République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaïa

Faculté des Sciences Exactes

Département Informatique

Mémoire de fin d'étude

En vue d'obtention du diplôme de Master Professionnel en Informatique
Spécialité : Administration et Sécurité des Réseaux

Thème

Interconnexion de deux serveurs de VoIP Asterisk sur un réseau multi-sites sécurisé par un canal VPN IPSec
Cas d'étude : Campus NTS

Réalisé par

- **Mlle AIT SALAH Yasmine**
- **Mlle LALOUCHE Kenza**

Membres du jury :

▪ **Mme HAMZA Lamia**	**MCA**	**U.A/Mira Bejaia**	**Présidente**
▪ **Mme BACHIRI Lina**	**MCA**	**U.A/Mira Bejaia**	**Encadrante**
▪ **Mme ZIDANI Ferroudja**	**MCB**	**U.A/Mira Bejaia**	**Examinatrice**

Année universitaire 2022/2023

Remerciement

Nous remercions tout d'abords, dieu le tout puissant de nous avoir accordé la force, la volonté et la connaissance pour réaliser ce travail ;

Nos plus sincères remerciements s'adressent à notre encadrante Mme L. BACHIRI, pour ses précieux conseils et encouragements tout au long de notre projet ;

Nous tenons aussi à remercier vivement les membres du jury pour avoir accepté d'évaluer notre projet. Nous leurs présentons toute nos gratitudes et nos profonds respects ;

Nos sincères remerciements vont aussi à notre encadrant de stage Mr Y. Djebbari pour son accueil, suivi et conseils durant toute notre période de stage pratique.

Nous adressons nos reconnaissances, nos remerciements et notre plus profonde gratitude à nos familles, en particulier nos parents, nos frères et sœurs pour leurs encouragements, aide et leur soutien tout au long de notre travail ;

Nous tenons à remercier tous nos amis et collègues qui nous ont soutenus en particulier ;

Enfin, nous tenons à exprimer notre profonde gratitude envers toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce projet. Leurs conseils, leur soutien et leur encouragement ont été d'une valeur inestimable tout au long de notre parcours.

Table des matières

Table des figures V
Liste des tableaux VII
Liste des abréviations VIII
Intoduction Générale 1

CHAPITRE 1 GÉNÉRALITÉS SUR LES RÉSEAUX ET LA SÉCURITÉ INFORMATIQUE **3**

Intoduction 4
Partie 1 : Généralités sur les réseaux informatiques 4
1 DÉFINITION 4
2 TOPOLOGIES D'UN RÉSEAU 4
2.1 Topologie logique 4
2.2 Topologie physique 4
3 ARCHITECTURES D'UN RÉSEAU LOCAL 6
3.1 Réseau poste à poste 6
3.2 Réseau client/serveur 6
4 MODÈLE D'UN RÉSEAU HIÉRARCHIQUE 6
4.1 Couche d'accès 7
4.2 Couche distribution 7
4.3 Couche cœur réseau 7
5 MODÈLE DE RÉFÉRENCE OSI 8
5.1 Définition 8
5.2 Principe 8
5.3 Rôle des différentes couches 8
6 MODÈLE TCP/IP 9
7 PROTOCOLE IP 11
Partie 2 : Initiation à la sécurité des réseaux informatique 11
1 SÉCURITÉ DES SYSTÈMES INFORMATIQUES 11
2 PRINCIPES DE LA SÉCURITÉ INFORMATIQUE 11

3 LES ATTAQUES INFORMATIQUES . . . 12
3.1 Définition . . . 12
3.2 Objectifs . . . 12
3.3 Types . . . 12
4 EXEMPLES D'ATTAQUES INFORMATIQUES [5] . . . 12
4.1 Les programmes malveillants . . . 12
4.2 Attaque de mots de passe . . . 13
4.3 Usurpation d'adresse IP . . . 13
4.4 Attaque par déni de service(DoS) . . . 13
5 MÉCANISMES DE DÉFENSE [5] . . . 13
5.1 Antivirus . . . 13
5.2 Chiffrement . . . 14
5.3 Pare-feu . . . 15
5.4 Proxys . . . 16
5.5 Systèmes de détection d'intrusion . . . 17
5.6 Sytèmes de prévention d'intrusion . . . 17
Conclusion . . . 17

CHAPITRE 2 ETAT D'ART SUR LA VOIP . . . 18

1 INTRODUCTION . . . 19
2 DÉFINITION . . . 19
3 AVANTAGE . . . 19
4 PRINCIPE DE FONCTIONNEMENT . . . 19
5 ARCHITECTURE ET MODES D'ACCÈS . . . 20
5.1 Architecture . . . 20
5.2 Modes d'accès . . . 21
6 DIFFÉRENCE ENTRE VOIP ET TOIP . . . 23
7 DIFFÉRENCE ENTRE PABX ET IPBX . . . 23
8 PROTOCOLES DE LA VOIP . . . 24
8.1 Protocoles de signalisation . . . 24
8.2 Protocoles de transport . . . 25
9 PROTOCOLES RTP . . . 27
9.1 Fonctions . . . 27
9.2 En-tête RTP . . . 27
9.3 Avantages et inconvénients . . . 28
10 PROTOCOLE SIP . . . 29
10.1 Définition . . . 29
10.2 Architecture . . . 29
10.3 Adressage SIP . . . 31

10.4 Méthodes utilisées . . . 31
10.5 Codes de réponses . . . 31
10.6 Communication SIP . . . 32
10.7 Avantages . . . 34
10.8 Inconvénients . . . 34
11 PROTOCOLE IAX/IAX2 . . . 34
11.1 Définition . . . 34
11.2 Caractéristiques . . . 35
11.3 Requêtes et réponses IAX . . . 35
11.4 Etablissement d'une connexion IAX . . . 36
12 QUALITÉ DE SERVICE (QOS) . . . 36
12.1 Définition . . . 36
12.2 Temps de latence . . . 37
12.3 La gigue . . . 37
12.4 L'Echo . . . 37
12.5 La perte de paquets . . . 37
13 CONCLUSION . . . 38

CHAPITRE 3 LES ATTAQUES ET LA SÉCURITÉ DE LA VOIP . . . 39

1 INTRODUCTION . . . 40
2 ATTAQUES CONTRE LA VOIP . . . 40
2.1 Spam . . . 40
2.2 Suivie d'appels . . . 40
2.3 Voice Phishing . . . 41
2.4 Sniffing . . . 41
2.5 Déni de service (DoS) . . . 42
3 SOLUTIONS DE SÉCURITÉ . . . 44
3.1 VPN . . . 44
3.2 VLANs . . . 47
3.3 Pare-feu . . . 49
4 CONCLUSION . . . 50

CHAPITRE 4 RÉALISATION . . . 51

Intoduction . . . 52
Partie 1 : Présentation de l'organisme d'accueil . . . 52
1 PRÉSENTATION DE L'ENTREPRISE CAMPUS NTS . . . 52
1.1 Création et évolution . . . 52
1.2 Localisation . . . 52
1.3 Fiche technique . . . 53

1.4 Objectifs, Missions et activités de l'entreprise NTS 53
1.5 Organigramme général 54
2 ETUDE DE L'EXISTANT 58
2.1 Présentation du réseau campus NTS 58
2.2 Analyse du parc informatique 59
Partie 2 : Réalisation 61
1 OUTILS DE TRAVAIL 61
2 EQUIPEMENTS UTILISÉS 63
3 MÉTHODOLOGIE DE TRAVAIL 63
4 ARCHITECTURE PROPOSÉE 64
5 INSTALLATIONS 64
5.1 PFsense 64
5.2 FreePBX 65
6 CONFIGURATIONS DE BASE 68
6.1 Plan d'adressage 68
6.2 Interfaces en mode trunk 69
6.3 Configuration VTP 70
6.4 Création des Vlans 71
6.5 Affectation des ports mode access 71
6.6 Configurations routeur 72
6.7 Configuration Firewall 74
7 CONFIGURATION DES VPN 76
7.1 VPN site to site IPSec 76
7.2 VPN client to site 79
8 CONFIGURATION DE FREEPBX 84
8.1 Création des comptes SIP 84
8.2 Interconnexion des deux serveurs VoIP 85
9 TESTS 88
9.1 Interfaces mode trunk 88
9.2 Configuration VTP 89
9.3 Configuration VLANs 89
9.4 Vérification du tunel IPSec 90
9.5 Tests des configurations FreePBX 90
Conclusion 91
Conclusion Générale 92
Bibliographie 93
Annexe i

Table des figures

1.1 Topologie en bus 5
1.2 Topologie en étoile 5
1.3 Topologie en anneau 6
1.4 Modèle d'un réseau hiérarchique [19] 7
1.5 Encapsulation de données 9
1.6 Chiffrement symétrique 14
1.7 Chiffrement asymétrique 14
1.8 Pare-feu 15
1.9 Proxy 16

2.1 Principe de fonctionnement de la VoIP [7] 20
2.2 Architecture d'un réseau VoIP 21
2.3 Mode d'accès PC à PC 22
2.4 Mode d'accès PC à téléphone 22
2.5 Mode d'accès entre deux téléphones 22
2.6 Protocoles de transport 26
2.7 Enregistrement d'un utilisateur 29
2.8 Serveur Proxy SIP 30
2.9 Communication SIP 33
2.10 Echange de données entre plusieurs serveurs Asterisk 35

3.1 Voice Phishing attack 41
3.2 Sniffing attack 42
3.3 DoS de type CANCEL 43
3.4 DoS de type BYE 44
3.5 VPN 45
3.6 VPN d'accès 45
3.7 Extranet VPN 46
3.8 VLAN niveau 1 48

4.1 Localisation de l'entreprise NTS 52
4.2 Objectifs, Messions et Activités du Campus NTS 53
4.3 Organigramme général du Campus NTS 54
4.4 organigramme du service infrastructure réseau et sécurité 55
4.5 Architecture du réseau NTS 59
4.6 GNS3 61
4.7 VMware 61
4.8 PFsense 62
4.9 FreePBX 62
4.10 Softphones 62

4.11 Méthodologie de travail 63
4.12 Architecture proposée 64
4.13 Démarrage du PFsense 64
4.14 Début de processus d'installation 65
4.15 Début d'installation 65
4.16 Démarrage de l'installation 65
4.17 Paramètres d'avant installation 66
4.18 Authentification de l'administrateur 66
4.19 Adresse IP du serveur FreePBX 67
4.20 Login au serveur FreePBX 67
4.21 Interface de FreePBX 68
4.22 Interfaces de FW-bejaia 74
4.23 L'interface de login du PfSense 75
4.24 Règle d'autorisation 75
4.25 Routage vers les vlans 76
4.26 Phase 1 : Création de la clé de chiffrement 77
4.27 Phase 2 : Négociation du chiffrement de tunnel VPN 78
4.28 Autorisation du trafic dans le tunnel 79
4.29 Création d'un certificat d'autorité 80
4.30 Création d'un certificat serveur 81
4.31 Création d'un certificat OpenVPN 82
4.32 Création d'un utilisateur VPN 83
4.33 Package OpenVPN-client-export 83
4.34 Comptes SIP du site Bejaia 85
4.35 Comptes SIP du site Alger 85

Liste des tableaux

1.1 Couches OSI correspondantes aux couches TCP/IP 10

2.1 En-tête RTP 27

4.1 Fiche technique du Campus NTS 53
4.2 L'environnement hardware et software 60
4.3 Détails des ressources disponibles de l'entreprise 60
4.4 Détails des équipements utilisés 63
4.5 Adressage des équipements 68
4.6 Adressage des Vlans 69
4.7 Routage inter Vlans 69

Liste des abréviations

ACK	ACKnowledged
AH	Authentication Header
ARP	Address Resolution Protocol
BICC	Bearer Independent Call Control
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DSP	Digital Signal Processor
ESP	Encapsulating Security Payload
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
IAP	Internet Access Provider
IAX	Inter Asterisk eXchange
ICMP	Internet Control Message Protocol
IDS	Intrusion detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPBX	Internet Protocol Private Branch eXchange
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
LLC	Logical Link Control
L2TP	Layer 2 Tunneling Protocol
MAC	Media Access Control
MGCP	Media Gateway Control Protocol
NAT	Network Address Translation
NIDS	Network Intrusion Detection System

NTS	Nouvelles Technologies de l'information et Sécurité
OSI	Open Systems Interconnection
PABX	Private Automated Branch Exchange
PBX	Private Branch eXchange
POP	Post Office Protocol
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
RARP	Reverse Adresse Résolution Protocol
RTC	Réseau téléphonique commuté
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SMTP	SimpleMail Transfer Protocol
TCP	Transmission Control Protocol
TELNET	TELecommunication NETwork
ToIP	Telephony over Internet Protocol
UDP	User Datagram Protocol
UIT	Union Internationale des Télécommunications
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
WAN	Wide Area Network

Introduction générale

Actuellement, le développement de la technologie de transmission vocale basée sur le protocole IP (Internet Protocol) est un aspect essentiel de la transformation en cours du secteur des communications.

Il y a quelque temps, la seule option de communication disponible était le service téléphonique traditionnel ou RTC (Réseau Téléphonique Commuté). L'arrivée de la technologie révolutionnaire VoIP a transformé la façon dont les communications vocales sont effectuées, offrant une alternative aux systèmes de téléphonie traditionnels. En exploitant les infrastructures existantes d'Internet, la VoIP a ouvert de nouvelles possibilités pour les particuliers, les entreprises et les institutions, offrant une flexibilité, une efficacité et une économie sans précédent.

Au lieu de disposer à la fois d'un réseau informatique et d'un RTC, l'entreprise peut, grâce à la VoIP (Voice over Internet Protocol), tout fusionner sur un même réseau. Cette innovation technologique permet donc de simplifier le travail et de réaliser des économies significatives en termes de coûts de communication.

Les systèmes de VoIP fournissent une gamme variée de prestations selon divers modes de communication, tels que PC à PC, PC à téléphone, etc. En incorporant des outils d'interface pour les réseaux téléphoniques traditionnels, cette technologie a évolué en un outil de communication via Internet. Elle emploie des protocoles spécialement élaborés pour cette catégorie d'application, tels que RTP (Real-time Transport Protocol), qui travaille conjointement avec des protocoles de signalisation comme SIP (Session Initiation Protocol), IAX (Inter Asterisk eXchange), etc.

L'apparition de la VoIP comporte des inconvénients, notamment en ce qui concerne la sécurité, puisque elle cumule les vulnérabilités de la téléphonie classique et celles des réseaux informatiques. Ainsi, lorsqu'une entreprise ou un particulier met en place ou adopte une solution de VoIP, cela peut exposer ses systèmes à de nouveaux risques.

En raison de l'intégration étroite avec l'infrastructure informatique, il est crucial de prendre en compte la sécurité des flux vocaux lors de l'administration des systèmes et des périphériques. Cela est particulièrement important avec l'émergence de solutions IP, qui renforcent la nécessité de sécurité et de fiabilité. En bref, plus la sécurité est renforcée, moins il y a de risques.

Afin d'explorer en profondeur le domaine de VoIP, et de mettre en pratiques les connaissances théoriques acquises au cours de nos études, nous avons choisi d'effectuer un stage pratique au sein de l'entreprise Campus NTS (Nouvelles Technologies de l'information et Sécurité) spécialisée dans l'étude, la conception et la réalisation de solutions.

Problématique

Les difficultés sont multiples au sein de l'entreprise Campus NTS en ce qui concerne le système des communications pour ses personnels.
De cet ordre d'idées, il convient de se poser quelques questions, telles que :

- ➢ **Est-il possible d'améliorer les moyens de communication au sein de Campus NTS ?**
- ➢ **Est-il possible d'implémenter la solution VoIP dans un réseau informatique à multi-sites ?**
- ➢ **Comment sécuriser la solution VoIP qui sera implémentée ?**

Dans ce contexte, et dans le cadre de notre projet de fin d'étude, nous sommes appelé à interconnecter deux serveurs PBX (Private Branch eXchange) pour deux sites de l'entreprise "Campus NTS", un à Bejaia et l'autre à Alger, où chaque site dispose de son propre serveur PBX local. Pour assurer la sécurité des communications entre ces deux sites, nous allons procéder à la création de trois VLANs (Virtual Local Area Network) pour chaque site (vlan voix, vlan data et vlan gestion), en plus de ça, un canal VPN (Virtual Private Network) IPsec (Internet Protocol Security) sera établi. L'IPsec offre des mécanismes de cryptage, d'authentification et d'intégrité des données, garantissant ainsi la confidentialité et la protection contre les attaques potentielles.

Objectif

L'objectif principal de ce travail est de montrer l'importance de l'intégration de la VoIP dans les entreprises, et de proposer l'implémentation de cette technologie au sein du réseau informatique de l'entreprise Campus NTS.

Structure du mémoire

Ce mémoire est composé de quatre chapitres :

Le premier chapitre intitulé " Généralités sur les réseaux et la sécurité informatique" où nous présenterons quelques concepts de base des réseaux informatiques, et certaines notions sur la sécurité informatique.

Le deuxième chapitre intitulé " Etat d'art sur la VoIP " nous permet d'avoir une idée sur la VoIP, son architectures, son fonctionnement et les différents protocoles utilisés au sein du réseau VoIP.

Le troisième chapitre "Les attaques et sécurité de la VoIP" est consacré à une brève étude sur les attaques sur la VoIP et quelques solutions de sécurisation.

Le dernier chapitre "Réalisation" est divisé en deux parties : la première présente l'entreprise qui nous a accueilli pour faire notre stage pratique, la deuxième présente la réalisation de notre solution VoIP.

Chapitre 1

Généralités sur les réseaux et la sécurité informatique

Introduction

Pour mener à bien notre projet, nous allons commencer par expliquer les concepts des réseaux informatiques, et définir certains concepts de la sécurité informatique.

Nous avons divisé ce premier chapitre en deux grandes parties. Dans la première, nous allons aborder les concepts des réseaux informatiques, puis dans la deuxième partie nous passerons à la sécurité informatique, ses principes et son utilisation au sein des réseaux informatiques.

Partie 1 : Généralités sur les réseaux informatiques

1 Définition

Un réseau informatique est un ensemble d'équipements reliés entre eux qui permettent la communication et le partage de données et de ressources. Les équipements peuvent inclure des ordinateurs, des serveurs, des routeurs, des périphériques de stockage de données, etc. Les réseaux informatiques peuvent être locaux (LAN (Local Area Network)) ou étendus sur de grandes distances (WAN (Wide Area Network)).

2 Topologies d'un réseau

Pour pouvoir utiliser un réseau, Il faut définir, en plus du type de réseau, une méthode d'accès entre les ordinateurs, ce qui nous permettra de connaître la manière dont les informations sont échangées.

Il existe deux types de topologies : topologie logique et topologie physique [2].

2.1 Topologie logique

Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token ring et FDDI (Fiber Distributed Data Interface).

2.2 Topologie physique

La topologie physique est la façon dont les équipements sont connectés physiquement les uns aux autres grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, etc.).

Il existe trois topologies physiques dans les réseaux locaux : la topologie en bus, en étoile, et en anneau qui peuvent être combinées pour obtenir des topologies hybrides [2].

- **Topologie en bus :** Est une topologie dans laquelle tous les dispositifs sont connectés à un même câble (généralement coaxial) appelé « bus » (figure 1.1).
  Elle est souvent utilisée dans les petits réseaux locaux pour connecter les ordinateurs, les imprimantes et d'autres dispositifs.

FIGURE 1.1 – Topologie en bus

- **Topologie en étoile :** Est une topologie dans laquelle tous les nœuds sont connectés à un périphérique central, formant ainsi une étoile (figure 1.2). Deux types de périphériques fournissant un point de connexion central commun aux nœuds du réseau sont un Hub et un Switch.

FIGURE 1.2 – Topologie en étoile

- **Topologie en anneau :** Est une topologie dans laquelle les dispositifs sont connectés en un cercle fermé (boucle) (figure 1.3). Les données sont transmises dans un seul sens autour de l'anneau, permettant à chaque dispositif de recevoir et de transmettre les données.

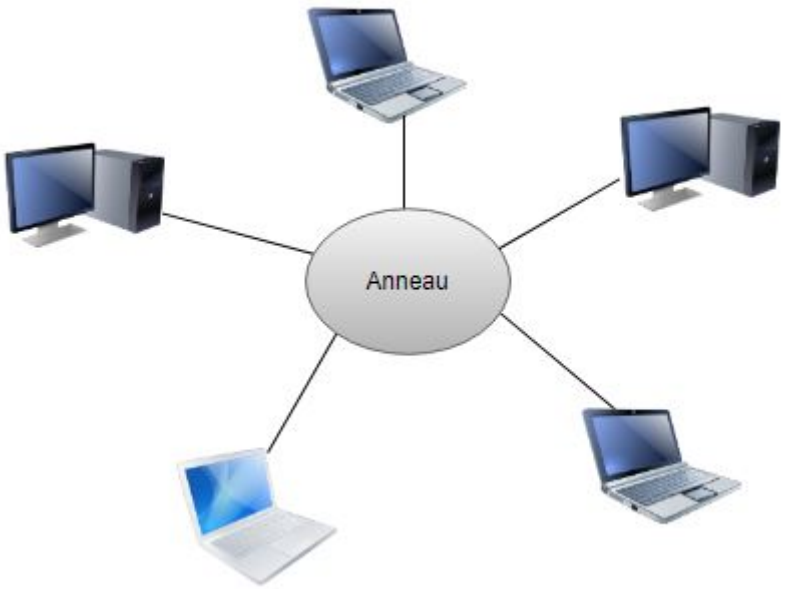


FIGURE 1.3 – Topologie en anneau

3 Architectures d'un réseau local

On distingue deux types d'architecture de réseaux : le poste à poste et le client/serveur [1].

3.1 Réseau poste à poste

Est un type d'architecture dans lequel chaque ordinateur ou logiciel est à la fois client et serveur. Cette architecture ne convient que pour un petit réseau.

3.2 Réseau client/serveur

L'architecture client/serveur désigne un mode de communication entre plusieurs ordinateurs d'un réseau qui distingue un ou plusieurs clients du serveur : chaque logiciel client peut envoyer des requêtes à un serveur. Un serveur peut être spécialisé en serveur d'applications, de fichiers ou encore de messagerie électronique.

4 Modèle d'un réseau hiérarchique

Le modèle hiérarchique à trois couches est proposé par Cisco Systems pour les topologies de conception de réseau. Il permet l'agrégation et le filtrage du trafic à trois niveaux successifs de routage ou de commutation. Cela rend le modèle hiérarchique à trois couches évolutif pour les grandes infrastructures Internet internationales [19]. La figure 1.4 explique l'architecture d'un réseau hiérarchique.

4.1 Couche d'accès

Cette couche permet de connecter les périphériques des utilisateurs finaux au réseau. A ce niveau, on utilise des switches de niveau 2 car la configuration de ce type de switches pose moins de contraintes : le besoin en performance n'est pas vraiment une nécessité car chaque switch aura un nombre d'utilisateur égal à son nombre de ports. Les traitements restent basiques et demandent peu de ressources.

4.2 Couche distribution

Le rôle de cette couche est de filtrer, router et autoriser ou non les paquets. La segmentation du réseau commence ici en ajoutant plusieurs switches de niveau 3 qui sont reliés à la fois à la couche cœur et d'accès.

4.3 Couche cœur réseau

C'est la couche supérieure dont le rôle consiste à relier entre les différents segments d'un réseau à savoir : les sites distants, les réseaux locaux (LANs) etc.

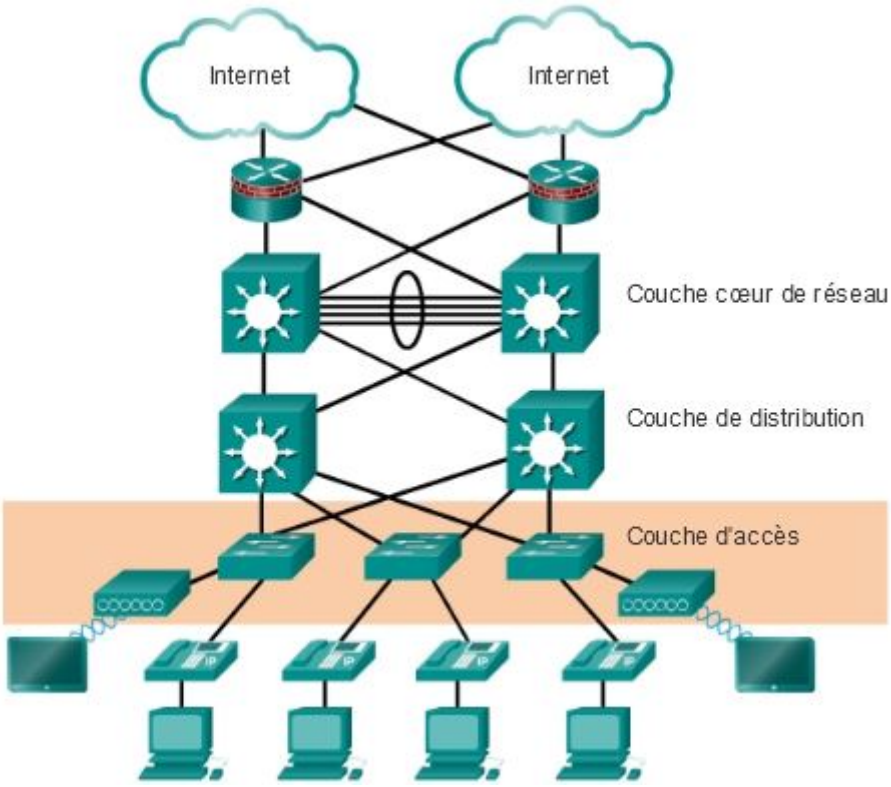


FIGURE 1.4 – Modèle d'un réseau hiérarchique [19]

5 Modèle de référence OSI

5.1 Définition

Le modèle OSI (Open Systems Interconnections) est un modèle de référence standard utilisé pour décrire les fonctionnalités nécessaires pour assurer la communication efficace entre les ordinateurs sur un réseau informatique. Il définit sept couches de fonctionnalités qui doivent être implémentées pour permettre une communication réseau efficace [3].

5.2 Principe

Le principe de ce modèle est basé sur l'encapsulation de données (figure 1.5) qui est un processus qui consiste à empaqueter les données à transmettre en unités logiques appelées "paquets" ou "datagrammes". Cela permet à chaque couche du modèle OSI d'ajouter des informations supplémentaires, telles que les en-têtes, qui fournissent des informations de contrôle sur la transmission de données, cela garantit que les données soient transmises de manière cohérente et fiable à travers les différentes couches du modèle OSI.

5.3 Rôle des différentes couches

Chaque couche définie par le modèle a un rôle bien précis, qui va du transport du signal codant les données à la présentation des informations pour l'application du destinataire [4] :

1. **La couche physique :** Elle convertit les signaux électriques en bits de données et inversement, selon qu'elle transmet ou reçoit les informations de la couche suivante.
2. **La couche liaison de données :** Elle est divisée en deux sous-couches :
   - La couche MAC (Media Access Contro) qui structure les bits de données en trames et gère l'adressage des cartes réseaux.
   - La couche LLC (Logical Link Contro) qui assure le transport des trames et gère l'adressage des utilisateurs, c'est à dire des logiciels des couches supérieures.
3. **La couche réseau :** Elle traite la partie donnée utile contenue dans la trame. Elle connaît l'adresse de tous les destinataires et choisit le meilleur itinéraire pour l'acheminement. Elle gère donc l'adressage logique et le routage
4. **La couche transport :** Elle segmente les données de la couche session, prépare et contrôle les taches de la couche réseau. Elle peut multiplier les voies d'accès et corriger les erreurs de transport.
5. **La couche session :** Son unité d'information est la transaction. Elle s'occupe de la gestion et la sécurisation du dialogue entre les machines connectées, les applications et les utilisateurs (noms d'utilisateurs, mots de passe, etc.)

6. **La couche présentation :** Elle convertit les données en informations compréhensibles par les applications et les utilisateurs ; syntaxe, sémantique, conversion des caractères graphiques, format des fichiers, cryptage, compression.
7. **La couche application :** C'est l'interface entre l'utilisateur ou les applications et le réseau. Elle concerne la messagerie, les transferts et partages de fichiers, l' ´émulation de terminaux.

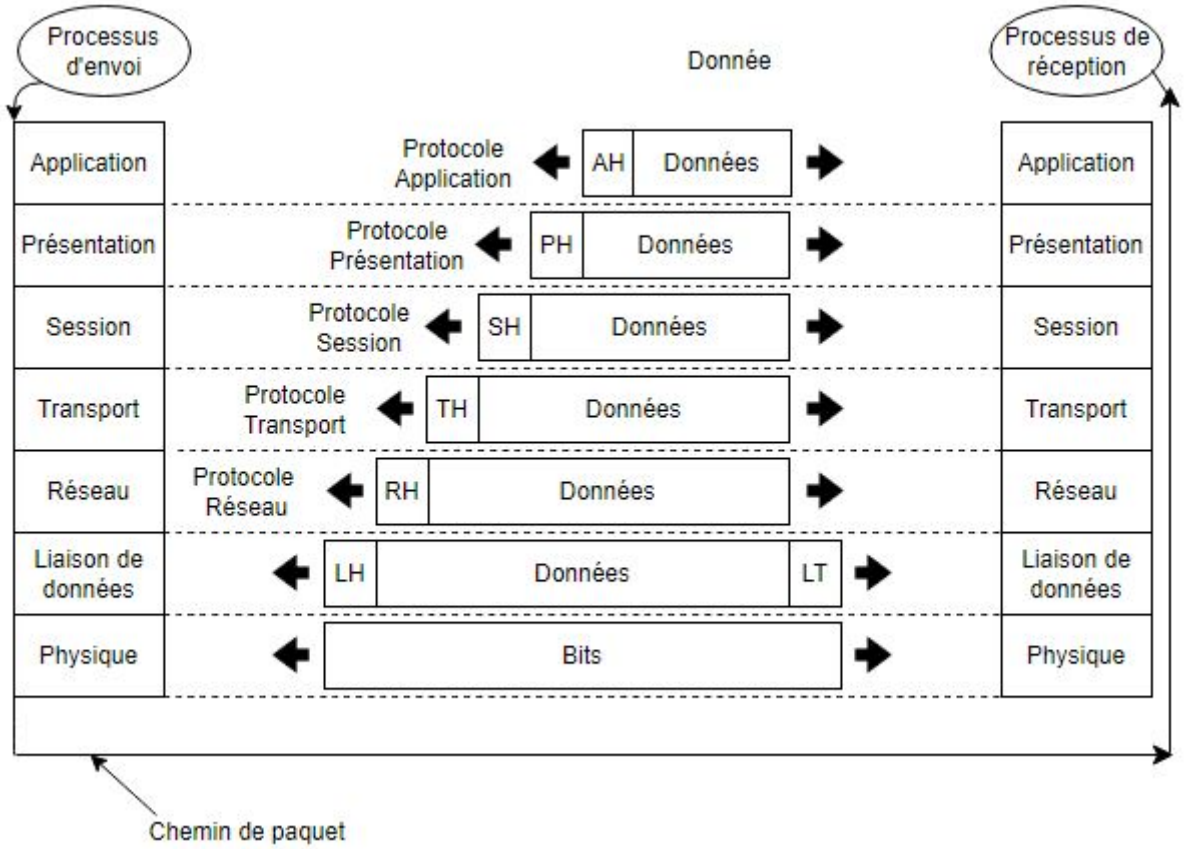


FIGURE 1.5 – Encapsulation de données

6 Modèle TCP/IP

TCP/IP est un protocole de liaison de données utilisé sur Internet pour permettre aux ordinateurs et autres appareils d'envoyer et de recevoir des données. L'acronyme TCP/IP signifie Transmission Control Protocol/Internet Protocol. Il permet aux appareils connectés à Internet de communiquer entre eux via les réseaux. Les deux protocoles dominats dans ce modèle sont : IP qui se charge de l'acheminement des paquets de données à travers le réseau, et TCP qui est responsable de la retransmission des paquets altérés ou perdus dans le réseau, c'est un protocole fiable et orienté connexion ce qui lui

permet de garantir l'ordre de remise des paquets.

