

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. Authentification des joueurs.
   5. 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.

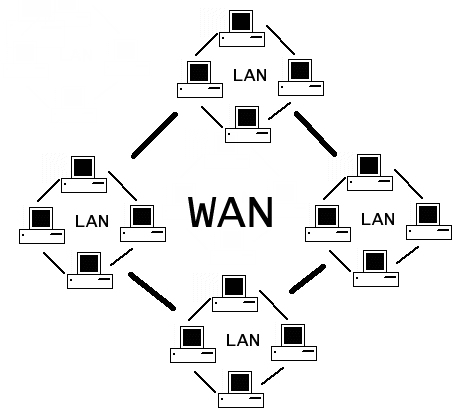


Fig. 1

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. C’est d’autant plus un évènement qui permet une collecte de fonds via les produits vendus au sein de l’établissement et la présentation d’entreprises qui sponsorisent la WAN via des lots, affiches, financements etc.

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 :

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 » :

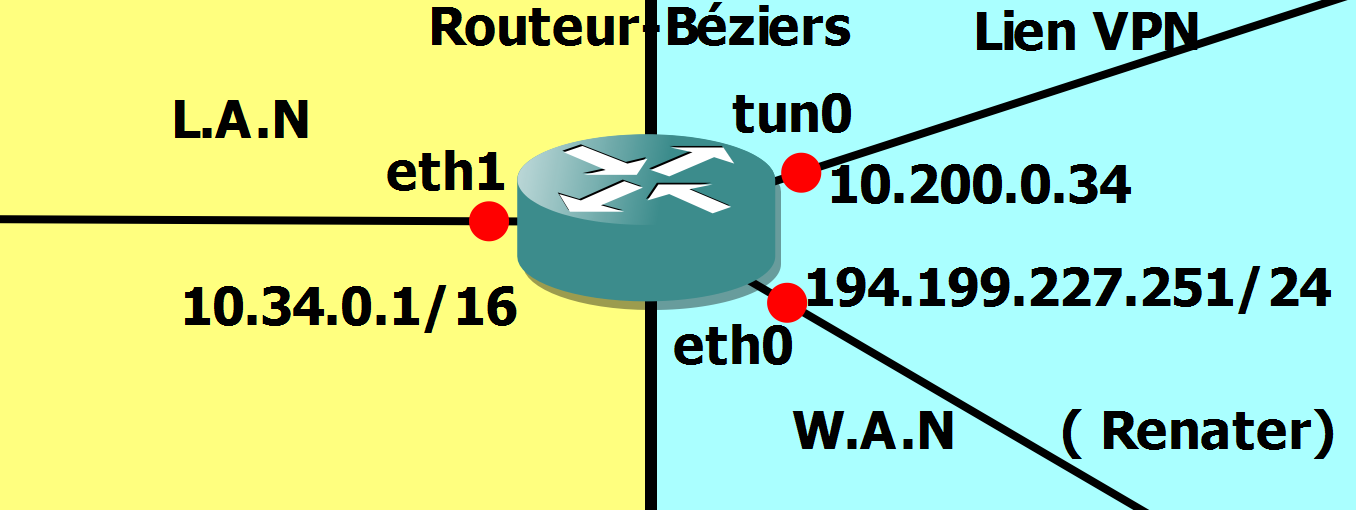
* Eth0 : Interface coté extérieur (Internet), elle donne sur le réseau 194.199.227.0/24.
* Eth1 : Interface coté intérieur (IUT/Joueurs), elle donne sur le réseau 10.34.0.0/16.
* Tun0 : Interface du tunnel VPN, elle joint le serveur basé à Nice en 10.200.0.1.

Figure :Vue du routeur de Béziers.

Infrastructure au niveau national :

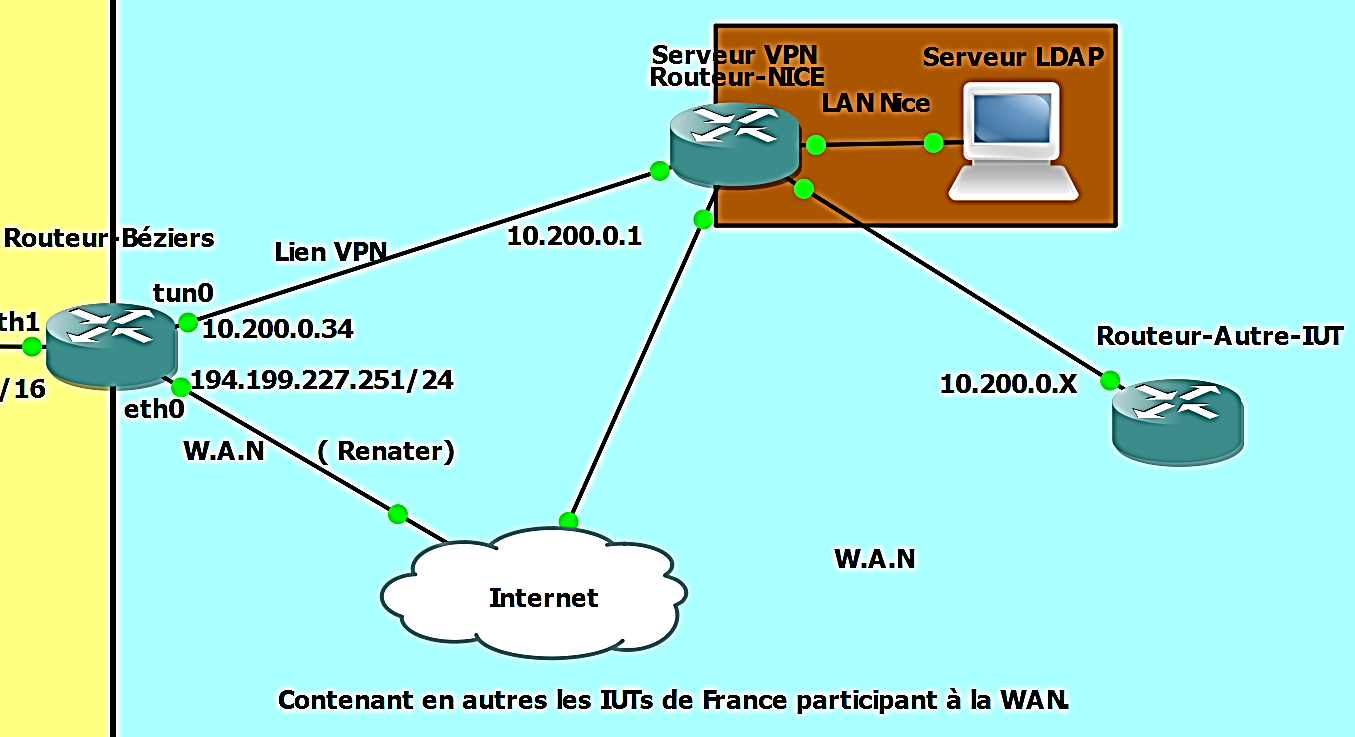
Comme précisé précédemment, les différents clients VPN peuvent se « voir » entre eux. Notre routeur peut ainsi joindre le routeur « Autre-IUT » comme montré dans le schéma ci-dessous, un projet de supervision commune avait été évoqué ; en utilisant ce procédé mais n’as pas été mis en place.

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

Dans notre cas seul 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).

