Université Paris-Saclay

Master 2 Computer Network Systems (CNS–SR)

Projet R&D

Zero Trust Networking

Présenté par :
SOORIYAKUMAR Karthikan
DIALLO Boubacar

Encadrant :
Monsieur Mehdi Denou

Année universitaire : 2025–2026

Remerciements

Nous souhaitons tout d'abord exprimer notre profonde gratitude à nos familles, qui nous ont soutenus avec patience, confiance et encouragement tout au long de notre parcours. Leur présence et leur bienveillance ont été un pilier essentiel dans la réalisation de ce mémoire.

Nous tenons aussi à remercier chaleureusement l'ensemble des enseignants du Master *Computer Network Systems* de l'Université Paris-Saclay, qui ont contribué à notre formation et à notre progression.

Nos remerciements les plus sincères vont tout particulièrement à **Monsieur Mehdi Dénou**, notre encadrant, pour son accompagnement constant, ses conseils avisés et sa pédagogie toujours stimulante. C'est également sous sa direction que nous avions réalisé, dès le Master 1, le projet *Spine*, qui a été pour nous une expérience extrêmement formatrice et fondatrice. Sa disponibilité et son exigence ont largement contribué à la qualité de ce travail.

Nous remercions également **Monsieur Pascal Petit**, dont les enseignements l'année dernière ont profondément renforcé notre compréhension des architectures et technologies réseau. Son sens de la vulgarisation et sa rigueur nous ont permis d'aborder ce mémoire avec des bases solides.

Nous adressons enfin nos remerciements à **Docteur Abdelhamid Agoulmine**, dont les cours ont apporté une vision élargie et structurante du domaine, en particulier sur les aspects avancés des réseaux et de la gestion des systèmes.

À toutes celles et ceux qui, de près ou de loin, ont contribué à ce parcours : merci.

Table des matières

Introduction

L'évolution des usages numériques, cloud, mobilité, télétravail et objets connectés a profondément transformé les réseaux. Dans cet environnement distribué, le modèle de sécurité traditionnel ne suffit plus. Le **Zero Trust** s'impose alors comme une approche plus adaptée : ne jamais accorder d'accès par défaut et vérifier chaque action en fonction du contexte réel.

Cependant, la littérature traite surtout de l'authentification et de l'attribution des droits, et beaucoup moins d'une question pourtant essentielle : **que faire si un utilisateur devient soudainement risqué après avoir été autorisé ?** Un appareil peut être compromis en cours de session ou un comportement anormal peut apparaître. Il devient alors nécessaire de **révoquer automatiquement** les droits déjà accordés.

Les réseaux programmables, en particulier le *Software-Defined Networking* (SDN), offrent une solution intéressante grâce à leur capacité à modifier rapidement et centralement les règles du réseau. Ils permettent d'envisager un **Zero Trust dynamique**, capable de réagir en temps réel.

La problématique de ce mémoire est donc :

> *Comment mettre en place un contrôle d'accès Zero Trust capable de révoquer automatiquement les droits d'un utilisateur ou d'un appareil devenu suspect, en exploitant des informations de contexte dans un environnement SDN ?*

Ce mémoire présente les bases du Zero Trust, un état de l'art ciblé sur les limites actuelles, puis une expérimentation démontrant la faisabilité d'un mécanisme de révocation dynamique dans un réseau SDN minimaliste.

1. Les bases du Zero Trust

Zero Trust est un **modèle de sécurité** utilisé pour protéger les réseaux informatiques avec pour principe "Ne faire jamais confiance, toujours vérifier". Cette approche remet en cause la confiance des utilisateurs et appareils qu'ils soient de l'extérieur ou de l'intérieur afin de réduire la surface d'attaques. Ce modèle se concentre plus à protéger une ou plusieurs ressources plutôt que défendre un périmètre. Un accès aux ressources exige une vérification avant d'être accordé.

1.1 Du périmètre au Zero Trust

La sécurité des architectures réseaux traditionnelles se repose sur la protection du périmètre en empêchant seulement les attaques extérieures par l'utilisation d'un ou plusieurs pare-feux, et accorde beaucoup de confiance aux éléments présents dans le réseau interne. Ce dernier a aussi quelques sécurités comme la segmentation (VLAN, sous-réseaux) et la liste de contrôle d'accès au niveau liaison. Mais cette approche ainsi que ces implémentations ne suffissent pas face aux cyberattaques modernes comme l'hameçonnage. De même que cette approche de défense du périmètre est devenue obsolète avec l'émergence des usages modernes tels que le cloud ou le télétravail se situant hors du réseau interne.

Selon le **NIST SP 1800-35E** *(référence [2], p. 9)*, la sécurité périmétrique repose sur une hypothèse erronée : celle que tout ce qui est à l'intérieur du réseau est digne de confiance. Or, cette vision ne prend pas en compte la mobilité des utilisateurs, les services hébergés sur des clouds publics et la multiplication des connexions tierces. Le document souligne que la frontière réseau « ne peut plus être considérée comme une zone de confiance unique », car les menaces internes et les compromissions d'identités sont devenues aussi critiques que les attaques externes.

Ainsi, le modèle **Zero Trust** propose de déplacer la confiance vers un mécanisme dynamique et contextuel : chaque requête d'accès doit être évaluée selon plusieurs critères comme l'identité, l'état du terminal, le type de ressource visée et le comportement récent de l'utilisateur. Cette approche permet une **vérification continue** plutôt qu'une simple authentification initiale, garantissant que la sécurité ne dépend plus d'une frontière physique mais d'une évaluation en temps réel du risque.

Zero Trust intervient donc pour ces raisons et devient de plus en plus utilisé dans

les architectures réseaux modernes, car ses mécanismes s'appliquent aussi bien à l'extérieur (cloud, télétravail) qu'à l'intérieur du réseau. En d'autres termes, il redéfinit la sécurité comme une **défense de zones multiples et adaptatives**, dépassant la simple périmétrisation.

Analogie : du modèle périmétrique au Zero Trust

Pour mieux comprendre cette évolution, imaginons deux maisons : l'une construite selon l'ancien modèle périmétrique, et l'autre selon le modèle Zero Trust.

