

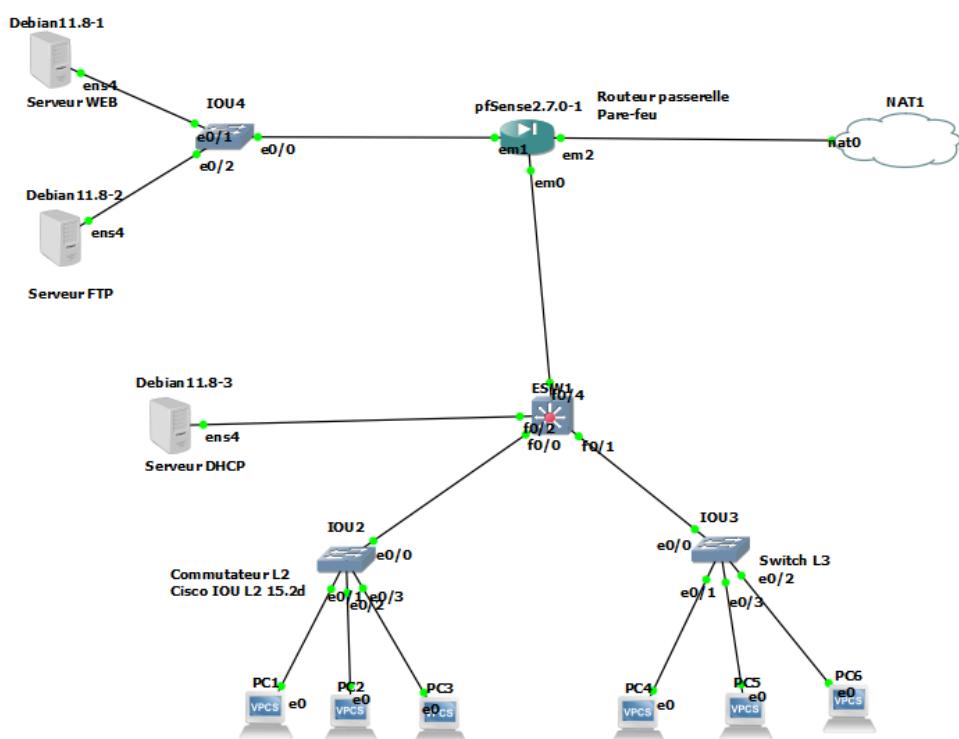
SAE 2.01 : Construire un réseau informatique pour une petite structure

**Voici le rapport final
comportant les procédures et
résultats pour la mise en place
d'une infrastructure de réseau
d'entreprise :**

Une fois toutes les licences obtenues,

```
[license]
gns3vm = 73635fd3b0a13ad0;
```

On commence par créer la topologie de notre futur réseau :



Puis on décide du plan d'adressage de cette structure :

VLAN	NOM	Réseaux	PASSERELLE	Plage du service DHCP
10	DIRECTION	192.168.10.0	192.168.10.2	192.168.10.99 - 192.168.10.200
20	GESTION	192.168.20.0	192.168.20.2	192.168.20.99 - 192.168.20.200
30	COMTECH	192.168.30.0	192.168.30.2	192.168.30.99 - 192.168.30.200

Il faut ensuite créer un réseau segmenté comprenant la mise en place et la configuration des VLAN (Dans les deux commutateurs d'accès de couche 2) :

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	unset	up	up
Ethernet0/1	unassigned	YES	unset	up	up
Ethernet0/2	unassigned	YES	unset	up	up
Ethernet0/3	unassigned	YES	unset	up	up
Ethernet1/0	unassigned	YES	unset	up	up
Ethernet1/1	unassigned	YES	unset	up	up
Ethernet1/2	unassigned	YES	unset	up	up
Ethernet1/3	unassigned	YES	unset	up	up
Ethernet2/0	unassigned	YES	unset	up	up
Ethernet2/1	unassigned	YES	unset	up	up
Ethernet2/2	unassigned	YES	unset	up	up
Ethernet2/3	unassigned	YES	unset	up	up
Ethernet3/0	unassigned	YES	unset	up	up
Ethernet3/1	unassigned	YES	unset	up	up
Ethernet3/2	unassigned	YES	unset	up	up
Ethernet3/3	unassigned	YES	unset	up	up
Vlan1	unassigned	YES	unset	administratively down	down

Voici donc l'affectation des différents ports aux différents VLAN et donc réseaux :

Port (pour les Switchs IOU2 et IOU3)	Affectation	Réseaux
Ethernet 0/0-3	VLAN 10	192.168.10.0
Ethernet 1/0-3	VLAN 20	192.168.20.0
Ethernet 2/0-3	VLAN 30	192.168.30.0

On obtient donc ce script de configuration de switch :

```
enable
configure terminal

vlan 10
name Direction
exit

vlan 20
name Gestion
exit

vlan 30
name COMTECH
exit
```

```
interface Gi0/0
no switchport
ip address 192.168.69.2 255.255.255.0
```

```
interface Gi0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

```
interface Gi0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

```
interface Gi0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

```
interface vlan 10
ip address 192.168.10.1 255.255.255.0
exit
```

```
interface vlan 20
ip address 192.168.20.1 255.255.255.0
exit
```

```
interface vlan 30
ip address 192.168.30.1 255.255.255.0
exit
```

```
ip routing
```

```
end
wr
```

Idem pour l'autre switch de niveau 2 :

```
enable
configure terminal
```

```
vlan 10
name DIRECTION
exit
```

```
vlan 20
name GESTION
exit
```

```
vlan 30
name COMTECH
exit
```

```
interface range eth0/0-3
switchport mode access
switchport access vlan 10
exit
```

```
interface range eth1/0-3
switchport mode access
```

```
switchport access vlan 20
exit
```

```
interface range eth2/0-3
switchport mode access
switchport access vlan 30
exit
```

```
interface eth3/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

On peut ensuite mettre en place et configuration du routage inter-VLAN (nécessitant donc un commutateur de distribution de couche 3 expliquant le choix du Switch L3 :

```
enable
configure terminal
```

```
vlan 10
name Direction
exit
```

```
vlan 20
name Gestion
exit
```

```
vlan 30
name COMTECH
exit
```

```
interface Gi0/0
no switchport
ip address 192.168.69.2 255.255.255.0
```

```
interface Gi0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

```
interface Gi0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

```
interface Gi0/3
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

```
interface vlan 10
ip address 192.168.10.1 255.255.255.0
exit
```

```
interface vlan 20
ip address 192.168.20.1 255.255.255.0
exit
```

```
interface vlan 30
ip address 192.168.30.1 255.255.255.0
exit
ip routing

end
wr
```

On peut alors installer et configurer des services **DHCP**, **FTP**, **HTTP** et **SSH** sur des serveurs (virtualisés) de l'infrastructure réseau (ce qui explique notre choix des Debian 11.8) :

Voici comment on configure et valide notre service DHCP opérationnel :

On commence par installer le paquet “isc-dhcp-server” puis modifier le fichier /etc/network/interfaces afin de permettre l’attribution des adresses statiques pour chaque VLAN sur le serveur DHCP :

```
# VLAN 10
auto ens4.10
iface ens4.10 inet static
    address 192.168.10.1
    netmask 255.255.255.0
    vlan-raw-device ens4

# VLAN 20
auto ens4.20
iface ens4.20 inet static
    address 192.168.20.1
    netmask 255.255.255.0
    vlan-raw-device ens4

# VLAN 30
auto ens4.30
iface ens4.30 inet static
    address 192.168.30.1
    netmask 255.255.255.0
    vlan-raw-device ens4
```

Puis on modifie le fichier /etc/dhcp/dhcpd.conf pour créer le pool DHCP pour chaque VLAN :

```
GNU nano 5.4                               /etc/dhcp/dhcpd.conf *
# VLAN 10
subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.100 192.168.10.200;
    option routers 192.168.10.2;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
}

# VLAN 20
subnet 192.168.20.0 netmask 255.255.255.0 {
    range 192.168.20.100 192.168.20.200;
    option routers 192.168.20.2;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
}

# VLAN 30
subnet 192.168.30.0 netmask 255.255.255.0 {
    range 192.168.30.100 192.168.30.200;
    option routers 192.168.30.2;
```

Puis on configure le fichier /etc/default/isc-dhcp-server pour activer notre service DHCP sur les bonnes interfaces :

```
GNU nano 5.4                               /etc/default/isc-dhcp-server
Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDV4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDV6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDV4_PID=/var/run/dhcpcd.pid
#DHCPDV6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens4 ens4.10 ens4.20 ens4.30"
INTERFACESv6=""
```

Et on peut vérifier que notre service DHCP fonctionne correctement :

```
debian@debian:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - LSB: DHCP server
  Loaded: loaded (/etc/init.d/isc-dhcp-server; generated)
  Active: active (running) since Fri 2024-06-14 07:05:05 UTC; 1min 13s ago
    Docs: man:systemd-sysv-generator(8)
      Tasks: 1 (limit: 1905)
     Memory: 1.0M
        CPU: 0.000 CPU seconds total (idle)
          CPU: 0.000% user + 0.000% system
          CPU: 0.000% idle
```

Voici donc les sous-interfaces prises en compte par le serveur DHCP :

```
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0c:b9:55:a5:00:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet6 fe80::eb9:55ff:fea5:0/64 scope link
        valid_lft forever preferred_lft forever
3: ens4.10@ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 0c:b9:55:a5:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/24 brd 192.168.10.255 scope global ens4.10
        valid_lft forever preferred_lft forever
    inet6 fe80::eb9:55ff:fea5:0/64 scope link
        valid_lft forever preferred_lft forever
4: ens4.20@ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 0c:b9:55:a5:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.1/24 brd 192.168.20.255 scope global ens4.20
        valid_lft forever preferred_lft forever
    inet6 fe80::eb9:55ff:fea5:0/64 scope link
        valid_lft forever preferred_lft forever
5: ens4.30@ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 0c:b9:55:a5:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.1/24 brd 192.168.30.255 scope global ens4.30
        valid_lft forever preferred_lft forever
    inet6 fe80::eb9:55ff:fea5:0/64 scope link
        valid_lft forever preferred_lft forever
debian@debian:~/$
```

Et plus rien ne devrait empêcher notre serveur DHCP d'offrir des adresses IP aux PCs (On effectuer un test sur le VLAN 10) :

Une requête sur le PC1 suffit pour que le serveur DHCP lui offre l'adresse IP 192.168.10.100/24 :

```
PC1> ip dhcp  
DORA IP 192.168.10.100/24 GW 192.168.10.2  
  
PC1> show ip  
  
NAME : PC1[1]  
IP/MASK : 192.168.10.100/24  
GATEWAY : 192.168.10.2  
DNS : 8.8.8.8 8.8.4.4  
DHCP SERVER : 192.168.10.1  
DHCP LEASE : 447, 451/225/394  
DOMAIN NAME : example.org  
MAC : 00:50:79:66:68:00  
LPORT : 10006  
RHOST:PORT : 127.0.0.1:10007  
MTU: : 1500
```

Idem pour le PC4 qui obtient l'adresse IP 192.168.10.101/24 :

```
PC4> ip dhcp
DORA IP 192.168.10.101/24 GW 192.168.10.2

PC4> show ip

NAME      : PC4[1]
IP/MASK   : 192.168.10.101/24
GATEWAY   : 192.168.10.2
DNS       : 8.8.8.8  8.8.4.4
DHCP SERVER : 192.168.10.1
DHCP LEASE  : 594, 600/300/525
DOMAIN NAME : example.org
MAC        : 00:50:79:66:68:03
LPORT      : 10012
RHOST:PORT : 127.0.0.1:10013
MTU:       : 1500
```

Et la connectivité se fait bel et bien entre les machines du même réseau :

```
PC4> ping 192.168.10.100
84 bytes from 192.168.10.100 icmp_seq=1 ttl=64 time=5.414 ms
84 bytes from 192.168.10.100 icmp_seq=2 ttl=64 time=5.306 ms
84 bytes from 192.168.10.100 icmp_seq=3 ttl=64 time=5.859 ms
84 bytes from 192.168.10.100 icmp_seq=4 ttl=64 time=10.412 ms
84 bytes from 192.168.10.100 icmp_seq=5 ttl=64 time=8.654 ms
```

Le précédent test était un test de connection intra-VLAN (puisque le PC1 et le PC4 font parti du même VLAN) alors effectuons à présent un test de connection inter-VLAN :

Une requête sur le PC2 suffit pour que le serveur DHCP lui offre l'adresse IP 192.168.20.101/24 :

```
PC2> ip dhcp
DORA IP 192.168.20.101/24 GW 192.168.20.2

PC2> ping 192.168.10.100
192.168.10.100 icmp_seq=1 timeout
192.168.10.100 icmp_seq=2 timeout
84 bytes from 192.168.10.100 icmp_seq=3 ttl=63 time=5.889 ms
84 bytes from 192.168.10.100 icmp_seq=4 ttl=63 time=4.730 ms
84 bytes from 192.168.10.100 icmp_seq=5 ttl=63 time=6.881 ms
```

Au passage, voici des informations supplémentaires sur le PC2 :

```
PC2> show ip

NAME      : PC2[1]
IP/MASK   : 192.168.20.101/24
GATEWAY   : 192.168.20.2
DNS        : 8.8.8.8  8.8.4.4
DHCP SERVER : 192.168.20.1
DHCP LEASE  : 555, 600/300/525
DOMAIN NAME : example.org
MAC        : 00:50:79:66:68:01
LPORT      : 10008
RHOST:PORT : 127.0.0.1:10009
MTU:       : 1500
```

On a donc un DHCP opérationnel, attaquons la suite...

Voici comment on configure et valide notre service FTP opérationnel :

On commence par installer le paquet “vsftpd” qui, parmi tout les choix de serveurs FTP, est un des plus populaires car réputé pour sa sécurité (d'où le “vs” dans son nom pour “Very Secure”) :

```
debian@debian:~$ sudo apt install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 31 not upgraded.
Need to get 153 kB of archives.
After this operation, 358 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 vsftpd amd64 3.0.3-12+b1 [153 kB]
Fetched 153 kB in 1s (140 kB/s)
Preconfiguring packages ...
```

On peut alors configurer le fichier de configuration principal de vsftpd qui est vsftpd.conf :

```
GNU nano 5.4                               /etc/vsftpd.conf
listen=YES
anonymous_enable=NO
local_enable=YES
ftp_banner=Bienvenue !

