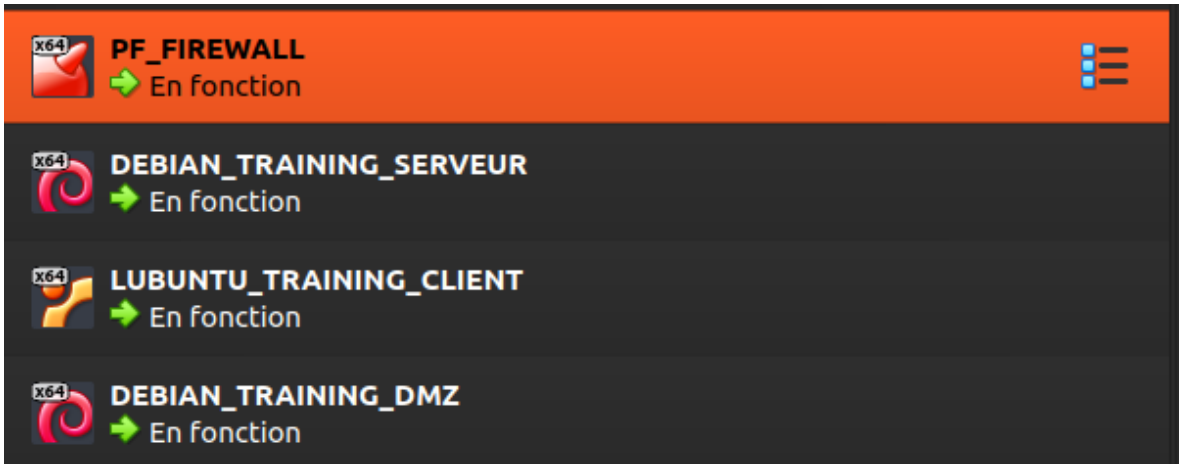
Tout d'abord on va vérifier la config de ces 4 machines :



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.

LUBUNTU_TRAINING_CLIENT :

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

DEBIAN_TRAINING_SERVEUR :

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

DEBIAN_TRAINING_DMZ :

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

Ensuite on démarre les 4 machines

Il faut ensuite modifier le serveur DNS afin de changer les forwarder.

Sur DEBIAN_TRAINING_SERVEUR on va faire :

```
nano /etc/bind/named.conf.options
```

```
options {
        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; };
};
```

On va modifier à l'intérieur de forwarders pour avoir la même chose que le screen au dessus

Et ensuite on va restart bin9 :

service bind9 restart

Et on va vérifier qu'il n'y a pas de souci avec bind9 avec :

