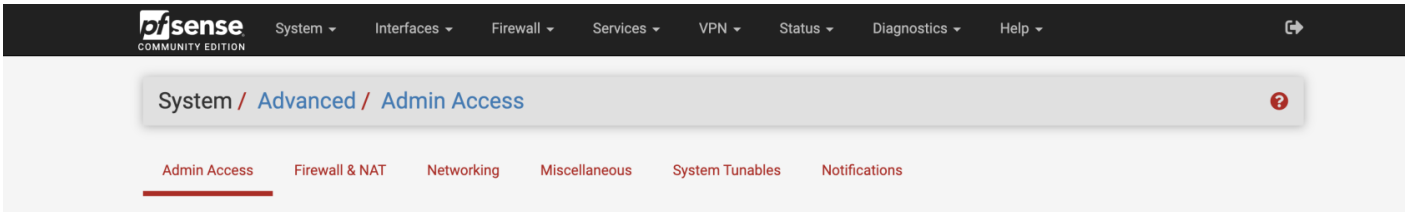
Ajouter PfSense à l'active directory

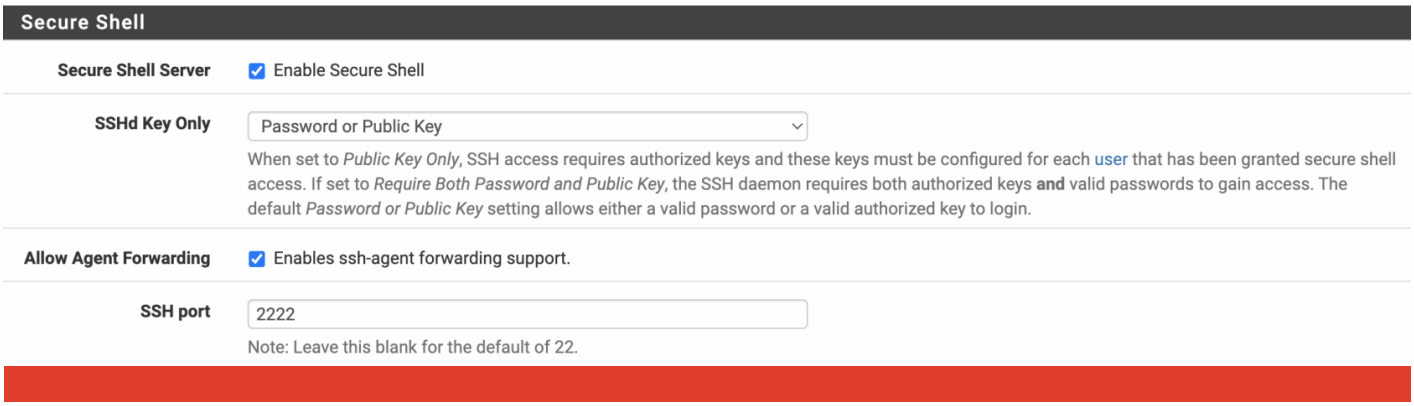
On va commencer par activer le secure shell pour administrer la VM en ssh.

Acceder à PfSense -> System -> Advanced -> Admin Access



Enable + Enable ssh-agent

On renseigne le ssh port en **2222**



Se connecter en ssh à l'infra **192.168.1.4** dans mon cas.

Puis se connecter au PfSense

```
ssh root@192.168.1.4 -p 2222
```

(user@ipPfsense -p PortConfiguré)

```
jules@MacBook-Pro-de-Navarro ~ % ssh jg@192.168.1.4
jg@192.168.1.4's password:
Linux adm-front-01 6.8.4-2-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.4-2 (2024-04-10T17:36Z)
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: Tue Dec 10 10:17:56 2024 from 192.168.1.21
❯ ssh root@192.168.1.4 -p 2222
KVM Guest - Netgate Device ID: 2f8a84bd2402715342fc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on fw-front-01 ***

 WAN (wan)       -> vtnet0     -> v4: 192.168.1.4/26
 LAN (lan)       -> vtnet1     -> v4: 172.16.1.1/27
 DMZ (opt1)      -> vtnet2     -> v4: 10.10.10.1/28

 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) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

Option 8 (Shell)

On va éditer :

```
/usr/local/etc/pkg/repos/pfSense.conf
```

```
FreeBSD: { enabled: yes }


pfSense-core: {
    url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",
    mirror_type: "srv",
    signature_type: "fingerprints",
    fingerprints: "/usr/local/share/pfSense/keys/pkg",
    enabled: yes
}
```

```
pfSense: {
    url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-pfSense_v2_7_2",
    mirror_type: "srv",
    signature_type: "fingerprints",
    fingerprints: "/usr/local/share/pfSense/keys/pkg",
    enabled: yes
}
```

ET

