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 : Sécurité Informatique

Présenté par :
Bernard Ulrich **RODRIGUEZ**

Implémentation d'un Réseau Sécurisé avec pfSense: Étude de la Sécurisation des Communications

Sous la supervision :
Ing Victor **OYETOLA**

Membres du jury :

SAHO Nelson	Docteur	IFRI	Président
HOUZANMIN Vladimir	Ingénieur	IFRI	Examinateur
OYETOLA Victor	Ingénieur	IFRI	Rapporteur

Année Académique : **2023-2024**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract iv

Table des figures v

Liste des tableaux vi

Liste des acronymes vii

Glossaire 1

Introduction 2

1 État de l'art 5

2 Présentation de la solution 17

3 Conception et mise en œuvre de la solution 27

Conclusion 37

Bibliographie 38

Table des matières 40

Dédicace

Je dédie cette œuvre à :

Mon père RODRIGUEZ Patrick
Ma mère GBEGNON Annick
Mes frères et sœurs

Je dédie ce travail à : Mes très chers parents : RODRIGUEZ Patrick GBEGNON Annick qui ont investi leur temps et leur énergie pour me soutenir dans mon apprentissage durant ces longues années. Monsieur Victor OYETOLA qui fut mon encadreur à l'université. À mon frère et mes sœurs qui ne manquent pas de me soutenir.

Remerciements

Je remercie Dieu pour m'avoir prêté vie et gardé en bonne santé, sans quoi ce travail n'aurait abouti.

• Je transmets mes mots de remerciement à l'ensemble des membres de l'administration de l'Institut de Formation et de Recherche en Informatique et en particulier à Monsieur Eugène C. EZIN, le directeur de l'institut pour cette formation de qualité que nous avons pu recevoir durant ces trois années d'apprentissage.

• Mes sincères remerciements à mon maître de mémoire Monsieur Victor OYETOLA, pour m'avoir accordé son temps et pour m'avoir suivi durant la réalisation de ce travail.

• Mes sincères remerciements à tout le staff de la Direction des Systèmes d'Informations (DSI) du Ministère de l'Économie et des Finances (MEF) qui m'a accueilli pour mon stage académique et a su m'offrir un cadre adéquat pour la réalisation de mon mémoire.

• Et en fin mes mots de remerciements vont à l'endroit de toute personne ayant contribué d'une quelconque manière à la réalisation de ce travail.

Résumé

Ce mémoire explore l'implémentation d'un réseau sécurisé en utilisant pfSense, une solution open source basée sur FreeBSD, pour améliorer la sécurité des communications, un enjeu crucial pour toute organisation moderne. pfSense a été choisi pour ses fonctionnalités avancées de pare-feu, son support VPN intégré et sa robustesse. Le travail se concentre sur l'utilisation du protocole IPsec pour garantir des communications chiffrées et sécurisées, assurant l'intégrité, la confidentialité et l'authentification des données échangées. Une analyse comparative des solutions de pare-feu open source disponibles a été réalisée, mettant en évidence les avantages de pfSense. Le processus de configuration de pfSense est détaillé, incluant la mise en place de tunnels VPN IPsec, avec un accent sur les meilleures pratiques pour maximiser la sécurité et la performance du réseau. Les résultats obtenus démontrent que pfSense, associé à IPsec, fournit une solution fiable, robuste et économique pour sécuriser les communications en entreprise.

Mots clés : Sécurité réseau, pfSense, IPsec, VPN, pfSense

Abstract

This thesis explores the implementation of a secure network using pfSense, an open source solution based on FreeBSD, to improve communications security, a crucial issue for any modern organization. pfSense was chosen for its advanced firewall features, integrated VPN support and robustness. The work focuses on the use of the IPsec protocol to guarantee encrypted and secure communications, ensuring the integrity, confidentiality and authentication of exchanged data. A comparative analysis of available open source firewall solutions has been carried out, highlighting the advantages of pfSense. The pfSense configuration process is detailed, including the setting up of IPsec VPN tunnels, with a focus on best practices for maximizing network security and performance. The results demonstrate that pfSense, combined with IPsec, provides a reliable, robust and cost-effective solution for securing corporate communications.

Key words: Network security, pfSense, IPsec, VPN, pfSense

Table des figures

1 Organigramme structurel de la DSI [1] 4

1.1 Défense en profondeur [2] 6
1.2 SOURCEFORGE [3] 14

2.1 pfSense Firewall 17
2.2 Architecture du réseau utilisé 22
2.3 GNS3 24
2.4 Packet tracer 24
2.5 Vmware 25
2.6 VirtualBox 26

3.1 Présentation GNS3 27
3.2 Création de passerelle sur pfSense du Site A 29
3.3 Création de route statique sur pfSense du Site A 29
3.4 Création de passerelle sur pfSense du Site B 29
3.5 Création de route statique sur pfSense du Site B 30
3.6 Configuration de phase 1 pour le VPN IPSec sur pfSense A 30
3.7 Configuration de phase 1 pour le VPN IPSec sur pfSense B 30
3.8 Configuration de phase 2 pour le VPN IPSec sur pfSense A 31
3.9 Configuration de phase 2 pour le VPN IPSec sur pfSense 31
3.10 Règles de pare-feu sur l'interface IPSec du pfSense A 32
3.11 Règles de pare-feu sur l'interface IPSec du pfSense B 32
3.12 Règles de pare-feu sur l'interface WAN du pfSense A 32
3.13 Règles de pare-feu sur l'interface WAN du pfSense B 32
3.14 Interface de connexion d'IPsec sur pfSense A 33
3.15 Interface de connexion d'IPsec sur pfSense B 33
3.16 Connexion de phase 1 et 2 pour le VPN IPSec du site A 33
3.17 Connexion de phase 1 et 2 pour le VPN IPSec du site B 33
3.18 Ping du 192.168.1.101 ==> 192.168.10.100 34
3.19 Ping du 192.168.10.100 ==> 192.168.1.101 34

Liste des tableaux

1.1 Benchmarking comparatif entre pfSense et autres solutions 15

Liste des acronymes

AAA : Authentication Authorization Accounting
ACL : Access Control List
AD : Assistant du Directeur des Systèmes d'Information

DA : Division Application
DD : Division Datacenter
DE : Division Exploitation
DEC : Division Expérience Client
DEI : Division E-Services et Interopérabilité
DGDDI : Direction Générale des Douanes et Droits Indirects
DGI : Direction Générale des Impôts
DGML : Direction Générale du Matériel et de la Logistique
DGS : Division de Gestion des Savoirs
DHCP : Dynamic Host Configuration Protocol
DIR : Division Infrastructures et Réseaux
DMZ : Demilitarized Zone
DNS : Domain Name System
DPA : Division de Pré-Archivage
DPP : Direction de la Programmation et de la Prospective
DRFM : Direction des Ressources Financières et du Matériel
DRH : Direction des Ressources Humaines
DS : Division Systèmes
DSI : Direction des Systèmes d'Information

FAGACE : Fonds Africain de Garantie et de Coopération Economique
FTP : Ministère de l'Économie et des Finances

H-IDS : Host Based Intrusion Detection System
Helpdesk : Division Helpdesk
HTTP : Hyper Text Transfer Protocol

IDS : Intrusion detection System
IGF : Inspection Générale des Finances
IP : Chargés de Programmes de Proximité Digitale
IP : Internet Protocol

IPsec : Internet Protocol Security
ISO : International Standard Organization

LAN : Local Area Network
LNB : Loterie Nationale du Bénin

MAC : Media Access Control
MAN : Metropolitan Area Network
MEF : Ministère de l'Économie et des Finances
MR/BOAD : Mission Résidente de la Banque Ouest-Africaine de Développement

NAT : Network Address Translation

OSI : Open System Interconnect

pfSense : Packet Filter Sense
PMO/USP : Unité de Suivi des Projets
PRMP : Personne Responsable des Marchés Publics

RSCP : Responsable du Suivi des Carrières du Personnel
RSSI : Responsable de la Sécurité des Systèmes d'Information

SA : Secrétariat Administratif
SAeS : Service Applications et e-Services
SEP : Service Exploitation et Postes de Travail
SGAM : Secrétaire Général Adjoint du Ministère
SGM : Secrétaire Général du Ministère
SI : Système d'Information
SIS : Service des Infrastructures et Systèmes
SP : Secrétariat Particulier
SPAGS : Service de Pré-Archivage et de Gestion des Savoirs
SPM : Service du Protocole du Ministère

TCP : Transmission Control Protocol

UDP : User Datagram Protocol
UGR : Unité de Gestion des Ressources
UT-FED : Unité Technique d'Appui à l'Ordonnateur National du Fonds Européen de Développement

VLAN : Virtual Local Area Network
VPN : Virtual Private Network

WAN : Wide Area Network

Glossaire

Pare-feu : Un dispositif ou un logiciel qui contrôle le trafic réseau en filtrant les paquets et en appliquant des règles de sécurité pour protéger le réseau.

NAT : La traduction d'adresse réseau permet de convertir les adresses IP privées en adresses IP publiques et vice versa pour permettre la communication entre différents réseaux.

GUI : Interface utilisateur graphique (Graphical User Interface) qui fournit une interface visuelle conviviale pour interagir avec pfSense.

CLI : Interface en ligne de commande (Command Line Interface) qui permet d'interagir avec pfSense en utilisant des commandes textuelles.

Introduction générale

Dans le monde moderne des affaires, la sécurité des réseaux est essentielle pour protéger les données sensibles, prévenir les intrusions et garantir des communications sécurisées. Avec l'augmentation des cybermenaces, les entreprises doivent adopter des infrastructures réseau robustes et sécurisées. Le système d'information, comprenant des ressources telles que serveurs et ordinateurs, est crucial pour l'efficacité opérationnelle, nécessitant une surveillance et une protection constante.

Problématique

Face à la multiplication des cybermenaces et des attaques sophistiquées, comment une entreprise peut-elle sécuriser efficacement ses communications internes et externes tout en garantissant la confidentialité, l'intégrité et la disponibilité de ses données ? Quelles sont les solutions les plus adaptées pour mettre en place une infrastructure réseau sécurisée, et comment pfSense peut-il répondre à ces exigences de sécurité de manière fiable et économique ?

Contexte et justification

La sécurisation des réseaux informatiques est devenue une préoccupation essentielle pour les organisations, en raison des échanges de données fréquents et cruciaux qu'elles effectuent quotidiennement. L'adoption de solutions open source permet de bénéficier de fonctionnalités avancées de sécurité sans les coûts élevés des solutions propriétaires.
Afin de garantir une sécurité optimale des communications, il est essentiel de mettre en place des technologies et des concepts de sécurité avancés tels que les VPN (OpenVPN, IPsec).
C'est dans cette perspective que s'inscrit notre étude, qui vise à implémenter un réseau sécurisé avec pfSense pour étudier la sécurisation des communications.

Objectifs

L'objectif principal de notre étude est d'implémenter un réseau sécurisé utilisant pfSense pour garantir des communications sécurisées. Cette solution devra répondre aux besoins spécifiques suivants :
- Authentification des extrémités

- Confidentialité des données échangées
- Intégrité des données échangées
- Protection contre les écoutes et analyses de trafic
- Protection contre le rejeu

Présentation de la DSI du MEF

La Direction des Systèmes d'Information (DSI) nouvelle appellation de la Direction de l'Informatique et du Pré-archivage (DIP) assure, en relation avec toutes les structures du Ministère assure la conception, la mise en œuvre, la coordination et le suivi évaluation d'actions intégrées visant à :

- Organiser et coordonner les activités informatiques de toutes les structures du Ministère ;

- Assurer la fluidité et l'accessibilité de l'information ;

- Garantir la sécurisation formelle, l'authentification et la sauvegarde des documents administratifs et autres productions intellectuelles ;

- Faciliter les relations entre les directions techniques et les usagers/clients pour un service public efficace et efficient ;

- Proposer la politique informatique du Ministère et veiller à sa mise en œuvre ;

- Piloter la mise en œuvre du schéma directeur informatique du Ministère (Plan d'Evolution du Système d'Information) ;

- Concevoir et réaliser des applications spécifiques pour toutes les structures relevant du Ministère ou d'autres Institutions de l'Etat ;

- Aligner les technologies de l'information avec les objectifs stratégiques du Ministère ;

- Évaluer l'organisation et les procédures du Ministère et proposer le cas échéant, les solutions optimales de réorganisation et de modernisation ;

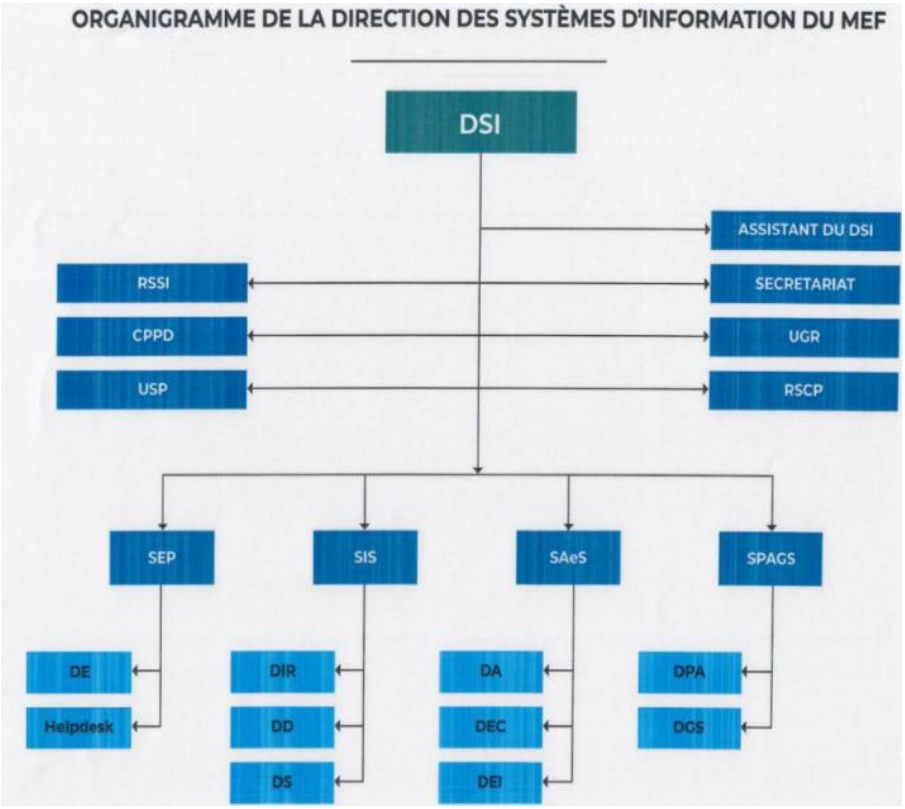
- Proposer la politique archivistique et de gestion des savoirs et veiller à sa mise en œuvre ; - Garantir la mémoire du Ministère par le développement et la préservation de son patrimoine archivistique et documentaire ;

- Définir les normes et standards en matière de classement, de description, de conservation, d'élaboration de référentiels, d'outils de gestion des documents, quels que soient leurs supports matériels et d'instruments de dématérialisation ; - Faciliter les relations entre les directions techniques et les usagers/clients de manière à donner une satisfaction maximale à ces derniers ;

- Dynamiser le Standard Central du Ministère.

