Table des matières

Liste des figures

Liste des tableaux

Introduction générale

L'infrastructure système et réseaux d'entreprise est le cœur de la majeure partie de l'activité informatique de l'entreprise.

Bien que les infrastructures puissent varier beaucoup en fonction de la taille de l'entreprise et de son activité, le réseau local, « outil » transverse par excellence et commun à tous les acteurs de l'entreprise, aura toujours une importance capitale au sein de celle-ci.

Ceci est particulièrement vrai pour les entreprises et autres entités qui sont fortement tributaires de leur système d'information pour la conduite des revenus. Les sociétés opérant dans des domaines comme le commerce, le service, la communication, etc. en sont le parfait exemple.

Par ailleurs, le réseau d'entreprise retracera souvent, par son évolution et sa complexité, l'historique et le vécu de toute l'entreprise. En effet, pour répondre au mieux à l'évolution des besoins et en essayant de tirer profit des évolutions de technologies, dispositifs et stratégies, ce dernier évolue considérablement. La virtualisation et les architectures orientées services en sont de parfaits exemples.

La gestion du réseau d'entreprise devient ainsi tout aussi importante dans la mesure qu'il devient essentiel d'en assurer la disponibilité. Ceci est d'autant plus difficile en raison des différentes menaces telles que le piratage, les attaques de déni de service, les virus et autre vol d'informations, etc., synonymes d'indisponibilité, de perte de données voire de baisse de crédibilité et de rentabilité globale.

C'est dans ce contexte que s'inscrit notre projet de fin d'études, intitulé « Refonte d'infrastructure système et réseaux informatique d'un client dans le secteur industrielle de câblage et de montage », proposé dans le cadre d'une collaboration entre Université Virtuelle de Tunis (UVT) et la société B2M.

Notre projet consistera à installer, configurer et mettre en place une nouvelle solution d'infrastructure système et réseaux informatique chez le client ICeM.tn (Industrielle de Câblage et de Montage) afin d'offrir un service informatisé robuste, optimal et fiable qui répondra à ses besoins et qui lui donnera plus de moyens afin de mieux répondre aux exigences de ses projets.

Afin d'illustrer la démarche de notre travail, nous présenterons dans ce qui suit l'organisation

générale du présent rapport qui s'articulera autour de quatre chapitres :

Dans le premier chapitre, nous exposerons le cadre du projet à travers une présentation de la société, et une présentation générale du projet ainsi qu'une étude de l'existant (description et critique).

Le deuxième chapitre sera consacré à l'état de l'art, dans lequel nous introduirons les différents domaines que touchera notre projet.

Dans le troisième chapitre qui concerne la présentation générale de notre solution, nous analyserons les solutions à mettre en place ainsi que les technologies à utiliser.

Le dernier chapitre sera consacré à la mise en place de la solution sécurisée. Nous présenterons l'environnement matériel et logiciel. Nous détaillerons aussi les étapes de la réalisation et la mise en place de la solution et nous illustrerons enfin quelques scénarios de fonctionnement de notre nouvelle architecture.

Pour conclure, nous présenterons les connaissances acquises durant ce stage et nous proposerons un ensemble de perspectives d'évolution de notre travail.

Chapitre 1 : Présentation générale du projet

Introduction

Ce chapitre sera consacré à une représentation du cadre générale de notre projet. Cette partie portera sur une présentation de l'organisme d'accueil et l'infrastructure réseau existante dans le but de comprendre le contexte général du projet et sa mise en œuvre en précisant les différentes étapes de réalisation.

1. Présentation de la société d'accueil

B2M-IT est une SSII tunisienne spécialisée dans les solutions intégrées d'entreprise.

Depuis 2008, année de création, B2M ne cesse de s'affirmer sur le marché IT tunisien comme un acteur de référence dans le monde des solutions IT, Progiciels de gestion et ERP, ingénierie logicielle, infogérance et développement web.

Aujourd'hui, B2M déploie des projets en Europe, Moyen-Orient et Afrique et s'est forgé une expérience confirmée et reconnue dans l'outsourcing des services informatiques offshore.

Grâce à son expertise éprouvée dans l'intégration de solutions de gestion, B2M a réussi à se positionner également comme un partenaire stratégique pour les entreprises leaders dans le marché des solutions IT. C'est ainsi qu'elle s'est vue attribuer la réputation d'être tout d'abord un conseiller et partenaires à ses clients avant d'être un prestataire de services et fournisseur de solution IT.

Figure 1- 1 : Logo B2M

1.1. B2M Partenariat

Le partenariat que nous avons établi avec Microsoft est un des piliers de la stratégie deB2M, étant donné que l'intégration des solutions de gestion, notamment la gamme Microsoft Dynamics (NAV et AX) fait partie du cœur du métier de B2M.

Pour construire ses solutions et ses services, B2M a fait le choix des solutions et des technologies de Microsoft, notamment Microsoft Dynamics NAV (NAVISION), Microsoft Dynamics AX (AXAPTA) et Microsoft Dynamics CRM devenant ainsi le cœur du métier de l'intégration des solutions de gestion chez B2M.

B2M et Microsoft ont su développer une relation forte. Nos clients bénéficient ainsi d'une vraie valeur ajoutée, à travers une démarche dynamique, innovante et complémentaire.

Afin d'intégrer des solutions métier adaptées à l'activité de ses clients, cette entreprise a fait le choix des solutions de gestion verticales NAVIBAT, la solution bâtiment, pour le secteur BTP et NAVIONE, la solution de gestion d'affaires, pour les entreprises des services professionnels, bureaux d'études Gesway développe une véritable activité d'éditeur, et distribue ses offres à l'échelon national et international au travers d'un réseau de partenaires.

B2M est le partenaire et représentant exclusif des solutions métier NAVIBAT et NAVIONE en Tunisie.

Depuis 2009, une collaboration est née entre B2M et ACCENTURE, notre partenariat a été fondé sur le partage du savoir-faire et des compétences. En effet, les consultants de B2M ont assuré pour ACCENTURE le roll-out des projets Dynamics NAV dans différents pays africains (côte d'ivoire, Cameroun, Ghana), au Moyen orient et en Amérique du sud chez les filiales des clients finaux d'ACCENTURE.

Fière de ce partenariat, B2M a su gagner la confiance d'ACCENTURE et renouveler les collaborations avec les autres filiales, toujours autour des solutions Dynamics.

Le secteur textile étant l'un des secteurs les plus importants en Tunisie, B2M a pensé à offrir aux entreprises appartenant à ce secteur la solution de gestion qui réponde à leurs besoins particuliers. B2M a été choisi par K3, éditeur de *Pebblestone Fashion*, pour représenter la solution en Tunisie. Cela nous permet d'être à l'écoute du secteur textile, chaussures, cuir, mode et accessoires

Figure 1- 2 Partenariat B2M

2. Présentation de la société client

ICeM.tn est une société spécialisée confirmé dans l'étude et la fabrication des câbles et faisceaux électrique aux véhicules (légers, moyens et lourds). Elle fait lancé dans le domaine d'évolution et de développement technologique afin de faire face à la conjoncture actuelle dans l'industrie automobile qui se caractérise par la compétitivité et les profonds changements quotidiens malgré la stagnation des marchés traditionnels qui dure depuis des années et l'augmentation du coût des matières premières ainsi que celui de l'énergie. 7

Figure 1- 3: Logo ICEM.tn

3. Description général du projet

3.1. Cadre du stage

Le présent travail s'inscrit dans le cadre du stage de fin d'études en vue de l'obtention du Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux "N2TR" de l'université Virtuelle de Tunis. Le Stage s'est déroulé sur 4 mois au sein des locaux de B2M et ICEM.tn.

3.2. Contexte général du projet

Toute entreprise existante d'une certaine taille dispose en général d'un réseau informatique, même celles qui n'en sont qu'à une idée de projet y pensent sérieusement à l'infrastructure système et réseau au sein de leur future structure. Vu l'importance des informations qui sont souvent véhiculées dans les réseaux, ceux-ci requièrent un certain degré de sécurité.

Toutes ces raisons ont amené ICEM.tn à réfléchir pour renforcer son réseau local et mettre en place une nouvelle Infrastructure Système et Réseaux plus robuste et plus sécurisée en bénéficiant des nouvelles fonctionnalités du réseau local et de la sécurité du système d'information.

3.3. Objectif du projet

Notre client ICEM.tn a décidé de faire, une refonte complète de son infrastructure informatique, afin de répondre mieux à l'évolution de sa croissance et ses besoins.

Le travail qui nous a été confié consiste à :

- Mettre en place une solution de virtualisation
- Configuration des serveurs virtuels
- Configurer une méthode d'authentification avec AD pour accéder à internet.
- Mettre en place un Progiciel de gestion intégré EPR
- Mettre en place une solution d'outils de productivité et de collaboration Microsoft via cloud
- Mise en place d'une politique de sauvegarde
- Superviser les travaux de câblages

- Mettre en place et paramétrer des nouveaux équipements réseaux LAN.
- Segmenter le réseau local par département.
- Mettre en œuvre de nouvelles politiques de sécurité (Internes et Externes).
- Configurer les règles de filtrage Pare-feu web et application.

4. Etude de l'existant

Cette partie couvre l'ensemble des spécifications de l'infrastructure Informatique et technologique requise par ICEM.tn. Elle contient tous les détails sur l'infrastructure réseaux, matériels et systèmes.

4.1. Architecture réseaux

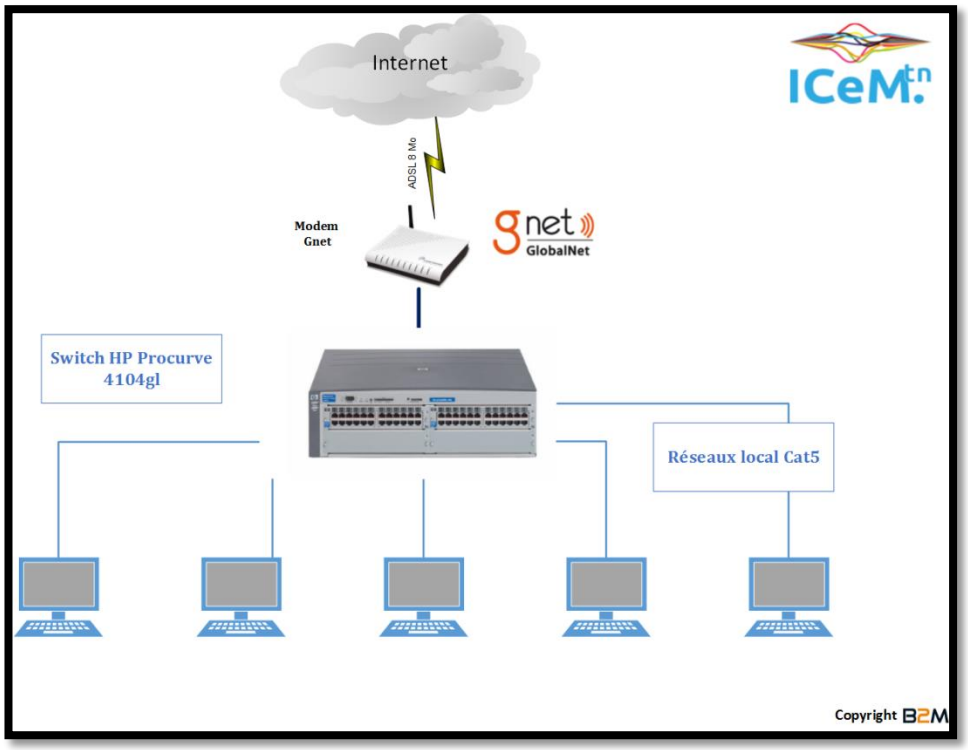


Figure 1- 4: Architecture réseaux

- **Switch HP Procurve 4104gl**

Ce switch prend en charge 96 ports 10/100, ou 80 ports Gigabit et 8 mini-GBIC (maximum) ou une combinaison des deux.

Principales caractéristiques :

- Montage en rack : Se monte dans une armoire telco ou une armoire pour matériel 19 pouces EIA standard (montage à l'horizontale uniquement)
- Capacité de routage/commutation : 18,3 Gbit/s
- Débit : Jusqu'à 37.5 mpps (millions d'impulsions par seconde)
- Fonctions d'administration : ProCurve Manager Plus ; ProCurve Manager (inclus) ; interface de ligne de commande ; navigateur Web ; menu de configuration ; gestion hors bande (RS-232C série)
- Alimentation électrique nécessaire : 100 - 127 V CA/200 - 240 V CA ; 50/60 Hz
- Consommation électrique : 630 Watts

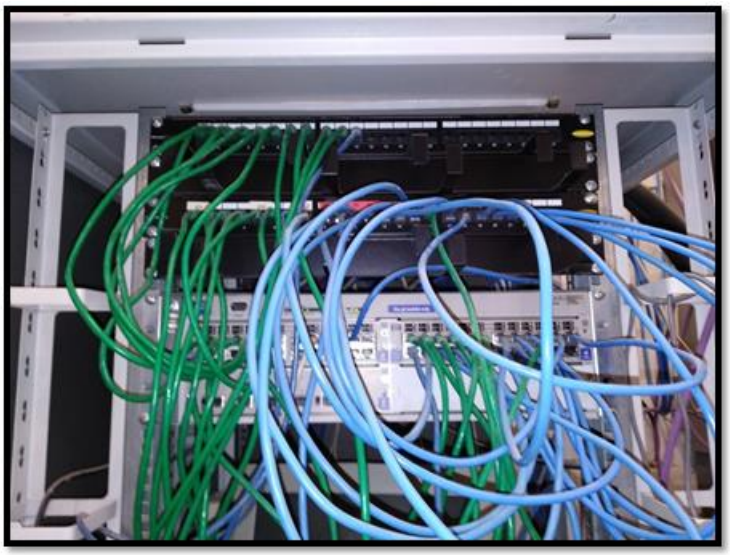


Figure 1- 5: Etat d'armoire avant le projet

Siége	Description
ICeM « usine »	1 x Switch HP Procurve 4104gl
Câblage informatique et téléphonique	3 Platines de 24 ports dont 1 informatique, 2 téléphonique.
Connexion Internet	Modem ADSL GlobalNet 4 Mbps

Tableau 1- 1: Les composants des réseaux LAN et WAN

L'architecture réseaux existante est basée seulement sur le switch Switch HP Procurve 4104gl niveau 2 non configuré ancien model et l'exploitation du réseau Wan avec le modem internet

Gnet qui couvre seulement 5% de la totalité de l'usine en wifi.

Voici les différents constats :

- Câblage informatique ancien qui occupe de la place dans les armoires ainsi que l'état des prises du côté utilisateurs.
- Absence de Prises Réseau dédiée pour chaque utilisateur.
- Absence d'un schéma de câblage informatique clair.
- Utilisation de plusieurs catégories de câble réseau (Cat5, Cat5E, Cat6).
- Partage d'un seul câble réseau entre plusieurs utilisateurs et machines.
- Absence de Configuration pour la sécurité Réseaux.
- Absence d'une architecture en étoile pour le réseau informatique.
- Absence d'une esthétique de l'armoire informatique du répartiteur général.
- Problème de lenteur (débit) de la connexion Internet ADSL GlobalNet.
- Absence d'une politique de partage de données entre les serveurs et les applications
- An33cienne technologie de téléphonie qui pose des problèmes de qualité de communication.

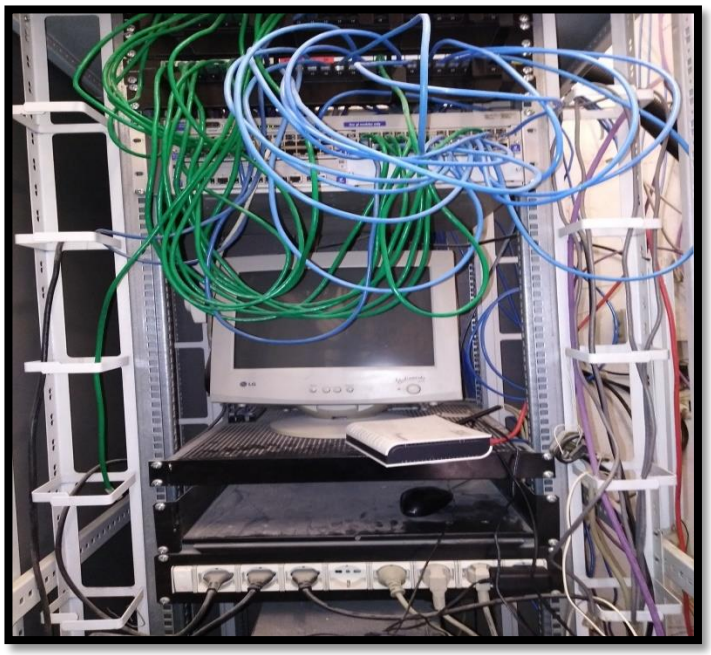


Figure 1- 6: Etat de l'armoire avant le projet im2

4.2. Architecture Système

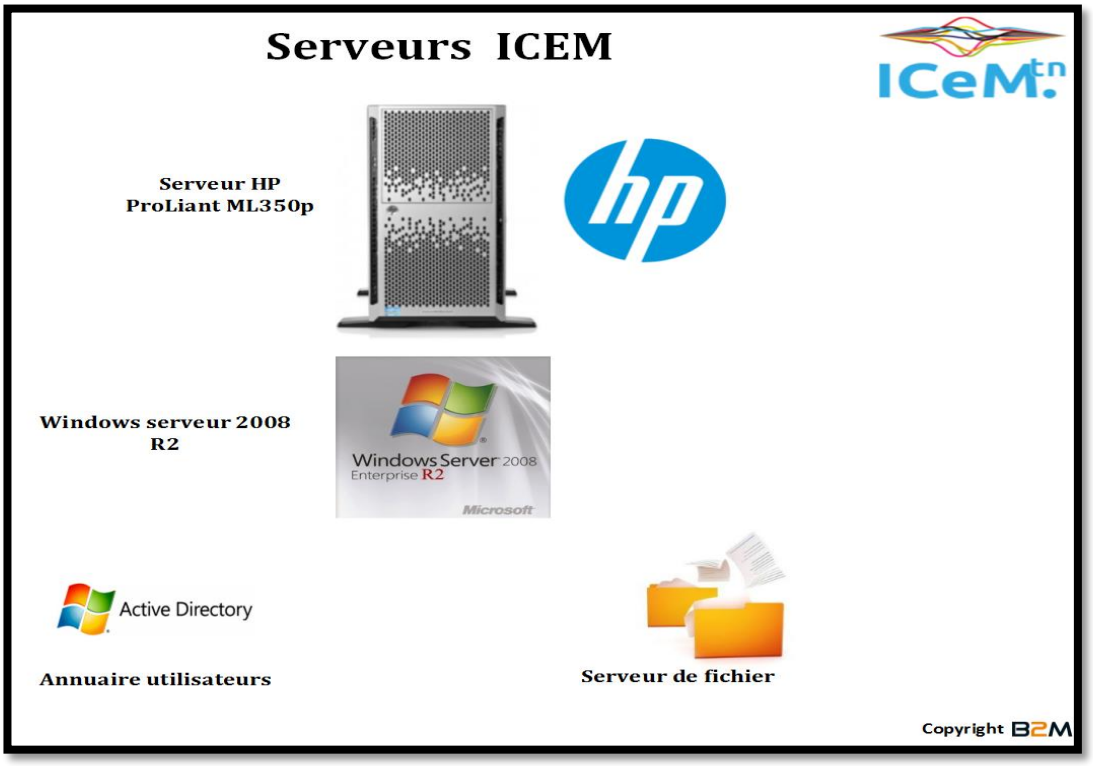


Figure 1- 7: Architecture Système Existante

4.2.1. Architecture Système Existante

L'architecture système est composée d'un seul serveur physique HP Proliant ML350P G8 non virtualisée a pour système d'exploitation Windows server 2008 R2 qui comporte l'annuaire utilisateurs active directory et les fichiers partager de la société.

Nom serveur	Caractéristiques	Services
Serveur-ICeM	HP Proliant ML350P G8 16G RAM / 300G * 3 Windows Server 2012 R2 Standard 64Bits 4 * Carte réseau	Active directory DHCP, DNS Application Production

Tableau 1- 2:Serveur-ICeM

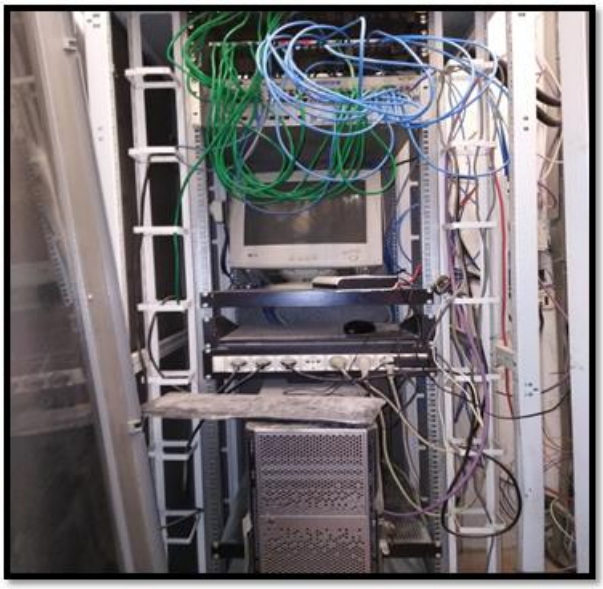


Figure 1- 8: Etat de l'armoire avant-projet im3

5. Solution proposée

Comme solution proposée nous visons à mettre en place un une nouvelle infrastructure système et réseaux.

Doit être segmenté en modules principales :

- Un module qui représente le réseau informatique d'entreprise LAN.
- Un module qui représente un Datacenter pour l'hébergement des serveurs locaux.

Chacun des modules aura des spécifications en sécurité, performance et disponibilité. Certains modules peuvent être fusionnés.

5.1. Objectifs visés et résultats attendus

Pour mettre en place un réseau d'entreprise modulaire voilà la liste des instructions proposées

Refonte de l'infrastructure et de l'architecture Réseau Local :

- Câblage Informatique de toutes les prises Réseaux Cat6.
- Mise en place des nouveaux switches Ethernet.
- Mise en place d'un Firewall (contrôle d'accès et filtrage web).
- Mise en place d'un point d'accès WIFI.

- Augmenter le débit internet : Mise en place d'une connexion Fibre Optique.
- Vérification du câblage téléphonique.
- Mise en place d'une nouvelle solution téléphonique.

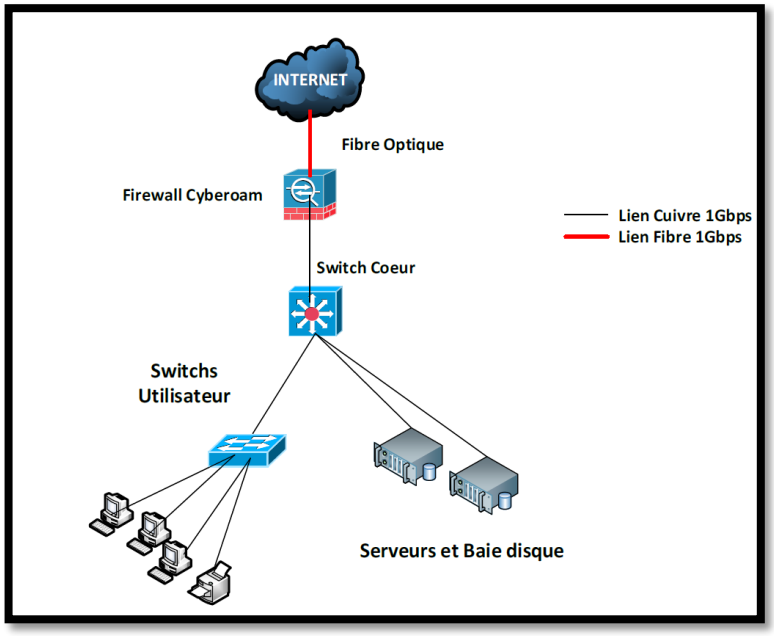


Figure 1- 9: Architecture Réseaux Proposer

Désignation	Quantité
Switch Cisco Switch 2960X 24 Ports 10/100/1000	2
Point d'accès Wifi CISCO AIR-LAP1041N-E-K9	2
Firewall Cyberoam CR25, 4 ports 10/100/1000	1
Prises Réseaux Informatique	42
Connexion Internet FO 10 Mbps	1

Tableau 1- 3: Listes des matérielles pour le projet

Refonte de l'infrastructure et de l'architecture Système :

- Reconfiguration du serveur Physique.
- Installation d’un Hyperviseur
- Configuration du domaine Active directory.
- Configuration des postes Client.
- Mise en place d’un serveur de partage
- Mise en place d’une politique de sauvegarde.

Conclusion

Comme le montre ce chapitre, l’évolution de l’entreprise exige une modification de l’infrastructure actuelle afin de renforcer le réseau et le système local et avoir une infrastructure conforme aux obligations colossales prévues. Il sera donc nécessaire de comprendre et détailler le réseau informatique, les différents protocoles et les équipements de l’entreprise avant d’entamer la phase de réalisation du projet

Chapitre 2 : Etat dès l'Art &Technologies Utilisées dans le Projet

Introduction

Le premier chapitre nous a permis d'avoir une idée sur les différentes technologies à utiliser, ce qui nous permet de placer notre projet dans son contexte.

Dans ce chapitre, nous commençons dans une première partie par définir le système informatique d'entreprise et la virtualisation informatique, ensuite, nous allons citer les avantages et les inconvénients de la virtualisation et leur impact sur les entreprises.

Puis dans une deuxième partie nous définissons le réseau informatique d'entreprise et les différents protocoles ainsi les équipements de base d'un réseau informatique sécurisé.

1. Le système informatique

Le système d'information est aujourd'hui un élément central du fonctionnement d'une organisation. Un système d'information peut être défini comme un ensemble de ressources (personnel, logiciels, processus, données, matériels, équipements informatique et de télécommunication...) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion des informations (textes, images, sons, vidéo...) au sein d'une organisation. Parmi les ressources informatiques figurent en particulier les fichiers de données, bases de données et système de gestion de bases de données (S.G.B.D.), les progiciels de gestion intégrés, les outils de gestion des clients, les outils de travail collaboratif, les applications métiers, les serveurs d'application ou de présentation (Web...), les systèmes de workflow, les architectures d'intégration, les infrastructures réseaux.

1.1. La virtualisation

La virtualisation est le processus qui joue le rôle de faire fonctionner plusieurs systèmes, serveurs et applications, sur un même serveur physique.

La virtualisation est un mécanisme informatique qui repose sur le processus suivant :

- Un système hôte c'est un système d'exploitation principal est installé sur un serveur physique unique, ce système sert d'accueil à d'autres systèmes d'exploitation.
- Un Hyperviseur c'est un logiciel de virtualisation, il est installé sur le système d'exploitation principal, il permet l'implémentation d'environnements sur lesquels seront installés d'autres systèmes d'exploitation, ces environnements sont des machines virtuelles.
- Chaque système installé dans une machine virtuelle fonctionne indépendamment des autres systèmes d'autres machines virtuelles.
- Chaque machine virtuelle possède un accès aux ressources du serveur physique (mémoire, espace disque…). [1]

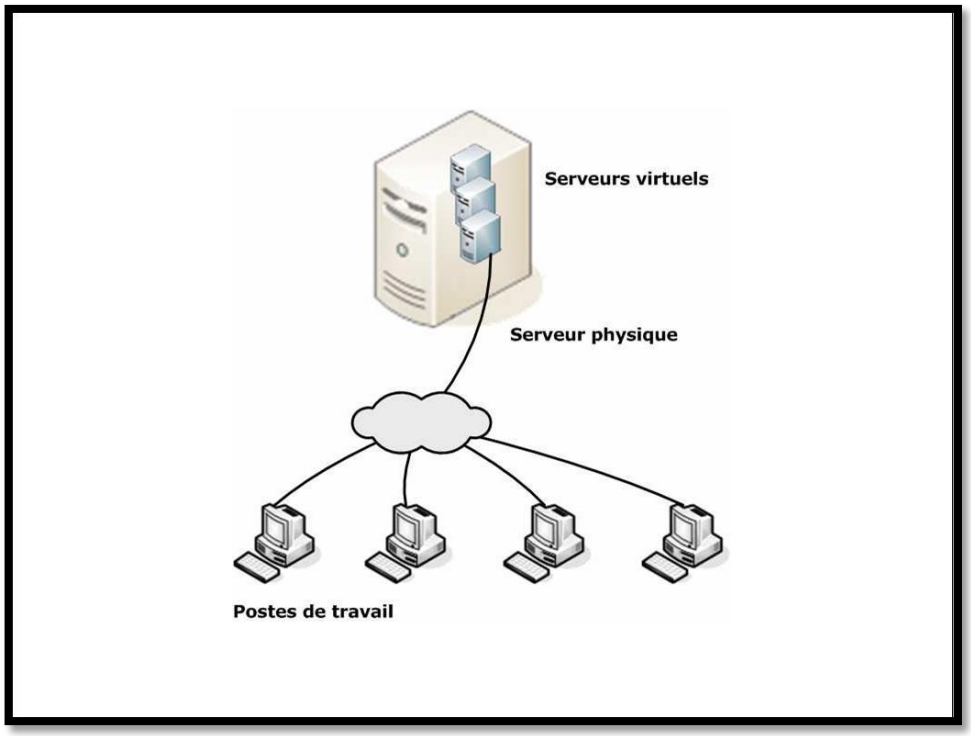


Figure 2- 1:Architecture générale de la virtualisation

1.1.1. Usages

La virtualisation sert différents types d'application :

- L'installation de différents systèmes d'exploitation sur un seul serveur.
- L'implémentation d'un Plan de retour d'activité rapide en cas d'incident.
- Test des applications sur de nombreux systèmes dans les phases de développement.
- L'amélioration de la montée en puissance du système d'information [1].

