REPUBLIQUE TOGOLAISE

Travail – Liberté – Patrie

UNIVERSITE DE LOME

RAPPORT DE CERTIFICATION DU RESEAU INTRANET DE L'UNIVERSITE DE LOME

COMMANDE N°00011/2024/DC/UL/S/BA

ADRESSE

BUYMORE SARL U Rue des Evala à 10 m de la pharmacie Mathilda

TELEPHONE

+228 90 97 76 05 / 96 07 38 32 / 22 50 02 08

BP

22 BP 177 Lomé-Togo

EMAIL

info@buymoretogo.com / stbuymore@yahoo.fr

SITE WEB

INFORMATIONS

Attention

Ce document, rédigé par **BUYMORE**, est strictement confidentiel et destiné exclusivement à **l'Université de Lomé**. Toute divulgation, reproduction ou diffusion, partielle ou totale, sans l'autorisation écrite et préalable de **l'Université de Lomé** est formellement interdite.

Toute violation de cette confidentialité exposera son auteur à des poursuites, conformément aux lois et règlements en vigueur en matière de protection des informations confidentielles.

Evolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	12/03/2025	Version initiale

Table des matières

LISTE DES TABLEAUX

LISTE DES FIGURES

GLOSSIARE

Acronyme	Définition
UL	Université de Lomé
SI	Système d'information
IT	Information Technology
DSI	Directeur du Système Informatique
ISO 27001	International Organization for Standardization
NIST	National Institute of Standards and Technology
CIS	Center for Internet Security
SIEM	Security Information and Event Management
EDR	Endpoint detection and response
PSSI	Politique de Sécurité des Systèmes d'Information
SOC	Security Operations Center
DRSI	Direction des Ressources et des Systèmes d'Information
CIC	Centre Informatique et de Calcul
QoS	Quality of Service
DMZ	Demilitarized Zone
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
SMSI	Système de management de la sécurité de l'information
ITSM	Information Technology Service Management
GLPI	Gestionnaire Libre de Parc Informatique

RESUME EXECUTIF

Objectif de l'audit

La certification du réseau intranet de l'Université de Lomé s'inscrit dans le cadre d'un audit de validation, dont l'objectif principal est d'évaluer la mise en œuvre des recommandations issues de l'audit initial du Système d'Information (SI). Il vise à :

- vérifier l'état d'avancement des actions correctives et des améliorations apportées ;
- identifier les éventuelles lacunes persistantes ou nouvelles vulnérabilités ;
- s'assurer de la conformité du SI aux bonnes pratiques et standards de sécurité ;
- proposer des recommandations stratégiques pour renforcer la résilience et la gouvernance du SI.

Contexte de l'audit initial

L'audit initial du SI de l'Université de Lomé a mis en lumière plusieurs failles de sécurité et insuffisances impactant la confidentialité, l'intégrité et la disponibilité des systèmes.
Parmi les principales observations :

- absence de gouvernance IT et de documentation du SI ;
- manque de contrôle des accès physiques et logiques aux ressources critiques ;
- absence de solution de centralisation des logs et d'outils de supervision avancés ;
- vulnérabilités sur l'infrastructure réseau et les systèmes applicatifs ;
- absence d'une politique de gestion des mises à jour et des vulnérabilités ;
- faiblesse des mesures de sauvegarde et de continuité d'activité.

Face à ces constats, des recommandations stratégiques ont été formulées pour renforcer la sécurité et l'efficacité du SI de l'université.

Méthodologie utilisée

L'audit de validation a été conduit selon une approche multicritère et structurée, combinant :

- analyse documentaire : rapport de l'audit initial et architecture réseau à jour ;
- tests techniques : scans de vulnérabilités ;
- entretiens avec les parties prenantes : DSI et équipes IT ;
- revue des mesures de sécurisation mises en place depuis l'audit initial ;
- benchmark avec les bonnes pratiques et standards internationaux.

Principaux résultats

L'audit de validation a permis de constater des avancées significatives sur certains aspects du SI, notamment :

- renforcement de la sécurité physique avec la mise en place de la vidéosurveillance dans les salles serveurs ;
- correction de certaines vulnérabilités ;
- segmentation du réseau de l'université de Lomé.

Cependant, plusieurs lacunes critiques subsistent :

- salle serveur inadapté ;
- manque de documentation du SI ;
- absence d'un SIEM pour la corrélation et la surveillance des événements de sécurité ;
- manque d'une solution EDR avancée pour la protection des postes de travail ;
- existence de certaines failles de sécurité non corrigées exposées sur Internet, augmentant le risque d'attaques externes ;
- utilisation de protocoles et d'algorithmes de chiffrement obsolètes ;
- absence d'une politique de gestion des mises à jour et des vulnérabilités ;
- faible sensibilisation des utilisateurs aux risques cyber.

Recommandations principales

Les principales recommandations adressées à l'Université de Lomé sont les suivantes :

- mise en place de nouveaux datacenter normés ;
- la mise en place d'une gouvernance de la cybersécurité à travers un Schéma Directeur du SI et une PSSI ;
- le déploiement d'un SIEM pour la centralisation et l'analyse des logs en temps réel ;
- l'adoption d'une solution EDR pour renforcer la protection des postes ;
- l'intégration d'une solution de gestion des mises à jour et des vulnérabilités ;
- la création d'une équipe SOC interne ou externalisation auprès d'un prestataire spécialisé ;
- l'organisation de tests d'intrusion réguliers pour identifier et corriger les failles exploitables ;
- le déploiement d'une plateforme de sensibilisation pour renforcer la cybersécurité au sein de l'université.

1. CONTEXTE GENERAL

Dans un contexte de transformation numérique et d'amélioration continue des infrastructures informatiques, l'Université de Lomé a initié une série d'actions visant à renforcer la performance et la sécurité de son réseau Intranet. Dans cette dynamique, un premier audit du réseau de l'UL a été commandité afin d'identifier les manquements et les améliorations à apporter, notamment en matière de :

- performance et évolutivité du réseau, en mettant l'accent sur la mise à niveau du cœur du réseau et le câblage complémentaire en fibre optique ;
- gestion des services disponibles, avec un focus sur l'optimisation et l'intégration de nouvelles fonctionnalités adaptées aux besoins croissants des utilisateurs.

À la suite de cet audit, des recommandations ont été formulées et mises en œuvre par la Direction des Ressources et des Systèmes d'Information (DRSI), anciennement le Centre Informatique et de Calcul (CIC), qui gère l'Intranet de l'UL. Ces recommandations ont conduit à l'acquisition et à l'installation de nouveaux équipements au second semestre de 2020, permettant ainsi d'améliorer :

- la disponibilité et la continuité de service, grâce à l'installation d'un groupe électrogène couplé aux onduleurs et à l'énergie fournie par la CEET ;
- la sécurité physique, avec le remplacement des portes et fenêtres en bois par portes et fenêtres en aluminium ;
- la résilience du système, par la mise en place d'une redondance du système de climatisation et l'installation d'extincteurs dans les locaux techniques ;
- la capacité d'hébergement et de traitement, à travers l'acquisition de serveurs plus puissants ;
- l'évolutivité de l'infrastructure, avec l'intégration de nouveaux switchs au cœur du réseau et d'un pare-feu (firewall) performant ;
- la gestion optimisée du trafic et de la qualité de service (QoS), via l'ajout d'un Peplink pour la redondance des connexions Internet et la gestion de la DMZ.

Depuis ces améliorations, l'Intranet de l'UL a connu une augmentation significative du trafic ainsi qu'une mise à niveau des logiciels et services proposés aux utilisateurs. Cependant, cette évolution rapide entraîne l'émergence de nouveaux besoins et de nouveaux défis en termes de performance, de cybersécurité et d'optimisation des opérations.

Ainsi, ce nouvel audit vise à certifier la conformité des recommandations précédentes, évaluer leur efficacité et proposer de nouvelles orientations stratégiques adaptées aux pratiques actuelles et aux exigences futures. Les résultats de cet audit contribueront également à l'élaboration d'un budget prévisionnel pour assurer le bon fonctionnement et la pérennité du système d'information de l'UL, sous la supervision de la DRSI.

2. MANAGEMENT DU PROJET DE CERTIFICATION

2.1 Objectifs de la certification

L'objectif de cet audit de validation est la vérification des installations réalisées dans les deux locaux techniques afin de confirmer ou d'émettre des réserves sur les recommandations faites lors de l'audit réalisé en 2020 concernant les améliorations à apporter au niveau :

- des alimentations de secours ;
- de la sécurité des portes des locaux techniques ;
- de la redondance du système de climatisation dans les salles serveurs et de la mise à disposition des extincteurs
- de l'acquisition de serveurs adaptée aux besoins des sollicitations et de stockage ;
- des équipements de filtrage et d'évolutivité au niveau du cœur du réseau ;
- de la disponibilité des outils de gestion de la qualité de service (QoS) et de la bande passante ;
- de l'optimisation et gestion sécurisée des serveurs avec les services offerts comme DHCP, DNS, la messagerie, les services web et services connexes ;
- des recommandations pour les opérations futures de veille technologique.

2.2 Périmètre de la mission

Le périmètre de notre mission porte sur la validation des mesures correctives mises en place dans le système d'information de l'Université de Lomé, en réponse aux recommandations de l'audit initial, ainsi que sur la proposition de nouvelles directives. Cette évaluation couvre les domaines suivants :

- l'infrastructure du SI : analyse de l'architecture réseau, des équipements, des serveurs et du stockage ;
- l'organisation du SI : évaluation des processus, des responsabilités et de la gouvernance du système d'information ;
- la sécurité du SI : identification des vulnérabilités, des mesures de protection en place et des bonnes pratiques de cybersécurité ;
- la disponibilité du SI : vérification des mécanismes de redondance, de sauvegarde et des solutions de continuité d'activité.

et subdivisée en 5 catégories du SI : données, environnement & matériel, logiciels & systèmes, pilotage & gouvernance SI, enfin Réseaux et Télécommunications.

Cette mission a été réalisée sans accès à la configuration des actifs du système d'information de l'université de Lomé.

Elle s'est limitée à :

- l'évaluation des infrastructures existantes sur la base des observations physiques et des échanges avec les équipes techniques ;
- l'analyse des documents disponibles relatifs à l'architecture du SI et aux politiques de sécurité en place ;
- l'identification des vulnérabilités et des risques majeurs impactant le SI.

L'absence d'accès direct aux configurations des équipements réseau, serveurs et systèmes de sécurité a restreint l'analyse aux éléments observables et déclarés par les responsables informatiques.

2.3 Référentiels utilisés

Cet audit a été réalisé en s'appuyant sur les normes et bonnes pratiques suivantes :

- ISO/IEC 27001 : système de management de la sécurité de l'information (SMSI) ;
- ISO/IEC 27002 : code de bonnes pratiques pour la gestion de la sécurité de l'information ;
- ISO/IEC 27005 : gestion des risques liés à la sécurité de l'information ;
- ISO/IEC 27040 : sécurité des informations stockées ;
- ISO/IEC 27033 : sécurité des réseaux ;
- COBIT 5 : gouvernance et management des systèmes d'information ;
- ITIL 4 : gestion des services informatiques (ITSM).

2.4 Equipe du projet

L'équipe du projet est constituée comme suit :

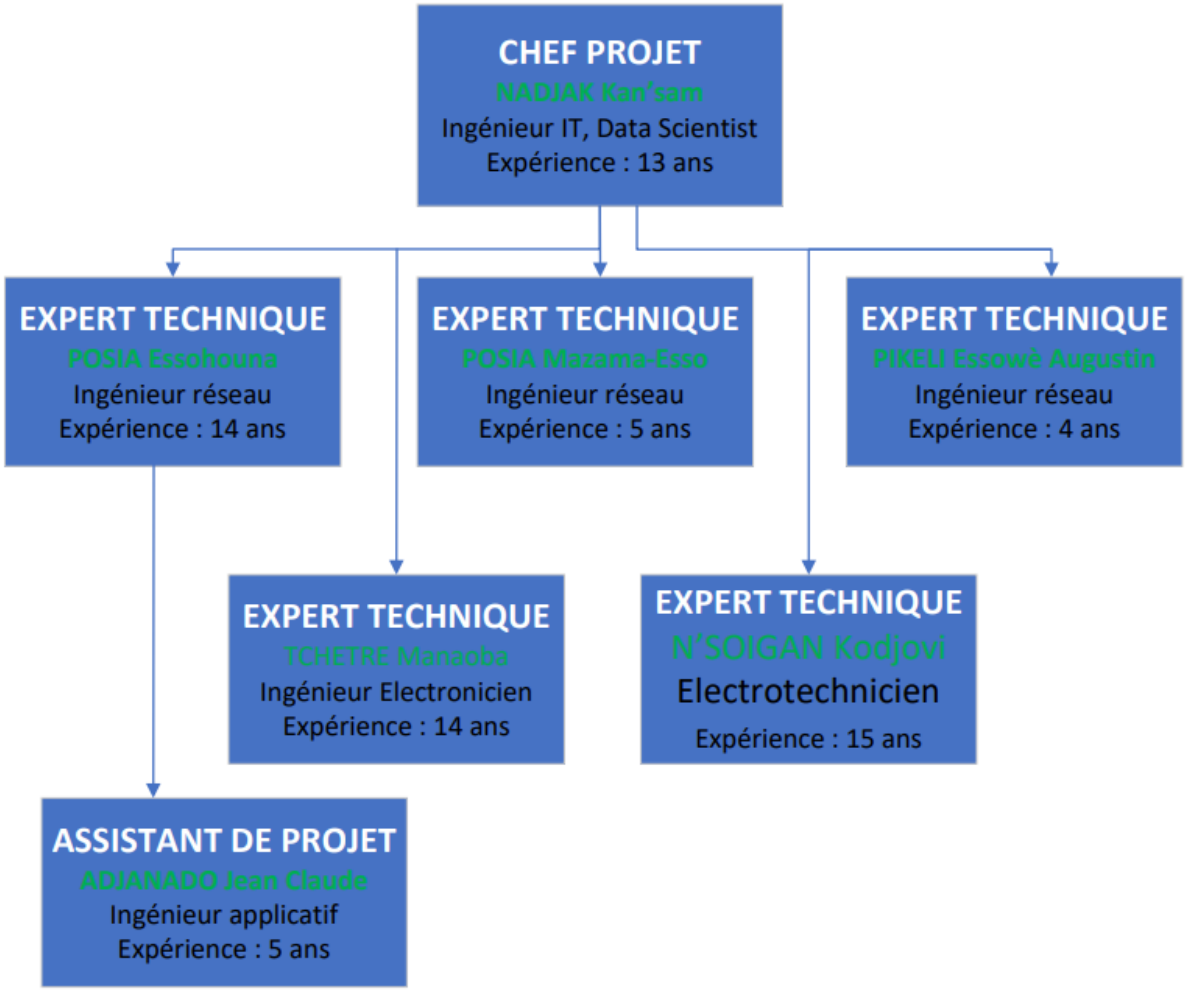


Figure 1: Equipe projet

2.5 Planification de la mission

CALENDRIER DES PRESTATIONS ET PRODUCTION DES RAPPORTS	S1							S2							S3							S4							S5							S6						
	L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D	L	M	M	J	V	S	D
Activité 0 : Préparation et Planification																																										
Act 0.1 Rencontre Initiale et Planification																																									
Réunion de démarrage avec les responsables de la DRSI pour clarifier les objectifs et attentes.																																									
Collecte et analyse des documents pertinents (rapports d'audit, schémas du réseau, etc.).																																									
Définition du calendrier détaillé des activités.																																									
Allocation des ressources nécessaires pour chaque étape de la mission.																																									
Coordination avec les équipes internes et externes.																																									
Analyse des schémas et informations collétées																																									
Activité 1 : Verification des installations et reponse aux questionnaires																																									
Act 1.1 Séance de reponses aux questionnaires																																									
Presenter l'ensemble du questionnaire pour donner une meilleur analyse de l'Infrastructure																																									
Analyse des équipements réseau, y compris les switchs, routeurs, et firewalls.																																									
Act 1.2 : Inspection Physique des Locaux Techniques																																									
Vérification des installations électriques, du systèmes de climatisation, et des équipements de sécurité.																																									
Évaluation des locaux techniques et des équipements de sécurité																																									
Act 1.3 Analyse des Équipements Réseau et systèmes																																									
Vérification de l'installation et du fonctionnement des serveurs.																																									

CALENDRIER DES PRESTATIONS ET PRODUCTION DES RAPPORTS	S1	S2	S3	S4	S5	S6
Évaluation de la capacité et de la résilience du cœur du réseau						
Identification des points de congestion ou de saturation au niveau du cœur						
Analyse des équipements réseau, y compris les switchs, routeurs, et firewalls.						
Inspection des performances des réseaux de distribution cuivre et fibre optique						
Act 1.4 Scans de vulnérabilités						
Exécution d'un scan de vulnérabilités sur les équipements réseau internes						
Identification des failles potentielles						
Act 1.5 Certification des médias						
Certification des câbles Ethernet et fibre optique à l'aide d'un testeur certifié						
Activité 2 : Validation et Comparaison						
Act 2.1:Comparaison avec l'Audit Précédent						
Identification des écarts entre les installations actuelles et les recommandations de l'audit précédent.						
Documentation des écarts et propositions de mesures correctives						
Act 2.2:Recommandations Futures						
Propositions d'améliorations pour la gestion des services et des équipements réseau.						
Identification des besoins futurs pour assurer la veille technologique.						
Activité 3 :Rédaction et Présentation du Rapport						
Act 3.1:Rédaction du Rapport						
Compilation des observations et résultats.						
Rédaction d'un rapport détaillé incluant les améliorations constatées, les nouveaux problèmes éventuels, et les recommandations.						
Act 3.2:Présentation du Rapport						

CALENDRIER DES PRESTATIONS ET PRODUCTION DES RAPPORTS	S1	S2	S3	S4	S5	S6
Organisation d'une réunion avec les responsables de la DRSI pour présenter et discuter le rapport final.						
Ajustements et modifications en fonction des retours des responsables de la DRSI.						
Soumission du Rapport Final et Signature des Procès-Verbaux de Réception du Projet de Certification						

Tableau 1: Planification de la mission

2.6 Méthodologie de la mission de certification

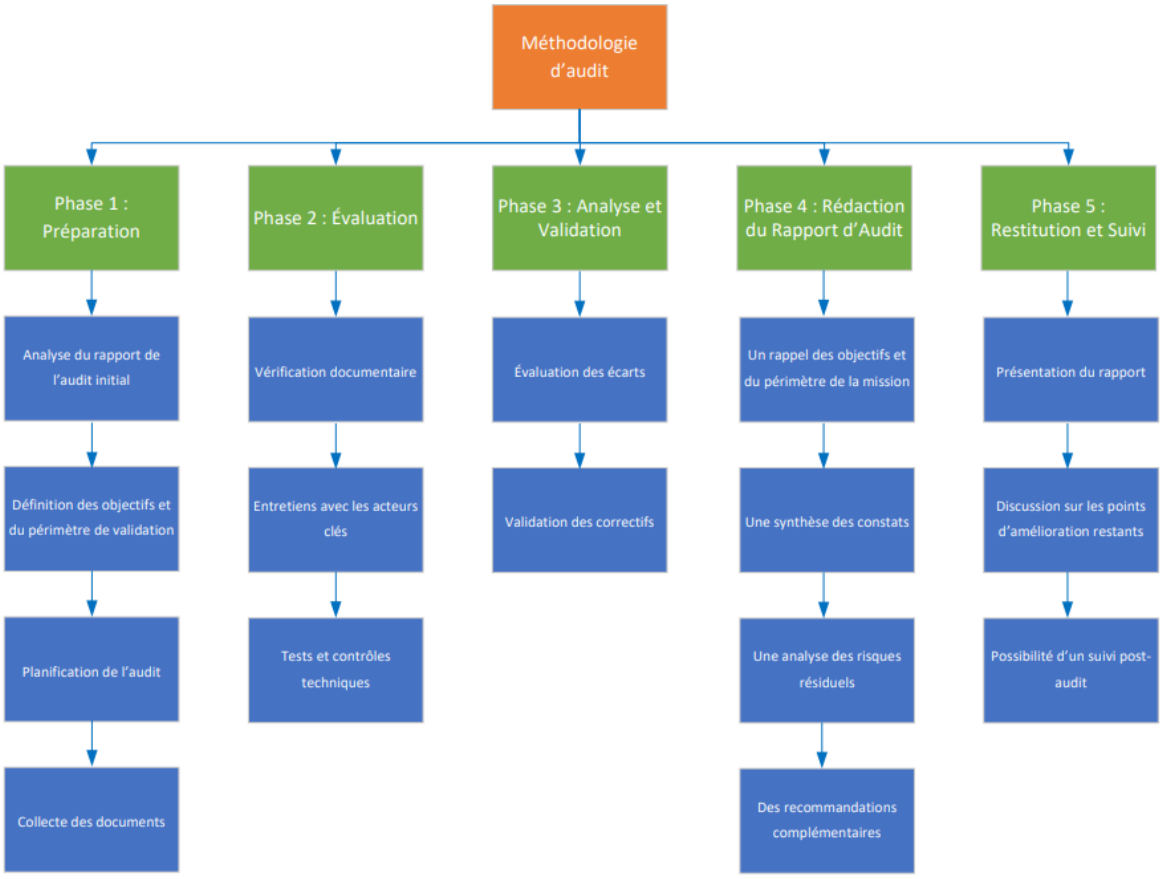


Figure 2: Méthodologie d'audit

3. RAPPEL DU CONTEXTE

3.1 Objectifs de l'audit initial

L'audit initial visait à analyser et évaluer le système d'information de l'Université de Lomé à travers plusieurs aspects clés, notamment :

- L'étude du réseau d'interconnexion Ethernet ;
- L'évaluation de la sécurité du réseau ;
- L'analyse de la gestion du système d'information ;
- L'examen de l'architecture d'entreprise ;
- L'identification des considérations générales liées à un système d'information modernisé.

À l'issue de cet audit, l'Université de Lomé et ses acteurs ont bénéficié des résultats suivants :

- diagnostic du réseau d'interconnexion Ethernet réalisé ;

- état des lieux du fonctionnement des infrastructures réseau et de la sécurité établi ;
- analyse des besoins en modernisation de la gestion de la sécurité de l'information effectuée ;
- identification des forces et faiblesses du système d'information actuel, accompagnée de recommandations d'amélioration.

3.2 Principales non-conformités identifiées

Lors de l'audit initial, plusieurs lacunes et non-conformités ont été détectées et classées selon leur domaine d'application. Ci-dessous les non-conformités identifiées, issues du rapport des auditeurs :

Description des Sujets	Lacunes identifies
Technologie de mise en réseaux	
Configuration des composants réseau et infrastructures	Le réseau Ethernet est à reconstituer
	On constate un manque d'organisation de la gestion de l'infrastructure réseau
	Il n'y a pas une équipe d'architecture dédiée à la gestion des infrastructures informatiques de l'université
	Il n'y a pas un plan ni schéma directeur du système d'information élaboré
	Sans plan directeur, le système d'information n'est pas géré
	Le SI est géré par une division
	On constate une méthode archaïque de gestion du patrimoine informatique
	Les configurations sont gérées de façon manuelle donc exposée a des erreurs humaines
Connexion Internet et performances	
Internet & Network Performance	Nous avons du réseau Ethernet et rien dans le cloud
	Il y a trois besoins de bande passante
	L'expression du besoin est basée sur les services
	Avec 3 sources de bande passante il serait difficile de gérer un réseau stable
	On note une bonne mesure de suivi de la performance mais il manque un outil.
	On note une congestion lors des inscriptions scolaires et les saisies des notes donc l'utilisation des applicatifs métiers / scolaires
	Mais ces utilisations des bandes passantes ne sont pas nécessairement alignées avec les besoins du métier
	Pas de mesure de filtrage de flux ni de mesure d'amélioration de performance du réseau
Communications de Données	
	Aucune classification des données

	Aucun contrôle des données trafiquées. Il n'y a pas de traitement spécial des données
Outils de surveillance	
	Nous constatons l'existence de bonne méthode de réseau mais sans corrélation des incidents ni une journalisation efficace. Ceci peut exposer à des risques sévères
Sécurité du Réseau	
LAN	Le schéma fournit n'est pas descriptif de la réalité au sol et une constitution du réseau sera faite
	17 VLANs et deux zones existent pour le réseau mais avec une absence de règles pare-feu spécifiques et donc sans rapports
	La liste des équipements fournis n'est pas complète et ne reflète pas le réseau au sol.
Infrastructure	Seulement deux composants mineurs sont utilisés pour le contrôle de la sécurité. Pas d'anti-virus sur tous les éléments pour contrôler la sécurité et pas d'outils de prévention de la perte de donnée. La sécurité du réseau n'est pas bien gérée et cause de sérieux risques.
WI FI	Les réseaux Wifi sont mal configurés, pas de sécurité et mal gérés
Backups	Il y a une procédure de sauvegarde mais nous constatons que les données ne sont pas répliquées. Le réseau est exposé à des risques de perte de données des applications
Vulnerability Management & Intrusion tests	Aucune mesure de vulnérabilité prises dans la gestion des infrastructures
Continuité des activités et reprise après sinistre	
	Aucune stratégie de continuité des activités. Pas de plan de continuité d'affaires et de reprises de données

Tableau 2: Lacunes identifiées issue de l'audit initial

3.3. Recommandations formulées

Les recommandations formulées à l'issue de l'audit initial sont :

3.3.1 Gestion de l'infrastructure réseaux

Item #	Topics	Description de l'Analyse Faite	Action corrective prévue
Technologies Réseaux			
1	**Technologie réseau**	***Infrastructure physique***	Veiller lors de l'acquisition à avoir des équipements réseaux professionnels de même marque pour faciliter l'interopération et l'administration
			Reprise des câblages non conformes des sites distants
			Les équipements amateurs ne doivent être installés que dans le réseau d'accès
			Les liaisons pour la distribution vers les bâtiments doivent être en FO
			Les liaisons de la distribution doivent être redondantes ou deux paires de brins dans la FO
			Changer le switch de CIC par un CLUSTER de niveau 3 et veiller à avoir ces switchs de niveau 3 au cœur et dans la distribution du réseau
			Dans le CORE NETWORK, enlever les switchs NETIS et relier directement les switchs CISCO au PEPLINK
2		***Performance du réseau***	Respecter les normes de la topologie étoile suivant le Coeur, la distribution et l'accès
			Tous les 34 bâtiments doivent être reliés au cœur du réseau
			définir des access-list pour éviter tous les paquets empruntent tous les chemins
3		***Gestion du réseau***	Exploiter en plus de PRTG, PEPLINK et MONIT, les outils des équipements professionnels uniformisés qui seront installés sur le réseau pour faire la découverte du réseau et son administration
4			Prévoir l'extension du réseau dans sa configuration
Internet Connection and Performance			
5		***Accessibilité***	Segmenter le réseau

Item #	Topics	Description de l'Analyse Faite	Action corrective prévue
	Performance de la connexion internet		Définir les accès à la connexion internet suivant les périodes d'affluence
		Stabilité et fiabilité	Dédier les connexions internet selon les besoins
			Solliciter une bande passante suffisante pour l'université
Data Communication			
6	**Communication de données**	***Accessibilité et fluidité***	Installer des logiciels actualisés sur les périphériques du réseau
			Définir des access-lists sur les switchs à l'entrée des blocs pour une rationalisation des ressources du réseau
Sécurité du Réseau			
7	**La sécurité des données**	***Sécurité physique du réseau***	Veiller à avoir une sale des serveurs qui respectent les normes en la matière
			Installer les équipements de bout de chaine dans des Racks
			Restreindre l'accès aux locaux informatiques aux personnes indiqués
			Eviter d'accepter sur le réseau tous les périphériques non identifiés et authentifiés
8		***Sécurité logique du réseau***	Installés des logiciels certifiés sur le réseau
			Bloquer au niveau des swiths et des routeurs tous les ports non nécessaires
			Préférer le protocole ssh au telnet pour l'accès aux équipements réseaux
			Veiller à l'installation d'antivirus à jour sur les postes des utilisateurs

Tableau 3: Recommandations infrastructure réseaux issue de l'audit initial

3.3.2 Recommandations de la sécurité

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité
Réseau					
Réseau UL segmenté non cloisonné	*Réseau UL*	**Elevée**	**INT1**	Il est recommandé de segmenter le réseau de l'UL en zones spécifiques. Envisager notamment de séparer les serveurs, les administrateurs, les utilisateurs, le top management, les DMZ (public, privée, partenaire, ...)	**2**
Usurpation d'IP sur le réseau interne (Ecoute des flux)	*Réseau UL*	**Elevée**	**INT2**	Enregistrer statiquement les tables ARP dans les systèmes d'exploitation. Bloquer les paquets gratuitous ARP » (paquets réseau non voulus / inutile / suspect) Détecter par les IDS Mettre en place un DAI (Dynamic ARP Protection) Utiliser les protocoles sécurisés comme SSH, SFTP, HTTPS.. à la place de Telnet, FTP, HTTP	**1**
Service Telnet et HTTP non crypté	*Réseau UL*	**Elevée**	**INT3**	Désactivez le service Telnet et utiliser SSH à la place et https à la place de http	**2**
Constats sur les Postes de travail /Serveurs					
Système d'exploitation obsolète avec multiple vulnérabilités	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT4**	Il est recommandé de passer vers une version de Windows qui est actuellement pris en charge (Microsoft Windows Server 2016 & 2019 pour les	**1**

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité
				serveurs ; Windows 10 pour les PCs), et assurer les mises à jour.	
Applications installées vulnérable	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT5**	Mettre à jour les applications installées sur les serveurs et les postes de travail	**1**
Stockage des mots de passe vulnérable	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT6**	Désactiver le stockage des paramètres d'authentification windows via le LM Hash	**1**
Multiples vulnérabilités au niveau du protocole SSL/TLS	*Postes / Serveurs du Parc Informatique*	**Moyen**	**INT8**	Mettre à jour le protocole comme suit : Utiliser OpenSSL 3.0 Désactiver les versions SSL 2.0 et SSL 3.0, pour n'utiliser que le TLS 1.3 et RDP, HTTP, et il est recommandé d'installer RDS (Remote Desktop Service) pour prendre en charge le protocole TLS 1.3	**3**
Vulnérabilités liées au manque de mise à jour et les correctifs de sécurité	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT9**	Appliquer les mises à jour du serveur en suivant la politique des mises à jour et à l'aide des outils dédiés comme WSUS pour Microsoft,	**1**
Politique de contrôle des applications et des périphériques USB	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT10**	Créer et appliquer une politique de contrôle des applications et des périphériques USB	**1**
Signature de sécurité SMB désactivé	*Postes / Serveurs du*	**Moyen**	**INT11**	Activer et mettre à jour la signature de sécurité SMB	**2**

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité
	Parc Informatique				
Microsoft Windows divulgation de l'information	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT12**	Appliquer les patchs publiés par microsoft	**1**
MS10-061: Microsoft Windows buffer overflow	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT13**	Appliquer les patchs publiés par microsoft	**1**
Equipement de sécurité					
Multiple Vulnérabilités port SSH /FTP /HTTP .. ouvert	*172.20.0.2*	**Elevée**	**INT15**	Faire une revue des règles, désactiver les ports inutiles non sécurisés et activer TLSv1.3 avec une suite de chiffrement fiable	**1**
Utilisation d'une solution obsolète	*172.20.0.2*	**Elevée**	**INT16**	Il faut migrer vers une version plus récente du firmware	**1**
Serveurs					
Multiple Vulnérabilités SSL	*172.20.1.3*	**Moyen**	**INT18**	Désactiver SSLv2, SSLv3, TLSv1 et TLSv1.1 et activer TLSv1.3 avec une suite de chiffrement fiable	**1**
CVSS v3.0 Vulnérabilité Exécution Code à distance PHP	*172.20.1.3*	**Elevée**	**INT19**	Mettre à jour PHP vers une version récente	**1**
Détection de la version de PHP non supportée	*172.20.1.3*	**Elevée**	**INT20**	Mettre à jour PHP vers une version à jour	**1**
JQUERY 1.2 < 3.5.0 Multiple XSS	*172.20.1.2*	**Moyen**	**INT21**	Mettre à jour la version de Jquery vers 3.5.0 ou ultérieure	**1**

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité
Le serveur Web distant autorise la methode TRACK et TRACE	*172.20.1.2* *172.20.1.8*	**Moyen**	**INT22**	Désactiver ces méthodes HTTP	**1**
Le serveur Web distant ne fixe pas d'en-tête de réponse X-Frame-Options	*41.207.188.27*	**Elevée**	**INT23**	Retournez l'en-tête HTTP X-Frame-Options ou Content-Security-Policy (avec la directive « frame-ancestor » avec la réponse de la page.	**1**
Le Certificat SSL ne peut pas être approuvé	*172.20.1.2*	**Moyen**	**INT24**	Générer un Certificat SSL propre à ce service	**1**
Agent SNMP avec communauté par défaut (public)	*172.20.1.2*	**Elevée**	**INT25**	Désactivez le service SNMP sur l'hôte distant s'il n'est pas utilisable Restreindre et surveiller l'accès à ce service ; changer la chaîne de communauté par défaut	**1**

Tableau 4: Recommandations de la sécurité issue de l'audit initial

3.3.3 Bonnes pratiques

ID	Bonnes pratiques	Constat	Statut	Action corrective prévue	Priorité
PC1	**Utilisation d'un système d'exploitation supporté pour toutes les machines utilisateur**	Les machines du parc informatique utilisent des différents OS tel que windows Xp, 7, 8,1 et 10.	**NC**	Utiliser un OS supporté (windows 8,1 ou 10) sur toutes les machines du parc informatique	**1**
PC2	**Mise en place d'un serveur Active Directory et Intégrer les postes de travail du SI au domaine**	Pas de serveur Active Directory dans le réseau et donc les postes de travail appartiennent par défaut au WORKGROUP	**NC**	Il est recommandé de mettre en place un serveur Active Directory et d'intégrer les postes de travail au domaine afin de pouvoir appliquer des stratégies de groupe définies pour chaque ordinateur / utilisateur	
PC3	**Installation des mises à jour Windows**	Les mises à jour sont gérées individuellement et manuellement	**NC**	Il est recommandé de mettre en place une solution de gestion des MAJs comme WSUS pour les produits Microsoft	**2**
PC4	**Antivirus**	La solution antivirale "Kaspersky" est déployée pour certains postes de travail.	**NC**	Faire une acquisition d'une solution antivirale Professionnelle de préférence "Client-Serveur" permettant de mieux gérer le	**1**

ID	Bonnes pratiques	Constat	Statut	Action corrective prévue	Priorité
				déploiement et la gestion des mises à jour	
		L'Université de Lomé ne dispose pas à date de licence de solution antivirale déployée sur l'ensemble du parc Informatique		Appliquer une politique de sécurité optimale et effectuer une revue régulière des mises à jour des postes de travail	
PC5	**Restriction des droits d'installation**	Les utilisateurs ont des privilèges sur les postes de travail et peuvent installer toute application sans validation de l'équipe SI.	**NC**	Définir pour chaque groupe les applications autorisées à l'installation.	**2**
				Rappeler la nécessité de n'installer que les applications autorisées et nécessaires dans le cadre professionnel	
PC6	**Utilisation des supports amovibles**	Les ports USB ne sont pas verrouillés.	**NC**	Faire une revue régulière des utilisateurs ayant les droits d'utilisation des ports USB	**1**
		Tous les utilisateurs ont le droit d'utiliser les ports USB (administrateurs, direction, …)			

ID	Bonnes pratiques	Constat	Statut	Action corrective prévue	Priorité
PC7	**Pare-feu local**	Les postes utilisateurs sont protégés par le pare-feu de la solution antivirale (Protection contre les menaces réseau).	**NC**	Activer le parfeux de la solution antivirale ou de windows	**2**
PC8	**Connexions RDP vers les serveurs**	Tous les postes de travail ont accès aux ports de connexion à distance de tous les serveurs (SSH, RDP, …)	**NC**	Limiter les connexions possibles sur les serveurs depuis les postes utilisateur (utiliser de préférence un pare-feu interne à cet effet, et une segmentation adéquate du réseau)	**1**
PC9	**Sécurité du BIOS**	Le mot de passe du BIOS n'est pas activé	**NC**	Définir un mot de passe du BIOS pour tous les postes du parc informatique	**2**
PC10	**Verrouillage automatique de session**	La politique de fermeture automatique des sessions n'est pas définie pour l'ensemble des postes de travail Les sessions de plusieurs postes de travail ont été trouvées non verrouillées	**NC**	Définir dans la politique de groupe du contrôleur de domaine le délai de verrouillage automatique de sessions et la déployée à l'ensemble des postes de travail	**1**

ID	Bonnes pratiques	Constat	Statut	Action corrective prévue	Priorité
		au-delà d'une heure d'inactivité			

Tableau 5: Bonnes pratiques issue de l'audit initial

3.4 Objectifs de la validation

Cet audit de validation vise à évaluer la mise en œuvre des recommandations issues de l'audit initial et à s'assurer que les mesures correctrices adoptées répondent aux exigences définies. Plus précisément, il poursuit les objectifs suivants :

- Vérification de l'application des recommandations :
    - examiner l'état d'avancement des actions correctives mises en place ;
    - identifier les recommandations pleinement appliquées, partiellement mises en œuvre ou non traitées.
- contrôle de la conformité :
    - s'assurer que les nouvelles pratiques respectent les bonnes pratiques et réglementations applicables ;
    - détecter d'éventuelles nouvelles non-conformités ou lacunes.
- proposition d'améliorations complémentaires
    - formuler des recommandations supplémentaires si des faiblesses persistent ;
    - accompagner l'Université de Lomé dans l'optimisation continue de son système d'information.

Cet audit de validation permettra ainsi de garantir que les correctifs apportés sont efficaces, conformes et adaptés aux besoins de l'université.

4. ETATS DES RECOMMANDATIONS DE L'AUDIT INITIAL

A l'issue de l'audit initial, ci-après les recommandations formulées par les précédents auditeurs, accompagnées de leur statut indiquant si elles ont été mises en œuvre ou, le cas échéant, restent en attente de mise en place.