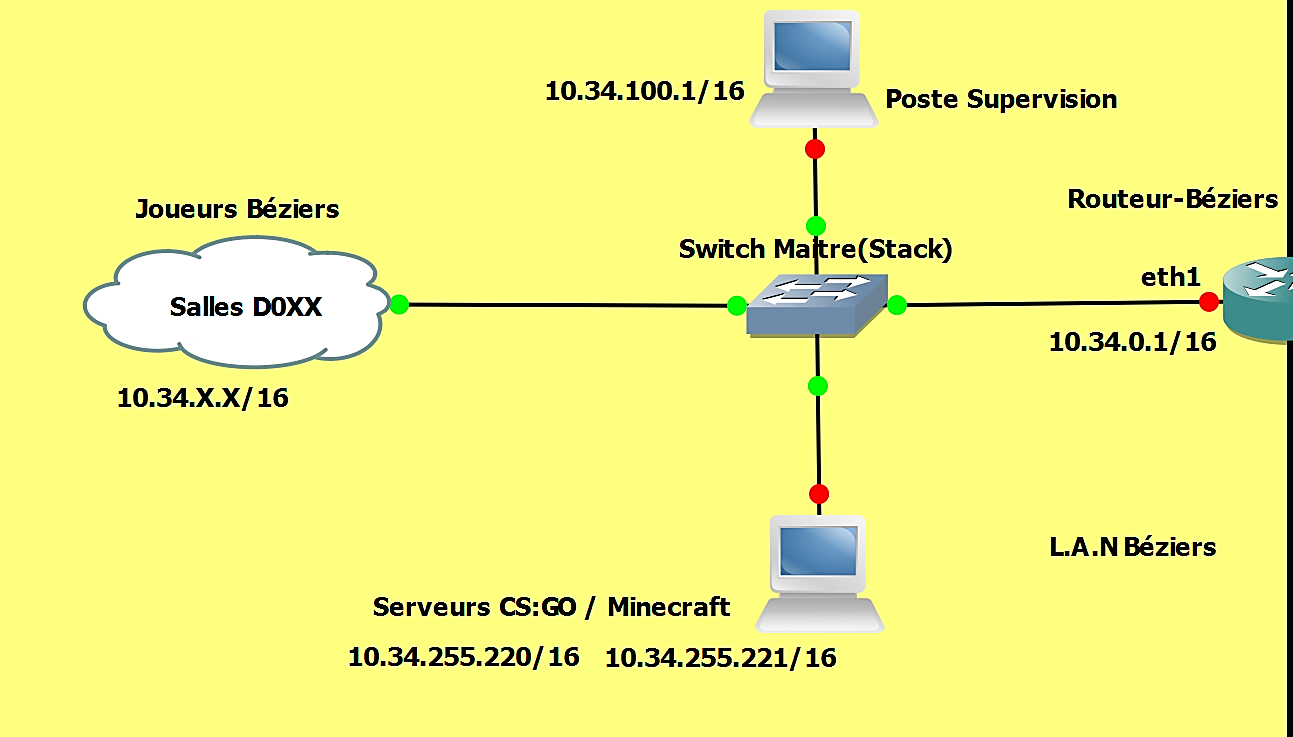
Les joueurs situés dans les salles D013 à D015 ont été brassés sur les prises des salles, reliées directement aux 3 switches principaux de la baie (voir schéma ci-dessous Fig.3).

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 : Switchs maitres.

Figure 3: Serveurs de jeux et routeur.

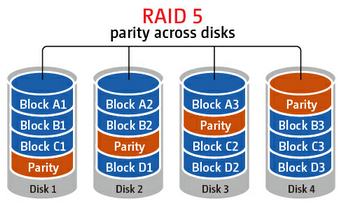
Figure 1 : Baie des Serveurs.

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)



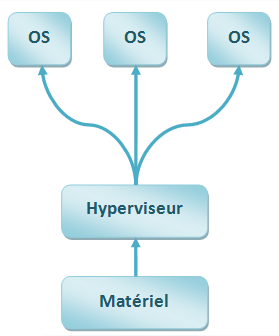
Ainsi nous avons choisis ce type de RAID pour ses performances et sa tolérance à la panne. Nous avons donc utilisés 3 disques pour le système et de disque secours en cas de panne de l’un des trois autres.

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 :

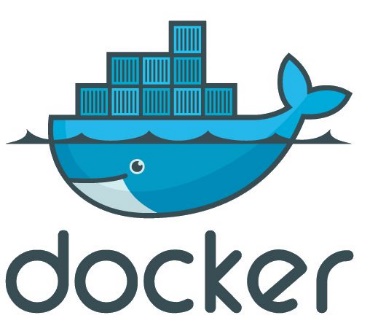
Dans le cadre de ce projet, quelques idées nous sont venues afin d’apporter une innovation sur le plan technique. Ainsi, nous avons pensé à faire un « cluster » de 3 serveurs avec un hyperviseur de type 1 : Proxmox, la figure 1 décrit le fonctionnement d’un tel hyperviseur :





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 déployer 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).

Docker présentant une facilité de déploiement cela aurait pu être un plus pour notre infrastructure.

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 l’utilitaire 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. Nous avons cependant constaté des contradictions dans ces règles ; par exemple la police par défaut de la chaine INPUT était DROP et une règle dans la chaine indiquait ACCEPT ALL.

Un point à améliorer pour l’année prochaine sera de reconfigurer le pare-feu dans son intégralité afin de le rendre plus utile et compréhensible. 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 prévisibles tels que les mises à jour Windows. Pour ce faire, nous avons listé la liste des éventuels serveurs de mise à jour Microsoft (cf. annexes) et nous les avons bannis.

Afin de rentrer les serveurs et les postes qui allaient servir à la supervision, nous avons rentré manuellement les adresses de ces machines dans le pare-feu à l’aide d’un script bash :

root@R-34:~/scripts# ./firewall\_client\_add.sh 10.34.255.221 Serveur\_minecraft

\*\*\*NEW: /sbin/iptables -t mangle -I CLIENTS -s 10.34.255.221 -m mac --mac-source 00:e0:81:72:ba:be -j RETURN

Chain CLIENTS (1 references)

num pkts bytes target prot opt in out source destination

1 0 0 RETURN all -- \* \* 10.34.255.221 0.0.0.0/0 MAC 00:E0:81:72:BA:BE

2 0 0 RETURN all -- \* \* 10.34.0.0/29 0.0.0.0/0

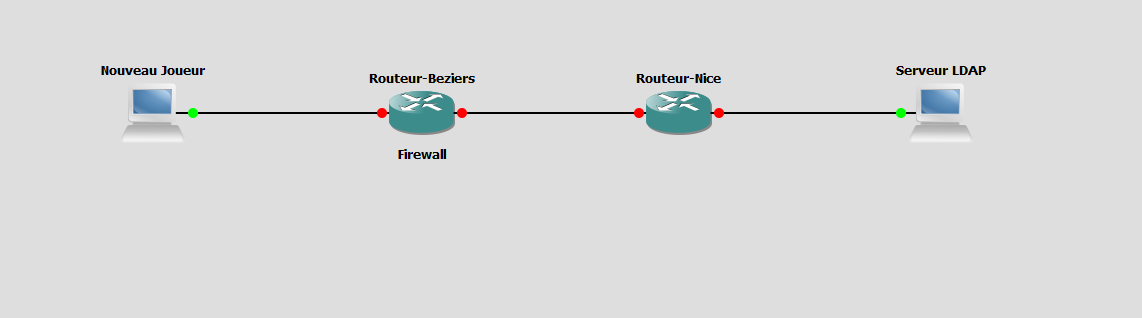
3 4 240 MARK all -- \* \* 0.0.0.0/0 !10.34.0.1

MARK set 0x63

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/mot de passe

Si Authentification validée : Accès autorisé + ajout règles pare-feu

Si Authentification échouée : Accès refusé gles pare-feu

Recherche dans l’annuaire …

V-Divers :

Installation de monitoring pour les serveurs de jeux : Minecraft [McMyAdmin] / Monitorix.

Afin de garder un œil sur l’état et la charge des serveurs de jeux, nous avons installé deux solutions.

McMyAdmin : Ce petit utilitaire permet la surveillance et l’administration d’un serveur Minecraft via une interface web. Toutefois, il n’est pas libre et demande une licence pour un serveur ayant une capacité supérieure à 20 joueurs. Le nombre d’inscrits pour Minecraft étant largement en dessous de ce seuil, nous avons choisis de le mettre en place.



Monitorix : Logiciel libre de supervision, il nous a été utile pour le serveur CS : GO.

Serveur Mumble :

Installé par Florian Caliz. Il a été mis en place pour la communication entre les membres du staff et lentre les joueurs, nous avons installé deux serveurs Mumble. La raison de l’installation d’un Mumble pour les joueurs était du point de vue technique, un moyen de faire communiquer les joueurs localement pour libérer un peu plus la bande passante du routeur. Nous avons choisis Mumble car c’est un logiciel  « opensource » et simple d’utilisation pour les clients. L’une des deux instances était sur le serveur Minecraft qui était donc relié directement au réseau local et l’autre sur une machine à part qui a été fourni par un tiers et relié uniquement à un AP Wi-Fi Cisco emprunté au CRI pour l’occasion (réf : AIR-AP1242G-E-K9).

