RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
http://www.ifri-uac.bj Courriel : contact@ifri-uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Systèmes d'Information et Réseaux Informatiques

Présenté par :
Tychique **AVALLA**

Utilisation de Pfsense pour l'implémentation d'un portail captif avec authentification radius dans une entreprise.

Sous la supervision :
Ing. Francky **ADEOSSI**

Membres du jury :

Année Académique : **2020-2021**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux vii

Liste des acronymes viii

Glossaire 1

Introduction 2

1 Revue de littérature 4

2 Solution et choix techniques 15

3 Mise en œuvre du réseau, résultats et discussions 29

Conclusion générale et perspectives 36

Bibliographie 37

Webographie 38

Table des matières 40

Dédicace

A
Mon père Paul AVALLA
Ma mère Françoise HOUETON
Mon frère Chrispus AVALLA

Remerciements

Nous remercions Dieu tout puissant pour toutes ses grâces et de nous avoir accompagné jusqu'au bout de ce cycle sans douter de notre potentiel.

Nous exprimons notre vive gratitude aux personnes physiques qui ont contribué à rendre meilleur notre travail et formation, notamment :

- Eugène C. EZIN, Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI UAC) pour ses conseils et pour cette formation accordée ;
- Dr Gaston EDAH, Directeur Adjoint de l'IFRI pour son suivi et sa disponibilité à nous accompagner durant toute la formation ;
- M. Francky ADEOSSI, Ingénieur en Audit Informatique et mon maître de mémoire ;
- Ma famille, pour leur soutien et l'amour qu'ils portent à mon égard ;
- Tous les enseignants de notre institut pour avoir accepté partager une partie de leurs connaissances avec nous ;
- Nos parents, proches et amis qui nous ont soutenus de près ou de loin tout au long de ce travail.

Résumé

Les problèmes de sécurité sont fréquemment présents dans les réseaux informatiques en raison de l'expansion et de la connectivité des utilisateurs. Les administrateurs doivent cependant prendre toutes les précautions nécessaires pour maintenir la sécurité et la confidentialité des informations des utilisateurs. Les objectifs de la sécurité informatique, y compris la confidentialité des données internes sur Internet, doivent être pleinement atteints dans les réseaux câblés et sans fil. Ainsi, dans notre système réseau, pour palier à ces menaces, les administrateurs peuvent mettre en place un portail captif avec authentification RADIUS en utilisant l'outil Pfsense. Ce dispositif permet de restreindre l'accès au réseau en obligeant les utilisateurs à s'authentifier avant de pouvoir accéder aux ressources. L'authentification RADIUS offre une sécurité accrue en utilisant des identifiants uniques pour chaque utilisateur et en évitant l'utilisation de mots de passe partagés. Ainsi, les administrateurs peuvent garantir la confidentialité des données internes sur Internet tout en permettant aux utilisateurs d'accéder aux ressources dont ils ont besoin pour leur travail. En utilisant cette méthode, les administrateurs peuvent s'assurer que seuls les utilisateurs autorisés ont accès au réseau. Aussi, des politiques de sécurité peuvent être établies pour régir les actions des utilisateurs, tandis que les activités du réseau peuvent être surveillées pour détecter tout comportement inhabituel.

Mots clés : RADIUS, authentification, pfsense, sécurité informatique, confidentialité, réseau informatique.

Abstract

Security issues are frequently present in computer networks due to the expansion and connectivity of users. However, administrators must take every precaution to maintain the security and privacy of user information. The objectives of computer security, including the confidentiality of internal data on the Internet, must be fully met in both wired and wireless networks. Thus, in our network system, to address these threats, administrators can implement a captive portal with RADIUS authentication using the Pfsense tool. This device allows restricting access to the network by forcing users to authenticate themselves before they can access resources. RADIUS authentication provides increased security by using unique credentials for each user and avoiding the use of shared passwords. In this way, administrators can ensure the confidentiality of internal data over the Internet while allowing users to access the resources they need to do their jobs. By using this method, administrators can ensure that only authorized users have access to the network. Also, security policies can be established to govern user actions, while network activity can be monitored for unusual behavior.

Keywords: RADIUS, authentication, pfsense, computer security, privacy, computer network

Table des figures

1.1 Exemple de réseau informatique[10] . . . 5
1.2 Architecture d'internet[11] . . . 6
1.3 Principaux éléments du NAC[15] . . . 9
1.4 Fonctionnement de RADIUS . . . 11
1.5 Éléments constitutifs d'un portail captif . . . 12
1.6 Modèle catch and release . . . 13

2.1 Architecture du réseau . . . 19
2.2 Création du NAT . . . 20
2.3 Création de Host-Only Network . . . 20
2.4 Shell et configuration pfsense . . . 21
2.5 Interface WEB de pfsense . . . 22
2.6 Tableau de bord de pfsense . . . 22
2.7 Package FreeRadius . . . 23
2.8 Serveur DHCP . . . 24
2.9 Alias . . . 24
2.10 Les règles . . . 25
2.11 Configuration des clients . . . 26
2.12 Ajout des utilisateurs . . . 26
2.13 Serveur RADIUS . . . 27
2.14 Portail Captif . . . 28

3.1 Ping vers l'adresse de Google . . . 29
3.2 Login Page . . . 30
3.3 Test de ping . . . 31
3.4 Redirection vers Bing . . . 31
3.5 Utilisateur "Agent" . . . 32
3.6 Connexion de l'utilisateur . . . 32
3.7 Statut du portail captif . . . 33
3.8 Accès des fichiers . . . 33
3.9 Configuration de Squid . . . 34
3.10 Bloquer les sites . . . 34
3.11 Interface d'un site bloquer . . . 34

Liste des tableaux

2.1 Tableau de comparaison des différentes solutions 18

Liste des acronymes

ALCASAR :

Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau 16

AR :

Access Requestor 9

CD :

Compact Disc 16

DCN :

Data Communication Network 4

DHCP :

Dynamic Host Configuration Protocol 12

DNS :

Domain Name System 12

HTTP :

Hypertext transfer protocol 11

HTTPS :

Hypertext transfer protocol Secure 16

LDAP :

Lightweight Directory Access Protocol 10

NAC :

Network Access Control 8

NAS :

Network Access Server 10

RADIUS :

Remote Authentication Dial-In User Service iv, v, 10

RPM :

Red Hat Package Manager 18

SSH :

Secure Shell 16

TCP/IP :

Transmission Control Protocol/Internet Protocol 6

URL :

Uniform Resource Locator 13

VPN :

Virtual Private Network 8

WISP :

Wireless Internet Service Provider roaming 16

WPA :

Wifi Protected Access 16

Glossaire

FreeBSD : FreeBSD est un système d'exploitation utilisé pour les serveurs modernes, les ordinateurs de bureau et les plates-formes embarquées. Une large communauté l'a continuellement développé depuis plus de trente ans. Ses fonctionnalités avancées en matière de réseau, de sécurité et de stockage ont fait de FreeBSD la plateforme de choix pour la plupart des sites web les plus fréquentés et des périphériques de réseau et de stockage embarqués les plus répandus. 16

Open Source : Open Source est un code source qui est rendu librement disponible pour une éventuelle modification et redistribution. 15

Introduction Générale

Le réseau de l'entreprise met en œuvre des données sensibles en les stockant, les partageant en interne et les communiquant parfois à d'autres individus. Cette ouverture vers l'extérieur est une condition préalable pour gagner en productivité et en compétitivité. Il est donc impossible de renoncer aux bénéfices de l'informatisation, d'isoler le réseau de l'extérieur ou de risquer la confidentialité des données de l'entreprise. Les données sensibles de l'entreprise sont vulnérables aux attaques malveillantes, qui évoluent constamment en termes de nature et de méthodes d'intrusion. La sécurité des systèmes d'information représente une préoccupation majeure nécessitant la mise en œuvre d'une gamme variée d'outils et de mécanismes de sécurité informatique. Parmi ces mécanismes, on peut distinguer les solutions de sécurité comme les systèmes de prévention tels que l'authentification, dont l'objectif est de prouver l'identité des utilisateurs, le contrôle d'accès qui consiste à définir les droits accordés aux utilisateurs sur les données et les pares-feux dont le rôle est de filtrer l'accès aux services du système d'information par rapport au monde extérieur.

0.1 Contexte et justification

Dans les milieux professionnels, la grande majorité des employés utilisent Internet. Cette forte demande pour les technologies de l'information et de la communication (TIC) entraîne une nécessité croissante d'élargir l'offre de services Internet. En effet, de nombreux utilisateurs possèdent désormais un appareil mobile tel qu'un ordinateur portable ou un smartphone, et ils souhaitent pouvoir accéder à Internet dans la plupart des endroits qu'ils fréquentent. L'essor rapide des points d'accès sans fil pour répondre aux besoins de connexion des appareils nomades a conduit à une diversification des politiques d'accès à Internet propres à chaque réseau. Toutefois, chaque réseau cherche à limiter l'accès uniquement aux utilisateurs autorisés. Pour répondre à ce défi, il est impératif de déployer un système d'authentification unifié, applicable à tous les modes d'accès (sans fil ou filaire), afin de contrôler l'accès à ces réseaux de manière efficace. La mise en place d'une telle solution fera l'objet de notre étude intitulé '' Utilisation de Pfsense pour l'implémentation d'un portail captif avec authentification radius dans une entreprise"

0.2 Problématique

Les systèmes informatiques sont constamment exposés à de nouvelles vulnérabilités et failles, tandis que les risques d'attaques à distance augmentent également en raison de la connexion permanente des réseaux à Internet. Actuellement, les pares-feux permettent de réduire partiellement ces risques. Outre la mise en place de ces derniers, il est nécessaire, pour renforcer cette sécurité, d'installer une

infrastructure sécurisée d'accès internet qui garantira un accès sécurisé à internet pour les utilisateurs autorisés tout en limitant l'accès aux utilisateurs non autorisés, en protégeant les données et les communications et en respectant les réglementations et normes en vigueur en matière de sécurité de l'information.

0.3 Objectif

L'objectif principal de ce travail est de mettre en place un contrôle d'accès à internet sécurisé dans un réseau en utilisant l'outil pfsense avec quelques de ses fonctionnalités. Il s'agit de :

- Émuler un réseau fonctionnel et configurer les éléments d'infrastructure ;
- Installer pfsense dans le réseau ;
- Configurer le portail captif avec le serveur RADIUS ;
- Authentifier tous les utilisateurs du réseau avant leur accès à internet ;

0.4 Organisation du travail

Notre travail est structuré en trois chapitres. Après la revue de littérature nous présentons la solution et les choix techniques puis les résultats et les discussions de notre projet. Dans la conclusion nous proposons quelques perspectives afin d'améliorer notre système.

Chapitre 1

Revue de littérature

Introduction

Dans ce chapitre, nous expliquons les notions essentielles liées à la sécurité informatique ainsi qu'aux contrôles d'accès dans un réseau d'entreprise.

1.1 Sécurité Informatique

La sécurité informatique englobe toutes les mesures prises pour minimiser la vulnérabilité d'un système face aux menaces, qu'elles soient accidentelles ou intentionnelles. Il est essentiel d'identifier les exigences fondamentales en matière de sécurité informatique. Ces exigences définissent les attentes des utilisateurs en termes de sécurité des systèmes informatiques :

- **Disponibilité** : demande que l'information système soit accessible uniquement aux personnes autorisées.
- **Confidentialité** : demande que l'information système soit uniquement lue par les personnes autorisées.
- **Intégrité** : demande que l'information système soit uniquement modifiée par les personnes autorisées.

En matière de sécurité informatique, une menace désigne une atteinte potentielle à la sécurité, qu'elle soit causée de manière accidentelle, intentionnelle (sous forme d'attaque), ou qu'elle se manifeste de manière active ou passive. [4]

1.2 Réseau Informatique

Un réseau informatique, également connu sous le nom de réseau de communication de données DCN en anglais, désigne un ensemble de dispositifs matériels et logiciels interconnectés qui permettent l'échange d'informations et le partage de ressources. Cette interconnexion peut se faire via des liaisons filaires ou sans fil. Un réseau basique peut consister en deux ordinateurs connectés par un câble, formant ce qu'on appelle une configuration pair à pair (P2P), où il n'y a pas de hiérarchie

entre les participants : chacun a un accès aux données de l'autre et peut partager des ressources telles qu'un espace de stockage, des programmes ou des périphériques comme une imprimante.

Les réseaux modernes sont généralement beaucoup plus complexes et intègrent un large éventail d'outils informatiques, bien au-delà de la simple connexion de deux ordinateurs. Pour les systèmes impliquant plus de dix participants, une configuration client-serveur est souvent utilisée. Dans ce modèle, un ordinateur agit comme un serveur central, mettant ses ressources à disposition des autres participants, appelés clients. [9]

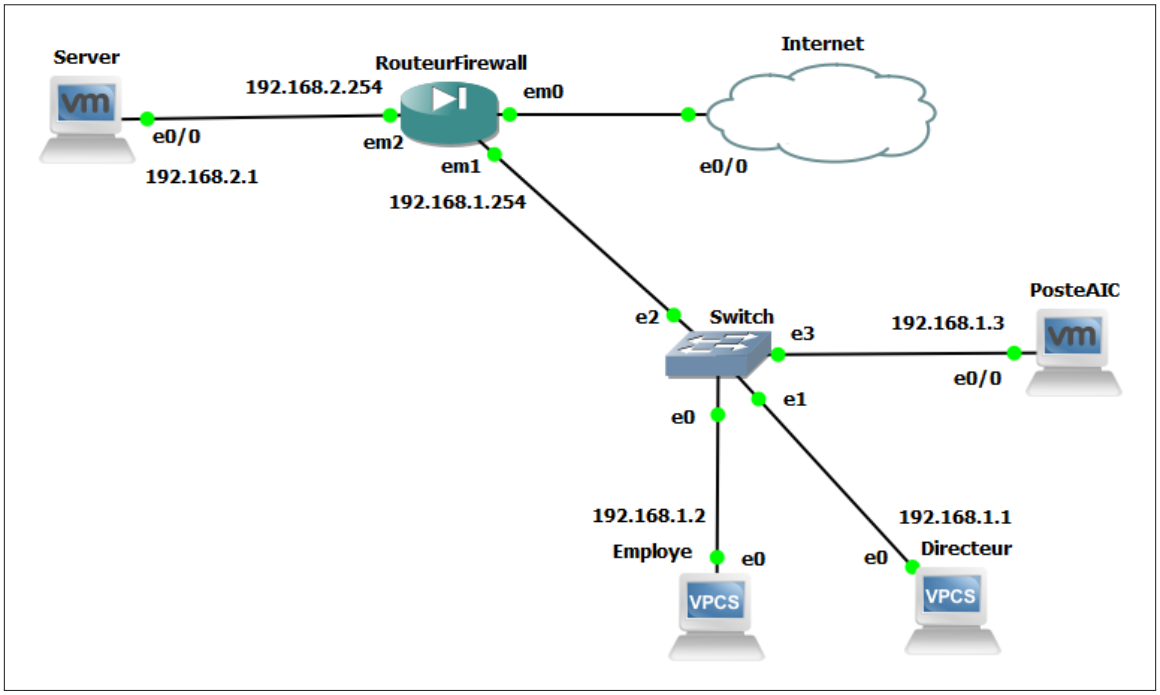


FIGURE 1.1 : Exemple de réseau informatique[10]

1.2.1 Les types de réseaux

Il existe divers types de réseaux, qui se différencient par leur taille, leur débit de transfert de données et la distance maximale entre les points les plus éloignés.

