TABLE DES MATIERES

TABLE DES FIGURES

TABLE DES TABLEAUX

Acronymes

A	**AP**	Access Point
	ARP	Address Resolution Protocol
	ATI	Agence Tunisienne d'Informatique
B	**BRAS**	Broadband Remote Access Server
	BIRUNI	BIbliothèque des Ressources UNIversitaires
C	**CCK**	Centre Calcul Khawarizmi
	CEI	Concept Européen Informatique
	CEREP	CEntre de REcherche en Productique
	CERT	Centre d'Etudes et de Recherche des Télécommunications
	CMO	Chimie Moléculaire Organique
	CNI	Centre National d'Informatique
	CPE	Customer Premises Equipment
	C3S	Commande Surveillance et Sûreté des Systèmes.
D	**DHCP**	Dynamic Host Configuration Protocol
	DMMP	Dynamique Moléculaire et Matériaux Photoniques
	DNS	Domain Name Server
E	**ENSIT**	Ecole Nationale Supérieure d'Ingénieurs de Tunis
	ERP	Enterprise Resource Planning
F	**FO**	Fibre Optique
	FTP	File Transfer Protocol
H	**HTTP**	HyperText Transfer Protocol
I	**ICMP**	Internet Control Message Protocol
	IDS	Intrusion Detection System

	IEC	International Electronic Commission
	IP	Internet Protocol
	IPS	Intrusion Prevention System
	ISO	International Standard Organisation
L	**LAN**	Local Area Network
	LATICE	LAboratoire de Technologies de l'Information et de la Communication & génie Electrique
	LMMP	Laboratoire de Mécanique, Matériaux et Procédés
	LS	Ligne Spécialisée
M	**MSSDT**	Mécanique des Solides, des Structures et de Développement Technologique
P	**PC**	Personal Computer
	POE	Power Over Ethernet
	POP	Point Of Presence
	PRTG	Paessler Router Traffic Grapher
R	**RG**	Répartiteur Général
	RNIA	Réseau National Inter-Administratif
	RNIS	Réseau Numérique à Intégration de Services
	RSSI	Responsable de la Sécurité des Systèmes d'Information
S	**SGBD**	Système de Gestion de Base de Données
	SSH	Secure Shell
	SI	Système d'Information
	SIME	Signal, Image et Maitrise de l'Energie
	SMSI	Système de Management de la Sécurité d'Information
	SNMP	Simple Network Management Protocol
	SR	Sous-Répartiteur
	SREX	Sous-Répartiteur EXistant

	SSI	Sécurité des Système d'Information
	SSID	Service Set IDentifier
U	**UTP**	Unshielded Twisted Pair
V	**VLAN**	Virtual Local Area Network
	VNC	Virtual Network Computing
W	**WAN**	Wided Area Network
	WIFI	WIrless FIdelity

Introduction Générale

A l'heure actuelle, il est vital pour toute entreprise d'évoluer en permanence, en effet le dynamisme des systèmes, la compétitivité et le besoin continu de modernisation et de rénovation incitent les entreprises à suivre le développement technologique qui offre plus de possibilités et de solutions.

Le défi s'accentue pour les entrepreneurs pour travailler au rythme de l'innovation, raison pour laquelle, il est crucial d'évaluer les systèmes en permanence afin de recourir aux démarches d'innovation et d'amélioration des performances.

Dans ce contexte, avoir recours à des missions d'audit périodiques est devenu une nécessité afin d'évaluer un système à la lumière des règles en vigueur.

On peut définir l'audit :

« L'audit est une démarche spécifique d'investigation, de recherche d'information et d'évaluation à partir d'un référentiel incluant un diagnostic et conduisant à des Recommandations ». *[ARDOUIN Thierry et LACAILLE Sylvain]*

L'audit intéresse multiples domaines et est réalisé en prenant en compte différents aspects. Cette évaluation permet de relever les faiblesses et les forces d'un système afin d'évaluer sa conformité aux normes admises comme étant des référentiels tout au long du processus de l'audit et de porter connaissance à l'entrepreneur des solutions allant dans le sens des objectifs de son entreprise.

Dans ce cadre, l'objectif de ce projet, intitulé «Audit du Réseau Informatique de l'ENSIT» sera d'auditer le réseau de l'Ecole Nationale Supérieure d'Ingénieurs de Tunis et de mettre en évidence les défaillances et les faiblesses de son Système Informatique qui est appelé à évoluer et à être rénové pour pouvoir supporter les nouveaux besoins en terme de connexions et d'ouverture sur d'autres projets, surtout que l'ENSIT est une établissement universitaire qui

accueille et forme des ingénieurs en domaines technologiques et doit donner l'exemple par sa propre plateforme.

Le présent rapport sera composé de cinq chapitres, il comportera :

- Un premier chapitre qui sera dédié à la présentation du cadre du projet, l'établissement d'accueil « ENSIT » et les services qu'il offre ;
- Un deuxième chapitre exposant un aperçu sur les normes et standards du domaine objet de l'audit ainsi que des généralités sur le processus d'audit informatique ;
- Le troisième chapitre comprendra une étude détaillée du Système Informatique installé ;
- Un quatrième chapitre présentant une analyse des résultats de l'audit en classant les failles en failles organisationnelles, physiques et techniques et établissant un bilan identifiant les points de vulnérabilité ;
- Un cinquième chapitre qui s'intéressera aux recommandations pour remédier aux faiblesses relevées et aux solutions déployées.

Chapitre I : **Cadre du projet et présentation de l'organisme d'accueil**

Introduction

Le présent rapport s'introduit dans le cadre d'une mémoire de mastère dont le projet s'est déroulé au sein de l'Ecole Nationale Supérieure d'Ingénieurs de Tunis : ENSIT.

On commence dans ce premier chapitre par une présentation générale du cadre du projet, ses activités et son organisation et on finit par une présentation de la problématique de notre mémoire.

1. Présentation de l'organisme d'accueil

1.1 Présentation générale

L'Ecole Nationale Supérieure d'Ingénieurs de Tunis nommée ENSIT est une institution publique à caractère administratif qui fait partie de l'ensemble des établissements universitaires offrant une formation pour les métiers d'ingénieurs.

La formation se déroule sur une période de trois ans après avoir réussi le concours national d'entrée aux écoles d'ingénieurs.

L'ENSIT accueille aussi des mastériens et des doctorants dans des spécialités variées.

1.2 Fiche d'identité

Tableau 1: Fiche d'identité de l'ENSIT

Caractéristique	Valeur
Dénomination	Ecole Nationale Supérieure d'Ingénieurs de Tunis
Logotype	ensit Ecole Nationale Supérieure d'Ingénieurs de Tunis
Domaine d'activité	Enseignement Supérieure et Recherche Scientifique
Site web	http://www.ensit.tn
Adresse e-mail	mail@esstt.rnu.tn
Adresse	Avenue Taha Hussein Montfleury, 1008 Tunis
Téléphone	(+216) 71 49 60 66 / 71 49 40 20 / 71 39 95 25

1.3 Historique

L'établissement a connu des transformations statutaires dictées par les besoins stratégiques de formation :

- L'École Nationale Supérieure d'Ingénieurs de Tunis (ENSIT) crée en 2011 ;
- L'École Supérieure des Sciences et Techniques de Tunis (ESSTT) crée en 1994 ;
- L'Ecole Normale Supérieur de l'Enseignement Technique (ENSET) crée en 1973 ;
- L'Ecole Normale des Professeurs Adjoints (ENPA) crée en 1962.

Elle fait partie des institutions de l'Université de Tunis.

1.4 Rôle et Missions

L'ENSIT est habillée à former des étudiants de deuxième et troisième cycle dans les domaines suivants :

- **Génie Electrique** : divisée en trois branches : électrotechnique, informatique industrielle et électronique ;
- **Génie Mécanique** : divisée en trois branches : conception des produits industriels, conception et fabrication assistées par ordinateur et génie mécanique productique ;
- **Génie Civil** ;
- **Physiques** ;
- **Génie Informatique** ;
- **Génie Industriel** ;
- **Génie Mathématiques Appliquées et Modélisation**.

1.5 Organisation

L'ENSIT compte plus de 250 enseignants-chercheurs et plus d'une centaine d'agents administratifs, techniciens et ouvriers. Elle fait aussi appel à des compétences de l'industrie ainsi qu'à des experts étrangers.

Elle comporte :

- Une Direction des Etudes ;
- Une Direction des Stages ;

- Une Ecole Doctorale qui contribue à la formation des doctorants dans les disciplines de Génie Mécanique, Génie Électrique et Physique ;
- Six Départements d'Etudes : Génie Electrique, Génie Mécanique, Génie Civil, Informatique, Mathématiques, Physique et Chimie Industrielle ;
- Trois Laboratoires de Recherche :
  - **SIME :** Signal, Image et Maitrise de l'Energie ;
  - **LATICE :** LAboratoire de Technologies de l'Information et de la Communication & Génie Electrique ;
  - **LMMP :** Laboratoire de Mécanique Matériaux et Procédés.
- Cinq Unités de Recherche :
  - **DMMP :** Dynamique Moléculaire et Matériaux Photoniques ;
  - **CEREP :** CEntre de REcherche en Productique ;
  - **MSSDT :** Mécanique des Solides, des Structures et de Développement Technologique ;
  - **CMO :** Chimie Moléculaire Organique ;
  - **C3S :** Commande Surveillance et Sûreté des Systèmes.

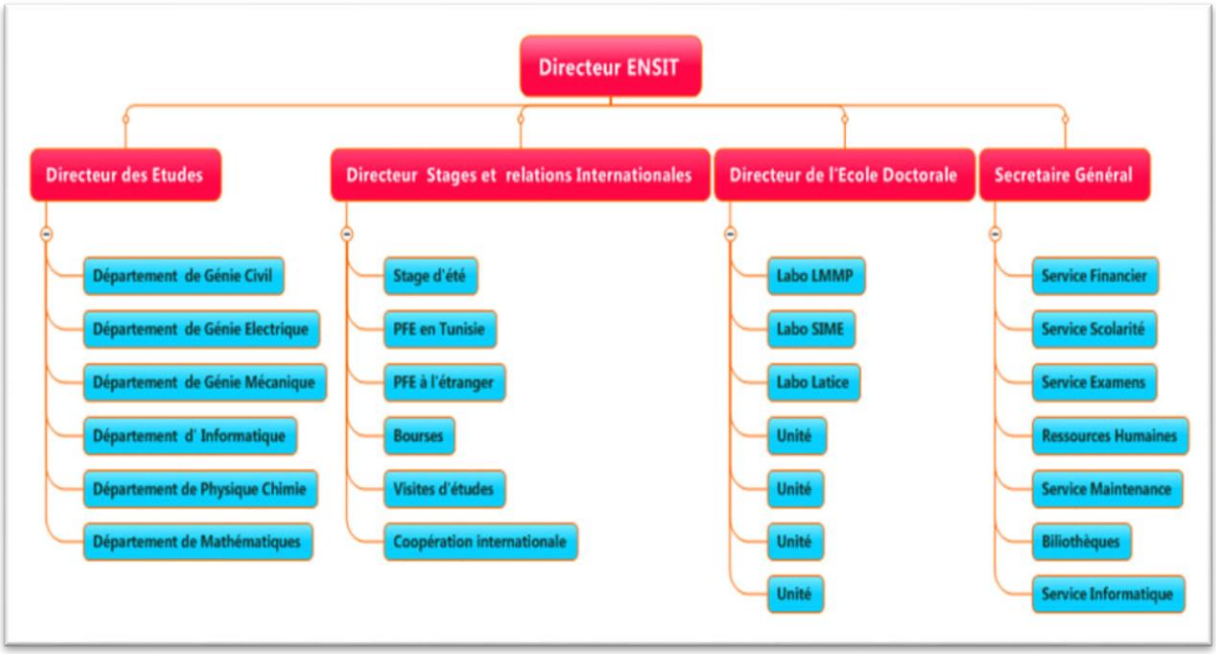


Figure 1 : Organigramme de l'ENSIT [8]

2. Problématique

Un établissement d'enseignement supérieur qui assure la formation d'Ingénieurs, de mastériens et de doctorants dans des domaines de sciences physiques, techniques et surtout sciences informatiques, doit répondre à certaines exigences d'innovation et de modernisation de sa plateforme informatique éducative afin de garantir une meilleure qualité pour l'enseignement et la recherche.

Le corps administratif et pédagogique de l'école sollicite de façon continue l'innovation des moyens de bord technologiques pour qu'il puisse diriger ses tâches en toute sécurité et souplesse et se trouve motivé à accomplir ses devoirs.

C'est dans ce cadre que le Système Informatique de l'ENSIT doit être audité afin d'établir une cartographie précise de son infrastructure et s'assurer que les différentes composantes de son réseau répondent aux processus métiers de l'établissement au niveau de qualité et sécurité requises.

Conclusion

Dans ce chapitre, on a présenté le cadre de notre projet à travers la présentation de son organisation et les différents services qu'il offre et par la suite on a exposé brièvement la problématique du projet qu'on va essayer de traiter dans les chapitres qui suivent.

Chapitre II : **Généralités et Etat de l'art**

Introduction

La qualité, la rapidité et la sécurité de la communication de l'information dans un Système Informatique sont devenues, pour toute entreprise, l'immense défi à l'égard du type de cette dernière ; ce domaine est en évolution continue, c'est pourquoi toute entreprise est appelée à auditer son Système Informatique afin d'avoir une cartographie détaillée des états des lieux, à partir de laquelle elle peut agir pour atteindre ses objectifs.

Ce chapitre exposera les normes et standards sur lesquels reposera notre mission d'audit, ainsi qu'une description du processus d'audit et de la démarche adoptée pour accomplir la mission.

1. Réseaux informatiques

La mission confiée aux réseaux informatiques à travers leurs infrastructures consiste à transporter des données selon un protocole défini.

La nécessité d'échanger des données de plus en plus vite de façon flexible, fiable et rapide passe par une évolution des protocoles. Le câblage structuré est la réponse à ces exigences, une installation de câblage structuré permet des éventuelles modifications et ce en permettant de reconfigurer rapidement le réseau de transmission, sans avoir à intervenir directement sur l'infrastructure de support pendant toute la durée de vie du système. [1]

2. Principes du câblage structuré

Le câblage structuré comprend les techniques, méthodes et normes à respecter qui permettent l'interconnexion physique de différents locaux afin que le système déployé soit :

• **Universel** : L'infrastructure est adaptable au transport de tous les types d'informations ;

• **Banalisé :** Tous les câbles, les prises et les conventions qui les raccordent doivent être identiques dans tout le réseau ;

• **Reconfigurable :** (au niveau topologie) sans recours à la modification structurelle du câblage ;

• **Ayant une compatibilité descendante :** permettant d'utiliser des équipements de catégorie inférieure sur un câblage de catégorie supérieure.

2.1 Les Normes relatives au câblage structuré

Avant 1990, il n'existait aucune norme sur l'infrastructure du câblage de télécommunications, exception faite de quelques normes particulières adoptées par différentes entreprises.

Au début des années 1990, des organismes de normalisation ont publié des normes de télécommunications définissant cette infrastructure. Ces normes établissent des exigences de rendement ainsi que des lignes directrices visant la conception et l'installation de l'infrastructure des télécommunications. [2]

Les normes définissent des "implantations de référence" avec une correspondance entre la classe du canal et la catégorie des composants.

Les normes de référence pour le câblage structuré incluent le design et l'installation du système dans son ensemble ainsi que les caractéristiques techniques de chaque composant. Les normes sont structurées de façon différente selon les continents, mais couvrent dans tous les cas tous les sujets importants.

Les normes intègrent les conditions de Performance, de sécurité et de conformité d'installation. [3]

- ***La norme internationale ISO/CEI*11801** a été publié en septembre 2002 et définit les conditions spécifiques et les recommandations pour la conception du système de câblage de télécommunication (câblage structuré). Cette norme possède un champ d'application très large (téléphonie analogique et RNIS, différents standards de communication de données, systèmes de contrôle et de gestion technique du bâtiment, automatisation de production) et couvre à la fois le câblage cuivre et en fibre optique ; [4]
- ***La norme internationale ISO/CEI14763-2*** définit les règles d'installation, de planification, de gestion et de maintenance des câblages ;
- ***La norme internationale ISO/CEI 14763-3*** définit les règles de test du câblage optique.

2.2 Les Lois législatives régissant le déploiement des réseaux informatiques en Tunisie

Les principales lois législatives et réglementaires tunisiennes en vigueur sont comme suivies :

- **Arrêté n°2014_1281** du 1er août 2014, relatif aux activités d'intégration et de réalisation des réseaux et portant sur l'organisation du domaine et fixant les règles générales de réalisation des réseaux publics dans le domaine des technologies de l'information et de la communication ; [5]
- **Décret n° 2014-2152** du 19 mai 2014, relatif à l'exercice des activités d'études, d'intégration et de réalisation des réseaux dans le domaine des technologies de l'information et de la communication. [6]

3. La sécurité Informatique

La valeur de toute entreprise consiste en son capital informationnel, ce capital doit être protégé de tout risque pouvant nuire aux activités et intérêts de l'entreprise. Le système informatique représenté par l'ensemble des moyens organisationnels, physiques, humains et technologiques mis en place doit être à l'abri de toute faille de sécurité susceptible de menacer la confidentialité de l'information, son intégrité ou sa disponibilité. Dans ce contexte, certaines normes et standards ont été développés afin de définir des règles appropriées à suivre pour préserver la sécurité informatique d'un système et veiller à l'amélioration permanente de sa performance.

3.1 Les Normes relatives à la Sécurité Informatique

Plusieurs normes régissant la sécurité informatique ont été définies, on cite :

- **ISO 27001** : Système de Management de la Sécurité des Systèmes d'Information, intitulé « **Exigences de *SMSI* »** ;
- **ISO 27000** : vocabulaire SSI ;
- **ISO 27002** (Ancien 17799) : catalogue de mesures de sécurité, intitulé « ***Code de bonnes pratiques pour la gestion de la sécurité de l'information*** » ;
- **ISO 27003** : implémentation du SMSI ;
- **ISO 27004** : indicateurs de suivi du SMSI ;
- **ISO 27005** (Ancien ISO 13335) : évaluation et traitement du risque, intitulé « **Gestion du risque en sécurité de l'information** » ;
- **ISO 27006** : certification du SMSI ;
- **ISO 27007** : audit du SMSI. [7].

3.2 Les Lois législatives relatives à la Sécurité Informatique en Tunisie

Plusieurs lois ont été promulguées en Tunisie afin de préserver la sécurité de l'information.

Les différents ministères tunisiens incitent leurs institutions filiales, via des circulaires, à régir leurs Systèmes d'Informations selon les normes et lois en vigueur pour préserver la sécurité de l'information. On peut citer parmi ces textes :

- **Loi n° 5 - 2004 du 3 février 2004** : relative à la sécurité informatique et portant sur l'organisation du domaine de la sécurité informatique et fixant les règles générales de protection des systèmes informatiques et des réseaux ; [8]
- **Décret n° 1250 - 2004du 25 mai 2004 :** fixant les systèmes informatiques et les réseaux des organismes soumis à l'audit obligatoire périodique de la sécurité informatique et les critères relatifs à la nature de l'audit et à sa périodicité et aux procédures de suivi de l'application des recommandations contenues dans le rapport d'audit ; [8]
- **Circulaire n° 36/09du 16 avril 2009 :** du ministre de l'Enseignement Supérieur, de la Recherche Scientifique et de la Technologie à propos de la sécurité du réseau national universitaire. [9]

4. Objectif d'une mission d'audit

L'objectif d'une mission d'audit est d'établir une cartographie nette et précise de l'objet sujet de l'audit. Toute composante doit être analysée et testée par rapport aux normes en vigueur afin de repérer les défaillances, prévenir les risques, anticiper un dysfonctionnement ou réparer des problèmes encourus pour pouvoir établir à la fin un plan de correction, d'amélioration et d'optimisation.

La mission d'audit de notre Projet de Fin d'Etudes va aborder deux composantes dépendantes du système : l'infrastructure et la sécurité du Système d'Informatique de l'ENSIT.

5. Les étapes de réalisation d'une mission d'audit

L'audit est un processus qui doit être réalisé de façon périodique pour contrôler l'état de son système et se déroule généralement suivant trois étapes principales :

- **La préparation de l'audit :**

  Elle consiste à définir le cadre de la mission d'audit : Objectifs, Référentiels, Champs d'application et planification.

- **La réalisation de la mission d'audit :**

La mission d'audit est l'étude de l'existant (faire l'audit sur site, recueil d'informations et de documents) selon plusieurs visions : une vision organisationnelle et physique, généralement suivie d'une vison technique.

L'audit organisationnel et physique s'appuie sur l'identification des faiblesses menaçant la fiabilité du Système d'Information en relation avec l'aspect organisationnel et physique. L'évaluation de ces risques se fait par l'analyse de l'organisation des processus informatiques et la manière dont l'environnement informatique est exploité.

En ce qui concerne l'audit de la sécurité informatique, le volet organisationnel et physique peut être traité comme dans notre cas à l'aide d'un questionnaire basé sur la norme ISO 27002 et adressé au personnel de l'organisme audité.

Pour l'audit de l'infrastructure, les outils utilisés sont : des observations sur terrain, analyse de documents, réconciliation des données, entretiens avec le personnel, ...

L'audit technique s'appuie sur l'identification et l'évaluation des vulnérabilités et des failles à l'aide de logiciels et de sondes de détection selon le système à auditer.

On distingue différents types d'outils :

- Outils de sondage et de reconnaissance du réseau ;
- Outils d'analyse et d'interception de flux réseaux ;
- Outils de test automatique de vulnérabilités du réseau ;
- Outils spécialisés dans l'audit des types de système d'exploitation ;
- Outils spécialisés dans l'audit des équipements réseau (routeurs, Switchs) ;
- Outils de test de la solidité des outils de sécurité réseau (firewalls, IDS, outils d'authentification) ;
- …..

Dans une phase plus avancée de l'audit technique, certaines missions d'audit adoptent : ***l'audit intrusif*** qui permet d'apprécier le comportement du réseau face à des attaques.

- **Conclusion de la mission d'audit :**

A partir du bilan de l'étude effectuée dans le cadre de l'audit et l'analyse des résultats il y aura en dernier lieu rédaction du rapport d'audit comprenant les recommandations correctives selon un plan d'action.

Dans la figure ci-dessous, on illustre le processus d'audit d'un Système d'Information :

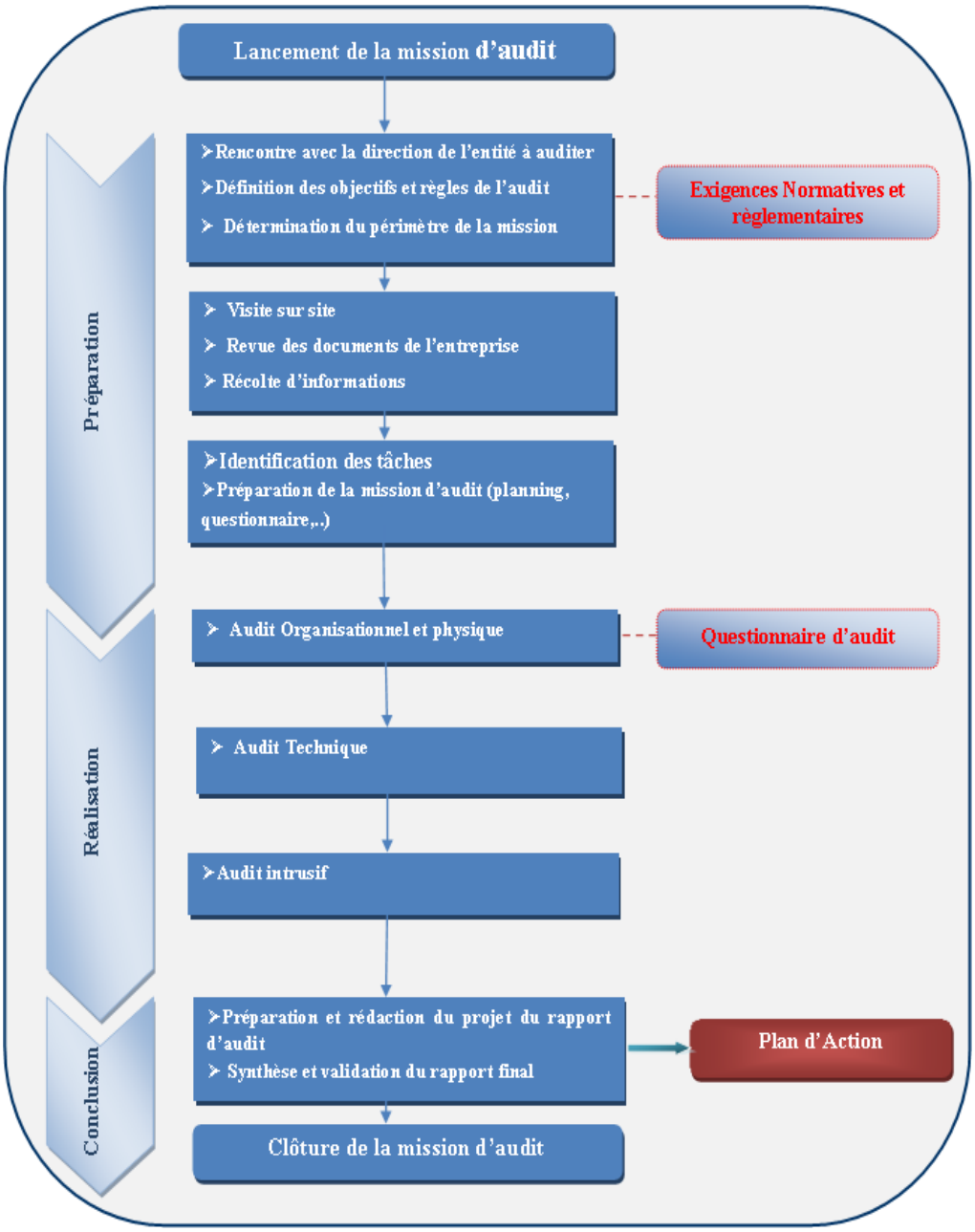


Figure 2 : Démarche d'une mission d'audit

Conclusion

La mission d'audit définie dans ce présent chapitre représente une procédure méthodique qui consistera à analyser toute une infrastructure en détail selon différents volets pour aboutir à des résultats et des recommandations.

Chapitre III : **Etude de l'existant**

Introduction

Dans cette partie on va dresser un état des lieux du Système Informatique de l'ENSIT tout en détaillant les composantes qui le constituent.

Cette cartographie générale sera illustrée par des tableaux d'inventaire des entités et des plans du réseau dans les différents étages.

1. Etude de l'Existant

1.1 Description du Système Informatique de l'ENSIT

L'audit de cet établissement sera un peu spécifique parce que le nombre d'utilisateurs peut changer d'un jour à l'autre.

1.1.1 Inventaire des ordinateurs

L'ENSIT compte plus de 400 Ordinateurs de bureau installés dans les différents laboratoires d'enseignement, les laboratoires et unités de recherches, l'administration et les bureaux d'enseignants et aux alentours de 400 Ordinateurs portables appartenant aux étudiants, chercheurs et enseignants ;

1.1.2 Inventaire des logiciels et systèmes d'exploitation

Les postes de travail sont équipés de :

- **Systèmes exploitation :** Windows XP (SP2/SP3), Windows 7 (SP1), Windows 8 et Windows 10 non licenciés et Linux ;
- **Suite bureautique :** office 2003, 2007, 2010 et 2016 tous non licenciés.

Les applications exploitées par le service financier et dont les serveurs sont hébergés au Centre National d'Informatique CNI sont :

- **RACHED** : permet l'automatisation de la gestion des procédures relatives aux missions effectuées à l'étranger ;
- **ADEB** : est une application d'aide à la décision Budgétaire ;
- **INSAF** : permet la gestion intégrée des ressources humaines et de la paie du personnel de la fonction publique.

Un très grand nombre de logiciels est exploité dans le domaine de l'enseignement et de la recherche :

- **Visual Studio ;**
- **Borland C/C++ Compiler ;**
- **NetBeans IDE ;**
- **Dev-C++ ;**
- **MySQL ;**
- **JAVA ;**
- **PowerAMC ;**
- **Matlab ;**
- **Eclipse ;**
- **CATIA v5 ;**
- **AweSim Visual SLAM ;**
- **CPAO Prlude ;**
- **SWI-Prolog ;**
- **Abaqus 6.12 ;**
- …..

Tous les logiciels cités ci-dessus ne sont pas licenciés.

L'école dispose uniquement de deux logiciels avec licences qui sont : **Cadmould** et **SolidWorks**.

1.2 Le réseau informatique

Cette partie est dédiée à identifier toutes les composantes formant l'infrastructure du réseau de l'ENSIT et ce d'après les visites sur site et les documents fournis.

