RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

MODÈLE ZERO TRUST

LES FONDAMENTAUX

ANSSI-PA-111
20/06/2025

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI s'intitule **« Modèle *Zero Trust* »**. Il est téléchargeable sur le site `cyber.gouv.fr`.

Sauf disposition réglementaire contraire, les recommandations n'ont pas de caractère normatif ; elles sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	20/06/2025	Version initiale

Table des matières

1
Préambule

Avec l'accroissement des usages liés au télétravail, à la pratique du « *Bring Your Own Device* » (BYOD [1]) et aux accès hétérogènes à des services *on-premise* ou dans le *cloud*, les produits dérivés du modèle *Zero Trust* sont promus par les éditeurs. Le principal objectif de ce modèle est de réduire la confiance implicite accordée à un sujet souhaitant accéder au système d'information (SI). Le contrôle d'accès logique repose alors sur :

- une évaluation dynamique et régulière du sujet cherchant à accéder à une ressource ;
- une évaluation dynamique et régulière du contexte d'accès d'un sujet incluant notamment l'état de sécurité du poste utilisé pour réaliser ces accès ;
- la criticité en termes de disponibilité, d'intégrité et de confidentialité de la ressource accédée.

Les produits dits *Zero Trust* sont vus comme des solutions permettant de pallier certaines limitations des mesures traditionnelles telles que la protection des flux par VPN ou le filtrage réseau par des pares-feux périmétriques. Bien souvent, les modèles *Zero Trust* et de défense périmétrique sont opposés alors qu'ils sont complémentaires et partagent de nombreux principes communs. Ainsi le modèle *Zero Trust* doit être inclus dans une stratégie de défense en profondeur et il ne doit en aucun cas être vu comme un remplacement d'une défense périmétrique.

En effet, l'idée d'une rupture entre les modèles *Zero Trust* et de défense périmétrique pourrait mener à une dégradation du niveau de sécurité global des entités. Le déploiement de produits dits *Zero Trust* n'est pas sans risque et doit impérativement être intégré dans une démarche globale de maîtrise des risques. En particulier, les politiques de contrôle d'accès dans le contexte du *Zero Trust* sont complexes à définir et à mettre en œuvre. Cela peut mener à un faux sentiment de sécurité en cas d'accès illégitime autorisé à tort, ou se révéler un frein à l'opération en cas d'accès légitime non autorisé à tort. Toutefois, si ce modèle est bien implémenté et sa configuration maintenue à jour dans le temps, celui-ci pourrait permettre à une entité d'avoir une posture de sécurité plus proactive face aux menaces.

Ce document a pour objectif d'apporter un éclairage, complémentaire à l'avis scientifique et technique de l'ANSSI publié en 2020 [1], sur le modèle *Zero Trust* et sur la manière dont il peut être mis en œuvre progressivement dans le cadre d'une stratégie de défense en profondeur. Ce document traite uniquement des principes généraux et des principales recommandations en la matière, et ne se veut ni exhaustif ni détaillé sur les cas d'usage. Il ne présente pas de stratégie de migration, dont une approche est, par exemple, proposée dans un document de la CISA [12].

1. Terme français équivalent : AVEC – Apportez votre équipement personnel de communication.

2
Principes généraux

2.1 Glossaire

***Application Programming Interface* (API)** Interface logique de communication d'un logiciel permettant l'utilisation d'un ensemble de ses fonctionnalités par d'autres logiciels.

Assurance sécurité Ensemble d'activités permettant d'assurer la pertinence et l'efficacité des mesures de sécurité mises en œuvre pour couvrir les objectifs de sécurité d'un système, produit, service, ou d'une organisation. Ces activités incluent notamment la démonstration du bon fonctionnement des mesures de sécurité et de leurs robustesses face à des tentatives de contournements accidentelle ou intentionnelle.

***Attribute-Based Access Control* (ABAC)** Mécanisme de contrôle d'accès reposant sur des attributs associés au sujet demandant un accès, à la ressource devant être accédée et au contexte de la demande d'accès du sujet (heure, lieu, équipement utilisé, etc.).

***Endpoint Detection and Response* (EDR)** Solution de collecte et d'analyse d'évènements de sécurité ayant pour but de détecter des menaces au niveau d'un équipement et de répondre de manière automatique à certaines alertes de sécurité.

Niveau de confiance explicite (score de confiance) Estimation du niveau d'intégrité d'un utilisateur, composant matériel ou logiciel en opération. Cette estimation repose sur une évaluation continue et dynamique (i) du niveau de conformité à la politique de sécurité de l'entité et (ii) du niveau de menace (active ou passée) du sujet et de l'appareil utilisé pour accéder aux ressources. Ce score ne peut pas être supérieur au niveau de confiance implicite accordé aux fonctions et aux sources de données utilisées pour évaluer ce score.

Niveau de confiance implicite Estimation du niveau d'intégrité attendu d'un utilisateur, composant matériel ou logiciel. Cette estimation prend en compte l'ensemble des mesures de la politique de sécurité d'une entité mise en oeuvre et est déterminée indépendamment de toute évaluation du contexte à un instant donné. Dans le modèle théorique du *Zero Trust*, le niveau de confiance implicite est considéré comme nul.

Niveau de criticité Estimation, pour une ressource, de ses impacts métier au niveau de l'entité en cas d'atteinte à ses besoins de sécurité en disponibilité (D), intégrité (I) et confidentialité (C). Un niveau de criticité est défini par critère de sécurité DIC.

Niveau de menace explicite Estimation de la présence potentielle ou avérée d'une menace active pouvant impacter les besoins en disponibilité, intégrité et confidentialité de l'entité.

Niveau de risque Estimation du risque, au niveau de l'entité, se basant sur le niveau de confiance explicite de l'utilisateur et de l'équipement utilisé (vraisemblance), ainsi que sur le niveau de criticité DIC de la ressource accédée (impact).

Plan de contrôle Ensemble des composants, qui dans le cadre du modèle *Zero Trust*, permettent la supervision, la prise des décisions de contrôle d'accès, ainsi que la configuration des conditions d'accès dans le plan de données.

Plan de données Ensemble des composants hébergeant les fonctions métier et permettant les échanges des données métier selon les conditions d'accès définies par le plan de contrôle.

Ressource Entité passive contenant ou recevant des informations et sur lequel un ou des sujets réalisent des opérations (p. ex. un équipement, un processus automatique, un fichier de données). Une ressource peut être physique ou virtuelle.

***Role-Based Access Control* (RBAC)** Mécanisme de contrôle d'accès reposant sur le ou les rôles associés à un sujet. Un rôle représente un ensemble de permissions accordées à un sujet.

***Security Information Event Management* (SIEM)** Solution de collecte et d'analyse d'évènements de sécurité à partir de multiples sources au sein d'un ou plusieurs systèmes d'une entité pour la détection des menaces.

Session Temps d'exploitation d'un canal reliant un sujet à une ressource et sur lequel circule les actions du sujet. À l'établissement d'une session authentifiée, l'authentification du sujet permet de relier de façon fiable les actions circulant sur ce canal à l'identité du sujet, et d'en assurer un suivi des états.

Sujet Utilisateur, processus automatique ou équipement actif réalisant des opérations sur une ressource.

2.2 Objectif du modèle Zero Trust

L'objectif principal du modèle *Zero Trust* est de réduire la confiance implicite accordée à un sujet souhaitant accéder au système d'information.

Pour réduire cette confiance implicite, les contrôles doivent être granulaires, dynamiques et réguliers [10] :

- l'accès aux ressources doit être accordé sur la base du besoin d'en connaître ;
- l'accès doit être donné sur la base du plus faible niveau de privilège nécessaire pour réaliser la tâche ;
- les demandes d'accès doivent être contrôlées avec la même attention quelles que soient leurs origines (provenant de l'« intérieur » ou de l'« extérieur » de l'entité) ;
- la politique d'accès aux ressources doit inclure des attributs dynamiques s'adaptant aux comportements du sujet et à son contexte d'accès (analyse comportementale de l'utilisateur, horaires d'accès, localisation géographique, etc.) ;
- les conditions d'accès aux ressources doivent faire l'objet de réévaluations régulières.

2.3 Architecture fonctionnelle de contrôle d'accès Zero Trust

Cette section a pour objectif de décrire de manière générale l'architecture fonctionnelle des mécanismes de contrôle d'accès *Zero Trust* et des différentes interactions d'un sujet avec les composants de l'architecture afin d'accéder à une ressource. Les contraintes à prendre en compte afin d'assurer l'efficacité de ces contrôles d'accès sont ensuite présentées. Finalement, une description des différents composants d'architecture est fournie.

2.3.1 Principes du contrôle d'accès

L'architecture fonctionnelle du contrôle d'accès *Zero Trust*, illustrée par la figure 1, repose sur l'implémentation du modèle *Attribute-Based Access Control* [9] (ABAC). Pour rappel, ce modèle permet la définition de politiques de contrôle d'accès granulaire en s'appuyant sur des attributs portant sur :

- le sujet, avec par exemple son niveau d'habilitation, son rôle dans l'entité, etc. ;
- la ressource, avec par exemple son niveau de classification, son propriétaire, etc. ;
- le contexte de la demande d'accès, avec par exemple l'heure, le lieu, l'état des mises à jour du moyen d'accès utilisé, etc.

Lors d'une demande d'accès, un système de contrôle d'accès de type ABAC évalue les attributs et actions associés à la demande par rapport aux règles de contrôle d'accès définies par l'entité.

