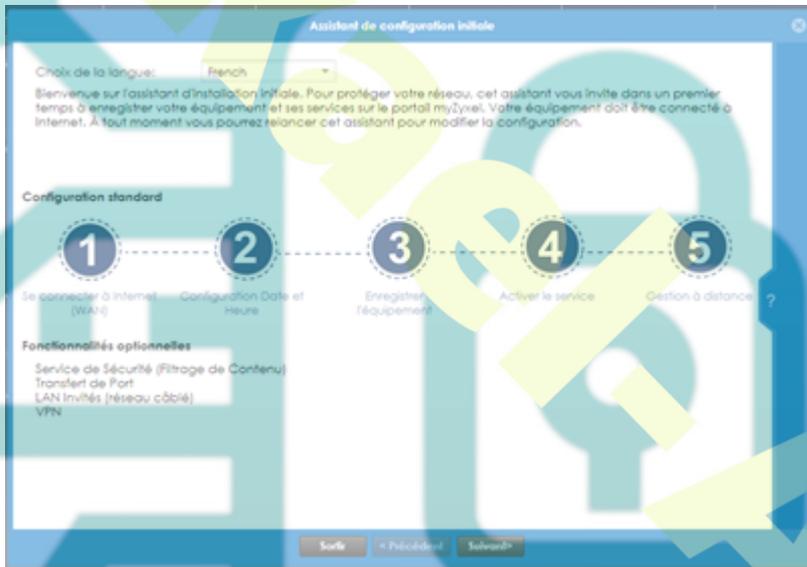


Tuto ZYXEL – NAT & VPN

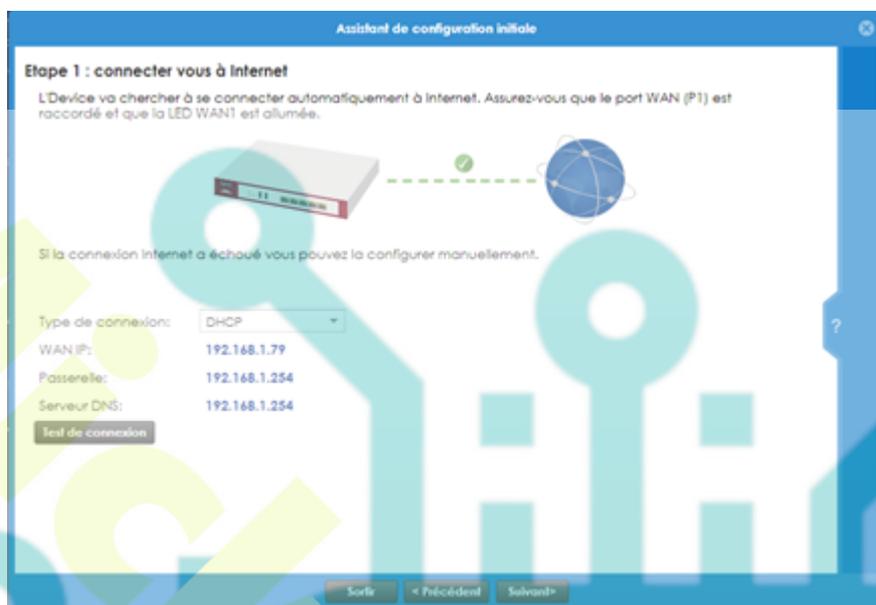
Configuration routeur ZYXEL USG20

Etape 1 – Configuration de base du routeur

Utiliser le WIZARD



Choisir d'être client DHCP coté WAN