Le modèle périmétrique : la maison à une seule serrure. Dans la maison traditionnelle, seule la **porte d'entrée** est verrouillée. Une fois à l'intérieur, les habitants ou les visiteurs peuvent se déplacer librement : accéder à la cuisine, au salon ou même au coffre-fort sans autre vérification. C'est exactement le principe de la sécurité périmétrique : tant qu'on est "à l'intérieur" du réseau, on est considéré comme sûr.

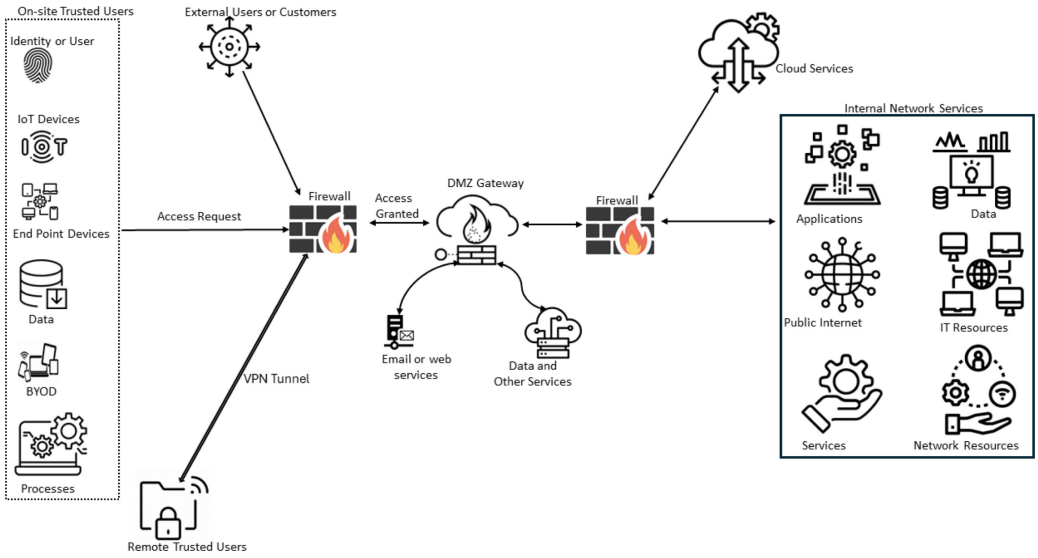

FIGURE 1.1 – Modèle de sécurité périmétrique : une seule barrière protège tout le réseau interne. Illustration inspirée de la **Figure 5** dans *Azad, M. et al., Verify and Trust : A Multidimensional Survey of Zero-Trust*, (réf. [6]).

Le modèle Zero Trust : la maison intelligente et surveillée. Dans la maison Zero Trust, chaque **pièce sensible** possède sa propre serrure et un système d'authentification. La porte d'entrée vérifie l'identité du visiteur, mais ensuite, l'accès à la cuisine, au bureau ou au coffre-fort nécessite une nouvelle autorisation. De plus, des capteurs vérifient en permanence le comportement des occupants : s'ils se déplacent dans une zone inhabituelle, le système peut demander une nouvelle authentification ou bloquer temporairement l'accès.

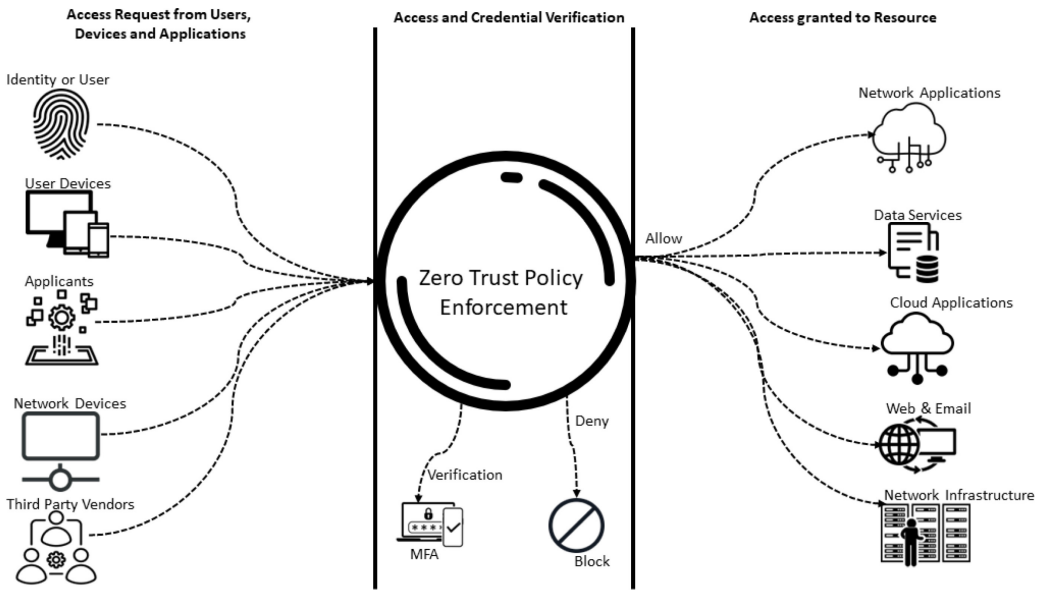

FIGURE 1.2 – Modèle Zero Trust : chaque ressource est protégée par sa propre politique d'accès et de contrôle. Illustration inspirée de la **Figure 3** dans *Azad, M. et al., Verify and Trust : A Multidimensional Survey of Zero-Trust*, (réf. [6]).

Cette analogie montre que le Zero Trust ne cherche pas seulement à fermer la porte d'entrée, mais à instaurer une **confiance conditionnelle et renouvelée en permanence**. Même un utilisateur déjà "à l'intérieur" doit prouver qu'il est toujours légitime, à chaque étape de son parcours.

1.2 Référentiels et modèles

Le modèle *Zero Trust* s'appuie sur plusieurs cadres de référence qui définissent comment évaluer, contrôler et révoquer les accès. Dans ce mémoire, nous avons retenu les référentiels du **NIST**, de l'**ANSSI**, ainsi que plusieurs travaux récents qui proposent des mécanismes de décision plus dynamiques, en lien direct avec notre problématique de révocation automatique.

