# SECURITE INFORMATIQUE

# RÉSUMÉ

La sécurité est un enjeu majeur des technologies numériques modernes. Avec le développement de l'Internet et de la notion du partage en général, les besoins en sécurité sont de plus en plus importants. Le développement d'applications Internet telles que le commerce électronique, les applications médicales ou la vidéoconférence, implique de nouveaux besoins comme, l'identification des entités communicantes, l'intégrité des messages échangés, la confidentialité de la transaction, l'authentification des entités, l'anonymat du propriétaire du certificat, l'habilitation des droits, la procuration, etc..

Qu'il s'agisse de données médicales, fiscales ou bancaires, le besoin en sécurité est essentiel afin de crédibiliser le système, tout en respectant à la fois les besoins des utilisateurs et des applications. Cette sécurité a néanmoins un prix : celui de l'établissement de la confiance entre les partenaires en communication. La confiance des utilisateurs passe par la sécurisation des transactions, en utilisant par exemple le chiffrement, la signature électronique et les certificats.

Le travail présenté dans ce mémoire, consiste en la proposition d'une architecture réseau sécurisée

Ce mémoire sera constitué de deux grandes parties. La première traitera, les enjeux actuels de la sécurité dans le monde, les types d'attaques qui s'appuient essentiellement sur des vulnérabilités humaines, systèmes et logiciels. Puis on parlera des technologies et des solutions mises en place sur le marché afin de mieux sécuriser son réseau d'entreprise. Dans la seconde partie, on déploiera une maquette de sécurité complète selon une architecture bien spécifique afin de pallier aux problèmes cités dans la première partie.

**SECURITE INFORMATIQUE**

# TABLE DES MATIÈRES

# INDEX DES FIGURES

# INDEX DES TABLEAUX

## Objectifs

L'objectif de cette partie est de traiter les points suivants :

- Présentation du projet
- Enjeux de la sécurité au sein de l'entreprise
- Définition des technologies œuvrant pour la sécurité des réseaux
- Présentation des solutions de sécurité réseau existantes sur le marché

# I. PRÉSENTATION DU PROJET

## 1. Objectif

« La sécurité informatique est tout un processus ». Afin de garder un très bon niveau de sécurité, il faut des contrôles réguliers (audits / tests d'intrusion), des règles respectées (politiques de sécurité) et des solutions intelligemment déployées (Firewalls applicatifs, Proxies, etc.). Le tout fait que la sécurité converge vers des niveaux satisfaisants mais jamais parfaits. Si une composante s'affaiblit c'est tout le processus qui est en danger.

L'objectif du projet est de répondre à une partie de la problématique de la sécurité Informatique au sein des entreprises marocaines. La solution proposée au niveau de ce projet ne cadre que la partie liée à l'architecture réseau, qui représente un maillon parmi d'autres dans la politique de sécurité de l'entreprise. Cette solution a été conçue de façon modulaire dans le but de respecter les différents besoins des entreprises. Allant de la simple utilisation d'un Firewall jusqu'à l'utilisation des certificats avec les PKI « Public Key Infrastructure » pour l'authentification, le VPN « Virtual Private Network » – IPSEC pour le cryptage des données et les IDS "Intrusion Detection System » pour la détection des intrusions.

Le modèle réseau de l'entreprise qui sera utilisé lors de ce projet est celui mentionné dans la Figure 1 se trouvant ci-dessous.

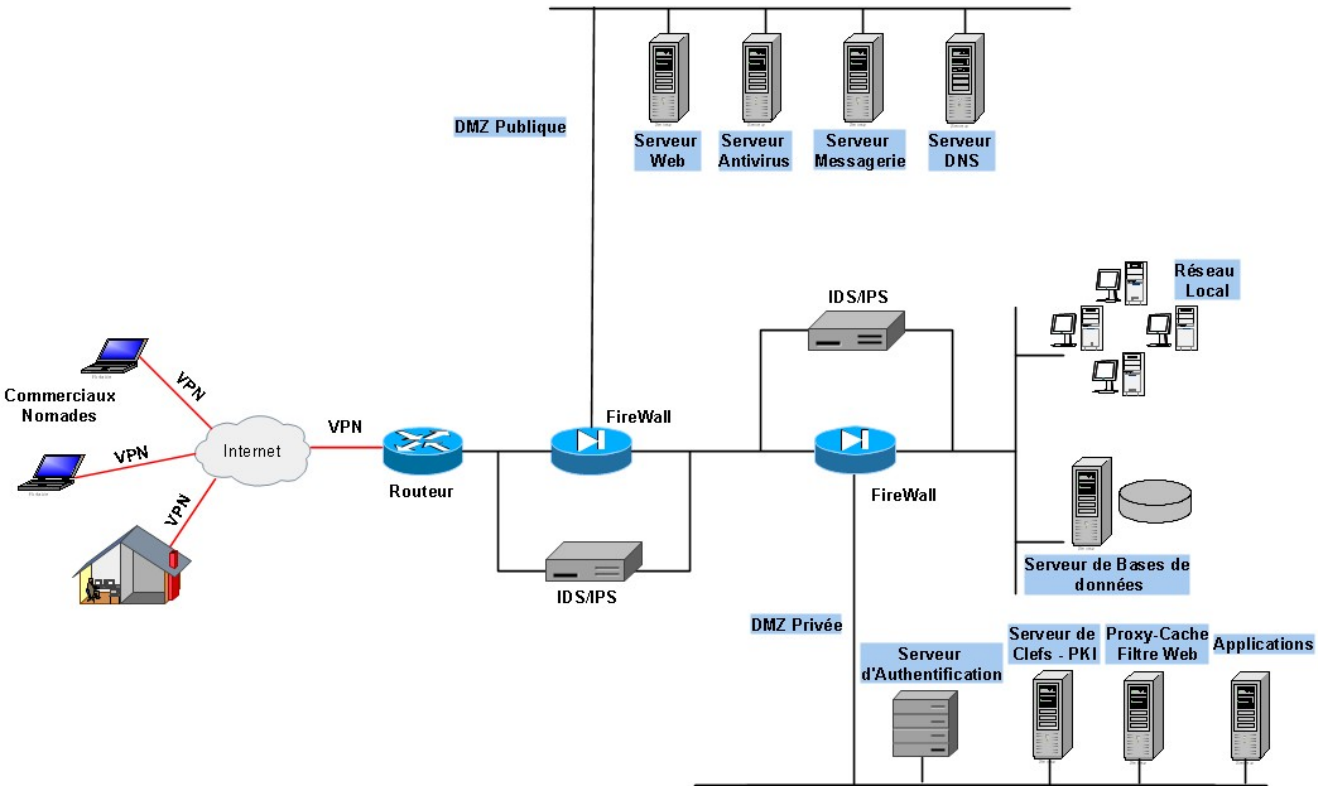



**Figure 1 :** Schéma réseau complet de la maquette

Ce modèle est constitué de quatre grandes parties qui sont les suivantes :

- **Extérieur :** Cette partie concerne toutes les entités qui sont à l'extérieur de l'entreprise. Ces entités peuvent être des commerciaux nomades qui transmettent leurs données, des employés qui veulent avoir accès à leurs comptes, des internautes voulant naviguer sur le site institutionnel de l'entreprise ou des partenaires commerciaux qui veulent faire des échanges à travers l'Extranet de l'entreprise.
- **DMZ Publique :** Cette partie de l'architecture contiendra les serveurs et les services accessibles de l'extérieur. On trouvera par exemple le serveur Web, le serveur de messagerie, le serveur de résolution de Noms – DNS et le serveur d'antivirus pour analyser le trafic entrant. Cette partie sera au réseau interne seulement pour la messagerie.
- **DMZ Privée** : Cette DMZ est plus sécurisée que la DMZ Publique. Elle sera seulement accessible à partir du réseau Interne et de la DMZ Publique selon des règles bien définies. Cette partie contiendra un serveur d'authentification et un serveur de clefs pour l'authentification des utilisateurs. Un proxy-cache et un filtre Web. Enfin, on mettra un serveur d'applications spécifiques à l'entreprise.

- **Réseau Interne :** Cette partie regroupera les différents utilisateurs de l'entreprise. Elle doit être la plus sécurisée des différentes autres parties. C'est pour cela qu'elle n'est pas accessible de l'extérieur.

Il est à noter qu'on a utilisé des IDS au niveau de chaque Firewall afin d'analyser le trafic réseau, et de remonter toute anomalie ou comportement anormal qui peut correspondre à une attaque.

Toutes les technologies qui ont été mentionnées dans ce chapitre, seront expliquées en détail dans le chapitre 3 de ce document.

# II. Enjeux de la sécurité au sein de l'entreprise.

Avant d'aborder le domaine technique, il est préférable de prendre un peu de recul et de considérer la sécurité dans son ensemble, pas comme une suite de technologies ou de processus remplissant des besoins bien spécifiques, mais comme une activité à part entière pour laquelle s'appliquent quelques règles (axiomes) simples.

- Pour une entreprise ou une institution connectée à l'Internet, le problème n'est pas savoir si on va se faire attaquer mais quand cela va arriver. Une solution est donc de repousser le risque dans le temps et dans les moyens à mettre en œuvre en augmentant le niveau de sécurité permettant d'écarter les attaques quotidiennes, pas forcément anodines et non spécifiquement ciblées.
- Aucun système d'information n'est 100% sûr.

Ces deux premières règles ne sont pas du tout les manifestations d'une paranoïa mais bien un simple constat qu'il est bon d'avoir toujours en tête pour ne pas se sentir – à tort – à l'abri de tout « danger ». En sécurité informatique, on ne parle pas d'éliminer complètement les risques mais de les réduire au minimum par rapport aux besoins/contraintes d'affaires. Il ne faut pas oublier non plus de considérer les actions provenant de l'intérieur de l'organisation, qui forment une partie (la majorité selon certaines données) non négligeable des sources d'attaques.

## 1. La sécurité informatique : C'est quoi ?

Nous pouvons considérer que la sécurité informatique est divisé e en deux grands domaines :

- La sécurité organisationnelle
- La sécurité technique

La sécurité organisationnelle concerne la politique de sécurité d'une société (code de bonne conduite, méthodes de classification et de qualification des risques, plan de secours, plan de continuité, …).

Une fois la partie organisationnelle traitée, il faut mettre en œuvre toutes les recommandations, et plans dans le domaine technique de l'informatique, afin de sécuriser les réseaux et systèmes : cet aspect relève de la sécurité technique.

Le périmètre de la sécurité est très vaste :

- La sécurité des systèmes d'information
- La sécurité des réseaux
- La sécurité physique des locaux
- La sécurité dans le développement d'applications

- La sécurité des communications
- La sécurité personnelle
- …

Un risque se définit comme une combinaison de menaces exploitant une vulnérabilité et pouvant avoir un impact. De manière générale, les risques sont soit des causes (attaques, pannes, …) soit des conséquences (fraude, intrusion, divulgation …).

Les objectifs de la sécurité sont simples : empêcher la divulgation de données confidentielles et la modification non autorisée de données.

Nous retrouvons ainsi les principes fondamentaux de la sécurité :

- La confidentialité,
- L'intégrité,
- L'authentification,
- Le contrôle d'accès,
- La non répudiation[1].

Une seule entrave à l'un de ces principes remet toute la sécurité en cause.

## 2. La sécurité informatique : Pourquoi ?

Une politique de sécurité informatique mal gérée peut conduire à trois types d'impacts négatifs :

- La pénétration d'un réseau,
- Le vol ou détérioration d'informations,
- Les perturbations.

La pénétration d'un réseau ou système peut se faire soit par vol d'identité soit par intrusion. Ce vol d'identité peut se faire par vol du « nom d'utilisateur/mot de passe » de connexion au système d'information. Tous les moyens sont bons pour obtenir des informations. On peut citer à titre d'exemples :

- L'écoute des réseaux,
- L'ingénierie sociale[2],

[1] Assurance qu'un message est bien parti d'un émetteur spécifié pour arriver à un récepteur lui aussi spécifié. En fait, c'est surtout l'émetteur qui est visé, il ne peut pas « répudier » son message (dire qu'il ne l'a pas envoyé)

[2] Approche utilisée afin de soutirer des informations à un utilisateur sans même qu'il ne s'en rende compte. Par exemple, voler une carte de crédit, puis téléphoner au possesseur légitime de la carte en se faisant passer pour sa banque, et lui demander son code confidentiel. Ce genre de techniques se base sur la naïveté et le manque de suspicion des gens.

- Ou tout simplement le fait de regarder par-dessus l'épaule de l'utilisateur qui s'authentifie.

La pénétration d'un réseau ou système peut aussi se faire à distance ; par exemple un hacker[3] peut pénétrer le réseau via un serveur de messagerie. Mais il existe d'autres méthodes moins visibles, comme l'installation d'un logiciel à l'insu de l'utilisateur, suite à la lecture d'une page web sur un site. Ainsi un script contenu dans la page web chargée, peut envoyer des messages de votre logiciel de messagerie vers d'autres personnes.

### .3. La sécurité informatique : Comment ?

Des produits existent sur le marché, qui permettent d'éviter ces problèmes. Nous trouverons par exemple des antivirus, des Firewall, du VPN, de la signature numérique, du proxy[4], etc.

Chacune des ces technologies ou produits dispose d'une couverture spécifique. Par exemple, l'antivirus va permettre de bloquer les virus ou Chevaux de Troie entrants par la messagerie ou par échange de fichiers.

Le très connu firewall, dont la configuration n'est ni simple, ni rapide va permettre de filtrer les échanges entre deux réseaux afin de limiter les accès, et de détecter les éventuelles tentatives d'intrusion.

Une fonctionnalité supplémentaire a tendance à se retrouver intégrée dans les firewalls : le VPN. Celui-ci permet de garantir la confidentialité des échanges d'informations passant par son intermédiaire en chiffrant[5] le flux d'informations.

Il est possible de mettre en outre une signature numérique en place. Ainsi, dans le système de messagerie, le destinataire du message sera certain de l'identité de l'émetteur et de l'intégrité[6] du message. Il pourra être le seul lecteur si le message a été chiffré (clef privé e/clef publique).

Le serveur Web reste vulnérable, car accessible directement depuis l'extérieur du réseau. La mise en place d'un reverse proxy[7] résout l'affaire. En effet, toute tentative de connexion au serveur Web parvient au serveur proxy, qui lui-même envoie une requête au serveur Web. Ainsi le serveur Web n'est plus accessible depuis l'extérieur du réseau.

Les certificats étant utilisés pour la messagerie, pour les VPN ou pour chiffrer les documents, il est possible de regrouper tous ces certificats dans une PKI. La PKI est un

[3]

[4] Serveur recevant des requêtes qui ne lui sont pas destinées et qui les transmet à d'autres serveurs.

[5]

[6] Assurance que le contenu de l'information n'a pas été altéré ou modifié au cours d'un échange.

[7] Comme un serveur proxy, mais préservant les accès directs depuis l'Internet vers les serveurs internes.

système de gestion de clef publique permettant d’en assurer la fiabilité. La PKI pose des problèmes organisationnels mais pas techniques.

# III. DÉFINITION DES TECHNOLOGIES ŒUVRANT POUR LA SÉCURITÉ DES RÉSEAUX

## 1. La Cryptologie

La cryptographie permet l'échange sûr de renseignements privés et confidentiels. Un texte compréhensible est converti en texte inintelligible (chiffrement), en vue de sa transmission d'un poste de travail à un autre. Sur le poste récepteur, le texte chiffré est reconverti en format intelligible (déchiffrement). On peut également utiliser la cryptographie pour assurer l'authentification, la non-répudiation et l'intégrité de l'information, grâce à un processus cryptographique spécial appelé signature numérique. Celle-ci permet de garantir l'origine et l'intégrité de l'information échangée, et aussi de confirmer l'authenticité d'un document.

### 1.1 Cryptographie Symétrique

La cryptographie classique repose sur l'utilisation d'une « clef » mathématique qui sert au chiffrement et au déchiffrement des données. Ainsi, pour faire parvenir un message de façon sûre, il faut le chiffrer à l'aide d'une clef connue uniquement de l'expéditeur et du destinataire, puis faire parvenir au destinataire prévu à la fois le message et la clef de façon à ce que seul celui-ci puisse décoder le message. La cryptographie classique est également appelée cryptographie symétrique.

### 1.2 Cryptographie Asymétrique

La cryptographie à clef publique utilise deux clefs. La première demeure privée, tandis que la seconde est publique. Si l'on utilise la clef publique pour chiffrer un message, la clef privée permet de le déchiffrer. Autrement dit, il suffit de chiffrer un message à expédier à l'aide de la clef publique du destinataire, et ce dernier peut ensuite utiliser la clef privée pour le déchiffrer

### 1.3 La signature numérique

La cryptographie à clef publique[8] rend possible l'utilisation des signatures numériques. Celles-ci permettent de corroborer l'origine d'un message. Pour «signer» un message, on utilise une fonction mathématique qui produit un résumé du message (Hash). Le résumé obtenu est chiffré à l'aide de la clef privée de l'expéditeur. Le résultat, qui constitue la signature numérique, est annexé au message. Le destinataire du message peut ensuite s'assurer de l'origine du message et de l'intégrité de l'information qu'il contient en déchiffrant la signature numérique au moyen de la clef publique de l'expéditeur, puis en comparant le résultat avec le résumé obtenu en appliquant la même fonction mathématique au message reçu. Cela semble un peu compliqué, mais en pratique, il suffit de cliquer sur une icône à l'écran pour lancer tout le processus.

## 2. VPN « Virtual Private Network »

8

VPN ont aujourd'hui pris une place importante dans les réseaux informatique et l'informatique distribuées. Nous verrons ici quelles sont les principales caractéristiques des VPN. Nous nous intéresserons ensuite au protocole IPSEC permettant leur mise en place.

## 2.1 Principe général

Un réseau VPN repose sur un protocole appelé « protocole de tunneling ». Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

## 2.2 Fonctionnalités des VPN

### 2.2.1 Les VPN d'accès

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

- La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée, ce qui peut poser des problèmes de sécurité.
- Sur la deuxième méthode, ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée.

- Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification "login / mot de passe".

### 2.2.2 L'Intranet VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage « infaillible ». Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

#### 2.2.3 L'Extranet VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci.

#### 2.2.4 Caractéristiques fondamentales d'un VPN

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

- Authentification d'utilisateur. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel.
- Gestion d'adresses. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.
- Cryptage des données. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- Gestion de clefs. Les clefs de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

## 2.3 Protocoles utilisés pour réaliser une connexion VPN

#### 2.3.1 Le protocole IPSEC

IPSEC, définit par la RFC 2401, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau IPV4 étant largement déployé et la migration vers IPV6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à IPV4 et IPV6. Ces mécanismes sont couramment désignés par le terme IPSEC pour **IP Security Protocols**. IPSEC est basé sur deux mécanismes. Le premier, AH, pour **Authentication Header** vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par ce protocole ne sont pas encodées. Le second, ESP, pour **Encapsulating Security Payload** peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement. Enfin, le protocole IKE permet de gérer les échanges ou les associations entre protocoles de sécurité. Avant de décrire ces différents protocoles, nous allons exposer les différents éléments utilisés dans IPSEC.

Les mécanismes mentionnés ci-dessus font bien sûr appel à la cryptographie et utilisent donc un certain nombre de paramètres (algorithmes de chiffrement utilisés, clefs, mécanismes sélectionnés...) sur lesquels les tiers communicants doivent se mettre d'accord. Afin de gérer ces paramètres, IPSEC a recours à la notion d'association de sécurité (Security Association, SA).

Une association de sécurité IPSEC est une « connexion » simplexe qui fournit des services de sécurité au trafic qu'elle transporte. On peut aussi la considérer comme une structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée.

Une SA est unidirectionnelle ; en conséquence, protéger les deux sens d'une communication classique requiert deux associations, une dans chaque sens. Les services de sécurité sont fournis par l'utilisation soit de AH soit de ESP.

Chaque association est identifiée de manière unique à l'aide d'un triplet composé de :

- L'adresse de destination des paquets,
- L'identifiant du protocole de sécurité utilisé (AH ou ESP),
- Un index des paramètres de sécurité (Security Parameter Index, SPI). Un SPI est un bloc de 32 bits inscrit en clair dans l'en-tête de chaque paquet échangé ; il est choisi par le récepteur.

Pour gérer les associations de sécurité actives, on utilise une « base de données des associations de sécurité » (Security Association Database, SAD). Elle contient tous les paramètres relatifs à chaque SA et sera consultée pour savoir comment traiter chaque paquet reçu ou à émettre.

Les protections offertes par IPSEC sont basées sur des choix définis dans une « base de données de politique de sécurité » (Security Policy Database, SPD). Cette base de données est établie et maintenue par un utilisateur, un administrateur système ou une application mise en place par ceux-ci. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer ou rejeté.

### 2.3.2 Principe de fonctionnement du protocole IPSEC

On distingue deux situations :

- Trafic sortant

  Lorsque la couche IPSEC reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD). Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPSEC fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.

- Trafic entrant

  Lorsque la couche IPSEC reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services IPSEC et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la Spd est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité.

Dans le cas où le paquet reçu est un paquet IP classique, la SPD permet de savoir s'il a néanmoins le droit de passer. Par exemple, les paquets IKE sont une exception. Ils sont traités par IKE, qui peut envoyer des alertes administratives en cas de tentative de connexion infructueuse.

### 2.3.3 Le protocole AH « Authentication Header »

L'absence de confidentialité permet de s'assurer que ce standard pourra être largement répandu sur Internet, y compris dans les endroits où l'exportation, l'importation ou l'utilisation du chiffrement dans des buts de confidentialité est restreint par la loi.

Son principe est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données incluses dans le datagramme. Ce bloc de données est appelé « valeur de vérification d'intégrité » (Integrity Check Value, ICV). La protection contre le rejet se fait grâce à un numéro de séquence.

### 2.3.4 Le protocole ESP « Encapsulating Security Payload »

ESP peut assurer au choix, un ou plusieurs des services suivants :

- Confidentialité (confidentialité des données et protection partielle contre l'analyse du trafic si l'on utilise le mode tunnel).
- Intégrité des données en mode non connecté et authentification de l'origine des données, protection contre le rejeu.

La confidentialité peut être sélectionnée indépendamment des autres services, mais son utilisation sans intégrité/authentification (directement dans ESP ou avec AH) rend le trafic vulnérable à certains types d'attaques actives qui pourraient affaiblir le service de confidentialité.

Le champ bourrage peut être nécessaire pour les algorithmes de chiffrement par blocs ou pour aligner le texte chiffré sur une limite de 4 octets. Les données d'authentification ne sont présentes que si ce service a été sélectionné.

Voyons maintenant comment est appliquée la confidentialité dans ESP.

L'expéditeur :

- Encapsule, dans le champ « charge utile » d'ESP, les données transportées par le datagramme original et éventuellement l'en-tête IP (mode tunnel).
- Ajoute si nécessaire un bourrage.
- Chiffre le résultat (données, bourrage, champs longueur et en-tête suivant).
- Ajoute éventuellement des données de synchronisation cryptographiques (vecteur d'initialisation) au début du champ « charge utile ».

### 2.3.5 La gestion des clefs pour IPSEC : ISAKMP et IKE

Les protocoles sécurisés présentés dans les paragraphes précédents ont recours à des algorithmes cryptographiques et ont donc besoin de clefs. Un des problèmes fondamentaux d'utilisation de la cryptographie est la gestion de ces clefs. Le terme « gestion » recouvre la génération, la distribution, le stockage et la suppression des clefs.