# Permettre aux utilisateurs d'écrire dans le répertoire
write_enable=YES

chroot_local_user=NO
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list

# Limiter les utilisateurs à leur répertoire personnel
chroot_local_user=YES
allow_writeable_chroot=YES

# Permettre les uploads anonymes (désactivé, mais utile à mentionner)
#anon_upload_enable=NO

# Spécifier le répertoire partagé
# Permettre les uploads anonymes (désactivé, mais utile à mentionner)
#anon_upload_enable=NO

# Spécifier le répertoire partagé
local_root=/srv/ftp/shared

# Activer la création de fichiers avec les permissions du groupe
file_open_mode=0770

# Permettre la création de nouveaux fichiers et répertoires
local_umask=007
```

Puis créer le dossier de partage :

```
debian@debian:~$ sudo mkdir -p /srv/ftp/shared
```

On peut alors créer les utilisateurs de notre service FTP avec ici un exemple de création de l'utilisateur ftpuser2 (la même chose est faite pour ftpuser1) :

```
debian@debian:~$ sudo adduser ftpuser2
Adding user `ftpuser2' ...
Adding new group `ftpuser2' (1003) ...
Adding new user `ftpuser2' (1003) with group `ftpuser2'
Creating home directory `/home/ftpuser2' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ftpuser2
Enter the new value, or press ENTER for the default
      Full Name []:
      Room Number []:
      Work Phone []:
      Home Phone []:
      Other []:
Is the information correct? [Y/n]
debian@debian:~$
```

On peut alors créer le groupe d'utilisateurs du service FTP nommé ftpaccess :

```
debian@debian:~$ sudo groupadd ftpaccess
```

Avant d'y insérer les deux utilisateurs préalablement créés :

```
debian@debian:~$ sudo usermod -aG ftpaccess ftpuser1
debian@debian:~$ sudo usermod -aG ftpaccess ftpuser2
```

Il faut également que le dossier de partage appartienne au groupe des utilisateurs du service FTP :

```
debian@debian:~$ sudo chgrp ftpaccess /srv/ftp/shared
debian@debian:~$ sudo chmod 770 /srv/ftp/shared
```

Il n'y a donc plus aucune raison que les différents utilisateurs du service FTP ne puisse l'utiliser :

Ici l'utilisateur ftpuser1 partage le fichier test4 :

```
ftp> put test4
local: test4 remote: test4
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp> ls -l
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwx--- 1 1002 1002 0 Jun 14 10:17 test
-rwxrwx--- 1 1003 1003 0 Jun 14 10:25 test2
-rwxrwx--- 1 1002 1002 0 Jun 14 10:41 test3
-rwxrwx--- 1 1002 1002 0 Jun 14 10:48 test4
226 Directory send OK.
```

Et l'utilisateur ftpuser2 le récupère correctement :

```
ftp> get test4
local: test4 remote: test4
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for test4 (0 bytes).
226 Transfer complete.
ftp> █
```

On peut donc dire que le fichier test4 a été transféré avec succès.

On a donc un FTP opérationnel, attaquons la suite...

[Voici comment on configure et valide notre service HTTP opérationnel :](#)

On commence par installer le paquet “apache2” puis démarrer le service :

```
debian@debian:/var/www$ sudo systemctl start apache2
```

Un service fonctionnant correctement :

```
debian@debian:/var/www$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
  Active: active (running) since Fri 2024-06-14 06:20:08 UTC; 1h 46min ago
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 351 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUC>
 Main PID: 371 (apache2)
   Tasks: 55 (limit: 546)
  Memory: 7.4M
     CPU: 872ms
    CGroup: /system.slice/apache2.service
            └─371 /usr/sbin/apache2 -k start
              ├─374 /usr/sbin/apache2 -k start
              ├─375 /usr/sbin/apache2 -k start

Jun 14 06:20:06 debian systemd[1]: Starting The Apache HTTP Server...
Jun 14 06:20:08 debian apachectl[365]: AH00558: apache2: Could not reliably det>
Jun 14 06:20:08 debian systemd[1]: Started The Apache HTTP Server.
lines 1-17/17 (END)
```

On édite alors le fichier 000-default.conf afin de modifier la racine du serveur web qui sera donc sae201.com. Le répertoire racine du site web, est celui où le serveur Apache cherchera les fichiers lorsqu'il recevra une requête HTTP :

```
GNU nano 5.4                               000-default.conf *
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port t>
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/sae201.com

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log

    ^G Help      ^O Write Out  ^W Where Is  ^K Cut      ^T Execute  ^C Location
    ^X Exit      ^R Read File  ^\ Replace   ^U Paste    ^J Justify  ^_ Go To Line
```

Il faut également changer les droits du répertoire sae201.com pour que le serveur Web ait les autorisations d'accès au répertoire et ce qu'il contient, c'est faisable de cette manière :

```
debian@debian:/etc/apache2/sites-available$ sudo chown -R www-data:www-data /var/www/sae201.com
debian@debian:/etc/apache2/sites-available$ sudo chmod -R 755 /var/www/sae201.com
```

On peut alors créer un fichier index.html dans le répertoire sae201.com :

```
GNU nano 5.4                               index.html *
<!DOCTYPE html>
<html>
<head>
    <title>SAE201</title>
</head>
<body>
    <h1>Serveur Web de la SAE201</h1>
    <p>Bienvenue sur notre site !</p>
</body>
</html>
```

Les tests du services HTTP sont effectués une fois pfSense appliqué à toute l'infrastructure.

On a donc un HTTP opérationnel, attaquons la suite...

Voici comment on configure et valide notre service SSH opérationnel :

On commence par installer les paquets pour faire fonctionner notre serveur SSH :

```
debian@debian:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libcbor0
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libcbor0.8 libfido2-1 libssl3 openssh-client openssh-sftp-server
  runit-helper
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard ufw
Recommended packages:
  xauth ncurses-term
The following NEW packages will be installed:
  libcbor0.8 libssl3
The following packages will be upgraded:
  libfido2-1 openssh-client openssh-server openssh-sftp-server runit-helper
5 upgraded, 2 newly installed, 0 to remove and 272 not upgraded.
Need to get 3641 kB of archives.
After this operation, 8278 kB of additional disk space will be used.
Do you want to continue? [Y/n] 
```

Puis les paquets pour faire fonctionner nos clients ssh :

```
debian@debian:~$ sudo apt install openssh-client
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-client is already the newest version (1:8.4p1-5+deb11u3).
openssh-client set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 31 not upgraded.
```

Après cela on active la fonction Permitrootlogin pour que le compte root puisse connecter directement via SSH :

```
GNU nano 5.4                               /etc/ssh/sshd_config
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Les tests du services SSH sont effectués une fois pfSense appliqué à toute l'infrastructure.

On a donc un SSH opérationnel, attaquons la suite...

Configuration de pfSense

On commence par configurer les adresses ip des interfaces du routeur pfSense :

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.69.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0     = 16
      255.0.0.0       = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Et voilà donc nos interfaces configurées :

```
from: 192.168.69.2

FreeBSD/amd64 (pfensesae201.iut.re) (ttyv0)

QEMU Guest - Netgate Device ID: 3ae45b5af40eba2a1276

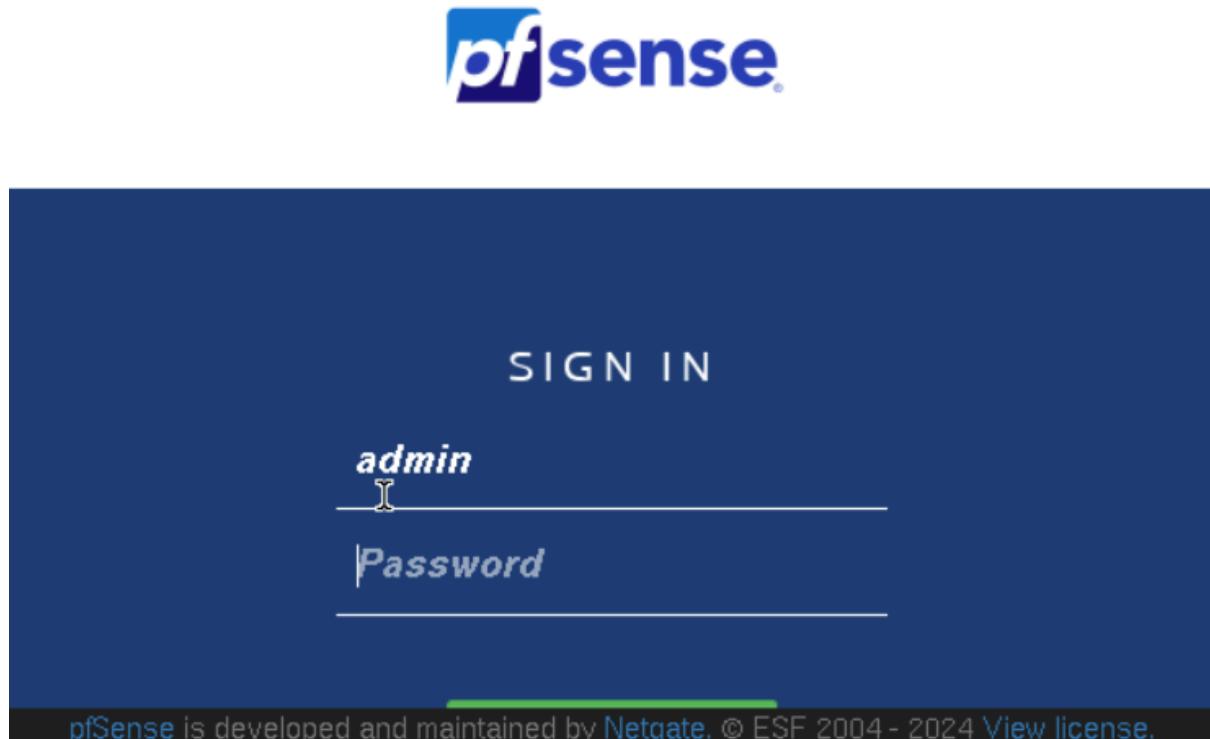
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfensesae201 ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.122.19/24
LAN (lan)      -> em1          -> v4: 192.168.69.1/24
DMZ (opt1)     -> em2          -> v4: 192.168.1.1/24

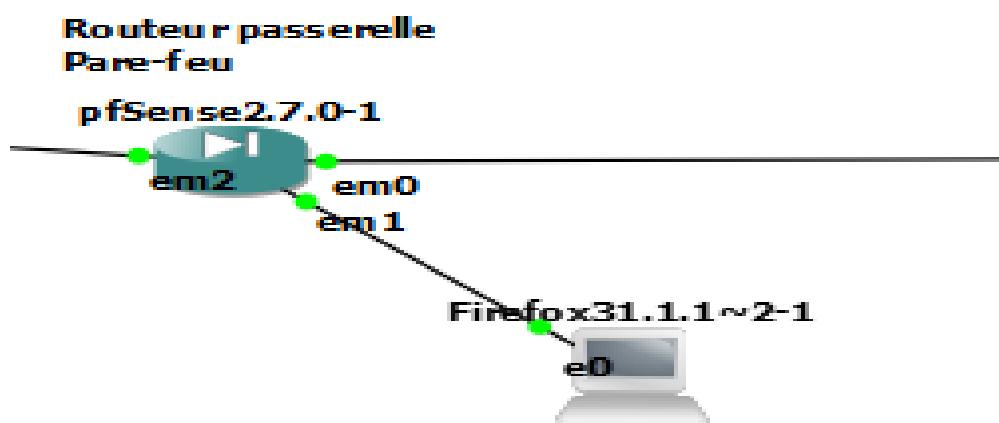
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: ■
```

On peut à présent configurer pfSense graphiquement :



On décide de configurer graphiquement pfSense depuis l'interface LAN afin de faciliter cette tâche :



Voici donc le commencement de la configuration de pfSense où l'on définit les différents paramètres de notre pare feu et autres :

General Information

On this screen the general pfSense parameters will be set.

Hostname

Name of the firewall host, without domain part.

Examples: pfSense, firewall, edgefw

Domain

Domain name for the firewall.

Examples: home.arpa. example.com

Time Server Information

Please enter the time, date and time zone.

Time server hostname

Enter the hostname (FQDN) of the time server.

Timezone

>> Next

Wizard: pfSense Setup: Configure WAN Interface - Mozilla Firefox Step 4 of 9

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

Selected Type

DHCP

General configuration

MAC Address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following field.

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address

192.168.69.1

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

24

>> Next

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

» Next

Reload configuration 

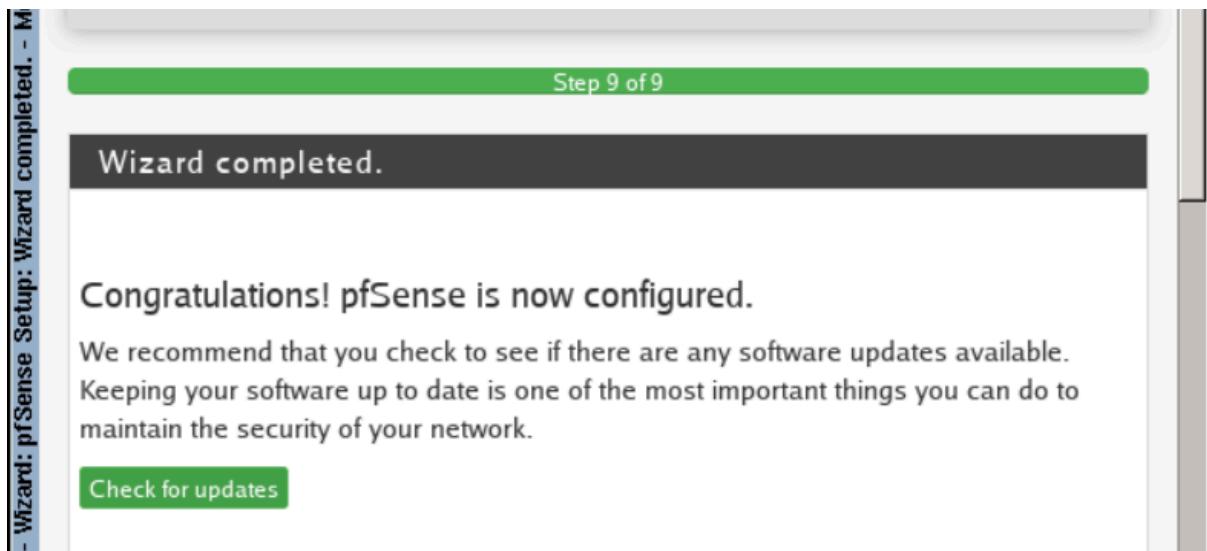
Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

» Reload 

Et voici donc notre pare feu configuré :



