Guide sécurité réseau pour vidéosurveillance IP

Référence	Version	Date	Catégorie
GUID-PREM-004	v1.1	Avril 2025	Documents Premium

> ***Premium***

Le réseau IP est l'infrastructure sur laquelle repose l'ensemble d'un système de vidéosurveillance moderne. Sa sécurisation conditionne directement la confidentialité des images, la disponibilité du système et la protection contre les attaques latérales vers d'autres systèmes de l'organisation. Ce guide définit l'architecture réseau recommandée, les protocoles autorisés et interdits, et les mécanismes de détection et de supervision applicables.

---

01. Architecture réseau recommandée

L'isolation réseau des équipements de vidéosurveillance est le principe fondateur de l'architecture recommandée. Les caméras IP, NVR et serveurs VMS doivent être déployés sur un VLAN dédié, sans accès direct au réseau utilisateurs et sans accès direct à Internet. La communication entre le VLAN vidéo et les autres segments réseau est contrôlée par le pare-feu et limitée aux flux strictement nécessaires (accès des clients VMS depuis les postes opérateurs, accès de la supervision).

Pour les sites nécessitant un accès distant au système de vidéosurveillance (télémaintenance, supervision multi-sites), une DMZ est mise en œuvre. Le serveur VMS n'est jamais exposé directement sur Internet ; seul un reverse proxy ou un équipement de type passerelle d'accès sécurisé (VPN concentrator, bastion) est accessible depuis l'extérieur, et uniquement sur les ports strictement nécessaires.

La séparation des flux management et des flux vidéo sur des sous-réseaux distincts est recommandée pour les déploiements de grande taille. Les flux de management (administration des caméras,

configuration du NVR) transitent sur un sous-réseau dédié accessible uniquement depuis les postes d'administration identifiés. Les flux vidéo (streaming vers le VMS et les postes clients) transitent sur un sous-réseau optimisé pour le débit et la qualité de service.

---

02. Protocoles autorisés et interdits

Les protocoles autorisés pour la vidéosurveillance IP sont : HTTPS (administration des caméras et interfaces web de NVR, port 443), RTSP over TLS (streaming vidéo chiffré, port 322 ou configurable), SSH (accès administration en ligne de commande sur équipements le supportant, port 22 configuré avec clés uniquement), ONVIF over HTTPS (découverte et contrôle des caméras en environnement fermé). Le protocole ONVIF Discovery (multicast UDP) est autorisé uniquement sur le segment vidéo isolé.

Les protocoles formellement interdits sur les systèmes de vidéosurveillance sont : HTTP (administration en clair), Telnet (accès console non chiffré), FTP/TFTP (transfert de fichiers non chiffré), RTSP sans chiffrement (streaming vidéo en clair accessible par capture réseau), SNMP v1 et v2c (gestion réseau avec authentification en clair). L'utilisation de ces protocoles constitue une non-conformité bloquante dans la checklist de mise en service.

---

03. Détection d'intrusion réseau

La mise en place d'un IDS/IPS (Intrusion Detection/Prevention System) sur le segment vidéo est recommandée à partir du niveau Renforcé. Il permet de détecter les comportements anormaux caractéristiques d'une attaque : scans de ports depuis l'intérieur du réseau vidéo, tentatives de connexion sur des ports non autorisés, volumes de trafic sortant anormaux (exfiltration de données), tentatives d'exploitation de vulnérabilités connues.

Des règles de détection spécifiques aux systèmes de vidéosurveillance doivent être configurées, couvrant notamment : les signatures des exploits connus ciblant les principaux constructeurs de caméras et NVR, les tentatives de connexion avec les identifiants par défaut des équipements courants, et les communications vers des adresses IP de commande et contrôle référencées dans les listes de réputation.

04. Monitoring du trafic vidéo

Le monitoring du trafic réseau vidéo sert deux objectifs complémentaires : la performance (garantir que la bande passante est suffisante et identifier les caméras consommant anormalement des ressources) et la sécurité (détecter des comportements suspects). Un tableau de bord de supervision réseau dédié est configuré, accessible au responsable informatique du client et à l'équipe de télémaintenance de Mileo Technology.

> **Des seuils d'alerte sont définis pour les indicateurs clés : bande passante globale du VLAN vidéo (alerte à 80 % de la capacité), nombre de tentatives d'authentification échouées par équipement (alerte à 5 tentatives en 10 minutes), trafic sortant du VLAN vidéo vers Internet (alerte sur tout trafic non prévu dans la politique). Ces alertes sont envoyées par mail et, dans les contrats Premium, intégrées au SIEM du client.**