- **Le PAN** ou Personal Area Network connecte sur quelques mètres différents équipements personnels appartenant à un même utilisateur. (Exemples : la technologie Bluetooth ou le service Wi-Fi ad hoc)
- **Le LAN** ou Local Area Network est couramment utilisé au sein des entreprises. Il permet de connecter les machines et tous les dispositifs utilisés par l'entreprise.
- **Le MAN** ou Metropolitan Area Network interconnecte les ordinateurs situés dans une même zone géographique. Il regroupe ainsi plusieurs réseaux locaux.
- **Le WAN** ou Wide Area Network est constitué d'une collection de LAN et de MAN, et peut donc s'étendre à l'échelle nationale voire internationale.
- **Le SAN** ou Storage Area Network : il est conçu pour des performances élevées, principalement dédié au transfert de données entre des serveurs informatiques et des ressources spécifiquement dédiées au stockage.

Il convient de noter que ces divers types de réseaux se chevauchent partiellement. L'utilisateur d'un WLAN (Wireless Local Area Network) est simultanément inclus dans un WAN ou un GAN (Global Area Network) dès lors qu'il est connecté à Internet. [8]

1.3 Internet

Internet, provenant de l'expression anglaise "International Network", est un réseau mondial d'ordinateurs. En effet, Internet est composé de millions de réseaux d'ordinateurs connectés les uns aux autres par le biais de systèmes appelés routeurs, qui acheminent l'information. Un réseau d'ordinateurs est un ensemble d'ordinateurs et de matériels informatiques interconnectés afin de partager des informations et des ressources, grâce à un ordinateur central appelé serveur, qui fournit des services à d'autres ordinateurs. [7]

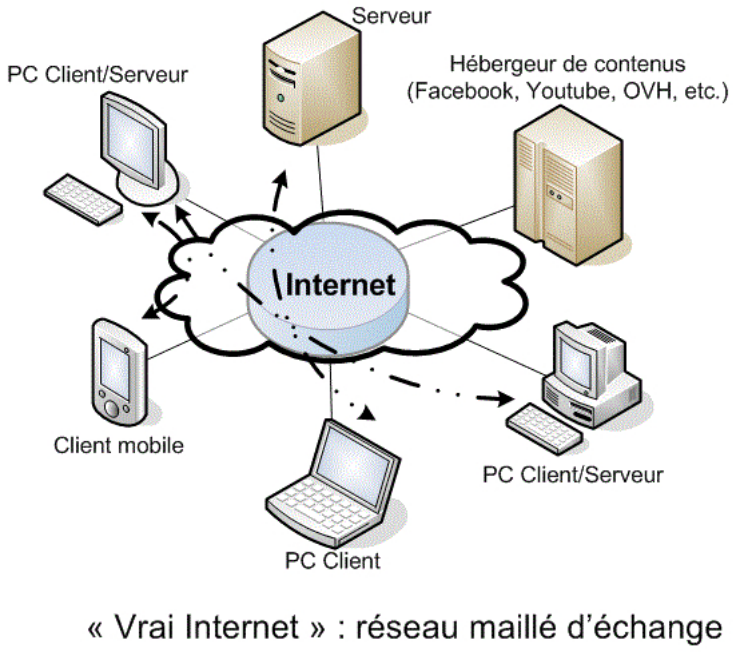


FIGURE 1.2 : Architecture d'internet[11]

1.3.1 Mode de fonctionnement d'Internet

Pour faciliter l'échange d'informations entre des ordinateurs situés dans différents endroits du monde, quatre éléments essentiels sont nécessaires :

- L'adressage IP,
- Les fournisseurs d'accès à Internet,
- Le protocole de communication entre ordinateurs TCP/IP,
- Les routeurs, qui acheminent l'information.

Pour que les données puissent être transférées d'un ordinateur à un autre, il est indispensable que les deux ordinateurs puissent se localiser mutuellement. Cela est rendu possible grâce au système

d'adressage IP. Chaque ordinateur connecté à Internet dispose d'une adresse unique, appelée adresse IP (Internet Protocol), présentée sous forme de numéros.

Les adresses IP sont attribuées par des organismes, tels que Skynet, Belnet, Win, etc., communément appelés fournisseurs d'accès ou providers. Ces entités, via leurs serveurs, proposent divers services aux utilisateurs, dont l'accès à Internet, qui est fourni à travers un numéro spécifique.

Le système TCP/IP assure la transmission des données entre les ordinateurs selon un modèle de requête/réponse, garantissant ainsi que les données parviennent à destination sans être altérées. Concrètement, lorsque qu'un ordinateur envoie un message à un autre, le protocole de communication TCP/IP segmente l'information en petits paquets de données de 1024 caractères ou octets, puis les encode de manière universelle pour tous les ordinateurs et routeurs d'Internet. Chaque paquet contient des informations sur son origine et sa destination. Ces paquets sont ensuite transportés via divers moyens tels que des câbles, des lignes téléphoniques, des satellites, etc., jusqu'à l'ordinateur de destination. Une fois là-bas, les paquets sont réassemblés pour reconstituer le message initial.

Pour que les ordinateurs d'un réseau puissent communiquer avec ceux d'un autre réseau et échanger des informations, un autre élément essentiel appelé "routeur" est nécessaire. Ces routeurs, des dispositifs compacts contenant les chemins d'accès vers d'autres routeurs, sont des points d'ancrage essentiels sur Internet. Leur rôle principal est de diriger le trafic d'information sur Internet.[7]

1.3.2 Infrastructure d'accès internet sécurisée

Une infrastructure informatique désigne l'ensemble des éléments nécessaires au fonctionnement et à la gestion des environnements informatiques d'une entreprise. Elle englobe les composants matériels, logiciels et réseau, ainsi qu'un système d'exploitation et un système de stockage de données utilisés pour fournir des services et des solutions informatiques. Ces produits peuvent être des applications téléchargeables s'exécutant sur les ressources informatiques existantes ou des solutions en ligne proposées par des prestataires de services.

Une infrastructure d'accès Internet sécurisée, quant à elle, se compose d'un ensemble de technologies, de protocoles et de procédures visant à protéger les données et les communications transitant sur un réseau informatique. [12]

1.4 Sécurité réseau

La sécurité d'un réseau consiste en un ensemble de politiques et de pratiques adoptées pour prévenir et surveiller l'accès non autorisé, la modification abusive ou le refus d'accès à un réseau informatique et à ses ressources. Elle englobe également la protection des transactions et des communications entre les entreprises, les agences gouvernementales et les particuliers. Les réseaux peuvent être privés, tels que ceux au sein d'une entreprise, ou ouverts à un accès public, et la sécurité est essentielle dans les deux cas. La sécurisation d'un réseau d'entreprise implique également le choix de solutions et de technologies appropriées, ainsi que leur maintenance régulière. Cela englobe tout, de l'infrastructure aux protocoles, de la structure aux ressources informatiques et aux systèmes de sauvegarde. Tous ces éléments contribuent à la robustesse et à la performance des opérations, et jouent un rôle crucial dans l'optimisation de la sécurité du système. Voici quelques-uns des différents types de sécurité réseau :

- Les pares-feux ;
- Antivirus / Antimalware ;
- Segmentation du réseau ;
- Contrôle d'accès ;
- Sécurité des applications ;
- Détection de la prévention des intrusions ;
- Sécurité sans fil ;
- Sécurité Web ;
- VPN ;

1.5 Le contrôle d'accès

Le contrôle d'accès réseau NAC est une solution de sécurité qui utilise un ensemble de protocoles pour empêcher les utilisateurs et les périphériques non autorisés d'accéder à un réseau privé ou pour donner un accès restreint aux périphériques conformes aux politiques de sécurité réseau. Il est également connu sous le nom de contrôle d'admission réseau. Il gère la gestion et la sécurité du réseau qui implémente la politique de sécurité, la conformité et la gestion du contrôle d'accès à un réseau.

NAC fonctionne sur les réseaux filaires et sans fil en identifiant les différents périphériques connectés au réseau. Pour la configuration d'une solution de sécurité réseau NAC, les administrateurs détermineront les protocoles qui décideront comment les périphériques et les utilisateurs sont autorisés pour le bon niveau d'autorisation. Les règles d'accès sont généralement basées sur des critères tels que l'appareil utilisé, l'emplacement à partir duquel on accède, les droits d'accès des différentes personnes, ainsi que les données et ressources spécifiques auxquelles on accède. [14]

1.5.1 Principaux éléments du NAC (Network Access Control)

Il y a principalement trois éléments principaux du NAC qui sont :

1. Access Requestor (AR) ;
2. Serveurs de stratégies ;
3. Network Access Server (NAS).

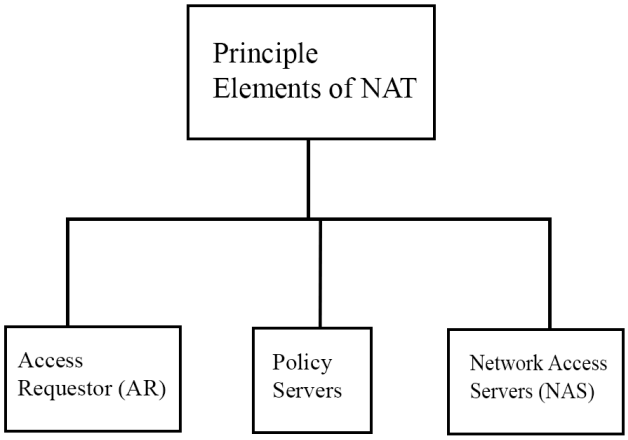


FIGURE 1.3 : Principaux éléments du NAC[15]

1. **Access Requestor (AR)**

   Nous pouvons déterminer à partir du nom qu'il s'agit d'une personne qui tente d'obtenir l'accès en le demandant. Cet accès peut être accordé à n'importe quelle entité, telle qu'un appareil, une personne ou un processus. Cette entité tente d'accéder aux ressources réseau. Il peut s'agir de n'importe quel périphérique géré par le système NAC, tel que des serveurs, des caméras, des imprimantes et d'autres périphériques IP. Les AR sont également connus sous le nom de suppliants ou de clients à certains moments. Les AR garantissent qu'aucune entité n'a un accès illégal aux ressources protégées.
   Pour y avoir accès, ces derniers doivent respecter les lignes directrices ou les politiques spécifiques de l'organisation.

2. **Serveur de stratégie**

   Le serveur de stratégie analyse quel accès doit être fourni à l'AR en fonction de l'identité de l'AR, du niveau de permission, de la tentative de demande et de la politique d'accès établie par l'organisation.
   Le serveur de stratégies s'appuie fréquemment sur des services principaux, tels qu'un antivirus, la gestion des correctifs ou un répertoire utilisateur pour fonctionner.
   Le serveur de stratégies permet de déterminer l'état de l'hôte. Une organisation crée différentes stratégies d'accès pour autoriser ou rejeter clairement cet accès. Si le AR suit la stratégie de l'organisation, le serveur de stratégies accorde l'accès en fonction de l'autorisation du demandeur ; sinon, l'AR ne sera pas autorisé à accéder sur la base de son autorisation. Il convient de noter qu'il existe actuellement divers systèmes commerciaux sur le marché qui fournissent de tels serveurs de politique pour l'informatique sur site et en nuage. Parmi les exemples les plus courants, citons Cisco Identity Services Engine (ISE), Forescout Platform, Aruba ClearPass Policy Manager et FortiNAC.

Ces outils offrent des moyens très détaillés de définir des règles organisationnelles et de contrôler l'ensemble de l'infrastructure IP de l'organisation.

3. **Serveur d'accès réseau (NAS) :**

   Les utilisateurs qui se connectent au réseau interne d'une organisation à partir d'emplacements distants utilisent le NAS comme point de contrôle d'accès. Ceux-ci servent souvent de VPN et donnent aux utilisateurs l'accès au réseau interne de l'entreprise. De nos jours, la fonctionnalité NAS est fréquemment incluse dans les systèmes de serveurs de stratégies.
   Les employés distants peuvent se connecter au réseau interne de l'entreprise via le NAS, qui leur sert de point d'accès. Cela permet à l'entreprise et à ses employés de créer une connexion sécurisée et d'accorder un accès autorisé au réseau. Il s'agissait donc des trois principaux éléments du NAC (contrôle d'accès au réseau).[14]

1.6 Le protocole RADIUS

Le protocole RADIUS (Remote Authentication Dial-In User Service), initialement développé par Livingston, est un protocole standard d'authentification défini par un certain nombre de RFC (Request for Comments).

Son fonctionnement repose sur un système client/serveur chargé de gérer l'accès des utilisateurs distants à un réseau. Il est largement utilisé par les fournisseurs d'accès à Internet en raison de sa standardisation et de ses fonctionnalités de comptabilité, qui permettent aux FAI de facturer précisément leurs clients

Le protocole RADIUS se compose principalement d'un serveur RADIUS, connecté à une base d'identification (telle qu'une base de données ou un annuaire LDAP), et d'un client RADIUS appelé NAS (Network Access Server), qui agit comme un intermédiaire entre l'utilisateur final et le serveur. Toutes les transactions entre le client RADIUS et le serveur RADIUS sont chiffrées et authentifiées à l'aide d'un secret partagé.

Il est à noter que le serveur RADIUS peut également agir en tant que proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS. [6]

1.6.1 Mode de fonctionnement

Le fonctionnement de RADIUS suit un scénario où un utilisateur envoie une requête au NAS pour autoriser une connexion à distance. Le NAS transmet ensuite cette demande au serveur RADIUS. Ce dernier consulte la base de données d'identification pour déterminer le type de scénario d'authentification requis pour l'utilisateur. Si le scénario actuel est approprié, le processus continue. Sinon, une autre méthode d'identification peut être demandée à l'utilisateur. Le serveur RADIUS retourne ainsi l'une des quatre réponses suivantes :

1. **ACCEPT :** l'identification a réussi ;
2. **REJECT :** l'identification a échoué ;
3. **CHALLENGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « challenge ») ;
4. **CHANGE PASSWORD :** le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

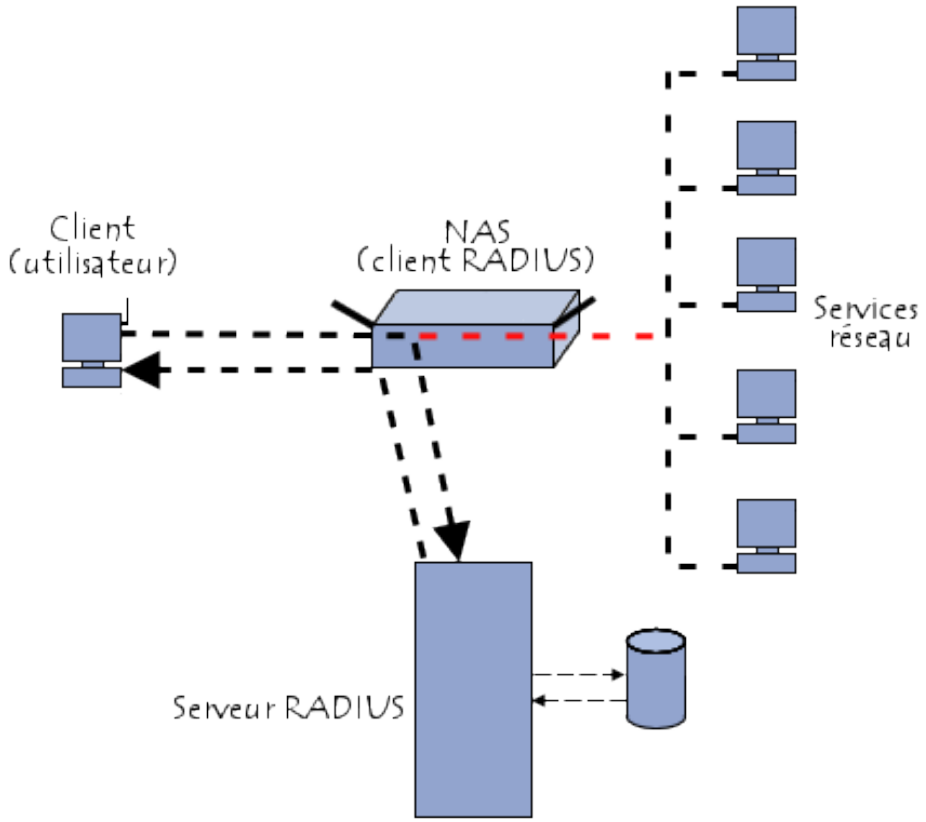


FIGURE 1.4 : Fonctionnement de RADIUS
[2]

Après la phase d'authentification, débute une phase d'autorisation où le serveur RADIUS renvoie les autorisations spécifiques de l'utilisateur.