4.1 Gestion de l'infrastructure réseaux

Item #	Topics	Description de l'Analyse Faite	Action corrective prévue	Action mise en place ? (Oui/Non/En cours)	Commentaires
Technologies Réseaux					
1	**Technologie réseau**	***Infrastructure physique***	Veiller lors de l'acquisition à avoir des équipements réseaux professionnels de même marque pour faciliter l'interopération et l'administration	Non	Aucune action mise en place
			Reprise des câblages non conformes des sites distants	Oui	Certains ont été repris
			Les équipements amateurs ne doivent être installés que dans le réseau d'accès	Oui	Certains ont été remplacé
			Les liaisons pour la distribution vers les bâtiments doivent être en FO	Oui	Cela a été corrigé
			Les liaisons de la distribution doivent être redondantes ou deux paires de brins dans la FO	Oui	Action mise en place
			Changer le switch de CIC par un CLUSTER de niveau 3 et veiller à avoir ces switchs de niveau 3 au cœur et dans la distribution du réseau	Non	Action non mise en place
			Dans le CORE NETWORK, enlever les switchs NETIS et relier directement les switchs CISCO au PEPLINK	Oui	Action mise en place

Item #	Topics	Description de l'Analyse Faite	Action corrective prévue	Action mise en place ? (Oui/Non/En cours)	Commentaires
2		***Performance du réseau***	Respecter les normes de la topologie étoile suivant le Coeur, la distribution et l'accès	Oui	La topologie étoile suivant le cœur, la distribution et l'accès a été respecté par contre tous les bâtiments n'ont pas été reliés au cœur du réseau
			Tous les 34 bâtiments doivent être reliés au cœur du réseau	Non	
			Définir des access-list pour éviter tous les paquets empruntent tous les chemins	Oui	Action mise en place
3		***Gestion du réseau***	Exploiter en plus de PRTG, PEPLINK et MONIT, les outils des équipements professionnels uniformisés qui seront installés sur le réseau pour faire la découverte du réseau et son administration	Oui	Nagios installé au cœur du réseau
5			Prévoir l'extension du réseau dans sa configuration	Non	Aucune action mise en place
Internet Connection and Performance					
6	**Performance de la connexion internet**	***Accessibilité***	Segmenter le réseau	Oui	
			Définir les accès à la connexion internet suivant les périodes d'affluence	Non	
		Stabilité et fiabilité	Dédier les connexions internet selon les besoins	Non	Mise à jour 100 Mps en symétrique

Item #	Topics	Description de l'Analyse Faite	Action corrective prévue	Action mise en place ? (Oui/Non/En cours)	Commentaires
			Solliciter une bande passante suffisante pour l'université	Oui	
Data Communication					
7	**Communication de données**	***Accessibilité et fluidité***	Installer des logiciels actualisés sur les périphériques du réseau	En cours	Certains équipements réseaux restent vulnérable Des switchs de management en cours d'installation sur les sites
			Définir des access-lists sur les switchs à l'entrée des blocs pour une rationalisation des ressources du réseau	En cours	
Sécurité du Réseau					
8	**La sécurité des données**	***Sécurité physique du réseau***	Veiller à avoir une sale des serveurs qui respectent les normes en la matière	En cours	Certains serveurs toujours posés sur des tables ; les entrées ne sont pas documentées
			Installer les équipements de bout de chaine dans des Racks	Non	
			Restreindre l'accès aux locaux informatiques aux personnes indiqués	Oui	
			Eviter d'accepter sur le réseau tous les périphériques non identifiés et authentifiés	Oui	
9		***Sécurité logique du réseau***	Installés des logiciels certifiés sur le réseau	Oui	Certains équipements réseaux utilisent toujours du Telnet

Item #	Topics	Description de l'Analyse Faite	Action corrective prévue	Action mise en place ? (Oui/Non/En cours)	Commentaires
			Bloquer au niveau des switchs et des routeurs tous les ports non nécessaires	Oui	
			Préférer le protocole ssh au telnet pour l'accès aux équipements réseaux	Non	
			Veiller à l'installation d'antivirus à jour sur les postes des utilisateurs	Non	

Tableau 6: Etat des recommandations sur l'infrastructure réseaux

4.2 Sécurité du SI

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
Réseau							
Réseau UL segmenté non cloisonné	*Réseau UL*	**Elevée**	**INT1**	Il est recommandé de segmenter le réseau de l'UL en zones spécifiques.	**2**	Oui	Réseau segmenté

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
				Envisager notamment de séparer les serveurs, les administrateurs, les utilisateurs, le top management, les DMZ (public, privée, partenaire, ...)		Oui	Action mise en place
Usurpation d'IP sur le réseau interne (Ecoute des flux)	*Réseau UL*	**Elevée**	**INT2**	Enregistrer statiquement les tables ARP dans les systèmes d'exploitation.	**1**	Non	Action non mise en place
				Bloquer les paquets gratuitous ARP » (paquets réseau		Non	Action non mise en place

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
				non voulus / inutile / suspect)			
				Détecter par les IDS		Non	Action non mise en place
				Mettre en place un DAI (Dynamic ARP Protection)		Oui	Action mise en place
				Utiliser les protocoles sécurisés comme SSH, SFTP, HTTPS.. à la place de Telnet, FTP, HTTP		En cours	Certains protocoles non sécurisés restent utilisés dans le SI
Service Telnet et HTTP non crypté	*Réseau UL*	**Elevée**	**INT3**	Désactivez le service Telnet et utiliser SSH à la place et https à la place de http	**2**	En cours	Il en reste encore
Constats sur les Postes de travail /Serveurs							

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
Système d'exploitation obsolète avec multiple vulnérabilités	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT4**	Il est recommandé de passer vers une version de Windows qui est actuellement pris en charge (Microsoft Windows Server 2016 & 2019 pour les serveurs ; Windows 10 pour les PCs), et assurer les mises à jour.	**1**	Non	Pas de Windows server dans le SI Pas de contrôle sur les mises à jour
Applications installées vulnérable	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT5**	Mettre à jour les applications installées sur les serveurs et les postes de travail	**1**	En cours	Pas de politique de gestion de mise à jour

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
Stockage des mots de passe vulnérable	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT6**	Désactiver le stockage des paramètres d'authentification windows via le LM Hash	**1**	Non	Aucune action mise en place
Multiples vulnérabilités au niveau du protocole SSL/TLS	*Postes / Serveurs du Parc Informatique*	**Moyen**	**INT8**	Mettre à jour le protocole comme suit :	**3**		
				Utiliser OpenSSL 3.0		En cours	
				Désactiver les versions SSL 2.0 et SSL 3.0, pour n'utiliser que le TLS 1.3 et RDP, HTTP, et il est recommandé d'installer RDS (Remote Desktop		En cours	

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
				Service) pour prendre en charge le protocole TLS 1.3			
Vulnérabilités liées au manque de mise à jour et les correctifs de sécurité	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT9**	Appliquer les mises à jour du serveur en suivant la politique des mises à jour et à l'aide des outils dédiés comme WSUS pour Microsoft,	**1**	Non	Aucune action mise en place
Politique de contrôle des applications et des périphériques USB	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT10**	Créer et appliquer une politique de contrôle des applications et des périphériques USB	**1**	Non	Aucune solution mise en place

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
Signature de sécurité SMB désactivé	*Postes / Serveurs du Parc Informatique*	**Moyen**	**INT11**	Activer et mettre à jour la signature de sécurité SMB	**2**	Non	Aucune solution mise en place
Microsoft Windows divulgation de l'information	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT12**	Appliquer les patchs publiés par microsoft	**1**	Oui	Mais pas de solution centralisée de gestion des mises à jour
MS10-061: Microsoft Windows buffer overflow	*Postes / Serveurs du Parc Informatique*	**Elevée**	**INT13**	Appliquer les patchs publiés par microsoft	**1**	Oui	Mais pas de solution centralisée de gestion des mises à jour
Equipement de sécurité							
Multiple Vulnérabilités port SSH /FTP /HTTP .. ouvert	*172.20.0.2*	**Elevée**	**INT15**	Faire une revue des règles, désactiver les ports inutiles non sécurisés et activer TLSv1.3	**1**	Oui	

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
				avec une suite de chiffrement fiable			
Utilisation d'une solution obsolète	*172.20.0.2*	**Elevée**	**INT16**	Il faut migrer vers une version plus récente du firmware	**1**	N/A	Service migré vers firewall ASA
Serveurs							
Multiple Vulnérabilités SSL	*172.20.1.3*	**Moyen**	**INT18**	Désactiver SSLv2, SSLv3, TLSv1 et TLSv1.1 et activer TLSv1.3 avec une suite de chiffrement fiable	**1**	Oui	Action mise en place (voir les scans)
CVSS v3.0 Vulnérabilité Exécution Code à distance PHP	*172.20.1.3*	**Elevée**	**INT19**	Mettre à jour PHP vers une version récente	**1**	Oui	Action mise en place (voir les scans)

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
Détection de la version de PHP non supportée	*172.20.1.3*	**Elevée**	**INT20**	Mettre à jour PHP vers une version à jour	**1**		
JQUERY 1.2 < 3.5.0 Multiple XSS	*172.20.1.2*	**Moyen**	**INT21**	Mettre à jour la version de Jquery vers 3.5.0 ou ultérieure	**1**	Oui	Action mise en place (voir les scans)
Le serveur Web distant autorise la methode TRACK et TRACE	*172.20.1.2* *172.20.1.8*	**Moyen**	**INT22**	Désactiver ces méthodes HTTP	**1**	Non	Action non mise en place
Le serveur Web distant ne fixe pas d'en-tête de réponse X-	*41.207.188.27*	**Elevée**	**INT23**	Retournez l'en-tête HTTP X-Frame-Options ou Content-Security-Policy (avec la directive	**1**	Non	Action non mise en place

Non-conformité identifiée	Actif concerné	Gravité	ID	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)	Commentaires
Frame-Options				« frame-ancestor » avec la réponse de la page.			
Le Certificat SSL ne peut pas être approuvé	*172.20.1.2*	**Moyen**	**INT24**	Générer un Certificat SSL propre à ce service	**1**	Non	Action non mise en place
Agent SNMP avec communauté par défaut (public)	*172.20.1.2*	**Elevée**	**INT25**	Désactivez le service SNMP sur l'hôte distant s'il n'est pas utilisable	**1**	Oui	Action mise en place (voir les scans)
				Restreindre et surveiller l'accès à ce service ; changer la chaîne de communauté par défaut		Oui	Action mise en place (voir les scans)

Tableau 7: Etat des recommandations sur la sécurité du SI

4.3 Bonnes pratiques du SI

ID	Bonnes pratiques	Constat	Statut	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)
PC1	**Utilisation d'un système d'exploitation supporté pour toutes les machines utilisateur**	Les machines du parc informatique utilisent des différents OS tel que windows Xp, 7, 8,1 et 10.	**NC**	Utiliser un OS supporté (windows 8,1 ou 10) sur toutes les machines du parc informatique	**1**	En cours
PC2	**Mise en place d'un serveur Active Directory et Intégrer les postes de travail du SI au domaine**	Pas de serveur Active Directory dans le réseau et donc les postes de travail appartiennent par défaut au WORKGROUP	**NC**	Il est recommandé de mettre en place un serveur Active Directory et d'intégrer les postes de travail au domaine afin de pouvoir appliquer des stratégies de groupe définies pour chaque ordinateur / utilisateur		Non
PC3	**Installation des mises à jour Windows**	Les mises à jour sont gérées individuellement et manuellement	**NC**	Il est recommandé de mettre en place une solution de gestion des MAJs comme WSUS pour les produits Microsoft	**2**	Non

ID	Bonnes pratiques	Constat	Statut	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)
PC4	**Antivirus**	La solution antivirale "Kaspersky" est déployée pour certains postes de travail.	**NC**	Faire une acquisition d'une solution antivirale Professionnelle de préférence "Client-Serveur" permettant de mieux gérer le déploiement et la gestion des mises à jour	**1**	Non
		L'Université de Lomé ne dispose pas à date de licence de solution antivirale déployée sur l'ensemble du parc Informatique		Appliquer une politique de sécurité optimale et effectuer une revue régulière des mises à jour des postes de travail		En cours
PC5	**Restriction des droits d'installation**	Les utilisateurs ont des privilèges sur les postes de travail et peuvent installer toute application sans validation de l'équipe SI.	**NC**	Définir pour chaque groupe les applications autorisées à l'installation.	**2**	Non
				Rappeler la nécessité de n'installer que les applications autorisées et nécessaires dans le cadre professionnel		Oui, les sensibilisations sont faites

ID	Bonnes pratiques	Constat	Statut	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)
PC6	**Utilisation des supports amovibles**	Les ports USB ne sont pas verrouillés. Tous les utilisateurs ont le droit d'utiliser les ports USB (administrateurs, direction, …)	**NC**	Faire une revue régulière des utilisateurs ayant les droits d'utilisation des ports USB	**1**	Non
PC7	**Pare-feu local**	Les postes utilisateurs sont protégés par le pare-feu de la solution antivirale (Protection contre les menaces réseau).	**NC**	Activer le pare-feu de la solution antivirale ou de Windows	**2**	Oui, captures si possibles
PC8	**Connexions RDP vers les serveurs**	Tous les postes de travail ont accès aux ports de connexion à distance de tous les serveurs (SSH, RDP, …)	**NC**	Limiter les connexions possibles sur les serveurs depuis les postes utilisateur (utiliser de préférence un pare-feu interne à cet effet, et une segmentation adéquate du réseau)	**1**	Oui, segmentation effectuée avec l'ASA par contre pas de pare-feu dédié aux flux interne

ID	Bonnes pratiques	Constat	Statut	Action corrective prévue	Priorité	Action mise en place ? (Oui/Non)
PC9	**Sécurité du BIOS**	Le mot de passe du BIOS n'est pas activé	**NC**	Définir un mot de passe du BIOS pour tous les postes du parc informatique	**2**	En cours, pas tous
PC10	**Verrouillage automatique de session**	La politique de fermeture automatique des sessions n'est pas définie pour l'ensemble des postes de travail Les sessions de plusieurs postes de travail ont été trouvées non verrouillées au-delà d'une heure d'inactivité	**NC**	Définir dans la politique de groupe du contrôleur de domaine le délai de verrouillage automatique de sessions et la déployée à l'ensemble des postes de travail	**1**	Non

Tableau 8: Etat des Bonnes pratiques

4.4 Autres lacunes et recommandations

Item #	Non-conformité/ Recommandation	Action entreprise
1	Schéma directeur du SI inexistant	Pas été rédigé
2	Câble réseau de mauvaise qualité	Remplacement progressif
3	Des utilisateurs directement connectés au cœur du réseau	A été corrigé avec la segmentation du réseau
4	Serveurs de données et serveurs Internet installés dans la même zone	Aucune action menée
5	Pas de proxy (cache) pour les connectivités web (HTTP, HTTPS…)	Aucune action menée
6	Absence de protection interne vers le réseau des serveurs	Corrigé avec le cloisonnement et la segmentation du réseau
7	Présidence directement connectée à internet	Le réseau de la présidence a été rattaché au réseau de l'UL
8	Pas de QOS sur les trafics	QoS mise en place avec le PEPLINK
9	Implémentation du nouvel organigramme recommandé	En cours
10	Mise en place d'une solution WiFi unifiée qui permettra une gestion centralisée via un contrôleur	En cours, solution en cours de déploiement
11	Création de plusieurs SSID sur le contrôleur wifi (Un dédié aux visiteurs et un autre aux membres de la Direction), où les VLANs dédiés aux réseaux WIFI doivent être séparés de ceux des réseaux filaires et n'auront accès qu'au réseau Edge INTERNET	En cours, solution en cours de déploiement
12	Mise en place d'un système de communication sur IP : VoIP	Il n'y a que la présidence et la RH qui utilise le système de VOIP

Item #	Non-conformité/ Recommandation	Action entreprise
13	Assurer une formation régulière des utilisateurs et leur sensibilisation aux usages professionnels des Technologies de l'Information et de la Communication	Les IT en reçoivent mais le reste du personnel
14	Mise en place d'un Call Center	Aucune action mise en place

Tableau 9: Autres lacunes et recommandations

5. ETUDE ET ANALYSES DU DATACENTER DE L'UL

5.1 Collecte des informations sur l'existant

La collecte des informations sur l'existant s'est effectuée à travers un questionnaire structuré, couvrant les cinq catégories ci-dessous définies dans le périmètre du projet :

- données ;
- environnement/matériel ;
- logiciels/systèmes ;
- pilotage et gouvernance SI ;
- réseaux et télécommunications.

Ci-après le questionnaire et les réponses collectées avec les administrateurs réseau et systèmes

5.1.1 Données

CAT: SI	QUESTIONS	Réponse	Commentaire
DONNÉES	Les bases de données sont sauvegardées localement?	Oui	Sauvegarde locale et distante
DONNÉES	Serveur de gestion de sauvegarde en place existant ?	Non	
DONNÉES	La sauvegarde est effectuée sur un NAS / SAN dédié (si déjà existant) ?	Non	Pas de NAS
DONNÉES	La sauvegarde est effectuée sur bandes ou autes supports externes ?	Non	
DONNÉES	La sauvegarde est assurée selon un plan de sauvegarde formalisé, et validé par les métiers ?	Oui	
DONNÉES	Des tâches/Plans de sauvegarde ont été créés pour chaque Serveurs/Services/Applications ?	Non	Non, que les données qui sont sauvegardées
DONNÉES	Des notifications de la tâche sauvegarde sont envoyées automatiquement ?	Non	
DONNÉES	Est-ce qu'un Contrôle quotidien des sauvegardes est effectué et documenté ?	Non	Pas de solution de sauvegarde, juste des scripts
DONNÉES	Les bases de données SQL sont sauvegardées directement via le logiciel de backup ?	Non	Scripts
DONNÉES	Un échantillon d'informations de sauvegarde est utilisé lors des tests du plan d'urgence ?	Non	
DONNÉES	Le stockage de sauvegarde ou son replicat sont sur un emplacement distinct de la salle de production ?	Oui	
DONNÉES	Toutes les données sont-elles sauvegardées et externalisées ?	Oui	
DONNÉES	Les sauvegardes externalisées sont stockées dans un coffre ignifugé ?	Non	
DONNÉES	Est-que les sauvagardes sont chiffrées ?	Non	
DONNÉES	Présence d'une externalisation backup sur un 2nd site géographique (réplication) ?	Non	
DONNÉES	Un planning de test des sauvegardes existe ?	Non	
DONNÉES	Le dernier test de sauvegarde a été réalisé conformément au plan ?	Non	
DONNÉES	Les tests de restauration réalisés sont documentés et archivés ?	Non	
DONNÉES	Un serveur physique dédié au test des restauration est disponible sur le site ?	Non	
DONNÉES	Une solution d'archivage légal sur bande est disponible ?	Non	
DONNÉES	Le type de données a sauvegarder sur site principale /site secondaire sont documentés ?	Non	
DONNÉES	Les informations de sauvegarde sont testées pour vérifier la fiabilité des supports et l'intégrité des informations ?	Oui	
DONNÉES	Des copies de sauvegarde sont stockées dans une installation séparée ou dans un conteneur résistant au feu qui n'est pas colocalisé avec le système opérationnel ?	Non	
DONNÉES	La fonction de compression des données est mise en configuration lorsque vous effectuez des sauvegardes ?	Non	
DONNÉES	Des mesures techniques adéquates sont prises afin de détruire efficacement les données qui ne sont plus en production ou qui ont été réaffectés ?	Non	
DONNÉES	Les mots de passe des comptes à privilège sont stockés de manière sécurisée, sous forme de hash ?	Oui	
DONNÉES	Des contrats de confidentialités ont été signés avec les prestataires qui interviennent sur les systèmes ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
DONNÉES	L'attribution des informations secrètes d'authentification est réalisée dans le cadre d'un processus de gestion formel ?	Non	
DONNÉES	Un système qui gère les mots de passe est mis en œuvre ?	Non	
DONNÉES	Les mots de passe sont stockés de manière sécurisée, sous forme de hash ?	Oui	
DONNÉES	Tout mouvement d'un collaborateur doit faire l'objet d'une revue de ses droits ? (Suppression systématique en cas de départ des effectifs)	Non	Problèmes de gouvernance SI
DONNÉES	Est-ce qu'un processus de continuité de l'activité a été élaboré ?	Non	
DONNÉES	Est-ce les plans de continuité de l'activité sont soumis à l'essai et mis à jour régulièrement afin de s'assurer qu'ils sont actualisés et efficaces ?	Non	
DONNÉES	En fonction des enjeux, une cartographie des risques est basée sur la criticité des données (confidentialité, intégrité, disponibilité, traçabilité) ?	Non	
DONNÉES	Les informations relatives à l'ensemble des incidents de sécurité SI sont conservées pendant un minimum de trois ans ?	Non	

Tableau 10: Questionnaire sur la catégorie des données

5.1.2 Environnement/matériel

CAT: SI	QUESTIONS	Réponse	Commentaire
ENVIRONNEMENT/MATÉRIEL	RAID 6 est configuré pour les disques du NAS/SAN de sauvegardes ?	Non	
ENVIRONNEMENT/MATÉRIEL	Présence de disques de spare en stock pour le NAS/SAN en plus du disque hotspare ?	Non	
ENVIRONNEMENT/MATÉRIEL	Présence des supports de sauvegarde externes en spare ?	Non	
ENVIRONNEMENT/MATÉRIEL	La salle serveur est-elle dédiée aux serveurs, onduleur et le matériel de communication nécessaire (IT) et rien d'autre ?	Oui	
ENVIRONNEMENT/MATÉRIEL	Est-ce que Les racks abritant les serveurs sont tous fermés à clé ?	Non	
ENVIRONNEMENT/MATÉRIEL	Les baies serveurs doivent être équipées de 2 PDU branchés sur 2 sources d'énergie différentes ?	Non	
ENVIRONNEMENT/MATÉRIEL	Les racks et la salle des serveurs sont-ils aspirés d'une manière périodique (3 mois minimum) ?	Non	
ENVIRONNEMENT/MATÉRIEL	Les centres serveurs fonctionnent-ils avec un plancher surélevé pour accommoder les câbles et autres équipements informatiques ?	Non	
ENVIRONNEMENT/MATÉRIEL	Si vos centres serveurs fonctionnent avec des planchers surélevés, le plancher surélevé est-il nettoyé à fond une fois tous les trois mois ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
ENVIRONNEMENT/MATÉRIEL	Les autorisations d'accès individuelles sont-elles vérifiées avant d'accorder l'accès ?	Oui	
ENVIRONNEMENT/MATÉRIEL	Des systèmes ou dispositifs de contrôle d'accès physique définis par l'organisation sont mises en place ?	Non	
ENVIRONNEMENT/MATÉRIEL	Existent -t-ils des journaux d'audit des accès physiques aux salles des serveurs ?	Non	
ENVIRONNEMENT/MATÉRIEL	Les visiteurs sont escortés et l'activité des visiteurs est contrôlée et documentée ?	Non	
ENVIRONNEMENT/MATÉRIEL	L'accès physique à l'installation où résident les serveurs est surveillé à l'aide d'alarmes d'intrusion physique et d'équipements de surveillance ?	Non	
ENVIRONNEMENT/MATÉRIEL	Est-ce que Les armoires abritant les équipements d'interconnexion sont toutes fermées à clé	Non	
ENVIRONNEMENT/MATÉRIEL	Un protocole d'étiquetage de câble est mis en œuvre ?	Oui	
ENVIRONNEMENT/MATÉRIEL	Existe-t-il une surveillance à distance ainsi qu'un asservissement d'arrêt en fonction des conditions environnementales de la salle serveurs' ?	Non	
ENVIRONNEMENT/MATÉRIEL	Des systèmes de détection et d'extinction d'incendie sont mises en place ?	Non	Présence d'un extinctinteur mécanique
ENVIRONNEMENT/MATÉRIEL	Les systèmes de détection et d'extinction sont soutenus par une source d'énergie indépendante ?	Non	
ENVIRONNEMENT/MATÉRIEL	Les systèmes de détection d'incendie s'activent automatiquement et avertissent ?	Non	
ENVIRONNEMENT/MATÉRIEL	L'installation subit a des inspections de protection contre les incendies par des inspecteurs autorisés et qualifiés et que les lacunes identifiées sont résolues ?	Non	
ENVIRONNEMENT/MATÉRIEL	Utiliser une surveillance de contrôle environnemental qui fournit une alarme ou une notification des changements potentiellement de température dangereux pour le personnel ou l'équipement ?	Non	
ENVIRONNEMENT/MATÉRIEL	Les moyens de détection des fuites d'eau/liquide sont mises en place ?	Non	
ENVIRONNEMENT/MATÉRIEL	La salle possède un système de climatisation avec une régulation très précise ?	Oui	

CAT: SI	QUESTIONS	Réponse	Commentaire
ENVIRONNEMENT/MATÉRIEL	La température de la salle est paramétrée sur 20-26 °C ?	Oui	
ENVIRONNEMENT/MATÉRIEL	Les vannes d'arrêt principales ou les vannes d'isolement sont accessibles ?	Non	
ENVIRONNEMENT/MATÉRIEL	La salle informatique dispose d'un générateur de secours d'une puissance suffisante au minimum pour prendre l'ensemble de la salle informatique et ses climatiseurs ?	Oui	
ENVIRONNEMENT/MATÉRIEL	Les vannes d'arrêt principales et les vannes d'isolement fonctionnent correctement et connues du personnel clé ?	Non	
ENVIRONNEMENT/MATÉRIEL	L'humidité est contrôlée de sorte à rester entre 50 à 60% HR ?	Non	Aucun capteur environnemental installé
ENVIRONNEMENT/MATÉRIEL	Des formations initiales sont fournies aux employées et personnels définis par l'organisation sur l'emploi et le fonctionnement des contrôles environnementaux (moyens de détections/ simulation de cas de désastre) ?	Oui	Uniquement pour l'IT
ENVIRONNEMENT/MATÉRIEL	Ce contrôle d'accès dispose d'un historique consultable ?	Non	Pas de control d'accès
ENVIRONNEMENT/MATÉRIEL	l'accès aux locaux est distinctif et nominatif (on sait qui est rentré quand, etc. …) ?	Non	
ENVIRONNEMENT/MATÉRIEL	Est-ce que la salle serveurs est aveugle ? (aucune fenêtre sur l'extérieur)	Non	
ENVIRONNEMENT/MATÉRIEL	Les salles informatiques disposent d'un contrôle d'accès ?	Non	Pas de control d'accès
ENVIRONNEMENT/MATÉRIEL	La résilience RAID est configuré ?	Non	Exclusion ==> Pas de NAS/SAN
ENVIRONNEMENT/MATÉRIEL	L'ensemble des disques du stockage en place sont fonctionnels (pas d'alarmes)?	Non	Exclusion ==> Pas de NAS/SAN
ENVIRONNEMENT/MATÉRIEL	Les stockages ont leur accès LAN (SAN / NAS) connecté à 10 Gb ?	Non	Exclusion ==> Pas de NAS/SAN
ENVIRONNEMENT/MATÉRIEL	Les stockages ont leur accès LAN (SAN / NAS) redondé (Teaming) ?	Non	Exclusion ==> Pas de NAS/SAN
ENVIRONNEMENT/MATÉRIEL	L'espace de stockage libre est au moins 30%	Non	Exclusion ==> Pas de NAS/SAN
ENVIRONNEMENT/MATÉRIEL	Le stockage production (SAN) est optimisé avec l'usage d'espace disque rapides (ssd) et lent (hd) ?	Non	Exclusion ==> Pas de NAS/SAN

CAT: SI	QUESTIONS	Réponse	Commentaire
ENVIRONNEMENT/MATÉRIEL	Le site dispose de disques de spare ?	Non	Exclusion ==> Pas de NAS/SAN
ENVIRONNEMENT/MATÉRIEL	Les onduleurs des baies sont de type double conversion ?	Pending	Information manquante
ENVIRONNEMENT/MATÉRIEL	le site dispose d'un onduleur central ? (Qui alimente user et salle informatique ?	Oui	Un seul onduleur central
ENVIRONNEMENT/MATÉRIEL	L'ensemble des onduleurs sont administrés (ils ont une IP configurée / accessible) ?	Non	
ENVIRONNEMENT/MATÉRIEL	L'ensemble des onduleurs est supervisé en SNMP ?	Non	
ENVIRONNEMENT/MATÉRIEL	L'onduleur central dispose d'une protection amont par disjoncteur Différentiel ?	Non	
ENVIRONNEMENT/MATÉRIEL	L'onduleur central dispose d'une protection de la distribution par disjoncteur divisionnaire / Différentiel ?	Oui	Disjoncteur de tête de 40A
ENVIRONNEMENT/MATÉRIEL	L'organisation possède un plan de topologie pour les types d'onduleurs ? (simple conversion , double conversion , multimodes) ?	Non	
ENVIRONNEMENT/MATÉRIEL	Vous établissez une liste de tous les équipements qui sont protégés par votre onduleur ?	Non	
ENVIRONNEMENT/MATÉRIEL	L'alimentation du site dispose d'un groupe électrogène ou plus pour le secoure du SI entre autres ?	Oui	Présence d'un groupe électrogène
ENVIRONNEMENT/MATÉRIEL	Vous déployez un groupe électrogène affichant une puissance nominale en kVA 1,25 à 3 fois supérieure à celle de votre onduleur ?	Pending	Information manquante
ENVIRONNEMENT/MATÉRIEL	Le groupe électrogène s'appuie sur une réserve de gasoil pour assurer la continuité de fonctionnement des systèmes informatiques pendant un laps de temps compris entre 10 minutes et 7 jours ou plus ?	Oui	
ENVIRONNEMENT/MATÉRIEL	Des onduleurs à montage en rack sont mises en place pour centraliser le plus de matériel possible dans les baies ?	Non	Les PDU sont directement raccordés au coffret eletrique ondulé, pas d'onduleur dans les baies
ENVIRONNEMENT/MATÉRIEL	Un ou plusieurs onduleurs assurent la protection dédiée d'une partie du data center, ainsi, si un onduleur tombe en panne lors d'une coupure de courant, les conséquences sont limitées à la zone protégée par cet appareil (architecture redondante)?	Non	Un seul onduleur central par salle serveur

CAT: SI	QUESTIONS	Réponse	Commentaire
ENVIRONNEMENT/MATÉRIEL	Plusieurs onduleurs sont raccordées en serie ?	Non	
ENVIRONNEMENT/MATÉRIEL	Plusieurs onduleurs indépendants raccordées en parallèle pour améliorer la redondance ?	Non	
ENVIRONNEMENT/MATÉRIEL	Les onduleurs envoient des notifications en temps réel lorsqu'apparaissent des problèmes potentiels ?	Non	
ENVIRONNEMENT/MATÉRIEL	Une arrivée électrique indépendante du bâtiment est installé ? pour les UPS central	Oui	
ENVIRONNEMENT/MATÉRIEL	L'armoire électrique est indépendante, clairement étiquetée et documentée ? pour les UPS central	Oui	
ENVIRONNEMENT/MATÉRIEL	Puissance de 10 Kva et plus pour les UPS central ?	Oui	Onduleur central de 10KVa
ENVIRONNEMENT/MATÉRIEL	Pour les UPS rack d'armoire une taille minimum de 5 KVA et une marge de Puissance de 35% du nominal cible ?	Non	
ENVIRONNEMENT/MATÉRIEL	Carte de Gestion SNMP et asservicement des serveurs sont mises en place pour l'arrêt automatique serveur ?	Non	
ENVIRONNEMENT/MATÉRIEL	Présence de sonde de température externe ?	Non	
ENVIRONNEMENT/MATÉRIEL	Des prises électriques dans la salle alimentée par le circuit du bâtiment (secours) sont installés ?	Oui	Prises électriques alimentées par le GE et l'onduleur
ENVIRONNEMENT/MATÉRIEL	Vous effectuez des entretiens pour les onduleurs et vous générer des rapport périodiquement ?	Non	
ENVIRONNEMENT/MATÉRIEL	Les baies serveur disposent de leurs propres onduleurs (eux-mêmes alimentés par l'onduleur central)?	Non	
ENVIRONNEMENT/MATÉRIEL	La procédure de shutdown par l'onduleur à été mise en place sur les serveurs et elle fonctionne ?	Non	
ENVIRONNEMENT/MATÉRIEL	Le courant généré par le réseau électrique est triphasé ?	Oui	
ENVIRONNEMENT/MATÉRIEL	Sur les centres informatiques Multi Zones, une double arrivée électrique et un onduleur redondant sont mises en place ? Pour les ups central	Non	
ENVIRONNEMENT/MATÉRIEL	Une protection parafoudre est en place (bi-étage avec plus de 5 m entre les deux étages et dernier étage écrêter à plus de 5 m de l'équipement (M Distance câblé) ?	Pending	Information manquante

CAT: SI	QUESTIONS	Réponse	Commentaire
ENVIRONNEMENT/MATÉRIEL	Une protection paratonnerre est en place ?	Oui	
ENVIRONNEMENT/MATÉRIEL	La terre est raccordée sur les baies / les PDU et d'une manière générale sur tous les châssis ?	Non	
ENVIRONNEMENT/MATÉRIEL	La terre est équipotentielle ? (Une boucle de terre existe …?)	Pending	Information manquante
ENVIRONNEMENT/MATÉRIEL	L'Énergie du bâtiment est protégée en amont par des parafoudres à cartouche ?	Pending	Information manquante
ENVIRONNEMENT/MATÉRIEL	Les composants constitutifs des systèmes sont explicitement définis et documentés ?	Pending	Information manquante
ENVIRONNEMENT/MATÉRIEL	Les personnes qui remplissent les rôles et responsabilités du système sont identifiés ?	Pending	Information manquante
ENVIRONNEMENT/MATÉRIEL	Procédure d'installation d'un nouveau poste avec OS est mise en place ?	Non	Sujet assez complexe dans la mesure ou chaque département de l'organisation est autonome en terme de PC utilisateurs
ENVIRONNEMENT/MATÉRIEL	Noms de machines conformes aux normes de votre organisation?	Non	Gestion des postes utilisateurs non centraliser. Pas vraiment d'inventaire disponible l'UL
ENVIRONNEMENT/MATÉRIEL	L'accès à la configuration système BIOS/UEFI n'est pas possible pour l'utilisateur ?	Non	
ENVIRONNEMENT/MATÉRIEL	Une étiquette apposée sur le poste de travail doit préciser l'identifiant unique du poste de travail ?	Non	
ENVIRONNEMENT/MATÉRIEL	Le démarrage du poste ne doit être possible que depuis le disque dur interne ?	Non	
ENVIRONNEMENT/MATÉRIEL	Tous les serveurs disposent d'une IP fixe ? (@IP fixe + gateway + DNS)	Oui	
ENVIRONNEMENT/MATÉRIEL	Le site dispose de ressources serveurs de secours/spare ? RAM, Disque, bloc d'alimentation	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
ENVIRONNEMENT/MATÉRIEL	Le RAID est-il configuré sur vos serveur	Oui	
ENVIRONNEMENT/MATÉRIEL	Les serveurs sont tous de la même marque ?	Non	IBM/ HPE/ DELL
ENVIRONNEMENT/MATÉRIEL	Carte ilo/idrac/ou autres en place / administrée avec une IP ?	Non	
ENVIRONNEMENT/MATÉRIEL	Serveur proprement fixé (Rail / guide câble) ?	Non	Pas de guide câble, câblage en spaghetti
ENVIRONNEMENT/MATÉRIEL	L'état général des serveurs (propreté & intégrité) est Ok ?	Oui	Salle serveur propre, pas de poussière
ENVIRONNEMENT/MATÉRIEL	les serveurs ont tous moins de 8 ans ?	Non	Présence de serveur vieux de plus de 8 ans HP ProLiant DL380 G7
ENVIRONNEMENT/MATÉRIEL	Est-ce que les biens importants ont été clairement identifiés et inventoriés ?	Oui	
ENVIRONNEMENT/MATÉRIEL	Est-ce qu'une autorisation préalable est nécessaire pour sortir un matériel des locaux de votre organisation?	Non	Plus en Vigueur
ENVIRONNEMENT/MATÉRIEL	Tout le matériel est étiqueté de façon visible ?	Non	Présence de serveur sans étiquettes dans les deux salles
ENVIRONNEMENT/MATÉRIEL	Aucune possibilité pour démarrer le poste de l'utilisateur depuis un support amovible ?	Non	
ENVIRONNEMENT/MATÉRIEL	Est-ce les supports qui ne servent plus ont été mis au rebut de façon sûre en suivant des procédures formelles ?	Non	
ENVIRONNEMENT/MATÉRIEL	Des détecteurs de fluides ont été installés ?	Non	

Tableau 11: Questionnaire sur la catégorie Environnement et Matériel

5.1.3 Logiciels/systèmes

CAT: SI	QUESTIONS	Réponse	Commentaire
LOGICIELS/SYSTÈMES	Avez-vous une sauvegarde régulière de la configuration DHCP ?	Oui	
LOGICIELS/SYSTÈMES	Avez-vous une stratégie de durée de bail DHCP ?	Oui	Une durée de 1 semaines est défini pour tous les pools
LOGICIELS/SYSTÈMES	Pas de vieilles réservations DHCP ?	Oui	
LOGICIELS/SYSTÈMES	Les options de scope du serveur DHCP sont-elles définies (routeur 003, serveurs DNS 006, nom de domaine DNS 015) ?	Oui	Exclusion du nom de domaine ==> Pas de d'annuaire
LOGICIELS/SYSTÈMES	Réplication DHCP en place (au moins 2 serveurs) ?	Non	Présence de deux serveurs, mais pas de réplications
LOGICIELS/SYSTÈMES	DHCP snooping est déployé sur le réseau (tous les switchs) ?	Pending	Information manquante
LOGICIELS/SYSTÈMES	Est-ce que toutes les plages sont répliquées ?	Non	Pas réplication DNS
LOGICIELS/SYSTÈMES	Les plages d'adresses DHCP déclarées sont conformes aux normes ?	Oui	
LOGICIELS/SYSTÈMES	Utilisation du serveur DNS pour les services locaux ?	Oui	
LOGICIELS/SYSTÈMES	Réplication serveur DNS en place (au moins 2) ?	Oui	Exclusions ==> 2 serveurs le second en standby
LOGICIELS/SYSTÈMES	Est-ce que le nettoyage automatique est activé ?	Non	Nettoyage manuelle
LOGICIELS/SYSTÈMES	La journalisation DNS (DNS LOGGING) est-elle activée ?	Oui	
LOGICIELS/SYSTÈMES	Les identifiants désactivés depuis plus de 3 mois sont supprimé (sauf si une contrainte technique empêche la traçabilité) ?	Non	
LOGICIELS/SYSTÈMES	Les mots de passe de comptes à privilège suivent une politique de gestion renforcée ?	Oui	
LOGICIELS/SYSTÈMES	Tout compte est bloqué après 5 tentatives infructueuses de connexion ?	Non	Ici c'est chaque 6 Mois
LOGICIELS/SYSTÈMES	Tout mot de passe est renouvelé à minima tous les 90 jours ?	Oui	
LOGICIELS/SYSTÈMES	Lors d'un renouvellement, le nouveau mot de passe ne contient pas des caractères de l'ancien mot de passe ?	Oui	
LOGICIELS/SYSTÈMES	Est-ce que vous avez une solution de gestion des tickets ?	Non	Pas de helpdesk disponible
LOGICIELS/SYSTÈMES	L'alimentation des serveurs est redondante ?	Non	
LOGICIELS/SYSTÈMES	Si alimentation redondante : sont-elles connectées sur différentes sources d'énergie ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
LOGICIELS/SYSTÈMES	Solution inventaire matériel/logiciel/OS en place (OCS, Fusion Inventory, ...)?	Non	
LOGICIELS/SYSTÈMES	Différents sous-réseaux pour séparer les réseaux d'administration, de données et de réplication de VM sont mis en place ?	Non	
LOGICIELS/SYSTÈMES	Chaque rôle est seul sur sa machine, pas de machine hébergent plusieurs rôle ?	Non	Cela dépend de la criticité du service

Tableau 12: Questionnaire sur la catégorie Logiciels et Systèmes

5.1.4 Pilotage et gouvernance SI

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Les récurrences paramétrées dans les plans?	Oui	Via des scripts
PILOTAGE ET GOUVERNANCE SI	Les paramètres de rétention sont conformes aux objectifs définis ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Existe t-il un plan d'urgence et est ce qu'il est testé régulièrement ?	Non	
PILOTAGE ET GOUVERNANCE SI	La charte administrateur est signé et accordé par les administrateurs ?	Non	
PILOTAGE ET GOUVERNANCE SI	Le document est portée à la connaissance de chaque utilisateur des systèmes d'information par tout moyen de communication adéquat ?	Non	
PILOTAGE ET GOUVERNANCE SI	Présence d'un document (charte) déterminant les règles de sécurité et d'usage des systèmes d'information de l'utilisateur ?	Non	
PILOTAGE ET GOUVERNANCE SI	Intègrez-vous cette charte dans leur règlement intérieur ou équivalent suivant les règles du pays ?	Non	
PILOTAGE ET GOUVERNANCE SI	La charte est appliqué aux personnels des sociétés extérieures (prestataire ou partenaires commerciaux) ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Un document de dérogation à la politique de Sécurité du SI est utilisé ?	Non	Pas de politique de sécurité
PILOTAGE ET GOUVERNANCE SI	Le document de dérogation est transmis à la DRSI ?	Non	Pas de politique de sécurité
PILOTAGE ET GOUVERNANCE SI	Audit journalier des journaux d'évènements ?	Non	
PILOTAGE ET GOUVERNANCE SI	Est-ce qu'examen périodique des règles de pare-feu est effectué et documenté ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Analysez-vous les règles et les configurations de pare-feu par rapport aux normes réglementaires, telles que ISO 27001, ISO 27002, ainsi qu'aux politiques d'entreprise qui définissent les configurations matérielles et logicielles de base auxquelles les appareils doivent adhérer ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Vous avez établit un processus pour auditer en permanence les pares-feux?	Oui	
PILOTAGE ET GOUVERNANCE SI	Documentez-vous correctement vos procédures d'audit et fournissez-vous une piste d'audit complète de toutes les activités de gestion du pare-feu ?	Non	Non documentées ==> pas de preuves
PILOTAGE ET GOUVERNANCE SI	Avez-vous mis en place un workflow de changement de pare-feu robuste pour maintenir la conformité au fil du temps ?	Non	Non documentées ==> pas de preuves
PILOTAGE ET GOUVERNANCE SI	Examinez-vous régulièrement les rapports antivirus et les messages des logs ?	Non	
PILOTAGE ET GOUVERNANCE SI	Procédures de gestion de comptes utilisateurs (Annuaires, VPN, métiers …) existante ?	Non	
PILOTAGE ET GOUVERNANCE SI	Procédures d'arrivée et de départ des utilisateurs existante ?	Non	
PILOTAGE ET GOUVERNANCE SI	Procédures de revues des habilitations existante ?	Non	Pas de départements Qualité

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Procédures de gestion des accès temporaires existante ?	Non	
PILOTAGE ET GOUVERNANCE SI	Toutes les actions liées au cycle de vie d'une identité sont tracées ? (création, suppression, modification d'une identité, attribution ou retrait d'habilitation)	Non	
PILOTAGE ET GOUVERNANCE SI	La création de comptes à privilèges (admin) est liée à une demande validée par le responsable du bénéficiaire et par le propriétaire du service SI concerné ?	Non	Pas gestion centralisée
PILOTAGE ET GOUVERNANCE SI	Le format du compte à privilège a été défini de manière à le différencier des comptes standards en prenant la précaution que le standard défini ne permette pas à une personne externe de déduire qu'il s'agit d'un compte à privilège?	Non	Pas gestion centralisée
PILOTAGE ET GOUVERNANCE SI	En cas de système biométrique, déclaration effectuée auprès de l'organisme gouvernemental en charge ?	Non	
PILOTAGE ET GOUVERNANCE SI	Les mots de passe administrateurs ont été communiqués à la Direction ?	Non	
PILOTAGE ET GOUVERNANCE SI	Les utilisateurs ont uniquement accès au réseau et aux services réseau pour lesquels ils ont spécifiquement reçu une autorisation ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Une politique de contrôle d'accès est établie, documentée et revue sur la base des exigences métier et de sécurité de l'information ?	Non	
PILOTAGE ET GOUVERNANCE SI	L'allocation et l'utilisation des droits d'accès à privilèges sont restreintes et contrôlées ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Les droits d'accès aux informations et aux moyens de traitement des informations de l'ensemble des salariés et utilisateurs tiers sont supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord ?	Non	Accès non centralisé
PILOTAGE ET GOUVERNANCE SI	Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications est contrôlé par une procédure de connexion sécurisée ?	Non	
PILOTAGE ET GOUVERNANCE SI	Un processus formel de distribution des accès aux utilisateurs est mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisateurs sur l'ensemble des services et des systèmes ?	Non	Accès non centralisé

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Identifiez-vous les privilèges d'accès associés à chaque système ?	Non	
PILOTAGE ET GOUVERNANCE SI	Procédez-vous à une revue régulière des accès à privilèges afin de vérifier qu'elles sont conformes ?	Non	Tous les accès sont gérés par une même personne
PILOTAGE ET GOUVERNANCE SI	Vous disposez d' une liste explicite des salariés du fournisseur autorisés à recevoir ou à accéder à l'information de l'organisation, soit des procédures ou conditions liées à l'octroi et au retrait d'autorisations pour l'accès à l'information de l'organisation ou la réception d'information de l'organisation à destination des salariés du fournisseur ?	Oui	
PILOTAGE ET GOUVERNANCE SI	La porte d'accès à la salle informatique est de type Blindée /Coupe-feu ?	Non	Porte en alu
PILOTAGE ET GOUVERNANCE SI	Toute création de compte utilisateur est liée à une demande d'habilitation formelle par le responsable hiérarchique ou un prestataire ?	Non	Pas d'annuaire
PILOTAGE ET GOUVERNANCE SI	Les comptes utilisateurs sont rattachés à une identité de votre organisation?	Oui	Comptes locaux
PILOTAGE ET GOUVERNANCE SI	Les comptes désactivés depuis plus de trois mois sont supprimés, sauf si une contrainte technique empêche la traçabilité relative à ce compte ?	Non	
PILOTAGE ET GOUVERNANCE SI	Les opérations relatives à la désactivation ou à la suppression d'un compte garde une traçabilité ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Toute attribution d'un accès suit une procédure documentée ?	Non	
PILOTAGE ET GOUVERNANCE SI	Les comptes à privilèges sont utilisés uniquement pour la réalisation de tâches qui les nécessitent ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Les comptes d'accès à privilèges ne sont pas partagés entre plusieurs utilisateurs ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Les accès à privilège sont différents des accès au sein du SI de votre organisation ?	Oui	Pas d'annuaire