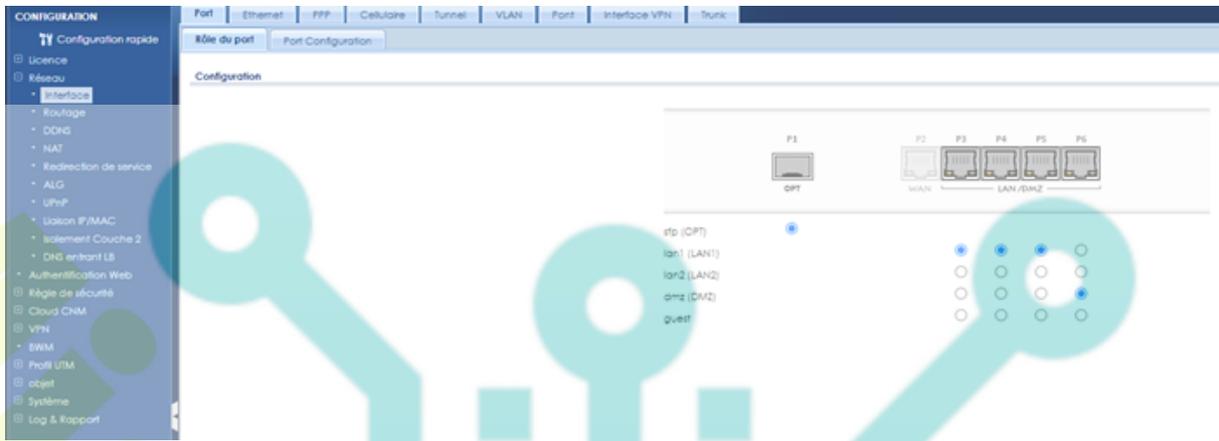


Sélectionner Gestion à distance



Etape 2 – répartition des ports

Choisir les ports LAN et celui qui servira à la DMZ

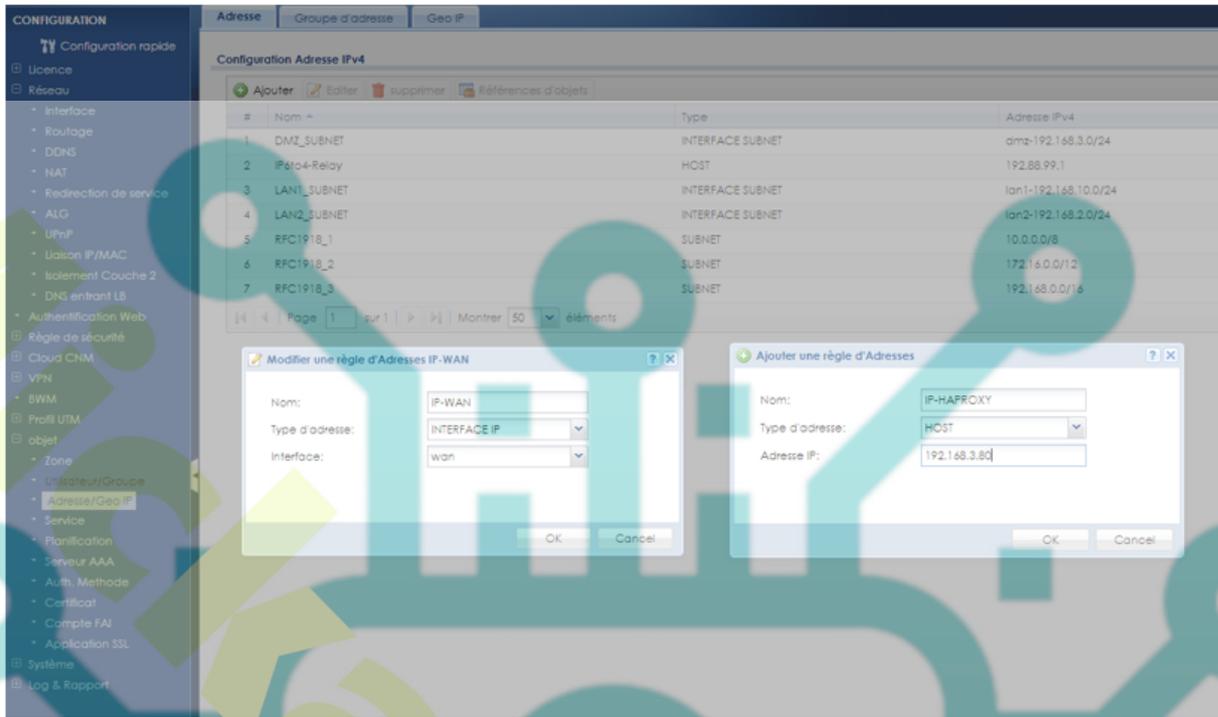