1.2.1 Description du réseau de l'ENSIT

L'Ecole Nationale Supérieure d'Ingénieurs de Tunis est formée de deux bâtiments : Le bloc A formé de 4 étages et le Bloc B d'un sous-sol plus 3 étages, trois installations de réseaux informatiques existent :

- Un réseau physiquement séparé du réseau local de l'école installé dans le service financier et lié au Centre National d'Informatique (CNI) via le réseau National Inter Administratif « RNIA » ;

- Une installation qui a été mise en place en 2008 dans le cadre d'un projet ministériel de rénovation des réseaux universitaires. L'installation a été certifiée conforme aux normes par le CERT : Centre d'Etudes et de Recherche des Télécommunications. La nouvelle installation a intégré quelques segments du réseau déjà existant ;
- L'ancien réseau non utilisé qui a été conservé et dont le répartiteur est cascadé au répartiteur du service financier pour assurer la connexion d'un seul agent au réseau RNIA dont le bureau est loin du local où est implanté le réseau du service financier, cette connexion a été réalisée à travers l'ancienne prise du réseau toujours fonctionnelle dans l'ancienne armoire.

1.2.2 Topologie du réseau

La topologie mise en place est la topologie en étoile : un Répartiteur Général (RG) interconnecte des Sous Répartiteurs (SR) couvrants les différentes zones composant les étages des deux blocs de l'école.

Les sous répartiteurs sont connectés en étoile autour du Répartiteur Général :

- **13 Sous-Répartiteurs** raccordés avec des liaisons en Fibre Optiques ;
- **11 Sous-Répartiteurs** raccordés avec des cascades en Cuivre.

Le réseau compte plus de 600 prises Ethernet.

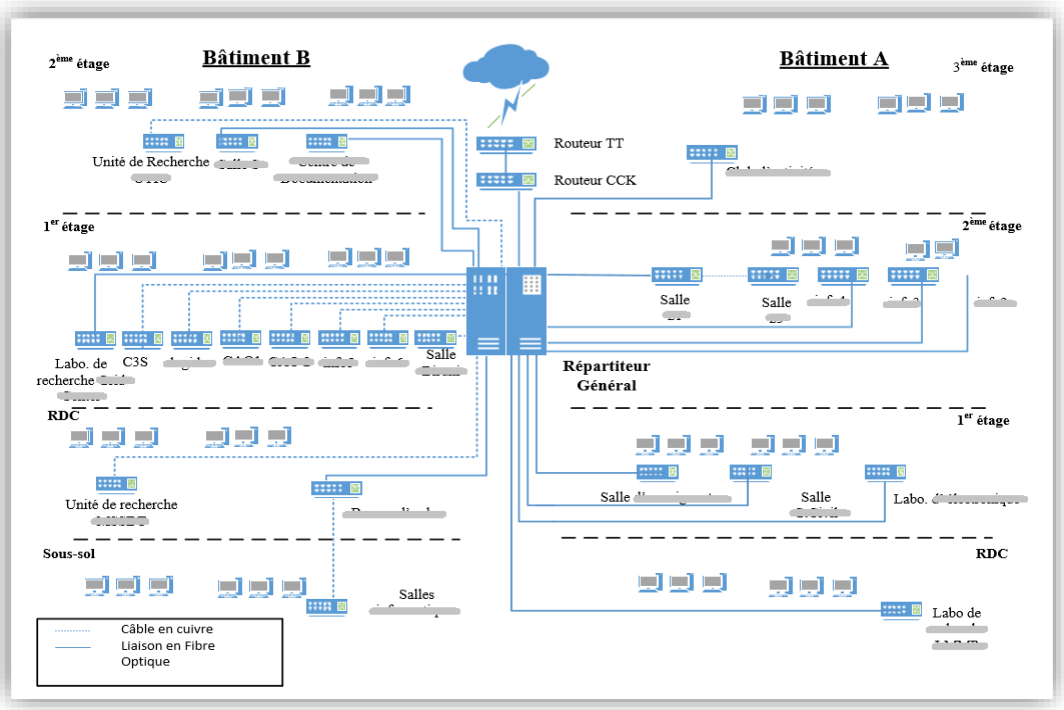


Figure 3 : Schéma Synoptique du Réseau Informatique de l'ENSIT

1.2.3 Adressage IP

Trois types d'adressages sont utilisés à l'école :

- ***Un adressage privé*** : 192. attribué via DHCP ;
- ***Un adressage privé*** : 10. statique ;
- ***Un adressage public*** : 41. utilisé pour les applications exigeant une reconnaissance IP comme certains sites de ressources électroniques, aussi l'implémentation et la mise à jour du catalogue collectif des bibliothèques universitaires dans le cadre du projet BIRUNI.

1.3 Les équipements Réseaux installés

1.3.1 Les Répartiteurs et Switchs

Tableau 2 : Liste des Répartiteurs et Switchs du réseau

Bâtiment	Local	Nom du Répartiteur	Marque et modèle des switchs	Niveau (2 ou 3)	Nombre de ports	Débit des ports	Ports Up Link	Débit up Link	Baie	Observation
	Labo. de recherche	**SR**	SMC TigerStack 10/100 6248 M	2	48	100Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	12U	
	Salle des	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	24U	Porte de baie défoncée
	Labo. d'	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	24U	
	Atelier	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	12U	
	Salle	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	21U	
	Salle	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	12U	
	Salle	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	12U	
	Salle	**Cas. Cuivre avec SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	12U	Répartiteur est cascadé avec un autre sous répartiteur et pas avec le répartiteur général.
		SR	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	21U	Baie n'est pas bien fixée au mur.
	Salle	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	15U	Porte de la baie défoncée
	Centre	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)		24U	

	Salle	**SR**	PAS DE SWITCH						12U	Switch déplacé Le SR n'a jamais fonctionné
	Salle		- (2) SMC TigerStack10/100 6248 M	2	(2) 48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	33U	
			- EM4700BD-12GT12GC	3		1Gb/s	24 ports RJ45 + 12 ports SFP			
			- EM4700BD-8GC16GX	3		1Gb/s	8 ports RJ45 + 16 ports SFP			
			EM4710BD-Agent (Management Module)	3						
	Salle	**Cas. Cuivre**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	15U	
	Salle	**Cas. Cuivre**	Accton EdgeCore ES 3528M	2	48	100 Mb/s	4 Gigabit Combo (RJ45 / SFP)	1Gb/s	15U	
	Labo. de recherche	**SR**	SMC TigerStack 10/100 6248 M	2	48	100 Mb/s	2 Gigabit Combo (RJ45 / SFP)	1Gb/s	15U	
	Unité de recherche	**Cas. Cuivre**	SMC EZ Switch 10/100 1024 DT	2 (Non administrable)	24	100 Mb/s	Lié au RG avec un port normal (pas de port uplink)		12U	
	Salle	**Cas. Cuivre**	SMC EZ Switch 10/100 1024 DT	2 (Non administrable)		100 Mb/s	Lié au RG avec un port normal (pas de port uplink)		15U	
	Salle	**Cas. Cuivre**	D-Link DES-3225G 10/100	2 (Non administrable)		100 Mb/s	Lié au RG avec un port normal (pas de port uplink)		12U	
	Salle	**Cas. Cuivre**	- SMC FS2401 - SMC FS1601	2 (Non administrable) 2 (Non administrable)	24 16	100 Mb/s 100 Mb/s	Lié au RG avec un port normal (pas de port uplink)		15U	
	Salle	**Cas. Cuivre**	SMC EZ Switch 10/100 1024 DT	2 (Non administrable)		100 Mb/s	Lié au RG avec un port normal (pas de port uplink)		12U	

	Salle	**Cas. Cuivre**	HP procure Switch J4813A	2 (Non administrable)		100 Mb/s	Lié au RG avec un port normal (pas de port uplink)		12U	
	Unité de recherche	**Cas. Cuivre**	HP procure Switch J4813A	2 (Non administrable)		100 Mb/s	Lié au RG avec un port normal (pas de port uplink)		15U	
	Unité de recherche	**Cas. Cuivre**	SMC EZ Switch 10/100 1024 DT	2 (Non administrable)	24	100 Mb/s	Lié au RG avec un port normal (pas de port uplink)		15U	
	Salle	**Cas. Cuivre Avec SR1**							15U	Le sous répartiteur serve deux salles câblées, et il est cascadé avec un autre sous répartiteur et non le RG.
	Salle								15U	Salle câblée, Baie installée, pas de Switch ni de liaison avec le réseau existant
	Salle								15U	Salle câblée, Baie installée, pas de Switch ni de liaison avec le réseau existant
	Salle								15U	Salle câblée Baie installée, pas de Switch ni de liaison avec le réseau existant
	Salle								15U	Salle câblée Baie installée, pas de Switch ni de liaison avec le réseau existant

1.3.2 Equipements d'accès WAN

Tableau 3 : Liste des routeurs

Equipement	Marque et Modèle	Interfaces	Débit Interface	Année d'acquisition
Routeur	Huawei AR2200series	3	1Gb/s	2014
Commutateur d'accès	Cisco ME 3400series de Tunisie Télécom	3	1Gb/s	2014

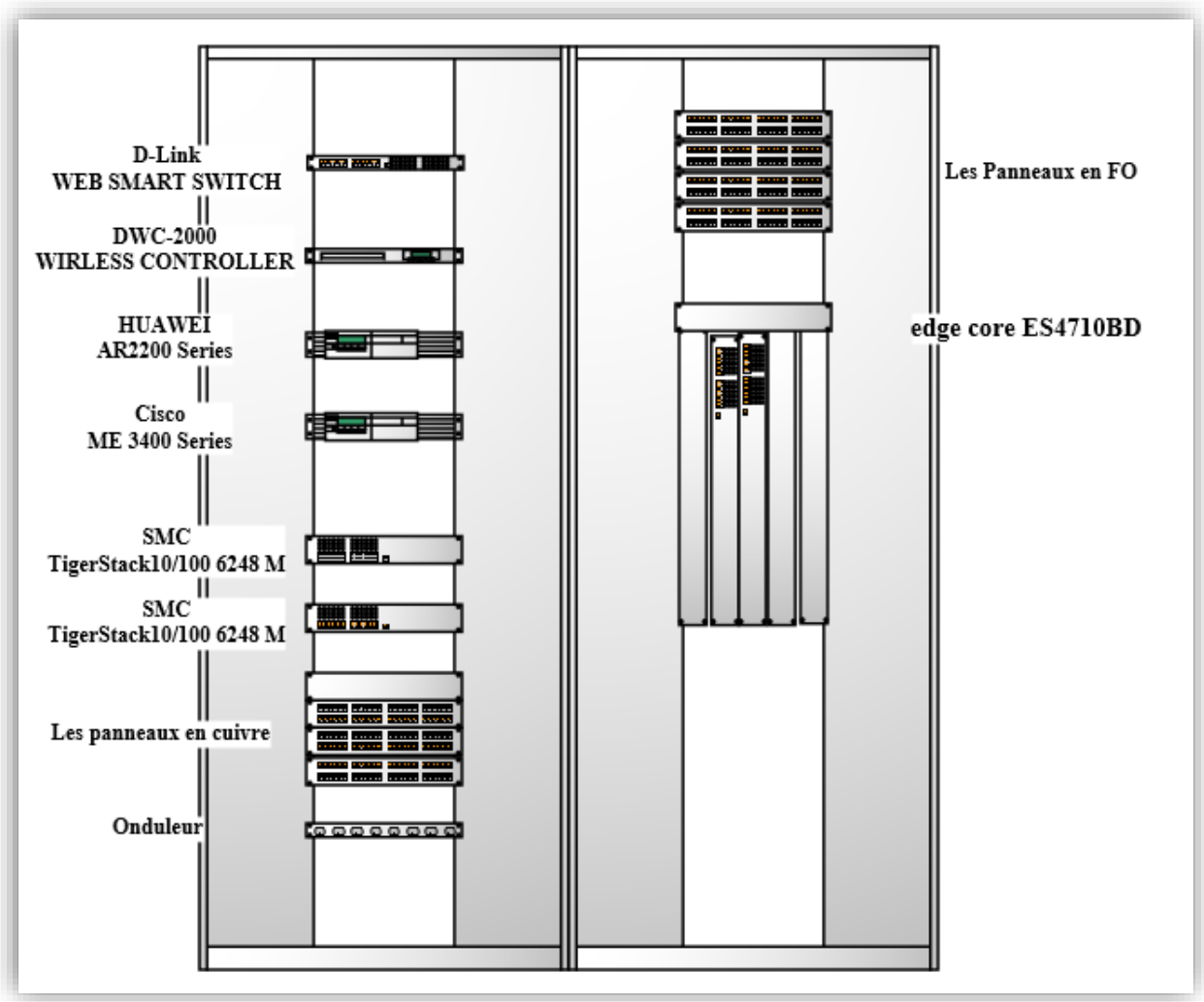


Figure 4 : Diagramme de montage en rack du RG

1.3.3 Liaison Internet avec le FSI : CCK

Le réseau de l'école est connecté à Internet via le réseau National Universitaire RNU2 déployé par le Centre de Calcul Khawarizmi (CCK), le FSI officiel de tous les établissements universitaires tunisiens. Il s'agit d'une liaison(LS) Fibre optique à un débit de **50Mb/s**.

Tableau 4 : Liaison du réseau local avec l'Internet

Type de liaison	Débit	Taux d'utilisation
Fibre Optique	50 Mb/s	**100%**

1.4 Câblage

1.4.1 Les câbles en Fibre Optique

Pour couvrir tous les étages des deux bâtiments, 13 Sous-Répartiteurs sont raccordés au Répartiteur Générale à travers des Liaisons en Fibre Optiques :

Tableau 5 : Les Liaisons Fibres Optiques avec le RG

Locaux d'interconnexion	Métrique (m)	Type de la fibre	Type du lien	Débit max	Observation
Labo. de recherche	203.2	Multimode	FO à 6 brins	1 Gb/s	
Salle	143.3	Multimode	FO à 6 brins	1 Gb/s	
Labo.	244.3	Multimode	FO à 6 brins	1 Gb/s	
Atelier	214.6	Multimode	FO à 6 brins	1 Gb/s	
Salle	156	Multimode	FO à 6 brins	1 Gb/s	
Salle	192.2	Multimode	FO à 6 brins	1 Gb/s	Baie et switch désinstallés. Liaison fibre optique avec tiroir toujours existante.
Salle		Multimode	FO à 6 brins	1 Gb/s	
Salle	236.6	Multimode	FO à 6 brins	1 Gb/s	

[illegible]	226	Multimode	FO à 6 brins	1 Gb/s	
Bureau [illegible]	42.8	Multimode	FO à 6 brins	1 Gb/s	Armoire défoncée
Labo. de recherche [illegible]	83.1	Multimode	FO à 6 brins	1 Gb/s	
Centre [illegible]	156.8	Multimode	FO à 6 brins	1 Gb/s	
Salle [illegible]	131.5	Multimode	FO à 6 brins	1 Gb/s	Switch déplacé et liaison non fonctionnelle

1.4.2 Les cascades en paires torsadées

- Les salles informatiques se trouvent dans le même étage que la salle système, elles ont été raccordées au Répartiteur Général avec des cascades en Cuivre ;
- L'unité de recherche [illegible] et l'unité [illegible] se trouvent dans différents étages mais ont été aussi raccordées de la même manière ;
- La salle [illegible] se trouve au sous-sol et le répartiteur installé dans cette salle est cascadé avec un autre sous répartiteur ;
- Le répartiteur installé dans la salle [illegible] est cascadé avec un autre sous répartiteur.

Tableau 6 : Les raccordements avec des cascades en cuivre

Local	Type du lien (UTP/FTP)	Catégorie	Débit max
Salle [illegible]	UTP	6	1Gb/s
Salle [illegible]	UTP	6	1Gb/s
Salle [illegible]	UTP	6	1Gb/s
Salle [illegible]	UTP	6	1Gb/s
Salle [illegible]	UTP	6	1Gb/s
Salle [illegible]	UTP	6	1Gb/s
Salle [illegible]	UTP	6	1Gb/s
Unité de recherche [illegible]	UTP	6	1Gb/s
Unité de recherche [illegible]	UTP	6	1Gb/s
Unité de recherche [illegible]	UTP	6	1Gb/s
Salle [illegible]	UTP	6	1Gb/s
Salle [illegible]	UTP	6	1Gb/s

1.4.3 Inventaire des prises RJ45 du réseau sur plan étage

Dans cet inventaire nous avons essayé de repérer toutes les prises Ethernet dans les différents étages des deux bâtiments tout en décrivant leurs états, cela constitue une étape indispensable pour pouvoir définir ultérieurement les défectuosités et procéder aux recommandations nécessaires.

Toutes les prises ont été illustrées sur les plans des différents étages qui ont été élaborés pour ce faire : l'ENSIT ne dispose pas de plans de son réseau informatique. (Voir Annexe 2)

Tableau 7 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique En Cuivre (m)	Fonctionnel	Etat	Repérage
Bureau	SR	6	32	1	1	1	P01	28	Oui	Bon	Oui
		6					P02	15	Oui	Bon	Oui
		6					P03	14	Oui	Bon	Oui
		6					P04	21	Oui	Bon	Oui
		6					P05	13	Oui	Mauvais	Non
		6					P06	27	Oui	Mauvais	Oui
		6					P07	17	Oui	Bon	Oui
		6					P08	37	Oui	Bon	Oui
		6					P09	30	Oui	Bon	Oui
		6					P10	24	Non	Mauvais	Non
		6					P11	48	Oui	Bon	Oui
		6					P12	48	Oui	Bon	Oui
		6					P13	49	Oui	Bon	Oui
		6					P14	40	Oui	Bon	Oui
		6					P15	51	Oui	Bon	Oui
		6					P16	54	Oui	Bon	Oui
		6					P17	62	Oui	Bon	Oui
		6					P18	71	Oui	Mauvais	Non
		6					P19	81	Oui	Bon	Oui
		6					P20	81	Non	Mauvais	Non
		6					P21	81	Oui	Bon	Oui
		6					P22	81	Oui	Bon	Oui
		6					P23	72	Oui	Bon	Oui
		6					P24	81	Oui	Bon	Oui
		6					P25	76	Non	Mauvais	Non
		6					P26	72	Oui	Mauvais	Non
		6					P27	63	Oui	Bon	Oui
		6					P28	42	Oui	Bon	Oui
		6					P29	39	Oui	Bon	Oui
		6					P30	37	Oui	Bon	Oui

		6					P31	73	Non	Mauvais	Non
		6					P32	77	Oui	Non fixé	Oui

Tableau 8 : Etat des prises du SREX dans l'unité de recherche

Local	Nom du Répartiteur	Cat. du câble	Nombre de Prises RJ45	Etat	Repérage
L'unité de recherche	SREX	5	16	1	Toutes les prises ne sont pas fonctionnelles

Tableau 9 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrage En Cuivre (m)	Fonctionnel	Etat	Repérage
Salle		6	50	3	4	13	P01	39	Oui	Mauvais	Non
		6					P02	38	Oui	Bon	Oui
		6					P03	32	Oui	Bon	Oui
		6					P04	44	Oui	Bon	Non
		6					P05	58	Non	Mauvais	Non
		6					P06	68	Oui	Bon	Oui
		6					P07	68	Non	Mauvais	Non
		6					P08	70	Oui	Bon	Oui
		6					P09	64	Non	Mauvais	Non
		6					P10	93	Oui	Bon	Oui
		6					P11	85	Oui	Bon	Oui
		6					P12	66	Non	Mauvais	Non
		6					P13	58	Non	Mauvais	Non
		6					P14	58	Non	Bon	Oui
		6					P15	55	Non	Mauvais	Non
		6					P16	58	Non	Mauvais	Non
		6					P17	60	Oui	Mauvais	Oui
		6					P18	63	Oui	Mauvais	Oui
		6					P19	66	Oui	Mauvais	Oui
		6					P20	69	Oui	Mauvais	Oui
		6					P21	69	Non	Mauvais	Oui
		6					P22	69	Oui	Mauvais	Oui
		6					P23	72	Oui	Mauvais	Oui
		6					P24	73	Non	Bon	Oui
		6					P25	44	Oui	Mauvais	Non
		6					P26	30	Oui	Mauvais	Non
		6					P27	46	Oui	Bon	Oui

		6					P28	31	**Oui**	**Bon**	**Oui**
		6					P29	31	**Oui**	**Bon**	**Oui**
		6					P30	26	**Oui**	**Bon**	**Oui**
		6					P31	26	**Oui**	**Bon**	**Oui**
		6					P32	6	**Oui**	**Bon**	**Oui**
		6					P33	16	**Oui**	**Bon**	**Oui**
		6					P34	6	**Oui**	**Bon**	**Oui**
		6					P35	6	**Oui**	**Bon**	**Oui**
		6					P36	6	**Oui**	**Bon**	**Oui**
		6					P37	6	**Oui**	**Bon**	**Oui**
		6					P38	16	**Oui**	**Bon**	**Oui**
		6					P39	6	**Oui**	**Bon**	**Oui**
		6					P40	16	**Oui**	**Bon**	**Oui**
		6					P41	6	**Oui**	**Mauvais**	**Non**
		6					P42	8	**Oui**	**Mauvais**	**Non**
		6					P43	9	**Oui**	**Mauvais**	**Non**
		6					P44	11	**Non**	**Mauvais**	**Non**
		6					P45	14	**Non**	**Mauvais**	**Non**
		6					P46	16	**Oui**	**Mauvais**	**Oui**
		6					P47	19	**Non**	**Mauvais**	**Non**
		6					P48	20	**Oui**	**Mauvais**	**Non**
		6					P49	22	**Non**	**Mauvais**	**Non**
		6					P50	23	**Oui**	**Fonctionnel**	**Non**

Tableau 10 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre de Prises RJ45	Nombre de Panneaux de brassage RJ45	Fonctionnel	Etat	Repérage
Labo. De recherche	SR	6	16	1	Toutes les prises sont fonctionnelles	Toutes les prises sont en bon état	Toutes les prises sont repérées

Tableau 11 : Etat des prises des salles et

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Fonctionnel	Etat	Repérage
Salles et	SR	6	24	1	Toutes les prises sont fonctionnelles	Toutes les prises sont en bon état	Toutes les prises sont repérées

Tableau 12 : Etat des prises de la salle

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Fonctionnel	Etat	Repérage
Salle	SR	6	24	1	Toutes les prises sont fonctionnelles	Toutes les prises sont en bon état	Toutes les prises sont repérées

Tableau 13 : Etat des prises des salles

Local	Nom du Répartiteur	Cat. du câble	Nombre De prises RJ45	Nombre de Panneaux de brassage RJ45	Etat	Repérage
Salle	SR	6	21	1	Toutes les prises ne sont pas encore exploitées, elles sont en bon état.	Toutes les prises sont repérées.
Salle	SR	6	21	1		
Salle	SR	6	21	1		
Salle	SR	6	21	1		

Tableau 14 : Etat des prises de la salle [redacted]

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Prises	Fonctionnel	Etat	Repérage
Salle [redacted]	SREX	6	28	1	P01	Oui	Bon	Oui
		6			P02	Oui	Bon	Oui
		6			P03	Oui	Bon	Oui
		6			P04	Oui	Bon	Oui
		6			P05	Oui	Bon	Oui
		6			P06	Oui	Bon	Oui
		6			P07	Oui	Bon	Oui
		6			P08	Oui	Bon	Oui
		6			P09	Oui	Bon	Oui
		6			P10	Oui	Bon	Oui
		6			P11	Oui	Bon	Oui
		6			P12	Oui	Bon	Oui
		6			P13	Oui	Bon	Oui
		6			P14	Oui	Bon	Oui
		6			P15	Oui	Bon	Oui
		6			P16	Oui	Bon	Oui
		6			P17	Oui	Bon	Oui
		6			P18	Oui	Bon	Oui
		6			P19	Oui	Bon	Oui
		6			P20	Oui	Bon	Oui
		6			P21	Oui	Bon	Oui
		6			P22	Oui	Bon	Oui
		6			P23	Oui	Bon	Oui
		6			P24	Oui	Bon	Oui
		6			P25	Oui	Bon	Oui
		6			P26	Oui	Bon	Oui
		6			P27	Oui	Bon	Oui
		6			P28	Oui	Bon	Oui

Tableau 15 : Etat des prises de la salle [redacted]

Local	Nom du Répartiteur	Cat. du câble	Nombre de prises RJ45	Nombre de Panneaux de brassage RJ45	Prises	Fonctionnel	Etat
Salle [redacted]	SREX	5	22	1	Prises non repérés	19 prises fonctionnelles et 3 prises défectueuses.	Mauvais état

Tableau 16 : Etat des prises de la salle

Local	Nom du Répartiteur	Cat. du câble	Nombre de Prises RJ45	Nombre de Panneaux de brassage RJ45	Prises	Fonctionnel	Etat
Salle	SREX	5	22	1	Prises non repérés	Toutes les prises sont fonctionnelles	Mauvais état

Tableau 17 : Etat des prises de la salle

Local	Nom du Répartiteur	Cat. du câble	Nombre de Prises RJ45	Nombre de Panneaux de brassage RJ45	Prises	Fonctionnel	Etat
Salle	SREX	5	16	1	Prises non repérés	14 prises défectueuses 2 prises fonctionnelles	Mauvais état

Tableau 18 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre de Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique En Cuivre (m)	Fonctionnel	Etat	Repérage
	SR	6	82	2	1	1	P01	78	Oui	Bon	Oui
		6					P02	79	Oui	Bon	Oui
		6					P03	68	Oui	Bon	Oui
		6					P04	66	Oui	Mauvais	Oui
		6					P05	62	Oui	Bon	Oui
		6					P06	60	Non	Mauvais	Non
		6					P07	61	Non	Mauvais	Non
		6					P08	61	Non	Mauvais	Non
		6					P09	61	Oui	Bon	Oui
		6					P10	63	Oui	Bon	Oui
		6					P11	53	Oui	Bon	Oui
		6					P12	52	Oui	Bon	Oui
		6					P13	64	Oui	Bon	Oui
		6					P14	48	Oui	Bon	Oui

		6					P15	65	Non	Mauvais	Non
		6					P16	60	Oui	Bon	Oui
		6					P17	62	Non	Mauvais	Non
		6					P18	61	Oui	Bon	Oui
		6					P19	58	Oui	Bon	Oui
		6					P20	54	Oui	Bon	Oui
		6					P21	57	Oui	Bon	Oui
		6					P22	46	Oui	Bon	Oui
		6					P23	41	Oui	Bon	Oui
		6					P24	39	Oui	Bon	Oui
		6					P25	43	Oui	Bon	Oui
		6					P26	33	Oui	Bon	Oui
		6					P27	30	Oui	Bon	Oui
		6					P28	27	Oui	Bon	Oui
		6					P29	26	Oui	Bon	Oui
		6					P30	28	Oui	Bon	Oui
		6					P31	23	Oui	Bon	Oui
		6					P32	19	Oui	Bon	Oui
		6					P33	14	Oui	Bon	Oui
		6					P34	22	Oui	Bon	Oui
		6					P35	17	Oui	Bon	Oui
		6					P36	21	Oui	Bon	Oui
		6					P37	23	Oui	Bon	Oui
		6					P38	27	Oui	Bon	Oui
		6					P39	29	Oui	Bon	Oui
		6					P40	31	Oui	Bon	Oui
		6					P41	16	Oui	Mauvais	Oui
		6					P42	16	Non	Mauvais	Oui
		6					P43	6	Oui	Bon	Oui
		6					P44	35	Oui	Bon	Oui
		6					P45	36	Oui	Bon	Oui
		6					P46	38	Oui	Bon	Oui
		6					P47	39	Oui	Bon	Oui
		6					P48	44	Oui	Bon	Oui
		6					P49	41	Oui	Bon	Oui
		6					P50	45	Oui	Bon	Oui
		6					P51	52	Oui	Bon	Oui
		6					P52	53	Oui	Bon	Oui
		6					P53	55	Oui	Bon	Oui
		6					P54	54	Oui	Bon	Oui
		6					P55	61	Oui	Mauvais	Oui
		6					P56	58	Oui	Bon	Oui
		6					P57	62	Oui	Bon	Oui
		6					P58	62	Oui	Bon	Oui
		6					P59	62	Oui	Bon	Oui
		6					P60	63	Oui	Bon	Oui
		6					P61	63	Oui	Bon	Oui
		6					P62	65	Oui	Bon	Oui
		6					P63	65	Oui	Bon	Oui

