Les firewalls comme solution aux problèmes de sécurité

Mme Nadia Nouali-Taboudjemat*
Laboratoire Systèmes Répartis et Réseaux CERIST
Email : nnouali@wissal.dz

1. Introduction :

Internet est un réseau de réseaux à l'échelle mondiale qui utilise le protocole de transmission TCP/IP(Transmission Control Protocol/Internet Protocol). Internet est un réseau vital et en pleine extension et qui est en train de changer la manière avec laquelle les organisations et les individus communiquent et traitent leurs affaires. Cependant, Internet souffre d'importants problèmes de sécurités. Les attaques subies par certaines organisations ont eu un impact important sur leur productivité et leur réputation. En effet, dans certains cas des organisations ont dû se déconnecter temporairement d'Internet et ont dû faire des investissements significatifs dans la réparation des dégats subis par leurs systèmes et la révision de la configuration de leurs réseaux.
Heureusement, des solutions aux problèmes de sécurité existent. Un **système firewall** est l'une des techniques qui peut nettement améliorer le niveau de sécurité d'un site dans sa globalité, en obligeant toutes les connexions à passer à travers une passerelle pour être examinées, évaluées et authentifiées. Ce papier donne une présentation des différents aspects de la technique du firewall.

2. Un apercu sur les problèmes de sécurité :

La sécurité d'un réseau d'ordinateurs est basée sur la réalisation de la **confidentialité**, de l'**intégrité**, et de la **disponibilité** dans un système informatique. La confidentialité nécessite que les informations ne soient accessibles que par les utilisateurs autorisés, l'intégrité nécessite que les informations ne soient pas altérées, et la **disponibilité** nécessite que le système reste à tout moment opérationel et sans aucune dégradation de son fonctionnement.

Un grand nombre de facteurs sont à l'origine des problèmes de sécurité. Le problème fondamental est, peut être, le fait qu'Internet n'a pas été conçu pour être très sécurisé. En effet, au moment de l'implémentation d'Internet, l'accès libre a été favorisé afin de répondre aux besoins de communication et d'échange des chercheurs. Cependant, son succès phénoménal durant les années 80s et 90s et l'introduction de différents types d'utilisateurs a aggravé les problèmes de sécurité. D'autres facteurs favorisant ces problèmes sont :

- la vulnérabilité des services TCP/IP: des services tels que Telnet, FTP, e-mail peuvent être compromis par des attaquants connaisseurs,
- la facilité d'espionnage et de déguisement : le trafic sur Internet n'est généralement pas crypté; les messages, les mots de passe et les transferts de fichiers peuvent être lus par les

* Communication présentée au SICOM'97

intrus qui n'auront alors qu'à réutiliser ces informations pour accèder par effraction aux systèmes,

- l'absence de politique de sécurité : de nombreux sites sont configurés pour assurer une grande ouverture sur Internet, sans tenir compte des problèmes de sécurité, et permettent plus d'accès aux services TCP/IP qu'il n'est nécessaire,
- la compléxité de configuration : les contôles d'accès sont souvent difficiles et complexes à spécifier.

Ainsi tous ces facteurs favorisent les menaces de violation de la sécurité qui peuvent être classées en :

- accès non autorisés aux ressources,
- divulgation d'informations, telles que le contenu du fichier des mots de passe qui conduirait alors à des accès non autorisés,
- dénie de service pouvant rendre un réseau inutilisable pour avoir été innondé de paquets par les attaquants, pour avoir été partitionné car la fonction de routage aurait été inhibée dans le routeur connectant les segments du réseau, ou bien parce qu'un virus aurait alourdi le temps de réponse du réseau en consommant des ressources système.

Toutes ces **menaces** peuvent être **accidentelles** ou **intentionnelles**. L'émission d'une information confidentielle à un mauvais destinataire et la modification d'informations conduisent à la violation de la confidentialité et de l'intégrité des informations font partie des menaces accidentelles. Une attaque est une menace intentionnelle exécutée dans le but de violer la sécurité. Le dénie de service est une attaque contre la disponibilité du système l'empêchant de délivrer un service approprié.