Etape 3 – Configuration de la partie LAN

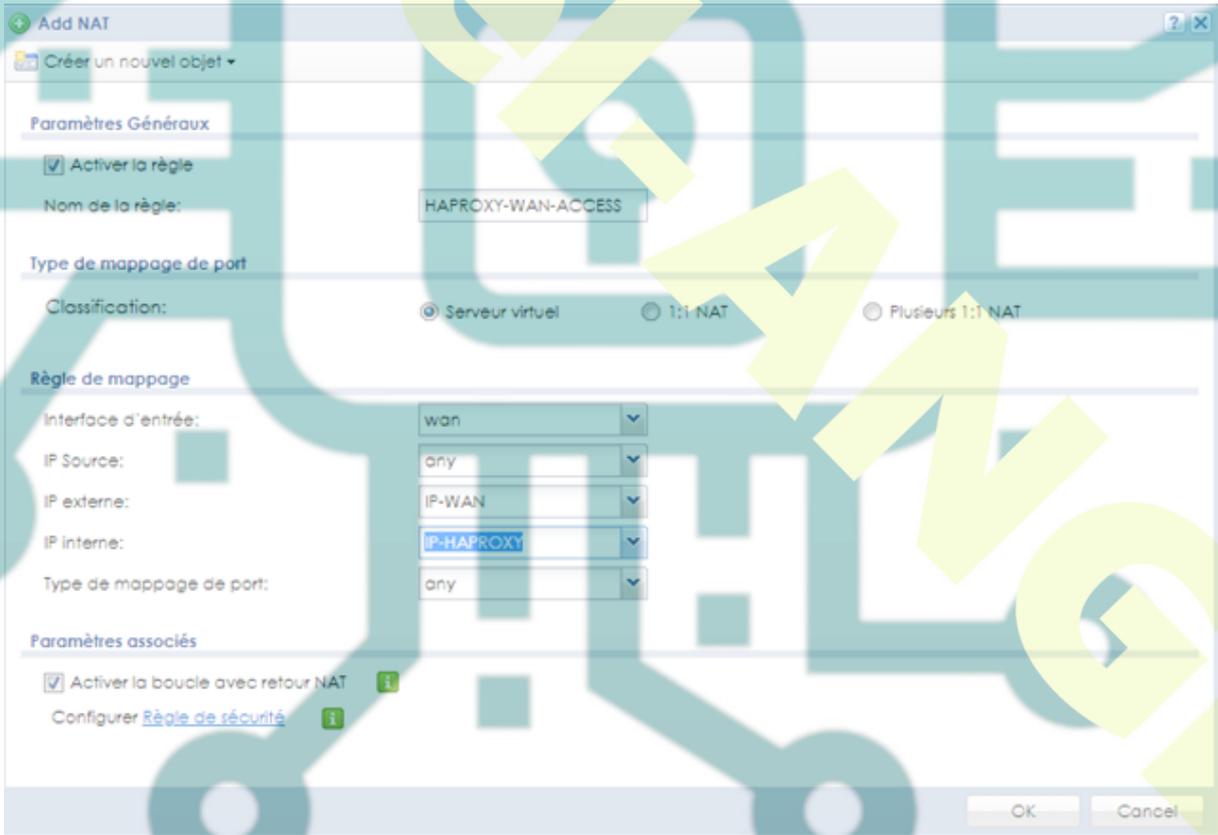


Configuration de la DMZ et du NAT

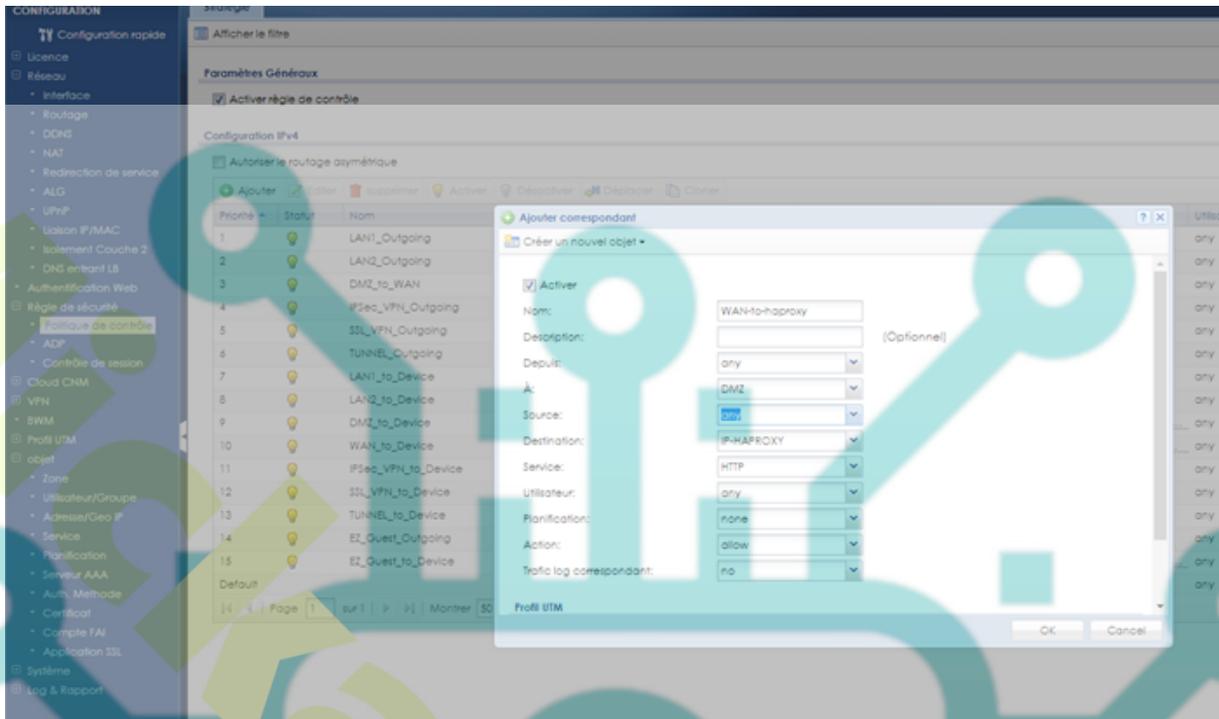
Ajouter 2 objets nommé IP-HAPROXY avec l'IP du proxy et IP-WAN avec interface du WAN



