Solutions.com
LA FIBRE VENDÉENNE

Dossier U5

Mission 1

Ce document présente ma première mission concernant la mise en place d'une solution VPN pour les salariés d'une entreprise cliente.

GOBERT PIERRE-LOUIS
BTS SIO - OPTION A - SISR
CANDIDAT N°02046022493
SESSION 2026

UIMM PÔLE FORMATION LA FABRIQUE DE L'AVENIR
Fab Academy PAYS DE LA LOIRE

Tables des matières

PARTIE 1

Présentation du projet

1.1 Contexte

Une entreprise cliente a exprimé le besoin de permettre à ses collaborateurs d'accéder à distance aux ressources internes de son système d'information.

L'infrastructure actuelle repose sur une box opérateur (Livebox Orange) pour l'accès Internet, derrière laquelle est placé un pare-feu Zyxel USG Flex 20W afin d'assurer la sécurité et la segmentation réseau.

Avec la généralisation du télétravail et les besoins de mobilité, il est devenu indispensable de mettre en place une solution fiable et sécurisée permettant aux utilisateurs de se connecter depuis l'extérieur (domicile, réseau 4G, déplacements professionnels) tout en garantissant la confidentialité et l'intégrité des données.

GOBERT PIERRE-LOUIS
DATE 20/09/2025

1.2 Expression du besoin

- Permettre aux utilisateurs d'établir une connexion sécurisée vers le réseau interne de l'entreprise.
- Garantir la confidentialité des échanges grâce à un tunnel chiffré.
- Assurer une authentification fiable des utilisateurs.
- Rendre la solution simple à utiliser, notamment via un client VPN SSL.
- Offrir aux collaborateurs distants le même accès que s'ils étaient connectés en local au LAN de l'entreprise.

1.3 Objectifs

- Mettre en place une solution de VPN SSL sur le pare-feu Zyxel USG Flex 20W.
- Configurer les règles de sécurité nécessaires (firewall, NAT, DMZ).
- Créer et gérer les utilisateurs VPN avec les droits appropriés.
- Tester et valider l'accès à distance depuis un poste externe (réseau domestique ou 4G).

PARTIE 2

Études et choix de la solution

2.1 Comparaison des solutions

Solution VPN	Avantages	Inconvénients
IPsec	Très sécurisé (chiffrement fort, standardisé). Convient bien aux interconnexions site-à-site.	Plus complexe à configurer côté client. Moins adapté pour des utilisateurs non techniques.
SSL	Facile à déployer (client Zyxel fourni, compatible Windows/Linux). Accès utilisateur simple (login + mot de passe). Très adapté au télétravail.	Légèrement moins performant qu'IPsec pour de gros volumes de données.
L2TP	Largement supporté par les systèmes d'exploitation.	Configuration plus complexe, nécessite souvent l'ouverture de multiples ports et peut poser des problèmes de compatibilité.

GOBERT PIERRE-LOUIS
DATE 20/09/2025

2.2 Choix retenu

Après analyse, la solution retenue est le VPN SSL pour les raisons suivantes :

- Solution adaptée au travail à distance et aux besoins de mobilité.
- Compatible avec l'équipement existant (pare-feu Zyxel USG Flex 20W).
- Mise en œuvre plus simple qu'un tunnel IPSec tout en restant suffisamment sécurisé.
- Utilisation d'un port unique (TCP/443 ou personnalisé) ce qui facilite la configuration derrière la Livebox et évite des problèmes de compatibilité.

PARTIE 3

Planification et organisation

3.1 Étapes du projet

Le projet a été découpé en plusieurs étapes afin de structurer la mise en place de la solution :

1. Analyse du besoin et validation avec l'entreprise cliente.
2. Comparaison des solutions VPN disponibles (L2TP, IPSec, SSL).
3. Choix du VPN SSL comme solution adaptée.
4. Préparation du matériel et des adresses IP (plan d'adressage).
5. Configuration de base du pare-feu Zyxel USG Flex (interfaces WAN, LAN, DMZ).
6. Mise en place du VPN SSL :
   - Création du pool d'adresses (SSL_POOL),
   - Création des objets réseaux (HOME_LAN, etc.),
   - Configuration du portail VPN et des règles d'accès.
7. Tests internes pour valider la connectivité entre VPN et réseau local.
8. Tests externes via connexion 4G et Internet hors entreprise.
9. Rédaction de la documentation (captures d'écran, rapport, axes d'amélioration).