1.2.1 Référentiels du NIST

Le **NIST SP 800-207** constitue la base architecturale du Zero Trust. Il décrit la séparation entre la décision (PE), l'application (PA) et l'exécution (PEP), et introduit l'idée d'une évaluation continue du contexte. Le guide **SP 1800-35E** complète cette vision en montrant comment intégrer IAM, supervision et segmentation dans un déploiement progressif. Ces documents structurent notre analyse mais laissent ouvertes les questions liées à la réévaluation instantanée des accès en cours de session.

1.2.2 Modèles orientés révocation dynamique

Plusieurs travaux récents s'intéressent précisément à ces limites. Nous avons retenu les modèles suivants, qui proposent chacun une réponse partielle au besoin de réévaluation continue :

— **OAuth2 et la révocation des jetons** : propose une invalidation explicite des jetons, mais la propagation n'est pas instantanée.

— **Continuous Access Evaluation (CAE) — Microsoft** : permet de révoquer les sessions en fonction d'événements (changement d'IP, posture, compromission), et pose les bases d'un contrôle réellement continu.

— **Shared Signals Framework (SSF) et CAEP — OpenID Foundation** : standardisent l'échange d'événements de sécurité entre services. Ces mécanismes apportent une vision interopérable de la révocation.

— **BeyondCorp — Google** : propose un modèle centré sur un proxy d'accès, permettant une vérification systématique à chaque requête. Couplé au standard RISC, il améliore la remontée d'incidents.

Ces approches ont été sélectionnées car elles traitent explicitement du maintien ou de la révocation d'une session, un aspect peu détaillé dans les référentiels initiaux du Zero Trust.

1.2.3 Approche française de l'ANSSI

L'**ANSSI** propose une lecture pragmatique du Zero Trust, centrée sur la gouvernance des accès, la supervision et la mise en œuvre progressive. Bien que ses documents n'entrent pas dans le détail des mécanismes de révocation temps réel, ils constituent un cadre structurant pour définir les niveaux de confiance et les scénarios d'accès.

Dans la suite du mémoire, nous mobilisons ces différents référentiels afin d'analyser les limites actuelles du Zero Trust, notamment en matière de prise en compte des changements de contexte et de mise à jour des décisions d'accès.

1.3 Principes clés

Le modèle Zero Trust repose sur plusieurs principes qui permettent de sécuriser les ressources en s'appuyant sur des informations issues des utilisateurs, des appareils et des journaux systèmes. Les éléments essentiels sont les suivants :

— **Vérification continue et contextuelle :** chaque demande d'accès est évaluée en fonction de plusieurs facteurs, comme l'identité de l'utilisateur (IAM, MFA), l'état de l'appareil (présence de menaces, version du système, conformité via un EDR) ou

encore des éléments de contexte tels que l'heure, la localisation ou les comportements récents.

— **Principe du moindre privilège :** les utilisateurs ne reçoivent que les droits strictement nécessaires, et souvent pour une durée limitée (JIT/JEA). Cela réduit les risques d'abus ou d'élévation de privilèges en cas de compromission.

— **Micro-segmentation :** le réseau est divisé en petits segments avec leurs propres règles d'accès. Cette organisation limite les déplacements latéraux d'un attaquant et renforce la maîtrise des flux internes.

— **Journalisation et détection centralisées :** les événements et logs sont collectés dans une plateforme unique afin de détecter rapidement les comportements anormaux (par règles ou analyse comportementale, comme l'UEBA) et d'automatiser certaines réponses aux incidents.

Les composants de Zero Trust

Le NIST structure le Zero Trust autour de trois rôles :

— **Policy Engine (PE)** : décide des accès selon l'identité, la posture et le niveau de risque ;

— **Policy Administrator (PA)** : applique les décisions du PE ;

— **Policy Enforcement Point (PEP)** : autorise ou bloque le trafic.

Ce modèle introduit une **boucle de rétroaction continue** : collecte du contexte, décision, application, puis réévaluation. Le NIST montre également que cette architecture peut être adoptée progressivement, sans transformation complète des infrastructures.

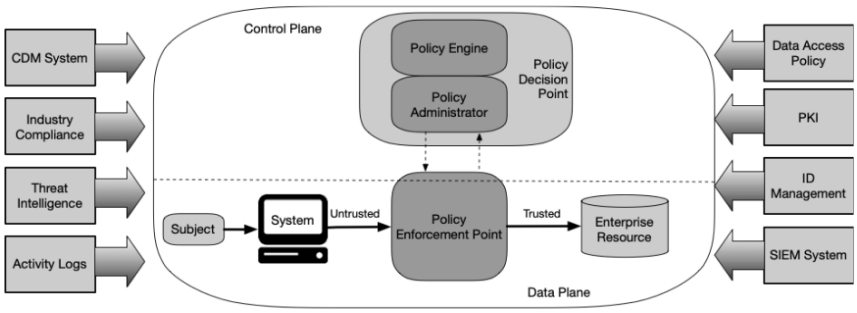

FIGURE 1.3 – Schéma simplifié inspiré du modèle NIST SP 800-207.

2. L'état de l'art

2.1 Briques techniques et solutions

2.1.1 Monitoring continue et méthode de détection des anomalies

Le monitoring en temps réel et la détection d'anomalies constituent le fondement de tout système de révocation automatique. Sans capacité à détecter rapidement qu'un utilisateur ou un appareil est devenu suspect, aucune révocation ne peut être déclenchée à temps pour prévenir les dommages.

Sources de télémétrie (réf[15][16]) :

Données au niveau des flux :

— Volume, fréquence et direction du trafic

— Protocoles utilisés et ports de destination

— Patterns temporels (heures d'accès inhabituelles)

— Géolocalisation des connexions

Télémétrie des appareils :

— État des agents de sécurité (antivirus, EDR)

— Processus en cours d'exécution

— Modifications du système de fichiers

— Connexions réseau établies

— Utilisation des ressources (CPU, mémoire, disque)

Logs d'authentification et d'accès :

— Tentatives d'authentification

— Accès aux ressources et patterns d'utilisation

— Élévations de privilèges

— Changements de configuration

Sondes terminaux et points d'inspection :

— Inspection profonde des paquets (DPI)

— Analyse de contenu et de charge utile

— Détection de signatures de malware

Approches de détection par apprentissage automatique :

Les travaux récents s'appuient massivement sur l'apprentissage automatique pour détecter les anomalies comportementales (réf.[15][26][31]) :

Les travaux de Mangla (réf[26]) proposent une architecture Zero Trust pilotée par l'IA qui intègre des modèles ML pour l'analyse comportementale en temps réel, permettant de détecter des patterns d'accès anormaux (accès à des ressources inhabituelles, volumes de données exfiltrées, horaires d'activité atypiques) et de déclencher automatiquement des actions de révocation ou de renforcement d'authentification.

