Sécurité des Systèmes d'Information

CM2: Implémentation concrète de la sécurité

Sommaire

1. Les stratégies de sécurité

Stratégie des périmètres de sécurité :

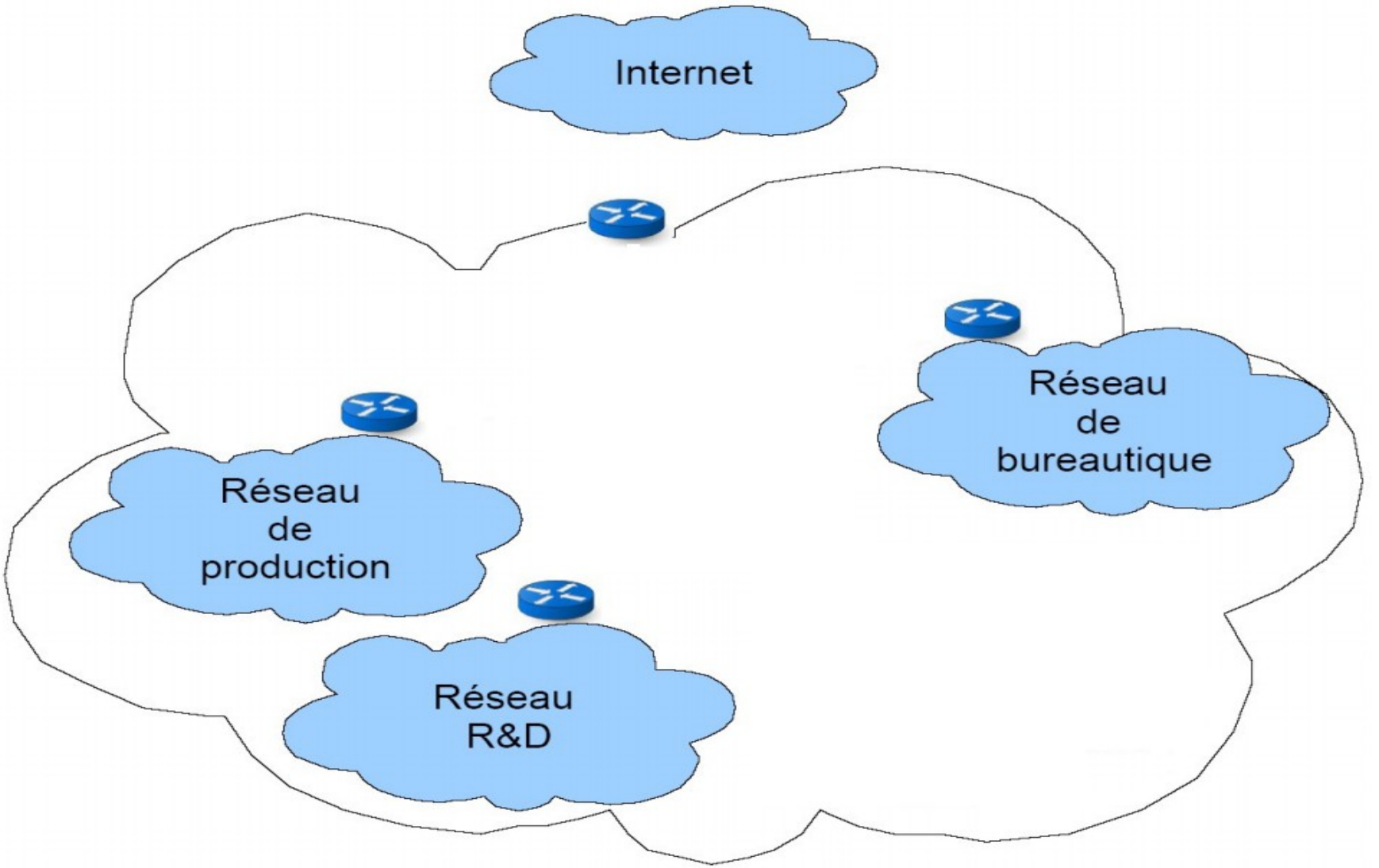
L'objectif est de découper le réseau d'entreprise en périmètres de sécurité logiques regroupant des entités ou fonctions afin de mettre en place des **niveaux de sécurité** à la fois **imbriqués** et **séparés**.

La première étape est la définition d'un périmètre de sécurité autour du réseau d'entreprise face au réseau Internet.

Il faut également définir un périmètre de sécurité autour de chacun de ces réseaux inclus dans le réseau intranet.

Cette compartimentation du réseau intranet rend plus difficile une éventuelle pénétration.

Stratégie des périmètres de sécurité :



Stratégie des périmètres de sécurité :

Cependant, cette stratégie n'est pas suffisante et doit être couplée avec celle des goulets d'étranglement.

Stratégie des goulets d'étranglement :

L'objectif est de définir des contrôles d'accès différenciés et en nombre limité pour permettre l'accès à chaque périmètre de sécurité du réseau intranet.

Les contrôles d'accès définissent ce qu'il est autorisé de faire pour entrer dans un périmètre de sécurité du réseau.

Stratégie des goulets d'étranglement :

Tout ce qui n'est pas autorisé doit être interdit et les contrôles d'accès définissent les conditions à respecter pour avoir le droit d'entrer dans un périmètre donné.

Les contrôles d'accès s'accompagnent des quelques règles évidentes suivantes :

• chaque système ne dispose que d'une seule connexion au réseau d'entreprise pour éviter les attaques par rebonds.

→ Si un ordinateur est connecté au réseau de l'entreprise d'un côté et de l'autre à Internet, un pirate pourrait, depuis Internet rebondir dans le réseau intranet !

Stratégie des goulets d'étranglement :

• Internet est un outil de travail et ne doit être utilisé que dans un cadre professionnel ;

• des contraintes sont installées sur les stations de travail pour éviter les installations de programmes non validés par l'équipe technique ;

• les logiciels de sécurité installés sur le poste doivent être mis à jour régulièrement ;

• interdiction d'utiliser un outil qui permettrait d'obtenir des informations sur le réseau de l'entreprise (scanner de vulnérabilité, outil de découverte de réseau, etc...).

Stratégie des goulets d'étranglement :

Les communications entre le réseau intranet et d'autres réseaux doivent être contrôlées et les services réseau accessibles sur Internet définis.

Ces flux doivent être également contrôlés pour vérifier qu'ils ne véhiculent pas de virus.

