Table des matières

Table des Figures

Introduction Générale

Dans un monde connecté et ouvert, l'accès à l'information et aux ressources partagés ont créé une vulnérabilité dans les systèmes informatiques, d'où la nécessité de mettre en place des solutions convenables.

La mise en place d'une solution de sécurité informatique doit prendre en considération tous les paramètres, que ce soit matérielles, logicielles et même les ressources humaines.

Avoir un système informatique sécurisé et organisé rend le travail de l'utilisateur final et du gestionnaire plus rentable en termes de temps et de ressources, c'est dans ce contexte, que le projet de fin d'étude pour l'obtention de la License Appliquée en Sciences et Technologies de l'Information et de Communication que nous allons réaliser au Conseil de la Concurrence de Tunisie a pour sujet : « Mise en place d'une Solution de Sécurité Informatique ».

La possibilité d'exercer mes compétences m'a donné l'opportunité de faire les recherches et découvrir beaucoup dans le monde de la sécurité informatique.

Chapitre I : Présentation Générale

Introduction

Dans ce chapitre nous allons tout d'abord, présenter l'organisme d'accueil qui est le Conseil de la Concurrence (CC), puis, nous allons introduire le contexte de ce travail, la problématique et les grandes lignes du travail à réaliser.

I. Présentation de l'organisme d'accueil

Le CC est un établissement public a double rôle, rôle juridictionnel et consultatif, il agit et veille sur la bonne application du droit de la concurrence en Tunisie.

Le CC a été créé en 1995 grâce à la loi n°1995-42 du 24-4-1995 modifiant et complétant la loi n°1991-64 du 29-07-1991 relative à la concurrence et des prix et il est venu en remplacement de la Commission de la concurrence établie en 1991.

Aujourd'hui le CC est régi par la loi n°36-15 du 15 septembre 2015 relative à la réorganisation de la concurrence et des prix venant remplacer la loi de 1991.

Malgré que le législateur n'ait pas précisé la nature juridique du CC on peut en déduire, de la jurisprudence et de la doctrine, que c'est une autorité indépendante prononçant des jugements et ayant une fonction consultative.

L'organigramme du CC se compose de :

- Présidence du CC : Président et deux vice-présidents
- Rapporteurs : Rapporteur général et 15 rapporteurs
- Secrétaire Permanent :
  - Greffe : (Greffe Judiciaire, Greffe Consultatif)
  - Service Administratif
  - Service Financier
  - Service de la Documentation et de l'Informatique

L'organigramme peut être représenté comme suit :

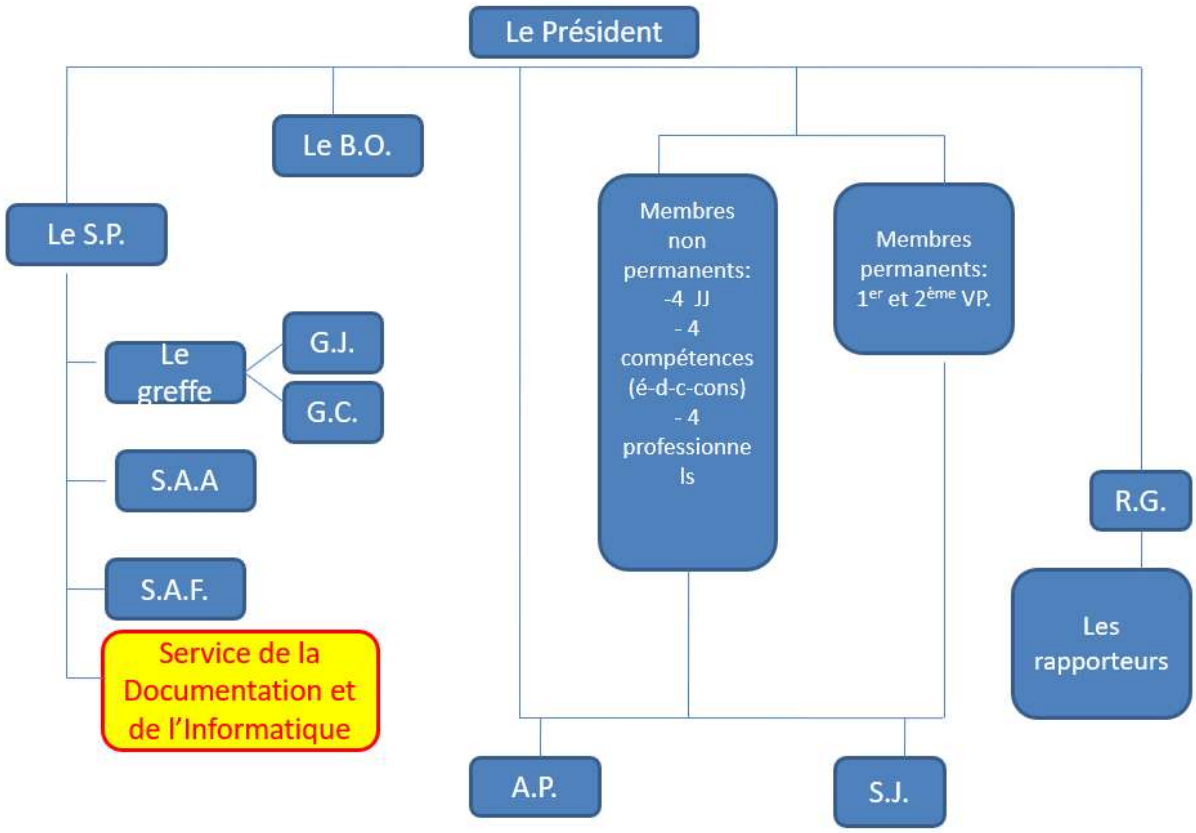


Figure I -1 Organigramme du Conseil de la Concurrence

Le service de la Documentation et de l'Informatique, dans son volet Informatique assure et réalise ces différentes tâches :

- Achats de matériel informatique : PC, Imprimantes, Toners, et accessoires informatiques, etc...
- Configuration et installation : Matériel informatique, Systèmes d'exploitation, etc...
- Administration Systèmes : Serveur de sauvegarde, Serveur Antiviral
- Administration Réseaux : Configuration ip (LAN, WAN, LS CNI)
- Assistance et Helpdesk : Accès à internet, utilisation des logiciels de bureautique (MS WORD, MS OUTLOOK), etc…

Toutes ces différentes tâches sont réalisées par un seul technicien que je suis. Accomplir ces tâches avec plus de célérité mais dans moins de temps et d'effort tout en garantissant un

système Informatique sécurisé et pertinent est le sujet de projet de fin d'étude : « Mise en Place d'une Solution de Sécurité Informatique ».

II. Contexte du projet

Ce projet de fin d'études entre dans le contexte de l'obtention de la Licence Appliquée en Sciences et Techniques de l'Informatique et de la Communication au niveau 3 et ceci en réalisant un projet fonctionnel dans le CC afin d'établir une stratégie de partage et de transfert sécurisé au sein du réseau informatique.

Un réseau informatique n'est pas plus qu'un ensemble de terminaux reliés les uns aux autres dans le but d'échanger des données d'une manière sûre, rapide et sécurisée. Pour assurer cet échange, nous devons avoir un système d'administration qui assure le partage et le transfert des données d'une manière automatique, fiable et sécurisée. Dans ce cadre se situe notre PFE qui consiste à mettre en place et configurer différents services open source pour assurer le contrôle des utilisateurs et le partage des ressources d'une façon qui respecte la hiérarchie de l'entreprise. De plus, nous allons s'intéresser à la sécurité des données contre les intrusions internes et externes qui peuvent attaquer nos ressources.

III. Problématique

Le réseau du CC manque de plusieurs éléments essentiels pour la bonne administration et la protection des différentes ressources, que ce soient matérielles ou bien logicielles, parmi lesquelles, on peut citer :

- Absence d'une séparation logicielle entre le réseau local (LAN) et le réseau internet (WAN) à part la séparation par défaut du fournisseur de services Internet (FSI).
- Absence de sécurité et de règles d'accès aux ressources et périphériques mis en réseau.
- Manque de stratégie de sécurité ce qui donne le droit à quiconque qui a le mot de passe pour se connecter à l'internet par wifi de voir, par simple scan du réseau, tous les postes de travail du réseau de l'entreprise.
- Les tâches d'administration des systèmes et des réseaux n'est pas centralisée puisque nous sommes sur un workgroup et non pas sur un domaine.

La prise en compte des problèmes évoqués précédemment a abouti à l'élaboration d'une solution d'administration que nous allons présenter ses buts dans la partie suivante.

IV. Travail à réaliser

Le réseau du Conseil de Concurrence présente plusieurs problèmes d'organisation et manque de serveurs et de services d'administration. Ainsi, afin de résoudre ces problèmes, il est primordial de munir ce réseau d'un serveur Linux pour profiter des services open source, et pour éviter les problèmes d'authentification des systèmes d'exploitation Windows.

Ensuite, nous allons passer à la mise en place et la configuration d'un ensemble de services pour assurer :

- La sécurité du système informatique
- La mise en place du domaine
- Le gestion centralisée des utilisateurs
- L'adressage IP automatique

Finalement, nous passons à la sécurisation du réseau de notre établissement contre les intrusions internes et externes par la mise en place d'une solution firewall pour la séparation de flux des données circulant dans le réseau. Ainsi, nous définissons une politique de sécurité qui protège les documents, les postes de travail et l'accès au réseau.

La mise en place de ces services permet la migration de notre SI de la gestion des différents composants de manière séparée et unique pour chacun des périphériques à la gestion centralisée et sécurisée de tous les périphériques du réseau.

Conclusion :

Dans ce chapitre, nous avons fait une présentation générale du cadre de projet en décrivant les problématiques et le travail à réaliser.

