



**TITRE :** Procédure de déploiement des nouvelles technologies de sécurité

**PROJET :** Architecture Réseau OpenBank - Interconnexion et Télétravail

**AUTEUR :** Hoëllard Calix

**DATE :** 29/01/2026

**VERSION :** 1.0

---

## Tableau de Versionning (Traçabilité)

Version	Date	Auteur	Description des modifications	Validé par
0.1	28/01/2026	Calix Hoëllard	Création du document (Draft - Maquette)	-
1.0	29/01/2026	Calix Hoëllard	Validation des tests VPN, Proxy & ZTNA	Samir Assaf (DSI)

---

# Sommaire

<b>Tableau de Versionning (Traçabilité)</b>	<b>1</b>
<b>Sommaire</b>	<b>2</b>
<b>I. Introduction et Contexte</b>	<b>3</b>
A. Objectif	3
B. Périmètre technique	3
C. Contraintes et Accessibilité	3
<b>II. Gestion des Certificats (PKI)</b>	<b>3</b>
A. Création de l'Autorité de Certification (CA)	3
B. Certificats Serveurs	4
<b>III. Interconnexion Site-à-Site (VPN IPsec)</b>	<b>5</b>
A. Topologie et Adressage	5
B. Configuration du Tunnel (Phase 1 & 2)	5
C. Sécurité Post-Quantique (Le point critique)	6
D. Validation et Traçabilité	6
<b>IV. Sécurisation de la Navigation (Proxy &amp; Filtrage)</b>	<b>7</b>
A. Configuration de l'authentification	7
B. Règles de Filtrage URL	7
C. Règle de Firewall (ACL) dédiée au Proxy	7
D. Critères d'acceptation (Tests)	8
<b>V. Accès Distant (VPN SSL &amp; ZTNA)</b>	<b>9</b>
A. Configuration ZTNA (Conformité)	9
B. Règle de Firewall (ACL) dédiée au VPN SSL	10
C. Validation (Critères d'acceptation)	11
<b>VI. Plan de Déploiement et Retour Arrière</b>	<b>12</b>
A. Phases de déploiement	12
B. Plan de Retour Arrière (Rollback)	12

---

# I. Introduction et Contexte

## A. Objectif

Ce document détaille la procédure technique pour la sécurisation de l'infrastructure réseau d'OpenBank. Il décrit les étapes de mise en œuvre de l'interconnexion sécurisée entre le siège (Paris) et la nouvelle agence (Nantes), ainsi que le déploiement d'une solution de télétravail conforme aux normes de sécurité modernes.

## B. Périmètre technique

Le déploiement concerne les équipements suivants :

- **Sécurité Périmétrique** : Firewalls Stormshield Network Security (SNS) sur les deux sites.
- **Systèmes** : Serveurs Windows 2022 (ADDS, DNS, DFS) et Postes clients Windows 10/11.
- **Architecture** : Réseau hybride (LAN Paris, LAN Nantes, Zones VPN).

## C. Contraintes et Accessibilité

Cette procédure intègre les contraintes de production suivantes :

- **Continuité de service** : Les interruptions sont planifiées hors heures ouvrées.
- **Accessibilité** : L'environnement de travail a été adapté pour les collaborateurs en situation de handicap (Mise en place des outils d'ergonomie pour Ana Garcia via GPO). Ce document respecte également les normes d'accessibilité numérique (structure hiérarchique, textes alternatifs pour les images).

---

# II. Gestion des Certificats (PKI)

Afin de garantir une authentification forte des équipements et d'éviter les alertes de sécurité lors du déchiffrement SSL, une Infrastructure à Clés Publiques (PKI) interne a été déployée.

## A. Création de l'Autorité de Certification (CA)

**Explication technique :**

Nous avons choisi de créer une Autorité de Certification (CA) privée "OpenBank Root CA" directement sur le firewall principal. Cette approche permet de maîtriser la chaîne de confiance en interne. Tous les certificats émis par cette autorité seront automatiquement reconnus comme fiables par les machines du domaine (via GPO)

et par les boîtiers Stormshield, évitant ainsi l'achat coûteux de certificats publics pour des usages internes.

