République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira Bejaïa

Faculté de Technologie

Département de Génie électrique

Mémoire de Fin d'Etudes

Spécialité : Réseaux et télécommunications

Filière :Télécommunications

Thème

Etude et implémentation d'une architecture réseau pour SONATRACH-Bejaia

Présenter *par :*

HAMADOUCHE CYLIA

KABLI INES

Encadré par

M.AZNI

Devant jury

Mme. Hamzaoui

Mme. Gagaoua

Année Universitaire: 2020/2021

Dédicace

On a le plaisir de dédier ce travail reflétant notre effort consenti durant le cursus universitaire à :

Nos chers parents, pour lesquels nulle dédicace ne peut exprimer nos sincères sentiments, pour leur patience illimitée, leurs encouragements continus, leur aide, en témoignage de nos profond amour et respect pour leurs grands sacrifices.

A mon père, mon premier encadreur, depuis ma naissance

Que la terre lui soit légère et que son âme repose en paix (Ines Kabli)

A ma mère qui m'a toujours encourager dans mes étude et ma toujours apporter son amour son soutien infaillible

A mon chers frères et sœurs pour leur grand amour et leur soutien; qu'ils trouvent ici l'expression de notre haute gratitude.

A mon père (Hamadouche ABDELAH), mon premier encadreur, depuis ma naissance ;

A ma très chère mère : quelle trouve ici l'hommage de ma gratitude qui, si

Grande quelle puisse être ne sera à la hauteur de ses sacrifices et ses prières

Pour moi ;

A mes deux frère à qui je souhaite beaucoup de réussite et

De bonheur ;

A Toutes nos familles sans exception, à tous nos chers amis(e) pour leurs encouragements, et à tous ceux qu'on aime.

A tous nos enseignants. A tous le personnel du département Génie Electrique.

A toutes les personnes qui nous ont apporté de l'aide.

Remerciements

Nous remercions avant toute chose dieu le tout puissant qui a guidé nos pas pour l’accomplissement de ce modeste travail. Nous tenons aussi à remercier et à exprimer notre profonde gratitude à Mr« Azni », notre promoteur de nous avoir fait confiance durant le projet. Nous adressons aussi nos remerciements au président et aux membres du jury qui nous font honneur en acceptant de juger notre travail. Notre reconnaissance s’adresse à nos familles qui ont su nous apporter, sans relâche, leurs soutiens durant toutes ces longues années d’études. Enfin que tous ceux qui, de près ou de loin ont contribué à l’aboutissement de ce travail soient assurés de nos profondes gratitudes.

Sommaire

Table des figures

La liste des tableaux

Liste des abréviations

AVG : Active Virtual Gateway

AVF : Active Virtual Forwarder

B: Béjaïa

DHCP : Dynamic Host Configuration Protocol

D: Mesdar

D: Dédoublement

E: Expansion

EM: Enrico Mattei

EIGRP: Enhanced Interior Gateway Routing Protocol

FHRP: First Hop Redundancy Protocol

GLBP: Gateway Load Balancing Protocol

G: Gaz / Gazoduc

HSRP: Host Standby Router Protocol

HEH: Haoud-El- Hamra

IP: Internet Protocol

G: Alger

K: Skikda

LACP: Link Agregation Control Protocol

LAN : Local Area Network

L: GPL / Oléoduc

N: Condensat / Oléoduc

O:Pétrole brut / Oléoduc

OSPF: Open Shortest Path First

O: OuedSafSaf

PAGP: Port Agregation Protocol

PDF: Pedro Duran Farel

PABX: Private Automatic Branch eXchange)

RIP: Routing Information Protocol

R: Hassi R'mel

SSH: Secure Shell

STP: Spanning Tree Protocol

Telnet: Terminal Network

T: Tunisie

TMB: Terminal Marin Bejaia

UDP: User Datagram Protocol

VTP: VLAN Trunking Protocol

VPN: Virtual Private Network

VRRP: Virtual Router Redundancy Protocol

WAN: Wide Area Network

Z: Arzew

INTRODUCTION GÉNÉRALE

Aujourd'hui, le monde se développe avec la technologie et surtout dans le domaine de télécommunication où l'entreprise quelle que soit sa taille, pour un but de rapidité, fiabilité et accès à distance doit se munir d'un outil capable de traiter les données et d'informatiser son système afin de l'améliorer.

Ces outils ne sont rien d'autres que les ordinateurs interconnectés en vus d'échanger et de partager les données, avoir l'accès à distance, ce qui est très indispensable pour la modernisation et le développement d'une entreprise, et aussi avoir une gestion plus centralisée et un accès plus rapide à l'information convoitée. À cet effet, la mise en place d'une infrastructure réseau comportant un service d'annuaire géré par un ou plusieurs contrôleurs de domaines devient une nécessité dans la mesure où les données, les utilisateurs et les accès utilisateurs à ces données seront gérés en parallèle.

Un domaine dans les services d'annuaire regroupe un ensemble d'ordinateurs offrant une infrastructure pour la gestion des utilisateurs, groupes et ordinateurs du réseau qui partagent une base de données d'annuaires centralisée cette dernière reprend les comptes d'utilisateurs et les informations de sécurité spécifique au domaine. La gestion des différents domaines est basée sur le service d'annuaire Active directory(AD).

C'est dans ce contexte, au cours du stage effectué au niveau de l'entreprise de la région transport Bejaia, on a été appelé à concevoir et à mettre en œuvre un réseau local avec une architecture réseau conforme, dans le but de permettre une gestion plus optimale que possible des ressources de l'entreprise.

Pendant le stage, il a été question de répondre aux exigences de l'entreprise en termes de services rendus, donc le choix s'est porté sur un réseau local, dont l'architecture est une architecture client/serveur où toutes les applications, informations et données de l'entreprise seront stockées sur des machines dites serveurs et un service d'annuaire Active Directory de la famille Windows Server. Active directory comprend plusieurs services; à savoir, identité, certificats et gestion numérique des droits, il permet aux administrateurs réseaux de gérer centralement les ordinateurs interconnectés, tout en offrant une infrastructure permettant d'héberger différents services. Le choix du système d'exploitation des serveurs s'est porté sur Windows server 2016 de Microsoft pour sa convivialité, son niveau de sécurité et sa flexibilité.

L'objectif du travail est de mettre en place une infrastructure informatique pour L'administration et la sécurité du réseau local de La SONATRACH Bejaia où nous commencerons par faire une synthèse de l'état de l'art des technologies utilisées puis nous allons tenter d'apporter des solutions aux problèmes et lacunes recensées et cela en procédant à la concrétisation des solutions proposées à savoir :

- La création des contrôleurs de domaines, des ordinateurs et des utilisateurs ainsi que desStratégies de groupes
- La mise en place d'une infrastructure de clés publique
- Installation du serveur de base de données;
- La mise en place d'un serveur de voix ASTERISK ;
- La sécurisation du réseau et le filtrage web avec une solution pare-feu ;
- Connexion aux sites distants à l'aide de tunnels VPN.

Pour cela, ce présent mémoire est subdivisé en quatre chapitres, le premier sera consacré sur la présentation de l'organisme d'accueil à donner quelques notions de base et généralités sur les technologies qui seront utilisées tout au long de ce travail.

Le second chapitre concerne l'étude du réseau local existant dans le but de proposer d'éventuelles améliorations, ainsi qu'à la présentation de la nouvelle architecture à suivre.

Le troisième chapitre décrit les différents outils nécessaires à la mise en œuvre de l'infrastructure Active Directory, suivi par la configuration et la mise en œuvre des solutions proposées en commençant par la mise en place et le paramétrage des contrôleurs de domaines sous Windows Server 2016, la mise en place des serveurs de bases de données ainsi que le serveur ASTERISK, pour finir, nous procèderons à la sécurisation du réseau avec le pare-feu pfSense ainsi que la configuration des liaisons VPN avec les sites distants

Introduction

L'étude de l'organisme d'accueil est une étape importante qui sert à représenter les contraintes sous lesquelles se réalisera notre projet. Dans ce chapitre, nous allons présenter l'entreprise SONATRACH, citer les déférents départements qui la constituent et donner quelques informations qui nous seront utiles dans notre travail.

I.1 Présentation de l'entreprise

SONATRACH est la compagnie nationale algérienne de recherche, d'exploitation, de transport par canalisations, de transformation et de commercialisation des hydrocarbures et de leurs dérivées, elle est Créée au lendemain de l'indépendance le 31 décembre 1963.

Le groupe pétrolier et gazier SONATRACH est compagnie nationale algérienne d'envergure internationale dont le nom est une abréviation de SOciété NAtionale de TRAnsport et de Commercialisation des Hydrocarbures.

Fleuron de l'Algérie indépendante, SONATRACH, de par son envergure et son domaine d'activité, a été le long de son histoire intimement liée au destin de l'Algérie. Etablie comme entreprise nationale par excellence suite à la nationalisation des hydrocarbures le 24 février 1971, elle a toujours été dans une dialectique féconde avec les différentes phases du développement économique. [1]

Organigramme

La figure1 illustre l'organigramme de la macrostructure de SONATRACH

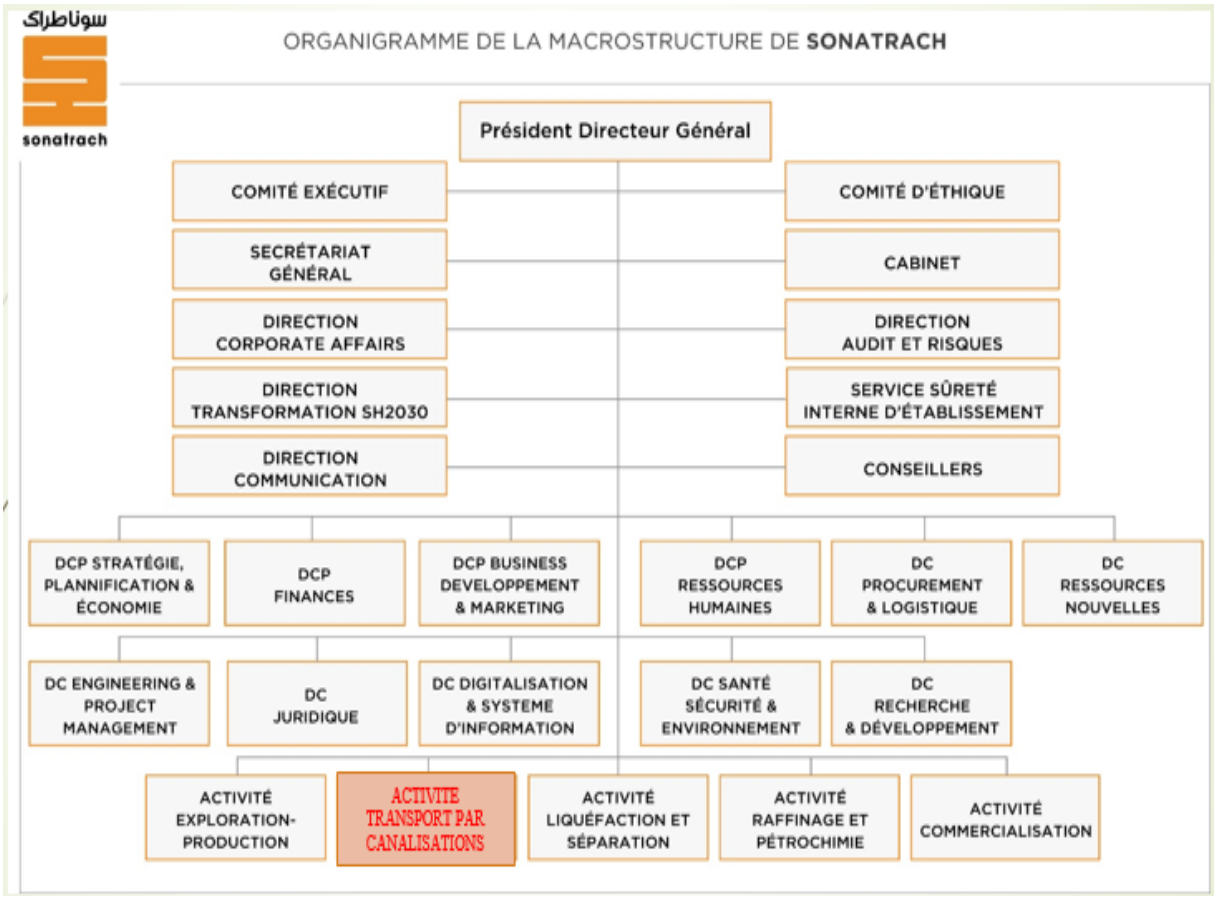


Figure 1: Organigramme de la macrostructure de SONATRACH.

I.2 Les structures opérationnelle

Les structures opérationnelles sont organisées autour des activités ci-après :

- Exploration-Production (E&P)
- Transport par canalisations (TRC)
- Liquéfaction et Séparation(LQS)
- Raffinage et Pétrochimie (RPC)
- Commercialisation (COM)

Chaque activité exerce ses métiers, développe son portefeuille d'affaires et contribue, dans son domaine de compétences, au développement des activités internationales de la Société.

I.3Système de Transport par Canalisation (STC)

Le réseau de transport des hydrocarbures liquides et gazeux est constitué d'un ensemble de canalisations, de stations de pompage, de stations de compression, de parcs de stockage, assurant le transport des effluents issus des champs de production, d'un centre de stockage, vers les pôles industriels de traitement et de liquéfaction, de transformation, d'exportation et d'alimentation du marché national.

Le réseau de transport inclut également les lignes d'expédition et les installations de chargement situées au niveau des ports d'Arzew, de Bejaïa et de Skikda, faisant partie des Extensions des STC Nord de pétrole brut et Condensat

Le développement du Réseau de Transport depuis la construction de la première canalisation en 1959, a été engendré par les besoins en matière de transport en constante croissance, nécessitant ainsi le développement continu de nouvelles Capacités de transport.

- Région Transport Centre - Bejaia (RTC),
- Région Transport de Haoud-el- Hamra(HEH),
- Région Transport d'In Amenas (RTI),
- Région Transport Est -Skikda (RTE),
- Région Transport Ouest Arzew (RTO),
- Gazoduc Espagne/Maroc (GEM),
- Gazoduc Tunisie/Italie (GPDF),
- Gazoduc Hassi R'mel (GHR).

La figure2 montre Cartographie actuelle du Réseau de Transport

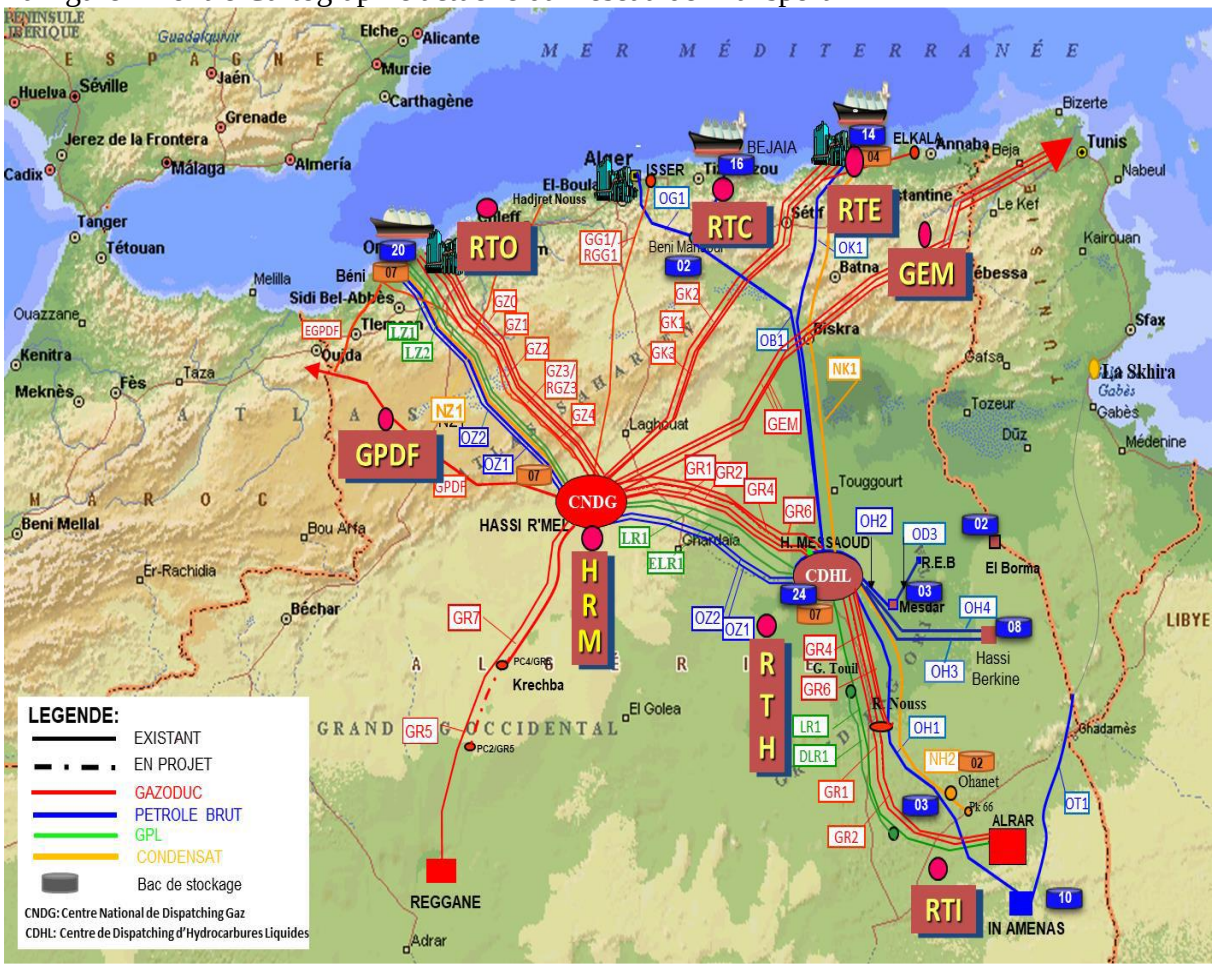


Figure 2: Organigramme de la macrostructure de SONATRACH

I.4 Présentation de la Région Transport Centre (Bejaia)

La Région Transport Centre est une région parmi les huit (08) régions composant l'activité de transport par canalisation, Elle est chargée de l'exploitation de deux oléoducs et d'un gazoduc.

C'est une ou plusieurs canalisations transportant des Hydrocarbures des produits pétroliers et de Gaz desservant exclusivement le marché national. [2]

- **L'oléoduc OB1 HEH-TMB :**

  D'une longueur de 668km et d'un diamètre de 24"/22", achemine du pétrole depuis centre de stockage Haoud El Hamra vers le terminal marin de Bejaia.

  - ✓ **Les Groupes de stations de pompage :**
    - SPA Touggourt / SP1 Bis Djamaa El M'ghair
    - SPB /SP2 El Outaya Biskra ;
    - SPC /SP3 M'sila.
    - Terminal Arrivée Béjaia

La figure3 montre le parc de stockage de la région transport Béjaïa

Figure 3:Organigramme de la macrostructure de SONATRACH

- **L'Oléoduc ROB1 SP3-TMB**

  Cette opération a concerné 164 km de l'oléoduc entre la station de pompage SP3 à M'sila et la station d'isolement SP13 située à Oued-Ghir, Bejaia

  - SP3New M'sila.

- Terminal Arrivée Béjaïa

➢ **L'oléoduc DOG1**
D'une longueur de 144 kms et d'un diamètre de 20", il est piqué sur l'oléoduc H.E.H-Bejaia et alimente la raffinerie d'Alger située à Sidi-Arcine.

- Beni-Mansour M'sila.
- Terminal Arrivée Raffinerie d'Alger

➢ **Le gazoduc GG1 42'' HRM – Bord-Menail**
D'une longueur de 437 kms et d'un diamètre de 42", il approvisionne en gaz naturel toutes les villes et pôles industriels du centre du pays.

- SC3 Moudjebara
- Terminal Arrivée Bordj-Menail

- **Le gazoduc RGG1 42'' Medjdal– Bord-Menail**

D'une longueur de 210 kms et d'un diamètre de 42", il approvisionne en gaz naturel toutes les villes et pôles industriels du centre du pays.

- TD Medjdel M'sila
- Terminal Arrivée Bordj-Menail

I.5 Présentation des différentes structures de la RTC:

La RTC est composée de trois sous-directions qui sont elles-mêmes décomposées en départements que nous allons décrire ci-dessous.

Les différents sous- directions et départements de la RTC sont représentés sur Figure 4

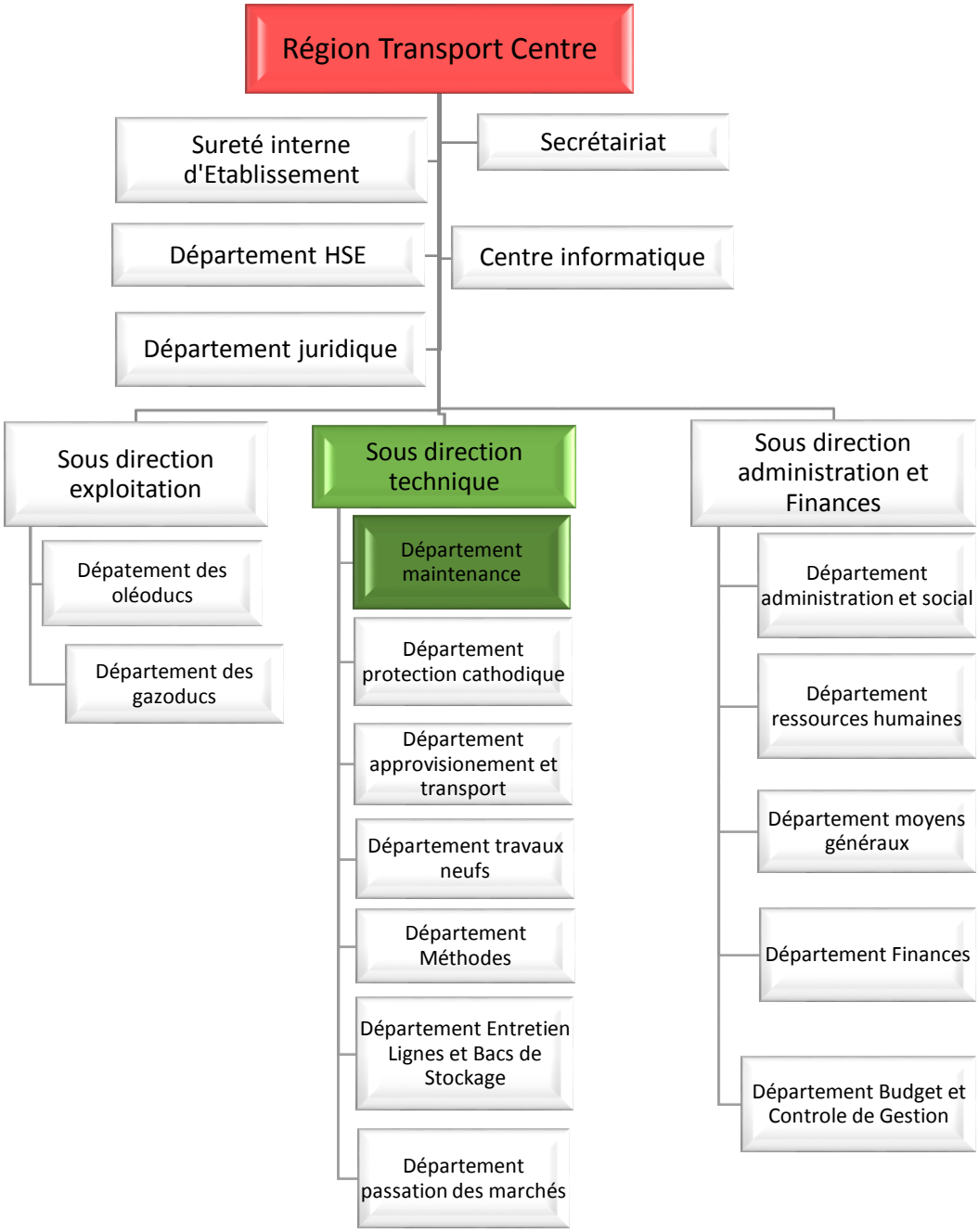


Figure 4: Organigramme de la macrostructure de SONATRACH

I.6Département maintenance.

I.6.1 Objectif de département maintenance.

Dans le cadre de la politique de la maintenance s'effectue le choix entre les méthodes de maintenance. Le choix de la méthode est basé sur la connaissance du fonctionnement et les caractéristique du matériel, son comportement et sa manière d'exploitation; les conditions

d'application de chaque méthode ; les coûts de la maintenance et les coûts de pertes de production.

I.6.2 Les missions de département maintenance.

Parmi les missions principales du département c'est de veiller au maintien en bon état des installations techniques de la région c'est-à-dire d'assurer la maintenance des équipements industriels tournants (Groupes Electropompes, Turbines et auxiliaires).

La figure6 représente la Structure de département maintenance

I.6.3 Sa structure est représentée sur la figure.

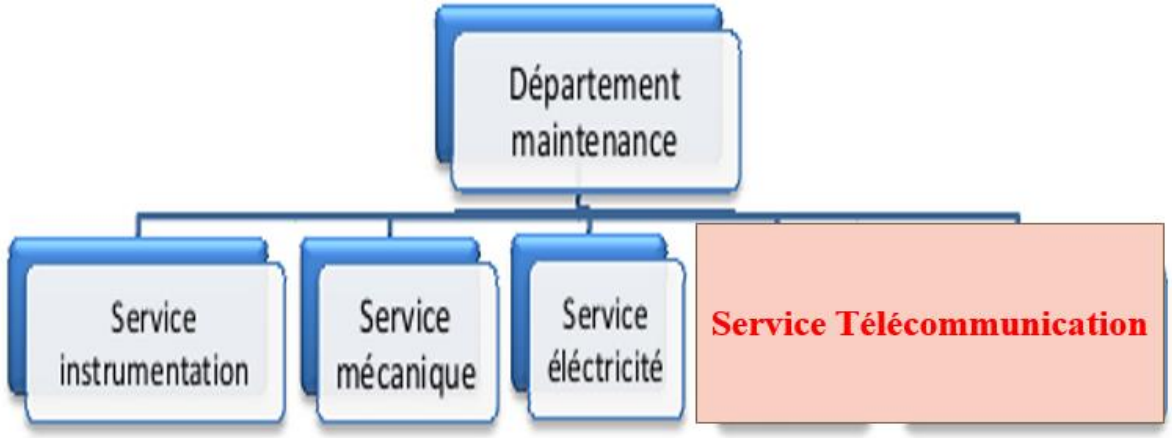


Figure 5:Structure de département maintenance

I.7Service télécommunication

Les services de télécommunications est le moyen actuel et indispensable au contrôle des mouvements des produits et la consolidation quotidienne de gestion.

Les différentes sections du service télécom sont représentées dans la figure 7:

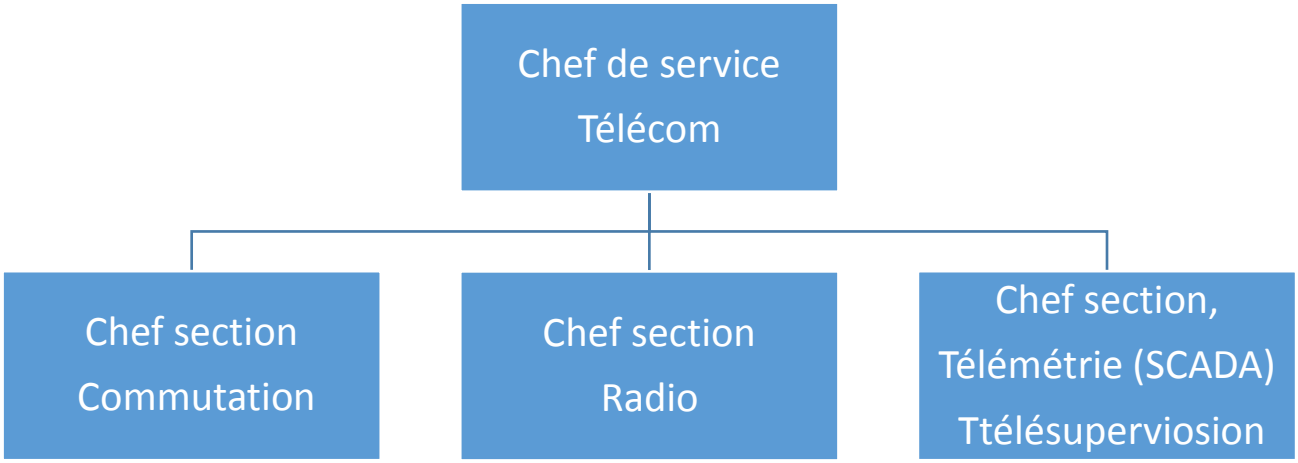


Figure 6: Structure de service télécommunication

I.7.1 Section Commutation :

Le réseau de commutation est constitué de 08 PABX, les tâches assignées à cette section sont :

- ✓ maintenance curative et préventive des (08) huit PABX installés au niveau du siège et stations
- ✓ Essai et entretien des différentes liaisons téléphoniques en relation avec les autres entités (HEH)
- ✓ Elaboration de plans de modification du réseau téléphonique.
- ✓ programmation et mise à jour des fichiers de données.
- ✓ maintenance des équipements d'énergie (redresseur, batterie).
- ✓ Suivi de réparation fibre optique de l'OB1, et GG1
- ✓ pose de câble et suivi de pose de la fibre optique
- ✓ Mise à jour les plans de câblage du réseau téléphonique.

I .7.2 Section télémétrie (SCADA):

Les systèmes SCADA à gérer sont composés de 60 RTU et 02 systèmes de supervisions, les taches de cette section sont :

- ✓ Installation des automates programmables et connexes
- ✓ maintenance des automates programmables et auxiliaires siège et stations
- ✓ Réalisation les différentes images de processus et leur dynamisation
- ✓ Mise à jour des plans de câblage et des programmes.
- ✓ Formation des opérateurs à l'exploitation du système de télé supervision.

Conclusion

Dans ce chapitre, nous avons présenté l'organisme d'accueil (Sonatrach) et ses différents sites ainsi la structure de la RTC .on s'est basé sur le service télécom on a étudié les différentes tache de ce service

Introduction

L'étude de l'organisme d'accueil est une étape importante qui sert à représenter les contraintes sous lesquelles se réalisera notre projet. Dans ce chapitre, nous allons présenter l'entreprise SONATRACH, citer les déférents départements qui la constituent et donner quelques informations qui nous seront utiles dans notre travail, tout en posant la problématique autours de laquelle tournera notre mémoire

II.1 Etude de l'existant

Une bonne compréhension de l'environnement informatique aide à déterminer la portée du projet d'implémentation de la solution. Il est essentiel de disposer d'informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau. En effet, ces informations affectent une grande partie des décisions que nous allons prendre dans le choix de la solution et de son déploiement.

II.2Présentation du réseau SONATRACH

Le réseau Sonatrach ST, est un réseau Ethernet commuté à 1000 Mb/s, il est basé sur la topologie hiérarchique.

Le réseau ne contient aucun sous réseau, ce qui réduit ses performances compte tenu du nombre important du trafic qui en découle.

II.2.1 Modèle de conception hiérarchique

Il existe deux structures de modèles de réseau : le modèle hiérarchique et le modèle maillé. Dans une structure maillée, la topologie du réseau est linéaire. Tous les routeurs remplissent essentiellement les mêmes fonctions et il n'existe généralement pas de définition précise des fonctions exécutées par chaque routeur. L'expansion du réseau s'effectue par hasard et de façon arbitraire.[4]

La figure 7 représente l'architecture du réseau maillé

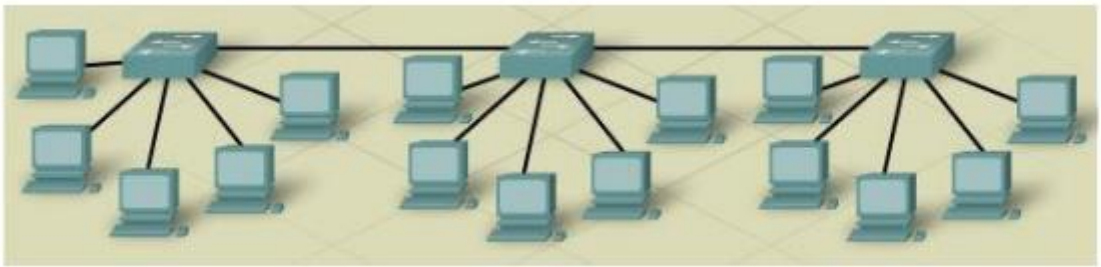


Figure 7: Réseau maillé

Dans la structure hiérarchique, on regroupe les périphériques en un certain nombre de réseaux distincts qui sont organisés en couches. Une ou plusieurs fonctions précises sont associées à chaque couche. Le modèle de conception hiérarchique possède trois couches de base :

- ✓ Couche Cœur du réseau
- ✓ Couche de Distribution
- ✓ Couche d'Accès

La figure 8 représente le réseau hiérarchique et les différentes couches qu'il possède

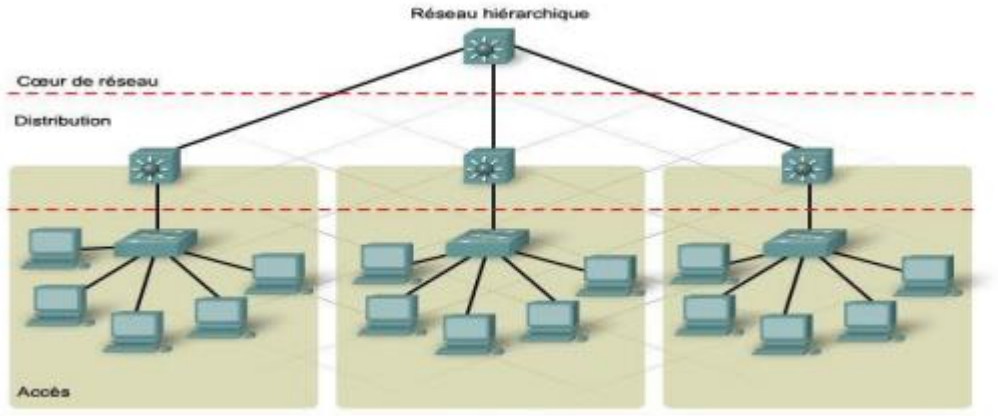


Figure 8:Réseau hiérarchique

Cette architecture hiérarchique offre au réseau les avantages suivants :

•**Evolutivité :** possibilité d'une forte croissance du réseau sans effet négatif sur le contrôle et la facilité de gestion. En effet, les fonctionnalités sont localisées et il est plus facile de détecter les problèmes éventuels.

