



Filtrage web pour L'optimisation d'un Réseau Informatique Universitaire. « Cas de l'Université Adventiste de Goma (U.A.GO.) »

KWITONDA BAVUGE Theophile

Résumé – Ce travail vise à proposer une méthode pour améliorer la disponibilité des données. Pour ce faire, L'instrument qui permet de contrôler, limiter et réguler l'accès au réseau Internet est un proxy http. Le recours à un mandataire est recommandé dans les réseaux où les utilisateurs n'ont pas accès à toutes les informations présentes sur Internet. Comme dans le réseaux universitaire les étudiants ne doivent pas accéder à des certaines ressources pendant les heures d'étude, en plus de filtrer les demandes des utilisateurs et les réponses du serveur, il maximise également le débit en mettant en cache les sites Web précédemment visités. Nous allons d'abord vous donner une explication détaillée du fonctionnement d'un http avant d'introduire le Proxy. Nous examinerons les différentes données échangées entre un client et un serveur web, permettant de comprendre le fonctionnement échangé protocole http. Après cela, nous allons passez en revue les nombreuses fonctionnalités du proxy. Enfin, une présentation des résultats de notre proxy.

Mots clés : Internet, Filtrage Web, Proxy, Réseau Informatique, Réseau Sociaux

Abstract: This work aims to propose a method to improve data availability. To do this, the instrument that allows you to control, limit and regulate access to the Internet network is an http proxy. The use of a proxy is recommended in networks where users do not have access to all the information on the Internet. As in university networks students do not have to access certain resources during study hours, in addition to filtering user requests and server responses, it also maximizes throughput by caching previously visited websites. We will first give you a detailed explanation of how an http works before introducing the Proxy. We will examine the different data exchanged between a client and a web server, allowing us to understand how the http protocol exchanges work. After that, we'll review the proxy's many features. Finally, a presentation of the results of our proxy.

Digital Object Identifier (DOI): <https://doi.org/10.5281/zenodo.15663374>

1 Introduction

A l'heure actuelle, l'intégration des Technologies de l'Information et de la Communication (TIC) dans le système d'information ne peut que leur être bénéfique tant au niveau interne et aux relations qu'elle mène avec l'extérieur en modifiant le monde du travail avec l'apparition des plusieurs outils facilitant les échanges des informations.[1]

L'internet est utilisé pour une variété de domaine, y compris la communication, l'éducation, le divertissement et le commerce. Il est devenu un outil indispensable pour les individus et les entreprises du monde entier.

L'éducation permet aux individus de construire des vies et des sociétés plus prospères et fructueuses pour atteindre la prospérité économique et le bien-être social. L'accès à internet contribue à l'amélioration de la qualité éducative, ouvre des portes à des nombreuses informations, connaissances et des ressources, ce qui augmente les performances des enseignants et les possibilités d'apprentissages au-delà des connaissances recueillies dans la salle de classe aux apprenants. Le terme « filtrage des informations » est utilisé pour décrire un large éventail de procédures conçues pour fournir aux personnes des informations pertinentes aux leurs domaines d'intérêt.[3]

Les bienfaits de l'internet ont été bien compris et beaucoup exploités par les pays développés, l'arrivée de l'internet était plus forte en Amérique du Nord depuis les années 1969 issu du réseau appelé Arpanet créé dans l'objectif de faciliter d'un côté les échanges des informations universitaires, militaires et d'autre côté expérimenter les techniques de transmission des données découpées en paquets ; l'internet se développe plus rapidement aujourd'hui sous l'impulsion des opérateurs privés, les grandes entreprises seules s'y relient directement par des liaisons permanentes et les petites entreprises grâce aux fournisseurs d'accès internet.[4]

1.1 Problématique

L'internet est un réseau informatique accessible au public. Il est toujours constaté que bien des gens ne s'intéressent pas à savoir en détail au fond du fonctionnement de ce fameux réseau.

Le fait de s'intéresser aux visibles et négliger ceux qui se déroulent exactement au fond, c'est un grand danger manifeste aux violations des données, aux vols d'identités etc.

L'université doit échanger des données avec bon niveau de confidentialité, contrôler et surveiller la façon dont les personnels et les étudiants utilisent l'internet.

Néanmoins, avec l'Université Adventiste de Goma (UAGO), il a été constaté que dans son réseau ; l'exploitation des sites web sans restriction, une consommation extrêmement coûteuse de la bande passante et un non suivi de l'utilisation de l'internet sont des situations rencontrées. Par conséquent, avec cet usage non contrôlé présente toujours : l'utilisation abusive de l'internet, exploitation des sites malveillants et des publicités malveillantes, un objet de distraction, une déconcentration aux étudiants, des lenteurs dans le réseau etc.