1.7 Le portail Captif

Un portail captif est une application conçue pour gérer l'authentification des utilisateurs d'un réseau local qui souhaitent se connecter à un réseau externe, généralement Internet. Il contraint les utilisateurs du réseau local à s'authentifier avant de pouvoir accéder au réseau externe. Lorsqu'un utilisateur tente d'accéder à Internet pour la première fois, le portail intercepte sa demande de connexion via un routage interne, puis lui propose de s'identifier afin de pouvoir obtenir l'accès requis. Cette procédure d'authentification s'effectue généralement via une page web hébergée localement sur le portail captif, grâce au serveur HTTP.

Ce système assure la sécurité du réseau mis à disposition en permettant de respecter la politique de filtrage web de l'entreprise grâce à un module proxy intégré. De plus, il offre la possibilité, grâce à un pare-feu intégré, d'interdire l'accès à certains protocoles selon les besoins et les exigences de l'entreprise. [16]

1.7.0.1 Principe et fonctionnement d'un portail captif

1. **Les éléments constitutifs de l'architecture**

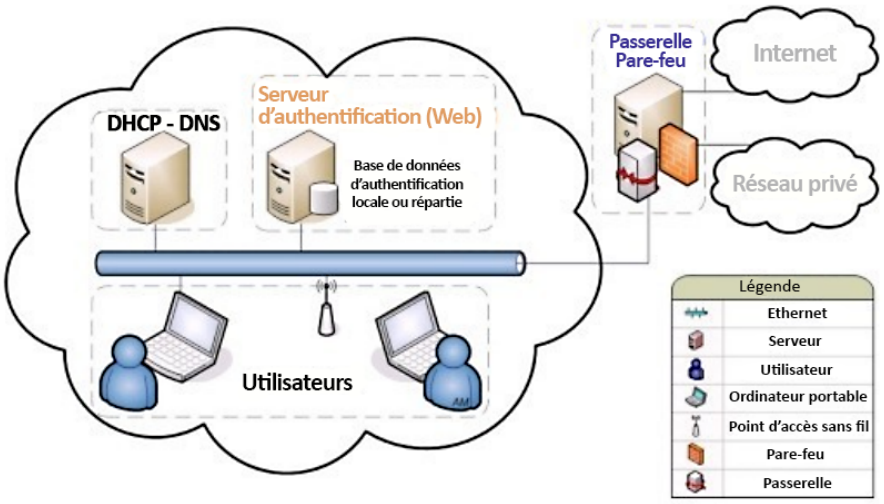


FIGURE 1.5 : Éléments constitutifs d'un portail captif

Les portails captifs reposent sur les identités suivantes :

- Les clients : ils utilisent un navigateur Web pour accéder au portail,
- La passerelle/pare-feu : passerelle entre plusieurs réseaux - elle joue en même temps le rôle de pare-feu,
- Le serveur d'authentification (+Web) : portail Web d'authentification et gestion des fonctionnalités d'authentification des utilisateurs et de leurs droits,
- Un service DHCP, DNS : pour l'allocation dynamique des adresses IP aux clients et la fourniture d'un service DNS d'infrastructure (le DNS peut être facultatif)
- Et éventuellement un point d'accès Wi-Fi (dans le cadre de réseaux sans fils).

Bien que couramment associé aux réseaux Wi-Fi, le portail captif peut également être adapté aux réseaux locaux filaires. Cependant, les préoccupations de sécurité spécifiques aux réseaux Wi-Fi justifient l'accent mis sur ces solutions dans ce domaine.

2. **Le modèle catch and release** Le portail captif opère selon le principe du "Capture and Release" (Capture et Libération). Lorsqu'un utilisateur cherche à accéder à une ressource, il est immédiatement "capturé" et redirigé vers le serveur Web d'authentification. Il ne sera "libéré" qu'une fois son processus d'authentification achevé avec succès. Les numéros entre parenthèses font référence aux numéros du schéma :

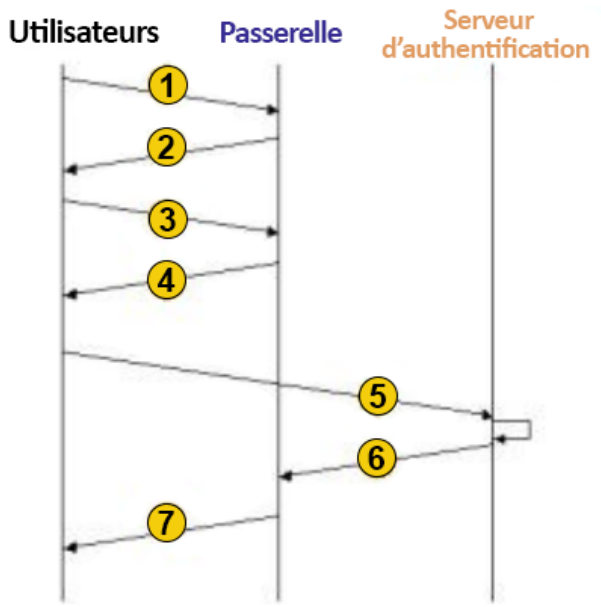


FIGURE 1.6 : Modèle catch and release

Étape 1 : Le client se connecte au réseau.

Étape 2 : Il reçoit les paramètres de connexion par le DHCP.
A ce stade, il n'a aucun droit car la passerelle/pare-feu bloque l'accès réseau, sauf le port 80 qui est redirigé vers le portail Web.

Étape 3 : Le client lance son navigateur Web, saisit et valide son URL.

Étape 4 : Le serveur Web de l'architecture lui demande alors :

- D'approuver les conditions d'utilisation du réseau si le portail est en mode Open (il n'y a pas de processus d'authentification dans ce cas). Dès l'acceptation des conditions d'utilisation, l'utilisateur a accès aux ressources mises à sa disposition,
- De s'authentifier pour avoir accès à un réseau local sécurisé et/ou au réseau Internet par exemple.

Étape 5 : L'utilisateur doit s'authentifier, selon un quelconque moyen : nom d'utilisateur/mot de passe... En cas de refus, le client verra ses droits conservés, sans possibilité aucune d'accès aux ressources réseau.

Étape 6 : Si le client s'identifie correctement, la passerelle/pare-feu modifie alors dynamiquement ses paramètres.

Étape 7 : La passerelle définit les paramètres de qualité (temps de connexion, services...) relatifs à l'utilisateur authentifié. Sa connexion est maintenue tant qu'il ne ferme pas une fenêtre du navigateur qui maintient sa connexion en arrière-plan. On parle de portail « intelligent » lorsque celui-ci enregistre l'URL saisie par l'utilisateur lors de l'ouverture de son navigateur Web pour le renvoyer directement à cette URL dès que son authentification s'est déroulée avec succès et que ses droits le lui permettent. [17]

Conclusion

Dans ce chapitre, nous avons fait une revue de littérature en définissant les concepts. Il s'agira dans le chapitre suivant de présenter quelques solutions existantes et les raisons de choix de l'outil utilisé pour notre travail.

Chapitre 2

Solution et choix techniques

Introduction

Un pirate peut attaquer n'importe quel ordinateur connecté à Internet. L'approche typique du pirate consiste à scanner le réseau en envoyant des paquets de données aléatoires à la recherche d'un système connecté, puis à rechercher une machine vulnérable. Afin d'accéder aux données d'une machine connectée, il faut d'abord rechercher les failles de sécurité. L'installation d'un dispositif de protection est donc essentielle, tant pour les réseaux d'entreprises que pour les consommateurs d'Internet connectés, afin de se protéger des attaques du réseau.

Nous allons explorer les solutions actuelles dans ce chapitre afin de réaliser une étude comparative pour le choix de l'outil.

2.1 Description de la solution

La solution que nous proposons consiste à utiliser une plateforme Open Source de sécurité réseau, pour mettre en place un portail captif avec authentification radius dans une entreprise. Le portail captif permettra de contrôler l'accès au réseau de l'entreprise en obligeant les utilisateurs à s'authentifier avant d'accéder à Internet, tandis que l'authentification radius assurera une sécurité supplémentaire en utilisant des identifiants d'utilisateurs uniques. Cette solution permettra également de configurer des règles de pare-feu avancées pour surveiller et contrôler le trafic réseau, ainsi que la surveillance de l'utilisation de la bande passante. Tout ceci en utilisant une infrastructure réseau existante pour assurer une mise en œuvre rapide et peu coûteuse. En utilisant cette solution, l'entreprise peut facilement gérer l'accès à Internet de ses employés, assurer une sécurité réseau adéquate et suivre les activités des utilisateurs.

2.2 Aperçu des principaux solutions de portails captifs

Au cours de nos recherches, nous avons trouvé plusieurs solutions pour la mise en place de notre système. Au nombre de ces solutions, nous pouvons citer :

2.2.1 Pfsense

Pfsense est une distribution basée sur FreeBSD, lancée en 2004. Initialement conçue pour assurer les fonctions de pare-feu et de routeur, elle a depuis élargi son champ d'action grâce à un fort engouement. Aujourd'hui, Pfsense propose une gamme étendue de fonctionnalités telles que le portail captif, le serveur proxy, le DHCP, etc. Son installation est simple grâce à une distribution dédiée, et toutes les configurations peuvent être effectuées soit en ligne de commande (SSH) soit via une interface web sécurisée (HTTPS). La sauvegarde et la restauration de la configuration sont également disponibles via l'interface web, permettant de générer un fichier de taille raisonnable. Pfsense bénéficie d'une évolution continue grâce à des mises à jour régulières, dont l'installation est automatiquement gérée dans une partie du panneau d'administration.

2.2.2 ALCASAR

ALCASAR est un projet français axé principalement sur les fonctionnalités du portail captif. Pour son installation, il utilise un script pris en charge par la distribution Linux Mandriva. Les configurations peuvent être réalisées via une interface de gestion sécurisée en HTTPS ou directement en ligne de commande sur le Serveur Mandriva. La sauvegarde de la configuration est gérée en créant un "ghost système" (fichier système) dans le panneau d'administration, ce qui entraîne la création d'un fichier de taille considérable. Des mises à jour régulières sont effectuées pour assurer la durabilité de la solution.

2.2.3 ZeroShell

Zeroshell est une distribution Linux conçue pour les serveurs et les périphériques embarqués, destinée à fournir les principaux services réseau nécessaires à un LAN. Disponible sous forme de Live CD ou d'image Compact Flash, il peut être configuré et administré via un navigateur Web. Son installation est simple grâce à une distribution dédiée. Bien qu'il soit conçu pour être utilisé à partir du Live CD, les données de configuration peuvent également être enregistrées sur le disque dur. L'image Compact Flash offre suffisamment d'espace de stockage pour cela. Quelle que soit la version utilisée, l'interface de gestion de Zeroshell est assez complète. Chaque fonctionnalité de Zeroshell est accessible et personnalisable via un navigateur, à l'exception de l'exécution du script wifi-manager, qui n'est pas encore pris en charge par l'interface utilisateur du navigateur, et de l'activation du client DHCP sur l'interface de gestion.

2.2.4 ChilliSpot

ChilliSpot est un portail captif open source ainsi qu'un contrôleur de points d'accès pour les réseaux locaux sans fil. Il est utilisé pour authentifier les utilisateurs sur un réseau local sans fil et gère l'ouverture de session web, qui est le standard actuel pour les hot-spots publics, ainsi que l'authentification d'un "smart-client" WISP et le Wi-Fi Protected Access (WPA et WPA2). Le protocole RADIUS est chargé de gérer l'authentification, l'autorisation et la comptabilité (protocole AAA) à bord ou à distance. Son installation est relativement simple grâce à un package applicatif disponible sur les distributions Red Hat et Fedora. La page de connexion est accessible en HTTPS à condition que le serveur web (Apache) ait été configuré au préalable pour écouter sur le port 443. Bien que la documentation soit assez complète, la communauté est moins active et le projet est en régression, la

dernière version stable datant d'octobre 2007. De plus, le projet est en suspens depuis le départ du développeur principal.[23]

2.3 Comparaison des portails captifs

Dans l'étude comparative des solutions nous avons mis en évidence plusieurs critères importants que doivent prendre en compte les différentes solutions :

- **Prise en charge de l'authentification RADIUS :** la solution de portail captif doit prendre en charge l'authentification RADIUS, ce qui permettra de connecter le réseau Wi-Fi ou filaire de l'entreprise à l'annuaire des utilisateurs existant ;
- **Sécurité des échanges lors de l'authentification :** pour éviter la récupération de mot de passe sur le réseau ;
- **Disponibilité de mise à jour :** La mise à jour régulière du système peut aider à garantir que le système reste sécurisé et performant, et peut également aider à corriger les bugs et les vulnérabilités connues.
- **Personnalisation de l'interface :** la solution doit offrir une interface personnalisable pour adapter le logiciel à la charte graphique de l'entreprise et ainsi le rendre plus convivial ;
- **Intégration facile avec votre réseau :** la solution de portail captif doit être facilement intégrable au réseau existant de l'entreprise ;
- **Configuration requise :** la solution de portail captif doit utiliser moins de ressources pour fonctionner plus rapidement et plus efficacement ;
- **Condition d'installation :** pour permettre à différentes personnes d'administrer le logiciel ;
- **Présence d'une documentation complète :**pour assurer la rapidité de mise en place de la solution.

Critères/Solutions	**Pfsense**	**ALCASAR**	**Zeroshell**	**Chillispot**
Prise en charge de l'authentification RADIUS	+	+	+	+
Sécurité des échanges lors de l'authentification	HTTPS	HTTPS	HTTPS	HTTPS
Disponibilité de mise à jour	Évolutif	Évolutif	Moins évolutif	Non évolutif
Personnalisation de l'interface	+	+	-	+
Intégration facile avec votre réseau	+	+	+	-
Configuration requise	Mémoire vive : 512 Mo Stockage : 4Go	Mémoire vive : 8 Go Stockage : 25 Go	Mémoire vive : 256 Mo Stockage : 8 Go	Dépends de la mémoire utilisée par la distribution Linux
Installation	Installation via distribution dédié	Installation via script automatisé	Installation via distribution dédié	Installation Via RPM (Red Hat Package Manager) sur Red Hat et Fedora
Documentation et support	Disponibilité élevée	Disponibilité élevée	Disponibilité moyenne	Disponibilité moyenne

TABLEAU 2.1 : Tableau de comparaison des différentes solutions

Le tableau ci-dessous résume les critères de comparaison et les caractéristiques de (04) quatre systèmes de portail captif à savoir : Pfsense, ALCASAR, Zeroshell et Chillispot. Chacun de ces systèmes est évalué sur sa capacité à gérer l'authentification RADIUS, à chiffrer les échanges d'authentification, à s'améliorer au fil du temps, à permettre la personnalisation de l'interface utilisateur, à s'intégrer facilement dans un réseau et à nécessiter peu de ressources pour son déploiement.

En considérant les critères de comparaison listés, on peut remarquer que la mise en œuvre des portails captifs Zeroshell et Chillispot peut être difficile, car elles ne sont pas faciles à administrer.

De plus, selon l'article [25] Zeroshell a été mise hors service le 30 septembre 2021. Il ressort donc que ce portail captif ne subit plus de mise à jour. Quant à Chillispot, sa dernière version date de 2007 [23]. Aucun de ces portails captifs n'est donc fiable comme solution.