Les services rattachés à la Direction des Systèmes d'Information sont représentés sur la figure suivante :

FIGURE 1 : Organigramme structurel de la DSI [1]



Activités menées à la DSI

Au cours de notre stage au sein du département Service et Infrastructure Système (SIS) de la DSI, j'ai eu l'opportunité de renforcer mes compétences en interventions techniques. De plus, ce stage académique m'a permis de mener à bien l'expérimentation de la solution pfSense, avec succès.

Organisation du mémoire

Les conclusions de cette recherche se déclinent en trois parties. Le premier chapitre traite de l'état de l'art. Le deuxième chapitre se penche sur la présentation de la solution. Enfin, le troisième chapitre met en lumière une mise en pratique concrète de la solution proposée.

Chapitre 1

État de l'art

Introduction

Ce chapitre analyse et compare plusieurs solutions open source de sécurisation des réseaux, telles qu'OpenWrt, OPNsense, IPFire, et pfSense. L'objectif est d'évaluer leurs fonctionnalités, performances, facilité d'installation et support communautaire pour justifier le choix de pfSense comme solution optimale pour la sécurisation des communications.

1.1 Sécurité du réseau : concepts et enjeux

1.1.1 Principes de Sécurité des Réseaux [4]

Les principes de sécurité des réseaux sont des concepts fondamentaux qui guident la conception, la mise en œuvre et la gestion des infrastructures réseau afin de protéger les données, les systèmes et les utilisateurs contre les menaces potentielles. Voici quelques principes clés de sécurité des réseaux :
1. Confidentialité : La confidentialité vise à assurer que les données sensibles ne sont accessibles qu'aux personnes autorisées. Cela implique l'utilisation de techniques de chiffrement pour empêcher toute interception ou visualisation non autorisée des données en transit.
2. Intégrité : L'intégrité garantit que les données ne sont pas modifiées de manière non autorisée pendant leur transmission ou leur stockage. Les mécanismes de vérification d'intégrité détectent toute altération non autorisée des données.
3. Disponibilité : La disponibilité assure que les ressources réseau et les services sont accessibles lorsque nécessaire. Les mesures de disponibilité incluent la mise en place de redondances, la prévention des attaques par déni de service (DDoS) et la planification de la reprise après sinistre.
4. Authentification : L'authentification vérifie l'identité d'un utilisateur, d'un appareil ou d'un système avant d'accorder l'accès. Cela peut impliquer l'utilisation de mots de passe, de certificats numériques, de biométrie ou d'autres méthodes d'identification.
5. Autorisation : Une fois qu'un utilisateur est authentifié, l'autorisation détermine les ressources et les actions auxquelles cet utilisateur a le droit d'accéder. Cela implique la mise en place de rôles et de permissions pour contrôler les privilèges d'accès.
6. Audit : L'audit consiste à enregistrer et à surveiller les activités effectuées sur le réseau et les sys-

tèmes. Les journaux d'audit permettent de détecter les comportements suspects, de suivre les actions des utilisateurs et de faciliter l'enquête en cas d'incident.

7. Principe du Moindre Privilège : Ce principe consiste à accorder aux utilisateurs et aux systèmes uniquement les privilèges nécessaires pour accomplir leurs tâches spécifiques. Cela réduit le risque en limitant l'exposition potentielle en cas de compromission.

8. Segmentation du Réseau : La segmentation consiste à diviser le réseau en segments logiques pour limiter la propagation des menaces. Les segments isolent les ressources sensibles et permettent un contrôle plus précis du trafic.

Mise à jour et Patching : Maintenir les systèmes et les logiciels à jour avec les derniers correctifs de sécurité est essentiel pour réduire les vulnérabilités et protéger contre les attaques connues.

10. Formation et Sensibilisation : La formation des utilisateurs et du personnel de l'organisation sur les bonnes pratiques de sécurité est cruciale pour minimiser les risques liés aux erreurs humaines et aux attaques de type phishing.

En adoptant ces principes dans la conception et la gestion d'un réseau, nous pouvons renforcer la sécurité globale et réduire les risques de cyberattaques et de violations de données.

1.1.2 Principes de défense en profondeur et de gestion de la sécurité

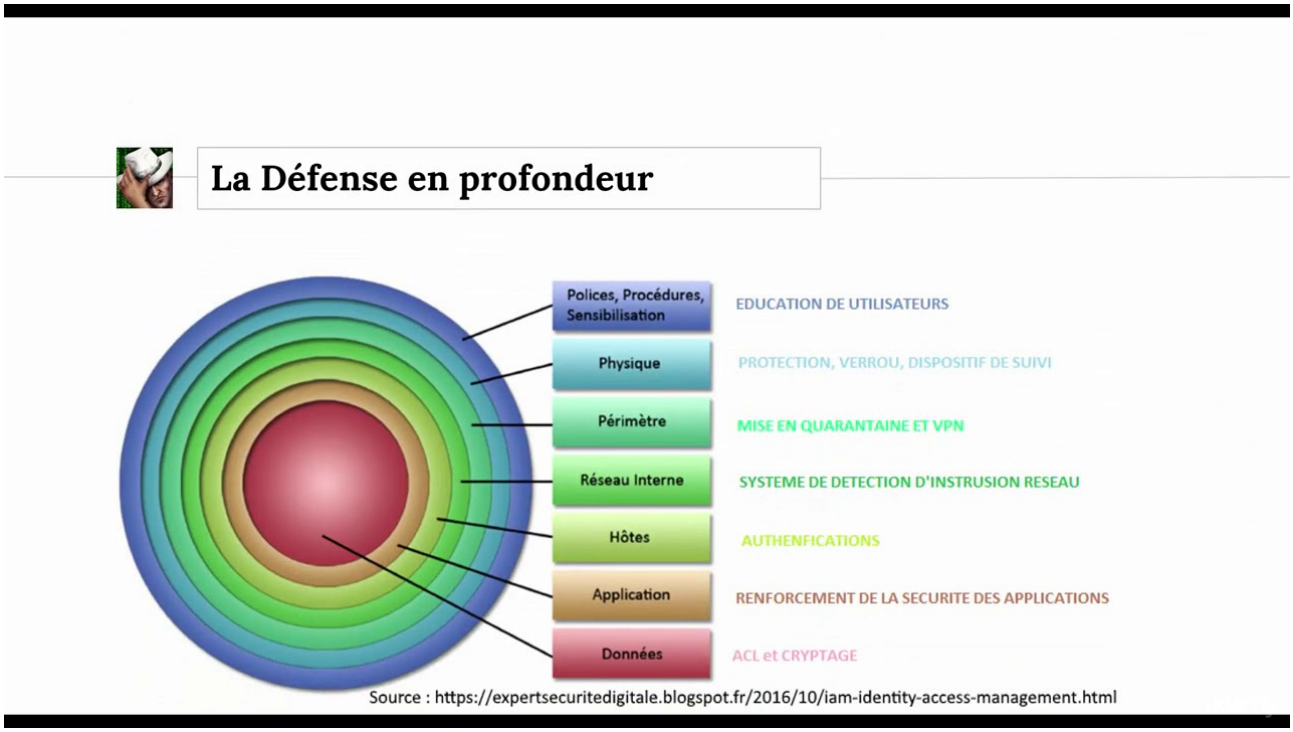


FIGURE 1.1 : Défense en profondeur [2]

La défense en profondeur est une approche de sécurité qui consiste à superposer plusieurs couches de sécurité pour renforcer la protection d'un réseau. Cela comprend des mesures telles que la segmentation du réseau, la mise en place de pare-feu, de détection d'intrusion, de chiffrement des données, d'authentification forte, etc. La gestion de la sécurité implique la planification, la mise en œuvre et la surveillance de ces mesures pour assurer une sécurité efficace et continue du réseau.

1.1.3 Politiques de sécurité et processus de gestion [5]

Les politiques de sécurité et les processus de gestion sont des éléments essentiels de la gestion de la sécurité de l'information au sein d'une organisation. Ils fournissent le cadre nécessaire pour protéger les actifs et les données sensibles de l'organisation, gérer les risques de sécurité et garantir la conformité aux réglementations applicables. Voici une explication plus détaillée de ces deux concepts :

1. Politiques de sécurité :

Les politiques de sécurité sont des directives et des règles qui définissent les objectifs, les principes et les responsabilités en matière de sécurité de l'information au sein de l'organisation. Elles sont élaborées pour établir une approche cohérente de la sécurité et pour guider les actions des employés. Les politiques de sécurité couvrent différents aspects de la sécurité de l'information, tels que la gestion des accès, la classification des données, la gestion des risques, la sensibilisation à la sécurité, etc. Ces politiques fournissent des instructions claires sur les comportements et les actions attendus de la part des employés pour assurer la sécurité des informations de l'organisation.

2. Processus de gestion :

Les processus de gestion de la sécurité de l'information sont des méthodes structurées pour mettre en œuvre, maintenir et améliorer la sécurité de l'information au sein de l'organisation. Ces processus comprennent des étapes définies, des rôles et des responsabilités assignés, ainsi que des activités spécifiques à effectuer. Par exemple, la gestion des incidents de sécurité, la gestion des changements, la gestion des risques, la gestion des accès, la sensibilisation à la sécurité, etc. Ces processus garantissent une approche systématique et cohérente de la gestion de la sécurité de l'information dans toute l'organisation.

1.1.4 Technologies et solutions de sécurité du réseau

Il existe une multitude de technologies et de solutions disponibles pour renforcer la sécurité du réseau. Cela comprend des pare-feu, des systèmes de prévention d'intrusion (IPS), des systèmes de détection d'intrusion (IDS), des systèmes de gestion des journaux, des antivirus, des VPN, etc. L'adoption et la mise en œuvre des technologies et solutions appropriées sont essentielles pour une gestion efficace de la sécurité du réseau.

1.2 Présentation des solutions open source

1.2.1 Définition et avantages des solutions open source en sécurité des réseaux

Les logiciels open source sont des programmes dont le code source est librement accessible, modifiable et redistribuable par quiconque. Cela contraste avec les logiciels propriétaires, où le code source est fermé et les utilisateurs n'ont pas le droit de le modifier.

Avantages des solutions open source en sécurité des réseaux :

- Coût réduit : Les solutions open source sont généralement gratuites, ce qui permet aux entreprises de réduire les coûts liés aux licences logicielles.

- Flexibilité : Les utilisateurs peuvent modifier le code source pour répondre à leurs besoins spécifiques.

- Sécurité : Avec de nombreuses paires d'yeux examinant le code, les vulnérabilités peuvent être

identifiées et corrigées plus rapidement.
- Support communautaire : Les projets open source bénéficient souvent d'une large communauté d'utilisateurs et de développeurs qui partagent des conseils, des solutions et des améliorations.
- Transparence : L'accès au code source permet aux utilisateurs de vérifier par eux-mêmes l'absence de portes dérobées et de comprendre exactement ce que fait le logiciel.

1.2.2 Critères de sélection des solutions à étudier

Pour l'étude des solutions open source de sécurisation des réseaux, nous avons retenu les critères suivants :
- Fonctionnalités de sécurité : Capacité à offrir des fonctionnalités essentielles telles que le pare-feu, le VPN, le NAT, etc.
- Performance : Efficacité et capacité à gérer un trafic réseau important sans compromettre la sécurité.
- Facilité d'installation et de configuration : Simplicité du processus d'installation et des options de configuration.
- Communauté et support : Taille et activité de la communauté d'utilisateurs et de développeurs. - Coûts et licences : Modèle économique et coût total de possession.

1.3 Analyse des Principales Solutions Open Source

1.3.1 OpenWrt [6]

Présentation :
OpenWrt est un projet open source visant à créer un système d'exploitation pour routeurs et autres dispositifs embarqués. Il est connu pour sa flexibilité et ses capacités de personnalisation.
Caractéristiques :
1. Plateformes supportées
OpenWrt prend en charge une grande variété de plateformes matérielles, notamment les architectures x86, ARM et MIPS. Cela en fait une solution flexible pouvant être déployée sur différents types de matériel, des routeurs domestiques aux équipements réseau professionnels.
2. Facilité d'utilisation
L'interface utilisateur d'OpenWrt est moins intuitive et plus technique comparée à certaines autres solutions de firewall. Cela peut représenter un défi pour les utilisateurs novices, mais elle offre une grande flexibilité pour les utilisateurs avancés qui ont besoin d'une configuration fine et personnalisée.
3. Fonctionnalités de sécurité
OpenWrt fournit des fonctionnalités de sécurité de base qui peuvent être étendues grâce à l'ajout de packages supplémentaires. Il est possible d'installer des outils comme les pare-feu avancés, les systèmes de détection d'intrusion, et d'autres logiciels de sécurité pour renforcer la protection du réseau.
4. Performance
OpenWrt est optimisé pour le routage et offre des performances élevées, en particulier pour les

connexions sans fil. Son architecture modulaire permet d'optimiser l'utilisation des ressources matérielles, ce qui le rend idéal pour les environnements nécessitant un haut débit et une faible latence.

5. Personnalisabilité

OpenWrt est extrêmement personnalisable. Grâce à un large choix de packages disponibles, les utilisateurs peuvent ajouter et configurer des fonctionnalités spécifiques selon leurs besoins. Cette modularité permet une adaptation fine de la solution à divers cas d'utilisation.

6. Communauté et Support

OpenWrt bénéficie d'une grande communauté active. Cette communauté fournit une documentation extensive et de nombreux forums de support où les utilisateurs peuvent trouver de l'aide et partager leurs expériences. La large base d'utilisateurs contribue également au développement continu et à l'amélioration du logiciel.

7. Fréquence des mises à jour

OpenWrt reçoit des mises à jour régulières qui incluent des améliorations de sécurité et de nouvelles fonctionnalités. Cette fréquence assure que le système reste sécurisé et à jour avec les dernières technologies et vulnérabilités connues.

8. Support VPN

OpenWrt supporte les VPN, notamment OpenVPN et WireGuard. Ces fonctionnalités VPN permettent de sécuriser les communications réseau et de créer des tunnels sécurisés entre différents points du réseau.

