



INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

RAPPORT DE PROJET

CONCEVOIR ET DÉPLOYER UN RÉSEAU DE PETITES ENTREPRISES

Projet réalisé par

Nhat Huy TRAN

Année 2024-2025

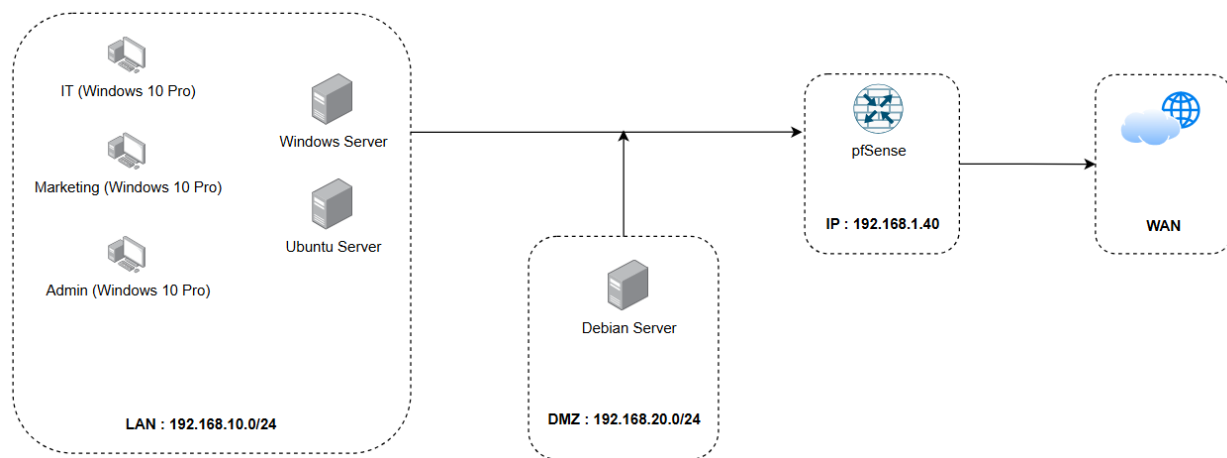
TABLE DES MATIÈRES

I. Présentation du projet	2
II. Composants du projet	3
1. Réseau LAN:.....	3
2. Réseau DMZ:	4
3. PfSense (Firewall/Routeur):.....	4
III. Détails de la configuration	5
IV. Fonctionnalités principales	6
1. Serveur Debian:	6
2. Serveur Windows 2022:	6
3. Serveur Ubuntu:	9
4. PfSense:.....	10
V. Conclusion	15

I. Présentation du projet

Ce projet consiste à simuler l'infrastructure réseau d'une petite entreprise. Le réseau est divisé en trois segments principaux : **réseau LAN (Local Area Network)**, **réseau DMZ (Demilitarized Zone)** et **réseau WAN (Wide Area Network)**. L'objectif du projet est de créer un système réseau sécurisé, avec un contrôle d'accès efficace et permettant une gestion à distance des serveurs internes.

Étant donné que je n'ai pas les ressources matérielles (câble ethernet, routeur, communicateur, pare-feu, imprimante,...) et que mon ordinateur portable est limité à 16 Go de RAM, je vais simuler l'ensemble du système sur VMware.



L'adresse IP **192.168.1.40** joue le rôle d'IP publique du système. Par conséquent, la machine hôte (**192.168.1.x**) est considérée comme étant sur le réseau **WAN**.

II. Composants du projet

1. Réseau LAN:

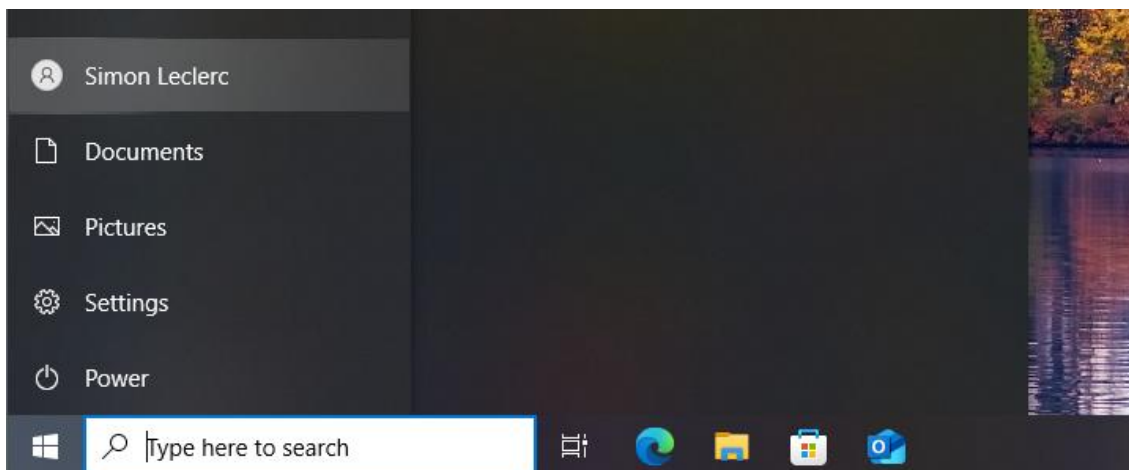
- **Serveur Windows Server 2022** : Il est configuré avec les services IIS, DNS, Active Directory (AD) et SMB.



