PROJET JURIS NOVA

Réalisé par Rafael MAIA et Adam EL ASRAOUI

2024/2025

Objectif de la mission

L’objectif était de concevoir une infrastructure réseau sécurisée, segmentée en plusieurs zones, et conforme au cahier des charges fourni. Le tout a été simulé dans Marionnet.

Schéma réseau

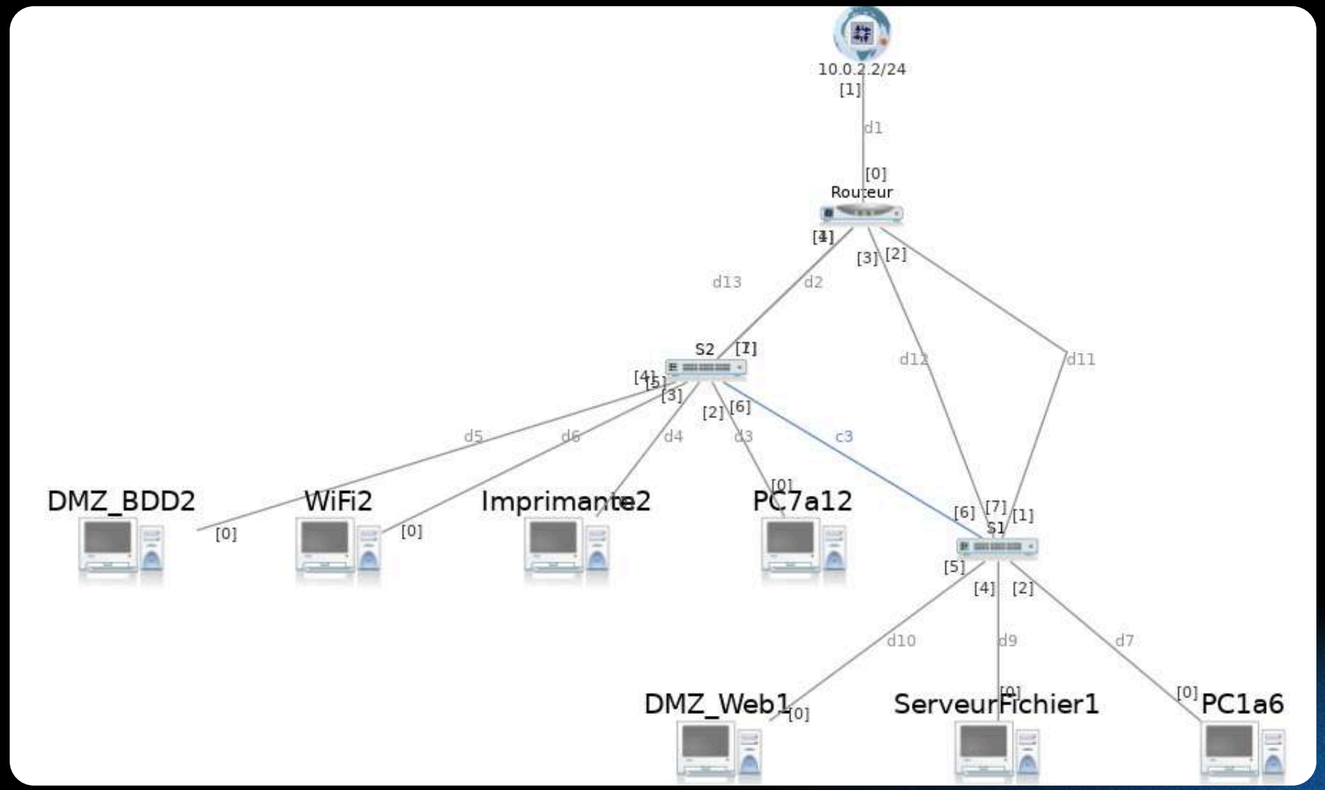
ARCHITECTURE RÉSEAU

Ce schéma montre l'architecture globale avec les différents VLANs. Les équipements sont interconnectés et segmentés pour garantir la sécurité et le bon fonctionnement des services.

