlateform).

ALCASAR peut envoyer des e-mails selon 3 méthodes différentes :

1. il est serveur de messagerie ;
2. Il relaie vers un serveur de messagerie externe (serveur d'entreprise par exemple) ;
3. Il utilise un compte de messagerie géré par un serveur externe (free, sfr, orange, etc.).



Debug:

Les journaux de Postfix sont visibles via « journalctl -f -u postfix ». Il est possible d'augmenter le niveau de log par serveur de mail en ajoutant l'entrée « debug_peer_list = free.fr, gmail.com » dans « /etc/postfix/main.cf » La configuration de postfix est visualisable via la commande « postconf -a ».

Pour gérer la queue de messages de postfix : <https://mailmum.io/posts/manage-postfix-mail-server-queues/>

- Lire la queue de messages : « postqueue -p » ou « mailq »
- Lire le message Id de la queue : « postcat -q Id »
- Supprimer le message Id de la queue : « postsuper -d Id » ou « postsuper -d ALL »

Pour la 3^e méthode (postfix comme « client de messagerie »), Postfix exploite les bibliothèques « cyrus-sasl » pour s'authentifier sur un serveur externe (vérifiable via la commande « postconf -A »).

La qualité des Email peut-être testée via le site « mail-tester.com ».

8.4 - Watchdog

Ce script (« [alcasar-watchdog.sh](#) ») est lancé toutes les 3 minutes par le Daemon « crond ». Il permet de couvrir les fonctions suivantes :

- éviter les « oublis » de déconnexion (utilisateur ayant fermé la fenêtre de connexion, panne d'équipement réseau, etc.) ;
- limiter le risque lié à l'usurpation d'adresse IP et d'adresse MAC sur le réseau de consultation (pirate interne) ;
- modifier la page WEB présentée aux utilisateurs en cas de problèmes de connectivité détectés coté Internet

il peut possible de désactiver le « watchdog » en commentant la ligne ci-dessous dans le fichier

« /etc/cron.d/alcasar-watchdog », puis, d'avertir « crond » de la modification : « `systemctl restart crond.service` »

```
# activation du "chien de garde" (watchdog) toutes les 3'
#*/3 * * * * root /usr/local/bin/alcasar-watchdog.sh > /dev/null 2>&1
```

8.5 - Statistiques réseau

Afin de protéger la vie privée des utilisateurs conformément aux préconisations de la CNIL, les statistiques de navigation ne comportent pas d'éléments permettant de lier les flux aux comptes des utilisateurs.

Il est possible via l'interface d'administration d'obtenir une représentation graphique de la charge réseau d'ALCASAR. Une sonde Netflow a été compilée à cet effet. Deux règles de pare-feu permettent de traiter tous les flux sortants par cette sonde

- Flux transitant dans les proxy HTTP internes : `$IPTABLES -A OUTPUT -o $EXTIF -p tcp --dport http -j NETFLOW`
- Flux sortant directement : `$IPTABLES -A FORWARD -i $TUNIF -s $PRIVATE_NETWORK_MASK -m state --state NEW -j NETFLOW`

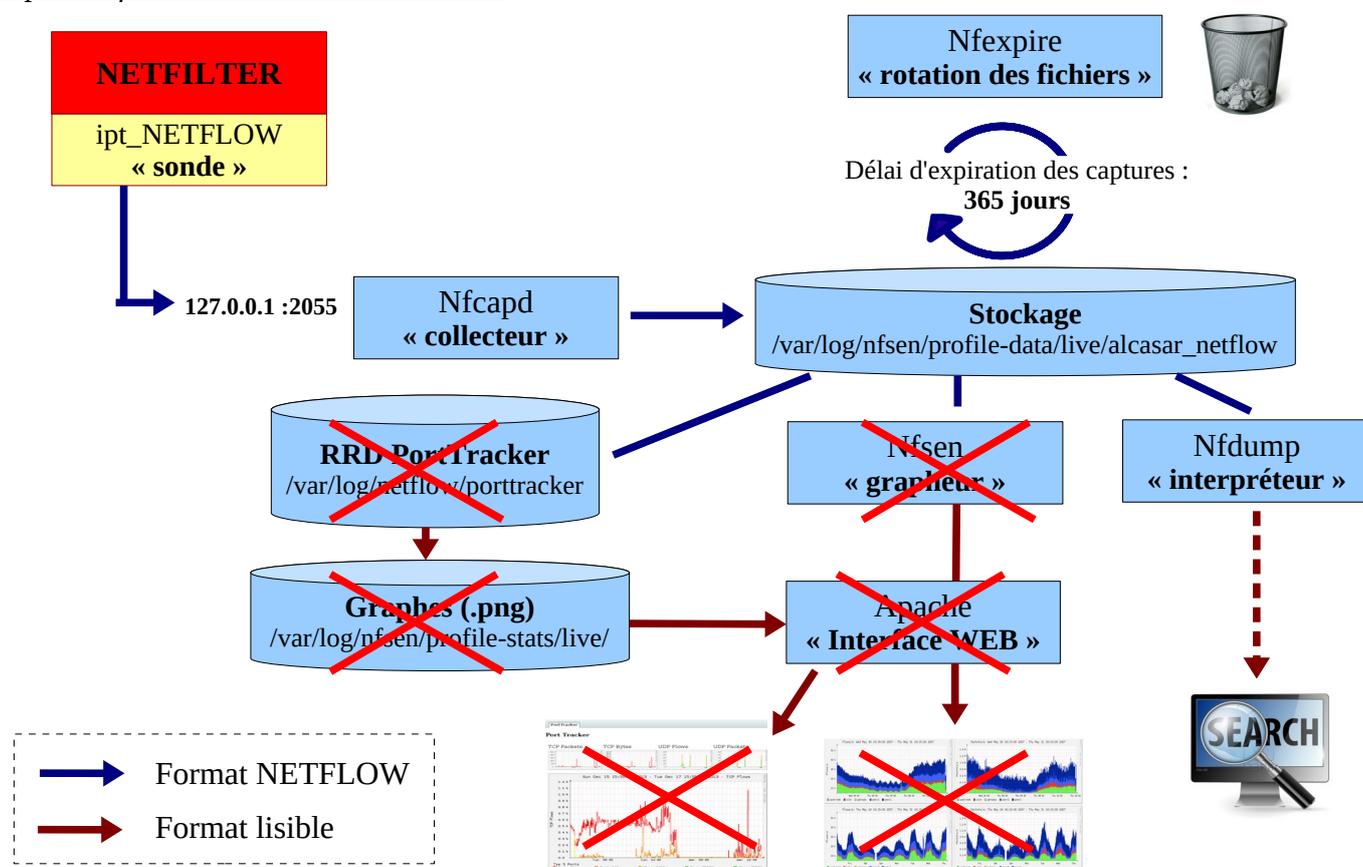
Le module `ipt_NETFLOW` d'ALCASAR exporte ses informations sur la socket `127.0.0.1 :2055`.

La fonction de collecteur est prise en compte par le démon « `nfcapd` » en écoute sur le port 2055. Il collecte les flux NetFlow et crée un fichier toutes les 5 minutes dans le répertoire « `/var/log/nfsen/profile-data/live/alcasar_netflow/` ».

Le module `Nfexpire` (installé avec le RPM « `nfdump` ») permet de réaliser une rotation sur les fichiers capturés par « `nfcapd` ». Une règle ajoutée à « `/etc/cron.d/alcasar-nfcapd-expire` » permet d'actualiser tous les jours le délai d'expiration sur le répertoire contenant les fichiers de capture Netflow : `nfexpire -e /var/log/nfsen/profile-date/live/alcasar_netflow/ -t 365d`

Tel quel, le format Netflow n'est pas lisible, en revanche il est possible à tout moment d'afficher le contenu des fichiers de capture de manière lisible. Il faut pour cela utiliser un **interpréteur Netflow** (ex : « `nfdump` ») comme suit : `nfdump -R <fichier_au_format_netflow> -o extended -a`

Récapitulatif de l'architecture NETFLOW



TODO : le grapheur « `nfsen` » a été supprimé (non maintenu). Une étude est menée pour le remplacer (Ntop-NG couplé à Crowdsec ou `nfsen-NG`).

8.6 - Contournement (by-pass)

En cas de problème technique concernant une des briques logicielles du portail (principalement « coova-chilli »), il est possible de court-circuiter le module d'authentification tout en maintenant le traçage des logs réseau (pare-feu).