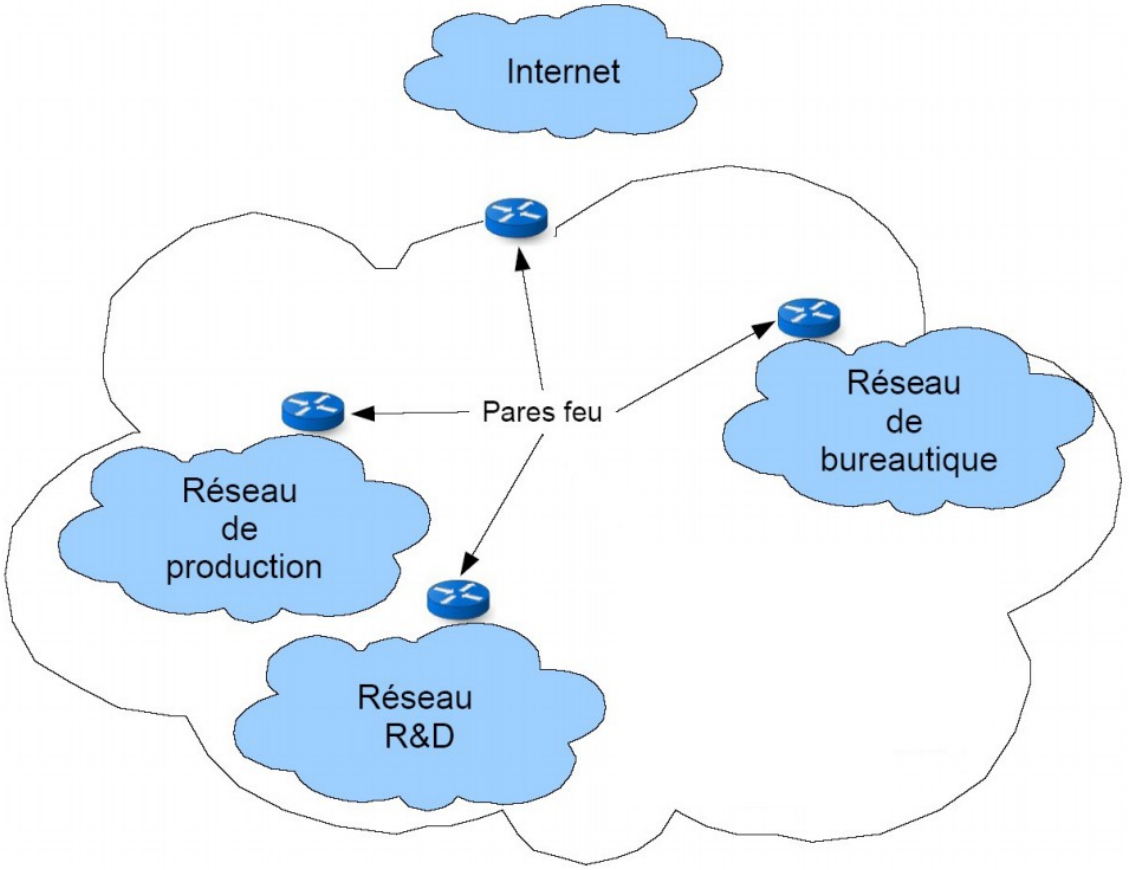
Une solution de filtrage de contenu pourra être mise en place pour s'assurer que les employés ne naviguent pas sur des sites interdits par la loi (pédophiles, pornographiques, pirates, etc...).

Stratégie des goulets d'étranglement :

Des mécanismes de surveillance doivent être appliqués aux périmètres de sécurité et toucher les domaines suivants :

- collecte et stockage des logs ;
- analyse des attaques (comme les sondes d'intrusion) ;
- analyse de trafic.

Stratégie des goulets d'étranglement :



Maintenant que les périmètres sont définis ainsi que les goulets d'étranglement, attelons-nous à authentifier les utilisateurs du réseau.

Stratégie d'authentification en profondeur :

L'objectif est de mettre en place des contrôles d'authentification pour authentifier les accès aux périmètres de sécurité.

Pour ce faire, il est recommandé d'installer des systèmes de contrôle d'authentification au sein d'un périmètre qui leur est réservé.

Ces contrôles peuvent avoir lieu au moment de la sortie sur Internet mais également au niveau de chaque serveur pour accéder au réseau interne.

Chaque fois qu'un utilisateur s'authentifie, un ticket est créé sur un système chargé de stocker les logs afin que le parcours de l'utilisateur soit connu à tout moment.

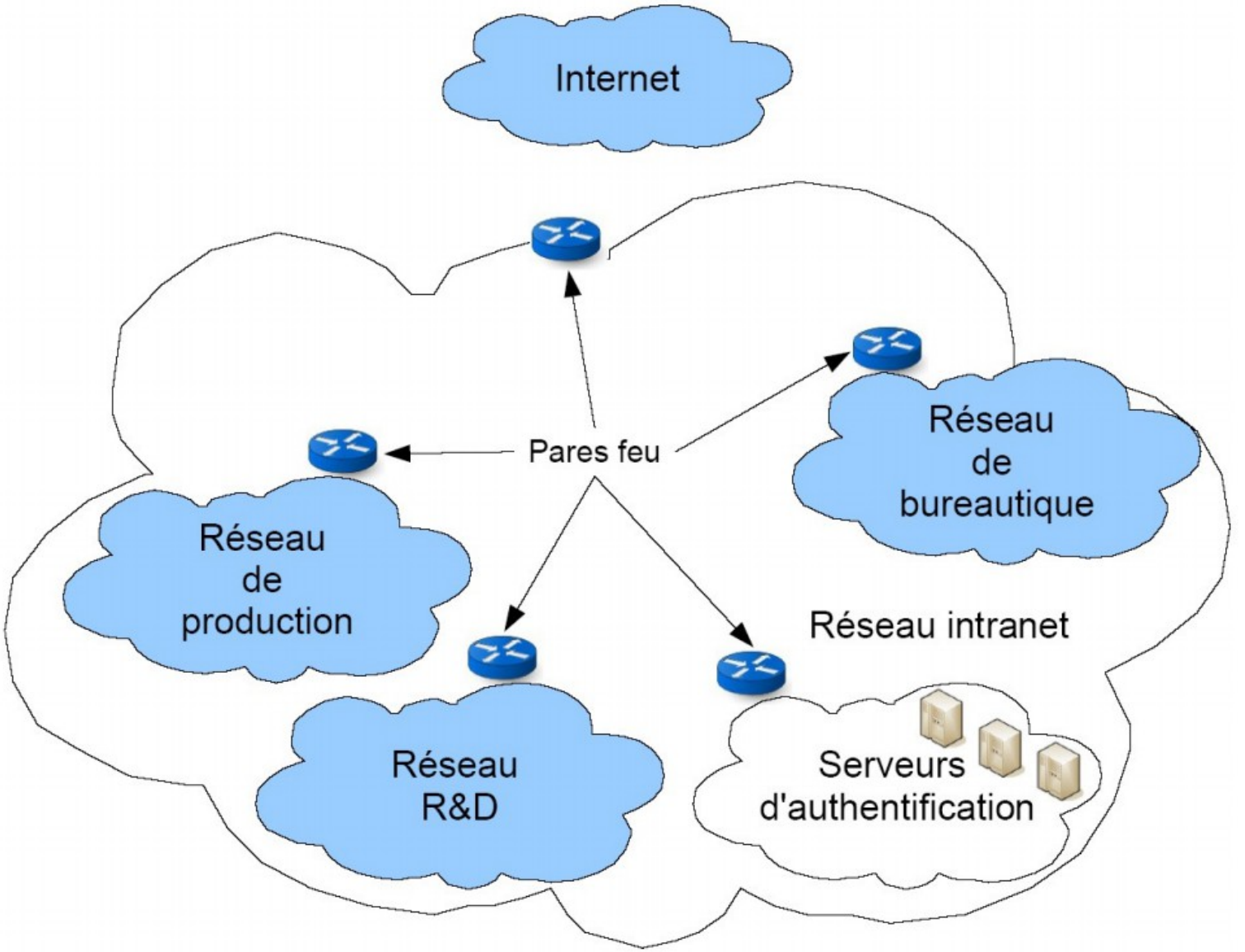
Stratégie d'authentification en profondeur :

Cette logique peut être étendue à chaque action de l'utilisateur comme la création, suppression ou impression d'un document ou encore les adresses Web visitées.

Lorsqu'un tel système est mis en place, on parle de modèle AAA (« Authentication, Authorization, Accounting ») ou authentification, autorisation et comptabilité d'événements.

Cependant la mise en place de ce type de systèmes est lourde et souvent très coûteuse.

Stratégie d'authentification en profondeur :



Stratégie d'authentification en profondeur :

On peut voir :

- les zones qui ont été définies par la stratégie des périmètres de sécurité ;

- les pare-feu qui constituent l'unique point d'entrée pour chaque zone, comme spécifié dans la stratégie par goulets d'étranglement ;

- les serveurs d'authentification qui servent à authentifier les accès aux périmètres de sécurité, comme spécifié dans la stratégie d'authentification en profondeur.