OBJETS / CERTIFICATS ET PKI

Entrer un filtre... Filtre : Tous

+ Ajouter Révoquer Actions Télécharger Vérifier l'utilisation

- sslvpn-full-default-authority
- CA\_OpenBank**
- SSL proxy default authority

DÉTAILS RÉVOCATION (CRL) PROFILS DE CERTIFICATS

Émis pour

Sujet	C=FR,ST=Ile de France,L=Paris,O=OpenBank,OU=Banque,CN=OpenBank Root CA
Nom (CN)	OpenBank Root CA
Nom de l'organisation (O)	OpenBank
Nom de l'unité (OU)	Banque
Nom du lieu (L)	Paris
Nom de l'état ou de la province (ST)	Ile de France
Pays (C)	FR
E-mail	
Somme de contrôle	af6dfa0e

## B. Certificats Serveurs

Chaque pare-feu dispose de son propre certificat d'identité (Server Certificate) signé par la CA racine. Cela permet d'identifier formellement chaque extrémité des tunnels VPN.

OBJETS / CERTIFICATS ET PKI

Entrer un filtre... Filtre : Tous

+ Ajouter Révoquer Actions Télécharger Vérifier l'utilisation

- sslvpn-full-default-authority
- CA\_OpenBank
- Certif\_Paris**
- Certif\_Nantes
- SSL proxy default authority

DÉTAILS RÉVOCATION (CRL) PROFILS DE CERTIFICATS

Émis pour

Sujet	C=FR,ST=Ile de France,L=Paris,O=OpenBank,OU=Banque,CN=firewall-paris
Nom (CN)	firewall-paris
Nom de l'organisation (O)	OpenBank
Nom de l'unité (OU)	Banque
Nom du lieu (L)	Paris
Nom de l'état ou de la province (ST)	Ile de France
Pays (C)	FR
E-mail	
Somme de contrôle	e71af210