•**Facilité de mis en œuvre** : celle-ci est due à l'attribution des fonctionnalités précises à chaque couche.

•**La facilité de dépannage** : on peut isoler les problèmes qui peuvent survenir au réseau puisque ce dernier est modulaire ; il est aussi facile de segmenter temporairement le réseau pour réduire l'étendue du problème.

•**La prévisibilité :** on peut comprendre et prévoir le comportement d'un réseau utilisant des couches fonctionnelles ; la planification de la capacité de croissance du réseau et la modélisation de ses performances peuvent être simplifiées.

•**La prise en charge des protocoles :** l'organisation logique de l'infrastructure sous-jacente sur le réseau permet la facilité de combiner les applications et les protocoles actuels et futurs.

Couche d'accès

Cette couche est habituellement un LAN ou un groupe de LAN, de type Ethernet ou Token Ring, qui assure aux utilisateurs un accès de première ligne aux services réseau. C'est au niveau de cette couche que la plupart des hôtes, tels que tous les serveurs et les stations de travail des utilisateurs, sont reliés au réseau. Les services et les périphériques de cette couche sont situés dans chaque bâtiment de campus, dans chaque site distant et à la périphérie du réseau d'entreprise. 48 La topologie de la couche d'accès peut être en étoile ou à maillage globale. Elle utilise la technologie de commutation de couche 2. L'accès peut se faire à partir d'une infrastructure câblée permanente ou de points d'accès sans fil. L'emplacement physique des équipements représente alors l'une des plus grandes préoccupations lors de la conception d'une couche d'accès.

Couche de distribution

La couche de distribution est une frontière de routage entre la couche d'accès et la couche cœur de réseau ; c'est aussi le point de connexion entre les sites distants et la couche cœur de réseau. Elle assure le filtrage (ACL ou Access Control List), la gestion de flux de trafic et le routage des VLAN ; elle permet aussi d'isoler la couche cœur de réseau par rapport aux pannes ou aux interruptions de service au niveau de la couche d'accès. La couche de distribution est créée à partir des périphériques de couche 3 tels que les routeurs ou les commutateurs multicouches. Ces périphériques gèrent les files d'attente et la hiérarchisation du trafic avant la transmission vers la couche cœur. Ils présentent aussi des liaisons agrégées et redondantes pouvant être configurées pour un équilibrage de charge, augmentant ainsi la bande passante disponible pour les applications. Cette couche est câblée selon une topologie à maillage partielle tout comme la couche cœur de réseau.

Couche cœur

La couche cœur de réseau appelée aussi réseau fédérateur relie les périphériques de la couche distribution. Les routeurs et les commutateurs de cette couche offrent une connectivité haute vitesse. Elle contient une ou plusieurs liaisons vers les périphériques de la périphérie du réseau pour la prise 49 en charge de l'accès à Internet, aux réseaux privés virtuels (VPN), à l'extranet et aux réseaux étendus (WAN). Ainsi, on conçoit la couche cœur de réseau afin de transférer efficacement et rapidement des données entre deux sections de réseau ; faciliter la croissance du réseau et sa gestion. Toutefois, elle ne s'occupe pas du filtrage ou de la sécurité et une défaillance au niveau de cette couche entraine un problème de grande échelle au niveau du réseau global. Les technologies utilisées au niveau de cette couche sont les routeurs ou

commutateurs multicouches, la redondance pour la continuité de service en cas de panne, les liaisons de haute vitesse, les protocoles de routage tels qu'EIGRP et OSPF ayant des fonctionnalités importantes telles qu'une convergence rapide et le partage de charge

II.2.2 Architecture du réseau existant

Dans la figure 9 on montre l'architecture existante de Sonatrach :

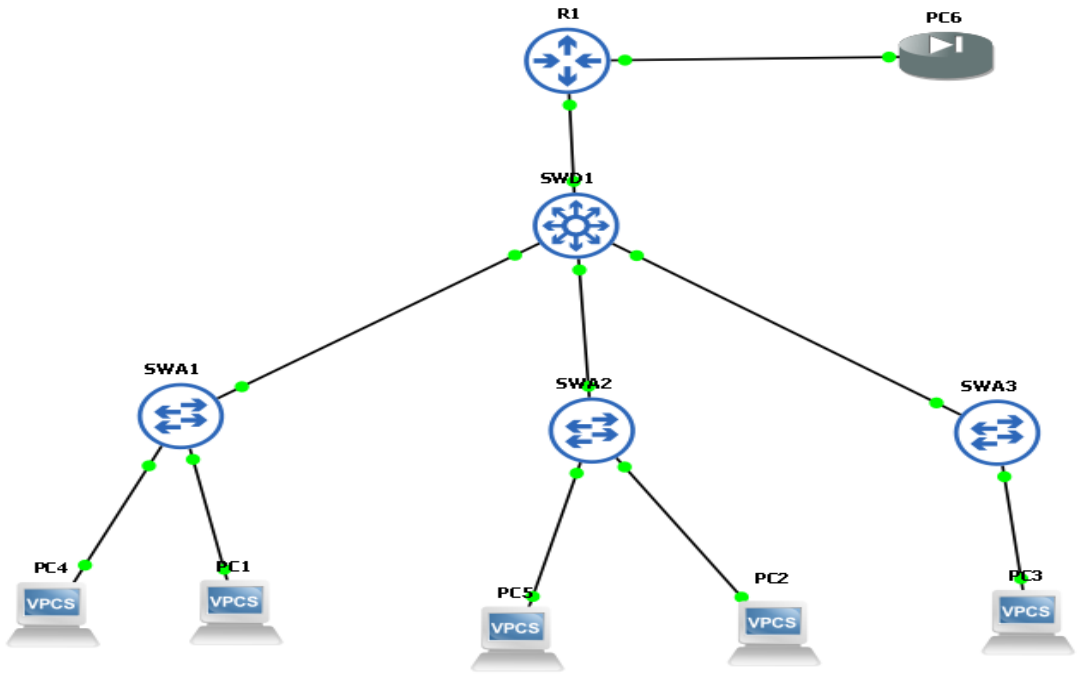


Figure 9: l'architecture existante de Sonatrach

II.3Analyse du parc informatique

II.3.1 Environnement client

SONATRACH ST dispose d'un parc informatique de plus de cinquante (50) postes de travail de type IP TOUCH repartie sur un seul site.

Les postes sont dimensionnés comme suit :

Tableau 1:les postes du parc informatique

Type	Système
HP	Windows +10+linux
Poste téléphonique Alcatel	Android 8.1 Oreo
Dell	Windows 7/8.1/10

II.3.2 Environnement serveur

Le réseau de SONATRACH ST est composé d'une quinzaine (15) de serveurs Il faut préciser que l'ensemble des serveurs de la structure est configuré avec la technologie RAID ….

Cette technologie permet de stocker des données sur de multiples disques durs afin d'améliorer, en fonction du type de RAID choisi, la tolérance aux pannes et/ou les performances de l'ensemble.

La quantité importante du nombre de serveur est dueaux quantités nombreuses des applications et des bases de données développés en client serveur

Les serveurs sont dimensionnés comme suit :

Tableau 2:les serveurs

Type fournisseur	Rôle	Capacité
Dell	VOIX IP ET ASTERISK	RAM 16GO
HP	Serveur AD, DNS, DHCP	RAM 32GO

II.4 Le matériel d'interconnexion

Les équipements d'interconnexion représentent le cœur du réseau dans une architecture.

S'ils sont mal dimensionnés, ils pourront avoir des effets négatifs sur le trafic du réseau, allant à la détérioration de celui-ci. Dans notre cas d'étude, l'infrastructure du réseau sonatrach comporte des commutateurs Cisco monté en cascade. Ces équipements par leur fonction permettent de segmenter des réseaux par la technologie VLAN afin de réduire significativement la congestion sur réseau au sein de chaque segment.

Mais nous remarquons que cette solution N'est pas implémentée. L'infrastructure comprend les équipements d'interconnexion suivant :

Tableau 3:le matériel d'interconnexion

Nombre	**Equipements**
Firewall	PfSense
Routeur	Cisco 2900
Commutateurs	Catalyst série 3750

II.4.1Firewall

Un firewall, appelé aussi coupe-feu ou pare-feu a pour but de contrôler et de filtrer l'accès entre un réseau d'entreprise ou l'ordinateur d'un particulier et un autre réseau qui est ici Internet comme le montre le figure10 :

Figure 10: Firewall

II.4.2 Routeur Cisco 2900

La gamme Cisco 2900 reprend et améliore l'ensemble des avancées de la gamme existante de routeurs à services intégrés Cisco 2800 en proposant quatre plates-formes (Figure 1) : les routeurs à services intégrés Cisco 2901, 2911, 2921 et 2951. Les routeurs à services intégrés de deuxième génération (ISR G2) offrent une souplesse et une intégration des services supérieures. Conçue dans un objectif d'évolutivité, l'architecture modulaire de ces plates-formes permet d'adapter votre infrastructure réseau aux besoins de votre entreprise au fur et à mesure que celle-ci se développe.[5]

II.4.3 Commutateurs Catalyst série 3750

La gamme Catalyst série 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables [6]

II.5Critique de l'existant et spécification des besoins

L'étude du réseau Sonatrach ST, nous a permis de définir un nombre importants de contraintes pouvant réduire ses performances voir sa dégradation :

- Augmentation rapide du nombre des utilisateurs
- Volume accru du trafic généré par chaque utilisateur

- Echange volumineux de fichiers non nécessaire entre utilisateurs
- Applications toujours plus complexes et fichiers plus volumineux.
- Augmentation accrue des bases de données des serveurs
- Trafic web important
- Flux messagerie important
- Les collisions important dans le réseau
- Réseau non segmenté

II.6 Spécification des besoins

Suite à la critique de l'existant, plusieurs besoins ont été relevés.

II.6.1 Besoins fonctionnels

Les besoins fonctionnels expriment une action qui doit être menée sur l'infrastructure à définir en réponse à une demande. C'est le besoin exprimé par le client.

Pour cela, nous aurons :

- Besoin de segmenter le réseau en créant des VLANs. Deux raisons sont à la base de cette segmentation du réseau. La première a pour but d'isoler le trafic entre les segments la seconde a pour but de fournir davantage de bande passante par utilisateur et par groupe de serveur par la création de domaine de collision de petite taille.
- Besoin de mettre en place une sécurité qui permettra à tous les VLANs de ne pas communiquer.

II.6.2Les besoins non fonctionnels

Ils se groupent autour des points suivant :

- Besoin d'indisponibilité du réseau
- Besoin d'administration du réseau à travers les Vlan
- Besoin d'incompatibilité du commutateur à pouvoir gérer les bandes passantes
- Besoin de performance des commutateurs
- Besoin de sécurité des commutateurs

II.7Problématique et solutions

II.7.1 Problématique

Sonatrach dispose d'une architecture réseau de taille très importante composé d'une plateforme de service constitué de deux environnements (client et serveur), reliant plusieurs sites locaux.

La gestion de ce réseau est accompagnée par le service maintenance qui veille à le rendre performantet stable

Malgré la haute performance de cette architecture l'inconvénient se trouve dans l'absence des équipements d'interconnexion, après l'étude de l'architecture existante de Sonatrach nous avons constaté que la présence d'un seul routeur cœur et un seul switch distribution n'est pas suffisant pour le bon fonctionnement du réseau la défaillance de l'un des équipements engendrera la disfonctionnement du tout le réseau de l'entreprise.

II.7.2 L'objectif principal

L'objectif principal de ce projet est de mettre en place une solution

- Nouvelle architecture réseau en la développant en une architecture réseau hiérarchique
- Solution de redondance qui réduit le taux de risque d'un arrêt total du réseau
- d'optimisation de la bande passante du réseau par la segmentation des domaines de broadcast Sonatrach ST.
- Configuration du réseau est l'étape essentielle à entreprendre pour améliorer cette architecture et évité tout disfonctionnement
- une haute disponibilité

II.7.3Les solutions

Il est toujours important de définir une architecture flexible de segmentation du réseau. L'implémentation d'une telle architecture aboutira à un gain de performance du réseau.

II.7.3.1 protocole HSRP

La solution du protocole HSRP est une étape très importante à prendre dans notre architecture car le fait qu'on a ajouté d'autre switch de distribution on a surement besoin de cette technologie qui permet la gestion des équipements redondants cette solution repose sur l'hypothèse d'avoir 2 switch de distribution si le premier fonctionne (mode active) le deuxième est en attente (mode standby) prêt à prendre le relais en cas de problème sur le premier

II.7.3.2 Spanning Tree

Dans un réseau commuté de type Ethernet il doit y'avoir en moins deux chemise une chemin principal et un autre alternatif au cas où y'a une coupure du chemin principale ou une panne de switch la présence du protocole stp est très importante dans ce cas ce dernier permet d'avoir un réseau redondant et sans boucle il permet aussi d'augmenter la bande passante.

II.7.3.2 VPN

La technologie VPN permet une connexion sécurisé a un réseau pour un PC ou une entreprise distant cette connexion est créé de bout en bout par réseau privé vers des réseaux comme internet ou extranet cette technologie permet de relier distants de communiquer de manière sure (site Bejaia et Alger)

Conclusion

Dans ce chapitre, nous avons appris à mieux comprendre la structure et l'organisation du réseau de la RTC de Bejaïa, et d'étudier notre problématique afin de proposer les solutions adéquates et les objectifs à atteindre.

Introduction

Après avoir présenté l'organisme de l'entreprise et les différents problèmes, nous allons élaborer une étude descriptible des solutions, ainsi qu'une argumentation du choix de ces dernières qui seront implémentées en illustrant les avantages et les atouts de chaque solution.

III.1 Accès à distance.

Nous avons tous besoin d'accéder à une ressource distante, dans la plupart des cas nous devons transporter des données sur un réseau non sécurisé tel qu'un internet, nous accédons aux données dans le Cloud ou au bureau distant, via un ordinateur portable en SO/HO, sur un appareil mobile

Il y'a plusieurs types d'accès à distance tel que Telnet et SSH.

III.1.1 Telnet « terminal network ou Télécommunication network ».

Telnet est un protocole permettant d'émuler un terminal à distance, permettant de communiquer avec un serveur distant. Il permet aussi de tester les ports ouvert Autrement dit, il permet d'exécuter des commandes saisies au clavier sur une machine distante [7].Le problème de ce protocole c'est justement qu'il est trop simple : les données sont transférées en clair sur le réseau. Il n'y a aucun chiffrement. Donc les données ne sont pas sécurisées.

III.1.1.1 Fonctionnement de Telnet.

Il fonctionne dans un environnement client/serveur, la machine distante est configurée en serveur et par conséquence attend qu'une machine lui demande un service. Ainsi, étant donné que la machine distante envoie les données à afficher, l'utilisateur a l'impression de travailler directement sur la machine distante.

Exemple

Le fonctionnement de Telnet est représenté dans La figure 11 ci-dessous

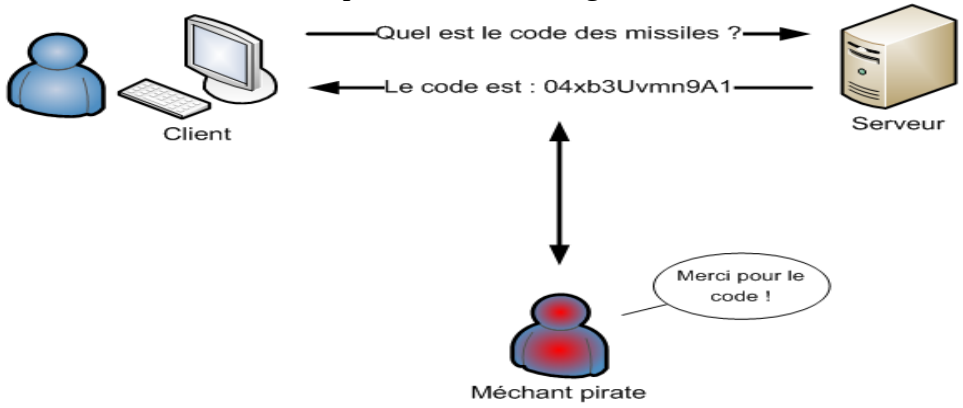


Figure 11: Le protocole Telnet.

III.1.2 SSH «Secure Shell »

Secure Shell est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion.

La figure12 montre l'échange de clé de chiffrement à travers le tunnel SSH

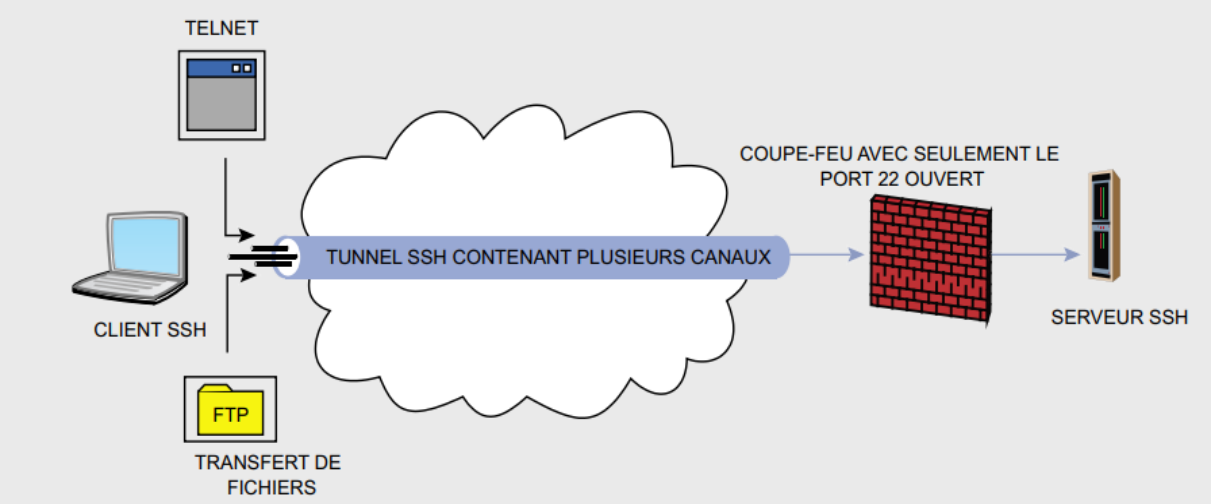


Figure 12: le tunnel SSH.

III.1.2.1 Fonctionnalités des différents algorithmes employés par SSH.

Tout d'abord, il convient de rappeler les différents algorithmes utilisés par SSH. En effet, SSH utilise deux algorithmes pour assurer l'authentification, RSA et DSA, ce dernier ne fonctionnant qu'avec la version 2 du protocole. Pour chiffrer les données, SSH-1 utilise les algorithmes DES, 3DES, SSH-2 emploie AES.

Le chiffrement symétrique est représenté dans la figure 13.

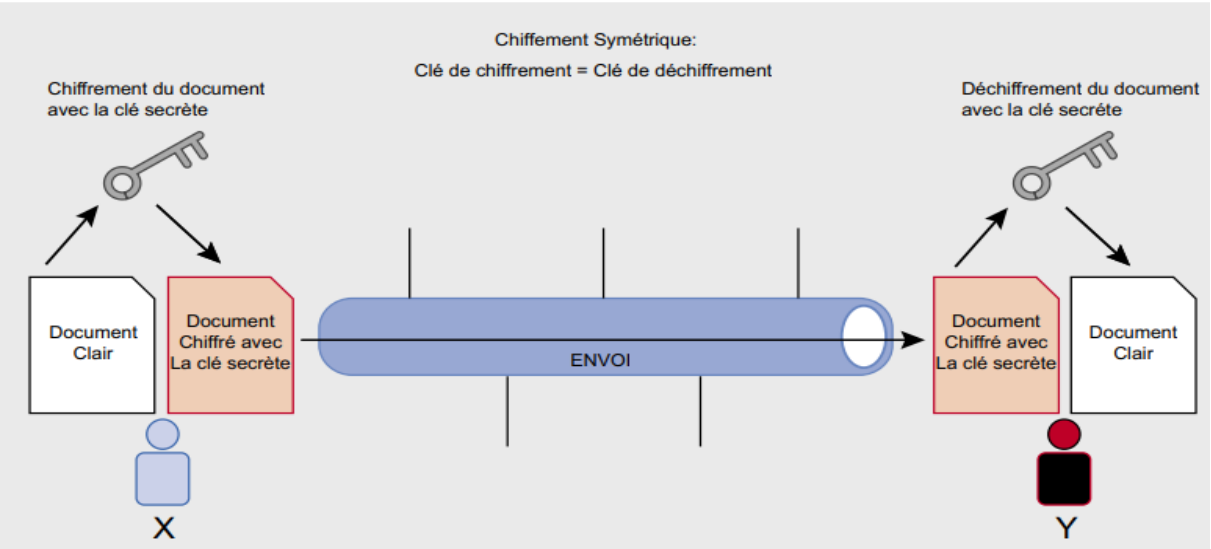


Figure 13: Chiffrement symétrique.

III.1.2.2 Différence entre SSH-v1 et SSH-v2.

SSHv1 ne permet d'établir qu'un seul et unique canal par session contrairement à la version 2 où il est possible de créer une multitude de canaux par session.

Les usages de SSH sont entre autre :

- Accéder à distance à la console en ligne commande (Shell), ce qui permet d'effectuer la totalité des opérations courantes et/ou d'administration sur la machine distante.
- Déporter l'affichage graphique de la machine distante.
- Transferts de fichiers en ligne de commande.
- Montage ponctuel de répertoires distants, soit en ligne de commande.
- Montage automatique de répertoires distants.
- Déporter de nombreux autres services ou protocoles

III.1.2.3 Fonctionnalités

- L'accès à distance
- Le transfert de fichier SFTP (Secure File Transfert Protocol)
- Le tunneling
- La redirection de port
- La redirection de l'authentification

III.1.2.4 Les avantage de ce protocole.

- La confidentialité
- L'intégrité
- L'authentification

III.2VPN (Virtual Private Network)

Le VPN représente un réseau privé virtuel qui est un réseau crypté dans le réseau internet permettant à une société dont ses locaux sont géographiquement dispersés, de communiquer et partager des documents d'une façon complètement sécurisée comme si n'y avait qu'un local avec réseau interne.

Les VPNs sont basé sur les protocoles de tunnelisation.Ces protocoles permettent de sécuriser les données passant entre deux réseaux physiques en utilisant des algorithmes de chiffrage. [8]

La représentation d'un VPN est donnée dans la figure 14.

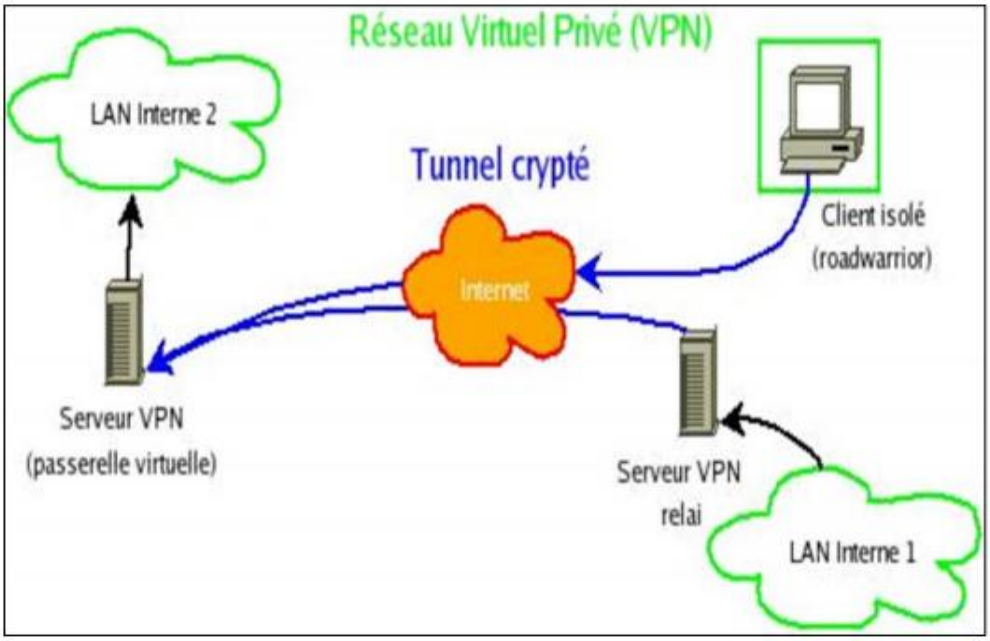


Figure 14: Schéma d'un VPN.

III.2.1 Types de VPNS

- Extranet VPN entre une entreprise et ses partenaires et clients privilégiés.
- Intranet VPN entre les succursales et le siège d'une entreprise.

III.2.1.1 Extranet VPN

L'extranet VPN entre une compagnie et ses clients (site a site) et ses sites distants (poste à site).Partenaires stratégiques nécessite une solution ouverte afin d'assurer l'interopérabilité avec les diverses solutions que les partenaires peuvent implémenter. Le standard actuel pour les VPN basés sur Internet est IPsec (Internet Protocol Security). Il est également important de gérer le trafic afin d'éviter le goulot d'étranglement à l'entrée du réseau, pour obtenir un temps de réponse le plus court possible à une demande critique.

La figure 15 représente le VPN extranet.

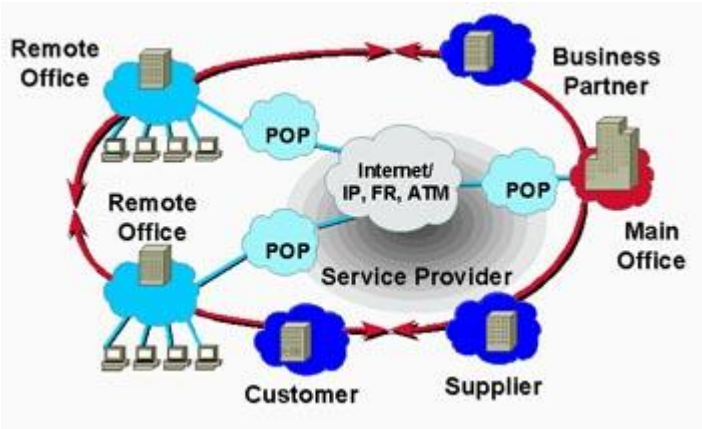


Figure 15: Extranet VPN

III.2.1.1.1 Site à site

VPN site à site correspond à un type d'infrastructure de réseau étendu, c'est-à-dire que l'interconnexion entre les VPN remplace et améliore les réseaux privés existant. Elle est utilisée pour relier un site avec des filiales à moindre coût et en toute sécurité.

Pour ce type de réseau VPN on compte deux façons de déploiement qui sont les suivantes :

Le réseau privé virtuel de site à site interne

Le réseau privé virtuel Site-a-Site par Internet

L'architecture du VPN site à site est représentée dans la figure 16.

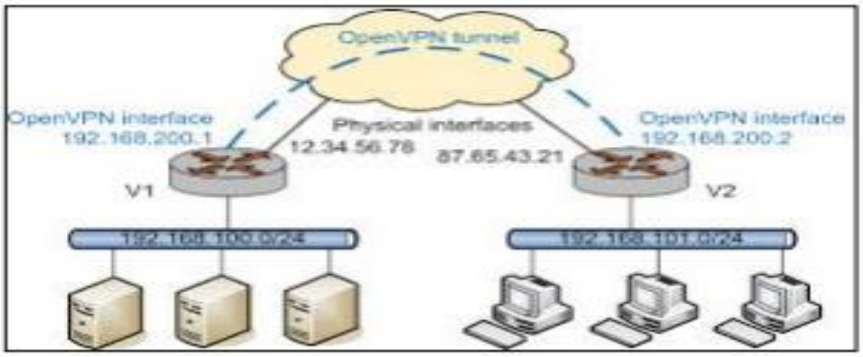


Figure 16: Architecture site to site.

III.2.1.2Intranet VPN

L'intranet VPN favorise la communication entre les départements interne (poste à poste) d'une entreprise. Les VPN s'appuient alors sur le réseau d'un opérateur.

Il est nécessaire de développer un fort en cryptage afin de protéger les informations sensibles qui peuvent circulé tels que les bases de données clients.

La figure 17montre le VPN intranet.

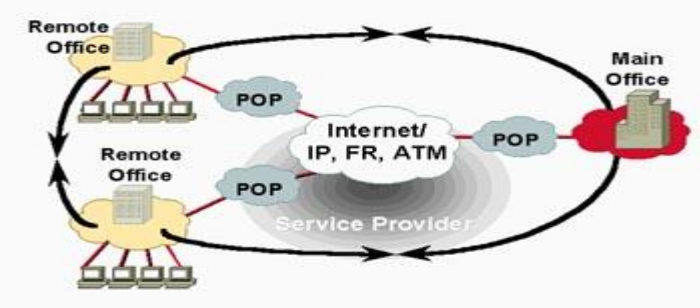


Figure 17: Architecture site to site.

III.2.1.2.1Principaux avantages des VPN

Cost saving (réduction des couts) : les entreprises peuvent utiliser des VPN pour réduire leurs couts de connectivité tout en augmentant simultanément la bande passante de la connexion distante.

Security (sécurité) : les VPN offrent le plus haut niveau de sécurité possible, en utilisant des protocoles de cryptage et d'authentification avancés qui protègent les données contre les accès non autorisé.

Scalability (évolutivité) : les VPN facilite l'ajout de nouveaux utilisateurs sans ajouter d'infrastructure significative.

Compatibility (compatibilité) : les VPN peuvent être mise en œuvre sur une grande variété d'option de liaison WAN, compris toutes les technologies à large bande populaires.

III.3 La redondance

III.3.1 La redondance au premier saut

La redondance au premier saut est un type de protocole de couche 3 appelé FHRP dont le propriétaire CISCO c'est aussi la capacité d'un réseau à effectuer une reprise dynamique après la défaillance d'un périphérique jouant le rôle de passerelle par défaut.

III.3.2 Principe de la redondance au premier saut

Un protocole est utilisé pour identifier au moins deux routeurs comme périphérique chargés de traiter les trames envoyée à l'adresse MAC ou l'adresse IP d'un routeur virtuel unique.

- Ce protocole de redondance offre le mécanisme nécessaire pour déterminer quel routeur doit être actif dans le réacheminement du trafic.
- Il détermine également quand le rôle de réacheminement doit être repris par un routeur en veille.
- La transition d'un routeur de transfert à un autre est transparente pour les périphériques finaux.
- Les périphériques hôtes transmettent le trafic à l'adresse du routeur virtuel. Le routeur physique qui réachemine ce trafic est transparent pour les périphériques hôte.

III.3.3 Fonctions du protocole FHRP

- Redondance de passerelles par défaut ;
- Répartition de charge : Dans un groupe, un routeur est effectif pour certains VLANs dans un autre groupe, il est sauvegarde pour d'autres VLANs ;
- Il est possible d'influencer une élection via priorité et préemption (preempt). Avec cette fonctionnalité de préemption, le routeur avec la haute priorité devient immédiatement le routeur actif. Le routeur envoie un message 'Coup' ou un message "Hello" (HSRP).

- Il est possible de suivre l'état d'une interface au-delà du LAN (track) et d'influencer une élection dans un groupe en réduisant la valeur de priorité même d'un routeur actif "preempt".

III.3.4 Protocoles de redondance au premier saut

Les protocoles qui offrent ce service sont :

- Host Standby Router Protocol (HSRP)
- Gateway Load Balancing Protocol (GLBP)
- Virtual Router Redundancy Protocol (VRRP)

III.3.4.1 Protocole HSRP (Host Standby Router Protocol)

Le protocole HSRP (Host Standby Router Protocol) est un protocole propriétaire de continuité de service implémenté dans les routeurs Cisco pour la gestion des liens de secours. Ce protocole sert à augmenter la tolérance de panne sur les réseaux en créant un routeur virtuel à partir de 2 (ou plus)routeur physique : un actif et l'autre (ou autre) en attente en fonctions des priorités accordés à chacun de ces routeur. Sur ce protocole les communications se font part l'envoi des paquets multicast vers le port des routeurs concerner.

III.3.4.2 Protocole GLBP (Gateway Load Balancing Protocol):

Le protocole GLPB (Gateway Load Balancing Protocol) est protocole propriétaire Cisco qui reprend les concepts de base de HSRP et l'utilisation simultanée de plusieurs passerelles disponibles. De plus ce protocole permet d'assurer le basculement automatique entre ces passerelles

La figure 19résume le fonctionnement du protocole GLBP.