IKE (Internet Key Exchange) est un système développé spécifiquement pour IPSEC qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'Internet. Lorsqu'il est utilisé pour IPSEC, IKE est de plus complété par un « Domaine d'interprétation » pour IPSEC.

#### 2.3.5.1 ISAKMP (Internet Security Association and Key Management Protocol)

ISAKMP a pour rôle la négociation, l'établissement, la modification et la suppression des associations de sécurité et de leurs attributs. Il pose les bases permettant de construire divers protocoles de gestion des clefs (et plus généralement des associations de sécurité). Il comporte trois aspects principaux :

Il définit une façon de procéder, en deux étapes appelées phase 1 et phase 2 : dans la première, un certain nombre de paramètres de sécurité propres à ISAKMP sont mis en place, afin d'établir entre les deux tiers un canal protégé ; dans un second temps, Ce canal est utilisé pour négocier les associations de sécurité pour les mécanismes de sécurité que l'on souhaite utiliser (AH et Esp par exemple).

Il définit des formats de messages, par l'intermédiaire de blocs ayant chacun un rôle précis et permettant de former des messages clairs.

Il présente un certain nombre d'échanges types, composés de tels messages, qui permettant des négociations présentant des propriétés différentes : protection ou non de l'identité, perfect forward secrecy...

#### 2.3.5.2 IKE (Internet Key Exchange)

IKE utilise ISAKMP pour construire un protocole pratique. Il comprend quatre modes :

- Le mode principal (Main mode)
- Le mode agressif (Aggressive Mode)
- Le mode rapide (Quick Mode)
- Le mode nouveau groupe (New Groupe Mode)

Main Mode et Aggressive Mode sont utilisés durant la phase 1, Quick Mode est un échange de phase 2. New Group Mode est un peu à part : Ce n'est ni un échange de phase 1, ni un échange de phase 2, mais il ne peut avoir lieu qu'une fois qu'une SA ISAKMP est établie ; il sert à se mettre d'accord sur un nouveau groupe pour de futurs échanges Diffie-Hellman.

**Phase 1 : Main Mode et Aggressive Mode**

Les attributs suivants sont utilisés par IKE et négociés durant la phase 1 : un algorithme de chiffrement, une fonction de hachage, une méthode d'authentification et un groupe pour Diffie-Hellman.
Trois clefs sont générées à l'issue de la phase 1 : une pour le chiffrement, une pour l'authentification et une pour la dérivation d'autres clefs. Ces clefs dépendent des cookies, des aléas échangés et des valeurs publiques Diffie-Hellman ou du secret partagé préalable. Leur calcul fait intervenir la fonction de hachage choisie pour la SA ISAKMP et dépend du mode d'authentification choisi.

**Phase 2 : Quick Mode**

Les messages échangés durant la phase 2 sont protégés en authenticité et en confidentialité grâce aux éléments négociés durant la phase 1. L'authenticité des messages est assurée par l'ajout d'un bloc Hash après l'en-tête ISAKMP et la confidentialité est assurée par le chiffrement de l'ensemble des blocs du message.
Quick Mode est utilisé pour la négociation de SA pour des protocoles de sécurité donnés comme IPSEC. Chaque négociation aboutit en fait à deux SA, une dans chaque sens de la communication. Plus précisément, les échanges composant ce mode ont le rôle suivant :

- Négocier un ensemble de paramètres IPSEC (paquets de SA)
- Échanger des nombres aléatoires, utilisés pour générer une nouvelle clef qui dérive du secret généré en phase 1 avec le protocole Diffie-Hellman. De façon optionnelle, il est

possible d'avoir recours à un nouvel échange Diffie-Hellman, afin d'accéder à la propriété de Perfect Forward Secrecy, qui n'est pas fournie si on se contente de générer une nouvelle clef à partir de l'ancienne et des aléas.

- Optionnellement, identifier le trafic que ce paquet de SA protégera.

**Les groupes : New Groupe Mode**

Le groupe à utiliser pour Diffie-Hellman peut être négocié, par le biais du bloc SA, soit au cours du Main Mode, soit ultérieurement par le biais du New Group Mode. Dans les deux cas, il existe deux façons de désigner le groupe à utiliser :

- Donner la référence d'un groupe prédéfini : il en existe actuellement quatre, les quatre groupes Oakley (deux groupes MODP et deux groupes EC2N).
- Donner les caractéristiques du groupe souhaité : type de groupe (MODP, ECP, EC2N), nombre premier ou polynôme irréductible, générateurs...

### 2.3.6 Les deux modes de fonctionnement d'IPSEC

Le mode transport prend un flux de niveau transport du modèle OSI et réalise les mécanismes de signature et de chiffrement puis transmet les données à la couche IP. Dans Ce mode, l'insertion de la couche IPSEC est transparente entre TCP et IP. TCP envoie ses données vers IPSEC comme il les enverrait vers IPv4.

L'inconvénient de ce mode réside dans le fait que l'en-tête extérieur est produit par la couche IP c'est-à-dire sans masquage d'adresse. De plus, le fait de terminer les traitements par la couche IP ne permet pas de garantir la non-utilisation des options IP potentiellement dangereuses. L'intérêt de ce mode réside dans une relative facilitée de mise en œuvre.

Dans le mode tunnel, les données envoyées par l'application traversent la pile de protocole jusqu'à la couche IP incluse, puis sont envoyées vers le module IPSEC. L'encapsulation IPSEC en mode tunnel permet le masquage d'adresses. Le mode tunnel est utilisé entre deux passerelles de sécurité (routeur, firewall, ...) alors que le mode transport se situe entre deux hôtes.

## 5. Définition des PKI « Public Key Infrastructure »

### 5.1 Infrastructure à Clef publique

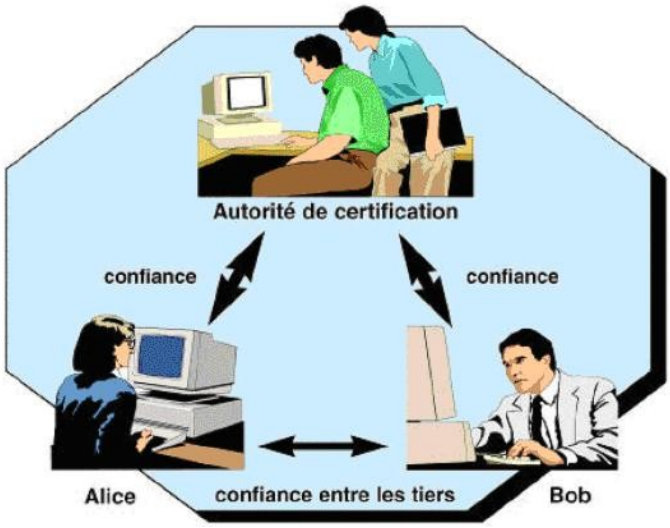
Une PKI assure la sécurité des transactions électroniques et l'échange de renseignements sensibles grâce à des clefs cryptographiques et à des certificats. Une PKI offre divers services : confidentialité, contrôle d'accès, intégrité, authentification, services de non-répudiation pour les transactions commerciales électroniques et les applications informatiques connexes. En outre, elle gère la production et la distribution des paires de clefs publique et privée, et diffuse la clef publique (ainsi que l'identification de l'utilisateur) sous forme de "certificat" sur des babillards électroniques publics

Une PKI comprend ce qui suit :

- Autorité de certification ;
- Annuaire de certificats ;
- Système de révocation de certificats ;
- Système de sauvegarde et de récupération de clefs ;
- Soutien à la non-répudiation ;
- Mise à jour automatique des clefs ;
- Gestion de l'historique des clefs ;
- Horodatage ;
- Logiciel client interagissant de manière fiable et continue avec tout ce qui est énuméré ci-dessus.

Une PKI assure donc, avec un haut niveau de confiance, la protection des clefs privées, veille à ce que des clefs publiques spécifiques soient véritablement associées à des clefs privées spécifiques, et vérifie que les parties qui possèdent une paire de clefs publique et privée sont bien celles qu'elles prétendent être.

## 5.2 Confiance entre les tiers




On entend par la confiance entre les tiers, le fait que deux entités ou deux personnes aient implicitement confiance l'une en l'autre, même si elles n'ont pas établi au préalable de liens commerciaux ou personnels. Dans un tel cas, les deux parties ont cette confiance implicite et mutuelle parce qu'elles partagent une relation avec une tierce partie commune, et parce que celle-ci se porte garante de la légitimité des deux premières parties.

La confiance entre les tiers est une exigence fondamentale de toute implantation à grande échelle de services de sécurité reposant sur la cryptographie à clef publique. En effet, celle-ci nécessite l'accès à la clef publique d'un utilisateur. Toutefois, dans un réseau de grande taille, il est impossible et irréaliste de s'attendre à ce que chaque utilisateur établisse au préalable des relations avec tous les autres utilisateurs. En outre, comme la clef publique d'un utilisateur doit être accessible à l'ensemble des autres utilisateurs, le lien entre une clef publique et une personne donnée doit être garanti par une tierce partie de confiance, afin que nul ne puisse se faire passer pour un utilisateur légitime. Une tierce partie de confiance, dont les mécanismes sont sûrs, permet aux utilisateurs d'avoir implicitement confiance dans toute clef publique certifiée par cette tierce partie.

Un agent de certification tiers est appelé **Autorité de Certification** « CA [9]».

## 5.3 Autorité de Certification

Une CA est une entité de confiance dont la responsabilité est essentiellement de certifier l'authentification des utilisateurs. La fonction d'une CA est très analogue à celle d'un bureau chargé de l'émission des passeports dans un gouvernement. Un passeport est un document authentique, émis par une autorité appropriée, qui certifie que son détenteur est bien la personne qu'elle prétend être. C'est à toute fin pratique le «document d'identité» de la personne. Tout pays qui a confiance en l'autorité d'un bureau de passeports d'un pays étranger honorera les passeports des ressortissants de ce pays. Ceci illustre bien ce qu'on entend par confiance entre les tiers.

Tout comme un passeport, l'«identité électronique» de l'utilisateur d'un réseau, émise par une CA, est une preuve que cet utilisateur est connu par l'autorité de certification. Par conséquent, grâce au mécanisme de confiance entre les tiers, quiconque a confiance dans la CA peut avoir confiance en l'identité de l'utilisateur. Les critères qui établissent les CAs et les politiques qui en balisent le cadre de fonctionnement sont d'une importance primordiale pour déterminer le degré de confiance que l'on peut avoir dans les CAs.

## 5.4 Certificats

Pour un utilisateur du réseau, un certificat est l'équivalent électronique d'un passeport. Il contient de l'information que l'on peut utiliser pour vérifier l'identité du détenteur (exemple : son nom). Un élément d'information crucial contenu dans le certificat d'un utilisateur est sa clef publique. Celle-ci peut servir soit à chiffrer les données destinées au détenteur du certificat, soit à vérifier la signature numérique du détenteur.

La notion de certificat soulève plusieurs questions au sujet du degré de « confiance ». Par exemple, au sujet de la protection de l'information dans un certificat : comment peut-on être sûr que le nom et la clef publique dans un certificat appartiennent véritablement au présumé détenteur de celui-ci ?

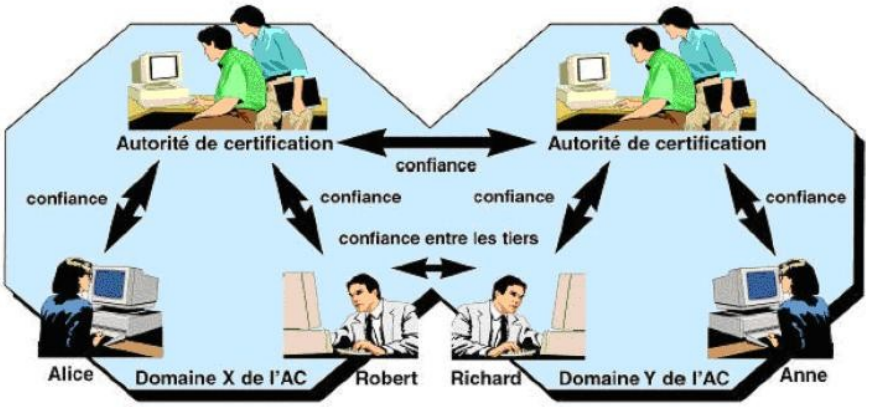
En fait, sans ce niveau de confiance, la cryptographie à clef publique n'est d'aucune utilité, car il n'y aurait aucune garantie que l'information est chiffrée pour la bonne personne, ou qu'une signature numérique puisse être associée à une personne donnée.

Afin d'assurer la légitimité de la clef publique d'un utilisateur et des autres renseignements (par exemple, son nom) qui figurent dans un certificat, une CA signe numériquement l'information du certificat au moyen de sa propre clef de signature privée. La signature numérique de la CA offre ainsi trois éléments importants pour la sécurité et la confiance à l'égard du certificat. Tout d'abord, par définition, une signature numérique valide sur un certificat est garantie de son intégrité. En deuxième lieu, comme la CA est la seule entité qui a accès à sa propre clef de signature privée, quiconque vérifie la signature de la CA sur le certificat est assuré que c'est seulement la CA qui

[9] Certification Authority

peut avoir créée et signée ce certificat. Enfin, comme seul la CA a accès à sa clef de signature privée, la CA ne peut pas nier avoir signé le certificat. Ce concept est souvent appelé non-répudiation.

### 5.5 Certification Réciproque




La certification réciproque est tout simplement un prolongement du concept de confiance entre les tiers. Dans ce processus, deux CA échangent en toute sécurité de l'information sur les clefs cryptographiques, de sorte que chacun puisse certifier efficacement la fiabilité des clefs de l'autre. D'un point de vue technique, il s'agit de créer des « Certificats réciproques » entre les deux CA. Lorsqu'une CA d'une organisation et une CA d'une deuxième organisation font cette certification réciproque, la CA de la première organisation crée et signe numériquement un certificat contenant la clef publique de la CA de la deuxième organisation. De la même manière, la deuxième organisation crée et signe un certificat contenant la clef publique de la CA de la première organisation. Les utilisateurs relevant d'une CA peuvent donc implicitement avoir confiance dans les utilisateurs relevant de l'autre CA.

Comme la certification réciproque élargit le concept de confiance entre les tiers, il importe que chaque domaine relevant d'une CA n'ait aucune réserve à la vigilance des politiques et pratiques de sécurité de l'autre domaine en ce qui concerne l'émission des certificats et la réalisation de ses activités. La certification croisée va donc au-delà du simple échange d'information sur les clefs cryptographiques.

## 7. Firewall

### 7.1 Qu'est-ce qu'un Firewall ?

De nos jours, toutes les entreprises possédant un réseau local possèdent aussi un accès à Internet, afin d'accéder à la manne d'information disponible sur le réseau des réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable... et dangereuse en même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, parfois gratuites, de destruction, vol d'informations confidentielles, ... Les mobiles sont nombreux et dangereux.

Pour parer à ces attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basé sur un firewall. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela

représente une sécurité supplémentaire rendant le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur. En effet, des employés peuvent s'adonner à des activités que l'entreprise ne cautionne pas, le meilleur exemple étant le jeu en ligne. En plaçant un firewall limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Le firewall[10] propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données. Il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseaux suivantes telles que montrées dans la Figure 2 :

- Une interface pour le réseau à protéger (réseau interne)
- Une interface pour le réseau externe

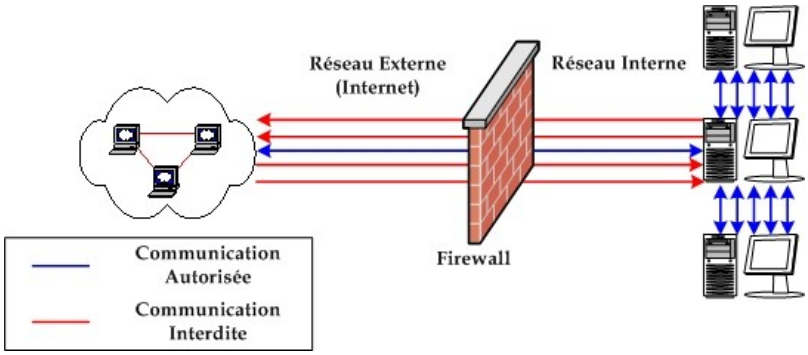



**Figure 2 :** Schéma d'une architecture réseau utilisant un Firewall

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) et un ou plusieurs réseaux externes. Il est possible de mettre un système Firewall sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic ;
- Le système soit sécurisé ;
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

Dans le cas où le système Firewall est fourni dans une boîte noire « clef en main », on utilise le terme d'« Appliance ».

## 7.2 Fonctionnement d'un système Firewall

Un système Firewall contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (allow)
- De bloquer la connexion (deny)

[10] Terme Anglais, appelé aussi pare-feu, coupe-feu ou garde-barrière

- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées :

**« TOUT CE QUI N'EST PAS EXPLICITEMENT AUTORISÉ EST INTERDIT »**

- Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

### 7.2.1 Le filtrage simple de paquets

Un système Firewall fonctionne sur le principe du filtrage simple de paquets (en anglais « Stateless Packet Filtering »). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le Firewall et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- Adresse IP de la machine émettrice ;
- Adresse IP de la machine réceptrice ;
- Type de paquet (TCP, UDP, etc.) ;
- Numéro de port (un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). La plupart des dispositifs Firewall sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).

Le port 23 est par exemple souvent bloqué par défaut par les dispositifs Firewall car il correspond au protocole Telnet, permettant d'émuler un accès par terminal à une machine distante de manière à pouvoir exécuter des commandes à distance. Les données échangées par Telnet ne sont pas chiffrées, ce qui signifie qu'un individu est susceptible d'écouter le réseau et de voler les

éventuels mots de passe circulant en clair. Les administrateurs lui préfèrent généralement le protocole SSH[11], réputé sûr et fournissant les mêmes fonctionnalités que Telnet.

**Limites du Filtrage simple de paquets**

Le premier problème vient du fait que l'administrateur réseau est rapidement contraint à autoriser un trop grand nombre d'accès, pour que le Firewall offre une réelle protection. Par exemple, pour autoriser les connexions à Internet à partir du réseau privé, l'administrateur devra accepter toutes les connexions TCP provenant de l'Internet avec un port supérieur à 1024. Ce qui laisse beaucoup de choix à un éventuel pirate.

Il est à noter que de définir des ACL[12] sur des routeurs haut de gamme - c'est à dire, supportant un débit important - n'est pas sans répercussion sur le débit lui-même. Enfin, ce type de filtrage ne résiste pas à certaines attaques de type **IP Spoofing / IP Flooding**, la mutilation de paquet, ou encore certaines attaques de type **DoS**. Ceci est vrai sauf dans le cadre des routeurs fonctionnant en mode distribué. Ceci permettant de gérer les ACL directement sur les interfaces sans remonter à la carte de traitement central. Les performances impactées par les ACL sont alors quasi nulles.

### 7.2.2 Le filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente. La figure suivante illustre l'échange entre un Client et un Serveur FTP.

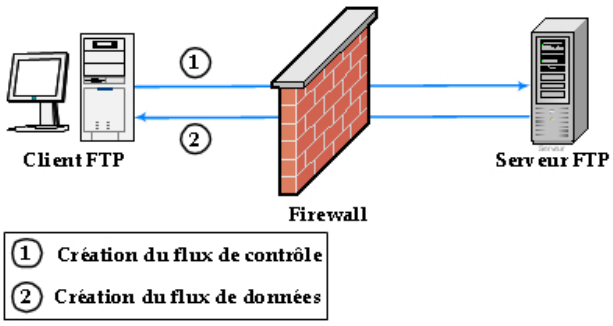



**Figure 3 :** Établissement de la connexion entre un Client et un Serveur FTP en passant par un Firewall

Ainsi, il est impossible avec un filtrage simple de paquets de prévoir les ports à laisser passer ou à interdire. Pour y remédier, le système de **filtrage dynamique de paquets** est basé sur l'inspection des couches 3 et 4 du modèle OSI, permettant d'effectuer un suivi des transactions

[11] **SSH** (*Secure Shell*) permet aux utilisateurs (ou bien des services TCP/IP) d'accéder à une machine à travers une communication chiffrée (appelée *tunnel*)
[12] Access Control List

entre le client et le serveur. Le terme anglo-saxon est **« Stateful inspection »** ou **« Stateful packet filtering »**, qui se traduit en « filtrage de paquets avec état ».

Un dispositif pare-feu de type « Stateful inspection » est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine situé de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en terme de sécurité.

**Limites du filtrage dynamique**

Tout d'abord, il convient de s'assurer que les deux techniques sont bien implémentées par les Firewalls, car certains constructeurs ne l'implémentent pas toujours correctement. Ensuite une fois que l'accès à un service a été autorisé, il n'y a aucun contrôle effectué sur les requêtes et réponses des clients et serveurs. Un serveur HTTP pourra donc être attaqué impunément.

Enfin les protocoles maisons utilisant plusieurs flux de données ne passeront pas, puisque le système de filtrage dynamique n'aura pas connaissance du protocole.

### 7.2.3 Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 « Couche application » du modèle OSI, contrairement au filtrage de paquets simple « Niveau 4 ». Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application.

Le filtrage applicatif permet, comme son nom l'indique, de filtrer les communications application par application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).

Un firewall effectuant un filtrage applicatif est appelé généralement « passerelle applicative » ou « proxy », car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

Il s'agit d'un dispositif performant, assurant une bonne protection du réseau, pour peu qu'il soit correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.

Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles afférentes pour être efficace.

**Limites du filtrage applicatif**

Le premier problème qui se pose est la finesse du filtrage réalisé par le proxy. Il est extrêmement difficile de pouvoir réaliser un filtrage qui ne laisse rien passer, vu le nombre de protocoles de niveau 7. En outre le fait de devoir connaître les règles protocolaires de chaque protocole filtré pose des problèmes d'adaptabilité à de nouveaux protocoles ou des protocoles maisons.

Mais il est indéniable que le filtrage applicatif apporte plus de sécurité que le filtrage de paquet avec état, mais cela se paie en performance. Ce qui exclut l'utilisation d'une technologie 100 % proxy pour les réseaux à gros trafic au jour d'aujourd'hui. Néanmoins d'ici quelques années, le problème technologique sera sans doute résolu.

Enfin, un tel système peut potentiellement comporter une vulnérabilité dans la mesure où il interprète les requêtes qui transitent par son biais. Ainsi, il est recommandé de dissocier le pare-feu (dynamique ou non) du proxy tel que montré dans la Figure 4, afin de limiter les risques de compromission.

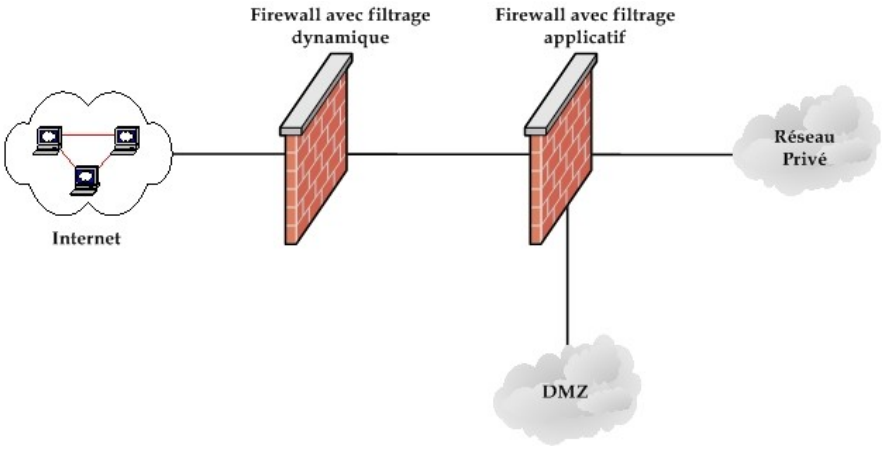



**Figure 4 :** Choix des Firewall dans une architecture réseau

## 7.3 Les différents types de Firewall

### 7.3.1 Les Firewall Bridge

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de Firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le Firewall est indétectable pour un hacker lambda. En effet, quand une requête ARP est émise sur le câble réseau, le Firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le Firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le

contourner est de passer outre ses règles de drop. Toute attaque devra donc « faire » avec ses règles, et essayer de les contourner.

Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence.

Ces Firewalls se trouvent typiquement sur les switchs.

| Avantages | Inconvénients |
|---|---|
| ♦ Impossible de l'éviter (les paquets passeront par ses interfaces)<br>♦ Peu coûteux | ♦ Possibilité de le contourner (il suffit de passer outre ses règles)<br>♦ Configuration souvent contraignante<br>♦ Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless) |

**Tableau 1 :** Avantages et inconvénients d'un Firewall Bridge

### 7.3.2 Les Firewalls matériels

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau. Souvent relativement peu flexibles en terme de configuration, ils sont aussi peu vulnérables aux attaques, car présent dans la « boite noire » qu'est le routeur. De plus, étant souvent très liés au matériel, l'accès à leur code est assez difficile, et le constructeur a eu toute latitude pour produire des systèmes de codes « signés » afin d'authentifier le logiciel (système RSA ou assimilés). Ce système n'est implanté que dans les firewalls haut de gamme, car cela évite un remplacement du logiciel par un autre non produit par le fabricant, ou toute modification de ce dernier, rendant ainsi le firewall très sûr. Son administration est souvent plus aisée que les Firewalls bridges, les grandes marques de routeurs utilisant cet argument comme argument de vente. Leur niveau de sécurité est de plus très bon, sauf découverte de faille éventuelle comme tout firewall. Néanmoins, il faut savoir que l'on est totalement dépendant du constructeur du matériel pour cette mise à jour, ce qui peut être, dans certains cas, assez contraignant. Enfin, seules les spécificités prévues par le constructeur du matériel sont implémentées. Cette dépendance induit que si une possibilité nous intéresse sur un firewall d'une autre marque, son utilisation est impossible. Il faut donc bien déterminer à l'avance ses besoins et choisir le constructeur du routeur avec soin.

| Avantages | Inconvénients |
|---|---|
| ♦ Intégré au matériel réseau | ♦ Dépendant du constructeur pour les |

| | |
|---|---|
| ♦ Administration relativement simple<br>♦ Bon niveau de sécurité | mises à jour<br>♦ Souvent peu flexible |

**Tableau 2 :** Avantages et inconvénients d'un Firewall matériel

### 7.3.3 Les Firewalls logiciels

Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories :

#### 7.3.3.1 Les Firewalls personnels

Ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

| Avantages | Inconvénients |
|---|---|
| ♦ Sécurité en bout de chaîne (Poste Client)<br>♦ Personnalisable assez facilement | ♦ Facilement contournable<br>♦ Difficiles à départager de par leur nombre énorme |

**Tableau 3 :** Avantages et inconvénients d'un Firewall personnel

#### 7.3.3.2 Les Firewalls plus « Sérieux »

Tournant généralement sous linux, car cet OS offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les firewalls matériels des routeurs, à ceci prêt qu'ils sont configurables à la main. Le plus courant est iptables (anciennement ipchains), qui utilise directement le noyau linux. Toute fonctionnalité des firewalls de routeurs est potentiellement réalisable sur une telle plateforme.

| Avantages | Inconvénients |
|---|---|
| ♦ Personnalisables<br>♦ Niveau de sécurité très bon | ♦ Nécessite une administration système supplémentaire |

**Tableau 4 :** Avantages et inconvénients d'un Firewall plus sérieux

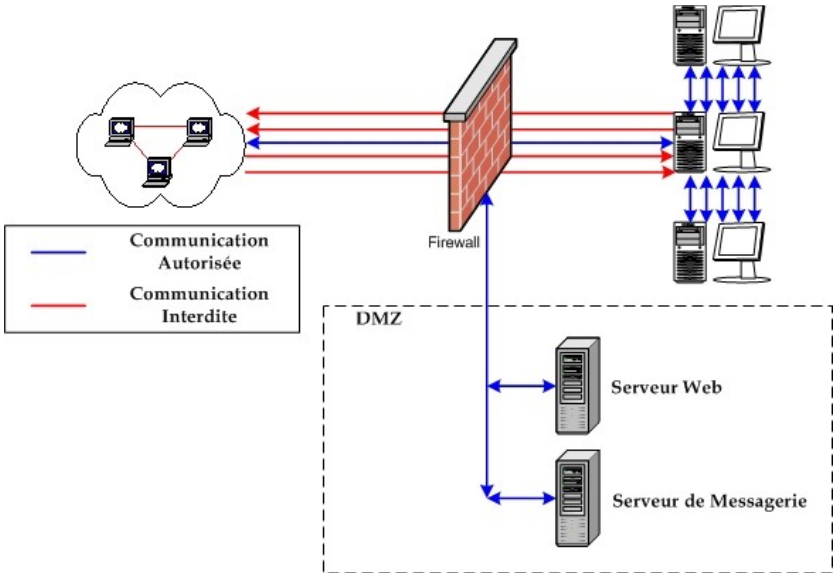
Ces firewalls logiciels ont néanmoins une grande faille : ils n'utilisent pas la couche bas réseau. Il suffit donc de passer outre le noyau en ce qui concerne la récupération de ces paquets, en utilisant une librairie spéciale, pour récupérer les paquets qui auraient été normalement « droppés » par le Firewall. Néanmoins, cette faille induit de s'introduire sur l'ordinateur en question pour y faire des modifications... chose qui induit déjà une intrusion dans le réseau, ou une prise de contrôle physique de l'ordinateur, ce qui est déjà Synonyme d'inefficacité de la part du firewall.

## 7.4 DMZ « Zone Démilitarisée »

### 7.4.1 Notion de cloisonnement

Les systèmes pare-feu permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feux permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « **cloisonnement des réseaux** » (le terme isolation est parfois également utilisé).

### 7.4.2 Architecture DMZ




Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « **zone démilitarisé** » (notée **DMZ** pour *DeMilitarized Zone*) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile. La figure ci-dessous montre la position d'une DMZ au sein d'un réseau.

Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant poste dans le réseau de l'entreprise.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ **autorisé** ;
- Trafic du réseau externe vers le réseau interne **interdit** ;
- Trafic du réseau interne vers la DMZ **autorisé** ;
- Trafic du réseau interne vers le réseau externe **autorisé** ;
- Trafic de la DMZ vers le réseau interne **interdit** ;
- Trafic de la DMZ vers le réseau externe **interdit**.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

## 7.5 NAT « Network Address Translation »

### 7.5.1 Principe du NAT

Le mécanisme de **translation d'adresses** « **NAT** » a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4 (le protocole IPv6 répondra à terme à ce problème).

En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines nécessitant d'être connectées à internet de l'être.

Le principe du NAT consiste donc à utiliser une adresse IP routable (ou un nombre limité d'adresses IP) pour connecter l'ensemble des machines du réseau en réalisant, au niveau de la passerelle de connexion à internet, une translation (littéralement une « traduction ») entre l'adresse interne (non routable) de la machine souhaitant se connecter et l'adresse IP de la passerelle. Cette passerelle peut être un routeur tel que montré dans la figure suivante.

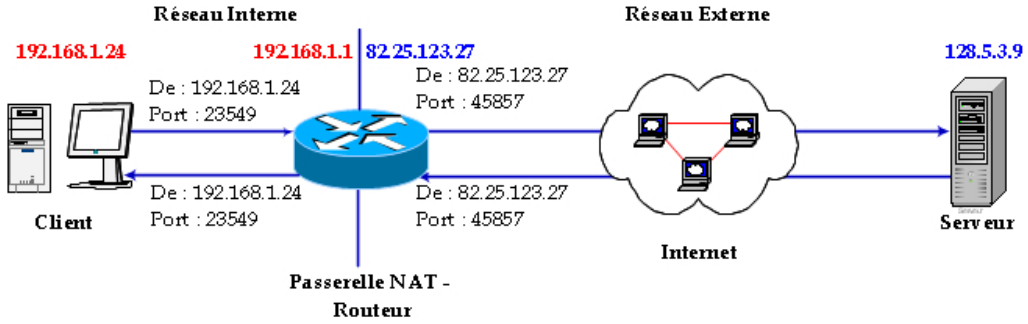



**Figure 5 :** Fonctionnement du NAT

D'autre part, le mécanisme de translation d'adresses permet de **sécuriser** le réseau interne étant donné qu'il camoufle complètement l'adressage interne. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de la même adresse IP.

### 7.5.2 Espaces d'adressages

L'organisme gérant l'espace d'adressage public (adresses IP routables) est l'**IANA**[13]. La RFC 1918 définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses IP aux machines de son réseau interne sans risque d'entrer en conflit avec une adresse IP publique allouée par l'IANA. Ces adresses dites non-routables correspondent aux plages d'adresses suivantes :

- **Classe A :** plage de 10.0.0.0 à 10.255.255.255 ;
- **Classe B :** plage de 172.16.0.0 à 172.31.255.255 ;
- **Classe C :** plage de 192.168.0.0 à 192.168.255.55 ;

[13] Internet Assigned Number Authority

Toutes les machines d'un réseau interne, connectées à internet par l'intermédiaire d'un routeur et ne possédant pas d'adresse IP publique doivent utiliser une adresse contenue dans l'une de ces plages. Pour les petits réseaux domestiques, la plage d'adresses de 192.168.0.1 à 192.168.0.255 est généralement utilisée.

### 7.5.3 Translation statique

Le principe du **NAT statique** consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée (par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.

#### 7.5.3.1 Avantages et inconvénients du NAT statique

En associant une adresse IP publique à une adresse IP privée, nous avons pu rendre une machine accessible sur Internet. Par contre, on remarque qu'avec ce principe, on est obligé d'avoir une adresse publique par machine voulant accéder à Internet. Cela ne va pas régler notre problème de pénurie d'adresses IP... D'autre part, tant qu'à donner une adresse publique par machine, pourquoi ne pas leur donner cette adresse directement plutôt que de passer par un intermédiaire ? A cette question, on peut apporter plusieurs éléments de réponse. D'une part, il est souvent préférable de garder un adressage uniforme en interne et de ne pas mêler les adresses publiques aux adresses privées. Ainsi, si on doit faire des modifications, changements, interventions sur le réseau local, on peut facilement changer la correspondance entre les adresses privées et les adresses publiques pour rediriger les requêtes vers un serveur en état de marche. D'autre part, on gâche un certain nombre d'adresses lorsqu'on découpe un réseau en sous-réseaux (adresse de réseau, adresse de broadcast...), comme lorsqu'on veut créer une DMZ pour rendre ses serveurs publiques disponibles. Avec le NAT statique, on évite de perdre ces adresses.

Malgré ces quelques avantages, le problème de pénurie d'adresses n'a toujours pas été réglé. Pour cela, on va se pencher sur la NAT dynamique.

### 7.5.4 Translation dynamique

Le **NAT dynamique** permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP. C'est la raison pour laquelle le terme de « **mascarade IP**[14] » est parfois utilisé pour désigner le mécanisme de translation d'adresse dynamique.

Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables, le NAT dynamique utilise le mécanisme de translation de port (**PAT** - Port Address

[14] En anglais IP masquerading

Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.

7.5.4.1 Avantages et inconvénients du NAT dynamique

Comme nous l'avons vu, le NAT dynamique permet à des machines ayant des adresses privées d'accéder à Internet. Cependant, contrairement au NAT statique, il ne permet pas d'être joint par une machine de l'Internet. Effectivement, si le NAT dynamique marche, c'est parce que le routeur qui fait le NAT reçoit les informations de la machine en interne (Adresse IP, port TCP/UDP). Par contre, il n'aura aucune de ces informations si la connexion est initialisée de l'extérieur... Le paquet arrivera avec comme adresse de destination le routeur, et le routeur ne saura pas vers qui rediriger la requête en interne.

La NAT dynamique ne permet donc que de sortir sur Internet, et non pas d'être joignable. Il est donc utile pour partager un accès Internet, mais pas pour rendre un serveur accessible. De plus, étant donné que l'on peut "cacher" un grand nombre de machines derrière une seule adresse publique, cela permet de répondre à notre problème de pénurie d'adresses.

Par contre, les machines n'étant pas accessibles de l'extérieur, cela donne un petit plus au niveau de la sécurité.

## 8. Les systèmes de détections d’intrusions

La sécurité des systèmes d'information vise à garantir la confidentialité, l'intégrité et la disponibilité des services. C'est une tâche difficile, tout particulièrement dans un contexte de connectivité croissante.

Pour améliorer la sécurité, il faut mettre en place des mécanismes, d'une part pour assurer que seules les personnes autorisées peuvent consulter ou modifier des données, d'autre part pour assurer que les services peuvent être rendus correctement.

La première mesure à prendre est la protection physique des équipements. Les accès aux locaux et aux unités centrales doivent être contrôlés car, par exemple, tous les efforts de protection de données sont vains si on peut s'emparer du disque dur.

Il faut également mettre en œuvre les mécanismes d'authentification et de contrôle d'accès. L'authentification consiste pour l'utilisateur à prouver son identité au système d'une ou plusieurs façons : mot de passe, objet de sécurité (carte à puce, clef électronique) ou biométrie (empreinte digitale, vocale ou rétinienne). Le contrôle d'accès permet de définir les droits que l'on accorde aux différents utilisateurs sur les données (droits de lecture, écriture et exécution) ou les machines (droit de se connecter).

L'étape suivante consiste à utiliser des outils d'analyse automatique des vulnérabilités du système (ex : COPS, SATAN). Cela permet de trouver certaines failles dues à une mauvaise configuration du système. Ainsi, des droits d'accès trop permissifs à des fichiers sensibles ou à des machines

peuvent permettre à un utilisateur, par un enchaînement approprié de commandes, d'obtenir des privilèges d'accès supérieurs à ceux prévus initialement.

Avec l'interconnexion croissante des réseaux et le développement de l'internet, les possibilités d'attaque à distance ont considérablement augmenté. Pour contrôler au niveau réseau l'accès à une machine depuis l'extérieur, il faut installer un pare-feu qui devient un point de passage obligé. Il a pour rôle de filtrer les paquets indésirables échangés avec l'extérieur (services non disponibles, adresse source suspecte, adresse destination prohibée) et de relayer les flux applicatifs. Il permet par ce biais d'éviter de nombreuses attaques en déni de service (*Ping Of Death, SYN Flood, ...*) et réduit le nombre d'informations que l'on peut collecter sur le réseau interne à partir de l'extérieur.

Malheureusement, il existe la plupart du temps des moyens pour contourner les mécanismes évoqués ci-dessus. Pour ce faire, il n'est même plus nécessaire d'être un pirate expérimenté car de nombreux « outils » sont offerts sur l'internet. Ces outils exploitent les failles qui sont continuellement découvertes dans les systèmes, services et protocoles.

Les pare-feux, aussi indispensables soient-ils, ne doivent pas être pris pour la panacée. En effet, ils ne protègent, ni d'une configuration incomplète ou erronée, ni de ce qui les traverse en mode « tunnel ». Par ailleurs, ils peuvent être compromis par un attaquant externe. De plus, ils sont impuissants face à une menace interne (80% des attaques seraient d'origine interne) puisqu'ils ne surveillent que les échanges réseau avec l'extérieur.

On ne peut donc envisager un système sécurisé sans contrôle de ce que font les utilisateurs. C'est le rôle de l'audit de sécurité et de la détection d'intrusions.

## 8.1 La détection d'intrusions : une nécessité

L'audit de sécurité est un mécanisme intégré aux systèmes d'exploitation et à toutes les grandes catégories d'applications. Il permet d'enregistrer tout ou partie des actions effectuées sur le système. Une analyse ultérieure des informations enregistrées doit permettre de détecter d'éventuelles intrusions. Cette analyse est appelée détection d'intrusions.

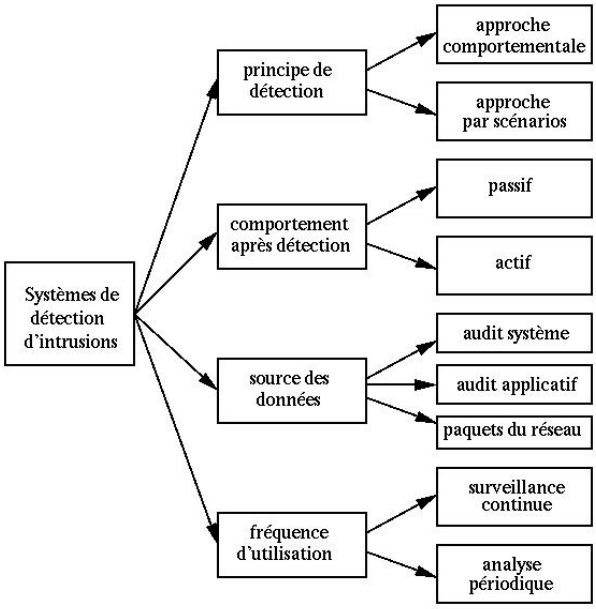
Il n'est pas envisageable de faire cette détection manuellement car la recherche d'actions suspectes se fait dans d'immenses volumes de données. Il a donc fallu trouver des méthodes et développer des outils pour analyser automatiquement les traces d'audit.

Le grand nombre de systèmes de détection d'intrusions développés à ce jour, ne permet pas d'en envisager une présentation exhaustive. Nous présentons donc dans ce paragraphe une typologie des méthodes proposées à ce jour. On reprend à cet effet un travail fait dans le laboratoire d'IBM à Zurich, qui utilise les critères de classification suivants (voir figure 1) :

- Le principe de détection utilisé,
- Le comportement en cas d'attaque détectée,
- La source des données à analyser,

- La fréquence d'utilisation.

### 8.1.1 Principes de détection




Les deux approches qui ont été proposées à ce jour sont l'approche comportementale et l'approche par scénarios. La première se base sur l'hypothèse que l'on peut définir un comportement « normal » de l'utilisateur et que toute déviation par rapport à celui-ci est potentiellement suspecte. La seconde s'appuie sur la connaissance des techniques employées par les attaquants : on en tire des scénarios d'attaque et on recherche dans les traces d'audit leur éventuelle survenue.

#### 8.1.1.1 L'approche comportementale

Le comportement normal d'un utilisateur ou d'une application (profil) peut être construit de différentes manières. Le système de détection d'intrusions compare l'activité courante au profil. Tout comportement déviant est considéré intrusif. Parmi les méthodes proposées pour construire les profils, les plus marquantes sont les suivantes :

- Méthodes statistiques : Le profil est calculé à partir de variables considérée comme aléatoires et échantillonnées à intervalles réguliers. Ces variables peuvent être le temps processeur utilisé, la durée et l'heure des connexions, etc. Un modèle statistique (ex : covariance) est alors utilisé pour construire la distribution de chaque variable et pour mesurer, au travers d'une grandeur synthétique, le taux de déviation entre un comportement courant et le comportement passé. L'outil NIDES[15] utilise, entre autres, cette méthode.
- **Systèmes experts :** Ici, c'est une base de règles qui décrit statistiquement le profil de l'utilisateur au vu de ses précédentes activités. Son comportement courant est comparé aux règles, à la recherche d'une anomalie. La base de règles est rafraîchie régulièrement. L'outil Wisdom&Sense[16] utilise cette méthode, aujourd'hui tombée en désuétude.
- **Réseaux de neurones :** La technique consiste à apprendre à un réseau de neurones le comportement normal d'un utilisateur. Par la suite, lorsqu'on lui fournira les actions

[15] H.S. Javitz, A. Valdes, T.F. Lunt, A. Tamaru, M. Tyson, and J. Lowrance. Next generation intrusion detection expert system (NIDES). Technical Report A016-Rationales, SRI, 1993.
[16] H.S. Vaccaro and G.E. Liepins. Detection of anomalous computer session activity. In Proceedings of the IEEE Symposium on Security and Privacy, May 1989.

courantes, il devra décider de leur normalité. L'outil Hyperview[17] comporte un module de ce type et plusieurs travaux de recherche vont dans le même sens. Cette méthode reste prometteuse, mais n'est pas encore industrialisée.

- **Immunologie :** Cette analogie informatique de l'immunologie biologique a été proposée par Forrest[18]. Il s'agit de construire un modèle de comportement normal des services réseaux Unix (et non un comportement normal d'utilisateurs). Le modèle consiste en un ensemble de courtes séquences d'appels système représentatifs de l'exécution normale du service considéré. Des séquences d'appels étrangères à cet ensemble sont alors considérées comme la potentielle exploitation d'une faille du service.

L'approche comportementale permet de détecter des attaques inconnues auparavant ainsi que les abus de privilèges des utilisateurs légitimes du système. Par contre, le comportement de référence n'étant jamais exhaustif, on s'expose à des risques de fausses alarmes (faux positifs). De plus, si des attaques ont été commises durant la phase d'apprentissage, elles seront considérées comme normales (risque de faux négatifs).

8.1.1.2. L'approche par scénarios

Des scénarios d'attaques sont construits et l'analyse des traces d'audit se fait à la recherche de ces scénarios. Les méthodes proposées à ce jour et à cet effet sont les suivantes :

**Systèmes experts :** Le système expert comporte une base de règles qui décrit les attaques. Les événements d'audit sont traduits en des faits qui ont une signification sémantique pour le système expert. Son moteur d'inférence décide alors si une attaque répertoriée s'est ou non produite. Les outils récents ne l'utilisent plus.

**Algorithmes génétiques :** L'outil GASSATA utilise des algorithmes génétiques pour rechercher des attaques dans des traces d'audit. Chaque individu de la population code un sous-ensemble particulier d'attaques qui sont potentiellement présentes dans les traces d'audit. La valeur d'un individu est proportionnelle au degré de réalisme de l'hypothèse qu'il code, au vu du fichier d'audit.

**Pattern matching :** Il s'agit là de la méthode la plus en vue actuellement. Des signatures d'attaques sont fournies, à des niveaux sémantiques divers selon les outils (de la suite d'appels système aux commandes passées par l'utilisateur). Divers algorithmes sont utilisés pour localiser ces signatures dans les traces d'audit.

On peut voir deux inconvénients à cette approche : on ne peut détecter que des attaques connues et il faut remettre à jour la base de scénarios d'attaque très souvent.

[17] H. Debar, M. Becker, and D. Siboni. A neural network component for an intrusion detection system. In Proceedings of the IEEE Symposium of Research in Computer Security and Privacy, pages 240-250, May 1992.
[18] S. Forrest, S.A. Hofmeyr, and A. Somayaji. Computer immunology. Communications of the ACM, 40(10):88-96, October 1997.

8.1.1.3. Approche comportementale ou approche par scénarios ?

Chacune de ces deux approches présente des avantages et des inconvénients (voir tableau 1). C'est pourquoi une approche hybride semble indispensable.

| | Avantages | Inconvénients |
|---|---|---|
| Comportementale | Détection d'intrusion inconnue possible. | Choix délicat des mesures à retenir pour un système cible donné.<br>Pour un utilisateur au comportement erratique, toute activité est "normale".<br>En cas de profonde modification de l'environnement du système cible, déclenchement d'un flot ininterrompu d'alarmes (faux positifs)<br>Utilisateur pouvant changer lentement de comportement dans le but d'habituer le système à un comportement intrusif (faux négatifs). |
| Par scénarios | Prise en compte des comportements exacts des attaquants potentiels. | Base de règles délicate à construire.<br>Seules les attaques contenues dans la base sont détectées. |

**Tableau 5 :** Approche comportementale ou approche par scénarios ?

### 8.1.2 Comportements en cas d'attaque détectée

Une autre façon de classer les systèmes de détection d'intrusions, consiste à voir quelle est leur réaction lorsqu'une attaque est détectée. Certains se contentent de déclencher une alarme (réponse passive) alors que d'autres prennent des mesures correctives (réponse active).

