PACK SKube

Parce que toutes les entreprises sont de plus en plus exposées aux risques liés à Internet, **Security Keepers** a créé le **Pack SKube.** Conçu pour les entreprises disposant d'une architecture réseau mono site, équipées d'un accès aux réseaux publics utilisant une bande passante inférieures ou égales à 1Mb/s.
Grâce à ses aspects technologique et « tout en un », la solution SKube, qui est équipée de 2 interfaces Ethernet 10/100, procure des performances, une fiabilité et une sécurité exceptionnelles permettant ainsi à l'entreprise de protéger plus efficacement du monde extérieur.
Les nombreuses fonctionnalités complémentaires (relais SMTP, relais HTTP/FTP, filtrage d'URL, ...) affinent la mise en place de la politique globale de sécurité qui convient à l'entreprise, tout en lui facilitant le contrôle et l'optimisation de l'utilisation d'internet..

Le pack SKube est composé d'une plate-forme dédiée, de logiciels (*firewall,VPN,nIDS etc…)*, associés à des services de surveillance et de télé administration 24/7, dans le cadre de mensualités financières sur 24, 36 ou 48 mois.

Descriptif du Pack SKube :

- **Equipements**

  Comme chaque réseau d'information est unique, Security Keepers a mis au point la gamme « SKube » dimensionné pour les réseaux à débits modéré (inférieur ou égal à 1Mb/s) ayant 50 utilisateurs maximums comme des TPE, agences commerciales ou certaines PME/PMI.

- **Une suite logicielle de sécurité**

  - Un firewall stateful avec proxys doté d'un agent de supervision contrôlant le trafic.
  - Un VPN vous permettant de sécuriser les connexions avec d'autres établissements et le personnel nomade de l'entreprise.
  - Un système de détection d'intrusion réseau (nIDS) utilisant le moteur d'analyse SNORT, sur une base de signature enrichie et mise à jour par Security Keepers.

- **Le Centre de Supervision & de Réponse Security Keepers à votre service**

  Le Security Center (centre de supervision) supervise l'intégrité de vos réseaux et liens VPN externes. Il veille au bon fonctionnement des machines et vous alerte en cas de trafics réseaux douteux externes ou de problèmes d'exploitation machine.
  Chaque machine étant sous monitoring constant, le **Security Center** a la capacité de cloner la machine à l'identique.

Services liés au Pack SKube :

- **Le contrat de service EverProtect Silver**

  La solution SKube est associée à un montant mensuel de service de niveau Silver (cf. grille tarifaire).

  L'objet d'EverProctect est de fournir des prestations de services de supervision de trafic et de flux Internet, des services de télémaintenance & télé administration et des services de mise à jours. Fonctions assurées à l'échelon humain par nos spécialistes en sécurité informatique : les « **keepers** »

  - **Services de supervision de trafic et de flux Internet**

    Les connexions vers l'Internet et/ou vers un autre site distant au moyen d'une ligne spécialisée utilisant la connexion « wan » du SKube, sont contrôlées dans le but de surveiller la continuité de service du fournisseur d'accès Internet.

    Le « **Keeper** » peut intervenir à tout moment pour vérifier un « paquet suspect » (blocage des attaques non détectées par les systèmes, en temps réel) C'est le **double niveau de protection « EverProtect** Ò**»**

    L'intégrité de fonctionnement et la performance des logiciels de protection et de réglage de trafic de flux provenant de la ligne spécialisée Internet sont surveillés et contrôlés.

    La supervision de ces deux éléments du SKube est assurée en mode 24/7/365.

- **Services de Télémaintenance et Télé-administration**

  Dans le cadre d'un dysfonctionnement des services réseaux du **SKube**, les **Keepers** interviennent pour constater et dépanner la machine par le biais de services de télémaintenance.

  Le client peut être amené à demander au **Security Center** de réaliser des changements de configuration de sa plate-forme **SKube**. Le superviseur réalisera les changements par des services de télé-administration après avalisation.

  L'ensemble de ces services sont réalisés en mode 24/7/365. Ils résultent d'ordres de mission du client sous la forme de Tickets d'Incidents.

- **Le reporting**

  Afin de connaître et contrôler l'activité de sécurité , l'utilisation faite d'Internet dans l'entreprise, le **Security Center** vous délivre un **rapport mensuel détaillé,** consultable en ligne (accès sécurisé).

Descriptif fonctionnel

Système

- Noyau Linux sécurisé et optimisé
- Protection contre les attaques de type Buffer Overflow

Filtrage

- Suivi de session TCP, UDP, ICMP niveaux 3 et 4 (stateful) et niveau 7
- Filtrage des protocoles HTTP, FTP, SMTP, DNS
- Détection d'intrusion

Routage

- Routage statique sur toutes les interfaces (ADSL, câble, ...)
- Translation d'adresse statique et dynamique (NAT, PAT)
- Client ADSL (PPPoE, PPTP)

Relais HTTP/FTP

- Filtrage d'URL par black list personnalisable effectué par le Security Center
- Filtrage des contenus
- Gestion et protection des users par l'utilisation systématique des proxys

Relais de messagerie SMTP

- Filtrage par mots-clé
- Contrôle UCE par black list temps réel et ACLs
- Routage multi-domaines

Virtual Private Network

- Compatibilité IPSEC
- Echange de clés IKE
- Certificat X509, clés partagées ou clés RSA
- Cryptage 3DES

Authentification MD5 / SHA1

Administration et monitoring

- Administration centralisée et sécurisée
- Module de configuration Maître/Esclave (distribution automatique des configurations)
- Export automatique des logs
- Remontée des alertes

Performances

- Débit utile : Gb/s
- Nombre maximum de sessions simultanées : million
- Débit IPSec algorithme 3DES : supérieur à Mb/s
- Nombre de nouvelles sessions par seconde :

*Incompatible avec l'option Haute Disponibilité

Architecture Type