Kumar et al. (réf.[15]) décrivent l'algorithme AACTMA (Adaptive Access Control and Threat Mitigation Algorithm) qui utilise le machine learning pour établir des références comportementales dans des environnements BYOD. Le système détecte les anomalies comportementales (tentatives d'accès répétées, scans de réseau, communications avec des IPs malveillantes) et reconfigure dynamiquement les politiques SDN pour isoler les dispositifs suspects.

Les travaux de Charalampos Katsis et Elisa Bertino utilisent un modèle de séquence profonde (CALSeq2Seq) pour la détection d'anomalies en temps réel (réf.[31]). L'architecture comprend :

— Module de collecte : Agrégation de flux réseau depuis le contrôleur SDN

— Module d'apprentissage : Modèle séquence-à-séquence entraîné sur le trafic normal

— Module de détection : Comparaison en temps réel avec les prédictions du modèle

— Module d'application : Mise à jour dynamique des règles de flux pour bloquer les anomalies

Performances :

— Précision de détection d'anomalies : 99,56%

— Maintien de 80,5% du débit sous attaque dans des simulations Mininet

— Capable de détecter des attaques DDoS, scans de ports, et mouvements latéraux

Limitations :

— Évaluation limitée à des simulations (pas de déploiement en production)

— Taux de faux positifs non explicitement rapporté

— Scalabilité pour les très grands réseaux non démontrée

— Coût computationnel de l'inférence en temps réel non quantifié

2.1.2 Score de confiance dynamique

Plusieurs études présentent des modèles de confiance dynamique qui combinent divers signaux (identité, comportement, posture, contexte) pour générer un score de risque ou de confiance évoluant en temps réel (réf.[28][18]). Ces scores ont un impact direct sur les décisions d'accès : un score de confiance élevé peut permettre un accès élargi, tandis qu'une diminution du score entraîne des actions progressives (demande de réauthentification, restriction des privilèges, révocation totale).

Kapoor et Varma (réf.[18]) introduisent un modèle d'évaluation de confiance dynamique pour SDN qui prend en compte des métriques de comportement réseau, de conformité des dispositifs, et d'historique d'accès pour établir un score de confiance. Ce modèle dirige des actions SDN commme redirection de flux, terminaison de session, déploiement de règles de remédiation en fonction du niveau de confiance déterminé.

L'architecture AI-ZTA de Mangla (réf.[28]) propose une orchestration de politiques multi-couches où les modèles ML évaluent des scores de risque en temps réel, permettant des décisions d'accès adaptatives et automatisées. Le système a pour objectif de diminuer les faux positifs grâce à un apprentissage continu et à l'intégration de contextes variés.

Limitations identifiées : Les modèles de scoring de risque nécessitent un calibrage minutieux des poids et des seuils pour éviter les faux positifs et négatifs. La transparence et l'explicabilité des décisions de scoring sont cruciales pour la conformité réglementaire et l'acceptation par les utilisateurs, mais les modèles ML complexes peuvent s'avérer opaques (réf.[28][18]). En outre, les métriques de performance (latence de calcul du score, overhead computationnel) sont rarement abordées.

2.1.3 Le contrôleur SDN

Dans une architecture Zero Trust, le **contrôleur SDN** décide et applique les règles d'accès. Il peut créer des chemins sécurisés, installer des règles sur les équipements ou isoler une machine compromise. Le SDN sépare le plan de contrôle du plan de données, ce qui rend le réseau plus flexible.

Cette séparation présente plusieurs bénéfices pour Zero Trust :

— Visibilité centralisée : Le contrôleur SDN offre une vue d'ensemble de la topologie du réseau et des flux, facilitant l'analyse du trafic et la détection d'anomalies à l'échelle du réseau réf.[18][17].

— Programmabilité : Les politiques de sécurité peuvent être converties dynamiquement en règles de flux OpenFlow, permettant une adaptation instantanée aux changements de contexte et de risque réf.[18][17].

— Granularité : SDN permet un contrôle au niveau du flux (5-tuple : IP source/destination, port source/destination, protocole), fournissant une granularité précise pour l'ap-

plication des politiques et la microsegmentation réf[18].

Le NIST décrit deux approches principales :

— **Approche par agent :** un agent installé sur l'appareil envoie son état au contrôleur (sécurité, version, configuration). Cette solution est moins adaptée au BYOD.

— **Approche par portail :** le trafic est redirigé vers un portail qui authentifie l'utilisateur et applique les politiques d'accès sans installer d'agent, ce qui convient mieux aux appareils personnels.

Ces approches peuvent être combinées selon les usages.

Le SDN en tant que solution pour la révocation des accès au niveau réseau

L'intégration SDN propose une alternative ou un complément aux mécanismes d'invalidation de tokens au niveau applicatif, en permettant une application au niveau réseau :

Terminaison de Session Réseau :

Lorsqu'un comportement anormal ou une dégradation de posture est détecté, le contrôleur SDN peut mettre en place des règles de flux pour bloquer tous les paquets liés à la session compromise (identifiée par 5-tuple ou par des attributs de couche supérieure extraits via DPI). Les connexions TCP en cours sont ainsi interrompues, mettant effectivement fin à la session (réf.[18][17]).

Avantages : Révocation immédiate indépendante des mécanismes applicatifs ; applicable à tout type de trafic (non limité aux protocoles supportant l'invalidation de tokens) réf.[18][17].

Limitations : Nécessite une identification précise des flux associés à l'utilisateur ou au dispositif révoqué ; peut mettre fin brutalement à des sessions légitimes si l'identification est imprécise ; ne prévient pas la réutilisation de tokens valides pour établir de nouvelles sessions (nécessite une coordination avec les mécanismes applicatifs) réf.[18][17].