9. Exigences matérielles

OpenWrt a des exigences matérielles modestes, ce qui le rend compatible avec une large gamme d'appareils. Les spécifications minimales incluent un CPU de 400MHz, 64MB de RAM et 16MB de stockage, ce qui permet de l'installer sur du matériel moins puissant tout en offrant des performances adéquates.

OpenWrt est donc une solution très flexible et performante, particulièrement adaptée pour les utilisateurs avancés et les environnements nécessitant une gestion fine et une performance élevée en termes de routage et de connexion sans fil.

Fonctionnalités :

- Pare-feu basé sur iptables : OpenWrt utilise iptables pour fournir des fonctionnalités de pare-feu robustes.
- Support VPN (OpenVPN, WireGuard) : OpenWrt prend en charge divers protocoles VPN, notamment OpenVPN et WireGuard, pour sécuriser les communications.
- QoS (Quality of Service) : Il offre des fonctionnalités QoS pour gérer la bande passante et prioriser le trafic réseau.
- Support matériel étendu : OpenWrt est compatible avec une large gamme de routeurs et autres équipements réseau.

Avantages :

- Grande flexibilité et personnalisation
- Large support matériel

Inconvénients :

- Courbe d'apprentissage élevée pour les nouveaux utilisateurs
- Interface utilisateur moins conviviale comparée à d'autres solutions

1.3.2 OPNsense [7]

Présentation :
OPNsense est une distribution open source de pare-feu et de routeur, dérivée de pfSense, avec un accent sur la sécurité et la facilité d'utilisation.
Caractéristiques :
1. Plateformes supportées
OPNsense est conçu pour fonctionner principalement sur des plateformes x86-64. Cettecompatibilité permet de l'installer sur une large gamme de matériel, des petits routeurs domestiques aux serveurs d'entreprise plus puissants.
2. Facilité d'utilisation
OPNsense est reconnu pour son interface utilisateur moderne et intuitive. La navigation et la configuration sont simplifiées grâce à un tableau de bord bien organisé et des menus clairs, rendant cette solution accessible aussi bien aux débutants qu'aux utilisateurs avancés.
3. Fonctionnalités de sécurité
OPNsense propose des fonctionnalités de sécurité avancées, telles que la détection et la prévention d'intrusion (IDS/IPS), le blocage géographique (GeoIP), et des plugins antivirus. Ces outils permettent de sécuriser efficacement le réseau contre une variété de menaces.
4. Performance
OPNsense offre une haute performance grâce à une optimisation logicielle efficace. Il supporte le multi-threading et peut gérer des charges de travail élevées, ce qui le rend adapté aux environnements nécessitant une gestion de trafic intense et une faible latence.
5. Personnalisabilité
OPNsense est hautement personnalisable grâce à son système de plugins. Les utilisateurs peuvent facilement ajouter ou supprimer des fonctionnalités en fonction de leurs besoins spécifiques, permettant une adaptation fine de la solution à divers scénarios d'utilisation.
6. Communauté et Support
OPNsense bénéficie d'une communauté active et d'une documentation extensive. Les utilisateurs peuvent trouver de l'aide via les forums communautaires, les guides en ligne, et les tutoriels. De plus, une documentation officielle détaillée est régulièrement mise à jour.
7. Fréquence des mises à jour
OPNsense est connu pour ses mises à jour fréquentes. Ces mises à jour incluent des correctifs de sécurité, des améliorations de performance et de nouvelles fonctionnalités, assurant que le système reste sécurisé et performant.
8. Support VPN
OPNsense supporte plusieurs types de VPN, notamment OpenVPN, WireGuard et IPsec. Ces options VPN permettent de sécuriser les communications réseau et de créer des tunnels sécurisés pour des connexions à distance fiables.
9. Exigences matérielles
OPNsense nécessite au minimum un CPU de 1GHz, 1GB de RAM et 10GB de stockage. Ces exigences matérielles modestes permettent son déploiement sur une large gamme de matériel tout en assurant une bonne performance.

En résumé, OPNsense est une solution de firewall et de routeur robuste, offrant une interface utilisateur intuitive, des fonctionnalités de sécurité avancées et une grande flexibilité grâce à son sys-

tème de plugins. Il convient aussi bien aux utilisateurs domestiques qu'aux entreprises, grâce à sa performance élevée et à son support communautaire solide.
Fonctionnalités :
- Pare-feu basé sur FreeBSD - Support VPN (IPsec, OpenVPN) - IDS/IPS (Suricata) - Proxy (Squid)
Avantages : - Interface utilisateur conviviale
- Mises à jour régulières de sécurité
- Large communauté et documentation
Inconvénients :
- Peut être moins performant sur du matériel plus ancien
- Moins de fonctionnalités par défaut comparé à pfSense

1.3.3 IPFire [8]

Présentation :
IPFire est une solution de sécurité réseau open source orientée vers la facilité d'utilisation et la sécurité.
Caractéristiques :

1. Plateformes supportées
IPFire prend en charge les architectures x86-64 et ARM, permettant ainsi son installation sur une variété de matériels, des petits dispositifs embarqués aux serveurs plus puissants. Cette flexibilité le rend adapté à divers environnements réseau.
2. Facilité d'utilisation
IPFire est réputé pour son interface utilisateur conviviale. Son GUI (interface graphique utilisateur) intuitive permet aux utilisateurs, même novices, de naviguer et de configurer facilement le système. Les options de configuration sont clairement organisées, facilitant ainsi la gestion des paramètres de sécurité et de réseau.
3. Fonctionnalités de sécurité
IPFire offre des fonctionnalités de sécurité robustes, y compris la détection et la prévention d'intrusion (IDS/IPS) via Snort, ainsi qu'un antivirus intégré avec ClamAV. Ces outils contribuent à protéger le réseau contre diverses menaces et attaques. IPFire se concentre sur la sécurisation du web avec des mises à jour régulières pour maintenir un haut niveau de sécurité.
4. Performance
IPFire offre une bonne performance globale, capable de gérer efficacement le trafic réseau dans des environnements variés. Bien que ses fonctionnalités soient moins nombreuses que certaines autres solutions, IPFire reste performant pour les usages courants, avec une gestion efficace des ressources système.
5. Personnalisabilité
La personnalisation dans IPFire est modérée. Il offre des options de configuration basiques, mais celles-ci sont suffisantes pour la plupart des besoins de sécurité réseau. Les utilisateurs peuvent facilement comprendre et appliquer des configurations grâce à une interface claire et intuitive. Les couleurs (vert pour interne, bleu pour sans fil, rouge pour externe) aident à identifier et à gérer les différentes zones du réseau.
6. Communauté et Support

IPFire dispose d'une communauté plus petite comparée à certaines autres solutions de firewall, mais elle est active et engagée. La documentation disponible est moins étendue, mais elle couvre les aspects essentiels de la configuration et de l'utilisation du système. Le support communautaire via forums et guides est disponible pour aider les utilisateurs.

7. Fréquence des mises à jour

IPFire reçoit des mises à jour régulières, principalement axées sur l'amélioration de la sécurité et la correction des bugs. Ces mises à jour fréquentes assurent que le système reste sécurisé face aux nouvelles menaces et vulnérabilités.

8. Support VPN

IPFire supporte les VPN, notamment OpenVPN et IPsec. Ces fonctionnalités permettent de sécuriser les communications réseau et de créer des tunnels sécurisés entre différents points du réseau, assurant ainsi la confidentialité et l'intégrité des données en transit.

9. Exigences matérielles

IPFire a des exigences matérielles modestes : un CPU de 1GHz, 1GB de RAM et 4GB de stockage. Ces spécifications permettent à IPFire de fonctionner sur du matériel moins puissant tout en offrant des performances adéquates pour les tâches de firewall et de routage.

En résumé, IPFire est une solution de firewall et de routeur simple et efficace, idéale pour ceux qui recherchent une interface utilisateur conviviale et des fonctionnalités de sécurité robustes sans la complexité des systèmes plus avancés. Son focus sur la sécurité web et ses mises à jour régulières en font un choix solide pour sécuriser les réseaux domestiques et de petites entreprises.

Fonctionnalités :

- Pare-feu basé sur Linux (iptables)
- IDS/IPS (Snort)
- Support VPN (IPsec, OpenVPN)
- Filtrage de contenu web

Avantages :

- Interface utilisateur intuitive
- Bonnes performances sur du matériel modeste

Inconvénients :

- Moins flexible que d'autres solutions comme OpenWrt
- Moins de plugins et de modules comparé à pfSense ou OPNsense

1.3.4 pfSense [9]

Présentation :

pfSense est une distribution open source basée sur FreeBSD, spécialement conçue pour servir de pare-feu et de routeur pour les réseaux informatiques. Réputée pour sa fiabilité, sa sécurité et sa flexibilité, pfSense est largement utilisée dans les environnements professionnels et domestiques pour sécuriser et gérer les réseaux.

Caractéristiques :

1. Plateformes supportées

pfSense est conçu pour fonctionner sur des plateformes x86-64. Cette compatibilité permet de l'instal-

ler sur une large gamme de matériel, allant des petits routeurs domestiques aux serveurs d'entreprise plus puissants.

2. Facilité d'utilisation

pfSense propose une interface utilisateur riche en fonctionnalités mais relativement complexe. Les utilisateurs peuvent configurer des paramètres détaillés, ce qui peut être intimidant pour les novices mais extrêmement puissant pour les utilisateurs avancés et les administrateurs réseau.

3. Fonctionnalités de sécurité

pfSense offre des fonctionnalités de sécurité avancées, y compris la détection et la prévention d'intrusion (IDS/IPS) avec Snort, un antivirus intégré avec ClamAV, et de nombreuses autres fonctionnalités de sécurité. Ces outils permettent de protéger efficacement le réseau contre diverses menaces et attaques.

4. Performance

pfSense est reconnu pour sa haute performance, capable de gérer des charges de travail importantes et des environnements réseau complexes. Il supporte le multi-threading et peut tirer parti des configurations matérielles avancées pour offrir une faible latence et un débit élevé.

5. Personnalisabilité

pfSense est extrêmement personnalisable grâce à un système de packages étendu. Les utilisateurs peuvent ajouter ou supprimer des fonctionnalités en fonction de leurs besoins spécifiques, permettant une adaptation fine de la solution à divers scénarios d'utilisation. Les options de configuration avancées permettent de personnaliser presque tous les aspects du firewall.

6. Communauté et Support

pfSense bénéficie d'une grande communauté active et d'une documentation très complète. Les utilisateurs peuvent trouver de l'aide via les forums communautaires, les guides en ligne, les tutoriels, et la documentation officielle. Cette base de connaissances étendue permet de résoudre rapidement les problèmes et d'optimiser les configurations.

7. Fréquence des mises à jour

pfSense reçoit des mises à jour stables mais moins fréquentes comparées à certaines autres solutions. Ces mises à jour incluent des correctifs de sécurité, des améliorations de performance et des nouvelles fonctionnalités. La politique de mise à jour met l'accent sur la stabilité et la fiabilité.

8. Support VPN

pfSense supporte plusieurs types de VPN, notamment OpenVPN, WireGuard et IPsec. Ces options VPN permettent de sécuriser les communications réseau et de créer des tunnels sécurisés pour des connexions à distance fiables, répondant ainsi aux besoins des entreprises et des utilisateurs avancés.

9. Exigences matérielles

pfSense nécessite au minimum un CPU de 1GHz, 1GB de RAM et 8GB de stockage. Ces exigences matérielles sont raisonnables et permettent de déployer pfSense sur une large gamme de matériel tout en assurant une bonne performance.

En résumé, pfSense est une solution de firewall et de routeur robuste et puissante, offrant une interface utilisateur riche en fonctionnalités, des options de sécurité avancées et une grande flexibilité grâce à son système de packages. Il convient parfaitement aux utilisateurs avancés et aux entreprises qui ont besoin de configurations détaillées et de performances élevées pour leurs environnements réseau.

Fonctionnalités :

- Pare-feu robuste : pfSense utilise le moteur de filtrage de paquets PF (Packet Filter) pour fournir des

fonctionnalités de pare-feu avancées, permettant de contrôler le trafic entrant et sortant.
- Support VPN : pfSense offre un support intégré pour les protocoles VPN tels que IPsec, OpenVPN et L2TP/IPsec, facilitant la création de tunnels VPN sécurisés pour la communication à distance.
- Détection et prévention des intrusions (IDS/IPS) : pfSense intègre des fonctionnalités d'IDS/IPS permettant de détecter et de bloquer les activités suspectes sur le réseau, renforçant ainsi la sécurité.
- Qualité de service (QoS) : pfSense permet de gérer la bande passante en appliquant des règles de priorisation du trafic, garantissant ainsi des performances optimales pour les applications critiques.
- Filtrage de contenu web

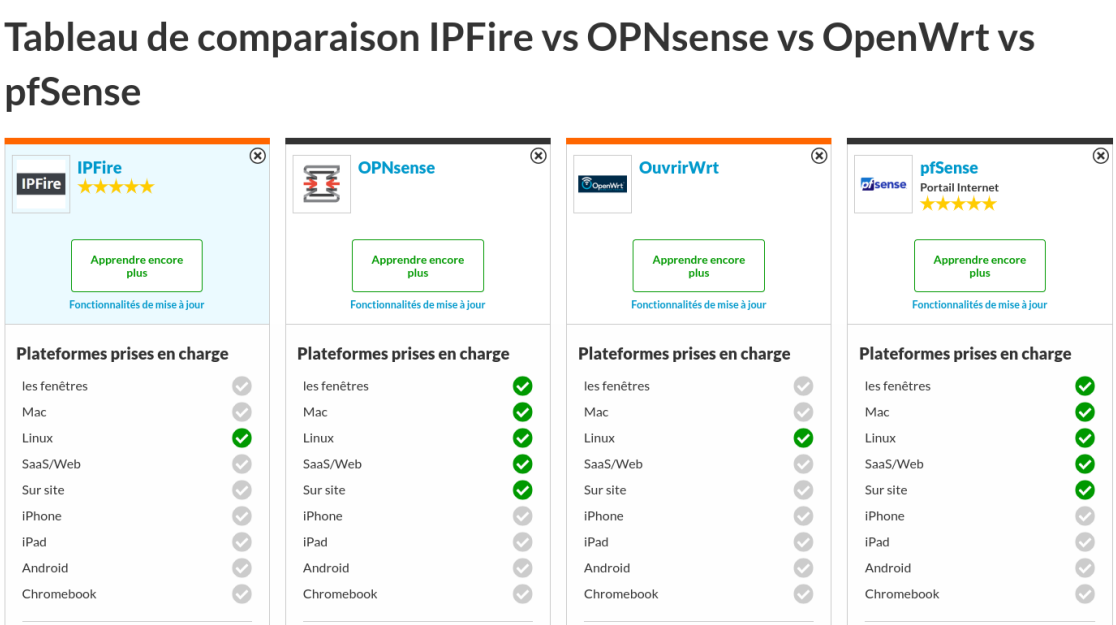
Avantages :
- Fiabilité et stabilité : pfSense est réputé pour sa robustesse et sa capacité à fonctionner de manière stable, même dans des environnements à haute charge.
- Large éventail de fonctionnalités : pfSense offre une gamme complète de fonctionnalités de sécurité et de routage, répondant ainsi aux besoins variés des entreprises et des particuliers.