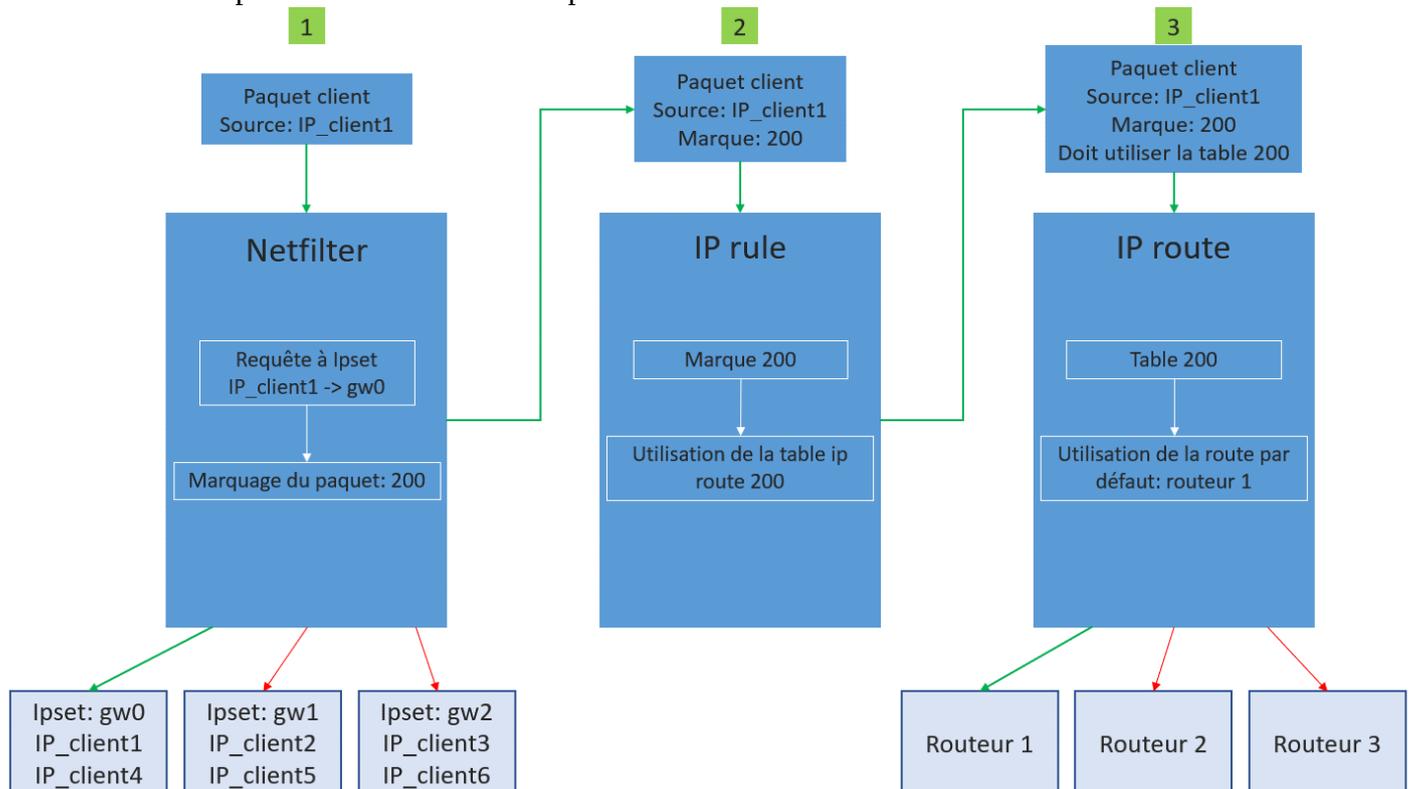
Un script lancé localement en root `alcasar-bypass.sh -on | --off` permet au choix de mettre :

- en mode « On » le bypass → le portail désactive les services coova-chilli et E²Guardian
- en mode « Off » : le portail est en mode normal. Tous les services nécessaires sont activés.

8.7 - Équilibrage de charge en sortie (load balancing)

ALCASAR intègre un dispositif spécial permettant d'équilibrer la charge sur plusieurs routeurs de sortie. Ce dispositif est décrit dans un document externe disponible sur le site WEB. Nous avons décidé de créer notre propre dispositif d'équilibrage de charge après avoir constaté que les systèmes existants ne donnaient plus satisfaction (équilibrage de charge par adresses de destination ou par protocoles réseau). Le système mis en oeuvre dans ALCASAR effectue un équilibrage de charge par systèmes/utilisateurs authentifiés.

Le fichier de configuration d'ALCASAR (`/usr/local/etc/alcasar.conf`) intègre ainsi une entrée d'activation (MULTIWAN=On/Off) et autant d'entrées que de routeurs complémentaires (WAN1=w.x.y.z,1 WAN2=a.b.c.d,1 WAN3=...). Le routeur par défaut reste défini par l'entrée "GW=". Un "ipset" est créé pour chaque routeur (gw0, gw1, etc.). Les @ip des systèmes authentifiés (utilisateurs ou @MAC) sont distribués (algorithme "Round Robin" ou "tourniquet") dans chacun de ces ipsets. Des règles de routage (ip rule) intégrant ces ipsets distribuent les utilisateurs sur leur routeur respectif. L'administrateur peut affecter un "poids" à chaque routeur afin d'ajuster la charge qu'il recevra en termes de nombre d'utilisateurs. C'est le script "`alcasar-network.sh`" (qui est appelé par l'ACC) qui applique les différentes règles de routage en fonction du nombre de routeurs et de leur poids. Le schéma suivant présente le cheminement des flux d'un utilisateur :



Étape 1 : À chaque authentification réussie, « coova » lance le script « `alcasar-conup.sh` » qui détermine le routeur de sortie en fonction de la répartition de charge et qui affecte l'@IP de l'utilisateur dans l'ipset correspondant (gwX). Dans sa table de « prerouting », Netfilter marque les paquets en fonction de cet ipset (200, 201, 202, etc.). Lors d'une déconnexion, « coova » lance le script « `alcasar-condown.sh` » qui supprime l'@IP de l'utilisateur de son ipset.

Étape 2 : Des règles de routage sont mises en place par le script « `alcasar-network.sh` » (lancé au démarrage et/ou appelé par l'ACC). Ces règles sont visibles via la commande « `ip rule` ». Exemple avec 2 routeurs :

```
ip rule
0:    from all lookup local
32764: from 172.16.0.0/16 fwmark 0xc9 lookup 201
32765: from 172.16.0.0/16 fwmark 0xc8 lookup 200
32766: from all lookup main
32767: from all lookup default
```

Étape 3 : Les paquets de l'utilisateur sont traités par la table de routage associée à la marque. La commande « `ip r` » permet d'afficher une synthèse des tables de routage. La commande « `ip r show table xxx` » permet d'afficher la table de routage xxx. Exemple avec 2 tables :

```
ip r (ou ip r show table main)
default
    nexthop via 192.168.0.254 dev eno1 weight 1
    nexthop via 192.168.0.253 dev eno1 weight 1
172.16.0.0/16 dev tun0 proto kernel scope link src 172.16.0.1
192.168.0.0/24 dev eno1 scope link src 192.168.0.201
```

```
ip r show table 200
default via 192.168.0.254 dev eno1
192.168.0.0/24 dev eno1 scope link src 192.168.0.201
```

```
ip r show table 201
default via 192.168.0.253 dev eno1
192.168.0.0/24 dev eno1 scope link src 192.168.0.201
```

8.8 - Sauvegardes

Les sauvegardes d'ALCASAR sont disponibles sous 3 formes : l'archive des journaux de traçabilité, la base de données des utilisateurs et le rapport d'activité hebdomadaire.

8.8.1 - Sauvegarde des journaux de traçabilité

Les journaux du firewall (`/var/log/firewall/*`) et de la sonde Netflow (`/var/log/nfsen/profiles-data/live/alcasar-netflow`) sont « rotatés » chaque semaine. Chaque semaine (lundi à 5h35), une tâche planifiée appelle le script « `alcasar-archive.sh -now` » qui crée une archive compressée, constituée de ces journaux et de la base de données des utilisateurs. Cette archive est copiée dans le répertoire « `/var/Save/archive` » afin d'être disponible dans l'ACC pour téléchargement (fichier « `traceability-<date>.tar.gz` »). Afin de limiter la conservation des traces à 1 an, ce script efface toutes les archives dont la date de création est supérieure à 365 jours.

8.8.2 - Sauvegarde de la base de données

Chaque semaine (lundi à 04h45), le script « `alcasar-mysql.sh -dump` » vérifie, sauvegarde et compresse la base de données des utilisateurs dans le répertoire « `/var/Save/base` » sous la forme : « `alcasar-users-database-<date>.sql.gz` ».

Chaque nuit à 4h40, le script « `alcasar-mysql.sh --expire_user` » supprime les utilisateurs dont la date d'expiration est dépassée de plus de 7 jours.

