Rapport de Tests de Configuration

AP-3 ARCHISITE

Projet :	ArchiSite – SAVEOL
Période :	07/10 – 14/11/2025
Groupe :	Groupe 1
Étudiants :	Caron Cyprien / Naimi Abdelaadim
Formation :	BTS SIO 2ème année
Lycée :	Saint Adjutor

Synthèse des Tests

N°	Test	Responsable	Résultat
1	Serveur Web – Apache HTTPS (local)	Cyprien	✓ Réussi
2	Serveur Web – Accès depuis navigateur Edge (local)	Cyprien	✓ Réussi
3	Serveur Web – Accès depuis navigateur Firefox (poste client)	Cyprien	✓ Réussi
4	Certificat SSL – Vérification GPO	Cyprien	✓ Réussi
5	DNS – Résolution locale (serveur)	Abdelaadim	✓ Réussi
6	DNS – Résolution depuis contrôleur de domaine (AD)	Abdelaadim	✓ Réussi
7	DNS – Résolution depuis poste client (Compta1)	Abdelaadim	✓ Réussi
8	DNS – Accès web via nom de domaine (AD)	Abdelaadim	✓ Réussi
9	DNS – Accès web via nom de domaine (client)	Abdelaadim	✓ Réussi
10	FTPS – Service vsftpd actif	Abdelaadim	✓ Réussi
11	FTPS – Connexion FileZilla (compte dev)	Abdelaadim	✓ Réussi
12	NAT Statique – Serveur Web (172.18.51.250)	Cyprien	✓ Réussi
13	NAT Statique – Serveur BDD (172.18.51.251)	Cyprien	✓ Réussi

14	Switch DMZ – SSH administration distante	Cyprien	✓ Réussi
15	ACL – Règles d'accès ZYXEL / RNET1 / RNET2	Cyprien	✓ Réussi

1. Tests – Serveur Web Apache & HTTPS

1.1 Vérification du service Apache2

Objectif :

Vérifier que le service Apache2 est bien démarré et actif sur le serveur web Ubuntu (10.11.10.11).

Résultat attendu :

Le service Apache2 doit être en état "active (running)".

Procédure / Commandes :

```
root@srvweb:/# systemctl restart apache2
root@srvweb:/# systemctl status apache2
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
Active: active (running) since Tue 2025-10-14 09:59:00 UTC; 6s ago
Main PID: 71438 (apache2)
Tasks: 55 (limit: 4612) Memory: 6.3M
```

Résultat obtenu :

✓ **Test réussi – Le service Apache2 est actif et en cours d'exécution.**

1.2 Accès HTTPS depuis navigateur (Edge – poste local)

Objectif :

Vérifier l'accessibilité du site en HTTPS via le navigateur Microsoft Edge depuis le poste client Windows.

Résultat attendu :

Le site https://www.saveol.coop doit être accessible et la connexion doit être sécurisée.

Constat : Navigation vers https://www.saveol.coop → cadenas vert visible. La pop-up Edge indique "La connexion est sécurisée" et le certificat SAVEOL_CERTS est reconnu.

Résultat obtenu :

✓ **Test réussi – Le cadenas HTTPS est présent ; "La connexion est sécurisée" affiché dans Edge.**

1.3 Accès HTTPS depuis navigateur (Firefox – poste client)

Objectif :

Vérifier l'accessibilité du site en HTTPS via Firefox depuis le poste client Windows (Compta1).

Résultat attendu :

Le site doit répondre en HTTPS sur le port 443. Firefox peut afficher un avertissement si le certificat interne n'est pas encore importé dans son magasin.

Note : Firefox signale "Connexion vérifiée par un émetteur de certificat non reconnu par Mozilla" car le certificat est auto-signé (CA interne). L'option "Passer automatiquement ce site vers une connexion sécurisée" est activée.

Résultat obtenu :

✓ **Test réussi – Firefox accède au site saveol.coop ; connexion surclassée en HTTPS (port 443).**

1.4 Vérification du certificat SSL via GPO

Objectif :

Vérifier que le certificat myCA.pem est bien déployé via GPO dans le magasin "Autorités de certification racines de confiance" des postes du domaine.

Résultat attendu :

L'importation doit réussir et la stratégie de groupe se mettre à jour sans erreur.