1.1.2. Avantages

La virtualisation fournit les avantages suivants :

- Stabilisation et consolidation d'un parc de serveurs en entreprise : les entreprises ne sont plus obligées d'acheter un serveur physique pour chaque application.
- Optimisation des coûts de matériels informatiques.
- L'installation de plusieurs systèmes d'exploitation sur une même machine.
- La portabilité des serveurs : une machine virtuelle peut être déplacée d'un serveur physique vers un autre.
- Accroissement d'applications en entreprise et des déploiements de systèmes.
- L'ensemble des serveurs est administré de façon simple.
- Baisse de la facture d'électricité, en minimisant le nombre de serveurs physiques. [1]

1.1.3. Inconvénients

Ils existent plusieurs inconvénients de la virtualisation :

- **Coût considérable**

Pour un fonctionnement convenable d'une architecture virtualisée, l'entreprise doit réaliser un investissement dans un serveur physique comportant plusieurs processeurs et largement de mémoires.

- **Pannes étendus :**

Les machines virtuelles tombent automatiquement en panne si le serveur physique tombe en panne.

- **Vulnérabilité généralisée :**

Lorsque l'Hyperviseur se bloque ou il y a une faille de sécurité, les machines virtuelles ne sont plus protégées [1].

1.2. Les impacts de la virtualisation sur les entreprises

Aujourd'hui les entreprises sont exposées à plusieurs enjeux dont la virtualisation leurs trouve plusieurs solutions.

Parmi ces solutions : La réduction des coûts, gain de productivité, augmentation de la sécurité….. La diminution des coûts est généralement l'enjeu n°1 des entreprises, précisément en période de crise économique ou la stratégie repose davantage sur l'adage « faire plus avec moins », la virtualisation présente donc un moyen technologique de baisser les dépenses.

- **Réduction des coûts de matériel**

La virtualisation permet de minimiser le nombre de serveurs physiques du parc informatique de l'entreprise.

L'entreprise diminue ses achats de machines en utilisant la virtualisation car un seul serveur peut supporter plusieurs systèmes et applications.

- **Diminution des coûts immobiliers**

L'entreprise améliore son espace disponible en réduisant le nombre de serveurs de son parc informatique.

La virtualisation permet aux grandes entreprises d'améliorer leurs dépenses vers d'autres départements et offre ainsi un gain de place.

- **Réduction des coûts de maintenance**

La virtualisation facilite la tâche de l'administrateur de système d'information de l'entreprise car il doit s'occuper d'un nombre limité de machine et son temps est ainsi amélioré.

Les opérations de maintenance de chaque serveur sont devenues plus faciles grâce à la

virtualisation qui permet de mutualiser plusieurs serveurs sur une même machine.

- **Réduction de la facture énergétique**

La facture d'électricité diminue lorsque le nombre de serveurs physiques dans l'entreprise réduit.

- **Augmentation de la sécurité**

La sécurité du système d'information des entreprises est optimisée grâce au rôle principal qui joue la virtualisation.

L'impact des machines virtuelles sur la sécurité est notable à plusieurs niveaux :

- ✓ Lorsque on utilise le mécanisme de virtualisation les systèmes et les applications sont divisés dans des unités fermées appelées machines virtuelles, et isolés des autres services, des autres machines et du reste du réseau.
- ✓ Les machines virtuelles sont distinctes du système hôte, elles possèdent des adresses IP, un système de fichier et leur propre accès au service.
- ✓ Le serveur physique devient invisible sur le réseau et il reste que les machines virtuelles visibles.
- ✓ Le déplacement des machines virtuelles d'un serveur physique à un autre est possible sans arrêt de service.

- **Tests d'applications**

Les développeurs ont l'opportunité de tester et de déboguer leurs applications avant la mise en production par suite de l'installation de plusieurs systèmes sur une seule machine.

La mise à disposition de plusieurs machines distinctes est nécessaire pour toutes ces procédures.

- **Amélioration de la disponibilité des services de l'entreprise**

La virtualisation permet de lier des machines virtuelles à des systèmes clés de l'entreprise (comme le stockage) et d'y garantir en permanence l'accès.

Une autre machine virtuelle permet de préserver la qualité de service lorsqu'il y a une défaillance [2].

1.3. Les différents types de virtualisation :

La **Figure 2.2** montre les différents types de la virtualisation

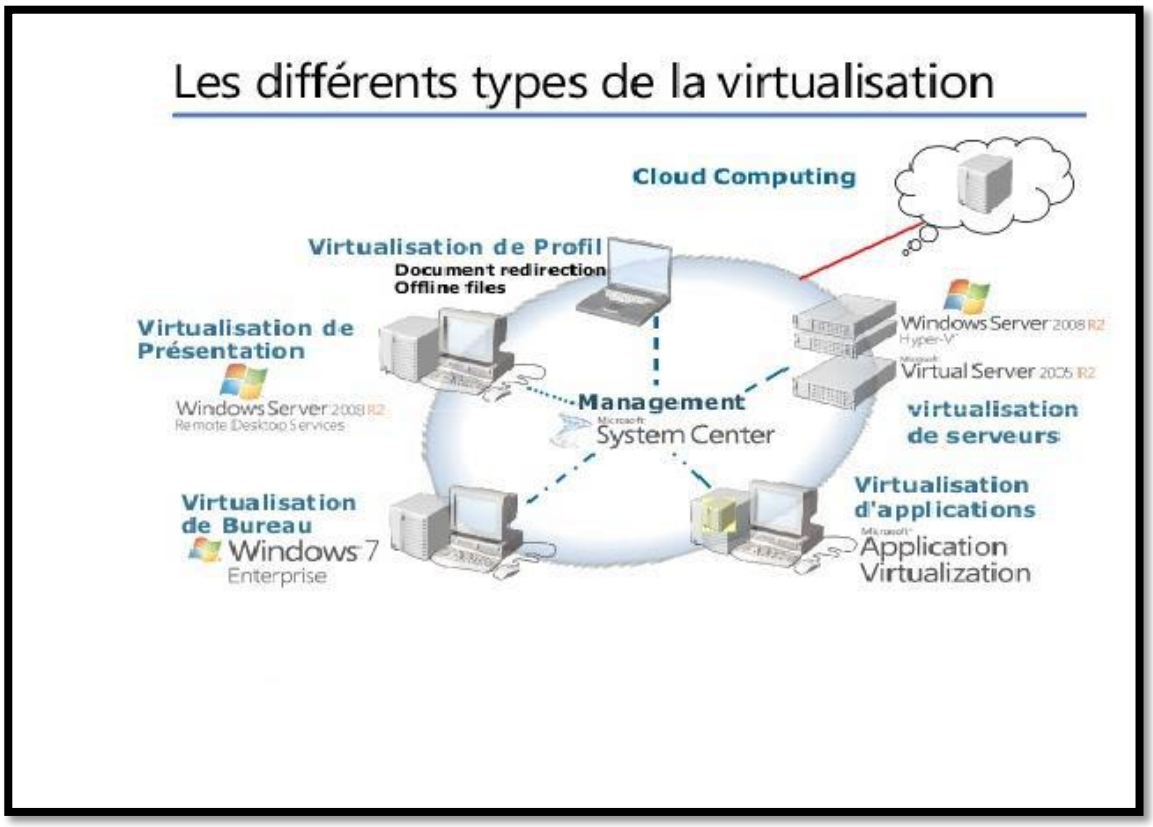


Figure 2- 2:Les différents types de la virtualisation

Il existe quatre types de virtualisation :

- ✓ La virtualisation de serveur
- ✓ La virtualisation d'application
- ✓ La virtualisation de postes de travails
- ✓ La virtualisation de stockage

- **La virtualisation de serveur**

La virtualisation de serveur sert à rassembler plusieurs serveurs physiques sur un seul hôte qui exécute des systèmes virtuels et minimise le nombre d'administration.

- **La virtualisation d'application:**

Elle permet de diviser l'application du système d'exploitation hôte et des autres applications

présentes pour éviter les conflits.

D’autre part elle est probablement la technologie qui permet la séparation de l’environnement du bureau et des autres applications associées de la machine physique.

- **La virtualisation des postes de travail**

Grâce à La virtualisation des postes de travail les administrateurs systèmes et réseaux peuvent gérer facilement les postes de travail et de répondre avec docilité aux requêtes des utilisateurs.

Un poste de travail virtualisé peut être concentré soit directement sur l’ordinateur de l’utilisateur soit sur un serveur dans le centre de données.

- **La virtualisation de stockage**

La virtualisation des stockages facilite la meilleure exploitation des ressources, et des disques durs.

Tout d’abord le centre de données doit être équipé d’un SAN (Storage Area Network) pour centraliser et sécuriser les données et un NAS (Network Attached Storage) c’est un élément de stockage lié directement au réseau local d’une entreprise [3].

2. Le réseau Informatique « IT Network »

En reliant toutes les stations de travail, les périphériques, les terminaux et les autres unités de contrôle du trafic, le réseau informatique a permis aux entreprises de partager efficacement différents éléments des fichiers, des imprimantes, etc. Il a permis aussi de relier les serveurs de données, de communication et de fichiers.

2.1. Réseau informatique d’entreprise

Le réseau d'entreprise permet de relier chaque ordinateur via un serveur qui va gérer l'accès à Internet, les mails, les droits d'accès aux documents partagés et le travail collaboratif.

Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe et est authentifié par le serveur. L'utilisateur peut accéder à ses données et au partage de fichiers.

Le réseau en entreprise permet à l'entreprise de centraliser ses données, de travailler en équipe de manière productive [4].

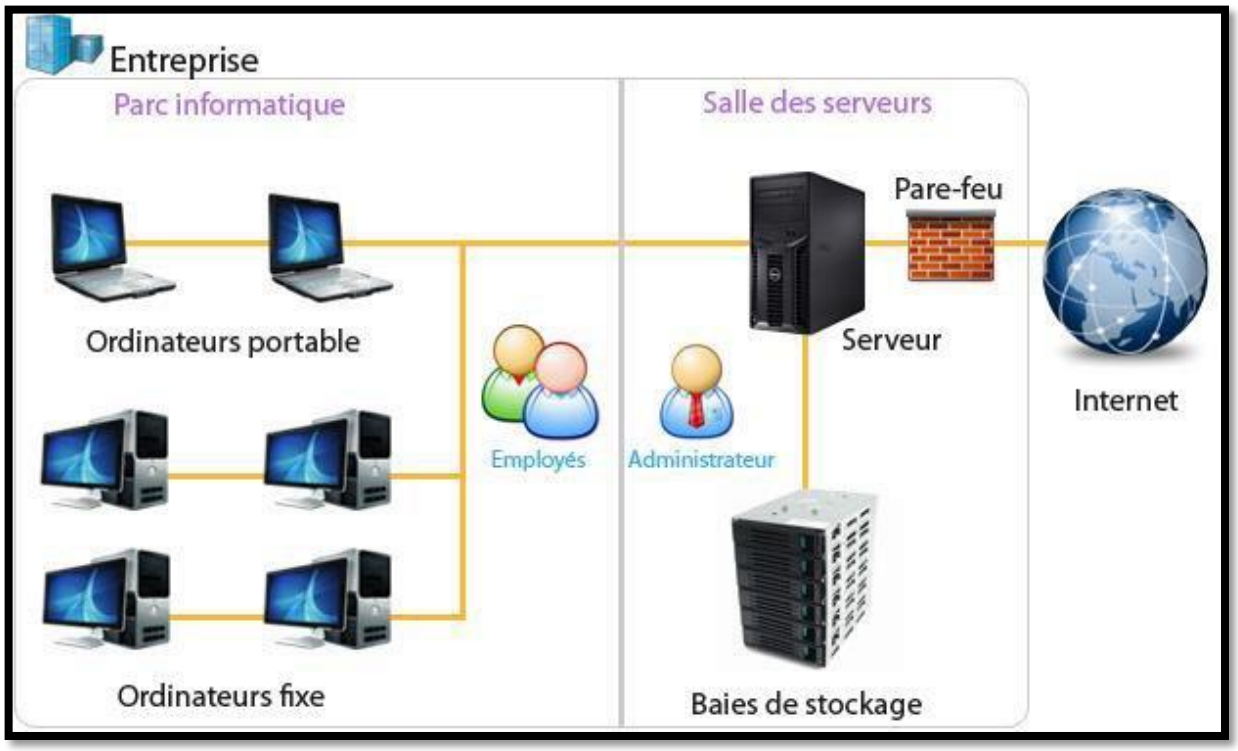


Figure 2- 3:Shéma type d'un réseau d'entreprise

2.2. Les protocoles du réseau LAN

La plupart des réseaux informatiques sont classée en réseaux locaux LAN et en réseaux WAN. Les réseaux locaux sont généralement situés à l'intérieur d'un immeuble ou d'un complexe et servent aux communications internes, alors que les réseaux WAN couvrent de vastes superficies et relient des villes et des pays. Les réseaux locaux et les réseaux WAN peuvent aussi être interconnectés.

2.3. Le modèle OSI

La première évolution des réseaux informatiques a été la plus anarchique, chaque constructeur développant presque sa propre technologie. Pour pallier à cela, l'ISO (Institut de normalisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseau Le modèle de référence OSI (Figure2.2) comporte sept couches numérotées, chacune illustrant une fonction réseau bien précise. Cette répartition des fonctions réseau est appelée organisation en couches [5].

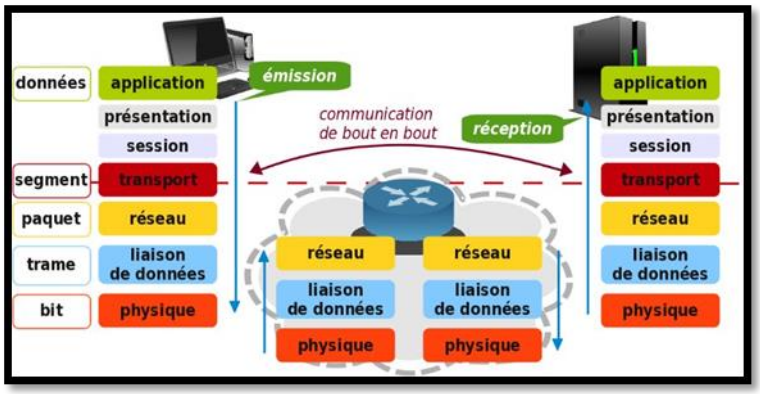


Figure 2- 4: Schéma du modèle OSI

2.4. Le modèle TCP/IP

Même si le modèle de référence OSI est universellement reconnu, historiquement et techniquement, la norme ouverte d'Internet est le protocole TCP/IP (pour Transmission Control Protocol/Internet Protocol). Le modèle de référence TCP/IP et la pile de protocoles TCP/IP rendent possible l'échange de données entre deux ordinateurs, partout dans le monde, à une vitesse quasi équivalente à celle de la lumière.

Les objectifs principaux de cette modélisation sont :

- Relier des réseaux hétérogènes de façon transparente
- (lignes téléphoniques, réseaux locaux, etc),
- Garantir les connexions quel que soit l'état des lignes de transmission
- (commutation de paquets),
- Assurer le fonctionnement d'applications très différentes
- (transfert de fichier, multimédia, etc) [5].

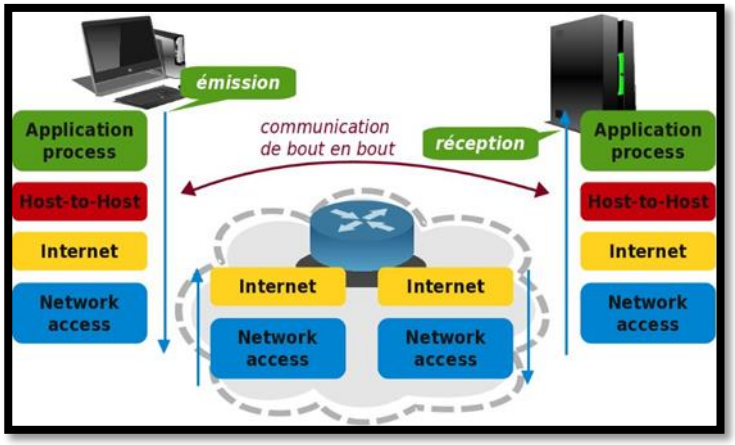


Figure 2- 5: Schéma modèle TCP/IP

2.5. Les réseaux locaux virtuels (VLAN)

Un réseau local virtuel (ou VLAN) est un groupe d'unités réseau ou d'utilisateurs qui ne sont pas limités à un segment de commutation physique. Les unités ou les utilisateurs d'un VLAN peuvent être regroupés par fonction, service, application, etc., et ce quel que soit le segment physique où ils se trouvent. Un VLAN crée un domaine de broadcast unique qui n'est pas limité à un segment physique et qui est traité comme un sous-réseau. La configuration d'un VLAN est effectuée, par logiciel, dans le commutateur. Les VLAN ont été uniformisés conformément à la spécification IEEE 802.1Q. Ils subsistent cependant des variantes d'implémentation d'un constructeur à l'autre [6].

2.6. Le protocole VTP

Le VTP (VLAN Trunking Protocol) est un protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques Cisco. Le VTP permet d'ajouter, renommer ou supprimer un ou plusieurs Vlans sur un seul switch (serveur) qui propagera cette nouvelle configuration à l'ensemble des autres switchs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des Vlans sur l'ensemble d'un réseau local [7].

2.7. Protocole Spanning-Tree

Le protocole *Spanning-Tree* (STP) est un protocole de couche 2 (liaison de données) conçu pour les *switchs* et les bridges. La spécification de STP est définie dans le document IEEE 802.1d. Sa principale fonction est de s'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes entre des matériels de couche 2. STP détecte et désactive des boucles de réseau et fournit un mécanisme de liens de backup. Il permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre deux stations

d'extrémité. Le protocole RSTP (*Rapid Spanning-Tree Protocol*) est défini par le standard IEEE 802.1w. Il diffère principalement de STP par sa convergence plus rapide. En effet, RSTP offre une convergence au minimum 5 fois plus rapide que STP. RSTP prend moins de 10 secondes pour converger. [8].

3. Les équipements de base d'un réseau informatiques

3.1. Les unités hôtes

Les unités directement connectées à un segment de réseau sont appelées hôtes. Ces hôtes peuvent être des ordinateurs, des clients, des serveurs, des imprimantes, des scanneurs ainsi que de nombreux autres types d'équipements

3.2. Les commutateurs « switchs »

Le commutateur est une unité de couche 2. Il prend des décisions en fonction adresses MAC (*Media Access Control address*). En raison des décisions qu'il prend, le commutateur rend le LAN beaucoup plus efficace [8].

Figure 2- 6:Commutateurs "Switchs" Cisco

3.3. Les routeurs

Le routeur est la première unité que vous utiliserez qui fonctionne au niveau de la couche réseau du modèle OSI, également appelée couche 3.En raison de leur capacité d'acheminer les paquets en fonction des informations de couche 3, les routeurs sont devenus le *backbone* d'Internet et exécutent le protocole IP. Le rôle du routeur consiste à examiner les paquets entrants (données de couche 3), à choisir le meilleur chemin pour les transporter sur le réseau et à les commuter ensuite au port de sortie approprié. Sur les grands réseaux, les routeurs sont les équipements de régulation du trafic les plus importants [9].

Figure 2- 7:Routeur Cisco

4. Sécurité Informatique d'entreprise

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet

Par ailleurs, avec le nomadisme, consistant à permettre au personnel de se connecter au système d'information à partir de n'importe quel endroit, les collaborateurs sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisé de l'entreprise.

La menace représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité constitue le niveau d'exposition face à la menace dans un contexte particulier.

Enfin la contre-mesure est l'ensemble des actions mises en œuvre en prévention de la menace.

Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon dont l'ennemi procède. Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions [10].

Figure 2- 8:Sécurité Informatique

La sécurité informatique vise généralement cinq principaux objectifs :

L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être.

La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.

- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information.
- Le non répudiation, permettant de garantir qu'une transaction ne peut être niée.
- L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

La sensibilisation des utilisateurs aux problèmes de sécurité

- La sécurité logique, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- La sécurité des télécommunications : technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
- La sécurité physique, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels [10].

5. Firewall « Pare-feu »

Chaque ordinateur connecté à internet (et d'une manière plus générale à n'importe quel réseau informatique) est susceptible d'être victime d'une attaque d'un pirate informatique.

La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant.

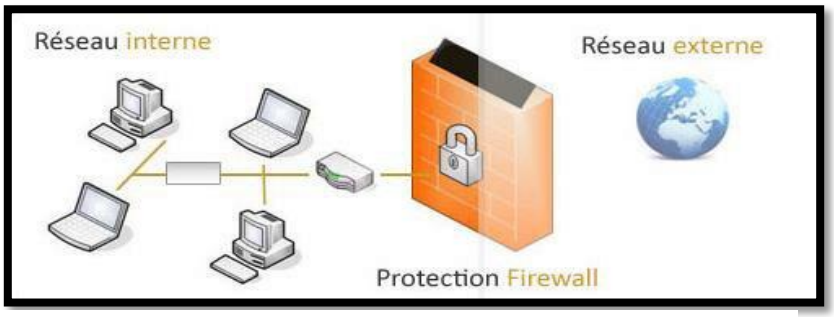


Figure 2- 9:Firewall (Pare-Feu)

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne).
- une interface pour le réseau externe.

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic.
- Le système soit sécurisé.
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Dans le cas où le système pare-feu est fourni dans une boîte noire « clé en main », on utilise le terme d'Appliance.

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées
- Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition

précise et contraignante des besoins en communication.

5.1. Les limites des firewalls

Un système pare-feu n'offre bien évidemment pas une sécurité absolue, bien au contraire. Les firewalls n'offrent une protection que dans la mesure où l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité

De la même manière, l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter fortement préjudice à la politique de sécurité globale.

Enfin, afin de garantir un niveau de protection maximal, il est nécessaire d'administrer le pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies.

6. VPN Réseau Privé Virtuel et sécurité

Un VPN est un réseau virtuel (c'est à dire non physique) permettant de faire comme si plusieurs machines (ordinateurs, tablette, smartphone, serveur…) faisaient partie d'un même réseau local, bien qu'elles soient en réalité à plusieurs endroits géographiques différents et reliées entre elles par le réseau Internet (qui lui n'est pas sécurisé).

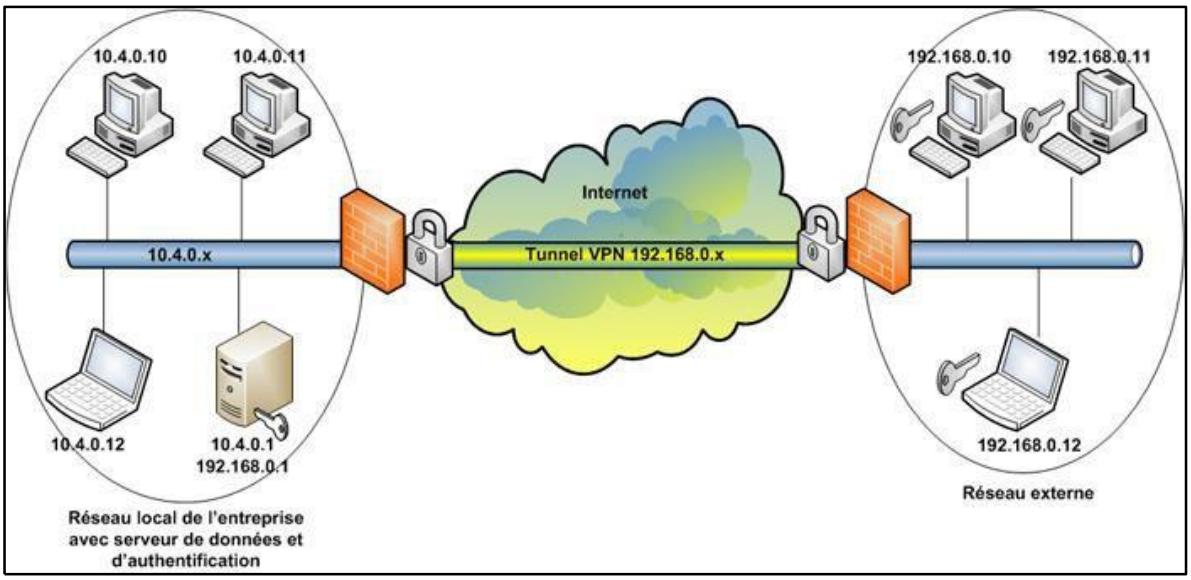


Figure 2- 10:VPN Réseau Privé Virtuel

Les VPN créent une connexion sécurisée qui permet de se prémunir contre l'interception des données par des tiers malveillants. Lorsqu'on utilise un VPN, l'ensemble du trafic Internet est crypté, contrairement à un proxy, qui passe par l'application utilisée pour accéder au web (par exemple le navigateur). Il existe cependant des solutions dites de « *split tunnelling* » permettant de déterminer quelles applications doivent faire transiter leurs données via le VPN, et quelles autres peuvent utiliser une connexion directe.

6.1. Usage Du VPN en entreprise

Grâce à l'utilisation d'un VPN, il n'est pas nécessaire pour les employés d'une entreprise d'être physiquement présents dans les locaux de cette dernière pour accéder au réseau local : intranet, imprimantes, applications métier… L'usage d'un VPN renforce également la sécurité et la confidentialité des données, notamment lorsque les employés sont en déplacement et utilisent des connexions wifi d'hôtel non sécurisées pour accéder à des données de l'entreprise [10].

7. Notion d'audit de sécurité

Un audit de sécurité (en anglais Security audit) consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité.

L'objectif de l'audit est ainsi de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions prises forme un tout cohérent.

Un audit de sécurité permet de s'assurer que l'ensemble des dispositions prises par l'entreprise sont réputées sûres [10].

Conclusion

Dans ce chapitre nous avons étudié quelques notions sur le système et le réseau d'informatique en général et le réseau de l'entreprise en particulier, tout en détaillant les principales caractéristiques et les différents protocoles et technologies utilisés. Ceci nous a permis de constituer une idée sur les fonctionnalités que doit assurer notre infrastructure informatique.

La prochaine étape sera donc l'analyse et la conception de la nouvelle architecture Système et réseau au sein d'ICEM.tn.

Chapitre 3 : Design de l'architecture Système et Réseaux

Introduction

La conception d'architecture d'un modèle type est l'une des étapes essentielles permettant d'assurer la rapidité et la stabilité d'un système d'information. Si un réseau n'est pas conçu adéquatement, de nombreux problèmes imprévus peuvent survenir, ce qui peut entraver son fonctionnement. La conception est véritablement un processus en profondeur. Dans ce chapitre, nous définirons un processus de conception d'un modèle type de configuration.

1. Architecture Système :

Notre solution consiste à l'implémentation et l'administration d'un environnement virtualisé de notre client ICEM.tn, l'objectifs essentiels pour notre solution sont : la réduction des coûts du matériels, une meilleur sécurité qui permettra de cloisonner les services par la séparation des différentes tâches du serveur physique aux machines virtuelles distinctes, l'amélioration de la disponibilité des services, la réduction de la facture énergétique et des coûts de maintenance.

Tout d'abord on va installer le logiciel VMware Esxi 6.5 pour gérer l'environnement virtuel sur le serveur, déployer et surveiller des machines virtuelles.

Ensuite on va installer Windows server 2016 et 2012 R2, pour chacun de nos serveurs et on va installer des fonctionnalités selon les besoins.

Par la suite, on va mettre en place l'AD active directory (services d'annuaire).

Enfin on va implémenter, installer et configurer différents serveurs :

- Serveur Exchange 2016 (gestion des Emails)
- Serveur de fichier (gestion des fichiers)
- Serveur Dynamics Navision 2016 (ERP)
- Serveur Symantec endpoint protection (anti-virus)

- Serveur Paie (gestion de paie)
- Configuration plateforme Office 365

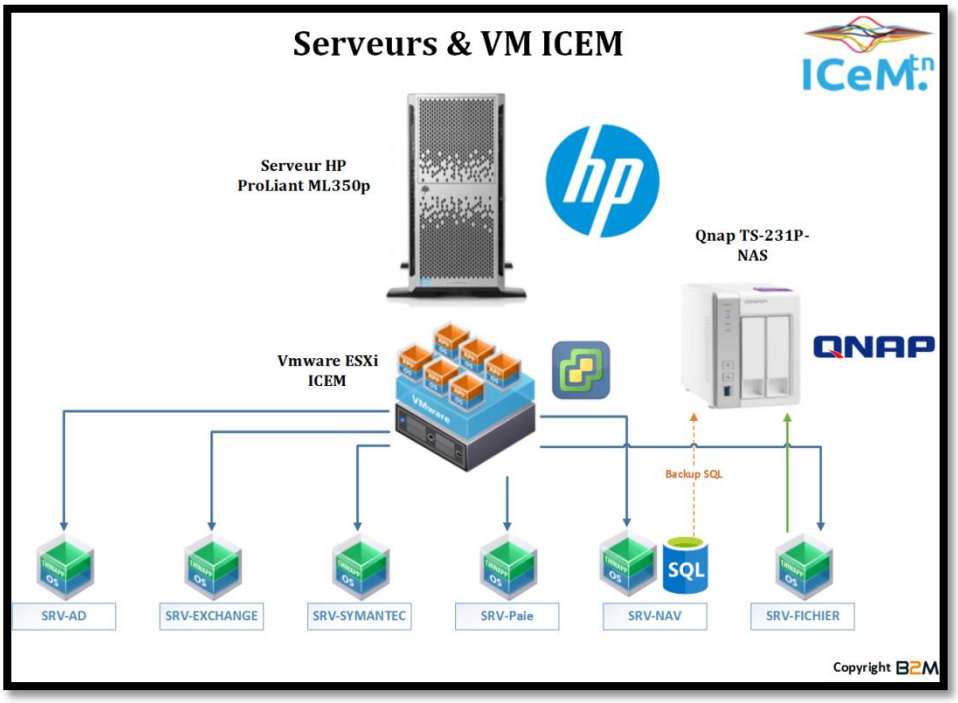


Figure 3- 1:Architecture générale de la solution

1.1. Equipements système

- Un serveur HP Proliant ML350P Format Tour 5U - Processeur Xeon® E5-2620 v2 (6 core, 2.1 GHz)- Memoire Cache 15 MO Level 3- Mémoire Standard 16GB (2x8GB) RDIMM- Disque Dur 3 x 300Go SAS 10K SFF up to 8
  Dernière génération de la gamme ProLiant ML (la gamme la plus vendue au monde)

Les serveurs HP ProLiant ML350p Gen8 offrent les performances, la disponibilité et l'extensibilité les plus élevées qui soient pour les datacenters d'entreprise, les filiales distantes et les entreprises en pleine croissance. En intégrant les technologies HP clés issues de l'architecture HP ProActive Insight, les produits ML350p Gen8 innovent en termes de mémoire, de gestion des serveurs et de micrologiciels, et de stockage de serveur. En associant ces innovations aux tout derniers processeurs Intel® Xeon®, ils offrent un système à la souplesse et à des performances inégalées [11].