		6					P64	68	Oui	Bon	Oui
		6					P65	69	Oui	Bon	Oui
		6					P66	69	Oui	Bon	Oui
		6					P67	73	Oui	Bon	Oui
		6					P68	73	Oui	Bon	Oui
		6					P69	58	Oui	Bon	Oui
		6					P70	73	Non	Mauvais	Non
		6					P71	31	Oui	Bon	Oui
		6					P72	28	Oui	Bon	Oui
		6					P73	32	Oui	Bon	Oui
		6					P74	35	Oui	Bon	Oui
		6					P75	41	Oui	Bon	Oui
		6					P76	38	Oui	Bon	Oui
		6					P77	45	Oui	Bon	Oui
		6					P78	47	Oui	Bon	Oui
		6					P79	49	Oui	Bon	Oui
		6					P80	52	Oui	Bon	Oui
		6					P81	73	Non	Mauvais	Non
		6					P82	73	Non	Mauvais	Non

Tableau 19 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre de prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique en cuivre (m)	Fonctionnel	Etat	Repérage
		6					P01	29	Oui	Bon	Oui
		6					P02	28	Oui	Bon	Oui
		6					P03	29	Oui	Bon	Oui
		6					P04	23	Oui	Bon	Oui
		6					P05	35	Oui	Bon	Oui
		6					P06	38	Oui	Bon	Oui
		6					P07	30	Oui	Bon	Oui
		6					P08	37	Oui	Bon	Oui
		6					P09	37	Oui	Bon	Oui
		6					P10	35	Oui	Bon	Oui
	SR	6	59	3	1	1	P11	41	Oui	Bon	Oui
		6					P12	42	Oui	Bon	Oui
		6					P13	46	Oui	Bon	Oui
		6					P14	44	Oui	Bon	Oui
		6					P15	45	Oui	Bon	Oui
		6					P16	62	Oui	Bon	Oui
		6					P17	62	Oui	Bon	Oui
		6					P18	54	Oui	Bon	Oui
		6					P19	58	Oui	Bon	Oui
		6					P20	62	Oui	Bon	Oui
		6					P21	64	Oui	Bon	Oui

		6					P22	62	**Oui**	**Bon**	**Oui**
		6					P23	66	**Oui**	**Bon**	**Oui**
		6					P24	62	**Oui**	**Bon**	**Oui**
		6					P25	65	**Oui**	**Bon**	**Oui**
		6					P26	67	**Oui**	**Bon**	**Oui**
		6					P27	66	**Oui**	**Bon**	**Oui**
		6					P28	61	**Oui**	**Bon**	**Oui**
		6					P29	62	**Oui**	**Bon**	**Oui**
		6					P30	63	**Oui**	**Bon**	**Oui**
		6					P31	53	**Oui**	**Bon**	**Oui**
		6					P32	45	**Oui**	**Bon**	**Oui**
		6					P33	55	**Oui**	**Bon**	**Oui**
		6					P34	61	**Oui**	**Bon**	**Oui**
		6					P35	61	**Oui**	**Bon**	**Oui**
		6					P36	45	**Oui**	**Bon**	**Oui**
		6					P37	42	**Oui**	**Bon**	**Oui**
		6					P38	45	**Oui**	**Bon**	**Oui**
		6					P39	48	**Oui**	**Bon**	**Oui**
		6					P40	37	**Oui**	**Bon**	**Oui**
		6					P41	51	**Oui**	**Bon**	**Oui**
		6					P42	35	**Oui**	**Bon**	**Oui**
		6					P43	35	**Oui**	**Bon**	**Oui**
		6					P44	30	**Non**	**Mauvais**	**Oui**
		6					P45	30	**Non**	**Mauvais**	**Oui**
		6					P46	23	**Oui**	**Bon**	**Oui**
		6					P47	25	**Non**	**Mauvais**	**Oui**
		6					P48	20	**Oui**	**Bon**	**Oui**
		6					P49	21	**Oui**	**Bon**	**Oui**
		6					P50	21	**Oui**	**Bon**	**Oui**
		6					P51	17	**Oui**	**Bon**	**Oui**
		6					P52	17	**Oui**	**Bon**	**Oui**
		6					P53	19	**Oui**	**Bon**	**Oui**
		6					P54	15	**Oui**	**Bon**	**Oui**
		6					P55	10	**Oui**	**Bon**	**Oui**
		6					P56	35	**Oui**	**Bon**	**Oui**
		6					P57	35	**Oui**	**Bon**	**Oui**
		6					P58	19	**Oui**	**Bon**	**Oui**
							P58	19	**Non**	**Mauvais**	**Oui**

Tableau 20 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique En Cuivre (m)	Fonctionnel	Etat	Repérage
Salle	SR	6	44	2	1	1	P01	61	Oui	Bon	Oui
		6					P02	61	Oui	Bon	Oui
		6					P03	57	Oui	Bon	Oui
		6					P04	58	Oui	Bon	Oui
		6					P05	59	Oui	Bon	Oui
		6					P06	53	Oui	Bon	Oui
		6					P07	53	Oui	Bon	Oui
		6					P08	50	Oui	Bon	Non
		6					P09	50	Oui	Bon	Oui
		6					P10	51	Oui	Bon	Oui
		6					P11	51	Oui	Bon	Oui
		6					P12	55	Non	Mauvais	Oui
		6					P13	55	Oui	Bon	Oui
		6					P14	55	Oui	Bon	Oui
		6					P15	55	Oui	Bon	Oui
		6					P16	56	Oui	Bon	Oui
		6					P17	46	Oui	Bon	Oui
		6					P18	46	Oui	Bon	Oui
		6					P19	50	Oui	Bon	Oui
		6					P20	50	Oui	Bon	Oui
		6					P21	53	Oui	Bon	Oui
		6					P22	53	Oui	Bon	Oui
		6					P23	47	Oui	Bon	Oui
		6					P24	47	Oui	Bon	Oui
		6					P25	43	Oui	Bon	Oui
		6					P26	43	Oui	Bon	Oui
		6					P27	49	Oui	Bon	Oui
		6					P28	52	Oui	Bon	Oui
		6					P29	52	Oui	Bon	Oui
		6					P30	52	Oui	Bon	Oui
		6					P31	58	Oui	Bon	Oui
		6					P32	58	Oui	Bon	Oui
		6					P33	52	Oui	Bon	Oui
		6					P34	52	Oui	Bon	Oui
		6					P35	49	Oui	Bon	Oui
		6					P36	49	Oui	Bon	Oui
		6					P37	47	Oui	Bon	Oui
		6					P38	47	Oui	Bon	Oui
		6					P39	32	Oui	Bon	Oui
		6					P40	13	Oui	Bon	Oui
		6					P41	21	Oui	Mauvais	Oui
		6					P42	26	Oui	Mauvais	Non
		6					P43	35	Oui	Mauvais	Non
		6					P44	35	Oui	Bon	Oui

Tableau 21 : Etat des prises du SR

Local	Nom du Répartiteur	Nombre De Prises RJ45	Cat. du câble	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique En Cuivre (m)	Fonctionnel	Etat	Repérage
Salle	SR	11 (prises qui se trouvent en dehors de la salle)	6	2	1	1	P01	43	Oui	Bon	Oui
							P02	45	Oui	Bon	Oui
							P03	47	Oui	Bon	Oui
							P04	44	Oui	Bon	Oui
							P05	44	Oui	Bon	Oui
							P06	48	Oui	Bon	Oui
							P07	48	Oui	Bon	Oui
							P08	24	Oui	Bon	Oui
							P09	32	Oui	Bon	Oui
							P10	24	Non	Mauvais	Oui
							P11	15	Non	Mauvais	Non
		20 (prises dans la salle)	5				-	-	Oui	Mauvais état	Ne sont pas repérées

Tableau 22 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Etat
Salle	SR	5	16	1	1	1	Les prises ne sont pas repérées	Mauvais états pour toutes les prises

Tableau 23 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique En Cuivre (m)	Fonctionnel	Etat	Repérage
Salle	SR	6	33	2	1	1	P01	54	Oui	Bon	Oui
		6					P02	48	Oui	Bon	Oui
		6					P03	41	Non	Mauvais	Non
		6					P04	38	Oui	Bon	Oui
		6					P05	35	Non	Mauvais	Oui
		6					P06	41	Non	Mauvais	Non
		6					P07	43	Oui	Bon	Oui
		6					P08	44	Oui	Bon	Oui

		6					P09	44	Oui	Bon	Oui
		6					P10	48	Oui	Bon	Oui
		6					P11	48	Oui	Bon	Oui
		6					P12	35	Non	Mauvais	Non
		6					P13	33	Oui	Bon	Oui
		6					P14	48	Non	Mauvais	Non
		6					P15	46	Oui	Bon	Oui
		6					P16	35	Oui	Bon	Oui
		6					P17	46	Oui	Bon	Oui
		6					P18	40	Oui	Bon	Oui
		6					P19	46	Oui	Bon	Oui
		6					P20	45	Non	Mauvais	Non
		6					P21	54	Non	Mauvais	Non
		6					P22	54	Non	Mauvais	Non
		6					P23	29	Oui	Bon	Non
		6					P24	48	Oui	Bon	Non
		6					P25	46	Oui	Bon	Oui
		6					P26	44	Oui	Bon	Oui
		6					P27	43	Oui	Bon	Oui
		6					P28	55	Oui	Bon	Oui
		6					P29	49	Oui	Bon	Oui
		6					P30	54	Oui	Bon	Oui
		6					P31	51	Oui	Bon	Oui
		6					P32	49	Oui	Bon	Oui
		6					P33	61	Oui	Bon	Oui
		6					P34	70	Oui	Bon	Oui
		6					P35	74	Oui	Bon	Oui
		6					P36	77	Oui	Bon	Oui
		6					P37	82	Oui	Bon	Oui

Tableau 24 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique En Cuivre (m)	Fonctionnel	Etat	Repérage
Salle	SR	6	11	1	1	1	P01	32	Toutes les prises sont fonctionnelles	Toutes les prises sont en bon état	Toutes les prises sont fonctionnelles
		6					P02	30			
		6					P03	30			
		6					P04	12			
		6					P05	9			
		6					P06	9			
		6					P07	5			
		6					P08	3			
		6					P09	4			
		6					P10	3			
		6					P11	25			

Tableau 25 : Etat des prises du SR

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique En Cuivre (m)	Fonctionnel	Etat	Repérage
Labo.	SR	6	48	2	1	1	P01	32	Oui	Bon	Oui
		6					P02	30	Oui	Bon	Oui
		6					P03	30	Oui	Mauvais	Oui
		6					P04	12	Oui	Bon	Oui
		6					P05	9	Oui	Mauvais	Oui
		6					P06	9	Oui	Bon	Oui
		6					P07	5	Oui	Bon	Oui
		6					P08	3	Oui	Bon	Oui
		6					P09	4	Oui	Bon	Oui
		6					P10	3	Oui	Bon	Oui
		6					P11	25	Oui	Mauvais	Oui
		6					P12	50	Non	Mauvais	Oui
		6					P13	50	Oui	Mauvais	Oui
		6					P14	50	Oui	Bon	Oui
		6					P15	58	Non	Mauvais	Oui
		6					P16	58	Oui	Bon	Oui
		6					P17	52	Oui	Bon	Oui
		6					P18	62	Oui	Bon	Oui
		6					P19	64	Oui	Bon	Oui
		6					P20	85	Non	Mauvais	Non
		6					P21	85	Non	Mauvais	Non
		6					P22	85	Non	Mauvais	Non
		6					P23	85	Non	Mauvais	Non
		6					P24	85	Non	Mauvais	Non
		6					P25	86	Oui	Bon	Oui
		6					P26	28	Oui	Bon	Oui
		6					P27	19	Oui	Bon	Oui
		6					P28	13	Oui	Bon	Oui
		6					P29	6	Oui	Bon	Oui
		6					P30	6	Oui	Bon	Oui
		6					P31	22	Oui	Bon	Oui
		6					P32	24	Oui	Bon	Oui
		6					P33	29	Oui	Bon	Oui
		6					P34	38	Oui	Bon	Oui
		6					P35	44	Oui	Bon	Oui
		6					P36	55	Oui	Bon	Oui
		6					P37	62	Oui	Bon	Oui
		6					P38	26	Non	Mauvais	Non
		6					P39	20	Non	Mauvais	Non
		6					P40	21	Oui	Bon	Oui
		6					P41	32	Oui	Bon	Oui
		6					P42	20	Oui	Bon	Oui
		6					P43	28	Oui	Bon	Oui
		6					P44	32	Oui	Bon	Oui
		6					P45	34	Oui	Bon	Oui
		6					P46	38	Oui	Bon	Oui
		6					P47	38	Oui	Bon	Oui
		6					P48	50	Oui	Bon	Oui

Tableau 26 : Etat des prises du SR[redacted]

Local	Nom du Répartiteur	Cat. du câble	Nombre De Prises RJ45	Nombre de Panneaux de brassage RJ45	Nombre de Panneaux de brassage Optique	Nombre de jarretières optiques	Prises	Métrique En Cuivre (m)	Fonctionnel	Etat	Repérage
Labo. de recherche [redacted]	SR[redacted]	6	50	2	1	1	P01	20	Oui	Bon	Oui
		6					P02	20	Oui	Bon	Oui
		6					P03	20	Oui	Bon	Oui
		6					P04	17	Oui	Bon	Oui
		6					P05	17	Oui	Bon	Oui
		6					P06	16	Oui	Bon	Oui
		6					P07	28	Oui	Bon	Oui
		6					P08	28	Oui	Bon	Oui
		6					P09	25	Oui	Bon	Oui
		6					P10	22	Oui	Bon	Oui
		6					P11	37	Oui	Bon	Oui
		6					P12	31	Oui	Bon	Oui
		6					P13	31	Oui	Bon	Oui
		6					P14	35	Oui	Bon	Oui
		6					P15	31	Oui	Bon	Oui
		6					P16	22	Oui	Bon	Oui
		6					P17	17	Oui	Bon	Oui
		6					P18	14	Oui	Bon	Oui
		6					P19	13	Oui	Bon	Oui
		6					P20	13	Non	Bon	Oui
		6					P21	14	Non	Bon	Oui
		6					P22	14	Non	Bon	Oui
		6					P23	16	Non	Bon	Oui
		6					P24	16	Non	Bon	Oui
		6					P25	20	Non	Bon	Oui
		6					P26	20	Non	Bon	Oui
		6					P27	20	Non	Bon	Oui
		6					P28	20	Non	Bon	Oui
		6					P29	22	Non	Bon	Oui
		6					P30	22	Non	Bon	Oui
		6					P31	26	Non	Bon	Oui
		6					P32	27	Non	Bon	Oui
		6					P33	32	Non	Bon	Oui
		6					P34	33	Non	Bon	Oui
		6					P35	16	Oui	Bon	Oui
		6					P36	15	Oui	Bon	Oui
		6					P37	11	Oui	Bon	Oui
		6					P38	11	Oui	Bon	Oui
		6					P39	11	Oui	Bon	Oui
		6					P40	11	Oui	Bon	Oui
		6					P41	16	Oui	Bon	Oui
		6					P42	16	Non	Bon	Bon
		6					P43	11	Non	Mauvais	Non
		6					P44	11	Non	Mauvais	Non
		6					P45	9	Oui	Bon	Oui
		6					P46	16	Oui	Bon	Oui

		6					P47	8	**Oui**	**Bon**	**Oui**
		6					P48	11	**Oui**	**Bon**	**Oui**
		6					P49	29	**Oui**	**Bon**	**Oui**
		6					P50	58	**Oui**	**Bon**	**Oui**

1.5 Projet du réseau sans fil

Avec la dégradation et la limitation des connexions filaires existantes ainsi que le besoin exponentiel des utilisateurs à Internet surtout les étudiants, l'ENSIT s'est lancé dans la mise en place d'un réseau WIFI pour couvrir certaines zones à fortes besoins.

Cette partie sera dédiée à la description de la mise en place de ce projet.

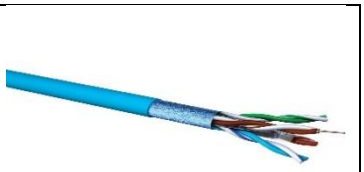
1.5.1 Equipements de l'infrastructure du réseau sans fil

Le matériel qui a été installé se présente comme suit :

a. Equipements Actifs

15 points d'accès D-Link DWL-6600 et DWL-6610	
1 contrôleur DWC2000	
1 switch POE D-Link- web smart switch 1210-24P	
3 switch POE D-Link-Web Smart switch -1210-10P	

b. Connectiques

Câble F/UTP écranté POE Legrand	
6 Jarretières FO LC/SC 50/125	
6 modules SFP	

1.5.2 Architecture Déployée

La topologie du réseau sans fil mise en place est en étoile. Les 15 points d'accès sont placés dans des zones éloignées les unes des autres, pour les interconnecter au contrôleur placé dans le RG dans la salle système, on a utilisé comme liens de connexions deux brins secondaires de la fibre optique déjà existante du réseau câblé. Ces fibres atteignent les sous répartiteurs qui se trouvent à proximité des zones à couvrir.

Tableau 27 : Répartition géographique des points d'accès

Zones à couvrir	Nombre de Points d'accès	Répartiteur où est installé le switch
Direction	1	
Amphi	1	
	1	
Labo. de recherche	1	
Labo. de recherche	1	
	2	
Labo. de recherche	1	

Labo. de recherche	1	
Salle	1	
Département	1	
Département	1	
Département	1	
Laboratoire	1	
Unités de recherches	1	

1.5.3 Adressage IP pour la connexion sans fil

Les appareils mobiles se connectent au réseau WIFI de l'école via les adresses automatiques attribuées par le DHCP du routeur.

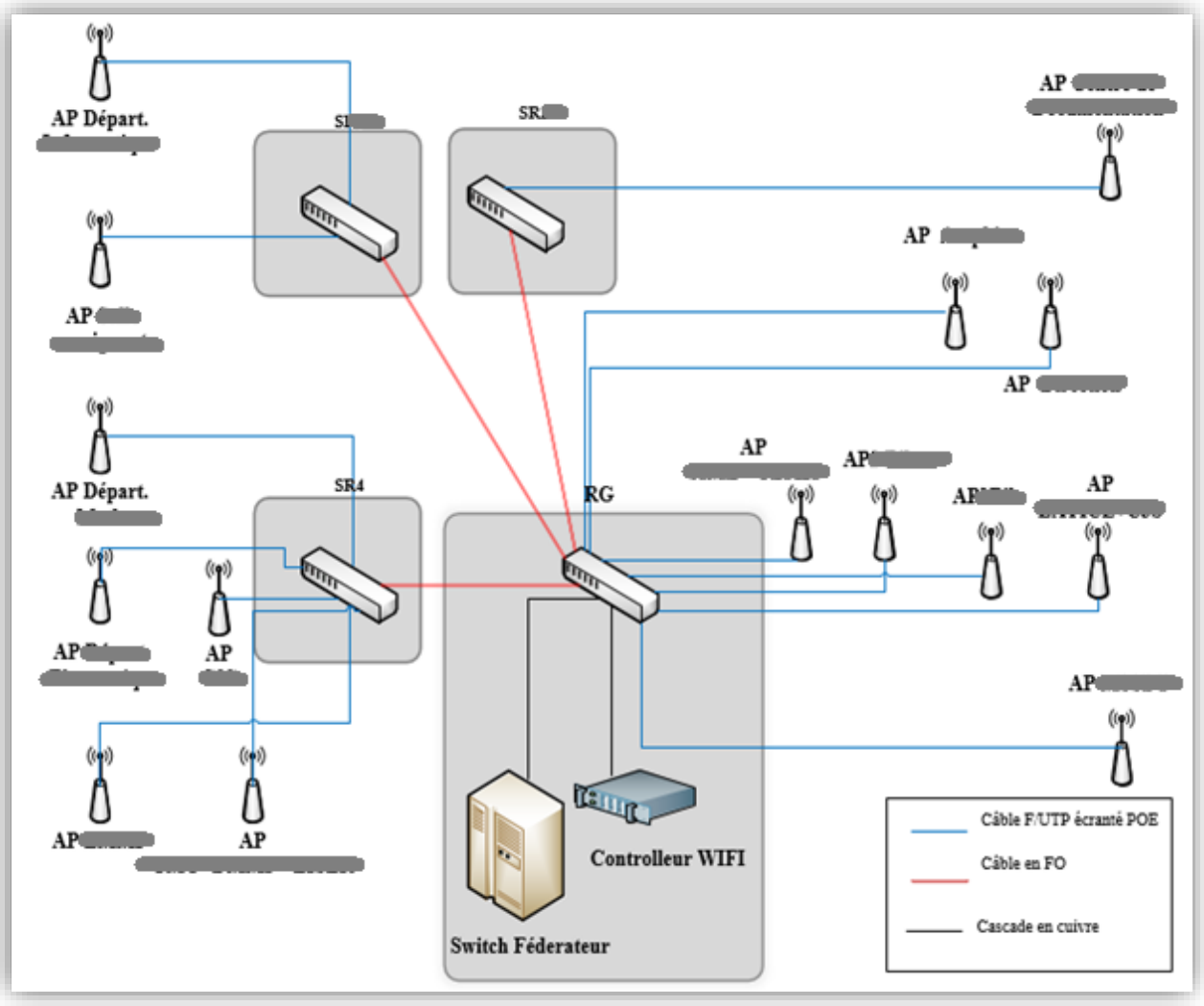


Figure 5 : Schéma synoptique du réseau sans fil

2. Aspects de sécurité existants

Dans cette partie, on va décrire les aspects de sécurité existants dans l'école selon quatre facettes :

2.1 Sécurité physique

- L'ENSIT est un établissement d'enseignement supérieur et de recherche, les accès à l'école ne peuvent pas être contrôlés vu le grand nombre d'étudiants : 1319 étudiants, en plus il y a toujours des visiteurs : enseignants, chercheurs, étudiants d'autres établissements, des chercheurs étrangers, des fournisseurs... ;
- L'école ouvre ses portes depuis 06 :30 h du matin jusqu'à 19 :00h ;
- La salle système est verrouillée avec clés et seules les personnes autorisées peuvent y accéder ;
- Les sous répartiteurs du système et les points d'accès WIFI sont placés dans des locaux (salles d'enseignement, laboratoires de recherche, bureaux d'administration) accessibles par les utilisateurs : étudiants, administratifs, enseignants et même les visiteurs ;
- Aucune redondance matérielle n'existe afin d'éviter l'arrêt des services en cas de problèmes ;
- Les prises du courant électrique ne sont pas ondulées, seul le routeur *Huawei Ar2200 séries* est ondulé via un onduleur *Huawei* ;
- Le système de vidéosurveillance installé ne couvre pas les zones sensibles (emplacement des points d'accès WIFI et des répartiteurs) et la résolution des caméras existantes est faible ;
- La climatisation de la salle système est assurée par un climatiseur domestique ;
- Les extincteurs d'incendies ne sont pas répartis sur tous les étages de l'école.

2.2 Sécurité du réseau

- Le réseau n'est pas segmenté en sous réseaux ;
- Il n'y a pas de pare-feu installé au niveau du réseau informatique de l'école et par conséquent aucun filtrage d'accès dans le réseau interne ni du trafic externe est assuré ;
- Le routeur et le commutateur d'accès ne sont pas accessible en local, chacun d'entre eux est géré par le Fournisseur qui l'a mis en place.

2.3 Sécurité des systèmes

La solution antivirale est fournie par le CCK et renouvelée chaque année, l'antivirus utilisé actuellement est ESET NODE 2017. Il assure un certain niveau de sécurité mais comme tout antivirus il n'est pas efficace à 100%. La mise à jour se fait régulièrement de façon individuelle pour chaque ordinateur (pas de serveur d'antivirus local).

2.4 Sécurité logique

Dans l'école plusieurs données sont critiques comme les données d'inscription, les notes des examens... La sauvegarde de ces données se fait manuellement sans aucune politique dédiée impliquant sécurité et intégrité.

Conclusion

Dans ce chapitre on a procédé à une description fine de l'infrastructure du réseau, et des aspects de sécurité présents dans l'école.

Dans le chapitre suivant on va procéder à l'analyse de l'état des lieux suivant l'étude organisationnelle, physique et technique des failles du système pour affiner d'avantage l'étude de l'existant.

Chapitre IV : **Analyse et Bilan**

Introduction

Ce chapitre nous permettra d'avoir une vision globale du réseau informatique dans son environnement ainsi que des facteurs qui l'influencent directement ou indirectement.

Dans une autre étape on va évaluer la sécurité informatique afin d'identifier les vulnérabilités du SI, pour parvenir à la fin à proposer des actions d'amélioration au niveau de l'infrastructure informatique et de la sécurité d'informations.

1. Audit Organisationnel et Physique

Il s'agit dans cette partie d'évaluer l'aspect organisationnel et physique en relation avec l'infrastructure informatique et la sécurité de l'information.

1.1 Objectif

L'objectif principal de cet audit est de comprendre l'organisation du système dans son environnement et la manière avec laquelle il est aménagé, géré et exploité. A la fin de cette phase, on pourra déterminer les dérivations par rapport aux bonnes pratiques

1.2 Approche adoptée

Ce volet d'audit est réalisé en se référant à des entretiens avec le personnel et les utilisateurs ainsi que des observations recueillis sur site.

Pour l'évaluation de la sécurité notre référentiel était la norme ISO 27002 :2013 formée de 14 chapitres contenant 114 mesures de sécurité qui représentent un recueil de « bonnes pratiques » de la Sécurité de l'Information applicables aux entreprises quel que soit leurs tailles ou secteur d'activité.

Cette phase d'audit a été effectuée moyennant un questionnaire (un exemplaire est joint en Annexe 1) cohérent avec ladite norme.

Figure 6 : Contenu de la norme ISO 27002 : 2013

1.3 Failles Organisationnelles et Physiques affectant le réseau

Lors de cette phase on a essayé de répertorier nos constatations selon les volets ci-dessous :

Aménagement du réseau

- Les travaux d'extension sont autorisés par les responsables suite aux demandes des utilisateurs sans aucun avis technique du spécialiste qui n'est même pas notifié pour mise à jour de l'existant de l'infrastructure, aussi ces extensions ne respectent pas la topologie existante et ne sont même pas contrôlé après mise en place ;
- Les utilisateurs sont libres de brancher du matériel actif (switch, point d'accès wifi) que l'école elle-même achète suite à leurs demandes sans recours au avis du technicien et sans se référer aux normes.

L'administration du réseau

- Le réseau informatique de l'école n'est pas considéré comme une entité ou un service à gérer par un agent ou une équipe spécialiste du domaine ;
- Il existe un technicien principal qui a été nommé responsable technique du réseau suite aux recommandations décrites dans la circulaire du ministre de l'Enseignement Supérieur, de la Recherche Scientifique et de la Technologie n° 36/09. Il est à noter que cette nomination

est purement formelle puisque son rôle se limite à la soumission des données techniques ou à la résolution des problèmes liés au réseau et à la coordination avec les opérateurs télécom et le FSI en ce qui concerne les problèmes de la liaison WAN. Toutefois il ne peut pas assurer le rôle de l'administrateur de réseau avec les moyens de bord qu'il dispose et les contraintes humaines, matérielles et logicielles ;

- Le présumé s'occuper du réseau n'a suivi aucune formation depuis son recrutement et pendant plus de 10 ans de carrière.

L'Exploitation du réseau

- Le réseau est exploité par différentes catégories d'utilisateurs : des administratifs, des enseignants et des étudiants, il est ouvert à tous de la même façon sans aucune restriction ou contrôle d'accès et il n'y a aucune politique appliquée ni notions de profils utilisateurs.

Développement

- Depuis 9 ans le réseau n'a pas subi de travaux de rénovation ou d'amélioration ;
- Quatre nouvelles salles ont été câblées en 2015 mais ne sont pas raccordées au système.

Maintenance

- Les travaux de maintenance ne sont pas régis, ils ne sont ni étudiés d'avance ni suivi au cours des travaux, ni contrôlés après finalisation ;
- La société qui répare les prises Ethernet et installe les nouvelles connexions est une société spécialiste en câblage téléphonique (contrainte budgétaire).

Réseau et environnement

- Suite à l'exécution des différents travaux à l'école : réaménagement des locaux, rénovation de l'électricité, déménagements des services… Le réseau informatique a subi plusieurs déformations : des moulures tombantes, des câbles coupés à mi-chemin, des baies déplacées, défoncés. Ces anomalies sont dues à l'inexistence d'une structure qui assure le suivi des travaux afin de réclamer et d'interdire ces dépassements.

1.4 Failles Organisationnelles et Physiques affectant la sécurité de l'information

Lors de cette phase on a essayé de répertorier nos constatations selon les volets ci-dessous :

Politique de sécurité de l'information

- L'ENSIT ne dispose pas d'une politique de sécurité formelle et bien définie, rédigée par des spécialistes, approuvée par les responsables et communiquée à tout le monde.