Inconvénients :
- Courbe d'apprentissage : En raison de sa richesse fonctionnelle, pfSense peut présenter une courbe d'apprentissage initiale pour les nouveaux utilisateurs, en particulier pour ceux qui ne sont pas familiers avec FreeBSD ou les pare-feu.
- Configuration initiale : La configuration initiale de pfSense peut nécessiter une certaine expertise technique pour garantir une mise en place sécurisée et efficace.

1.3.5 Benchmarking comparatif entre les solutions open source

Nous avons réalisé une analyse comparative des plateformes prises en charge par chaque solution, telles que répertoriées sur SourceForge, comme illustré dans l'image ci-dessous :

FIGURE 1.2 : SOURCEFORGE [3]



Dans le tableau comparatif ci-dessous, nous examinons les principales caractéristiques et fonctionnalités de différentes solutions open source de sécurisation des réseaux, telles que pfSense, OpenWrt, OPNsense, et IPFire, pour aider à guider le choix de la solution la plus adaptée aux besoins spécifiques en matière de sécurité réseau.

TABLE 1.1 : Benchmarking comparatif entre pfSense et autres solutions

Critères	Forces	Faiblesses
IPFire	**- Interface utilisateur intuitive :** Facile à utiliser, même pour les débutants. **- Sécurité robuste :** Intégration d'un système de détection d'intrusion (IDS) pour surveiller et analyser le trafic réseau. **- Gestion des segments de réseau :** Capacité à gérer plusieurs segments de réseau avec des règles de sécurité spécifiques pour chaque segment.	**- Fonctionnalités limitées :** Moins d'options avancées comparé à pfSense et OPNsense. **- Personnalisation :** Interface utilisateur moins flexible pour les configurations réseau complexes.
OpenWrt	**- Support matériel étendu :** Compatible avec une large gamme de matériels de routeur, y compris des appareils embarqués. **- Personnalisation élevée :** Hautement configurable avec un accès à des milliers de packages pour étendre les fonctionnalités. **- Excellente prise en charge sans fil :** Performance robuste pour les réseaux sans fil, y compris le support des VLAN et PPPoE.	**- Complexité de la configuration :** Moins convivial pour les utilisateurs novices, surtout pour les configurations de pare-feu. **- Documentation :** Bien que complète, la documentation peut être complexe et difficile à naviguer pour les débutants.
OPNsense	**- Interface utilisateur moderne :** Facile à naviguer avec une interface utilisateur attrayante et intuitive. **- Sécurité complète :** Inclut des fonctionnalités avancées comme IDS/IPS, VPN, et pare-feu. **- Mises à jour régulières :** Bénéficie d'une communauté active avec des mises à jour fréquentes pour améliorer les fonctionnalités et la sécurité.	**- Complexité :** Peut être complexe à configurer pour les nouveaux utilisateurs. **- Exigences matérielles :** Nécessite du matériel plus performant pour tirer pleinement parti de toutes les fonctionnalités avancées.
pfSense	**- Riche en fonctionnalités :** Offre une gamme étendue de fonctionnalités, adaptées aux environnements professionnels et exigeants. **- Performance robuste :** Capable de gérer des flux de données élevés et des configurations réseau complexes. **- Documentation et communauté :** Large communauté d'utilisateurs et documentation exhaustive pour le support et la résolution des problèmes.	**- Interface complexe :** Courbe d'apprentissage abrupte pour les nouveaux utilisateurs. **- Configuration avancée :** Les paramètres et configurations personnalisées peuvent être difficiles à implémenter sans expertise technique.

1.3.6 Choix de la solution

Après une analyse approfondie des différentes solutions open source disponibles, à savoir OpenWrt, OPNsense, IPFire et pfSense, nous avons décidé d'opter pour pfSense pour l'implémentation d'un réseau sécurisé dans notre entreprise.

Fondement du Choix

- Fiabilité et Stabilité : pfSense est réputé pour sa fiabilité et sa stabilité. Son utilisation généralisée dans des environnements professionnels témoigne de sa capacité à maintenir des opérations réseau continues et sans faille, même dans des situations à haute charge.

- Fonctionnalités de Sécurité Avancées : pfSense offre une gamme complète de fonctionnalités de sécurité, allant d'un pare-feu robuste à des fonctionnalités avancées de détection et de prévention des intrusions (IDS/IPS). Cette richesse fonctionnelle répond à nos besoins en matière de sécurisation des communications sensibles en entreprise.

- Support VPN Intégré : La prise en charge native des protocoles VPN tels qu'IPsec, OpenVPN et L2TP/IPsec permet de mettre en place des connexions VPN sécurisées, essentielles pour les communications à distance et l'accès sécurisé aux ressources réseau.

- Large Communauté et Support Professionnel : pfSense bénéficie d'une large communauté d'utilisateurs et de contributeurs, ainsi que d'un support professionnel disponible en cas de besoin. Cette combinaison assure une assistance fiable et efficace pour la résolution de problèmes et la configuration de solutions sur mesure.

- Flexibilité et Personnalisation : pfSense offre une grande flexibilité et une capacité de personnalisation étendue, permettant de configurer précisément les paramètres de sécurité et les fonctionnalités réseau en fonction de nos besoins spécifiques.

- Coût Abordable : En tant que solution open source, pfSense est disponible gratuitement, ce qui réduit les coûts initiaux d'acquisition et de déploiement tout en offrant des fonctionnalités comparables, voire supérieures, à celles des solutions propriétaires.

En résumé, pfSense se distingue par sa fiabilité, sa sécurité, sa flexibilité et son large support communautaire, ce qui en fait le choix idéal pour sécuriser les communications en entreprise et garantir la confidentialité et l'intégrité de nos données sensibles.

Conclusion

Ce premier chapitre a permis d'analyser et comparer plusieurs solutions open source pour la sécurité réseau, notamment OpenWrt, OPNsense, IPFire, et pfSense. L'analyse des fonctionnalités, des performances, de la facilité d'installation et du support communautaire a conduit à la sélection de pfSense comme la solution la plus adaptée pour sécuriser les communications en entreprise, en raison de sa robustesse, de sa richesse fonctionnelle et de son coût abordable. Le chapitre suivant se concentrera sur l'implémentation pratique de pfSense dans un environnement d'entreprise pour garantir des communications sécurisées.

Chapitre 2

Présentation de la solution

Introduction

Après avoir comparé les différentes solutions de sécurité réseau open source et justifié le choix de pfSense dans le premier chapitre, ce deuxième chapitre se consacre à l'implémentation pratique de pfSense dans un environnement de simulation. Nous aborderons les étapes de configuration nécessaires pour déployer un réseau sécurisé, en mettant un accent particulier sur l'utilisation du protocole IPsec pour garantir des communications chiffrées. L'objectif est de fournir un guide pratique et détaillé pour tirer le meilleur parti de pfSense dans la sécurisation des communications d'entreprise.

2.1 Présentation de pfSense et de ses fonctionnalités

2.1.1 Présentation générale de pfSense

pfSense est une solution open source de pare-feu et de routage basée sur le système d'exploitation FreeBSD. Elle offre une interface graphique conviviale qui facilite la configuration et la gestion de la sécurité du réseau. PfSense est connu pour sa flexibilité, sa stabilité et sa robustesse, en faisant un choix populaire pour de nombreuses organisations.

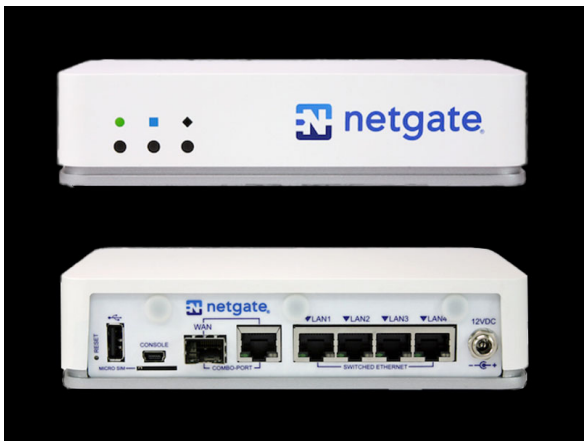


FIGURE 2.1 : pfSense Firewall

2.1.2 Fonctionnalités clés pour la gestion de la sécurité du réseau

pfSense offre un large éventail de fonctionnalités pour la gestion de la sécurité du réseau. Cela inclut le filtrage de paquets, la prévention d'intrusion, la détection de logiciels malveillants, la création de VPN, la gestion des journaux, etc. Ces fonctionnalités offrent des outils puissants pour protéger le réseau contre les menaces et les attaques.

pfSense offre un large éventail de fonctionnalités pour la gestion de la sécurité du réseau. Cela inclut :

Pare-feu Avancé : pfSense propose un pare-feu de niveau professionnel capable de filtrer le trafic en fonction de règles personnalisées. Il surveille l'état des connexions pour une sécurité accrue et une meilleure gestion du trafic.
VPN (Virtual Private Network) : pfSense permet la création de connexions VPN sécurisées pour les utilisateurs distants ou les sites distants. Les protocoles tels qu'IPsec et OpenVPN sont pris en charge, garantissant des communications chiffrées.
Passerelle sécurisée : En tant que passerelle Internet, pfSense gère les connexions entrantes et sortantes, offrant une connectivité sécurisée. Il peut également fonctionner comme un serveur DHCP pour attribuer des adresses IP de manière dynamique.
Filtrage de Contenu et Proxy : pfSense permet de filtrer le contenu web en bloquant l'accès à des sites spécifiques ou indésirables. Il peut également agir en tant que proxy pour améliorer les performances en cache.
Détection des Intrusions : pfSense est capable de détecter les activités suspectes sur le réseau grâce à des mécanismes de détection d'intrusion. Il peut générer des alertes et des rapports en temps réel pour permettre une réponse rapide.
Gestion Centralisée : Une interface web conviviale permet de gérer toutes les fonctionnalités de pfSense à partir d'un seul point. Cela facilite la configuration, le suivi et la maintenance du réseau.
Évolutivité et Personnalisation : pfSense est hautement personnalisable et peut être adapté à nos besoins spécifiques. Nous pouvons ajouter des fonctionnalités et des modules complémentaires en fonction de notre infrastructure.

2.1.3 Avantages et limites de pfSense

pfSense présente plusieurs avantages, notamment sa nature open source qui lui confère une grande flexibilité et une communauté active de support. De plus, pfSense est économique, car il n'y a pas de coûts de licence élevés associés à son utilisation.

1. Sécurité Complète : pfSense offre une gamme complète de fonctionnalités de sécurité, y compris un pare-feu robuste, des VPN sécurisés et la détection d'intrusion, ce qui contribue à protéger le réseau contre les menaces potentielles.
2. Gestion Centralisée : L'interface web conviviale de pfSense permet une gestion centralisée de toutes les fonctionnalités, ce qui facilite la configuration, la surveillance et la maintenance du réseau.
3. Flexibilité : pfSense est hautement personnalisable et peut être adapté aux besoins spécifiques d'une organisation. Il peut être configuré pour répondre aux exigences uniques de notre infrastructure.
4. VPN Sécurisés : La prise en charge des protocoles VPN tels qu'IPsec et OpenVPN permet de créer des connexions sécurisées pour les utilisateurs distants et les sites distants.
5. Filtrage de Contenu : La fonction de filtrage de contenu améliore la sécurité et la productivité en

bloquant l'accès à des sites non autorisés ou inappropriés.
6. Support de la Communauté : pfSense bénéficie d'une communauté active qui fournit un support, des conseils et des ressources en ligne, ce qui peut être précieux en cas de problèmes ou de questions.
7. Économique : Étant une solution open source, pfSense élimine les coûts de licence élevés associés aux solutions propriétaires, ce qui peut conduire à des économies significatives.

Cependant, pfSense peut nécessiter des compétences techniques pour une configuration et une gestion avancées, et il peut ne pas être adapté à toutes les infrastructures réseau spécifiques.

Les limites de pfSense, bien que souvent compensées par ses avantages, doivent être considérées lors de l'évaluation de cette solution pour répondre aux besoins spécifiques d'une organisation. Voici quelques-unes des principales limites de pfSense :

1. Complexité Initiale : La configuration initiale de pfSense peut être complexe, en particulier pour les utilisateurs novices en matière de réseau et de sécurité. La variété des fonctionnalités et des options de configuration peut nécessiter une courbe d'apprentissage.
2. Maintenance et Mises à Jour : pfSense nécessite une maintenance continue, y compris des mises à jour régulières pour assurer la sécurité et la stabilité du système. Cela peut demander du temps et des ressources pour maintenir le système à jour.
3. Support Professionnel : Bien qu'une communauté active offre un support en ligne, un support professionnel dédié peut nécessiter des coûts supplémentaires. Les organisations ayant besoin d'un support rapide et spécifique peuvent envisager des services de support payants.
4. Performance Matérielle : Pour des environnements de réseau complexes ou à grande échelle, pfSense peut exiger des ressources matérielles plus puissantes. Les performances du système dépendent largement du matériel sur lequel il est déployé.
5. Évolutivité Limitée : Bien que pfSense soit capable de gérer des réseaux de taille moyenne, sa capacité à évoluer pour répondre aux besoins de réseaux très grands et complexes peut être limitée.
6. Documentation et Formation : En raison de la richesse des fonctionnalités de pfSense, la documentation est essentielle pour une configuration correcte. La recherche de la documentation appropriée et l'acquisition des compétences nécessaires peuvent prendre du temps.
7. Compatibilité du Matériel : Bien que pfSense puisse fonctionner sur un large éventail de matériels, la compatibilité avec certaines configurations spécifiques peut être un défi. Il est important de vérifier la compatibilité matérielle avant le déploiement.
8. Intégration Complexes : L'intégration de pfSense dans des environnements réseau existants peut nécessiter des ajustements et des configurations spécifiques, ce qui peut être complexe selon la complexité de l'infrastructure existante.
9. Licence et Propriété : Bien que pfSense soit open source, certaines fonctionnalités avancées ou spécifiques peuvent nécessiter une licence payante. Il est important de comprendre les implications de la licence pour une utilisation appropriée.