Figure 3- 2:Serveur HP ProLiant ML350p Gen8

- Un serveur QNAP NAS TS-231P est un centre de stockage réseau puissant mais facile à utiliser pour la sauvegarde, la synchronisation, l'accès à distance et le divertissement à domicile [12].

Figure 3- 3:Serveur QNAP NAS TS-231P

1.2. Les Besoins fonctionnels

1.2.1. Installation de VMware Esxi 6.5

VMware ESX permet une gestion plus précise des ressources de chaque machine virtuelle et de meilleures performances. La solution VMware ESX est la solution la plus industrielle de la gamme. VMware ESX est basé sur une distribution RHEL5 (Red Hat Enterprise Linux 5)

modifiée, et comprend deux modules :

VMKERNEL : Ce module « noyau » gère et hiérarchise l'ensemble des ressources matérielles (mémoire, processeur, disques, réseaux) en fonction de chaque serveur, et gère les ressources physiques pour ESX.

SERVICE CONSOLE : permet la gestion de l'hyperviseur en mode commande. Accessible depuis le port 22 (SSH), cette console sert à lancer certaines commandes inaccessibles depuis l'interface graphique ou encore de parcourir les dossiers dans lesquels sont stockées les machines virtuelles.

Enfin elle peut permettre de collecter des informations de débogage sur les machines virtuelles ou sur le serveur ESX.

Nombres d'options sont disponibles par le biais de la "service console", il est cependant déconseillé de manipuler ESX depuis cette interface pour les novices.

La gestion des serveurs se fait à l'aide d'un navigateur via une interface web, à l'aide d'une console cliente (Virtual Infrastructure Client) ou d'un outil de gestion centralisé VMware nommé Virtual Center. La Service Console est devenue une machine virtuelle à part entière dans vSphere, et la Service Console est absente de la version ESXi du produit (le contrôle est alors effectué à travers une "BusyBox" directement sur la console matérielle ou à travers une console DRAC/iLO) [13].

1.2.2. Installation de Windows server 2016

Windows Server 2016 est un système d'exploitation pour serveurs x64 de Microsoft, faisant partie de la famille Windows NT destinée aux serveurs d'entreprise. Il est connu aussi sous le nom « Windows Server vNext ».

Parmi les nouvelles fonctionnalités figurent l'utilisation de containers (avec fonction d'isolation), les micros services et le cloud hybride.

Il utilise le noyau Windows NT 6.4, au même titre que Windows 10, ce qui fait qu'il ressemble visuellement à Windows 10 [14].

1.2.3. Installation de Windows server 2012

Microsoft Windows Server 2012, anciennement connu sous le nom de code Windows Server 8, est la seconde avant dernière version du système d'exploitation réseau Windows Server Page

d'aide sur l'homonymie. La version suivante est Windows Server 2012 R2. Windows Server 2016 est sorti le 1er octobre 2014 en phase de développement et est prévu pour le 3e trimestre 2016 en version finale [15].

1.2.4. Installation d'Active Directory

Active Directory (AD) est la mise en place par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

Il a comme base les standards TCP/IP et il existe dans le système d'exploitation Microsoft Windows Server 2000.

Le but d'Active Directory est de procurer des services centralisés d'authentification et d'identification à un réseau d'ordinateurs ayant comme système d'exploitation Windows.

Active Directory permet aussi d'appliquer et d'attribuer des stratégies, de distribuer des logiciels, et d'installer des mises à jour par les administrateurs [16].

1.2.5. Installation de serveur Exchange 2016

Microsoft Exchange server est un logiciel de groupe de travail « groupware » pour serveur de messagerie électronique.

Microsoft Exchange est hautement sollicité par les entreprises, il s'agit d'un produit de la gamme des serveurs Microsoft, destiné pour la messagerie électronique, encore plus pour l'organisation d'agenda, de contacts et de tâches, Il permet le stockage des informations.

Les avantages du serveur Exchange sont :

- Utilisation rapide et souple à travers des temps de basculement raccourcis.
- Une prise en charge de plusieurs bases de données par volume.
- Déploiement simple et rapide, haute disponibilité et équilibrage de charge client, interopérabilité avec les versions antérieures.
- Préserver toutes les données au même endroit en attribuant aux manipulateurs une archive sur place [17].

1.2.6. Installation de serveur de fichiers (Home-Folder)

Un serveur de fichiers est un serveur utilisé pour la gestion et l'emmagasinage des fichiers utilisateurs qui sont partagés dans des bases de données.

Il doit permettre un fonctionnement permanent, être performant, fiable, disposer de plusieurs types d'extensions et autoriser les changements des disques sans interruption de fonctionnement du serveur [18].

1.2.7. Installation de serveur Dynamics Navision 2016

Microsoft Dynamics NAV est un progiciel de gestion intégré, composant de Microsoft Dynamics, conçu pour les PME-PMI internationales et les filiales de grands groupes. Il permet de gérer l'ensemble des processus de l'entreprise : commerce & marketing, achats, production, logistique et distribution, gestion de projets, services client, gestion financière. Il y a aujourd'hui plus de 100 000 installations de Microsoft Dynamics NAV et plus d'un million d'utilisateurs dans le monde [19].

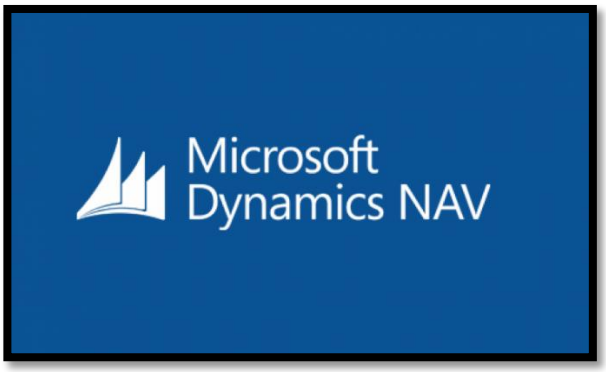


Figure 3- 4 : Logo Dynamics Nav

1.2.8. Installation de serveur Microsoft SQL Server 2014

Microsoft SQL Server est un système de gestion de base de données relationnelle développé par Microsoft. En tant que serveur de base de données, il s'agit d'un produit logiciel dont la fonction principale consiste à stocker et à récupérer des données, comme le demandent d'autres applications logicielles, qui peuvent être exécutées sur le même ordinateur ou sur un autre ordinateur via un réseau (y compris Internet).

Microsoft commercialise au moins une douzaine d'éditions différentes de Microsoft SQL Server, destinées à différents publics et à des charges de travail allant de petites applications pour un seul ordinateur à de grandes applications faisant face à Internet avec de nombreux utilisateurs simultanés [20].

1.2.9. Installation du serveur Symantec endpoint protection

Symantec Endpoint Protection, développé par Symantec, est une suite logicielle de sécurité qui comprend des fonctionnalités de protection contre les logiciels malveillants, de prévention des intrusions et de pare - feu pour les ordinateurs de serveur et de bureau. Il possède la plus grande part de marché de tous les produits pour la sécurité des terminaux.

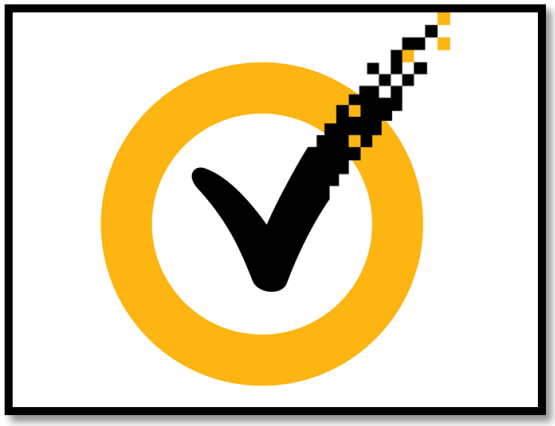


Figure 3- 5: Logo Symantec

1.2.10. Configuration Office 365:

Office 365 est la marque désignant les formules permettant de louer la dernière version de Microsoft Office (installation pour PC ou Mac, ainsi que des appareils mobiles), un ensemble de services Cloud (tels que OneDrive, Exchange Online, Skype Entreprise, SharePoint Online, Yammer...) en abonnement mensuel ou annuel, par opposition aux licences Office 2016 dites perpétuelles, qui s'installent pour une durée indéterminée sur un seul ordinateur à la fois. Office 365 est une marque fille d'Office et rassemble différentes offres pour les particuliers, les petites et les grandes entreprises. Chaque licence Office 365 est rattachée à un utilisateur (identifié par son identifiant et son mot de passe Office 365) et non plus à une machine.

Office 365 réunit un ensemble de services en ligne qui requièrent une connexion internet. Néanmoins, la suite Office comprise dans certaines offres en abonnement peut être installée sur plusieurs appareils (PC/Mac, Smartphones, Tablettes...) et permet le travail en mode déconnecté comme toute suite perpétuelle habituelle. Le mode connecté permet la synchronisation des documents avec son compte Office 365 dans le Cloud. L'abonnement Office 365 ne doit donc pas être confondu avec Office Online (qui est la suite bureautique allégée Office 100 % en ligne et qui s'utilise depuis un navigateur web). Office 365 inclut désormais les nouveaux logiciels Office 2016 [21].

Figure 3- 6: Architecture Office 365

2. Architecture Réseaux :

Notre architecture réseaux est réalisée en collaboration avec notre partenaire NextStep spécialisé dans l'implémentation des solutions réseaux informatique pour les entreprises.

- **Présentation générale de la solution**

Cette section décrit les principes généraux utilisés dans la définition de l'architecture LAN/WLAN et propose une vue d'ensemble de la solution.

Le réseau LAN/WLAN de la société est conçu avec une topologie hiérarchique avec trois couches à savoir : coeur, couche distribution et accès. Chaque couche est associée à un ou plusieurs switches. La couche core est située au niveau du firewall CR25. La couche de distribution est située au niveau des switch et Serveur (Cisco Catalyst 2960X-. Le switches (Cisco Catalyst 2960-Plus 24PST-S) sera utilisés pour connecter les utilisateurs finaux.

Ce switch sera utilisé comme switche d'accès uniquement. Il offre la fonctionnalité PoE aux terminaux adéquats comme les points d'accès, les caméras selon le standard 802.3af.

L'accès au réseau WAN sera possible à partir de Switch serveurs qui sera connecté à un firewall Cyberoam (Cyberoam CR25iNG).

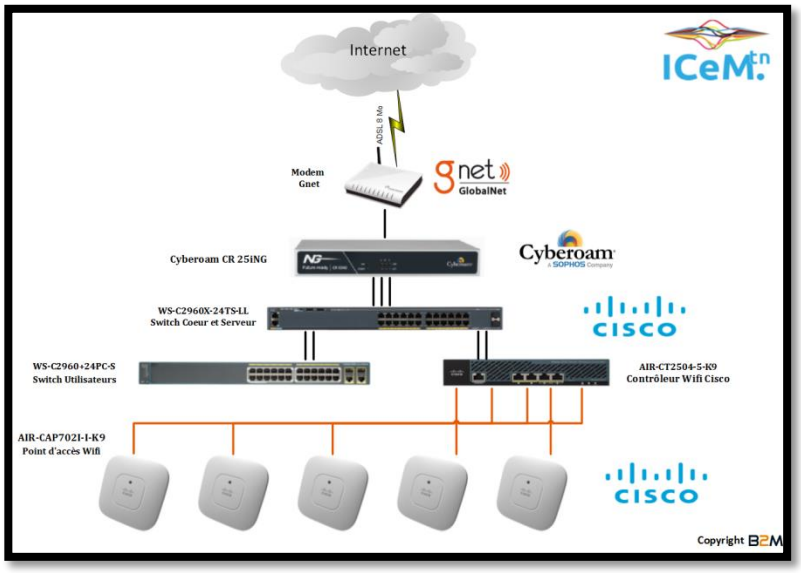


Figure 3- 7: Architecture globale de la solution LAN/WLAN

2.1. Equipements Réseaux

2.1.1. Configuration Firewall Cyberoam CR25

Intégrer une solution de sécurité UTM – La solution sécurité unifiée de Cyberoam intègre les éléments suivants :

- Pare-feu dynamique
- VPN (IPSec et SSL)
- Système de prévention des intrusions
- Antivirus et Antispyware, Antispam
- Filtrage Web
- Gestion de la bande passante
- Gestion des liens multiples

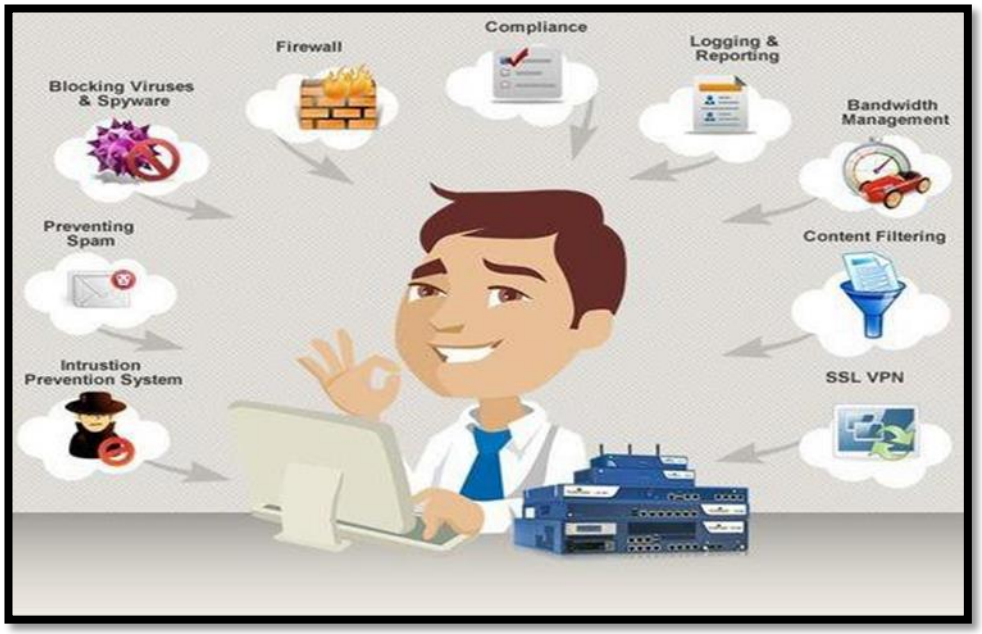


Figure 3- 8: Points forts de l'UTM Cyberoam

Pare-feu tous niveaux (couche 1 à 8) : Le pare-feu dynamique de l'UTM de Cyberoam met en place des politiques basées sur les couches 1 (physique) à 7 (application) et 8 (utilisateur) en plus des politiques classiques basées sur la source, la destination, l'adresse IP et l'application.

Ainsi, les entreprises peuvent contrôler l'accès aux ressources réseau en se basant sur l'identité de l'utilisateur, le profil professionnel et les besoins d'accès aux applications des utilisateurs externes (clients ou partenaires), des utilisateurs internes et de tous les employés se trouvant en dehors du réseau (utilisateurs mobiles et télétravailleurs). La sécurité des réseaux dynamiques

Wi-Fi, DHCP et partagés est donc assurée [22].

VPN : L'UTM de Cyberoam intègre un VPN IPSec et un VPN SSL certifié par le VPNC qui garantissent un accès à distance sécurisé, souple et facile à gérer tout en réduisant les coûts d'investissement et de fonctionnement qu'implique le déploiement de VPN dédiés. [Net3.4]

IPS : Cyberoam comprend un système de prévention des intrusions (IPS) s'appuyant sur des milliers de signatures applicables aux couches utilisateur et application pour détecter et bloquer automatiquement les intrusions par MI et P2P, par porte dérobée et autres logiciels malveillants. L'IPS de Cyberoam s'appuie sur des signatures de proxy HTTP et des signatures

personnalisées afin d'offrir une protection permettant de répondre aux exigences uniques de chaque entreprise en matière de sécurité. [22]

Une sécurité réseau avancée : Dans le but d'assurer la continuité des activités de l'entreprise, de réduire les temps d'indisponibilité, d'offrir un débit réseau accru, de prendre en charge un développement rapide du réseau tout en répondant aux normes de sécurité, Cyberoam propose des fonctionnalités de sécurité réseau avancées :

- Haute disponibilité avec basculement en cas de panne.
- Routage dynamique.
- Zones VLAN multiples pour créer des groupes basés sur le profil professionnel sur l'ensemble des sites distants.
- Hôte virtuel permettant de sécuriser l'hébergement de services au sein des réseaux LAN et DMZ.
- Gestion, journalisation et *reporting* centralisés [22].

2.1.2. Configuration Switch Cisco Catalyst C2960X:

Le switch Cisco Catalyst C2960X-24TS est un commutateur Gigabit Ethernet non-modulaire, empilable, offrant une solution d'accès pour les réseaux de campus et les sites distants.

Les commutateurs de la série Cisco Catalyst 2960-X offrent une gestion de trafic intelligente qui permettent aux flux de s'écouler conformément aux requis techniques imposés par les applications. Des mécanismes flexibles de marquage, classification, gestion de queue offrent une performance supérieure aux flux de voix, vidéo et données, tout cela au débit des interfaces.

Les switches Cisco Catalyst 2960-X offrent un ensemble de fonctionnalités de sécurité pour contrôler et limiter les accès au réseau et prévenir les menaces [23].

Caractéristiques principales

- 24 ports Gigabit Ethernet avec une performance "line-rate"
- 2 ports SFP (interconnexion "uplink" Gigabit Small Form-Factor Pluggable)
- FlexStack-Plus pour empiler jusqu'à 8 commutateurs et une bande-passante sur la pile de 80 Gb/s (optionnel)
- Consommation électrique réduite avec des fonctions avancées de gestion de l'énergie
- Ports de management USB et Ethernet pour la simplification des opérations

Pour plus d'informations et spécification technique voir tableau 3.2 et tableau 3.3

Figure 3- 9: Switch Coeur Cisco Catalyst C2960X - 24 ports

INFORMATIONS GÉNÉRALES	
Designation	Cisco Catalyst C2960X-24TS-L
Marque	Cisco Systems
Modèle	WS-C2960X-24TS-L

Tableau 3- 1:Informations Générales Cisco Catalyst C2960X [23]

SPÉCIFICATIONS TECHNIQUES	
Nombre de Ports	24
Norme(s) réseau	10/100/1000Mbps
Nombre de Ports 10/100/1000 Mbps	24
Nombre de Ports combo SFP (RJ45/Fibre)	2
Rackable	Oui
Manageable	Oui
Niveau d'administration	Niveau 3
SNMP	Oui
PoE (Power over Ethernet)	Oui
Compatible IPv6	Oui
Largeur	445 mm
Profondeur	279 mm
Hauteur	45 mm
Poids	4 kg

Tableau 3- 2: Spécification technique Cisco Catalyst C2960X [23]

2.1.3. Configuration Switch Cisco Catalyst 2960 Plus 24 :

Les commutateurs intelligents Cisco Catalyst 2960 Plus, nouvelle famille de périphériques autonomes à configuration fixe, apportent aux postes de travail une connectivité

Fast Ethernet et Gigabit Ethernet optimisant les services de LAN.

La gamme Catalyst 2960 Plus offre une sécurité intégrée avec contrôle de l'admission sur le réseau (NAC), qualité de service (QoS) évoluée et résilience, pour distribuer des services intelligents à la périphérie du réseau [23].

Caractéristiques principales

- Fonctionnalités intelligentes à la périphérie du réseau, par exemple des listes de contrôle d'accès (ACL) élaborées et une sécurité optimisée
- Liaisons ascendantes à deux fonctions favorisant la flexibilité de la liaison montante Gigabit Ethernet et permettant d'utiliser du cuivre ou de la fibre optique.
- Chaque port de liaison ascendante à deux fonctions offre un port 10/100/1000 Ethernet et un port Gigabit Ethernet SFP (Small Form-FactorPluggable).
- Sécurité du réseau assurée par une série de méthodes d'authentification, des technologies de cryptage des données et le contrôle des admissions sur le réseau basé sur les utilisateurs, les ports et les adresses MAC.

Pour plus d’informations et spécification technique voir tableau 3.4 et tableau 3.5

Figure 3- 10:Switch User Cisco Catalyst 2960 Plus - 24 Ports

INFORMATIONS GÉNÉRALES	
Designation	Cisco Catalyst 2960-24TC-S
Marque	Cisco Systems
Modèle	WS-C2960-24TC-S

Tableau 3- 3: Information générale Cisco Catalyst 2960 Plus [23]

SPÉCIFICATIONS TECHNIQUES	
Nombre de Ports	24
Norme(s) réseau	10/100 Mbps
Nombre de Ports combo SFP (RJ45/Fibre)	Oui
Rackable	Oui
PoE (Power over Ethernet)	Oui
Norme PoE	Non

Tableau 3- 4:Spécifications techniques Cisco Catalyst 2960 Plus [23]

2.1.4. Contrôleur sans fil Cisco 2500 Model 2504

Le contrôleur d'accès au réseau local sans fil Cisco AIR- CT2504-5-K9 Wireless LAN Controller fonctionne en réseau avec le contrôleur d'accès léger Cisco et le système de contrôle sans fil Cisco (Cisco Wireless Control System _WCS). Il s'agit d'un contrôleur d'accès à l'entrée du réseau, conçu pour distribuer des fonctionnalités de réseau LAN sans fil sur l'ensemble du système dans les bureaux des petites et moyennes entreprises.

Ces contrôleurs peuvent simplifier la gestion des points d'accès pour les organisations disposant de réseau de petite taille ou déployé sur un seul site au bénéfice d'environ 500 utilisateurs ou moins.

Caractéristiques principales

- Contrôle centralisé : En tant que composant du système UWN, le contrôleur d'accès au réseau LAN sans fil de la gamme Cisco 2500 permet aux administrateurs du réseau de gérer, sur l'ensemble du système, les politiques de sécurité, ainsi que les services de mobilité tels que la voix et les accès invités, ou encore les services de localisation.
- Capacité à monter en charge : le contrôleur peut supporter jusqu'à 500 clients et un maximum de 50 points d'accès grâce aux extensions des licences Adder [23].

Figure 3- 11: Contrôleur sans fil Cisco 2500 Model 2504

2.1.5. Point d'accès Cisco Aironet 702i

Le point d'accès autonome sans fil Cisco Aironet 702i offre une connexion sans fil fiable et sécurisée, adaptée aux besoins des entreprises. Ce modèle bénéficie d'une technologie Wi-Fi 802.11 a/g/n et peut atteindre un débit maximum de 300 Mbps à l'aide du WiFi MIMO à 2 flux.

Grâce à son design compact et ses excellentes performances, le point d'accès sans fil Cisco Aironet 702i sera idéal pour apporter un signal sans fil de haute qualité au sein d'une entreprise, dans des zones de travail ordinaires (bureaux, etc.).

Caractéristiques principales :

- Point d'accès sans fil autonome
- Design fin et compact avec antennes internes, pour un faible encombrement
- Technologie Wi-FI ac MIMO (2x2) avec vitesse maximale de 300 Mbps
- Température de fonctionnement de 0°C à 40°C [23]
- Dual Band / Antennes internes : 2,4GHz - 5 GHz
- Connexion sécurisée avec cryptage WPA / WPA2
- Alimentation par injecteur PoE (en option) ou alimentation local (en option) [23].

Figure 3- 12: Point d'accès Cisco Aironet 702i

2.2. Wireless LAN

Un réseau WLAN a été déployé au niveau ICEM en utilisant l'architecture centralisé conseillé par Cisco. Ce réseau se compose de 5 point d'accès Lighweight 702i qui seront contrôlé d'une façon centralisée par un contrôleur WLC 2504.

3. Vlan et Plan d'adressage

La liste des Vlans et le plan d'adressage sont considérés des points clés pour la réussite de la mise en place de réseau LAN. Les vlans sont répartis suivant la nature du trafic ou administration.

La liste illustrée dans le tableau ci-dessous des vlans proposés ainsi que les réseaux correspondants dans le siège n'est pas la liste finale, elle sera modifiée suivant les besoins du client tout au long de ce projet :

Nom de VLAN	VLAN ID	Description
VL-User	10	VLAN des Utilisateurs
VL-serveurs	20	VLAN Infra Système et serveurs
VL-Wifi-VIP	30	VLAN Wifi VIP
VL-Wifi-DATA	40	VLAN Wifi User Data
VL-Wifi-Guest	50	Vlan Wifi Guest
VL-T-MOBILE	60	VL-T-MOBILE
VL- Mgmt_Reseau	99	VLAN Equipements réseau
VL-Native	999	VLAN native pour les trunk inter-switches

Tableau 3- 5: liste des Vlans

3.1. Le protocole VTP

VTP est un protocole propriétaire Cisco qui permet de circuler les informations des VLANs sur des différentes switches sans avoir besoins de configurer les VLANs sur chaque switch. Durant la phase de déploiement, nous allons configurer un des deux switch coeur en tant que VTP Server alors que les autres switches seront des VTP Client. Après avoir effectué la synchronisation entre le VTP Server et les VTP Client, tous les switches seront mis en mode « Transparent » et cela pour les raisons suivantes :

- Le VTP n'est pas sécurisé. Beaucoup d'attaques peuvent avoir lieu en profitant de cette faille de sécurité et peuvent avoir des mauvais impacts sur le réseau.
- Il y a un risque de détruire la base de données des VLANs à chaque fois qu'un nouveau switch sera inséré avec un nombre de révision élevé.

La configuration VTP est comme suit :

- VTP domain-name ICEM
- VTP mode transparent
- VTP password ICEM*2017

3.2. Le routage IP

Comme l'architecture du réseau ne présente pas une complexité de mise en place, nous proposons d'adopter le routage statique simple afin d'atteindre tous les segments de réseaux. Un routage inter-vlan ainsi que vers Internet sera assuré par le *firewall* Cyberoam

4. Sécurité périmétrique

La sécurité du périmètre de l'entreprise sera réalisée par le cluster des UTM Cyberoam CR25iNG.

Le tableau suivant décrit les zones qui seront mises en place ainsi que la configuration réseau associé.

ZONE	Interface	Adresse IP
LAN	Port A	192.168.99.254
	Port A.10	192.168.10.254
	Port A.30	192.168.30.254
	Port A.40	192.168.40.254
	Port A.60	192.168.60.254
Wifi-guest	Port A.50	
WAN	Port B	192.168.1.14
DMZ		192.168.0.1

Tableau 3- 6: Zones des Firewalls

Conclusion

Dans ce chapitre nous avons indiqué les objectifs de notre mission. D'abord nous avons commencé par présenter la nouvelle architecture système et réseau ainsi que ces points forts. Ensuite nous avons enchainé par une description du design physique et logique de l'infrastructure qui nous a permet de détaillé les caractéristique et les spécifications du matérielle réseau nécessaires à la réalisation du projet. En fin nous avons clôturé par la description du design de sécurité réseau afin préciser les aspects de sécurité de notre architecture. L'étape suivante consistera donc à une concrétisation de l'architecture envisagée et la mise en place de l'infrastructure.

Chapitre 4 : réalisations

Introduction

Après l'achèvement de l'étude du projet et la partie design d'architecture, on entamera dans ce chapitre la phase de réalisation. Cette partie portera sur une présentation de l'architecture du matériel utilisé lors des phases de la migration vers la nouvelle infrastructure système et réseau, sa mise en place et sa configuration.

1. Infrastructure système

Durant cette partie on va présenter les différentes phases de l'implémentation de notre environnement virtualisé, les différents outils logiciels utilisés pour la réalisation de notre solution.

On va aussi présenter les fonctionnalités des applications et quelques tests permettant de démontrer le bon déroulement de leurs fonctionnalités.

1.1. Description de l'application

1.1.1. Installation de VMware ESXi

L'installation de VMware ESXi est assez simple, un assistant d'installation avec une interface utilisateur minimale rassemble les paramètres nécessaires tels que le nom d'hôte, la configuration du réseau, le mot de passe, etc.

Une fois toutes les informations fournies, l'installation peut démarrer.