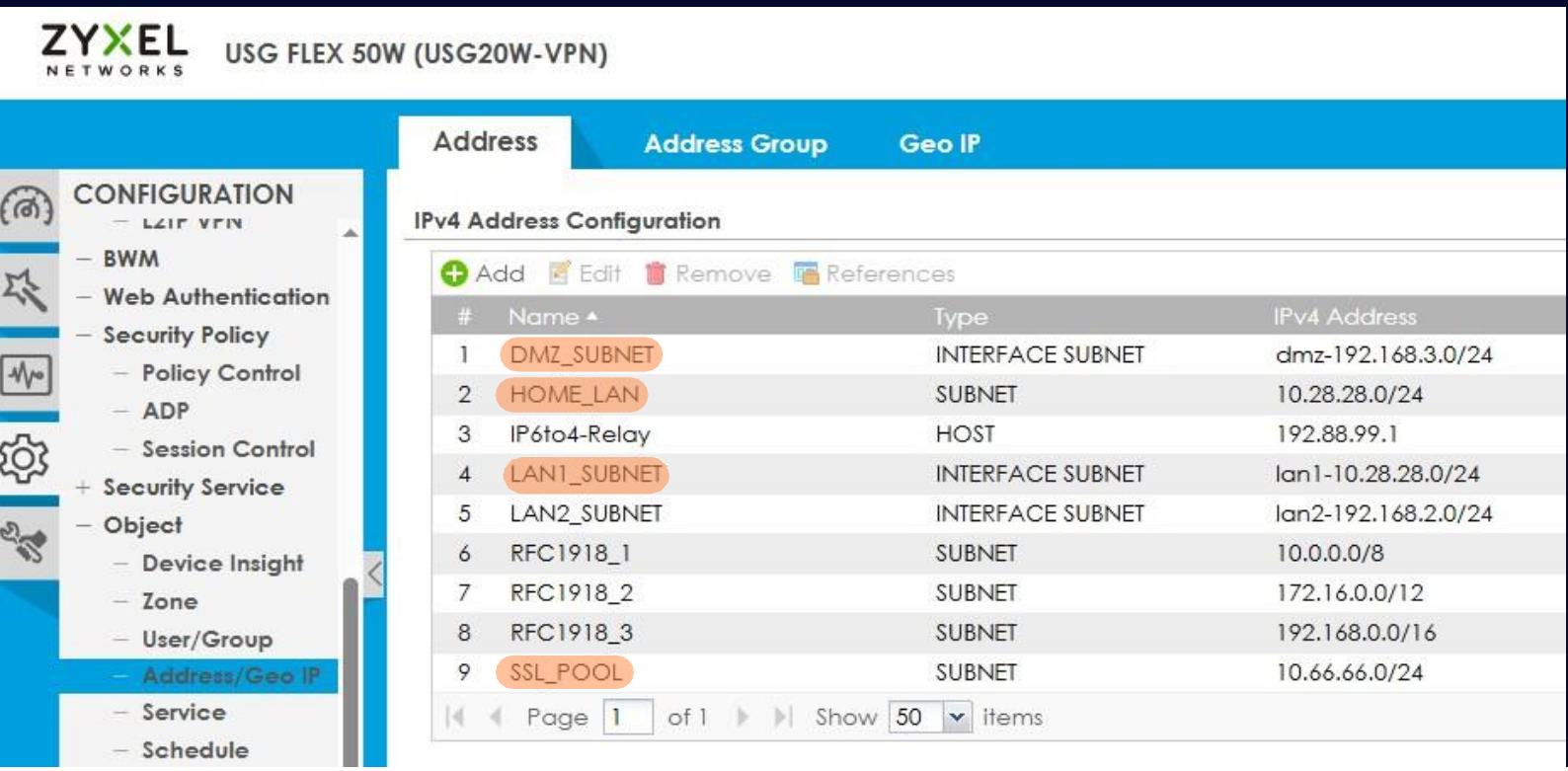
3.2 Matériels et logiciels utilisées

Matériel / Logiciel	Description
Zyxel USG 20W 	Par-feu et passerelle VPN de l'entreprise
Poste clients (Windows/Linux) 	Machines utilisées pour tester la connexion VPN
Client VPN Zyxel 	Logiciel permettant la connexion SSL VPN
Accès Internet 	Connexion WAN pour les tests
Livebox Pro 	Fournisseur d'accès Internet
Navigateur web 	Administration

3.3 Plan d’adressage

Réseau / Zone	Adresse	Masque	Rôle
WAN (vers Livebox)	192.168.1.20	255.255.255.0	Adresse de l’USG côté Internet
Livebox (passerelle)	192.168.1.1	255.255.255.0	Routeur FAI
LAN1 (interne)	10.28.28.1	255.255.255.0	Réseau interne de l’entreprise
DMZ	192.168.3.1	255.255.255.0	Réseau isolé pour les services
SSL_POOL (VPN)	10.66.66.0/24	255.255.255.0	Pool attribué aux clients VPN
HOME_LAN (objet)	10.28.28.0/24	255.255.255.0	Réseau interne accessible en VPN

Dans la section Address/Geo IP, on retrouve les configurations des adresses IPv4 de DMZ, HOME_LAN, Lan1 et SSL_POOL



