Documentation technique et rapport de tests – Projet ArchiSite

AP 3 – RIOCA (groupe 3) · BTS SIO 2 option SISR · Campus Carlo Acutis

Réalisé par Souhir (chef de projet) et Maxime Forest · Novembre 2026

Aucun mot de passe n'apparaît dans ce document : les identifiants sont dans la fiche de configuration. Le numéro entre parenthèses dans les légendes renvoie à la carte Trello de la tâche.

Sommaire

1. Présentation du projet

2. Architecture

3. Gestion de projet

4. Étude ANSSI et choix d'architecture

5. Serveur Web (SRV-WEB1)

6. Autorité de certification interne, HTTPS et TLS

7. Base de données (srv-bdd-3)

8. Serveur FTPS (SRV-WEB1)

9. Serveur DNS (BIND9 sur SRV-WEB1)

10. Pare-feu Zyxel : règles de filtrage

11. Accès des développeurs depuis le Wi-Fi (tâche non prévue)

12. Rapport de tests

13. Difficultés rencontrées et solutions

14. Limites et améliorations possibles

15. Livrables et annexes

Annexe A. Diagramme de Gantt

1. Présentation du projet

1.1 Contexte

RIOCA est une entreprise fictive, cliente du projet. Après le projet Infra-Site (cloisonnement LAN / DMZ / Internet), la lettre de mission ArchiSite demande de mettre en place et de sécuriser le site web de l'entreprise, hébergé en DMZ, avec sa base de données et un dépôt de fichiers pour les développeurs de l'équipe SLAM.

1.2 Objectifs

- Héberger le site www.rioca-corp.com sur un serveur Web Linux (Apache + PHP), accessible en HTTPS depuis le LAN, sans alerte de certificat.
- Héberger la base de données du site (MariaDB) dans une zone séparée, sans accès direct depuis les postes.
- Fournir aux développeurs SLAM un dépôt de fichiers chiffré (FTPS) et un accès à la base par phpMyAdmin.
- Mettre en place un serveur DNS dans la DMZ pour le domaine rioca-corp.com.
- Filtrer tous les flux avec le pare-feu Zyxel selon le principe du moindre privilège.

- Documenter, tester et fournir les preuves (rapport de tests, fiche de configuration).

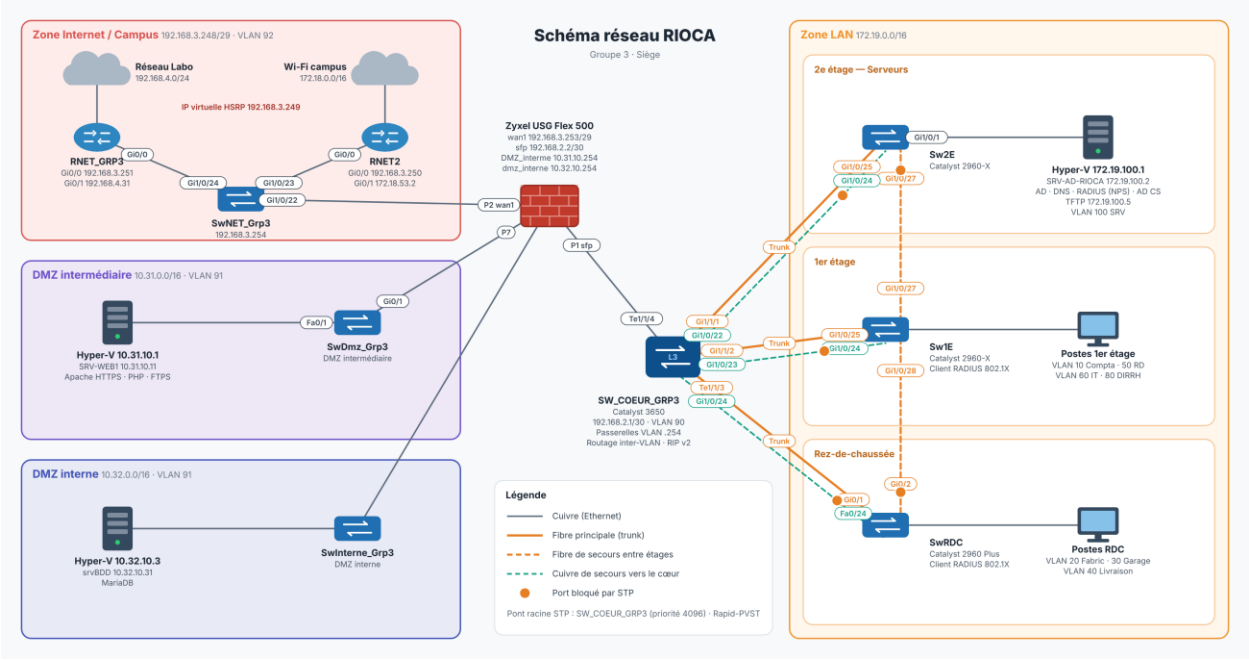
1.3 Organisation

Élément	Détail
Équipe	Souhir (chef de projet) et Maxime Forest
Budget prévisionnel	28 h par personne, tâches en duo comprises
Mise en production prévue	03/11/2026 à 17h30
Outils de suivi	Trello (6 colonnes), diagramme de Gantt Excel (GANT_Archisite_MAXIME_SOUHIR.xlsm)

2. Architecture

2.1 Zones réseau

Le schéma cible de la lettre de mission sépare l'ancienne DMZ unique en deux zones, conformément aux recommandations de l'ANSSI : une DMZ intermédiaire pour les services exposés (Web, FTPS, DNS) et une DMZ interne pour la base de données.



Capture : schéma réseau final : zones Internet/Campus, DMZ intermédiaire (10.31.0.0/16), DMZ interne (10.32.0.0/16) et LAN, avec les liens de secours Spanning Tree

Zone	Réseau	Équipements
LAN de l'entreprise	172.19.0.0/16	Contrôleur de domaine SRV-AD-RIOCA (172.19.100.2), postes Windows 11 du domaine rioca.local
DMZ intermédiaire	10.31.0.0/16	Passerelle Zyxel 10.31.10.254, hôte Hyper-V 10.31.10.1, SRV-WEB1 10.31.10.11 (Web + FTPS + DNS)
DMZ interne	10.32.0.0/16	Passerelle Zyxel 10.32.10.254, hôte Hyper-V 10.32.10.3, srv-bdd-3 10.32.10.31 (MariaDB)

Zone	Réseau	Équipements
Internet / WAN	192.168.3.248/29	Interface WAN du Zyxel 192.168.3.253, routeurs RNET_GRP3 (192.168.3.251, actif) et RNET2 (192.168.3.250) en HSRP, IP virtuelle 192.168.3.249
Wi-Fi du campus	172.18.0.0/16	Postes des développeurs SLAM (hors domaine), derrière RNET2 (172.18.53.1)

2.2 Serveurs

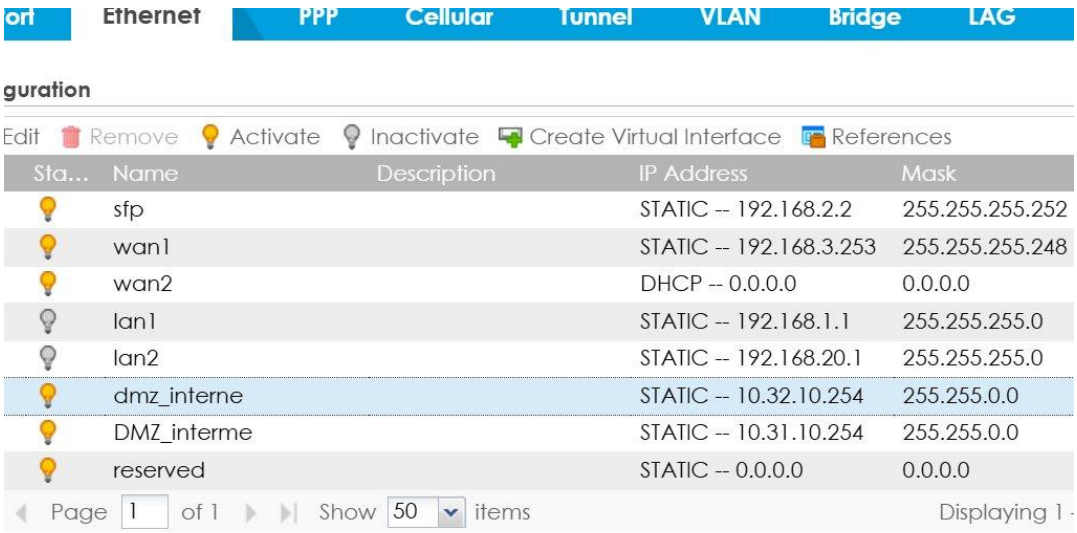
Serveur	Rôle	Système	Services
SRV-WEB1 (10.31.10.11)	Web, FTPS, DNS, autorité de certification	Debian 13	Apache 2, PHP 8.4, phpMyAdmin, vsftpd 3.0.5, BIND9 9.20, OpenSSL (CA)
srv-bdd-3 (10.32.10.31)	Base de données	Ubuntu 26.04	MariaDB 11.8.6, UFW
SRV-AD-RIOCA (172.19.100.2)	Annuaire et DNS du LAN	Windows Server	AD, DNS, GPO

Chaque serveur est une machine virtuelle sur l'hyperviseur Hyper-V de sa DMZ (10.31.10.1 pour la DMZ intermédiaire, 10.32.10.3 pour la DMZ interne), administré à distance. Un compte d'administration est créé par membre du groupe.

2.3 Migration DMZ 10.31 / 10.32 (tâche non prévue au Gantt)

Au départ, le serveur Web et la base étaient dans une DMZ unique en 10.3.0.0/16. Le besoin de séparer les zones est apparu pendant le projet :

- Deux interfaces distinctes déclarées sur le Zyxel (une par DMZ).
- Switch SwInterne_Grp3 pour la DMZ interne, avec l'hyperviseur et le serveur BDD derrière.
- Routes 10.31 et 10.32 annoncées sur RNET en RIP.
- Mise à jour des objets du pare-feu (ex. LAN_to_WebServ pointait encore vers l'ancienne IP du serveur Web).



Capture : *interfaces des deux DMZ déclarées sur le Zyxel (Migration DMZ)*

3. Gestion de projet

3.1 Découpage en 8 missions

1. Planification du projet (Gantt, Trello)
2. Installation des serveurs Web et BDD
3. Accès entrant vers les ressources
4. Sécurisation du serveur Web
5. Serveur FTPS
6. Règles d'accès aux services (pare-feu)
7. Serveur DNS dans la DMZ
8. Documentation

3.2 Répartition des tâches

Souhir a choisi de prendre les règles Zyxel pour apprendre à les configurer. Les tests d'intégration finaux sont une tâche commune.

Souhir	Maxime
Gantt et Trello (en duo), VM BDD, MariaDB, comptes et droits BDD, règles Zyxel (Web, BDD, FTPS, DNS, Internet), tests des flux, DNS BIND9, étude ANSSI, rapport de tests, migration DMZ interne	Gantt (en duo), VM Web, Apache + PHP, CA interne, certificat Web, TLS, vsftpd, certificat FTPS, présentation DSI sur les certificats, tests Web et FTPS, fiche de configuration, accès Wi-Fi des développeurs

3.3 Suivi

Le tableau Trello comporte les colonnes À faire, En cours, À tester, À corriger, Terminé et Gestion de projet. Chaque tâche du Gantt est une carte avec un responsable, une durée prévue et un temps réel. Les rapports

hebdomadaires de chaque membre sont dans les commentaires de la carte de la semaine. Le diagramme de Gantt complet (prévu et réel) est en annexe A.

4. Étude ANSSI et choix d'architecture

La répartition des services dans les zones s'appuie sur le guide ANSSI-PA-066 (interconnexion d'un SI à Internet, v3.0), complété par PA-044 (pare-feux), PA-022 (administration) et le guide TLS de l'ANSSI.

Recommandation par défaut : Web et FTPS en zone de services exposés (DMZ), base de données hors de cette zone, DNS et administration séparés.

Application à ArchiSite : Web et FTPS en DMZ intermédiaire, BDD en DMZ interne, seul SRV-WEB1 autorisé à joindre la BDD (TCP 3306).

Écarts justifiés (cadre pédagogique) : services mutualisés sur SRV-WEB1, un seul pare-feu Zyxel, pas de reverse proxy, compte BDD partagé.

Livrable : Etude_ANSSI_ArchiSite.docx (pièce jointe de la carte 3).

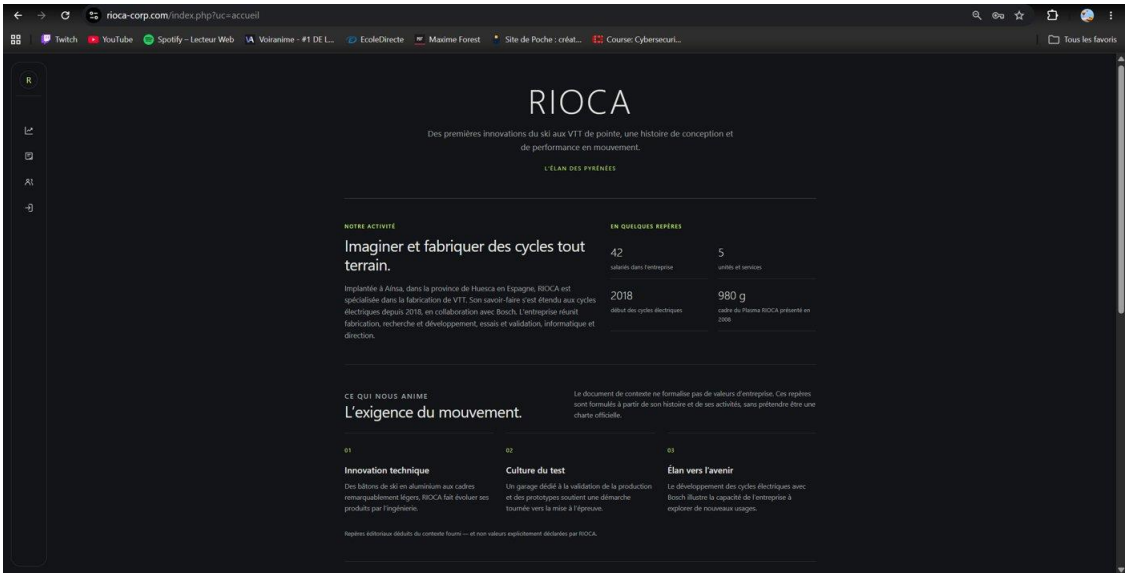
5. Serveur Web (SRV-WEB1)

5.1 Installation

Choix d'Apache 2 avec PHP 8.4 (module PHP pour Apache, extension MySQL) : le site SLAM exécute des pages PHP côté serveur. VirtualHost www.rioca-corp.com, DocumentRoot `/var/www/rioca`, listage des dossiers désactivé, site par défaut désactivé, droits www-data sur le dossier du site.