Les **Figures 4.1, 4.2, 4.3, 4.4,** montrent quelques impressions du processus d'installation :

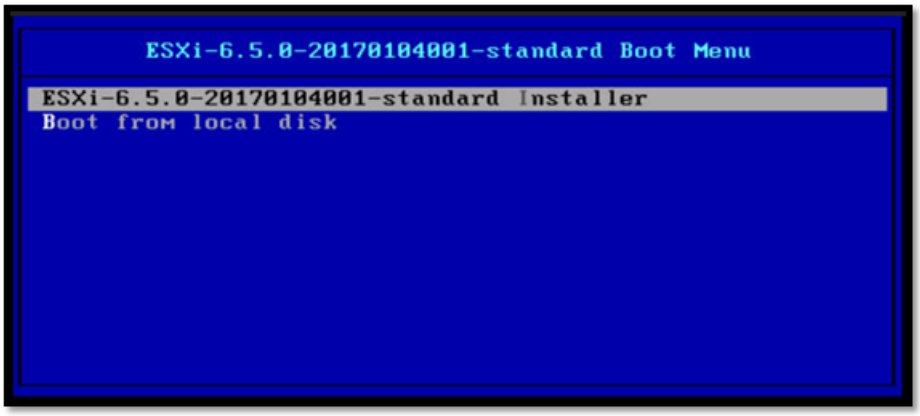


Figure 4- 1:ESXi Setup

Figure 4- 2:Chargement des fichiers d'installation

Figure 4- 3:Configuration de l'adressage

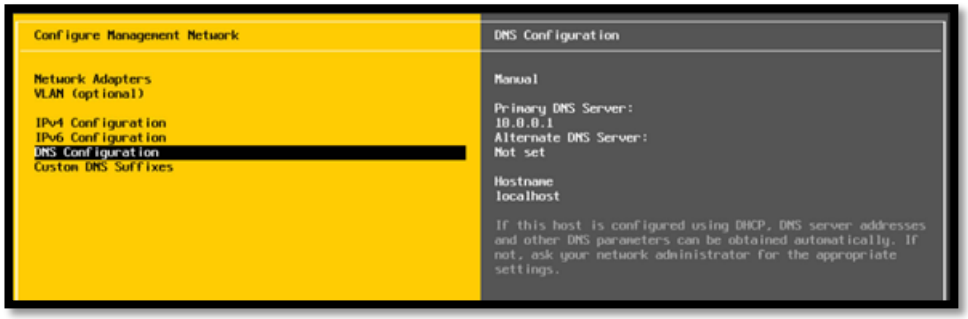


Figure 4- 4: Configuration du serveur DNS

Une fois l'installation est terminée, le système peut être géré à distance via Vmware Vcenter. Il s'agit d'un logiciel de gestion graphique basé sur Windows, en tapant simplement l'adresse IP du serveur dans un navigateur Web

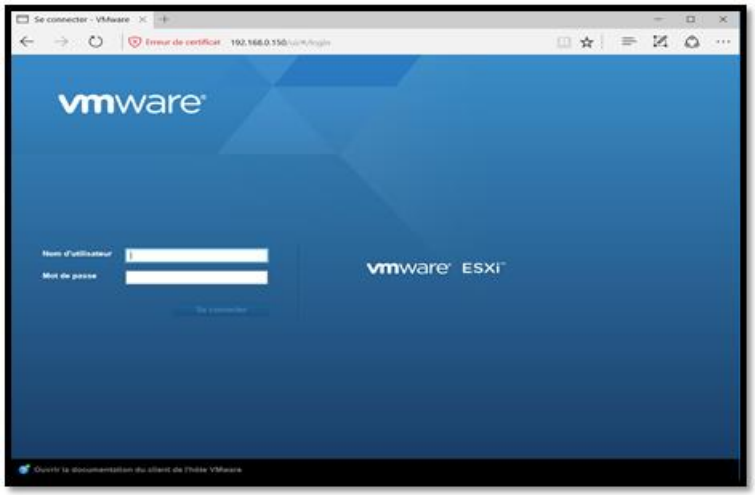


Figure 4- 5:L'interface web pour l'administration du serveur

Figure 4- 6:Version ESXi

1.1.2. Ajout d'une machine virtuelle :

Dans le cadre de notre projet, nous allons donc poursuivre en ajoutant nos serveurs « Windows SERVER » à notre Vmware Vcenter

Les **Figures 4.7, 4.8, 4.9, 4.10, 4.11** montrent les d'ajouter une nouvelle machine virtuelle :

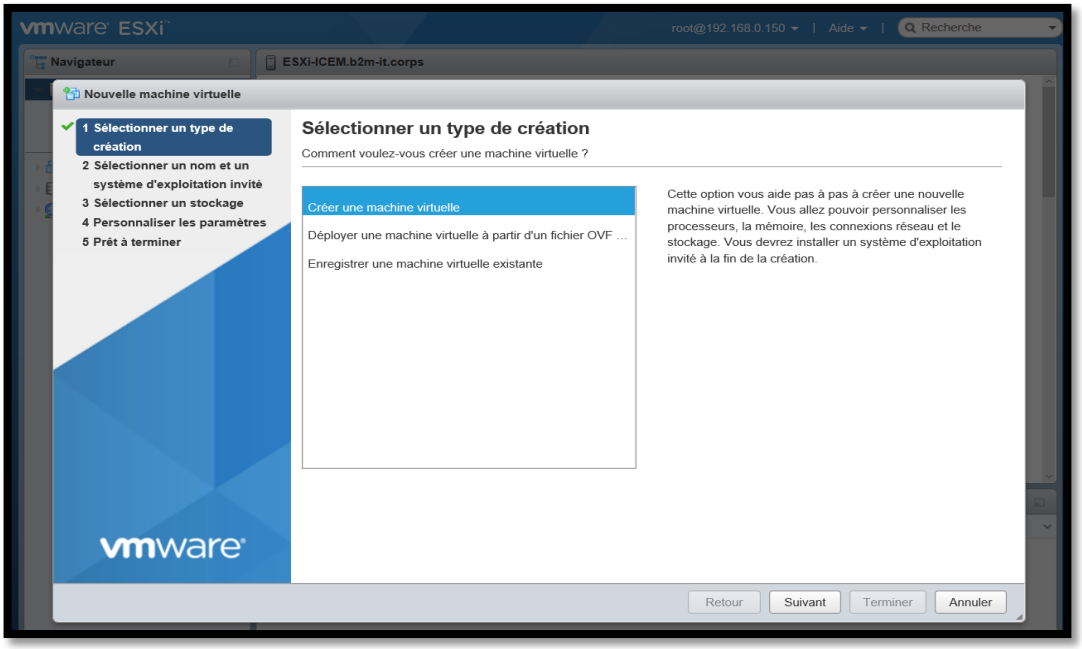


Figure 4- 7:Création d'une machine virtuelle

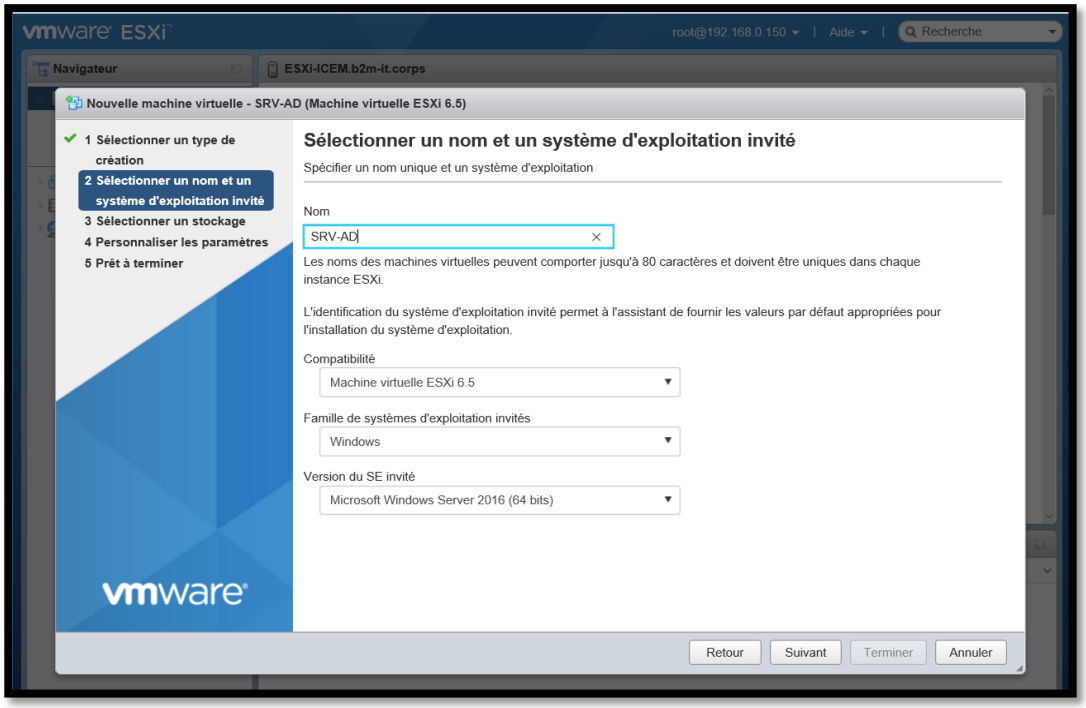


Figure 4- 8:Configuration Système d'exploitation et version

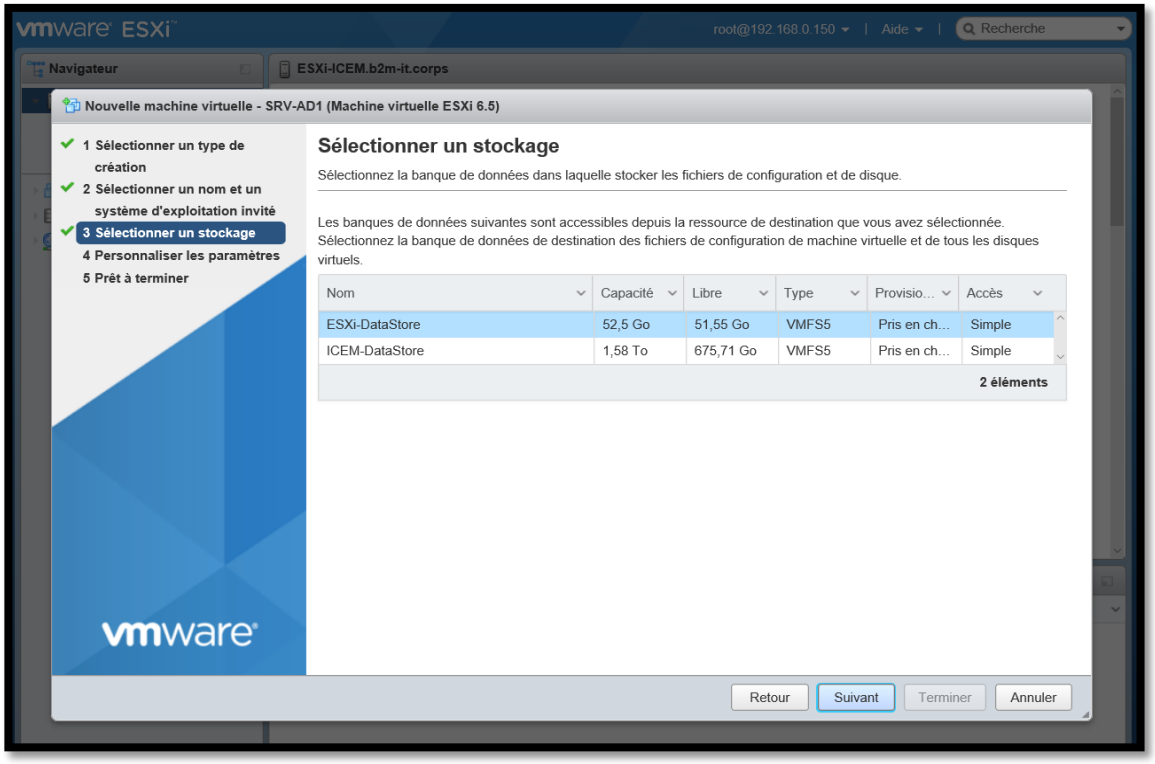


Figure 4- 9: Définir le stockage de la machine

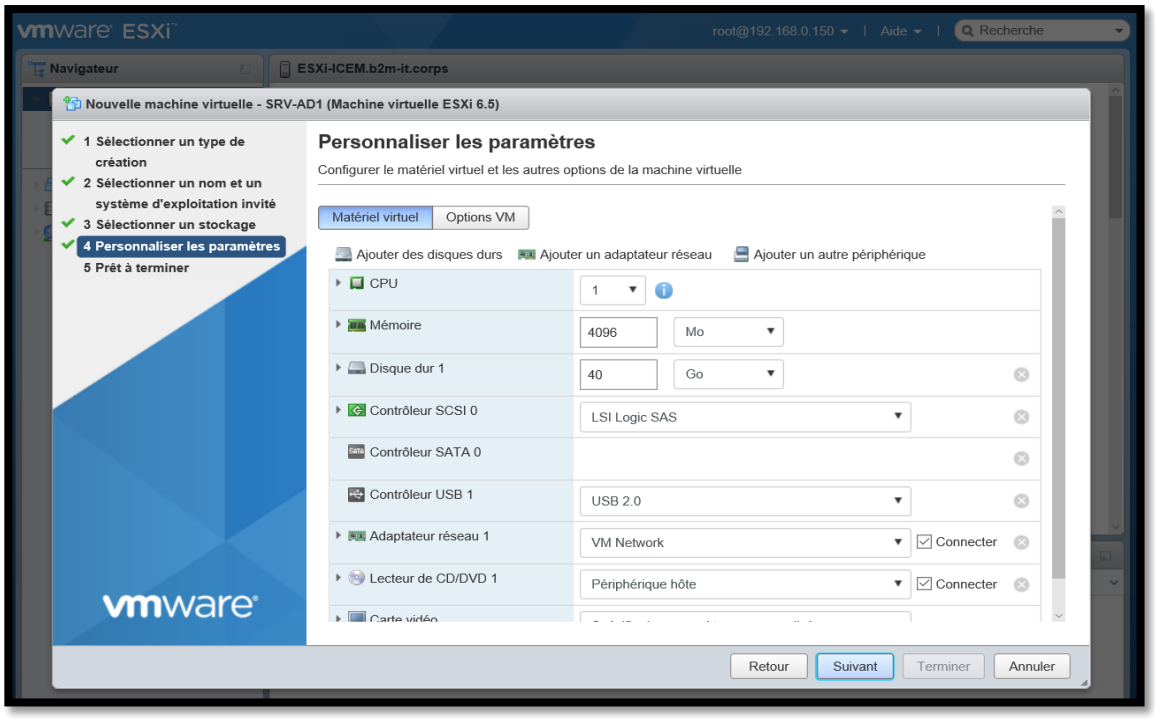


Figure 4- 10:Personnaliser les paramètres de la machine

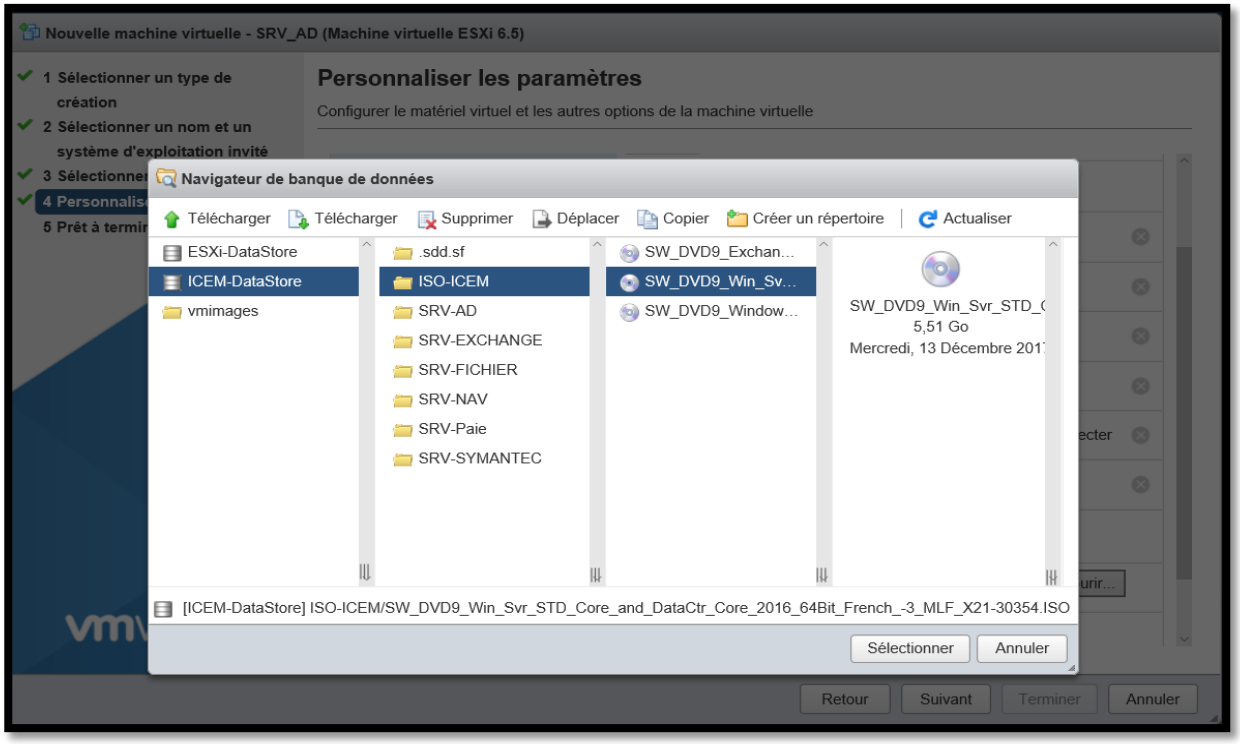


Figure 4- 11:Affecter le CD d'installe spécifier

Lorsqu'on termine toutes les informations nécessaires, notre machine virtuelle est prête pour l'utilisation et on passe à l'installation de système d'exploitation qui est dans notre cas Windows server 2016.

1.1.3. Installation de Windows server 2016

Les **Figures 4-12, 4-13, 4-14, 4.15** montrent les déroulements pour l'installation Windows server 2016 :

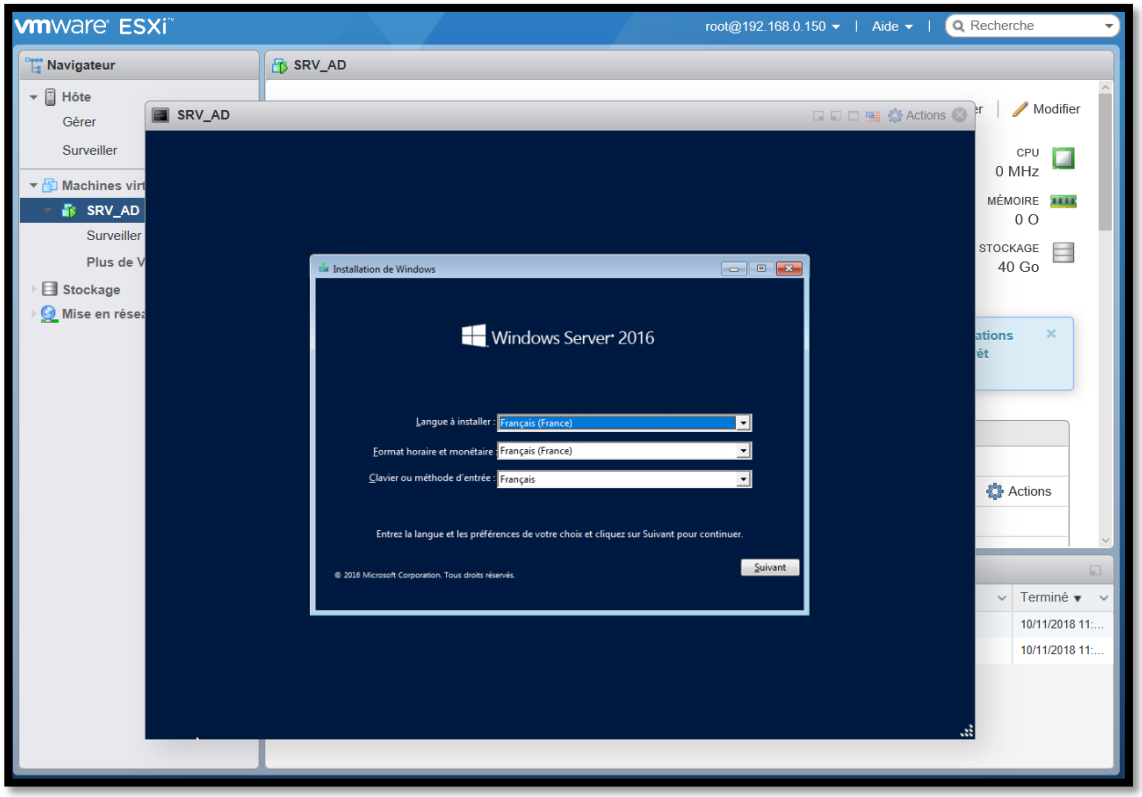


Figure 4- 12: Boot Windows server 2016

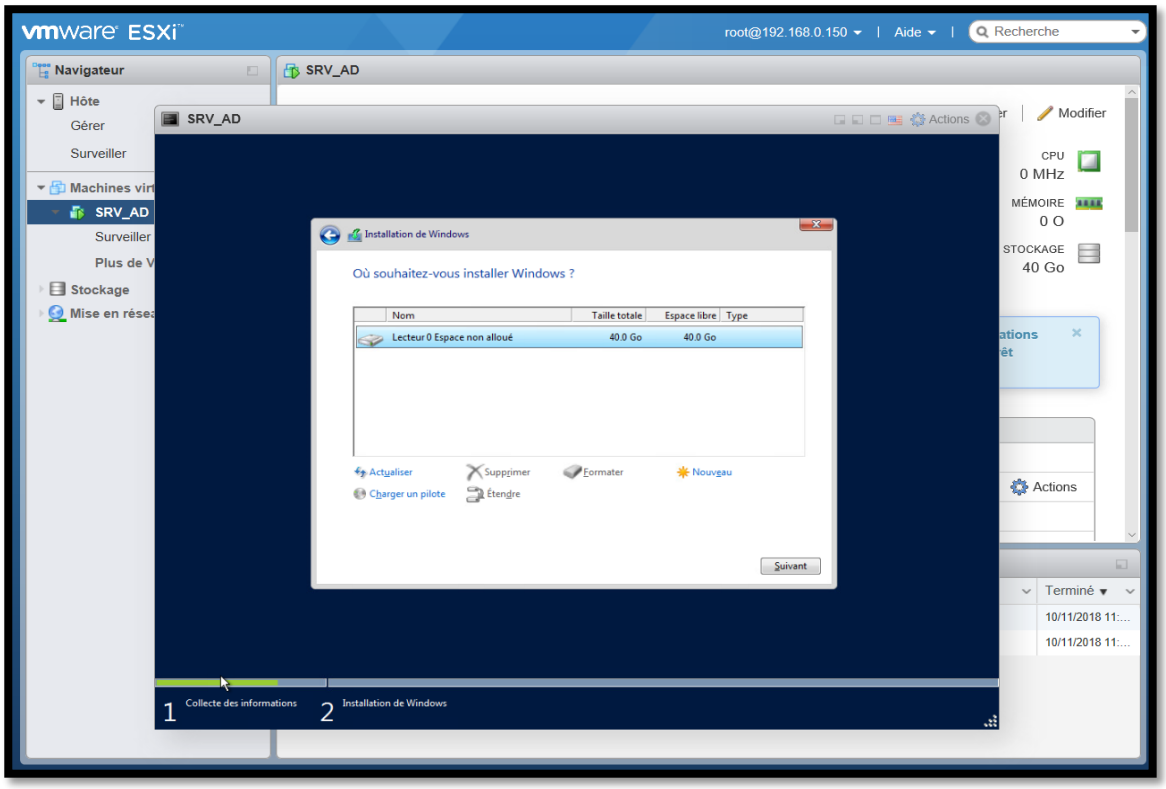


Figure 4- 13: Partition des disques durs

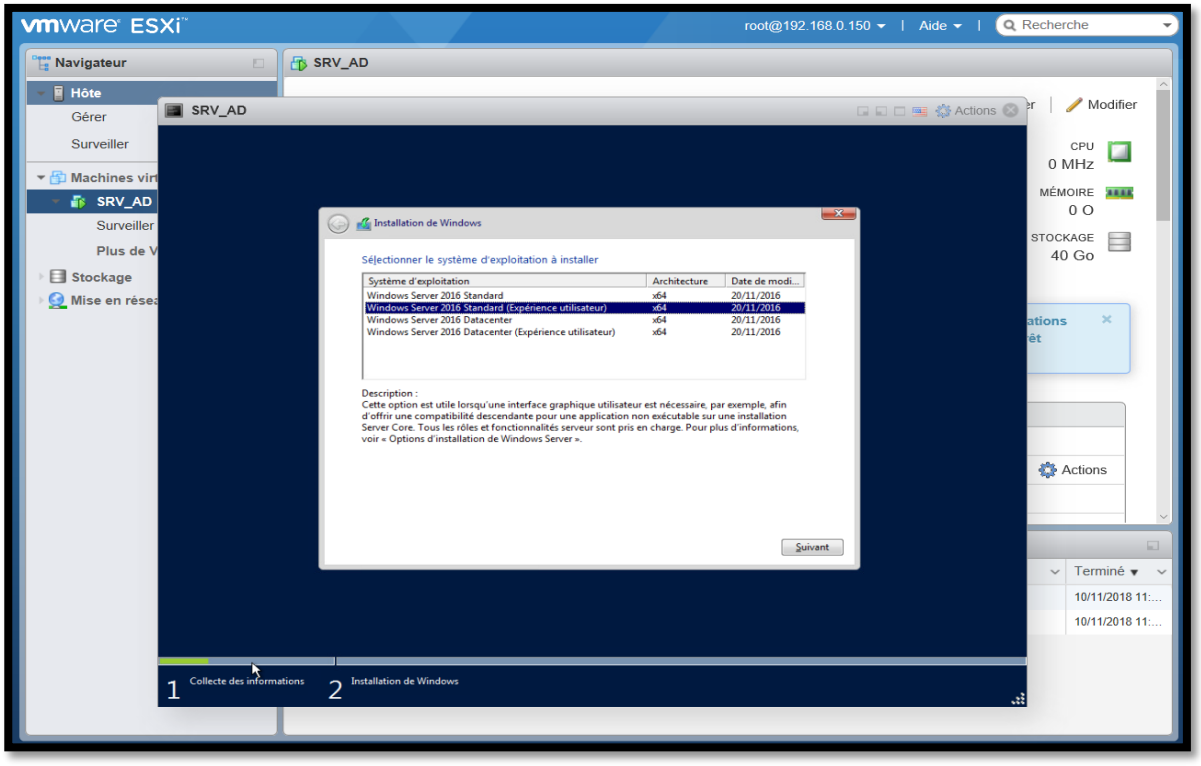


Figure 4- 14: Installation Windows server 2016 standard avec interface graphique

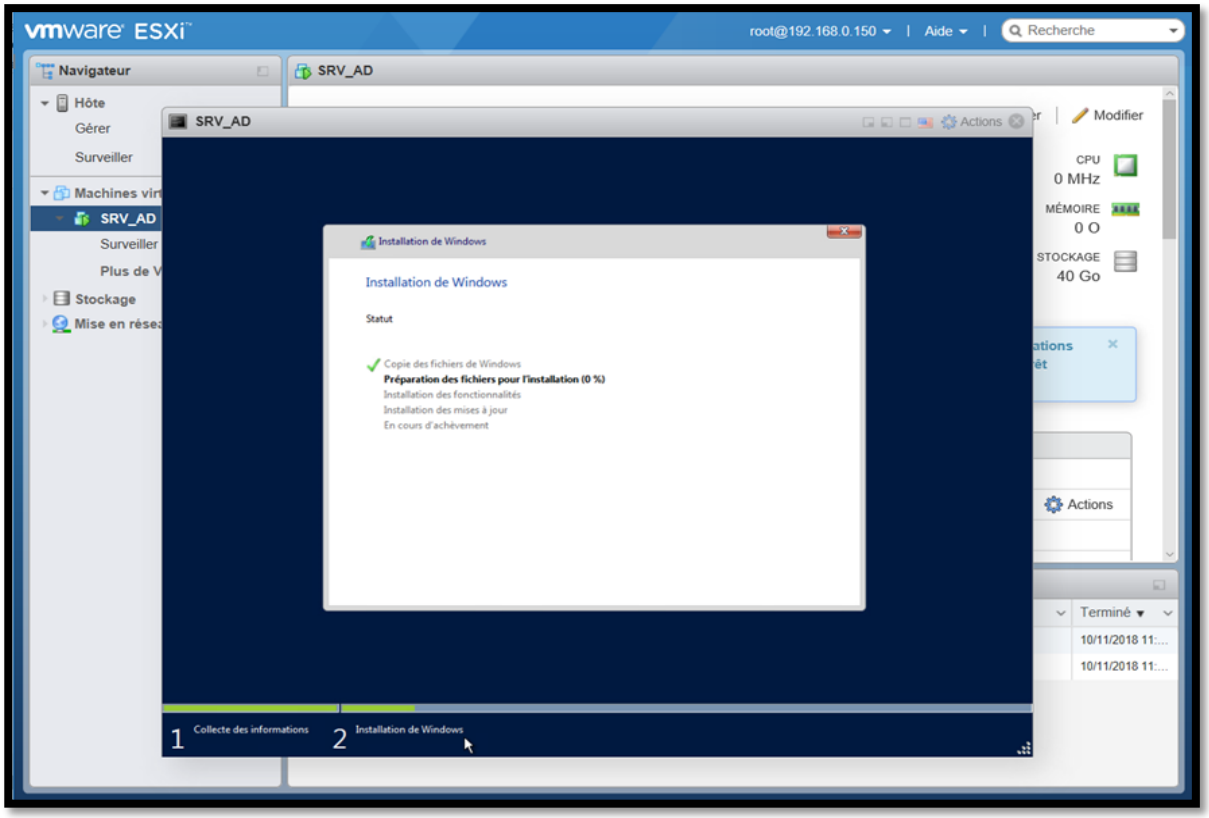


Figure 4- 15: début de l'installation

1.1.4. Installation d'Active Directory

Le premier serveur à installer est le serveur AD (active directory), vue son importance au niveau des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. On va poursuivre les étapes d'installation de la fonctionnalité AD DS selon la **(Figure 4-16)**.