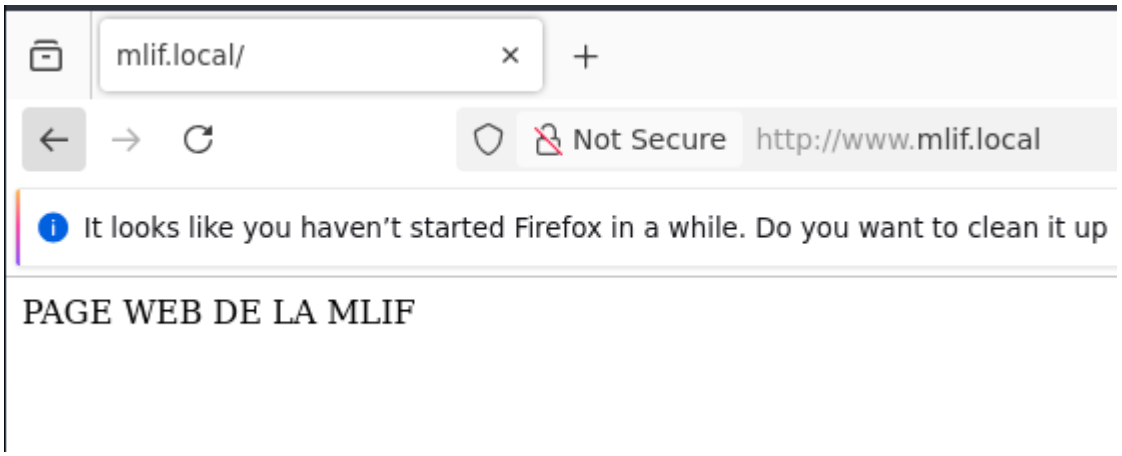
service bind9 status

```
root@messagelab:~# service bind9 status
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-09-12 16:38:56 CEST; 31s ago
       Docs: man:named(8)
   Main PID: 1038 (named)
     Status: "running"
      Tasks: 4 (limit: 1097)
     Memory: 11.1M
        CPU: 21ms
     CGroup: /system.slice/named.service
             └─1038 /usr/sbin/named -f -u bind

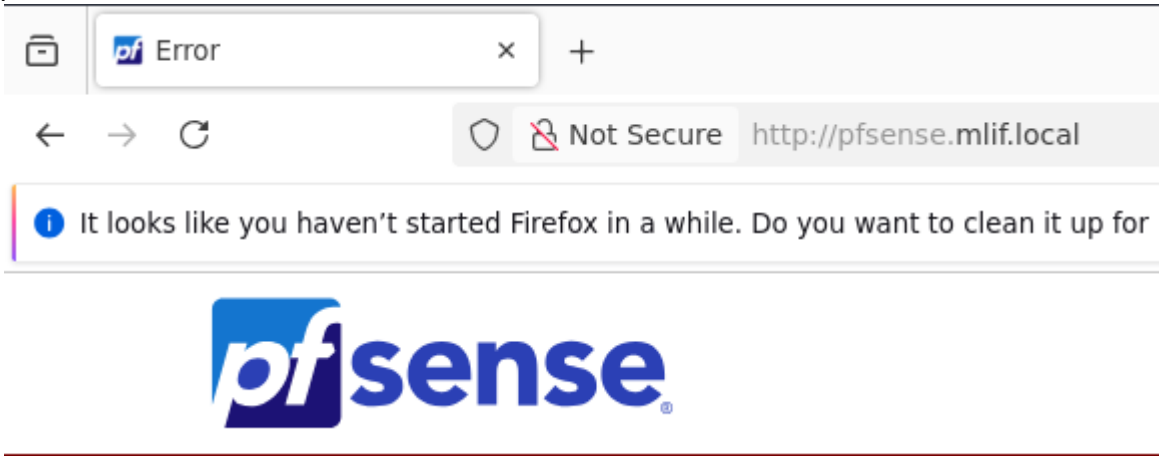
sept. 12 16:38:56 messagelab named[1038]: zone 0.in-addr.arpa/IN: loaded serial 1
sept. 12 16:38:56 messagelab named[1038]: zone 255.in-addr.arpa/IN: loaded serial 1
sept. 12 16:38:56 messagelab named[1038]: zone mlif.local/IN: loaded serial 11
sept. 12 16:38:56 messagelab named[1038]: zone 100.168.192.in-addr.arpa/IN: loaded serial 9
sept. 12 16:38:56 messagelab named[1038]: zone 200.168.192.in-addr.arpa/IN: loaded serial 1
sept. 12 16:38:56 messagelab named[1038]: zone 127.in-addr.arpa/IN: loaded serial 1
sept. 12 16:38:56 messagelab named[1038]: zone localhost/IN: loaded serial 2
sept. 12 16:38:56 messagelab named[1038]: all zones loaded
sept. 12 16:38:56 messagelab systemd[1]: Started named.service - BIND Domain Name Server.
sept. 12 16:38:56 messagelab named[1038]: running
```

Ouvrir le navigateur et tester un accès au serveur web en saisissant www.mlif.local. A l'aide d'un second onglet, tester un accès au pare-feu en saisissant https://pfsense.mlif.local. Enfin tester un accès à Internet en effectuant une recherche sur google en ouvrant un troisième onglet

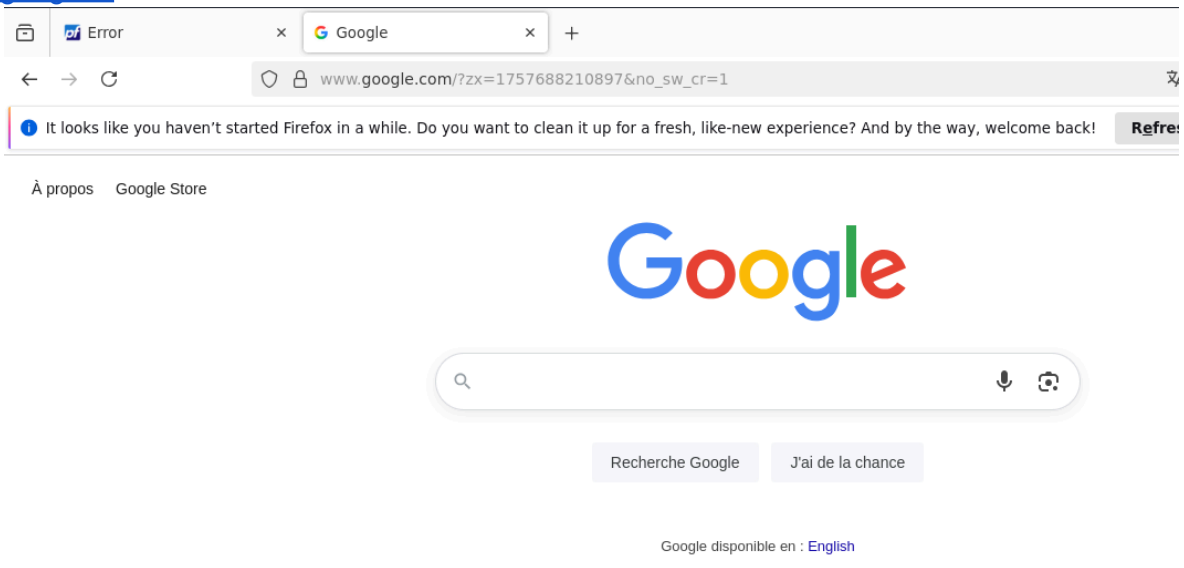
mlif.local :