- **Serveur Ubuntu** : Fournit des services de gestion des utilisateurs et du système.

```
simon@ubuntu-server:/home$ ls
martin simon
simon@ubuntu-server:/home$ 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e9:43:9d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.56/24 metric 100 brd 192.168.10.255 scope global dynamic ens33
        valid_lft 5492sec preferred_lft 5492sec
    inet6 fe80::20c:29ff:fee9:439d/64 scope link
        valid_lft forever preferred_lft forever
simon@ubuntu-server:/home$
```

- **3 ordinateurs Windows 10 Pro** : Utilisés par les trois employés de l'entreprise.



2. Réseau DMZ:

- **Serveur Debian** : Fournit des services web et FTP accessibles publiquement depuis le réseau WAN.

```
user@debian-server:~$ 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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:17:40:51 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.51/24 brd 192.168.20.255 scope global dynamic ens33
        valid_lft 5582sec preferred_lft 5582sec
    inet6 fe80::20c:29ff:fe17:4051/64 scope link
        valid_lft forever preferred_lft forever
user@debian-server:~$
```

3. PfSense (Firewall/Routeur):

Un firewall/routeur avec trois cartes réseau configurées pour segmenter les trois parties du réseau (LAN, WAN, DMZ).

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.40/24
                                v6/DHCP6: 2001:861:5d00:ab20:20c:29ff:fe64:7e2
e/64
LAN (lan)      -> em1      -> v4: 192.168.10.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.20.1/24

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
```

The screenshot shows the pfSense web interface in a browser. The address bar indicates the URL is <https://192.168.10.1>. The page title is "Status / Dashboard". The main content area is divided into two panels. The left panel, titled "System Information", contains details about the system, including the name "pfSense.home.arpa", user "admin@192.168.10.54", system "VMware Virtual Machine", BIOS vendor "Phoenix Technologies LTD", and version "2.7.2-RELEASE (amd64)". The right panel, titled "Netgate Services And Support", shows the contract type as "Community Support" and provides links to "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES".




System Information	
Name	pfSense.home.arpa
User	admin@192.168.10.54 (Local Database)
System	VMware Virtual Machine Netgate Device ID: ef3fae5c1230b684211b
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Mon Mar 4 20:53:00 CET 2024 FreeBSD 14.0-CURRENT

Netgate Services And Support	
Contract type	Community Support Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES	
If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY .	

III. Détails de la configuration

PfSense dispose de trois cartes réseau:

- **Bridged** : Connexion entre les segments de réseau.
- **Lan Segment DMZ** : Connexion au réseau DMZ.
- **Lan Segment LAN** : Connexion au réseau LAN.

Interfaces			
 WAN	↑	1000baseT <full-duplex>	192.168.1.40 2001:861:5d00:ab20:20c:29ff:fe64:7e2e
 LAN	↑	1000baseT <full-duplex>	192.168.10.1
 DMZ	↑	1000baseT <full-duplex>	192.168.20.1

Serveur Debian : Configuré avec une carte réseau connectée au **Lan Segment DMZ**.

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:17:40:51 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.20.51/24 brd 192.168.20.255 scope global dynamic ens33
        valid_lft 5582sec preferred_lft 5582sec
    inet6 fe80::20c:29ff:fe17:4051/64 scope link
        valid_lft forever preferred_lft forever
user@debian-server:~$ _
```