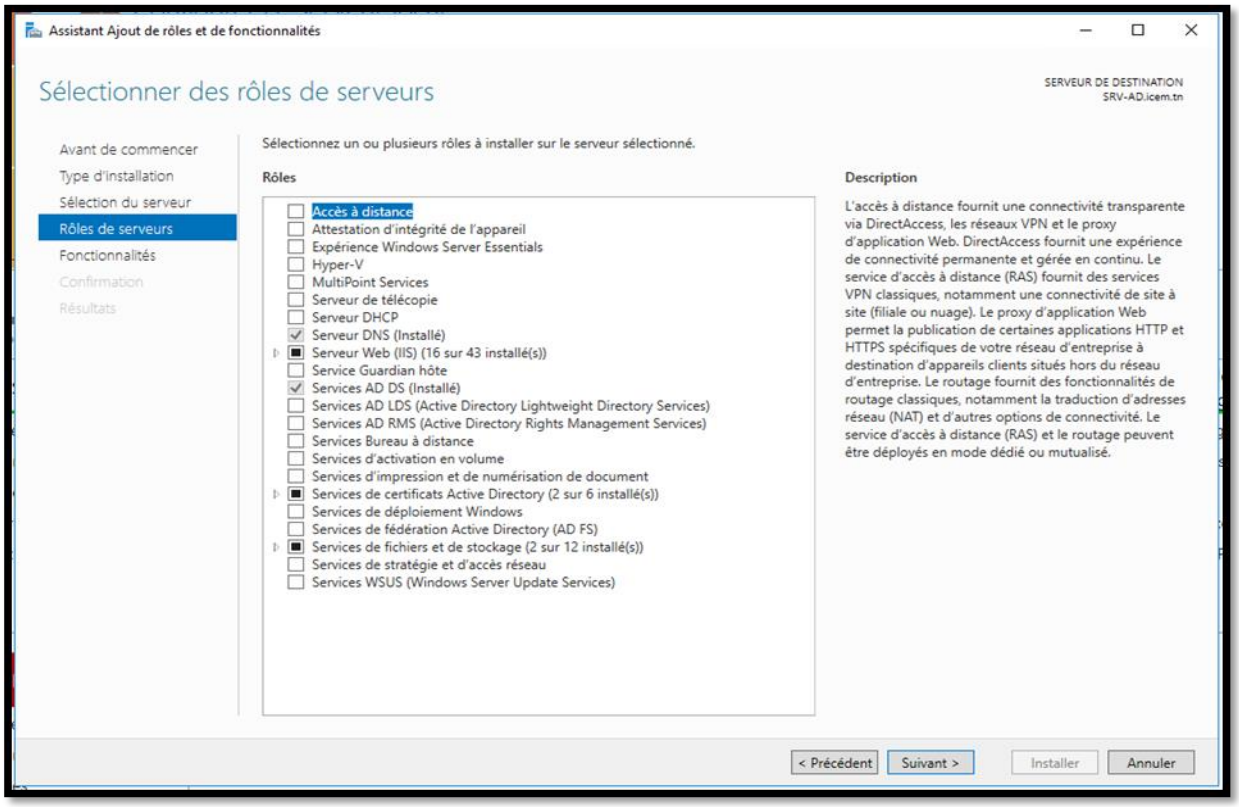


Figure 4- 16: Configuration et installation rôle serveur AD

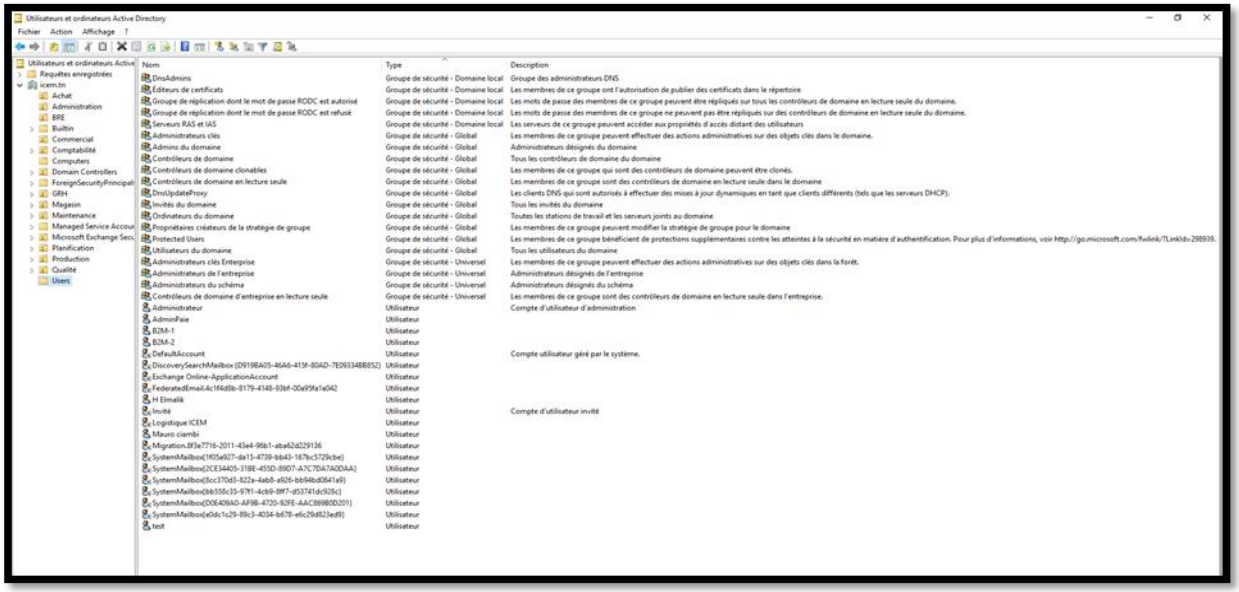


Figure 4- 17: Configuration compte utilisateurs du domaine ICEM.tn

1.2. Serveur Applicatif

1.2.1. Exchange 2016

Pour mettre en place votre serveur Exchange 2016 vous devez installer les prérequis suivants :

Votre serveur doit être ajouté au domaine de votre entreprise et le rôle Active Directory DS installé.

- Votre serveur doit être ajouté au domaine de votre entreprise et le rôle Active Directory DS installé.
- Votre système doit être à jour.
- Votre domaine et forêt doit être d'un niveau fonctionnel minimal en WINDOWS SERVER 2008R2
- Téléchargez la dernière version (rollup) d'Exchange 2016 (juillet 2018 nous sommes au ROLLUP 10).

Apres la vérification des prérequis, on va entamer l'installation du serveur de messagerie exchange.

Les **Figures 4-18, 4.19, 4.20** montrent quelques impressions du processus d'installation :

Figure 4- 18:Vérification des mises ajours

Étape importante maintenant, le rôle du serveur. Si avec les précédentes versions cela nécessitait

une réflexion particulière, Exchange 2016 a simplifié les choses puisqu'on ne se retrouve qu'avec 2 rôles : Boite aux lettres (MB pour Mailbox) et EDGE.

Ainsi, les 2 rôles primordiaux qu'étaient CAS et MB sur Exchange 2013 ont été réunis dans le MB sur Exchange 2016.

Le rôle Mailbox assure par conséquent le routage de mail, la gestion des bases de données, les accès clients, etc…

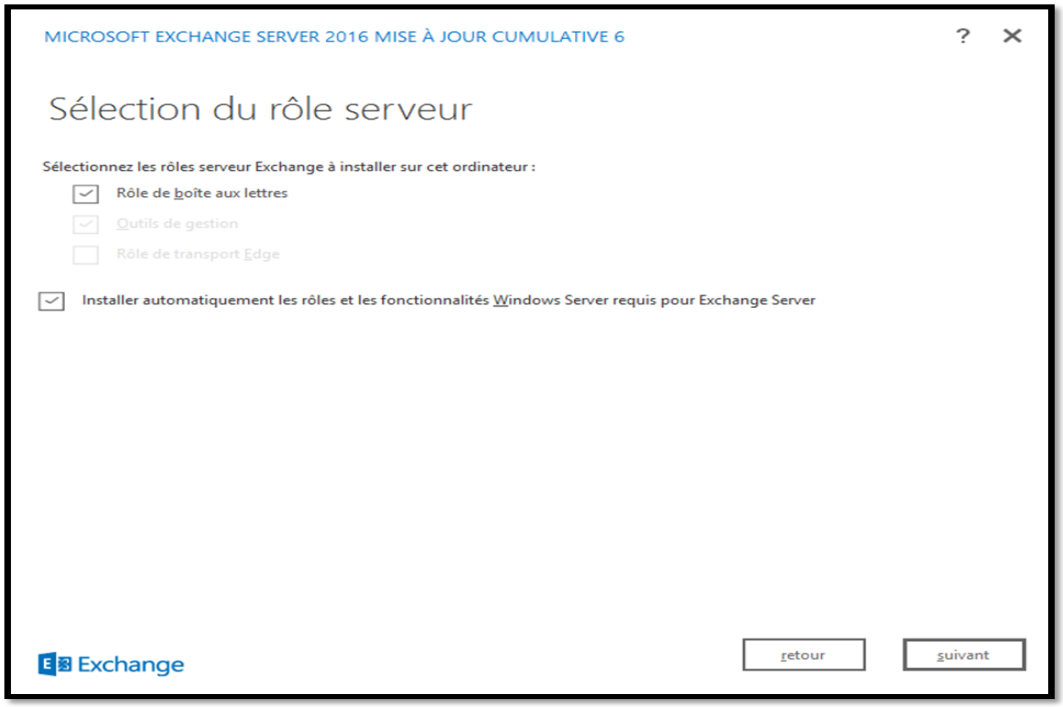


Figure 4- 19:Sélection du rôle de serveur

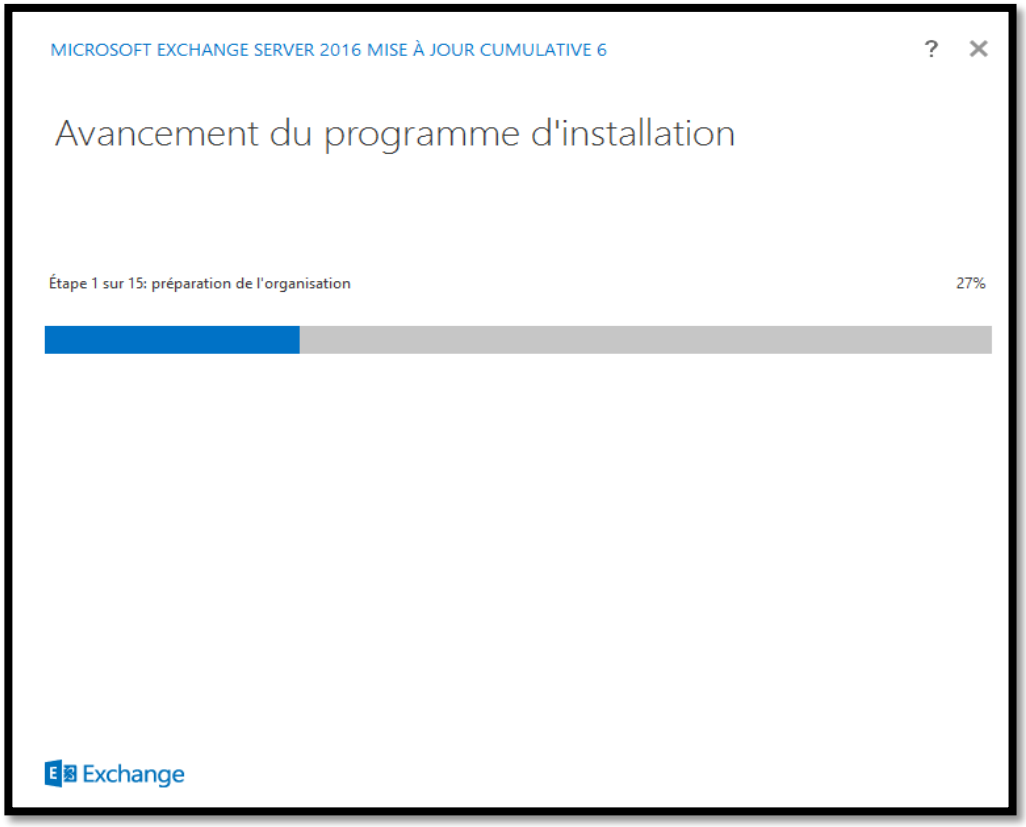


Figure 4- 20: Avancement de l'installation

Le navigateur se lance alors et vous amène sur l'ECP (l'interface web qui vous permet de gérer votre Organisation Exchange)

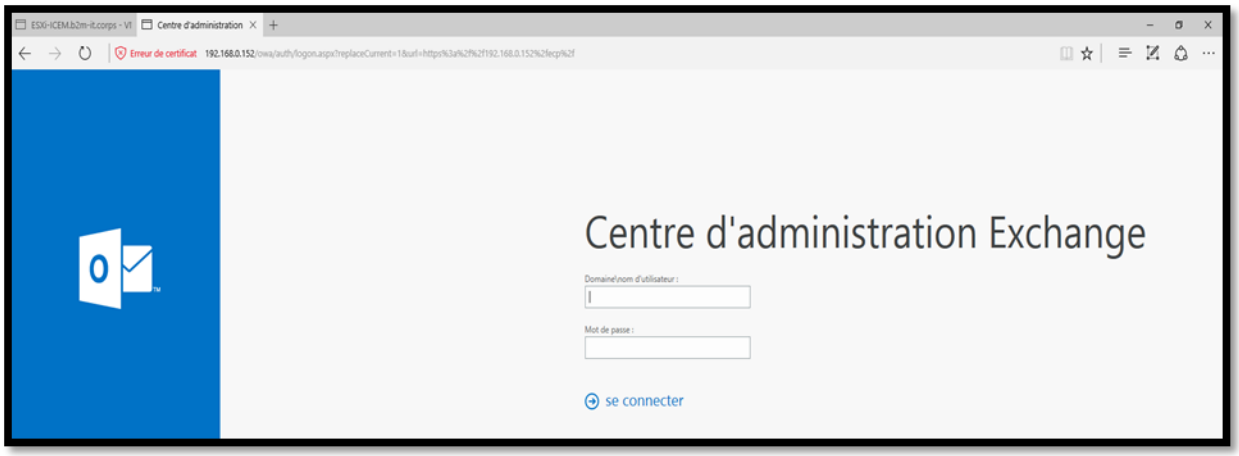


Figure 4- 21:Interface d'administration exchange

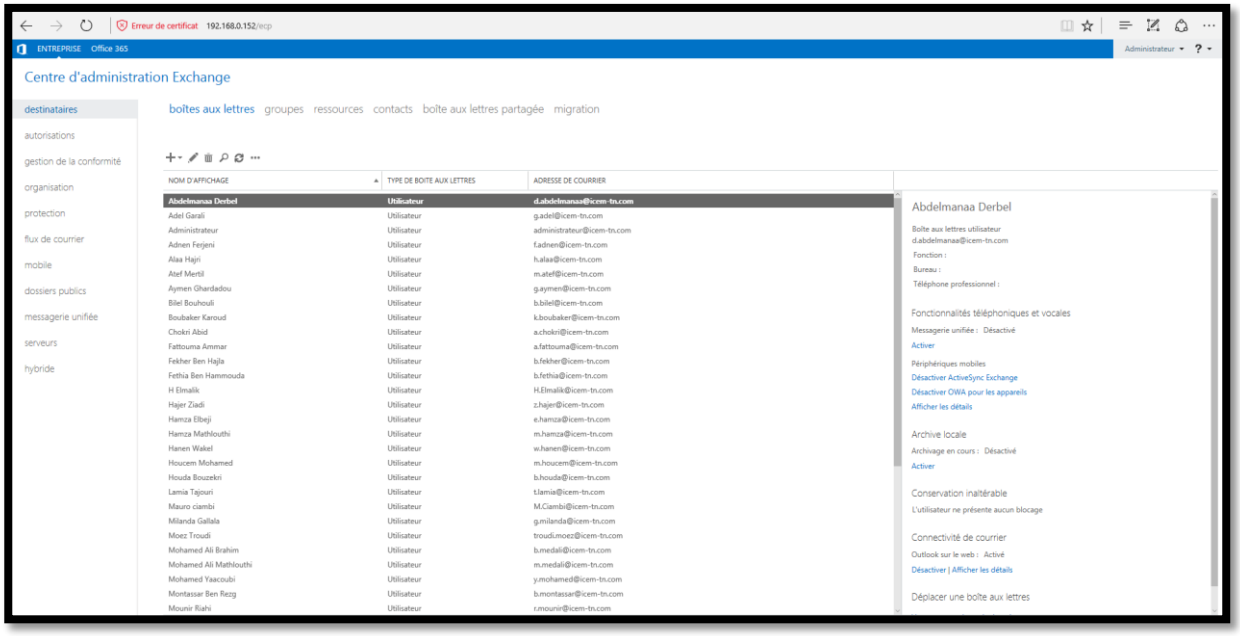


Figure 4- 22: Configuration des boites a lettre Exchange

1.2.2. SQL Server 2014 et Dynamics Navision 2016

Pour installer le serveur Dynamics Navision 2016, il faut tout d'abord préparer l'environnement base de données SQL 2014 et restaurer la base Prod Navision. Puis l'installation et configuration du serveur Navision.

- **Installation SQL Server 2014**

Les **Figures 4.23, 4.24, 4.25, 4.26, 4.27** montrent quelques impressions du processus d'installation :

Figure 4- 23:Installation SQL server 2014

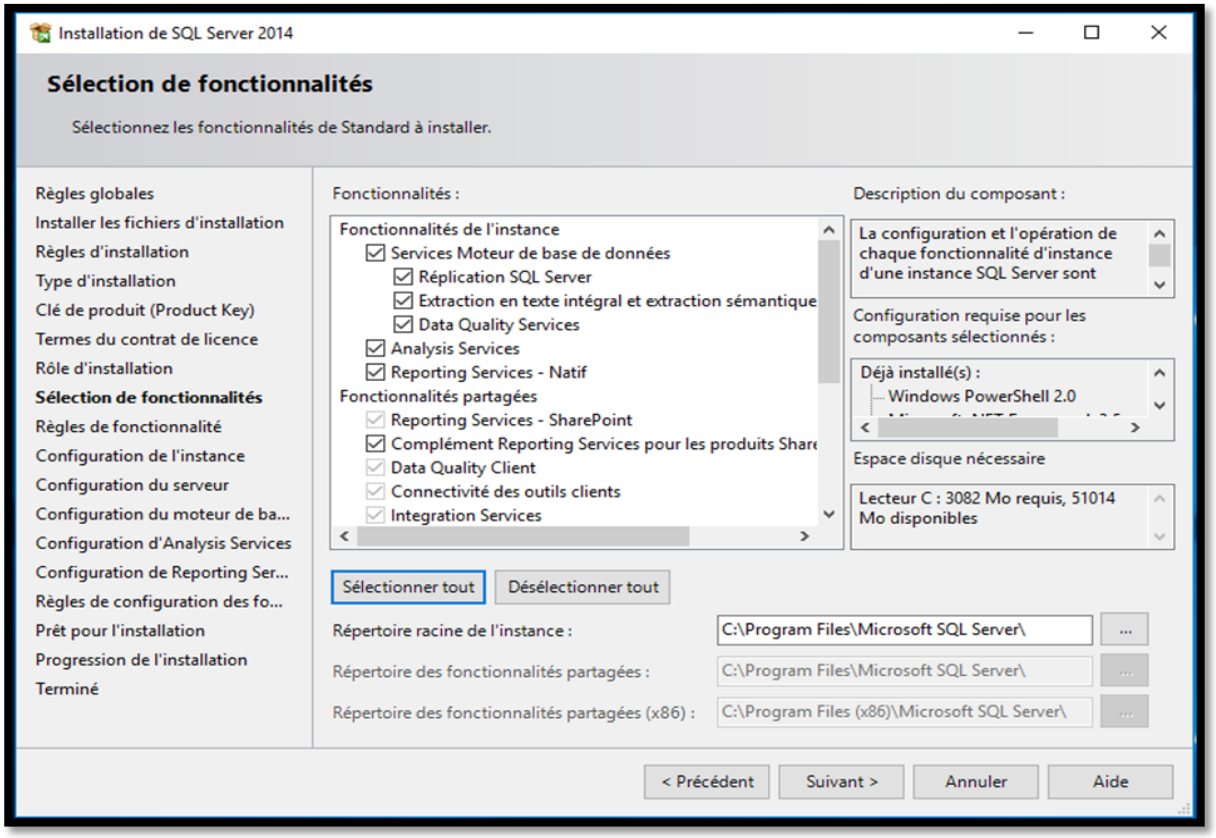


Figure 4- 24:Sélection des fonctionnalités

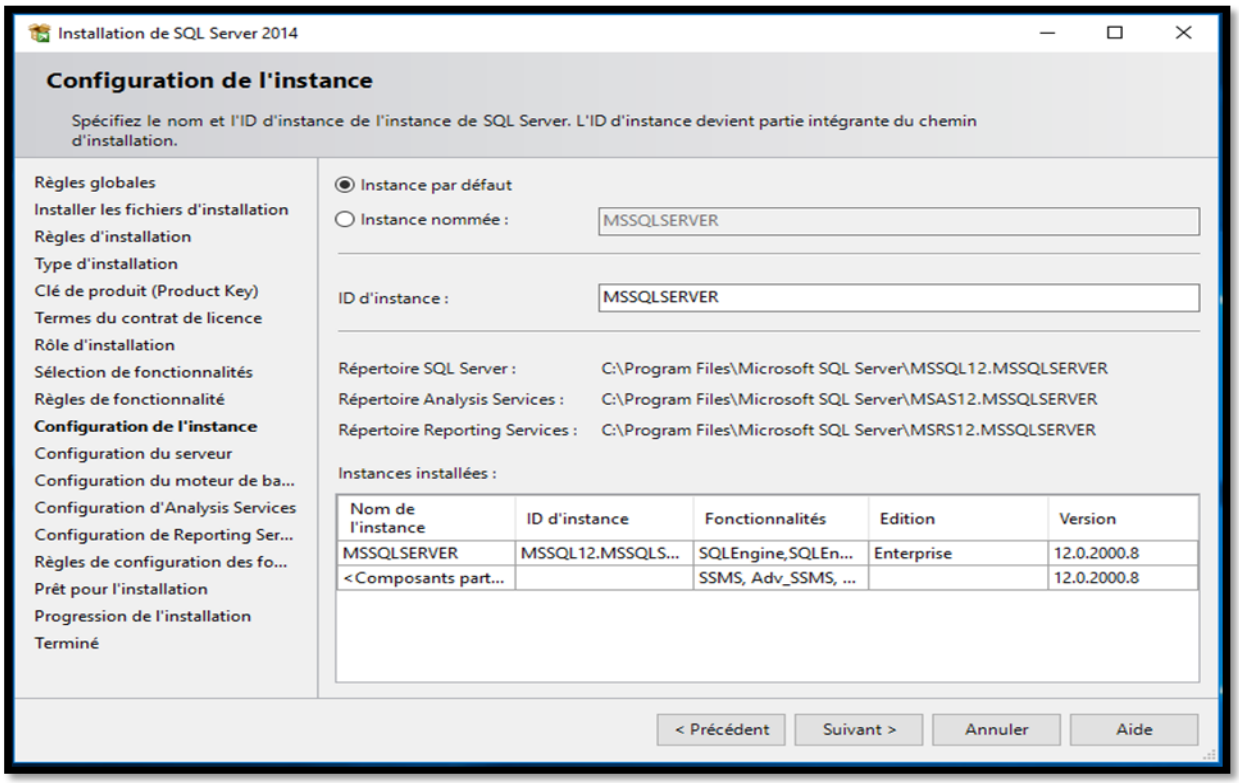


Figure 4- 25:Configuration de l'instance

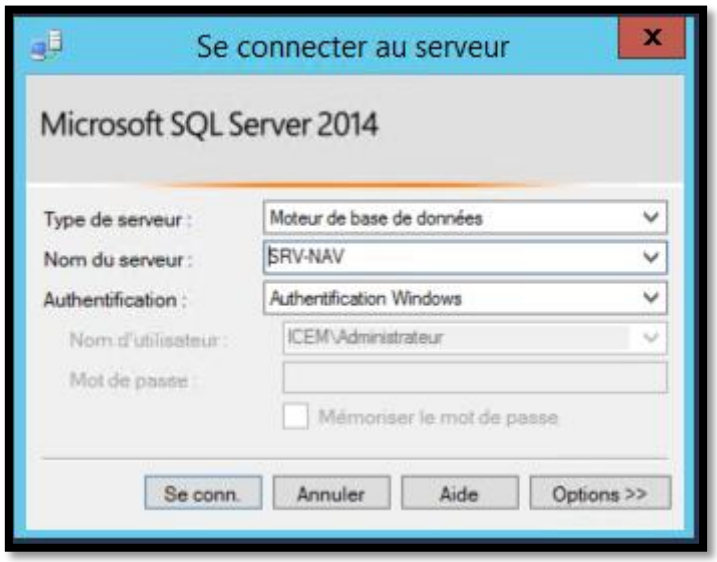


Figure 4- 26:Authentification SQL Server

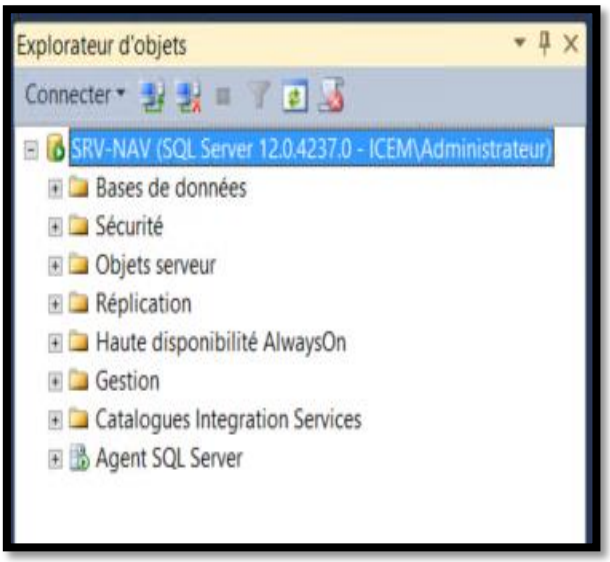


Figure 4- 27: Structure des objets SQL Serveur

- L'étape suivante c'est de restaurer la base Prod ICEM :

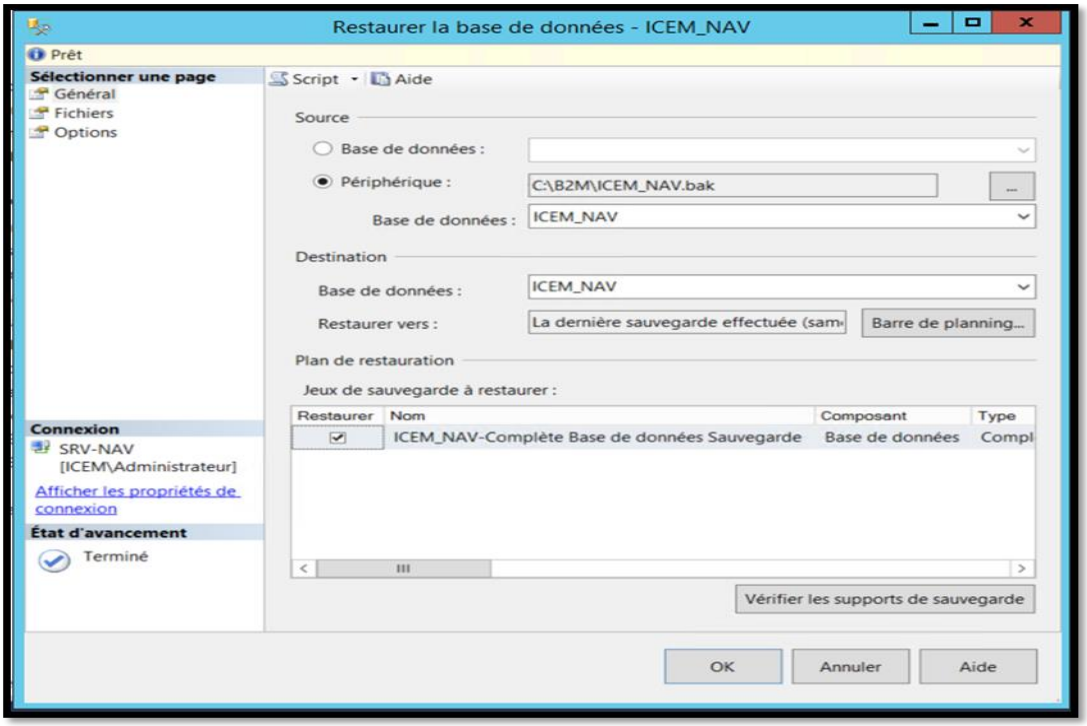


Figure 4- 28:Phase de de restauration SQL

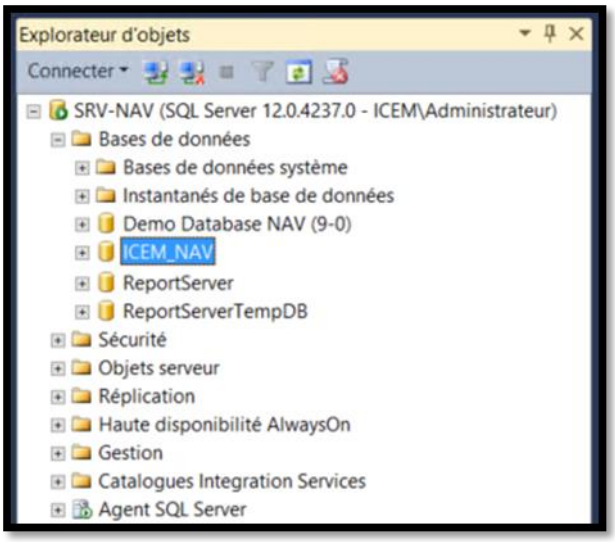


Figure 4- 29:Base SQL Prod restauré

Installation Dynamics Navision 2016 :

Apres l'installation du serveur SQL est préparé la base Production, on va maintenant installer Dynamics Navision 2016.

