OPEN BANK

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

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)

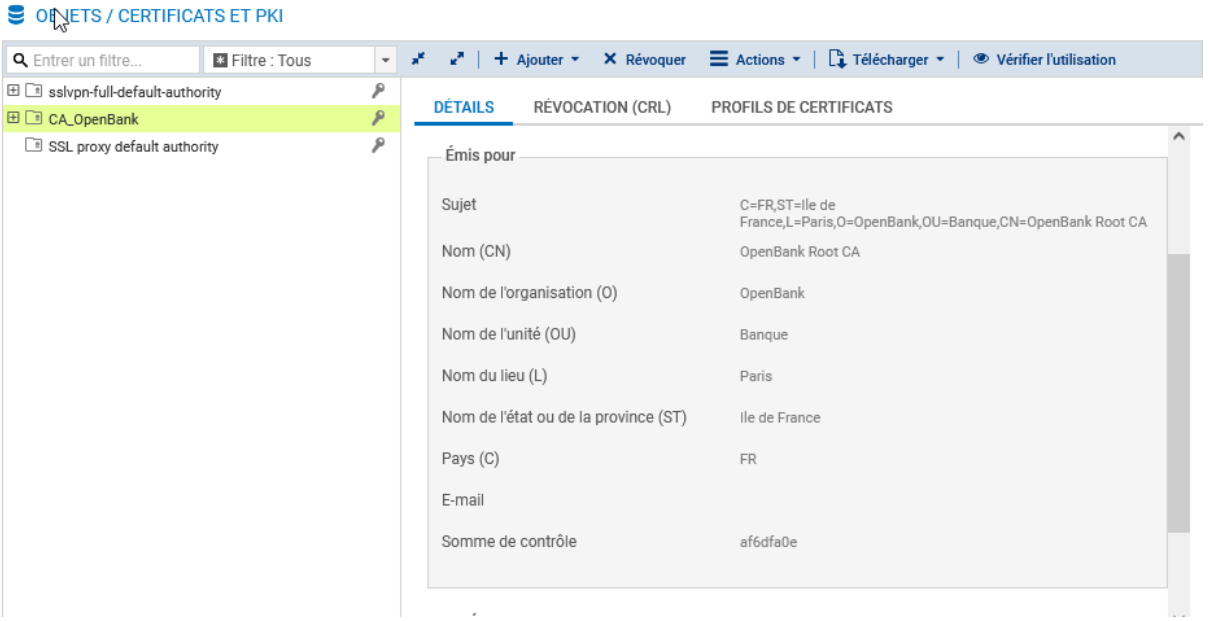
Afin de garantir une authentification forte des équipements et d'éviter les alertes de sécurité lors du déchiffrement SSL, une Infrastructure à Clés Publiques (PKI) interne a été déployée.

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

Explication technique :