GOBERT PIERRE-LOUIS
DATE 20/09/2025

PARTIE 4

Mise en œuvre technique

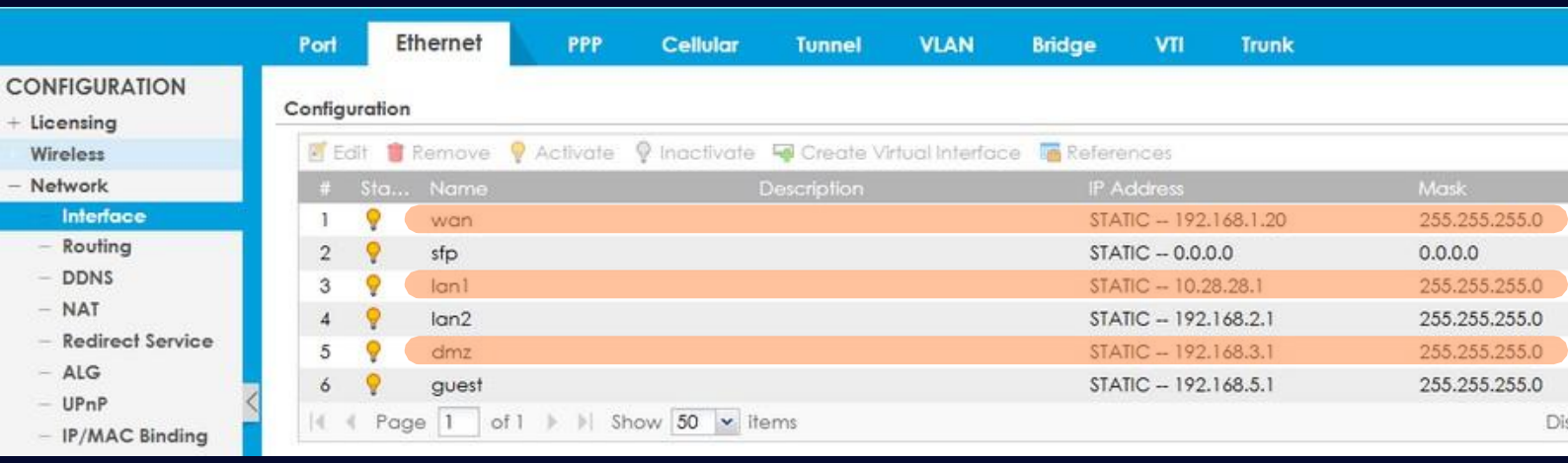
4.1 Configuration de base du pare-feu

Définition des interfaces réseau :

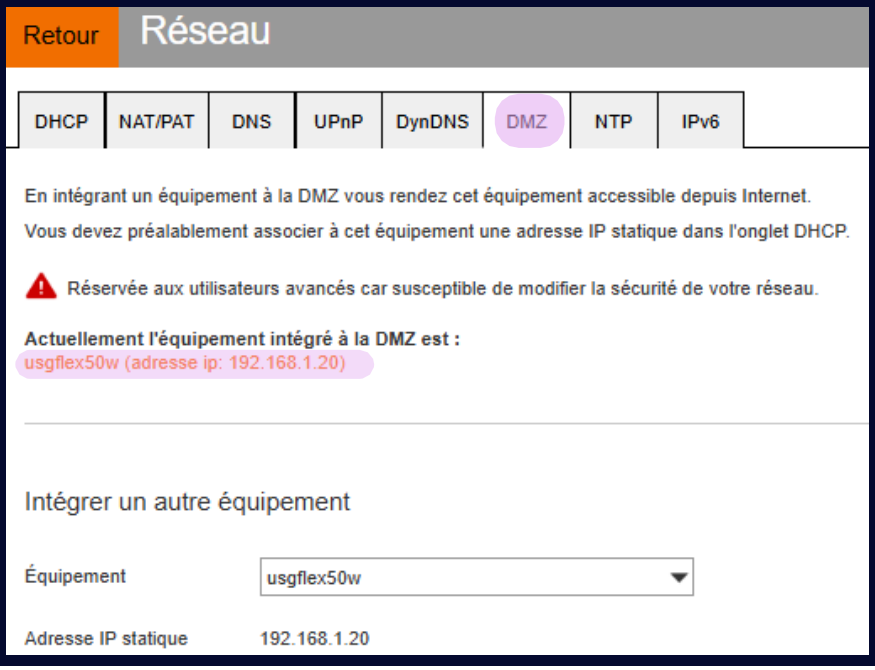
WAN (192.168.1.20/24 relié à la Livebox, en DMZ).
LAN1 (10.28.28.1/24 pour le réseau interne).
DMZ (192.168.3.1/24 isolée).
SSL VPN (pool 10.66.66.0/24).

Intégration de l'USG dans la DMZ de la Livebox afin de rendre les services VPN accessibles depuis Internet.

