

Projet de 2ème Année :

W.A.N Party 2016



Equipe Technique :

Florian Caliz

Benjamin Calvet

Paul Gallo

Laura Piano

Sommaire :

1. Introduction :
   1. Contexte.
   2. Objectifs.
   3. Coordination.
2. Planification du projet :
   1. Répartition des tâches à effectuer.
   2. Dates Importantes.
3. Développement du projet :
   1. Présentation de l’infrastructure réseau.
   2. Inventaire du matériel disponible.
   3. Mise en place de l’infrastructure interne (L.A.N).
      1. Solutions alternatives et innovations.
      2. Le Pare-Feu.
   4. Tests sur l’infrastructure réseau externe (W.A.N).
   5. Authentification des joueurs.
   6. Divers.
4. Exécution du projet « D-Day ».
   1. Organisation.
   2. Mise en place de la baie et opérations de dernière minute.
   3. Supervision des flux.
   4. Problèmes Rencontrés.
5. Conclusion.

1-Introduction :

I-Contexte :

La **WAN party** est un événement organisé par tous les Instituts Universitaires Technologiques enseignants la spécialité Réseaux et Télécoms en France. Elle fut créée en 2013 par un groupe d’étudiants qui souhaitaient créer une L.A.N (Local Area Network) à l’échelle nationale, où des personnes extérieures pourraient venir dans les établissements pour participer et s’affronter dans des tournois de jeux vidéo en ligne. Le terme W.A.N signifie Wide Area Network, en d'autres termes, réseau étendu sur une grande zone où tous les IUTs de France formeraient un vaste réseau comme illustré ci-dessous (Fig. 1) ainsi cet évènement nécessite la mise en place d’un vaste réseau afin de relier tous les établissements entre eux. Le rôle des étudiants est de mettre en place ce réseau et de veiller à ce qu'il fonctionne parfaitement le jour J.

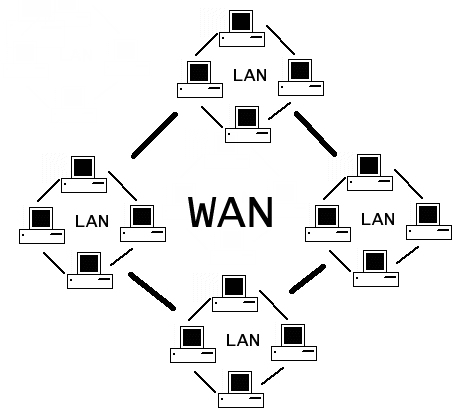


Fig. 1

C’est à la fois un projet avec une durée de préparation plutôt courte et qui exige un soin tout particulier quand à la sécurité. Dans un tel évènement, les machines physiques ne sont pas la seule préoccupation il faut également gérer le côté « humain », partie prise en charge par les étudiants de 1ère Année. Outre le fait d’héberger un événement de type “gaming”, la W.A.N party est devenue une journée de promotion pour l'IUT, en effet des lycéens et collégiens viennent participer, et peuvent ainsi visiter poser des questions sur les formations dispensées au sein de notre département.

II-Objectifs :

L’objectif principal est de permettre le bon fonctionnement de la topologie réseau évoquée plus-haut et ainsi de proposer aux joueurs un environnement correct pour les activités qui leurs seront proposées durant cette journée.

Il en découle des objectifs secondaires cités ci-dessous :

Coordination avec les autres I.U.Ts R&T pour préparation de la W.A.N (PHP, LDAP, monitoring).

Effectuer des tests sur des maquettes.

Faire une répétition générale le jeudi 10 mars (à j-2).

Assurer l’intercommunication inter-IUT le jour J et gérer les rotations des matchs durant l’évènement.

Réduire au strict-nécessaire la consommation de bande passante.

* Garantir l’authentification des joueurs.

III-Coordination entre les différents IUTs :

Suite à la réunion de début d’année à Paris, des objectifs ont été créés et répartis afin d’impliquer chaque IUT dans le projet commun :

Répartition du travail au sein des différents UITs participant à la W.A.N party :

Blagnac, Clermont, Valence, Saint Malo : Métrologie.

Béziers, Colmar : Mur de la WAN +WEBTV + Matchs à jouer / en cours diffusion des finales.

Béthune, Saint Malo : Médiatisation.

Blois, Sofia, Saint-Malo : Gestion des jeux.

