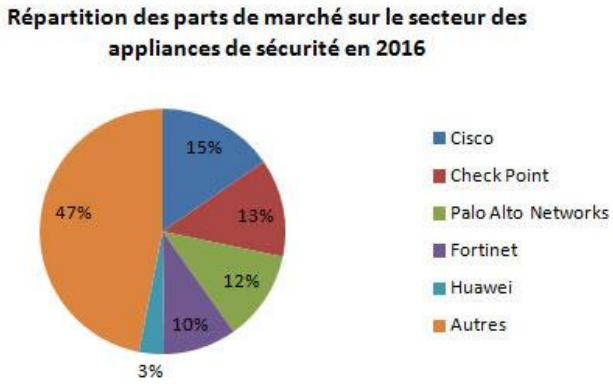
SÉCURITÉ : LE MARCHÉ DE LA SÉCURITÉ – INFRASTRUCTURE RÉSEAUX

Le marché des UTM, (Unified Threat Management)

Leader du marché :

- Cisco
- Palo Alto
- Check Point
- Networks
- Fortinet
- français Stormshield
-



Ce marché représente près de 50% des revenus mondiaux des appliances de sécurité à ce jour.

A l'inverse, les segments des appareils de IDP (Intrusion Detection and Prevention) et de VPN (VPN) connaissent des baisses de 4,6% et 4,3%.

Les Appliances de sécurité :

Les "appliances" de sécurité multifonctions regroupent tous les aspects de la sécurité d'une connexion internet dans un seul boîtier, qui se veut simple à administrer.

Ces produits ont différentes fonctionnalités: firewall, passerelle VPN, prévention et détection d'intrusions, ainsi que filtrage d'URL, antivirus et parfois "anti-spam".

Le matériel prend la forme d'une boîte noire administrable via une interface web, et qui tourne sous un système propriétaire généralement dérivé de Linux.

Pour clore le volet matériel, certains appliances troquent, pour des raisons de fiabilité, le disque dur contre une mémoire flash. Côté connectivité, ces équipements qui s'insèrent

entre le LAN et le WAN n'excèdent pas pour la plupart quatre à huit ports Ethernet, sur lesquels seront reliés des commutateurs de plus grande capacité. Excepté sur les produits d'entrée de gamme, il est possible de définir des politiques de sécurité spécifiques à chaque port, donc des DMZ. D'autre part, CheckPoint, SoniWALL et Symantec innovent en lançant des "appliances" intégrant une borne Wi-Fi. Grâce à un chiffrement IP-Sec, le réseau sans fil est alors mieux protégé que via les standards WEP et WPA.

Quatre acteurs majeurs se dégagent dans l'ordre :

- **Cisco** : Ils disposent de la première part de marché de par leur capacité à adresser une offre technologique extrêmement large et donc pénétrer les comptes facilement.
  (tu m'achètes des switchs du sol au plafond et je te mets des Firewalls pas chers).
  Technologiquement, c'est plutôt fade même si ils font des efforts de développement.

- **CheckPoint Software :** arrive en deuxième position, c'est L'acteur historique des Firewalls avec les brevets (1990) dits « Statefull Inspection » (j'autorise un flux donc également son flux retour implicitement).
  Leur business model s'appuie sur une base installée extrêmement solide et génère du cash sur le renouvellement du support et les très nombreuses licences qu'il est possible d'attacher.
  Ils doivent continuer à assurer le lien avec leurs anciennes technologies donc ils peinent à révolutionner leur offre même si elle est déjà excellente.
  C'est une société Israélienne (comme beaucoup d'acteurs dans la sécurité) aux méthodes commerciales affûtées.

- **Palo Alto Networks :** arrive en troisième position et s'impose comme un leader du Gartner en seulement 10 années d'existence, ils sont les inventeurs des Firewall dits de nouvelle génération (basée sur l'identification des applications et non des ports).
  Leur « business model » s'appuie sur une constante innovation, ils font la course en tête sur ce point et adresse de nouveaux marchés en permanence.

- **Fortinet :** est l'acteur trublion car ils se positionnent en excellent acteur avec le meilleur rapport prix/performance/fonctionnalités.
  Leur mode de fonctionnement est de coller l'actualité, de ne jamais rien inventer et de « imiter» la concurrence.
  C'est l'acteur qui nous fait le plus mal sur le marché, ils sont en capacité de casser les prix, sans réellement atteindre le même niveau fonctionnel dans les faits.

Plus loin, noyé dans la masse, arrive l'acteur Français **StormShield,**
c'est la fusion de deux acteurs Français **Arkoon** et **Netasq**.
Produit largement diffusé dans les institutions régaliennes (Ministère de la Défense, interieur,…).

