Livre blanc sur la sécurité des produits Dahua

V2.0

Zhejiang Dahua Technology Co., Ltd

Avis juridique

Avis de droit d’auteur

Sans l’autorisation écrite préalable de Zhejiang Dahua Technology Co., Ltd. (ci-après dénommée « Dahua »), personne n’est autorisé à copier, transmettre, distribuer ou stocker le contenu de ce document sous quelque forme que ce soit.

Les produits décrits dans ce document peuvent contenir des logiciels protégés par le droit d’auteur de Dahua et d’autres tiers. Personne ne peut copier, distribuer, modifier, extraire, décompiler, désassembler, décrypter, faire de l’ingénierie inverse, louer, transférer, accorder une sous-licence ou enfreindre de quelque manière que ce soit le droit d’auteur du logiciel sous quelque forme que ce soit, sauf avec l’autorisation du propriétaire concerné.

Avis de marques déposées

- , , , , HDCVI sont des marques commerciales ou des marques déposées de Zhejiang Dahua Technology Co., Ltd.
- Les noms des autres marques déposées ou sociétés qui peuvent être mentionnées dans ce document appartiennent à leurs propriétaires respectifs.

Déclaration de responsabilité

- Dans la mesure où les lois applicables le permettent, la société ne compensera en aucun cas les dommages spéciaux, annexes, indirects et secondaires causés par les contenus et produits pertinents décrits dans ce document, ni les pertes de bénéfices, de données, de clientèle, de documents ou d’économies escomptées.
- Les produits décrits dans ce document sont fournis « conformément au statu quo ». Sauf si les lois applicables l’exigent, la société ne fournit aucune garantie explicite ou implicite pour tous les contenus du document.

Déclaration de conformité au contrôle des exportations

Dahua se conforme aux lois et règlements applicables en matière de contrôle des exportations et met en œuvre les exigences liées à l’exportation, à la réexportation et au transfert de matériel, de logiciels et de technologies. En ce qui concerne les produits décrits dans ce manuel, nous vous prions de bien vouloir comprendre et respecter strictement les lois et réglementations nationales et étrangères applicables en matière de contrôle des exportations.

À propos de ce document

- Les produits, services ou fonctionnalités que vous achetez sont soumis aux contrats et conditions commerciales de l'entreprise. Tout ou partie des produits, services ou fonctionnalités décrits dans ce document peuvent ne pas entrer dans le cadre de votre achat ou de votre utilisation.
- Si l'opération n'est pas effectuée conformément aux instructions de ce document, toute perte causée par celle-ci sera à la charge de l'utilisateur.
- Si le document PDF obtenu ne peut être ouvert, veuillez mettre à jour le logiciel de lecture de documents utilisé ou utiliser d'autres outils de lecture courants.
- La société se réserve le droit de modifier toute information contenue dans ce document à tout moment, et le contenu modifié sera ajouté dans la nouvelle version de ce document sans préavis.
- Ce document peut contenir des inexactitudes techniques, des incohérences avec les fonctions et les opérations du produit ou des erreurs typographiques, sous réserve de l'interprétation finale de la société.

Présentation

Le développement continu et approfondi de l'AIoT doit être établi sur la base d'une cybersécurité et d'une protection de la vie privée responsables, ouvertes, professionnelles et systématiques. Dahua a toujours considéré la cybersécurité et la protection de la vie privée comme l'un des principaux objectifs de l'entreprise, et continue de mettre en place des fonds spéciaux pour s'assurer que la recherche, le développement et la livraison de la sécurité des produits, la recherche sur les technologies de sécurité clés et la construction du système de réponse aux incidents de sécurité soient continuellement mis en avant. Avant de sortir les produits, tous doivent passer des tests rigoureux menés par le laboratoire d'attaque et de défense. À l'heure actuelle, Dahua a obtenu des résultats fructueux dans des domaines des technologies de sécurité tels que l'informatique de confiance, le chiffrement des données, la protection de la vie privée et les tests d'attaque et de défense, et a intégré des applications dans une gamme complète de produits.

Ce livre blanc sur la sécurité des produits vise à fournir aux utilisateurs une compréhension plus approfondie des capacités de sécurité des produits Dahua grâce à une élaboration complète de la construction du cadre de sécurité des produits Dahua, des pratiques de base en matière de sécurité, des applications de technologie de sécurité et des recommandations d'utilisation de la sécurité.

Glossaire

Abréviation	Explication
UCD (User Centered Design)	Conception axée sur l'utilisateur dans le processus de conception, l'expérience de l'utilisateur est au centre des décisions de conception, et un modèle de conception priorisant l'utilisateur est mis en avant.
sSDLC (Secure Software Development Lifecycle)	Cycle de vie du développement logiciel sécurisé
ESD (Electrostatic Discharge)	Décharge électrostatique, technologie permettant de protéger les composants électroniques de l'appareil contre les dommages électrostatiques.
I2C (Inter-Integrated Circuit Bus)	Bus de circuits intégrés, le bus I2C a été conçu par Philips au début des années 80 pour permettre une communication facile entre les composants qui se trouvent sur le même circuit imprimé.
SPI (Serial Peripheral Interface)	L'interface pour périphériques série est un bus de communication synchrone à haut débit en duplex intégral.

Abréviation	Explication
RBAC (Role-Based Access Control)	Contrôle d'accès basé sur les rôles, permet d'associer des autorisations à des rôles ; les utilisateurs deviennent membres des rôles appropriés et reçoivent les autorisations correspondantes.
PKI (Public Key Infrastructure)	Infrastructure à clé publique, utilisée pour mettre en œuvre la génération, la gestion, le stockage, la distribution et la révocation de clés et de certificats basés sur le système de chiffrement à clé publique.
KMS (Key Management Service)	Service de gestion des clés, fournit des services de séquestre de clés sécurisés et conformes.
KDF (Key Derivation Function)	Fonction de dérivation de clé, méthode de dérivation de clé qui utilise une fonction pseudo-aléatoire pour dériver une nouvelle clé à partir de la clé principale.
TLS (Transport Layer Security)	Sécurité de la couche de transport, protocole de chiffrement de la couche de transport.
ARP (Address Resolution Protocol)	Protocole de résolution d'adresses, protocole réseau sous-jacent permettant d'obtenir des adresses MAC physiques à partir d'adresses IP.
RGPD (General Data Protection Regulation)	Règlement général sur la protection des données, une loi importante sur la protection des données personnelles édictée par l'Union européenne.
CCPA (California Consumer Privacy Act)	La Loi californienne sur la protection de la vie privée des consommateurs est une loi californienne visant à protéger la vie privée et les informations des consommateurs.
C5 (Cloud Computing Compliance Controls Catalog)	Le Catalogue de contrôles de conformité du Cloud Computing, la norme de sécurité du cloud proposée par le BSI (Office fédéral allemand pour la sécurité de l'information).
BSI	L'Office fédéral allemand de la sécurité de l'information.

Historique des révisions

N°	Version	Contenu révisé	Date de sortie
1	V1.0.0	Première publication	2017.6.30
2	V2.0.0	Ajout des touts derniers résultats de la Référence de base de sécurité v1.3/v2.0/v2.1 et d'une recherche sur les technologies de sécurité.	2020.2.28

Table des matières

1 Cycle de vie du développement de la sécurité

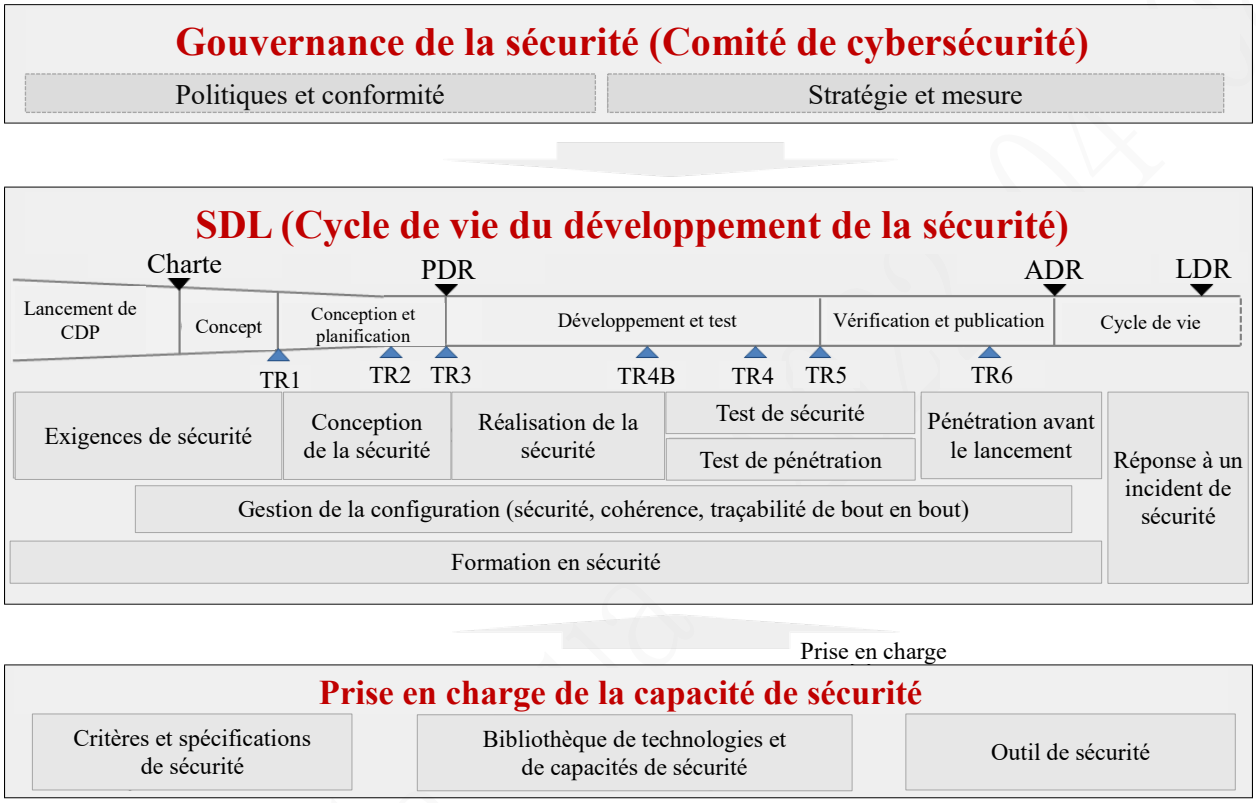

Figure 1-1 Processus de développement de la sécurité des produits

Dahua encourage continuellement la construction d'un sSDLC (cycle de vie de développement logiciel sécurisé), effectue une évaluation complète et approfondie de la maturité des activités de sécurité, et établit un système de gestion et de contrôle de la R&D en matière de sécurité adapté à Dahua en standardisant le processus de développement et en contrôlant l'ingénierie logicielle.

- Mettre en place une équipe de sécurité professionnelle chargée de former tous les membres du centre de R&D. Cette formation portera sur la compréhension des exigences de sécurité, les méthodes de conception de la sécurité, les normes de codage de la sécurité, les méthodes de test de la sécurité et l'utilisation de divers outils de sécurité.
- Effectuer des évaluations des risques liés à la sécurité et à la vie privée lors de la phase de définition du produit, en considérant la base de référence de sécurité et la base de référence de vie privée comme les exigences de sécurité les plus fondamentales pour le produit, et en formulant des activités et des exigences de sécurité proportionnelles au niveau de risque en fonction des résultats de l'évaluation des risques.

- Lors de la phase de conception du produit, suivre strictement les principes de base de la conception de la sécurité tels que la surface d'attaque minimale, l'autorité minimale, la sécurité par défaut, la défense en profondeur, etc., mettre en œuvre la modélisation et l'atténuation des menaces avec la combinaison d'experts en sécurité réseau et d'experts en produits, et pratiquer la « sécurité dès la conception ».
- Lors de la phase de développement du produit, suivre strictement les spécifications de codage sécurisé. Dans le cadre de l'inspection croisée du code, la détection statique de la sécurité du code et la réparation des défauts sont effectuées de manière standardisée (comme Coverity, etc.).
- Lors de la phase de vérification du produit, effectuer une analyse antivirus complète, une analyse de la vulnérabilité du système, une analyse de la vulnérabilité du Web, une vérification des vulnérabilités connues, une vérification des fonctions de sécurité, une vérification des tests de pénétration pour les attaques et des tests par fuzzing.
- Effectuer des contrôles de sécurité avant le lancement du produit, portant notamment sur la cohérence des exigences de sécurité et de la conception de la sécurité, la conformité des données, le nettoyage des audits de sécurité du code, la vérification de l'exhaustivité des tests de sécurité et des tests de pénétration, les documents d'orientation sur la sécurité du produit, etc.