Le chapitre suivant, sera consacré à l'étude de l'existant, la critique de l'existant, ainsi que la présentation détaillée de la solution proposée.

Chapitre II :

Etude de l'Existant

Introduction

L'étude de l'existant constitue une étape préliminaire pour la réalisation d'une solution informatique. En effet, elle permet d'analyser, d'évaluer et de critiquer le fonctionnement habituel, tout en élaborant la liste de solutions possibles.

Ce chapitre sera réservé pour présenter l'étude préalable de notre projet. Nous commençons par une description détaillée du réseau actuel mis en place. Cette description nous mène à une analyse et une critique de l'existant. Enfin, nous proposons les différentes solutions aux problèmes soulevés.

I. Etude de l'Existant :

Le parc informatique du Conseil de Concurrence comprend les ressources matérielles et logicielles suivantes :

A. Ressources Matérielles

- 40 stations de travail (PC de bureau et PC portables)
- 03 Serveurs au format tour
- 05 imprimantes réseaux

B. Ressources Logicielles

- Une Solution de Sauvegarde et de backup : « URBackUP[i] » freeware et open source en mode Client/serveur
- Une Solution antivirale (Client/serveur)
- Une Application de Gestion de Stock (en mode monoposte)
- Une Application de Gestion des Biens (en mode connecté avec le CNI)

Nous notons aussi que 60 % des systèmes d'exploitation sont sous Windows XP que Microsoft ne supporte plus les mises à jour et les correctifs de sécurité.

C. Liaisons réseau et équipements d'interconnexion

- 01 Ligne ADSL de 20 Mb/s pour l'accès à internet.
- 01 Ligne spécialisée (en cour de migration vers la Fibre Optique) entre le CC et le Centre National de l'Informatique pour l'exploitation des applications (INSAF, ADEB, RACHED, etc..).

- 01 Ligne spécialisée entre le CC et le ministère du commerce pour l'accès à une base des données.
- 04 switchs de niveau, un dans chaque niveau (R+3)
- 02 Routeurs Cisco pour la liaison spécialisée (Une avec le CNI et une avec le ministère)
- Un modem ADSL en liaison avec l'Agence Tunisienne de l'Internet.

Pour mieux comprendre l'architecture du réseau existant dans notre organisme, nous avons résumé tout ce que nous avons décrit dans le schéma ci-dessous.

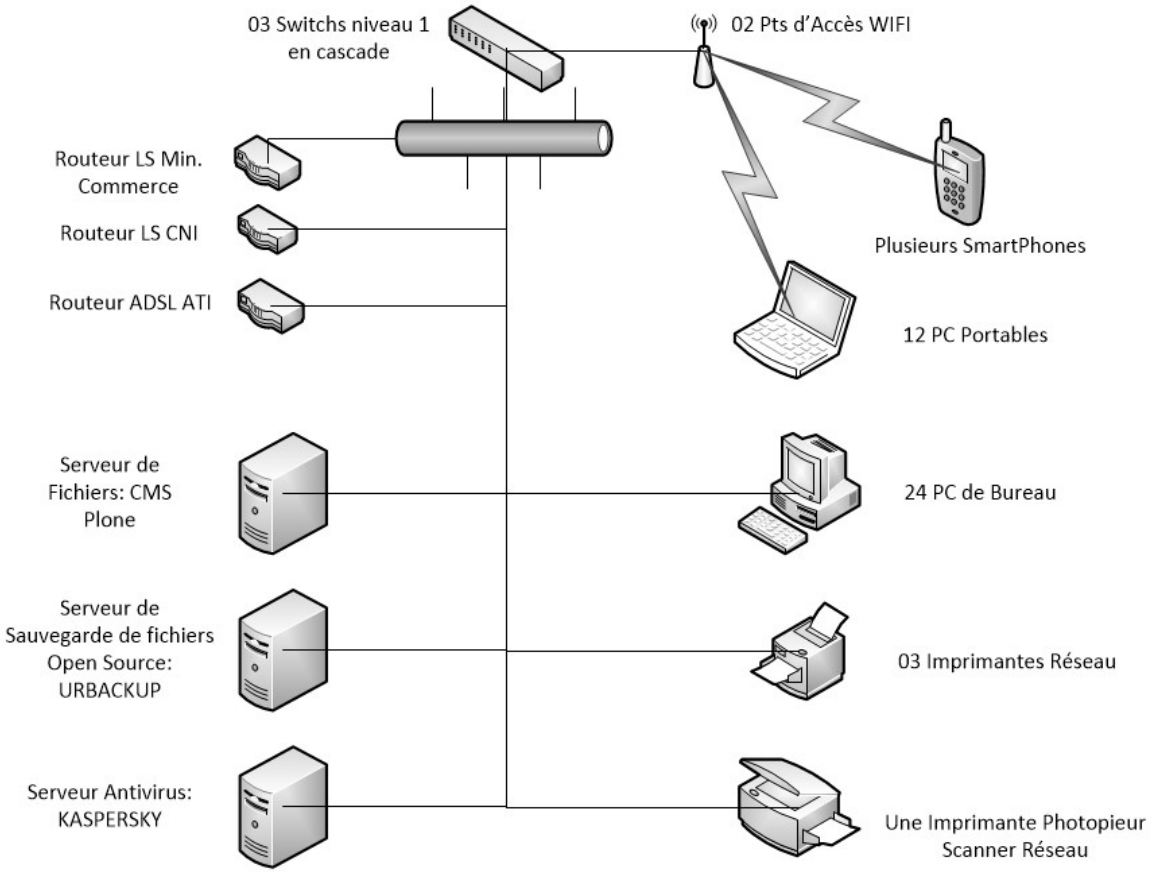


Figure II – 1 Architecture réseau initiale

D. Gestion des authentifications :

L'authentification au sein du système informatique du Conseil de Concurrence que ce soit au réseau ou bien aux terminaux tels que les PC n'est pas organisée ou bien centralisée, par exemple il suffit de brancher un câble réseau au PC pour avoir une adresse ip de la forme : 192.168.1.X/24 depuis la passerelle à l'internet de l'ATI ce qui permettra d'accéder au réseau local.

Du côté de l'authentification aux postes de travail et à l'ouverture de sessions, chaque utilisateur est administrateur sur son poste et n'est pas obligé d'utiliser un mot de passe.

Cependant, sur chaque PC, la session « Administrateur » est verrouillée par mot de passe et n'est utilisée que par l'administrateur système.

E. Politique d'accès aux ressources partagées

La politique d'accès aux ressources partagées n'est pas organisée ni par emplacement ni par droits, c'est-à-dire que tout utilisateur peut partager depuis son pc et toute personne ayant le chemin d'accès peut accéder aux ressources.

F. Politique d'accès des membres visiteurs

Il suffit d'avoir le mot de passe du wifi pour se connecter sur internet et l'accès à tout le réseau du CC devient possible et l'impression sur l'imprimante réseau est accordée.

G. Politique d'affectation des adresses IP

L'affectation des adresses ip se fait manuellement pour les postes de travail, ce qui oblige l'administrateur réseau de connaitre les adresses déjà attribuées pour éviter le conflit d'avoir la même adresse ip attribuée à deux périphériques.

H. Conditions de protection des ressources matérielles

Les ressources matérielles ne sont protégées ni contre l'accès malveillant, ni contre les dégâts et les accidents.

L'armoire principale qui contient les routeurs des trois lignes, les switchs en cascade, et les serveurs est placée dans un coin au Rez-de-Chaussée, près de l'entrée principale. Ce coin n'est pas fermé, en plus, il est à côté de la salle d'eau, par conséquent, une simple fuite d'eau peut présenter un risque majeur pour le matériel.

L'espace manque aussi d'aération et de système de détection d'incendies.

I. Politique de sécurité contre les accès ou attaques malveillantes (antivirus, ..)

Le système informatique du conseil de la concurrence comprend une liaison ADSL avec l'ATI ce qui rend tous les postes de travail connectés directement au modem sans un serveur mandataire ou une sonde de détection d'intrusion, seuls les firewalls personnels des systèmes d'exploitation ou bien l'antivirus peuvent protéger ces accès.

II. Critique de l'existant

Le système informatique du Conseil de Concurrence comprend plusieurs anomalies que ce soient en solutions de sécurité de réseau ou en solutions de gestion des utilisateurs. En effet :

- Le réseau LAN n'est pas protégé contre les intrusions du réseau WAN.
- L'absence d'une politique d'accès au réseau local et à l'internet rend le SI vulnérable et affecte négativement la bande passante ce qui induit à une lenteur remarquable lors de l'accès au réseau et aux documents partagés.
- Les utilisateurs internes peuvent, par mauvaise manipulation, infecter ou rendre l'accès impossible à tout le système informatique en absence d'une politique d'accès aux ressources partagées.
- Le réseau en workgroup et l'absence du domaine rend les tâches pénibles sur le pc et se font de façon indépendante pour chaque utilisateur.
- L'absence du serveur DHCP provoque des conflits d'adressage et interruption d'accès au réseau.
- L'absence d'une salle serveur dédiée, rend le matériel réseau et les serveurs vulnérables aux incidents d'inondation, d'incendies ou même au vol.

III. Solution proposée

Le but de notre projet est la mise en place d'une solution fiable pour l'administration du réseau de l'établissement et la résolution des problèmes déjà décrits dans la partie précédente. Les solutions proposées pour l'optimisation de l'administration du réseau, du matériel informatique et de la sécurité informatique sont les suivantes :

- Equiper le coin contenant le matériel réseau d'une porte pour interdire les accès, équiper la salle fermée de l'aération nécessaire ainsi qu'un capteur d'incendies et d'inondations.
- Mettre en place une solution jouant le rôle de firewall entre le LAN et le WAN et appliquant les règles d'accès préalablement définies selon le niveau de protection approprié.
- Migrer depuis le workgroup au domaine pour une administration système meilleure
- Mettre en place un serveur d'annuaire
- Mettre en place un serveur DHCP et un serveur DNS
- Mettre en place un serveur d'impression

Conclusion :

Dans ce chapitre nous avons présenté l'architecture existante dans notre établissement.