Sofia, Blagnac : Inscriptions.

Sofia, Béthune : Docu-WIKI.

Béziers : Outil d’aide à l’installation des joueurs (recherche de la place des joueurs, modification des infos si prêt de matériel, mineurs, présence des documents, ...).

Calendrier des réunions effectuées en visio-conférence : (Voir Annexe pour les comptes-rendus)

1ère Réunion le jeudi 15 octobre.

2ème Réunion le jeudi 19 novembre.

3ème Réunion jeudi 17 décembre.

4ème Réunion jeudi 14 janvier.

5ème Réunion jeudi 11 février.

Dernière Réunion jeudi 10 mars à J-2.

2-Planification du projet :

I-Répartition des tâches à effectuer :

L’organisation d’un tel évènement requiert un travail assez important, sans compter le travail effectué par les étudiants de 1ère Année. Afin de nous simplifier la tâche, nous nous sommes divisés le travail entres équipiers :

Paul Gallo : Script PHP d’aide à l’installation des joueurs, aide à l’installation des serveurs.

Laura Piano : Configuration du point d’accès, mise en place de la baie.

Florian Caliz : Mise en place du serveur Mumble, câblage de la baie.

Benjamin Calvet : Mise en place de l’infrastructure et installation des serveurs (jeux et routeur).

II-Dates importantes : (Gantt)

Réunion de Paris : 1 Octobre 2015

Planification des objectifs : Fin Octobre – Début Novembre.

Développement du projet : Novembre – Fin Février.

Finalisation : Première semaine de Mars.

Répétition Générale : Jeudi 10 Mars 2016.

Mise en Œuvre/Exécution : Samedi 12 Mars 2016.

3-Développement du projet :

I-Présentation de L’infrastructure :

Avant toute chose, il faut préciser que tous les tests effectués avant la mise en place finale de l’infrastructure, ont été réalisés en salle B204.

Le but étant de relier chaque établissement, il a été pensé une architecture VPN en étoile. Chaque routeur présent dans le réseau est alors client VPN et peut accéder à ses voisins en passant par le serveur VPN situé à Nice (10.200.0.1/26).Les adresses IP sont attribuées par le serveur VPN en fonction du département où se localise chaque IUT (exemple avec Béziers : 10.200.0.34). Est relié également au routeur une interface vers l’extérieur (internet) d’où les joueurs pourront avoir accès aux serveurs de jeux. On peut rajouter qu’il est possible de faire passer tout le flux sortant par le tunnel VPN afin d’avoir un flux chiffré et ainsi plus sécurisé, mais cela aurai rajouté de la consommation de bande passante.

Ainsi notre routeur dispose de **3 interfaces** dont une interface « tun » :

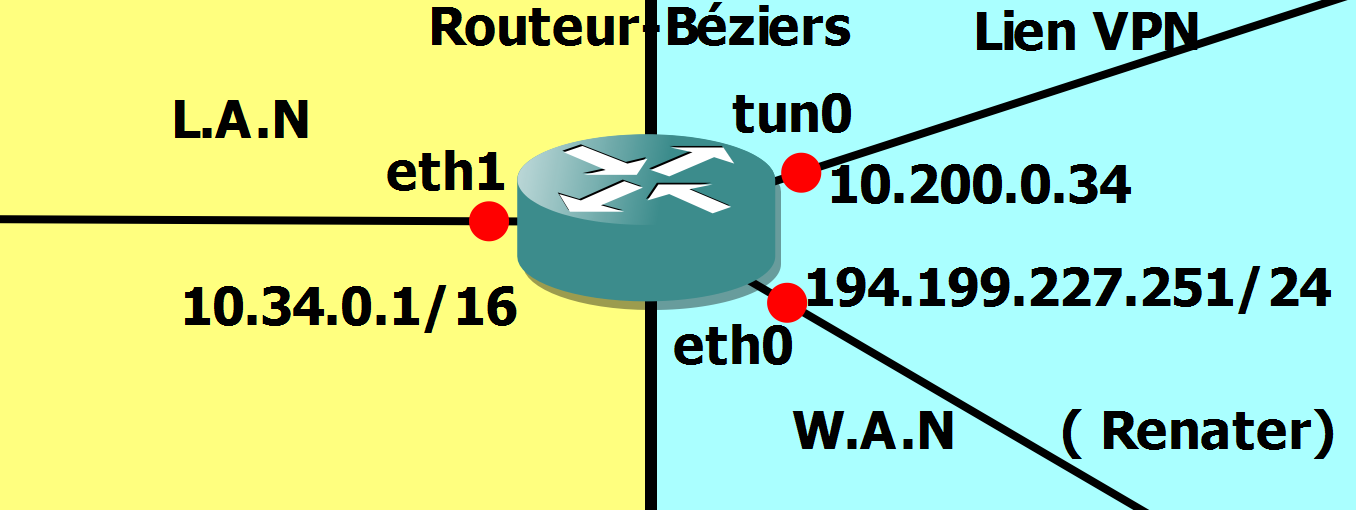
* Eth0 : Interface coté extérieur (Internet), elle donne sur le réseau 194.199.227.0/24.
* Eth1 : Interface coté intérieur (IUT/Joueurs), elle donne sur le réseau 10.34.0.0/16.
* Tun0 : Interface du tunnel VPN, elle joint le serveur basé à Nice en 10.200.0.1.