8.8.3 - Le rapport d'activité hebdomadaire

Ce rapport au format « PDF » est généré par le script « `alcasar-activity_report.sh` » tous les dimanches matin à partir de 5h35. Les rapports sont disponibles via l'ACC. Ils sont stockés dans le répertoire « `/var/Save/activity_report/` ».

8.9 - WIFI4EU

La procédure technique est disponible ici :

https://ec.europa.eu/inea/sites/inea/files/wifi4eu/cnect-2017-00250-00-11-fr-tra-00_0.pdf

Deux attributs du fichier de conf d'alcazar sont utilisés (WIFI4EU=on/off et WIFI4EU_CODE=). Le code de test est « 123e4567-e89b-12d3-a456-426655440000 ».

Dans l'ACC, la page de gestion des services permet de modifier l'identifiant de réseau et d'activer/désactiver ce service en appelant le script « alcazar-wifi4eu.sh » qui effectue les modifications suivantes :

- ajout du site « collection.wifi4eu.ec.europa.eu » comme site de confiance (inscription dans le fichier : « /usr/local/etc/alcazar-uamdomain »).
- Les pages « /var/www/html/index.php », active le code suivant entre leur balises <head>

```
<script type="text/javascript">
  var wifi4euTimerStart = Date.now();
  var wifi4euNetworkIdentifier = '123e4567-e89b-12d3-a456-426655440000';
  var wifi4euLanguage = 'fr';
  //var selftestModus = true;
</script>
```

```
<script type="text/javascript" src="https://collection.wifi4eu.ec.europa.eu/wifi4eu.min.js"></script>
```

- Dans ces pages, on remplace le titre de la page par la bannière « WIFI4EU » ()
 - index.php (ligne 563)
 - status.php (ligne)
 - intercept.php (ligne)

Test de bon fonctionnement :

Pour évaluer la validité de cette intégration, décommentez la ligne « var selftestModus = true; ». Ouvrez la « console web » de débog du navigateur pour afficher le journal de validation :



The screenshot shows a web browser interface. At the top, there is a banner for WiFi4EU. On the left of the banner is a penguin wearing a military-style jacket. In the center, it says "WIFI4EU" with a map of Europe and Wi-Fi symbols. On the right is the Alcazar logo, which is circular and contains the text "ALCASAR" and "ASSOCIATION LIBRE POUR LE CONTRÔLE ET LA SÉCURITÉ DES RESEAUX". Below the banner, there is a button that says "Se déconnecter d'internet" with a globe icon and a red 'X'. To the right, it says "Utilisateur connecté : test" and "3 dernières connexions : 2021-03-28 21:47:48 (0 h 10 m 0 s)". At the bottom, the browser's developer console is open, showing a log of messages. The messages include "completelyInViewPortAfterLoadingCheck: true", "Validating portal compliance end", and a summary stating "The Policy Enforcement Component is correctly installed." and "The portal is compliant with WIFI4EU regulations.".

Le portail est compatible avec WIFI4EU

9 - Annexes

Ce chapitre reprend les fichiers de configuration spécifiques à ALCASAR.

9.1 - CoovaChilli

Les fichiers se situent sous « */etc/*, */etc/chilli* et */usr/local/etc* ».

- Fichier principal : *chilli.conf* (sous */etc/*)
- Exceptions Domaines : *alcasar-uamdomain* (sous */usr/local/etc/*)
- Exceptions URLs : *alcasar-uamallowed* (sous */usr/local/etc/*)
- Exceptions d'authentification par MAC Adresses : *alcasar-macallowed* (sous */usr/local/etc/*)
- L'association dynamique d'*@IP* statiques s'effectue par le biais du fichier : *alcasar-ethers* (sous */usr/local/etc/*)

9.2 - Freeradius

Les fichiers du démon radius se situent sous « */etc/raddb* ».

- Fichier principal : *radiusd.conf*
- Fichier de connexion BDD : *sql.conf*
- Fichier des clients autorisés à requêter le service radiusd : *clients.conf*
- Fichier dédié : *alcasar* (sous */etc/raddb/sites-available* avec un lien symbolique qui lie les « *sites-enable* »)

Voici la liste des attributs (source : <https://raw.githubusercontent.com/coova/coova-chilli/master/doc/attributes>)

| # Name | Type | Comment |
|--------------------------------|---------|--|
| User-name | String | Full username as entered by the user. |
| User-Password | String | Used for UAM as alternative to CHAP-Password and CHAP-Challenge. |
| CHAP-Password | String | Used for UAM CHAP Authentication |
| CHAP-Challenge | String | Used for UAM CHAP Authentication |
| EAP-Message | String | Used for WPA Authentication |
| NAS-IP-Address | IPAddr | IP address of Chilli (set by the "nasip" or "radiuslisten" option, and otherwise "0.0.0.0") |
| Service-Type | Integer | Set to Login (1) for normal authentication requests. The Access-Accept message from the radius server for configuration management messages must also be set to Administrative-User. |
| Framed-IP-Address | IPAddr | IP address of the user, which is configurable during MAC authentication in the Access-Accept. |
| Framed-IP-Netmask | IPAddr | IP netmask of the user, which is configurable during MAC authentication in the Access-Accept. |
| Filter-ID | String | Filter ID pass on to scripts possibly. |
| Reply-Message | String | Reason of reject if present. |
| State | String | Sent to chilli in Access-Accept or Access-Challenge. Used transparently in subsequent Access-Request. |
| Class | String | Copied transparently by chilli from Access-Accept to Accounting-Request. |
| Session-Timeout | Integer | Logout once session timeout is reached (seconds) |
| Idle-Timeout | Integer | Logout once idle timeout is reached (seconds) |
| Called-Station-ID | String | Set to the "nasmac" option or the MAC address of chilli. |
| Calling-Station-ID | String | MAC address of client |
| NAS-Identifier | String | Set to radiusnasid option if present. |
| Acct-Status-Type | Integer | 1=Start, 2=Stop, 3=Interim-Update |
| Acct-Input-Octets | Integer | Number of octets received from client. |
| Acct-Output-Octets | Integer | Number of octets transmitted to client. |
| Acct-Session-ID | String | Unique ID to link Access-Request and Accounting-Request messages. |
| Acct-Session-Time | Integer | Session duration in seconds. |
| Acct-Input-Packets | Integer | Number of packets received from client. |
| Acct-Output-Packets | Integer | Number of packets transmitted to client. |
| Acct-Terminate-Cause | Integer | 1=User-Request, 2=Lost-Carrier, 4=Idle-Timeout, 5=Session-Timeout, 11=NAS-Reboot |
| Acct-Input-Gigawords | Integer | Number of times the Acct-Input-Octets counter has wrapped around. |
| Acct-Output-Gigawords | Integer | Number of times the Acct-Output-Octets counter has wrapped around. |
| NAS-Port-Type | Integer | 19=Wireless-IEEE-802.11 |
| Message-Authenticator | String | Is always included in Access-Request. If present in Access-Accept, Access-Challenge or Access-reject chilli will validate that the Message-Authenticator is correct. |
| Acct-Interim-Interval | Integer | If present in Access-Accept chilli will generate interim accounting records with the specified interval (seconds). |
| WISPr-Location-ID | String | Location ID is set to the radiuslocationid option if present. Should be in the format |
| WISPr-Location-Name | String | Location Name is set to the radiuslocationname option if present. Should be in the format |
| WISPr-Logoff-URL | String | Included in Access-Request to notify the operator of the log off URL. Defaults to "http |
| WISPr-Redirection-URL | String | If present the client will be redirected to this URL once authenticated. This URL should include a link to WISPr-Logoff-URL in order to enable the client to log off. |
| WISPr-Bandwidth-Max-Up | Integer | Maximum transmit rate (b/s). Limits the bandwidth of the connection. Note that this attribute is specified in bits per second. |
| WISPr-Bandwidth-Max-Down | Integer | Maximum receive rate (b/s). Limits the bandwidth of the connection. Note that this attribute is specified in bits per second. |
| WISPr-Session-Terminate-Time | String | The time when the user should be disconnected in ISO 8601 format (YYYY-MM-DDThh |
| CoovaChilli-Max-Input-Octets | Integer | Maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected. |
| CoovaChilli-Max-Output-Octets | Integer | Maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected. |
| CoovaChilli-Max-Total-Octets | Integer | Maximum total octets the user is allowed to send or receive. After this limit has been reached the user will be disconnected. |
| CoovaChilli-Bandwidth-Max-Up | Integer | Maximum bandwidth up |
| CoovaChilli-Bandwidth-Max-Down | Integer | Maximum bandwidth down |
| CoovaChilli-Config | String | Configurations passed between chilli and back-end as name value pairs |
| CoovaChilli-Lang | String | Language selected in user interface |
| CoovaChilli-Version | String | Contains the version of the running CoovaChilli |
| CoovaChilli-DHCP-Netmask | IPAddr | DHCP IP netmask of the user, which is configurable during MAC authentication in the Access-Accept. |
| CoovaChilli-DHCP-DNS1 | IPAddr | DHCP DNS1 of the user, which is configurable during MAC authentication in the Access-Accept. |
| CoovaChilli-DHCP-DNS2 | IPAddr | DHCP DNS2 of the user, which is configurable during MAC authentication in the Access-Accept. |
| CoovaChilli-DHCP-Gateway | IPAddr | DHCP Gateway of the user, which is configurable during MAC authentication in the Access-Accept. |
| CoovaChilli-DHCP-Domain | IPAddr | DHCP Domain of the user, which is configurable during MAC authentication in the Access-Accept. |
| MS-MPPE-Send-Key | String | Used for WPA |
| MS-MPPE-Recv-Key | String | Used for WPA |

9.3 - Unbound

En fonctionnement normal, 4 instances de unbound sont lancées (une instance en mode « forward » sur le port 53, une instance en mode « blacklist » sur port 54, une instance en mode whitelist sur le port 55 et une instance en mode « blackhole » sur le port 56).