Le serveur pour les joueurs était configuré pour pouvoir accueillir sans le moindre problème 150 joueurs, divisé pour tous les jeux et avec assez de canaux pour accueillir un peu plus que les équipes qui était inscrites avec un mot de passe différent pour chaque canal.

Pour la configuration de l’AP il a fallu tout d’abord lui donner une adresse IP, lui donner un SSID, une clé de sécurité et configurer le serveur DHCP. La couverture du point d’accès couvrait quasiment l’intégralité du couloir et des salles.

4- Exécution du projet « D-Day » :

I-Organisation :

En ce qui concerne l’organisation de l’évènement même, tout a été prévu et défini à l’avance lors de nos réunions en visio-conférence. La préparation à commencer la veille le vendredi soir, nous avons descendu la baie des serveurs dans le couloir au rez-de-chaussée. Nous avons ensuite fait l’inventaire des prises à brasser dans les salles D0XX.

Nous pouvons ensuite organiser la suite des événements comme une liste :

* Agencement de toutes les salles D0XX pour la W.A.N Party.
* Brassage de toutes les prises des salles sur les switchs maitres.
* Brassage de la DMZ sur l’interface externe du routeur.
* Adressage externe en 194.199.227.251/24.
* Mise en place des switchs et multiprises pour les joueurs.
* Rapide test de l’infrastructure.
* Test du matériel réseau (switchs joueurs).

Le samedi, la journée a commencée à 7h, nous avons tout mis sous tension, démarré les services de monitoring. Nous avons attendu l’arrivée des joueurs 9h. La journée s’est relativement bien déroulée, hormis quelques petits problèmes au niveau des serveurs de jeux que nous détailleront dans une partie ci-après. Nous devons une grande participation aux « helpers » et aux autres étudiants qui nous ont aidés à la mise en place des salles.

La journée s’est achevée vers 23h le temps de tout ranger.

II-Mise en place de la baie/infra :

Nous avons mis en place la baie le soir avant l’évènement, étiqueter tout ce qui semblait nécessaire et brasser les prises voici quelques images de la baie :



Figure 1 : Switchs maitres stackés.



Figure 2 : Serveurs physiques.

Réécriture du fichier /etc/network/interfaces : (exemple de l’interface externe)

#Interface externe (eth0)

allow-hotplug eth0

iface eth0 inet static

address 194.199.227.251

netmask 255.255.255.0

network 194.199.227.0

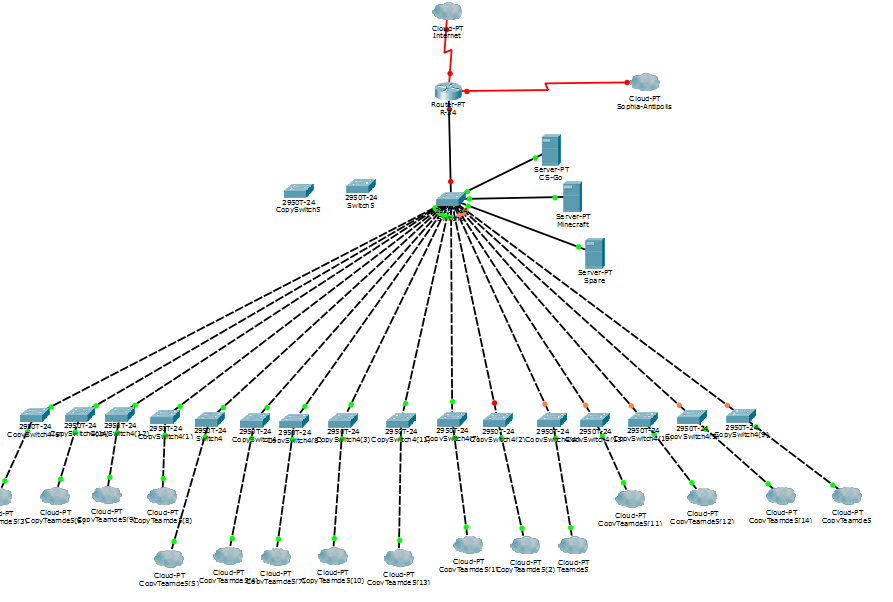
broadcast 194.199.227.255

gateway 194.199.227.254

dns-nameservers 127.0.0.1

dns-search wan-rt

Schéma récapitulatif de l’infrastructure L.A.N :



III-Supervision des flux :

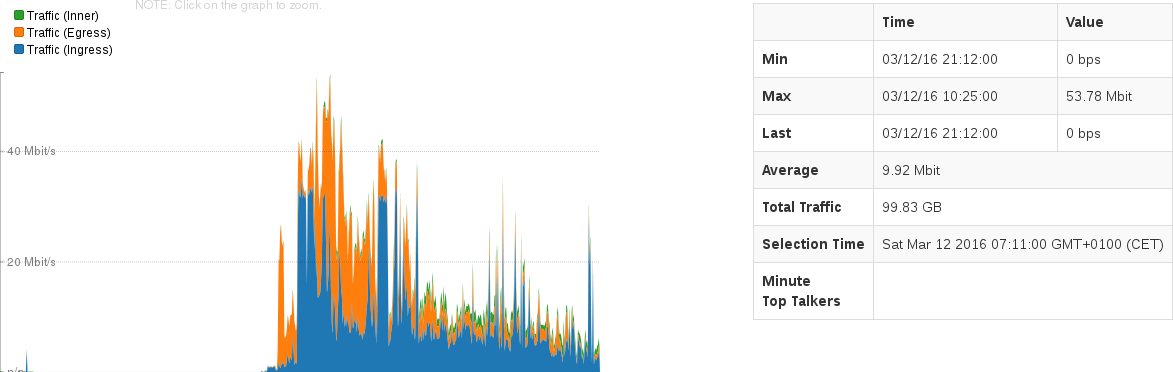
La supervision des flux a été effectuée sur le routeur via NTOPNG (ntop next-generation) basé sur libpcap , est un logiciel sous licence GPLv3 codé en C++ avec une interface web Lua sur le port 3000 comme présenté dans le document ci-dessous.

NTOPNG nous délivre une interface avec de nombreuses options, telle que la visualisation des flux réseaux en temps réel, le tri par applications, montre les statistiques sur le nombre de requêtes transmises/reçues. Très utile également la petite jauge en bas le page qui indique les pics de consommation de bande-passante, ce qui aide à visualiser rapidement les facteurs de cette consommation et ainsi d’intervenir rapidement.



Visualisation des flux réseaux par ordre de consommation décroissante.

Nous avons constamment surveillé le réseau tout au long de la journée pour repérer d’éventuels problèmes et cette surveillance s’est avérée payante. Vous pouvez voir ci-dessous une représentation graphique du débit de données qui ont transitées sur le routeur tout au long de la journée, aussi bien le flux entrant que sortant.



Vue sur la journée de la consommation de bande-passante.