En tenant compte de toutes ces conséquences citées dans les lignes précédentes ; nous avons décidé de mettre en place un filtrage web afin d'optimiser le réseau informatique de l'UAGO et faciliter le suivi de l'utilisation de l'internet par moyen d'application d'un serveur proxy.

1.2 Objectifs

L'objectif général de cet article est de résoudre les difficultés que rencontre l'UAGO dans le cadre d'administration réseau en mettant en exercice un filtrage du contenu web et amélioration de la disponibilité des ressources dans le but de suivre de l'utilisation correcte de l'internet.

Spécifiquement :

- Le contrôle de l'utilisation de l'internet (Refuser l'accès à des certains sites)
- Mise en cache
- Gestion de la confidentialité des utilisateurs

2 Revue théorique

Voulant mettre en place le filtrage web, nous allons passer en revue sur les différentes pratiques de filtrages afin d'acquérir une compréhension approfondie sur le sujet.

2.1 Logiciels de filtrage Web :

Les logiciels de filtrage Web sont des applications qui peuvent être installés sur un serveur ou sur un appareil client. Ils fonctionnent en analysant le trafic Web et en bloquant l'accès aux sites Web ou au contenu qui ne sont pas autorisés.

Exemples: Cybersitter, Net Nanny, AdGuard Home

Un logiciel de filtrage de contenu peut bloquer l'accès à un site Web d'actualités qui contient des images de violence, peut bloquer également l'accès à un site Web qui contient des informations sur la santé sexuelle si sa référence est basée sur les mots-clés.

Les logiciels de filtrage comportemental peuvent être utilisés pour surveiller les activités en ligne des utilisateurs, ce qui peut porter atteinte à leur vie privée.

2.2 Services de filtrage Web :

Les services de filtrage Web sont des services fournis par des fournisseurs externes. Ces services utilisent des serveurs centralisés pour analyser le trafic Web et bloquer l'accès aux sites Web ou au contenu qui ne sont pas autorisés.

Nous pouvons avoir :

Cisco Umbrella : est un service de filtrage Web payant qui offre une gamme de fonctionnalités avancées, notamment la protection contre les ransomwares, les attaques par hameçonnage et les fuites de données.

Sophos Web Protection : est un autre service de filtrage Web payant qui offre une protection complète contre les menaces en ligne.

2.3 Filtrage Web intégré :

Le filtrage Web intégré est une fonctionnalité qui est incluse dans certains appareils et logiciels. Par exemple, de nombreux routeurs et modems incluent une fonction de filtrage Web qui peut être utilisée pour bloquer l'accès à des sites Web ou à du contenu spécifique.

Il est important de noter que les filtres Web ne sont pas parfaits. Ils peuvent bloquer des sites Web ou du contenu légitimes par erreur surtout que leur gestion est d'issus des logiciels ou des services proposés en ligne. Raison pour laquelle notre sujet vient en application d'un serveur proxy qui pourra intégrer le filtrage web contrôlé par l'administrateur du réseau et l'amélioration de la disponibilité des ressources dans un réseau informatique universitaire par la mise en cache.

3 Un Mandataire (Proxy)

Un serveur mandataire est un serveur qui agit comme intermédiaire entre un client et un serveur. Il est utilisé pour diverses raisons, notamment pour améliorer la sécurité, la performance, autorisation d'accès et la confidentialité.

Fonctionnement

Un serveur mandataire proxy fonctionne en interceptant les requêtes du client et en les transférant au serveur. Le serveur mandataire proxy peut ensuite modifier les requêtes ou les réponses avant de les renvoyer au client selon la politique de gestion.[15]

Les données qui passent par un proxy sont filtrées, sauvegarder temporairement et distribuées. Ce qui nous donne les fonctionnalités suivantes :

- 3.1 - **Le proxy filtre** : pour cette fonctionnalité le proxy est utilisé entant que filtre pour d'un côté, bloquer certains contenus du web destine à des clients ou de l'autre côté pour rejeter automatiquement des demandes douteuses provenant des serveurs.
- 3.2 **Proxy anonyme** : Etant donné que les serveurs proxy empêchent les connexions directes entre les émetteurs et les récepteurs, il est possible de cacher l'adresse IP du client et laisser l'adresser du serveur proxy vers le destinataire.
- **Le proxy cache** : pour pouvoir répondre rapidement à des demandes récurrentes provenant d'un réseau local, un serveur proxy configuré sauvegardera de manière dans le cache une copie des données qu'il reçoit de la part serveurs. [16]