- Fichiers principaux : `/etc/unbound/unbound.conf` et `/etc/unbound/vonf.d/*`
- les utilisateurs sont redirigés sur une instance de Unbound en fonction de leur attribut de filtrage.

9.4 - PAREFEU

- Fichier principal du pare-feu d'ALCASAR : `alcasar-iptables.sh` (sous `/usr/local/bin`)
- Règles personnalisées du pare-feu : `alcasar-iptables-local.sh` (sous `/usr/local/etc.`)
- Fichier de filtrage Réseau (associé à `alcasar-nf.sh`) : `alcasar-iptables-exception`
- Activer/désactiver le filtrage web : `alcasar-bl.sh` (sous `/usr/local/bin`)
- Fichier listant les catégories de filtrage : `alcasar-bl-categories-enabled` ; utilisée par le fichier `alcasar-bl.sh` pour le filtrage Unbound et E²Guardian.
- Fichier contenant la liste complète des domaines par catégories issues de la liste noire de Toulouse : `alcasar-dnsfilter-available` (sous `/usr/local/etc./`)
- Fichier du pare-feu d'ALCASAR utilisé en mode ByPass : `alcasar-iptables-bypass.sh` (sous `/usr/local/bin`)

9.5 - E²Guardian

Les fichiers d'E²Guardian se situent sous « `/etc./e2guardian` ».

- Fichier principal de configuration : `e2guardian.conf`
- Fichier concernant le groupe 1 utilisé par ALCASAR : `e2guardianf1.conf`
- Le répertoire « `lists` » contient les fichiers de filtrage proprement dits :
 - « `bannedsitelist` » : non exploité (cf. §6.2)
 - « `exceptionsitelist` » : non exploité
 - « `bannediplist` » : non exploité
 - « `exceptioniplist` » : exploité pour la liste des adresses IP en exception de filtrage
 - « `exceptionurlist` » exploité pour la liste des URLs réhabilitées
 - « `bannedurllist` » contient la liste des catégories d'URL à filtrer
 - « `blacklists` » : contient la BL de Toulouse. Les répertoires « `urls` » de chaque catégorie sont exploités pour le filtrage d'URLs.

9.6 - Ulogd

Le daemon ulogd centralise les logs du pare-feu (dissociés des logs 'messages') ; tous les journaux d'évènements sont gérés en mode texte.

- Fichier de configuration : `ulogd.conf`
- Fichier concernant les flux SSH extérieurs en provenance de eth0 : `ulogd-ssh.conf`
- Fichier concernant les flux bloqués en provenance du réseau extérieur : `ulogd-ext-access.conf`

La rotation des logs s'effectue de manière hebdomadaire pour lighttpd et tracability

9.7 - Distribution Mageia et ses dépôts

La distribution Mageia est utilisée comme système d'exploitation support pour ALCASAR. Les mises à jour et l'installation des paquets s'effectuent à l'aide des outils natifs : « `urpmi` ».

Les fichiers de configurations se trouvent sous `/etc./urpmi` :

- source des miroirs : `urpmi.cfg` ;
- exceptions des mises à jour de paquets : `skip.list` ; permet d'exclure des mises à jour certains paquets pouvant éventuellement troubler le fonctionnement du portail.
- Pour effectuer une mise à jour automatique : `urpmi -auto-update -auto`
- Pour effectuer du ménage : `urpme -auto-orphans -auto`

9.8 - Étude du remplacement de DNSMasq par Unbound

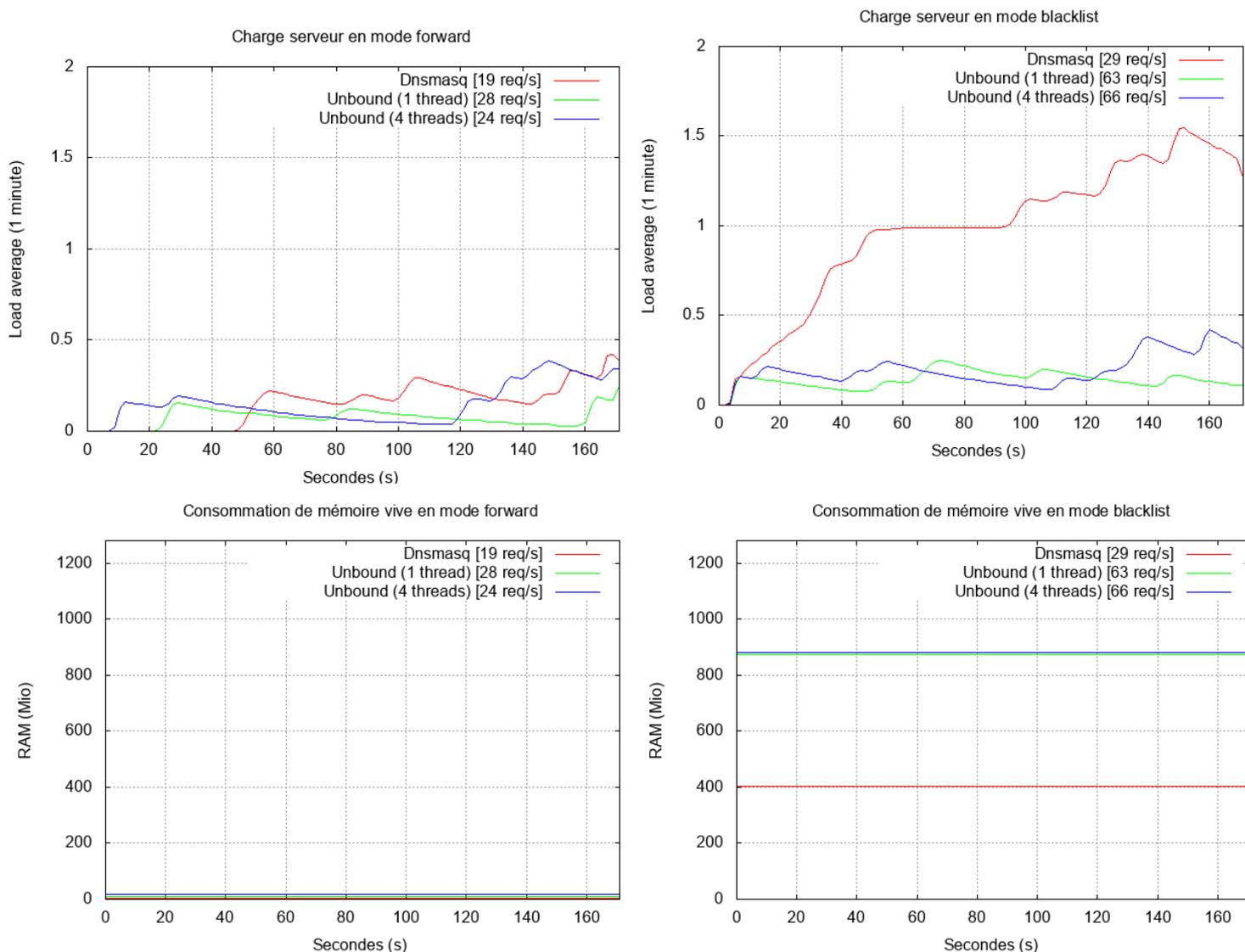
Étude réalisée par Lucas ECHARD

Problématique : À forte charge, le service « Dnsmasq » en mode blacklist consomme beaucoup de ressources et impacte les performances des serveurs ALCASAR.

