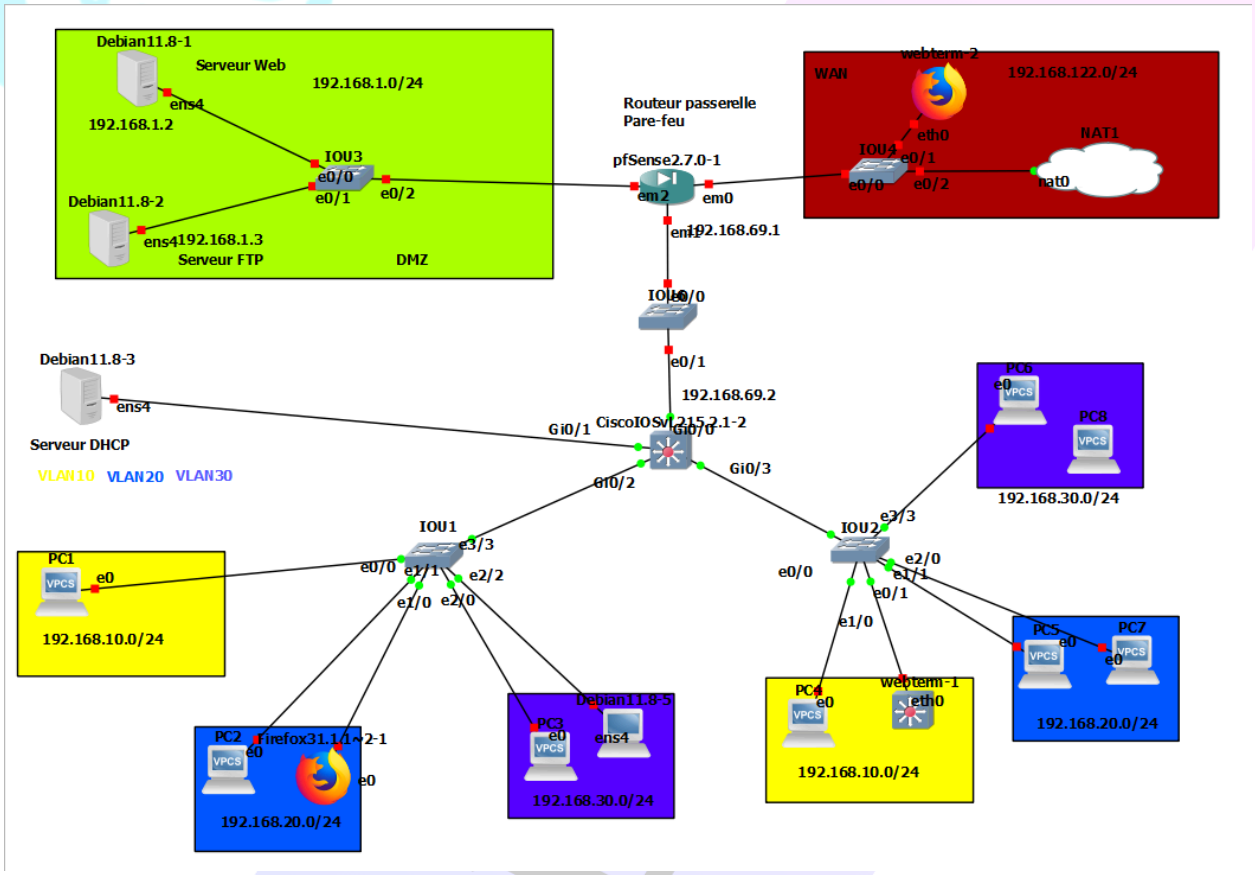


Tâche 1

Élaboration du plan d'adressage IPv4 (comprenant les adresses réseaux des VLAN, les adresses des passerelles par défaut, les adresses des machines serveurs, etc.)

VLAN	Nom	Réseau	Passerelle par défaut	Plage DHCP
10	Direction	192.168.10.0/24	192.168.10.2	192.168.10.100 - 192.168.10.150
20	Gestion	192.168.20.0/24	192.168.20.2	192.168.20.100 - 192.168.20.150
30	Comtech	192.168.30.0/24	192.168.30.2	192.168.30.100 - 192.168.30.150

Ports	Affectation	Réseau logique
IOU1 et IOU2 eth0/0-3	VLAN 10	192.168.10.0/24
IOU1 et IOU2 eth1/0-3	VLAN 20	192.168.20.0/24
IOU1 et IOU2 eth2/0-3	VLAN 30	192.168.30.0/24
EWS1 gi0/0	TRUNK	192.168.69.0/24

Serveur	Système	Adresse IP	Emplacement
Serveur Web	Debian11.8-1	192.168.1.2	DMZ
Serveur FTP	Debian11.8-2	192.168.1.3	DMZ
Serveur DHCP	Debian11.8-3	ens4.10: 192.168.10.1 ens4.20: 192.168.20.1 ens4.30: 192.168.30.1	VLAN 10,20,30

Tâche 2

Création d'un réseau segmenté avec la mise en place et la configuration des VLAN (sur les 2 commutateurs d'accès de couche 2)

Pour IOU1 et IOU2:

```
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
```

```
IOU1#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et3/0, Et3/1, Et3/2
10   Direction                        active    Et0/0, Et0/1, Et0/2, Et0/3
20   Gestion                          active    Et1/0, Et1/1, Et1/2, Et1/3
30   Comtech                          active    Et2/0, Et2/1, Et2/2, Et2/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
IOU2#show vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et3/0, Et3/1, Et3/2
10   Direction                        active    Et0/0, Et0/1, Et0/2, Et0/3
20   Gestion                          active    Et1/0, Et1/1, Et1/2, Et1/3
30   Comtech                          active    Et2/0, Et2/1, Et2/2, Et2/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Tâche 3

Mise en place et configuration du routage inter-VLAN (commutateur de distribution de couche 3 -> prendre un Switch L3 dans GNS3)

 # Sur IOU1

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

 # Sur IOU2

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

```
IOU1#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et3/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et3/3       10,20,30

Port        Vlans allowed and active in management domain
Et3/3       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Et3/3       10,20,30
```

```
IOU2#show int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et3/3       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et3/3       10,20,30

Port        Vlans allowed and active in management domain
Et3/3       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Et3/3       10,20,30
```

SUR ESW1:

```
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
 no shutdown
exit

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 192.168.10.2 255.255.255.0
no shut
exit
```

```
interface vlan 20
 ip address 192.168.20.2 255.255.255.0
no shut
exit

interface vlan 30
 ip address 192.168.30.2 255.255.255.0
no shut
exit

ip routing
```

```
Switch#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.69.2    YES NVRAM  up                    up
GigabitEthernet0/1     unassigned      YES unset  up                    up
GigabitEthernet0/2     unassigned      YES unset  up                    up
GigabitEthernet0/3     unassigned      YES unset  up                    up
GigabitEthernet1/0     unassigned      YES unset  down                  down
GigabitEthernet1/1     unassigned      YES unset  down                  down
GigabitEthernet1/2     unassigned      YES unset  down                  down
GigabitEthernet1/3     unassigned      YES unset  down                  down
GigabitEthernet2/0     unassigned      YES unset  down                  down
GigabitEthernet2/1     unassigned      YES unset  down                  down
GigabitEthernet2/2     unassigned      YES unset  down                  down
GigabitEthernet2/3     unassigned      YES unset  down                  down
GigabitEthernet3/0     unassigned      YES unset  down                  down
GigabitEthernet3/1     unassigned      YES unset  down                  down
GigabitEthernet3/2     unassigned      YES unset  down                  down
GigabitEthernet3/3     unassigned      YES unset  down                  down
Vlan10                 192.168.10.2    YES NVRAM  up                    up
Vlan20                 192.168.20.2    YES NVRAM  up                    up
Vlan30                 192.168.30.2    YES NVRAM  up                    up
```

```
Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.2/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.2/32 is directly connected, Vlan20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Vlan30
L        192.168.30.2/32 is directly connected, Vlan30
      192.168.69.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.69.0/24 is directly connected, GigabitEthernet0/0
L        192.168.69.2/32 is directly connected, GigabitEthernet0/0
```

Pour le réseau LAN, avec la DMZ qui est 192.168.1.0/24 on fait une route statique et avec Internet qui est 192.168.122.0/24 et l'adresse de saut est 192.168.69.1:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip route 192.168.1.0 255.255.255.0 192.168.69.1
Switch(config)#ip route 192.168.122.0 255.255.255.0 192.168.69.1
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.69.1
Switch(config)#end
Switch#
*Jun 14 18:31:05.461: %SYS-5-CONFIG_I: Configured from console by console
Switch#wr
Building configuration...
Compressed configuration from 4002 bytes to 1860 bytes[OK]
Switch#
*Jun 14 18:32:53.601: %GRUB-5-CONFIG_WRITING: GRUB configuration is being updated on disk. Please wait...
*Jun 14 18:32:54.345: %GRUB-5-CONFIG_WRITTEN: GRUB configuration was written to disk successfully.
```

```
Switch#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 192.168.69.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.69.1
S     192.168.1.0/24 [1/0] via 192.168.69.1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.2/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.2/32 is directly connected, Vlan20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.30.0/24 is directly connected, Vlan30
L        192.168.30.2/32 is directly connected, Vlan30
      192.168.69.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.69.0/24 is directly connected, GigabitEthernet0/0
L        192.168.69.2/32 is directly connected, GigabitEthernet0/0
S     192.168.122.0/24 [1/0] via 192.168.69.1
```

Mais le ping ne fonctionne pas car le Pfsense n'est pas encore configuré.

Tâche 4

Installation et configurations des services DHCP, SSH, FTP et HTTP sur des serveurs (virtualisés) de l'infrastructure réseau -> prendre machine Debian 11.8

Debian 11.8.1: Serveur Web

Pour créer un serveur web avec Debian 11.8 et héberger un site web simple à l'adresse sae201.com, vous pouvez suivre ces étapes :

Étapes principales :

1. Installer Apache (serveur HTTP) :

```
sudo apt update
sudo apt install apache2
```

Apache est maintenant installé sur votre serveur Debian et démarre automatiquement après l'installation.

2. Configurer Apache pour héberger votre site :

a. Assurez-vous que le service Apache est en cours d'exécution :

```
sudo systemctl status apache2
```

b. Créez un répertoire pour votre site web. Par convention, les sites web sont souvent stockés dans `/var/www/` :

```
sudo mkdir /var/www/sae201.com
```

c. Créez un fichier `index.html` dans ce répertoire pour votre page d'accueil :

```
sudo nano /var/www/sae201.com/index.html
```

Ajoutez-y le contenu de votre page web, par exemple :

```
<!DOCTYPE html>
<html>
<head>
    <title>Bienvenue sur SAE201.com</title>
</head>
<body>
    <h1>Site web SAE201.com</h1>
    <p>Bienvenue sur notre site web!</p>
</body>
</html>
```

Enregistrez et fermez le fichier (`Ctrl+X`, puis `Y` pour confirmer et `Enter`).

d. Définissez les permissions correctes pour que Apache puisse servir ces fichiers :

```
sudo chown -R www-data:www-data /var/www/sae201.com
sudo chmod -R 755 /var/www/sae201.com
```

3. Configurer Apache pour servir le site :

a. Créez un fichier de configuration pour votre site dans le répertoire des sites disponibles d'Apache :

```
sudo nano /etc/apache2/sites-available/sae201.com.conf
```

Ajoutez-y la configuration suivante (remplacez `sae201.com` par votre nom de domaine réel si vous en avez un) :

```
<VirtualHost *:80>
    ServerAdmin webmaster@sae201.com
    ServerName sae201.com
    DocumentRoot /var/www/sae201.com

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Enregistrez et fermez le fichier.

b. Activez ce fichier de configuration de site :

```
sudo a2ensite sae201.com.conf
```

c. Désactivez le site par défaut si nécessaire :

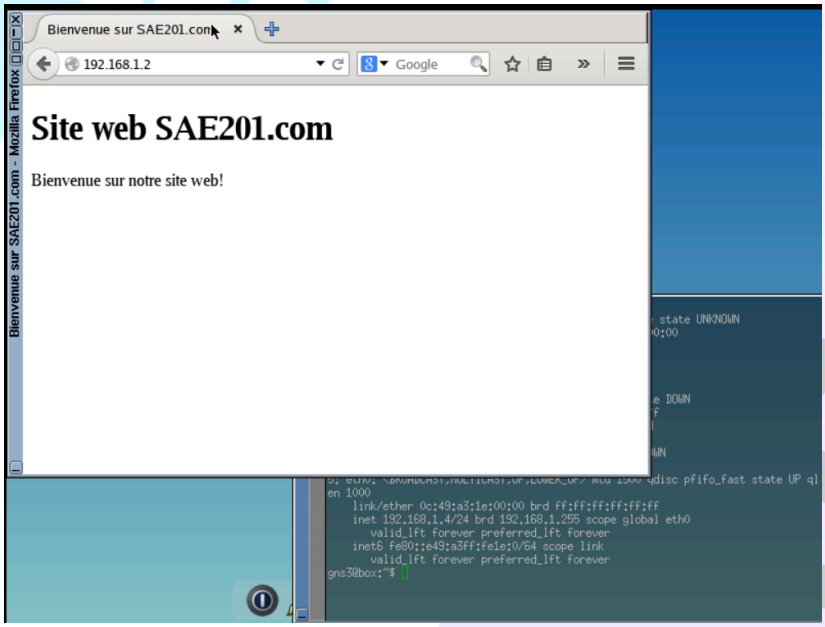
```
sudo a2dissite 000-default.conf
```

4. Redémarrez Apache pour appliquer les modifications :

```
sudo systemctl restart apache2
```

```
debian@debian:~$ sudo systemctl restart apache2
debian@debian:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese>
     Active: active (running) since Thu 2024-06-13 10:36:22 UTC; 6s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 2156 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU>
   Main PID: 2160 (apache2)
      Tasks: 55 (limit: 546)
     Memory: 4.6M
        CPU: 149ms
     CGroup: /system.slice/apache2.service
             ├─2160 /usr/sbin/apache2 -k start
             ├─2161 /usr/sbin/apache2 -k start
             └─2162 /usr/sbin/apache2 -k start

Jun 13 10:36:22 debian systemd[1]: Starting The Apache HTTP Server...
Jun 13 10:36:22 debian apachectl[2159]: AH00558: apache2: Could not reliably de>
Jun 13 10:36:22 debian systemd[1]: Started The Apache HTTP Server.
debian@debian:~$
```

Sur un PC :



Debian 11.8.2:Serveur FTP

Pour configurer un serveur FTP sur Debian 11.8, nous allons utiliser `vsftpd`, un serveur FTP sécurisé, rapide et stable. Voici les étapes pour installer et configurer `vsftpd` :

Étapes pour installer et configurer `vsftpd` :

1. Mettre à jour le système et Installer `vsftpd` :