Le modèle TCP/IP est divisé en quatre couches [4] :

1. **La couche application :** La Couche Application reprend les applications standards en réseau informatique et Internet. Elle dispose des protocoles suivants : SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol), TELNET (TELecommunication NETwork), FTP (File Transfert Protocol).
2. **La couche transport :** La couche transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP, fournit d'excellents moyens de créer, en souplesse, des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé.
3. **La couche internet :** La couche Internet est chargée de fournir le paquet des données. Elle définit les datagrammes et gère la décomposition / recomposition des segments. La couche Internet utilise les cinq protocoles suivants : IP, ARP (Adresse Résolution Protocol), ICMP (Internet Control Message Protocol), RARP (Reverse Adresse Résolution Protocol), IGMP (Internet Group Management Protocol).
4. **La couche accès réseau :** Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On lui donne également le nom de couche hôte-réseau. Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches physiques et liaison de données du modèle.

Couches du modèle TCP/IP	Couches du modèle OSI
Application	Application
	Présentation
	Session
Transport	Transport
Internet	Réseau
Accès réseau	Liaison de données
	Physique

TABLE 1.1 – Couches OSI correspondantes aux couches TCP/IP

7 Protocole IP

IP est un protocole de la couche réseau du modèle TCP/IP. Il est responsable de l'acheminement des paquets de données à travers un réseau en utilisant des adresses IP uniques pour identifier les ordinateurs. Il ne garantit pas la fiabilité de la transmission de données, mais se concentre sur la livraison des paquets à leur destination.

IP est un protocole non connecté, ce qui signifie qu'il n'établit pas de connexion préalable avant de transmettre des données et n'assure pas la livraison des paquets dans l'ordre. C'est pourquoi d'autres protocoles sont utilisés conjointement avec IP pour garantir la fiabilité de la transmission de données.

IP est un protocole essentiel pour les réseaux informatiques et est utilisé sur de nombreux réseaux, y compris Internet, pour transmettre des données entre des ordinateurs distants.

Partie 2 : Initiation à la sécurité des réseaux informatique

1 Sécurité des systèmes informatiques

La sécurité des systèmes informatiques est l'ensemble des mesures et des pratiques visant à protéger les systèmes informatiques et les données qui y sont stockées contre les menaces telles que les attaques, les intrusions, les virus et les erreurs de manipulation. Cela comprend la mise en œuvre de politiques de sécurité, la formation des utilisateurs, la mise à jour de logiciels de sécurité, l'encryption des données sensibles, etc.

2 Principes de la sécurité informatique

La sécurité des systèmes d'information vise à assurer les propriétés suivantes [4] :

- **Confidentialité :** Garantir que les données sensibles ne sont accessibles qu'aux personnes autorisées.
- **Intégrité :** S'assurer que les données ne sont pas altérées ou modifiées sans autorisation.
- **Disponibilité :** Garantir que les systèmes et les données sont accessibles aux utilisateurs autorisés en tout temps.
- **Authentification :** S'assurer que les utilisateurs et les transactions sont légitimes.
- **Non-répudiation :** Permettre de prouver l'origine d'une transaction ou d'un message pour empêcher les utilisateurs de nier leur participation.

3 Les attaques informatiques

3.1 Définition

Une attaque informatique est l'exploitation d'une faille d'un système informatique pour endommager, compromettre ou pénétrer dans ce système sans autorisation [5]. Les attaques informatiques peuvent être menées par des individus, des groupes criminels ou même des gouvernements.

3.2 Objectifs

L'objectif de ces attaques peut varier : vol d'informations confidentielles, corruption de données, interruption de service, destruction de données, surveillance illégale, prise de contrôle à distance des systèmes informatiques, etc.

3.3 Types

3.3.1 Attaques passives

Les attaques passives sont des formes d'intrusion dans les systèmes informatiques qui visent à recueillir des informations sensibles en écoutant le réseau de manière non autorisée sans interrompre ou endommager les systèmes cibles.

3.3.2 Attaques actives

Les attaques actives sont des formes d'intrusion dans les systèmes informatiques qui visent à endommager ou interrompre les systèmes cibles.

4 Exemples d'attaques informatiques [5]

4.1 Les programmes malveillants

Sont des logiciels conçus pour causer des dommages ou pour compromettre les systèmes informatiques sans l'autorisation de l'utilisateur. Il existe plusieurs types de programmes malveillants, notamment :

- Virus : Est un programme qui se propage à d'autres ordinateurs en se copiant lui-même dans des fichiers ou des dossiers.
- Vers : Ou virus réseau, est un programme qui se propage de manière autonome (sans avoir besoin d'un support physique ou logique) à partir d'un ordinateur infecté à d'autres ordinateurs en utilisant les réseaux informatiques.
- Logiciels espions : Sont conçus pour surveiller les activités de l'utilisateur sans son consentement et sans qu'il en soit informé.

- Chevaux de Troie : Est un programme malveillant qui se dissimule sous un autre logiciel légitime pour compromettre les systèmes informatiques.
- Ransomware : Est un type de logiciel malveillant qui chiffre les fichiers de l'utilisateur et exige une rançon pour déchiffrer les données.
- Bombe logique : Est un type de logiciel malveillant conçu pour causer des dommages à un système informatique en exécutant une tâche spécifique au moment programmé (date ou événement déterminé).
- Rootkit : Est un type de logiciel malveillant qui permet à un attaquant de prendre le contrôle d'un système informatique sans être détecté.

4.2 Attaque de mots de passe

Est une tentative de vol de mot de passe par un pirate. Il existe plusieurs types d'attaque de mot de passe notamment :

- **La force brute :** qui consiste à casser un mot de passe en testant tous les combinaisions possibles.
- **Attaque par dicionnaire :** est une attaque qui consiste à tester une série de mots de passe qui utilisent des mots du dictionnaire ou des expressions courantes. Cette méthode repose sur le fait que de nombreuses personnes utilisent des mots de passe ayant une signification réelle (nom, date de naissance, etc.).

4.3 Usurpation d'adresse IP

Est une technique qui consiste à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate de cacher son identité.

4.4 Attaque par déni de service(DoS)

Est un type d'attaque informatique qui vise à rendre un système ou un service inaccessible aux utilisateurs légitimes pendant un temps indéterminé en mettant le système en panne ou le ralentissant au point de le rendre inutilisable. Pour cela, différentes techniques sont utilisées telles que : l'envoi massif de demandes de connexion au système, l'utilisation de logiciels malveillants pour épuiser les ressources du système ou la saturation du trafic réseau.

5 Mécanismes de défense [5]

5.1 Antivirus

Sont des logiciels de sécurité informatique conçus pour détecter et éliminer les logiciels malveillants. Ils utilisent des algorithmes de détection pour rechercher des signatures connues de malware

dans les fichiers et les processus en cours d'exécution sur un système.

5.2 Chiffrement

Est une technique de sécurité informatique utilisée pour protéger l'intégrité et la confidentialité des données. Il implique l'utilisation d'un algorithme de chiffrement pour convertir les données en un format codé appelé chiffré, qui ne peut être déchiffré que par une personne ayant la clé de déchiffrement correspondante.

- **Chiffrement symétrique :** Il utilise la même clé pour chiffrer et déchiffrer les données (figure 1.6). Cette clé doit être partagée en toute sécurité entre les parties impliquées.

FIGURE 1.6 – Chiffrement symétrique

- **Chiffrement asymétrique :** Il utilise une paire de clés publique et privée pour chiffrer et déchiffrer les données (figure 1.7). La clé publique peut être partagée publiquement, tandis que la clé privée doit être protégée.

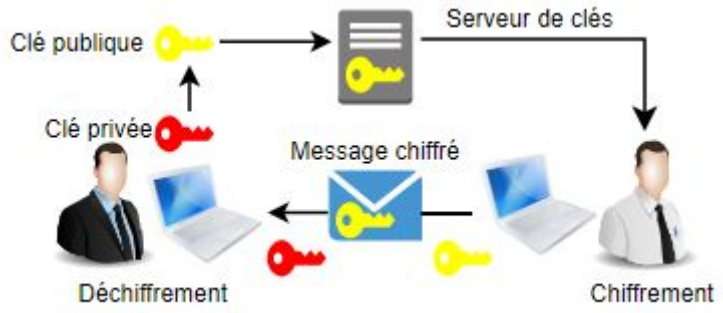


FIGURE 1.7 – Chiffrement asymétrique

- **Signature numérique :** Est un mécanisme permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification) et de vérifier l'intégrité du message reçu (fonction de hachage). Elle assure également une fonction de non répudiation, qui permet d'assurer que l'expéditeur a bien envoyé le message (empêche l'expéditeur de nier avoir expédié le message).

- **Certificats éléctroniques :** Les algorithmes de chiffrement asymétrique sont basés sur le partage d'une clé publique entre les différents utilisateurs. Généralement le partage de cette clé se fait à travers un annuaire électronique ou bien un site web. Toutefois ce mode de partage a une grande lacune : rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée. En effet un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique. Il a donc fallu créer un mécanisme supplémentaire, qui est les certificat électronique, pour assurer la validité de la clé publique.

  Un certificat est équivalent à une carte d'identité utilisé pour lier une clé publique à son entité. Il est délivré et signé par une autorité de certification. Un certificat contient les informations suivantes : La version de X.509 à laquelle le certificat correspond,lLe numéro de série du certificat,lL'algorithme de chiffrement utilisé pour signer le certificat, le nom de l'autorité de certification émettrice, la date de début et de fin de validité du certificat, l'objet de l'utilisation de la clé publique, la clé publique du propriétaire du certificat et la signature électronique de l'autorité de certification.

5.3 Pare-feu

Un pare-feu est un système de sécurité informatique utilisé pour contrôler l'accès au réseau. Il agit en agissant comme une barrière entre un réseau interne considéré comme fiable et un réseau externe considéré comme potentiellement dangereux, tels que Internet (figure 1.8).

Les pare-feu peuvent être logiciels ou matériels et sont configurés pour autoriser ou bloquer le trafic en fonction de règles définies. Les règles peuvent inclure des restrictions en matière de protocoles de communication, de ports et d'adresses IP.

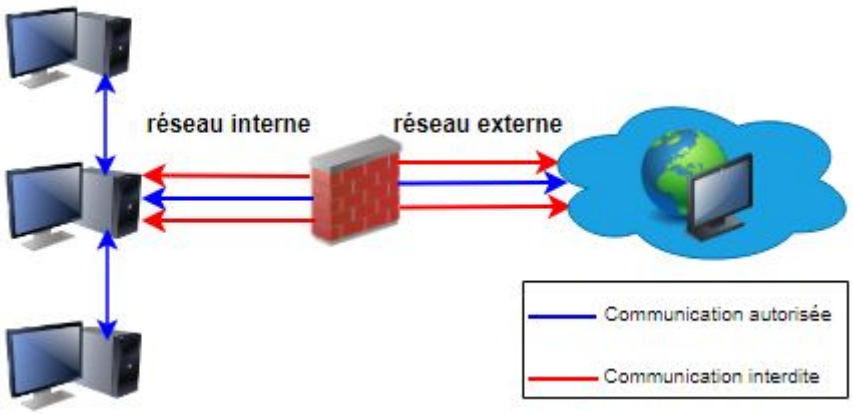


FIGURE 1.8 – Pare-feu

5.4 Proxys

Un proxy est un serveur mandataire qui agit comme un intermédiaire entre un client et un autre serveur (figure 1.9). Il peut être utilisé pour plusieurs raisons, notamment :

- Anonymat : Le proxy cache l'adresse IP du client, ce qui le rend plus difficile à localiser en ligne.
- Filtrage de contenu : Le proxy peut être configuré pour bloquer l'accès à certains types de sites web ou à certains types de contenu.
- Accélération de la vitesse : Le proxy peut stocker en cache les pages web les plus populaires pour les servir plus rapidement aux utilisateurs.
- Contournement de restrictions : Le proxy peut être utilisé pour contourner les restrictions géographiques et les filtres de contenu.

Il existe plusieurs types de proxy, notamment les proxies HTTP(Hypertext Transfer Protocol), les proxies SOCKS et les proxies anonymes. Chacun de ces types de proxy peut être utilisé pour répondre à des besoins spécifiques en matière de confidentialité, de vitesse et de filtrage.

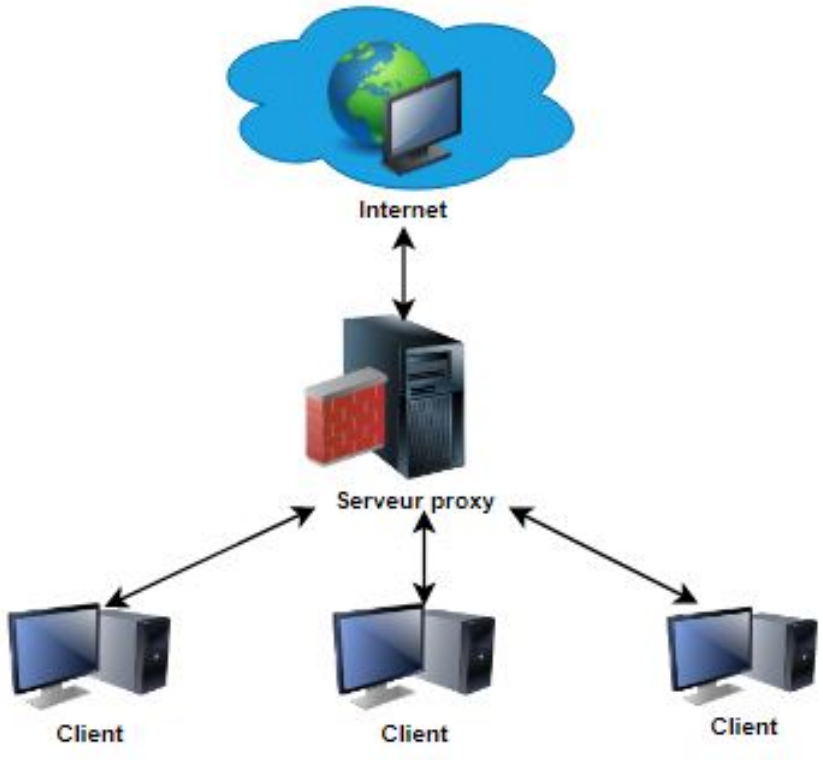


FIGURE 1.9 – Proxy

5.5 Systèmes de détection d'intrusion

Un IDS (Intrusion Detection System) est un mécanisme de sécurité qui permet de repérer les activités douteuses ou anormales sur un réseau ou un système et alerter les responsables de sécurité. On peut ainsi obtenir une connaissance des tentatives réussies ou échouées d'attaque ou d'intrusion sur le système.

On distingue trois types d'IDS : les NIDS (Network Intrusion Detection System), qui assurent la sécurité au niveau du réseau, les HIDS (Host Intrusion Detection System), qui surveillent l'activité d'un hôte, et enfin les IDS hybrides, qui combinent HIDS et NIDS pour avoir des alertes plus pertinentes.

5.6 Sytèmes de prévention d'intrusion

Les IPS (Intrusion Prevention System)ont pour fonction principale d'empêcher toute activité suspecte détectée au sein d'un système, ils sont capables de prévenir une attaque avant qu'elle atteigne sa destination. Contrairement aux IDS, les IPS sont des outils aux fonctions « actives », qui en plus de détecter une intrusion, tentent de la bloquer.

Conclusion

Ce chapitre nous a permis en premier lieu de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques, et en deuxième lieu de comprendre les concepts et principes de la sécurité informatique, et plus particulièrement la sécurité des réseaux informatiques.

Chapitre 2

Etat d’art sur la VoIP

1 Introduction

La voix sur IP est devenue importante pour les entreprises. L'enjeu est de réussir à faire converger le réseau de données IP et le réseau téléphonique actuel.

Dans ce chapitre, nous allons concentrer sur l'étude approfondie de la technologie VoIP et de ses divers aspects. Nous étudierons en détail l'architecture de la VoIP, ses éléments constitutifs et son principe de fonctionnement. Nous décrirons également les protocoles de signalisation et de transport de la VoIP, en expliquant leurs principes de fonctionnement et en identifiant leurs avantages et inconvénients principaux.

2 Définition

La VoIP est uen technologie qui permet de transmettre des signaux audio (voix) sous forme de paquets IP via Internet plutôt que par les réseaux téléphoniques traditionnels (RTC). La VoIP utilise des protocoles de communication numériques pour transformer les signaux vocaux en paquets de données, qui sont ensuite transmis via internet [20].

3 Avantage

- Coût : La VoIP est souvent beaucoup moins chère que les appels téléphoniques traditionnels, surtout pour les appels internationaux.
- Flexibilité : La VoIP peut être utilisée sur n'importe quel appareil connecté à Internet, ce qui permet une grande flexibilité et mobilité pour les utilisateurs.
- Fonctionnalités : La VoIP offre une variété de fonctionnalités, telles que la messagerie vocale, la vidéoconférence, le transfert d'appels, la mise en attente et bien d'autres.
- Qualité audio : La qualité audio de la VoIP s'est grandement améliorée au fil du temps et peut souvent être comparable à celle des appels téléphoniques traditionnels.
- Évolutivité : La VoIP est facilement évolutive, ce qui signifie qu'elle peut facilement s'adapter aux besoins changeants d'une entreprise ou d'un utilisateur.

4 Principe de fonctionnement

La première étape consiste à capter la voix à l'aide d'un micro, puis convertir le signal analogique en signal numérique à l'aide d'un convertisseur analogique/numérique. Une fois la numérisation terminée, le signal sera compressé par un DSP (Digital Signal Processor) pour diminuer son débit, et donc réduire la bande passante nécessaire pour sa transmission. Ensuite, un habillage d'en-têtes (RTP,

UDP, IP) est important pour former les paquets finaux qui seront transmis sur n'importe quel réseau IP.

Au niveau du récepteur, les paquets transmis seront réassemblés, le signal de données obtenu sera décomprimé puis converti en signal analogique à l'aide d'un convertisseur numérique/analogique pour restitution sonore à l'utilisateur [6]. La figure 2.1 illustre les différentes étapes citées.

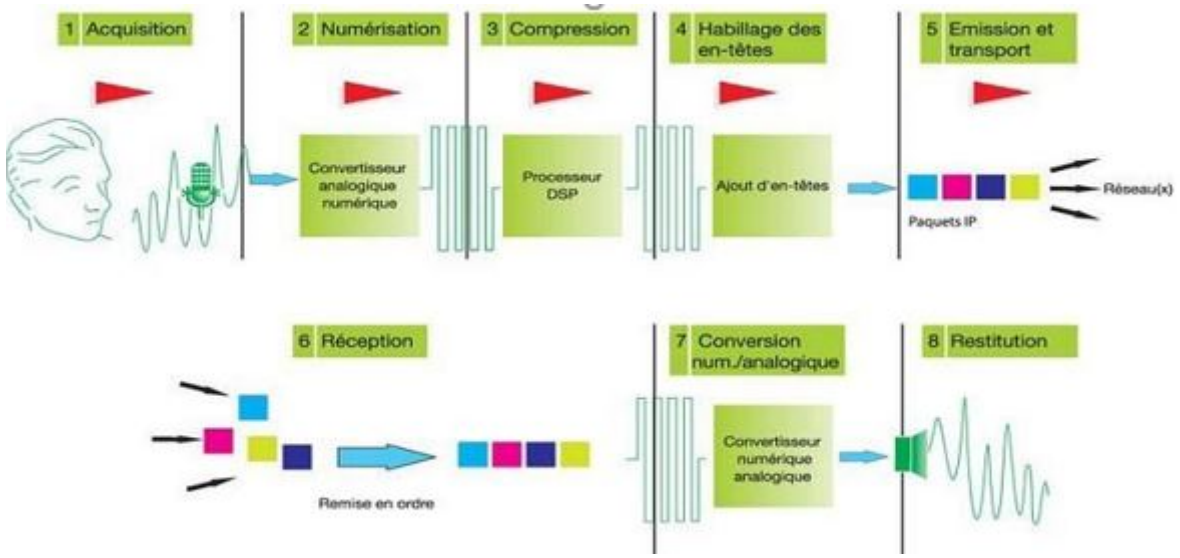


FIGURE 2.1 – Principe de fonctionnement de la VoIP [7]

5 Architecture et modes d'accès

5.1 Architecture

L'architecture d'un système de VoIP est composée des éléments suivants (illustrés dans la figure 2.2) :

- **Le terminal :** qui peut être un téléphone IP, un softphone ou un adaptateur analogique pour connecter un téléphone traditionnel à un réseau VoIP.
- **Le réseau IP lui même :** qui permet la transmission des données VoIP entre les différents terminaux et les serveurs de communication.
- **Le serveur de communication :** également appelé PBX IP, qui est chargé de gérer les appels et les fonctionnalités de téléphonie, telles que la gestion des lignes, la messagerie vocale et les conférences téléphoniques.
- **La passerelle VoIP :** qui permet de connecter un réseau VoIP à un réseau téléphonique traditionnel, afin de permettre les appels entre les deux réseaux.

Le système peut inclure des contrôleurs de commutation (Gatekeeper), des protocoles de signalisation et des protocoles de transport pour gérer la qualité de service, la sécurité et la gestion du trafic [20].

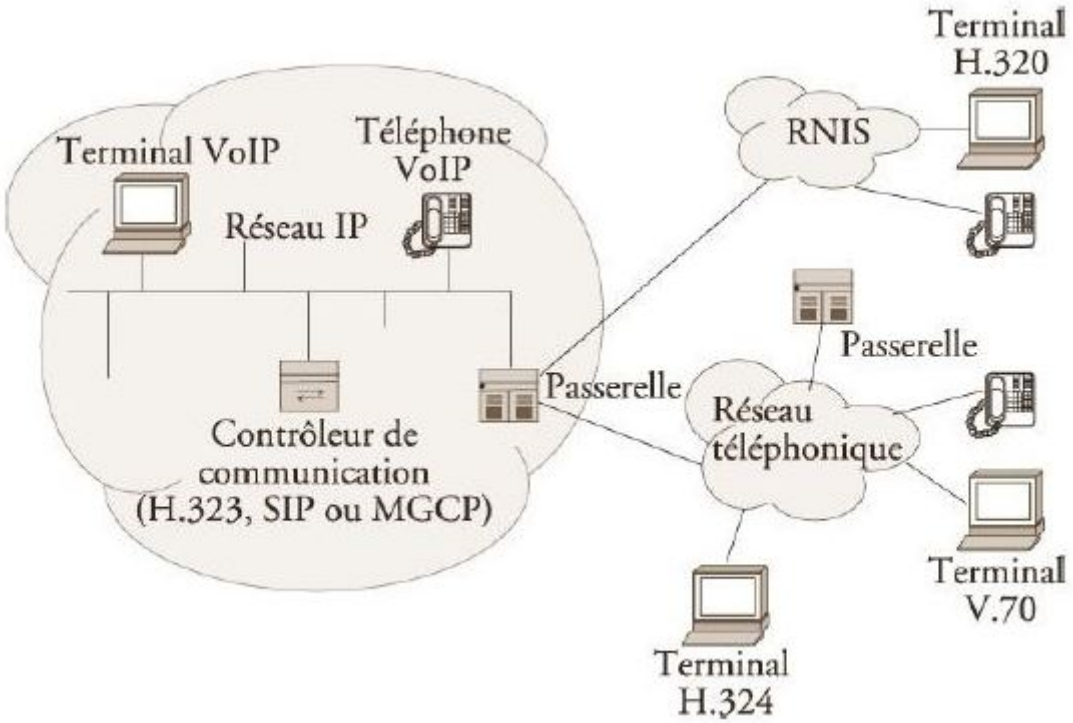


FIGURE 2.2 – Architecture d'un réseau VoIP

5.2 Modes d'accès

Selon le type de terminal utilisé, on peut distinguer trois modes d'accès possibles [21] :

5.2.1 Entre deux PC

C'est le cas le plus simple (figure 2.3). Les correspondants utilisent des PC possédants des micros, écouteurs et des logiciels de VoIP compatibles avec chaque PC. Il faut également connaître l'adresse IP de chacun des terminaux pour établir la communication.

FIGURE 2.3 – Mode d'accès PC à PC

5.2.2 Entre PC et téléphone

Ce cas nécessite une conversion des signaux entre le RTC et le réseau IP. En effet, ces deux terminaux utilisant des technologies différentes (la commutation de circuits et la commutation de paquets), l'échange des informations nécessite une passerelle. L'utilisateur possédant un ordinateur et désirant appeler l'autre sur son téléphone doit se connecter à un service spécial sur Internet, offert par un fournisseur de service (ISP (Internet Service Provider)) ou par son fournisseur d'accès à Internet (IAP (Internet Access Provider)) (figure 2.4).

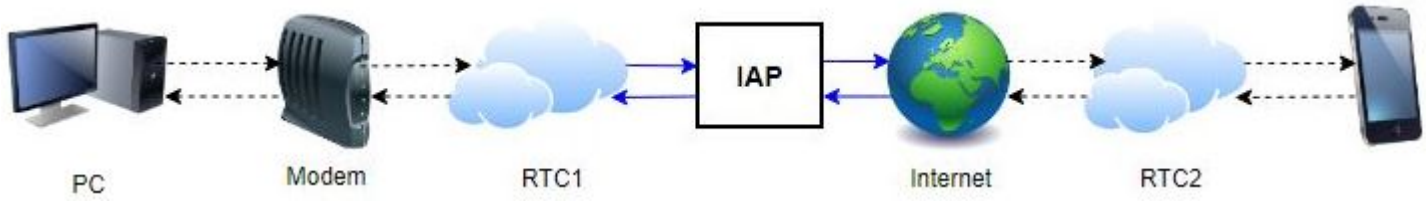


FIGURE 2.4 – Mode d'accès PC à téléphone

5.2.3 Entre deux téléphones

C'est le cas le plus complexe car il nécessite deux conversions de signaux. Un correspondant souhaitant appeler un numéro, doit passer par une passerelle qui lui communiquera le numéro du correspondant qu'il cherche à joindre (figure 2.5).

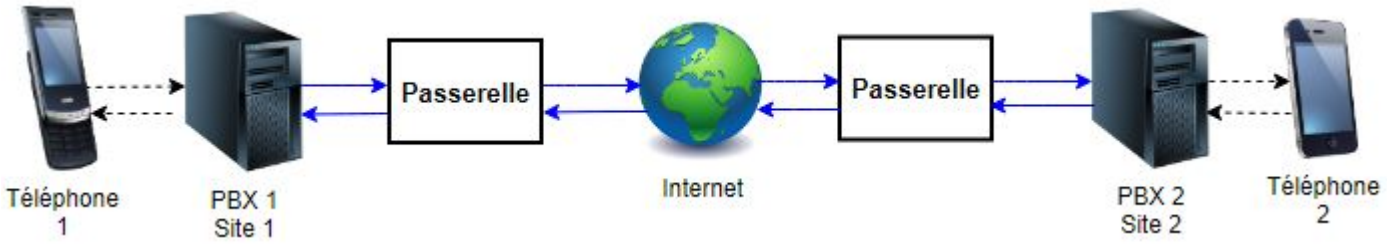


FIGURE 2.5 – Mode d'accès entre deux téléphones

6 Différence entre VoIP et ToIP

La ToIP (Telephony over Internet Protocol) et la VoIP sont deux technologies proches mais pourtant distinctes. Les deux utilisent le protocole internet IP, mais leur mode de fonctionnement diffère. La VoIP transforme la voix en fichiers numériques, qu'elle envoie sous forme de paquets sur un réseau de données (par exemple Internet) au travers de lignes IP. Elle regroupe l'ensemble des techniques permettant ce transit : d'un téléphone IP à un PC ou un téléphone normal, ou encore d'un ordinateur à un autre sur les réseaux internes et externes d'une entreprise.

La ToIP est quant à elle un système de téléphonie basé sur la VoIP, qui se limite au réseau IP local. Elle utilise un simple routeur créant la connexion entre le réseau LAN (société) et le réseau WAN (opérateur) : l'IPBX (Internet Protocol Private Branch eXchange).

La ToIP regroupe tous les échanges entre deux téléphones IP, ou encore entre deux ordinateurs utilisant le même logiciel.

La VoIP offre des applications et services multiples au-delà de la simple téléphonie : visioconférence sur IP, messageries vocales unifiées, etc. Cette technologie permet une convergence entre la voix, la vidéo et les données [7].

7 Différence entre PABX et IPBX

Le PABX (Private Automatic Branch Exchange) et l'IPBX sont deux types de systèmes téléphoniques privés utilisés par les entreprises pour gérer automatiquement les appels téléphoniques. La principale différence entre les deux est la technologie utilisée pour acheminer les appels.

Le PABX est un autocommutateur traditionnel qui utilise des lignes téléphoniques analogiques ou numériques pour acheminer les appels, il est installé sur un site et nécessite un câblage dédié pour connecter les téléphones aux lignes téléphoniques. Le PABX offre des fonctionnalités de base telles que la mise en attente des appels, la transfert d'appel et la gestion des files d'attente.

L'IPBX, en revanche, est un autocommutateur qui utilise le protocole IP pour acheminer les appels téléphoniques. L'IPBX peut être installé sur un site ou dans le cloud et permet aux entreprises de connecter des téléphones IP (téléphones qui se connectent directement à Internet) ou des téléphones analogiques via un adaptateur téléphonique IP. L'IPBX offre des fonctionnalités avancées supplémentaires par rapport au PABX telles que la messagerie vocale unifiée, la visioconférence et la gestion centralisée des téléphones. Il peut être géré à distance, ce qui en fait un choix populaire pour les entreprises qui cherchent à moderniser leur infrastructure téléphonique.

8 Protocoles de la VoIP

8.1 Protocoles de signalisation

8.1.1 SIP

Est un protocole de signalisation au niveau de la couche Application du modèle OSI, normalisé et standardisé par l'IETF (Internet Engineering Task Force), conçu pour établir, modifier et terminer des sessions de communication multimédia [7].

8.1.2 H.323

H.323 est un protocole de communication en temps réel développé par l'Union internationale des télécommunications (UIT) pour le traitement et la signalisation des données multimédias avec de fortes contraintes temporelles, comme la voix et la vidéo sur des réseaux IP.

Le protocole H.323 utilise un ensemble de protocoles pour permettre la communication entre les terminaux, les passerelles et les réseaux. Les protocoles comprennent le protocole H.225 pour la signalisation de l'appel, la synchronisation, la mise en paquets des données et l'enregistrement auprès d'un Gatekeeper, le protocole H.245 Pour la négociation des codecs ainsi l'ouverture et la fermeture des canaux, le protocole RAS (Registration/Admission/Status) pour la communication avec le Gatekeeper, il permet le contrôle d'admission et la gestion de la bande passante, et enfin les protocoles de transport en temps réel RTP et RTCP pour le transport des données multimédia [8].

8.1.3 IAX (Inter-Asterisk eXchange)

Est un protocole de signalisation utilisé dans les systèmes de VoIP basés sur le logiciel libre Asterisk. Il a été conçu pour faire transiter voix et vidéo sur des débits plus faibles en utilisant un seul port de communication UDP (User Datagram Protocol) pour les données et la signalisation [7].

8.1.4 Skiny/SCCP

Est un protocole propriétaire de Cisco visant à simplifier l'utilisation du protocole H.323, qui est considéré comme étant relativement complexe. Ce protocole est léger et ne consomme que peu de bande passante, ce qui le rend idéal pour les communications entre les téléphones et le call manager, ainsi que pour la gestion des conférences [9].

8.1.5 MGCP (Media Gateway Control Protocol)

Est utilisé pour permettre la transmission de messages de signalisation entre un contrôleur de passerelles de médias et des passerelles réparties dans un réseau IP. Ce protocole utilise des signaux et des événements pour établir et libérer les connexions. Toutefois, la normalisation de MGCP a été stoppée pour faire place au protocole MEGACO/H.248 qui est développé par l'IETF. Il est très

difficile de passer vers ce nouveau standard MEGACO/H.248 car ce dernier n'est pas basé sur MGCP [9].