Organisation de la sécurité de l'information

- Inexistence d'agents spécialistes dans la sécurité dont les responsabilités concernent la protection des actifs et l'exécution des processus de sécurité spécifiques ;
- La mise en place des mesures de sécurité de l'information ne bénéficie pas d'un soutien clair de la direction de l'Ecole au moyen de directives claires ;
- Absence de comité de pilotage du SI.

Sécurité des ressources humaines

- Les utilisateurs ne sont pas informés par leurs devoirs et responsabilités en matière de sécurité de l'information chacun selon sa fonction ;
- Les utilisateurs ne sont pas sensibilisés aux règles et mesures générales de protection de l'information ;
- Inexistence de processus disciplinaire formalisé en cas de manquement aux règles de sécurité ou de violation de procédures ;
- Lors de la cessation ou d'un changement d'activité, les devoirs et responsabilités d'un collaborateur (interne ou sous contrat) ne sont pas définis et précisés dans une procédure ou document ;
- Lors de cessation ou de changement d'activité, il n'existe pas de règles concernant le retour à l'école des biens confiés au personnel ;
- Les droits d'accès des employés de l'école et des utilisateurs tiers à l'information ne sont ni supprimés ni changés à la fin de leur période d'emploi, mais plutôt communiqué au nouvel employé.

Gestion des actifs

- Les types d'actifs à identifier et inventorier sont définis à l'école. Mais l'inventaire des types d'actifs n'est pas à jour (dans le magasin de l'école on travaille toujours manuellement) ;
- L'inexistence des règles d'utilisation des biens et des services.

Contrôle d'accès

- Inexistence de politique de contrôle d'accès qui permet l'attribution ou le retrait des privilèges approuvée par la direction ;
- Les utilisateurs ne sont pas sensibilisés aux bonnes pratiques informatiques et aux mesures de sécurité (exemple : verrouiller leurs sessions et choisir les mots de passe...) ;
- Absence du contrôle par authentification en accédant au système ;
- Le réseau n'est pas segmenté en zones ;

Cryptographie

- Absence de chiffrement dans l'échange d'informations.

Sécurité physique et environnementale

- Il n'existe pas de protection physique des biens de l'établissement contre les incendies, la feu et autre forme de désastres (tout un laboratoire de recherche a été inondé) ;
- Absence de système de détection automatique d'incendies lié à des postes de surveillance pour les locaux sensibles ;
- Les installations de câblage ne sont pas schématisées afin de séparées les installations de courant fort du courant faible ;
- Les opérations de maintenance ne sont pas régies : y'a pas de diagnostic par les spécialistes ni de contrôle après finalisation de travaux ni de compte-rendu ou traces des travaux effectués ;
- Il n'existe pas de charte définie et documentée concernant la sortie des actifs en dehors des locaux de l'école.

Sécurité liée à l'exploitation

- Les opérations d'exploitation dans les différents services ne sont ni documentées ni mises à jour ;
- Absence de procédures de contrôle en vue de mettre à jour les équipements et systèmes dépassés ;
- Absence de définition de différents profils d'utilisateurs ;
- Absence de consignes interdisant l'utilisation de logiciels sans licences.

Sécurité des communications

- Absence de plan de sauvegarde, couvrant l'ensemble des objets à sauvegarder et la fréquence des sauvegardes ;

- Absence de définition des actions à mener par le personnel informatique pour prévenir, détecter et corriger les attaques.

Acquisition, développement et maintenance des systèmes d'information

- Inexistence d'une procédure de maintenance périodique des équipements ;
- Absence de procédure de validation lors d'acquisition d'actifs.

Relations avec les fournisseurs

- Inexistence de politique de sécurité destinée aux fournisseurs en les engageant à respecter la sécurité du SI dans les contrats.

Gestion des incidents liés à la sécurité de l'informatique

- Absence d'un système de gestion des incidents ;
- Absence d'un système de *reporting* des incidents liés à la sécurité de l'information ;
- Les employés ne sont pas formés aux comportements à prendre si un incident survient.

Aspects de la sécurité de l'information dans la gestion de la continuité d'activité

- Absence de plan de secours en cas d'interruption de services suite à des pannes, incidents ou sinistres ;
- Absence de solutions de restauration en cas de problèmes.

Conformité

- Inexistence d'une documentation explicite et mise à jour de toutes les exigences légales, réglementaires et contractuelles en vigueur et de leurs applications à l'école ;
- Procéder à des contrôles fréquents visant à vérifier que les logiciels installés sont conformes aux logiciels déclarés ou qu'ils possèdent une licence en règle ;
- Inexistence d'un contrôle de conformité technique ;
- Inexistence d'une procédure définissant une bonne utilisation des technologies de l'information par les employés ;
- Absence de notes qui précisent ce qui est toléré et les limites à ne pas dépasser dans l'utilisation des biens de l'école.

2. Audit Technique

Dans cette partie et après l'audit organisationnel et physique on va présenter les résultats de l'audit technique.

2.1 Objectif

L'audit technique consiste à l'analyse de toutes les composantes du SI pour relever les failles d'ordre technique existantes.

L'audit technique permet la détection des vulnérabilités suivantes :

- Les erreurs liées à l'architecture ;
- Les erreurs de configuration ;
- Les problèmes liés aux équipements d'interconnexion ;
- Les problèmes liés aux applications ;
- Les problèmes au niveau du trafic réseau.

2.2 Approche adoptée

On procèdera à analyser en profondeur le SI à l'aide d'un ensemble d'outils pour déceler les différentes vulnérabilités présentes dans le réseau informatique de l'ENSIT.

2.3 Audit de l'architecture du réseau

Dans cette partie on va essayer de déterminer le mappage du réseau pour avoir une description détaillée des différents protocoles existants à l'école, les flux réseau observés et les systèmes d'exploitation utilisés.

2.3.1 Inspection de la topologie du réseau

a) Outils utilisés

	Plate forme	Licence	Description
Network View	Windows	Evaluation	Reconnaissance réseau
LANsurveyor	Windows	Evaluation	Reconnaissance réseau

NetworkView est un outil de traçage de réseau qui cherche tous les nœuds TCP/IP du LAN et les cartographie, il permet aussi de vérifier le statut des nœuds sélectionnés en utilisant la

technique de l'ICMP polling, et permet également l'utilisation de Telnet, FTP et des connexions VNC à distance sur l'équipement réseau sélectionné.

LANsurveyor permet de tracer le réseau local. Il emploie pour le mappage plusieurs différentes méthodes, y compris ICMP, NetBIOS, et SNMP. Les cartes réseaux peuvent être imprimées ou exportées pour l'affichage ou éditer dans Visio ou d'autres programmes d'édition.

b) Résultats des scans

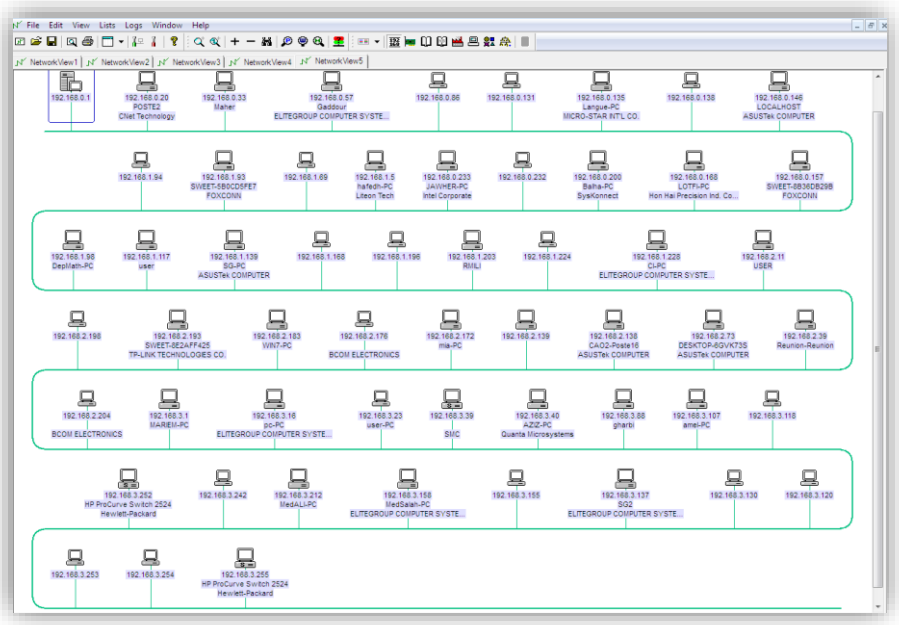


Figure 7 : Scan de l'adressage privé avec NetworkView

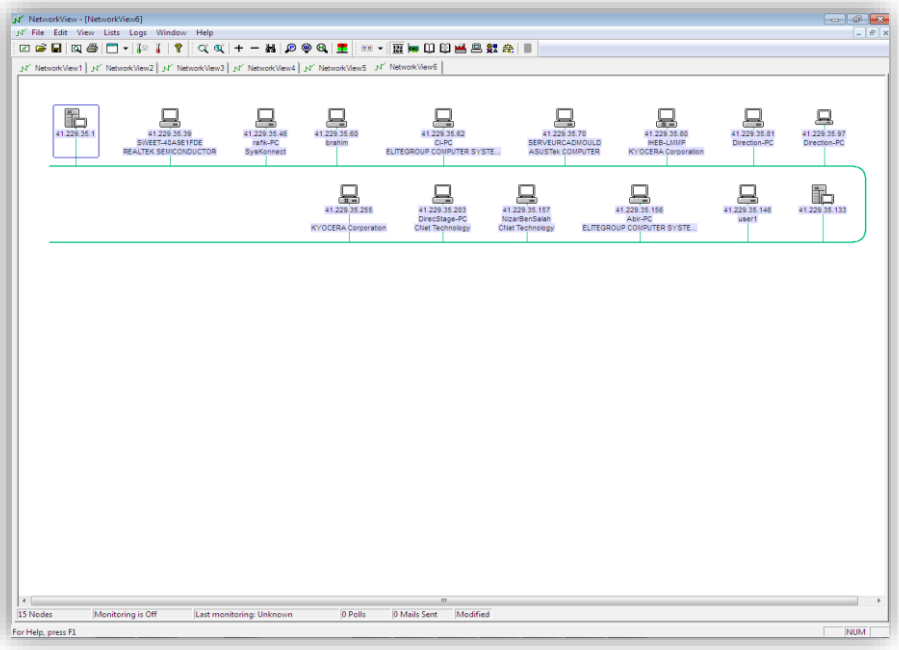


Figure 8: Scan de l'adressage public avec NetworkView

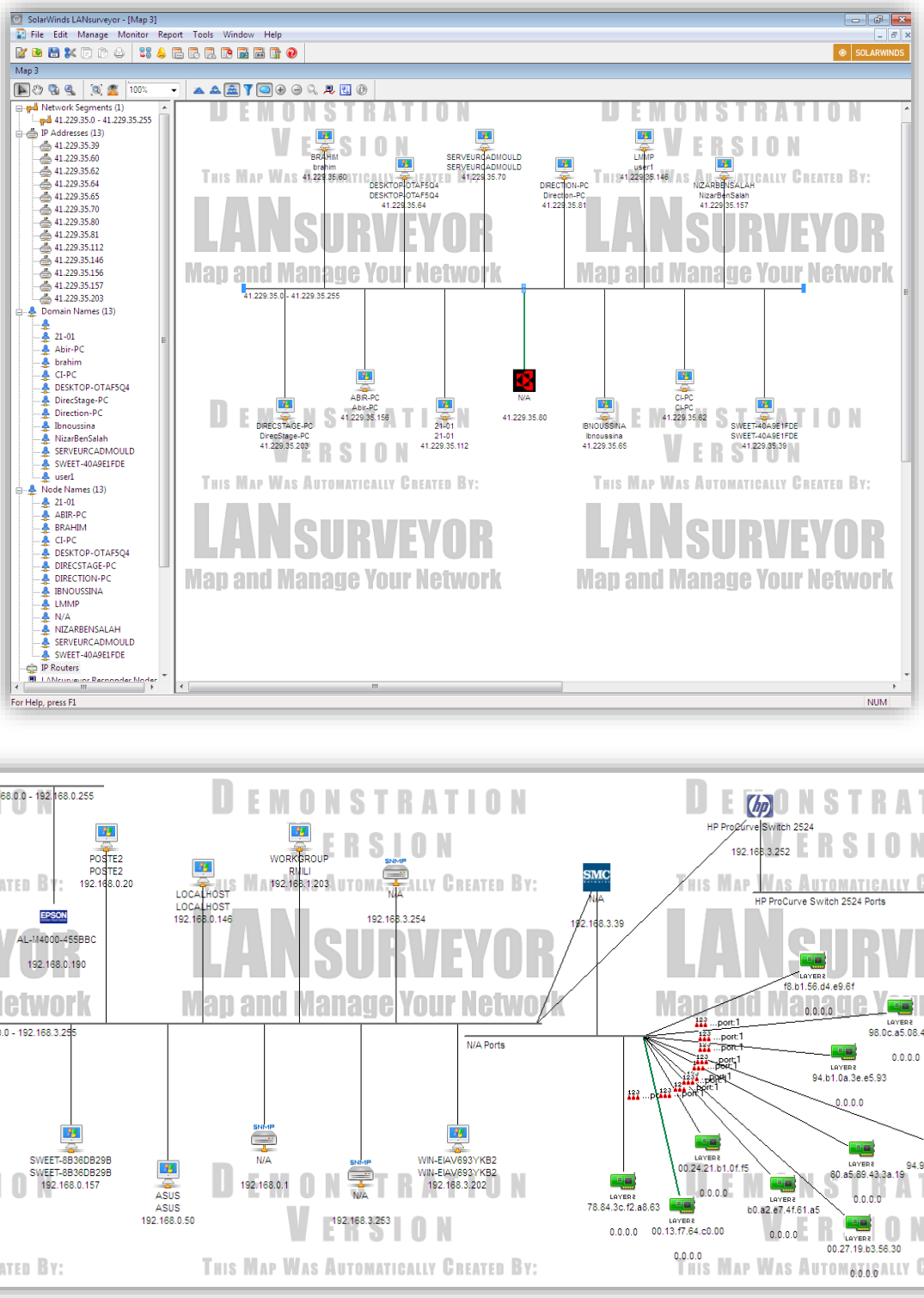


Figure 9 : Topographie des PC présents dans le réseau avec LANsurveyor

c) *Analyse des résultats*

- Le plan d'adressage présent sur le réseau local de l'école est formé de deux plages d'adresses :
    - *Une plage d'adresses publiques :* ***41.*** ***;***
    - *Une plage d'adresses privées :* ***192.*** ***.***
- Les adresses IP privées sont attribuées automatiquement, chaque machine envoie une demande qui sera acheminée vers le DHCP du routeur ;
- On remarque que la majorité des noms des machines (PC) portent le nom de la personne qui l'utilise ce qui facilite la connaissance des équipements critiques, cependant il existe certains serveurs et postes de travail qui ne sont pas nommés ;
- La configuration des cartes réseau au niveau des postes n'est pas protégée contre la modification, en effet, pour la plage d'adresses publiques chaque utilisateur est libre de faire entrer n'importe quelle adresse ce qui génère souvent des conflits d'adresses dans l'école.
- Une attaque de type IP Spoofing (usurpation d'identité) peut être facilement menée dans le réseau et peut entrainer une dégradation de performances et même générer un déni du service (remplacer l'adresse IP d'un poste du réseau par celle d'un équipement critique) ;
- L'outil ***NetworkView*** a dégagé certaines marques de constructeurs de cartes réseau, ce qui constitue une défaillance exploitable par des tierces personnes pour des attaques ciblées basées sur les vulnérabilités connues de ces marques.

2.3.2 Repérage des équipements d'interconnexion

Cette étape consiste à tracer le chemin de sortie des paquets vers le réseau externe, tout en essayant de détecter les équipements de contrôle d'accès présents sur le chemin.

a) *Présentation de la commande « Tracert » :*

L'utilitaire de ligne de commande « Tracert » permet de suivre le chemin emprunté par un paquet IP pour arriver à sa destination. Elle permet ainsi de dresser une cartographie des routeurs présents entre une machine source et une machine cible et de détecter les équipements de contrôle d'accès sur les frontières qui protègent le réseau local des intrusions externes.

La commande « Tracert » fonctionne par envoi de paquets d'écho ICMP.

b) *Résultat de la commande Tracert :*

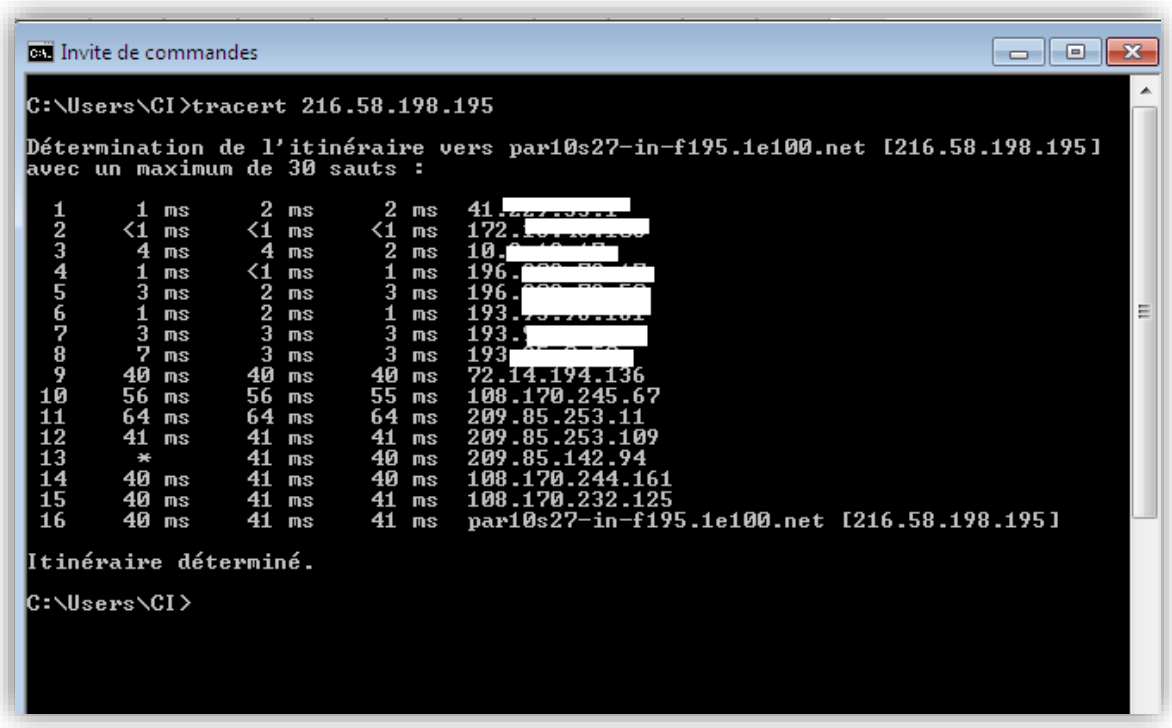


Figure 10 : Résultat de la commande "Tracert"

c) *Analyse des résultats*

La commande « Tracert » affiche les noms et adresses IP des routeurs successifs, précédés d'un numéro d'ordre et de temps de réponse minimum, moyen et maximum :

41. L'adresse du routeur de l'école ;

172. L'adresse WAN entre le routeur Huawei du CCK et le CPE (Customer Premises Equipment) de Tunisie Telecom ;

10. L'adresse BRAS (Broadband Remote Access Server) de Tunisie Telecom kasbah ;

196. Firewall du CCK kasbah ;

196. Routeur Frontal du CCK ;

193. Routeur Frontal ATI avec le CCK ;

193. Adresse routeur ATI ;

193. Adresse routeur ATI.

Les autres adresses IP sont des adresses externes au réseau Tunisien, pour cela le temps de latence est élevé.

2.3.3 Sécurité des échanges sur le réseau

Les échanges réseau ne sont pas chiffrés. L'utilisation d'un sniffer pourrait intercepter des mots de passe ou d'autres informations confidentielles.

a) Présentation de l'outil Wireshark :

	Plate forme	Licence	Description
Wireshark	Linux- Windows	Libre	Sniffer de trafic

Wireshark est un logiciel libre d'analyse réseau (sniffer), multi plate-forme, utilisé dans l'interception et l'analyse des paquets transitant sur un réseau informatique.

b) Résultat de l'outil Wireshark :

La figure ci-dessous représente l'interface d'interception des paquets de Wireshark :

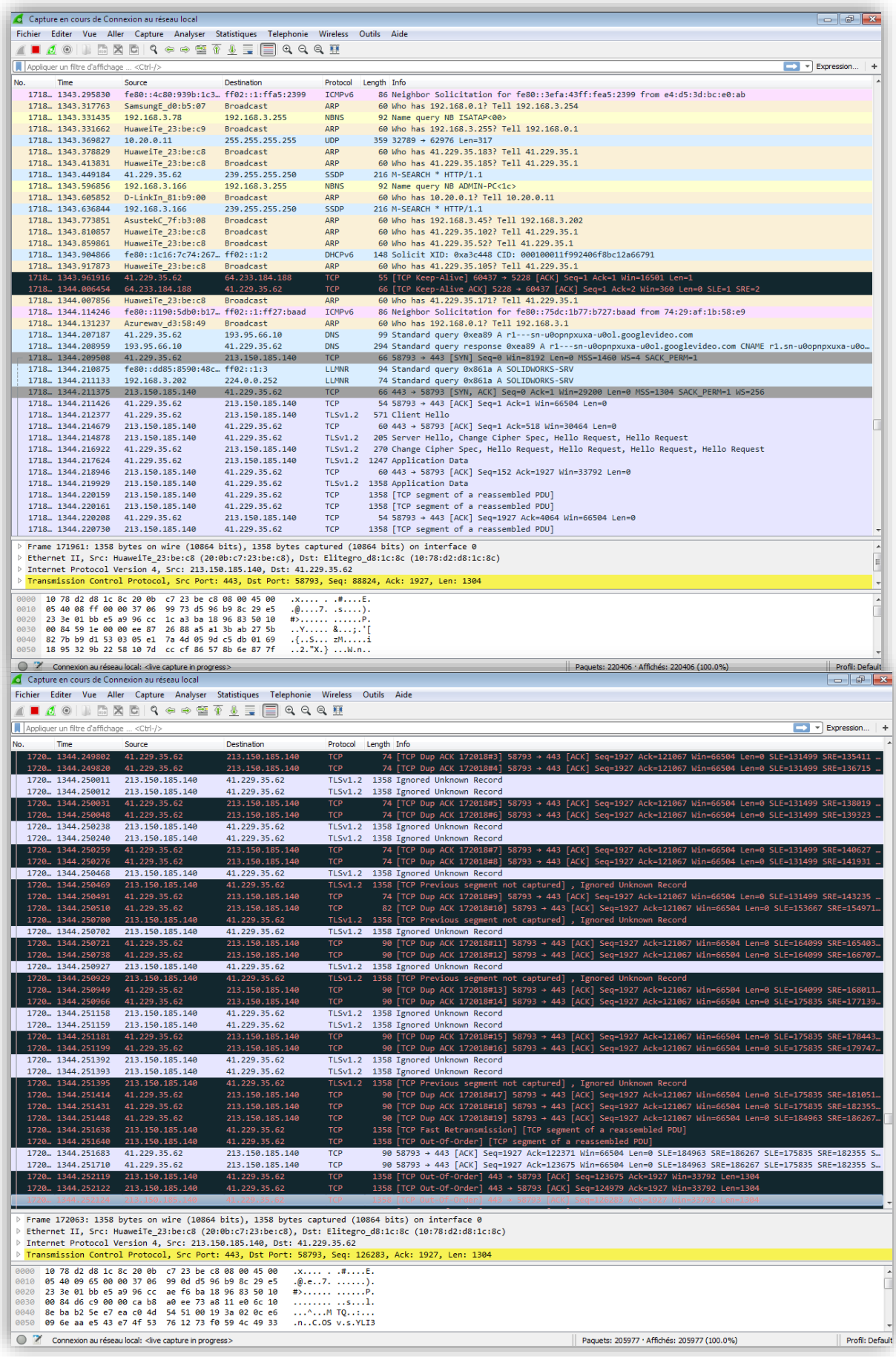


Figure 11 : Captures des flux avec Wireshark

c) Analyse des résultats :

L'installation de Wireshark sur le réseau et l'interception de données montrent que les échanges réseau ne sont pas chiffrés et qu'il n'y a pas d'anti-sniffer dans le réseau.

Wireshark liste les paquets IP capturés transitant sur le réseau, les détails sur un paquet sélectionné dans la 2ème fenêtre et le contenu du paquet en hexadécimale dans la troisième fenêtre.

On remarque un grand trafic broadcast dû au protocole ARP, tout cela génère des informations gratuites qui peuvent être exploitées par des personnes malintentionnées pour mener des attaques.

2.3.4 Mesure de la bande passante et son taux d'utilisation

a) Présentation de l'outil PRTG :

	Plate forme	Licence	Description
PRTG Network Monitor	Windows	Evaluation	Détecter les protocoles

PRTG (Paessler Router Traffic Grapher) est un logiciel qui supervise l'ensemble des systèmes, appareils et applications de l'infrastructure informatique à l'aide de certaines technologies (SNMP, SSH, requêtes http...), il permet grâce aux capteurs crées sur les appareils du réseau l'analyse de trames et la création de graphiques.

b) Résultat de l'outil PRTG :

On présente ici trois graphes illustrant la surveillance de la bande passante de la connexion à Internet dans l'école, pour cela on a configuré dans PRTG trois capteurs au niveau des trois interfaces du routeur pour mesurer le trafic à l'aide de SNMP.