Par la suite, nous avons passé à une critique de l'existant. Finalement, nous avons proposé un ensemble de solutions pour la résolution de ces problèmes. Nous passons dans le chapitre suivant à l'installation de notre plateforme de travail ainsi que les services de base.

Chapitre III :

Choix de la plateforme matérielle et logicielle

Introduction

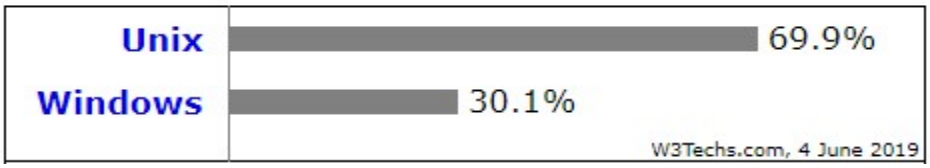
Dans la première partie de ce chapitre, nous allons détailler une comparaison entre les différents systèmes d'exploitation existants et choisir le meilleur entre eux. Par la suite, nous allons faire une présentation détaillée deux services réseaux à savoir : DNS (Domain Name System) qui assure la correspondance entre l'adresse IP et le nom de la machine et DHCP (Dynamic Host Configuration Protocol) qui permet la configuration dynamique des adresses IP. Cette partie nous permettra de justifier nos choix des plateformes et des services à installer.

I. Choix du Système d'exploitation

Le choix des systèmes d'exploitation représente un facteur très important pour la mise en place des solutions qui seront implémentées.

A. Comparaison Linux/Windows

Certes le nombre de systèmes d'exploitation les plus utilisés en stations de travail est très clair et favorise Microsoft Windows, mais du côté des serveurs la balance favorise les versions linux :



I - 1 Pourcentage des serveurs hébergeurs de sites web

L'utilisation des serveurs linux peut être expliquée par une comparaison du prix, de l'accès au code source, de l'accès au support technique, de l'évolution d'une version à l'autre, des compétences techniques nécessaires pour la mise en place et l'exploitation des services, comme indiqués dans le tableau comparatif ci-dessous :

OS	Coût	Code Source	Support	MAJ évolutive	Compétences technique
Windows	Payant (3000DT WinSRV 2016 16 cœurs)	Protégé	Microsoft + Communauté	Achat de nouvelle license	Pas très avancée
Linux	Gratuit	Ouvert	Communauté	Illimité	Très avancée

Tableau III - 1 Comparaison Windows / Linux

Nous remarquons ainsi que le système Linux répond à tous nos besoins en termes d'accès au code source, de gratuité de licence, et de disponibilité de la documentation. Toutefois, il nous reste à choisir une parmi ses distributions.

B. Les distributions Linux

Une distribution Linux, appelée aussi distribution GNU/Linux pour faire référence aux logiciels du projet GNU, est un ensemble cohérent de logiciels. La plupart étant logiciels libres, assemblés autour du noyau Linux. Il existe une très grande variété de distributions, ayant chacune des objectifs et des caractéristiques particulières.

Les versions linux comprennent une grande variété puisque le code source et ouvert, ce qui permet aux différents industriels ou communautés de le modifier suivant leurs besoins.

Parmi les distributions les plus populaires, on peut citer :

- RED HAT [ii]: version commercialisée la plus populaire
- Fedora : qui est soutenu par REDHAT
- Ubuntu : supporté par DEBIAN.
- Suse : développée par une société allemande

C. Comparaison Ubuntu/Fedora

Parmi les différentes distributions sous linux, les plus populaires en utilisation que ce soit pour les postes de production ou des serveurs, on peut retenir les deux distributions que nous allons comparer dans ce tableau, à savoir Ubuntu et Fedora :

OS	UBUNTU	FEDORA
Version Serveur	Ubuntu Server	Fedora Server
Licences logiciels	Logiciels gratuits et payants.	Logiciels gratuits seulement
Communauté et utilisateurs	Communauté large et grand nombre d'utilisateurs	Communauté réduite et nbre d'utilisateurs restreint
Gestionnaires de paquets d'installation	$apt ; $dpkg ;	$yum ; $rpm ;
Durée de support	5 ans	1 an

Tableau III - 2 Comparatif Ubuntu / Fedora

Ubuntu [iii]est une distribution qui propose un système libre, gratuit, sécurisé et convivial. Ce système est utilisable aussi bien sur des serveurs que des postes de travail. Il est toutefois orienté grand public notamment grâce à sa simplicité d'utilisation qui favorise la prise en main. C'est une distribution compacte (fréquemment distribué sur CD) qui assure une grande compatibilité matérielle et dispose de nombreux logiciels, de base ou à installer.

Fedora[iv] et anciennement Fedora Core, est une distribution GNU/Linux bâtie sur le système RPM, développée par le projet Fedora et soutenue par la société Red Hat. Cette distribution se veut être un système d'exploitation complet, composé uniquement de logiciels libres. Fedora dérive donc de la distribution Red Hat Linux, et est destinée à l'expert plus tôt que les débutants ou les généralistes. Le maintien de Fedora est en grande partie redevable à sa communauté d'utilisateurs.

Cette distribution se distingue par le très grand nombre d'architectures supportées, son importante logithèque et par son cycle de développement relativement long, ce qui lui confère un gage d'une certaine stabilité. Sa qualité et son sérieux sont unanimement reconnus, mais elle garde l'image d'une distribution réservée aux experts, malgré que son ergonomie a beaucoup évolué.

Nous pouvons retenir que la distribution Ubuntu de linux est plus stable que celle de Fedora et qu'elle comprend une communauté et des forums d'entre-aide plus large que celle de la distribution de Fedora.

II. Le Service FireWall

A. Présentation du service firewall

Le firewall est une entité du système informatique qui contrôle le transfert de données en entrée et sortie suivant des règles bien définies.

Il y a deux types de firewall : le firewall système et le firewall réseau.

Le firewall système se contente de contrôler le flux et appliquer les règles seulement au niveau de l'unité centrale ou il est installé, tandis que le firewall réseau agit comme une passerelle entre deux réseaux en appliquant des règles prédéfinies par l'administrateur.

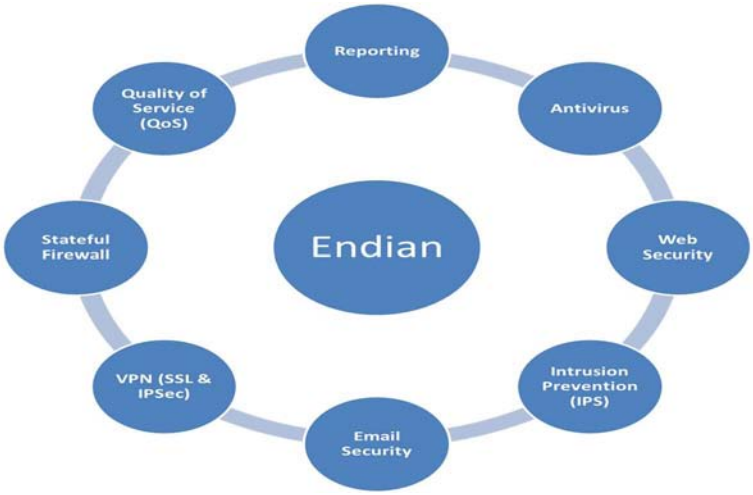
B. Choix du firewall

Pour le choix du firewall pour notre SI nous allons opter pour une solution freeware pour des raisons de coût en plus et puisque nous avons des difficultés à acquérir un serveur, nous allons adapter et recycler une ancienne machine de notre parc informatique qui est la « Fujitsu Siemens Esprimo P2510 » équipée d'un microprocesseur « intel dual core », que nous avons pu rassembler 2 Go de mémoire vive, et deux cartes réseaux extensibles à part la carte réseau intégrée.

Du coup, et vu la configuration matérielle nous avons choisi l'utilisation d'une architecture : « software appliance » : c'est-à-dire, pour des performances optimales du hardware, il n'est pas nécessaire d'installer tout un système par exemple UBUNTU SERVER 18 avec tous les services, mais le système sera optimisé pour intégrer la solution firewall et seulement les services indispensables au fonctionnement du firewall qui seront retenus et comme ça nous aurons un système léger qui ne fait tourner que le firewall.