Serveurs Windows 2022, Windows 10 Pro, Serveur Ubuntu : Ces machines ont une carte réseau connectée au **Lan Segment LAN**.

```
C:\Users\simon>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : home.arpa
    Link-local IPv6 Address . . . . . : fe80::2d7a:529e:1c06:ffe1%8
    IPv4 Address. . . . . : 192.168.10.55
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

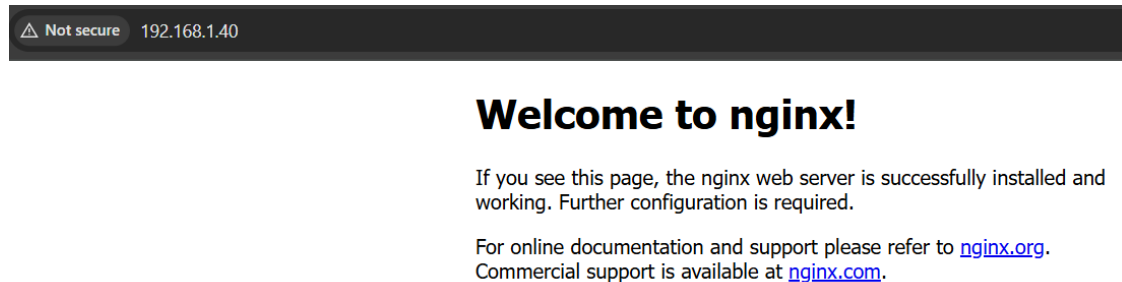
Ethernet adapter Bluetooth Network Connection:
```

Architecture du réseau : Les machines du LAN peuvent accéder au WAN et à la DMZ. Le WAN peut accéder à la DMZ pour utiliser des services publics tels que le web et FTP. Cependant, **le WAN et la DMZ ne peuvent pas accéder au LAN**.

IV. Fonctionnalités principales

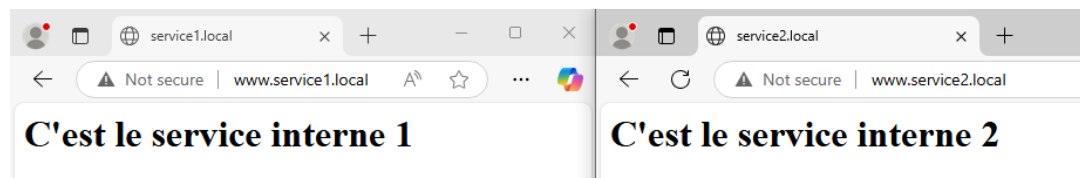
1. Serveur Debian:

- Fournit des services **Web** et **FTP** accessibles depuis le réseau WAN. Ces services sont accessibles publiquement via les ports appropriés.