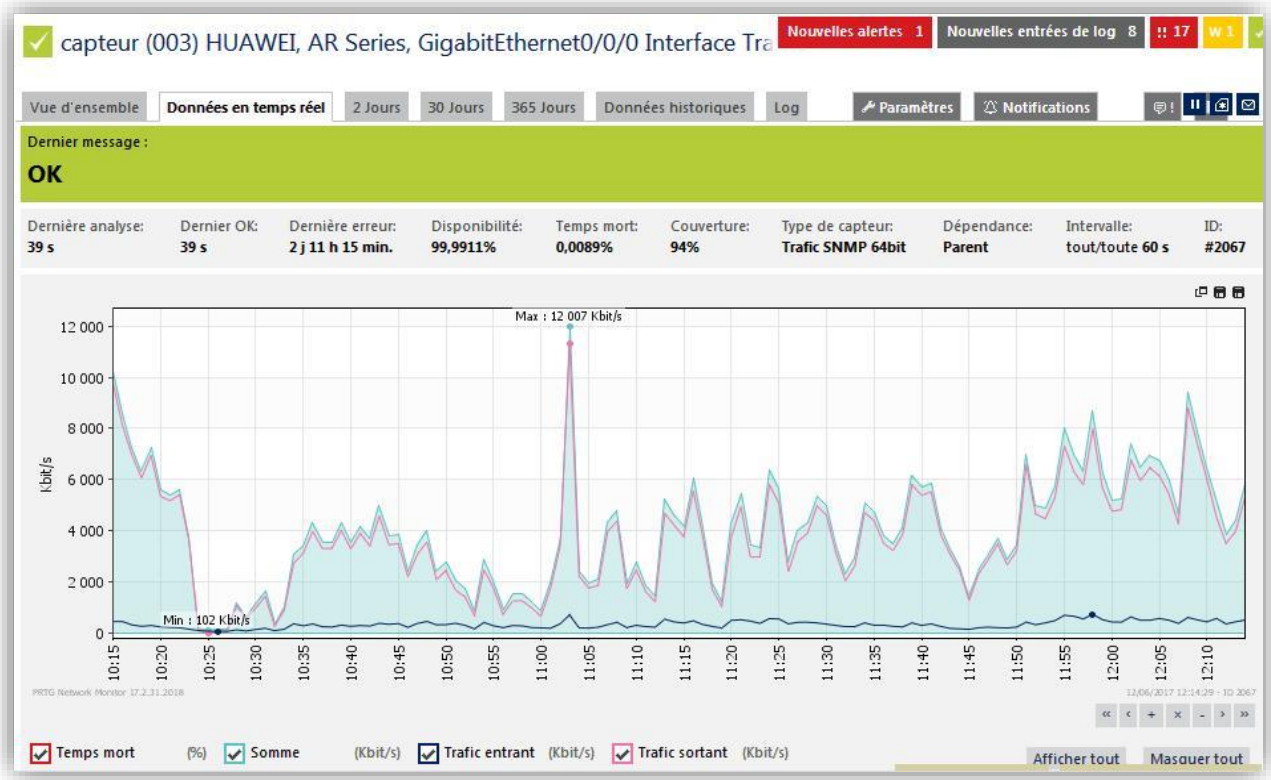


Figure 12 : Capteur PRTG sur le GE0/0/0 du routeur

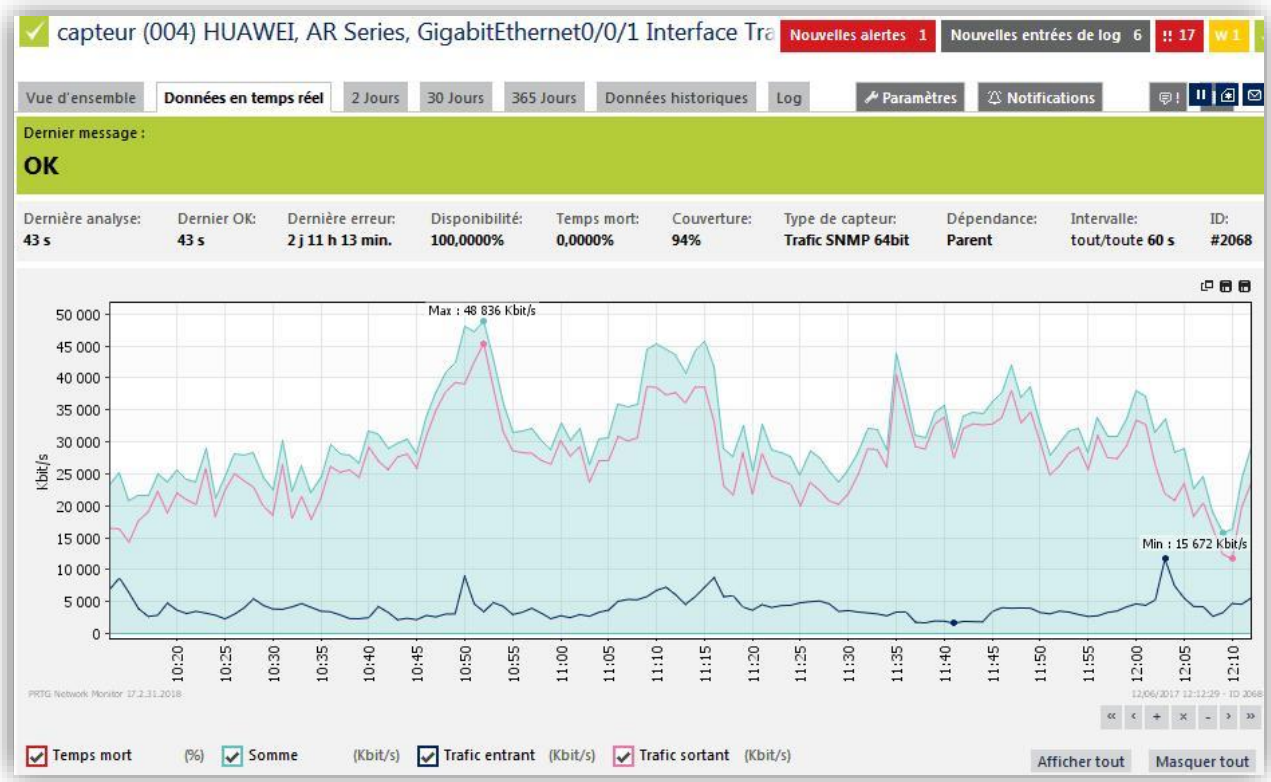


Figure 13 : Capteur PRTG sur le GE0/0/1 du routeur

Figure 14 : Capteur PRTG sur le GE0/0/2 du routeur

c) Analyse des résultats :

Les figures ci-dessus représentent le taux d'utilisation de la bande passante dans l'école sur les trois interfaces du routeur : le GE0/0/0, le GE0/0/1 et le GE0/0/2, le 12 juin 2017, pour une durée de 2 heures.

Le premier graphe illustre le taux de consommation de la bande passante des utilisateurs ayant des adresses publiques, le second celui des utilisateurs ayant des adresses privées et le troisième représente la somme ou la superposition des deux précédents graphes acheminés vers le commutateur de Tunisie télécom.

On remarque que l'interface GE0/0/0 achemine un trafic beaucoup moins important que celui de l'interface GE0/0/1 puisque la majorité des utilisateurs utilisent des adresses privées et non des adresses publiques. La somme des courbes des deux graphes relatifs aux GE0/0/0 et GE0/0/1 donnera le graphe relatif du GE0/0/2.

2.4 Audit de vulnérabilités

Dans cette partie de l'audit, on va utiliser un scanner de réseau afin de déterminer les vulnérabilités et essayer d'interpréter les différents résultats obtenus.

a) Présentation de l'outil GFI Languard :

GFI Languard permet d'explorer le réseau en utilisant la résolution NetBIOS et DNS des adresses IP des équipements du réseau.

Le scan sera effectué avec l'outil GFI Languard, en version d'évaluation limité à 25 postes.

	Plate forme	Licence	Description
GFI Languard	Windows	Evaluation	Scanner de Vulnérabilités

GFI Languard analyse et détecte les vulnérabilités d'un réseau. L'analyse se fait IP par IP pour identifier les problèmes de sécurité potentiels comme les ports ouverts qui peuvent être détournés, les applications non autorisées ou dangereuses qui les associe à des alertes de vulnérabilités, les connexions sans fil, les liens dangereux signalant une activité suspecte et les mises à jour manquantes...

b) Résultat de l'outil GFI Languard :

Dans les deux pages qui suivent on présente le résultat du scan avec l'outil GFI Languard : sur les deux plages d'adresses IP privée et publique avec les différentes vulnérabilités relevées :

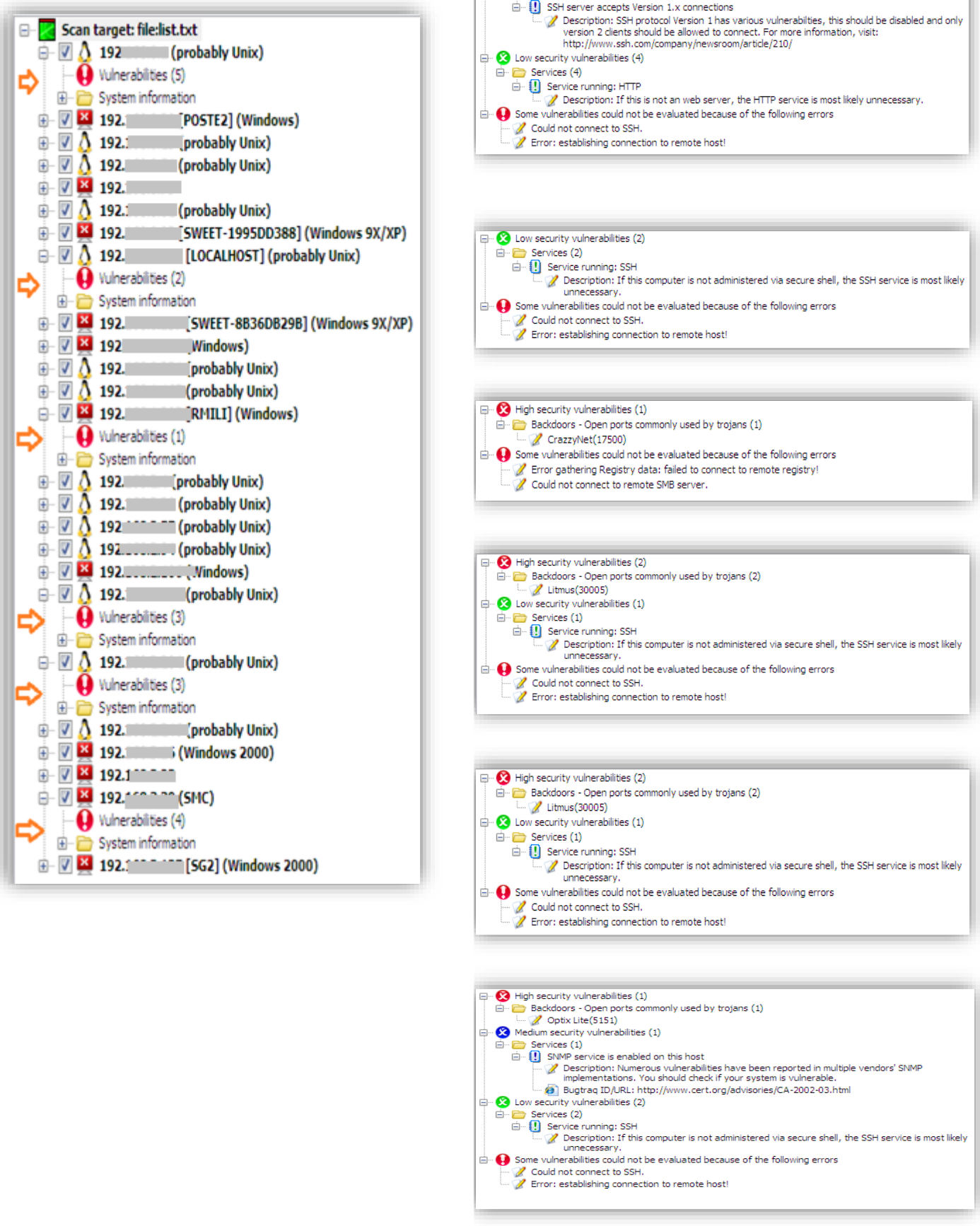
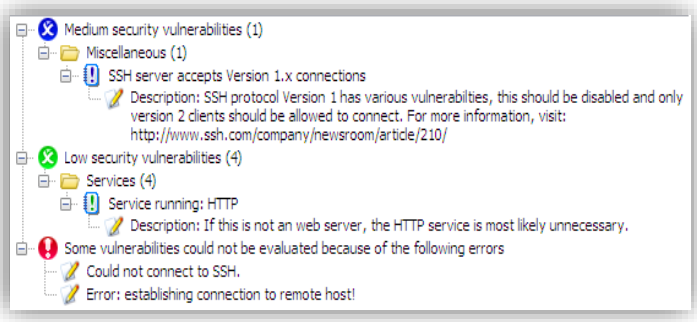
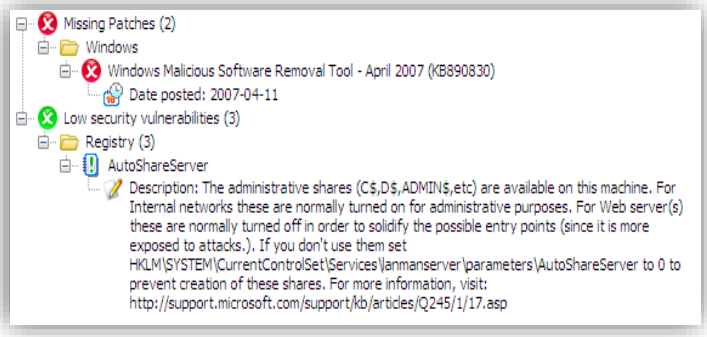
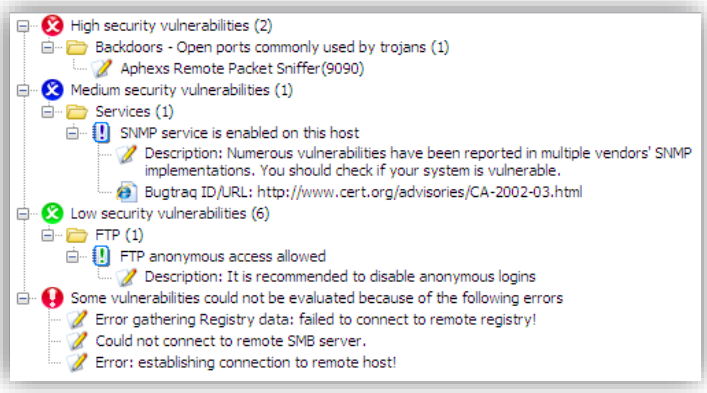


Figure 15 : Scan de vulnérabilités avec GFI Languard pour les adresses privées







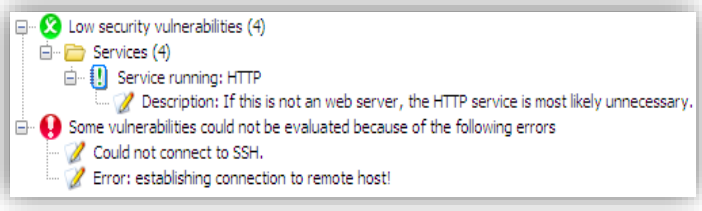


Figure 16 : Scan de vulnérabilités avec GFI Languard pour les adresses publiques

c) Analyse des résultats :

Le logiciel a fait un scan sur les deux réseaux (privé et publique), les résultats de scan donnent le type de système d'exploitation et tous les ports qui sont ouvert et qui peuvent être exploités par des troyens (trojans). Il classe ces vulnérabilités selon leurs criticités.

Le scan affiche le nom de la machine qui est dans la majorité des cas le nom de l'utilisateur, son adresse IP ainsi que le système d'exploitation installé.

Le sondage des ports avec la criticité des vulnérabilités associée :

Vulnérabilité d'ordre grave

- Aphexs Remote Packet sniffer (9090|TCP);
- CrazzyNet(1750|TCP) ;
- Litmus (30005|TCP) ;
- Optixelite(5151|TCP).

Ce sont des ports ouverts qui peuvent être utilisé par les troyens (trojans), il est recommandé de fermer ces ports afin d'empêcher une personne mal intentionnée de s'en servir.

Vulnérabilité d'ordre faible et moyenne

Certains services sont activés alors qu'ils ne sont pas exploités sur le réseau, ils doivent être désactivés pour qu'ils ne soient pas exploités dans des attaques, on a capturé les services suivants : SNMP, SSH, HTTP, SNMP, FTP, AutoShareServer (partage administratif sur le réseau).

2.5 Audit des composantes du réseau

Dans cette partie on va exposer nos remarques à propos de certaines composantes du réseau local :

2.5.1 Les Routeurs

- Les routeurs sont installés dans le répartiteur général qui se trouve dans la salle système qui héberge aussi un répartiteur propre au RNIA qu'utilise le service financier, la salle est fermée mais l'accès n'est pas surveillé avec un système de surveillance ;
- Toutes les manipulations et les tâches d'administration effectuées au niveau routeur se font à distance au niveau CCK ;
- Les mises à jour des IOS sont manquantes ;
- L'administration à distance s'effectue via le protocole Telnet ;

- Le mot de passe du routeur respecte les exigences de complexité.

2.5.2 Les Switchs

- Les switchs du réseau sont installés dans les différents sous répartiteurs qui se trouvent dans différents locaux non climatisés et dont l'accès n'est pas surveillé et certaines baies sont défoncées et ne se ferment pas à clés ;
- Certaines prises réseaux non utilisés ne sont pas désactivées ou débranchées à partir des répartiteurs.

2.5.3 Pare-feu

L'école ne dispose pas de Firewall, ni d'équipement matériel ou logiciel exerçant le filtrage de données afin de bloquer les intrusions provenant de l'extérieur de son LAN. Cependant le CCK veille à la sécurité des différents réseaux par la mise en place, le renouvellement et la mise à niveau de la plateforme de sécurité qui comporte un Système de Firewall en cluster et d'un système d'IPS (Intrusion Prevention System)au niveau des 4 points de présence « POP » du CCK, à savoir POP-Manar, POP-Manouba, POP-Kasbah et POP-Wardia (POP de secours), avec cette solution le réseau local de l'ENSIT est protégé de toutes attaques externes à l'RNU mais il est ouvert sur toutes les autres institutions universitaires.

Le CCK dans sa politique de sécurité, ouvre les ports standards tel que le WEB (accès aux sites web), le DNS service de résolution de noms, la messagerie (envoi et réception),

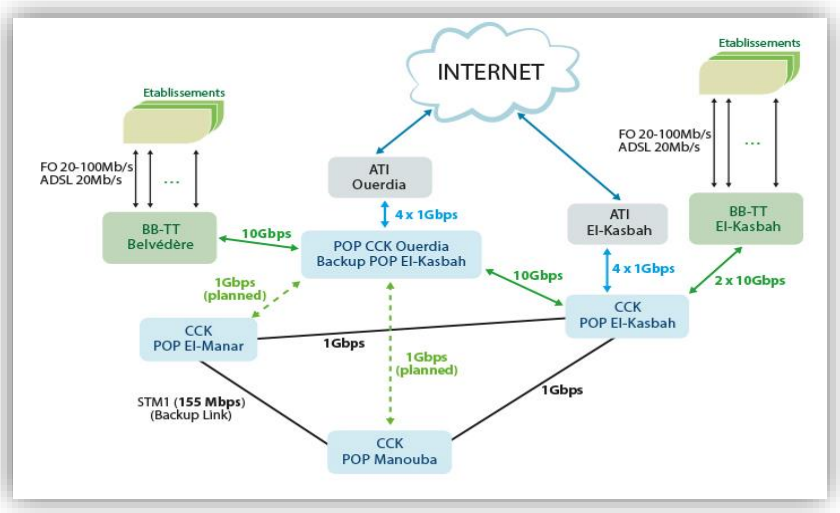


Figure 17 : Architecture du Réseau National Universitaire [10]

2.5.4 Pare-feu personnel sur poste de travail

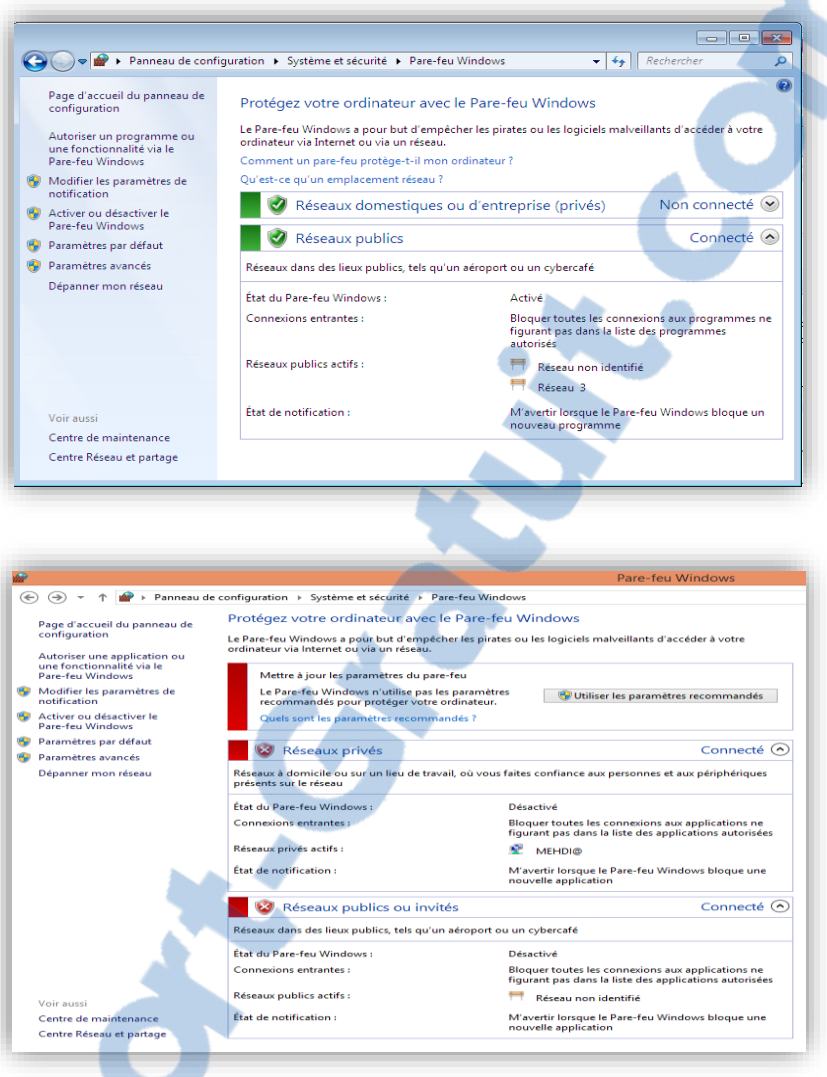


Figure 18 : Pares-feux Personnels sur les postes de travail

Les pares-feux des systèmes d'exploitation des postes ne sont pas tous activés, ça revient à l'utilisateur de l'activer ou de le désactiver.

2.5.5 La solution Antivirale

Pour se protéger contre les codes malveillants et les virus, le CCK fournit chaque année une solution de protection antivirale pour protéger le réseau local, cette application s'active en ligne et est centralisée au CCK pour administration.

Ci-dessous une étape de l'installation de l'antivirus qui achemine l'application à se connecter au serveur antiviral principal du CCK.

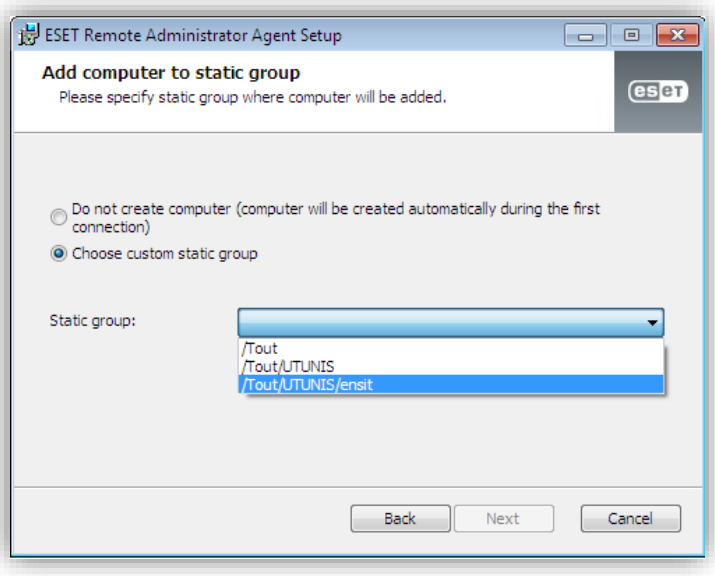


Figure 19 : Installation de l'agent d'administration distant de l'antivirus

Le fait que l'administration de la solution antivirale n'est pas locale, on ne peut pas s'assurer de la présence de l'antivirus sur tous les postes de travail et de l'installation des mises à jour de la base de connaissances de l'antivirus sur tous les postes.

On ne peut pas imposer aux utilisateurs nomades l'installation de l'antivirus de l'école ni pouvoir les obliger à installer un antivirus licencié et pertinent.

2.6 Audit applicatif

La notion de sécurité d'information a été fondée pour garantir la pérennité des informations et leurs intégrités et par défaut on doit parler de la sécurité des applications utilisées pour traiter ces informations.

Une application est considérée sécurisée selon son taux de disponibilité, son efficacité dans le traitement de l'information, l'intégrité de données traitées et sa sureté en termes d'accès.

a) Outils utilisés

Nous avons fait une inspection visuelle, en plus d'entretien avec les employés vu que l'école ne dispose pas d'applications.

b) Identification des applications critiques

- Le traitement des notes d'examens se fait jusqu'à nos jours via des feuilles Microsoft Excel avec des Macros pour faire les différentes opérations de calcul des moyennes, ces fichiers se trouvent sur des PC non connectés au réseau LAN de l'école pour éviter

toutes sortes d'erreurs ou problèmes liés à la sécurité, tout en effectuant des sauvegardes périodiques. En parallèle l'école a acheté un progiciel pour gérer l'ensemble des activités de l'école : gestion des formations, gestion des étudiants/enseignants, planification… y compris l'examen, encore en cours de mise en place et paramétrage. L'application est full-web et est hébergée sur des serveurs externalisés, l'accès se fait avec login et mot de passe.

- La bibliothèque de l'ENSIT est entrain de déployer comme toutes les universités tunisiennes le projet « Biruni » qui a pour objectif l'implémentation du catalogue collectif regroupant les fonds documentaires des bibliothèques universitaires. L'accès à cette application se fait par reconnaissance par adresses IP qui doivent être obligatoirement publiques (3 adresses de l'école sont reconnues pour cette application) plus une authentification par login et mot de passe.
- Les différents services comme la direction générale, la direction des stages, la direction des études, le service de ressources humaines, la scolarité utilisent tous les outils Microsoft Office (Word et Excel) pour le traitement de données.
- Le Magasin de l'école utilise encore des classeurs (travail manuscrit) pour gérer les stocks et les biens de l'école.
- L'ensemble des applications du service Financier qui assure le suivi des marchés, les missions à l'étranger, la gestion de trésorerie, sont inclut dans le pack assuré par le Centre National Informatique CNI (ADEB, INSAF, ...). Ces applications sont hébergées dans des serveurs au CNI et fonctionnent via une infrastructure séparée. Le réseau RNIA a été renouvelé : un Firewall a été mis en place, le débit a été élevé, l'accès aux applications est sécurisé avec login et mot de passe et l'adressage est différent de celui de l'école.

c) *Constatations*

Contrôle d'accès applicatif

- Aucun contrôle d'accès n'est mis en place.
- Il n'existe pas de politique concernant la gestion des mots de passe, en plus le choix des mots de passe ne respecte pas les bonnes pratiques.

Contrôle de l'intégrité des données :

- Absence d'une stratégie de définition de données sensibles.
- Absence de protection spécifique des données sensibles.

Contrôle de la confidentialité des données :

- Absence d'une solution approuvée de chiffrement.

Disponibilité des données :

- Absence d'une étude détaillée des scénarios de perte des fichiers sensibles.

Continuité de fonctionnement :

- Absence d'un plan de continuité des activités.

Détection et gestion des incidents et anomalies applicatives :

- Inexistence d'une étude des comportements anormaux et d'une mise en place de détecteurs d'actions illicites.
- Absence de fonctions de surveillance et de tableaux de bords des événements anormaux.
- Pas de définition formelle des solutions et des actions à entreprendre en cas d'alerte.

Conclusion

Après l'achèvement de la partie évaluation de notre mission d'audit, composée de l'évaluation organisationnelle, physique et technique, on a pu relever certaines anomalies de l'infrastructure informatique et failles qui menacent l'intégrité et la sécurité du SI.

Dans le prochain chapitre, on essayera de citer des recommandations précises et définir un plan d'action pour améliorer et optimiser l'exploitation de l'environnement de travail.

Chapitre V : **Recommandations et Solutions déployées**

Introduction

Dans ce dernier chapitre, on va exposer une multitude de solutions et correctives qui sont appropriées à l'état actuel du réseau de l'ENSIT. La mise en place de ces solutions et correctives aidera à arrêter la dégradation progressive que subit le réseau, à son amélioration et à assurer sa sûreté et la sécurité de ses données et échanges.

1. Recommandations Organisationnelles et Physiques

On va citer dans cette partie les recommandations organisationnelles :

1.1 Politiques et Chartes Informatiques

- L'ENSIT est appelé à établir sa propre politique de sécurité et formuler sa charte informatique qui doit être approuvée par les responsables et publiée aux usagers ;
- Chaque usager doit accepter et signer son adhésion à la charte et respecter les règles d'utilisation des ressources informatiques et de la confidentialité de l'information ;
- Cette charte doit être vérifiée et mise à jour périodiquement afin de tenir compte de tout changement (changement de l'infrastructure, problèmes encourus, nouvelles vulnérabilités...) ;
- Formuler une charte de sécurité destinée aux fournisseurs en les engageant à respecter la sécurité du SI pendant leurs travaux à l'école ;
- Formuler une charte de sécurité de données contrôlant la sortie des actifs en dehors des locaux de l'école.

1.2 Organisation

- Création d'un Service informatique au sein de l'administration de l'ENSIT, formé d'une équipe de spécialistes pour maintenir le système dans les règles de l'art et s'entraider à son amélioration et optimisation ;
- Nommer un agent responsable de la sécurité d'information au sein de l'école ;
- Programmer des formations de spécialité pour l'équipe informatique ;
- Informer le service informatique des différents chantiers au sein de l'école pour assurer le suivi des travaux et interdire les dépassements atteignant l'architecture, la performance et l'intégrité et éviter les déformations qui peuvent affecter les différentes composantes du réseau.

1.3 Sensibilisation des utilisateurs

- Préciser aux usagers leurs devoirs et responsabilités en matière d'exploitation des ressources informatiques ;
- Sensibiliser les usagers aux règles et mesures générales de protection de l'information et aux bonnes pratiques informatiques ;
- Etablir une procédure formée de règles concernant le retour à l'école des biens confiés au personnel lors de cessation ou de changement d'activité ;
- Définition des actions à mener par le personnel informatique, pour prévenir, détecter et corriger les attaques ;
- Définition d'un processus disciplinaire formalisé en cas de manquement aux règles de sécurité ou de violation de procédures.

1.4 Gestion des actifs

- Identifier et inventorier les types d'actifs présents à l'école et définir les règles d'utilisation.

1.5 Contrôle d'accès

- Segmentation du réseau ;
- Création de différents profils pour les utilisateurs ;
- Mise en place d'un système de surveillance dans les locaux techniques.

1.6 Chiffrement de données

- Acquisition d'un certificat électronique pour sécuriser les mises à jour du site Internet de l'école.

