ADMINISTRATION DES SYSTÈMES ET RÉSEAUX

PARE-FEUX ET ZONES DÉMILITARISÉES

Auteur: Bernard GIACOMONI

Autoentreprise GIACOMONI Bernard

Version	Date	Objet
1.0	23/11/2019	Version initiale

Table des matières

I.LES DISPOSITIFS PARE-FEUX:

I.1.DÉFINITION:

Un pare-feu (ou FIREWALL) est un élément du réseau informatique qui a pour fonction de sécuriser un réseau local en définissant les communications autorisés ou interdites entre ce réseau et son environnement. Le mot s'applique à un LOGICIEL supportant ces fonctionnalités ou à une MACHINE hébergeant ce type de logiciel.

Un pare-feu permet d'interconnecter plusieurs réseaux nécessitant des niveaux de sécurité différents (par exemple : internet et le réseau interne d'une entreprise). Le logiciel pare-feu contrôle les flux de données qui le traversent. Il permet ainsi de les analyser afin de les autoriser ou de les rejeter selon des règles de sécurité définies par personnes chargées de l'administrer. Il agit donc comme un FILTRE vis a vis des messages échangés par les réseaux qu'il contrôle.

I.2.RÈGLES DE FILTRAGES DES ACCÈS*:*

Les critères de filtrage peuvent être basés sur:

- L'origine ou la destination des paquets (règles de filtrage s'appuyant leurs adresses IP ou sur les numéros de ports TCP/UDP d'origine ou de destination;
- Les protocoles de transmission utilisés;
- La continuité des paquets échangés dans une connexion TCP;
- Les données elles-mêmes;
- Les utilisateurs.

I.3.TYPES DE PARE FEUX:

Il existe différents types de pare-feu en fonction de la nature de l'analyse et des traitement effectués :

I.3.1.LES PARE-FEUX SANS ÉTAT (OU STATELESS PACKET FIREWALL):

Ce type de pare-feu inspecte chaque paquet indépendamment des autres et vérifie qu'il satisfait à une série de règles de filtrages définies dans une liste de règles appelée Access Control Lists (ACL). Ces règles concernent les points suivants:

- Les adresses IP Source et Destination du paquet;
- Les numéro de port de la source et du destinataire du paquet;
- L'identificateur du protocole de communication.

Si le paquet ne satisfait pas à l'ensemble des règles spécifiées dans l'ACL, il est rejeté par le pare-feu.

EXEMPLE: une règle peut spécifier des conditions d'accès aux paquets en provenance de telle adresse IP, de telle plage de numéros de ports ou de tel protocole de communication (TCP, IP, ICMP, etc.).

LIMITES: Au fur et à mesure de l'évolution du réseau (augmentation du nombre des utilisateurs, évolution des besoins, etc.), l'administration d'un pare-feu sans états exige d'autoriser progressivement un nombre croissant d'accès, sans qu'il soit toujours possible d'en supprimer. Cette complexité grandissant risque de mener à des incohérences dangereuses. Ceci devrait amener progressivement l'abandon de cette technique. Cependant, ce type de pare-feux équipe encore beaucoup de routeurs.

I.3.2.PARE-FEU À ÉTATS (STATEFUL FIREWALL):

Contrairement aux pare-feux sans états qui inspectent chaque paquet individuellement sans tenir compte de l'historique des échanges, les pare-feux à états sont caractérisés par le fait qu'ils contrôlent la continuité des échanges pour détecter d'éventuelles incohérence dans la succession des paquets.

Ceci se traduit par le fait qu'ils vérifient que chaque paquet d'une CONNEXION est bien la suite logique du précédent paquet d'un même échange ou la réponse à un paquet expédié par le destinataire (ceci concerne évidemment les échanges en mode connecté, comme TCP).

Pour ce faire, les pare-feu à états:

- Maintiennent un tableau des CONNEXIONS OUVERTES;
- Associent les nouvelles demandes de connexion avec des connexions autorisées existantes.

Il en résulte que si une connexion est autorisée, tous les paquets constitutifs de l'échange effectué sous cette connexion seront implicitement acceptés.

Ce type de pare-feu peut donc décider du filtrage de chaque paquet en fonction des informations accumulées lors des connexions précédentes, et non plus seulement sur des règles définies par l'administrateur. Cependant, ce type de pare-feu se limite à garder un suivi du trafic et à rechercher des correspondances dans le cas de nouvelles connexions: dès que l'accès à un service a été autorisé, il n'effectue plus aucun contrôle sur les échanges effectués dans le cadre de ce service.