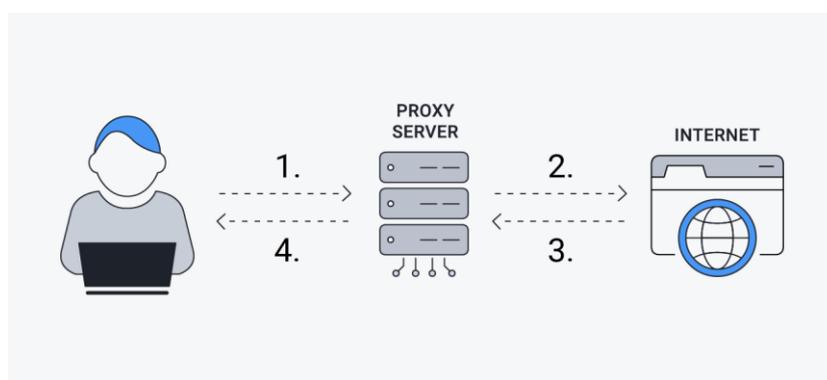


Figure 1: Serveur mandataire

Étape 1 : Un utilisateur saisit une adresse Web dans son navigateur (Envoi d'une requête).

Étape 2 : Le mandataire envoie une requête au serveur (à l'internet).

Étape 3 : Le serveur répond à la requête en envoyant le contenu de la ressource demandée.

Étape 4 : Le mandataire répond à la requête de l'utilisateur (Envoi réponse).

4 FILTRAGE web

Le filtrage web est un dispositif qui interdit aux utilisateurs de consulter certains liens ou certains sites web en empêchant à leur navigateur d'en charger les pages.

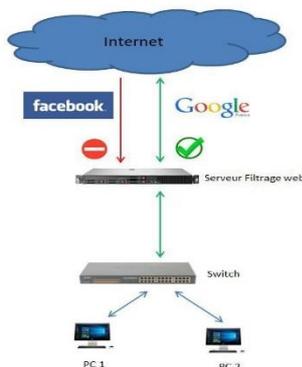


Figure 2: Filtrage web

Étape 1 : Un utilisateur saisit une adresse Web dans son navigateur.

Étape 2 : Le mandataire envoie une requête au serveur (Internet).

Étape 3 : Le serveur répond à la requête en envoyant le contenu de la ressource demandée.

Étape 4 : le mandataire examine le contenu si contenu est Facebook ou YouTube notifie l'utilisateur qu'il ne doit pas consulter les réseaux sociaux pendant les heures de cours. Et si le contenu est différent, le mandataire répond à la requête de l'utilisateur (Envoie réponse).

Le filtrage web est un processus qui consiste à bloquer ou à limiter l'accès à certains sites Web ou à certaines catégories de sites Web. Il est utilisé pour une variété de raisons, notamment pour protéger les utilisateurs contre le contenu inapproprié ou dangereux, pour améliorer la productivité ou pour répondre aux exigences réglementaires.[17]

4.1 Types de filtrage web

Il existe deux principaux types de filtrage web :

- Filtrage de contenu : ce type de filtrage empêche l'accès à des sites Web ou à du contenu spécifique. Il peut être utilisé pour bloquer du contenu nuisible, comme le contenu violent, le contenu sexuel ou le contenu haineux.
- Filtrage d'URL : ce type de filtrage bloque l'accès à des sites Web spécifiques en fonction de leur adresse URL. Il peut être utilisé pour bloquer des sites Web de jeux, des sites Web de réseaux sociaux ou des sites Web de contenu pour adultes.
- Filtrage DNS : ce type de filtrage bloque l'accès à des sites Web en modifiant les paramètres DNS de l'utilisateur. Lorsqu'un utilisateur tente d'accéder à un site Web bloqué, il est redirigé vers une page d'erreur.
- Filtrage de mots-clés : ce type de filtrage bloque l'accès à des sites Web ou à du contenu qui contiennent des mots-clés spécifiques. Il peut être utilisé pour bloquer du contenu offensant ou du contenu qui n'est pas approprié pour certains publics.
- Filtrage comportemental : ce type de filtrage surveille le comportement de l'utilisateur sur le Web et bloque l'accès à des sites Web ou à du contenu qui sont considérés comme dangereux ou nuisibles. Il peut être utilisé pour protéger les enfants des contenus dangereux ou pour empêcher les utilisateurs d'accéder à des sites Web qui pourraient contenir des logiciels malveillants.[18]

4.2 Méthodes de filtrage web

Il existe plusieurs méthodes de filtrage web, notamment :

- Le filtrage au niveau du réseau : Le filtrage au niveau du réseau est effectué par un appareil de réseau, tel qu'un pare-feu ou un routeur.
- Le filtrage au niveau du serveur : Le filtrage au niveau du serveur est effectué par un serveur, tel qu'un serveur proxy ou un serveur DNS.
- Le filtrage au niveau du client : Le filtrage au niveau du client est effectué par un logiciel installé sur l'appareil de l'utilisateur.

