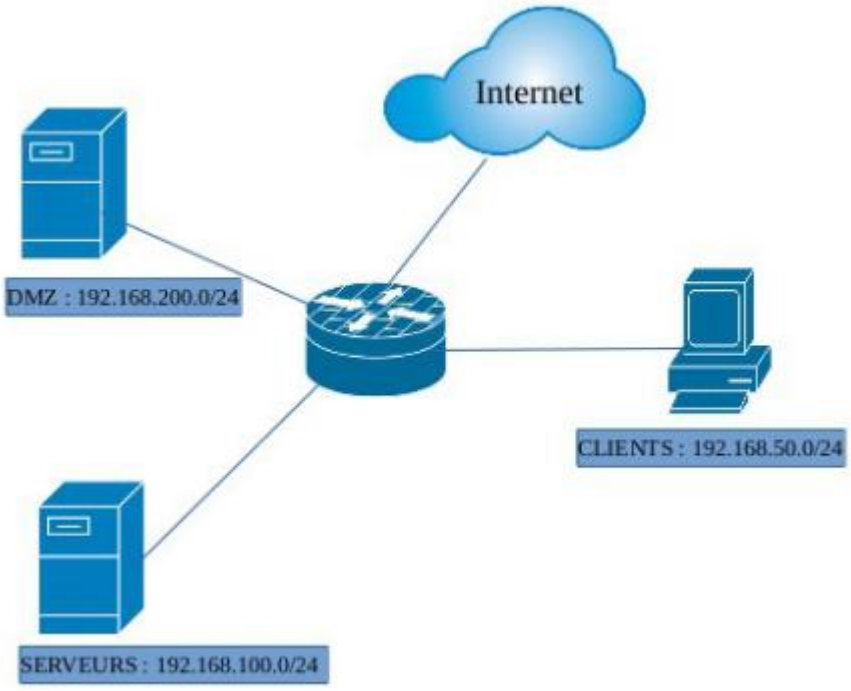
NOM Prénom : Ethan Georget
BTS SIO SISR - Bloc 3
Compte-Rendu : Filtrage et Traduction d'adresses (NAT) sous pfSense

DOSSIER TECHNIQUE : ADMINISTRATION ET FILTRAGE PÉRIMÉTRIQUE

1. Présentation de la maquette

L'objectif de ce laboratoire est la prise en main du pare-feu pfSense à travers la configuration du filtrage réseau et de la traduction d'adresses (NAT). L'infrastructure virtuelle MLIF simule trois zones distinctes : le réseau CLIENTS (192.168.50.0/24), la DMZ (192.168.200.0/24) hébergeant le serveur web, et le réseau SERVEURS (192.168.100.0/24) pour les services DNS et Mail.



1.1 Configuration des interfaces sous VirtualBox

Le routeur pfSense dispose de quatre interfaces réseau : une interface en accès par pont pour l'accès WAN et trois réseaux internes (sw-dmz, sw-serveur, sw-client). Toutes les machines virtuelles ont été configurées avec 1 Go de RAM pour garantir la stabilité des services .

Machine PF_FIREWALL :

CARTES	CONFIGURATIONS
Interface 1 (déjà activée)	Accès par pont sur la carte filaire du réseau du lycée.
Interface 2 (à activer)	Réseau interne nommé sw-dmz.
Interface 3 (à activer)	Réseau interne nommé sw-serveur.
Interface 4 (à activer)	Réseau interne nommé sw-client.

Machine DEBIAN_TRAINING_CLIENT :

CARTES	CONFIGURATIONS
Interface 1 (déjà activée)	Réseau interne nommé sw-client.

Machine DEBIAN_TRAINING_SERVEUR :

CARTES	CONFIGURATIONS
Interface 1 (déjà activée)	Réseau interne nommé sw-serveur.

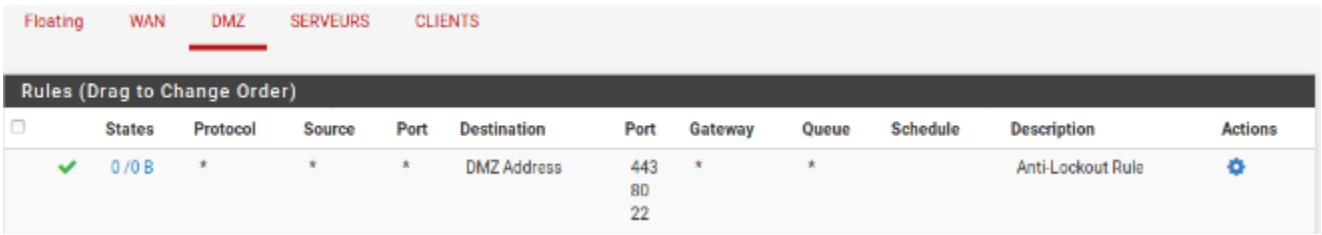
Machine DEBIAN_TRAINING_DMZ :

CARTES	CONFIGURATIONS
Interface 1 (déjà activée)	Réseau interne nommé sw-dmz.

2. Configuration initiale et Refus Implicite

Avant toute configuration, le serveur DNS Bind9 a été mis à jour avec les forwarders du lycée (172.16.10.20/21). Une politique de sécurité rigoureuse dite de 'Refus Implicite' (Implicit Deny) a été appliquée.