```
sudo apt update
sudo apt install vsftpd
sudo apt install ftp
```

3. Configurer `vsftpd` :

a. Ouvrez le fichier de configuration de `vsftpd` :

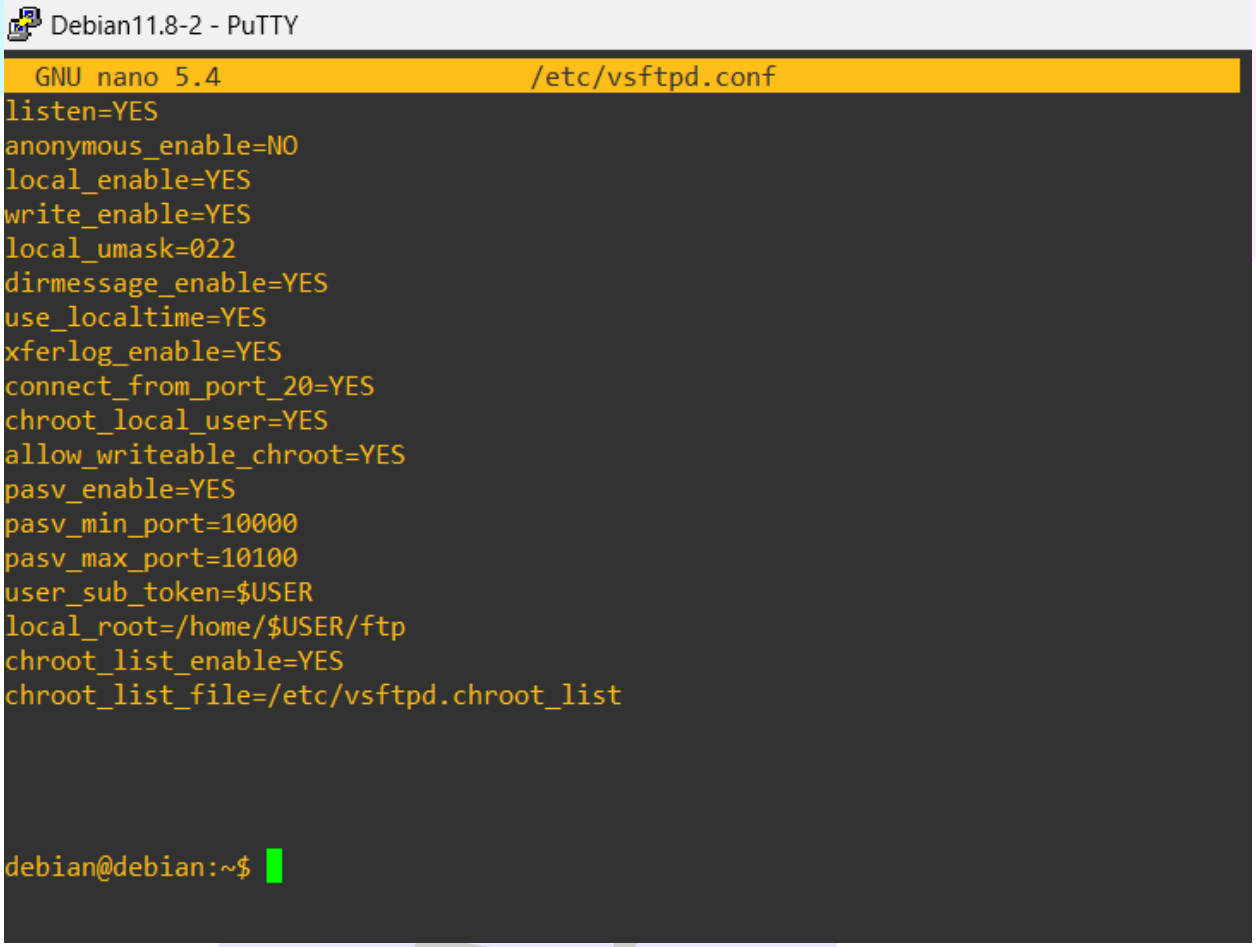
```
sudo nano /etc/vsftpd.conf
```

b. Modifiez les paramètres suivants (assurez-vous que ces lignes ne sont pas commentées en retirant le `#` devant les lignes) :

```
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES
allow_writeable_chroot=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

c. Ajoutez ou modifiez les lignes suivantes pour améliorer la sécurité :

```
user_sub_token=$USER
local_root=/home/$USER/ftp
pasv_min_port=10000
pasv_max_port=10100
ssl_enable=NO
```



Sauvegardez et fermez le fichier (`Ctrl+X`, puis `Y` et `Enter`).

4. Créer un répertoire FTP pour un utilisateur spécifique :

a. Créez des utilisateurs:

```
sudo adduser user1
sudo adduser user2
```

Suivez les instructions pour définir un mot de passe et des informations supplémentaires.

b. Créez un répertoire FTP pour cet utilisateur :

```
sudo mkdir -p /home/ftp/shared
sudo mkdir -p /home/user1/ftp
sudo mkdir -p /home/user2/ftp
sudo chown user1:ftp /home/user1/ftp
sudo chmod -R 775 /home/user1/ftp
sudo chown user2:ftp /home/user2/ftp
sudo chmod -R 775 /home/user2/ftp
sudo chmod a-w /home/user1/ftp
sudo chmod a-w /home/user2/ftp
sudo ln -s /home/ftp/shared /home/user1/ftp/shared
sudo ln -s /home/ftp/shared /home/user2/ftp/shared
sudo chown -R ftp:ftp /home/ftp/shared
```

5. Redémarrer `vsftpd` pour appliquer les modifications :

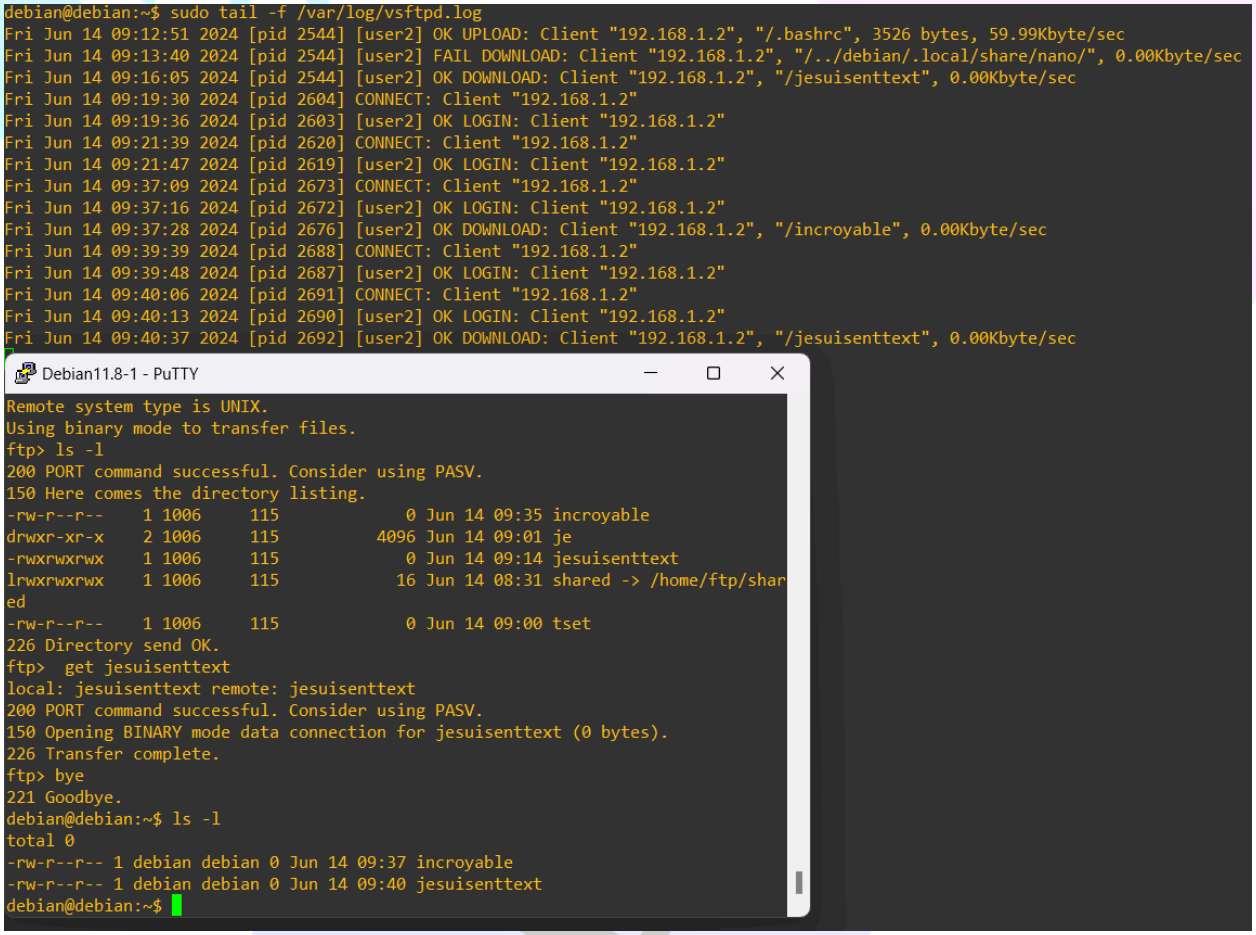
```
sudo systemctl restart vsftpd
```

Configuration supplémentaire :
Vous pouvez également ajouter des utilisateurs à la liste chroot `vsftpd' si vous souhaitez chrooter des utilisateurs spécifiques :
1.Modifier/créer le fichier de liste chroot :

```
sudo nano /etc/vsftpd.chroot_list
```

```
  GNU nano 5.4                  /etc/vsftpd.chroot_list
echo "user1" | sudo tee -a /etc/vsftpd.chroot_list
echo "user2" | sudo tee -a /etc/vsftpd.chroot_list
```

Test sur le serveur Web :



Le SSH sur les serveur:

Pour configurer SSH sur deux serveurs Debian 11.8, vous devez installer et configurer le serveur SSH sur chaque machine. Voici comment le faire :

Étapes pour configurer SSH sur chaque serveur :

1. Mettre à jour le système :

```
sudo apt update
sudo apt upgrade
```

2. Installer OpenSSH Server :

```
sudo apt install openssh-server
```

3. Vérifier que le service SSH est en cours d'exécution :

```
sudo systemctl status ssh
```

Vous devriez voir quelque chose comme "active (running)". Si le service n'est pas démarré, vous pouvez le démarrer avec :

```
sudo systemctl start ssh
```

4. Activer le service SSH au démarrage :

```
sudo systemctl enable ssh
```

5. Configurer le pare-feu (si nécessaire) :

Si vous utilisez un pare-feu, assurez-vous que le port SSH (par défaut 22) est ouvert :

```
sudo ufw allow ssh
sudo ufw enable
```

6. Configurer SSH pour plus de sécurité (optionnel mais recommandé) :

Ouvrez le fichier de configuration SSH :

```
sudo nano /etc/ssh/sshd_config
```

- Désactivez l'accès root direct via SSH :

```
PermitRootLogin no
```

- Changez le port par défaut pour éviter certaines attaques (facultatif) :

```
Port 2222
```

- Redémarrez le service SSH pour appliquer les modifications :

```
sudo systemctl restart ssh
```

Debian 11.8.3:Serveur DHCP

Pour configurer le serveur DHCP avec le paquet `isc-dhcp-server` et gérer les VLANs sous Debian, suivez les étapes ci-dessous.

1. Installation des paquets nécessaires
Installez le serveur DHCP et les outils VLAN :

```
sudo apt update
sudo apt install isc-dhcp-server vlan
```

2. Configuration des interfaces réseau pour les VLANs
Éditez le fichier `/etc/network/interfaces` pour configurer les VLANs. Supposons que l'interface physique est `ens4` :

```
# /etc/network/interfaces

# Interface physique
auto ens4
iface ens4 inet manual

# 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
```

3. Configuration du serveur DHCP

Modifiez le fichier de configuration DHCP pour définir les pools d'adresses pour chaque VLAN :

```
# /etc/dhcp/dhcpd.conf

default-lease-time 600;
max-lease-time 7200;

subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.100 192.168.10.150;
    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;
    option domain-name "direction.local";
}

subnet 192.168.20.0 netmask 255.255.255.0 {
    range 192.168.20.100 192.168.20.150;
    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;
    option domain-name "gestion.local";
}

subnet 192.168.30.0 netmask 255.255.255.0 {
    range 192.168.30.100 192.168.30.150;
    option routers 192.168.30.2;
    option subnet-mask 255.255.255.0;
```

```
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    option domain-name "comtech.local";
}
```

Éditez le fichier `/etc/default/isc-dhcp-server` pour configurer les VLANs.

```
INTERFACESv4="ens4 ens4.10 ens4.20 ens4.30"
```

4. Démarrage et activation des services
Redémarrez les services réseau et le serveur DHCP :

```
sudo systemctl restart networking
sudo systemctl restart isc-dhcp-server
```

Activer le service pour qu'il démarre au démarrage du système

```
sudo systemctl enable isc-dhcp-server
```

5. Vérification de la configuration
Vérifiez que les interfaces VLAN sont correctement configurées et que le serveur DHCP fonctionne :

```
# Vérifiez les interfaces réseau
ip addr show

# Vérifiez l'état du serveur DHCP
sudo systemctl status isc-dhcp-server

# Vérifiez les logs DHCP pour les adresses attribuées
tail -f /var/log/syslog | grep dhcpd
```

On teste avec les différents PCs.

```
PC1> ip dhcp
DDORA IP 192.168.10.100/24 GW 192.168.10.2
```

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

```
PC3> ip dhcp
DDORA IP 192.168.30.100/24 GW 192.168.30.2
```

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

```
PC5> ip dhcp
DDORA IP 192.168.20.100/24 GW 192.168.20.2
```

```
PC6> ip dhcp
DDORA IP 192.168.30.101/24 GW 192.168.30.2
```

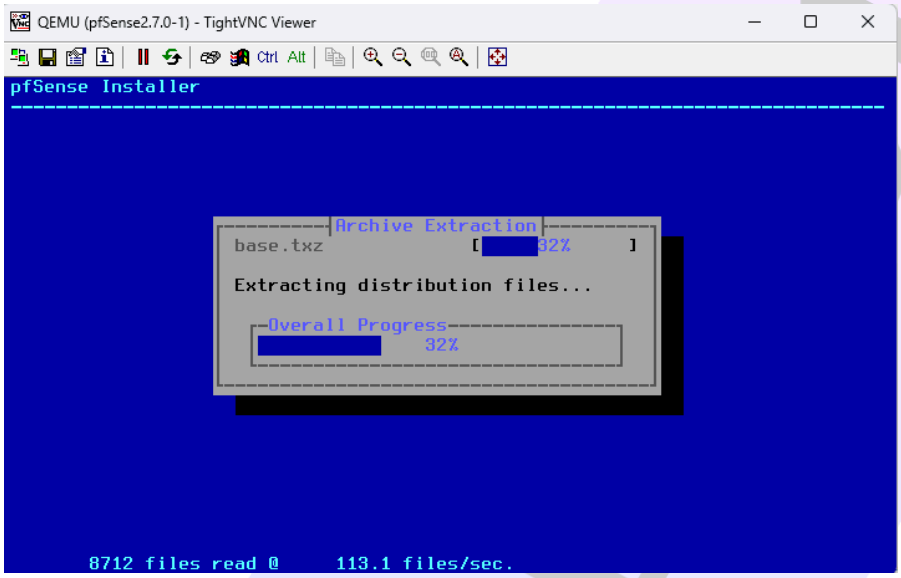
```
PC6> ping 192.168.10.100
192.168.10.100 icmp_seq=1 timeout
84 bytes from 192.168.10.100 icmp_seq=2 ttl=63 time=8.578 ms
84 bytes from 192.168.10.100 icmp_seq=3 ttl=63 time=9.460 ms
84 bytes from 192.168.10.100 icmp_seq=4 ttl=63 time=10.450 ms
84 bytes from 192.168.10.100 icmp_seq=5 ttl=63 time=11.879 ms
```

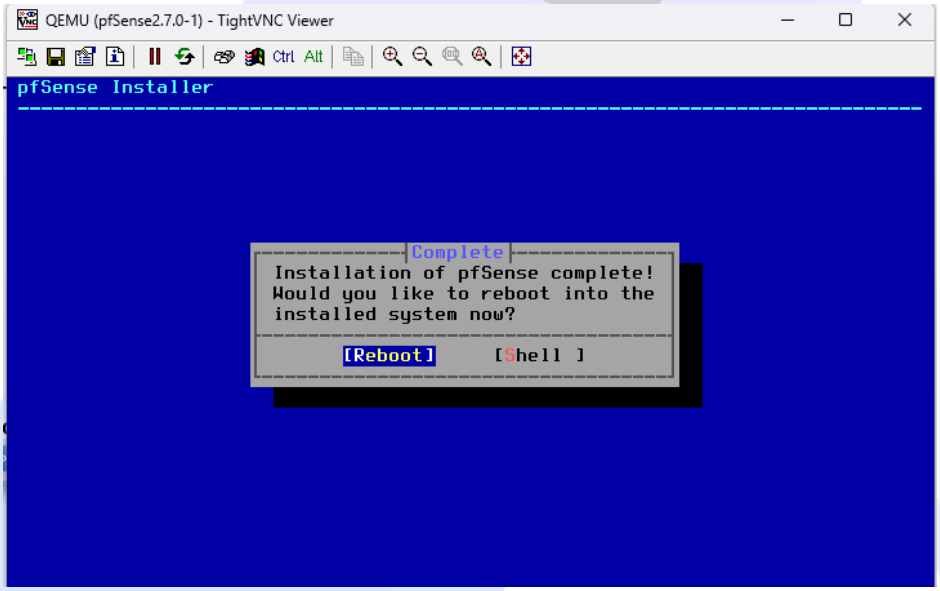
Tâche 5

Mise en place et configuration de l'accès à Internet (si cela s'avère nécessaire, penser aussi à mettre en œuvre un objet webterm ou Firefox pour tester la navigation sur Internet)