I.3.3.PARE-FEU APPLICATIF (PROXYING APPLICATIF):

Le pare feux applicatif agit au niveau des couches applicatives de l'ISO, c'est à dire qu'il applique des filtres en fonction des APPLICATIONS communicantes. Chaque requête est traitée par un processus dédiés au type d'application qui correspond à cette requête (par exemple une requête HTTP sera filtrée par un processus dédié à HTTP). Le pare-feu rejettera toute requête non conformes aux spécifications du protocole.

Le pare-feu applicatif joue un rôle d'intermédiaire entre le client et le serveur :

- il invoque le service à la place de l'utilisateur;
- Il valide les contenus;
- Il masque pour le serveur certaines informations du client (par exemple, il remplace dans les paquets l'adresse du client par sa propre adresse.

Un pare-feu applicatif se comporte donc, pour certains de ses aspects comme un PROXY. C'est ce qui explique que les différents processus de filtrages soient appelés PROXY HTTP, PROXY FTP, etc.

I.3.4.PARE-FEU IDENTIFIANT:

Un pare-feu identifiant réalise l'identification des connexions. Les règles de filtrage peuvent donc tenir compte de l'utilisateur déclaré.

I.3.5.PARE FEU PERSONNEL:

Dans le cas où la zone à protéger se limite à une seule machine, un logiciel pare-feu peut être installé sur cette machine. On l'appelle dans ce cas PARE-FEU PERSONNEL (PERSONNAL FIREWALL). Un tel pare-feux installé sur un poste de travail permet de contrôler l'accès au réseau des applications installées sur ce seul poste de travail, c'est à dire de repérer et d'empêcher l'ouverture de connexions par des applications non autorisées par l'administrateur.

I.4.L'INSPECTION PROFONDE DES PAQUETS:

L'inspection profonde des paquets (Deep Packet Inspection – D.P.I) est une technique qui s'intéresse au CONTENU des données transmises et non plus seulement aux données de transmission (adresse IP, numéro de port, identifiant de protocole, etc.). Certains pare-feu équipés de ces techniques peuvent ainsi repérer dans ces données des mots ou des configurations de caractères caractéristiques d'activités délictueuses.

I.5.LE PARAMÉTRAGE DES PARE-FEUX :

I.5.1.INTRODUCTION :

Le paramétrage d'un pare-feu revient à définir un certain nombre de règles. Chacune de ces règles peut concerner :

- Soit les PAQUETS possédant en commun certaines caractéristiques (n° de protocole, adresse IP et port d'émission, adresse IP et port destinataire) ;
- Soit une APPLICATION particulière.

I.5.2.RÈGLES CONCERNANT LES PAQUETS :

Ces règles permettent au pare-feu d'autoriser ou de bloquer le transit de paquets possédant certaines caractéristiques. Chacune de ces règles peut être définie en définissant les paramètres suivants :

PARAMÈTRE	VALEUR À DÉFINIR
Nom :	Nom donné à la règle (chaîne de caractères)
Sens de transit :	Entrant/Sortant/Entrant et sortant
Protocole :	TCP, IP, TCP/IP, ICMP, etc.
Adresse destinataire	Adresse IP du destinataire du paquet (y compris adresses multicast ou broadcast).
Port local :	N° du port émetteur du paquet
Port distant :	N° du port destinataire du paquet
Action :	Choisir une option ; • Autoriser • Bloquer • Décision automatique • Demander l'autorisation au coup par coup.

Dans la plupart des pare-feux "courants", le menu permettant de gérer l'ensemble des règles de paquets est présenté sous la forme d'un tableau dont chaque ligne représente une règle.

EXEMPLE :

nom	sens	protocole	@IP dest	Port local	Port distant	Action
CWeb	Entrant	TCP/IP	192.168.1.23		80	Autoriser
FTP	E/S	TCP/IP		21	21	Bloquer

- La première ligne définit une règle qui interdit l'interrogation du serveur web 192.168.1.23 situé dans l'espace protégé depuis l'espace public ;
- La deuxième ligne définit une règle qui interdit tout transfert FTP sur port 21 entre l'espace public et l'espace protégé.