Créer une règle NAT



Configurer une ou plusieurs règles de sécurité pour la DMZ

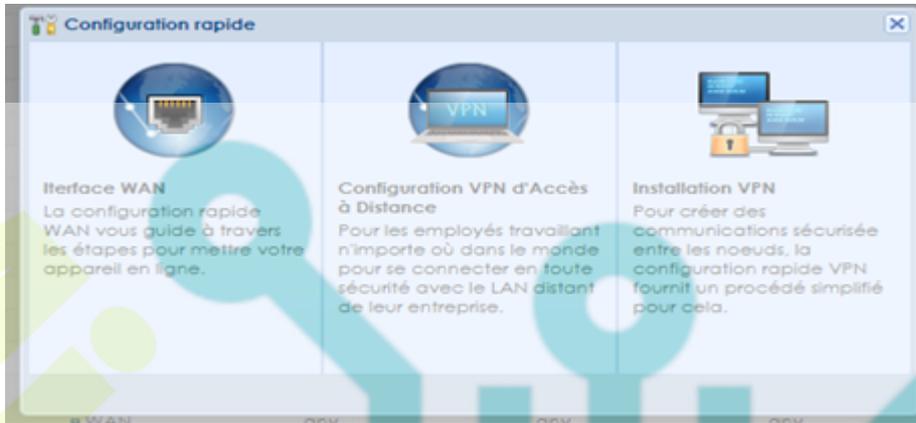


Configuration de la table de routage vers switch routage vlan



Configuration du VPN IPSEC

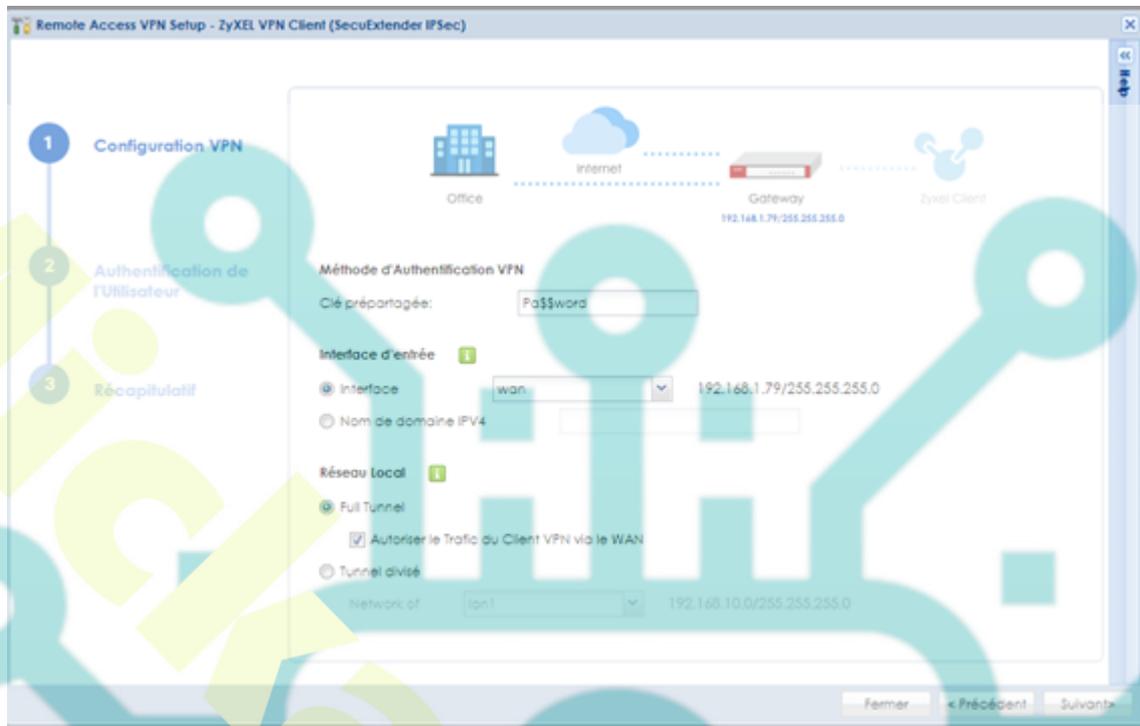
Utiliser dans le mode expert la configuration rapide et configuration VPN d'accès à distance