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Les accès aux environnements ne sont réalisés qu'à partir de postes de travail de votre organisation ?	Pending	Exclusion ==> Adoption du BYOD, mais pour les taches d'administration une machine est fournie
PILOTAGE ET GOUVERNANCE SI	Les identifiants d'un compte à privilèges sont constitués de façon à respecter les règles de construction ?	Non	Accès non centralisé
PILOTAGE ET GOUVERNANCE SI	Les accès à privilèges respectent une politique de mot de passe renforcée ?	Non	
PILOTAGE ET GOUVERNANCE SI	Est-ce que vous avez une Procédure de gestion Helpdesk ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Le Service HELPDESK fournit-il un point de contact unique pour toutes les questions des utilisateurs ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Des revues de direction hebdomadaires sont-elles organisées pour mettre en évidence la disponibilité des services, la satisfaction des utilisateurs et les zones d'incidents majeurs ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Existe-t-il un contrat de maintenance et d'assistance ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Fournissez-vous à la direction des informations concernant les performances opérationnelles du Service HELPDESK ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Fournissez-vous à la direction des informations concernant les besoins de sensibilisation/formation des utilisateurs ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Organisez-vous des réunions régulières avec les parties intéressées au cours desquelles les questions relatives au Service HELPDESK sont discutées ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Est-ce que vous documentez les interventions et changements ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Organisez-vous des réunions régulières avec le Service Desk pour discuter des incidents signalés, progressés, escaladés et clôturés ?	Non	Pas de helpdesk disponible

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Fournissez-vous à la direction des informations concernant la satisfaction des clients à l'égard des services ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Y a t-il une procédure de gestion des changements mise en place?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Gestion des tickets exploités ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Pas de tickets datant de +30 jours ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	A la clôture d'un ticket le demandeur reçoit un email ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Règles attribution automatique catégorie ticket en place ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Règles attribution automatique groupe de support pour ticket en place ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Une base de connaissance existe et alimentée régulièrement ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Un programme de sensibilisation et/ou de formation a-t-il été organisé pour les utilisateurs sur l'utilisation du Service HELPDESK et ses avantages ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	Le Service HELPDESK fournit-il une mise à jour de l'état au utilisateur sur la clôture des incidents ?	Non	Pas de helpdesk disponible
PILOTAGE ET GOUVERNANCE SI	L'accès au SI de l'organisation en nomadisme est restreint à certaines ressources identifiées et autorisées à l'avance à être accédées à distance ?	Pending	Exclusion ==> Pas de VPN Site à Clients
PILOTAGE ET GOUVERNANCE SI	Tout accès au système d'information en nomadisme doit se faire à l'aide d'une authentification à plusieurs facteurs et à travers une connexion chiffrée ?	Pending	Exclusion ==> Pas de VPN Site à Clients

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	En cas d'incident de sécurité les utilisateurs préviens leurs hiérarchie, ainsi que le responsable de la sécurité, au téléphone ou de vive voix (l'intrus peut-être capable de lire les courriels) ?	Oui	La DRSI est solliciter pour les incidents par téléphone par les responsables des différents services et départements
PILOTAGE ET GOUVERNANCE SI	Est-ce que le Planning entretien des serveurs est documenté ?	Non	En cours de rédaction
PILOTAGE ET GOUVERNANCE SI	Est-ce que l'entretien des serveurs est effectué est documenté ?	Non	Fait mais pas de PV pour lever le point
PILOTAGE ET GOUVERNANCE SI	Nommage serveurs conforme aux normes de votre organisation ?	Oui	Présence d'une politique
PILOTAGE ET GOUVERNANCE SI	Nommage des cartes réseau conforme aux normes de votre organisation ?	Non	Exclusion ==> Serveurs Linux
PILOTAGE ET GOUVERNANCE SI	Une identification est présente sur le serveur (nom du serveur) ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Existe-t-il un gestionnaire d'incidents responsable de la gestion et de l'escalade des incidents ?	Non	
PILOTAGE ET GOUVERNANCE SI	Existe-t-il au moins certaines activités de gestion des problèmes établies dans l'organisation, par ex. détermination du problème, analyse du problème, résolution du problème ?	Non	Cette prestation à fait l'objet d'une étude
PILOTAGE ET GOUVERNANCE SI	Le plan de crise est formalisé et maintenu en condition opérationnelle. Il doit être associé au plan de continuité d'activité et au plan de reprise d'activité (PCA/PRA)?	Non	
PILOTAGE ET GOUVERNANCE SI	Un bilan de gestion des incidents majeurs est réalisé, partagé, communiqué ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Une communication de crise liée au SI s'appuie sur une procédure associée. La communication de crise doit prendre en compte l'importance et la célérité des attaques cyber?	Oui	
PILOTAGE ET GOUVERNANCE SI	solution de supervision en place ?	Oui	

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Tous les incidents sont-ils gérés conformément aux procédures documentées dans les SLA ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Des rapports sont-ils régulièrement produits pour toutes les équipes contribuant au processus de résolution des incidents, concernant l'état des incidents ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Les problèmes potentiels sont-ils formellement évalués et identifiés avant que la perturbation ne se produise ?	Oui	
PILOTAGE ET GOUVERNANCE SI	L'organisation dispose-t-elle de procédures pour l'enregistrement des problèmes et leur résolution ?	Non	
PILOTAGE ET GOUVERNANCE SI	Des rapports standard concernant les problèmes sont-ils produits régulièrement ?	Non	
PILOTAGE ET GOUVERNANCE SI	Le site dispose-t-il d'écrans de supervision ?	Oui	Mais non fonctionnel
PILOTAGE ET GOUVERNANCE SI	Un dispositif de surveillance de la température et de l'hygrométrie est en place dans les salles informatiques	Non	
PILOTAGE ET GOUVERNANCE SI	Cette supervision émet des rapports de disponibilité sur l'ensemble des objets ?	Non	Les rapports de disponibilité à mettre en place
PILOTAGE ET GOUVERNANCE SI	Carte de synthèse pour les accès internet/interco est disponible et complète ?	Non	Le réseau Wi-Fi de l'UL est gérer par YAS (ex Togocom)
PILOTAGE ET GOUVERNANCE SI	Carte de synthèse pour les équipements réseaux est disponible et complète ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Carte de synthèse conditions environnementales est disponible et complète ?	Non	
PILOTAGE ET GOUVERNANCE SI	Solution de gestion du stock en place ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	les objectifs et le contexte de la supervision sont bien définis ?	Oui	La DRSI maitrise les objectifs et le contexte de sa supervision, mais amélioration toujours possible
PILOTAGE ET GOUVERNANCE SI	L'escalade de notifications est activé ?	Non	
PILOTAGE ET GOUVERNANCE SI	Les notifications par E-mail/SMS en cas de pannes détectées par la solution de supervision est activées ?	Oui	La notification effective pour les équipements couvert par le périmètre de la supervision
PILOTAGE ET GOUVERNANCE SI	Toute alarme qui sort vous donne quelque chose d'exploitable ?	Oui	Oui, les alarmes et les notifications exploitable
PILOTAGE ET GOUVERNANCE SI	Est-ce que vous avez mis en place une politique et une organisation de gestion des risques, couvrant l'ensemble des processus critiques de l'entreprise, intégrée au sein des métiers et de la fonction informatique?	Non	
PILOTAGE ET GOUVERNANCE SI	Le périmètre d'analyse des risques SI s'appuie sur le périmètre des processus métiers définis comme critiques pour l'organisation ?	Non	
PILOTAGE ET GOUVERNANCE SI	Est-ce qu'une politique, des procédures et des programmes opérationnels spécifiques au télétravail a été élaborée et mise en œuvre ?	Pending	Exclusion ==> Pas de télétravail
PILOTAGE ET GOUVERNANCE SI	Est-ce que des procédures ont été mises en place pour contrôler l'installation du logiciel sur les systèmes en exploitation ?	Non	
PILOTAGE ET GOUVERNANCE SI	Existe-t-il une procédure pour soulever et émettre des demandes de changement ?	Non	
PILOTAGE ET GOUVERNANCE SI	L'organisation a-t-elle des normes ou d'autres critères de qualité pour la levée et l'enregistrement des changements ?	Non	
PILOTAGE ET GOUVERNANCE SI	Des enregistrements formels des changements sont-ils conservés ?	Oui	

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Des indicateurs ont été définis et mis en place pour mesurer la valeur apportée aux métiers lors d'une externalisation de services ?	Non	
PILOTAGE ET GOUVERNANCE SI	Carte de synthèse pour les serveurs est disponible et complète ?	Non	Disponible mais pas complète
PILOTAGE ET GOUVERNANCE SI	Les évènements survenus sont historisés/documentés ?	Oui	
PILOTAGE ET GOUVERNANCE SI	Est-ce que la documentation SI a été protégée contre les accès non autorisés ?	Oui	
PILOTAGE ET GOUVERNANCE SI	SNMPv3 ou SNMPv2 sont déployés au lieu de SNMPv1 ?	Non	Présence de snmp v1
PILOTAGE ET GOUVERNANCE SI	Des enregistrements d'incidents sont-ils conservés pour tous les incidents signalés ?	Non	
PILOTAGE ET GOUVERNANCE SI	Le taux de disponibilité des services est-il d'au moins 99%?	Oui	
PILOTAGE ET GOUVERNANCE SI	Votre QoS est-il surveillé ?	Non	Visio pas encore en place
PILOTAGE ET GOUVERNANCE SI	Les espaces disque des serveurs sont suffisants (> 30 % d'espace disque disponibles min) ?	Non	Pas d'accès au serveur et au monitoring
PILOTAGE ET GOUVERNANCE SI	Le cadre et les règles de fonctionnement sont définis et l'inventaire des ressources mobilisables est réalisé ?	Non	
PILOTAGE ET GOUVERNANCE SI	Les responsables de services SI ou des domaines SI impactés par l'incident de sécurité SI sont tenus informés continuellement de la résolution de l'incident ?	Non	
PILOTAGE ET GOUVERNANCE SI	Les incidents de plus haut niveau de criticité donne lieu à un retour d'expérience avec une analyse des causes profondes après leur clôture ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
PILOTAGE ET GOUVERNANCE SI	Le site dispose-t-il d'une solution de journalisation centrale (syslog) ?	Non	Pas de solution de journalisation
PILOTAGE ET GOUVERNANCE SI	Tout acquisition de ressource ou de solution informatique s'effectue selon les règles définies dans la politique thématique "Sécurité SI" dans les contrats passés avec des Tiers ?	Oui	Dépendants de chaque département, il y a une procédure comptable pour l'acquisition des ressources informatiques
PILOTAGE ET GOUVERNANCE SI	Des solutions de scans de vulnérabilités sont mises en place et exploitées vis-à-vis des ressources les plus sensibles ?	Oui	NMAP et metasploit
PILOTAGE ET GOUVERNANCE SI	Des solutions de lutte contre les codes malveillants sont installés et activées sur tout élément connecté au SI la mesure où cela est techniquement possible ?	Non	Kaspersky, aucune visibilité
PILOTAGE ET GOUVERNANCE SI	Nommage des cartes réseau conforme aux vos nomes?	Non	
PILOTAGE ET GOUVERNANCE SI	Tous les tests sont effectués dans un environnement de pré-production ?	Oui	

Tableau 13: Questionnaire sur la catégorie Pilotage et Gouvernance SI

5.1.5 Réseaux et télécommunications

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Est-ce que vous avez des SLAs (Service Level Agreement) avec les opérateurs pour les liaisons Telco et internet ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Est-ce que Contrôle quotidien des lignes Internet/Intranet est effectué et documenté ?	Oui	Tests effectués, évolution vers l'automatisation de ce contrôle

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	La connectivité filaire (ex. Ethernet, etc.) est-elle renforcée par le service sans fil (ex. WIMAX) ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Des dispositifs anti-DDoS sont mis en œuvre pour détecter les dénis de service distribués (DDoS) ?	Pending	Information manquante
RESEAUX ET TELECOMMUNICATIONS	Les sites et téléchargements sont surveillés et/ou bloqués s'ils sont jugés nuisibles et/ou non productifs pour l'organisme ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Y a-t-il des restrictions sur le téléchargement, la copie ou le piratage de logiciels et de fichiers électroniques protégés par le droit d'auteur ou sans autorisation ?	Oui	PEPLINK
RESEAUX ET TELECOMMUNICATIONS	Avez-vous un conditionnement du trafic ?	Pending	Information manquante
RESEAUX ET TELECOMMUNICATIONS	Un mécanisme de restriction aux employés qui empêche d'accéder a des messages ou d'images discriminatoires, harcelants ou menaçants sur Internet ou via le service de messagerie de l'organisme ?	Oui	Oui avec le PEPLINK, par défaut tous les users ont accès à tous
RESEAUX ET TELECOMMUNICATIONS	Aucune ressource interne ne doit accéder à Internet sans passer par une chaine de liaison de sécurité maîtrisée par la DRSI ?	Oui	Firewall Cisco ASA
RESEAUX ET TELECOMMUNICATIONS	Est-ce que vous avez au moins deux liens internet deux fournisseurs différents ?	Oui	3 liens internet
RESEAUX ET TELECOMMUNICATIONS	Est-ce les liaisons internet sont installées dans deux salles serveurs différentes ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Redondance des Liens WAN en place ?	Oui	Grace aux projet e-gouv

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Est-ce que tous les dispositifs de face publiques sont placés dans DMZ ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Les serveurs DMZ sont-ils entièrement mise à jour pour faire face aux dernières vulnérabilités de sécurité ?	Oui	Mais de gestion centralisée
RESEAUX ET TELECOMMUNICATIONS	Des analyses des vulnérabilités quotidiennes et automatisées sont-elles effectuées sur les systèmes DMZ afin de fournir des alertes rapides des vulnérabilités nouvellement détectées ?	Oui	NMAP pour les scans de vul et Metaploit pour les tests d'intrusion
RESEAUX ET TELECOMMUNICATIONS	Les serveurs DMZ sont-ils entièrement séparés des réseaux LAN ?	Oui	Firewall Cisco ASA
RESEAUX ET TELECOMMUNICATIONS	La méthode Zero Trust Network Access est-elle mise en œuvre ?	Oui	Firewall Cisco ASA
RESEAUX ET TELECOMMUNICATIONS	La zone DMZ est configurée pour des firewalls frontales (non dorsale) ? (s'ils existent)	Oui	Firewall Cisco ASA (frontale et dorsale)
RESEAUX ET TELECOMMUNICATIONS	Les DNS locaux sont paramétrés dans le Firewall ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Aucunes des règles de pare-feu autorisent-elles les services à risque de votre zone démilitarisée (DMZ) vers votre réseau interne ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Est-ce que tous les points d'entrée et de sortie de votre réseau sont protégés par un pare-feu ?	Oui	Tout le réseau est protégé par un firewall
RESEAUX ET TELECOMMUNICATIONS	Est-ce que la connexion à l'interface du firewall est sécurisée par le protocole SSL (https) ?	Oui	HTTP non activé, configuration en mode commande

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Utilisation des groupes pour authentification client VPN ?	Oui	Il y a que les VPN site to site
RESEAUX ET TELECOMMUNICATIONS	Les adresses IP attribuées sont paramétrées suivant vos normes ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Au niveau des Règles Firewall, les groupes users sont utilisés ?	Oui	Exclusion ==> Pas de VPN clients
RESEAUX ET TELECOMMUNICATIONS	au niveau des Règles Firewall, les groupes ports sont utilisés ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Firewall à jour dans sa dernière version ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Pas de règles sortantes autorisant la sortie sur tous les protocoles et pour tous ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Pas de règles autorisant les applications et site interdit (P2P / site adulte, etc. …) ?	Non	
RESEAUX ET TELECOMMUNICATIONS	IPS à jour et en fonction ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Antivirus Firewall à jour et en fonction ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Est-ce que les règles de pare-feu non utilisées / périmées sont supprimées / désactivées ?	Oui	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Utilisation des groupes pour limitation accès VPN au service concerné ?	Oui	Exclusion ==> Pas de VPN clients
RESEAUX ET TELECOMMUNICATIONS	Utilisation des groupes pour autorisation navigation internet/Webfilter ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Vous n'avez pas de flux Internet qui ne sont pas gérés par un firewall (sites distants, dépôt ..)?	Oui	Tous les flux internet sont géré par ASA
RESEAUX ET TELECOMMUNICATIONS	Est-ce que les politiques de filtrage présentes dans les firewall portent des commentaires descriptifs.	Oui	
RESEAUX ET TELECOMMUNICATIONS	Filtrage web en fonction ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	La vérification des mises à jour auto est activée ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Notifications alertes emails envoyées lors connexion clients VPN ?	Oui	Exclusion ==> Pas de VPN clients
RESEAUX ET TELECOMMUNICATIONS	Notifications alertes emails envoyées lors des modifications règles trafic ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Nommage firewalls conforme aux normes ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Le Backup auto de la configuration est activé ?	Oui	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Le Firewall est en HA -Haute Disponibilité- ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Aucunes règles de pare-feu enfreignent-elles votre politique de sécurité ?	Non	Pas de politique de sécurité
RESEAUX ET TELECOMMUNICATIONS	Aucunes des règles de pare-feu autorisent-elles les services à risque provenant d'Internet ?	Non	Pas de politique de sécurité
RESEAUX ET TELECOMMUNICATIONS	Avez-vous mis en place un système d'alerte pour les événements ou activités importants, par exemple, les modifications de certaines règles ou si vous identifiez un nouveau risque très grave dans votre policy ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Le pare-feu et les serveurs de gestion sont-ils physiquement sécurisés avec un accès contrôlé ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Avez-vous une liste à jour des personnes autorisées à accéder aux salles de serveurs du pare-feu et configurer ce dernier ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Les interruptions SNMPv3 sont-elles configurées au niveau du firewall ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Les options HTTP et Telnet sont-elles désactivées pour l'interface de gestion du firewall ?	Oui	Que du SSH
RESEAUX ET TELECOMMUNICATIONS	Les options HTTP et Telnet sont-elles désactivées pour tous les profils de gestion du firewall ?	Oui	Que du SSH
RESEAUX ET TELECOMMUNICATIONS	Existe-t-il un ensemble de certificats valides pour une interface administrateur basée sur un navigateur ?	Oui	Que du SSH

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Les règles restrictant les exigences minimales en matière de mot de passe ('Minimum Password Complexity', 'Minimum Length') sont activées et configurées ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Exigence d'une authentification MFA et/ou une politique de mots de passe forts est mise en place ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Enregistrez-vous (en terme de log) uniquement le trafic nécessaire ?	Non	Pas activé sur le Firewall
RESEAUX ET TELECOMMUNICATIONS	Activez-vous uniquement l'inspections SSL sur les applications critiques ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Utilisez-vous NTP pour synchroniser l'heure sur le Firewall ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	L'analyse antivirus à la périphérie du réseau pour tous les services est-elle activée ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Ne mettez-vous pas les fichiers en quarantaine, sauf si vous les surveillez et les révisez régulièrement ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Utilisez-vous les moteurs antispam ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	L'analyse IPS à la périphérie du réseau pour tous les services est activée ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les signatures IPS sont-elles configurées pour bloquer les signatures correspondantes ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Aucune des règles de pare-feu autorisent-elles le trafic d'Internet vers des serveurs, des réseaux, des appareils ou des bases de données sensibles hors DMZ ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Réduisez-vous la taille maximale du fichier à analyser par AV ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Des tests d'intrusion sont réalisés régulièrement, par une entité tierce ?	Non	
RESEAUX ET TELECOMMUNICATIONS	La segmentation réseau est-elle renforcée par un firewall CORE ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Les liaisons "backbone" sont résilientes (chaque switch peut atteindre la salle serveur par deux chemins possibles) ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Câblage distribution certifié et rapport de certification disponible / présenté ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Pas de câbles apparent coté user ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les armoires ferment à clés et sont fermées ?	Non	
RESEAUX ET TELECOMMUNICATIONS	La fibre optique est exploitée avec des SFP (pas de présence des convertisseurs d'interface) ?	Non	
RESEAUX ET TELECOMMUNICATIONS	état général des goulottes / chemins de câbles : propres et intègre ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Pas de câblage qui a plus de 15 ans ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Câble exploité pour le backbone et distribution est du cat 6A ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Pas de cocheminement courant fort / faible de plus de 1 m dans les armoires?	Non	
RESEAUX ET TELECOMMUNICATIONS	Pas de cocheminment dans les chemins de câbles ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les cordons de raccordements ne sont pas des "home-made"	Non	
RESEAUX ET TELECOMMUNICATIONS	État général des armoires (poussiéreuses / présence d'éléments inutiles) ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les fibres optiques sont installées dans des coffrets de brassage optique ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	La salle serveurs dispose de faux planchers amovibles ?	Non	
RESEAUX ET TELECOMMUNICATIONS	La salle serveurs dispose de chemins de câble par le haut ?	Non	Pas de cablofil en hauteur
RESEAUX ET TELECOMMUNICATIONS	Le câblage réseau ne passent pas à côté des serveurs pour ne pas bloquer leur passage dans leur extraction pour maintenance ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Les courants faibles (servant à la communication) sont éloignés des courants forts (dédiés à l'alimentation) avec un espacement minimum de 10 cm entre les deux à l'exception des CC en Z des serveur ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Vous avez un Plan de câblage avec tableau de correspondance des prises RJ45 avec les ports des panneaux de brassage ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Vous utilisez un qualifieur réseau avec des fonctionnalités L3 pour vérifier le branchement ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Vous utilisez un câblage qui protège le signal par blindage ?	Non	Présence de cable Ftp par endroits
RESEAUX ET TELECOMMUNICATIONS	Vous respectez la norme T568B pour la convention câblage de votre entreprise ?	Non	Echec de certification dans la majeure partie des prises testées
RESEAUX ET TELECOMMUNICATIONS	Avant d'installer n'importe quel câble l'agencement du bâtiment est pris en considération de façon à ce que le plan de numérisation utilisé permette aux câbles d'être insérés dans la baie dans le bon ordre ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Le dégainage des connecteurs 'enveloppants' n'est pas visible ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Le dégainage visible ne doit pas excéder 3 mm en dehors du connecteur ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les écrans (le cas échéant) restent fermés après l'opération de coupe ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les espaces de rangement verticaux sont conçus pour permettre la gestion d'un plus grand nombre (30% par rapport à l'installation prévue) de cordons de brassage ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Le site de stockage ne présentant pas de risque d'humidité excessive, de chute d'objets, de déversement chimique (pétrole,graisse,etc.),de flammes nues ou de chaleur excessive ?	Non	
RESEAUX ET TELECOMMUNICATIONS	La distance autorisée entre les éléments de support du système de cheminement est de 1500 mm ou moin ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les chemins constitués d'assemblage de goulottes sont positionnés au dessus de la plinthe de façon à laisser un espace de 5 cm ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les systèmes de cheminement de câbles a une surface lisse et exempts de bavures ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Pas Co cheminement entre câbles courant fort et réseaux cuivre sans séparateurs ?	Non	
RESEAUX ET TELECOMMUNICATIONS	La distance de co-cheminement minimal des câbles FTP avec les courants forts est de minimum 40 mm ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les câbles de données et d'alimentation sont maintenus en place par un collier ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Le tracé des chemins évite les sources localisées de chaleur, d'humidité ou de vibration qui augmentent le risque d'endommagement de la construction ou la performance du câble ?	Non	
RESEAUX ET TELECOMMUNICATIONS	L'emplacement des armoires, châssis et baies laisse un dégagement minimum de 1,2 m sur tous les côtés ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Un coffret de communication qui permet de distribuer les signaux de courant faible est mises en place ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Un nettoyage minutieux est effectué régulièrement avec une éliminations des éléments inutiles ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les fibres optiques sont installées dans des coffrets de brassage actif ou Tripe Play ou aussi un coffret de communication grade 4) ?	Non	
RESEAUX ET TELECOMMUNICATIONS	QoS sur Visio ?	Non	Visio pas encore en place
RESEAUX ET TELECOMMUNICATIONS	La solution de monitoring supervise tous les équipements et périphériques IP ?	Oui	Pour les équipements qui ont des IP
RESEAUX ET TELECOMMUNICATIONS	La solution de supervision est déployée à un endroit qui la rende hautement disponible tout en atteignant tous les systèmes surveillés ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	La solution de supervision communique, graphiquement et régulièrement ?	Oui	Oui les rapports envoyés régulièrements
RESEAUX ET TELECOMMUNICATIONS	Un schéma WAN et interco à jour est disponible ?	Oui	Le schéma disponible
RESEAUX ET TELECOMMUNICATIONS	Toutes les prises réseaux sont étiquetées ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Un schéma du réseau Lan à jour est disponible ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Présence d'un équipement de type Coreswitch ?	Oui	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Le cœur de réseau est-il résilient (2 core switch) ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Présence d'un Firewall LAN?	Non	
RESEAUX ET TELECOMMUNICATIONS	Est-ce que les switchs sont synchronisés avec un serveur NTP ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Définition des flux métier (matrice des flux inter vlan à autoriser) ?	Non	
RESEAUX ET TELECOMMUNICATIONS	L'accès en gestion est en SSH et Telnet désactivé ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Les alimentations des switchs sont elles redondantes ?	Non	
RESEAUX ET TELECOMMUNICATIONS	IP Helper en place sur core switch ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	les credentiaux d'accès switch présentent un niveau de complexité satisfaisant ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Les ports non utilisés dans les coffrets d'accès sont désactivés ?	Non	
RESEAUX ET TELECOMMUNICATIONS	L'activation et désactivation des ports sont documentées ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Une liste des définitions des flux inter-vlan pour applications autorisées à t-elle été rédigée ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Les switchs sont à jour de leur firmware ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Nommage switch conforme aux normes de votre Organisation ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Pas de Présence de switch non-manageable ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Pas de Présence de switch d'autre marque	Non	
RESEAUX ET TELECOMMUNICATIONS	Affectation correcte des équipements à leur VLAN cible ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Adressage IP conforme aux vos normes	Oui	
RESEAUX ET TELECOMMUNICATIONS	Existence de l'ensemble des VLAN nécessaire ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	la sauvegarde automatiques des switch est configurée ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Vous disposez de la sauvegarde configuration de tous vos switch ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	la segmentation vlan est en place ?	Oui	Mais une refonte néccéssaire pour se conformer aux nouvelles exigences
RESEAUX ET TELECOMMUNICATIONS	Core switch (fédérateur) sont-ils hautement disponible, et tolérant aux pannes ?	Non	Pas de double alimentations
RESEAUX ET TELECOMMUNICATIONS	Si deux ou plus sont installés dans une même baie, sont-ils stackés ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Un test pour vous assurer que les utilisateurs non SSH ne peuvent pas effectuer de Telnet est effectué ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Vous disposez d'une alimentation SPARE ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Vous prévoyez des câbles spare pour 10% du nombre de switch*2 ?	Non	
RESEAUX ET TELECOMMUNICATIONS	A partir de 3 switchs, vous utilisez un câble « data » de 1m pour connecter le 1er et le dernier switch ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Pour les câbles, vous prenez garde à la longueur nécessaire, les câbles supérieurs à 100 m vous utilisez les modules + fibre ?	Non	
RESEAUX ET TELECOMMUNICATIONS	La vitesse Bande Passante est déclarée sur chaque interface du peplink ?	Oui	
RESEAUX ET TELECOMMUNICATIONS	Le portail captif est configuré dans le réseau "Invité" ?	Non	

CAT: SI	QUESTIONS	Réponse	Commentaire
RESEAUX ET TELECOMMUNICATIONS	Contrôleur en place et configuré ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Est-ce que le Suivi mensuel des d'accès Wifi est effectué et documenté ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Firmware des bornes est à jour ?	Non	
RESEAUX ET TELECOMMUNICATIONS	Multiple ssid en place et chacun sur son vlan ?	Non	
RESEAUX ET TELECOMMUNICATIONS	L'accès aux équipements critiques (Ex:Firewall) pour la gestion via WIFI pour des raisons de sécurité est désactivée ?	Non	

Tableau 14: Questionnaire sur la catégorie Réseaux et Télécommunications

5.1.6 Synthèse des résultats

Sur la base des réponses collectées, une analyse a été réalisée pour évaluer le niveau de conformité du Système d'Information (SI) de l'Université de Lomé sur les cinq catégories définies.

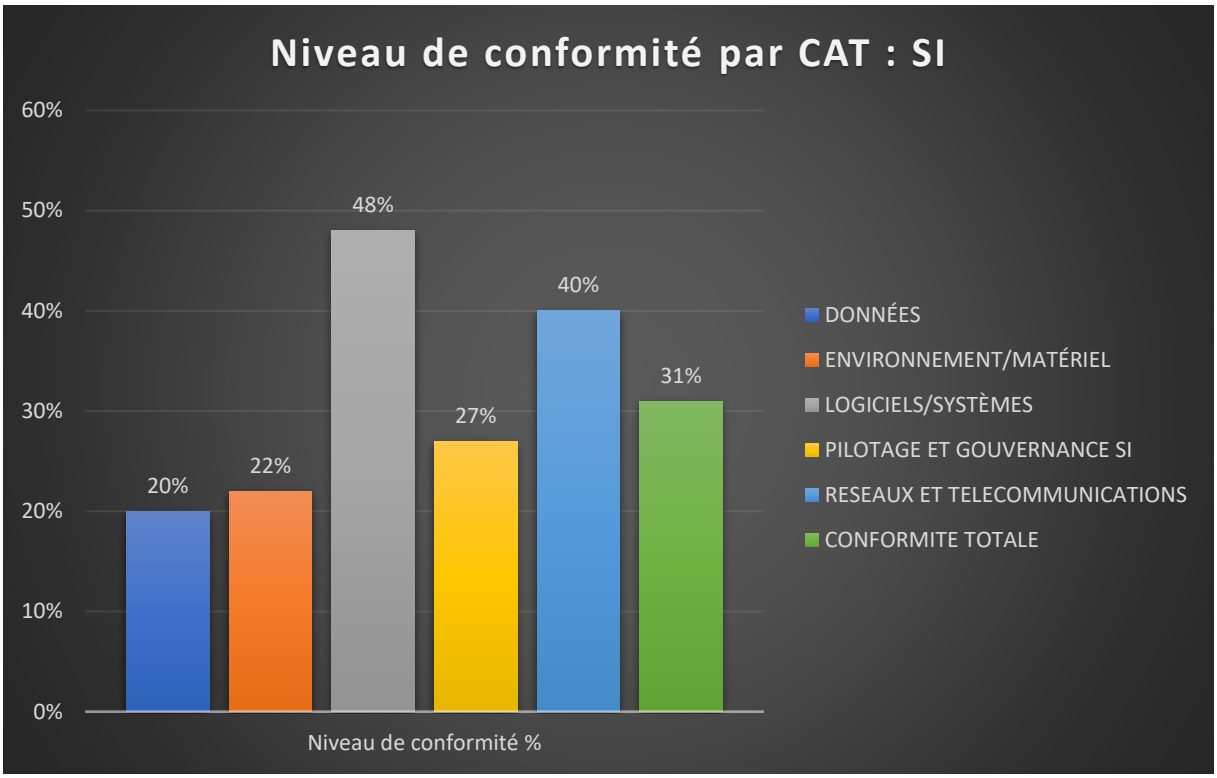


Figure 3: Résumé des conformités par catégorie

Les résultats des évaluations ont permis d'identifier des écarts significatifs entre l'état actuel du SI et les bonnes pratiques en matière de gouvernance, de sécurité et de performance. On observe des faiblesses notables sur toutes les catégories

5.2 Infrastructure réseau du datacenter

Depuis l'audit initial, l'architecture réseau de l'université n'a pas connu de modifications majeures.

Au niveau du cœur de réseau, trois équipements principaux sont en place :

- Routeur PEPLINK Balance 710 : Il assure la répartition de charge (load balancing) des différentes connexions Internet.
- Pare-feu Cisco ASA 5525x : Connecté au routeur PEPLINK, il assure des fonctions de filtrage et d'inspection du trafic interne (LAN) et externe (WAN).
- Switch Cisco 3850 24x : Situé au cœur du réseau, il connecte les switches de distribution (Cisco 2960) ainsi que les serveurs situés dans la DMZ.

Constats

- Absence de redondance au niveau du cœur et de la distribution du réseau, augmentant ainsi les risques de panne critique.

- Mutualisation des fonctions de pare-feu interne et externe, ce qui peut limiter la segmentation et la sécurité du réseau.
- Obsolescence des équipements réseau :
    - Pare-feu Cisco ASA 5525x : Plus disponible à la vente depuis le 2 septembre 2022 (EOS) et arrivera en fin de support le 30 septembre 2025 (EOL), nécessitant une migration.
    - Switch Cisco 3850 24x : EOL depuis le 7 mars 2023 et EOS depuis le 5 septembre 2023, rendant sa migration indispensable.
    - Switches Cisco 2960 : EOL depuis le 7 septembre 2023, EOS depuis le 5 septembre 2023, et fin de support prévue le 30 septembre 2025.

    Leur maintien en service représente un risque majeur en cas de panne, justifiant une mise à niveau urgente.

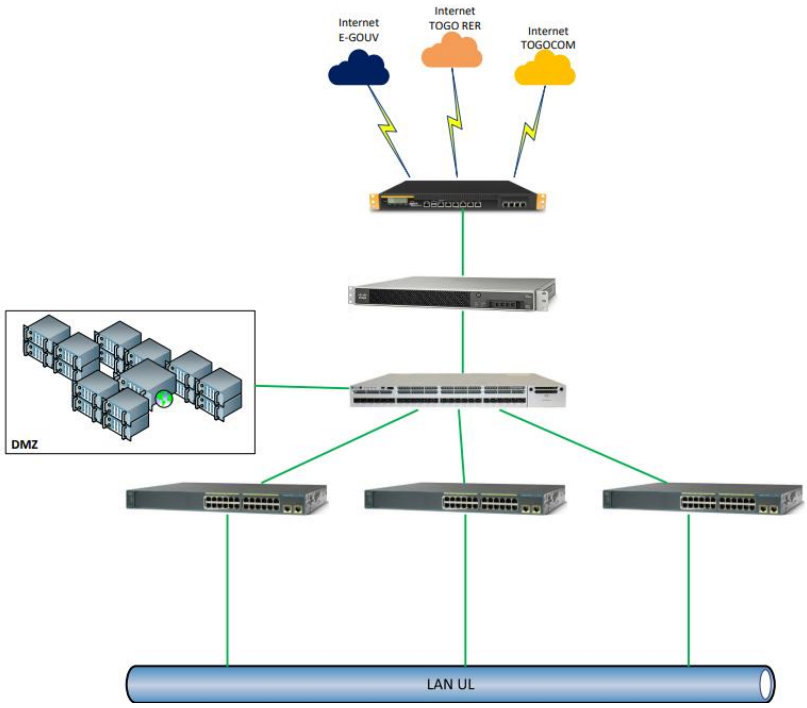


Figure 4: Architecture simplifiée de l'UL

5.3 Infrastructure physique

L'infrastructure physique des salles serveurs de l'Université de Lomé présente plusieurs lacunes qui compromettent leur efficacité et leur sécurité. Parmi les principales insuffisances relevées :

Conditions Environnementales Inadaptées

- Présence de câblages désordonnés (« en spaghetti ») dans les baies, compliquant la maintenance et augmentant les risques de panne.
- Absence de chemins de câbles, ce qui entraîne un câblage désorganisé et un risque d'endommagement des connexions.

Problèmes d'Aménagement et de Sécurité

- Serveurs installés sur des tables au lieu d'être correctement montés en baie, augmentant le risque de dommages physiques.
- Salle sans contrôle d'accès, exposant les équipements à des intrusions non autorisées.
- Utilisation de rallonges électriques dans les baies, augmentant le risque de surcharge et d'incendie.
- Sol en béton sans faux plancher, rendant difficile l'organisation et la protection des câbles.

Encombrement et Gestion des Espaces

- Présence d'équipements obsolètes ou hors production dans les baies, limitant l'espace disponible pour les équipements en service.
- Accumulation d'objets inutiles (cartons d'équipements, matériels hors d'usage, etc.) dans les salles serveurs, réduisant l'accessibilité.
- Absence d'étiquetage des câbles dans les coffrets.
- Câbles mal rangés dans les coffrets informatiques.
- Coffrets non étiquetés et non numérotés.
- Coffrets non fermés.

Figure 5: quelques Images du datacenter de l'UL

5.4 Rapports de certification des médias

5.4.1 Certification des prises informatiques

Université de Lomé

TREND AnyWARE®
Résumé du rapport de certification

Nom du Répertoire:	Entreprise qui teste et installe	Date de tests	Certificateurs utilisés pour le projet
CRETIFICATIONS DES PRISES RESE...	BUY MORE	14 FEB 2025	LanTEK III 1000 / 1612238 / 15 APR 2016
Université de Lomé	69698985	vers	
Ancien CIC		10 MAR 2025	
Lomé			
Togo			
00000000			

Paire torsadée	Coaxial	Fibre optique	Techniciens sur le projet
Nombre de tests: 11	Nombre de tests: 0	Nombre de tests: 0	AUGUSTIN
Succès: 6	Succès: 0	Succès: 0	
Échec: 5	Échec: 0	Échec: 0	
% de succès: 54.55	% de succès: 0	% de succès: 0	
Longueur (m): 114.5	Longueur (m):	Longueur (m):	

Notes du répertoire:

Résumé de la marge la plus basse sur paire torsadée

	NEXT	PSNEXT	Pertes par retour	Perte d'insertion
Marge (dB)	6.10	6	-2.10	1.30
ID du test	FDS PRISE I18	FDS PRISE I18	DRSI PRISE 84	DRSI PRISE 1

	ACR-F	ACR-N
Marge (dB)	14.40	16
ID du test	FDS PRISE I19	DRSI PRISE 1

Câble le plus long: DRSI PRISE 1 : 30.9(m)

Paires torsadées marge moyenne

	NEXT	PSNEXT	Pertes par retour	Perte d'insertion
Marge (dB)	9.67	10.71	2.51	1.96

	ACR-F	ACR-N
Marge (dB)	17.51	19.50

Longueur moy. 16.4(m)

Figure 6: Résumé de la certification des prises informatiques

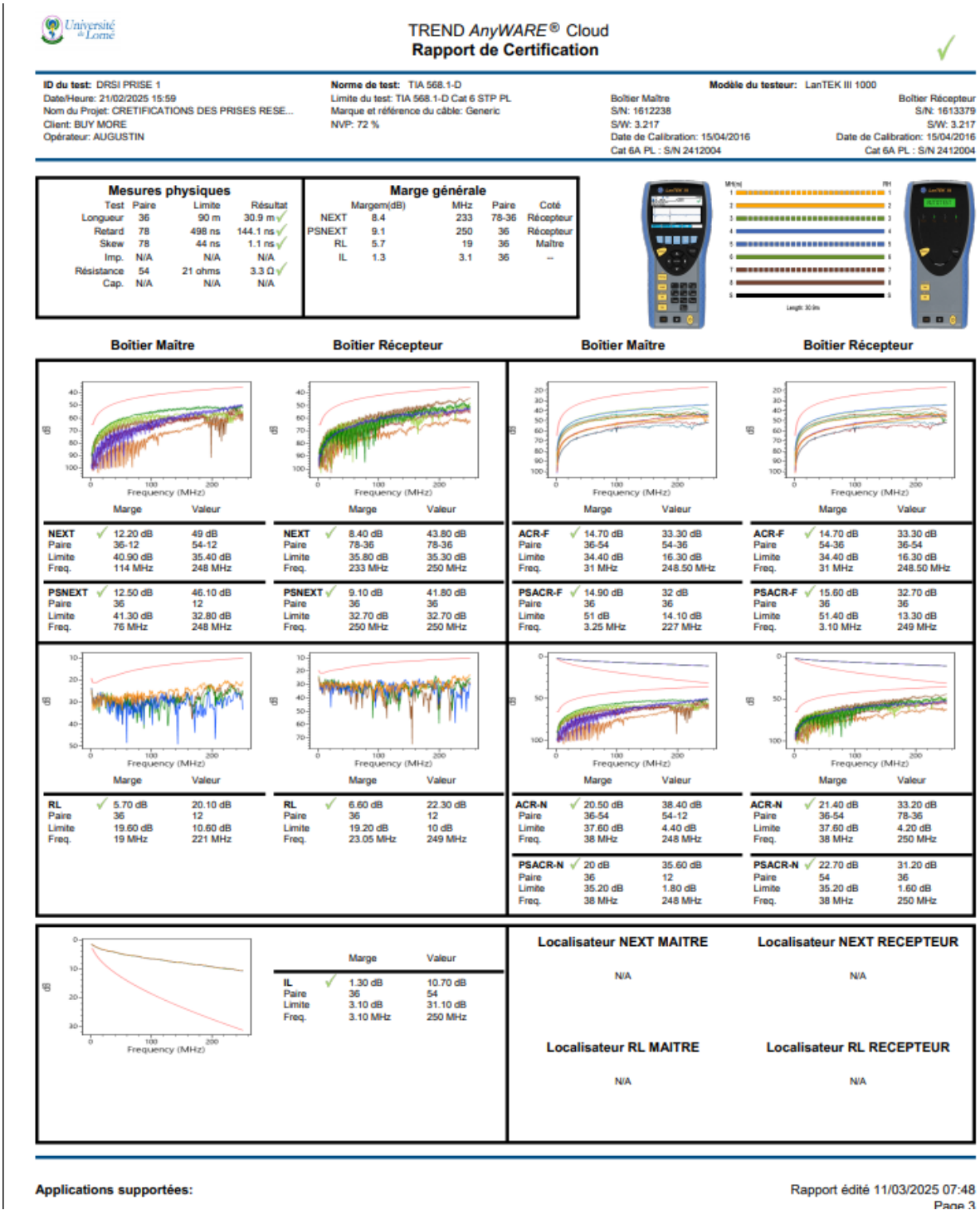
Université de Lomé

TREND *AnyWARE*® Cloud
Rapport de Certification

CRETIFICATIONS DES PRISES RESEAU FDS - DRSI
BUY MORE
11/03/2025

Nom du test	Longueur (m)	Date	Catégorie du câble	Norme de certification	Marge NEXT (dB)	Résultat
DRSI PRISE 1	30.9	21/02/2025 15:59	TIA 568.1-D Cat 6 STP PL	TIA 568.1-D	8.40	Passe
DRSI PRISE 2	16.6	14/02/2025 13:38	TIA 568.1-D Cat 5E STP PL	TIA 568.1-D	15.00	Passe
DRSI PRISE 21		14/02/2025 13:35	TIA 568.1-D Cat 5E STP PL	TIA 568.1-D	N/A	Échec
DRSI PRISE 33	9.7	14/02/2025 13:31	TIA 568.1-D Cat 5E STP PL	TIA 568.1-D	12.30	Passe
DRSI PRISE 38	10.2	14/02/2025 13:30	TIA 568.1-D Cat 5E STP PL	TIA 568.1-D	11.60	Passe
DRSI PRISE 52		14/02/2025 13:45	TIA 568.1-D Cat 5E STP PL	TIA 568.1-D	N/A	Échec
DRSI PRISE 53		14/02/2025 13:43	TIA 568.1-D Cat 5E STP PL	TIA 568.1-D	N/A	Échec
DRSI PRISE 84	24.0	14/02/2025 13:48	TIA 568.1-D Cat 5E STP PL	TIA 568.1-D	7.90	Échec
FDS PRISE I12		10/03/2025 17:01	TIA 568.1-D Cat 6 STP PL	TIA 568.1-D	N/A	Échec
FDS PRISE I18	10.1	10/03/2025 16:55	TIA 568.1-D Cat 6 STP PL	TIA 568.1-D	6.10	Passe
FDS PRISE I19	13.0	10/03/2025 16:56	TIA 568.1-D Cat 6 STP PL	TIA 568.1-D	6.40	Passe