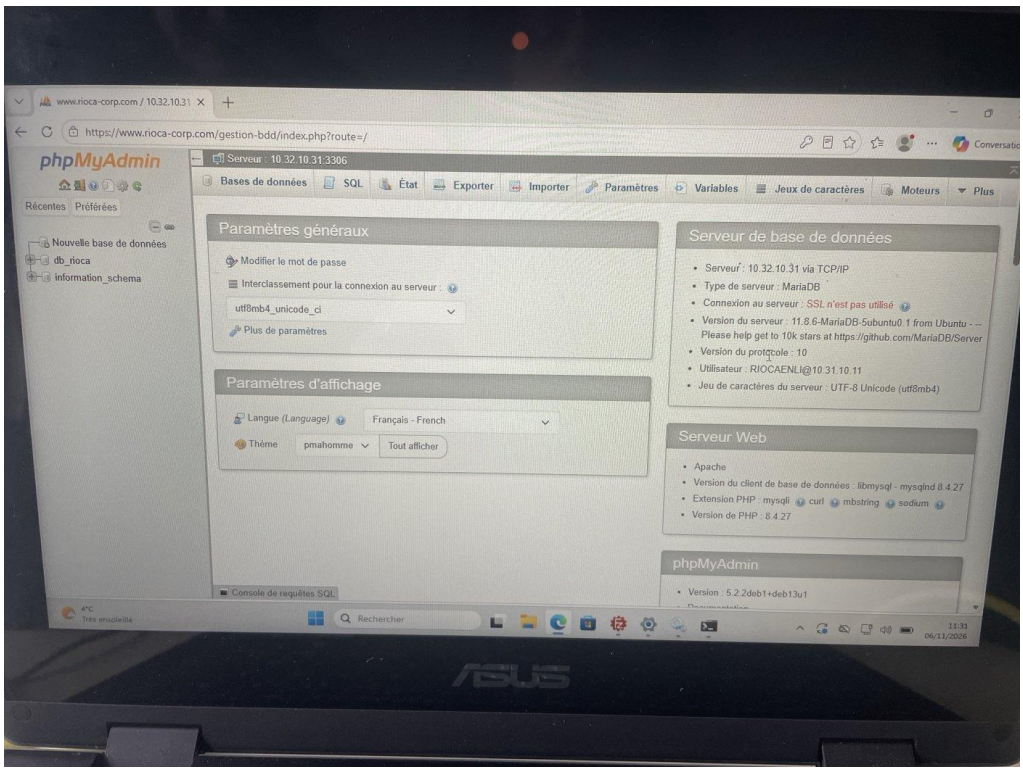
Choix du service Web : Apache plutôt que Nginx. PHP s'intègre directement en module, la configuration par VirtualHost est simple et déjà connue de l'équipe, et la documentation est abondante. Ce choix est détaillé dans le document Choix_service_web_ArchiSite.docx.

Le site et sa base sont fournis par l'équipe SLAM. Il est déposé par FTPS dans `/var/www/rioca`, et la connexion du site à la base est validée par la connexion d'un utilisateur en HTTPS.



Capture : *site SLAM : connexion d'un utilisateur validée avec la base (carte 9)*

phpMyAdmin est publié sur https://www.rioca-corp.com/gestion-bdd, en HTTPS uniquement, réservé au LAN et au Wi-Fi des développeurs, compte root refusé.



Capture : *connexion du compte RIOCAENLI à phpMyAdmin sur /gestion-bdd*

5.2 Durcissement

- Version d'Apache masquée (`ServerTokens Prod`, `ServerSignature Off`), modules autoindex et status désactivés.
- Aucun fichier de test laissé en place (page phpinfo supprimée).

6. Autorité de certification interne, HTTPS et TLS

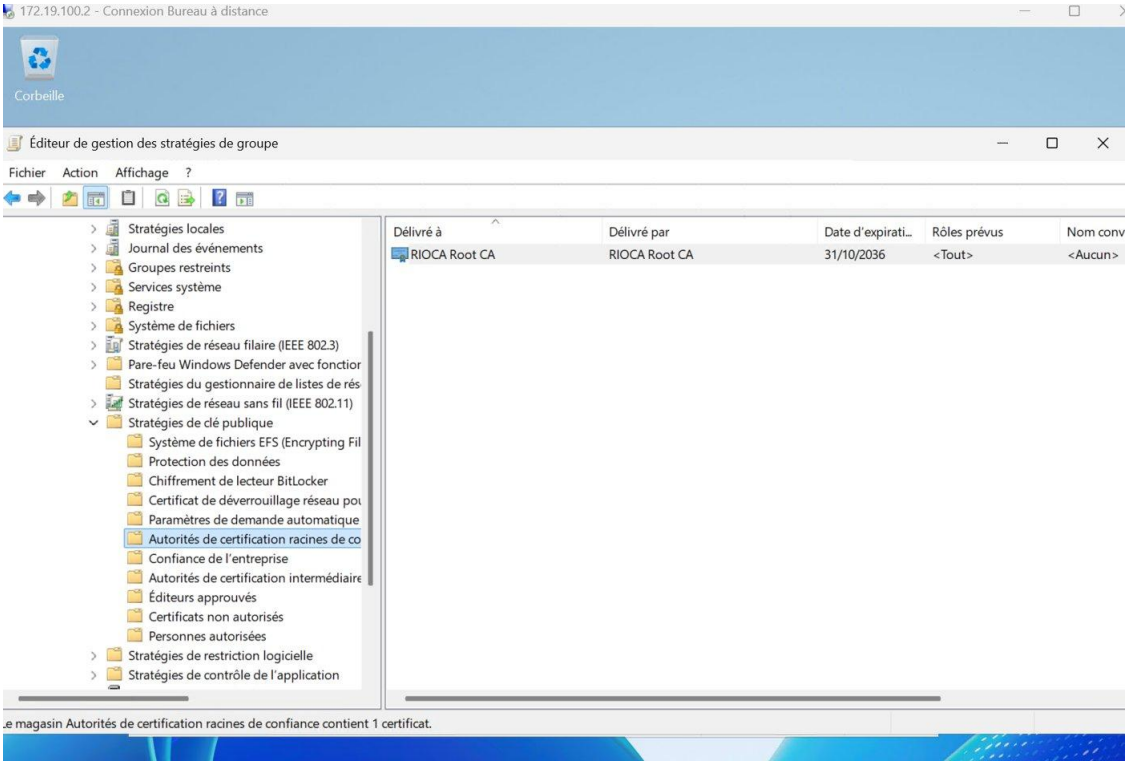
RIOCA gère sa propre autorité de certification (certificat interne). Le site est réservé aux salariés : un certificat externalisé, signé par une autorité publique, demanderait un nom de domaine public et un coût de renouvellement sans apporter plus de sécurité ici. La comparaison complète est dans la présentation DSI (carte 14).

6.1 CA interne « RIOCA Root CA »

- Créée avec OpenSSL sur SRV-WEB1 (arborescence, openssl.cnf).
- Clé privée RSA 4096 protégée par phrase de passe, droits 400, accessible au seul administrateur.
- Certificat racine valable 10 ans. Vérifié : émetteur = sujet, `CA:TRUE`.
- Déploiement sur les postes par la GPO GPO_Certificat_Racine_RIOCA liée au domaine rioca.local, dans le magasin « autorités de certification racines de confiance ».

```
root@srv-web:~/rioca-ca# openssl x509 -in certs/rioca-ca.crt -noout -subject -issuer -dates -ext basicConstraints,keyUsa
ge
ls -l private certs
subject=C=FR, O=RIOCA, CN=RIOCA Root CA
issuer=C=FR, O=RIOCA, CN=RIOCA Root CA
notBefore=Nov  3 15:49:23 2026 GMT
notAfter=Oct 31 15:49:23 2036 GMT
X509v3 Basic Constraints: critical
    CA:TRUE
X509v3 Key Usage: critical
    Certificate Sign, CRL Sign
certs:
total 4
-rw-r--r-- 1 root root 1919  3 nov.  16:49 rioca-ca.crt

private:
total 4
-r-------- 1 root root 3446  3 nov.  16:48 rioca-ca.key
```

Capture : *vérification du certificat racine : émetteur = sujet, CA:TRUE (carte 10)*



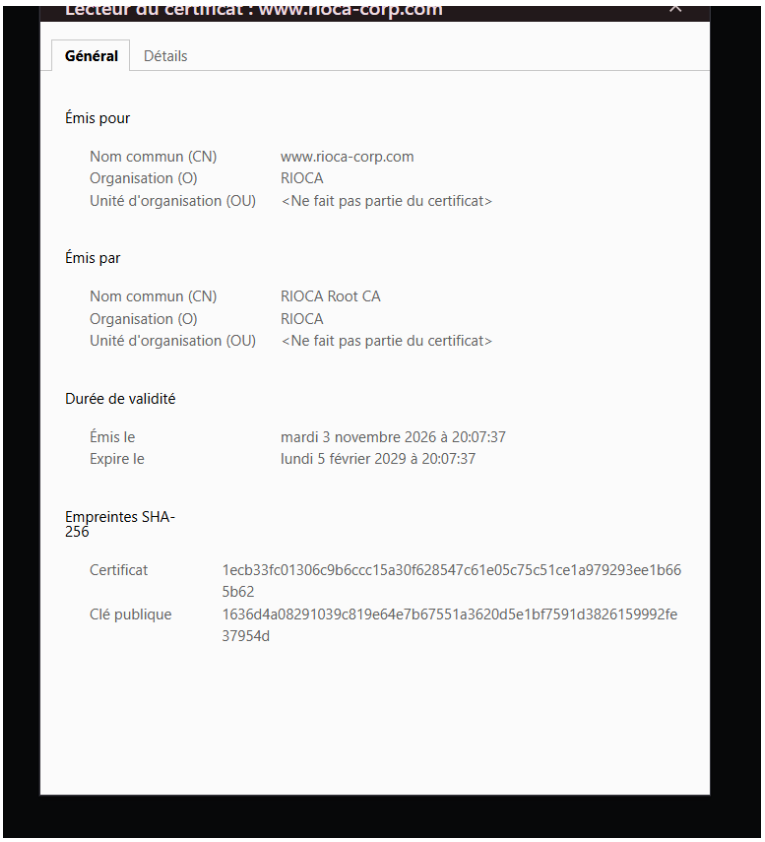
Capture : *GPO : certificat racine importé (carte 10)*

6.2 Certificat du serveur Web

- Clé privée RSA 2048 (droits 600), demande de signature (CSR) avec CN et SAN www.rioca-corp.com.
- Signé par RIOCA Root CA, vérifié avec `openssl verify`. Validité du 03/11/2026 au 05/02/2029.
- Module SSL activé, VirtualHost HTTPS sur le port 443.

```
root@srv-web:~/rioca-ca# openssl verify -CAfile certs/rioca-ca.crt certs/www.rioca-corp.com.crt
openssl x509 -in certs/www.rioca-corp.com.crt -noout -subject -issuer -ext subjectAltName
certs/www.rioca-corp.com.crt: OK
subject=C=FR, O=RIOCA, CN=www.rioca-corp.com
issuer=C=FR, O=RIOCA, CN=RIOCA Root CA
X509v3 Subject Alternative Name:
    DNS:www.rioca-corp.com
```

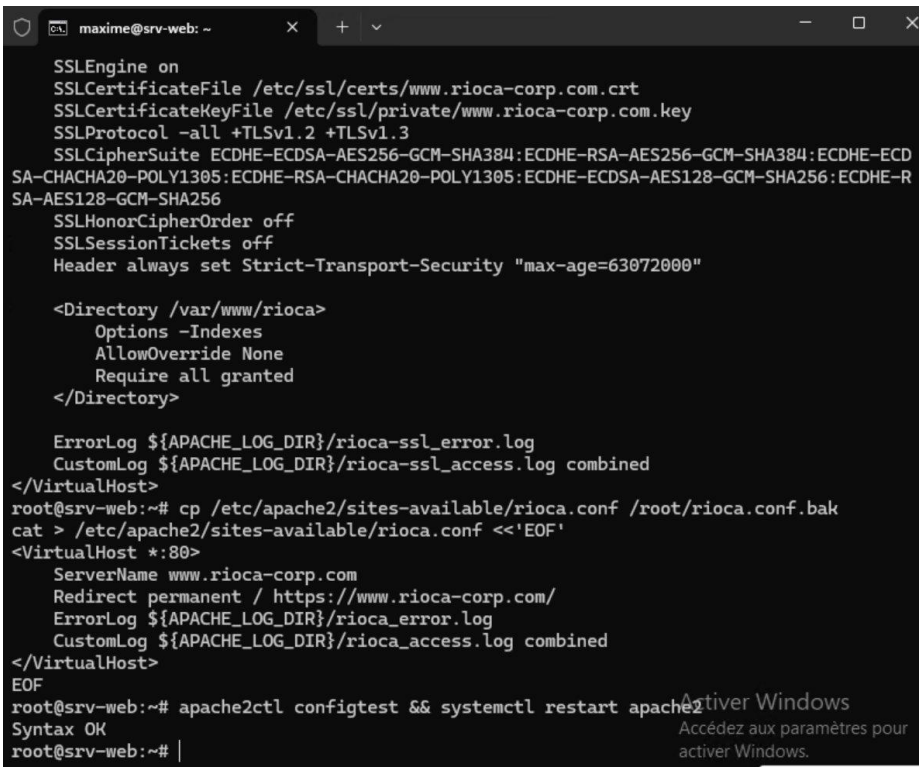
Capture : *vérification openssl du certificat du serveur Web (carte 11)*



Capture : certificat www.rioca-corp.com émis par RIOCA Root CA, valide du 03/11/2026 au 05/02/2029 (carte 19)

6.3 Durcissement TLS

Mesure	Valeur
Protocoles	TLS 1.2 et 1.3 uniquement (TLS 1.0 et 1.1 refusés)
Suites de chiffrement	ECDHE avec AES-GCM ou ChaCha20
Tickets de session	Désactivés
HSTS	Activé, 2 ans
HTTP vers HTTPS	Pas de redirection : le site répond aussi en HTTP sur le port 80, à la demande de l'enseignante (accès depuis le Wi-Fi)