4.3 Avantages du filtrage web

Le filtrage web offre plusieurs avantages, notamment :

- Protection des utilisateurs : Le filtrage web peut aider à protéger les utilisateurs contre le contenu inapproprié ou dangereux, tel que le contenu nuisible, le contenu violent ou le contenu à caractère sexuel.
- Amélioration de la productivité : Le filtrage web peut aider à améliorer la productivité des employés en bloquant l'accès à des sites Web non pertinents.
- Réponse aux exigences réglementaires : Le filtrage web peut aider à répondre aux exigences réglementaires de l'institution, la famille, Etc.

4.4 Inconvénients du filtrage web

Le filtrage web présente également quelques inconvénients, notamment :

- Limitation de la liberté d'expression : Le filtrage web peut limiter la liberté d'expression des utilisateurs en bloquant l'accès à certains sites Web.
- Erreurs de filtrage : Le filtrage web peut bloquer des sites Web qui ne devraient pas être bloqués.
- Coût : Le filtrage web peut être coûteux à mettre en œuvre et à maintenir.[19]

4.5 Exemples de filtrage web

Le filtrage web est utilisé dans une variété de contextes, notamment :

- **Les entreprises** : Les entreprises utilisent le filtrage web pour protéger leurs employés contre le contenu inapproprié ou dangereux et pour améliorer la productivité.
- **Les écoles** : Les écoles utilisent le filtrage web pour protéger les étudiants contre le contenu inapproprié ou dangereux.
- **Les bibliothèques** : Les bibliothèques utilisent le filtrage web pour protéger les utilisateurs contre le contenu inapproprié ou dangereux.
- **Les gouvernements** : Les gouvernements utilisent le filtrage web pour répondre aux exigences réglementaires et pour protéger la sécurité nationale.[20]

5 Optimisation Du Réseau Informatique Universitaire

La mise en cache est un processus qui consiste à stocker des copies de données dans un endroit accessible rapidement afin de pouvoir les récupérer plus facilement à l'avenir. En informatique, la mise en cache est souvent utilisée pour améliorer les performances des applications et des systèmes. Par exemple, un navigateur Web peut mettre en cache des pages Web afin de ne pas avoir à les télécharger à nouveau à chaque fois que l'utilisateur les visite. Un serveur Web peut également mettre en cache les fichiers statiques, tels que les images et les scripts, afin de réduire la charge sur le serveur.

La mise en cache peut être utilisée à différents niveaux d'un système informatique. Elle peut être effectuée au niveau du client, du serveur ou d'un réseau.

Mise en cache au niveau du client

La mise en cache au niveau du client est la mise en cache la plus courante. Elle consiste à stocker des copies de données sur l'appareil de l'utilisateur. Par exemple, un navigateur Web stocke les pages Web que l'utilisateur a visitées dans son cache.

Mise en cache au niveau du serveur

La mise en cache au niveau du serveur consiste à stocker des copies de données sur le serveur. Par exemple, un serveur Web peut mettre en cache les fichiers statiques, tels que les images et les scripts.

Mise en cache au niveau du réseau

La mise en cache au niveau du réseau consiste à stocker des copies de données sur un réseau. Par exemple, un réseau de diffusion de contenu (CDN) peut mettre en cache les pages Web sur des serveurs situés à proximité des utilisateurs.[21]

5.1 Avantages de la mise en cache

La mise en cache offre plusieurs avantages, notamment :

- Amélioration des performances : La mise en cache permet de réduire le temps nécessaire pour accéder aux données.
- Réduction de la charge sur les serveurs : La mise en cache permet de réduire la charge sur les serveurs en leur évitant de devoir répondre aux mêmes requêtes plusieurs fois.
- Amélioration de la disponibilité : La mise en cache peut aider à améliorer la disponibilité des données en cas de panne du serveur d'origine.

5.2 Inconvénients de la mise en cache

La mise en cache présente également quelques inconvénients, notamment :

- Augmentation de la complexité : La mise en cache peut augmenter la complexité d'un système en ajoutant des mécanismes de gestion du cache.
- Risque de corruption : Les données mises en cache peuvent être corrompues si le cache est endommagé ou corrompu.
- Baisse de la sécurité : La mise en cache peut réduire la sécurité d'un système en rendant les données accessibles à des utilisateurs non autorisés.[22]

6 Méthodologie

Pour réaliser cet article nous avons utilisé premièrement la recherche appliquée qui consiste à comprendre le contexte d'un problème ou pour identifier les besoins non satisfaits, de résoudre des problèmes concrets et de répondre aux besoins des utilisateurs. (Améliorer les performances d'un système ou d'un processus). Deuxièmement une étude comparative des pratiques de filtrages web qui existe afin d'acquérir une idée approfondie à notre sujet.

À ces méthodes de recherche nous y associons la technique d'observation à laquelle nous avons observé les comportements des étudiants en utilisant l'internet.