I.5.3.RÈGLES CONCERNANT LES APPLICATIONS :

Il est également possible de créer des règles concernant les applications. Les menus permettant de définir ce type de règle on la structure suivante:

Définition de l'application	Choix de la règle
Sous-menu de choix d'une application (liste de propositions ou recherche d'une application installée)	Sous-menu de choix de la règle à appliquer (par exemple "ouvrir vers internet").

En fait, la création d'un règle d'application entraîne la création de règles sur les paquets. Par exemple, la création d'une règle de type "ouvrir telle application vers internet" va engendrer la création d'une règle de paquets permettant l'émission vers internet de paquets adressés au port 80 (port générique des serveurs web).

I.5.4.AUTRES TYPES DE RÈGLES :

Selon le type de pare-feu et les fonctionnalites qu'il supporte, d'autres règles peuvent être définies :

I.5.4.1.RÈGLES PAR DÉFAUT :

Le plus souvent, les pare-feux permettent de définir des règles générales applicables par défaut à tous les paquets ou à toutes les applications. Ainsi, on peut définir une règle par défaut bloquant tout trafic pour toutes les applications ou demandant une autorisation "manuelle" pour chaque accès.

L'utilisation de cette possibilité est recommandée pour définir le paramétrage initial d'un pare-feu. On procède ainsi :

- On bloque le trafic pour toutes les applications (ou bien on le soumet à autorisation au coup par cour);
- Puis on définit des règles pour débloquer les trafics nécessaires.

I.5.4.2.RÈGLES PORTANT SUR LES IDENTIFIANTS DE CONNEXION :

Ces règles peuvent être définies pour les pare-feu de type "identifiant" qui permettent de filtrer les paquets en fonction des identifiants d'utilisateurs. Il est ainsi possible de bloquer certains paquets en fonction de l'identifiant de la connexion, donc de l'utilisateur.

I.5.4.3.RÈGLES PORTANT SUR LE CONTENU UTILE DES PAQUETS :

Elles concernent les pare-feux dotés de fonctionnalités d'inspection profonde des paquets". Elles permettent de filtrer des paquets en fonction de configuration de caractères recherchées dans les données utiles transportées (Payload Datas). Il peut s'agir par exemple de mots-clefs caractéristiques de certaines activités.

II.LES ZONES DÉMILITARISÉES:

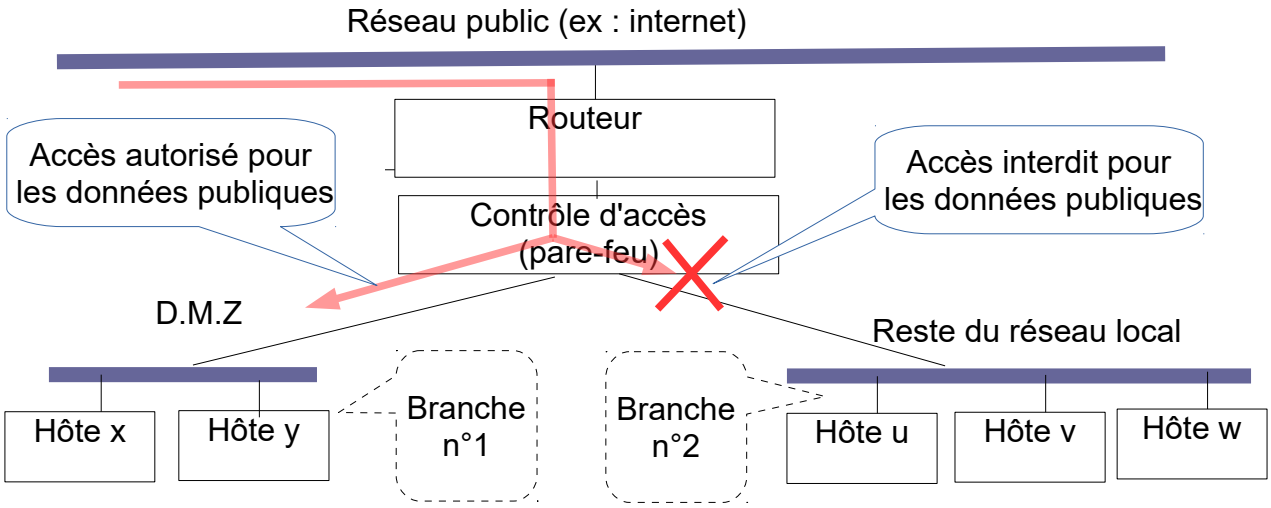
II.1.DÉFINITION:

En informatique de réseau, une ZONE DÉMILITARISÉE (DeMilitarized Zone – DMZ), désigne une partie d'un réseau local dans laquelle les hôtes peuvent accéder aux service du réseau public auquel le réseau local est connecté, par opposition aux zones du réseau local où ces accès sont interdits par les règles d'administration :

EXEMPLE :

Le schéma suivant représente un réseau local relié au réseau public par un routeur. Les différents hôtes ont été séparés en deux branches de réseau :

- La branche N°1 comprend tous les postes qui ont besoin de communiquer avec le réseau public (par exemple : les postes des utilisateurs qui ont besoin d'accéder à des ressources d'internet : sites web, serveurs de fichiers, messagerie électronique, serveurs mis à disposition du public ou d'autres implantations, etc.) ;
- La branche n°2 comprend tous les postes qui n'ont pas besoin d'accéder à internet et que l'on veut protéger d'attaques venues de l'extérieur.



La séparation des flux destinés à chaque branche est réalisée ici par un seul PARE-FEUX.

II.2.FONCTION :

La fonction principale d'une DMZ est donc de séparer les machines du réseau local qui ont besoin de communiquer avec l'extérieur de celles qui n'en ont pas besoin et qu'il importe de protéger contre des attaques de l'extérieur. Le trafic potentiellement dangereux est obligé de transiter par la DMZ. De ce fait, la «compromission» d'un des services hébergés dans la DMZ ne donne accès qu'aux machine de la D.M.Z et non au réseau local.

En termes de sécurité, la DMZ joue le rôle de « zone tampon » entre un réseau que l'on désire protéger et un réseau potentiellement hostile, afin que:

- Les ressources sensibles du lAN ne soient jamais exposés directement à Internet ;
- Les agents extérieurs au réseau local n'aient jamais directement accès à des ressources du LAN.

REMARQUE: Il est également possible de mettre en place des DMZ en interne dans un LAN afin de cloisonner le réseau interne selon différents niveaux de protection.

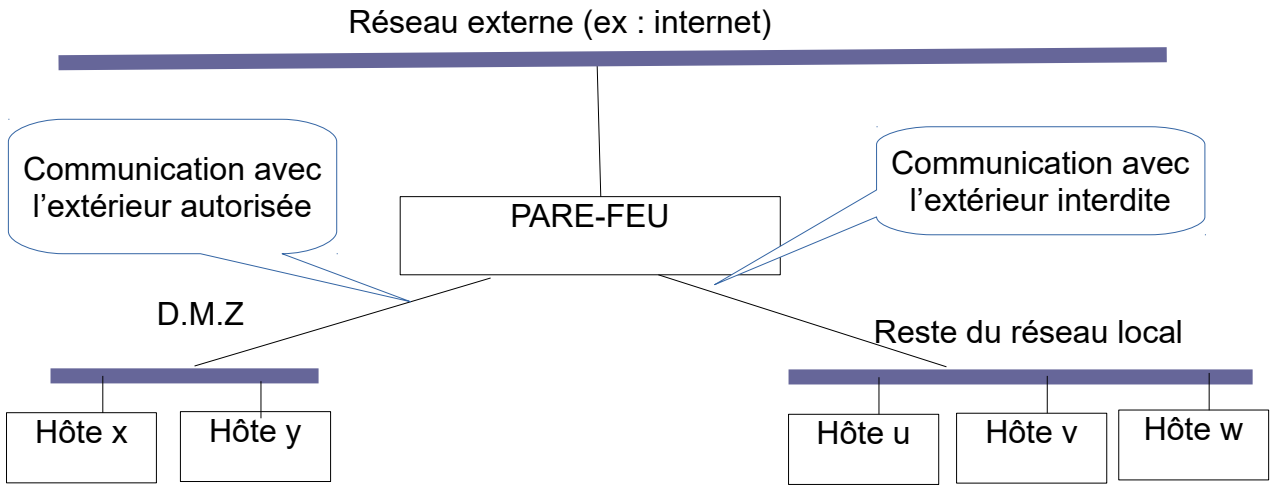
II.3.ASPECT ARCHITECTURAL:

En première analyse, on peut distinguer deux méthodes possibles pour installer une DMZ dans un réseau local:

II.3.1.LA DMZ AVEC UN SEUL PARE-FEU:

C'est le cas de l'exemple ci-dessus: cette architecture utilise un seul composant physique pare-feu supportant et gérant trois interfaces réseau. Le réseau externe est connecté à la première interface. Le réseau interne protégé est connecté à une deuxième interface, tandis que la troisième interface se connecte à la DMZ.

