MÉMOIRE FIN DE FORMATION POUR L'OBTENTION DU DIPLÔME DE LICENCE PROFESSIONNELLE

OPTION : TELECOMMUNICATIONS ET INFORMATIQUE

SPÉCIALITÉ : ADMINISTRATION & SECURITE DES RESEAUX

THÈME

Etude et sécurisation d'une architecture réseau critique pour garantir la disponibilité des services

Sous la direction de

Dr James **KOUAWA**

Enseignant – chercheur à l'ESMT

Présenté et soutenu par

Mme Madeleine BIAYE

Promotion 2022 - 2025

Août 2025

ETUDE ET SECURISATION D'UNE INFRASTRUCTURE RESEAU CRITIQUE POUR GARANTIR LA DISPONIBILITE DES SERVICES

AVANT PROPOS

Ce travail a été réalisé dans le cadre de ma formation en cycle de Licence en Télécommunications et Informatique, au cours de l'année de spécialisation en Administration et Sécurité des Réseaux Informatiques (ASR) à l'ESMT.

L'Ecole Supérieure Multinationale des Télécommunications (ESMT) située à Dakar, a été créée en 1981 à l'initiative de sept pays d'Afrique de l'Ouest (Bénin, Burkina Faso, Mali, Mauritanie, Niger, Sénégal, Togo), dans le cadre d'un projet du Programme des Nations Unies pour le développement (PNUD), avec le soutien de l'UIT, et de la coopération française, canadienne et suisse. La Guinée Conakry a rejoint les membres fondateurs en 1998.

L'ESMT est une institution multinationale qui a pour vocation de former des diplômés (Techniciens supérieurs, Licences, Ingénieurs, Masters, Mastères spécialisés) dans les domaines techniques et managériaux des télécommunications/TIC.

Le sujet de ce mémoire découle d'une réflexion approfondie sur les défis actuels en matière de cybersécurité. En observant l'augmentation des attaques informatiques ciblant la disponibilité des services dans les réseaux critiques (banques, hôpitaux, transports), je me suis posé les questions suivantes : ***Comment concevoir un réseau capable de continuer à fonctionner, même en cas d'attaque ? Les solutions classiques suffisent-elles encore aujourd'hui ? Quelle architecture permettrait réellement de garantir la disponibilité ?***

Ces interrogations ont été renforcées par plusieurs lectures, cours, et échanges avec mon encadrant, et m'ont naturellement conduit à choisir comme sujet de mémoire :
« Etude et sécurisation d'une architecture réseau critique pour garantir la disponibilité des services ».

Ce travail s'inscrit ainsi dans une volonté de **proposer une solution moderne, robuste et réaliste**, face aux failles des modèles traditionnels, en m'appuyant notamment sur l'approche **Zéro Trust**, devenue une référence dans la protection des systèmes critiques.

DEDICACE

Je dédie ce travail à toute ma famille : mon père, ma mère, ma sœur, mes oncles et tantes, mes cousins et cousines, ainsi qu'à mes amis.

REMERCIEMENTS

Ce mémoire n'aurait pu voir le jour sans la miséricorde d'Allah, Le Tout-Puissant. Je Lui exprime toute ma gratitude et prie sur Son noble prophète et messager Mouhamed (paix et salut sur lui).

Je tiens à rendre un hommage sincère à mes parents, dont l'amour, la patience et le soutien inconditionnel ont été la base de mon éducation, de mon épanouissement personnel et de mon parcours académique. Mon père, toujours engagé à m'offrir les meilleures conditions de réussite, et ma mère, par sa tendresse, sa disponibilité et sa foi en moi, m'ont apporté un équilibre aussi bien moral que matériel.

Je remercie également ma tante , véritable modèle de persévérance et de sagesse, pour sa présence constante, ses conseils précieux et son soutien moral tout au long de cette aventure.

Mes plus profonds remerciements vont au **Dr James Kouawa**, Enseignant-Chercheur à l'ESMT, pour son encadrement rigoureux, sa disponibilité et ses conseils techniques tout au long de la réalisation de ce mémoire.

Je n'oublie pas **Monsieur Mady Mbodj**i étudiant en Master en Sécurité des Systèmes d'Information, pour l'aide précieuse qu'il m'a apportée tant sur le plan technique que stratégique et moral.

Je remercie chaleureusement l'ensemble du corps enseignant et administratif de l'ESMT pour la qualité de la formation dispensée, leur disponibilité, leur écoute et leur engagement à transmettre leur savoir.

Un merci tout particulier à mes camarades de classe pour leur soutien continu, leur esprit d'équipe et les nombreuses heures de collaboration enrichissantes.

Enfin, j'exprime ma gratitude à toutes les personnes, connues ou anonymes, qui ont, de près ou de loin, contribué à la réussite de ce mémoire.

GLOSSAIRE :

Infrastructure critique : Ensemble de ressources, systèmes ou installations essentiels au bon fonctionnement de la société (santé, finance, énergie…), dont la défaillance peut entraîner des conséquences graves.

Transformation digitale : Processus d'intégration des technologies numériques dans les activités d'une organisation afin d'en améliorer l'efficacité, l'accessibilité et la performance.

Architecture réseau : Structure logique et physique d'un réseau informatique, définissant comment les composants (routeurs, serveurs, clients…) sont interconnectés.

Réseau informatique : Ensemble d'équipements interconnectés permettant la transmission, le partage et l'accès à des données ou des services numériques.

Disponibilité des services : Capacité d'un système ou d'un service à rester accessible et fonctionnel au moment voulu par les utilisateurs.

Résilience : Capacité d'un système à maintenir son fonctionnement ou à se rétablir rapidement après une perturbation (panne, attaque…).

PRA (Plan de Reprise d'Activité) : Ensemble de procédures permettant de rétablir les services critiques après un incident majeur.

PCA (Plan de Continuité d'Activité) : Ensemble des mesures mises en place pour assurer la continuité des services essentiels en cas de crise.

Menace : Tout événement ou action susceptible de compromettre la confidentialité, l'intégrité ou la disponibilité d'un système d'information.

Vulnérabilité : Faiblesse ou faille dans un système pouvant être exploitée pour compromettre sa sécurité.

Cyberattaque : Tentative malveillante d'exploiter des failles dans un système informatique pour en compromettre l'intégrité, la disponibilité ou la confidentialité.

Déni de service (DoS) : Attaque visant à rendre un service inaccessible en saturant le système avec un grand nombre de requêtes.

Déni de service distribué (DDoS) : Variante du DoS lancée simultanément depuis plusieurs sources compromises (botnets), la rendant plus puissante.

Botnet : Réseau de machines infectées contrôlées à distance par un attaquant, utilisé pour mener des attaques massives (ex. : DDoS).

Ransomware : Logiciel malveillant qui chiffre les données d'un système et demande une rançon pour restituer l'accès.

Phishing : Technique de fraude visant à tromper l'utilisateur pour qu'il divulgue des informations sensibles via un message falsifié.

Intrusion interne : Menace provenant d'un utilisateur autorisé (employé, prestataire…) qui abuse de ses accès ou commet une erreur compromettante.

Politique du moindre privilège : Principe consistant à limiter les droits d'un utilisateur ou d'un processus au strict nécessaire.

Défaillance technique : Incident non malveillant causé par une panne matérielle, un bug logiciel ou une erreur de configuration.

UEBA (User and Entity Behavior Analytics) : Méthode de détection d'anomalies basée sur l'analyse du comportement des utilisateurs et des entités réseau.

SOC (Security Operations Center) : Centre de surveillance chargé de détecter, analyser et réagir face aux incidents de cybersécurité.

SIEM (Security Information and Event Management) : Plateforme centralisant et corrélant les journaux de sécurité pour détecter des incidents en temps réel.

MFA (Multi-Factor Authentication) : Méthode d'authentification nécessitant plusieurs facteurs (mot de passe, appareil, biométrie…) pour valider l'identité d'un utilisateur.

IAM (Identity and Access Management) : Système de gestion des identités et des accès aux ressources numériques, basé sur des rôles ou des règles.

Zéro Trust (ZTA) : Modèle de sécurité fondé sur le principe « ne jamais faire confiance, toujours vérifier », qui impose une validation continue de chaque accès.

ZTNA (Zero Trust Network Access) : Approche de contrôle d'accès réseau fondée sur l'identité, le contexte et le risque, limitant l'accès aux ressources aux utilisateurs vérifiés.

Micro-segmentation : Technique consistant à diviser le réseau en segments isolés pour limiter la propagation des attaques.

EDR (Endpoint Detection and Response) : Solution de détection et de réponse aux menaces ciblant les terminaux (ordinateurs, serveurs…).

SASE (Secure Access Service Edge) : Architecture cloud intégrant sécurité réseau et connectivité pour les utilisateurs distants.

CARTA (Continuous Adaptive Risk and Trust Assessment) : Approche adaptative de la sécurité évaluant le niveau de risque et de confiance en temps réel et de manière continue.

Cloud-native security : Sécurité spécifiquement conçue pour les environnements cloud, intégrée dès la phase de développement (DevSecOps).

CNAPP (Cloud-Native Application Protection Platform) : Plateforme intégrée protégeant les applications cloud natives dans l'ensemble du cycle de vie.

CSPM (Cloud Security Posture Management) : Outil permettant de surveiller et corriger les configurations incorrectes dans les environnements cloud.

Blockchain : Technologie de registre distribué, immuable et décentralisé, garantissant la transparence et la traçabilité des échanges.

SSI (Self Sovereign Identity) : Modèle d'identité numérique décentralisée permettant à un utilisateur de contrôler directement son identité sans autorité centrale.

Routeur : Appareil réseau assurant la liaison entre différents réseaux et dirigeant les paquets de données vers leur destination.

Switch (commutateur) : Équipement réseau connectant les dispositifs d'un réseau local et gérant la circulation du trafic interne.

Pare-feu (Firewall) : Dispositif de sécurité qui filtre le trafic réseau selon des règles prédéfinies pour bloquer ou autoriser certaines connexions.

ACL (Access Control List) : Mécanisme de contrôle d'accès définissant quels utilisateurs ou équipements peuvent accéder à quelles ressources réseau.

VLAN (Virtual Local Area Network) : Réseau local virtuel permettant de segmenter logiquement un réseau physique pour isoler des flux ou des services.

Proxy : Serveur intermédiaire permettant de filtrer, surveiller ou rediriger les requêtes entre les utilisateurs et Internet.

DMZ (Demilitarized Zone) : Zone neutre du réseau où sont placés les services accessibles depuis l'extérieur tout en étant isolés du réseau interne.

Pentest (Test d'intrusion) : Simulation d'attaque informatique visant à identifier les vulnérabilités d'un système pour les corriger avant exploitation.

Scan de vulnérabilités : Analyse automatique des failles potentielles dans un réseau ou un système informatique.

ELK Stack / Splunk : Plateformes d'analyse centralisée des journaux (logs) permettant la détection, la corrélation et la traçabilité des incidents.

Nessus / OpenVAS : Outils de scan de vulnérabilités servant à identifier les failles de sécurité dans les systèmes et réseaux.

Metasploit / Burp Suite : Frameworks de tests d'intrusion permettant de simuler des attaques et d'automatiser l'identification des failles.

Wazuh : Plateforme open-source pour la surveillance de sécurité, la détection d'intrusions et l'analyse de conformité.

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTES DES CAPTURES

CAP

SOMMAIRE

INTRODUCTION

La transformation digitale aux services numériques a profondément transformé le fonctionnement des institutions, entreprises et infrastructures stratégiques. Si cette numérisation apporte des gains notables en efficacité et en accessibilité, elle expose également ces systèmes à des risques majeurs, notamment celui de l'indisponibilité des services. Ces interruptions, qu'elles soient causées par des pannes, des erreurs humaines ou des cyberattaques, peuvent entraîner des conséquences graves, surtout lorsqu'elles touchent des secteurs critiques comme la santé, les finances ou les transports.

Dans ce contexte, la garantie de la disponibilité des services devient un enjeu prioritaire pour les responsables qui gèrent les architectures réseaux. De nombreuses attaques informatiques modernes ciblent justement ce pilier fondamental : déni de service distribué (DDoS), ransomwares, intrusions internes… Si les méthodes classiques : sécurité périmétrique, VLAN, ACL, pare-feu apportent une première couche de défense, elles se révèlent de plus en plus inefficace face à l'évolutivité et la robusticité des menaces.

Parmi les solutions émergentes, le modèle Zéro Trust s'impose comme une alternative efficace. Basé sur le principe du « ne jamais faire confiance, toujours vérifier », il remet en question les modèles de confiance traditionnels en misant sur une vérification systématique de chaque accès, qu'il soit interne ou externe, en fonction du contexte, de l'identité et du comportement. Ainsi il pourrait constituer une alternative pour apporter une deuxième couche de sécurité.

Ce mémoire vise donc à proposer une architecture réseau sécurisée et résiliente, capable de garantir la disponibilité continue des services, même en cas d'incident. Pour cela, nous nous appuierons sur les principes du Zéro Trust et sur des outils modernes de cybersécurité.

Notre réflexion s'articulera en trois grandes parties , dans un premier temps, nous analyserons les enjeux de sécurité des infrastructures critiques et les menaces pesant sur leur disponibilité ; dans un second temps, nous comparerons les approches de sécurité existantes en identifiant leurs forces et limites ; enfin, nous proposerons une architecture Zéro Trust adaptée, que nous validerons à travers des simulations ciblées.