8.1.6 BICC (Bearer Independent Call Control)

Est un protocole de signalisation utilisé pour prendre en charge les services numériques intégrés à bande étroite (ISDN) sur un réseau à large bande. Il s'appuie sur le protocole N-ISUP (Network ISDN User Part) pour acheminer les informations de signalisation entre les commutateurs. BICC est conçu pour permettre l'interfonctionnement avec les technologies de transport existantes et offrir une grande flexibilité pour la fourniture de services ISDN. Il est spécifié dans la recommandation Q.1901 de l'UIT-T [22].

8.2 Protocoles de transport

8.2.1 UDP

Est un protocole de communication de la couche de transport du modèle OSI. C'est un protocole sans connexion et non fiable, ce qui signifie qu'il n'assure pas la livraison des données ni l'ordre dans lequel elles sont envoyées.

UDP est souvent utilisé pour des applications où la vitesse est plus importante que la fiabilité, comme la diffusion en temps réel de données audio et vidéo, la diffusion de jeux en ligne ou encore la surveillance de réseaux. UDP est également utilisé pour des applications où la perte de données est acceptable [1].

8.2.2 TCP

Est un protocole de communication de la couche transport dans le modèle OSI. Il est largement utilisé pour les applications qui nécessitent une transmission fiable des données, comme le transfert de fichiers et l'accès à des pages Web sécurisées utilisant HTTPS.

Le protocole TCP établit une connexion à état entre deux appareils pour assurer la fiabilité de la transmission des données. Il gère la segmentation des données en paquets, la numérotation des paquets, le contrôle de la congestion et le contrôle de flux. TCP garantit également que les paquets arrivent dans l'ordre correct et détecte les erreurs de transmission [1].

- ➢ Dans la VoIP, la rapidité est plus prioritaire que la fiabilité (ça ne sert à rien de retransmettre les paquets de voix perdus, et les conversations doivent se passer en temps réel), donc le protocole TCP n'est pas utile.
- ➢ Udp est mieux adapté sauf qu'il manque de fiabilité, pour cela, d'autre protocoles de transport sont utilisés dans la VoIP tel que RTP et RTCP.

8.2.3 RTP

Est un protocole de communication de la couche application utilisé pour gérer les flux multimédias ainsi que la transmission de données en temps réel, telles que la voix et la vidéo, sur des réseaux IP. Il a été proposé pour compléter UDP en lui ajoutant des fonctionnalités d'ordonnancement lui permettant la reconstitution de l'ordre de flux [11].

8.2.4 RTCP

Est un protocole de communication de la couche application utilisé en conjonction avec RTP pour gérer les rapports de qualité de service (QoS) et le contrôle de la session sur les réseaux IP.

RTCP fournit des informations de contrôle pour les sessions RTP en envoyant des paquets de contrôle périodiques à tous les participants de la session RTP. Ces paquets incluent des informations telles que la qualité du service, les statistiques de performance et les informations de synchronisation. RTCP permet également de détecter les pertes de paquets et les retards excessifs, ce qui permet aux applications de prendre des mesures pour améliorer la qualité de la transmission [11].

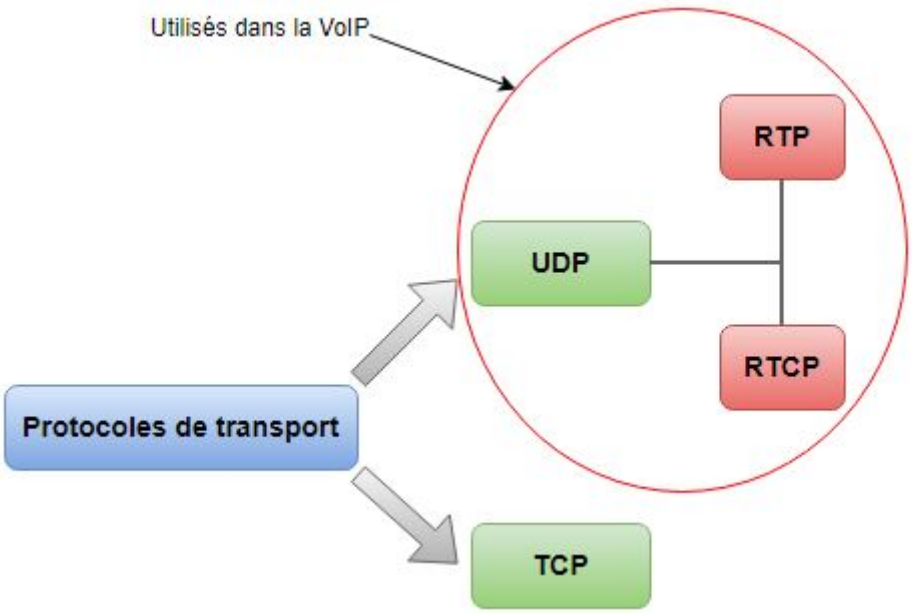


FIGURE 2.6 – Protocoles de transport

9 Protocoles RTP

Le rôle principal du protocole RTP est de permettre la transmission de données audio et vidéo en temps réel sur les réseaux IP. Il met en oeuvre des numéros de séquence pour assurer la livraison des données multimédias dans l'ordre correct et pour détecter les pertes de paquets. En plus de la livraison de données, RTP permet également la synchronisation des flux multimédias entre les différentes parties prenantes d'une session de communication [11].

9.1 Fonctions

Les principales taches du protocole RTP sont :

1. Encapsulation des données multimédias : les données audio ou vidéo sont encapsulées dans des paquets RTP avec un en-tête RTP contenant des informations telles que le numéro de séquence, l'horodatage, le type de codec utilisé, etc.
2. Transmission des paquets RTP : les paquets RTP sont transmis sur le réseau IP à l'aide du protocole UDP, qui offre une transmission non fiable mais rapide des données.
3. Réception des paquets RTP : le récepteur reçoit les paquets RTP et les assemble pour former un flux multimédia continu. Les numéros de séquence des paquets sont utilisés pour s'assurer que les paquets sont reçus dans l'ordre correct et pour détecter les pertes de paquets.
4. Décompression des données multimédias : les données multimédias encapsulées dans les paquets RTP sont décompressées à l'aide d'un codec approprié pour être jouées ou affichées à l'utilisateur.
5. Synchronisation des flux multimédias : RTP utilise des horodatages pour synchroniser les différents flux multimédias d'une session de communication en temps réel, tels que la vidéo et l'audio.

9.2 En-tête RTP

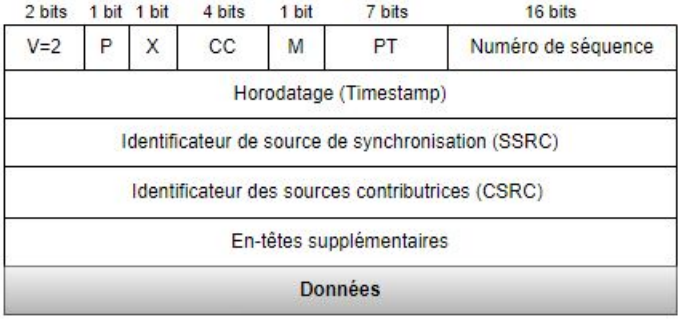


TABLE 2.1 – En-tête RTP

9.2.1 Différents champs de l'en-tête RTP

V : pour version (sur 2 bits), indique la version du protocole RTP utilisée. Actuellement, c'est la 2 qui est exploitée.

P : pour padding (sur 1 bit), si P=1, le paquet contient des octets additionnels de bourrage (padding) pour compléter les champs optionnels en multiple de 32.

X : pour extension (sur 1 bit), si X=1 l'en-tête est suivie d'un paquet d'extension (qui complète un autre paquet).

CC : pour CSRC Count (sur 4 bits), nombre de sources ayant contribué à la génération du paquet (Conférences).

M : pour Maker (sur 1 bit), utilisé par les applications pour marquer certains événements dans les flux RTP.

PT : pour Payload Type (sur 7 bits), décrit le format de données (pour qu'il puisse être compris par le destinataire).

Numéro de séquence : Numéro de séquence ou compteur incrémenté d'une unité entre chaque paquet (sur 16 bits).

Timestamp : estampille temporelle permettant la synchronisation des flux (sur 32 bits).

SSRC : pour Synchronization Source (sur 32 bits), identifiant unique de la source qui a généré le paquet RTP.

CSRC : pour contributing source (optionnel, sur n fois 32 bits), identifie les contributeurs à la génération du paquet.

9.3 Avantages et inconvénients

Le protocole RTP assure la synchronisation temporelle des différents flux multimédia tels que l'audio, la vidéo et autres. Il est également capable de détecter la perte de paquets et d'identifier le contenu des paquets pour une transmission sécurisée.

Cependant, le protocole RTP ne dispose pas de fonctionnalités permettant de réserver des ressources ni d'assurer une fiabilité dans le réseau. De ce fait, il ne peut pas garantir le délai de livraison des paquets [8].

10 Protocole SIP

10.1 Définition

Comme on l'a déjà défini, le protocole SIP est un protocole de signalisation utilisé pour établir, modifier et terminer des sessions multimédia. Il se charge de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol).

SIP ne transporte pas directement les données de la session, telles que la voix ou la vidéo. Les données sont échangées par l'intermédiaire d'autres protocoles indépendants de SIP. Cela permet d'utiliser différents types de données et de protocoles pour l'échange. De plus, SIP est de plus en plus utilisé pour remplacer le protocole H323, en raison de ses nombreux avantages et fonctionnalités [7].

10.2 Architecture

Le protocole SIP repose entièrement sur une conception logicielle. Elle est soutenue par divers serveurs qui communiquent entre eux et partagent la charge du réseau. Elle est organisée autour de cinq composants [7] :

10.2.1 Agent utilisateur

L'utilisateur d'agent est composé de deux parties : Le client (UAC : User Agent Client) et le Server (UAS : User Agent Server). Le client envoie les requêtes SIP lorsqu'il initialise un appel, l'UAS est une application qui contacte l'utilisateur si un appel lui est destiné.

10.2.2 Serveur d'enregistrement

Il gère les requêtes REGISTER envoyées par le terminal afin de communiquer la position actuelle de l'utilisateur (user agent) tout en gérant sa mobilité. Ces requêtes contiennent donc une adresse IP, associée à une URI SIP (sip :utilisateur@domaine.com), qui seront stockées dans une base de données (figure 2.7).

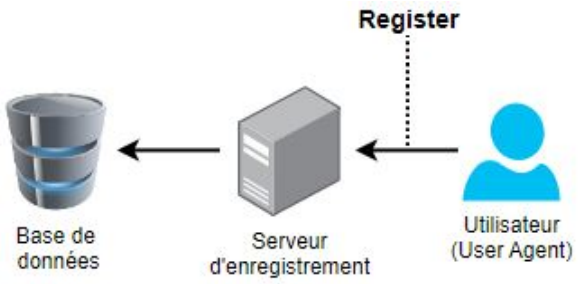


FIGURE 2.7 – Enregistrement d'un utilisateur

10.2.3 Serveur de localisation

Le serveur de localisation complète le serveur d'enregistrement en permettant de déterminer la localisation de l'abonné. Ce serveur dispose de la base de données de tous les abonnés qu'il gère.

10.2.4 Serveur de redirection

Le serveur de redirection (Redirect Server) agit comme un intermédiaire entre le terminal client et le serveur de localisation. Il est sollicité par le terminal client pour contacter le serveur de localisation afin de déterminer la position courante d'un utilisateur.

10.2.5 Serveur Proxy

Parfois appelé serveur mandataire, il agit comme un relais pour les demandes SIP entre les clients, en recevant une demande d'un client et en la transmettant à un autre serveur SIP ou à un client final (figure 2.8). Le proxy SIP peut également exécuter des fonctions de routage et de filtrage des demandes SIP.

Il existe deux types de serveurs proxy :

- **Proxy statefull :** qui conserve l'état des connexions au fil des sessions.
- **Proxy stateless :** qui transmet les messages indépendamment les uns des autres sans conserver l'état des connexions.

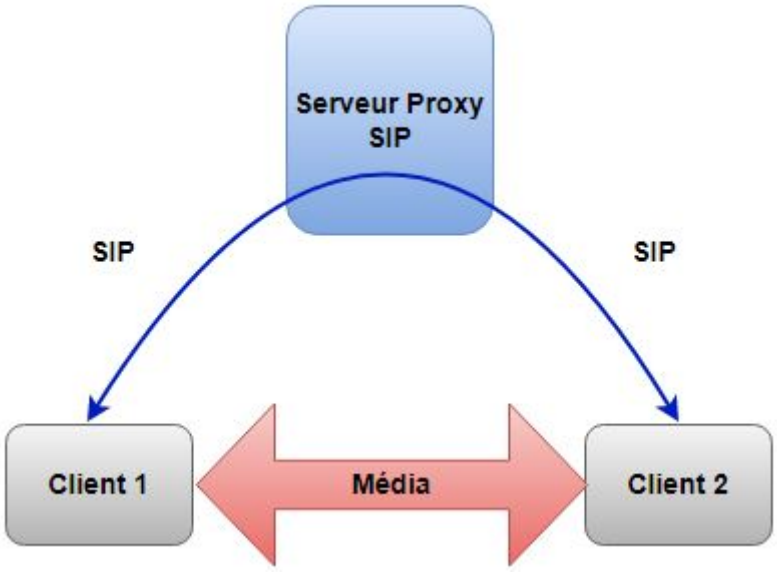


FIGURE 2.8 – Serveur Proxy SIP

10.3 Adressage SIP

C'est l'une des étapes essentielles qui a pour but de localiser les utilisateurs au sein d'un réseau. Les utilisateurs doivent pouvoir être identifiés de manière unique afin d'être localisés. Voici la forme que prend une adresse SIP [7] :

sip : identifiant[:mot-de-passe]@serveur[?paramètres].

- **SIP :** spécifie le protocole utilisé pour la communication.
- **Identifiant :** c'est le nom ou le numéro de l'utilisateur qui est unique.
- **Mot de passe :** il est facultatif et est utilisé pour l'authentification au niveau du serveur.
- **Serveur :** spécifie le serveur chargé du compte SIP de l'utilisateur. Le serveur est indiqué par son adresse IP ou par un nom qui sera résolu par DNS (Domain Name System).
- **Paramètres :** est facultatif, il permet de modifier le comportement par défaut tel que le protocole de transport ou bien de spécifier des informations complémentaires tel que l'objet d'un appel.

10.4 Méthodes utilisées

Une méthode SIP est une commande utilisée pour établir, modifier ou terminer une session de communication multimédia sur un réseau IP.

Voici quelques méthodes les plus utilisées dans SIP [7] :

- **INVITE :** utilisée pour initier une session de communication.
- **ACK :** utilisée pour confirmer la réception d'un message INVITE.
- **OPTIONS :** permet d'interroger un serveur SIP sur différentes informations.
- **BYE :** utilisée pour terminer une session de communication.
- **CANCEL :** utilisée pour annuler une demande d'invitation qui a été envoyée mais qui n'a pas encore été traitée.
- **REGISTER :** permet d'enregistrer un utilisateur au niveau d'un serveur d'enregistrement.

10.5 Codes de réponses

Un code de réponse SIP est une indication numérique envoyée par un serveur SIP à un client SIP pour indiquer le résultat d'une requête envoyée par le client. Les codes de réponse SIP sont généralement regroupés en 6 catégories, en fonction de leur premier chiffre [7] :

- **1xx - Message d'information :** Indique que le serveur a reçu la requête du client et continue à traiter la demande.
  Ex : **100 TRYING** Tentative d'appel en cours.
- **2xx - Message de succès :** La requête a été reçue, comprise et acceptée par le serveur. Ex : **200 ok** La requête a été exécutée avec succès.
- **3xx - Message de redirection :** Indique que la requête du client doit être dirigée vers un autre serveur ou une autre adresse.
  Ex : **301 Moved Permanently** la requête du client doit être dirigée vers une nouvelle adresse permanente.
- **4xx - Message d'erreur client :** Indique que la demande du client ne peut pas être traitée en raison d'une erreur de la part du client lui-même.
  Ex : **400 BAD REQUEST** Le format de la requête est incorrect et ne peut être compris.
- **5xx - Message d'erreur serveur :** Indique que la demande du client ne peut pas être traitée en raison d'une erreur de la part du serveur.
  Ex : **500 Internal Server Error** Une erreur inattendue s'est produite sur le serveur.
- **6xx - Message d'erreur globale :** Aucun serveur ne peut traiter cette requête, car ils sont occupés, inaccessibles ou refusent l'appel.
  Ex : **600 BUSY EVERYWHERE** Le destinataire a été joint, mais il est occupé sur tous les postes et ne peut prendre la communication.

10.6 Communication SIP

La communication SIP se fait en 5 étapes (figure 2.9) [7] :

Etape 1 : Un message d'invitation (requête INVITE) est envoyé du terminal A vers son serveur SIP. À la réception de ce message, le serveur A utilise la partie domaine de l'adresse SIP de B pour déterminer le serveur en charge de la gestion du compte B. À cette fin, un serveur DNS peut être sollicité. En parallèle, le serveur proxy informe A qu'il prend en charge la requête et tente de la mettre en relation. La réponse temporaire 100 TRYING indique que le message a été reçu et qu'il est en cours de traitement.

Etape 2 : Le serveur A transmet l'invitation au serveur B après l'avoir localisé. C'est le message d'invitation original qui est intégralement relayé du serveur A vers le serveur B. Ce dernier informe le serveur A (par un message de réponse temporaire 100 TRYING) de la réception de la requête et de la tentative d'initialisation. Parallèlement, il recherche la localisation du terminal B en utilisant le service de localisation. Une fois la position du terminal dans le réseau trouvé, il lui transmet l'invitation de A.

Etape 3 : Le téléphone B (éventuellement un softphone) reçoit l'invitation et la fait connaître à l'utilisateur B, le plus souvent par une sonnerie. En parallèle, il indique à son serveur (par un message 180 RINGING) que l'appel est en train d'être notifié à B et que la communication est en attente de son acceptation. Ce message informatif est relayé jusqu'à l'émetteur A, qui reçoit généralement un retour audio ou visuel (une tonalité de sonnerie particulière le plus souvent).

Etape 4 : B répond au téléphone. On suppose le cas où B a choisi de répondre à l'appel. À l'instant où il décroche, un message 200 OK est retourné pour l'informer que l'appel est accepté.
Ce message est relayé par les différents serveurs. À ce stade, la communication n'a pas encore débuté, et aucun son n'est transmis.

Etape 5 : Le terminal A confirme les paramètres d'appel. En tenant compte des capacités prises en charge par les correspondants, le terminal A envoie un message d'acquittement ACK qui spécifie les paramètres définitifs à utiliser lors de cette session

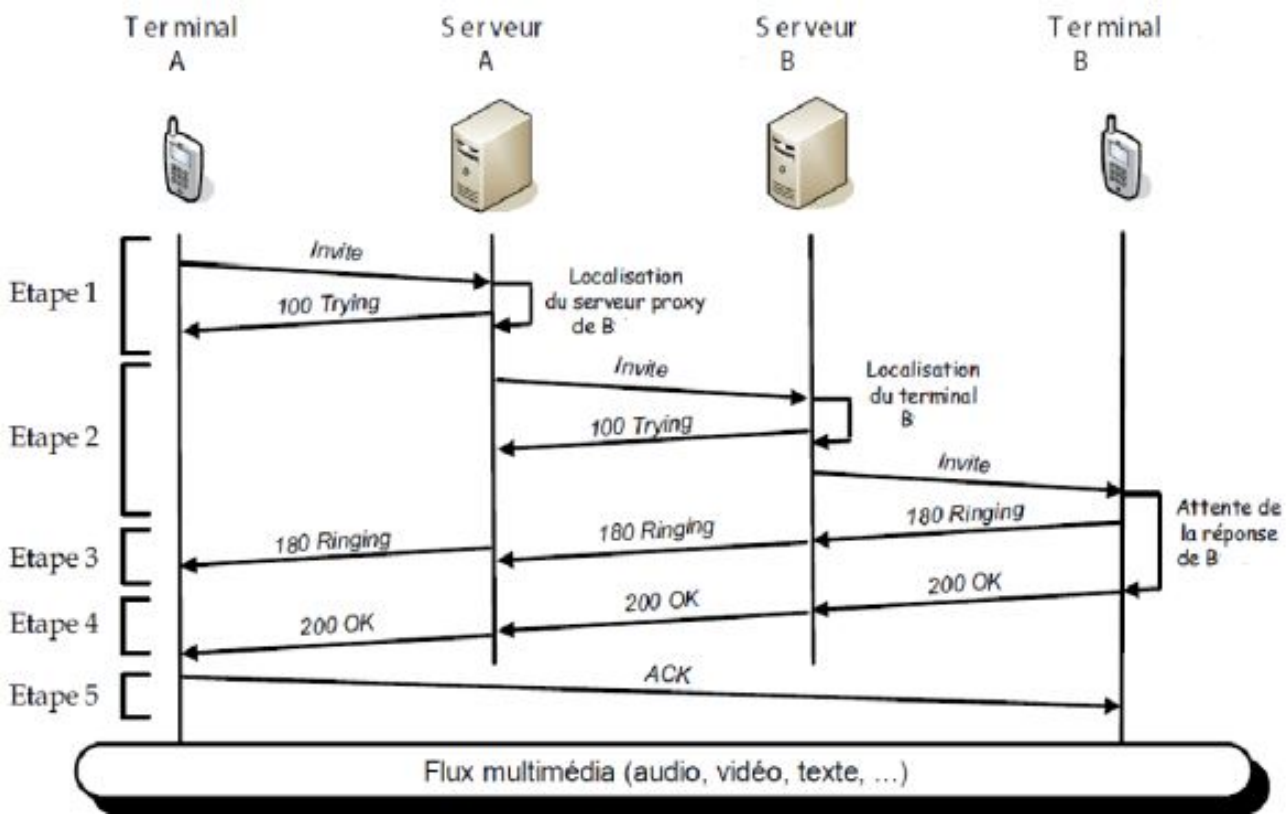


FIGURE 2.9 – Communication SIP

10.7 Avantages

- **Open source :** Les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.
- **Flexible :** SIP peut être utilisé pour tout type de sessions multimédia (voix, vidéo, réalité virtuelle, etc.)
- **Simple :** SIP est simple et très similaire à http. En effet, le client envoie des requêtes au serveur, qui lui renvoie une réponse.
- **Standard :** l'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP [7].

10.8 Inconvénients

- **Basé sur l'adresse IP :** SIP rencontre des difficultés avec les systèmes de translation d'adresse (NAT) et les pare-feu car il nécessite la connaissance de l'adresse IP des communicants.
- **Mauvaise implémentation :** une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les USER Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau.

11 Protocole IAX/IAX2

11.1 Définition

IAX/IAX2 (version améliorée d'IAX), est un protocole de signalisation qui est une alternative au protocole SIP. Il s'agit du protocole sur lequel s'appuie Asterisk bien que celui-ci soit en mesure de supporter les autres principaux protocoles VoIP tel que SIP. Il permet la communication entre client et serveur Asterisk ainsi qu'entre deux serveurs Asterisk. Il a été conçu pour le contrôle et la transmission de flux multimédia avec un débit plus faible.

Contrairement à SIP qui utilise 2 paires de flux (l'une pour la signalisation, l'autre pour la voix), IAX utilise une seule paire de flux pour communiquer entre les extrémités de la ligne (téléphone ou central téléphonique). La signalisation comme les données (la conversation vocale) sont transmises sur le même canal, par opposition à SIP qui utilise un second canal pour les flux de données (RTP) transportant la voix.

De plus, IAX2 permet à plusieurs appels d'être rassemblés dans un seul ensemble de paquets IP. Ce mécanisme est appelé « trunking » (figure 2.10) [7].

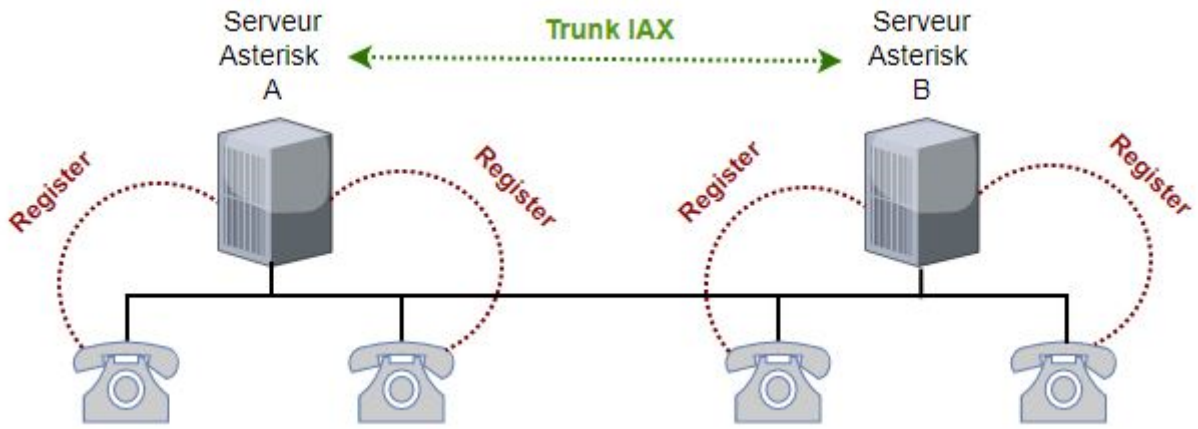


FIGURE 2.10 – Echange de données entre plusieurs serveurs Asterisk

11.2 Caractéristiques

- Minimise la bande passante par appel.
- Réduit la consommation de bande passante pour un ensemble d'appels (par l'utilisation du « trunking ») [7].

11.3 Requêtes et réponses IAX

Requêtes :

— **NEW :** est une requête envoyée par un équipement lorsqu'il souhaite initier une nouvelle session IAX avec un autre équipement ou un serveur Asterisk.

— **REGREQ :** est une requête envoyée pour demander l'enregistrement d'un équipement auprès d'un serveur Asterisk.

— **AYTHREQ :** est une requête envoyée pour demander une autorisation d'accès à un serveur Asterisk.

Réponses :

— **ACK :** est une réponse pour confirmer la réception d'un message IAX précédent.

— **AUTHREP :** est envoyé en réponse à un message IAX AUTHREQ pour confirmer ou refuser l'autorisation d'accès.

— **REGACK :** envoyé en réponse à une requête REGREQ pour confirmer l'enregistrement d'un équipement auprès d'un serveur Asterisk.

— **ACCEPT :** envoyée pour indiquer qu'une requête NEW est acceptée.

— **REJECT :** envoyée pour indiquer qu'une requête NEW est refusée [11].

11.4 Etablissement d'une connexion IAX

L'établissement d'une connexion IAX implique plusieurs étapes. Voici les principales :

1. La première étape consiste à établir une connexion réseau entre le client et le serveur IAX. Cette connexion peut être établie via un réseau local (LAN) ou via Internet.
2. Ensuite, le client envoie une requête "AUTHREQ" au serveur pour s'authentifier. Cette requête contient des informations d'identification telles que le nom d'utilisateur et le mot de passe. Le serveur vérifie ces informations et renvoie une réponse "AUTHREP" si l'authentification est réussie.
3. Le client envoie ensuite une requête "REGREQ" au serveur pour s'enregistrer. Cette requête contient des informations sur l'identité du client telles que l'adresse IP, le nom d'utilisateur et le mot de passe. Le serveur vérifie ces informations et enregistre le client s'il est valide.
4. Une fois que le client est enregistré, il peut envoyer une requête "NEW" pour établir une nouvelle session. Cette requête contient des informations sur l'appel que le client souhaite effectuer, telles que l'adresse IP de destination et le numéro de téléphone.
5. Le serveur vérifie si l'adresse IP de destination est disponible et répond avec une réponse "ACCEPT" si elle l'est. Le client peut alors envoyer une requête "ACK" pour confirmer l'établissement de la session.
6. Enfin, les données audio et vidéo peuvent être échangées entre le client et le serveur via la session établie.

12 Qualité de service (QoS)

12.1 Définition

La qualité de service (QoS) fait référence à l'ensemble des exigences imposées par un utilisateur, qu'il s'agisse d'un être humain ou d'un composant logiciel, à la performance d'une application pendant son exécution. Afin de fournir de manière satisfaisante les services demandés, tels que les aspects fonctionnels, une application répartie doit également prendre en compte des aspects complémentaires, tels que le type de communication, la gestion d'état partagé, la sécurité, etc [23].

La qualité de service est généralement mesurée en termes de disponibilité, de fiabilité, de latence, de gigue et de perte de paquets. Elle est importante pour garantir que les utilisateurs peuvent avoir des conversations téléphoniques claires et sans interruption, sans être interrompus par des problèmes techniques tels que des retards, des pertes de paquets ou des distorsions audio. Pour atteindre une QoS élevée, il est important d'avoir une bande passante suffisante, une latence et une gigue faibles, et des mécanismes de priorisation des paquets pour assurer une transmission de voix fluide et cohérente.

12.2 Temps de latence

La latence dans la VoIP désigne le délai nécessaire pour que les paquets de données audio atteignent leur destination. Elle peut être affectée par divers facteurs tels que la qualité de la connexion Internet, la distance entre les points de terminaison, la congestion du réseau et la qualité des équipements utilisés pour la VoIP.

Une latence élevée peut entraîner des retards dans la transmission audio, ce qui peut perturber la communication entre les utilisateurs. Cela peut se traduire par des interruptions dans la conversation, des chevauchements de voix, des coupures ou même des problèmes de compréhension de la voix. Afin d'assurer une qualité de service optimale en VoIP, il est important de maintenir une latence faible, généralement inférieure à 150 ms, afin de permettre une communication fluide et claire [23].

12.3 La gigue

La gigue en VoIP se réfère à la variation du temps d'acheminement des paquets de données audio. Elle est due au mode de mise en paquets par les codeurs, à l'encapsulation des paquets IP dans des protocoles support tels que le Frame Relay ou l'ATM, et à la variation de routes dans le réseau. Cela peut provoquer des perturbations de la conversation et des pertes de qualité audio.

Pour compenser la gigue, on utilise des mémoires tampons (buffer de gigue). L'idée est de stocker les paquets audio dans une mémoire tampon pendant une courte période de temps avant de les lire. Cela permet de lisser les variations de la latence et d'assurer que les paquets audio sont lus à un intervalle régulier [23].

12.4 L'Echo

L'écho dans la VoIP est le phénomène où l'on entend sa propre voix répétée avec un léger délai, généralement moins d'une seconde, après avoir parlé dans un téléphone VoIP. Cela peut être causé par la réflexion du signal vocal à partir de l'extrémité distante du réseau VoIP ou par la réflexion de la voix de l'utilisateur dans l'environnement dans lequel il se trouve. L'écho peut être très gênant pour les utilisateurs de VoIP, car il peut rendre la conversation difficile à comprendre et perturber la communication. Pour réduire ou éliminer l'écho dans la VoIP, des techniques telles que l'annulation d'écho acoustique (AEC) sont utilisées [23].

12.5 La perte de paquets

La perte de paquets en VoIP se produit lorsque les paquets de données audio ou vidéo envoyés d'un point à un autre sont perdus en cours de route. Cela peut être dû à la congestion du réseau, les interférences, les erreurs de transmission, les problèmes de connectivité ou la mauvaise qualité de service.La perte de paquets peut provoquer une mauvaise qualité audio ou vidéo, des interruptions ou

des coupures dans la communication, des retards, des échos ou des perturbations dans le son. Pour minimiser la perte de paquets en VoIP, il est important d'avoir une connexion Internet de qualité, une bande passante suffisante et une infrastructure réseau appropriée [23].

13 Conclusion

Durant ce chapitre, on a présenté la technologie de la VoIP, ses avantages, ses protocoles, son principe de fonctionnement, et son architecture. On a pu alors déduire que la VoIP est la solution la plus rentable pour effectuer des conversations : Cette technologie permet l'émergence de services performants et beaucoup moins coûteux, tant pour les entreprises que pour les particuliers.