Figure 1:Vue du routeur de Béziers.

Infrastructure au niveau national :

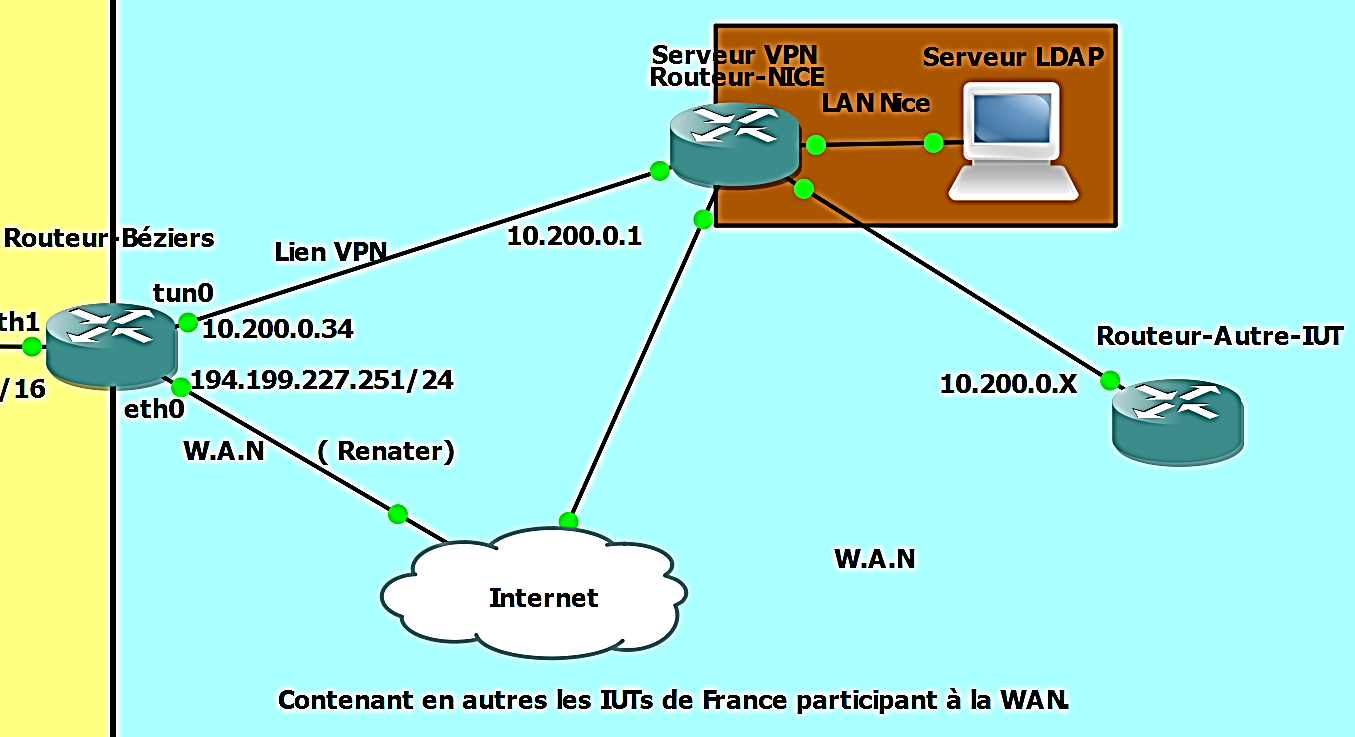
Comme précisé précédemment, les différents clients VPN peuvent se « voir » entre eux. Notre routeur peut ainsi joindre le routeur « Autre-IUT » comme montré dans le schéma ci-dessous, un projet de supervision commune avait été évoqué ; en utilisant ce procédé mais n’as pas été mis en place.