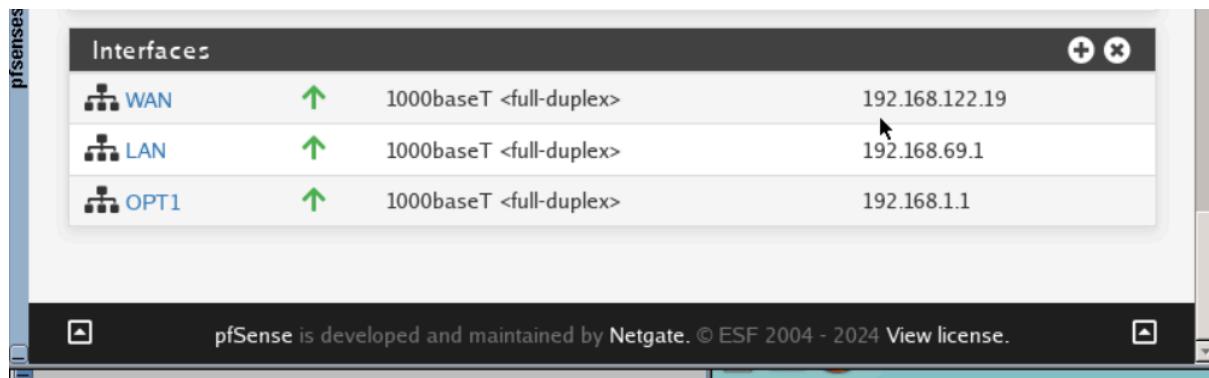
On arrive donc sur cette page affichant des informations sur notre configuration :

The screenshot shows the pfSense Status / Dashboard page. At the top, it says "Status / Dashboard" with a "+" and a question mark icon. Below that is a "System Information" section with the following details:

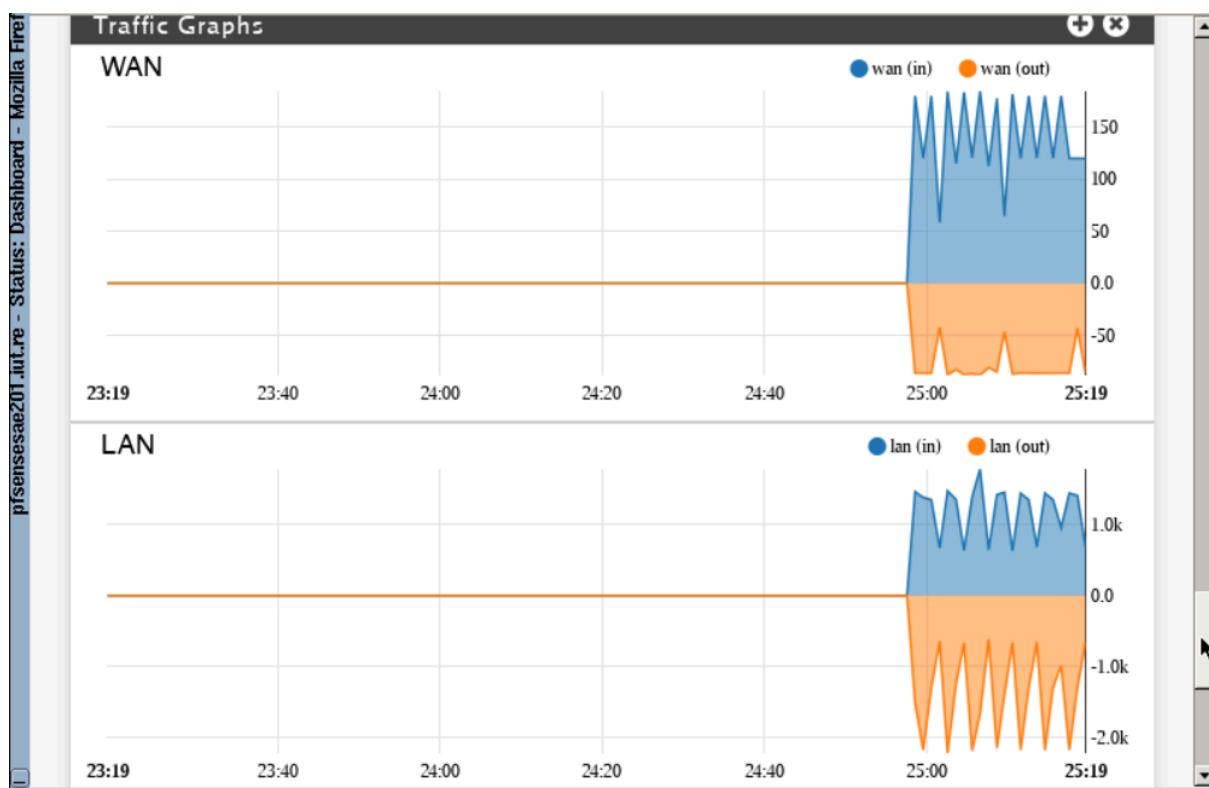
Name	pfsensesae201.iut.re
User	admin@192.168.69.2 (Local Database)
System	QEMU Guest Netgate Device ID: 3ae45b5af40eba2a1276
BIOS	Vendor: SeaBIOS Version: 1.13.0-1ubuntu1.1 Release Date: Tue Apr 1 2014
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT

At the bottom of the dashboard, it says "Version 2.7.2 is available." with a download icon, and "Version information updated at Fri Jun 14 15:09:40 +04 2024" with a refresh icon.

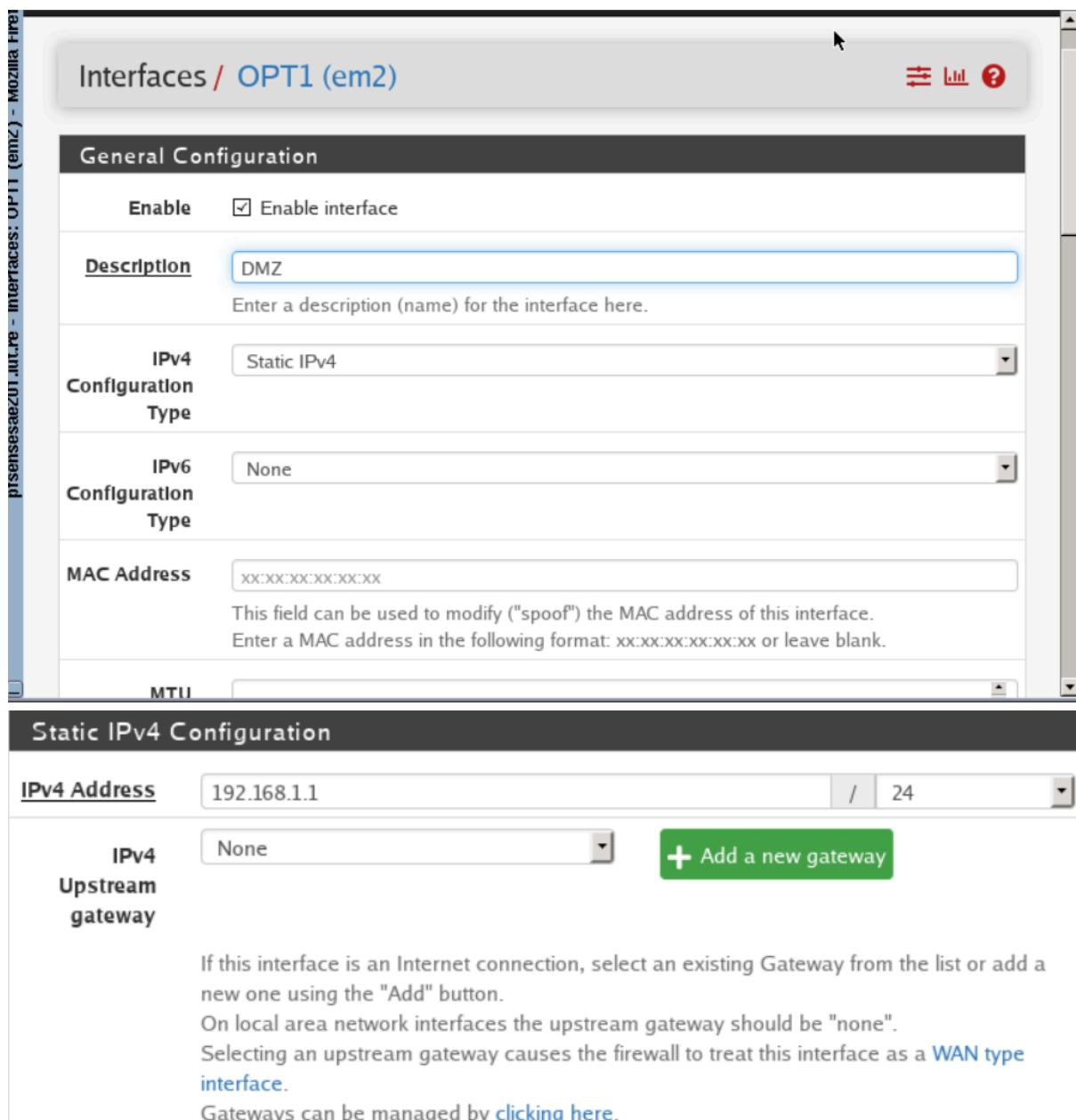
On peut également accéder à des informations sur nos interfaces :



On ajoute le widget Traffic graph pour afficher l'activité de chaque réseaux :



Et on peut à présent débuter la configuration de la DMZ :



The screenshot shows a web-based interface for configuring a network interface. The top bar indicates the interface is **OPT1 (em2)**. The main configuration screen is titled **General Configuration**.

General Configuration:

- Enable:** Enable interface
- Description:** DMZ
- IPv4 Configuration Type:** Static IPv4
- IPv6 Configuration Type:** None
- MAC Address:** XXXX:XXXX:XXXX:XXXX
- MTU:** [Input field]

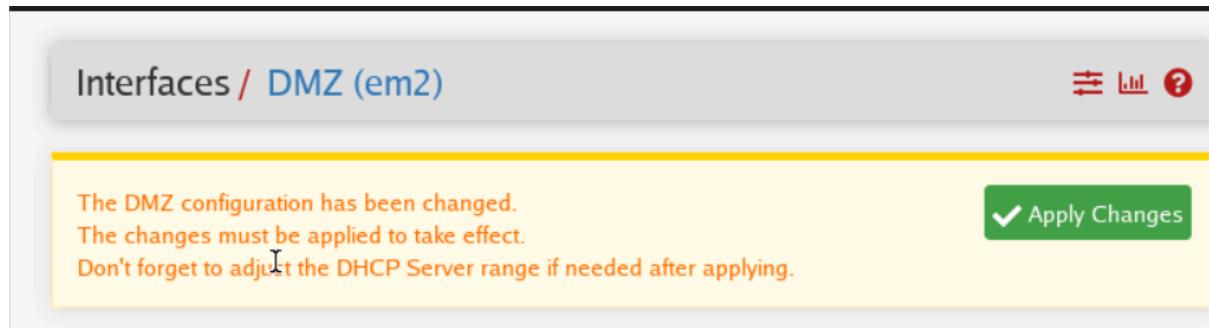
Static IPv4 Configuration:

- IPv4 Address:** 192.168.1.1 / 24
- IPv4 Upstream gateway:** None
- Add a new gateway:** [Green button with plus sign]

Below the configuration sections, there is descriptive text:

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
 On local area network interfaces the upstream gateway should be "none".
 Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**.
 Gateways can be managed by [clicking here](#).

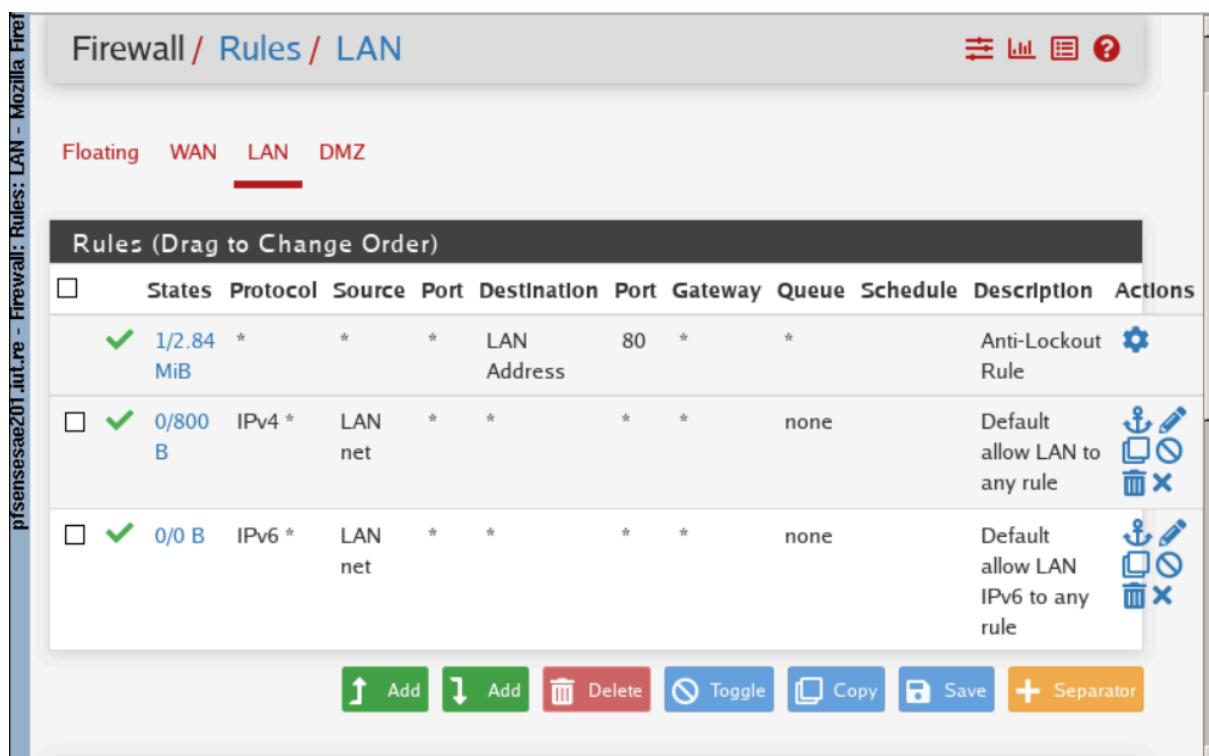
Configuration sauvegardée et appliquée :



The DMZ configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

Apply Changes

On peut donc attaquer la configuration des règles du pare feu selon l'interface, ici le LAN est configuré pour accéder à tous les réseaux :