Figure 7: Résumé de la certification des prises informatiques



TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: DRSI PRISE 1
Date/Heure: 21/02/2025 15:59
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 6 STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	36	90 m	30.9 m ✓
Retard	78	498 ns	144.1 ns ✓
Skew	78	44 ns	1.1 ns ✓
Imp.	N/A	N/A	N/A
Résistance	54	21 ohms	3.3 Ω ✓
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	8.4	233	78-36	Récepteur
PSNEXT	9.1	250	36	Récepteur
RL	5.7	19	36	Maître
IL	1.3	3.1	36	--

Boîtier Maître

		Marge	Valeur
NEXT	✓	12.20 dB	49 dB
Paire		36-12	54-12
Limite		40.90 dB	35.40 dB
Freq.		114 MHz	248 MHz
PSNEXT	✓	12.50 dB	46.10 dB
Paire		36	12
Limite		41.30 dB	32.80 dB
Freq.		76 MHz	248 MHz

Boîtier Récepteur

		Marge	Valeur
NEXT	✓	8.40 dB	43.80 dB
Paire		78-36	78-36
Limite		35.80 dB	35.30 dB
Freq.		233 MHz	250 MHz
PSNEXT	✓	9.10 dB	41.80 dB
Paire		36	36
Limite		32.70 dB	32.70 dB
Freq.		250 MHz	250 MHz

Boîtier Maître

		Marge	Valeur
ACR-F	✓	14.70 dB	33.30 dB
Paire		36-54	54-36
Limite		34.40 dB	16.30 dB
Freq.		31 MHz	248.50 MHz
PSACR-F	✓	14.90 dB	32 dB
Paire		36	36
Limite		51 dB	14.10 dB
Freq.		3.25 MHz	227 MHz

Boîtier Récepteur

		Marge	Valeur
ACR-F	✓	14.70 dB	33.30 dB
Paire		54-36	36-54
Limite		34.40 dB	16.30 dB
Freq.		31 MHz	248.50 MHz
PSACR-F	✓	15.60 dB	32.70 dB
Paire		36	36
Limite		51.40 dB	13.30 dB
Freq.		3.10 MHz	249 MHz

		Marge	Valeur
RL	✓	5.70 dB	20.10 dB
Paire		36	12
Limite		19.60 dB	10.60 dB
Freq.		19 MHz	221 MHz

		Marge	Valeur
RL	✓	6.60 dB	22.30 dB
Paire		36	12
Limite		19.20 dB	10 dB
Freq.		23.05 MHz	249 MHz

		Marge	Valeur
ACR-N	✓	20.50 dB	38.40 dB
Paire		36-54	54-12
Limite		37.60 dB	4.40 dB
Freq.		38 MHz	248 MHz
PSACR-N	✓	20 dB	35.60 dB
Paire		36	12
Limite		35.20 dB	1.80 dB
Freq.		38 MHz	248 MHz

		Marge	Valeur
ACR-N	✓	21.40 dB	33.20 dB
Paire		36-54	78-36
Limite		37.60 dB	4.20 dB
Freq.		38 MHz	250 MHz
PSACR-N	✓	22.70 dB	31.20 dB
Paire		54	36
Limite		35.20 dB	1.60 dB
Freq.		38 MHz	250 MHz

		Marge	Valeur
IL	✓	1.30 dB	10.70 dB
Paire		36	54
Limite		3.10 dB	31.10 dB
Freq.		3.10 MHz	250 MHz

Localisateur NEXT MAITRE
N/A

Localisateur NEXT RECEPTEUR
N/A

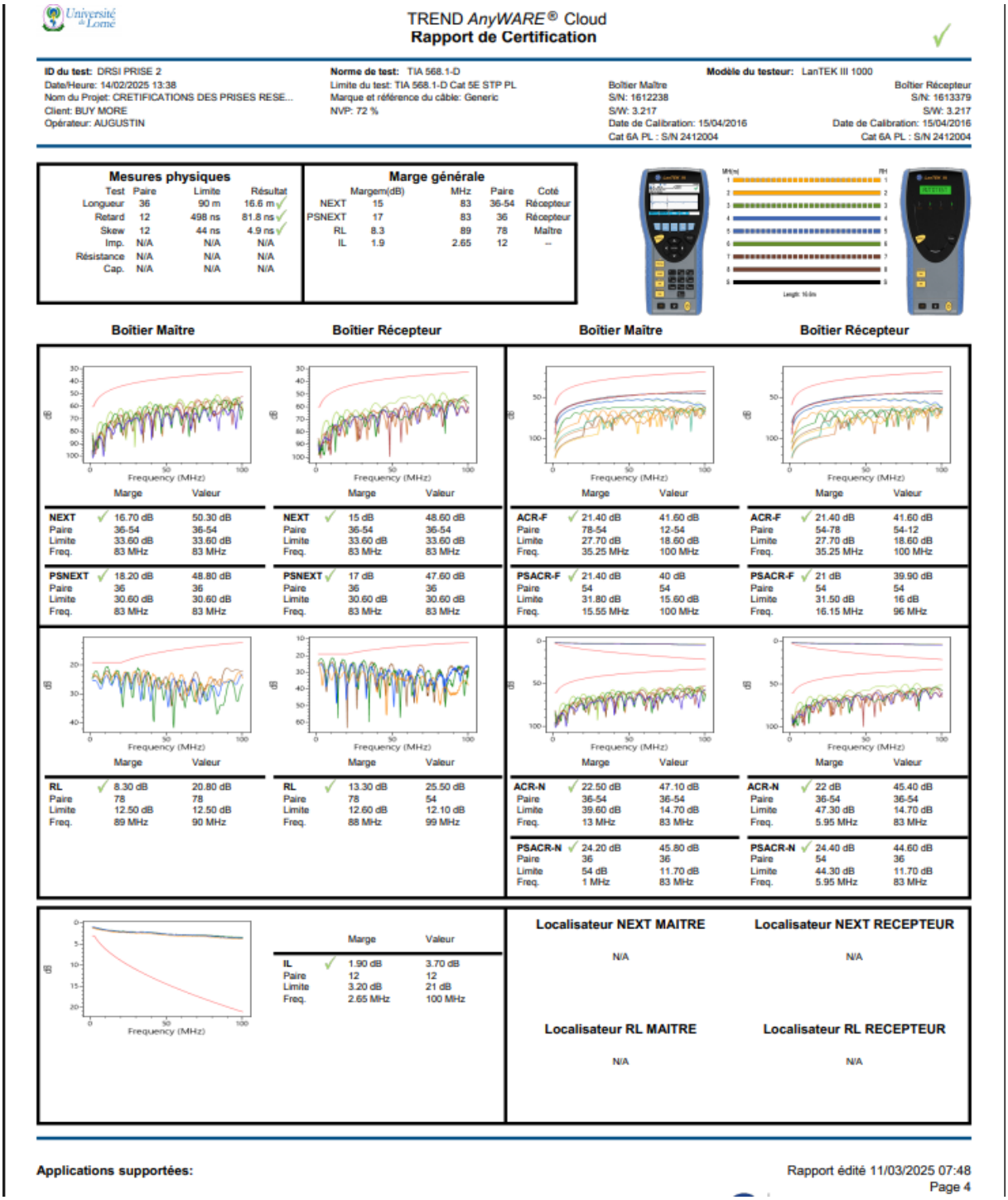
Localisateur RL MAITRE
N/A

Localisateur RL RECEPTEUR
N/A

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 3

Figure 8: Certification 1er prise



TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: DRSI PRISE 2
Date/Heure: 14/02/2025 13:38
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 5E STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	36	90 m	16.6 m ✓
Retard	12	498 ns	81.8 ns ✓
Skew	12	44 ns	4.9 ns ✓
Imp.	N/A	N/A	N/A
Résistance	N/A	N/A	N/A
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	15	83	36-54	Récepteur
PSNEXT	17	83	36	Récepteur
RL	8.3	89	78	Maître
IL	1.9	2.65	12	--

Boîtier Maître — **Boîtier Récepteur** — **Boîtier Maître** — **Boîtier Récepteur**

Frequency (MHz)

	Marge	Valeur	Marge	Valeur	Marge	Valeur	Marge	Valeur
	✓		✓		✓		✓	
	16.70 dB	50.30 dB	15 dB	48.60 dB	21.40 dB	41.60 dB	21.40 dB	41.60 dB
Paire	36-54	36-54	36-54	36-54	78-54	12-54	54-78	54-12
Limite	33.60 dB	33.60 dB	33.60 dB	33.60 dB	27.70 dB	18.60 dB	27.70 dB	18.60 dB
Freq.	83 MHz	83 MHz	83 MHz	83 MHz	35.25 MHz	100 MHz	35.25 MHz	100 MHz
	NEXT		NEXT		ACR-F		ACR-F	
	✓ 18.20 dB	48.80 dB	✓ 17 dB	47.60 dB	✓ 21.40 dB	40 dB	✓ 21 dB	39.90 dB
Paire	36	36	36	36	54	54	54	54
Limite	30.60 dB	30.60 dB	30.60 dB	30.60 dB	31.80 dB	15.60 dB	31.50 dB	16 dB
Freq.	83 MHz	83 MHz	83 MHz	83 MHz	15.55 MHz	100 MHz	16.15 MHz	96 MHz
	PSNEXT		PSNEXT		PSACR-F		PSACR-F	

	Marge	Valeur	Marge	Valeur	Marge	Valeur	Marge	Valeur
	✓		✓		✓		✓	
	8.30 dB	20.80 dB	13.30 dB	25.50 dB	22.50 dB	47.10 dB	22 dB	45.40 dB
Paire	78	78	78	54	36-54	36-54	36-54	36-54
Limite	12.50 dB	12.50 dB	12.60 dB	12.10 dB	39.60 dB	14.70 dB	47.30 dB	14.70 dB
Freq.	89 MHz	90 MHz	88 MHz	99 MHz	13 MHz	83 MHz	5.95 MHz	83 MHz
	RL		RL		ACR-N		ACR-N	
					✓ 24.20 dB	45.80 dB	✓ 24.40 dB	44.60 dB
					36	36	54	36
					54 dB	11.70 dB	44.30 dB	11.70 dB
					1 MHz	83 MHz	5.95 MHz	83 MHz
					PSACR-N		PSACR-N	

	Marge	Valeur
	✓	
IL	1.90 dB	3.70 dB
Paire	12	12
Limite	3.20 dB	21 dB
Freq.	2.65 MHz	100 MHz

Localisateur NEXT MAITRE — N/A
Localisateur NEXT RECEPTEUR — N/A
Localisateur RL MAITRE — N/A
Localisateur RL RECEPTEUR — N/A

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 4

Figure 9: Certification 2ième prise

Université de Lorné

TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: DRSI PRISE 21
Date/Heure: 14/02/2025 13:35
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 5E STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

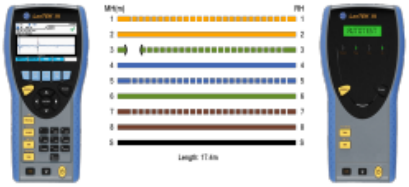
Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	N/A	N/A	N/A
Retard	N/A	N/A	N/A
Skew	N/A	N/A	N/A
Imp.	N/A	N/A	N/A
Résistance	N/A	N/A	N/A
Cap.	N/A	N/A	N/A

Marge générale

Marge(dB)	MHz	Paire	Coté
NEXT N/A	N/A	N/A	N/A
PSNEXT N/A	N/A	N/A	N/A
RL N/A	N/A	N/A	N/A
IL N/A	N/A	N/A	--



Boîtier Maître	Boîtier Récepteur	Boîtier Maître	Boîtier Récepteur

NEXT (dB) — Boîtier Maître

	Marge	Valeur
NEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSNEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

NEXT (dB) — Boîtier Récepteur

	Marge	Valeur
NEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSNEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-F (dB) — Boîtier Maître

	Marge	Valeur
ACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-F (dB) — Boîtier Récepteur

	Marge	Valeur
ACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

RL (dB) — Boîtier Maître

	Marge	Valeur
RL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

RL (dB) — Boîtier Récepteur

	Marge	Valeur
RL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-N (dB) — Boîtier Maître

	Marge	Valeur
ACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-N (dB) — Boîtier Récepteur

	Marge	Valeur
ACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

	Marge	Valeur
IL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

Localisateur NEXT MAITRE
N/A

Localisateur NEXT RECEPTEUR
N/A

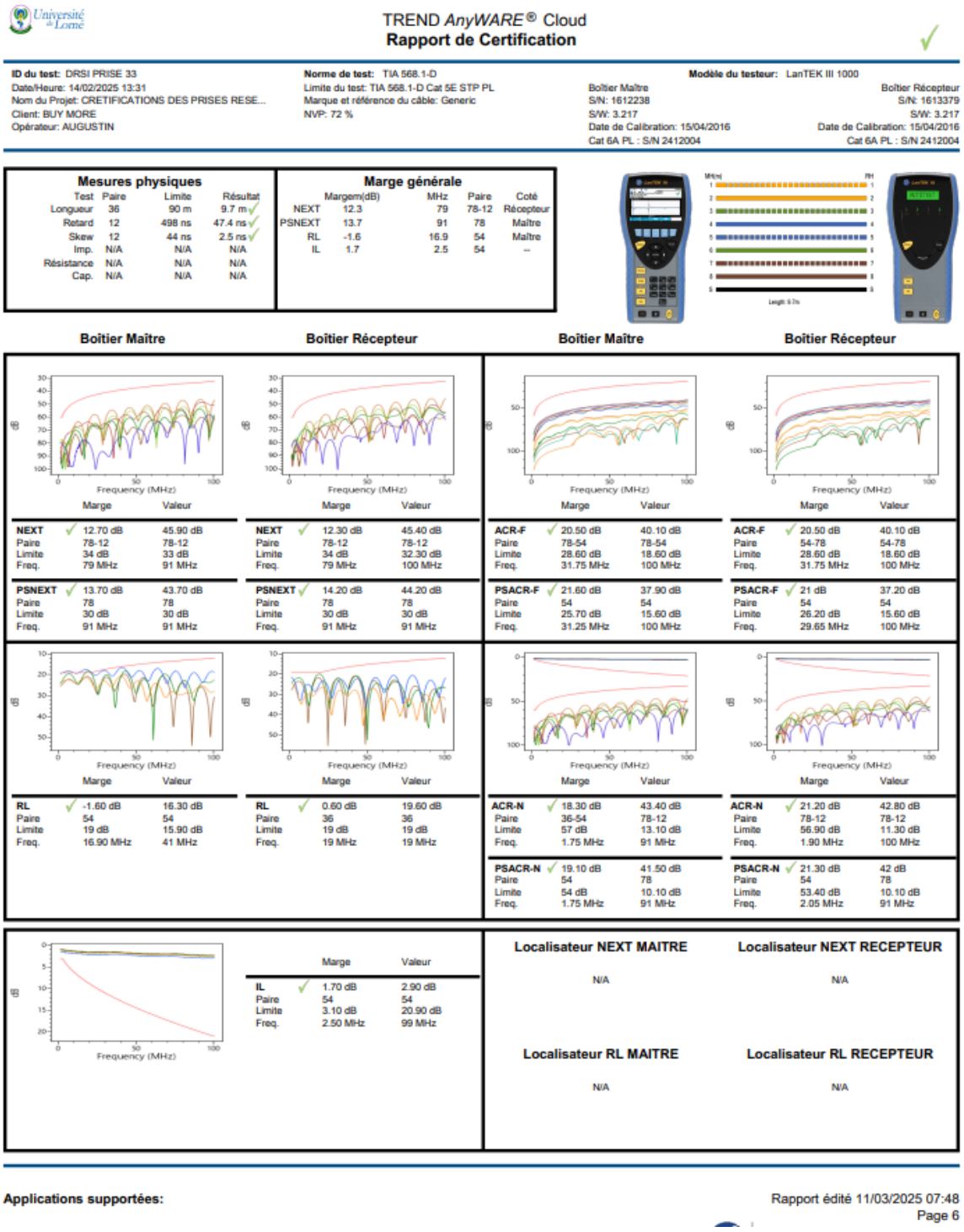
Localisateur RL MAITRE
N/A

Localisateur RL RECEPTEUR
N/A

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 5

Figure 10: Certification 3ième prise



TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: DRSI PRISE 33
Date/Heure: 14/02/2025 13:31
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 5E STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	36	90 m	9.7 m ✓
Retard	12	498 ns	47.4 ns ✓
Skew	12	44 ns	2.5 ns ✓
Imp.	N/A	N/A	N/A
Résistance	N/A	N/A	N/A
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	12.3	79	78-12	Récepteur
PSNEXT	13.7	91	78	Maître
RL	-1.6	16.9	54	Maître
IL	1.7	2.5	54	--

Boîtier Maître — **Boîtier Récepteur** — **Boîtier Maître** — **Boîtier Récepteur**

Frequency (MHz)

	Marge	Valeur	Marge	Valeur	Marge	Valeur	Marge	Valeur
	NEXT ✓	12.70 dB	45.90 dB	NEXT ✓	12.30 dB	45.40 dB	ACR-F ✓	20.50 dB	40.10 dB	ACR-F ✓	20.50 dB	40.10 dB
	Paire	78-12	78-12	Paire	78-12	78-12	Paire	78-54	78-54	Paire	54-78	54-78
	Limite	34 dB	33 dB	Limite	34 dB	32.30 dB	Limite	28.60 dB	18.60 dB	Limite	28.60 dB	18.60 dB
	Freq.	79 MHz	91 MHz	Freq.	79 MHz	100 MHz	Freq.	31.75 MHz	100 MHz	Freq.	31.75 MHz	100 MHz
	PSNEXT ✓	13.70 dB	43.70 dB	PSNEXT ✓	14.20 dB	44.20 dB	PSACR-F ✓	21.60 dB	37.90 dB	PSACR-F ✓	21 dB	37.20 dB
	Paire	78	78	Paire	78	78	Paire	54	54	Paire	54	54
	Limite	30 dB	30 dB	Limite	30 dB	30 dB	Limite	25.70 dB	15.60 dB	Limite	26.20 dB	15.60 dB
	Freq.	91 MHz	91 MHz	Freq.	91 MHz	91 MHz	Freq.	31.25 MHz	100 MHz	Freq.	29.65 MHz	100 MHz
	RL ✓	-1.60 dB	16.30 dB	RL ✓	0.60 dB	19.60 dB	ACR-N ✓	18.30 dB	43.40 dB	ACR-N ✓	21.20 dB	42.80 dB
	Paire	54	54	Paire	36	36	Paire	36-54	78-12	Paire	78-12	78-12
	Limite	19 dB	15.90 dB	Limite	19 dB	19 dB	Limite	57 dB	13.10 dB	Limite	56.90 dB	11.30 dB
	Freq.	16.90 MHz	41 MHz	Freq.	19 MHz	19 MHz	Freq.	1.75 MHz	91 MHz	Freq.	1.90 MHz	100 MHz
							PSACR-N ✓	19.10 dB	41.50 dB	PSACR-N ✓	21.30 dB	42 dB
							Paire	54	78	Paire	54	78
							Limite	54 dB	10.10 dB	Limite	53.40 dB	10.10 dB
							Freq.	1.75 MHz	91 MHz	Freq.	2.05 MHz	91 MHz

	Marge	Valeur
IL ✓	1.70 dB	2.90 dB
Paire	54	54
Limite	3.10 dB	20.90 dB
Freq.	2.50 MHz	99 MHz

Localisateur NEXT MAITRE N/A

Localisateur NEXT RECEPTEUR N/A

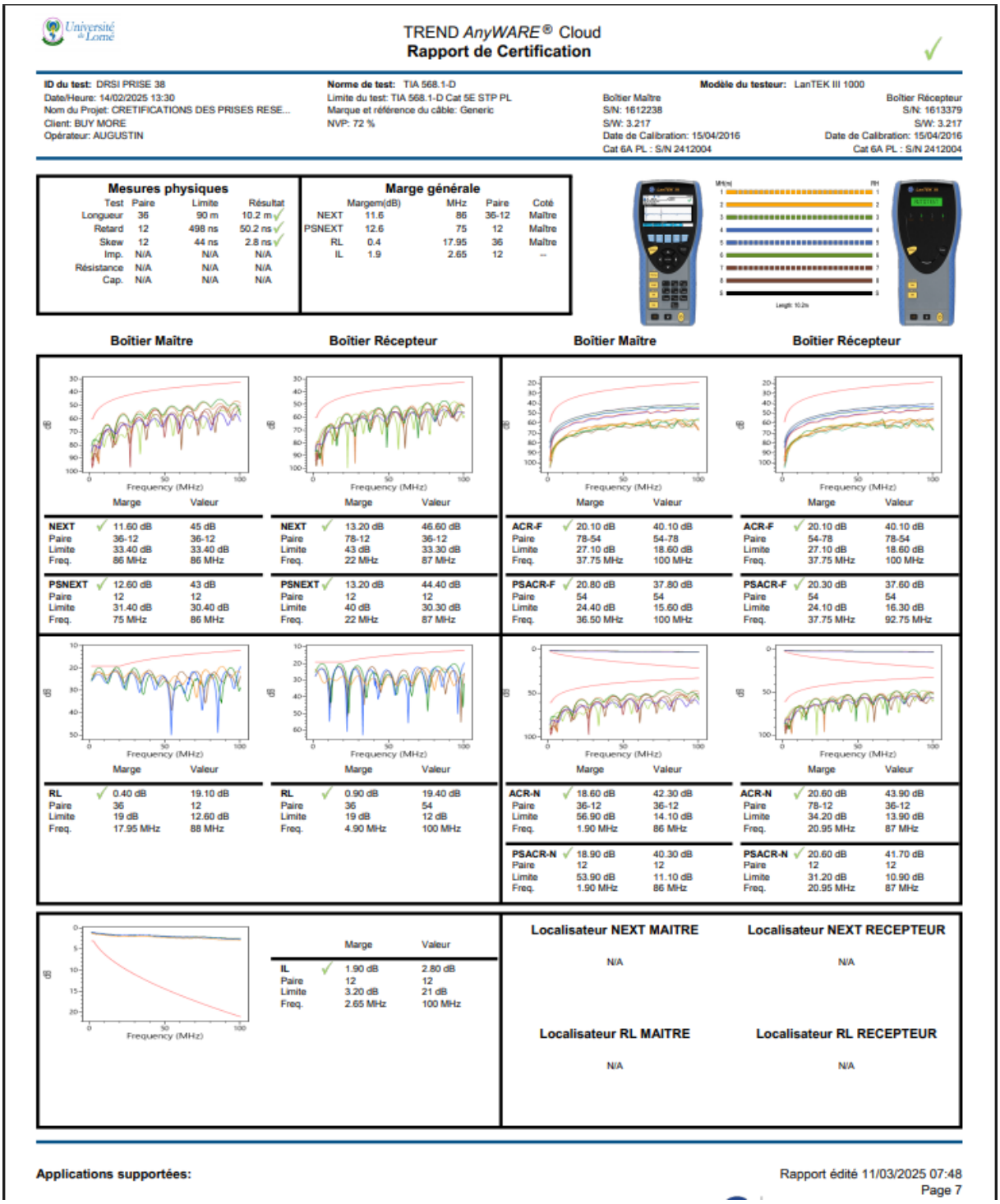
Localisateur RL MAITRE N/A

Localisateur RL RECEPTEUR N/A

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 6

Figure 11: Certification 4ième prise



TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: DRSI PRISE 38
Date/Heure: 14/02/2025 13:30
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 5E STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	36	90 m	10.2 m ✓
Retard	12	498 ns	50.2 ns ✓
Skew	12	44 ns	2.8 ns ✓
Imp.	N/A	N/A	N/A
Résistance	N/A	N/A	N/A
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	11.6	86	36-12	Maître
PSNEXT	12.6	75	12	Maître
RL	0.4	17.95	36	Maître
IL	1.9	2.65	12	--

Boîtier Maître — **Boîtier Récepteur** — **Boîtier Maître** — **Boîtier Récepteur**

	Marge	Valeur	Marge	Valeur	Marge	Valeur	Marge	Valeur
	✓	11.60 dB	✓	13.20 dB	✓	20.10 dB	✓	20.10 dB
	Paire	36-12	Paire	78-12	Paire	78-54	Paire	54-78
	Limite	33.40 dB	Limite	43 dB	Limite	27.10 dB	Limite	27.10 dB
	Freq.	86 MHz	Freq.	22 MHz	Freq.	37.75 MHz	Freq.	37.75 MHz
	✓	12.60 dB	✓	13.20 dB	✓	20.80 dB	✓	20.30 dB
	Paire	12	Paire	12	Paire	54	Paire	54
	Limite	31.40 dB	Limite	40 dB	Limite	24.40 dB	Limite	24.10 dB
	Freq.	75 MHz	Freq.	22 MHz	Freq.	36.50 MHz	Freq.	37.75 MHz
	✓	0.40 dB	✓	0.90 dB	✓	18.60 dB	✓	20.60 dB
	Paire	36	Paire	36	Paire	36-12	Paire	78-12
	Limite	19 dB	Limite	19 dB	Limite	56.90 dB	Limite	34.20 dB
	Freq.	17.95 MHz	Freq.	4.90 MHz	Freq.	1.90 MHz	Freq.	20.95 MHz
	✓	1.90 dB			✓	18.90 dB	✓	20.60 dB
	Paire	12			Paire	12	Paire	12
	Limite	3.20 dB			Limite	53.90 dB	Limite	31.20 dB
	Freq.	2.65 MHz			Freq.	1.90 MHz	Freq.	20.95 MHz

Localisateur NEXT MAITRE : N/A
Localisateur NEXT RECEPTEUR : N/A
Localisateur RL MAITRE : N/A
Localisateur RL RECEPTEUR : N/A

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 7

Figure 12: Certification 5ième prise

TREND AnyWARE® Cloud

Rapport de Certification

ID du test: DRSI PRISE 52
Date/Heure: 14/02/2025 13:45
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 5E STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

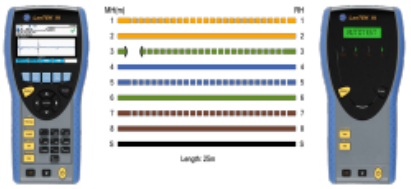
Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	N/A	N/A	N/A
Retard	N/A	N/A	N/A
Skew	N/A	N/A	N/A
Imp.	N/A	N/A	N/A
Résistance	N/A	N/A	N/A
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	N/A	N/A	N/A	N/A
PSNEXT	N/A	N/A	N/A	N/A
RL	N/A	N/A	N/A	N/A
IL	N/A	N/A	N/A	--



Boîtier Maître | **Boîtier Récepteur** | **Boîtier Maître** | **Boîtier Récepteur**

NEXT (dB)

	Marge	Valeur
NEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSNEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

NEXT (dB)

	Marge	Valeur
NEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSNEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-F (dB)

	Marge	Valeur
ACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-F (dB)

	Marge	Valeur
ACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

RL (dB)

	Marge	Valeur
RL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

RL (dB)

	Marge	Valeur
RL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-N (dB)

	Marge	Valeur
ACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-N (dB)

	Marge	Valeur
ACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

	Marge	Valeur
IL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

Localisateur NEXT MAITRE
N/A

Localisateur NEXT RECEPTEUR
N/A

Localisateur RL MAITRE
N/A

Localisateur RL RECEPTEUR
N/A

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 8

Figure 13: Certification 6ième prise

Université de Lomé

TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: DRSI PRISE 53
Date/Heure: 14/02/2025 13:43
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 5E STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

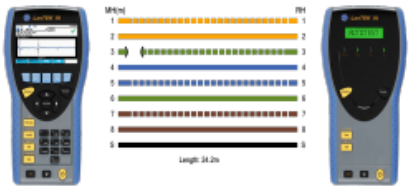
Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	N/A	N/A	N/A
Retard	N/A	N/A	N/A
Skew	N/A	N/A	N/A
Imp.	N/A	N/A	N/A
Résistance	N/A	N/A	N/A
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	N/A	N/A	N/A	N/A
PSNEXT	N/A	N/A	N/A	N/A
RL	N/A	N/A	N/A	N/A
IL	N/A	N/A	N/A	--



Boîtier Maître

NEXT (dB)

	Marge	Valeur
NEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSNEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

Boîtier Récepteur

NEXT (dB)

	Marge	Valeur
NEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSNEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

Boîtier Maître

ACR-F (dB)

	Marge	Valeur
ACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

Boîtier Récepteur

ACR-F (dB)

	Marge	Valeur
ACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

RL (dB)

	Marge	Valeur
RL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

RL (dB)

	Marge	Valeur
RL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-N (dB)

	Marge	Valeur
ACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-N (dB)

	Marge	Valeur
ACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

	Marge	Valeur
IL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

Localisateur NEXT MAITRE
N/A

Localisateur NEXT RECEPTEUR
N/A

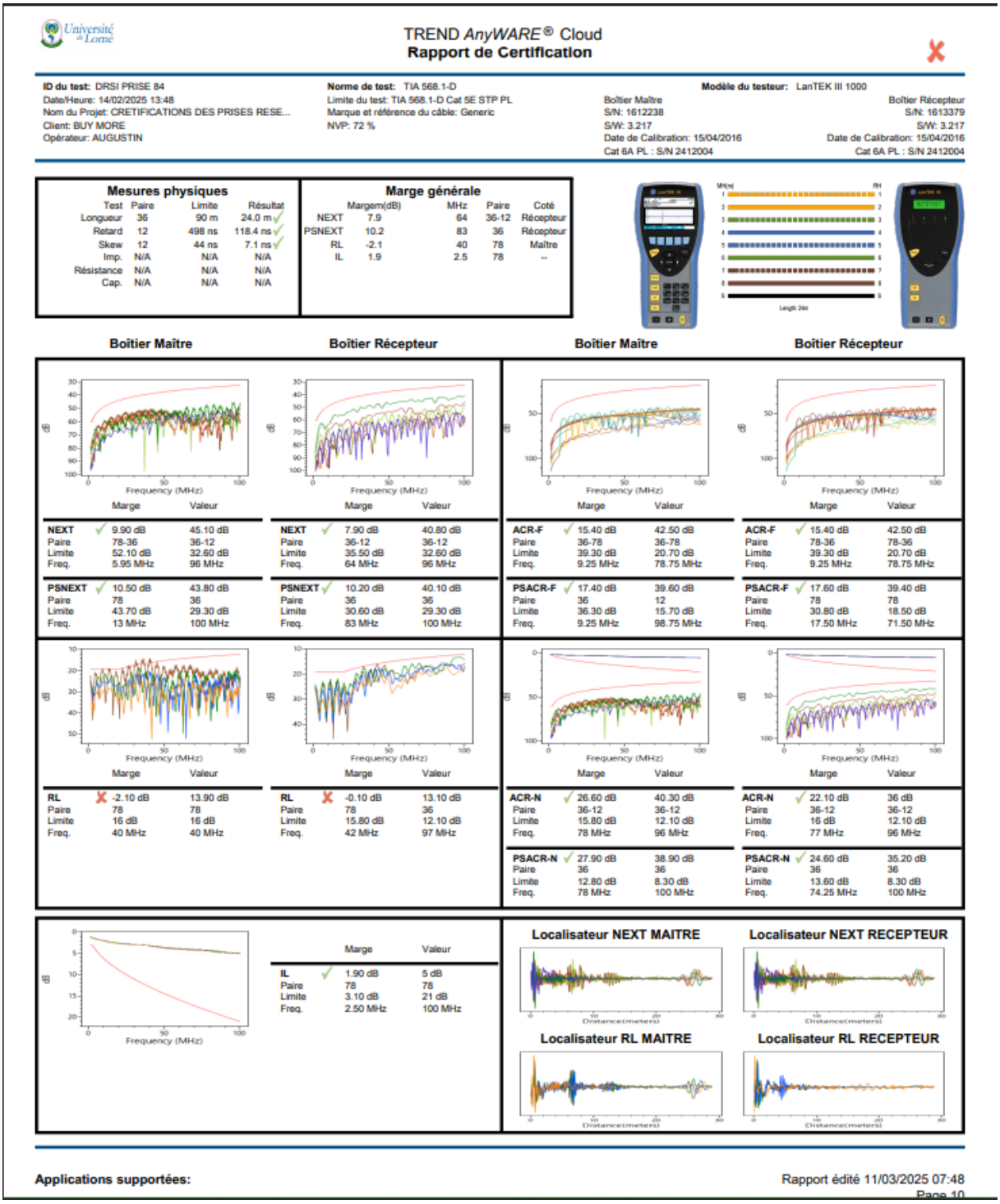
Localisateur RL MAITRE
N/A

Localisateur RL RECEPTEUR
N/A

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 9

Figure 14: Certification 7ième prise



TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: DRSI PRISE 84
Date/Heure: 14/02/2025 13:48
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 5E STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	36	90 m	24.0 m ✓
Retard	12	498 ns	118.4 ns ✓
Skew	12	44 ns	7.1 ns ✓
Imp.	N/A	N/A	N/A
Résistance	N/A	N/A	N/A
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	7.9	64	36-12	Récepteur
PSNEXT	10.2	83	36	Récepteur
RL	-2.1	40	78	Maître
IL	1.9	2.5	78	--

Boîtier Maître — **Boîtier Récepteur** — **Boîtier Maître** — **Boîtier Récepteur**

Frequency (MHz)

	Marge	Valeur	Marge	Valeur	Marge	Valeur	Marge	Valeur
NEXT	✓ 9.90 dB	45.10 dB	✓ 7.90 dB	40.80 dB	**ACR-F** ✓ 15.40 dB	42.50 dB	✓ 15.40 dB	42.50 dB
Paire	78-36	36-12	36-12	36-12	Paire 36-78	36-78	78-36	78-36
Limite	52.10 dB	32.60 dB	35.50 dB	32.60 dB	Limite 39.30 dB	20.70 dB	39.30 dB	20.70 dB
Freq.	5.95 MHz	96 MHz	64 MHz	96 MHz	Freq. 9.25 MHz	78.75 MHz	9.25 MHz	78.75 MHz
PSNEXT ✓	10.50 dB	43.80 dB	✓ 10.20 dB	40.10 dB	**PSACR-F** ✓ 17.40 dB	39.60 dB	✓ 17.60 dB	39.40 dB
Paire	78	36	36	36	Paire 36	12	78	78
Limite	43.70 dB	29.30 dB	30.60 dB	29.30 dB	Limite 36.30 dB	15.70 dB	30.80 dB	18.50 dB
Freq.	13 MHz	100 MHz	83 MHz	100 MHz	Freq. 9.25 MHz	98.75 MHz	17.50 MHz	71.50 MHz
RL ✗	-2.10 dB	13.90 dB	✗ -0.10 dB	13.10 dB	**ACR-N** ✓ 26.60 dB	40.30 dB	✓ 22.10 dB	36 dB
Paire	78	78	78	36	Paire 36-12	36-12	36-12	36-12
Limite	16 dB	16 dB	15.80 dB	12.10 dB	Limite 15.80 dB	12.10 dB	16 dB	12.10 dB
Freq.	40 MHz	40 MHz	42 MHz	97 MHz	Freq. 78 MHz	96 MHz	77 MHz	96 MHz
					PSACR-N ✓ 27.90 dB	38.90 dB	✓ 24.60 dB	35.20 dB
					Paire 36	36	36	36
					Limite 12.80 dB	8.30 dB	13.60 dB	8.30 dB
					Freq. 78 MHz	100 MHz	74.25 MHz	100 MHz

	Marge	Valeur
IL	✓ 1.90 dB	5 dB
Paire	78	78
Limite	3.10 dB	21 dB
Freq.	2.50 MHz	100 MHz

Localisateur NEXT MAITRE — **Localisateur NEXT RECEPTEUR**

Localisateur RL MAITRE — **Localisateur RL RECEPTEUR**

Distance(meters)

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 10

Figure 15: Certification 8ième prise

Université de Lomé

TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: FDS PRISE I12
Date/Heure: 10/03/2025 17:01
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 6 STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

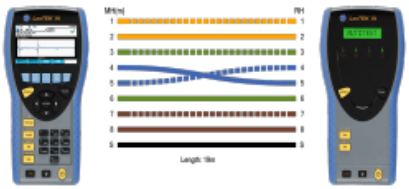
Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	N/A	N/A	N/A
Retard	N/A	N/A	N/A
Skew	N/A	N/A	N/A
Imp.	N/A	N/A	N/A
Résistance	N/A	N/A	N/A
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	N/A	N/A	N/A	N/A
PSNEXT	N/A	N/A	N/A	N/A
RL	N/A	N/A	N/A	N/A
IL	N/A	N/A	N/A	--



Boîtier Maître — **Boîtier Récepteur** — **Boîtier Maître** — **Boîtier Récepteur**

NEXT (dB)

	Marge	Valeur
NEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSNEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

NEXT (dB)

	Marge	Valeur
NEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSNEXT	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-F (dB)

	Marge	Valeur
ACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-F (dB)

	Marge	Valeur
ACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-F	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

RL (dB)

	Marge	Valeur
RL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

RL (dB)

	Marge	Valeur
RL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-N (dB)

	Marge	Valeur
ACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

ACR-N (dB)

	Marge	Valeur
ACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A
PSACR-N	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

	Marge	Valeur
IL	N/A	N/A
Paire	N/A	N/A
Limite	N/A	N/A
Freq.	N/A	N/A

Localisateur NEXT MAITRE
N/A

Localisateur NEXT RECEPTEUR
N/A

Localisateur RL MAITRE
N/A

Localisateur RL RECEPTEUR
N/A

Applications supportées:

Rapport édité 11/03/2025 07:48

Figure 16: Certification 9ième prise

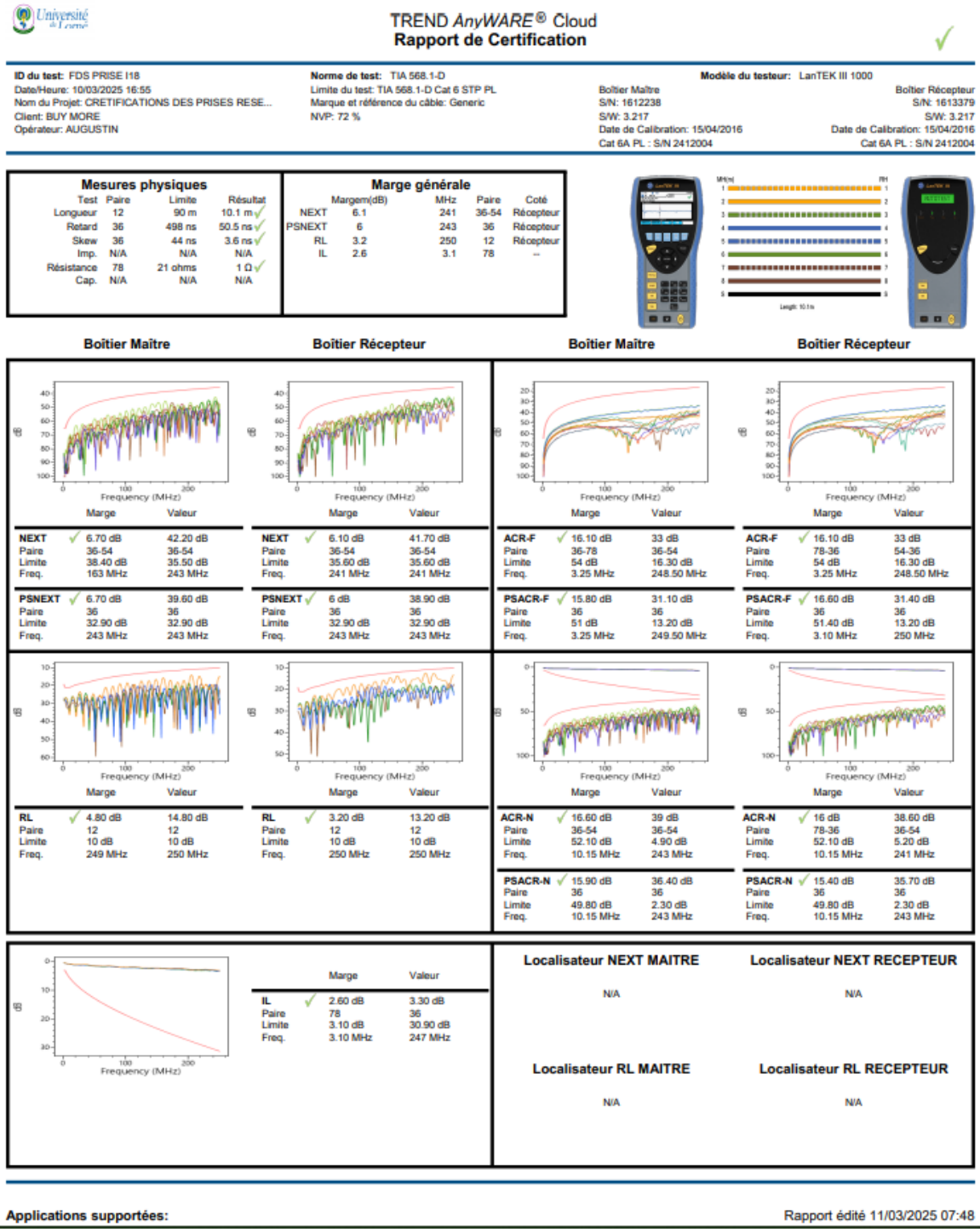
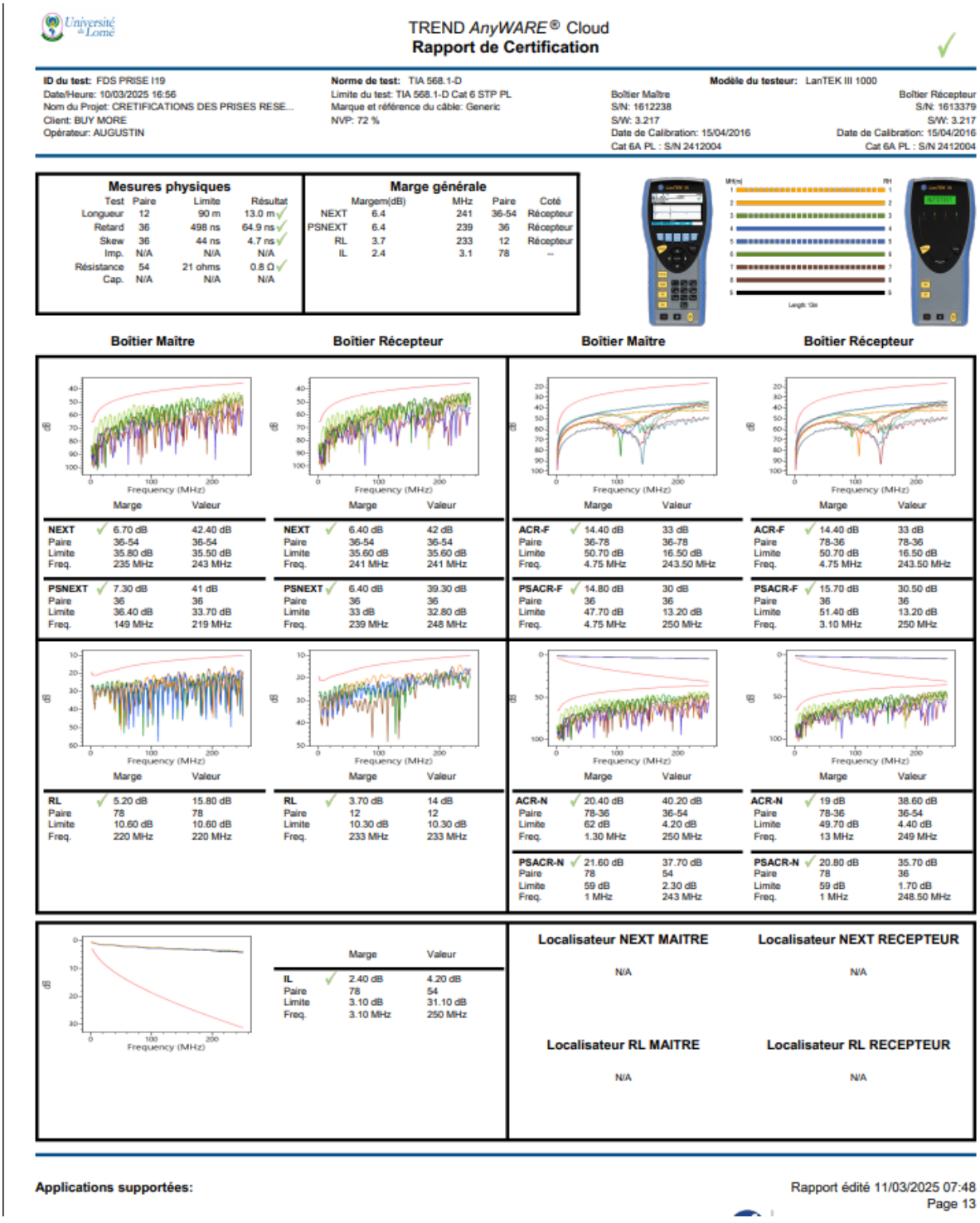