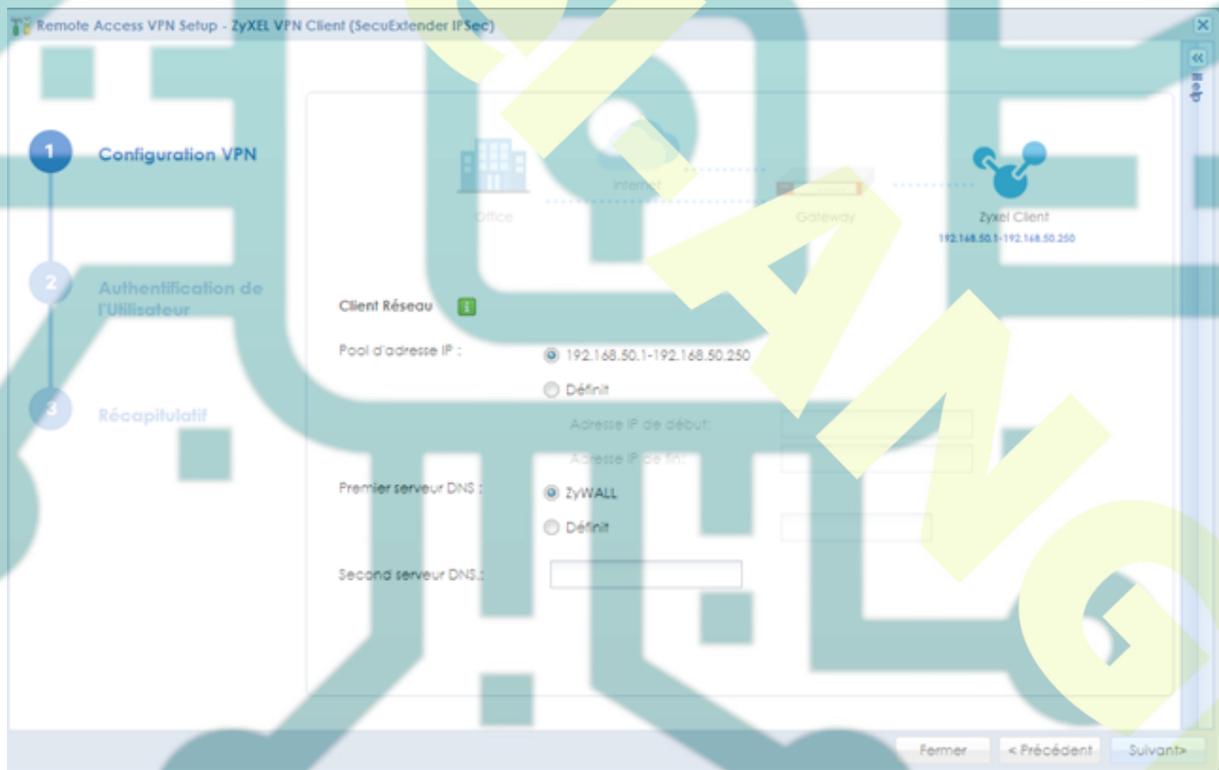
Choisir Zyxel VPN Client



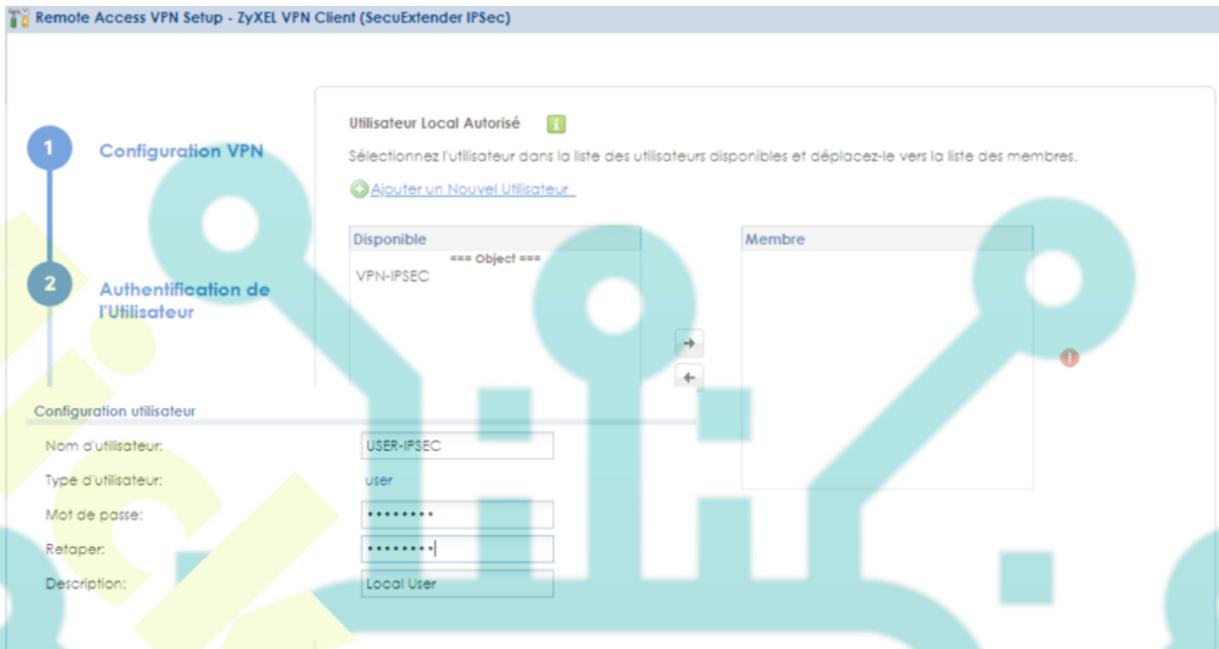
Paramétrer la clé partagée



Choisir le pool d'adresses utilisé pour le VPN



Créer un utilisateur



Autoriser cet utilisateur à utiliser le VPN



Configuration client VPN-IPSEC

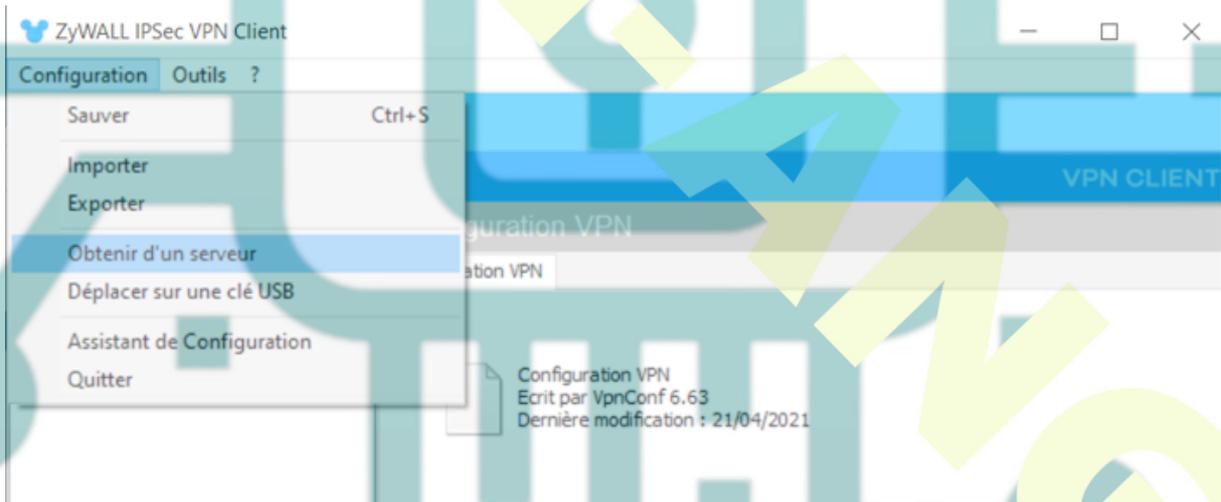
Télécharger le client sur le site de Zyxel

SecuExtender_IPSEC_VPN_Client_3.8.204.61.32

Lancer le client



Dans le menu Configuration, récupérer le provisionning du routeur



Choisir un compte utilisateur ayant droit

NB-vérifier que cet utilisateur est bien répertorié dans les règles du routeur

Assistant Serveur de Configuration VPN ×**Etape 1 : Authentification**Quels sont les paramètres de la connexion au Serveur ?  

Vous allez télécharger votre Configuration VPN depuis le Serveur de Configuration VPN.
Entrer ci-dessous les informations d'authentification requises pour la connexion au Serveur.