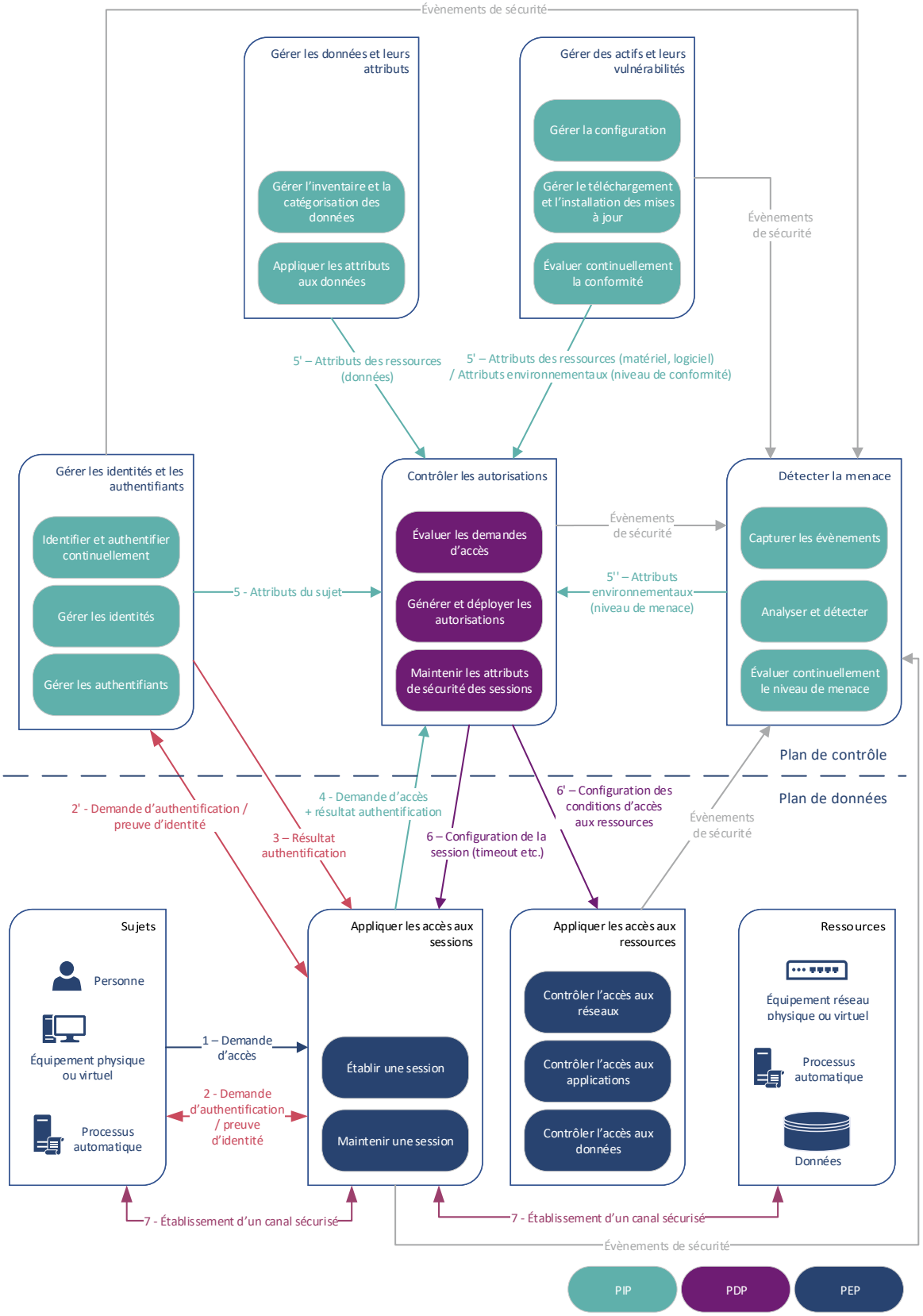

FIGURE 1 – Architecture fonctionnelle du modèle *Zero Trust* pour le contrôle d'accès

Les fonctions définies dans la figure 1 sont regroupées, comme illustré dans la figure 2 du document [10], selon les blocs fonctionnels suivants :

- *Policy Decision Point* (PDP) : ensemble des fonctions permettant l'évaluation et les décisions d'accès, ainsi que la définition des conditions d'accès à appliquer entre le sujet et la ressource.
- *Policy Information Point* (PIP) : ensemble des attributs utilisés par le PDP afin d'évaluer une demande d'accès. Cela inclut notamment les attributs du sujet, de la ressource et le contexte de la demande d'accès.
- *Policy Enforcement Point* (PEP) : ensemble des fonctions permettant la transmission des demandes d'accès au PDP et l'application des conditions d'accès retournées par celui-ci afin de permettre la communication entre un sujet et une ressource.

Ces fonctions sont généralement réparties de la manière suivante :

- Les fonctions du plan de données permettent l'établissement de la session de données et les échanges d'actions entre le sujet et la ressource selon les conditions d'accès définies par les fonctions du plan de contrôle.
- Les fonctions du plan de contrôle permettent de définir les conditions d'accès à appliquer par le plan de données. Ces fonctions incluent l'acquisition des attributs associés aux demandes d'accès, l'évaluation des demandes d'accès et la génération des conditions d'accès.

Information

La figure 1 est une représentation **fonctionnelle** des mécanismes de contrôle d'accès selon le modèle *Zero Trust*. La répartition des fonctions sur les composants d'une architecture technique est dépendante des solutions des éditeurs et des choix d'architecture de l'entité. À titre d'exemple, la fonction de détection de la menace peut être répartie sur différents composants d'une architecture technique avec une analyse et une détection d'évènements locales aux équipements (via un agent logiciel de type *Endpoint Detection and Response* - EDR) et/ou centralisées (via un ou plusieurs serveurs centraux hébergeant une solution logicielle de type *Security Information and Event Management* (SIEM).

Lors d'une demande d'accès d'un sujet à une ressource, les principales étapes du contrôle d'accès sont les suivantes :

- **Établissement d'une session entre un sujet et une ressource**
  - À la demande d'accès initiale, une authentification est demandée et le sujet prouve son identité (cf. 1 à 3 de la figure 1).
  - La demande d'accès à la ressource est évaluée selon les attributs associés au sujet, à la ressource et au contexte de la demande (cf. 4 à 5 de la figure 1). Plus particulièrement, les attributs de contexte permettent :
    - de définir l'heure et le lieu géographique associés à la demande d'accès ;
    - d'identifier l'équipement utilisé lors de la demande d'accès et d'estimer son niveau de conformité à la politique de sécurité de l'entité ;
    - d'estimer le niveau de menace associée à l'utilisateur et/ou de l'équipement utilisé (par analyse comportementale, analyse par signature, etc.).

- Selon l'évaluation, soit les conditions d'accès sont générées et fournies pour application lors de l'établissement de la session (cf. 6 à 7 de la figure 1), soit l'ouverture de session est refusée.

- **Contrôle des actions au sein d'une session authentifiée**
  - Les actions du sujet sur la ressource, au sein d'une session authentifiée, sont contrôlées soit dynamiquement par action conformément aux principes *Zero Trust*, soit en transmettant les conditions d'accès à la ressource et en accordant au sujet une confiance implicite, limitée dans le temps. Par exemple, les conditions d'accès transmises peuvent inclure le groupe ou rôle d'appartenance du sujet (*Discretionary Access Control* - DAC , *Role-Based Access Control* - RBAC , etc.) afin d'en déterminer les permissions sur la ressource.

- **Maintien d'une session**
  - Une réauthentification périodique du sujet est demandée.
  - Une évaluation continue des attributs du sujet, de la ressource, et du contexte de la session est réalisée.
  - Selon l'évaluation, la session peut être soit maintenue, soit mise à jour (par exemple avec une mise à jour du rôle associé au sujet), soit fermée.

Exemple

Alice (le sujet) tente d'accéder à une application de partage de fichiers (la ressource).

- Une authentification multifacteur est demandée à Alice et celle-ci prouve son identité.
- Le moteur de décision évalue les attributs d'Alice (par exemple son rôle dans l'entreprise, la méthode d'authentification utilisée etc.), les attributs associés à la solution de partage de fichiers (par exemple son niveau de sensibilité) et le contexte de la demande (par exemple la demande est réalisée en heure ouvrée à partir du poste bureautique d'Alice, qui est à jour des correctifs).
- La demande est conforme aux règles définies dans le moteur de décision et l'accès à l'application est autorisé avec des conditions d'accès incluant le rôle d'Alice (dans une approche mixte ABAC/RBAC).
- Alice dispose d'une session sur l'application et accède aux différents fichiers selon les permissions qui lui ont été octroyées via son rôle.
- Le comportement d'Alice est évalué de manière continue ainsi que toute autre information de contexte pertinente pour les prises de décisions d'accès.
- A plusieurs reprises, Alice cherche à accéder à des fichiers pour lesquels elles ne disposent pas des droits nécessaires. Le niveau de confiance d'Alice est réduit et déclenche une perte de ses droits d'accès à l'application.
- La session d'Alice est fermée et toutes ses nouvelles demandes d'accès sont rejetées.

2.3.2 Contraintes de sécurité relatives aux attributs

Le niveau de sécurité offert par un mécanisme de contrôle d'accès de type ABAC est dépendant des attributs utilisés et de leur gestion dans le temps. Les principaux critères liés aux besoins de disponibilité et d'intégrité de ses attributs [2] sont définis ci-après.