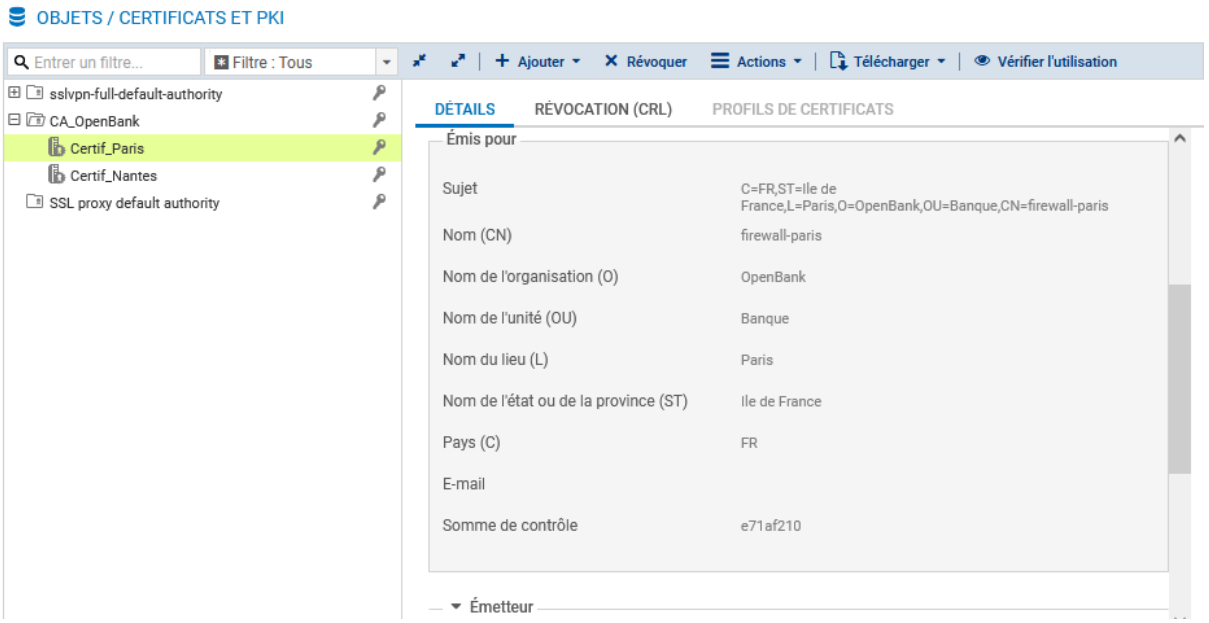
Nous avons choisi de créer une Autorité de Certification (CA) privée "OpenBank Root CA" directement sur le firewall principal. Cette approche permet de maîtriser la chaîne de confiance en interne. Tous les certificats émis par cette autorité seront automatiquement reconnus comme fiables par les machines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

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



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.