Firewall / Rules / LAN

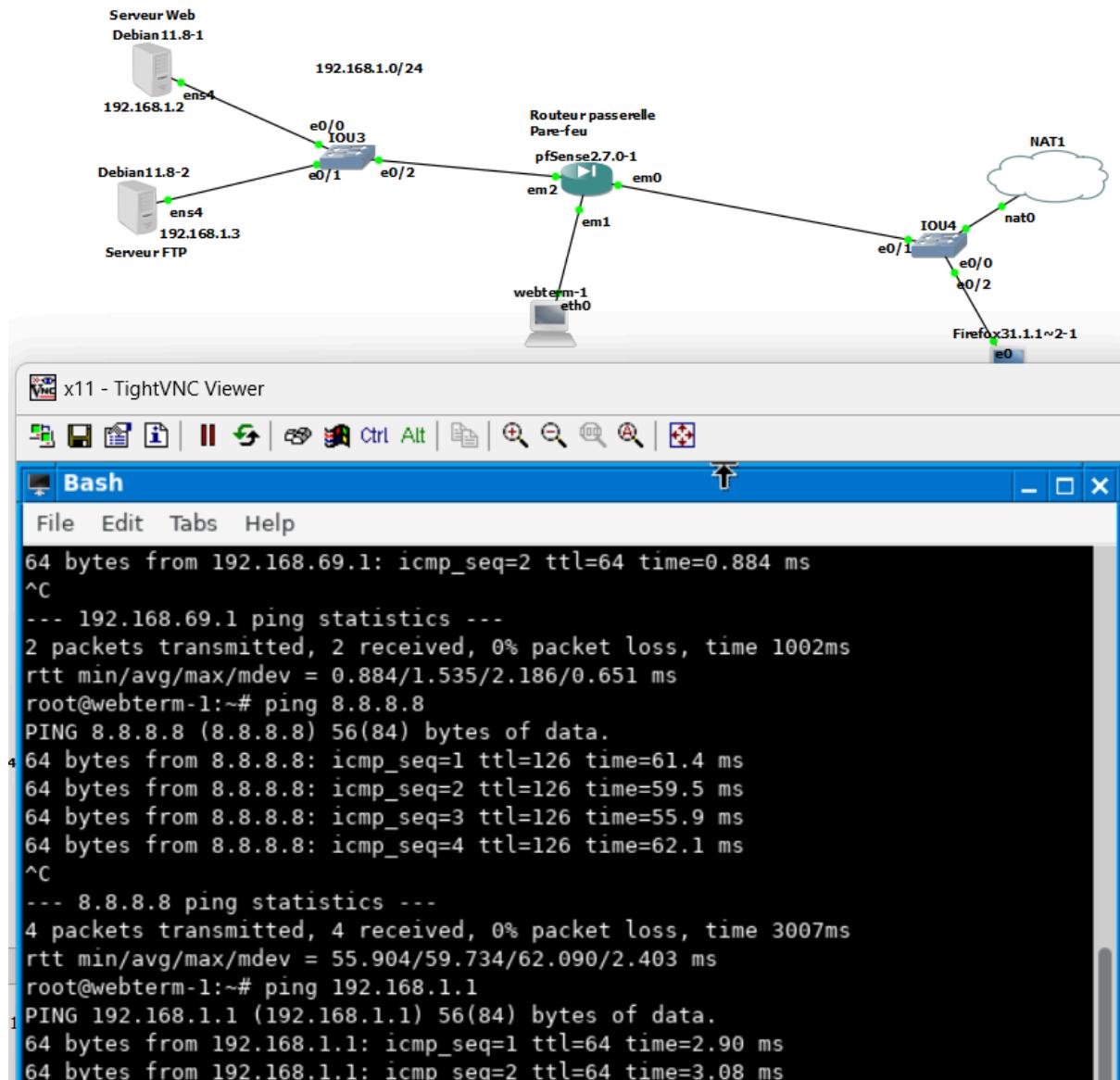
Floating WAN LAN DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/2.84 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 0/800 B	IPv4	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Up Add Down Delete Toggle Copy Save Separator

Et voici des pings du LAN qui est bel et bien autorisée à se connecter à toutes les machines (LAN qui est représenté par la machine reliée par em1) :



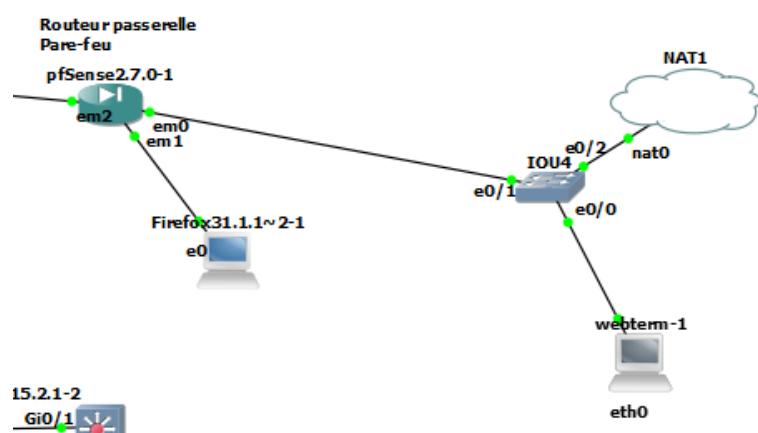
Et voici un test de connectivité de la DMZ qui n'est donc pas autorisée à accéder à internet sans les règles :

```
debian@debian:/home$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^Xc^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4088ms
```

On peut donc configurer des règle sur la DMZ qui n'en a pas pour le moment :



On effectue donc des modifications dans la topologie pour faire des test entre le NAT, la DMZ et le LAN :



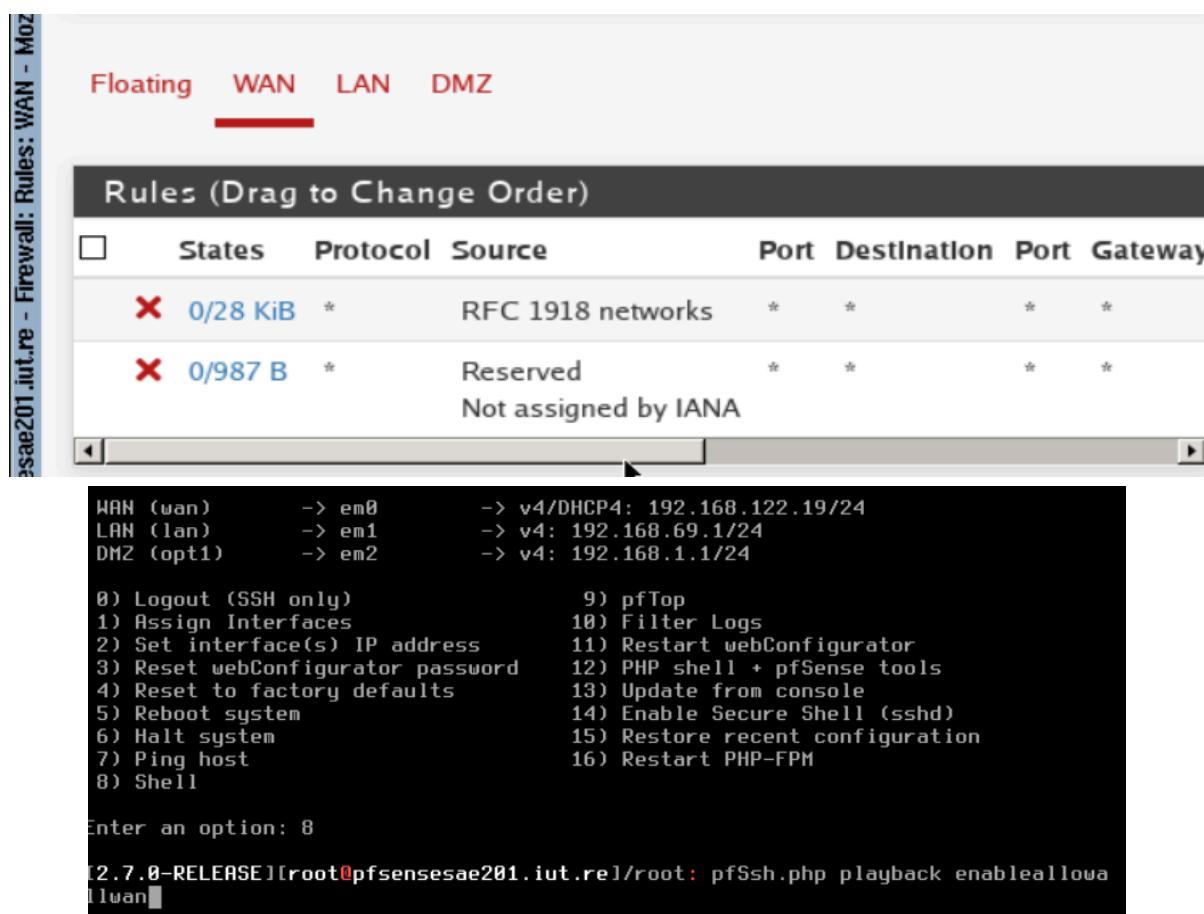
Voici donc une machine du WAN tentant de ping l'interface routeur WAN depuis le WAN :

```
15: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether b6:dc:4d:e3:7d:e3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.126/24 brd 192.168.122.255 scope global eth0
        valid_lft forever preferred_lft forever
root@webterm-1:~#
```

Interfaces			
	WAN	↑ 1000baseT <full-duplex>	192.168.122.19
File Edit Tabs Help			

```
root@webterm-1:~# ping 192.168.122.19
PING 192.168.122.19 (192.168.122.19) 56(84) bytes of data.
```

On va modifier les règles du WAN pour que le WAN puisse accéder à la DMZ :



Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway
✗	0/28 KiB	*	RFC 1918 networks	*	*	*	*
✗	0/987 B	*	Reserved	*	*	*	*
Not assigned by IANA							

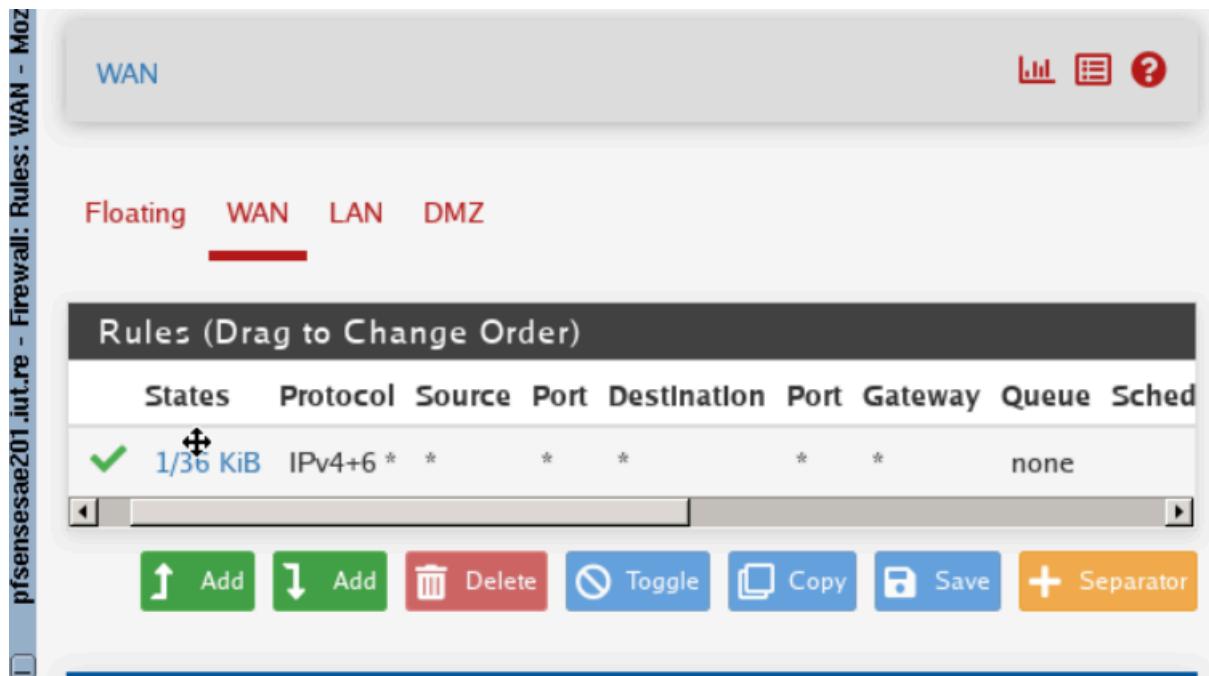
WAN (wan) → em0 → v4/DHCP4: 192.168.122.19/24
 LAN (lan) → em1 → v4: 192.168.69.1/24
 DMZ (opt1) → em2 → v4: 192.168.1.1/24

0) Logout (SSH only) 9) pfTop
 1) Assign Interfaces 10) Filter Logs
 2) Set interface(s) IP address 11) Restart webConfigurator
 3) Reset webConfigurator password 12) PHP shell + pfSense tools
 4) Reset to factory defaults 13) Update from console
 5) Reboot system 14) Enable Secure Shell (sshd)
 6) Halt system 15) Restore recent configuration
 7) Ping host 16) Restart PHP-FPM
 8) Shell

Enter an option: 8

```
[2.7.0-RELEASE][root@pfsensesae201.iut.re]/root: pfSsh.php playback enableallowwan
```

Et donc on obtient après la commande :



The screenshot shows the 'WAN' tab in the pfSense Firewall Rules interface. At the top, there are tabs for Floating, WAN, LAN, and DMZ, with 'WAN' selected. Below the tabs is a table titled 'Rules (Drag to Change Order)' with columns: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, and Sched. One rule is listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Sched
✓ 1/36 KiB	IPv4+6	*	*	*	*	*	*	none

At the bottom of the interface are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

On peut à présent accéder à l'interface WAN du routeur pfSense depuis le NAT :

```
root@webterm-1:~# ping 192.168.122.19
PING 192.168.122.19 (192.168.122.19) 56(84) bytes of data.
64 bytes from 192.168.122.19: icmp_seq=1 ttl=64 time=1.69 ms
64 bytes from 192.168.122.19: icmp_seq=2 ttl=64 time=0.955 ms
64 bytes from 192.168.122.19: icmp_seq=3 ttl=64 time=0.641 ms
```

On va configurer les services de la DMZ pour que le WAN y accède.

On configure le paramètre NAT du Pare feu pour ajouter lesdits services :

HTTP

From port

Custom

HTTP

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Single host

Type

192.168.1.2

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope (::1)

Redirect target port

HTTP

Destination

Invert match.