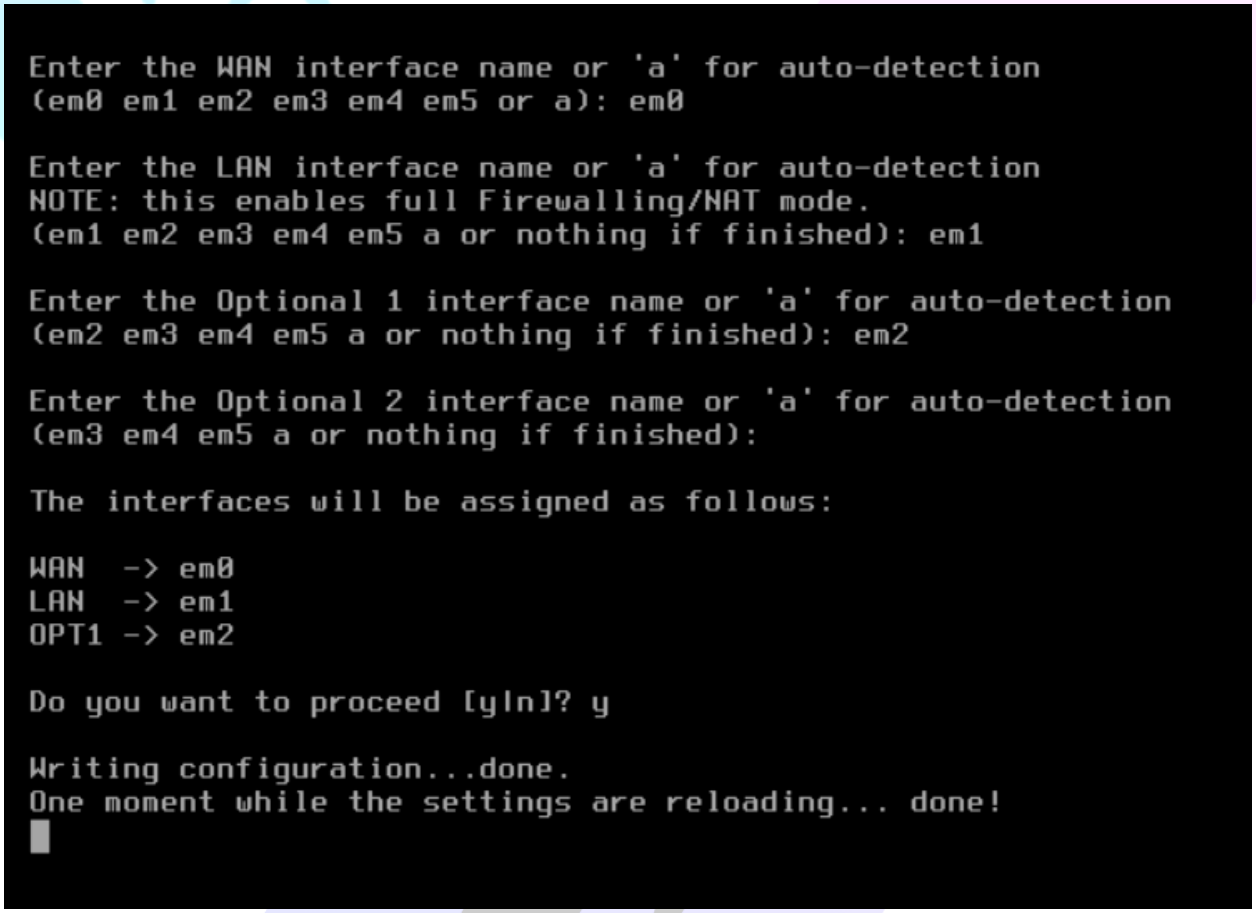
Tâche 6

Installation et configuration d'un pare-feu (si cela s'avère nécessaire, penser à se connecter directement avec un objet webterm ou Firefox pour avoir accès à l'interface web de pfSense). Utiliser le TP de configuration de pfSense.





On configure les interfaces du Pfsense donc em0 pour le NAT qui est le WAN, em1 pour le LAN et em3 pour le DMZ noté pour le moment OPT1


Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 em5 or a): em0
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 em5 a or nothing if finished): em1
Enter the Optional 1 interface name or 'a' for auto-detection
(em2 em3 em4 em5 a or nothing if finished): em2
Enter the Optional 2 interface name or 'a' for auto-detection
(em3 em4 em5 a or nothing if finished):
The interfaces will be assigned as follows:
WAN -> em0
LAN -> em1
OPT1 -> em2
Do you want to proceed [y|n]? y
Writing configuration...done.
One moment while the settings are reloading... done!

On configure les adresses IP.

```
 6) Halt system                          15) Restore recent configuration
 7) Ping host                            16) Restart PHP-FPM
 8) Shell

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
```

```
>

Configure IPv6 address LAN interface via DHCP6? (y/n) N

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) N
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) Y

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...
 Restarting webConfigurator...

The IPv4 LAN address has been set to 192.168.69.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.69.1/

Press <ENTER> to continue.
```

```
For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via DHCP6? (y/n) N

Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? (y/n) N
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to OPT1...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 OPT1 address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.1.1/

Press <ENTER> to continue.
```

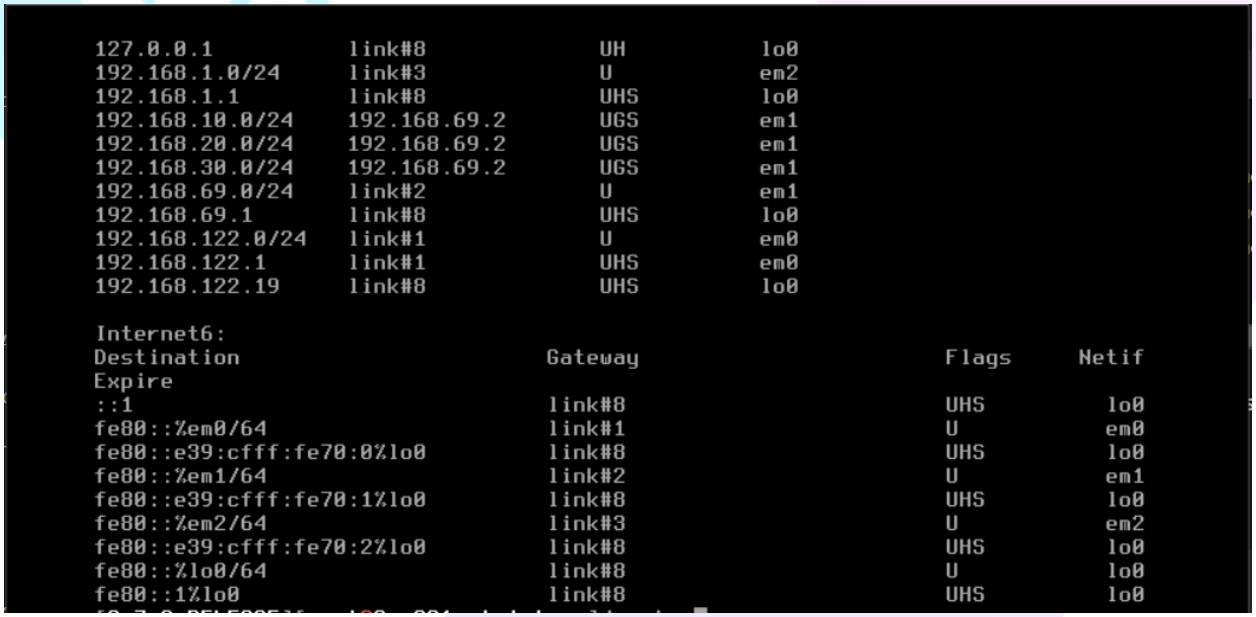
On va ajouter les routes statiques pour les réseaux du LAN sur le Pfsense.

```
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@Sae201.rt-iut.re]/root:
```

```
route add -net 192.168.10.0/24 192.168.69.2
route add -net 192.168.20.0/24 192.168.69.2
route add -net 192.168.30.0/24 192.168.69.2
route add default gw 192.168.1.1
```

```
[2.7.0-RELEASE][root@Sae201.rt-iut.re]/root: route add -net 192.168.10.0/24 192.
168.69.2
[fib_algo] inet.0 (bsearch4#34) rebuild_fd_flm: switching algo to radix4_lockles
s
add net 192.168.10.0: gateway 192.168.69.2
[2.7.0-RELEASE][root@Sae201.rt-iut.re]/root: route add -net 192.168.20.0/24 192.
168.69.2
add net 192.168.20.0: gateway 192.168.69.2
[2.7.0-RELEASE][root@Sae201.rt-iut.re]/root: route add -net 192.168.30.0/24 192.
168.69.2
add net 192.168.30.0: gateway 192.168.69.2
[2.7.0-RELEASE][root@Sae201.rt-iut.re]/root:
```

```
netstat -rn
```

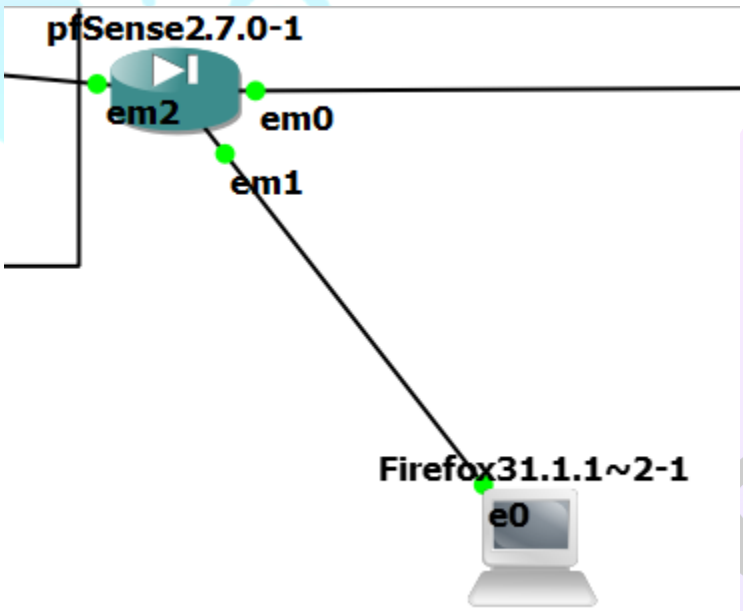


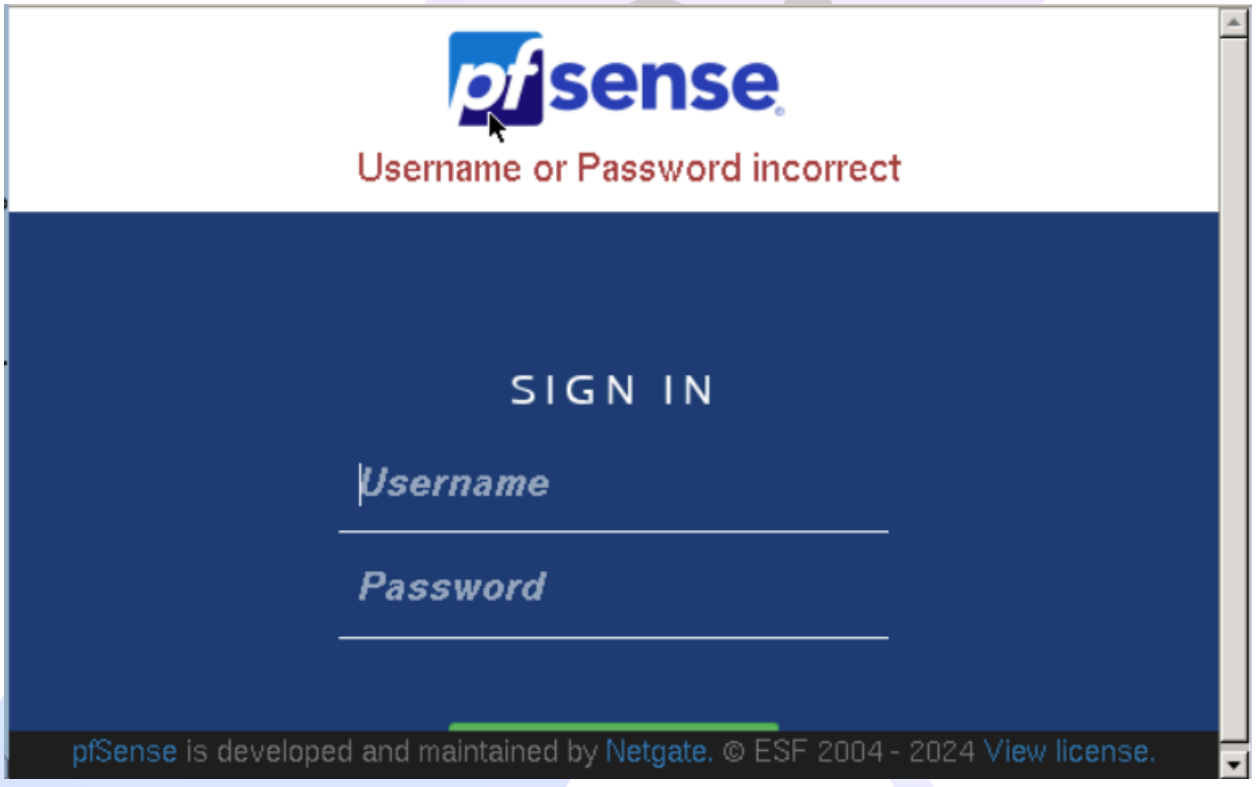
```
127.0.0.1          link#8             UH          lo0
192.168.1.0/24     link#3             U           em2
192.168.1.1        link#8             UHS         lo0
192.168.10.0/24    192.168.69.2       UGS         em1
192.168.20.0/24    192.168.69.2       UGS         em1
192.168.30.0/24    192.168.69.2       UGS         em1
192.168.69.0/24    link#2             U           em1
192.168.69.1       link#8             UHS         lo0
192.168.122.0/24   link#1             U           em0
192.168.122.1      link#1             UHS         em0
192.168.122.19     link#8             UHS         lo0

Internet6:
Destination                       Gateway                       Flags     Netif
Expire
::1                               link#8                        UHS         lo0
fe80::%em0/64                     link#1                        U           em0
fe80::e39:cfff:fe70:0%lo0         link#8                        UHS         lo0
fe80::%em1/64                     link#2                        U           em1
fe80::e39:cfff:fe70:1%lo0         link#8                        UHS         lo0
fe80::%em2/64                     link#3                        U           em2
fe80::e39:cfff:fe70:2%lo0         link#8                        UHS         lo0
fe80::%lo0/64                     link#8                        U           lo0
fe80::1%lo0                       link#8                        UHS         lo0
```