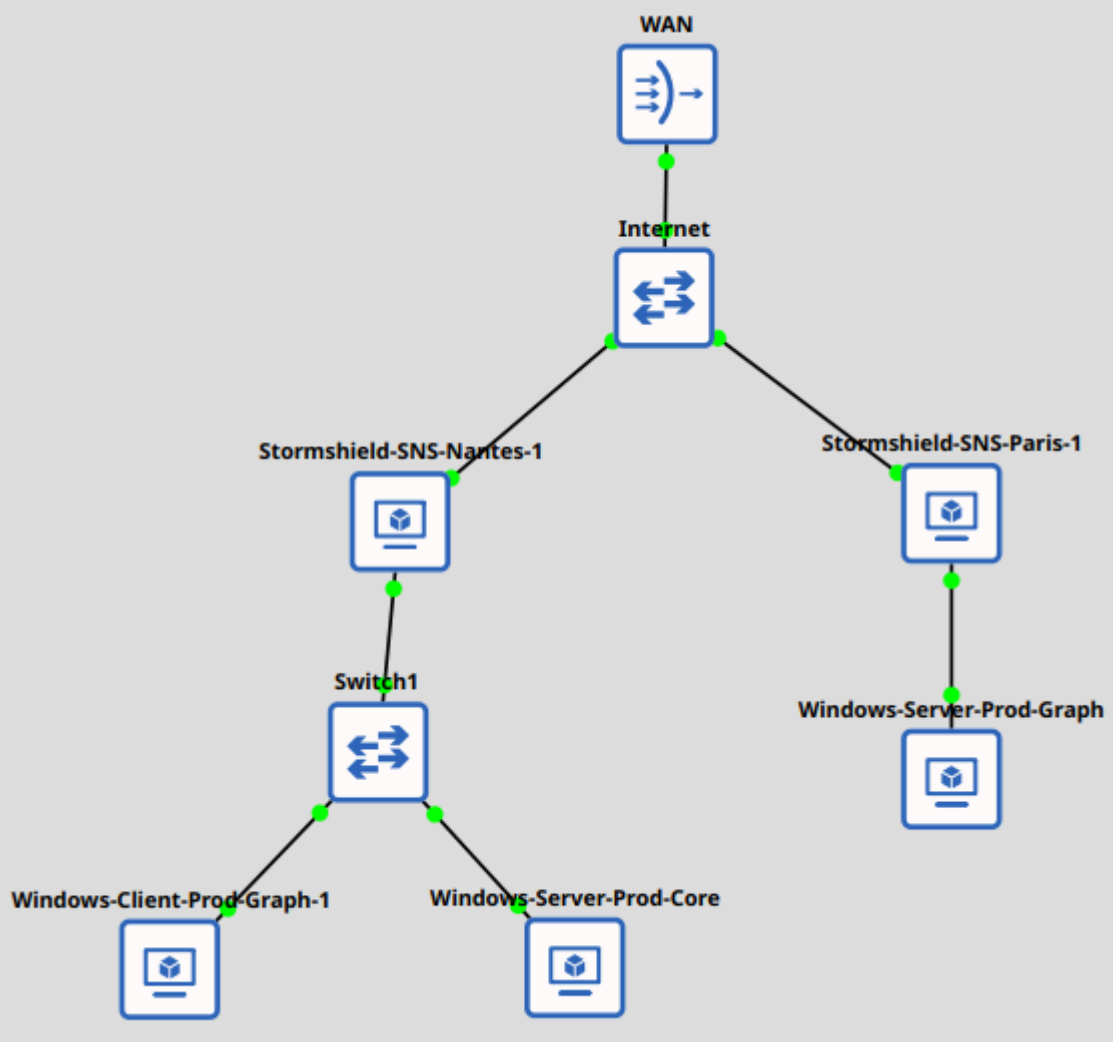


III. Interconnexion Site-à-Site (VPN IPsec)

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).

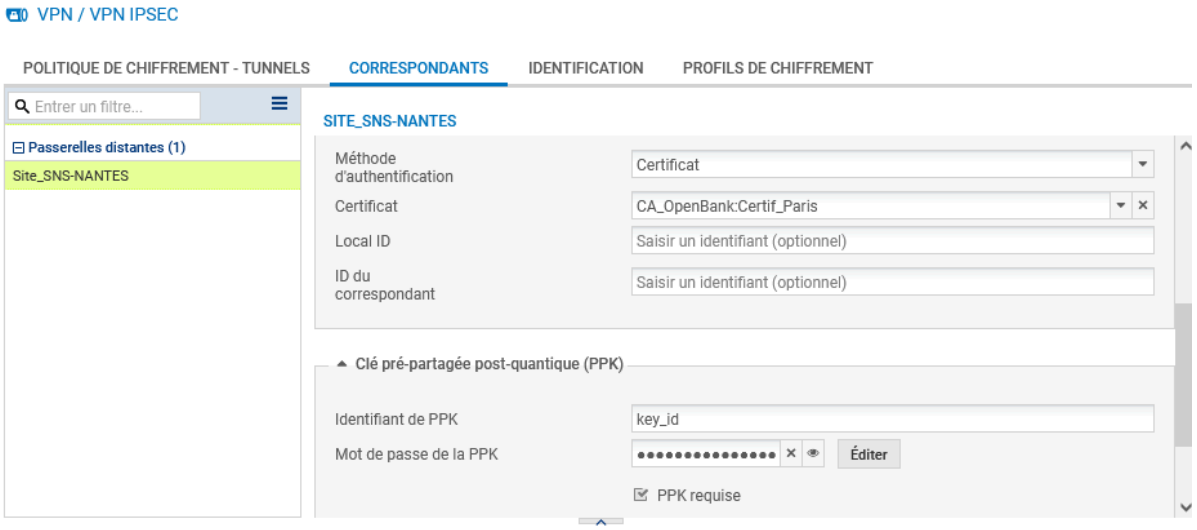
- **Sécurité :** Contrairement à un mot de passe (PSK) qui peut être volé ou bruteforcer, le certificat lie cryptographiquement l'identité à la machine.