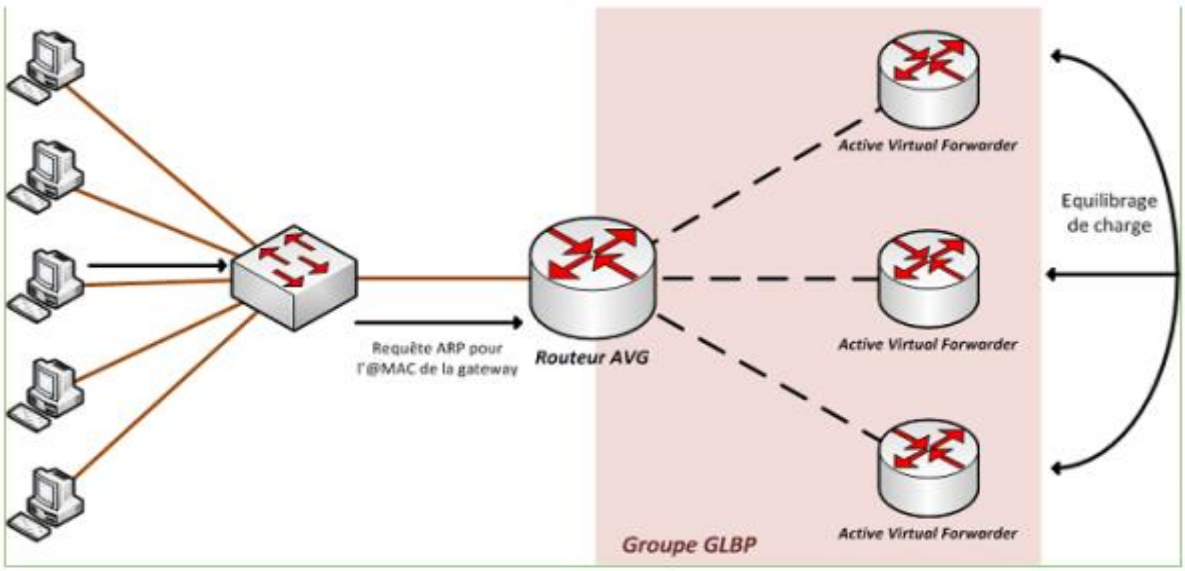


Figure 18: Fonctionnement du GLBP

III.3.4.3 VRRP (Virtual Router Redundancy Protocol):

C'est un protocole standard défini dans la RFC 5789. VRRP est, à l'instar de HSRP, également un protocole qui fournit une solution de continuité de service principalement pour la redondance de passerelles par défaut. Il présente l'avantage d'être compatible aux routeurs non Cisco

La figure 20 montre le fonctionnement VRRP.

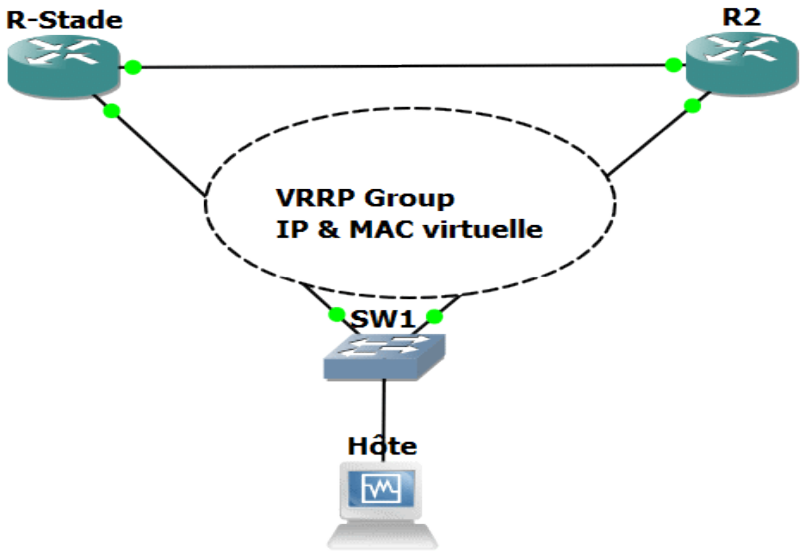


Figure 19:Fonctionnement de VRRP.

III.4 Etherchannel

La technologie Etherchannel a été inventée par la société Kalpana au début des années 1990.Cette société a ensuite été acquise par Cisco Systems en 1994.En 2000, IEEE a publié le standard 802.3ad, qui est une version ouverte de Etherchannel.

Etherchannel est une technologie d'agrégation de liens, de port ou une architecture de canal de port, utilisée principalement sur les commutateurs Cisco. Il permet de regrouper plusieurs liaisons Ethernet physiques pour créer une seul liaison Ethernet logique dans le but de fournir une tolérance aux pannes et des liaisons à haut débit entre les commutateurs, les routeurs et les serveurs.

Un lien Etherchannel groupe de deux (2) à huit (8) liens actifs de 100Mbitps, 1Gbitps et 10Gbitps.Il est principalement utilisé sur la dorsale du réseau local entre la couche Access et Distribution, on peut aussi l'utiliser pour connecter des postes d'utilisateurs et des serveurs.

La figure 21 représente l'équilibrage de charge et de la redondance sur 2 commutateurs.

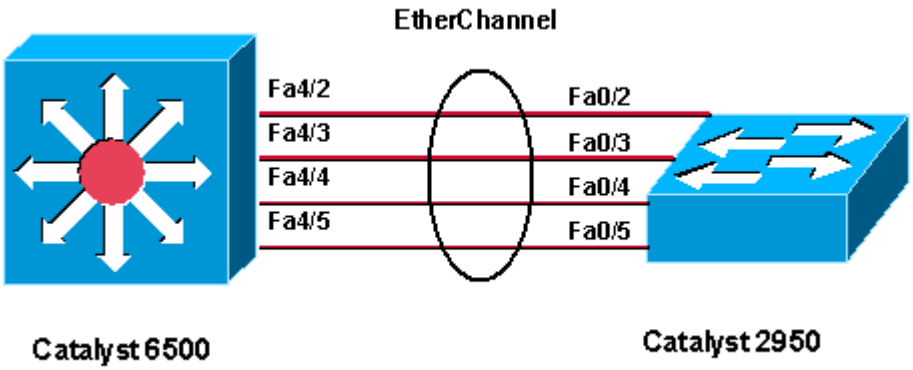


Figure 20: l'Etherchannel.

.

III.4.1Comparaison entre EtherChannel et IEEE 802.3ad.

Les protocoles EtherChannel et IEEE 802.3ad sont très semblables et accomplissent le même but. Il y a néanmoins quelques différences entre les deux :

- EtherChannel est un protocole propriétaire de Cisco, alors que 802.3ad est un standard ouvert
- EtherChannel nécessite de configurer précisément le commutateur, alors que 802.3ad n'a besoin que d'une configuration initiale
- EtherChannel prend en charge plusieurs modes de distribution de la charge sur les différents liens, alors que 802.3ad n'a qu'un mode standard
- EtherChannel peut être configuré automatiquement à la fois par LACP et par PAgP, tandis que 802.3ad ne peut l'être que par LACP.

III.4.2 Négociation de l'agrégation

Il existe deux manières de créer une agrégation de lien :

- En forçant l'agrégation(ON)
- En utilisant un protocole de négociation (PAGP 'Port Agregation Protocol', LACP 'Link Agregation Control Protocol').

III.4.2.1 PAgP ' Port Agregation Protocol'

PAgP est le protocole de négociation propriétaire Cisco. En choisissant ce protocole, il est possible de configurer les ports dans 2 modes différents :

- Auto: le port attend une requête du port voisin.
- Désirable : le port négocié avec le port voisin.

- Avec PAGP, si le port est en mode Auto, une agrégation de lien sera créée si le port d'en face est en mode Désirable. Si le port d'en face est en mode Auto, aucune agrégation n'est créée.
- Si le port est configuré en mode Désirable, une agrégation sera créée à condition que le port d'en face soit en mode Auto ou Désirable.
- Attention, il n'est pas possible d'avoir un port en mode ON d'un côté, et d'utiliser un protocole de négociation (PAGP ou LACP) de l'autre côté d'une agrégation.

Tableau 4:Fonctionnement de PAgP

PAgP	Désirable	Auto
Désirable	Compatible	Compatible
Auto	Compatible	Non compatible

III.4.2.2LACP 'Link Aggregation Control Protocol'.

LACP est un protocole standardisé par IEEE, (802.3ad) très similaire à PAgP. La seule différence est le nom des modes de port. Nous retrouvons donc deux modes de ports :

Passif (mode par défaut) : le port attend les paquets LACP du port voisin pour y répondre, sans aucune négociation.

Actif : le port négocie avec le port voisin.

Tableau 5:fonctionnemnt de LACP

LACP	Actif	Passif
Actif	Compatible	Compatible
Passif	Compatible	Non compatible

L'aggregation des liens est représnteé dans la figure 22 ci-dessus :

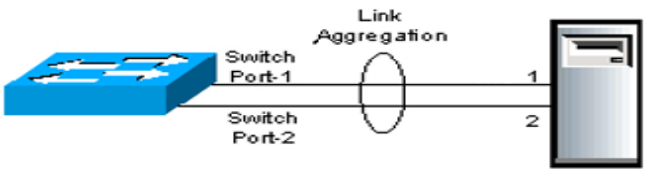


Figure 21: Une application de l'agrégation de liens.

A noter que si nous ne voulons pas utiliser de protocole de négociation, le port devra être mis en mode ON, pour forcer l'agrégation de lien.

III.5 Segmentation des VLANS.

Un VLAN est un Réseau Local Virtuel regroupant un ensemble de machines de façon logique et non physique. En définissant une segmentation logique (logiciel basé sur un regroupement de machine à des critères tel que l'adresse MAC.[9]

III.5.1 Avantage de VLAN.

Le VLAN permet de définir un nouveau réseau au-dessus de réseau physique à ce titre offre les avantages suivants :

- Plus de souplesse pour l'administration et les modifications des réseaux.
- Gain en sécurité car les informations sont encapsulé dans un niveau supplémentaire et éventuellement analysé.
- Réduction de la diffusion de trafic sur le réseau.

III.5.2 VLAN Natif.

Certaines trames véhiculées sur un trunk ne sont pas marquées d'un tag dot1q. Alors il faut pouvoir les placer quelque part. C'est là qu'intervient le vlan natif.

Le vlan natif, est le vlan dans lequel sont véhiculées les trames non taguées dot1q. Donc si un switch reçoit sur une interface trunk une trame Ethernet standard, il la placera dans ce vlan natif, en quelque sorte, un vlan par défaut (de marquage).

La figure 23 représente comment sont véhiculée les trames d'un vlan natif.

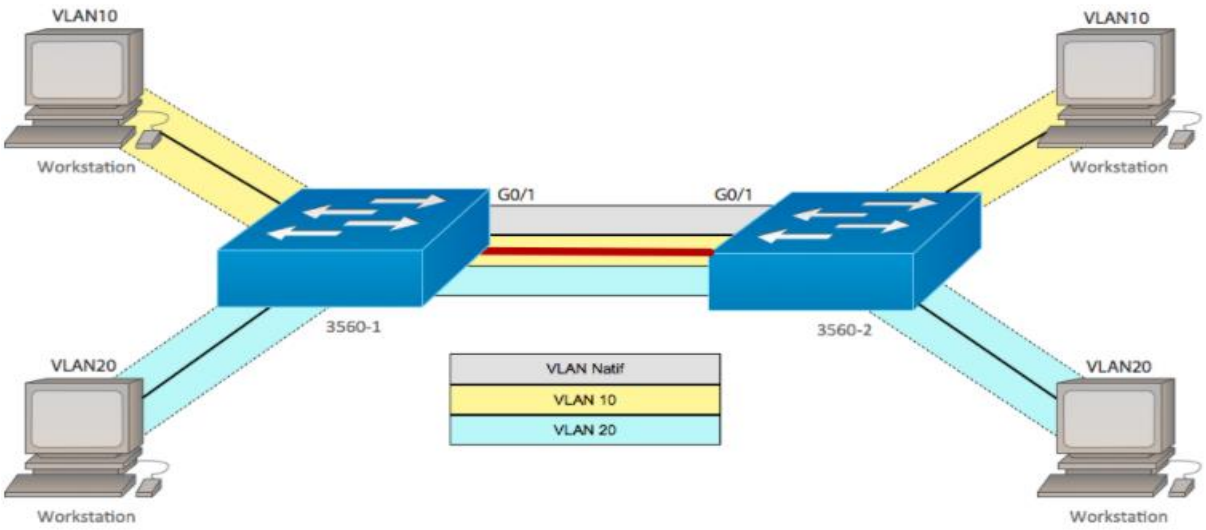


Figure 22: VLAN Natif.

III.5.2.1 Avantage de VLAN natif

Il est toujours bon d'utiliser un VLAN autre que VLAN1 comme VLAN natif pour les raison de sécurité, il est utilisé pour prendre en charge et transporter le trafic non balisé (tagué) comme CDP et DTP (protocole de gestion).Pour séparer le trafic envoyé par les appareils vers les différents PC.

Cela offre plus de flexibilité.

Lorsqu'il est configuré sur 802.1Q sur un commutateur Cisco, il est alors possible de définir

II.5.3 VLAN Voice

Dans les réseaux Ethernet basés sur IP, le VLAN Voice est essentiel pour assurer la qualité de la transmission des données vocales. Autrement dit, lorsque d'autres services (données, vidéo, etc.) sont transmis simultanément, le service vocal sera priorisé et transmis avec une priorité d'acheminement plus élevée.

La figure 24 montre comment sont véhiculée les trames d'un VLAN Voice

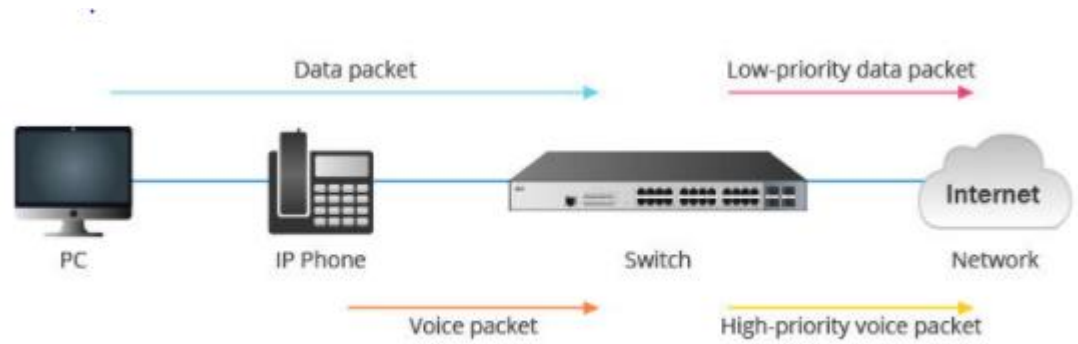


Figure 23: VLAN Voice

III.6 Sécurité et conception VLAN

III.6.1 MAC Attaque

Chaque carte réseau Ethernet possède une adresse MAC qu'il identifie univoquement ni au moins au hacker peut usurpe cette adresse MAC.

III.6.2ARP Attaque

Le protocole ARP 'Address Resolution Protocol', sert a réalisé la table de correspondance entre les adresse MAC et adresse IP.

Ce type d'attaque permet au hacker d'usurper l'identité d'un ou plusieurs autres stations afin de capturer le trafic qui lui associe.

III.6.3DHCP Snooping

La hacker fait un sort de jouer le rôle de serveur d'adressage réseau.

III.6.4Spanning Tree Attaque

Ce protocole est utilisé par un commutateur qui sert à éviter qu'une boucle de communication ou diffusion ne soit créé (tempête de diffusion).

Une autre attaque sur ce protocole consiste pour le hackeur à envoyer des messages particuliers BPDU (Bridge Protocole Data Unit) pour devenir le commutateur racine (maitre).

III.7 Routage

Pour savoir le chemin à emprunter parmi tous les liens pour aller d'un réseau A à un réseau B, il faut qu'un protocole de routage ait été mis en place. Le but du routage est de définir une route ou un chemin à un paquet quand celui-ci arrive sur un routeur.

III.7.1 Routage statique

Dans le routage statique, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes (par l'intermédiaire de port de sortie ou d'IP de destination) à emprunter pour aller sur tel ou tel réseau.

III.7.2 Routage dynamique

Un protocole de routage est un ensemble de processus, d'algorithmes et de messages utilisés pour échanger des informations de routage, qui seront utilisées pour remplir la table de routage avec les meilleurs chemins vers les destinations sur le réseau.

III.7.2.1Types de routage dynamique

III.7.2.1.1 EIGRP «Enhanced Interior Gateway Routing Protocol »

Le protocole de routage dynamique propriétaire Cisco est un protocole de routage dynamique intérieur hautement fonctionnel. Il est appelé protocole de vecteur de distance hybride ou avancé, il permet de contrôler finement la métrique de manière à influencer les entrées de la table de routage. EIGRP est alors capable de répartir la charge de trafic sur des liaisons à coûts inégaux.

III.7.2.1.1.2 OSPF (Open Shortest Path First)

C'est un protocole standard ouvert, à état de lien permettent une convergence rapide. Contrairement au protocole EIGRP qui lui, est propriétaire Cisco, donc il ne fonctionne que sur des routeurs Cisco. La version utilisée est l'OSPFv2

III.7.2.1.1.2.1 Caractéristiques du protocole OSPF:

- Convergence rapide les mises à jour sont incrémentielles.
- Utilisé dans les grands réseaux.
- Les aires OSPF sont hiérarchisées, l'aire 0 est obligatoire.
- Authentification possible sous OSPF.
- C'est un protocole ouvert.

III.7.2.1.1.3 RIP

Un protocole de routage à vecteur de distance est utilisé principalement sur de petits réseaux, il converge lentement.

III.7.2.2 Avantages de routage dynamique

- Le routage dynamique présente les avantages suivants.
- Une maintenance réduite par l'automatisation des échanges et des décisions de routage
- Une modularité et une flexibilité accrue, il est plus facile de faire évoluer le réseau avec un réseau qui se met à jour automatiquement.
- Sa performance et sa mise en place ne dépendent pas de la taille du réseau

III.8 Routage Inter VLAN

Les hôtes dans un VLAN ont besoin de communiquer avec des hôtes dans un autre VLAN, le trafic doit être conduit entre eux. Ceci est appelé « Routage inter- VLAN ».

Le routage inter-VLAN est un processus qui permet de transférer du trafic réseau d'un VLAN à un autre à l'aide d'un périphérique de couche 3.

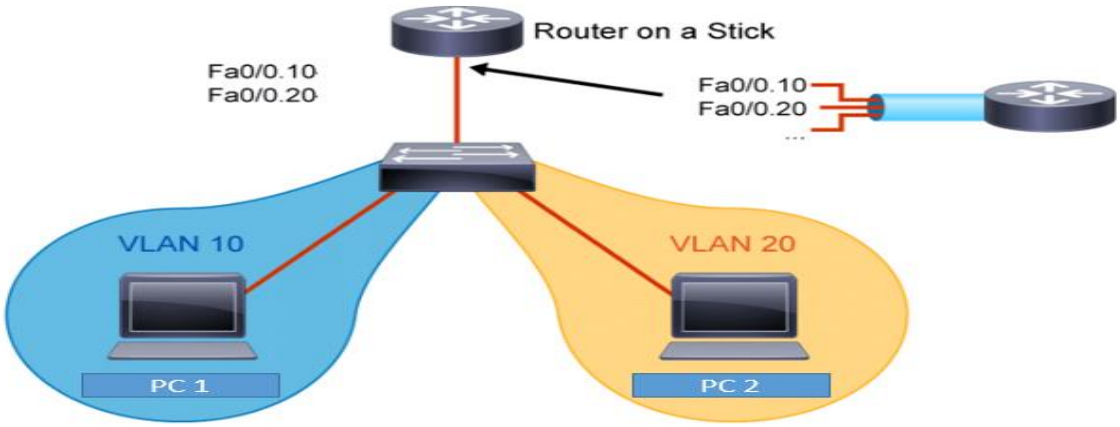
III.8.1 Router on a Stick

C'est un type de configuration dans lequel une seule interface physique relie le trafic entre plusieurs VLAN sur un réseau.

Le routeur effectue le routage inter-VLAN à l'aide de ses sous-interfaces. Chacune de ses sous-interfaces est configurée indépendamment avec une adresse IP.

Les sous-interfaces sont configurées pour différents sous-réseaux correspondant à leur affectation VLAN (dans l'Exemple, Fa0/0.10 pour le vlan 10 et Fa0/0.20 pour le vlan 20).

La figure 25 montre comment 2 vlan sont reliés par une seule interface



.

Figure 24: Router on a stick.

III.9 VLAN Trunking Protocol (VTP).

La création de VLAN sur plus d'un switch peu devenir fastidieuse. VTP, qui est un protocole propriétaire Cisco permet de propager les VLAN sur les différents switch. Son avantage principal est sa capacité de propager automatiquement des VLAN configurés sur un commutateur en mode 'server' vers les autres commutateurs configurés en mode 'client'.

Pour qu'il y'ait propagation, il faut configurer les switch en conséquence.

III.9.1 Les modes de configuration de VTP

Il existe 3 modes de configuration pour le VTP :

- **Mode server :** c'est, généralement le switch sur lequel l'administrateur effectue les modifications. Il autorise le switch à envoyer des mises à jour VTP au client VTP,
- **Mode client :** c'est le mode qui va recevoir les mises à jour VTP,
- **Mode transparent :** si le switch est configurer sur ce mode, il ne mettra pas de ses VLAN à jour via VTP, cependant il transmet les informations VTP à ces voisins.

III.10 Spanning Tree STP

Spanning Tree Protocol est un protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle (appelée algorithme de l'arbre recouvrant) dans les LAN avec ponts. Il est défini dans la norme IEEE 802.1D et est basé sur un algorithme décrit par Radia Perlman en 1985.

III.10.1 Objectif de STP

Les réseaux commutés de type Ethernet doivent avoir un chemin unique entre deux points, cela s'appelle une topologie sans boucle. En effet, la présence de boucle génère des tempêtes de diffusion qui paralysent le réseau : tous les liens sont saturés de trames de diffusion qui tournent en rond dans les boucles et les tables d'apprentissage des commutateurs (switch) deviennent instables.

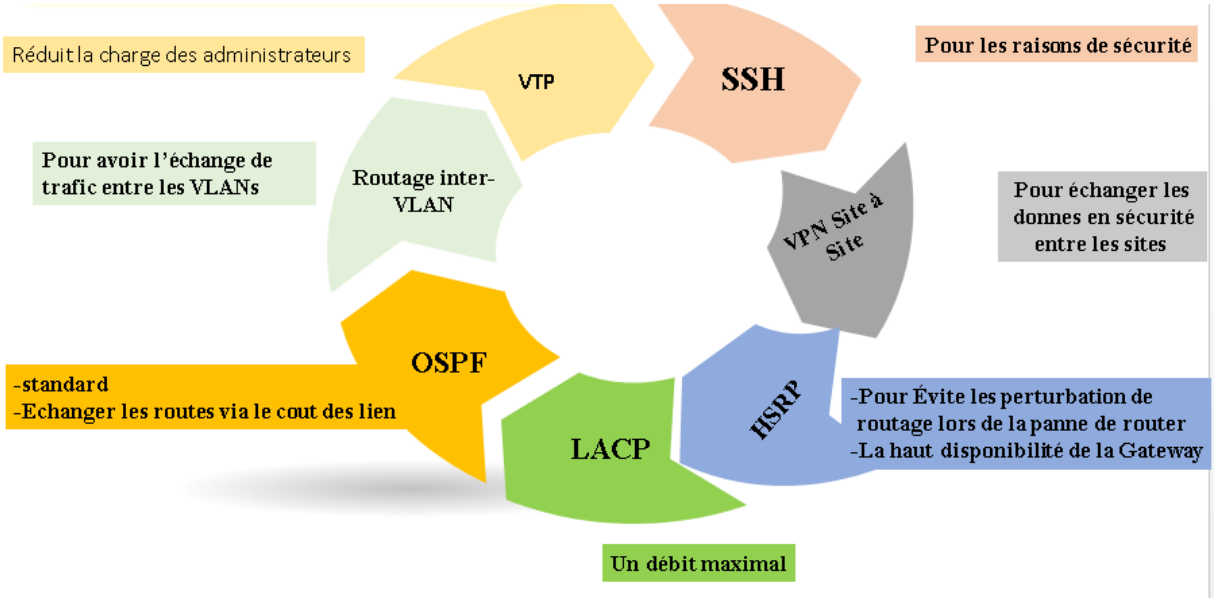
Une solution serait de ne pas tirer les câbles en surnombre de manière à ne pas avoir de boucles dans le réseau. Néanmoins, un bon réseau doit aussi offrir de la redondance pour proposer un chemin alternatif en cas de panne d'une liaison ou d'un commutateur. L'algorithme de SpanningTree garantit l'unicité du chemin entre deux points du réseau tout en n'interdisant pas les câbles en surnombre. Pour cela, il bloque administrativement certains ports des commutateurs

III.10.2 Mode de fonctionnement

L'algorithme STP procède en plusieurs phases :

- élection du commutateur racine.
- détermination du port racine sur chaque commutateur.
- détermination du port désigné sur chaque segment.
- blocage des autres ports.

III.11 Les solutions adapter dans notre simulation



Conclusion

Dans ce chapitre, nous avons appris à mieux comprendre la structure et l'organisation du réseau de la RTC de Bejaïa, et voire les les solutions adéquates et les objectifs à atteindre.

Introduction

Ce présent chapitre consiste à mettre en œuvre les solutions proposées pour la réalisation de notre projet, en exposant les différentes configurations nécessaires à implémenter sur le LAN. Ces configurations entourent entre la configuration des VLANs, VTP, STP, LACP, HSRP, OSPF et le routage inter vlan en suit on a configuré le serveur de voix Asterisk et le serveur de gestion et administration (AD), en fin la partie sécurité et VPN en se basant sur le logiciel open source GNS 3 et l'hyperviseur VMware Workstation. Pour présenter les configurations que nous avons réalisées, nous nous sommes servies des captures d'écran qui illustrent les étapes de la configuration afin d'éclaircir chaque composant de cette dernière et son fonctionnement. Enfin, des tests de validation sont effectués pour confirmer le bon fonctionnement du réseau seront réalisés.

IV.1 Présentation de l'architecture réseau après la configuration

La figure suivante illustre l'architecture réseau que nous avons réalisée sous le logiciel GNS3 :

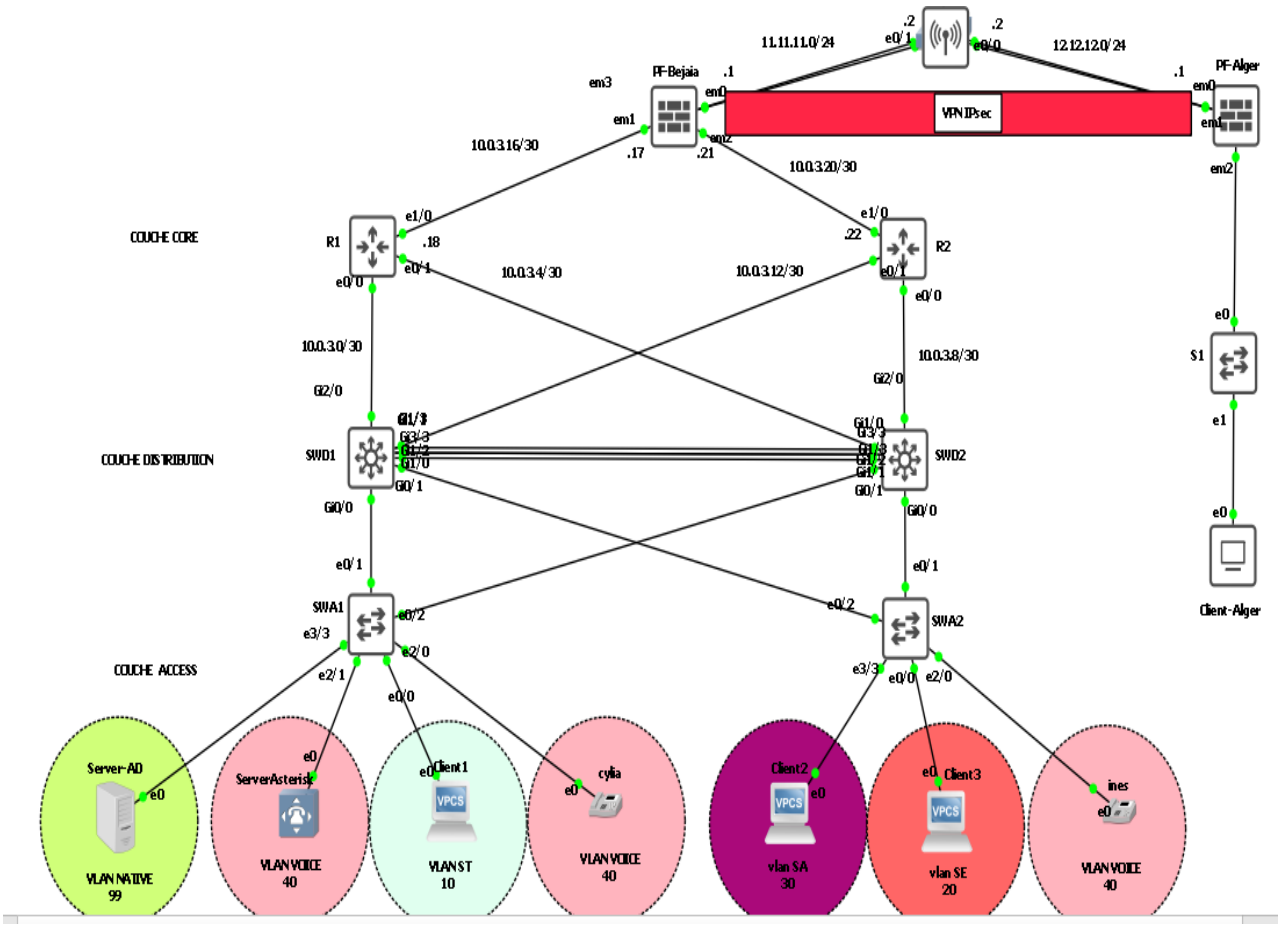


Figure 25: Architecture proposée.

IV.2 Plan d'adressage

Tableau 6:Le plan d'adressage

DEVICE	INTERFACE	IP ADDRESS	MASQUE	DESCRIPTION	PASSEREL
INTERNET					
ROUTER INTERNET	Eth 0 Eth 0/1	11.11.11.2 12.12.12.2	255.255.255.0 255.255.255.0	Connecté à pfsense-bejaia Connecté à pfsense-alger	/ /
SITE ALGER					
PFSENS	Em0 Em1	12.12.12.1 172.16.0.1	255.255.255.0 255.255.255.0	Connecté à internet Connecté au Lan alger	12.12.12.2 /
CLIENT	ETH 0	DHCP	/	Client lan alger	/
SITE BEJAIA					
PFSENSE	Em0 Em1 Em2	11.11.11.1 10.0.3.17 10.0.3.21	255.255.255.0 255.255.255.252 255.255.255.252	Connecté à internet Connecté à router 1 Connecté à router 2	11.11.11.2 / /
ROUTER1	Eth 0/0 Eth 0/1 Eth 0/2	10.0.3.1 10.0.3.5 10.0.3.18	255.255.255.252 255.255.255.252 255.255.255.252	Connecté à swd1 Connecté à swd2 Connecté à pfsense	/ / /
ROUTER2	Eth 0/0 Eth 0/1 Eth 0/3	10.0.3.9 10.0.3.13 10.0.3.22	255.255.255.252 255.255.255.252 255.255.255.252	Connecté à swd2 Connecté à swd1 Connecté à pfsense	/ / /
SWD1	G 2/0 G 3/3 Svi 10 Svi 20 Svi 30 Svi 40 Svi 99	10.0.3.2 10.0.3.14 10.10.10.1 10.10.20.1 10.10.30.1 10.10.40.1 10.10.99.1	255.255.255.252 255.255.255.252 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connecté à router 1 Connecté à router 2 Connecté au lan st Connecté au lan Se Connecté au lan Tea Connecté au lan Voice Connecté au lan admin	/ / / / / / /
SWD2	G 2/0 G 3/3 Svi 10 Svi 20 Svi 30 Svi 40 Svi 99	10.0.3.10 10.0.3.6 10.10.10.2 10.10.20.2 10.10.30.2 10.10.40.2 10.10.99.2	255.255.255.252 255.255.255.252 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Connecté à router 2 Connecté à router 1 Connecté au lan st Connecté au lan Se Connecté au lan Tea Connecté au lan Voice Connecté au lan admin	/ / / / / / /
SWA1	Svi 99	10.10.99.3	255.255.255.0	/	10.10.99.250
SWA2	Svi 99	10.10.99.4	255.255.255.0	/	10.10.99.250
SERVER-AD	Eth 0	10.10.99.200	255.255.255.0	Server ad-dhcp-dns	10.10.99.250
ASTERISK	Eth 0	10.10.40.11	255.255.255.0	Server voice	10.10.40.250
CLIENT 1	Eth 0	DHCP	/	Connecté vlan 10	/
CLIENT 2	Eth 0	DHCP	/	Connecté vlan 30	/
CLIENT 3	Eth 0	DHCP	/	Connecté vlan 20	/
INESS	Eth 0	DHCP	/	Connecté vlan voice	/
CYLIA	Eth 0	DHCP	/	Connecté vlan voice	/

IV.3 Installation du GNS3

GNS3 est un logiciel open source gratuit distribué sous la licence publique générale GNU version 3.