7 Présentation de l'existant

L'analyse de l'existant est une étape importante de tout projet, que ce soit un projet de recherche, de développement ou de changement. Elle consiste à étudier les systèmes, les processus et les technologies existants afin de comprendre leurs forces et leurs faiblesses.

7.1 Topologie réseau

Elle décrit comment les nœuds sont connectés entre eux, en utilisant des câbles, des ondes radio ou d'autres moyens.

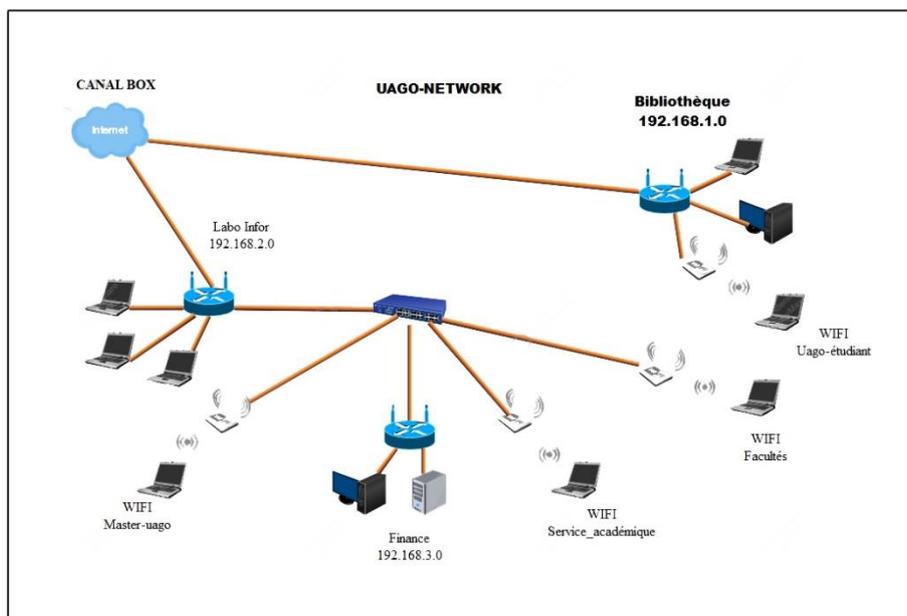


Figure 3: Topologie réseau

8 Resultats

Dans le cadre de filtrage web dans un réseau informatique universitaire, vue la tendance que prennent l'utilisation de l'internet en grande partie les réseaux sociaux (Facebook et YouTube), qui crée une perte de temps pour les étudiants ; notre filtrage tient part à bloquer certains sites web pendant les heures de cours disons dans l'intervalle de 7h30 à 17h00 et cela dans 300Jours équivalant à l'année universitaire de 10 mois.

Nous avons utilisé Pfsense qui est un pare-feu open source avec l'aide de Squid (un serveur proxy) et de SquidGuard (le filtre web).

Squid : Squid est un proxy de cache pour le Web prenant en charge HTTP, HTTPS, FTP Squid optimise le flux de données entre le client et le serveur pour améliorer les performances.

Squidguard : SquidGuard est un logiciel de redirection d'URL, qui peut être utilisé pour le contrôle du contenu des sites Web auxquels les utilisateurs peuvent accéder. Il est écrit en tant que plug-in pour Squid et utilise des listes noires pour définir les sites pour lesquels l'accès est redirigé.