Tâche 7

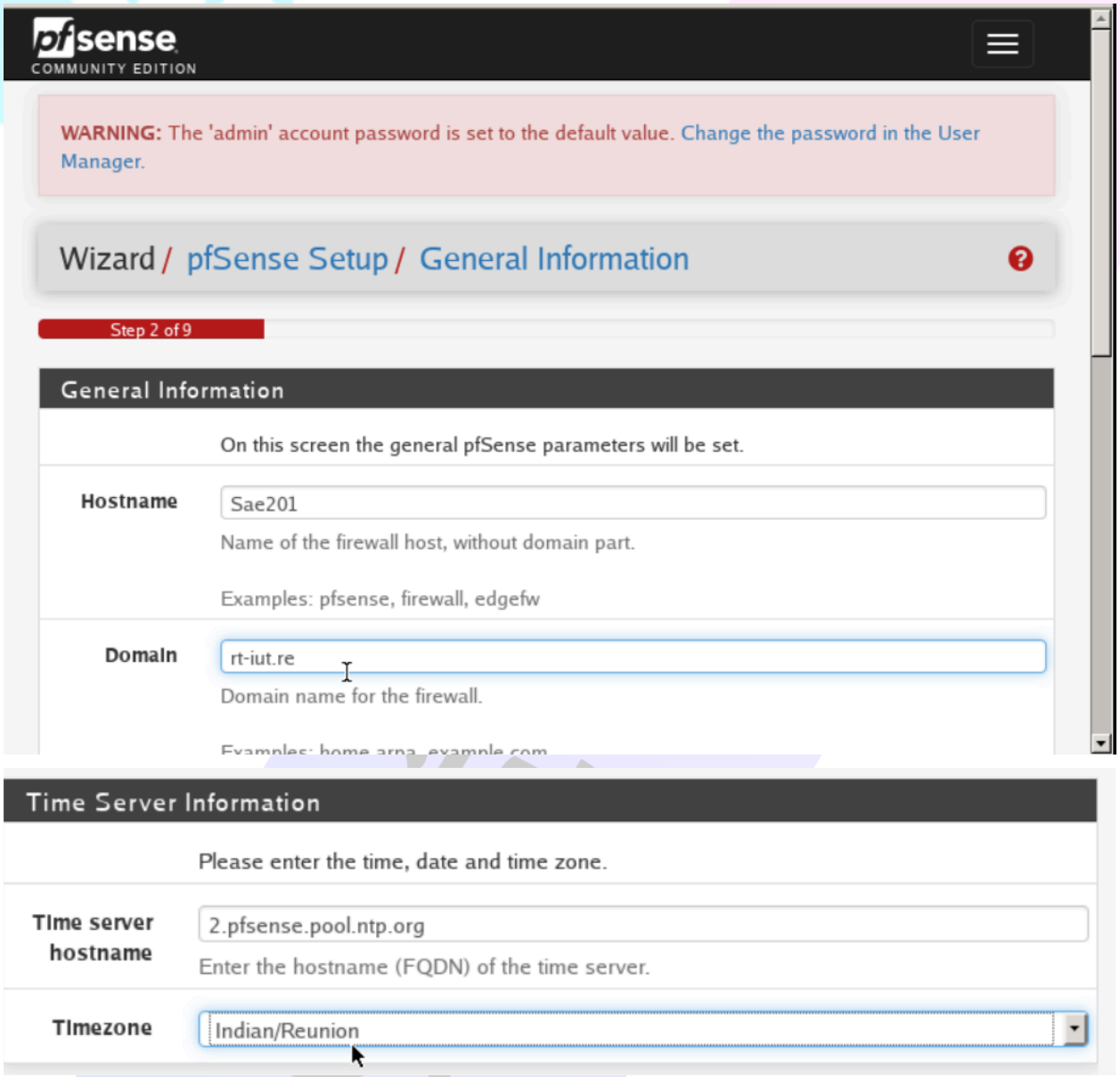
Mettre en place et configurer la DMZ pour les serveurs FTP et Web (HTTP)

Configuration graphique

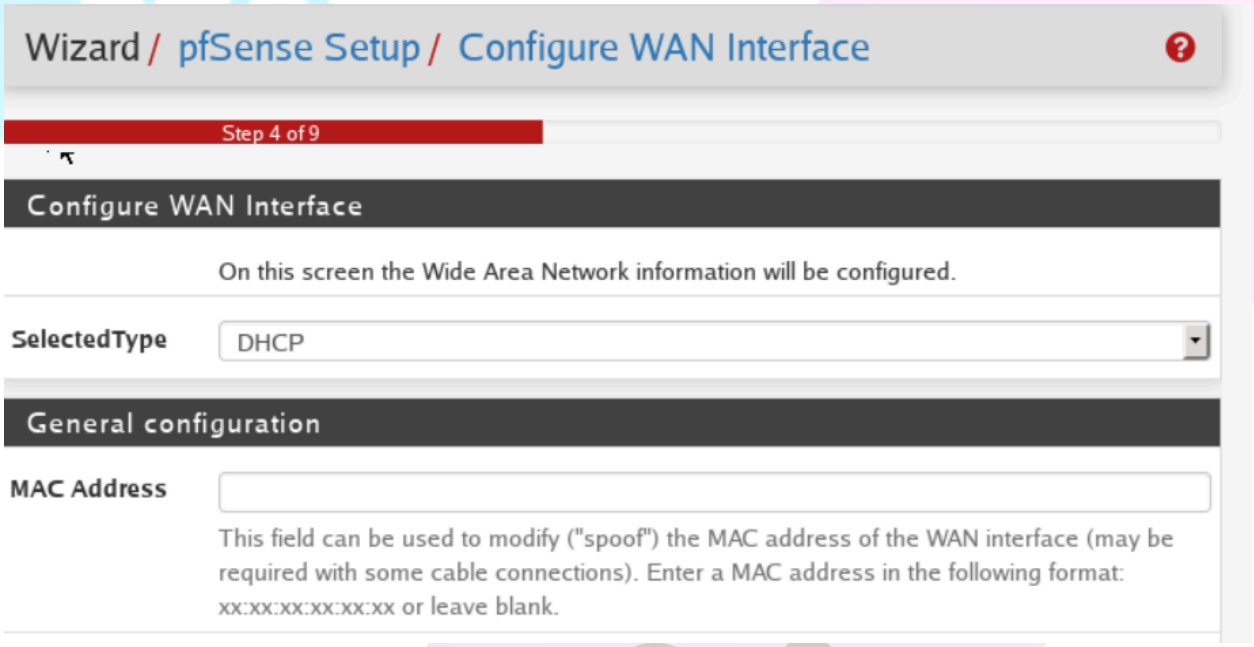


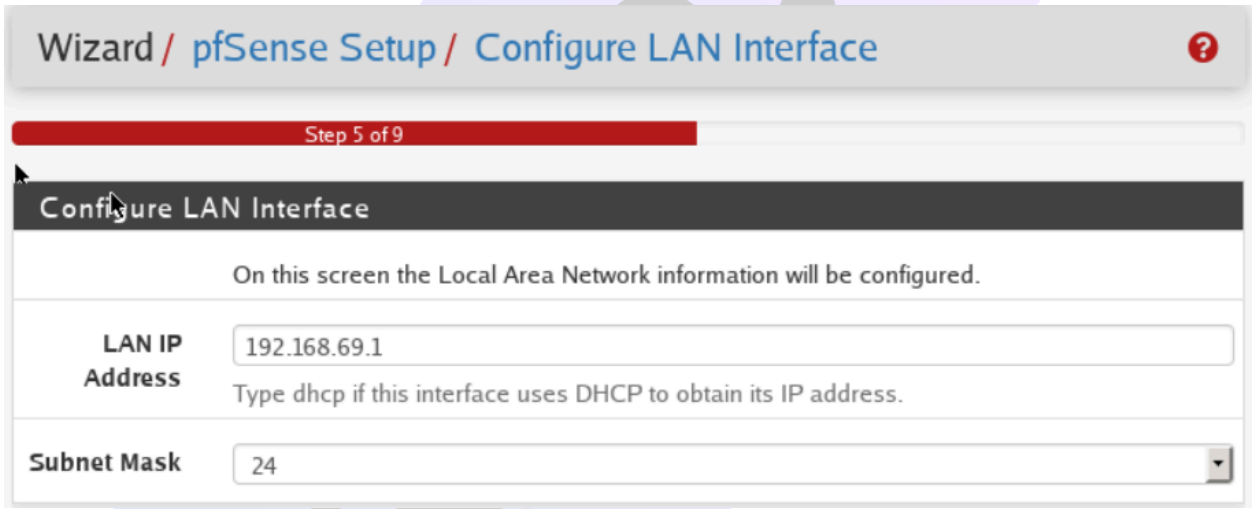


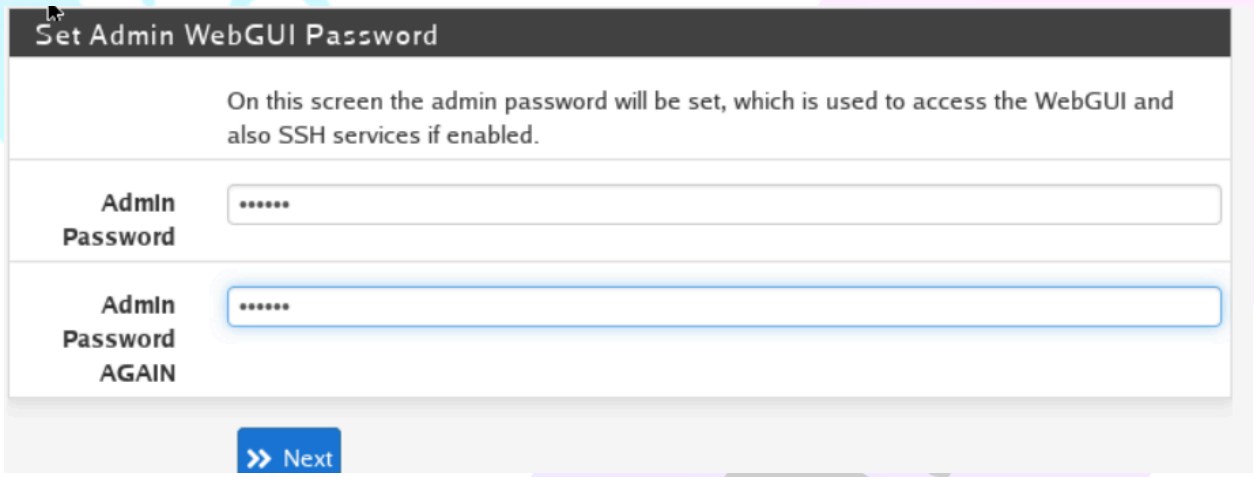
admin
pfsense



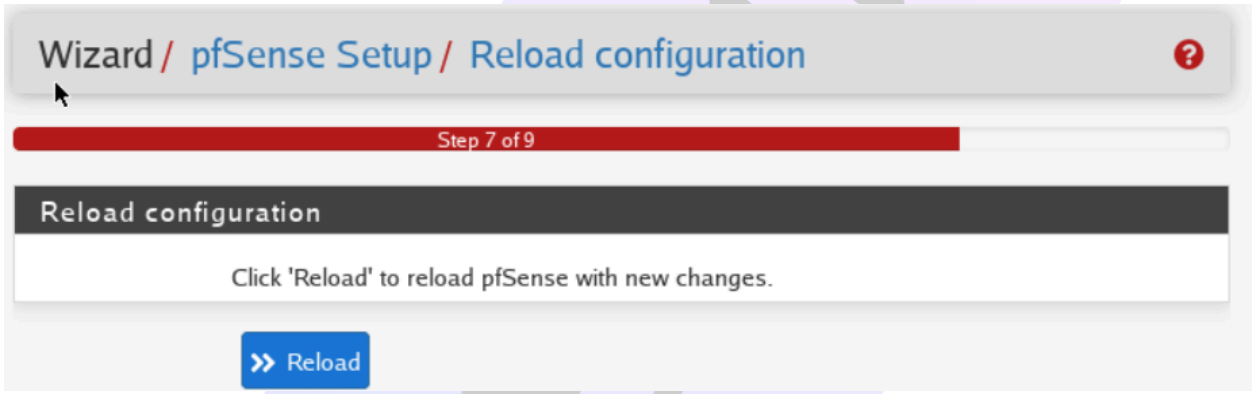
Vérification des informations:

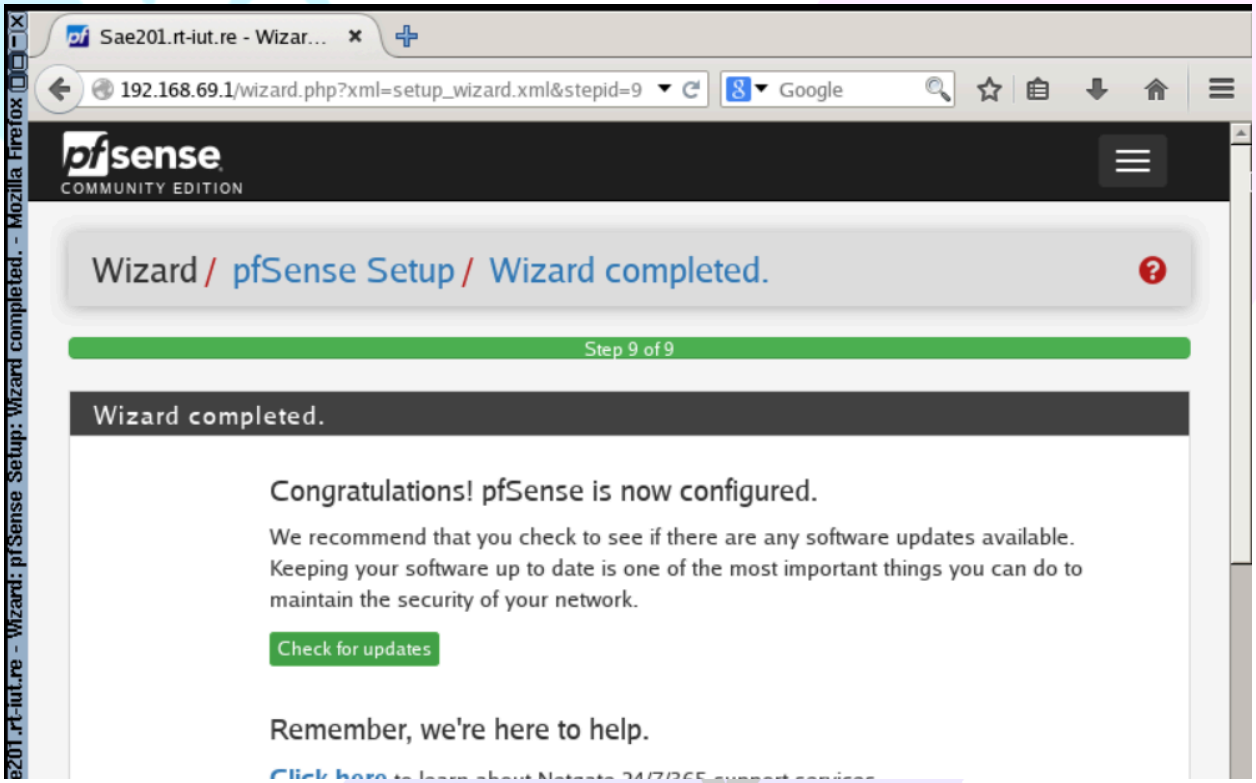

Wizard / pfSense Setup / Configure WAN Interface
Step 4 of 9
Configure WAN Interface
On this screen the Wide Area Network information will be configured.
SelectedType
DHCP
General configuration
MAC Address
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.