Procédure / Commandes :

```
C:\Users\Cyprien> gpupdate /force
Mise à jour de la stratégie...
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

Résultat obtenu :

✓ **Test réussi – Certificat SAVEOL_CERTS importé avec succès ; GPO appliquée sans erreur.**

---

2. Tests – Serveur DNS (BIND9)

2.1 Test local – Résolution de noms sur le serveur DNS

Objectif :

Vérifier la résolution de noms en local directement sur le serveur DNS (10.11.10.11).

Résultat attendu :

La résolution de nom doit s'effectuer correctement pour saveol.coop et www.saveol.coop.

Procédure / Commandes :

```
root@srvweb:/# dig @localhost saveol.coop
;; ANSWER SECTION:
saveol.coop. 604800 IN A 10.11.10.11
;; Query time: 0 msec SERVER: 127.0.0.1#53(localhost) (UDP)

root@srvweb:/# dig @localhost www.saveol.coop
;; ANSWER SECTION:
www.saveol.coop. 604800 IN A 10.11.10.11
```

Résultat obtenu :

✓ **Test réussi – La résolution de nom fonctionne correctement sur le serveur.**

2.2 Test depuis le Contrôleur de Domaine (AD)

Objectif :

Vérifier la résolution du nom de domaine "saveol.coop" depuis le contrôleur de domaine (srv-dc-grp1).

Résultat attendu :

La résolution du nom de domaine "saveol.coop" doit aboutir.

Procédure / Commandes :

```
C:\Windows\System32> ipconfig /flushdns
Cache de résolution DNS vidé.

C:\Windows\System32> nslookup saveol.coop
Serveur : UnKnown
Address: ::1
Nom : saveol.coop
Address: 10.11.10.11

C:\Windows\System32> ping saveol.coop
Réponse de 10.11.10.11 : octets=32 temps=1ms TTL=62 [x4]
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%)
```

Résultat obtenu :

✓ **Test réussi – Le nom de domaine "saveol.coop" est correctement résolu depuis l'AD.**

2.3 Test d'accès web depuis le Contrôleur de Domaine

Objectif :

Vérifier l'accessibilité de la page web via le nom de domaine depuis le contrôleur de domaine.

Résultat attendu :

La page web doit être accessible via https://www.saveol.coop.

Constat : Le navigateur affiche "Index of /" servi par Apache/2.4.58 (Ubuntu) sur le port 443. L'URL saveol.coop est accessible.

Résultat obtenu :

✓ **Test réussi – L'accès à la page web via le nom de domaine fonctionne depuis le contrôleur de domaine.**

2.4 Test depuis un Poste Client Windows (Compta1)

Objectif :

Vérifier la résolution du nom de domaine "saveol.coop" depuis un poste client Windows (Compta1 – VLAN 10).

Résultat attendu :

La résolution du nom de domaine "saveol.coop" doit aboutir depuis le poste client.

Procédure / Commandes :

```
C:\Users\compta1> ipconfig /flushdns
Cache de résolution DNS vidé.

C:\Users\compta1> nslookup saveol.coop
Serveur : UnKnown
Address: 10.11.10.11
Nom : saveol.coop
Address: 10.11.10.11

C:\Users\compta1> ping saveol.coop
Réponse de 10.11.10.11 : octets=32 temps=2ms TTL=62 [x4]
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%)
```

Résultat obtenu :

✓ **Test réussi – Le nom de domaine "saveol.coop" est correctement résolu depuis le poste client.**

2.5 Test d'accès web depuis le poste client (Compta1)

Objectif :

Vérifier l'accessibilité de la page web via le nom de domaine depuis le poste client Windows.

Résultat attendu :

La page web doit être accessible via le nom de domaine.

Constat : Le navigateur affiche la page Index of / servie par Apache/2.4.58 (Ubuntu) sur le port 443 – saveol.coop.

Résultat obtenu :

✓ **Test réussi – L'accès à la page web via le nom de domaine fonctionne correctement depuis le poste client.**

3. Tests – Serveur FTPS (vsftpd)

3.1 Vérification du service vsftpd

Objectif :

Vérifier que le service vsftpd est démarré et actif sur le serveur web (10.11.10.11).

Résultat attendu :

Le service vsftpd doit être en état "active (running)".

Procédure / Commandes :

```
root@srvweb:/# systemctl restart vsftpd
root@srvweb:/# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
Active: active (running) since Thu 2025-10-09 11:45:34 UTC; 6s ago
Main PID: 18828 (vsftpd) Tasks: 1 (limit: 4612) Memory: 1.0M
```

Résultat obtenu :

✓ **Test réussi – Le service vsftpd est actif et fonctionne correctement.**

3.2 Connexion FTPS depuis FileZilla (compte dev)

Objectif :

Vérifier qu'un développeur peut se connecter au serveur FTPS via FileZilla avec le compte "dev" et déposer des fichiers dans le répertoire de l'application web.

Résultat attendu :

La connexion FTPS doit s'établir et le dépôt de fichiers doit réussir.

Procédure / Commandes :