CHAPITRE 1 : CADRE ORGANISATIONNEL ET PRÉSENTATION DU SUJET

Ce premier chapitre, divisé en deux grandes sections, constitue une introduction au mémoire. Il permet de comprendre le contexte institutionnel dans lequel s'inscrit ce travail ainsi que la réflexion ayant conduit au choix du sujet. Dans une première partie, nous présenterons l'environnement organisationnel d'accueil, à savoir l'ESMT. Dans la seconde, nous reviendrons sur les motivations et enjeux qui ont conduit à la formulation du sujet portant sur la **conception et la sécurisation d'une architecture réseau critique pour garantir la disponibilité des services**.

1.1 Cadre organisationnel

1.1.1 Présentation de l'institution d'accueil

L'**École Supérieure Multinationale des Télécommunications (ESMT)** est une institution inter-États créée en 1981 par sept pays africains membres de l'Union Africaine des Télécommunications (UAT), avec le soutien de l'Union Internationale des Télécommunications (UIT) et du Programme des Nations Unies pour le Développement (PNUD). Elle est basée à Dakar, au Sénégal.

L'ESMT a pour mission principale de **former des ingénieurs et techniciens de haut niveau** dans les domaines des télécommunications, de l'informatique, de la cybersécurité, du numérique et de la gestion des réseaux. Elle se positionne comme un centre d'excellence pour le renforcement des compétences techniques en Afrique, et contribue activement à la stratégie de transformation numérique du continent.

À travers ses programmes de formation initiale, continue et professionnelle, l'ESMT répond aux besoins des administrations, des entreprises publiques et privées, et des opérateurs télécoms dans toute l'Afrique francophone.

1.1.2 Missions de l'ESMT

L'ESMT remplit plusieurs missions clés, notamment : Former des cadres qualifiés dans les domaines des technologies de l'information, des réseaux, de la cybersécurité, de l'intelligence artificielle et de la régulation des télécommunications ;

- Contribuer à la recherche appliquée et au développement technologique dans ses domaines de spécialisation ;
- Accompagner les États et les entreprises dans la mise en œuvre de projets liés au numérique et à l'optimisation des infrastructures télécoms ;
- Renforcer la coopération régionale et internationale, en tant qu'établissement panafricain d'enseignement supérieur.

1.1.3 Gouvernance

La gouvernance de l'ESMT s'appuie sur une architecture institutionnelle rigoureuse, fondée sur des mécanismes participatifs et hiérarchisés :

- Le Conseil des Ministres (CM) constitue l'organe décisionnel suprême. Il définit les grandes orientations stratégiques de l'institution.
- Le Conseil d'Administration (CA) est chargé de la gestion stratégique globale. Il valide les choix pédagogiques, budgétaires et administratifs majeurs.
- Le Conseil Scientifique et Pédagogique, composé d'experts du monde académique, veille à la qualité de l'enseignement, à la pertinence des contenus pédagogiques ainsi qu'à l'encadrement des activités de recherche.
- Le Directeur Général, en sa qualité de responsable exécutif, assure la mise en œuvre des décisions du Conseil d'Administration. Il est assisté dans ses fonctions par plusieurs structures techniques, notamment :
    - ❖ Le Secrétariat Particulier et le Pool de Conseillers,
    - ❖ Le service d'Audit et de Contrôle de Gestion.

1.1.4 Organisation interne

L'organisation interne de l'ESMT repose sur une structuration fonctionnelle articulée autour de **trois directions principales**, chacune regroupant des départements spécialisés assurant la mise en œuvre opérationnelle des missions de l'institution :

1.1.4.1 : Secrétariat Général

Chargé de la coordination administrative globale, le Secrétariat Général supervise l'ensemble des services supports et assure le bon fonctionnement des activités transversales. Il englobe notamment :

- Le Service de Secrétariat Administratif
- Le Département ESMT Entreprise
- Le Département Scolarité, Information, Stage et Placement
- Le Département des Ressources Humaines, Moyens Généraux et Achats
- Le Département Marketing et Développement Institutionnel

1.1.4.2 : Direction Financière et Comptable

Responsable de la gestion budgétaire et comptable, cette direction veille à la soutenabilité financière de l'ESMT. Elle encadre deux départements essentiels :

- Le Département Comptabilité et Fiscalité
- Le Département Finance, Trésorerie et Recouvrement

1.1.4.3 : Direction de l'Enseignement, de la Formation et de la Recherche

Pilier académique de l'institution, cette direction organise l'offre de formation, encadre la recherche et supervise les activités pédagogiques. Elle comprend :

- Le Département de la Formation Continue
- Le Département ESMT TIC
- Le Département ESMT Management
- Le Département FOAD (Formation Ouverte à Distance)
- Le Département Recherche et Innovation
- Le Centre de Ressources Techniques (CRT)

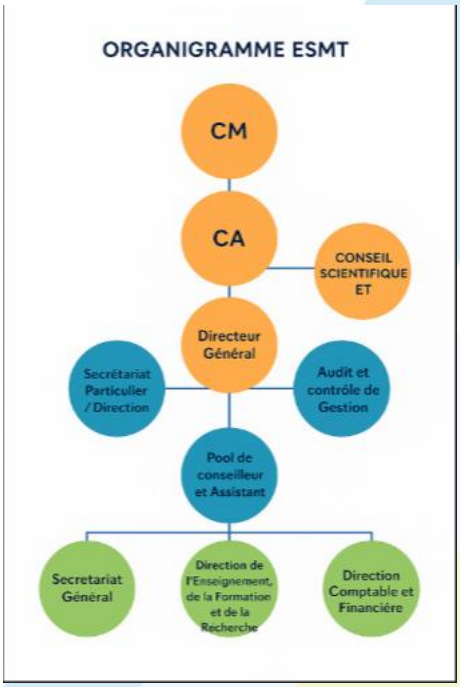


figure 1 : organigramme de l'ESMT

1.2 Présentation du sujet

1.2.1 Contexte

Dans un monde de plus en plus connecté, les infrastructures réseau critiques qu'il s'agisse d'hôpitaux, de systèmes bancaires, de services publics ou de plateformes de communication sont devenues essentielles au bon fonctionnement de nos sociétés. La moindre interruption de service peut entraîner des conséquences importantes, qu'elles soient économiques, sociales ou même vitales.

Cependant, à mesure que ces infrastructures se modernisent, elles deviennent aussi la cible d'attaques de plus en plus fréquentes et sophistiquées. Face à cette réalité, la **garantie de la disponibilité des services** s'impose comme un enjeu central de la cybersécurité, nécessitant des stratégies proactives de prévention, de détection et de réponse aux incidents.

1.2.2 Problématique

L'évolution technologique et la numérisation massive des services ont permis d'atteindre un haut niveau d'efficacité dans la gestion des ressources et la communication. Mais cette même transformation a accentué la vulnérabilité des infrastructures critiques face aux cybermenaces. Les

attaques visant spécifiquement la **disponibilité** comme les attaques par déni de service (DDoS), les ransomwares ou les intrusions sur des équipements réseau sensibles peuvent entraîner des interruptions graves, voire totales, des services essentiels. Ces attaques peuvent se propager à partir de points d'entrée multiples (internes ou externes), souvent dus à une mauvaise segmentation, à des failles de configuration ou à des méthodes d'authentification trop statiques.

Dans ce contexte, une question cruciale se pose :

Comment concevoir et sécuriser une infrastructure réseau capable de résister aux cyberattaques tout en garantissant la disponibilité permanente des services critiques ?

1.2.3 Objectifs du projet

L'objectif général de ce mémoire est de **concevoir et sécuriser une architecture réseau critique** capable d'assurer la continuité des services, même en cas de tentative d'attaque ou de compromission.

Les objectifs spécifiques sont les suivants :

- Identifier les vulnérabilités techniques et organisationnelles d'un réseau critique.
- Étudier les principales menaces qui compromettent la disponibilité des services (DDoS, ransomwares, défaillances…).
- Comparer les approches de sécurisation existantes et identifier leurs limites.
- Proposer une solution basée sur l'**approche Zéro Trust**.
- Mettre en œuvre un environnement de simulation pour tester l'efficacité de l'architecture proposée.

1.2.4 Méthodologie d'approche

1.2.4.1 Délimitation du sujet

L'étude portera sur un **réseau critique simulé dans un environnement virtuel**, représentatif d'une infrastructure réelle (ex. réseau hospitalier ou bancaire). Les tests d'attaque porteront sur les services essentiels à forte disponibilité.

1.2.4.2 Démarche adoptée

Pour mener à bien cette étude, une **approche structurée** sera suivie :

- **Analyse des menaces** : étude des types d'attaques affectant la disponibilité des services.
- **Comparaison des méthodes de protection** : évaluation des solutions traditionnelles (VLAN, ACL, RBAC, PARE-FEU) et présentation du modèle Zéro Trust.
- **Conception de l'architecture** : proposition d'une topologie sécurisée intégrant des outils comme Wazuh , Fortinet ZTNA, MFA.
- **Implémentation** : déploiement d'un environnement test avec simulations d'attaques avant et après sécurisation.
- **Évaluation** : comparaison des résultats et recommandations finales.

La problématique posée comment concevoir une architecture réseau résiliente et disponible face aux cyberattaques oriente l'ensemble de la réflexion et des actions à mener dans les prochains chapitres. Les objectifs spécifiques identifiés guideront une démarche rigoureuse alliant théorie, simulation et évaluation technique. Il s'agit désormais d'approfondir les enjeux liés à la sécurité des infrastructures critiques afin de mieux comprendre les risques encourus et la nécessité d'un changement de paradigme en matière de cybersécurité.

CHAPITRE 2 – ENJEUX DE LA SECURITE POUR LES INFRASTRUCTURES CRITIQUES

2.1. Définition d'une infrastructure critique

Une **infrastructure critique** peut être définie comme un ensemble de ressources, de systèmes, de services ou d'installations physiques ou virtuelles, qui sont **indispensables au fonctionnement normal de la société** et de l'économie. Leur indisponibilité ou leur dégradation, volontaire (cyberattaque, sabotage) ou accidentelle (panne, catastrophe naturelle), peut entraîner de **graves conséquences humaines, économiques ou politiques**.

D'après l'**Union Européenne** la définition la plus adapte est **:** "Une infrastructure critique est un actif, un système ou une partie de celui-ci, qui est essentiel au maintien des fonctions vitales de la société, de la santé, de la sécurité, de la prospérité économique ou du bien-être social des personnes."

Exemples de secteurs identifiés comme "critiques" :

- **Énergie** : centrales nucléaires, barrages hydroélectriques, réseaux électriques
- **Santé** : hôpitaux, systèmes de secours, bases de données médicales
- **Transport** : aéroports, chemins de fer, ports, réseaux routiers intelligents
- **Télécommunications** : data centers, satellites, opérateurs de réseau
- **Finance** : banques, systèmes de paiement, bourses

Enjeux liés :

- Protection contre les **cyberattaques** ciblées
- Prévention des **catastrophes technologiques**
- Maintien de la **confiance publique**

2.2. Importance de la disponibilité des services

2.2.1) La disponibilité comme pilier de la cybersécurité

La **disponibilité** est l'un des trois piliers fondamentaux de la sécurité de l'information (avec l'intégrité et la confidentialité). Elle désigne la capacité d'un système ou d'un service à rester accessible et opérationnel, au moment où l'utilisateur en a besoin. Dans un contexte numérique où les services sont fortement interconnectés et dépendants des technologies, elle est essentielle pour assurer la continuité des opérations critiques (finance, santé, logistique, communication). Cela implique un **accès en temps réel** aux ressources, une **tolérance aux pannes** via la redondance ou la virtualisation, une **protection contre les menaces** telles que les attaques DDoS ou les ransomwares, ainsi qu'une **capacité de rétablissement rapide** grâce à des plans de continuité (PCA) et de reprise d'activité (PRA).

2.2.2) Dans le contexte des infrastructures critiques

Les infrastructures critiques telles que les hôpitaux, réseaux électriques, systèmes de transport ou de communication jouent un rôle central dans le bon fonctionnement de la société. Une interruption, même brève, de ces services peut entraîner des répercussions majeures sur la population, l'économie et la sécurité nationale. La disponibilité des services y devient donc une exigence prioritaire.

Pour cela, ces infrastructures doivent intégrer des mécanismes robustes permettant d'assurer une continuité de service maximale, même en cas de panne, d'attaque ou de surcharge. Trois principes essentiels doivent être respectés :

- Tolérance aux pannes : Les systèmes doivent être conçus pour continuer à fonctionner malgré des défaillances matérielles ou logicielles. Cela se traduit par l'utilisation de composants redondants (serveurs, alimentations, connexions), la mise en place de systèmes de basculement automatique ou encore l'usage de technologies de virtualisation capables de migrer les charges en temps réel.
- Résilience face aux attaques : Les infrastructures critiques doivent être capables de résister à des attaques malveillantes (ex. : ransomwares, DDoS, tentatives d'intrusion) sans interruption de service. Cela implique l'intégration de pare-feu avancés, de mécanismes de détection d'intrusion (IDS/IPS), d'une surveillance continue via un Security Operations Center (SOC), et de protocoles de réponse aux incidents.

- Systèmes de secours redondants : Des plans de secours doivent être prévus pour chaque service critique. Il peut s'agir de serveurs de sauvegarde, de sites géographiquement distincts (*site de secours* ou *site miroir*), ou encore de générateurs d'énergie de secours pour les installations sensibles. Ces redondances permettent une reprise immédiate ou rapide de l'activité, sans perte de données ou de disponibilité.