Stratégie du moindre privilège :

Cette stratégie a pour objectif de s'assurer que chacun dispose uniquement des privilèges dont il a besoin.

La portée de tout acte de malveillance s'en retrouve réduite aux privilèges dont dispose la personne qui le commet et il faudra une complicité de plusieurs personnes pour pouvoir mettre en péril le réseau intranet.

Un moyen simple de renforcer cette stratégie est d'augmenter les autorisations nécessaires pour accéder à une ressource.

Par exemple, pour accéder aux données comptables, la comptable a besoin de son code et de celui de sa responsable.

Stratégie du moindre privilège :

Cependant, ce mécanisme implique des contraintes supplémentaires de disponibilité, qui font qu'une comptable ne pourra accéder aux données comptables si sa responsable est en vacances.

L'application stricte de cette stratégie est difficile à réaliser et n'est souvent possible qu'avec la mise en place d'un système ***SSO*** (« ***Single Sign On*** »), qui permet d'authentifier un utilisateur quelle que soit son adresse réseau et de lui appliquer un profil à droit d'accès spécifique.

Stratégie de confidentialité des flux réseau :

L'objectif de cette stratégie est de protéger tout message qui doit être émis vers un autre réseau ou Internet.

Cette stratégie est généralement utilisée lorsqu'une entreprise a plusieurs sites qui sont reliés par le biais de réseau publics comme Internet, X25 ou encore de Lignes Spécialisées (***LS***).

Lorsqu'une entreprise crée un réseau de type WAN, elle construit un réseau central (« ***backbone*** ») et relie ces sites à ce réseau.

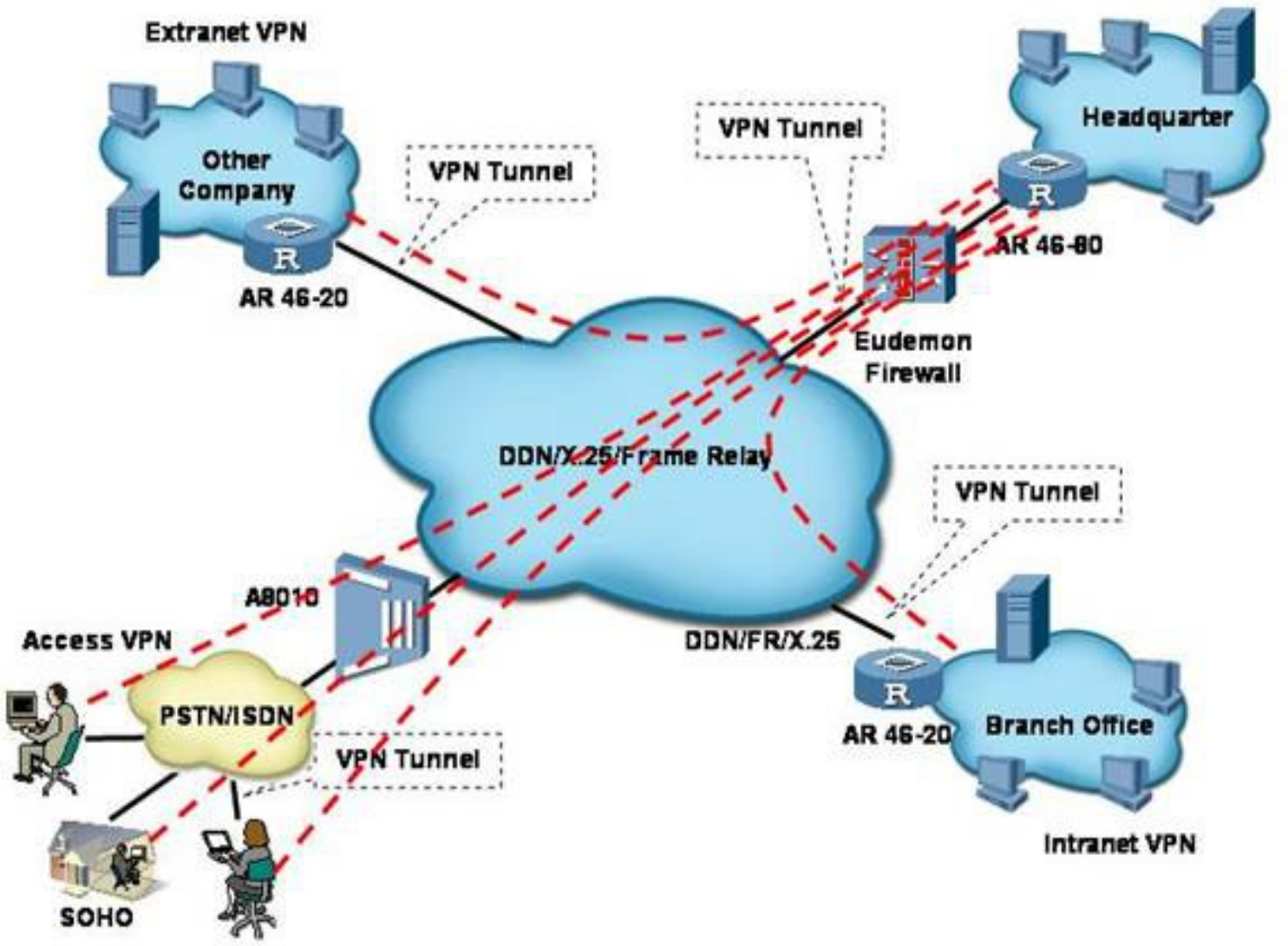
Des boîtiers de chiffrement, tel que des passerelles ***IPsec***, peuvent être installés entre les routeurs et les pare-feu pour garantir la confidentialité des communications inter-sites.

Stratégie de confidentialité des flux réseau :

Ainsi, tous les flux qui sortent de chaque site sont chiffrés à la volée par le boîtier de chiffrement placé en goulet d'étranglement sur les connexions inter-sites.

Il existe d'autres moyens de chiffrer les communications comme SSL, qui est très utilisé pour chiffrer les flux des serveurs Web.

Stratégie de confidentialité des flux réseau :



Stratégie de séparation de pouvoirs :

L'objectif est de créer des entités séparées chacune responsables de zones de sécurité distinctes du réseau intranet.

Cette stratégie s'adresse particulièrement aux entreprises de grande taille.

En effet, les petites entreprises, qui n'ont pas beaucoup de ressources à protéger, se contentent souvent d'un seul département chargé de leur maintenance.

En revanche, dans des entreprises plus grandes, il est nécessaire de séparer ou limiter les pouvoirs de chaque entité afin de limiter les conséquences d'un acte de malveillance.

Stratégie de séparation de pouvoirs :

Maintenant que des responsables sont définis pour chaque périmètre, il s'agit de contrôler tous les accès à ces périmètres.

Stratégie d'accès au réseau local :

L'objectif de cette stratégie est d'assurer qu'aucune porte dérobée interne ne permette d'accéder au cœur du réseau.

Pour contourner ce risque, il faut créer un contrôle d'accès à toutes les portes d'entrée du périmètre de sécurité.

Ce contrôle sera sous la responsabilité du périmètre de sécurité qui déterminera la politique d'accès à mettre en œuvre.

Stratégie d'accès au réseau local :

Pour y parvenir, il faut que tous les premiers éléments intelligents d'accès au réseau (commutateurs ou routeurs) fassent un contrôle d'accès.

La technologie ***AAA***, vue précédemment est particulièrement adaptée.