Parmi les menaces les plus connues on peut citer les checaux de Troie qui sont des programmes effectuant des fonctions illicites en donnant l'apparence d'effectuer une fonction ligitime(une bombe logique en est un cas particulier). Les virus et les vers sont des programmes concus pour céer des copies d'eux même dans d'autres programmes et systèmes. Un virus se multiplie en s'introduisant dans d'autres programmes alors que les vers se propagent dans les réseaux de façon autonome. La fonction des virus et des vers peut être la perturbation d'un système ou l'implémentation d'un cheval de Troie ou d'une bombe logique.

3. Pourquoi un firewall ?

Sans l'utilisation d'un firewall, les différents systèmes du sous-réseau s'exposent à des attaques venant de l'extérieur. Dans un environnement, sans firewall, la sécurité du réseau est basée sur la sécurité au niveau des hôtes et tous les hôtes doivent, dans un sens, coopérer pour atteindre un haut niveau uniforme de sécurité. Plus le sous-réseau est grand, moins il est facile de maintenir tous les hôtes au même niveau de sécurité. Lorsque les erreurs et les défaillances en sécurité deviennent courantes, les intrusions n'apparaitteront plus comme le résultat d'attaques complexes, mais à cause de simples erreurs de configuration et de choix de mots de passe inadéquats. Il suffirait alors qu'un des sytèmes hôtes soit compromis pour que tout le site devienne vulnérables.

4. Les composants d'un firewall :

Les composants d'un système firewall sont principalement :

- une politique de sécurité du réseau (network policy),
- des mécanismes d'authentification avancée(advanced authentication mechanisms),
- le filtrage de paquets(packets filtering), et
- des passerelles application(application gateway).

4.1. Politique de sécurité du réseau :

Le but d'une politique de sécurité du réseau est de définir les prévisions de l'organisation en termes d'utilisation de ses propres systèmes et réseau ainsi que les procédures de prévention et d'intervention aux incidents de sécurité.

La politique de sécurité est définie en deux niveaux qui influent directement sur la conception et l'utilisation d'un système firewall.

- **La politique d'accès aux services :** il s'agit du niveau supérieur qui définit les services dont l'accès sera permis et ceux dont il sera interdit, comment ces services seront utilisés, et les conditions d'exception à cette politique. La politique définie doit être une extension à la politique globale concernant la protection des ressources informationnelles de l'organisation. Elle doit être réaliste dans la mesure où elle assurera une protection du réseau contre les risques connus d'attaques tout en préservant les intetrêts de ses utilisateurs en matière d'accès aux services réseau, quand cela est nécessaire, moyennant des techniques d'authentification.

- La potitique de conception du firewall : il s'agit du niveau le plus bas indiquant comment le firewall pourra mettre en oeuvre les restrictions d'accès et le filtrage des services tels que définis par la politique de sécurité. La conception d'une telle politique doit être faite en ayant connaissance des capacités et des limitations d'un firewall ainsi que, des risques et des vulnérabilités associées aux aux services et protocoles TCP/IP. Les firewalls implémentent généralement une des deux politiques de conception de base suivantes :

1. Ce qui n'est pas explicitement permis est interdit.
2. Ce qui n'est pas explicitement interdit est autorisé.

La première politique interdit, par défaut, l'accès à tous les services excépté à ceux qui ont été explicitement identifiés comme étant accessibles. C'est le modèle d'accès classique qui est utilisé dans tous les domaines de sécurité de l'information. La seconde politique autorise, par défaut, tous les accès sauf ceux identifiés par la politique d'accès comme étant non autorisés. Cette solution est moins désirable, car elle offre plus de possibilités pour contourner un firewall(par exemple, accèder à des services nouveaux non encore interdits d'accès).