2.2.3) Exemples concrets :

Tableau 1 : Risques et conséquences majeur par secteur en cas d'indisponibilité

Secteur	Incident	Date	Organisation visée	Risque	Conséquence
Santé	Attaque par ransomware sur Synnovis, prestataire de services de laboratoires	3 juin 2024	NHS (King's College Hospital, St Thomas')	Indisponibilité des résultats d'analyses	10 000 rendez-vous annulés, 170 cas de préjudice, **1 décès** confirmé dû au retard des résultat
Transport	Piratage du système de signalisation ferroviaire en Pologne via faux signaux "radio-stop"	25au28 août 2023	Polish State Railways (PKP)	Arrêts d'urgence de trains	20 trains immobilisés, trafic fret paralysé, disruption des services, enquêtes en cours
Finance	Panne du système de paiement TARGET2 de la BCE	23 octobre 2020	Banque Centrale Européenne (TARGET2)	Blocage des paiements interbancaires	11 heures de perturbation affectant salaires, retraits, règlements, pertes financières non chiffrées

2.2.4) Objectifs techniques associés :

- Haute disponibilité (>99.99%)
- Plans de reprise d'activité (PRA)
- Mise en place de SOC (Security Operations Center)

2.3. Impacts d'une interruption de service

Les impacts sont **multidimensionnels**, affectant à la fois les **individus**, les **entreprises**, et les **États**. On peut les catégoriser ainsi :

2.3.1) Impacts sur la santé publique

- Arrêt des équipements médicaux vitaux (respirateurs, IRM)
- Rupture de la chaîne d'approvisionnement en médicaments
- Perturbation des appels d'urgence (SAMU, pompiers)

2.3.2) Impacts économiques

- Fermeture de sites industriels (perte de production)
- Pertes financières directes (fraudes, ransomwares)
- Dégradation de l'image de marque

Exemple : Une attaque contre Colonial Pipeline (États-Unis, 2021) a paralysé l'approvisionnement en carburant de plusieurs États de la côte Est pendant plusieurs jours.

2.3.3) Impacts sociaux et politiques

- Perte de confiance des citoyens envers les autorités
- Soulèvements en cas de pénurie (eau, carburant, alimentation)
- Détérioration de la stabilité sociale (désinformation)

2.3.4) Impacts sur la sécurité nationale

- Piratage de systèmes militaires ou stratégiques
- Sabotage d'infrastructures sensibles (centrales nucléaires)

- Collecte illégale de données classifiées

➤ Risques systémiques

Lorsque plusieurs infrastructures sont interconnectées, une attaque ou une panne peut entraîner un **effet domino** :

"Une simple défaillance dans le réseau électrique peut affecter les télécommunications, les services de secours, les banques et même la distribution alimentaire."

2.4. Présentation simplifiée d'un réseau d'entreprise privée et de ses équipements critiques

Dans une entreprise privée, l'infrastructure réseau repose sur une architecture composée de plusieurs équipements interconnectés, chacun jouant un rôle spécifique dans la connectivité, la sécurité et la performance du système.

2.4.1) les équipements :

- **Routeur** : Il permet de connecter le réseau interne de l'entreprise à Internet. Il joue un rôle essentiel dans le routage des paquets de données entre les réseaux externes et internes.
- **Switch (commutateur)** : Il connecte les différents équipements internes (ordinateurs, imprimantes, serveurs) entre eux au sein du réseau local. Un switch intelligent peut aussi permettre une gestion fine du trafic.
- **Pare-feu (Firewall)** : C'est la barrière de sécurité entre le réseau interne et l'extérieur. Il filtre les connexions entrantes et sortantes selon des règles de sécurité préétablies, empêchant ainsi les intrusions non autorisées.
- **Serveurs** : Hébergent les applications critiques, bases de données, fichiers, messagerie, etc. Leur sécurité et disponibilité sont vitales.
- **Points d'accès Wi-Fi sécurisés** : Pour la mobilité interne tout en contrôlant les connexions via authentification.
- **Contrôleur de domaine (Active Directory)** : Il gère l'authentification des utilisateurs, leurs permissions, et l'accès aux ressources de l'entreprise.

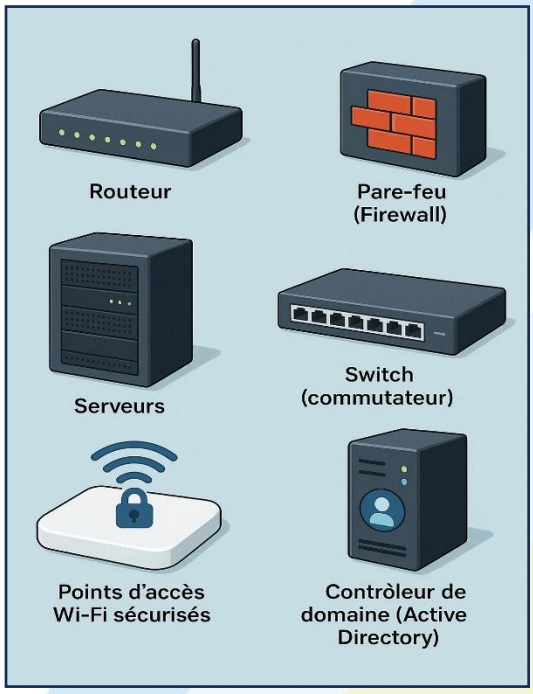


Figure 2: présentation des équipements

2.4.2) Pourquoi ces équipements rendent un réseau critique ?

Parce qu'ils assurent :

- La connectivité continue (interne et externe)
- La protection contre les cybermenaces (filtrage, segmentation, surveillance)
- L'accès sécurisé aux données et aux ressources
- La gestion centralisée des utilisateurs et des politiques de sécurité

Une panne ou une compromission sur l'un de ces éléments peut suffire à paralyser toute l'entreprise (ex. : un firewall mal configuré peut bloquer l'accès aux applications critiques ; un routeur piraté peut détourner le trafic vers un serveur malveillant).

2.4.3) exemple de structure d'une infrastructure prive

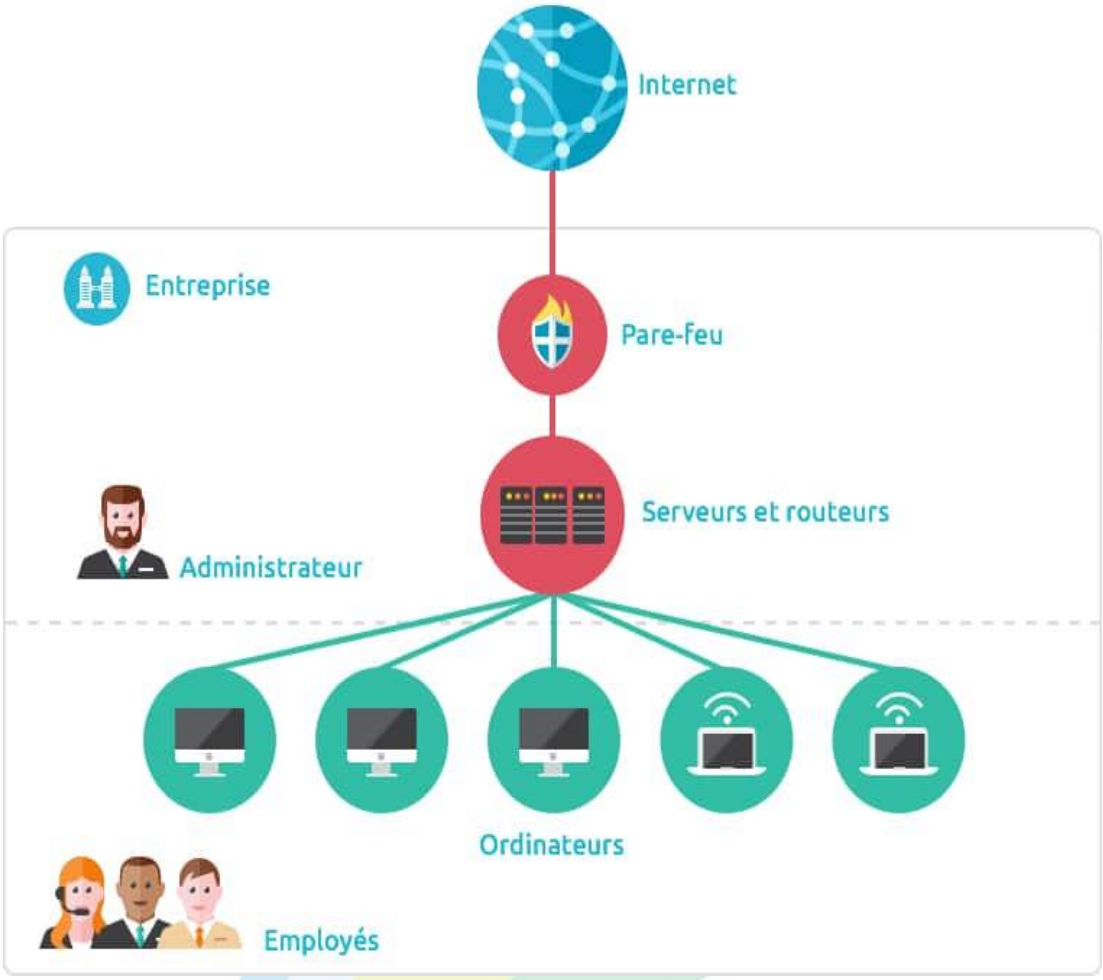


Figure 3 : Organisation du réseau classique interne d'une entreprise

Ce chapitre a montré que la disponibilité des services est vitale pour les infrastructures critiques, dont le bon fonctionnement repose sur des équipements clés (pare-feu, routeurs, serveurs…). Des exemples concrets ont illustré les impacts graves d'une interruption. Pour mieux protéger ces infrastructures, il est maintenant essentiel d'analyser les menaces et attaques auxquelles elles sont exposées.

CHAPITRE 3 – MENACES ET CAS D'ATTAQUE SUR LES RESEAUX

La sécurité des infrastructures critiques repose en grande partie sur la robustesse des réseaux qui les soutiennent. Cependant, ces réseaux sont constamment soumis à des menaces croissantes et sophistiquées, issues aussi bien d'acteurs externes malveillants que de failles internes ou de défaillances techniques. Ce chapitre vise à présenter les principales menaces pesant sur les réseaux informatiques des infrastructures critiques, en s'appuyant sur des exemples concrets, des typologies d'attaque et des méthodes d'évaluation des vulnérabilités.

Les attaques sur les réseaux, qu'elles soient **externes, internes ou involontaires**, constituent une menace directe pour la continuité des services essentiels. Dans un contexte où la transformation numérique s'accélère, les infrastructures critiques deviennent de plus en plus vulnérables à des attaques ciblées et persistantes. Il est donc impératif de déployer une **stratégie de cybersécurité intégrée**, alliant **prévention, détection, réponse et résilience**, tout en identifiant en continu les points de faiblesse à fort potentiel de rupture.

3.1. Attaques de type DoS/DDoS

3.1.1 Définition et fonctionnement

Une attaque par déni de service (DoS - Denial of Service) consiste à submerger un serveur ou un réseau par un volume de requêtes excessif, rendant le service indisponible pour les utilisateurs légitimes. Lorsqu'elle est distribuée (DDoS - Distributed Denial of Service), l'attaque est menée à partir de plusieurs machines infectées (botnets), ce qui en complique la détection et l'atténuation.

3.1.2 Objectifs visés

Les attaques DoS/DDoS ciblent prioritairement la **disponibilité des services**, ce qui, dans le cadre d'infrastructures critiques, peut provoquer des conséquences majeures telles que :

- Interruption des services d'urgence
- Désorganisation des communications étatiques
- Perturbation des systèmes de gestion d'énergie ou de transport

3.1.3 Cas concret

Tableau 2 : Exemples d'attaques DDoS ayant ciblé des infrastructures critiques

Date de l'incident	Entreprise touchée	Nombre de victimes	Données / Infrastructures endommagées	Méthode ou technique utilisée	Mesures de sécurité mises en place par l'entreprise	Source
21 octobre 2016	Dyn (fournisseur DNS, USA)	Millions d'utilisateurs indirectement touchés	Infrastructure DNS de Dyn affectant Twitter, Netflix, PayPal, Amazon, etc.	Attaque DDoS via botnet Mirai	Filtrage renforcé du trafic, augmentation de la redondance DNS, coordination avec les FAI et le FBI	KrebsOnSecurity

3.1.4 Contre-mesures

- Mise en place de services d'atténuation spécialisés (Cloudflare, Akamai)
- Usage de pare-feu applicatifs et systèmes IDS/IPS
- Analyse comportementale du trafic réseau et blocage dynamique

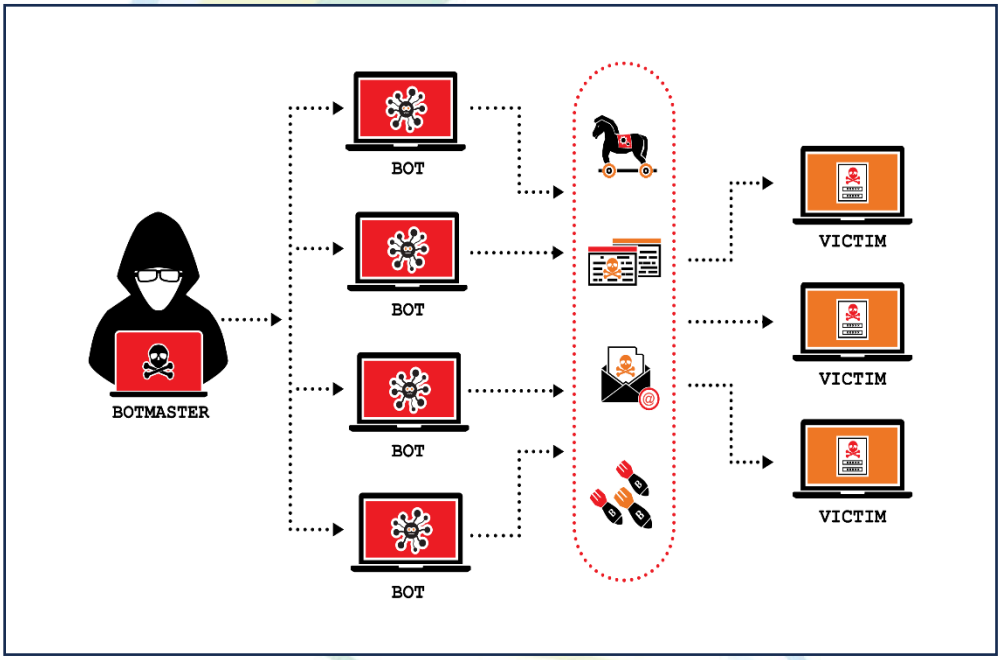


Figure 4 : Attaques DDOS

3.2. Ransomwares

3.2.1 Définition

Un **ransomware** est un logiciel malveillant qui chiffre les fichiers d'un système ou réseau et exige une rançon en échange de la clé de déchiffrement. Il représente aujourd'hui une menace majeure, notamment pour les secteurs de la santé, de l'énergie ou des administrations publiques.