La solution que nous avons choisie est : ''ENDIAN UTM SOFTWARE APPLIANCE[v]''

Cette solution de gestion de menaces unifiée (UTM : Unified Threats Management) englobe plusieurs fonctionnalités comme indiquée dans ce schéma :



II - 2 Fonctionnalités de l'UTM ENDIAN

Figure III.1 : Schémas des fonctionnalités de ENDIAN UTM

Ci-dessous un tableau indiquant la configuration minimale requise pour cette solution :

System Requirements	
CPU	Intel x86_64 compatible / 1GHz minimum (Dual-core 2 GHz recommended)
□Multi-Processor	Symmetric multi-Processor (SMP) support included
RAM	2 GB minimum (4 GB recommended)
Disk	SCSI, SATA, SAS or IDE disk is required (8GB minimum 20GB recommended)
Software RAID	For software RAID1 (mirroring) two disks of the same type are required (capacity can be different)
Hardware RAID	SCSI and SAS RAID systems and controllers are supported
CD-ROM	An IDE, SCSI or USB CDROM drive is required for installation (not required after installation)
Network Cards	Most common Network Interface Cards are supported including Gigabit and fiber NICs
Monitor Keyboard	Only required for the installation but not for configuration and use
Operating System	Endian UTM includes a Hardened Linux-based Operating System

Figure III - 3 Caractéristiques minimales requises pour héberger ENDIAN

Pour la mise en place d'une solution de sécurité complète dans un SI, quelques services doivent être présents, tels que : le service DNS, le service DHCP, un annuaire comprenant la liste des utilisateurs pour faciliter leur gestion et un domaine ce qui nous donnera le schéma suivant :

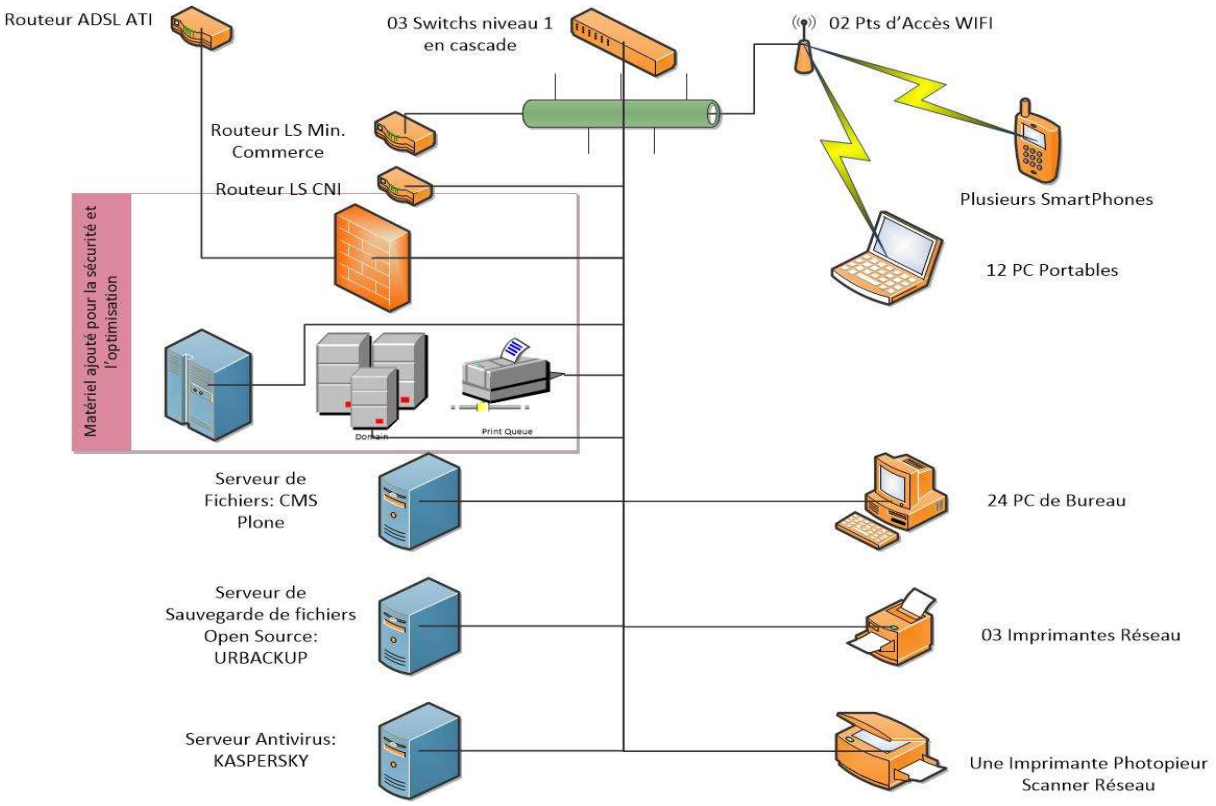


Figure III - 4 Architecture réseau optimisée

III. Le service DNS

Le service DNS (Domain Name System) est le service de correspondance entre le nom des machines et leur adresse ip. Ce service facilite la reconnaissance des destinataires en enregistrant leurs adresses ip dans un fichier disponible en consultation pour les clients.

IV. Le service DHCP

Le service DHCP (Dynamic Host Configuration Protocol) est destiné à l'attribution automatique des adresses ip aux terminaux d'un réseau.

La solution ENDIAN et comme tous les firewalls des 3ème génération ou NGF (Next Generation Firewall) contient un service DHCP intégré.

V. Le service d'annuaire

Le service d'annuaire comme AD (Active Directory) de Microsoft ou bien openLDAP qui est une solution libre qui sert à organiser hiérarchiquement les unités informatiques telles que des

machines, des utilisateurs, des services, pour les utiliser et faciliter la gestion et l'administration au sein du réseau.

Conclusion :

Dans ce chapitre nous avons fait la comparaison entre les systèmes d'exploitation et les solutions de sécurité qui conviennent à notre système informatique.

Par la suite, nous allons passer à la mise en place de la sécurité envisagée pour obtenir un SI plus sécurisé et centralisé comme défini précédemment dans la figure ci-dessus.

Chapitre IV :

Mise en place et configuration de la solution de sécurité

Introduction

Dans ce chapitre nous allons mettre en place une solution de sécurité FireWall puis nous allons mettre en œuvre un serveur Ubuntu Server 18.04.2 qui va jouer le rôle d'un contrôleur de domaine AD avec SAMBA qui va assurer l'échange entre les deux environnements Windows et Linux.

I. Mise en place de la solution

Tout d'abord nous allons commencer par l'installation de la solution firewall ENDIAN sur la machine dédiée et précédemment définie :

A. Installation de la solution FireWall

1. Installation de l'UTM ENDIAN

Au démarrage de la machine, après le boot sur le support comprenant l'image iso de l'Appliance software qui est disponible au téléchargement gratuitement à travers son site web officiel.

Nous avons cette interface :

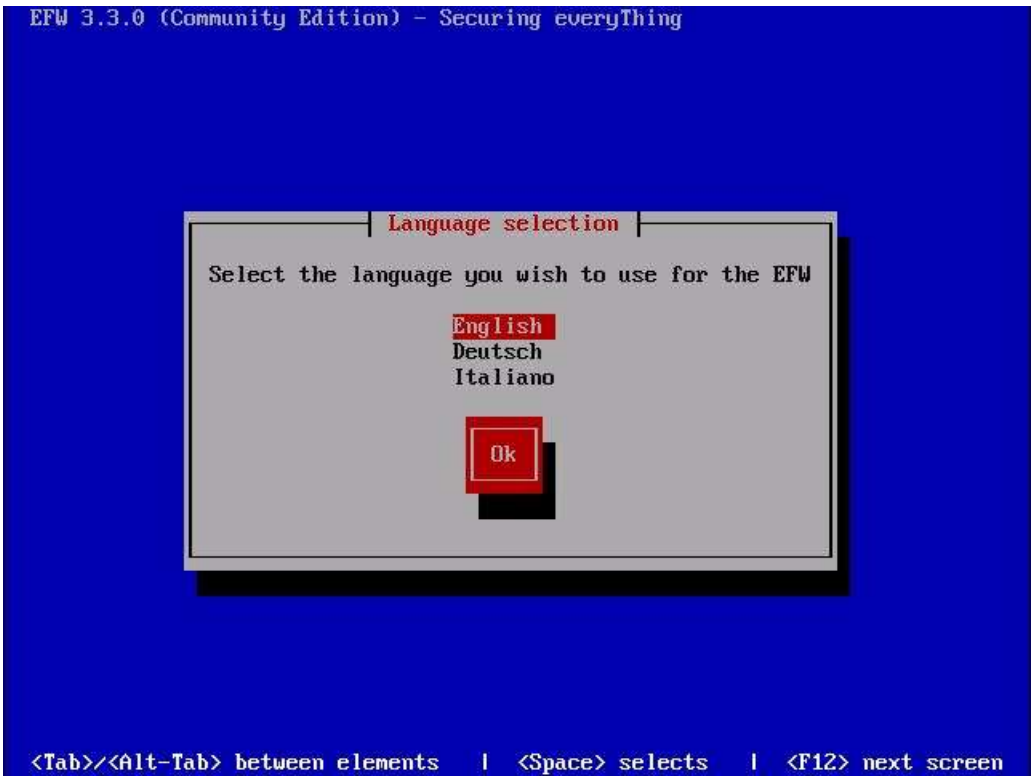


Figure IV – 1 Interface d'installation de l'UTM ENDIAN

Le 1er écran de l'installation vous prompt pour choisir la langue d'installation, nous avons trois choix comme indiqués ci-dessus.