Quarantaine dynamique :

Au lieu de couper complètement l'accès, le système peut transférer le dispositif vers un réseau de quarantaine avec un accès limité. L'utilisateur peut être informé de la situation et orienté vers des actions de remédiation (mise à jour de logiciels, réauthentification, scan de sécurité) réf[15][17].

L'approche AACTMA (réf.[15]) illustre la quarantaine dynamique dans des environnements BYOD : les dispositifs présentant des anomalies comportementales ou des faiblesses de posture sont isolés dans un segment de quarantaine grâce à une reconfiguration SDN, limitant leur accès tout en maintenant une connectivité pour la remédiation.

Application de la Contrôle d'Accès Basé sur les Fonctions (FBAC) :

Le cadre Gargoyle (réf.[17]) propose un modèle FBAC dans lequel les politiques d'accès sont établies en fonction des opérations (fonctions) que l'utilisateur souhaite réaliser, plutôt que simplement sur les ressources. Les applications SDN extraient les Attributs

de Contexte Réseau (NCA) des flux (par exemple, détection de tentatives de copie de fichiers, de téléchargements massifs, d'accès à des APIs sensibles) et mettent en œuvre des règles de filtrage détaillées.

Exemple : Si un utilisateur essaie de copier un fichier sensible alors que son score de risque a augmenté, Gargoyle peut spécifiquement bloquer l'opération de copie tout en permettant la lecture, offrant ainsi une révocation partielle et contextuelle (réf.[17]).

Avantages :

— Application contextuelle et précise fondée sur les opérations réelles plutôt que sur les seules ressources.

— Intégration approfondie avec les fonctionnalités SDN pour automatiser la réponse.

— Résilience face aux attaques internes en restreignant les actions même pour les utilisateurs authentifiés.

Limitations :

— L'extraction de NCA par le biais de DPI peut s'avérer complexe pour le trafic chiffré

— Évaluation principalement architecturale et de faisabilité ; les métriques quantitatives concernant la latence de révocation et la scalabilité sont limitées.

— Absence de mécanisme explicite pour l'invalidation des tokens applicatifs ; l'accent est mis sur l'application des règles réseau.

2.2 Avancées récentes et tendances

Le Zero Trust évolue aujourd'hui vers des approches plus opérationnelles et automatisées. L'objectif n'est plus seulement de supprimer la confiance implicite, mais d'**évaluer en continu** la fiabilité des utilisateurs, des appareils et du contexte pour adapter les décisions d'accès. Les travaux récents montrent une transition vers une sécurité plus dynamique et fondée sur le risque.

2.2.1 Implémentation de Tao Chuan et al. (2020)

Tao Chuan et ses collègues proposent une mise en œuvre concrète du Zero Trust destinée aux environnements hybrides. Leur modèle repose sur quatre composants : un serveur d'application, un serveur d'évaluation, un centre de génération de jetons (TGC) et une passerelle. L'état du serveur (configuration, vulnérabilités, ports, comptes) est analysé pour produire un score ; si celui-ci est suffisant, un **jeton temporaire** est délivré et validé par la passerelle avant d'établir une connexion sécurisée. Ce fonctionnement illustre la tendance vers un contrôle d'accès **adaptatif**, basé sur la posture réelle du système.

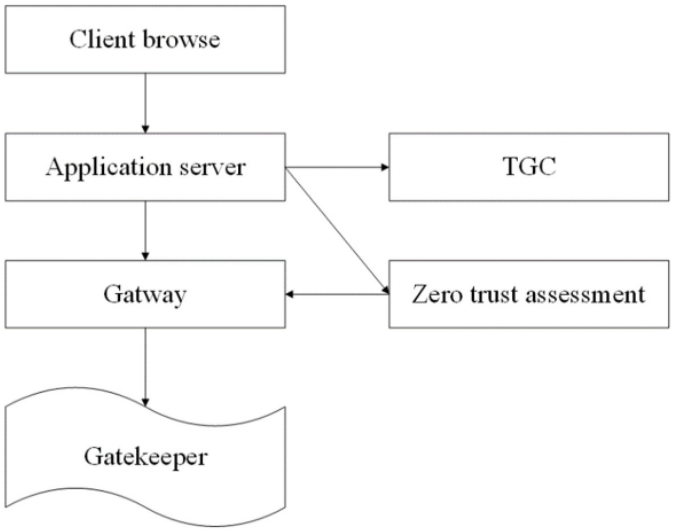

Figure 1. Block diagram of zero-trust architecture

FIGURE 2.1 – Architecture Zero Trust proposée par Tao Chuan et al. (2020).

2.2.2 Approche pragmatique de l'ANSSI

L'ANSSI propose une adaptation réaliste du Zero Trust pour les organisations françaises. Elle met en avant :

— une **gouvernance de la confiance** basée sur le risque et la traçabilité ;

— un **déploiement progressif** (cartographie, segmentation, supervision) ;

— l'intégration et la corrélation des **signaux de sécurité** pour ajuster automatiquement les politiques.

L'agence souligne aussi le rôle essentiel du **facteur humain** : sensibilisation, compréhension des enjeux et comportement des utilisateurs.

2.2.3 Intégration Blockchain ML dans Zero Trust

SecureChain-ZT combine apprentissage automatique, apprentissage par renforcement et blockchain pour créer un système Zero Trust robuste (réf.[30)]. Les composants clés incluent :

— Blockchain d'identité : Enregistrement immuable des identités et des authentifications

— ML pour détection : Modèles d'apprentissage automatique pour identifier les menaces

— Apprentissage par renforcement : Adaptation des politiques basée sur les résultats

— Microsegmentation dynamique : Reconfiguration automatique des segments réseau

Performances :

— Précision d'authentification : 97,8-98,6%

— Précision de détection de menaces : 99,3%

— Temps de mise à jour de politique : 180 ms

— Réduction de latence : 62,6% par rapport aux approches traditionnelles

Avantages :

— Traçabilité complète des décisions d'accès (audit blockchain)

— Résistance à la falsification des logs

— Adaptation continue via apprentissage par renforcement

Limitations :

— Latence accrue due au consensus blockchain (bien que mitigée à 180 ms)