2 Modèle de sécurité

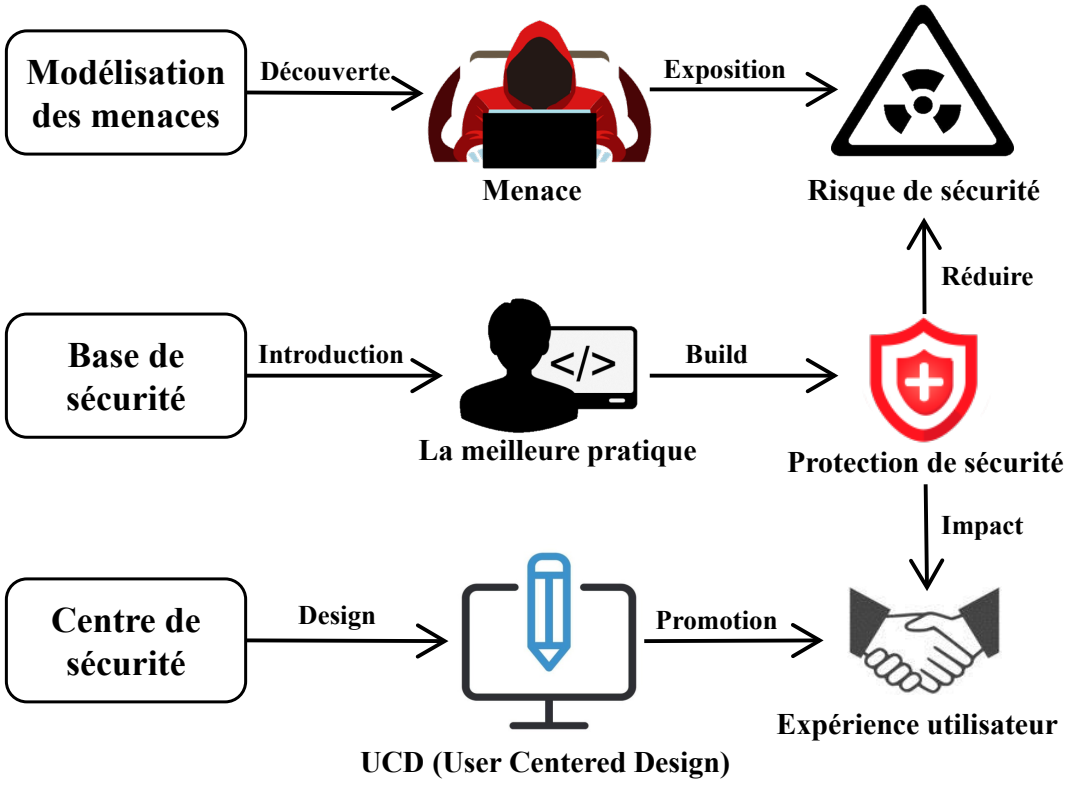

Figure 2-1 Modèle de sécurité des produits

L'étape des exigences et de la conception de la sécurité du produit comprend : une modélisation des menaces basée sur l'exploration en profondeur qui expose les risques de sécurité potentiels ; une protection de la sécurité hiérarchique et systématique basée sur une norme de base de sécurité itérative continue ; une expérience utilisateur basée sur un centre de sécurité axé sur l'utilisateur avec une gestion de la sécurité pratique et un statut de sécurité visible. Ces trois activités de sécurité fonctionnent ensemble pour améliorer continuellement le modèle technique itératif de protection de la sécurité.

3 Modélisation des menaces

La modélisation des menaces est un processus basé sur une méthode structurée qui identifie et évalue systématiquement les risques de sécurité des produits et développe des mesures d'atténuation ciblées. Dahua adopte la méthode de modélisation des menaces, qui vise à réfléchir aux points faibles et aux failles de la sécurité des produits du point de vue d'un attaquant, afin d'améliorer continuellement les mesures de sécurité des produits et de réduire les risques de sécurité.

Dahua emploie la méthode de modélisation des menaces la plus populaire du secteur, basée sur le modèle STRIDE. L'idée de base est d'effectuer une évaluation et une analyse basées sur les six types de menaces principales suivantes :

- Usurpation
- Sabotage
- Répudiation
- Divulgation d'informations
- Déni de service
- Élévation de privilège

Dans le même temps, le modèle d'arborescence d'attaque a été introduit pour améliorer efficacement la mise en œuvre de la modélisation des menaces STRIDE et approfondir l'analyse des risques de sécurité des produits. Avec le développement de la technologie et l'enrichissement continu des méthodes d'attaque, l'introduction des modèles d'arborescence d'attaque aide à identifier les menaces posées par les nouvelles méthodes d'attaque le plus tôt possible.

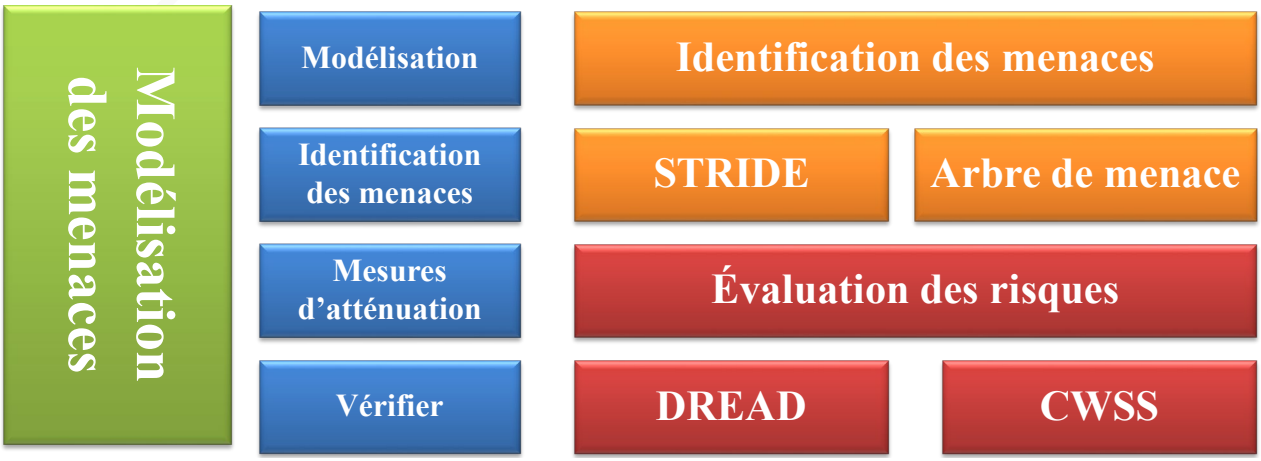

Figure 3-1 Modélisation des menaces

4 Protection de sécurité

4.1 Base de sécurité

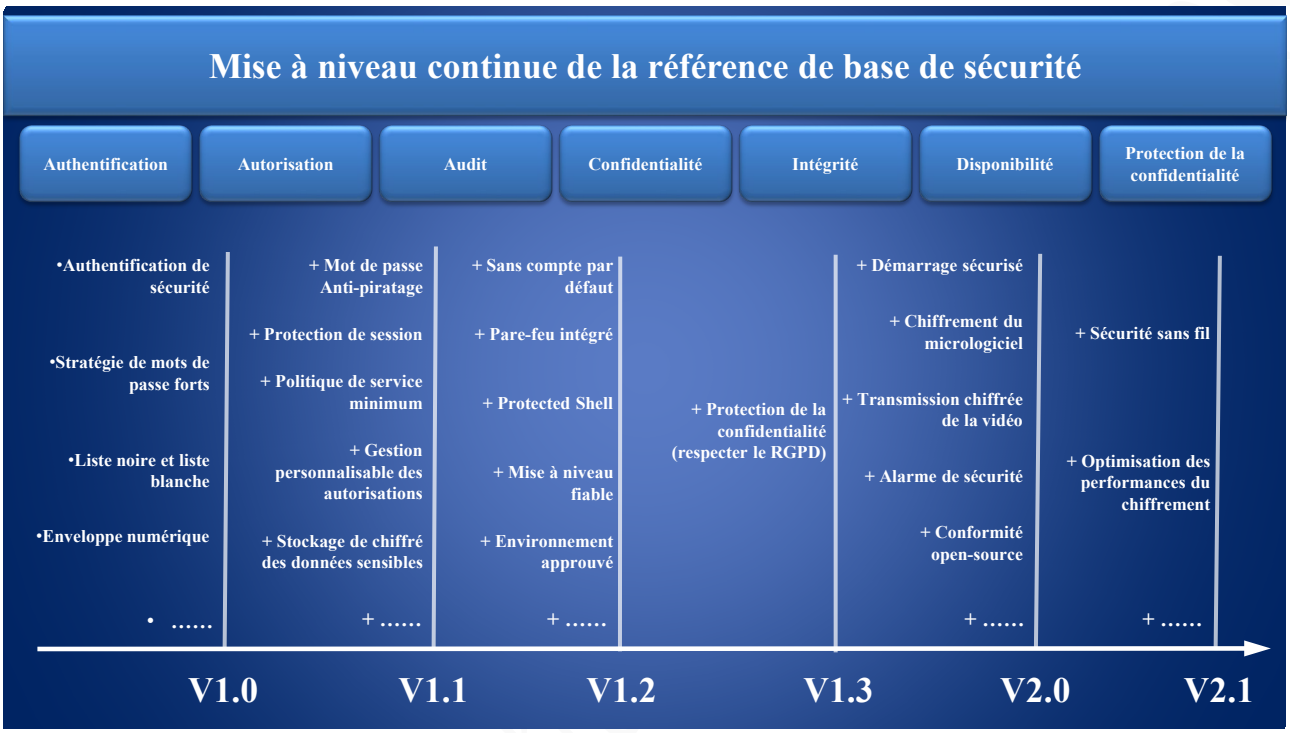

Figure 4-1 Référence de base de sécurité

Depuis le lancement du plan « Security Baseline » (base de sécurité), Dahua adhère aux principes fondamentaux de « sécurité dès la conception » et de « sécurité par défaut », effectue des recherches approfondies sur les technologies de sécurité des produits et fournit aux utilisateurs des protections de sécurité suffisantes.

La base de sécurité est basée sur les principes de la conception de la sécurité et de la vie privée et met ceux-ci en œuvre. Elle agence les éléments de sécurité « AAA + CID + P » et forme un cadre de protection systématique couvrant la sécurité physique, la sécurité du système d'exploitation, la sécurité des applications, la sécurité des données, la sécurité du réseau et la protection de la vie privée.

L'agencement des éléments de sécurité « AAA + CIA + P » est le suivant :

- AAA : authentification, autorisation, audit
- CIA : confidentialité, intégrité, disponibilité
- P : Protection de la confidentialité

Afin de garantir l'adéquation des éléments de sécurité de base, Dahua a mené une série d'activités telles que : « Conformité légale et réglementaire », « Étude des normes et des spécifications », « Suivi dynamique de l'industrie », « Analyse de la modélisation des menaces », « Recherche préalable sur les technologies clés », « Recherche des exigences de sécurité » pour produire en permanence des exigences de sécurité efficaces et de grande valeur en guise de référence de base en matière de sécurité.

En tant que l'une des normes d'entreprise importantes de Dahua, la Référence de base de sécurité est une partie importante du sSDLC (Cycle de vie du développement sécurisé d'un application) de Dahua. Il a été profondément intégré dans le système d'assurance qualité des produits pour garantir que toute la série de produits Dahua bénéficie du niveau par défaut de sécurité de l'usine.

4.2 Cadre de sécurité

Figure 4-2 Cadre de sécurité des produits

Le cadre de sécurité du produit protège la sécurité du produit en vertu de six dimensions : Sécurité physique, Sécurité du système d'exploitation, Sécurité des applications, Sécurité des données, Sécurité du réseau et Protection de la confidentialité :

- Sécurité physique : Du point de vue de la protection physique du produit lui-même, en

utilisant des moyens structurels physiques réels comme mesure de protection pour fournir un cadre physique à la fois sûr et fiable pour le produit.

- Sécurité du système d'exploitation : Le système d'exploitation est le gestionnaire des ressources, il fournit l'environnement d'exécution de base pour les services et construit un environnement d'exécution de base sécurisé et fiable, grâce à une informatique fiable, à la technologie virtuelle, au contrôle des autorisations et à d'autres technologies.
- Sécurité des applications : La formation d'une structure de protection de sécurité en boucle fermée basée sur l'authentification, l'autorisation et l'audit pour renforcer les capacités d'auto-sécurité du service au niveau de la couche application.
- Sécurité des données : Elle est basée sur la cryptographie, la signature numérique et d'autres technologies, construit la protection de sécurité du cycle de vie complet du stockage, de la transmission, du partage et de la destruction des données pour éviter les fuites, les altérations et la destruction des données.
- Sécurité du réseau : Introduction d'une alarme de sécurité, d'un pare-feu et d'autres technologies de défense contre les attaques pour améliorer les capacités de détection et de défense contre les attaques du réseau.
- Protection de la confidentialité : Fournir des mesures de protection de la vie privée couvrant tout le cycle de vie des données, incluant la collecte, la transmission, le stockage, l'utilisation, le partage, l'affichage, la copie et la suppression de données, etc.

4.3 Description de la technologie de sécurité

4.3.1 Sécurité physique

4.3.1.1 Démarrage sécurisé

Sur la base du démarrage sécurisé du SoC, une chaîne de confiance de démarrage est construite basée sur la puce physique, ce qui permet de garantir efficacement l'intégrité et la légalité du processus de démarrage de l'appareil et éviter de charger un micrologiciel non approuvé.

4.3.1.2 Trust Zone

La technologie Trust Zone est une fonction de sécurité importante fournie par ARM. Sur la base de cette technologie, il est possible de mettre en œuvre une zone d'exploitation sécurisée physiquement séparée et une zone de stockage sécurisée, et de fournir une base sécurisée pour les services de la couche d'application supérieure.

4.3.1.3 OTP

L'OTP (One Time Programmable) est une zone de stockage programmable à usage unique. Les données (telles que les informations d'identification uniques de l'appareil) ne peuvent pas être modifiées après avoir été écrites, ce qui permet de garantir efficacement l'intégrité des données écrites.

4.3.1.4 TRNG

TRNG (True Random Number Generator) consiste à convertir des phénomènes physiques imprévisibles en signaux électriques, et à obtenir une série de nombres aléatoires en collectant à plusieurs reprises des signaux aléatoires. En théorie, ces nombres aléatoires sont complètement imprévisibles.

4.3.1.5 Puce de sécurité

La puce de sécurité fournit un algorithme de cryptage de sécurité et prend en charge le stockage sécurisé des données sensibles telles que la clé, protégeant ainsi efficacement la confidentialité des données.