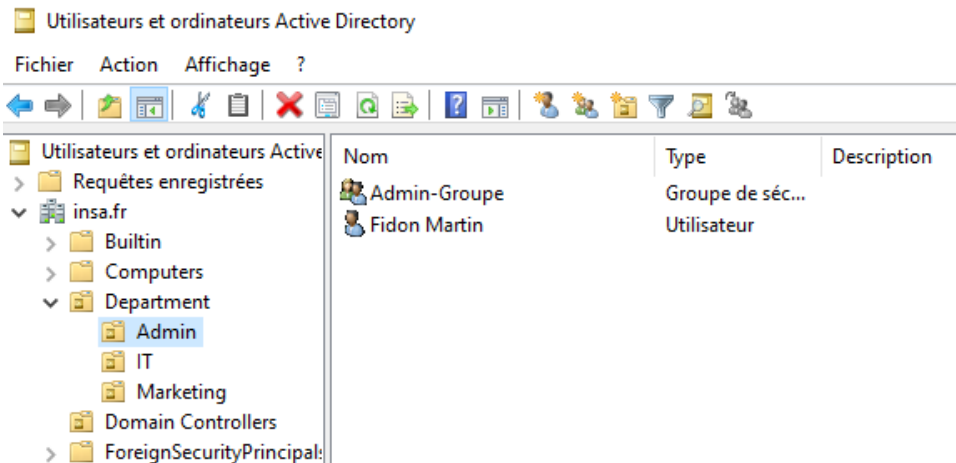


2. Serveur Windows 2022:

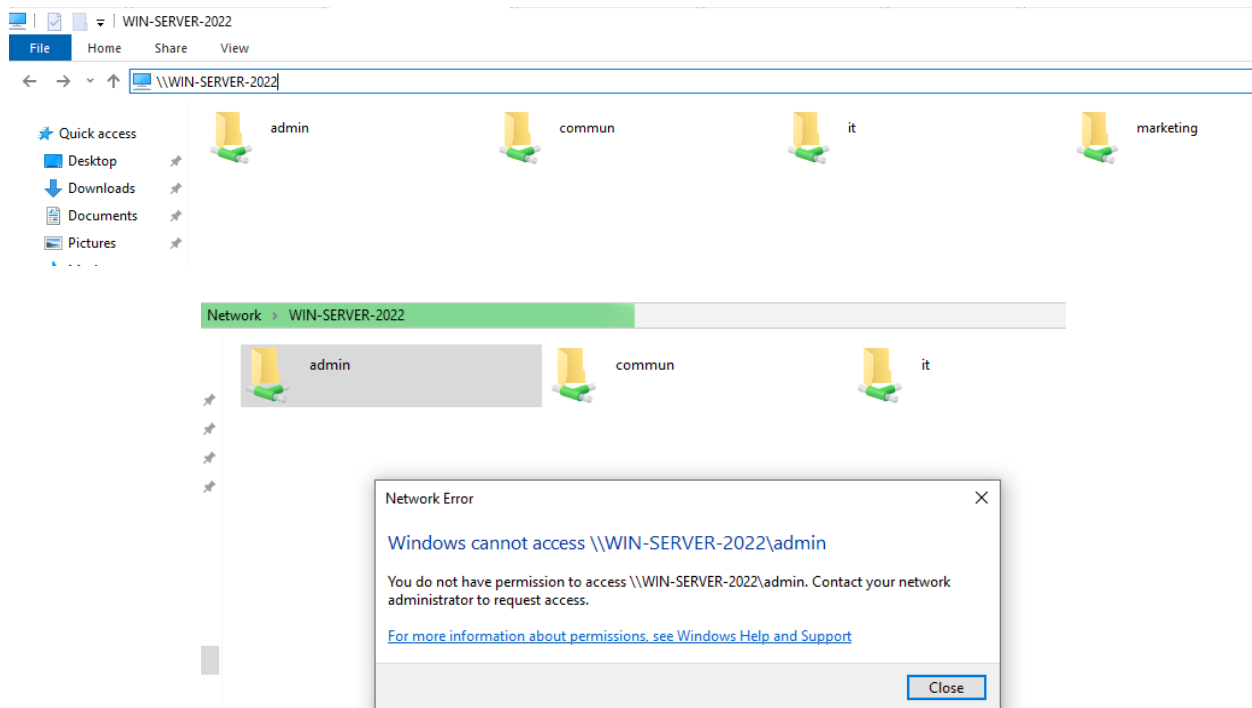
- **Services IIS** : Crée des sites web internes tels que **service1.local** et **service2.local**.

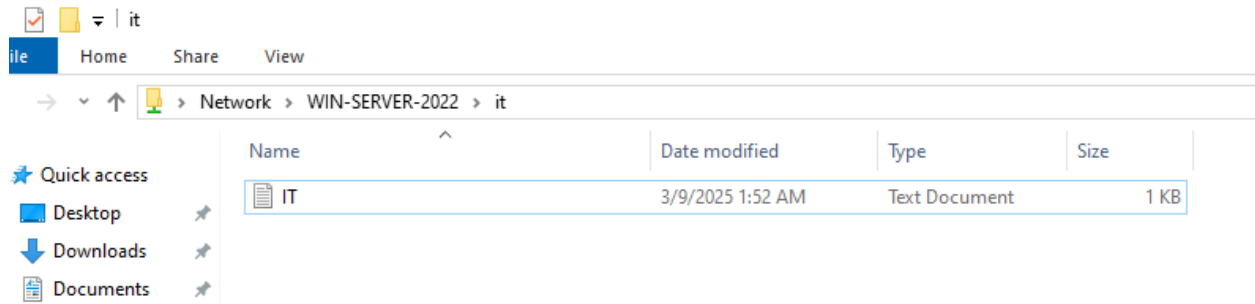
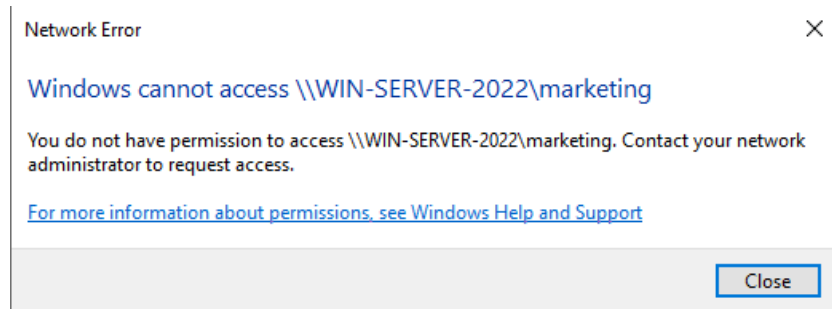


- **DNS et Active Directory** : Configure le domaine **insa.fr**, crée une **OU (Organizational Unit)** appelée **Department** et des sous-OU : Admin, IT, Marketing.
- **Création d'utilisateurs et de groupes**:
 - Dans **OU Admin** : Crée l'utilisateur **Fidon Martin** et le groupe **Admin**.
 - Dans **OU IT** : Crée l'utilisateur **Simon Leclerc** et le groupe **IT**.
 - Dans **OU Marketing** : Crée l'utilisateur **Sara Taki** et le groupe **Marketing**.