Figure 17: Certification 10ième prise



TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: FDS PRISE I19
Date/Heure: 10/03/2025 16:56
Nom du Projet: CRETIFICATIONS DES PRISES RESE...
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.1-D
Limite du test: TIA 568.1-D Cat 6 STP PL
Marque et référence du câble: Generic
NVP: 72 %

Modèle du testeur: LanTEK III 1000

Boîtier Maître
S/N: 1612238
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Boîtier Récepteur
S/N: 1613379
S/W: 3.217
Date de Calibration: 15/04/2016
Cat 6A PL : S/N 2412004

Mesures physiques

Test	Paire	Limite	Résultat
Longueur	12	90 m	13.0 m ✓
Retard	36	498 ns	64.9 ns ✓
Skew	36	44 ns	4.7 ns ✓
Imp.	N/A	N/A	N/A
Résistance	54	21 ohms	0.8 Ω ✓
Cap.	N/A	N/A	N/A

Marge générale

	Margem(dB)	MHz	Paire	Coté
NEXT	6.4	241	36-54	Récepteur
PSNEXT	6.4	239	36	Récepteur
RL	3.7	233	12	Récepteur
IL	2.4	3.1	78	--

Boîtier Maître

	Marge	Valeur
NEXT ✓	6.70 dB	42.40 dB
Paire	36-54	36-54
Limite	35.80 dB	35.50 dB
Freq.	235 MHz	243 MHz
PSNEXT ✓	7.30 dB	41 dB
Paire	36	36
Limite	36.40 dB	33.70 dB
Freq.	149 MHz	219 MHz

Boîtier Récepteur

	Marge	Valeur
NEXT ✓	6.40 dB	42 dB
Paire	36-54	36-54
Limite	35.60 dB	35.60 dB
Freq.	241 MHz	241 MHz
PSNEXT ✓	6.40 dB	39.30 dB
Paire	36	36
Limite	33 dB	32.80 dB
Freq.	239 MHz	248 MHz

Boîtier Maître

	Marge	Valeur
ACR-F ✓	14.40 dB	33 dB
Paire	36-78	36-78
Limite	50.70 dB	16.50 dB
Freq.	4.75 MHz	243.50 MHz
PSACR-F ✓	14.80 dB	30 dB
Paire	36	36
Limite	47.70 dB	13.20 dB
Freq.	4.75 MHz	250 MHz

Boîtier Récepteur

	Marge	Valeur
ACR-F ✓	14.40 dB	33 dB
Paire	78-36	78-36
Limite	50.70 dB	16.50 dB
Freq.	4.75 MHz	243.50 MHz
PSACR-F ✓	15.70 dB	30.50 dB
Paire	36	36
Limite	51.40 dB	13.20 dB
Freq.	3.10 MHz	250 MHz

Boîtier Maître

	Marge	Valeur
RL ✓	5.20 dB	15.80 dB
Paire	78	78
Limite	10.60 dB	10.60 dB
Freq.	220 MHz	220 MHz

Boîtier Récepteur

	Marge	Valeur
RL ✓	3.70 dB	14 dB
Paire	12	12
Limite	10.30 dB	10.30 dB
Freq.	233 MHz	233 MHz

Boîtier Maître

	Marge	Valeur
ACR-N ✓	20.40 dB	40.20 dB
Paire	78-36	36-54
Limite	62 dB	4.20 dB
Freq.	1.30 MHz	250 MHz
PSACR-N ✓	21.60 dB	37.70 dB
Paire	78	54
Limite	59 dB	2.30 dB
Freq.	1 MHz	243 MHz

Boîtier Récepteur

	Marge	Valeur
ACR-N ✓	19 dB	38.60 dB
Paire	78-36	36-54
Limite	49.70 dB	4.40 dB
Freq.	13 MHz	249 MHz
PSACR-N ✓	20.80 dB	35.70 dB
Paire	78	36
Limite	59 dB	1.70 dB
Freq.	1 MHz	248.50 MHz

	Marge	Valeur
IL ✓	2.40 dB	4.20 dB
Paire	78	54
Limite	3.10 dB	31.10 dB
Freq.	3.10 MHz	250 MHz

Localisateur NEXT MAITRE
N/A

Localisateur NEXT RECEPTEUR
N/A

Localisateur RL MAITRE
N/A

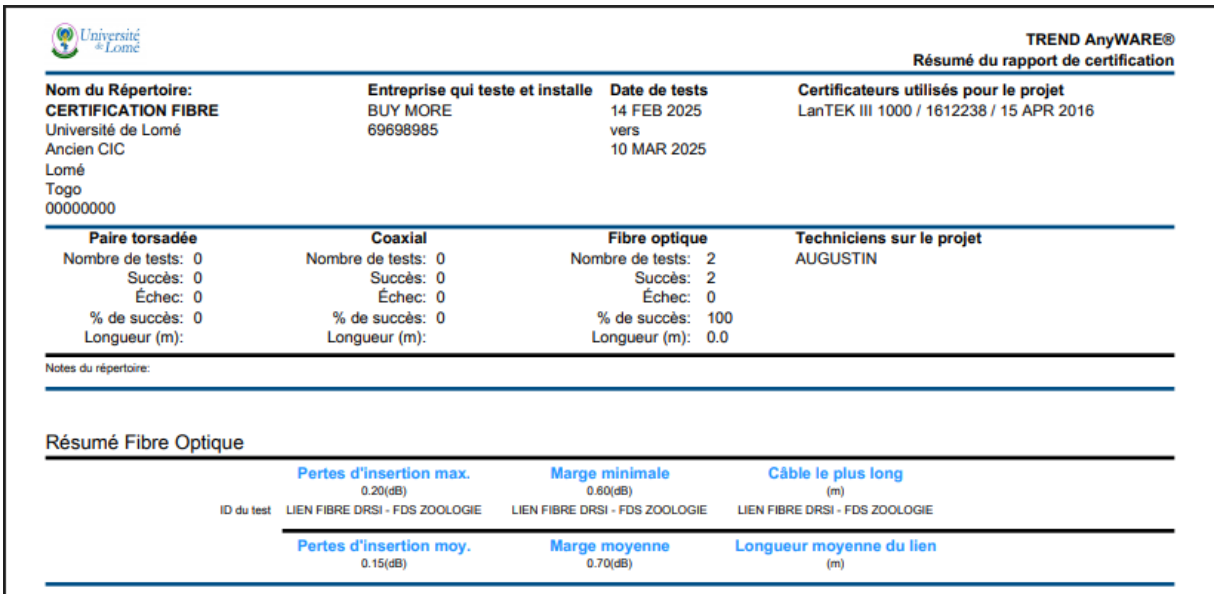
Localisateur RL RECEPTEUR
N/A

Applications supportées:

Rapport édité 11/03/2025 07:48
Page 13

Figure 18: Certification 11ième prise

5.4.2 Certification de la fibre optique



Université de Lomé

TREND AnyWARE®
Résumé du rapport de certification

Nom du Répertoire:	Entreprise qui teste et installe	Date de tests	Certificateurs utilisés pour le projet
CERTIFICATION FIBRE Université de Lomé Ancien CIC Lomé Togo 00000000	BUY MORE 69698985	14 FEB 2025 vers 10 MAR 2025	LanTEK III 1000 / 1612238 / 15 APR 2016

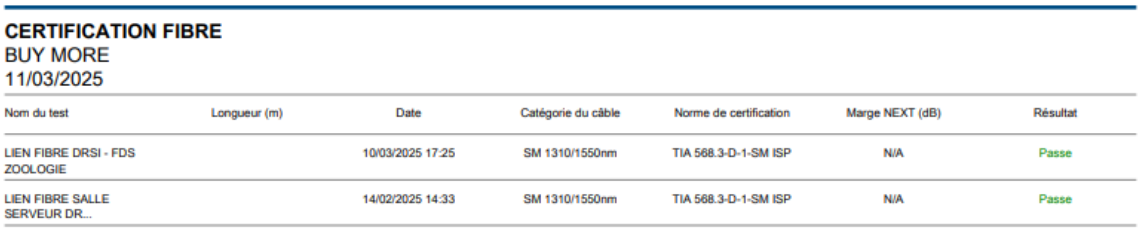
Paire torsadée	Coaxial	Fibre optique	Techniciens sur le projet
Nombre de tests: 0	Nombre de tests: 0	Nombre de tests: 2	AUGUSTIN
Succès: 0	Succès: 0	Succès: 2	
Échec: 0	Échec: 0	Échec: 0	
% de succès: 0	% de succès: 0	% de succès: 100	
Longueur (m):	Longueur (m):	Longueur (m): 0.0	

Notes du répertoire:

Résumé Fibre Optique

	Pertes d'insertion max. 0.20(dB)	Marge minimale 0.60(dB)	Câble le plus long (m)
ID du test	LIEN FIBRE DRSI - FDS ZOOLOGIE	LIEN FIBRE DRSI - FDS ZOOLOGIE	LIEN FIBRE DRSI - FDS ZOOLOGIE
	Pertes d'insertion moy. 0.15(dB)	**Marge moyenne** 0.70(dB)	**Longueur moyenne du lien** (m)

Figure 19: Résumé de la certification de la fibre optique



CERTIFICATION FIBRE
BUY MORE
11/03/2025

Nom du test	Longueur (m)	Date	Catégorie du câble	Norme de certification	Marge NEXT (dB)	Résultat
LIEN FIBRE DRSI - FDS ZOOLOGIE		10/03/2025 17:25	SM 1310/1550nm	TIA 568.3-D-1-SM ISP	N/A	Passe
LIEN FIBRE SALLE SERVEUR DR...		14/02/2025 14:33	SM 1310/1550nm	TIA 568.3-D-1-SM ISP	N/A	Passe

Figure 20: Résumé de la certification de la fibre optique

TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: LIEN FIBRE DRSI - FDS ZOOLOGIE
Date/Heure: 10/03/2025 17:25
Nom du Projet: CERTIFICATION FIBRE
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.3-D-1-SM ISP
Limite du test:
Type de Test: Fiber Autotest
Type de Fibre:
Marque et référence du câble:
Connecteur maître:
Connecteur récepteur:

Modèle du testeur: LanTEK IV / FiberTEK IV OLTS

Boîtier Maître	Boîtier Récepteur
S/N: 1612238	S/N: 1613379
S/W: 3.217	S/W: 3.217
Date de Calibration: 15/04/2016	Date de Calibration: 15/04/2016
SM Fiber : S/N 2324017	SM Fiber : S/N 2324017

Informations sur le test

Type de Test	Fiber Autotest
Configuration	2-Ended
Type de Référence	3 Jumper
Classe jarretière	N/A

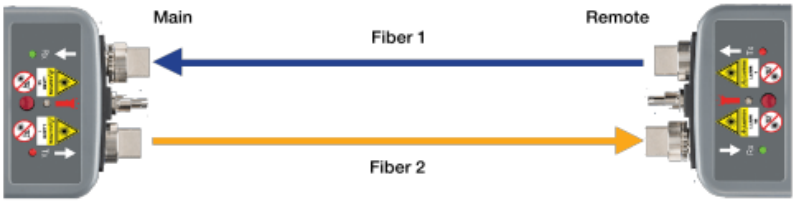
Marge

Fibre #	Marge	Longueur d'onde
Fiber 1 :	0.80 dB	1550 nm
Fiber 2 :	0.60 dB	1550 nm

Longueur

IR	Limite	Résultat
N/A	40000 m	0.0 m ✓

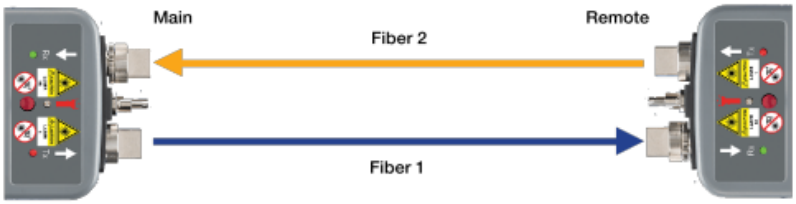
Normal en bidirectionnel - ÉTAPE 1



Test 1

Fibre Nombre	Test Direction	Longueur d'onde (nm)	Perte d'insertion (dB)	Budget de perte/Limite (dB)	Marge (dB)	Résultat
Fibre 1	Boîtier récepteur vers maître	1310.00	0.00	5.00	5.00	✓
Fibre 1	Boîtier récepteur vers maître	1550.00	0.00	0.80	0.80	✓
Fibre 2	Boîtier maître vers récepteur	1310.00	0.00	5.00	5.00	✓
Fibre 2	Boîtier maître vers récepteur	1550.00	0.00	0.80	0.80	✓

Normal en bidirectionnel - ÉTAPE 2



Test 2

Fibre Nombre	Test Direction	Longueur d'onde (nm)	Perte d'insertion (dB)	Budget de perte/Limite (dB)	Marge (dB)	Résultat
Fibre 1	Boîtier maître vers récepteur	1310.00	0.00	5.00	5.00	✓
Fibre 1	Boîtier maître vers récepteur	1550.00	0.20	0.80	0.60	✓
Fibre 2	Boîtier récepteur vers maître	1310.00	-0.10	5.00	5.10	✓
Fibre 2	Boîtier récepteur vers maître	1550.00	0.00	0.80	0.80	✓

Applications supportées:
16G Fibre Channel 1600-SM-LC-L,1G Fibre Channel 100-SM-LC-L,2G Fibre Channel 200-SM-LC-L,4G Fibre Channel 400-SM-LC-L,4G Fibre Channel 400-SM-LC-M,8G Fibre Channel 800-SM-LC-I,8G Fibre Channel 800-SM-LC-L,10G Fibre Channel 1200-SM-LL-L,Ethernet 100GBASE-LR4,Ethernet 10GBASE-E,Ethernet

Rapport édité 11/03/2025 07:35
Page 3
TREND NETWORKS

Figure 21: Certification 1ière fibre

Université de Lomé

TREND *AnyWARE*® Cloud
Rapport de Certification

ID du test: LIEN FIBRE SALLE SERVEUR DRSI RDC - SALL...
Date/Heure: 14/02/2025 14:33
Nom du Projet: CERTIFICATION FIBRE
Client: BUY MORE
Opérateur: AUGUSTIN

Norme de test: TIA 568.3-D-1-SM ISP
Limite du test:
Type de Test: Fiber Autotest
Type de Fibre:
Marque et référence du câble:
Connecteur maître:
Connecteur récepteur:

Modèle du testeur: LanTEK IV / FiberTEK IV OLTS

Boîtier Maître	Boîtier Récepteur
S/N: 1612238	S/N: 1613379
S/W: 3.217	S/W: 3.217
Date de Calibration: 15/04/2016	Date de Calibration: 15/04/2016
SM Fiber : S/N 2324017	SM Fiber : S/N 2324017

Informations sur le test

Type de Test	Fiber Autotest
Configuration	2-Ended
Type de Référence	3 Jumper
Classe jarretière	N/A

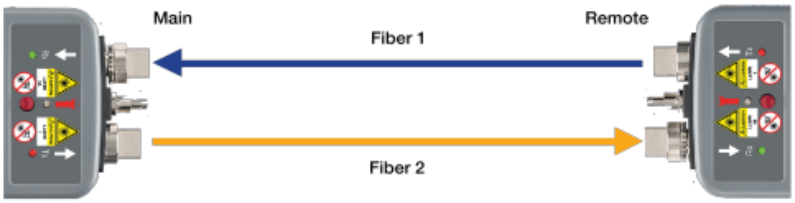
Marge

Fibre #	Marge	Longueur d'onde
Fiber 1 :	0.80 dB	1550 nm
Fiber 2 :	0.80 dB	1550 nm

Longueur

IR	Limite	Résultat
N/A	40000 m	0.0 m ✓

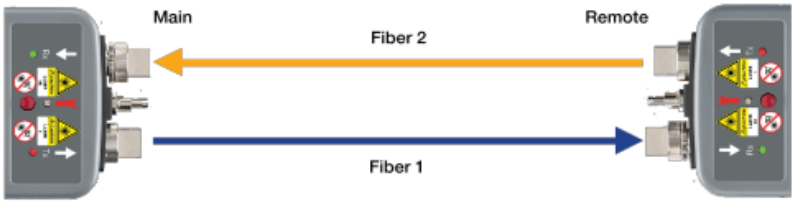
Normal en bidirectionnel - ÉTAPE 1



Test 1

Fibre Nombre	Test Direction	Longueur d'onde (nm)	Perte d'insertion (dB)	Budget de perte/Limite (dB)	Marge (dB)	Résultat
Fibre 1	Boîtier récepteur vers maître	1310.00	0.00	5.00	5.00	✓
Fibre 1	Boîtier récepteur vers maître	1550.00	0.00	0.80	0.80	✓
Fibre 2	Boîtier maître vers récepteur	1310.00	0.00	5.00	5.00	✓
Fibre 2	Boîtier maître vers récepteur	1550.00	0.00	0.80	0.80	✓

Normal en bidirectionnel - ÉTAPE 2



Test 2

Fibre Nombre	Test Direction	Longueur d'onde (nm)	Perte d'insertion (dB)	Budget de perte/Limite (dB)	Marge (dB)	Résultat
Fibre 1	Boîtier maître vers récepteur	1310.00	0.00	5.00	5.00	✓
Fibre 1	Boîtier maître vers récepteur	1550.00	0.00	0.80	0.80	✓
Fibre 2	Boîtier récepteur vers maître	1310.00	0.10	5.00	4.90	✓
Fibre 2	Boîtier récepteur vers maître	1550.00	0.00	0.80	0.80	✓

Applications supportées:

Rapport édité 11/03/2025 07:35

Figure 22: Certification 2ième fibre

6. ANALYSES DES ECARTS ET PROBLEMES PERSISTANTS

Au cours de nos différents interviews avec les membres du SI, nous notons de nombreux efforts effectués pour renforcer la résilience du SI de l'université de Lomé depuis l'audit initial, en revanche certaines recommandations sont en cours d'étude et d'autres reste non prise en compte jusqu'à ce jour.

6.1 Organigramme recommandé

Le nouvel organigramme recommandé pour l'Université de Lomé n'a pas encore été mis en œuvre. Cette absence de structuration formelle peut engendrer des lacunes dans la gouvernance du Système d'Information, notamment en ce qui concerne la répartition des responsabilités, la gestion des risques et la prise de décision. La mise en place de cet organigramme reste essentielle pour améliorer l'efficacité opérationnelle et assurer une meilleure coordination des actions liées à la sécurité et à l'administration du SI.

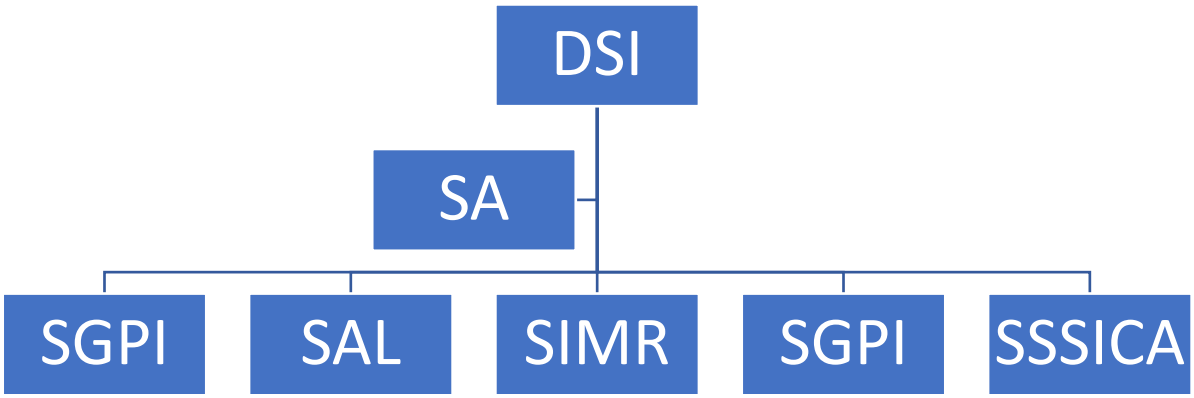


Figure 23: Organigramme cible issue de l'audit initial

L'architecture cible proposée, basée sur un modèle à trois niveaux, est en cours de déploiement. Elle repose sur :

- Un cœur de réseau ;
- Une couche de distribution ;
- Une couche d'accès.

Cependant, une lacune majeure a été identifiée : l'absence de redondance au niveau des équipements actifs, tant au cœur qu'à la distribution du réseau de l'Université de Lomé.

Actuellement, le cœur du réseau est basé sur un switch Cisco 3850, ce qui représente un Single Point of Failure (SPOF). De même que la partie Edge. En d'autres termes, toute panne de cet équipement entraînerait une interruption totale des services réseau, affectant ainsi la disponibilité et la résilience du système d'information.

Afin d'améliorer la fiabilité et la continuité du service, il est essentiel d'ajouter une redondance au cœur et à la distribution du réseau, notamment par :

- La mise en place de switches redondants en haute disponibilité (HA).
- L'utilisation de protocoles de redondance tels que HSRP, VRRP ou GLBP pour assurer un basculement automatique en cas de défaillance.

Cela permettrait d'améliorer la tolérance aux pannes, d'augmenter la disponibilité du réseau et d'assurer une meilleure continuité des services critiques de l'université.

En plus de l'absence de redondance au niveau du cœur et de la distribution du réseau, il est également à noter que :

- Certains équipements obsolètes ou non conformes sont toujours présents dans l'infrastructure, ce qui peut entraîner des problèmes de compatibilité, de performance et de sécurité.
- L'uniformisation des équipements actifs n'a pas été réalisée, avec la coexistence de matériels de différents fournisseurs, ce qui peut compliquer l'administration du réseau, la maintenance et le support technique.

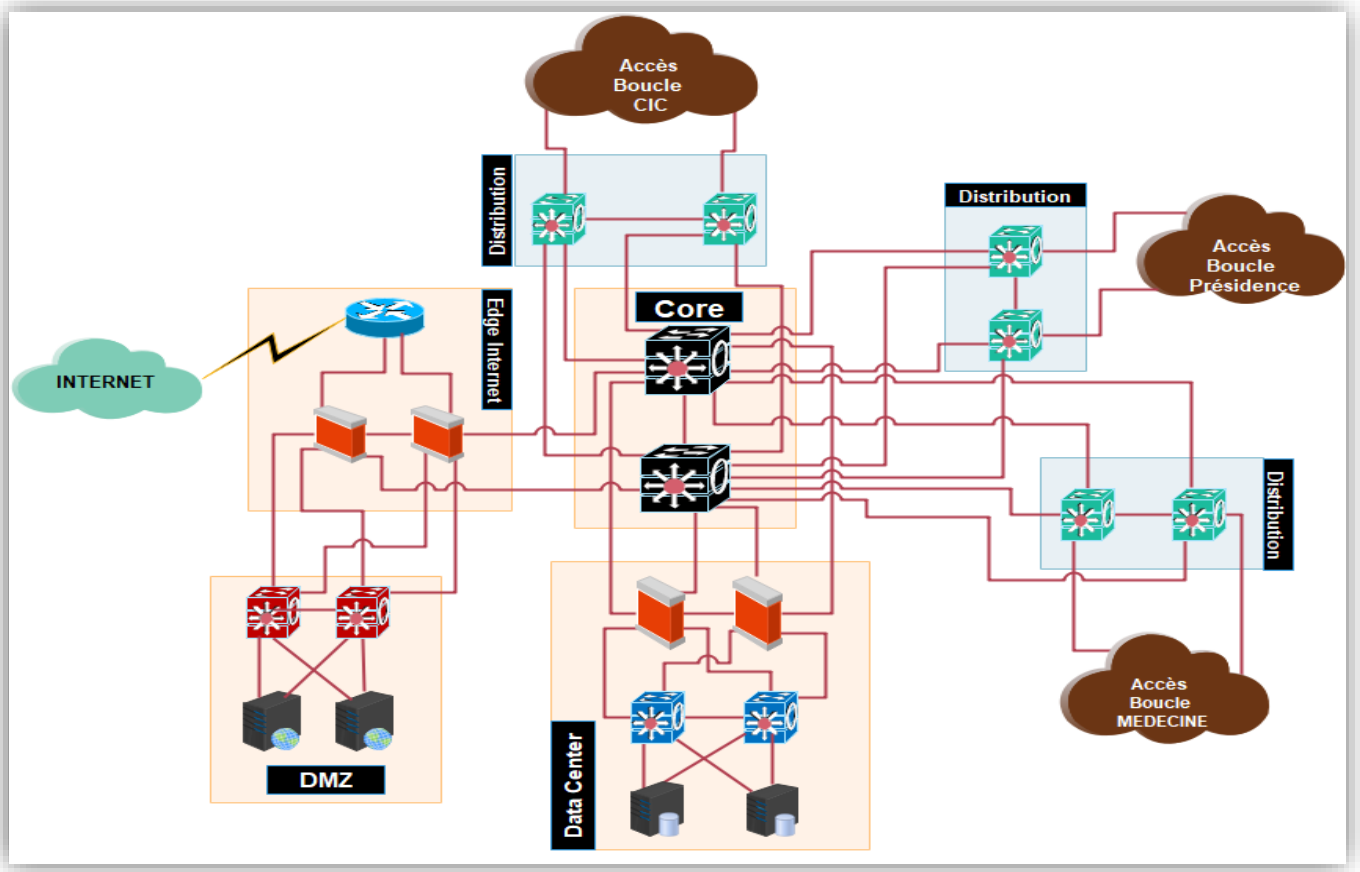


Figure 24: Architecture cible issue de l'audit initial

6.3 Réseau WIFI

L'audit initial a révélé plusieurs problèmes persistants liés au réseau Wi-Fi de l'Université de Lomé, notamment :

- Mauvaise gestion de la bande passante, entraînant une saturation du réseau et une dégradation des performances.
- Absence de filtrage d'accès, augmentant les risques de congestion et de failles de sécurité.
- Manque de contrôle et d'uniformisation des points d'accès Wi-Fi, compliquant l'administration et la maintenance du réseau.

Pour répondre à ces lacunes, il avait été recommandé la mise en place d'une solution Wi-Fi unifiée, permettant d'optimiser la gestion de la bande passante, de sécuriser et de filtrer les accès, ce qui n'a pas encore été mise en œuvre.

Les bénéfices de la mise en place d'une telle solution sont entre autres :

- L'Amélioration de la qualité et de la stabilité de la connexion.
- Le Renforcement de la sécurité du réseau Wi-Fi.
- La Gestion optimisée des utilisateurs et des équipements.

La mise en place d'un Wi-Fi unifié est essentielle pour garantir une connectivité fiable et sécurisée sur l'ensemble du campus universitaire.

6.4 Gestion du temps du personnel de l'UL

L'audit a révélé que les recommandations visant à améliorer la gestion du temps, notamment par :

- La mise en place d'un système de communication téléphonique performant
- L'implantation d'un call center dédié

n'ont pas été mises en œuvre.

Les conséquences identifiées de cette non-Implémentation sont

- Manque d'efficacité dans la communication interne et externe, ce qui ralentit la transmission des informations et la prise de décision.

- Absence d'un canal structuré pour le support et l'assistance, augmentant les risques d'insatisfaction et d'inefficacité dans le traitement des préoccupations.

Il est essentiel d'accélérer la mise en place des solutions recommandées afin d'optimiser la gestion du temps et la communication par :

- La Mise en place d'un IPBX (système de téléphonie IP) pour gérer les appels internes et externes de manière centralisée.
- Mise en place d'un Call Center

La mise en place de ces solutions permettra d'améliorer la fluidité des échanges, de renforcer l'expérience utilisateur et d'accroître la productivité au sein de l'Université de Lomé.

6.5 Audit de la sécurité

L'audit de la sécurité d'un système d'information vise à évaluer les dispositifs en place pour protéger les données, les infrastructures et les utilisateurs contre les menaces internes et externes. Son objectif premier est d'identifier les vulnérabilités du système d'information.

Lors du dernier audit, il était possible de pouvoir depuis un quelconque réseau utilisateur faire un test de scan vers les autres réseaux. Aujourd'hui ceci n'est plus possible avec la segmentation et la mise des politiques de filtrages sur le pare-feu WAN de l'université de Lomé (Cisco ASA).

Pour procéder au scan du réseau de l'université de Lomé, le poste ayant servi pour le scan a été placé sur le réseau des serveurs de la DMZ. Ceci pose un risque majeur car un attaquant ayant compromis un serveur de la DMZ pourra facilement effectuer des mouvements latéraux pour infecter d'autres hôtes dans le LAN ou exfiltrer les données.

Adressage du poste sur le réseau des serveurs ayant servi pour le scan

```
Carte Ethernet Ethernet 4 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Realtek USB FE Family Controller
   Adresse physique . . . . . . . . . . . : 00-E0-4C-36-0E-37
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::e8ed:93ad:1211:3488%8(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.20.1.57(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.20.1.1
   IAID DHCPv6 . . . . . . . . . . . : 1006690380
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2F-3D-32-EB-4C-EB-BD-7E-1F-FB
   Serveurs DNS. . .  . . . . . . . . . . : 172.20.1.2
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Figure 25: Adressage du PC ayant servi pour les scans

6.5.1 Scan Interne

Le scan interne a été effectué sur les adresses IP suivantes du réseau de l'UL :

RESEAUX MANAGEMENT			
Equipements	***Adresse réseau***	***Masque réseau***	***Commentaires***
Serveurs	172.20.0.0	255.255.0.0	DMZ
Switches	192.168.254.0	255.255.255.0	

Tableau 15: Réseaux Management scannés

RESEAUX UTILISATEURS			
Départements	***Adresse réseau***	***Masque réseau***	***Commentaires***
IT	192.168.210.0	255.255.255.0	Sous-réseaux de la DRSI
FDS	192.168.216.0	255.255.255.0	Sous-réseaux de la FDS
ESA	192.168.224.0	255.255.255.0	Sous-réseaux de l'ESA
FSS	192.168.150.0	255.255.255.0	Sous-réseaux de la FSS
ENSI/EPL	192.168.223.0	255.255.255.0	Sous-réseaux de l'EPL
FASEG/PRESIDENCE	192.168.228.0	255.255.255.0	Sous-réseaux de la FASEG/PRESIDENCE

Tableau 16: Réseaux Utilisateurs scanné

Quelques Résultats du scan sur la partie des serveurs

Résumé :

Host	High	Medium	Low	Log	False Positive
172.20.1.11	2	6	1	0	0
172.20.1.23	2	5	1	0	0
172.20.1.8	1	3	1	0	0
172.20.1.58	1	6	1	0	0
172.20.1.18	1	3	1	0	0
172.20.1.2	1	4	1	0	0
172.20.1.201	0	9	1	0	0
172.20.1.250	0	2	1	0	0
172.20.1.71	0	3	1	0	0
172.20.1.252	0	8	1	0	0
172.20.1.3	0	2	0	0	0
172.20.1.60	0	4	1	0	0
172.20.1.6	0	1	1	0	0
172.20.1.21	0	1	1	0	0
172.20.1.24 univ-lome.tg	0	2	1	0	0
172.20.1.9	0	2	1	0	0
172.20.1.55	0	2	1	0	0
172.20.1.57	0	1	0	0	0
172.20.1.4	0	5	1	0	0
172.20.1.253	0	1	0	0	0
172.20.1.35	0	0	1	0	0
172.20.1.160	0	0	1	0	0
172.20.1.56	0	0	1	0	0
172.20.1.10	0	0	1	0	0
172.20.1.41	0	0	1	0	0
172.20.1.42	0	0	1	0	0
172.20.1.14	0	0	1	0	0
172.20.1.15	0	0	1	0	0
172.20.1.7	0	0	1	0	0
172.20.1.153	0	0	1	0	0
Total: 30	8	70	27	0	0

Figure 26: Résumé du scan des serveurs

- ***Serveur 172.20.1.2***

Service (Port)	Threat Level
10000/tcp	High
10000/tcp	Medium
22/tcp	Medium
22/tcp	Low

Figure 27: Ports ouverts sur le serveur 172.20.1.2

High (CVSS: 7.5)
NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Solution:
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.
Please see the references for more resources supporting you with this task.

Figure 28: vulnérabilité 1 serveur 172.20.1.2

Medium (CVSS: 5.9)
NVT: SSL/TLS: Report Weak Cipher Suites

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

Solution:
Solution type: Mitigation

Figure 29: vulnérabilité 2 serveur 172.20.1.2

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Product detection result

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪-----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Figure 30: vulnérabilité 3 serveur 172.20.1.2

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The remote server's SSL/TLS certificate has already expired.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service expired on 2024-02-23 23:59:59.
Certificate details:

fingerprint (SHA-1)	025780AD3A22D0F12D4138F2522A8112E6B597BC
fingerprint (SHA-256)	309268CC450BDF9DCA94398785CBC36E80BAD68AEB085E5A9CA23ECCB7E12E80
issued by	CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB
public key algorithm	RSA
public key size (bits)	2048
serial	00B44852541D5894C30F67A24DD2C9DE07
signature algorithm	sha256WithRSAEncryption
subject	CN=*.univ-lome.tg
subject alternative names (SAN)	*.univ-lome.tg, univ-lome.tg
valid from	2023-01-23 00:00:00 UTC
valid until	2024-02-23 23:59:59 UTC

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Figure 31: vulnérabilité 4 serveur 172.20.1.2

❖ **Constats en rapport à l'audit initial**

- La vulnérabilité en rapport au service SNMP a été corrigée
- L'utilisation de faibles algorithmes de chiffrement n'a pas été mitigée
- Apparition d'une nouvelle vulnérabilité : Certificat TLS expiré

❖ ***Serveur 172.20.1.8***

Service (Port)	Threat Level
general/tcp	High
22/tcp	Medium
80/tcp	Medium
22/tcp	Low

Figure 32: Ports ouverts sur le serveur 172.20.1.8

High (CVSS: 10.0)
NVT: Operating System (OS) End of Life (EOL) Detection

Product detection result

```
cpe:/o:centos:centos:7
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0
↪.105937)
```

Summary

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The "CentOS" Operating System on the remote host has reached the end of life.
CPE:                cpe:/o:centos:centos:7
Installed version,
build or SP:        7
EOL date:           2024-06-30
EOL info:           http://wiki.centos.org/Download
```

Impact

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

Solution type: Mitigation

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Figure 33: vulnérabilité 1 serveur 172.20.1.8

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                      | Reason
-----------------------------------------------------------------------------
↪----------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group
↪) and SHA-1
```

Impact

An attacker can quickly break individual connections.

Solution:

Solution type: Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Figure 34: vulnérabilité 2 serveur 172.20.1.8

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc

cast128-cbc

Solution:
Solution type: Mitigation

Figure 35: vulnérabilité 3 serveur 172.20.1.8

Medium (CVSS: 5.8) NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled
Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.
Quality of Detection (QoD): 99%
Vulnerability Detection Result `The web server has the following HTTP methods enabled: TRACE`
Impact An attacker may use this flaw to trick your legitimate web users to give him their credentials.
Solution: **Solution type:** Mitigation Disable the TRACE and TRACK methods in your web server configuration. Please see the manual of your web server or the references for more information.

Figure 36: vulnérabilité 4 serveur 172.20.1.8

- **Constats en rapport à l'audit initial**
  - La vulnérabilité HTTP TRACE affectant le service http n'a pas été corrigé
  - L'utilisation de faibles algorithmes de chiffrement n'a pas été mitigée

- ***Serveur 172.20.1.3***

Ports ouverts

Service (Port)	Threat Level
22/tcp	Medium

Figure 37: Ports ouverts sur le serveur 172.20.1.3

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary

The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                     | Reason
-------------------------------------------
diffie-hellman-group-exchange-sha1 | Using SHA-1
```

Impact

An attacker can quickly break individual connections.

Solution:

Solution type: Mitigation

Disable the reported weak KEX algorithm(s)

- 1024-bit MODP group / prime KEX algorithms:

Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Figure 38: vulnérabilité 1 sur le serveur 172.20.1.3

Medium (CVSS: 4.3)
NVT: Weak Encryption Algorithm(s) Supported (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)

Summary
The remote SSH server is configured to allow / support weak encryption algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server encryption al
↪gorithm(s):
aes128-cbc
aes256-cbc
The remote SSH server supports the following weak server-to-client encryption al
↪gorithm(s):
aes128-cbc
aes256-cbc

Solution:
Solution type: Mitigation
Disable the reported weak encryption algorithm(s).

Figure 39: vulnérabilité 2 sur le serveur 172.20.1.3

- **Constats en rapport à l'audit initial**
- L'utilisation de faibles algorithmes de chiffrement n'a pas été mitigée
- Vulnérabilité en rapport à la version du PHP sur le serveur a été corrigée

- ***Serveur 172.20.1.6 : elearn.univ-lome.tg***

Ports ouverts

Service (Port)	Threat Level
8181/tcp	Medium
22/tcp	Low

Figure 40: Ports ouverts sur le serveur 172.20.1.6

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

Summary
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The cookie(s):
Set-Cookie: MoodleSession=***replaced***; path=/; secure
is/are missing the "HttpOnly" cookie attribute.
```

Solution:
Solution type: Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

Figure 41: vulnérabilité 1 sur le serveur 172.20.1.6

Medium (CVSS: 5.0)
NVT: Source Control Management (SCM) Files/Folders Accessible (HTTP)

Summary
The script attempts to identify files/folders of a SCM accessible at the webserver.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following SCM files/folders were identified:
Match:      0000000000000000000000000000000000000000 c6e727732a7f3f1060b1c1fbd78
↪75746db5f1000 root <root@moniteur.univ-lome.tg> 1695925148 +0000
clone: from g
↪it://git.moodle.org/moodle.git
```

```
c6e727732a7f3f1060b1c1fbd7875746db5f1000 da9ebc40f66f3a4a44c3f888a0d8318ee86e172
↪a root <root@moniteur.univ-lome.tg> 1695925233 +0000 checkout: moving from mas
↪ter to MOODLE_402_STABLE
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        https://elearn.univ-lome.tg:8181/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
[branch "MOODLE_402_STABLE"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        https://elearn.univ-lome.tg:8181/.git/config
Match:      # git ls-files --others --exclude-from=.git/info/exclude
Used regex: ^# git ls-files
URL:        https://elearn.univ-lome.tg:8181/.git/info/exclude
Match:      DIRC
Used regex: ^DIRC
URL:        https://elearn.univ-lome.tg:8181/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        https://elearn.univ-lome.tg:8181/.git/description
Match:      ref: refs/heads/MOODLE_402_STABLE
Used regex: ^ref: refs/
URL:        https://elearn.univ-lome.tg:8181/.git/HEAD
```

Figure 42: Vulnérabilité 2 sur le serveur 172.20.1.6

❖ **Constats**

- Système vulnérable au SCM Files/Folders et attaques XSS

Quelques Résultats du scan sur la partie des switchs

❖ ***Switch 192.168.254.2***

Ports ouverts

Service (Port)	Threat Level
22/tcp	Medium
23/tcp	Medium
22/tcp	Low

Figure 43: Ports ouverts sur le switch 192.168.254.2

Medium (CVSS: 5.3)
NVT: Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary
The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak KEX algorithm(s):
KEX algorithm                     | Reason
-------------------------------------------
diffie-hellman-group-exchange-sha1 | Using SHA-1
```

Impact
An attacker can quickly break individual connections.

Solution:
Solution type: Mitigation
Disable the reported weak KEX algorithm(s)
- 1024-bit MODP group / prime KEX algorithms:
Alternatively use elliptic-curve Diffie-Hellmann in general, e.g. Curve 25519.

Figure 44: Vulnérabilité 1 sur le switch 192.168.254.2

Medium (CVSS: 4.8) NVT: Telnet Unencrypted Cleartext Login
Summary The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.
Quality of Detection (QoD): 70%
Vulnerability Detection Result Vulnerability was detected according to the Vulnerability Detection Method.
Impact An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.
Solution: **Solution type:** Mitigation Replace Telnet with a protocol like SSH which supports encrypted connections.
Vulnerability Detection Method Details: `Telnet Unencrypted Cleartext Login` OID:1.3.6.1.4.1.25623.1.0.108522 Version used: `2023-10-13T05:06:09Z`

Figure 45: Vulnérabilité 2 sur le switch 192.168.254.2

❖ **Constats**

- Utilisation de faibles algorithmes de chiffrement
- Utilisation de protocole moins sécurisé (Telnet)

Quelques Résultats du scan sur la partie du réseau utilisateur

❖ ***Hôte 192.168.210.57***

Ports ouverts

Service (Port)	Threat Level
80/tcp	High
23/tcp	Medium

Figure 46: Ports ouverts sur l'hôte 192.168.210.57

High (CVSS: 9.8)
NVT: Lighttpd < 1.4.35 Multiple Vulnerabilities - Active Check

Product detection result
cpe:/a:lighttpd:lighttpd:1.4.28
Detected by Lighttpd Server Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.111079)

Summary
Lighttpd is prone to multiple vulnerabilities.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
Vulnerable URL: http://192.168.210.57/etc/passwd

Impact
Successful exploitation will allow remote attackers to execute arbitrary SQL commands and remote attackers to read arbitrary files via hostname.

Solution:
Solution type: VendorFix
Update to version 1.4.35 or later.

Figure 47: Vulnérabilité 1 sur l'hôte 192.168.210.57

Medium (CVSS: 4.8)
NVT: Telnet Unencrypted Cleartext Login

Summary
The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution:
Solution type: Mitigation
Replace Telnet with a protocol like SSH which supports encrypted connections.

Figure 48: Vulnérabilité 2 sur l'hôte 192.168.210.57

❖ **Constats**

- Problème d'Adressage : Serveur ou équipement réseau placé sur le réseau des Utilisateurs
- Utilisation de protocole moins sécurisé (Telnet)

❖ ***Hôte 192.168.210.73***

Ports ouverts

Service (Port)	Threat Level
general/tcp	High
80/tcp	Medium
general/tcp	Medium
22/tcp	Medium
21/tcp	Medium
23/tcp	Medium
22/tcp	Low

Figure 49: Ports ouverts sur hôte 192.168.210.73

High (CVSS: 8.1)
NVT: MikroTik RouterOS RCE Vulnerability (CVE-2021-41987)

Product detection result

```
cpe:/o:mikrotik:routeros:6.47.10
Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.
↪0.810608)
```

Summary
MikroTik RouterOS is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 6.47.10
Fixed version:     6.48.6
```

Solution:
Solution type: VendorFix
Update to version 6.48.6, 6.49.1, 7.1 or later.