4.3.1.6 Interface de communication physique

L'interface physique de l'appareil adopte une protection statique ESD pour assurer le fonctionnement sécurisé de l'interface et du système. La carte mère ne réserve pas les ports série inactifs, USB, I2C, SPI et autres interfaces de communication sur la périphérie de la puce, et elle est directement fermée à l'intérieur du système pour empêcher les interfaces non autorisées d'accéder aux ressources internes du système. Pour le port de débogage JTAG, le port d'écriture du programme, etc., la carte mère ne réserve pas d'interfaces pertinentes.

4.3.1.7 Sauvegarde à double flash

L'espace Flash inactif est utilisé pour sauvegarder les données du micrologiciel dans la zone flash principale. Lorsque les données flash principales sont détruites, l'appareil redémarre automatiquement et restaure le micrologiciel dans la zone flash principale en fonction des données de sauvegarde.

4.3.1.8 Technologie à double contrôleur

L'appareil est doté d'une structure de conception à double carte mère. Les cartes mères fonctionnent ensemble et se sauvegardent l'une par rapport à l'autre. Lorsque la carte mère principale est endommagée, l'hôte passe de manière transparente à la carte mère de secours pour assurer un suivi ininterrompu et permettre la continuité et la robustesse de l'activité de l'appareil.

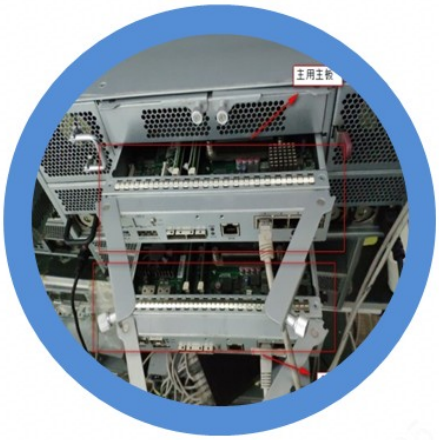

Figure 4-3 Technologie à double contrôleur

4.3.1.9 Alimentation double de secours

L'appareil adopte une conception multi-alimentation pour maintenir plusieurs alimentations en fonctionnement en même temps. Lorsqu'une des alimentations est interrompue en raison d'une panne, la double alimentation peut continuer à maintenir l'alimentation et à maintenir le fonctionnement normal de l'appareil.

Figure 4-4 Technologie à double alimentation de secours

4.3.2 Sécurité du système d'exploitation

4.3.2.1 Démarrage fiable

Le périphérique utilise le SoC/CPU comme « racine de confiance physique » pour un démarrage sécurisé. Pendant le processus de démarrage du système, la confiance est vérifiée étape par étape pour réaliser le transfert sécurisé du contrôle jusqu'au démarrage du service d'application final. En établissant une chaîne de démarrage fiable complète pour construire l'état de confiance initial de l'appareil, cela permet une garantie de base fiable pour le fonctionnement ultérieur de l'appareil.

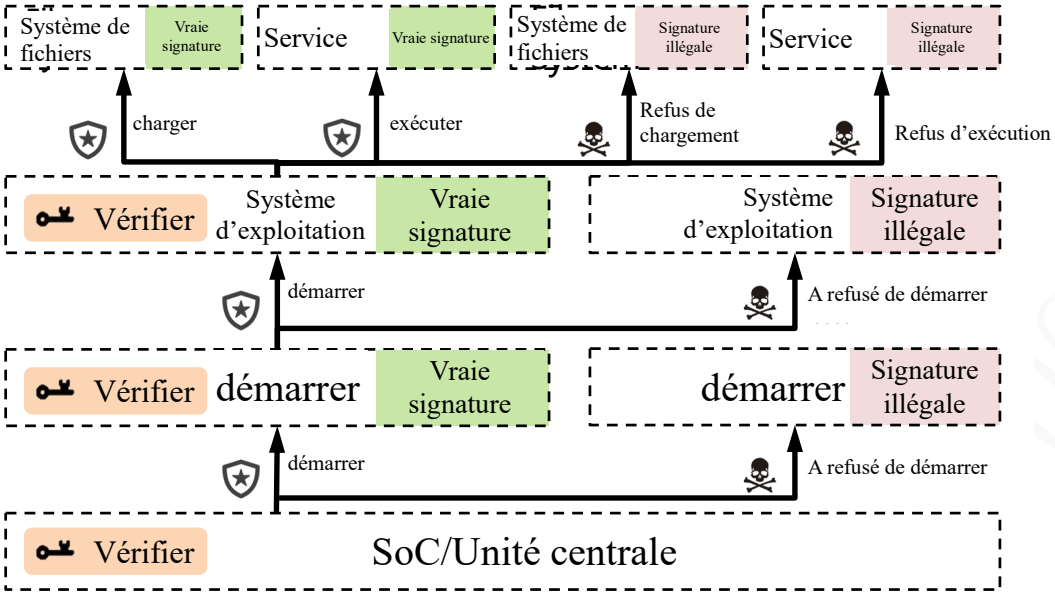

Figure 4-5 Principe de Démarrage fiable

4.3.2.2 Exécution fiable

Pendant le fonctionnement du périphérique, avant qu'un programme exécutable ne soit chargé et exécuté, il doit passer la vérification de confiance du noyau pour empêcher les programmes malveillants (tels que les virus, chevaux de Troie, etc.) d'envahir l'appareil.

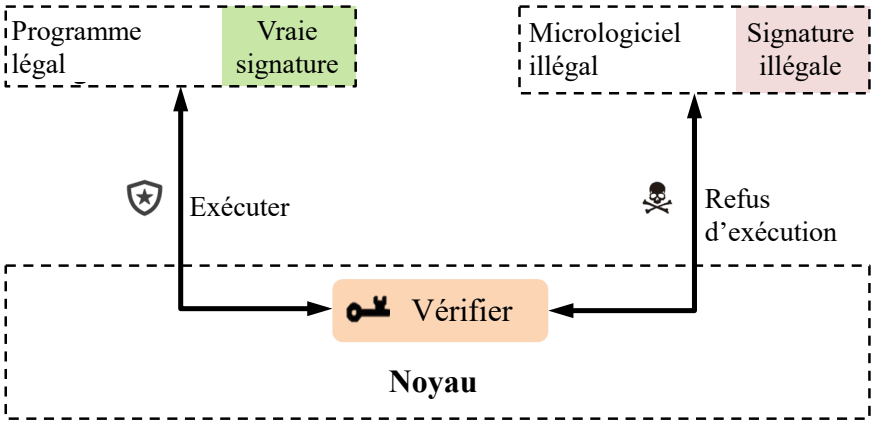

Figure 4-6 Principe d'exécution fiable

4.3.2.3 Mise à niveau fiable

Lorsque l'appareil effectue une mise à niveau du micrologiciel, le service de mise à niveau effectuera une vérification de confiance sur le micrologiciel cible et refusera d'écrire un micrologiciel illégal ou falsifié sur l'appareil.

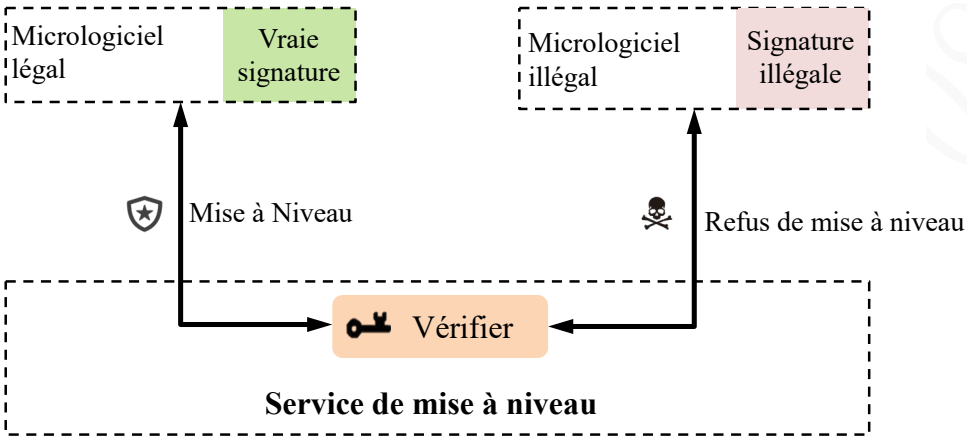

Figure 4-7 Vérification sécurisée de la mise à niveau du micrologiciel

4.3.2.4 Protected Shell

Shell est le terminal de contrôle de commande de l'appareil et est généralement utilisé pour le débogage, la détection et la localisation des problèmes. Protected Shell est une protection d'authentification multifacteur basée sur la technologie Hook pour empêcher des opérations malveillantes d'endommager l'appareil.

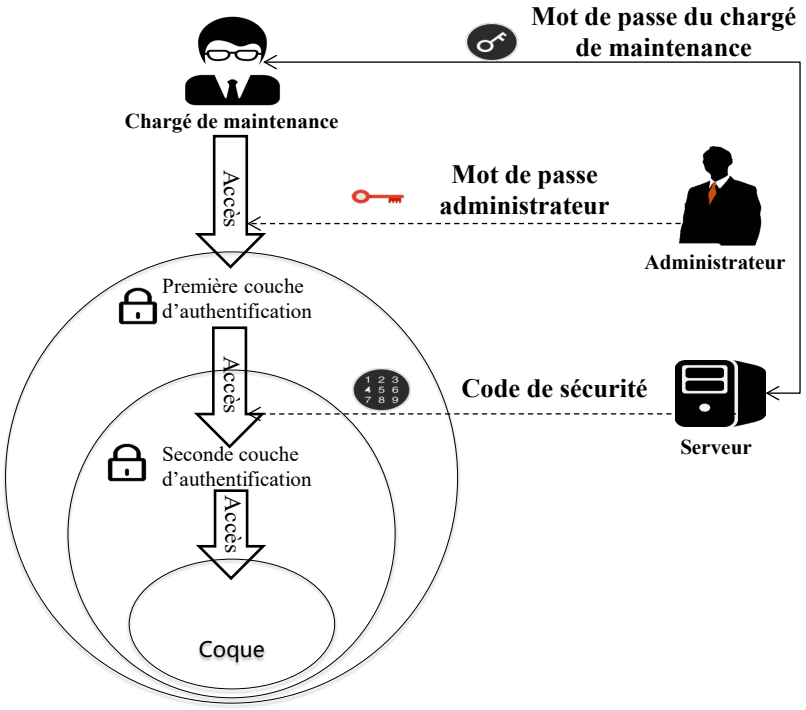

Figure 4-8 Principe du Protected Shell

L'authentification multifacteur comprend deux niveaux d'autorisation :

- Autorisation administrateur : basée sur le système de gestion des utilisateurs de l'appareil, l'administrateur est authentifié pour obtenir l'autorisation de premier niveau de l'appareil.
- Autorisation serveur : utilisation des informations d'identification du personnel de maintenance pour obtenir le code de sécurité du serveur d'authentification assurant l'autorisation de deuxième niveau.

4.3.2.5 Mise à niveau par cloud

Dans l'industrie de l'IdO, la mise à niveau des appareils a été un grand défi en raison du grand nombre d'appareils, de la complexité du réseau et des emplacements dispersés d'installation. Une mise à niveau avec le dernier micrologiciel permet non seulement aux utilisateurs de profiter des dernières fonctionnalités, mais aide également l'appareil à améliorer ses capacités de sécurité. Dahua a proposé une solution de mise à niveau à partir du cloud pour permettre aux utilisateurs de mettre à niveau l'appareil de manière pratique et sécurisée :

- Prend en charge la détection automatique de version
- Prend en charge les mises à niveau automatisées par lots

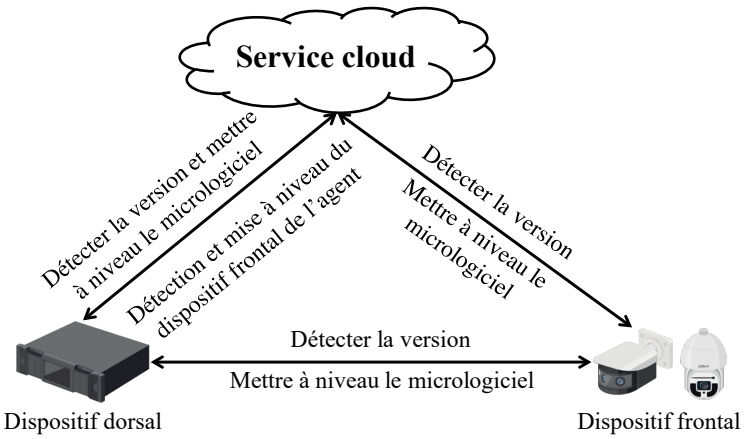

Figure 4-9 Diagramme de mise à niveau par le cloud

4.3.2.6 Anti-inversion

Le micrologiciel est l'un des atouts importants de l'appareil. Afin de prévenir les attaques inversées par des pirates informatiques, Dahua a conçu un schéma de cryptage du micrologiciel pour garantir que celui-ci reste chiffré pendant le processus de transfert de données. Le principe de base est le suivant :

- Création d'une clé de sécurité basée sur la technologie KDF et cryptage des données du micrologiciel ;
- Lorsque l'appareil effectue une mise à niveau du micrologiciel, écriture du micrologiciel dans la Flash sous forme cryptée ;
- Pendant le processus de démarrage de l'appareil, les données de la partition Flash sont déchiffrées et chargées.

4.3.3 Sécurité des applications

4.3.3.1 Technologie d'authentification de sécurité

4.3.3.1.1 Politique de sécurité des utilisateurs

L'appareil n'a pas de compte par défaut avant de quitter l'usine et celui-ci doit être créé par l'utilisateur lors du déploiement. La composition du mot de passe doit répondre aux exigences suivantes :

- Il doit avoir au moins 8 caractères ;
- Il doit contenir pas moins de deux types de caractères.