Ce sont les seuls produits à être Qualifiés par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information),
Bien qu'ils soient qualifiés par l'ANSSI, ils ne sont pas à la pointe de la technologie et leurs pérennités n'est pas garanties.
Stormshield appartient à EADS (et EAD est aussi un client de **Palo Alto Networks** pour ses besoins propres de EADS…).

Un ancien grand acteur de la sécurité **Juniper** (après avoir racheté **NetScreen**) s'est recentré sur les solutions réseau et BackBone opérateurs, ils sont quasiment inexistants du marché de la sécurité alors qu'ils ont connus l'âge d'or il y a encore quelques années.

Pour la petite histoire, un nombre important de développeurs **Palo Alto Networks** viennent de **NetScreen** il y a 10 ans (ils ont traversés le boulevard dans la Silicon Valley).

Tous les autres acteurs du Gartner, ne sont pas réellement significatifs.

En terme de portfolio technique et de positionnement marché, il se dégage trois piliers :

- Les **platesformes de sécurité** (Parefeu, Firewall ou encore UTM (même si un UTM est une sous-catégorie, dépassée).
  Ces plates formes de sécurité peuvent être au format physique (des appliances) mais aussi des machines virtuelles qui peuvent être déployées dans des environnements VmWare, Microsoft, Citrix, Amazon, Microsoft Azure, OpenStack KVM, etc..

  Les déploiements sur les DataCenters virtualisés sont la grosse tendance du moment avec des besoins complémentaires à adresser.

  Les pare feux physiques sont destinés à filtrer les flux dits « Nord-Sud » qui entrent et qui sortent du DC alors que les VM Firewall sont destinées à filtrer les flux dits « Est-Ouest » entre les machines virtuelles (des applications métiers) qui résident sur un même hyperviseur.
  Exemple : Un frontal Web utilise une base de données. Si le site web est compromis alors on peut facilement rebondir sur la base de données si il n'y a pas de protection et que ces deux machines virtuelles sont installées sur le même hyperviseur VmWare par exemple.
  C'est pour cette raison que les clients avaient tendance à faire ressortir physiquement les flux sur des FW physiques. Désormais les VM Firewall permettent de répondre à ce besoin.

- Les solutions dites « **EndPoint** » qui se déploient sur le poste de travail avec des méthodes nouvelles de protection (TRAP est le produit Palo Alto Networks pour ça).

- Les solutions qui s'implémentent dans le Cloud pour les applications SaaS, c'est LA grosse tendance à venir car les usages explosent.
  On parle de produits de type **CASB** (Cloud Access Security Broker) et permettent de contrôler les usages d'applications SaaS vers applications SaaS, c'est-à-dire des flux qui ne passent plus par l'infrastructure du client.

  L'ensemble des entités régaliennes est peu concerné, conservation de leurs Datacenter et regroupement à priori.

La montée en puissance du Cloud Computing public est en train de modifier la donne, avec en première ligne les solutions de Sotfware as a Service (Saas). Elles foisonnent, sont en général bien faites et surtout permettent aux sociétés de bénéficier de l'application tout en se dégageant des problématiques d'intégration et de maintenance.
Les exemples les plus communs sont Salesforce, Google Apps, Microsoft Office365 ou encore Dropbox.
Les solutions de type Infrastructure as a Service (IaaS) comme Amazon Web Services (AWS) ou Platform as a service (PaaS) engendrent la même problématique, la donnée à protéger n'est plus uniquement physiquement présente à l'intérieur du réseau de l'entreprise !

Les équipes IT sont donc ou seront bientôt confrontées à de nouvelles problématiques. Elles doivent potentiellement découvrir les Applications « as a Service » utilisées sans leur accord – ce que l'on appelle le Shadow IT – détecter les comportements suspects dans l'usage des applications « as a Service » approuvées, prévenir les transferts de données non autorisés dans le Cloud, et sécuriser la donnée d'entreprise présente dans le Cloud.

Les pare-feux de nouvelle génération

Trois des principaux rôles que tout pare-feu moderne doit tenir :

1. Être au cœur de votre infrastructure de sécurité réseau.

2. Servir de point de contrôle d'accès à tout le trafic afin d'autoriser ou de refuser le trafic en fonction des politiques définies.

3. Éliminer le risque de l'« inconnu » au moyen d'un modèle de contrôle positif de type « autoriser certaines applications et refuser implicitement tout le reste ».

Parmi les applications et les menaces présentes sur votre réseau, citons notamment :

Applications populaires : médias sociaux, partage de fichiers, vidéo, messagerie instantanée et messagerie électronique.