Dans le chapitre qui suit, nous allons aborder les aspects liés aux vulnérabilités de la VoIP, ainsi que les solutions de sécurité.

Chapitre 3

Les attaques et la sécurité de la VoIP

1 Introduction

Le passage de la téléphonie classique à la téléphonie IP a présenté de nombreux avantages pour les entreprises, notamment l'accès à de nouveaux services tels que la vidéoconférence et la transmission de données. Cependant, l'intégration de ces services dans une plateforme unique exige un niveau de sécurité accru.

Dans ce chapitre, nous allons décrire les différentes attaques et vulnérabilités qui menacent la VoIP ainsi que les meilleures solutions de sécurisation des communications VoIP.

2 Attaques contre la VoIP

2.1 Spam

Consiste à envoyer un grand nombre de messages non sollicités, souvent des appels ou des messages vocaux, à un utilisateur ou à un groupe d'utilisateurs dans le but de surcharger le réseau VoIP avec un trafic inutile.

On peut distinguer trois formes principales de Spams [9] :

- **Call Spam :** Ce type de spam est défini comme une masse de tentatives d'initiation de session souvent effectuées par un utilisateur client SIP qui lance simultanément un grand nombre d'appels. Ces tentatives se présentent sous forme de requêtes INVITE.
- **IM (Instant Message) Spam :** Ce type de spam est similaire au spam électronique. Il se caractérise par l'envoi en masse des messages instantanés non sollicitées sous forme de requêtes SIP, qui peuvent être des requêtes INVITE avec des en-têtes très volumineux ou avec un corps en format texte ou HTML (HyperText Markup Language). L'IM spam est particulièrement envahissant car les messages instantanés s'affichent automatiquement sous forme de fenêtres pop-up à l'utilisateur, contrairement aux e-mails.
- **Présence Spam :** Ce type de spam est similaire à l'IM spam. Il se caractérise par l'envoie d'une masse de requêtes de présence (requêtes SUBSCRIBE) non sollicitées dans le but de figurer sur la liste blanche d'un utilisateur et ainsi lui envoyer des messages instantanés ou initier d'autres formes de communication. Contrairement à l'IM spam, le spam de présence ne transmet pas réellement de contenu dans les messages.

2.2 Suivie d'appels

Le suivi d'appels, également appelé Call tracking, est une attaque qui cible les terminaux (soft/hard phone) au niveau du réseau LAN/VPN. Son objectif est d'identifier les communications en cours et de déterminer leur durée et les parties impliquées. L'attaquant doit intercepter les messages INVITE

et BYE en écoutant le réseau pour obtenir les informations concernant les appels en cours (qui communique, à quelle heure, pendant combien de temps) [9].

2.3 Voice Phishing

Est une technique d'attaque qui vise à tromper les utilisateurs de la VoIP en les incitant à divulguer des informations personnelles ou confidentielles par téléphone (figure 3.1). Les attaquants se font souvent passer pour une entité de confiance, comme une banque, une entreprise ou une organisation gouvernementale, afin de convaincre les victimes de leur fournir des informations sensibles, telles que des numéros de carte de crédit, des mots de passe ou des informations d'identification personnelle [24].

Les techniques courantes utilisées pour réaliser le Voice Phishing incluent l'utilisation de messages vocaux automatisés (robocalls), la création de fausses identités, l'enregistrement de messages vocaux préenregistrés, et l'imitation de numéros de téléphone légitimes pour tromper les destinataires. Les attaques de Voice Phishing peuvent également être ciblées, dans lesquelles l'attaquant recueille des informations sur la victime pour personnaliser l'attaque et augmenter les chances de réussite.

FIGURE 3.1 – Voice Phishing attack

2.4 Sniffing

Est une technique d'espionnage qui permet à un attaquant de capturer et d'analyser les données vocales échangées lors d'une communication VoIP (figure 3.2). Cette technique consiste à intercepter les paquets de données non cryptés circulant dans le réseau pour extraire des informations telles que les numéros de téléphone, les noms d'utilisateur, les mots de passe et les conversations vocales [9].

Le Sniffing en VoIP peut être réalisé à travers plusieurs méthodes, par exemple en utilisant des outils de capture de paquets tels que Wireshark ou tcpdump pour intercepter le trafic réseau, ou en utilisant des logiciels malveillants pour infiltrer les systèmes VoIP et collecter les données.

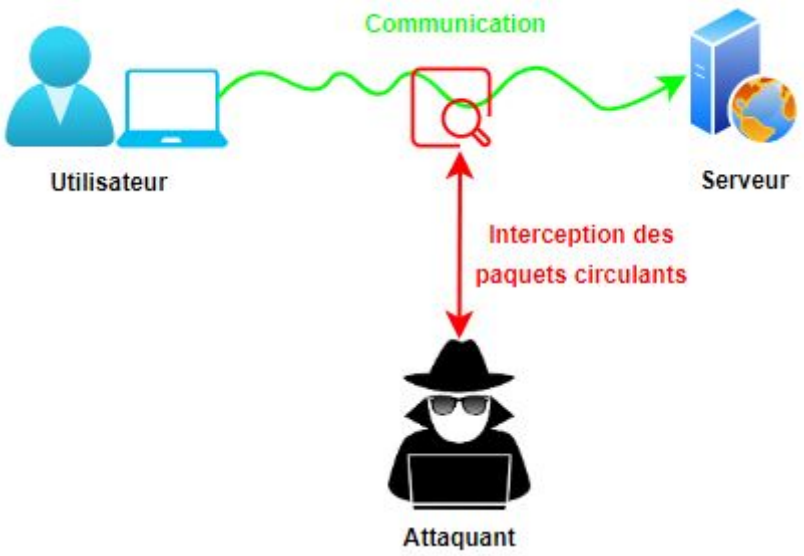


FIGURE 3.2 – Sniffing attack

2.5 Déni de service (DoS)

Les attaques de déni de service visent à rendre un service VoIP indisponible en inondant le réseau ou les serveurs VoIP avec un trafic illégitime. Les attaquants peuvent utiliser des techniques telles que l'envoi de paquets de signalisation SIP malveillants ou l'inondation de paquets RTP pour surcharger le réseau et les serveurs VoIP.

Dans le cas du protocole SIP, une attaque DoS (SIP flooding) peut être directement dirigée contre les utilisateurs finaux ou les dispositifs tels que téléphones IP, routeurs et proxy SIP, ou contre les serveurs concernés par le processus, en utilisant le mécanisme du protocole SIP ou d'autres techniques traditionnelles de DoS. Il existe différentes formes d'attaques DoS, on peut citer [9] :

- **DoS de type CANCEL :** C'est un type de déni de service lancé contre l'utilisateur. L'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique. Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant envoie immédiatement une requête CANCEL. Cette requête produit une erreur sur le dispositif de l'appelé et termine l'appel. Ce type d'attaque est employé pour interrompre la communication.

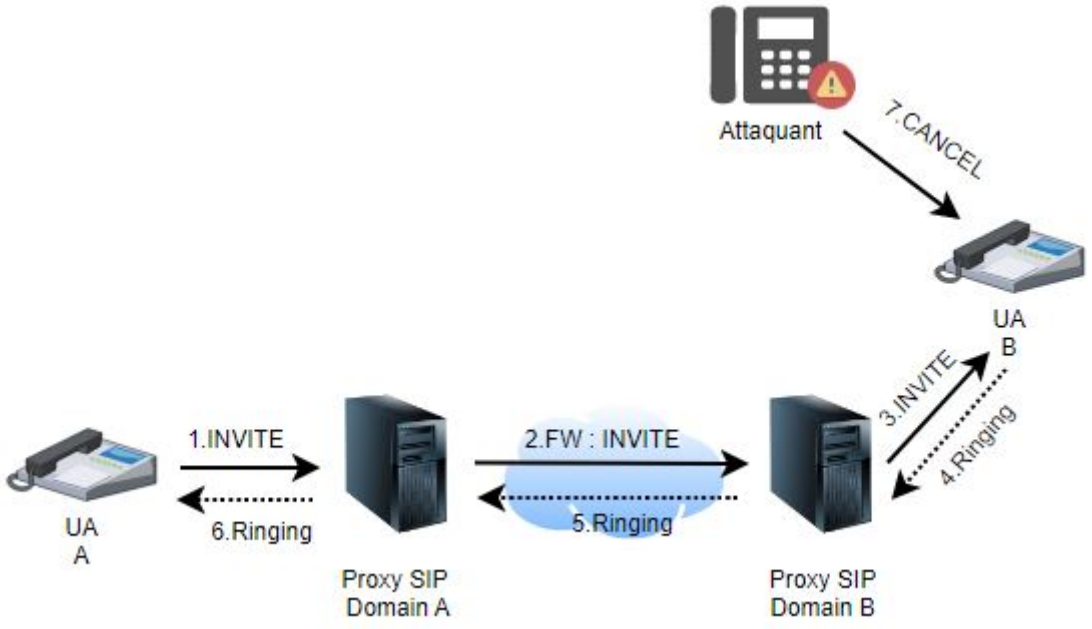


FIGURE 3.3 – DoS de type CANCEL

La figure ci-dessus montre un scénario d'attaque DoS CANCEL, l'utilisateur (UA : User Agent) A initie l'appel, envoie une invitation (1) au proxy auquel il est rattaché. Le proxy du domaine A achemine la requête (2) au proxy qui est responsable de l'utilisateur B. Ensuite c'est le proxy du domaine B qui prend le relais et achemine la requête INVITE (3) qui arrive enfin à destination. Le dispositif B, quand il reçoit l'invitation, sonne (4). Cette information est réacheminée jusqu'au dispositif A. L'attaquant qui surveille l'activité du proxy SIP du domaine B envoie une requête CANCEL (7) avant que B n'ait pu envoyer la réponse OK qui accepte l'appel. Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu. L'activité du proxy SIP du domaine B envoie une requête CANCEL (7) avant que B n'ait pu envoyer la réponse OK qui accepte l'appel. Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu.

- **DoS de type BYE :** Un autre type d'attaque lancée contre les utilisateurs est le déni de service par requête BYE. Cette dernière est envoyée soit à l'appelant, soit à l'appelé, peut être utilisé pour perturber l'appel à n'importe quel moment de la communication.

  C'est exactement le même scénario que DoS de type CANCEL sauf que dans ce cas-ci, l'attaquant attend qu'une réponse positive acceptant l'appel (4) soit envoyée par B pour lancer son attaque. Dès que la 200 OK est envoyée, l'attaquant envoie une requête BYE à l'un des participants ou même aux deux, ce qui terminera l'appel sans que les communiquant n'y puissent rien.

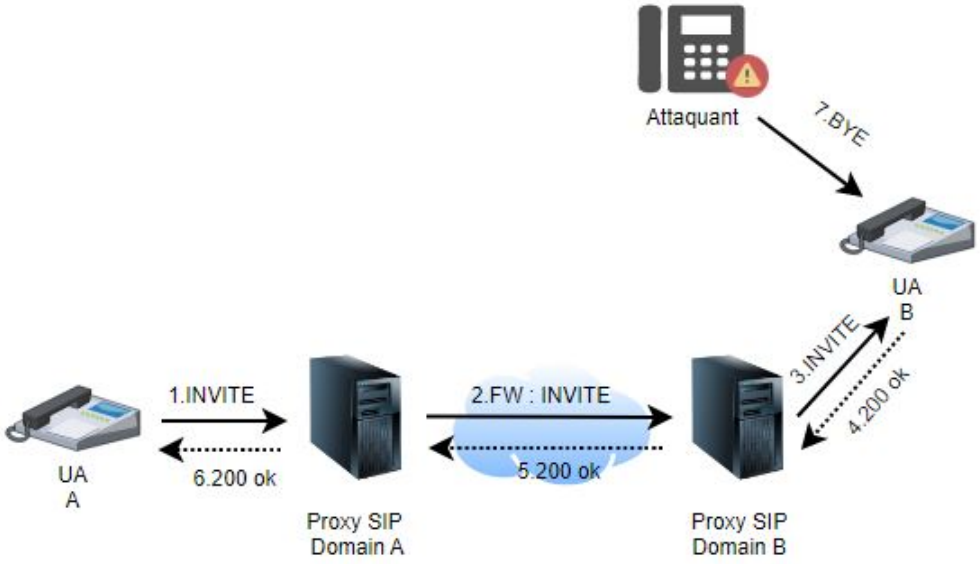


FIGURE 3.4 – DoS de type BYE

3 Solutions de sécurité

3.1 VPN

3.1.1 Définition

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers des réseaux peu sûrs comme peut l'être le réseau Internet (figure 3.5). Les VPN ont pour objectif de contribuer à la sécurisation des échanges de données privées, sensible sur les réseaux publics.

Un VPN fonctionne selon un système de tunnelisation privé, c'est-à-dire qu'un tunnel est créé, à l'intérieur duquel transitent toute la communication et toutes les données transmises qui sont cryptées.

Un VPN est très fermé, un utilisateur non autorisé, ne peut en aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles, et donc inutilisables.

Le fonctionnement des VPN repose sur des technologies appelées protocoles de tunnelisation ou protocoles VPN et parmi eux nous retrouvons [5] :

- Internet Protocol Security (IPSec).
- Layer 2 Tunneling Protocol (L2TP).
- Point-to-Point Tunneling Protocol (PPTP).
- Hybrid VPN.

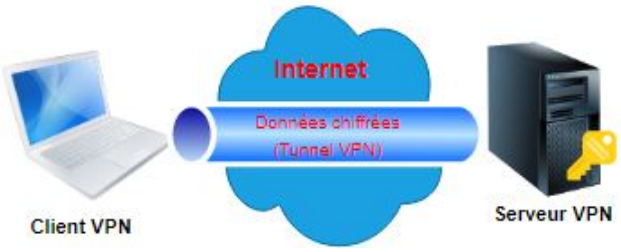


FIGURE 3.5 – VPN

3.1.2 Types

On distingue trois types de VPNs :

- **VPN d'accès :** Le VPN d'accès est utilisé pour permettre à un utilisateur itinérant ou isolé de se connecter dans un réseau local interne par exemple, de son entreprise (figure 3.6). L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN [14].

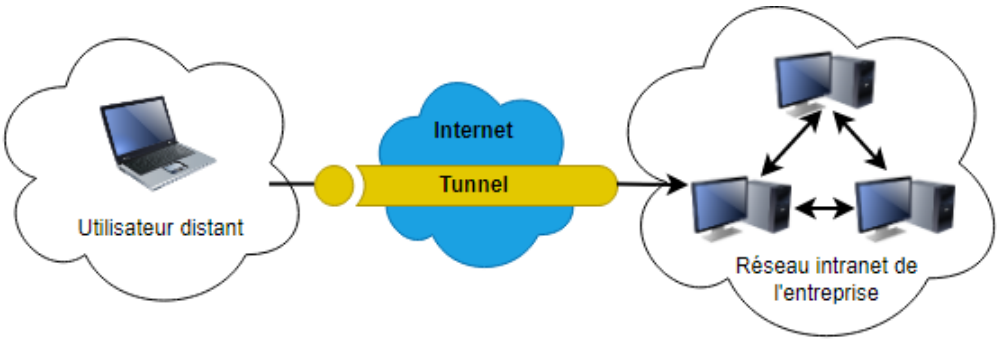


FIGURE 3.6 – VPN d'accès

- **Intranet VPN :** Dans une entreprise l'Intranet met à la disposition des employés des documents divers (texte, vidéo, image…), ce qui permet d'avoir un accès centralisé et cohérent aux informations de l'entreprise.
  L'intranet peut remplir plusieurs fonctions [13] :
  - Mise à disposition de documents techniques.
  - Mise à disposition d'informations sur l'entreprise.
  - Forums de discussion, listes de diffusion, chat en direct.
  - Portail vers internet
  - Messagerie électronique
  - Visioconférence

- **Extranet VPN :** L'utilisation d'un VPN extranet permet à une entreprise d'établir une communication sécurisée avec ses clients, fournisseurs et partenaires via un intranet d'entreprise reposant sur une infrastructure partagée et des connexions dédiées (figure 3.7). Dans cette configuration, il est essentiel que l'administrateur du VPN ait la capacité de surveiller les clients présents sur le réseau et de gérer les droits d'accès de chacun de manière appropriée [14].

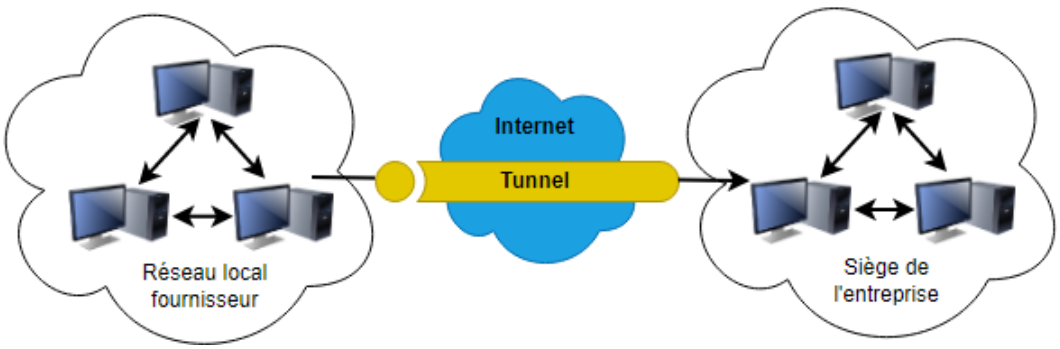


FIGURE 3.7 – Extranet VPN

3.1.3 OpenVPN

Le Protocole Open VPN est une application informatique ouverte pour la mise en place de techniques de VPN, avec des connexions sécurisées point-par-point ou site-par-site, pour des configurations via routage ou pont, ainsi que pour les accès à distance. Il exploite un protocole de sécurité sur mesure qui utilise SSL/TLS pour les échanges des clés.

Un protocole Open VPN permet à des homologues de s'authentifier mutuellement en utilisant une clé secrète pré-partagée, des certificats ou un nom d'utilisateur / mot de passe. Lorsqu'il est utilisé dans une configuration multi client-serveur, il permet au serveur de libérer un certificat d'authentification pour chaque client, en utilisant la signature et l'autorité de certification [13].

3.1.4 Protocole IPSec

Définition : IPSec est un protocole fournissant un mécanisme de sécurisation au niveau de la couche réseau du modèle OSI. Il assure la confidentialité (grâce au cryptage), l'authentification (qui permet d'être certain de l'identité de l'émetteur) et l'intégrité des données permettant de s'assurer que personne n'a pu avoir accès aux informations.

IPSec permet de protéger les données et également l'en-tête d'une trame, en masquant le plan d'adressage grâce à l'ajout d'un en-tête IPSec à chaque datagramme IP. IPSec de par sa position, agit sur chaque datagramme IP et permet ainsi d'offrir une protection unique pour toutes les applications [12].

Protocoles associés [15] :

- **ISAKMP :** (Internet Security Association and Key Management Protocol) consiste à définir des procédures et des formats de paquets pour établir, négocier, modifier et supprimer des associations de sécurité entre deux extrémités IPsec.

  Une association de sécurité est une relation entre deux entités de réseau qui garantit les services de sécurité pour le trafic généré. Elle définit l'ensemble des opérations IPSec devant être appliquées aux paquets.
- **IKE :** (Internet Key Exchange) est un protocole non connecté opérant sur UDP (port500), au niveau delacouche Application. Il est chargé de négocier la connexion en se basant sur le protocole ISAKMP. Avant qu'une transmission IPsec puisse être possible, IKE est utilisé pour authentifier les deux extrémités d'un tunnel sécurisé en échangeant des clés partagées.
- **AH :** (Authentication Header) fournit l'intégrité et l'authentification. Il authentifie les paquets en les signant, ce qui assure l'intégrité de l'information. Une signature unique est créée pour chaque paquet envoyé et empêche que l'information soit modifiée3.
- **ESP :** (Encapsulating Security Payload), en plus de l'authentification et l'intégrité, fournit également la confidentialité par l'entremise de la cryptographie.

Modes [18] :

- **Mode transport :**
  - Assure la protection pour les protocoles de la couche transport.
  - ESP chiffre (et optionnellement authentifie) uniquement l'information utile du paquet IP (l'en-tête reste inchangé).
  - AH authentifie l'information utile IP et des parties de l'en-tête IP.
- **Mode tunnel :**
  - Assure la protection du paquet IP tout entier.
  - Ce mode est utile lorsqu'une des extrémités du tunnel n'est pas celle de la destination finale(une passerelle de sécurité (pare-feu, passerelle implémentant IPSec, etc.)). Dans ce mode, la passerelle encapsule et décapsule les paquets lors de leur traversée.

3.2 VLANs

3.2.1 Définition

Un VLAN est un concept de réseau informatique qui permet de regrouper des dispositifs dans un même segment logique, indépendamment de leur emplacement physique dans le réseau. En utilisant les VLANs, les administrateurs réseau peuvent subdiviser un réseau physique en plusieurs réseaux logiques distincts.

3.2.2 Classification

Les VLANs sont classifiés en trois niveaux [16] :

- **VLAN niveau 1 :** Chaque port physique du commutateur est configuré par l'administrateur du réseau pour appartenir à un VLAN, et toute machine (ou ensemble de machines) qui se trouve branchée sur ce port fera partie de ce VLAN (figure 3.8). C'est le mode de fonctionnement le plus simple.

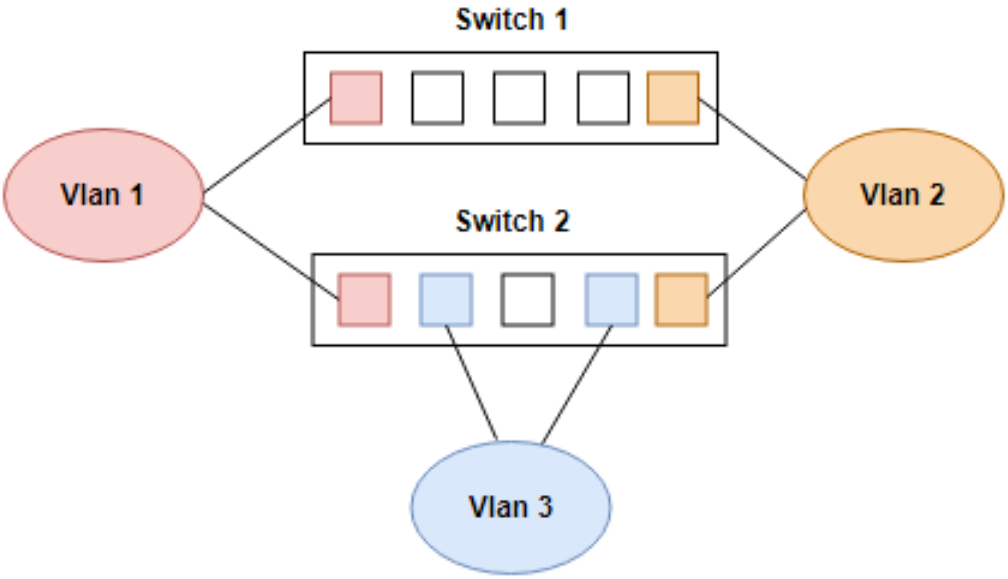


FIGURE 3.8 – VLAN niveau 1

- **VLAN niveau 2 :** Dans ce modèle, l'appartenance d'une station à un VLAN est déterminée par son adresse MAC, ce qui conserve la répartition des VLANs même après le déplacement d'une station.

  Contrairement au modèle de VLAN basé sur le port, des stations appartenant à des VLAN différents peuvent être connectées au même port d'un commutateur. Une station peut potentiellement être membre de plusieurs VLANs différents.

- **VLAN niveau 3 :** On distingue deux types :
  - Vlan par sous réseau ou les vlan sont constitué selon les adresse IP.
  - Vlan par protocoles ou les vlan sont constitué selon le type de protocole.

3.2.3 Types [16]

- **VLAN par défaut :** Au démarrage initial du commutateur, tous les ports du commutateur deviennent membres du VLAN par défaut, ce qui les place tous dans le même domaine de diffusion. Cela permet à tout périphérique réseau connecté à l'un des ports du commutateur de communiquer avec d'autres périphériques sur les autres ports du commutateur.
- **VLAN de données :** Il peut également être considéré comme un VLAN utilisateur. Le VLAN de données est configuré pour transporter uniquement le trafic généré par l'utilisateur. L'importance de séparer les données utilisateur de tout autre type de VLANs réside dans la gestion et le contrôle des commutateurs appropriés.
- **VLAN natif :** Il est utilisé pour traiter le trafic qui ne porte pas de balise VLAN (untagged traffic) lorsqu'il est reçu sur un port d'un commutateur configuré avec des VLANs. Par défaut, le VLAN natif est généralement le VLAN 1, mais il peut être configuré pour être un autre VLAN selon les besoins spécifiques du réseau.
- **VLAN de gestion :** Un VLAN de gestion est tout VLAN configuré pour accéder aux fonctions de gestion du commutateur. La configuration ddu VLAN de gestion se fait en lui attribuant une adresse IP et un masque de sous-réseau.
- **VLAN de voix :** Il est utilisé pour isoler et prioriser le trafic vocale des autres types de trafic dans un réseau afin de bénificier d'une bande passante garantie et d'une latence réduite, ce qui est essentiel pour des communications vocales fluides et sans interruption.

3.2.4 Protocole VTP (VLAN Trunking Protocol)

Est un protocole développé par Cisco servant à échanger des informations VLAN sur des liaisons agrégées, afin de réduire l'administration VLAN et les erreurs de configuration. Il permet de circuler les informations des VLAN sur des différents commutateurs sans avoir besoins de configurer les VLAN sur chaque commutateur [17].

3.3 Pare-feu

Un pare-feu dédié à la VoIP est conçu pour sécuriser les communications VoIP et protéger le réseau contre les intrusions malveillantes. Il permet de bloquer les tentatives d'accès non autorisées, de contrôler le trafic entrant et sortant, et de filtrer les paquets de données pour éviter les attaques par déni de service (DoS).

Le pare-feu doit être configuré pour reconnaître et traiter les protocoles de VoIP couramment utilisés, et doit être mis à jour régulièrement avec les derniers correctifs de sécurité pour garantir une protection maximale contre les menaces. De plus, les règles de firewall doivent être testées régulièrement

pour s'assurer qu'elles fonctionnent correctement et qu'elles n'empêchent pas le bon fonctionnement de la VoIP.

4 Conclusion

La technologie VoIP est considérée comme l'une des innovations les plus prometteuses de ces dernières années et est en train de devenir une application clé d'Internet. Malheureusement, sa popularité croissante en fait également une cible de choix pour les attaquants, et de nombreuses attaques ont été recensées.

Au cours de ce chapitre, nous avons examiné les attaques les plus courantes et les plus répandues qui peuvent menacer la sécurité des réseaux VoIP ainsi que quelques solutions de sécurité possibles pour remédier à ces attaques.

Chapitre 4

Réalisation

Introduction

Dans ce chapitre nous allons procéder à la phase pratique et pour cela nous l'avons divisé en deux parties. La première partie est consacrée à la présentation de l'organisme d'accueil et l'étude de l'existant afin de définir les insuffisances pour améliorer le système existant.
Dans la deuxième partie nous allons entamer la phase réalisation qui constitue le dernier volet de ce rapport et qui a pour objectif d'exposer le travail réalisé. Pour ce faire, on va commencer tout d'abord par préciser l'environnement matériel et logiciel de ce travail. Ensuite, on va présenter le travail accompli tout au long de ce projet.

Partie 1 : Présentation de l'organisme d'accueil

1 Présentation de l'entreprise Campus NTS

1.1 Création et évolution

NTS est une jeune entreprise axée sur la recherche, la conception et la mise en oeuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et le conseil. Elle a été créé en 2020 à Bejaia par Yassine djebbari, qui a de nombreuses années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays : Air Algérie, Retelem Alger, Poste d'Algérie...

1.2 Localisation

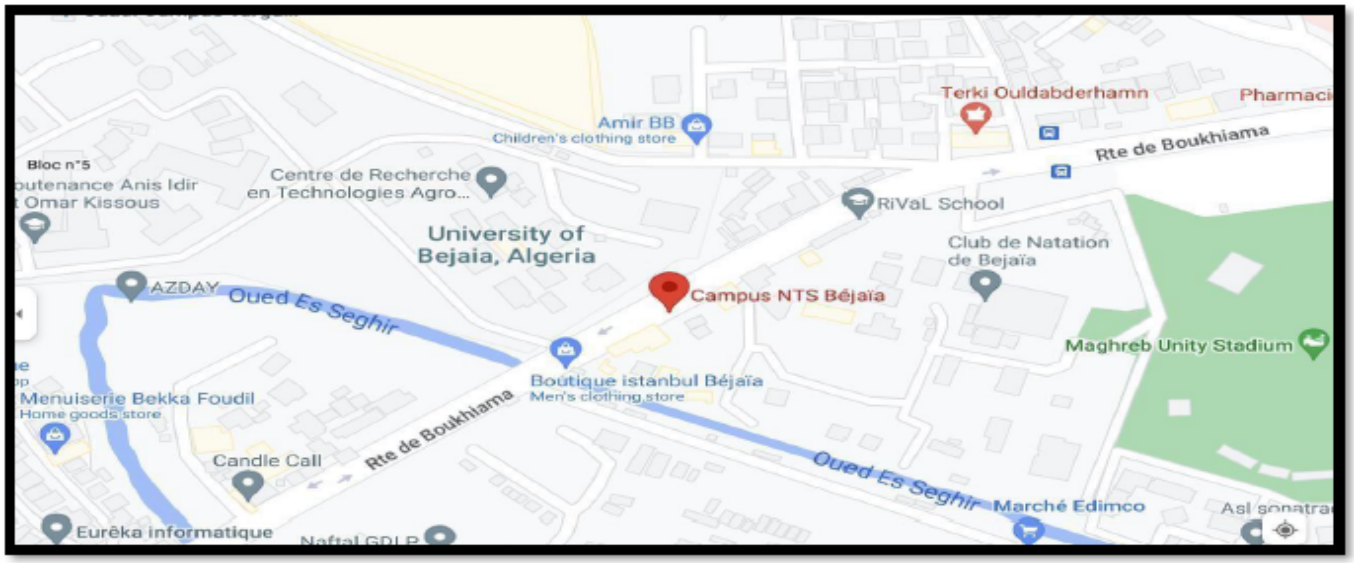


FIGURE 4.1 – Localisation de l'entreprise NTS

1.3 Fiche technique

Dénomination	Campus NTS
Logo	
Siège	Bâtiment A les beaux quartiers Targa Ouzemour, Béjaïa 06000
Secteurs d'activités	Informatique et télécommunication
Numéros de FAX	044 204 400
Numéros de Téléphone	0770446101
Email	contact@campus-nts.com
Site Internet	http://www.campus-nts.com/

TABLE 4.1 – Fiche technique du Campus NTS

1.4 Objectifs, Missions et activités de l'entreprise NTS

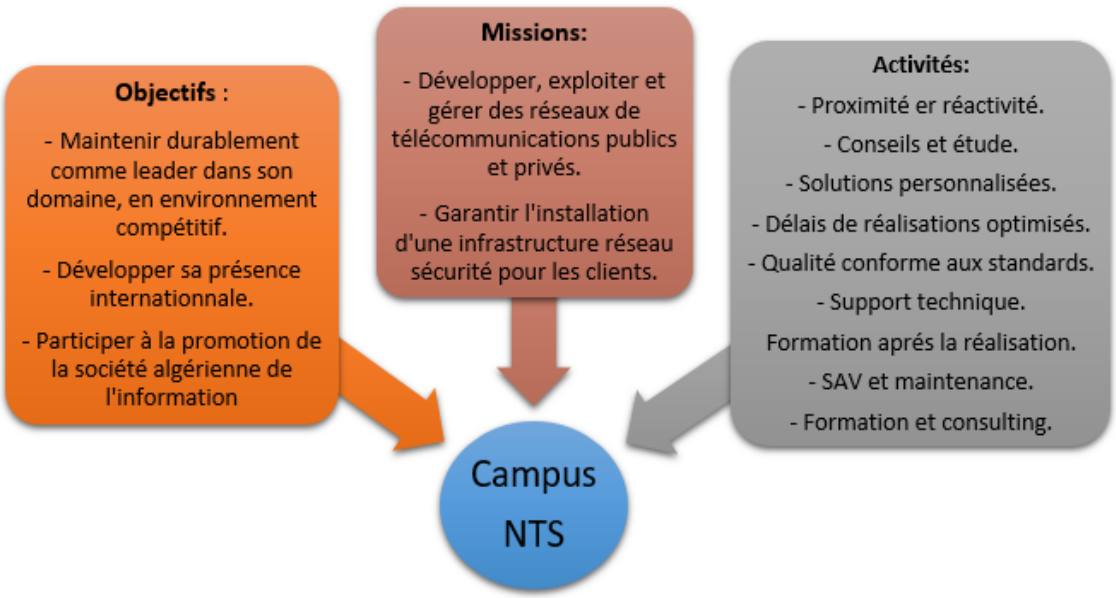


FIGURE 4.2 – Objectifs, Messions et Activités du Campus NTS

1.5 Organigramme général

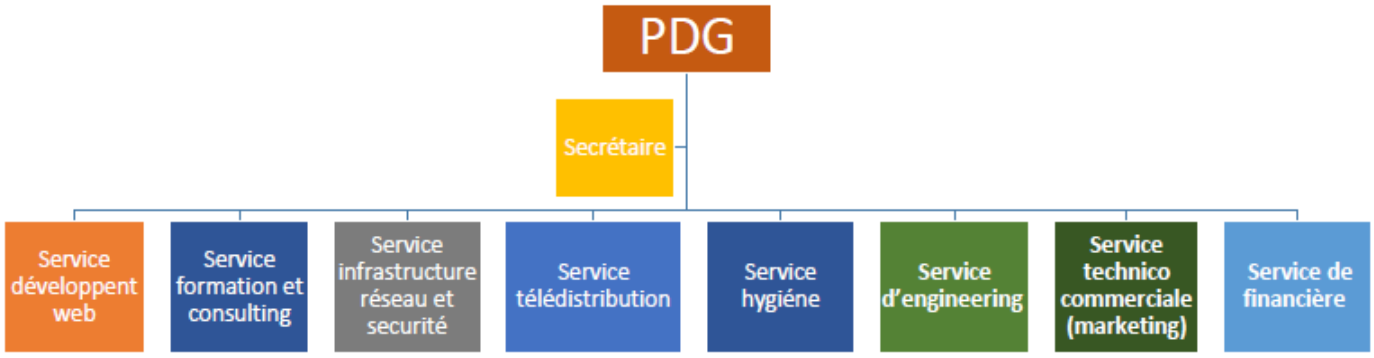


FIGURE 4.3 – Organigramme général du Campus NTS

Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du campus NTS :

1.5.1 Service développement web

Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des langages de programmation informatique tels que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

1.5.2 Service formation et consulting

Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :

- Installation et configuration des réseaux informatiques.
- Administration et sécurité des réseaux et système.
- Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto…).
- Installation et configuration des réseaux sans fil professionnel.
- Installation et configuration des caméras de surveillance analogique et numérique.
- Fibre optique les réseaux d'accès FTTH/FTTX.
- Création des sites web.
- Programmation (C, C++, Java, Python…etc.).