4.2. Authentification avancée :

Le système d'authentification traditionnel basé sur le mot de passe (password) statique n'est plus suffisant en particulier dans un environnement réseau. Des mesures d'authentification sont concues pour pallier aux faiblesses de ce système. Malgé la diversité des nouvelles techniques d'authentification, leur similitude riside dans le fait que les mots de passe qu'elles génèrent ne peuvent être réutilisés par un attaquant qui aurait espionné la connexion. En effet, le mot de passe n'est généré qu'une seule fois à l'établissement de la connexion entre l'utilisateur et le système et n'est plus valable par la suite.

Au lieu d'implémenter les mécanismes d'authentification au niveau de chaque système hôte du site, il est plus pratique de centraliser ces techniques au niveau d'un firewall qui sera chargé de protéger l'ensemble des systèmes. Ces derniers peuvent alors continuer à implémenter en parallèle la technique classique des mots de passe à leur niveau.

4.3. Filtrage de paquets :

Le filtrage de paquets est réalisé en utilisant des routeurs de filtrage conçus pour filtrer les paquets qui passent par leurs ports en se basant sur les champs suivants, figurant dans l'entête des paquets : l'adressse IP source, l'adresse IP destination, le port source et le port destination. Actuellement, les routeurs ne permettent pas tous le filtrage sur les ports. Cependant, les constructeurs incorporent de plus en plus cette foncionnalité dans leurs produits.

Le filtrage peut être utilisé d'une variété de façons pour bloquer les connexions en provenance ou en partence de systèmes hôtes ou de réseaux spécifiques, et pour bloquer les connexions sur des ports spécifiques. Un site peut bloquer les connexions provenant de certaines adresses, telles que des sites ou des hôtes considérés suspects. L'association du filtrage sur les ports à celui des adresses IP, conduit à une fléxibilité dans l'implémentation des politiques de sécurité. Il sera possible alors pour un site de n'autoriser que les connexions sur un sous-ensemble de ses systèmes hôtes. Pour ces derniers seuls quelques services tels que Telnet, FTP ou e-mail seront accessibles.

Les problèmes de filtrage :

Les routeurs de filtrage de paquets présentent des inconvénients qui peuvent être résumées en ce qui suit :

- La compléxité de spécification des règles de filtrage dont la vérification se fait, en général, manuellement. Souvent, les exceptions aux règles d'accès rendent encore plus complexe leur gestion. Par exemple, il est relativement simple de spécifier une règle qui bloque l'accès au port 23 associé au serveur Telnet que de spécifier une règle pour chaque système auquel les appels Telnet sont autorisés.
- L'authentification sur les adresses IP identifie le sytème hôte mais pas l'utilisateur réel; d'où la nécessité de mécanismes d'authentification.

- Il n'est pas toujours possible de connaite à priori les ports associés aux serveurs, dans ce cas un filtrage basé sur les adresses source/destination et sur les ports source/destination n'est souvent pas suffisant pour assurer un niveau de sécurité élevé.
- Les routeurs de filtrage de paquets ayant plus de deux interfaces réseaux, n'ont pas toujours l'aptitude de filtrer les paquets suivant l'interface à laquelle ils arrivent ou à partir de laquelle ils partent.

- De manière général, il est plus difficile d'implémenter une politique rigoureuse, n'autorisant que les accès explicitement spécifiés, lorsque l'on ne dispose pas d'un routeur offrant la possibilité de filtrage sur les ports et les interfaces d'entrée et de sortie.

4.4. Les passerelles application (Application gateway ou Bastion host) :

Pour parer à certains problèmes ne pouvant être traités au niveau des routeurs de filtrage, les firewalls utilisent des programmes applications pour filter les connexion à des services tels que Telnet et FTP. Une application de ce type est appelée "*proxy service*" et la machine hôte exécutant le proxy service est appelé "a*pplication gateway*" ou passerelle application. La passerelle bloque tous les accès sauf ceux pour lesquels des "proxy services" existent. Ces derniers jouent le rôle d'intermédiaires entre les demande de connexion emises par les clients et les serveurs destinataires.