Applications professionnelles de base : vous utilisez ces applications pour mener à bien vos activités professionnelles. Elles hébergent notamment vos actifs les plus précieux (bases de données, serveurs de fichiers et d'impression, annuaires et autres).

Applications système et personnalisées : il s'agit des applications d'infrastructure de base comme SSL, SSH et DNS, des applications personnalisées développées en interne ou d'applications totalement inconnues.

Pour le Gartner Group, le pare-feu nouvelle génération est un outil novateur, axé sur l'entreprise, qui « intègre des systèmes d'inspection complets assurant la prévention des intrusions, la surveillance des applications et un contrôle granulaire des politiques ».

Si les responsables de la sécurité sont intéressés par les fonctionnalités d'un pare-feu nouvelle génération, ils doivent avant tout chercher à savoir si cette technologie les aidera ou non à sécuriser.
L'utilisation des applications au sein de l'entreprise. Pour cela, ils doivent se poser les questions suivantes :

- La visibilité et l'interprétation du trafic des applications transitant par le réseau seront-elles meilleures ?
- Les options de contrôle du trafic iront-elles au-delà du modèle classique « autorisation/blocage » ?
- Le réseau sera-t-il protégé contre les menaces et cyber attaques connues et inconnues ?
- Sera-t-il possible d'identifier et de gérer systématiquement le trafic inconnu ?
- Sera-t-il possible de mettre en œuvre les stratégies de sécurité voulues sans nuire aux performances ?
- Les tâches d'administration des pare-feu seront-elles minimisées ?
- La gestion des risques sera-t-elle simplifiée et plus efficace ?
- Les stratégies mises en œuvre contribueront-elles à la rentabilité de l'entreprise ?

Pare-feu nouvelle génération :

1. Identifier les applications indépendamment du port, du protocole, de la technique d'évasion ou du chiffrement.
2. Identifier les utilisateurs indépendamment de leur équipement ou de leur adresse IP.
3. Bloquer en temps réel les menaces connues et inconnues embarquées dans les applications.
4. Offrir une parfaite visibilité des applications, des utilisateurs et du contenu et proposer un contrôle granulaire des politiques
5. Fournir un débit multi-gigabits pour un déploiement en ligne prévisible.

Considérations sur l'architecture des pare-feu et l'identification du trafic

1. Intégrer l'identification des applications au pare-feu, qui devient le principal moteur de classification.
2. Ajouter un moteur de filtrage des signatures d'applications à un pare-feu basé sur les ports.

Un modèle de sécurité positif (pare-feu ou autre) permet d'écrire des politiques qui autorisent certaines applications ou fonctions (comme WebEx, SharePoint et Gmail) et interdisent implicitement tout le reste.

Un modèle de sécurité négatif (IPS, antivirus ou autre) permet de rechercher et de bloquer des éléments spécifiques (généralement des menaces ou des applications indésirables) et de laisser passer tout le reste.

Les 10 principales fonctions que doit posséder votre prochain pare-feu :

1. Identifier et contrôler les applications sur n'importe quel port
2. Identifier et contrôler tous les moyens de contournement
3. Déchiffrer les flux SSL sortants et contrôler les flux SSH
4. Contrôler les différentes fonctions d'une même application
5. Gérer systématiquement le trafic inconnu
6. Détecter les virus et les logiciels malveillants dans toutes les applications, sur tous les ports
7. Offrir la même visibilité et les mêmes outils de contrôle pour tous les utilisateurs et équipements
8. Simplifier la sécurité réseau tout en intégrant le contrôle des applications
9. Fournir le même débit et les mêmes performances une fois le contrôle des applications activées
10. Assurer les mêmes fonctions de pare-feu qu'il s'agisse d'un environnement physique ou virtuel

Dans le monde toujours connecté actuel, le contrôle des applications ne s'arrête pas au simple principe de blocage/autorisation. Il est question de sécuriser l'utilisation des applications pour renforcer le pouvoir de l'entreprise.

La première chose qu'un nouveau pare-feu, indépendamment de son type, doit impérativement faire est de déterminer avec précision la nature du trafic, puis se baser sur ce résultat pour élaborer l'ensemble des politiques de sécurité.

Le modèle positif,
permet de contrôler et d'utiliser les applications, ce qui est un élément stratégique important dans le monde toujours connecté où évoluent aujourd'hui les entreprises.
Si la recherche des applications est confiée à des éléments annexes tels qu'un système IPS, cela signifie qu'un modèle de contrôle négatif est appliqué (tout autoriser à l'exception de ce qui est expressément refusé par le système IPS).