Wizard / pfSense Setup / Configure LAN Interface
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

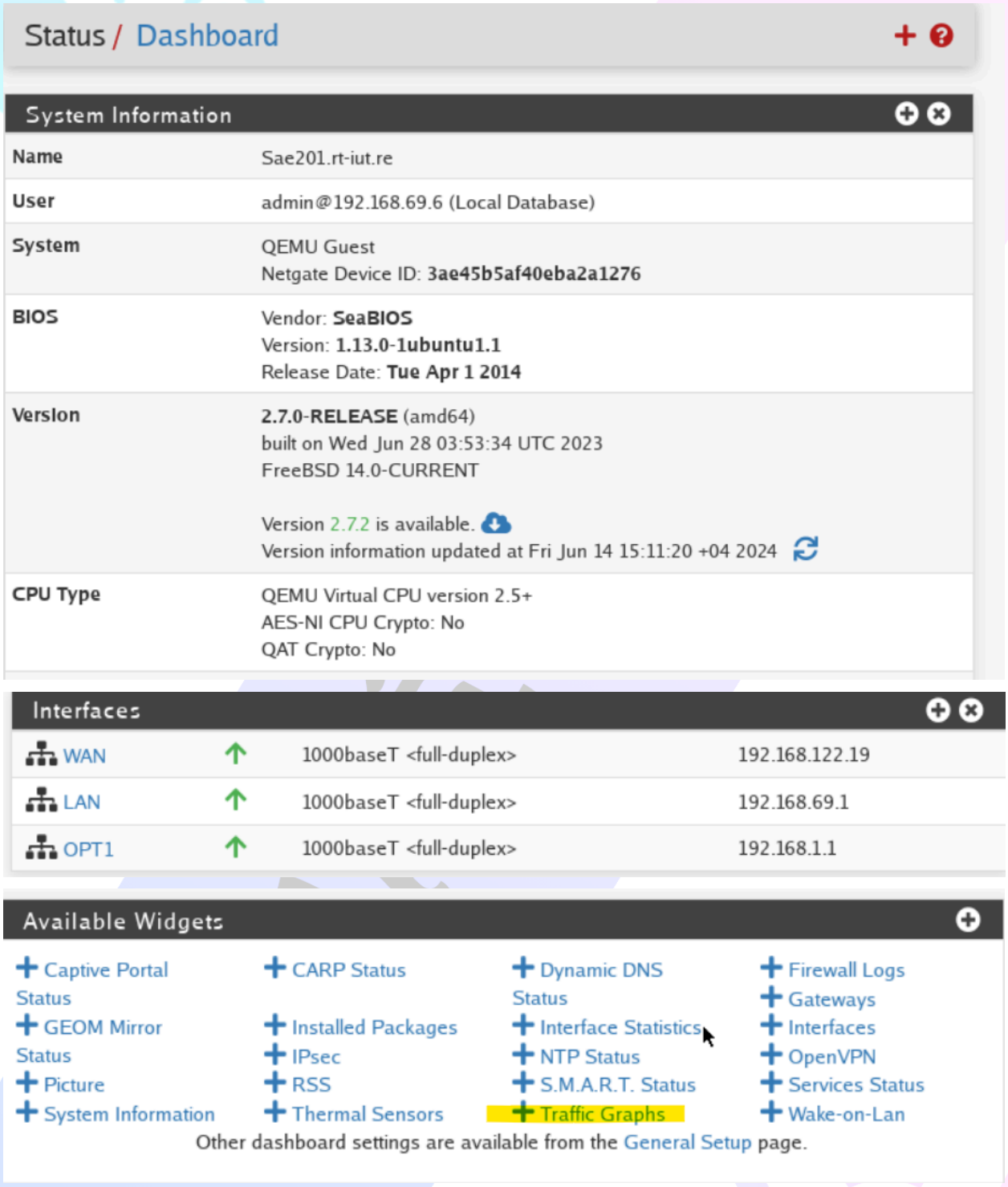

Set Admin WebGUI Password
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.
Admin Password
Admin Password AGAIN
Next

mdp: denice

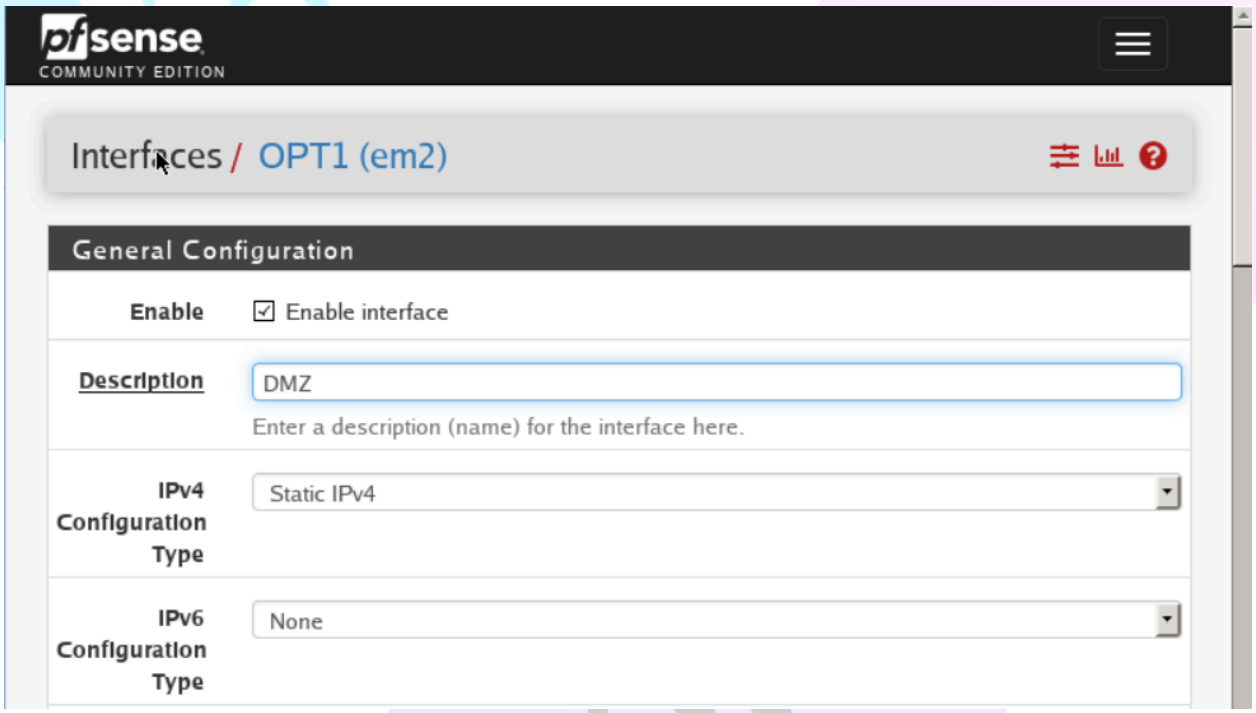

Wizard / pfSense Setup / Reload configuration
Step 7 of 9
Reload configuration
Click 'Reload' to reload pfSense with new changes.
Reload

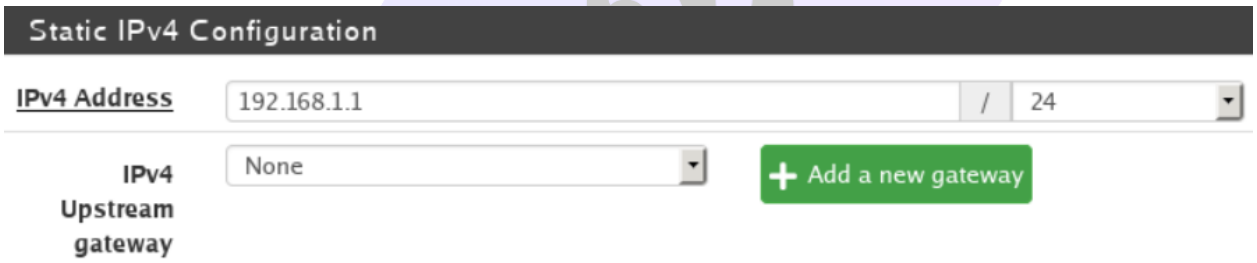


Je clique sur “Finish”

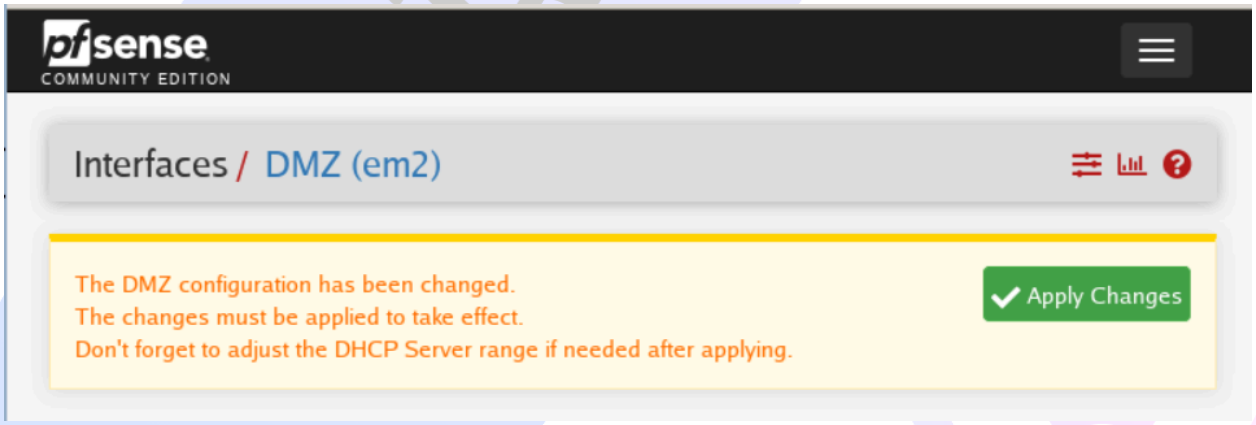


Pour l'activité de chaque réseau.
Configuration de em2:





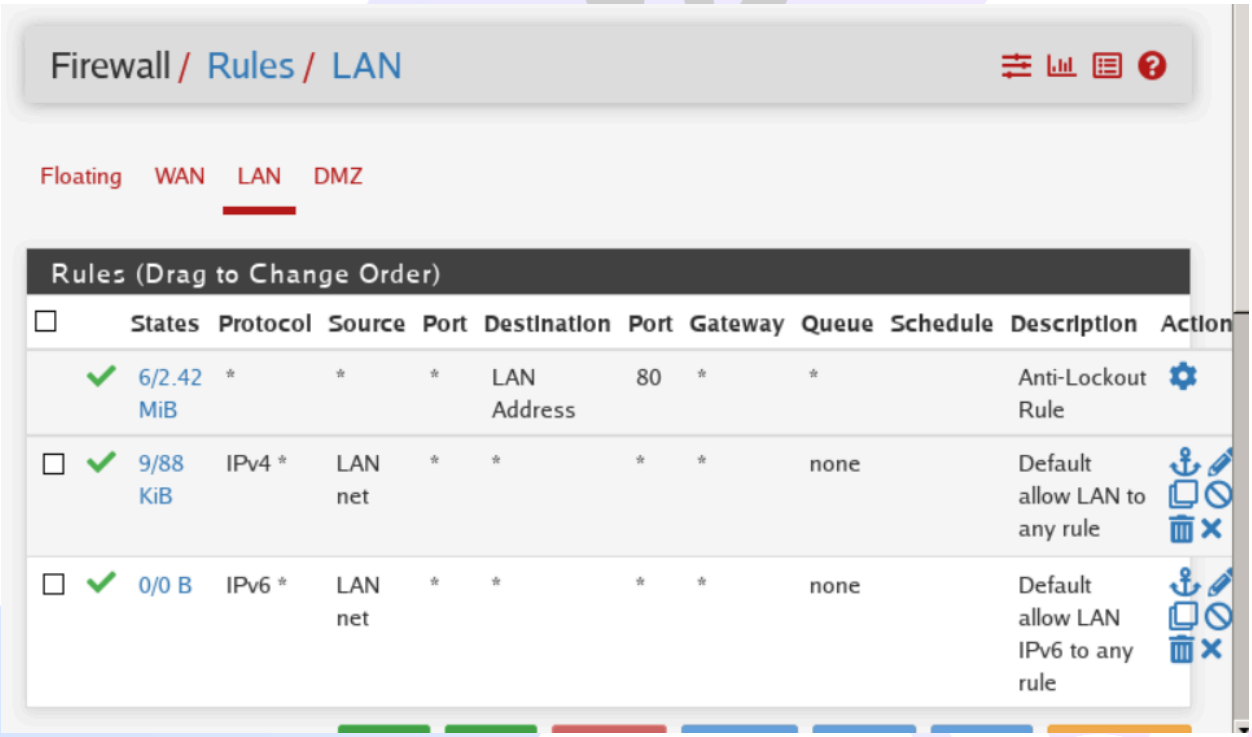
On sauvegarde et applique les changements



```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on Sae201 ***

 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:
```

Mettre en place les règles de filtrage

Configuration des règles :



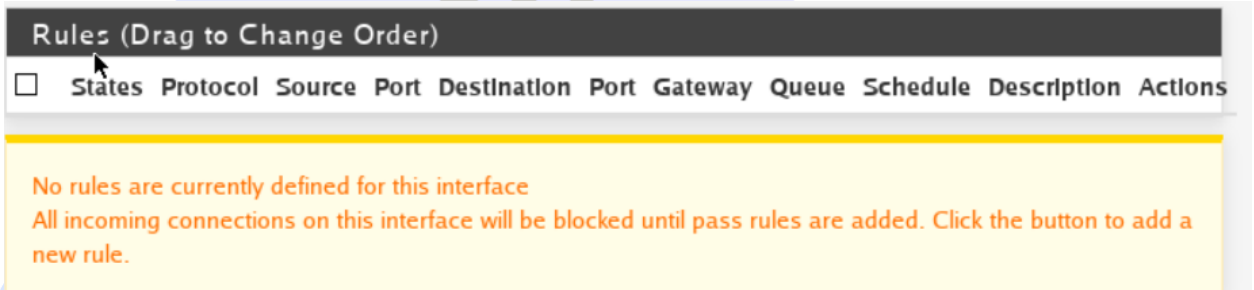
Le LAN est déjà configuré pour accéder à tous les réseaux.
On teste avec le PC connecté au LAN
Sur les serveurs :

```
round-trip min/avg/max = 5.658/15.682/30.430 ms
gns3@box:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
gns3@box:~$ ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5): 56 data bytes
64 bytes from 192.168.1.5: seq=0 ttl=63 time=23.460 ms
64 bytes from 192.168.1.5: seq=1 ttl=63 time=12.361 ms
^C
--- 192.168.1.5 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 12.361/17.910/23.460 ms
gns3@box:~$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3): 56 data bytes
64 bytes from 192.168.1.3: seq=0 ttl=63 time=23.064 ms
64 bytes from 192.168.1.3: seq=1 ttl=63 time=7.318 ms
64 bytes from 192.168.1.3: seq=2 ttl=63 time=16.002 ms
^C
--- 192.168.1.3 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.318/15.461/23.064 ms
gns3@box:~$
```

Sur le NAT

```
gns3@box:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=126 time=94.054 ms
64 bytes from 8.8.8.8: seq=1 ttl=126 time=60.996 ms
64 bytes from 8.8.8.8: seq=2 ttl=126 time=59.395 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 packets received, 25% packet loss
round-trip min/avg/max = 59.395/71.481/94.054 ms
gns3@box:~$
```

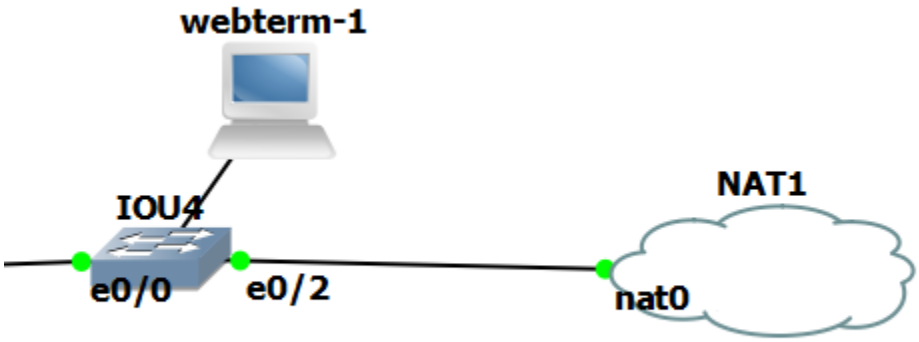
On teste avec les serveurs pour aller sur Internet ils sont DMZ qui n'a pas encore de règles.




```
debian@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 8222ms
```

La partie NAT :

```
root@webterm-1:~# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
19: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOW
N group default qlen 1000
    link/ether 16:bc:ff:c8:bd:e8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.15/24 brd 192.168.122.255 scope global eth0
       valid_lft forever preferred_lft forever
root@webterm-1:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=96.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=75.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=61.3 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3021ms
rtt min/avg/max/mdev = 61.320/77.715/96.600/14.510 ms
root@webterm-1:~#
```

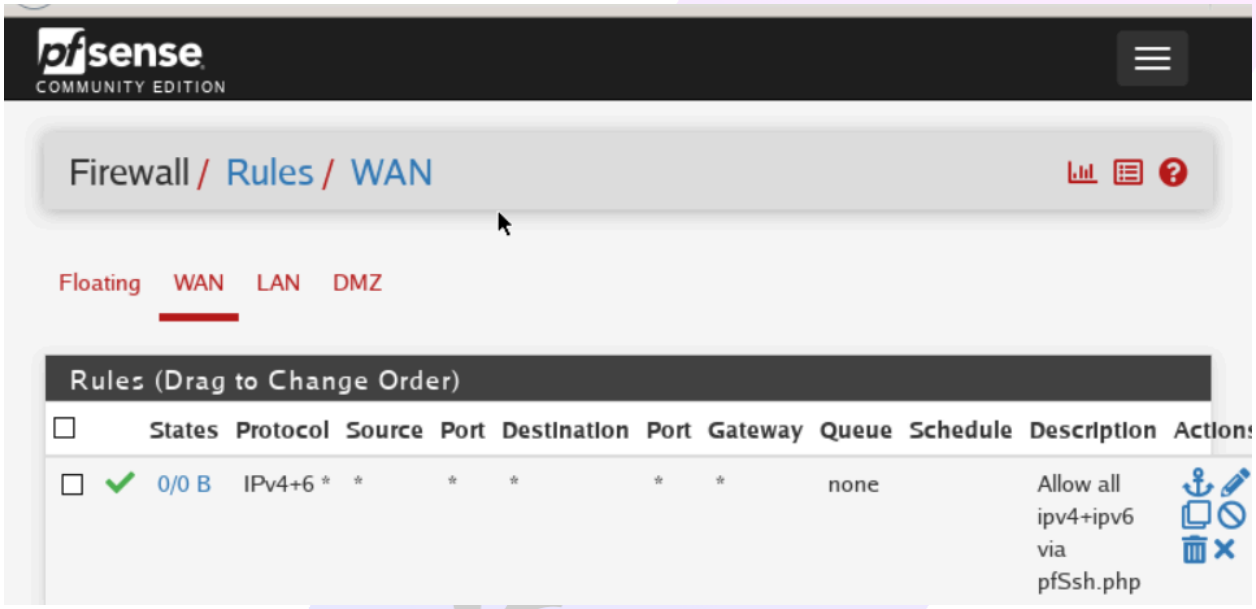


Avec la configuration de base, le réseau NAT ne peut pas aller dans les autres réseaux.

```
root@webterm-1:~# ping 192.168.122.19
PING 192.168.122.19 (192.168.122.19) 56(84) bytes of data.
^C
--- 192.168.122.19 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4095ms
```