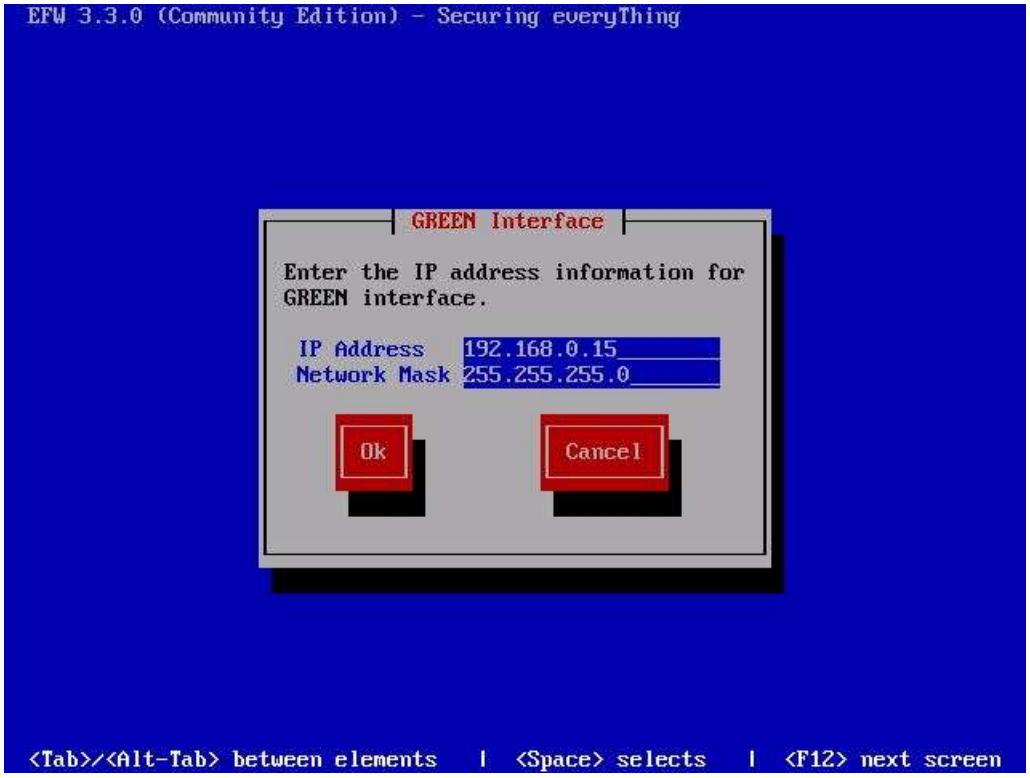


Figure IV - 1 Interface de configuration réseau de l'UTM

Puis, au cours de l'installation qui ne prends pas trop de temps, nous sommes invités à définir la première interface réseau (GREEN) celle du réseau local. Pour ce faire, nous avons choisis la dernière adresse de la plage : 192.168.0.15.

Figure IV - 2 Interface de finalisation de l'installation

A la fin, un message de succès de l'installation, suivi du redémarrage donne cette interface :

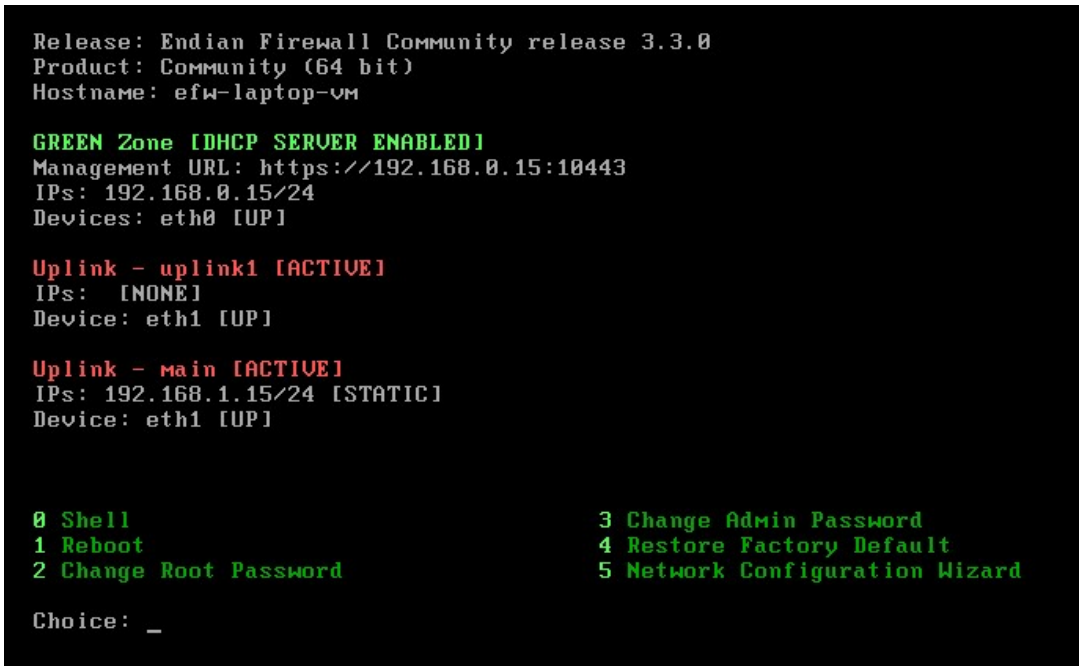
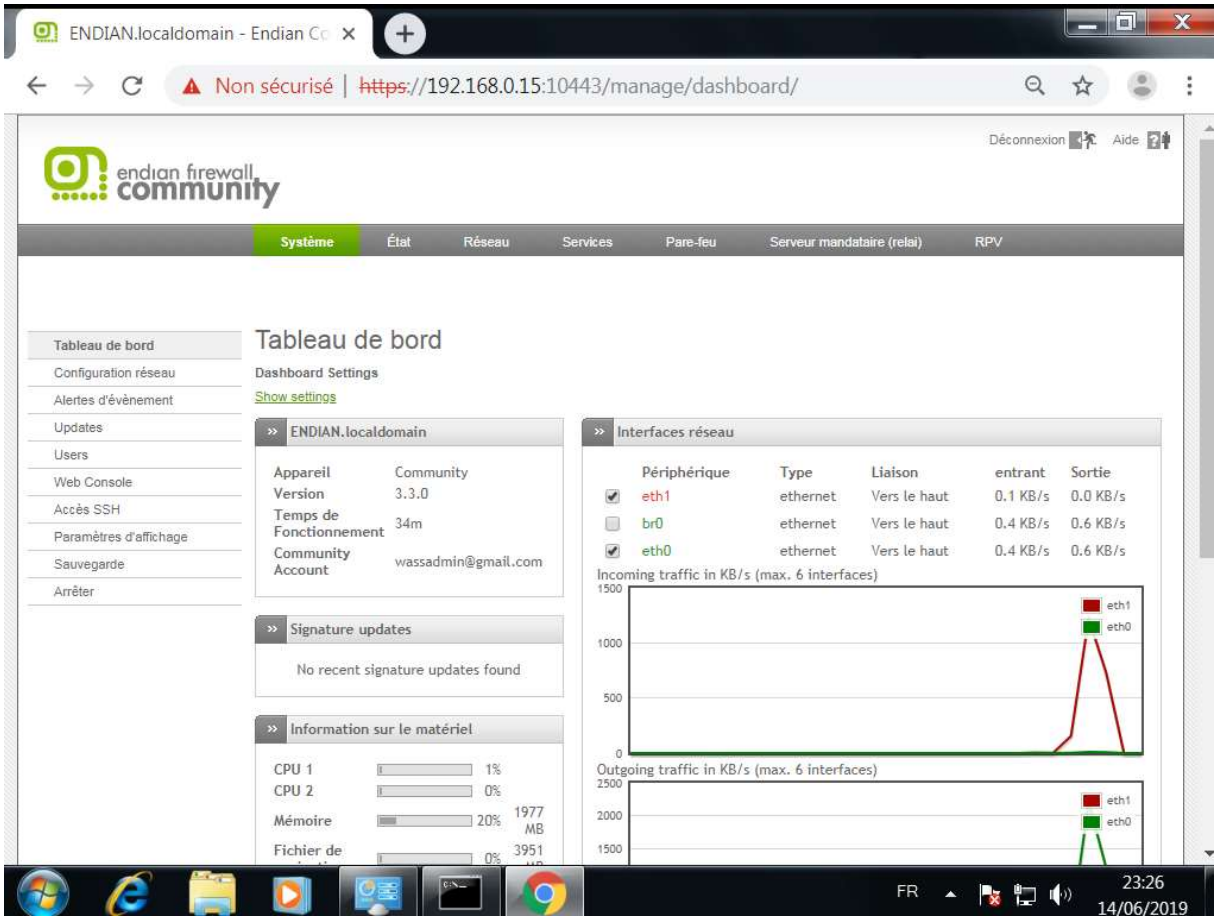
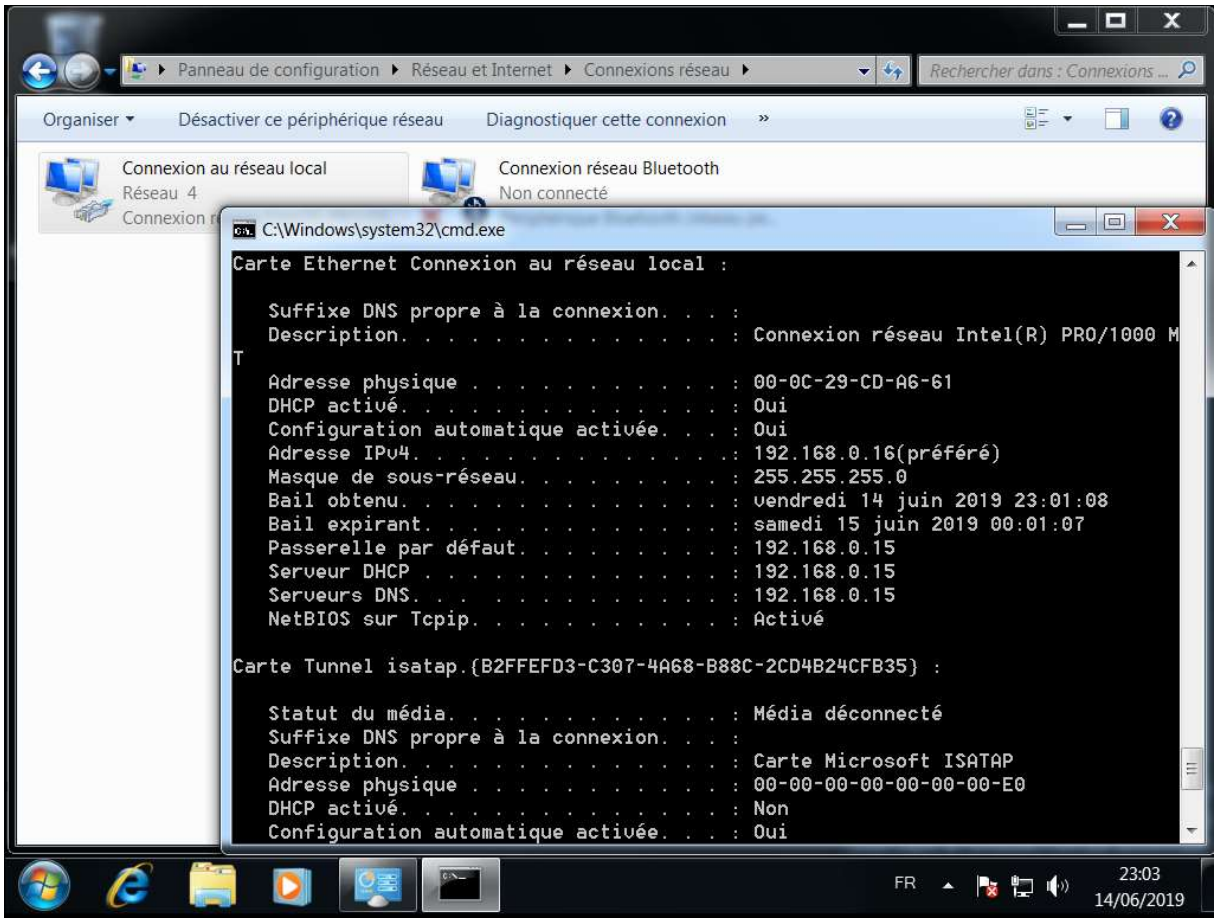