```
# Paramètres FileZilla
Hôte : 10.11.10.11
Protocole : FTP – Protocole de transfert de fichiers
Chiffrement : Connexion FTP explicite sur TLS
Identifiant : dev
Mot de passe: dev
```

Note : L'utilisateur "dev" a les droits sur le répertoire /home/$USER/ftp (chroot activé). Il appartient au groupe www-data pour pouvoir accéder à l'emplacement de l'application web.

Résultat obtenu :

✓ **Test réussi – Connexion FTPS établie ; dépôt de fichiers dans le répertoire web confirmé.**

3.3 Vérification du chiffrement SSL sur FTPS

Objectif :

Vérifier que le service FTPS utilise bien le chiffrement SSL (ssl_enable=YES dans vsftpd.conf) et que le certificat vsftpd.cert.pem est correctement configuré.

Résultat attendu :

Le chiffrement SSL doit être activé ; le certificat doit pointer vers /certs/vsftpd.cert.pem.

Procédure / Commandes :

```
# Extrait de /etc/vsftpd.conf
ssl_enable=YES
rsa_cert_file=/certs/vsftpd.cert.pem
rsa_private_key_file=/certs/vsftpd.key.pem
```

```
connect_from_port_20=NO
listen=YES
listen_ipv6=NO
anonymous_enable=NO
local_enable=YES
chroot_local_user=YES
```

Résultat obtenu :

✓ **Test réussi – Le chiffrement SSL est activé et le certificat FTPS est correctement configuré.**

---

4. Tests – NAT Statique (RNET2)

4.1 NAT Statique – Serveur Web

Objectif :

Vérifier que le NAT statique sur RNET2 redirige correctement le trafic vers le serveur web interne (10.11.10.11) depuis l'adresse externe 172.18.51.250.

Résultat attendu :

L'adresse externe 172.18.51.250 doit être redirigée vers 10.11.10.11 (Serveur Web).

Procédure / Commandes :

```
RNET2(config)# ip nat inside source static 10.11.10.11 172.18.51.250
RNET2(config)# exit
RNET2#

# Vérification
RNET2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 172.18.51.250:443 10.11.10.11:443 --- ---
```

Résultat obtenu :

✓ **Test réussi – Le NAT statique vers le serveur Web (10.11.10.11 ↔ 172.18.51.250) est opérationnel.**

4.2 NAT Statique – Serveur BDD

Objectif :

Vérifier que le NAT statique sur RNET2 redirige correctement le trafic vers le serveur BDD interne (10.12.10.31) depuis l'adresse externe 172.18.51.251.

Résultat attendu :

L'adresse externe 172.18.51.251 doit être redirigée vers 10.12.10.31 (Serveur BDD).

Procédure / Commandes :

```
RNET2(config)# ip nat inside source static 10.12.10.31 172.18.51.251

# Vérification show running-config
ip nat inside source static 10.11.10.11 172.18.51.250
ip nat inside source static 10.12.10.31 172.18.51.251
```

Résultat obtenu :

✓ **Test réussi – Le NAT statique vers le serveur BDD (10.12.10.31 ↔ 172.18.51.251) est opérationnel.**

---

5. Tests – Administration à distance des Switch DMZ

5.1 SSH – Switch DMZ Intermédiaire (SwDmzIntermediaire)

Objectif :

Vérifier que l'accès SSH est opérationnel sur le switch de la DMZ Intermédiaire (IP : 10.11.10.253) depuis un poste administrateur.

Résultat attendu :

La connexion SSH doit s'établir correctement avec les identifiants admin/admin.

Procédure / Commandes :

```
# Configuration SSH sur SwDmzIntermediaire
SwDmzIntermediaire(config)# crypto key generate rsa general-keys modulus 2048
% Generating 2048 bit RSA keys... [OK]
SwDmzIntermediaire(config)# line vty 0 4
SwDmzIntermediaire(config-line)# transport input ssh
SwDmzIntermediaire(config-line)# login local