- **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)

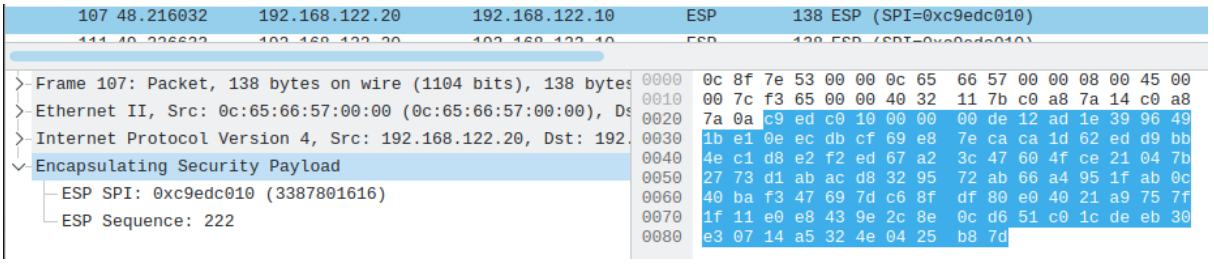
Conformément aux directives de l'ANSSI pour anticiper les futures menaces de déchiffrement, nous avons activé la protection Post-Quantique.

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.



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.

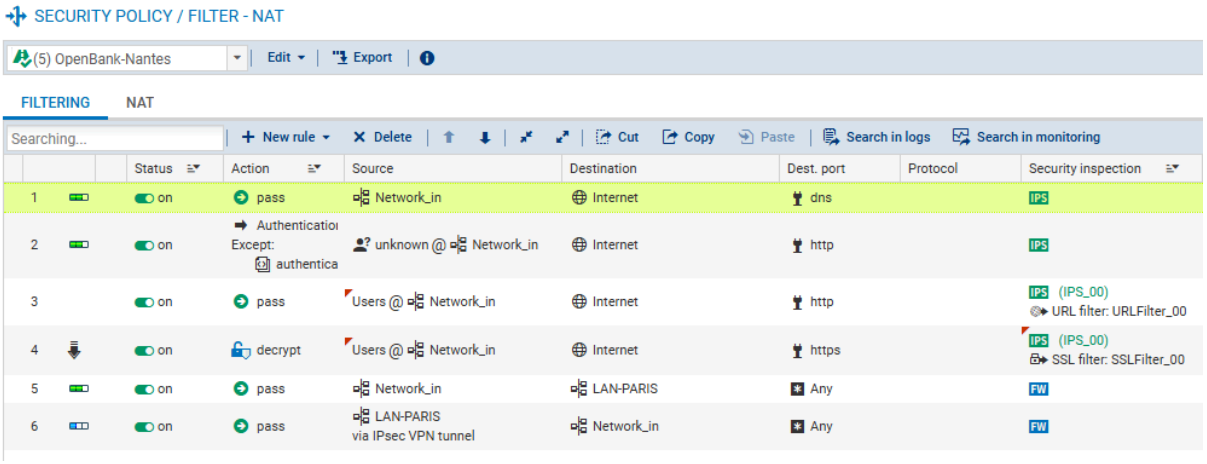
B. Règles de Filtrage URL

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.