Tous les flux sont interdits par défaut, à l'exception des règles d'administration (Anti-Lockout Rule) permettant de conserver l'accès web et SSH au pare-feu. Cette étape a été validée par la création d'un snapshot nommé 'IMPLICIT-DENY'.



2.1 Paramétrage des redirecteurs DNS (Forwarders)

Afin de permettre la résolution de noms externes depuis le réseau de la MLIF, j'ai édité le fichier /etc/bind/named.conf.options sur le serveur Debian. J'y ai renseigné les adresses IP des serveurs DNS du lycée (172.16.10.20 et 172.16.10.21) dans la clause forwarders, puis j'ai redémarré le service pour valider la configuration.

```
directory "/var/cache/bind";

// If there is a firewall between you and nameservers you want
// to talk to, you may need to fix the firewall to allow multiple
// ports to talk.  See http://www.kb.cert.org/vuls/id/800113

// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

 forwarders {
        172.16.10.20;
        172.16.20.21;
};

allow-query {192.168.0.0/16; 172.16.10.0/24; localnets;};
//========================================================================
// If BIND logs error messages about the root key being expired,
// you will need to update your keys.  See https://www.isc.org/bind-keys
//========================================================================
dnssec-validation no;

auth-nxdomain no;    # conform to RFC1035
listen-on-v6 { any; };
```

3. Gestion des Aliases et Règles de filtrage

Pour simplifier l'administration et la maintenance des règles, nous avons créé des Aliases de type IP (SRV_DNS, SRV_MAIL) et de type PORT (PORT_WEB, PORT_DNS).

Firewall Aliases IP

Name	Values	Description	Actions
DEBIAN_TRAINING_DMZ	192.168.200.5		
DEBIAN_TRAINING_SERVEUR	192.168.100.10		
IPS_DNS_LYCEE	IP_DNS_LYCEE_1, IP_DNS_LYCEE_2		
IP_BLACKLIST_CLIENTS	192.168.50.20		
IP_DNS_LYCEE_1	172.16.10.6		
IP_DNS_LYCEE_2	172.16.10.7		
SRV_DNS	192.168.100.10		
SRV_FTP	192.168.100.10		
SRV_MAIL	192.168.100.10		

En complément des adresses IP, j'ai créé des alias de ports pour regrouper les services par thématiques (DNS, Web, Mail). Par exemple, l'alias PORT_WEB regroupe les ports 80 (HTTP) et 443 (HTTPS). Cette centralisation permet de modifier une seule fois l'alias pour mettre à jour l'ensemble des règles de filtrage qui l'utilisent.

Firewall Aliases Ports

Name	Values	Description	Actions
PORT_DNS	53		
PORT_IMAP	143		
PORT_MAIL	PORT_IMAP, PORT_SMTP		
PORT_SMTP	25		
PORT_WEB	80, 443		

3.1 Mise en œuvre de la politique de filtrage

Quatre règles majeures (R1 à R4) ont été déployées :
- R1 : Autorisation des requêtes DNS vers SRV_DNS (avec exclusion de l'IP 192.168.50.20).
- R2 : Autorisation du serveur DNS local vers les DNS extérieurs.
- R3 : Accès Internet autorisé pour le réseau CLIENTS et les serveurs critiques (DMZ/SERVEURS).
- R4 : Administration SSH du serveur Web restreinte au seul serveur de messagerie.

Pour valider le fonctionnement de la règle R1 (autorisation DNS), j'ai utilisé la commande nslookup depuis la machine cliente vers www.mlif.local. Après avoir vidé le cache DNS local, j'ai pu confirmer que pfSense autorisait bien la requête et que le serveur DNS interne répondait avec l'adresse IP correcte.

Firewall / Rules / LAN

Floating | WAN | LAN | SRV | DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1/1.01 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
0/0 B	IPv4 UDP	IP_BLACKLIST_CLIENTS	*	SRV_DNS	53 (DNS)	*	none			
73/114 KiB	IPv4 UDP	LAN net	*	SRV_DNS	53 (DNS)	*	none			

4. Traduction d'adresses (NAT)

4.1 NAT Outbound

Les adresses RFC 1918 (privées) n'étant pas routables sur Internet, pfSense effectue une traduction de source (Outbound NAT). Le mode 'Automatic Outbound' est activé par défaut pour permettre aux machines internes d'accéder au WAN.

4.2 NAT Inbound (Port Forwarding)

Afin de rendre le serveur web accessible depuis l'extérieur (réseau du lycée), une redirection de port (Destination NAT) a été configurée. Cette règle redirige le trafic entrant sur l'interface WAN vers l'adresse 192.168.200.5.

J'ai créé une règle de transfert de port (Destination NAT) sur l'interface WAN. Toute requête TCP arrivant sur l'adresse IP du pare-feu avec l'alias PORT_WEB est automatiquement redirigée vers l'adresse IP interne du serveur web (192.168.200.5). pfSense a automatiquement généré la règle de filtrage correspondante pour autoriser ce flux.

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐ ✓ ⇄	WAN	TCP	*	*	WAN address	PORT_WEB	192.168.200.5	PORT_WEB		✎ ⧉ 🗑

5. Conclusion

Ce TP a permis de valider la maîtrise du pare-feu pfSense. La mise en place du refus implicite couplée à l'utilisation des aliases garantit une infrastructure à la fois sécurisée et facile à administrer.