L'assistant de configuration GNS3 s'affiche. Cliquer sur Suivant > pour démarrer l'installation

Les figures ci-dessus montrent les étapes d'installation du GNS3 figure27

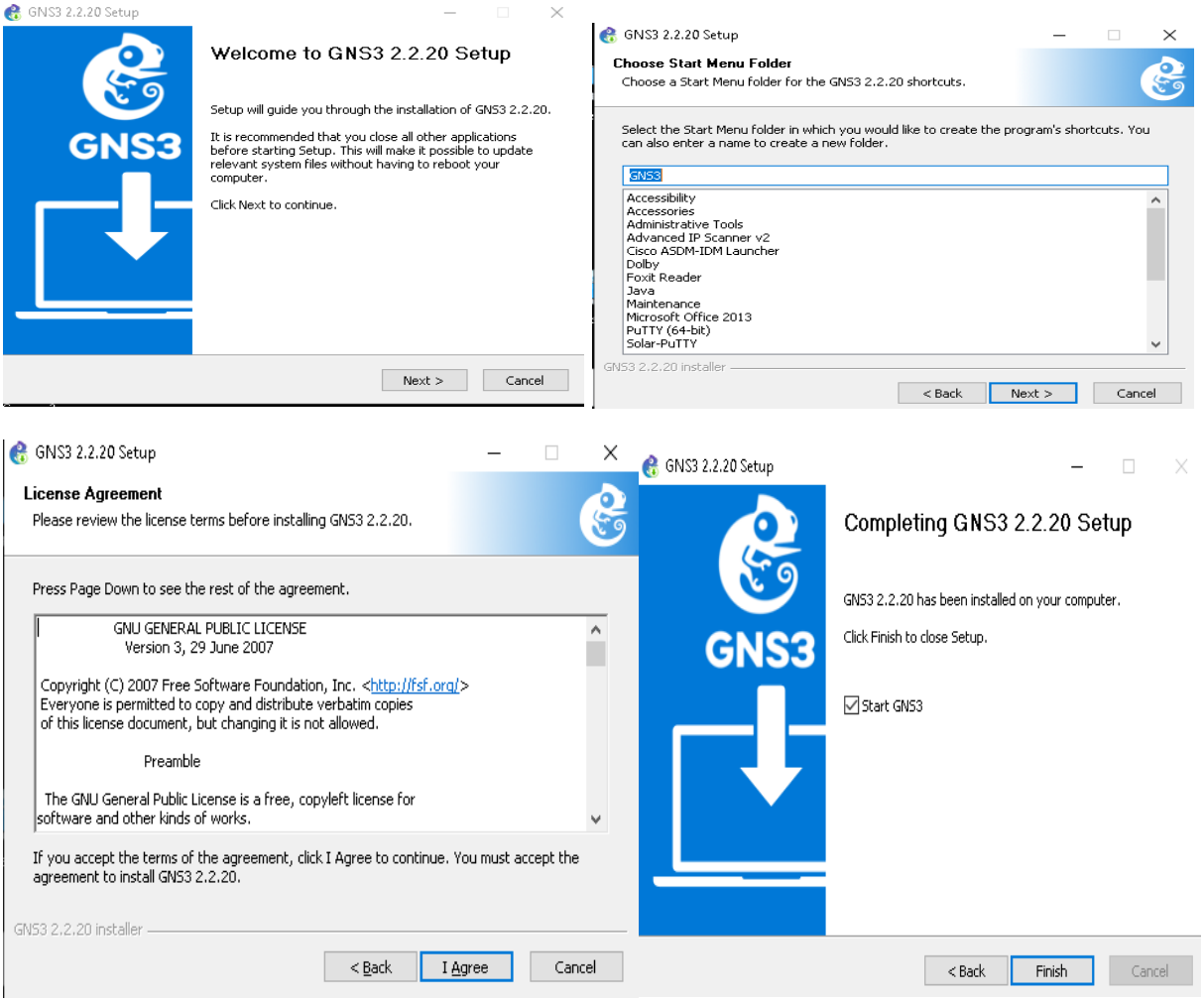
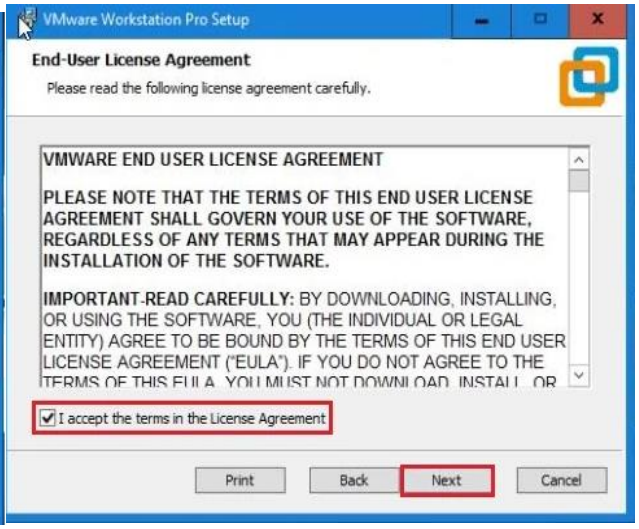


Figure 26: installation du GNS3.

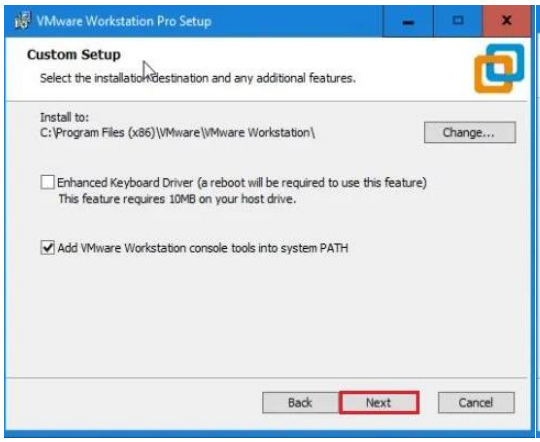
IV.4 Installation du VMware Workstation pro 16

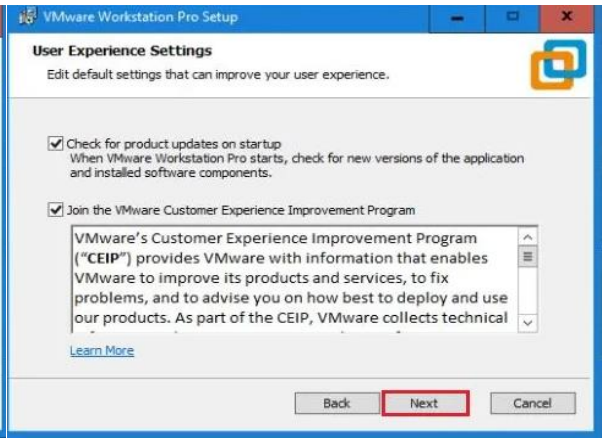
C'est un hyperviseur de type 2, on peut dire qu'il s'agit d'un outil de virtualisation qui permet à plusieurs systèmes d'exploitation de fonctionner simultanément sur une même machine physique. Théoriquement, c'est une couche logicielle très légère qui permet d'allouer un maximum de ressources physiques aux machines virtuelles.

Bienvenue dans l'assistant VMware Workstation, cliquez sur suivant



Configuration de VMware Workstation Pro, cliquez sur suivant.





IV.5Vérification de la configuration du serveur VTP

L'ensemble des commutateurs de distribution de LAN seront configurés comme des serveurs -VTP. Donc, ce sont eux qui gèrent l'administration de l'ensemble des VLANs. Un nom de domaine est attribué.

VTP (Virtual Trunking Protocol) est un protocole propriétaire Cisco servant à maintenir la base de données de VLANs sur plusieurs commutateurs de manière cohérente.

Sur les deux (2) switches de distribution, on réalise la configuration suivante.

La figure 28 montre la vérification de la configuration du serveur VTP

```
SWD1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sonatrach.lan
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0500
Configuration last modified by 0.0.0.0 at 7-11-21 12:23:07
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        : 5
Configuration Revision          : 2
MD5 digest                      : 0x05 0x60 0x92 0xC8 0xD5 0x96 0xEE 0x56
                                  0x18 0xFA 0xF0 0xE8 0xE5 0x20 0x52 0x1A
```

Figure 27:Vérification de la configuration du serveur VTP

.

IV.6 Vérification de la configuration du VTP client.

La figure 29 montre la vérification des VLAN du switch VTP client

```
SWA4#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : sonatrach.lan
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0700
Configuration last modified by 0.0.0.0 at 7-5-21 23:07:17

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 10
Configuration Revision          : 12
```

Figure 28: Vérification des VLAN sur le switch VTP client.

Une fois les VLANs sont créé ils seront redistribué aux switches d'Access (vtp client)

Vérification sur la figure 30

```
SWA4#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Et0/2, Et0/3, Et1/0, Et1/1
                                                   Et1/2, Et1/3, Et2/0, Et2/1
                                                   Et2/2, Et2/3
10   ST                                  active
20   SA                                  active
30   SE                                  active
40   voice                               active
99   native                              active
1002 fddi-default                        act/unsup
1003 trcrf-default                       act/unsup
1004 fddinet-default                     act/unsup
1005 trbrf-default                       act/unsup
```

Figure 29: Vérification des VLAN sur VTP client

IV.7 Vérification de la création des VLANs

Sur la figure31

```
SWD1#show  vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/2, Et3/3
10   ST                               active
20   SA                               active
30   SE                               active
40   voice                            active
99   Native                           active
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 trcrf 101003     4472  1005   3276   -        -    srb      0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
```

Figure 30: vérification des VLANs

.

IV.8Vérification des ports “Trunk”

Un port dit “Trunk” est un port qui transporte le trafic appartenant à plusieurs VLANs.

Les interfaces des équipements d’interconnexion à configurer en mode trunk, existent toutes entre l’ensemble des commutateurs Accès et le commutateur core. Les commandes suivantes nous permettent d’associer un port à un VLAN en mode trunk en s’aidant de la commande ‘range ‘qui pourra réunir toutes les interfaces en une seule fois.

Vérification sur la Figure 32 :

```
SWA1#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      99
Et0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Et0/0       10,20,30,40,99
Et0/1       10,20,30,40,99
```

Figure 31: Vérification des ports.

IV.9 Vérification d'un port "Trunk"

Dans cette sortie fournie par la commande show interfaces trunk, on prendra connaissance du mode DTP de l'interface ("on", "dynamic auto", "desirable", "nonegociate"), du protocole d'encapsulation ("802.1q"), le statut et le numéro du VLAN natif sur le Trunk.

La figure 33 montre les interfaces trunk

```
SWD1#show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      99
Et0/2       on               802.1q         trunking      99
Et0/3       on               802.1q         trunking      99
Et1/0       on               802.1q         trunking      99
```

Figure 32:vérification des interfaces trunk.

Vérificationl'assignation de port au VLAN 40.

Pour la sécurité et bonnes pratique STP on utilise la commande portfast, c'est une fonctionnalité propriétaire Cisco. Elle s'exécute uniquement sur des ports connectant des périphériques terminaux et dans une infrastructure VLAN uniquement sur des ports en mode Access.

Assigniez le VLAN VOICE '40' au interfaces.

L'assignation de ports au VLAN 40 est représentée sur la figure 34

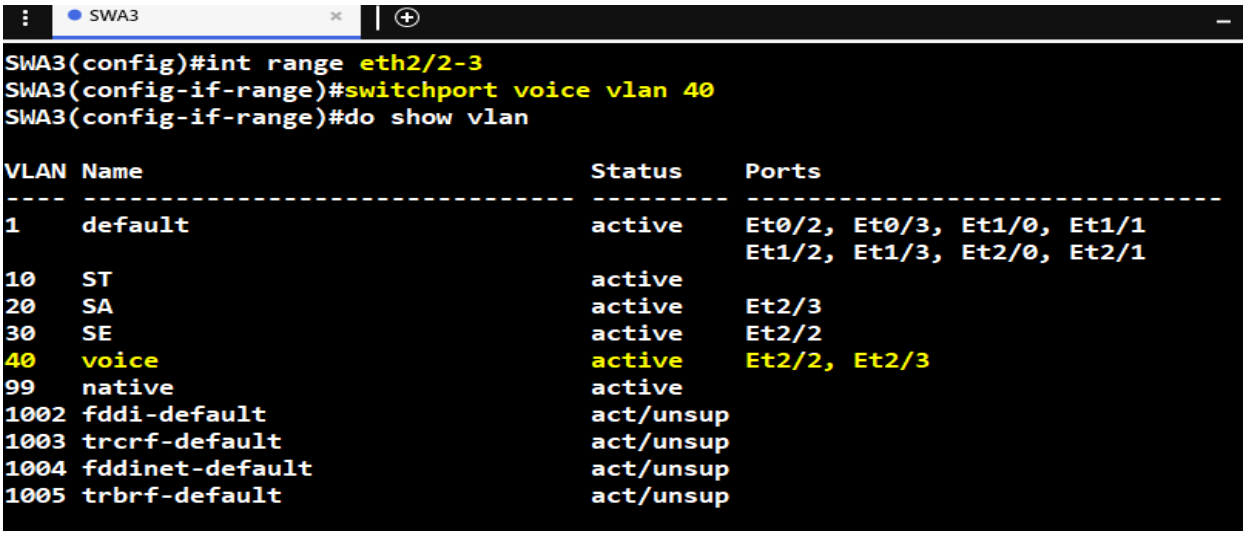


Figure 33: vérification l'assignation de ports au VLAN 40.

IV.10 Configuration manuel des ports Access

Par défaut, un port physique d'un commutateur est un "switchport", configuré en mode "dynamic auto" mais il opère en mode Access.

Les paramètres switchport sont représentés sur la figure 35

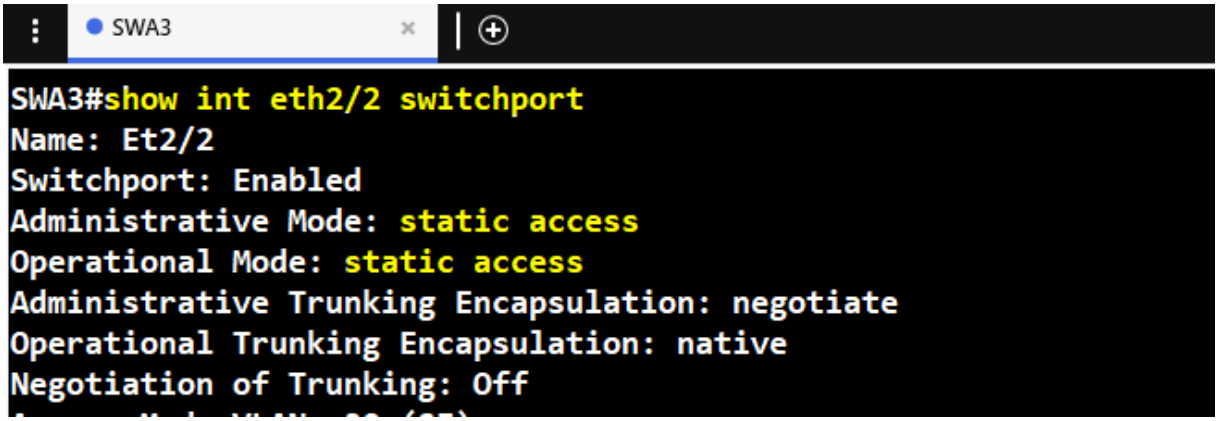


Figure 34: Vérification des paramètres switchport

IV.10 Vérification de la configuration etherchannel

```
SWD1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Et2/0(P)    Et2/1(P)    Et2/2(P)
                                 Et2/3(P)
```

Figure 35: vérification de la configuration SWD1

```
SWD2#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Et2/0(P)    Et2/1(P)    Et2/2(P)
                                 Et2/3(P)
```

Figure 36: vérification de la configuration SWD2

IV.11 Vérification des interfaces SVI (Switch Virtuel Interface)

A l'aide de la commande show IP interface brief.

```
Vlan10                 10.10.10.1      YES NVRAM  up                    up
Vlan20                 10.10.20.1      YES NVRAM  up                    up
Vlan30                 10.10.30.1      YES NVRAM  up                    up
Vlan40                 10.10.40.1      YES NVRAM  up                    up
Vlan99                 10.10.99.1      YES NVRAM  up                    up
SWD1#
```

Figure 37: vérification des SVI SWD1

```
Vlan10                 10.10.10.2      YES NVRAM  up                    up
Vlan20                 10.10.20.2      YES NVRAM  up                    up
Vlan30                 10.10.30.2      YES NVRAM  up                    up
Vlan40                 10.10.40.2      YES NVRAM  up                    up
Vlan99                 10.10.99.2      YES NVRAM  up                    up
```

Figure 38: vérification des SVI SWD2

IV.12 Vérification de protocole HSRP

Comme dans les commandes de configuration d'interface du protocole HSRP, on retrouve le mot-clé standby dans show standby.

```
SWD1#SH STANDBY
SWD1#SH STANDBY
Vlan10 - Group 10
  State is Active
    2 state changes, last state change 00:47:44
  Virtual IP address is 10.10.10.250
  Active virtual MAC address is 0000.0c07.ac0a (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.384 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
  Group name is "hsrp-Vl10-10" (default)
Vlan20 - Group 20
  State is Active
    2 state changes, last state change 00:22:19
  Virtual IP address is 10.10.20.250
  Active virtual MAC address is 0000.0c07.ac14 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.904 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 110 (configured 110)
```

Figure 39: vérification de la configuration de HSRP SWD1

```
SWD2(config)#DO SH STANDBY
Vlan10 - Group 10
  State is Standby
    7 state changes, last state change 00:23:03
  Virtual IP address is 10.10.10.250
  Active virtual MAC address is 0000.0c07.ac0a (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.032 secs
  Preemption disabled
  Active router is 10.10.10.1, priority 110 (expires in 9.632 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl10-10" (default)
Vlan20 - Group 20
  State is Standby
    1 state change, last state change 00:28:33
  Virtual IP address is 10.10.20.250
  Active virtual MAC address is 0000.0c07.ac14 (MAC Not In Use)
    Local virtual MAC address is 0000.0c07.ac14 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.600 secs
  Preemption disabled
  Active router is 10.10.20.1, priority 110 (expires in 8.912 sec)
```

Figure 40: Vérification de la configuration de HSRP SWD2

IV.13 Vérification de Spanning Tree.

La configuration de l'équilibrage de charge de VLAN qui vient de terminer optimise l'utilisation des liaisons redondantes entre deux switch de distribution La conservation des valeurs STP par défaut engendre la terminaison de toutes les liaisons redondantes entre les deux switch distribution en mode de blocage. L'ajustement de la priorité STP permet à plusieurs liaisons d'être utilisées en même temps, pour différents VLAN. Ceci augmente la bande passante globale disponible entre les deux périphériques. En cas de panne d'un lien, STP redistribue les VLAN dans les liaisons restantes au moment où il reconverge.

Voici un court résumé de la configuration : Le commutateur Distribution SWD1 est configuré pour devenir un pont racine principal pour les VLAN 10,20 et le pont racine secondaire pour les VLAN 30, 40,99.

```
spanning-tree vlan 10,20 priority 24576
spanning-tree vlan 30,40,99 priority 28672
SWD1#
```

Figure 41: Vérification de Spanning Tree sur SWD1

Le commutateur Distribution SWD2 est configuré pour devenir un pont racine principal pour les VLAN 30, 40, 99 et le pont racine secondaire pour les VLAN 10, 20

```
spanning-tree vlan 10,20 priority 28672
spanning-tree vlan 30,40,99 priority 24576
SWD2#
```

Figure 42: Vérification de Spanning Tree sur SWD2

IV.14 Sécurisé l'architecture

IV.14.1 Vérification des ports de sécurité

Cette fonction permet de contrôler les adresses MAC autorisées sur un port. En cas de "violation", c'est-à-dire en cas d'adresses MAC non autorisées sur le port, une action est prise.[10]

```
SWA1(config)#
*Aug 28 18:42:54.712: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/3, put
ting Et0/3 in err-disable state
SWA1(config)#
*Aug 28 18:42:54.747: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 0050.7966.6802 on port Ethernet0/3.
SWA1(config)#
*Aug 28 18:42:55.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, chan
ged state to down
*Aug 28 18:42:56.752: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to down
SWA1(config)#
```

Figure 43: Vérification d'état du port en violation

IV.14.2 DHCP Snooping

Afin d'empêcher le DHCP Snooping, l'idée est de préciser où trouver les bons serveurs DHCP. Pour cela, nous allons travailler sur le switch et préciser sur quel port se trouver les serveurs DHCP authentiques, est de spécifier que c'est un port dit "trusted" (port de confiance). Ainsi, les ports "trusted" pourront emmètre des requêtes DHCP Offer et DHCP Ack alors que l'équipement du pirate informatique ne sera pas sur un port de confiance (unstrusted). Ses requêtes seront alors bloquées.

```
SWA1(config)#ip dhcp snooping
SWA1(config)#ip dhcp snooping database disk0
SWA1(config)#ip dhcp snooping vlan 10,20,30,40,99
SWA1(config)#int eth1/0
SWA1(config-if)#ip dhcp snooping trust
SWA1(config)#no ip dhcp snooping information option
```

Figure 44:Configuration DHCP Snooping

IV.14.3 BPDU Guard

BPDU est synonyme de Pont Protocol Data Unit, qui est un paquet de donnée, envoyé sur les réseaux locaux ou LAN, qui travaille pour détecter les boucles dans un réseau. Les boucles peuvent provoquer des paquets de données en double pour être envoyés, ce qui peut prendre de la bande passante sur un réseau. BPDU Guard est utilisée pour protéger la topologie STP de couche 2 contre les attaques liées aux BPDU.

```
SWA1(config-if)#spanning-tree bpduguard enable
SWA1(config-if)#spanning-tree portfast
```

Figure 45:Configuration du BPDU Guard.

IV.14.4 Passive interface

Cette commande indique à OSPF de ne pas envoyer de paquets Hello sur certaines interfaces.

```
SWD2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWD2(config)#router ospf 1
SWD2(config-router)#passive-interface default
SWD2(config-router)#
*Aug 28 23:31:48.835: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on GigabitEthernet2/0 from
 FULL to DOWN, Neighbor Down: Interface down or detached
*Aug 28 23:31:48.845: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on GigabitEthernet3/3 from
 FULL to DOWN, Neighbor Down: Interface down or detached
*Aug 28 23:31:48.848: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Vlan10 from FULL to DOW
N, Neighbor Down: Interface down or detached
*Aug 28 23:31:48.850: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Vlan20 from FULL to DOW
N, Neighbor Down: Interface down or detached
*Aug 28 23:31:48.852: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Vlan30 from FULL to DOW
N, Neighbor Down: Interface down or detached
*Aug 28 23:31:48.855: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Vlan40 from FULL to DOW
N, Neighbor Down: Interface down or detached
*Aug 28 23:31:48.858: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Vlan99 from FULL to DOW
N, Neighbor Down: Interface down or detached
SWD2(config-router)#no passive-interface gi2/0
SWD2(config-router)#no passive-interface gi3/3
SWD2(config-router)#
*Aug 28 23:32:58.247: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on GigabitEthernet3/3 from
 LOADING to FULL, Loading Doned
```

Figure 46:Configuration de la passive interface.

IV.14.5 Optimisation du protocole HSRP

Cette optimisation désigne le processus de répartition d'un ensemble de tâches sur un ensemble de ressources, dans le but d'en rendre le traitement global plus efficace. Les techniques de répartition de charge permettent à la fois d'optimiser le temps de réponse pour chaque tâche, tout en évitant de surcharger de manière inégale les nœuds de calcul.

```
SWD1(config-if)#int vlan 30
SWD1(config-if)# standby 30 priority 100
SWD1(config-if)#int vlan 40
SWD1(config-if)# standby 40 priority 100
SWD1(config-if)#int vlan 99
SWD1(config-if)# standby 99 priority 100
```

Figure 47:Optimisation du HSRP sur SWD1.

```
SWD2(config)#int vlan 30
SWD2(config-if)#standby 30 priority 150
SWD2(config-if)#standby 30 preempt
SWD2(config-if)#int vlan 40
SWD2(config-if)#standby 40 priority 150
SWD2(config-if)#standby 40 preempt
SWD2(config-if)#int vlan 99
SWD2(config-if)#standby 99 priority 150
SWD2(config-if)#standby 99 preempt
```

Figure 48:Optimisation du HSRP sur SWD2.

IV.14.6 Sécuriser les ports inutilisés

Les ports non utilisés sur un switch peuvent constituer un risque pour la sécurité. Une personne malveillante pourrait se brancher sur un port du switch non utilisé et ainsi accéder au réseau.

Une méthode simple est de désactiver tous les ports non utilisés et les mettre dans un vlan non utilisé.

Sur SWA1

```
SWA1(config)#int range eth0/3,eth1/0-3,eth2/2-3,eth3/0-2
SWA1(config-if-range)#switchport access vlan 100
SWA1(config-if-range)#switchport mode access
```

Figure 49: Sécurisé les ports sur SWA1

Vérification de la sécurisé des ports sur SWA

```
SWA1(config)#do sh vlan br

VLAN  Name                             Status    Ports
----  -------------------------------- --------- -------------------------------
1     default                          active    Et0/2
10    st                               active    Et0/0
20    SE                               active
30    SA                               active
40    voice                            active    Et2/0, Et2/1
99    native                           active    Et3/3
100   sec                              active    Et0/3, Et1/0, Et1/1, Et1/2
                                                 Et1/3, Et2/2, Et2/3, Et3/0
                                                 Et3/1, Et3/2
```

Figure 50: Vérification de la sécurisé des ports sur SWA1

IV.14.7 Sécurisation de l'accès à distance SSH

Il est possible de lancer une connexion SSH ou Telnet à l'aide d'un client comme Putty qui est installé sur son PC.

Vérification de la configuration du SSH.

```
SWD1#ssh -l ines 10.10.99.4
Password:
SWA2>en
Password:
% Password:  timeout expired!
Password:
Password:
SWA2#
```

Figure 51: Vérification de la configuration du SSH.

IV.15 Serveur de voix Asterisk

IV.15.1 Introduction

En 2002, le projet Asterisk sort au grand jour et fait son entrée dans un marché encore naissant. C'est un PBX (Private Branch eXchange) logiciel qui propose des fonctionnalités avancées pour une somme dérisoire car la (bonne) surprise est que sa licence GPL (donc projet libre et open-source). D'abord utilisé plus ou moins expérimentalement, il commence à convaincre peu à peu les entreprises de toute taille. Asterisk est un serveur téléphonique IP (PBX-IP) open source capable de concurrencer des systèmes commerciaux tels que les Call Manager de Cisco System.

IV.15.2 Fonctionnement du serveur Asterisk

Asterisk fournit tous les services de base d'un PABX comme la connexion des postes entre eux (qu'ils soient locaux ou distants), la messagerie unifiée, les services Web intégrés (ex: annuaire, gestion salle de conférence, etc.), le service de répondeur interactif, la musique d'attente, interconnexion avec le réseau téléphonique public, etc.

Asterisk est basé sur le plan de numérotation, le but du PABX grâce au plan de numérotation est de trouver le canal de sortie il peut être le même canal SIP dans le cas d'un appel en VoIP à l'intérieur du bâtiment, Ce canal de sortie peut également être un des autres types de canaux géré par Asterisk. Les contextes servent à réduire (ou augmenter) les possibilités de sortie d'un appel. Cela peut par exemple servir pour autoriser les appels à l'international pour certains utilisateurs.

IV.16 Protocole SIP

Protocole de signalisation de vidéo et voix sur IP est basé sur des messages en clair et fonctionn sur le port 5600 en TCP et UDP.

IV.16.1 Installation

Démarrer la machine à partir du CD GoAutoDial et appuyez sur Entrée pour commencer.

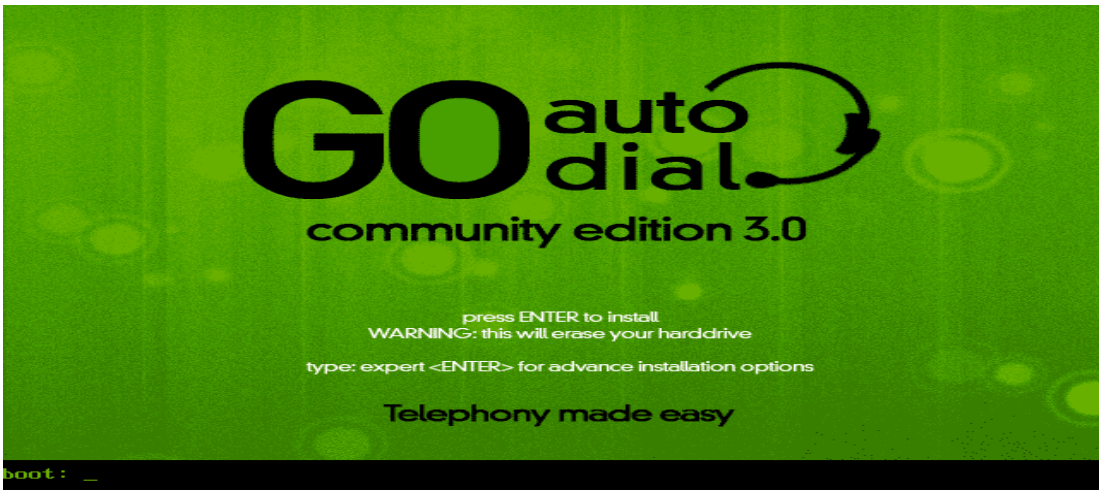


Figure 52: page d'accueil de GoAutoDial

L'installateur automatisé s'occupe de tout, il vous suffit donc d'attendre environ 15 minutes en fonction de votre matériel pour que l'ensemble du processus d'installation se termine

Entrez votre mot de passe root souhaité

Figure 53: installation de GoAutoDial

Installation complète! Retirer le CD d'installation puis appuyez sur ENTER pour redémarrer. Après le redémarrage, vous devez exécuter une mise à jour. Tapez "yum update" sur votre console (voir image ci-dessous). Une fois la mise à jour terminée, redémarrez votre serveur.

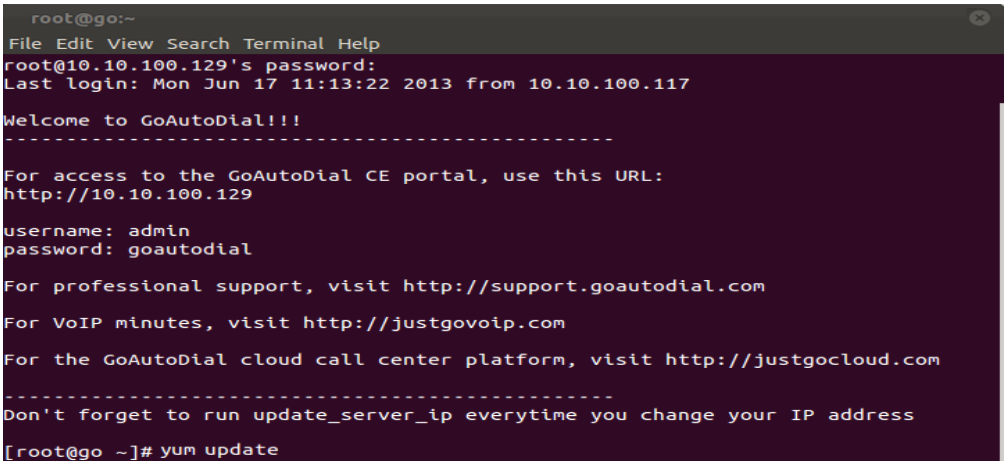


Figure 54: installation complète de GoAutoDial

Ouvrer votre portail GoAutoDial CE via un navigateur en mettant l'adresse IP dans la barre d'adresse.

Login : admin

Mot de passe : GoAutoDial|

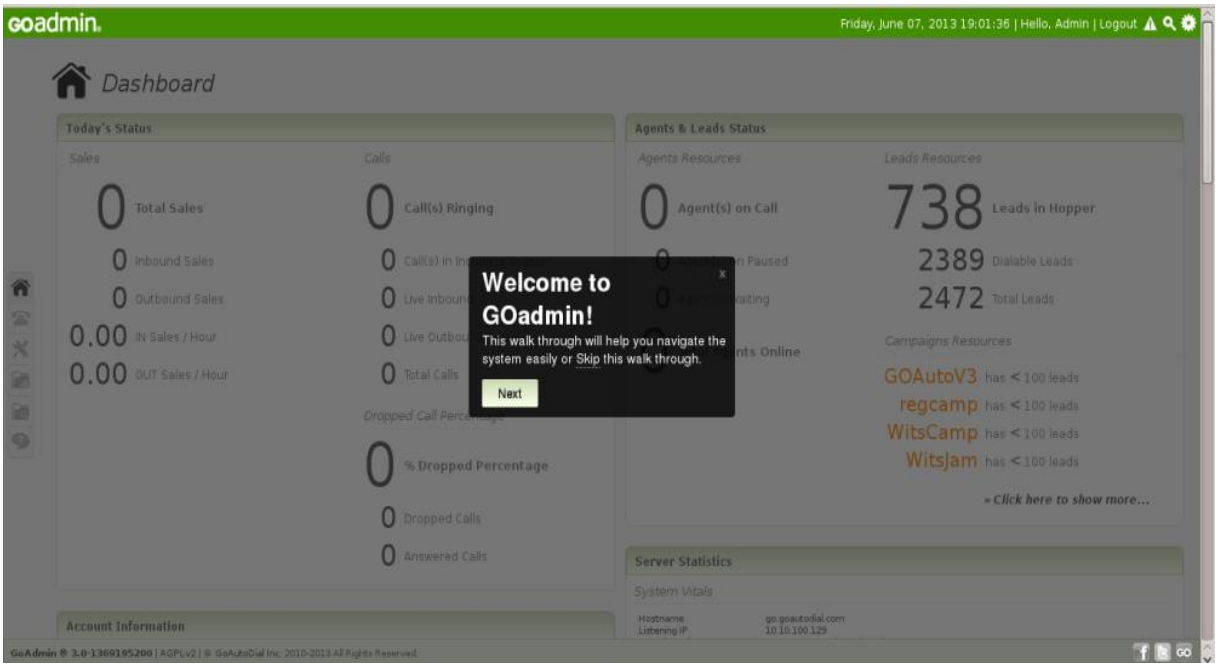


Figure 55: portail GoAutoDial

IV.17 EyeBeam

Ce logiciel a été créé en 2004, La première version est adaptée pour Windows.

Ce logiciel s'utilise aussi bien pour une simple conversation que pour une conférence

comprenant plusieurs personnes.

L'interface est facile à prendre en main et permet à n'importe quel utilisateur de bénéficier des fonctionnalités de ce logiciel.

Ce logiciel peut être utilisé par tout type d'utilisateur, malgré une interface légèrement plus complexe que certains autres softphones.