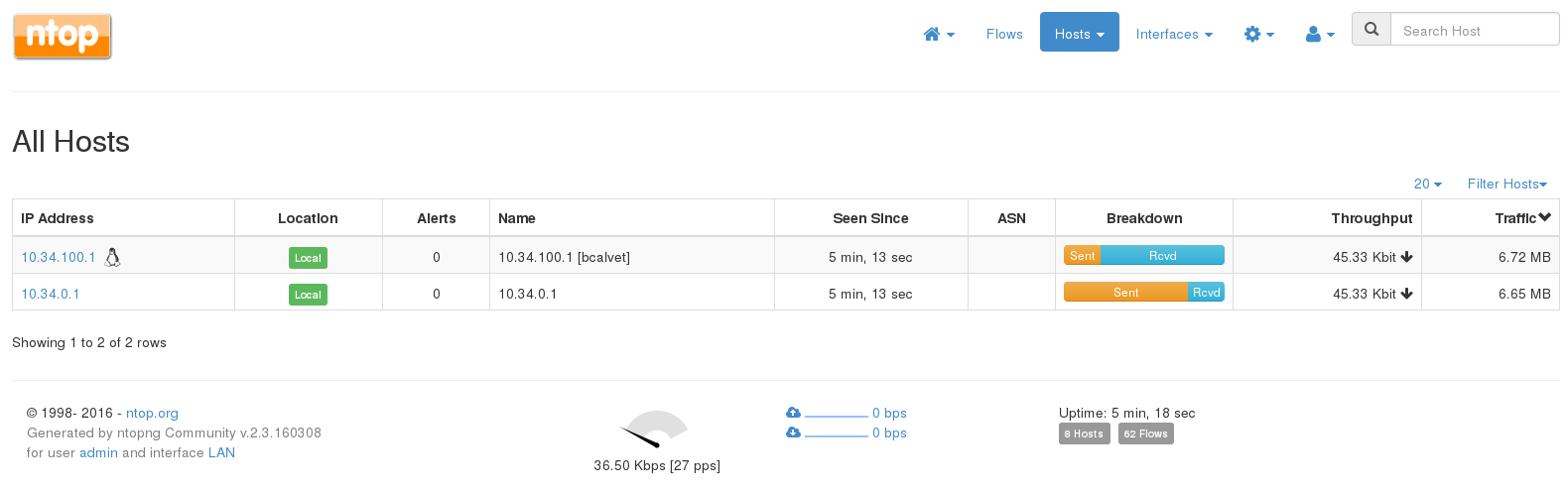
Comme vous pouvez le remarquer, l’allure de la courbe varie énormément au cours de la journée, ces pics et chutes de trafic ont étés provoqués par des problèmes techniques rapidement résolus ; ceux-ci sont décrit dans la rubrique “problèmes rencontrés”.

Nous avons réussi à limiter la bande passante en enlevant certains flux :

* YouTube.
* Skype.
* Logiciels de Torrents.
* Certaines mises à jour de jeux en ligne.

Il a été décidé de notre propre initiative d’installer un NTOPNG, en effet, celui proposé par l’équipe de l’IUT de Blagnac qui était en charge de la métrologie nous semblait un peu trop vétuste bien que facile à installer et à utiliser.

Ce NTOPNG a été compilé et installé par Benjamin CALVET, suite à une installation longue il a décidé de rédiger un script d’installation (cf. Annexe) afin d’automatiser l’installation sur n’importe quelle machine Debian.



Exemple de vue des hôtes présents sur le réseau.

NTOPNG propose une résolution des noms de domaine, cela nous a été très utile pour ne pas bannir n’importe quelle adresse IP.

IV-Problèmes rencontrés :

Dans cette rubrique nous allons passer en revue tous les problèmes auxquels nous avons étés confrontées durant la journée de la WAN Party :

Mise à jour subite : Le serveur CS:GO dont nous disposions n'était pas à jour, nous avons eu la malchance d’avoir une mise à jour entre le vendredi soir et le samedi. Les joueurs qui ont tenté de se connecter en fin d'après-midi ont donc étés forcés d’attendre que nous fassions la mise à jour. Celle-ci s’est avérée trop coûteuse en débit pour la laisser tourner pendant que les joueurs disputaient des matchs au niveau national en effet cela induisait beaucoup trop de latence. Nous avons donc dû attendre que certains aient fini. Cette mise à jour est la cause d’une partie des pics de débit de la fin d’après-midi, elle fut néanmoins achevée.

Un autre problème auquel nous avons été confrontés s’est avéré être notre propre matériel, en effet lors de la mise en route des switchs maitres, deux d’entre eux ont cessé de fonctionner environ un quart d’heure après. Ce qui nous contraint à rebrasser tous les clients sur le switch restant.

Deuxième problème que nous avons eu au niveau matériel sont les switchs des joueurs qui sont eux aussi tomber en panne quelques minutes après le début, cela n’étant pas prévisible nous sommes allés chercher d’autres switchs dans les salles réseau en urgence afin de rétablir au plus vite la connexion des joueurs. Ces switchs étaient des Nortels qui avaient vraisemblablement plusieurs heures de fonctionnement au compteur et qui n’étaient donc pas fiables.

Retard au national

Ban de mauvaises IP

L’antenne a été emprunté à l’IUT mais ne comportait pas d’antennes, il a fallu en emprunter a une personne de l'extérieur.

L’AP était très instable et n’arrivais pas a gérer beaucoup de clients à la fois donc souvent des déconnexions.

ANNEXES

**Script de bannissement  des adresses IP :**

#!/bin/bash

#SCRIPT INSTALL

apt-get install at

clear

LOGFILE="/var/log/logs\_ban\_wan"

if test -z $1 ; then

   echo "Utilisation :"

   echo "----"

   echo "-[un|de]ban :"

   echo "Entre dans le mode pour [un|de]ban une IP"

   echo "----"

fi

if test "$1" = "-ban" ; then

while true ; do

   echo "################################################"

   echo "Quelle IP bannir ? :"

   read IP

   echo "Combien de minutes ? [1-720] (defaut 1min) :"

   read T

   if test -z $T || test $T -lt 0 || test $T -gt 720 ; then

      T=1

   fi

   if [[ "$IP" =~ ^(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.){3}([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])$ ]] ; then //regex IP

      echo "Bannir l'IP $IP ? [O/n]"

      read confirm

      if test -z "$confirm" || test "$confirm" = "O" || test "$confirm" = "o" ; then

          echo "+ $IP ; `date -R |cut -d' ' -f5`" >> $LOGFILE

          iptables -A PREROUTING -t mangle -s $IP -j DROP

          echo "IP bannie : $IP"

          (sleep "$T"m ; iptables -D PREROUTING -t mangle -s $IP -j DROP ; echo "- $IP ; `date -R |cut -d' ' -f5`" >> $LOGFILE) &

      fi

   else

      echo "Ce n'est pas une IP..."

   fi

done

elif test "$1" = "-unban" || test "$1" = "-deban" ; then

while true ; do

   echo "################################################"

   echo "Quelle IP débannir ? :"

   read IP

if [[ "$IP" =~ ^(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.){3}([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][│0-9]|25[0-5])$ ]] ; then

       echo "Débannir l'IP $IP ? [O/n]"

       read confirm

       if test -z "$confirm" || test "$confirm" = "O" || test "$confirm" = "o" ; then

           iptables -D PREROUTING -t mangle -s $IP -j DROP ; echo "- $IP ; `date -R |cut -d' ' -f5`" >> $LOGFILE

           echo "IP débannie : $IP"

       fi

   else

      echo "Ce n'est pas une IP..."

   fi

done

fi

**Script de bannissements externes**

#!/bin/bash

#

# Ici je bloque youtube...

#iptables -A PREROUTING -t mangle -s 216.58.0.0/16 -j DROP

# Ici je bloque twitch...

iptables -A PREROUTING -t mangle -s 192.16.64.0/21 -j DROP

iptables -A PREROUTING -t mangle -s 192.16.64.0/21 -j DROP

iptables -A PREROUTING -t mangle -s 192.16.64.0/21 -j DROP

# Ici je bloque spotify...

iptables -A PREROUTING -t mangle -s 194.132.198.165 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.197.147 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.198.228 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.196.178 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.198.115 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.196.163 -j DROP

iptables -A PREROUTING -t mangle -s 185.31.17.246 -j DROP

iptables -A PREROUTING -t mangle -s 193.235.232.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 78.31.8.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 78.31.12.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 23.92.96.0/20 -j DROP

iptables -A PREROUTING -t mangle -s 194.71.148.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.68.28.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.68.183.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.68.181.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.68.176.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.68.165.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.68.116.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.14.177.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.204.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.196.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.176.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.173.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.172.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.168.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.162.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.132.152.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.103.36.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 194.103.13.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 194.103.10.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.235.32.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.235.232.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 193.235.224.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.235.206.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.235.203.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.234.240.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 193.182.8.0/21 -j DROP

iptables -A PREROUTING -t mangle -s 193.182.7.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.182.3.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.182.244.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.182.243.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 193.181.4.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 193.181.180.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 192.165.160.0/22 -j DROP

iptables -A PREROUTING -t mangle -s 192.121.53.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 192.121.132.0/24 -j DROP