Les principales fonctionnalités de la virtualisation des serveurs

Cette catégorisation n'a pas vocation à être exhaustive, cependant, elle apporte un premier niveau de lecture aux services informatiques des établissements d'enseignement agricole pour choisir une solution de virtualisation.

Dans le cadre de cette étude, quatre solutions ont été expérimentées :
- Microsoft Hyper-V Server 2008 R2 (SP1),
- VMware vSphere Hypervisor (ESXi) 5.1,
- Citrix XenServer 6,
- Proxmox Proxmox VE 2.2.

Les outils de migration

Les éditeurs de solutions de virtualisation proposent aux administrateurs des outils qui permettent de migrer des systèmes installés sur des serveurs physiques vers des VM hébergées au sein de l'architecture de virtualisation. Selon les éditeurs, il existe différents outils gratuits qui permettent une conversion des « serveurs physiques » vers des « serveurs virtuels » (PtoV, ou P2V).

L'éditeur VMware met à disposition le logiciel de P to V, VMware Converter10. Cet outil supporte le clonage à froid et à chaud. Toutefois, le clonage n'est pas recommandé pour les serveurs d'applications qui utilisent des bases de données. VMware Converter permet la conversion, de façon pratique et intuitive, d'une machine physique vers une machine virtuelle en l'insérant immédiatement dans l'architecture de virtualisation. Cet outil parait simple et ergonomique.

Microsoft met à disposition un utilitaire « disk-to-vhd »11 qui permet de dupliquer un disque dur physique vers un disque dur virtuel au format Virtual Hard Disk (VHD) compatible avec Hyper-V 2012.

Citrix propose l'outil de conversion « XenConvert »12 qui est ergonomique et offre de nombreuses fonctionnalités comme le redimensionnement des partitions ou la conversion vers plusieurs formats de VM dont le format VHD.

Pour la solution Proxmox VE 2.2, il n'y a pas d'outil de conversion disponible. Cependant, il est possible de créer un clone de la machine physique, créer une machine virtuelle et son fichier de disque dur virtuel, puis appliquer l'image précédemment clonée.

Snapshots et Sauvegarde

Une mauvaise utilisation des snapshots peut entraîner des chutes de performance de l'architecture de virtualisation (VMware, 2012). Il convient donc de ne pas conserver un snapshot après la période de validation des modifications apportées à une VM. **Les snapshots ne doivent pas être considérés comme un outil de sauvegarde à part entière de la VM**, et encore moins des données contenues par les VM.

La sauvegarde complète des machines virtuelles peut être réalisée avec différents outils plus ou moins automatisés et intégrés à la solution de virtualisation. Certains éditeurs rendent possible la réalisation de scripts de sauvegarde appelés « scripting », par exemple Ghettovcb.sh (script de backup) pour les solutions de virtualisation de l'éditeur VMware. La sauvegarde des VM peut être aussi réalisée à l'aide d'outils plus élaborés fournis par les éditeurs de solutions de virtualisation ou leurs partenaires, comme Veeambackup.

Points d'attention

La concentration de services sur un seul serveur physique, bien qu'économiquement avantageuse, expose le système d'information à plus de vulnérabilités en cas de panne. Ainsi, le risque d'arrêt ou de panne totale du serveur de virtualisation ou la montée en charge anormale d'un des services entraîne une situation qui peut être catastrophique pour la structure. Il est donc important de réfléchir en amont à un plan de reprise d'activité (PRA) et un plan de sauvegarde sérieux qui comprend des éléments comme les notions de duplication de machines virtuelles, la redondance de serveurs et les sauvegardes des données.

Réflexion sur le choix NAS et SAN

Dans le cadre d'une architecture de virtualisation intermédiaire, il est difficile de faire un choix entre une solution professionnelle de stockage NAS ou SAN.
En effet, l'offre des constructeurs est abondante et toujours plus concurrentielle. De plus, les deux solutions ont tendance à converger, car les offres SAN intègrent parfois les mêmes protocoles que les NAS et inversement.
Toutefois, le choix de la solution de stockage réseau peut être orienté par plusieurs critères comme :
 La volumétrie de stockage nécessaire à la plate-forme de virtualisation,
 Les performances en opération d'entrées-sorties par seconde (IOPS)21 et en vitesse de transferts de données (Mb/s),
 La capacité d'extension de volumétrie du stockage caractérisée par la capacité à ajouter de nouvelles baies de disques,
 Le niveau de garantie et de support fournis par le constructeur,
 La rapidité et la facilité de mise en œuvre,
 La mise à disposition d'espace disque en mode bloc, basée sur les LUN (Logical Unit Number) et le protocole iSCSI,
 La certification des modèles de serveurs NAS par les éditeurs de solution de virtualisation,
 Le budget.