Figure 50: Vulnérabilité 1 sur hôte 192.168.210.73

High (CVSS: 7.5)
NVT: MikroTik RouterOS < 6.46.7, 6.47.x < 6.48beta40, 7.x < 7.1beta3 DoS Vulnerability

Product detection result
cpe:/o:mikrotik:routeros:6.47.10
Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.
↪0.810608)

Summary
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability in the SMB server.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 6.47.10
Fixed version: 6.48beta40

Solution:
Solution type: VendorFix
- Update to version 6.46.7 (long-term release), 6.48beta40 (testing release), 7.1beta3 (development release) or later
- Disable the SMB server / functionality
Note: Please set an override for this result if the SMB server / functionality is already disabled

Figure 51: Vulnérabilité 2 sur hôte 192.168.210.73

High (CVSS: 7.5)
NVT: MikroTik RouterOS 6.0.0 < 6.48.8, 6.49.x < 6.49.10 DoS Vulnerability

Product detection result
cpe:/o:mikrotik:routeros:6.47.10
Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.
↪0.810608)

Summary
MikroTik RouterOS is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 6.47.10
Fixed version: 6.48.8

Solution:
Solution type: VendorFix
Update to version 6.48.8, 6.49.10 or later.

Figure 52: Vulnérabilité 3 sur hôte 192.168.210.73

High (CVSS: 7.2)
NVT: MikroTik RouterOS < 6.49.8 Privilege Escalation Vulnerability

Product detection result

```
cpe:/o:mikrotik:routeros:6.47.10
Detected by MikroTik RouterOS Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.
↪0.810608)
```

Summary

MikroTik RouterOS is prone to a privilege escalation vulnerability.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 6.47.10
Fixed version:     6.49.8
```

Solution:

Solution type: VendorFix

Update to version 6.49.8 or later.

Figure 53: Vulnérabilité 4 sur hôte 192.168.210.73

Medium (CVSS: 6.4)
NVT: MikroTik RouterOS < 6.49.12, 7.x < 7.13.3 DoS Vulnerability (Loop DoS)

Summary

MikroTik RouterOS is prone to a denial of service (DoS) vulnerability dubbed 'Loop DoS'.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
Installed version: 6.47.10
Fixed version:     6.49.12
Installation
path / port:       /
```

Solution:

Solution type: VendorFix

Figure 54: Vulnérabilité 5 sur hôte 192.168.210.73

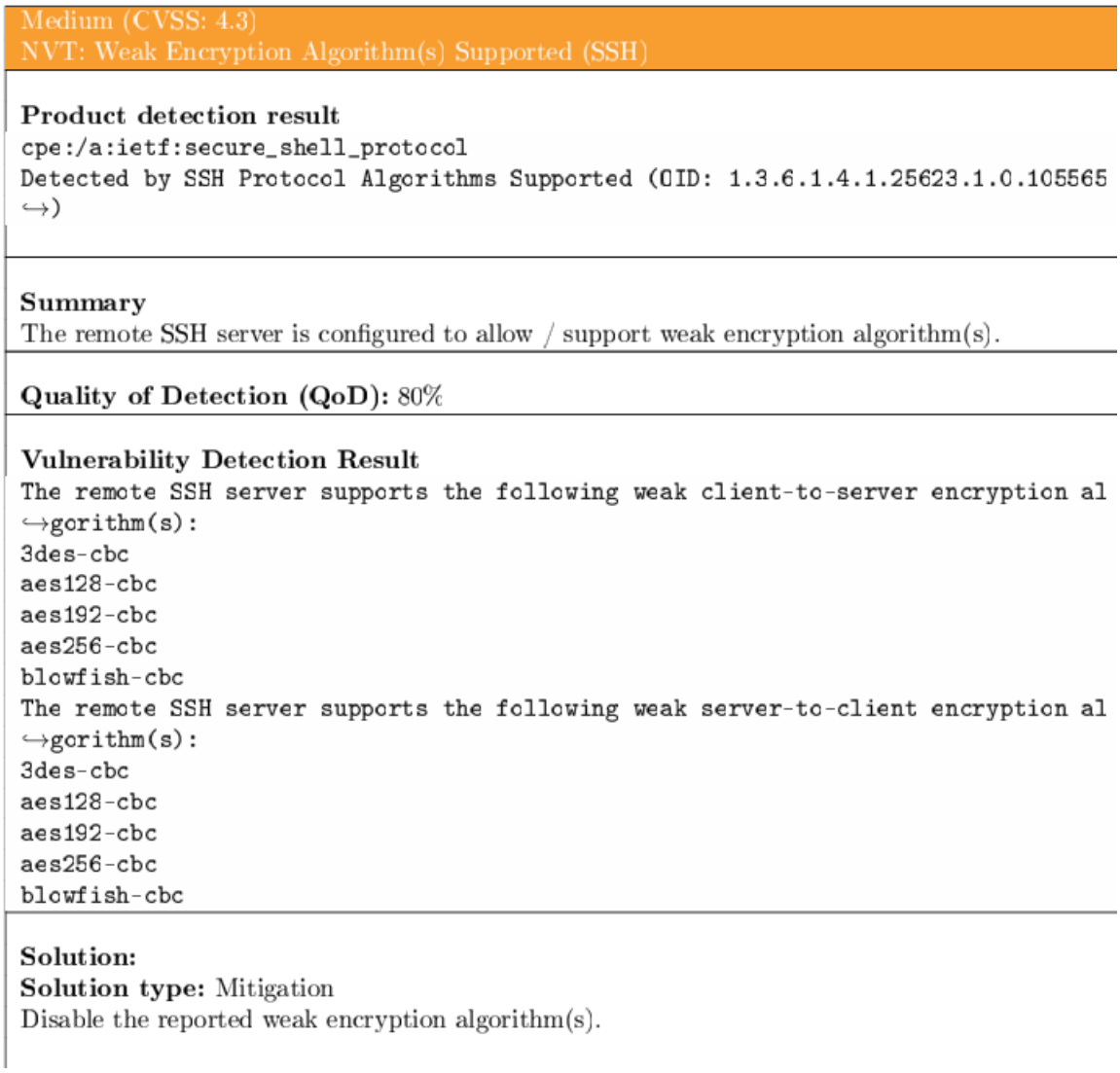


Figure 55: Vulnérabilité 6 sur hôte 192.168.210.73

❖ **Constats**

- Problème d'Adressage : équipement réseau placé sur le réseau des utilisateurs
- Utilisation de protocole moins sécurisé
- Hôte vulnérable aux attaques DOS et escalades de privilège

6.5.2 Scan externe

Le scan externe a été effectué sur les adresses IP publiques et DNS suivantes :

APPLICATIONS WEB		
Nom du site	***Adresse URL***	***Accessibilité (interne/externe)***
Site principal de l'Université	https://univ-lome.tg/	oui/oui
Portail académique (étudiants)	https://etu.univ-lome.tg/	oui/oui
Site d'apprentissage en ligne	https://elearn.univ-lome.tg:8181/	oui/oui

Webmail de l'Université	https://webmail.univ-lome.tg:8443/	oui/oui

Tableau 17: Applications web scannées

ADRESSES IP PUBLIQUES		
Adresse réseau	***Masque réseau***	***Commentaires***
41.207.188.16	255.255.255.240	