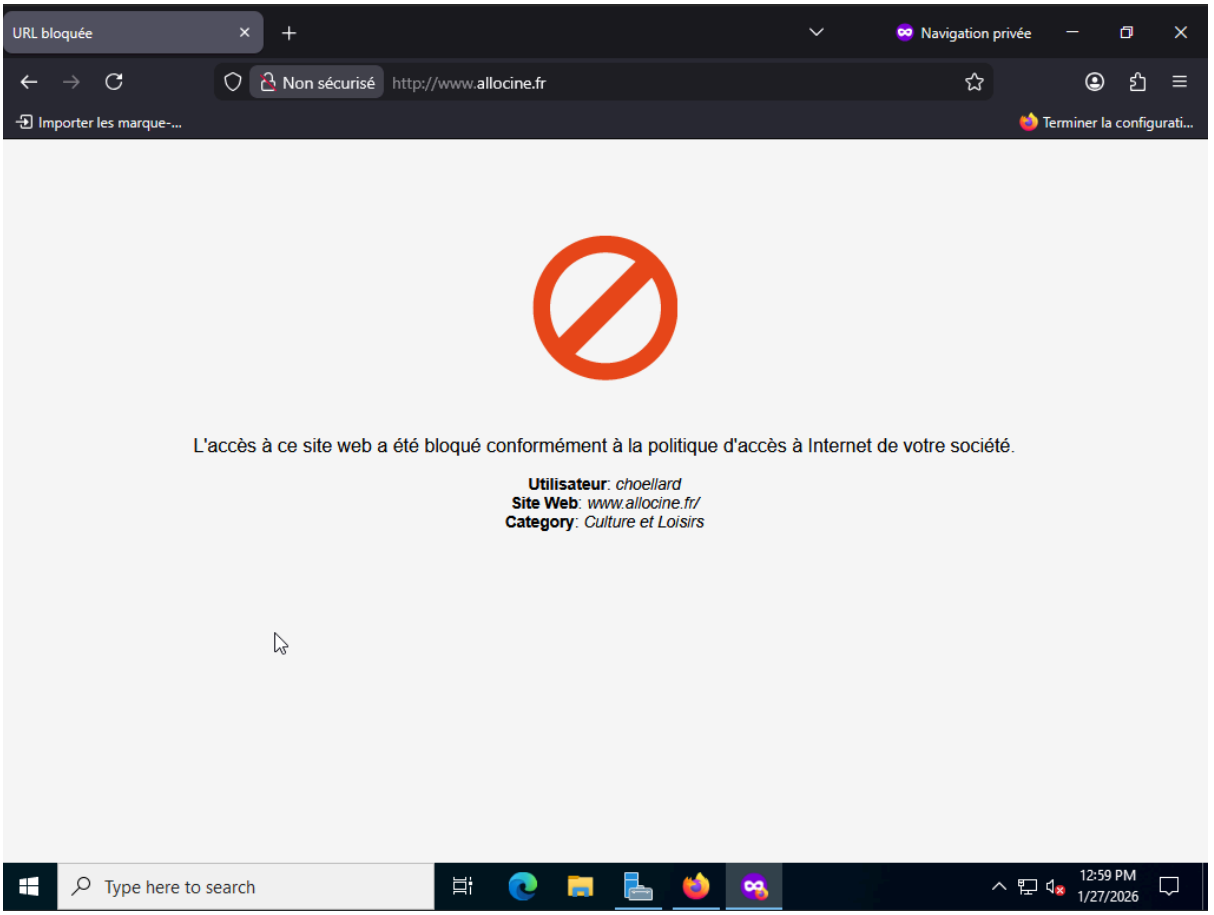


Explication de la règle :

Cette règle stipule que tout trafic venant du réseau interne (Source : Any + User : Authentified) 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.