1.7 Sécurité physique et environnementale

- Mise en place d'un système de protection physique des biens de l'établissement contre les incendies et les désastres ;
- Installation de système de détection automatique d'incendie lié à des postes de surveillance pour les locaux sensibles ;
- Schématiser toutes les installations de câblage afin de les prendre en considération pendant les travaux de chantiers (passage de courant fort et courant faible) ;
- Certains équipements requièrent des systèmes d'Antivol ;
- Assurer la climatisation pour les locaux contenant des répartiteurs.

1.8 L'exploitation

- Documenter les différentes opérations de traitement et d'exploitation de l'information dans les différents services et les mettre à jour périodiquement.

1.9 Acquisition, développement et maintenance des Systèmes d'Information

- Organiser les opérations de maintenance et d'extension du réseau, qui doivent passer forcément par les spécialistes de l'école pour diagnostic, étude, suivi et contrôle pendant les travaux et validation après finalisation ;
- Arrêter l'achat de matériel actif au profit des utilisateurs et les sensibiliser aux problèmes qu'ils créent en mettant en place ces équipements et des dommages qu'ils encourent au SI ;
- Les opérations de maintenance et d'extension du réseau de l'école doivent forcément être réalisés par des fournisseurs spécialistes du domaine informatique ayant le profil d'intégrateurs des services des technologies de l'information et de la communication ayant obtenu l'agrément accordé par le Ministère des Technologies de la Communication et de l'Economie Numérique pour exercer des travaux selon les normes en vigueur ;
- Développer une procédure périodique d'entretien et de maintenance des équipements.

1.10 Gestion de la continuité d'activité

- Concevoir des plans de sauvegarde définissant les objets à sauvegarder et la fréquence des sauvegardes pour les données sensibles de l'école et l'ensemble des configurations du système ;
- Mise en place des plans de secours en cas d'interruption de services suite à des pannes, incidents ou sinistres ;
- Développer des solutions de restauration rapides en cas de problème.

1.11 Conformité

- Rédiger une documentation explicite et mise à jour de toutes les exigences légales, réglementaires et contractuelles en matière de l'informatique et essayer de les appliquer à l'école ;
- Planifier un contrôle périodique de conformité technique ;
- Chercher des solutions pour les licences des logiciels utilisés ;

2. Recommandations Techniques

On va citer dans cette partie les recommandations techniques :

2.1 Au niveau Réseau

- Démontage complet de l'ancien réseau ;
- Entretien et maintenance des baies défoncées ;
- Renouveler les segments de l'ancien réseau et les prises Ethernet défectueuses ou étendre le réseau wifi pour couvrir ces zones ;
- Remplacer le matériel actif dépassé par du nouveau ;
- Cascader les 4 nouvelles salles câblées en 2015 au système ;
- Eliminer les cascades en cuivre et les remplacer par des cascades en FO ;
- Corriger l'état des connexions qui ne respecte pas la topologie du réseau.
- Segmenter le réseau en VLANs séparés : pour l'enseignement, l'administration et les étudiants ;

2.2 Au niveau Sécurité

- Acquérir un Firewall logiciel ou matériel ;
- Déployer une solution de sécurité pour le réseau WIFI ;
- Instaurer une procédure de contrôle d'accès au SI par la mise en place d'un serveur d'authentification et la création de différents profils.

2.3 Au niveau Services

- Mise en place d'un serveur DNS pour garantir la rapidité de connexion ;
- Virtualisation : Acquisition de matériel pour déployer un Cloud privé ;
- Equiper des laboratoires « High-tech » par différents types d'équipements informatiques de pointe pour les exploiter dans le cursus de formation des ingénieurs, et dans les évènements organisés par l'école ;
- S'ouvrir sur le projet Eduroam : « Education roaming », qui est en cours de déploiement par le CCK et qui assure un accès sans fil sécurisé à Internet, pour les utilisateurs des établissements d'enseignement supérieur et de recherche, à travers le monde, dans les sites des adhérents, en utilisant les mêmes paramètres de connexion.

3. Plan d'action

Tableau 28 : Plan d'action

À court terme	✓ Effectuer les différentes opérations de renouvellement, d'entretien, de correction et de maintenance des différents composantes et segments du réseau en respectant les normes en vigueur ; ✓ Innovation et réaménagement de la salle Système et réaménagement des locaux hébergeant des équipements ; ✓ Création d'un Service informatique formé de spécialistes pour maintenir le système dans les règles de l'art et désigner un Responsable de Sécurité du Système d'Information (RSSI) ; ✓ Programmer de façon régulière des formations de spécialité pour l'équipe informatique ; ✓ Organiser les opérations de maintenance, d'entretien du SI ainsi que celles d'acquisition de matériel informatique ; ✓ Assurer le suivi de chantiers pouvant impacter le SI ; ✓ Sécuriser l'accès au réseau WIFI ; ✓ Acquisition d'un Firewall logiciel ou matériel ; ✓ La mise en place d'un serveur d'authentification ; ✓ Elaboration d'une charte informatique ; ✓ Planifier des formations et faire circuler des notes périodiquement au profit des utilisateurs rappelant les bonnes pratiques de l'usage du SI et la sécurité de l'information ; ✓ Mise en place d'un système de protection physique des biens de l'établissement contre les incendies et les désastres ; ✓ Installation d'un système de détection automatique d'incendie lié à des postes de surveillance pour les locaux sensibles.
À moyen	✓ Acquisition d'un certificat électronique pour sécuriser les mises à jour du site Internet de l'école ; ✓ Création de différents VLANs ; ✓ Mise en place d'un serveur DNS.
À long terme	✓ Documenter les différentes opérations d'exploitation dans les différents services et les mettre à jour périodiquement ; ✓ Planifier un contrôle périodique de conformité technique ; ✓ Réaliser l'inventaire complet et régulier des biens et les classifier tout en mettant en place les règles d'utilisation ; ✓ Création d'une procédure formée de règles concernant le retour à l'école des biens confiés au personnel lors de cessation ou de changement d'activité ; ✓ Mettre à jour périodiquement les inventaires ; ✓ Equiper des laboratoires « High-tech » par différents types d'équipements informatiques de pointe ; ✓ Virtualisation : Déploiement d'un Cloud privé ; ✓ Rédaction de documentation pour les différents actifs composant le SI, schématisation des plans pour toutes les installations de câblage et révision et mise à jour périodique de ces documents ; ✓ Collecte et Classification des différentes exigences légales et réglementaires en relation avec le SI.

4. Les solutions déployées

Parmi les nombreuses solutions à développer dans le réseau de l'ENSIT, on a choisi de déployer trois recommandations citées à la fin de cette mission d'audit :

1- Rédiger la première charte informatique pour l'ENSIT ;

2- Mettre en place une solution de Firewalling ;

3- Sécuriser l'accès au réseau WIFI.

Cette partie a été développée malgré les contraintes matérielles et logicielles avec les moyens de bords existants.

4.1 Chartes informatiques pour l'ENSIT

Avec la diversité des utilisateurs du Système Informatique de l'ENSIT, la rédaction d'une charte qui régisse l'utilisation des outils informatique est un acte fondamental.

Cette charte servira à informer les utilisateurs de leurs droits et leurs devoirs, mais aussi à protéger le capital informatique de l'école et surtout garantir un bon niveau de service et sécurité.

Les chartes citées ci-dessous sont jointes à ce rapport dans l'annexe 3 :

- « La charte informatique de l'ENSIT » ;
- « Charte de bon usage du réseau WIFI » ;
- « Charte de la Sécurité du Système d'Information de l'ENSIT dédiée aux fournisseurs »

4.2 Installation d'un Firewall

Un firewall est soit un équipement physique ou une application qui permet de contrôler les connexions entrantes et sortantes sur un réseau afin d'assurer une politique de sécurité via des contrôles d'accès.

4.2.1 Choix de la solution

On a choisi ***Pfsense2.3.4*** comme pare-feu, une solution qui correspond le mieux à notre profil : une solution open source basé sur le système d'exploitation FreeBSD, ayant une

interface graphique de gestion, un niveau de sécurité considérable et une stabilité approuvée, tout en intégrant plusieurs autres services : DHCP, Captive Portal, IDS, IPS, etc…

4.2.2 Installation de Pfsense

Le pare-feu doit permettre la connexion aux utilisateurs des adresses publiques et aux utilisateurs des adresses privés aussi bien qu'aux utilisateurs du réseau sans fil.

L'ensemble des figures ci-après présente les différentes étapes d'installation de l'interface WAN via la console de Pfsense :

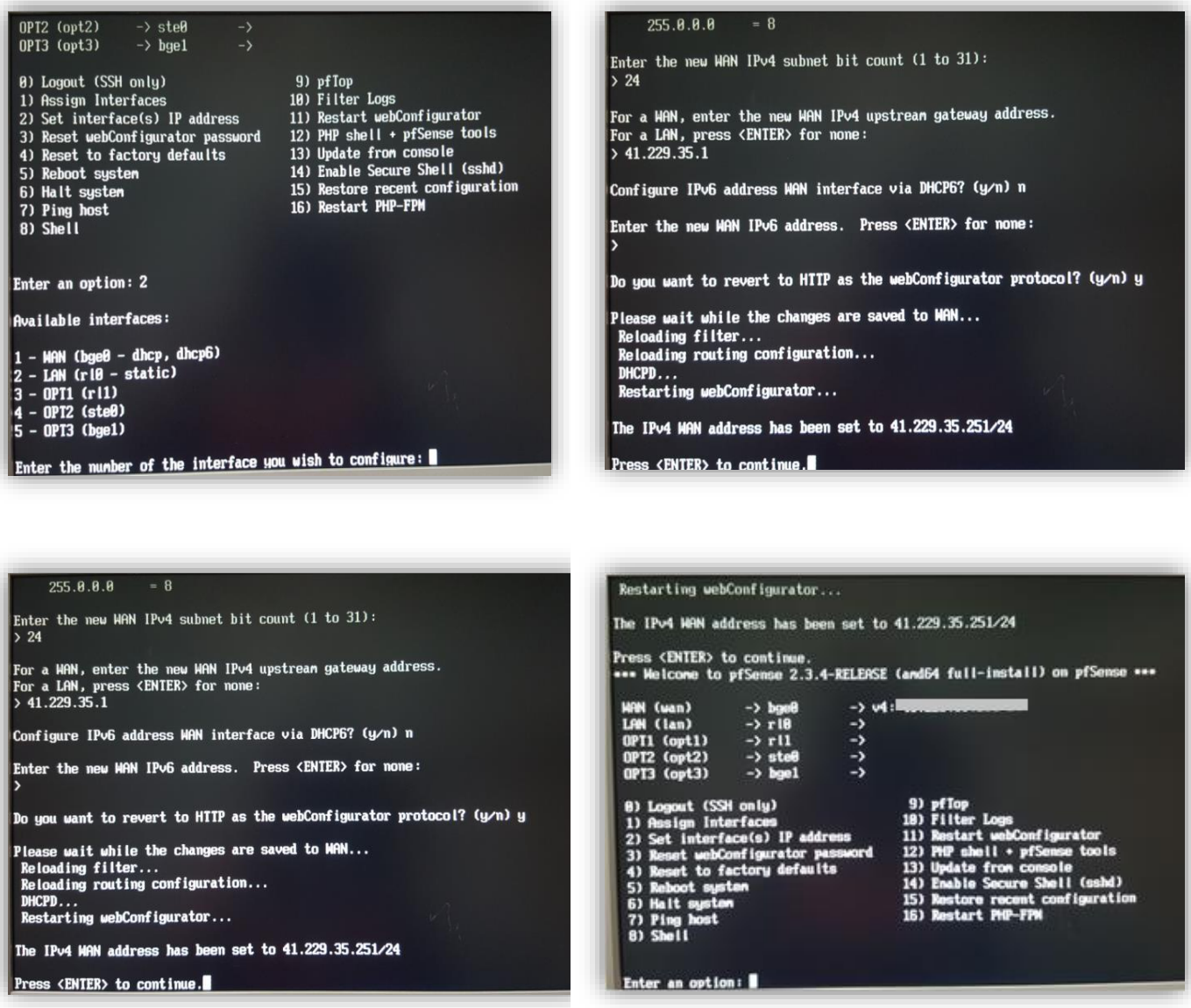


Figure 20 : Etapes de configuration de l'interface WAN dans le firewall

Figure 21 : Ecran d'accueil de Pfsense après configuration des trois interfaces

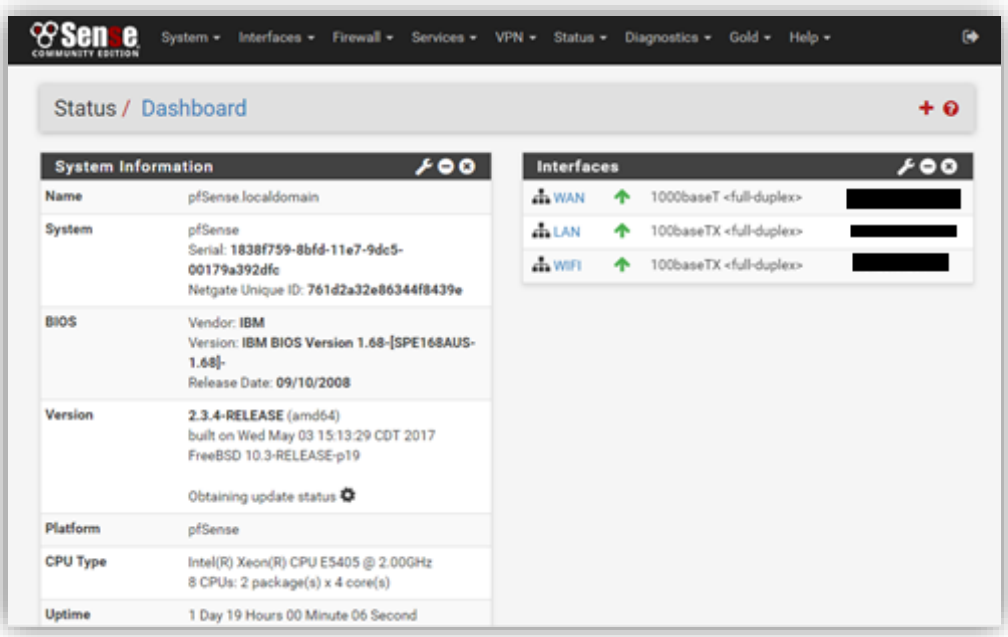


Figure 22 : Interface graphique de Pfsense

4.2.3 Configuration du serveur DHCP

Via l'interface graphique du Pfsense on active le service du serveur DHCP pour le réseau LAN et configure les étendues d'adresses à affecter aux utilisateurs du réseau local.

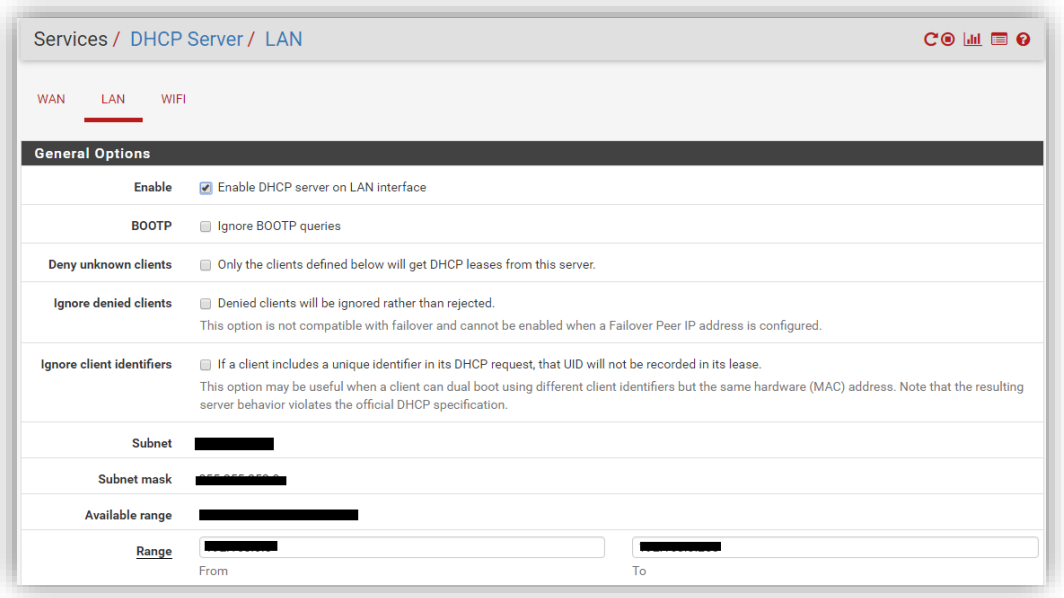


Figure 23 : Activation du DHCP sur l'interface LAN

4.2.4 Alias, Règles d'accès et NAT

Après configuration des interfaces du firewall et activation du DHCP pour le LAN, il faut instaurer l'ensemble des règles qui permettront le fonctionnement du réseau et la sécurité des connexions.

a) Alias :

La création d'Alias simplifie la mise en place des règles d'accès.

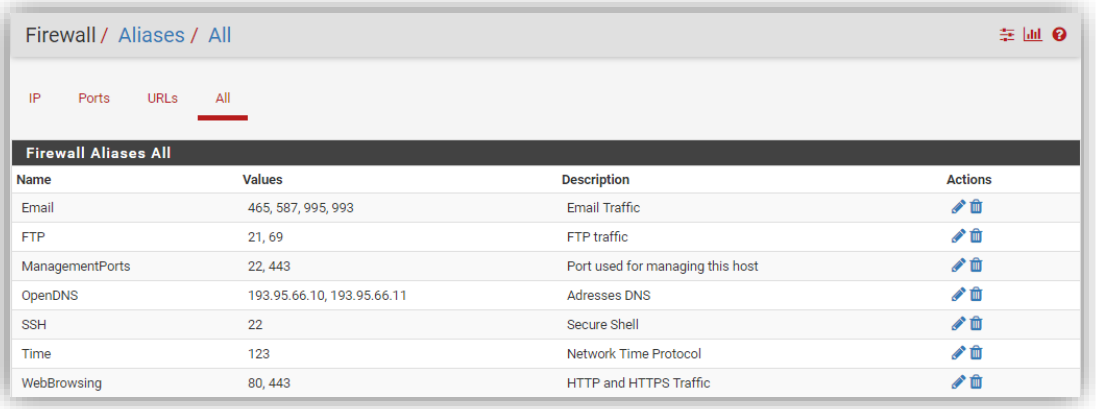


Figure 24 : Alias crées

b) Règles d'accès

Les deux figures ci-dessous présente la liste des contrôles d'accès pour les réseaux LAN et le WIFI.

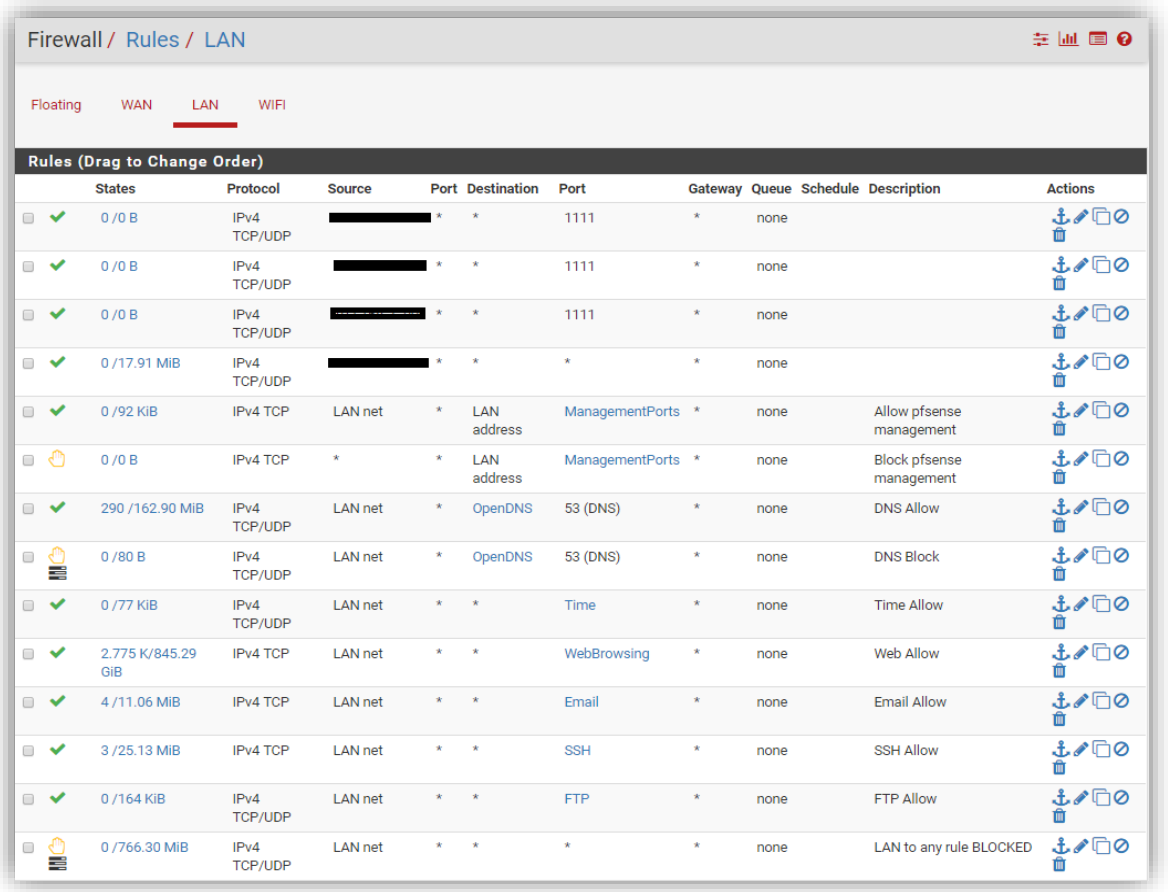


Figure 25 : Les règles d'accès pour le LAN

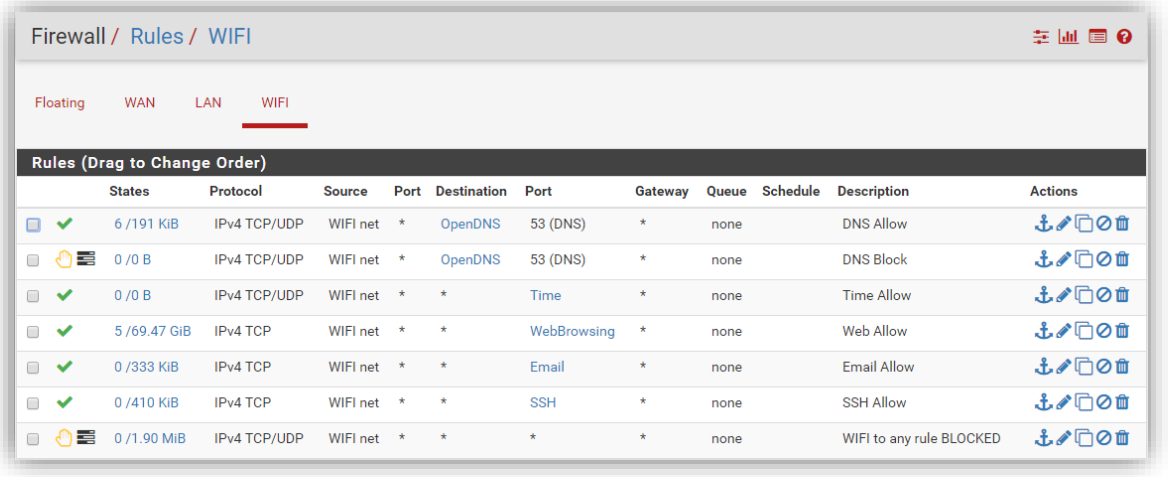


Figure 26 : Les règles d'accès pour le WIFI

c) *NAT :*

Pour exploiter les adresses IP publiques on les a introduites dans le Pfsense comme étant des « IP virtuelles », qu'on a associé par la suite à des adresses privées via le NAT et à la fin on définit les règles d'accès propres à chaque adresse selon son utilisation dans l'interface appropriées.

La **figure 36** ci-après présente trois règles d'accès pour des adresses privées qui ont été translatées en adresses publiques reconnues par la plateforme BIRUNI et qui fonctionnent via le port '1111'.

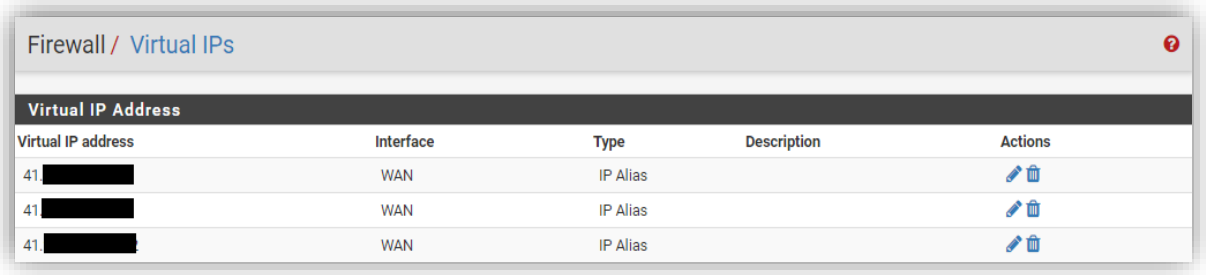


Figure 27 : Virtual IPs

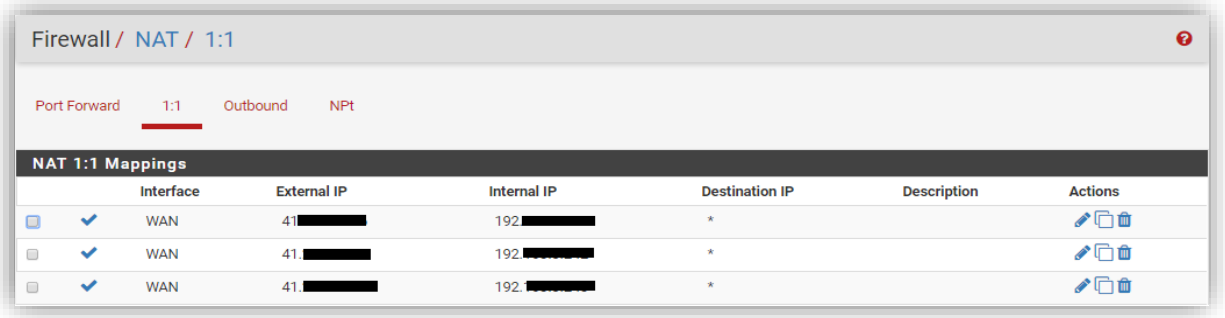


Figure 28 : NAT des adresses ip privées avec des adresses ip publiques

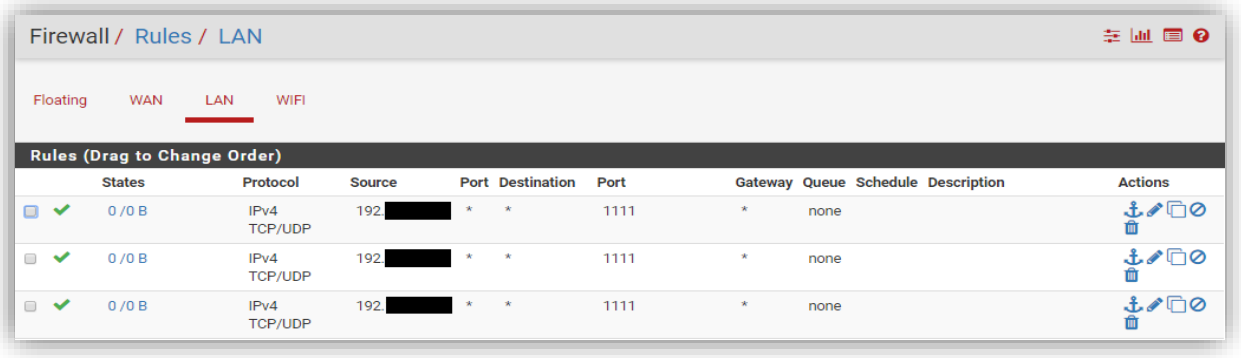


Figure 29 : Règles pour accès à la plateforme BIRUNI

4.2.5 Détection d'intrusions sur Pfsense

Dans Pfsense on peut installer le paquet ***Snort*** qui est un Système de Détection d'Intrusions (IDS) open source, il peut aussi être configuré pour fonctionner comme un Système de Prévention d'Intrusions (IPS). Snort analyse en temps réel les paquets et permet de détecter les anomalies et repérer de nombreuses attaques réseau connues.

