SÉCURITÉ DES RÉSEAUX
Travaux pratiques : lab n°4 – 8 heures

Utilisation avancé du filtrage de paquets réseaux
Construction d'une DMZ complexe

---

1 Aperçu du lab :

Au cours de ce TP, vous allez devoir utiliser toutes les connaissances que vous avez acquises sur le filtrage de paquets réseaux pour mettre en œuvre l'architecture d'une DMZ « complexe ». L'entreprise dans laquelle vous intervenez a besoin de mettre en ligne une application web présente sur son réseaux local. Cette application dispose d'une base de données.

Vous décidez donc de prévoir la création de deux DMZ :

- l'une, publique, contenant uniquement le serveur Web et le code source de l'application,
- l'autre privée, contenant le serveur de base de données.

Le caractère publique ou privé de chacune de ces zones sera déterminé par les règles de filtrage qui leur sont appliquées. Après étude vous disposez à la fois d'un schéma d'architecture[1], et d'une liste de flux à autoriser.

Les technologies employées sur ce réseau sont déjà en place, et vous devrez donc vous adapter à l'existant. Aussi vous serez amené à configurer des règles de filtrage sur des serveurs linux de deux façons différentes (iptables et nftables) ainsi que sur deux firewalls pfsense.

2 Objectifs du lab :

Les objectifs de ce lab sont multiples :

- vous faire manipuler le concept de DMZ en réfléchissant aux interconnexions, ainsi qu'en implémentant les règles de filtrage,
- vous faire manipuler des firewalls au niveau réseau, et non plus au niveau hôte,
- vous faire prendre en main plusieurs technologies de filtrage de paquets (iptables[2], nftables[3], pfsense[4], …)

1 *Cf Annexe – Schéma de l'architecture réseau de la DMZ*
2 *Cf site internet : https://netfilter.org/projects/iptables/index.html*
3 *Cf site internet : https://wiki.nftables.org/wiki-nftables/index.php/Main_Page*
4 *Cf site internet : https://docs.netgate.com/pfsense/en/latest/index.html*

3 Les consignes :

3.1 Préparation de l'architecture :

3.1.1 Considérations générales :

Pour chacun des firewalls, que vous devrez par la suite configurer, vous :

- appliquerez une politique par défaut très restrictive. **Aussi, à défaut de règle explicite, tout le trafic entrant et sortant sera bloqué.**
- Configurer le firewall pour qu'il soit « à état ». (**stateful**)

3.1.2 Préparation du serveur Web :

Le serveur Web devra être positionné sur un réseau dédié comme indiqué sur le schéma, et disposer d'une adresse IP fixe. Il hébergera sur un serveur Apache l'application Wordpress, et fonctionnera sous Centos 7.

Vous devrez configurer les règles de filtrage sur le serveur à l'aide de **iptables** compte-tenu des informations suivantes :

1. Le serveur doit être en mesure de faire ses mises à jour.
2. Le site internet doit pouvoir interroger la base de données présente sur le serveur de base de données.
3. Il doit être possible de se connecter au site internet depuis n'importe où, y compris du réseau local et d'internet.
4. Les informaticiens doivent pouvoir se connecter en SSH sur ce serveur.
5. Les informaticiens doivent être en mesure de »pinguer » ce serveur.

3.1.3 Préparation du serveur de base de données :

Le serveur de base de données devra être positionné sur un réseau dédié comme indiqué sur le schéma, et disposer d'une adresse IP fixe. Il fonctionnera sous Centos 8 , et hébergera via un serveur mysql la base de données du site Wordpress.

Vous devrez configurer les règles de filtrage sur le serveur à l'aide de **nftables** compte-tenu des informations suivantes :

1. Le serveur doit être en mesure de faire ses mises à jour.
2. La base de données doit pouvoir être consultée par le serveur web (et uniquement par lui).
3. Les informaticiens doivent pouvoir se connecter en SSH sur ce serveur.
4. Les informaticiens doivent être en mesure de »pinguer » ce serveur.

3.2 Construction de la DMZ :

3.2.1 Préparation du firewall frontal

Note : les ports TCP 80 et 443 du firewall frontal devront être transférés vers ceux du serveur Web.

Sur le firewall frontal pfsense vous devrez configurer les règles de filtrage compte-tenu des informations suivantes :

1. Les visiteurs d'internet et du réseau local, y compris VLAN informaticiens doivent pouvoir consulter le site internet.
2. La base de données doit pouvoir être consultée par le serveur web (et uniquement par lui).
3. Les informaticiens doivent pouvoir se connecter en SSH sur les deux serveurs.
4. Les informaticiens doivent être en mesure de »pinguer » les deux serveurs.
5. Les postes du réseau local doivent pouvoir naviguer sur internet.