Méthodologie : Un benchmark comparatif a été réalisé entre « Unbound » et « Dnsmasq ». Voici les conditions dans lesquelles les tests ont été réalisés :

- utilisation d'une machine virtuelle Mageia 6 (4 cœurs, 8 Gio de RAM) comprenant uniquement Unbound et Dnsmasq ainsi que les fichiers de blacklist/whitelist correspondant ;
- les services dnsmasq, dnsmasq-blacklist, unbound, unbound-blacklist ont été testés indépendamment ;
- une seconde VM faisant office de machine de consultation contenant un script générant des requêtes DNS (50 % whitelist, 50 % blacklist) pour stresser le serveur ;
- le « load average » et la consommation de mémoire vive liée au service testé sont sauvegardés à intervalle régulier sur le serveur.

Résultats : Voici ci-dessous les graphiques obtenus en fonction des données relevées.



Conclusion : comparé à « Dnsmasq », « Unbound » gère mieux la montée en charge au niveau du CPU mais consomme deux fois plus de RAM que « Dnsmasq » en mode blacklist.

Suite à cette étude, il a été décidé de lancer les travaux de migration vers « Unbound » à partir de la version 3.3 (fin 2018).

10 - Test plan

Installation / désinstallation / mise à jour

| Function to test | Expected | 3.6 |
|---|---|--|
| Install script (alcasar.sh -i) <ul style="list-style-type: none"> disconnect the wire on EXTIF disconnect the router Internet off (?) Set debug mode : change the DEBUG_ALCASAR variable to « on » (line 40) Install again (new installation) | <ul style="list-style-type: none"> The script stops The script stops The script stops End of installation without error or warning End of re-installation without error or warning | <ul style="list-style-type: none"> ✓ ✓ ✓ ✓ ✓ |
| After first reboot <ul style="list-style-type: none"> All services needed are started No error during the boot process All ALCASAR services are started | <ul style="list-style-type: none"> “systemctl - - failed” must return 0 line “journalctl -b grep 'failed error' ” “alcasar-daemon.sh” | <ul style="list-style-type: none"> ✓ ✓ ✓ |
| Uninstall script (alcasar.sh -u) <ul style="list-style-type: none"> Stop & uninstall all services Network is working | <ul style="list-style-type: none"> All services are removed (ps fax) ping Internet | <ul style="list-style-type: none"> ✓ ✓ |
| Minor update <ul style="list-style-type: none"> Install on a running system (update mode) verify that old parameters are take into account | <ul style="list-style-type: none"> End of re-installation without error or warning network parameters DNS (local & remote resolutions) security certificates admin accounts users database | <ul style="list-style-type: none"> ✓ ✓ ✓ ✓ ✓ ✓ |
| Major update <ul style="list-style-type: none"> Create a conf file in /var/tmp Install Linux without formatting /var Install ALCASAR verify that old parameters are taken into account | <ul style="list-style-type: none"> alcasar-conf.sh -create (or ACC) /var/tmp/alcasar-conf.tar.gz is still present The conf file is taken into account (see minor update) | <ul style="list-style-type: none"> ✓ ✓ ✓ ✓ |
| User management <ul style="list-style-type: none"> Create 5 users (“direct”, “av_bl”, “av_wl”, “av” & “ws”) each-one with a different filtering system (‘ws’ for without “status page”). Set also other attributes to test. av test av_bl test ws change a user attribute & test create a group “student” with a filtering | <p>The PDF voucher is ok.</p> <p>“ipset list -n“ to see the name of the ipset</p> <p>“ipset list xxx”, list the content of the ipset xxx (xxx = 'not_filtered', 'av_bl', 'av_wl' or 'av')</p> <ul style="list-style-type: none"> eicar test (http://www.csm-testcenter.org) DNS blacklist test (www.warez.com & www.rael.org) URL blacklist test (wawa-mania.eu/warez) IP blacklist test (151.196.210.42 & 207.239.30.20) URL with IP@ instead of domain name Google safesearch <p>in “/tmp/current_users.txt” the flag “PERM” should be set in the @ip line of this user</p> <ul style="list-style-type: none"> student group : check this user 'with edit a user'. Two columns should appear. The first one is | <ul style="list-style-type: none"> ✓ ✓ ✓ ✓ ✓ ✓ X X ✓ ✓ |

| Function to test | Expected | 3.6 |
|--|---|---|
| <p>attribute. Set other attributes (ie : redirect_url). Create a user in this group and verify that the attributes are inherited.</p> <ul style="list-style-type: none"> • Empty the database <ul style="list-style-type: none"> ◦ with the script “alcasar-mysql.sh -raz” ◦ via “ACC” • Import a users list (simple text file with and without password) • import a users database <ul style="list-style-type: none"> ◦ with the script “alcasar-mysql.sh -i xxx.sql” ◦ via ACC • Connection to an AD server & test remote users • Connection to a LDAP server & test remote users | <p>group attributes and second one is user attributes</p> <ul style="list-style-type: none"> • the connected users are disconnected. The database is empty. • pdf & txt password file is generated (remove after 24h) • do nothing for users already exist (just change their password if it exists in text file) • To get a SQL database sample. Go to /var/Save/base then use 'gzip -d' to extract. | <p>✓</p> <p>X</p> <p>X</p> <p>X</p> <p>X</p> |
| <p>Exceptions</p> <ul style="list-style-type: none"> • Create a user with a PC MAC address as login and 'password' as password • Add domain names and IP addresses in exception form | <ul style="list-style-type: none"> • The PC should connect to Internet without interception • Users should connect to these IP & domain names without interception | <p>✓</p> <p>✓</p> |
| <p>Watchdog</p> <ul style="list-style-type: none"> • Disconnect the Ethernet cable on EXTIF • Connect again the Ethernet cable on EXTIF | <ul style="list-style-type: none"> • All the DNS requests are send to the DNS blackhole (port 56). “iptables -nvL -tnat” to verify (first line redirect DNS to port 56) • for the users : Internet unavailable page • The main page alert that the access is down • Everything return to normal state | <p>✓</p> <p>✓</p> <p>✓</p> |
| <p>Blacklist/Whitelist filtering</p> <p>The 3 following actions are performed when the admin wants to update BL with ACC</p> <ul style="list-style-type: none"> • alcasar-bl.sh -download • alcasar-bl.sh -adapt • alcasar-bl.sh -reload • enable all categories to know if there isn't any bad lines in blacklist files • add and remove a 'blacklist' file containing IP and domain names | <p>Download the last BL from Toulouse (saved in /tmp)</p> <p>compute the BL in order to create three sub-BL (domains, URL and IP)</p> <p>Reload the services that use the BL (unbound-blacklist, unbound-whitelist and netfilter)</p> <p>Verify that the IPs are really in the ipset (command “ipset test bl_ip_blocked @IP”)</p> <p>Verify that the domain names are really blocked.</p> <p>Remove the file</p> | <p>✓</p> <p>✓</p> <p>✓</p> <p>✓</p> <p>✓</p> <p>✓</p> |

| Function to test | Expected | 3.6 |
|--|--|------------------|
| <ul style="list-style-type: none"> ipset list whitelist_ip_allowed ipset list av_wl | show ip allowed by the whitelist show current user filtered by the whitelist | ✓ ✓ |
| <ul style="list-style-type: none"> cat /usr/local/share/unbound-wl/ossi.conf cat /usr/local/share/iptables-wl-enabled/ossi | Show allowed website manually added with ACC the same for IP address | ✓ ✓ |
| Network protocols filtering <ul style="list-style-type: none"> switch the 1st filter on (http + https) switch the 2nd filter on Add a custom port (ex : ssh) | Check that you can't connect to a ssh/ftp server Check that you can now connect to a ssh/ftp server Check that you can connect to that port | ✓ ✓ ✓ |
| Users activities <ul style="list-style-type: none"> login & logout with the alcasar main page logout with the URL : 'http://logout' Change password Import the CA certificate | | ✓ ✓ ✓ ✓ |
| SMS (autoregistration) <ul style="list-style-type: none"> Check gammu (it's not a standard service) Check with « Wavecom » Modem | /var/log/gammu-smsd/gammu-smsd.log Receive a SMS a create an account | ✓ ✓ |
| After several days working <ul style="list-style-type: none"> “journalctl -b grep 'failed error' ” logrotate process test | View and analyze errors <ul style="list-style-type: none"> logrotate -vf /etc./logrotate.conf (test all file in /etc./logrotate.d) logrotate -vf /etc./logrotate.d/file_to_test | |
| Admin <ul style="list-style-type: none"> alcasar-bypass.sh -on alcasar-bypass.sh -off importation of an official certificate | ACC isn't available. Users can surf without interception ACC is available. Users are intercepted | X X |
| Uninstall <ul style="list-style-type: none"> alcasar.sh -u | All services are stopped and the modified config files are removed. | ✓ |
| Update a previous version | A conf file (alcasar-conf.tar.gz) is created in /var/tmp The parameters of the previous version are enabled (logo, admin accounts, users database, network parameters, SSL certificates, custom BL&WL). | |
| MultiWAN | Command : “ip route list” to see the gateways and their weights. | |