L'utilisation simultanée d'un routeur de filtrage et d'une passerelle permet d'obtenir un niveau de sécurité et de fléxibilité, dans l'implémentation de la politique d'accès, plus élevé que dans le cas de l'utilisation de l'un des deux mécanismes séparément. Soit par exemple, un site bloquant toutes les demandes de connexion à Telnet et FTP en utilisant un routeur de filtrage de paquets. Ce dernier autorise les paquets Telnet et FTP à se diriger sur un seul hôte, la passerelle Telnet/FTP. Un utilisateur désirant se connecter à un site devra d'abord se connecter à la passerelle et ensuite aux hôtes destinataires.

Des proxy services peuvent être spécifiés pour tous les services réseaux Telnet, FTP, email, http, gopher, X Windows, etc.

Les avantages et les inconvénients des passerelles :

Les passerelle application présentent les avantages suivants :

- Confidentialité de l'information dans la mesure où les noms des hôtes internes au réseau ne sont pas nécessairement connus vers l'extérieur, puisqu'il est possible que seul le nom de la passerelle soit rendu public.

- Authentification et logging plus robustes, dans la mesure où le trafic peut être préauthentifié avant d'atteindre les machines hôtes internes.

- Le coût intéressant, car les équipement et les logiciels nécessaires à l'authentification et au contôle des accès sont localisés seulement au niveau de la passerelle.

- Des règles de filtrage moins complexes, le routeur sera chargé seulement d'autoriser le trafic vers la passerelle et de rejeter le reste. C'est la passerelle qui se chargera du reste du filtrage grâce à des "proxy services".

L' inconvénient des passerelles application est la nécessité pour un utilisateur de se connecter en deux étapes au lieu d'une; car il doit transiter par la passerelle avant d'atteindre la machine hôte désirée. Ceci nécessite parfois la modification du client associé au service demandé. Cette modification peut être vu comme un avantage si elle permet de rendre le firewall transparent à l'utilisateur.

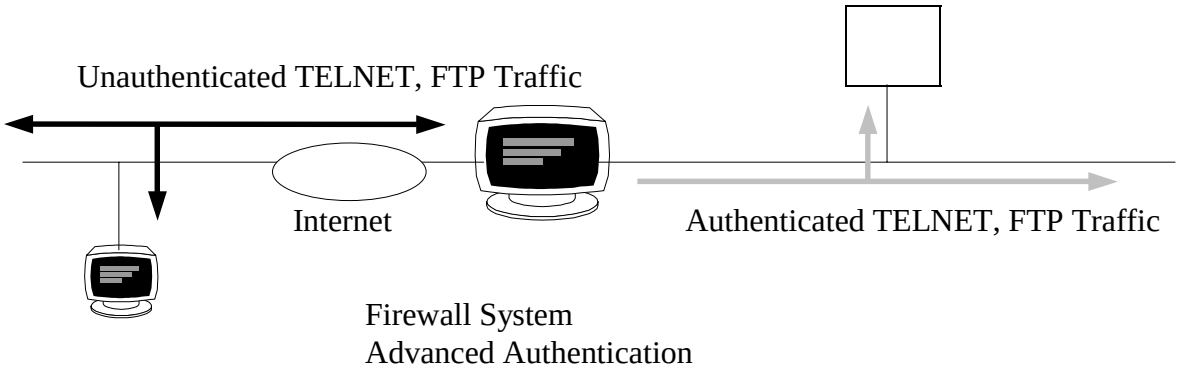

Figure 1 : Préauthentification des trafic Telnet et FTP

5. Les avantages d'un firewall :

Les avantages d'un firewall peuvent être résumés dans les points suivants :

- La protection contre des services vulnérables : on peut par exemple définir que seules les connexions extérieurs vers les services Web et FTP seront accepté sur un système hôte donné.

- Le contôle d'accès aux systèmes : Le firewall fournit l'habilité à contrôler les accès aux systèmes du site protégé. Par exemple, on peut rendre accessibles certains des systèmes hôtes à partir de réseaux externes, tout en bloquant les accès vers les autres.

- La concentration de la sécurité au niveau d'un seul point : Le firewall est un outil qui permet de gérer en un seul point les accès vers ou en provenance du réseau local.