Architecture évoluée

L'architecture professionnelle évoluée permet un niveau important de disponibilité et de performance pour répondre aux besoins d'applications très critiques et fortement consommatrices de ressources. Dans cette architecture, le risque d'indisponibilité des machines virtuelles est réduit au maximum et celles qui sont considérées comme critiques, disposent d'un niveau de performance élevé et garanti. Ce niveau de service requiert des

solutions de virtualisation professionnelle avec des fonctionnalités à la carte comme l'allocation des ressources dynamiques, la haute disponibilité ou l'allocation dynamique de l'espace de stockage. Afin de bien utiliser ces différentes fonctionnalités, le service informatique de l'établissement doit disposer de compétences pointues d'administration. Pour une architecture de virtualisation évoluée, l'investissement budgétaire sur le plan matériel et logiciel est nettement plus important que pour l'architecture intermédiaire. Le schéma suivant présente les différents éléments constitutifs de l'architecture professionnelle évoluée.

Équipements réseaux

Le raccordement entre serveurs hôtes et baie(s) de stockage est réalisé par un chemin réseau de stockage garanti, soit par l'intermédiaire d'un switch physique ou virtuel. Ce chemin réseau nécessite un réseau physique haut débit dédié constitué d'actifs réseaux redondés et reliés entre eux par un câblage en fibre optique ou en cuivre avec des câbles de catégorie 5 ou 6. Les interfaces réseaux peuvent être redondantes ou agrégées, pour offrir un niveau de performance et de sécurité élevé. L'intérêt est de fournir aux serveurs hôtes physiques, des débits de l'ordre de plusieurs gigabits par secondes (Gbps), constants et performants.

Les actifs réseaux sont administrables à distance. Ces switches manageables de niveau 2 ou 3 permettent la prise en charge de technologies comme les réseaux virtuels (Vlan) ou l'agrégation de liens (trunking), le support des trames géantes (jumbo frame) ou les algorithmes évolués de topologie réseaux (par exemple, le spanning tree). La figure ci-dessous illustre un switch réseau modulaire pour raccorder les serveurs hôtes et une baie de stockage.

Plateforme VMware

Si on prend l'exemple de la solution VMware,
les offres et les modèles de licence d'exploitation (licensing) proposés sont nombreux et complexes. Dans l'optique d'une architecture de virtualisation intermédiaire, il est probable qu'il soit nécessaire d'acquérir la licence : Kit VMware vSphere Essentials Plus « Consolidation des serveurs et continuité d'activité pour les petits environnements ». Cette formule de tarification est prévue pour 3 serveurs, dotés chacun de 2 processeurs au maximum, et comprend les fonctionnalités suivantes : vSphere Hypervisor, vMotion, High Availability, Data Protection, vShield Endpoint et vSphere Replication. Le descriptif de cette offre commerciale est consultable sur le site de l'éditeur.

Plateforme Citrix
La solution Citrix XenServer est intéressante, car le produit est passé dans le domaine open source. Cependant pour bénéficier d'une assistance et d'un support, il faut se tourner vers la solution payante fournie par Citrix au prix de 400 € par processeur.

Plateforme Microsoft
L'éditeur Microsoft propose sa solution de virtualisation dans deux éditions, Datacenter et Standard. L'édition Standard est limitée à deux machines virtuelles par licence. La

tarification, commune aux deux éditions, est fonction du nombre de processeurs et de licences d'accès client (CAL).

Plateforme Proxmox Server Solutions
L'éditeur Proxmox Server solutions propose un ensemble de services autour la solution de virtualisation libre Proxmox Virtual Environment. Le support professionnel permet d'accéder au dépôt de « Proxmox VE Enterprise » pour les mises à jour logicielles avancées, les mises à jour de sécurité, ainsi qu'au service technique. Ces services sont payants, de l'ordre de 4 à 66 €/mois et par processeur.

Éditeurs logiciels partenaires
Des éditeurs logiciels, partenaires des éditeurs de solution de virtualisation, proposent des logiciels très complets dédiés à la gestion de la sauvegarde et la restauration des machines virtuelles comme, par exemple, le logiciel **Veeam Backup** (http://www.veeam.com/fr/buy-veeam-backup-replication.html).
Compte tenu de la fluctuation des politiques commerciales d'une année sur l'autre, avant tout investissement, il faut prendre contact avec l'éditeur et plusieurs revendeurs agréés.