

UCOPIA, une gamme de contrôleurs pour la sécurité intérieure et l'accueil des visiteurs des PME.



Les PME s'équipent contre les risques de sécurité Internet : les pare feu ou les UTM protègent des virus, logiciel espion, et autres attaques Internet. Mais les risques de sécurité intérieure du réseau sont négligés : confidentialité, connexions pirates, ...

Parallèlement, les employés circulent dans leur entreprise et accueillent des visiteurs : consultants, partenaires, clients, ou prestataires. Tous ont besoin de se connecter en différents lieux de l'entreprise, sur un réseau filaire ou sans fil, simplement et sans assistance technique.

UCOPIA propose aux PME une gamme de contrôleurs tout en un, faciles à déployer et à administrer qui répondent aux besoins de sécurité intérieure, de nomadisme des employés et des visiteurs.

Les besoins de sécurité intérieure et de nomadisme

Le passage de la porte d'entrée ne constitue pas un droit d'accès au réseau de l'entreprise. L'entreprise doit identifier tout utilisateur qui se connecte puis contrôler son trafic. Les employés et les visiteurs de l'entreprise sont demandeurs de moyen de connexion au système d'information en dehors de leur poste de travail. La combinaison des risques de sécurité intérieure et du nomadisme rend indispensable la mise en oeuvre d'un SMAC (Secure Mobile Access Controller) afin de se protéger des risques de sécurité intérieure et de gérer le nomadisme des employés comme des visiteurs.

- Risques de sécurité Intérieure :

- Réseau Wi-Fi et connexion du parking
- Client en formation accédant par erreur à des informations confidentielles
- Un employé accédant à un site interdit

- Nomadisme :

- Accès partout et à toute heure
- Contrôle d'accès par profil, lieu et heure
- Accès zéro configuration, zéro assistance aux applications
- Accueil des visiteurs.

*: Le décret d'application de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme portant notamment sur la conservation des données relatives au trafic des communications électroniques en France a été publié le 27 mars 2006

Selon ce texte, les opérateurs de communications électroniques sont obligés de conserver pendant un an les données relatives au trafic des communications électroniques susceptibles d'aider à l'identification ou à la poursuite de personnes recherchées.

UCOPIA propose une gamme complète de contrôleurs de type SMAC (Secure Mobile Access Controller) pour les besoins de sécurité intérieure, et de nomadisme des employés et des visiteurs.

UCOPIA protège le réseau INTERNE :

- **Authentification des utilisateurs** : UCOPIA permet une authentification par type de population

- **Confidentialité** : UCOPIA est compatible avec les mécanismes de chiffrement.

- **Contrôle d'accès par profil** : Une fois authentifié, l'utilisateur est associé à un profil préalablement défini qui va déterminer ses droits.

- **Traçabilité** : Afin d'être conforme à loi dite anti-terroriste du 26 janvier 2006*, UCOPIA enregistre dans une base de donnée l'ensemble des données de connexions et de trafic (date de connexion et identité de l'utilisateur), en complément du contrôle d'accès.

- **Intégration à l'existant** : UCOPIA s'intègre parfaitement avec les solutions et architectures déjà en place (réseaux filaires, annuaires, VLAN) et assure ainsi à l'organisation la pérennité des choix de matériel en s'adaptant aux évolutions du parc.

communications
UCOPIA

Le Wi-Fi à la hauteur des exigences professionnelles

Sécurité intérieure

- **Authentification des utilisateurs :**

L'authentification est un passage obligé pour une sécurité professionnelle.

Quiconque veut se connecter doit d'abord être authentifié par un mot de passe, une carte à puce ou encore un certificat. UCOPIA propose différentes méthodes d'authentification en accord avec les contraintes de sécurité de chaque type de population. UCOPIA intègre pour cela serveur RADIUS, annuaire, portail sécurisé et interagit avec les dispositifs en place.

- **Confidentialité :**

Toutes les informations qui circulent sur le réseau sont cryptées afin d'en garantir la confidentialité. UCOPIA opère en complémentarité des mécanismes de chiffrement comme 802.11i, WPA, WPA2, VPN IPSEC.

- **Contrôle d'accès par profil :**

Une fois authentifié, l'utilisateur est associé à un profil préalablement défini. Ce profil précise, compte tenu de l'identité de l'utilisateur et de sa fonction, du lieu ou encore de l'heure, les droits de l'utilisateur. UCOPIA intègre pour cela des mécanismes de filtrage des flux réseau.

- **Réponse à l'obligation légale (LCT2006) : la traçabilité :**

En complément du contrôle d'accès, UCOPIA enregistre dans ses journaux l'ensemble des données de connexions et de trafic (date de connexion et identité de l'utilisateur). En France, la LCT 2006, oblige à la conservation des données de connexion pendant 12 mois et à la capacité de les communiquer à la Justice à sa demande.

- **Intégration à l'existant :**

UCOPIA ne remplace pas les mécanismes de sécurité en place (annuaire, authentification, VPN) mais s'appuie sur eux pour renforcer la sécurité : isolation des flux sur différents VLANs selon le profil, utilisation automatique de la sortie Internet sécurisée (proxy).

Nomadisme

- **Gestion des nomades :**

Pour les visiteurs, UCOPIA permet à une personne habilitée à ouvrir un accès très simplement pour un visiteur. Le visiteur peut également se déclarer tout seul et recevoir un mot de passe sur son téléphone mobile. Dans certains environnements, l'accès pourra être lié à un paiement Internet. Tous ces mécanismes sont intégrés dans UCOPIA et peuvent être activés ou masqués si l'entreprise le souhaite.

- **Accès nomade zéro configuration :**

Les nomades se déplacent avec leur PC et se connectent dans différents endroits. Grâce à UCOPIA, l'utilisateur n'a pas besoin de modifier la configuration de son PC, ni faire appel à l'assistance technique. UCOPIA analyse les flux qui entrent et sortent du PC, détecte les besoins de l'utilisateur et met automatiquement les flux en conformité avec le réseau.



UCOPIA Communications

99, rue Pierre Séward

92324 CHATILLON cedex

Tél.: +33(0)1 40 92 73 90

Fax : +33(0)1 40 92 73 99

E-mail : contactus@ucopia.com

Web: www.ucopia.com

communications
UCOPIA