Exécuter le fichier d'exécution depuis le CD officiel Navision :

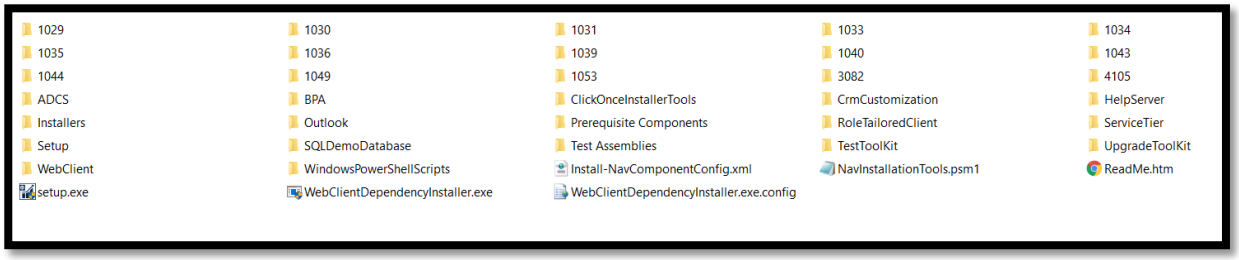


Figure 4- 30: Cd d'installe Dynamics Navision 2016

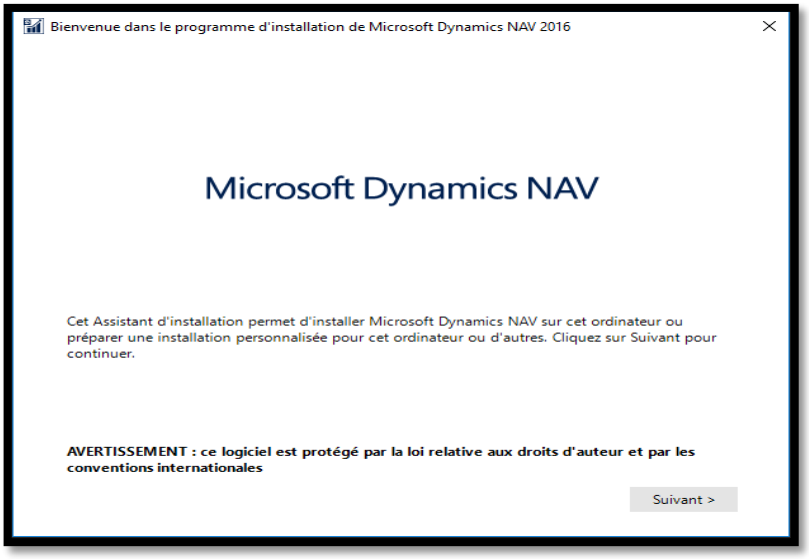


Figure 4- 31:Programme d'installation Navision 2016

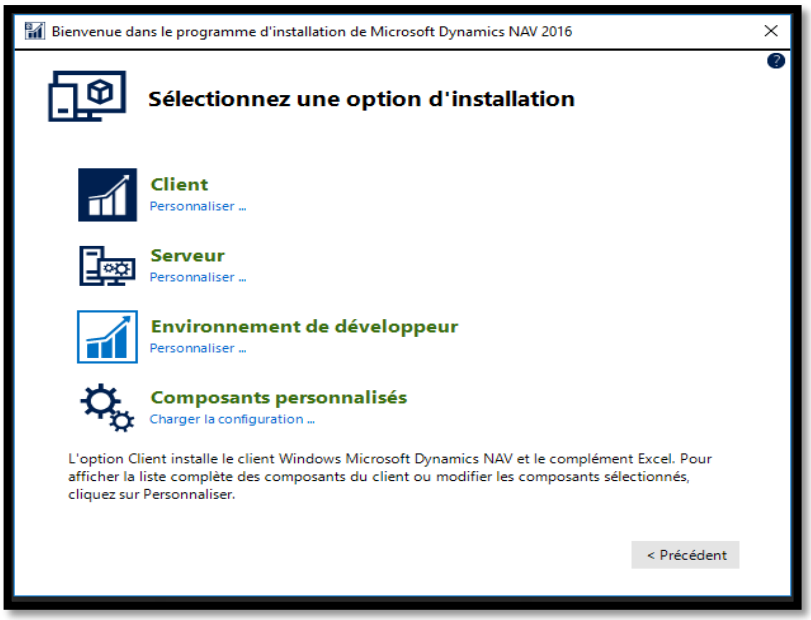


Figure 4- 32:Sélectionner les options d'installation

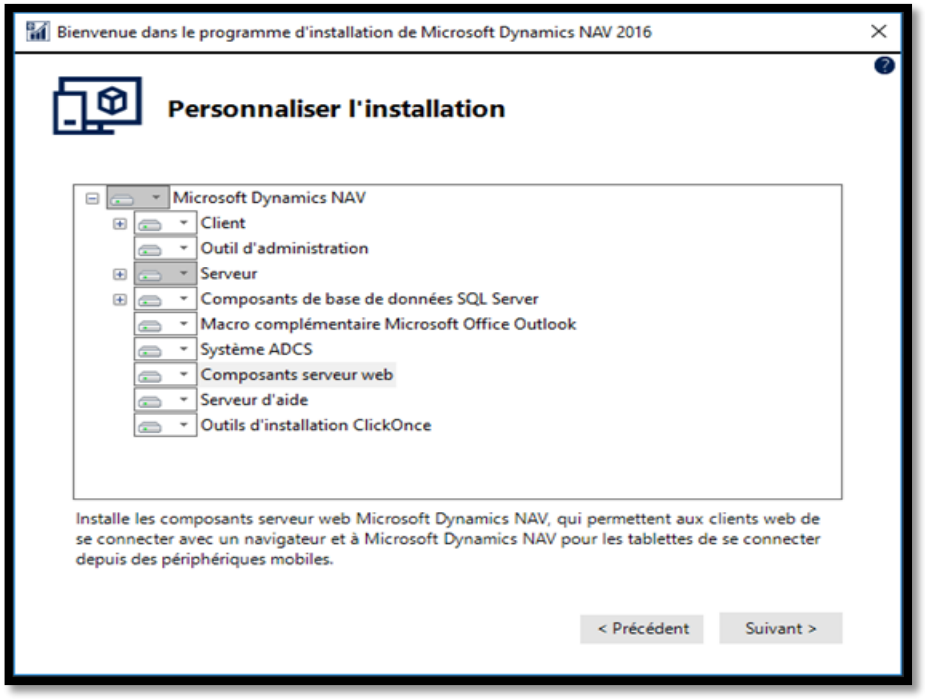


Figure 4- 33:Sélectionner les fonctionnalités du serveur

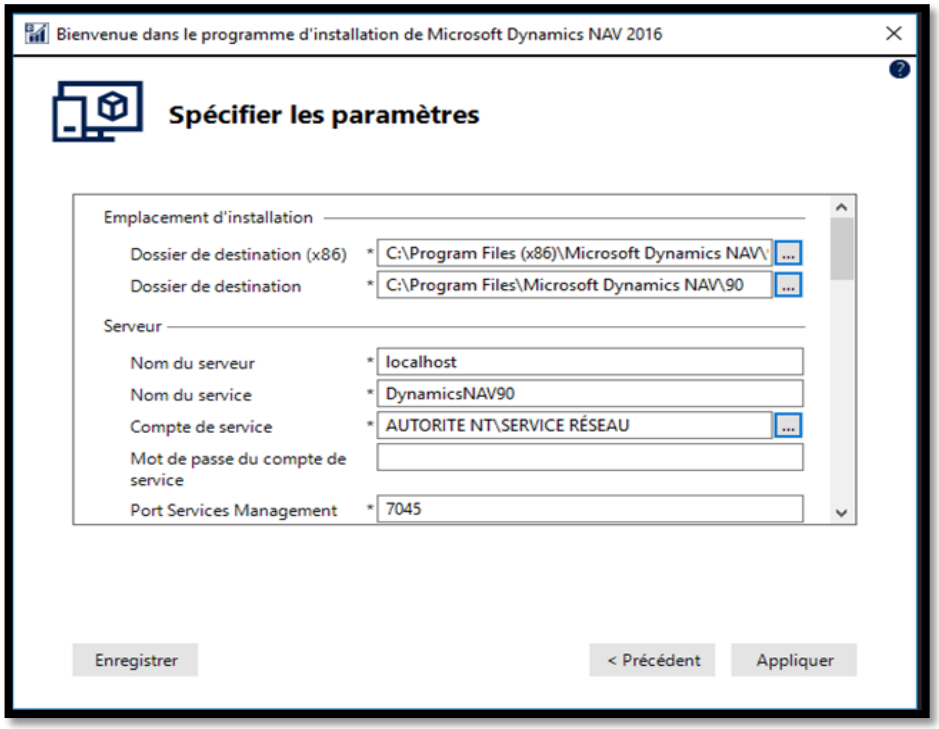


Figure 4- 34: Configuration du serveur page 1

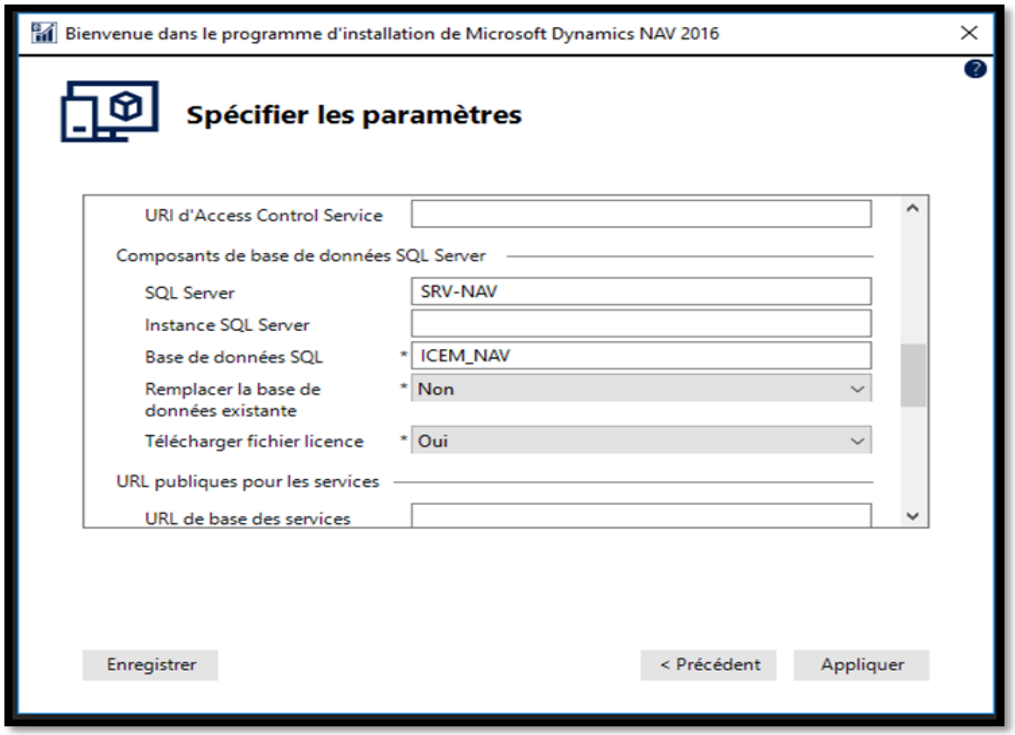


Figure 4- 35: Configuration du serveur page 2

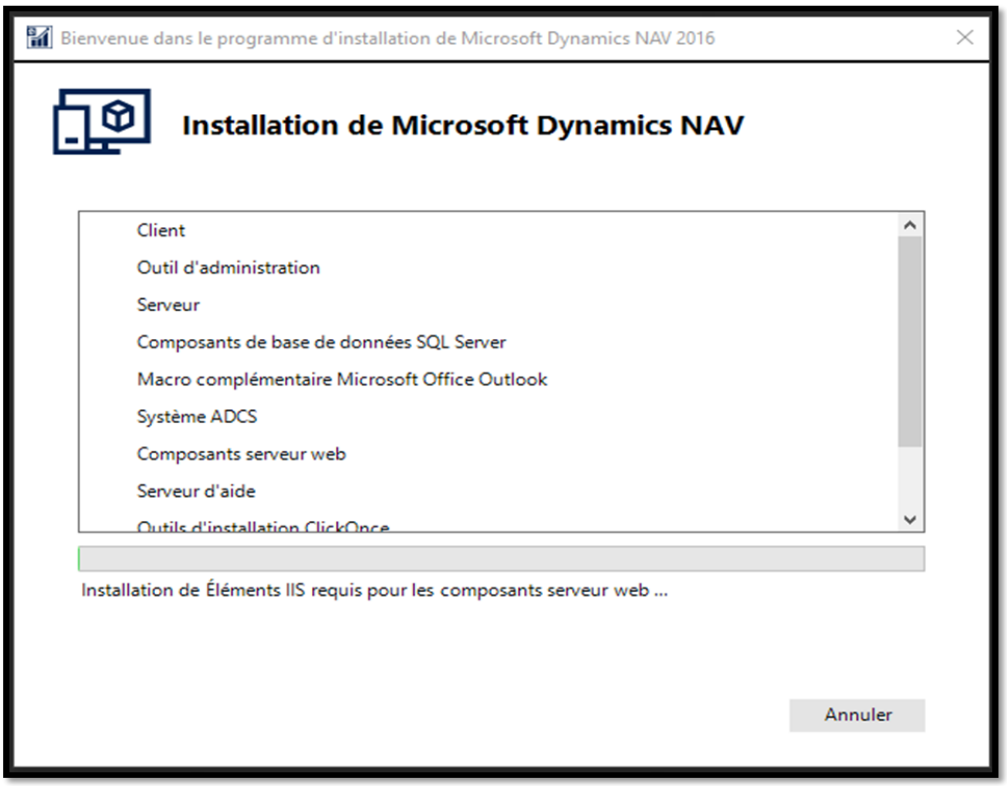


Figure 4- 36:Lancement de l'installation

Apres l'installation du serveur il faut vérifier l'état et la configuration de l'instance Navision installer via cette interface d'administration :

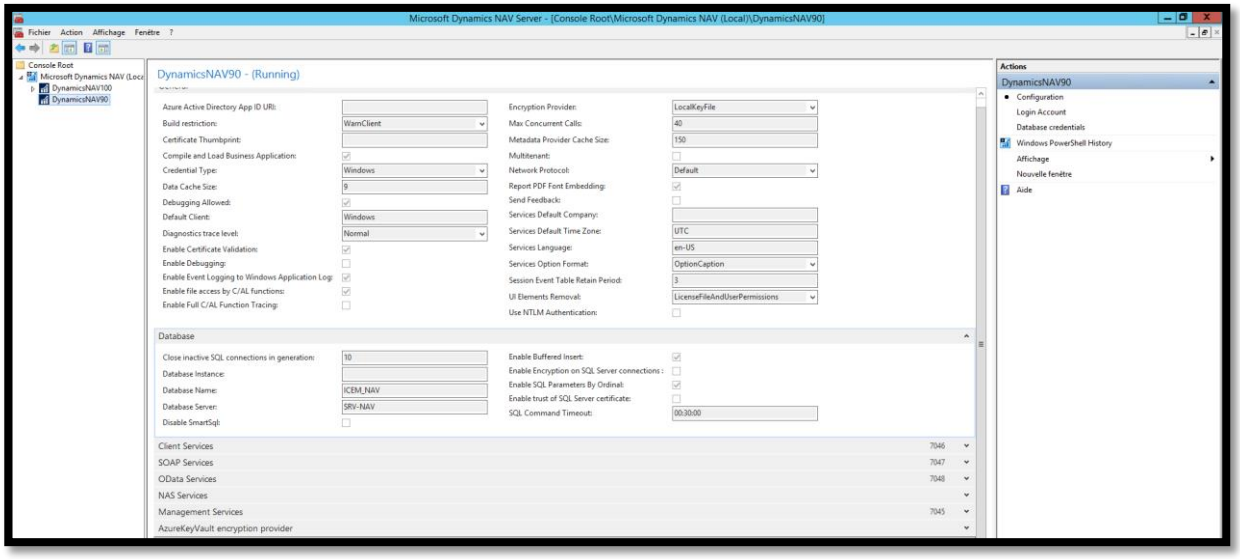


Figure 4- 37: Administration centrale serveur Dynamics Navision

Figure 4- 38:Instance Dynamics Navision 2016

Apres la vérification de l'instance installée on peut lancer client Navision 2016 :

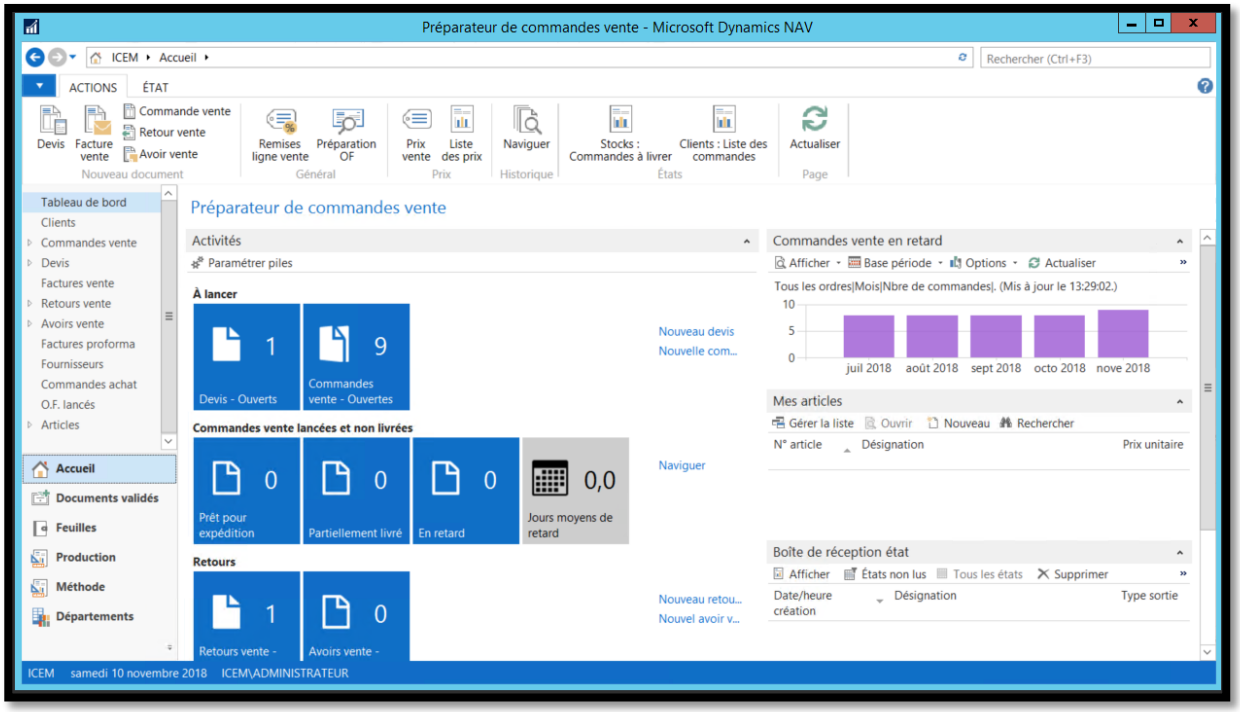


Figure 4- 39:Tableau de bord Serveur Navision 2016

1.2.3. Serveur Symantec Endpoint Protection

L'installation du logiciel de gestion pour la première fois comporte deux parties. La première partie installe Symantec Endpoint Protection Manager. La deuxième partie installe et configure la base de données Symantec Endpoint Protection Manager. Dans la première, vous pouvez accepter tous les paramètres par défaut. Dans la deuxième partie, vous devez sélectionner le type de configuration de Symantec Endpoint Protection Manager, Simple ou Avancée, en fonction du nombre de clients pris en charge par le serveur. La configuration simple, conçue pour un serveur prenant en charge moins de 100 clients, crée automatiquement une base de données incorporée et applique les valeurs par défaut à la plupart des paramètres, avec une intervention minime de votre part. La configuration avancée, destinée aux administrateurs d'environnements plus importants, vous permet de définir des paramètres spécifiques à votre environnement.

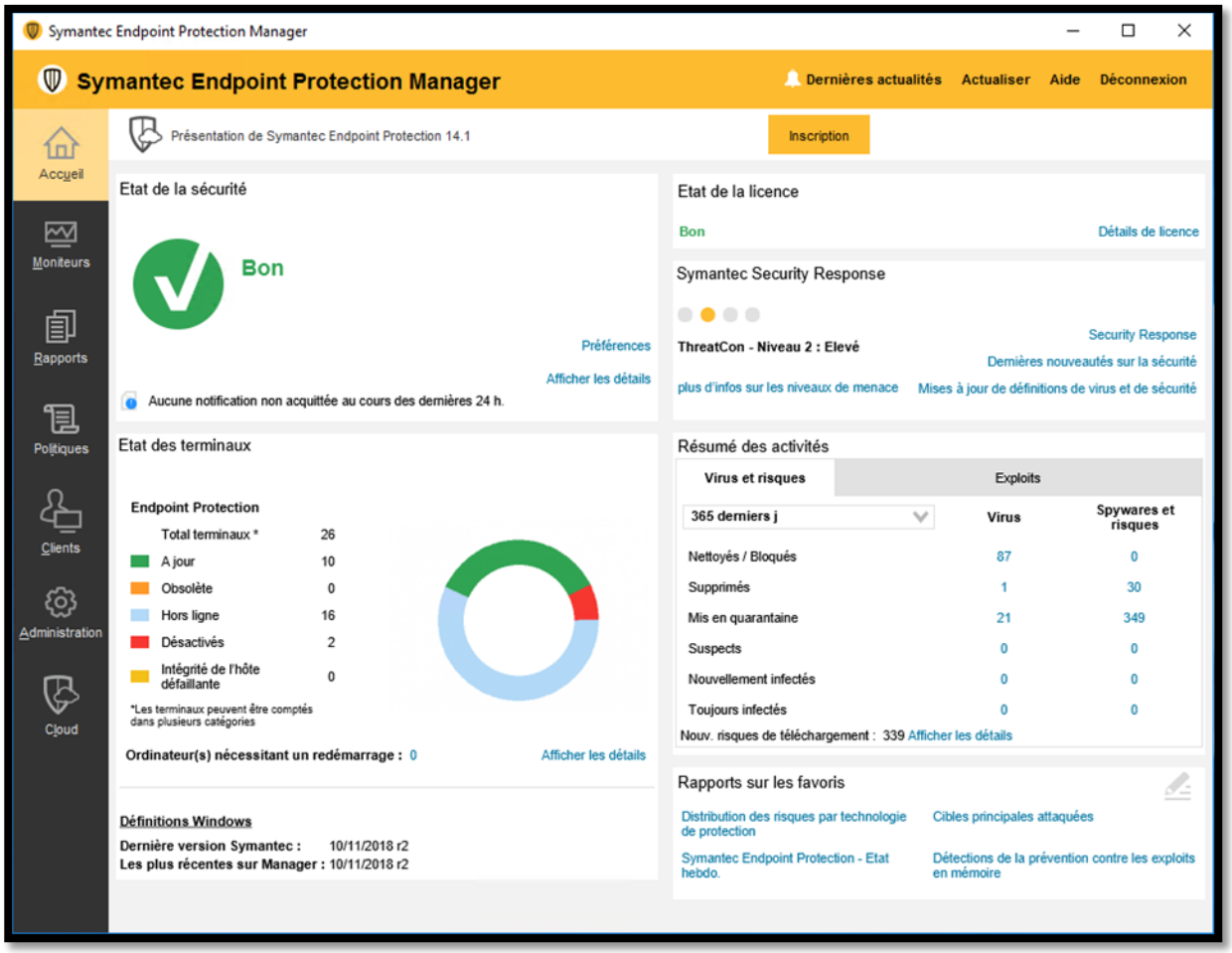


Figure 4- 40:Interface d'administrateur serveur Symantec Endpoint Protection

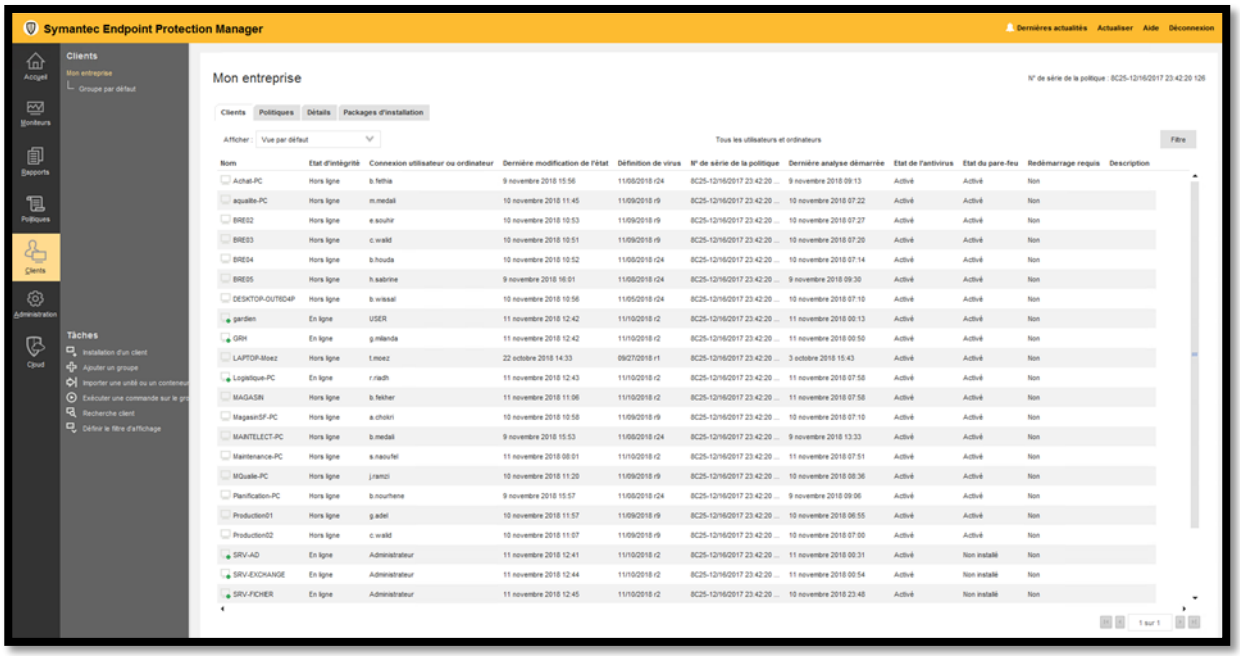


Figure 4- 41:Vue sur l'administration utilisateurs

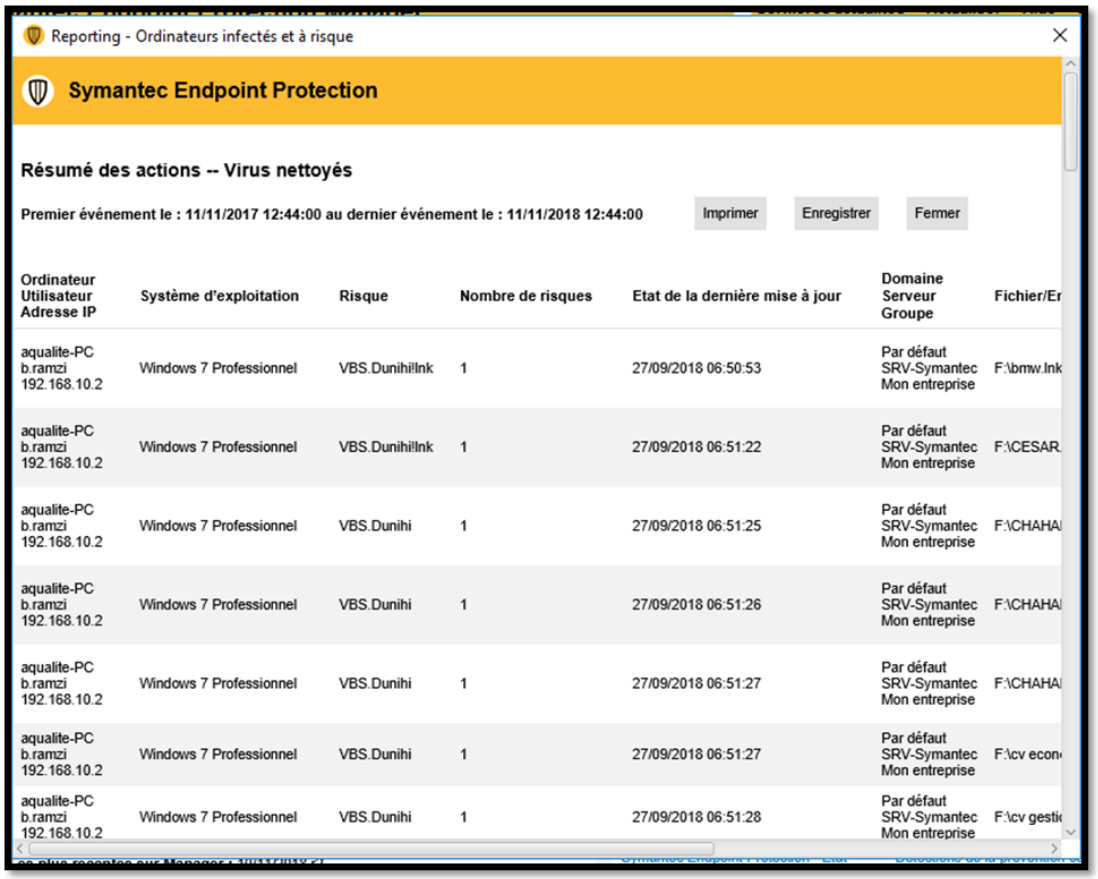


Figure 4- 42:Protection a temps réel

1.3. Etat final de la plateforme de virtualisation

Ces interfaces montrent L'état final VMware Vcenter, les différentes machines virtuelles et les différents serveurs de notre entreprise après leurs installations et leurs configurations. **(Figure 4.43 ,4.44).**

Figure 4- 43:Caractéristiques du serveur

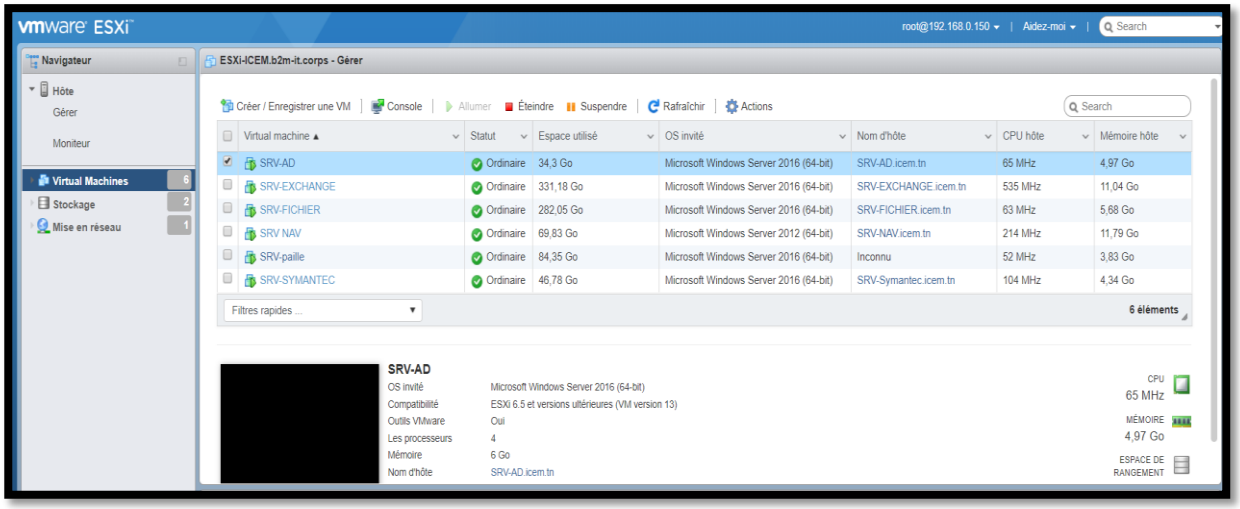


Figure 4- 44:Les différentes machines virtuelles installées

1.4. Plateforme Office 365

Office 365 est un abonnement incluant les versions Premium des applications Office sur tous vos appareils, des mises à jour de fonctionnalités exclusives mensuelles et 1 To de stockage en ligne. Office 2019 est un achat définitif qui inclut les versions classiques des applications Office installées sur un PC ou un Mac (ou 5 et plus avec une licence en volume).