3.2.2 Mode d'infection

Les vecteurs d'entrée les plus courants incluent :

- Le phishing (courriels contenant des pièces jointes malveillantes)
- L'exploitation de vulnérabilités non corrigées
- Le protocole RDP mal sécurisé

3.2.3 Impacts spécifiques

Les conséquences sont souvent immédiates et critiques :

- Interruption complète des opérations
- Perte de données sensibles
- Pression médiatique et institutionnelle

3.2.4 Exemples

Tableau 3 : Exemples d'attaques par ransomware ciblant des infrastructures critiques

Date de l'incident	Entreprise touchée	Nombre de victimes	Données / Infrastructures endommagées	Méthode ou technique utilisée	Mesures de sécurité mises en place par l'entreprise	Source
12 mai 2017	NHS (Royaume-Uni)	Plus de 200 000 ordinateurs, 80 hôpitaux affectés	Systèmes hospitaliers, fichiers médicaux, postes Windows	Ransomware « WannaCry » (via vulnérabilité SMB)	Patching urgent de Windows, déploiement de sauvegardes, mise à jour de l'antivirus, migration vers systèmes sécurisés	The Guardian
8–10 mars 2021	Ville de La Rochelle (France)	Services administratifs, écoles, cantines impactés	Réseaux internes, services numériques municipaux	Ransomware « Ryuk »	Réseau coupé, restauration progressive via sauvegardes, collaboration avec l'ANSSI	Le Figaro

3.2.5 Mesures de défense

- Politique de sauvegarde fréquente et hors ligne
- Segmentation réseau pour limiter la propagation
- Surveillance des comportements anormaux

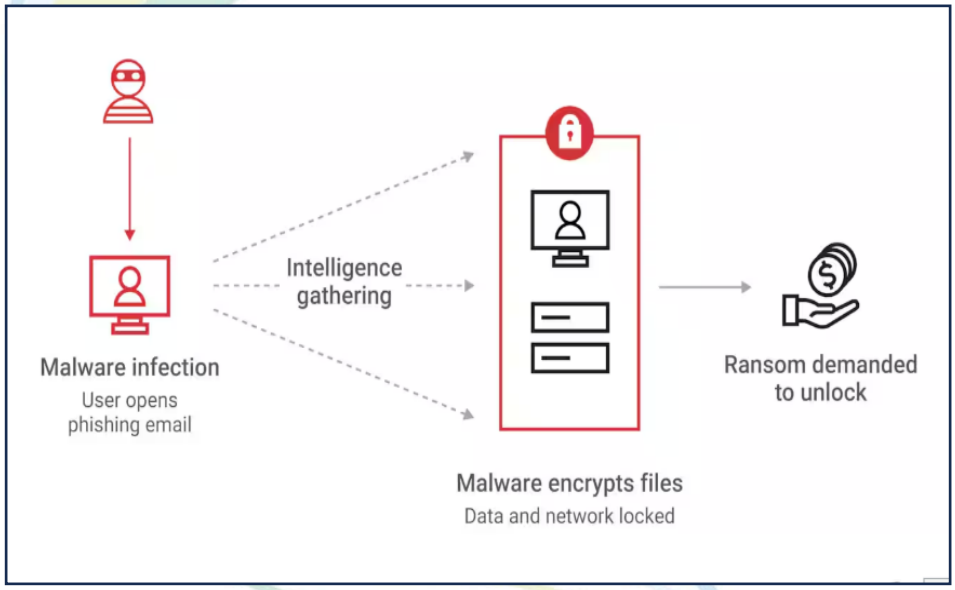


Figure 5 : fonctionnement d'un Ransomware

3.3. Intrusions internes

3.3.1 Nature des menaces internes

Les **menaces internes** proviennent d'employés, sous-traitants ou anciens collaborateurs disposant d'un accès légitime. Elles peuvent être intentionnelles (malveillance) ou non (erreur humaine).

3.3.2 Formes d'intrusion

- Vol d'information confidentielle
- Sabotage de systèmes ou de bases de données
- Détournement de comptes à privilèges

3.3.3 Facteurs aggravants

- Absence de séparation des rôles
- Manque de surveillance des comptes à privilèges
- Culture de sécurité faible ou inexistante

3.3.4 Exemple

Tableau 4 : Exemple d'intrusion interne dans des infrastructures critiques

Date de l'incident	**Entreprise touchée**	**Nombre de victimes**	**Données / Infrastructures endommagées**	**Méthode ou technique utilisée**	**Mesures de sécurité mises en place par l'entreprise**	**Source**
Juin 2018	Tesla (Gigafactory Nevada, USA)	Risque sur la chaîne de production	Code source modifié, données sensibles exfiltrées	Employé malveillant modifiant le	Audit de sécurité, révocation des accès, renforcement du contrôle des	CNBC

Date de l'incident	Entreprise touchée	Nombre de victimes	Données / Infrastructures endommagées	Méthode ou technique utilisée	Mesures de sécurité mises en place par l'entreprise	Source
				code source interne	identifiants, poursuite judiciaire engagée	

3.3.5 Mesures correctives

- Mise en œuvre de la politique du **moindre privilège**
- Audit régulier des journaux d'accès
- Détection basée sur l'analyse du comportement (UEBA)

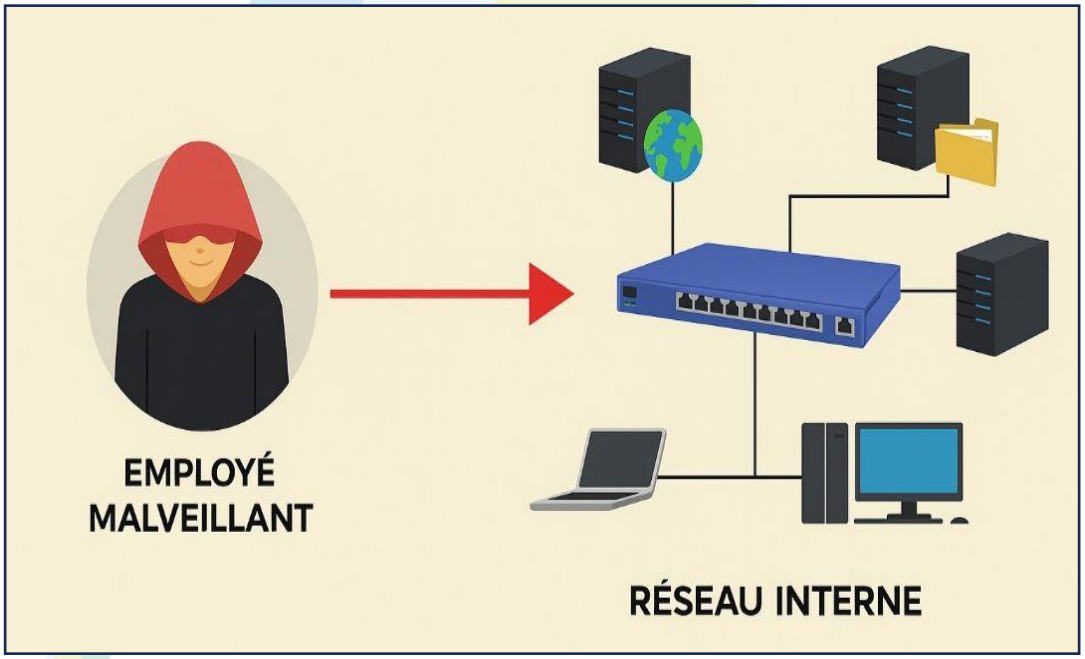


Figure 6 : intrusions internes

3.4. Défaillances techniques

3.4.1 Définition

Il s'agit d'incidents non provoqués par une action humaine malveillante, incluant les pannes matérielles, les bugs logiciels ou les erreurs de configuration.

3.4.2 Exemples fréquents

- Défaillance des disques ou serveurs
- Mauvaise mise à jour du firmware réseau
- Configuration erronée des accès

3.4.3 Impacts

Même en l'absence d'attaque, une défaillance technique peut avoir des effets comparables à une cyberattaque :

- Indisponibilité temporaire ou prolongée
- Réduction de la fiabilité
- Perte ou corruption de données

3.4.4 Exemples

Tableau 5 : Exemples de cas de Défaillances techniques dans des infrastructures critiques

Date de l'incident	**Entreprise touchée**	**Nombre de victimes**	**Données / Infrastructures endommagées**	**Méthode ou technique utilisée**	**Mesures de sécurité mises en place par l'entreprise**	**Source**
23 octobre 2020	Banque centrale européenne (TARGET2)	Des milliers de banques et clients affectés	Plateforme de paiement interbancaire (TARGET2)	Défaillance matérielle non liée à une cyberattaque	Mise à jour de l'infrastructure, renforcement de la redondance, audit complet du système	ECB

3.4.5 Prévention

- Maintenance régulière et planifiée

- Redondance matérielle (RAID, serveurs miroirs)
- Test systématique des PRA (Plans de Reprise d'Activité)

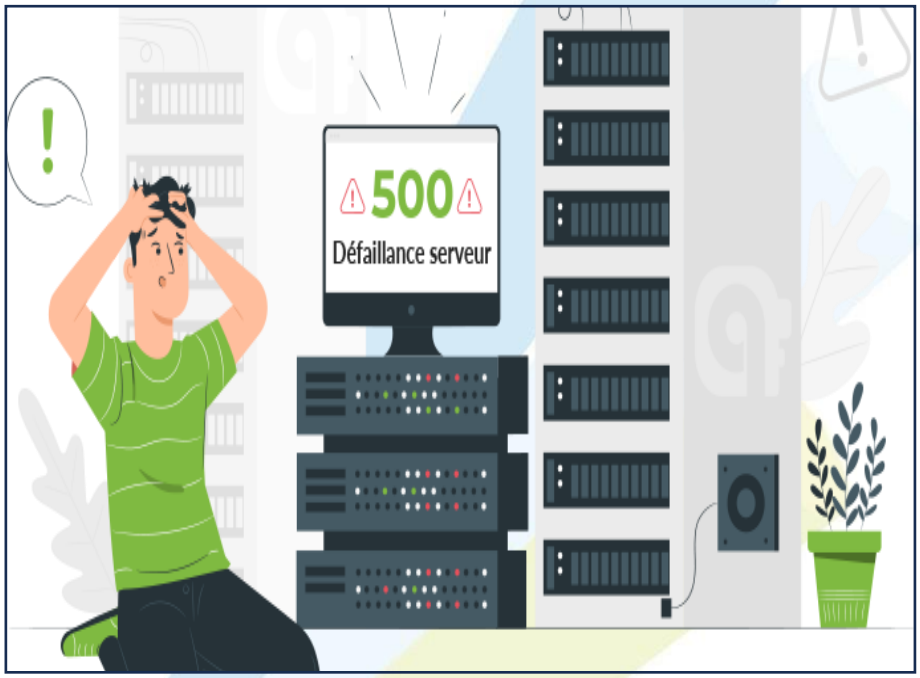


Figure 7 : défaillance serveur ERROR 500

3.5. Identification des points faibles

3.5.1 Importance stratégique dans la détermination des failles de sécurité

La **cartographie des vulnérabilités** constitue une étape indispensable pour renforcer la sécurité d'un réseau. Elle permet d'agir en amont, avant qu'une faille ne soit exploitée.

3.5.2 Méthodes de détection

- **Scans de vulnérabilités** (ex : Nessus, OpenVAS)
- **Pentests internes ou externes** (Boîte noire / Boîte blanche)
- **Audit de sécurité** complet (technique + organisationnel)

3.5.3 Faiblesses courantes dans les réseaux critiques

- Services exposés non utilisés (port FTP, Telnet, SNMPv1)

- Absence de journalisation ou d'alertes
- Mots de passe par défaut encore en usage

3.5.4 Outils de référence

Tableau 6: Exemple d'outils de référence

Objectif	**Outil recommandé**
Scan de vulnérabilités	Nessus, Qualys, OpenVAS
Test de pénétration	Metasploit
Analyse de logs	Splunk, ELK Stack
Cartographie réseau	Nmap, Wireshark

Ce chapitre a permis d'explorer les principales menaces pesant sur les réseaux des infrastructures critiques, qu'il s'agisse d'attaques externes (DDoS, ransomwares), d'intrusions internes, de défaillances techniques ou de failles de sécurité non corrigées. Ces menaces, souvent interconnectées, soulignent la vulnérabilité croissante des systèmes face à une cybercriminalité de plus en plus sophistiquée. Face à cette réalité, il devient indispensable de mettre en place des solutions de protection robustes, combinant approches classiques et dispositifs intelligents.