IV.17.1 Fonctionnalités de l'EyeBeam:

- Bénéficier de la conférence par appel vocal avec EyeBeam.
- Communiquer instantanément grâce à la fonctionnalité de la messagerie instantanée.
- Accéder aux appels vidéo et vidéo-conférence de qualité.
- Les services d'EyeBeam sont sécurisés et cryptés.
- Bénéficier du détail de la liste de vos appels et de votre historique d'appels.
- EyeBeam vous permet de rediriger les appels en cas d'absence ou de déplacement.
- Possibilité renvoyer les appels vers un poste fixe.
- Vous pouver mettre un utilisateur en attente lors de conversation avec EyeBeam.

IV.17.2 Tester les appels à l'aide d'application EyeBeam

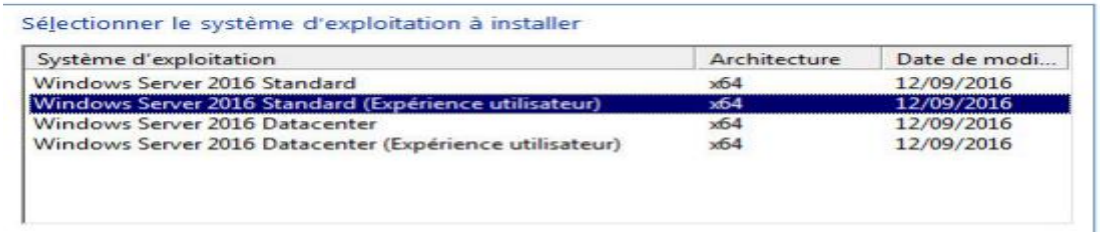
Test l'appel entre les utilisateurs.

Figure 56: Tester les appels à l'aide d'application EyeBeam

IV.18 Installation de Windows Server 2016 Standard.

- Installation de Windows : Faire le choix de la langue d'installation, puis on clique sur Suivant.
- Installation de Windows : On clique sur Installer Maintenant.

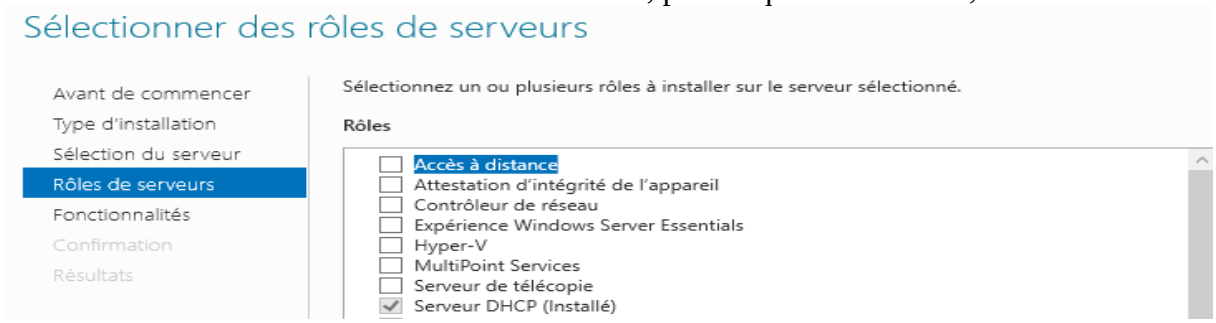
- Sélectionner le système d'exploitation à installer.



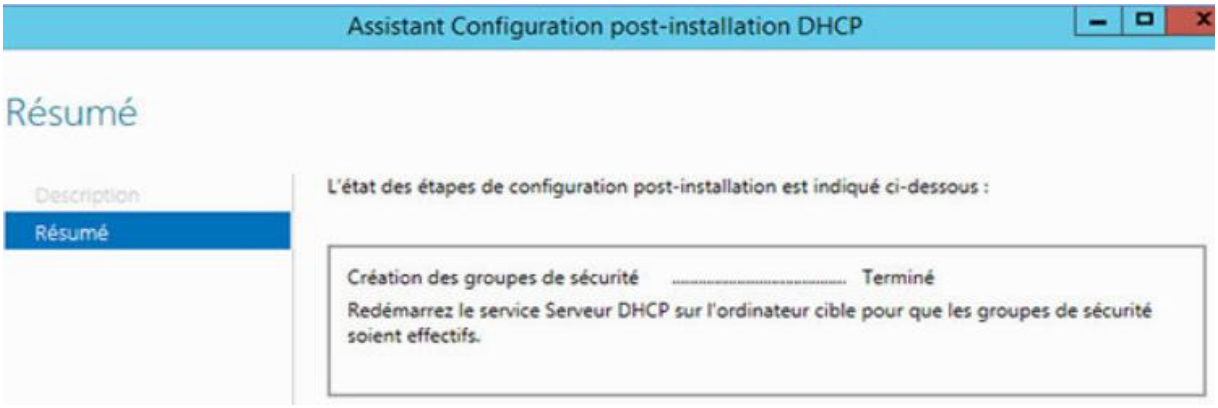
- Déverrouillage : appuyez sur Ctrl + Alt + Suppr.
- Entrer le mot de passe Administrateur.
- Résultat attendu :

IV.18.1 Installation du DHCP sur le Windows Server 2016

- Rôles de serveurs : Cochez Serveur DHCP, puis cliquez sur Suivant,

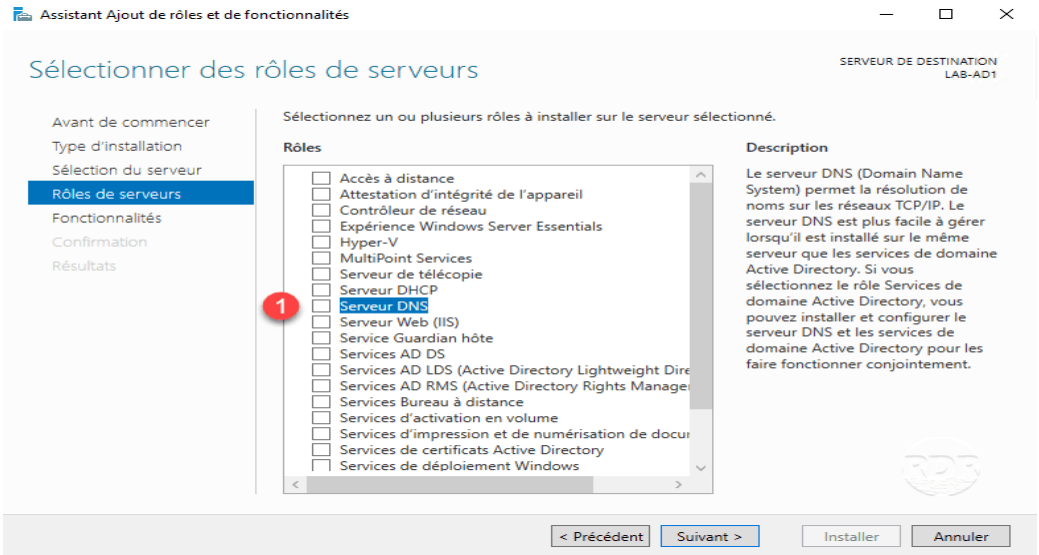


- Fin de l'installation du rôle DHCP.

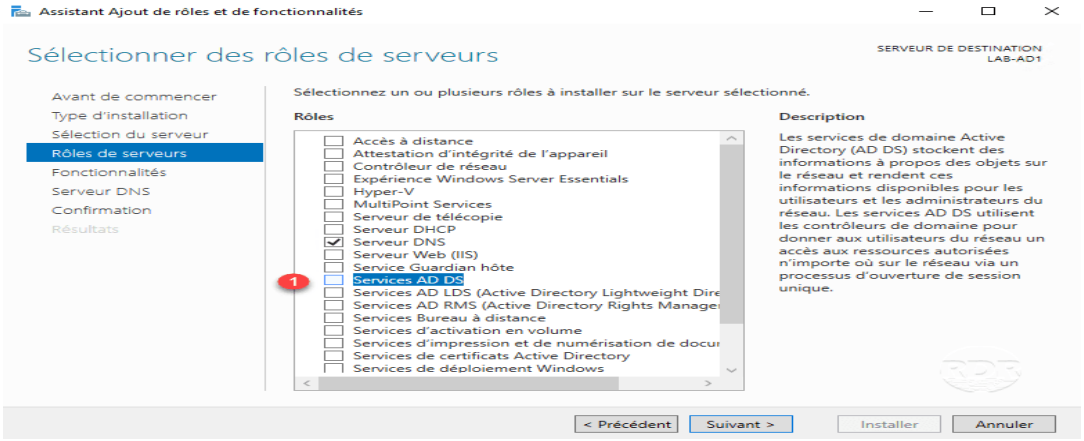


IV.18.2 Installation des rôles : contrôleur de domaine / DNS

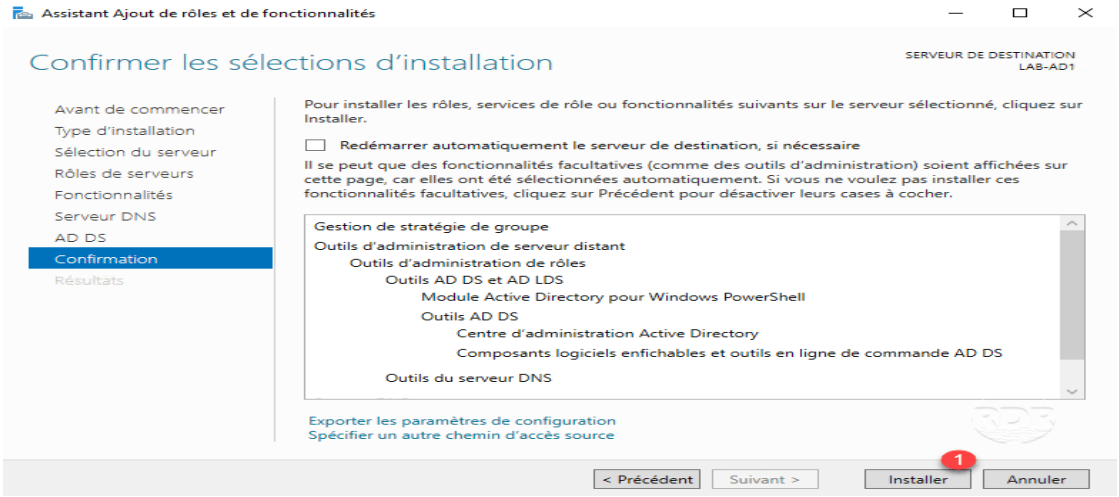
- Depuis le gestionnaire de serveur, cliquer sur Ajouter des rôles et des fonctionnalités
- Cocher le rôle Serveur DNS.



- Cocher le rôle : Services AD DS



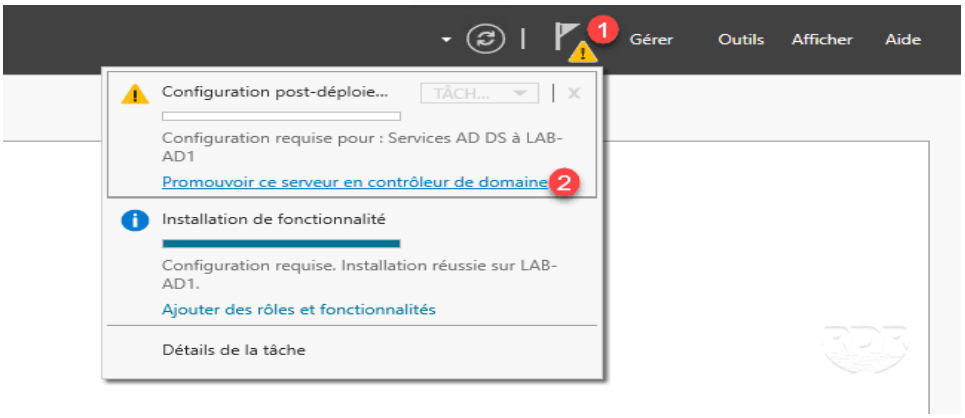
- Cliquer sur le bouton Installer



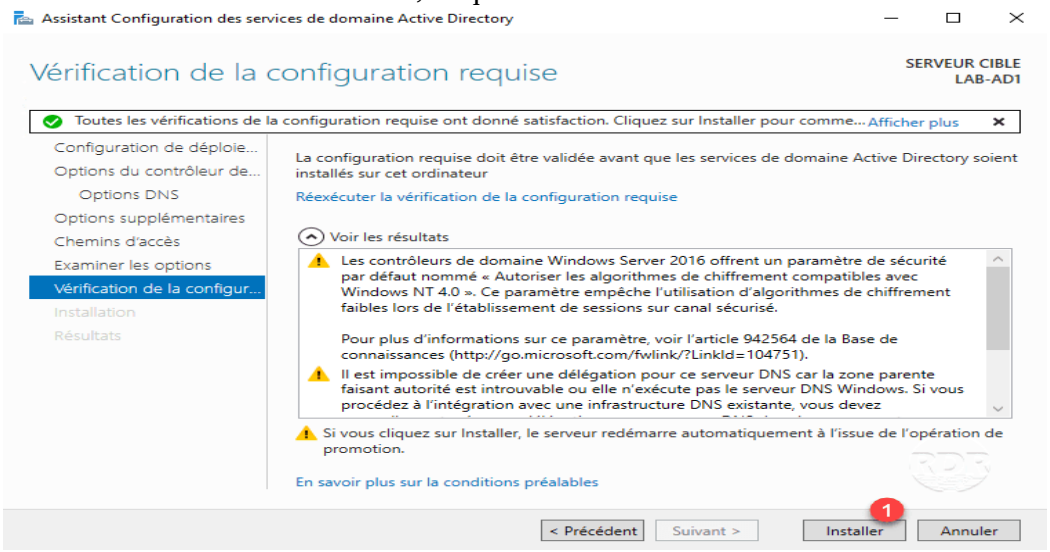
- Les rôles installés, quitter l'assistant en cliquant sur Fermer

IV.18.3 Promouvoir le serveur contrôleur de domaine

- Depuis le gestionnaire de serveur, cliquer sur l'icône de notification 1 puis sur le lien Promouvoir ce serveur en contrôleur 2 de domaine pour lancer l'assistant.

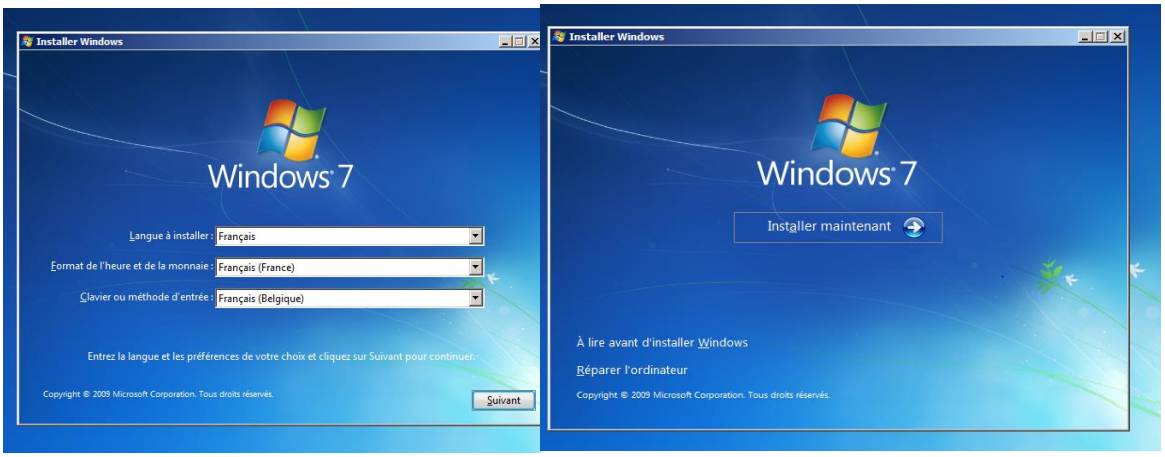


- Une fois les tests validés, cliquer sur Installer.



- Depuis le gestionnaire de serveur, vérifier que le serveur est bien membre du domaine

IV.20 Installation Windows 7



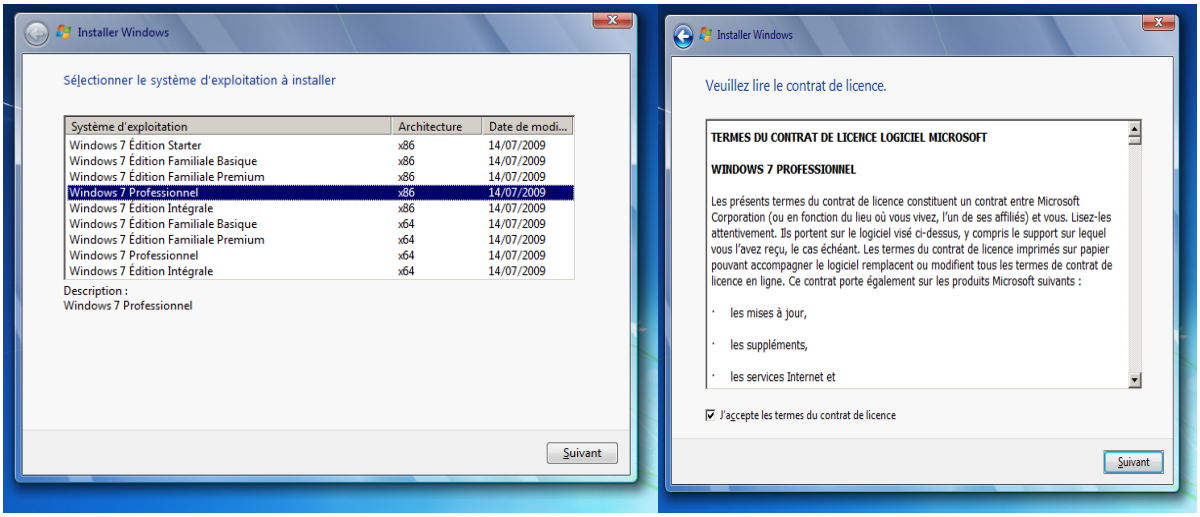


Figure 57: Installation Windows 7

IV.21 PfSense

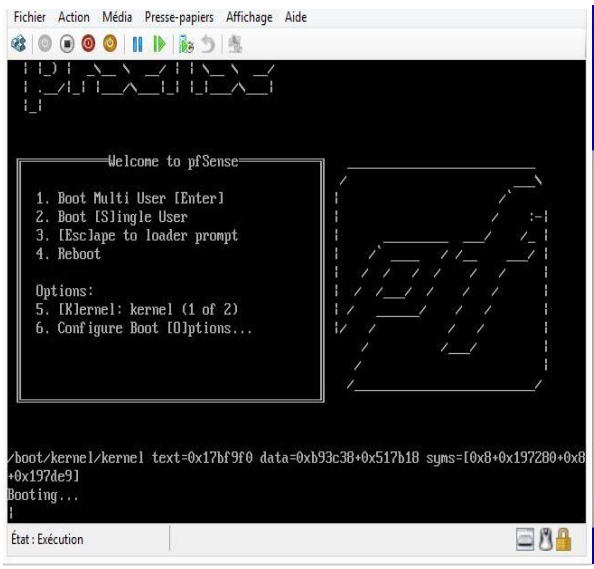
PfSense est un pare-feu open source à états, peut être configuré à l'aide de son interface web ou ligne de commande, support plusieurs futures comme le routage et NAT. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires.

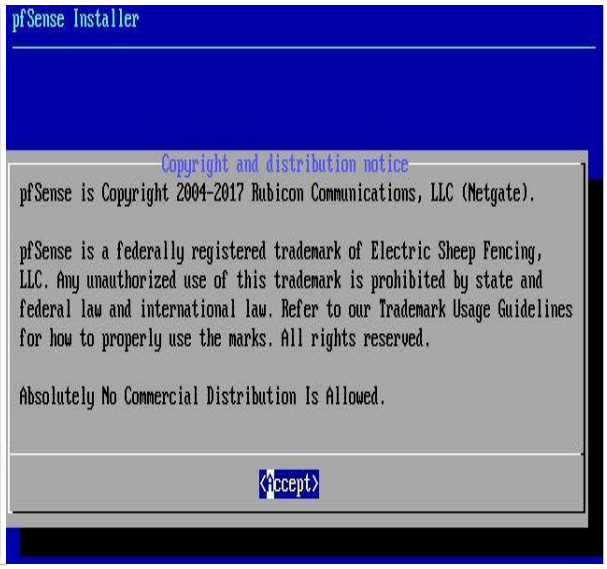
IV.21.1 Avantage de PfSense :

- Il est adapté pour une utilisation en tant que pare-feu et routeur
- Il comprend toutes les fonctionnalités des pare-feu coûteux commercialement
- Il offre des options de firewalling /routage plus évolué qu'IPCOP
- Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres
- Simplicité de l'activation / désactivation des modules de filtrage
- Système très robuste basée sur un noyau FreeBSD
- Des fonctionnalités réseaux avancées

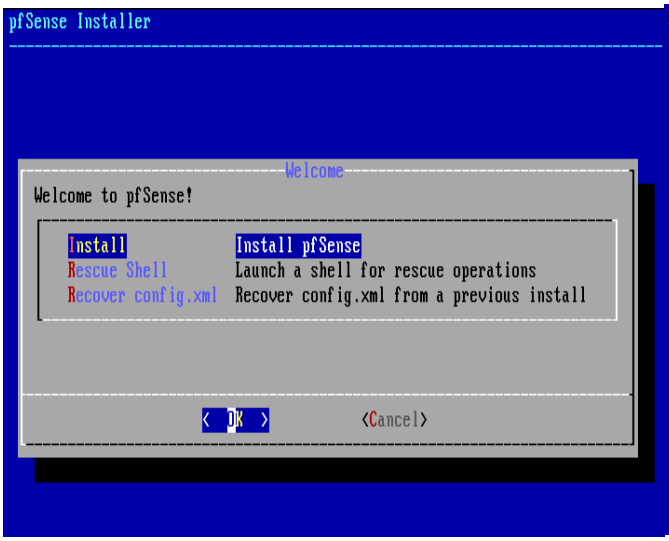
IV.21.2 Installation PFSense sur VMware

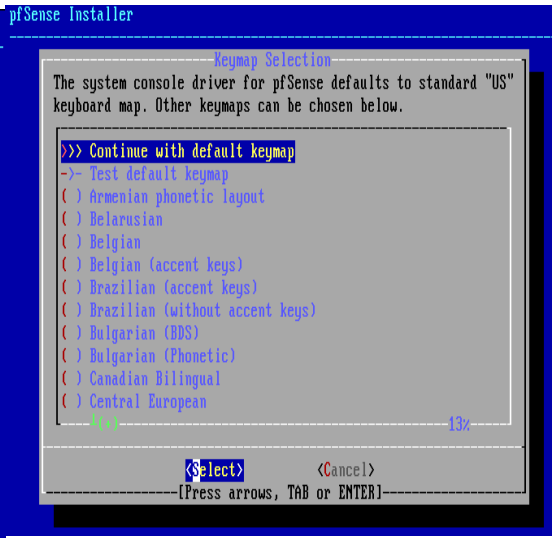
Démarrer la VM, Accepter la licence

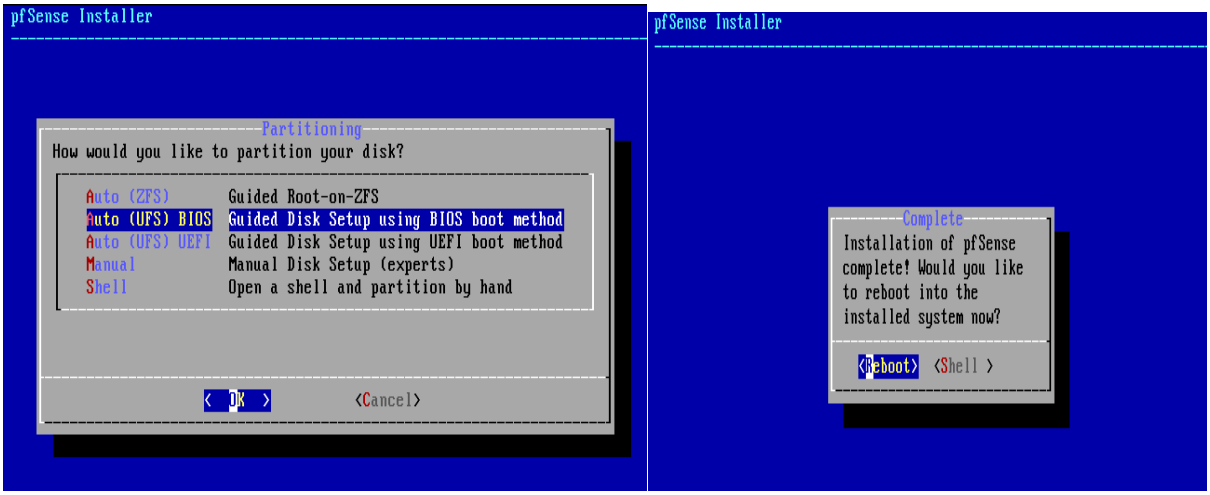




Install PFSense : OK







Vérification de la création des interfaces

Sur le PFSense de Bejaïa

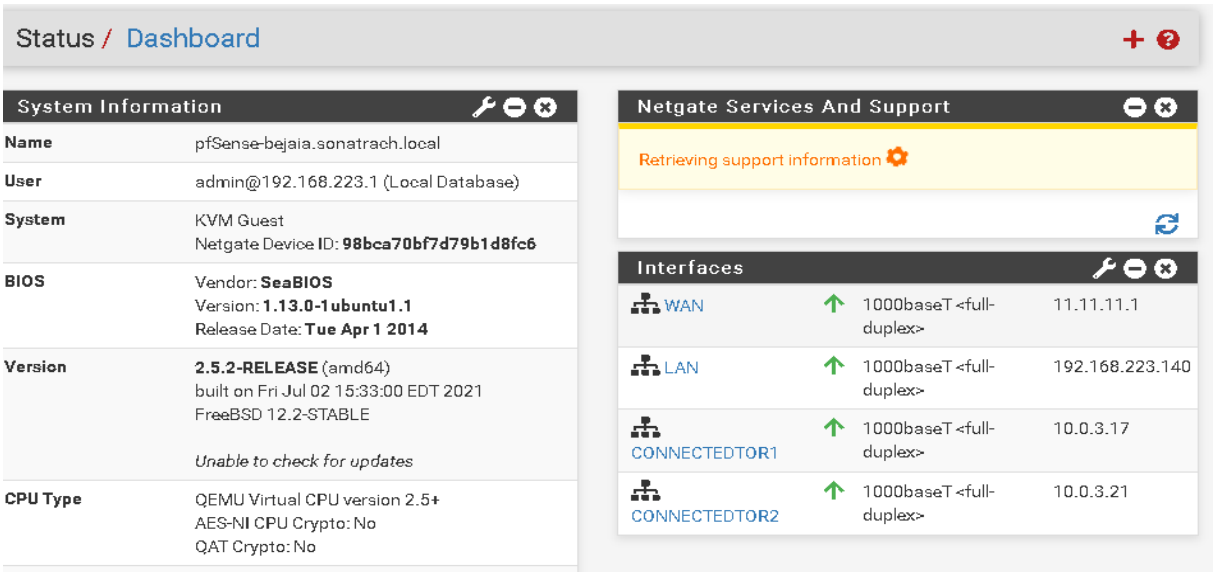


Figure 58: les interfaces sur PFSense Bejaïa

Sur le PFSense Alger

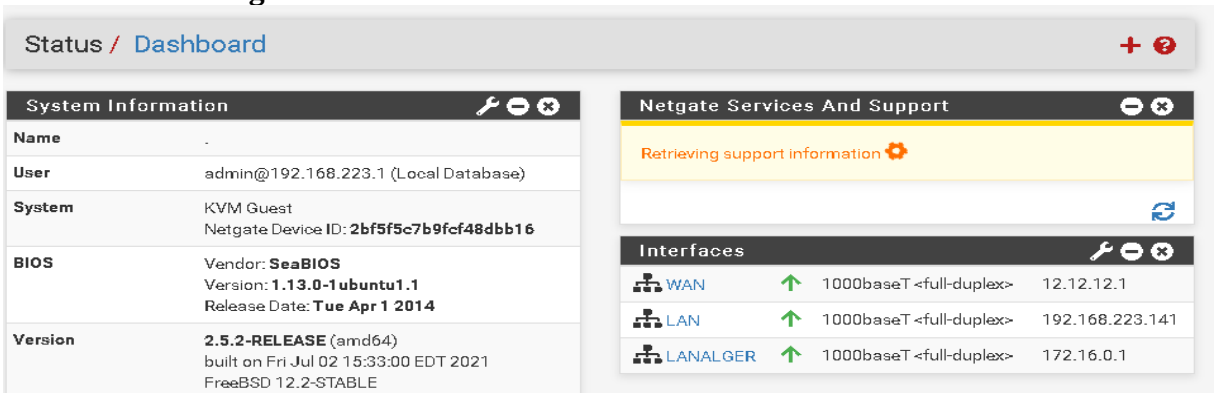
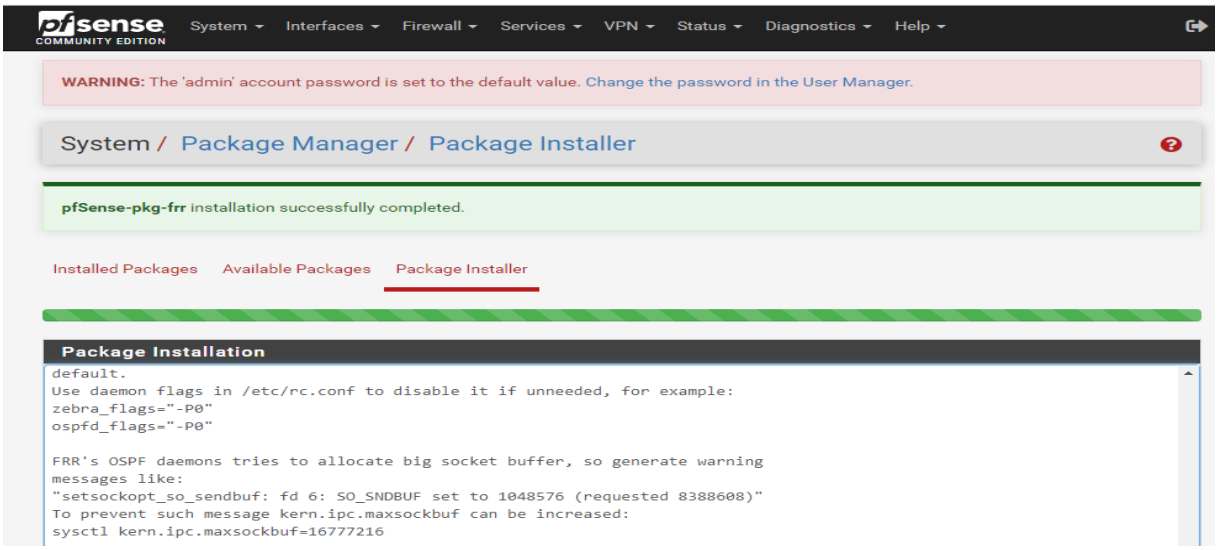


Figure 59: les interfaces sur PFSense Alger

IV.22Installation package FRR

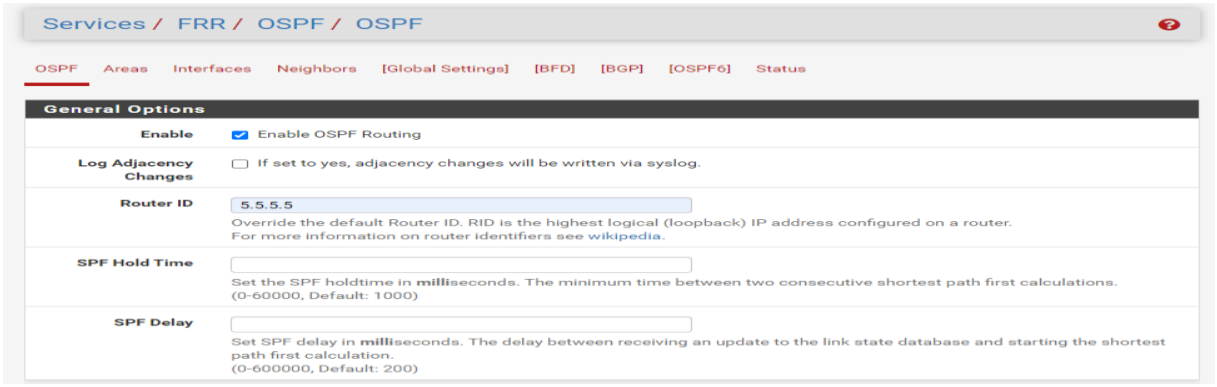
Package FRR est un outil qui dispose des protocoles de routage

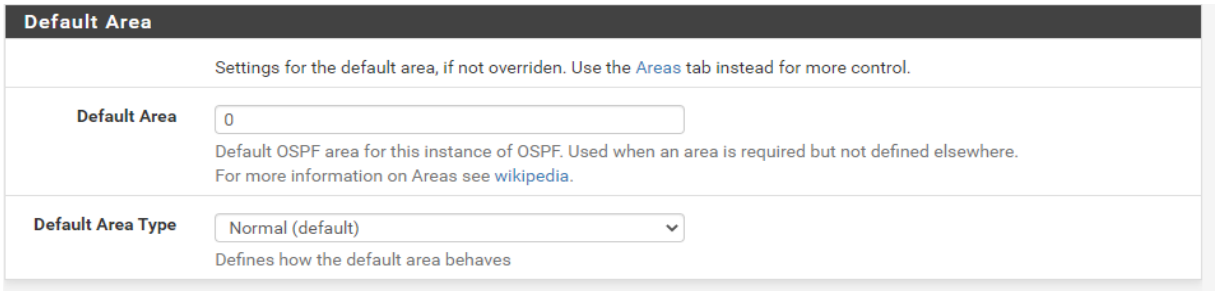


Configuration de l'OSPF

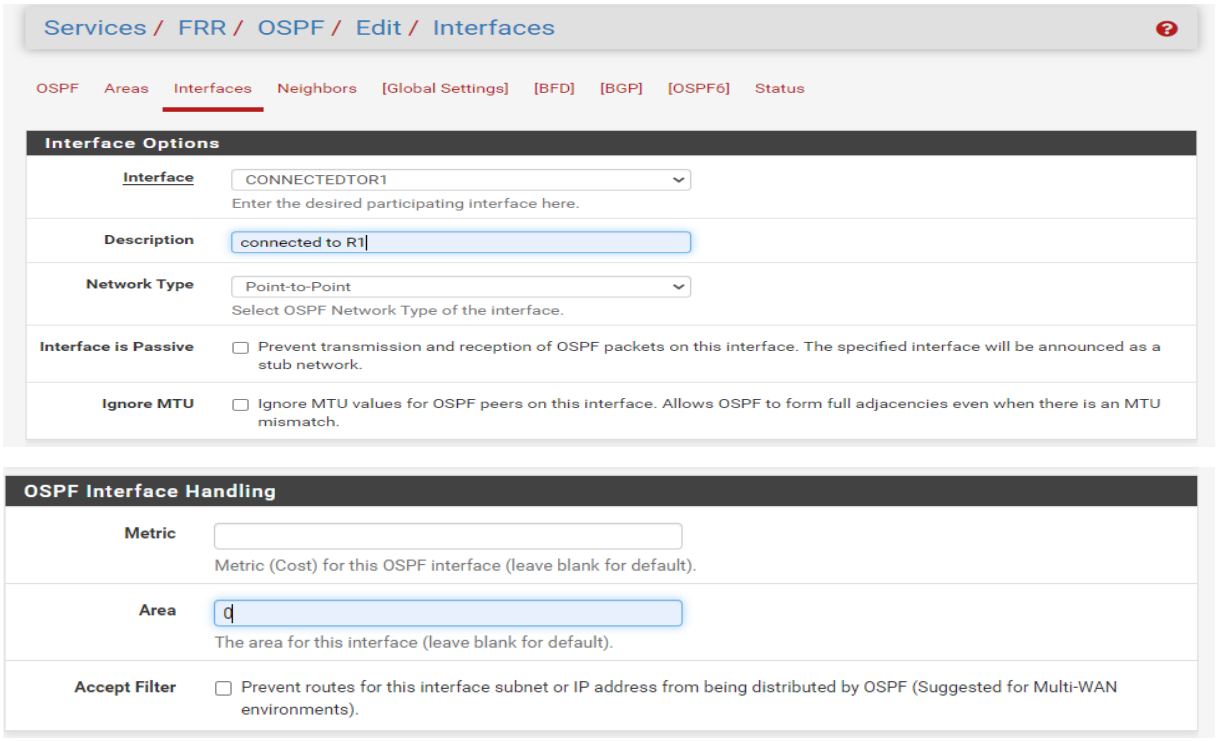
Activation du protocole OSPF

Configuration de ID router.





