



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)

Versio n	Date	Auteur	Description des modifications	Validé par
0.1	28/01/202 6	Calix Hoëllard	Création du document (Draft - Maquette)	-
1.0	29/01/202 6	Calix Hoëllard	Validation des tests VPN, Proxy & ZTNA	Samir Assaf (DSI)

Sommaire

Tableau de Versionning (Traçabilité)	1
Sommaire	2
I. Introduction et Contexte	3
A. Objectif	3
B. Périmètre technique	3
C. Contraintes et Accessibilité	3
II. Gestion des Certificats (PKI)	3
A. Création de l'Autorité de Certification (CA)	3
B. Certificats Serveurs	4
III. Interconnexion Site-à-Site (VPN IPsec)	5
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
IV. Sécurisation de la Navigation (Proxy & Filtrage)	7
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
V. Accès Distant (VPN SSL & ZTNA)	9
A. Configuration ZTNA (Conformité)	9
B. Règle de Firewall (ACL) dédiée au VPN SSL	10
C. Validation (Critères d'acceptation)	11
VI. Plan de Déploiement et Retour Arrière	12
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.

Émis pour	
Sujet	C=FR,ST=Île 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)	Île 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.

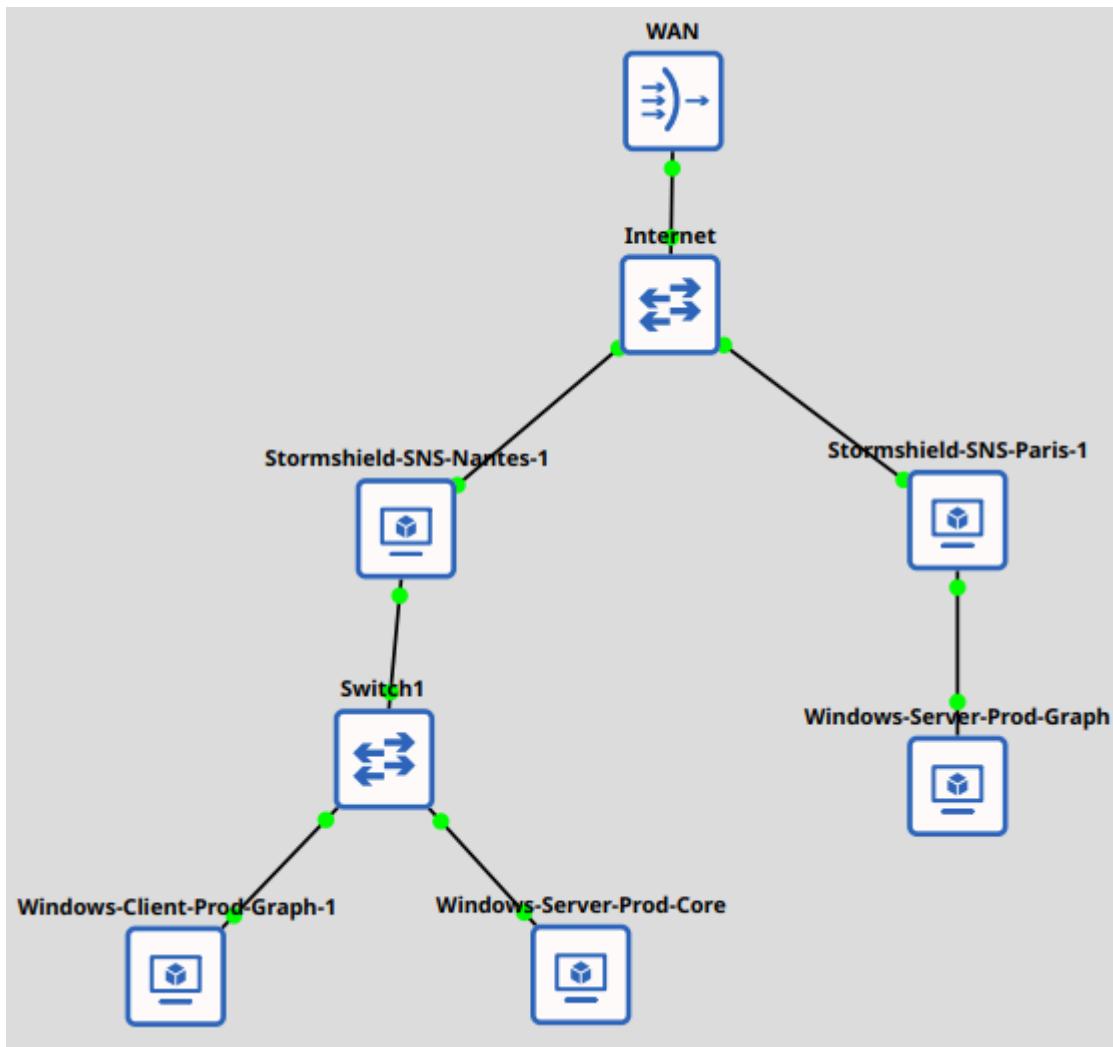
Émis pour	
Sujet	C=FR,ST=Île de France,L=Paris,O=OpenBank,OU=Banque,CN=firewall-paris
Nom (CN)	firewall-paris
Nom de l'organisation (O)	OpenBank
Nom de l'unité (OU)	Banque
Nom du lieu (L)	Paris
Nom de l'état ou de la province (ST)	Île de France
Pays (C)	FR
E-mail	
Somme de contrôle	e71af210