— Complexité opérationnelle élevée

— Coût de stockage et de calcul de la blockchain

— Scalabilité limitée par le débit de la blockchain

2.2.4 Continuous Access Evaluation (CAE)

Le Continuous Access Evaluation est une évolution importante comparé aux modèles d'authentification traditionnels. Au lieu d'accorder un accès pour une durée fixe (jetons), le CAE réévalue en permanance la légétimité de l'accès. Les systèmes d'entreprise modernes reposent souvent sur des jetons d'accès valables pendant une durée fixe, ce qui ignore les changements de contexte (position, état du poste, comportement) survenant pendant une session et crée des risques si un jeton est compromis. CAE vise à rendre l'autorisation continue et réactive, en informant les participants d'une session à chaque événement pertinent afin qu'ils réévaluent l'accès. (réf.[29])

Concept et architecture

CAE utilise un modèle publish–subscribe asynchrone où des émetteurs (Transmitters) publient des événements (Events) encodés en Security Event Tokens et des récepteurs (Receivers) s'abonnent à des flux (Streams) pour recevoir uniquement les sujets qui les intéressent . Le flux typique inclut la publication de changements de contexte, la notification des fournisseurs d'identité (IdP) et la remédiation par le Relying Party selon la décision de politique. (réf.[29])

Standardisation Shared Signals Framework SSF :

Le SSF (OpenID Foundation) est la première réalisation standard de CAE et définit deux profils principaux : CAEP (Continuous Access Evaluation Protocol) pour événements de session et d'appareil, et RISC pour incidents et sécurité de compte. CAEP spécifie des types d'événements clés (session révoquée, changement d'attributs de jeton, changement de conformité de l'appareil, etc.) et des claims optionnels pour contexte et traçabilité. (réf.[29])

Adoption et cas réels

Les plus grands acteurs sont déjà impliqués : Microsoft a intégré CAE dans Entra ID (tokens CAE, Conditional Access) et supporte divers cas d'usage (MFA, état du device, localisation). Google utilise des idées proches via BeyondCorp et le profil RISC pour Cross-Account Protection, et Cisco propose des implémentations open source et participe au développement du SSF. (réf.[12][13][14])

Limites

L'article montre certaines limites de CAE : la latence entre l'émission et l'application effective des règles et la compatibilité entre les IdP et SDN.

2.3 Divergences et lacunes

Les travaux récents montrent que, malgré une base commune, les approches Zero Trust diffèrent encore sur plusieurs points et présentent des limites importantes pour une mise en œuvre opérationnelle.

2.3.1 Divergences

La littérature met en avant plusieurs orientations différentes :

— **Zero Trust assisté par IA :** certains auteurs proposent d'utiliser l'IA pour analyser en continu les flux et ajuster automatiquement les politiques. Cette piste est prometteuse mais pose des questions de fiabilité et de gestion des faux positifs.

— **Modèles décentralisés :** des approches basées sur des jetons distribués cherchent à réduire la dépendance à une autorité centrale. Elles améliorent la résilience, mais rendent plus complexe la gestion et la révocation des accès.

— **Trust score dynamique :** d'autres travaux calculent un score pour chaque utilisateur ou appareil afin d'adapter les droits en fonction de la posture. Le défi principal reste le choix de métriques fiables et non biaisées.

— **Interprétations variées :** la communauté ne partage pas encore une définition opérationnelle unique. Certains mettent l'accent sur l'identité, d'autres sur la micro-segmentation ou la posture du terminal.

2.3.2 Lacunes

Même si le Zero Trust progresse, plusieurs limites restent visibles dans les études récentes :

— **Tests rarement réalisés en conditions réelles.** Beaucoup de travaux restent théoriques. Par exemple, Alnaim (réf. [30]) obtient une très bonne précision (**98,7 %**) et une mise à jour des politiques en **180–250 ms**, mais uniquement dans un environnement contrôlé, loin d'un vrai réseau 5G.

— **Latence ajoutée par les décisions.** Les modèles basés sur l'IA ou le SDN introduisent une latence supplémentaire. ZT-SDN (réf. [31]) ajoute en moyenne **12–25 ms** pour analyser le trafic et mettre à jour les règles, ce qui peut ralentir la révocation.

— **Machine Learning.** Les ML nécessitent une grande quantité de données (sources de télémetrie) et continues, affectant la confidentialité et la performance. De plus, les attaquant peuvent adapter leur comportement pour échapper à la détection (adversaire).

— **Surcharge du contrôleur SDN.** Lorsqu'il reçoit trop d'événements Zero Trust, le contrôleur peut devenir un goulot d'étranglement. Katsis & Bertino (réf. [31]) observent une augmentation de **15–25 % du temps de traitement** et une hausse de **18 % de la charge CPU**.

— **Problèmes de détection (faux positifs / faux négatifs).** Les systèmes automatiques ne sont pas parfaits : le modèle ZT-SDN (réf. [31]) présente encore **2 à 4 % de faux positifs**, ce qui peut entraîner la coupure de connexions légitimes (expérience utilisateur affecté) et des attaques qui n'ont pas été détecter.

— **IoT difficile à intégrer.** Les appareils IoT ont peu de ressources. Liu (réf. [12]) montre que la vérification continue dépasse souvent leurs capacités (CPU, mémoire, batterie), ce qui limite l'application du Zero Trust dans ces environnements.

— **Peu de plateformes reproductibles.** Les résultats publiés (réf. [12], [30], [31]) sont difficiles à reproduire, car les auteurs utilisent leurs propres environnements. Il manque des maquettes standard pour comparer les approches.

2.3.3 Conclusion

Cet état de l'art démontre que certaines solutions marchant à certains niveaux comme le SDN au niveau réseau. Le contexte enrichit les décisions d'accès : l'utilisation d'informations contextuelles (comportement réseau, posture de l'appareil, localisation, etc.) permet

des décisions d'autorisation plus précises et adaptatives. La révocation automatique est implémentable où les mécanismes de révocation automatique basés sur la détection d'anomalies, et les changements de score de risque ont pour la plupart été démontrés avec des temps de réponse de l'ordre de la seconde. L'apprentissage automatique est central pour l'analyse comportementale et la détection d'anomalies. Mais des défis subsistent comme la latence, la scalabilité, les faux positifs, la complexité opérationnelle, et l'intégration avec les systèmes existants restent des obstacles à l'adoption généralisée.