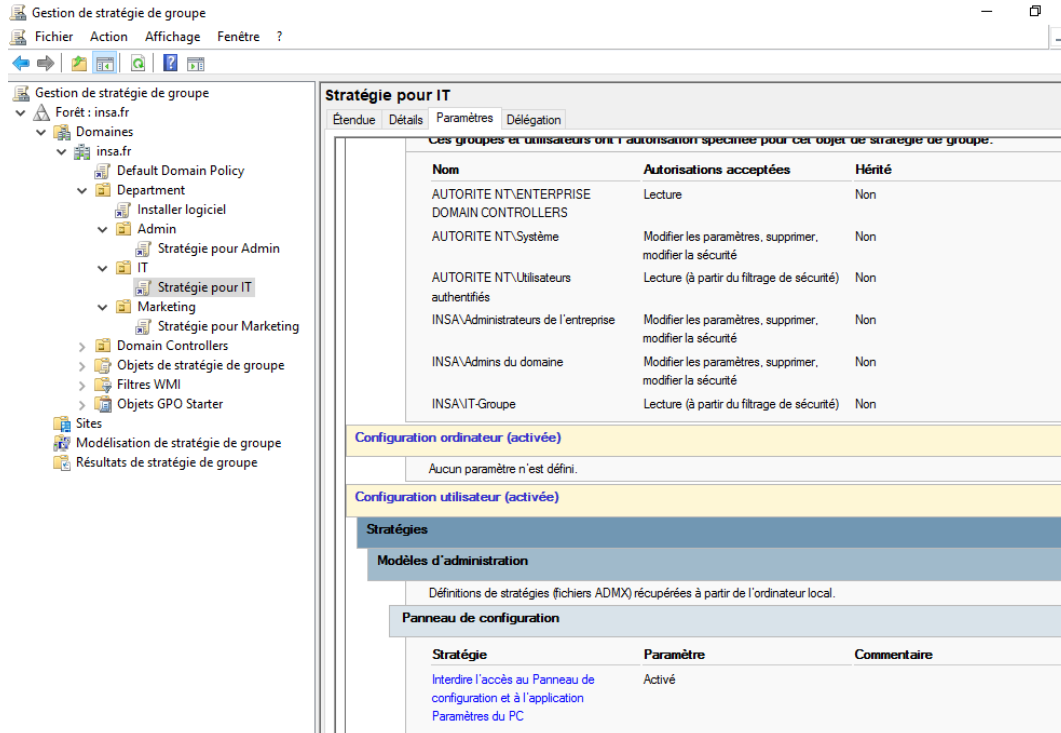
- **Services SMB** : Crée des dossiers **common**, **it**, **marketing**, **admin** avec des droits d'accès spécifiques:
 - **common** : Accessible par tous les utilisateurs.
 - **it** : Accessible uniquement par les utilisateurs du groupe IT et groupe Admin.
 - **marketing** : Accessible uniquement par les utilisateurs du groupe Marketing et groupe Admin.
 - **admin** : Accessible uniquement par les utilisateurs du groupe Admin.