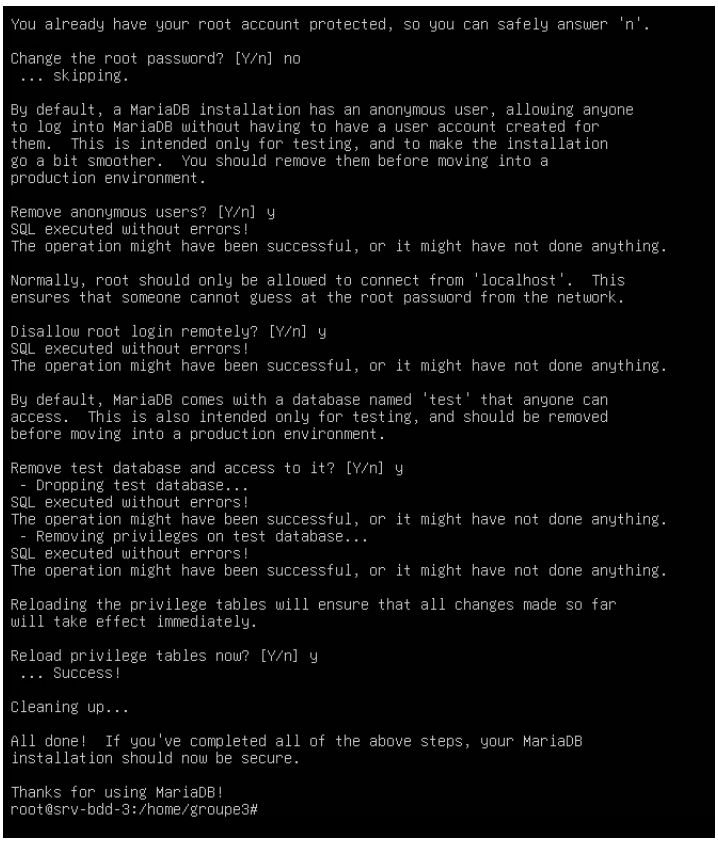


Capture : configuration TLS et HSTS, configtest (carte 12)

7. Base de données (srv-bdd-3)

7.1 Installation et sécurisation

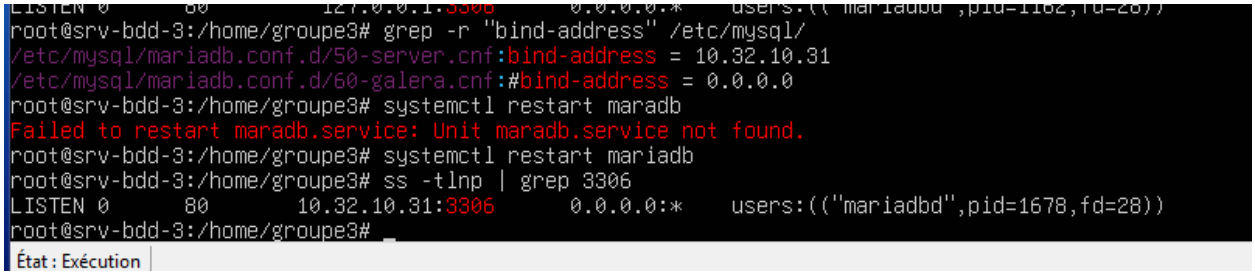
- Installation de mariadb-server et mariadb-client (version 11.8.6) sur la VM de la DMZ interne.
- `mariadb-secure-installation` : authentification root par unix_socket, utilisateurs anonymes supprimés, accès distant de root désactivé, base de test supprimée.
- Base dédiée au site : db_rioca. L'import du fichier SQL est réalisé par les développeurs SLAM.



Capture : mariadb-secure-installation : utilisateurs anonymes, accès distant de root et base de test supprimés (carte 7)

7.2 Écoute réseau

Par défaut MariaDB n'écoute que sur 127.0.0.1. Le paramètre a été modifié dans `/etc/mysql/mariadb.conf.d/50-server.cnf` : `bind-address = 10.32.10.31`. Cette IP est préférée à 0.0.0.0 pour limiter l'écoute à l'interface nécessaire (moindre privilège). Contrôle avec `ss -tlnp | grep 3306`.



Capture : bind-address = 10.32.10.31 dans 50-server.cnf, puis ss -tlnp : MariaDB écoute sur 10.32.10.31:3306 (carte 8)

7.3 Comptes et droits

Le compte de test créé au départ pour valider l'installation a été supprimé. Vérifications : `SELECT user,host FROM mysql.user;` et `SHOW GRANTS FOR 'RIOCAENLI'@'10.31.10.11';`.

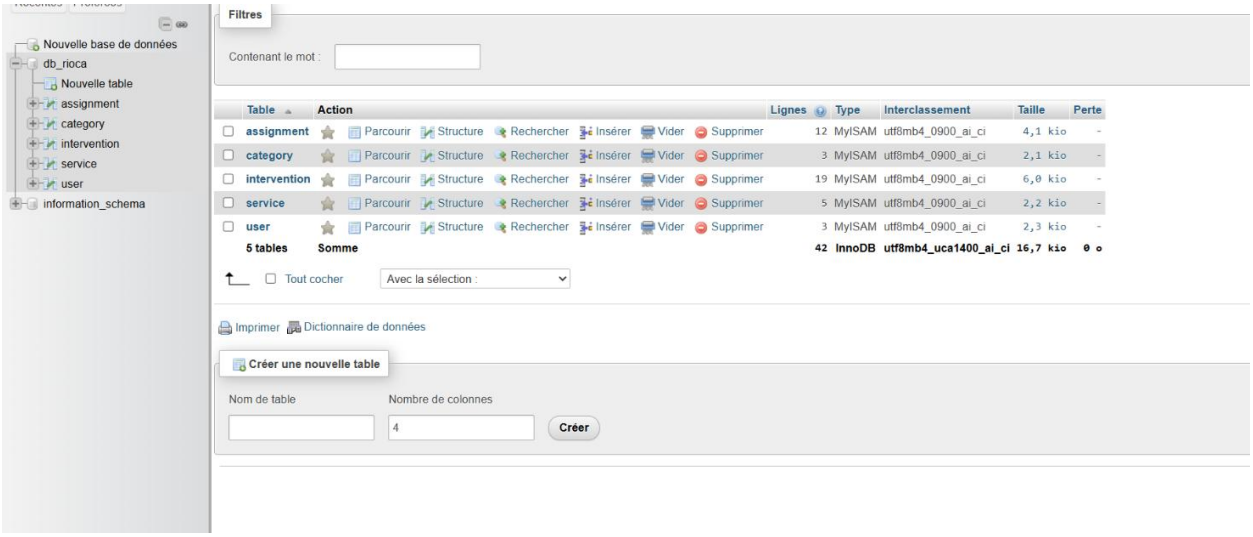
Compte	Hôte autorisé	Droits
RIOCAENLI (compte développeur imposé, validé par la professeure)	10.31.10.11 (SRV-WEB1 uniquement)	ALL PRIVILEGES sur db_rioca.* uniquement
Comptes système (root, mysql, mariadb.sys)	localhost	Comptes système

```
groupe3@srv-bdd-3:~$

groupe3@srv-bdd-3:~$ sudo mariadb -e "SELECT user,host FROM mysql.user;"
[sudo: authenticate] Password:
+-------------+-------------+
| User        | Host        |
+-------------+-------------+
| RIOCAENLI   | 10.31.10.11 |
| mariadb.sys | localhost   |
| mysql       | localhost   |
| root        | localhost   |
+-------------+-------------+
```

Capture : SELECT user,host FROM mysql.user; : RIOCAENLI n'existe que depuis 10.31.10.11 (carte 8)

```
MariaDB [(none)]> SHOW GRANTS FOR 'RIOCAENLI'@'10.31.10.11';
+-----------------------------------------------------------------------------------------------------------------+
| Grants for RIOCAENLI@10.31.10.11                                                                                |
+-----------------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `RIOCAENLI`@`10.31.10.11` IDENTIFIED BY PASSWORD '[redacted]' |
| GRANT ALL PRIVILEGES ON `db_rioca`.* TO `RIOCAENLI`@`10.31.10.11`                                               |
+-----------------------------------------------------------------------------------------------------------------+
2 rows in set (0,000 sec)
```

Capture : SHOW GRANTS FOR 'RIOCAENLI'@'10.31.10.11'; : ALL PRIVILEGES sur db_rioca. uniquement, empreinte du mot de passe masquée (carte 8)*



Capture : phpMyAdmin : les 5 tables de db_rioca après l'import du fichier SQL des SLAM (carte 8)

7.4 Double filtrage

- UFW sur la VM : actif, OpenSSH autorisé, TCP 3306 autorisé uniquement depuis 10.31.10.11. Le reste du trafic entrant est refusé par défaut.
- Zyxel : règle DMZ_WEB_to_BDD (voir §10).

La base n'est jamais exposée au campus ni au LAN. Les développeurs passent par phpMyAdmin sur SRV-WEB1.

```
groupe3@srv-bdd-3:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] OpenSSH                    ALLOW IN    Anywhere
[ 2] 3306/tcp                   ALLOW IN    10.31.10.11                # SRV-WEB1
[ 3] OpenSSH (v6)               ALLOW IN    Anywhere (v6)

groupe3@srv-bdd-3:~$
```

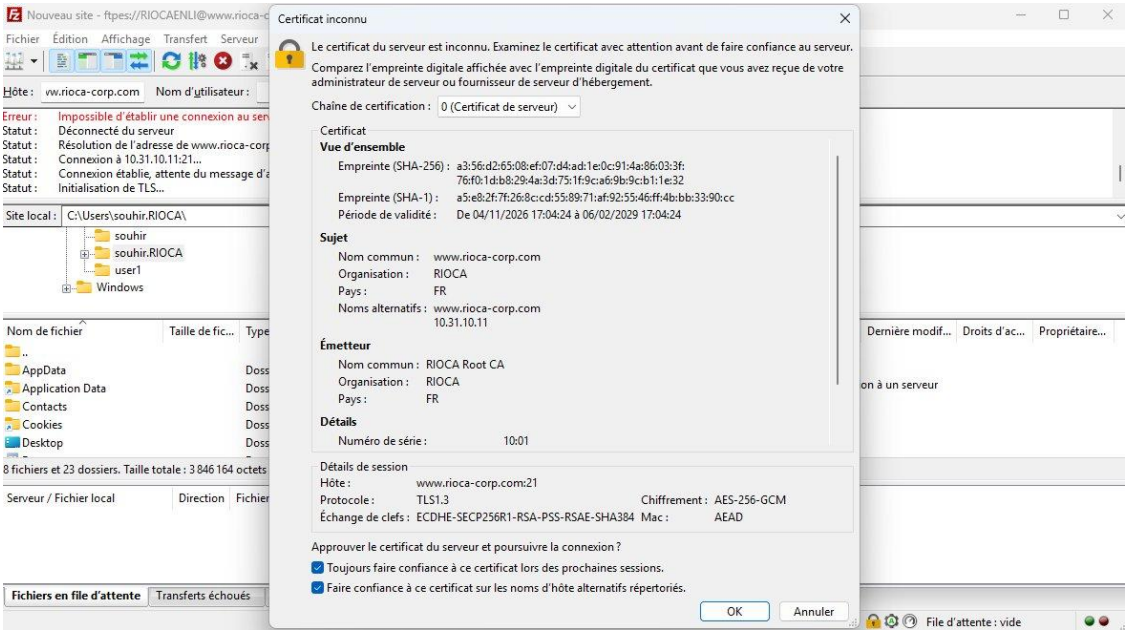
Capture : sudo ufw status numbered : 3306/tcp autorisé uniquement depuis 10.31.10.11 (SRV-WEB1) (carte 8)

8. Serveur FTPS (SRV-WEB1)

Le FTPS permet aux seuls développeurs de déposer les fichiers du site de façon chiffrée.

Paramètre	Valeur
Service	vsftpd 3.0.5, FTPS explicite sur le port 21
TLS	Obligatoire pour le login et les données (`force_local_logins_ssl=YES`, `force_local_data_ssl=YES`)
Accès	Anonyme désactivé, liste blanche, compte RIOCAENLI sans shell
Dossier	/var/www/rioca (chroot), groupe www-data
Mode passif	Plage fixe 40000 à 40100 (pour le filtrage pare-feu)
Certificat	Signé par RIOCA Root CA (numéro de série 1001), clé privée lisible par root uniquement

Tests : voir T5, T15 et T19 dans le rapport de tests (partie 12).



Capture : *certificat du serveur affiché dans FileZilla (carte 16)*

```
maxime@srv-web:~$ grep -E 'ssl_enable|force_local|require_ssl|rsa_cert_file' /etc/vsftpd.conf
ssl_enable=YES
rsa_cert_file=/etc/ssl/certs/vsftpd.crt
force_local_logins_ssl=YES
force_local_data_ssl=YES
require_ssl_reuse=NO
maxime@srv-web:~$
```

Capture : vsftpd : TLS activé et forcé pour la connexion et les données (carte 18)

```
maxime@srv-web:~$ grep -E 'pasv' /etc/vsftpd.conf
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=40100
pasv_address=172.18.53.1
maxime@srv-web:~$
```

Capture : vsftpd : ports passifs 40000 à 40100 (carte 18)

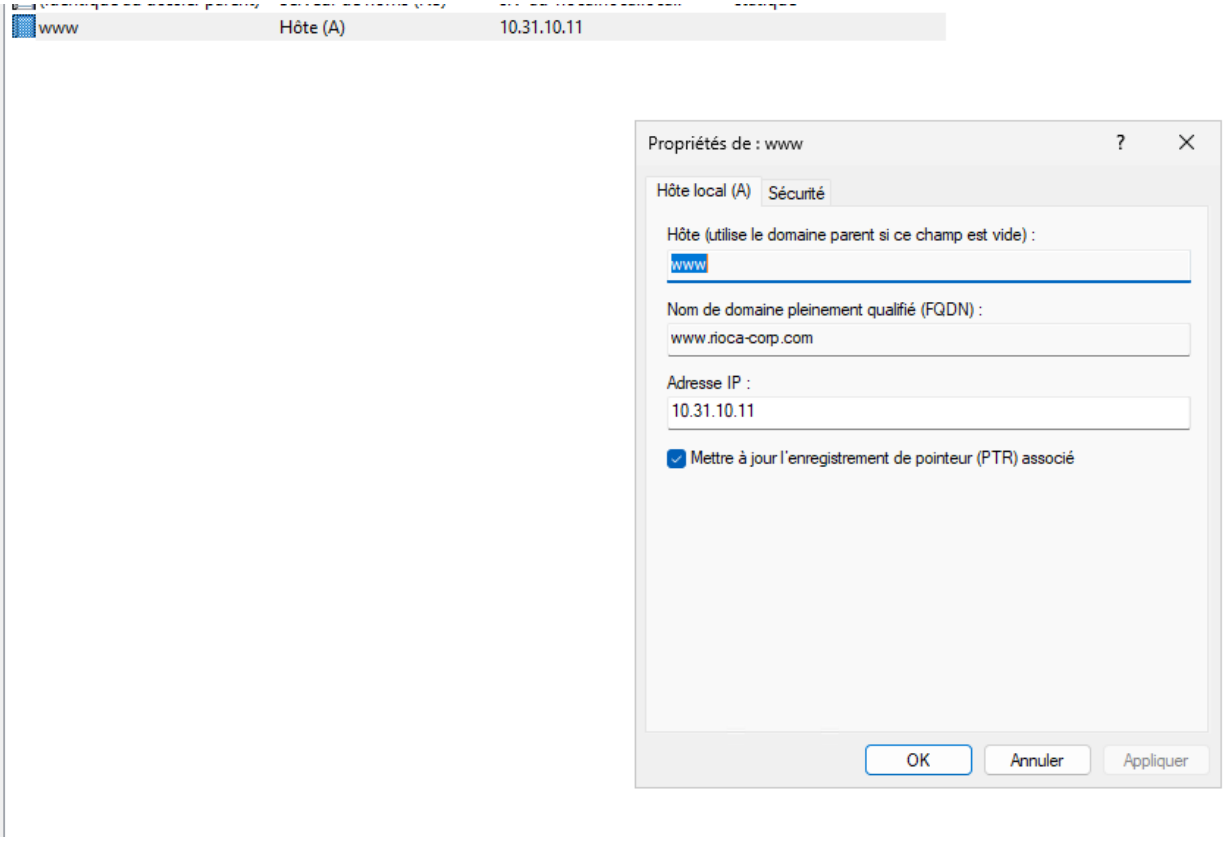
9. Serveur DNS (BIND9 sur SRV-WEB1)

9.1 Configuration

- BIND9 installé sur la VM du serveur Web (pas de VM DNS séparée).
- `/etc/bind/named.conf.options` : configuration de serveur faisant autorité (récursivité désactivée, transferts de zone interdits, redirecteurs supprimés). La configuration initiale était celle d'un résolveur récursif.
- `/etc/bind/named.conf.local` : zone rioca-corp.com de type master, fichier `/etc/bind/db.rioca-corp.com`, `allow-transfer { none; }`.
- Fichier de zone : SOA ns1.rioca-corp.com, enregistrement NS ns1, enregistrements A ns1 et www vers 10.31.10.11.