Configuration des machines :

```
21 ip addr add 10.0.30.1/24 dev eth0
22 ip link set up dev eth0
23 ip route add default via 10.0.30.254
```

Voici l'architecture du réseau :



Switch du 1er étages :

```
3 vlan/create 10
4 vlan/create 20
5 vlan/create 30
6 vlan/create 40
7
8 # Ports accès
9 vlan/addport 10 2        # PC1-A6
0 vlan/addport 10 4        # Serveur Fichier
1 vlan/addport 20 5        # DMZ Web
2
3 # Trunk vers S2
4 vlan/addport 10 6
5 vlan/addport 20 6
6 vlan/addport 30 6
7 vlan/addport 40 6
8
9 # Vers routeur
0 vlan/addport 30 7        # vers eth3 du routeur
1 vlan/addport 40 1        # vers eth4 du routeur
```

Switch du 2ème étages :

```
13 vlan/create 10
14 vlan/create 20
15 vlan/create 30
16 vlan/create 40
17
18 # Ports accès
19 vlan/addport 10 2        # PC7-A12
20 vlan/addport 10 3        # Imprimante réseau
21 vlan/addport 40 4        # Wi-Fi invité
22 vlan/addport 30 5        # Serveur BDD 2
23
24 # Trunk vers S1
25 vlan/addport 10 6
26 vlan/addport 20 6
27 vlan/addport 30 6
28 vlan/addport 40 6
29
30 # Vers routeur
31 vlan/addport 10 1        # vers eth1 du routeur
32 vlan/addport 20 7        # vers eth2 du routeur
```

Routeur :

```
20 # === Interface Internet
21 ip addr add 10.0.2.254/24 dev eth0
22 ip link set eth0 up
23 ip route add default via 10.0.2.2
24 # === VLAN 10 – LAN
25 ip addr add 10.0.10.254/24 dev eth1
26 ip link set eth1 up
27 # === VLAN 20 – Web / GLPI
28 ip addr add 10.0.20.254/24 dev eth2
29 ip link set eth2 up
30 # === VLAN 30 – BDD
31 ip addr add 10.0.30.254/24 dev eth3
32 ip link set eth3 up
33 # === VLAN 40 – Wi-Fi invité
34 ip addr add 10.0.40.254/24 dev eth4
35 ip link set eth4 up
```

Répartition des machines

Vlan 10 : (10.0.10.X/24)
Pc employé / Imprimante / Serveur fichier
Vlan 20 : (10.0.20.X/24)
DMZ Web
Vlan 30 : (10.0.30.X/24)
DMZ BDD
Vlan 40 : (10.0.40.X/24)
Wifi invité

Liste d'équipements

Nous avons décider de choisir les composant suivant pour la réalisation de votre réseau :

Désignation	Modèle / Référence	Quantité	Fournisseur	Prix unitaire HT (€)	Prix total HT (€)	SLA
PC portables (utilisateurs)	Dell Latitude 3540, i5, 8Go RAM, 256Go SSD	12	LDLC / Dell Pro	650	7800	J+1
Serveur Web (Apache + GLPI)	Dell PowerEdge T150, Xeon, 16Go RAM, 512Go SSD	1	Dell Pro	1200	1200	H+4
Serveur BDD (MariaDB)	HP ProLiant MicroServer Gen10, 4Go RAM	1	HP / Inmac WStore	650	650	H+4
Serveur de fichiers	Synology DS923+ + 2x 1To WD Red Pro	1	Amazon Pro / Synology	850	850	H+4
Imprimante réseau A4/A3	Brother MFC-L9570CDW (PDF natif, 30 ppm)	1	LDLC Pro / Brother	700	700	J+1
Switch manageable 8 ports	Netgear GS308EP (VLAN, QoS, STP)	2	LDLC / Amazon	100	200	N/A
Routeur 5 ports iptables	PC Engines APU2E5 + 5 NIC + SSD	1	PC Engines / Amazon	300	300	N/A
Point d'accès Wi-Fi pro	Ubiquiti UniFi 6 Lite	1	Ubiquiti / LDLC	120	120	N/A
Câbles RJ45 droit Cat6	2m Cat6 RJ45 blindé	13	LDLC / Amazon	4	52	N/A
Câble RJ45 croisé Cat6	2m Cat6 croisé blindé (trunk)	1	LDLC / Amazon	5	5	N/A
					11877	

Sécurité du réseau

RÈGLES ACL

Des règles ACL ont été mises en place sur le routeur pour filtrer les échanges entre les VLANs. Par exemple, le Wi-Fi invité ne peut accéder qu'à Internet, et le LAN ne peut pas joindre la base de données.

Test de ces règles:

Ping vers le réseaux de l'entreprise :

```
[1 root@WiFi2 ~]$ ping -c1 10.0.10.1
PING 10.0.10.1 (10.0.10.1) 56(84) bytes of data.

--- 10.0.10.1 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Ping vers le monde extérieur :

```
[0 root@WiFi2 ~]$ ping -c1 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_req=1 ttl=254 time=1.26 ms

--- 10.0.2.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.268/1.268/1.268/0.000 ms
```

Règles ACL définie sur le routeur :