Sur la page Ethernet de l'interface de l'USG on voit que WAN, LAN1 et DMZ sont bien configurés



On configure le DMZ sur la LiveBox pour intégrer notre USG



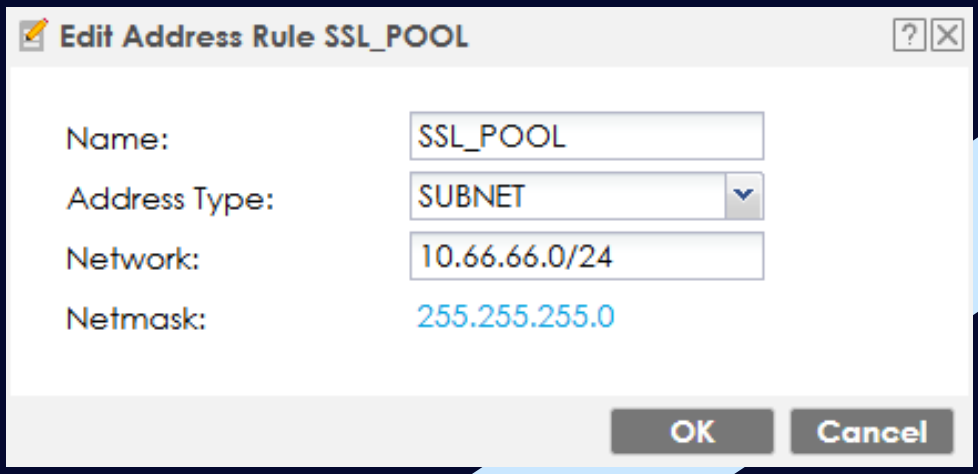
4.2 Mise en place du VPN SSL

Activation du service SSL VPN dans l'USG.

Définition des paramètres globaux :

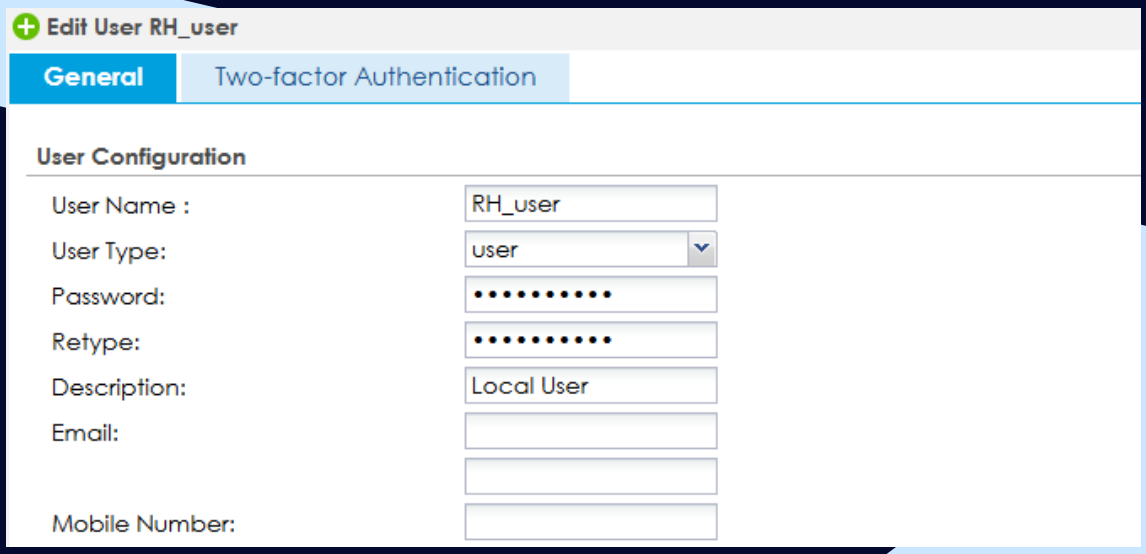
Extension réseau locale : 10.66.66.1
Port du serveur SSL VPN : 443 (pour éviter conflit avec 8443 admin).