CHAPITRE 4 : SOLUTIONS DE SÉCURISATION : CLASSIQUES ET INTELLIGENTS

4.1 Approches traditionnelles : périmétrique, VLAN, ACL, RBAC, pare-feu

Historiquement, la sécurité informatique s'est fondée sur un modèle périmétrique, dans lequel le réseau interne est considéré comme fiable, et le réseau externe (Internet) comme potentiellement dangereux. Cette architecture repose principalement sur l'idée que les menaces proviennent de l'extérieur, justifiant la mise en place de pare-feux, proxys et DMZ à la frontière du système d'information (SI).

Cette vision repose sur la mise en place d'un périmètre de sécurité défini, défendu et surveillé. Une fois à l'intérieur du périmètre, les utilisateurs, services et appareils sont considérés comme de confiance.

4.1.1 Pare-feu (firewall)

Le pare-feu est un dispositif de filtrage du trafic réseau, situé à l'entrée du système d'information. Il permet de bloquer ou d'autoriser les connexions en fonction de règles prédéfinies (ports, adresses IP, protocoles). Il joue un rôle essentiel dans la défense périmétrique, en constituant la première ligne de protection contre les connexions non autorisées ou malveillantes. Il existe des pare-feux matériels et logiciels, souvent couplés à des fonctions de NAT, filtrage d'applications, inspection de paquets ou détection d'intrusions.

4.1.2 VLAN (Virtual Local Area Network)

Les VLAN permettent de segmenter logiquement le réseau local au sein d'une même infrastructure physique. Ils limitent la communication directe entre groupes d'utilisateurs ou de machines, afin de contenir d'éventuelles attaques ou erreurs de configuration.Cette segmentation favorise l'isolement des flux sensibles, comme ceux des ressources critiques, du trafic utilisateur ou des invités.

4.1.3 ACL (Access Control List)

Les ACL sont des règles de filtrage définies au niveau des routeurs, commutateurs ou pare-feux, qui permettent ou interdisent des flux spécifiques entre des hôtes ou des réseaux.Elles précisent qui peut accéder à quoi, à travers des critères comme les adresses IP, les ports ou les protocoles utilisés. C'est une approche granulaire mais rigide, qui peut devenir difficile à maintenir dans des environnements complexes ou dynamiques.

4.1.4 RBAC (Role-Based Access Control)

Le contrôle d'accès basé sur les rôles (RBAC) repose sur le principe d'attribution des permissions en fonction des responsabilités de l'utilisateur. Ainsi, un utilisateur peut se voir accorder des droits d'accès selon son poste (employé, manager, administrateur).

Cette méthode simplifie l'administration des droits d'accès et contribue à limiter l'exposition inutile des ressources.

4.1.5 Proxys et DMZ

Les proxys jouent un rôle d'intermédiaire entre les utilisateurs internes et Internet, permettant de contrôler, filtrer et enregistrer les requêtes sortantes.

Quant à la DMZ (Demilitarized Zone), elle héberge les services accessibles depuis Internet (site web, messagerie, VPN) tout en les isolant du cœur du réseau interne. C'est une zone tampon conçue pour limiter les risques en cas de compromission.

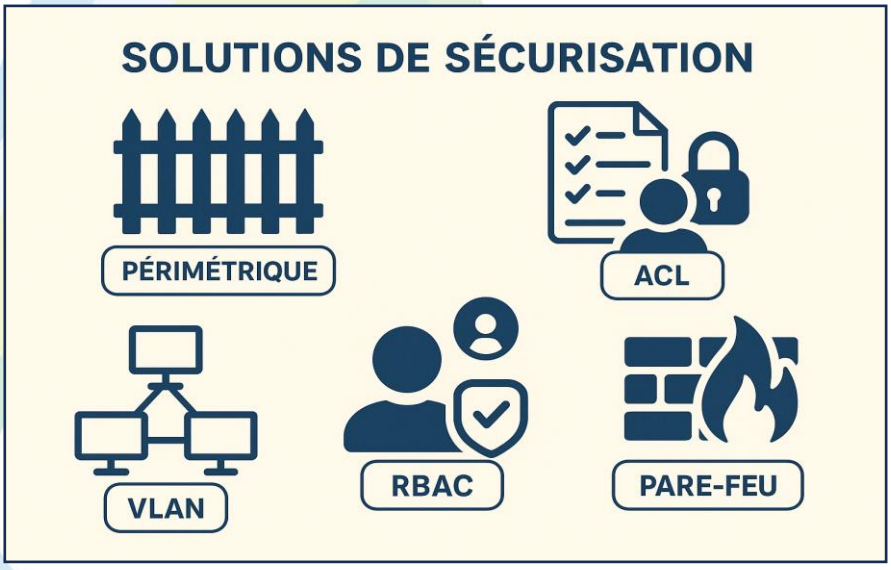


Figure 8 : solutions de sécurisation traditionnel

4.2 Limites des approches classiques

Si les modèles de sécurité traditionnels ont longtemps permis de protéger efficacement les infrastructures informatiques, ils se révèlent aujourd'hui inadaptés face aux profondes mutations numériques. Plusieurs tendances majeures ont contribué à souligner les **insuffisances structurelles** de ces approches :

4.2.1 Explosion de la mobilité et du télétravail

L'accès aux ressources informatiques ne se limite plus aux locaux de l'entreprise. Les utilisateurs se connectent depuis une multitude de lieux (domicile, espaces de coworking, transports, pays étrangers), avec des appareils variés souvent personnels ou non maîtrisés (Bring Your Own Device – BYOD).Cela rend **inefficace la notion de périmètre réseau fixe**, sur laquelle reposent les pares-feux et les VLANS .Un collaborateur distant, connecté via un VPN à l'environnement interne, peut involontairement introduire des malwares s'il utilise un poste non sécurisé.

4.2.2 Massification du cloud computing

Le recours massif aux services Office 365, AWS, Azure, Google Cloud, etc fragilise encore davantage le périmètre traditionnel :

- Les applications critiques ne sont plus hébergées sur des serveurs internes, mais dans des **environnements distribués et souvent publics**.
- Les flux réseau passent **en dehors des pares-feux traditionnels**, ce qui rend leur surveillance beaucoup plus complexe.
- Les données sont copiées, synchronisées ou partagées sur des clouds tiers, sans visibilité ou contrôle centralisé.

Les outils de protection périmétrique sont **contournés par l'architecture même du cloud**.

4.2.3 Évolution et complexification des menaces

Les cyberattaques actuelles sont plus furtives, plus ciblées et souvent **initiées depuis l'intérieur du réseau** ou via des accès utilisateurs compromis. Parmi ces menaces :

- **Ransomwares** se propageant latéralement après une intrusion initiale.
- **Menaces internes** (utilisateurs malveillants ou négligents).

- **APT (Advanced Persistent Threats)** qui s'installent discrètement sur le long terme.

Le paradigme "interne = fiable" devient **dangereux**, car il facilite la progression silencieuse de l'attaquant une fois le périmètre franchi.

4.2.4 Manque de vérification dynamique et contextuelle

Les approches traditionnelles reposent sur des règles statiques : une fois que l'accès est autorisé, il n'y a **plus de vérification en temps réel**. Elles n'intègrent pas de critères contextuels comme :

- La **localisation géographique** de l'utilisateur
- L'**état de conformité du terminal** (patchs de sécurité, antivirus actif, etc.)
- L'**horaire ou le volume de données consultées**
- Le **comportement utilisateur** (ex. : tentative de télécharger des volumes anormaux)

Cette **absence d'intelligence adaptative** empêche de détecter les comportements suspects en cours de session.

4.2.5 Absence de visibilité continue et de corrélation avancée

Les dispositifs classiques (pare-feu, ACL, VPN, etc.) génèrent des logs basiques et souvent **déconnectés entre eux**. Cette fragmentation :

- Empêche d'avoir une vision globale et en temps réel de l'activité réseau et utilisateur.
- Rend difficile la détection de **signaux faibles ou de compromissions progressives**.
- Limite la capacité des outils de sécurité (SIEM, SOC) à corréler les événements et à répondre rapidement.

Une attaque lente et discrète peut ainsi rester **invisible pendant plusieurs semaines**, faute d'une surveillance unifiée et contextuelle.

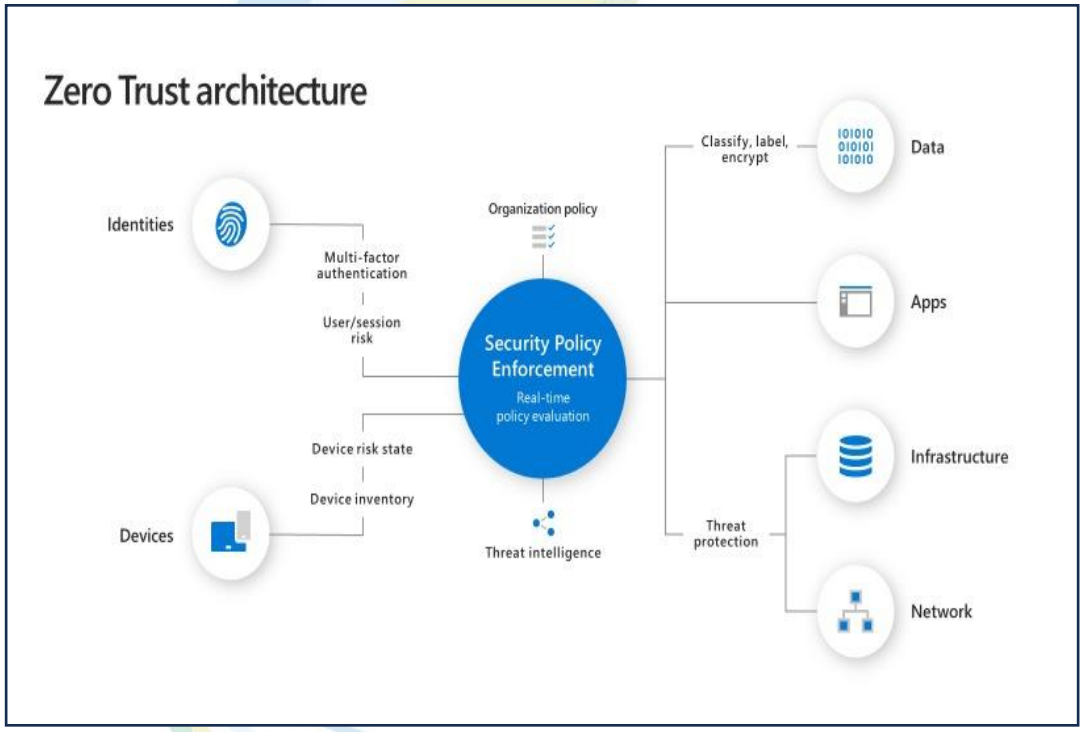
4.3 Modèles modernes de sécurité

L'évolution rapide des usages numériques, marquée par la montée en puissance du cloud, le travail à distance, l'hétérogénéité des terminaux et la sophistication des menaces, a entraîné l'émergence de nouveaux modèles de sécurité. Contrairement aux approches traditionnelles fondées sur un

périmètre fixe et une confiance implicite, ces modèles modernes reposent sur des principes dynamiques, centrés sur l'identité, la vérification continue, la décentralisation et l'adaptabilité du contrôle.

4.3.1 Zéro Trust Architecture (ZTA)

Le modèle Zéro Trust remet en question le postulat classique selon lequel un utilisateur interne serait par défaut digne de confiance. Dans cette architecture, chaque demande d'accès à une ressource est soumise à une vérification explicite et contextuelle. L'identité de l'utilisateur, l'état de sécurité de l'appareil utilisé, la localisation géographique, l'heure, ainsi que les comportements passés sont autant de facteurs pris en compte avant d'accorder l'accès. De plus, les autorisations sont limitées au strict nécessaire, selon le principe du moindre privilège, et ne sont valables que pour une durée déterminée. Ce modèle s'appuie sur des technologies comme l'authentification multifacteur (MFA), la micro-segmentation, la surveillance comportementale (UEBA), les plateformes SIEM, et les outils d'analyse en temps réel. Il permet d'empêcher les mouvements latéraux en cas de compromission, tout en renforçant la sécurité dans des environnements hybrides ou distribués.



4.3.2 Secure Access Service Edge (SASE)

Le modèle SASE, proposé par Gartner, vise à fusionner les services de sécurité réseau avec les capacités de connectivité dans une architecture unifiée et basée sur le cloud. L'objectif est de fournir un accès sécurisé aux utilisateurs où qu'ils se trouvent, sans avoir à rediriger le trafic par des points centralisés. Les services traditionnellement déployés en local comme les pare-feux, les proxies, les passerelles web sécurisées (SWG), ou encore les contrôleurs d'accès cloud (CASB) sont intégrés dans le cloud et rapprochés géographiquement des utilisateurs via des points de présence. Cette approche améliore non seulement la performance des connexions, mais offre également une protection homogène pour les ressources internes et cloud, sans alourdir l'architecture réseau. Elle est particulièrement adaptée aux entreprises multisites, aux environnements de travail hybrides, et aux organisations ayant recours à des applications SaaS.