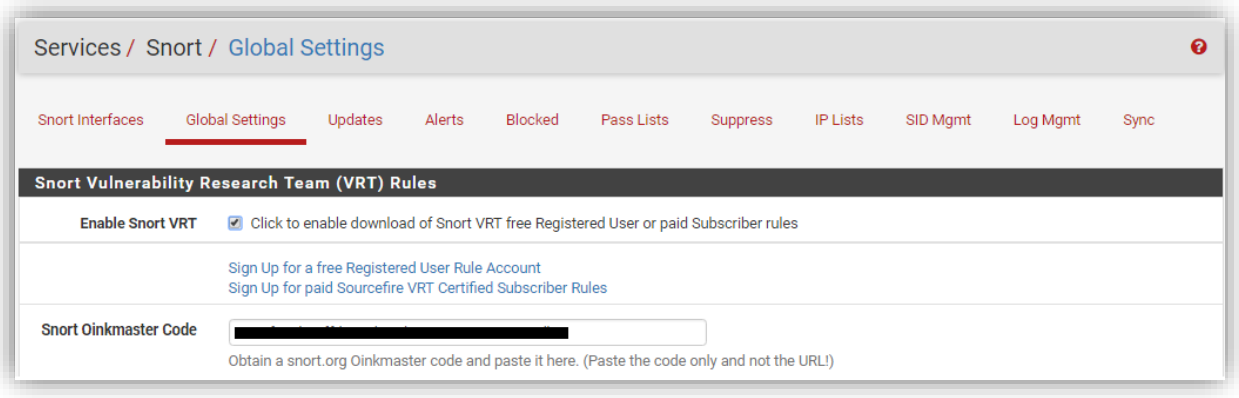


Figure 30 : Activation de Snort

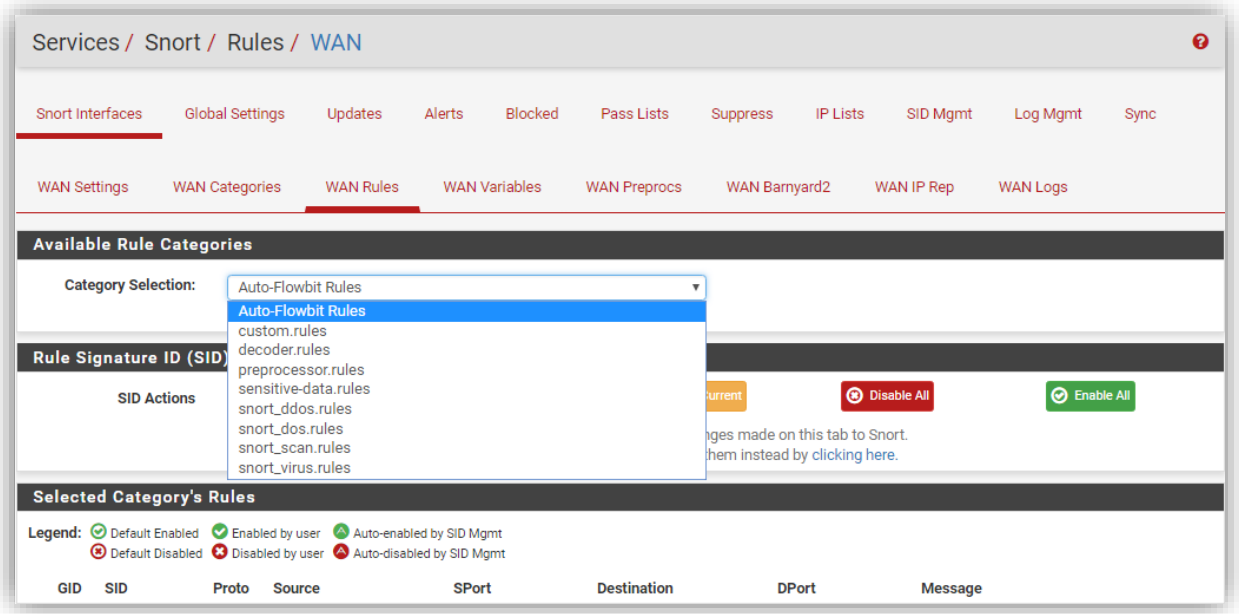


Figure 31 : Règles activées sur Snort pour l'interface WAN

Dans la figure ci-dessous une liste d'alertes interceptées et bloquées par Snort :

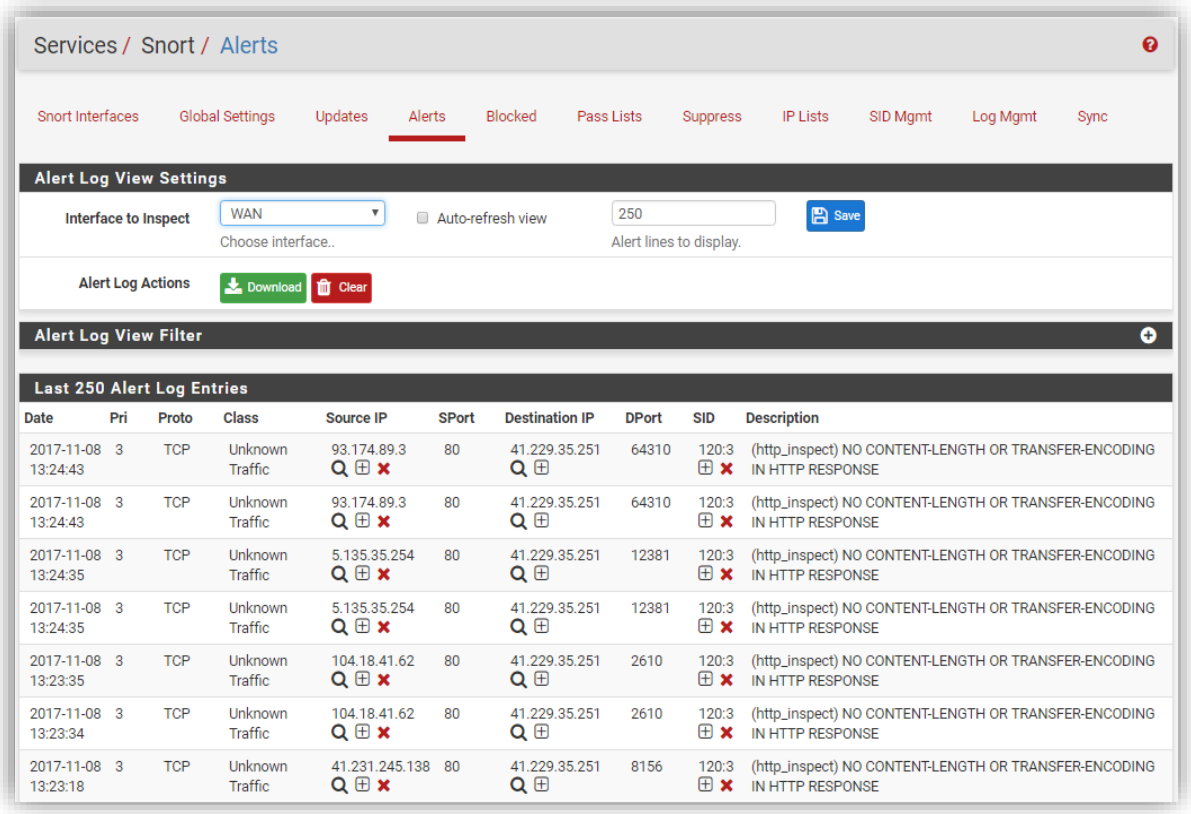


Figure 32 : Exemples d'alertes bloquées par Snort

4.3 Sécurisation du réseau sans fil

Le réseau sans fil était ouvert sur le réseau filaire et les deux réseaux utilisaient la même plage d'adresses depuis le même DHCP avec uniquement comme aspect de sécurité une clé WEP connue par tout le monde.

4.3.1 Configuration du serveur DHCP pour le réseau sans fil

Suite à la séparation des deux réseaux filaires et sans fil, on a procédé à configurer un DHCP au niveau du contrôleur WIFI.

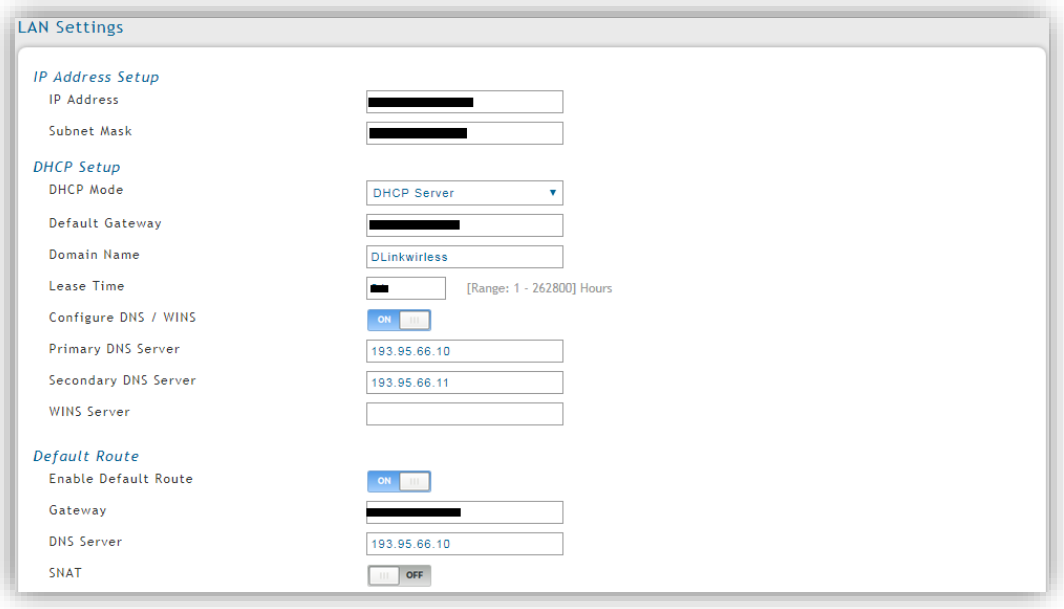


Figure 33 : Activation du DHCP sur le contrôleur WIFI

4.3.2 Portail Captif

La technique du portail captif consiste à forcer les utilisateurs du réseau à s'authentifier, elle consiste à rediriger tous les paquets HTTP ou HTTPS vers une page web d'authentification. On va appliquer cette technique pour les utilisateurs du réseau WIFI :

- Dans un premier temps on a procédé à créer un groupe d'utilisateurs pour le portail captif :

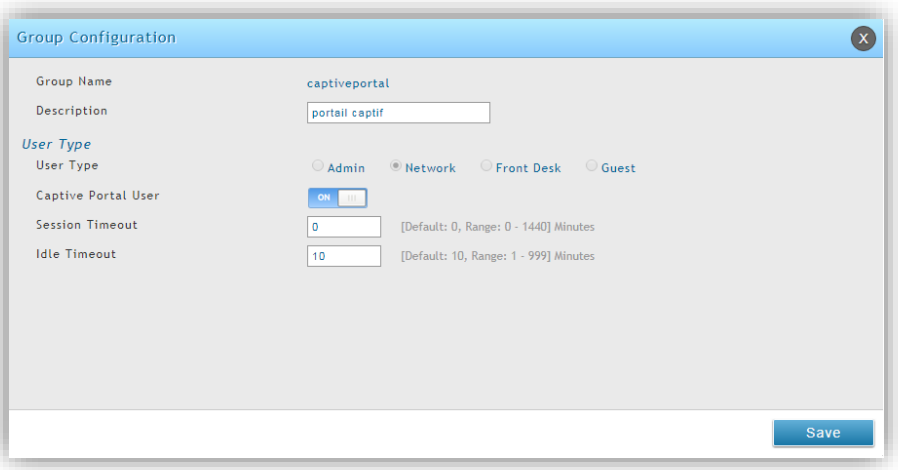


Figure 34 : Création du groupe des utilisateurs du portail captif

- Ensuite lors de création de l'SSID, on active l'option d'authentification via le portail captif et on choisit la page d'authentification à laquelle rediriger les utilisateurs :

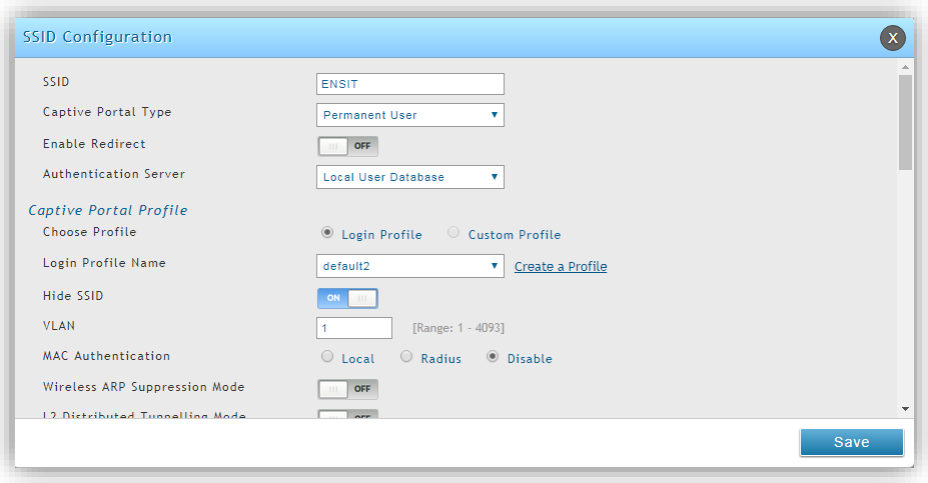


Figure 35 : Création du SSID : « ENSIT »

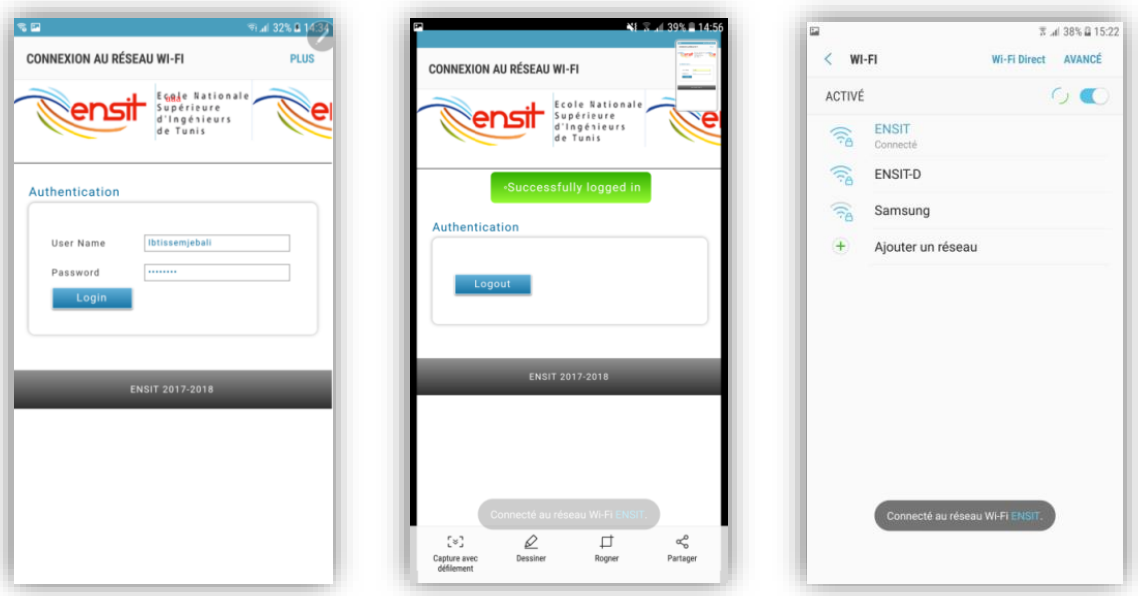


Figure 36 : Captures d'écran sur un Smartphone se connectant au réseau ENSIT

4.4 Nouvelle architecture réseau

La figure ci-après présente l'architecture de notre réseau après la mise en place du firewall et la sécurisation de l'accès au réseau sans fil via l'authentification à travers le portail captif.

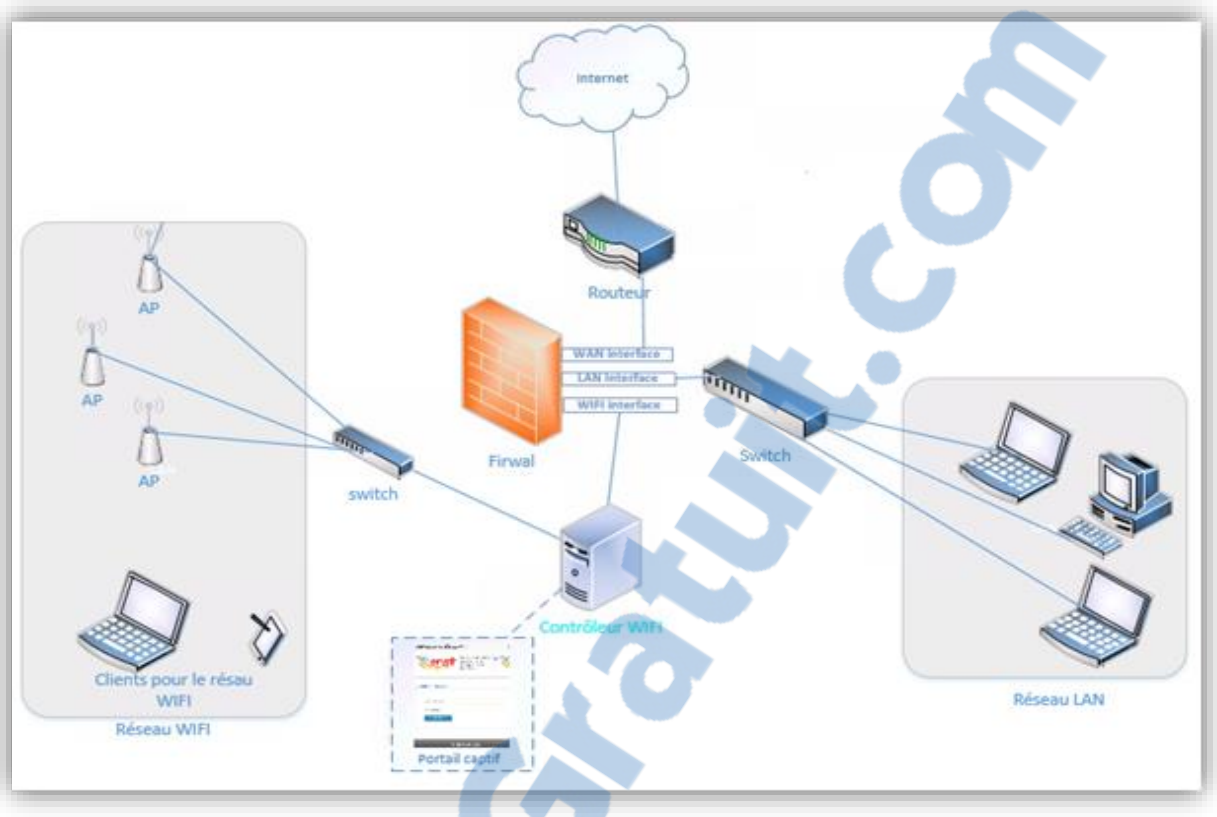


Figure 37 : La nouvelle architecture du réseau de l'ENSIT

Conclusion

L'Ecole Nationale Supérieur d'Ingénieur de Tunis est un très grand site : son Système d'Information est composé d'un grand réseau filaire, un réseau sans fil et un grand nombre d'utilisateurs qui diffèrent en profils.

La mise à jour et l'optimisation de ce réseau doivent être faites de façon continue et selon les normes en vigueur afin d'assurer le maintien de service, l'efficacité et garder un haut niveau de sécurité.

Dans ce chapitre on a livré des recommandations pragmatiques accompagnées d'un plan d'actions correctives.

On a enrichi nos compétences en termes d'installation et configuration d'une solution firewall Open Source à savoir Pfsense, et la sécurisation du réseau sans fil.

Conclusion Générale

L'objectif recherché, à travers cette mémoire est d'exécuter une mission d'Audit Globale du Système d'Information de l'Ecole Nationale Supérieure d'Ingénieurs de Tunis. Ce projet nous a permis de tirer et exposer un exemple typique d'un Système d'Information dans une entreprise publique Tunisienne.

À l'origine, le but premier de cette étude était axé principalement sur le théorique mais a nécessité un travail assez considérable sur le plan pratique malgré les contraintes matérielles et logicielles rencontrés.

Dans ce rapport on a établi un diagnostic de la situation, souligner l'ampleur des dégâts en dressant un bilan des failles organisationnelles, physiques et techniques, et asseoir le processus de réforme sur des bases solides dans la définition des recommandations correctives, et ce en faisant en sorte que les standards soient la référence et le socle essentiel de toute action exécutée au niveau du Système.

En fait, Il est obligatoire de finir avec les pratiques pernicieuses au fonctionnement et développement du réseau informatique et s'orienter vers la construction d'un nouveau Système Informatique maîtrisé, sécurisé et évolutif fondé sur des principes et des normes internationalement reconnus.

Bibliographie

Webographie

[1] :http://www.legrand.com/files/fck/File/pdf/EXB13011_Infrastucture_numerique_du_batimen t_FR.pdf

[2] : https://www.tpsgc-pwgsc.gc.ca/biens-property/sngp-npms/bi-rp/tech/telecommunications/normes-standard-fra.html

[3] :http://www.legrand.com/files/fck/File/pdf/EXB13011_Infrastucture_numerique_du_batiment_FR.pdf

[4] : (https://fr.wikipedia.org/wiki/ISO/CEI_11801)

[5] : http://www.legislation.tn/sites/default/files/fraction-journal-officiel/2015/2015F/007/Tf201500204.pdf

[6] : http://www.cnudst.rnrt.tn/jortsrc/2014/2014f/jo0672014.pdf

[7] : https://www.iso.org

[8] https://www.ansi.tn/fr/pages/cadre.html

[9] : http://www.mes.tn/cilculaire.php?code_menu=58#?

[10] : http://www.cck.rnu.tn

[11] : http://www.ensit.tn

https://fr.slideshare.net/BRAHIMMELLOUL/droulement-dune-mission-daudit

https://www.ansi.tn/fr/documents/guides/guides/charte_informatique.pdf

http://www.di.u-psud.fr/telechargement/charte/charte_informatique_ups11.pdf

Annexes

Annexe 1 :

Questionnaire sur la sécurité du Système d'Information inspiré de la norme ISO 27002

1. Politiques de Sécurité de l'information	
Est' ce que l'ENSIT dispose-elle d'un document décrivant la politique de sécurité de l'information, actualisé périodiquement et approuvé par le directeur de l'Ecole et communiqué à tous les utilisateurs ?	N
La politique de sécurité définie-elle : - les objectifs de la sécurité dans l'école ; - les principes d'organisation ; - le management et le pilotage de la sécurité : rôles et responsabilités.	N
De quoi est formée la politique de sécurité : chartes, procédures ?	N
Etablit-on un rapport annuel en matière de sécurité de l'information ?	N
Y-a-il une démarche de certification ISO pour l'école dans le domaine de sécurité informatique ?	N
2. Organisation de la sécurité de l'information	
Est-ce que la politique de sécurité bénéficie d'un soutien clair de la direction de l'Ecole pour initialiser, contrôler, entretenir, adapter la mise en œuvre de la sécurité de l'information au moyen de directives claires, d'un engagement approprié et d'une affectation adéquate des ressources ?	N
Est-ce que la mise en place des mesures de sécurité de l'information est effectuée par des agents qui occupent des fonctions diverses dans les sections concernées de l'ENSIT ?	N
Existe-il des agents spécialistes dans la sécurité dont les responsabilités concernant la protection des actifs et l'exécution des processus de sécurité spécifiques sont clairement définies ?	N
Assure-t-on une veille technologique en matière de sécurité (participation à des cercles, associations, congrès...) ?	N
3. Sécurité des ressources humaines	
Y a-t-il une procédure d'information préliminaire auprès du personnel, en ce qui concerne leurs devoirs et responsabilités et les exigences de sécurité de la fonction ?	N
Est-ce que les responsabilités de l'employé en matière de sécurité de l'information sont mentionnées dans leurs conditions d'emploi ?	N
Existe-t-il un programme de formation du personnel aux règles et mesures générales de protection de l'information ?	N
Existe-t-il un processus disciplinaire formalisé en cas de manquement aux règles de sécurité ou de violation de procédure ?	N
Les devoirs et responsabilités lors de la cessation ou d'un changement d'activité d'un collaborateur (interne ou sous contrat) sont-ils définis et précisés dans une procédure ou document ?	N
Les règles concernant le retour à l'école des biens confiés au personnel, lors de cessation ou de changement d'activité, sont-elles clairement définies et précisées ?	N
Les droits d'accès des utilisateurs sont-ils supprimés à la fin de leur période d'emploi ?	N
4. Gestion des actifs	
Tient-on à jour un inventaire des types d'actifs ?	N
A-t-on défini les types d'actifs devant être identifiés et inventoriés ?	O
A-t-on désigné pour chaque actif identifié et inventorié un "propriétaire" de cet actif ?	O
A-t-on défini et documenté, pour chaque actif, les règles d'utilisation acceptables ?	N
A-t-on effectué une classification des informations (documents, données, fichiers, bases de données, etc.) en fonction de l'impact qu'un sinistre touchant ces informations aurait sur l'école ?	N
5. Contrôle d'accès	
A-t-on établi une politique de gestion des droits d'accès au réseau local s'appuyant sur une analyse préalable des exigences de sécurité ?	N
Existe-t-il des procédures formelles d'enregistrement et de révocation des personnes ?	N
Est-ce que les utilisateurs suivent de bonnes pratiques de sécurité lors de la sélection et de l'utilisation des mots de passe ?	N
Est-ce que l'école veille à ce que le matériel sans surveillance ait une protection appropriée ?	Partiellement

Est-ce que l'école a adopté une politique de bureaux propre et d'écrans vides afin de protéger les informations contre des accès non autorisés, de perte d'information et de dommages ?	N
Est-ce que les utilisateurs n'ont un accès direct qu'aux services spécifiques pour lesquels ils ont été autorisés ?	O
Y a-t-il un mécanisme d'authentification et de contrôle d'accès de chaque utilisateur pour toute connexion au réseau local depuis l'extérieur ?	N
Pour les connexions qui l'exigent, y a-t-il une identification de l'équipement appelant (adresse MAC, adresse IP, etc.) en association avec des règles de contrôle d'accès ?	N
A-t-on effectué un partitionnement du réseau local en domaines de sécurité et à des espaces de confiance à l'intérieur desquels des contrôles peuvent être adaptés ?	N
Est-ce que les capacités de connexion des utilisateurs sont limitées et basées sur la politique de contrôle d'accès ?	N
Tout accès au système requiert-il la présentation d'un identifiant reconnu par le système ?	N
Tout identifiant reconnu par le système correspond-il à une personne physique unique et identifiable, directement ou indirectement ?	N
6. Cryptographie	
A-t-on défini et mis en place des solutions de chiffrement pour les échanges d'informations ?	N
7. Sécurité physique et environnementale	
Est-ce que des périmètres de sécurité ont été utilisés afin de protéger les zones contenant des infrastructures de traitement de l'information en fonction de la sensibilité des informations ?	Partiellement
Y a-t-il des batteries intermédiaires (alimentant un ou plusieurs onduleurs) garantissant une autonomie suffisante pour que les équipements s'arrêtent dans de bonnes conditions ?	N
Les locaux sensibles sont-ils situés dans des zones non accessibles par le public ?	Partiellement
Est-ce que les zones de sécurité sont protégées à l'entrée par des mesures appropriées pour faire en sorte que seul le personnel autorisé puisse y avoir accès ?	N
Existe-t-il une protection physique des biens de l'établissement contre les incendies, le feu et d'autres formes de désastres ?	N
Existe-t-il des détecteurs d'humidité à proximité des ressources sensibles reliés à un poste permanent de surveillance ?	N
Existe-t-il une installation de détection automatique d'incendie complète pour les locaux sensibles ?	N
Les locaux sensibles sont-ils protégés par une installation d'extinction automatique (ambiance, faux planchers, faux plafonds) ?	N
Utilise-t-on un système de contrôle d'accès systématique aux locaux sensibles ?	N
Est-ce que les zones de livraison et de chargement sont contrôlées et isolées des infrastructures de traitement de l'information afin d'éviter tout accès non autorisé ?	Partiellement
Les installations sont-elles faites avec un souci de protection physique (accès protégé, absence de vue directe externe sur les équipements, absence de menaces physiques diverses, conditions climatiques, protection contre la foudre, protection contre la poussière, etc.) ?	N
Les courants forts et faibles sont-ils bien séparés ?	Partiellement
Le câblage est-il protégé contre les risques d'accident (goulottes protégées) ?	N
Conserve-t-on une trace de toute opération de maintenance ?	N
Est-ce que le matériel est entretenu correctement afin d'assurer sa disponibilité et son intégrité continues ?	N
Les personnes susceptibles de travailler en dehors des locaux de l'école reçoivent-elles une sensibilisation et une formation sur les mesures à appliquer pour protéger les documents utilisés, leurs systèmes et les données qu'ils contiennent ? Ces protections concernent la sécurité physique et logique contre le vol mais aussi les indiscrétions ou les accès non autorisés par la famille tout autant qu'en public.	N
Existe-t-il une procédure décrivant en détail les opérations à mener, avant appel à la maintenance, pour empêcher que celle-ci ait accès aux données critiques (clés de chiffrement ou de protection de réseau, configurations des équipements de sécurité, etc.) ?	N