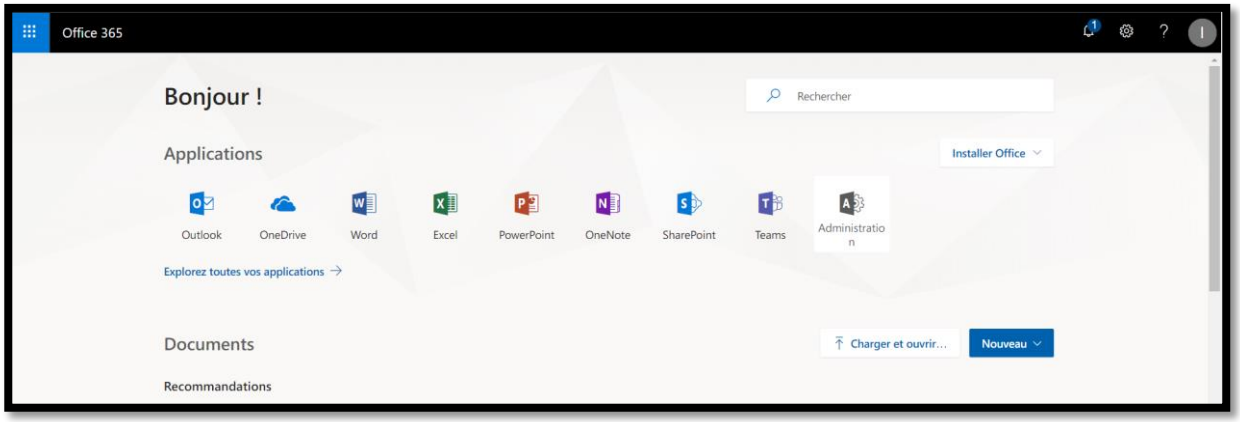


Figure 4- 45:Tableau de bord Office 365

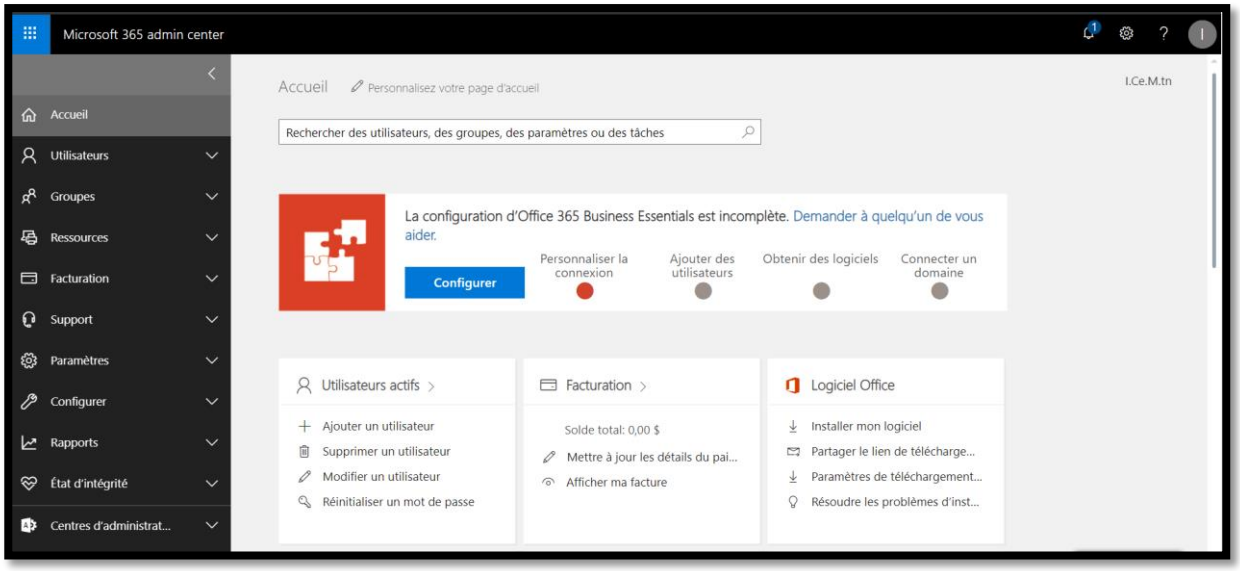


Figure 4- 46:Centre d'administrateur Office 365

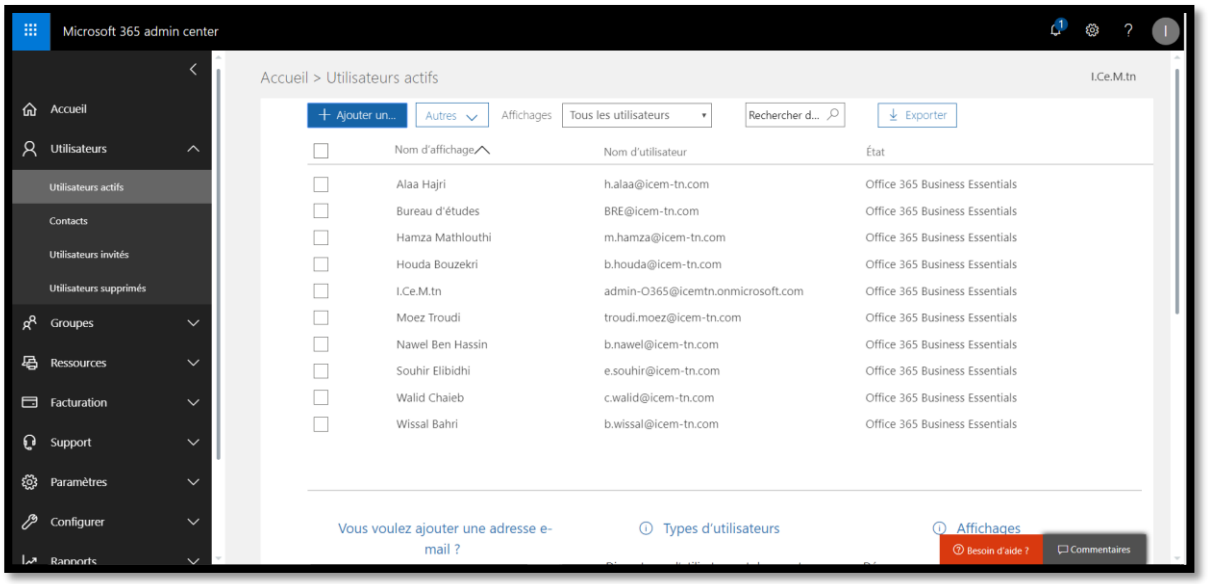


Figure 4- 47:Liste des utilisateurs actifs

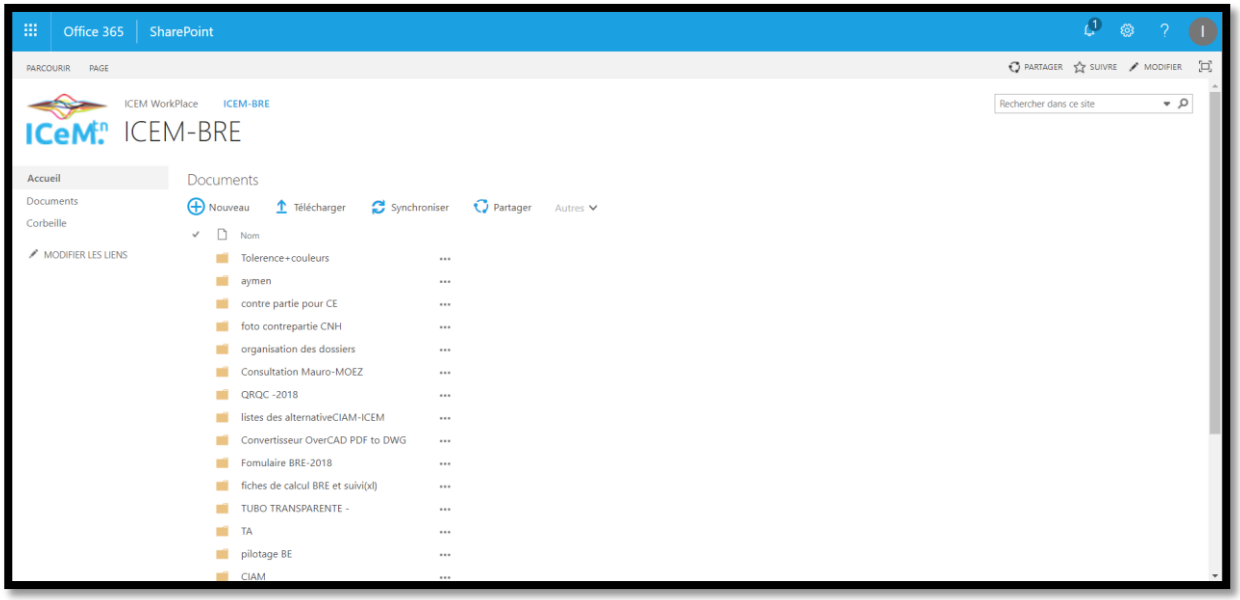


Figure 4- 48:Partage des fichiers sur SharePoint Office 365

2. Infrastructure Réseaux :

Cette partie a pour objet de contribuer à détailler le matériel utilisé dans l'infrastructure et à présenter les équipements nécessaires à la mise en place de la nouvelle infrastructure réseau ainsi que l'implémentation de la politique sécurité.

La figure 4.1 ci-dessous présente une vue globale sur tous les équipements matériels de la nouvelle infrastructure réseau. Cette architecture est composée de quatre parties :

- Partie accès du réseau présente les commutateurs utilisateur ou d'accès.
- Partie cœur du réseau regroupe les commutateurs gigabit du réseau LAN.
- Partie sécurité du réseau héberge les pare-feux *Cyberoam.*
- Partie connexion sans fil Wifi

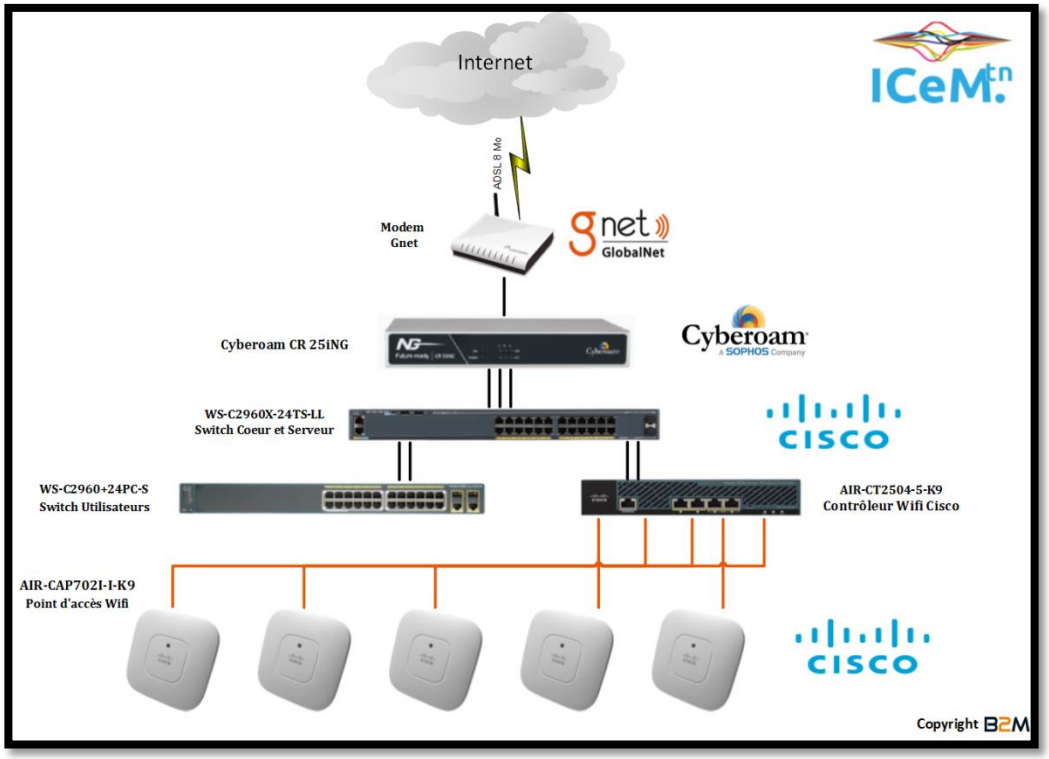


Figure 4- 49:Architecture réseaux

2.1. Couche accès du réseau

La partie accès du réseau est présentée par un commutateur de type Catayst 2960+24 nommé comme suit SW-ACC-252. Ces commutateurs permettent d'interconnecter les hôtes utilisateurs. Cette partie associe aussi trois points d'accès Wi-Fi de type Cisco Aironet 702i.

Figure 4- 50:Commutateurs d'accès Cisco Catalyst 2960 Plus - 24 Ports

2.2. Couche cœur du réseau

La partie cœur du réseau est composée de d'un commutateur gigabit de type Catalyst C2960X-24TS-L nommé comme suit : SW-SRV-253. Ces commutateurs permettent de relier la partie accès du réseau.

Figure 4- 51:Commutateurs cœur Cisco Catalyst C2960X - 24 ports

2.3. Couche sécurité du réseau

Pour la mise en place de notre politique de sécurité on a eu recours à une solution UTM du Cyberoam. Son action combinée propose une sécurité complète basée sur une identification des utilisateurs selon leur authentification. En effet elle attribue une authentification AD pours les utilisateurs locaux alors qu'elle crée des comptes temporaires au niveau Cyberoam pour les visiteurs du siège. Ce qui garantit une sécurité de l'environnement.

Cette Appliance comporte entre autres des fonctionnalités de pare-feu, VPN, antivirus, anti spam et anti logiciel malveillant, IDP, filtrage de contenu et gestion de la bande passante ainsi qu'un *reporting* détaillé basé sur l'identité de l'utilisateur.

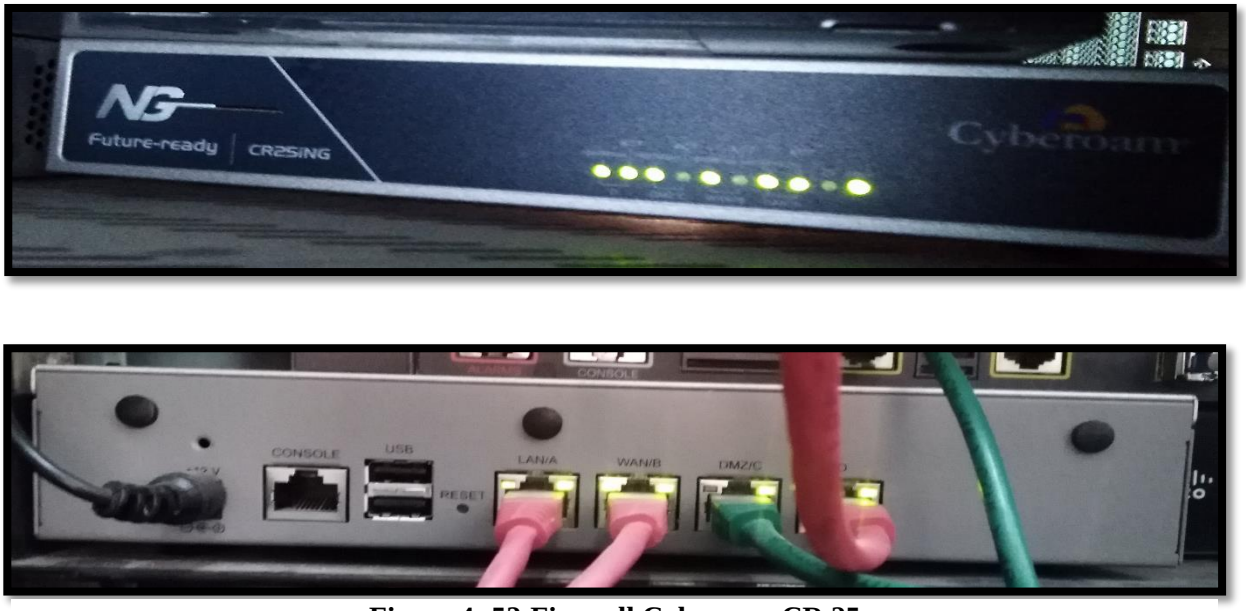


Figure 4- 52:Firewall Cyberoam CR 25

2.4. Couche réseaux sans fil

La partie réseaux sans fil est composée par un contrôleur sans fil Cisco 2500 Model 2504 qui

lier directement avec switch cœur et 5 point d'accès Cisco Aironet 702i lier avec le switch utilisateurs.

Figure 4- 53:Contrôleur sans fil Cisco 2500

2.5. Mise en place et paramétrage des équipements réseaux

Dans ce qui suit nous présentons la configuration détaillée pour chaque équipement réseau de l'infrastructure

2.5.1. Configuration des commutateurs d'accès du réseau

Pour la configuration des quatre commutateurs d'accès nous avons :

- Nommé le commutateur lors de la phase design de l'architecture réseau.
- Déclaré le protocole du routage *spanning tree* à utiliser.
- Déclaré la liste des VLAN déterminée lors de la phase design de l'architecture réseau.
- Affecté une adresse IP pour chaque commutation selon l'architecture choisie.
- Déclaré la passerelle par défaut.

Tous les détails de configuration du commutateur d'accè se trouvent dans la partie **Annexe A**.

2.5.2. Configuration des commutateurs cœur du réseau

Pour la configuration le commutateur cœur du réseau LAN :

- Nommé le commutateur lors de la phase design de l'architecture réseau.
- Déclaré le protocole du routage à utiliser *spanning tree*.
- Déclarer la liste des VLAN déterminée lors de la fasse design de l'architecture réseau.
- Déclaré la priorité de chaque VLAN pour le routage *spanning tree*.
- Affecté chaque port de commutateur à un VLAN déterminé.

- Affecté une adresse IP pour chaque commutation selon l'architecture choisie.
- Déclaré la passerelle par défaut.

Tous les détails de configuration des commutateurs cœur se trouvent dans la partie **Annexe B**.

2.5.3. Configuration des points d'accès sans fil et contrôleur

Les points d'accès sont éparpillés sur le différent emplacement pour assurer la couverture WIFI à tout point du bâtiment. Les adresses IP des points d'accès sont attribuées automatiquement etappartiennent au réseau de management. Les points d'accès sont connectés à des switches PoE sur des interfaces associés au VLAN 99 ce qui leurs permet de s'associer au contrôleur sans avoir besoins de configuration supplémentaires.

Pour le contrôleur, la configuration de l'adresse de management se fait en mode setup. Une fois le mode setup est terminé, toutes les configurations sur le contrôleur peuvent se faire en utilisant un accès HTTPS en utilisant l'adresse de management.

Quatre réseaux WLAN ont été définis :

- ICEM-Data : permettant de se connecter au réseau VL-Wifi-Data selon les paramètres d'authentification.
- ICEM -Guest : permettant de véhiculer l'ensemble du trafic des visiteurs sans fil au réseau VL-Wifi-Visiteurs.
- ICEM -VIP : permettant de véhiculer l'ensemble du trafic du groupe VIP sans fil au réseau VL-VIP.
- T-MOBILE : permettant de véhiculer l'ensemble du trafic des tablettes sans fil au réseau T-MOBILE.

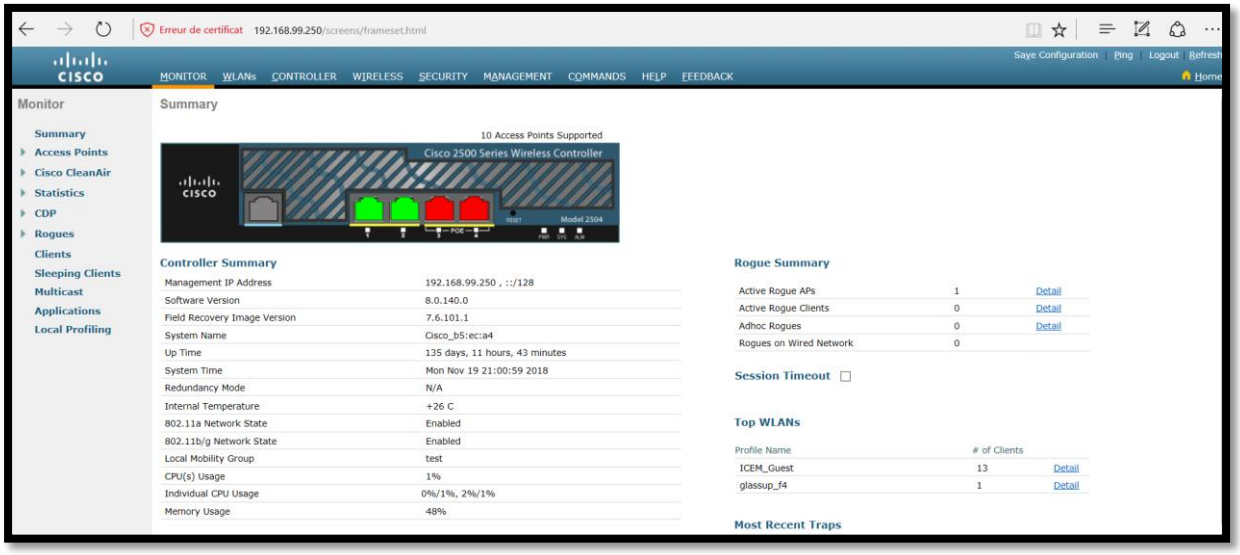


Figure 4- 54:Tableau de bord contrôleur wifi

2.1.1. Configuration pare-feu Cyberoam

Dans cette partie nous entamons la mise en œuvre de la politique de sécurité interne et externe de notre infrastructure.

Cyberoam offre une sécurité de grande souplesse à l'entreprise tout en assurant une protection contre les attaques mixtes, les logiciels malveillants, les chevaux de Troie, les attaques DoS et DDoS, les attaques par usurpation d'adresse IP, les spams, les intrusions et les fuites de données.

Durant cette phase de mise en place d'une politique de sécurité, nous utilisons et nous exploitons les différents onglets de l'interface web de management *Cyberoam* détaillés dans la Figure 4.55 :

Figure 4- 55:Cyberoam management

- **Segmentaion du réseau LAN**

La figure 4.56 ci-dessous illustre la configuration des vlan pour la segmentation du réseau local par département ainsi que la déclaration de l'interface du zone DMZ et les interfaces physiques WAN. Au niveau de cette interface Cyberoam, chaque sous interface de port A est déclarée comme une passerelle par défaut du VLAN correspondant :

	Nom de l'interface	Type d'interface	Statut	Adresse IP		Nom de la zone
				IP	Type	
	PortA	Physique	Connected, 1000 Mbps - Full Duplex	192.168.99.254/255.255.255.0	Statique	LAN
	PortA.10	VLAN	-	192.168.10.254/255.255.255.0	Statique	LAN
	PortA.30	VLAN	-	192.168.30.254/255.255.255.0	Statique	LAN
	PortA.40	VLAN	-	192.168.40.254/255.255.255.0	Statique	LAN
	PortA.60	VLAN	-	192.168.60.254/255.255.255.0	Statique	LAN
	PortA.80	VLAN	-	192.168.80.254/255.255.255.0	Statique	WIFI_CASQUE

Figure 4- 56: Déclaration des Vlan au Niveau Firewall Cyberoam

Afin de déclarer les passerelles externes du réseau local nous utilisons l'interface illustrée dans la figure 4.57 pour ajouter les ports WAN. Ces ports, à travers lesquels tout trafic réseau vers et depuis l'extérieur sera acheminé, assurent l'accès au réseau externe.

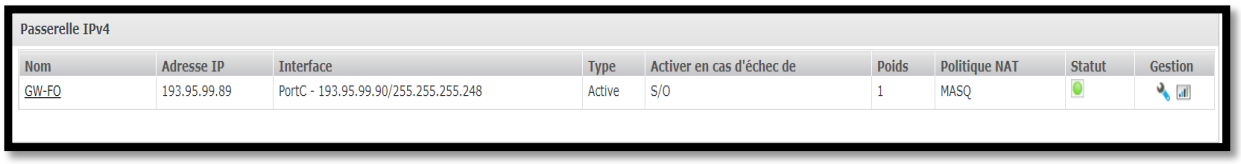


Figure 4- 57:Passerelle WAN

- **Définition des règles de filtrages et de la sécurité réseau**

Dans cette partie, nous utilisons l'interface présentée dans la figure 4.58 pour déclarer les règles de pare-feu et assurer le filtrage du trafic réseau entre les différentes zones de l'infrastructure. Comme il est mentionné dans cette figure, nous avons déclaré 16 règles de filtrages pour contrôler tout le trafic réseaux.

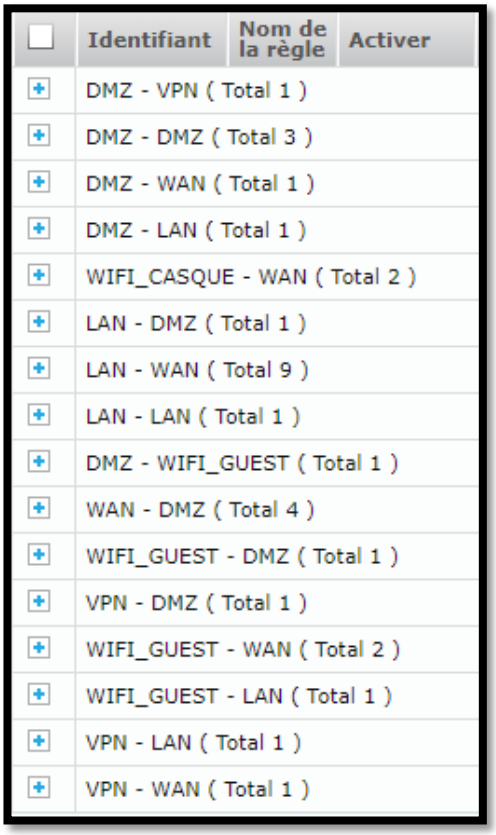


Figure 4- 58: les règles de pare-feu

La figure 4.59 ci-dessous montre les règles du filtrage web et applicatif pour contrôler

le trafic de la zone LAN vers la zone WAN :

- La règle VIPTOWAN : Autorise l'accès internet pour la Vlan-VIP.
- La règle filtrage wifi-data : Activer le filtrage Web et applicatif sur les utilisateurs Wifi-Data.
- Lan –avant-150 : Activer le filtrage Web et applicatif sur la Vlan10 qui appartient au groupe adressage moins de 10.150 IP

LAN - WAN (Total 9)							
19	VIPTOWAN	ON	VLAN-VIP	N'importe quel hôte	N'importe quel service	Accepter
29	wifi-Guest	OFF	LAN-Guest	N'importe quel hôte	N'importe quel service	Accepter
28	LAN-T-MOBILE	ON	LAN60	N'importe quel hôte	N'importe quel service	Accepter
27	filtrage-wifi-data	ON	filtrage-wifi-data	N'importe quel hôte	N'importe quel service	Accepter
16	LAN-AVANT-150	ON	LAN-AVANT-150	N'importe quel hôte	N'importe quel service	Accepter
15	LAN-APRES-150	ON	LAN-APRES-151	N'importe quel hôte	N'importe quel service	Accepter
5	LANTOWAN	ON	N'importe quel hôte	N'importe quel hôte	N'importe quel service	Bloquer
2	#LAN_WAN_LiveUserTraffic	ON	N'importe quel hôte	N'importe quel hôte	N'importe quel service	Bloquer
1	#LAN_WAN_AnyTraffic	ON	N'importe quel hôte	N'importe quel hôte	N'importe quel service	Bloquer

Figure 4- 59:Règles de filtrage Wan (Internet)

- **VPN PPTP :**

La configuration du Vpn PPTP est niveau d'interface utilisateur comme nous montre la figure ci-dessous :

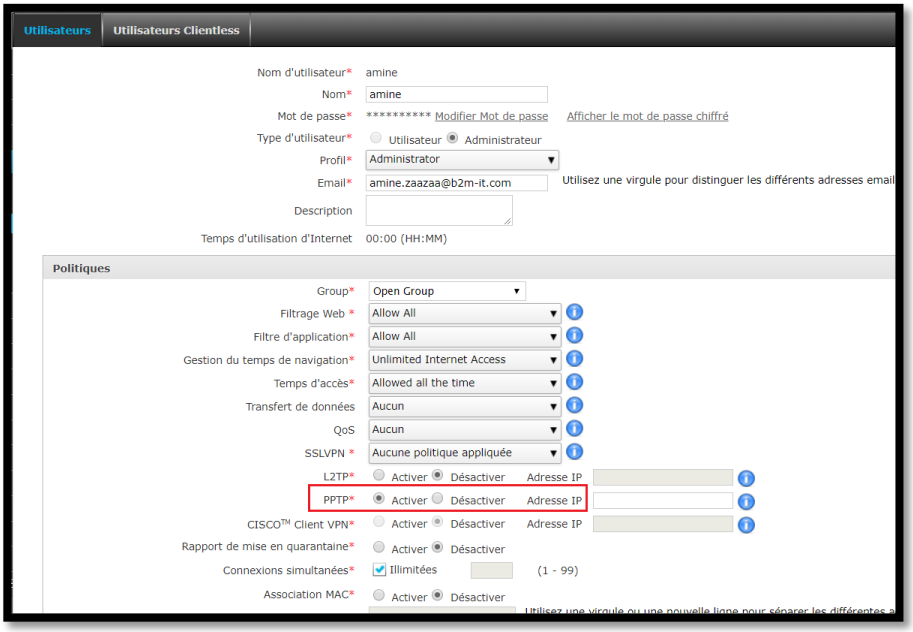


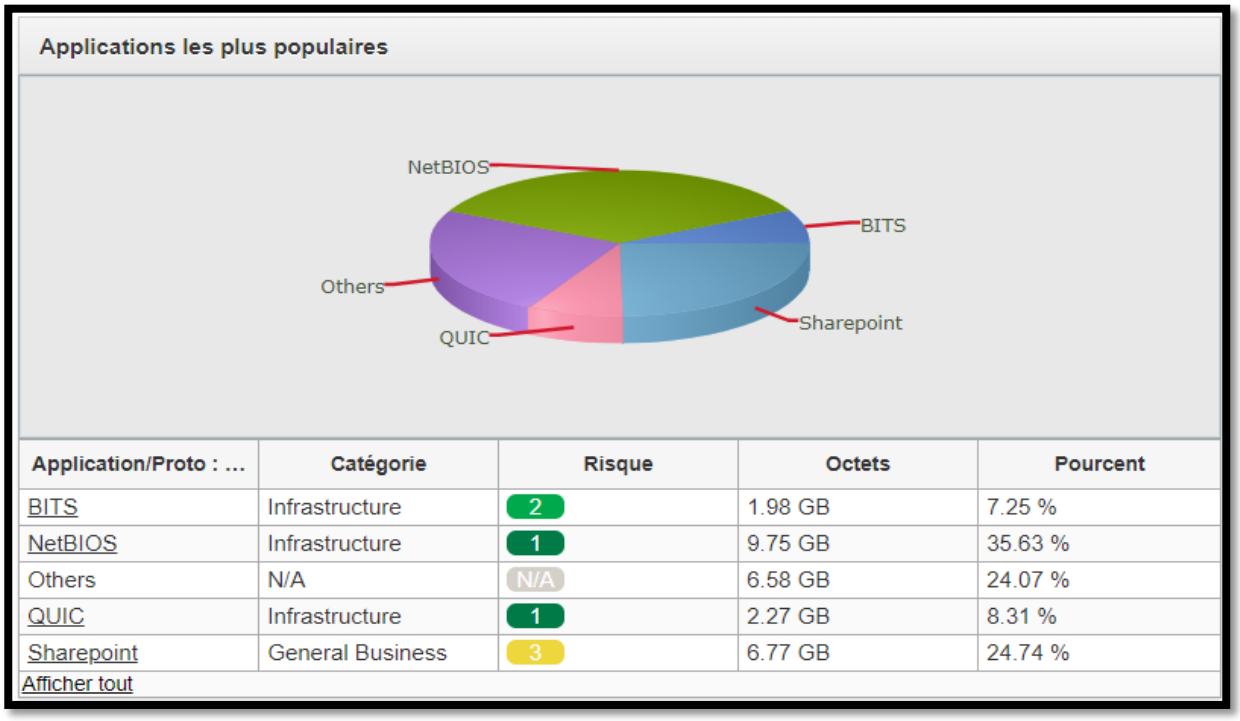
Figure 4- 60: Configuration d'un utilisateur

2.6. Journalisation et rapports

Après la réalisation de la configuration et le paramétrage des équipements réseaux, nous exposons dans ce qui suit, les différents écrans de la journalisation et du monitoring de notre infrastructure réseau.