Pour guider l'utilisateur dans la définition d'un mot de passe fort, l'appareil vérifie la force du mot de passe défini par l'utilisateur et invite l'utilisateur lors de l'ajout d'un compte ou de la modification d'un mot de passe.

4.3.3.1.2 Authentification Digest

La technologie d'authentification Digest est une méthode d'authentification complexe basée sur l'algorithme HASH sur les mots de passe et les nombres aléatoires (valable une fois) pour garantir la confidentialité et la non-répétabilité du processus d'authentification.

L'algorithme HASH est le suivant :

- HA1 = HASH (« nom d'utilisateur:portée:mot de passe »)
- HA2 = HASH (« méthode:uri »)
- DigestPassword = HASH (« HA1:nouce:nc:cnonce:qop:HA2 »)

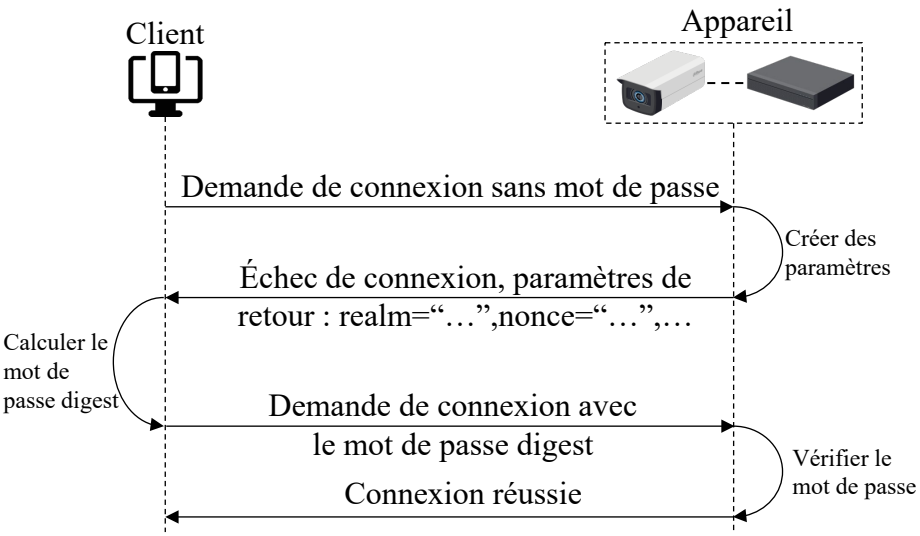

Figure 4-10 Technologie d'authentification Digest

4.3.3.1.3 Authentification WSSE

La technologie d'authentification WSSE est basée sur l'algorithme HASH du mot de passe, du nombre aléatoire, de l'heure et d'autres facteurs pour garantir la confidentialité du processus de transmission du mot de passe. En se basant sur le facteur de nombre aléatoire non répétitif dans un temps limité, le processus d'authentification de non-répétabilité est garanti.

L'algorithme WSSE est le suivant :

- HA1 = HASH (« nom d'utilisateur:portée:mot de passe »)
- HA2 = HASH (« méthode:uri »)
- HA3 = HASH (« HA1:nouce:nc:cnonce:qop:HA2 »)
- WSSEPassword = Base64 (HASH (Nonce + CreationTimestamp + HA3))

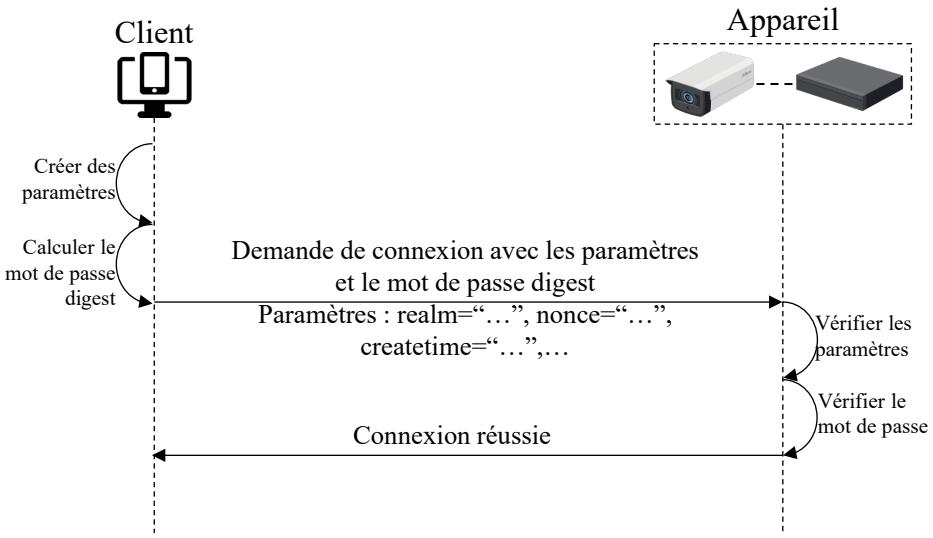

Figure 4-11 Technologie d'authentification WSSE

4.3.3.2 Système de gestion des autorités

Basé sur le modèle RBAC, l'appareil Dahua dispose d'un système de gestion et de contrôle d'autorité à la fois flexible et efficace pour répondre aux besoins des utilisateurs déployant des appareils dans différents scénarios.

4.3.3.3 Politique de sécurité des journaux

4.3.3.3.1 Enregistrement des spécifications des journaux

L'appareil enregistre entièrement la piste des opérations de l'utilisateur, y compris (mais sans s'y limiter) les opérations suivantes :

- Connexion au compte et déconnexion
- Ajout, suppression, modification du compte utilisateur et du mot de passe
- Importation ou exportation des configurations système
- Modification de la configuration du système
- Téléchargement de fichiers
- Redémarrage et mise à niveau l'appareil
- Modification de l'heure du système
- Événements anormaux (y compris déconnexion du réseau, absence de disque dur, erreur de disque dur, faible capacité du disque dur ou perte vidéo, etc.)
- Événements de sécurité (tels que le verrouillage du compte, l'explosion de session, etc.)

Le contenu du journal enregistré par l'appareil contient les facteurs importants suivants :

- Source opérationnelle, y compris le compte et l'adresse IP source
- Contenu opérationnel
- Temps opérationnel
- Résultat opérationnel

4.3.3.3.2 Journaux de sécurité séparés

En fonction de la sensibilité des événements de sécurité, et afin de garantir davantage la traçabilité de ces événements, la zone de stockage du journal de sécurité est divisée pour être indépendante. Bien qu'ils n'affectent pas les enregistrements du journal des opérations commerciales, les enregistrements du journal des événements de sécurité sont prioritaires.

4.3.3.3.3 Journal réseau

L'appareil Dahua prend en charge le protocole syslog, qui peut enregistrer simultanément des journaux importants sur un serveur de journaux.

4.3.3.4 Politique sur la sécurité des composants

Dahua a établi un processus de contrôle pour les composants tiers et open-source. Constituant une part importante du Cycle de vie de développement de logiciels sécurisés (sSDLC), il a été intégré au système de contrôle de la qualité des produits. La gestion des composants tiers et open-source du produit inclut principalement les points suivants :

- Les composants doivent être couronnés de succès lors de l'évaluation et de l'audit de sécurité, notamment de l'audit de conformité open-source, de la détection des vulnérabilités, de l'évaluation des risques, etc.
- Une fois le produit sorti, utilisez régulièrement la toute dernière bibliothèque de vulnérabilités pour détecter l'état de la vulnérabilité des composants et identifier l'étendue des produits affectés afin de veiller à ce que les vulnérabilités soient corrigées dans les meilleurs délais.

4.3.3.5 Politique sur la sécurité des services

S'appuyant sur le principe de la minimisation, Dahua a mis en œuvre des dispositions rigoureuses de gestion et de contrôle pour tous les services de l'équipement. Par défaut, seuls les services de base sont autorisés, notamment :

- Le service WEB
- Le service RTSP
- Le service de recherche d'appareils

- …

L’équipement prend en charge d’autres protocoles de services sécurisés et dote les utilisateurs d’autres options sécurisées pour les mêmes fonctions, notamment :

- La prise en charge du protocole HTTPS pour remplacer le protocole HTTP
- La prise en charge du protocole SFTP pour remplacer le protocole FTP
- La prise en charge du protocole SNMP v3 pour remplacer le protocole SNMP v1/v2
- La prise en charge du protocole SSH pour remplacer le protocole Telnet
- …

4.3.3.6 Politique sur la sécurité des sessions

Les services web prennent en charge l’interaction de session reposant sur une brève connexion, et les stratégies de protection sont comme suit :

- utilisation d’identifiants de session aléatoires, forts et très complexes ;
- la session valide est solidement associée à l’hôte source, et le partage d’identifiants de session entre hôtes est interdit ;
- surveillance en temps réel du piratage par force brute des identifiants de session, et déconnexion active de tous les utilisateurs en ligne d’hôtes à risque ;
- fermeture automatique des sessions inactives pendant longtemps.

4.3.4 Sécurité des données

4.3.4.1 Technologie de signature numérique

S’appuyant sur l’infrastructure PKI et sur un algorithme de signature, cette technologie met en œuvre des fonctions de signature et de vérification des données pour garantir l’intégrité des données cibles.

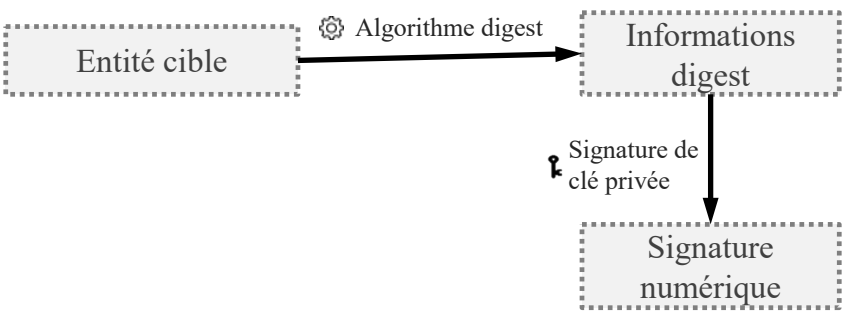

Figure 4-12 Processus de signature numérique

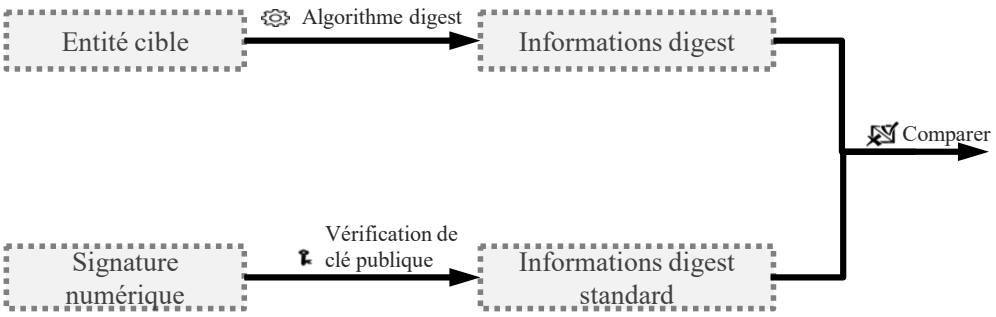

Figure 4-13 Processus de vérification numérique

4.3.4.2 Technologie d'enveloppe numérique

La technologie d'enveloppe numérique est similaire à des courriers classiques. S'appuyer sur cette technologie peut garantir que seul le destinataire prévu pourra déchiffrer et lire les données transmises sur le réseau.

- Le client utilise une clé symétrique générée aléatoirement pour chiffrer les données cibles puis chiffre la clé symétrique générée en se basant sur la clé publique fournie par l'équipement ;
- Lorsque l'équipement reçoit les données chiffrées et la clé symétrique, il utilise la clé privée correspondante pour commencer par déchiffrer la clé symétrique, puis il utilise la clé symétrique pour déchiffrer les données en texte chiffré.

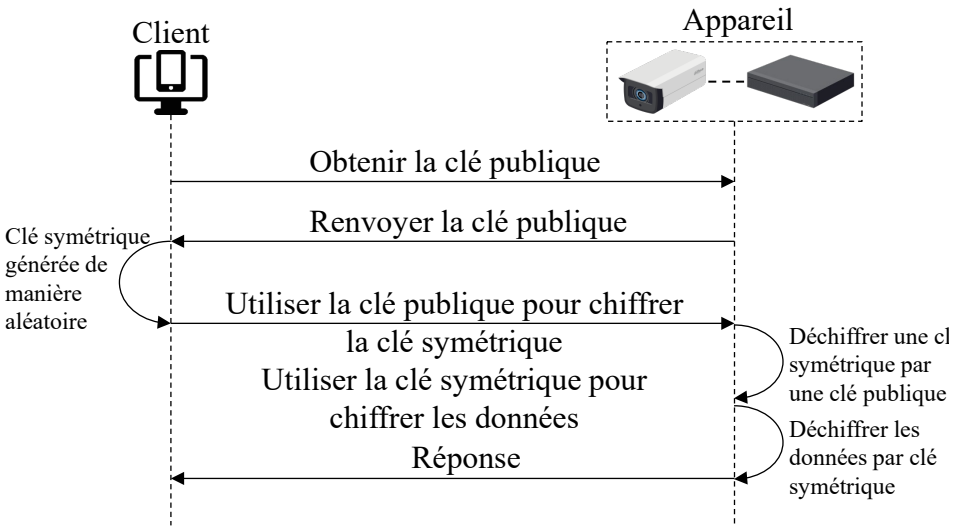

Figure 4-14 Technologie d'enveloppe numérique

4.3.4.3 Transmission chiffrée de la vidéo

4.3.4.3.1 Technologie de chiffrement des données d'images

La technologie de chiffrement des données d'images, c'est-à-dire, le chiffrement et la protection reposant sur les données des images de diffusion multimédia, prend actuellement en charge l'algorithme de chiffrement AES256-OFB. Le protocole privé de Dahua, RTSP, utilise cette technologie. Le processus spécifique est le suivant :

- l'équipement génère une clé aléatoire et chiffre les données d'images ;
- la technologie d'enveloppe numérique est utilisée pour synchroniser et mettre à jour la clé entre l'équipement et le client ;
- le client déchiffre les données d'images en se basant sur la clé synchronisée.