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).

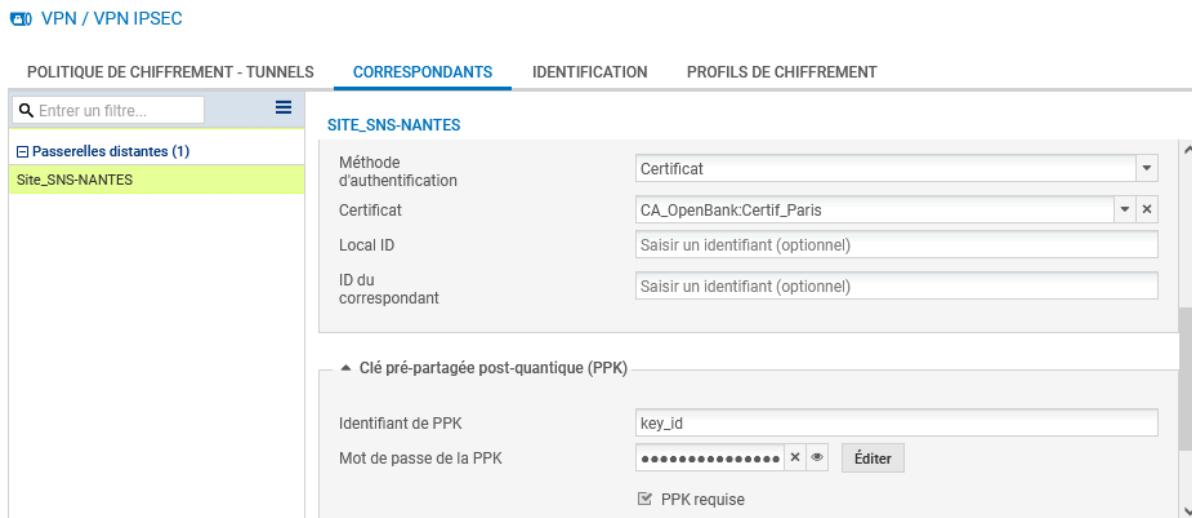
- **Sécurité** : Contrairement à un mot de passe (PSK) qui peut être volé ou bruteforcer, le certificat lie cryptographiquement l'identité à la machine.

- **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.



D. Validation et Traçabilité

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

Frame 107: Packet, 138 bytes on wire (1104 bits), 138 bytes on wire (1104 bits)
> Ethernet II, Src: 0c:65:66:57:00:00 (0c:65:66:57:00:00), Dst: 192.168.122.20 (192.168.122.20)
> Internet Protocol Version 4, Src: 192.168.122.20, Dst: 192.168.122.10
└ Encapsulating Security Payload
ESP SPI: 0xc9edc010 (33878001616)
ESP Sequence: 222
0000 0c 8f 7e 53 00 00 0c 65 66 57 00 00 08 00 45 00
0010 00 7c f3 65 00 00 40 32 11 7b c0 a8 7a 14 c0 a8
7a 0a c9 ed c0 10 00 00 00 de 12 ad 1e 39 96 49
0020 1b e1 0e ec db cf 69 e8 7e ca ca 1d 62 ed d9 bb
0030 4e c1 d8 e2 f2 ed 67 a2 3c 47 60 4f ce 21 04 7b
0040 27 73 d1 ab ac d8 32 95 72 ab 66 a4 95 1f ab 0c
0050 40 ba f3 47 69 7d 6c 8f df 80 e0 40 21 a9 75 7f
0060 1f 11 e0 e8 43 9e 2c 8e 0c d6 51 c0 1c de eb 30
0070 e3 07 14 a5 32 4e 04 25 b8 7d
0080

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.