Stratégie d'administration sécurisée :

L'objectif de cette stratégie est de créer une zone d'administration dédiée et séparée du réseau afin d'assurer une isolation des systèmes chargés de l'administration de chaque périmètre de sécurité.

Une zone d'administration est en charge de vérifier le bon fonctionnement de tous les composants d'un périmètre de sécurité donné.

Cette zone est donc particulièrement sensible et doit être protégée de manière adéquate.

Stratégie d'administration sécurisée :

Cette stratégie est à mettre en place avec celle des goulets d'étranglement qui visent ici à réduire le nombre de points d'entrée dans les zones d'administration.

Conclusion :

Toute politique de sécurité réseau s'accompagne de stratégies ayant pour objectifs d'établir un premier niveau de règles de sécurité et, dans un deuxième temps, de mettre en œuvre des solutions techniques.

Les architectures réseau et les services offerts deviennent tellement complexes qu'il faut remettre en cause les mécanismes de sécurité préalablement définis le plus souvent possible.

Cette adaptabilité et cette réactivité vont permettre à l'entreprise de protéger au mieux ses périmètres de sécurité.

2. Les outils et technologies

Le pare-feu est un composant réseau qui permet :

• de concentrer l'administration de la sécurité en des points d'accès limités au réseau d'entreprise ;
• de créer un périmètre de sécurité.

Une architecture à base de pare-feu offre l'avantage de concentrer les efforts de sécurité en un unique point d'entrée.

Grâce à des mécanismes de filtrage en profondeur ainsi qu'à des fonctions de journalisation des événements, les pare-feu fournissent des informations de premier choix quand des investigations de sécurité doivent être menées.

Les principaux concepts du pare-feu sont :

- le filtrage de paquets ;
- le filtrage à mémoire ;
- la passerelle de niveau circuit ;
- la passerelle de niveau applicative.

Filtrage de paquets :

La première technologie de pare-feu réalise le **filtrage** :

- au niveau des protocoles de la **couche 3 du modèle OSI** ;
- sans mémoire des états des sessions ;
- sans conservation des informations ni analyse de chaque paquet ;
- sans aucune corrélation entre les paquets.

Le pare-feu agit comme une sonde placée sur le trafic réseau qui n'intervient pas sur les connexions TCP établies.

Filtrage de paquets :

Le filtrage est généralement effectué selon les critères suivants :

- adresse IP de l'émetteur et du destinataire ;
- port source et destination ;
- type de protocole (GRE, ICMP, IP, etc...).

La mise en œuvre de tels mécanismes de filtrage est relativement aisée, notamment au travers de règles Iptables sous Linux.

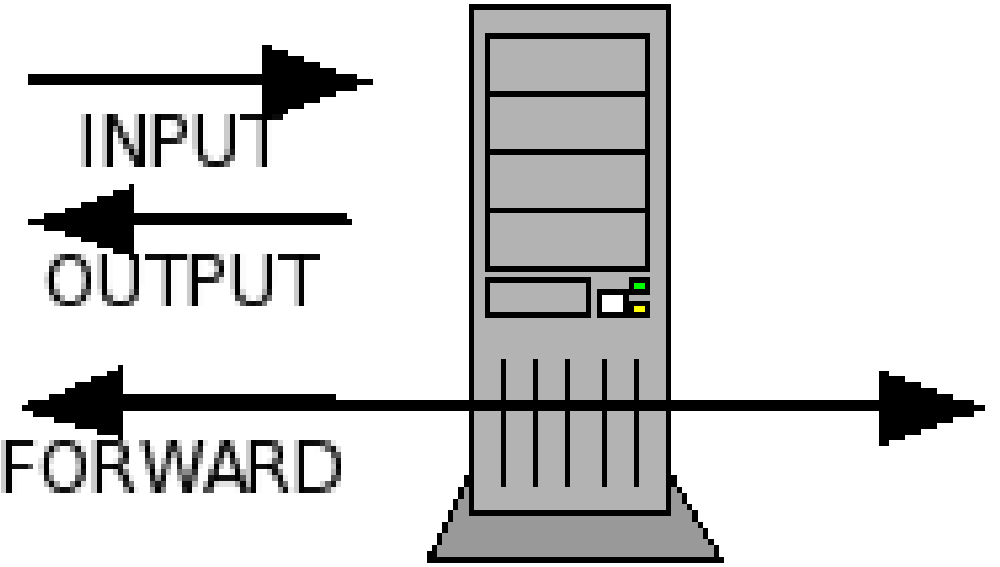
 # iptables -A INPUT -p tcp --dport 80 -j ACCEPT

(pour ouvrir le port *TCP/80* → laisser passer *HTTP*)

Filtrage de paquets :

Il existe trois chaînes dans la table ***filter*** d'Iptables :

- INPUT : pour filtrer le trafic entrant ;
- OUTPUT : pour filtrer le trafic sortant ;
- FORWARD : pour filtrer le trafic traversant.



Filtrage dynamique :

Les applications utilisent des ports sources dont on ne peut connaître la valeur à l'avance (valeur prise aléatoirement entre 1024 et 65535).

Le filtrage dynamique, ou « ***stateful*** », de paquets permet de suivre les sessions et d'adapter de manière dynamique les règles du pare-feu.

Les performances de ce type de pare-feu sont bonnes, puisque le filtrage consiste en une simple inspection du trafic de données.

Filtrage dynamique :

Cependant, la configuration de tels équipements est complexe du fait du grand nombre d'options de filtrages disponibles.

Ils sont généralement couplés à des solutions de **translation d'adresse** et de translation de port qui permettent de masquer le plan d'adressage internet du réseau d'entreprise.

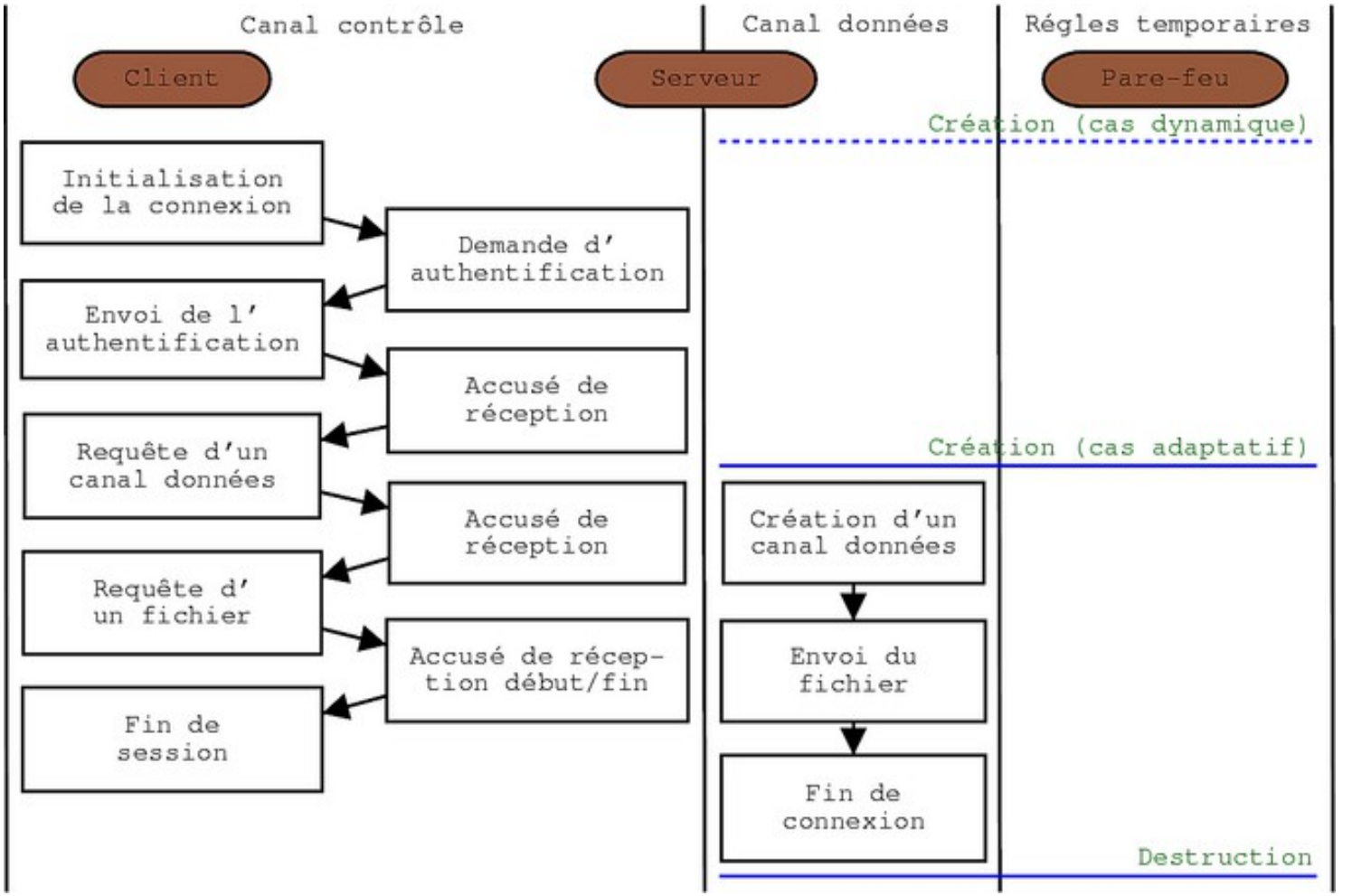
Filtrage dynamique :