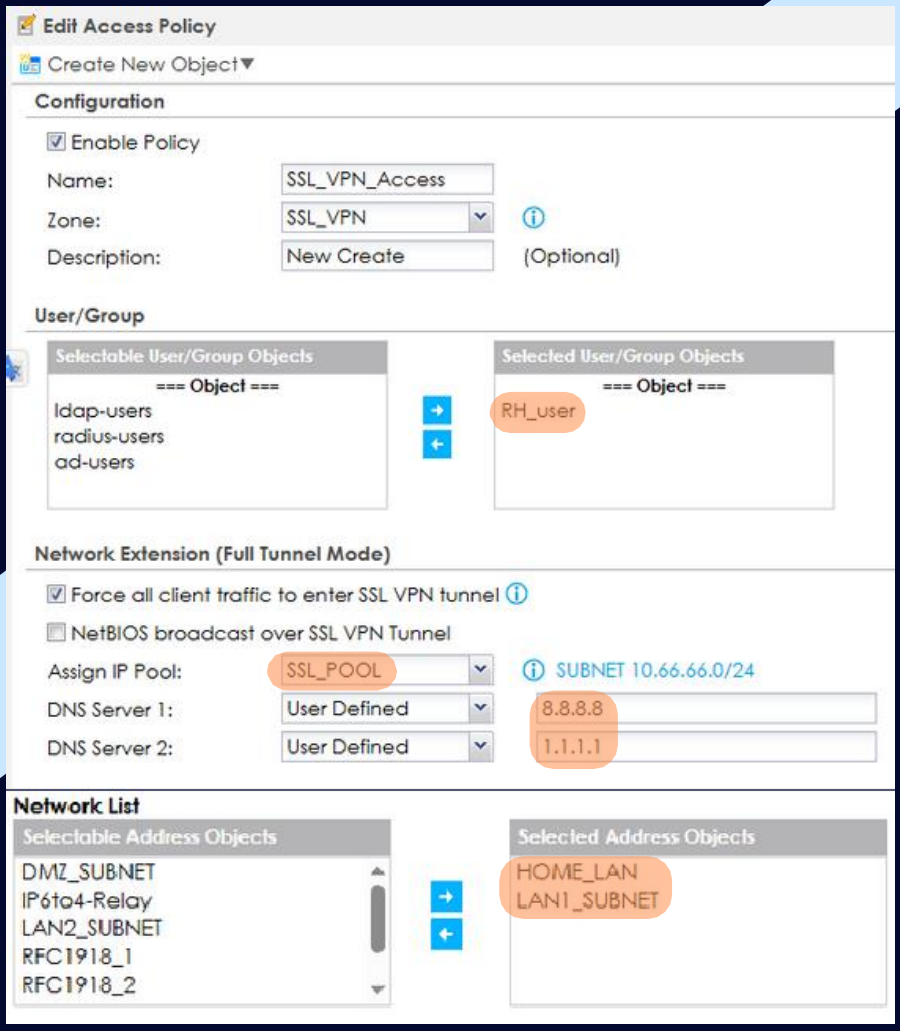
Création d'un pool d'adresses dédié (SSL_POOL : 10.66.66.0/24).



4.3 Gestion des utilisateurs et des accès

Création d'un utilisateur VPN avec mot de passe robuste.





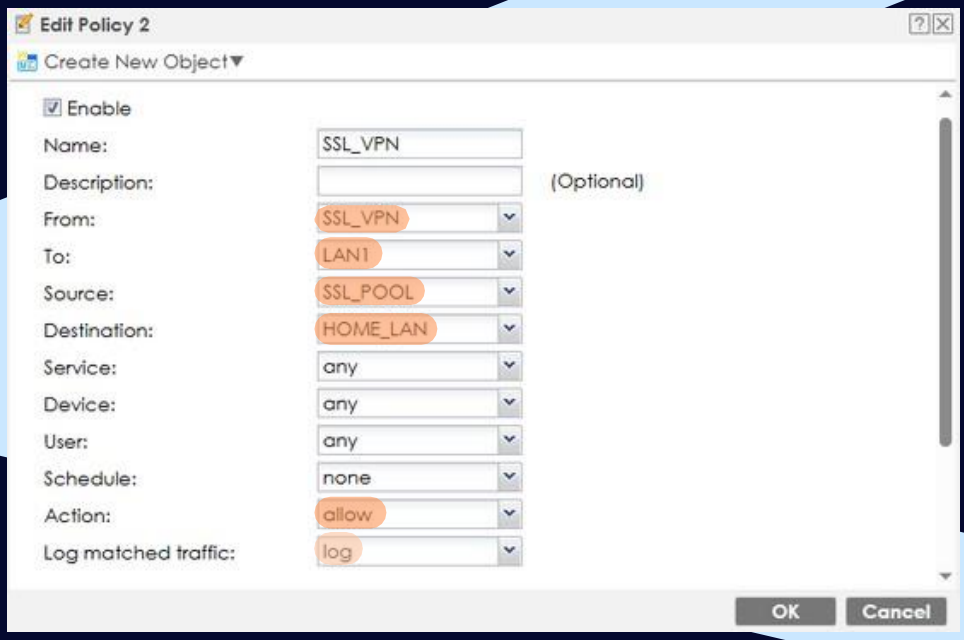
Création d'une Access Policy associant cet utilisateur au VPN SSL :

- IP Pool : SSL_POOL
- DNS : 8.8.8.8 et 1.1.1.1
- Réseaux autorisés : HOME_LAN et LAN1_SUBNET

GOBERT PIERRE-LOUIS
DATE 20/09/2025

4.4 Règles de sécurité (firewall, filtrage)

Ajout d'une règle Policy Control :



Ajout d'une règle dans le pare-feu de la Livebox qui contourne les limites du firewall :