Ensuite, d'après les données du tableau, les solutions Pfsense et ALCASAR sont plus avantageuses car elles prennent en charge l'authentification RADIUS et sécurisent les échanges lors de l'authentification avec HTTPS. Elles sont également disponibles pour des mises à jour régulières et permettent une bonne administration du réseau. Cependant, ALCASAR s'installe à l'aide d'un script automatisé et nécessite plus de ressources, tandis que Pfsense nécessite moins de ressources avec une installation plus rapide via une distribution dédiée. En termes de coût, de mise en œuvre et de performance, Pfsense est une solution fiable à adopter. De plus, ce dernier présente une interface plus conviviale, une multitude de fonctionnalités et une page principale sous forme de tableau de bord où l'on retrouve toutes les informations essentielles et que l'on peut modifier en fonction des

besoins. Ce produit présente aussi une plus grande assurance, car la communauté des utilisateurs est très active.

2.4 Architecture du réseau

Notre solution pare-feu open-source, pfSense, est déployée au sein d'un environnement réseau composé d'un switch interconnectant les divers services du réseau local. Ce switch est connecté au pare-feu, qui à son tour, est relié au réseau externe. Le schéma ci-dessous illustre notre configuration réseau actuelle, avec pfSense en tant que composant central assurant la sécurité et la gestion du trafic entre le réseau local et le réseau externe.

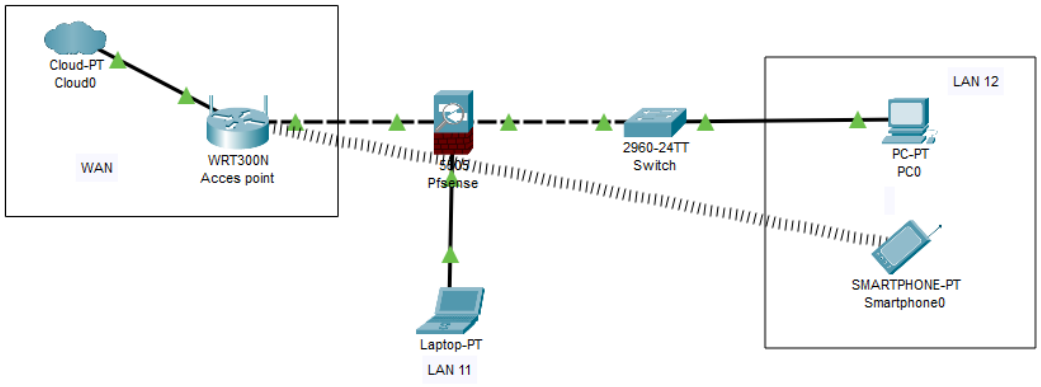


FIGURE 2.1 : Architecture du réseau

2.5 Étapes de mise en œuvre

Pour la mise en œuvre de notre solution, nous avons subdivisé le travail en étapes :

- l'installation de VirtualBox ;
- l'installation et Configuration de Pfsense dans une machine virtuelle sous VirtualBox ;
- implémentation de FreeRadius ;
- création du portail captif pour authentification des utilisateurs.

2.6 Installation de VirtualBox

Suite au téléchargement de VirtualBox depuis le site www.virtualbox.org, nous avons procédé à son installation en suivant les instructions. Après l'installation, nous avons créé une adresse WAN (la carte réseau étant en mode NAT) que nous avons nommée WAN-1 en activant la fonction "Enable DHCP". Ceci permettra à plusieurs machines virtuelles d'accéder à Internet via une seule adresse IP. La fonction "Enable DHCP" permettra à pfSense, une fois installé, de configurer automatiquement son adresse WAN.

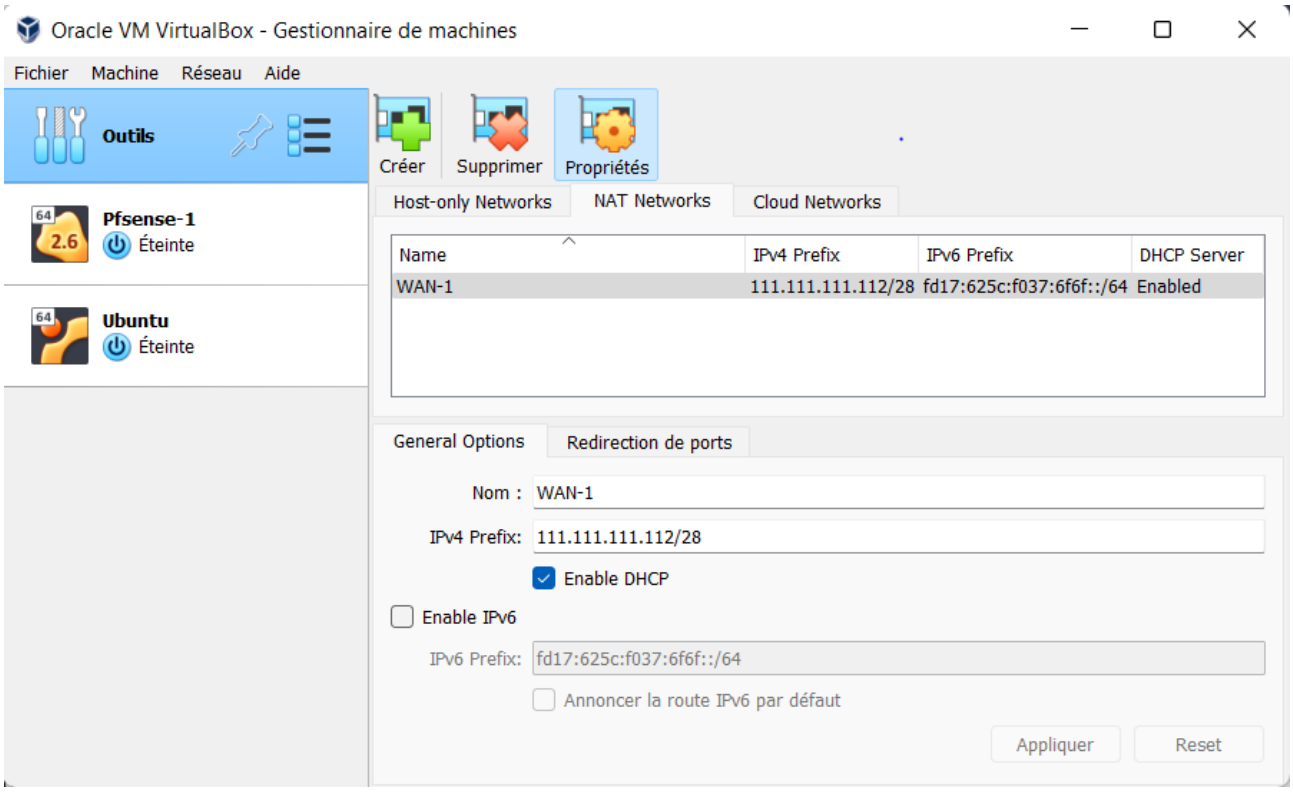


FIGURE 2.2 : Création du NAT

Ensuite, nous avons créé deux réseaux en mode hôte uniquement, également appelés "Host-Only Network", pour permettre à nos machines virtuelles d'interagir avec l'hôte ou l'ordinateur physique. Ici, le serveur DHCP est désactivé.

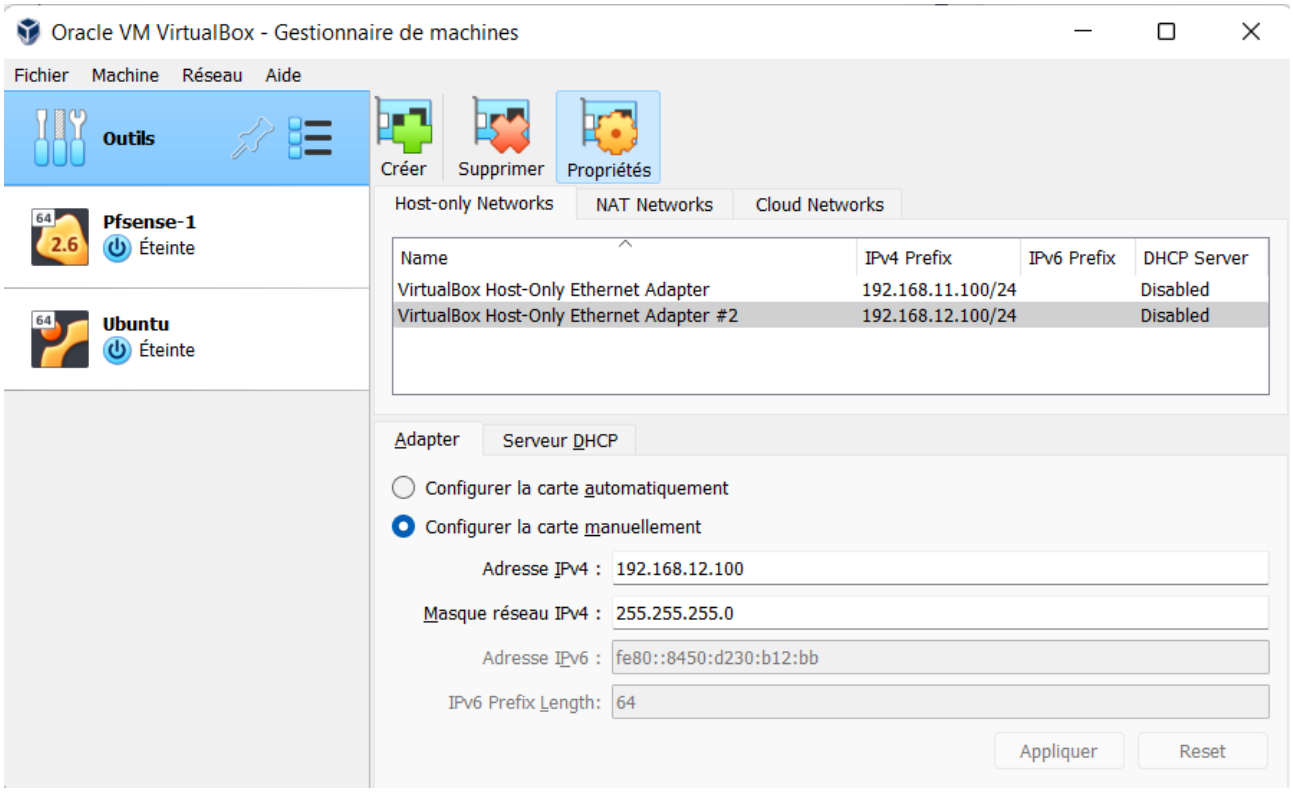


FIGURE 2.3 : Création de Host-Only Network

2.7 Installation de Pfsense

Dans notre contexte, nous allons effectuer l'installation sous VirtualBox version 7.0.12. La version spécifique de pfSense que nous utiliserons est la 2.7.0, et nous avons téléchargé l'image ISO nécessaire, disponible sur le site https ://www.pfsense.org, sous le nom pfSense-CE-2.7.0-RELEASE-amd64.iso. La procédure commence par la création d'une nouvelle machine virtuelle dans VirtualBox, que nous baptisons "PfSense-1". Nous procédons à l'installation en suivant les instructions fournies.

Après le démarrage de la machine pfSense, on définit l'interface WAN en mode DHCP et les interfaces LAN en leur assignant des adresses IP statiques. Après l'attribution, un menu shell est présenté sur la console avec un certain nombre d'options. pfSense est maintenant prêt à être accédé via le réseau LAN, dans notre cas.

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): ^CKVM Guest - Netgate Device ID: 01d198de4753a6148f1c

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN1 (wan)       -> em2        -> v4/DHCP4: 111.111.111.116/28
 LAN11 (lan)      -> em0        -> v4: 192.168.11.1/24
 LAN12 (opt1)     -> em1        -> v4: 192.168.12.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

FIGURE 2.4 : Shell et configuration pfsense

La configuration du pare-feu pfSense peut être effectuée soit via la console, soit à partir d'une interface web. L'interface web, appelée WebGUI, est largement utilisée pour configurer la plupart des éléments dans pfSense. Nous avons choisi de configurer pfSense via l'interface web pour plus de convivialité. Pour ce faire, nous avons connecté notre PC client à l'interface LAN de pfSense. Nous avons débuté en ouvrant un navigateur web et en accédant à l'adresse http ://192.168.11.1 pour atteindre l'interface de connexion. À cet endroit, on nous a demandé de saisir un nom d'utilisateur et un mot de passe (voir figure 3.4). Nous nous sommes connectés à l'interface pfSense en utilisant les paramètres par défaut : le nom d'utilisateur (admin) et le mot de passe (pfsense), nous permettant ainsi d'accéder en tant qu'administrateur.

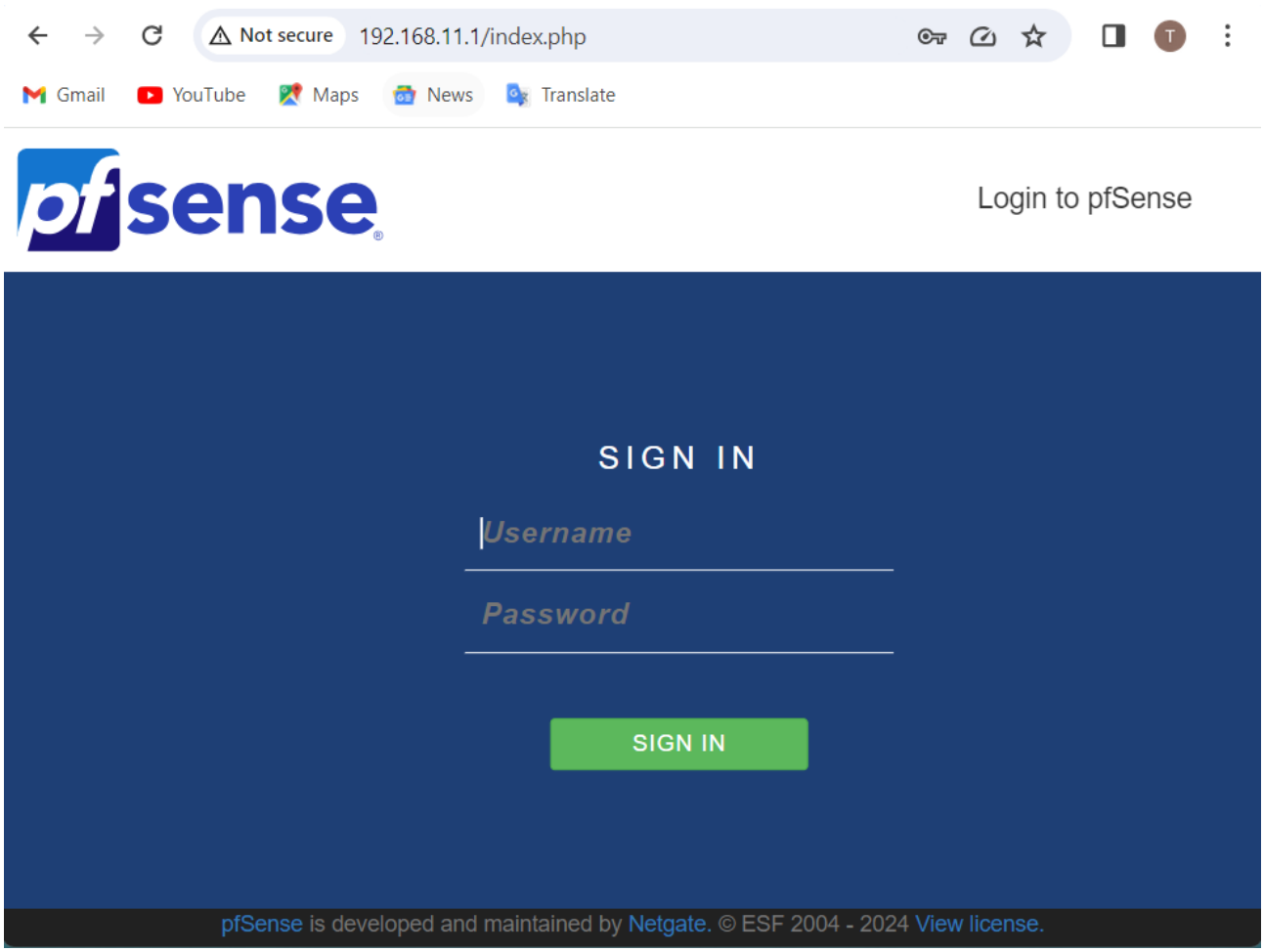


FIGURE 2.5 : Interface WEB de pfsense

On accède ensuite au menu général de Pfsense (figure 3.6) qui donne les informations globales du logiciel (version, date de sortie, version du noyau, le nombre d'interfaces connectées, etc.) :