pfsense.mlif.local :



google.fr :



ping messagelab.mlif.local :

```
root@www:~# ping messagelab.mlif.local
PING messagelab.mlif.local (192.168.100.10) 56(84) bytes of data.
64 bytes from messagelab.mlif.local (192.168.100.10): icmp_seq=1 ttl=63 time=0.277 ms
64 bytes from messagelab.mlif.local (192.168.100.10): icmp_seq=2 ttl=63 time=0.616 ms
64 bytes from messagelab.mlif.local (192.168.100.10): icmp_seq=3 ttl=63 time=0.496 ms
^C
--- messagelab.mlif.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 0.277/0.463/0.616/0.140 ms
```

nslookup www.mlif.local :

```
root@www:~# nslookup www.mlif.local
Server:         192.168.100.10
Address:        192.168.100.10#53

Name:   www.mlif.local
Address: 192.168.200.5

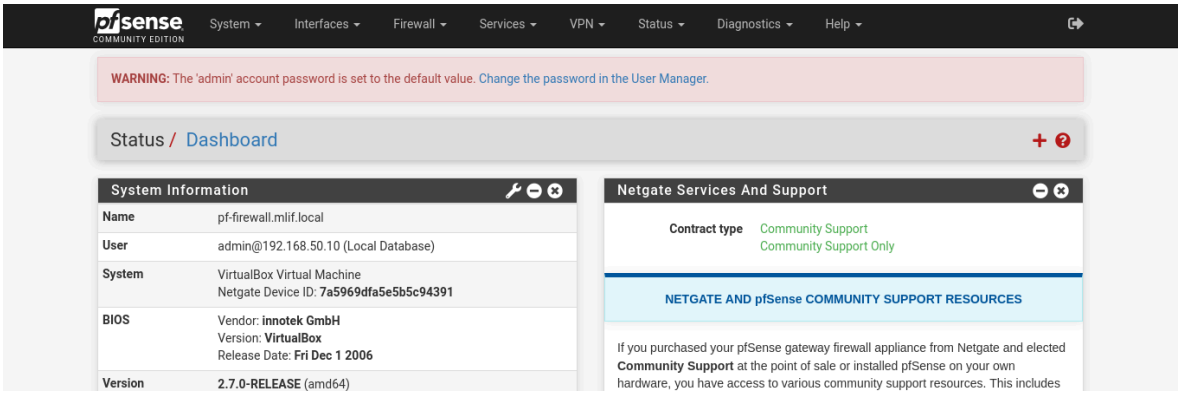
root@www:~#
```

ping www.cisco.com :

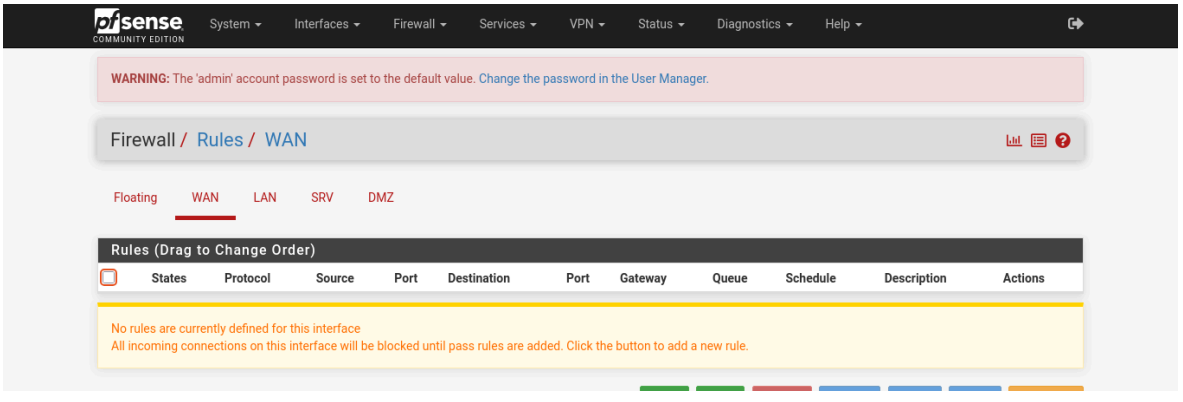
```
root@www:~# ping www.cisco.com
PING e2867.dsca.akamaiedge.net (2.20.10.35) 56(84) bytes of data.
64 bytes from a2-20-10-35.deploy.static.akamaitechnologies.com (2.20.10.35):
```

Depuis la machine client, se connecter sur le pare-feu avec le compte admin/pfsense.