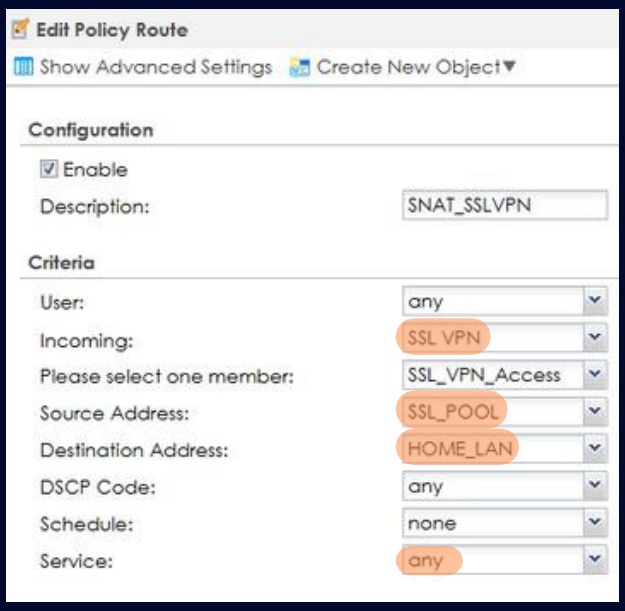
Retour **Pare-feu**

Règles personnalisées IPv4

Ajouter une règle

Application/Service	Protocole	Adresse IP source	Masque sous réseau	Port source	Adresse IP destination	Masque sous réseau	Port destination	Action
HTTP	TCP						80	accepter
HTTPS	TCP						443	accepter
POP3	TCP						110	accepter
POP3S	TCP						995	accepter
SMTPAuth	TCP						587	accepter
SMTP	TCP						25	accepter
FTP	UDP/TCP						20-21	accepter
SSH	TCP						22	accepter
NTP	UDP						123	accepter
NNTP	TCP						119	accepter
NNTPS	TCP						563	accepter
DNS	UDP/TCP						53	accepter
IRC	TCP						6666-6667	refuser
IMAP	TCP						143	accepter
IMAPS	TCP						993	accepter
ISAKMP	UDP						500	accepter
STUN	UDP						3478	accepter
IPSEC-NAT-T	UDP						4500	accepter
ESP-ALARM-TOOL	TCP						30000	accepter
ESP-ALARM	TCP						30100	accepter
SSLVPN	TCP				192.168.1.20	255.255.255.255	10443	accepter

Ajout d'une règle de SNAT Policy Route :



GOBERT PIERRE-LOUIS

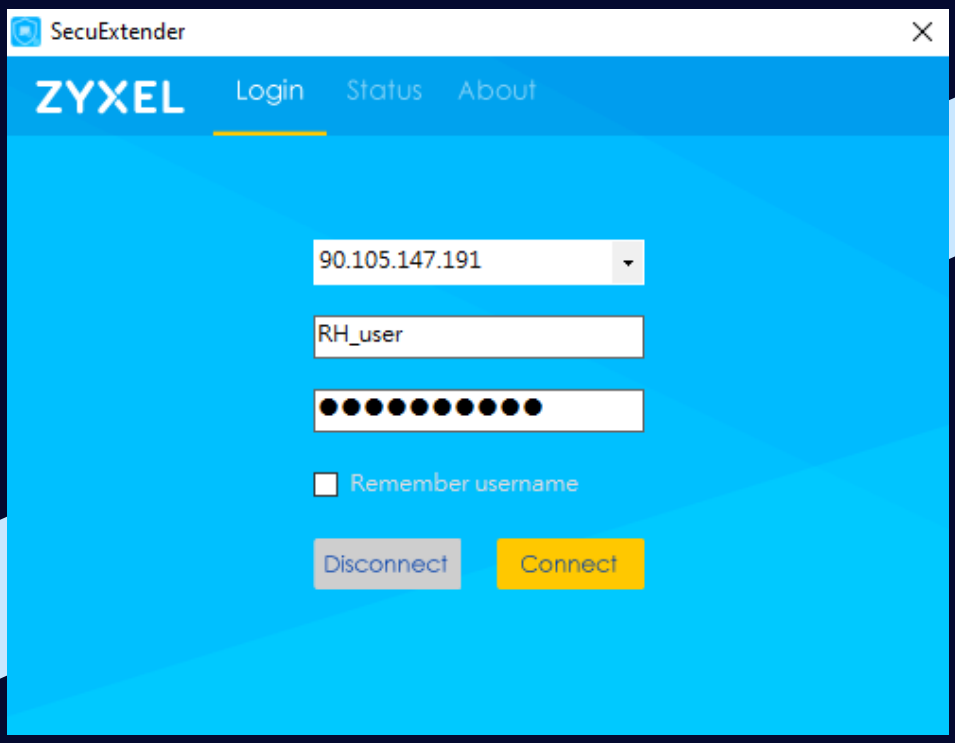
DATE 20/09/2025

PARTIE 5

Tests et validation

5.1 Connexion VPN depuis l'extérieur

Un test a été réalisé depuis un poste client connecté en 4G afin de simuler un utilisateur distant. L'utilisateur s'est connecté via Zyxel SecuExtender en utilisant l'IP publique de la Livebox et le port 443.