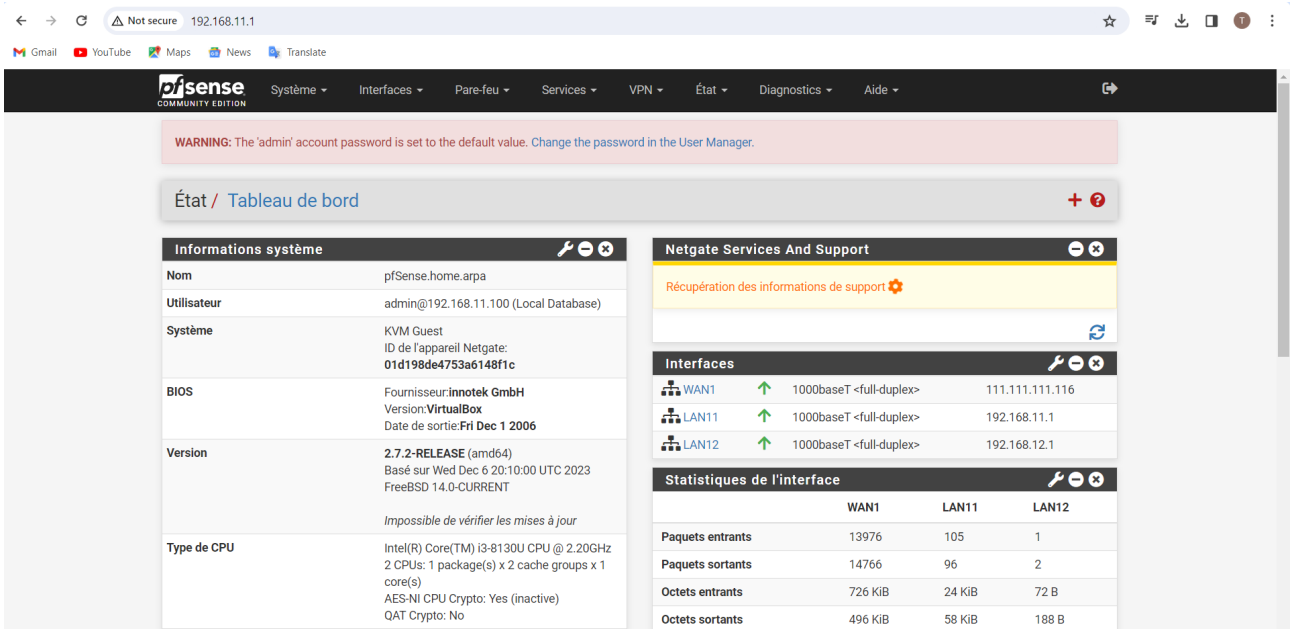


FIGURE 2.6 : Tableau de bord de pfsense

2.8 Implémentation de FreeRadius

Pour implémenter FreeRadius, nous allons tout d'abord installer son package. Une fois connectés à l'interface web de pfSense, nous accédons à la section "System" et sélectionnons "Package Manager". Dans le gestionnaire de packages, nous recherchons FreeRadius et procédons à son installation.

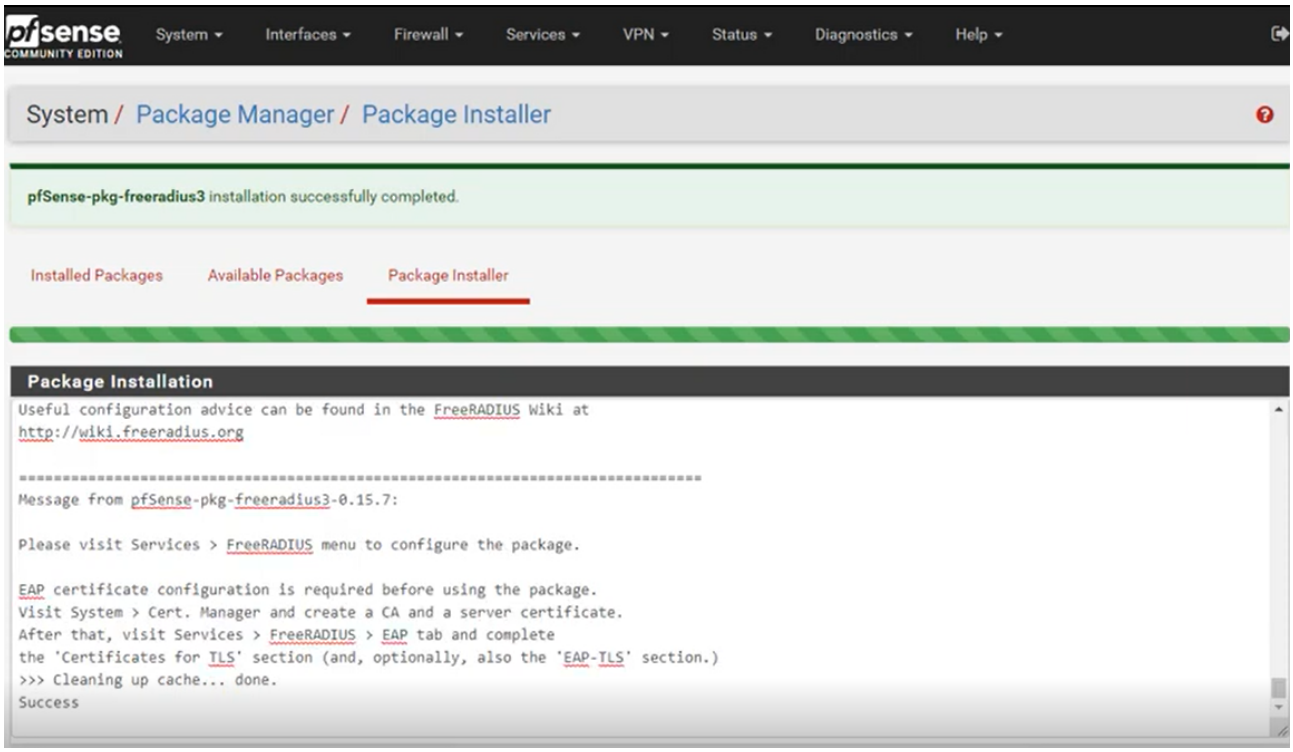


FIGURE 2.7 : Package FreeRadius

2.8.1 Configuration du serveur DHCP

Dans cette étape, nous procédons à la configuration du serveur DHCP pour le réseau local (LAN12), qui servira à faire le test dans le but de simplifier la connexion des clients. Pour ce faire, accédons à l'onglet "Services", puis à la section "Serveur DHCP", où nous activons le serveur DHCP sur l'interface LAN en cochant la case correspondante. Avant d'activer le service DHCP, il est essentiel de vérifier qu'aucun autre serveur DHCP n'est activé sur le réseau afin d'éviter tout conflit d'adresses. Ensuite, nous définissons la plage d'adresses IP qui sera attribuée aux clients. Nous saisissons également le nom de domaine qui sera assigné aux clients, ainsi que la passerelle, tandis que les autres paramètres restent inchangés par défaut.

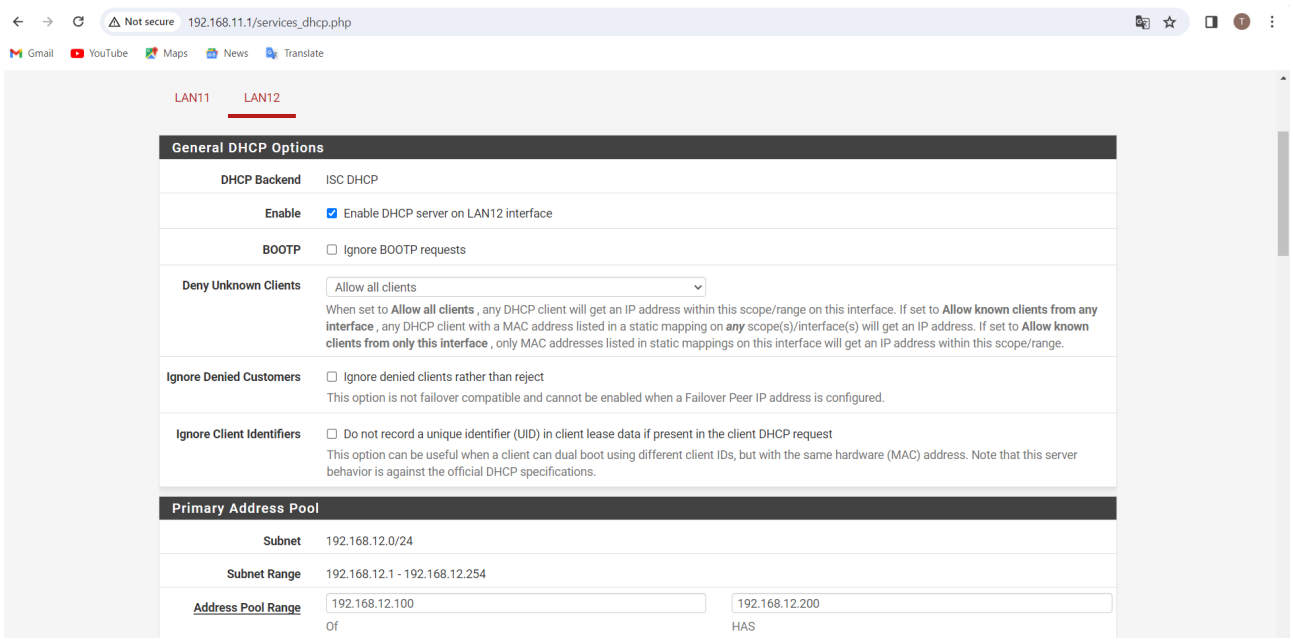


FIGURE 2.8 : Serveur DHCP

2.8.2 Configuration d'un Alias

Dans pfSense, un alias est une fonctionnalité qui permet de regrouper un ensemble d'adresses IP, de ports réseau ou d'autres types d'entités réseau sous un seul nom symbolique. On nommera cet alias "Wifi Users". Sous l'onglet "Pare-feu", nous nous rendons à la section "Alias" pour définir une plage d'adresses permettant aux utilisateurs connectés au réseau Wi-Fi d'accéder à Internet.

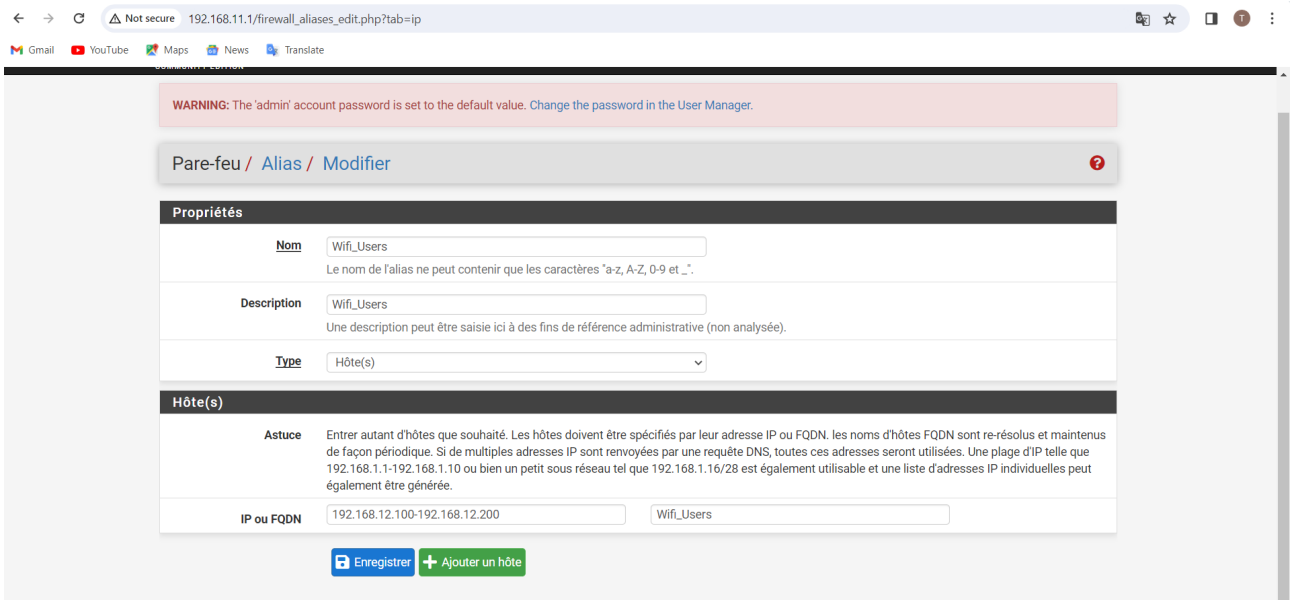


FIGURE 2.9 : Alias

2.8.3 Configuration de règles de Pare-feu

Dans l'onglet "Pare-feu", nous nous rendons à la section "Règles" pour établir une règle permettant l'accès à Internet pour les utilisateurs du réseau Wi-Fi. Afin d'accomplir cette tâche, nous allons inclure l'alias "Wifi Users", créé précédemment, et spécifier la passerelle permettant l'accès à Internet

tout en ajustant certains paramètres, tandis que d'autres seront laissés inchangés par défaut.

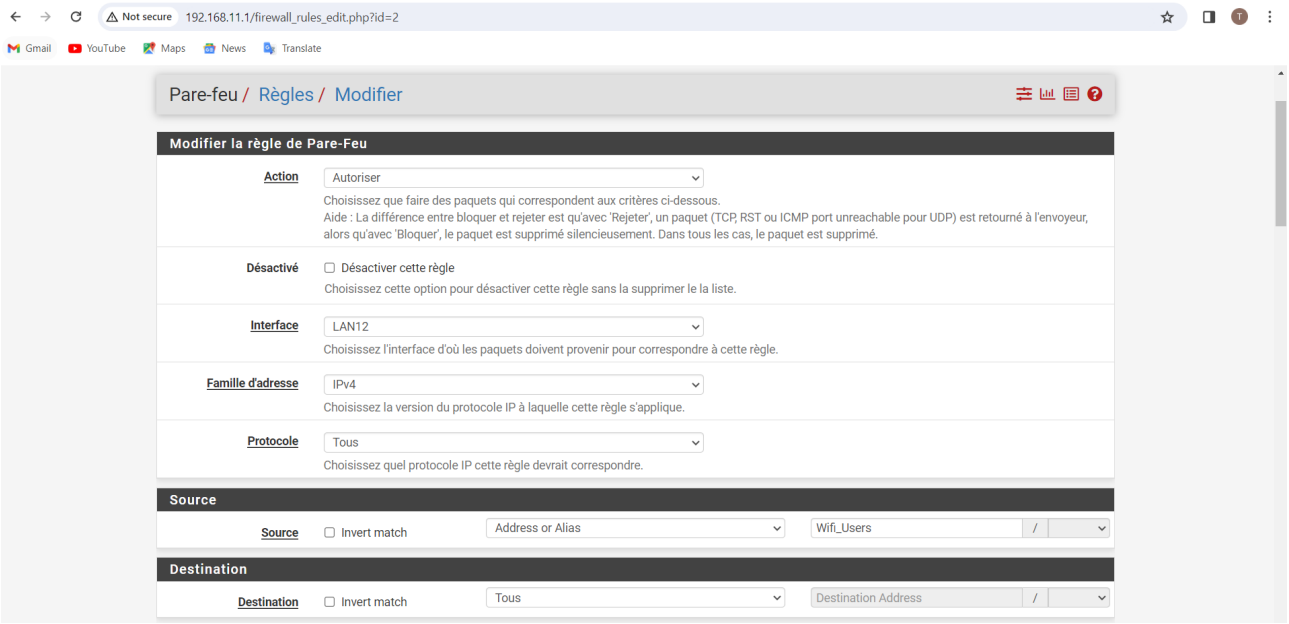


FIGURE 2.10 : Les règles

2.8.4 Configuration de FreeRadius

Une fois l'installation terminée, nous accédons à l'onglet "Services", puis sélectionnons "FreeRadius" apparu dans le menu, pour configurer les paramètres du serveur RADIUS.