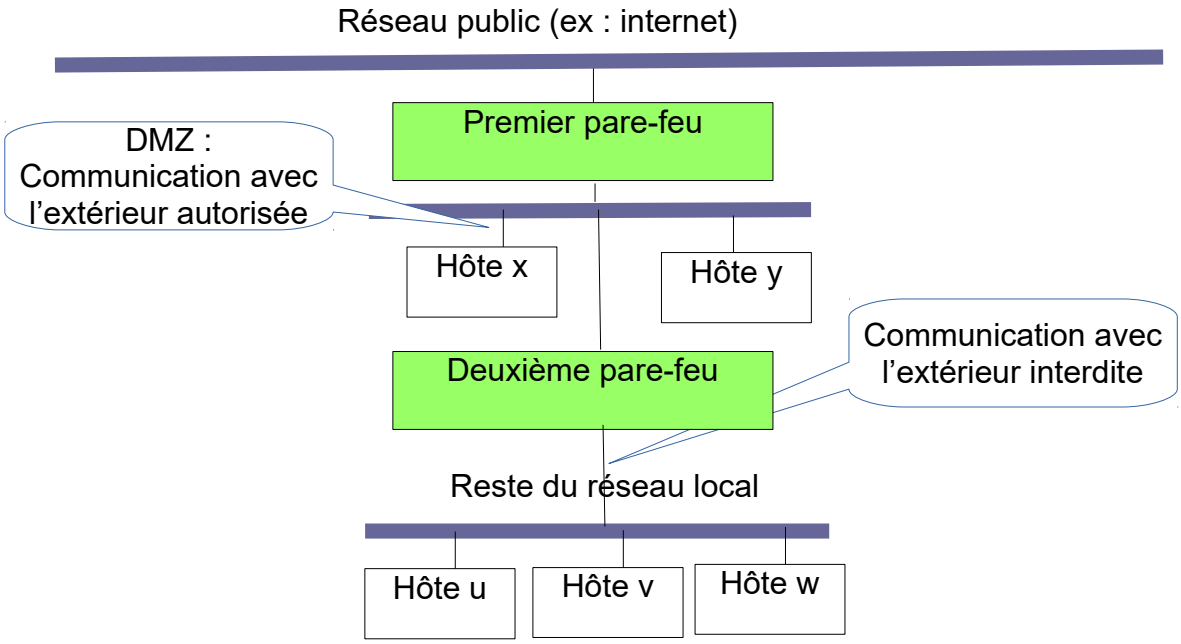
Le pare-feu va contrôler le trafic circulant entre le réseau externe et la DMZ, et entre le réseau local et la DMZ:



La faiblesse de cette architecture résulte du fait que si le pare-feu est compromis, la sécurité du LAN «tombe» entièrement.

II.3.2.LA DMZ AVEC DEUX PARE-FEUX:

Une architecture plus sécurisée consiste à utiliser deux composants pare-feux gérant chacun au moins deux interfaces réseau, pour créer une DMZ: le premier pare-feu filtre le trafic entre l'extérieur et la DMZ tandis que le deuxième filtre le trafic entre la DMZ et le reste du réseau local:



Le premier pare-feu ne laisse passer que le trafic entre l'extérieur et la DMZ. Le second n'autorise que le trafic entre la DMZ et le réseau interne. Cette configuration est mieux sécurisée car il faut compromettre deux machines pour accéder au réseau interne.

II.3.3.REMARQUE : UTILITÉ DES PARE-FEUX PERSONNELS DANS UN ENVIRONNEMENT PROTÉGÉ:

Le fait pour un poste de travail d'être situé das un LAN incluant une DMZ n'exclue pas l'utilisation d'un pare-feu personnel sur ce poste. En effet :

- Il est souvent prudent de limiter les communications extérieures permises à un poste situé dans la D.M.Z au strict nécessaires. Par exemple, si le poste n'a besoin que d'accéder au WEB, on peut limiter l'accès aux seuls paquets correspondant à des requêtes HTTP sur le port 80;
- Il peut être utile d'interdire l'accès de certains logiciels à un poste situé en zone protégée (pour éviter par exemple les prises en main à distance depuis le réseau local).