```
/usr/local/etc/pkg/repos/FreeBSD.conf
```

```
            FreeBSD: {
                url: "pkg+https://pkg.freebsd.org/${ABI}/latest",
                enabled: true,
                signature_type: "fingerprints",
                fingerprints: "/usr/share/keys/pkg",
                mirror_type: "srv"
            }
```

On installe maintenant les packets

```
pkg install -y adcli sssd2 samba416
```

Une fois installés, on va éditer :

```
/etc/krb5.conf
```

```
[logging]
default = FILE:/var/log/krb5libs.log

[libdefaults]
default_realm = megaproduction.local
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true
rdns = false
```

default_realm = Nom de domaine

```
/usr/local/etc/smb4.conf
```

```
[global]
security = ads
realm = MEGAPRODUCTION.LOCAL
workgroup = MEGAPRODUCTION
log file = /var/log/samba/%m.log
log level = 3
kerberos method = secrets and keytab
client signing = yes
load printers = no
cups options = raw
printcap name = /dev/null
ntlm auth = disabled
idmap config MYDOMAIN: backend = sss
idmap config MYDOMAIN: range = 200000-2147483647
idmap config * : backend = tdb
idmap config * : range   = 100000-199999
inherit acls = no
server min protocol = SMB3
map to guest = bad user
unix extensions = no
```

(EN MAJUSCULE)

realm = NOM DE DOMAINE.LOCAL
workgroup = NOM DE DOMAINE

On redémarre les services

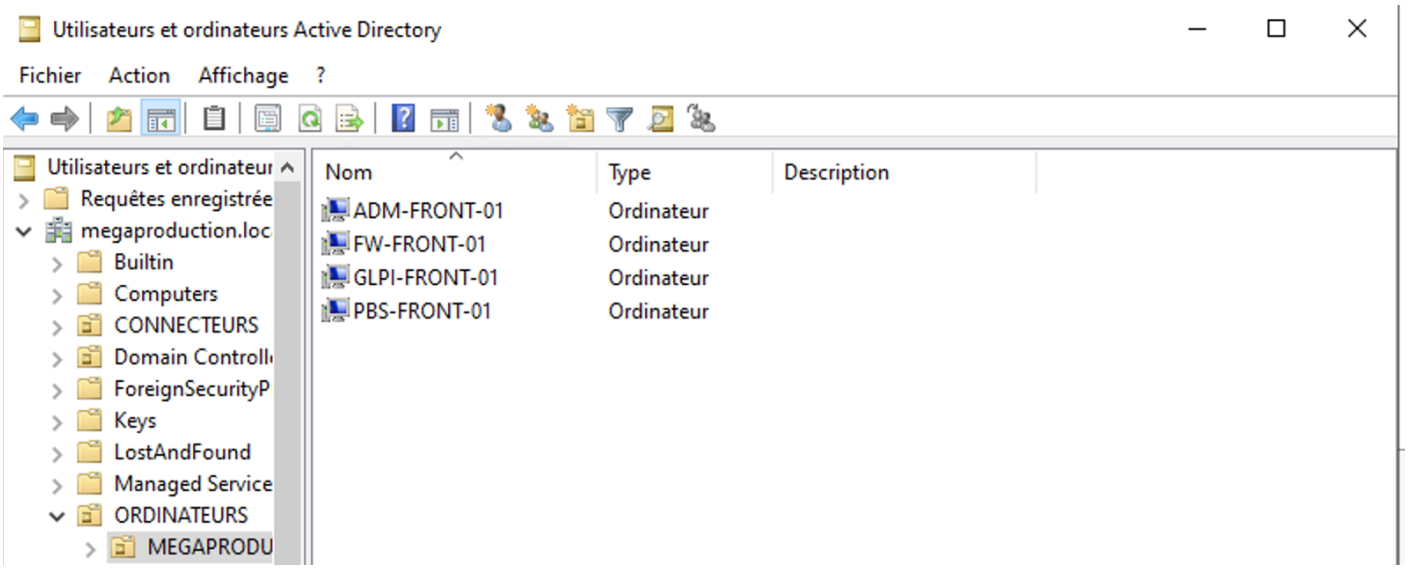
```
service kerberos restart && service samba_server restart
```

Maintenant, on va pouvoir découvrir la machine :

```
net ads join -U administrateur@megaproduction.local
```

```
[2.7.2-RELEASE][admin@fw-front-01.megaproduction.local]/root: net ads join -U administ
rateur@megaproduction.local
Password for [administrateur@megaproduction.local]:
Using short domain name -- MEGAPRODUCTION
Joined 'FW-FRONT-01' to dns domain 'megaproduction.local'
```

Voilà la machine est maintenant ajoutée à l'AD.



Revision #3
Created 2024-12-11 07:47:54 UTC by Seluj
Updated 2025-01-14 07:31:55 UTC by Seluj