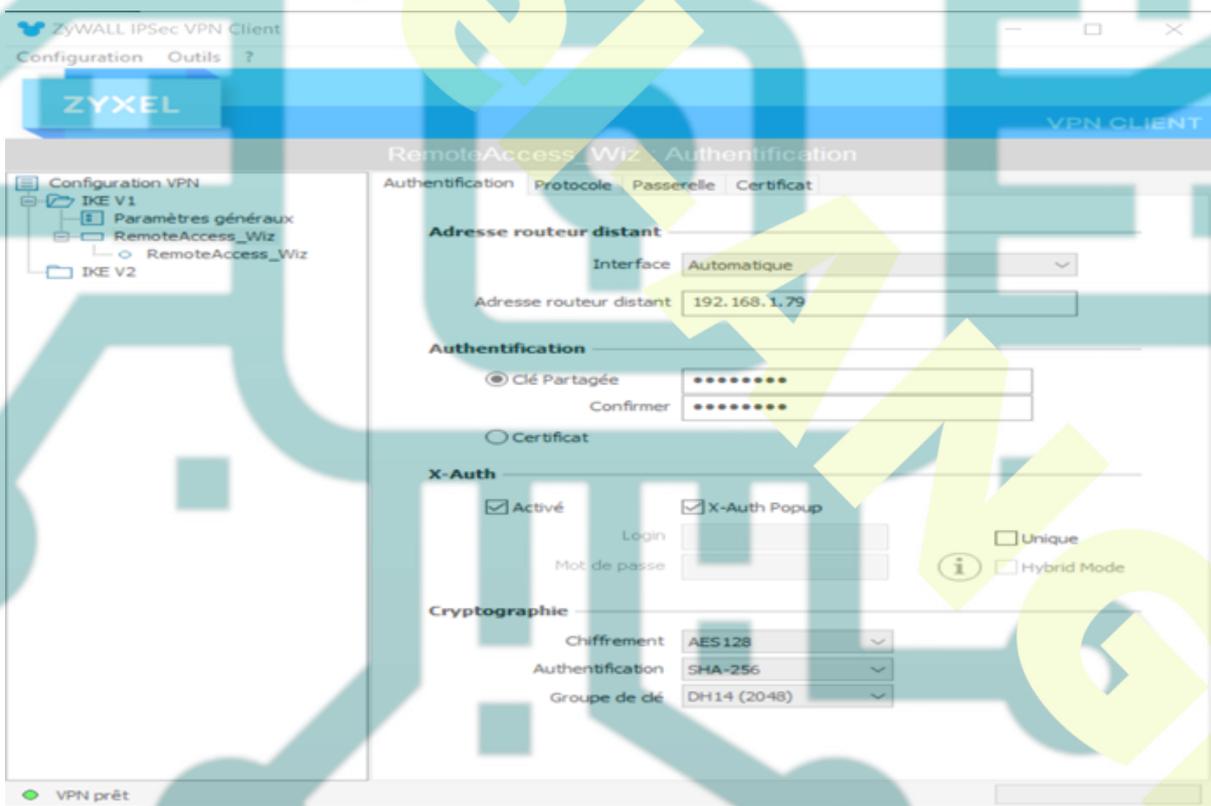
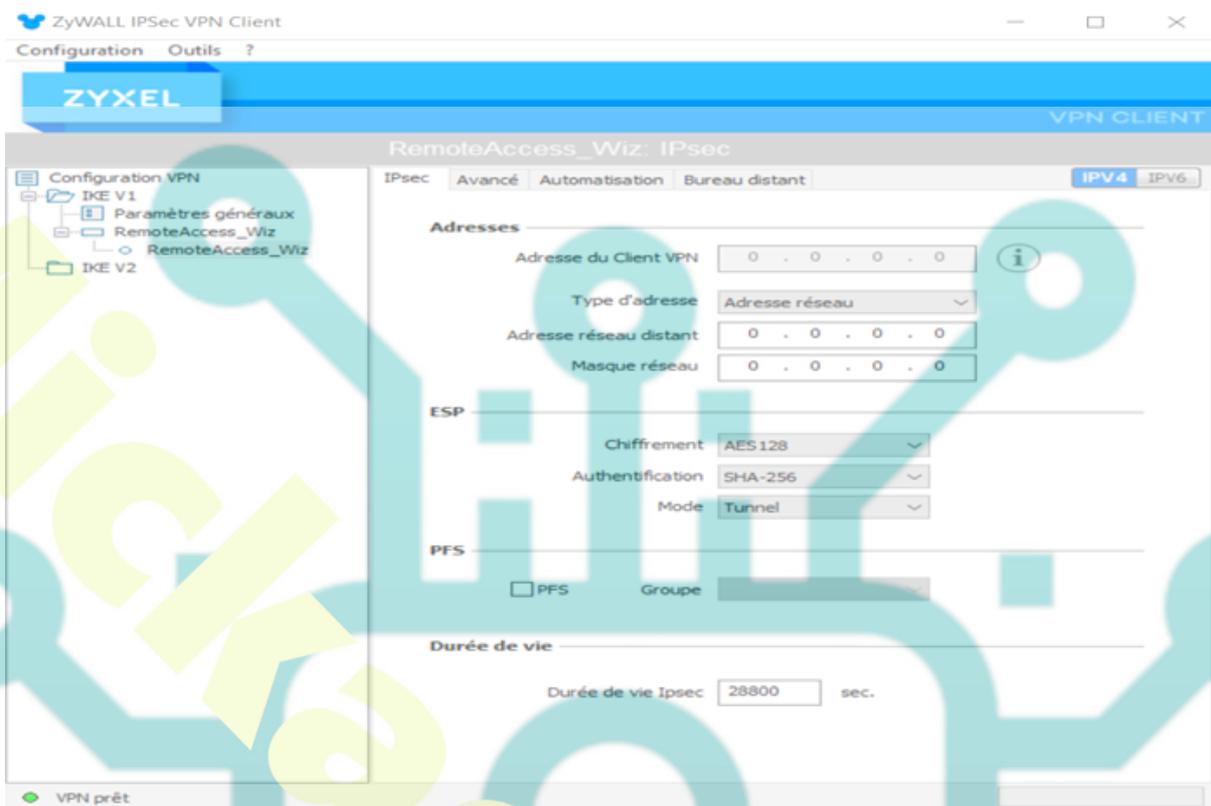
Adresse de la passerelle : Port : Authentification : Login : Mot de passe : Assistant Serveur de Configuration VPN ×**Etape 2 : En cours de traitement...**Récupération de la configuration VPN.  

Téléchargement de la configuration VPN depuis le serveur :



- Initialisation Ok.
- Init crx server (192.168.1.79) Ok.
- Envoi de la requête HTTP-S
 - Réception de la configuration...
 - Ecriture de la configuration VPN...
 - Application de la configuration...