Figure IV - 3 Console d'administration du FireWall

Cette interface permet la configuration classique des interfaces réseau du serveur, cependant l'interface avancée du firewall est accessible à travers le navigateur via le protocole sécurisé https et le port : 10443



0- 4 Interface web avancée d'administration de l'UTM ENDIAN



0 - 5 Connexion d'un poste client au FireWall

Une machine sous windows 7 configuré à acquérir une adresse dynamiquement, le firewall qui a l'adresse ip : 192.168.0.15 lui attribue l'adresse ip 192.168.0.16 avec succès.

2. Mise en place du Proxy-Cache

Le proxy est un service intermédiaire entre un client et un serveur qui sert à relayer les requêtes.

Grâce à son emplacement, un serveur proxy peut être utilisé de différentes manières et pour des raisons différentes, par exemple :

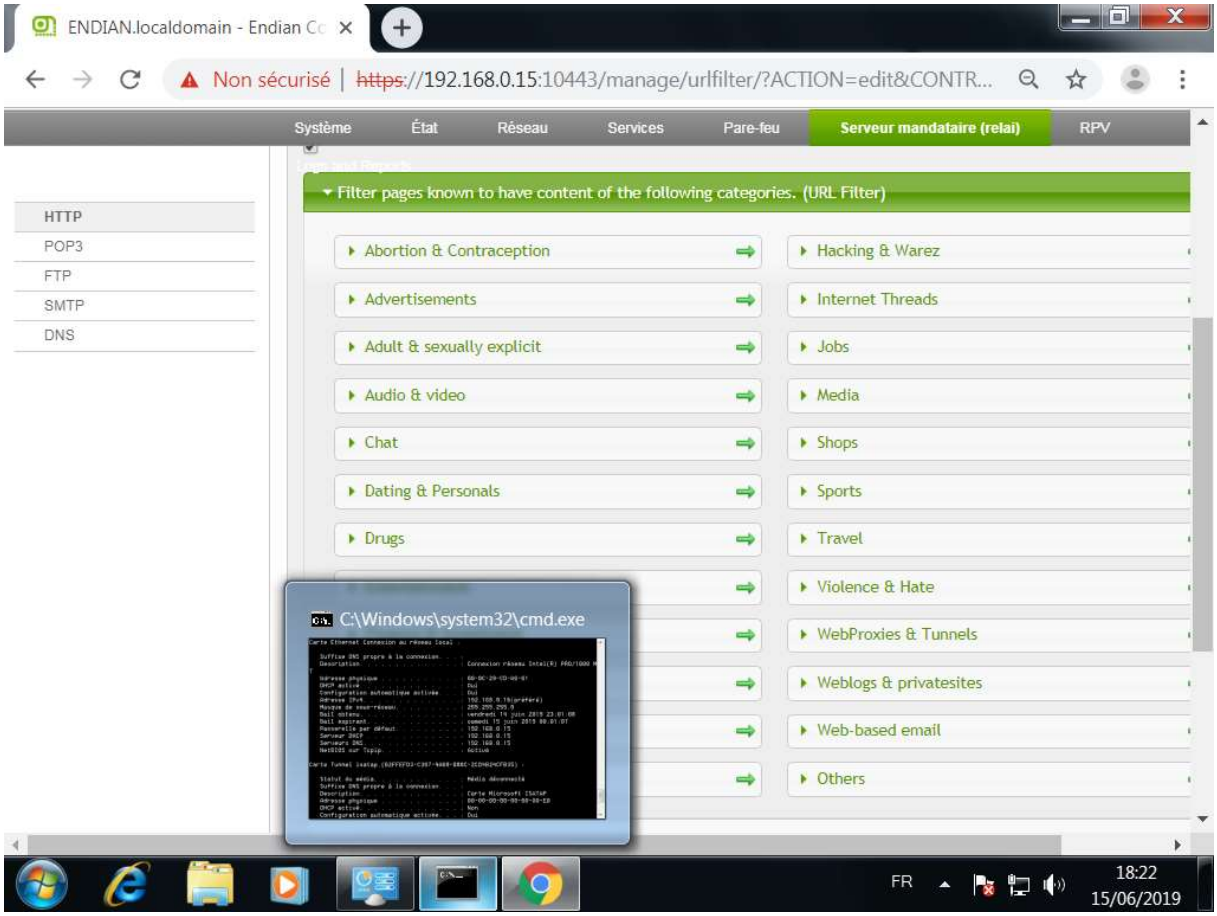
- Une accélération de la navigation grâce au cache : Les données qui ont été téléchargés depuis internet par un poste client X et suivant des paramètres bien définies telles que la taille, la date d'expiration, le type, restent sauvegardées sur le disque du serveur et

ceci pour ne pas les télécharger une deuxième fois par un poste Y ce qui donne une rapidité d'accès.

- Une journalisation des connexions : Les connexions aux sites distants ou fichiers partagés en internes sont enregistré sur un fichier log
- Une sécurité du réseau par authentification : l'accès peut être par authentification, cette authentification peut être faite par différentes applications telles que les navigateurs web
- Un filtrage d'accès web : sert à contrôler l'accès aux sites web inutiles qui peuvent apporter des virus ou user de la bande passante du réseau.

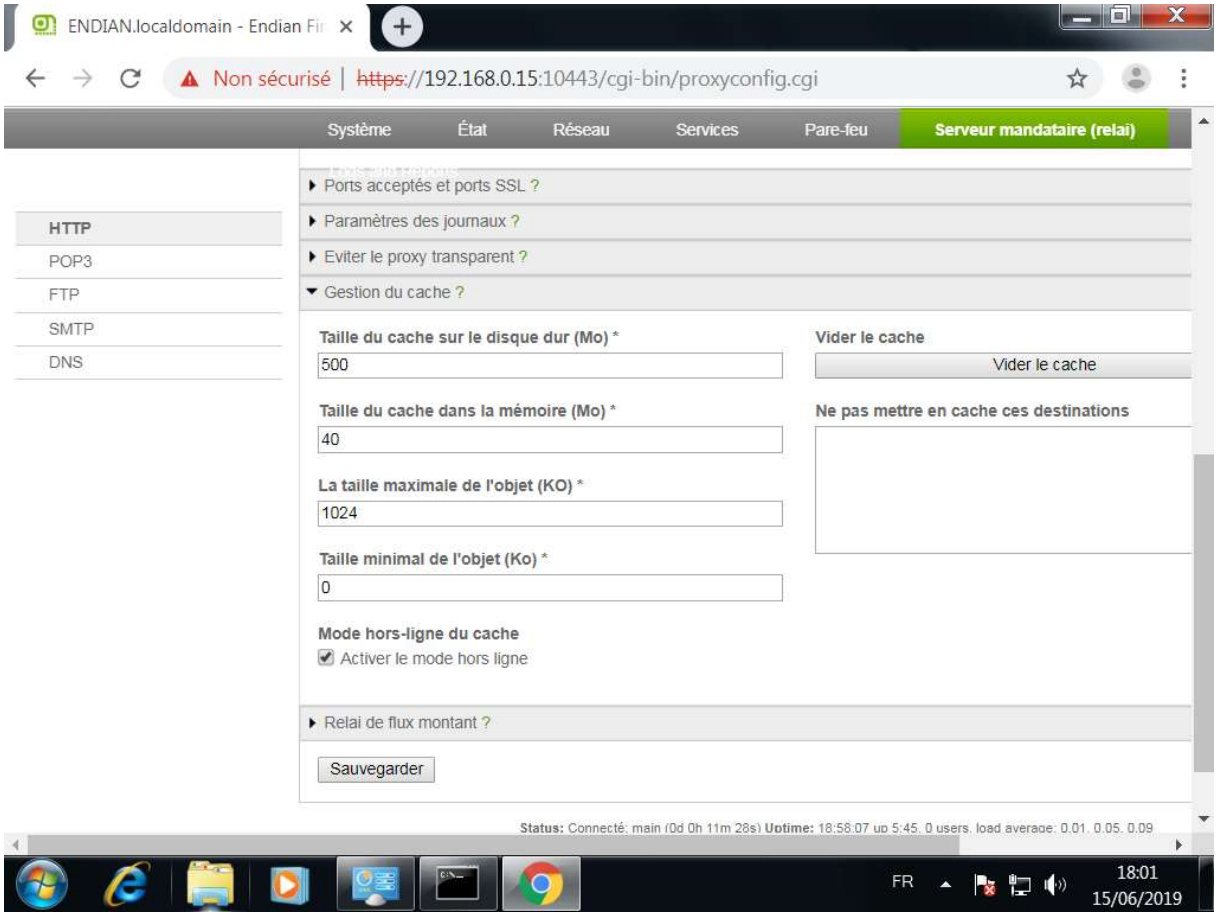
Dans notre cas, nous allons utiliser le proxy pour deux raisons : filtrage d'accès web et proxy-cache pour fournir une navigation internet plus rapide.