9.2 Intégration à l'Active Directory

Les postes du LAN interrogent le DNS de l'AD (SRV-AD-RIOCA, 172.19.100.2). La zone rioca-corp.com y est aussi déclarée, avec le même enregistrement www (A) vers 10.31.10.11 que sur BIND9 : les deux serveurs renvoient la même adresse.



Capture : console DNS de SRV-AD-RIOCA : enregistrement www (A) vers 10.31.10.11 dans la zone rioca-corp.com (carte 20)

9.3 Résolution selon le réseau

Depuis	DNS interrogé	www.rioca-corp.com renvoie
LAN	172.19.100.2 (AD)	10.31.10.11
Wi-Fi du campus	172.17.172.4 (DNS du campus)	172.18.53.1 (adresse publiée par le NAT de RNET2)

Tests : voir T3, T4 et T17 dans le rapport de tests (partie 12).

```
maxime@srv-web:~$ sudo named-checkconf
maxime@srv-web:~$
maxime@srv-web:~$ sudo systemctl restart named
maxime@srv-web:~$ systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Fri 2026-11-13 11:33:59 CET; 7s ago
 Invocation: 07acf824b5404411bf8ffd59f247bd91
       Docs: man:named(8)
   Main PID: 4539 (named)
     Status: "running"
      Tasks: 8 (limit: 2223)
     Memory: 30.2M (peak: 30.3M)
        CPU: 30ms
     CGroup: /system.slice/named.service
             └─4539 /usr/sbin/named -f -u bind
maxime@srv-web:~$
maxime@srv-web:~$
maxime@srv-web:~$
maxime@srv-web:~$
maxime@srv-web:~$ cat /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
    listen-on { any; };
    listen-on-v6 { none; };
    allow-query { any; };
    recursion no;
    allow-transfer { none; };
    dnssec-validation no;
};
maxime@srv-web:~$
```

Capture : named.conf.options : serveur faisant autorité, récursivité désactivée, transferts interdits (carte 20)

```
maxime@srv-web:~$ cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

zone "rioca-corp.com" {
        type master;
        file "/etc/bind/db.rioca-corp.com";
        allow-transfer { none;};
};
maxime@srv-web:~$ $
-bash: $ : commande introuvable
maxime@srv-web:~$
maxime@srv-web:~$
maxime@srv-web:~$ sudo named-checkconf
maxime@srv-web:~$
```

Capture : named.conf.local : zone rioca-corp.com de type master (carte 20)

```
maxime@srv-web:~$ cat /etc/bind/db.rioca-corp.com
$TTL    86400
@   IN   SOA ns1.rioca-corp.com. admin.rioca-corp.com. (
        2026110501 ; Serial
        3600       ; Refresh
        1800       ; Retry
        604800     ; Expire
        86400  )   ; Minimum TTL

@       IN  NS ns1.rioca-corp.com.
ns1 IN A  10.31.10.11
www IN A  10.31.10.11
maxime@srv-web:~$ sudo named-checkzone rioca-corp.com /etc/bind/db.rioca-corp.com
zone rioca-corp.com/IN: loaded serial 2026110501
OK
maxime@srv-web:~$ ss -tulnp | grep :53
udp   UNCONN 0      0        10.31.10.11:53        0.0.0.0:*
udp   UNCONN 0      0        10.31.10.11:53        0.0.0.0:*
udp   UNCONN 0      0          127.0.0.1:53        0.0.0.0:*
udp   UNCONN 0      0          127.0.0.1:53        0.0.0.0:*
tcp   LISTEN 0      10         127.0.0.1:53        0.0.0.0:*
tcp   LISTEN 0      10         127.0.0.1:53        0.0.0.0:*
tcp   LISTEN 0      10       10.31.10.11:53        0.0.0.0:*
tcp   LISTEN 0      10       10.31.10.11:53        0.0.0.0:*
maxime@srv-web:~$ dig @localhost www.rioca-corp.com +short
;; communications error to ::1#53: connection refused
;; communications error to ::1#53: connection refused
;; communications error to ::1#53: connection refused
10.31.10.11
maxime@srv-web:~$
```

Capture : fichier de zone db.rioca-corp.com, named-checkzone OK, écoute sur le port 53 (carte 20)

```
maxime@srv-web:~$ dig @127.0.0.1 www.rioca-corp.com

; <<>> DiG 9.20.30-1~deb13u1-Debian <<>> @127.0.0.1 www.rioca-corp.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22020
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 2f5a279fc15c192d010000006af6f95bad35c4f2465be710 (good)
;; QUESTION SECTION:
;www.rioca-corp.com.            IN      A

;; ANSWER SECTION:
www.rioca-corp.com.     86400   IN      A       10.31.10.11

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Fri Nov 13 12:49:47 CET 2026
;; MSG SIZE  rcvd: 91

maxime@srv-web:~$
```

Capture : dig @127.0.0.1 www.rioca-corp.com : NOERROR, drapeau aa, réponse 10.31.10.11 (carte 20)

10. Pare-feu Zyxel : règles de filtrage

Les règles d'accès sont en allow avec journalisation, placées au-dessus des refus par défaut. Deux règles de refus isolent les DMZ. Les flux sans règle sont bloqués par la règle par défaut (DROP).

Règle	Source → destination	Service	Rôle
LAN_to_WebServ	LAN_ALL (172.19.0.0/16) → DMZ_WEB3 (10.31.10.11)	WEB (HTTP 80, HTTPS 443, DNS 53)	Accès des postes au site par le FQDN
LAN_to_SRV-WEB1_FTPS	LAN_ALL → DMZ_WEB3	FTPS_GRP (FTP 20-21 et passifs 40000-40100)	Administration et tests depuis le LAN
DMZ_WEB_to_BDD	DMZ_WEB3 (10.31.10.11) → SRV_MARIADB (10.32.10.31)	MariaDB_3306	Le site interroge la base
DMZINT_to_Internet	DMZ_INT → WAN	G_INTERNET_SERVICES (+ NTP)	Mises à jour de la DMZ interne
Campus_vers_WebFTPS	Campus 172.18.0.0/16 → serveur Web	G_WebFTPS (HTTP, HTTPS, FTPS_GRP)	Accès des développeurs depuis le Wi-Fi
Isolation_DMZ_LAN	DMZ → LAN	tous	Refus : la DMZ ne peut pas initier vers le LAN
DMZINT_to_DMZWEB_Deny	DMZ interne → DMZ intermédiaire	tous	Refus d'isolation entre les deux DMZ
Campus_vers_MariaDB	Campus → BDD	3306	Désactivée, pour ne pas exposer la base

Objets utilisés dans les règles :

Objet	Type	Valeur	Utilisé par
LAN_ALL	Sous-réseau	172.19.0.0/16	LAN_to_WebServ, LAN_to_SRV-WEB1_FTPS
DMZ_WEB3	Hôte	10.31.10.11 (SRV-WEB1)	Règles Web, FTPS et BDD
SRV_MARIADB	Hôte	10.32.10.31 (srv-bdd-3)	DMZ_WEB_to_BDD
WEB	Services	HTTP 80, HTTPS 443, DNS 53 (TCP et UDP)	LAN_to_WebServ
MariaDB_3306	Service	TCP 3306	DMZ_WEB_to_BDD
FTPS_GRP	Groupe de services	FTP TCP 20-21 + FTPS_PASSIF TCP 40000-40100	Règles FTPS
G_WebFTPS	Groupe de services	HTTP, HTTPS, FTPS_GRP	Campus_vers_WebFTPS

Remarque :

- Les postes du VLAN IT (172.19.60.x) passent par la règle d'administration G_ADMIN_IT, créée pendant le projet Infra-Site et placée avant LAN_to_WebServ : dans les logs, c'est elle qui apparaît pour ces postes.


Show Filter
Allow Asymmetrical Route
Add Edit Remove Activate Inactivate Move Clone

Priority	Status	Name	From	To	IPv4 Source	IPv4 Destination	Service	User	Schedule	Action	Log	Profile
1		Campus_vers_WebFTPS	WAN	DMZ	CAMPUS_172_18	DMZ_WEB3	G_WebFTPS	any	none	allow	log	
2		Campus_vers_MariaDB	WAN	DMZ	CAMPUS_172_18	SRV_MARIADB	MariaDB_3306	any	none	allow	log	
3		LAN_to_SRV-WEB1_FTPS	LAN1	DMZ	LAN_ALL	DMZ_WEB3	FTPS_GRP	any	none	allow	log	
4		DMZ_WEB_to_BDD	DMZ	DMZ	DMZ_WEB3	SRV_MARIADB	MariaDB_3306	any	none	allow	log	
5		DMZINT_to_Internet	DMZ	WAN	DMZ_interne	any	G_INTERNET_SER...	any	none	allow	log	
6		ADMIN_IT_EXTERNE	WAN	ZyWALL	IT_EXTERNE	any	G_ADMIN_IT	any	none	allow	log	
7		Admin_IT_Local	LAN1	any (Excluding Zy...	LAN_IT	any	G_ADMIN_IT	any	none	allow	log	
8		Admin_IT_Distant	LAN1	ZyWALL	LAN_IT	any	G_ADMIN_IT	any	none	allow	log	
9		Allow_RIPv2	any	ZyWALL	any	any	RIP	any	none	allow	log	
10		Allow_TFTP_Backups	any	LAN1	EQUIP_BACKUP	TFTP_SRV	TFTP	any	none	allow	log	
11		Internet_to_WebServ	WAN	DMZ	any	DMZ_WEB_GRP	WEB	any	none	allow	log	
12		LAN_to_WebServ	LAN1	DMZ	LAN_ALL	DMZ_WEB3	WEB	any	none	allow	log	
13		LAN_to_Internet	LAN1	WAN	LAN_ALL	any	G_INTERNET_SER...	any	none	allow	log	
14		DMZ_to_Internet	DMZ	WAN	DMZ_SUBNET	any	G_INTERNET_SER...	any	none	allow	log	
15		Isolation_DMZ_LAN	DMZ	LAN1	any	any	any	any	none	deny	log	
16		LAN1_Outgoing	LAN1	any (Excluding Zy...	any	any	any	any	none	deny	log	
17		LAN2_Outgoing	LAN2	any (Excluding Zy...	any	any	any	any	none	allow	no	
18		DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	deny	no	
19		IPSec_VPN_Outgoing	IPSec_VPN	any (Excluding Zy...	any	any	any	any	none	allow	no	
20		SSL_VPN_Outgoing	SSL_VPN	any (Excluding Zy...	any	any	any	any	none	allow	no	
21		TUNNEL_Outgoing	TUNNEL	any (Excluding Zy...	any	any	any	any	none	allow	no	
22		LAN1_to_Device	LAN1	ZyWALL	any	any	any	any	none	deny	log	
23		LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	none	allow	no	
24		DMZ_to_Device	DMZ	ZyWALL	any	any	Default_Allow_D...	any	none	deny	log	
25		WAN_to_Device	WAN	ZyWALL	any	any	Default_Allow_W...	any	none	deny	log	
26		IPSec_VPN_to_Device	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	no	
27		SSL_VPN_to_Device	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no	
28		TUNNEL_to_Device	TUNNEL	ZyWALL	any	any	any	any	none	allow	no	
Default			any	any	any	any	any	any	none	deny	log	

Page 1 of 1 Show 50 items — Displaying 1 - 29 of 29

Capture : liste des règles du Zyxel (état final)


3 DMZ_WEB_to_BDD DMZ DMZ_INT DMZ_WEB3 SRV_MAR... MariaDB_... any none allow log

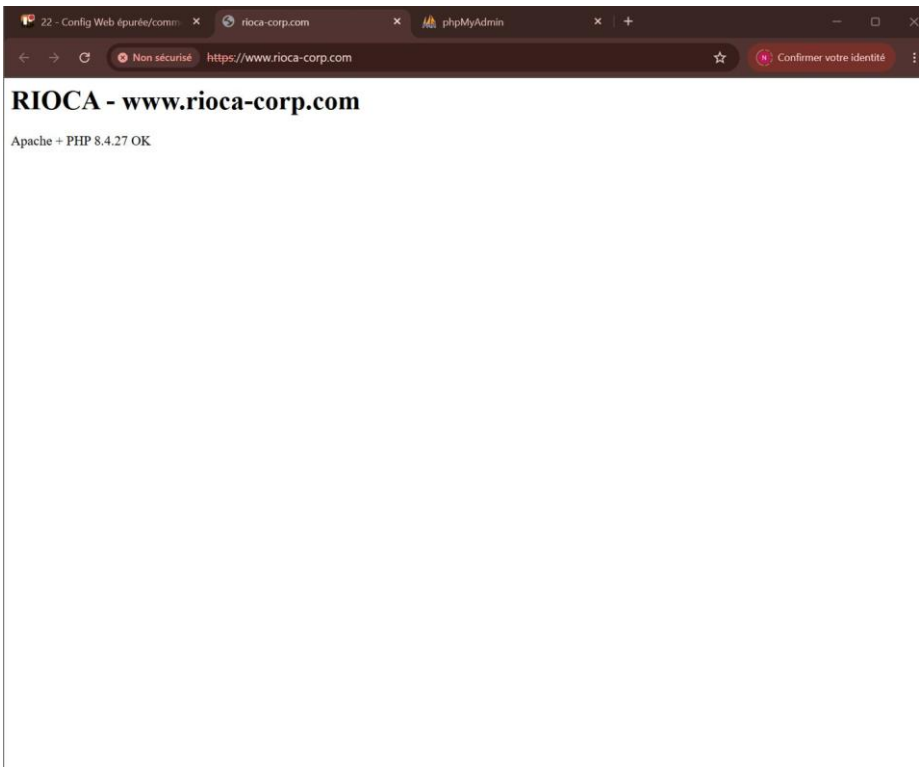
Capture : règle DMZ_WEB_to_BDD : DMZ vers DMZ_INT, DMZ_WEB3 vers SRV_MARIADB, service MariaDB_3306 (carte 18)