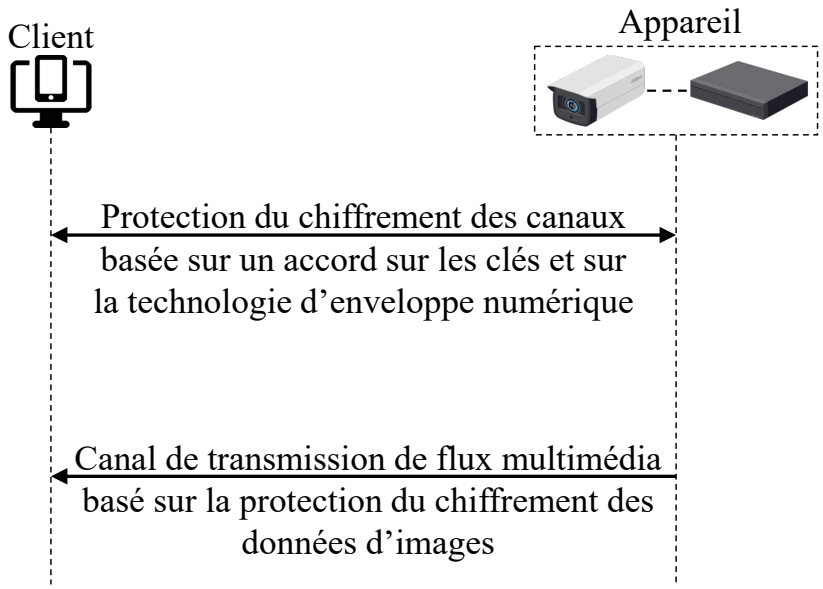

Figure 4-15 Flux interactif de la technologie de chiffrement des images

4.3.4.3.2 Technologie de chiffrement des canaux

Le protocole RTSP de Dahua prend en charge la transmission de diffusion multimédia reposant sur une protection par chiffrement TLS des canaux. Les protocoles RTSP et TLS sont tous deux mis en œuvre via des protocoles standard,. Ils prennent en charge la connexion de clients tiers lors de leur mise en œuvre standard. Le processus spécifique est le suivant :

- le client et l'équipement établissent un tunnel de chiffrement de confiance reposant sur le protocole TLS ;
- transmission de flux multimédia basée sur le canal TLS.

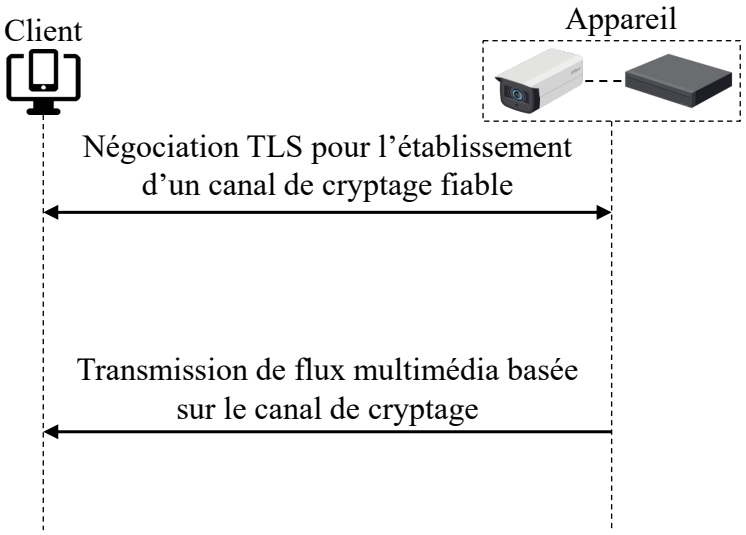

Figure 4-16 Technologie de chiffrement des canaux

4.3.4.4 Stockage chiffré des vidéos

4.3.4.4.1 Stockage chiffré reposant sur KMS

KMS est un serveur professionnel de gestion des clés qui permet aux équipements du réseau qui effectuent une gestion unifiée des clés de garantir la stabilité et la sécurité des clés. Le processus spécifique est le suivant :

- utilisation de clés générées aléatoirement pour chiffrer les données vidéo, et prise en charge de l'algorithme de chiffrement AES256 ;
- connexion au système KMS pour protéger la clé aléatoire en utilisant des protocoles standard de l'industrie, KMIP et HTTPS, pour se connecter au système KMS ;
- prise en charge de la mise à jour régulière des clés.

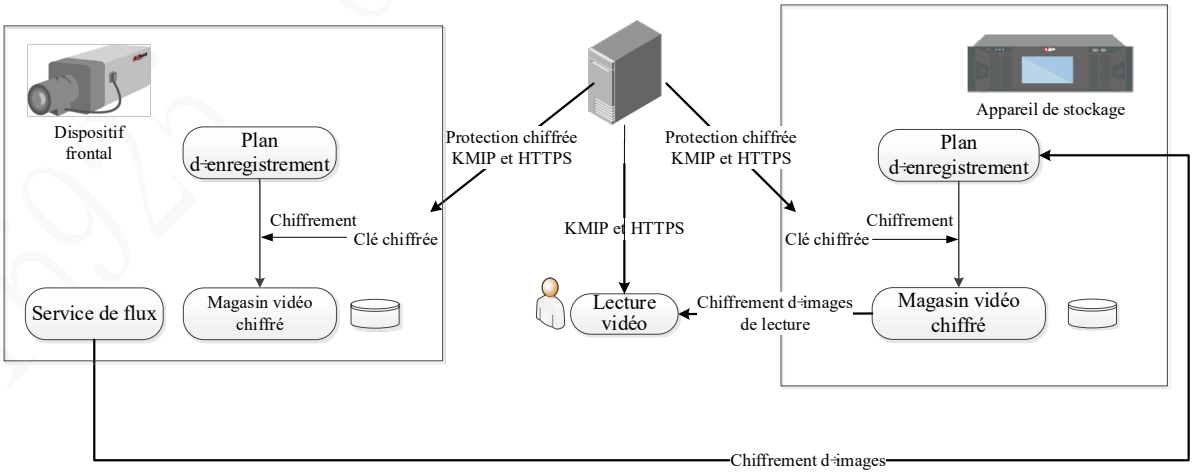

Figure 4-17 Protection par chiffrement des vidéos reposant sur KMS

4.3.4.4.2 Stockage chiffré reposant sur la dérivation de mots de passe

Pour simplifier le déploiement de la gestion des clés utilisateur, l'équipement Dahua met en œuvre un stockage chiffré des données vidéo reposant sur des mots de passe définis par l'utilisateur. Le principe de base est le suivant :

- utilisation de clés générées aléatoirement pour chiffrer les données vidéo, et prise en charge de l'algorithme de chiffrement AES256 ;
- utilisation de la technologie KDF pour déduire une clé du mot de passe configuré par l'utilisateur, puis chiffrer et protéger la clé des vidéos.

4.3.4.5 Téléchargement chiffré des vidéos

L'équipement prend en charge une fonction de téléchargement de vidéos. Pour garantir la sécurité des données vidéo des dispositifs de stockage portables, l'équipement prend également en charge une fonction de téléchargement chiffré assurant la confidentialité du processus de transmission de données vidéo du dispositif de stockage portable. Le principe de base est le suivant :

- exploitation du mot de passe de chiffrement du téléchargement de vidéos pour exécuter la dérivation de clé KDF et l'obtenir ;
- utilisez la clé pour chiffrer la vidéo cible et la télécharger sur le client.

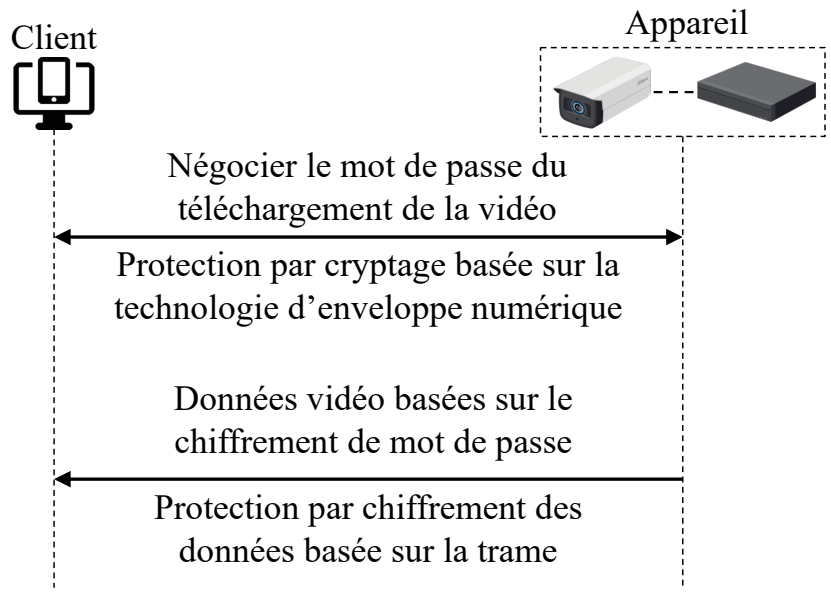

Figure 4-18 Principe du téléchargement chiffré des vidéos

4.3.4.6 Stockage chiffré des configurations

S'appuyant sur les différentes capacités de l'équipement, la fonction de stockage chiffré configurée utilise différents algorithmes de chiffrement, notamment :

- si l'équipement prend en charge la puce de sécurité, utilisation de la puce de sécurité pour le stockage chiffré ;
- si l'équipement ne prend pas en charge la puce de sécurité, une clé est générée en se basant sur la technologie KDF, et les données sont chiffrées en utilisant la clé.

4.3.4.7 Exportation chiffrée des configurations

La fonction d'exportation des configurations est principalement utilisée pour la sauvegarde et la synchronisation des données de configuration de l'équipement. Le fichier de configuration exporté peut contenir des renseignements sensibles telles que des informations sur les comptes et des mots de passe. Pour préserver la confidentialité et l'intégrité des données de configuration, l'équipement Dahua crée une clé de sécurité reposant sur la technologie KDF et chiffre entièrement les données de configuration exportées.

4.3.5 Sécurité réseau

4.3.5.1 Protection contre les attaques

4.3.5.1.1 Technologie anti-usurpation ARP

L'usurpation ARP fait référence à l'envoi continu de paquets d'usurpation ARP pour implanter des mappages IP-MAC usurpés sur les équipements ou hôtes réseau, ce qui permet d'intercepter les données envoyées à l'hôte cible. Mappage IP-MAC usurpé fait référence à la relation de mappage constituée de l'IP de l'hôte cible de l'attaque et de l'adresse MAC de l'hôte de l'auteur de l'attaque

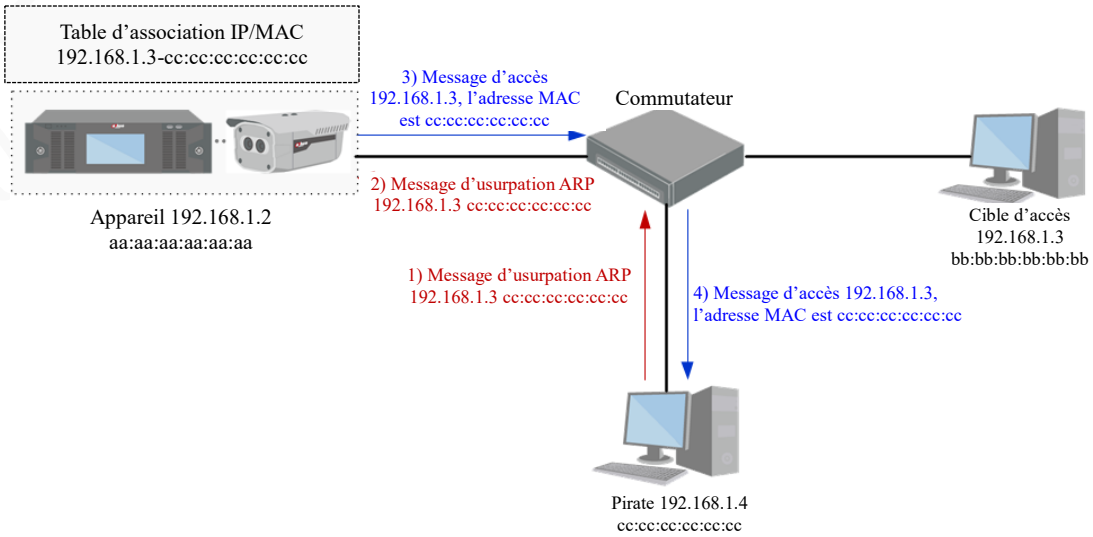

Figure 4-19 Technologie d'usurpation ARP

La technologie anti-usurpation ARP est utilisée pour renforcer la liste de mappages IP-MAC de l'hôte source, bloquer les messages d'usurpation ARP et empêcher l'implantation de relations de mappage IP-MAC usurpées