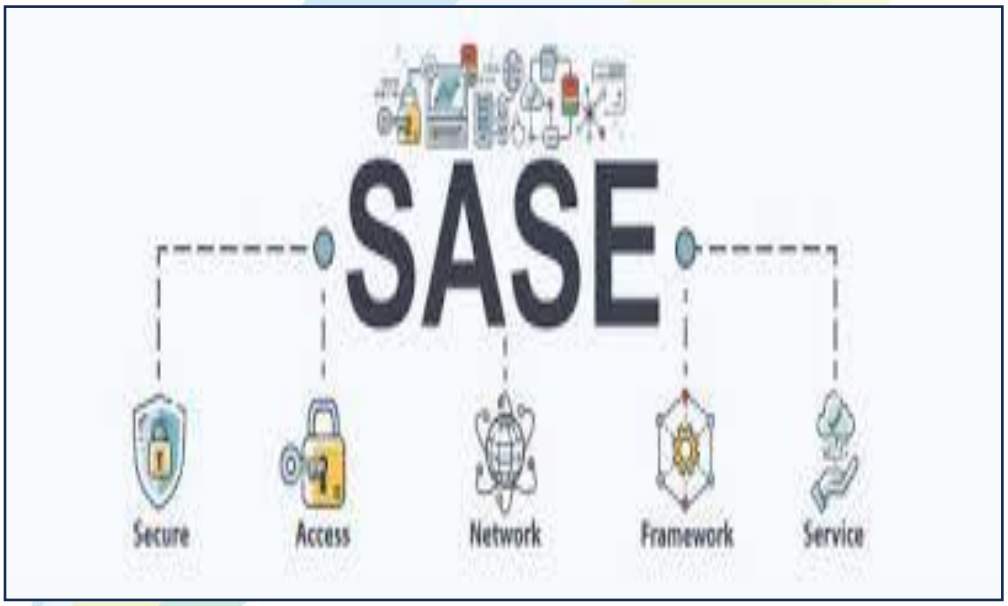


Figure 10 : Secure Access Service Edge (SASE)

4.3.3 Continuous Adaptive Risk and Trust Assessment (CARTA)

Le modèle CARTA repose sur une approche adaptative et en temps réel de l'évaluation du risque et de la confiance. Contrairement aux systèmes d'accès traditionnels qui prennent une décision unique au moment de la connexion, CARTA préconise une évaluation continue durant toute la session utilisateur. Chaque action qu'il s'agisse de consulter un fichier, de transférer des données ou d'accéder à une application est réévaluée à la lumière de nouvelles informations

comportementales ou contextuelles. En s'appuyant sur des outils de machine learning, d'analyse comportementale et de corrélation d'événements, CARTA permet de réagir immédiatement à un changement de contexte ou à une activité suspecte. Il s'intègre particulièrement bien aux environnements à forte variabilité, comme les infrastructures DevOps ou les services soumis à de fréquents changements de configuration.

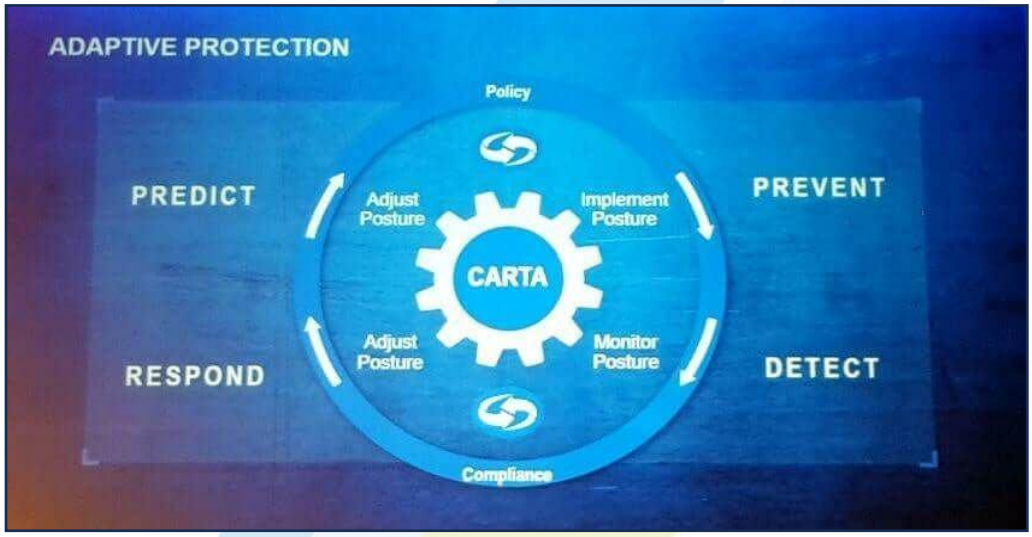


Figure 11 : Carta

4.3.4 Sécurité cloud-native

La transformation numérique des entreprises s'est accompagnée d'un transfert massif de données et de services vers le cloud, rendant nécessaire une approche de sécurité spécifiquement conçue pour ces environnements. La sécurité cloud-native ne consiste pas à adapter les outils traditionnels au cloud, mais à déployer des solutions pensées pour la flexibilité, l'automatisation et la scalabilité. Des plateformes comme CSPM (Cloud Security Posture Management) ou CNAPP (Cloud-Native Application Protection Platform) permettent de détecter les erreurs de configuration, d'assurer la conformité continue, de sécuriser les charges de travail et de protéger les applications déployées dans des environnements multicloud. Ces outils s'intègrent généralement aux chaînes DevSecOps, garantissant ainsi une sécurité « by design » dès les premières étapes du développement applicatif.

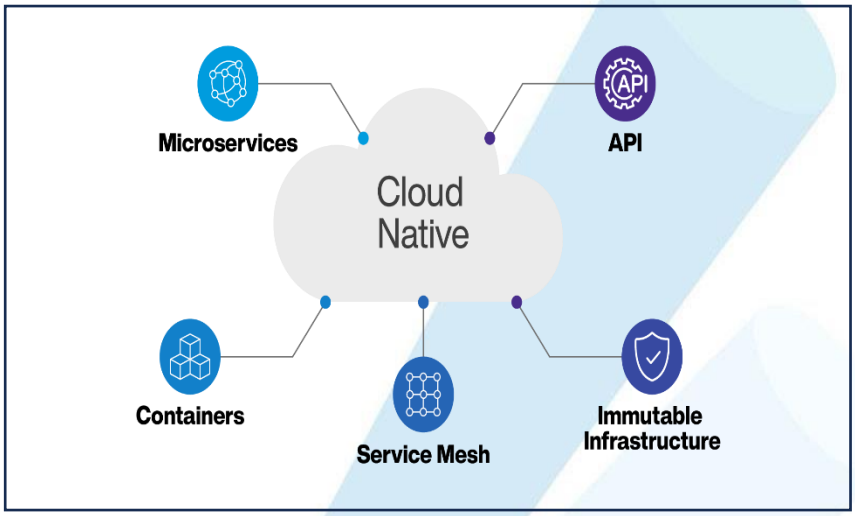


Figure 12 : Sécurité cloud-native

4.3.5 Blockchain et sécurité décentralisée

La blockchain, technologie initialement développée pour les cryptomonnaies, s'est progressivement imposée comme un vecteur de sécurité dans des contextes nécessitant de la transparence, de l'intégrité et de la traçabilité. En offrant un registre distribué et immuable, elle permet de sécuriser des transactions ou des événements sans dépendre d'un tiers de confiance. Dans le domaine de la cybersécurité, la blockchain est utilisée pour garantir l'intégrité des journaux d'audit, gérer des identités décentralisées (SSI – Self Sovereign Identity), ou encore pour automatiser des politiques de sécurité via des contrats intelligents. Si son déploiement reste encore limité à certains cas d'usage, elle ouvre de nouvelles perspectives pour des architectures distribuées, résilientes et inviolables.

Figure 13 :blockchain et sécurité décentralisée

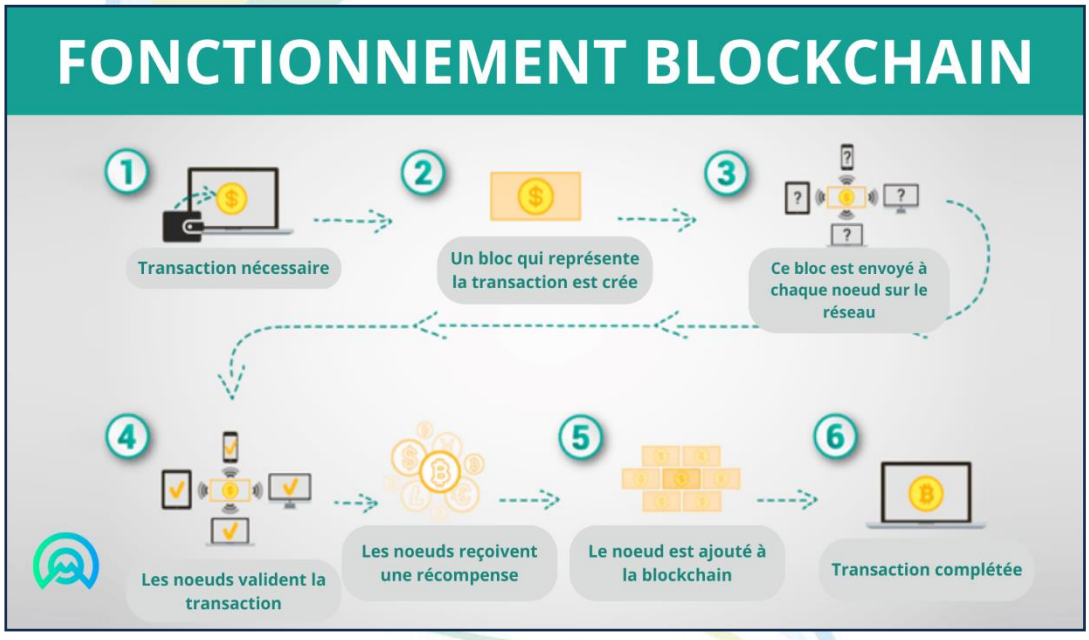


Figure 13 : blockchain et sécurité décentralisée

4.4 Choix du Modèle

4.4.1 Tableau comparatif des principales solutions de sécurité intelligentes

4.4.1.1. Tableau comparatif

Tableau 7 : Tableau comparatif des principales solutions de sécurité intelligentes

Critères	**Zero Trust Architecture (ZTA)**	**SASE (Secure Access Service Edge)**	**CARTA (Continuous Adaptive Risk and Trust Assessment)**	**Sécurité cloud-native**	**Blockchain et sécurité décentralisée**	**Autres approches (ex: périmétrique, VPN, NAC)**
Principe fondamental	Ne jamais faire confiance, toujours vérifier.	Fusion réseau + sécurité cloud en périphérie	Évaluation continue et adaptative des risques et de la confiance	Sécurité intégrée dans le cycle DevOps et cloud	Transparence et traçabilité via registre distribué	Sécurité basée sur le périmètre ou des règles statiques
Contrôle d'accès granulaire (user, device, app, data)	✅ Très fort (policy-based, micro-segmentation,	✅ Fort, mais dépend de la solution et du	✅ Adaptatif, mais dépend d'un moteur de	❌ Variable selon l'architecture cloud	❌ Faible – blockchain n'offre pas nativement du	❌ Faible à modéré selon configuration (ex. ACL,

	contextualisation)	fournisseur	scoring continu		contrôle d'accès granulaire	VLAN, VPN)
Résilience aux attaques internes	✅ Très élevée – segmentation logique + authentification continue	✅ Élevée – filtrage cloud distribué	✅ Bonne – détection dynamique des anomalies	❌ Faible sans intégration d'outils spécifiques	❌ Faible – pas conçu pour protéger contre des accès internes	❌ Très faible – perimeter breach = accès total
Détection et réponse adaptative	✅ Intégrée – en fonction du contexte, du comportement et de l'identité	✅ Bonne – via convergence avec solutions SSE/SD-WAN	✅ Excellente – modèle basé sur l'évaluation en temps réel	✅ Bonne – si CI/CD bien sécurisée	❌ Très limitée – pas de réponse automatisée	❌ Réponse souvent manuelle ou tardive
Garantie de la disponibilité des services critiques (OT/IT)	✅ Priorité – segmentation + gestion des accès critiques	✅ Bonne – dépend de la connectivité cloud	✅ Moyenne – dépend de l'intégration avec les systèmes	❌ Pas d'orientation explicite sur la disponibilité	❌ Réseau distribué = latence + absence de contrôle en temps réel	❌ Forte dépendance à l'intégrité de l'infrastructure
Visibilité et traçabilité centralisées	✅ Totale journaux, SIEM, surveillance de l'identité et des sessions	✅ Bonne si couplée avec un fournisseur SSE	✅ Bonne logs en continu	❌ Dépend de la stack cloud utilisée	✅ Forte – mais surtout orientée preuve et conformité	❌ Limitée – difficile à corréler
Adaptabilité à une infrastructure critique hybride	✅ Excellente – protection indépendante	✅ Bonne – surtout orientée	✅ Bonne – mais nécessite	❌ Spécifiquement cloud – peu	❌ Faible – absence d'intégration avec	❌ Difficulté à s'adapter à

(OT/IT, cloud/edge)	de la localisation physique ou logique	WAN et travail distant	une bonne orchestration	adapté à l'OT ou au edge	des systèmes critiques complexes	l'évolution des usages
Maturité et standards disponibles	✅ Haute – NIST 800-207, nombreux frameworks industriels	✅ Élevée – portée par les grands fournisseurs de cloud	⚠️ Émergente – concept en évolution continue	✅ Maturité croissante – via DevSecOps	⚠️ Très émergente – peu de standards pratiques	✅ Ancienne – mais souvent dépassée face aux nouvelles menaces
Complexité de mise en œuvre initiale	⚠️ Moyenne à élevée – nécessite une refonte du modèle de confiance	✅ Moyenne – dépend du fournisseur choisi	⚠️ Élevée – nécessite beaucoup de capteurs et d'IA	✅ Faible à moyenne – dépend des outils cloud natifs	⚠️ Élevée – intégration difficile, peu d'expertise disponible	✅ Faible – solutions connues mais peu flexibles
Pertinence pour les environnements critiques (industriels, santé, etc.)	✅ Parfaite – contrôle strict, segmenté, adaptable aux exigences métiers	✅ Bonne – surtout pour l'accès distant sécurisé	⚠️ Bonne, mais secondaire	❌ Faible – orientée cloud public et DevOps	❌ Faible – plus orientée vers la sécurité des échanges ou de la donnée brute	❌ Obsolète – expose à des menaces modernes non couvertes
Orientation vers la disponibilité et la continuité d'activité (PCA/PRA)	✅ Forte – intégration avec les plans de résilience	✅ Moyenne à bonne – selon configuration	✅ Bonne – si bien intégrée	❌ Pas une priorité – dépend du fournisseur cloud	❌ Non – pas conçu pour la haute disponibilité des services critiques	❌ Pas ou peu de mécanismes automatisés de reprise

Analyse : Parmi les différentes approches modernes de cybersécurité (ZTA, SASE, CARTA, sécurité cloud-native, blockchain, etc.), la Zéro Trust Architecture (ZTA) se distingue comme la solution la plus adaptée pour renforcer la sécurité d'une architecture réseau critique et garantir la disponibilité des services

4.4.1.2 Pourquoi adopter le modèle Zéro Trust ?

Les modèles traditionnels de sécurité, fondés sur un périmètre réseau clairement défini, ne répondent plus aux exigences des environnements numériques modernes. Avec l'adoption massive du cloud, la généralisation du télétravail, l'explosion des objets connectés et la sophistication des cybermenaces, ces modèles montrent leurs limites. En effet, ils reposent sur la présomption que tout ce qui est « à l'intérieur » du réseau est digne de confiance, une logique aujourd'hui dépassée face à des attaques qui exploitent souvent des identifiants compromis ou des failles internes.