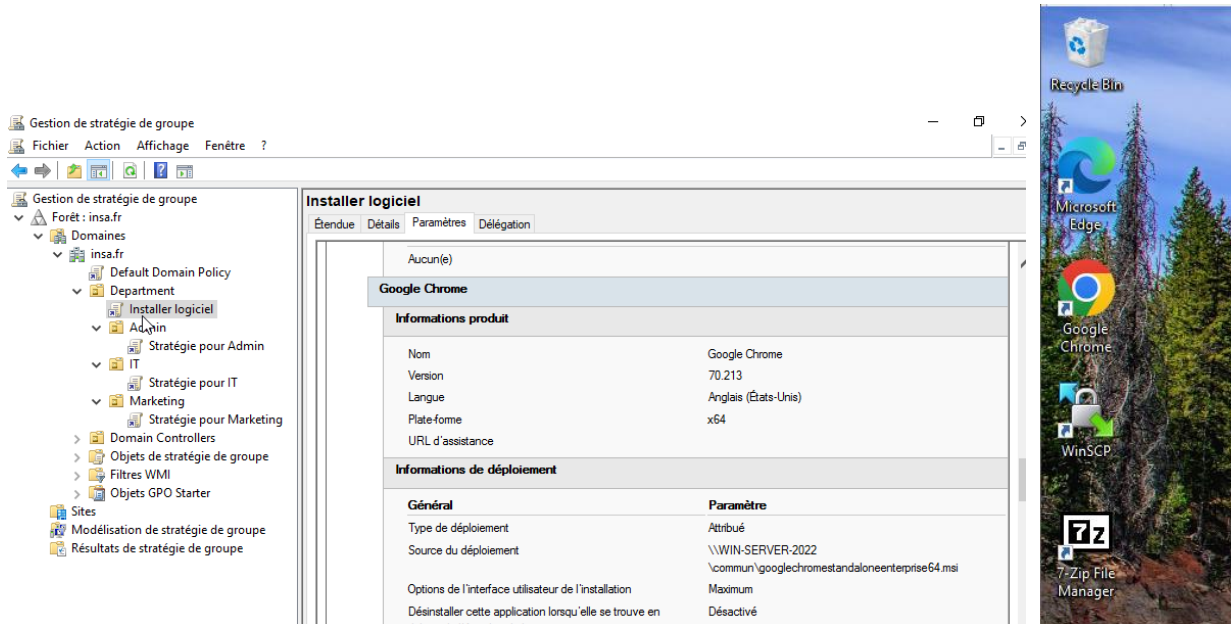


- **GPO (Group Policy Objects) :**

- Applique des **GPO spécifiques pour chaque OU** pour restreindre l'accès, comme l'interdiction d'accéder au **Panneau de configuration** et l'interdiction d'exécuter des programmes téléchargés depuis Internet.



- Écrire un GPO **Install logiciel** supplémentaire pour installer des programmes pour les ordinateurs clients



3. Serveur Ubuntu:

- Crée des comptes pour **l'utilisateur Simon (IT)** et **l'utilisateur Martin (Admin)**. **L'utilisateur Martin** est ajouté au groupe **root** pour avoir des droits administratifs.

```
simon@ubuntu-server:/home$ su - martin
Password:
martin@ubuntu-server:~$ sudo -i
[sudo] password for martin:
root@ubuntu-server:~# whoami
root
root@ubuntu-server:~# _
```

4. PfSense:

- Configurer un **VPN** sur PfSense pour permettre un accès à distance aux serveurs Windows 2022.

The screenshot shows the PfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Firewall / Rules / OpenVPN'. Below this, there are tabs for Floating, WAN, LAN, DMZ, and OpenVPN, with OpenVPN being the active tab. A table titled 'Rules (Drag to Change Order)' displays a single rule. The rule is enabled (checkbox checked), has a status of '0/0 B', protocol of 'IPv4 *', source of '10.10.10.0/24', port of '*', destination of 'LAN subnets', port of '*', gateway of '*', queue of 'none', and description of 'none'. Below the table are buttons for 'Add', 'Delete', 'Toggle', 'Copy', 'Save', and 'Separator'.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	10.10.10.0/24	*	LAN subnets	*	*	none		Add Delete Toggle Copy Save Separator

```
(kali㉿kali)-[~]
$ ip 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default ql
   en 1000
   link/ether 00:0c:29:05:f3:07 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.48/24 brd 192.168.1.255 scope global dynamic eth0
       valid_lft 86335sec preferred_lft 86335sec
   inet6 2001:861:5d00:ab20:20c:29ff:fe05:f307/64 scope global dynamic mngtmpaddr proto ker
   nel_ra
       valid_lft 86337sec preferred_lft 14337sec
   inet6 fe80::20c:29ff:fe05:f307/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

```

(kali㉿kali)-[~]
$ cd Downloads/pfSense-UDP4-1194-adminremote

(kali㉿kali)-[~/Downloads/pfSense-UDP4-1194-adminremote]
$ ls
pfSense-UDP4-1194-adminremote.ovpn  pfSense-UDP4-1194-adminremote-tls.key
pfSense-UDP4-1194-adminremote.pl2

(kali㉿kali)-[~/Downloads/pfSense-UDP4-1194-adminremote]
$ sudo openvpn *.ovpn
[sudo] password for kali:
2025-03-10 19:08:18 OpenVPN 2.6.13 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [
PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-03-10 19:08:18 library versions: OpenSSL 3.4.0 22 Oct 2024, LZO 2.10
2025-03-10 19:08:18 DCO version: N/A
Enter Auth Username: adminremote
Enter Auth Password: .....
2025-03-10 19:08:36 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.40:
1194
2025-03-10 19:08:36 UDPv4 link local: (not bound)
2025-03-10 19:08:36 UDPv4 link remote: [AF_INET]192.168.1.40:1194
2025-03-10 19:08:36 WARNING: this configuration may cache passwords in memory -- use the aut
h-nocache option to prevent this
2025-03-10 19:08:36 [insacvl] Peer Connection Initiated with [AF_INET]192.168.1.40:1194
2025-03-10 19:08:37 TUN/TAP device tun0 opened
2025-03-10 19:08:37 net_iface_mtu_set: mtu 1500 for tun0
2025-03-10 19:08:37 net_iface_up: set tun0 up
2025-03-10 19:08:37 net_addr_ptp_v4_add: 10.10.10.6 peer 10.10.10.5 dev tun0
2025-03-10 19:08:37 Initialization Sequence Completed

```