Glossaire et acronymes

Acronymes

5G — **Fifth Generation**
Réseau mobile de cinquième génération, offrant forte bande passante, faible latence et support massif d'appareils connectés.

AAA — **Authentication, Authorization and Accounting**
Ensemble des fonctions permettant d'authentifier une entité, contrôler ses droits et tracer ses actions.

ACL — **Access Control List**
Liste de règles utilisées pour autoriser ou bloquer du trafic selon des critères précis (adresse, port, protocole).

BYOD — **Bring Your Own Device**
Pratique permettant aux utilisateurs d'accéder aux ressources d'une organisation depuis un appareil personnel.

CSA — **Cloud Security Alliance**
Organisation promouvant les bonnes pratiques de sécurité dans le cloud, dont l'architecture SDP.

CSF — **Cybersecurity Framework**
Référentiel du NIST structurant la gestion des risques en cinq fonctions (Identify, Protect, Detect, Respond, Recover).

EDR — **Endpoint Detection and Response**
Solutions de sécurité destinées à détecter, analyser et répondre aux incidents sur les postes et serveurs.

IAM — **Identity and Access Management**
Ensemble des processus et technologies dédiés à la gestion des identités numériques et des autorisations.

IA — **Intelligence Artificielle**
Techniques d'apprentissage automatique utilisées pour analyser les comportements et automatiser certaines décisions de sécurité.

IdP **Identity Provider**
Service responsable de l'authentification et de la délivrance de preuves d'identité (tokens, assertions).

IoT **Internet of Things**
Ensemble des objets connectés communicants (capteurs, actionneurs, équipements embarqués).

MFA **Multi-Factor Authentication**
Authentification reposant sur plusieurs facteurs distincts (mot de passe, appareil, biométrie...).

NAC **Network Access Control**
Mécanismes contrôlant l'accès réseau en fonction de l'identité et de la posture des terminaux.

NIST **National Institute of Standards and Technology**
Organisme américain publiant des standards de cybersécurité, dont ceux relatifs au Zero Trust.

OT **Operational Technology**
Systèmes industriels spécialisés (SCADA, automates) aux contraintes différentes des environnements IT classiques.

PA **Policy Administrator**
Composant chargé d'appliquer les décisions d'accès prises par le Policy Engine.

PDP **Policy Decision Point**
Élément évaluant les politiques de sécurité et décidant d'autoriser ou non une requête.

PE **Policy Engine**
Composant central de la ZTA, chargé de déterminer les décisions d'accès en fonction du contexte et des politiques.

PEP **Policy Enforcement Point**
Point du réseau où les décisions du Policy Engine sont effectivement appliquées.

PIP **Policy Information Point**
Source fournissant les informations contextuelles nécessaires à l'évaluation des politiques.

PKI **Public Key Infrastructure**
Infrastructure gérant les certificats et clés cryptographiques pour authentifier utilisateurs et services.

SDN **Software-Defined Networking**
Modèle réseau séparant plan de contrôle et plan de données afin de rendre l'architecture programmable.

SDP **Software-Defined Perimeter**
Architecture rendant les ressources invisibles et accessibles seulement après authentification.

SIEM **Security Information and Event Management**
Solutions collectant et corrélant les journaux afin d'identifier les comportements suspects.

SSO **Single Sign-On**
Mécanisme permettant à un utilisateur de se connecter une fois pour accéder à plusieurs services.

TLS **Transport Layer Security**
Protocole cryptographique assurant la confidentialité et l'intégrité des communications.

VLAN **Virtual Local Area Network**
Mécanisme de segmentation logique d'un réseau au sein d'une même infrastructure physique.

ZT **Zero Trust**
Modèle de sécurité éliminant toute confiance implicite et reposant sur une vérification systématique.

ZTA **Zero Trust Architecture**
Architecture appliquant les principes Zero Trust à l'ensemble du système d'information.

ZTNA **Zero Trust Network Access**
Solutions d'accès réseau reposant sur l'identité et la posture plutôt que sur le périmètre.

Glossaire

Attaque par hameçonnage Technique d'ingénierie sociale visant à tromper un utilisateur pour lui soutirer des identifiants ou lui faire exécuter une action malveillante.

Confiance implicite Hypothèse selon laquelle un utilisateur ou un appareil présent dans le réseau interne serait automatiquement fiable — notion supprimée par le Zero Trust.

Contexte d'accès Ensemble d'attributs (identité, posture, localisation, horaire, comportement) utilisés pour déterminer si une requête est légitime.

Cybersecurity Framework (CSF) Référentiel du NIST pour structurer la gestion des risques cyber.

Gestion d'identité Processus visant à administrer les identités numériques et les droits associés dans un système d'information.

Jeton d'accès Preuve cryptographique temporaire permettant d'autoriser l'accès à une ressource.

Micro-segmentation Découpage fin du réseau en segments isolés afin de limiter les mouvements latéraux et réduire la surface d'attaque.

Mouvement latéral Déplacement d'un attaquant d'un système compromis vers d'autres cibles au sein du réseau.

Passerelle Zero Trust Élément appliquant les décisions d'accès (score, posture, jeton) et contrôlant le passage des flux réseau.

Plan de contrôle Partie logique du réseau qui prend les décisions d'acheminement et de politique.

Plan de données Partie du réseau qui transporte effectivement les paquets selon les règles du plan de contrôle.

Policy Administrator Composant chargé d'appliquer la décision du Policy Engine sur les éléments du système.

Policy Engine Élément central de la ZTA, responsable des décisions d'accès.

Posture de sécurité État global d'un appareil (mises à jour, configuration, vulnérabilités, conformité) utilisé pour autoriser ou non l'accès.

Surface d'attaque interne Ensemble des points exploitables à l'intérieur du réseau, souvent sous-estimés dans les modèles historiques.

Surveillance continue Observation permanente des activités et comportements pour détecter des anomalies et adapter les politiques.