# Ici je bloque deezer...

iptables -A PREROUTING -t mangle -s 78.40.123.183 -j DROP

iptables -A PREROUTING -t mangle -s 78.40.123.182 -j DROP

# Ici je bloque soundcloud...

iptables -A PREROUTING -t mangle -s 93.184.220.127 -j DROP

# Ici je bloque dailymotion...

iptables -A PREROUTING -t mangle -s 195.8.215.136 -j DROP

# Ici je bloque skype...

iptables -A PREROUTING -t mangle -s 23.97.215.12 -j DROP

iptables -A PREROUTING -t mangle -s 111.221.74.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 111.221.77.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 157.55.130.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 157.55.235.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 157.55.56.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 157.56.52.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 213.199.179.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 64.4.23.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 65.55.223.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 91.190.218.0/23 -j DROP

iptables -A PREROUTING -t mangle -s 91.190.216.0/23 -j DROP

iptables -A PREROUTING -t mangle -s 192.26.92.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.31.80.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.12.94.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.35.51.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.42.93.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.54.112.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.43.172.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.48.79.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.52.178.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.41.162.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.55.83.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.33.14.30 -j DROP

iptables -A PREROUTING -t mangle -s 192.5.6.30 -j DROP

iptables -A PREROUTING -t mangle -s 111.221.74.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 111.221.77.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 157.55.130.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 157.55.235.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 157.55.56.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 157.56.52.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 213.199.179.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 64.4.23.0/24 -j DROP

iptables -A PREROUTING -t mangle -s 65.55.223.0/24 -j DROP

# Ici je bloque tor (le browser)...

iptables -A PREROUTING -t mangle -s 193.11.114.43 -j DROP

iptables -A PREROUTING -t mangle -s 188.166.154.140 -j DROP

# Ici je bloque le torrent (j'essaie)...

iptables -A PREROUTING -t mangle -p tcp --dport 6881:6889 -j DROP

iptables -A PREROUTING -t mangle -p tcp --sport 6881:6889 -j DROP

iptables -A PREROUTING -t mangle -p tcp --dport 6969 -j DROP

iptables -A PREROUTING -t mangle -p tcp --sport 6969 -j DROP

iptables -A PREROUTING -t mangle -p udp --dport 6881:6889 -j DROP

iptables -A PREROUTING -t mangle -p udp --sport 6881:6889 -j DROP

iptables -A PREROUTING -t mangle -p udp --dport 6969 -j DROP

iptables -A PREROUTING -t mangle -p udp --sport 6969 -j DROP

**Script de bannissement des updates windows**

#!/bin/bash

for ip in `cat static\_ban` ; do

       iptables -A PREROUTING -t mangle -s $ip -j DROP

       iptables -A PREROUTING -t mangle -d $ip -j DROP

done

iptables -A PREROUTING -t mangle -p udp --destination-port 8530 -j DROP

iptables -A PREROUTING -t mangle -p udp --destination-port 8531 -j DROP

iptables -A PREROUTING -t mangle -p udp --source-port 8530 -j DROP

iptables -A PREROUTING -t mangle -p udp --source-port 8531 -j DROP

iptables -A PREROUTING -t mangle -p tcp --destination-port 8530 -j DROP

iptables -A PREROUTING -t mangle -p tcp --destination-port 8531 -j DROP

iptables -A PREROUTING -t mangle -p tcp --source-port 8530 -j DROP

iptables -A PREROUTING -t mangle -p tcp --source-port 8531 -j DROP

**Script d’installation NTOP**

#!/bin/bash

#Created by Benjamin Calvet (benjamin.calvet@iutbeziers.fr)

#At 18:00:32 Saturday 05/03/2016

echo -e "Installation de ntopng-2.2:\n"

wget http://downloads.sourceforge.net/project/ntop/ntopng/ntopng-2.2.tar.gz

tar -zxvf ntopng-2.2.tar.gz

mv ntopng-2.2 /opt/ntopng

cd /opt/ntopng

echo -e "Installation des dépendances:\n(Press any key to continue)"

read ok

apt-get update

apt-get install subversion libglib2.0 libxml2-dev libpcap-dev libtool rrdtool librrd-dev autoconf automake autogen redis-server wget libsqlite3-dev libhiredis-dev libgeoip-dev libcurl4-openssl-dev libpango1.0-dev libcairo2-dev libpng12-dev git make gcc build-essentials dh-autoreconf libmysqlclient-dev

wget https://curl.haxx.se/download/curl-7.47.1.tar.gz

tar -zxvf curl-7.47.1.tar.gz

cd curl-7.47.1

make && make install

cd ..

chmod +x autogen.sh

bash autogen.sh

echo -e "Autogen OK ? "

read ok

chmod +x configure

bash configure

make

**Clients autorisés a avoir acces a internet le jour de la WAN:**

10.34.18.110 , 34-nat356:OK (Sat Mar 12 08:57:30 CET 2016 , d8:cb:8a:81:66:e3)

10.34.18.111 , Benoit.JACQUEMOND (Sat Mar 12 00:00:00 CET 2016 , f0:1f:af:42:53:f8)

10.34.18.119 , Paul.AZEMA.MUR (Sat Mar 12 00:00:00 CET 2016 , 08:60:6e:7f:2c:80)

10.34.18.123 , windows (vendredi 11 mars 2016 , 08:00:27:d2:35:24)

10.34.18.124 , Paul.AZEMA.MUR.D013 (Sat Mar 12 00:00:00 CET 2016 , 18:03:73:ba:cc:16)

10.34.18.127 , Paul.AZEMA.MUR.D016 (Sat Mar 12 00:00:00 CET 2016 , 18:03:73:bd:49:28)

10.34.18.128 , 34-GatoChocolat:OK (Sat Mar 12 08:17:47 CET 2016 , bc:5f:f4:d3:f9:92)

10.34.18.129 , 34-Tanatius:OK (Sat Mar 12 09:29:07 CET 2016 , 08:62:66:23:f6:8b)

10.34.18.130 , 34-Globus:OK (Sat Mar 12 08:17:17 CET 2016 , 40:8d:5c:49:eb:bd)

10.34.18.131 , Vivien.SEGAUD (Sat Mar 12 00:00:00 CET 2016 , 44:8a:5b:6d:a5:e7)

10.34.18.132 , Quentin.FRANKAWSER (Sat Mar 12 00:00:00 CET 2016 , d8:cb:8a:ef:5d:ff)

10.34.18.133 , Rémi.SPOLIDORO (Sat Mar 12 00:00:00 CET 2016 , d0:50:99:5d:10:a4)

10.34.18.134 , Paul.AZEMA.MUR.D018 (Sat Mar 12 00:00:00 CET 2016 , 18:03:73:bd:14:6a)

10.34.18.136 , 34-RainbawRaider:OK (Sat Mar 12 09:50:15 CET 2016 , e4:11:5b:fb:0e:bd)

10.34.18.137 , 34-braidd34:OK (Sat Mar 12 09:45:05 CET 2016 , 2c:60:0c:d3:71:56)

10.34.18.138 , 34-teamraider:OK (Sat Mar 12 09:48:32 CET 2016 , 8c:89:a5:08:0b:23)

10.34.18.139 , 34-SnowbawRaider:OK (Sat Mar 12 09:51:34 CET 2016 , d0:bf:9c:93:bd:bc)

10.34.18.140 , 34-DrDarkhitsu:OK (Sat Mar 12 09:45:21 CET 2016 , e8:03:9a:90:79:aa)

10.34.18.141 , 34-Grym34:OK (Sat Mar 12 09:45:24 CET 2016 , 58:20:b1:7c:47:9b)

10.34.18.142 , 34-LiMiToDriGe:OK (Sat Mar 12 09:04:25 CET 2016 , 54:04:a6:69:93:dc)

10.34.18.143 , 34-Sunbaw:OK (Sat Mar 12 09:50:52 CET 2016 , 64:00:6a:6c:10:e0)

10.34.18.144 , 34-Tuffouplumo:OK (Sat Mar 12 09:51:10 CET 2016 , 50:e5:49:32:d3:9a)

10.34.18.145 , Tristan.BANULSJOUEUR (Sat Mar 12 00:00:00 CET 2016 , 60:02:92:21:8a:3d)