- **Pertinence des attributs** : il s'agit de définir les attributs pertinents par rapport à la politique de sécurité de l'entité et les cas d'usage pour lesquels ceux-ci apportent un gain de sécurité. Cela comprend les attributs du sujet, de la ressource et de l'environnement, incluant les éléments de conformité et de niveau de menace. Par exemple, pour un système classifié au sens de l'IGI 1300 [8], le niveau d'habilitation du sujet et le niveau de classification de la ressource sont, dans ce cas, des attributs pertinents pour le contrôle d'accès.
- **Mise à jour des sources de données des attributs** : la mise à jour des sources de données utilisées pour le calcul d'attributs dynamiques est nécessaire pour éviter par exemple des refus d'accès. Il s'agit ici de maintenir l'état réel du système par rapport à son état attendu. Cela nécessite la mise en œuvre de nombreux processus organisationnels ainsi que d'outils d'automatisation afin de maintenir ces données dans le temps. Par exemple, un attribut représentant l'état de mise à jour des correctifs de sécurité d'un équipement nécessite la mise en oeuvre de moyens techniques et organisationnels permettant le téléchargement et l'installation de ces correctifs conformément à la base de référence des correctifs qui lui sont applicables.
- **Niveau de fraîcheur des attributs** : ce critère correspond au niveau de représentativité d'un attribut selon la date de sa dernière mise à jour et par rapport à ses sources de données ou sa valeur en cache. La fréquence de calcul ou de mise à jour en cache de certains attributs peut avoir un impact direct sur le niveau de sécurité avec des accès autorisés à tort. Par exemple, une identité peut avoir été compromise depuis la dernière consultation de l'attribut, mais ce nouvel état ne sera pas pris en compte tant qu'il ne sera pas actualisé dans la valeur en cache du moteur de contrôle d'accès.
- **Fiabilité de calcul d'un attribut** : la fiabilité de calcul d'un attribut correspond ici au niveau de robustesse et de justesse des algorithmes de calcul utilisés pour dériver la valeur associée à un attribut. Il s'agit ici de s'assurer que ces résultats de calcul sont cohérents et répétables malgré des données d'entrée légèrement erronées, et que ceux-ci sont corrects par rapport aux résultats attendus. Par exemple, le ou les attributs pour l'évaluation du niveau de confiance aux travers de mécanismes de détection de la menace et l'utilisation de *machine learning* ne sont pas triviaux à calculer et nécessitent un effort d'intégration conséquent avant d'obtenir des valeurs fiables. Un attribut dont la valeur est peu fiable pourrait mener à des accès ou des refus d'accès à tort.
- **Disponibilité d'accès d'un attribut** : ce critère correspond à l'accessibilité des attributs lors des prises de décision d'accès, notamment lorsque ceux-ci ne sont pas directement fournis par le sujet et/ou la ressource. La non disponibilité de ces attributs ou des temps de réponses élevés pour y accéder peuvent mener à des refus d'accès, et donc à un déni de service.
- **Authenticité d'un attribut** : ce critère est important pour s'assurer, lors d'une décision d'accès, que les attributs proviennent d'une source de confiance. Une perte en intégrité et en authenticité des attributs pourrait mener à des accès à tort, et donc à un faux sentiment de sécurité.

2. La confidentialité n'est pas prise en compte dans le présent document puisque ce critère n'a pas d'impact sur le niveau d'efficacité du mécanisme de contrôle d'accès. Il est cependant important de noter que certains attributs, sur les sujets notamment, peuvent avoir des besoins forts en confidentialité.

2.3.3 Descriptions des fonctionnalités

2.3.3.1 Gérer les identités et les authentifiants

La gestion des identités et des authentifiants [3] couvre l'ensemble des mesures permettant à une entité de maîtriser les utilisateurs, les processus automatiques et les équipements cherchant à accéder à son système d'information. L'authenticité des attributs associés à un sujet, et donc la confiance qui peut leur être attribuée, est directement liée à la bonne maîtrise de cette thématique de sécurité. En particulier, il est nécessaire pour les entités (i) de gérer l'ensemble des sujets de l'entité interagissant avec son système, (ii) de déterminer le niveau de robustesse des mécanismes d'authentification permettant aux sujets de prouver leur identité et (iii) d'appliquer le principe de moindre privilège à ces accès. Les éléments suivants sont à prendre en compte :

- **Gérer les identités** : l'entité doit maintenir à jour un ou plusieurs référentiels centraux d'identités uniques [4] et des attributs de sécurité associés aux différents sujets de l'entité. Il est notamment nécessaire d'identifier de manière unique les utilisateurs, les processus automatiques et les équipements devant accéder au système. Les attributs d'un sujet ayant un impact direct sur le niveau de sécurité du mécanisme de contrôle d'accès, ceux-ci doivent être mis à jour régulièrement pour prendre en compte les changements de fonctions d'un utilisateur, la compromission d'un poste utilisateur, etc.
- **Assurer l'authentification des sujets** : l'authenticité des attributs du sujet utilisés lors de la décision d'accès est liée au niveau de robustesse de sa preuve d'identité. Les éléments à prendre en compte selon le niveau de criticité de la ressource accédée sont les suivants :
  - Gestion des authentifiants : la robustesse d'un authentifiant dépend de son type, de son niveau de protection (au repos ou en transit), de son niveau d'entropie, de son niveau de dissémination au sein du système et de sa durée de vie. Il s'agit ici d'être en capacité de dimensionner ce secret d'authentification selon les cas d'usage et d'en assurer la protection et le renouvellement sur l'ensemble de son cycle de vie.
  - Fonction d'authentification : les différents mécanismes d'authentification n'offrent pas le même niveau de robustesse face aux menaces de compromission des authentifiants (ex. : hameçonnage) ou contre le rejeu. Par exemple, l'utilisation d'un mécanisme d'authentification multifacteur forte (cf. [7]) peut permettre de faire face à ces menaces.
  - Authentification continue : les éléments précédents se focalisent sur le niveau de robustesse de la preuve d'identité lors de l'établissement d'une session. Une session pouvant cependant être usurpée (ex. : vol de *cookies* de session), le niveau de confiance initialement accordée à une authentification se dégrade dans le temps. Une authentification périodique devient ainsi nécessaire pour maintenir ce niveau de confiance et limiter les impacts en cas d'usurpation de session, par exemple.

3. Un authentifiant correspond à un secret d'authentification.
4. Ces référentiels alimentent le ou les services d'annuaire de comptes utilisés par les utilisateurs, les processus automatiques et les équipements d'un système.

Attention

Une vigilance particulière doit être accordée aux contraintes exportées vers les utilisateurs lors de la mise en œuvre d'une authentification continue. Afin d'assurer son acceptabilité par les utilisateurs, des mécanismes d'authentification passive [5] pourraient être envisagés. Ces mécanismes, cependant, ne répondent pas aux bonnes pratiques définies par l'ANSSI [7].

La majeure partie des mesures décrites ici n'est pas spécifique au modèle du *Zero Trust* et représente déjà une thématique importante et complexe à gérer dans une stratégie de défense en profondeur. Il s'agit cependant d'un prérequis qui, dans les hypothèses du *Zero Trust*, nécessite la mise en œuvre de mesures renforcées et à l'état de l'art (compte unique, généralisation de l'authentification forte et de l'authentification multi-facteur, etc.).

2.3.3.2 Gérer les données et leurs attributs

L'identification et la catégorisation des données à protéger ainsi que les attributs de sécurité à appliquer à ces données sont des prérequis essentiels. Comme pour n'importe quel modèle d'accès (ABAC, *Mandatory Access Control* - MAC, etc.), la politique d'accès définie par l'entité ne peut être appliquée qu'aux seules ressources identifiées et sur lesquelles les attributs sélectionnés sont appliqués. La gestion des matériels et des logiciels étant traitée dans la section 2.3.3.3, les éléments suivants se concentrent sur les données.

- **Inventorier et catégoriser les données** : l'entité doit inventorier et catégoriser l'ensemble des données à protéger. Cet inventaire doit permettre d'identifier les données existantes ainsi que leur localisation dans le système. Toute donnée identifiée doit être ensuite catégorisée, en particulier selon sa valeur pour l'entité et/ou les contraintes réglementaires qui leur sont applicables. Cette catégorisation est essentielle afin d'adapter les mécanismes de contrôle d'accès à la sensibilité de ces données.
- **Labéliser les données (application des attributs)** : selon la catégorisation de la donnée, les attributs pertinents pour les besoins de contrôle d'accès doivent être appliqués à l'ensemble des données existantes ainsi qu'à toute donnée nouvellement créée. Cette labélisation pourra être réalisée par l'ajout de métadonnées protégées par l'utilisation de mécanismes crytographiques assurant l'intégrité et l'authenticité des attributs.

Les éléments listés ci-dessus devraient déjà s'inscrire dans une démarche de protection des données des entités. Il est important de noter que la mise en œuvre du modèle *Zero Trust*, et plus particulièrement du modèle ABAC, implique la définition et l'application de nouveaux attributs (p. ex. un attribut définissant le niveau de criticité de la donnée en termes d'intégrité ou de confidentialité) sur les données existantes. De par la volumétrie et les localisations parfois multiples des données, leur identification et leur labélisation peuvent donc être un prérequis complexe à satisfaire dans la mise en œuvre du modèle *Zero Trust*.

5. Une authentification est dite passive lorsqu'elle ne nécessite pas une action de l'utilisateur (par exemple l'usage d'un facteur biométrique pour l'authentification comme la reconnaissance faciale).

