

## Sécurité : 10 fonctionnalités clés d'un pare-feu Next-Gen

### Sécurité

Posté par : JPilo

Publié le : 3/10/2011 11:00:00

La grande majorité des administrateurs de réseau s'accordent sur le fait que **le contrôle des applications** prend une part centrale dans la sécurité. Les utilisateurs adoptent continuellement de nouvelles applications et technologies, et les menaces qui vont avec. Pour beaucoup d'entreprises, restreindre l'adoption de ces nouvelles technologies freine leur développement.

Pouvoir utiliser une application donnée est parfois une nécessité pour effectuer une tâche ou gagner en productivité. La conséquence ? La sécurisation des applications en temps réel plutôt que leur blocage devient la bonne règle à appliquer. Mais pour cela, les équipes de sécurité doivent mettre en place la structure qui va définir les bonnes règles, les contrôler qui les activeront et disposer d'un pare-feu nouvelle génération (NGFW à Next-Generation Firewall)



Les 10 points présentés ci-dessous sont les fonctionnalités clés permettant la mise en place de contrôles nécessaires dans un environnement toujours plus riche en applications et en menaces.

### **Ainsi, un pare-feu nouvelle génération doit :**

- 1 - identifier et contrôler les applications sur n'importe quel port, pas seulement les ports standard (y compris les applications utilisant http ou d'autres protocoles)
- 2 - identifier les techniques d'évasion et les contournements : proxy, accès distant, applications dans un tunnel chiffré
- 3 - pouvoir chiffrer les flux SSL sortants
- 4 - permettre un contrôle des différentes fonctions d'une même application (ex. : SharePoint Admin face à SharePoint Docs)
- 5 - détecter les menaces dans les applications collaboratives autorisées (ex. : SharePoint, Box.net, MS Office Online...)
- 6 - gérer le trafic inconnu avec des règles et ne pas simplement les laisser passer
- 7 - identifier et contrôler les applications partageant une même connexion

8 - disposer du même contrôle et de la même visibilité sur les utilisateurs distants et mobiles que sur les utilisateurs internes

9 - simplifier la sécurité réseau : pouvoir contrôler les applications ne doit pas ajouter de complexité.

10 - fournir le même débit et les mêmes performances malgré l'activation de tous les contrôles applicatifs

### Le cabinet d'analyse Gartner a établi les exigences qu'un pare-feu doit remplir pour être qualifié de NGFW :

• Identifier les applications indépendamment du port, du protocole, du chiffrement SSL ou toute autre technique d'évasion

• Identifier les utilisateurs indépendamment de leur adresse IP

• Protéger en temps réel contre les menaces embarquées dans les applications

• Visibilité et contrôle des règles granulaires sur l'accès aux applications et leurs fonctionnalités

• Déploiement en ligne multi-gigabits, sans dégradation de performance

**Alors que le pare-feu nouvelle génération** (Next-Generation Firewall : NGFW) est bien défini par Gartner comme un élément nouveau, concentré sur l'entreprise et distinct du pare-feu classique, de nombreux éditeurs de sécurité présentent le NGFW comme un sous-ensemble de fonctions qu'ils proposent déjà (UTM, IPS). La plupart des vendeurs de sécurité réseau essaient de fournir de la visibilité et du contrôle applicatifs en utilisant un nombre limité de signatures d'applications supportées dans leur IPS ou dans une base de données externe. La réalité derrière cette façade est que ces fonctions sont faiblement intégrées et que leurs produits sont encore basés sur une technologie classique de blocage de port et non pas sur la technologie NGFW.

**Encore plus important**, ces acteurs passent à côté de l'essentiel : il ne s'agit pas de bloquer des applications, mais de sécuriser leur utilisation. En fait, les produits proposés par les éditeurs traditionnels sont effectivement des systèmes de prévention d'applications et ignorent pour beaucoup ce que les entreprises font aujourd'hui des applications à elles pour faire « tourner » l'entreprise et par conséquent, les entreprises ont besoin de s'assurer qu'elles s'exécutent en toute sécurité. Il est évident qu'un pare-feu nouvelle génération représente une classe de produits différente et révolutionnaire, mais la demande venant des entreprises pour ce type de produit est tellement forte que les acteurs traditionnels de la sécurité se servent de cet intérêt et essaient de faire diversion en tentant de ressembler à un pare-feu nouvelle génération.