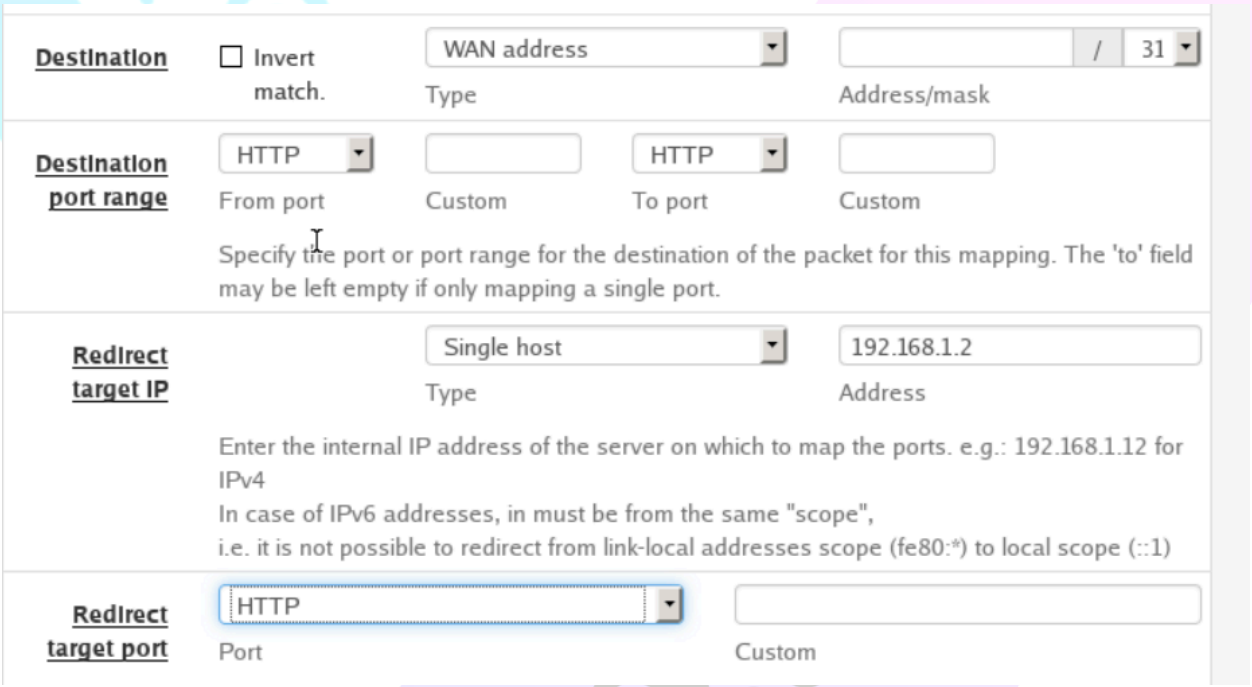
Modification des règles NAT :
Pour que le WAN puisse aller à DMZ.

```
[2.7.0-RELEASE][root@Sae201.rt-iut.re]/root: pfSsh.php playback enableallowallwa
n
Adding allow all rule...
Turning off block private networks (if on)...
Turning off block bogon networks (if on)...
Reloading the filter configuration...
```

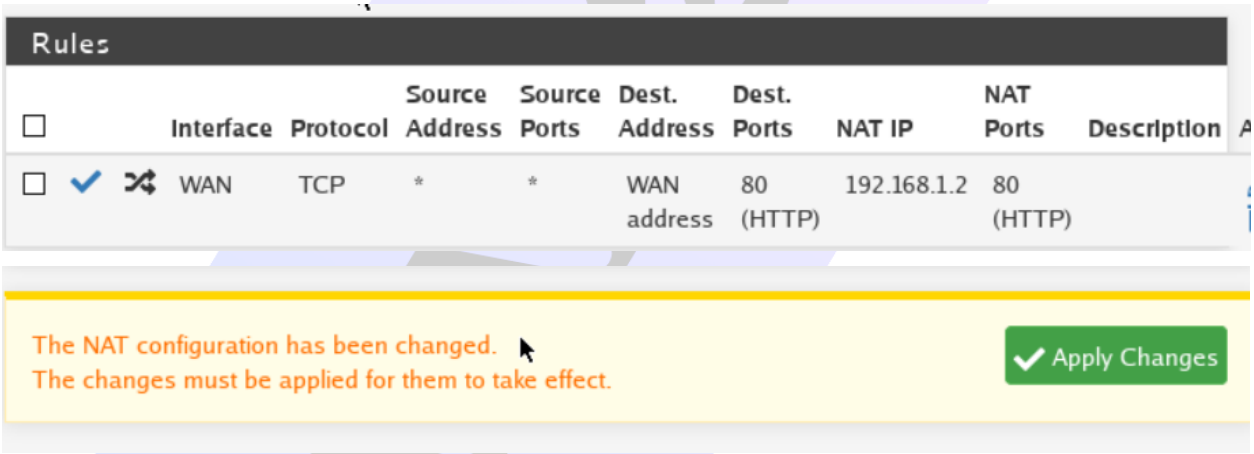



```
root@webterm-1:~# ping 192.168.122.19
PING 192.168.122.19 (192.168.122.19) 56(84) bytes of data.
64 bytes from 192.168.122.19: icmp_seq=1 ttl=64 time=10.5 ms
64 bytes from 192.168.122.19: icmp_seq=2 ttl=64 time=7.58 ms
64 bytes from 192.168.122.19: icmp_seq=3 ttl=64 time=3.15 ms
64 bytes from 192.168.122.19: icmp_seq=4 ttl=64 time=9.99 ms
^C
--- 192.168.122.19 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3039ms
rtt min/avg/max/mdev = 3.146/7.800/10.494/2.904 ms
```

Maintenant le WAN peut accéder au routeur.
On va configurer les services dans la DMZ pour le WAN.
On commence avec HTTP.

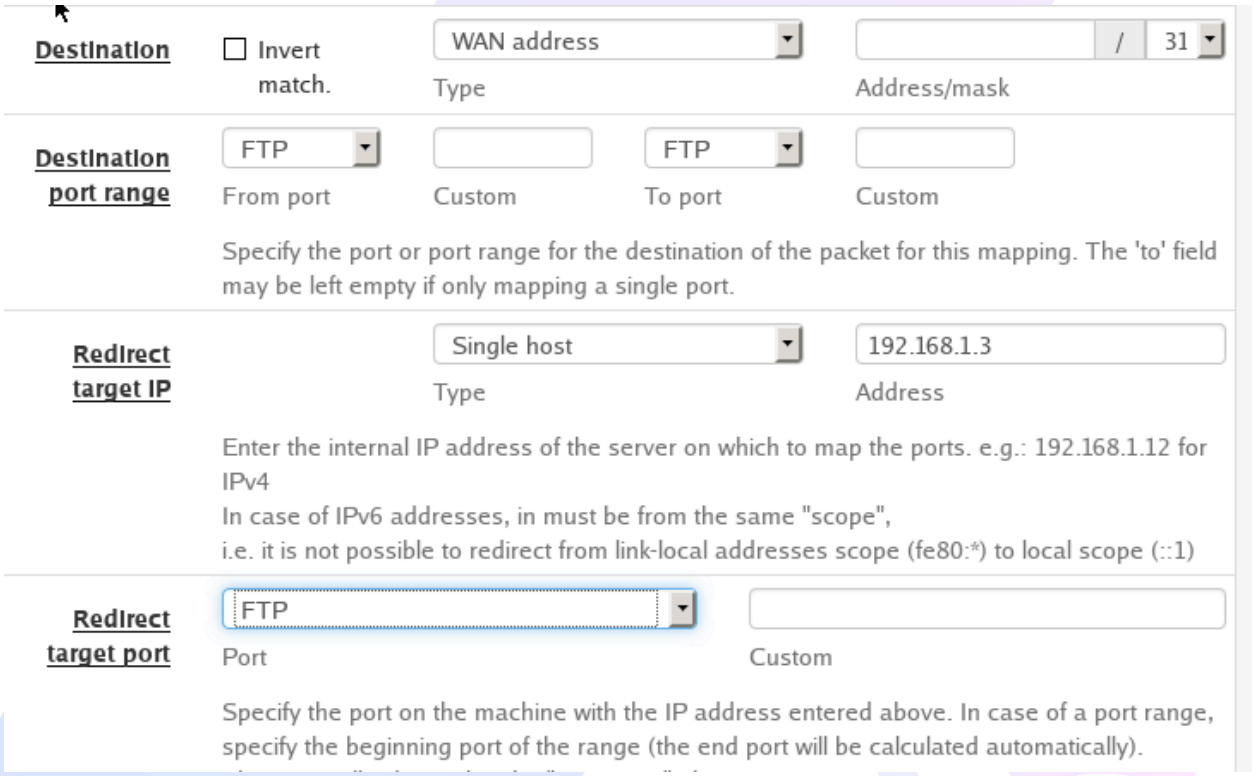


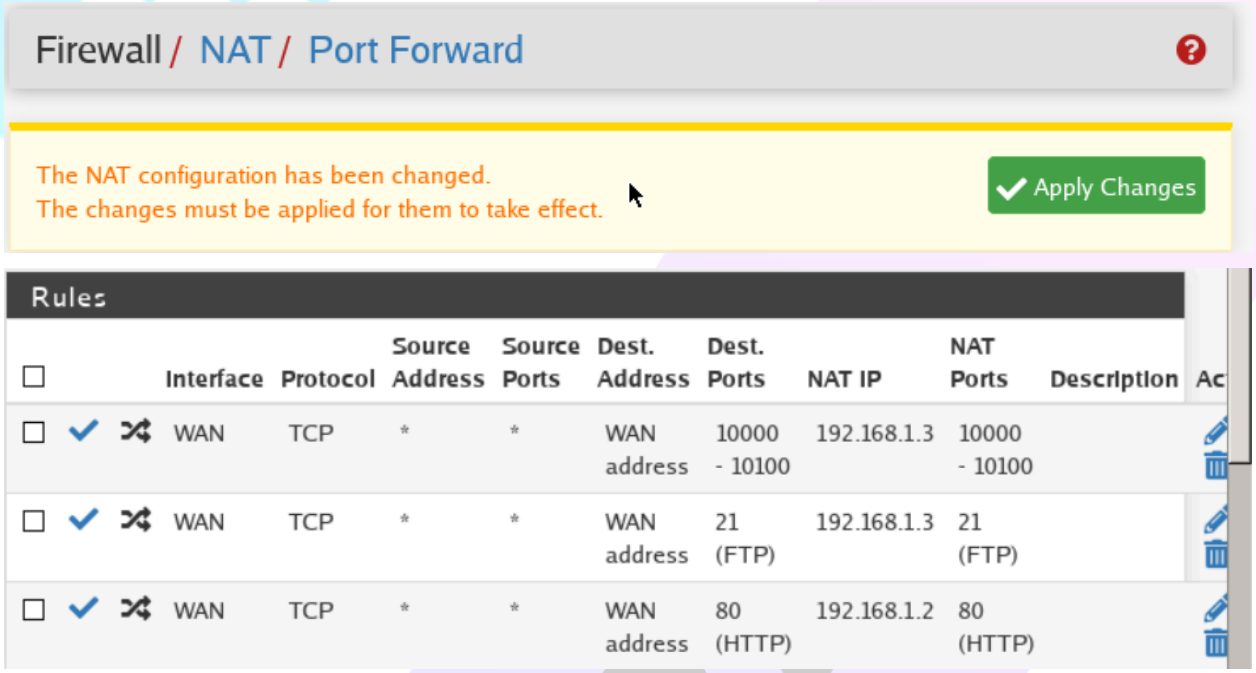
On sauvegarde.



On teste :

Maintenant avec FTP :





Pour le passive mode fonctionne il faut une bonne rangée de port.

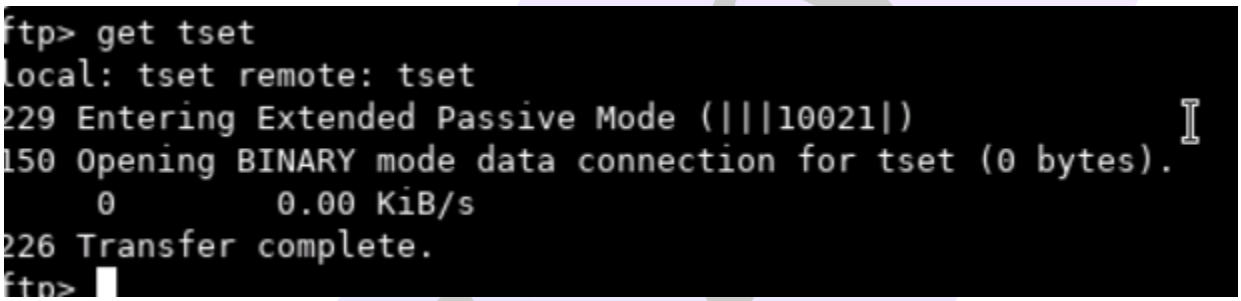
```
root@webterm-1:~# ftp 192.168.122.19
Connected to 192.168.122.19.
220 (vsFTPd 3.0.3)
Name (192.168.122.19:root): user2
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode (|||10082|)
150 Here comes the directory listing.
-rw-r--r--    1 1006     115             0 Jun 14 09:35 incroyable
drwxr-xr-x    2 1006     115          4096 Jun 14 09:01 je
-rwxrwxrwx    1 1006     115             0 Jun 14 09:14 jesuisenttext
lrwxrwxrwx    1 1006     115            16 Jun 14 08:31 shared -> /home/ftp/shar
ed
-rw-r--r--    1 1006     115             0 Jun 14 09:00 tset
226 Directory send OK.
ftp>
```

```
Name (192.168.122.19:root): user2
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put texte.txt
local: texte.txt remote: texte.txt
229 Entering Extended Passive Mode (|||10050|)
150 Ok to send data.
    0        0.00 KiB/s
226 Transfer complete.
ftp> ls -l
229 Entering Extended Passive Mode (|||10096|)
150 Here comes the directory listing.
-rw-r--r--    1 1006     115             0 Jun 14 09:35 incroyable
drwxr-xr-x    2 1006     115          4096 Jun 14 09:01 je
-rwxrwxrwx    1 1006     115             0 Jun 14 09:14 jesuisenttext
lrwxrwxrwx    1 1006     115            16 Jun 14 08:31 shared -> /home/ftp/shar
ed
-rw-r--r--    1 1006     1006            0 Jun 14 17:29 texte.txt
-rw-r--r--    1 1006     115             0 Jun 14 09:00 tset
226 Directory send OK.
ftp>
```