```
### === ACL VLAN 10 (LAN) ===
iptables -A FORWARD -i eth1 -o eth3 -j DROP
iptables -A FORWARD -i eth1 -j ACCEPT
### === ACL VLAN 20 (Web/GLPI) ===
iptables -A FORWARD -i eth0 -o eth2 -j DROP
iptables -A FORWARD -i eth2 -j ACCEPT
### === ACL VLAN 30 (BDD) ===
iptables -A FORWARD -i eth2 -o eth3 -j ACCEPT
iptables -A FORWARD -o eth3 -j DROP
### === ACL VLAN 40 (Wi-Fi invité) ===
iptables -A FORWARD -i eth4 -o eth0 -j ACCEPT
iptables -A FORWARD -i eth4 -o eth0 -j DROP
```

Installation des services

BASE DE DONNÉES MARIA BDD

La base de données MariaDB est installée dans la DMZ BDD, sur une machine séparée. Elle est uniquement accessible par le serveur GLPI via une règle ACL spécifique, conformément au cahier des charges.

Résultat de la configuration :

```
MariaDB [siteweb]> use siteweb
Database changed
MariaDB [siteweb]> show tables
    -> ;
+--------------------+
| Tables_in_siteweb  |
+--------------------+
| contact            |
+--------------------+
1 row in set (0.001 sec)

MariaDB [siteweb]>
```

Video de l'installation de la configuration :

Installation des services

INSTALLATION DE GLPI

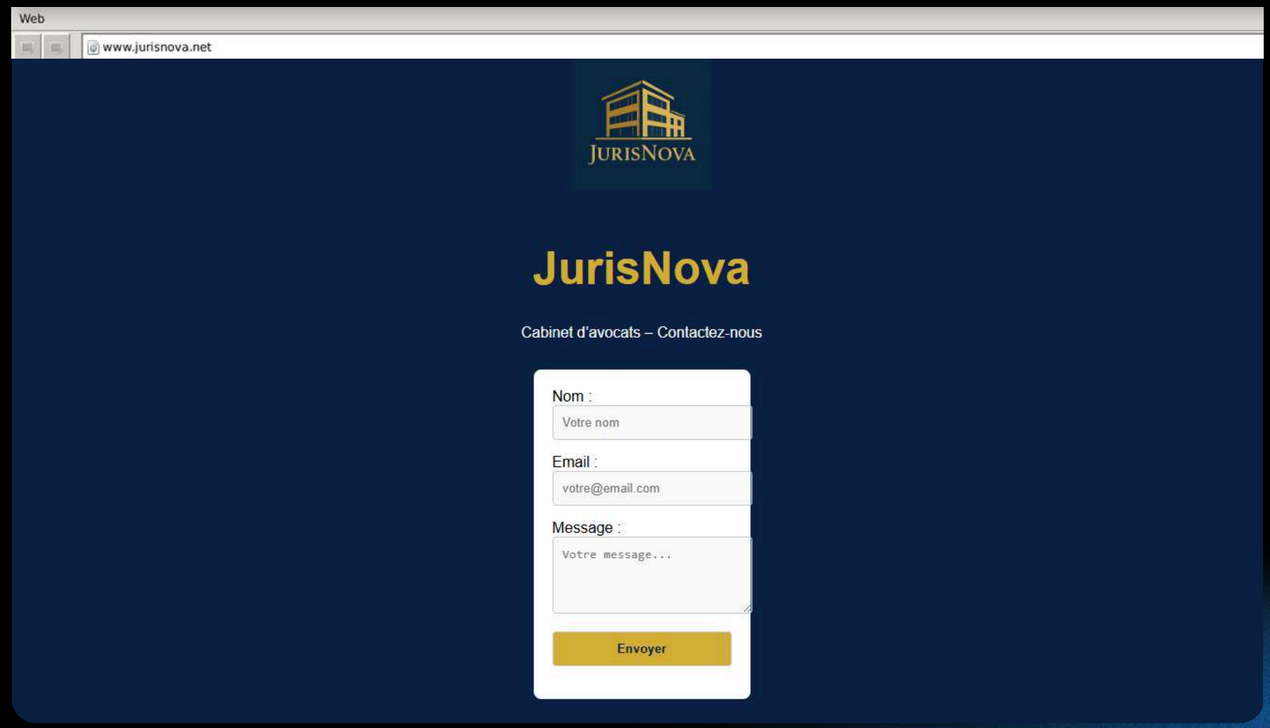
GLPI est installé sur le serveur Web dans la DMZ. Nous avons adapté l'installation hors-ligne à Marionnet, avec une liaison fonctionnelle vers la base MariaDB distante.

Installation des services

SITE VITRINE PHP

En plus de GLPI, un site web vitrine de l'entreprise a été déployé en PHP sur le même serveur. Cela permet de centraliser les services tout en maintenant une structure réseau sécurisée.

Résultat de la configuration :




conclusion