11. Accès des développeurs depuis le Wi-Fi (tâche non prévue)

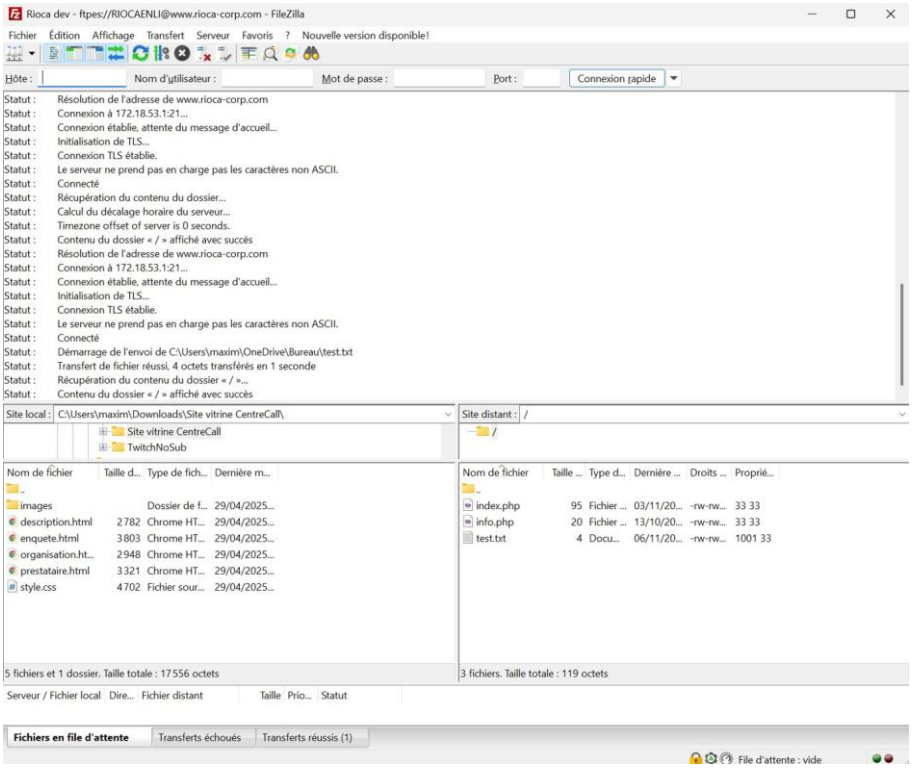
Les développeurs SLAM, connectés au Wi-Fi du campus et hors domaine, doivent atteindre le site, phpMyAdmin et le FTPS.

- NAT statique sur RNET2 : 172.18.53.1 vers SRV-WEB1 (10.31.10.11). Une erreur initiale pointait vers 10.31.10.1 (hyperviseur), corrigée.
- Route statique sur le Zyxel : 172.18.0.0/16 via RNET2 (192.168.3.250). Sans elle, le flux retour était perdu, car RNET2 était en Standby HSRP.
- Base de données jamais exposée : accès uniquement par phpMyAdmin sur SRV-WEB1.
- Postes hors domaine : import du certificat RIOCA Root CA décrit dans le document des développeurs.

Tests : voir T4 et T19 dans le rapport de tests (partie 12).



Capture : *site accessible depuis le Wi-Fi (carte 44)*



Capture : *FileZilla depuis le Wi-Fi : dépôt de test réussi (carte 44)*

12. Rapport de tests

Chaque test a un numéro, une commande, le résultat obtenu et une preuve. Pour les tests de filtrage, la commande est suivie du log Zyxel qui montre la règle appliquée (ACCEPT ou DROP). Quand la preuve est déjà dans une partie précédente, le test y renvoie.

Test	Commande ou méthode	Résultat	Statut
T1 – LAN vers Web HTTPS	Test-NetConnection 10.31.10.11 -Port 443	TcpTestSucceeded True, ACCEPT (poste du VLAN IT, donc règle G_ADMIN_IT)	Validé
T2 – Site par le nom	https://www.rioca-corp.com depuis le LAN	Page affichée sans alerte, certificat RIOCA Root CA	Validé
T3 – Résolution DNS LAN	nslookup www.rioca-corp.com	10.31.10.11	Validé
T4 – Résolution DNS Wi-Fi	nslookup depuis le Wi-Fi	172.18.53.1	Validé
T5 – LAN vers FTPS	Test-NetConnection 10.31.10.11 -Port 21	True, ACCEPT (FTPS_GRP)	Validé
T6 – Port 990 (témoin)	Test-NetConnection 10.31.10.11 -Port 990	False, DROP : aucun service n'écoute	Validé
T7 – Web vers BDD	/dev/tcp/10.32.10.31/3306 depuis SRV-WEB1	Port ouvert, ACCEPT (DMZ_WEB_to_BDD)	Validé
T8 – LAN vers BDD (flux interdit)	Test-NetConnection 10.32.10.31 -Port 3306	False, DROP (règle par défaut)	Validé
T9 – DMZ vers LAN (flux interdit)	/dev/tcp/172.19.60.1/445 depuis SRV-WEB1	Bloqué, DROP (Isolation_DMZ_LAN)	Validé
T10 – Flux sans règle	Test-NetConnection 10.31.10.11 -Port 8080	False, DROP (règle par défaut)	Validé
T11 – Sortie Internet DMZ interne	Depuis srv-bdd-3 : ping 8.8.8.8 et nslookup deb.debian.org	0 % de perte, nom résolu, ACCEPT	Validé
T12 – UFW sur la BDD	ufw status numbered	3306 autorisé depuis 10.31.10.11 seulement	Validé
T13 – Compte RIOCAENLI	phpMyAdmin, SHOW DATABASES;	Seulement db_rioca et information_schema	Validé
T14 – Droits du compte	SHOW GRANTS	ALL PRIVILEGES sur db_rioca.* uniquement	Validé
T15 – FTPS chiffré	FileZilla en TLS 1.3	Connexion et dépôt OK (chroot), refus sans TLS et refus d'un compte non autorisé (530)	Validé
T16 – TLS	Tests des versions TLS avec openssl s_client	TLS 1.0/1.1 refusés, 1.2/1.3 acceptés	Validé
T17 – BIND9	named-checkconf, named-checkzone, dig	Aucune erreur, NOERROR avec drapeau aa	Validé
T18 – DMZ interne vers Web (flux interdit)	curl -k -m 5 https://10.31.10.11 depuis srv-bdd-3	Timeout, DROP (DMZINT_to_DMZWEB_Deny)	Validé
T19 – Wi-Fi vers site (développeurs)	Test-NetConnection 172.18.53.1 -Port 443 depuis le Wi-Fi	True, site affiché et dépôt FileZilla OK	Validé
T20 – Site relié à la base	Connexion d'un utilisateur sur le site SLAM en HTTPS	Connexion validée avec la base db_rioca	Validé

Preuves des tests

T1 – LAN vers Web HTTPS

```
   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::eaa9:70c5:906b:c892%2
   Adresse IPv4. . . . . . . . . . . . . .: 172.19.60.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.19.60.254

Carte réseau sans fil Connexion au réseau local* 9 :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Connexion au réseau local* 10 :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Wi-Fi :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
PS C:\Users\admin> Test-NetConnection 10.31.10.11 -Port 443


ComputerName     : 10.31.10.11
RemoteAddress    : 10.31.10.11
RemotePort       : 443
InterfaceAlias   : Ethernet 3
SourceAddress    : 172.19.60.1
TcpTestSucceeded : True


PS C:\Users\admin>
```

Capture : Test-NetConnection 10.31.10.11 -Port 443 depuis le LAN : True (carte 19)

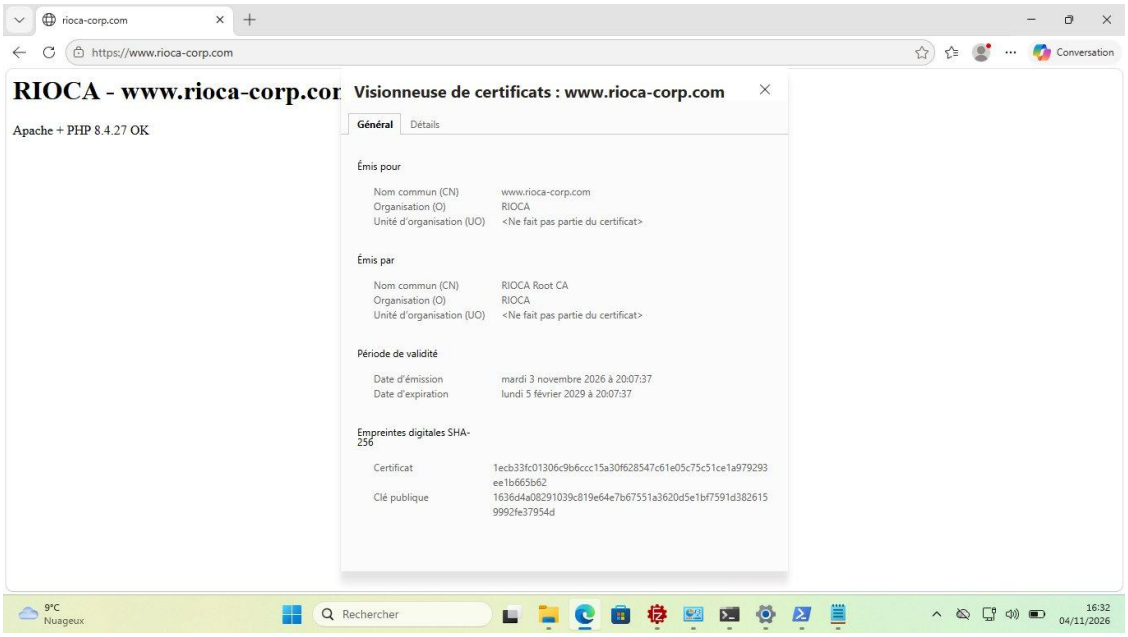
Email Log Now | Refresh | Clear

#	Time	Priority	Category	Message	Source	Destination	Note
1	202...	notice	Security Policy Control	priority:8, from LAN1 to ZyWALL, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:52653	192.168.2.2:443	ACCESS FORWARD
2	202...	notice	Security Policy Control	priority:8, from LAN1 to ZyWALL, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:62754	192.168.2.2:443	ACCESS FORWARD
3	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52690	80.10.246.2:53	ACCESS FORWARD
4	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, TCP, service G_INTERNET_SERVICES, A...	10.32.10.31:36146	151.101.130.49:443	ACCESS FORWARD
5	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.31:60398	8.8.8.8:53	ACCESS FORWARD
6	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.31:35832	8.8.8.8:53	ACCESS FORWARD
7	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.31:59634	8.8.8.8:53	ACCESS FORWARD
8	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.31:54024	8.8.8.8:53	ACCESS FORWARD
9	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, TCP, service G_INTERNET_SERVICES, A...	10.32.10.31:50714	151.101.2.49:443	ACCESS FORWARD
10	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.31:57211	8.8.8.8:53	ACCESS FORWARD
11	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.31:57106	8.8.8.8:53	ACCESS FORWARD
12	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.31:33168	8.8.8.8:53	ACCESS FORWARD
13	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.31:58002	8.8.8.8:53	ACCESS FORWARD
14	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, TCP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:49941	52.178.17.238:443	ACCESS FORWARD
15	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52644	80.10.246.2:53	ACCESS FORWARD
16	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=2]	172.19.60.1:137	10.31.10.11:137	ACCESS BLOCK
17	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64661	80.10.246.2:53	ACCESS FORWARD
18	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:50231	95.217.148.210:443	ACCESS FORWARD
19	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=4]	172.19.60.1:137	10.31.10.11:137	ACCESS BLOCK
20	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:65162	80.10.246.2:53	ACCESS FORWARD
21	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:54195	10.31.10.11:443	ACCESS FORWARD
22	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.5:54362	52.123.242.155:443	ACCESS FORWARD
23	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52274	80.10.246.2:53	ACCESS FORWARD

Page 1 of 1 | Show 200 items | Displaying 1 - 23 of 23

Capture : log Zyxel : flux du LAN vers 10.31.10.11:443 en ACCEPT, règle G_ADMIN_IT (carte 19)

T2 – Site par le nom



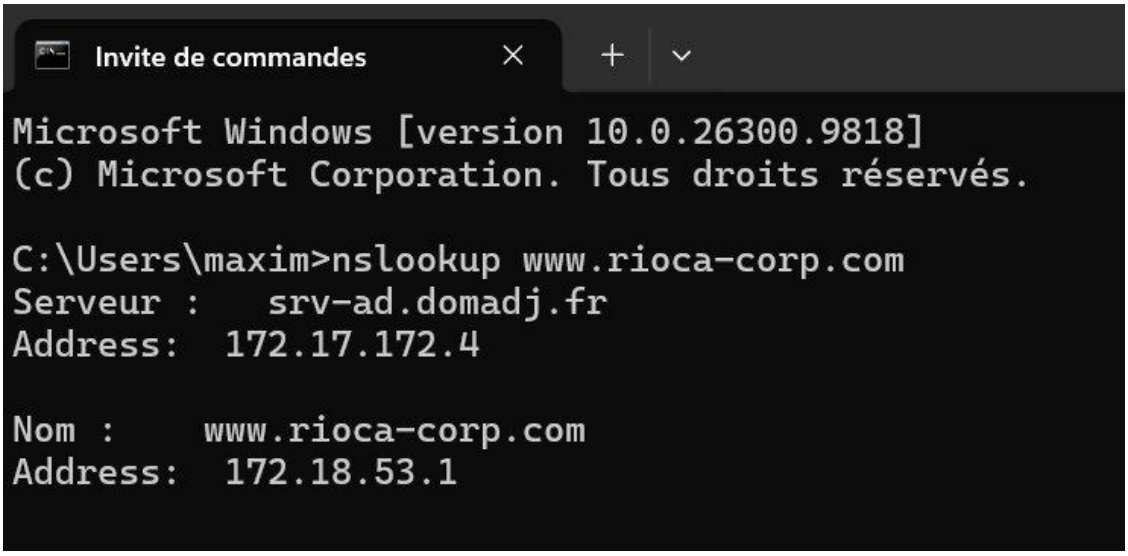
Capture : *site en HTTPS sans alerte depuis un poste du domaine (cartes 11 et 13)*