Topologie réseau

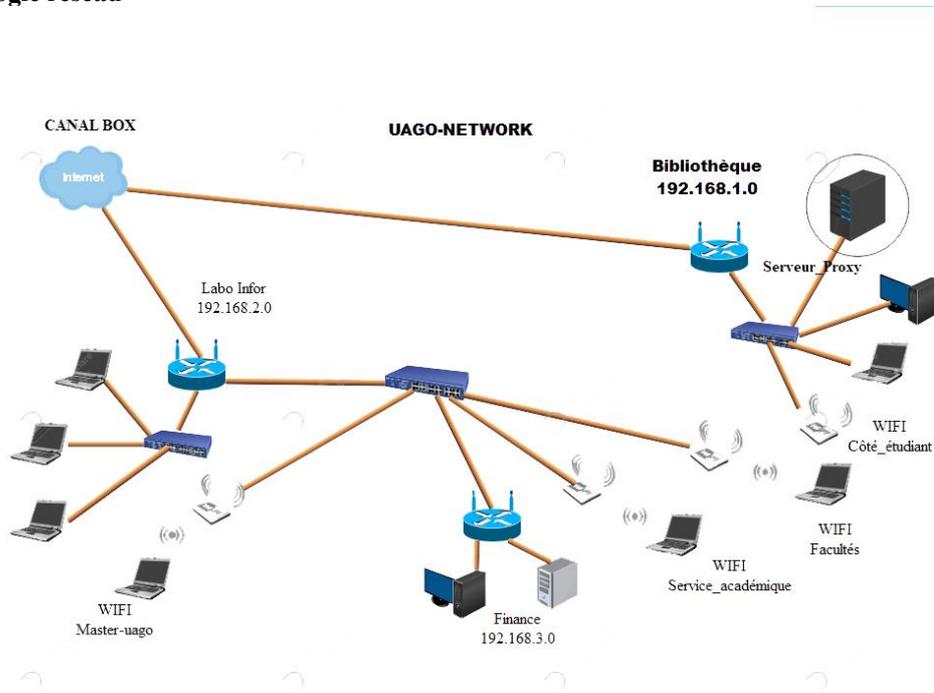


Figure 4: Topologie future

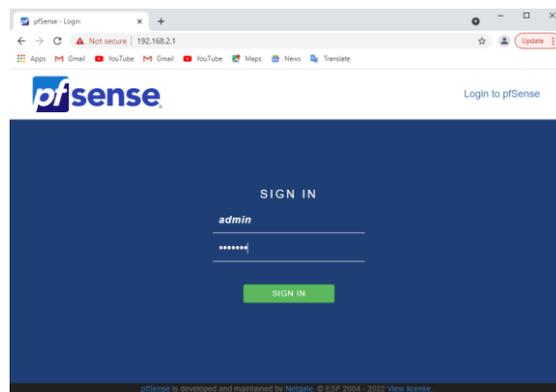


Figure 5: Présentation pfsense

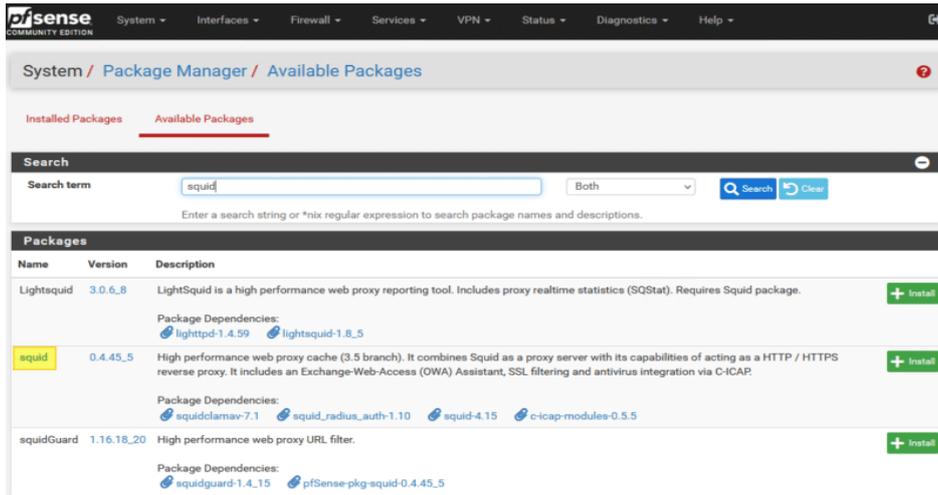


Figure 6: Installation squid

Mise en cache

Etant donné que notre proxy va aussi faire des copies de sites web pour faciliter la navigation, nous allons procéder à octroyer une capacité de stockages de 1Go et définir l'emplacement de notre cache.

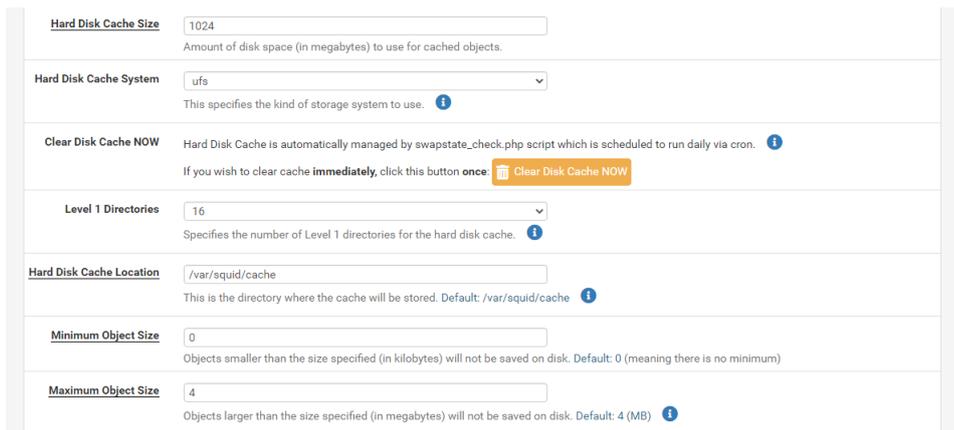


Figure 7: Mise en cache

Présentation de filtrage

Dans la liste noire des sites non autorisé nous avons Facebook et YouTube.