11 - Security tests

- « **Lynis** » **internal audit** with the following modifications :
 - INTIF is whitelisted in « default.prf ». Remove « php.ini.default » in « include/test_php »
 - Result : Lynis V3.0.1 - 10/2020 - **Hardening index : [69]**
- **Open ports enumeration on Extif** (nmap -p 1-65535 -T4 -v @IP_Extif)
Not shown: 65534 filtered ports
22/tcp open ssh OpenSSH 8.0 (protocol 2.0)
- **Open ports enumeration on Intif** (nmap -p 1-65535 -T4 -v @IP_Extif)
- **Audit sshd on Extif**
 - nmap --script-update (all scripts are in /usr/share/nmap/scripts/)
 - nmap -p 22 --script ssh2-enum-algos,ssh-hostkey,ssshv1,ssh-auth-methods,ssh-publickey-acceptance,ssh-run @IP_Extif
 - 22/tcp open ssh
ssh-auth-methods:
Supported authentication methods:
publickey
password
keyboard-interactive
ssh-hostkey:
3072 6a:c0:23:a1:99:2f:29:c1:5c:ac:b3:07:89:5e:c4:da (RSA)
256 f8:8c:5c:12:8e:ef:b6:72:f9:89:81:29:72:cd:82:7f (ECDSA)
256 a0:c0:60:fd:7b:3f:d3:bc:c8:00:d0:81:4d:f0:ca:5b (ED25519)
ssh-publickey-acceptance:
Accepted Public Keys: No public keys accepted
_ssh-run: Failed to specify credentials and command to run.
ssh2-enum-algos:
kex_algorithms: (10)
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256
diffie-hellman-group14-sha1
server_host_key_algorithms: (5)
rsa-sha2-512
rsa-sha2-256
ssh-rsa
ecdsa-sha2-nistp256
ssh-ed25519
encryption_algorithms: (6)
chacha20-poly1305@openssh.com
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
mac_algorithms: (10)
umac-64-etm@openssh.com
umac-128-etm@openssh.com

```

| hmac-sha2-256-etm@openssh.com
| hmac-sha2-512-etm@openssh.com
| hmac-sha1-etm@openssh.com
| umac-64@openssh.com
| umac-128@openssh.com
| hmac-sha2-256
| hmac-sha2-512
| hmac-sha1
| compression_algorithms: (2)
| none
|_ zlib@openssh.com

```

- **Fail2ban** (tail -f /var/log/fail2ban)

- with sshd (test with “nmap p 22 –script ssh-brute @IP_Extif|@IP_Intif”)

```

2020-10-17 18:11:57,133 fail2ban.filter [2291]: INFO [ssh-iptables] Found 192.168.182.69 - 2020-10-17 18:11:56
2020-10-17 18:11:57,134 fail2ban.filter [2291]: INFO [ssh-iptables] Found 192.168.182.69 - 2020-10-17 18:11:56
2020-10-17 18:11:57,135 fail2ban.filter [2291]: INFO [ssh-iptables] Found 192.168.182.69 - 2020-10-17 18:11:56
2020-10-17 18:11:57,646 fail2ban.actions [2291]: NOTICE [ssh-iptables] Ban 192.168.182.69
2020-10-17 18:14:59,993 fail2ban.actions [2291]: NOTICE [ssh-iptables] Unban 192.168.182.69

```

- with lighttpd (5 failed user connections attempts)

```

2020-10-17 19:12:50,134 fail2ban.filter [2291]: INFO [alcasar_intercept] Found 192.168.182.69 - 2020-10-17 19:12:49
2020-10-17 19:12:50,646 fail2ban.actions [2291]: NOTICE [alcasar_intercept] Ban 192.168.182.69
2020-10-17 19:15:51,993 fail2ban.actions [2291]: NOTICE [alcasar_intercept] Unban 192.168.182.69

```

- with lighttpd (5 failed user password change attempts)

```

2020-10-18 16:16:51,766 fail2ban.filter [2291]: INFO [alcasar_change_pwd] Found 192.168.182.69 - 2020-10-18 16:16:50
2020-10-18 16:16:51,846 fail2ban.actions [2291]: NOTICE [alcasar_intercept] Ban 192.168.182.69
2020-10-18 19:19:50,393 fail2ban.actions [2291]: NOTICE [alcasar_intercept] Unban 192.168.182.69

```

- with lighttpd (5 failed ACC connection attempts)

```

2020-10-18 19:06:13,897 fail2ban.filter [7223]: INFO [alcasar_acc] Found 172.16.0.3 - 2020-10-18 19:06:10
2020-10-18 19:06:14,632 fail2ban.actions [7223]: NOTICE [alcasar_acc] Ban 172.16.0.3
2020-10-18 19:09:10,915 fail2ban.actions [7223]: NOTICE [alcasar_acc] Unban 172.16.0.3

```

12 - Tests de débit

Voici un exemple de test de bande passante utilisateur (sans filtrage) sur une même fibre (Freebox) à travers 2 ALCASARs 3.5.4 installés sur des PC de génération et de puissance différentes :

- ALCASAR-1 (light) : CPU Intel Atom D2550 1,8G - 4 Go-DDR3 - 2 Gigabit Ethernet BCM57788
- ALCASAR-2 : CPU Xeon E3 3.2G - 8GO-DDR3 - 1 Gigabit Ethernet Intel I212 + 1 Gigabit Ethernet Atheros AR8161

Les tests sont réalisés avec le script « speedtest.py » (<https://github.com/sivel/speedtest-cli>). Étant donné que les serveurs Internet réceptionnant les tests ne sont pas maîtrisés (on ne connaît pas leur charge à un instant T), nous avons décidé de mesurer la perte engendrée par ALCASAR en lançant 2 tests simultanément devant et derrière l'ALCASAR (sur un PC d'utilisateur). Les résultats sont les suivants :

- 3 tests simultanés de débit descendant de chaque côté de l'ALCASAR-1 :
 - ALCASAR-1 : 482.06 Mbit/s. PC utilisateur : 411.09 Mbit/s (14%)
 - ALCASAR-1 : 430.47 Mbit/s. PC : 417.17 Mbit/s (3%)
 - ALCASAR-1 : 482.48 Mbit/s. PC : 442.03 Mbit/s (8%)
- 3 tests simultanés de débit descendant de chaque côté de l'ALCASAR-2
 - ALCASAR-2 : 485.23 Mbit/s. PC : 465.08 Mbit/s (4%)
 - ALCASAR-2 : 447.56 Mbit/s. PC : 447.38 Mbit/s (0%)
 - ALCASAR-2 : 517.78 Mbit/s. PC : 454.55 Mbit/s (12%)

En moyenne, la perte engendrée par ALCASAR sur le débit descendant est inférieure à 10 %.

13 - Arbre de dépendance JS et CSS

13.1 - JS

```
alcasar-rexy[/var/www/html/js]$ ll
total 1136
drwxr-xr-x 2 apache apache 4096 janv. 8 19:57 ./
drwxr-xr-x 9 root root 4096 janv. 16 09:50 ../
-rw-r--r-- 1 apache apache 62440 janv. 8 19:57 bootstrap-4.6.1.min.js
lrwxrwxrwx 1 apache apache 22 janv. 8 19:57 bootstrap.min.js -> bootstrap-4.6.1.min.js
-rw-r--r-- 1 apache apache 201572 janv. 8 19:57 Chart.bundle.min.js
-rw-r--r-- 1 apache apache 26625 janv. 8 19:57 ChilliLibrary.js
-rw-r--r-- 1 apache apache 34363 janv. 8 19:57 epoch_classes.js
-rw-r--r-- 1 apache apache 1072 janv. 8 19:57 error_translate.js
-rw-r--r-- 1 apache apache 12824 janv. 8 19:57 error_translation_i18n.js
-rw-r--r-- 1 apache apache 3087 janv. 8 19:57 fonctions.js
-rw-r--r-- 1 apache apache 67015 janv. 8 19:57 gstatic-loader.js
-rw-r--r-- 1 apache apache 83488 janv. 8 19:57 jquery-1.12.1-ui.min.js
-rw-r--r-- 1 apache apache 72818 janv. 8 19:57 jquery-3.6.3.slim.min.js
-rw-r--r-- 1 apache apache 89501 janv. 8 19:57 jquery-3.6.min.js
-rw-r--r-- 1 apache apache 6283 janv. 8 19:57 jquery.connections.js
-rw-r--r-- 1 apache apache 422284 janv. 8 19:57 jquery.dataTables.js
lrwxrwxrwx 1 apache apache 17 janv. 8 19:57 jquery.min.js -> jquery-3.6.min.js
lrwxrwxrwx 1 apache apache 24 janv. 8 19:57 jquery.slim.min.js -> jquery-3.6.3.slim.min.js
lrwxrwxrwx 1 apache apache 23 janv. 8 19:57 jquery-ui.min.js -> jquery-1.12.1-ui.min.js
-rw-r--r-- 1 apache apache 3139 janv. 8 19:57 login-time.js
-rw-r--r-- 1 apache apache 15405 janv. 8 19:57 pdwometer.js
-rw-r--r-- 1 apache apache 11398 janv. 8 19:57 schedule.js
-rw-r--r-- 1 apache apache 6753 janv. 8 19:57 statusControler.js
```