```

(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.48 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2001:861:5d00:ab20:20c:29ff:fe05:f307 prefixlen 64 scopeid 0x0<global>
    inet6 fe80::20c:29ff:fe05:f307 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:05:f3:07 txqueuelen 1000 (Ethernet)
    RX packets 2996 bytes 1305939 (1.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1979 bytes 312789 (305.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    An error occurred during a connection to 192.168.10.1
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 (Local Loopback)
    RX packets 12 bytes 732 (732.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 732 (732.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.10.6 netmask 255.255.255.255 destination 10.10.10.5
    inet6 fe80::d8b3:b3fa:ab95:a39 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 37 bytes 9002 (8.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

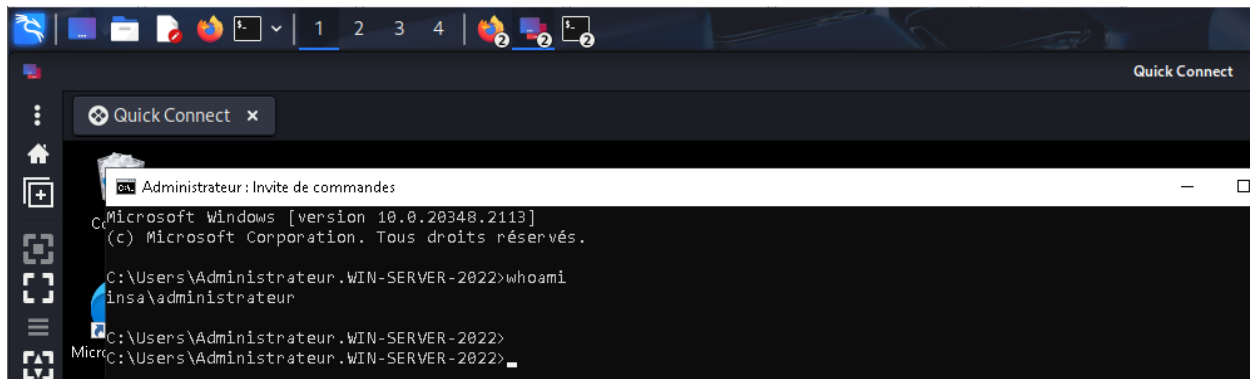
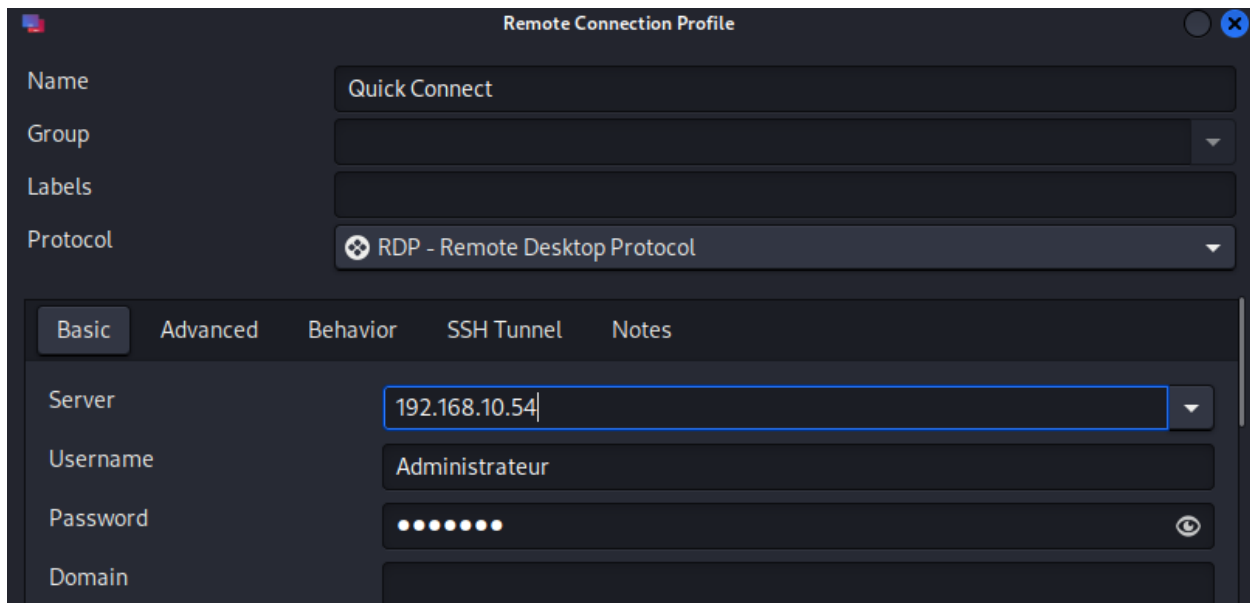
```