2.2 Alignement des besoins avec les fonctionnalités de pfSense

2.2.1 Correspondance des fonctionnalités de pfSense aux besoins de sécurité

Voici comment les fonctionnalités clés de pfSense correspondent aux besoins de sécurité typiques au sein d'une organisation :

1. Pare-feu Avancé :
- Besoins Correspondants : Protection contre les cyberattaques, filtrage du trafic indésirable, surveillance du trafic entrant et sortant.
- Correspondance : Le pare-feu puissant de pfSense permet de créer des règles personnalisées pour filtrer le trafic et surveiller l'état des connexions. Cela renforce la sécurité en empêchant l'accès non autorisé et en réduisant les risques d'intrusion.
2. VPN Sécurisés :
- Besoins Correspondants : Accès distant sécurisé, communication chiffrée pour les utilisateurs distants et les sites distants.
- Correspondance : pfSense prend en charge des protocoles VPN tels qu'IPsec et OpenVPN, permettant la mise en place de connexions VPN sécurisées. Cela répond au besoin d'accès sécurisé aux ressources internes à partir d'emplacements distants.
3. Filtrage de Contenu et Proxy :
- Besoins Correspondants : Contrôle de l'accès à Internet, amélioration de la productivité en bloquant l'accès à des sites inappropriés.
- Correspondance : pfSense offre la possibilité de filtrer le contenu web, bloquant l'accès à des sites spécifiques et améliorant ainsi la politique de sécurité et la productivité des utilisateurs.
4. Détection des Intrusions :
- Besoins Correspondants : Détection rapide des activités suspectes ou non autorisées sur le réseau.
- Correspondance : pfSense peut être configuré pour détecter les tentatives d'intrusion et générer des alertes en temps réel. Cela renforce la sécurité en permettant une réponse rapide aux incidents de sécurité.
5. Gestion Centralisée :
- Besoins Correspondants : Gestion cohérente des politiques de sécurité, des règles de pare-feu et des configurations.
- Correspondance : L'interface web conviviale de pfSense offre une plateforme centralisée pour gérer toutes les fonctionnalités de sécurité. Cela simplifie la gestion quotidienne et la mise en place de mesures de sécurité cohérentes.
6. Contrôle de Bande Passante :
- Besoins Correspondants : Optimisation des performances réseau en gérant l'utilisation de la bande passante.
- Correspondance : pfSense permet de configurer des règles de trafic pour gérer la bande passante, prioriser certains types de trafic et garantir des performances réseau optimales.

En évaluant comment les fonctionnalités de pfSense répondent aux besoins spécifiques de sécurité, il est possible de déterminer si cette solution unifiée est appropriée pour renforcer la sécurité et la gestion du réseau au sein de l'organisation.

2.2.2 Adaptation et personnalisation de pfSense pour répondre aux exigences spécifiques

L'adaptation et la personnalisation de pfSense pour répondre aux exigences spécifiques peuvent être réalisées en suivant les étapes suivantes pour chaque fonctionnalité requise :

1. Pare-feu Avancé :

- Accédez à l'interface d'administration de pfSense.
- Configurez des règles de pare-feu personnalisées en fonction des besoins de l'organisation.
- Identifiez les types de trafic autorisés et restreints.
- Surveillez l'état des connexions et ajustez les règles au besoin.
- Mettez en œuvre des mécanismes de blocage des tentatives d'intrusion

2. VPN Sécurisés :

- Configurez les protocoles de VPN requis (IPsec, OpenVPN).
- Générez des certificats et des clés pour sécuriser les connexions VPN.
- Paramétrez les tunnels VPN pour permettre aux utilisateurs distants d'accéder au réseau interne de manière sécurisée.
- Appliquez des règles de pare-feu spécifiques pour le trafic VPN.

3. Filtrage de Contenu et Proxy :

- Activez le service de filtrage de contenu et de proxy.
- Créez des listes de blocage pour les sites web non autorisés.
- Configurez les règles pour rediriger le trafic web via le proxy.
- Surveillez les journaux pour identifier les tentatives d'accès à des sites bloqués.

4. Détection des Intrusions :

- Activez les mécanismes de détection d'intrusion (par exemple, Snort ou Suricata).
- Configurez les règles de détection pour surveiller les activités suspectes.
- Mettez en place des alertes en temps réel pour les incidents de sécurité détectés.
- Analysez les journaux d'intrusion pour prendre des mesures correctives.

5. Gestion Centralisée :

- Utilisez l'interface web de pfSense pour configurer toutes les fonctionnalités de sécurité.
- Créez des profils de configuration pour différents groupes d'utilisateurs ou de périphériques.
- Implémentez une stratégie cohérente pour les règles de pare-feu, les politiques de sécurité et les paramètres réseau.

6. Contrôle de Bande Passante :

- Déterminez les priorités et les quotas de bande passante pour différents types de trafic.
- Mettez en place des règles de contrôle de bande passante pour réguler le flux de données.
- Utilisez des outils de surveillance pour vérifier l'utilisation de la bande passante et ajuster les règles en conséquence.

Chaque étape nécessite une configuration minutieuse en fonction des besoins spécifiques de l'organisation. Il est recommandé de suivre la documentation officielle de pfSense, d'explorer les ressources en ligne et de tester les configurations dans un environnement de test avant de les déployer en production. L'adaptation et la personnalisation de pfSense permettront à l'organisation de répondre de manière précise et efficace aux exigences de sécurité spécifiques.

2.3 Présentation du réseau

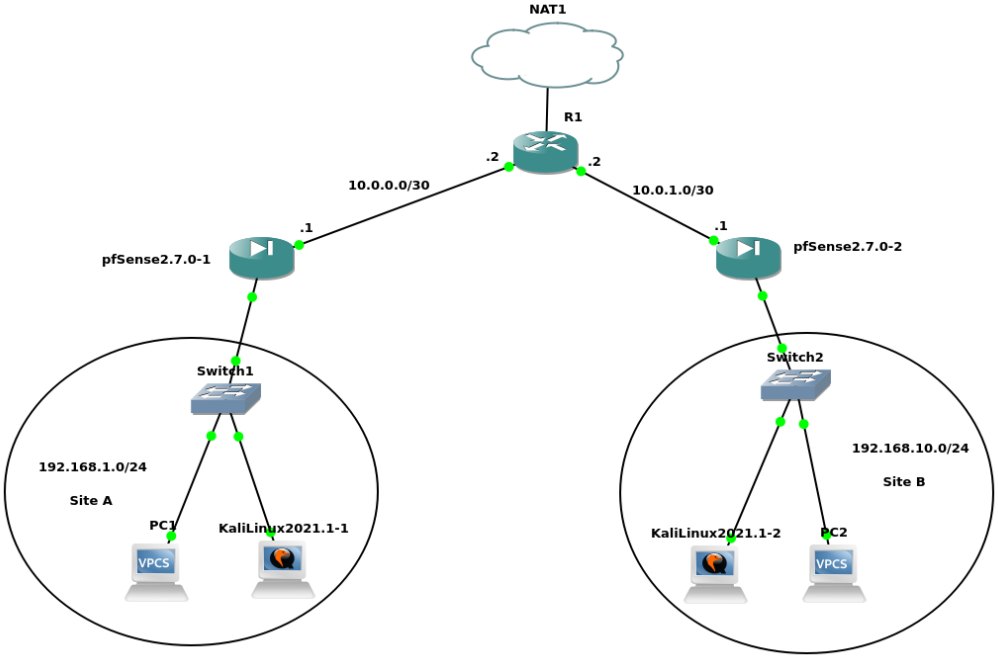


FIGURE 2.2 : Architecture du réseau utilisé

2.4 Choix du VPN

2.4.1 Etude des VPN

pfSense a intégré la prise en charge de l'interface graphique pour les technologies VPN telles que OpenVPN et IPSec. Dans le cadre de notre étude, nous devons choisir le protocole VPN le mieux adapté à nos besoins spécifiques. Pour cela, nous comparons les caractéristiques et les performances des deux protocoles comme suit :

Caractéristiques et Performances

- OpenVPN : OpenVPN est un protocole VPN open source réputé pour sa flexibilité et sa facilité de configuration. Il utilise des certificats SSL/TLS pour l'authentification et le chiffrement, offrant ainsi une sécurité robuste. OpenVPN est compatible avec une variété de plates-formes et peut fonctionner sur des ports UDP ou TCP, ce qui le rend idéal pour contourner les restrictions de pare-feu.
- IPsec : IPsec est un ensemble de protocoles standardisés largement utilisé pour sécuriser les communications réseau. Il offre un chiffrement et une authentification intégrés au niveau du protocole IP, assurant ainsi une sécurité transparente pour toutes les données échangées. IPsec est souvent utilisé pour les connexions de site à site et les connexions point à site, offrant une intégrité et une confidentialité des données élevées.

Pertinence par Rapport aux Besoins de l'Entreprise

- OpenVPN : Idéal pour les utilisateurs nomades ou distants nécessitant un accès sécurisé au réseau de l'entreprise depuis n'importe où. Sa flexibilité en termes de configuration en fait un choix polyva-

lent pour les environnements hétérogènes.
- IPsec : Convient mieux aux connexions de site à site ou point à site, offrant une sécurité robuste pour les réseaux d'entreprise étendus et les connexions inter-sites.

2.4.2 Choix du VPN adéquat

Après une analyse approfondie des caractéristiques et des performances de chaque protocole, ainsi qu'une évaluation de leur pertinence par rapport aux besoins spécifiques de notre architecture, nous avons choisis d'implémenter le protocole IPsec.

2.4.3 Présentation IPSEC

IPsec (Internet Protocol Security) est un protocole de sécurité utilisé pour sécuriser les communications sur un réseau IP. Il peut être utilisé pour protéger les communications à la fois sur Internet et sur des réseaux privés, comme un réseau d'entreprise. Il utilise différents protocoles pour fournir des services de sécurité, notamment :

- **Authentication Header (AH) :** assure l'intégrité des données et l'authenticité de l'expéditeur.
- **Encapsulating Security Payload (ESP) :** assure la confidentialité des données en les chiffrant.
- **Internet Key Exchange (IKE) :** permet d'établir des clés de session pour sécuriser la communication.

IPsec peut être utilisé pour deux principaux types de communication : le mode tunnel et le mode transport :

Le mode tunnel est utilisé pour sécuriser les communications entre deux réseaux, tels qu'un réseau d'entreprise et un réseau partenaire. Dans ce mode, les données sont encapsulées dans un nouveau paquet IP avec une nouvelle adresse IP de destination. Ce nouveau paquet IP est alors chiffré et envoyé via Internet ou un autre réseau public. À l'arrivée, le paquet est désencapsulé, déchiffré et envoyé à sa destination finale.

Le mode transport est utilisé pour sécuriser les communications entre deux hôtes sur un même réseau, comme deux ordinateurs sur le même réseau local. Dans ce mode, seules les données elles-mêmes sont chiffrées et envoyées via le réseau. Le mode transport est moins utilisé que le mode tunnel, mais il peut offrir des performances meilleures dans certains cas.

En résumé, le mode tunnel est utilisé pour sécuriser les communications entre réseaux, tandis que le mode transport est utilisé pour sécuriser les communications entre hôtes sur un même réseau. IPsec, d'une manière extrêmement simplifiée, fournit un moyen de communiquer en toute sécurité en fournissant un cryptage au niveau de la couche réseau.

2.5 Choix techniques

2.5.1 Emulateurs réseaux

Dans le cadre de l'implémentation d'un réseau sécurisé avec pfSense, un choix doit être fait entre GNS3 et Cisco Packet Tracer pour la simulation et la modélisation des réseaux. Voici une analyse comparative pour aider à prendre cette décision :

- **GNS3 (Graphical Network Simulator-3) :**

GNS3 est un simulateur de réseau open source largement utilisé, permettant de modéliser des réseaux informatiques complexes. Il offre une grande flexibilité en permettant aux utilisateurs de déployer une large gamme de périphériques réseau virtuels, y compris des routeurs, des commutateurs et des pare-feu, provenant de différents fournisseurs. GNS3 est populaire pour sa capacité à créer des environnements de réseau réalistes, à simuler des scénarios complexes et à intégrer des périphériques réseau réels, offrant ainsi une grande polyvalence.



FIGURE 2.3 : GNS3

- **Cisco Packet Tracer :**

Packet Tracer est un simulateur de réseau développé par Cisco, conçu spécifiquement pour l'apprentissage et la formation aux technologies réseau Cisco. Il propose une interface utilisateur intuitive et conviviale, idéale pour les débutants en réseau. Packet Tracer offre une vaste bibliothèque de périphériques Cisco préconfigurés, permettant aux utilisateurs de créer des topologies réseau simples à moyennement complexes. Il est largement utilisé dans les environnements éducatifs pour illustrer les concepts de réseau et pour simuler des configurations Cisco.



FIGURE 2.4 : Packet tracer

Analyse du Choix Technique : Le choix entre GNS3 et Packet Tracer dépendra des besoins spécifiques du projet et des compétences des utilisateurs :

- Complexité du Réseau : Pour des projets impliquant des réseaux complexes avec une variété de périphériques provenant de différents fournisseurs, GNS3 offre une meilleure adaptabilité et une plus grande flexibilité pour modéliser des scénarios avancés.

- Formation et Apprentissage : Si l'objectif est principalement l'apprentissage des technologies Cisco et l'acquisition de compétences de base en réseau, Packet Tracer peut être plus adapté en raison de sa simplicité d'utilisation et de son orientation spécifique vers les équipements Cisco.

- Intégration de Périphériques Réels : Pour des tests impliquant l'intégration de périphériques réseau réels, tels que des routeurs et des commutateurs physiques, GNS3 offre une meilleure prise en charge grâce à sa capacité à intégrer des équipements de différents fournisseurs.

- Disponibilité et Coût : Packet Tracer est souvent préféré dans les environnements éducatifs en raison de sa disponibilité gratuite pour les étudiants et les instructeurs. GNS3, bien qu'il dispose d'une version gratuite, peut nécessiter des frais pour l'utilisation de fonctionnalités avancées ou pour l'hébergement de dispositifs virtuels.

2.5.2 Logiciels de virtualisation

Lorsqu'il s'agit de créer des environnements de virtualisation sur des postes de travail individuels, VMware Workstation Pro et VirtualBox sont deux des solutions les plus populaires. Cependant, il existe également d'autres alternatives à considérer. Voici une analyse comparative entre VMware Workstation Pro, VirtualBox et quelques autres solutions similaires :

- **VMware Workstation Pro :**

VMware Workstation Pro est une application de virtualisation de poste de travail avancée qui permet aux utilisateurs de créer et de gérer des machines virtuelles sur leur ordinateur local. Elle offre une gamme étendue de fonctionnalités, y compris le support des systèmes d'exploitation invités multiples, la compatibilité avec les technologies de virtualisation matérielles, et des outils avancés de gestion et de configuration.