10.34.18.146 , 34-Asayari:OK (Sat Mar 12 09:44:39 CET 2016 , 40:8d:5c:01:21:af)

10.34.18.147 , Mario.ORSCUCCI (Sat Mar 12 00:00:00 CET 2016 , f8:a9:63:3f:a9:a2)

10.34.18.148 , 34-ehavon:OK (Sat Mar 12 09:51:59 CET 2016 , f4:6d:04:ae:31:69)

10.34.18.149 , 34-Ryukusen:OK (Sat Mar 12 09:47:41 CET 2016 , 5c:f9:dd:5f:ac:f4)

10.34.18.150 , 34-Athinis:OK (Sat Mar 12 09:48:12 CET 2016 , 54:04:a6:10:e4:03)

10.34.18.151 , 34-Kickleo:OK (Sat Mar 12 09:47:36 CET 2016 , 54:a0:50:8c:c3:9f)

10.34.18.152 , 34-lecelebre:OK (Sat Mar 12 09:46:19 CET 2016 , a4:5d:36:73:dd:2d)

10.34.18.153 , 34-damdji4434:OK (Sat Mar 12 09:46:59 CET 2016 , d4:3d:7e:b7:32:01)

10.34.18.154 , 34-SlakR:OK (Sat Mar 12 10:11:56 CET 2016 , ac:9e:17:be:7a:66)

10.34.18.155 , 34-ivaylo123:OK (Sat Mar 12 09:41:27 CET 2016 , 5c:f9:dd:60:4b:27)

10.34.18.156 , 34-InfernalCane:OK (Sat Mar 12 09:46:53 CET 2016 , 44:8a:5b:9e:3c:4d)

10.34.18.157 , 34-Neodozone:OK (Sat Mar 12 10:10:26 CET 2016 , 10:bf:48:4c:59:54)

10.34.18.158 , 34-Ostgard:OK (Sat Mar 12 09:18:46 CET 2016 , 58:20:b1:7c:c4:f5)

10.34.18.159 , 34-Nokiazz:OK (Sat Mar 12 09:45:59 CET 2016 , 00:25:22:d4:0c:ca)

10.34.18.160 , 34-neosky:OK (Sat Mar 12 09:46:30 CET 2016 , 44:8a:5b:cb:71:ab)

10.34.18.161 , 34-djedkk:OK (Sat Mar 12 09:47:08 CET 2016 , 54:a0:50:c7:9a:ca)

10.34.18.162 , 34-rydeforlife:OK (Sat Mar 12 09:42:20 CET 2016 , 78:24:af:1d:80:70)

10.34.18.163 , 34-Exl:OK (Sat Mar 12 09:29:24 CET 2016 , d8:cb:8a:81:23:06)

10.34.18.164 , 34-Stanou:OK (Sat Mar 12 09:30:37 CET 2016 , 30:85:a9:a6:0d:4f)

10.34.18.165 , 34-tik3402:OK (Sat Mar 12 09:31:13 CET 2016 , d8:cb:8a:53:6c:58)

10.34.18.167 , 34-DraxxsLight:OK (Sat Mar 12 09:45:49 CET 2016 , 44:8a:5b:ed:a4:12)

10.34.18.168 , 34-Tonitto34:OK (Sat Mar 12 09:37:38 CET 2016 , 2c:56:dc:9d:05:9e)

10.34.18.169 , 34-Xtremely34:OK (Sat Mar 12 09:55:27 CET 2016 , 08:9e:01:f8:ec:d2)

10.34.18.170 , 34-Fistouse744:OK (Sat Mar 12 09:47:14 CET 2016 , a0:2b:b8:59:e5:22)

10.34.18.171 , 34-featful:OK (Sat Mar 12 09:49:16 CET 2016 , 34:64:a9:76:c9:42)

10.34.18.172 , 34-BeeFire:OK (Sat Mar 12 09:33:37 CET 2016 , 34:64:a9:76:c7:e8)

10.34.18.173 , 34-lawlcraft34:OK (Sat Mar 12 09:41:43 CET 2016 , 58:20:b1:7d:d9:bb)

10.34.18.174 , 34-BenjiX34:OK (Sat Mar 12 09:38:06 CET 2016 , ec:a8:6b:26:8d:94)

10.34.18.175 , 34-timobi:OK (Sat Mar 12 09:42:07 CET 2016 , 44:8a:5b:99:87:4f)

10.34.18.176 , 34-Juju34:OK (Sat Mar 12 09:42:43 CET 2016 , 5c:f9:dd:60:7c:f5)

10.34.18.177 , 34-Godsuke:OK (Sat Mar 12 09:47:15 CET 2016 , 1c:b7:2c:20:fa:b6)

10.34.18.178 , 34-IrroZ34:OK (Sat Mar 12 09:36:58 CET 2016 , ac:9e:17:9b:38:d5)

10.34.18.179 , 34-Tometjean24:OK (Sat Mar 12 09:50:48 CET 2016 , 1c:75:08:e4:97:bd)

10.34.18.180 , 34-RDV2017:OK (Sat Mar 12 09:47:15 CET 2016 , f0:76:1c:c1:13:9b)

10.34.18.181 , 34-Metropolis:OK (Sat Mar 12 09:50:07 CET 2016 , 00:26:9e:2a:c5:ad)

10.34.18.182 , 34-Futte:OK (Sat Mar 12 09:37:15 CET 2016 , d8:50:e6:0c:08:8e)

10.34.18.183 , 34-Fazz:OK (Sat Mar 12 09:45:27 CET 2016 , 6c:c2:17:5d:ea:43)

10.34.18.184 , 34-ange200:OK (Sat Mar 12 09:47:13 CET 2016 , d0:50:99:27:60:38)

10.34.18.185 , 34-louis34340:OK (Sat Mar 12 09:53:19 CET 2016 , 40:8d:5c:52:5a:b6)

10.34.18.186 , 34-nuts34:OK (Sat Mar 12 09:46:25 CET 2016 , 1c:b7:2c:3a:e4:c4)

10.34.18.187 , 34-lucatoncou:OK (Sat Mar 12 09:52:24 CET 2016 , d4:3d:7e:4c:a6:a1)

10.34.18.188 , 34-SkyZz:OK (Sat Mar 12 09:51:41 CET 2016 , e8:40:f2:c8:ec:85)

10.34.18.189 , 34-Opus:OK (Sat Mar 12 09:48:31 CET 2016 , 5c:f9:dd:60:75:dd)

10.34.18.190 , 34-399pDq9H:OK (Sat Mar 12 09:47:24 CET 2016 , 08:62:66:b6:3c:66)

10.34.18.191 , 34-Hugo3452:OK (Sat Mar 12 09:42:32 CET 2016 , 08:62:66:b7:7e:90)

10.34.18.192 , 34-LordAlshade99:OK (Sat Mar 12 10:13:06 CET 2016 , 94:57:a5:01:5e:f1)

10.34.18.193 , 34-Zaskai:OK (Sat Mar 12 09:09:19 CET 2016 , 8c:89:a5:0d:39:19)

10.34.18.194 , 34-5dF94skpG39:OK (Sat Mar 12 11:22:26 CET 2016 , 1c:87:2c:e1:2e:e7)

10.34.18.196 , 34-bapt120:OK (Sat Mar 12 10:18:06 CET 2016 , 58:20:b1:80:1c:a3)

10.34.18.197 , 34-xXbananeXx:OK (Sat Mar 12 10:11:42 CET 2016 , 44:8a:5b:5c:83:92)

10.34.18.198 , 34-azerty34120:OK (Sat Mar 12 10:13:54 CET 2016 , 58:20:b1:7f:74:9b)

10.34.18.199 , 34-RDV2018:OK (Sat Mar 12 09:51:39 CET 2016 , d0:bf:9c:1a:28:5d)

10.34.18.200 , 34-MrDarkaxX:OK (Sat Mar 12 09:54:24 CET 2016 , 60:a4:4c:e5:f1:44)

10.34.18.201 , 34-BboyYumsy:OK (Sat Mar 12 10:01:24 CET 2016 , b8:70:f4:90:77:3e)