- Les statistiques sur l'utilisation du réseau : Si tous les accès passent par le firewall, ce dernier pourra fournir des statistiques sur l'utilisation du réseau. Si de plus, le firewall, possède des alarmes appropriées, il signalera une activité suspecte en donnant des informations sur l'attaque éventuelle.

6. Les problèmes et les limites des firewalls :

Malgré les avantages cités ci-dessus, un firewall présente un certain nombre de désavantages qui sont cités dans ce paragraphe.

- Un potentiel pour l'exploitation des backdoors(portes dérobées) : les firewalls ne protègent pas contre les problèmes des backdoors. Par exemple, si un accès par modem non restrectif est autorisé à un site protégé par un firewall, les attaquants pourraient contourner ce dernier.

- Une protection peu efficace contre les fuites d'information : il ne peut empêcher, par exemple, un utilisateur interne de copier des données sur une bande et de l'emporter vers l'extérieur du site.

- Les firewalls ne protègent pas contre le chargement de programmes infectés de virus à partir d'Internet : il existe une multitude de méthodes de codage de fichiers binaires pour le transfert, et une variété d'architectures et de virus pour tenter de les détecter tous par le firewall.

- Un système firewall est faillible comme tout autre systéme : il faut veiller à ce qu'il soit sécurisé au maximum.

Malgé ces désavantages, NIST(National Intitut for Security Techniques, de U.S. Department of Commerce) recomande la protection des sites par des firewalls et d'autres outils et techiques qui s'y rapportent.

7. Différentes configurations de firewalls :

Dans ce qui suit est présenté un échantillon de configurations possibles de firewalls possibles :

- packets filtering firewall,
- dual-homed gateway firewall,
- screened host firewall,
- sceened subnet firewall.

7.1. Packets filtering firewalls :

Le firewall de filtrage de packets est peut être le plus commun et le plus facile à employer pour des sites petits et non complexes. Cependant, il est le moins efficace parmis les firewalls cités dans ce paragraphe.

Le routeur de filtrage de paquets est installé au niveau de la passerelle de connexion avec Internet ou tout autre sous-réseau, et les règles de filtrage de paquets y sont configurées. Les systèmes hôtes du site protégé ont accès direct à Internet alors que tous ou la plupart des accès émanant d'Internet vers les sytèmes du site sont bloqués. Cependant, le routeur pourrait autoriser les accès selectifs aux systèmes et aux services selon la politique d'accès prédéfinie.
Un "*packet filtering firewall*" présente les inconvénients d'un routeur de filtrage de paquets.

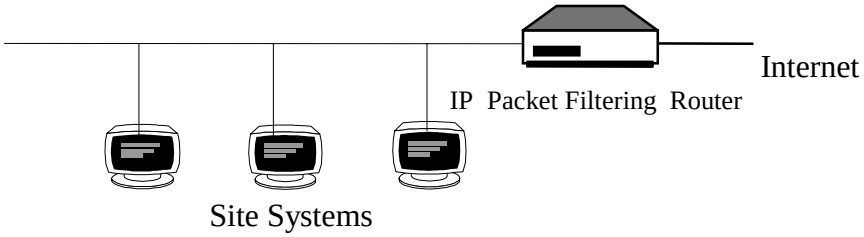

Figure 2 : Packets filtering firewall

7.2. Dual-homed gateway firewall :

Ce type de passerelle (figure 3) est une meilleure solution que la précédente.
Le terme "dual-homed" décrit un hôte qui a deux interfaces, l'une connectée au réseau externe et l'autre au réseau interne. La capacité de routage IP de cette passerelle est inhibée(c'est-à-dire, par défaut le système n'assure pas la fonction de routage entre les deux réseaux). De plus, un routeur de filtrage de paquets peut être placé à la connexion Internet. Ceci permettrait de céer un sous-réseau intérieur (entre la passerelle et le routeur) qui serait utilisé pour la localisation de systèmes spécialisés tels que des serveurs d'information et une réseve de modems.