FIGURE 2.5 : Vmware

- **VirtualBox :**

VirtualBox est une solution de virtualisation open source développée par Oracle. Elle offre une interface utilisateur conviviale et prend en charge une large gamme de systèmes d'exploitation invités. Bien que moins riche en fonctionnalités que VMware Workstation Pro, VirtualBox est populaire pour sa simplicité d'utilisation et sa disponibilité gratuite et open-source.



FIGURE 2.6 : VirtualBox

Analyse du Choix Technique : Le choix entre VMware Workstation Pro, VirtualBox et d'autres solutions similaires dépendra des critères suivants :

- Performance et Stabilité : VMware Workstation Pro est généralement considéré comme offrant des performances supérieures et une meilleure stabilité par rapport à VirtualBox et d'autres solutions.

- Fonctionnalités et Flexibilité : VMware Workstation Pro propose un ensemble étendu de fonctionnalités et d'outils de gestion avancés, ce qui en fait un choix privilégié pour les utilisateurs ayant des besoins avancés en matière de virtualisation. Cependant, VirtualBox peut être plus adapté pour les utilisateurs recherchant une solution simple et gratuite.

- Compatibilité et Support : VMware Workstation Pro a tendance à offrir une meilleure compatibilité avec les systèmes d'exploitation invités, ainsi qu'un support technique plus solide par rapport à VirtualBox et d'autres solutions.

- Coût : VirtualBox est gratuit et open source, ce qui en fait une option attrayante pour les utilisateurs avec des contraintes budgétaires. VMware Workstation Pro, en revanche, est une solution payante, mais offre des fonctionnalités avancées et un support professionnel.

Conclusion

Ce chapitre a offert un guide pratique pour configurer pfSense dans un environnement d'entreprise, avec un focus sur l'utilisation du protocole IPsec pour sécuriser les communications. Nous avons exploré les meilleures pratiques de configuration et de gestion des fonctionnalités avancées de sécurité, ainsi que les méthodes de surveillance du réseau. L'implémentation de pfSense a montré qu'il s'agit d'une solution robuste et flexible, capable de répondre efficacement aux besoins de sécurisation des communications en entreprise. Le prochain chapitre évaluera les performances et l'efficacité de cette solution.

Chapitre 3

Conception et mise en œuvre de la solution

Introduction

Dans ce chapitre, nous nous penchons sur la conception et l'implémentation de la solution de sécurisation des communications avec pfSense, en mettant l'accent sur le déploiement du VPN IPsec. Nous débuterons par une brève présentation des outils, suivi d'une description des étapes nécessaires à la mise en place d'IPsec dans notre infrastructure pfSense. Cette introduction énonce clairement notre choix du VPN IPsec et établit le contexte pour les détails à venir sur son déploiement et sa configuration.

3.1 Présentation des outils

3.1.1 Le logiciel GNS3

GNS3 (Graphical Network Simulator) est un logiciel libre permettant l'émulation ou la simulation de réseaux informatiques. De plus, il est possible de s'en servir pour tester les fonctionnalités des IOS Cisco. La figure suivante présente l'emplacement des différents outils de GNS3 que nous utiliserons pour simuler un réseau.

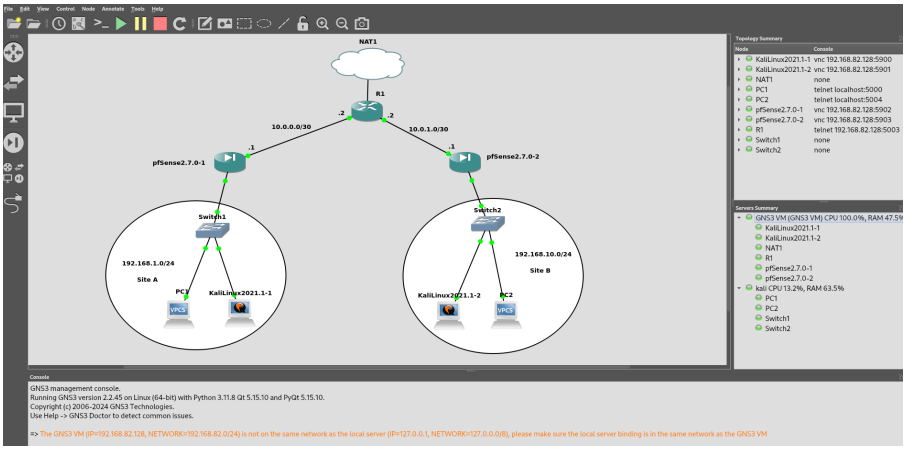


FIGURE 3.1 : Présentation GNS3

3.1.2 VM WARE Workstation 17 Pro

Pour l'émulation de notre réseau, nous avons choisi d'utiliser VMware Workstation 17 Pro. Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou linux). Ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique. Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'hôte physique. Cette version exécute les applications les plus exigeantes, elle utilise le dernier matériel pour répliquer l'environnement des serveurs postes de travail tout en étant accessible de n'importe quel périphérique grâce à son interface web.

3.2 Implémentation de l'architecture réseau

3.2.1 Emulation du réseau

Configuration du réseau

1. Expliquons les appareils utilisés et leurs fonctionnalités :

    - Deux instances pfSense avec FreeBSD. Celles-ci serviront de 2 passerelles VPN pour les 2 sites. En mode tunnel site à site, les 2 sites ne peuvent pas avoir de sous-réseaux qui se chevauchent. La raison en est que nous avons besoin que les appareils de chacun des sites traitent les appareils pfSense comme passerelle.
    - Le routeur se situe entre les deux pfSense dans cette disposition, représente un appareil sur Internet et assure la connectivité entre les 2 passerelles. Nous avons choisi ici un routeur CiscoIOS C3745.
    - Il y a une machine dans chacun des sites locaux qui sont des systèmes d'exploitation basés sur Ubuntu et qui sont également utilisées pour administrer le pare-feu pfSense sur leurs sites respectifs.
    - Le périphérique NAT sert à donner aux pare-feu pfSense l'accès à Internet.

2. Configurons les différentes interfaces sur chacun des appareils. Le périphérique du milieu dispose de deux interfaces chacune dans le domaine de diffusion/sous-réseau d'interfaces de chacun des sites.

    - Le firewall pfSense dispose de 2 interfaces par défaut. Le WAN (em0) que nous connectons habituellement au sous-réseau Internet et l'interface Lan (em1) utilisée pour s'administrer et se configurer via WebGUI.
    - Nous connecterons les interfaces WAN (em0's) au routeur R1 pour chacun des pfSense, et l'interface LAN est l'interface participant au sous-réseau pour chacun des sites.
    - Les interfaces LAN devront être configurées de manière à se trouver sur un espace de sous-réseau différent. Notons que par défaut pfSense a un sous-réseau 192.168.1.0/24 configuré sur em1 (LAN). Donc, pour le site A, nous l'avons laissé tel quel, puis nous avons modifié la configuration du DHCP du site B.

- L'étape suivante consiste à configurer les interfaces connectant le routeur au pfSense. Puisque seulement 2 machines sont présentes ici, nous pouvons utiliser un sous-réseau /30. Pour pfSense du site A, nous avons utilisé 10.0.0.0/30 et pour pfSense du site B 10.0.1.0/30. Notons que la vérification ping peut échouer en raison des règles de pare-feu.

3. Ensuite, nous voulons voir si le pfSense du site A peut pinger l'interface du routeur connecté au pfSense du site B.
   Pour cela, nous devons-nous assuré de configurer les passerelles et la route. Cela signifie que nous devons indiquer à pfSense sur le site A qu'il existe un chemin vers 10.0.1.0/30 via R1. Nous devons faire deux choses sur chacune des machines pfSense. La première serait de configurer une passerelle, puis de configurer une route statique via cette passerelle créée. L'image suivante le montre (nous devons le faire sur l'autre machine pfSense en conséquence). Nous avons montré les étapes ci-dessous pour le site B pfSense, la même configuration a été également effectuée sur l'autre pfSense. Nous avons accédé à **Système->Routage** à partir de l'interface graphique Web. Une fois cela fait, nous avons configuré une route statique pour utiliser la passerelle nouvellement créée, comme indiqué dans l'image suivante.

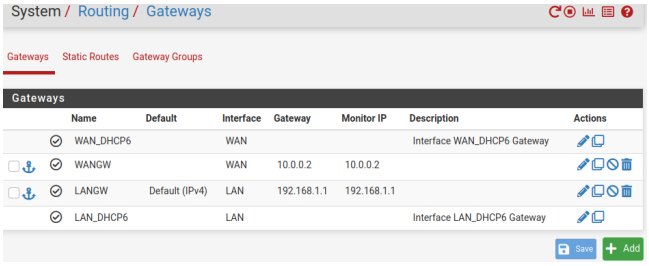


FIGURE 3.2 : Création de passerelle sur pfSense du Site A

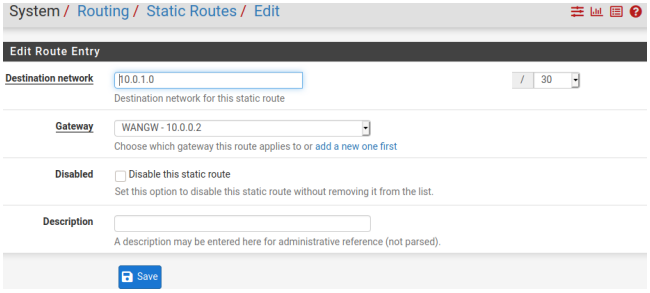


FIGURE 3.3 : Création de route statique sur pfSense du Site A

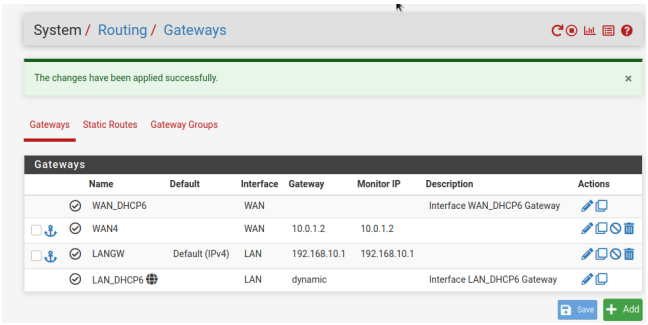


FIGURE 3.4 : Création de passerelle sur pfSense du Site B

4. Ensuite, nous devons configurer IPSec sur les deux pfSense.

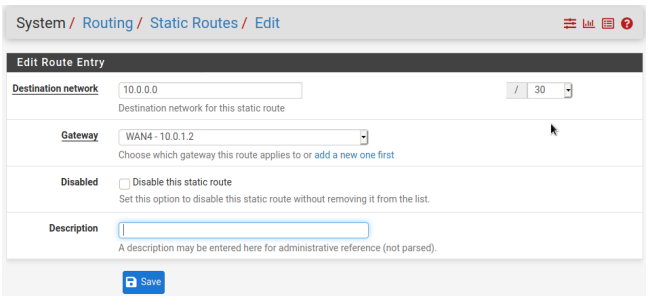


FIGURE 3.5 : Création de route statique sur pfSense du Site B

Une chose importante à noter ici est que R1 n'a pas besoin de savoir quoi acheminer ni les sous-réseaux locaux, car le mode tunnel empêchera R1 de voir les en-têtes IP réels. Ainsi, R1 n'a pas besoin de connaître ou de configurer les routes vers et depuis les sous-réseaux du site.

5. Passons à la partie VPN.
   Donc pour IPSec nous avons 2 phases. Dans la phase 1, nous configurons les mécanismes de sécurité tels que le cryptage, les algorithmes de hachage et l'authentification à utiliser pour la configuration VPN. Il s'agit d'un accord entre les 2 parties participant à la connexion VPN IPSec. Pour accéder aux paramètres IPSec, nous avons accédé à **Services->VPN->IPSEC**

   - Ensuite, nous avons appuyé sur "ajouter p1" qui correspond à la phase 1. Nous avons configuré la version d'échange de clés comme **IKEv2**, l'interface comme WAN et l'IP de la passerelle distante. Pour pfSense sur le site A, il doit s'agir de l'adresse IP de l'interface WAN de pfSense sur le site B "**10.0.1.1**". Nous avons choisi la méthode d'authentification **Mutual PSK**. Nous avons défini un mot de passe, celui-ci doit être le même sur les deux pfSense. Nous avons vérifié et enregistré les modifications.

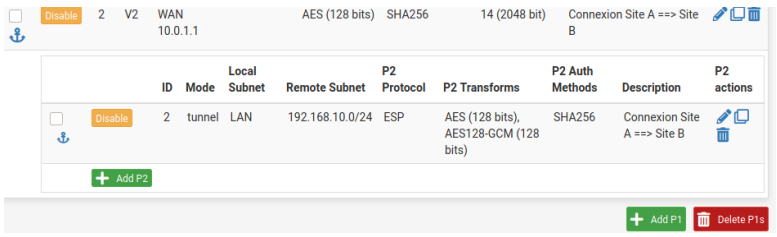


FIGURE 3.6 : Configuration de phase 1 pour le VPN IPSec sur pfSense A

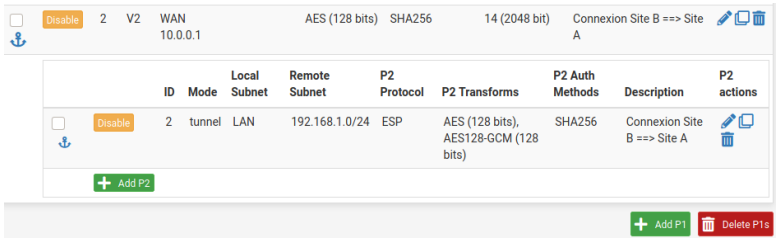


FIGURE 3.7 : Configuration de phase 1 pour le VPN IPSec sur pfSense B

   - Nous devons ensuite configurer la phase 2. Une fois la phase 1 configurée, une option pour ajouter la phase 2 en dessous nous est apparue. C'est sous **Services->VPN->IPSec->Tunnel**. Cliquez sur **ajouter p2**. Le sous-réseau du site local mentionne l'adresse du sous-réseau ou bien l'interface dont nous configurons pfSense. Pour le réseau distant, nous

avons configuré le sous-réseau du site distant comme indiqué (site A pfSense).