3.2.2 Préparation du firewall de seconde ligne

Sur le second firewall pfsense vous devrez configurer les règles de filtrage compte tenu de la matrice des flux suivantes :

1. Les visiteurs du réseau local, y compris VLAN informaticiens doivent pouvoir consulter le site internet.
2. Les informaticiens doivent pouvoir se connecter en SSH sur les deux serveurs.
3. Les informaticiens doivent pouvoir se connecter à la webgui des deux firewalls.
4. Les informaticiens doivent être en mesure de »pinguer » les deux serveurs.
5. Les postes du réseau local doivent pouvoir naviguer sur internet.

4 Les livrables :

A l'issue de ce TP, vous devrez me présenter vos résultats. Votre présentation devra contenir également les réponses aux éventuelles questions théoriques posées Toutes les manipulations que vous allez faire devront être testée et vous devrez prouver leur bon fonctionnement.
La note tiendra compte de vos résultats, l'implication sur le lab, ainsi que la clarté de vos explications.

5 Annexes :

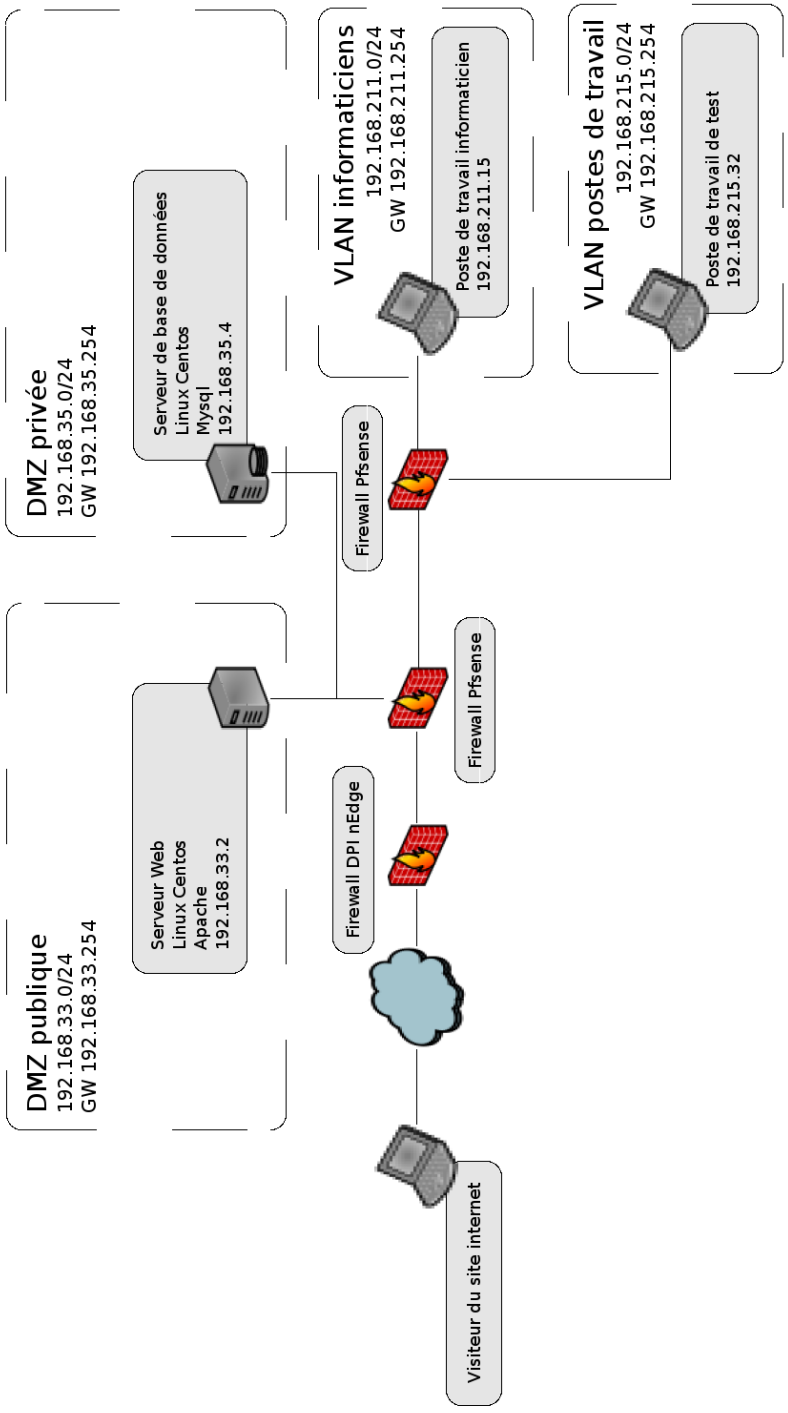

Illustration 1: Schéma de l'architecture réseau de la DMZ