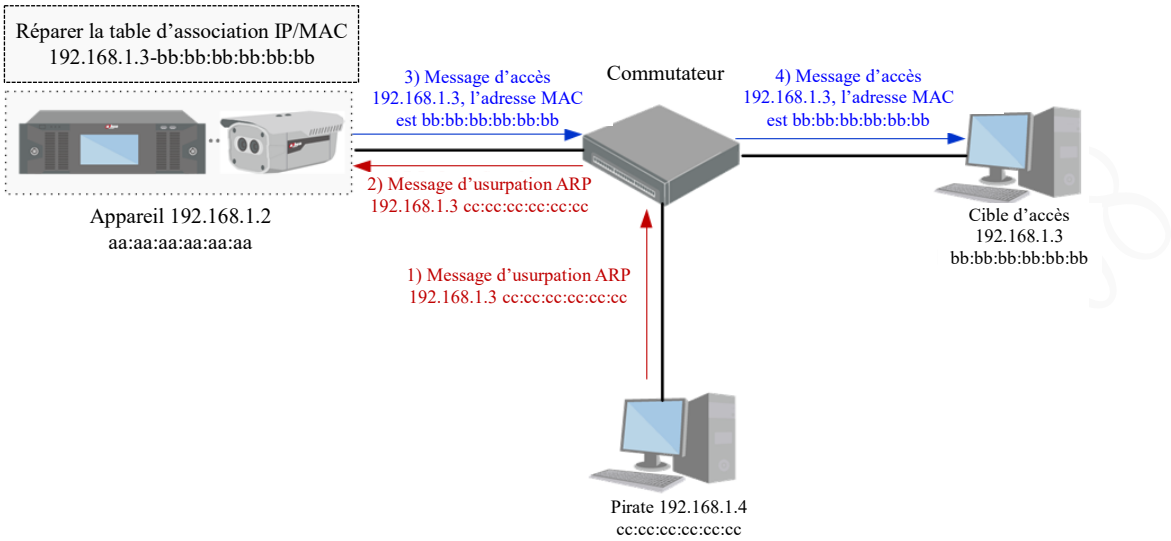

Figure 4-20 Technologie anti-usurpation ARP

4.3.5.1.2 Technologie anti-attaques par déni de service

Dans le cadre d'une attaque par déni de service, l'auteur de l'attaque épuise les ressources de service de l'hôte cible en envoyant des paquets réseau malveillants afin que l'hôte cible ne puisse pas fournir de services normaux aux utilisateurs légitimes. L'équipement Dahua offre des technologies de défense contre les attaques par déni de service suivantes :

- l'ICMP Flood, qui consiste en l'envoi d'un grand nombre de paquets de messages ICMP à l'équipement afin qu'il ne puisse plus répondre aux requêtes de service légitimes ;
- le Syn Flood, qui consiste en une attaque par semi-connexion TCP. En envoyant continuellement de fausses requêtes de connexion TCP, l'auteur de l'attaque pousse l'équipement à établir un grand nombre de ressources de semi-connexion TCP, épuisant ainsi la pile du protocole TCP pour mettre en œuvre les attaques par déni de service.

4.3.5.1.3 Technologie anti-piratage de mots de passe

Attaque de piratage de mot de passe fait référence à l'utilisation d'un hôte hautes performances pour effectuer des tentatives d'entrée de mots de passe très fréquentes sur la cible jusqu'à ce que l'équipement soit connecté avec succès, l'objectif étant d'obtenir le bon mot de passe de connexion de l'équipement.

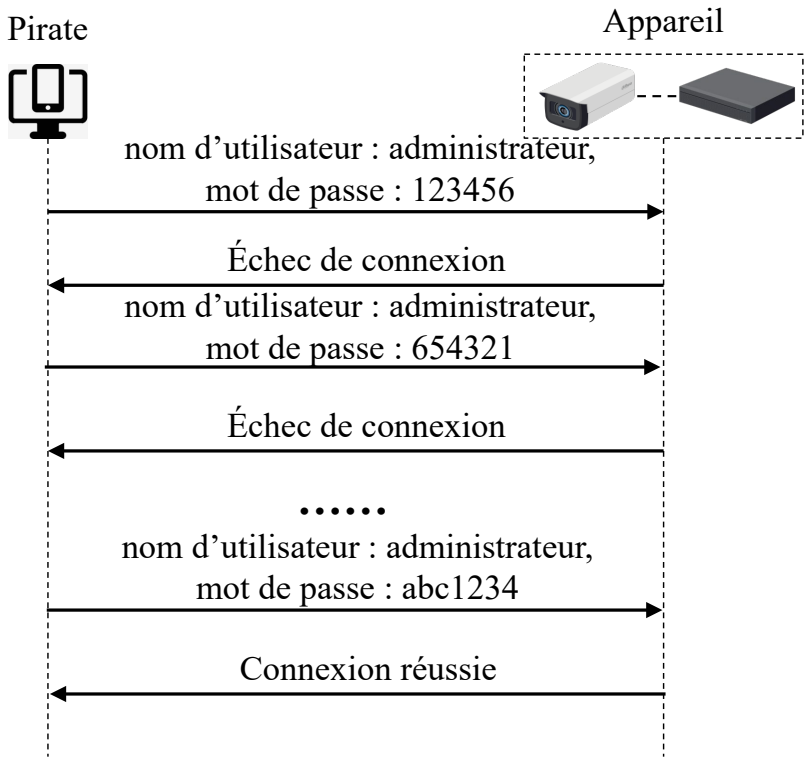

Figure 4-21 Technologie de piratage de mots de passe

L'équipement se base sur les caractéristiques de l'attaque ci-dessus et verrouillera automatiquement le compte et le comportement de connexion de l'hôte pendant une certaine période lorsqu'il reconnaîtra cette attaque de piratage de mot de passe.

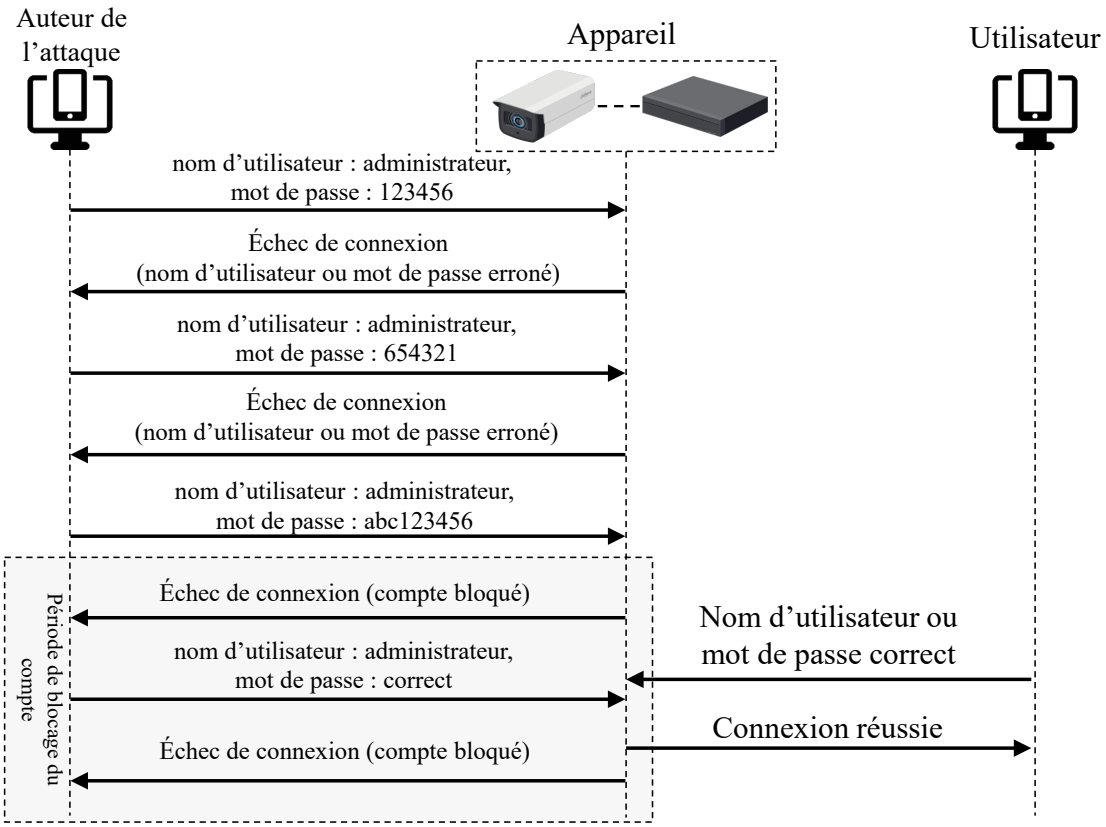

Figure 4-22 Technologie anti-piratage de mots de passe

4.3.5.2 Contrôle d’accès

4.3.5.2.1 Pare-feu

Le pare-feu est mis en œuvre en se basant sur une technologie de filtrage des paquets réseau. S’appuyant sur des règles de filtrage préconfigurées, il vérifie les caractéristiques des paquets réseau reçus ou envoyés et décide s’il faut les laisser passer, réduisant ainsi le risque réseau. Ses informations sur les caractéristiques des paquets de données réseau incluent principalement ce qui suit :

- Adresse IP de l’hôte source
- Adresse IP de l’hôte de destination
- Adresse MAC de l’hôte source
- Adresse MAC de l’hôte de destination
- Port de l’hôte source
- Port de l’hôte de destination
- Protocole Réseau

4.3.5.2.2 Liste blanche d’étalonnage de l’heure

L’heure est l’une des ressources importantes de l’équipement et sa précision affecte de nombreuses fonctions importantes, notamment la journalisation, l’horodatage des enregistrements, etc. L’équipement Dahua prend en charge une fonction de liste blanche d’étalonnage de l’heure. Conformément aux règles préconfigurées, seuls les hôtes spécifiés sont autorisés à étalonner l’heure du dispositif, ce qui évite les sabotages malveillants de l’heure.

4.3.5.2.3 802.1x

Le protocole 802.1x est un protocole standard pour le contrôle d’accès réseau. Il peut appliquer des restrictions aux équipements et hôtes non autorisés, les empêchant ainsi d’accéder au réseau privé. Le principe de base est le suivant :

- dans l’état initial du port réseau physique du commutateur réseau, seuls les messages d’authentification 802.1x sont autorisés à communiquer ;
- l’équipement ou l’hôte connecté au commutateur déclenche l’authentification d’identité par le biais du protocole 802.1x ;
- après vérification du service d’authentification, le commutateur réseau ouvre la communication de ses données d’entreprise.

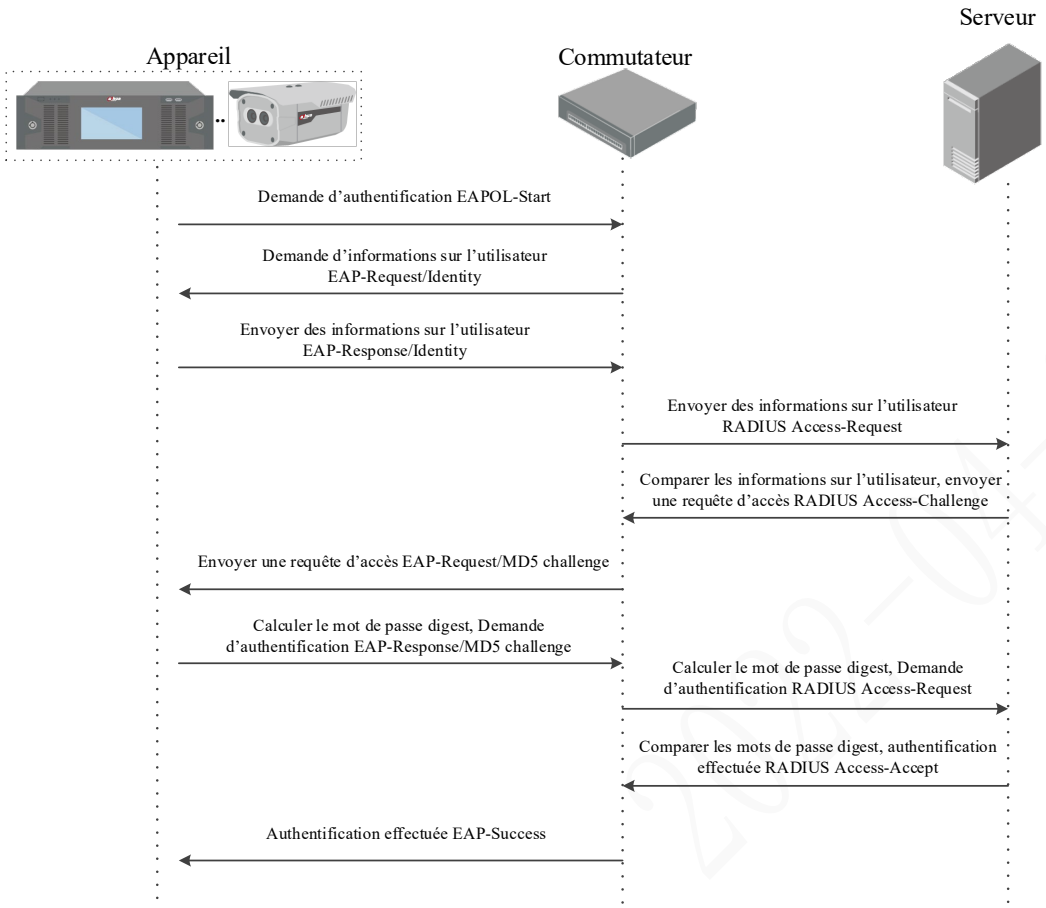

Figure 4-23 Processus d'authentification 802.1x

4.3.5.3 Alarme de sécurité

L'équipement surveille les comportements d'attaque anormaux en temps réel, informe les utilisateurs par email, notification push mobile, bip, etc. et déclenche l'alarme de sécurité en temps réel. La surveillance d'événements d'attaque prise en charge inclut principalement :

- Les accès IP interdits
- Les tentatives de connexion à une heure interdite
- Le piratage de noms d'utilisateur et de mots de passe
- Le piratage de sessions
- Le piratage de chemins web
- Le nombre de connexions de session dépassant la limite
- Les tentatives d'exécution interdite de programmes

4.3.5.4 Certificat CA

L'équipement prend en charge les certificats numériques à la norme x.509, l'importation de certificats numériques délivrés par une autorité tierce de certification et la génération de requêtes de signature de certificat au format PKCS#10. Vous pouvez demander un certificat numérique auprès d'une autorité tierce de certification puis l'importer.