Dans ce contexte, le modèle Zéro Trust émerge comme une alternative crédible et structurée. Il propose un changement de paradigme fondamental : ne jamais accorder de confiance implicite, même à l'intérieur du réseau, et vérifier systématiquement chaque requête d'accès. Ce modèle permet de mieux se protéger contre les mouvements latéraux d'un attaquant, les compromissions de comptes à privilèges, ou encore les erreurs humaines. Il constitue une réponse cohérente aux enjeux de sécurité actuels, car il met l'accent sur le contrôle dynamique, l'identité numérique, la réduction de la surface d'attaque, et la traçabilité complète des accès.

En résumé on peut retenir :

- ZTA offre un contrôle d'accès granulaire, adaptatif et intelligent, même dans des environnements hybrides ou OT/IT complexes.
- Sa philosophie de méfiance permanente est la plus adaptée aux environnements critiques, où une seule faille peut être fatale.
- Elle permet de protéger la disponibilité des services en limitant la propagation latérale des attaques et en isolant les composants critiques.
- ZTA est soutenue par des standards industriels reconnus (ex. NIST SP 800-207) et une large communauté de pratique.

4.4. 2. Présentation du modèle Zéro Trust

4.4.2.1 Qu'est-ce que le Zéro Trust ?

Le Zéro Trust est une approche de cybersécurité qui repose sur l'idée qu'aucune entité qu'il s'agisse d'un utilisateur, d'un appareil ou d'un service ne doit être considérée comme fiable par défaut. L'accès à chaque ressource est conditionné par une vérification explicite, prenant en compte l'identité de l'utilisateur, la posture de l'appareil, la localisation, le moment de l'accès et le comportement antérieur. Cette logique s'applique aussi bien aux utilisateurs internes qu'externes, aux environnements cloud comme aux réseaux sur site.

4.4.2.2 Quels sont les principes fondamentaux du modèle Zéro Trust ?

Le modèle repose sur des principes fondamentaux : la vérification explicite et continue, l'application du moindre privilège et la présomption de compromission. En pratique, cela signifie que chaque accès est accordé uniquement après une authentification renforcée, une évaluation contextuelle du risque, et une confirmation que la demande est légitime et conforme aux politiques de sécurité. La surveillance reste active tout au long de la session, permettant de détecter toute anomalie en temps réel. Ses principes peuvent s'articulée autour de sept piliers interdépendants visant à renforcer la sécurité des systèmes d'information :

- **Ne jamais faire confiance, toujours vérifier (Never Trust, Always Verify)** : aucun utilisateur ou appareil ne doit être implicitement approuvé ; chaque demande d'accès doit être validée, peu importe sa provenance.
- **Accès au strict nécessaire (Least Privilege Access)** : chaque utilisateur ou processus ne se voit accorder que les autorisations minimales requises, réduisant ainsi la surface d'attaque.
- **Partir du principe d'une compromission (Assume Breach)** : le système est conçu comme si une attaque était déjà en cours, ce qui pousse à segmenter les accès et à limiter les déplacements latéraux des menaces.
- **Vérification explicite (Verify Explicitly)** : chaque accès doit être authentifié selon plusieurs critères (utilisateur, appareil, emplacement, niveau de risque), en utilisant des politiques dynamiques.
- **Micro-segmentation** : le réseau est divisé en zones isolées pour empêcher une compromission d'un segment de se propager à l'ensemble du système.

- **Surveillance continue (Continuous Monitoring)** : les activités des utilisateurs, des appareils et des flux réseau sont surveillées en permanence même après l'autorisation d'accès, afin de détecter toute anomalie.
- **Sécuriser toutes les ressources** : des contrôles de sécurité sont appliqués de façon uniforme à tous les environnements, y compris le cloud, les environnements locaux, les terminaux, etc.

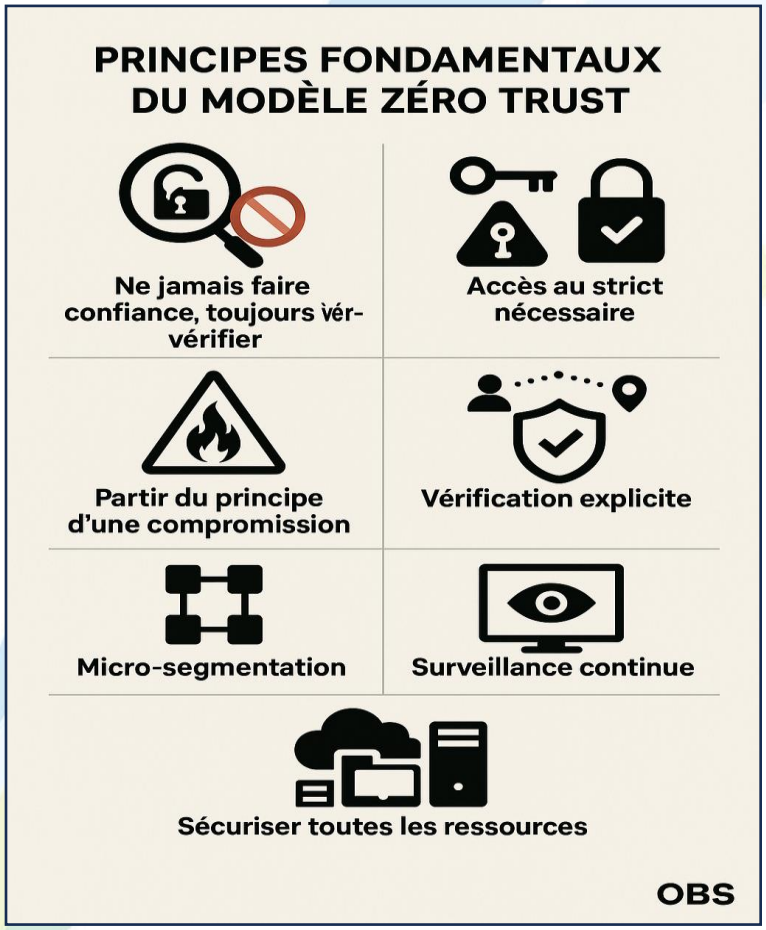


Figure 14 **:** les principes fondamentaux du modèle Zéro Trust

4.4.2.3 L'identité : pivot de la sécurité dans une architecture Zéro Trust

Dans un environnement où les utilisateurs, les applications et les ressources sont de plus en plus dispersés entre le cloud, le télétravail, les appareils mobiles et les réseaux hybrides l'identité devient le seul point de convergence et donc le nouveau périmètre à sécuriser.

Le modèle Zéro Trust repose sur l'idée que chaque **identité**, qu'elle soit humaine ou machine, doit faire l'objet d'un **contrôle strict et continu**. Ce contrôle s'appuie sur plusieurs mécanismes complémentaires :

- **MFA (Multi-Factor Authentication)** : exige que l'utilisateur prouve son identité par au moins deux moyens distincts (mot de passe, empreinte digitale, code reçu sur mobile, etc.).
- **IAM (Identity and Access Management)** : permet de gérer les identités numériques et de contrôler avec précision qui peut accéder à quoi, selon le rôle, la fonction ou le niveau de risque.
- **Certification de conformité des postes** : garantit que les appareils utilisés répondent aux exigences de sécurité (antivirus à jour, chiffrement, configuration approuvée, etc.).

Grâce à ces dispositifs, **l'identité devient un périmètre de sécurité logique, dynamique et indépendant de l'infrastructure physique**. Deplus le périmètre logique centré sur l'identité est complété par plusieurs mesures techniques essentielles. La **micro-segmentation du réseau**, mise en œuvre par des solutions comme *Cisco ACI* ou *VMware NSX*, permet d'isoler les différentes zones internes pour empêcher toute communication non autorisée entre elles. Le **contrôle applicatif** renforce cette approche en limitant l'exécution aux seuls logiciels validés, réduisant ainsi les risques liés aux programmes malveillants ou non conformes. Par ailleurs, une **surveillance continue** est assurée à l'aide de plateformes de type *SIEM* (Security Information and Event Management), *XDR* (Extended Detection and Response) ou *UEBA* (User and Entity Behavior Analytics), qui permettent de détecter des comportements suspects, comme une tentative de connexion à un horaire inhabituel ou depuis une localisation anormale. Enfin, la **protection des données** repose sur leur **chiffrement systématique**, que ce soit en transit via des protocoles comme *TLS 1.3*, au repos avec le chiffrement des disques, ou dans les communications sensibles grâce à des technologies comme *S/MIME* pour les courriels Cela permet de s'adapter à toutes les configurations de travail modernes et de garantir que seul un utilisateur autorisé, disposant d'un appareil conforme, puisse accéder à des ressources sensibles.

Figure 15 : L’identité : pivot de la sécurité dans une architecture Zéro Trust

4.4.2.4 le modèle d’architecture Zéro Trust

Le modèle Zéro Trust repose sur une architecture modulaire. Elle intègre des contrôles au niveau de l’identité, de l’appareil, du réseau, de la session et de l’application. Des composants comme les proxys ZTNA, les passerelles sécurisées, les outils de gestion des terminaux (EDR, MDM), les plateformes de surveillance centralisée (SIEM, SOAR) ou encore les moteurs de politique d’accès s’articulent pour former un système cohérent, piloté par des règles dynamiques et contextualisées.

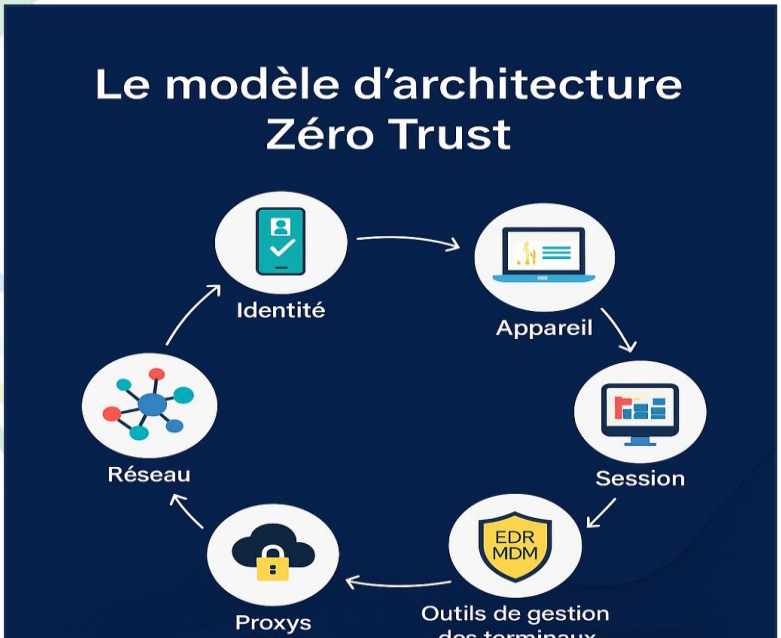


Figure 16 : le modèle d’architecture Zéro Trust

4.4.2.5 les avantages de la mise en œuvre du modèle Zéro trust

La mise en œuvre du modèle Zéro Trust permet de renforcer significativement la posture de cybersécurité d’une organisation en apportant plusieurs bénéfices majeurs. Elle permet d’abord une réduction significative de la surface d’exposition, en appliquant un contrôle strict à chaque point d’accès, qu’il soit interne ou externe. Elle assure également une meilleure résistance aux compromissions, en limitant les déplacements latéraux des attaquants grâce à la micro-segmentation et au principe du moindre privilège. En parallèle, Zéro Trust garantit une traçabilité complète des accès et des activités, facilitant les audits, la détection des incidents et le respect des obligations réglementaires. Ce modèle offre aussi une flexibilité accrue pour les équipes métiers et IT, en permettant un accès sécurisé aux ressources, quel que soit le lieu, le réseau ou le terminal utilisé, sans compromettre l’expérience utilisateur. Enfin, la granularité du contrôle permet une adaptation fine aux contraintes organisationnelles. Ainsi, le modèle Zéro Trust concilie sécurité, agilité et visibilité, ce qui en fait une réponse efficace aux défis des environnements numériques hybrides, mobiles et décentralisés.