Ouvrir la configuration du client



Se connecter au VPN



Sur le client, vérifier la configuration du VPN

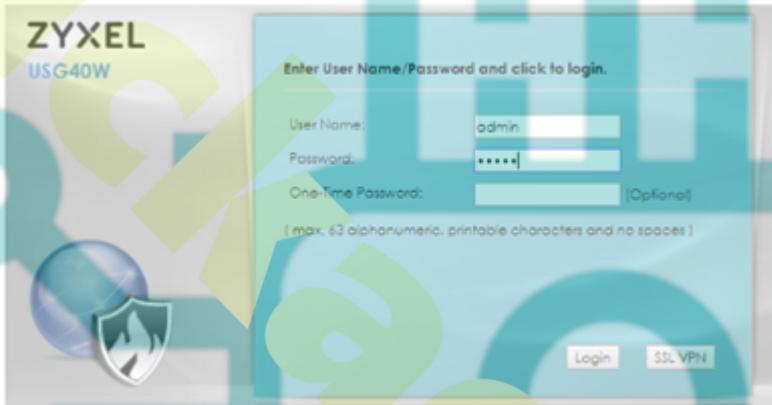
```
Carte Ethernet TGB RemoteAccess_Wiz-RemoteAccess_Wiz :  
Suffixe DNS propre à la connexion. . . . . :  
Adresse IPv6 de liaison locale. . . . . : fe80::95eb:2451:32de:84e%66  
Adresse IPv4. . . . . : 192.168.50.1  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 192.168.50.2
```

Faire un test de ping vers le réseau local

Configuration du VPN SSL

Etape 1

Connectez-vous à l'unité en saisissant son adresse IP et les informations d'identification d'un compte administrateur (par défaut, le nom d'utilisateur est «admin», le mot de passe est «1234»).



Etape 2

Allez dans **Configuration > VPN > VPN SSL**

Cliquez sur « Ajouter » et entrez le nom souhaité, laissez la zone sous «SSL_VPN» et déplacez les utilisateurs souhaités vers «Objets utilisateur / groupe sélectionnés» sur le côté droit. Cliquez sur **Créer un nouvel objet > Utilisateur / Groupe** pour ajouter un utilisateur si vous le souhaitez.

Edit Access Policy

Create new Object ▾

Configuration

Enable Policy

Name: Test_SSL

Zone: SSL_VPN

Description: New Create (Optional)

Clean browser cache when user logs out

User/Group

Selectable User/Group Objects
 === Object ===
 ldap-users
 radius-users
 ad-users
 test
 === Group ===

Selected User/Group Objects
 === Object ===
 admin
 VPN_USER

Etape 3

3 Faites défiler jusqu'à «**Extension réseau**» et cochez «**Activer l'extension réseau (Mode tunnel complet)**». Créez un nouvel objet adresse de type «RANGE». Choisissez cette plage plus tard comme Assign IP Pool

Assurez-vous de définir une plage qui ne soit pas en conflit avec un sous-réseau existant ou connu de votre USG

Network Extension (Optional)

Enable Network Extension (Full Tunnel Mode)

Force all client traffic to enter SSL VPN tunnel

Assign IP Pool: Test_SSL RANGE 192.168.100.10-192.168.100.100

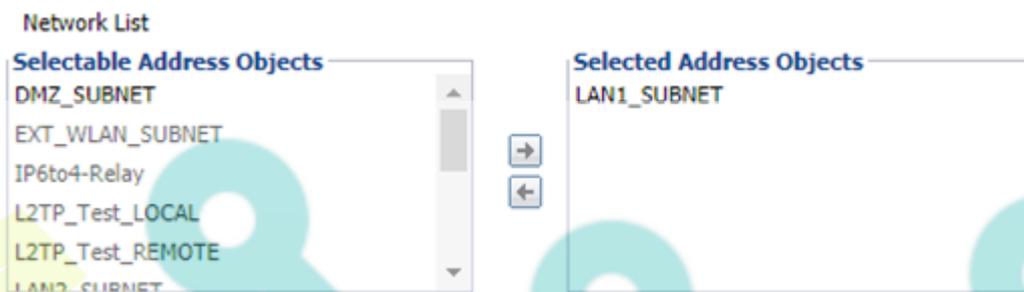
DNS Server 1: none

DNS Server 2: none

WINS Server 1: none

WINS Server 2: none

4 Sous «Liste du réseau», déplacez le réseau souhaité auquel vos clients VPN SSL doivent avoir accès, vers les «objets d'adresse sélectionnés» et cliquez sur «Appliquer».



Configuration du client SSL

Etape 1

Installer le logiciel client SecuExtender

Si nécessaire, vous devez installer Java pour utiliser ce service.

Etape 2

Lancer le logiciel, saisir l'adresse IP WAN du Zyxel, puis le compte utilisateur et le mot de passe.

Si SecuExtender dit que la connexion n'est pas sécurisée, cliquez sur OUI