4.3.5.5 Sécurité sans fil

Dahua prend en charge les méthodes d'authentification avec chiffrement WPA/WPA2 basées sur l'authentification Radius, et également les méthodes d'authentification avec chiffrement WPA-PSK/WPA2-PSK.

4.3.6 Protection de la confidentialité

Avec le développement continu et approfondi de l'AIoT, la sécurité des données et la protection de la confidentialité est une priorité absolue pour les pays du monde entier. Depuis la promulgation de la « Loi relative à la sécurité des réseaux » de Chine, du « Règlement sur la sécurité des renseignements personnels-Technologie de sécurité de l'information GB/T 35273-2017 », du « RGPD UE », et de la « Loi sur la protection des renseignements personnels des consommateurs résidant en Californie (CCPA) », Dahua a toujours adopté une attitude et une politique proactives et pragmatiques pour réagir, et a mis en place le Comité spécial sur la sécurité des données et la protection de la vie privée en prêtant une attention particulière aux lois et réglementations mondiales, effectue des vérifications de conformité exhaustives, et encourage activement la rectification de la conformité et la certification. Afin d'améliorer globalement le niveau de protection de confidentialité des produits et services, et mieux aider les clients à se conformer, Dahua a énoncé les « Normes de protection des données personnelles et de la confidentialité Dahua » en combinaison avec les principes de conception de sécurité interne, les spécifications sur la sécurité des renseignements personnels, les réglementations RGPD et les normes TÜV Rheinland, et a introduit un référentiel de confidentialité à l'étape de la demande et de la conception du produit, à partir de la politique de confidentialité, des paramètres respectueux de la vie privée, de la collecte de données, de la transmission de données, du stockage de données, de la suppression de données et d'autres aspects pour la spécification et l'orientation générales du traitement des données. Les produits Dahua respectent scrupuleusement les exigences de base de la minimisation des données et des paramètres respectueux de la vie privée, et intègrent en permanence les technologies et les applications de protection de la vie privée telles que le masquage des données, le cryptage des données, l'occlusion de visage, l'informatique de confiance, etc.

Grâce à la technologie de reconnaissance intelligente, il localise et bloque dynamiquement (en prenant en charge les visages et les corps humains) afin de renforcer les capacités de la protection de la confidentialité.

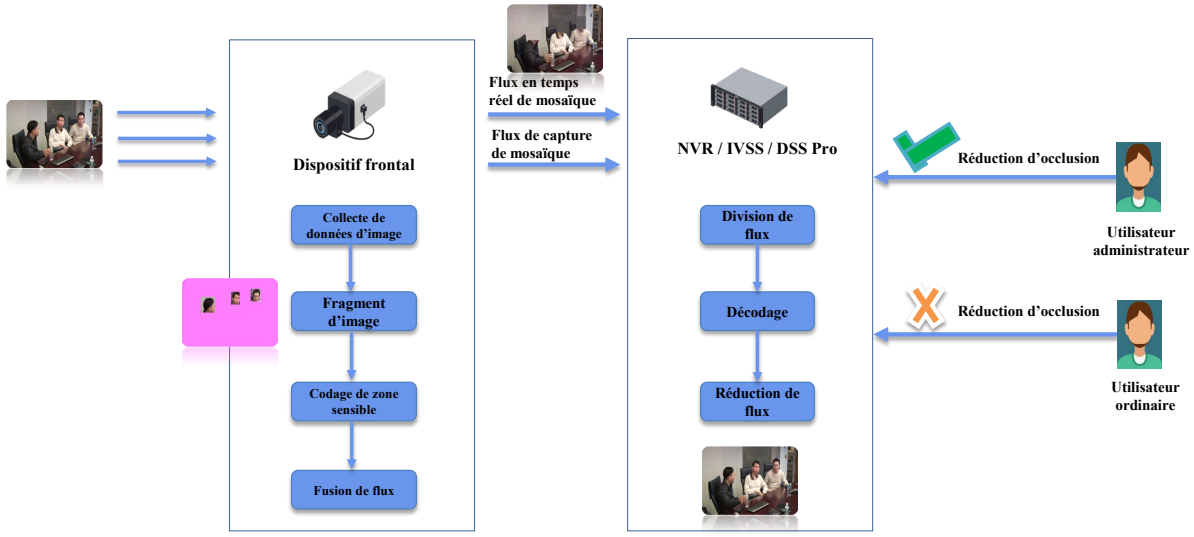

Figure 4-24 Technologie d'occlusion de visage

En fonction de la technologie intelligente de reconnaissance faciale, les parties du visage dans l'image collectée sont identifiées lors de l'étape d'encodage des images, et un détourage intelligent est réalisé pour masquer les données personnelles de confidentialité dans l'image. Seuls les utilisateurs disposant de droits d'administrateur peuvent restaurer l'image originale, les utilisateurs ordinaires ne peuvent pas la restaurer.

5 Centre de sécurité

5.1 Présentation

L'objectif principal du centre de sécurité est d'intégrer en profondeur la protection de la sécurité et les scénarios commerciaux, d'aider les utilisateurs à comprendre clairement l'état et les capacités de sécurité de l'appareil, et de permettre aux utilisateurs de définir facilement et aisément la meilleure configuration de sécurité adaptée au scénario.

Sur la base de l'inspection et de l'analyse de l'état du compte courant, de la configuration fonctionnelle, du module de sécurité et d'autres caractéristiques de l'appareil, il présente de façon exhaustive les vulnérabilités de l'appareil à l'utilisateur. Au même moment, l'appareil offre des capacités de gestion centralisées des fonctions de sécurité, qui se complètent l'une l'autre pour mieux aider les utilisateurs à comprendre et à renforcer l'appareil.

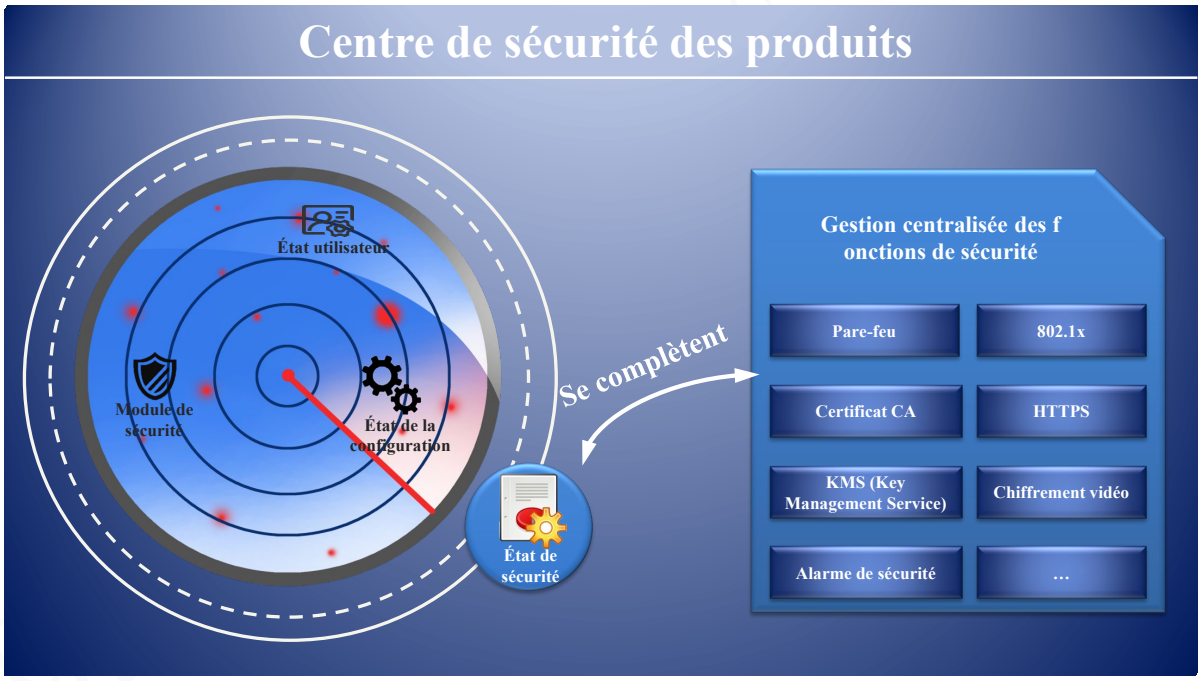

Figure 5-1 Centre de sécurité

5.2 Analyse de sécurité

Le module d'analyse de sécurité intégré dans l'appareil peut analyser de manière exhaustive l'état du compte, l'état de la configuration de la fonction, l'état de journalisation et la capacité du module de sécurité de l'appareil en fonction de l'état de fonctionnement actuel de l'appareil, afin d'aider les utilisateurs à comprendre l'état de sécurité de la configuration de l'appareil et les capacités de sécurité prises en charge par l'appareil. Les utilisateurs peuvent optimiser et améliorer la sécurité des appareils en fonction des résultats d'analyse et des exigences des scénarios commerciaux.

5.3 Gestion centralisée de la configuration de la sécurité

Toutes les fonctions de sécurité configurables de l'appareil ont été chargées dans la page de configuration du centre de sécurité pour créer un centre de gestion centralisée de la sécurité de l'appareil. Au même moment, une liaison efficace est formée entre les modules de sécurité, ceci pour aider les utilisateurs à mieux appliquer les fonctions de sécurité des appareils.

6 Conformité aux normes de sécurité

6.1 Certification UL CAP (UL 2900)

La certification UL CAP est le premier et unique programme d'évaluation de la sécurité au monde fondé sur des normes pour les appareils et les systèmes IoT, dont l'objectif principal porte sur les vulnérabilités et les faiblesses des logiciels, et la mise en œuvre adéquate des contrôles de sécurité. Les critères techniques dans la certification UL 2900 reposent sur les meilleures pratiques existantes de l'industrie et les documents d'orientation ainsi que sur les normes CEI, ISO et autres normes internationales. L'évaluation de CAP comprend l'examen de la documentation, l'analyse du code source, les tests de vulnérabilité connus, l'analyse des logiciels malveillants et des virus, les tests à données aléatoires et les tests de pénétration, etc., pour examiner de manière approfondie les performances de sécurité du produit.

Dahua a obtenu la certification de sécurité UL CAP en octobre 2019, et le numéro du certificat est ULCAP_133.

Tous les produits de Dahua doivent passer avec succès l'analyse de code unifiée et stricte, les tests de vulnérabilité, l'analyse des logiciels malveillants et des virus, les tests à données aléatoires, les tests de pénétration et d'autres évaluations de sécurité avant d'être mis sur le marché.

Adresse de demande d'informations sur les certificats : https://iq.ulprospector.com/en

6.2 Certification des produits IoT pour la protection de la confidentialité TÜV Rheinland

La promulgation du RGPD, la réglementation la « plus stricte » de l'histoire en matière de protection des données, a établi des normes de protection strictes, de haut niveau et de grande portée en matière de sécurité des données et de protection de la vie privée.

Sur la base du RGPD UE, des Mécanismes cryptographiques TR-02102 selon les référentiels techniques de BSI et de la Norme interne 2PfG, TÜV Rheinland assure l'audit de documents, la protection des données personnelles, le traitement des données confidentielles, les tests de pénétration, les inspections dans les usines et d'autres services complets d'essai et d'évaluation de l'IPC, du NVR, de la Plateforme DSS, de l'IVS et autres produits de Dahua.

La série des produits Dahua a obtenu la Certification de protection de la confidentialité des produits IoT, Produit IoT de confidentialité protégée TÜV Rheinland en 2018, dont les numéros des certificats sont :

- IPC (Caméra IP) Q 50437998
- NVR (Enregistreur vidéo réseau) Q 50437996
- Plateforme DSS (Plateforme de système de surveillance numérique) Q 50459589
- IVS (Serveur de vidéosurveillance intelligent) Q 50433648

Dahua a réussi l'évaluation et obtenu la certification de protection de la confidentialité des produits IoT, ce qui signifie que les produits de Dahua se conforment davantage aux exigences du RGPD et servent de point de référence pour l'industrie en matière de cybersécurité et de protection de la confidentialité.

En s'inspirant des principes internes de conception de la sécurité, des spécifications en matière de sécurité des renseignements personnels, de la Loi relative au RGPD et des normes TÜV Rheinland, Dahua a énoncé les « Normes de protection des données personnelles et de la confidentialité Dahua », a introduit un référentiel de confidentialité dans les exigences du produit et l'étape de la conception, et qui a été rigoureusement appliqué dans toute la série de produits.

Adresse de demande d'informations sur les certificats : https://www.certipedia.com/quality_marks

6.3 Certification des services IoT pour la protection de la confidentialité TÜV Rheinland

Sur la base du RGPD UE, des Mécanismes cryptographiques TR-02102 selon C5 et les référentiels techniques de BSI et de la Norme interne 2PfG, TÜV Rheinland fournit des services d'évaluation complets tels que la sécurité physique, la sécurité des données, la sécurité des applications, la cybersécurité et la sécurité des applications, le processus de développement de la sécurité, et le processus d'urgence de sécurité pour la couche Iaas / PaaS / SaaS du Cloud Imou de Dahua, et réalise des tests de pénétration.

Dahua a obtenu la Certification des services IoT pour la protection de la confidentialité TÜV Rheinland en décembre 2019 portant le numéro de certificat 50458168.

Dahua a réussi l'évaluation et obtenu la certification de protection de la confidentialité des services IoT, ce qui signifie que les capacités de cybersécurité et de protection de la vie privée Imou Cloud ont atteint des niveaux de pointe dans l'industrie.