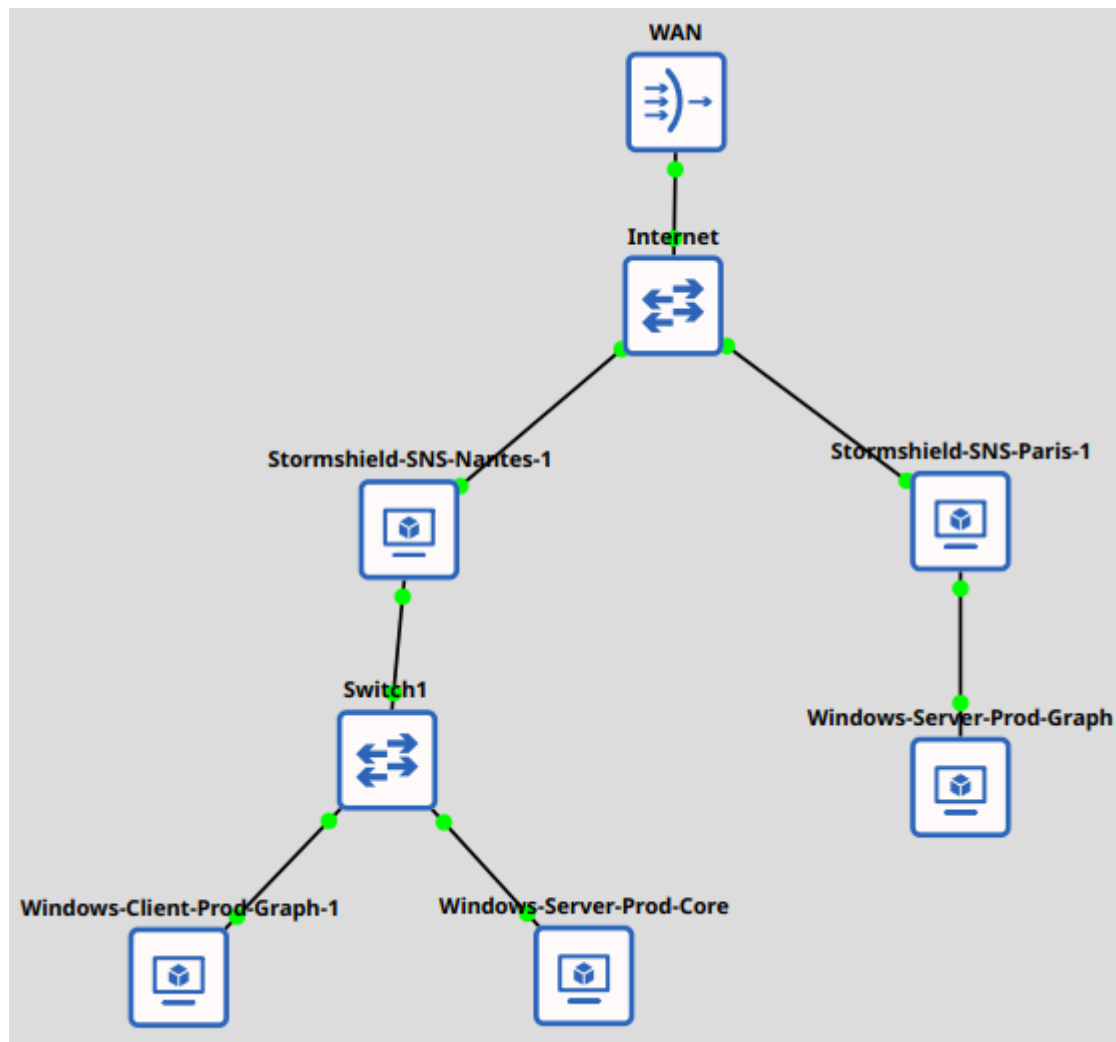
▼ Émetteur

### III. Interconnexion Site-à-Site (VPN IPsec)

L'interconnexion permanente entre Paris et Nantes est assurée par un tunnel VPN IPsec.

#### A. Topologie et Adressage

Le schéma ci-dessous présente l'architecture validée en pré-production (GNS3), détaillant les plans d'adressage IP des interfaces WAN et LAN.



#### B. Configuration du Tunnel (Phase 1 & 2)

Explication du choix d'authentification :

L'authentification par **Certificats X.509** a été privilégiée par rapport aux clés pré-partagées (PSK).

- **Sécurité** : Contrairement à un mot de passe (PSK) qui peut être volé ou bruteforcer, le certificat lie cryptographiquement l'identité à la machine.

- **Gestion** : La révocation d'un certificat compromis est plus simple que le changement d'un mot de passe sur tous les équipements.

## C. Sécurité Post-Quantique (Le point critique)

Conformément aux directives de l'ANSSI pour anticiper les futures menaces de déchiffrement, nous avons activé la protection Post-Quantique.

**Configuration du correspondant IKEv2 en mode Hybride : Authentification forte par Certificat X.509 associée à une Clé Pré-Partagée Post-Quantique (PPK - RFC 8784) pour garantir la résistance des échanges face aux futures attaques quantiques.**

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS    **CORRESPONDANTS**    IDENTIFICATION    PROFILS DE CHIFFREMENT

🔍 Entrer un filtre... ☰

☑ Passerelles distantes (1)

**Site\_SNS-NANTES**

Méthode d'authentification: Certificat

Certificat: CA\_OpenBank:Certif\_Paris

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: Saisir un identifiant (optionnel)

▲ Clé pré-partagée post-quantique (PPK)

Identifiant de PPK: key\_id

Mot de passe de la PPK: ..... x 👁 Éditer

☒ PPK requise

## D. Validation et Traçabilité

L'analyse réseau confirme que le trafic inter-sites est encapsulé et illisible depuis Internet.