WAN address

Type

/ 31

Address/mask

Destination port range

HTTP

From port

Custom

HTTP

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Single host

Et voici l'ajout des règles :

The screenshot shows the pfSense Firewall configuration interface. The left sidebar contains the following navigation items:

- System
- Interfaces
- Firewall** (highlighted)
- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper

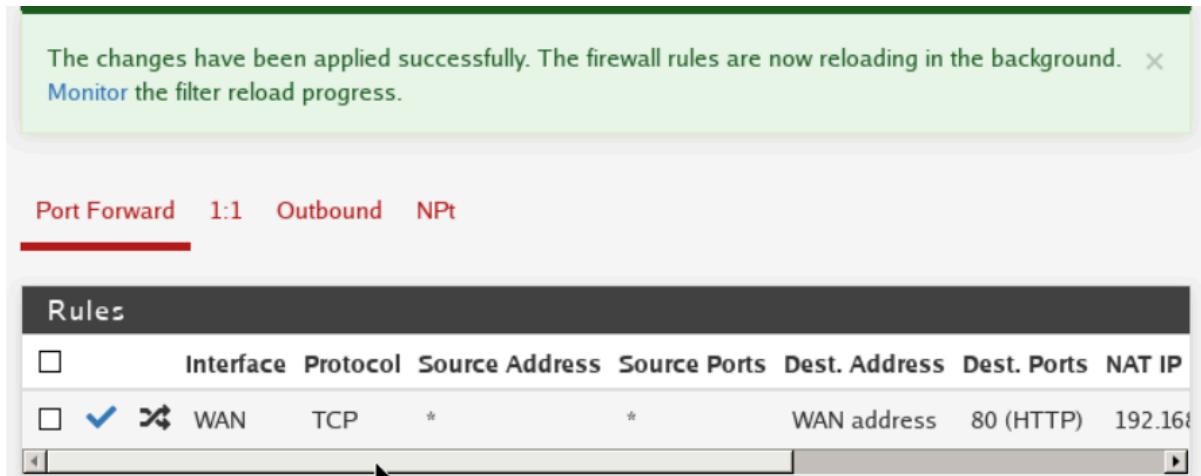
The screenshot shows the pfSense NAT configuration interface. The browser address bar indicates the URL is `192.168.69.1/firewall_nat.php`. A message box at the top states: "The NAT configuration has been changed. The changes must be applied for them to take effect." with a green "Apply Changes" button.

The main table displays the following NAT rule:

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP
WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.1.2

Below the table are several action buttons: Add, Add, Delete, Toggle, Save, and Separator.

Nos configurations sont bel et bien sauvegardées :



The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor the filter reload progress.](#)

Port Forward 1:1 Outbound NPt

Rules

<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.1.1

Et le WAN peut donc accéder à la DMZ :

```
root@webterm-1:~# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=127 time=8.70 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=127 time=9.59 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=127 time=9.65 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=127 time=11.0 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=127 time=8.96 ms
```

Le protocole HTTP est donc fonctionnel depuis le NAT vers la DMZ :



On peut donc faire la même chose que le HTTP pour le FTP :

Destination port range

FTP

From port

Custom

FTP

To port

Destination

Invert match.

WAN address

Type

/ 31

Address/mask

Destination port range

FTP

From port

Custom

FTP

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Single host

Type

Redirect target IP

Type: Single host
Value: 192.168.1.3

Address

Enter the internal IP address of the server on which to map the ports. e.g.:
192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope
(::1)

Redirect target port

Type: Other
Value: 21

Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

On sauvegarde nos configurations :

pfSense
COMMUNITY EDITION

Port Forward

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Port Forward **1:1** **Outbound** **NPt**

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports
WAN	TCP	*	*	WAN address	21 (FTP)
WAN	TCP	*	*	WAN address	80 (HTTP)

Actions:

Et on peut alors tester le ftp depuis le WAN (NAT) :

```
root@webterm-1:~# apt install ftp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  tnftp
The following NEW packages will be installed:
  ftp tnftp
0 upgraded, 2 newly installed, 0 to remove and 1 not upgraded.
Need to get 166 kB of archives.
After this operation, 319 kB of additional disk space will be used.
Do you want to continue? [Y/n] ■
```

```
root@webterm-1:~# ftp 192.168.122.19
Connected to 192.168.122.19.
220 Bienvenue !
Name (192.168.122.19:root): ftpuser1
331 Please specify the password.
Password: ■
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
```

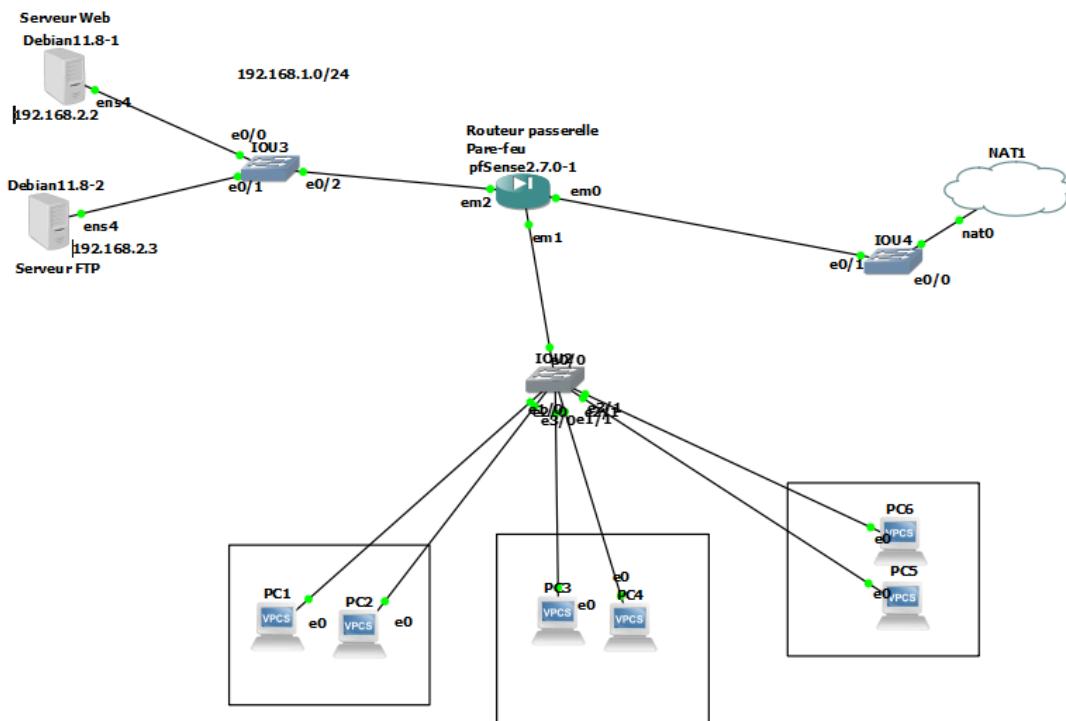
Voici les vérification du fonctionnement de ftp sur la machine NAT :

```
ftp> ls -l
229 Entering Extended Passive Mode (|||29378|)
150 Here comes the directory listing.
-rwxrwx--- 1 1002 1004 0 Jun 14 10:17 test
-rwxrwx--- 1 1003 1004 0 Jun 14 10:25 test2
-rwxrwx--- 1 1002 1004 0 Jun 14 10:41 test3
-rwxrwx--- 1 1002 1004 0 Jun 14 10:48 test4
226 Directory send OK.
ftp> ■
```

On peut à présent configurer les routes du switch vers les différents réseaux via pfSense :

```
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.69.1
Switch(config)#■
```

On fait également le choix de passer à la nouvelle topologie proposée pour la SAE qui est également autorisée :



Voici donc la configuration du switch de niveau 2 :

```

enable
configure terminal
vlan 10
name DIRECTION
exit
vlan 20
name GESTION
exit
vlan 30
name COMTECH
exit

interface range G1/0-3
switchport mode access
switchport access vlan 10
exit

interface range G2/0-3
switchport mode access
switchport access vlan 20
exit

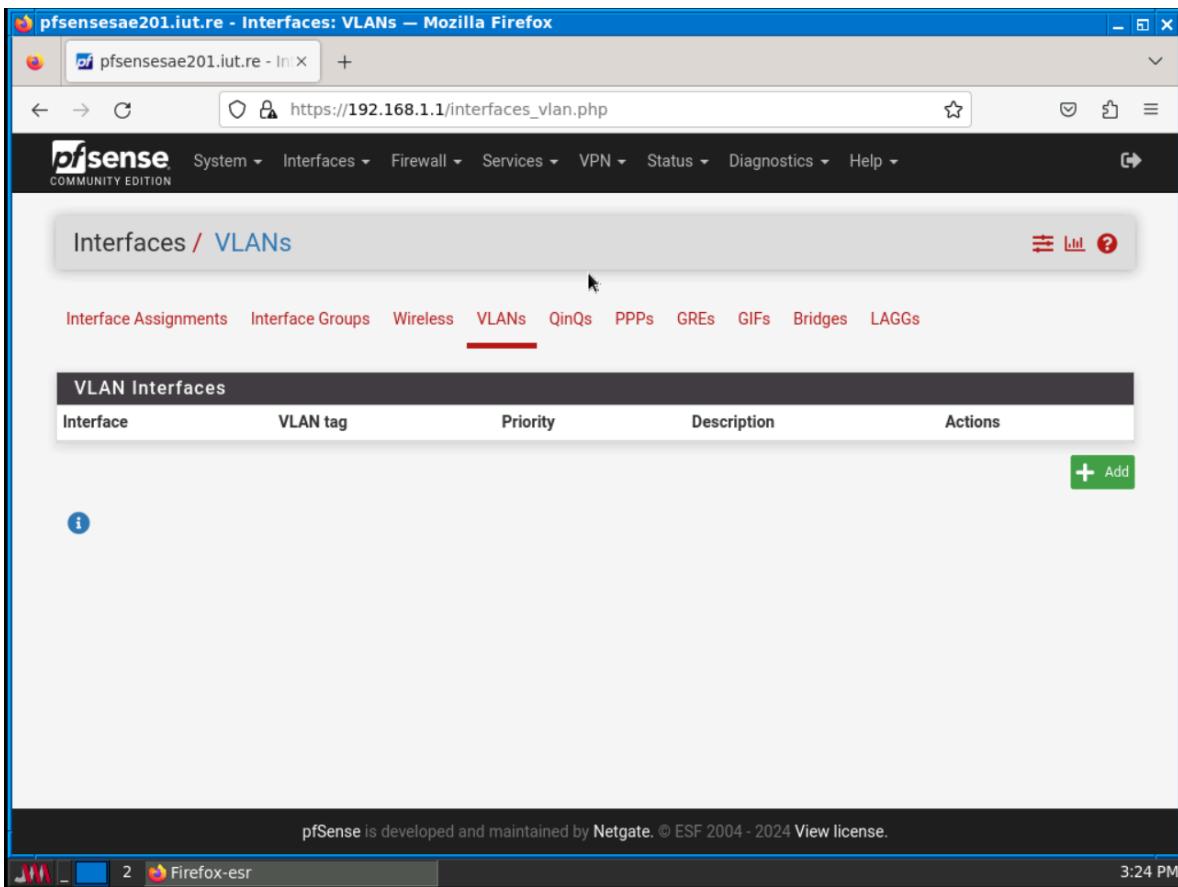
interface range G3/0-3
switchport mode access

```

```
switchport access vlan 30
exit
```

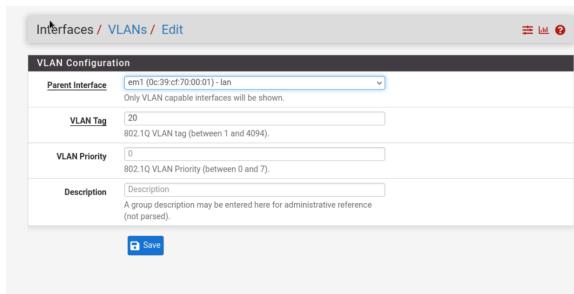
```
interface G0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20,30
exit
```

On peut donc configurer pfsense (vlan) en branchant un pc directement sur le pfsense :



The screenshot shows the pfSense web interface with the URL https://192.168.1.1/interfaces_vlan.php. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main title is "Interfaces / VLANs". Below it, a sub-navigation bar has "VLANs" selected. A table titled "VLAN Interfaces" lists columns for Interface, VLAN tag, Priority, Description, and Actions. A green "Add" button is visible at the bottom right of the table area. The footer of the browser window shows "2:24 PM" and the Firefox icon.

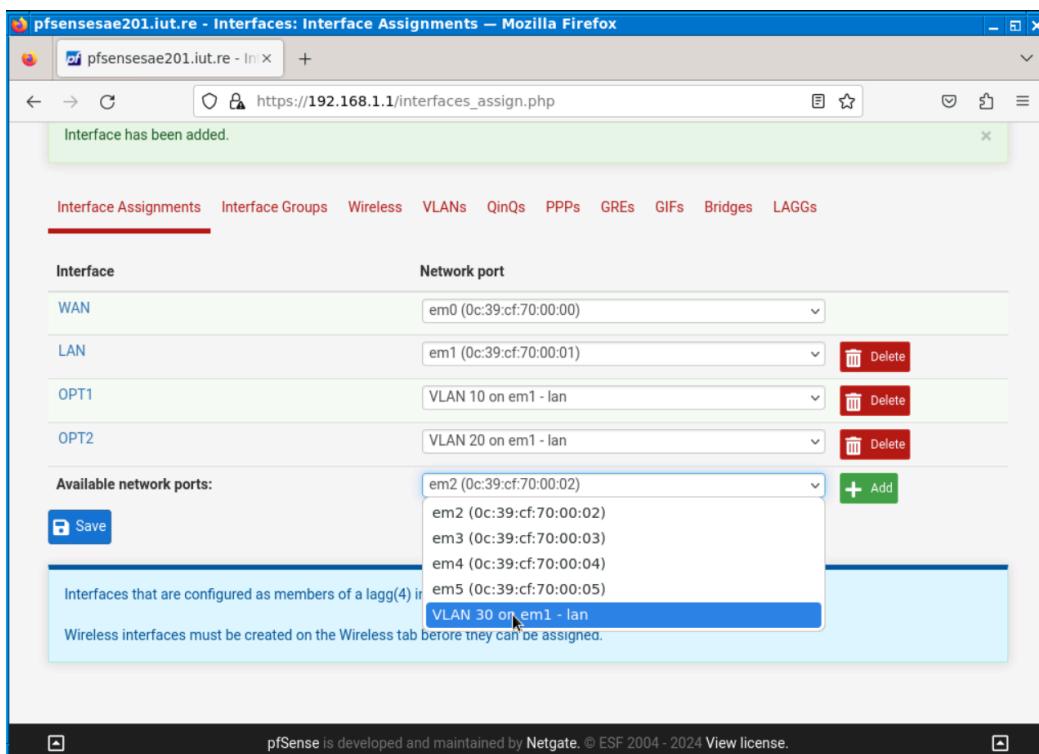
On peut donc ajouter les VLAN dans pfsense, avec comme exemple ci-dessous le VLAN 20 :



The screenshot shows the "VLAN Configuration" edit screen. It includes fields for Parent Interface (set to "em1"), VLAN Tag (set to 20), VLAN Priority (set to 0), and a Description field containing the note "A group description may be entered here for administrative reference (not parsed)". A blue "Save" button is located at the bottom of the form.