Certains pare-feu bénéficient de technologies propriétaires comme ceux de la marque Checkpoint qui peuvent, grâce à leur technique de hachage du trafic, pointer directement sur la bonne règle de filtrage sans avoir à parcourir l'ensemble de l'ACL.

Les routeurs de la marque Cisco avec leur technologie CBAC (« *Context-Based Access Control* ») peuvent, quant à eux, réaliser des filtrages sur l'état des connexions des couches 3 et 4 du modèle OSI pour déterminer d'éventuelles attaques.

Filtrage dynamique :

Ci-dessous un schéma qui explique le déroulement d'une connexion FTP :



Passerelle de niveau circuit :

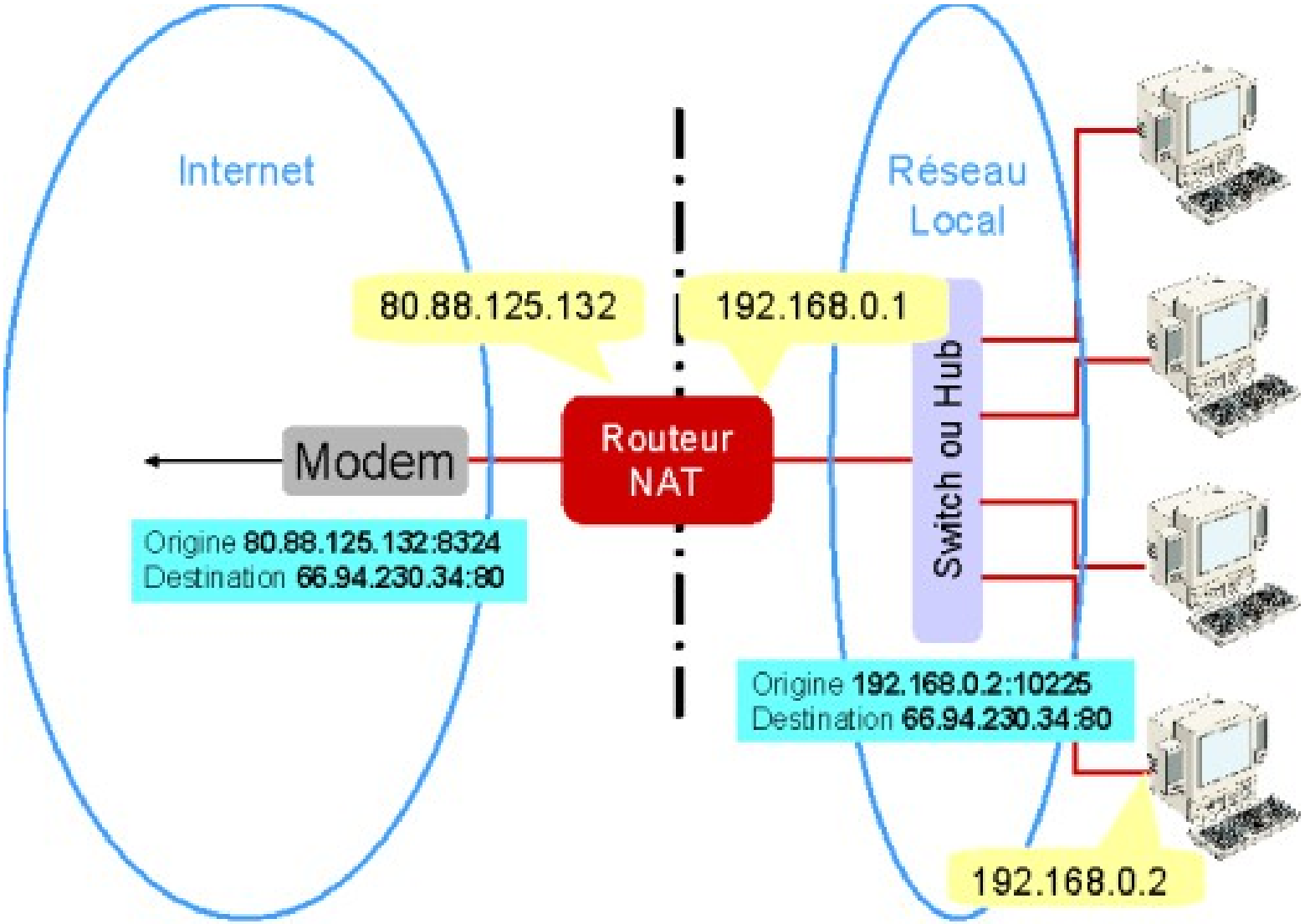
Une passerelle de niveau circuit est un pare-feu qui agit comme intermédiaire, ou passerelle, au niveau du périmètre de sécurité du réseau.

Chaque connexion qui traverse le périmètre de sécurité correspond à deux connexions réalisées par la passerelle, l'une entre l'utilisateur et la passerelle, l'autre entre la passerelle et le système visé par l'utilisateur.

Passerelle de niveau circuit :

Bien que cette technologie de translation d'adresse NAT (« ***Network Address Translation*** ») ait été initialement mise en place pour faire face à la pénurie d'adresses Ipv4, elle permet de « cacher » un grand nombre de systèmes derrière une seule adresse IP, améliorant ainsi la sécurité du réseau interne.

Passerelle de niveau circuit :



Passerelle de niveau applicatif :

Dans le filtrage de niveau applicatif, également appelé proxy, le pare-feu agit comme un filtre au niveau 7 du modèle OSI.

Pour y parvenir, chaque application est implémentée sur le pare-feu par l'intermédiaire d'un agent agissant comme un relais applicatif.