- Electricités Bâtiments et industriels.
- Formation Cisco CCNA, CCNP.
- Virtualisation.
- Microsoft server, SQL.
- Cyber sécurité.

Ces stages s'adressent aux étudiants, ouvriers, entreprises en fin de projet et à tous ceux qui apprécient le terrain pour développer leurs compétences en sécurité, acquérir des qualifications supérieures et leur expérience en entreprise.

NTS repose sur la capacité des ressources et des structures à délivrer à ses clients et à ses partenaires (Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei).

1.5.3 Service infrastructure réseau et sécurité

L'infrastructure réseau est au coeur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.
Il est divisé en trois services :

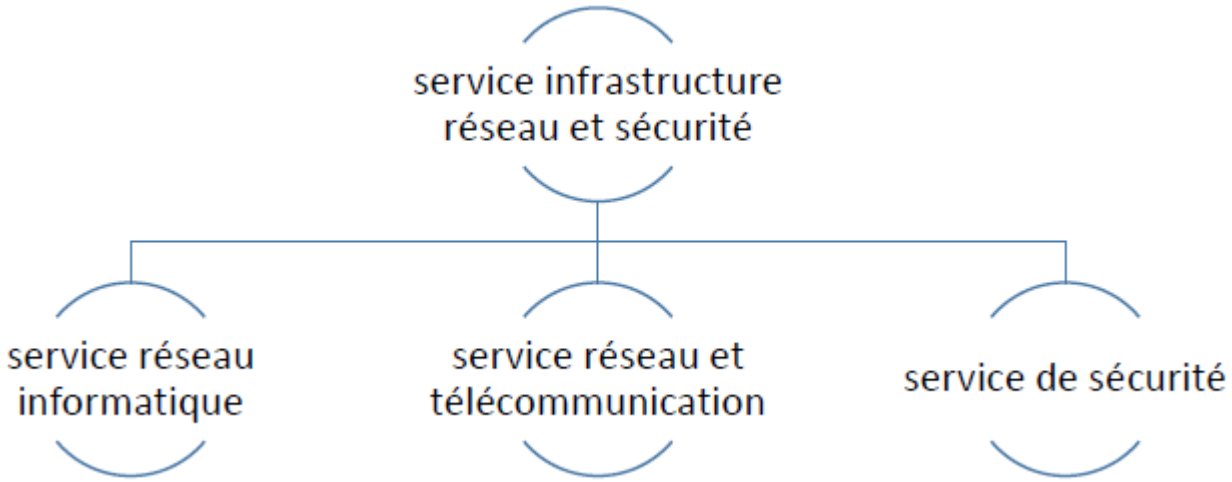


FIGURE 4.4 – organigramme du service infrastructure réseau et sécurité

- **Service réseau informatique :** Qui représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autre méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que :
  Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.
- **Service réseau et télécommunication :** Les services de télécommunications sont conçus pour transmettre des informations en un temps réel (synchronisation des informations) sous forme analogique ou numérique à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications.
  Voici des exemples de services d'infrastructure de télécommunications :
  - Pose de fibre optique.
  - Emplacement du site de la tour cellulaire.
  - Test d'antenne radio.
  - Installation d'équipements téléphoniques standards et réseau de données.
  - Téléphonie standard.
- **Service de sécurité :** Cette entreprise NTS accomplit à la fois le gardiennage et l'installation des systèmes de sécurité électroniques. Aussi elle fournit aux clients des solutions complètes et fiables pour protéger leurs ressources.
  Les services qu'elle réalise sont les suivants :
  - Caméras de surveillance.
  - Alarme anti- intrusion.
  - Détection incendie.
  - Pointeuse et Contrôles d'accès.
  - Vidéophonie.

1.5.4 Service télédistribution

Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numériques terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit.

Enfin, les services de télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tel que :

- Rediffusion de programmation par satellite.
- Transmission de chaînes de télévision par abonnement.
- Services interactifs.
- Programmation locale.

1.5.5 Service d'engineering

Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet.

L'équipe de campus NTS n'hésite pas à se circuler sur le terrain pour consulter l'état d'avancement du projet afin de faire face à d'éventuelles difficultés qui auraient pu survenir auparavant. Cette équipe est composée :

- D'ingénieurs en télécommunications.
- D'informaticiens en gestion et sécurité des réseaux.
- D'administrateurs de systèmes d'information.
- D'informaticiens en programmation.
- De techniciens fibre.
- De techniciens supérieurs en informatique.

1.5.6 Service technico commerciale (marketing)

Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.

1.5.7 Service de financière

Le service financier situé au coeur de l'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte.
Ce service contient un ensemble de tâches et rôles au sein de la société NTS :

Tâches :

- Assurer une saine gestion des ressources financières de l'entreprise par la planification.
- La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.
- La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

Rôle :

- La préparation et du suivi des budgets de fonctionnement et d'investissement.
- La préparation des états financiers.
- La gestion de la trésorerie et de des encaissements.
- La rémunération des employés, des comptes à payer.
- L'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.
- La réception des marchandises et du courrier.

1.5.8 service hygiène

La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tel que :

- Des actions de prévention des risques professionnels et de la pénibilité au travail.
- La mise en place d'une organisation et de moyens adaptés.

2 Etude de l'existant

2.1 Présentation du réseau campus NTS

L'entreprise a une architecture en couches et, pour assurer la communication entre ses différents services, elle connecte son LAN à une connexion FTTH fournie par un fournisseur d'accès Internet. Le schéma ci-dessous nous montre l'infrastructure du réseau NTS :

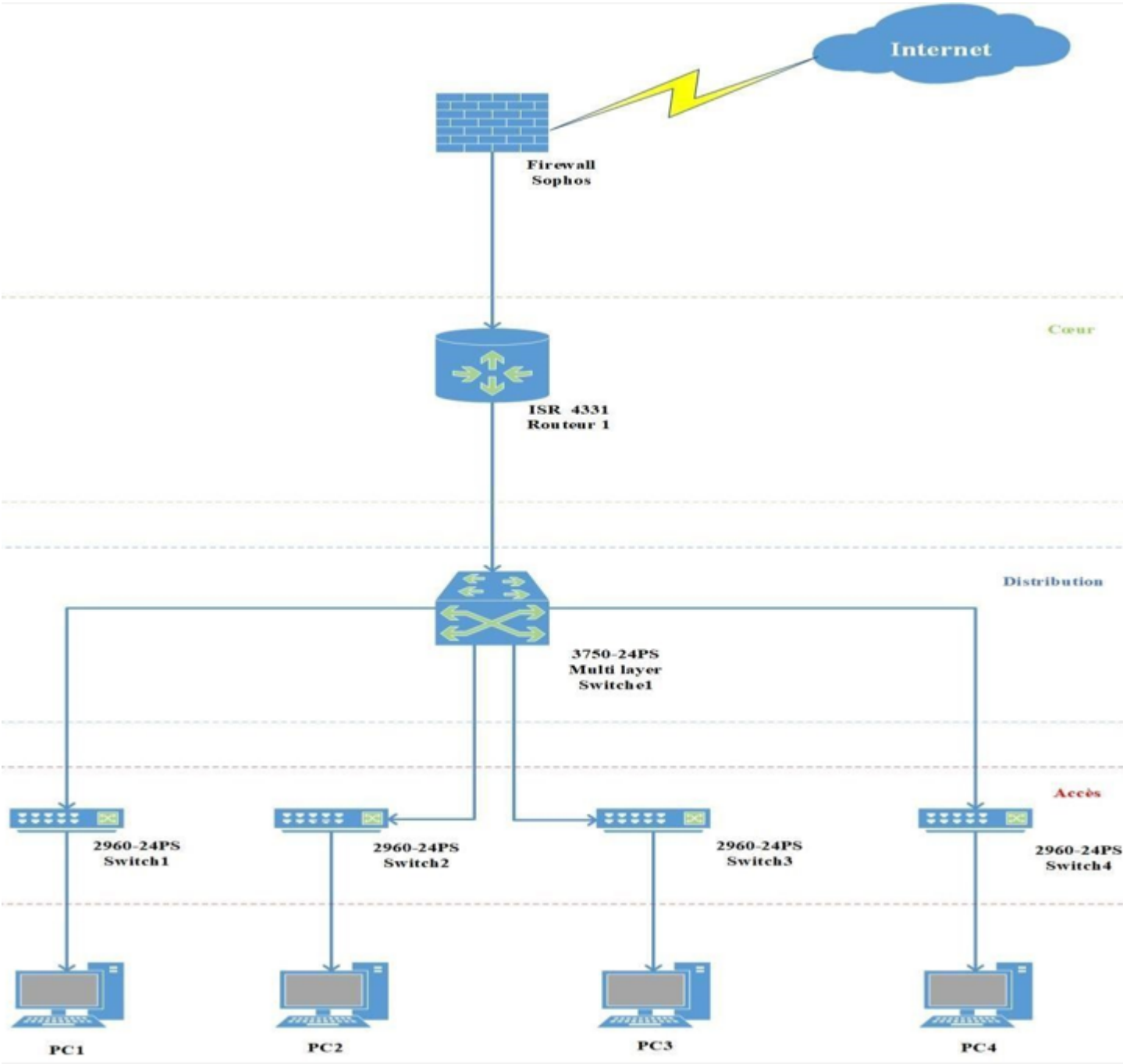


FIGURE 4.5 – Architecture du réseau NTS

2.2 Analyse du parc informatique

2.2.1 Présentation d'environnement hard et soft

Nom de l'équipement	Le hardware (hard)	Software (soft)
Routeur	ISR 4331	IOS (International Organisation For Standardisation)
Pare-feu	SOPHOS XG	Linux
Switch	• Cisco Catalyst 3750-24PS • Cisco Catalyst 2960-24PS	IOS (International Organisation for Standardisation)
Server	HP ProLiant DL380P génération 10	Windows server 2012
PC portable	Dell IAER 35 R	Windows 10

TABLE 4.2 – L'environnement hardware et software

2.2.2 Caractéristiques des équipements par niveaux

Nom de l'équipement	Modèle	Caractéristique
Router 	ISR 4331	• **RAM** : 4 G0 (installé) /16 GO (maximum) • **Débit** :100 Mb/s • **Mémoire Flash** :4000 MO • **Protocole de liaison de données** : Ethernet, fast Ethernet et gigabit-ethernet
Pare-feu 	SOPHOS XG	• **Débit** : 4000 Mbit/s • **Débit IPS** : 2700Mbit/s • **Débit VPN IP sec** : 560 Mbit/s • **@ IP/Numéro de port**
Switch 	Cisco Catalyst 3750-24PS Switch	• **Ports** : 24 ports • **Mémoire Flash** : 16MO • **Mémoire RAM** : 128MO • **Capacité de commutation** : 32 Gbit/s
Switch 	Cisco Catalyst 2960-24PS Switch	• **Ports** : 24 ports • **Mémoire Flash** : 128MO • **Mémoire RAM** : 512MO • **Capacité de commutation** : 56 Gbit/s
Server 	HP ProLiant DL380P génération 10	• Processeur Intel Xeon • 16 G0 DDR4 RDIMM (1x 16 GO -12 slots) • Silver 4110 (Octo-Core 2.1 GHZ / 3.0 GHZ Turbo-16 Threads-cache 11Mo)
PC portable 	Dell IAER 35 R	• **AMD core** : i5 8th génération **RAM** : 8GO **Disque** : 256GO • **Ecran** : UHD Graphies 620 (1920 × 1080 × 32b)

TABLE 4.3 – Détails des ressources disponibles de l'entreprise

Partie 2 : Réalisation

1 Outils de travail

- **GNS3** :
  Est un logiciel de simulation des réseaux informatiques. Il permet aux utilisateurs de créer des topologies réseau virtuelles en utilisant des dispositifs virtuels et des images d'exploitation réelles provenant de divers fournisseurs tel que Cisco. GNS3 est utilisé par les professionnels des réseaux, les ingénieurs système et les étudiants pour concevoir, tester et déployer des architectures réseau virtuelles avant de les mettre en œuvre dans un environnement réel. C'est un logiciel gratuit qui fonctionne sur plusieurs plates-formes, y compris Windows, Linux et MacOs.

FIGURE 4.6 – GNS3

- **VMware** :
  Une machine virtuelle (VM) est un environnement entièrement virtualisé qui s'exécute sur une machine physique. Elle exécute son propre système d'exploitation (OS) et bénéficie des mêmes équipements qu'une machine physique : CPU, mémoire RAM, disque dur et carte réseau.Elle permet d'exécuter plusieurs systèmes d'exploitation et applications simultanément sur une même machine physique [25].

FIGURE 4.7 – VMware

- **PFsense** :
  Pfsense ou « Packet Filter Sense » est un applicatif qui fait office de routeur/pare-feu open source basé sur le système d'exploitation FreeBSD [26]. Il permet d'analyser, de sécuriser et de gérer le trafic réseau pour empêcher tout accès non autorisé à ce réseau.

FIGURE 4.8 – PFsense

- **FreePBX** :
  FreePBX est une interface utilisateur graphique (GUI) open source basée sur le web qui gère le serveur de téléphonie Asterisk. Il a été développé par la société Sangoma en 2004 [27].

FIGURE 4.9 – FreePBX

- **Softphone** :
  Est un logiciel de téléphonie utilisé pour effectuer des appels téléphoniques sur Internet à partir d'un ordinateur plutôt que d'un téléphone [28].Nous utilisons les deux softphones 3CX et X-Lite pour tester nos appels téléphoniques.

FIGURE 4.10 – Softphones

2 Equipements utilisés

Sites	Equipements	Types	Images
Bejaia	Pare-feu (pf-bejaia)	Pfsense 2.6.0	Free BSD
	Routeur (Core1)	Cisco 7200	IOU UNIX
	Switch (Dist1)	Cisco 3750 N3	IOU UNIX
	Switch (Sw-A, Sw-B)	Cisco 2690	IOU UNIX
	FreePBX	16.0.19	Centos
Alger	Pare-feu (pf-Alger)	Pfsense 2.6.0	Free BSD
	Routeur (Core2)	Cisco 7200	IOU UNIX
	Switch (Dist2)	Cisco 3750 N3	IOU UNIX
	Switch (Sw 1, Sw 2)	Cisco 2690	IOU UNIX
	FreePBX	16.0.19	Centos

TABLE 4.4 – Détails des équipements utilisés

3 Méthodologie de travail

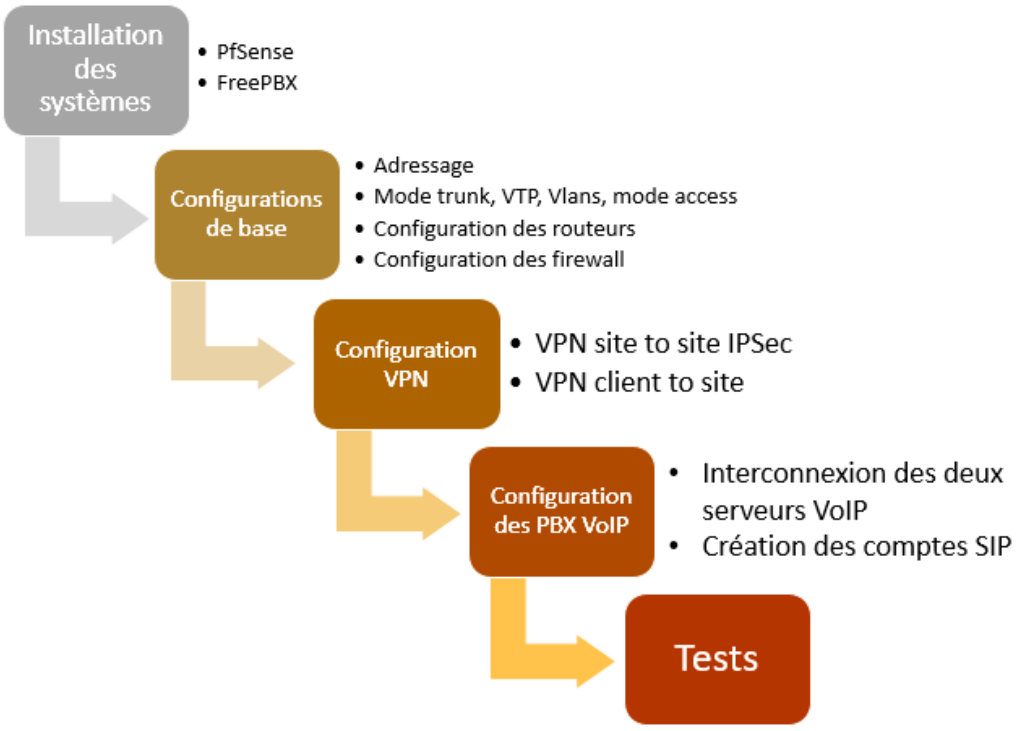


FIGURE 4.11 – Méthodologie de travail

4 Architecture proposée

La figure 4.12 représente l'architecture proposée basée sur le modèle hièrarchique, ou nous avons interconnecter deux sites distants par un canal VPN IPSec. Nous avons créé trois VLANs sur chaque site (data, gestion et voix dans lequel nous avons mis le serveur PBX).

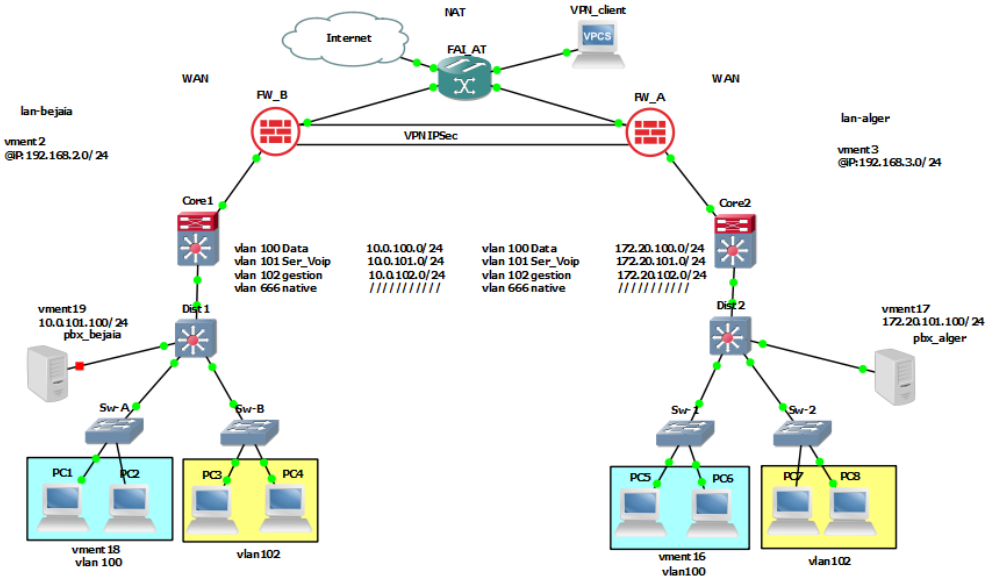


FIGURE 4.12 – Architecture proposée

5 Installations

5.1 PFsense

Nous lançons l'installation du PFsense.

FIGURE 4.13 – Démarrage du PFsense

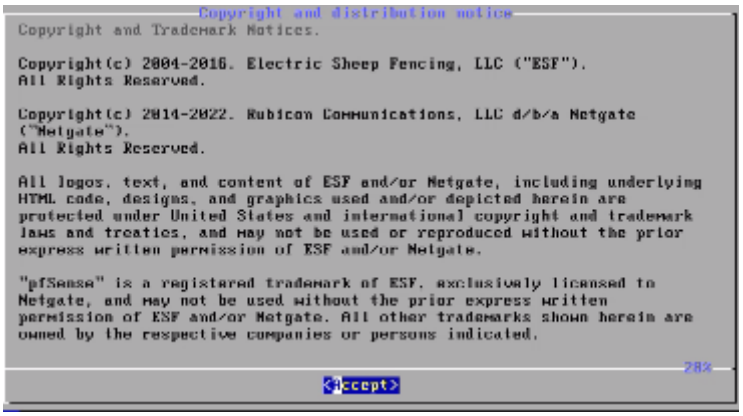


FIGURE 4.14 – Début de processus d'installation

Nous cliquons sur "accepter" pour confirmer l'installation et nous continuons sur les option par défaut jusqu'à la confirmation finale, l'installation se lance.

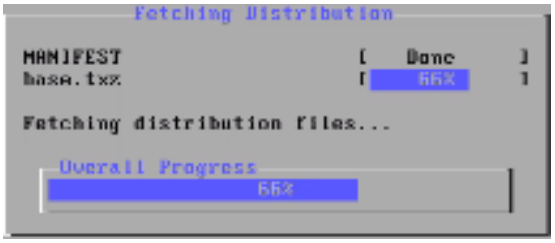


FIGURE 4.15 – Début d'installation

5.2 FreePBX

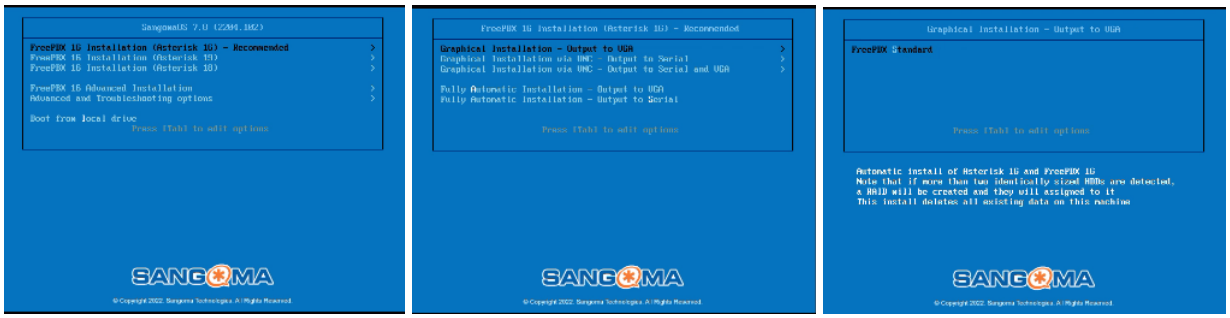


FIGURE 4.16 – Démarrage de l'installation

Aprèse le démarrage une fenêtre de paramètrage d'avant installation apparaitra.

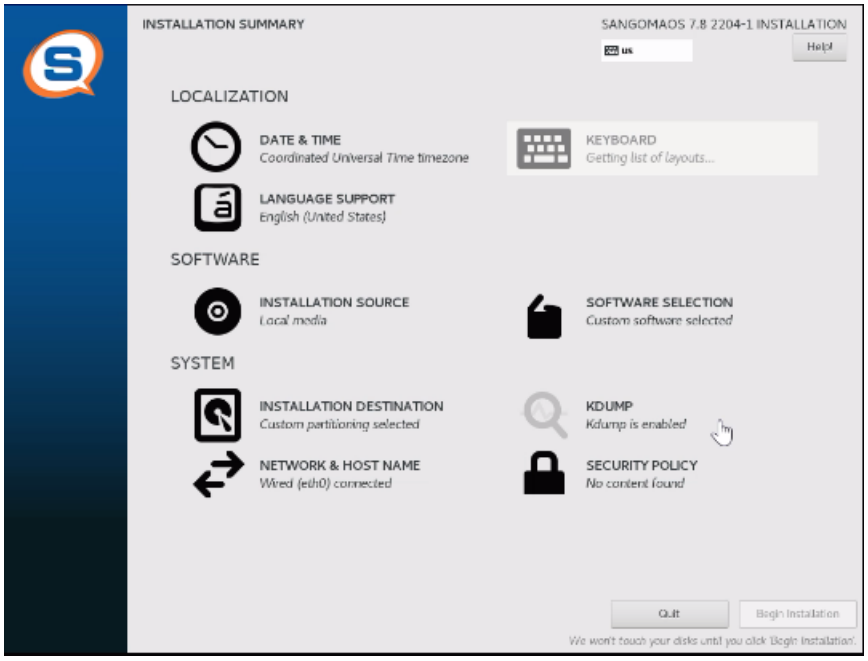


FIGURE 4.17 – Paramètres d'avant installation

Nous entrons le mot de passe qui sera utilisé par l'administrateur FreePBX.

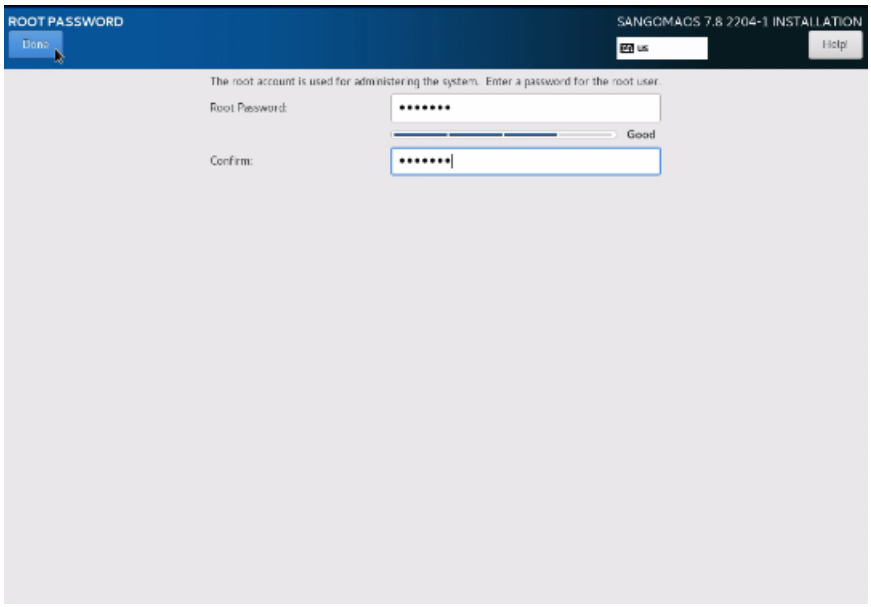


FIGURE 4.18 – Authentification de l'administrateur

Après l'installation, l'addresse IP du serveur s'affiche :

FIGURE 4.19 – Adresse IP du serveur FreePBX

Pour accéder au serveur, nous tapons son adresse IP dans un navigateur web et la page de connexion au serveur apparaitra.