On ajoute ensuite les interfaces, chose faite pour tous les VLAN ainsi que la DMZ, voici un petit avant-après pour des configurations :

AVANT



pfensesae201.iut.re - Interfaces: Interface Assignments – Mozilla Firefox

Interface has been added.

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (0c:39:cf:70:00:00)
LAN	em1 (0c:39:cf:70:00:01)
OPT1	VLAN 10 on em1 - lan
OPT2	VLAN 20 on em1 - lan

Available network ports:

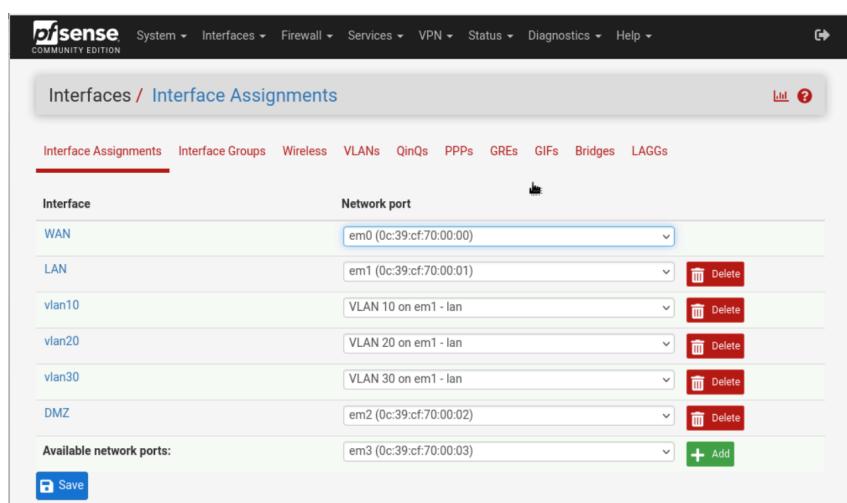
- em2 (0c:39:cf:70:00:02)
- em3 (0c:39:cf:70:00:03)
- em4 (0c:39:cf:70:00:04)
- em5 (0c:39:cf:70:00:05)
- VLAN 30 on em1 - lan

Save

Interfaces that are configured as members of a lagg(4) in Wireless interfaces must be created on the Wireless tab before they can be assigned.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 [View license](#).

APRÈS



pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (0c:39:cf:70:00:00)
LAN	em1 (0c:39:cf:70:00:01)
vlan10	VLAN 10 on em1 - lan
vlan20	VLAN 20 on em1 - lan
vlan30	VLAN 30 on em1 - lan
DMZ	em2 (0c:39:cf:70:00:02)

Available network ports:

- em3 (0c:39:cf:70:00:03)

Save

On peut alors adresser les interfaces pour les trois VLAN, en commençant par le VLAN 10 :

General Configuration

IPv4 Configuration Type: Static IPv4

MAC Address

MTU

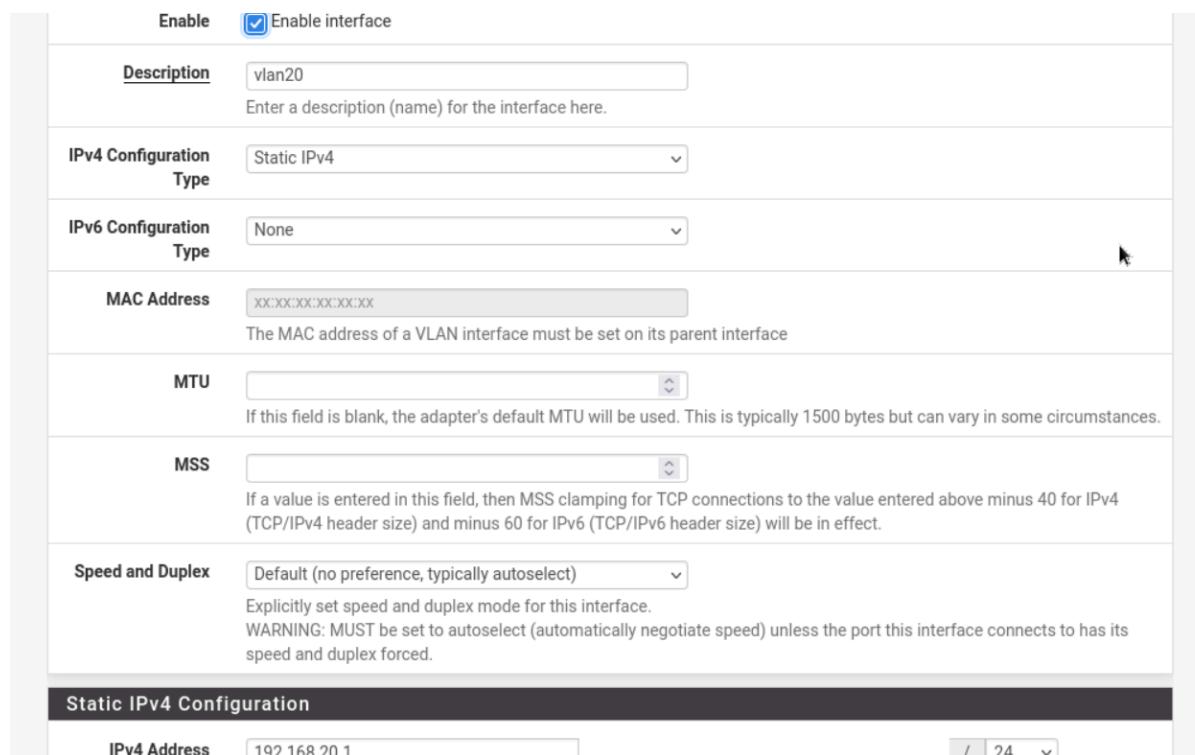
MSS

Static IPv4 Configuration

IPv4 Address: 192.168.10.1 / 32

IPv4 Upstream gateway: None

Puis le VLAN 20 :



Enable Enable interface

Description vlan20
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address XX:XX:XX:XX:XX:XX
The MAC address of a VLAN interface must be set on its parent interface

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

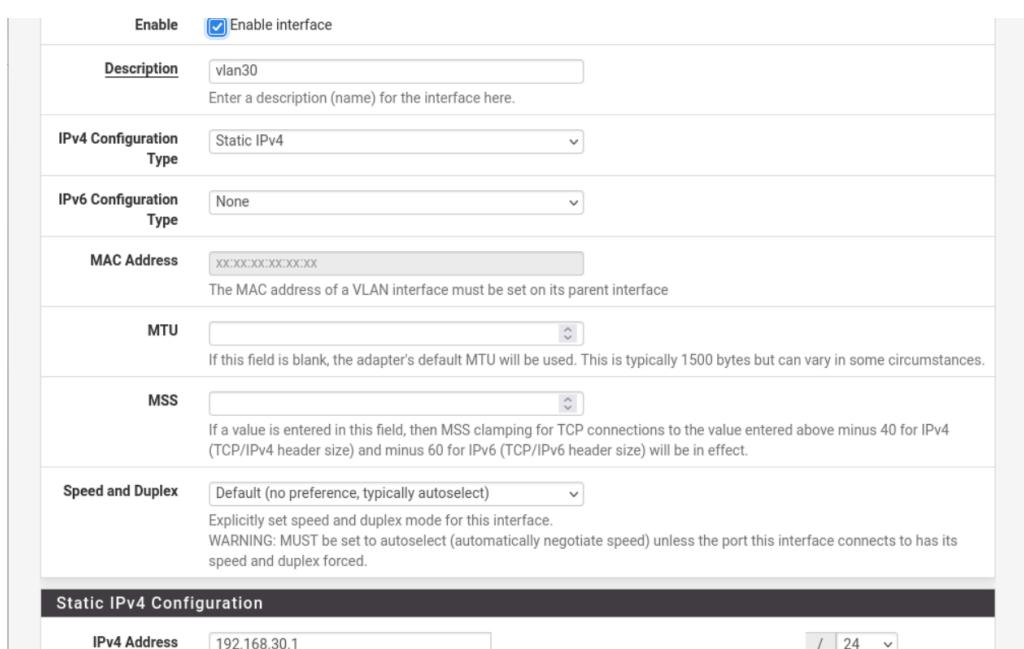
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address 192.168.20.1 / 24

Puis le VLAN 30 :



Enable Enable interface

Description vlan30
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address XX:XX:XX:XX:XX:XX
The MAC address of a VLAN interface must be set on its parent interface

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

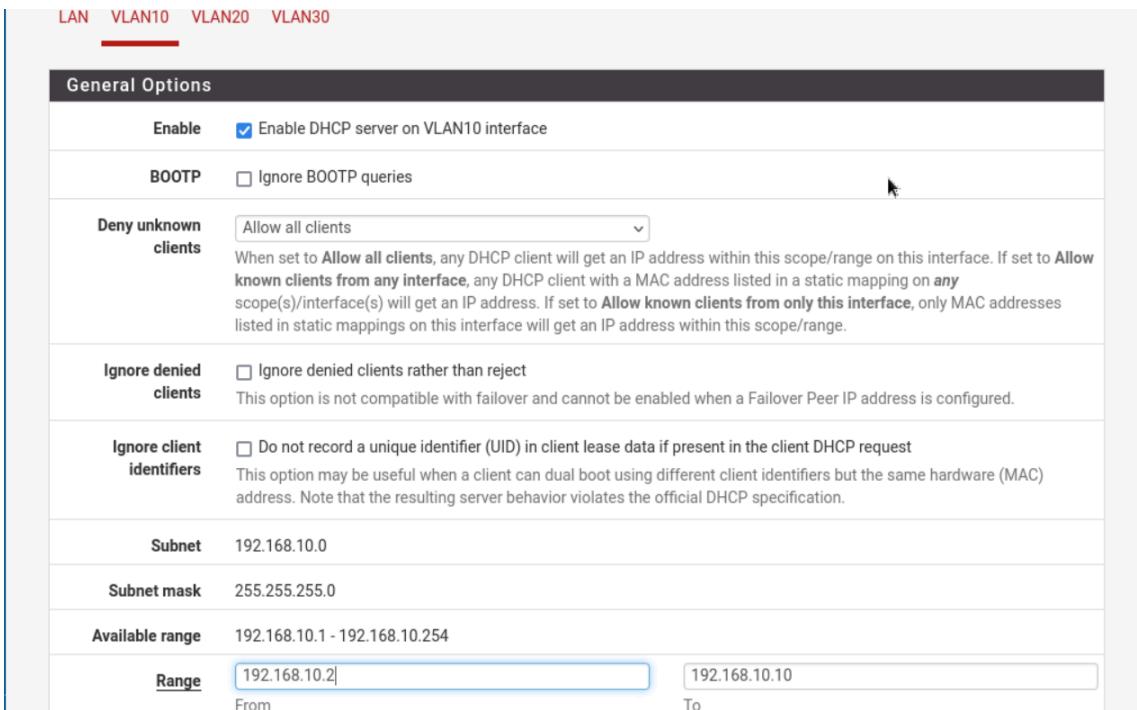
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address 192.168.30.1 / 24

Puis on configure DHCP pour les trois VLAN en commençant par le VLAN 10 :



General Options

Enable Enable DHCP server on VLAN10 interface

BOOTP Ignore BOOTP queries

Deny unknown clients Allow all clients
 When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore denied clients Ignore denied clients rather than reject
 This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
 This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

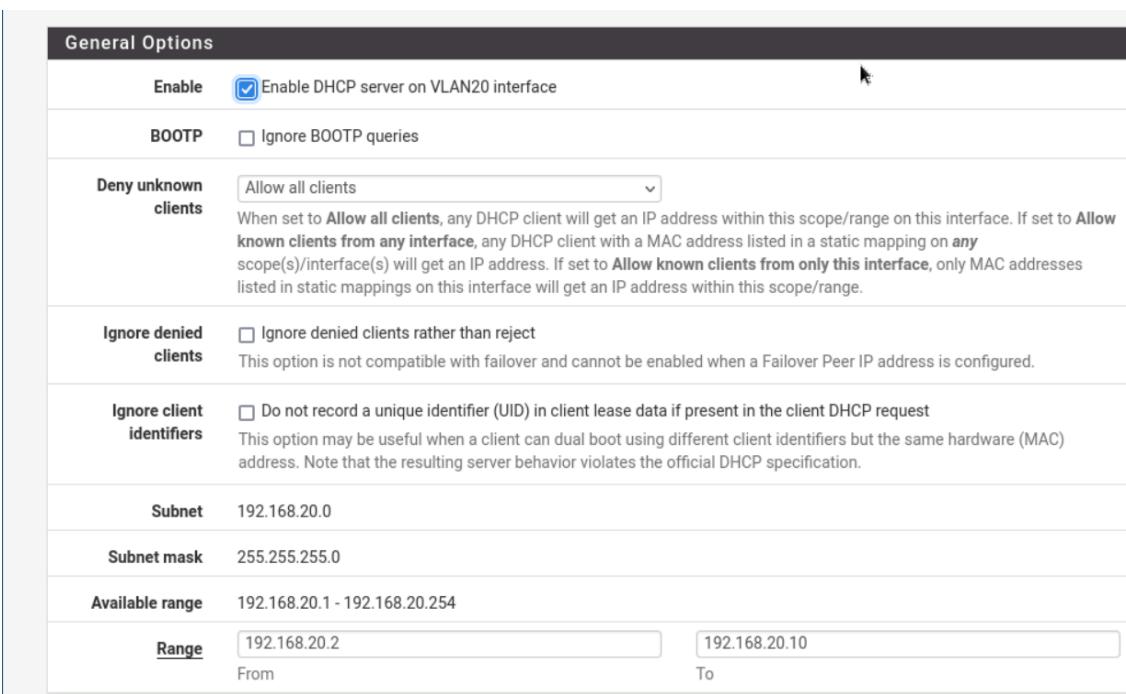
Subnet 192.168.10.0

Subnet mask 255.255.255.0

Available range 192.168.10.1 - 192.168.10.254

Range From 192.168.10.2 To 192.168.10.10

Puis le VLAN 20 :



