Procédure de segmentation réseau

Référence	Version	Date	Catégorie
PROC-CYB-004	v1.1	Mai 2025	Cybersécurité

La segmentation du réseau est une mesure de sécurité fondamentale pour protéger les systèmes de vidéosurveillance des menaces internes et des compromissions latérales. Un réseau vidéo non segmenté expose l'ensemble du système d'information d'un client à des risques majeurs. Mileo Technology impose une architecture réseau segmentée sur toutes ses installations, comme l'ANSSI le recommande pour les systèmes de sécurité.

---

01. Séparation par VLAN dédié

Le réseau de vidéosurveillance est systématiquement isolé sur un VLAN dédié, distinct du réseau bureautique, du réseau d'accueil (WiFi invités) et de tout autre réseau du site. Cette séparation est réalisée au niveau des commutateurs réseau par configuration des ports en mode accès sur le VLAN vidéo approprié.

Les caméras IP, enregistreurs NVR et postes de travail dédiés à la supervision vidéo sont les seuls équipements autorisés sur le VLAN vidéo. Tout autre équipement (ordinateurs bureautiques, téléphones IP, imprimantes) est formellement interdit sur ce VLAN.

Pour les installations de contrôle d'accès, un VLAN distinct du réseau vidéo est créé. Les systèmes d'hypervision et d'intégration communiquent entre VLAN via des règles de pare-feu explicitement définies, en appliquant le principe de moindre flux.

---

02. Règles de pare-feu inter-VLAN

Toutes les communications entre le VLAN vidéo et les autres réseaux sont contrôlées par un pare-feu ou un commutateur de niveau 3

configuré avec des listes de contrôle d'accès (ACL). Le principe de base est le refus de tout trafic non explicitement autorisé (default deny).

Les règles autorisées sont strictement limitées aux flux nécessaires : accès du poste de supervision au VMS (port et protocole spécifiés), accès des caméras au NVR (protocoles RTSP/ONVIF spécifiés), synchronisation NTP depuis un serveur interne. Chaque règle est documentée avec sa justification.

Les règles de pare-feu sont révisées annuellement et lors de chaque modification de l'architecture. Les règles obsolètes sont supprimées. Un audit des flux autorisés est réalisé à l'aide d'outils d'analyse réseau lors de la mise en service et annuellement.

---

03. Interdiction de pont réseau

La création de ponts réseau (bridge) entre le VLAN vidéo et tout autre réseau est formellement interdite. Cette interdiction s'applique à tous les équipements : commutateurs, enregistreurs, ordinateurs, caméras disposant de ports réseau supplémentaires.

Les caméras disposant d'un port réseau passant (switch intégré) sont configurées pour isoler les équipements connectés à ce port du réseau vidéo, ou ce port est désactivé. La configuration de chaque caméra est vérifiée à cet égard lors de la mise en service.

---

04. DMZ pour accès distants

Les accès distants entrants (maintenance par VPN, flux vidéo pour télésurveillance) transitent par une zone démilitarisée (DMZ) séparant Internet du réseau vidéo interne. Le serveur VPN ou le proxy vidéo est hébergé dans cette DMZ, avec des règles de pare-feu strictes vers le réseau vidéo.

Aucun équipement du réseau vidéo interne (caméra, NVR, VMS) n'est directement exposé sur Internet. Toute tentative de configuration d'un accès direct depuis Internet vers un équipement vidéo interne est refusée et documentée comme non-conformité.

---

05. Documentation du schéma réseau

Un schéma réseau complet et à jour est une exigence obligatoire de chaque projet. Ce schéma représente l'ensemble des équipements, leur VLAN d'appartenance, les adresses IP, les flux autorisés entre VLAN et les interfaces de connexion à Internet. Il est réalisé avec un outil de modélisation et intégré au DOE.

Le schéma réseau est mis à jour immédiatement lors de toute modification de l'architecture (ajout de caméras, modification du réseau). La version en vigueur est conservée dans le dossier de configuration du site et accessible aux équipes d'intervention. Un historique des versions est maintenu.

Boulevard de Courcelles, 75008 Paris — hello@mileotech.com

© 2026 Mileo Technology. Tous droits réservés.