Tableau 18: Adresse IP publiques scannées

- ***Hôte 41.207.188.28***

Ports ouverts

Service (Port)	Threat Level
443/tcp	Medium
80/tcp	Medium

Figure 56: Ports ouverts sur l'adresse publique 41.207.188.28

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

The remote server's SSL/TLS certificate has already expired.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The certificate of the remote service expired on 2021-07-17 07:30:14.
Certificate details:
fingerprint (SHA-1)             | E5037E811D542E28B10BDE76575E4F6E4CA2CCCA
fingerprint (SHA-256)           | 42C97AFB101233F2F01C5369D778293316442221E81820
↪AF7E17AB1F3F333511
issued by                       | CN=Go Daddy Secure Certificate Authority - G2,
↪OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=A
↪rizona,C=US
public key algorithm            | RSA
public key size (bits)          | 2048
serial                          | 00E4FEA1131DA14AEB
signature algorithm             | sha256WithRSAEncryption
subject                         | CN=captive-portal.peplink.com,OU=Domain Contro
↪l Validated
subject alternative names (SAN) | captive-portal.peplink.com, www.captive-portal
↪.peplink.com
valid from                      | 2019-07-17 07:30:14 UTC
valid until                     | 2021-07-17 07:30:14 UTC
```

Solution:
Solution type: Mitigation
Replace the SSL/TLS certificate by a new one.

Figure 57: vulnérabilité sur l'adresse publique 41.207.188.28

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following input fields were identified (URL:input name):
http://41.207.188.28/cgi-bin/MANGA/index.cgi:password

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Figure 58: vulnérabilité sur l'adresse publique 41.207.188.28

- **Constats**
  - Certificat du serveur web expiré
  - Informations transitant en clair

- ***Hôte 41.207.188.29***

Ports ouverts

Service (Port)	Threat Level
443/tcp	Medium
80/tcp	Medium

Figure 59: Ports ouverts sur l'adresse publique 41.207.188.29

Medium (CVSS: 5.0)
NVT: SSL/TLS: Certificate Expired

Product detection result
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary
The remote server's SSL/TLS certificate has already expired.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
The certificate of the remote service expired on 2021-07-17 07:30:14.
Certificate details:

fingerprint (SHA-1)	E5037E811D542E28B10BDE76575E4F6E4CA2CCCA
fingerprint (SHA-256)	42C97AFB101233F2F01C5369D778293316442221E81820 ↪AF7E17AB1F3F333511
issued by	CN=Go Daddy Secure Certificate Authority - G2, ↪OU=http://certs.godaddy.com/repository/,O=GoDaddy.com\, Inc.,L=Scottsdale,ST=A ↪rizona,C=US
public key algorithm	RSA
public key size (bits)	2048
serial	00E4FEA1131DA14AEB
signature algorithm	sha256WithRSAEncryption
subject	CN=captive-portal.peplink.com,OU=Domain Contro ↪l Validated
subject alternative names (SAN)	captive-portal.peplink.com, www.captive-portal ↪.peplink.com
valid from	2019-07-17 07:30:14 UTC
valid until	2021-07-17 07:30:14 UTC

Solution:
Solution type: Mitigation

Figure 60: vulnérabilité 1 sur l'adresse publique 41.207.188.29

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The following input fields were identified (URL:input name):`
`http://41.207.188.29/cgi-bin/MANGA/index.cgi:password`

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Figure 61:vulnérabilité 2 sur l'adresse publique 41.207.188.29

- ***Hôte 41.207.188.27***

Ports ouverts

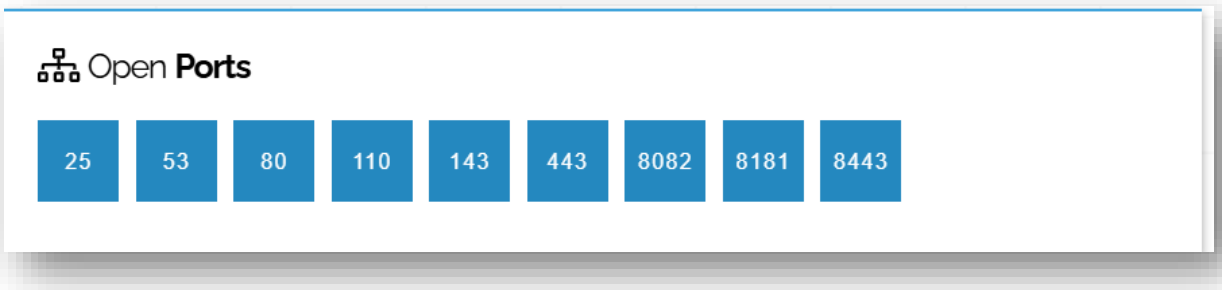


Figure 62: Ports ouverts sur l'adresse publique 41.207.188.27

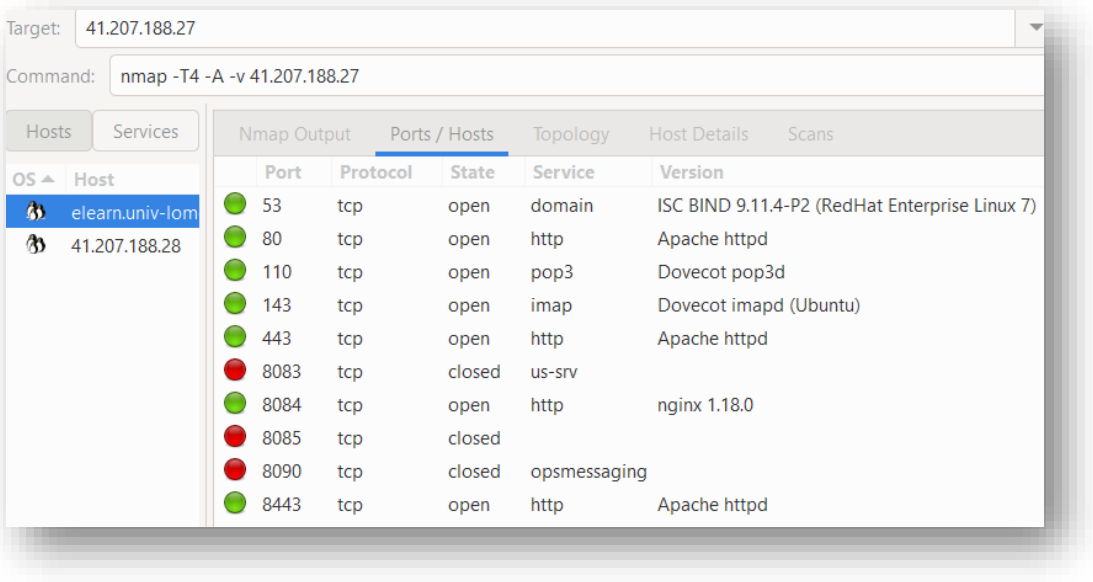


Figure 63: Ports ouverts sur l'adresse publique 41.207.188.27

Technologies utilisées associées

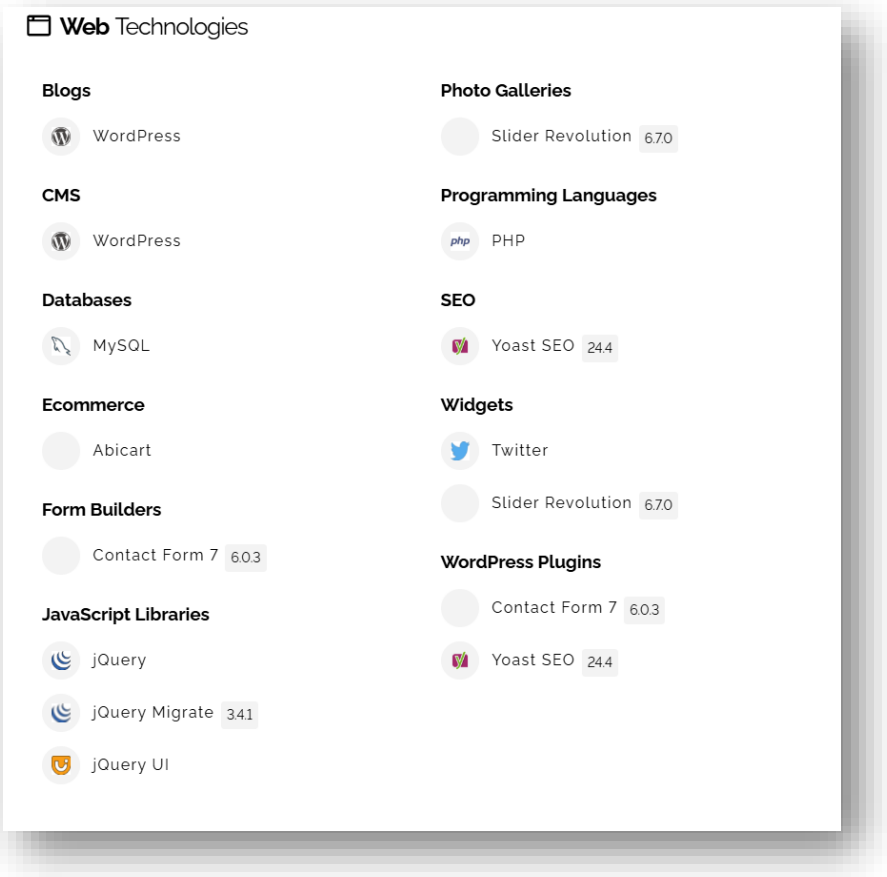
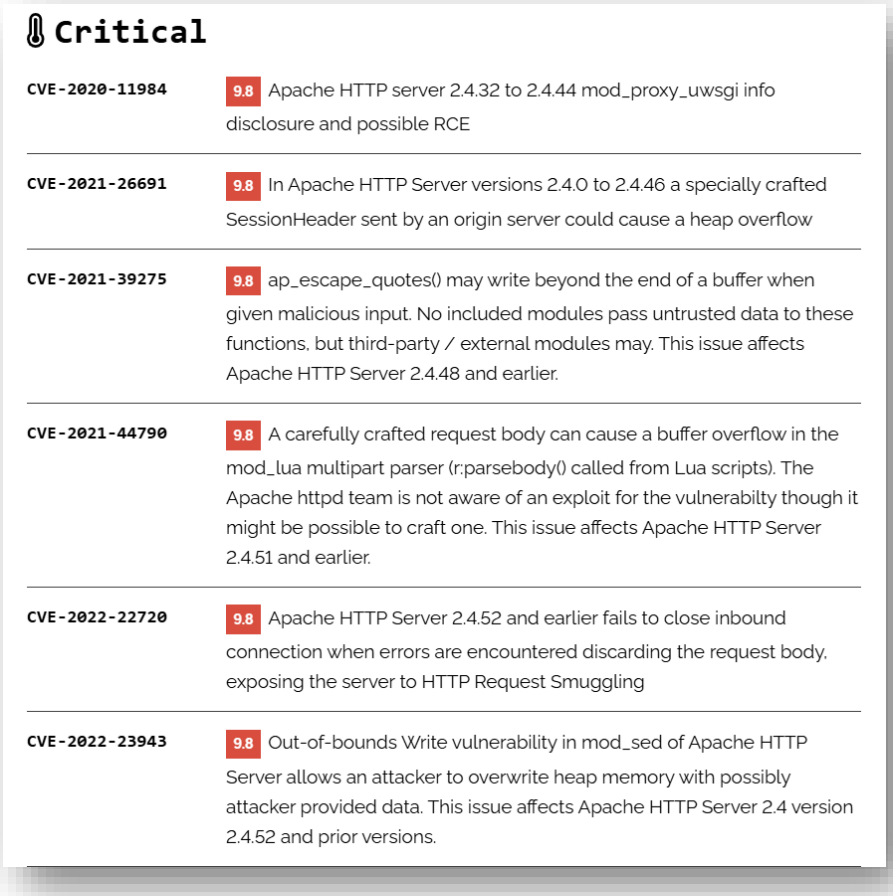


Figure 64: Technologies web utilisées sur l'adresse publique 41.207.188.27

Vulnérabilités de la plus critique à la moins critique



Critical

CVE-2020-11984	9.8 Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE
CVE-2021-26691	9.8 In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
CVE-2021-39275	9.8 ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2021-44790	9.8 A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
CVE-2022-22720	9.8 Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
CVE-2022-23943	9.8 Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

Figure 65: Vulnérabilité sur l'adresse publique 41.207.188.27

CVE-2022-31813	9.8 Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2023-25690	9.8 Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
CVE-2024-38474	9.8 Substitution encoding issue in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows attacker to execute scripts in directories permitted by the configuration but not directly reachable by any URL or source disclosure of scripts meant to only to be executed as CGI. Users are recommended to upgrade to version 2.4.60, which fixes this issue. Some RewriteRules that capture and substitute unsafely will now fail unless rewrite flag "UnsafeAllow3F" is specified.

Figure 66: Vulnérabilité sur l'adresse publique 41.207.188.27

CVE-2024-38476	9.8 Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vulnerably to information disclosure, SSRF or local script execution via backend applications whose response headers are malicious or exploitable. Users are recommended to upgrade to version 2.4.60, which fixes this issue.
CVE-2022-22721	9.1 If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2022-28615	9.1 Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
CVE-2021-40438	9.0 A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2022-36760	9.0 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

Figure 67: Vulnérabilité sur l'adresse publique 41.207.188.27

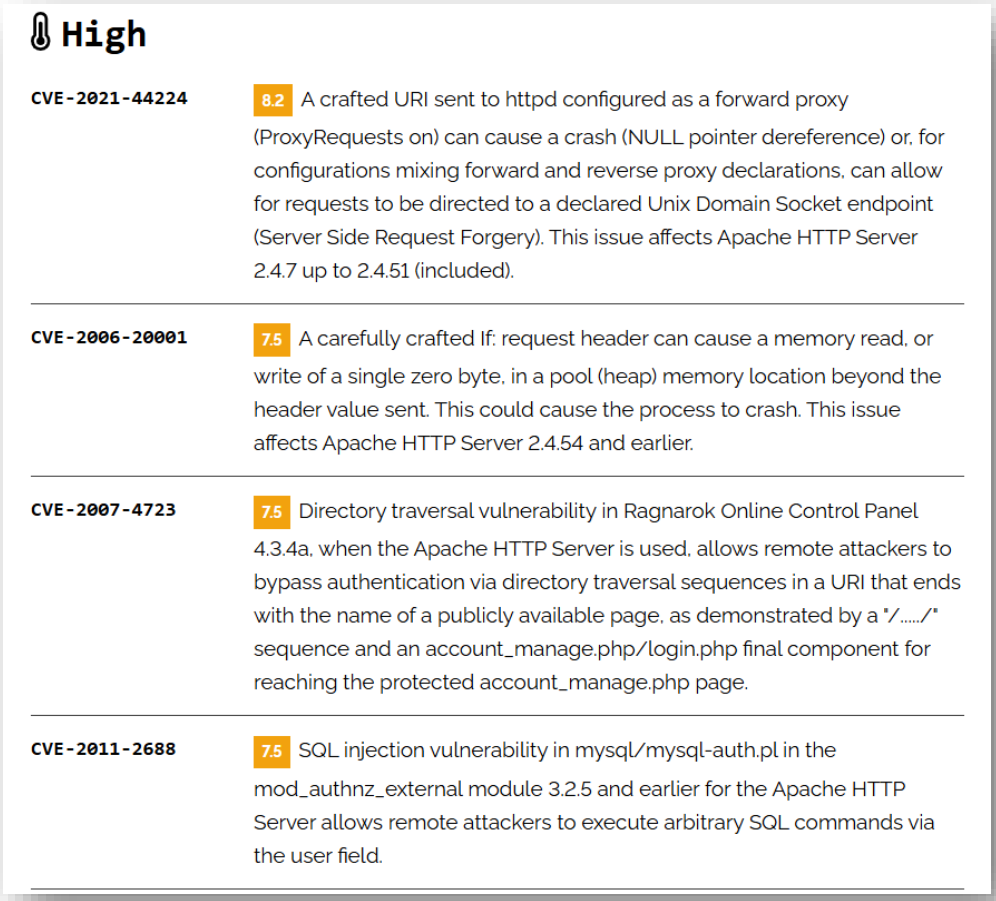


Figure 68: Vulnérabilité sur l'adresse publique 41.207.188.27

CVE-2013-4365	7.5 Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.
CVE-2020-9490	7.5 Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.
CVE-2020-11993	7.5 Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.
CVE-2020-13950	7.5 Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service
CVE-2021-26690	7.5 Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

Figure 69: Vulnérabilité sur l'adresse publique 41.207.188.27

CVE-2021-33193	7.5 A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
CVE-2021-34798	7.5 Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2021-36160	7.5 A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).
CVE-2022-22719	7.5 A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2022-26377	7.5 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
CVE-2022-29404	7.5 In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-30556	7.5 Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Figure 70: Vulnérabilité sur l'adresse publique 41.207.188.27

CVE-2023-27522	7.5 HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.
CVE-2023-31122	7.5 Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.
CVE-2024-27316	7.5 HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.
CVE-2024-38477	7.5 null pointer dereference in mod_proxy in Apache HTTP Server 2.4.59 and earlier allows an attacker to crash the server via a malicious request. Users are recommended to upgrade to version 2.4.60, which fixes this issue.
CVE-2024-40898	7.5 SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue.

Figure 71: Vulnérabilité sur l'adresse publique 41.207.188.27

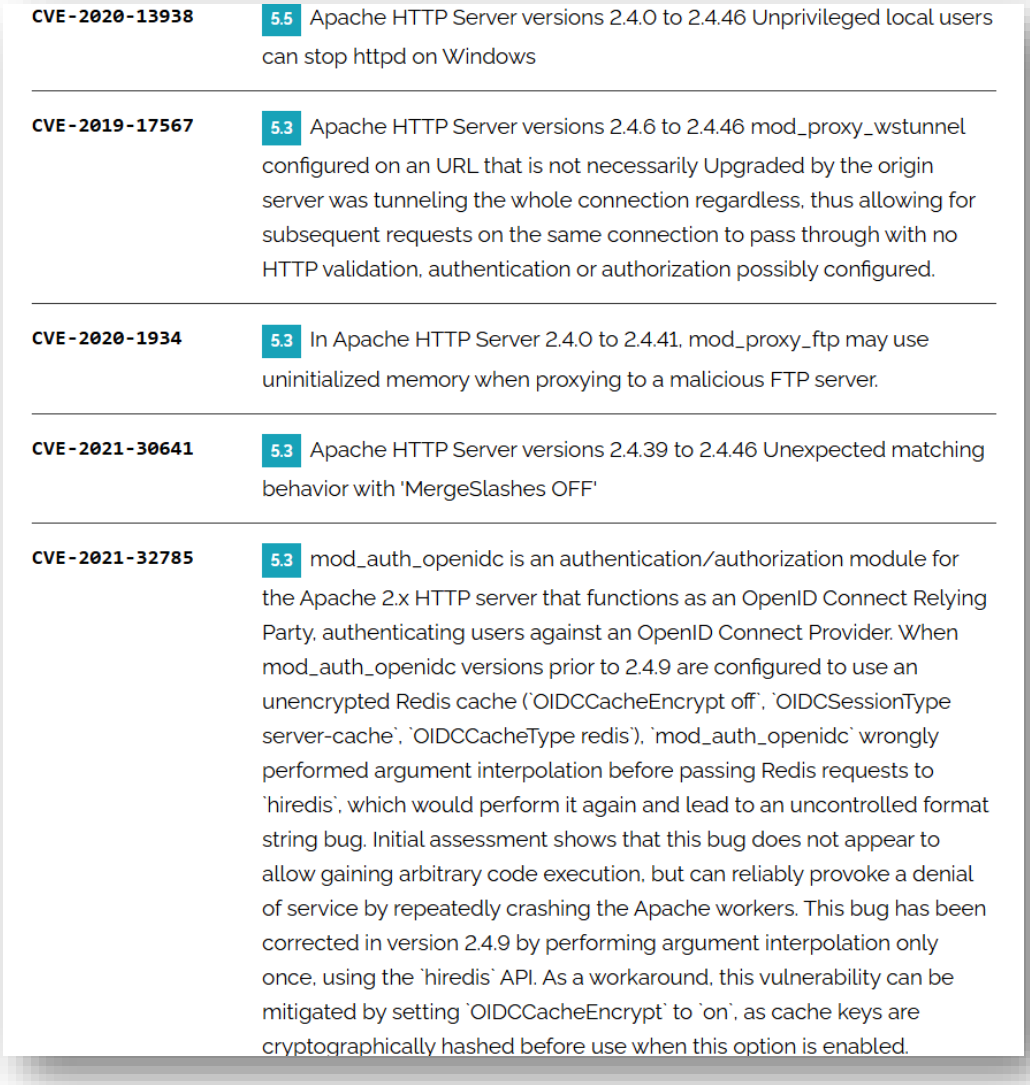
CVE-2020-35452	7.3 Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

Figure 72: Vulnérabilité sur l'adresse publique 41.207.188.27

Medium

CVE-2020-1927	6.1 In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2021-32791	5.9 mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, the AES GCM encryption in mod_auth_openidc uses a static IV and AAD. It is important to fix because this creates a static nonce and since aes-gcm is a stream cipher, this can lead to known cryptographic issues, since the same key is being reused. From 2.4.9 onwards this has been patched to use dynamic values through usage of cjose AES encryption routines.
CVE-2023-45802	5.9 When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

Figure 73: Vulnérabilité sur l'adresse publique 41.207.188.27



CVE-2020-13938	5.5 Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
CVE-2019-17567	5.3 Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.
CVE-2020-1934	5.3 In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
CVE-2021-30641	5.3 Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'
CVE-2021-32785	5.3 mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. When mod_auth_openidc versions prior to 2.4.9 are configured to use an unencrypted Redis cache (`OIDCCacheEncrypt off`, `OIDCSessionType server-cache`, `OIDCCacheType redis`), `mod_auth_openidc` wrongly performed argument interpolation before passing Redis requests to `hiredis`, which would perform it again and lead to an uncontrolled format string bug. Initial assessment shows that this bug does not appear to allow gaining arbitrary code execution, but can reliably provoke a denial of service by repeatedly crashing the Apache workers. This bug has been corrected in version 2.4.9 by performing argument interpolation only once, using the `hiredis` API. As a workaround, this vulnerability can be mitigated by setting `OIDCCacheEncrypt` to `on`, as cache keys are cryptographically hashed before use when this option is enabled.

Figure 74: Vulnérabilité sur l'adresse publique 41.207.188.27

CVE-2022-28330	5.3 Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
CVE-2022-28614	5.3 The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
CVE-2022-37436	5.3 Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.
CVE-2009-2299	5.0 The Artofdefence Hyperguard Web Application Firewall (WAF) module before 2.5.5-11635, 3.0 before 3.0.3-11636, and 3.1 before 3.1.1-11637, a module for the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via an HTTP request with a large Content-Length value but no POST data.
CVE-2012-3526	5.0 The reverse proxy add forward module (mod_rpaf) 0.5 and 0.6 for the Apache HTTP Server allows remote attackers to cause a denial of service (server or application crash) via multiple X-Forwarded-For headers in a request.

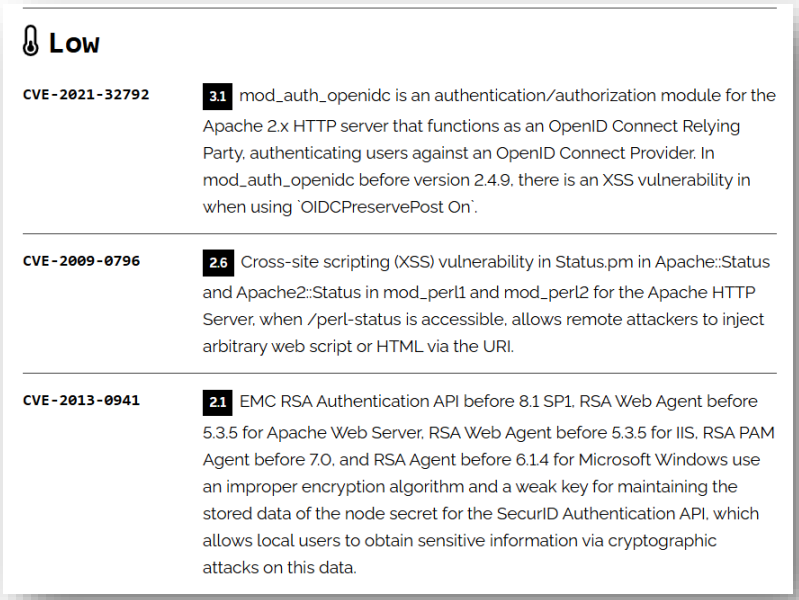
Figure 75: Vulnérabilité sur l'adresse publique 41.207.188.27

CVE-2012-4001	5.0 The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.
CVE-2013-2765	5.0 The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.
CVE-2021-32786	4.7 mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9, `oidc_validate_redirect_url()` does not parse URLs the same way as most browsers do. As a result, this function can be bypassed and leads to an Open Redirect vulnerability in the logout functionality. This bug has been fixed in version 2.4.9 by replacing any backslash of the URL to redirect with slashes to address a particular breaking change between the different specifications (RFC2396 / RFC3986 and WHATWG). As a workaround, this vulnerability can be mitigated by configuring `mod_auth_openidc` to only allow redirection whose destination matches a given regular expression.
CVE-2011-1176	4.3 The configuration merger in itk.c in the Steinar H. Gunderson mpm-itk Multi-Processing Module 2.2.11-01 and 2.2.11-02 for the Apache HTTP Server does not properly handle certain configuration sections that specify NiceValue but not AssignUserID, which might allow remote attackers to gain privileges by leveraging the root uid and root gid of an mpm-itk process.

Figure 76: Vulnérabilité sur l'adresse publique 41.207.188.27

CVE-2012-4360	4.3 Cross-site scripting (XSS) vulnerability in the mod_pagespeed module 0.10.19.1 through 0.10.22.4 for the Apache HTTP Server allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-0942	4.3 Cross-site scripting (XSS) vulnerability in EMC RSA Authentication Agent 7.1 before 7.1.1 for Web for Internet Information Services, and 7.1 before 7.1.1 for Web for Apache, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

Figure 77: Vulnérabilité sur l'adresse publique 41.207.188.27



Low

CVE-2021-32792	3.1 mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In mod_auth_openidc before version 2.4.9, there is an XSS vulnerability in when using `OIDCPreservePost On`.
CVE-2009-0796	2.6 Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.
CVE-2013-0941	2.1 EMC RSA Authentication API before 8.1 SP1, RSA Web Agent before 5.3.5 for Apache Web Server, RSA Web Agent before 5.3.5 for IIS, RSA PAM Agent before 7.0, and RSA Agent before 6.1.4 for Microsoft Windows use an improper encryption algorithm and a weak key for maintaining the stored data of the node secret for the SecurID Authentication API, which allows local users to obtain sensitive information via cryptographic attacks on this data.

Figure 78: Vulnérabilité sur l'adresse publique 41.207.188.27

Résumé de toutes les vulnérabilités

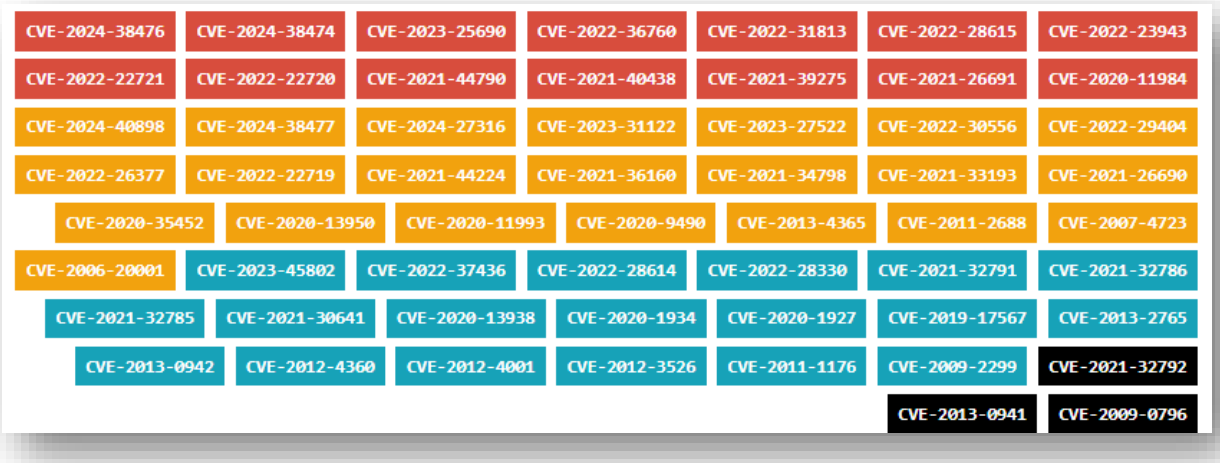
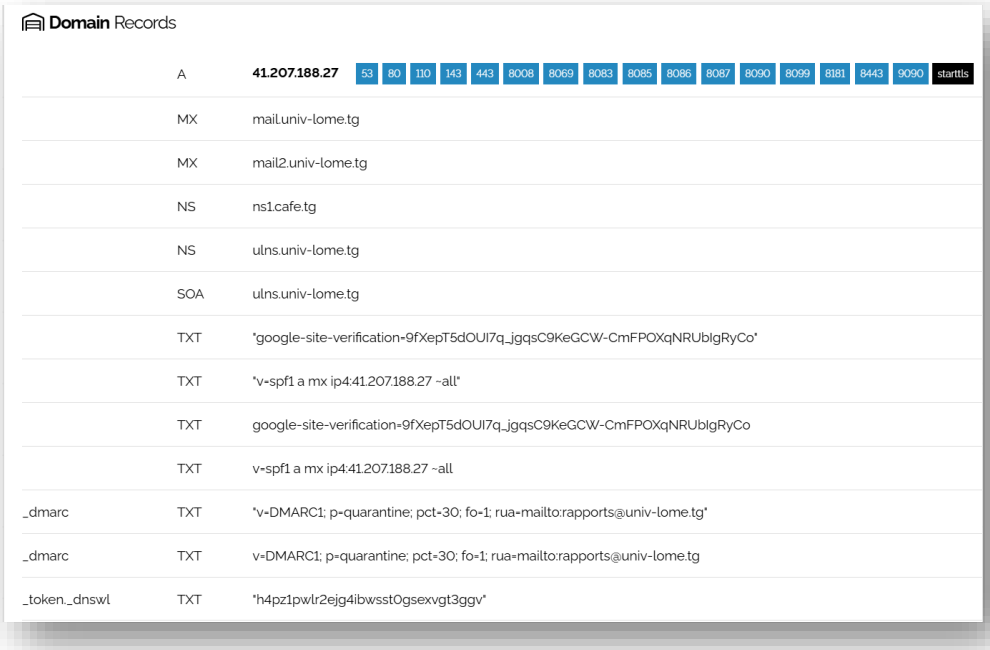


Figure 79: Résumé des CVE sur l'adresse publique 41.207.188.27

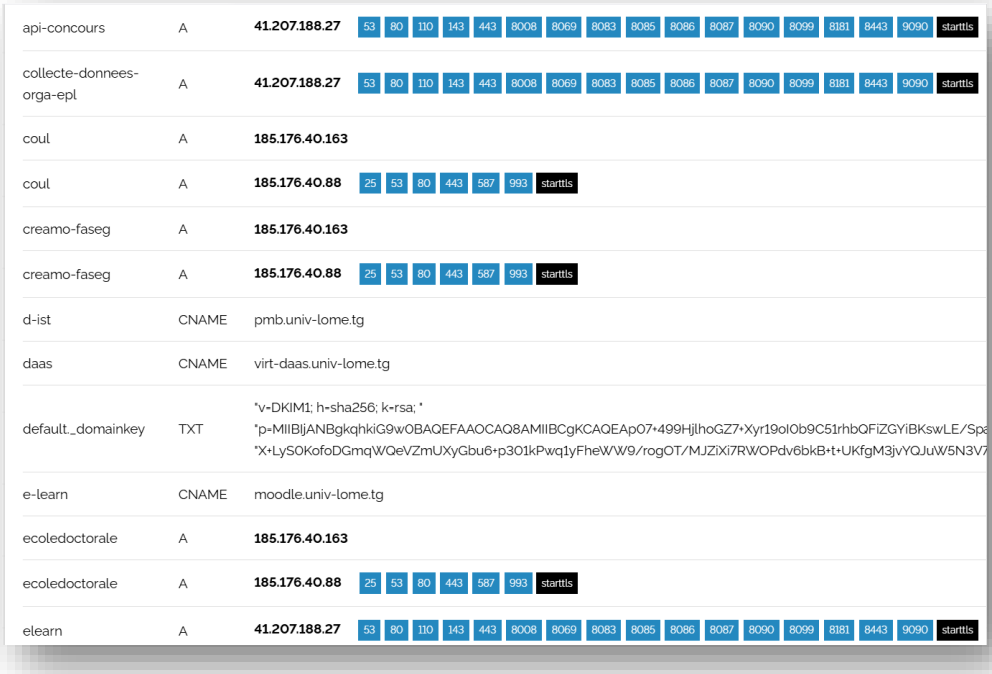
Enregistrement DNS associés à l'adresse publique



Domain Records

	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
	MX	mail.univ-lome.tg
	MX	mail2.univ-lome.tg
	NS	ns1.cafe.tg
	NS	ulns.univ-lome.tg
	SOA	ulns.univ-lome.tg
	TXT	"google-site-verification=9fXepT5dOUI7q_jgqsC9KeGCW-CmFPOXqNRUblgRyCo"
	TXT	"v=spf1 a mx ip4:41.207.188.27 ~all"
	TXT	google-site-verification=9fXepT5dOUI7q_jgqsC9KeGCW-CmFPOXqNRUblgRyCo
	TXT	v=spf1 a mx ip4:41.207.188.27 ~all
_dmarc	TXT	"v=DMARC1; p=quarantine; pct=30; fo=1; rua=mailto:rapports@univ-lome.tg"
_dmarc	TXT	v=DMARC1; p=quarantine; pct=30; fo=1; rua=mailto:rapports@univ-lome.tg
_token._dnswl	TXT	"h4pz1pwlr2ejg4ibwsst0gsexvgt3ggv"

Figure 80: Enregistrement DNS

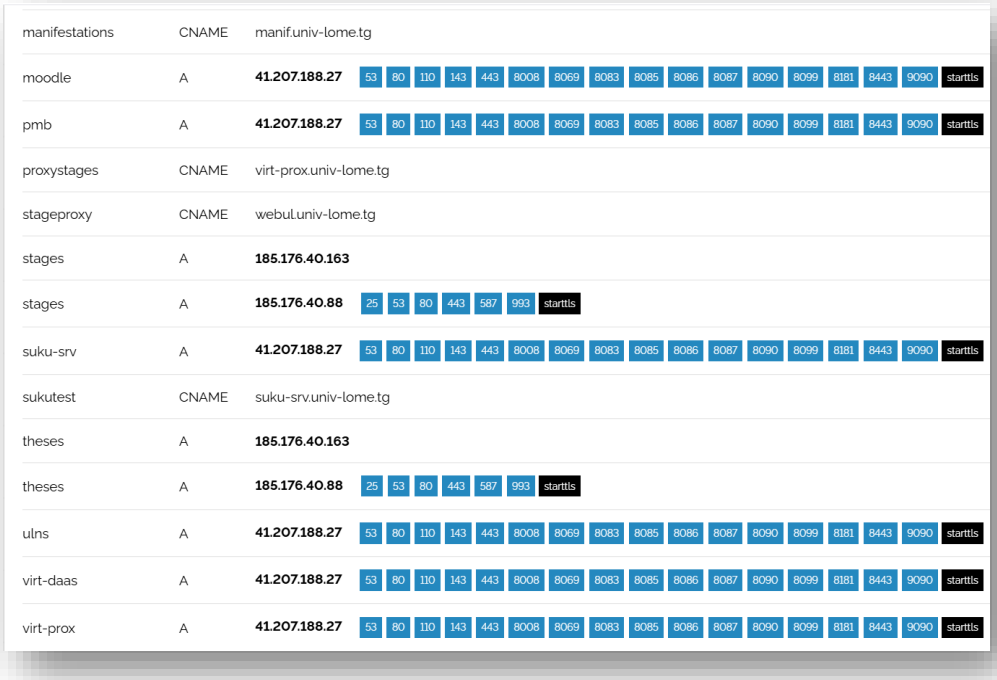


api-concours	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
collecte-donnees-orga-epl	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
coul	A	**185.176.40.163**
coul	A	**185.176.40.88** 25 53 80 443 587 993 starttls
creamo-faseg	A	**185.176.40.163**
creamo-faseg	A	**185.176.40.88** 25 53 80 443 587 993 starttls
d-ist	CNAME	pmb.univ-lome.tg
daas	CNAME	virt-daas.univ-lome.tg
default._domainkey	TXT	"v=DKIM1; h=sha256; k=rsa; " "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAp07+499HjlhoGZ7+Xyr19ol0b9C51rhbQFiZGYiBKswLE/Spa "X+LyS0KofoDGmqWQeVZmUXyGbu6+p301kPwq1yFheWW9/rogOT/MJZiXi7RWOPdv6bkB+t+UKfgM3jvYQJuW5N3V7
e-learn	CNAME	moodle.univ-lome.tg
ecoledoctorale	A	**185.176.40.163**
ecoledoctorale	A	**185.176.40.88** 25 53 80 443 587 993 starttls
elearn	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls

Figure 81: Enregistrement DNS

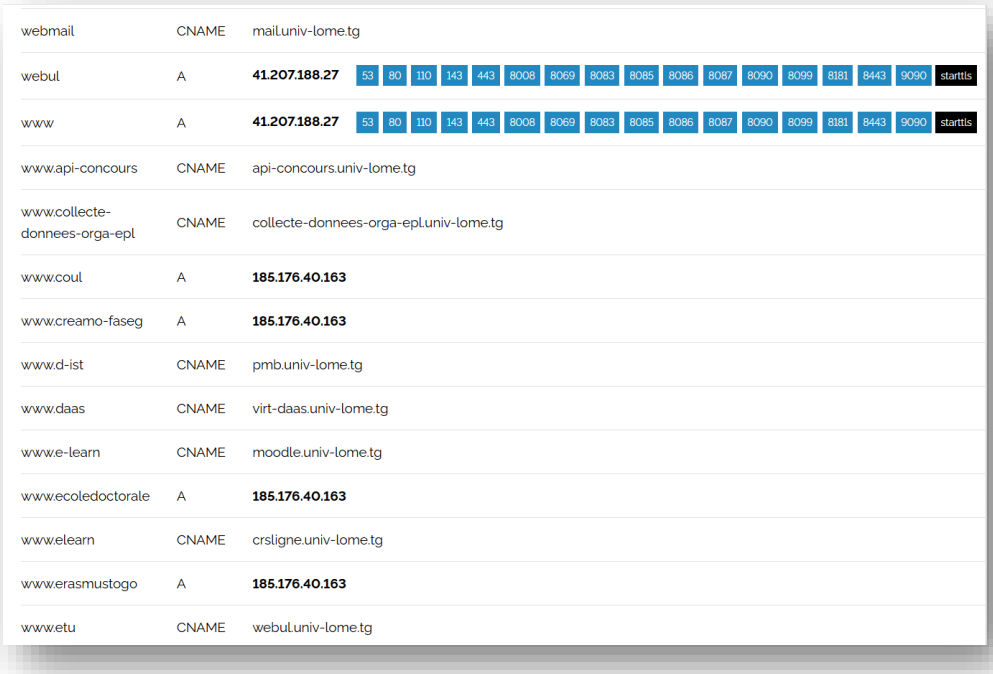
erasmustogo	A	**185.176.40.163**
erasmustogo	A	**185.176.40.88** 25 53 80 443 587 993 starttls
etu	CNAME	webul.univ-lome.tg
gbif	A	**185.176.40.163**
gbif	A	**185.176.40.88** 25 53 80 443 587 993 starttls
inscription-epl	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
jrsul	A	**185.176.40.163**
jrsul	A	**185.176.40.88** 25 53 80 443 587 993 starttls
jsil	A	**185.176.40.163**
jsil	A	**185.176.40.88** 25 53 80 443 587 993 starttls
mail	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
mail2	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
mailbox	CNAME	mail2.univ-lome.tg
manif	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls

Figure 82: Enregistrement DNS



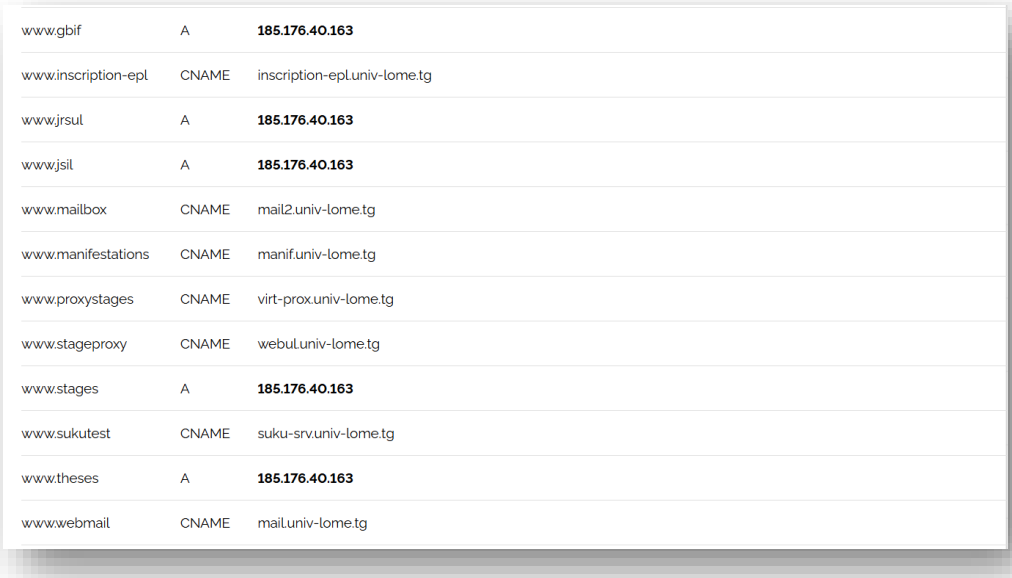
manifestations	CNAME	manif.univ-lome.tg
moodle	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
pmb	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
proxystages	CNAME	virt-prox.univ-lome.tg
stageproxy	CNAME	webul.univ-lome.tg
stages	A	**185.176.40.163**
stages	A	**185.176.40.88** 25 53 80 443 587 993 starttls
suku-srv	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
sukutest	CNAME	suku-srv.univ-lome.tg
theses	A	**185.176.40.163**
theses	A	**185.176.40.88** 25 53 80 443 587 993 starttls
ulns	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
virt-daas	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
virt-prox	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls

Figure 83: Enregistrement DNS



webmail	CNAME	mail.univ-lome.tg
webul	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
www	A	**41.207.188.27** 53 80 110 143 443 8008 8069 8083 8085 8086 8087 8090 8099 8181 8443 9090 starttls
www.api-concours	CNAME	api-concours.univ-lome.tg
www.collecte-donnees-orga-epl	CNAME	collecte-donnees-orga-epl.univ-lome.tg
www.coul	A	**185.176.40.163**
www.creamo-faseg	A	**185.176.40.163**
www.d-ist	CNAME	pmb.univ-lome.tg
www.daas	CNAME	virt-daas.univ-lome.tg
www.e-learn	CNAME	moodle.univ-lome.tg
www.ecoledoctorale	A	**185.176.40.163**
www.elearn	CNAME	crsligne.univ-lome.tg
www.erasmustogo	A	**185.176.40.163**
www.etu	CNAME	webul.univ-lome.tg

Figure 84: Enregistrement DNS



www.gbif	A	**185.176.40.163**
www.inscription-epl	CNAME	inscription-epl.univ-lome.tg
www.jrsul	A	**185.176.40.163**
www.jsil	A	**185.176.40.163**
www.mailbox	CNAME	mail2.univ-lome.tg
www.manifestations	CNAME	manif.univ-lome.tg
www.proxystages	CNAME	virt-prox.univ-lome.tg
www.stageproxy	CNAME	webul.univ-lome.tg
www.stages	A	**185.176.40.163**
www.sukutest	CNAME	suku-srv.univ-lome.tg
www.theses	A	**185.176.40.163**
www.webmail	CNAME	mail.univ-lome.tg

Figure 85: Enregistrement DNS

❖ **Constats**

- Centralisation des sites web sur une seule IP publique : Risque de single point of failure : si cette IP est attaquée ou mise hors service, tous les sites web deviennent inaccessibles
- Présence de vulnérabilités critiques non corrigées exposées sur Internet

- Problèmes liés aux enregistrements DNS : Certains sous-domaines comme crsligne.univ-lome.tg sont inaccessibles, indiquant un problème de gestion des DNS (erreurs de configuration, absence de mise à jour des enregistrements).

6.5.3 Synthèse audit de la sécurité

Bien que l'Université de Lomé ait consenti des efforts pour corriger certaines vulnérabilités, de nombreuses lacunes persistent. Il est important de noter que, si ces failles ne sont pas correctement atténuées, elles pourraient compromettre la confidentialité, l'intégrité et la disponibilité du système d'information de l'Université de Lomé.

Parmi les principales vulnérabilités encore présentes, on distingue :

Risques liés à l'infrastructure web

- Centralisation des sites web sur une seule IP publique : Risque de *single point of failure* en cas d'attaque ou de panne.
- Présence de vulnérabilités critiques exposées sur Internet et Potentiellement exploitables par des attaquants.
- Problèmes DNS : Certains sous-domaines comme crsligne.univ-lome.tg sont inaccessibles, indiquant des erreurs de configuration ou un manque de mise à jour des enregistrements DNS.

Vulnérabilités et faiblesses de sécurité

- Certificat TLS expiré : risque de compromission des connexions sécurisées.
- Utilisation de faibles algorithmes de chiffrement (non mitigée malgré les recommandations précédentes).
- Vulnérabilité HTTP TRACE toujours active sur le service HTTP.
- Système vulnérable aux attaques SCM Files/Folders et XSS : risque d'injection de scripts malveillants.
- Utilisation de protocoles obsolètes ou peu sécurisés à savoir Telnet
- Certains serveurs et équipements réseau sont vulnérables aux attaques DoS et à l'escalade de privilèges
- Absence de chiffrement des données sensibles, entraînant la transmission d'informations en clair et exposant ainsi les communications aux interceptions et attaques de type Man-in-the-Middle (MitM).

Problèmes d'adressage et de segmentation

- Problème d'adressage : Certains serveurs et équipements réseau sont situés sur le réseau des utilisateurs, augmentant les risques d'accès non autorisé.
- Hôte dans la DMZ pouvant joindre l'ensemble du réseau interne : Problème d'adressage et de filtrage.

Cette liste de scans n'est pas exhaustive ; le rapport complet sera joint en annexe à ce document.

7. RECOMMENDATIONS ET ACTIONS CORRECTIVES

7.1 Refonte de l'infrastructure réseau

Un datacenter normé est essentiel pour garantir la sécurité, la disponibilité et la performance des infrastructures informatiques. En respectant les normes en vigueur, il assure une meilleure résilience face aux pannes, cyberattaques et catastrophes naturelles.

Ainsi, en complément des recommandations de l'audit initial sur la nouvelle architecture cible, nous proposons la construction de deux nouveaux datacenters, l'un situé au nord et l'autre au sud de l'Université de Lomé, afin de pallier les insuffisances des infrastructures actuelles jugées inadaptées.

- Le premier datacenter servira de site primaire, hébergeant les ressources critiques.
- Le second sera une réplique du primaire, garantissant la redondance et la continuité des services en cas de défaillance du premier.

L'infrastructure réseau de l'Université s'appuiera sur ces deux salles, qui seront interconnectées et renforcées par un bouclage au niveau Edge (Zone Internet) et Cœur (Zone centrale du réseau).

Cette nouvelle architecture apportera une résilience accrue, renforçant ainsi la sécurité, la disponibilité et les performances du système d'information.

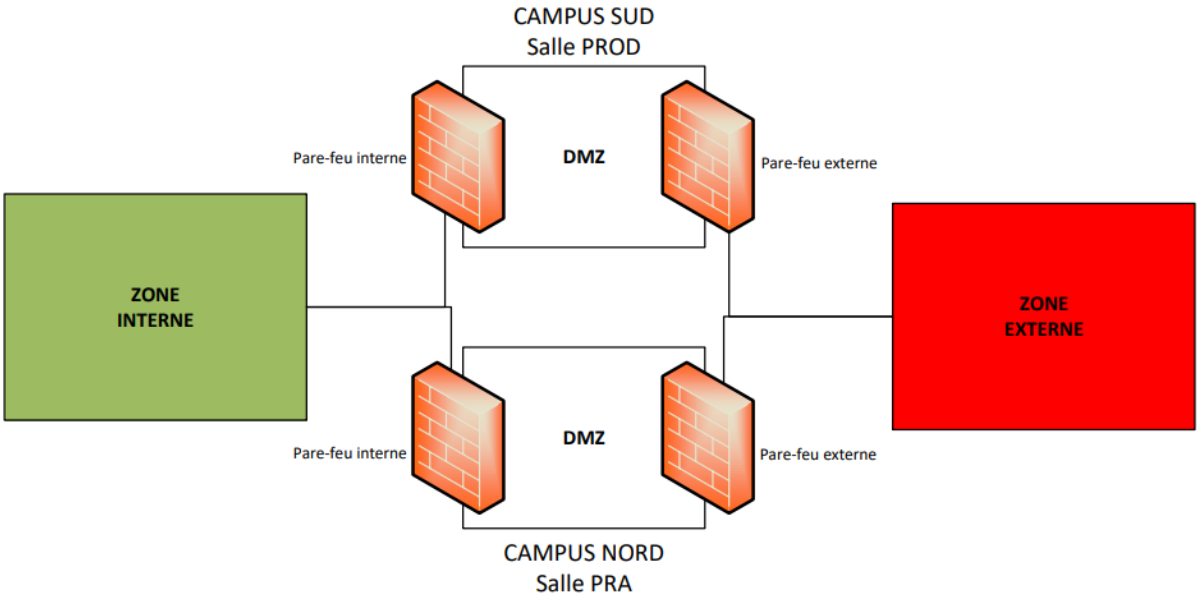


Figure 86: Architecture réseau cible

7.2 Sécurité du SI

7.2.1 Sécurité des applications WEB

Afin de renforcer la sécurité des applications web de l'Université de Lomé, nous recommandons vivement la mise en place d'un Web Application Firewall (WAF). Ce dispositif de sécurité permettra de filtrer et de surveiller les requêtes HTTP/HTTPS entrant et sortant des serveurs web, afin de protéger ces derniers contre diverses attaques telles que l'injection SQL, les cross-site scripting (XSS), les attaques par force brute, et d'autres menaces en rapport avec les applications web.

7.2.1.1 Avantages du WAF

Le WAF offrira les avantages suivants :

- Protection renforcée contre les attaques Web : Le WAF interceptera et bloquera toute tentative d'exploitation de vulnérabilités connues ou inconnues dans les applications web.
- Sécurisation des serveurs dans la DMZ : Il permettra de filtrer les accès aux serveurs web dans la zone démilitarisée (DMZ), en s'assurant que seules les connexions légitimes atteignent les applications.
- Réduction des risques de compromission : En empêchant l'exécution de requêtes malveillantes, il limite les risques d'accès non autorisé, de perte de données et de compromission des serveurs.

- Détection et prévention des attaques DDoS : Le WAF, en fonction de sa configuration, pourra offrir une défense contre les attaques par déni de service distribué (DDoS) ciblant les applications web.

7.2.1.1 Mise en œuvre du WAF

Nous recommandons FortiWeb comme solution WAF à intégrer dans le SI de l'UL pour la protection des applications dans la DMZ. Son intégration sera comme suit :

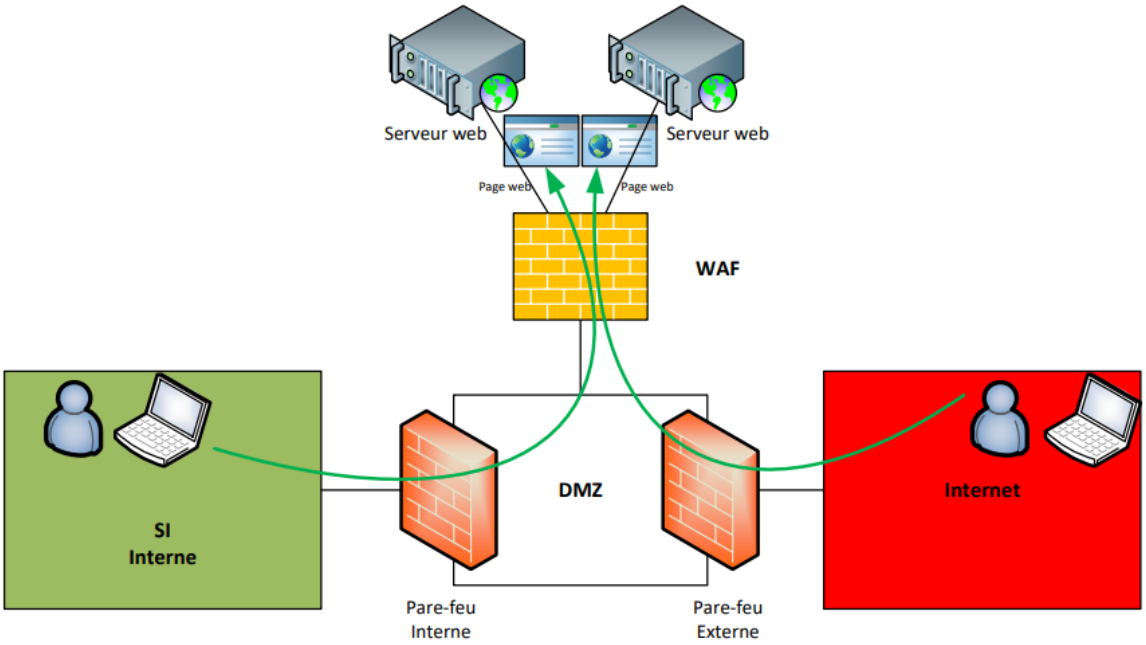


Figure 87: Architecture cible avec un WAF

Il sera configuré en cluster avec un second dans à la salle serveur PRA afin d'assurer une continuité de service et éviter les points de défaillance unique

7.2.2 Sécurité du serveur de messagerie

Pour renforcer la protection du serveur de messagerie de l'Université de Lomé contre les attaques sophistiquées ciblant les emails tels que : phishing, malware, usurpation d'identité ; nous recommandons la mise en place d'un ProxyMail.

7.2.2.1 Fonctionnalités d'un ProxyMail

Les fonctionnalités clés d'un ProxyMail sont :

- Mise en place d'un filtre antispam avec analyse comportementale et heuristique.
- Blocage des emails contenant des pièces jointes suspectes ou des liens malveillants.

- Analyse en temps réel des en-têtes des emails pour identifier les tentatives de spoofing.
- Sandboxing des pièces jointes : ouverture et analyse des fichiers dans un environnement isolé avant transmission
- Implémentation de SPF, DKIM et DMARC pour protéger contre le spoofing et garantir l'authenticité des emails
- Vérification des expéditeurs grâce à des listes blanches et noires dynamiques.
- Détection des tentatives de fraude BEC (Business Email Compromise) par analyse du comportement des expéditeurs.
- Alertes automatiques en cas de détection d'attaques ciblées ou de compromission d'un compte.

7.2.2.2 Mise en œuvre du ProxyMail

Nous recommandons FortiMail comme solution ProxyMail à mettre en œuvre à l'université de Lomé.

Ci-après son architecture d'intégration :

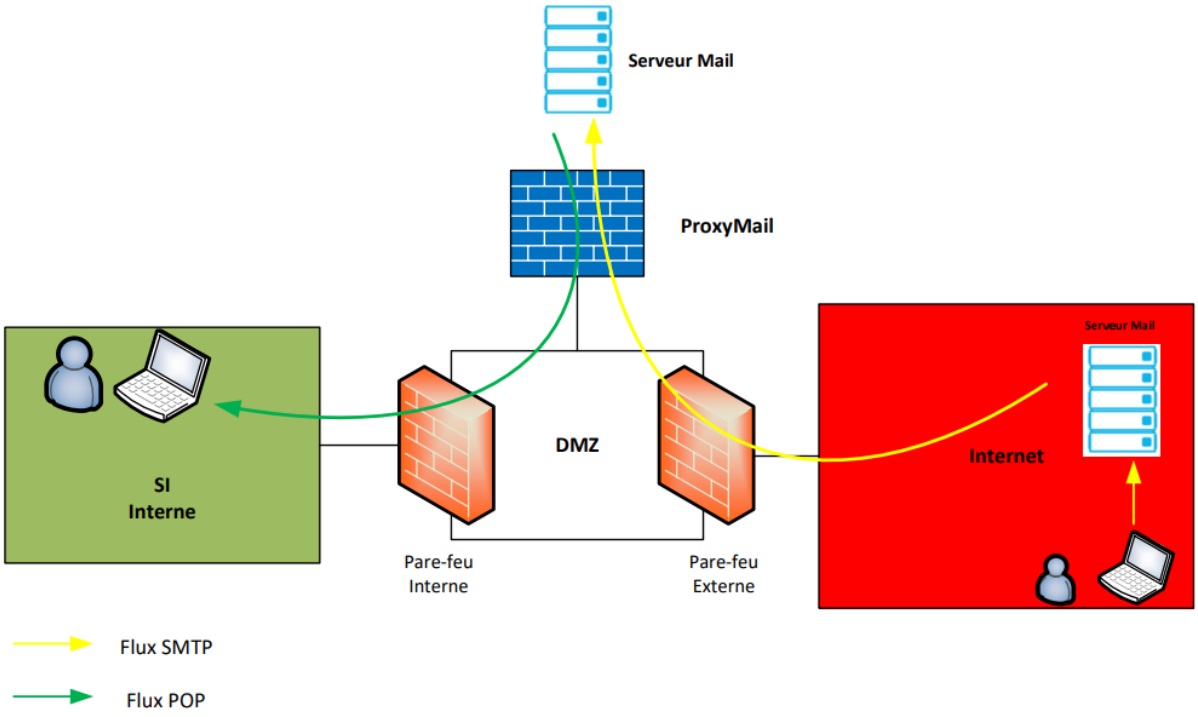


Figure 88: Architecture cible avec ProxyMail

7.2.3 Sécurité des accès aux ressources systèmes

Pour renforcer la sécurité des accès aux ressources sensibles du système d'information de l'Université de Lomé, nous proposons d'implémenter une solution de gestion des accès privilégiés (PAM - Privileged Access Management).

Cette solution permettra de sécuriser, contrôler, surveiller et auditer les connexions des utilisateurs ayant des privilèges élevés (administrateurs systèmes, responsables réseau, etc.), en offrant un contrôle centralisé sur les accès aux applications, serveurs et équipements critiques.

7.2.3.1 Avantages du PAM

Les avantages de l'implémentation d'un PAM sont :

- Contrôle et gestion des accès privilégiés : il permet de contrôler finement les accès des utilisateurs privilégiés, en définissant des politiques d'accès et en attribuant des permissions spécifiques en fonction des rôles.
- Sécurisation des sessions d'administration : En enregistrant et surveillant toutes les actions effectuées pendant une session privilégiée, il offre un audit détaillé et une traçabilité complète des opérations effectuées par les administrateurs.
- Réduction des risques d'accès non autorisés : La solution bloque les accès non autorisés en temps réel et empêche les tentatives d'escalade de privilèges, contribuant à limiter les risques liés aux erreurs humaines ou à la compromission des comptes privilégiés.
- Supervision et audit des accès : Toutes les sessions d'accès privilégié sont enregistrées sous format vidéo pour des sessions RDP et SSH ou texte pour uniquement des sessions SSH, offrant ainsi une visibilité complète et un historique détaillé des actions effectuées, ce qui facilite la détection d'activités anormales ou malveillantes.

7.2.3.1 Mise en œuvre du PAM

Nous recommandons Wallix Bastion comme solution PAM.

Son architecture est la suivante :

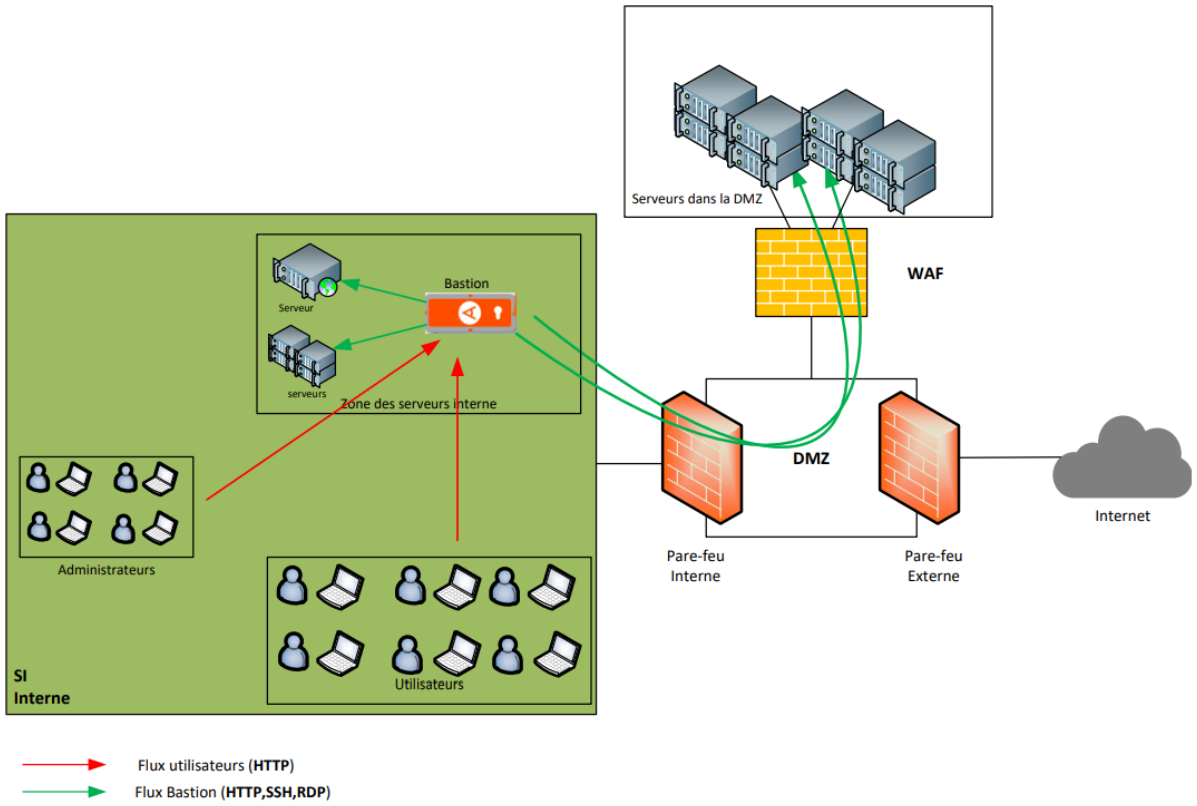


Figure 89: Architecture cible avec WAF et PAM

7.2.4 Sécurité des accès physiques

La sécurité des accès physiques est un élément essentiel de la protection d'un Système d'Information (SI). Elle vise à empêcher l'accès non autorisé aux infrastructures critiques (datacenters, salles serveurs, bureaux IT, etc.), réduisant ainsi les risques de sabotage, de vol ou d'intrusion.

Lorsqu'un accès physique n'est pas contrôlé efficacement, plusieurs menaces peuvent survenir. On peut citer :

- **Intrusion non autorisée** : Accès non contrôlé aux salles serveurs par du personnel non habilité.
- **Vol ou altération de matériel** : Un attaquant pourrait subtiliser ou endommager des équipements critiques.
- **Risque de sabotage** : Une personne malveillante pourrait déconnecter des serveurs, insérer un périphérique infecté ou altérer des systèmes.
- **Attaques sur les câbles et réseaux** : Un accès non sécurisé aux équipements réseau pourrait permettre une interception des communications ou une attaque réseau.

Nous avons constaté qu'aucun contrôle d'accès n'est actuellement en place pour réguler l'entrée et la sortie des salles serveurs de l'Université de Lomé, ce qui entraîne un manque de traçabilité et de sécurisation des accès.

Bien que des caméras de surveillance soient installées dans ces salles, cela reste insuffisant, car elles ne permettent pas d'empêcher une intrusion non autorisée en temps réel.

À cet effet, nous recommandons la mise en place d'un système de contrôle d'accès sécurisé, intégrant :

- Badges RFID/NFC ou authentification biométrique pour restreindre l'accès aux seuls personnels autorisés.
- Gestion centralisée des accès permettant de définir des niveaux d'autorisation selon les rôles et responsabilités.
- Journalisation des accès avec enregistrement des entrées et sorties pour une meilleure traçabilité.
- Système d'alerte en cas d'accès non autorisé (tentative de forçage, badge non reconnu, etc.).

Cette solution permettra de renforcer la sécurité physique des infrastructures critiques et de limiter les risques d'intrusion ou de manipulation non autorisée des équipements sensibles.

L'architecture finale proposée à la partie sécurité est la suivante :

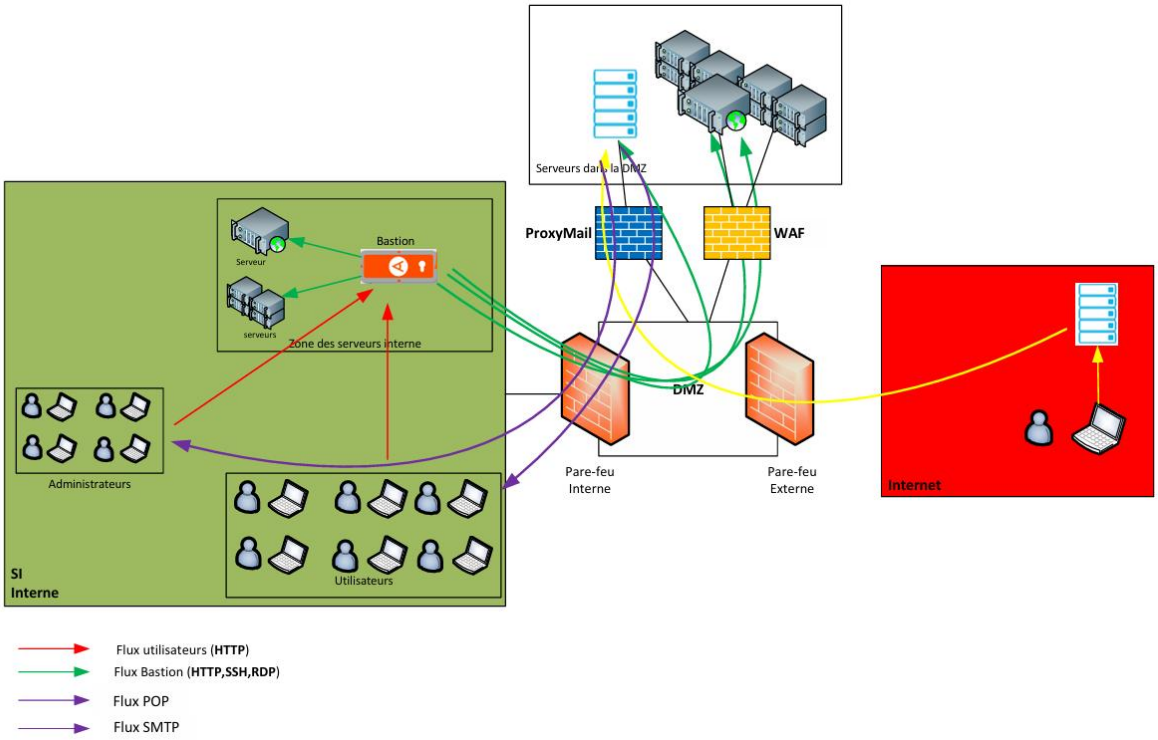


Figure 90: Architecture cible finale avec les solutions proposées

7.3 Gestion des identités et des accès

L'Université de Lomé ne dispose actuellement pas d'un système d'authentification centralisé pour la gestion des utilisateurs et des ressources du système d'information. Cette absence entraîne plusieurs problématiques :

- Multiplication des identifiants : Chaque utilisateur doit gérer plusieurs comptes distincts pour accéder aux différents services.
- Gestion des accès non sécurisée : L'attribution et la révocation des droits d'accès ne sont pas uniformisées, augmentant le risque d'accès non autorisés.
- Absence de traçabilité : Il est difficile de suivre et d'auditer les actions des utilisateurs sur le réseau.

Nous proposons ainsi la mise en place d'un Active Directory (AD**)** basé sur Microsoft Windows Server ou une alternative open-source comme Samba AD basé sur la distribution Linux pour centraliser la gestion des accès et des ressources informatiques.

Les bénéfices attendus sont entre autres :

- Authentification unique (SSO) : Chaque utilisateur aura un identifiant unique pour accéder à l'ensemble des services (messagerie, fichiers partagés, applications, Wi-Fi, etc.).
- Gestion centralisée des droits : Attribution et révocation des accès selon les rôles et départements (principe du moindre privilège).
- Sécurisation renforcée : Mise en place de politiques de sécurité (mots de passe complexes, authentification multifactorielle, etc.).
- Traçabilité et audibilité : Suivi des connexions et des actions effectuées pour détecter les anomalies et garantir la conformité.
- Automatisation et simplification de l'administration : Ajout/suppression des utilisateurs facilité, gestion optimisée des groupes et des ressources partagées.

La mise en place d'un Active Directory apportera une meilleure gestion des accès, une sécurisation accrue du SI et une réduction de la charge administrative pour le personnel IT.

7.4 Solution de sauvegarde sur NAS et bandes

Il convient de noter que, malgré la criticité des données gérées par l'Université de Lomé, notamment celles des étudiants, aucune solution de sauvegarde formelle et structurée n'a été mise en place. Actuellement, les sauvegardes sont effectuées de manière traditionnelle sur des disques stockés à des emplacements non sécurisés et non centralisés.

Cette situation expose le système d'information à un risque élevé de perte de données en cas d'incident (panne matérielle, cyberattaque, sinistre, etc.). Or, les sauvegardes constituent la dernière ligne de défense en cas de problème. Une gestion inadéquate des sauvegardes pourrait entraîner une perte irrémédiable d'informations essentielles, compromettant ainsi la continuité des services et la fiabilité du SI.

7.4.1 Stratégie de sauvegarde

Nous recommandons la mise en place d'une stratégie de sauvegarde robuste comprenant :

- Une solution de sauvegarde automatisée et centralisée.
- L'application de la règle 3-2-1 (3 copies, sur 2 supports différents, dont 1 hors site).
- Une segmentation et sécurisation des sauvegardes pour éviter toute compromission en cas de cyberattaque.
- Le chiffrement des sauvegardes effectuées
- Une politique de tests réguliers pour garantir la fiabilité des restaurations.

Cette approche garantira la protection et la disponibilité des données critiques de l'université.

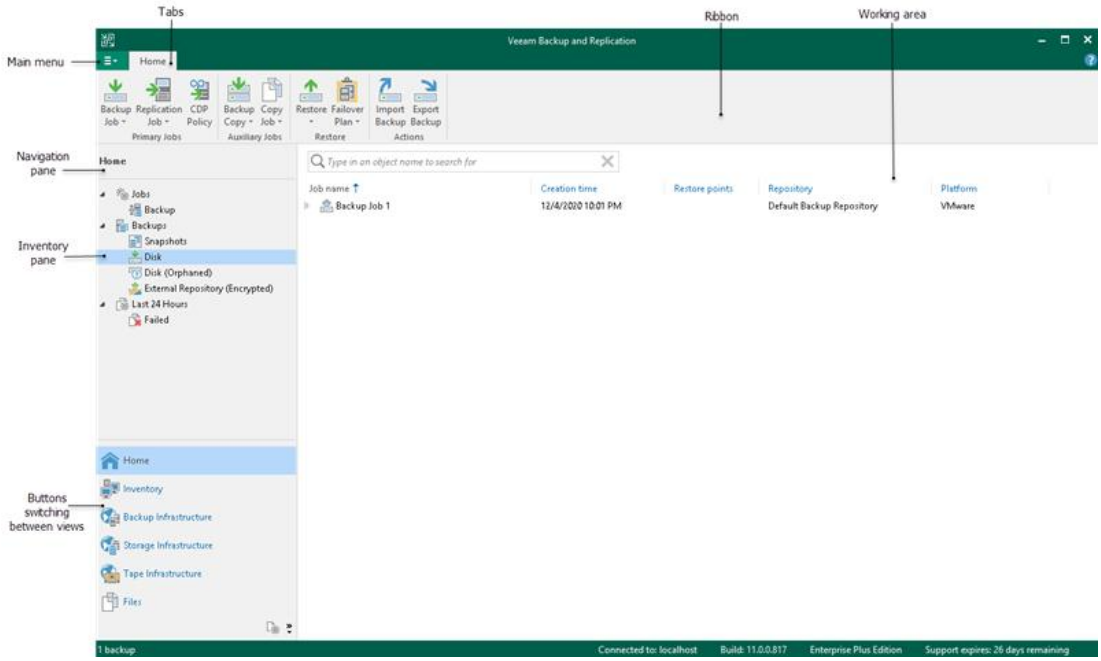
7.4.2 Mise en œuvre de la solution de sauvegarde

Afin de garantir la pérennité et la protection des données critiques de l'Université de Lomé, nous recommandons la mise en place de Veeam Backup & Replication, leader du marché en matière de sauvegarde et de reprise après sinistre.

Les principales fonctionnalités de Veeam Backup & Replication sont les suivantes :

- Sauvegarde : sauvegardes de machines virtuelles, physiques, cloud, sauvegardes de fichiers partagés NAS et stockage objet.
- Restauration : restauration à partir de fichiers de sauvegarde vers l'emplacement d'origine ou vers un nouvel emplacement.
- Réplication : création d'une copie exacte d'une VM et maintien de la copie en synchronisation avec la VM d'origine.
- Protection continue des données (CDP) : technologie de réplication qui aide à protéger les VM critiques et à atteindre un objectif de point de récupération (RPO) pouvant aller jusqu'à quelques secondes, c'est à dire restaurer en quelque secondes une machine virtuelle indépendamment de sa taille.
- Copie de sauvegarde (Backup Copy) : copie des fichiers de sauvegarde vers un Repository secondaire.
- Intégration aux baies de stockage : sauvegarde et restauration des machines virtuelles en utilisant les snapshots natifs de baie de stockage créés sur les systèmes de stockage.
- Sauvegarde sur bande : stockage des copies de sauvegarde sur bande.
- Test de restauration : test des sauvegardes et des réplicas des machines virtuelles avant la restauration.

L'ergonomie de l'interface graphique de Veeam Backup & Replication permet de trouver rapidement les commandes de gestion et d'administration.



Matériel de sauvegarde recommandé :

- Deux NAS de sauvegarde, dimensionnés selon le volume des données à sauvegarder.
- Deux serveurs LTO (Linear Tape-Open) pour l'archivage sur bande.
- Bandes LTO pour garantir une rétention longue durée et une protection contre les cyberattaques.
- Un espace de sauvegarde dans le Cloud pour la restauration des données en cas de sinistre sur le site de l'Université de Lomé
- Deux coffrets ignifuges pour la protection des bandes LTO contre les incendies, l'humidité et les chocs physiques.

Répartition et Redondance des Équipements

Les équipements seront installés selon le principe de séparation géographique afin d'assurer une résilience accrue :

Salle serveur principale

- Un NAS de sauvegarde pour stocker les sauvegardes locales.
- Un serveur LTO pour la sauvegarde sur bande.
- Un coffret ignifuge

Salle serveur PRA (site secondaire)

- Un second NAS de sauvegarde pour la redondance.
- Un second serveur LTO pour la continuité des sauvegardes sur bande.
- Un second coffret ignifuge

Les avantages de cette architecture sont entre autres :

- Protection contre les pertes de données grâce à une sauvegarde multi-niveaux (disque + bande + Cloud).
- Amélioration du temps de récupération (RTO/RPO optimisés) en cas d'incident.
- Réduction des risques de cyberattaques avec des sauvegardes air-gapped sur bandes LTO.
- Mise en conformité avec les bonnes pratiques et exigences en matière de gestion des données.

Cette solution assure une sauvegarde fiable, évolutive et sécurisée, garantissant ainsi la disponibilité et l'intégrité des données stratégiques de l'Université de Lomé.

7.5 Solution EDR pour une protection avancée

Face à l'évolution des cybermenaces de plus en plus sophistiquées, il est essentiel pour l'Université de Lomé d'adopter une approche proactive et moderne en matière de cybersécurité.

Traditionnellement, les solutions antivirus reposent sur une détection basée sur des signatures : elles comparent les fichiers et applications à une base de données de logiciels malveillants connus, puis prennent des mesures correctives (quarantaine ou suppression). Cependant, cette approche est limitée face aux nouvelles menaces Zero-Day, aux ransomwares évolutifs et aux attaques ciblées.

Ainsi, nous recommandons l'implémentation d'une solution de type EDR (Endpoint Detection and Response).

7.5.1 Avantages de l'EDR

Contrairement aux antivirus classiques, l'EDR intègre des technologies avancées telles que : L'apprentissage automatique et l'intelligence artificielle pour identifier des comportements suspects en temps réel.

- ❖ L'analyse comportementale pour détecter les menaces connues et inconnues, y compris celles qui n'ont pas encore de signature spécifique.

- ❖ Une visibilité accrue sur les activités des points de terminaison (serveurs, postes de travail, équipements réseau) pour identifier les anomalies.
- ❖ Une réponse rapide et automatisée en cas d'attaque

7.5.2 Mise en œuvre de la solution EDR

Parmi les solutions EDR leaders du marché, nous recommandons **CrowdStrike Falcon**, reconnu pour :

- **Une protection avancée basée sur le cloud** : CrowdStrike Falcon fonctionne sans nécessiter d'infrastructure lourde sur site, ce qui facilite son déploiement et sa gestion.