```

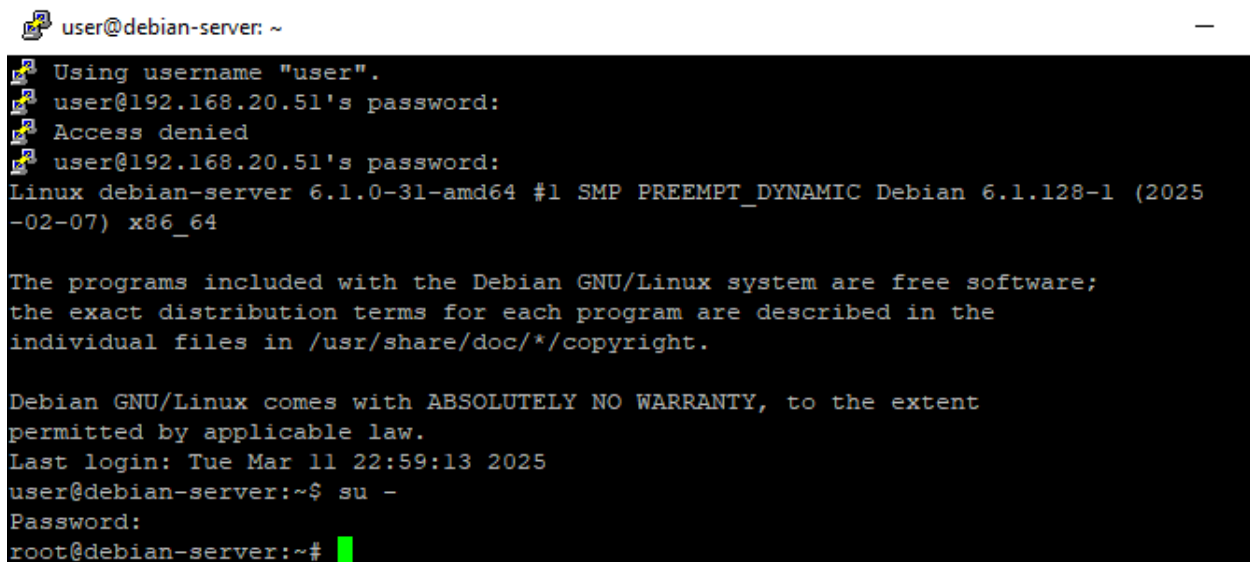
(kali㉿kali)-[~]
$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=1.22 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=1.89 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=1.70 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.68 ms
^C
--- 192.168.10.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.218/1.622/1.886/0.246 ms

(kali㉿kali)-[~]
$

```



- **Les utilisateurs du groupe Admin** peuvent accéder au serveur Debian dans la DMZ pour effectuer des opérations de gestion.



- Les règles sur chaque interface réseau pour protéger le système.

Firewall / Rules / WAN 📊 📋 ?

Floating WAN LAN DMZ OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/668 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogus networks	⚙️
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Accès distant OpenVPN	📌 ✎ 📋 🚫 ✖
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	192.168.20.51	80 (HTTP)	*	none		NAT	📌 ✎ 📋 🚫 🗑

⬆ Add
⬇ Add
🗑 Delete
🔄 Toggle
📋 Copy
💾 Save
+ Separator

Firewall / Rules / LAN 📊 📋 ?

Floating WAN LAN DMZ OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 4/999 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✓ 3/43.30 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	📌 ✎ 📋 🚫 🗑

⬆ Add
⬇ Add
🗑 Delete
🔄 Toggle
📋 Copy
💾 Save
+ Separator

Firewall / Rules / DMZ



Floating WAN LAN **DMZ** OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	none		Bloquer flux vers le LAN	
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	DMZ subnets	*	*	80 (HTTP)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	DMZ subnets	*	*	443 (HTTPS)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP/UDP	DMZ address	*	*	53 (DNS)	*	none		

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Firewall / Rules / OpenVPN



Floating WAN LAN DMZ **OpenVPN**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 *	10.10.10.0/24	*	LAN subnets	*	*	none		

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

V. Conclusion

Le projet de simulation de réseau interne pour l'entreprise a été achevé avec une architecture réseau claire et sécurisée. Les fonctionnalités telles que le VPN, la gestion des droits d'accès et la sécurité des services ont été correctement mises en place, garantissant ainsi que le système fonctionne de manière sécurisée et efficace. Le système répond aux exigences de sécurité, d'accès à distance et de gestion des ressources dans le réseau interne.

Ce projet n'est peut-être pas parfait car il contient quelques erreurs et il peut ne pas être adapté à l'environnement réel, mais il peut décrire certaines de ses applications.