Existe-t-il des règles concernant la sortie des actifs (autorisations préalables, personnes autorisées, enregistrement de la sortie et de la rentrée, effacement des données inutiles, etc.) ?	**Partiellement**
8. Sécurité liée à l'exploitation	
Les procédures opérationnelles d'exploitation sont-elles documentées, maintenues à jour et rendues disponibles à toute personne en ayant besoin ? Les modifications de ces procédures sont-elles approuvées par le management ?	**N**
Les décisions de changements et d'évolutions des équipements et systèmes font-elles l'objet de procédures de contrôle ?	**N**
A-t-on défini, pour chaque profil, les droits privilégiés nécessaires ?	**N**
Les systèmes de développement et de test sont-ils séparés des systèmes opérationnels ?	**N**
9. Sécurité des communications	
Le respect des clauses de sécurité, par les prestataires, est-il sous contrôle et fait-il l'objet de revues régulières ?	**N**
Les décisions de changement s'appuient-elles sur des analyses de la capacité des nouveaux équipements et systèmes à assurer la charge requise en fonction des évolutions des demandes prévisibles ?	**N**
A-t-on défini les actions à mener par le personnel informatique, pour prévenir, détecter et corriger les attaques par des codes malveillants ?	**N**
A-t-on établi un plan de sauvegarde, couvrant l'ensemble des configurations du réseau, définissant les objets à sauvegarder et la fréquence des sauvegardes ?	**N**
Est-ce qu'un ensemble de mesures est mis en œuvre afin d'obtenir et de maintenir la sécurité dans les réseaux informatiques ?	**N**
Les dispositifs de sécurité nécessaires, les niveaux de services, ont-ils été identifiés pour chaque service réseau et inclus dans un contrat de service (que ces services soient assurés en interne ou par un prestataire externe) ?	**N**
Existe-t-il des procédures de gestion des supports informatiques amovibles tels que les bandes, les disques, les cassettes et les rapports imprimés ?	**N**
Existe-t-il une procédure garantissant, en cas de mise au rebut, la non divulgation des informations sensibles jusqu'à la destruction de leur support ?	**N**
Existe-t-il un document définissant les règles générales à appliquer en ce qui concerne la protection des moyens et supports de stockage, de traitement et de transport de l'information (équipements de réseau et de travail, systèmes, applications, données, media, etc.) et les conditions requises pour l'attribution, la gestion et le contrôle des droits d'accès ?	**N**
Est-ce que la documentation est protégée contre un accès indu ou illicite, par des mécanismes forts ?	**N**
Est-ce que des accords ont été établis sur les échanges d'informations et de logiciels entre l'école et d'autres parties externes ?	**N**
Les procédures de supervision des systèmes sont-ils établis ? et les résultats des activités de supervision sont-ils régulièrement revus ?	**N**
10. Acquisition, développement et maintenance des systèmes d'information	
Les données sensibles font-elles l'objet d'un autocontrôle formel (par la personne assurant la saisie) ?	**O**
Existe-t-il un contrôle global sur des séries de saisie (somme, fourchette, min, max., etc.) ?	**O**
Est-ce que la validation des données de sortie d'un système d'application assure que le traitement des informations stockées soit correct et approprié aux circonstances ?	**Partiellement**
Est-ce que des procédures ont été établies afin de contrôler l'implantation de logiciels sur les systèmes opérationnels ?	**N**
Est-ce que les implémentations des modifications sont examinées et testés ?	**O**
Lorsque le développement logiciel est sous-traité, a-t-on pris soin de régler les questions d'accord de licence et de propriété intellectuelle du code développé ?	**N**
Est-ce que les vulnérabilités techniques sont contrôlées évaluées et prises en considérations par les mesures de remédiation nécessaires ? et est-ce que l'exposition de l'entreprise à ces vulnérabilités est régulièrement évaluée ?	**N**

11. Relation avec les fournisseurs	
Est ce qu'il existe à l'école une politique de sécurité destinée aux fournisseurs, formés d'articles relatifs à la sécurité des SI dans les contrats pour que les fournisseurs s'engagent dans le domaine ?	N
Est-ce que les fournisseurs apportent la preuve qu'ils respectent leurs engagements en matière de sécurité ?	N
Est-ce que les contrats avec les tiers impliquant l'accès aux infrastructures de traitement de l'information mentionnent toutes les exigences de sécurité pour assurer la conformité aux politiques et aux normes de sécurité de l'école ?	N
Est-ce que les risques associés à l'accès par les tiers aux infrastructures de traitement de l'information de l'organisation ont été évalués ? et les mesures de contrôle ont-elles été implantées ?	N
12. Gestion des incidents liées à la sécurité de l'informatique	
Est-ce que les signalisations des évènements de la sécurité de l'information sont reportées et communiquées le plus rapidement possible ?	N
Ce système de reporting des incidents inclut-il tous les incidents (exploitation, développement, maintenance, utilisation du SI) physiques, logiques ou organisationnels ?	N
Ce système de reporting des incidents inclut-il les tentatives d'actions malveillantes ou non autorisées n'ayant pas abouti ?	N
Est-ce que les employées, contractuels et les tiers signalent les failles des sécurités dans les meilleurs délais ?	N
Existent-ils des mécanismes qui surveillent et quantifient les coûts et les volumes des incidents de sécurité ?	N
Y a-t-il une collecte des preuves suite à un incident de sécurité ?	N
13. Aspects de la sécurité de l'information dans la gestion de la continuité d'activité	
Existe-t-il des processus, régulièrement mis en œuvre, d'analyse des risques liés à l'information, pouvant conduire à une interruption des activités de l'entreprise, débouchant sur une définition des exigences de sécurité, des responsabilités, des procédures à appliquer et moyens à mettre en œuvre afin de permettre l'élaboration des plans de continuité ?	N
14. Conformité	
L'ensemble des exigences réglementaires, contractuelles, et légales a-t-il été explicitement identifié et son application par l'organisation figure-t-elle dans un document tenu à jour ?	N
Procède-t-on à des contrôles fréquents visant à vérifier que les logiciels installés sont conformes aux logiciels déclarés et qu'ils possèdent une licence en règle ?	N
Existe-t-il un document précisant les exigences, les responsabilités et les procédures à appliquer afin de protéger les archives importantes pour l'organisation ?	N
Existe-t-il un recueil regroupant l'ensemble des dispositions légales ou réglementaires liées au système d'information et à la protection des renseignements personnels, applicables à l'entreprise ou à l'organisme ?	N
Y a-t-il des notes qui précisent- ce qui est toléré et les limites à ne pas dépasser (usage des biens de l'entreprise à des fins personnelles, par exemple) ?	N
Existe-t-il un recueil regroupant l'ensemble des dispositions légales ou réglementaires liées au système d'information et concernant l'usage de la cryptologie ?	N
Les responsables s'assurent-ils de la conformité du comportement de leurs collaborateurs aux politiques et standards en vigueur ?	N
Procède-t-on à des tests périodiques du réseau et à des audits techniques spécialisés approfondis ?	N

Annexe 2 :

Cartographie du réseau sur plan étage

Plan du réseau du [redacted] Bloc [redacted]

Plan du réseau du ■ étage Bloc ■

Plan du réseau du [redacted] étage Bloc [redacted]

Plan du réseau du SR

Plan du réseau [illegible] étage Bloc [illegible]

Plan du réseau du étage Bloc

Plan du réseau du [redacted] du Bloc [redacted]

Annexe 3 :

Chartes Informatiques

Charte Informatique

Ecole Nationale Supérieure d'Ingénieurs de Tunis

Version	1		
	Responsable	**Qualité**	**Date**
Propriétaire	**Mr Rached GHARBI**	Directeur de l'Ecole Nationale Supérieure d'Ingénieurs de Tunis	
Rédigé par	**Ibtissem JEBALI**	Technicien Principal	
Approuvé par	**Le Conseil scientifique de l'ENSIT**		

Historique de mises à jour		
Date	**Modifié par**	**Description du changement**

Adresse :5 Avenue Taha Hussein,
BP, 56, Bâb Manara,1008 Tunis
Tél :(+216)71392591-
Fax :(+216)71391166

العنوان: 5 شارع طه حسين ص.ب
56 باب منارة، تونس 1008
الهاتف: 71392591
الفاكس: 71391166

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université de Tunis
École Nationale Supérieure d'Ingénieurs
de Tunis (ENSIT)

وزارة التعليم العالي والبحث العلمي

جامعة تونس
المدرسة الوطنية العليا للمهندسين بتونس

Le présent document est porté à la connaissance de tout utilisateur des ressources informatiques de l'Ecole Nationale Supérieure d'Ingénieurs de Tunis : l'ENSIT.

Il définit les règles régissant l'usage des ressources informatiques et les règles de sécurité du Système d'Information que l'utilisateur et l'établissement s'engagent à respecter et précise les droits et devoirs de chacun.

Le Système d'Information représente :

- L'ensemble des moyens matériels, logiciels, applications, bases de données, fichiers et réseaux de télécommunications ;
- L'informatique nomade est également un des éléments constitutifs du système d'information tel que les ordinateurs portables, les smartphones, les assistants personnels … ;
- L'infrastructure des liaisons et équipements réseaux ainsi que les locaux techniques.

L'utilisateur est la personne ayant accès, dans le cadre de l'exercice de sa fonction, aux ressources du Système d'Information quel que soit son statut :

- Tout agent titulaire ou non titulaire, vacataire, invité, etc. ;
- Tous les étudiants : ingénieurs, mastériens, doctorants ;
- Tout fournisseur, sous-traitant ou autre personne en contact avec le système informatique ayant contracté avec l'école.

Adresse :5 Avenue Taha Hussein,
BP, 56, Bâb Manara,1008 Tunis
Tél :(+216)71392591-
Fax :(+216)71391166

العنوان: 5 شارع طه حسين ص.ب
56 باب منارة، تونس 1008
الهاتف: 71392591
الفاكس: 71391166

Article 1 Continuité de service

L'ENSIT s'efforce, dans la mesure du possible de maintenir accessible le service qu'elle propose de manière permanente mais peut interrompre l'accès pour des raisons de maintenance, de mise à niveau ou de sécurité sans pouvoir être tenue pour responsable des conséquences de ces interruptions tant à l'égard des utilisateurs que des tiers.

L'utilisateur doit garantir l'accès à tout moment à ses données professionnelles. En cas d'absence non planifiée et pour des raisons exceptionnelles, si un utilisateur se trouve dans l'obligation de communiquer ses codes d'accès au Système d'Information, il doit procéder dès que possible au changement de ces derniers ou en demander la modification à l'administrateur.

Article 2 Utilisation conforme aux lois en vigueur

Respect de la propriété intellectuelle

L'utilisation des moyens informatiques implique le respect des droits de propriété intellectuelle. En conséquence, chaque utilisateur doit :

- Utiliser les logiciels dans les conditions des licences souscrites ;
- A ne pas reproduire, copier, diffuser, modifier ou utiliser des données protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits ;
- Respecter le droit des marques.

Adresse :5 Avenue Taha Hussein,
BP, 56, Bâb Manara,1008 Tunis
Tél :(+216)71392591-
Fax :(+216)71391166

العنوان: 5 شارع طه حسين ص.ب
56 باب منارة، تونس 1008
الهاتف: 71392591
الفاكس: 71391166

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université de Tunis
École Nationale Supérieure d'Ingénieurs
de Tunis (ENSIT)

وزارة التعليم العالي والبحث العلمي

جامعة تونس
المدرسة الوطنية العليا للمهندسين بتونس

Respect de la vie privée

L'utilisation des moyens informatiques implique le respect même pendant le temps de service et sur le lieu de travail le secret des correspondances et de leurs contenus personnels.

Respect des clauses contractuelles

L'abonnement aux ressources documentaires électroniques éditoriales implique un usage raisonnable, personnel et strictement non commercial (interdiction de distribuer des copies papier ou de diffuser des versions numériques à toute personne extérieure à l'université, même à titre gratuit).

Responsabilité en matière de transmission d'informations

L'utilisateur devra entre autres s'abstenir :

- De diffuser des messages diffamatoires ou injurieux (ces faits sont répréhensibles quel que soit leur mode de diffusion, public ou privé) ;
- D'utiliser certaines formes d'apologie (crime, racisme, négationnisme, crimes de guerre, ...) ;
- D'utiliser toute forme de provocation et de haine raciale ;
- De diffuser des informations confidentielles sans autorisation préalable d'une personne habilitée.

Adresse :5 Avenue Taha Hussein,
BP, 56, Bâb Manara,1008 Tunis
Tél :(+216)71392591-
Fax :(+216)71391166

العنوان: 5 شارع طه حسين ص.ب
56 باب منارة، تونس 1008
الهاتف: 71392591
الفاكس: 71391166

Pour mémoire, les textes de référence en matière informatique sont :

Loi n° 63 - 2004, du 27 juillet 2004 Portant sur la protection des données à caractère personnel ;

Loi n° 5 - 2004 du 3 février 2004 Relative à la sécurité informatique et portant sur l'organisation du domaine de la sécurité informatique et fixant les règles générales de protection des systèmes informatiques et des réseaux ;

Circulaire n° 19 - du 11 avril 2007 relatif au renforcement des mesures de sécurité informatique dans les établissements publiques ;

Guide de sécurité informatique de l'ANSI.

Article 3 Règles de sécurité

Les codes d'accès, sont personnels et confidentiels pour tout utilisateur afin de protéger les données et les outils auxquels il a accès de toute utilisation malveillante ou abusive. Cette mesure ne confère pas pour autant un caractère personnel à ces données ou outils.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

De la part de l'ENSIT :

- Limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;
- Maintenir la qualité du service fourni aux utilisateurs dans la limite des moyens alloués ;

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université de Tunis
École Nationale Supérieure d'Ingénieurs
de Tunis (ENSIT)

وزارة التعليم العالي والبحث العلمي

جامعة تونس
المدرسة الوطنية العليا للمهندسين بتونس

- Veiller à respecter la confidentialité des correspondances électroniques et des fichiers ;
- Veiller à la bonne utilisation du SI ;
- Assurer la sécurité des ressources ;
- Garder les traces ("logs") en respect de la législation :
- Toute activité sur le réseau et les systèmes fait objet d'une surveillance automatisée.
- Les responsables informatiques peuvent, en cas d'urgence, prendre toutes mesures nécessaires pour assurer ou préserver le bon fonctionnement et la disponibilité normale des ressources informatiques dont ils ont la charge ;
- L'administrateur doit accéder aux systèmes, aux réseaux et aux données nécessaires à des fins d'administration, de configuration et de diagnostic et, tout en respectant les règles de confidentialité de ces informations.
- L'administrateur ne doit pas altérer volontairement les systèmes, les réseaux et les données dont il a accès ;
- L'administrateur doit établir des procédures de surveillance de toutes les tâches exécutées sur les systèmes et les réseaux, afin de déceler les violations ou les tentatives de violation de la présente charte.
- L'administrateur doit prendre en cas d'infraction à la charte des mesures conservatoires, si l'urgence l'impose, sans préjuger des sanctions qui pourraient en résulter.

Adresse :5 Avenue Taha Hussein,
BP, 56, Bâb Manara,1008 Tunis
Tél :(+216)71392591-
Fax :(+216)71391166

العنوان: 5 شارع طه حسين ص.ب
56 باب منارة، تونس 1008
الهاتف: 71392591
الفاكس: 71391166

- L'administrateur doit informer les utilisateurs, les sensibiliser aux problèmes de sécurité informatique et leur faire connaître les règles de sécurité à respecter.
- L'administrateur doit veiller à mettre à jour les correctifs de sécurité sur les systèmes et équipements dont il est responsable.
- L'administrateur doit veiller à mettre à jour les signatures Antivirales sur les systèmes dont il est responsable.
- L'administrateur doit limiter les accès aux ressources sensibles et acquérir les droits de propriété intellectuelle ou obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

De la part de l'utilisateur :

- Garder strictement confidentiel(s) son (ou ses) mot(s) de passe et ne pas le(s) dévoiler à un tiers ;
- Respecter la gestion des accès, en particulier ne pas utiliser les noms et mots de passe d'un autre utilisateur, ni chercher à les connaître et s'interdire d'accéder ou de tenter d'accéder à des ressources du Système d'Information entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite ;
- Procéder au changement de mot de passe régulièrement ;
- Protéger son certificat électronique (si elle existe) par un mot de passe sûr gardé secret.

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université de Tunis
École Nationale Supérieure d'Ingénieurs
de Tunis (ENSIT)

وزارة التعليم العالي والبحث العلمي

جامعة تونس
المدرسة الوطنية العليا للمهندسين بتونس

- Ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- Ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'école et ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée ;
- Ne pas installer, télécharger ou utiliser sur le matériel connecté au réseau de l'ENSIT, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittées, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ;
- Ne pas déposer des données sur un serveur interne ou ouvert au grand public ou sur le poste de travail d'un autre utilisateur sans y être autorisé par les responsables habilités ;
- Ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites (virus, chevaux de Troie, bombes logiques...).
- Signaler sans délai tout fonctionnement suspect ou incident de sécurité aux responsables ;

Adresse :5 Avenue Taha Hussein,
BP, 56, Bâb Manara,1008 Tunis
Tél :(+216)71392591-
Fax :(+216)71391166

العنوان: 5 شارع طه حسين ص.ب
56 باب منارة، تونس 1008
الهاتف: 71392591
الفاكس: 71391166

- Se conformer aux dispositifs mis en place par l'école pour lutter contre les virus et les attaques ;
- Assurer la protection de ses informations et plus particulièrement celles considérées comme sensibles, en utilisant différents moyens de sauvegarde individuels ou mis à sa disposition. L'utilisateur ne doit pas transporter sans protection des données sensibles sur des supports non fiables tels que ordinateurs portables, clés USB, disques externes, etc., les supports de sauvegarde doivent être placés dans un endroit sûr ;
- Ne pas quitter son poste de travail en libre-service, laissant des ressources ou services accessibles.
- Ne pas oublier de récupérer, sur les fax, imprimantes ou photocopieurs, les documents sensibles envoyés, imprimés ou photocopiés, ...

Article 4 Antivirus

L'ENSIT dispose d'un antivirus, que chaque utilisateur doit se conformer aux instructions de l'Administrateur pour son installation et sa mise à jour.

Seul l'administrateur est autorisé à introduire dans le système d'information de nouveaux matériels et logiciels. En cas de besoin exprimé par un utilisateur pour un nouveau matériel ou logiciel, il devra demander, à l'Administrateur, une autorisation préalable. Le non-respect de ces dispositions peut exposer l'utilisateur à des sanctions et à la mise en jeu de sa responsabilité en cas d'intrusion, de virus ou d'un tiers non – autorisé dans le système d'information ou de pertes de données.

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université de Tunis
École Nationale Supérieure d'Ingénieurs
de Tunis (ENSIT)

وزارة التعليم العالي والبحث العلمي

جامعة تونس
المدرسة الوطنية العليا للمهندسين بتونس

Article 5 Messagerie électronique

L'école recommande l'utilisation d'adresse de messagerie officielle offerte par le CCK suite à une demande formulée et approuvée par le directeur hiérarchique et le directeur général de l'école ;

L'accès à cette messagerie est strictement personnel ;

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages ;

L'utilisateur doit être vigilant sur la nature des messages électroniques qu'il échange, c'est un écrit pouvant engager l'école, il faut accorder une attention particulière à sa rédaction et sa diffusion ; il peut être considéré comme preuve pour établir un fait ou un acte juridique.

Article 6 Internet

Il est dangereux pour l'école de diffuser des informations techniques (ou de documents) sur les ressources du système d'information de l'école via des sites Internet ;

L'ENSIT se réserve le droit de filtrer ou d'interdire l'accès à certains sites ;

L'ENSIT se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus, code malicieux, programmes espions ...) ;

L'utilisation du réseau pour se connecter à Internet doit être rationnelle de manière à éviter toute consommation abusive des ressources ;

Adresse :5 Avenue Taha Hussein,
BP, 56, Bâb Manara,1008 Tunis
Tél :(+216)71392591-
Fax :(+216)71391166

العنوان: 5 شارع طه حسين ص.ب
56 باب منارة، تونس 1008
الهاتف: 71392591
الفاكس: 71391166

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Université de Tunis
École Nationale Supérieure d'Ingénieurs
de Tunis (ENSIT)

وزارة التعليم العالي والبحث العلمي

جامعة تونس
المدرسة الوطنية العليا للمهندسين بتونس

Le téléchargement de fichiers, de logiciels et tous autres documents doivent s'effectuer dans le respect des droits de la propriété intellectuelle et être en rapport avec les missions d'activité professionnelle, d'enseignement et de recherche de l'école ;
L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel et ne gêne pas la bonne marche du Système d'Information et le travail des autres utilisateurs.

Article 7 Limitations des usages

En cas de non-respect des règles définies dans la présente charte, le directeur de l'école pourra, sans prévoir des actes de sanctions, limiter les usages par mesure conservatoire ;

Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extraprofessionnelles, peut engendrer des sanctions.

Article 8 Entrée en vigueur de la charte

La présente charte sera affichée dès son adoption par le Conseil scientifique de l'ENSIT et sera publié sur le site Internet de l'école ;
Des extraits de cette charte seront diffusées auprès des étudiants et du personnel et annexés dans les contrats avec des prestataires.

Contactez le responsable informatique pour toute question relative à la Sécurité du Système d'Information.

Adresse :5 Avenue Taha Hussein,
BP, 56, Bâb Manara,1008 Tunis
Tél :(+216)71392591-
Fax :(+216)71391166

العنوان: 5 شارع طه حسين ص.ب
56 باب منارة، تونس 1008
الهاتف: 71392591
الفاكس: 71391166

CHARTE DE BON USAGE DU RESEAU WIFI DE L'ENSIT

1- OBJET

Ce document définit les conditions générales d'utilisation du réseau Wifi.

Un utilisateur authentifié peut se connecter à partir de son ordinateur portable, de sa tablette ou de son Smartphone à Internet depuis les zones couvertes par le réseau Wifi.

2- LA COUVERTURE DU RESEAU WI-FI A L'ECOLE

Le réseau Wi-Fi de l'Ecole Nationale Supérieure d'Ingénieurs de Tunis donne un accès à Internet depuis certains sites.

Le déploiement actuel des points d'accès couvre :

Bloc A	Bloc B
; ; ; ; ; ;	; ; ; ; ; ;

3- ACCES

L'utilisateur doit activer la carte Wifi et s'assurer que sa carte est paramétrée pour « obtenir une adresse IP automatiquement » puis sélectionner le réseau « ENSIT ».

Lors de la connexion à internet, l'utilisateur sera redirigé vers le portail du réseau et devra entrer les paramètres de connexion qui sont sous la forme :

Login: prenom.nom

Mot de passe : Code

Code : N° [redacted] pour les étudiants | **N°** [redacted] pour les enseignants et les administratifs.

- Les paramètres de connexion sont strictement personnels et confidentiels.
- L'accès au réseau WI-FI est limité.
- Le débit est proportionnel au nombre de personnes connectées sur une zone.

4- REGLES D'USAGE

Afin d'avoir une connexion stable à Internet et ne pas saturer le réseau WIFI, tous les utilisateurs sont appelés à :

- Utiliser la connexion dans le cadre exclusif des activités conformes aux missions de l'établissement (études, recherche, enseignement, administration) ;
- Ne pas effectuer d'opérations pouvant nuire au bon fonctionnement du réseau (manipulations anormales, spamming, virus …)
- Eviter toute consommation abusive d'Internet et le téléchargement répétitif de fichiers volumineux ;
- Ne jamais prêter les paramètres de connexion et signaler toute tentative de violation de ces paramètres au ***Centre d'Informatique et d'Internet***.

Tout abus sera privé d'accès.

CHARTE DE LA SECURITE DU SYSTEME D'INFORMATION DE L'ENSIT DEDIEE AUX FOURNISSEURS

1. OBJET

La présente Charte décrit les règles de sécurité en relation avec le Système d'Information, relatives aux interventions de tiers fournisseurs dans les locaux de l'Ecole Nationale Supérieure d'Ingénieurs de Tunis « ENSIT ».

En signant cette charte, le fournisseur ou prestataire reconnait en avoir pris connaissance et s'engage librement à en appliquer strictement le contenu.

2. REGLES REGISSANT LES INTERVENTIONS

Tout fournisseur doit admettre et appliquer les politiques sécurité de l'établissement.

Le fournisseur s'engage formellement à :

- Respecter les normes et standards relatifs à son domaine d'application en relation avec le domaine de Sécurité des Systèmes d'Information ;
- Protéger les actifs matériels et immatériels de l'école lors des interventions, ces actifs ne doivent pas être endommagés et doivent rester fonctionnels ;
- Préserver les documents et Informations utilisés pendant le déroulement des travaux et ne pas les utiliser pour des fins autres que celles spécifiées dans le contrat ;
- Ne pas divulguer les informations à d'autres personnes privées ou publiques, physiques ou morales ;
- Assurer les mesures de sécurité nécessaires pour garder l'intégrité des documents et informations traités pendant la durée du contrat ;
- Etre accompagné par un personnel habilité de l'école pendant les visites sur site et en zone sensible ;
- Préserver la confidentialité des données personnelles des employés de l'école ;
- Remettre les lieux en état après finalisation des travaux et avant de quitter le site, cela fera l'objet d'une validation formelle de la part de la direction de l'école.

3. NON RESPECT DU CHARTE

Le fournisseur est tenu responsable de toutes les conséquences résultantes au non-respect de cette Charte ; en conséquence, l'école se réserve le droit de résilier le contrat avec ce fournisseur et il prendra en charge tous les frais d'indemnisation relatifs aux conséquences du non-respect desdites règles.

Je soussigné (nom et prénom) :

.....

Agissant en qualité (fonction dans l'entreprise) :

.....

Représentant la société (raison sociale) :

.....

.....

Située à (adresse légale de l'entreprise) :

.....

.....

.....

Reconnais avoir pris connaissance du document contractuel « Charte de la sécurité du Système d'Information de l'ENSIT dédiée aux fournisseurs » applicable aux fournisseurs et prestataires de l'ENSIT, et m'engage à en respecter l'ensemble des règles.

Le ……

Signature ***Cachet de l'entreprise***

NB : Cette page doit être remplie et signée par les fournisseurs et prestataires de l'ENSIT.

Résumé

Le présent document est le fruit d'un travail qui a été réalisé dans le cadre d'une mission d'audit du réseau informatique au sein de l'Ecole Supérieure d'Ingénieurs de Tunis, il présente la succession d'étapes suivies pour accomplir la mission et la mise en place de quelques solutions proposées.

La mission d'audit est une opération assez vaste et complexe qui traite divers volets en relation avec le Système d'Information touchant des facteurs organisationnels, physiques et techniques pour cela elle est régie selon des démarches bien définies. La mission s'est déroulée sur trois principales étapes : D'abord *une étude de l'existant* pour donner un bilan complet de l'architecture informatique, ensuite *une analyse des résultats* en termes de performance technique et de la sécurité du Système Informatique afin d'identifier les anomalies et les faiblesses et enfin *la proposition des recommandations* selon un plan d'action pour remédier aux failles, améliorer la sécurité et la fiabilité du réseau et optimiser l'infrastructure informatique.

Mots clés : Audit ; Normes, Câblage structuré, ISO27002, Charte Informatique ; Pare-feu ; portail captif

Abstract

The following document is the result of work carried out during an audit assignment for the computer network at the Higher School of Engineers of Tunis. It presents the sequenced steps followed to accomplish the mission along with the implementation of some proposed solutions.

The audit assignment is a fairly large and complex operation. It treats different sides of organizational, physical and technical factors related to the Information System, for which it is organized according to well-defined procedures. The mission was carried out in three main stages:

1. *A study of the existing situation* to give a complete assessment of the IT architecture.
2. An *analysis of the results* in terms of technical performance and security of the IT system to identify anomalies and weaknesses.
3. A *proposal of recommendations* structured in an action plan to correct gaps, improve network security and reliability, and of course optimize IT infrastructure.

Keywords: Audit; Standards; Structured wiring; ISO27002, Charter use of IT; Firewall; Captive Portal