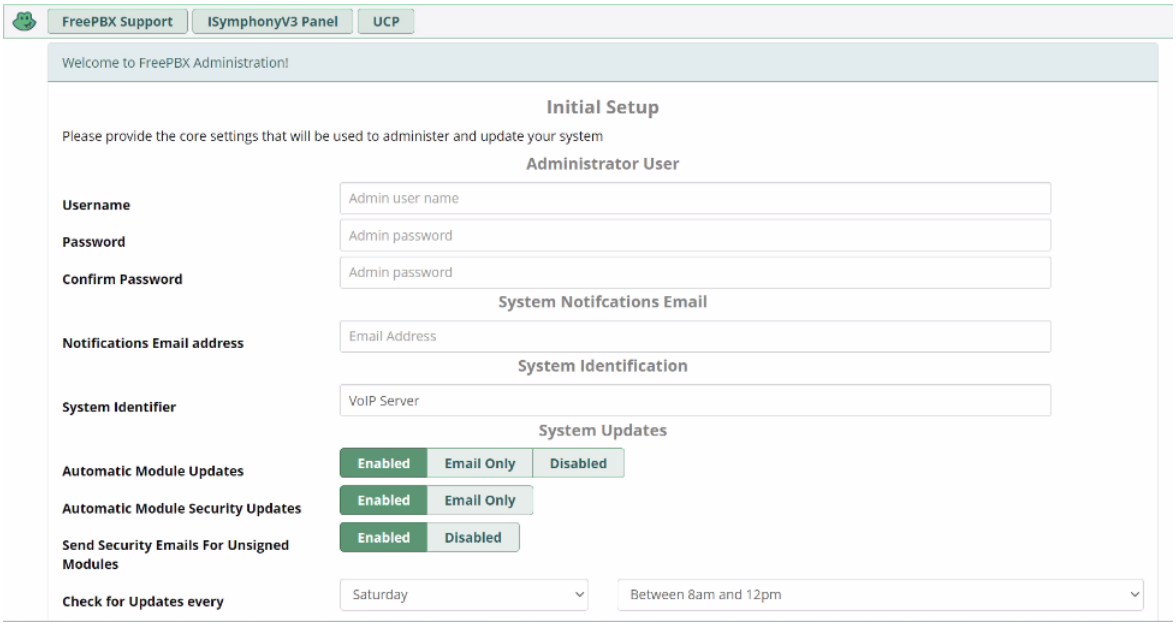


FIGURE 4.20 – Login au serveur FreePBX

Après le login, l'interface suivante s'affiche :

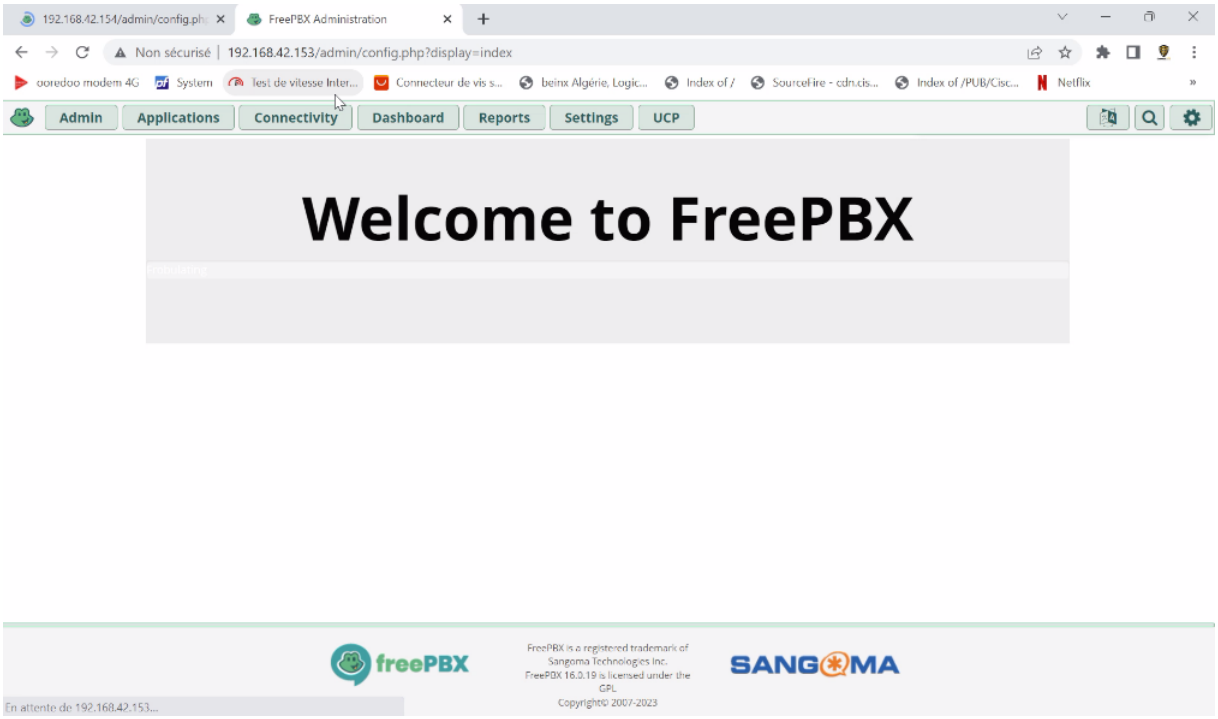


FIGURE 4.21 – Interface de FreePBX

6 Configurations de base

6.1 Plan d'adressage

6.1.1 Equipements

Equipement	Interface	Adresse IP
FW-bejaia	NAT LAN	192.168.116.130/24 192.168.2.1/24
FW-alger	NAT LAN	192.168.116.129/24 192.168.3.1/24
Pbx-bejaia	/	10.0.101.100/24
Pbx-alger	/	172.20.101.100/24
Routeur-bejaia	e 0/1	192.168.2.2/24
Routeur-alger	e 0/1	192.168.3.2/24

TABLE 4.5 – Adressage des équipements

6.1.2 Vlans

Vlan	Adresse IP (Bejaia)	Adresse IP (Alger)
Vlan 100 (Data)	10.0.100.0/24	172.20.100.0/24
Vlan 101 (Voice)	10.0.101.0/24	172.20.101.0/24
Vlan 102 (Gestion)	10.0.102.0/24	172.20.102.0/24
Vlan 666 (Native)	/	/

TABLE 4.6 – Adressage des Vlans

6.1.3 Routage inter Vlans

Routeur	Interface	Adresse IP
Core 1 (site Bejaia)	Interface e0/0 Sous interfaces : e 0/0.100 e 0/0.101 e 0/0.102	 10.0.100.1/24 10.0.101.1/24 10.0.102.1/24
Core 2 (site Alger)	Interface e0/0 Sous interfaces : e 0/0.100 e 0/0.101 e 0/0.102	 172.20.100.1/24 172.20.101.1/24 172.20.102.1/24

TABLE 4.7 – Routage inter Vlans

6.2 Interfaces en mode trunk

La configuration en mode trunk permet de transporter le trafic de plusieurs VLAN simultanément.

- Switch Dist1 (même configuration pour le switch Dist2) :

```
Dist1#Conf t
Dist1(config)#interface range ethernet 3/2-3
Dist1(config-if-range)#switchport trunk encapsulation dot1q
Dist1(config-if-range)#switchport mode trunk
Dist1(config-if-range)#exit
```

- Switch Sw-A (même configuration pour les autres switchs d'accès) :

```
Sw-A#Conf t
Sw-A(config)#interface ethernet 3/1
Sw-A(config-if)#switchport trunk encapsulation dot1q
Sw-A(config-if)#switchport mode trunk
Sw-A(config-if)#end
```

6.3 Configuration VTP

La configuration VTP est utilisée pour gérer et propager les informations relatives aux VLANs dans un réseau.

- VTP Server sur le switch Dist1 (même configuration pour le switch Dist2) :

```
Dist1#Conf t
Dist1(config)#vtp mode server
Dist1(config)#vtp password asr2023
Dist1(config)#vtp domain campusnts.vtp
Dist1(config)#vtp version 2
Dist1(config)#vtp pruning
Dist1(config)#end
```

- VTP Client sur le switch Sw-A (même configuration pour les autres switchs d'accès) :

```
Sw-A#Conf t
Sw-A(config)#vtp mode client
Sw-A(config)#vtp domain campusnts.vtp
Sw-A(config)#vtp password asr2023
Sw-A(config)#vtp version 2
Sw-A(config)#end
```

6.4 Création des Vlans

```
Dist1#Conf t
Dist1(config)#vlan 100
Dist1(config)#name data
Dist1(config)#vlan 101
Dist1(config)#name voice
Dist1(config)#vlan 102
Dist1(config)#name gestion
Dist1(config)#vlan 666
Dist1(config)#name native
Dist1(config)#end
```

La création se fait de la même manière sur le switch Dist2.

- **Configuration du vlan native**

```
Dist1#Conf t
Dist1(config)#interface range ethernet 3/2-3
Dist1(config-if-range)#switchport trunk native 666
Dist1(config-if-range)#switchport trunk allowed vlan 100-102,666
Dist1(config-if-range)#end
```

La configuration se fait de la même manière sur le switch Dist2.

6.5 Affectation des ports mode access

- **Switch Dist1**

```
Dist1#Conf t
Dist1(config)#interface ethernet 3/1
Dist1(config-if)#switchport mode access
Dist1(config-if)#switchport access vlan 101
Dist1(config-if)#end
```

- **Switch Sw-A**

```
Sw-A#Conf t
Sw-A(config)#interface range ethernet 3/2-3
Sw-A(config-if-range)#switchport mode access
Sw-A(config-if-range)#switchport access vlan 100
Sw-A(config-if-range)#end
```

- **Switch Sw-B**

```
Sw-B#Conf t
Sw-B(config)#interface range ethernet 3/2-3
Sw-B(config-if-range)#switchport mode access
Sw-B(config-if-range)#switchport access vlan 102
Sw-B(config-if-range)#end
```

6.6 Configurations routeur

➢ **Remarque :** Les configurations se font de la même manière pour le routeur Core2.

6.6.1 Configuration d'interface

```
Core1#Conf t
Core1(config)#interface ethernet 0/1
Core1(config-if)#no shutdown
Core1(config-if)#ip address 192.168.2.2 255.255.255.0
Core1(config-if)#end
```

6.6.2 Routage inter Vlans

```
Core1#Conf t
Core1(config)#interface ethernet 0/0
Core1(config-if)#no shutdown
Core1(config-if)#exit
Core1(config)#interface ethernet 0/0.100
Core1(config-subif)#encapsulation dot1q 100
Core1(config-subif)#ip address 10.0.100.1 255.255.255.0
Core1(config-subif)#exit
Core1(config)#interface ethernet 0/0.101
Core1(config-subif)#encapsulation dot1q 101
Core1(config-subif)#ip address 10.0.101.1 255.255.255.0
Core1(config-subif)#exit
Core1(config)#interface ethernet 0/0.102
Core1(config-subif)#encapsulation dot1q 102
Core1(config-subif)#ip address 10.0.102.1 255.255.255.0
Core1(config-subif)#end
```

6.6.3 Configuration DHCP

```
Core1#Conf t
Core1(config)#ip dhcp pool vlan100
Core1(dhcp-config)#network 10.0.100.0 255.255.255.0
Core1(dhcp-config)#default-router 10.0.100.1
Core1(dhcp-config)#dns-server 8.8.8.8 9.9.9.9
Core1(dhcp-config)#exit
Core1(config)#ip dhcp pool vlan101
Core1(dhcp-config)#network 10.0.101.0 255.255.255.0
Core1(dhcp-config)#default-router 10.0.101.1
Core1(dhcp-config)#dns-server 8.8.8.8 9.9.9.9
Core1(dhcp-config)#exit
Core1(config)#ip dhcp pool vlan102
Core1(dhcp-config)#network 10.0.102.0 255.255.255.0
Core1(dhcp-config)#default-router 10.0.102.1
Core1(dhcp-config)#dns-server 8.8.8.8 9.9.9.9
Core1(dhcp-config)#exit
Core1(config)#ip dhcp excluded-address 10.0.100.1 10.0.100.10
Core1(config)#ip dhcp excluded-address 10.0.101.1 10.0.101.10
Core1(config)#ip dhcp excluded-address 10.0.102.1 10.0.102.10
```

6.7 Configuration Firewall

6.7.1 Interfaces WAN et LAN

Nous avons configuré l'interface LAN, l'interface WAN a été configuré avec le serveur DHCP.

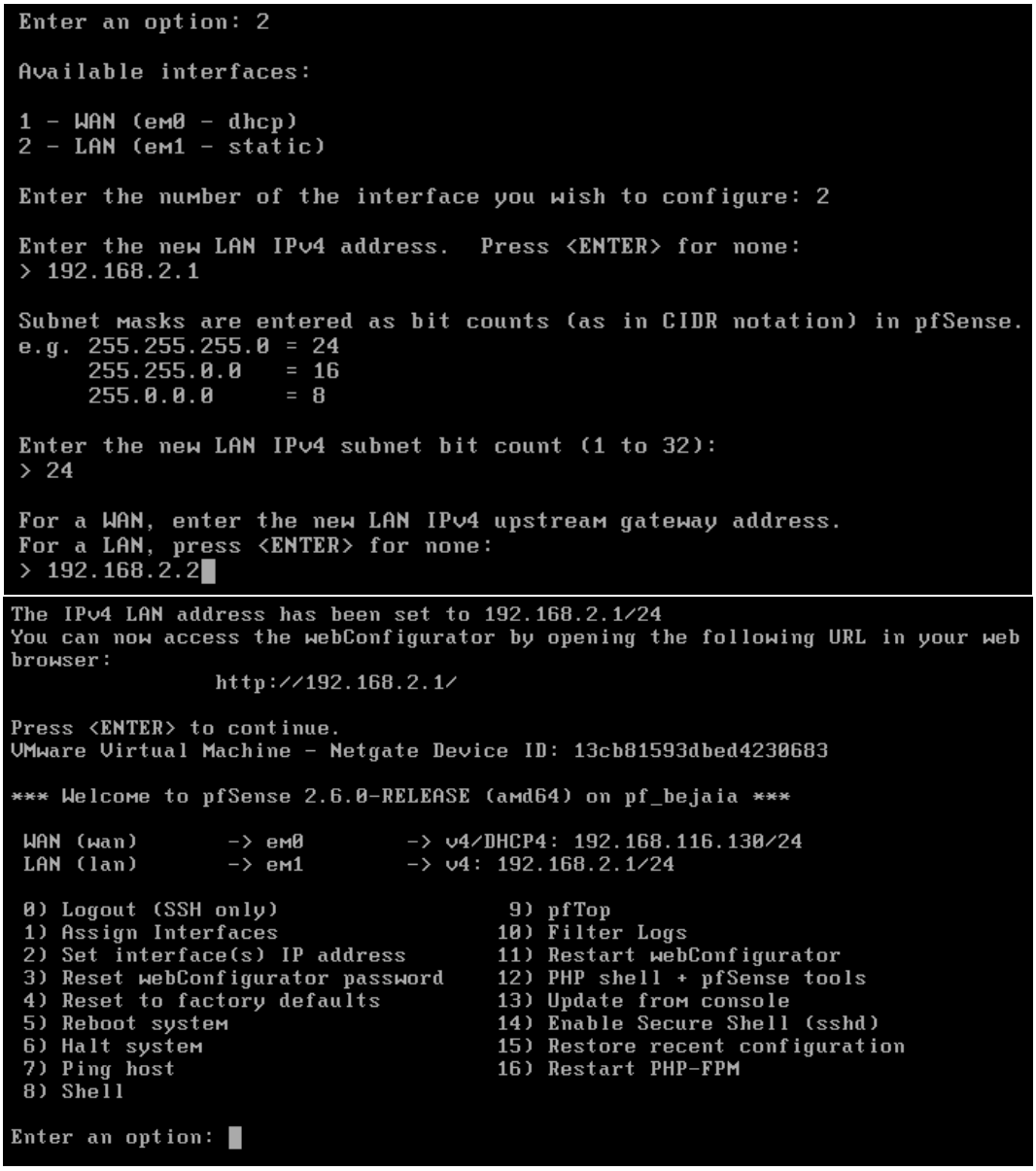


FIGURE 4.22 – Interfaces de FW-bejaia

Les étapes sont les mêmes pour le FW-alger :

- l'interface WAN : 192.168.116.129/24
- l'interface LAN : 192.168.3.1/24

Après avoir configurer les interfaces, nous tapons l'adresse du firewall dans un navigateur pour commencer les configurations.

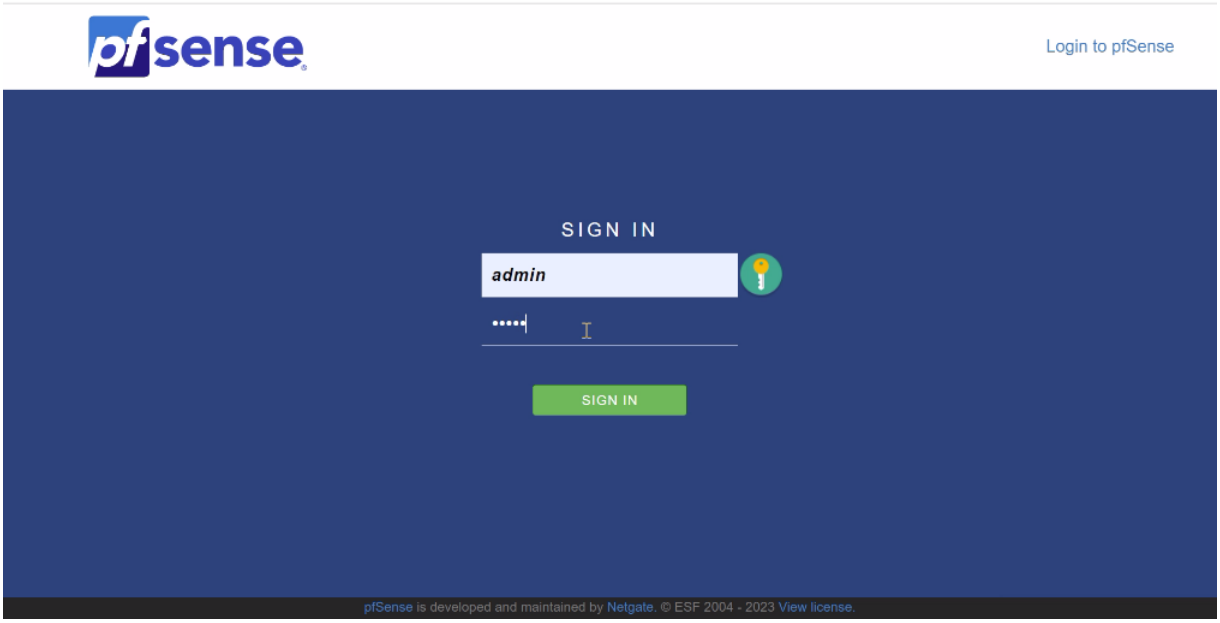


FIGURE 4.23 – L'interface de login du PfSense

6.7.2 Routage vers les vlans du réseaux

Nous devons d'abord appliquer une règle d'autorisation de trafic pour les vlans :

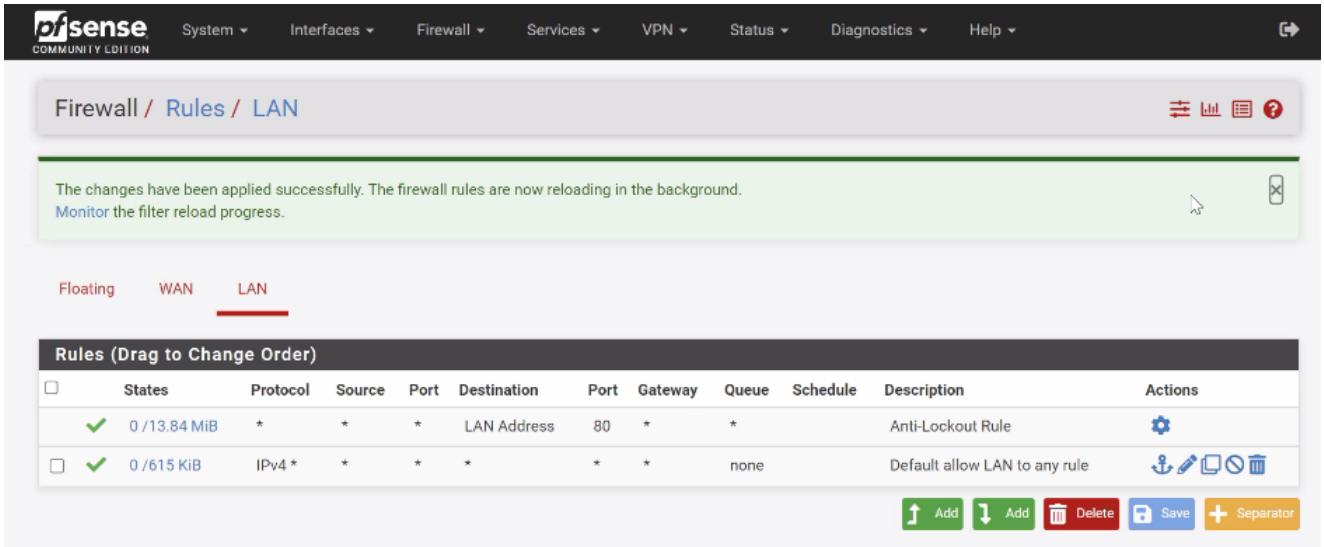


FIGURE 4.24 – Règle d'autorisation

Nous pouvons maintenant router notre firewall vers les vlans.

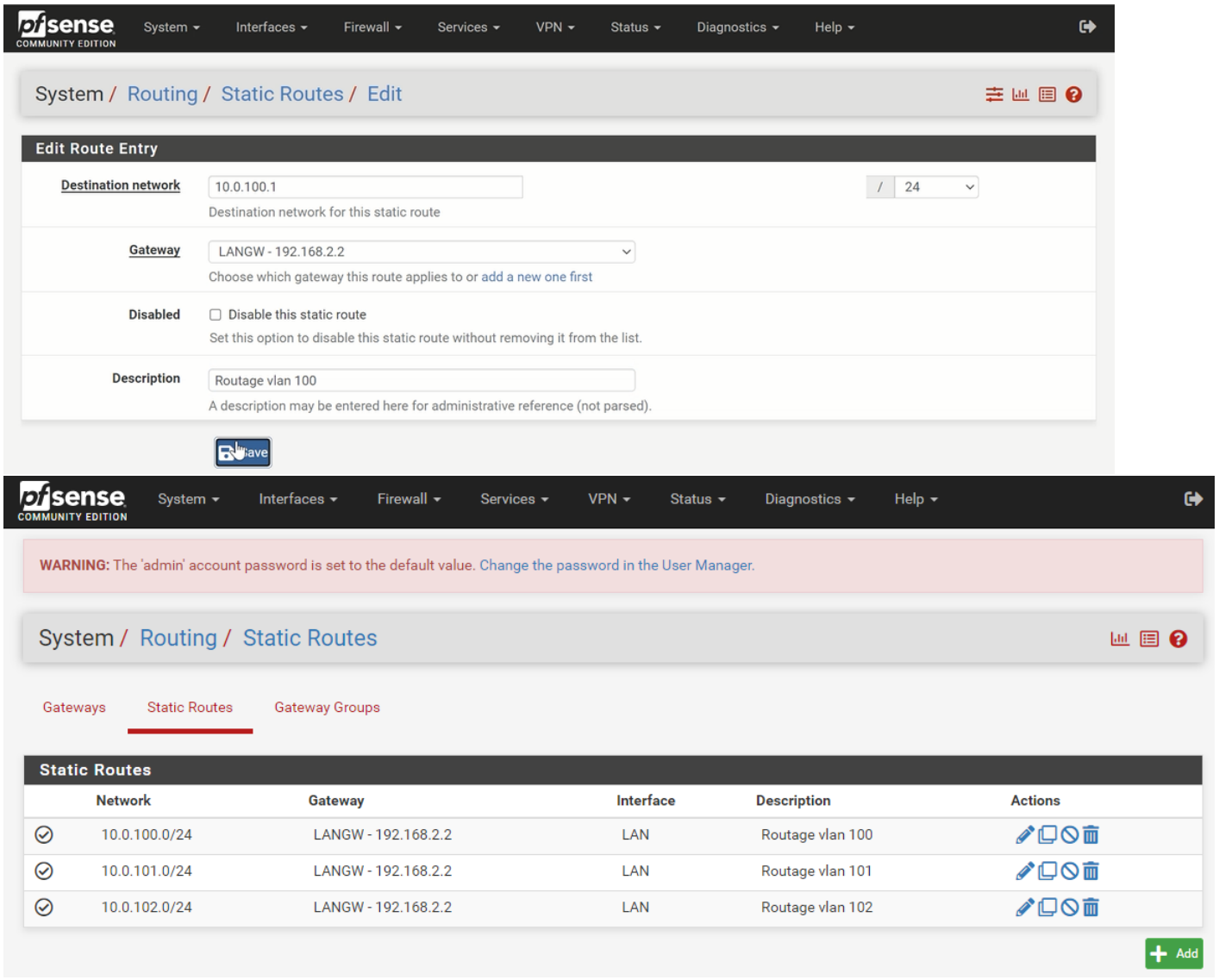


FIGURE 4.25 – Routage vers les vlans

Nous effectuons les mêmes configurations sur le firewall d'Alger

7 Configuration des VPN

7.1 VPN site to site IPSec

La création d'un tunnel VPN IPSec se fait en deux phase :

- **Phase 1** : C'est là que nous allons programmer la clé de chiffrement.

Nous somme sur le firewall de Bejaia, nous séléctionons l'interface WAN du firewall d'Alger comme passerelle distante. Nous allons créer une clé de chiffrement utilisant l'algorithme de cryptage AES-256 qui offre le plus haut niveau de sécurité disponible pour protéger tout le trafic qui passe sur nos serveurs.

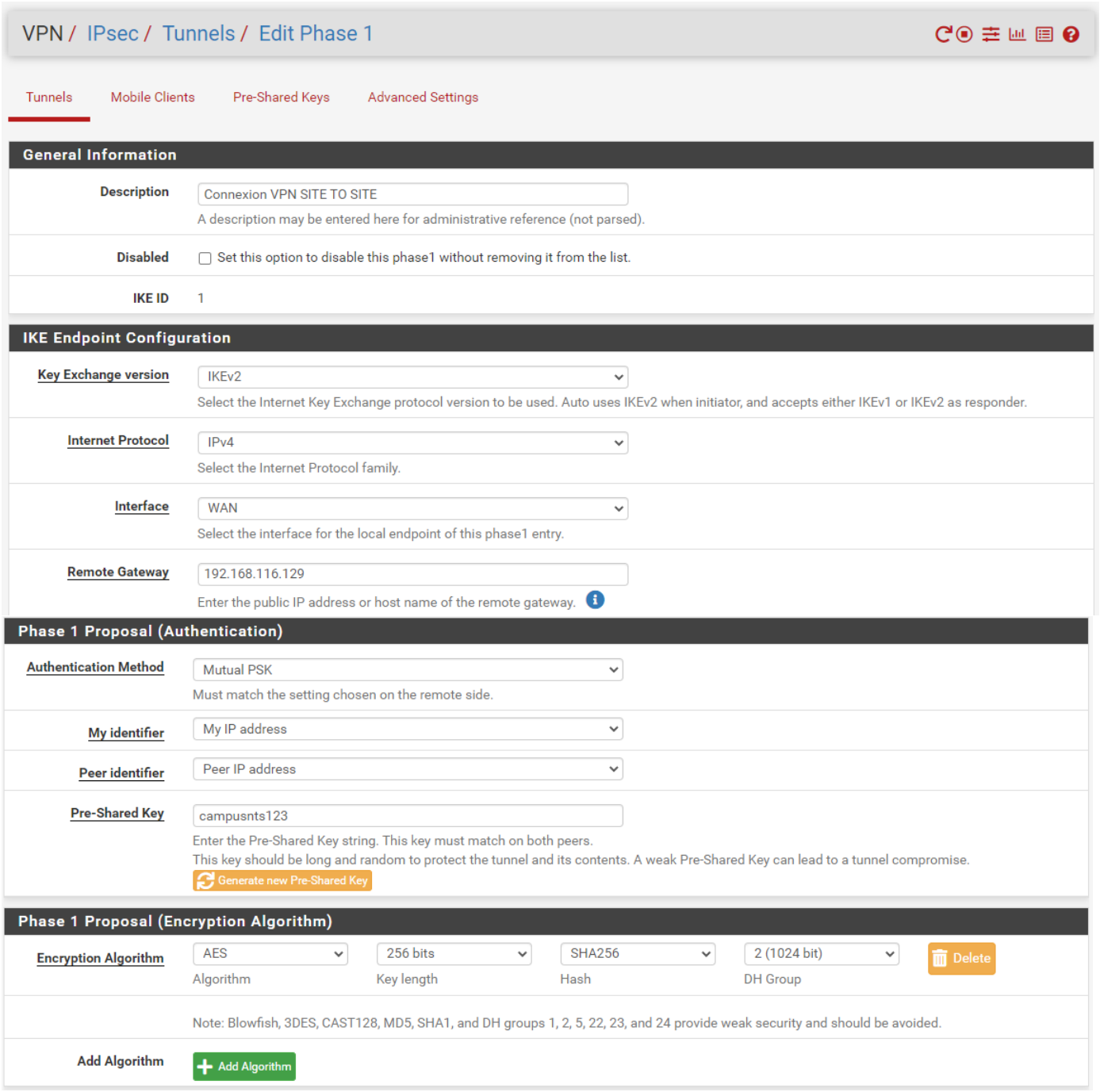


FIGURE 4.26 – Phase 1 : Création de la clé de chiffrement

- **Phase 2** : C'est là que se fait la négociation du chiffrement de tunnel VPN.
  Nous interconnectons les deux vlans de VoIP qui vont éffectuer des communications vocales à travers le tunnel crée. Les données échangées seront chiffrées avec le prtocole ESP qui fournit l'authentification, l'integrité et la confidentialité des données.

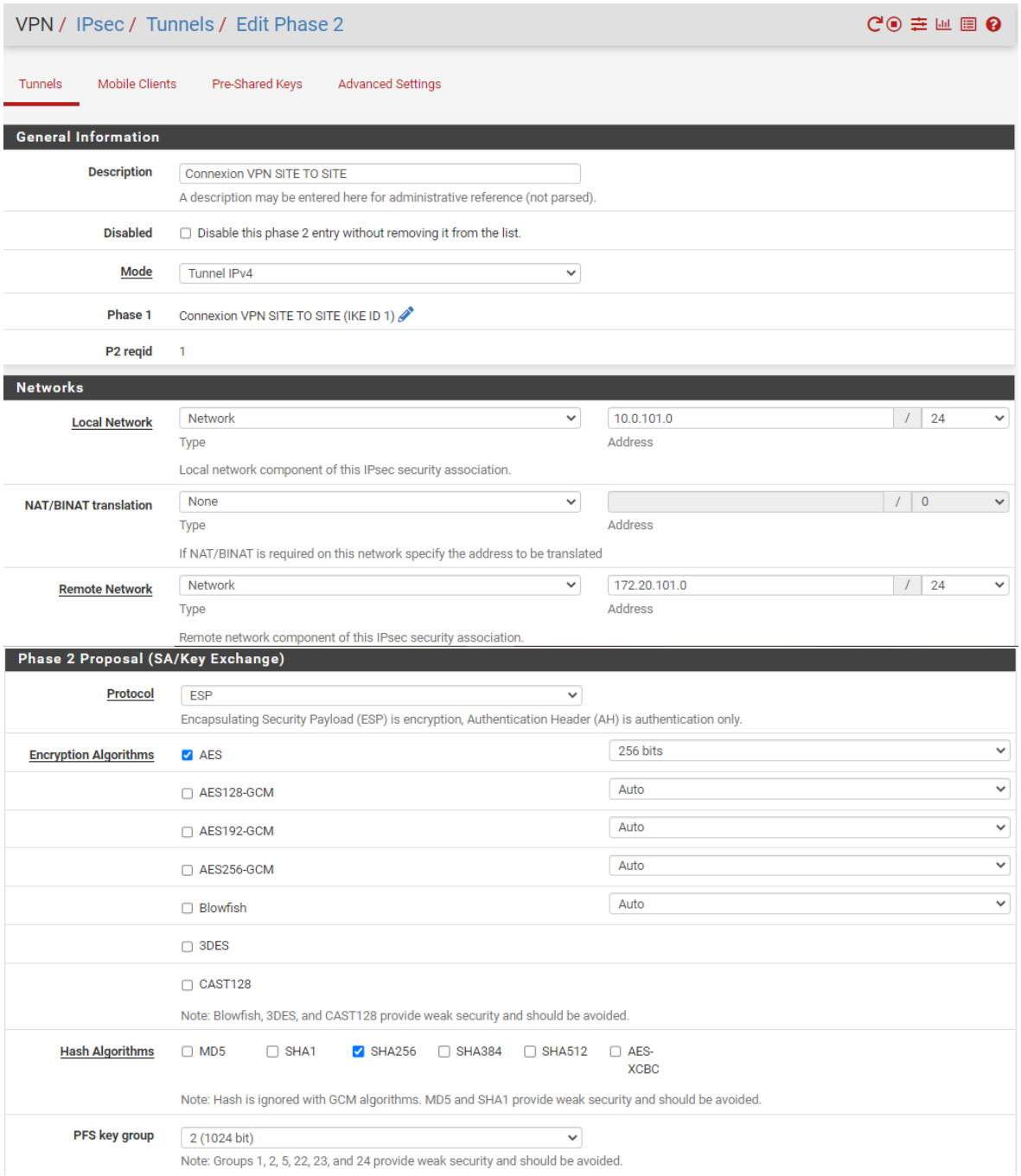


FIGURE 4.27 – Phase 2 : Négociation du chiffrement de tunnel VPN

Les mêmes paramètres doivent être appliqués sur le firewall d'Alger.

Une fois la création du tunnel VPN faite, nous allons autoriser le trafic passant dans ce tunnel entre les deux serveurs.