10.34.18.202 , 34-Mrisbo:OK (Sat Mar 12 10:12:51 CET 2016 , 44:8a:5b:ef:fd:ca)

10.34.18.203 , 34-RaitoninguTV:OK (Sat Mar 12 10:00:04 CET 2016 , 08:62:66:b5:50:22)

10.34.18.204 , 34-Luchappy:OK (Sat Mar 12 10:11:00 CET 2016 , 50:46:5d:cf:7d:0b)

10.34.18.205 , 34-aaronddu34:OK (Sat Mar 12 10:13:18 CET 2016 , 58:20:b1:7d:cf:60)

10.34.18.206 , 34-Unlick:OK (Sat Mar 12 10:15:13 CET 2016 , 44:8a:5b:d4:27:7c)

10.34.18.207 , 34-IrroZ34:OK (Sat Mar 12 10:17:07 CET 2016 , d8:cb:8a:3a:57:b2)

10.34.18.209 , 34-warma:OK (Sat Mar 12 10:43:04 CET 2016 , 3c:18:a0:02:b9:ae)

10.34.18.211 , 34-GoldmanSexe:OK (Sat Mar 12 10:52:21 CET 2016 , 5c:f9:dd:5f:0a:f2)

Salle de monitoring

10.34.100.1 , Ben-Calvet (Sat Mar 12 00:00:00 CET 2016 , d4:be:d9:4d:ba:ed)

10.34.100.2 , Maxime.POUVREAU (Sat Mar 12 00:00:00 CET 2016 , f8:a9:63:50:90:fc)

10.34.100.3 , Paul.GALLO (Sat Mar 12 00:00:00 CET 2016 , 10:c3:7b:1f:e1:21)

10.34.100.5 , Vincent.FRICOU (Sat Mar 12 00:00:00 CET 2016 , 08:60:6e:06:4f:75)

Serveurs

10.34.255.220 , CS:GO (Sat Mar 12 00:00:00 CET 2016 , 00:e0:81:72:ba:74)

10.34.255.221 , Minecraft (Sat Mar 12 00:00:00 CET 2016 , 00:e0:81:72:ba:be)

**Config DHCP**

ddns-update-style none;

option domain-name "wan.rt";

option domain-name-servers 10.34.0.1;

default-lease-time 54000;

max-lease-time 72000;

log-facility local7;

subnet 10.34.0.0 netmask 255.255.0.0 {

 range 10.34.0.50 10.34.255.254;

 option routers 10.34.0.1;

}

**Bind forwarder**

options {

       directory "/var/cache/bind";

        forwarders {

               10.200.0.1; //On Forward vers le tunnel VPN à Sofia

       //      10.6.0.1;

        };

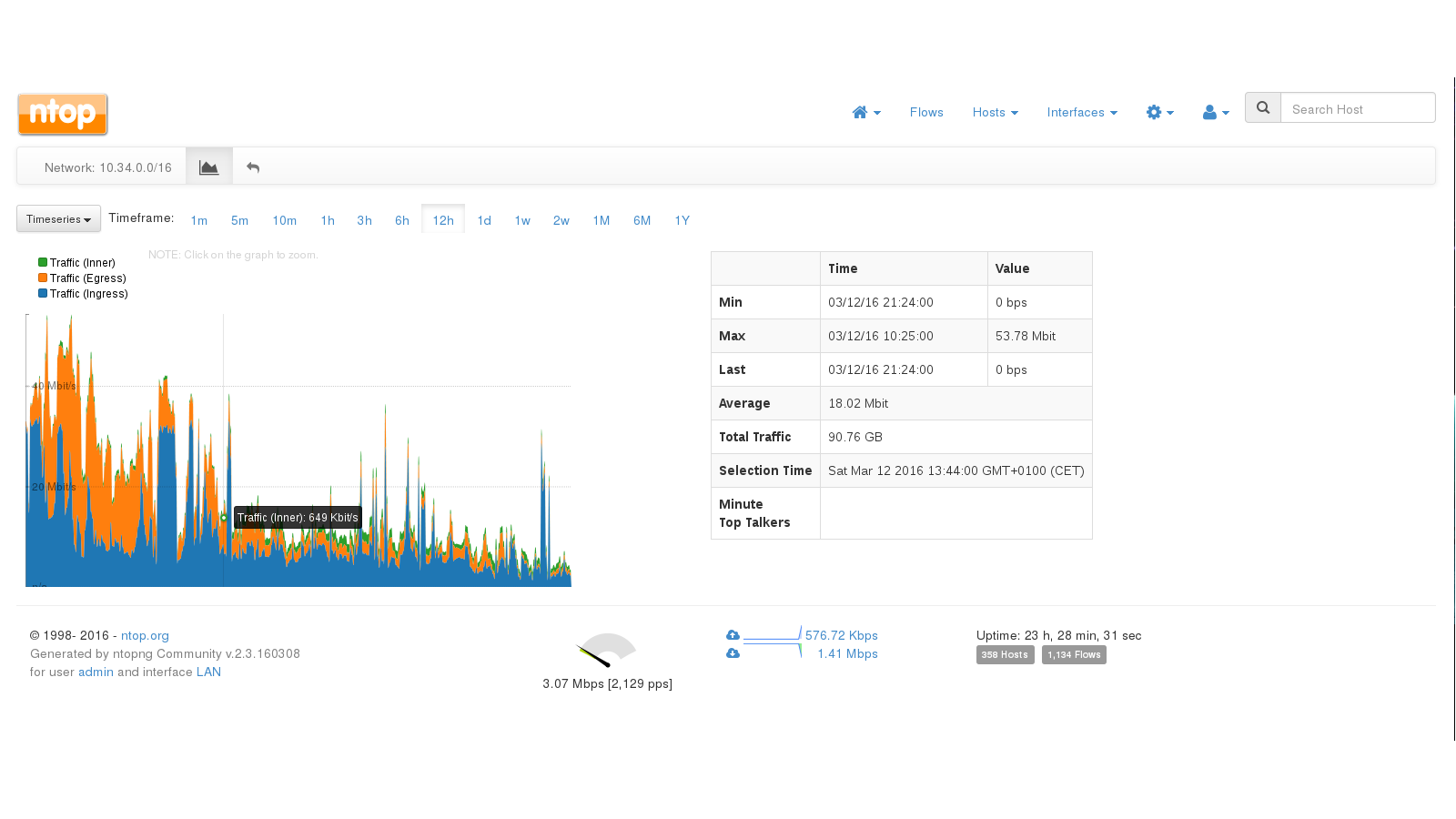
       dnssec-validation auto;