2.3.3.3 Gérer les actifs et leurs vulnérabilités

La gestion des actifs et de leurs vulnérabilités permet d'assurer la maîtrise des composants matériels et logiciels en production et leur niveau de conformité par rapport à la politique de sécurité de l'entité. Cette fonction permet d'évaluer le niveau de conformité d'un équipement lors d'une demande d'accès et de maintenir ce niveau de conformité dans le temps. Il s'agit donc pour une entité d'être en capacité (i) d'établir l'état attendu de son système et de ses composants, (ii) d'identifier les faiblesses des composants en production et (iii) de mettre en place un processus de gestion des changements. Afin d'atteindre cet objectif et de gérer les attributs de conformité dans le temps, les principales mesures suivantes sont nécessaires :

- **Établir l'état attendu du système et de ses composants**
  - Gérer les versions de référence : afin d'établir un état attendu du système et de ses composants, une gestion de configuration doit être mise en œuvre, permettant de définir les versions de référence applicables sur le système en production. Un inventaire de l'ensemble des actifs (systèmes, sous-systèmes, équipements, logiciels et matériels), de leur criticité DIC, ainsi que de leurs relations et dépendances nécessaires à leur bon fonctionnement doit être établi. Ces versions de référence portent notamment sur le paramétrage sécurisé des différents composants logiciels (ex. : les *Group Policy Object* - GPO Windows applicables) et matériels (ex. : la configuration des paramètres du *firmware* associé à la carte CPU).
- **Identifier les écarts entre les composants en production et la configuration attendue**
  - Gérer l'inventaire : pour des objets de configuration versionnés par l'éditeur ou par l'entité, un inventaire périodique des composants déployés en production doit être réalisé et comparé aux versions attendues (ex. : les correctifs de sécurité installés comparés aux correctifs de sécurité validés et à installer). Pour rappel, un inventaire n'offre aucune garantie d'intégrité en cas de modifications malveillantes mais permet à une entité de s'assurer du respect de sa politique de sécurité sur les objets de configuration versionnés.
  - Identifier les vulnérabilités connues : des scans de vulnérabilités devraient être réalisés afin d'identifier des faiblesses au niveau du paramétrage (ex. : utilisation de mécanismes cryptographiques non robustes, pare-feu désactivé) et au niveau des logiciels (ex. : CVE pour les vulnérabilités connues) sur les équipements maîtrisés par l'entité ou sur les équipements personnels (si ceux-ci sont autorisés par l'entité).
  - Vérifier l'intégrité et l'authenticité des logiciels : afin d'identifier des modifications non autorisées d'objets de configuration, un contrôle d'intégrité et d'authenticité pourrait aussi être utilisé. Ces contrôles peuvent par exemple s'appuyer sur des mécanismes de type *measured boot* et/ou des mécanismes de type liste d'applications autorisées (avec contrôle d'un condensat cryptographique ou de signature cryptographique).
- **Gérer les changements**
  - Définir les choix de traitement et les priorités : l'évolution des versions de référence doit obligatoirement passer par un processus de gestion des changements. Chaque faiblesse doit être qualifiée selon son niveau de criticité DIC, et un choix de traitement doit lui être appliqué. Les évolutions d'un référentiel applicable et les tests de non régression associés doivent être réalisés au regard du risque couvert et des coûts induits.
  - Déployer et installer les mises à jour et correctifs de sécurité : le maintien à jour d'un référentiel de configuration en exploitation par rapport à un référentiel de configuration attendue

devrait être automatisé. Cela est d'autant plus important que des équipements dont le niveau de conformité est faible se verront refuser l'accès au système. Afin de limiter les impacts sur la production, il est nécessaire de pouvoir mettre à jour un équipement de manière automatique et d'évaluer à nouveau son niveau de conformité afin que l'accès lui soit autorisé.

L'ensemble des mesures présentées dans cette section, comme dans la précédente, s'inscrit dans une stratégie de défense en profondeur. Les mécanismes de contrôle de posture de sécurité avant d'autoriser l'accès à un système existent, par exemple dans des solutions de type *Network Access Controller* (NAC). Le modèle *Zero Trust* vise principalement à utiliser ces mécanismes dans des cas d'usage plus étendus, et non plus uniquement pour des contrôles lors de l'accès initial au réseau de l'entité. Les attributs dits de conformité peuvent couvrir un large périmètre allant de la simple comparaison de numéro de version à un contrôle d'intégrité et d'authenticité des actifs. Une bonne maturité de l'entité est donc nécessaire pour la définition des attributs de conformité pertinents à prendre en compte et de leur qualité (une simple comparaison de numéro de version n'offre par exemple aucune assurance sur l'intégrité et l'authenticité de l'actif).

2.3.3.4 Détecter la menace

La détection de la menace joue un rôle central dans le modèle *Zero Trust*, et plus particulièrement dans l'évaluation du niveau de confiance accordée à un sujet lors d'une demande d'accès. L'objectif principal est de détecter au plus tôt toute compromission d'un compte d'accès, d'un moyen d'accès (par exemple un poste utilisateur) ou d'une ressource accédée afin d'en limiter les impacts sur le système, en réduisant ou révoquant les droits d'accès associés. Pour la mise en œuvre de ce type d'attribut, il est nécessaire de (i) identifier les scénarios de menaces à détecter [6], (ii) collecter les données nécessaires au besoin identifié, (iii) analyser ces données pour détecter les menaces et (iv) évaluer le niveau de menace du sujet et de l'équipement utilisé.

- **Identifier les scénarios de menaces à détecter :**
  - Identifier les évènements redoutés : l'entité doit d'abord définir ses objectifs de détection de sécurité, et donc les évènements redoutés sur lesquels elle souhaite être en capacité de réaliser des actions préventives ou correctives afin de les éviter ou d'en limiter les impacts sur son système. Ces objectifs correspondent à tout couple source de menace/événement redouté [3] que l'entité juge pertinent dans le contexte de son activité.
  - Identifier les composants à superviser : dans un deuxième temps, il est nécessaire d'identifier les composants du système à superviser et dont la compromission pourrait mener à la réalisation de l'évènement redouté. Cette activité nécessite l'identification des différents chemins d'attaque [7], pour chaque évènement redouté, pouvant être utilisés par la source de menace.
  - Identifier les techniques et actions d'un attaquant à superviser : finalement l'entité doit définir les évènements à superviser sur les différents composants précédemment identifiés. Ces évènements découlent de la définition des scénarios de menace et plus particulièrement des différentes techniques et actions utilisées par un attaquant afin d'atteindre ses objectifs. Avec l'évaluation de la vraisemblance des scénarios de menace, l'entité dispose des différents cas d'usage de détection adaptés à son contexte et associés à un niveau de risques permettant une gestion des priorités dans leur mise en œuvre.

6. Par exemple, la méthode EBIOS-RM [3] peut être utilisée pour identifier ces scénarios de menace.
7. Un chemin d'attaque se caractérise par la succession d'événements causés par la source de menace sur un ou plusieurs composants et menant à la réalisation de l'évènement redouté.

- **Générer et collecter les évènements de sécurité associés aux scénarios de menaces retenus** : les objectifs de détection et les différentes informations nécessaires pour couvrir chacun des cas d'usage identifiés étant définis, l'entité doit mettre en œuvre l'ensemble des capteurs nécessaires à leur supervision. Cette mise en œuvre est très souvent associée à des contraintes techniques liées par exemple au chiffrement des flux réseau limitant leur visibilité, aux équipements industriels ou embarqués ne disposant pas de fonctionnalité de génération d'évènements ou n'étant pas compatibles avec des capteurs logiciels du marché. La disponibilité de ces données peut donc être limitée (ou à l'inverse trop volumineuse et inutile à la détection) et impacter fortement l'efficacité de ces mécanismes de détection.
- **Analyser les évènements de sécurité pour la détection des menaces :**
  - Analyse par signature : cette approche repose sur la reconnaissance d'indicateurs de compromission ou sur la reconnaissance de techniques d'attaque connues [8]. Cette approche nécessite le maintien à jour d'un référentiel des différents indicateurs de compromission, ainsi que des techniques et actions attendus d'un acteur malveillant.
  - Analyse par anomalie : cette approche se focalise sur la reconnaissance de toute activité sortant d'un cadre d'utilisation considéré comme normal et défini par un modèle de référence. Ces modèles peuvent aller de la simple représentation d'un protocole de communication à la représentation beaucoup plus complexe du comportement d'un utilisateur, d'un processus automatique ou d'un équipement. L'analyse comportementale repose généralement sur des technologies de *machine learning* (ML) pour la création de ces modèles difficiles à caractériser.
- **Évaluer le niveau de menace** : le niveau de menace correspond à une estimation de la vraisemblance d'une compromission active d'un utilisateur ou d'un processus automatique ou d'un équipement. Cette évaluation peut s'appuyer sur une analyse par signature, une analyse par anomalie ou une combinaison des deux approches afin d'améliorer la fiabilité de l'évaluation. La réduction du niveau de faux positifs et de faux négatifs afin d'obtenir une juste évaluation est souvent un processus long et complexe.

Le sujet de la détection de la menace est un sujet complexe dans sa mise en œuvre et son maintien dans le temps. L'identification des besoins, et notamment l'identification des informations au regard des techniques et actions réalisées par des attaquants, est un sujet nécessitant un bon niveau d'expertise. Certains systèmes ou équipements ne disposent pas des prérequis nécessaires et les mécanismes d'analyse comportementale restent complexes à mettre au point. L'utilisation de la détection de la menace pour du contrôle d'accès dynamique n'est donc pas sans risques et pourrait mener soit à une dégradation des accès aux ressources de l'entité, soit à un faux sentiment de sécurité.