Bibliographie

Consensus (références de base et points d'accord)

1. **Tao Chuan**, Yao Lv, Zhenfei Qi, Linjiang Xie, Wei Guo ; *An Implementation Method of Zero-trust Architecture* ; https://iopscience.iop.org/article/10.1088/1742-6596/1651/1/012010/meta
2. **NIST** (Alper Kerman, Murugiah Souppaya, Karen Scarfone, Susane Symington, William Barker) ; *Implementing a Zero Trust Architecture* ; https://www.nccoe.nist.gov/sites/default/files/2022-12/zta-nist-sp-1800-35e-preliminary-draft.pdf
3. **NIST** ; *Zero Trust Architecture (SP 800-207)* ; https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
4. **ANSSI** (Agence nationale de la sécurité des systèmes d'information) ; *Les essentiels de l'ANSSI – Zero Trust* ; https://cyber.gouv.fr/publications/zero-trust
5. **ANSSI** (Agence nationale de la sécurité des systèmes d'information) ; *Modèle Zero Trust – Avis scientifique et technique* ; https://cyber.gouv.fr/publications/zero-trust
6. **Azad, M.** *et al.* ; *Verify and Trust : A Multidimensional Survey of Zero-Trust* ; https://www.sciencedirect.com/science/article/pii/S2542660524001689
7. **Gilman, E.** ; **Barth, D.** ; *Zero Trust Networks : Building Secure Systems in Untrusted Networks* ; https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/
8. **Dhiman, P.**, Neha Saini, Yonis Gulzar, Sherzod Turaev, Amandeep Kaur, Khair Ul Nisa, Yasir Hamid ; *A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model* ; https://www.mdpi.com/1424-8220/24/4/1328
9. **Sarkar, S.**, Gaurav Choudhary, Shishir Kumar Shandilya, Azath Hussain, Hwankuk Kim ; *Security of Zero Trust Networks in Cloud Computing : A Comparative Review* ; https://www.mdpi.com/2071-1050/14/18/11213
10. **Cloud Security Alliance** ; *Software Defined Perimeter and Zero Trust* ; https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-z

ero-trust

11. **Google** (Ward, C. ; Osborn, J.) ; *BeyondCorp : A New Approach to Enterprise Security* ; /mnt/data/login_dec14_02_ward.pdf, /mnt/data/login_spring16_06_osborn.pdf

12. **OpenID Foundation** ; *Shared Signals Framework (SSF) and Continuous Access Evaluation Profile (CAEP)* ; https://openid.net/specs/

13. **Microsoft Corporation** ; *Continuous Access Evaluation (CAE) in Entra ID – Technical Overview* ; https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation

14. **Google** ; *Risk and Incident Sharing and Coordination (RISC) – Cross-Account Protection* ; https://developers.google.com/identity/risc

15. **Kumar S., S., Bokka, R., Priyanka R. (2025)** ; *Adaptive Access Control and Threat Mitigation in SDN-Based Data Centers for BYOD Environments.* ; https://ijits.org/wp-content/uploads/2025/09/5.BYOD-IJITS-format.pdf

16. **Ashfaq, F. ; Wasim, M. ; Shah, M.A. ; Ahad, A. ; Pires, I.M.** ;*Enhancing Security in 5G Edge Networks : Predicting Real-Time Zero Trust Attacks Using Machine Learning in SDN Environments* ; https://www.mdpi.com/1424-8220/25/6/1905

17. **Shaghaghi, A., Kanhere, S. S., Kaafar, M. A., et al. (2018).** ; *Gargoyle : A Network-based Insider Attack Resilient Framework for Organizations* ;

18. **Kapoor, V., Varma, S.** *Dynamic Trust Evaluation Models for Enforcing Zero Trust Security in Software-Defined Networks. MIRA Journal of Research and Development.* ;https://openviewjournal.com/index.php/mira/article/view/21

Divergences (visions alternatives et débats)

19. **Hireche, O.**, Benzaïd, C., Taleb, T. ; *Deep data plane programming and AI for zero-trust self-driven networking in beyond 5G* ; https://www.sciencedirect.com/science/article/pii/S1389128621005442

20. **Jeong, E. ; Yang** ; *A Trust Score-Based Access Control Model for Zero Trust Architecture : Design, Sensitivity Analysis, and Real-World Performance Evaluation* ; https://www.mdpi.com/2076-3417/15/17/9551

21. **Buck, C.** *et al.* ; *Never trust, always verify : A multivocal literature review on Zero Trust* ; https://www.sciencedirect.com/science/article/abs/pii/S0167404821002601

Lacunes (manques identifiés et perspectives)

22. **Rodigari, S.**, O'Shea, D., McCarthy, P., McCarry, M., McSweeney, S. ; *Performance Analysis of Zero-Trust Multi-Cloud* ; https://arxiv.org/abs/2105.02334

23. **Liu, C.**, Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y. ; *Dissecting zero trust : research landscape and its implementation in IoT* ; https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00212-0

24. **Ahmadi, S.** ; *Zero Trust Architecture in Cloud Networks : Application, Challenges and Future Opportunities* ; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4725283

25. **Yeoh, W.** *et al.* ; *Zero trust cybersecurity : Critical success factors and analysis* ; https://www.sciencedirect.com/science/article/pii/S016740482300322X

26. **Alshamrani, A.** *et al.* ; *Zero Trust : Applications, Challenges, and Opportunities* ; https://arxiv.org/pdf/2309.03582

27. **Oladimeji, G.** ; *A Critical Analysis of Foundations, Challenges and Directions for Zero Trust Security in Cloud Environments* ; https://arxiv.org/abs/2411.06139

28. **Mangla, M** ; *AI-Driven Zero Trust Architecture : A Scalable Framework for Threat Detection and Adaptive Access Control. International Journal of Science and Technology,* ; https://scholar9.com/publication/128-135_Mukul+mangla_1759814713.pdf

29. **Tobias Hilbig, Vitali Serzantov, Thomas Schreck** ; *Continuous Access Evaluation* ; https://seclab.cs.hm.edu/assets/pdf/th-cae-2023.pdf

30. **Alnaim, A. K. (2025).** ; *Adaptive Zero Trust Policy Management Framework in 5G Networks.* ; https://www.mdpi.com/2227-7390/13/9/1501

31. **Charalampos Katsis, Elisa Bertino** ; *ZT-SDN : An ML-powered Zero-Trust Architecture for Software-Defined Networks. (2024).* ; https://dl.acm.org/doi/full/10.1145/3712262