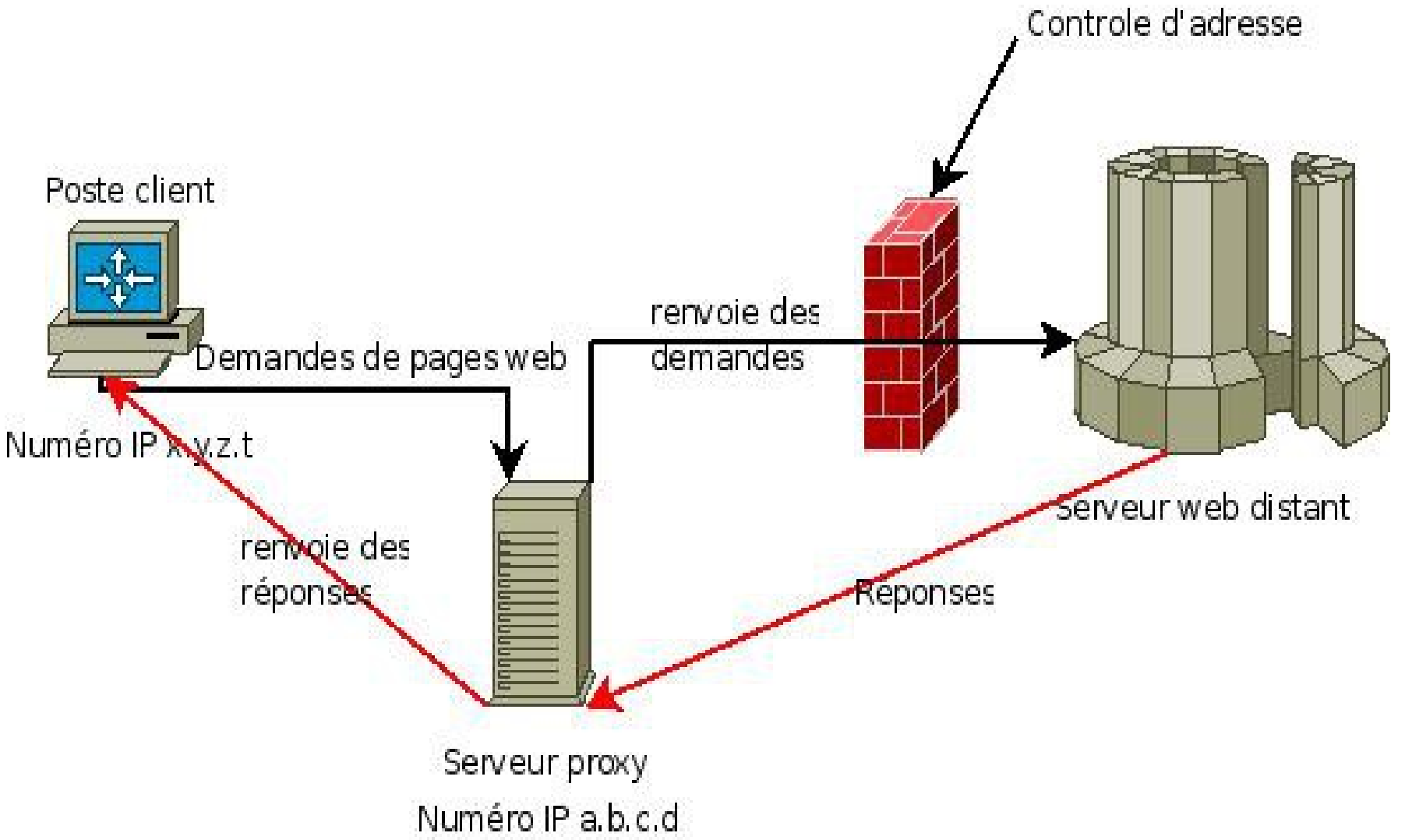
Chaque connexion qui traverse le périmètre de sécurité correspond donc à deux connexions par le proxy applicatif, comme expliqué pour la passerelle de niveau circuit.

Passerelle de niveau applicatif :

Ces pare-feu autorisent une authentification des utilisateurs beaucoup plus grande qu'avec les adresses IP.

Ils cachent le réseau interne de l'entreprise et offrent des informations de journalisation d'événements très détaillées.

Passerelle de niveau applicatif :



3. La sécurité périmétrique

Sécurité périmétrique ou zone démilitarisée :

Les systèmes pare-feu permettent de définir des règles d'accès entre deux réseaux.

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 permettant d'isoler les différents réseaux de l'entreprise.

On parle de « **cloisonnement des réseaux** » ou **isolation**

Sécurité périmétrique ou zone démilitarisée :

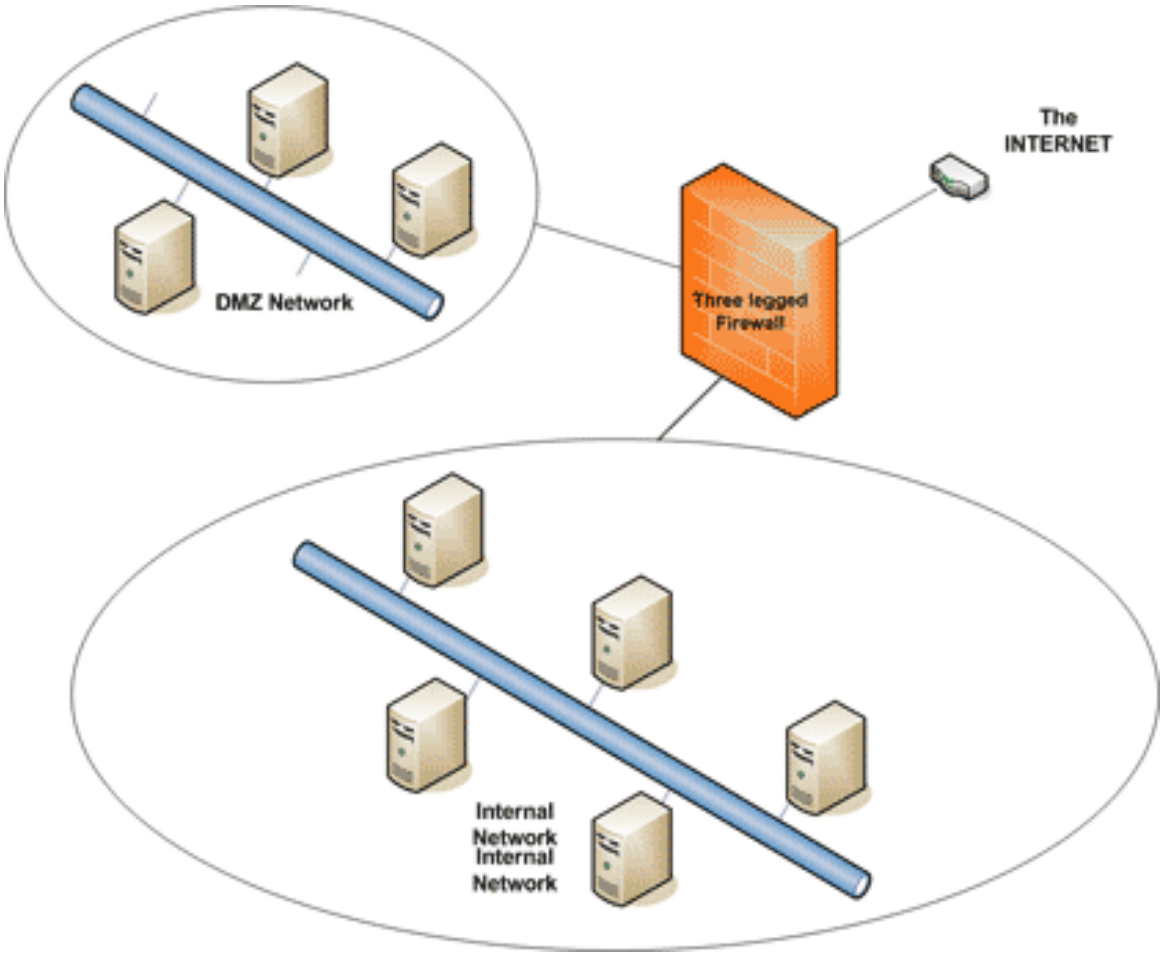
Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (Web, Messagerie, FTP, ...), il est nécessaire de créer une **nouvelle** interface vers un réseau à part.