2.3.3.5 Contrôler les autorisations

Les éléments définis précédemment viennent alimenter la fonction de contrôle d'accès dynamique avec les attributs du sujet, de la ressource et du contexte des demandes d'accès. Ces différents éléments permettent d'évaluer les demandes d'accès pour l'établissement d'une session entre le sujet et la ressource, de générer et configurer les autorisations de manière dynamique, et de maintenir la

8. Des bases de connaissances comme par exemple le MITRE ATTACK (`https://attack.mitre.org/`) peuvent aider les entités.

session dans le temps par une évaluation continue des attributs du sujet et de l'équipement utilisé. La fonction de contrôle d'accès repose sur (i) la définition et l'évaluation des règles d'accès et (ii) l'application des décisions et des conditions d'accès.

- **Définir et évaluer les règles d'accès** : la définition des règles d'accès doit être réalisée selon le principe du moindre privilège. Ces règles sont composées d'une combinaison de critères à satisfaire afin d'autoriser un accès. Ces critères peuvent être de différents types.
  - Critère de conformité simple : cette approche consiste à une évaluation unitaire de la demande d'accès selon une combinaison d'attributs précis de conformité (rôle de l'utilisateur, lieu et horaire de connexion, etc.). Si les critères sont validés, la condition est satisfaite.
  - Critère sur la base d'un score de confiance simple : cette approche consiste en une évaluation des demandes d'accès en incluant des pondérations sur des attributs de conformité et/ou des attributs de détection de la menace simple (sur la base de signature par exemple) afin d'établir un score de confiance. Si le score de confiance est au-dessus d'une certaine valeur, la condition est satisfaite.
  - Critère sur la base d'un score de confiance complexe : cette approche consiste en une évaluation des demandes d'accès sur la base du comportement du sujet et/ou de l'équipement utilisé. Si le score de confiance est au-dessus d'une certaine valeur, la condition est satisfaite.
- **Appliquer les décisions et les conditions d'accès selon le principe du moindre privilège**
  - Contrôle des sessions : les décisions et les conditions d'accès sont déterminées lors de l'établissement d'une session et sont revues de manière périodique pour le maintien de la session. À l'établissement de la session, certains attributs de sécurité peuvent être configurés de manière dynamique afin de déterminer, par exemple, la durée de vie maximale de la session, le délai avant ré-authentification, etc. Selon l'évaluation continue d'un sujet et de l'équipement utilisé, ces conditions d'accès peuvent être mises à jour ou la session peut être fermée.
  - Contrôle des ressources : après l'établissement d'une session, les actions sur une ressource peuvent être contrôlées selon deux approches, en évaluant chaque action de manière dynamique dans une pure approche ABAC ou en accordant une confiance implicite limitée dans le temps, par exemple dans une approche mixte ABAC (session) et RBAC (ressource). Dans cette seconde approche, le rôle du sujet est fourni lors de l'établissement de la session dans les conditions d'accès à appliquer. Ces rôles à appliquer sur la ressource devraient être définis et mis à jour de manière dynamique selon l'évaluation de la posture de sécurité du sujet et de l'équipement utilisé (cf. point précédent sur le contrôle des sessions).

Comme présenté dans cette section, le modèle ABAC est la brique de base du modèle *Zero Trust* pour un contrôle granulaire, dynamique et régulier des accès. L'efficacité de cette fonction de sécurité est dépendante des attributs et des sources de données utilisés, dont la gestion nécessite de nombreux prérequis techniques et organisationnels. Ces prérequis peuvent être complexes à satisfaire, voire dans certains cas se révéler non réalisables sur certains systèmes.

2.4 Mécanismes de sécurité pour la mise en œuvre du modèle Zero Trust

L'objectif de cette section est de présenter les principaux mécanismes de sécurité utilisés en complément du modèle ABAC afin d'implémenter le modèle *Zero Trust*. Ces mécanismes sont regroupés en deux grandes catégories : les mécanismes visant à renforcer le niveau de confiance accordée aux sujets et aux équipements utilisés, et les mécanismes visant à protéger les ressources selon le principe du moindre privilège.

2.4.1 Niveau de confiance des sujets et des équipements utilisés

2.4.1.1 Assurance de l'identité

Les hypothèses sur l'environnement dans le modèle *Zero Trust* nécessitent l'utilisation de mécanismes conformes à l'état de l'art et d'un niveau de robustesse élevé face aux menaces de compromission des authentifiants (force brute, hameçonnage, etc.), de rejeu des authentifiants et de contournement des mécanismes d'authentification par l'usurpation de sessions. Cela implique donc l'utilisation de mécanismes d'authentification forte et une demande d'authentification périodique des sujets. Notamment, les mécanismes à considérer sont :

- **Authentification multifacteur forte des utilisateurs** : utilisation d'un second facteur pour les utilisateurs permettant l'utilisation du certificat qui leur est associé.
- **Authentification forte des processus automatiques et équipements** (cf. [7]) : utilisation d'un protocole d'authentification s'appuyant sur un mécanisme de type défi/réponse et reposant sur des moyens cryptographiques conformes au Référentiel Général de Sécurité (RGS) et ses annexes B1 [6], B2 [5] et B3 [4].
- **Stockage des authentifiants dans un environnement matériel dédié** : utilisation d'un composant matériel dédié (ex. : *Hardware security module* - HSM) pour stocker les authentifiants au repos ou protéger ceux stockés sur une mémoire de masse.
- ***Single-Sign On* (SSO)** : limitation du nombre d'authentifiants à saisir à chaque authentification, en permettant la fédération d'identité.

À titre d'exemple, les mécanismes comme le mTLS ou l'IPsec avec authentification mutuelle par certificat peuvent être utilisés pour l'établissement d'un canal sécurisé. Pour l'authentification multifacteur des utilisateurs, le standard FIDO2 peut être utilisé avec un jeton (*token*) matériel incluant le certificat et la clé privée d'authentification associée dont l'accès est protégé par un code PIN ou par un facteur biométrique.

2.4.1.2 Assurance du niveau d'intégrité de l'équipement

Au niveau de l'équipement, plusieurs mécanismes peuvent être utilisés pour améliorer le niveau de confiance qui lui est accordée. En effet, le niveau de confiance d'un équipement est dépendant

des mesures de sécurité qui lui sont associées. Un équipement personnel et un équipement géré par l'entité n'ont, par défaut, pas le même niveau de confiance. Ces mesures sont notamment :

- **Intégrité et authenticité de la chaîne de démarrage** : l'utilisation des mécanismes *Secure Boot UEFI* ou *Measured Boot* visent à contrôler l'intégrité de la chaîne de démarrage d'un système d'exploitation par des mécanismes cryptographiques. Le niveau de confiance global d'un équipement est directement dépendant de l'intégrité et du niveau de confiance de la chaîne de démarrage.
- **Intégrité et authenticité des applicatifs** : l'utilisation de mécanismes par liste d'autorisations permet de contrôler l'intégrité et l'authenticité des applications s'exécutant sur l'équipement. Ces contrôles peuvent être réalisés par des mécanismes cryptographiques lorsque l'application dispose d'une signature cryptographique, ou par l'établissement d'empreintes cryptographiques de référence de l'ensemble des applications autorisées.
- **Mise à jour centralisée** : l'utilisation de mécanismes de mises à jour centralisées facilite le maintien à jour des logiciels et permet d'appliquer les correctifs de sécurité, lorsque ceux-ci existent.
- **Paramétrage de sécurité** : la mise en œuvre d'un durcissement de la configuration permettant de réduire la surface d'attaque d'un équipement devrait pouvoir être mis à jour de manière dynamique au travers d'une API afin d'appliquer les conditions d'accès requis par la fonction de contrôle d'accès.
- **Protection contre les codes malveillants** : l'utilisation d'un mécanisme de détection de la menace au niveau de l'équipement (ex. : EDR) permet d'analyser les évènements internes de l'équipement et d'identifier des correspondances avec des indicateurs de compromission ou des comportements malveillants.

2.4.2 Protection des ressources

2.4.2.1 Protection des réseaux

La protection des ressources réseau peut s'appuyer sur différents mécanismes :

- ***Software Defined Perimeter* (SDP) [11]** : ce mécanisme permet l'établissement d'un tunnel, notamment *Virtual Private Network* (VPN), dans des modèles de déploiement de type client/-serveur, client/passerelle ou serveur/serveur, par exemple. Par défaut, le port d'accès pour l'établissement du tunnel est fermé et une authentification préalable du sujet est nécessaire sur le plan de contrôle. Si l'accès est autorisé, les conditions d'accès sont fournis au client et à la passerelle (serveur SDP) afin de permettre l'établissement du tunnel. Ces conditions d'accès incluent notamment le port d'accès à ouvrir et à utiliser par le client, ainsi que la liste des ressources auxquelles le sujet peut accéder au travers du tunnel. Cette approche permet ainsi d'établir de manière dynamique un tunnel et d'appliquer les règles de filtrage reposant sur l'identité du sujet. L'utilisation de SDP nécessite cependant un agent local sur l'équipement afin de communiquer avec le plan de contrôle et d'appliquer les conditions d'accès fournies. Il est à noter que tous les échanges avec le plan de contrôle sont réalisés au travers d'un tunnel sécurisé. La figure 2 illustre les principes généraux des mécanismes d'accès SDP dans un déploiement client/passerelle.