Les identifiants de l'utilisateur RH_user ont permis une authentification réussie.

5.2 Accès aux ressources internes via le VPN

On ouvre l'invite de commande et on entre *ipconfig* qui nous permet d'observer l'ip attribué à notre poste client

```
Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::4aaa:8574:6186:6dd1%42
   Adresse IPv4. . . . . . . . . . . . . .: 10.66.66.2
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.66.66.1
```

Ping 10.66.66.1 (gateway du pool VPN) : ✅ réponse reçue.

```
C:\Users\Louis>ping 10.66.66.1

Envoi d'une requête 'Ping'  10.66.66.1 avec 32 octets de données :
Réponse de 10.66.66.1 : octets=32 temps=89 ms TTL=64
Réponse de 10.66.66.1 : octets=32 temps=60 ms TTL=64
Réponse de 10.66.66.1 : octets=32 temps=72 ms TTL=64
Réponse de 10.66.66.1 : octets=32 temps=261 ms TTL=64

Statistiques Ping pour 10.66.66.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 60ms, Maximum = 261ms, Moyenne = 120ms
```

Ping 10.28.28.1 (interface LAN de l'USG) : ✅ réponse reçue.

```
C:\Users\Louis>ping 10.28.28.1

Envoi d'une requête 'Ping'  10.28.28.1 avec 32 octets de données :
Réponse de 10.28.28.1 : octets=32 temps=72 ms TTL=64
Réponse de 10.28.28.1 : octets=32 temps=73 ms TTL=64
Réponse de 10.28.28.1 : octets=32 temps=88 ms TTL=64
Réponse de 10.28.28.1 : octets=32 temps=94 ms TTL=64

Statistiques Ping pour 10.28.28.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 72ms, Maximum = 94ms, Moyenne = 81ms
```

Ping google.com : ✅réponse reçue.

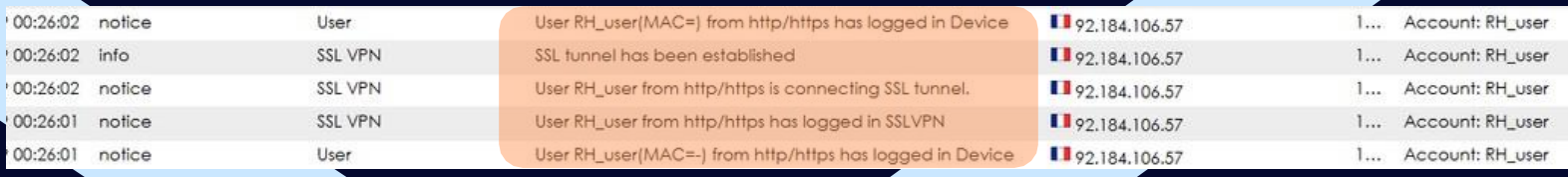
```
C:\Users\Louis>ping google.com

Envoi d'une requête 'ping' sur google.com [142.250.179.78] avec 32 octets de données :
Réponse de 142.250.179.78 : octets=32 temps=59 ms TTL=116
Réponse de 142.250.179.78 : octets=32 temps=67 ms TTL=116
Réponse de 142.250.179.78 : octets=32 temps=109 ms TTL=116
Réponse de 142.250.179.78 : octets=32 temps=54 ms TTL=116

Statistiques Ping pour 142.250.179.78:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 54ms, Maximum = 109ms, Moyenne = 72ms
```

5.3 Vérification de la sécurité

Plusieurs vérifications ont été effectuées afin de s'assurer du niveau de sécurité :

- Le service d'administration de l'USG est uniquement accessible en LAN (port 8443) et non depuis l'extérieur.
- Seul le service VPN SSL sur le port 443 est exposé côté WAN.
- Les règles du pare-feu de l'USG limitent le trafic des clients VPN au seul réseau interne autorisé (HOME_LAN).
- Les logs de l'USG confirment que les connexions VPN sont tracées et authentifiées.

Les logs de l'USG montrent l'authentification + tunnel + trafic + sécurité



PARTIE 6

Axes d'amélioration

6.1 Authentification forte (2FA)

Actuellement, la connexion SSL VPN se fait avec un identifiant et un mot de passe.

Pour renforcer la sécurité, il serait pertinent d'ajouter une authentification forte (2FA) via :

- Un token OTP (application type Google Authenticator, Microsoft Authenticator)
- Un envoi de code par SMS/email.

Cela limite les risques en cas de compromission du mot de passe utilisateur.

6.2 Supervision et logs

Les journaux du pare-feu USG montrent de nombreuses tentatives de connexion venant de l'extérieur (adresses IP étrangères).