# Test de connexion SSH
ssh admin@10.11.10.253
# → Connexion réussie
```

Résultat obtenu :

✓ **Test réussi – Connexion SSH au SwDmzIntermediaire (10.11.10.253) établie avec succès.**

5.2 SSH – Switch DMZ Interne (SwDmzInterne)

Objectif :

Vérifier que l'accès SSH est opérationnel sur le switch de la DMZ Interne (IP : 10.12.10.253) depuis un poste administrateur.

Résultat attendu :

La connexion SSH doit s'établir correctement avec les identifiants admin/admin.

Procédure / Commandes :

```
# Configuration SSH sur SwDmzInterne
SwDmzInterne(config)# crypto key generate rsa general-keys modulus 2048
% Generating 2048 bit RSA keys... [OK]
SwDmzInterne(config)# line vty 0 4
SwDmzInterne(config-line)# transport input ssh
SwDmzInterne(config-line)# login local

# Test de connexion SSH
ssh admin@10.12.10.253
# → Connexion réussie
```

Résultat obtenu :

✓ **Test réussi – Connexion SSH au SwDmzInterne (10.12.10.253) établie avec succès.**

---

6. Tests – ACL et Règles d'accès (ZYXEL / RNET1 / RNET2)

6.1 ACL RNET1 – Liste d'accès NET_LAN

Objectif :

Vérifier que la liste d'accès standard NET_LAN est correctement configurée sur RNET1 pour autoriser les réseaux 172.16.0.0/16, 10.11.0.0/16 et 10.12.0.0/16.

Résultat attendu :

Les trois réseaux doivent apparaître dans la liste d'accès NET_LAN.

Procédure / Commandes :

```
RNET1# show access-lists
Standard IP access list NET_LAN
10 permit 172.16.0.0, wildcard bits 0.0.255.255 (672 matches)
20 permit 10.11.0.0, wildcard bits 0.0.255.255
30 permit 10.12.0.0, wildcard bits 0.0.255.255
```

Résultat obtenu :

✓ **Test réussi – La liste d'accès NET_LAN sur RNET1 est correctement configurée.**

6.2 ACL RNET2 – Liste d'accès NET_LAN

Objectif :

Vérifier que la liste d'accès standard NET_LAN est correctement configurée sur RNET2 pour autoriser les réseaux 172.16.0.0/16, 10.11.0.0/16 et 10.12.0.0/16.

Résultat attendu :

Les trois réseaux doivent apparaître dans la liste d'accès NET_LAN.

Procédure / Commandes :

```
RNET2# show access-lists
Standard IP access list NET_LAN
10 permit 172.16.0.0, wildcard bits 0.0.255.255 (672 matches)
20 permit 10.11.0.0, wildcard bits 0.0.255.255
30 permit 10.12.0.0, wildcard bits 0.0.255.255
```

Résultat obtenu :

✓ **Test réussi – La liste d'accès NET_LAN sur RNET2 est correctement configurée.**

6.3 ZYXEL – Configuration des interfaces DMZ

Objectif :

Vérifier que les interfaces DMZ_INTERNE (10.12.10.254) et DMZ_MEDIAIR (10.11.10.254) sont correctement configurées sur le pare-feu ZYXEL.

Résultat attendu :

Les deux interfaces DMZ doivent être actives avec les bonnes adresses IP.

Procédure / Commandes :

```
# Interface DMZ Intermédiaire
Interface Name : DMZ_MEDIAIR | Zone : OPT
IP Address : 10.11.10.254 | Subnet : 255.255.0.0

# Interface DMZ Interne
Interface Name : DMZ_INTERNE | Zone : DMZ
IP Address : 10.12.10.254 | Subnet : 255.255.0.0
```

Résultat obtenu :

✓ **Test réussi – Les interfaces DMZ du ZYXEL sont correctement configurées.**

6.4 ZYXEL – RIP v2 et tables de routage

Objectif :

Vérifier que le protocole RIP v2 est configuré sur le ZYXEL et que les routes sont bien présentes sur RNET1 et RNET2.

Résultat attendu :

Les routes vers les réseaux 10.11.0.0 et 10.12.0.0 doivent apparaître via RIP.

Procédure / Commandes :

```
# Config RIP ZYXEL
router rip
version 2
network wan1
network lan1
network DMZ_INTERNE
network DMZ_MEDIAIR

# Routes RIP sur RNET1 (show ip route)
R 10.11.0.0 [120/1] via 192.168.3.253, GigabitEthernet0/1
R 10.12.0.0 [120/1] via 192.168.3.253, GigabitEthernet0/1
```

Résultat obtenu :

✓ **Test réussi – RIP v2 opérationnel ; routes DMZ présentes sur RNET1 et RNET2.**