- **Une détection proactive des menaces** : Grâce à l'intelligence artificielle et l'apprentissage automatique, il identifie et neutralise les menaces avant qu'elles ne puissent causer des dommages.
- **Une analyse comportementale en temps réel** : Falcon surveille en continu l'activité des endpoints et détecte toute anomalie ou activité suspecte, même en l'absence de signature connue.
- **Une réponse rapide et automatisée** : En cas de détection d'une menace, la solution peut isoler automatiquement les endpoints compromis, bloquer les processus malveillants et neutraliser l'attaque en quelques secondes.
- **Une visibilité complète sur l'ensemble du SI** : La plateforme fournit des rapports détaillés et une traçabilité des événements de sécurité, facilitant ainsi l'analyse des incidents et la mise en place de mesures préventives.
- **Une faible empreinte sur les performances des endpoints** : Contrairement aux solutions antivirus traditionnelles, CrowdStrike Falcon est conçu pour fonctionner efficacement sans ralentir les systèmes protégés.

L'intégration de **CrowdStrike Falcon** au sein du SI de l'Université de Lomé permettra de renforcer significativement la sécurité des endpoints, de réduire les risques d'attaques et d'améliorer la réactivité face aux menaces potentielles.

7.6 Solution de gestion des mises à jour et vulnérabilités

Au vu de la quantité non négligeable de vulnérabilités identifiées dans le SI de l'Université de Lomé, il est primordial qu'elle se dote d'une solution de gestion des mises à jour et des vulnérabilités afin de :

- Automatiser l'application des correctifs : Assurer le déploiement rapide et efficace des mises à jour de sécurité pour les systèmes d'exploitation, applications et équipements réseau, réduisant ainsi les fenêtres d'exposition aux attaques.

- Centraliser la gestion des vulnérabilités **:** Avoir une visibilité en temps réel sur l'état des actifs du SI, identifier les failles critiques et prioriser les correctifs en fonction du niveau de risque.
- Réduire la surface d'attaque : En corrigeant les vulnérabilités dès leur découverte, on limite les opportunités d'exploitation par les cybercriminels et on améliore la résilience globale du SI.

L'implémentation d'une telle solution garantira une meilleure sécurité et une réduction des risques liés aux failles de sécurité présentes dans l'environnement informatique de l'Université de Lomé, car, en réalité, les vulnérabilités sont la principale source des cyberattaques.

En effet, les cybercriminels exploitent les failles de sécurité pour pénétrer dans les systèmes et mener des attaques variées telles que le vol de données, les ransomwares, ou encore l'espionnage industriel. La gestion proactive des mises à jour et des vulnérabilités est donc essentielle pour empêcher ces attaques en fermant les portes d'entrée que représentent les faiblesses du système.

En éliminant ces vulnérabilités, l'Université pourra réduire significativement le risque d'attaques informatiques, assurer la confidentialité des données sensibles, et maintenir la continuité des services critiques.

Nous recommandons la solution SolarWinds pour la gestion des mises à jour et vulnérabilités à l'Université de Lomé.

7.7 Solution de centralisation et de corrélation des logs (SIEM)

Actuellement, l'Université de Lomé ne dispose pas d'une solution de gestion centralisée des logs, ce qui rend difficile la surveillance continue de son infrastructure informatique. Les incidents de sécurité peuvent passer inaperçus, augmentant ainsi les risques liés aux cyberattaques. La centralisation et la corrélation des logs sont essentielles pour garantir une visibilité complète et une détection rapide des anomalies ou des événements de sécurité.

Pour renforcer la sécurité du Système d'Information (SI) de l'Université, nous recommandons la mise en place d'un SIEM (Security Information and Event Management) pour centraliser et corréler les logs provenant des différents dispositifs, applications et services au sein de l'infrastructure.

7.7.1 Objectifs du SIEM

Les objectifs d'une solution SIEM sont :

- Centralisation des logs : Le SIEM permet de centraliser les journaux d'événements provenant de l'ensemble des systèmes, équipements réseau, applications et serveurs. Cela permet d'avoir une vue unifiée et complète des événements de sécurité.
- Corrélation des logs : La corrélation des logs permet de relier différents événements de sécurité pour identifier des attaques complexes qui peuvent se manifester sous forme de comportements suspects sur plusieurs systèmes. Par exemple, une tentative d'accès non autorisée à partir d'un terminal peut être mise en relation avec d'autres événements pour identifier une attaque de type "Brute Force" ou une compromission de compte.
- Détection des menaces en temps réel : En analysant les logs en temps réel, le SIEM permet de détecter des comportements anormaux, des vulnérabilités exploitées, des intrusions ou des tentatives de déviation des processus sécurisés. Cela réduit le temps de réaction aux incidents et minimise leur impact.
- Réponse automatisée aux incidents : Le SIEM peut être configuré pour automatiser certaines réponses aux incidents, comme l'isolement de dispositifs compromis, l'envoi d'alertes aux équipes de sécurité, ou même l'exécution de mesures correctives de manière autonome.
- Analyse et reporting : Grâce à des outils de reporting avancés, le SIEM facilite la création de rapports sur les activités critiques du réseau, les tentatives d'accès non autorisées, et les attaques détectées. Ces rapports peuvent également être utilisés pour les audits de sécurité et la conformité.

7.7.2 Solution SIEM recommandée

Nous recommandons **ELK Stack (Elasticsearch, Logstash, Kibana)**, une solution SIEM open-source populaire pour la collecte, l'analyse et la visualisation des logs. Il peut être adapté pour les infrastructures de taille variable.

7.8 Mise en place d'une équipe SOC dédiée ou externalisée

L'Université de Lomé, tout comme de nombreuses autres institutions, fait face à une évolution rapide des menaces informatiques. La cybercriminalité devient de plus en plus sophistiquée, et la gestion proactive de la sécurité devient primordiale. Cependant, avec la complexité croissante des cybermenaces, une simple gestion réactive des incidents ne suffit plus. Il est essentiel d'avoir une équipe spécialisée capable de surveiller, détecter et répondre rapidement à toute tentative d'intrusion ou incident de sécurité.

Ainsi**,** nous recommandons la mise en place d'une équipe SOC (Security Operations Center), soit internes à l'Université de Lomé ou externalisées par le biais d'un fournisseur de services spécialisés, afin de renforcer la capacité de l'université à gérer la cybersécurité de manière proactive.

7.8.1 Objectifs du SOC

La mise en place d'une équipe SOC donne droit aux avantages suivants :

- Surveillance continue : Un SOC permet une surveillance 24/7 du Système d'Information (SI), ce qui garantit la détection en temps réel des anomalies et des incidents de sécurité.
- Détection proactive des menaces : L'équipe SOC sera responsable de l'identification des attaques potentielles avant qu'elles n'impactent le SI. Grâce à des outils avancés comme les SIEM, les EDR et l'analyse comportementale, un SOC peut repérer des attaques inconnues ou nouvelles, même sans signatures de malware.
- Réponse rapide aux incidents : L'équipe SOC peut intervenir immédiatement en cas de détection d'une anomalie, en analysant l'incident, en contenant la menace, et en initiant des actions de remédiation (isolation d'un serveur, blocage d'une adresse IP malveillante, etc.).
- Amélioration continue de la sécurité : Grâce à la gestion des incidents et à l'analyse post-incident, un SOC fournit des retours précieux pour améliorer la sécurité du SI de l'université. Ces retours peuvent être utilisés pour ajuster les politiques de sécurité, les outils de défense et les contrôles existants.
- Reporting et conformité : Un SOC génère des rapports détaillés qui peuvent être utilisés pour la conformité avec des normes de sécurité et des régulations telles que le ISO 27001.

7.8.2 Mise en œuvre

7.8.2.1 Option 1 : SOC interne dédié

Cette option permet à l'Université de Lomé de disposer d'une équipe SOC directement en interne. Cette équipe pourrait être composée de :

- **Analystes SOC** (niveau 1, 2 et 3) : Chargés de surveiller les alertes de sécurité, d'analyser les incidents et de gérer les réponses aux incidents.
- **Responsable SOC** : Un leader expérimenté pour superviser les opérations du SOC et coordonner les interventions de sécurité.
- **Experts en cybersécurité** : Pour gérer les incidents complexes, effectuer des analyses forensiques et assurer l'amélioration continue des systèmes de sécurité.
- **Outils et infrastructure** : L'université devra investir dans les technologies nécessaires (SIEM, EDR, IDS/IPS) pour équiper le SOC de manière efficace.

Avantages du SOC interne :

- Contrôle total sur les opérations de sécurité.
- Proximité avec l'infrastructure IT de l'université, ce qui permet une gestion plus ciblée des incidents.
- Un meilleur alignement avec les objectifs stratégiques de l'université.

Inconvénients du SOC interne :

- Coûts de recrutement, de formation et de gestion d'une équipe spécialisée.
- Besoin d'un investissement substantiel dans les outils de sécurité et l'infrastructure.
- Risque de surcharge de travail ou d'inexpérience si l'équipe SOC est trop petite ou non qualifiée.

7.8.2.2 Option 2 : SOC externalisé

Dans cette option, l'Université de Lomé fait appel à un fournisseur tiers spécialisé dans les services SOC. Ce fournisseur prend en charge la surveillance continue, la détection et la réponse aux incidents de sécurité, en mettant à disposition une équipe dédiée de professionnels.

Avantages du SOC externalisé :

- **Expertise spécialisée** : Les fournisseurs de services SOC disposent souvent d'une expertise pointue et de technologies de pointe pour gérer les menaces avancées.
- **Économies de coûts** : L'externalisation permet à l'Université d'éviter des coûts liés au recrutement, à la formation et à la gestion de personnel interne. Le modèle de paiement par abonnement permet également de mieux gérer les coûts.
- **Flexibilité** : Une équipe SOC externalisée peut être rapidement mise en place et n'a pas besoin de la même gestion quotidienne qu'une équipe interne.
- **Surveillance 24/7** : Les fournisseurs de SOC externalisés disposent souvent des ressources nécessaires pour fournir une surveillance continue sans contraintes horaires.

Inconvénients du SOC externalisé :

- Moins de contrôle direct sur les opérations et la gestion des incidents.
- Dépendance vis-à-vis du fournisseur : en cas de problèmes avec le prestataire, cela peut affecter la gestion de la cybersécurité.

Nous recommandons de confier le service SOC de l'Université de Lomé à **CDA (Cyber Defense Agency)**, un fournisseur de services spécialisés en cybersécurité. Cette solution externalisée permet à l'université de bénéficier d'une expertise avancée en matière de sécurité, tout en ayant accès à des ressources et des outils spécialisés sans devoir investir massivement dans des infrastructures internes.

7.8.3 Conclusion

La mise en place d'un SOC dédié ou externalisé est une nécessité pour l'Université de Lomé afin de renforcer la cybersécurité de son infrastructure. Qu'il soit interne ou externalisé, un SOC améliorera la détection des menaces, optimisera la réponse aux incidents et réduira les risques liés à la cybersécurité. Ce dispositif permet à l'Université de disposer d'une protection proactive et réactive contre les cyberattaques, garantissant ainsi la continuité de ses services et la sécurité des données sensibles.

7.9 Mise en place de tests d'intrusion réguliers

Les tests d'intrusion (ou **pentests**) sont une composante clé de toute stratégie de cybersécurité efficace. Ils permettent de simuler des attaques réelles sur le système d'information afin de détecter des vulnérabilités, d'évaluer la résistance du système aux attaques externes et internes et de mettre en évidence les faiblesses dans les mécanismes de défense en place.

Nous recommandons la mise en place de tests d'intrusion réguliers, effectués par des experts en sécurité, pour identifier les vulnérabilités critiques, valider l'efficacité des contrôles de sécurité en place et garantir que les mesures de protection et de détection des menaces fonctionnent correctement.

7.9.1 Objectifs du Test d'Intrusion

Les tests d'intrusion ont pour objectifs :

- Identification des vulnérabilités : Détecter les failles de sécurité et les vulnérabilités dans les systèmes, applications, bases de données et infrastructures réseaux.
- Évaluation de la résistance aux attaques : Tester la capacité du SI à résister aux attaques réelles, telles que les injections SQL, les attaques XSS, l'élévation de privilèges, les attaques par déni de service (DoS) et d'autres menaces exploitant les faiblesses de sécurité.
- Validation des contrôles de sécurité : Évaluer les mécanismes de défense existants tels que les pares-feux, les systèmes de détection d'intrusion (IDS), la segmentation du réseau et l'authentification multifacteur pour s'assurer qu'ils sont efficaces.
- Tests sur la protection des données sensibles **:** Vérifier que les données sensibles des étudiants et du personnel sont bien protégées contre les accès non autorisés, qu'il s'agisse de données en transit ou de données au repos.
- Réactivité aux attaques **:** Tester la capacité du personnel en charge de la sécurité à détecter, répondre et atténuer les incidents de sécurité rapidement et efficacement

7.9.2 Fréquence des tests d'intrusion

Nous proposons d'effectuer ces tests au moins une fois par an ou après toute modification importante de l'infrastructure, des applications ou des processus métier, afin de garantir une couverture continue des risques de sécurité. En fonction des évolutions technologiques ou des menaces, ces tests peuvent être réalisés plus fréquemment.

7.9.3 Conclusion

La mise en place de tests d'intrusion réguliers est essentielle pour renforcer la cybersécurité de l'Université de Lomé. Ces tests permettent de simuler des attaques réelles, de détecter les vulnérabilités et d'identifier des mesures correctives pour protéger les infrastructures critiques, assurer la confidentialité des données et garantir la continuité des services. Ils doivent être réalisés de manière régulière pour répondre aux menaces et aux défis évolutifs en matière de cybersécurité.

7.10 Mise en place d'une plateforme de sensibilisation des utilisateurs

L'un des maillons les plus vulnérables d'un système d'information est l'utilisateur final. Les cyberattaques modernes exploitent souvent des failles humaines via l'ingénierie sociale, les phishing, l'utilisation de mots de passe faibles, ou encore le manque de vigilance face aux menaces numériques.

À l'Université de Lomé, il est donc crucial de renforcer la culture de cybersécurité auprès des enseignants, du personnel administratif et dans la mesure du possible des étudiants à travers une plateforme de sensibilisation et de formation continue.

Nous recommandons la mise en place d'une plateforme dédiée qui servira à :

- Former et sensibiliser les utilisateurs aux bonnes pratiques en matière de cybersécurité
- Tester et évaluer régulièrement leur niveau de connaissance à travers des simulations et des exercices pratiques
- Diffuser des alertes de sécurité en cas de menaces ou d'attaques détectées
- Donner accès à des ressources pédagogiques (vidéos, articles, webinaires, guides interactifs)

7.10.1 Solution recommandée et fonctionnalités clés de la plateforme

Nous recommandons l'utilisation de la plateforme Terranova Security pour la sensibilisation et la formation des utilisateurs.

Elle dispose des fonctionnalités clé suivantes :

Modules de formation interactifs

- Cours sur les bonnes pratiques de cybersécurité : gestion des mots de passe, protection des données personnelles, détection des emails frauduleux (phishing), etc.
- Simulations de cyberattaques pour évaluer la réaction des utilisateurs face à une tentative de phishing ou d'ingénierie sociale.
- Sensibilisation aux règles d'utilisation des équipements informatiques et des accès réseau de l'Université.

Campagnes de simulation de phishing

- Envoi régulier de faux emails de phishing pour tester la vigilance des utilisateurs.
- Analyse des résultats et identification des profils les plus vulnérables.
- Formation ciblée pour les personnes ayant cliqué sur des liens malveillants.

Évaluation et certification interne

- Quiz et tests périodiques pour mesurer l'évolution du niveau de sensibilisation des utilisateurs.
- Attestation de sensibilisation à la cybersécurité pour les étudiants et le personnel.

Alertes et actualités en cybersécurité

- Diffusion de bulletins de sécurité et d'alertes sur les menaces émergentes.
- Conseils pratiques pour se protéger contre les attaques en cours.

Accès à une assistance et à des ressources

- Foire aux questions (FAQ) sur les incidents courants.
- Possibilité de signaler un email suspect ou une tentative de fraude.
- Guides et vidéos accessibles à tous les utilisateurs.

7.10.2 Bénéfices pour l'Université de Lomé

Les avantages d'une telle initiative sont :

- La réduction des risques humains : Les utilisateurs deviennent des acteurs actifs de la sécurité et non des cibles faciles.
- L'amélioration de la posture de cybersécurité **:** Un personnel mieux formé limite les incidents liés aux erreurs humaines.
- La réduction des coûts liés aux incidents **:** Moins de pertes de données, de pannes et d'attaques réussies.

7.10.3 Conclusion

La cybersécurité est une responsabilité partagée, et l'éducation des utilisateurs est un pilier essentiel de la stratégie de défense de l'Université de Lomé. La mise en place d'une plateforme de sensibilisation permettra de créer une culture de cybersécurité, de minimiser les erreurs humaines et d'améliorer la protection globale du système d'information contre les menaces internes et externes.

7.11 Élaboration et mise en place d'une documentation structurée du SI

L'absence de documentation formelle du Système d'Information (SI) de l'Université de Lomé, notamment une Politique de Sécurité des Systèmes d'Information (PSSI), des chartes d'utilisation et des procédures opérationnelles, constitue une faiblesse majeure.

Sans ces référentiels, l'administration du SI manque de directives claires, ce qui entraîne :

- Une gestion non homogène de la sécurité et des accès
- Une mauvaise sensibilisation des utilisateurs aux bonnes pratiques
- Un manque de cadre pour l'application des mesures de cybersécurité
- Une difficulté à répondre aux exigences réglementaires et aux audits de sécurité

Nous recommandons la création et l'implémentation des documents essentiels suivants :

7.11.1 Politique de Sécurité des Systèmes d'Information (PSSI)

Ce document définit les règles et principes de protection du SI, ainsi que les responsabilités des différentes parties prenantes. Il a pour objectifs de :

- Définir une gouvernance de la sécurité informatique
- Fixer des exigences claires en matière de cybersécurité
- Harmoniser les pratiques de gestion du SI
- Réduire les risques de failles de sécurité

7.11.2 Charte d'Utilisation des Systèmes d'Information

Ce document encadre l'utilisation des ressources numériques de l'Université (ordinateurs, messagerie, accès internet, outils collaboratifs, etc.).
Il a pour objectifs de :

- Sensibiliser les utilisateurs aux bonnes pratiques

- Définir les comportements interdits
- Définir les responsabilités des utilisateurs et des administrateurs

7.11.3 Procédures de gestion et d'exploitation du SI

C'est une Série de documents opérationnels qui détaillent les processus internes du SI :

- Procédure de gestion des accès et des droits utilisateurs
- Procédure de gestion des incidents de sécurité
- Procédure de sauvegarde et de restauration des données
- Procédure de gestion des mises à jour et des correctifs de sécurité
- Procédure de réponse aux cyberattaques

7.11.4 Plan de Reprise et de Continuité d'Activité (PRA/PCA)

Décrit les actions à mettre en place en cas d'incident majeur (cyberattaque, panne critique, catastrophe naturelle) pour garantir la continuité des services informatiques.

Il a pour objectifs de :

- Assurer la disponibilité des services en cas de crise
- Réduire les temps d'arrêt des systèmes critiques
- Préparer une réponse efficace face aux cybermenaces

7.11.5 Schéma directeur

Afin d'aligner le Système d'Information (SI) de l'Université de Lomé sur ses objectifs stratégiques et d'assurer sa modernisation, nous recommandons la rédaction d'un Schéma Directeur du Système d'Information (SDSI).

Il a pour objectifs de :

- Définir une vision stratégique du SI en cohérence avec les ambitions de l'université.
- Planifier les évolutions technologiques et les projets SI prioritaires.
- Optimiser la gouvernance du SI pour une gestion plus efficace et sécurisée.
- Améliorer la performance et la résilience des infrastructures et services numériques.

7.12 Mise en place d'une solution Helpdesk

Dans le but d'améliorer la gestion des incidents à l'université de Lomé, nous recommandons la mise en place d'une solution Helpdesk centralisée et performante.

7.12.1 Objectifs d'une solution Helpdesk

Les objectifs de la mise en œuvre d'une solution Helpdesk sont :

- L'optimisation de la gestion des demandes et incidents liés aux services IT.
- L'amélioration de la réactivité des équipes techniques face aux problèmes rencontrés par les utilisateurs.
- Facilitation de la communication entre les utilisateurs et le support IT.

7.12.1 Solution recommandée

Nous proposons GLPI, une solution open-source robuste et flexible.

7.13 Recommandations sur la partie électrique

7.13.1 Equipements de mesure

- **CONTRÔLEUR D'INSTALLATION**

  ICT, CA6116N

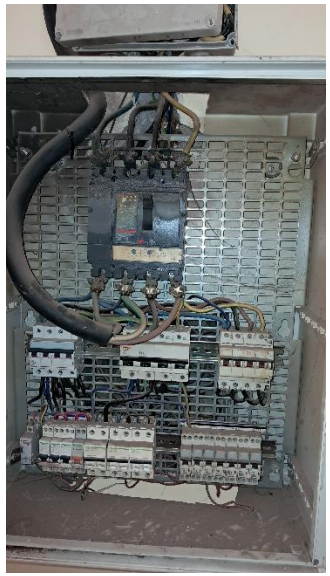
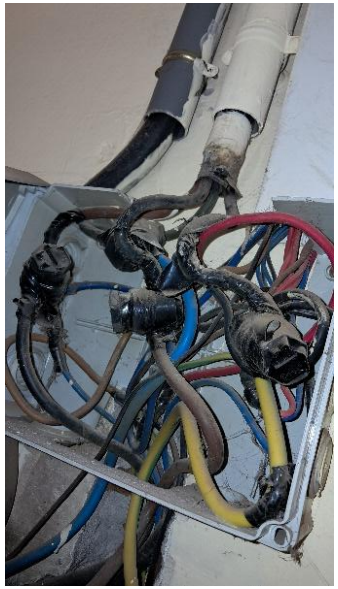
  Fonctions

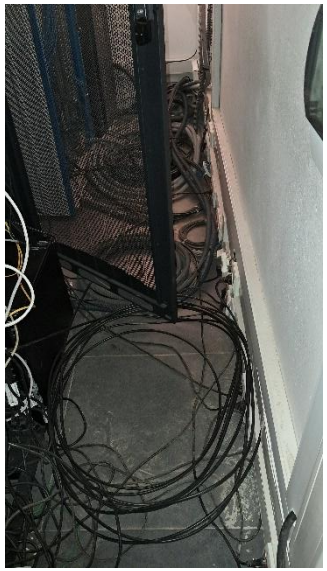
- ✓ Mesure de continuité ;
- ✓ Mesure d'isolement ;
- ✓ Mesure de résistance de prise de terre ;
- ✓ Mesure de tension et de courant ;
- ✓ Tests différentiels.

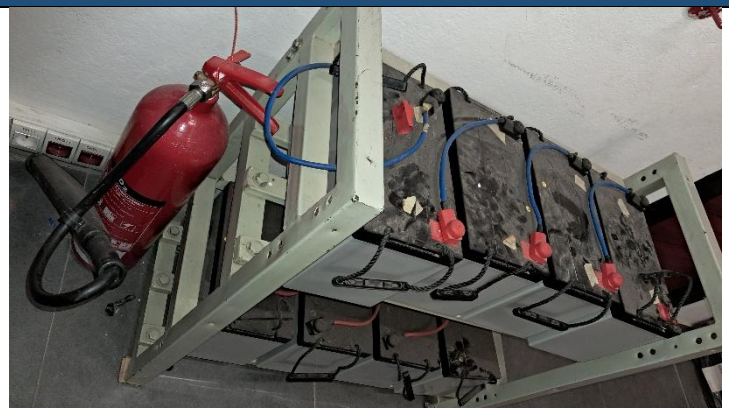
7.13.2 Référentiel

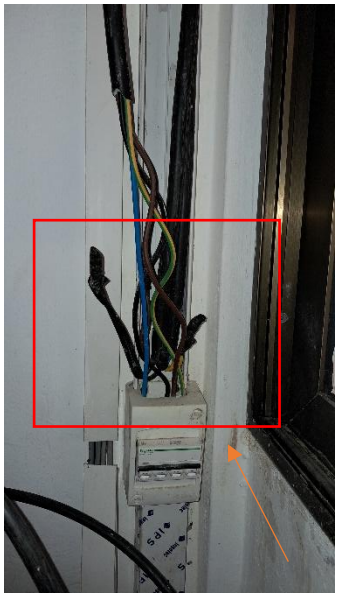
Textes applicables	
Code du travail togolais	Loi n°2006 – 010 du 13 décembre 2006 portant Code du travail.
Arrêté du 26 décembre 2011	Relatif aux vérifications ou processus de vérification des installations électriques ainsi, qu'au contenu des rapports correspondants.
Arrêté du 25 juin 1980	Relatif à la prévention du risque incendie et de panique dans les établissements recevant du public
Norme NF C 15 – 100	Relatif aux installations électriques à basse tension.
Guide UTE C 15 – 105	Relatif à la détermination des sections des conducteurs et aux choix des dispositifs de protection.
Guide UTE C 15 – 401	Relatif aux règles d'installation des groupes électrogènes.
Guide UTE C 15 – 443	Relatif à la protection des installations à basse tension, contre les surtensions d'origine atmosphérique.
Guide UTE C 15 – 520	Relatif au mode de pose des conducteurs et aux connexions des conducteurs – Installation à basse tension.

7.13.3 Bilan de l'inspection

RECAPITULATIF DES OBSERVATIONS			
I.	**ORIGINE DE LA DISTRIBUTION ELECTRIQUE**		
1	 **Photo P01**	 **Photo P02**	Mettre en œuvre des gaines thermo rétractables en lieu et en place du ruban adhésif, pour l'isolation des parties actives. Ce dernier ne devant servir qu'à isoler temporairement un conducteur hors tension. Mettre en œuvre des borniers de raccordement dédiés avec une fixation adéquate, pour éviter le contact entre les bornes, engendrer un court-circuit et un départ d'incendie. Les connexions devront avoir un indice de protection IP2X **Réf. : Art. 526 / NF C 15 –100** **Réf. : Art. 526.5 / NF C 15 –100**

RECAPITULATIF DES OBSERVATIONS			
II. LOCAUX SERVEURS			
1	 **Photo P03**	 **Photo P04**	Eviter l'encombrement des locaux à risques particuliers. Limiter aux strictes nécessaires pour l'exploitation ou la fonctionnalité. **Réf. : Art. 422.1.1 / NF C 15 –1 00**

RECAPITULATIF DES OBSERVATIONS		
2	 **Photo P05**	Assurer la dépose des équipements non utilisés. Limiter les équipements aux strictes nécessaires pour l'exploitation ou la fonctionnalité. **Réf. : Art. 422.1.1 / NF C 15 –1 00**
3	 **Photo P06**	Les tableaux électriques devront présenter un indice de protection IP2XX et être obturé en partie basse, notamment au niveau des passages de câbles. Ces dispositions permettent d'éviter que ne s'y introduisent des rongeurs et des reptiles, pouvant favoriser des risques de court-circuit sur les bornes actives. Assurer l'identification et le repérage des appareillages de façon durable avec des étiquettes. **Réf. : Art. 512.2 / NF C 15 –1 00**

RECAPITULATIF DES OBSERVATIONS			
4	 **Photo P07**	 **Photo P08**	Faire des raccordements directs, éviter les épissures et fermer les goulottes. Les câbles ne doivent pas pendre sous l'effet de leur poids. Il faut un fourreau de passage et calfeutrer ensuite. **Réf. : Art. 526 / NF C 15 –1 00**
III. SYSTEME DE CONDITIONNEMENT D'AIR | ACCES A LA SALLE | PRISE DE TERRE			

RECAPITULATIF DES OBSERVATIONS		
5	 **Photo P09**  **Photo P10**	*Nous notons dans chaque local serveur, la présence de deux climatiseurs qui assurent le conditionnement d'air. Le fonctionnement s'opère simultanément afin de maintenir la bonne température de fonctionnement des serveurs.* *Bien que le fonctionnement et la température n'appellent pas d'observations particulières, il est à noter que les climatiseurs installés ne sont pas ceux adaptés aux environnements de data centrer. Nous avons à faire à des* ***climatiseurs de confort*** *destinés aux usages communes (bureaux, chambres etc.)* *Les équipements adaptés sont des* ***climatiseurs de précision****. Ils génèrent la température appropriée aux serveurs et par la même occasion, contrôlent l'humidité environnante afin d'empêcher la condensation non perceptible et néfastes aux plaquettes électroniques des machines du local serveur.*

RECAPITULATIF DES OBSERVATIONS		
7	 **Photo P10**	Disposer sur l'accès à la salle serveur, d'une porte CF1H munie de barre antipanique et, s'ouvrant dans le sens de l'évacuation. **Réf. : Art. EL5§3 / Ar. 25 juin 1980**
8	 **Photo P11**	*La mesure de la prise de terre a été effectuée par la méthode des 62%.* *Valeur ohmique : **0.59 Ω*** *Les données de la mesure de terre sont jugées **favorables**.*

RECAPITULATIF DES OBSERVATIONS

OBSERVATIONS ET RECOMMANDATIONS D'ORDRE TRANSVERSALES

01- Le bâtiment a visiblement subi, de nombreux travaux d'extension et de modifications. Toutefois, il ne paraît pas que ceux-ci aient été mise en œuvre dans le cadre d'études parfaitement réalisé. En effet, nous notons l'absence de pièces graphiques et écrites actualisées, décrivant et représentant les installations.

02- En cas de réhabilitation, un bureau devra procéder à des études d'exécution, et faire valider par un organisme de contrôle technique, avant mise en œuvre sur le terrain. L'objectif étant de conformer au mieux le bâtiment.

03- L'absence ou l'inefficacité d'un système ASI (Alimentation Sans Interruption) dans les salles serveurs représente une faille de taille dans l'installation. Il est recommandé de mettre en place un onduleur central dans chaque salle, avec une distribution bien structurée à partir de disjoncteurs adaptés aux environnements serveurs.

04- Les coffrets électriques à partir desquels les serveurs seront alimentés doivent être munis en amont de parafoudres et de leurs déconnexions pour luter contre les effets indirects de la foudre. Chaque serveur doit être doté de deux départs différentiels pour favoriser l'alimentation de chaque patch d'alimentation redondante.

05- Dans la mesure du possible, créer un faux plancher pour faciliter l'acheminement des câbles. Cela pallierait l'encombrement des salles avec les éventuels nouveaux passages de câbles.

7.14 Recommandations sur la partie sécurité incendie

7.14.1 Introduction

À la suite de notre visite d'expertise des locaux du datacenter de l'UL, nous avons remarqué qu'il n'y a pas une installation du système de sécurité incendie qui pourrait alerter et gérer l'extinction automatique en cas du feu.

Selon la norme NF EN 15004-1 spécifiant des exigences et donnant des recommandations pour la conception, l'installation, les essais, la maintenance et la sécurité des systèmes d'extinction à gaz dans les bâtiments, nous vous proposons les recommandations suivantes pour les deux salles serveurs.

7.14.2 Description des salles serveurs

- La salle serveurs située à l'étage du bâtiment DRSI donne des dimensions suivantes : (Longueur=4.84m ; largeur=4.50m et hauteur=2.95m)
- La salle serveurs située au RDC du bâtiment DRSI donne des dimensions suivantes : (Longueur=4.20m ; largeur=3.40m et hauteur=3.13m)

7.14.3 Recommandations

7.14.3.2 Salle serveur R+1

- Prévoir une installation de détection et extinction automatique d'incendie à gaz FK-5-1-12 chargé à 56 kg dans une bouteille de 67l (voir résultat de calcul à la page
- Remplacer les vitres des anciennes fenêtres (Longueur 4.50m ; largeur=1.17m) par des vitres blindées afin de pouvoir supporter la pression de service du gaz du système d'extinction automatique qui est de 42bar
- Remplacer la porte d'entrée par une porte blindée coupe-feu résistant au feu d'une (01) heure en maintenant l'intégrité de la salle en cas d'incendie
- Prévoir du faux plancher technique pour le passage des câbles
- Prévoir un dispositif de mesure automatique de la température et du taux d'humidité dans la salle.
- Prévoir un système d'asservissement téléphonique pour les installations du système d'extinction et d'hygrométrie de la salle permettant d'appeler les premiers responsables en cas d'un incident.

7.14.3.2 Salle serveur RDC

- Prévoir une installation de détection et extinction automatique d'incendie à gaz **FK-5-1-12** chargé à 41kg dans une bouteille de 67l (voir résultat de calcul à la page 4)
- Remplacer les vitres des anciennes fenêtres (Longueur 3.40m ; largeur=1.15m) par des vitres blindées afin de pouvoir supporter la pression de service du gaz du système d'extinction automatique qui est de 42bar
- Remplacer l'ancienne séparation par une nouvelle à base de mur en agglo (voir photo ci-dessous) pour assurer l'étanchéité de la salle.
- Prévoir une porte blindée coupe-feu résistant au feu d'une (01) heure à l'entrée de la séparation créée
- Prévoir du faux plancher technique pour le passage des câbles
- Prévoir un dispositif de mesure automatique de la température et du taux d'humidité dans la salle.
- Prévoir un système d'asservissement téléphonique pour les installations du système d'extinction et d'hygrométrie de la salle permettant d'appeler les premiers responsables en cas d'un incident.

Ci-après les images illustrant les calculs effectués pour les futures recommandations

SIEMENS
Ingenuity for life

FK-5-1-12

Edition 2.03
08-2022

Back

Customer :	CIC
Location :	LOME
Made by :	SIEMENS
Room name :	SALLE SERVEUR R+1
Risk type :	ELECTRIQUE
Date :	07 03 2025
Remarks :	

Dimensions of the protected buildings:	Volume 1	Volume 2	Volume 3
Lenght	4,84 m	0,00 m	0,00 m
Width	4,50 m	0,00 m	0,00 m
Height	2,95 m	0,00 m	0,00 m
Calculated floor surface	21,8 m2		
Customized floor surface			
Cross volume	64,3 m3		
Volume to be deducted			
Volume to be added			
Calculated net volume	64,3 m3		
Customized net volume			
Global calculated net volume		64,3 m3	
Regulation		ISO 14520	ed.2016
Protected risk / C%	002 - Class A Higher hazard	002 - Class A Higher hazard	002 - Class A Higher hazard
Required concentration	5,60 %	5,60 %	5,60 %
Room temperature	20 °C	20 °C	20 °C
Altitude	150 m	Coef. 1,000	

Calculation amount of FK-5-1-12 necessary			
Specific volume of FK-5-1-12	0,0719 m3/kg	0,0719 m3/kg	0,0719 m3/kg
Mass of FK-5-1-12 required	0,8253 kg/m3	0,8253 kg/m3	0,8253 kg/m3
Mass of FK-5-1-12 required per volume	53,0 kg	0,0 kg	0,0 kg
Total quantity of FK-5-1-12	53,0 kg	+ mass of FK-5-1-12 lost per cylinder	

Help to choose the nozzles		Volume 1	Volume 2	Volume 3
Discharge time			10 second(s)	
Flow		5,3 kg/sec		
Quantity of layers		1		
Maximum coverage area per nozzle		30,0 m2	30,0 m2	30,0 m2
Minimal quantity of nozzle		0,7		
Quantity of nozzles per layer to supply the flow	3/8"	6		
	1/2"	3		
	3/4"	2		
	1"	1		
	1"1/4	1		
	1"1/2	1		
	2"	1		

Remark: the calculation of nozzles quantit
information and valid only if they are central
they arewall mounted, the quantity mu

	Max flow nozzle
	3/8"
	1/2"
	3/4"
	1"
	1"1/4
	1"1/2
	2"

Careful : if the filling ratio is too high yo
to calculate the piping. Then number o
have to be increased.

	Configuration	Centralized		
Cylinder volume	Total gas	Lost mass per cylinder	Quantity of cylinders	Gas mass per cylinder	Filling ratio
67 L	**55,0 kg**	**2,0 kg**	**1**	**55,0 kg**	**0,82 kg/l**
120 L	57,0 kg	4,0 kg	1	57,0 kg	0,48 kg/L
80 L	55,0 kg	2,0 kg	1	55,0 kg	0,69 kg/L
67 L	55,0 kg	2,0 kg	1	55,0 kg	0,82 kg/L
32 L	57,0 kg	2,0 kg	2	28,5 kg	0,9 kg
16 L	61,0 kg	1,6 kg	5	12,2 kg	0,8 kg
7 L	64,0 kg	1,0 kg	11	5,8 kg	0,8 kg

Calculation of the bidirectional venting flap based on the VdS equations			Calculation with ζ=	1,8
Discharge time		10 second(s)		
		Volume 1	Volume 2	Volume 3
Acceptable overpressure		1 mbar	1 mbar	1 mbar
DUCT DOWNSTREAM FLAP	Duct flow section (m²)			
	Equivalent duct circular diameter			
	Duct length (m)			
	Number of bends 90°			
	Inner duct material	Galvanized steel	Galvanized steel	Galvanized steel
	Rugosity (mm)	0,15	0,15	0,15
	Estimated pressure loss in the duct	0,00 mbar	0,00 mbar	0,00 mbar
Minimum required net opening of venting surface without duct		0,050 m2		
Minimum required opening of the venting surface with proposed duct				

Figure 91: Calcul Sécurité Incendie

SIEMENS
Ingenuity for life

FK-5-1-12

Edition 2.03
08-2022

Back

Customer :	CIC
Location :	LOME
Made by :	SIEMENS
Room name :	SALLE SERVEUR RDC
Risk type :	ELECTRIQUE
Date :	07 03 2025
Remarks :	

Dimensions of the protected buildings:	Volume 1	Volume 2	Volume 3
Lenght	4,20 m	0,00 m	0,00 m
Width	3,40 m	0,00 m	0,00 m
Height	3,13 m	0,00 m	0,00 m
Calculated floor surface	14,3 m2		
Customized floor surface			
Cross volume	44,7 m3		
Volume to be deducted			
Volume to be added			
Calculated net volume	44,7 m3		
Customized net volume			
Global calculated net volume		44,7 m3	
Regulation	ISO 14520		ed.2016
Protected risk / C%	002 - Class A Higher hazard	002 - Class A Higher hazard	002 - Class A Higher hazard
Required concentration	5,60 %	5,60 %	5,60 %
Room temperature	20 °C	20 °C	20 °C
Altitude	150 m	Coef. 1,000	

Calculation amount of FK-5-1-12 necessary			
Specific volume of FK-5-1-12	0,0719 m3/kg	0,0719 m3/kg	0,0719 m3/kg
Mass of FK-5-1-12 required	0,8253 kg/m3	0,8253 kg/m3	0,8253 kg/m3
Mass of FK-5-1-12 required per volume	36,9 kg	0,0 kg	0,0 kg
Total quantity of FK-5-1-12	36,9 kg	+ mass of FK-5-1-12 lost per cylinder	

Help to choose the nozzles		Volume 1	Volume 2	Volume 3
Discharge time			10 second(s)	
Flow		3,7 kg/sec		
Quantity of layers		1		
Maximum coverage area per nozzle		30,0 m2	30,0 m2	30,0 m2
Minimal quantity of nozzle		0,5		
Quantity of nozzles per layer to supply the flow	3/8"	4		
	1/2"	2		
	3/4"	2		
	1"	1		
	1"1/4	1		
	1"1/2	1		
	2"	1		

Remark: the calculation of nozzles quantit
information and valid only if they are central
they arewall mounted, the quantity mu

Max flow nozzle
3/8"
1/2"
3/4"
1"
1"1/4
1"1/2
2"

Careful : if the filling ratio is too high yo
to calculate the piping. Then number o
have to be increased.

Configuration			Centralized		
Cylinder volume	Total gas	Lost mass per cylinder	Quantity of cylinders	Gas mass per cylinder	Filling ratio
67 L	**38,9 kg**	**2,0 kg**	**1**	**38,9 kg**	**0,58 kg/l**
120 L	#VALEUR!	4,0 kg	1	Filling ratio too low	#VALEUR!
80 L	38,9 kg	2,0 kg	1	38,9 kg	0,49 kg/L
67 L	38,9 kg	2,0 kg	1	38,9 kg	0,58 kg/L
32 L	40,9 kg	2,0 kg	2	20,4 kg	0,6 kg
16 L	41,7 kg	1,6 kg	3	13,9 kg	0,9 kg
7 L	43,9 kg	1,0 kg	7	6,3 kg	0,9 kg

Calculation of the bidirectional venting flap based on the VdS equations			Calculation with C=	1,8
Discharge time		10 second(s)		
		Volume 1	Volume 2	Volume 3
Acceptable overpressure		1 mbar	1 mbar	1 mbar
DUCT DOWNSTREAM FLAP	Duct flow section (m²)			
	Equivalent duct circular diameter			
	Duct length (m)			
	Number of bends 90°			
	Inner duct material	Galvanized steel	Galvanized steel	Galvanized steel
	Rugosity (mm)	0,15	0,15	0,15
	Estimated pressure loss in the duct	0,00 mbar	0,00 mbar	0,00 mbar
Minimum required net opening of venting surface without duct		0,035 m2		
Minimum required opening of the venting surface with proposed duct				

Figure 92: Calcul Sécurité Incendie