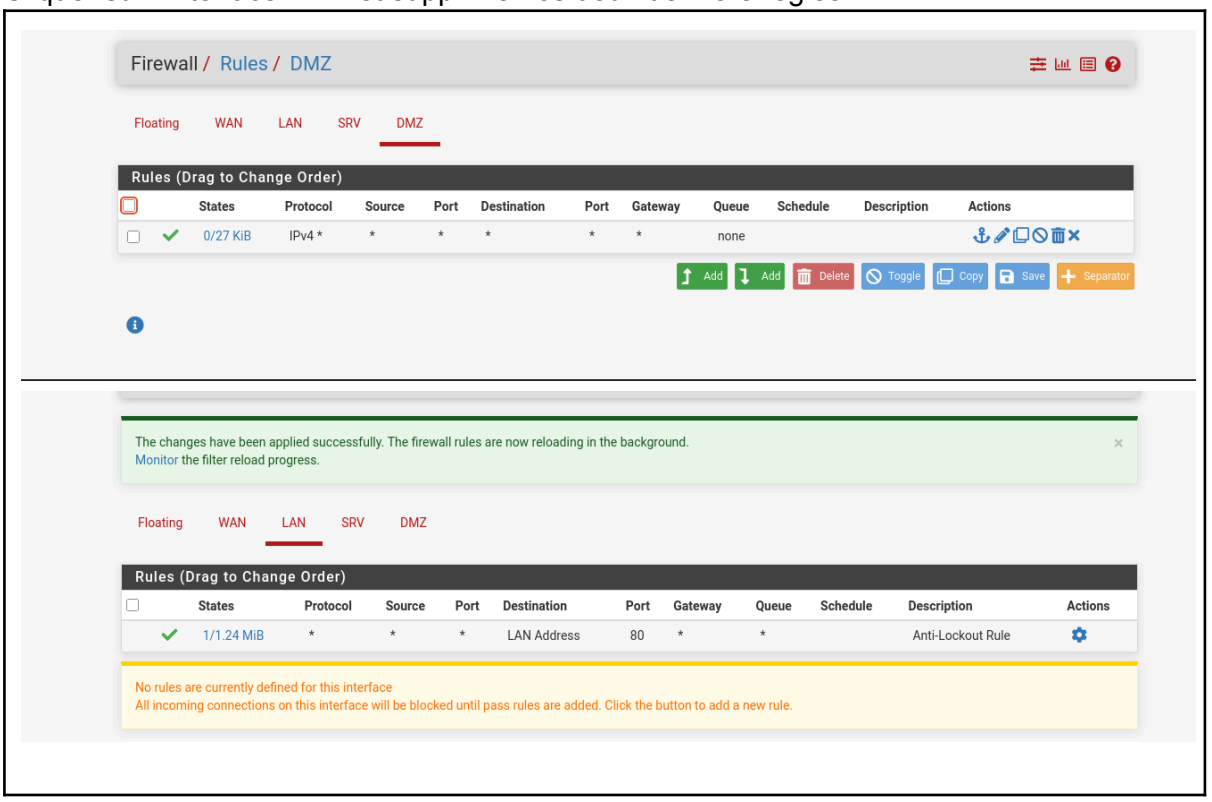
on tape dans l'url : 192.168.50.254



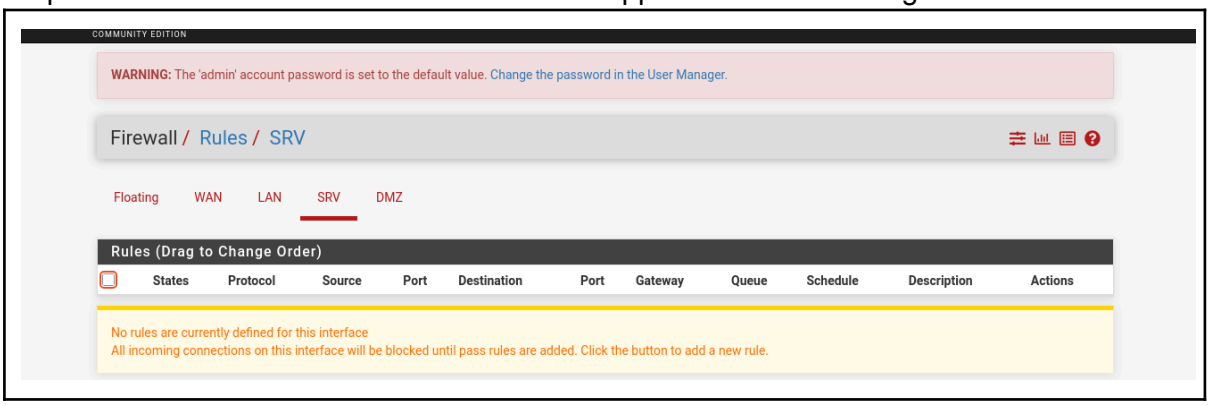
Ensuite, cliquer sur le menu Firewall puis sur Rules. Vous constatez qu'il y a autant d'onglets que d'interfaces.