La plupart des systèmes de détection d'intrusions n'apportent qu'une réponse passive à l'intrusion. Lorsqu'une attaque est détectée, ils génèrent une alarme en direction de l'administrateur système par email, message dans une console, voire même par beeper. C'est lui qui devra prendre les mesures qui s'imposent.

Si le système est plus sophistiqué (et surtout plus récent), il peut prendre automatiquement des mesures pour empêcher ou stopper l'attaque en cours. Par exemple, il coupera les connexions suspectes ou même (pour une attaque distante) reconfigurera le pare-feu pour qu'il refuse tout ce qui vient du site incriminé. Il pourra également prévenir l'administrateur.

### 8.1.3. Sources des données à analyser

Les sources possibles de données à analyser sont une caractéristique essentielle des systèmes de détection d'intrusions. Les données proviennent, soit de fichiers générés par le système d'exploitation, soit de fichiers générés par des applications, soit encore d'informations obtenues en écoutant le trafic sur le réseau.

8.1.3.1. Sources d'information système

Un système d'exploitation propose plusieurs sources d'information :

- **Historique des commandes systèmes :** Tous les systèmes d'exploitation fournissent des commandes pour avoir un "instantané" de ce qui se passe. Ainsi, sous UNIX, des commandes telles que ps, pstat ou vmstat fournissent des informations précises sur les événements système.
- **Accounting :** L'accounting fournit de l'information sur l'usage des ressources partagées par les utilisateurs (temps processeur, mémoire, espace disque, débit réseau, applications lancées, ...).
- **Système d'audit de sécurité :** Tous les systèmes d'exploitation proposent ce service pour définir des événements, les associer à des utilisateurs et assurer leur collecte dans un fichier d'audit. On peut donc potentiellement disposer d'informations sur tout ce que font les utilisateurs : accès en lecture à un fichier, exécution d'une application, etc.

Les outils utilisant ces sources de données sont appelés Host Based Intrusion Detection System, HIDS.

8.1.3.2. Sources d'information applicatives

Les grandes catégories d'applications savent toutes générer des informations sur l'utilisation qui en est faite. C'est le cas des fichiers de logs générés par les serveurs ftp et les serveurs web. Peu de systèmes de détection d'intrusions les utilisent. On peut toutefois citer l'outil WebStalker.

8.1.3.3. Sources d'information réseau

Des dispositifs matériels ou logiciels (sniffers) permettent de capturer le trafic réseau. Cette source d'information est intéressante car elle permet de rechercher les attaques en déni de service qui se passent au niveau réseau et les tentatives de pénétration à distance. Néanmoins, il est difficile de savoir qui est à l'origine de l'attaque car il est facile de masquer son identité en modifiant les paquets réseau. Presque tous les outils (commerciaux) récents utilisent cette source d'information.

Les outils utilisant ces sources de données sont appelés Network Based Intrusion Detection System, NIDS.

### 8.1.4. Fréquence d'utilisation

La dernière caractéristique des systèmes de détection d'intrusions est leur fréquence d'utilisation : périodique ou continue. Certains systèmes de détection d'intrusions analysent périodiquement les

fichiers d'audit à la recherche d'une éventuelle intrusion ou anomalie passée. Cela peut être suffisant dans des contextes peu sensibles (on fera alors une analyse journalière, par exemple).

La plupart des systèmes de détection d'intrusions récents effectuent leur analyse des fichiers d'audit ou des paquets réseau de manière continue afin de proposer une détection en quasi temps-réel. Cela est nécessaire dans des contextes sensibles (confidentialité) et/ou commerciaux (confidentialité, disponibilité). C'est toutefois un processus coûteux en temps de calcul car il faut analyser à la volée tout ce qui se passe sur le système.

## 8.2. Les limites actuelles de la détection d'intrusions

Nous avons déjà évoqué les inconvénients inhérents à chaque approche de la détection d'intrusions. Tout outil implémentant une approche présente bien sûr les inconvénients de cette approche. Nous n'y revenons donc pas.

Les systèmes de détection d'intrusions actuels sont trop fermés, ce qui limite, d'une part les possibilités de comparaison de performance, d'autre part les possibilités de coopération. Pourtant, diverses initiatives tendent à résoudre ce problème. Ainsi le groupe de travail Common Intrusion-Detection Framework (CIDF) vise à définir un standard d'interopérabilité entre outils. Par ailleurs, l'IETF a créé récemment un autre groupe, Intrusion Detection Working Group (IDWG), qui vient de commencer ses travaux. Nous ne développons pas plus ici.

Bien que le but principal des outils soit de détecter des intrusions afin de s'en protéger, un but annexe pourrait être de fournir des preuves lorsque des poursuites en justice sont envisagées. Dès lors, un problème se pose : l'inadéquation entre les preuves exigées par les tribunaux et celles fournies par les outils. Ceux-ci peuvent fournir des fichiers de logs du système, leurs propres diagnostics, une partie du trafic réseau capturé durant l'attaque, des adresses IP incriminées et divers autres fichiers. Pour autant, comment prouver que tout cela n'a pas été altéré, surtout si l'attaque a réussi ? Quels mécanismes peuvent garantir de manière sûre l'horodatage des événements sur l'ensemble du réseau ? Et surtout, comment prouver que les logiciels qui ont collecté ces preuves sont exempts de bugs lorsque l'on ne peut pas avoir accès au code source ? On le voit, les outils actuels ne peuvent prétendre délivrer des preuves légales d'intrusions.

Au delà de ces deux limites, il y a plus grave. Les systèmes de détection d'intrusions actuels peuvent être mis en défaut, soit parce qu'ils sont incapables de détecter certains types d'attaque, soit parce qu'ils sont eux-mêmes attaquables.

### 8.2.1 Attaques non détectables

Nous l'avons mentionné, certains systèmes récents permettent de prendre automatiquement des contre-mesures. Un attaquant suffisamment doué peut effectuer une attaque qui aura l'air de provenir d'une machine du réseau interne. L'outil coupera alors les connexions avec la machine incriminée, ce qui constitue un déni de service.

Un nouveau type d'attaque met en défaut tous les outils actuels : plusieurs personnes effectuent une attaque distribuée conjointe à la cadence d'une action toutes les quelques heures. La distribution et la lenteur de l'attaque la fait passer inaperçue.

Les outils basés réseau présentent quant à eux des faiblesses intrinsèques :

- Ceux qui surveillent en temps-réel le trafic sont incapables de suivre les débits des réseaux frame relay ou ATM.
- Une attaque qui consiste à envoyer des paquets altérés. Certains des paquets ne sont pris en compte que par une des deux machines, celle sur laquelle tourne l'outil de détection ou celle attaquée. Ainsi l'outil n'analyse pas réellement ce qui est vu par la machine cible.

### 8.2.2 Attaque des outils eux-mêmes

Les outils de détection d'intrusions peuvent eux-mêmes être la cible d'attaques les rendant inopérants sur un ou plusieurs aspects. L'attaque réelle passera ensuite inaperçue. Chacun des composants peut être attaquée : le module qui fournit les données à analyser (système d'audit ou autres), le module d'archivage, l'éventuel module de contre-mesures, le module d'analyse :

- Si on réussit à empêcher l'arrivée des données en entrée, la détection d'intrusions s'arrête, bien sûr.
- Si le dispositif d'archivage peut être compromis, alors on ne peut assurer, ni l'enregistrement effectif des détails d'une attaque, ni son intégrité.
- Si le module de contre-mesures est mis hors-service, alors l'attaque peut continuer puisque l'outil est incapable de réagir. Il n'y a que l'administrateur (s'il est présent) qui puisse agir après notification de l'intrusion.
- Le module d'analyse peut être mis à bout de ressources. En déterminant ce qui demande le plus de ressource à l'outil, un attaquant peut le surcharger avec des activités inutiles. Une autre manière de faire consiste à forcer l'outil à allouer toute la mémoire dont il dispose pour analyser des actions sans intérêt. Pour continuer à tourner, il sera amené à libérer de la mémoire en cessant, par exemple, la surveillance de connections restées inactives depuis longtemps. Toute attaque sur l'une d'entre elles restera indétectable. Enfin, si on réussit à faire consommer à l'outil tout son espace disque pour des activités sans importance, il ne pourra plus stocker les événements intéressants. Il n'y aura donc pas de traces d'une intrusion ultérieure.

**Conclusion**

Dans cette partie, on a montré que la détection d'intrusions dans les réseaux ne vient pas concurrencer les mécanismes de sécurité traditionnels mais, au contraire, les compléter. Même si on ne peut pas atteindre la sécurité absolue, on veut au moins pouvoir détecter l'intrusion afin d'y remédier. On a également présenté les principes mis en œuvre par les systèmes de détection d'intrusions pour atteindre leur but. Finalement, on a vu que de nombreux problèmes restent à résoudre avant que la détection d'intrusions soit fiable.

Cette technologie n'est pas encore arrivée à maturité et les outils existants ne sont pas toujours à la hauteur des besoins. Certaines approches théoriques doivent encore être validées dans la pratique. De nouvelles approches demandent encore à être approfondies comme l'immunologie ou les systèmes basés agents.

# **Partie 2 :** Les solutions adéquates pour les PME/PMI

## Objectifs

L'objectif de cette partie est de traiter les points suivants :

- Choix des mécanismes de sécurité
- Présentation des solutions de sécurité réseaux les plus répandus sur le marché

# I. CHOIX DES MÉCANISMES DE SÉCURITÉ

## 1. Les mécanismes de chiffrement

Les mécanismes de chiffrement se décomposent en deux grandes familles :

- **Le chiffrement applicatif :** dans ce cas le chiffrement est assuré par l'application. Le principal intérêt est que deux parties disposant de la même application peuvent bénéficier de la confidentialité de leurs échanges quel que soit le moyen et les équipements qui les relient ;
- **Le chiffrement IP ou VPN :** dans ce cas le chiffrement est assuré par les moyens ou équipements de connexion. Le principal intérêt est que les VPN permettent d'assurer la confidentialité quelle que soit l'application utilisée. Cependant, étant donné le manque encore présent de normes définitives sur les VPN, l'inconvénient est que les deux parties doivent posséder des équipements matériels ou logiciels compatibles.

Pour résumer, si une application spécifique dispose d'un mécanisme de chiffrement propre, il est actuellement préférable de l'utiliser. Le mécanisme de VPN doit être envisagé uniquement dans le cas ou il est le seul possible. Dans ce cas, le mécanisme VPN de Check Point, solide et ayant fait ses preuves, pourra être utilisé vers une passerelle VPN-1/Firewall-1 de l'architecture. Ce mécanisme pourra être utilisé de deux façons distinctes :

- **Mode client à passerelle :** si le client accède Internet depuis un poste client directement, il lui suffira d'installer sur son poste client le logiciel SecuRemote (gratuit) de Check Point ;

- **Mode passerelle à passerelle :** si le client est une société ayant sa propre plate-forme d'accès à Internet, il devra installé une passerelle VPN-1/Firewall-1 sur son site.

De plus, dans le cas de la présence de deux pare-feux de types différents, il est judicieux de gérer les VPN sur le pare-feu amont (le plus proche de l'extérieur) car dans le cas contraire, ce pare-feu serait amené à laisser passer tous les flux chiffrés sans possibilité de contrôle.

## 2. Les mécanismes d'authentification

De la même façon que les mécanismes de chiffrement, les mécanismes d'authentification peuvent être soit offert par l'application, soit par un mécanisme spécifique, nécessaire pour les accès nomades et peut être la maintenance tierce.

Pour les accès pouvant être de nature différentes (accès VPN par Internet ou accès RTC), il est nécessaire d'utiliser un mécanisme standard de dialogue entre l'équipement voulant effectuer l'authentification et le serveur d'authentification. Le seul choix réellement universel à l'heure actuelle est le protocole Radius.

Il faut également être en mesure de proposer des authentifieurs matériels (ou Token), au minimum pour les postes nomades. La tendance actuelle est de proposer des Token ergonomiques et très faciles d'utilisation pour les postes portables, qui nécessitent la présence de ports USB. L'autre choix reste les Token de type calculettes, moins simples mais utilisables avec tout poste client.

Ces considérations devront être prises en compte pour le choix d'un produit d'authentification.

## 3. Les mécanismes de messagerie

Le choix qui s'impose dans les structures de messagerie d'une architecture de sécurité est d'utiliser un relais de messagerie (effectuant du contrôle de contenu) puis de transmettre les messages à un serveur interne en utilisant toujours le protocole SMTP qui est un protocole utilisant un port TCP fixe (25) contrairement à Exchange. Il n'est pas raisonnable de faire transiter du protocole Exchange au travers d'un pare-feu.

## 4. Les mécanismes de contrôle de contenu

Les mécanismes de contrôle de contenu, spécifiquement les fonctions antivirales et de filtrage d'URLs peuvent être mises en œuvre suivant deux méthodes distinctes :

- **Couplés avec un équipements de type pare-feu :** les mécanismes de contrôle de contenu restent transparents pour les autres systèmes en étant utilisés automatiquement par les pare-feux. C'est le cas de l'utilisation des protocoles CVP et UFP de Check Point. L'avantage est d'offrir une structure simple à configurer. Les inconvénients incluent des problèmes de performances ainsi que l'impossibilité d'assurer la haute disponibilité.
- **Utilisés de façon autonomes :** dans ce cas, les systèmes assurant le contrôle de contenu sont utilisés en tant que relais applicatif, pour HTTP ou SMTP par exemple.

L'inconvénient est la non transparence pour le reste de l'architecture mais les avantages sont les performances et la possibilité d'être utilisés avec des pare-feu en haute disponibilité.

## 5. Les mécanismes d'accès Internet

Les besoins associés à l'accès Internet des utilisateurs peuvent être constitués de quatre grands axes :

- Cache interne ;
- Authentification ;
- Contrôle de contenu ;
- Filtrage d'URLs.

Les choix possibles sont axés sur le positionnement et le découpage des différentes fonctionnalités nécessaires. On peut envisager :

- **Le cumul des différentes fonctions sur un même système :** en interne une même machine offre les quatre services. Cela est peu envisageable d'un point de vue performance globale ;
- **La séparation des fonctions :** ceci permet d'améliorer les performances et de bien segmenter les fonctions. Cela peut être effectué de la façon suivante :
  - *Cache et authentification :* sur un système interne. Il est en effet obligatoire d'avoir l'authentification et le cache au plus près des utilisateurs ;
  - *Contrôle de contenu et filtrage d'URLs :* sur un ou deux système(s) en zone relais. Ceci permet de segmenter correctement les flux (en évitant les flux directs de l'intérieur vers l'extérieur). De plus, ce(s) système(s) pourrai(en)t également avoir un mécanisme de cache si le cache interne se révélait insuffisant.

## 6. Les critères de choix des solutions

Le dernier point important est le choix des produits susceptibles de supporter les différentes fonctions citées.

Afin de choisir des produits aptes à remplir correctement les fonctions souhaitées, il est nécessaire d'appliquer certains critères :

- **Fonctionnalité :** un produit choisi doit bien sûr posséder les fonctionnalités requises ;
- **Stabilité :** un produit choisi doit avoir acquis une certaine stabilité et surtout être de source (éditeur, constructeur) stable ;
- **Intégration :** un produit choisi doit pouvoir s'intégrer avec les autres produits de la plate-forme. Dans ce cas, il s'agit d'appliquer l'expérience de sociétés ayant déjà intégré ce type de produits ;

- **Administration :** un produit choisi doit pouvoir être administré de façon simple et si possible à distance (sans poser de problèmes de sécurité) ;
- **Existant :** il est important de tenir compte de l'existant en terme de produits déjà achetés/déployés ainsi que des compétences internes.

Il n'est pas question de faire ici une liste de produits possibles mais de présenter une liste de produits répondant aux besoins et critères cités.

# II. PRÉSENTATION DES SOLUTIONS DE SÉCURITÉ RÉSEAUX LES PLUS RÉPANDUS SUR LE MARCHÉ

L'objectif principal de cette partie est de présenter quelques solutions de sécurité proposées par les éditeurs. Ces solutions concernent essentiellement les technologies précitées dans les chapitres précédents, tels que les Firewalls, les VPN, les IDS/IPS, les solutions d'authentification, les antivirus, les PKI, etc. Aussi, notre objectif dans cette partie n'est pas de favoriser une solution par rapport à une autre mais de faire une comparaison technique entre les différentes solutions ainsi que sur leurs performances leurs fréquences d'utilisation sur le marché.

## 1. Les principales solutions de Firewall

Des boîtiers aux solutions logicielles, des technologies traditionnelles aux plus hybrides, ce panorama présente les principales solutions ou gammes de solutions de pare-feu du marché, qu'elles soient sous forme logicielle ou sous forme de boîtier (Appliance).

Dans ce chapitre, nous allons étudier les firewalls suivants :

- PIX pour les firewalls de niveau 4
- SideWinder pour les firewalls de niveau 7

### 1.1 PIX

Les pare-feu PIX Firewall garantissent une sécurité hautes performances inégalée.

#### 1.1.1 Hautes performances

La gamme Cisco Secure PIX Firewall est une gamme d'appareils de sécurisation à hautes performances, faciles à installer et intégrant composants matériels et logiciels. Elle permet de protéger les réseaux d'entreprises internes du monde extérieur et offre toutes les garanties de sécurité d'un pare-feu de réseau. Contrairement aux serveurs proxy permanents, gros consommateurs de ressources système, qui appliquent des procédures de sécurité à chaque

paquet de données au niveau applicatif, les pare-feu Cisco Secure PIX utilisent un système dédié de sécurisation en temps réel (non UNIX). Ces pare-feu PIX sont exceptionnellement performants : ils prennent en charge plus de 256 000 connexions simultanées, traitent plus de 6 500 connexions par seconde et atteignent des débits de près de 170 Mbits/s.

Ces capacités dépassent de loin celles des autres équipements pare-feu dédiés ou des pare-feu logiciels basés sur des systèmes d'exploitation centraux.

**1.1**.   

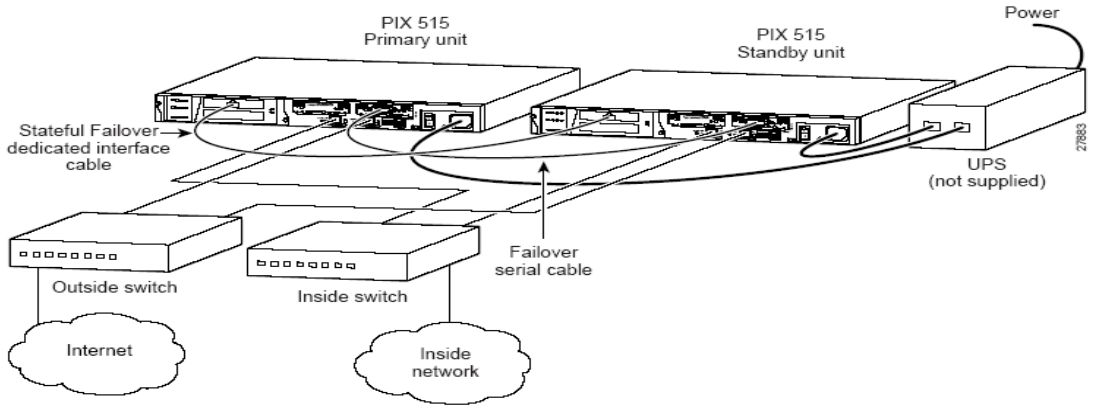
1.1.2.1 Cut-Through

Les pare-feu de la gamme PIX Firewall augmentent encore leurs performances de façon spectaculaire grâce à une fonction d'authentification évoluée appelée « cut-through proxy ». Certes, les serveurs proxy UNIX peuvent assurer une vérification de l'utilisateur et contrôler l'« état » (informations sur l'origine et la destination d'un paquet), toutefois leurs performances en sont considérablement réduites, car ils traitent tous les paquets au niveau de la couche applicative du modèle OSI (interconnexion de systèmes ouverts), gros consommateur de CPU.

En revanche, la fonction de cut-through proxy de la gamme PIX Firewall contrôle un utilisateur uniquement en début de session, au niveau de la couche applicative, comme un serveur proxy. Une fois que l'identité de l'utilisateur a été vérifiée, à l'aide d'une base de donnée standard adoptant le système de contrôle TACACS+ (Terminal Access Controller Access Control System) ou RADIUS (Remote Access Dial-In User Service), et que l'autorisation a été contrôlée, le pare-feu laisse passer le flux des données de la session. Le trafic circule directement et rapidement entre les deux parties, et l'état de la session est préservé sans que la sécurité soit compromise. Cette fonctionnalité assure au PIX Firewall des vitesses beaucoup plus rapides que les serveurs proxy.

1.1.2.2 Failover

Pour accroître encore la fiabilité, la gamme PIX Firewall propose en option un kit de secours d'urgence qui élimine tout risque de panne. Lorsque deux pare-feu fonctionnent en parallèle et qu'un incident se produit sur l'un des deux, le second prend le relais des opérations de sécurité, de façon totalement transparente.




### 1.1.3 Grande simplicité, donc faible coût d'exploitation

Pour simplifier l'administration de réseau, le PIX Firewall intègre une nouvelle interface utilisateur graphique et un outil de configuration basé sur le Web qui permet, par un simple clic de la souris, d'extraire, éditer et gérer sur un site central niveaux de sécurité. Grâce aux rapports de gestion, les administrateurs de réseaux peuvent faire des analyses statistiques sur les tentatives d'accès non autorisés, la densité du trafic et les enregistrements d'événements ; ces analyses permettent ensuite d'établir les coûts d'exploitation. Les administrateurs de réseaux peuvent également connaître les sites Web les plus visités, par utilisateur, en consultant le rapport des URL. Ils peuvent en outre définir des seuils qui permettent aux pare-feu PIX Firewall d'envoyer des messages d'alerte en temps réel via la messagerie électronique ou pager lorsqu'ils détectent des tentatives d'accès pirate. Le PIX Firewall peut également filtrer les applications Java potentiellement dangereuses.

**Remarque :** Grâce à la gamme PIX Firewall de Cisco, il est possible d’éviter tous les coûts dus à l'installation des pare-feu basés sur les systèmes d'exploitation grand-public. Avec ce type de système, il faut tout d'abord acquérir le matériel, puis installer le système d'exploitation et le configurer avec des paramètres sécurisés, et enfin installer l'application pare-feu de réseau. En outre, il faut avoir recours à un expert, pour configurer et installer les stations de travail NT ou UNIX haut de gamme et coûteuses.

### 1.1.4 Plus de problème de manque d'adresses IP

La gamme PIX Firewall dispose d'une fonction d'expansion et de reconfiguration de réseau IP qui évite d'être pénalisé par un manque d'adresses IP. Le système **NAT** de traduction d'adresses réseau permet d'exploiter chacune des adresses IP du pool de réserve défini par l'IANA (RFC 1918). En outre, les pare-feu PIX Firewall peuvent sélectionner un groupe d'adresses particulier et en autoriser ou refuser la traduction.