Les services et les accès sont fournis à travers des "proxy servers" situés sur la passerelle. Ce type de firewall permet d'implémenter la politique n'autorisant l'accès qu'à des services spécifiés explicitement puisque seuls les services pour lesquels des "proxy servers" ont été prévus sont accessibles. La capacité de routage de l'hôte étant inhibée, on est alors sûr que d'autres paquets ne passeront pas vers le sous-réseau protégé. On peut atteindre un haut degré de discrétion(privacy) du moment que les chemins (routes) vers le sous-réseau protègé n'ont a être connu que par le firewall et non par les autres systèmes Internet(car ces derniers ne peuvent pas router les paquets directement aux systèmes protégés).

Une simple configuration de ce type de passerelle serait de fournir des services proxies pour Telnet et FTP, un service e-mails. Comme le firewall utilise un système hôte, il peut héberger des logiciels d'authentification avancés.
Ce type de configuration firewall ainsi que la configuration qui sera présentée Dans le paragraphe suivant offre la possibilité de différencier le trafic concernant un serveur d'information des autres trafic.

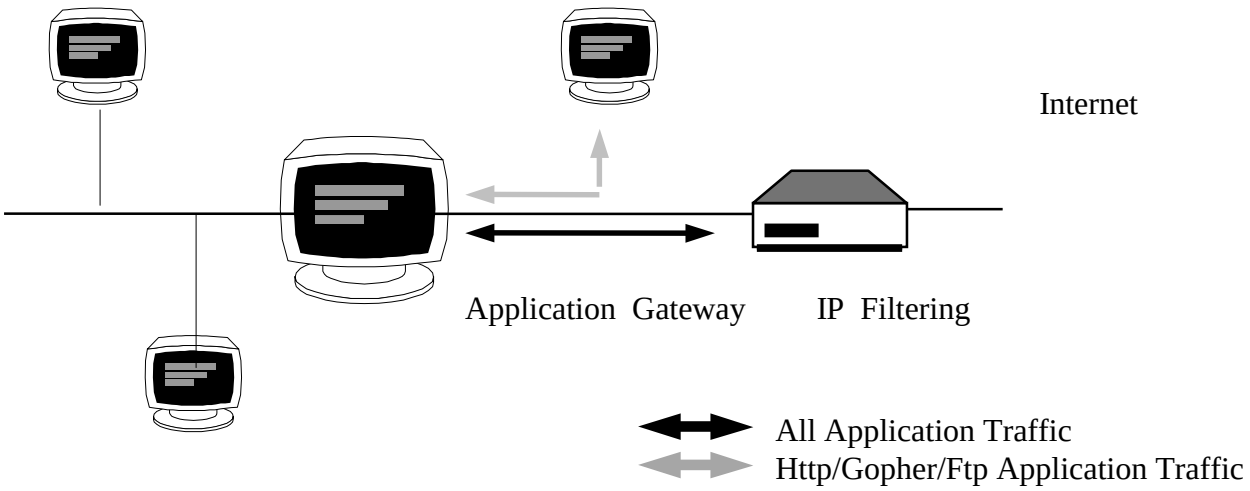

Figure 3 : Dual-homed gateway firewall with router

L'inféxibilité du dual-homed gateway pourrait être un inconvénient car tous les services seront bloqués sauf ceux dont les proxies exitent. Pour cela les sytèmes qui nécessitent l'accès devront être placés entre la passerelle et le routeur.

Il ne faut pas perdre de vue que le système hôte utilisé pour le firewall devra être très sécurisé, car si ce dernier vient à être compromis c'est tous le site qui le sera.

7.3. Screened host firewall :

Cette configuration est plus flexible que la précédente mais au prix d'une sécurité moins rigoureuse. En effet, il s'agit du même principe, mais la différence réside dans le fait que la passerelle nécessite une seule interface réseau et ne nécessite pas de sous-réseau entre le routeur et la passerelle. Ceci permet au routeur de passer certains services sûrs sans passer par la passerelle vers les systèmes internes. Les services considérés sûrs sont ceux pour lesquels des "proxies" n'existent pas mais dont les risques encourus en les utilisant ont été considérés acceptables(par exemple le service DNS). Dans cette configuration, le firewall implémente une combinaison des deux politiques avec des proportions qui dépendent du nombre et des types de services qui sont directement dirigés vers les systèmes du site.

Deux inconvénient peuvent découler de la fléxibilité de ce firewall. Le premier c'est d'avoir à configurer deux systèmes; le routeur et la passerelle. Or les règles de filtrage du routeur peuvent être très complexes et difficiles à tester. Cependant, le routeur n'est amené à filtrer que le trafic se dirigeant vers la passerelle, les règles ne seront pas aussi complexes que dans le cas de l'utilisation d'un "packet filtering firewall" qui doit générer le traffic vers de multiples systèmes). Le deuxième est le même que celui du "packet filtering firewall", c'est-à-dire que des risques de violation de sécurité existent vu qu'un certain trafic est autorisé du routeur vers le site.

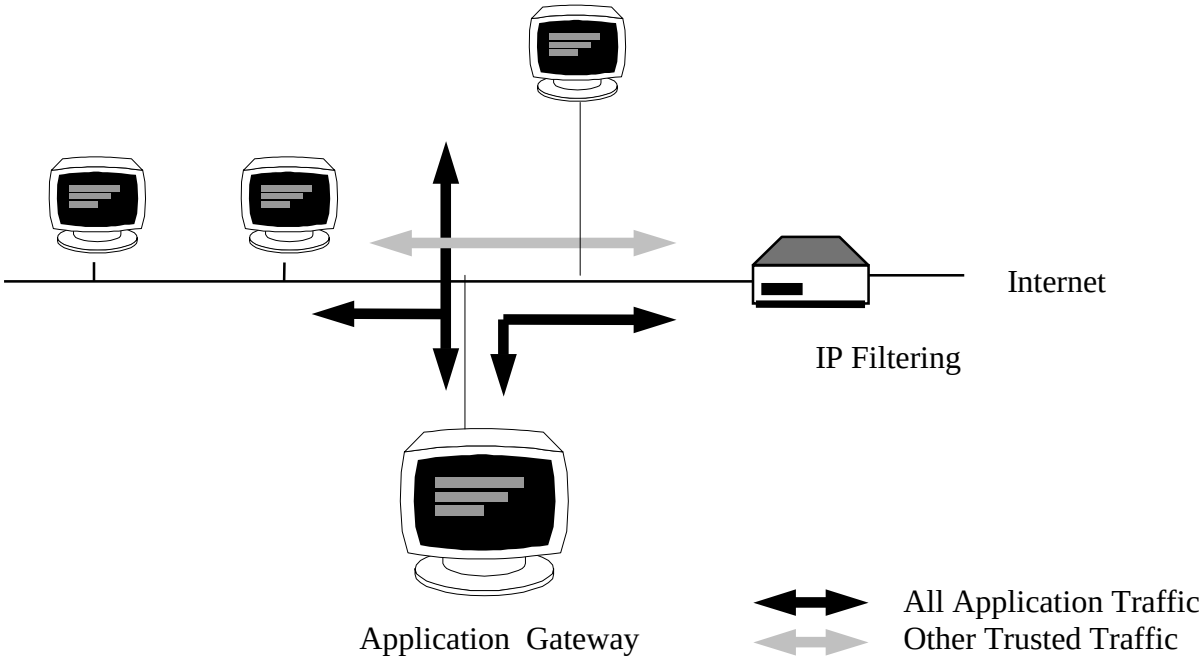

Figure 4 : Screened host firewall

7.4. Screened subnet firewall :

Il s'agit d'une variante du "dual-homed gateway firewall" et du "sceened host firawall" qui a pour objectifs d'avoir les avantages de ces deux solutions. Elle peut donc être utilisée pour localiser chaque composant du firewall sur un système séparé, afin d'atteindre un plus **grand débit** et une **bonne fléxibilité**. Chaque système composant du firewall, implémentera seulement une tâche spécifique, rendant ainsi la configuration moins complexe.

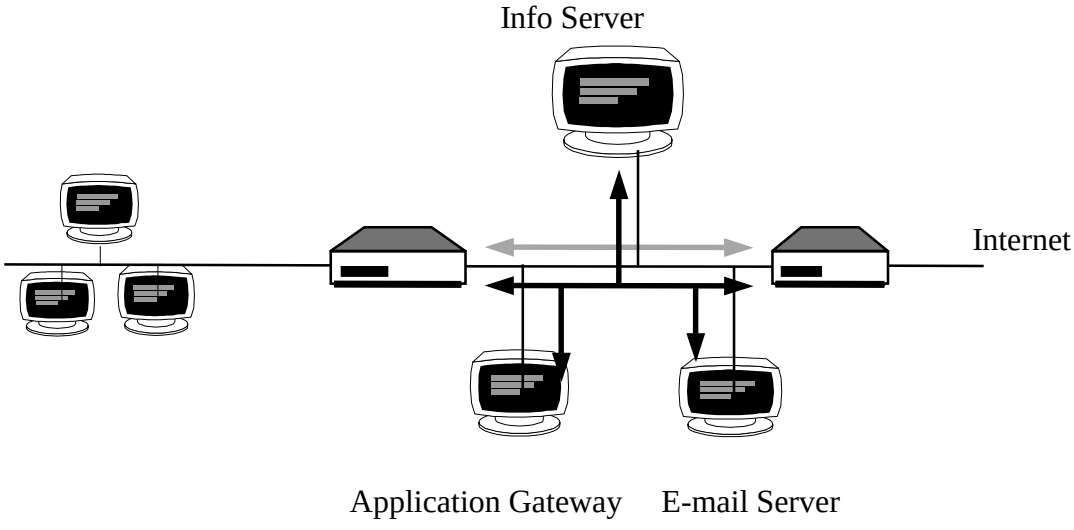

Figure 5 : Screened subnet firewall with additional systems

7.5. Integration de modems aux firewalls :

Certains sites permettent les accès dial-in à des modems situés à différents points du site. Or ces connexions représentent des portes ouvertes aux intrusions. Ces modems doivent être concentrés en une reserve à laquelle les connexions doivent être sécurisées.
Les firewalls du type dual-homed gateway et screened subnet offrent la possibilité d'une telle solution. La réserve de modems consiste en modems connectés à un serveur de terminaux qui sera localisé au niveau du réseau interieur(entre les routeurs et la passerelle) de manière à ce que les accès de ou vers les modems soient contôlés par les routeurs et les passerelles.

Conclusion :

Un firewall est un outil important pour la sécurité des rséseaux interconnectés mais il ne constitue pas la solution à tous les problèmes de sécurité. Sa force réside dans le fait de permettre de la réduction la zone à risques à un seul point qui est le firewall. Un firewall ne peut stopper un virus qui aurait été introduit par une diskette infectée, ni empêcher un employé d'appliquer une tension de 240 volts à un cable Ethernet avant de quitter son travail. Un firewall offre les moyens d'implémenter une politique d'accès réseau qui constitue une extension à la politique globale de l'organisation concernant la protection de ses ressources informationnelle. Les problèmes de sécurité informatqiue ne sont pas une fatalité, une approche qualitative des problèmes permet une définition précise des risques puis la mise en oeuvre de procédures, **pas exclusivement techniques**, assurant leur maitrise.

Bibligraphie :

[1] Michael G. Brown
Firewall concepts
Presented to the Tasmanian Unix Special Internet Group of the Australian Computer Society
Hobart, December 1993
http://info.dpac.tas.gov.au/papers/firewalls.html

[2] Y. Deswarte
Construction des systèmes d'exploitation répartis.
Chapitre 9: Tolérence aux fautes, sécurité et protection.
Collection didactique, INRIA, 1991.

[3] Marcus J. Ranum, Frederic M. Avolio
Trusted information systems, Inc.
ftp.tis.com: /pub/firewall/toolkit/

[4] John P. Wack, Lisa J. Carnahan
Keeping your site comfortably secure : an introduction to Internet firewalls
NIST special publication 800-10
US Department of Commerce
National Institute of Standards and Technology.