Activation des interfaces qui participe au processus OSPF



Vérification de l'activation des interfaces

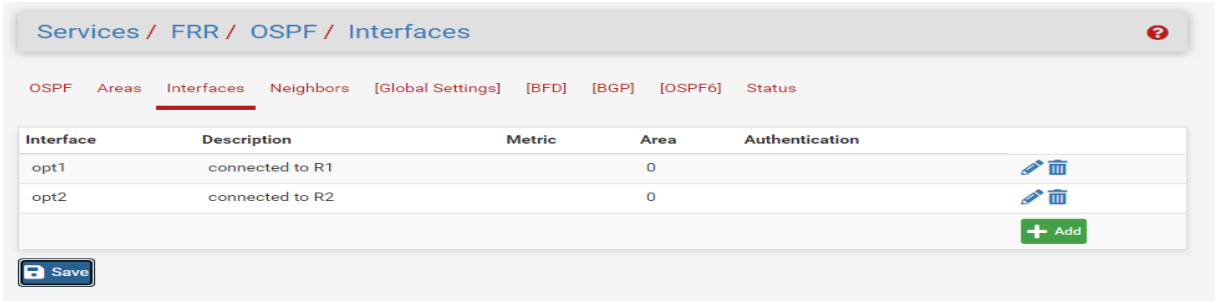


Figure 60: Vérification de l'activation des interfaces

IV.23Capture wiershark

IV.23.1 DHCP

DHCP DISCOVER (pour détecter les serveurs DHCP disponibles)

DHCP OFFER (réponse du serveur à un paquet DHCP DISCOVER, qui contient les premiers paramètres)

DHCP REQUEST (Le client retient une des offres reçues la première qui lui parvient, et diffuse sur le réseau Ce datagramme comporte l'adresse IP du serveur et celle qui vient d'être proposée au client).

DHCP ACK (réponse du serveur qui contient des paramètres et l'adresse IP du client).

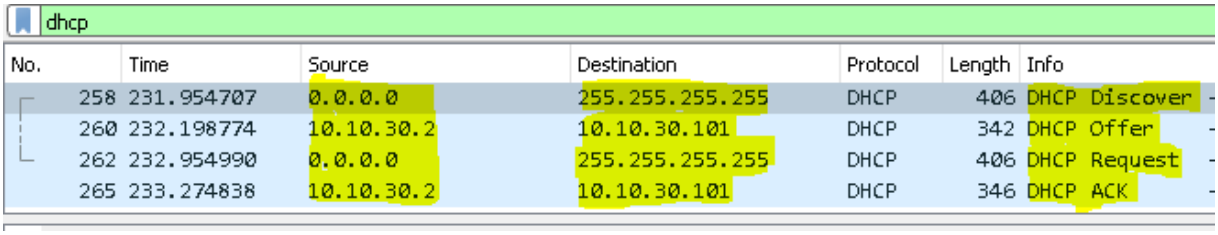


Figure 61: capture d'échange paquet client/serveur DHCP

IV.23.2 BPDU guard

Le port eths0/3 se met en état down/down lorsqu'il reçoit des messages BPDU

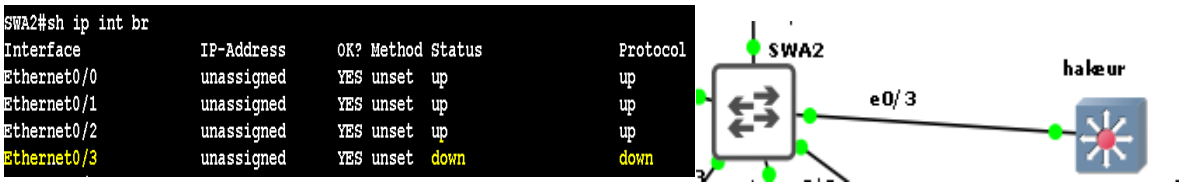


Figure 62: capture BPDU guard

IV.23.3 Port Security

Le port eths0/0 se met en état errdisable lorsqu' il reçoit un mac adresse no autorisé.

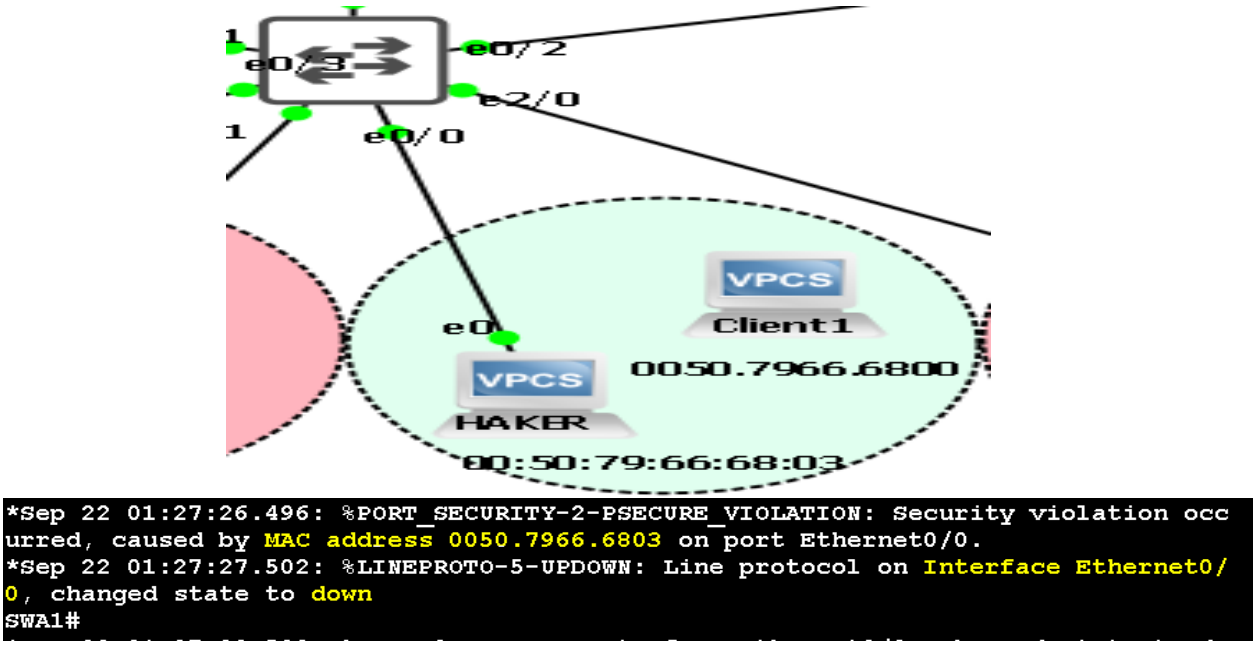


Figure 63: capture port Security

IV.23.4 HSRP

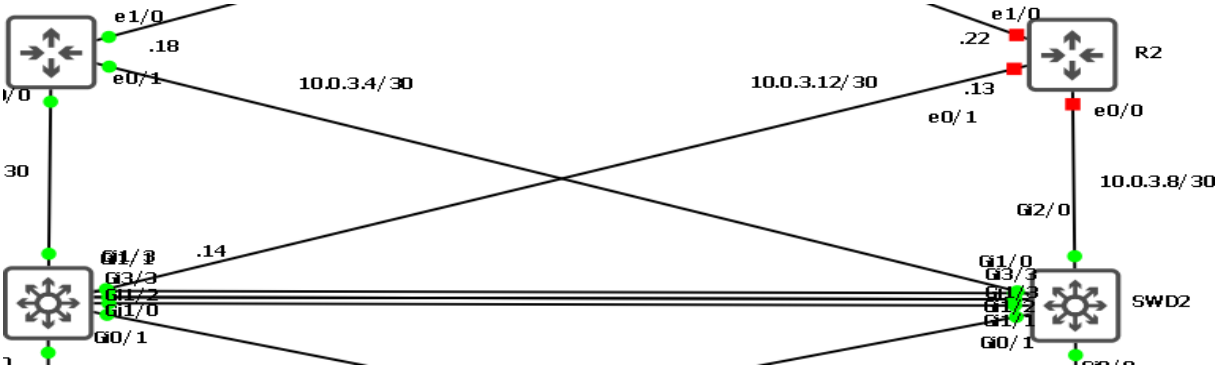
SWD1 devient active pour VLANs 30, 40,99 lorsque SWD2 est en panne


```
SWD1#
*Sep 22 01:48:42.162: %HSRP-5-STATECHANGE: Vlan30 Grp 30 state Standby -> Active
*Sep 22 01:48:43.327: %HSRP-5-STATECHANGE: Vlan40 Grp 40 state Standby -> Active
*Sep 22 01:48:44.246: %HSRP-5-STATECHANGE: Vlan99 Grp 99 state Standby -> Active
```

Figure 64: capture HSRP

Redondance N3 et amélioration de temps de convergence OSPF

La capacité de trouver intelligemment une autre route lorsqu'une liaison ou un nœud tombe en panne



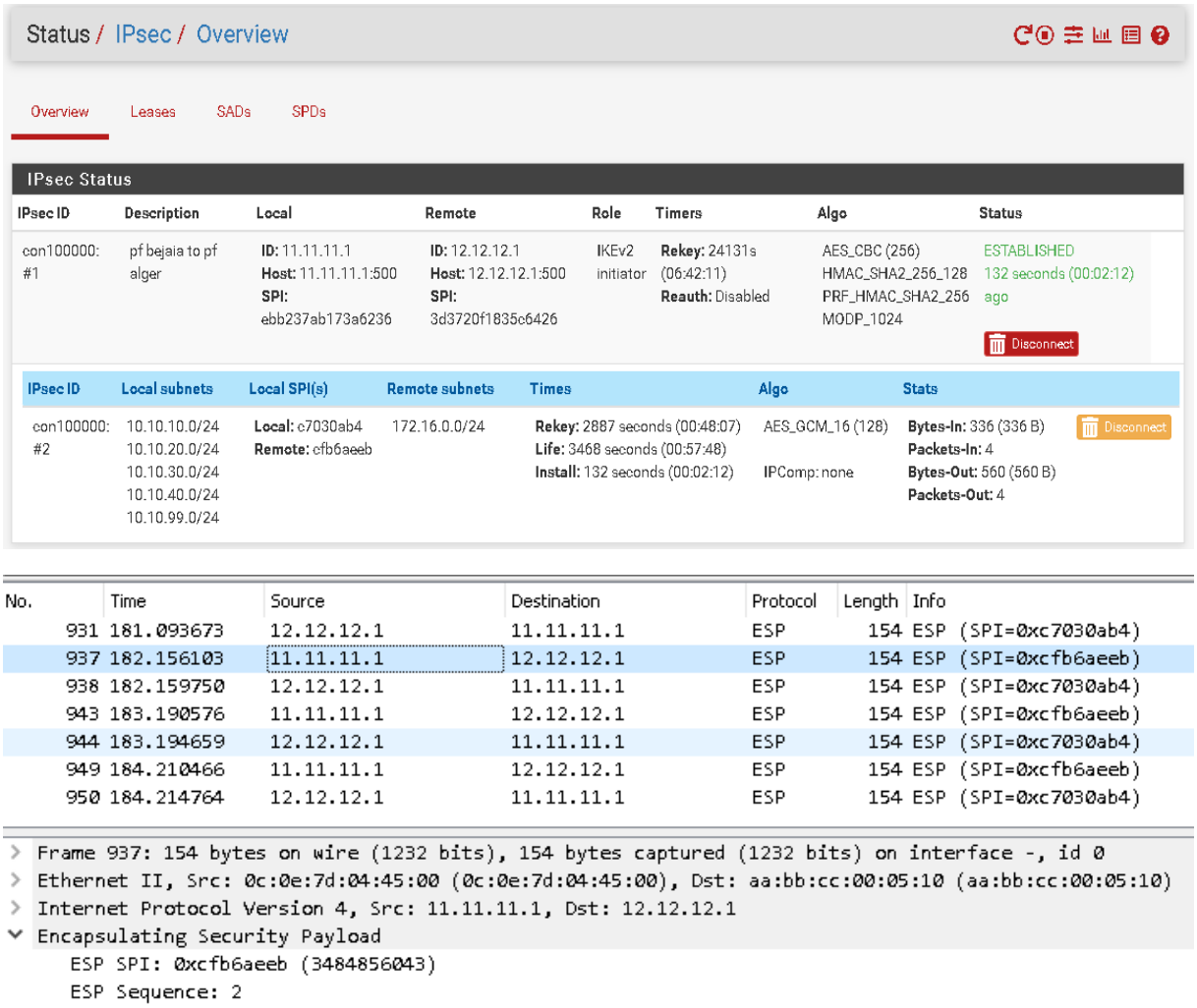

```
84 bytes from 11.11.11.2 icmp_seq=20 ttl=252 time=60.147 ms
84 bytes from 11.11.11.2 icmp_seq=21 ttl=252 time=31.922 ms
84 bytes from 11.11.11.2 icmp_seq=22 ttl=252 time=23.632 ms
84 bytes from 11.11.11.2 icmp_seq=23 ttl=252 time=26.414 ms
84 bytes from 11.11.11.2 icmp_seq=24 ttl=252 time=23.471 ms
11.11.11.2 icmp_seq=25 timeout
11.11.11.2 icmp_seq=26 timeout
11.11.11.2 icmp_seq=27 timeout
11.11.11.2 icmp_seq=28 timeout
11.11.11.2 icmp_seq=29 timeout
84 bytes from 11.11.11.2 icmp_seq=30 ttl=252 time=22.786 ms
84 bytes from 11.11.11.2 icmp_seq=31 ttl=252 time=24.082 ms
84 bytes from 11.11.11.2 icmp_seq=32 ttl=252 time=23.005 ms
84 bytes from 11.11.11.2 icmp_seq=33 ttl=252 time=18.735 ms
84 bytes from 11.11.11.2 icmp_seq=34 ttl=252 time=15.763 ms
84 bytes from 11.11.11.2 icmp_seq=35 ttl=252 time=17.854 ms
84 bytes from 11.11.11.2 icmp_seq=36 ttl=252 time=22.719 ms
84 bytes from 11.11.11.2 icmp_seq=37 ttl=252 time=18.666 ms

Client1>
```

Figure 65: temps de convergence OSPF

IV.23.5 PfSense

Établissement du tunnel VPN entre PFSense-Bejaia et PFSense -Alger



No.	Time	Source	Destination	Protocol	Length	Info
931	181.093673	12.12.12.1	11.11.11.1	ESP	154	ESP (SPI=0xc7030ab4)
937	182.156103	11.11.11.1	12.12.12.1	ESP	154	ESP (SPI=0xcfb6aeeb)
938	182.159750	12.12.12.1	11.11.11.1	ESP	154	ESP (SPI=0xc7030ab4)
943	183.190576	11.11.11.1	12.12.12.1	ESP	154	ESP (SPI=0xcfb6aeeb)
944	183.194659	12.12.12.1	11.11.11.1	ESP	154	ESP (SPI=0xc7030ab4)
949	184.210466	11.11.11.1	12.12.12.1	ESP	154	ESP (SPI=0xcfb6aeeb)
950	184.214764	12.12.12.1	11.11.11.1	ESP	154	ESP (SPI=0xc7030ab4)

```
> Frame 937: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface -, id 0
> Ethernet II, Src: 0c:0e:7d:04:45:00 (0c:0e:7d:04:45:00), Dst: aa:bb:cc:00:05:10 (aa:bb:cc:00:05:10)
> Internet Protocol Version 4, Src: 11.11.11.1, Dst: 12.12.12.1
v Encapsulating Security Payload
    ESP SPI: 0xcfb6aeeb (3484856043)
    ESP Sequence: 2
```

Figure 66 : capture trafic crypté entre site Bejaia et Alger

IV.24Vérification la connectivité à l'aide d'outil Ping

```
C:\Users\Administrateur.SERVER-AD>ping 172.16.0.100

Envoi d'une requête 'Ping'  172.16.0.100 avec 32 octets de données :
Réponse de 172.16.0.100 : octets=32 temps=43 ms TTL=60
Réponse de 172.16.0.100 : octets=32 temps=19 ms TTL=60
Réponse de 172.16.0.100 : octets=32 temps=24 ms TTL=60
Réponse de 172.16.0.100 : octets=32 temps=16 ms TTL=60

Statistiques Ping pour 172.16.0.100:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 16ms, Maximum = 43ms, Moyenne = 25ms
```

Figure 67: Statut de communication Serveur-ad ver client-Lan-Alger.

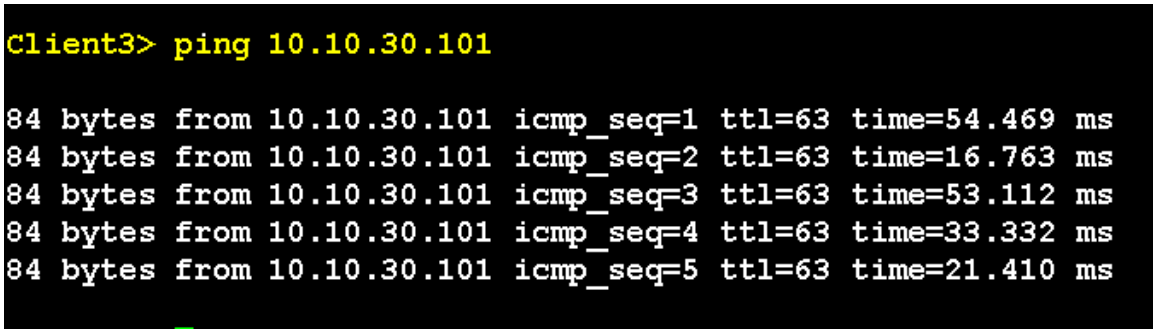


Figure 68: Statut de communication Vlan-20 ver Vlan 30

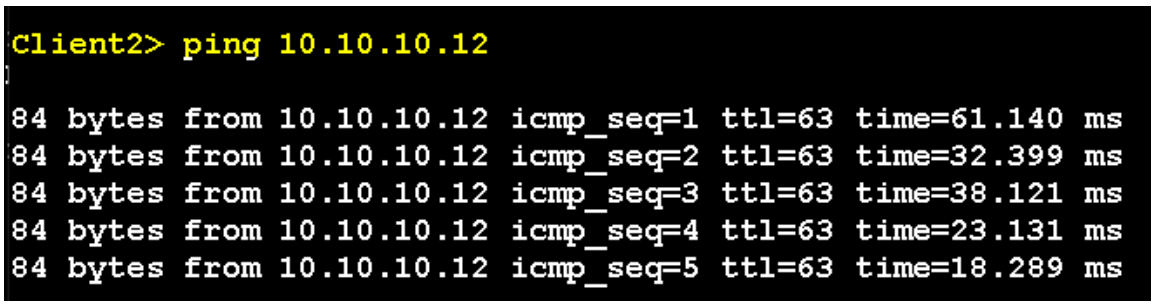


Figure 69: Statut de communication Vlan-30 ver Vlan 10

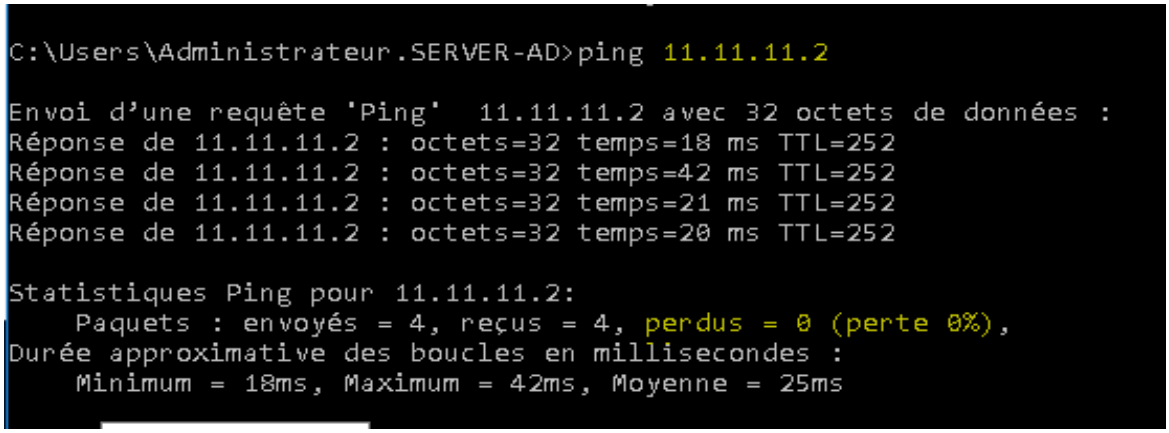


Figure 70: Statut de communication vert internet

Conclusion

Dans ce dernier chapitre, nous avons présenté la solution mise en place avec l'explication de la configuration des différents protocoles et les tests de validation pour nous assurer que notre objectif a bien été atteint.

Conclusion générale

Le présent mémoire a porté sur la proposition d'une architecture réseau et la mise-en place d'une infrastructure informatique pour l'administration et la sécurité du réseau local de L'entreprise SONATRACH de Bejaia.

Cette infrastructure fournit des services centralisés d'identification et d'authentification à un réseau d'ordinateur, elle permet également de répertorier les éléments d'un réseau administré; tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés et les imprimantes. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs peuvent contrôler leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées et la mise en place de la solution VOIP (serveur Asterisk et client eyebeam). La mise en place d'un vpn site-to-site permet une communication sécurisée avec le site SONATRACH ALGER, font l'objet de ce travail.

Durant le stage, nous avons d'abord commencé par faire une étude détaillée du réseau informatique de SONATRACH Bejaia afin de relever les différentes insuffisances présentées par le dit réseau. Après la synthèse des faiblisses et le recensement des besoins des utilisateurs et de l'entreprise en général pour le fonctionnement de l'infrastructure informatique, une solution assurant la centralisation, le partage, la fiabilité, la sécurité et une meilleure gestion des ressources a été proposée et mise en place.

Ce stage nous a été bénéfique car il nous a permis de mettre en pratique et d'enrichir nos Connaissances acquises au niveau de l'université de A. Mira Bejaïa et également de découvrir un ensemble d'outils employés dans l'administration des réseaux, aussi nous avons pu nous familiariser avec le matériel, les différents équipements utilisés, et le monde du travail.

Dans notre projet, l'ambition a été de mettre en place, d'administrer et de sécuriser un
Réseau local d'entreprise capable de répondre aux attentes des utilisateurs et de faciliter la tâche

```
SWD1
SWD1#configure tern
SWD1#configure ter,
SWD1#configure ter
SWD1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1(config)#vtp mode server
Device mode already VTP Server for VLANS.
SWD1(config)#vtp domain sonatrach.lan
Domain name already set to sonatrach.lan.
SWD1(config)#vtp version 2
VTP version is already in V2.
SWD1(config)#vtp password cisco
Password already set to cisco
SWD1(config)#vtp pruning
Pruning already switched on
SWD1(config)#
```

Configuration du protocole VTP

La configuration de VTP Client.

```
SWA1(config)#vtp mode client
Device mode already VTP Client for VLANS.
SWA1(config)#vtp domain sonatrach.lan
Domain name already set to sonatrach.lan.
SWA1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SWA1(config)#vtp password cisco
Password already set to cisco
```

Création des VLAN:

```
SWD1(config)#vlan 10
SWD1(config-vlan)#name ST
SWD1(config-vlan)#vlan 20
SWD1(config-vlan)#name SA
SWD1(config-vlan)#vlan 30
SWD1(config-vlan)#name SE
SWD1(config-vlan)#vlan 40
SWD1(config-vlan)#name voice
SWD1(config-vlan)#vlan 99
SWD1(config-vlan)#name Native
SWD1(config-vlan)#exit
```

Configuration des ports Trunks sur les switch d'accès.

```
SWA1(config-if-range)#interface range eth0/0-1
SWA1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,99
SWA1(config-if-range)#switchport trunk native vlan 99
SWA1(config-if-range)#exit
```

Configuration des liens trunks les switchs distribution.

```
SWD1(config-if-range)#int range eth0/2-3,eth1/0
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
SWD1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,99
SWD1(config-if-range)#switchport trunk native vlan 99
```

Assignations des ports au VLAN.

```
SWA1(config)#interface eth2/3
SWA1(config-if)#SWITCHPORT MODE ACCESS
SWA1(config-if)#SWITCHPORT  ACCESS VLAN 99
```

Configuration etherchannel

SWD1

```
SWD1(config-if-range)#interface range eth2/0-3
SWD1(config-if-range)#channel-protocol LACP
SWD1(config-if-range)#channel-group 2 mode active
SWD1(config-if-range)#interface port-channel 2
SWD1(config-if)#switchport trunk encapsulation dot1q
SWD1(config-if)#switchport mode trunk
SWD1(config-if)#switchport trunk allowed vlan 10,20,30,40,99
SWD1(config-if)#
```

```
SWD2(config-if)#int range eth2/0-3
SWD2(config-if-range)#channel-protocol LACP
SWD2(config-if-range)#channel-group 2 mode passive
SWD2(config-if-range)#interface port-channel 2
SWD2(config-if)#switchport trunk encapsulation dot1q
SWD2(config-if)#switchport mode  trunk
SWD2(config-if)#switchport trunk allowed vlan 10,20,30,40,99
SWD2(config-if)#
```

Les SVI

```
SWD2(config)#ip routing
SWD2(config)#int vlan 10
SWD2(config-if)#ip add 10.10.10.2 255.255.255.0
SWD2(config-if)#no shutdown
SWD2(config-if)#int vlan 20
SWD2(config-if)#ip add 10.10.20.2 255.255.255.0
SWD2(config-if)#no shutdown
SWD2(config-if)#int vlan 30
SWD2(config-if)#ip add 10.10.30.2 255.255.255.0
SWD2(config-if)#no shutdown
SWD2(config-if)#int vlan 40
SWD2(config-if)#ip add 10.10.40.2 255.255.255.0
SWD2(config-if)#
SWD2(config-if)#no shutdown
SWD2(config-if)#int vlan 99
SWD2(config-if)#ip add 10.10.99.2 255.255.255.0
SWD2(config-if)#no shutdown
```

La configuration des interfaces Ethernet sur R1 et R2.

```
interface Ethernet0/0
 ip address 10.0.3.1 255.255.255.252
 ip ospf message-digest-key 1 md5 pfsense
 ip ospf network point-to-point
end

R1#
```

```
interface Ethernet0/0
 ip address 10.0.3.9 255.255.255.252
 ip ospf message-digest-key 1 md5 pfsense
 ip ospf network point-to-point
end

R2#
```

Configuration de base HSRP

```
SWD1(config-if)#STandby 20 PRIority 110
*Jul 12 10:07:47.001: %HSRP-5-STATECHANGE: Vlan30 Grp 30 state Standby -> Active
SWD1(config-if)#NO STandby 20 PRIority 110
SWD1(config-if)# STandby 30 PRIority 110
SWD1(config-if)#interface  vlan 40
SWD1(config-if)#standby 40 ip 10.10.40.250
SWD1(config-if)# STandby 40 PRIority 110
SWD1(config-if)#standby 0 preempt
*Jul 12 10:09:06.234: %HSRP-5-STATECHANGE: Vlan40 Grp 40 state Standby -> Active
SWD1(config-if)#standby 40 preempt
SWD1(config-if)#interface  vlan 99
SWD1(config-if)#standby 99 ip 10.10.99.250
SWD1(config-if)# STandby 99 PRIority 110
SWD1(config-if)#standby 99 preempt
SWD1(config-if)#EXIT
```

```
SWD2(config)#interface vlan 10
SWD2(config-if)#STandby 10 ip 10.10.10.250
SWD2(config-if)#EXIT
SWD2(config)#interface vlan 20
SWD2(config-if)#STandby 20 ip 10.10.20.250
SWD2(config-if)#EXIT
SWD2(config)#interface vlan 30
SWD2(config-if)#STandby 30 ip 10.10.30.250
SWD2(config-if)#EXIT
SWD2(config)#interface vlan 40
SWD2(config-if)#STandby 40 ip 10.10.40.250
SWD2(config-if)#EXIT
SWD2(config)#interface vlan 99
SWD2(config-if)#EXIT
*Jul 12 10:15:55.496: %HSRP-5-STATECHANGE: Vlan30 Grp 30 state Speak -> Standby
SWD2(config-if)#STandby 40 ip 10.10.99.250
*Jul 12 10:16:13.053: %HSRP-5-STATECHANGE: Vlan40 Grp 40 state Speak -> Standby
SWD2(config-if)#STandby 99 ip 10.10.99.250
SWD2(config-if)#EXIT
SWD2(config)#DO WR
Building configuration...
Compressed configuration from 3120 bytes to 1431 bytes[OK]
```

Configuration de DHCP Relai.

```
SWD1(config)#interface vlan 10
SWD1(config-if)#ip helper-address 10.10.99.100
SWD1(config-if)#interface vlan 20
SWD1(config-if)#ip helper-address 10.10.99.100
SWD1(config-if)#interface vlan 30
SWD1(config-if)#ip helper-address 10.10.99.100
SWD1(config-if)#interface vlan 40
SWD1(config-if)#ip helper-address 10.10.99.100
SWD1(config-if)#exit
```

Configuration de OSPF

```
 ip ospf message-digest-key 1 md5 pfsense
 ip ospf network point-to-point
 ip ospf message-digest-key 1 md5 pfsense
 ip ospf network point-to-point
 ip ospf message-digest-key 1 md5 pfsense
 ip ospf network point-to-point
router ospf 1
 area 0 authentication message-digest
 network 10.0.3.1 0.0.0.0 area 0
 network 10.0.3.5 0.0.0.0 area 0
 network 10.0.3.18 0.0.0.0 area 0
R1#
```

La configuration des ports de sécurité

```
SWA1(config)#int eth0/3
SWA1(config-if)#switchport port-security maximum 1
SWA1(config-if)#switchport port-security mac-address  00:50:79:66:68:00
SWA1(config-if)#switchport port-security violation shutdown
```

BPDU Guard

```
SWA1(config-if)#spanning-tree bpduguard enable
SWA1(config-if)#spanning-tree portfast
```

SSH sur un switch

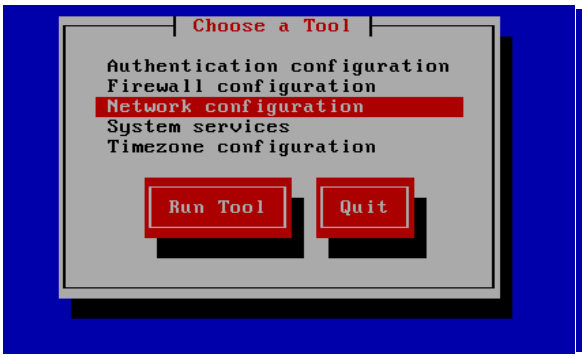
```
SWA1(config)#hostname SWA1
SWA1(config)#enable secret cisco
SWA1(config)#line console 0
SWA1(config-line)#password cisco
SWA1(config-line)#line vty 0 4
SWA1(config-line)#password cisco
SWA1(config-line)#transport input ssh
```

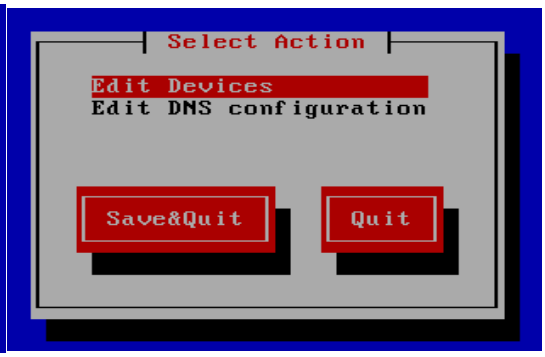
```
SWA2(config)#username  ines password cisco
SWA2(config)#ip domain name test.com
SWA2(config)#crypto key generate rsa
% You already have RSA keys defined named SWA2.test.com.
% Do you really want to replace them? [yes/no]:
% Please answer 'yes' or 'no'.
% Do you really want to replace them? [yes/no]: y
```

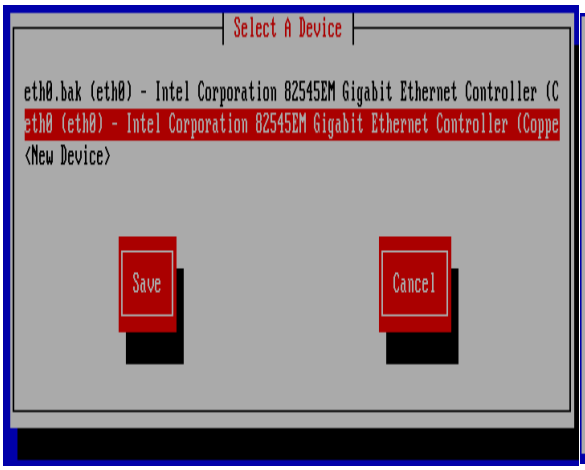
L'adresse du switch d'accès.