Une autre fonctionnalité de la gamme PIX Firewall est la traduction d'adresse de port (**PAT**) avec « multiplexage au niveau du port » : cette méthode préserve les données d'un pool d'adresses externe en autorisant la traduction de ports source dans les connexions TCP ou les conversions UDP. Les utilisateurs peuvent traduire plusieurs adresses locales internes en une adresse locale externe unique, à l'aide de numéros de port différents pour distinguer chaque traduction.

## 1.2 SideWinder

Préinstallée et préréglée pour faciliter son déploiement, la famille Sidewinder G2 de pare-feu/VPN fournit une solution de sécurité prête à l'emploi qui s'intègre de manière transparente à n'importe quel réseau IP. Aucune formation ou équipe d'experts informatiques n'est nécessaire. Les dispositifs Sidewinder G2 offrent une solution complète qui combine le pare-feu logiciel intransigeant de Secure Computing avec une famille de plates-formes de serveurs hautes performances montés en rack.

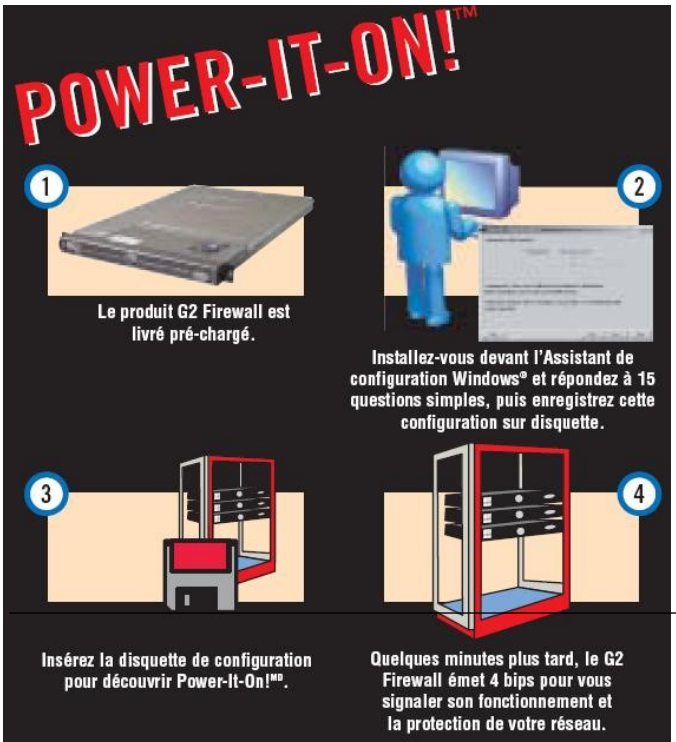
Les modèles Sidewinder G2 s'installent tous proprement dans un rack 19 pouces standard. Aucun terminal, clavier ou système d'alimentation dédié n'est nécessaire.

Convivial pour les réseaux, Sidewinder G2 comprend la prise en charge intégrée des principaux protocoles réseau « domestiques » (SNMP, OSPF, RIP, NTP, ICMP, PING, etc.). Les administrateurs peuvent aisément contrôler le bon fonctionnement de Sidewinder G2 grâce aux rapports et aux outils de surveillance intégrés. Ils peuvent également exporter les données d'analyse vers les meilleurs produits de reporting tiers tels que WebTrends.

Avec ses fonctionnalités de déploiement facile Power-It-On!, ses capacités de sauvegarde/restauration à distance, sa journalisation centralisée, sa surveillance exhaustive d'état/analyse et ses fonctionnalités précurseurs de détection d'intrusion et de réponse automatisée, Sidewinder G2 se positionne parmi les meilleures solutions Firewall de niveau 7.

### 1.2.1 Performances évolutives, Fiabilité et Haute disponibilité

Évolutivité et fiabilité sont profondément ancrées dans la conception du Sidewinder G2 Firewall. SecureOS UNIX de Secure Computing est le premier et unique système d'exploitation pare-feu optimisé pour les processeurs Pentium dans les laboratoires de test de performances Intel. Avec un débit en gigabits et plus de 1 millions de connexions simultanées sur le modèle 4000 haut de gamme. G2 Firewall comprend un logiciel de basculement par inspection d'état de grande qualité et, utilisé en combinaison avec les solutions d'équilibrage de charge certifiées de Secure Computing, Sidewinder offre une évolutivité illimitée et un débit élevé répondant aux besoins des différentes entreprises.




### 1.2.2 Sécurité hybride inégalée et Gestion de type Windows

L'architecture de la sécurité hybride du Sidewinder G2 combine toute la gamme des mécanismes de pare-feu, y compris les filtres de base des paquets, l'inspection complète de l'état, les proxy de niveau circuit, les proxy d'application, les serveurs sécurisés, les alertes

en temps réel de détection d'intrusion Strikeback et la protection contre les DoS au sein d'un unique package, simple et rentable. Sidewinder G2 combine l'inspection complète de l'état avec le filtrage de la couche application afin de contrecarrer les attaques les plus sophistiquées. Au fur et à mesure que le nombre d'entreprises et d'administrations s'appuyant sur des services Web comme .NET, XML et SOAP augmente, le filtrage de la couche application devient un élément incontournable de l'environnement sécuritaire. Les proxy intelligents de niveau application et les serveurs sécurisés protègent les services DNS, FTP, HTTP, la messagerie SMTP et d'autres services Internet très prisés d'une manière efficace.

## 2. Les principales solutions de systèmes de détection d'intrusions

Confrontés à une multiplication et à une complexité croissante des remontées d'alertes, les administrateurs de la sécurité et du réseau ont besoin qu'une information structurée et organisée leur soit remontée.

De même, lorsqu'ils déploient une solution ou des matériels de détection (IDS) ou de prévention d'intrusion (IPS), une console d'administration centralisée leur est indispensable, que ce soit pour un ou plusieurs serveurs stratégiques - solutions dites « Host IDS » - ou bien pour l'intégralité du réseau de l'entreprise - solutions « Network IDS ».

Fonctionnant comme des solutions anti-virus ou anti-spam, les IDS se réfèrent à une base de signatures d'attaques connues. Mais afin de donner à leur solution plus de réactivité lorsqu'une attaque surgit, certains éditeurs ont décidé de transformer leur offre en IPS (Intrusion Prevention System), axant leur technologie vers la prévention proactive, capable de réagir en temps réel lorsque qu'une anomalie est détectée ou qu'une intrusion est avérée.

Sur ce marché, on trouve deux acteurs phares que sont ISS et Cisco. Suivent ensuite dans le désordre Network Associates, Snort, Symantec, NetASQ, Top Layer Networks, Netscreen, Hogwash, TippingPoint, etc.

Dans ce chapitre, on va détailler l'offre d'ISS avec sa gamme Proventia et l'offre de Cisco avec son produit IPS4200.

### 2.1 La gamme Proventia d'Internet Security Systems

**Les appliances de Prévention d'Intrusions Proventia** d'Internet Security Systems bloquent automatiquement les attaques malveillantes tout en préservant la bande passante et la disponibilité du réseau. Les appliances Proventia G utilisent des technologies prouvées qui surpassent de loin les capacités de protection et la précision des pare-feux actuels, des systèmes de détection d'intrusions et des autres systèmes en coupure de protection contre les intrusions. Les attaques connues et inconnues sont bloquées en temps réel, telles que les dénis de services distribués, les chevaux de Troie, les attaques hybrides, éliminant la nécessité d'une implication continue de l'administrateur. Les appliances Proventia viennent compléter les autres offres de

protection réseau, serveur et postes de travail d'Internet Security Systems, gérées par la plate-forme d'administration centralisée SiteProtector.


### 2.1.1 Les avantages de Proventia

**Blocage dynamique**

- Active une réponse fiable de blocage immédiat contre le trafic illégitime
- Autorise le trafic légitime de passer librement sans impacter la performance du réseau
- Utilise un processus de purification du trafic dans le but de stopper les attaques précédemment
- Offre une protection immédiate contre les attaques connues et inconnues vous laissant le temps de tester les correctifs et de planifier leur application manuelle via le processus de Virtual Patch

**Prévention prouvée sans faux positif**

- Ces capacités d'analyse protocolaire approfondie garantissent une protection performante et précise contre les attaques connues et inconnues
- Analyse plus de 100 protocoles réseau et inclut plus de 2500 signatures uniques

**Administration centralisée avec SiteProtector**

- Contrôle, surveille et analyse avec un minimum de ressources humaines dédiées et de coûts opérationnels
- S'adapte à toutes tailles d'entreprise
- Corrélation avancée des données, analyse d'impacts et reconnaissance de schémas d'attaques suspectes avec le module SiteProtector SecurityFusion

**Performance et Fiabilité**

- Protège à la vitesse du lien réseau sans consommer de bande passante ou perturber la disponibilité du réseau
- Permet au trafic de passer en cas de coupure d'alimentation de l'appliance
- Des systèmes de qualité Premium basé sur l'équipement Intel qui inclut :
  - Des ventilateurs internes redondants

- Une unité de stockage RAID pour empêcher des échecs fatals hardware
- Alimentation interchangeable à chaud

**Une protection contre les intrusions en mode espion**

- Invisible aussi bien sur le réseau que pour les attaquants

## 2.2 La solution IPS de Cisco

La solution de prévention des intrusions Cisco IPS (Intrusion Prevention System) est une offre logicielle qui est conçue pour identifier, référencer et bloquer le trafic malveillant avant qu'il ne compromette la continuité de l'activité de l'entreprise. Avec ses capacités éprouvées de détection et de prévention en ligne de qualité industrielle, la solution Cisco IPS réalise une protection complète des données comme de l'infrastructure informatique. La solution Cisco IPS offre une protection précise et proactive qui permet à ses utilisateurs de bloquer davantage de menaces avec une confiance accrue grâce à :

- **L'identification globale des menaces –** L'inspection approfondie du trafic des couches 2 à 7 protège le réseau des violations de politiques, de l'exploitation de ses vulnérabilités et des activités malveillantes ;
- **Des technologies précises de prévention –** Elles vous permettent d'effectuer des actions de prévention en toute confiance sur un éventail élargi de menaces sans risquer de rejeter le trafic autorisé. Le système innovant d'évaluation des risques ainsi que le générateur de méta-événements MEG (Meta-Event Generator) de Cisco identifient les attaques avec précision et permettent de mettre rapidement en œuvre les actions de défense ;
- **Une collaboration en réseau originale –** La collaboration de réseau, avec ses techniques efficaces de capture du trafic, ses fonctions d'équilibrage de charge et sa capacité d'analyse du trafic crypté, apporte encore plus d'évolutivité et de robustesse ;
- **Des solutions complètes de déploiement –** L'offre logicielle Cisco IPS permet la mise en œuvre des solutions de détection et de prévention des intrusions dans tous les environnements. Environnements clients de tous types (depuis les PME et les agences d'entreprise jusqu'aux installations du siège social ou des fournisseurs de services), mais aussi environnements hardware adaptés. La gamme des équipements spécialisés Cisco IPS se compose des serveurs dédiés de la gamme Cisco IPS 4200 ainsi que des modules de commutation de la gamme Cisco Catalyst 6500. Le module de détection des intrusions (IDS) destiné aux routeurs d'accès Cisco fournit des fonctionnalités évoluées qui renforcent les fonctions traditionnelles de détection. De plus, un ensemble spécialisé de fonctions de prévention des intrusions est disponible en tant que solution

Cisco IOS pour les routeurs Cisco. Pour la configuration des unités et la visualisation des événements, Cisco propose des solutions comme IPS Device Manager, destiné à la gestion des serveurs uniques et à la surveillance des événements, ainsi que CiscoWorks VMS (VPN/Security Management Solution), spécialisé dans la gestion de plusieurs unités avec corrélation d'événements multiples.

Lorsqu'ils sont associés, ces éléments réalisent une solution de prévention en ligne complète qui vous permet, en toute confiance, de détecter et de bloquer les types les plus variés de trafics malintentionnés avant qu'ils compromettent la continuité des activités de l'entreprise.

### 2.2.1 Caractéristiques et Avantages

**Des services IPS pour bloquer les vers et les virus**

Destiné aux serveurs dédiés de gamme Cisco 4200 ainsi qu'au module IDSM-2 pour les commutateurs de la gamme Cisco Catalyst 6500, le logiciel Cisco IPS Version 5.0 fournit des fonctionnalités en ligne de prévention des intrusions qui bloquent efficacement les vers et les virus aux endroits stratégiques du réseau. La Figure 30 montre comment les serveurs dédiés et les modules Cisco IPS réalisent des solutions de déploiement complètes sur l'ensemble du réseau.

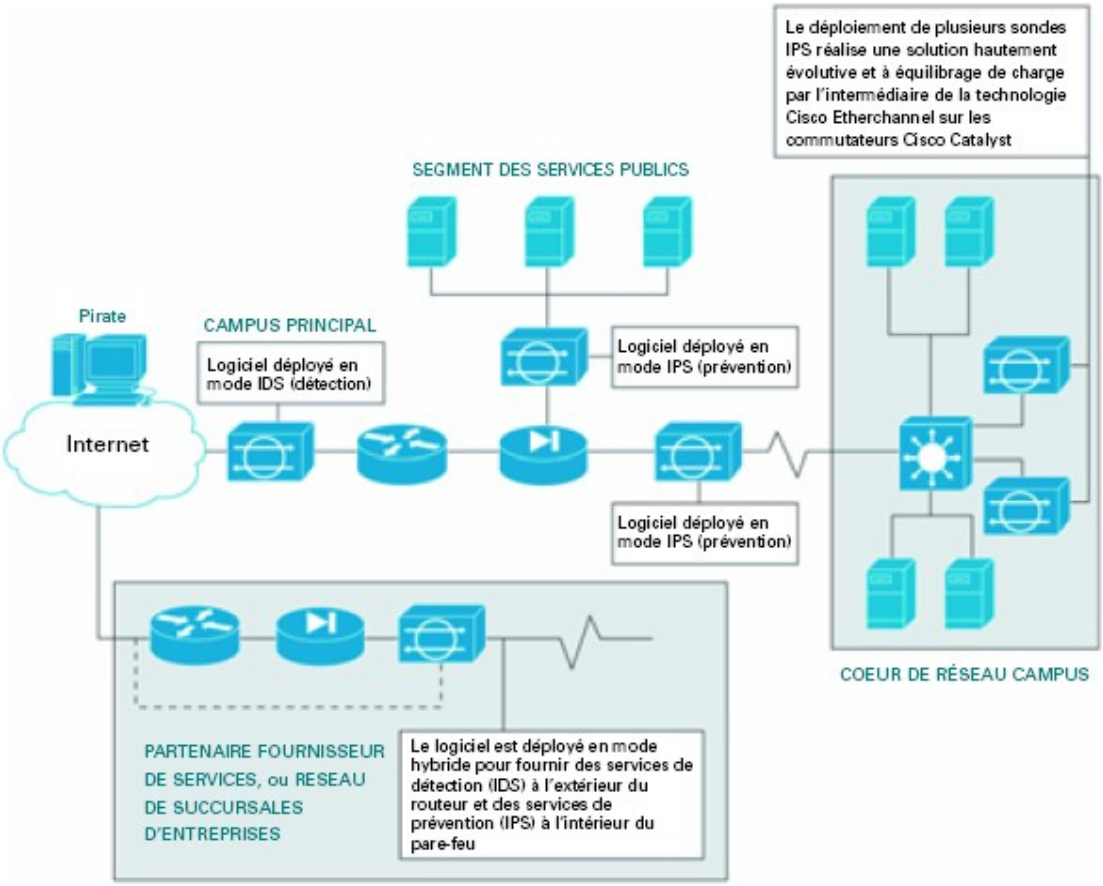



**Figure 6 :** Exemple de déploiement d'IDS et d'IPS au sein d'un réseau d'entreprise

- Support des services **hybrides IDS/IPS**, qui permet au même logiciel de travailler à la fois en mode de détection (IDS) et de prévention (IPS). La Figure 30 montre comment déployer stratégiquement des unités IPS pour qu'elles assurent, simultanément et

individuellement, des services de détection et de prévention. Cette fonctionnalité permet de réduire considérablement le coût total d'acquisition en supprimant la nécessité de déployer de multiples unités sur un même réseau.

- Support d'un **large éventail d'actions de rejet des paquets**, notamment la possibilité de rejeter individuellement les paquets malveillants, tous les paquets d'un flux contenant plusieurs paquets malveillants ou tous les paquets provenant de l'adresse IP du pirate. Ces actions **en ligne** complètent les actions de défense existantes, comme la réinitialisation des connexions et les modifications des listes de contrôle d'accès sur les commutateurs, les routeurs et les pare-feu, pour fournir un ensemble de techniques de contrôle des attaques **qui travaillent de concert** pour bloquer efficacement les vers et les virus.

### Des technologies de prévention précises

- **Cisco Meta Event Generator (MEG) –** Le générateur de méta-événements MEG effectue une corrélation « on-box » pour classer les attaques de manière précise. Le logiciel Cisco IPS Sensor Version 5.0 intègre des fonctions évoluées de corrélation des événements au niveau de l'équipement qui fournissent aux administrateurs de la sécurité une méthode automatisée pour accroître le niveau de confiance dans la classification des activités malveillantes détectées par l'IPS. Ce mécanisme permet, par des actions appropriées, de contenir les vecteurs d'injection des vers et des virus et de bloquer la propagation des vers à l'échelle du réseau tout entier.

  Ce mécanisme repose sur les techniques suivantes :

- **La corrélation des alertes** relatives aux vers qui exploitent des vulnérabilités multiples. La Figure 31 montre comment plusieurs alertes déclenchées sur une courte période peuvent être corrélées en temps réel afin de constituer un méta-événement unique qui assure une meilleure visibilité de l'activité d'un ver ;

- La corrélation d'**une séquence d'actions** caractérisant l'infestation par un ver. Les analyses de tendances historiques réalisées pour caractériser le cycle de vie des vers révèlent souvent une séquence particulière d'actions détectables juste avant qu'ils parviennent à s'infiltrer dans le système. Ces actions interviennent au cours de la « phase de sondage », une succession d'activités de reconnaissance du réseau cible. Le générateur MEG donne à l'utilisateur la possibilité de définir les précurseurs de l'infiltration du ver en désignant un algorithme logique qui se déclenchera en cas de détection d'une suite particulière d'événements. De telles corrélations engendrent des méta-événements qui permettent, avec un meilleur niveau de confiance, d'alerter l'utilisateur de la présence d'une activité malveillante ;

- La corrélation **de multiples événements** de faible dangerosité qui sous-entendent l'éventualité d'un événement unique bien plus grave. A mesure qu'un ver se propage dans le réseau, il génère des alertes plus ou moins sérieuses. Cisco MEG relie entre

elles des alertes de faible gravité et apparemment indépendantes qui signent un événement grave ou à haut risque pour permettre à l'utilisateur de rejeter, avec un haut niveau de confiance, les paquets associés (Figure 32) ;

- L'amélioration du niveau de **fiabilité** des alertes par la simultanéité des réponses positives d'algorithmes hybrides de détection. Par exemple, lorsque des activités caractéristiques d'attaque par saturation sont détectées (identification via une signature classique de type « saturation »), le générateur MEG peut servir à corroborer l'un des événements avec l'autre et fournir ainsi un méta-événement unique qui indique, avec une plus grande probabilité, qu'une attaque est en cours.

Ces niveaux complémentaires de sécurité apportent la confiance nécessaire pour déployer une action de prévention des intrusions en ligne **sans risque de rejet du trafic légitime**, tout en identifiant les vers et en les empêchant de se propager dans votre réseau.

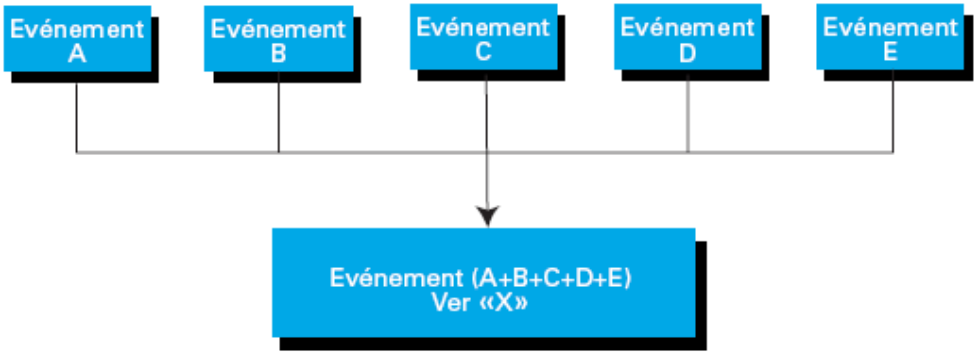



**Figure 7 :** Le générateur MEG corrèle de multiples événements pour détecter la présence d'un ver

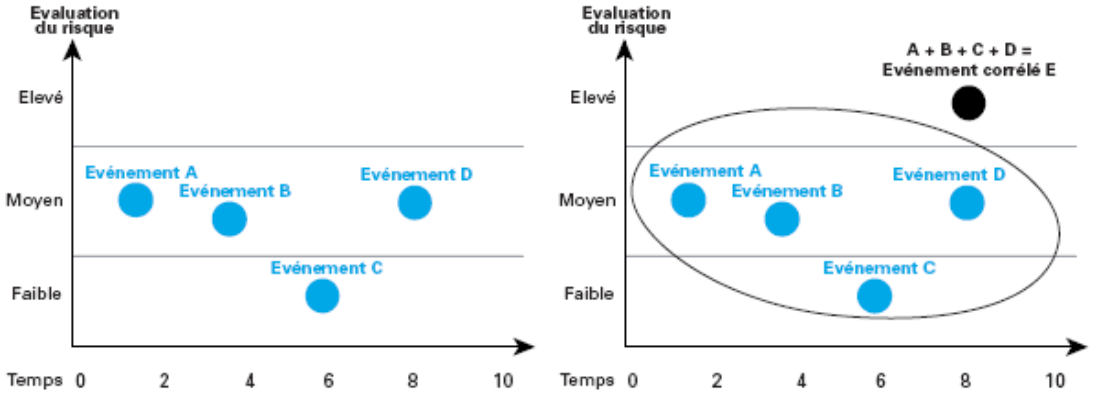



**Figure 8 :** Le générateur MEG corrèle de multiples événements de faible gravité pour générer un unique événement de présence de ver

**L'Évaluation du risque** augmente la précision et le niveau de confiance des actions de prévention (IPS) de rejets des paquets en classant les menaces en fonction des risques encourus (Figure 33). De manière automatisée, l'Évaluation du risque utilise un algorithme pluridimensionnel unique qui tient compte de différents facteurs, et notamment de :

- **La gravité de l'événement –** Valeur dont la pondération est modifiable par l'utilisateur et qui caractérise les dégâts potentiels du trafic suspect ;

- **La fiabilité de la signature –** Valeur dont la pondération est modifiable par l'utilisateur et qui définit dans quelle mesure la signature est susceptible de caractériser la menace ;
- **La valeur de l'équipement –** Paramètre défini par l'utilisateur et représentant la valeur qu'il attribue à l'hôte cible ;
- **La pertinence de l'attaque –** Pondération interne qui rend compte de tous les faits complémentaires que le logiciel possède sur la cible de l'événement.

L'Évaluation du risque ainsi obtenue est un nombre entier appliqué de manière dynamique à chaque signature IPS, politique ou algorithme de détection des anomalies. Plus cette valeur est élevée et plus le risque de sécurité est grand en cas de déclenchement de l'alerte correspondante. On obtient ainsi un mécanisme qui permet à l'utilisateur de développer des politiques de prévention des attaques contre son réseau ou de mieux classer les événements pour les étudier par la suite en fonction de leur priorité. L'utilisateur est ainsi mieux informé pour prendre des décisions concernant des actions de prévention en ligne et élimine pratiquement tout risque de rejet du trafic légitime.