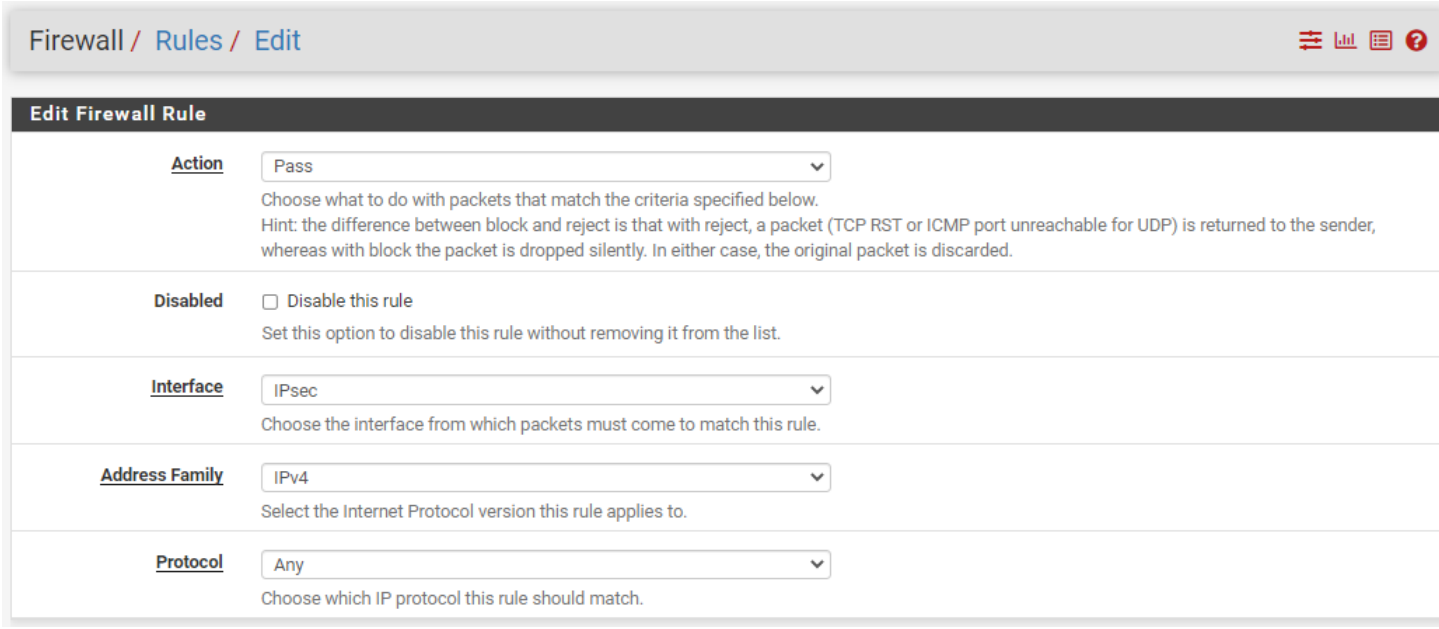


FIGURE 4.28 – Autorisation du trafic dans le tunnel

7.2 VPN client to site

Tout d'abord nous devons créer une autorité de certification interne, dotée de son propre certificat, afin de pouvoir auto-signer les différents certificats créées. Nous aurons besoin de deux certificats en particulier : celui du serveur, qui sera utilisé au niveau du pfSense, et celui du client. Ces certificats seront signés par notre autorité de certification interne que nous allons crée.

7.2.1 Création d'un certificat d'autorité interne

Pour créer un certificat d'autorité, nous allons sur : Système=>Certfificat manager et nous choisissons la méthode "Create an internal certificate authority".

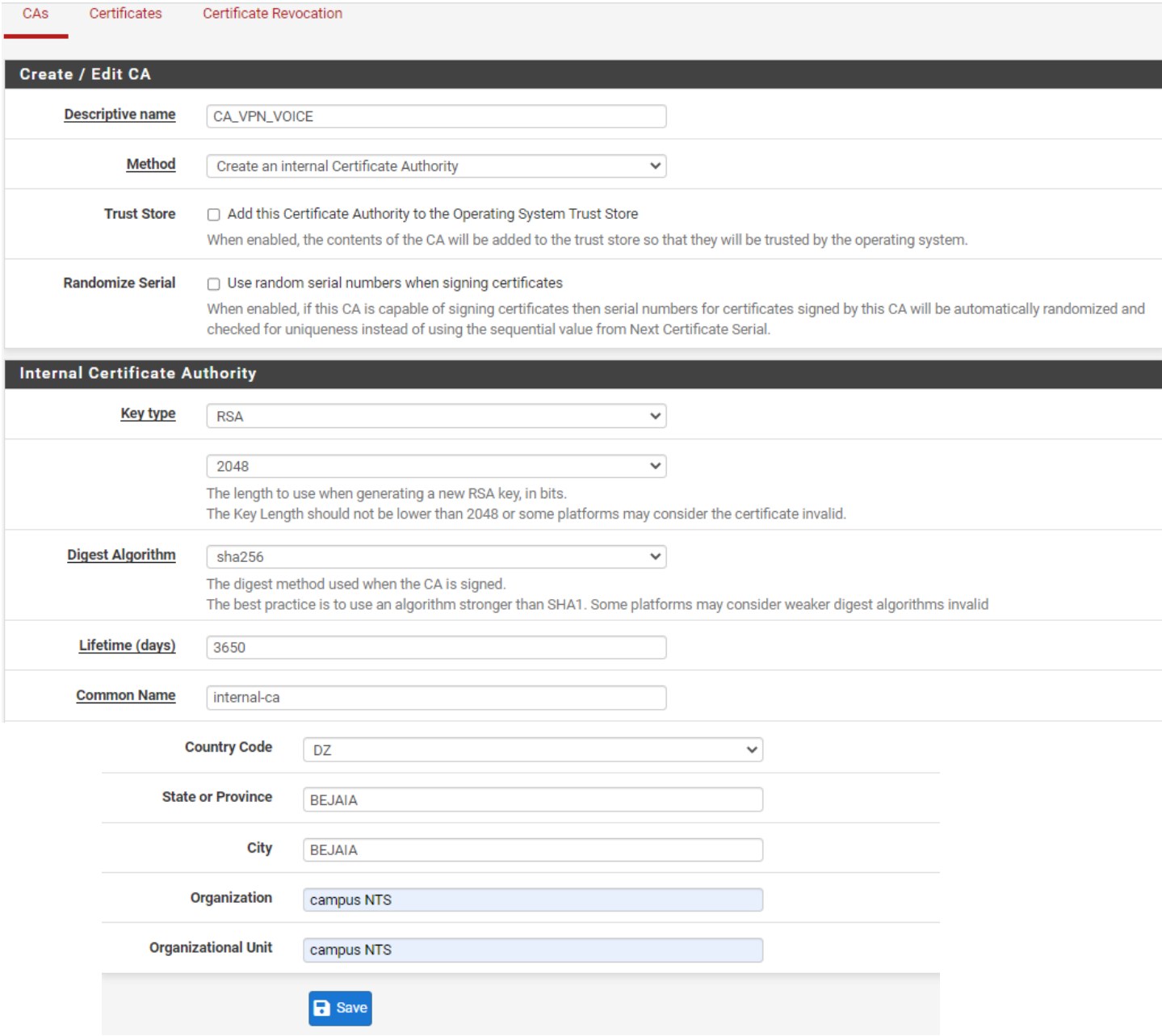


FIGURE 4.29 – Création d'un certificat d'autorité

7.2.2 Création du certificat serveur

Pour créer un certificat serveur, nous allons sur : Système=>Certfificat manager=>Certificates et nous remplissons les champs indiqués sur la figure 4.30 en séléctionnant le type "Server Certificate".

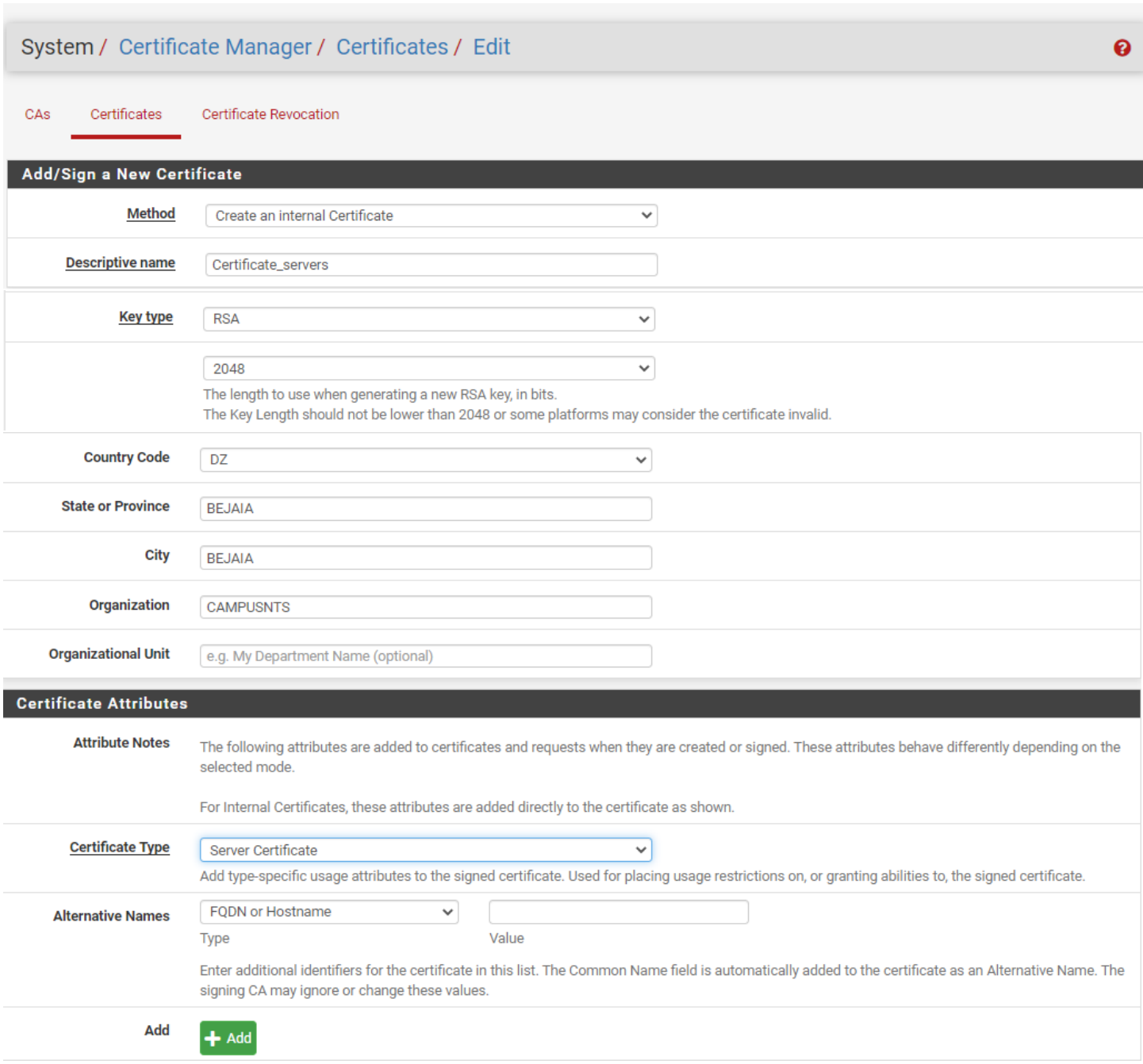


FIGURE 4.30 – Création d'un certificat serveur

7.2.3 Création du certificat OpenVPN

=> Interface sélectionnée : WAN. => Protocole de transport : UDP. => Numéro de port : 1194.

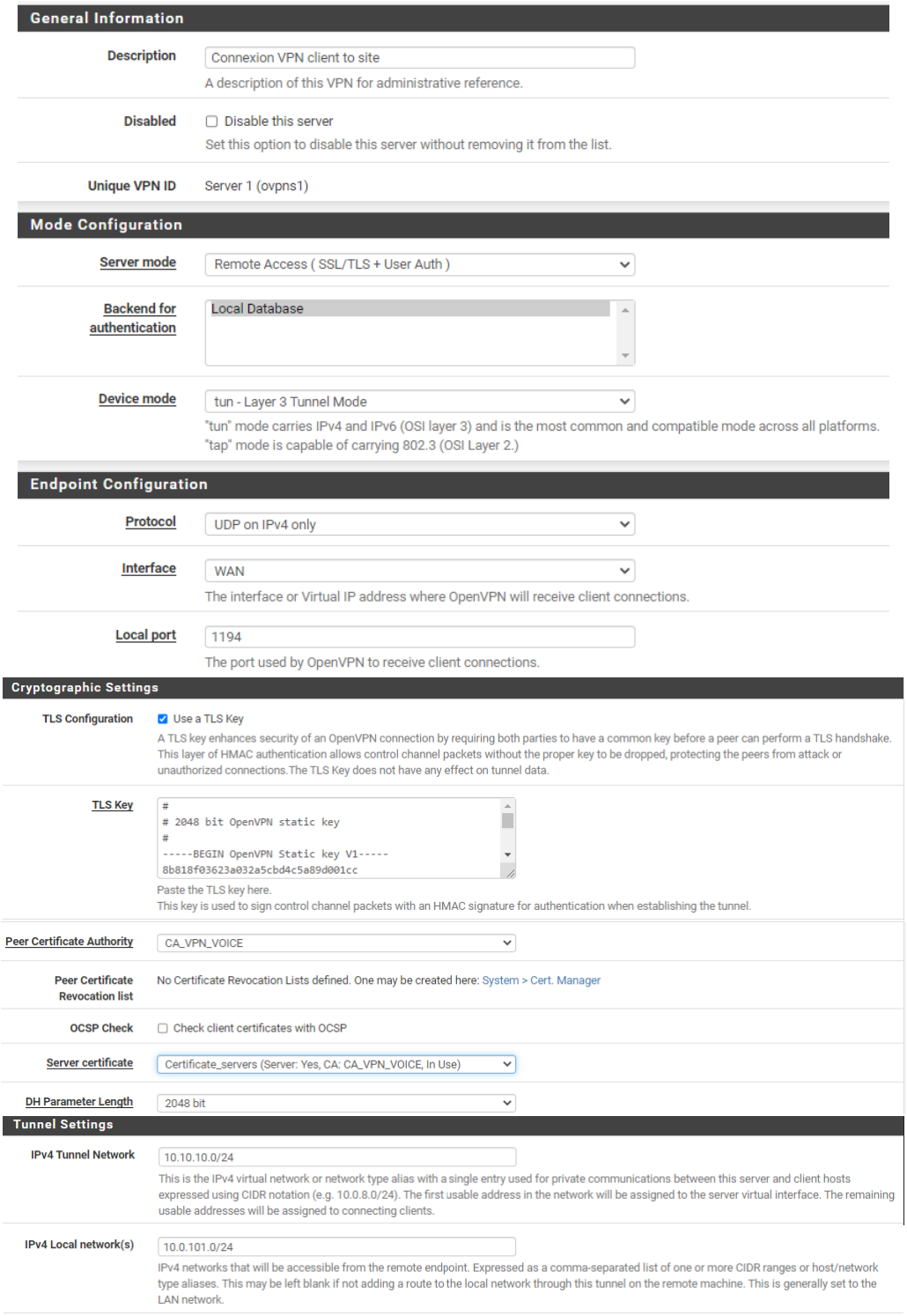


FIGURE 4.31 – Création d'un certificat OpenVPN

7.2.4 Création des utilisateurs

Pour créer un utilisateur autorisé à ce connecter au VPN, nous entrons sur : System=> User manager=> Add user et nous remplissons le formulaire suivant :

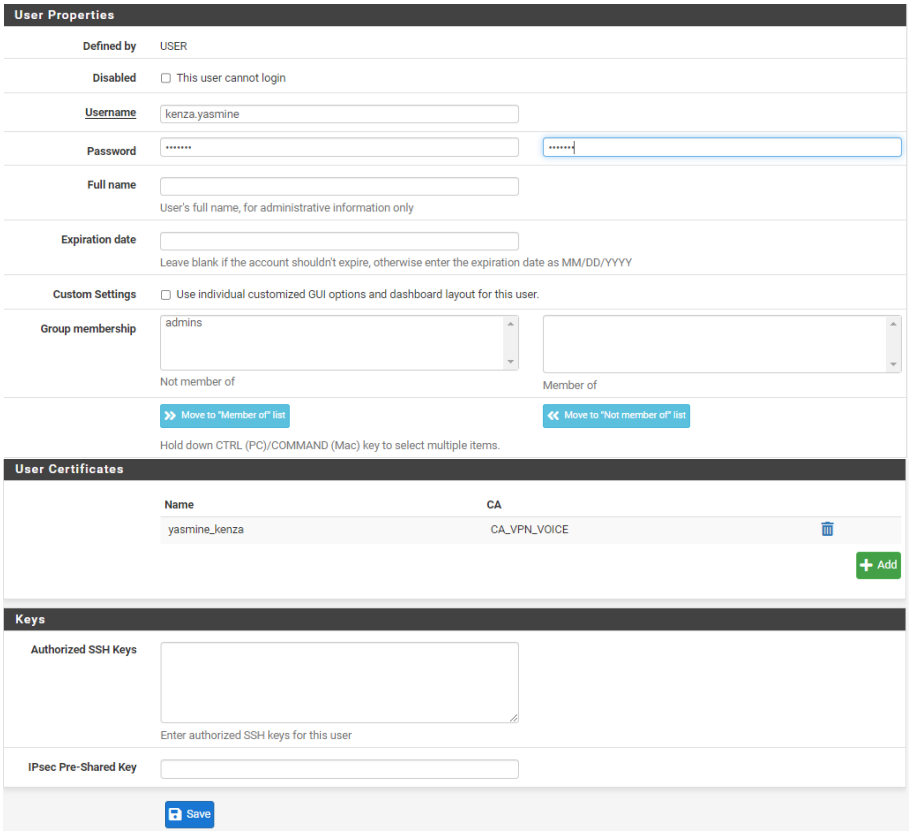


FIGURE 4.32 – Création d'un utilisateur VPN

Pour installer le package Open VPN-client-export utilisé pour exporter les certificats, nous allons sur : System=> Package manager=> Available packages.

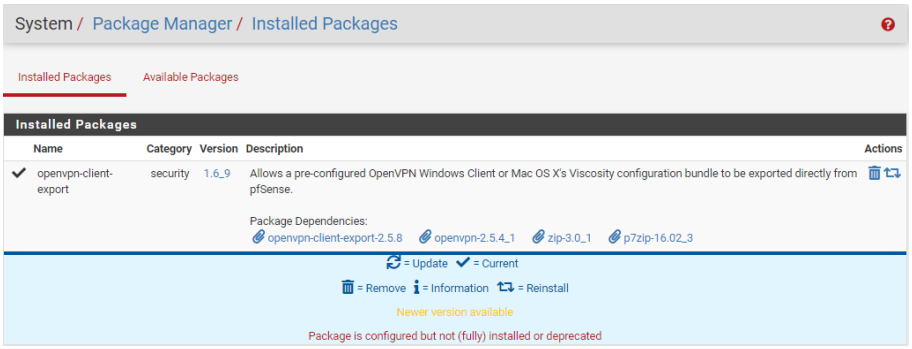
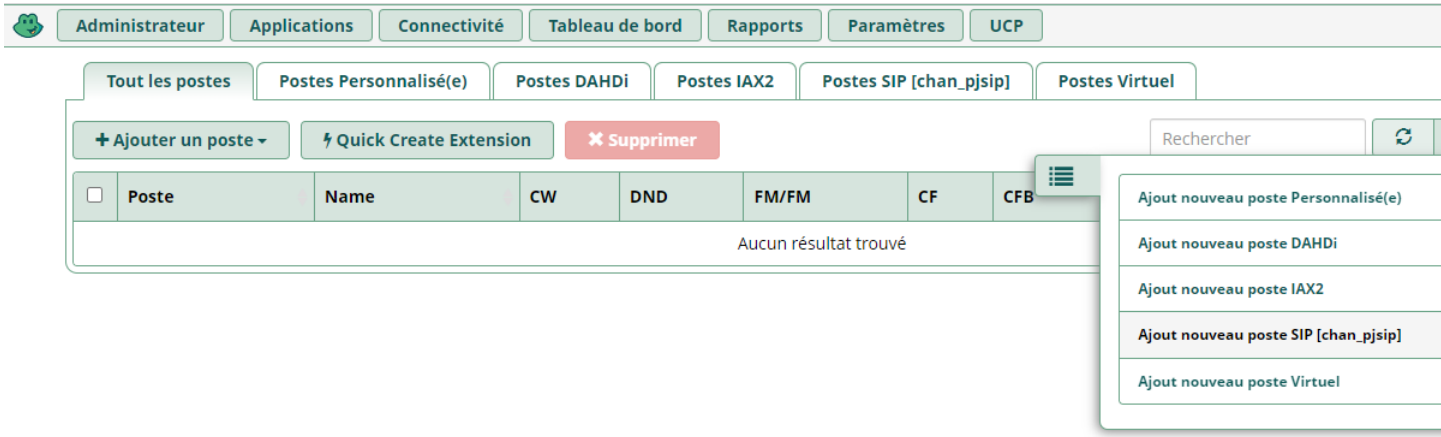


FIGURE 4.33 – Package OpenVPN-client-export

8 Configuration de FreePBX

8.1 Création des comptes SIP

Pour créer un nouveau compte SIP, nous cliquons sur l'onglet "Application" puis "Extension", la fenetre suivante s'affiche :



Nous cliquons sur "Ajout nouveau compte SIP".

Nous remplissons les champs puis nous créons les autres extensions des deux site de la meme manière. Nous avons besoin de deux comptes pour chaque site.

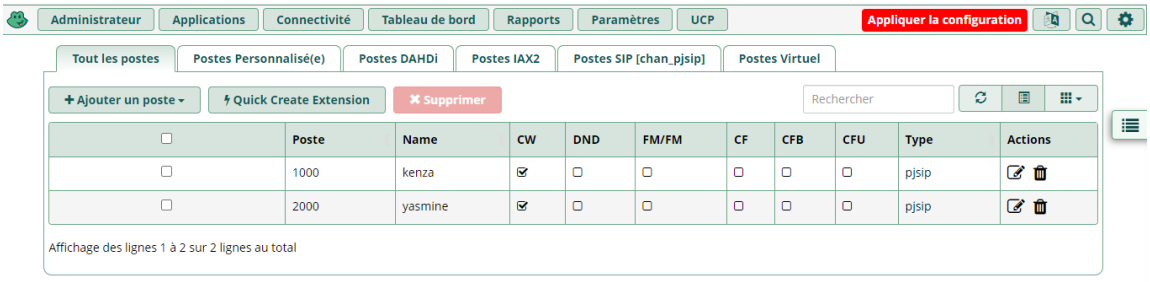


FIGURE 4.34 – Comptes SIP du site Bejaia

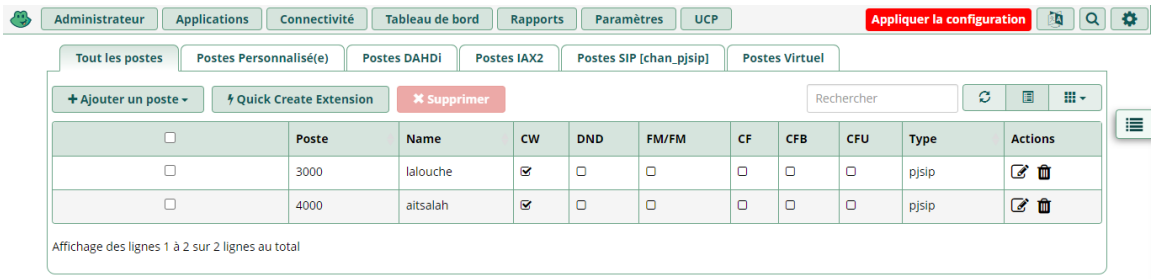
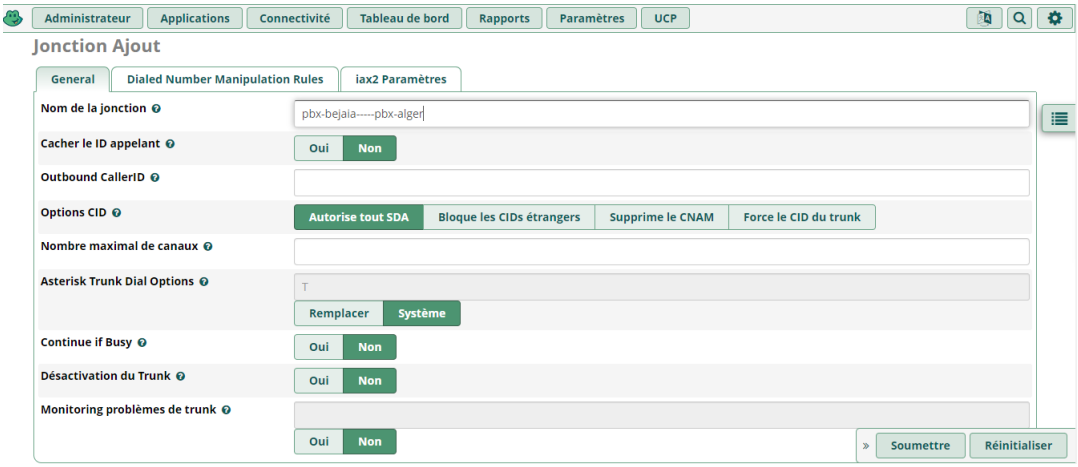


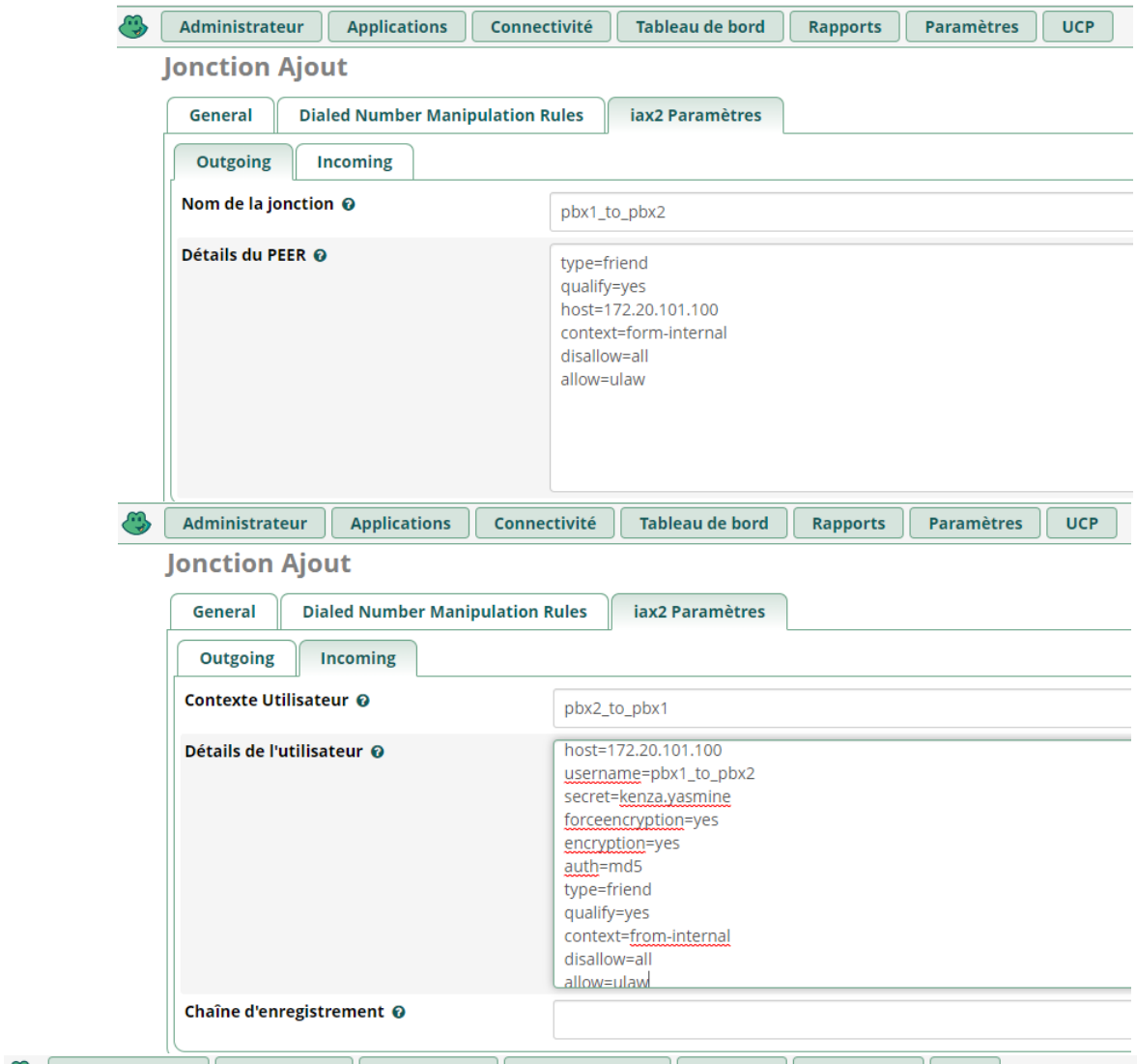
FIGURE 4.35 – Comptes SIP du site Alger

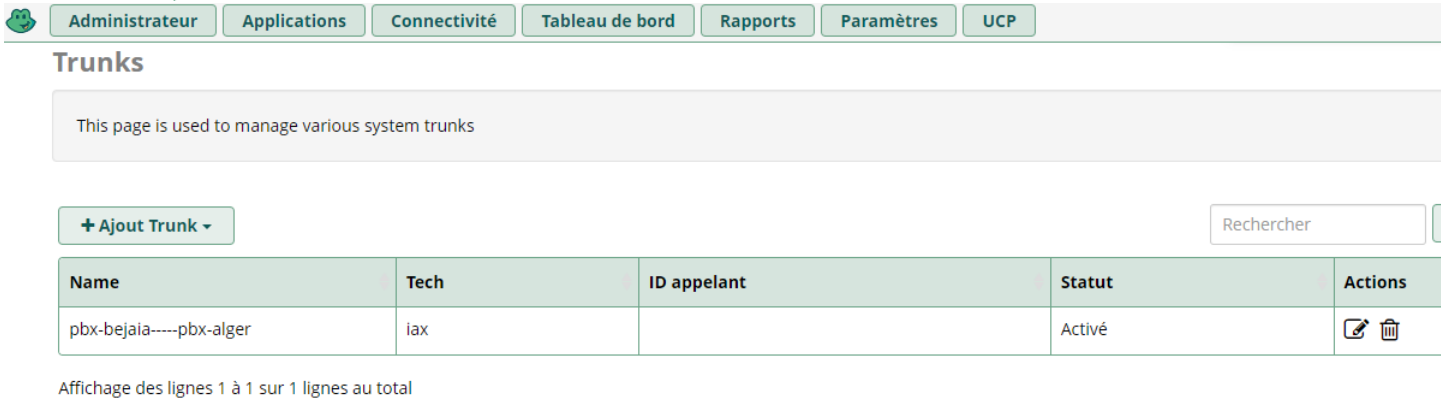
8.2 Interconnexion des deux serveurs VoIP

8.2.1 Configuration des trunks

Un trunk IAX2 est une ligne qui permet de transporter les communications vocales entre les deux sites. Pour configuer un trunk, nous entrons sur l'onglet "Connectivity" => "Trunk" =>"ADD Trunk"=> "IAX2 Trunk".