| Libraries | Use by |
|---------------------|--|
| bootstrap.min.js | web/email_registration_front.php web/acc/backup/log_generation.php web/acc/manager/htdocs/security.php |
| Chart.bundle.min.js | scripts/alcasar-activity-report.sh |
| ChilliLibrary.js | web/status.php |
| epoch_classes.js | web/acc/manager/htdocs/group_new.php web/acc/manager/htdocs/user_edit.php web/acc/manager/htdocs/user_new.php |
| error_translate.js | web/errors/error-400.html web/errors/error-401.html web/errors/error-403.html web/errors/error-404.html web/errors/error-405.html web/errors/error-408.html web/errors/error-410.html web/errors/error-411.html web/errors/error-413.html web/errors/error-414.html web/errors/error-415.html web/errors/error-500.html web/errors/error-501.html web/errors/error-502.html web/errors/error-503.html web/errors/error-506.html |
| fonctions.js | web/acc/manager/htdocs/group_new.php web/acc/manager/htdocs/user_edit.php web/acc/manager/htdocs/user_new.php |
| i18n.js | web/errors/error-400.html |

| Libraries | Use by |
|-----------------------|---|
| jquery-ui.min.js | web/errors/error-401.html web/errors/error-403.html web/errors/error-404.html web/errors/error-405.html web/errors/error-408.html web/errors/error-410.html web/errors/error-411.html web/errors/error-413.html web/errors/error-414.html web/errors/error-415.html web/errors/error-500.html web/errors/error-501.html web/errors/error-502.html web/errors/error-503.html web/errors/error-506.html |
| jquery.min.js | web/acc/manager/htdocs/group_new.php web/acc/manager/htdocs/user_edit.php web/acc/manager/htdocs/user_new.php scripts/alcasar-activity-report.sh web/email_registration_front.php web/sms_registration.php web/acc/menu.php web/acc/admin/network.php web/acc/admin/services.php web/acc/backup/log_generation.php web/acc/manager/htdocs/group_new.php web/acc/manager/htdocs/security.php web/acc/manager/htdocs/user_by_sms.php web/acc/manager/htdocs/user_edit.php web/acc/manager/htdocs/user_new.php |
| jquery.connections.js | web/acc/admin/network.php |
| jquery.dataTables.js | web/sms_registration.php web/acc/manager/htdocs/user_by_sms.php |
| login-time.js | web/acc/manager/htdocs/group_new.php web/acc/manager/htdocs/user_edit.php web/acc/manager/htdocs/user_new.php |
| pwdmeter.js | web/password.php |
| schedule.js | web/acc/manager/htdocs/group_new.php web/acc/manager/htdocs/user_edit.php web/acc/manager/htdocs/user_new.php |
| statusControler.js | web/status.php |

13.2 - CSS

```
alcasar-rexy[/var/www/html/css]$ ll
total 276
drwxr-xr-x 2 apache apache 4096 janv. 8 19:57 ./
drwxr-xr-x 9 root root 4096 janv. 16 09:50 ../
-rw-r--r-- 1 apache apache 4327 janv. 8 19:57 acc.css
-rw-r--r-- 1 apache apache 161996 janv. 8 19:57 bootstrap-4.6.1.min.css
lrwxrwxrwx 1 apache apache 23 janv. 8 19:57 bootstrap.min.css -> bootstrap-4.6.1.min.css
-rw-r--r-- 1 apache apache 1873 janv. 8 19:57 epoch_styles.css
-rw-r--r-- 1 apache apache 12805 janv. 8 19:57 error.css
-rw-r--r-- 1 apache apache 4745 janv. 8 19:57 index.css
-rw-r--r-- 1 apache apache 1844 janv. 8 19:57 intercept.css
-rw-r--r-- 1 apache apache 20739 janv. 8 19:57 jquery-1.12.1-ui.min.css
-rw-r--r-- 1 apache apache 15111 janv. 8 19:57 jquery.dataTables.css
lrwxrwxrwx 1 apache apache 24 janv. 8 19:57 jquery-ui.min.css -> jquery-1.12.1-ui.min.css
-rw-r--r-- 1 apache apache 2151 janv. 8 19:57 ldap.css
-rw-r--r-- 1 apache apache 805 janv. 8 19:57 menu.css
-rwxr-xr-x 1 apache apache 3887 janv. 8 19:57 pass.css*
-rwxr-xr-x 1 apache apache 5833 janv. 8 19:57 pwdmeter.css*
-rw-r--r-- 1 apache apache 378 janv. 8 19:57 report.css
-rw-r--r-- 1 apache apache 3248 janv. 8 19:57 status.css
```

CSS files

acc.css

Use by

web/acc/admin_log.php
web/acc/haut.php
web/acc/index.html
web/acc/menu.php
web/acc/welcome.php
web/acc/admin/bl_categories_help.php
web/acc/admin/bl_filter.php
web/acc/admin/ldap.php
web/acc/admin/logo.php
web/acc/admin/network.php
web/acc/admin/protocols_filter.php
web/acc/admin/services.php
web/acc/admin/wl_filter.php
web/acc/admin/backup/log_generaton.php
web/acc/admin/backup/sauvegarde.php
web/acc/manager/auth_exceptions.php
web/acc/manager/nfsen.php
web/acc/manager/vnstat.php
web/acc/manager/htdocs/activity.php
web/acc/manager/htdocs/badusers.php
web/acc/manager/htdocs/clear_opensessions.php
web/acc/manager/htdocs/failed_logins.php
web/acc/manager/htdocs/find.php
web/acc/manager/htdocs/group_admin.php
web/acc/manager/htdocs/group_new.php
web/acc/manager/htdocs/import_user.php
web/acc/manager/htdocs/security.php
web/acc/manager/htdocs/show_groups.php
web/acc/manager/htdocs/stats.php
web/acc/manager/htdocs/user_accounting.php
web/acc/manager/htdocs/user_admin.php
web/acc/manager/htdocs/user_by_email.php
web/acc/manager/htdocs/user_by_sms.php
web/acc/manager/htdocs/user_delete.php
web/acc/manager/htdocs/user_edit.php

web/acc/manager/htdocs/user_finger.php
 web/acc/manager/htdocs/user_new.php
 web/acc/manager/htdocs/user_stats.php
 web/acc/manager/htdocs/help/coovachilli_bandwith_max_down_help.html
 web/acc/manager/htdocs/help/coovachilli_bandwith_max_up_help.html
 web/acc/manager/htdocs/help/coovachilli_max_input_octets_help.html
 web/acc/manager/htdocs/help/coovachilli_max_output_octets_help.html
 web/acc/manager/htdocs/help/coovachilli_max_total_octets_help.html
 web/acc/manager/htdocs/help/expiration_help.html
 web/acc/manager/htdocs/help/expire_after_help.html
 web/acc/manager/htdocs/help/filtering_help.html
 web/acc/manager/htdocs/help/login_time_help.html
 web/acc/manager/htdocs/help/max_all_session_help.html
 web/acc/manager/htdocs/help/protocols_help.html
 web/acc/manager/htdocs/help/session_timeout_help.html
 web/acc/manager/htdocs/help/simultaneous_use_help.html
 web/acc/manager/htdocs/help/statusOpenRequired_help.html
 web/acc/manager/htdocs/help/wispr_redirection_url_help.html

bootstrap.min.css

conf/alcasar-e2g-en.html
 conf/alcasar-e2g-fr.html
 scripts/alcasar-activity_report.sh
 scripts/alcasar-generate_log.sh
 web/email_registration_front.php
 web/index.php
 web/intercept.php
 web/password.php
 web/sms_registration.php
 web/status.php
 web/acc/backup/log_generation.php
 web/acc/manager/htdocs/security.php
 web/acc/manager/vnstat/templates/module_header.tpl
 web/acc/phpsysinfo/templates/html/index_bootstrap.html

epoch_styles.css

web/acc/manager/htdocs/group_new.php
 web/acc/manager/htdocs/user_edit.php
 web/acc/manager/htdocs/user_new.php

web/errors/error-400.html
 web/errors/error-401.html
 web/errors/error-403.html
 web/errors/error-404.html
 web/errors/error-405.html
 web/errors/error-408.html
 web/errors/error-410.html
 web/errors/error-411.html
 web/errors/error-413.html
 web/errors/error-414.html
 web/errors/error-415.html
 web/errors/error-500.html
 web/errors/error-501.html
 web/errors/error-502.html
 web/errors/error-503.html
 web/errors/error-506.html

index.css

conf/alcasar-e2g-en.html
 conf/alcasar-e2g-fr.html
 web/sms_registration.php

intercept.css

web/intercept.php

jquery-ui.min.css

web/acc/manager/htdocs/group_new.php

| | |
|-----------------------|--|
| | web/acc/manager/htdocs/user_edit.php |
| | web/acc/manager/htdocs/user_new.php |
| jquery.dataTables.css | web/sms_registration.php |
| | web/acc/manager/htdocs/user_by_sms.php |
| ldap.css | web/acc/admin/ldap.php |
| menu.css | web/acc/menu.php |
| | web/email_registration_front.php |
| pass.css | web/password.php |
| pwdmeter.css | web/password.php |
| | scripts/alcasar-activity_report.sh |
| report.css | scripts/alcasar-generate_log.sh |
| | web/email_registration_front.php |
| status.css | web/status.php |