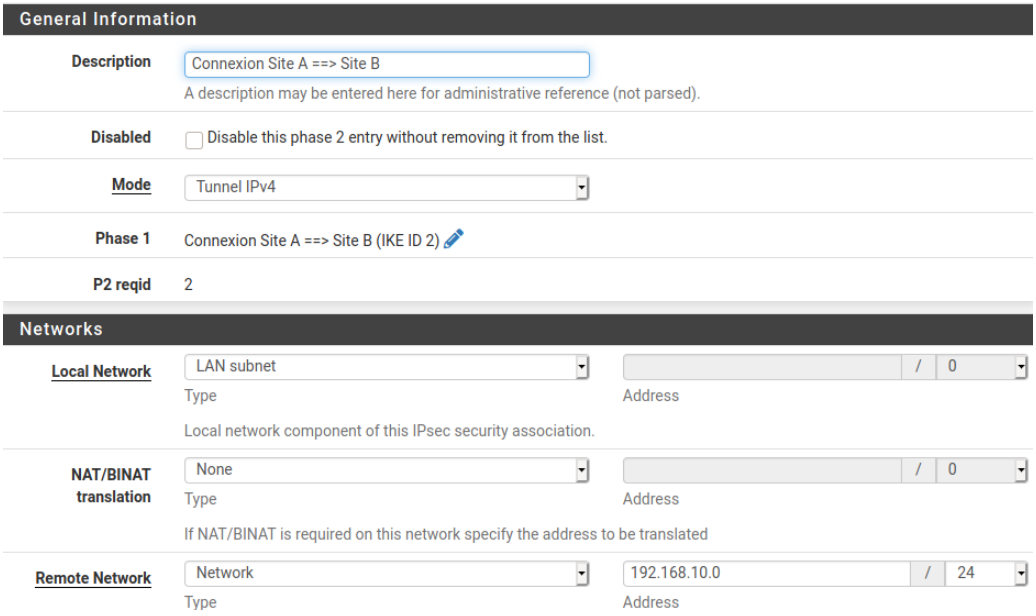


FIGURE 3.8 : Configuration de phase 2 pour le VPN IPSec sur pfSense A

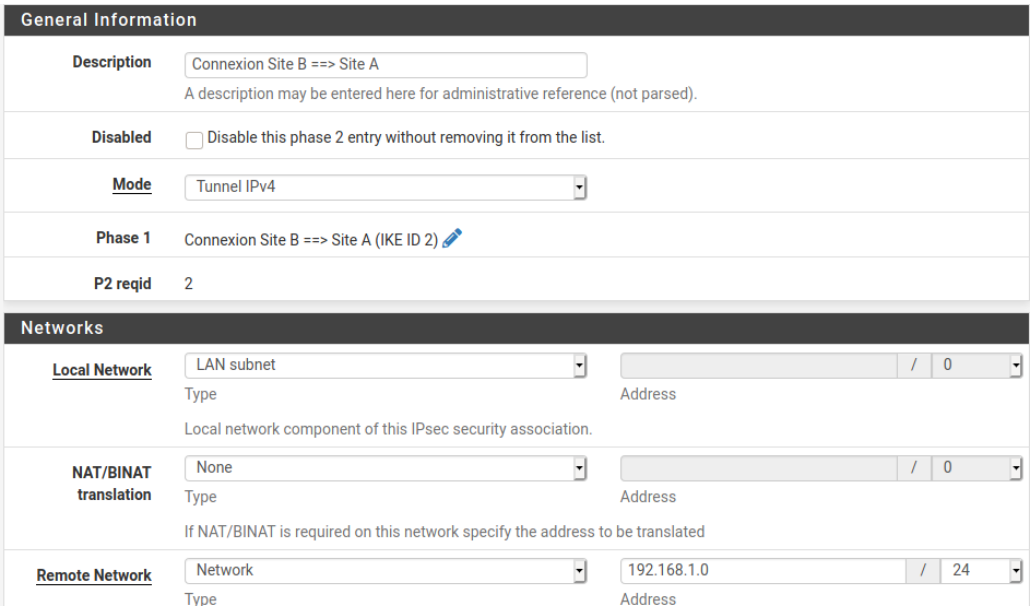


FIGURE 3.9 : Configuration de phase 2 pour le VPN IPSec sur pfSense

- Dans les paramètres qui suivent, nous avons défini le mécanisme d'authentification et de cryptage conformément à ce que nous avons sélectionné pour la phase 1.

6. Une fois que nous avons effectué les étapes ci-dessus pour les sites et pfSense respectivement, nous devons créer des règles de pare-feu pour autoriser exclusivement le trafic via pfSense. Dans pfSense, nous pouvons en fait définir des règles spécifiques uniquement à l'interface IPSec. Cela doit encore une fois être fait sur les deux pfSense. Ce qui suit montre la règle pour pfSense sur le site A. Nous avons accédé à **Pare-feu->Règles->IPSec**. (Cela n'apparaîtra qu'une fois que vous aurez configuré les phases). Par souci de simplicité, nous avons autorisé tous les protocoles IPv4 sur IPSec en provenance du sous-réseau du Site B sur le sous-réseau du Site A,

néanmoins nous pouvons être plus restrictifs dans ce que nous imposons.

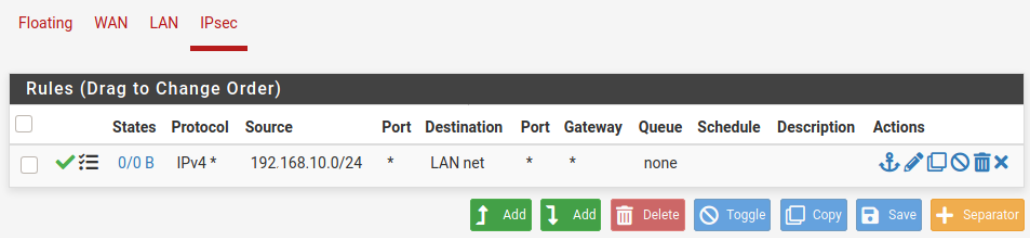


FIGURE 3.10 : Règles de pare-feu sur l'interface IPSec du pfSense A

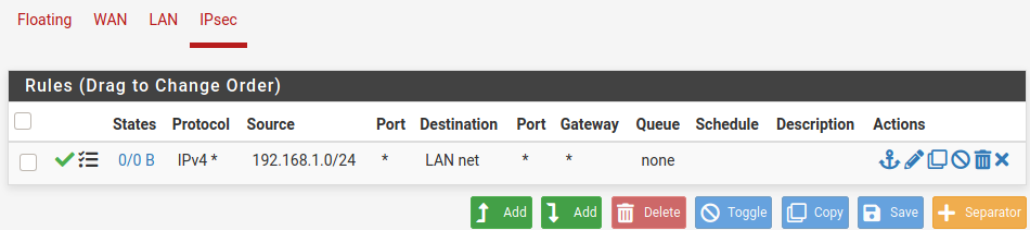


FIGURE 3.11 : Règles de pare-feu sur l'interface IPSec du pfSense B

7. Nous devons supprimer les règles de blocage par défaut sur l'interface WAN et autoriser le trafic pour tous les protocoles IPv4 en provenance du firewall du Site B sur le firewall du Site A afin que la connexion VPN puisse être établie de manière appropriée. La première chose que nous avons faite pour l'interface WAN de pfSense est de supprimer les règles d'usine. Nous avons ensuite autorisé le trafic, comme indiqué ci-dessous.

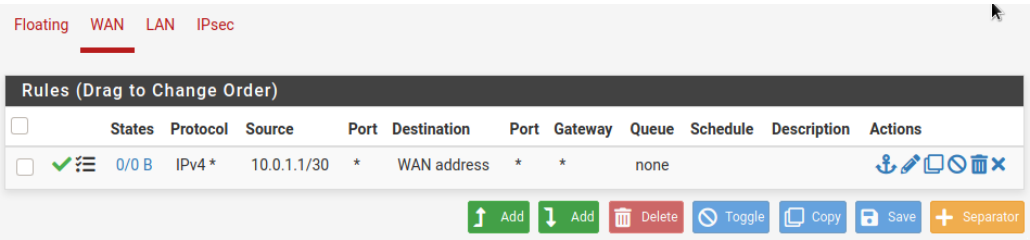


FIGURE 3.12 : Règles de pare-feu sur l'interface WAN du pfSense A

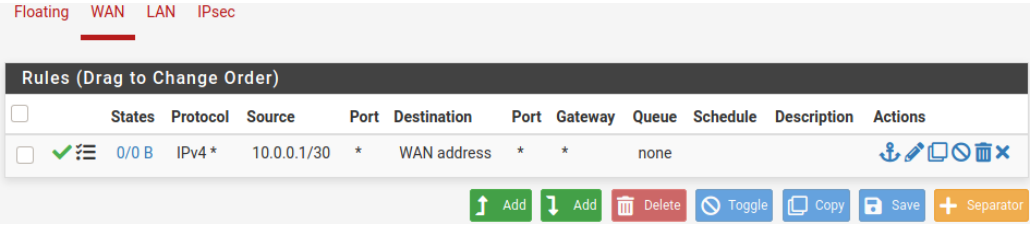


FIGURE 3.13 : Règles de pare-feu sur l'interface WAN du pfSense B

8. La prochaine chose est d'aller de l'avant et de sauvegarder les règles. Nous nous sommes assurés de l'avoir fait pour les deux pfSense. Une fois cela fait, nous pouvons établir la connexion VPN en allant dans **Statut->IPSec->Connecter**.

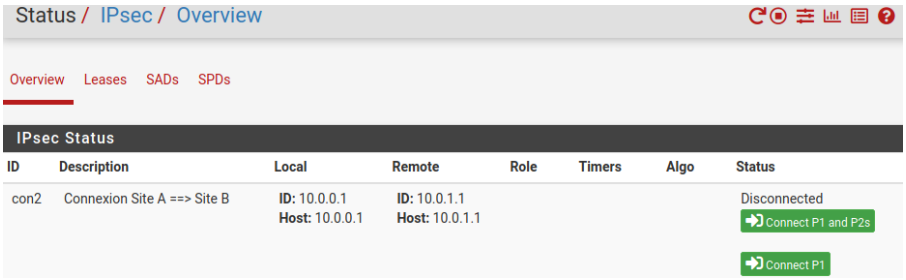


FIGURE 3.14 : Interface de connexion d'IPsec sur pfSense A

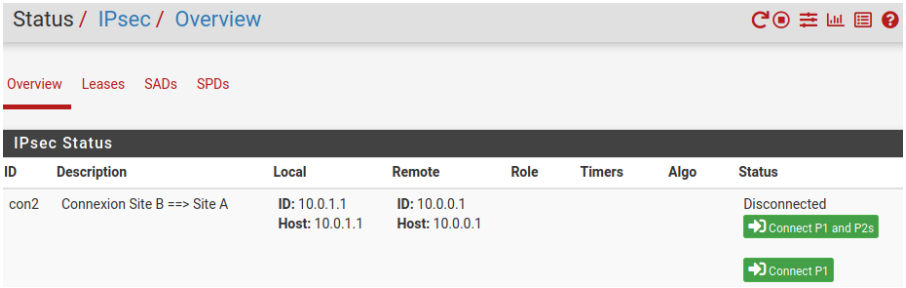


FIGURE 3.15 : Interface de connexion d'IPsec sur pfSense B

3.2.2 Test et résultats

Après avoir établi la connexion VPN sur le pfSense du site A, les machines du Site A peuvent désormais envoyer une requête ping aux machines du Site B et vice-versa (Site — connectivité du site en mode tunnel).