Figure 2:Vue de l'infrastructure externe (W.A.N).

Dans notre cas seule l’authentification des joueurs et les résolutions DNS passent par le tunnel VPN. Pour le reste (jeux en ligne, tchat) on utilise l’interface donnant sur l’extérieur. Dans un souci de sécurité et pour ne pas encombrer la bande-passante, l’accès à internet fut restreint aux jeux. Nous développerons ce sujet dans la partie sur le Pare-Feu.

L’adresse externe (à savoir 194.199.227.251) ainsi que l’accès à la DMZ nous ont étés fournie par le C.R.I, la passerelle par défaut étant 194.199.255.254. (cf. Annexe)

Infrastructure au niveau local :

Pour ce qui est du côté interne du routeur (L.A.N), nous avons mis en place une architecture composée d’un routeur qui fait également office de serveur DNS/DHCP et Pare-Feu, de deux serveurs de jeux (Minecraft et CS:GO), de 3 principaux switches stackés, d’autres switchs pour les joueurs et d’un routeur de secours (au cas où).

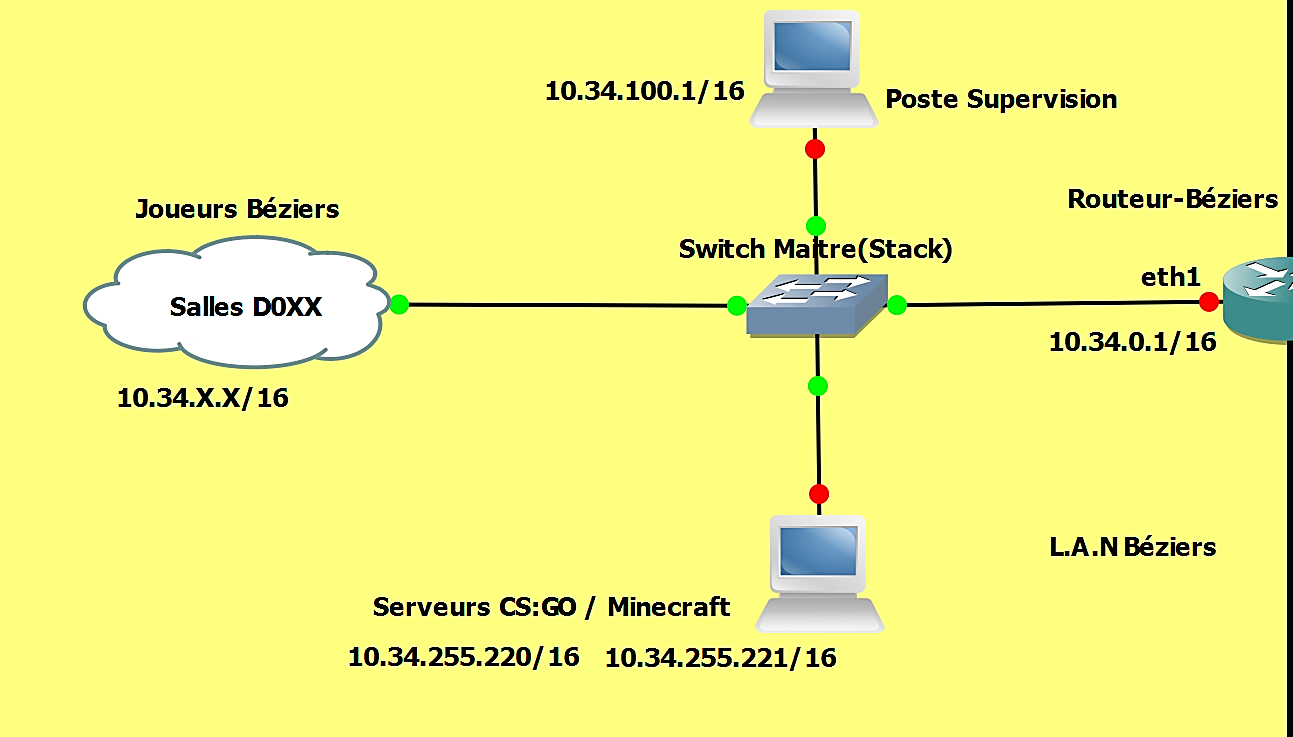
Les joueurs situés dans les salles D013 à D015 ont été brassés sur les prises des salles, reliées directement aux 3 switches principaux de la baie (voir schéma ci-dessous Fig.3).