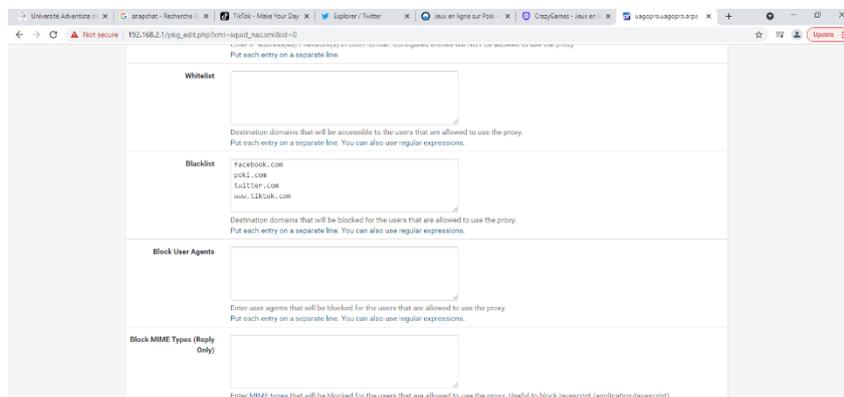


Figure 8: Listes noir des sites

Et quand nous essayons de visiter les sites www.uago.ac.cd. ça donne :

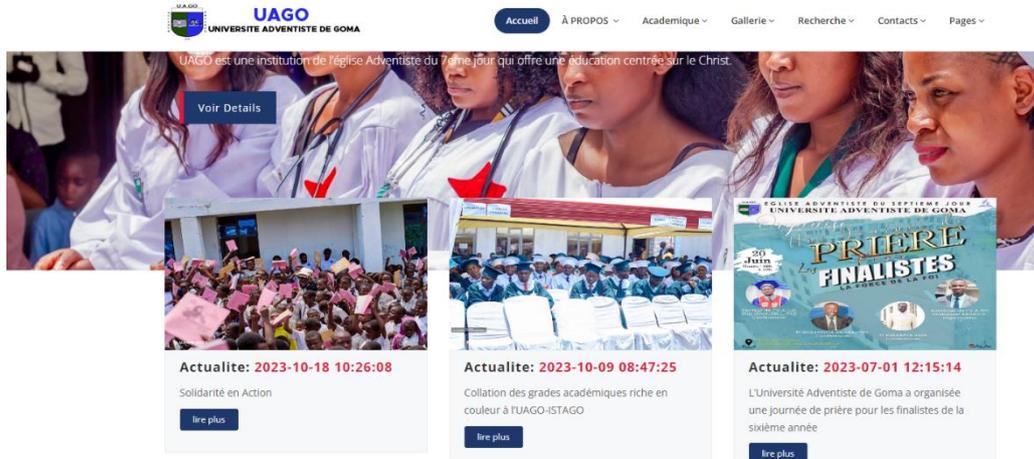


Figure 9: Site autorisé

Et quand nous essayons de visiter les sites www.facebook.com ça donne :

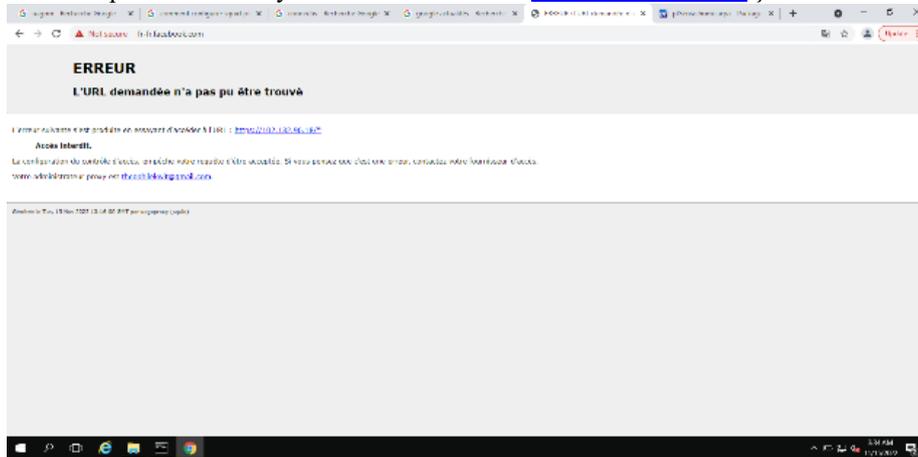


Figure 10: Site non autorisé

9 Matériels

Pour Réaliser Ce Travail, Il Faudra Avoir Un Ordinateur Portable, Avec Le Système D'exploitation Win10, Un Logiciel De Virtualisation (Virtualbox), Pfsense Et Une Connexion Internet Pour Installer Squid.