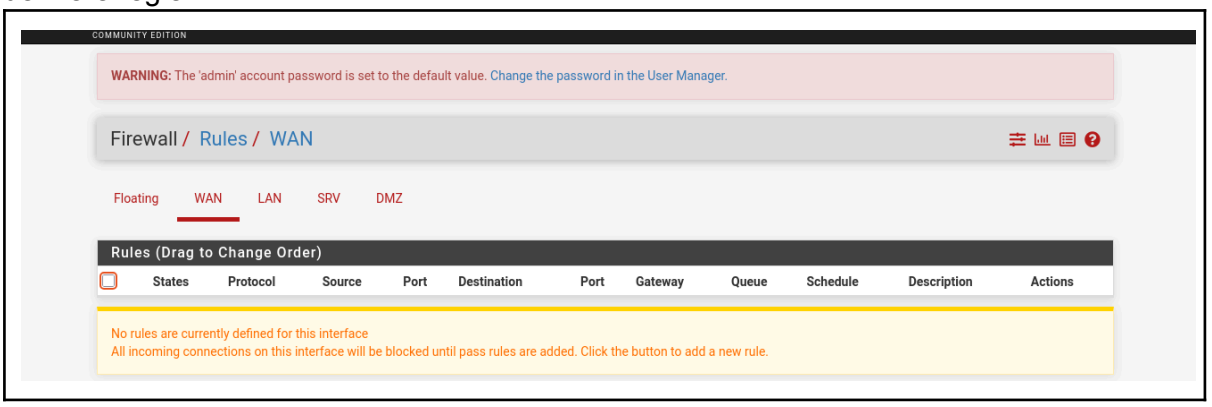
Cliquer sur l’interface DMZ et supprimer les deux dernière règles



Cliquer ensuite sur l’interface SERVEURS et supprimer la dernière règle seulement :



Cliquer ensuite sur l’interface CLIENTS et faire de même en supprimant uniquement la dernière règle.

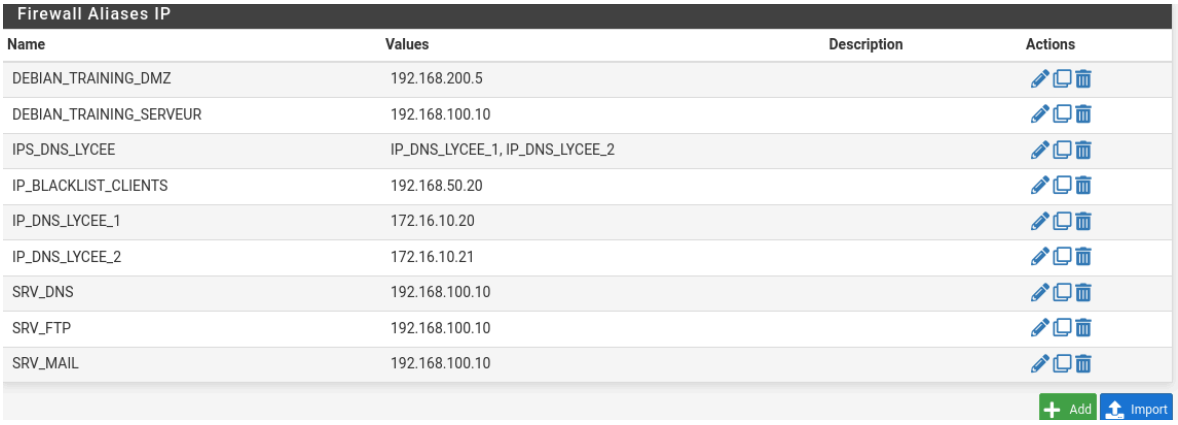


Tester les ping (les 2 doivent échouer) (depuis la DMZ) :



