Politique VPN et accès maintenance

Référence	Version	Date	Catégorie
POL-CYB-004	v1.0	Avril 2025	Cybersécurité

L'accès distant aux systèmes de vidéosurveillance pour la maintenance nécessite une infrastructure VPN robuste et correctement configurée. Une mauvaise configuration VPN peut annuler tous les bénéfices de la segmentation réseau et exposer les systèmes clients à des compromissions. Mileo Technology définit ici les exigences techniques et organisationnelles applicables à tout déploiement VPN réalisé dans le cadre de ses projets.

---

01. Solution VPN approuvée

Mileo Technology utilise et recommande des solutions VPN de niveau entreprise, basées sur des protocoles éprouvés (IPSec/IKEv2 ou OpenVPN). Les solutions retenues pour les déploiements clients sont sélectionnées parmi les produits dont la sécurité a été auditée et dont les mises à jour de sécurité sont régulières et pérennes.

Les solutions VPN grand public ou les offres gratuites sans garantie de sécurité sont formellement interdites. Les routeurs de marque reconnue (Fortinet, Cisco, Stormshield, pfSense avec support professionnel) sont privilégiés pour les passerelles VPN des sites clients. Le choix de la solution est documenté dans le dossier projet.

---

02. Paramètres de chiffrement

Les paramètres de chiffrement minimum imposés sont : algorithme de chiffrement AES-256-GCM, protocole d'échange de clés IKEv2 avec Perfect Forward Secrecy (PFS), algorithme d'intégrité SHA-256 minimum (SHA-384 ou SHA-512 recommandé), groupe Diffie-Hellman

14 minimum (groupe 19 ou 20 recommandé pour les nouveaux déploiements).

Les paramètres faibles ou obsolètes sont explicitement interdits : DES, 3DES, RC4, MD5, SHA-1, IKEv1 en mode agressif, groupe DH 1 ou 2. Les configurations par défaut des équipements intègrent parfois ces algorithmes faibles ; leur désactivation est vérifiée lors de chaque déploiement.

---

03. Authentification mutuelle par certificats

L'authentification VPN est réalisée par certificats X.509 sur l'infrastructure à clés publiques (PKI) de Mileo Technology. Chaque client dispose d'un certificat unique, et chaque poste de maintenance de Mileo Technology dispose de son propre certificat nominatif. L'authentification par simple pré-shared key (PSK) partagée est interdite.

Les certificats ont une durée de validité de 2 ans maximum. Le renouvellement est planifié 30 jours avant l'expiration. Les certificats révoqués sont immédiatement ajoutés à la liste de révocation (CRL) distribuée aux passerelles VPN concernées. Une infrastructure OCSP est mise en place pour les déploiements les plus critiques.

---

04. Split tunneling et restrictions

Le split tunneling — configuration permettant au poste de travail de communiquer simultanément avec le réseau client via VPN et avec Internet directement — est formellement interdit. Lorsque le VPN est connecté, l'ensemble du trafic du poste de maintenance doit transiter par la passerelle Mileo Technology, permettant un contrôle et une journalisation centralisés.

Cette restriction garantit qu'un poste de travail compromis ou infecté ne peut pas servir de vecteur pour attaquer simultanément le réseau client et communiquer avec un serveur de commande extérieur. La configuration du client VPN est standardisée et gérée centralement par Mileo Technology.

---

05. Conservation des logs de connexion

Les journaux de connexion VPN (date et heure de connexion, identité de l'utilisateur, adresse IP source, durée de session, volume de données échangées) sont conservés pendant 12 mois minimum dans l'infrastructure de Mileo Technology.

Ces journaux sont protégés contre toute modification non autorisée et accessibles uniquement au référent cybersécurité et à la direction. Ils peuvent être produits sur demande du client ou des autorités compétentes dans le cadre d'une investigation. Leur intégrité est garantie par un mécanisme de signature ou d'horodatage.

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