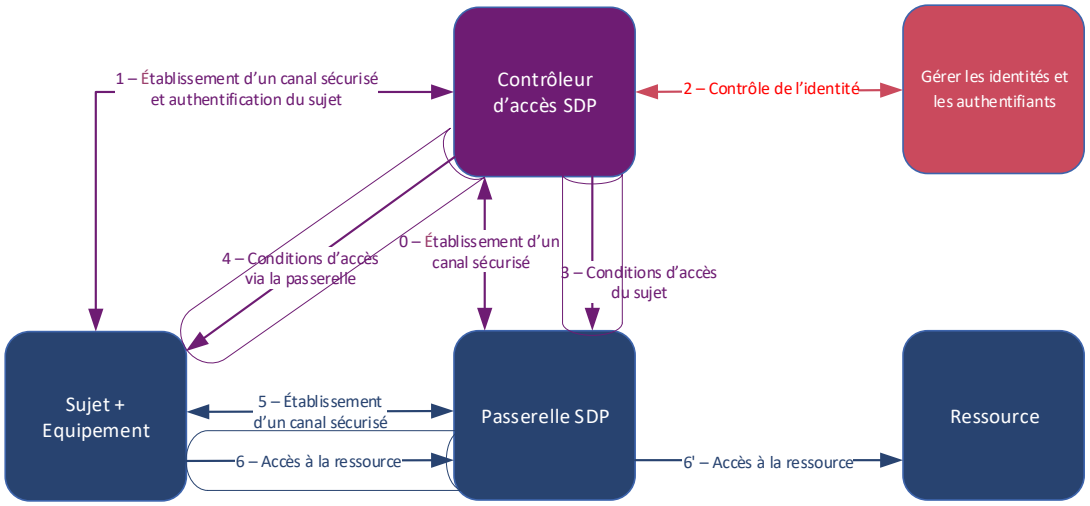

FIGURE 2 – Mécanismes d'accès SDP dans un déploiement client/passerelle

- **Cloisonnement réseau** : les conditions d'accès réseau définies dynamiquement à la suite de l'authentification du sujet sont applicables aux différentes couches du modèle TCP/IP selon le niveau d'accès réseau demandé.
  - Pour un accès local à un LAN, les conditions d'accès peuvent inclure le VLAN ou le PVLAN dans lequel le sujet est cloisonné afin de limiter sa visibilité au sein d'un segment réseau.
  - Pour un accès à un réseau IP distant, les conditions d'accès incluent la mise en œuvre d'un tunnel VPN de type IPsec ou TLS permettant un cloisonnement par le chiffre.
  - Pour un accès à un service applicatif distant et un cloisonnement réseau de bout en bout entre le sujet et le service applicatif, les services hébergés par les équipements sont par défaut inaccessibles (le service n'est pas accessible sur son réseau local et donc cloisonné de celui-ci). Les conditions d'accès incluent dans ce cas l'ouverture du port d'écoute du service à cet utilisateur et l'établissement d'un cloisonnement par le chiffre avec authentification mutuelle.

2.4.2.2 Protection des applications

Dans cette section, seuls les mécanismes de protection dont la configuration est déterminée dynamiquement au travers d'un mécanisme de contrôle d'accès de type ABAC sont abordés. En particulier, le cloisonnement applicatif avec l'utilisation de conteneurs ou l'assurance sécurité des différents logiciels (au travers des sujets de la chaîne d'approvisionnement) ne sont pas traités ici. Seule la protection des applications au travers de l'utilisation d'un proxy (serveur mandataire) ou d'un *reverse* proxy (serveur mandataire inverse) est abordée ci-après. Bien que ces composants peuvent offrir des services de protection réseau et donc être présentés dans la section 2.4.2.1, leurs objectifs principaux dans le modèle *Zero Trust* sont d'offrir des services de protection des applicatifs, et potentiellement de protection des données par analyse des flux de communication.

- **Proxy *Zero Trust*** : pour les accès à des services publics exposés sur Internet, les contrôles sont effectués au travers d'un proxy. Les contrôles réalisés sont identiques à tout autre proxy classique (ex. : filtrage d'URL pour les accès Web, analyse de contenus, etc.). La différence majeure réside dans l'authentification obligatoire du sujet au proxy et dans l'évaluation continue de ses autorisations. L'utilisation d'un modèle ABAC sur un proxy permet d'adapter les autorisations selon l'utilisateur et le poste utilisé. Le cas échéant, le proxy peut couper tous les accès à Internet de manière dynamique si le niveau de confiance accordé au sujet et à son équipement est dégradé. Ce mécanisme a pour objectif de protéger l'utilisateur, l'intégrité des applications de son poste et potentiellement empêcher une fuite de données.
- ***Reverse* proxy *Zero Trust*** : cette approche repose sur un *reverse* proxy nécessitant une authentification préalable de l'utilisateur afin de déterminer dynamiquement les conditions d'accès qui lui sont applicables. Cette approche permet de limiter les accès aux services de l'entité selon le profil de l'utilisateur. Il s'agit du socle minimal de fonctions assurées par un *reverse* proxy *Zero Trust*. En effet, différents mécanismes supplémentaires peuvent être utilisés, selon les cas d'usage, pour contrôler les flux entrants lorsque ceux-ci sont déchiffrés au niveau du *reverse* proxy. Cela peut notamment inclure des contrôles syntaxiques et sémantiques au niveau applicatif (ex. : WAF) pour protéger les applications internes de l'entité, des contrôles par liste d'autorisations sur les commandes pouvant être émises par le sujet vers des services internes, etc. Par rapport à une approche SDP, cette approche ne nécessite pas l'utilisation d'un agent de communication avec le plan de contrôle *Zero Trust* sur le client mais impose des limitations selon les protocoles supportés par le *reverse* proxy. La figure 3 illustre les principes généraux des mécanismes d'accès avec un *reverse* proxy *Zero Trust*.

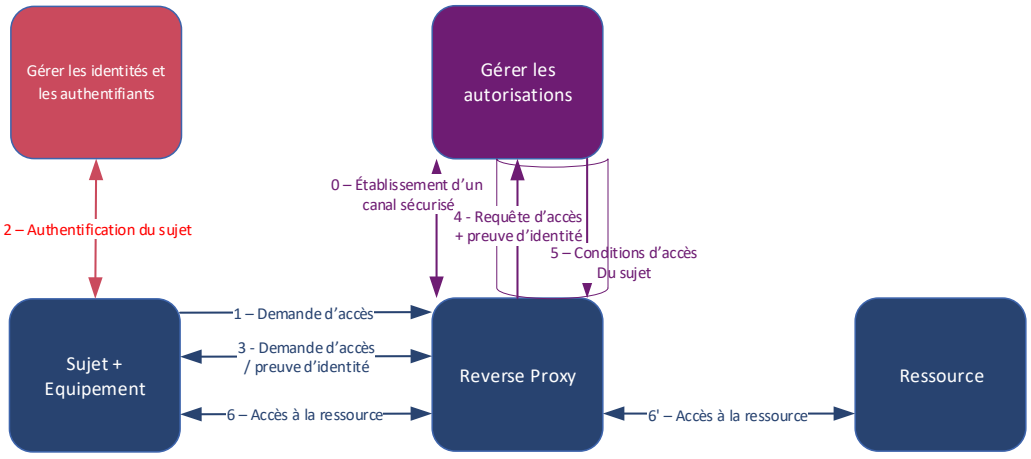

FIGURE 3 – Mécanismes d'accès avec un *reverse* proxy *Zero Trust*

Information

Bien que l'approche avec un *reverse* proxy *Zero Trust* ne nécessite pas l'utilisation d'un agent spécifique *Zero Trust*, il est important de distinguer le niveau de confiance et de visibilité qui peut être atteint entre des postes maîtrisés et des postes personnels. Bien souvent, les postes maîtrisés disposent d'autres types d'agent permettant de faciliter la gestion de leur conformité et/ou la détection de la menace. Les prises de décisions d'accès avec des postes maîtrisés se font donc avec un nombre d'attributs plus important et d'un niveau d'authenticité plus élevé qu'avec des postes personnels.

2.4.2.3 Protection des données

Les mécanismes de protection des données utilisés dans le modèle *Zero Trust* ne sont pas nouveaux. Il s'agit ici d'adapter ces mécanismes à l'utilisation du modèle de contrôle d'accès ABAC et aux hypothèses du *Zero Trust*. Ces mécanismes de protection sont :

- **Contrôle d'accès dynamique aux données** : il s'agit ici de contrôler les opérations sur les données et de limiter celles-ci de manière dynamique aux seules personnes autorisées et équipements conformes. Plus particulièrement, ces contrôles peuvent être mis en œuvre sur :
  - la création et l'import des données en rendant obligatoire la labélisation (l'application des attributs de sécurité et de leurs valeurs) ;
  - l'export des données pour limiter les risques de fuite de données ;
  - le masquage dynamique des données permettant un accès à un sous-ensemble des données.
- **Protection cryptographique des données** : une protection cryptographique des données devrait être appliquée en complément des mécanismes de contrôle d'accès dynamique afin de renforcer la sécurité de ces données en cohérence avec leurs besoins en confidentialité et en intégrité. Ces mécanismes sont applicables pour les données au repos et en transit.