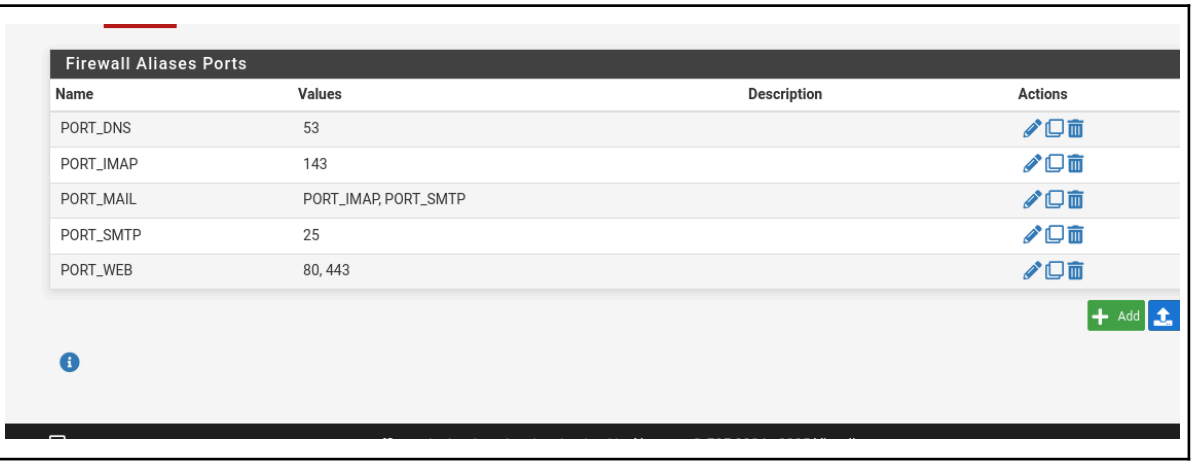
Vous devez créer les aliases suivants :

Aliases de type IP :



Cliquer sur add host pour avoir plusieurs values

Aliases de ports :



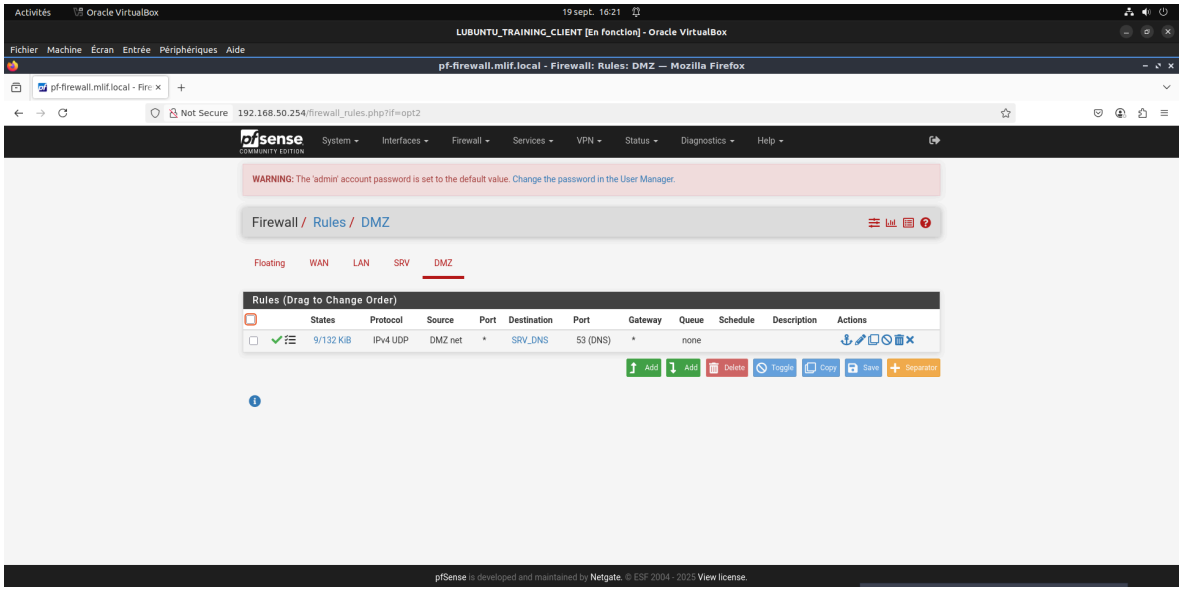
R1 : Autoriser toutes les machines des trois réseaux internes (DMZ, SERVEURS, CLIENTS) à interroger le serveur DNS du contexte à l'exception de la machine d'adresse IP 192.168.50.20.

Faîtes en sorte de garder une trace des flux associés à cette règle dans les logs.