General Options

Enable Enable DHCP server on VLAN20 interface

BOOTP Ignore BOOTP queries

Deny unknown clients Allow all clients
 When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore denied clients Ignore denied clients rather than reject
 This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
 This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 192.168.20.0

Subnet mask 255.255.255.0

Available range 192.168.20.1 - 192.168.20.254

Range From 192.168.20.2 To 192.168.20.10

Puis le VLAN 30 :

General Options		
Enable	<input checked="" type="checkbox"/> Enable DHCP server on VLAN30 interface	
BOOTP	<input type="checkbox"/> Ignore BOOTP queries	
Deny unknown clients	<input type="button" value="Allow all clients"/> <small>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</small>	
Ignore denied clients	<input type="checkbox"/> Ignore denied clients rather than reject <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>	
Ignore client identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request <small>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.</small>	
Subnet	192.168.30.0	
Subnet mask	255.255.255.0	
Available range	192.168.30.1 - 192.168.30.254	
Range	<input type="text" value="192.168.30.2"/> From	<input type="text" value="192.168.30.10"/> To

Et le DHCP est bien fonctionnel sur les PCs :

```
PC1> ip dhcp
DDORA IP 192.168.10.2/24 GW 192.168.10.1

PC1>
```

Et on peut tester la connectivité inter-VLAN :

```
PC2> ip dhcp
DDORA IP 192.168.20.2/24 GW 192.168.20.1

PC2> ping 192.168.10.2
192.168.10.2 icmp_seq=1 timeout
192.168.10.2 icmp_seq=2 timeout
84 bytes from 192.168.10.2 icmp_seq=3 ttl=63 time=4.263 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=63 time=4.317 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=63 time=3.750 ms
```

On fait configurer à présent les règles pour les VLAN 10, 20 et 30 sur le pare feu (avec ici l'exemple du 10) :

Edit Firewall Rule

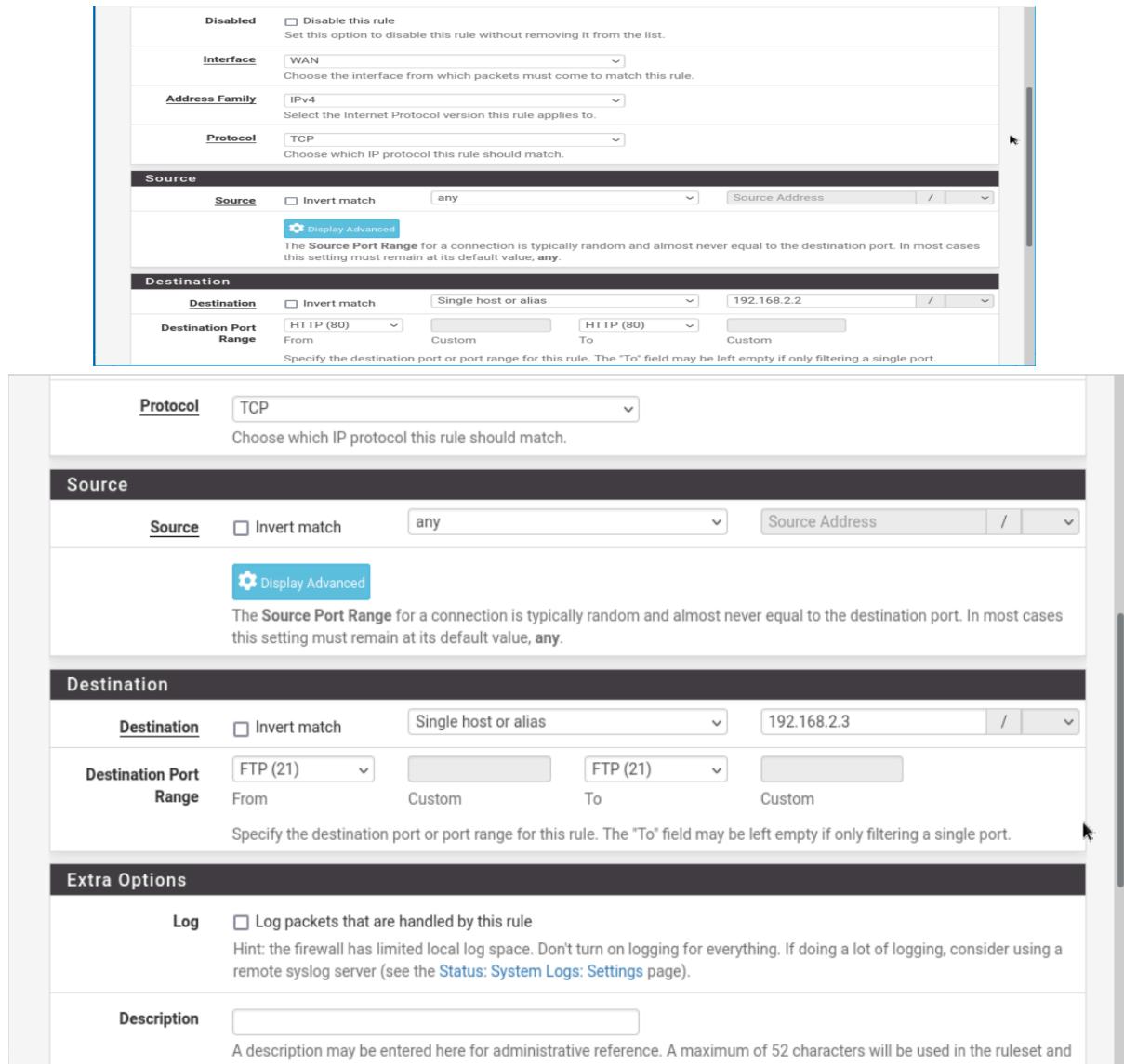
Action	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	VLAN10	Choose the interface from which packets must come to match this rule.
Address Family	IPv4	Select the Internet Protocol version this rule applies to.
Protocol	Any	Choose which IP protocol this rule should match.
Source		
Source	<input type="checkbox"/> Invert match	any
Source Address /		
Destination		
Destination	<input type="checkbox"/> Invert match	any
Destination Address /		
Extra Options		

Puis on configure les règles du WAN pour qu'il accède à la DMZ :

```
[2.7.0-RELEASE][root@pfsensesae201.iut.re]# pfSsh.php playback enableallowallwan
Adding allow all rule...
Turning off block private networks (if on)...
Turning off block bogon networks (if on)...
Reloading the filter configuration...
```

Et brièvement, voici les configurations pour chacun de nos services :

Voici les configurations pour notre service FTP :



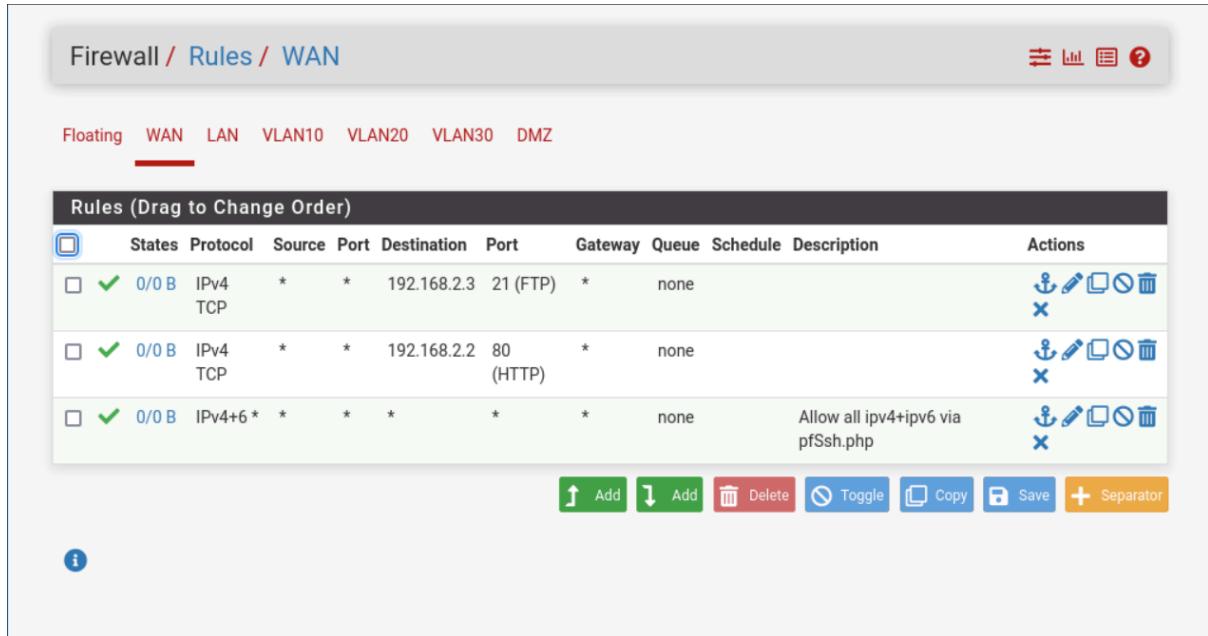
Rule 1 (Top Window):

- Disabled:** Disable this rule
- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP
- Source:** Source: Invert match any, Destination: Single host or alias 192.168.2.2
- Destination:** Destination: Invert match Single host or alias 192.168.2.2, Destination Port Range: From HTTP (80) To HTTP (80)

Rule 2 (Bottom Window):

- Protocol:** TCP
- Source:** Source: Invert match any, Destination: Single host or alias 192.168.2.3
- Destination:** Destination: Invert match Single host or alias 192.168.2.3, Destination Port Range: From FTP (21) To FTP (21)
- Extra Options:** Log: Log packets that are handled by this rule
- Description:** A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and

Et voici donc les configurations :

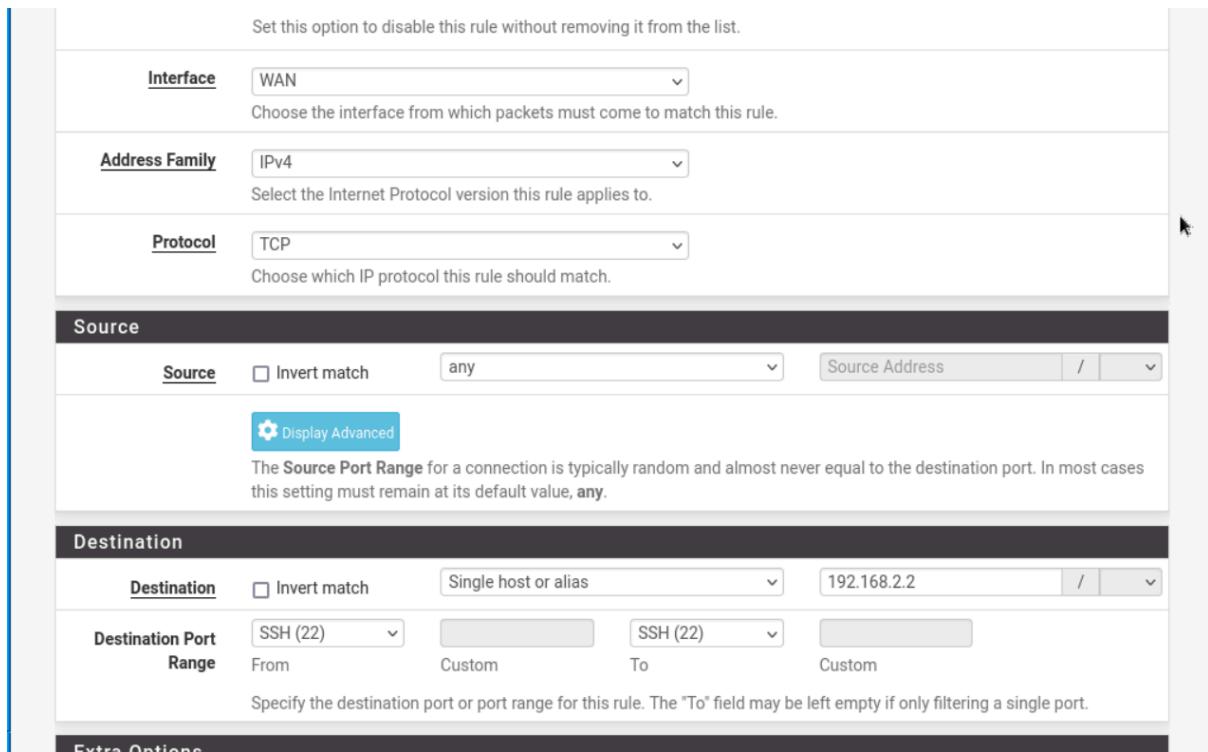


The screenshot shows a 'Firewall / Rules / WAN' interface. The top navigation bar includes tabs for Floating, WAN, LAN, VLAN10, VLAN20, VLAN30, and DMZ. The 'WAN' tab is selected. Below the tabs is a table titled 'Rules (Drag to Change Order)'. The table has columns for序号 (Index), States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are three rules listed:

序号	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1	0/0 B	IPv4 TCP	*	*	192.168.2.3	21 (FTP)	*	none			
2	0/0 B	IPv4 TCP	*	*	192.168.2.2	80 (HTTP)	*	none			
3	0/0 B	IPv4+6	*	*	*	*	*	none		Allow all ipv4+ipv6 via pfSsh.php	

At the bottom of the table are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Et voici les règles SSH pour les différents serveur en commençant par le serveur HTTP :



The screenshot shows a detailed configuration for a specific rule. At the top, there is a note: "Set this option to disable this rule without removing it from the list." Below this are dropdown menus for Interface (WAN), Address Family (IPv4), and Protocol (TCP). Each dropdown has a descriptive note below it: "Choose the interface from which packets must come to match this rule.", "Select the Internet Protocol version this rule applies to.", and "Choose which IP protocol this rule should match." Below these settings is a section titled "Source". It contains a "Source" field with an "Invert match" checkbox and a dropdown menu set to "any". To the right of this are dropdown menus for "Source Address" and a separator. A "Display Advanced" button is visible. A note below the source fields states: "The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any." Below the source section is a "Destination" section. It contains a "Destination" field with an "Invert match" checkbox and a dropdown menu set to "Single host or alias". To the right of this are dropdown menus for "Destination Address" and a separator. A "Destination Port Range" field is present, with "From" set to "SSH (22)", "Custom", "To" set to "SSH (22)", and "Custom". A note below the destination fields states: "Specify the destination port or port range for this rule. The 'To' field may be left empty if only filtering a single port." At the bottom of the configuration area is a "Extra Options" section.