Adresse de demande d'informations sur les certificats : https://www.certipedia.com/quality_marks

7 Suggestions pour la sécurité

7.1 Actions obligatoires à prendre pour la sécurité réseau d'équipements de base

1. **Utiliser des mots de passe robustes**

   Veuillez vous référer aux recommandations suivantes pour définir les mots de passe :

   - La longueur du mot de passe doit être d'au moins 8 caractères.
   - Ils doivent être composés de deux types de caractères comprenant des lettres majuscules et minuscules, des chiffres et des symboles.
   - Ils ne doivent pas être composés du nom du compte dans l'ordre normal ou inversé ;
   - Les caractères ne doivent pas se suivre, p. ex. 123, abc, etc.
   - Les caractères ne doivent pas se répéter, par ex. 111, aaa, etc. ;

2. **Mettre à jour le micrologiciel et le logiciel client à temps**

   - Conformément à la procédure standard de l'industrie technologique, nous vous recommandons de maintenir à jour le micrologiciel de votre équipement (enregistreurs NVR et DVR, caméra IP, etc.) afin de garantir que votre système est doté des correctifs de sécurité les plus récents. Lorsque l'équipement est connecté au réseau public, il est recommandé d'activer la fonction de vérification automatique de la disponibilité de mises à jour afin d'obtenir rapidement les informations sur les mises à jour du micrologiciel fournies par le fabricant.
   - Nous vous conseillons de télécharger et d'utiliser la version du logiciel client la plus récente.

7.2 Recommandations à suivre pour améliorer la sécurité réseau de votre équipement

1. **Protection matérielle**

   Nous vous suggérons de fournir une protection matérielle à vos équipements, en particulier les dispositifs de stockage. Par exemple, placez l'équipement dans une armoire ou une salle informatique spéciale, et appliquez des autorisations de contrôle d'accès et une gestion des clés sur mesure afin d'empêcher tout personnel non autorisé d'entrer en contact physique avec les équipements pour éviter p. ex. d'endommager le matériel, des connexions non autorisées à des équipements amovibles (disque flash USB, port série, etc.).

2. **Modifier régulièrement votre mot de passe**

   Nous vous conseillons de modifier régulièrement vos mots de passe pour réduire les risques qu'ils soient devinés ou déchiffrés.

3. **Définir et mettre à jour les informations de réinitialisation des mots de passe à temps**

   L'équipement prend en charge la fonction de réinitialisation du mot de passe. Veuillez définir les informations relatives à la réinitialisation du mot de passe à temps, y compris l'adresse électronique de l'utilisateur final et les questions de protection du mot de passe. Si les informations changent, veuillez les modifier à temps. Lors de la configuration des questions de protection du mot de passe, il est conseillé de ne pas utiliser des questions (réponses) trop faciles à deviner.

4. **Activer le blocage de compte**

   La fonction de blocage de compte est activée par défaut. Nous vous recommandons de la laisser activée pour garantir la sécurité des comptes. Si un pirate tente de se connecter plusieurs fois avec un mot de passe incorrect, le compte concerné et l'adresse IP de la source seront bloqués.

5. **Modifier les ports par défaut des services HTTP et d'autres services**

   Nous vous conseillons de modifier les ports par défaut du service HTTP et des autres services en les choisissant dans la plage numérique allant de 1 024 à 65 535, ce qui permet de réduire le risque que des étrangers puissent deviner les ports utilisés.

6. **Activer HTTPS**

   Nous vous conseillons d'activer le protocole HTTPS. Vous accéderez ainsi au service Web au moyen d'un canal de communication sécurisé.

7. **Activer la liste blanche**

   Nous vous conseillons d'activer la fonction de liste blanche pour empêcher tout le monde, à

l'exception des adresses IP spécifiées, d'accéder au système. Par conséquent, veillez à ajouter l'adresse IP de votre ordinateur et l'adresse de l'équipement qui l'accompagne à la liste blanche.

8. **Liaison d'adresse MAC**

   Nous vous recommandons de lier l'adresse IP et l'adresse MAC de la passerelle à l'équipement, réduisant ainsi le risque d'usurpation ARP.

9. **Assigner raisonnablement les comptes et les privilèges**

   En fonction des besoins d'activité et de gestion, ajoutez de manière raisonnable des utilisateurs et assignez-leur un ensemble d'autorisations minimales.

10. **Désactiver les services inutiles et choisir les modes sécurisés**

    S'ils ne sont pas nécessaires et pour réduire les risques, désactivez certains services, tels que SNMP, SMTP, UPnP, etc.

    En cas de besoin, il est fortement recommandé d'utiliser les modes sécurisés, y compris, mais sans limitation, les services suivants :

    - SNMP : choisissez SNMP v3 et configurez des mots de passe de chiffrement et d'authentification robustes.
    - SMTP : choisissez le protocole TLS pour accéder aux serveurs de messagerie.
    - FTP : choisissez le protocole SFTP et définissez des mots de passe robustes.
    - Point d'accès : choisissez le mode de chiffrement WPA2-PSK et définissez des mots de passe robustes.

11. **Chiffrement de la transmission audio et vidéo**

    Si vos contenus de données audio et vidéo sont très importants ou sensibles, nous vous recommandons d'utiliser la fonction de chiffrement de la transmission, afin de réduire les risques de vol des données audio et vidéo durant la transmission.

    Rappel : le chiffrement de la transmission entraînera une certaine baisse de l'efficacité de la transmission.

12. **Contrôle sécurisé**

    - Vérifier les utilisateurs connectés : nous vous conseillons de vérifier régulièrement les utilisateurs connectés afin de savoir si la connexion à l'appareil s'effectue sans autorisation.
    - Consulter le journal de l'équipement : en examinant les journaux, vous pouvez connaître les adresses IP utilisées pour la connexion à vos appareils et les principales opérations effectuées.

13. Journal réseau

Comme la capacité de stockage de l'équipement est limitée, le journal stocké sera limité. Si vous devez conserver le journal pour longtemps, il est recommandé d'activer la fonction de journal réseau afin de veiller à ce que les journaux essentiels soient synchronisés avec le serveur de journal réseau pour suivi.

14. Construire un environnement réseau sécurisé

Afin de garantir au mieux la sécurité des équipements et de réduire les cyberrisques potentiels, nous vous recommandons de :

- Désactiver la fonction de mappage de ports du routeur pour éviter les accès directs aux appareils Intranet à partir du réseau externe.
- Compartimenter et isoler le réseau en fonction des besoins réseau réels. Si la communication n'est pas nécessaire entre deux sous-réseaux, il est conseillé d'utiliser les technologies de réseau VLAN, GAP et d'autres pour compartimenter le réseau de sorte à obtenir une isolation réseau effective.
- Mettre en place le système d'authentification d'accès 802.1x pour réduire le risque d'accès non autorisés aux réseaux privés.

8 Réponse à un incident de sécurité

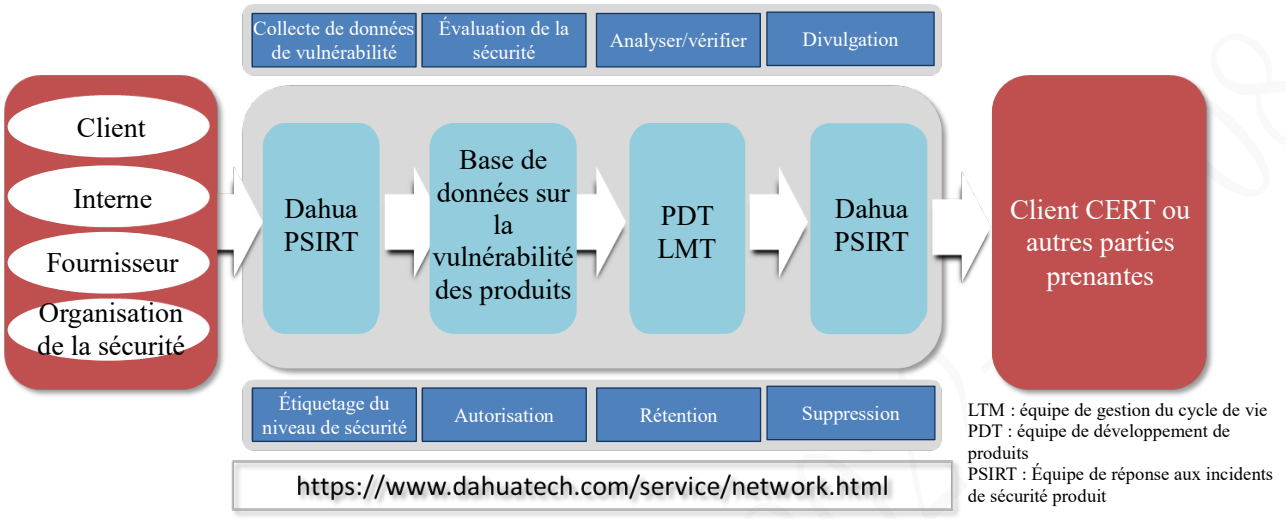

Figure 8-1 Système de réponse à un incident de sécurité du produit

La Dahua PSIRT (Équipe de réponse aux incidents de sécurité produit) est responsable de la gestion de l'écologie de sécurité et des vulnérabilités des produits conformément aux pratiques de l'industrie. Les réponses 24 h/24, 7 j/7 aux questions de sécurité mondiale offrent aux clients des alarmes de sécurité et des services de renforcement en temps opportun. Cela garantit que les problèmes de sécurité signalés à Dahua par les canaux officiels peuvent être réglés dans les 24 heures et au plus tard dans les 48 heures.

Pour la gestion des questions de sécurité, l'équipe Dahua PSIRT adopte deux formulaires – SN (Avis de sécurité) et SA (Alerte de sécurité) – pour communiquer avec les clients, ce qui garantit que nous informons les clients des problèmes de sécurité de manière appropriée au cours des différentes étapes de la découverte du problème.

L'équipe Dahua PSIRT respecte le processus de gestion des vulnérabilités ISO/IEC 30111:2013 et les normes de divulgation des vulnérabilités ISO/IEC 29147:2018, pour établir ainsi les processus de divulgation de la vulnérabilité de la sécurité des produits, des avis de sécurité et de l'alarme de sécurité. Dahua encourage également les utilisateurs finaux, les partenaires, les fournisseurs, les agences gouvernementales, les organisations industrielles et les chercheurs indépendants qui découvrent des risques potentiels ou des vulnérabilités liés aux produits Dahua à signaler activement de tels problèmes de sécurité.

L’équipe Dahua PSIRT participe activement aux activités de l’industrie et publiques, et entretient des communications ouvertes avec le CERT du gouvernement, le CERT/PSIRT du client, d’autres fournisseurs, chercheurs et des agences de coordination tierces. En rejoignant le FIRST (Forum des Équipes de réponse aux incidents de sécurité produit), les CNA (une agence internationale émettrice de numéro CVE), la CNNVD (Base de données nationale des vulnérabilités en matière de sécurité de l’information de Chine), la CNVD (Base de données nationale des vulnérabilités de Chine), la CCTGA (Alliance de gouvernance contre la menace cybernétique chinoise) et d’autres organisations chargées de la sécurité de l’information, nous sommes en mesure d’utiliser les avantages de l’affiliation afin d’assimiler le mécanisme de fonctionnement du partage des renseignements sur les menaces à la cybersécurité et de la coopération mutuelle.

9 Engagement en matière de sécurité

Dahua a toujours considéré la cybersécurité et la protection de la confidentialité comme l'un des programmes de haute importance de l'entreprise et a continuellement investi des fonds spéciaux pour renforcer de façon globale la sensibilisation aux questions de sécurité et les capacités afin d'assurer une protection suffisante de ses produits. Dahua a mis en place une équipe de sécurité professionnelle, qui assure la gestion et le contrôle de la sécurité tout au long du cycle de vie en ce qui concerne la conception, le développement, les essais, la production, les ventes et après-vente de produits. Tout en insistant sur la minimisation des données, la minimisation du service, l'interdiction stricte de la porte dérobée, l'élimination des services inutiles et non sécurisés (tels que Telnet, etc.), Dahua met en œuvre constamment des technologies de sécurité innovantes, s'efforce de promouvoir et d'améliorer la capacité de sécurité des produits, et répond de manière efficace aux exigences de sécurité des utilisateurs dans différents scénarios.

Dahua a fondé le Centre de cybersécurité de Dahua (DHCC) pour résoudre les problèmes de cybersécurité et fournir des solutions fiables et sécurisées à nos clients du monde entier, notamment les avis de sécurité, les alarmes de sécurité, les rapports de vulnérabilité et les processus d'intervention, et le partage des suggestions de sécurité et des résultats de recherche, etc. Pour obtenir les informations de sécurité les plus récentes et détaillées, visitez le site :https://www.dahuatech.com/service/network.html.

Dahua a également mis en place l'Équipe de réponse aux incidents de sécurité produit (PSIRT), qui est chargée de recevoir, d'enquêter et de communiquer publiquement les informations sur les vulnérabilités de sécurité relatives aux produits et solutions Dahua, de répondre aux questions de sécurité mondiale 24 h/24, 7 j/7, et de fournir aux clients des avis de sécurité et des services de renforcement en temps opportun. Dahua espère et encourage l'utilisateur final, le partenaire, le fournisseur, l'agence gouvernementale, l'organisation industrielle, et le chercheur indépendant qui découvre des risques ou des vulnérabilités à contacter activement Dahua PSIRT (CyberSecurity@dahuatech.com). S'il s'agit de renseignements sensibles, comme des vulnérabilités, nous vous recommandons d'utiliser la clé publique PGP Dahua pour le chiffrement.

[Pour une société plus sûre et une vie plus intelligente]