2.8.4.1 Définition des clients RADIUS

Toujours dans l'interface "FreeRadius", nous accédons à la section "NAS/Clients" pour ajouter les informations sur les clients RADIUS, telles que l'adresse IP et le secret partagé. Le secret partagé, également appelé "shared secret", est utilisé pour sécuriser les communications entre le client RADIUS (dans ce cas, un point d'accès sans fil) et le serveur RADIUS (dans ce cas, FreeRadius sur pfSense). Lorsqu'un client RADIUS envoie une requête d'authentification au serveur RADIUS, il inclut le secret partagé dans cette requête. Le serveur RADIUS utilise ensuite ce secret partagé pour vérifier l'authenticité de la requête et pour chiffrer les informations sensibles lors de la communication.

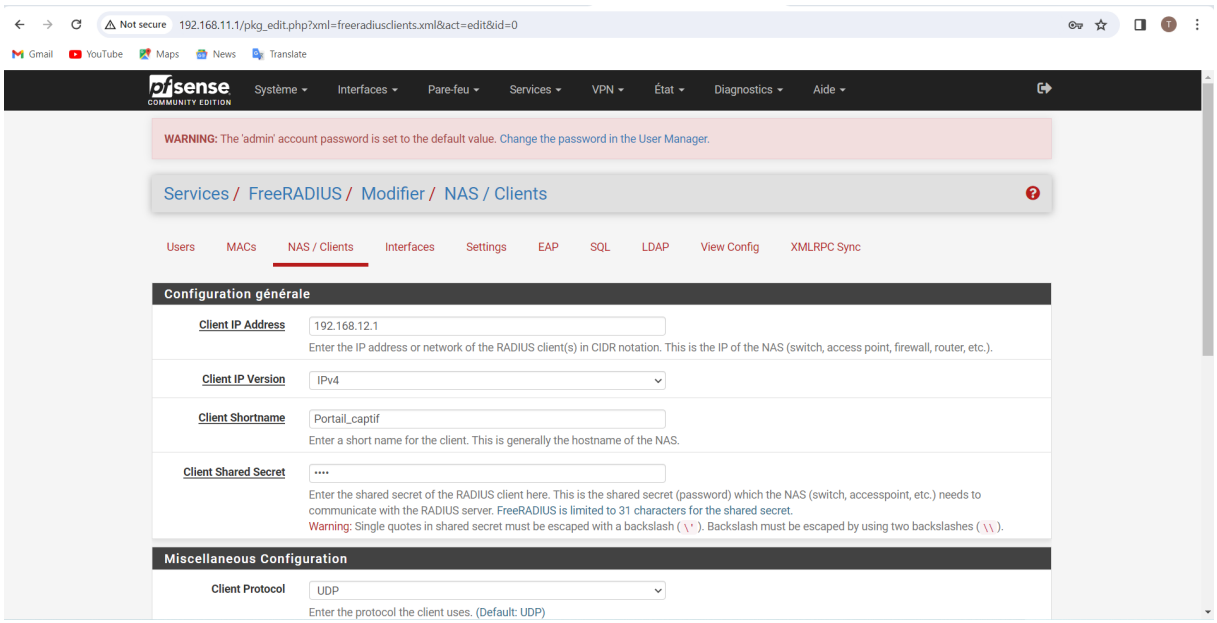


FIGURE 2.11 : Configuration des clients

2.8.4.2 Configuration des utilisateurs

Dans la section "Users", nous allons procéder à l'insertion des comptes d'utilisateurs manuellement comme cela se voit sur la figure 3.12 ci-dessus.

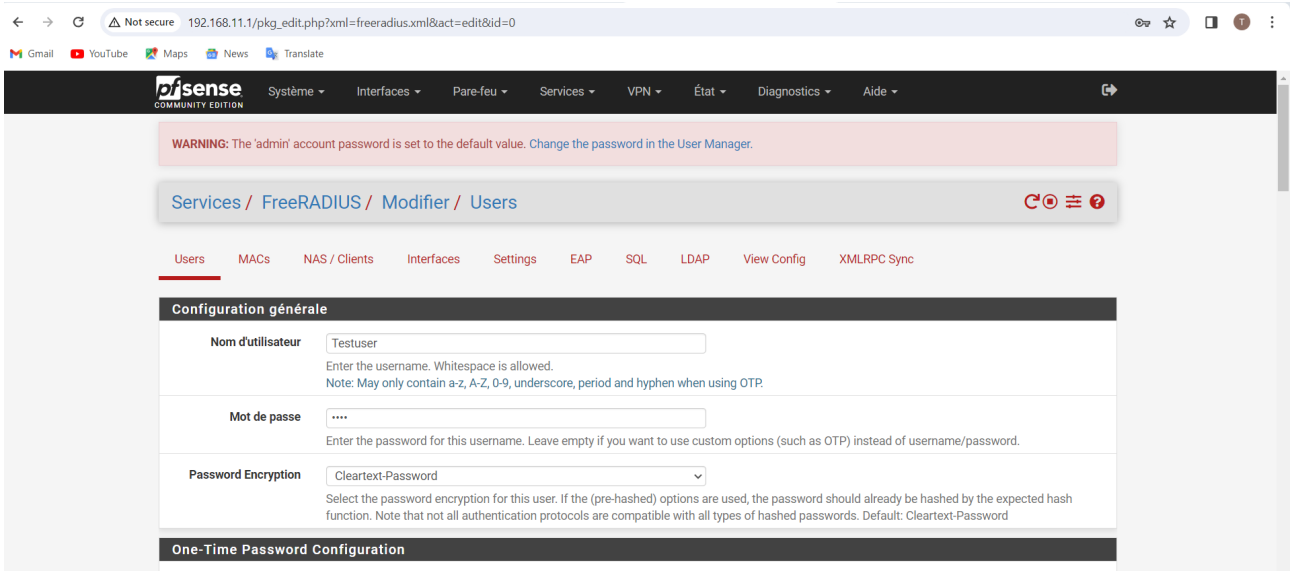


FIGURE 2.12 : Ajout des utilisateurs

2.8.4.3 Définition du serveur Radius comme serveur d'authentification

Dans l'interface web de pfSense, nous allons accéder à l'onglet "Système" et sélectionner "Gestionnaire d'usagers". Dans l'onglet "Serveurs", nous ajoutons le serveur RADIUS en cliquant sur le bouton "Ajouter un serveur". Nous remplissons les détails nécessaires, tels que l'adresse IP du serveur RADIUS, les services offerts (Authentification et Comptabilité), le port (habituellement 1812 pour l'authentification et 1813 pour la comptabilité), et la clé partagée (secret partagé) pour sécuriser la communication entre pfSense et le serveur RADIUS.

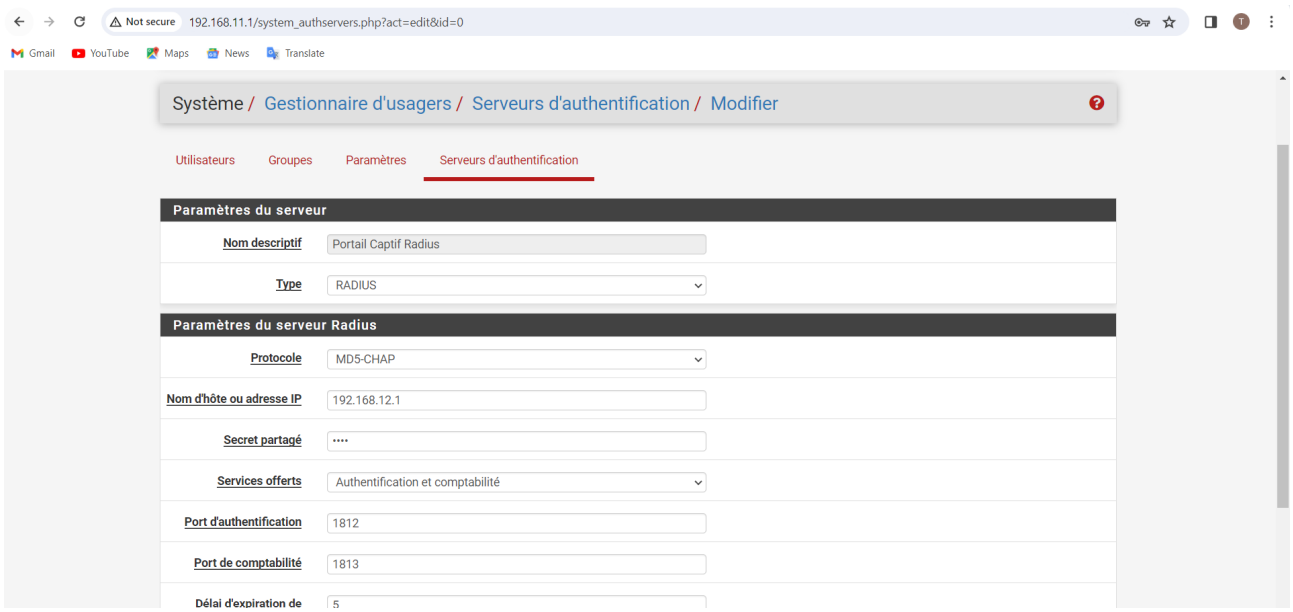


FIGURE 2.13 : Serveur RADIUS

2.9 Création du portail Captif

Nous accédons à l'onglet "Services" et sélectionnons "Portail Captif". Nous cocherons la case "Activer" pour activer le portail captif. En ce qui concerne la configuration de l'interface du portail captif, nous choisissons l'interface sur laquelle le portail captif sera activé, généralement l'interface LAN. Nous ajustons les paramètres supplémentaires tels que la zone horaire et l'adresse IP du portail captif. Pour la configuration de l'authentification, nous optons pour une méthode spécifique, comme "Authentication backend", pour forcer l'affichage de la page de connexion et authentifier les utilisateurs à l'aide de leur nom d'utilisateur et de leur mot de passe, ou à l'aide de bons. Comme serveur d'authentification, nous choisissons le serveur RADIUS "Portail Captif Radius" pour l'intégrer. Nous activons ensuite l'option "Reauthenticate Users", ce qui a pour effet d'envoyer des demandes au serveur pour chaque utilisateur connecté toutes les minutes. En ce qui concerne la personnalisation de la page de connexion, nous ajustons les paramètres sous l'onglet "Captive Portal Login Page", y compris l'ajout de notre logo et la modification de l'image d'arrière-plan. En ce qui concerne les autres paramètres, nous les laissons par défaut.

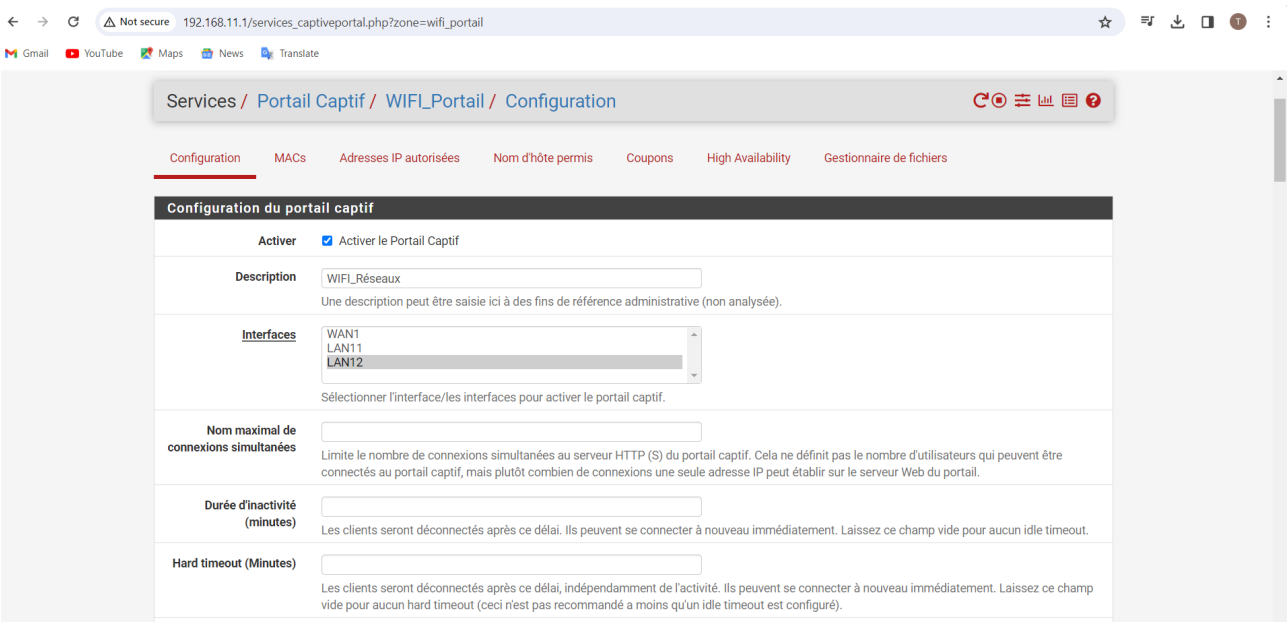


FIGURE 2.14 : Portail Captif

Conclusion

Dans ce chapitre, nous avons présenté les différentes solutions existantes ainsi qu'une comparaison de performance pour le choix de l'outil utilisé dans notre travail. Le chapitre suivant sera consacré aux résultats et au fonctionnement de notre solution.

Chapitre 3

Mise en œuvre du réseau, résultats et discussions

Introduction

Dans ce chapitre, nous présenterons dans un premier temps l'architecture du réseau, le déploiement de pfSense, ainsi que le détail des configurations. Ensuite, nous présenterons les résultats des simulations effectuées pour tester le fonctionnement de notre solution, et nous aborderons enfin une discussion.

3.1 Tests

3.1.1 Commande ping pour le test

Nous allons d'abord éffectuer un test en envoyant un ping vers l'adresse de Google.

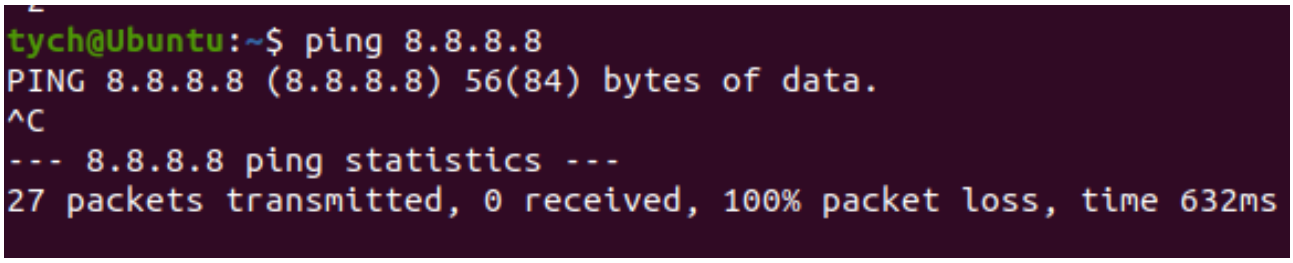


FIGURE 3.1 : Ping vers l'adresse de Google

Le test de ping a échoué. Nous allons tenter de nous connecter au réseau avant de réessayer.