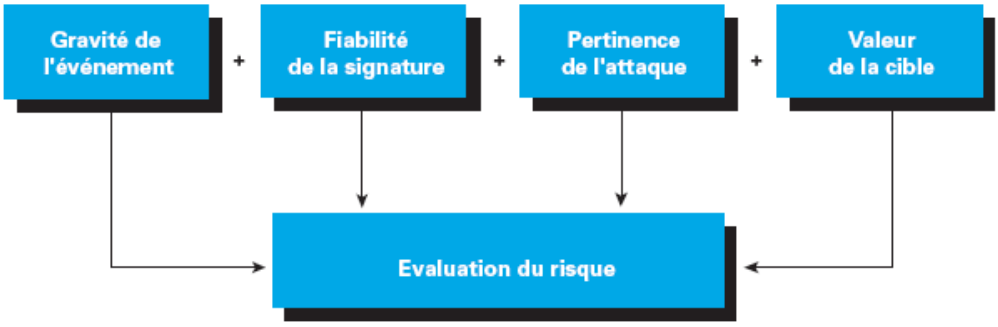



**Figure 9 :** L'Évaluation du risque améliore la précision des actions de prévention IPS

## 3. La solution pour le serveur d'authentification

Gérer ses mots de passe de façon simple, sécuriser ses accès à distance, se prémunir des renifleurs de clavier : autant de raisons qui peuvent pousser une entreprise à se tourner vers des solutions d'authentification forte.

L'authentification forte consiste à ajouter au traditionnel système de login/mot de passe, une solution annexe supplémentaire qui peut être un code supplémentaire généré aléatoirement pour une courte durée, un algorithme de cryptage, des certificats ou un système de signature électronique.

En matière d'authentification forte, trois types de solutions se distinguent : le principe de calculette, qui se présente sous la forme d'une petite calculatrice et génère un code automatique à durée de vie limitée (principe du Token ou jeton), la clef USB, capable de stocker des mots de passe cryptés ou de gérer les certificats électroniques d'accès aux documents, et enfin les systèmes de cartes à puce.

Dans cette partie nous allons faire un focus sur la solution de Secure Computing **SafeWord PremierAccess**, qui est une solution très utilisée sur le marché.

## 3.1 La solution SafeWord PremierAccess

SafeWord PremierAccess permet d'identifier catégoriquement les utilisateurs avant de les autoriser à accéder aux systèmes stratégiques de l'entreprise. PremierAccess élimine les inconvénients des mots de passe à l'aide d'un large choix d'options d'authentification plus sécurisées, plus conviviales et moins chères à implémenter que les mots de passe traditionnels. L'utilisation d'une telle solution présente plusieurs avantages, qui seront traités dans le point suivant.

### 3.1.1 Fonctionnalités et Avantages

- **Gérer plusieurs points d'accès et protéger les applications à l'aide d'un seul produit :** SafeWord PremierAccess permet de gérer de manière transparente les accès des utilisateurs au Web, au réseau VPN et aux applications réseau. Grâce à un système de gestion exclusif, PremierAccess vous permet de sécuriser tous vos points d'accès sans les dépenses et la complexité liées à l'intégration de plusieurs produits.
- **Choisir le mécanisme d'authentification approprié au niveau de sécurité désiré :** SafeWord PremierAccess assure une authentification fiable à plusieurs facteurs sur un large éventail de périphériques. Les jetons SafeWord génèrent de nouveaux mots de passe pour chaque connexion utilisateur, éliminant ainsi les risques de vol, d'emprunt, de piratage ou simplement de mise par écrit des mots de passe. Des mots de passe à usage unique peuvent également être délivrés par l'intermédiaire de jetons logiciels ou MobilePass, qui les envoie sous forme de messages texte à la plupart des téléphones mobiles, récepteurs de radiomessagerie et assistants numériques (PDA).


Il prend en charge un grand nombre de technologies d'authentification : mots de passe, jetons, certificats numériques, cartes à puce, jetons USB, périphériques sans fil et systèmes biométriques. Il permet aussi de choisir la puissance du mécanisme d'authentification en fonction des exigences de sécurité nécessaires à la protection des ressources de l'entreprise.

- **Sécurité de l'accès à distance :** Les autorisations et l'authentification des utilisateurs sont plus importantes que jamais pour l'accès aux systèmes distants tels que les réseaux VPN, les serveurs de clients légers et les réseaux WLAN, permettant un accès direct au cœur du réseau de l'entreprise.

PremierAccess assure une prise en charge transparente de l'authentification pour le protocole sans fil 802.11 et pour les principaux fournisseurs de clients légers et VPN, dont Citrix, Check Point, Cisco, Alcatel, Nortel et Microsoft.

- **Contrôler les accès (qui et où) grâce à des autorisations personnalisées basées sur des rôles :** L'identification des utilisateurs représente la première étape, mais contrôler quelles ressources leur sont disponibles et à quel endroit est tout aussi important. PremierAccess offre une autorisation granulaire basée sur le rôle de l'utilisateur ou sa relation avec l'organisation.
- **Connexion aux systèmes externes avec authentification :** PremierAccess présente la capacité exclusive de jouer le rôle de médiateur (broker) dans l'authentification pour les systèmes tiers de type RADIUS ou Active Directory. Cette fonctionnalité permet alors d'étendre les capacités de contrôle d'accès et d'autorisation de PremierAccess à l'infrastructure existante de l'entreprise.
- **Gestion simple et pratique :** Grâce aux fonctionnalités d'auto-inscription des utilisateurs, d'administration centralisée ou déléguée et de support technique, le déploiement et la gestion de PremierAccess est très simple. Le Centre d'enregistrement Web permet aux utilisateurs de s'inscrire aisément à l'aide des rôles pré-affectés et des règles d'accès.


**Figure 10 :** Écran d'enregistrement des utilisateurs

## 4. Le filtrage Web

Grâce à la facilité d'accès aux informations mondiales qu'il offre, le réseau Internet élargit l'horizon de toutes les entreprises et de tous les individus. Cependant, un accès illimité au Web peut avoir des conséquences négatives sur les individus, les performances du réseau et le chiffre

d’affaires de l’entreprise. Un filtrage Web efficace permet d’inculquer quelques valeurs de principe aux membres de l’organisation, tout en préservant l’accès aux informations indispensables à son succès.

Dans cette partie, nous allons étudier les trois solutions phares sur le marché qui sont :

- Websense Enterprise ;
- SurfControl ;
- SmartFilter.

## 4.1 Websense Enterprise


Utilisée à l'échelle mondiale par plus de 17 800 entreprises, dont la moitié des sociétés classées Fortune 500, Websense Enterprise est la solution logicielle EIM (Employee Internet Management) n° 1 du marché. Basé sur un serveur, le logiciel Websense vous permet de surveiller, gérer et émettre des rapports sur le trafic Internet généré depuis les réseaux internes de l’entreprise, en toute transparence.

Websense utilise une technologie d'émulation pour fournir la solution de filtrage Internet la plus précise, la plus fiable et la plus évolutive du marché. Ce filtrage consiste à faire passer toutes les requêtes de pages Web par un point de contrôle Internet tel qu'un pare-feu, un serveur proxy ou un moteur de cache. Websense s'intègre à ces points de contrôle pour vérifier chaque requête et déterminer si elle doit être autorisée ou refusée. Toutes les réponses sont consignées dans des rapports.

- Websense Enterprise protège les entreprises et les employés qui utilisent Internet d’un nombre croissant de menaces.
- Websense Enterprise améliore la productivité des employés, renforce la sécurité, limite la responsabilité légale et optimise l’utilisation des ressources informatiques.
- Websense Enterprise offre une intégration transparente aux produits phares de l’infrastructure réseau ainsi qu’une souplesse et un contrôle sans précédent.
- Websense Enterprise inclut la base de données principale et les outils de création de rapports Websense, produits phares du secteur, fournissant une analyse et une création de rapports performantes sur les activités Internet et bureautiques.

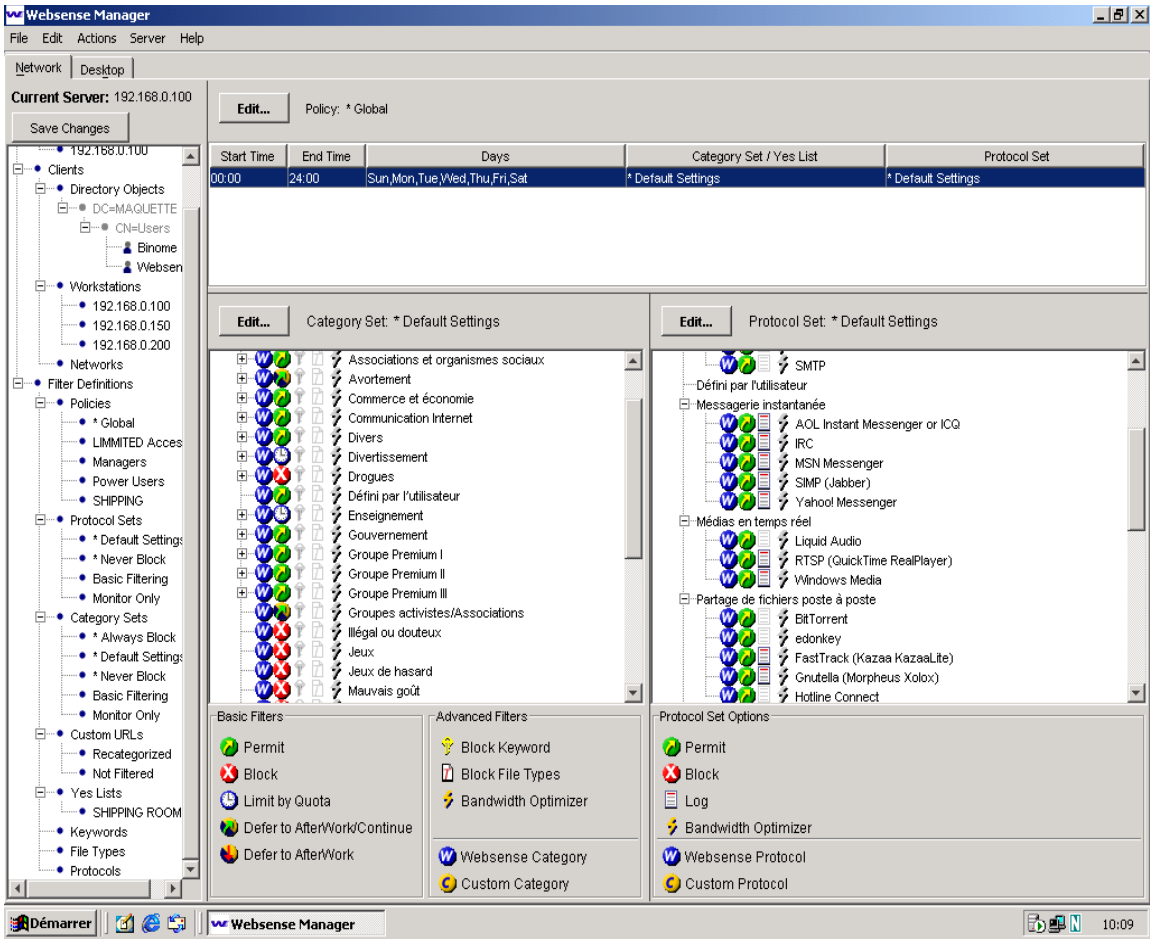



**Figure 11 :** Websense Enterprise Manager

### 4.1.1 Risque et défis en matière de productivité

- Les abus liés à Internet représentent pour les entreprises américaines des pertes annuelles de productivité de plus de 85 milliards de dollars
- Bien que 99% des entreprises utilisent un logiciel [antivirus], 78% d'entre elles ont été attaquées par des virus, vers, ou autres applications dangereuses
- 37% des employés utilisant Internet sur leur lieu de travail aux États-Unis ont visité un site Web classé X pendant les heures de bureau
- Plus de 72% des internautes utilisent des applications à forte consommation de bande passante incluant la messagerie instantanée, le téléchargement de musique et la lecture de clips vidéo

### 4.1.2 Avantages

Websense filtre le contenu Internet en utilisant la base de données Websense Master qui répertorie plus de 4 millions de sites, organisés en plus de 80 catégories, notamment MP3, jeux de hasard, shopping et contenus pour adultes. Vous pouvez choisir de bloquer, autoriser, limiter (par le biais de quotas horaires) ou différer les accès à l'une ou l'autre des catégories par utilisateur, groupe d'utilisateurs, station de travail ou réseau.

De nouveaux sites s'ajoutent chaque jour à la base de données et Websense Enterprise télécharge automatiquement les mises à jour, la nuit, sur votre serveur, vous permettant ainsi de rester en phase avec l'évolution de l'Internet.

- Amélioration de la productivité des employés
- Réduction du risque de violation de la sécurité
- Limitation des risques liés aux activités Internet des employés en matière de responsabilité légale
- Optimisation de l'utilisation des ressources informatiques, y compris de la bande passante et des ressources bureautiques.
- Mise en place de politiques d'utilisation des applications Internet.

**Websense Enterprise v5.5** aide à :

- **Préserver les précieuses ressources en bande passante**
  - Les annonces publicitaires en ligne consomment 10 % de la bande passante du réseau d'une entreprise.
  - Actuellement, les fichiers MP3 représentent l'un des principaux problèmes sur le lieu de travail et surchargent la bande passante de l'entreprise.
  - Le contenu multimédia représente la deuxième menace sur les lieux de travail. L'année dernière, en effet, 9 millions d'employés ont accédé à un contenu multimédia sur leur lieu de travail. Les sites proposant ces contenus (notamment les divertissements ou les films) prévoient une croissance de 2000 %, pour atteindre 20,5 milliards de dollars en 2004.
- **Eviter les problèmes juridiques**
  - Une entreprise sur quatre a pris des mesures contre une utilisation incorrecte d'Internet sur le lieu de travail, ce qui engendre coûts et contrariétés.
  - Les problèmes rencontrés sont notamment les suivants : distribution de documents à contenu préjudiciable (notamment des documents sur la pornographie, la drogue et le racisme), ainsi que le téléchargement de logiciels sans licence et de fichiers audio.
- **Optimiser la productivité des salariés**
  - 40 % des employés reconnaissent surfer sur Internet à des fins personnelles pendant les heures de bureau.
  - En moyenne, les employés visitent des sites à des fins privées environ 3 heures par semaine.

- Pour une entreprise de 500 utilisateurs, le coût engendré par l'utilisation d'Internet à des fins personnelles par les employés, dont le salaire moyen est de 16 $ par heure, pendant 3 heures par semaine, s'élève à 460 800 $ par an.

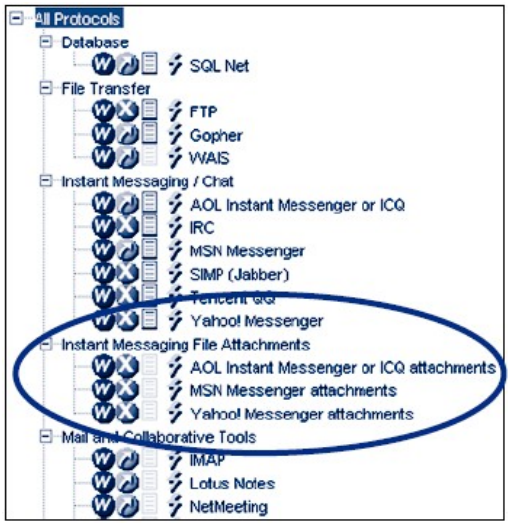
Ces avantages peuvent être étendus à l'aide des solutions Websense IM Attachment Manager, Bandwidth Optimizer.

### 4.1.3 Websense IM Attachment Manager

**Websense Enterprise IM Attachment Manager** est un module d'extension permettant aux responsables informatiques de contrôler l'envoi et la réception de fichiers via les clients de messagerie instantanée (MI). Websense Enterprise permet aux responsables informatiques d'élaborer des politiques souples d'utilisation de messagerie instantanée. IM Attachment Manager améliore ces capacités en limitant les risques en termes de sécurité et de responsabilité légale liés à l'utilisation non contrôlée de pièces jointes MI tout en améliorant la disponibilité des ressources informatiques et la productivité des employés.

IM Attachment Manager aide les entreprises à :

- Limiter les menaces de sécurité dues à des programmes malveillants porteurs de virus, de vers, de chevaux de Troie ou de logiciels espions.
- Minimiser les pertes en termes de propriété intellectuelle.
- Limiter la responsabilité concernant le partage illégal de matériaux dont les droits sont protégés ou le partage de contenus inappropriés.
- Réduire la consommation de bande passante relative aux transferts de fichiers à caractère non professionnel.




**Options de filtrage souples -** Configure différentes politiques de pièces jointes MI par utilisateur, groupe, station de travail, réseau, jour et heure.

**Application automatique de la politique -** Surveille automatiquement les pièces jointes MI et autorise ou refuse les demandes de transfert de fichiers MI conformément à la politique approuvée. Des mises à jour automatiques de la liste du protocole de pièces jointes MI garantissent la précision et minimisent les exigences administratives.

**Détection des menaces MI au sein de votre société -** Analyse les informations historiques et en temps réel sur l'utilisation par les employés des pièces jointes MI utilisant les outils de création de rapports Websense Enterprise incluant Explorer, Reporter et Real-Time Analyzer.

### 4.1.4 Websense Enterprise Bandwith Optimizer

**Websense Enterprise Bandwidth Optimizer** permet aux entreprises d'optimiser les ressources en bande passante de leur réseau en instaurant et en gérant des priorités en temps réel au niveau du trafic réseau. Lorsque le trafic réseau atteint les seuils prédéfinis, BWO bloque les utilisations non professionnelles et garantit un accès prioritaire des applications professionnelles critiques aux ressources du réseau.

Les bannières publicitaires, les fichiers audio et vidéo en temps réel, le partage de fichiers en Peer-to-Peer et autres applications utilisent des ressources réseau de plus en plus importantes.

- Plus de 72% des internautes utilisent des applications gourmandes en bande passante incluant la messagerie instantanée, le téléchargement de musique et la lecture de clips vidéo.
- 44% des employés utilisent des médias en temps réel. Alors qu'une partie du trafic réseau peut être aisément classée comme non cruciale pour l'entreprise, il est souvent difficile de déterminer si ce trafic est directement lié ou non au travail, notamment lorsqu'il s'agit de médias en temps réel. Les politiques de gestion de l'utilisation d'Internet qui se limitent à bloquer toutes les applications à forte consommation de bande passante au niveau du pare-feu de l'entreprise peuvent s'avérer inefficaces.

La solution **Bandwidth Optimizer** fournit un outil de gestion sophistiqué pour l'allocation de la bande passante réseau. Elle permet à l'administrateur de :

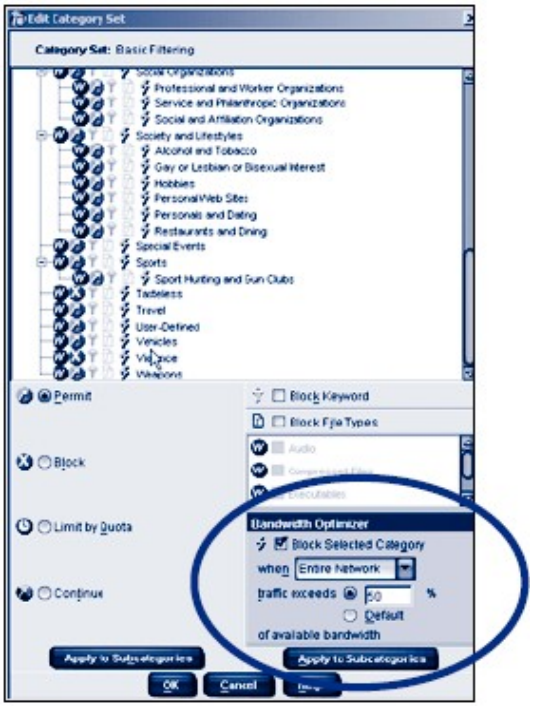
- Définir des seuils d'utilisation de la bande passante pour les sites Web non professionnels, notamment pour le shopping et le divertissement, et des seuils plus élevés pour les sites professionnels.
- Gérer la bande passante allouée aux sites de messagerie instantanée en fixant des seuils adaptés pour des utilisateurs ou des groupes spécifiques, permettant de bavarder en ligne lorsqu'une bande passante suffisante est disponible.
- Gérer la bande passante allouée aux médias en temps réel en bloquant ces applications lorsque la bande passante est insuffisante.

**Des options de filtrage souples -** Fixe les limites de la bande passante à l'aide des protocoles réseaux ou de catégories de sites Web.

**Plusieurs types de limitations de la bande passante -** BWO supporte deux types de seuils en temps réel basés sur des protocoles et des catégories de pages Web :

- *Une limitation basée sur le trafic réseau sortant total* – Les nouvelles demandes de bande passante sont refusées lorsque le trafic sortant total excède un seuil prédéfini.

- *Une limitation basée sur une utilisation de la bande passante par application* - Les nouvelles demandes spécifiques à une application sont refusées lorsque la bande passante totale utilisée par cette application excède un seuil prédéfini.




Lorsque la limite de la bande passante est atteinte, Websense Enterprise refuse les nouvelles requêtes jusqu'à ce que la bande passante retombe en dessous du seuil prédéfini, permettant ainsi le fonctionnement des applications professionnelles à pleine vitesse. Les connexions réseaux déjà établies ne sont pas affectées.

**Politiques basées sur l'utilisateur et sur l'heure -** Fixe différentes limitations pour l'utilisation de la bande passante en fonction des utilisateurs, des groupes, des postes de travail, des réseaux et de l'heure de la journée.

**Application dynamique des politiques -** Websense Enterprise contrôle automatiquement les niveaux de la bande passante du réseau et accepte ou refuse de manière dynamique les requêtes d'applications du réseau. Aucune intervention administrative n'est nécessaire.

## 4.2 SurfControl

SurfControl Web Filter est conçu pour parer aux risques liés aux contenus Internet et protéger de manière optimale votre réseau et votre entreprise contre les risques suivants :

- Responsabilité juridique,
- Sécurité,
- Productivité,
- Ressources réseau.

SurfControl Web Filter présente les atouts suivants :

- Filtrage du trafic Internet
- Filtrage du type de fichiers autorisés au téléchargement
- Multi-plates-formes
- Notification par e-mail
- Mise à jour journalière automatisée des bases
- Rapports prédéfinis, paramétrables et automatiques
- Interface web pour analyse en temps réel

- Technologie « intelligente » et dynamique

### 4.2.1 Avantages

SurfControl Web Filter est une solution complète qui fournit les outils pour comprendre et gérer l'utilisation d'Internet d'une manière parfaitement adaptée aux besoins de l'entreprise. SurfControl Web Filter protège contre les usages hostiles ou tout simplement inappropriés d'Internet et comprend :

**Une base de données parfaitement renseignée -** SurfControl Web Filter dispose de la plus grande base de données de recensement de sites web.