107	48.216032	192.168.122.20	192.168.122.10	ESP	138	ESP (SPI=0xc9edc010)
111	40.226622	192.168.122.20	192.168.122.10	ESP	138	ESP (SPI=0xc9edc010)
>	Frame 107: Packet, 138 bytes on wire (1104 bits), 138 bytes			0000	0c 8f 7e 53 00 00 0c 65	66 57 00 00 08 00 45 00
>	Ethernet II, Src: 0c:65:66:57:00:00 (0c:65:66:57:00:00), Dst: 02:00:00:00:00:00			0010	00 7c f3 65 00 00 40 32	11 7b c0 a8 7a 14 c0 a8
>	Internet Protocol Version 4, Src: 192.168.122.20, Dst: 192.168.122.10			0020	7a 0a c9 ed c0 10 00 00	00 de 12 ad 1e 39 96 49
>	Encapsulating Security Payload			0030	1b e1 0e ec db cf 69 e8	7e ca ca 1d 62 ed d9 bb
	ESP SPI: 0xc9edc010 (3387801616)			0040	4e c1 d8 e2 f2 ed 67 a2	3c 47 60 4f ce 21 04 7b
	ESP Sequence: 222			0050	27 73 d1 ab ac d8 32 95	72 ab 66 a4 95 1f ab 0c
				0060	40 ba f3 47 69 7d c6 8f	df 80 e0 40 21 a9 75 7f
				0070	1f 11 e0 e8 43 9e 2c 8e	0c d6 51 c0 1c de eb 30
				0080	e3 07 14 a5 32 4e 04 25	b8 7d

## IV. Sécurisation de la Navigation (Proxy & Filtrage)

Pour protéger le réseau interne des menaces web et contrôler les usages, un proxy HTTP/HTTPS avec authentification transparente a été mis en place.

### A. Configuration de l'authentification

Le proxy est couplé à l'annuaire Active Directory. Cela permet d'appliquer des politiques de filtrage basées sur l'identité de l'utilisateur (Groupe "Employés" vs "Direction") et d'assurer une traçabilité nominative dans les journaux (logs), plutôt que par simple adresse IP.

### B. Règles de Filtrage URL

La politique de filtrage interdit strictement les catégories suivantes :

- Jeux d'argent et Gaming.
- Sites malveillants (Phishing, Malware).

### C. Règle de Firewall (ACL) dédiée au Proxy

Pour être effective, une règle de filtrage doit intercepter le trafic Web.

SECURITY POLICY / FILTER - NAT

(5) OpenBank-Nantes

Edit

Export

FILTERING

NAT

Searching...

+ New rule

X Delete

↑

↓

↕

↗

↖

Cut

Copy

Paste

Search in logs

Search in monitoring

		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1			pass	Network_in	Internet	dns		IPS
2			Authentication Except: authentica	unknown @  Network_in	Internet	http		IPS
3			pass	Users @  Network_in	Internet	http		IPS (IPS_00) URL filter: URLFilter_00
4			decrypt	Users @  Network_in	Internet	https		IPS (IPS_00) SSL filter: SSLFilter_00
5			pass	Network_in	LAN-PARIS	Any		FW
6			pass	LAN-PARIS via IPsec VPN tunnel	Network_in	Any		FW