Figure 17 : avantage de la mise en œuvre du modèle zéro trust

4.4.2.6 Pourquoi il est adapter pour les infrastructure critique ?

Le modèle Zéro Trust s'avère particulièrement adapté à la protection des infrastructures critiques, où la sécurité est primordiale en raison de la sensibilité des services concernés. Face à l'interconnexion croissante entre systèmes industriels (OT, IoT, SCADA) et réseaux informatiques, il permet un contrôle d'accès précis et contextuel, une isolation des composants critiques via la micro-segmentation, et une surveillance continue des activités. Sa mise en œuvre progressive et sa capacité à offrir une visibilité globale renforcent la détection des menaces et la résilience des systèmes, faisant du Zéro Trust une stratégie efficace pour limiter les risques systémiques dans ces environnements essentiels.

Ce chapitre a comparé les approches classiques et modernes de sécurisation des réseaux. Il a mis en évidence les limites des modèles traditionnels face aux nouvelles menaces, tout en montrant que le modèle Zéro Trust constitue aujourd'hui la solution la plus adaptée pour garantir la disponibilité, la résilience et la sécurité des infrastructures critiques. En combinant vérification continue, contrôle granulaire et surveillance centralisée, ce modèle offre une réponse robuste aux défis actuels.

Le chapitre suivant présentera la mise en œuvre concrète de cette architecture, à travers une proposition technique intégrant les outils, les composants et les configurations nécessaires à la sécurisation d'un réseau critique simulé.

CHAPITRE 5 : MISE EN ŒUVRE DE LA SOLUTION ET ARCHITECTURE PROPOSÉE

5.1 Présentation détaillée des équipements de l'architecture réseau

- FORTIGATE

le pare-feu **fortigate** assure la sécurité périmétrique du réseau : il filtre et inspecte le trafic, gère le nat et le routage, applique des politiques firewall, segmente les flux via vlan, prend en charge ztna et l'authentification multifacteur, tout en s'intégrant à fortianalyzer et fortiauthenticator ; son interface web est accessible à l'adresse `https://192.168.1.99`, avec `port1` dédié au lan interne, `port2` au lien wan/internet, et des ports supplémentaires configurables .

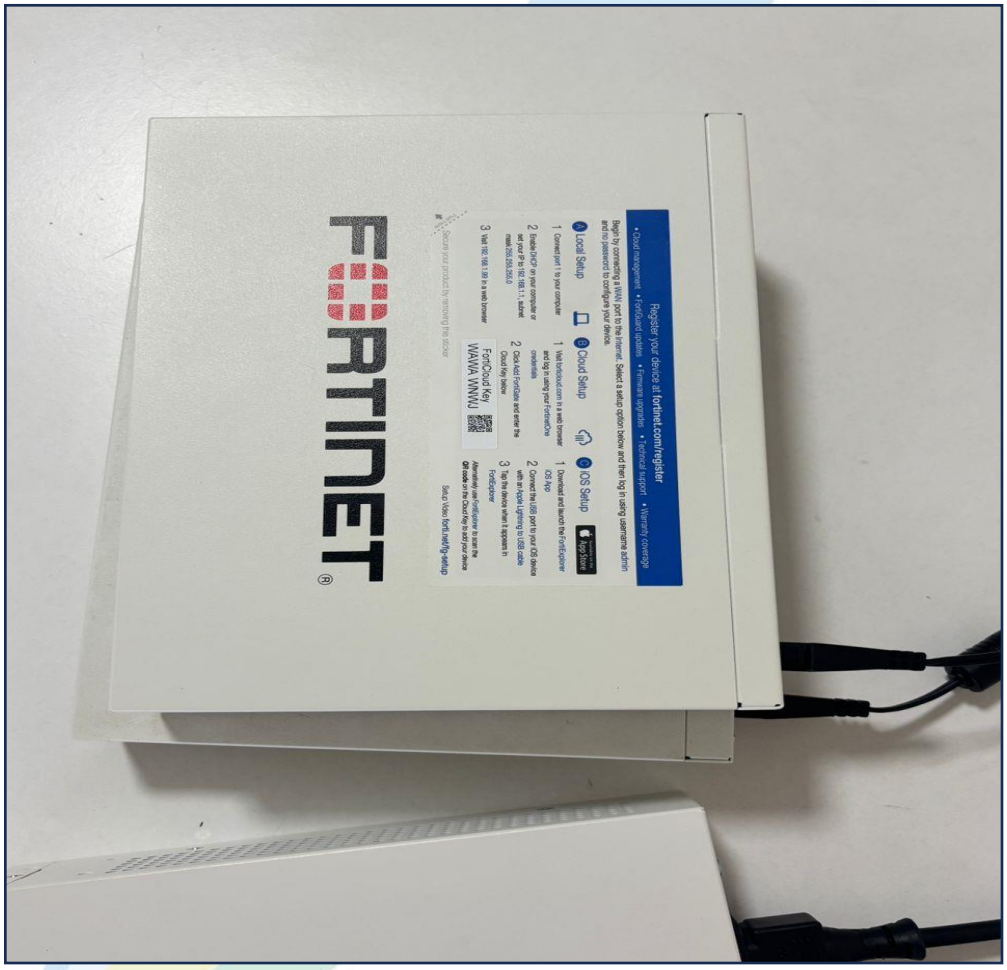


Figure 18 :Fortigate

Fortiswitch

Le **FortiSwitch** est un commutateur manageable de niveau 2/3 conçu pour fonctionner de manière intégrée avec les pare-feux FortiGate ; il assure l'interconnexion des différents VLANs, la segmentation du trafic, la priorisation (QoS), et l'application de politiques de sécurité. Il peut être

géré localement ou via FortiLink (mode de gestion centralisée depuis le FortiGate), simplifiant ainsi la configuration, la surveillance et la mise à jour du réseau. Il dispose de ports configurables pour les VLANs Admin, Utilisateurs, Invités, IoT ou Serveurs, et constitue une brique essentielle dans une architecture Zero Trust.

Figure 19 : fortiSwitch

FortiAp-221E

Le **FortiAP-221E** est un point d'accès WiFi sécurisé de la gamme Fortinet, conçu pour fournir une connectivité sans fil performante et segmentée au sein d'un réseau d'entreprise. Géré de manière centralisée via un contrôleur (souvent le FortiGate en mode FortiLink), il prend en charge plusieurs SSID avec affectation VLAN dynamique, permettant de séparer les accès internes, invités, IoT ou BYOD. Il supporte les protocoles de sécurité WPA2/WPA3-Enterprise avec authentification RADIUS ou LDAP, et peut intégrer un portail captif pour les visiteurs. Il joue un rôle crucial dans une architecture Zero Trust en contrôlant précisément qui accède au réseau sans fil, quand et comment.

Figure 20 : Access Point (fortiAp)

. Serveur Active Directory (AD)

Ce serveur centralise la **gestion des identités** et des **autorisations** dans le réseau. Il permet de contrôler **qui peut accéder à quoi**, d'appliquer des **politiques de sécurité** (GPO), de gérer les mots de passe et les groupes utilisateurs.

Figure 21 :Propriete du serveur

Ethernet

Ce routeur 4G/LTE fourni par Orange assure la connectivité Internet de l'infrastructure réseau via le réseau mobile. Il peut être utilisé soit comme **accès principal à Internet** .

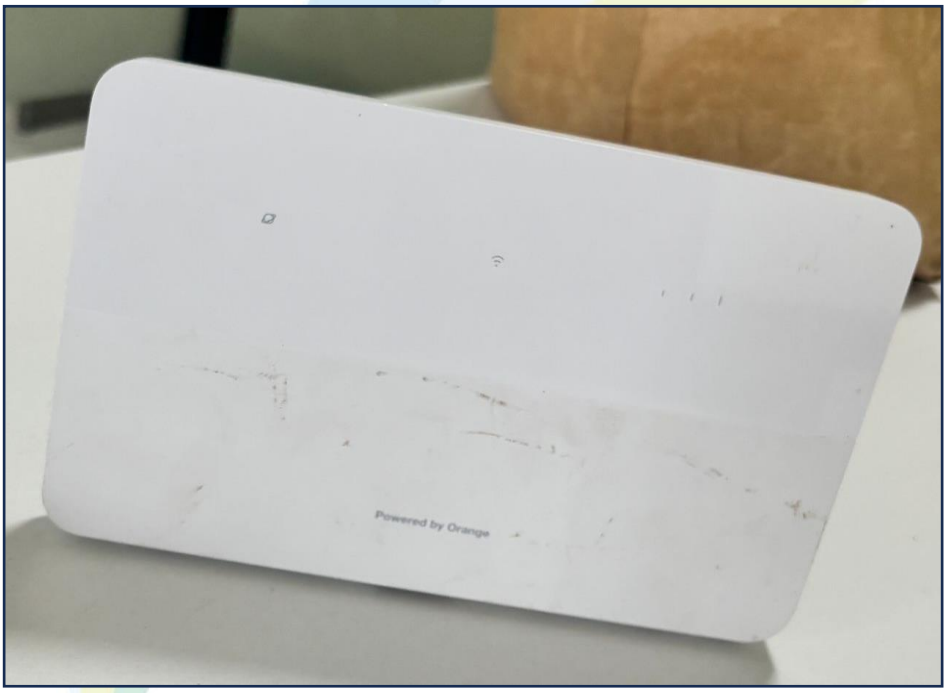


Figure 22 :accès internet

5.2 Proposition de topologie à améliorer

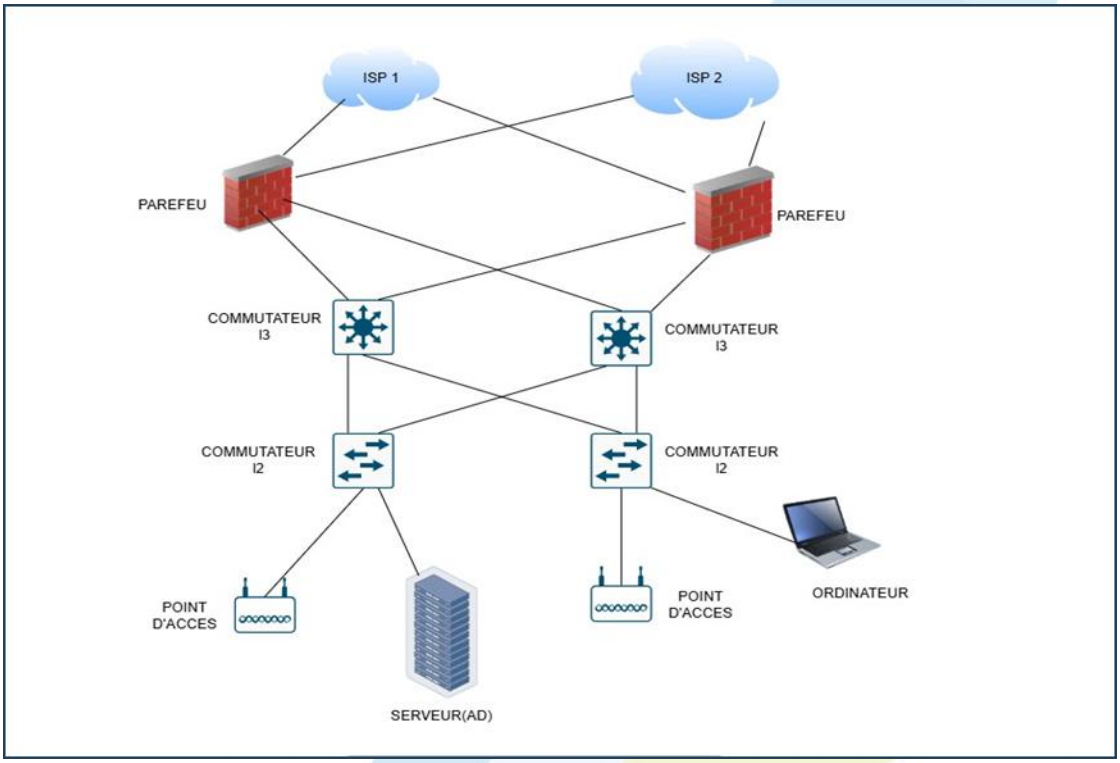


Figure 23 : Modèle d'architecture réseau d'entreprise avec segmentation, pare-feu et Active Directory

5.3 Implémentation

Pour améliorer l'architecture de sécurité proposée, nous allons dans un premier temps présenter les grandes lignes du modèle Zéro Trust, qui constitue une approche optimisée, cohérente et parfaitement adaptée aux exigences des infrastructures critiques modernes.

Ce modèle repose sur le principe fondamental du « **ne jamais faire confiance, toujours vérifier** ». Il vise à réduire la surface d'attaque, à contrôler rigoureusement chaque accès, et à renforcer la résilience du système face aux menaces, qu'elles proviennent de l'extérieur ou de l'intérieur du réseau.

Les composantes clés de cette architecture incluent notamment :

- **Une segmentation logique du réseau**, mise en œuvre à travers des **VLANs isolés**, afin de cloisonner les ressources critiques et limiter les mouvements latéraux en cas de compromission ;
- **Une authentification forte** des utilisateurs et des appareils, via un mécanisme de **double authentification (2FA)**, garantissant l'identité et la légitimité de chaque tentative d'accès ;

- **Un monitoring continu et intelligent** des activités réseau, assuré par un système de **SIEM** tel que **WAZUH**, capable de centraliser les logs, détecter les comportements suspects et générer des alertes en temps réel.

5.3.1. L'accès initial au FortiGate via liaison Ethernet