- 40 catégories faciles à administrer réparties en 8 thèmes et 32 activités
- 5,5 Millions d'URLs recensées
- Vérification du contenu en plusieurs langues (Anglais, Français, Allemand, Espagnol, Néerlandais)
- Mises à jour automatiques quotidiennes

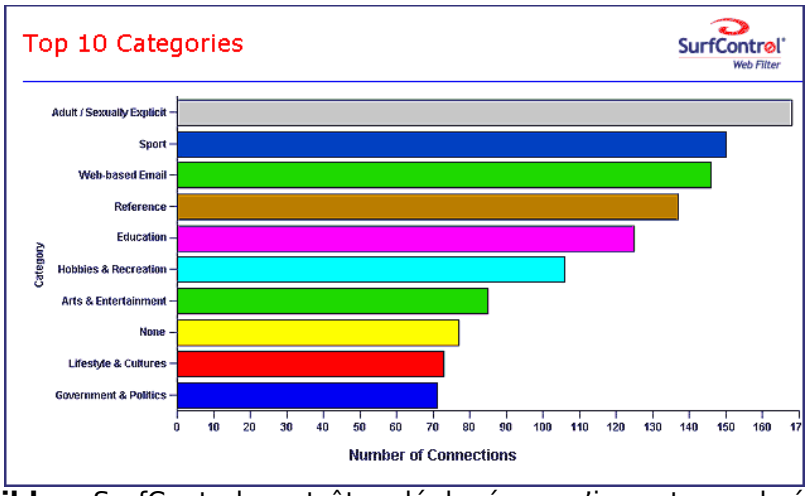
**Une technologie « intelligente ! » -** Les agents virtuels de contrôle (Virtual Control Agent) - des agents « intelligents » pour une catégorisation dynamique.

Avec la croissance exponentielle du nombre de sites web, les utilisateurs trouveront toujours de nouveaux sites, et ce, quelle que soit la qualité de la base de données à disposition pour surveiller le trafic. C'est pourquoi SurfControl a développé les « Virtual Control Agents » qui utilisent une technologie de raisonnement adaptative (ART) pour catégoriser de façon dynamique les nouveaux sites web.

**Simplicité d'utilisation -** L'interface, basée sur le "glisser-déposer" permet de créer très facilement les règles à appliquer. De plus, une fois installé et paramétré, le logiciel réclame très peu d'interventions humaines.

- Création de règles par glisser-déposer
- Activation des règles en un seul clic
- Partages de règles

**Des fonctions intégrées de comptes rendus et d'analyse -** Les outils d'analyse et de reporting fournis par le logiciel donnent tous les détails sur la façon dont l'accès à Internet est utilisé dans la société et sur les goulets d'étranglement susceptibles d'affecter les performances du réseau. On peut ainsi facilement repérer les failles dans les règles fixées et y remédier en quelques clics.




**Déploiement flexible -** SurfControl peut être déployé sur n'importe quel réseau. Les solutions indépendantes des plates-formes peuvent être intégrées au réseau sans tenir compte des firewalls, Proxy et autres périphériques alors que les solutions intégrées à la plate-forme s'installent sur des périphériques réseau spécifiques.

**Filtres par utilisateur et groupes -** On peut adapter les règles de filtrage aux besoins des différents utilisateurs ou groupes d'utilisateurs. Ces utilisateurs ou groupes d'utilisateurs peuvent être spécifiés en utilisant :

- Active Directory
- Novell DNS
- LDAP
- Les adresses IP
- Les adresses MAC
- Les noms des hôtes

**Contrôle des fichiers autorisés en téléchargement -** Limiter ou interdire le téléchargement de certains types de fichiers (MP3, zip, exe) allège le trafic sur la bande passante et limite les risques liés aux virus.

**Hiérarchisation de l'utilisation de la bande passante -** Il est possible d'appliquer des priorités pour l'utilisation de la bande passante. Ce qui permet l'accès à Internet en priorité pour l'utilisation professionnelle.

**Filtrage des bannières publicitaires et pop-up -** En filtrant les bannières, pop up et autres publicités indésirables, SurfControl Web Filter supprime le contenu susceptible d'utiliser plus de 10% de la bande passante.

**Application de règles d'accès à Internet en fonction des horaires -** Afin de conserver une certaine flexibilité, SurfControl Web Filter peut être configuré pour que les règles de filtrage ne s'appliquent qu'à certaines heures définies de la journée. Par exemple, l'accès à des sites sportifs

peut être interdit pendant les heures de travail et autorisé avant et après ces heures et/ou pendant la pause déjeuner.

**Gestion organisée de la liberté d'accès à Internet -** SurfControl Web Filter permet d'octroyer un certain volume de trafic ou un certain temps d'accès « libre » à Internet. Ainsi, l'entreprise peut appliquer des règles destinées à la protéger et à maintenir une bonne productivité tout en ménageant un espace de liberté pour ses employés.

**Notification par E mail -** Les responsables de services et administrateurs peuvent être tenus informés en temps réel par mail d'une tentative d'utilisation non appropriée d'Internet grâce à des mails paramétrables.

**L'interface de contrôle -** L'interface de surveillance permet d'appréhender facilement l'activité Internet de la société. Cette interface donne l'information adéquate pour prendre des mesures correctives rapides.

## 4.3 SmartFilter

SmartFilter est un outil simple et performant ayant pour but de contrôler et de restreindre l'utilisation de l'Internet professionnel. La restriction des accès n'est intéressante que si elle correspond à une adéquation parfaite entre le besoin professionnel de l'utilisateur et le profil d'accès proposé à ce même utilisateur. Ainsi, SmartFilter propose une gestion précise et simple des profils d'accès à l'Internet en fonction des utilisateurs, des groupes d'utilisateurs…


### 4.3.1 Avantages

**Filtrage et blocage des accès -** L'administrateur SmartFilter a la possibilité de filtrer les URL jugées non nécessaires à l'utilisateur en choisissant une restriction basée sur 62 catégories prédéfinies. Dix catégories libres sont également disponibles suivant les plates-formes (personnalisation par l'administrateur). Le message d'information standard de blocage de l'accès est modifiable par l'administrateur. Il est également possible de router les utilisateurs filtrés vers une URL d'information sur le blocage en cours (afin d'expliquer la politique de sécurité en vigueur).

**Coaching -** Cette fonctionnalité permet d'afficher des messages «d'alertes» aux utilisateurs les informant du filtrage activé sur leur session Internet. Ayant pris connaissance de l'information, l'utilisateur peut décider de continuer et accéder au site filtré. Les messages diffusés sont paramétrables par l'administrateur.

**Delay -** Cette fonctionnalité est unique à SmartFilter. Elle permet de ralentir progressivement les accès d'un utilisateur aux sites filtrés. Disposant d'un temps de réponse se dégradant à chaque accès, l'utilisateur se décourage rapidement et cesse d'accéder les sites filtrés. Les sites non filtrés conservent des temps de réponse non dégradés.

**Filtrage par REVERSE DNS -** SmartFilter réalise un filtrage sur la base d'URLs renseignées dans sa liste de contrôle. De plus, et afin d'éviter les tentatives de connexion par adresse IP, SmartFilter réalise une résolution reverse DNS qui renforce la sécurité.

**Profil par utilisateur et/ou par groupe -** La gestion des profils permet d'allouer une restriction à un utilisateur ou à un groupe d'utilisateurs (Exemple : Comptabilité, développement, front office…). Cette fonctionnalité permet d'utiliser aisément l'organisation de votre site comme référence des groupes d'utilisateurs. SmartFilter possède une interface LDAP, Active Directory et NTLM.

**Restriction par station de travail -** Cette fonctionnalité permet d'attacher une restriction à une station de travail ou à un groupe de stations de travail sans impacter les autres machines.

**Mise à jour automatique -** L'administrateur peut configurer le produit pour une mise à jour automatique auprès du site FTP de Secure Computing (Mise à jour automatique paramétrable : Journalièrement, une fois par semaine ou une fois par mois). La mise à jour manuelle est également possible par utilisation d'un raccourci. Le téléchargement de la liste de contrôle SmartFilter s'effectue en mode incrémental.

**Paramétrage des messages d'erreur -** Tous les messages visibles par les utilisateurs sont paramétrables et modifiables par l'administrateur du produit.

**Filtrage par tranche horaire -** Fonctionnalité permettant d'activer un filtrage pendant certaines heures de la journée, certains jours de la semaine. Ceci permet de bloquer les accès pendant les heures de bureau ou pendant les heures de saturation du réseau.

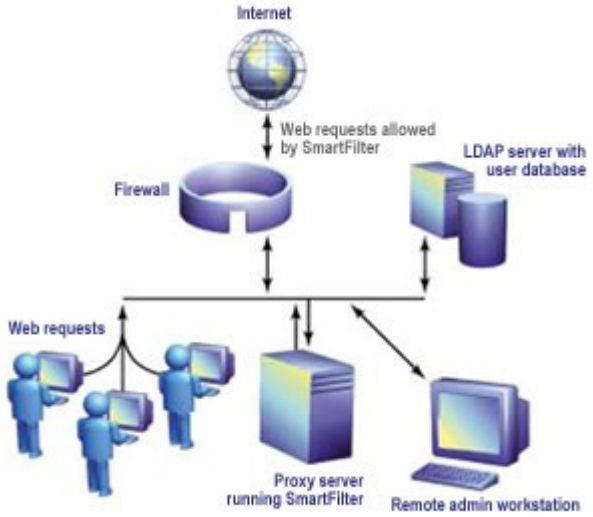
**Catégories paramétrables et personnalisation -** Cette fonctionnalité autorise l'administrateur à créer ses propres catégories et à restreindre l'accès à des sites non filtrés par la liste de contrôle

Secure Computing. Ces catégories permettent également la mise en place d'une liste blanche (Seules les URLs de la catégorie «liste blanche» sont accessibles par une population).

**Restriction par mots clés et "Pattern Matching" -** SmartFilter permet de mettre en œuvre une restriction par mots clés sur les moteurs de recherche. Cette fonctionnalité est paramétrable par l'administrateur de manière à pouvoir interdire les sujets indésirables. Le «Pattern Matching» permet re-catégoriser des groupes d'URLS. Ces niveaux supplémentaires de restriction permettent d'affiner le filtrage pour certaines populations.

**Restriction de téléchargements -** SmartFilter permet d'interdire le téléchargement «Enregistrer la cible sous» en fonction des extensions de fichiers. Ainsi, pour une population donnée, il est possible d'interdire les téléchargements de fichiers MP3, ZIP, AVI, EXE…

**Logs et rapports -** Le produit est livré avec la fonctionnalité de reporting. Cet outil permet de générer des rapports complets et détaillés sur les filtrages effectués, par catégories, par utilisateurs, par groupes, par temps de connexion…




## 5. Les principales solutions antivirales

Les virus informatiques sont aujourd'hui omniprésents dans la société du 21ème siècle. Les entreprises investissent des millions d'euro chaque année. Pourtant des entreprises perdent régulièrement de nombreuses données, des réseaux se trouvent bloqués malgré tout.

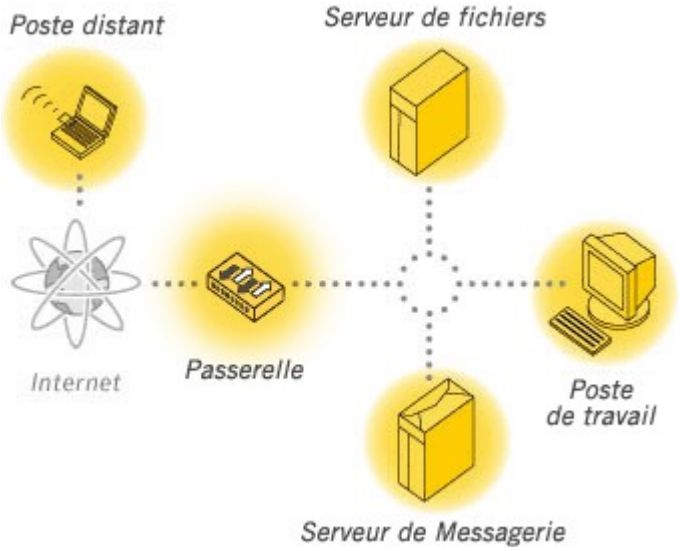
Dans cette partie, on vous propose de découvrir les deux principales solutions antivirales existantes sur le marché, qui sont :

- Symantec Antivirus Enterprise Edition ;
- Trend Micro.

## 5.1 Symantec Antivirus Enterprise Edition

La présente suite inclut les produits suivants :

- Symantec AntiVirus Corporate Edition 10.0
- Symantec Mail Security 4.6 pour Microsoft Exchange
- Symantec Mail Security 4.1 pour Domino
- Symantec Mail Security pour SMTP 4.1
- Symantec Web Security 3.0




L'objectif de cette suite est d'assurer une protection multi-niveaux au sein du réseau de l'entreprise tel que montré dans la figure suivante :

### 5.1.1 Symantec AntiVirus Corporate Edition

Symantec AntiVirus Corporate Edition assure une protection automatisée des postes de travail et des serveurs réseau contre les virus et les logiciels espions. La centralisation de la configuration, du déploiement, des alertes et de la journalisation permet aux administrateurs réseau de déterminer les nœuds vulnérables face aux attaques. Le contenu intégré permet en outre d'optimiser les temps de fonctionnement de vos systèmes, de réduire le coût de possession et de garantir l'intégrité des données.

La protection en temps réel réduit les risques de propagation des logiciels espions et publicitaires, tandis que la suppression automatique permet d'éliminer facilement les menaces de sécurité. La réparation des effets secondaires nettoie automatiquement les entrées de registre, les fichiers et les paramètres de navigation suite à une infection par des logiciels espions difficiles à identifier. Les administrateurs disposent d'une grande flexibilité et peuvent organiser, application par application, les politiques de sécurité de l'entreprise relatives aux logiciels espions et publicitaires. De plus, l'interface de gestion réputée de Symantec AntiVirus Corporate Edition offre un contrôle maximal des paramètres de protection. En outre, la protection renforcée contre les manipulations frauduleuses empêche les accès non autorisés et les attaques à l'encontre des processus et des entrées de registre.

Les menaces potentielles sont automatiquement soumises pour analyse à Symantec Security Response, qui propose une méthode d'intervention et de réparation. Grâce à une fonction de suivi approfondi (*Forensics ou assistance informatico-légale*), les administrateurs peuvent déterminer la

source des menaces combinées qui se propagent via les partages de fichiers ouverts. Par ailleurs, la fonction avancée de blocage en fonction des comportements empêche l'utilisation malveillante des systèmes clients en sortie (par ex. l'envoi de vers par courrier électronique). LiveUpdate assure la protection contre les virus, les codes malveillants et les logiciels espions à l'aide d'une mise à jour unique par un seul fournisseur. Enfin, la technologie de conformité des systèmes clients permet à l'administrateur de s'assurer que les systèmes distants et mobiles connectés aux ressources de l'entreprise via le réseau VPN sont conformes aux politiques de sécurité en vigueur.

### 5.1.2 Symantec Mail Security 4.6 pour Microsoft Exchange

La technologie antivirus extensible NAVEX™ de Symantec assure la protection contre les virus connus, même récents. Pour garantir une réaction et une protection immédiates contre les menaces émergentes, Symantec Mail Security s'appuie sur la mise à jour horaire des définitions de virus et sur une fonction de blocage en fonction de l'objet et des pièces jointes. La solution est également dotée de la fonction Mass-Mailer Cleanup, qui élimine les vers contenus dans le courrier de masse. Enfin, l'intégration de LiveUpdate permet de déployer les définitions de virus à l'échelle de l'entreprise sans interrompre les services d'analyse, ni provoquer l'arrêt des serveurs.

Symantec Mail Security pour Microsoft Exchange inclut des outils antispam de base tels que la détection heuristique, des règles de filtrage personnalisées et l'emploi de listes noires et blanches en temps réel. Les messages sont traités différemment selon le niveau choisi de spam SCL (Spam Confidence Level). Enfin, le contenu indésirable peut être filtré selon diverses caractéristiques du message (par ex. objet, pièce jointe, corps et taille du message).

Symantec Mail Security pour Microsoft Exchange assure une prise en charge totale de Microsoft Exchange 2003. Il peut être géré de manière centralisée à l'aide d'une console multi-serveurs pour une mise à jour simultanée des paramètres de serveur Microsoft Exchange à l'échelle de l'entreprise.

### 5.1.3 Symantec Mail Security 4.1 pour Domino

La protection antivirus de référence vous protège des virus connus et inconnus, en utilisant la technologie antivirus extensible NAVEX de Symantec. Les fonctions de blocage d'objet et de pièce jointe améliorent la protection en réagissant immédiatement face aux menaces émergentes. La fonction de nettoyage du courrier de masse permet également d'éliminer des bases de données Domino les messages infectés par des vers.

Les outils antispam de base comprennent un moteur antispam heuristique, des règles de filtrage personnalisées et plusieurs techniques de liste blanche afin d'optimiser la détection et de réduire les faux positifs. Les administrateurs peuvent filtrer le contenu indésirable en fonction des caractéristiques du message, telles que l'objet, la pièce jointe, la taille du message, ainsi que les mots et les phrases contenus dans le corps de message.

L'intégration transparente à l'environnement Lotus Domino permet aux administrateurs de configurer la protection en local ou à distance, de définir des configurations différentes pour

chaque serveur ou groupe de serveurs et de mettre à jour de manière dynamique la protection antivirus, sans bloquer les services d'analyse ni rendre les serveurs indisponibles. Grâce à sa fonctionnalité intégrée LiveUpdate, les nouvelles définitions de virus peuvent être immédiatement déployées en toute sécurité dans toute l'entreprise, offrant ainsi une protection optimale contre les infections virales se propageant rapidement. En outre, cette solution est prise en charge par Symantec Security Response, l'équipe mondiale d'intervention et de recherche en matière de sécurité.

### 5.1.4 Symantec Mail Security pour SMTP 4.1

Symantec Mail Security pour passerelle SMTP offre une protection intégrée et ultra performante contre les virus, le spam et tout autre contenu indésirable, au premier point d'accès du réseau : la passerelle (SMTP) de messagerie Internet. La protection antivirus de référence vous protège des virus connus et inconnus, en utilisant la technologie antivirus extensible NAVEX de Symantec. Les fonctions de blocage d'objet et de pièce jointe améliorent la protection en réagissant immédiatement face aux menaces émergentes. La fonction de nettoyage du courrier de masse permet également d'éliminer les messages infectés par des vers. Enfin, grâce à LiveUpdate, les définitions de virus peuvent être déployées dans l'entreprise sans interrompre les services d'analyse ni rendre les serveurs indisponibles.

Les outils antispam de base comprennent un moteur antispam heuristique, des règles de filtrage personnalisées, des listes noires tierces et personnalisées en temps réel et plusieurs techniques de liste blanche afin d'optimiser la détection et de réduire les faux positifs. La fonction de liste blanche auto-générée mémorise automatiquement les domaines de messagerie considérés comme fiables par votre entreprise pour faciliter la création d'une liste blanche complète. En outre, le traitement flexible des messages électroniques indésirables permet aux administrateurs d'ajouter des indicateurs personnalisés aux messages, de déterminer différentes mesures en fonction de la gravité du message électronique indésirable et de répartir les tâches associées au contrôle des messages électroniques indésirables. Les administrateurs peuvent filtrer le contenu indésirable en fonction des caractéristiques du message, telles que l'objet, la pièce jointe, la taille du message, ainsi que les mots et les phrases contenus dans le corps du message.

### 5.1.5 Symantec Web Security 3.0

Symantec Web Security protège votre trafic HTTP/FTP avec l'analyse ponctuelle évolutive et performante grâce aux technologies de filtrage de contenu et antivirus de référence. Elle optimise la productivité des employés et les performances réseau en limitant le trafic aux sites Web professionnels appropriés et en éliminant les attaques de codes malveillants sur Internet. Cette solution, développée exclusivement par Symantec, intègre des analyses contextuelles, heuristiques basées sur les listes pour protéger la passerelle Web contre les virus et le contenu indésirable.

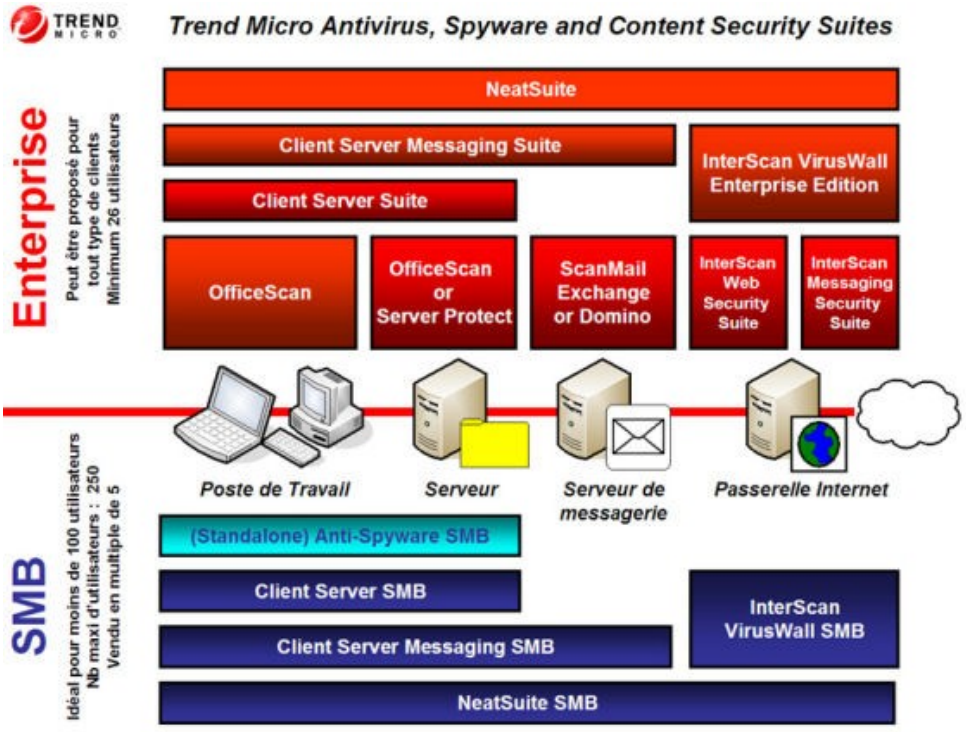
Symantec Web Security est une solution intégrée de filtrage antivirus et de contenu indésirable. Symantec recherche, développe, intègre et prend en charge ses propres listes de filtres URL

internationales et diverses technologies de protection de référence. Le moteur d'analyse modulaire NAVEX de Symantec détecte les nouvelles classes de virus sans désinstaller les logiciels existants, redéployer les nouveaux logiciels ou réinitialiser le système. Les technologies Striker Bloodhound et LiveUpdate de Symantec offrent une protection en temps réel, multi-niveaux et permanente contre les attaques de codes malveillants. La technologie d'analyse de contenu brevetée multilingue Dynamic Document Review de Symantec analyse les relations entre les mots pour bloquer l'accès au contenu Web inapproprié.

Les fonctions de gestion des politiques multi-serveurs centralisées et le support sécurisé et intégré des services d'annuaires externes, y compris Utilisateurs/Groupes LDAP et NT, garantissent une administration, une application des politiques et des notifications flexibles et simples pour plusieurs utilisateurs, groupes et serveurs. Symantec Web Security contrôle, consigne, lance un audit et fournit des outils d'alertes automatisés. Ce produit améliore également le débit réseau en réduisant tout le trafic Internet, optimisant ainsi la fiabilité et la sécurité du réseau et du pare-feu. Symantec Web Security est pris en charge par Symantec Security Response.