T3 – Résolution DNS LAN

```
PS C:\WINDOWS\system32> ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.
PS C:\WINDOWS\system32> nslookup www.rioca-corp.com
Serveur :   UnKnown
Address:  172.19.100.2

Nom :    www.rioca-corp.com
Address:  10.31.10.11

PS C:\WINDOWS\system32>
```

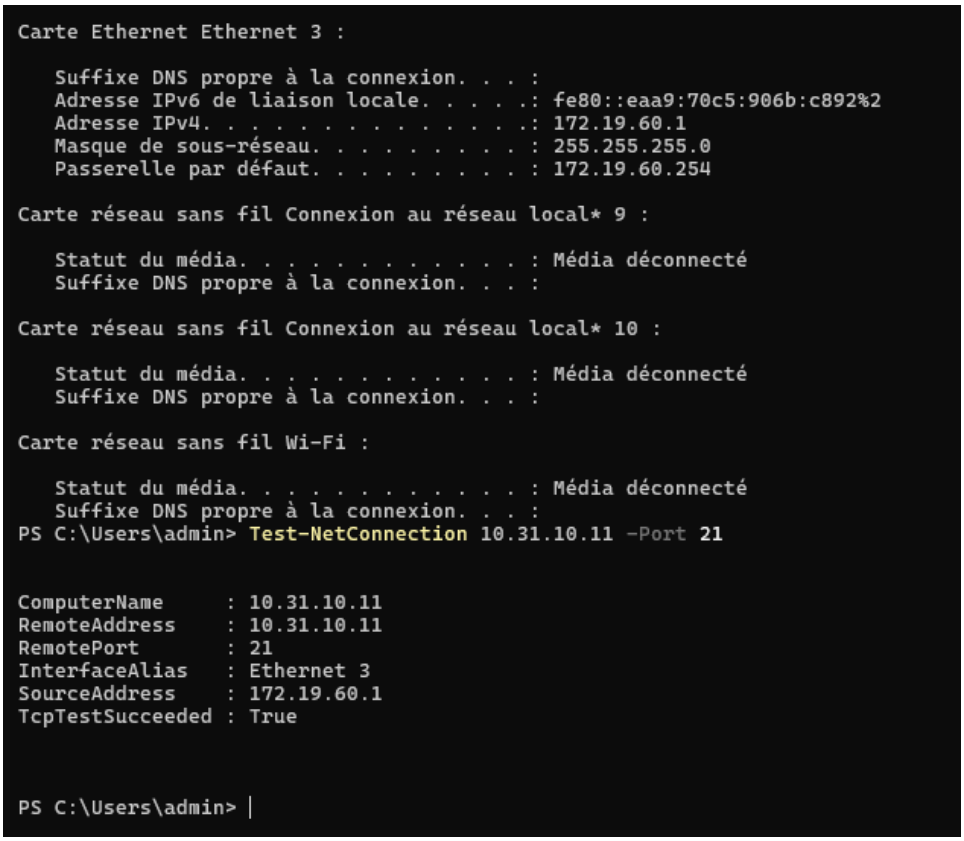
Capture : *nslookup depuis le LAN : www.rioca-corp.com (carte 21)*

T4 – Résolution DNS Wi-Fi



Capture : *nslookup depuis le Wi-Fi via le DNS du campus (carte 44)*

T5 – LAN vers FTPS



Capture : Test-NetConnection 10.31.10.11 -Port 21 depuis le LAN : True (carte 19)

Email Log Now | Refresh | Clear

#	Time	Priority	Category	Message	Source	Destination	Note
1	202...	notice	Security Policy Control	priority:8, from LAN1 to ZyWALL, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:65048	192.168.2.2:443	ACCESS FORWARD
2	202...	notice	Security Policy Control	priority:8, from LAN1 to ZyWALL, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:56048	192.168.2.2:443	ACCESS FORWARD
3	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=2]	172.19.60.1:137	10.31.10.11:137	ACCESS BLOCK
4	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64503	80.10.246.2:53	ACCESS FORWARD
5	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:65483	80.10.246.2:53	ACCESS FORWARD
6	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:49309	80.10.246.2:53	ACCESS FORWARD
7	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52878	80.10.246.2:53	ACCESS FORWARD
8	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64646	80.10.246.2:53	ACCESS FORWARD
9	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=6]	172.19.60.2:65004	172.217.114.4:443	ACCESS BLOCK
10	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.2:54386	172.217.114.4:443	ACCESS FORWARD
11	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52390	80.10.246.2:53	ACCESS FORWARD
12	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64174	80.10.246.2:53	ACCESS FORWARD
13	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52384	80.10.246.2:53	ACCESS FORWARD
14	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64902	80.10.246.2:53	ACCESS FORWARD
15	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52400	80.10.246.2:53	ACCESS FORWARD
16	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.2:61939	40.126.31.3:443	ACCESS FORWARD
17	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:65302	80.10.246.2:53	ACCESS FORWARD
18	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.2:61937	20.190.160.14:443	ACCESS FORWARD
19	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.2:61936	20.190.160.14:443	ACCESS FORWARD
20	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64497	80.10.246.2:53	ACCESS FORWARD
21	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=4]	172.19.60.1:137	10.31.10.11:137	ACCESS BLOCK
22	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:65129	80.10.246.2:53	ACCESS FORWARD
23	202...	notice	Security Policy Control	priority:2, from LAN1 to DMZ, TCP, service FTPS_GRP, ACCEPT	172.19.60.1:60804	10.31.10.11:21	ACCESS FORWARD
24	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:60800	92.122.166.7:80	ACCESS FORWARD
25	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:65441	80.10.246.2:53	ACCESS FORWARD
26	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52800	80.10.246.2:53	ACCESS FORWARD

Page 1 of 1 Show 200 items Displaying 1 - 26 of 26

Capture : log Zyxel : flux du LAN vers 10.31.10.11:21 en ACCEPT, service FTPS_GRP (carte 19)

T6 – Port 990 (témoin)

Test témoin : aucun service n'écoute sur le port 990, la connexion échoue (False). Il montre que le FTPS passe bien par le port 21.

T7 – Web vers BDD

```
maxime@srv-web:~$ timeout 3 bash -c '</dev/tcp/10.32.10.31/3306' && echo "Port 3306 ouvert" || echo "Port 3306 fermé"
Port 3306 ouvert
maxime@srv-web:~$
```

Capture : srv-web vers 10.32.10.31:3306 via /dev/tcp : Port 3306 ouvert (carte 19)

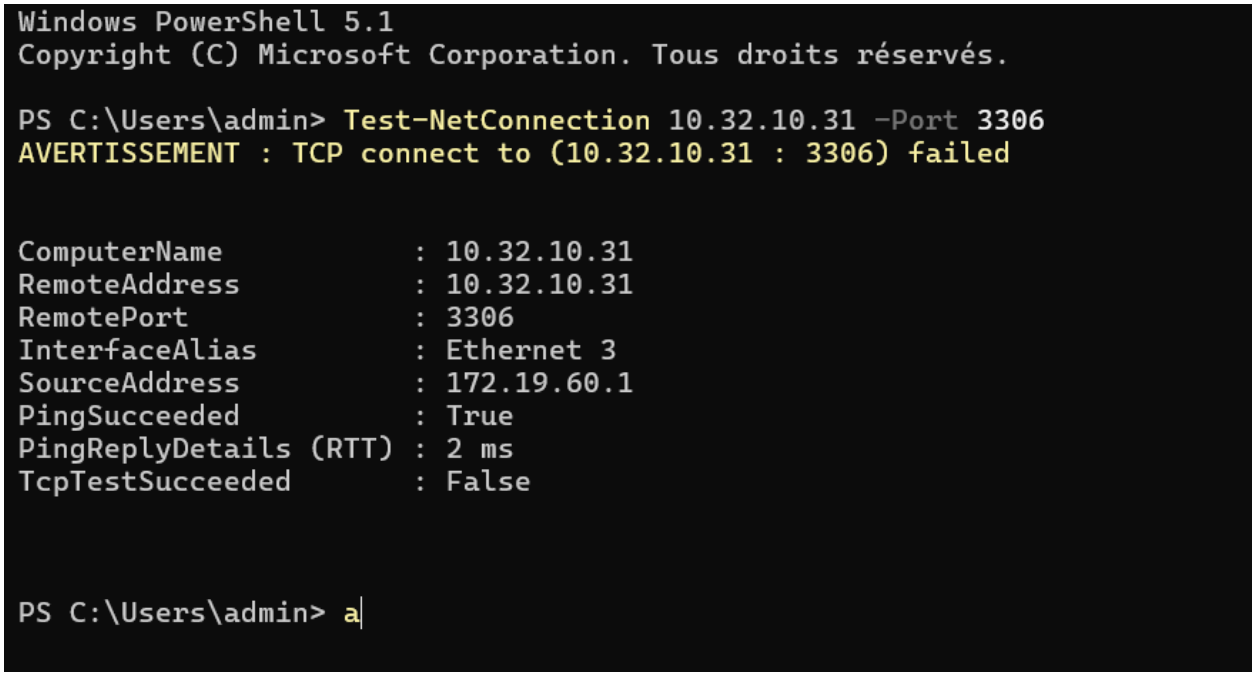
Email Log Now | Refresh | Clear

#	Time	Priority	Category	Message	Source	Destination	Note
1	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.2:1938	160.79.104.10:443	ACCESS FORWARD
2	202...	notice	Security Policy Control	priority:3, from DMZ to DMZ_INT, TCP, service MariaDB_3306, ACCEPT	10.31.10.11:48878	10.32.10.31:3306	ACCESS FORWARD
3	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:57989	20.190.160.67:443	ACCESS FORWARD
4	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52592	80.10.246.2:53	ACCESS FORWARD

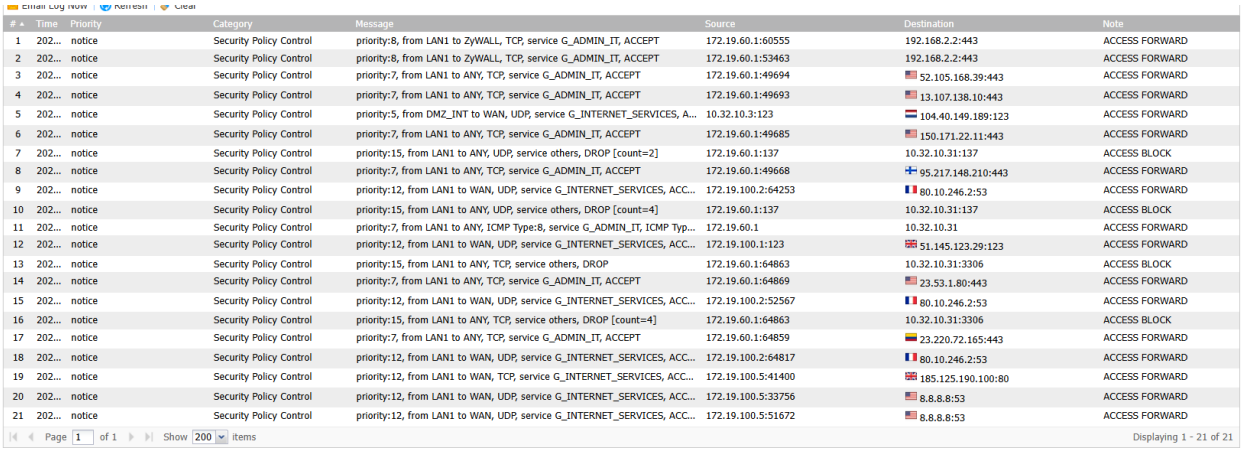
Page 1 of 1 Show 200 items Displaying 1 - 4 of 4

Capture : log Zyxel : ACCEPT de DMZ vers DMZ_INT, service MariaDB_3306 (carte 19)

T8 – LAN vers BDD (flux interdit)



Capture : LAN vers 10.32.10.31:3306 : TcpTestSucceeded False (carte 19)

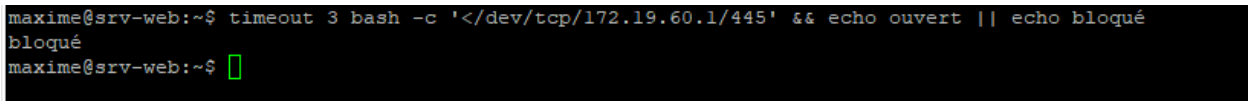


#	Time	Priority	Category	Message	Source	Destination	Note
1	202...	notice	Security Policy Control	priority:8, from LAN1 to ZyWALL, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:60555	192.168.2.2:443	ACCESS FORWARD
2	202...	notice	Security Policy Control	priority:8, from LAN1 to ZyWALL, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:53463	192.168.2.2:443	ACCESS FORWARD
3	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:49694	52.105.168.39:443	ACCESS FORWARD
4	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:49693	13.107.138.10:443	ACCESS FORWARD
5	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.3:123	104.40.149.189:123	ACCESS FORWARD
6	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:49685	150.171.22.11:443	ACCESS FORWARD
7	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=2]	172.19.60.1:137	10.32.10.31:137	ACCESS BLOCK
8	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:49668	95.217.148.210:443	ACCESS FORWARD
9	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64253	80.10.246.2:53	ACCESS FORWARD
10	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=4]	172.19.60.1:137	10.32.10.31:137	ACCESS BLOCK
11	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, ICMP Type:8, service G_ADMIN_IT, ICMP Typ...	172.19.60.1	10.32.10.31	ACCESS FORWARD
12	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.1:123	51.145.123.29:123	ACCESS FORWARD
13	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, TCP, service others, DROP	172.19.60.1:64863	10.32.10.31:3306	ACCESS BLOCK
14	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:64869	23.53.1.80:443	ACCESS FORWARD
15	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52567	80.10.246.2:53	ACCESS FORWARD
16	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, TCP, service others, DROP [count=4]	172.19.60.1:64863	10.32.10.31:3306	ACCESS BLOCK
17	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:64859	23.220.72.165:443	ACCESS FORWARD
18	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64817	80.10.246.2:53	ACCESS FORWARD
19	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, TCP, service G_INTERNET_SERVICES, ACC...	172.19.100.5:41400	185.125.190.100:80	ACCESS FORWARD
20	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.5:33756	8.8.8.8:53	ACCESS FORWARD
21	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.5:51672	8.8.8.8:53	ACCESS FORWARD

Page 1 of 1 Show 200 items Displaying 1 - 21 of 21

Capture : log Zyxel : DROP du 3306 vers 10.32.10.31 par la règle par défaut (carte 19)

T9 – DMZ vers LAN (flux interdit)



Capture : DMZ vers LAN : srv-web vers 172.19.60.1:445, bloqué (carte 19)



Email Log Now | Refresh | Clear

#	Time	Priority	Category	Message	Source	Destination	Note
1	202...	notice	Security Policy Control	priority:14, from DMZ to LAN1, TCP, service others, DROP [count=3]	10.31.10.11:55636	172.19.60.1:445	ACCESS BLOCK