Le filtrage d'accès par ENDIAN se fait comme suit :



0 IV - 6 Interface de filtrage web

ENDIAN UTM a le service proxy-cache intégré et on peut l'activer et le paramétrer comme suit :



0 IV - 7 Paramétrage du proxy

B. Installation du Serveur DE DOMAINE

L'utilisation d'un domaine fournit une administration centralisée des utilisateurs, des ressources partagées : imprimantes, dossiers..., configurations réseaux : adressage, dns…

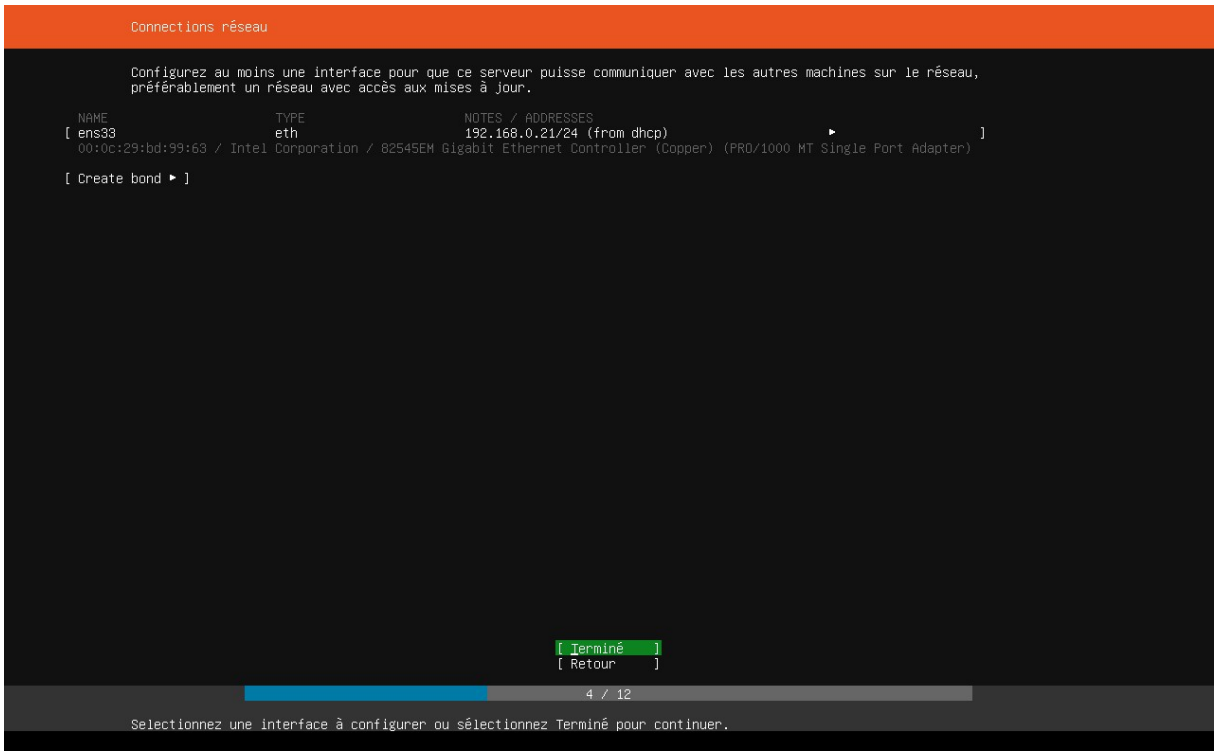
L'administration d'un réseau informatique sera plus facile en utilisant un domaine à la place du workgroup. En workgroup pour changer n'importe quel paramètre du poste client du réseau, il faut répéter la même tâche tant de fois que de postes, imaginez le cas dans grand réseau et d'une étendue géographique énorme le temps qu'il faut gaspiller pour changer une modification.

1. Installation du Serveur

Pour avoir tous ces services, nous avons besoin d'un système d'exploitation serveur comme UBUNTU SERVER 18.04.2. Ci-après la démarche de l'installation :

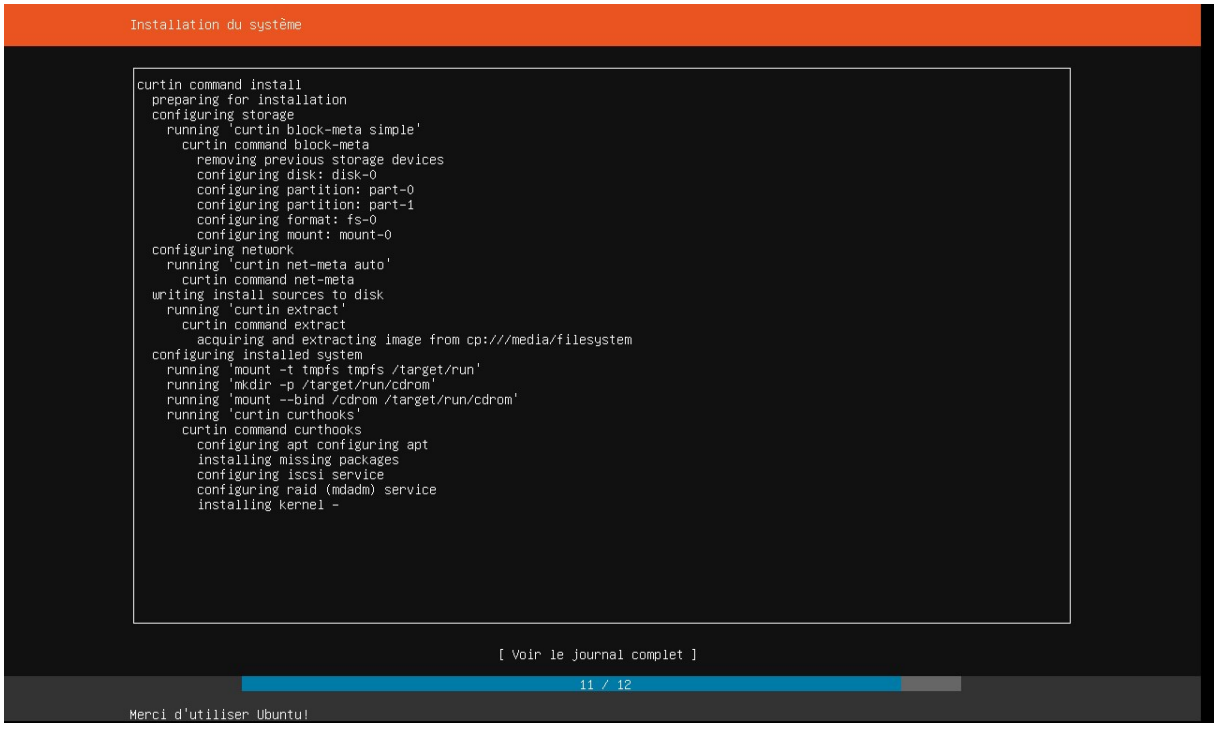
En bootant sur le disque d'installation que nous pouvons télécharger l'image iso à depuis la source officielle[vi], nous aurons la main pour choisir la langue système puis la disposition du clavier, puis trois modes d'installation, deux modes du cloud et un mode standard, pour notre cas nous allons faire une installation standard.

Puis le paramétrage réseau, puisque l'UTM ENDIAN fournit un service DHCP, le serveur domaine bénéficiera d'une adresse dynamique tel que :



0 - 8 Configuration de l'adresse réseau du serveur Ubuntu

L'installation du serveur se fait sans erreurs.



0-9 Processus d'installation du serveur Ubuntu 18.04.2

Il ne reste plus que d'installer les différents services tels que le service d'annuaire, le serveur DNS et le serveur d'impression dans ce qui va suivre.

2. Installation de SAMBA et Domaine

Le service d'annuaire est une base de données hiérarchique des entités qui représentent un système informatique qui est consultable par les membres du domaine suivant des règles.

Parmi les annuaires les plus connus on peut citer AD (Active Directory) de Microsoft.

L'architecture des SI des systèmes d'exploitation de la majorité des postes de travail du CC est sous Microsoft Windows, d'où la nécessité d'utiliser un annuaire qui est consultable facilement sur l'environnement Windows.

Pour cette raison, nous avons choisi SAMBA[vii] qui est à la base un projet soutenu par Microsoft et surtout avec sa version 4 qui inclut : DNS (Domain Name Server), LDAP (LightWeight Directory Access Protocol), Kerberos (le protocole d'authentification), GPO (Group Policy Object), NTP (Network Time Protocol), et d'autres services…

A. Avant l'installation de SAMBA

Avant de commencer l'installation, nous devons préciser les paramètres du domaine que nous allons créer puisque nous aurons besoin de les mettre en paramètres :

- Les paramètres :

Paramètre	Valeur
Realm	CCT.GOV
Domain	CCT
Server Role	DC (contrôleur de domaine)
DNS backend	SAMBA_INTERNAL
DNS forwarder IP address	none

Tableau IV - 1 Paramètres du Contrôleur de domaine

Le fonctionnement d'Active Directory nécessite une grande synchronisation entre les clients et le DC (Domain Controller), la synchronisation est faisable grâce au protocole NTP.