2.5 Principaux risques associés au modèle Zero Trust

- **Centralisation des décisions d'accès** : le déport des décisions d'accès local à une ressource vers une infrastructure centralisée implique une dépendance des accès aux fonctions et aux données métier à un nouveau service transverse. Ce service transverse peut devenir, selon les cas d'usage, critique au bon fonctionnement du SI ou à sa sécurité.
- **Disponibilité, intégrité et authenticité des attributs** : les décisions d'accès sont dépendantes des attributs utilisés par le moteur de règles. L'indisponibilité ou le manque d'intégrité/authenticité des données d'entrée utilisées par le moteur de règles peuvent mener à des pertes d'accès ou à des accès non autorisés aux ressources de l'entité. Répondre aux différentes contraintes de sécurité associées à ces attributs (cf. 2.3.2) est un sujet complexe à traiter.
- **Justesse du score de confiance** : la prise en compte du comportement des utilisateurs dans une évaluation dynamique du score de confiance nécessite un temps de mise au point conséquent et

une maturité forte sur la thématique de la détection de la menace. Dans le pire des cas, l'entité pourrait avoir un faux sentiment de sécurité alors que le taux de faux positifs est élevé (accès illégitime autorisé à tort).

- **Écarts entre le modèle théorique et les implémentations existantes** : le terme *Zero Trust* n'est, en soi, qu'un modèle et ne définit en aucun cas les fonctions de sécurité d'une technologie dite *Zero Trust*. Il est donc essentiel de revenir aux fonctionnalités de sécurité offertes par les différentes solutions des éditeurs et d'identifier leurs limitations avec le modèle théorique afin de bien évaluer leurs impacts d'un point de vue sécurité.
- **Manque de standardisation** : le manque de standardisation sur la définition des attributs ou des protocoles de communication permettant le contrôle d'accès dynamique engendre une interopérabilité limitée entre les différentes solutions des éditeurs ou entre différentes entités en cas de fédération d'identités, pour du partage de données par exemple. Une entité peut donc se retrouver avec une dépendance plus ou moins forte vis-à-vis de l'éditeur choisi, ou potentiellement dans l'incapacité de partager de l'information avec d'autres entités.
- **Impact sur les performances d'accès aux ressources** : l'entité doit prendre en compte les éventuels impacts sur les délais et les latences d'accès à ses ressources lors la mise en œuvre du modèle *Zero Trust*. En effet, l'évaluation continue des demandes d'accès (par exemple avec l'utilisation de nombreux attributs, un contrôle d'accès par action du sujet) pourrait avoir des impacts non acceptables sur les performances d'accès à certaines fonctions ou données métier de l'entité. Il est donc important de s'assurer que les composants utilisés pour réaliser ces contrôles d'accès soient dimensionnés de manière appropriée au regard du besoin en disponibilité des ressources accédées.
- **Dépendance avec les services *cloud*** : les mécanismes mettant en œuvre les principes du *Zero Trust* s'appuient sur des technologies avec des besoins en performance élevés, tels que le *machine learning* ou les décisions d'accès selon le modèle ABAC. Le *Zero Trust* n'implique pas l'utilisation de services *cloud*, même si ceux-ci disposent des infrastructures nécessaires pour faciliter leur mise en œuvre. L'utilisation de ces technologies pourrait augmenter la dépendance des entités auprès des fournisseurs de services *cloud* et complexifier davantage toute décision de ré-internalisation de ces différents services.

3
Recommandations

3.1 Objectifs de sécurité et état des lieux

- L'entité doit définir les objectifs de sécurité de chacun de ses systèmes selon une approche par les risques.

Information

Une approche par les risques permet à une entité de définir et de prioriser les actions à mener pour renforcer sa sécurité. En effet, pour une entité donnée, il pourrait être plus pertinent d'un point de vue de la gestion des risques d'engager des efforts d'amélioration de son système d'administration que de s'orienter vers l'utilisation de technologies dites *Zero Trust*.

- L'entité doit évaluer le niveau de sécurité de chacun de ses systèmes au travers d'audits techniques et organisationnels afin d'identifier les écarts entre sa posture de sécurité actuelle et les objectifs visés.
- L'entité doit utiliser les solutions déjà à sa disposition pour améliorer son niveau de sécurité et ainsi réduire le niveau de confiance implicite accordée aux utilisateurs, processus automatiques et équipements.

3.2 Évaluation de faisabilité et définition des besoins d'accès

3.2.1 Identification des cas d'usage

- L'entité doit identifier les cas d'usage pour lesquels la mise en œuvre du modèle *Zero Trust* apporterait un gain de sécurité. Au minimum, le niveau de sécurité de l'entité ne doit pas être dégradé lorsque sa mise en œuvre est motivée par des critères autres que la sécurité (financiers, de performance, etc.).

Pour chacun des cas d'usage retenus :

- L'entité doit avoir un inventaire détaillé et maintenu à jour des utilisateurs, des processus automatiques et des équipements associés aux cas d'usage.
- L'entité doit définir, de manière itérative, la cartographie détaillée des différents composants inclus dans le périmètre retenu et nécessaires à la réalisation des objectifs du cas d'usage.
- L'entité doit identifier les chemins d'accès entre chaque sujet et les ressources cibles (qui doit accéder à quoi et pour quel objectif) et établir, de manière itérative, les différents scénarios d'accès (comment accéder à la ressource selon la politique d'accès définie).

3.2.2 Attributs de sécurité

3.2.2.1 Identifier et appliquer les attributs de sécurité

- L'entité doit identifier l'ensemble des attributs de sécurité portant sur les sujets, les ressources et l'environnement. Pour chacun de ces attributs, les valeurs ou les plages de valeurs autorisées doivent être définies.
- L'entité doit identifier les sources de données nécessaires au calcul des attributs de sécurité dynamiques et la manière dont les valeurs associées seront calculées.
- L'entité doit définir les processus nécessaires pour l'application des attributs de sécurité sur l'ensemble des sujets et des ressources. Ces processus doivent être appliqués aux sujets et ressources lors de leur création, ainsi qu'à ceux déjà existants.
- L'entité doit documenter l'ensemble des attributs de sécurité identifiés en incluant les sources de données nécessaires, leurs modes de calcul, leurs plages de valeurs et une description du périmètre couvert.

3.2.2.2 Évaluer la disponibilité et la qualité des données

- L'entité doit s'assurer de disposer des données nécessaires pour générer les attributs de sécurité pertinents pour les cas d'usage de contrôle d'accès retenus.
- L'entité doit s'assurer de sa capacité à collecter ces données et à les mettre à disposition de la fonction de contrôle d'accès.
- Pour les attributs de conformité :
  - L'entité doit s'assurer de la définition et du maintien des versions de référence des logiciels, paramétrages de durcissement et correctifs applicables par type d'équipement.
  - L'entité doit s'assurer de sa capacité à collecter les données nécessaires au travers de l'utilisation d'agents logiciels locaux de conformité ou par des outils de scans centraux pour les équipements concernés.

- Pour les attributs de niveau de menace :
  - L'entité doit s'assurer, pour les différents scénarios de menace à détecter, que les journaux pertinents peuvent être générés ou que les flux d'information pertinents sont accessibles en clair.
  - L'entité doit s'assurer de sa capacité à capturer et analyser ces données par la mise en œuvre de capteurs physiques ou logiciels sur le réseau ou sur les équipements.
  - L'entité doit s'assurer de la fiabilité des alertes de détection de la menace (faible taux de faux positifs et de faux négatifs), en particulier celles reposant sur une analyse comportementale.

Information

L'amélioration des mesures de détection et d'automatisation des réponses visent à réduire fortement la fenêtre d'attaque d'un acteur malveillant, et ainsi limiter l'impact d'une compromission ou la vraisemblance de l'atteinte d'un événement redouté. Ce renforcement des mesures de détection et de réponse pourrait mener sur certains scénarios à justifier la réduction des mesures de protection sur les équipements, tout en maintenant un niveau de risque acceptable. Cependant, le principe de précaution prévaut. Ces mécanismes de détection et de réponse sont complexes à mettre en œuvre et peuvent être contournés. Le principe de défense en profondeur avec l'utilisation de plusieurs barrières de protection restent donc applicables.

3.2.2.3 Évaluer les contraintes pour la gestion des attributs de sécurité

Pour éviter un faux sentiment de sécurité ou des refus d'accès à tort, il est nécessaire de pouvoir maintenir à jour les différents attributs dans le temps. En particulier :

- L'entité doit s'assurer de l'utilisation de référentiels uniques et d'une gestion centralisée de ceux-ci. Cela inclut, sans être exhaustif, le référentiel des comptes d'accès utilisateurs, le référentiel des comptes d'accès administrateurs, le référentiel des ressources matérielles et logicielles.
- L'entité doit être en capacité de maintenir à jour les référentiels de comptes d'accès, et plus particulièrement de désactiver de manière automatique tout compte d'accès considéré comme compromis dans le système.
- L'entité doit être en capacité de renouveler les secrets des différents sujets et ressources. Cela implique, pour les certificats notamment, la mise en œuvre d'une infrastructure de gestion de clés.
- L'entité doit être en capacité de maintenir à jour ses équipements. Cela implique le maintien du référentiel de correctifs applicables et la gestion centralisée du processus de mise à jour des composants logiciels par rapport à ce référentiel.
- L'entité doit être en capacité de maintenir à jour ses référentiels de détection (indicateurs de compromission, modèles comportementaux, etc.) et avoir une activité de veille relative aux menaces (*Cyber Threat Intelligence*).