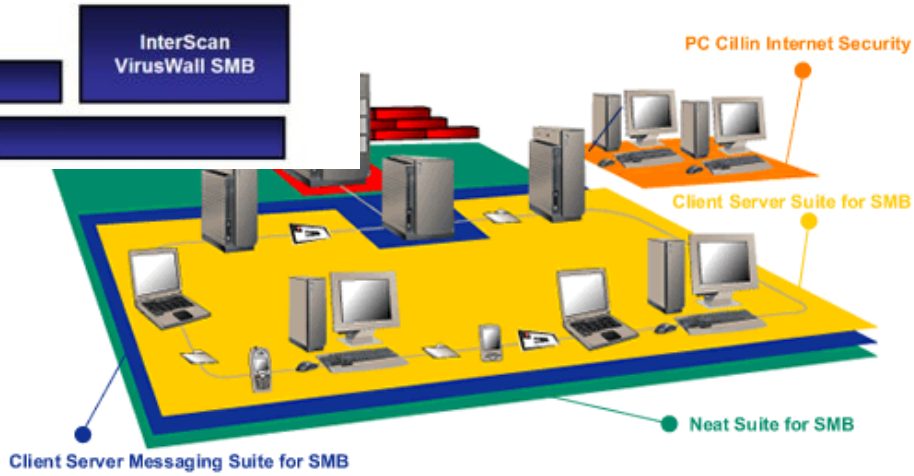
## 5.2 Trend Micro

Trend Micro propose des solutions multi-niveaux et à tout type d'entreprise tel que montré dans la figure suivante :




Pour les petites et moyennes entreprises, le défi consiste à optimiser les avantages commerciaux d'Internet sans les risques. Pour cette catégorie de clients, Trend Micro a créé une série de solutions qui permet de répondre à ces besoins.

Trend Micro propose une protection unique contre les virus informatiques et les menaces de la sécurité du contenu, dédiée aux PCs et serveurs.



- PC-Cillin Internet Security
- Client Server Suite for SMB
- Client Server Messaging Suite for SMB
- InterScan VirusWall for SMB
- NeatSuite for SMB

Les suites Trend Micro répondent aux besoins spécifiques des PME, avec une administration simplifiée de la sécurité du système de messagerie (Microsoft Exchange), des serveurs de fichiers ou d'application et des postes de travail.

Basées sur une technologie identique à celle des produits "Entreprise", les solutions de sécurité Trend Micro dédiées au Petites et Moyennes Entreprises sont spécifiquement conçues pour répondre à vos besoins et permettent de créer un environnement informatique sécurisé pour votre entreprise :

- **Ces solutions nécessitent peu ou pas de personnel IT dédié**
- **Facilité de gestion**
- **Procédure d'installation simple**

La solution globale que nous allons étudier est NeatSuite for SMB

### 5.2.1 NeatSuite for SMB

La solution NeatSuite de Trend Micro pour PME-PMI combine un moteur antispam heuristique élaboré avec fonction de recherche de la signature, des listes d´expéditeurs "autorisés" et/ou "interdits" afin de fournir un excellent niveau de détection des spams avec un nombre très faible de faux positifs.

Alors qu´un pare-feu restreint l´accès non autorisé à votre réseau, NeatSuite pour PME-PMI offre l´assurance que les menaces provenant d´Internet n´infiltrent pas le réseau via les canaux de communication ouverts nécessaires aux affaires de l´entreprise : messagerie (SMTP, POP3), accès au Web (HTTP) et téléchargement de fichiers (FTP). Avec ses moteurs d´antivirus, de filtrage du contenu et d´antispam reconnus, NeatSuite pour PME-PMI offre une protection complète au niveau de la passerelle, de la messagerie, du serveur et du poste de travail.

La Solution NeatSuite pour PME-PMI assure les fonctionnalités suivantes :

**Solution alliant antivirus, filtrage du contenu et antispam**

- Simplifie l'installation, la configuration et l'assistance via une console de management à interface Web unique et intuitive pour postes de travail, serveurs et serveurs de messagerie.
- Supprime les difficultés liées à la maintenance de plusieurs solutions antivirus.

### Protection WEB

- Scanne activement les fichiers téléchargés depuis Internet à la recherche de tout contenu malveillant
- Empêche l'introduction accidentelle de virus par les employés via leur compte personnel de messagerie Internet
- Scanne les codes de programmation Web suspects, comme les scripts et applets Java
- Définit et consigne les URL visitées, facilitant ainsi l'application des politiques de sécurité

### Moteur antispam heuristique

- Associe un moteur antispam heuristique à une base de données contenant les signatures des spams et à des listes d'expéditeurs "autorisés" et "refusés" afin d'assurer une détection précise et un nombre faible de faux positifs
- Bloque les messages considérés comme des spams ou les marque afin qu'ils soient filtrés

### Diminution des menaces

- Bloque les types de fichiers non souhaités ou suspects joints aux messages, tels que les fichiers VBS, SHS, JS, CGI ou DLL

### Protection fiable et intégrale

- Protège efficacement les postes de travail, serveurs, serveurs de messagerie et passerelle Internet de manière transparente, avec un niveau d'interférence minimum avec le système d'exploitation
- Élimine les virus, chevaux de Troie, vers et autres codes malveillants qui franchissent la passerelle Internet ou atteignent les postes de travail ou les serveurs via la messagerie électronique, les téléchargements à partir du Web ou le partage de fichiers
- Verrouille l'antivirus du poste de travail afin d'éviter toute fraude ou désactivation de la protection antivirus
- Consigne l'utilisation d'Internet, permettant ainsi aux employés de surveiller et d'appliquer les politiques d'utilisation des ressources

### Solution conçue pour une installation simple et rapide

- S'installe à distance et de manière transparente sur les postes de travail en réseau, les serveurs de fichiers et les serveurs de messagerie
- S'installe simultanément sur plusieurs postes de travail et serveurs, permettant une économie de temps et d'énergie
- Supprime automatiquement les produits antivirus non souhaités installés sur le poste de travail

### Mises à jour transparentes automatiques

- Maintient automatiquement la protection antivirus à jour, sans intervention de l'utilisateur
- Vérifie automatiquement, toutes les heures, la présence de mises à jour par l'intermédiaire de TrendLabs
- Rapidité de mise à jour réduisant le risque d'épidémie virale

### Surveillance des épidémies virales

- Surveille de manière proactive les activités du réseau et du système pour pouvoir émettre des avertissements sur les nouvelles menaces inconnues très tôt
- Initie un rapide balayage de virus au sein de l'entreprise en cas de menace d'épidémie, actualisant la protection de tous les postes de travail, serveurs, serveurs de messagerie et passerelle Internet à l'aide des dernières mises à jour des fichiers de signatures de virus et moteurs de scan

## 6. Les principales solutions VPN

Les réseaux privés virtuels ou VPN (*Virtual Private Network*) sont utilisés par les entreprises pour établir des connexions sécurisées de bout en bout, sur une infrastructure de réseau public.

Ils sont devenus la solution incontournable des connexions à distance pour deux raisons essentielles :

- Leur déploiement permet de réduire les coûts de communication en optimisant les infrastructures commutées locales des fournisseurs de services d'Internet.
- Les réseaux VPN permettent aux télétravailleurs, aux travailleurs mobiles comme à ceux qui emportent du travail à domicile de bénéficier d'un accès à haut débit.

Pour tirer le meilleur parti des réseaux VPN hautes performances, l'entreprise doit déployer une solution VPN solide et hautement disponible avec des périphériques VPN dédiés optimisés pour cet environnement.

Dans cette partie, on va vous présenter les deux principales solutions sur le marché en matière de VPN, qui sont celles de Cisco et d'Aventail.

### 6.1 La gamme Cisco VPN 3000

La gamme de concentrateurs professionnels VPN 3000 est une solution de pointe pour les réseaux VPN d'accès distant. Des clients VPN standard et simples à utiliser, ainsi que des équipements de terminaison de tunnel VPN évolutifs, sont livrés avec un système de gestion qui permet aux entreprises d'installer, de configurer et de contrôler facilement leurs réseaux VPN d'accès à distance. En intégrant des fonctions de haute disponibilité parmi les plus avancées et une architecture d'accès distant spécifiquement conçue à cet effet, le concentrateur Cisco VPN 3000 offre des performances exceptionnelles et évolutives ainsi que des infrastructures VPN solides pouvant prendre en charge les applications d'accès distant essentielles pour leur activité. Unique

sur le marché, il s'agit de la seule plate-forme évolutive avec composants échangeables sur site pouvant être mis à niveau par l'utilisateur. Ces composants, intitulés modules SEP (*Scalable Encryption Processing*), permettent à l'utilisateur d'augmenter facilement le débit et d'exploiter la capacité maximale du système. Les concentrateurs

Cisco VPN 3000 prennent en charge un grand nombre d'installations logicielles client VPN, dont le client Cisco VPN 3000, Microsoft Windows 2000 L2TP/IPSEC Client et Microsoft PPTP pour Windows 95, Windows 98, Windows NT 4.0 et Windows 2000.

Deux modèles de concentrateur Cisco VPN 3000 sont disponibles, pour répondre à tous les besoins professionnels des PME/PMI :

- **Concentrateur Cisco VPN 3005 -** Le concentrateur Cisco VPN 3005 est une plate-forme VPN conçue pour les PME disposant d'une bande passante ne dépassant pas le mode bidirectionnel T1/E1 (pas plus de 4 Mbits/s) avec un maximum de 100 sessions simultanées.

  Le traitement du cryptage est effectué par logiciel. Le Cisco VPN 3005 ne dispose pas de fonctions de mise à niveau intégrées.

- **Concentrateur Cisco VPN 3015 -** Le concentrateur Cisco VPN 3015 est une plate-forme VPN conçue pour les PME disposant d'une bande passante ne dépassant pas le mode bidirectionnel T1/E1 (pas plus de 4 Mbits/s) avec un maximum de 100 sessions simultanées.

  Comme pour le Cisco VPN 3005, le traitement du cryptage est effectué par logiciel.

### 6.1.1 Client Cisco VPN 3000

Son déploiement et son utilisation simples font du client Cisco VPN 3000 un moyen de définir des tunnels cryptés de bout en bout et sécurisés pour le concentrateur Cisco VPN 3000. Cet équipement compatible IPSEC extra plat est livré avec le concentrateur Cisco VPN 3000 et une licence pour un nombre illimité d'utilisateurs. Le client peut être préconfiguré pour un déploiement massif et ses connexions initiales requièrent une intervention minimale de l'utilisateur. La création et le stockage des politiques d'accès VPN sont centralisées sur le concentrateur Cisco VPN 3000 et transmises au client lors d'une connexion.

### 6.1.2 Cisco VPN 3000 Monitor

Le Cisco VPN 3000 Monitor est une application logicielle destinée à la centralisation de la surveillance, des alertes et de la collecte de données sur un ou plusieurs concentrateurs Cisco VPN 3000. Cette application de type Java est compatible avec Windows 95, Windows 98, Windows NT 4.0 et Windows 2000. Le dispositif d'interrogation SNMP (*Simple Network Management Protocol*) permet d'obtenir des données statistiques sur chaque équipement. La vue Enterprise View permet d'afficher l'état de chaque périphérique du réseau.

L'administrateur peut également afficher des données modulaires de chaque périphérique. En outre, le Cisco VPN 3000 Monitor enregistre des données rassemblées, les déroutements et les historiques d'analyse, de gestion des capacités et de dépannage.

### 6.1.3 Fonctions et avantages

#### Architecture à traitement distribué, hautes performances

- Support à grande échelle de tunnels IPsec, PPTP et L2TP/IPSEC. Évolutivité (Cisco VPN 3015)
- Conception modulaire (quatre emplacements d'extension) pour protéger les investissements, redondance et possibilité de mise à niveau simple.
- Architecture du système permettant de maintenir des performances régulières et une haute disponibilité.
- Conception numérique pour une fiabilité optimale et un fonctionnement ininterrompu, 24 heures sur 24.
- Équipements solides adaptés à la surveillance et aux alertes en cours d'exécution.
- Compatibilité Microsoft pour un déploiement client à grande échelle et une intégration continue aux systèmes associés.

#### Sécurité

- Support exhaustif des normes de sécurité existantes et émergentes pour l'intégration de systèmes externes d'authentification et l'interaction avec des produits tiers.
- Fonction de pare-feu à l'aide de filtrage de paquets sans état et de traduction d'adresses afin d'assurer la sécurité requise sur le réseau local d'une entreprise.
- Grande souplesse de la fonction de gestion des utilisateurs et des groupes.

#### Haute disponibilité

- Sous-systèmes redondants et systèmes automatiques de correction en cas de panne pour assurer une durée de fonctionnement optimale.
- Grand nombre d'outils et de fonctions de surveillance à la disposition des administrateurs réseau, état du système en temps réel et avertissements anticipés.

#### Gestion infaillible

- Les concentrateurs Cisco VPN 3000 peuvent être gérés à l'aide de navigateurs Web standard (HTTP ou HTTPS), par Telnet, Secure Telnet ou via le port de console.
- Les fonctions de configuration et de surveillance sont livrées aux entreprises et aux fournisseurs de services.

- Les niveaux d'accès peuvent être configurés par utilisateur ou par groupe, permettant ainsi de gérer facilement les politiques de sécurisation du système.

## 6.2 La gamme Aventail VPN SSL

Reconnu comme une des solutions VPN SSL les plus complètes du marché et comme la référence dans les produits et services VPN SSL « clientless », Aventail permet aux entreprises de fournir des accès distants fortement sécurisés vers tous types d'applications tout en considérant la spécificité et les contraintes de l'endroit où se trouve l'utilisateur : à la maison, dans un cyber café, chez un partenaire, ou dans un hotspot public par exemple.

Avec le VPN SSL, une entreprise va pouvoir disposer du même niveau de sécurisation apporté par les technologies IPSEC mais appliqué au niveau de l'application. Cette démarche granulaire, qui consiste à fixer les droits d'accès en prenant en compte les groupes d'utilisateurs, le lieu ou il se trouve et les applications une par une, va générer un gain de productivité important tant pour les utilisateurs finaux que les équipes informatiques chargées de l'administration.

L'EX-750 est construit sur la plate-forme ASAP (Anywhere Secure Access Policy) d'Aventail, qui supporte toutes les applications du marché, un logiciel complet d'administration de la politique de sécurité et des fonctions EPC (End Point Control) incluant notamment un cache cleaner aux fonctionnalités avancées.

L'EX-750 correspond exactement aux entreprises, désirant un produit capable de proposer les mêmes fonctionnalités évoluées présentes dans la version EX-1500 mais adapté aux besoins et ressources des PME/PMI.

### 6.2.1 Les options d'Aventail Smart Access

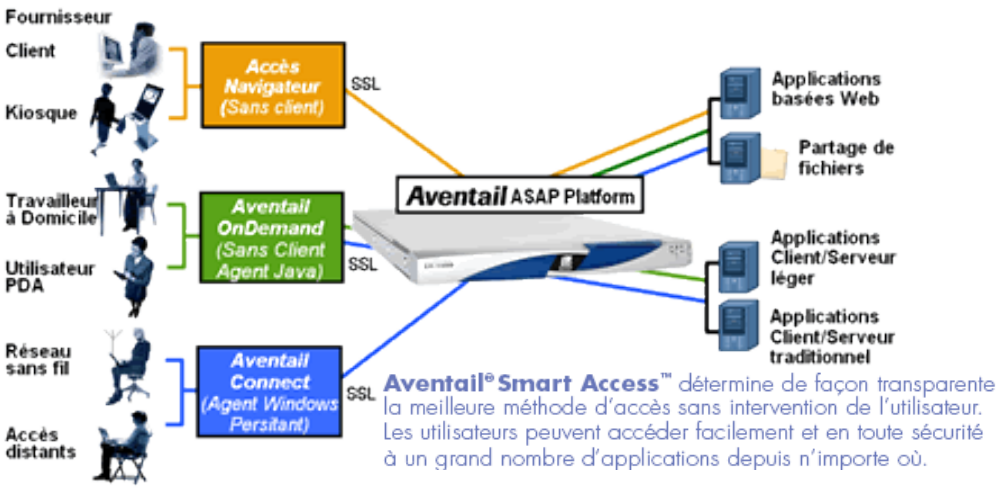
Les boîtiers VPN SSL d'Aventail offrent tout ce dont vous avez besoin pour fournir un accès sécurisé à n'importe quelle application sur n'importe quel périphérique. La plate-forme d'accès sécurisé aux applications est conçue pour fournir à l'utilisateur un accès pratique et facile à utiliser depuis n'importe où et, à l'administrateur, une gestion simple, conviviale et une réduction des risques.

Pour les utilisateurs finaux, Aventail Smart Access offre une expérience d'accès transparente :

- Accès par navigateur Web sans client pour les applications Web et de partage de fichiers.
- Accès transparent avec Aventail OnDemand, un petit agent Java, pour les applications client/serveur.
- Aventail Connect, un client Windows téléchargeable, pour un accès pratique et complet aux applications, avec une protection de réseau et de bureau supplémentaire.
- La méthode d'accès—ainsi que le niveau de sécurité—sont déterminés et déployés automatiquement pour une sécurité et une facilité d'utilisation poussées à l'extrême.

Pour les administrateurs, la Console de gestion (AMC) Aventail ASAP intuitive d'Aventail basée sur le Web et le modèle de règles orienté objet offrent le contrôle le plus puissant avec la plus faible quantité de travail. Unique dans le secteur, Aventail Unified Policy offre une administration centralisée et une configuration unique couvrant toutes les ressources et méthodes d'accès.

### 6.2.2 Aventail End Point Control




Si les avantages en termes de productivité d'un accès à distance depuis n'importe où sont clairs, les risques le sont tout autant : vous fournissez maintenant un accès depuis des sites et des périphériques que le service de TI ne peut probablement pas contrôler. Aventail End Point Control (EPC) répond à ces menaces inhérentes à la sécurité au moyen de Device Interrogation—qui élimine les risques avant l'authentification, de Policy Zones—qui associe les accès à un niveau de confiance, et d'une protection des données—qui empêche les utilisateurs de laisser des informations confidentielles derrière eux dans des environnements non gérés tels qu'un terminal d'accès public. Aventail gère chacun de ces

domaines plus en profondeur, avec une plus grande facilité d'utilisation et avec une plus grande sécurité que les autres distributeurs.

Par exemple, Aventail offre des fonctions de protection des données telles qu'Aventail Cache Control pour un nettoyage de la mémoire cache avancé et Aventail Secure Desktop qui encrypte les données locales de l'utilisateur et les détruit à la fin de la session. Pour une plus grande protection contre l'ensemble des menaces liées à l'accès à distance, Aventail s'intègre avec les pare-feux, la détection d'intrusions et la protection antivirus de ses partenaires technologiques et avec les autres solutions de sécurité côté client.

# 7. Les principales solutions d'infrastructures de clefs publiques

## 7.1 La solution de Baltimore

UniCERT est une architecture qui délivre et gère des certificats et fournit des solutions de sécurité pour une organisation.

UniCERT se compose de 3 niveaux de technologie :

- **UniCERT core Technology** est le cœur de la PKI et fournit des fonctionnalités d'autorité de certification, d'autorité d'enregistrement, et de gestion des certificats.
  - Certificate Authority
  - Certificate Authority Operator
  - Registration Authority
  - Registration Authority Operator
  - Gateway : fonction de réception des demandes de certificats et de renvoi des certificats et informations correspondantes vers le web, les e-mails et les VPN.
- **UniCERT Advanced Technology** fournit des fonctions d'archivage de clefs, d'enregistrement des fonctions PKI dans un système.
- **UniCERT Extended Technology** au sommet des fonctionnalités de la PKI, fournit des services à valeur ajoutée comme l'horodatage.

## 7.2 La solution d'Entrust

Entrust/PKI est une solution d'infrastructure à clef publique qui gère automatiquement tous les processus de sécurité de l'organisation. Ce logiciel permet l'utilisation des signatures numériques, du chiffrement, des services de gestion de droits pour différentes applications.

- **Entrust/AutoRA :** gestion des certificats
- **Entrust/Roaming :** authentification des utilisateurs à partir d'un poste de travail quelconque pour l'accès aux données
- **Entrust/Timestamp :** assure une non-répudiation des transactions

## 7.3 La solution de Certplus

Certplus a été créé en 1998 par Gemplus, France Telecom, EADS (Aérospatiale Matra) et VeriSign. Depuis début 2000, la CIBP (Confédération Internationale des Banques Populaires) a rejoint le cercle des fondateurs.

Initiale est une offre PKI pour aider les entreprises à bâtir leur propre infrastructure de gestion de clefs.

Elle propose un cadre pour définir la politique de certification, les procédures d'enregistrement des demandes et de validation, etc.

Elle offre également les techniques de protection des clefs de signature des certificats, gestion des volumétries, personnalisation de cartes à puce, etc.

Différents modules peuvent venir se rajouter :

- Ajout d'administrateur(s)
- Module d'hébergement local
- Module d'administration automatisée
- Module d'intégration aux annuaires LDAP

## 7.4 La solution de RSA

La gamme **RSA Keon** est une suite de produits fournissant, gérant et facilitant l'utilisation des certificats numériques pour les applications de commerce électronique, les ERP, les VPN, le courrier électronique et toutes les applications Internet qui se doivent d'être sécurisés.

La technologie utilisée repose sur le standard de chiffrement asymétrique RSA.

- **RSA Keon Advanced PKI** enrichit les principales fonctionnalités de la PKI en supportant les certificats numériques émis par les principaux CA.
- **RSA Keon Certificate Server** est un composant du système qui fournit un moteur de gestion de clefs, de certificats, un annuaire LDAP et une base de certificats révoqués.
- **RSA Keon Certificate Authority** est une autorité de certification qui délivre, gère et signe des certificats numériques.

Elle est compatible avec les navigateurs Web, des smart cards, des modules de sécurité hardware, des VPN, des programmes de courrier électronique.

Cette autorité travaille avec **RSA Keon Registration Authority** (RA) pour la prise en compte des demandes de certificats des utilisateurs et la vérification d'identité.

Un module de recouvrement des clefs et certificats peut également être installé dans l'infrastructure.

**RSA Keon Web Passport** fournit une infrastructure PKI destinée au commerce inter-entreprise.

## 7.5 La solution de Microsoft

Windows 2000 offre la possibilité de gérer une PKI intégrée, en interaction avec certaines fonctionnalités d'Active Directory.

Il est donc possible d'émettre des certificats, ou de les révoquer et de définir une stratégie.

Windows 2000 permet de gérer des certificats de type X.509v3. Les extensions standards de la version 3 permettent notamment de stocker des informations relatives à l'utilisation des clefs, à la stratégie de certificats employée, ou encore aux contraintes des chemins d'accès de certification.

Les utilisateurs peuvent se servir de la console MMC pour gérer leur certificat.

Du côté serveur, un composant permet de gérer les certificats. Un autre composant offre des pages d'inscription des Autorités de Certification sur le Web. Ainsi les utilisateurs peuvent soumettre une demande de certificat via un serveur web.

Windows 2000 permet de gérer une hiérarchie d'Autorités de Certification, avec une CA racine et des CA secondaires.

Les CA secondaires sont certifiées par le certificat de la CA racine.

Hiérarchiser les autorités de certification permet de développer des stratégies de certification différentes, en fonction de l'utilisation des certificats, ou des divisions organisationnelles ou géographiques.

Par exemple, si vous voulez donner des certificats pour sécuriser le mail et des certificats pour s'authentifier au réseau, mais que vous voulez des stratégies de certification différentes selon le cas, vous pouvez créer des autorités de certification différentes, ce qui vous permettra entre autre de séparer l'administration.

Windows 2000 permet la prise en charge des cartes à puce pour de l'authentification.

Le système gère l'ouverture d'une session dont l'identification se fait par un certificat stocké sur carte à puce.

Il permet également d'utiliser les cartes à puce pour stocker des informations confidentielles, sécuriser la messagerie ou pour tout type d'activité liée à l'utilisation de clef publique.

Enfin la stratégie de groupe Windows 2000 permet d'automatiser des tâches telles que la distribution des certificats ou l'établissement des listes d'approbation de certificats et des CA communes.