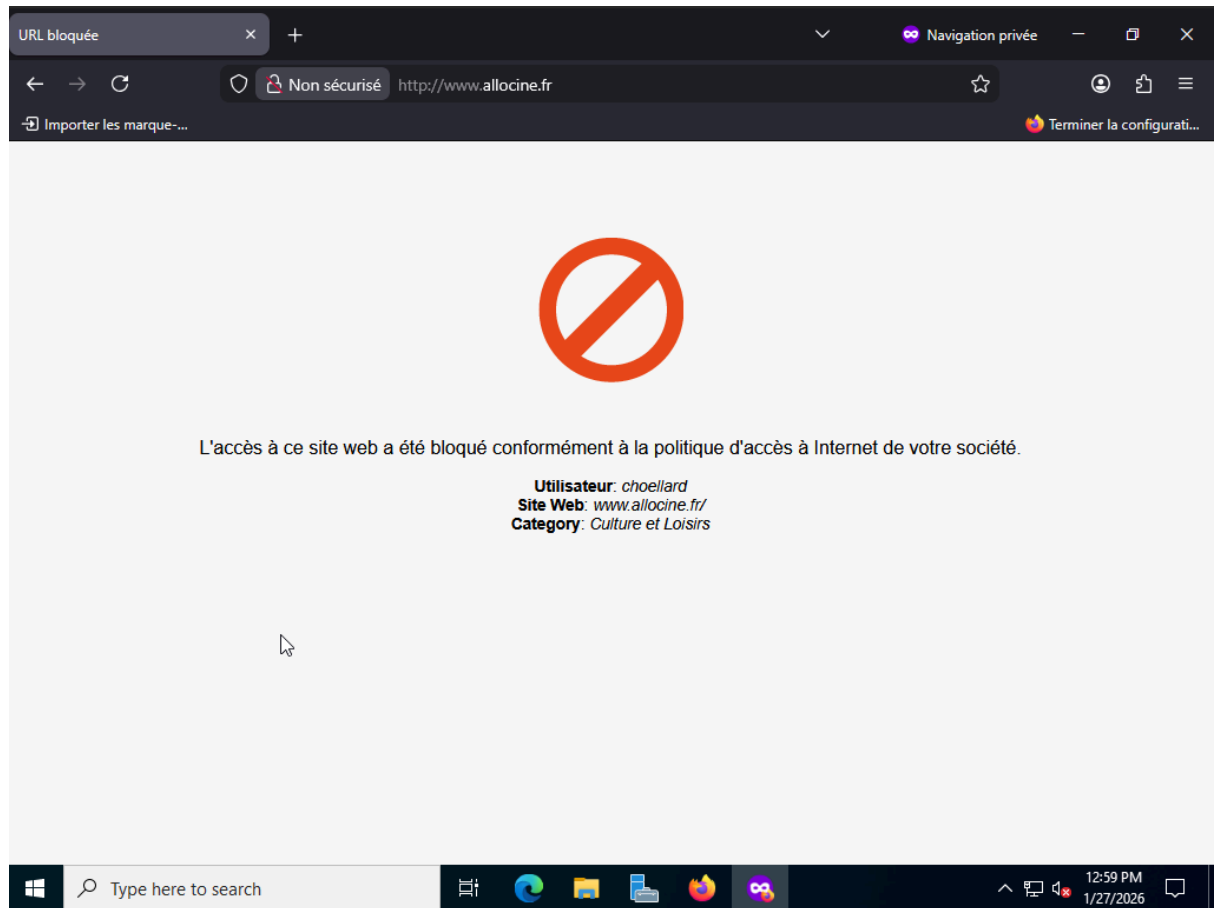
#### Explication de la règle :

Cette règle stipule que tout trafic venant du réseau interne (**Source : Any + User : Authenticated**) à destination d'Internet (**Dest : Internet**) sur les ports Web (**Port : HTTP/HTTPS**) doit être analysé par le module Proxy URL avant d'être autorisé.

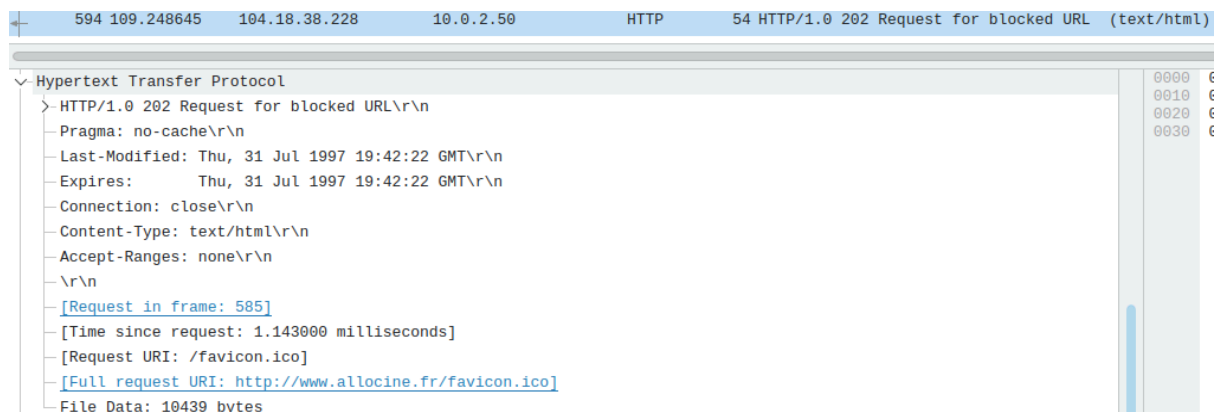


## D. Critères d'acceptation (Tests)

Le bon fonctionnement est validé par l'apparition de la page de blocage lors d'une tentative d'accès non autorisé.