3.1.2 Connexion sur le portail captif

Nous allons maintenant effectuer les tests en tant qu'utilisateur du réseau local sur notre machine client afin de nous assurer que nos règles ont bien été appliquées. Notre machine client dispose d'un système d'exploitation Ubuntu. Dans notre navigateur, nous voyons une barre d'aide s'afficher en haut, demandant de se connecter avant d'avoir accès à Internet, avec le bouton "Open Network

Login Page", qui signifie "Ouvrir la page de connexion au réseau". En cliquant immédiatement sur ce bouton, nous sommes redirigés vers un portail captif nous demandant d'entrer nos identifiants (nom d'utilisateur et mot de passe).

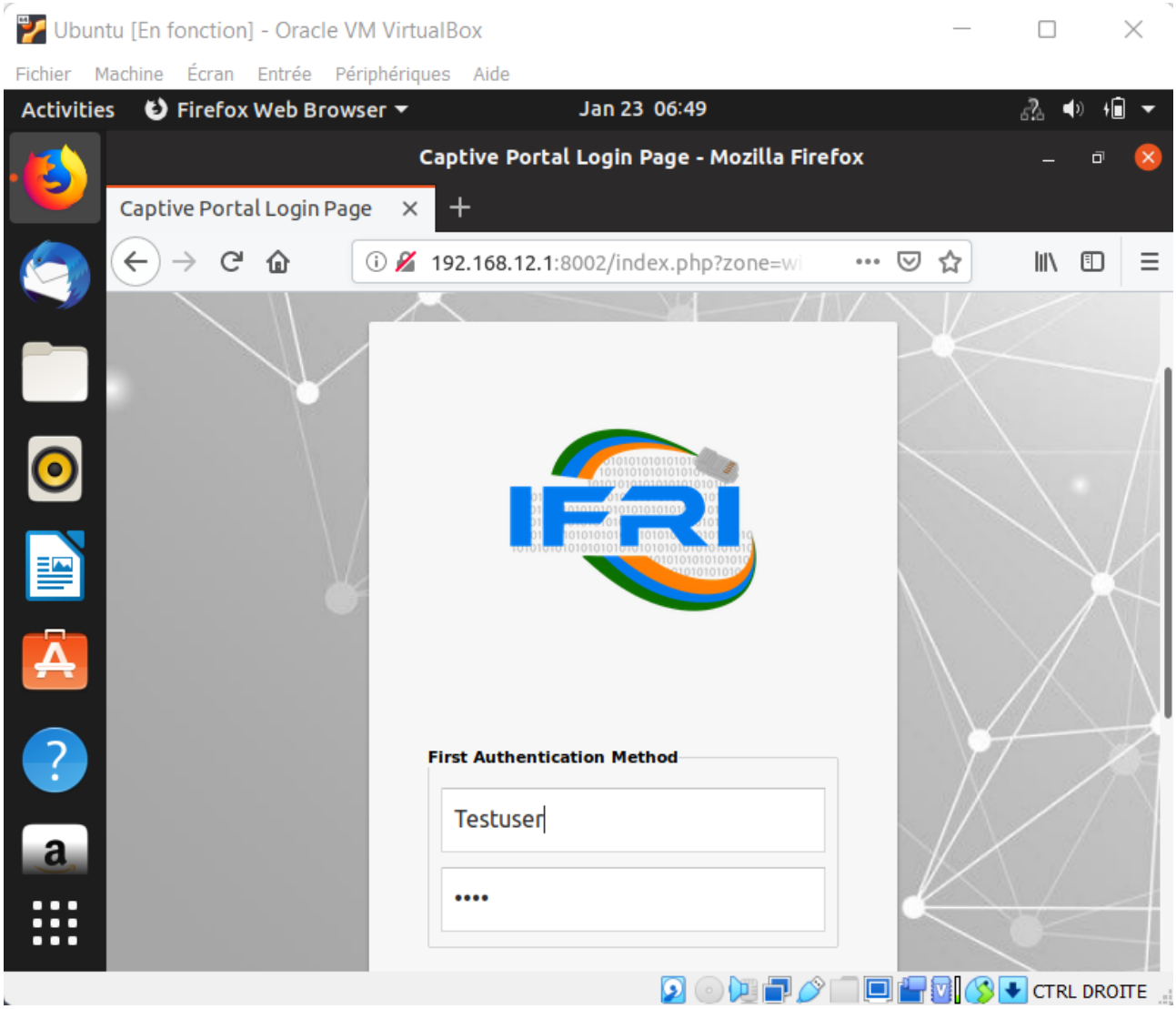


FIGURE 3.2 : Login Page

Après authentification, nous allons essayer de refaire un ping pour vérifier si la connexion passe réellement

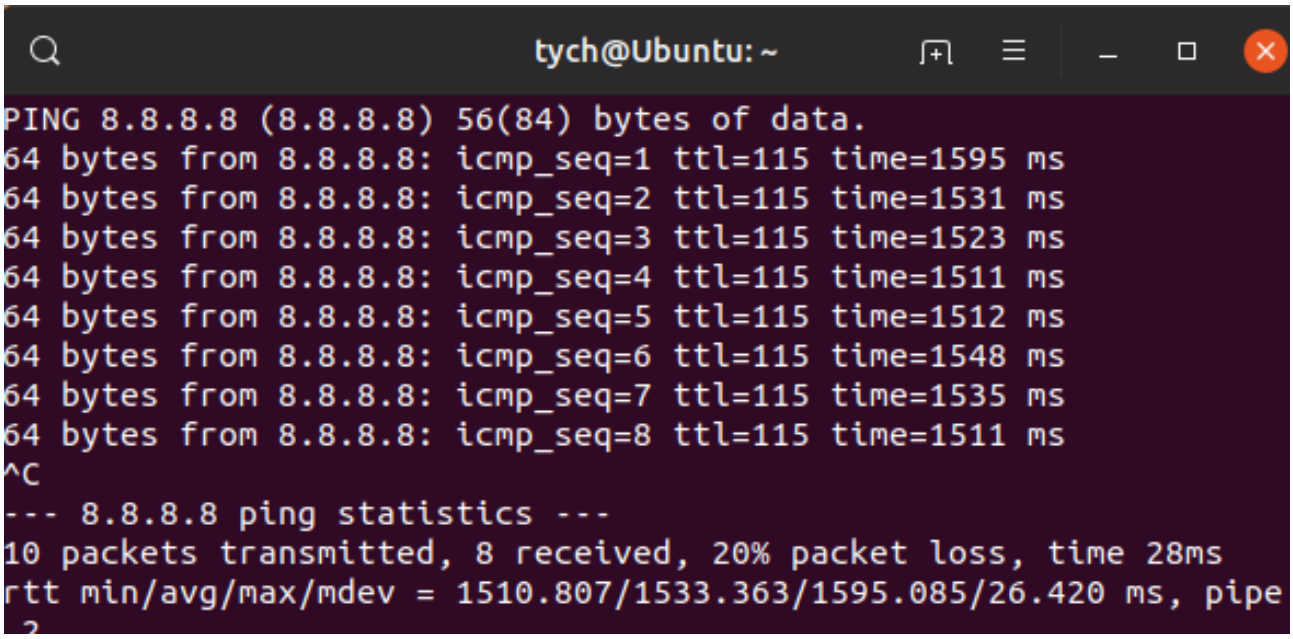


FIGURE 3.3 : Test de ping

Après l'authentification, nous sommes immédiatement redirigés vers la page d'accueil de Bing, d'où nous pouvons accéder à n'importe quelle page que nous souhaitons visiter.

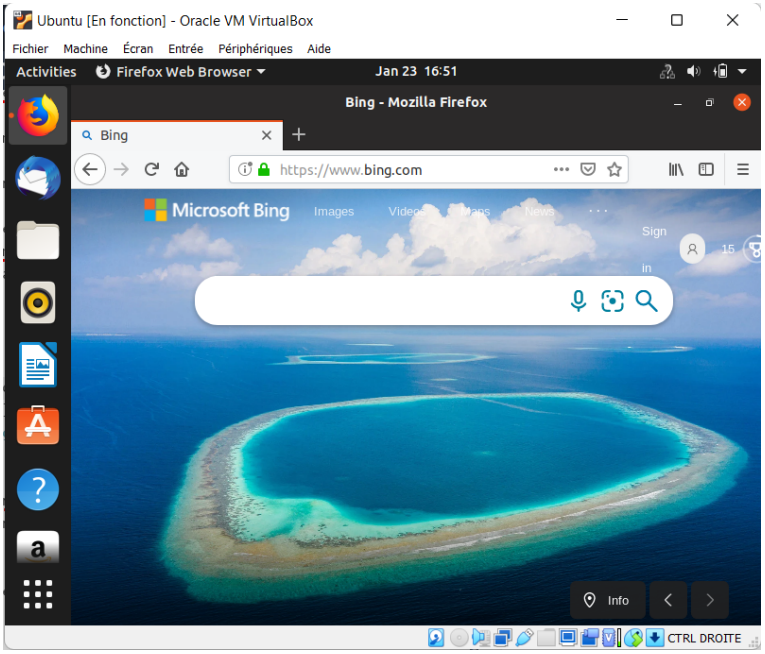


FIGURE 3.4 : Redirection vers Bing

3.1.3 Configuration du Groupe et des Utilisateurs pour la délégation du Portail Captif

Nous allons maintenant créer un groupe et un utilisateur dédiés, chargés de créer des utilisateurs autorisés à se connecter au Portail Captif. Ce groupe et ces utilisateurs auront exclusivement le droit de gérer les comptes du Portail Captif.

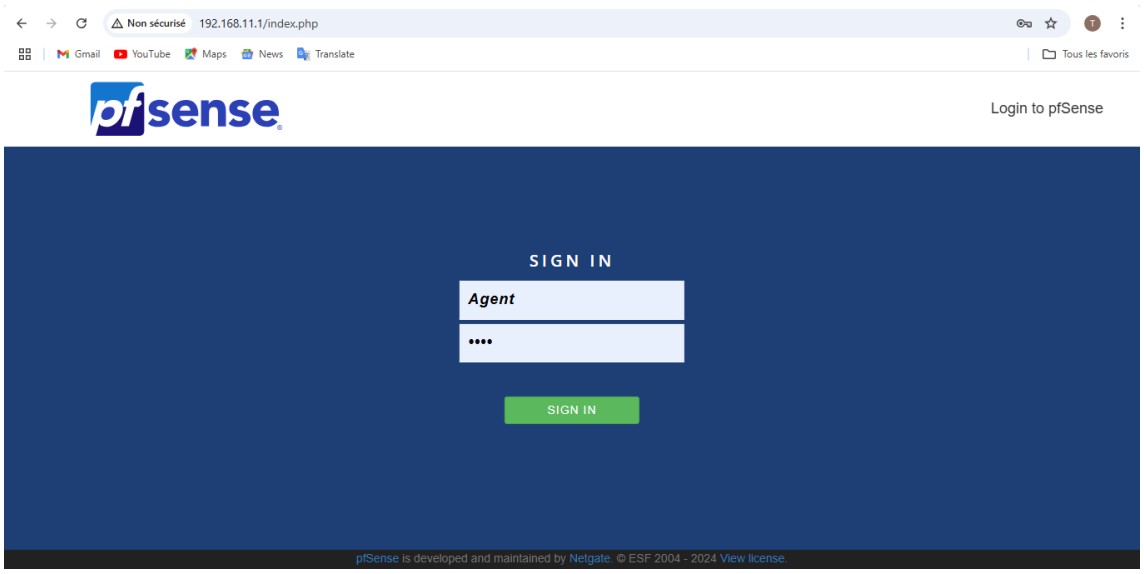


FIGURE 3.5 : Utilisateur "Agent"

Tableau de bord restreint. Seules les fonctions de création d'utilisateur et de statut du portail captif sont disponibles.

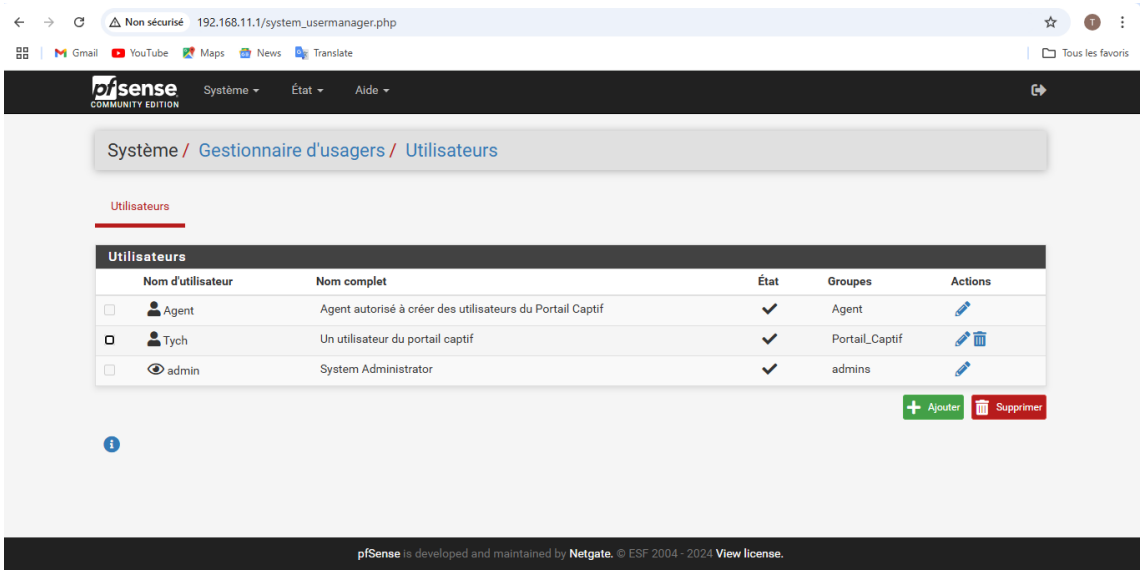


FIGURE 3.6 : Connexion de l'utilisateur

Le « statut du portail captif » permet de voir les utilisateurs connectés et de les déconnecter si besoin.

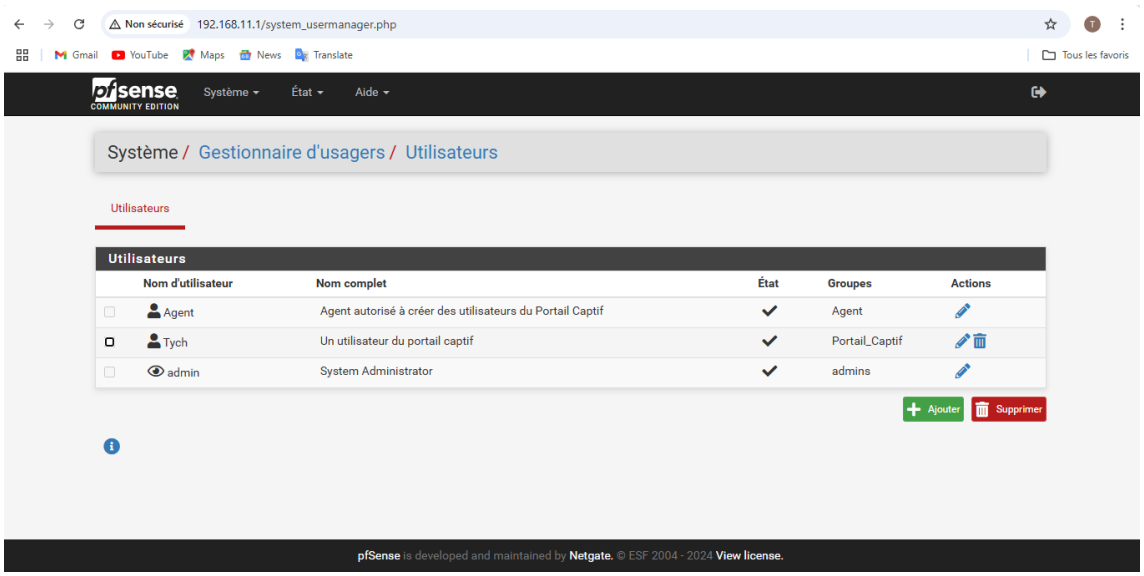


FIGURE 3.7 : Statut du portail captif

3.1.4 Authentification pour le partage de fichiers

Pour avoir accès au fichier partagé du réseau, il faut s'identifier.