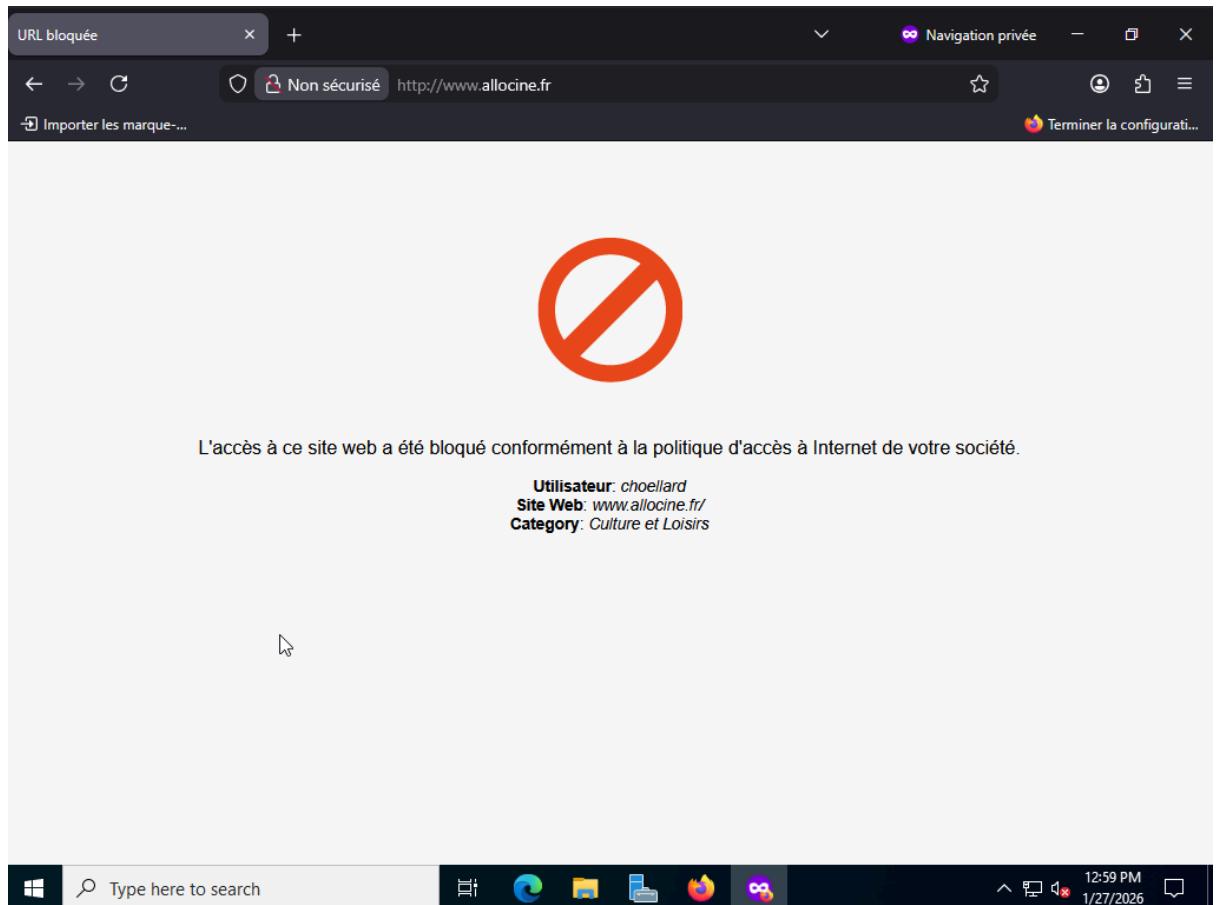
FILTERING NAT								
Searching...		Action	Source	Destination	Dest. port	Protocol	Security inspection	
1	on	pass	Network_in	Internet	dns		IPS	
2	on	Except:	unknown @ Network_in	Internet	http		IPS	
3	on	pass	Users @ Network_in	Internet	http		IPS (IPS_00) URL filter: URLFilter_00	
4	on	decrypt	Users @ Network_in	Internet	https		IPS (IPS_00) SSL filter: SSLFilter_00	
5	on	pass	Network_in	LAN-PARIS	Any		FW	
6	on	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.