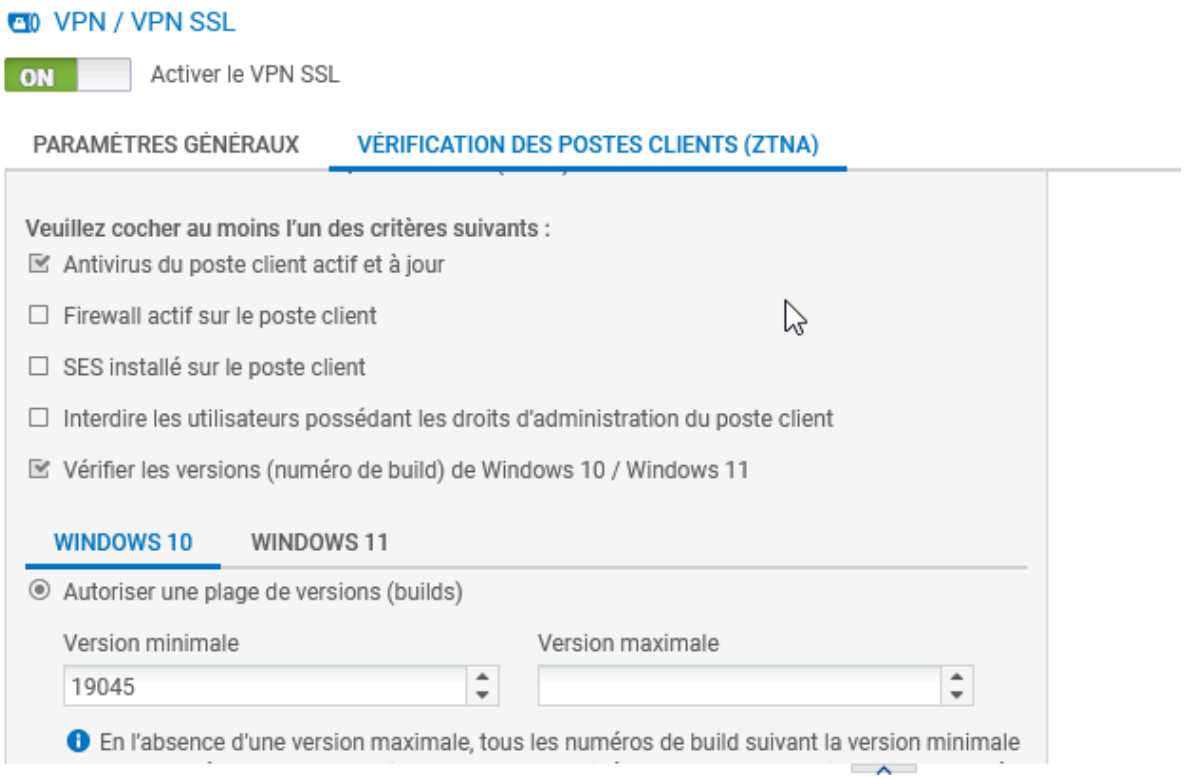
Texte Alternatif : Capture d'un navigateur web affichant le message "Accès Interdit" du firewall Stormshield.

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)

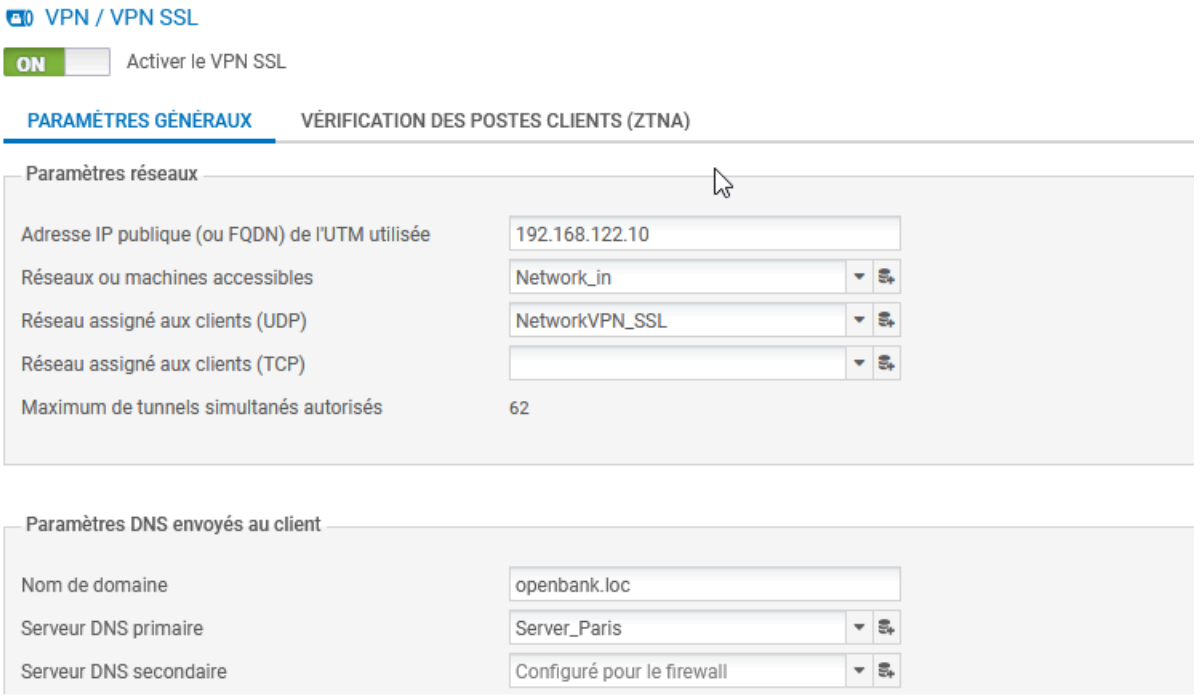
Le principe du ZTNA (Zero Trust Network Access) est de ne jamais faire confiance par défaut. Avant d'établir le tunnel, le firewall audite le poste client.