Figure 3 : Vue de l'infrastructure interne (L.A.N).

II-Inventaire du matériel :

Afin de réaliser ce projet, voici le matériel mis à notre disposition :

* 4 serveurs avec chacun 4 disques durs réf *:(*[*http://www.manualslib.com/download/500820/Tyan-Tank-Gt25-B5381.html*](http://www.manualslib.com/download/500820/Tyan-Tank-Gt25-B5381.html) *)*
* 1 Baie de serveurs.
* Une vingtaine de switchs. Réf : *(*[*http://www.manualslib.com/manual/113151/Nortel-2000.html?page=2#manual*](http://www.manualslib.com/manual/113151/Nortel-2000.html?page=2#manual))
* 110 câbles RJ45.
* 30 multiprises.
* Toutes les salles D0XX.
* Une adresse en DMZ 197.199.227.251.
* Un accès aux armoires de brassages du rez-de-chaussée de l’IUT.



Figure 3: Switchs maitres.

Figure 2: Serveurs de jeux et routeur.

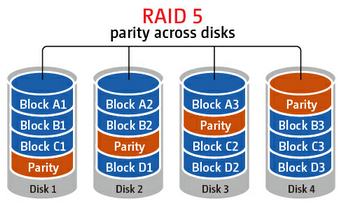
Figure 1 : Baie des Serveurs.

III-Mise en place de l’infrastructure interne (L.A.N) :

Nous avons présenté le fonctionnement de l’architecture L.A.N précédemment, voici comment nous avons procédé pour mettre celle-ci en état de marche :

Installation du routeur/serveurs de jeux : Tous nos serveurs ont été installés sur des serveurs TANK avec pour système d’exploitation : Debian 8 Jessie 64-bits. Ces machines étant dotés de quatre disques durs, nous avons optés pour une configuration en R.A.I.D 5, dont voici une brève explication :

*« Plus récent sur nos cartes mères, le RAID 5 combine performances disques et fiabilité des données, tout comme le RAID 0+1. A la différence que ce ne sont plus que trois disques qui sont ici au minimum requis. Les données sont segmentées, puis réparties entre les disques avec en plus une information de parité pour chaque donnée. Ce qui permettra en cas de panne de régénérer le disque après remplacement. » Source :* [*http://www.generation-nt.com*](http://www.generation-nt.com)



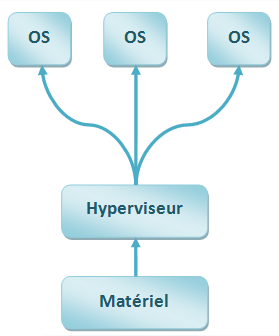
Ainsi nous avons choisis ce type de RAID pour ses performances et sa tolérance à la panne. Nous avons donc utilisés 3 disques pour le système et de disque secours en cas de panne de l’un des trois autres.

Installation du routeur : Après l’installation du système d’exploitation, et ajout d’une source dans le « sourcelist », nous avons installé le paquet WAN-VPN contenant les instructions pour la configuration automatique des serveurs WEB/DNS et DHCP en fonction du département. Présent également dans ce paquet : OpenVPN qui nous permet d’établir le tunnel avec Nice (les clés et les certificats sont livrés avec le paquet).

Tout est déjà fonctionnel dans le routeur, il ne reste qu’à configurer les adresses et le pare-feu.

