

## L'ACCÈS À INTERNET EN TOUTE SÉCURITÉ

**Avec son offre Firewall Management, Sodifrance apporte une solution pragmatique et rigoureuse pour prendre en charge la totalité de vos besoins liés aux Firewall et aux autres composants de sécurité.**

“ **Firewall Management fait parti de l'offre Global Security de Sodifrance. Global Security met en œuvre une approche globale des problématiques de sécurité, prend en compte les aspects à la fois techniques et fonctionnels de la démarche, et s'appuie sur un cycle d'amélioration en continu. Cette approche globale vous garantit un haut niveau de sécurité en permanence.** ”



Internet a profondément modifié les systèmes d'information. Initialement parfaitement étanches et cloisonnés, ceux-ci sont aujourd'hui accessibles par tous, 24H/24 de n'importe quel point du globe. Toutefois, l'adoption rapide de cette technologie oblige les services informatiques à reconsidérer leur existant en terme de sécurité.

### ■ POURQUOI SE PROTÉGER DES RISQUES LIÉS À UNE CONNEXION PERMANENTE À INTERNET ?

Si votre entreprise dispose d'un accès permanent à Internet (ADSL, ligne spécialisée...), la visibilité de son adresse IP rend votre système d'information vulnérable. De plus, l'arrivée massive des virus mutants de services et autres techniques d'attaques sophistiquées et facilement accessibles, sont autant de difficultés qui doivent être prises en compte pour assurer la protection de vos données et de l'image de votre entreprise.

### ■ POURQUOI S'ORIENTER VERS UNE DÉMARCHE GLOBALE ET CONTINUE ?

Les sociétés ont dans un premier temps cherché à se protéger en achetant des produits tels que des Firewall. Aujourd'hui, il apparaît clairement que ces produits considérés isolément, parfois non mis à jour, mal configurés ou peu supervisés, ne peuvent être suffisants pour se protéger.

« La sécurité des infrastructures réseaux et applicatives doit être administrée et pilotée dans un cadre global et continu pour vous garantir une protection optimale ».

### ■ COMMENT GARANTIR LA PERFORMANCE DE VOTRE ARCHITECTURE SÉCURITAIRE ?

Afin d'assurer la sécurité de votre système d'information, protégez vos données,

Sodifrance met à votre disposition ses experts en sécurité, formés et certifiés par les plus grands éditeurs et constructeurs du marché, pour :

- Etablir l'état des lieux de votre niveau de sécurité actuel
- Vous assister dans la définition de votre politique globale de sécurité
- Vous conseiller sur les meilleures solutions technologiques du marché
- Réaliser et suivre l'installation de votre plate-forme conformément à votre plan qualité
- Surveiller, administrer et maintenir votre plate-forme 24H/24, 7J/7
- Vous accompagner dans l'évolution de vos besoins
- Réaliser les rapports et analyses détaillées du fonctionnement de votre plate-forme.

### Les avantages de Firewall Management

- Matériels et logiciels dédiés
- Politique d'engagement de services formalisée dans un plan d'assurance qualité
- Grande disponibilité de notre Centre Opérationnel de Sécurité
- Hot-Line dédiée pour réagir rapidement aux anomalies
- Mise à jour systématique des composants de votre plate-forme
- Analyse des logs et édition de rapports d'activités
- Solution entièrement paramétrable et évolutive
- Possibilité de constituer des réseaux privés virtuels (VPN)
- Tarification mensuelle adaptée

## Firewall Management est une offre complète qui vous garantit une sécurité optimale de vos environnements

### Références

- Ville de Rennes
- CCI de Saint Malo
- Tricots Saint James
- S.A. Lorans
- Sofiquem
- SAGESS
- SDIS des Côtes d'Armor
- Anne Fontaine
- Verlingue
- ...

#### ■ UN INTERLOCUTEUR UNIQUE

Sodifrance met à votre disposition une hot-line qui transmet toute demande d'intervention ou question sur votre plate-forme au centre opérationnel de sécurité, seul habilité à effectuer toute modification de votre configuration.

#### ■ UN CENTRE OPÉRATIONNEL DE SÉCURITÉ SOUS HAUTE PROTECTION

Chaque plate-forme sous contrat est reliée à notre centre opérationnel à partir duquel nous pouvons, au travers d'une connexion sécurisée (VPN ou RNIS), effectuer les opérations de surveillance, d'analyse et de mise à jour.

**Toutes les interventions sont effectuées selon une procédure décrite dans un plan d'assurance qualité.**

Chaque modification est soigneusement analysée et contrôlée. De plus, toutes les connexions et évolutions sont enregistrées dans un rapport d'intervention.

#### ■ UNE POLITIQUE D'ENGAGEMENT DE SERVICES

Les solutions déployées sont accompagnées d'une politique de services qui spécifie précisément le périmètre et le niveau de nos engagements sur chacun des points sur lesquels nous intervenons.

#### ■ UNE PLATE-FORME SÉCURITÉ DÉDIÉE ET PERSONNALISÉE

Conformément à notre politique d'engagement de service, nous assurons la maintenance des équipements dans les plus brefs délais.

#### ■ DES RAPPORTS D'ANALYSE DE JOURNAUX D'ACTIVITÉS (LOG)

Toutes les nuits, les fichiers de logs sont téléchargés depuis vos environnements vers le centre opérationnel de sécurité. Ceux-ci sont traités et analysés par nos experts pour vous fournir **un document graphique**

#### repreant l'activité de votre plate-forme.

Ces rapports vous sont envoyés chiffrés afin de ne les rendre lisibles qu'aux personnes habilitées. Ceux-ci sont archivés et peuvent être synthétisés sur une période de six mois ou même d'un an afin de dégager des tendances sur une plus longue période.

#### ■ POUR UNE PLUS GRANDE SÉCURITÉ

Les matériels et logiciels que nous utilisons sont installés par nos équipes dans vos locaux. **Nos solutions sont facilement interconnectables afin d'établir des architectures VPN (réseau privé virtuel).**

Ainsi, vous pouvez en toute sécurité relier vos sites distants ou donner accès à vos commerciaux nomades à leurs environnements de travail (messagerie, application métier).

#### ■ CONTRÔLE ET AUDIT DU NIVEAU DE SÉCURITÉ

Sodifrance réalise des audits réguliers afin de mesurer l'écart entre les objectifs fixés et les objectifs atteints.

Ces tests automatisés, reproductibles et établis sur la base de plus de 6000 combinaisons et 1300 vulnérabilités, sont une aide précieuse pour faire évoluer votre politique sécuritaire face aux dernières signatures d'attaques.

#### ■ DES FONCTIONNALITÉS ÉVOLUTIVES POUR ACCROÎTRE LA SÉCURITÉ DE VOTRE ENVIRONNEMENT

Firewall Management peut être couplé à des solutions complémentaires :

- **URLfilter** : pour maîtriser l'accès des sites Internet accessibles à vos collaborateurs,
- **Contrôle de contenu et antivirus** : pour contrôler les flux de messagerie et de navigation qui entrent et sortent de votre entreprise,
- **Authentification forte** : pour renforcer l'authentification des utilisateurs nomades qui se connectent à votre environnement.