*Texte Alternatif : Capture d'un navigateur web affichant le message "Accès Interdit" du firewall Stormshield.*



## V. Accès Distant (VPN SSL & ZTNA)

Le télétravail est sécurisé par un tunnel VPN SSL associé à une politique "Zero Trust" (ZTNA).

### A. Configuration ZTNA (Conformité)

Le principe du ZTNA (Zero Trust Network Access) est de ne jamais faire confiance par défaut. Avant d'établir le tunnel, le firewall audite le poste client.

 VPN / VPN SSL

**ON** ☐ Activer le VPN SSL

PARAMÈTRES GÉNÉRAUX

VÉRIFICATION DES POSTES CLIENTS (ZTNA)


**Veillez cocher au moins l'un des critères suivants :**

- ☒ Antivirus du poste client actif et à jour
- ☐ Firewall actif sur le poste client
- ☐ SES installé sur le poste client
- ☐ Interdire les utilisateurs possédant les droits d'administration du poste client
- ☒ Vérifier les versions (numéro de build) de Windows 10 / Windows 11

**WINDOWS 10**    **WINDOWS 11**

☒ Autoriser une plage de versions (builds)


Version minimale	Version maximale
<input type="text" value="19045"/>	<input type="text"/>

 En l'absence d'une version maximale, tous les numéros de build suivant la version minimale

**Explication :** Si le poste ne remplit pas ces critères (ex: PC personnel non sécurisé), la connexion est refusée avant même l'authentification réseau.

## B. Règle de Firewall (ACL) dédiée au VPN SSL

Une fois le tunnel monté, le trafic doit être explicitement autorisé par une règle de filtrage.




 VPN / VPN SSL

**ON** ☐ Activer le VPN SSL



**PARAMÈTRES GÉNÉRAUX** VÉRIFICATION DES POSTES CLIENTS (ZTNA)

---

Paramètres réseaux

Adresse IP publique (ou FQDN) de l'UTM utilisée	<input type="text" value="192.168.122.10"/>
Réseaux ou machines accessibles	<input type="text" value="Network_in"/> 
Réseau assigné aux clients (UDP)	<input type="text" value="NetworkVPN_SSL"/> 
Réseau assigné aux clients (TCP)	<input type="text" value=""/> 
Maximum de tunnels simultanés autorisés	62