Page 1 of 1 Show 200 items Displaying 1 - 1 of 1

Capture : log Zyxel : DROP de DMZ vers LAN1 sur le port 445 (carte 19)

T10 – Flux sans règle

```
PS C:\Users\admin> Test-NetConnection 10.31.10.11 -Port 8080
AVERTISSEMENT : TCP connect to (10.31.10.11 : 8080) failed


ComputerName            : 10.31.10.11
RemoteAddress           : 10.31.10.11
RemotePort              : 8080
InterfaceAlias          : Ethernet 3
SourceAddress           : 172.19.60.1
PingSucceeded           : True
PingReplyDetails (RTT) : 2 ms
TcpTestSucceeded        : False
```

Capture : Test-NetConnection 10.31.10.11 -Port 8080 : False (carte 19)

Email Log Now | Refresh | Clear

#	Time	Priority	Category	Message	Source	Destination	Note
1	202...	notice	Security Policy Control	priority:8, from LAN1 to ZyWALL, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:56024	192.168.2.2:443	ACCESS FORWARD
2	202...	notice	Security Policy Control	priority:8, from LAN1 to ZyWALL, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:60771	192.168.2.2:443	ACCESS FORWARD
3	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:58713	52.105.168.39:443	ACCESS FORWARD
4	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:58711	13.107.136.10:443	ACCESS FORWARD
5	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:58701	13.107.139.11:443	ACCESS FORWARD
6	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52793	80.10.246.2:53	ACCESS FORWARD
7	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, TCP, service G_INTERNET_SERVICES, ACC...	172.19.100.5:49954	91.189.91.60:80	ACCESS FORWARD
8	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.5:37121	8.8.8.8:53	ACCESS FORWARD
9	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=2]	172.19.60.1:137	10.31.10.11:137	ACCESS BLOCK
10	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.5:55781	8.8.8.8:53	ACCESS FORWARD
11	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:64535	80.10.246.2:53	ACCESS FORWARD
12	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, UDP, service others, DROP [count=4]	172.19.60.1:137	10.31.10.11:137	ACCESS BLOCK
13	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:49385	80.10.246.2:53	ACCESS FORWARD
14	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, ICMP Type:8, service G_ADMIN_IT, ICMP Typ...	172.19.60.1	10.31.10.11	ACCESS FORWARD
15	202...	notice	Security Policy Control	priority:7, from LAN1 to ANY, TCP, service G_ADMIN_IT, ACCEPT	172.19.60.1:58693	150.171.22.17:443	ACCESS FORWARD
16	202...	notice	Security Policy Control	priority:12, from LAN1 to WAN, UDP, service G_INTERNET_SERVICES, ACC...	172.19.100.2:52095	80.10.246.2:53	ACCESS FORWARD
17	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, TCP, service others, DROP	172.19.60.1:57338	10.31.10.11:8080	ACCESS BLOCK
18	202...	notice	Security Policy Control	priority:5, from DMZ_INT to WAN, UDP, service G_INTERNET_SERVICES, A...	10.32.10.3:123	104.40.149.189:123	ACCESS FORWARD
19	202...	notice	Security Policy Control	priority:15, from LAN1 to ANY, TCP, service others, DROP [count=4]	172.19.60.1:57338	10.31.10.11:8080	ACCESS BLOCK

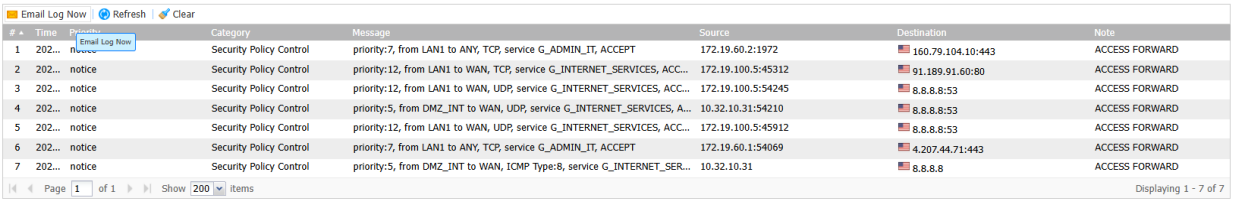
Page 1 of 1 | Show 200 items | Displaying 1 - 19 of 19

Capture : log Zyxel : DROP du 8080 par la règle par défaut (carte 19)

T11 – Sortie Internet DMZ interne

```
groupe3@srv-bdd-3:~$ ping -c 3 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=1 ttl=112 time=7.02 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=6.66 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=5.74 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 5.744/6.474/7.022/0.537 ms
groupe3@srv-bdd-3:~$ nslookup deb.debian.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
deb.debian.org  canonical name = debian.map.fastlydns.net.
Name:   debian.map.fastlydns.net
Address: 151.101.66.132
Name:   debian.map.fastlydns.net
Address: 151.101.130.132
Name:   debian.map.fastlydns.net
Address: 151.101.2.132
Name:   debian.map.fastlydns.net
Address: 151.101.194.132
Name:   debian.map.fastlydns.net
Address: 2a04:4e42::644
Name:   debian.map.fastlydns.net
Address: 2a04:4e42:600::644
Name:   debian.map.fastlydns.net
Address: 2a04:4e42:200::644
Name:   debian.map.fastlydns.net
Address: 2a04:4e42:400::644

groupe3@srv-bdd-3:~$
```

Capture : srv-bdd-3 : ping 8.8.8.8 et nslookup deb.debian.org (carte 19)

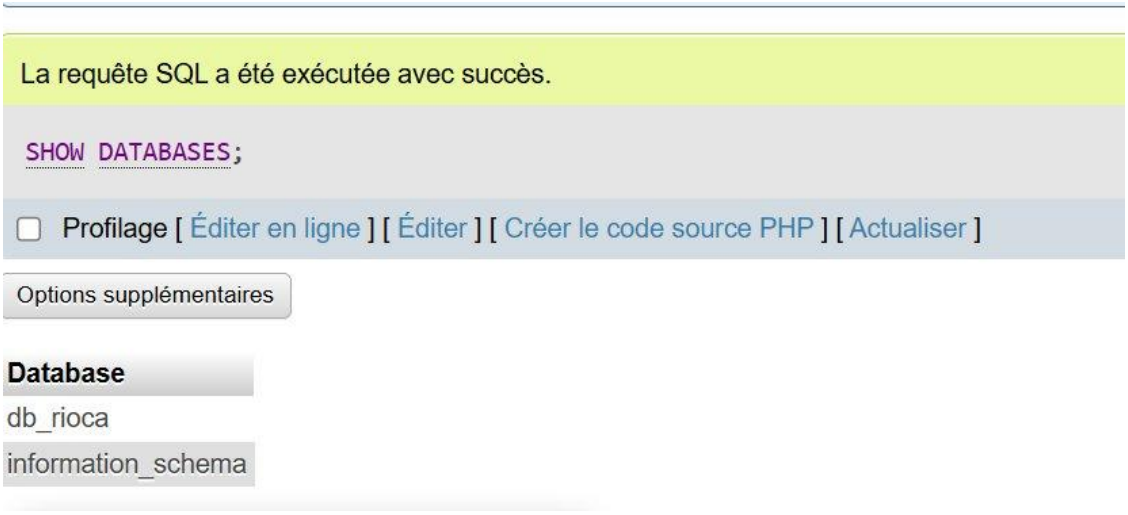


Capture : log Zyxel : ACCEPT de DMZ_INT vers WAN pour 10.32.10.31, ICMP et DNS (carte 19)

T12 – UFW sur la BDD

Preuve : capture de ufw status numbered en 7.4.

T13 – Compte RIOCAENLI

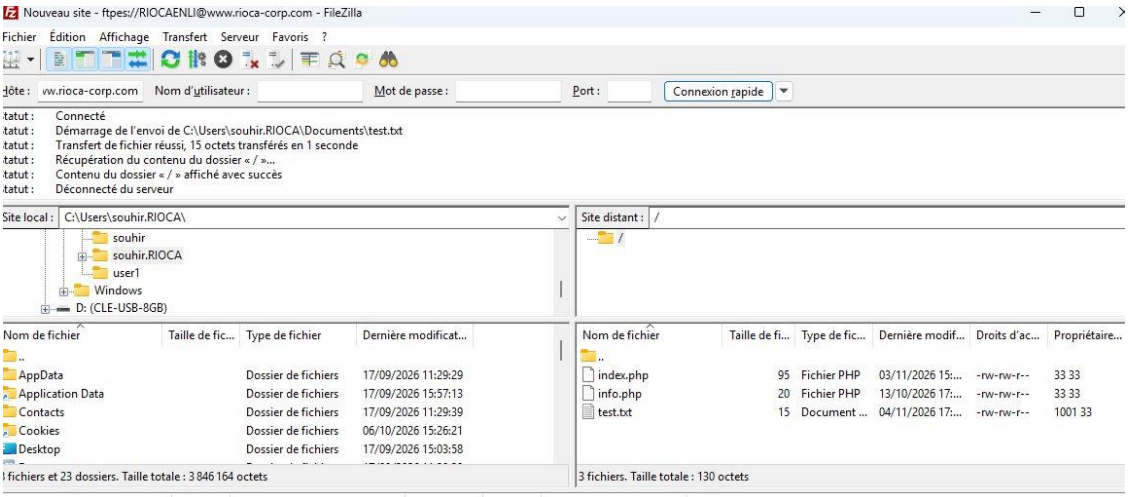


***Capture :** phpMyAdmin : SHOW DATABASES (carte 21)*

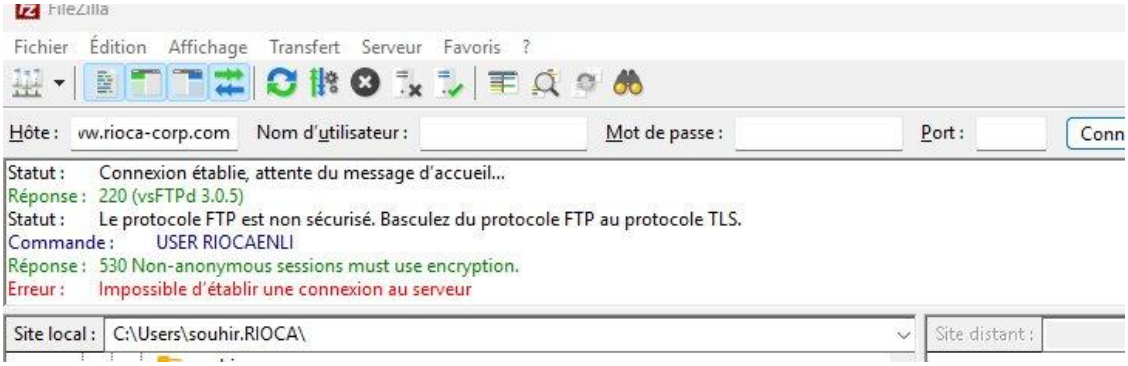
T14 – Droits du compte

Preuve : capture de SHOW GRANTS en 7.3.

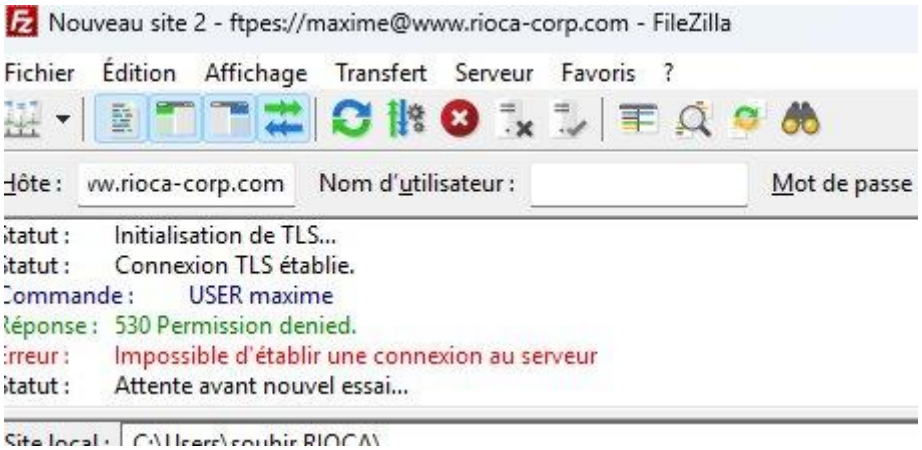
T15 – FTPS chiffré



Capture : *dépôt de test.txt avec FileZilla, chroot effectif (carte 15)*



Capture : *connexion non chiffrée refusée, erreur 530 (carte 15)*



Capture : *compte non autorisé refusé, erreur 530 (carte 15)*

T16 – TLS

```
root@srv-web:~# apache2ctl configtest && systemctl restart apache2
Syntax OK
root@srv-web:~# openssl s_client -connect 127.0.0.1:443 -tls1_1 -cipher 'DEFAULT@SECLE
VEL=0' </dev/null 2>&1 | grep -E "Protocol|alert|error"
openssl s_client -connect 127.0.0.1:443 -tls1_2 </dev/null 2>&1 | grep -E "Protocol|Ci
pher is"
openssl s_client -connect 127.0.0.1:443 -tls1_3 </dev/null 2>&1 | grep -E "Protocol|Ci
pher is"
40D7A84B997F0000:error:0A00042E:SSL routines:ssl3_read_bytes:tlsv1 alert protocol vers
ion:../ssl/record/rec_layer_s3.c:918:SSL alert number 70
Protocol: TLSv1.1
    Protocol  : TLSv1.1
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Protocol: TLSv1.2
    Protocol  : TLSv1.2
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Protocol: TLSv1.3
root@srv-web:~#
```

Activer Windows
Accédez aux paramètres pour activer Windows.

Capture : *TLS 1.0 et 1.1 refusés, 1.2 et 1.3 acceptés (cartes 12 et 13)*

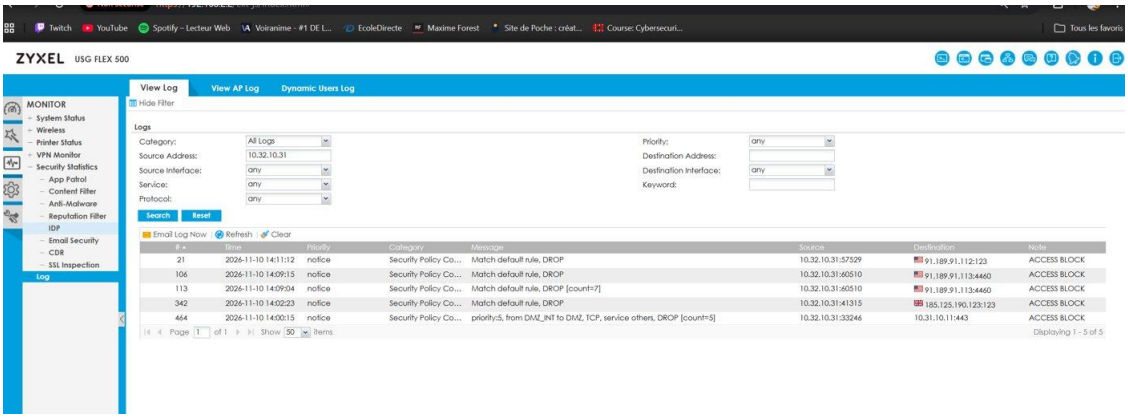
T17 – BIND9

Preuve : captures du fichier de zone (named-checkzone OK) et du dig en 9.3.