- Mise en œuvre du protocole NTP :

Installation du service :

```
# apt-get install ntp
```

Pour vérifier l'état du service :

```
# service ntp status
```

ce qui donne :

```
root@cctdcserver:~# service ntp status
● ntp.service - Network Time Service
   Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2019-06-17 11:18:24 UTC; 45s ago
     Docs: man:ntpd(8)
 Main PID: 2236 (ntpd)
    Tasks: 2 (limit: 2290)
   CGroup: /system.slice/ntp.service
           └─2236 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 112:115
```

- Configuration adressage ip :

Certes, la configuration réseau allouée au début grâce au protocole DHCP, mais pour les serveurs, il est préférable d'avoir un adressage statique. C'est pour ça que nous avons choisi d'attribuer l'adresse ip : 192.168.0.14 au serveur « cctdcserver », et ceci n'est pas avec à travers les anciens fichiers sous :

```
/etc/network/intefaces
```

Néanmoins, depuis la version 18 d'Ubuntu server, la configuration réseau se fait avec « netplan » sous :

```
/etc/netplan/*.yaml
```

Nous obtenons ainsi le fichier suivant :

```
# This file is generated from information provided by
# the datasource.  Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        ens33:
            dhcp4: false
            addresses: [ "192.168.0.14/24" ]
            gateway4: 192.168.0.15
            nameservers:
                addresses: [ "192.168.1.1", "8.8.8.8" ]
    version: 2
```

En plus le test du service réseau ne se fait plus grâce à l'ancienne commande :

 # service network status/start/stop/restart

Mais grâce à la commande :

 # service networking start

Ce qui donne :

```
root@cctdcserver:~# service networking
force-reload  reload        restart       start         stop
root@cctdcserver:~# service networking restart
root@cctdcserver:~# service networking reload
 * Reloading network interfaces configuration...                                [ OK ]
root@cctdcserver:~# service networking start
root@cctdcserver:~# _
```

A. Installation de SAMBA

Avant l'installation de SAMBA ou de n'importe quel package, il est préférable de faire la mise à jour des packages et des dépendances déjà installées et ceci grâce aux commandes :

 # apt update et *# apt upgrade*

Puis l'installation de SAMBA se fait avec la commande :

 # apt install samba

La vérification des packages de SAMBA installés se fait avec la commande :

 # whereis samba

Ce qui donne le résultat :

```
root@cctdcserver:~# whereis samba
samba: /usr/sbin/samba /usr/lib/x86_64-linux-gnu/samba /etc/samba /usr/share/samba /usr/share/man/ma
n7/samba.7.gz /usr/share/man/man8/samba.8.gz
root@cctdcserver:~# _
```

B. Configuration du DC (Contrôleur de domaine) grâce à SAMBA :

Maintenant que SAMBA est correctement installée, nous allons paramétrer le domaine grâce à la commande suivante et avec les paramètres suivants :

 # samba-tool domain provision --use-rfc2307 -interactive

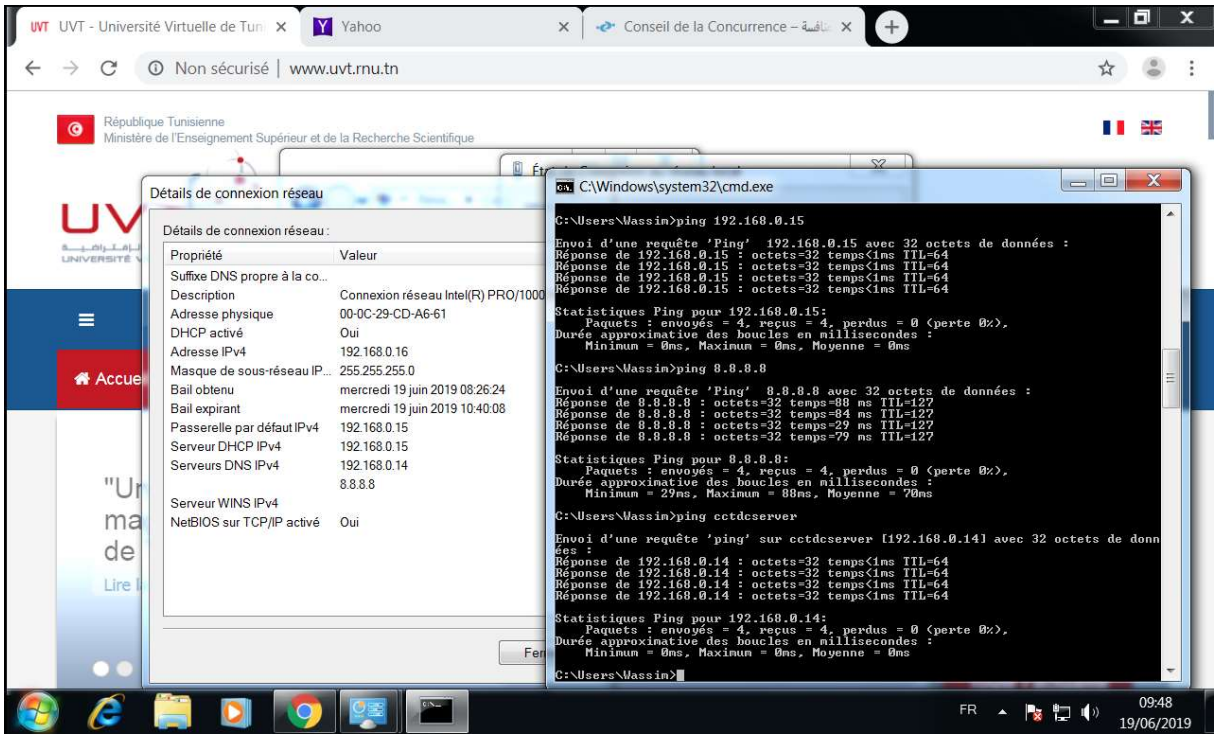
Et appliquant les paramètres cites dans le tableau précèdent, le succès du paramétrage donnera ceci :

```
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=cct,DC=gov
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=cct,DC=gov
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba AD has been generated at /var/lib/samba/private/krb5.con
f
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              cctdcserver
NetBIOS Domain:        CCT
DNS Domain:            cct.gov
DOMAIN SID:            S-1-5-21-2735544158-3251299587-3027047190

root@cctdcserver:~# _
```

B. Test DNS AD-SAMBA

En configurant un poste client sous « windows 7 » en DHCP pour l'attribution de l'adresse ip et l'accès à internet depuis le firewall, puis, en paramétrant le champ : Premier serveur DNS de la carte réseau sur l'adresse ip du serveur de domaine nous aurons ce résultat :



0- 10 Poste Client au FireWall et au Contrôleur de domaine

Conclusion

A travers ce chapitre, nous avons pu mettre en place un serveur de domaine qui jouera le rôle de contrôleur de domaine. L'administration des utilisateurs, des groupes et des politiques d'accès ont rendu l'administration plus organisée.

Conclusion Générale

De nos jours, le monde évolue et surtout les technologies, de plus en plus de gadgets sont connectés à la maison comme au travail, en plus dans beaucoup de cas on ne peut isoler les services et les terminaux de travail de ceux personnels ; Et avec cette évolution, les menaces des attaques informatiques et de la cyber criminalité sont toujours en avance d'un cran à la recherche des failles qui touchent à la fois les données et périphériques personnelles que professionnelles.

Sachant qu'en Tunisie, 24% des travailleurs pensent que la protection de leur vie privée en ligne est portée sur l'employeur.[1]

C'est un défi que nous avons remporté en donnant à notre établissement un environnement informatique plus sécurisé et organisé et à pouvoir travailler et accomplir nos devoirs de façon centralisée et confortable.

[1] Page 42 de l'enquête la plus vaste menée par Ipsos dans plus de 24 pays (America, Africa, Europe, Asia): http://bit.ly/2KWXycH CIGI-Ipsos 2019.

ملخّص

تعتبر التقنيات الحديثة من أبرز مؤشّرات التطوّر الاقتصادي وتطوّر الادارة وتمثل حماية الأنظمة والشبكات التحدّي الحقيقي الذي يتحتّم علينا رفعه خصوصا مع الطفرة التكنولوجية التي نعيشها. يندرج مشروع ختم الدّراسات في هذا الإطار بتحويل النظام المعلوماتي لمجلس المنافسة محميّا أكثر الكترونيا ومنظّما باستعمال وسائل الحماية الموحدة بنظام "انديان".

كلمات مفاتيح: حماية الأنظمة والشبكات الإعلامية، جدار ناري الكتروني، "انديان".

Résumé

Les nouvelles technologies sont considérées l'indice d'évolutions de l'économie et de l'administration, et la sécurité des systèmes et des réseaux informatiques représentent un défi que nous devons remporter surtout à l'ère de la révolution numérique que nous assistons. Dans ce cadre notre projet de fin d'études nous avons visé à transformer le système informatique du Conseil de la Concurrence plus organisé et sécurisé en mettant en place une solution de sécurité unifiée basée sur l'UTM ENDIAN.

Mots clé : Sécurité des systèmes et des réseaux informatiques, Pare-feu électronique, ENDIAN UTM.

Abstract

The new technologies are the ecoconomic and administrative power signs. Securing networks and systems is the challenge we have to gain in this IT revolution era. In this context, our end study project goal is to improve the Competition Council's information system by implementing a security system using the unified threats management solution ENDIAN.

Keywords : System and network security, FireWall, ENDIAN UTM

Webographie

[i] Site officiel de la solution de backup : www.urbackup.com

[ii] Site officiel de RedHat : www.redhat.com

[iii] Site officiel d'Ubuntu : www.ubuntu.com

[iv] Site officiel de Fedora Project : https://getfedora.org

[v] Site officiel de la solution ENDIAN : www.endian.com

[vi] Source officielle de téléchargement d'ubuntu server 18 : http://releases.ubuntu.com/18.04/ubuntu-18.04.2-live-server-amd64.iso

[vii] Projet SAMBA : https://www.samba.org/