Un système de supervision (ex. : Syslog, SIEM, ou plateforme type Graylog/ELK) permettrait :

- d'archiver les logs sur le long terme
- la détection automatiquement les tentatives suspectes
- d'alerter en temps réel l'administrateur.

00:32:18	notice	Security Policy Control	Match default rule, DROP	122.116.230.87:23422	1...	ACCESS BLOCK
00:32:11	notice	Security Policy Control	Match default rule, DROP	78.128.114.130:54734	1...	ACCESS BLOCK
00:32:09	notice	Security Policy Control	Match default rule, DROP	89.248.163.48:37470	1...	ACCESS BLOCK
00:32:09	notice	Security Policy Control	Match default rule, DROP [count=2]	192.168.1.10:8899	2...	ACCESS BLOCK
00:32:03	notice	Security Policy Control	Match default rule, DROP	192.168.1.1	2...	ACCESS BLOCK
00:31:49	notice	Security Policy Control	Match default rule, DROP [count=2]	192.168.1.10:8899	2...	ACCESS BLOCK
00:31:45	notice	Security Policy Control	Match default rule, DROP	18.223.104.85:34233	1...	ACCESS BLOCK
00:31:36	notice	Security Policy Control	Match default rule, DROP	138.197.166.67:61001	1...	ACCESS BLOCK
00:31:35	notice	Security Policy Control	Match default rule, DROP	92.42.201.26:48221	1...	ACCESS BLOCK
00:31:29	notice	Security Policy Control	Match default rule, DROP [count=2]	192.168.1.10:8899	2...	ACCESS BLOCK
00:31:25	notice	Security Policy Control	Match default rule, DROP	176.65.148.203:40887	1...	ACCESS BLOCK

PARTIE 7

Difficultés rencontrées

Au cours de cette mission, plusieurs obstacles techniques ont été rencontrés :

Accès au portail VPN : au départ, la connexion externe ne fonctionnait pas à cause du pare-feu Livebox.
- Solution : intégration de l'USG en DMZ et ajout d'une règle spécifique pour autoriser le port 443/10443.

SNAT/Policy Route : la configuration du routage des flux VPN vers le LAN interne a nécessité plusieurs ajustements.
- Solution : création d'une règle SNAT adaptée.

Conflit de ports d'administration : l'USG utilise par défaut le port 443 pour l'administration et pour le VPN SSL, ce qui a provoqué un blocage d'accès.
- Solution : modification du port d'administration (8443) et dédicace du port 443 uniquement au service VPN.

Ces difficultés ont permis de renforcer la compréhension du rôle du pare-feu et l'importance du filtrage.

GOBERT PIERRE-LOUIS
DATE 20/09/2025

PARTIE 8

Conclusion & Remerciements

En résumé, cette mission constitue un exemple concret de déploiement opérationnel d'une solution de sécurité réseau. La mise en place d'un VPN SSL sur l'USG Zyxel a apporté une réponse claire à un besoin fréquent en entreprise : permettre un accès distant sécurisé aux ressources internes. Cette réalisation a aussi contribué à développer des compétences techniques directement transposables en contexte professionnel, tout en soulignant les enjeux actuels de cybersécurité et de fiabilité des infrastructures.

Ce travail a mis en évidence plusieurs aspects essentiels pour un administrateur systèmes et réseaux :

- La compréhension des interactions entre différents équipements (box opérateur, pare-feu, clients VPN),
- La gestion fine des ports et des conflits de services,
- La vigilance nécessaire face aux menaces extérieures visibles dans les logs (scans, tentatives de connexion depuis l'étranger),
- Et l'importance d'une documentation précise et d'une méthodologie rigoureuse pour mener à bien une mise en œuvre technique.

Au-delà de la partie technique, ce projet illustre la valeur ajoutée d'un VPN dans un environnement professionnel : assurer la continuité d'activité pour les utilisateurs en mobilité, offrir une expérience fluide comme s'ils étaient présents sur site, et poser les bases d'améliorations futures telles que l'authentification forte, la supervision centralisée ou encore l'intégration de serveurs de fichiers internes.

GOBERT PIERRE-LOUIS
DATE 20/09/2025

Je tiens à exprimer mes sincères remerciements à Solutions.com pour m'avoir confié cette mission et permis de la réaliser au sein de l'entreprise cliente. Cette expérience m'a offert l'opportunité d'approfondir mes compétences techniques tout en découvrant la réalité des besoins de sécurité en environnement professionnel.

Je suis également reconnaissant envers mon formateur et mes encadrants pour leur disponibilité, leurs conseils avisés et leur accompagnement tout au long de ce projet.

Ce projet m'a également permis de mieux comprendre l'importance de la cybersécurité dans un contexte réel et de mesurer la responsabilité qui incombe à l'administrateur réseau.

Antonin Bollin

Antonin Ricou

Arnaud Dimarcq

GOBERT PIERRE-LOUIS
DATE 20/09/2025