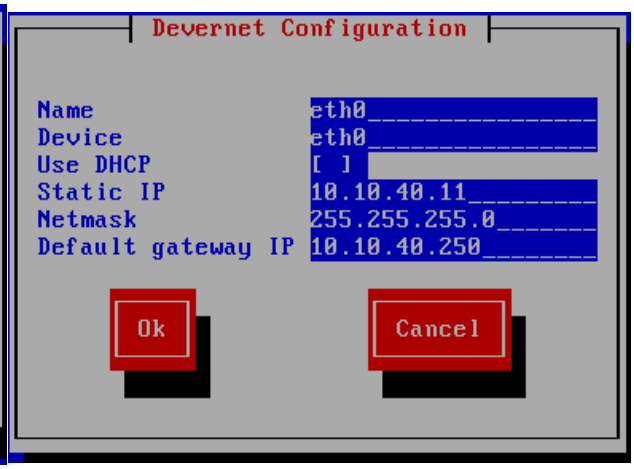
```
SWA2(config)#int vlan 99
SWA2(config-if)#ip add 10.10.99.4 255.255.255.0
SWA2(config-if)#no shutdown
```

Le serveur de voix Asterisk

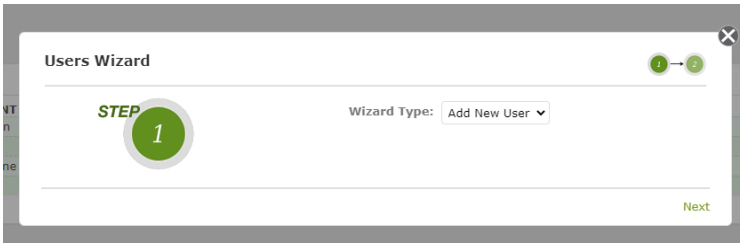


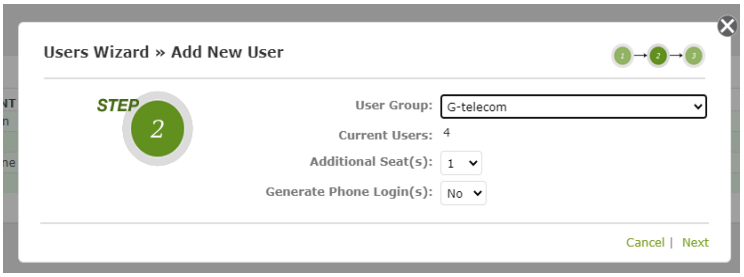


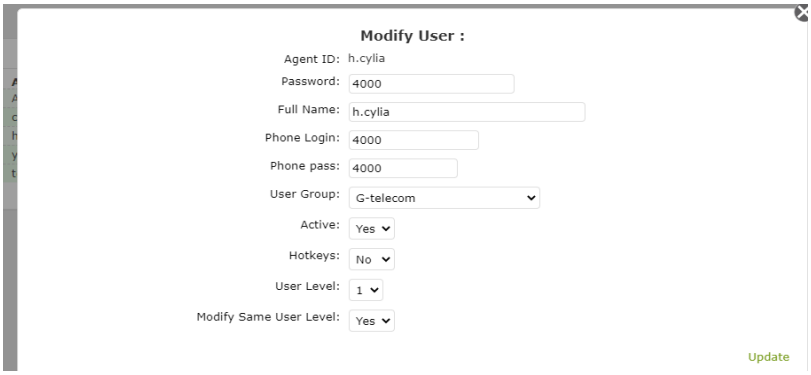




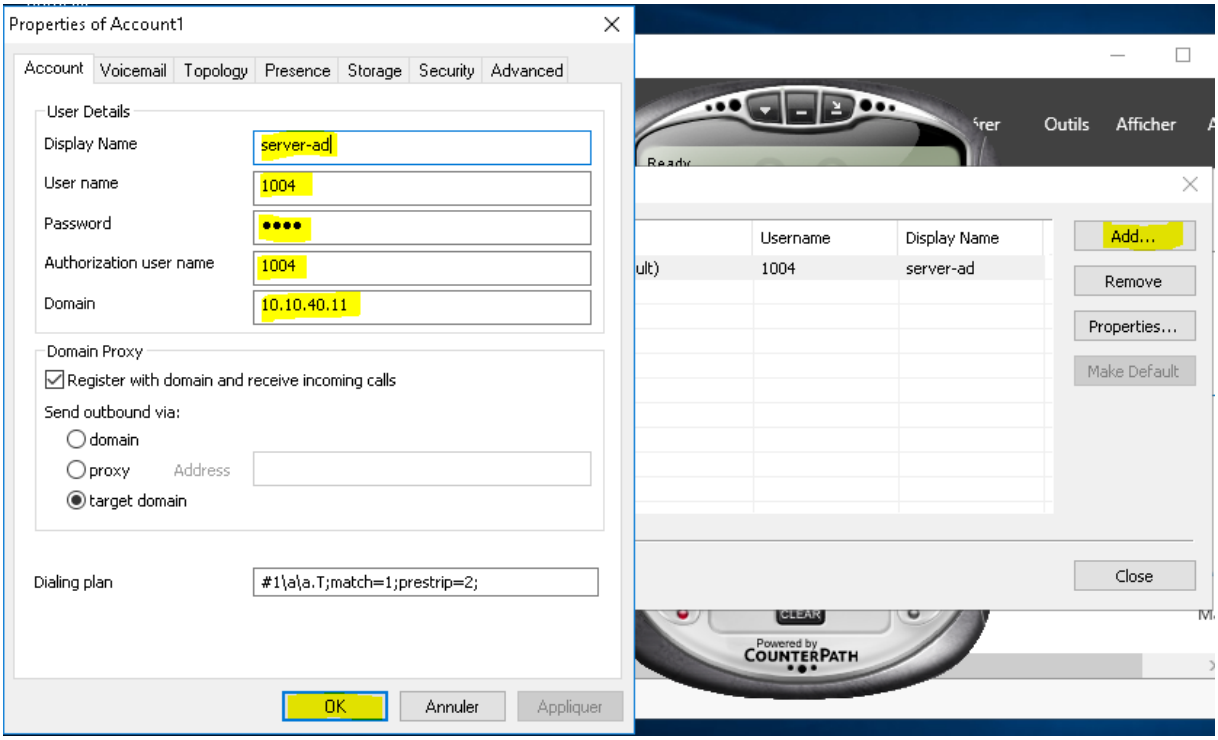
La configuration des phones



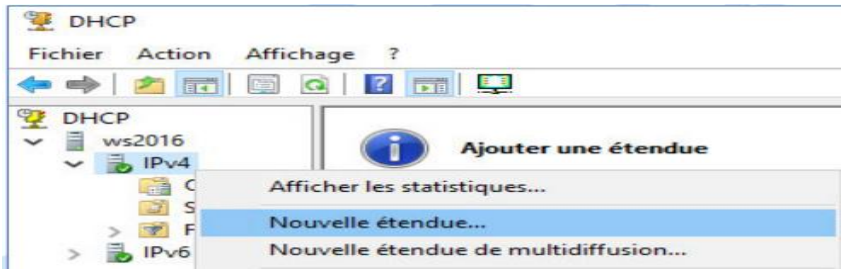


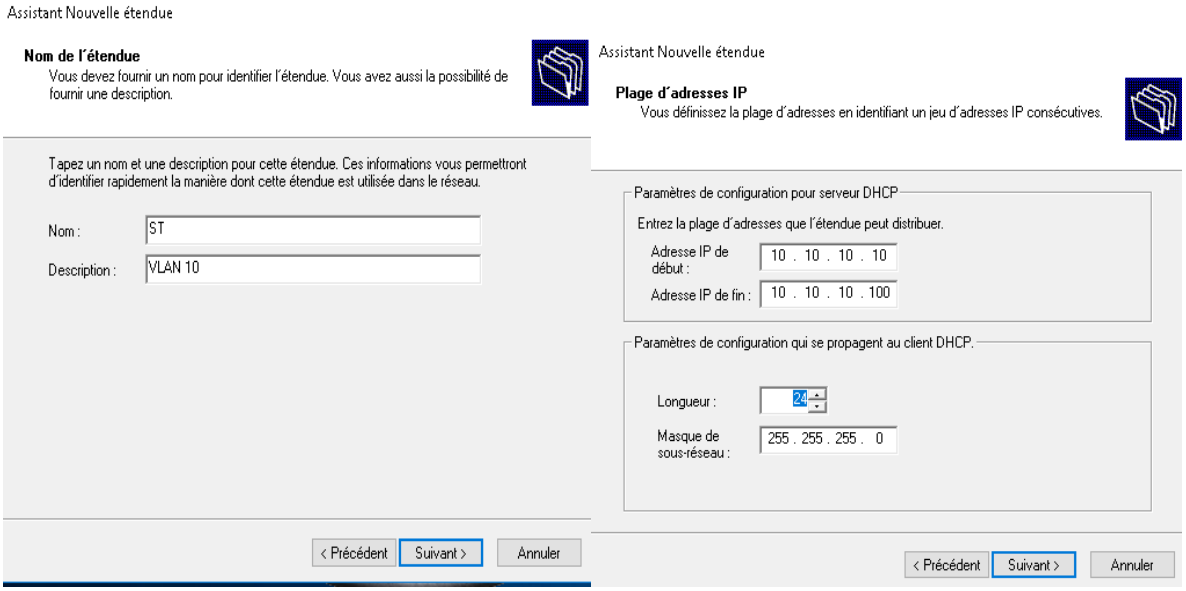


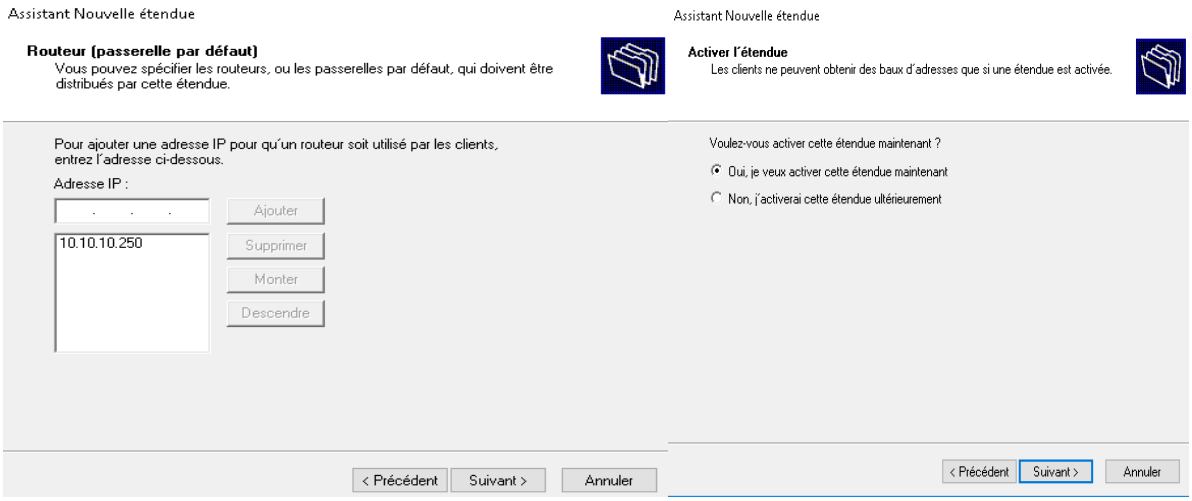
Configurer EyeBeam



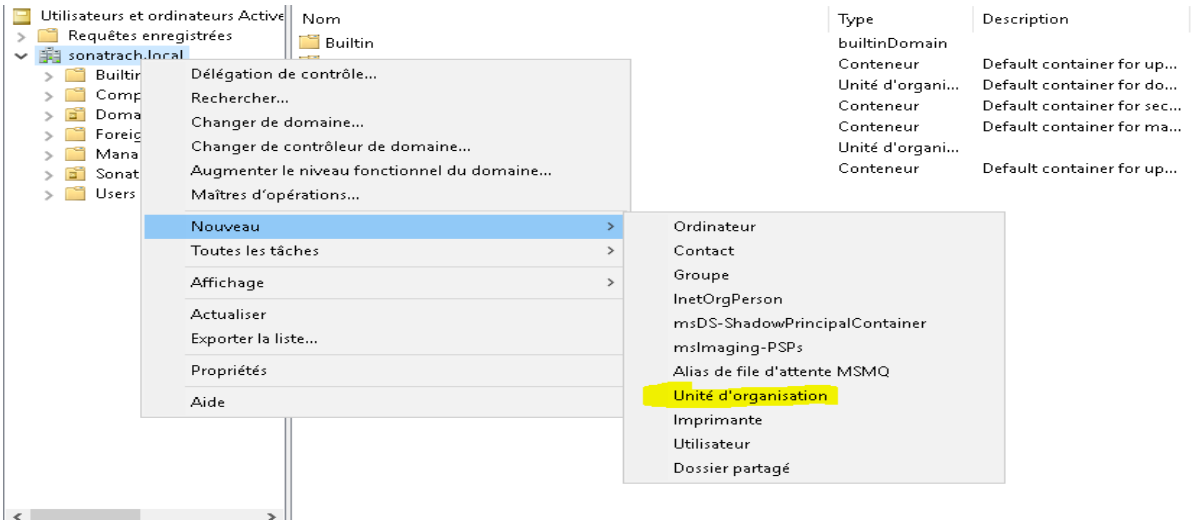
Configuration du DHCP dans le serveur AD