14 - TODO

| | |
|---|---|
| Intégrer une interface graphique de statistique sur les flux Netflow de sortie | Jusqu'à la version 3.4, les statistiques graphiques des flux Netflow de sortie étaient réalisées par « NfSen ». NfSen n'étant plus soutenu, il a été retiré d'ALCASAR avec les versions 3.5. Étudier la réintroduction de cette fonctionnalité via des projets comme « NfSenNG » ou « Nprobe + NtopNG » (qui prend aussi en compte les logs standards). POC réalisé et fonctionnel avec Ntop-NG. Il reste à tester le couplage avec le projet CrowdSec |
| blacklists/whitelists : homogénéiser la gestion des listes personnelles | L'architecture de gestion des blacklists personnelles doit être revue et homogénéisée. Pour rappel, cette architecture permet d'importer, de supprimer, d'activer, de désactiver et de synchroniser une blacklist personnelle qui surcharge la blacklist de Toulouse. Vérifier si l'IPSET « site-direct » a encore une utilité (/usr/local/etc./alcasar-site-direct). Revalider le fonctionnement des noms de domaine et @IP réhabilités. |
| ACC : simplifier le code des modules de gestion des utilisateurs et des groupes | Une partie de ce code est hérité du projet « freeradius-web » qui permet de gérer une base de données connectée à un serveur freeradius. Ce code avait été prévu modulaire afin de s'adapter à plusieurs cas de figure (pgsql, mysql, etc.). Sur ALCASAR, les modules non exploités ont été supprimés. Cependant, l'architecture du code reste basée sur cette gestion de modules, ce qui le complexifie inutilement. |
| Mettre à jour le module d'inscription par SMS | Le module d'inscription par SMS doit être mis à jour après avoir testé de nouveaux modem compatibles 3G/4G/5G (suppression de la 2G 900/1800Mhz à moyen terme). Modem actuel : Ostend (avec module wavecom Q2303A-RS232 ou Q2403A-USB). Idée de modems à tester : Ostend (avec module wavecom Q24plus), adaptateur USB-4G LTE (avec AP WIFI), adaptateur USB LTE , Cela nécessitera aussi d'intégrer le processus « gammu » dans la gestion des services de l'ACC ainsi que dans le processus de mise à jour. |
| E ² guardian : Intégrer le blocage d'URL contenant une @IP | Le filtrage d'URL pour les utilisateurs filtrés par blacklist est géré par E ² guardian. Ce filtrage peut être amélioré en bloquant les URL contenant une @IP à la place d'un nom de domaine (ex: http://25.56.58.59/erp/about.htm). Il faut réactiver/revalider cette option de l'ACC. |
| Groupe « default » pour les utilisateurs | Par défaut, tous les utilisateurs appartiennent à un groupe nommé « default ». Ce groupe n'est pas créé par défaut. Vérifier que quand ce groupe est créé, les utilisateurs sans groupe héritent bien des attributs de « default ». Vérifier l'affichage dans l'ACC. Question : est-il judicieux de créer de groupe lors de l'installation ? |
| Suppression de DNSMasq | FAIT : V3.6.0 |
| E ² Gardian : filtrage HTTPS avec et sans inspection SSL/TLS | Étudier les possibilités de filtrage sans inspection SSL/TLS <ul style="list-style-type: none">• validité des certificats• CRL• inspection du champ SNI (si non chiffré par l'option ESNI de TLS1.3)• autres Étudier les possibilités de filtrage avec inspection SSL/TLS |
| ACC : limitation d'accès par @IP | Ajouter une option permettant à l'administrateur de limiter l'accès à l'ACC à une liste d'@IP ou @IP de réseau. |
| Pages utilisateur : bug d'affichage | Quand ALCASAR affiche une page d'erreur à l'utilisateur (ex : 404), celle-ci n'est pas structurée correctement (CSS). |
| Pages utilisateur et ACC : utilisation plus poussée de « jQuery » | La page d'inscription par Email intègre des possibilités de jQuery/jQuery-ui intéressantes (typage des champs, info dynamique, etc.). Étudier les dernières possibilités de JQuery et les intégrer à toutes les pages utilisateurs. Étudier la migration de certaines pages de l'ACC. |
| Fédération d'ALCASAR | Étudier un système de synchronisation d'un parc d'ALCASAR (un ALCASAR primaire + n ALCASAR secondaires). Cf. forum). Une fois fonctionnel, vérifier le fonctionnement avec le module d'auto-enregistrement SMS en central. 2 POC ont été réalisés. Il faut les tester et en intégrer un. |

| | |
|--|--|
| Cybersurveillance | <p>Étudier l'ajout d'agents de Cybersurveillance comme « Wazuh » et/ou « Suricata ».</p> <p>Le module multi-WAN permet d'équilibrer la charge de navigation sur N routeurs de sorties. Le module réalise un équilibrage par utilisateur. Ce module fonctionne, mais présente un bizarrerie qu'il faut investiguer :</p> <ul style="list-style-type: none"> - constat : erreurs dans la résolution DNS chez les client |
| Multi-WAN : amélioration et intégration de la fonction « HA/failover » | <ul style="list-style-type: none"> - Piste : Vers quel routeur sont envoyées les requêtes générées par ALCASAR (certaines Box refusent les requêtes DNS vers des serveurs non référencés). <p>Le développement de la fonction « HA/failover » (analyse de la qualité de liaison sur chaque routeur) permettrait :</p> <ul style="list-style-type: none"> • une alerte dans l'ACC • le rééquilibrage dynamique de la charge |
| Multi-LAN | <p>ALCASAR contrôle plusieurs réseaux de consultation (VLAN et/ou plusieurs cartes Ethernet et/ou une carte WIFI en A.P.)</p> |
| Ajout d'un attribut utilisateur | <p>Ajouter un attribut utilisateur qui enregistre et autorise automatiquement son équipement (@MAC) lors d'une authentification réussie (pendant 24h par exemple)</p> |
| Email administrateur | <p>Depuis ALCASAR 3.5, un module Email a été intégré (utilisé pour l'auto-inscription d'utilisateur par Email). L'idée est d'utiliser ce module pour créer l'Email de l'administrateur afin d'offrir de nouvelle possibilité (envoi des rapports, envoi des fichiers de log, envoi d'alertes, etc.)</p> |
| Étude de la sécurité de l'UAM | <p>ALCASAR exploite la méthode UAM (Universal Access Method) pour authentifier et autoriser les utilisateurs. Cette méthode permet de s'affranchir d'un agent radius installé dans les équipements des utilisateurs (ce qui serait ingérable pour les cas d'usage d'ALCASAR). Ainsi, l'agent est remplacé par un cycle d'échange entre un serveur WEB, le navigateur de l'utilisateur et un agent radius (« coova » pour ALCASAR). L'étude de la sécurité de ce cycle permettra de vérifier si la sécurité mise en place est suffisante et/ou si elle peut être améliorée.</p> |
| ACC : améliorations graphiques | <p>Dans la page « activité » de l'ACC, trier les entrées par adresse IP.</p> |
| Créer des profils de blacklist/whitelist | <p>E2Guardian est capable de gérer des profils de filtrage par blacklist. Il peut être intéressant d'étudier la possibilité d'exploiter cette capacité sur ALCASAR.</p> <ul style="list-style-type: none"> - Ajout d'un attribut utilisateur : charte=on/off |
| Charte informatique | <ul style="list-style-type: none"> - si 'on' : l'utilisateur doit cocher une case 'charte lue' dans intercept.php. Une fois cochée : charte=off. |