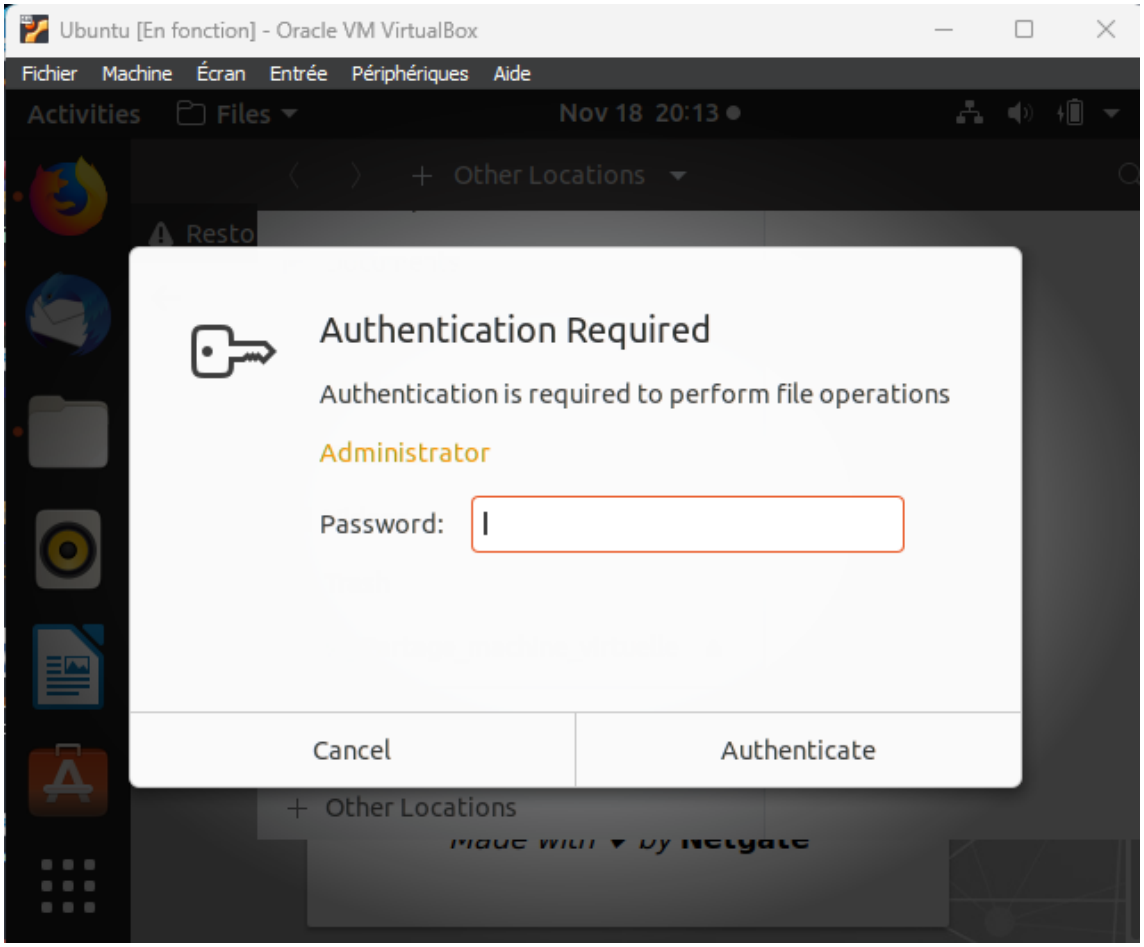


FIGURE 3.8 : Accès des fichiers

3.1.5 Configuration du serveur Proxy Squid

Après l'installation du package Squid, qui joue le rôle d'un serveur proxy (un serveur intermédiaire entre les postes utilisateurs et l'internet, et qui donne le rapport de comptabilisation des utilisateurs), nous l'avons configuré pour enregistrer les requêtes effectuées par tous les postes clients. Ensuite, nous avons cliqué sur "Services" > "Squid Proxy Server".

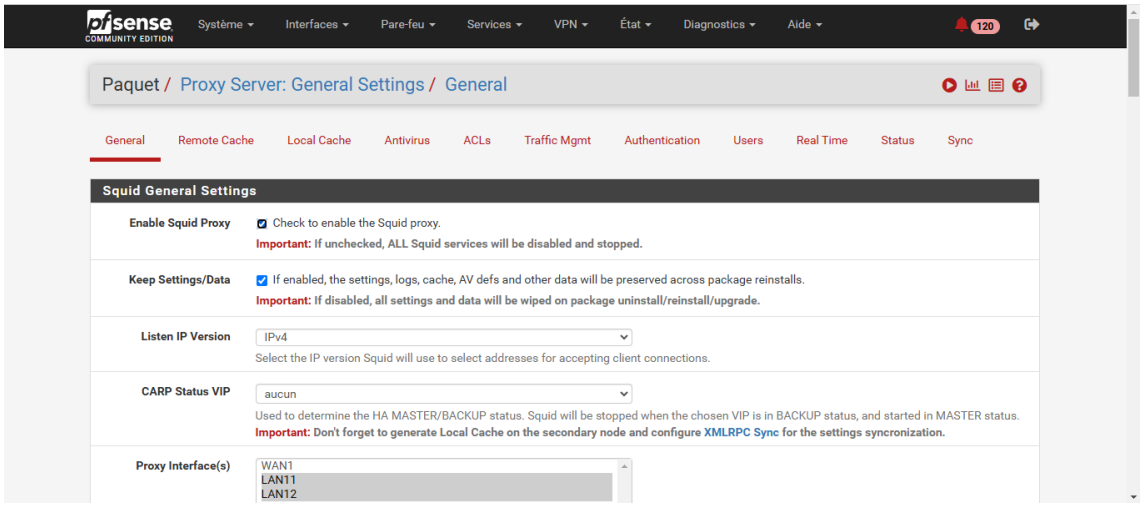


FIGURE 3.9 : Configuration de Squid

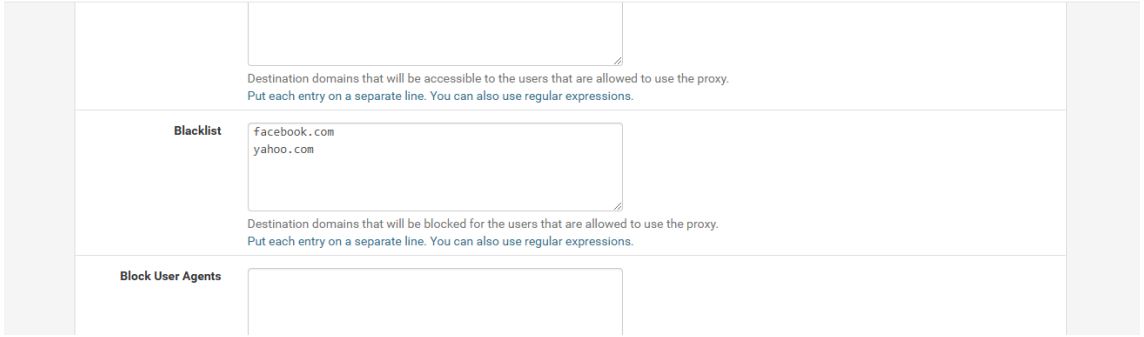


FIGURE 3.10 : Bloquer les sites

Lorsque l'utilisateur tente de se connecter à des sites non autorisés, voici le résultat.



FIGURE 3.11 : Interface d'un site bloquer

Conclusion

Ce chapitre nous a permis de décrire la conception du système que nous avons réalisée, de présenter les résultats obtenus et de mettre en évidence les limites de notre système.

Conclusion générale et perspectives

En conclusion, nous avons exploré en profondeur les nuances de la sécurisation d'un réseau d'entreprise grâce à l'implémentation judicieuse d'un portail captif de PfSense, accompagné de l'authentification RADIUS. À travers cette étude, nous avons mis en évidence les avantages notables de cette solution, tels que l'amélioration de la confidentialité des données, la gestion efficace des utilisateurs et la prévention des accès non autorisés.

Ce mémoire ne se limite pas à une simple analyse technique, mais explore également les implications pratiques de ces mesures de sécurité. L'authentification RADIUS avec le portail captif de PfSense s'est révélée être une approche prometteuse pour renforcer la protection des informations sensibles au sein des entreprises.

Tout au long de cette recherche, nous avons rencontré des défis, relevé des opportunités et développé une compréhension approfondie des mécanismes de sécurité. PfSense est un puissant firewall Open-source qui offre plusieurs possibilité pour accomplir des tâches habituellement réalisées par des solutions plus connues. C'est une solution à la hauteur pour concurrencer les plus grands car elle permet également d'implémenter des mécanismes de sécurité tel que la détection d'intrusions, la détection et le contrôle d'applications, la surveillance réseau et bien d'autres.

Bibliographie

[1] PODMILSAK, Audric. *Extended Authentication Protocol*, 2009.

[2] Duvallet Claude. *Le protocole RADIUS*, Cours-ServeurRadius, 2016.

[3] Duvallet Claude. *Architectures et Protocoles des Réseaux.*, MI-Cours-Reseau-Cours11, 2016.

[4] LESCOP Yves. *Sécurité*, Post BTS R2i, 2002.

[5] Duvallet Claude. *FreeRADIUS*, MI-Cours-Reseau-Cours11, 2016.

Webographie

[6] CommentCaMarche https://web.maths.unsw.edu.au/~lafaye/CCM/authentification/radius.htm

[7] crifa, https://www.crifa.ulg.ac.be/archives/kitnet/Ressources_eleves/Definition.htm

[8] Weodeo, https://www.weodeo.com/digitalisation/reseau-informatique-comment-ca-marche

[9] Uplink, https://www.uplink.fr/blog/informatique/quest-ce-quun-reseau-informatique#d%C3%A9finition%20Du%20R%C3%A9seau%20Informatique

[10] Openclassrooms, https://openclassrooms.com/forum/sujet/simulez-vos-architectures-reseaux-avec-gns3

[11] Ecomputernotes, https://ecomputernotes.com/computernetworkingnotes/services-and-applications/internet-architecture, Consulté le 15/09/2020.

[12] Redhat, *Qu'est-ce qu'une infrastructure informatique ?*, https://www.redhat.com/fr/topics/cloud-computing/what-is-it-infrastructure, Consulté le 20/08/2022.

[13] Geekflare, *Learn network security.*, https://geekflare.com/fr/learn-network-security/, Consulté le 15/09/2020.

[14] GeeksforGeeks, *What is Network Access Control ?*, https://www.geeksforgeeks.org/what-is-network-access-control/, Consulté le 20/09/2020.

[15] GeeksforGeeks, *What is Network Access Control ?*, https://media.geeksforgeeks.org/wp-content/uploads/20221221160947/PrincipleElementsOfNac.jpg, Consulté le 20/09/2020.

[16] Clicours, *Etude et mise en place d'un portail captif – Apprendre en ligne*, https://www.clicours.com/etude-et-mise-en-place-dun-portail-captif/, Consulté le 20/09/2020.

[17] Ameer93, *PORTAIL-CAPTIF*, http://ameer93.free.fr/wp-content/uploads/2016/10/PORTAIL-CAPTIF.pdf., Consulté le 20/09/2020.

[18] OSTEC | Segurança digital de resultados, *Get to know 6 best practices for applying a Captive Portal* https://ostec.blog/en/general/best-practices-captive-portal/, Consulté le 20/09/2020.

[19] boowiki.info, *portail captif. logiciel portail captif, matériel portails captifs*, https://boowiki.info/art/les-theories-du-reseau/portail-captif.html, Consulté le 20/09/2020.

[20] Wikipédia, *Portail captif*, https://fr.wikipedia.org/wiki/Portail_captif, Consulté le 20/09/2020.

[21] Adacis formation pfsense, *Formation-fw-Pfsense*, https://www.adacis.net/formation-fw-pfsense-003/, Consulté le 20/09/2020.

[22] Github, *zeroshell a linux distibution for network management*, https://mawuen.github.io/2020/07/16/zeroshell-a-linux-distibution-for-network-management/#fonctionalites-principales, Consulté le 20/09/2020.

[23] ChilliSpot, *Open Source Captive Portal*, http://www.chillispot.org/, Consulté le 20/09/2020.

[24] Everybodywiki, *ALCASAR*, https://everybodywiki.com, Consulté le 20/09/2020.

[25] Zeroshell, *Fin de Vie de Zeroshell– Routeur Linux Zeroshell*, https://www.zeroshell.org/zeroshell-end-of-life/, Consulté le 20/09/2020.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux vii

Liste des acronymes viii

Glossaire 1

Introduction 2
0.1 Contexte et justification . . . 2
0.2 Problématique . . . 2
0.3 Objectif . . . 3
0.4 Organisation du travail . . . 3

1 Revue de littérature 4
Introduction . . . 4
1.1 Sécurité Informatique . . . 4
1.2 Réseau Informatique . . . 4
1.2.1 Les types de réseaux . . . 5
1.3 Internet . . . 6
1.3.1 Mode de fonctionnement d'Internet . . . 6
1.3.2 Infrastructure d'accès internet sécurisée . . . 7
1.4 Sécurité réseau . . . 7
1.5 Le contrôle d'accès . . . 8
1.5.1 Principaux éléments du NAC (Network Access Control) . . . 8
1.6 Le protocole RADIUS . . . 10
1.6.1 Mode de fonctionnement . . . 10
1.7 Le portail Captif . . . 11
1.7.0.1 Principe et fonctionnement d'un portail captif . . . 11

2 Solution et choix techniques 15
Introduction . . . 15

2.1 Description de la solution . . . 15
2.2 Aperçu des principaux solutions de portails captifs . . . 15
2.2.1 Pfsense . . . 16
2.2.2 ALCASAR . . . 16
2.2.3 ZeroShell . . . 16
2.2.4 ChilliSpot . . . 16
2.3 Comparaison des portails captifs . . . 17
2.4 Architecture du réseau . . . 19
2.5 Étapes de mise en œuvre . . . 19
2.6 Installation de VirtualBox . . . 19
2.7 Installation de Pfsense . . . 21
2.8 Implémentation de FreeRadius . . . 23
2.8.1 Configuration du serveur DHCP . . . 23
2.8.2 Configuration d'un Alias . . . 24
2.8.3 Configuration de règles de Pare-feu . . . 24
2.8.4 Configuration de FreeRadius . . . 25
2.8.4.1 Définition des clients RADIUS . . . 25
2.8.4.2 Configuration des utilisateurs . . . 26
2.8.4.3 Définition du serveur Radius comme serveur d'authentification . . . 26
2.9 Création du portail Captif . . . 27
Conclusion . . . 28

3 Mise en œuvre du réseau, résultats et discussions 29
Introduction . . . 29
3.1 Tests . . . 29
3.1.1 Commande ping pour le test . . . 29
3.1.2 Connexion sur le portail captif . . . 29
3.1.3 Configuration du Groupe et des Utilisateurs pour la délégation du Portail Captif 31
3.1.4 Authentification pour le partage de fichiers . . . 33
3.1.5 Configuration du serveur Proxy Squid . . . 34
Conclusion . . . 34

Conclusion générale et perspectives 36

Bibliographie 37

Webographie 38

Table des matières 40