10 Conclusion

Le filtrage web est un outil puissant qui peut être utilisé pour protéger les utilisateurs aux ressources malveillantes présentes sur l'internet et répondre aux exigences réglementaires de l'institution. En intégrant un serveur mandataire proxy l'institution optimise la consommation de la bande passe et le contrôle total de l'utilisation des ressources de l'internet, la mise en cache jouera un grand rôle comme outil qui peut être utilisé pour améliorer les performances, la disponibilité et garantir un certain niveau de sécurité.

11 Recommandations

Notre recommandation s'adresse à l'Université Adventiste de Goma de pouvoir adopter ce système de filtrage web dans leur réseau informatique, mais aussi aux futurs chercheurs de pouvoir prendre par de la partie sécurité.

REFERENCES

- [1] A. Patard, « Étude sur l'usage d'Internet et des réseaux sociaux dans le monde en 2020 », BDM. Consulté le: 19 octobre 2023. [En ligne]. Disponible sur: <https://www.blogdumoderateur.com/internet-reseaux-sociaux-2020/>
- [2] M. R. Dahimene, « Filtrage et Recommandation sur les Réseaux Sociaux ».
- [3] H. Oufaida et O. Nouali, « Le filtrage collaboratif et le web 2.0. Etat de l'art », *Doc. Numér.*, vol. 11, n° 1-2, p. 13-35, 2008.
- [4] Valérie Schafer, « ARPANET, toute une histoire... », *Bull. 1024*, n° 16, p. 17-32, nov. 2020, doi: 10.48556/SIF.1024.16.17.
- [5] kellytourvieille, « LES DERNIERS CHIFFRES DU NUMÉRIQUE - JUILLET 2023 », We Are Social France. Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://wearesocial.com/fr/blog/2023/07/les-derniers-chiffres-du-numerique-juillet-2023/>
- [6] « Universalité de l'Internet, quelle approche pour la RDC - Ministre du Numérique RD Congo », Ministère du Numérique RD Congo. Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://numerique.gouv.cd/actualites/universalite-de-l%27internet-quelle-approche-pour-la-rdc-pdi12c>
- [7] A. Abdullatif, « Les pratiques numériques des étudiants de l'Université des Comores dans le processus d'apprentissage ».
- [8] « Opinion | Les réseaux sociaux libèrent la parole de la jeunesse ! | Les Echos ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://www.lesechos.fr/idees-debats/cercle/opinion-les-reseaux-sociaux-liberent-la-parole-de-la-jeunesse-959946>
- [9] « Réseaux sociaux : enjeux, méthodes, perspectives ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://calenda.org/198422>
- [10] J. Hunsinger et T. M. Senft, Éd., *The social media handbook*. New York: Routledge, 2014.
- [11] « M133_D1_HTTP_Introduction.pdf ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: https://www.epai-ict.ch/ict-modules/assets/M133_D1_HTTP_Introduction.pdf
- [12] « Http3-explained-fr.pdf ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://upload.wikimedia.org/wikipedia/commons/0/00/Http3-explained-fr.pdf>
- [13] « 201809_http2_explained_fr.pdf ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: https://lafibre.info/images/ssl/201809_http2_explained_fr.pdf
- [14] H. Melhem, « Usages et applications du web sémantique en bibliothèques numériques ».
- [15] « 1992 - Institut national de recherche en informatique et .pdf ». Consulté le: 19 octobre 2023. [En ligne]. Disponible sur: <https://inria.hal.science/inria-00073272v1/document>
- [16] « Qu'est-ce qu'un serveur Proxy et comment fonctionne-t-il ? | Varonis ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://www.varonis.com/fr/blog/serveur-proxy>
- [17] « 34288173.pdf ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://www.alainbensoussan.com/wp-content/uploads/2017/05/34288173.pdf>
- [18] « Filtrage_d_Internet_et_démocratie - Résumé Principal_1.pdf ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: https://www.laquadrature.net/files/Filtrage_d_Internet_et_d%C3%A9mocratie%20-%20R%C3%A9sum%C3%A9%20Principal_1.pdf
- [19] « Brochure-filtrage-des-sites-internet.pdf ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://www.connectdata.fr/wp-content/uploads/2020/02/Brochure-filtrage-des-sites-internet.pdf>
- [20] « psense-filtrage-https.pdf ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://lacroixwerley.files.wordpress.com/2018/11/psense-filtrage-https.pdf>
- [21] « mise-en-cache-intelligente-avec-django.pdf ». Consulté le: 20 octobre 2023. [En ligne]. Disponible sur: <https://zestedesavoir.com/tutoriels/pdf/1295/mise-en-cache-intelligente-avec-django.pdf>
- [22] G. Alaoui, « Système d'adaptation basé sur la personnalisation de contenu Web mobile ».