Ce réseau sera 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 démilitarisée** » ou **DMZ** pour DeMilitarized Zone.

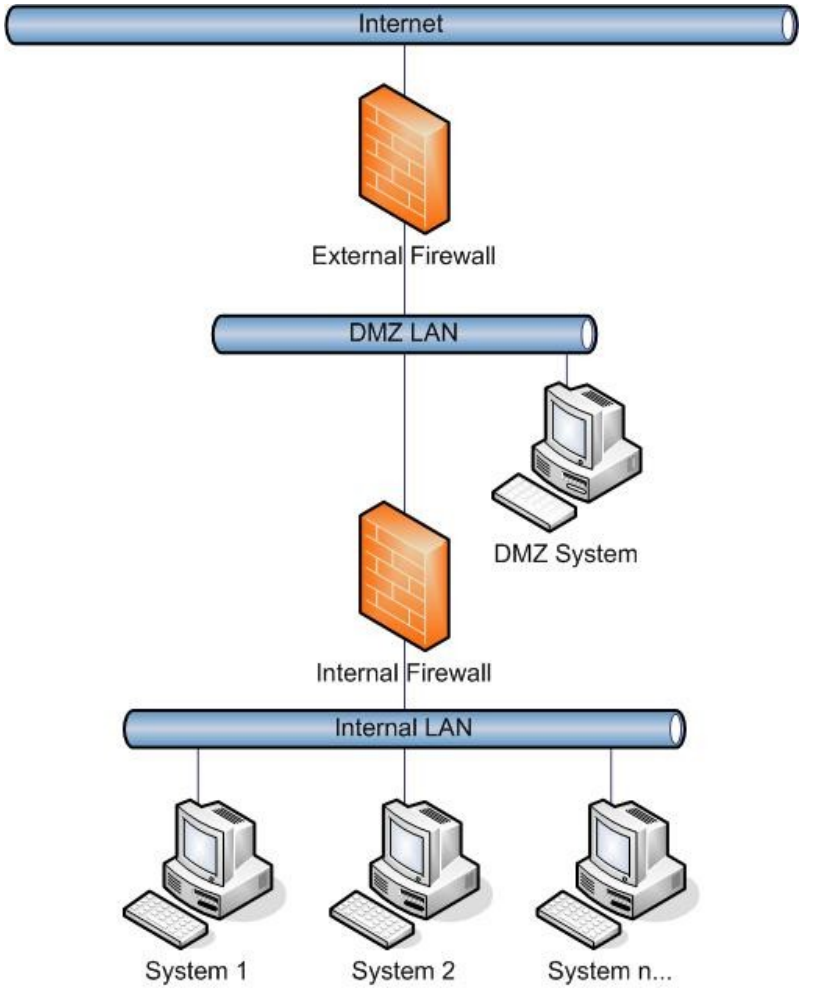
Sécurité périmétrique ou zone démilitarisée :

Cette zone isolée peut héberger des applications mises à disposition du public.



Sécurité périmétrique ou zone démilitarisée :

La DMZ peut aussi faire office de « zone tampon » entre le réseau à protéger et le réseau hostile.



4. Les antiX

L'appellation antiX regroupe tous les logiciels dont le rôle est de filtrer les « malwares » ou d'éviter la baisse de productivité.

On regroupe sous cette appellation :
- Antivirus ;
- Anti-spam ;
- Filtrage d'URL.

L'antivirus :

Les antivirus sont conçus pour identifier, neutraliser et éliminer les logiciels malveillants comme les virus, vers, trojan, …

Les principaux antivirus :

• utilisent des fichiers de signatures pour comparer les objets à vérifier avec des signatures virales ;

• fonctionnent de manière heuristique → ils recherchent des virus en fonction de leurs comportements.

• utilisent l'analyse de forme basée sur des expressions régulières (regexp).

L'antivirus :

Les zones parcourues peuvent changer d'un antivirus à l'autre.

Les plus anciens savent uniquement rechercher des virus sur ordre de l'utilisateur.

La dernière génération d'antivirus sait :

- faire des recherches dites « à l'accès » ;
- scanner la mémoire.

L'antivirus :

Si la majorité des antivirus sont applicatifs, c'est à dire installés sur un système d'exploitation, d'autres fonctionnent en tant que service embarqué.

Cette dernière génération d'antivirus est particulièrement intéressante car elle effectue des scans dits «à la volée».

Ils sont généralement embarqués sur des boîtiers UTM (**U**niversal **T**hreat **M**anagement) et ont l'avantage de scanner le trafic réseau qui passe à travers le boîtier.

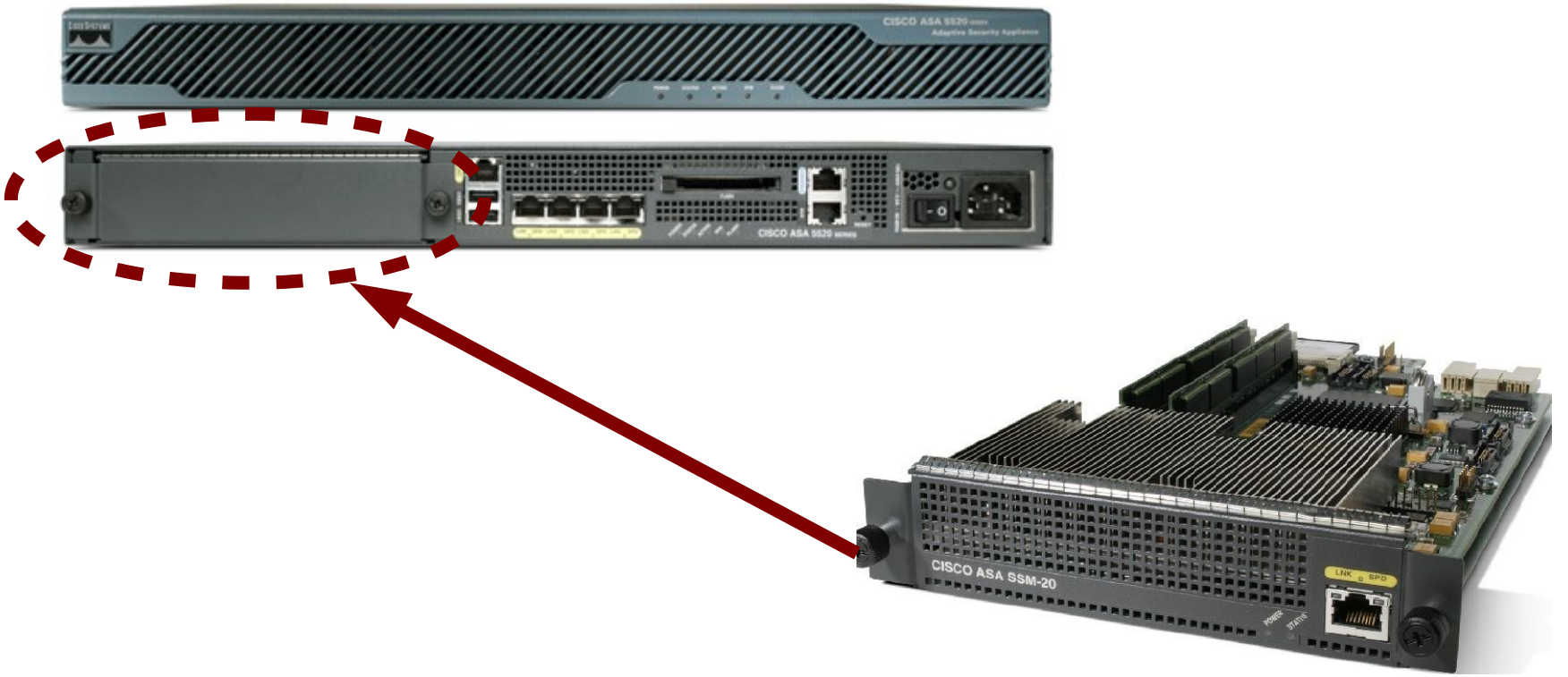
L'antivirus :

De la sorte, ils ne protègent plus un seul ordinateur mais tous les ordinateurs qui sont sur le réseau.