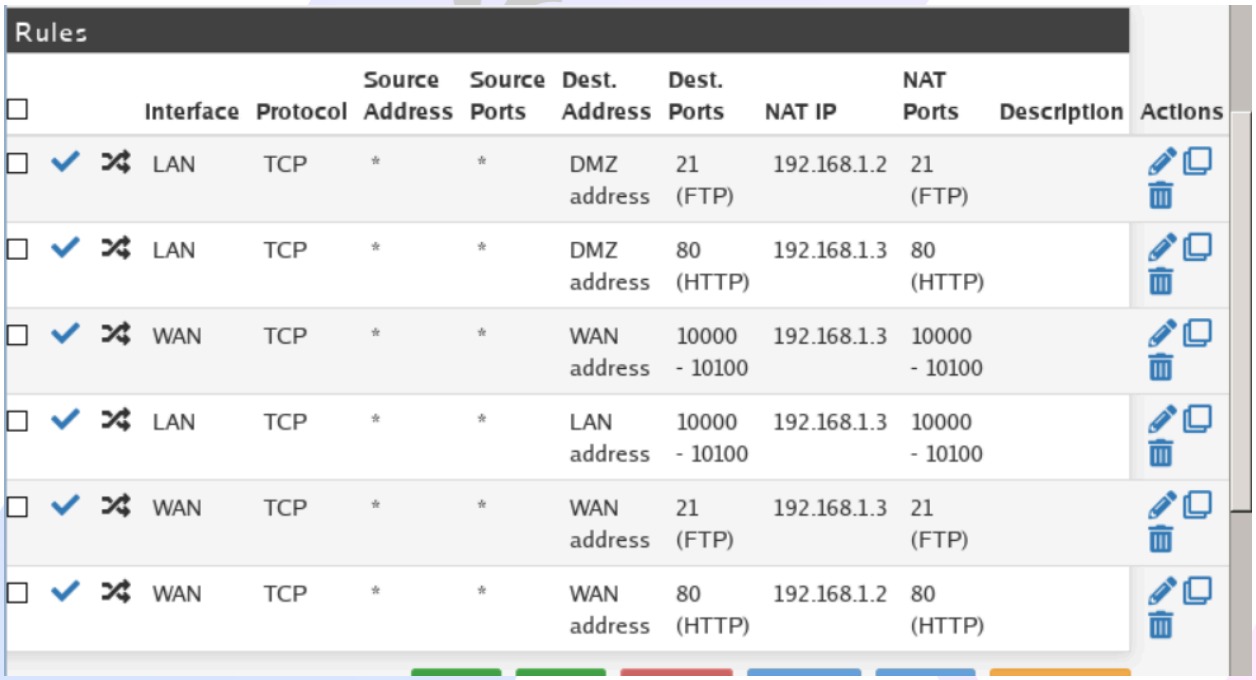
```
ftp> get tset
local: tset remote: tset
229 Entering Extended Passive Mode (|||10021|)
150 Opening BINARY mode data connection for tset (0 bytes).
    0        0.00 KiB/s
226 Transfer complete.
ftp>
```

```
root@webterm-1:~# ls -l
total 0
-rw-r--r-- 1 root root 0 Jun 14 17:29 texte.txt
-rw-r--r-- 1 root root 0 Jun 14 09:00 tset
```

On fait la même chose pour le réseau LAN pour accéder.



Voilà toutes les règles:



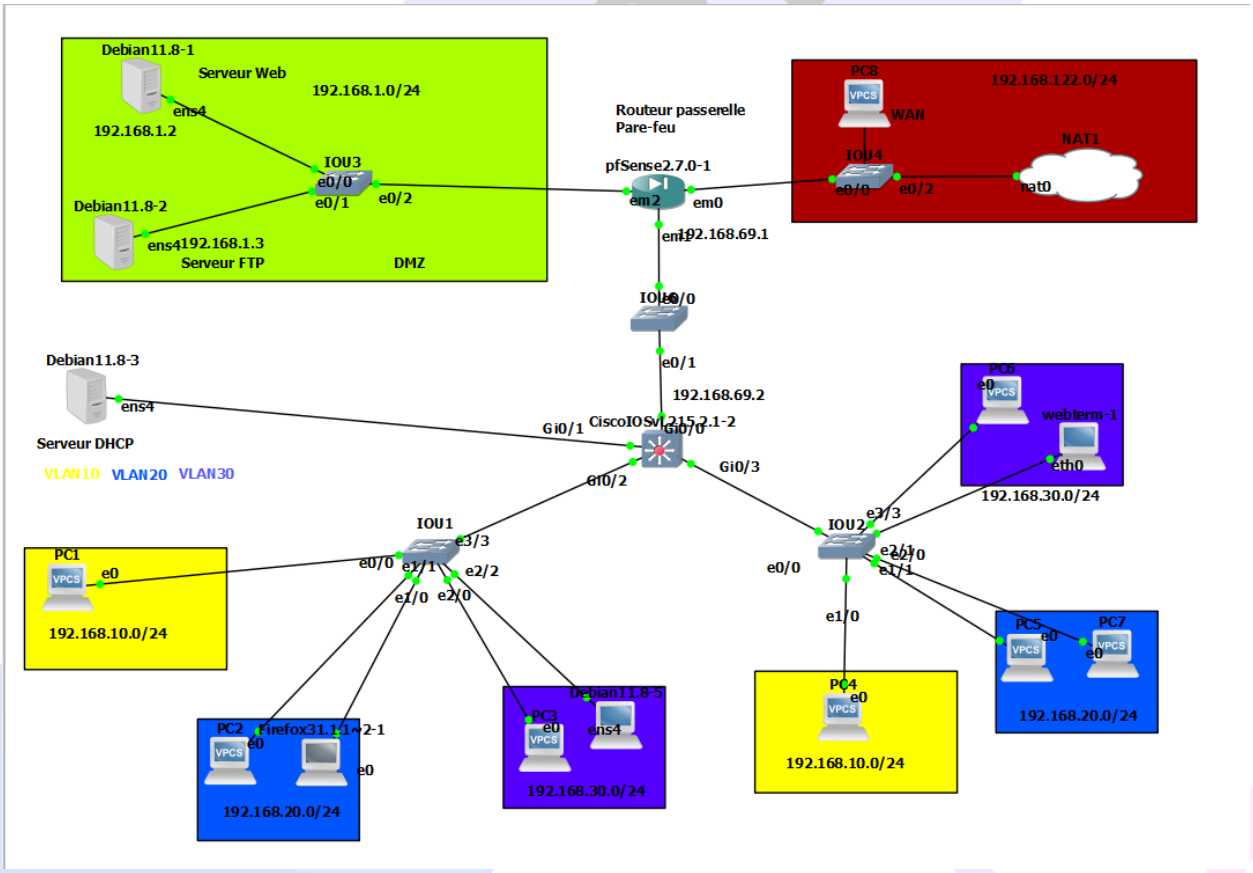
Pour l'accès à internet pour le LAN

☐	✓	47/474 KiB	IPv4	*	*	*	*	*	*	none	ACCES A INTERNET

Tests finaux pour valider les fonctionnalités du réseau d'entreprise (permet de vérifier que le réseau est opérationnel) :

Vérifier qu'un utilisateur interne à l'entreprise peut accéder aux services réseaux installés : Web et FTP (utiliser un objet webterm ou Firefox à la place d'un VPCS : Virtual PC Simulator)

Topologie actuelle pour ce test:

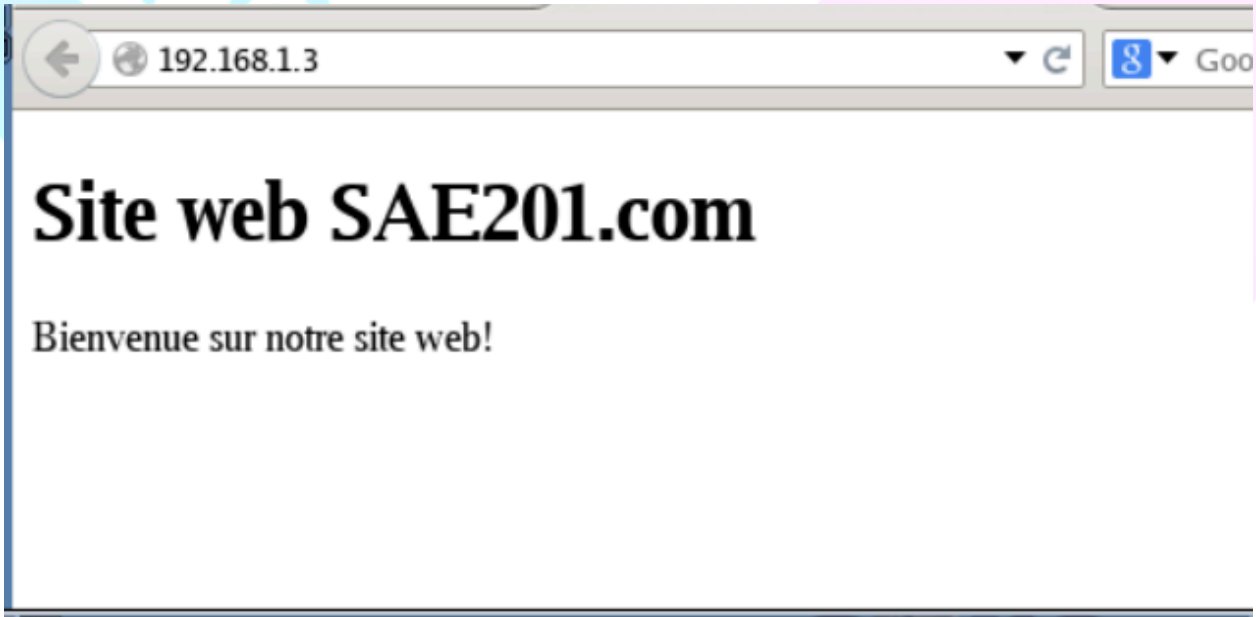


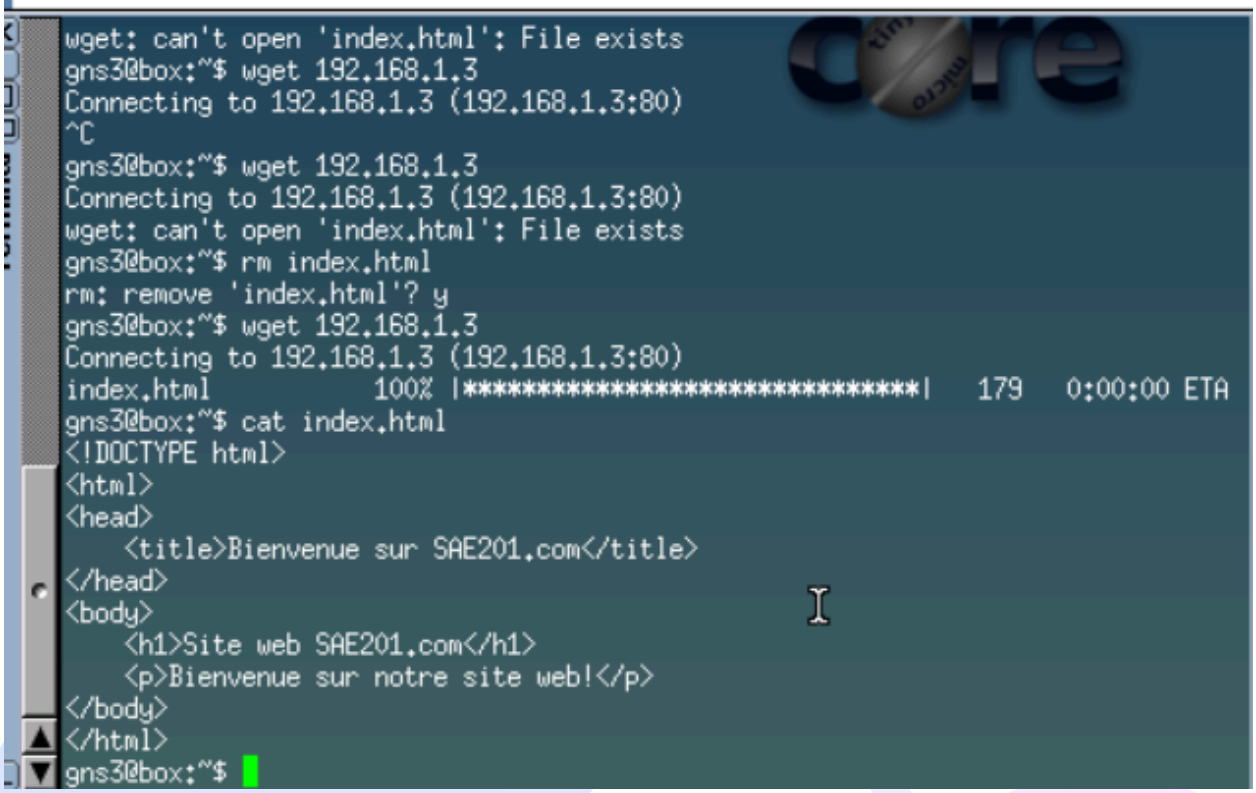
Firefox:

J'ai utilisé une debian 11.8-5 dupliquée pour le FTP car je ne trouve pas le paquet FTP sur firefox.

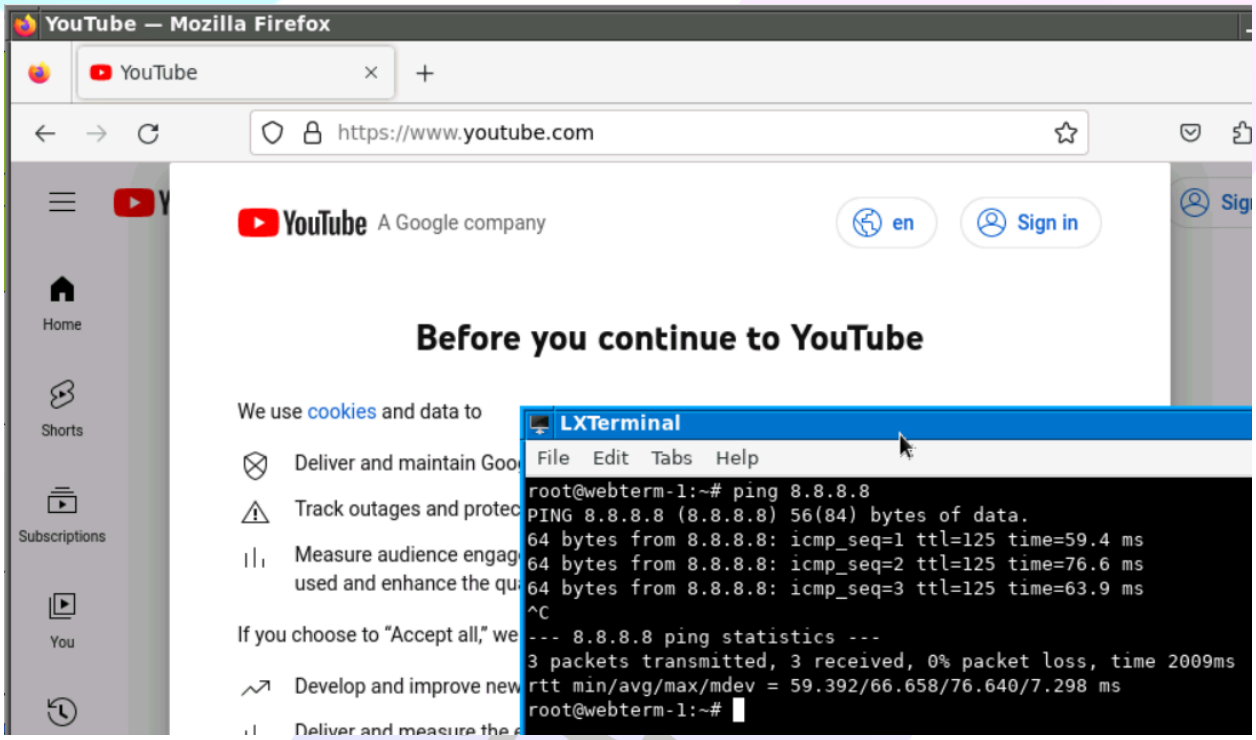
```
debian@debian:~$ ftp 192.168.1.3
Connected to 192.168.1.3.
220 (vsFTPd 3.0.3)
Name (192.168.1.3:debian): user1
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> ls -l
227 Entering Passive Mode (192,168,1,3,39,87).
150 Here comes the directory listing.
lrwxrwxrwx    1 1005     115            16 Jun 14 08:31 shared -> /home/ftp/shar
ed
-rw-r--r--    1 1005     1005            0 Jun 14 08:53 tset
226 Directory send OK.
ftp> get tset
local: tset remote: tset
227 Entering Passive Mode (192,168,1,3,39,78).
150 Opening BINARY mode data connection for tset (0 bytes).
226 Transfer complete.
ftp> exit
221 Goodbye.
debian@debian:~$ ls -l
total 0
-rw-r--r-- 1 debian debian 0 Jun 15 09:34 tset
debian@debian:~$
```


SAE 201 - Recherche ...
Sae201.rt-iut.re - Firewa...
Bienvenue sur SAE201.com
https://www.google.com/search?client=firefox-a&sca_esv=
Google
Google
SAE 201
Tous
Images
Vidéos
Maps
Actualités
Livres
Outils de recherche
formations.unistra.fr › formations › but-BT › sae-201-EN41359
SAÉ 201 - Catalogue des formations - Univ Strasbourg
Ressources et SAE Semestre 2; SAÉ 201. SAÉ. SAÉ 201. TEDS / DDRS (Transition écologique
pour un développement soutenable). Composante: IUT de Haguenau ...