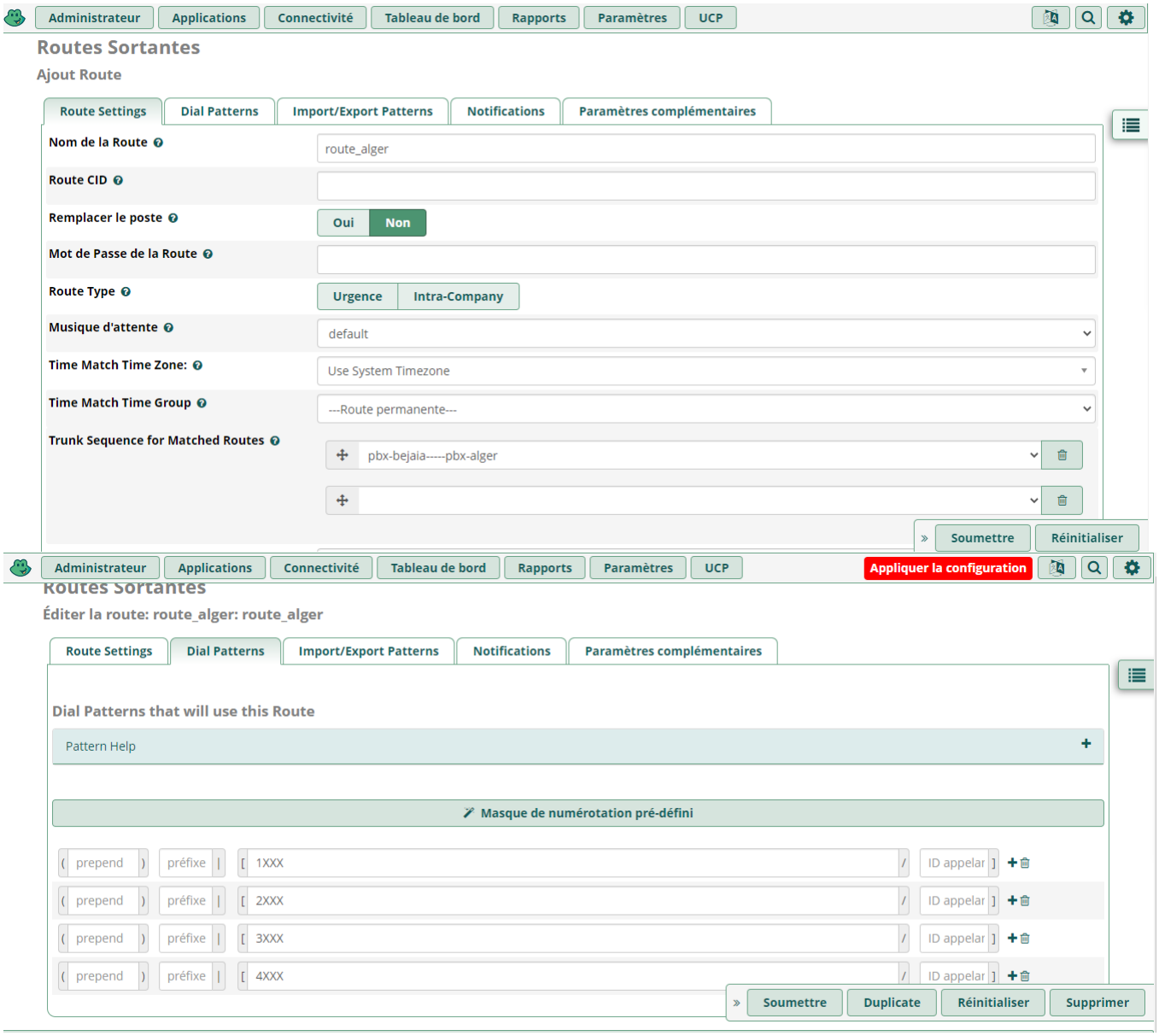




Nous appliquons les memes paramètres pour le site D'alger.

8.2.2 Routage des appels entre les deux serveurs

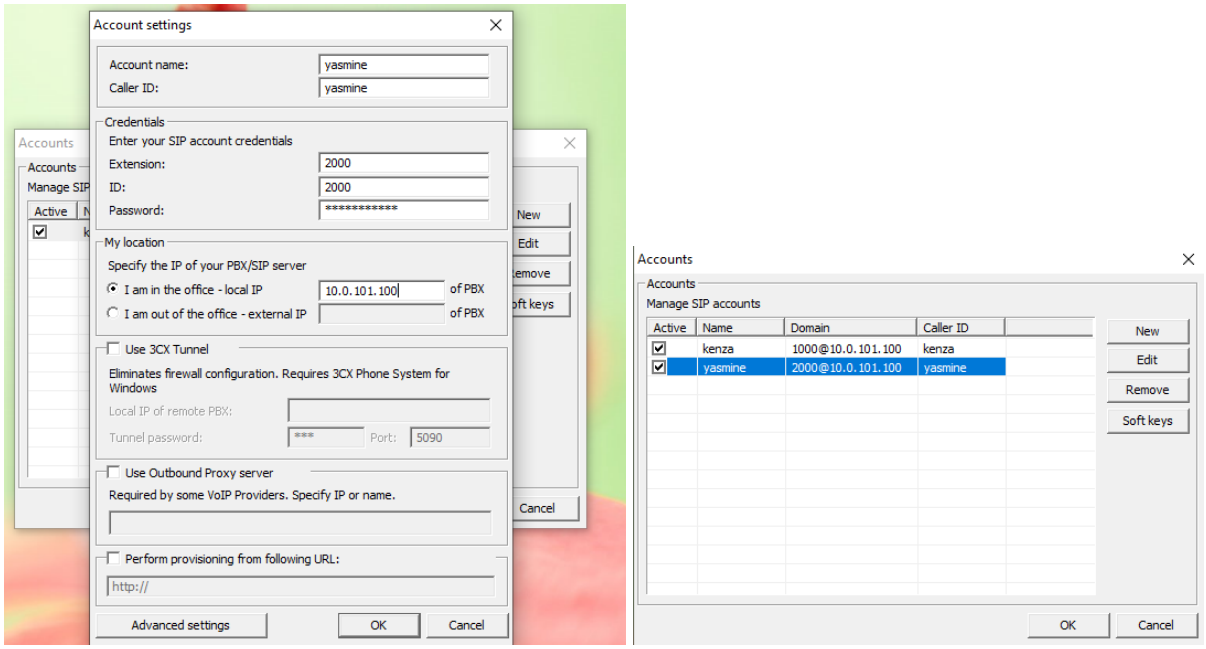
Cette étape permet de créer une route de communication entre les deux sites. Nous sélecionnons le trunk et les comptes SIP déja crées.



Nous créons la meme chose sur le site d'alger.

8.2.3 Création des comptes SIP sur les softphones

Nous allons créer sur les softphones les memes extentions SIP déja crées sur FreePBX afin d'efectuer les appels soit en local ou bien entre les deux sites.



De meme nous créons les aures comptes SIP.

9 Tests

9.1 Interfaces mode trunk

Pour vérifier la configuration des interfaces trunk entre deux switches nous tapons la commande : "Show interfaces trunk"

```
Dist1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et3/2       on               802.1q         trunking      666
Et3/3       on               802.1q         trunking      666
```

9.2 Configuration VTP

Pour vérifier la configuration VTP sur le switch Dist1, nous tapons la commande : "Show vtp status"

```
Dist1#show vtp st
Dist1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : campusnts.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 6-8-23 11:29:23
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 9
Configuration Revision          : 6
MD5 digest                      : 0xCC 0xBB 0xF2 0xF3 0xD2 0x29 0x48 0x90
                                  0x9B 0xD1 0xC4 0xD0 0x20 0x81 0x15 0xCF
```

9.3 Configuration VLANs

Pour vérifier la configuration des vlans, nous tapons la commande : "Show vlan brief"

```
Dist1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/1, Et0/2, Et0/3, Et1/0
                                                Et1/1, Et1/2, Et1/3, Et2/0
                                                Et2/1, Et2/2, Et2/3, Et3/0
100  data                             active
101  ser_voip                         active    Et3/1
102  gestion                          active
666  native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

```
Sw-A#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0
100  data                             active    Et3/2, Et3/3
101  ser_voip                         active
102  gestion                          active
666  native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

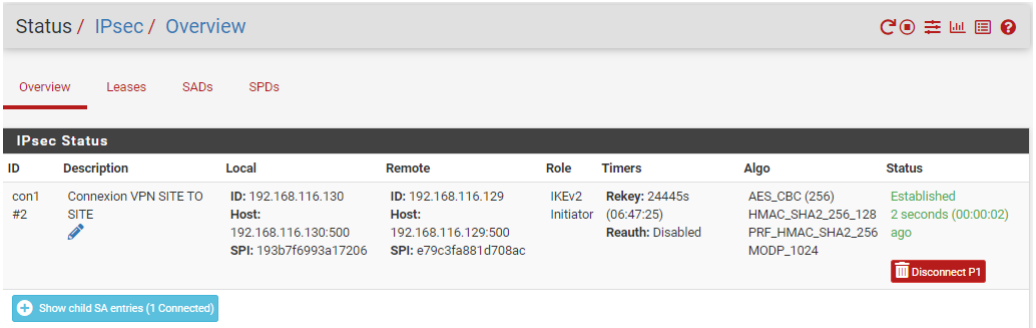
```
Sw-B#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0
100  data                             active
101  ser_voip                         active
102  gestion                          active    Et3/2, Et3/3
666  native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

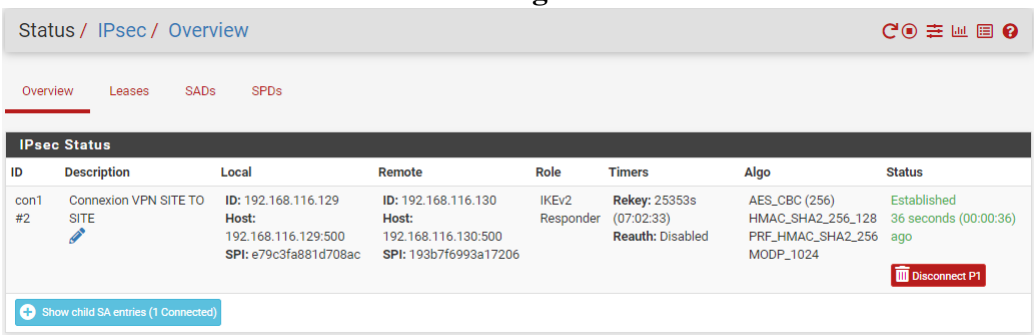
9.4 Vérification du tunel IPSec

Pour vérifier si le tunnel est établi, nous allons sur : Status=> IPsec.
Nous constatons que la connexion VPN est établie entre les deux sites.

Site Bejaia :



Site Alger :



9.5 Tests des configurations FreePBX

9.5.1 Trunks IAX2

Pour vérifier les trunks IAX2, nous entrons sur la CLI asterisk avec la commande "asterisk -r", puis nous tapons la commande "iax2 show peers".
Nous constatons que les trunks sont établis avec succès.

```
[root@pbx-bejaia ~]# asterisk -r
Asterisk 16.25.0, Copyright (C) 1999 - 2021, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 16.25.0 currently running on pbx-bejaia (pid = 2000)
pbx-bejaia*CLI> iax2 show peers
Name/Username    Host                                    Mask
      Port          Status      Description
pbx1_to_pbx2     172.20.101.100                          (S)  255.255.255.255
     4569          OK (18 ms)
pbx2_to_pbx1/pb  172.20.101.100                          (S)  255.255.255.255
     4569      (E)  OK (18 ms)
2 iax2 peers [2 online, 0 offline, 0 unmonitored]
pbx-bejaia*CLI> _
```

9.5.2 Test d'appel en locale (Site Bejaia)

Les deux figures suivante montrent que l'appel entre deux comptes SIP du meme site (en local) est effectué avec succès.

9.5.3 Test d'appel entre les deux sites

La figure suivante montre que l'appel entre deux comptes SIP, un de Bejaia et l'autre d'Alger, est établi avec succès, ce qui signifie que les deux serveurs de VoIP sont bien interconnectés.

Conclusion

Ce chapitre est divisé en deux parties, dans la première nous avons présenté l'entreprise "Campus NTS" qui nous a accueillie en stage , et dans la deuxième nous avons présenté la phase réalisation de notre projet en présentant la solution mise en place, la démarche de travail, les configurations et les implémentations effectuées, et enfin les tests qui ont montré le succès de notre solution.

Conclusion générale

Le VPN, en tant que technologie en plein essor, joue un rôle crucial dans l'interconnexion des sites. Il dépasse le simple statut de nécessité économique pour les entreprises, car il offre un accès distant sécurisé. Cette solution présente de multiples avantages, notamment sa simplicité d'installation et sa transparence pour les utilisateurs. De plus, elle permet l'intégration de divers services tels que la voix sur IP.

Grâce à la technologie VoIP, les entreprises peuvent communiquer via un unique protocole IP. C'est pourquoi elles choisissent cette solution, dans le but de réduire leurs dépenses et d'optimiser leur système d'information.

En outre, la voix sur IP (VOIP) englobe un ensemble de fonctionnalités qui vont au-delà de la simple transmission vocale. Par conséquent, notre objectif est de mener une étude approfondie pour identifier les différentes solutions et techniques disponibles, en prenant en compte l'infrastructure existante au sein de l'entreprise Campus NTS.

Campus NTS dispose de deux sites distants, chacun ayant une architecture téléphonique et informatique distincte, ce qui pose des problèmes en termes de communications entre ces deux sites. Pour résoudre cette situation, nous avons proposé d'intégrer VoIP au sein de cette entreprise en mettant en place deux serveurs PBX pour chaque site pour unifier le réseau et améliorer le système des communications, en plus de la création des VLANs et la mise en place d'un VPN pour assurer la sécurité de ces communications. Cette solution permettra de créer un environnement cohérent et harmonisé, tout en facilitant les échanges entre les différents sites de l'entreprise.

Nous avons procédé à des tests de notre solution en utilisant un tunnel VPN IPsec entre les deux sites Alger et Bejaia. Ces tests ont confirmé la faisabilité de l'implémentation de cette solution pour résoudre notre problème principal.

La réalisation de ce projet nous a offert l'opportunité d'acquérir de nouvelles connaissances sur les protocoles de la VoIP, tels que le protocole SIP et IAX, ainsi que sur les protocoles de sécurité. Nous avons approfondi notre compréhension de leur fonctionnement et de leurs principes grâce à une étude détaillée. En termes de perspectives, la prochaine étape consistera à passer à l'application concrète de ces connaissances. Il serait également intéressant d'étendre cette étude à d'autres entreprises, afin de partager notre expérience et de contribuer à l'avancement de ce domaine.

Bibliographie

[1] JF. PILLOU, Fabrice LEMAINAQUE, *Tout sur les réseaux et internet*, 3eme édition Dunod, 2012.

[2] G. PUJOLLE, *Initiation aux réseaux*, Édition Eyrolles, 2014.

[3] P.ATELIN, *Réseaux informatique notion fondamental*, 3eme édition ENI, 2009.

[4] JF.PILLOU, *Tout sur les systèmes d'information*, Dunod, 2006.

[5] JF. PILLOU, JF.BAY, *Tout sur la sécurité informatique*, 4eme édition Dunod, 2016.

[6] DA CUNHA José, VoIP et Asterisk/Trixbox, métrise en systèmes distribués et réseaux, Université de Franche Comté, 2007-2008.

[7] L. OUAKIL, G. PUJOLLE, *Téléphonie sur IP*, 2eme édition Eyrolles.

[8] G. PUJOLLE, *Les Réseaux*, Édition Eyrolles, 2003.

[9] Ahmed Aouadi, Mise en place d'une solution open Source VoIP et Visioconférence multi-sites sécurisée,Université Virtuelle de Tunis ,mémoire de fin d'étude, juillet 2015.

[10] J. OTT, S. WENGER, N. SATO, et all. Extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF). 2006.

[11] La norme RFC 5456 de l'IETF définissant les caractéristiques du protocole IAX version 2.

[12] Eric BAHATI - SHABANI , MISE EN PLACE D'UN RESEAU VPN AU SEIN D'UNE ENTREPRISE, Institut supérieur de commerce Kinshasa , Mémoire de Fin d'Etudes, 2011.

[13] Rahmani Tinhinan, Sadaoui Fadhila, Etude et mise en place d'un réseau VPN, Mémoire de fin d'étude, UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU, 2016/2017.

[14] Jacob NDWO MAYELE , Déploiement d'un coeur de réseau ip/mpls, cas de la banque centrale du congo,Université de kinshasa, 2017.

[15] ipsec(internet protocole security) , Centre Universitaire Nour Bachir , 2019-2020.

[16] Génael VALET, Les LANs virtuels, Greta industriel de technologies avancées, 2007.

[17] « Commutation et routage intermédiaire », CCNA 3 – Essentiel.

[18] Nadia BATTAT, Les systèmes de sécurité, cours Sécurité des infrastructures de télécommunication, Université A/Mira Bejaia, 2022-2023.

Webographie

[19] https ://bits-genius.com/topologie-reseau/, consulté le 21/06/2023

[20] https ://www.frameip.com/voip/, consulté le 21/06/2023

[21] https ://wikimemoires.net/2011/03/architecture-et-mode-access-de-la-telephonie-sur-ip/, consulté le 21/06/2023

[22] https ://www.gl.com/newsletter/barer-independent-call-control-bicc-protocol-emulator-newsletter.html, consulté le 21/06/2023

[23] https ://www.frameip.com/voip/#7_-_Probleme_et_Qos/, consulté le 21/06/2023

[24] https ://www.rapport-gratuit.com/vulnerabilites-contre-la-voip/, consulté le 21/06/2023

[25] https ://www.oracle.com/fr/cloud/definition-machine-virtuelle-vm/, consulté le 08/07/2023

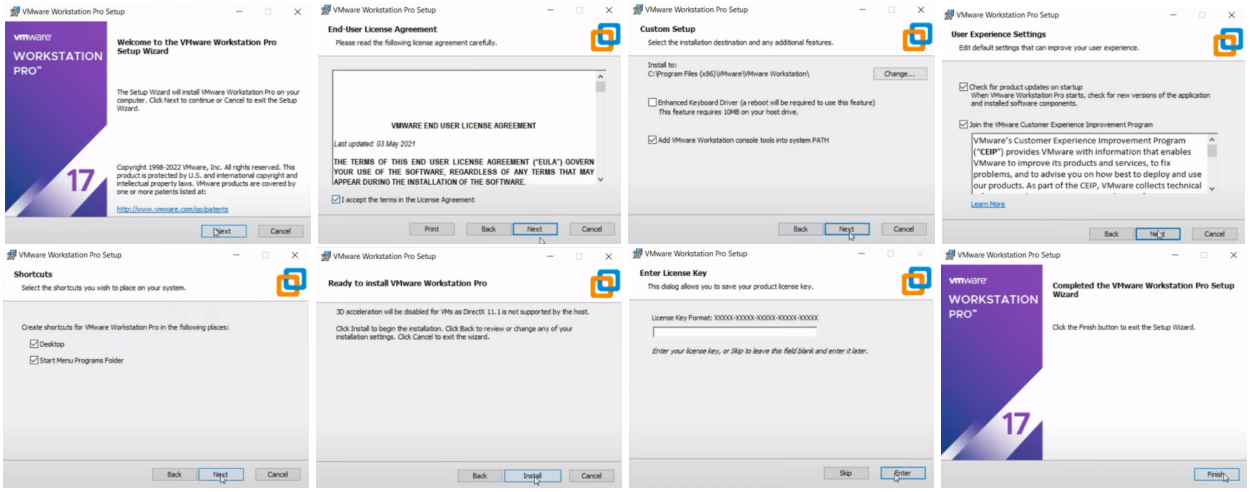
[26] https ://www.certilience.fr, consulté le 08/07/2023

[27] https ://sip.goffinet.org/asterisk/uc-solution-freepbx/, consulté le 08/07/2023

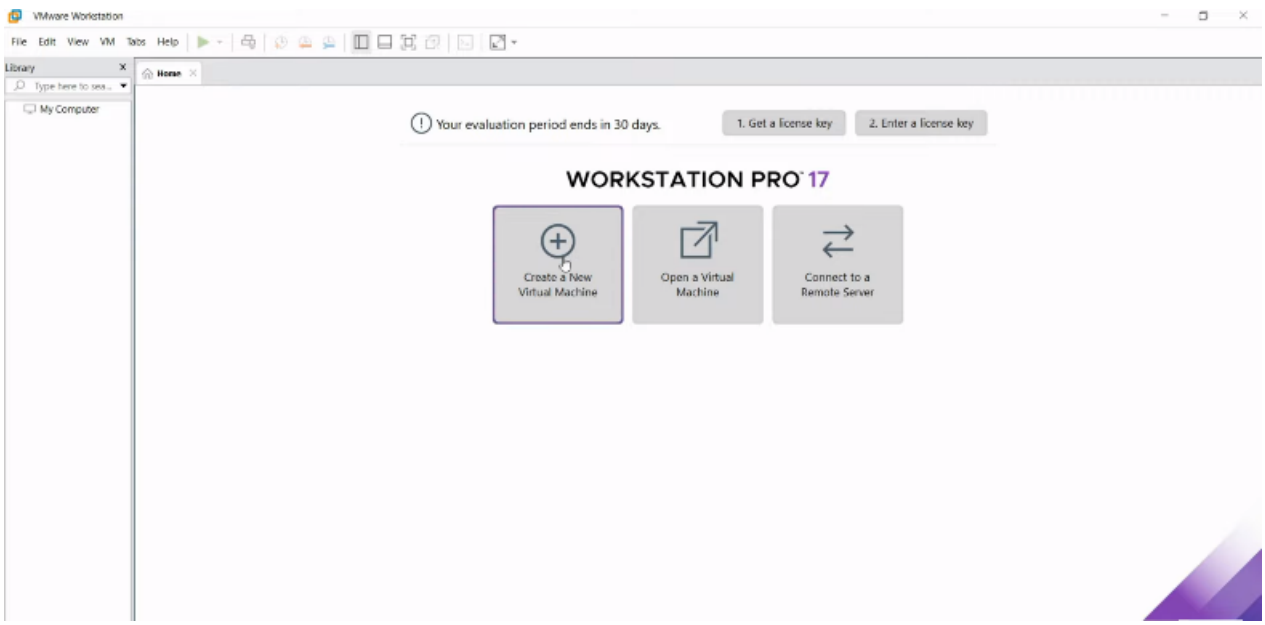
[28] https ://www.lalanguefrancaise.com/dictionnaire/definition/softphone, consulté le 08/07/2023

Annexe

A Installation de VMware Workstation 17

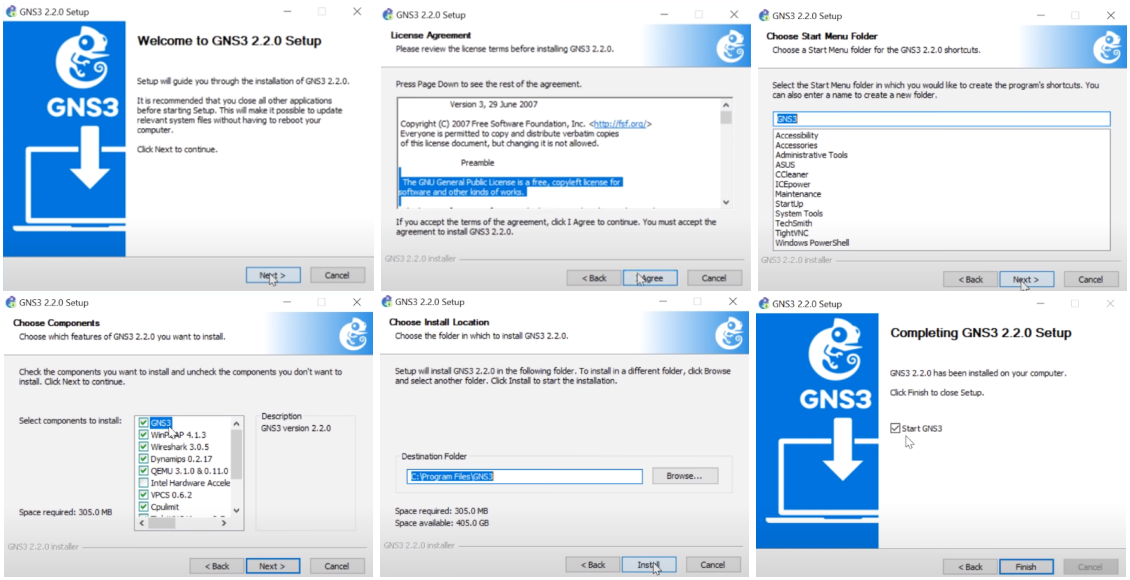


A la fin de l'installation, l'interface de VMware s'affiche :

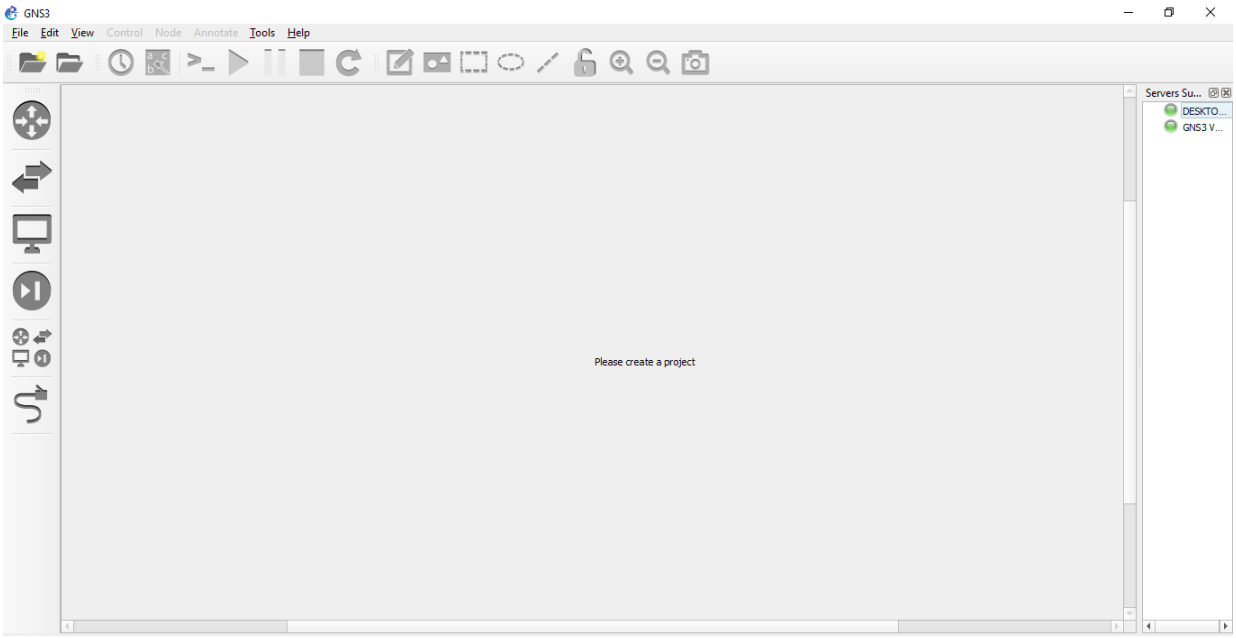


B Installation de GNS3

Vous pouvez télécharger GNS3 gratuitement sur le site `www.gns3.com`

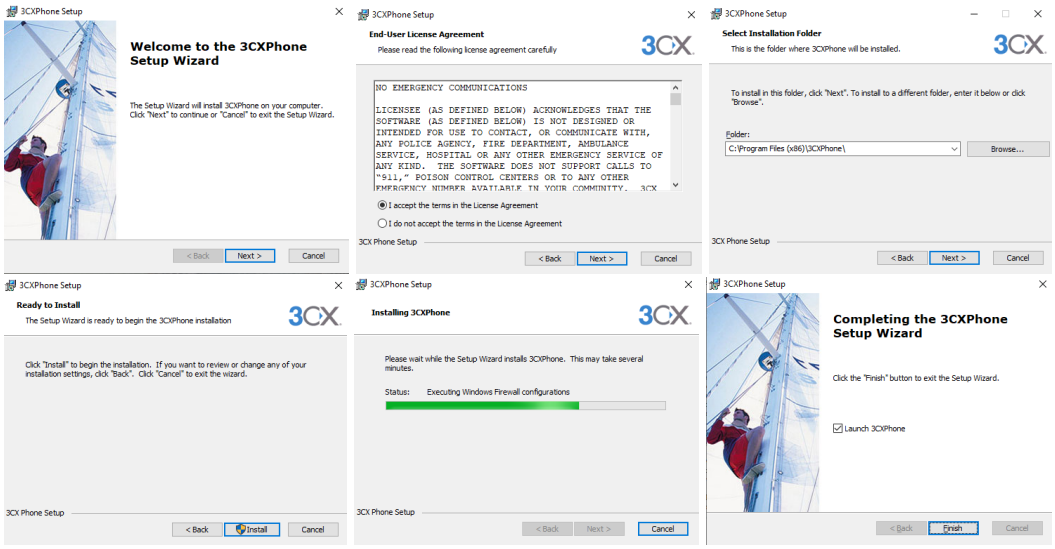


A la fin de l'installation, l'interface de GNS3 s'affiche :

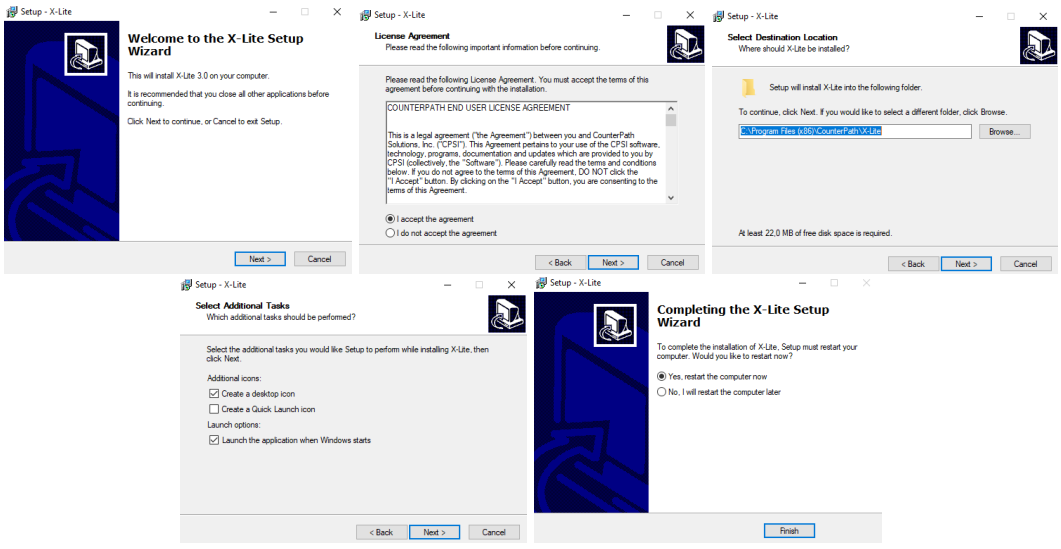


C Installation des softphones

a 3CX sofphone



b X-Lite



Résumé

La voix sur IP (VoIP) est une technologie qui s'impose progressivement dans tous les secteurs. C'est une bonne solution pour les entreprises en matière d'intégration, de fiabilité, d'évolutivité et de coûts. Cependant, en étant une nouvelle technologie, l'implémentation de la VoIP peut exposer le réseau de l'entreprise à plusieurs attaques. Pour cela, la sécurité du réseau VoIP n'est pas seulement une nécessité mais plutôt une obligation. Dans ce contexte, nous avons implémenté une solution VoIP au sein de l'entreprise Campus NTS en mettant en place et interconnectant deux serveurs PBX et en créant trois VLANs (data, gestion et voix) dans ses deux sites distants (Bejaia et Alger), pour améliorer les communications entre les personnels de l'entreprise en utilisant les deux protocoles de signalisation SIP et IAX. Cette solution est sécurisée par un canal VPN IPsec qui permet de chiffrer les données vocales échangées entre les deux sites distants avec le protocole ESP, garantissant ainsi la confidentialité et l'intégrité des informations.

Mots clés : VoIP, Sécurité, Campus NTS, PBX, VLAN, SIP, IAX, VPN IPSec, ESP.

Abstract

VoIP is a technology that is gradually taking hold in all sectors. It is a good solution for businesses in terms of integration, reliability, scalability and cost. However, being a new technology, the implementation of VoIP can expose the corporate network to several attacks. For this, the security of the VoIP network is not only a necessity but rather an obligation. In this context, we implemented a VoIP solution within the Campus NTS company by setting up and interconnecting two PBX servers and creating three VLANs (data, management end voice) in its two remote sites (Bejaia and Algiers), to improve communications between the company's personnel by using both SIP and IAX signaling protocols. This solution is secured by an IPsec VPN channel which encrypts the voice data exchanged between the two remote sites with the ESP protocol, thus guaranteeing the confidentiality and integrity of the information.

Key words : VoIP, Security, Campus NTS, PBX, VLAN, SIP, IAX, VPN IPSec, ESP.