Paramètres DNS envoyés au client

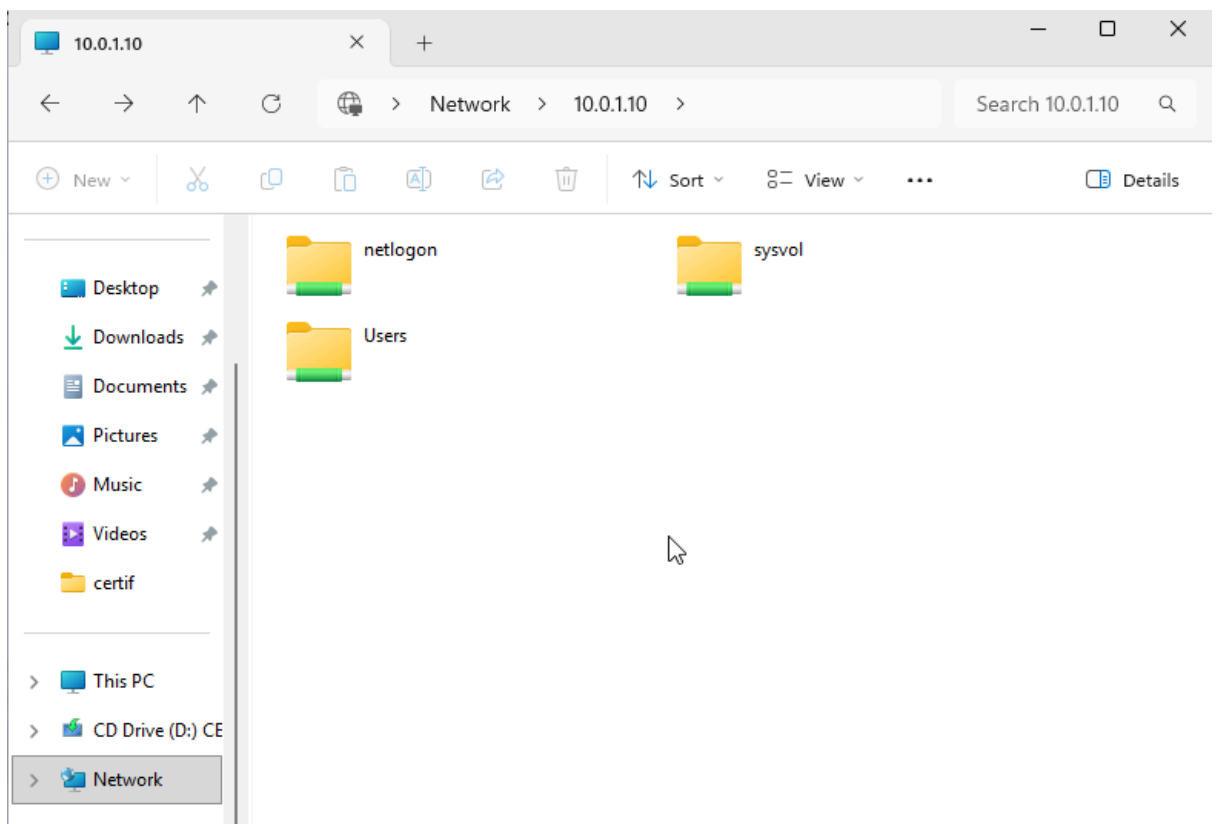
Nom de domaine	<input type="text" value="openbank.loc"/>
Serveur DNS primaire	<input type="text" value="Server_Paris"/> 
Serveur DNS secondaire	<input type="text" value="Configuré pour le firewall"/> 

### Explication de la règle :

- **Réseau assigné aux clients** : **NetworkVPN\_SSL** (Plage IP virtuelle 10.60.0.0/24).
- **Machines accessibles** : **LAN\_Paris** (Serveurs de fichiers et Contrôleur de domaine).

## C. Validation (Critères d'acceptation)

Le test final valide l'accès aux ressources partagées de l'entreprise.



## VI. Plan de Déploiement et Retour Arrière

Cette section décrit la méthodologie appliquée pour minimiser l'impact sur la production bancaire.

### A. Phases de déploiement

- **Phase 1 : Pré-production (J-2)**
  - Validation technique complète sur maquette iso-fonctionnelle (GNS3).
  - Préparation des scripts et fichiers de configuration.
- **Phase 2 : Mise en production (Jour J)**
  - **Horaire** : 20h00 - 22h00 (Heures non ouvrées) pour ne pas impacter les flux financiers.
  - **Action 1** : Snapshot des VMs (Serveurs) et Backup de la configuration Firewall.
  - **Action 2** : Déploiement des certificats et activation du VPN IPsec.
  - **Action 3** : Ouverture du service VPN SSL et tests ZTNA.

### B. Plan de Retour Arrière (Rollback)

En cas d'échec critique (perte de connexion inter-sites ou blocage abusif) :

1. **Immédiat** : Désactivation des règles de filtrage ZTNA et Proxy.
2. **Restauration** : Rechargement de la configuration de sauvegarde "J-1" sur les firewalls.
3. **Système** : Restauration des snapshots QEMU-KVM si l'AD a été corrompu.
4. **Secours** : Bascule temporaire sur une authentification VPN par clé pré-partagée (PSK) simple le temps du diagnostic PKI.