192.168.1.3
Site web SAE201.com
Bienvenue sur notre site web!

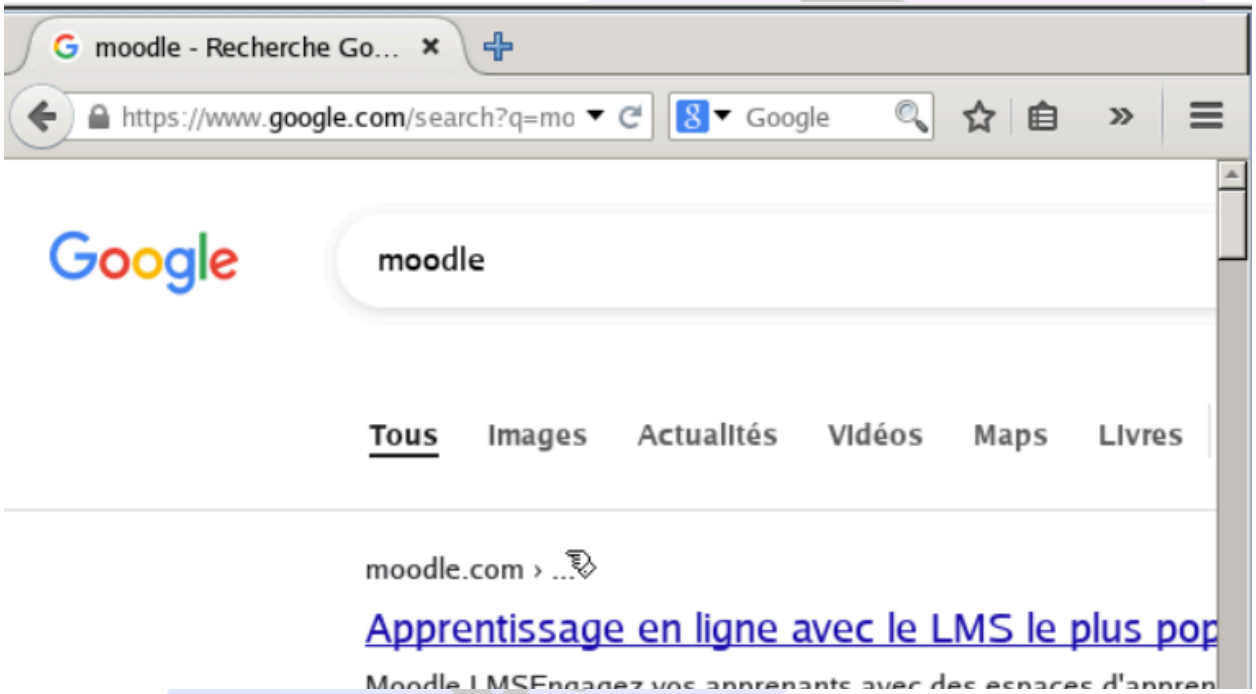

wget: can't open 'index.html': File exists
gns3@box:~$ wget 192.168.1.3
Connecting to 192.168.1.3 (192.168.1.3:80)
^C
gns3@box:~$ wget 192.168.1.3
Connecting to 192.168.1.3 (192.168.1.3:80)
wget: can't open 'index.html': File exists
gns3@box:~$ rm index.html
rm: remove 'index.html'? y
gns3@box:~$ wget 192.168.1.3
Connecting to 192.168.1.3 (192.168.1.3:80)
index.html 100% |*****| 179 0:00:00 ETA
gns3@box:~$ cat index.html
<!DOCTYPE html>
<html>
<head>
<title>Bienvenue sur SAE201.com</title>
</head>
<body>
<h1>Site web SAE201.com</h1>
Bienvenue sur notre site web!
</body>
</html>
gns3@box:~$

Vérifier qu'un utilisateur interne à l'entreprise peut se connecter à Internet



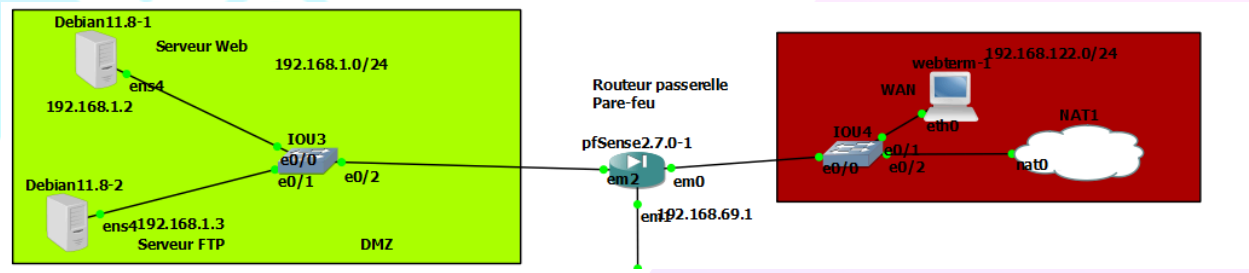

```
root@webterm-1:~# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
8: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN
 group default qlen 1000
    link/ether f2:b5:76:bb:68:e4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.30.105/24 scope global eth0
       valid_lft forever preferred_lft forever
```

```
gns3@box:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=125 time=58.969 ms
64 bytes from 8.8.8.8: seq=1 ttl=125 time=58.839 ms
64 bytes from 8.8.8.8: seq=2 ttl=125 time=66.422 ms
64 bytes from 8.8.8.8: seq=3 ttl=125 time=57.272 ms
64 bytes from 8.8.8.8: seq=4 ttl=125 time=58.958 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 5 packets received, 16% packet loss
round-trip min/avg/max = 57.272/60.092/66.422 ms
```



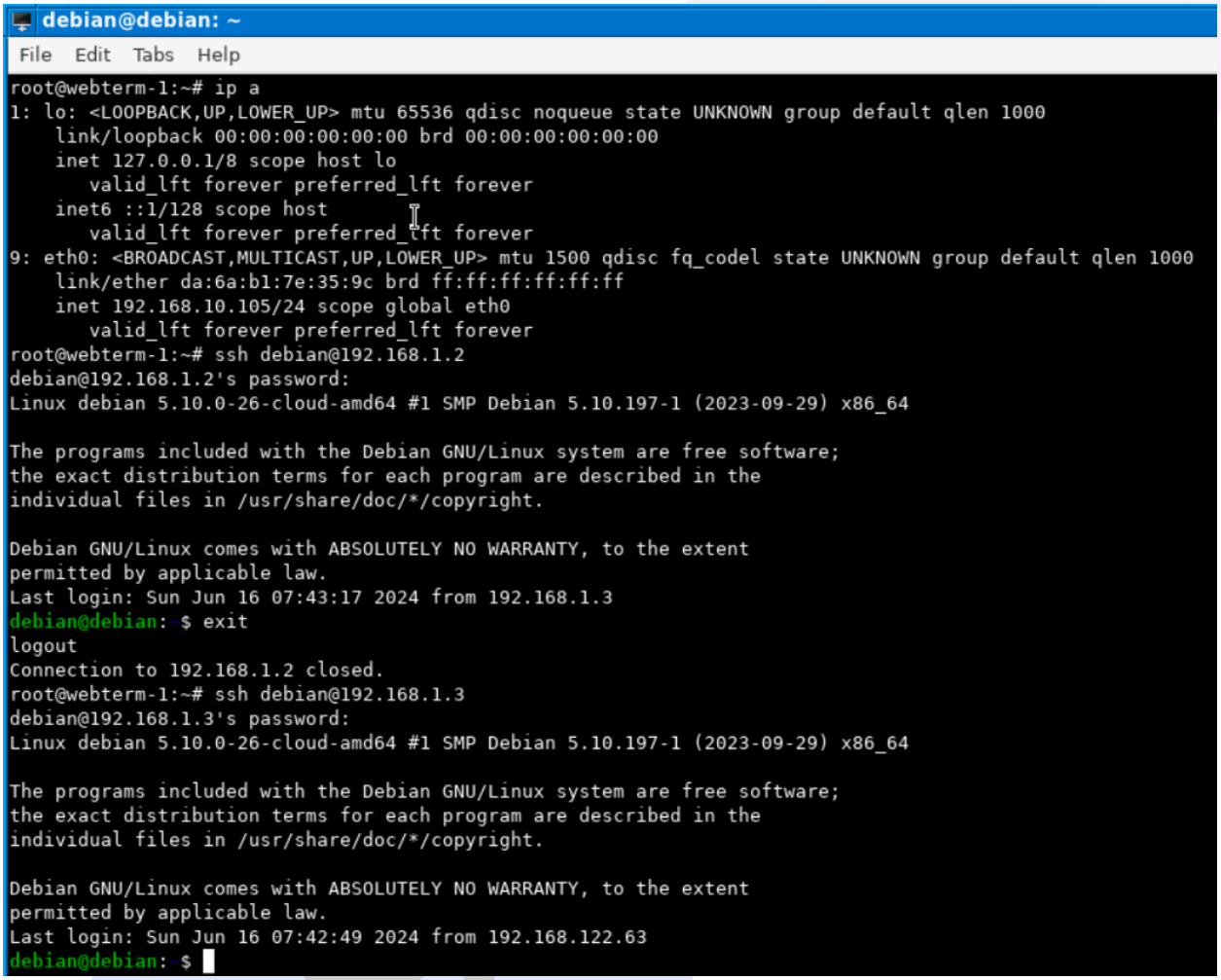
Vérifier si un utilisateur externe à l'entreprise peut se connecter au serveur Web ou FTP depuis l'extérieur (placer un objet webterm ou Firefox dans la partie WAN)

topologie actuelle:

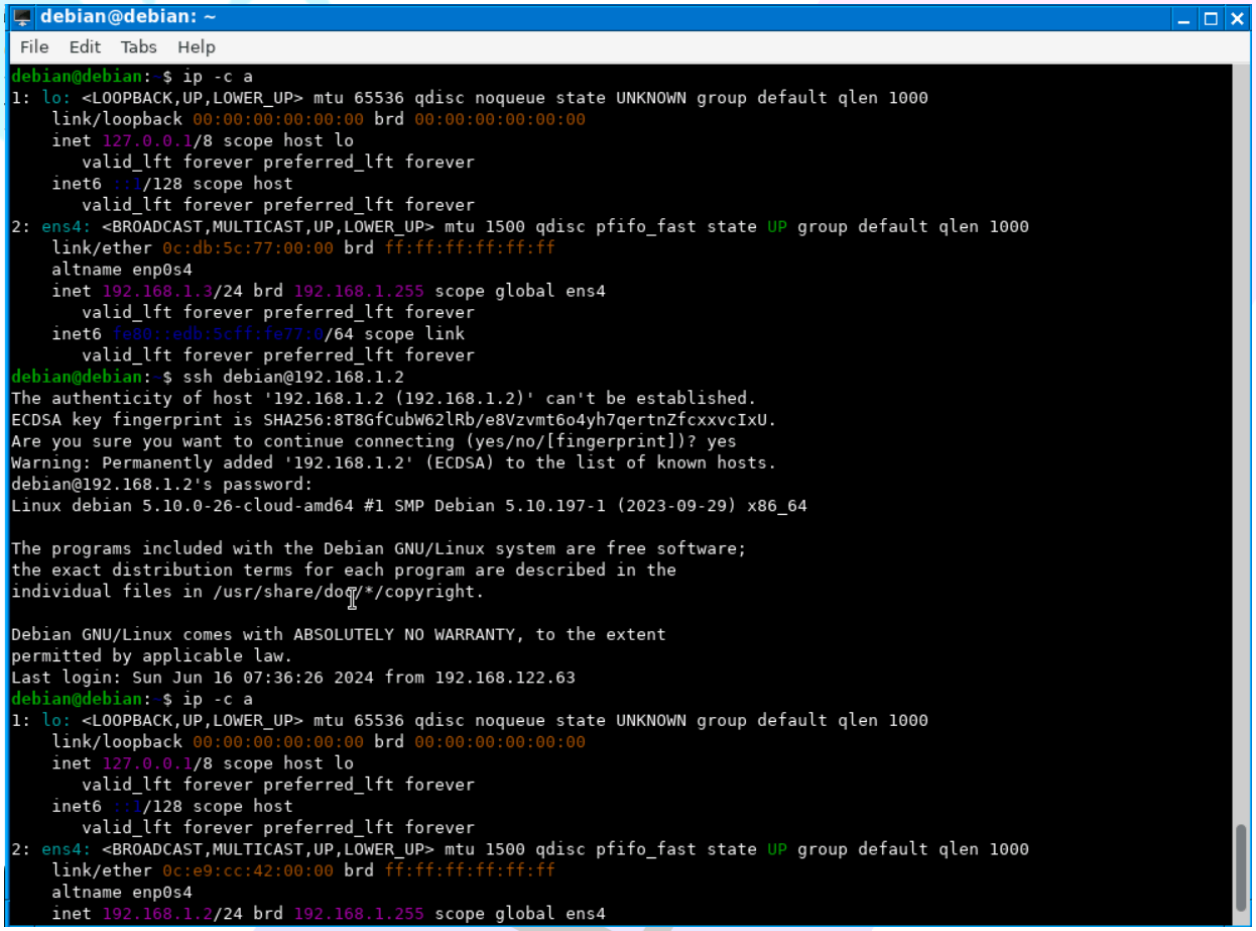



```
root@webterm-1:~# ftp 192.168.122.19
Connected to 192.168.122.19.
220 (vsFTPd 3.0.3)
Name (192.168.122.19:root): user2
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode (|||10099|)
150 Here comes the directory listing.
-rw-r--r--    1 1006     115             0 Jun 14 09:35 incroyable
drwxr-xr-x    2 1006     115          4096 Jun 14 09:01 je
-rwxrwxrwx    1 1006     115             0 Jun 14 09:14 jesuisenttext
lrwxrwxrwx    1 1006     115            16 Jun 14 08:31 shared -> /home/ftp/shared
-rw-r--r--    1 1006     1006            0 Jun 14 17:29 texte.txt
-rw-r--r--    1 1006     115             0 Jun 14 09:00 tset
226 Directory send OK.
ftp> get texte.txt
local: texte.txt remote: texte.txt
229 Entering Extended Passive Mode (|||10049|)
150 Opening BINARY mode data connection for texte.txt (0 bytes).
    0        0.00 KiB/s
226 Transfer complete.
```

Vérifier si l'administrateur réseau de l'entreprise peut gérer les équipements à l'aide d'une connexion SSH à l'intérieur de l'entreprise



Vérifier si l'administrateur réseau de l'entreprise peut gérer les équipements à l'aide d'une connexion SSH hors de l'entreprise


debian@debian: ~
File Edit Tabs Help
debian@debian: $ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 0c:db:5c:77:00:00 brd ff:ff:ff:ff:ff:ff
altname enp0s4
inet 192.168.1.3/24 brd 192.168.1.255 scope global ens4
valid_lft forever preferred_lft forever
inet6 fe80::edb:5cff:fe77:0/64 scope link
valid_lft forever preferred_lft forever
debian@debian: $ ssh debian@192.168.1.2
The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established.
ECDSA key fingerprint is SHA256:8T8GfCubW62lRb/e8Vzvmt6o4yh7qertnZfcxxvcIxU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.2' (ECDSA) to the list of known hosts.
debian@192.168.1.2'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 07:36:26 2024 from 192.168.122.63
debian@debian: $ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 0c:e9:cc:42:00:00 brd ff:ff:ff:ff:ff:ff
altname enp0s4
inet 192.168.1.2/24 brd 192.168.1.255 scope global ens4