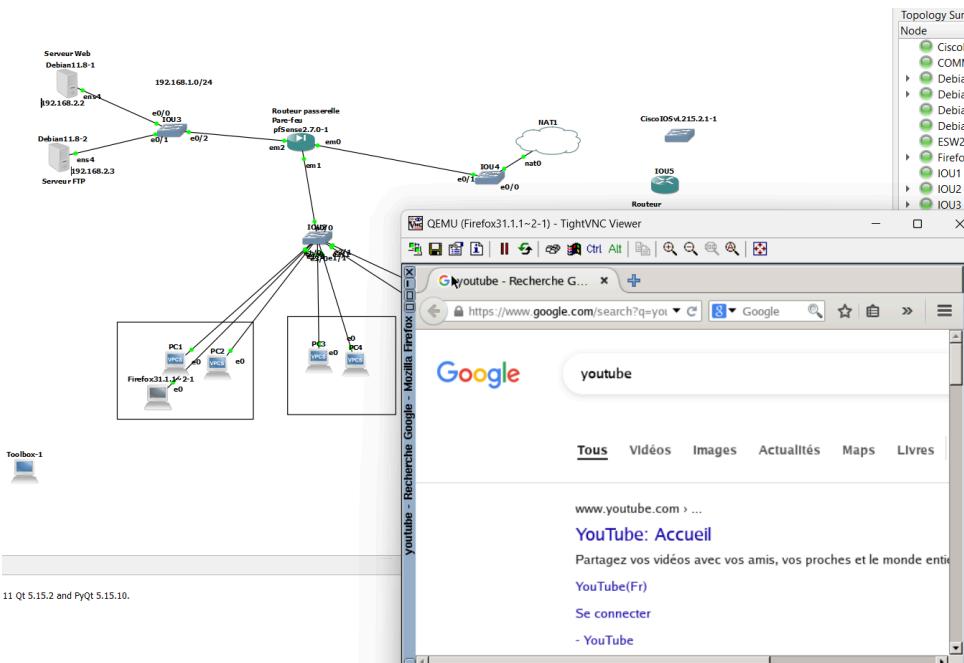
Puis le serveur FTP :

The screenshot shows a list of firewall rules for the 'LAN' interface. There are five rules listed:

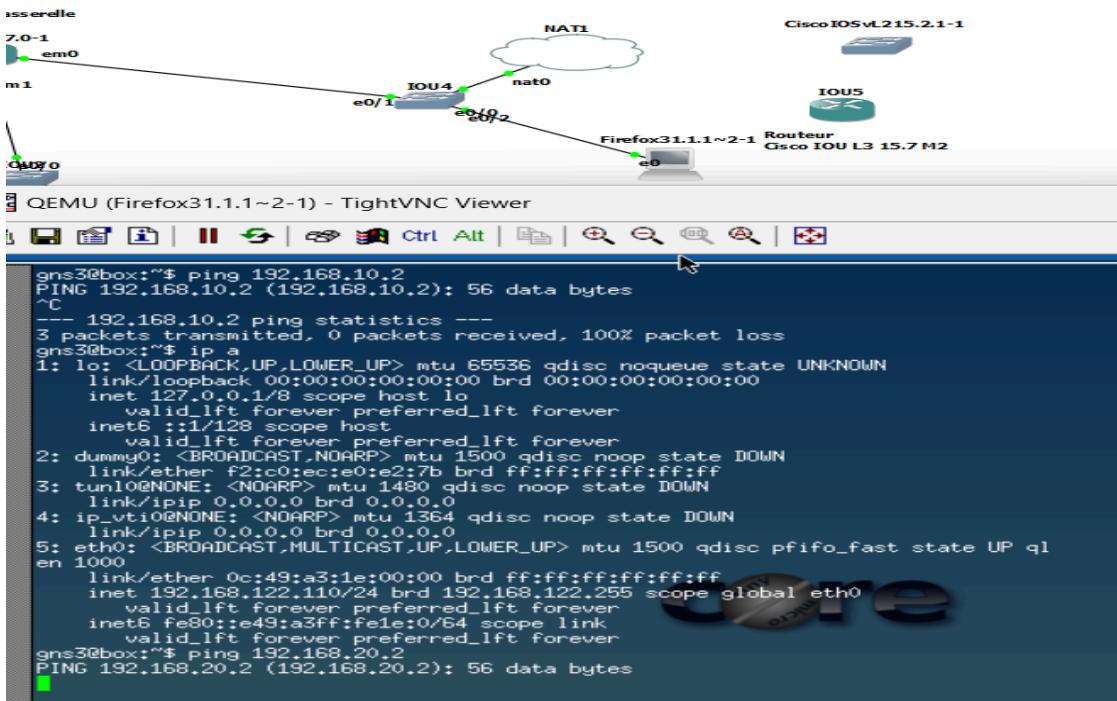
Index	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0	B	IPv4 TCP	*	*	192.168.2.3	22 (SSH)	*		none		Edit Delete
0/0	B	IPv4 TCP	*	*	192.168.2.2	22 (SSH)	*		none		Edit Delete
0/0	B	IPv4 TCP	*	*	192.168.2.3	21 (FTP)	*		none		Edit Delete
0/0	B	IPv4 TCP	*	*	192.168.2.2	80 (HTTP)	*		none		Edit Delete
0/1	KIB	IPv4+6	*	*	*	*	*	*	none	Allow all ipv4+ipv6 via pfSsh.php	Edit Delete

Buttons at the bottom include: [Add](#), [Delete](#), [Toggle](#), [Copy](#), [Save](#), and [Separator](#).

On peut alors effectuer les tests pour un PC du VLAN :

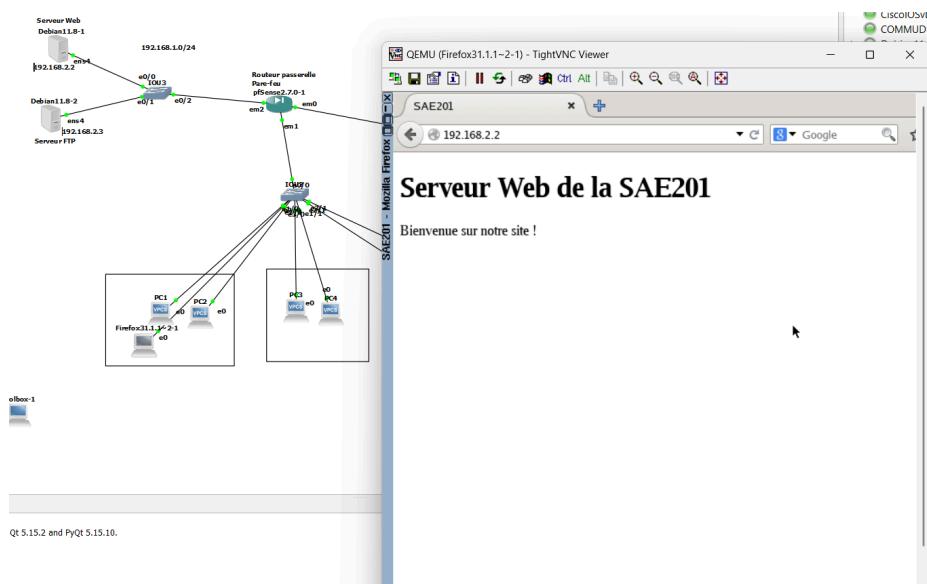


Et voici un test de connectivité du WAN vers le LAN :



Un échec logique et espéré car le WAN ne doit pas accéder au LAN !

On peut à présent vérifier qu'un utilisateur interne à l'entreprise peut accéder aux services réseaux installés soit Web et FTP (au moyen d'un objet webterm ou Firefox à la place d'un VPCS : Virtual PC Simulator) :

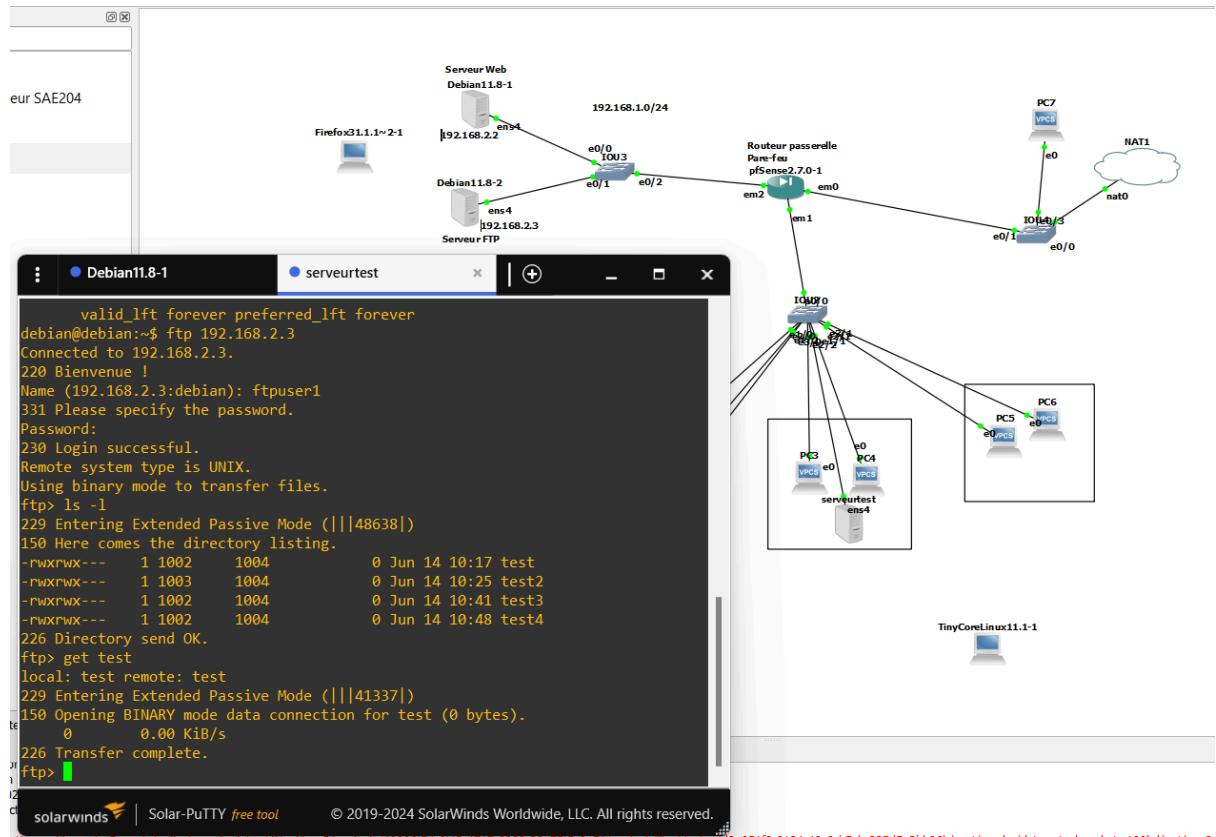


On peut alors installer ftp sur une machine du VLAN 20 qui peut donc accéder à nos services FTP :

```
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0c:b9:55:a5:00:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet 192.168.20.3/24 brd 192.168.20.255 scope global dynamic ens4
        valid_lft 7198sec preferred_lft 7198sec
    inet6 fe80::eb9:55ff:fea5:0/64 scope link
        valid_lft forever preferred_lft forever
debian@debian:~$ sudo apt install ftp
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  tftp
The following NEW packages will be installed:
  ftp tftp
0 upgraded, 2 newly installed, 0 to remove and 277 not upgraded.
Need to get 166 kB of archives.
After this operation, 319 kB of additional disk space will be used.
Do you want to continue? [Y/n] █
```

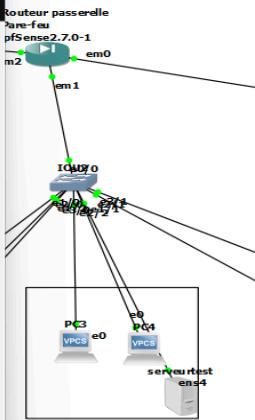
```
oup default qlen 1000
link/ether 0c:b9:55:a5:00:00 brd ff:ff:ff:ff:ff:ff
altname enp0s4
inet 192.168.20.3/24 brd 192.168.20.255 scope global dynamic ens4
    valid_lft 7087sec preferred_lft 7087sec
inet6 fe80::eb9:55ff:fea5:0/64 scope link
    valid_lft forever preferred_lft forever
debian@debian:~$ ftp 192.168.2.3
Connected to 192.168.2.3.
220 Bienvenue !
Name (192.168.2.3:debian): ftpuser1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode (|||48638|)
150 Here comes the directory listing.
-rwxrwx--- 1 1002 1004 0 Jun 14 10:17 test
-rwxrwx--- 1 1003 1004 0 Jun 14 10:25 test2
-rwxrwx--- 1 1002 1004 0 Jun 14 10:41 test3
-rwxrwx--- 1 1002 1004 0 Jun 14 10:48 test4
226 Directory send OK.
ftp> █
```

Et voici un test de transfert de fichier pour tenter de récupérer le fichier test :



On a donc un FTP entièrement fonctionnel...

On peut également utiliser SSH depuis le serveur test en root pour gérer le serveur HTTP (serveur web apache2) :



```

SAE204
Debian11.8-1
serveurtest

debian@debian:~$ ssh debian@192.168.2.2
The authenticity of host '192.168.2.2 (192.168.2.2)' can't be established.
ECDSA key fingerprint is SHA256:8T8GfCubW62lRb/e8Vzvmt6o4yh7qertrnZfcxxvcIxU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.2' (ECDSA) to the list of known hosts.
debian@192.168.2.2's password:
Linux debian 5.10.0-26-cloud-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jun 16 16:28:24 2024
debian@debian:~$ sudo -i
root@debian:~# sudo nano /var/www/sae201.com/

```

solarwinds | Solar-PuTTY *free tool* © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

```

serveurtest.

root@debian:~#
root@debian:~# exit
logout
debian@debian:~$ exit
logout
Connection to 192.168.2.2 closed.
debian@debian:~$ ssh debian@192.168.2.2
debian@192.168.2.2's password:
Linux debian 5.10.0-26-cloud-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun 17 06:23:10 2024 from 192.168.20.4
debian@debian:~$ sudo -i
root@debian:~#

```