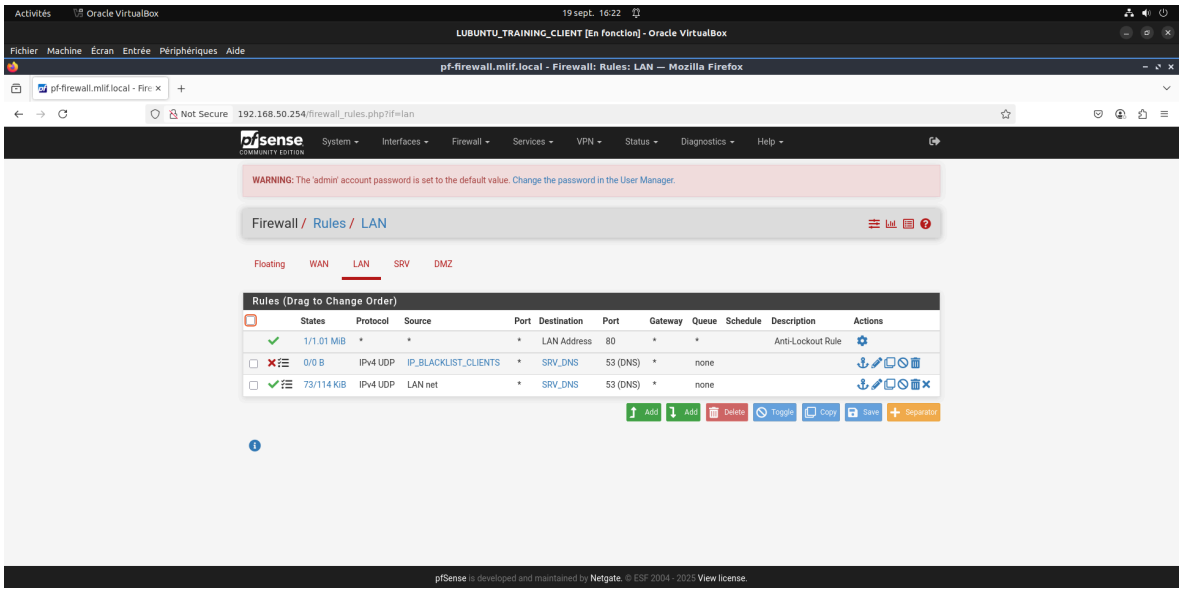
Pour créer cette règle, vous devez sélectionner les aliases de réseau implicite DMZ net, SERVEUR net et CLIENT net comme adresses IP source et sélectionner l'aliases d'hôte SRV_DNS comme adresse IP de destination et le port PORT_DNS comme port de destination. Noter que le trafic de retour est implicite.

Faites bien attention à l'ordre des règles que vous pouvez modifier par un glisser-déposer à l'aide de la souris.

R1 DMZ :



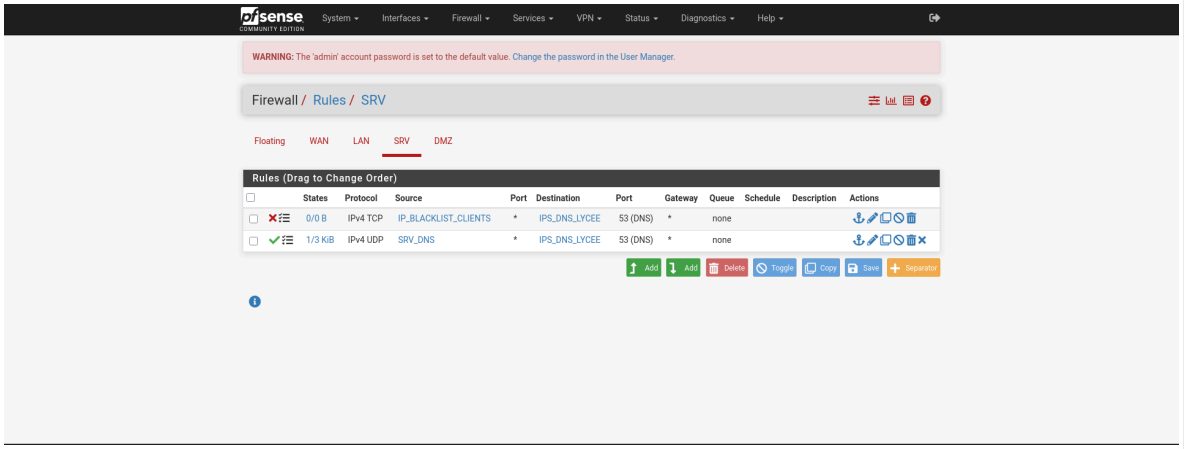
R1 LAN :



Commande pour clear le cache sur lubuntu : sudo resolvectl flush-caches
et sur dmz : systemctl restart networking
Puis nslookup www.mlif.local

R1 validé

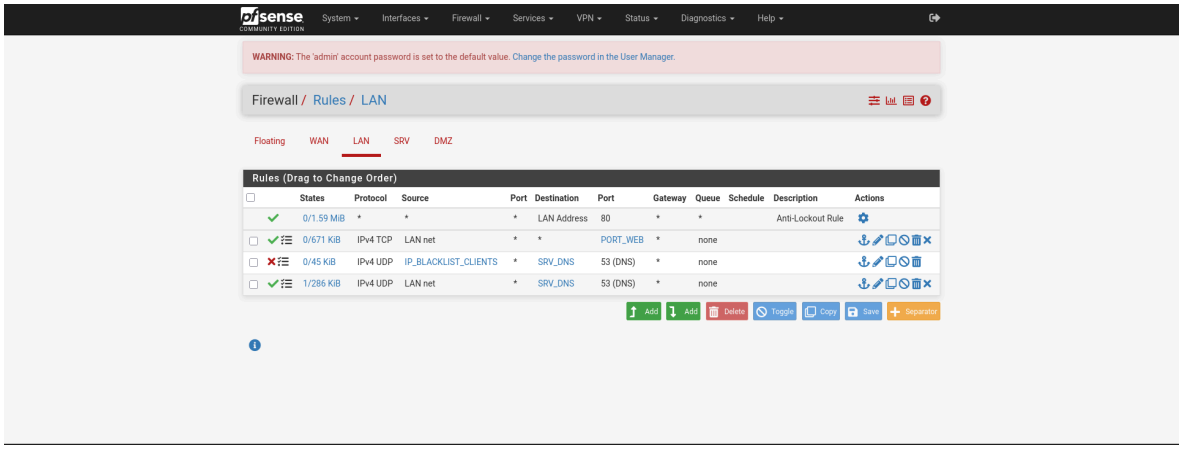
R2 :