Tout trafique réseau qu'il soit interne ou externe passe à travers les pare-feux Cyberoam d'où l'importance de cet outil dans la supervision du réseau.

L'interface « Applications les plus populaires », illustrée par la **figure 4-61**, permet de visualiser des statistiques sur les applications/protocoles les plus utilisés dans le réseau.

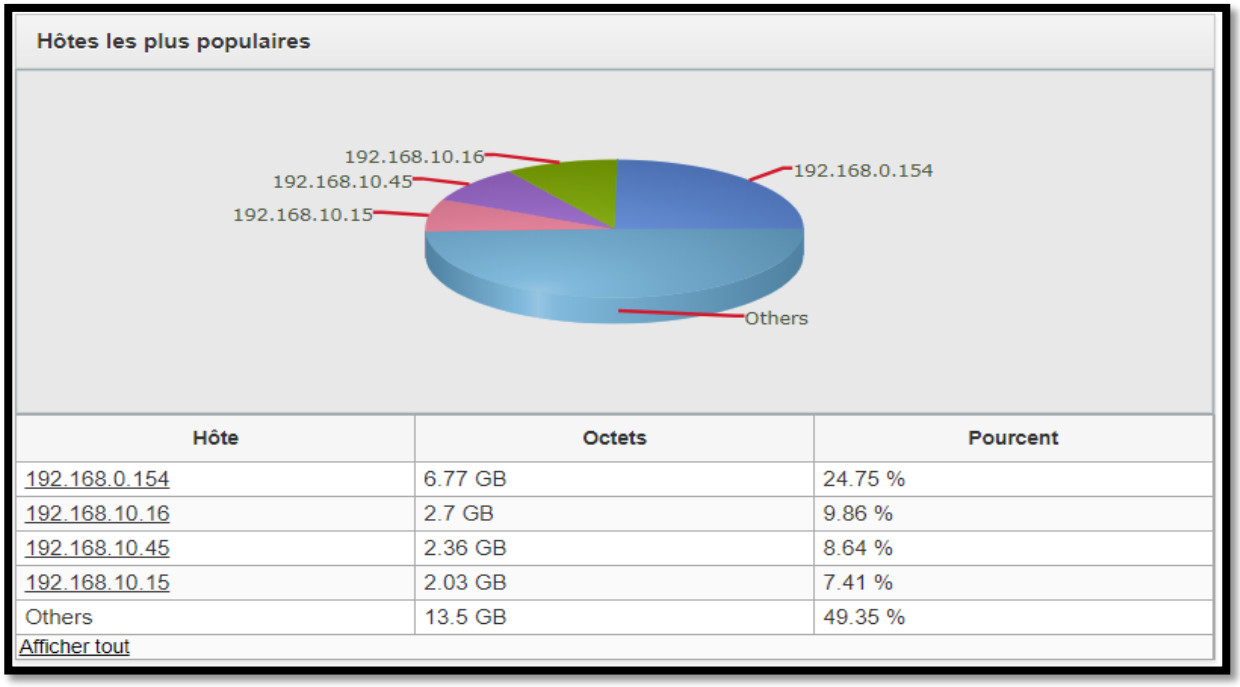


Application/Proto : ...	Catégorie	Risque	Octets	Pourcent
BITS	Infrastructure	2	1.98 GB	7.25 %
NetBIOS	Infrastructure	1	9.75 GB	35.63 %
Others	N/A	N/A	6.58 GB	24.07 %
QUIC	Infrastructure	1	2.27 GB	8.31 %
Sharepoint	General Business	3	6.77 GB	24.74 %

Afficher tout

Figure 4- 61:Tableau de bord Trafic

Dans le même contexte, la **figure 4.62** présente l'interface « les hôtes les plus populaires», qui visualise les statistiques des utilisateurs/hôtes les plus populaires dans le réseau, ainsi que leurs bandes passantes et leurs pourcentages d'utilisation



Hôte	Octets	Pourcent
192.168.0.154	6.77 GB	24.75 %
192.168.10.16	2.7 GB	9.86 %
192.168.10.45	2.36 GB	8.64 %
192.168.10.15	2.03 GB	7.41 %
Others	13.5 GB	49.35 %

Afficher tout

Figure 4- 62:Hôtes les plus populaires

On peut aussi afficher l'historique détaillé de téléchargement des fichiers par utilisateur comme le présente la **figure 4.63**.

Téléchargement de fichier le plus populaire

Date	Utilisateurs	IP source	Nom de domaine	Nom de fichier	Taille
2018-11-15 11:54:35	N/A	192.168.50.25	IT-MIL-INT-R002.teamviewer.com	IT-MIL-INT-R002.teamviewer.com/d...	488.28 KB
2018-11-15 11:55:41	N/A	192.168.50.25	IT-MIL-INT-R002.teamviewer.com	IT-MIL-INT-R002.teamviewer.com/d...	488.28 KB
2018-11-15 11:56:07	N/A	192.168.50.25	IT-MIL-INT-R002.teamviewer.com	IT-MIL-INT-R002.teamviewer.com/d...	488.28 KB
2018-11-15 11:56:10	N/A	192.168.50.25	IT-MIL-INT-R002.teamviewer.com	IT-MIL-INT-R002.teamviewer.com/d...	488.28 KB
2018-11-15 11:56:15	N/A	192.168.50.25	IT-MIL-INT-R002.teamviewer.com	IT-MIL-INT-R002.teamviewer.com/d...	488.28 KB
2018-11-15 11:57:09	N/A	192.168.50.25	IT-MIL-INT-R002.teamviewer.com	IT-MIL-INT-R002.teamviewer.com/d...	488.28 KB
2018-11-14 15:04:17	N/A	192.168.10.4	safebrowsing.googleusercontent.com	safebrowsing.googleusercontent.co...	14.53 KB
2018-11-12 16:59:44	N/A	192.168.10.16	ELB-for-CIP20-ASE-PRD-82843876...	{1f04b7d5-d925-4234-a799-586ccd...	10.68 KB
2018-11-17 11:58:10	N/A	192.168.10.16	ELB-for-CIP20-ASE-PRD-82843876...	{efb0244e-d02a-4669-9189-a7e482...	10.68 KB
2018-11-16 16:57:07	N/A	192.168.10.16	ELB-for-CIP20-ASE-PRD-82843876...	{601cd7ae-e2b1-4565-8ff7-7375511...	10.68 KB
2018-11-14 17:01:48	N/A	192.168.10.16	ELB-for-CIP20-ASE-PRD-82843876...	{ef36133c-994e-4fab-a518-c7b63ac...	10.68 KB
2018-11-19 15:51:57	N/A	192.168.10.16	ELB-for-CIP20-ASE-PRD-82843876...	{d25b246c-6274-459a-af99-66a413...	10.68 KB
2018-11-14 08:27:36	N/A	192.168.10.16	ELB-for-CIP20-ASE-PRD-82843876...	{b7f4f1dc-1af0-4e15-9f17-42e40f87...	10.68 KB
2018-11-12 13:19:03	N/A	192.168.10.16	ELB-for-CIP20-ASE-PRD-82843876...	{b494e880-ade8-4a5c-9191-05331b...	10.68 KB
2018-11-14 08:26:32	N/A	192.168.10.16	ELB-for-CIP20-ASE-PRD-82843876...	{9f5410ed-b47e-4f39-b349-f67ac86...	10.68 KB

Figure 4- 63:Historique de téléchargement

L'interface « Principales applications refusées », indiquée par la **figure 4.64**, permet de visualiser des statistiques sur les applications refusées par le pare-feu, leurs ports, leurs indices de risque, leurs catégories et le nombre total des requetés interceptés.

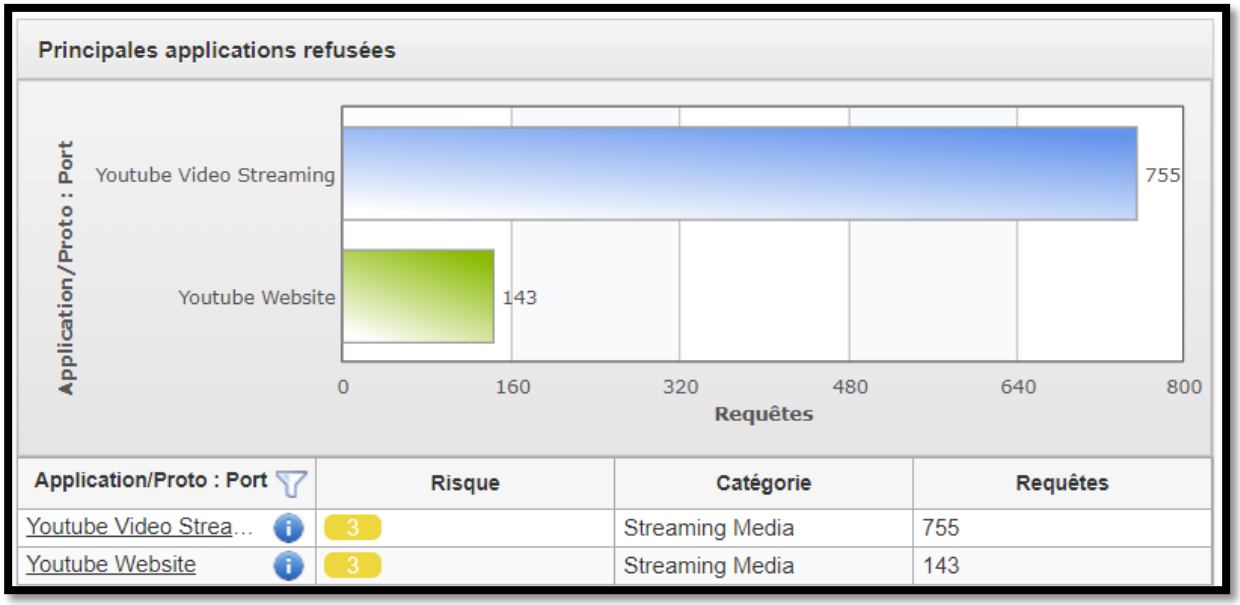


Figure 4- 64:Principales applications refusées

Conclusion

Cette partie constitue une concrétisation de notre projet. Ainsi, on a eu recours à une mise en place et un paramétrage de la nouvelle infrastructure système et réseau. Par ailleurs une configuration des nouveaux équipements et une nouvelle conception aussi bien des règles que la politique de sécurité de notre réseau ont été élaborées afin de garantir un réseau robuste.

Notre travail a été peaufiné par une journalisation et un monitoring de notre nouvelle infrastructure afin de détecter toute menace de trafic sur notre réseau.

Nous arrivons donc à la fin de notre rapport que nous clôturerons avec la conclusion générale et les perspectives.

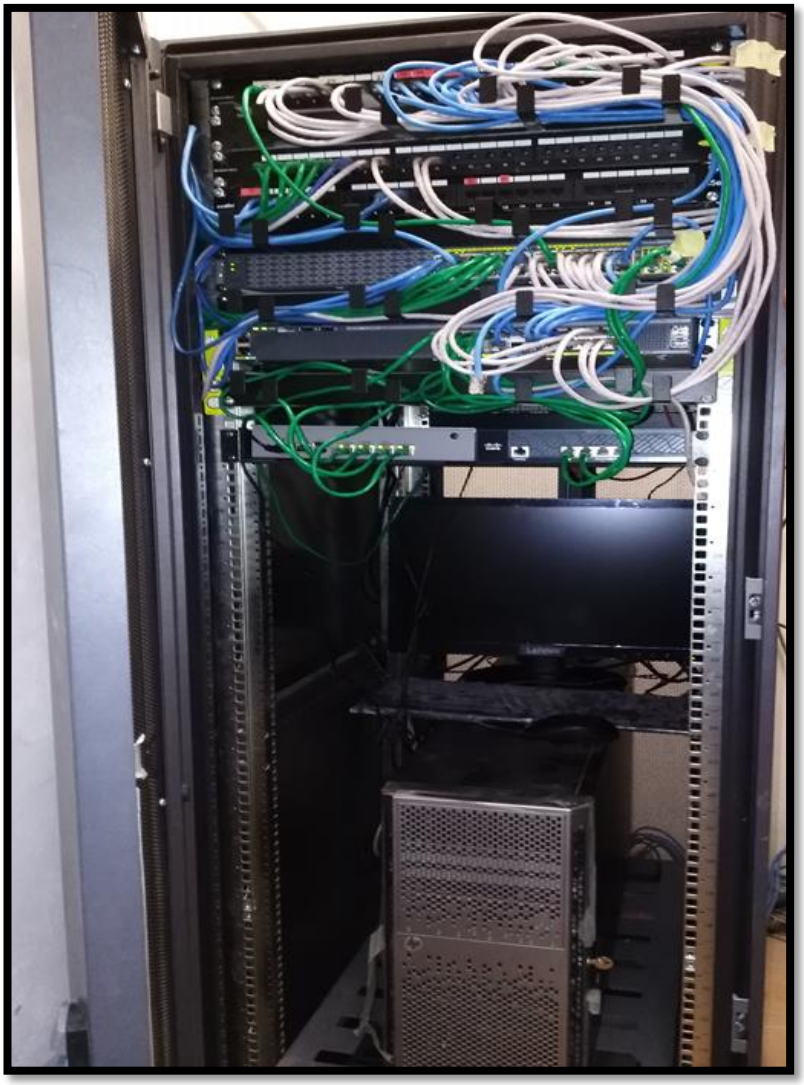


Figure 5 - 1: Vue réelle d'armoire après le projet

Conclusion générale

Tout au long de ce travail réalisé dans le cadre du projet de fin d'étude pour l'obtention diplôme de Mastère professionnel en Nouvelles Technologies des Télécommunications et Réseaux (N2TR), nos efforts se sont concentrés sur l'analyse, la conception et la mise en place d'une nouvelle infrastructure système et réseau sécurisée.

L'objectif de ce projet de fin d'études a été la mise en place d'une infrastructure compète, ce qui nous a permis de comprendre les concepts liés aux réseaux informatiques d'entreprise, les différentes technologies utilisées et leur mise en place grâce à des équipements réseaux professionnels. Nous avons donc procédé dans une première phase à l'étude complète de l'infrastructure réseau existante au siège ICEM.tn, et essayé d'en identifier les lacunes. Nous avons ensuite réalisé l'étude conceptuelle de la nouvelle architecture système et réseau visé par l'entreprise. Nous sommes ensuite passés à la phase de réalisation. Dans cette phase, nous avons d'abord assisté à l'étape de câblage et du déploiement de l'infrastructure physique et virtuelle puis nous avons installé et configuré tous les nouveaux équipements de la nouvelle infrastructure et implémenté une nouvelle politique de sécurité à l'échelle de la société pour protéger les différentes composantes du réseau. Nous avons, enfin, migré et testé la nouvelle architecture et en avons supervisé la mise en production de au sein de ICEM.tn.

En guise de conclusion, le travail que nous avons réalisé, nous a permis de mettre en pratique nos connaissances académiques acquises tout au long de notre formation et d'approfondir nos connaissances dans le domaine de Nouvelles Technologies des Télécommunications et Réseaux. Nous avons eu l'occasion d'améliorer nos compétences dans l'exploitation du matériel Cisco et maîtriser l'exploitation des politiques de sécurité ainsi que la compréhension des différentes composantes d'une infrastructure informatique.

Nous avons également appris tout au long de ce projet à perfectionner notre sens relationnel dans un cadre professionnel. La mise en place ayant été faite dans un contexte de production avec un système bien fonctionnel, ceci nous a amené à côtoyer les responsables et managers de B2M et à mieux comprendre les contraintes liées à la continuité de services lors de la migration. De cette perspective, ce stage nous a été d'un grand apport sur le plan humain.

Il nous a offert l'opportunité de nous intégrer dans l'environnement de l'entreprise et d'améliorer nos capacités de communication, d'adaptation à la vie professionnelle et au travail en équipe.

Référence

[1] : http://www.qsp-systems.com/la-virtualisation-mode-demploi/

[2] : http://reseau-informatique.prestataires.com/conseils/virtualisation-quels-enjeux-entreprise

[3] : https://www.supinfo.com/articles/single/2351-differents-types-virtualisation

[4] : http://www.cours-informatique-gratuit.fr/facile/materiel/8.reseau-d-entreprise

[5] : http://www.inetdoc.net/articles/modelisation/modelisations.osi.html

[6] : https://isrdoc.wordpress.com/2010/11/16/les-reseaux-locaux-virtuels-vlan/

[7] : http://www.cisco.com/cisco/web/support/CA/fr/109/1092/1092443_21.html

[8] : http://testeur-wifi.com/le_commutateur_reseau.html

[9] : http://www.cisco.com/web/FR/products/routers/products.html#N280492

[10] : http://www.ocean-securite.com/audit-de-securite-en-entreprise-c9-p31.html

[11] : https://www.insight.de/fr/productinfo/server/0001121663

[12] : https://www.qnap.com/fr-fr/product/ts-231p

[13] : https://www.supinfo.com/articles/single/1993-installation-esxi-vcenter-une-ferme-serveur

[14] : https://fr.wikipedia.org/wiki/Windows_Server_2016

[15] : https://fr.wikipedia.org/wiki/Windows_Server_2012

[16] : https://fr.wikipedia.org/wiki/Active_Directory

[17] : https://fr.wikipedia.org/wiki/Microsoft_Exchange_Server

[18] : https://fr.wikipedia.org/wiki/Windows_Server_2012

[19] : https://fr.wikipedia.org/wiki/Microsoft_Dynamics_NAV

[20] : https://fr.wikipedia.org/wiki/Microsoft_SQL_Server

[21] : https://fr.wikipedia.org/wiki/Microsoft_Office_365

[22] : http://www.cyberoam.com/

[23] : http://www.cisco.com/

Glossaire

AD: **A**ctive **D**irectory

ADSL : **A**symmetric **D**igital **S**ubscriber **L**ine « liaison numérique asymétrique »

ARP : **A**ddress **R**esolution **P**rotocol « Protocole de Résolution d'Adresse »

ACL: **A**ccess **C**ontrol **L**ist

DHCP: Dynamic **H**ost **C**onfiguration **P**rotocol

DNS Domain **N**ame **S**ystem

DMZ : De**M**ilitarized **Z**one

ERP : Enterprise **R**esource **P**lanning « planification des ressources de l'entreprise »

FSI : Fournisseur de **S**ervice **I**nternet

GESS : Gérable, **E**volutif, **S**table et **S**écurisé

IT: Information **T**echnology

IEEE: **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers

IPS : Intrusion **P**revention **S**ystem « Système de Prévention des Intrusions »

ICMP: **I**nternet **C**ontrol **M**essage **P**rotocol

LAN: Local Area Network

MAC: **M**edia **A**ccess **C**ontrol « Adresse Physique »

ECP : Exchange Control Panel

CAS : Client Access services

NAC: Network Access Control

OSI: Open **S**ystems **I**nterconnection

OSPF: **O**pen **S**hortest **P**ath **F**irst

PoE: Power over Ethernet

QoS: **Q**uality **o**f **S**ervice

RC : Rez-de-**C**haussee

SSL : **S**ecure **S**ockets **L**ayer

SSII : **S**ociété de **S**ervices en **I**ngénierie **I**nformatique

SPOF : Single **P**oint **o**f **F**ailure « Point unique de défaillance »

SSICE : Sécurité des **S**ystèmes **I**nformatiques **C**ommunicants et **E**mbarqué

TCP : Transmission **C**ontrol **P**rotocol « Protocole de Contrôle de Transmissions »

UTM : **U**nified **T**hreat **M**anagement Gestion Unifiée des Menaces

VM : **V**irtuelle **M**achine

VLAN: **V**irtual **L**ocal **A**rea **N**etwork Réseau local Virtuel

VTP : **V**LAN **T**runking **P**rotocol

VPN : Réseau **P**rivé **V**irtuel

WAN : Wide area network

MIMO : Multiple-Input Multiple-Output

SQL : Structured Query Language

EDGE: Edge Transport server

Annexes

Annexe A : Configuration du switch

Utilisateurs

```
sh run
Building configuration...

Current configuration : 6465 bytes
!
! Last configuration change at 03:05:41 UTC Sat Apr 10 1993
by admin
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW-ACC-251
!
boot-start-marker
boot-end-marker
!
!
username admin privilege 15 password 0 NextStep*2017
no aaa new-model
system mtu routing 1500
vtp domain ICEM
vtp mode transparent
!
!
!
ip domain-name ICEM
!
crypto pki trustpoint TP-self-signed-2340971392
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2340971392
 revocation-check none
 rsakeypair TP-self-signed-2340971392
!
!
crypto pki certificate chain TP-self-signed-2340971392
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609
2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66
2D536967 6E65642D 43657274
  69666963 6174652D 32333430 39373133 3932301E
170D3933 30333031 30303031
  30345A17 0D323030 31303130 30303030 305A3031
312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469
66696361 74652D32 33343039
  37313339 3230819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281
  8100A74F A2E8364B EF4F041E 40DD8A4A E0C267E2
87ACC052 11277730 F6C68FB0
  C403F682 BD298DE2 24CB4218 77349561 DD6F0E89
7BF41B52 16EF634D A1037474
  D07DBF70 FE889A21 BE2BD4AD 7F17CAFA
E2D9522C C25D43D7 5357271D ED534876
  8C409F4C C27FCB4D 50ED8743 6654E8FF C76AE089
80349F45 8E75A250 21E12AB7
  5B570203 010001A3 53305130 0F060355 1D130101
FF040530 030101FF 301F0603
  551D2304 18301680 14395844 32C8547D 05441090
311CE3D3 EBA7388A 36301D06
  quit
```

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
 name users
!
vlan 20
 name serveurs
!
vlan 30
 name wifi-vip
!
vlan 40
 name wifi-data
!
vlan 50
 name wifi-guest
!
vlan 60
 name VL-T-MOBILE
!
vlan 70
 name VL-OUTSIDE
!
vlan 80
 name wifi-casque
!
vlan 99
 name MGMT
!
vlan 999
 name VL-NATIVE
!
!
!
interface Port-channel1
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/14
 switchport access vlan 10
switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

```
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/22
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/23
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/24
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface GigabitEthernet0/1
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode active
!
interface GigabitEthernet0/2
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
 channel-group 1 mode active
!
interface Vlan1
 no ip address
no ip route-cache
 shutdown
!
interface Vlan99
ip address 192.168.99.251 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.99.254
ip http server
ip http secure-server
!
no vstack
!
line con 0
 logging synchronous
 login local
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 logging synchronous
 login local
 transport input ssh
!
end
```

Annexe B : Configuration du switch Utilisateurs

```
sh run
Building configuration...

Current configuration : 6040 bytes
!
! Last configuration change at 08:19:17 UTC Sat Jul 7 2018
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW-SRV-253
!
boot-start-marker
boot-end-marker
!
!
!
username admin privilege 15 password 0 NextStep*2017
no aaa new-model
!
!
!
ip domain-name ICEM
vtp domain ICEM
vtp mode transparent
!
!
crypto pki trustpoint TP-self-signed-841539456
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-841539456
 revocation-check none
 rsakeypair TP-self-signed-841539456
!
!
crypto pki certificate chain TP-self-signed-841539456
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609
2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66
2D536967 6E65642D 43657274
  69666963 6174652D 38343135 33393435 36301E17
0D313731 31313131 36353434
  375A170D 32303031 30313030 30303030 5A303031
2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966
69636174 652D3834 31353339
  34353630 819F300D 06092A86 4886F70D 01010105
0003818D 00308189 02818100
  BB75D534 3B453D87 8C26BA26 8FEE06B1 4F14FB83
860A1F05 6B5F9C05 9896A7FB
  C4B8DEA1 90E88DF6 2B7EA45F DE228164 12C7A657
13F238CD 1C00B1C8 2B485D93
  E069EA17 EC98C769 A0D1EFE4 58EF53F8 9B060AB0
D9D190AC 1435ED78 8B3D1920
  A312AFD2 99ED32B4 A6777E82 0BE36BE0 81B9F4DD
7A849A64 8B564D9E C04D836B
  02030100 01A35330 51300F06 03551D13 0101FF04
05300301 01FF301F 0603551D
  23041830 16801446 C5233506 61D30297 29332714
9029E136 1D4F4830 1D060355
  1D0E0416 041446C5 23350661 D3029729 33271490
29E1361D 4F48300D 06092A86
  4886F70D 01010505 00038181 0019B15C 1F2B4383
554D721C 93BA293D 396EEEE9
  1E8E8B0B 0D6F0F01 37FE580D D7983733 058BA17C
3CF66F39 968360C0 585024E4
  quit
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 24576
```

```
vlan internal allocation policy ascending
!
vlan 10
 name users
!
vlan 20
 name serveurs
!
vlan 30
 name wifi-vip
!
vlan 40
 name wifi-data
!
vlan 50
 name wifi-guest
!
vlan 60
 name T-MOBILE
!
vlan 70
 name VL-OUTSIDE
!
vlan 80
 name wifi-casque
!
vlan 99
 name MGMT
!
vlan 999
 name VL-NATIVE
!
!
interface Port-channel1
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
!
interface Port-channel2
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
!
interface Port-channel3
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 description LINK TO PORT LAN FW
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate
 spanning-tree portfast
!
interface GigabitEthernet0/2
 description LINk TO ZONE GUEST FW
 switchport access vlan 50
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/3
 description LAG TO SW-ACC
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode active
!
interface GigabitEthernet0/4
 description LAG TO SW-ACC
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
 channel-group 2 mode active
!
```

```
interface GigabitEthernet0/5
 description LINK TO WLC PORT 1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface GigabitEthernet0/6
 description LINK tO PORT 2 WLC
 switchport trunk native vlan 99
 switchport mode trunk
!
interface GigabitEthernet0/7
 description LINK TO PORT D DMZ-FW
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/8
 description LIN TO SRV AD
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/9
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/10
 description LINK TO DVR
 switchport access vlan 70
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/11
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/12
switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/13
description LAG TO SW-ACC-251
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
 channel-group 3 mode active
!
interface GigabitEthernet0/14
 description LAG TO SW-ACC-251
 switchport trunk native vlan 999
 switchport mode trunk
 switchport nonegotiate
 channel-group 3 mode active
!
interface GigabitEthernet0/15
 switchport access vlan 70
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/16
 switchport access vlan 70
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/18
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/19
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/20
 switchport access vlan 10
 switchport mode access
!
```

```
interface GigabitEthernet0/21
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/22
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/23
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/24
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet0/25
!
interface GigabitEthernet0/26
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan99
 ip address 192.168.99.253 255.255.255.0
!
ip default-gateway 192.168.99.254
ip http server
ip http secure-server
!
!
!
!
line con 0
 logging synchronous
 login local
line vty 0 4
 logging synchronous
 login local
 transport input ssh
line vty 5 15
 logging synchronous
 login local
 transport input ssh
!
end

SW-SRV-253#ter
SW-SRV-253#terminal le
SW-SRV-253#terminal length 24
SW-SRV-253#
```