T18 – DMZ interne vers Web (flux interdit)

```
groupe3@srv-bdd-3:~$ curl -k -m 5 https://10.31.10.11
curl: (28) Connection timed out after 5002 milliseconds
groupe3@srv-bdd-3:~$
```

Capture : *flux interdit : curl de srv-bdd-3 vers SRV-WEB1 en timeout (carte 13)*



Capture : *log Zyxel : DROP de la DMZ interne vers le Web (carte 13)*

T19 – Wi-Fi vers site (développeurs)

Preuve : captures du site et de FileZilla depuis le Wi-Fi en partie 11.

T20 – Site relié à la base

Preuve : capture de la connexion d'un utilisateur sur le site SLAM en 5.1.

13. Difficultés rencontrées et solutions

Problème	Cause	Solution
Flux retour perdu depuis le campus	RNET2 en Standby HSRP	Route statique 172.18.0.0/16 vers 192.168.3.250 sur le Zyxel

Problème	Cause	Solution
Site inaccessible depuis le WAN (environ 4 h perdues)	IP de NAT utilisée différente de celle du site	NAT de 172.18.53.1 corrigé vers 10.31.10.11
Base exposée au campus par erreur	Besoin mal compris, règle Zyxel et NAT 3306 créés	Règle Campus_vers_MariaDB désactivée et NAT 3306 supprimé sur RNET2 après vérification
FTPS injoignable	Objet Zyxel en TCP 990 alors que vsftpd écoute sur 21	Objet corrigé en TCP 21, plage passive ajoutée à FTPS_GRP
Mises à jour refusées, certificat jugé invalide	Horloge de SRV-WEB1 et de l'hyperviseur décalée, NTP bloqué depuis la DMZ	Heure corrigée, règle NTP ajoutée pour la DMZ interne
Certificat racine non reconnu	Import dans le magasin « intermédiaires »	Import refait dans « racines de confiance », puis GPO
DNS de la VM écrasé	Le DHCP remplaçait le DNS	Configuration IP fixe corrigée
curl bloque sur Windows	Pas de CRL publiée par la CA interne	Test avec `--ssl-no-revoke`
Objet pare-feu sur l'ancienne IP	Passage à la DMZ intermédiaire	Objet LAN_to_WebServ mis à jour

14. Limites et améliorations possibles

- Services mutualisés sur SRV-WEB1 (Web, FTPS, DNS, CA) : pour réduire le risque, séparer sur des VM distinctes.
- Un seul pare-feu Zyxel et pas de reverse proxy : ajouter un second niveau de filtrage et un reverse proxy pour la DMZ.
- Compte de base de données partagé entre développeurs (RIOCAENLI, imposé) : prévoir un compte par développeur.
- Pas de CRL publiée par la CA interne : publier une CRL ou un service OCSP.
- Le site répond encore en HTTP (port 80) pour l'accès depuis le Wi-Fi : remettre la redirection 301 vers HTTPS dès que tous les postes passent en HTTPS.
- Clé de la CA stockée sur SRV-WEB1, serveur exposé : la déplacer sur une machine hors DMZ.
- L'enregistrement DNS www existe à deux endroits (AD et BIND9) et doit être maintenu des deux côtés : un redirecteur conditionnel de l'AD vers 10.31.10.11 supprimerait ce doublon.

15. Livrables et annexes

Livrable	Où le trouver
Diagramme de Gantt	GANT_Archisite_MAXIME_SOUHIR.xlsm (carte 1), capture en annexe A
Étude ANSSI et schéma réseau modifié	Etude_ANSSI_ArchiSite.docx (carte 3)
Choix du service Web (Apache ou Nginx)	Choix_service_web_ArchiSite.docx (carte 5)
Fiche de configuration (paramétrages, adressage, comptes)	Fiche_configuration_ArchiSite.docx (carte 22)
Fichiers de configuration épurés et commentés	50-server.cnf, vsftpd.conf, named.conf.options, zone rioca-corp.com, fichiers Apache (cartes 22 et 23)
Rapport de tests	Partie 12 de ce document

Livrable	Où le trouver
Présentation DSI sur les certificats HTTPS (interne ou externalisé)	Diaporama de présentation (carte 14)
Document de communication pour l'équipe SLAM	Document_de_communication_equipe_developpeurs_RIOCA.docx : site, FTPS, BDD, identifiants transmis à part

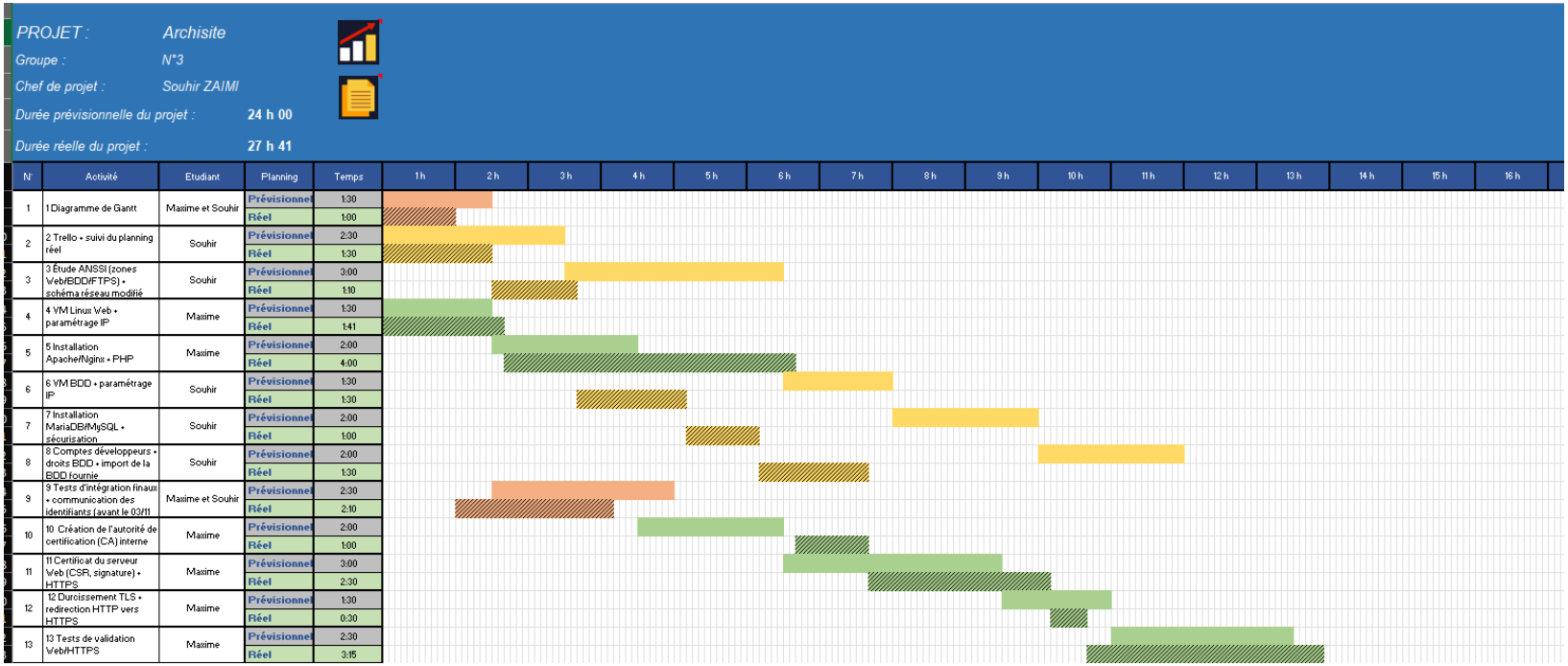
Temps passé sur quelques tâches

Tâche	Prévu	Réel
Étude ANSSI + schéma	3h00	1h10
Apache + PHP	2h00	4h00
MariaDB + sécurisation	2h00	1h00
Certificat Web + HTTPS	3h00	2h30
DNS BIND9 + zone	2h30	5h30
Tests de validation BDD/FTPS/DNS	2h00	4h35
Rapport de tests	4h30	3h00

Annexe A. Diagramme de Gantt

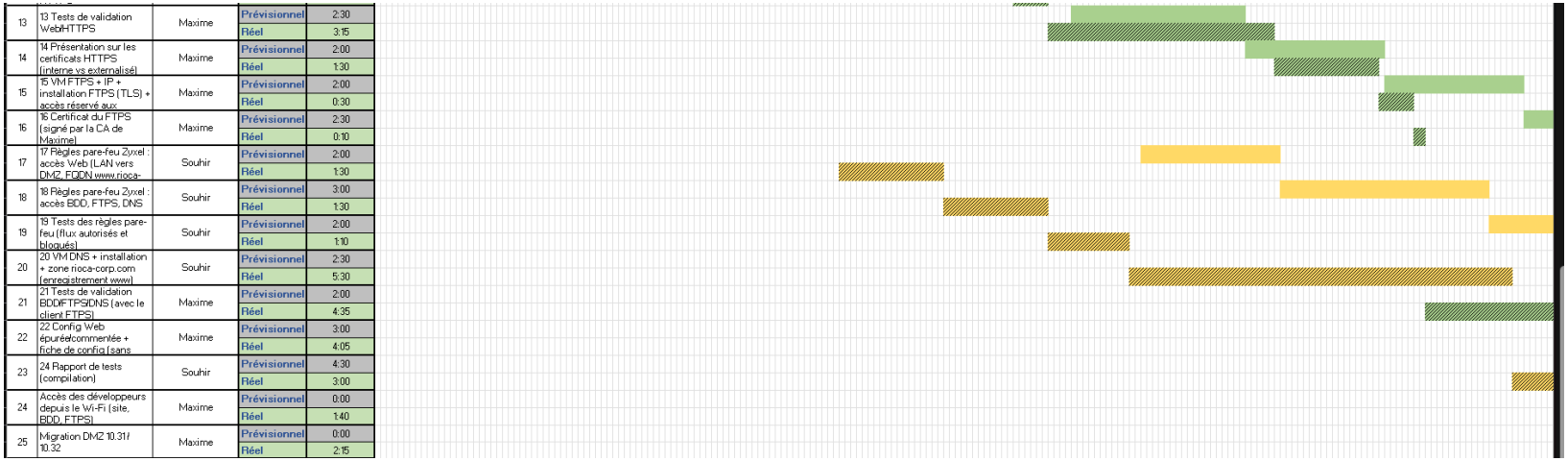
PROJET : Archisite
Groupe : N°3
Chef de projet : Souhir ZAIMI
Durée prévisionnelle du projet : 24 h 00
Durée réelle du projet : 27 h 41

N°	Activité	Etudiant	Planning	Temps
1	1 Diagramme de Gantt	Maxime et Souhir	Prévisionnel	1:30
			Réel	1:00
2	2 Trello + suivi du planning réel	Souhir	Prévisionnel	2:30
			Réel	1:30
3	3 Étude ANSSI (zones Web/BDD/FTPS) + schéma réseau modifié	Souhir	Prévisionnel	3:00
			Réel	1:10
4	4 VM Linux Web + paramétrage IP	Maxime	Prévisionnel	1:30
			Réel	1:41
5	5 Installation Apache/Nginx + PHP	Maxime	Prévisionnel	2:00
			Réel	4:00
6	6 VM BDD + paramétrage IP	Souhir	Prévisionnel	1:30
			Réel	1:30
7	7 Installation MariaDB/MySQL + sécurisation	Souhir	Prévisionnel	2:00
			Réel	1:00
8	8 Comptes développeurs + droits BDD + import de la BDD fournie	Souhir	Prévisionnel	2:00
			Réel	1:30
9	9 Tests d'intégration finaux + communication des identifiants (avant le 03/11	Maxime et Souhir	Prévisionnel	2:30
			Réel	2:10
10	10 Création de l'autorité de certification (CA) interne	Maxime	Prévisionnel	2:00
			Réel	1:00
11	11 Certificat du serveur Web (CSR, signature) + HTTPS	Maxime	Prévisionnel	3:00
			Réel	2:30
12	12 Durcissement TLS + redirection HTTP vers HTTPS	Maxime	Prévisionnel	1:30
			Réel	0:30
13	13 Tests de validation Web/HTTPS	Maxime	Prévisionnel	2:30
			Réel	3:15



Capture : diagramme de Gantt, tâches 1 à 13 (carte 1, fichier GANT_Archisite_MAXIME_SOUHIR)

13	13 Tests de validation Web/HTTPS	Maxime	Prévisionnel	2:30
			Réel	3:15
14	14 Présentation sur les certificats HTTPS (interne vs externalisé)	Maxime	Prévisionnel	2:00
			Réel	1:30
15	15 VM FTPS + IP + installation FTPS (TLS) + accès réservé aux	Maxime	Prévisionnel	2:00
			Réel	0:30
16	16 Certificat du FTPS (signé par la CA de Maxime)	Maxime	Prévisionnel	2:30
			Réel	0:10
17	17 Règles pare-feu Zyxel : accès Web (LAN vers DMZ, FQDN www.rioca-	Souhir	Prévisionnel	2:00
			Réel	1:30
18	18 Règles pare-feu Zyxel : accès BDD, FTPS, DNS	Souhir	Prévisionnel	3:00
			Réel	1:30
19	19 Tests des règles pare-feu (flux autorisés et bloqués)	Souhir	Prévisionnel	2:00
			Réel	1:10
20	20 VM DNS + installation + zone rioca-corp.com (enregistrement www)	Souhir	Prévisionnel	2:30
			Réel	5:30
21	21 Tests de validation BDD/FTPS/DNS (avec le client FTPS)	Maxime	Prévisionnel	2:00
			Réel	4:35
22	22 Config Web épurée/commentée + fiche de config (sans	Maxime	Prévisionnel	3:00
			Réel	4:05
23	24 Rapport de tests (compilation)	Souhir	Prévisionnel	4:30
			Réel	3:00
24	Accès des développeurs depuis le Wi-Fi (site, BDD, FTPS)	Maxime	Prévisionnel	0:00
			Réel	1:40
25	Migration DMZ 10.31/10.32	Maxime	Prévisionnel	0:00
			Réel	2:15



Capture : diagramme de Gantt, tâches 13 à 25 (carte 1)

Récapitulatif temps prévu et passé par étudiant		
Etudiant	Temps prévu	Temps réel
Maxime et Souhir	4h00	3h10
Souhir	24h00	19h20
Maxime	24h00	27h41

Capture : récapitulatif du temps prévu et passé par étudiant (carte 1)