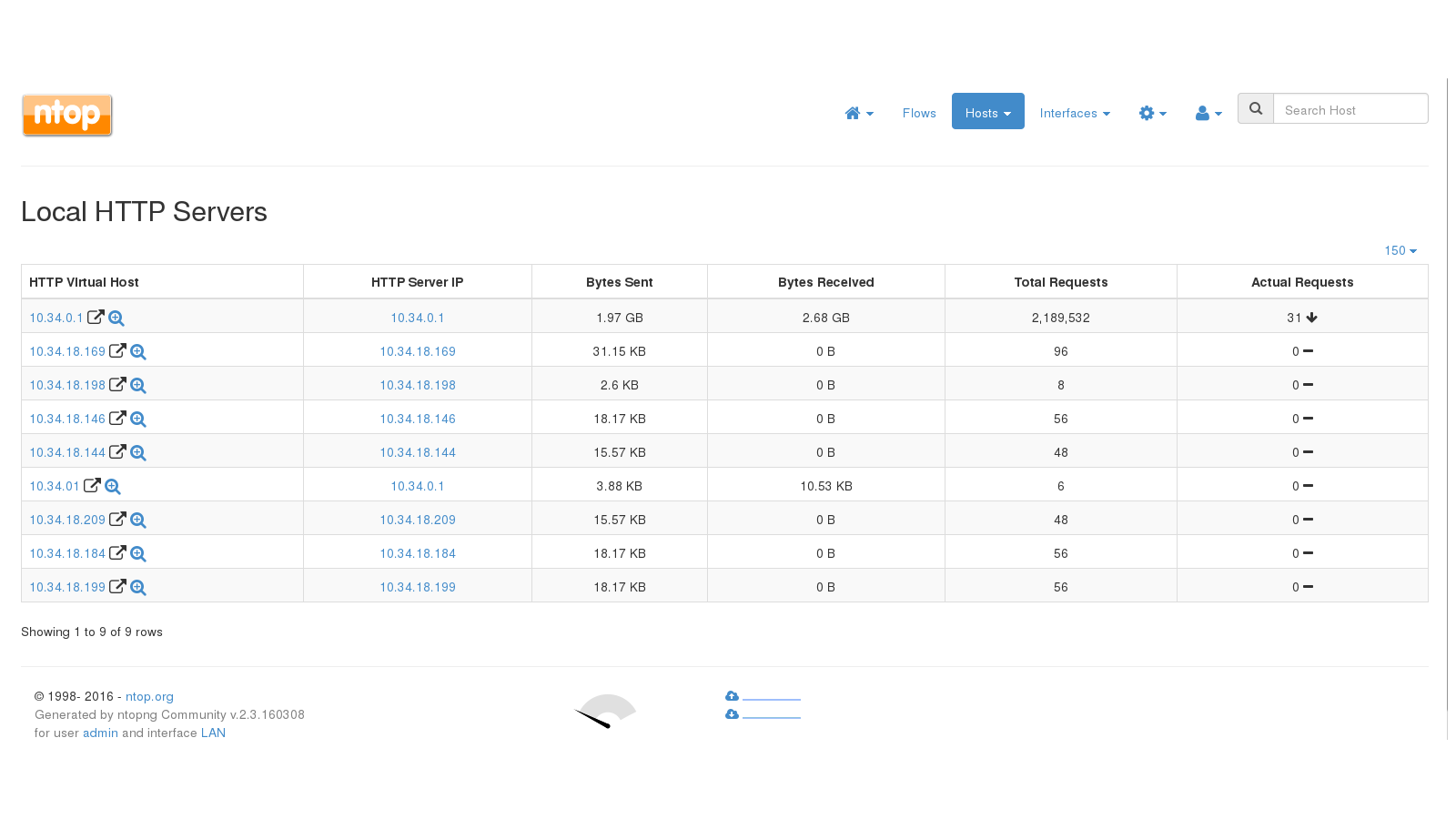
       auth-nxdomain no;    # conform to RFC1035

       listen-on-v6 { any; };

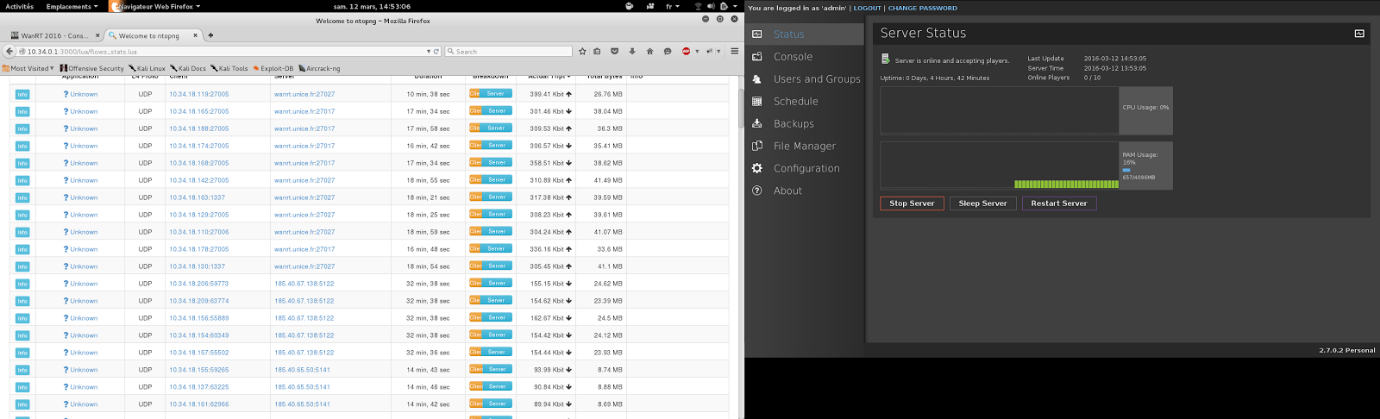
};

**Graphique du débit durant la journée de la WAN**

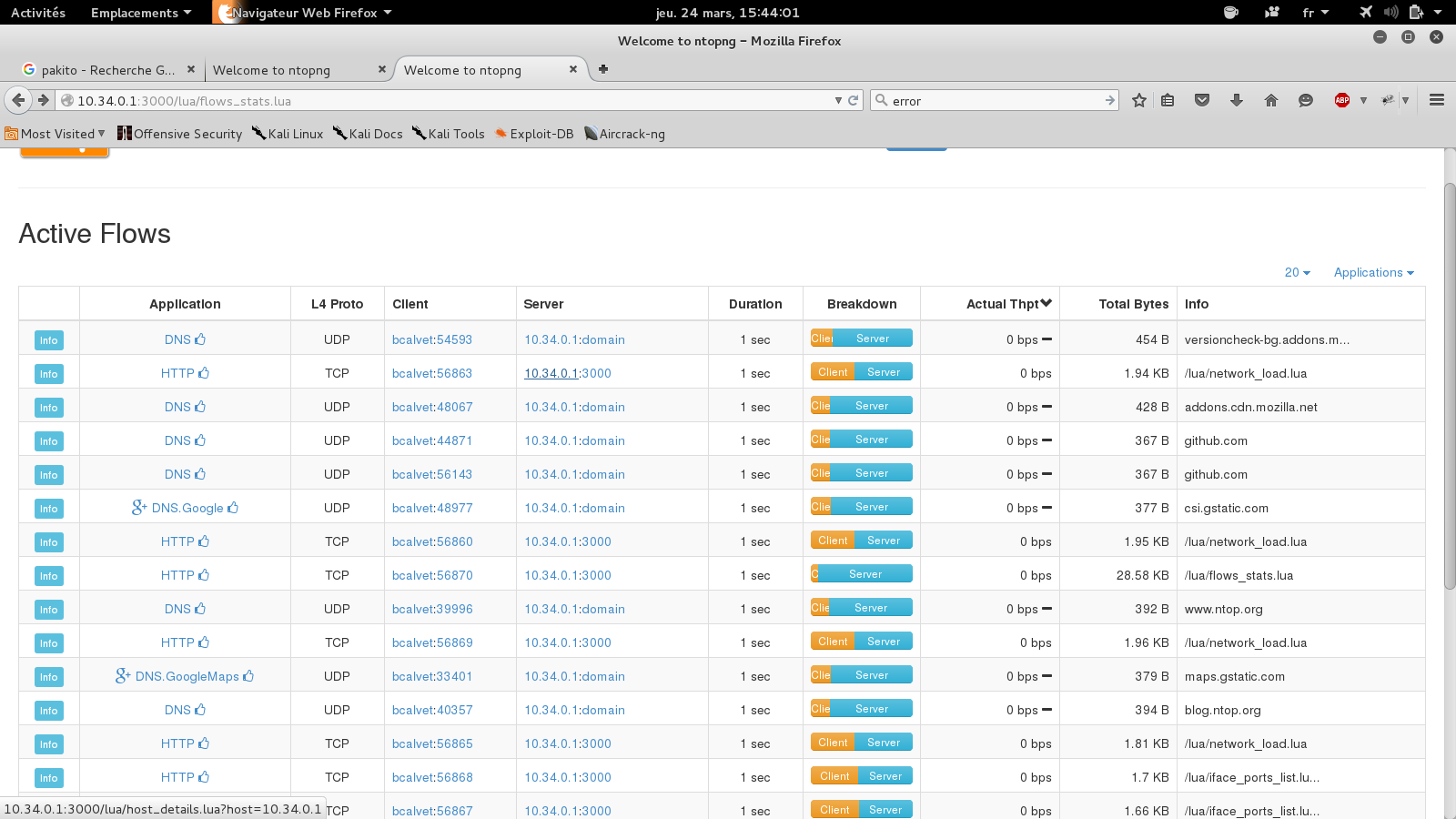
**Débit et données sur le routeur**

****

**Supervision minecraft**

****

**Supervision des flux**

****