Cependant, il ne permettent pas de protéger des virus ou « malwares » déjà présents sur le réseau par le biais de clés USB, disques durs ou encore CDROM et dégradent les performances du boîtier UTM.

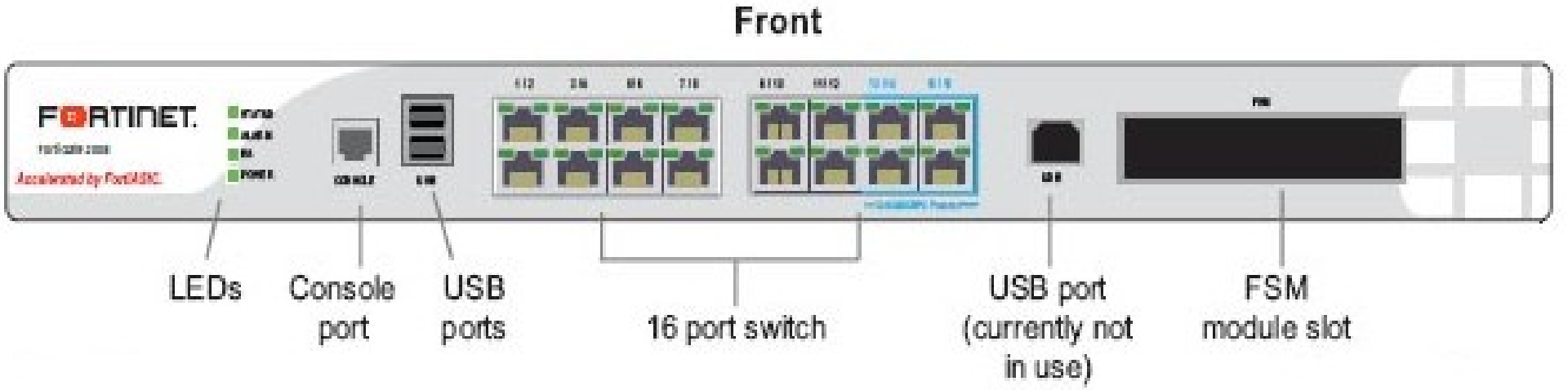
L'antivirus :

Pour faire un tour d'horizon des équipementiers, ***Cisco*** utilise une solution développée par ***Trend Micro*** dans son ***ASA*** (avec la carte ***CSC-SSM***).



L'antivirus :

Fortinet utilise une solution propriétaire qu'il réutilise dans son client VPN.



L'antivirus :

Juniper utilise une solution développée par ***Kaspersky***.

L'anti-spam :

Aujourd'hui, plus de 75% du courrier représente des spams, c'est à dire de la publicité non sollicitée.

Ce fléau, responsable d'une sérieuse baisse de la productivité dans les entreprises, représente une activité florissante où il est possible de gagner beaucoup d'argent en peu de temps.

L'objectif de l'anti-spam va être de faire le tri dans la multitude de messages reçus pour trier les non désirés des légitimes.

L'anti-spam :

Pour rechercher des spams il existe plusieurs filtrages :

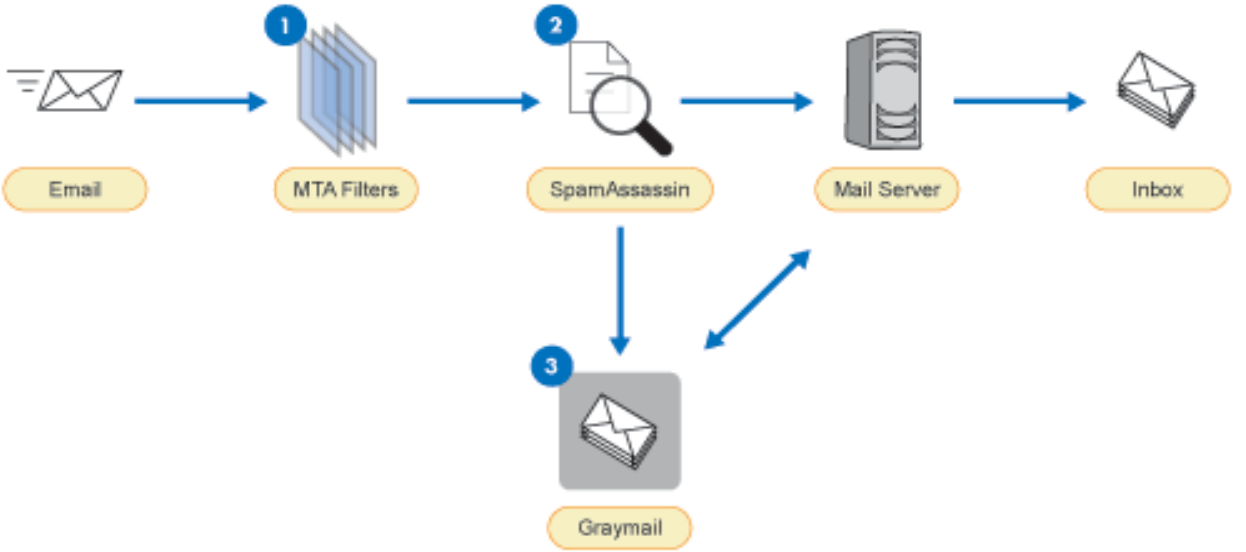
- d'enveloppe ;
- de contenu ;
- par mot clé ;
- d'adresses ;
- d'expressions rationnelles.

La méthode la plus efficace reste le filtrage heuristique qui filtre en fonction de comptage établi grâce aux mots présents dans le corps du message.

L'anti-spam :

L'anti-spam peut être installé directement sur le serveur de mails ou utilisé sur un boîtier ***UTM***.

Il existe des solutions logicielles gratuites comme ***SpamAssassin*** ou des solutions payantes comme celle de Microsoft pour son serveur de mail ***Exchange***.



L'anti-spam :

La solution embarquée sur les UTM est certainement la plus simple à déployer.

Il suffit d'activer le filtrage de contenu et de spécifier une **règle de filtrage** à destination du serveur de mails où l'on activera un **profil de contenu** utilisant l'anti-spam.

Ces profils peuvent contenir des listes blanches, spécifiant les domaines autorisés, ou noires, spécifiant les spammeurs.

Le filtrage d'URL :

L'objectif du filtrage d'URL est d'empêcher le surf sur des sites Web **non autorisés**.

Cette limitation peut avoir différentes origines comme le contrôle parental, les restrictions d'usage professionnel ou encore la protection des libertés individuelles.

Il existe plusieurs techniques de filtrage comme le filtrage par mots clés, par listes blanches, listes noires ou encore par catégories.

Le filtrage d'URL :

Ce filtrage peut se faire par le biais d'un logiciel installé sur le poste client ou directement sur le boîtier UTM.

L'avantage de le faire directement sur l'UTM est de concentrer toute la politique de filtrage en un seul endroit.

Les modifications et mises à jour s'en retrouvent grandement simplifiées.

Le filtrage d'URL :