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.

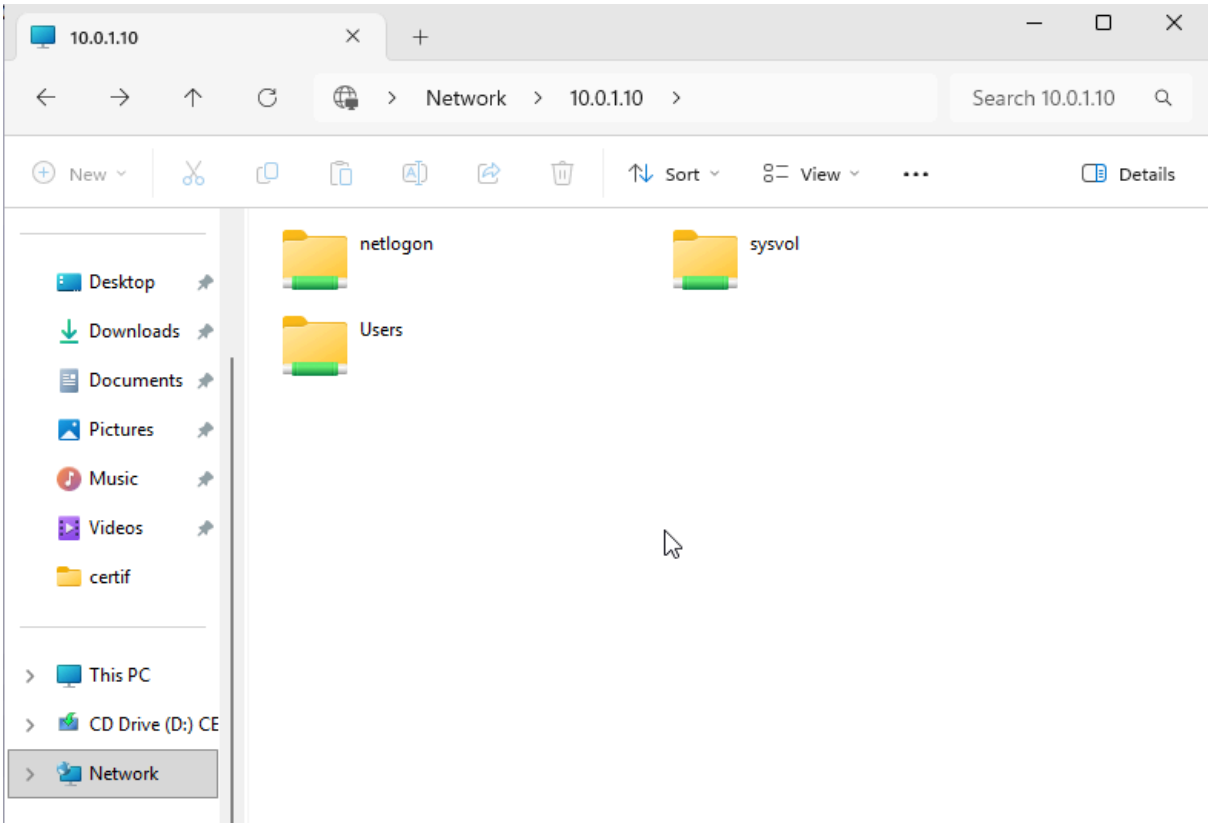


Explication de la règle :

- **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.