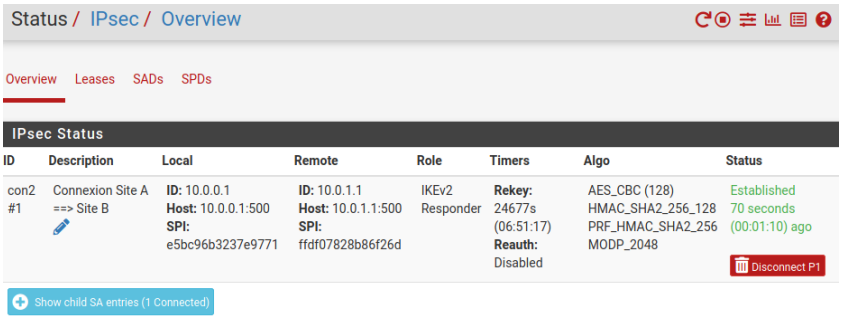


FIGURE 3.16 : Connexion de phase 1 et 2 pour le VPN IPSec du site A

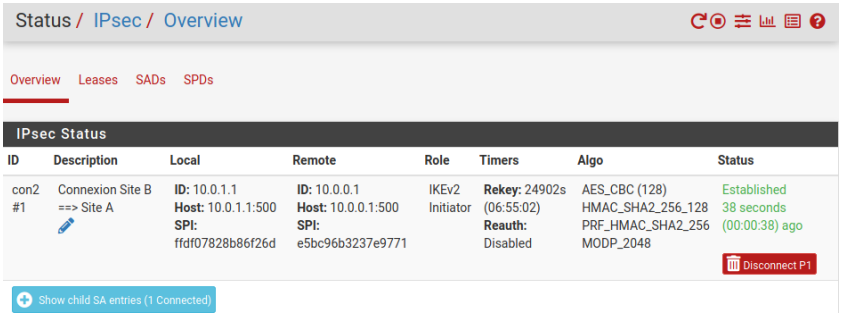


FIGURE 3.17 : Connexion de phase 1 et 2 pour le VPN IPSec du site B

Test de connectivité

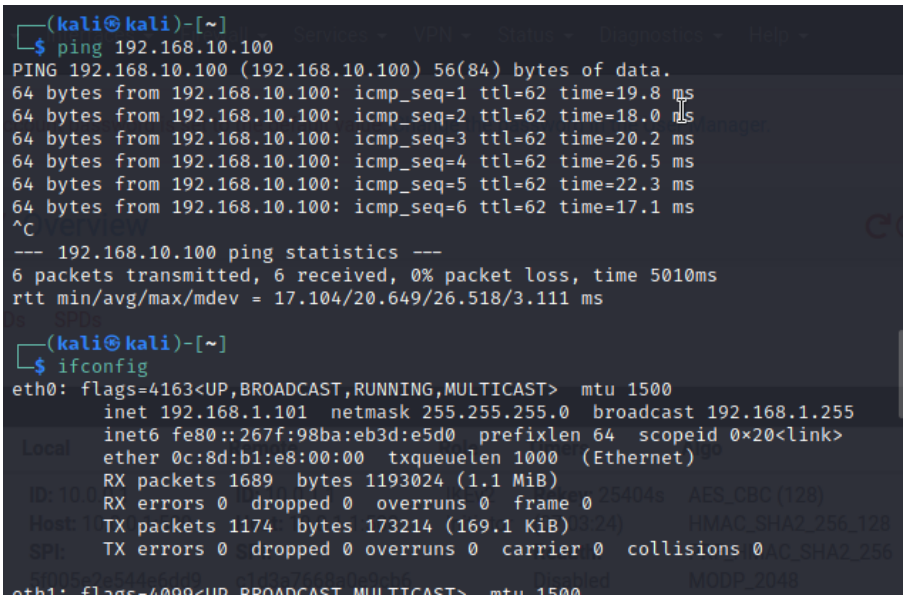


FIGURE 3.18 : Ping du 192.168.1.101 ==> 192.168.10.100

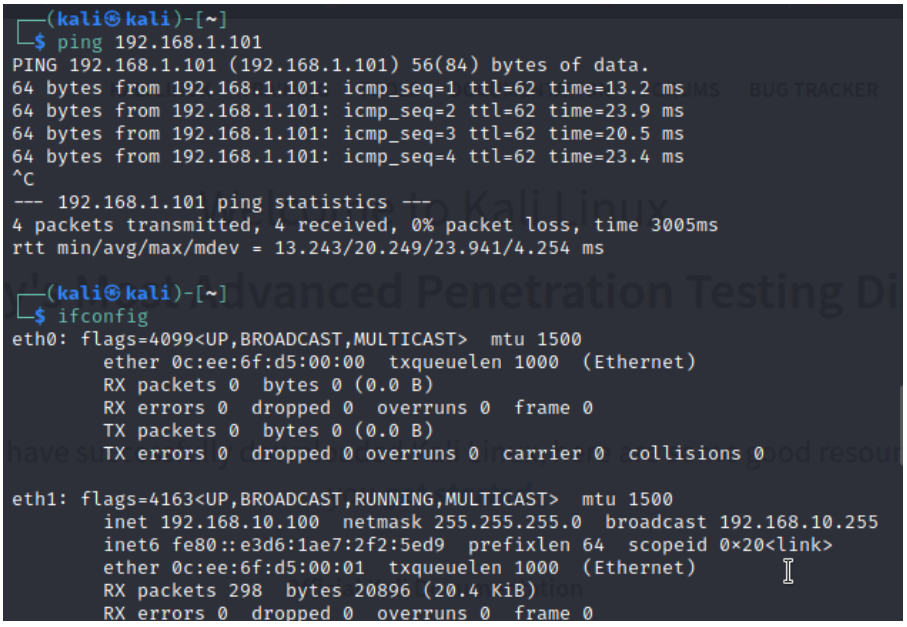


FIGURE 3.19 : Ping du 192.168.10.100 ==> 192.168.1.101

3.3 Réponse aux Objectifs de Sécurisation et limites de la solution

3.3.1 Réponse aux Objectifs de Sécurisation par l'Implémentation de pfSense

L'implémentation de pfSense répond aux objectifs de sécurisation des communications en entreprise de manière exhaustive et précise. Voici comment la solution mise en place avec pfSense répond à chaque besoin spécifique :

Authentification des Extrémités

pfSense utilise des protocoles VPN tels qu'IPsec et OpenVPN qui intègrent des mécanismes robustes d'authentification des extrémités. Cela permet de vérifier l'identité des parties communicantes avant

d'établir une connexion sécurisée, assurant ainsi que seules les entités autorisées peuvent accéder au réseau.

Confidentialité des Données Échangées

La solution pfSense garantit la confidentialité des données échangées grâce au chiffrement des communications via des protocoles sécurisés comme IPsec et OpenVPN. Le chiffrement assure que les données transmises restent illisibles pour toute personne non autorisée interceptant les communications.

Intégrité des Données Échangées

Pour assurer l'intégrité des données, pfSense utilise des algorithmes de hachage cryptographique dans ses protocoles VPN. Ces algorithmes génèrent des résumés de message (hashes) qui permettent de vérifier que les données n'ont pas été altérées pendant la transmission, garantissant ainsi l'intégrité des informations échangées.

Protection Contre les Écoutes et Analyses de Trafic

Les protocoles de chiffrement utilisés par pfSense (IPsec, OpenVPN) protègent contre les écoutes et les analyses de trafic. Le chiffrement rend les données incompréhensibles pour les attaquants et empêche l'analyse des paquets de données, ce qui rend difficile l'obtention d'informations sensibles à partir du trafic réseau.

Protection Contre le Rejeu

pfSense intègre des mécanismes de protection contre les attaques par rejeu dans ses protocoles VPN. Ces mécanismes incluent l'utilisation de numéros de séquence et de délais de session qui empêchent les attaquants de capturer et de réutiliser des paquets de données précédemment transmis pour tenter de perturber la communication ou d'obtenir un accès non autorisé.

En résumé, l'implémentation de pfSense répond efficacement à l'ensemble des objectifs de sécurisation définis pour garantir des communications sécurisées en entreprise. Elle offre une solution complète et robuste, assurant l'authentification des extrémités, la confidentialité et l'intégrité des données échangées, ainsi que la protection contre les écoutes, les analyses de trafic et les attaques par rejeu.

3.3.2 Limites de la solution implémentée avec pfSense

Bien que pfSense soit une solution robuste et flexible pour la sécurisation des communications en entreprise, elle présente également certaines limites qu'il est important de considérer. Voici les principales limites identifiées :

Complexité de la Configuration

pfSense, bien que puissant, peut être complexe à configurer correctement pour les utilisateurs moins expérimentés. La richesse des fonctionnalités et des options de configuration peut entraîner une courbe d'apprentissage élevée, nécessitant des compétences techniques avancées pour assurer une mise en œuvre optimale et sécurisée.

Performances sous Forte Charge

La performance de pfSense dépend en grande partie du matériel sur lequel il est déployé. Sous une charge de trafic élevée, ou avec l'activation de multiples services de sécurité (comme IDS/IPS), les performances peuvent diminuer si le matériel n'est pas suffisamment puissant. Cela peut nécessiter des investissements supplémentaires dans des équipements matériels plus robustes.

Gestion et Maintenance

La gestion et la maintenance d'une installation pfSense peuvent être exigeantes, surtout dans des environnements complexes ou de grande envergure. Cela inclut la gestion des mises à jour, la surveillance continue du réseau, et la réponse rapide aux incidents de sécurité. Une surveillance insuffisante peut laisser des vulnérabilités ouvertes.

Support et Documentation

Bien que pfSense bénéficie d'une large communauté et de documentation abondante, le support direct peut être limité pour les versions gratuites. Les entreprises qui nécessitent un support rapide et dédié pourraient devoir souscrire à des services de support commercial, ce qui peut représenter un coût additionnel.

Compatibilité et Intégration

L'intégration de pfSense avec d'autres systèmes et logiciels de gestion de réseau peut parfois être compliquée. Certaines fonctionnalités avancées peuvent nécessiter des ajustements ou des développements supplémentaires pour assurer une compatibilité et une intégration sans faille avec les infrastructures existantes.

Risques de Sécurité liés à la Configuration

Une mauvaise configuration de pfSense peut introduire des vulnérabilités de sécurité. Par exemple, une mauvaise gestion des règles de pare-feu ou des politiques de VPN peut exposer le réseau à des attaques. Il est donc crucial que les administrateurs réseau soient bien formés et conscients des meilleures pratiques en matière de sécurité.

Conclusion

En conclusion, ce chapitre marque la finalisation de la conception et de l'implémentation de notre solution de sécurisation des communications en entreprise avec pfSense, axée sur le déploiement réussi du VPN IPsec. Les configurations ont été effectuées avec succès, mettant ainsi en place un réseau sécurisé et fiable conforme aux besoins des entreprises. En suivant les meilleures pratiques et en adaptant pfSense aux besoins spécifiques, les administrateurs réseau peuvent créer un système performant et fiable.

Conclusion générale

Ce mémoire a examiné l'implémentation d'un réseau sécurisé en utilisant pfSense, une solution open source robuste et flexible. À travers une analyse comparative, pfSense s'est révélé être une solution optimale en termes de sécurité, de fiabilité et de coût. En déployant une architecture réseau sécurisée avec IPsec, nous avons démontré comment pfSense peut garantir des communications sécurisées au sein d'une entreprise.

Les résultats obtenus confirment l'efficacité de pfSense pour protéger les données, assurer la confidentialité et maintenir la continuité des opérations. En conclusion, pfSense constitue une solution fiable et économique pour sécuriser les communications en entreprise, répondant ainsi aux exigences de sécurité modernes.

Perspectives

Bien que ce travail ait permis de mettre en évidence les avantages de l'utilisation de pfSense pour sécuriser les communications en entreprise, plusieurs axes d'amélioration et de développement futurs peuvent être envisagés :

Automatisation et Gestion Centralisée : Développer des outils d'automatisation et de gestion centralisée pour faciliter la configuration, la gestion et la supervision de multiples instances pfSense au sein de grandes infrastructures.

Intégration de l'Intelligence Artificielle : Explorer l'intégration de solutions basées sur l'intelligence artificielle pour améliorer la détection et la réponse aux menaces, en complément des fonctionnalités IDS/IPS existantes.

Formation et Sensibilisation : Mettre en place des programmes de formation continue pour les administrateurs réseau et les employés afin de renforcer la culture de sécurité au sein de l'entreprise.

Évaluation de la Scalabilité : Étudier la scalabilité de pfSense dans des environnements de très grande envergure, incluant des tests de performance et de résilience sous des charges réseau extrêmes.

Sécurité des Dispositifs IoT : Élargir l'utilisation de pfSense pour inclure la sécurisation des dispositifs IoT (Internet of Things), de plus en plus présents dans les infrastructures d'entreprise.

Conformité et Audit : Développer des modules complémentaires pour faciliter la conformité aux réglementations en vigueur (GDPR, HIPAA, etc.) et pour simplifier les processus d'audit de sécurité.

Bibliographie

[1] Organigramme dsi, visité le 19/10/2023. https://www.finances.bj/dsi/.

[2] Défense en profondeur, visité le 11/06/2024. https://www.youtube.com/watch?v=6_e0JcO9U-c/.

[3] Benchmarking, visité le 10/06/2024. https://sourceforge.net/software/compare/IPFire-vs-OPNsense-vs-OpenWrt-vs-pfSense/.

[4] Anssi, visité le 28/02/2024. https://cyber.gouv.fr/bonnes-pratiques-protegez-vous.

[5] Politiques, visité le 28/02/2024. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.checkpoint.com/fr/cyber-hub/network-security/what-is-security-management/what-is-information-security-management/&ved=2ahUKEwjFuo2Y7aiHAxVshP0HHSdOAj8QFnoECBQQAQ&usg=AOvVaw2RHVjG5IfeMwfqd0z5f-Zb.

[6] Openwrt, visité le 29/02/2024. https://openwrt.org/docs/start.

[7] Opnsense, visité le 29/02/2024. https://docs.opnsense.org/index.html.

[8] Ipfire, visité le 29/02/2024. https://www.ipfire.org/docs.

[9] pfsense, visité le 29/02/2024. https://docs.netgate.com/pfsense/en/latest/.

[10] Mémoire, visité le 23/01/2024. https://www.slideshare.net/MortadhaBouallagui/mmoire-de-projet-de-fin-dtudes-151512104.

[11] Gns3, visité le 26/01/2024. https://www.gns3.com/.

[12] Manuel pfsense, visité le 23/01/2024. https://www.academia.edu/7825940/pfSense_Manuel_dInstallation_et_dUtilisation_du_Logiciel.

[13] Gestion de clée, visité le 18/02/2024. https://www.digitalocean.com/community/tutorials/how-to-set-up-an-ikev2-vpn-server-with-strongswan-on-ubuntu-20-04.

[14] Ipsec, visité le 20/02/2024. https://www.it-connect.fr/vpn-site-to-site-ipsec-entre-deux-pfsense/.

[15] Vpn, visité le 25/02/2024. https://lawrence.technology/networking/vpn-performance-scaling-for-openvpn-and-ipsec-onpfsense/.

[16] Comparatif, visité le 28/02/2024. https://geekflare.com/fr/virtualbox-vs-vmware/.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

. iv

Abstract iv

. iv

Table des figures v

Liste des tableaux vi

Liste des acronymes vii

Glossaire 1

Introduction 2

1 État de l'art 5

Introduction 5

1.1 Sécurité du réseau : concepts et enjeux 5

1.1.1 Principes de Sécurité des Réseaux [4] 5

1.1.2 Principes de défense en profondeur et de gestion de la sécurité 6

1.1.3 Politiques de sécurité et processus de gestion [5] 7

1.1.4 Technologies et solutions de sécurité du réseau 7

1.2 Présentation des solutions open source 7

1.2.1 Définition et avantages des solutions open source en sécurité des réseaux . . . 7

1.2.2 Critères de sélection des solutions à étudier 8

1.3 Analyse des Principales Solutions Open Source 8

1.3.1 OpenWrt [6] 8

1.3.2 OPNsense [7] 10

1.3.3 IPFire [8] 11

1.3.4 pfSense [9] 12

1.3.5 Benchmarking comparatif entre les solutions open source 14

1.3.6 Choix de la solution 16

Conclusion 16

2 Présentation de la solution 17

Introduction . . . 17
2.1 Présentation de pfSense et de ses fonctionnalités . . . 17
2.1.1 Présentation générale de pfSense . . . 17
2.1.2 Fonctionnalités clés pour la gestion de la sécurité du réseau . . . 18
2.1.3 Avantages et limites de pfSense . . . 18
2.2 Alignement des besoins avec les fonctionnalités de pfSense . . . 19
2.2.1 Correspondance des fonctionnalités de pfSense aux besoins de sécurité . . . 19
2.2.2 Adaptation et personnalisation de pfSense pour répondre aux exigences spécifiques . . . 20
2.3 Présentation du réseau . . . 22
2.4 Choix du VPN . . . 22
2.4.1 Etude des VPN . . . 22
2.4.2 Choix du VPN adéquat . . . 23
2.4.3 Présentation IPSEC . . . 23
2.5 Choix techniques . . . 23
2.5.1 Emulateurs réseaux . . . 23
2.5.2 Logiciels de virtualisation . . . 25
Conclusion . . . 26

3 Conception et mise en œuvre de la solution **27**
Introduction . . . 27
3.1 Présentation des outils . . . 27
3.1.1 Le logiciel GNS3 . . . 27
3.1.2 VM WARE Workstation 17 Pro . . . 28
3.2 Implémentation de l'architecture réseau . . . 28
3.2.1 Emulation du réseau . . . 28
3.2.2 Test et résultats . . . 33
3.3 Réponse aux Objectifs de Sécurisation et limites de la solution . . . 34
3.3.1 Réponse aux Objectifs de Sécurisation par l'Implémentation de pfSense . . . 34
3.3.2 Limites de la solution implémentée avec pfSense . . . 35
Conclusion . . . 36

Conclusion **37**
Perspectives . . . 37

Bibliographie **38**

Table des matières **40**