- L'entité doit protéger en authenticité et en intégrité les attributs au repos et en transit. Pour la protection des attributs associés à une donnée, cela implique l'utilisation de mécanismes cryptographiques sur les attributs et les métadonnées d'un fichier par exemple.

Attention

Assurer l'intégrité et l'authenticité des attributs utilisés pour le contrôle d'accès est très dépendant du niveau de sécurité des postes utilisés et de la visibilité que l'entité en a. La pratique du BYOD, en particulier, ne permet pas d'accorder un niveau d'assurance élevé vis-à-vis des valeurs retournées par ses équipements (lorsque celles-ci sont disponibles et collectables) pour la prise de décision d'accès.

3.2.3 Politique de contrôle d'accès

De manière générale :

- L'entité doit définir sa politique d'accès uniquement sur des attributs maîtrisés, c'est-à-dire des attributs qu'elle est capable de maintenir à jour et dont elle maîtrise le périmètre de couverture et le niveau de qualité.
- L'entité doit inclure de manière itérative les différents attributs de sécurité, allant d'attributs simples et faciles à maintenir à jour à des attributs plus complexes à mettre au point (ex. : l'analyse comportementale).
- À chaque itération, l'entité doit évaluer le niveau d'efficacité de ses mécanismes de contrôle d'accès dynamique et adapter sa politique de contrôle d'accès en cohérence.
- L'entité doit pondérer le ou les scores de confiance selon l'importance de l'attribut pour l'entité lors des décisions d'accès, et selon le niveau de fiabilité des attributs.
- L'entité doit construire sa politique d'accès sur un ensemble de critères de conformité. Le score de confiance doit être utilisé comme un critère de contrôle de sécurité supplémentaire.
- L'entité doit définir pour chaque type d'équipement un niveau de confiance implicite reposant sur la politique de sécurité qui leur est applicable lorsque le type d'équipement n'est pas utilisé comme critère de conformité lors de la prise de décision d'accès.
- L'entité doit réaliser des évaluations continues afin de calculer un score de confiance (c.-à-d. un niveau de confiance explicite). Le score de confiance d'un équipement ne peut pas pas être supérieur au niveau de confiance implicite qui lui est accordée pour accéder aux ressources de l'entité [9].
- L'entité doit définir des seuils de score de confiance en cohérence avec la criticité DIC des ressources accédées.

9. Le score de confiance d'un équipement doit toujours être calculé au regard du type d'équipement évalué (par exemple, un poste *BYOD* ou un poste maîtrisé par l'entité). Cette évaluation ne peut être qu'une dégradation de la confiance implicitement accordée à un type de poste. En aucun cas un poste *BYOD* ne peut être utilisé par un administrateur pour réaliser des actions d'administration même si l'évaluation explicite du poste semble indiquer que celui-ci est intègre

Information

Bien que le concept du *Zero Trust* permet, en théorie, d'améliorer le niveau de sécurité d'une entité avec une réorientation des mesures de sécurité vers des mesures de détection et de réaction, il est important d'évaluer à chaque étape de sa mise en œuvre son niveau d'efficacité réelle. En effet, celle-ci est dépendante des attributs utilisés ainsi que de leur niveau de protection en intégrité et authenticité (et donc dans la confiance implicite accordée à l'évaluation). Il est donc essentiel de mettre en cohérence le niveau de protection de l'équipement utilisé et le niveau de criticité DIC de la ressource accédée avec le niveau d'efficacité actuelle de la chaîne de contrôle d'accès.

Pour assurer un fort niveau de robustesse de la preuve d'identité, les recommandations suivantes sont applicables :

- Tout accès d'un utilisateur, d'un processus automatique ou d'un équipement devrait être identifié de manière unique et authentifié par l'utilisation d'un authentifiant de type certificat.
- Tout utilisateur devrait utiliser un second facteur d'authentification permettant l'utilisation de la clé privée associée à son certificat.
- Le secret d'authentification de type certificat devrait être protégé dans un composant matériel dédié. Pour les utilisateurs, un jeton (*token*) physique devrait être utilisé.
- Les mécanismes d'authentification passive ne devraient pas être utilisés.

Pour les équipements utilisés lors des demandes d'accès, les recommandations suivantes sont applicables :

- Les équipements personnels de type BYOD doivent être considérés par défaut comme de faible confiance et donc leurs accès limités à des services non critiques de l'entité.
- Les accès d'administration doivent être réalisés à partir de postes ayant un niveau de confiance implicite élevé. Les mesures du guide d'administration de l'ANSSI [2] pour la sécurisation des postes d'administration restent donc applicables y compris pour l'administration des fonctions du plan de contrôle *Zero Trust*.

Pour l'application du principe de moindre privilège à la suite de l'authentification des sujets, les recommandations suivantes sont applicables :

- Après l'authentification d'un sujet, un canal sécurisé doit être établi assurant la confidentialité, l'intégrité et l'authenticité des données par des mécanismes cryptographiques.
- Les accès à privilège doivent être réalisés au travers d'un tunnel VPN IPSec. Le cas échéant, l'utilisation exclusive d'un *reverse* proxy *Zero Trust* n'est pas recommandée.
- Les accès utilisateurs à des services publics exposés sur Internet doivent transiter par un proxy *Zero Trust*.

3.3 Acquisition, développement et maintenance

- L'entité doit définir des jalons intermédiaires dans la mise en œuvre du modèle *Zero Trust* pour les cas d'usage retenus. La cohérence des risques doit être assurée à chaque jalon.
- L'entité doit privilégier l'utilisation de protocoles standards, lorsque ceux-ci existent, afin de limiter sa dépendance à des solutions d'un même éditeur ou d'accepter le risque associé à cette dépendance.
- L'entité doit s'assurer de la compatibilité de ses ressources avec les fonctionnalités du modèle ABAC. Le cas échéant, l'entité doit prévoir le développement ou la mise en œuvre de solutions matérielles ou logicielles tierces supplémentaires.
- L'entité doit s'assurer du niveau d'assurance sécurité des solutions logicielles acquises ou développées dans le cadre de son architecture *Zero Trust*.
- L'entité doit réaliser des campagnes de tests pour identifier toutes les règles pouvant causer des accès refusés à tort.
- L'entité doit réaliser des tests de sécurité, notamment des audits de configuration et des tests d'intrusion pour identifier toute règle trop permissive menant à des accès autorisés à tort.
- L'entité doit prévoir une durée d'apprentissage conséquente afin de fiabiliser les décisions d'accès reposant sur les comportements de l'utilisateur et/ou de l'équipement.
- L'entité doit prévoir les moyens humains, techniques et organisationnels nécessaires pour le support des utilisateurs en cas d'accès refusé à tort, ainsi que leur accompagnement dans la gestion du changement.

3.4 Recommandations générales sur l'architecture

- L'entité doit cloisonner son réseau de manière logique ou physique. Cette segmentation reste nécessaire pour couvrir des attaques au niveau réseau.
- L'entité doit cloisonner de manière logique ou physique le plan de contrôle et le plan de données.
- L'entité doit s'assurer que tous les accès d'un équipement du plan de données vers le plan de contrôle est réalisé via l'établissement d'un canal sécurisé en confidentialité, intégrité et authenticité avec une authentification mutuelle.
- L'entité doit s'assurer de réaliser ses accès d'administration au travers d'une chaîne d'accès différente de celle des accès utilisateurs.
- L'entité doit mettre en œuvre des mécanismes de redondance et de synchronisation des états sur les équipements du plan de contrôle assurant le contrôle d'accès continu.
- L'entité doit répartir et segmenter les services de contrôle d'accès dynamique par type d'usage afin de limiter l'impact sur l'entité en cas de défaillance.

Bibliographie

[1] *Le Modèle Zero Trust*.
Publication scientifique, ANSSI, août 2020.
https://cyber.gouv.fr/publications/le-modele-zero-trust.

[2] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide ANSSI-PA-022 v3.0, ANSSI, mai 2021.
https://cyber.gouv.fr/guide-admin-si.

[3] *La méthode EBIOS Risk Manager - Le Guide*.
Guide ANSSI-PA-048 v1.5, ANSSI, mars 2024.
https://cyber.gouv.fr/ebios-rm.

[4] *RGS Annexe B3 : Règles et recommandations concernant les mécanismes d'authentification*.
Référentiel Version 1.0, ANSSI, janvier 2010.
https://cyber.gouv.fr/rgs.

[5] *RGS Annexe B2 : Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://cyber.gouv.fr/rgs.

[6] *RGS Annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques*.
Référentiel Version 2.03, ANSSI, février 2014.
https://cyber.gouv.fr/rgs.

[7] *Authentification multifacteurs et mots de passe*.
Guide ANSSI-PG-078 v1.0, ANSSI, octobre 2021.
https://cyber.gouv.fr/guide-authentification.

[8] *Instruction générale interministérielle n°1300*.
Référentiel, SGDSN, août 2021.
https://cyber.gouv.fr/igi1300.

[9] *Guide to Attribute Based Access Control (ABAC) Définition and Considerations*.
Rapport, NIST, janvier 2014.
https://doi.org/10.6028/NIST.SP.800-162.

[10] *Zero Trust Architecture*.
Rapport, NIST, août 2020.
https://doi.org/10.6028/NIST.SP.800-207.

[11] *Software-Defined Perimeter (SDP) Specification v2.0*.
Rapport, CSA, octobre 2022.
https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2.

[12] *Zero Trust Maturity Model*.
Rapport, CISA, avril 2023.
https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf.

Version 1.0 - 20/06/2025 - ANSSI-PA-111

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité