Filtrage et Firewall

Présentation

Sources de risques

L'ouverture des réseaux locaux sur internet, au départ source de meilleure communication, est devenue une porte ouverte aux dangers nombreux d'un système ouvert à tous :

- entrée de virus
- utilisation/monopolisation de la connexion pour du trafic non professionnel
- intrusion dans le SI de l'entreprise
- fuite de données
- *phishing*, *keylogging*, etc : techniques visant à intercepter des données confidentielles (comptes bancaires, identifiants de connexion, etc).
- **déni de service** (DoS, DDoS) : attaque par saturation empêchant un service de fonctionner normalement. Il peut être lancé depuis de multiples machines zombie (déni distribué)
- chevaux de Troie : permettent de lancer des attaques depuis un réseau infecté, de s'introduire dans un réseau pour y récupérer de l'information

Parades

Pour se protéger de ces dangers, on aura recours à un **antivirus** en réseau, des *spywares* et autres outils de protection sur les machines, mais surtout, d'une sécurité dès le point de passage entre le réseau local et le réseau extérieur.

On appelle **Firewall**, mur **pare-feu** ou **filtre** la fonction responsable de **limiter les informations et actions réseau autorisées** depuis ou vers l'extérieur.

> Bien que souvent assimilés, le **firewall** est différent du **proxy** Ce dernier sert de **mandataire** : il agit pour les postes en son propre nom, masquant les adresses des postes vers l'extérieur

.

Filtrage

Le filtrage consiste à déterminer les machines autorisées à communiquer (adresses IP, adresses réseau, plages d'adresse, etc), les services que l'on peut laisser actifs, ce que l'on veut autoriser à entrer ou sortir. Le filtrage est la technique mise en place sous l'appellation Firewall ou Pare-feu.

A Règles et filtrage

Il faut bien distinguer :

1. l'étape de constitution des règles, qui définit a priori les éléments (IP, ports, mots clés, URL, etc) interdits ou autorisés
2. le moment du filtrage qui s'applique à étudier les éléments d'une trame circulant du réseau interne vers l'extérieur (ou l'inverse) pour appliquer l'une des règles

Définition des règles

Le principe de la définition d'une règle de filtrage est le suivant :

- chercher les **informations techniques qui peuvent être étudiées** : adresse (ou plage) IP, ports, informations de niveau 7 ou mots clés, etc. Ces informations doivent pouvoir être valorisées dans la règle : on doit être certain des valeurs que l'on veut autoriser ou interdire, si on n'a pas l'information, on laissera le champ vide
- déterminer le **sens de l'échange à filtrer** : les informations d'adressage ou de port sont-elles à préciser pour la source ou pour la destination, par quelle interface du filtre parviendront les trames correspondant à cette règle ⇒ il est parfois nécessaire d'écrire deux règles (une pour l'envoi, une pour la réception) pour garantir l'efficacité d'un filtrage
- éventuellement, préciser l'**état d'un échange** dans le cadre du filtrage : on peut laisser entrer un trafic si la demande à été initiée depuis le réseau local (accès Web ou de messagerie par exemple)
- **ordonnancer les règles**

Une règle se présente sous la forme

N°	Interface	IP Source	IP Destinataire	Port Source	Port Destinataire	Etat[(1)]	Action[(2)]

[(1)] : optionnel : indique si la communication est déjà établie, s'il s'agit d'une demande nouvelle, etc.
[(2)] : autoriser, ignorer ou interdire

Application du filtrage

L'application du filtrage pour une trame parvenant sur un filtre se déroule selon les étapes suivantes :

- on cherche la **première règle pour laquelle les champs connus sont présents** dans la trame
- on **effectue l'action de filtrage** (autorisation, blocage, abandon) correspondante
- **si aucune règle ne correspond**, on applique la **politique par défaut** du filtre (tout autoriser [à éviter] ou tout interdire).

Le filtrage est une démarche fastidieuse pour laquelle des outils pré-configurés ou des listes prêtes à l'emploi sont disponibles. Il peut porter sur tout ou partie des éléments du modèle OSI.

B Filtrage par adresse

Première sécurité réelle, le filtrage IP repose sur les adresses de niveau 3, en en autorisant l'entrée où la sortie.

Il est ainsi possible :

- de limiter les seules adresses IP autorisées en sortie : dans le cadre d'un Extranet, seules les communications entre partenaires sont possibles, permet aussi d'éviter que des attaques soient lancées depuis le réseau de l'entreprise en passant par des sites anonymant
- de **limiter les seules adresses IP autorisées en entrée** : par exemple lorsque le site interne ne doit être autorisé qu'à des télétravailleurs
- de **limiter, pour une machine les adresses IP en sortie** : pour éviter la fuite d'information
- d'**interdire un certain nombre d'adresses en sortie** : si le site interne offre un portail (orientant vers une sélection de sites), on peut interdire les adresses des moteurs de recherche, ou encore de sites reconnus comme distrayants dans un cadre professionnel
- d'**interdire un certain nombre d'adresses en entrée** : pour éviter que des internautes passant par les sites anonymant ne pénètrent le réseau de l'entreprise

Cette partie est très fastidieuse à mettre en place. Il faut en effet travailler sur les adresses IP, ce qui demande de bien maîtriser son réseau interne, mais aussi de connaître les IP de l'extérieur. Un administrateur n'aurait pas le temps d'étudier, par le biais des Ping et des fonctions DNS, une stratégie suffisamment permissive et sécurisée sur son *firewall*. Toutefois, on peut envisager une mise en place progressive, partant d'une restriction maximale et s'ouvrant au fur et à mesure ou, à l'inverse, initialement très ouverte et se fermant progressivement. Il sera donc plus facile de travailler directement sur les fonctions réseau de la couche application.

C Le filtrage par port

Cette sécurisation monte au niveau 4. Le protocole TCP (ainsi que son équivalent sans contrôle UDP) associe à chaque service de la couche Application un port d'écoute standardisé (FTP –> 21, HTTP –> 80,...). Il va alors être possible d'autoriser ou d'interdire, pour le réseau ou par machine l'utilisation de ces fonctionnalités. Les Firewall autorisent ce filtrage, ainsi que les options avancées de configuration des cartes réseau sous 2000/XP/2003/Vista/2008 (sécurité).

On pourra :

- limiter les services autorisés en entrée : si le serveur assure la fonction FTP et Web, on pourra n'autoriser que ces fonctions, en interdisant par exemple le Telnet ou le mail
- limiter les services autorisés en sortie : si l'on ne souhaite pas que les employés passent leur temps à naviguer sur le net, mais qu'ils puissent utiliser la messagerie, par exemple
- interdire des services en entrée ou sortie : à l'opposé des restrictions ci-dessus, on autorise tout, mais on interdit des fonctions que l'on considère inutiles

On trouvera, sous Windows, la liste des ports standards dans le fichier services présent dans *winnt\system32\drivers* et dans ce même fichier quelque part sous Linux.

D Le filtrage utilisateur

Il s'agit d'effectuer les restrictions vues ci-avant, non plus à partir des adresses mais directement à partir de l'identification de l'utilisateur (soit définie auprès du Firewall, soit auprès du système d'annuaire de l'entreprise). On pourra limiter les plages horaires d'accès aux différents services.

E Le filtrage par mots-clé

Cette dernière restriction est sans doute la plus simple d'utilisation, mais pas forcément la plus sécurisée. Il s'agit d'autoriser la circulation des messages contenant tel mot, ou au contraire de les interdire :

- Dans un bureau de recherche et développement, tous les mots spécifiques au domaine de l'entreprise pourront ainsi être contenus dans les murs de la société, pour éviter toute fuite par le réseau.
- Dans une autre entreprise, on interdira les recherches sur le sexe, le racisme, les jeux, la télévision, la météo, les voyages...

Alors que cette technique semble simple, on se rend rapidement compte que faire la liste exhaustive de tous les mots que l'on souhaite interdire devient un travail titanesque, d'autant que les effets peuvent être inattendus lorsque le vocabulaire utilisé peut entraîner des contre-sens. Des listes publiques permettent de disposer de sites autorisés (listes blanches) ou interdits (listes noires).

La mise en place d'un firewall vise à filtrer le trafic entrant et sortant d'un réseau, et de mettre éventuellement en place une zone intermédiaire (DMZ) accessible de l'extérieur et du réseau interne.

Firewall et DMZ

Il est possible d'ouvrir un espace intermédiaire entre l'interne et l'externe, en assurant un filtrage sur chacun des accès possible.

Ce sas de communication offre ainsi des services en direction de l'extérieur (Serveurs Web, accès des employés mobiles et distants, extranet...) et laisse aux utilisateurs du réseau local une possibilité d'accès à la fois aux informations de cet espace (pour l'extranet, pour l'échange avec les clients mobiles...) et à internet.

On parle d'une **DeMilitarized Zone (DMZ)** ou **zone démilitarisée**. Il existe différentes mises en œuvre pour réaliser une DMZ, basée sur un unique filtre, ou créant une véritable zone contenue entre deux filtres

Démarche de défintiion des règles

1. Inventorier les éléments suivants :
    - serveurs à mettre en communication
    - échanges à autoriser vers ces serveurs : sens (par où cela arrive sur le filtre) de l'échange, source (quelles machines/adresses), service destinataire (port ou protocole)

    - interdictions spécifiques (sens, source, service)
2. Renseigner les règles une à une
3. Ordonner les règles de manière à éviter les failles : par exemple, une interdiction spécifique après une autorisation globale ne sera jamais étudiée.
4. Tester les autorisations/restrictions en positionnant des équipements correctement paramétrés (IP, Passerelle, DNS, etc) et en lançant les échanges correspondants

Table de filtrage

Les règles de filtrage d'un filtre peuvent être documentées, pour chaque interface du filtre, dans un tableau de la forme suivante (d'autres formes existent) :

Interface d'arrivée sur le filtre				
N°	**IP Source***	**IP Destination[(1)]**	**Port Serveur[(2)]**	**Action[(3)]**

[(1)] : on indiquera une adresse exacte, une plage d'adresses ou l'adresse d'un réseau
[(2)] : Numéro de port ou nom du protocole
[(3)] : Autoriser / Interdire

Le paramétrage dans le filtre devra s'adapter aux contraintes de l'interface ou de la syntaxe proposée par l'outil. Notamment, on peut trouver en plus :

- le sens de la communication (LAN → DMZ ou WAN → LAN, Incoming ou Forward, ...)
- le port source.

Interface du ZYXELL / ZYWALL

Chaque matériel possède sa propre interface pour gérer le filtrage. Le firewall Zyxell fonctionne ainsi :

- les règles sont appliquées d'une interface à l'autre (sens de circulation du trafic) :
    - Lan To DMZ : prend en compte le trafic venant du LAN et à destination d 'une machine ou du réseau sur la DMZ
    - WAN To LAN : prend en compte le trafic extérieur à destination du réseau local
    - LAN To LAN : trafic venant du LAN à destination de l'interface LAN du Zywall (par exemple, si on souhaite l'administrer par son interface Web)
- il y a autant de « paquets de règles » que de sens possibles, et une règle par défaut pour chaque sens de circulation
- les règles sont étudiées sur l'interface qui reçoit le trafic selon la procédure (première qui s'applique ou règle par défaut)

Les ports par défaut sont enregistrés dans des services connus par le nom du protocole (le port 80 correspond au service HTTP). On peut créer des « services » supplémentaires pour des ports non standards : par exemple, on créera un service MySQL correspondant au port 3306 utilisé par défaut par MySQL. On pourra ensuite définir dans les règles de trafic des autorisations ou interdictions pour ce service.