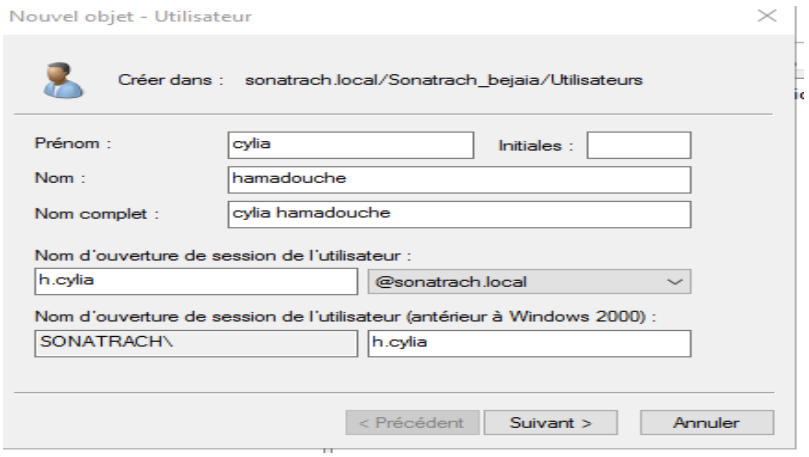


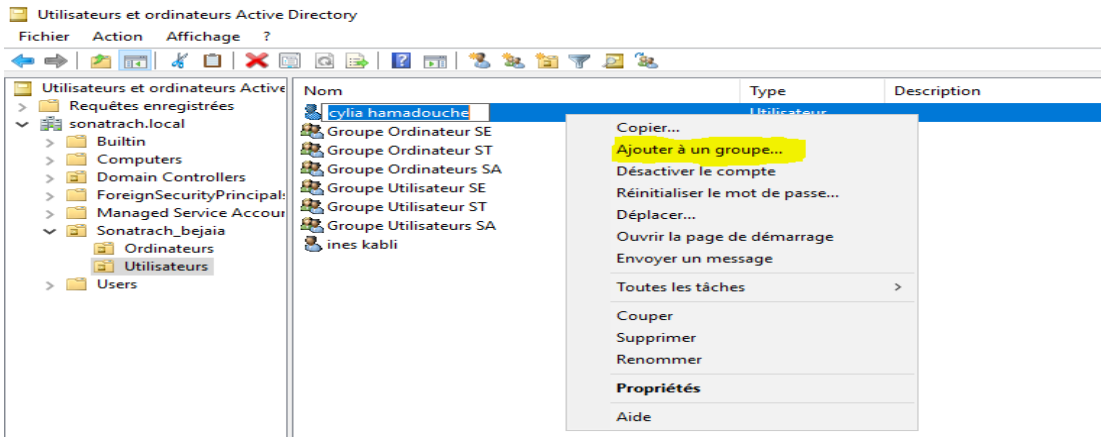


Création des Unités d'Organisation OU

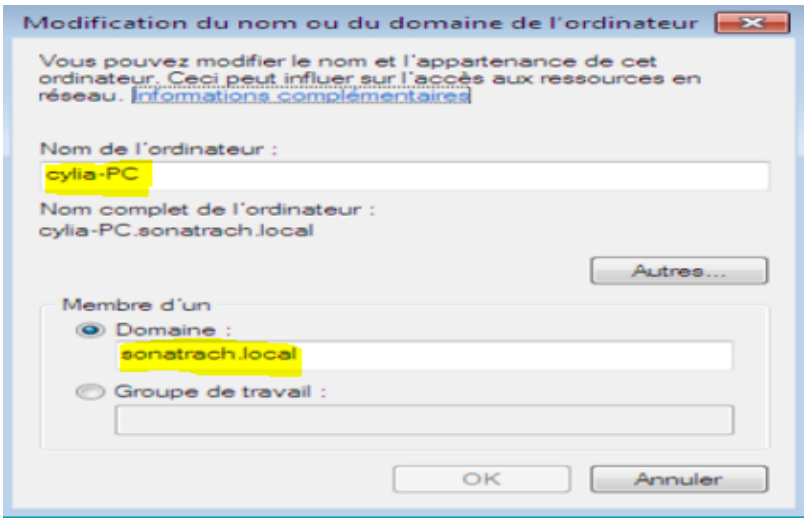


Création d'un utilisateur

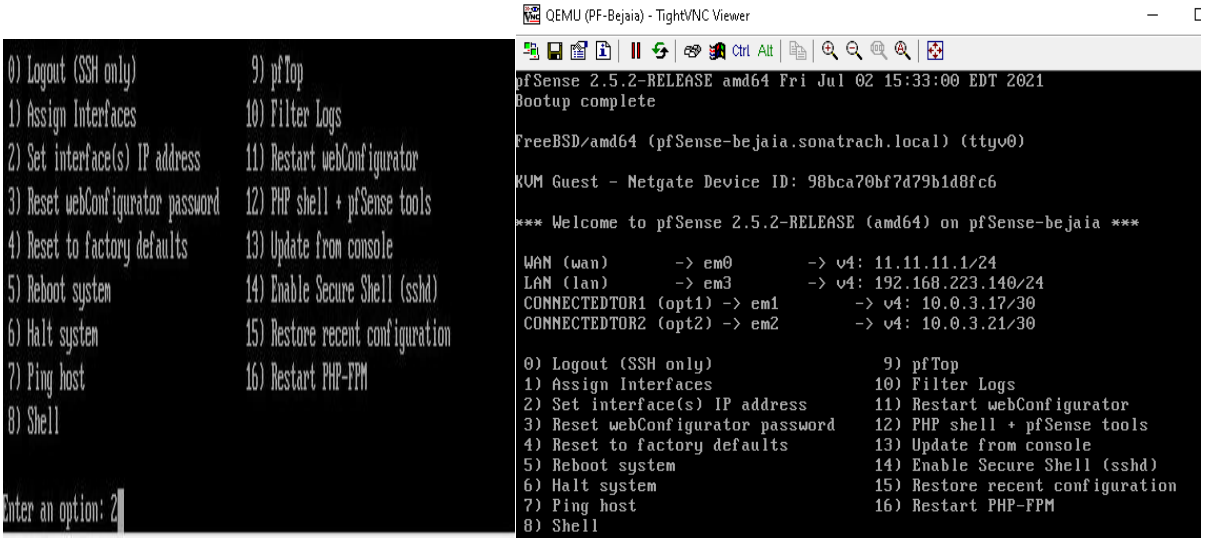




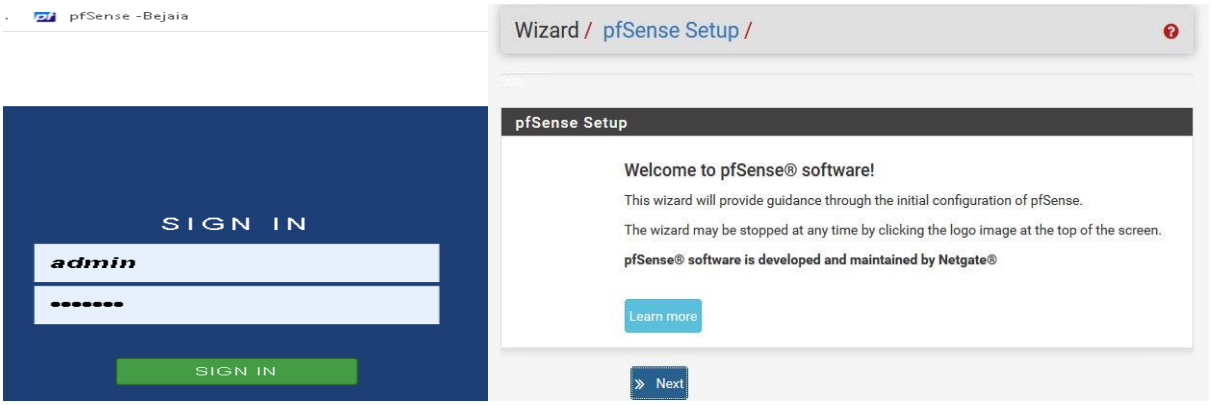
Joindre un poste au domaine

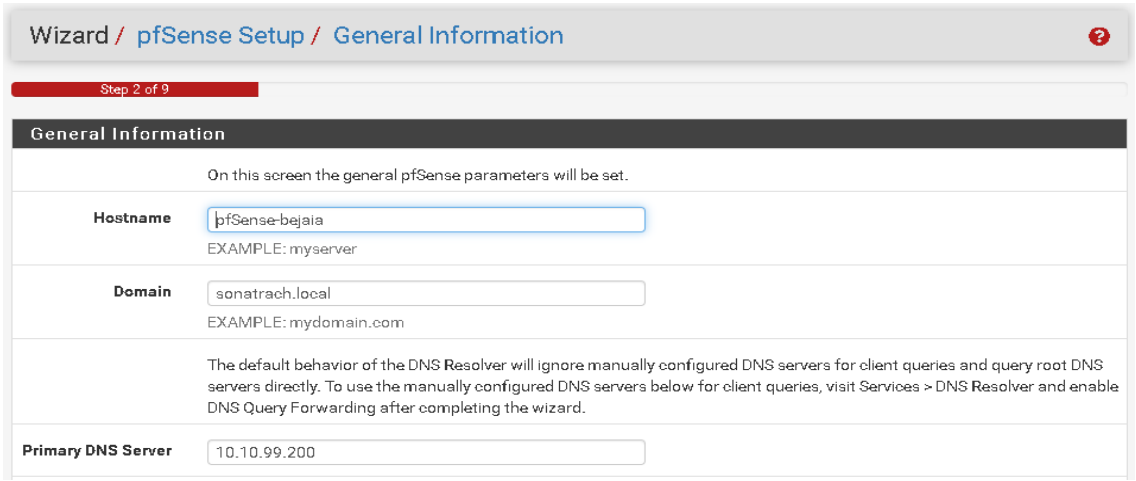


Configuration de l'adresse IP des cartes réseau du pfSense

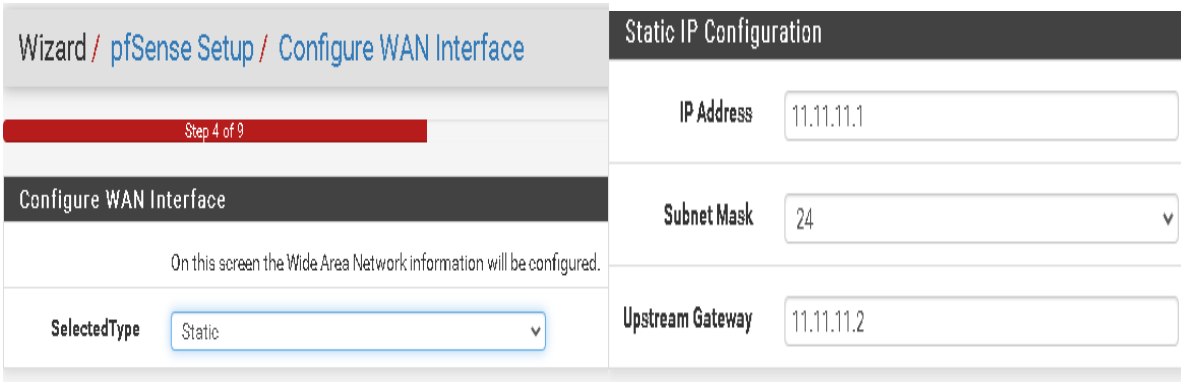


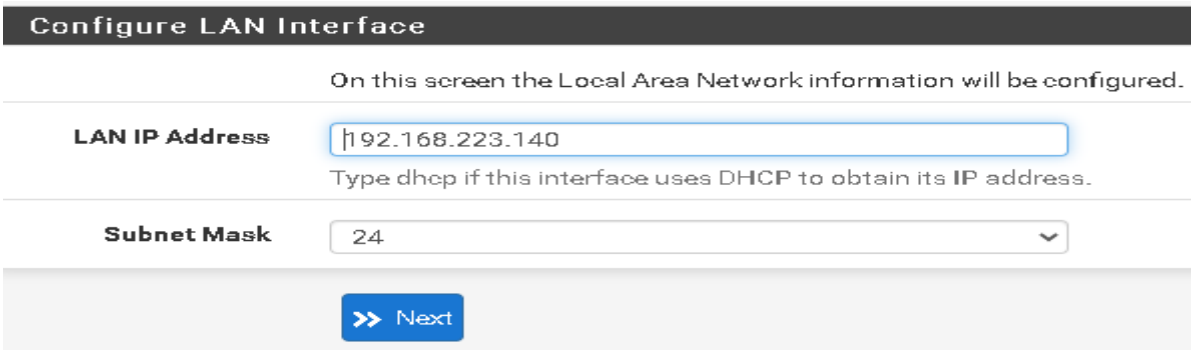
Configuration de Base de PFSense

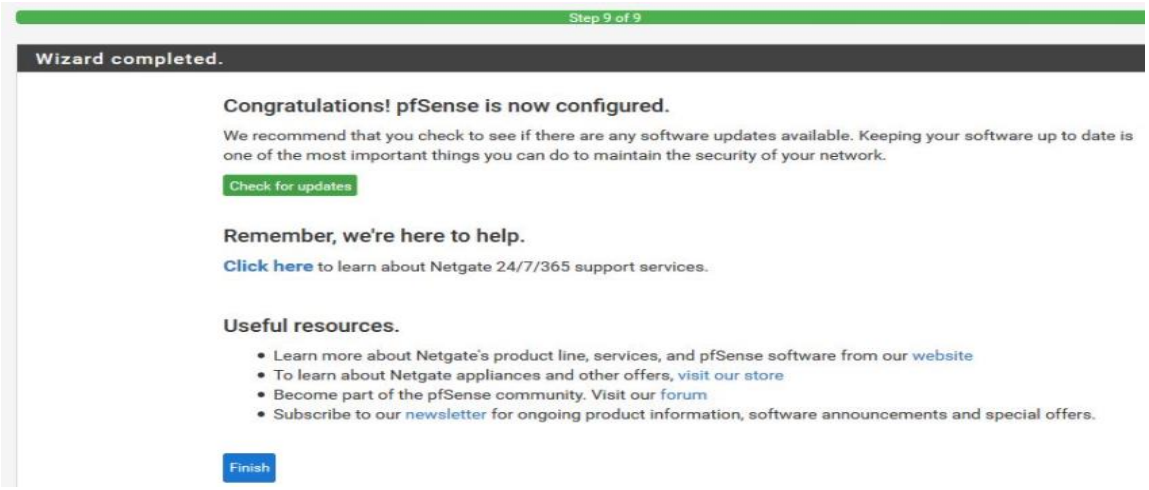




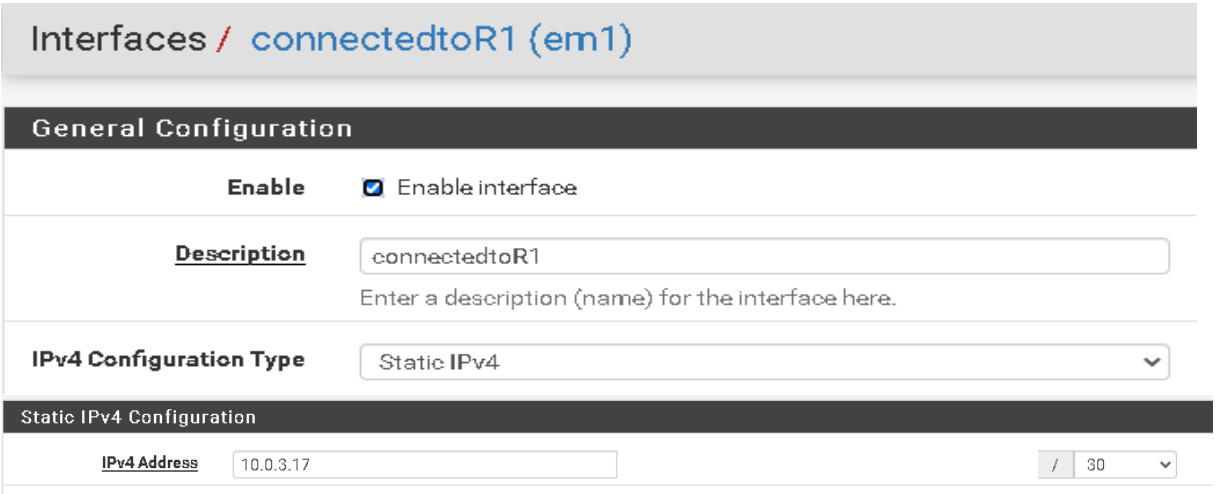
Sur PFSense Bejaia

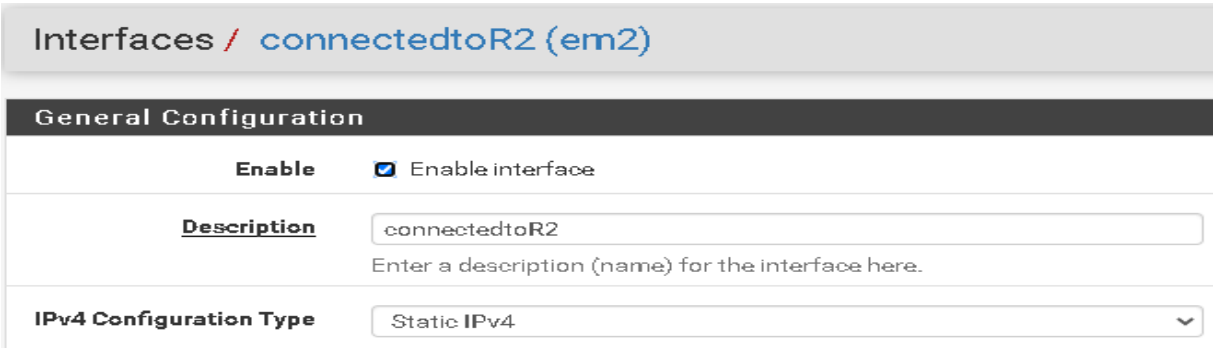




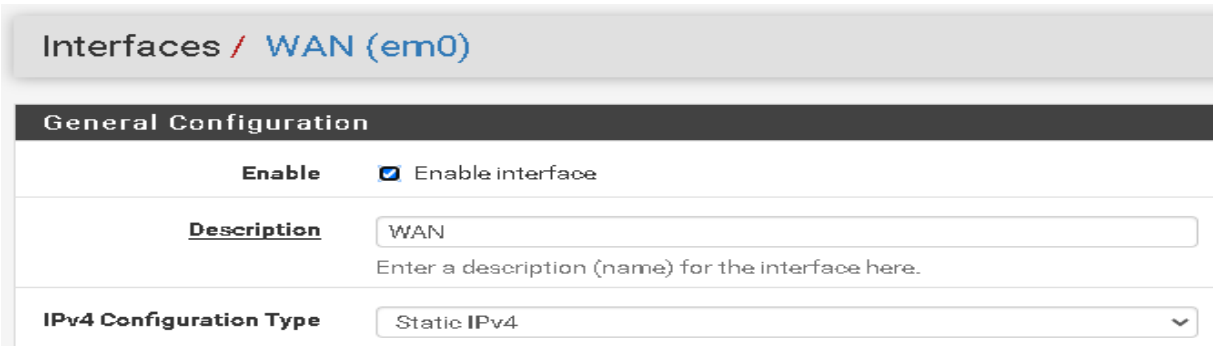


. Configuration des interfaces LAN1 et LAN2

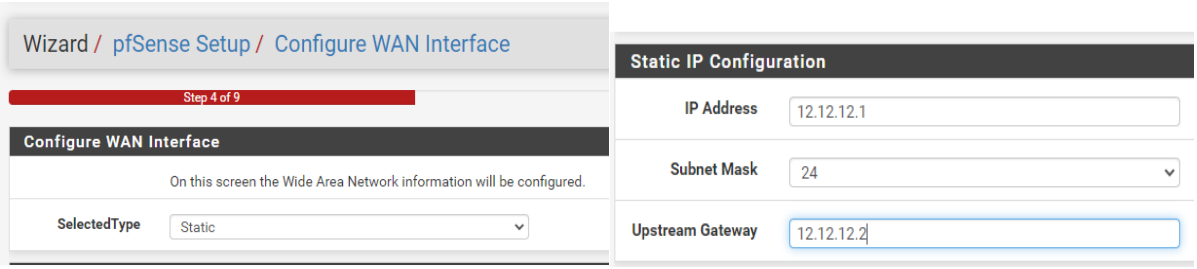




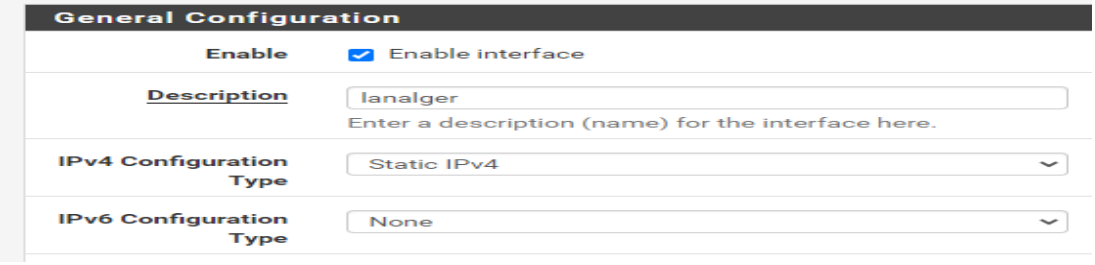
Configuration l'interface WAN

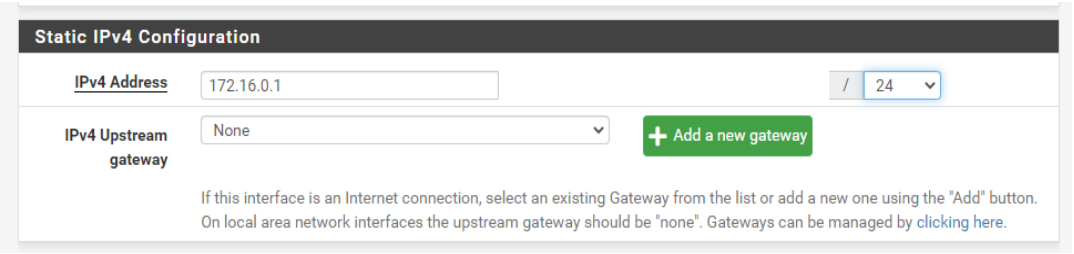


Sur PFSense Alger

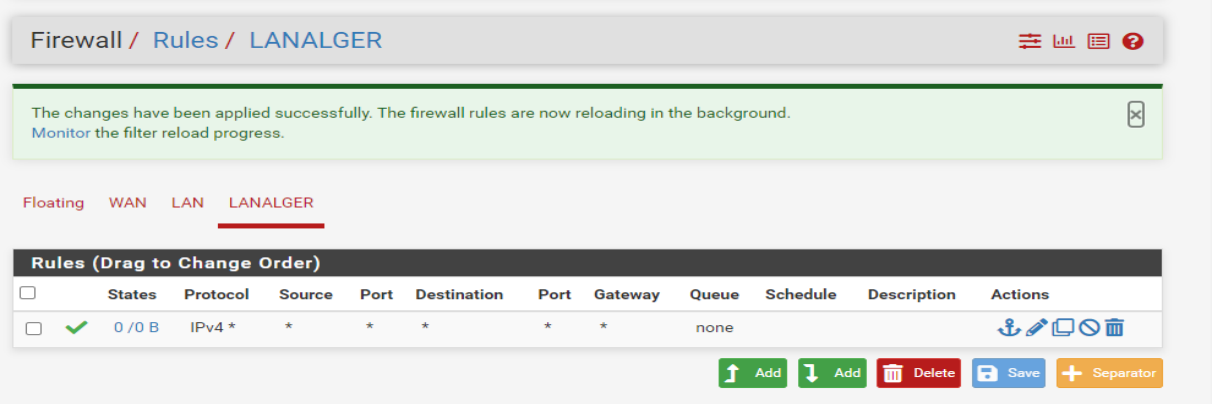


Configuration l'interfaces LAN

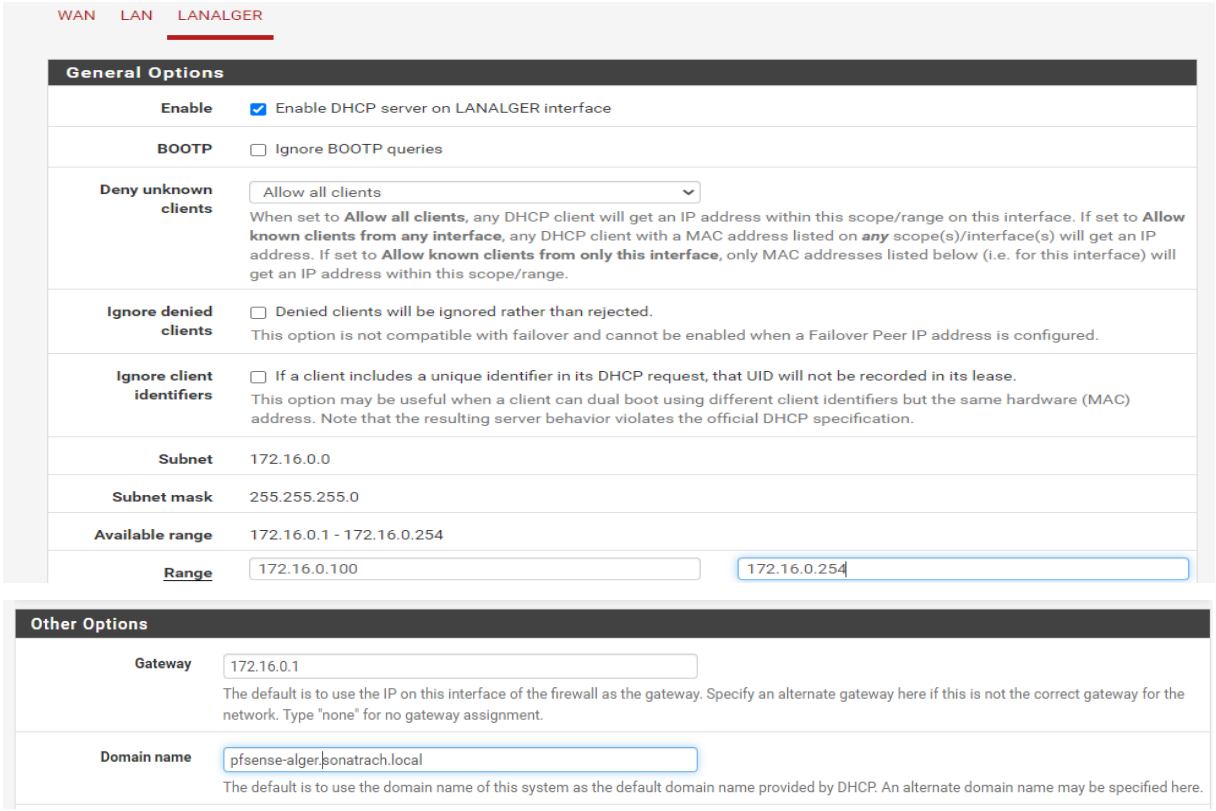




Les rules sur PfSense Alger

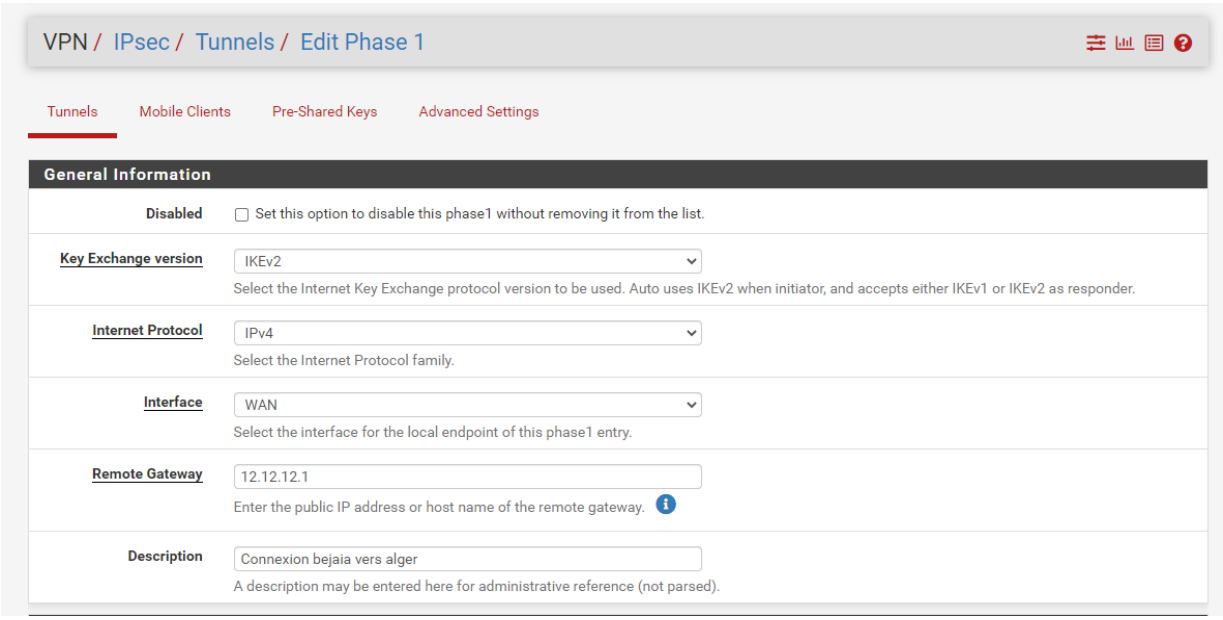


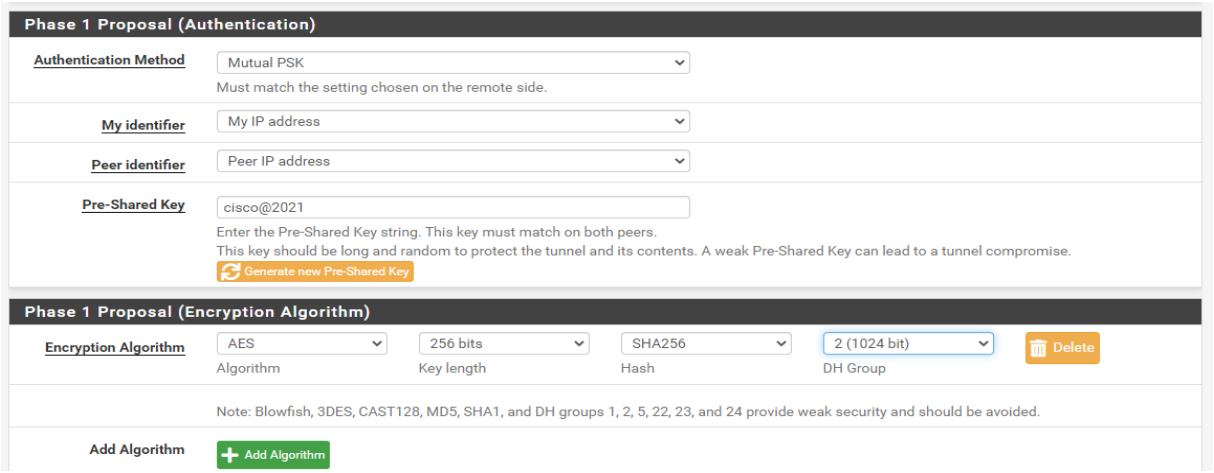
Configuration DHCP sur pfSense Alger



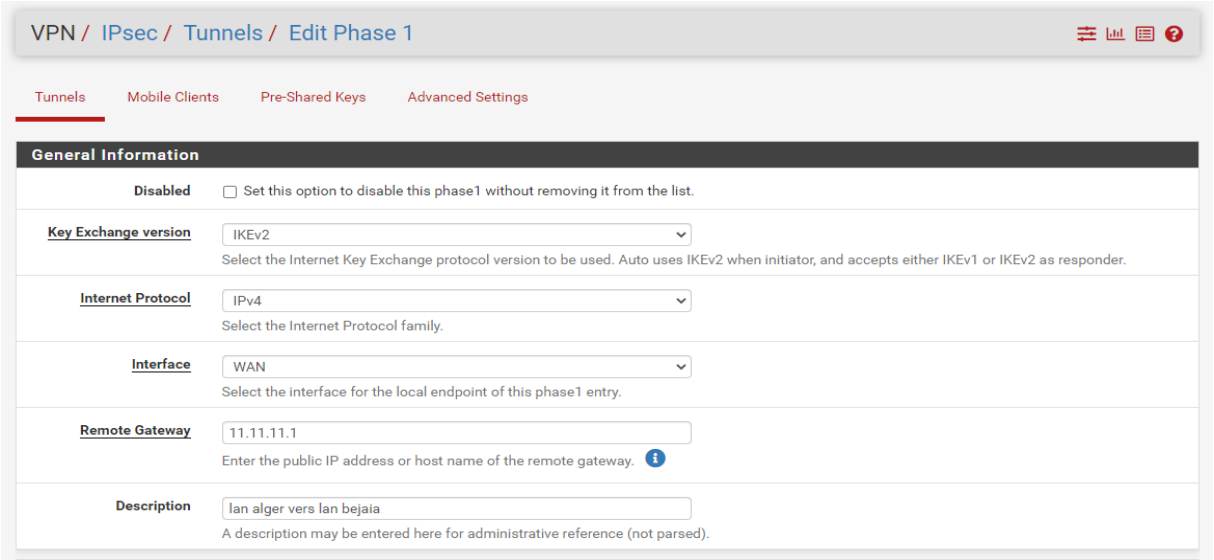
Configuration VPN/IPsec phase 1

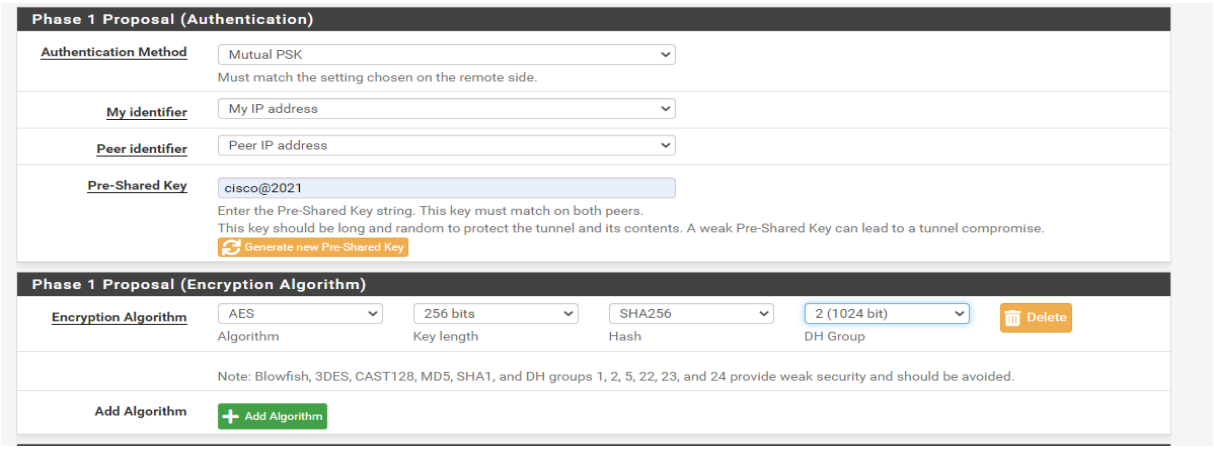
Sur PFSense Bejaia





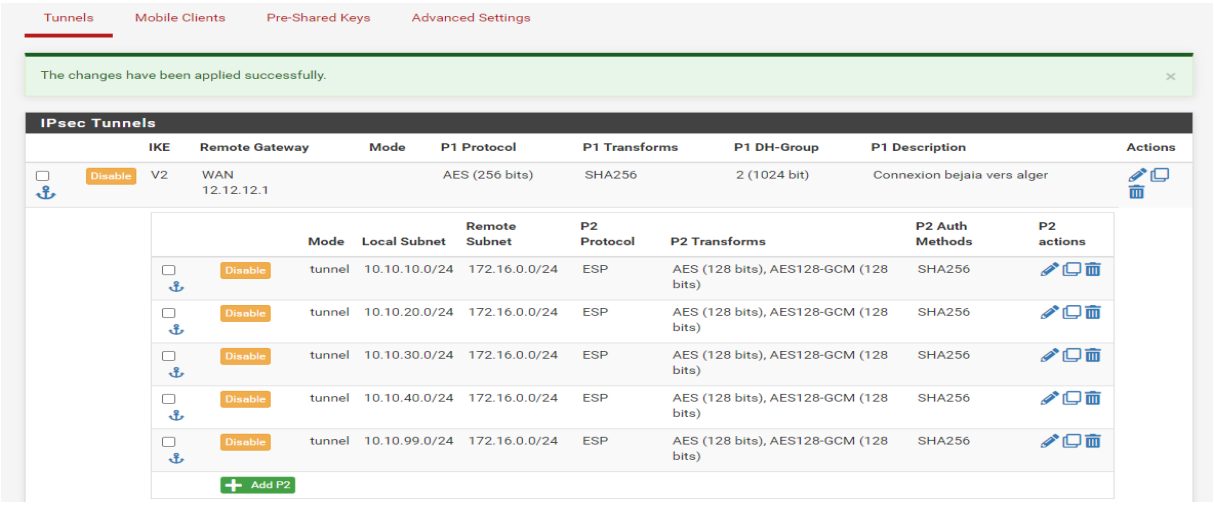
Sur PFSense Alger



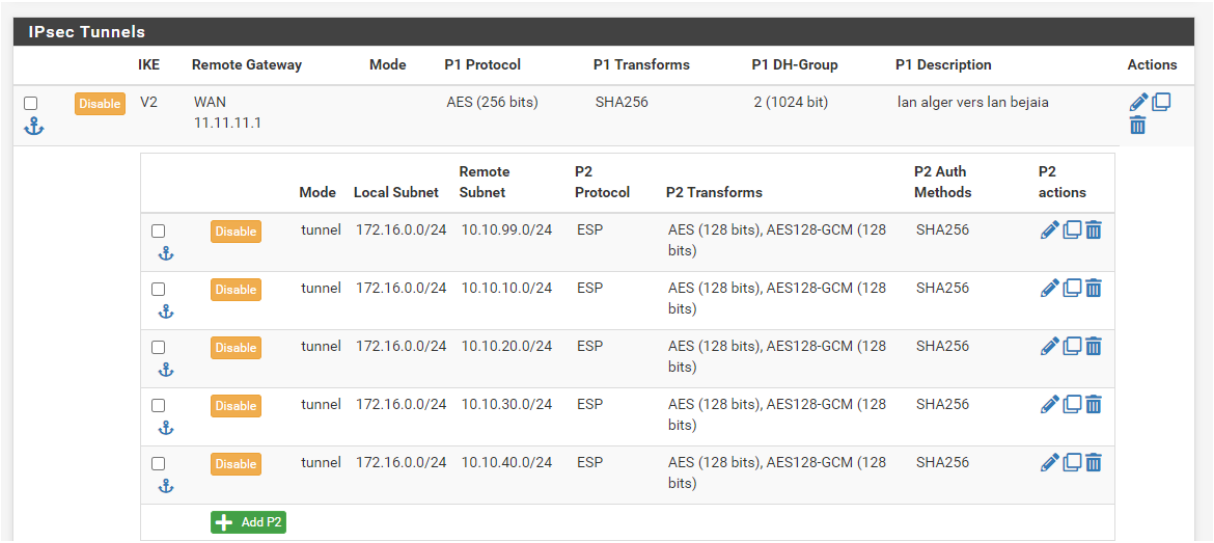


Configuration VPN/IPsec phase 2

Sur PFSense Bejaia

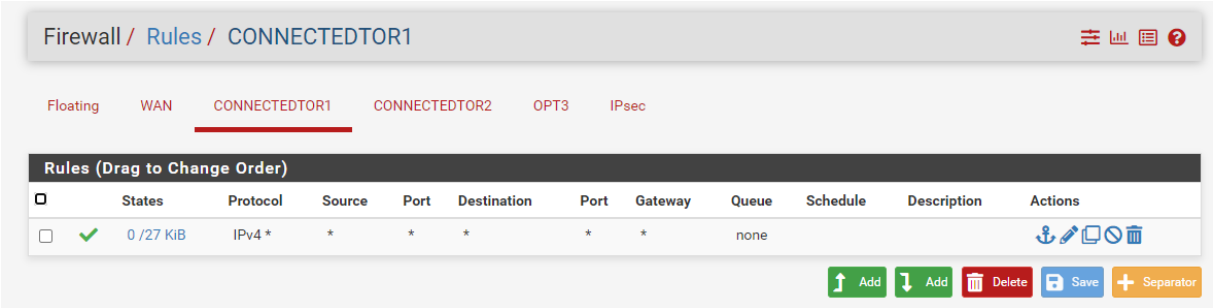


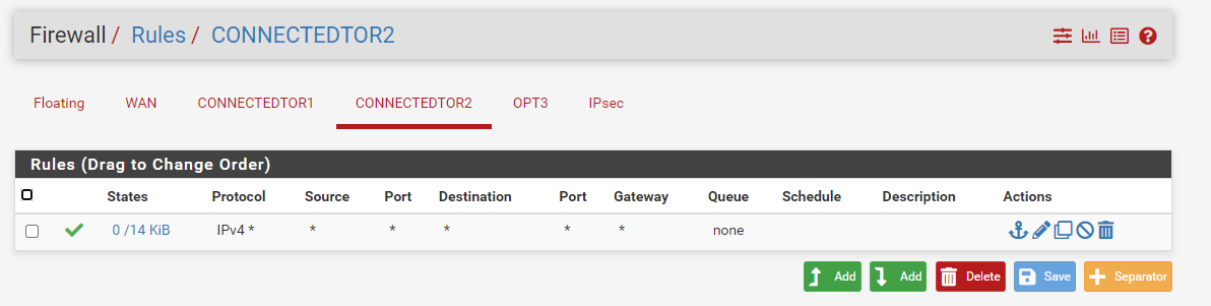
Sur PFSense Alger



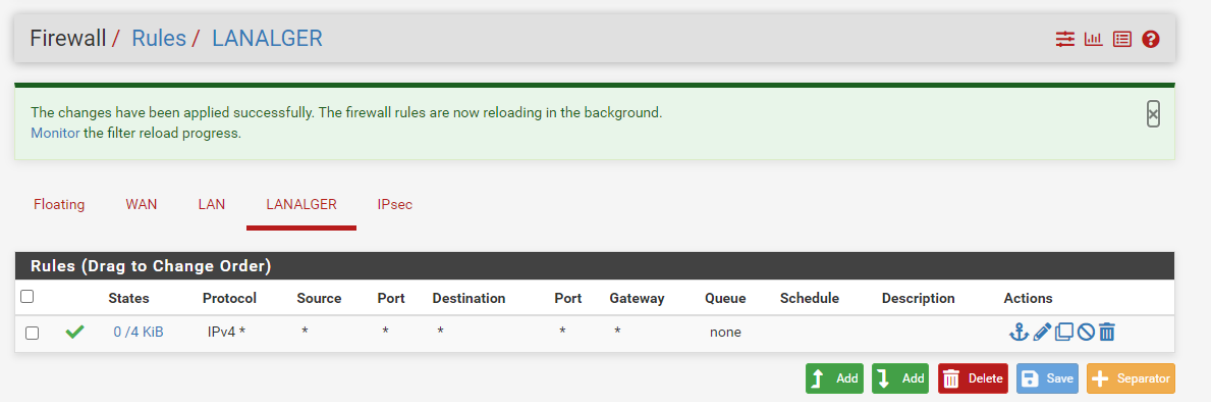
Les règles de filtrage

Sur PFSense Bejaia

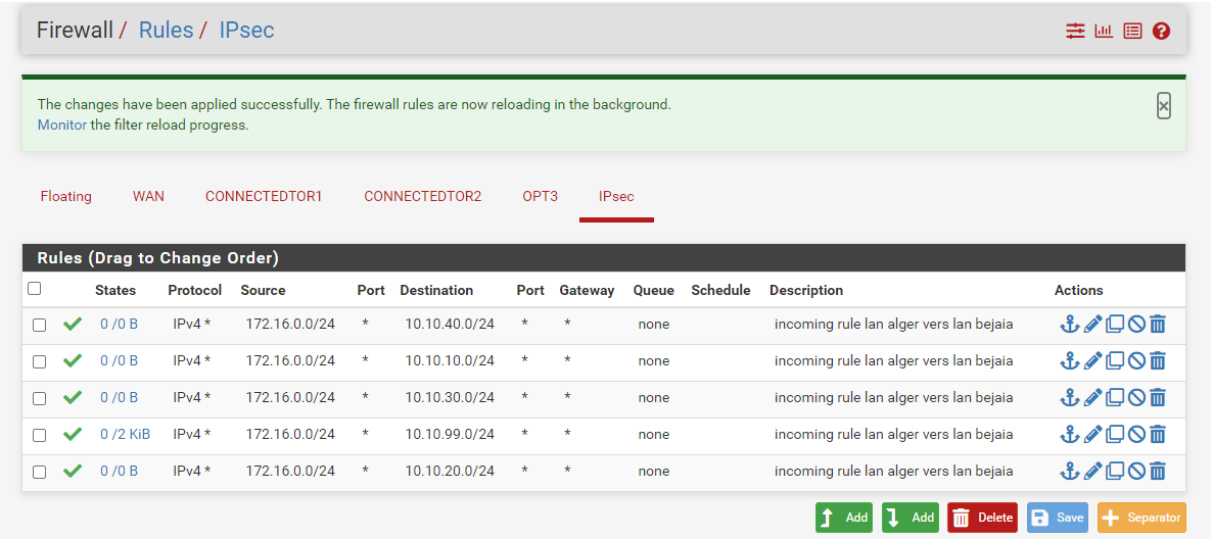




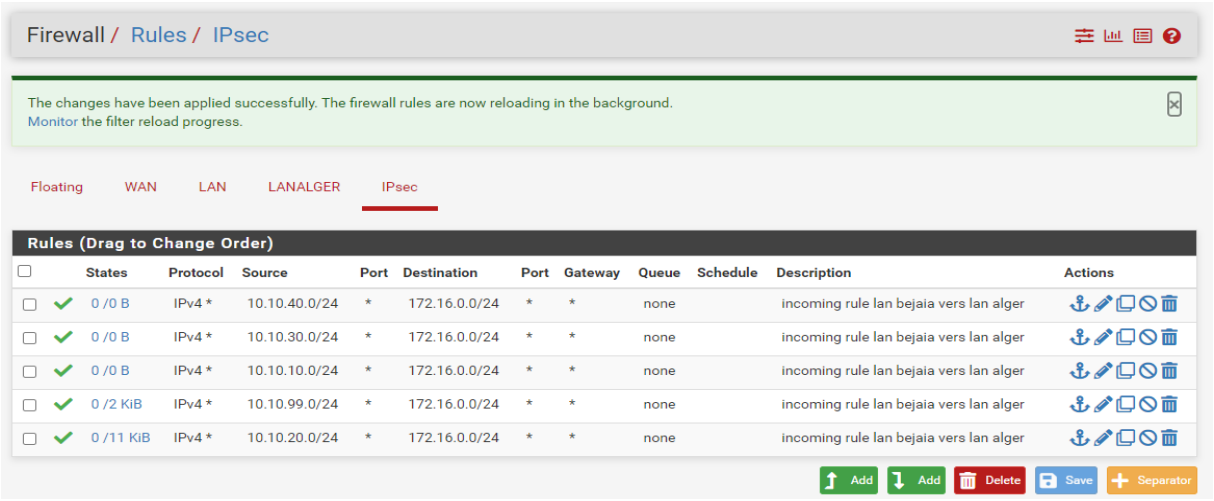
Sur PFSense Alger



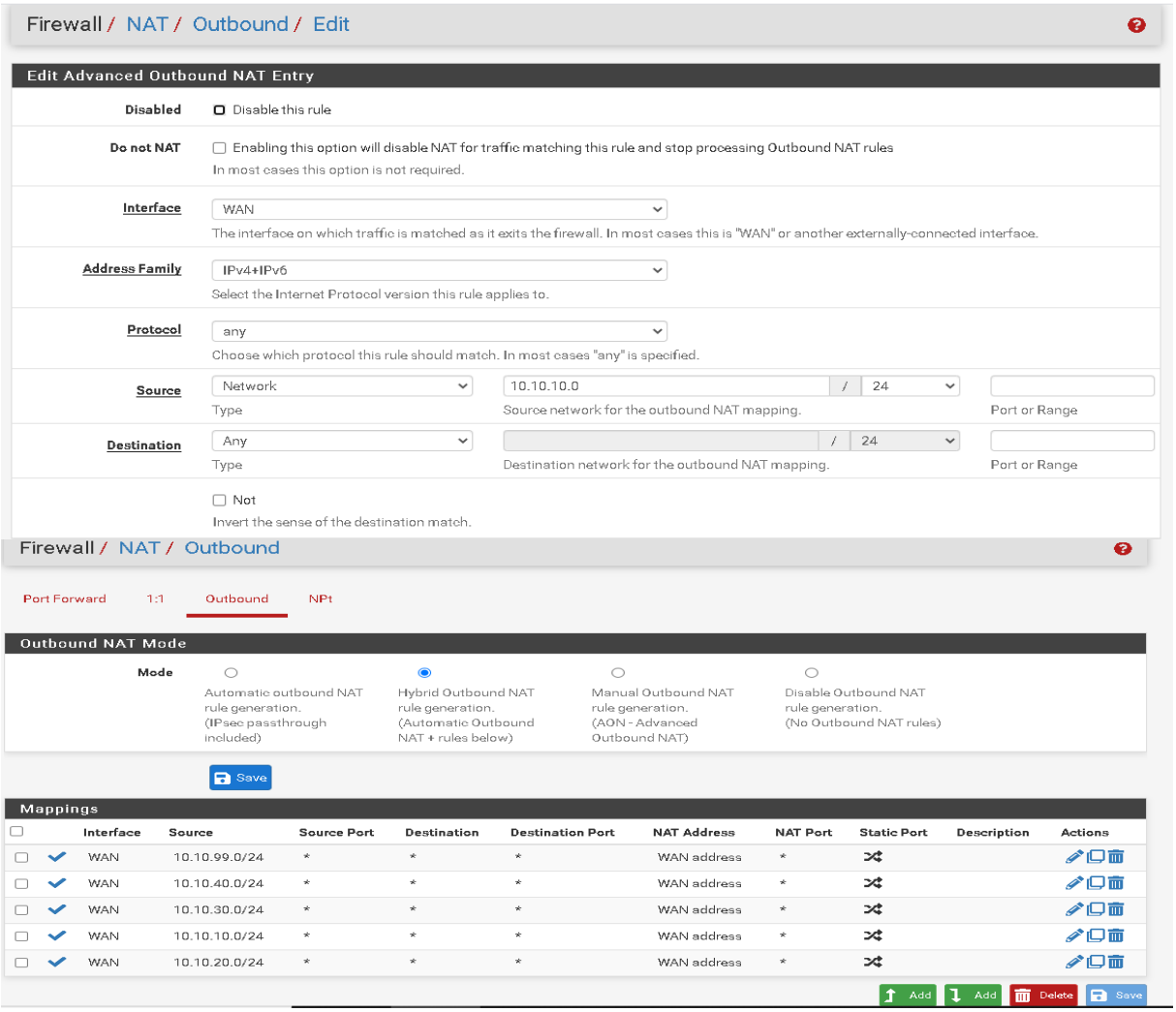
Sur PFSense Bejaia



Sur PFSense Alger



Configuration du NAT



Bibliographie

[1] :https://sonatrach.com/presentation

[2] : Code-Réseau-de-Transport-par-Canalisation_juin-2018

[3] : La haute disponibilité des réseaux campus. Cas d'étude Sonatrach

[4] :https://www.cisco.com/c/dam/global/fr_fr/assets/pdfs/isr/2900_data_sheet_c78_553896.pdf

[5] : https://www.cisco.com/c/en/us/support/switches/catalyst-3750-series-switches/series.html

[6] : https://formip.com/telnet-ssh/

[7] : https://www.cisco.com/c/fr_fr/products/security/vpn-endpoint-security-clients/index.html#~stickynav=3

[8] :https://cisco.goffinet.org/ccna/vlans/configuration-vlan-cisco-ios/

[9] : Le grand livre de sécuritéinfo ;consulté le 23 Mars 2016.

Résumé

Ce document s'inscrit dans le cadre de notre projet de fin d'études pour l'obtention du diplôme de master en Télécommunication, spécialité Réseau et Télécommunication à l'université ABDERRAHMANE Mira de Bejaïa. Il décrit notre travail durant notre stage au sein de la RTC Sonatrach.

L'objectif de la présente étude consiste à présenter une implémentation d'une architecture réseau pour la Région Transport Centre, cette solution consiste à mettre en place une redondance dans le réseau. A l'aide hyperviseur VMware et GNS 3, une architecture hiérarchique interconnectant différent équipements est proposée assurant ainsi la haute disponibilité afin de faciliter la communication entre les stations.