nslookup externe (exemple youtube.com

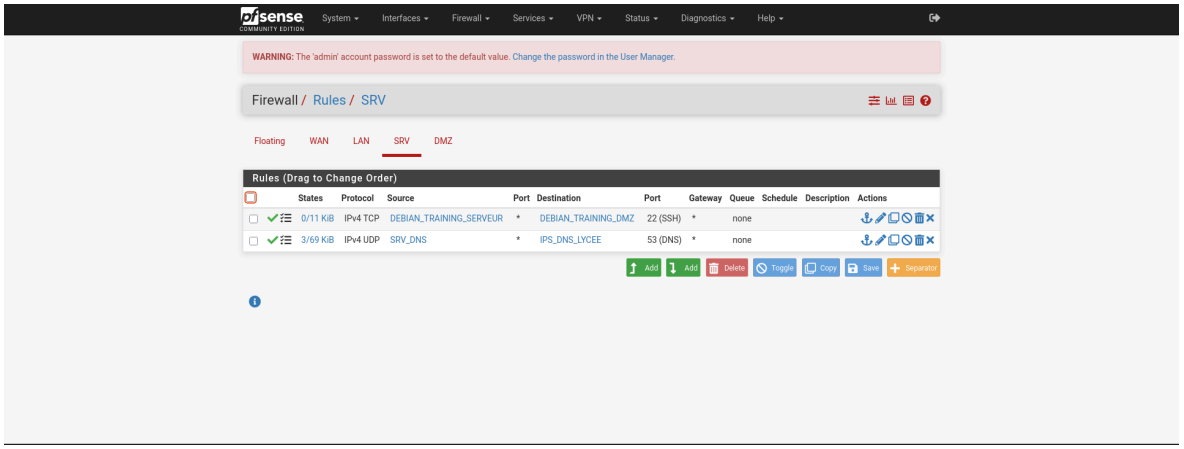
R2 validé

R3 :



faut surfer pour valider la règle depuis la lubuntu

R4 :

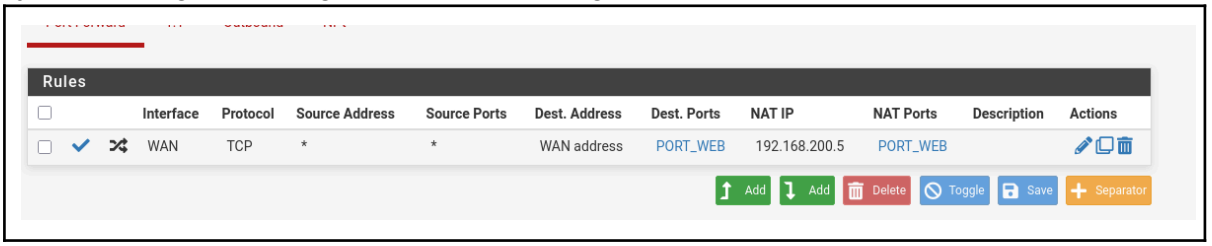


Tester la connexion ssh : ssh test@www.mlif.local

STOP 2

Cliquer sur Firewall puis sur NAT. Cliquer ensuite sur l'onglet Outbound. Vous constatez que le mode Automatic Outbound est coché. D'autres modes de configurations existent et ne sont pas abordés dans le
cadre de ce TP.

Par extérieur, on entend une machine appartenant au réseau du lycée (172.17.123.X ou 172.17.124.X).
Pour tester cette règle, vous saisirez l'adresse de l'interface WAN (adresse obtenue via DHCP) du pare-feu sur le navigateur de la machine externe. Attention, par défaut pfsense bloque les flux RFC1918 venant de l'extérieur à destination de l'interface WAN. Pour enlever provisoirement ce blocage, observez bien les deux règles par défaut présentes dans l'interface WAN et supprimez les. Remarquez aussi que le pare-feu a automatiquement ajouté une règle de filtrage associé à votre règle NAT



On rentre l'adresse de l'interface WAN obtenue sur le parefeu, on voit bien qu'on a site web local de la mlif
STOP3