3.2.1 Solutions alternatives et Innovations :

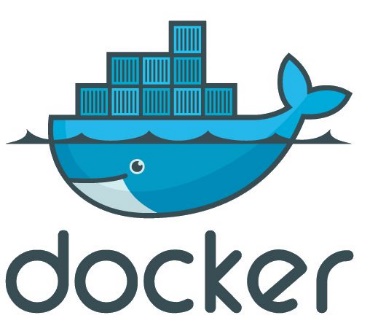
Dans le cadre de ce projet, quelques idées nous sont venues afin d’apporter une innovation sur le plan technique. Ainsi, nous avons pensé à faire un « cluster » de 3 serveurs avec un hyperviseur de type 1 : Proxmox, la figure 1 décrit le fonctionnement d’un tel hyperviseur :





Ainsi, pourquoi ne pas créer plusieurs machines virtuelles ? Chacune d’entre elles représentant un serveur de jeux/routeur. Cette solution avait un aspect assez intéressant mais ne pouvait pas être réalisée, en effet le nombre peu important de machines virtuelles et la stabilité de l’ensemble pour un événement tel que la W.A.N ne nous mettait pas en confiance. Peut-être qu’avec un peu plus d’expérience nous aurions mis cette solution en œuvre.

Le routeur de « spare » : dans le cadre de la W.A.N, une panne de l’un des serveurs pourrait s’avérer désastreuse, ainsi dans le but d’assurer une certaine redondance, nous avons installé sur l’un de nos 4 serveurs, un routeur de secours (SPARE) qui en cas de dysfonctionnement du routeur principal pourrait servir de roue de secours et de ne pas interrompre l’évènement trop longtemps.

Container docker pour applications de monitoring :

Nous aurions également aimé deployer un container docker fournit sur GitHub (<https://github.com/kamon-io/docker-grafana-influxdb>) contenant : Grafana, InfluxDB ( base de donnée) et StatsD (collecte de données).

3.2.2 Le Pare-Feu :

Le pare feu se trouvant sur notre routeur était un Netfilter intégré dans Debian que nous avons administré via iptables durant toute la journée de la WAN. Il nous a été fourni par le paquet WAN-VPN disponible sur wanparty.neticien.net/routeur/depot.

Constitué de plusieurs chaînes présentes dans toutes les tables (mangle, filter, nat) elles-mêmes imbriquées dans plusieurs autres pour un total de 113 règles (cf. annexes règles firewall).

Sachant que toutes ce règles interagissent les unes avec les autres, nous avons évité d’y toucher pour ne pas compromettre l'efficacité du pare-feu. On notera cependant des contradictions dans ces règles (policy deny all,regle accept all). La globalité de ses règles nous permet d’avoir un accès sécurisé des joueurs à internet (enfin presque).

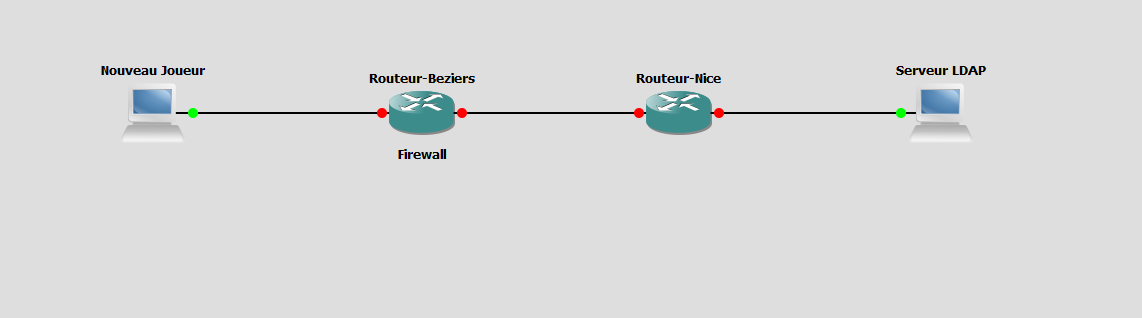
Nous pouvons noter qu’avant l’évènement le pare-feu a été préparé pour parer certains flux indésirables tels que les mises à jour Windows. Pour se faire nous avons listé la liste des éventuels serveurs Microsoft (cf. annexes).

IV-Authentification des joueurs :

L’authentification des joueurs se fait sur le serveur LDAP situé à Nice, chaque joueur lors de son inscription reçoit un couple identifiant/mot de passe qu’il doit entrer à sa première connexion sur notre infrastructure.

Le routeur possède un serveur web apache 2 qui affiche un script php où le joueur doit rentrer ses identifiants, une fois cela terminé, les identifiants sont envoyés par le tunnel VPN au serveur LDAP.

Si l’authentification réussie, le serveur renvoie un acquittement qui va créer des règles dans le pare-feu permettant l’accès à internet au joueur, comme l’illustre le schéma ci-dessous :



Envoie du couple login/mdp