The screenshot shows a configuration interface for a VPN connection. At the top, there is a green button labeled 'ON' and a grey button labeled 'Activer le VPN SSL'. Below this, there are two tabs: 'PARAMÈTRES GÉNÉRAUX' and 'VÉRIFICATION DES POSTES CLIENTS (ZTNA)', with the latter being active. In the 'VÉRIFICATION DES POSTES CLIENTS (ZTNA)' section, there is a note: 'Veuillez cocher au moins l'un des critères suivants :'. A list of checkboxes follows:

- 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

Below this, there are two tabs: 'WINDOWS 10' and 'WINDOWS 11', with 'WINDOWS 10' being active. Under 'WINDOWS 10', there is a radio button labeled 'Autoriser une plage de versions (builds)' and two dropdown menus for 'Version minimale' (set to 19045) and 'Version maximale'. A note below the dropdowns states: 'En l'absence d'une version maximale, tous les numéros de build suivant la version minimale'. The 'WINDOWS 11' tab is also visible.

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.

The screenshot shows the UTM interface under the 'VPN / VPN SSL' tab. The 'ON' button is selected, and the status is 'Activer le VPN SSL'. The configuration is divided into two main sections: 'PARAMÈTRES GÉNÉRAUX' and 'VÉRIFICATION DES POSTES CLIENTS (ZTNA)'.

PARAMÈTRES GÉNÉRAUX

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

VÉRIFICATION DES POSTES CLIENTS (ZTNA)

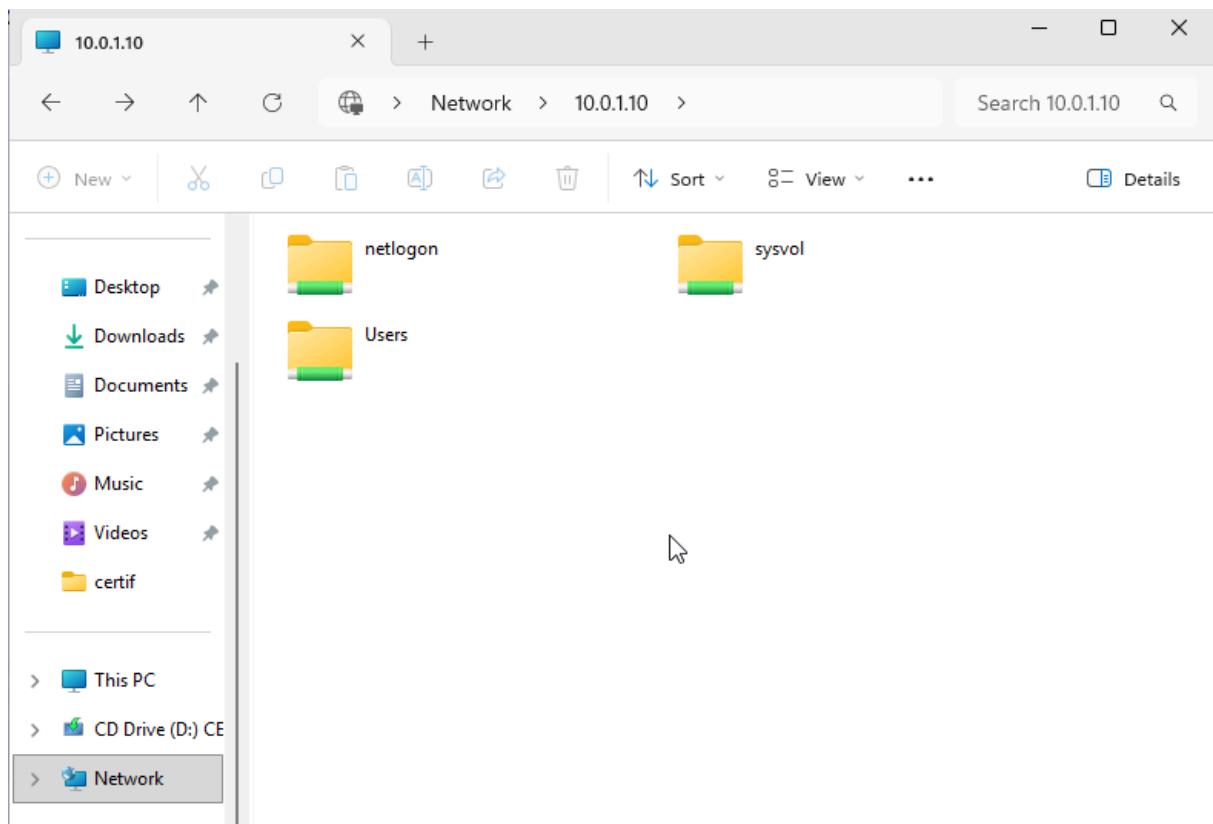
Paramètres DNS envoyés au client	<input type="button" value=""/>
Nom de domaine	openbank.loc
Serveur DNS primaire	Server_Paris
Serveur DNS secondaire	Configuré pour le firewall

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.