et cifom

CPLN Ecole technique

07 Le VPN

Module 146

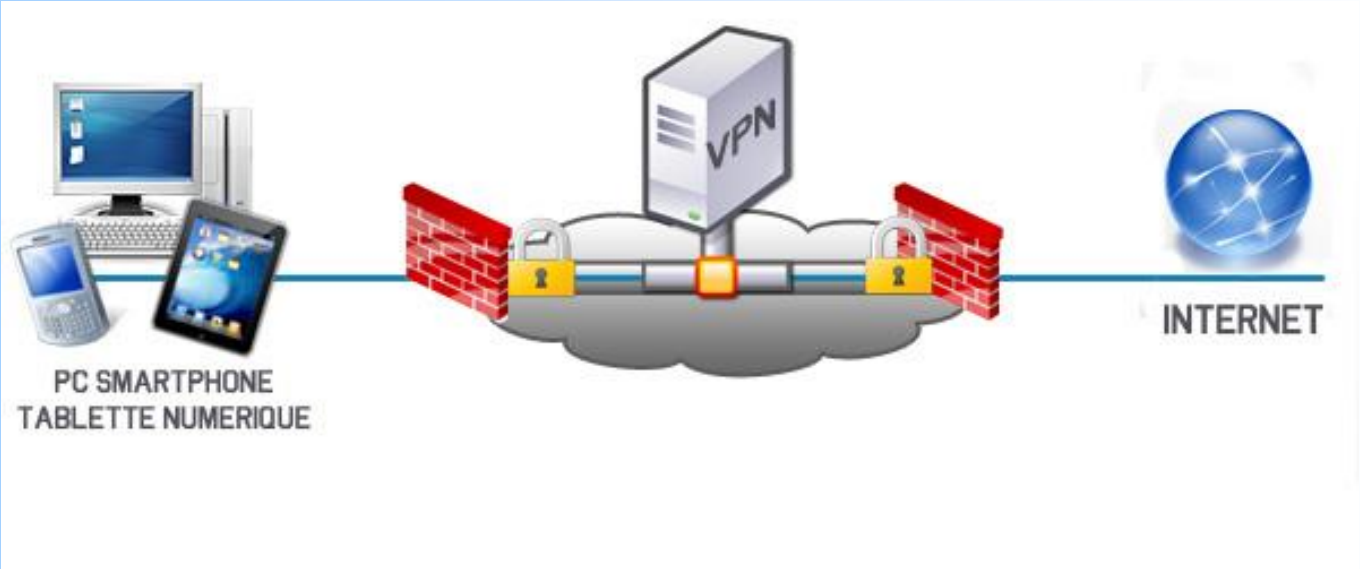
ICT Berufsbildung
Formation professionnelle
Formazione professionale

1. Introduction

Le VPN est un tunnel (ou une liaison virtuelle) sécurisé permettant la communication entre deux entités (Internet).

Cette technologie permet de créer une liaison virtuelle entre deux réseaux physiques distants de manière transparente pour les utilisateurs concernés.

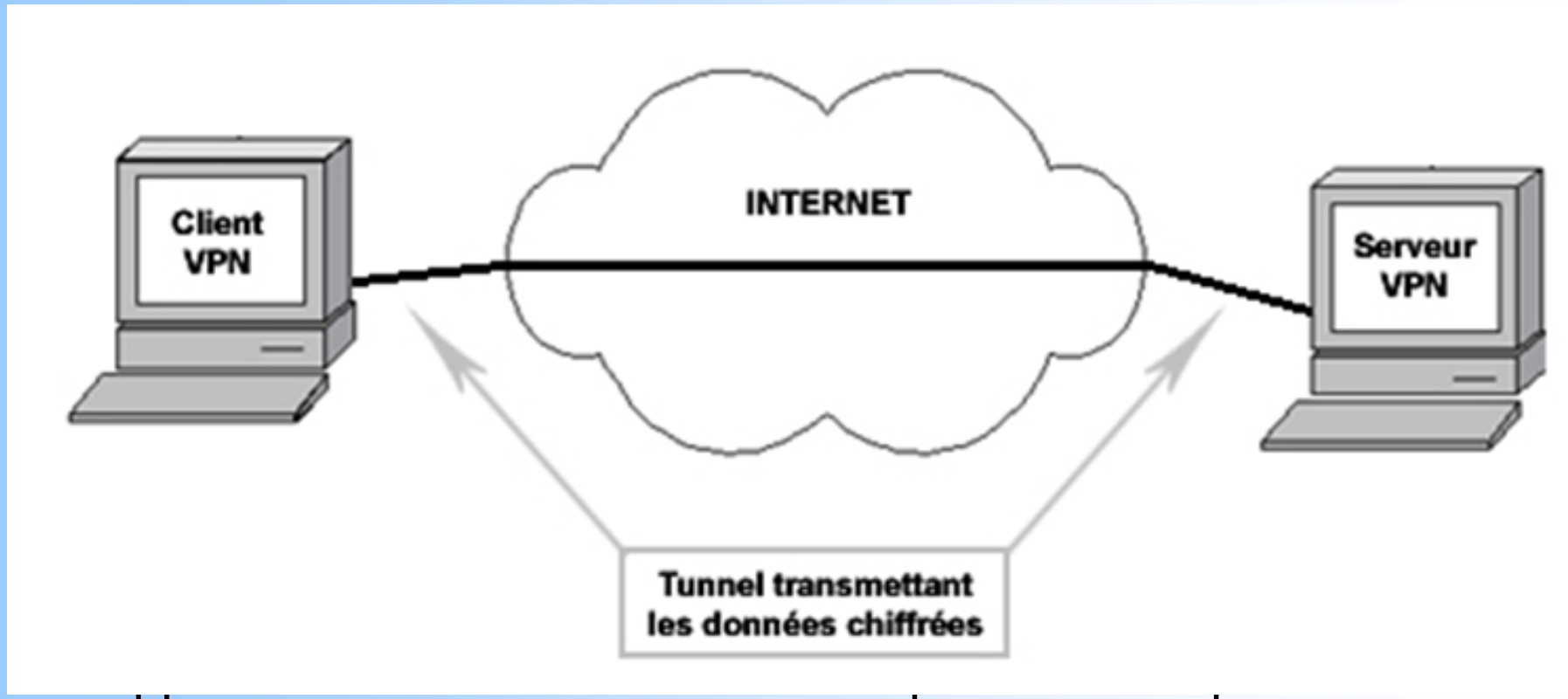
Les données envoyées au travers de ces liaisons virtuelles sont chiffrées, ceci garantit aux utilisateurs qu'en cas d'interception malveillante les données soient illisibles.



2. Fonctionnement

Comment fonctionne un réseau privé virtuel :

Un VPN repose sur un ou des protocoles, appelé protocoles de «tunnelisation» (tunneling).



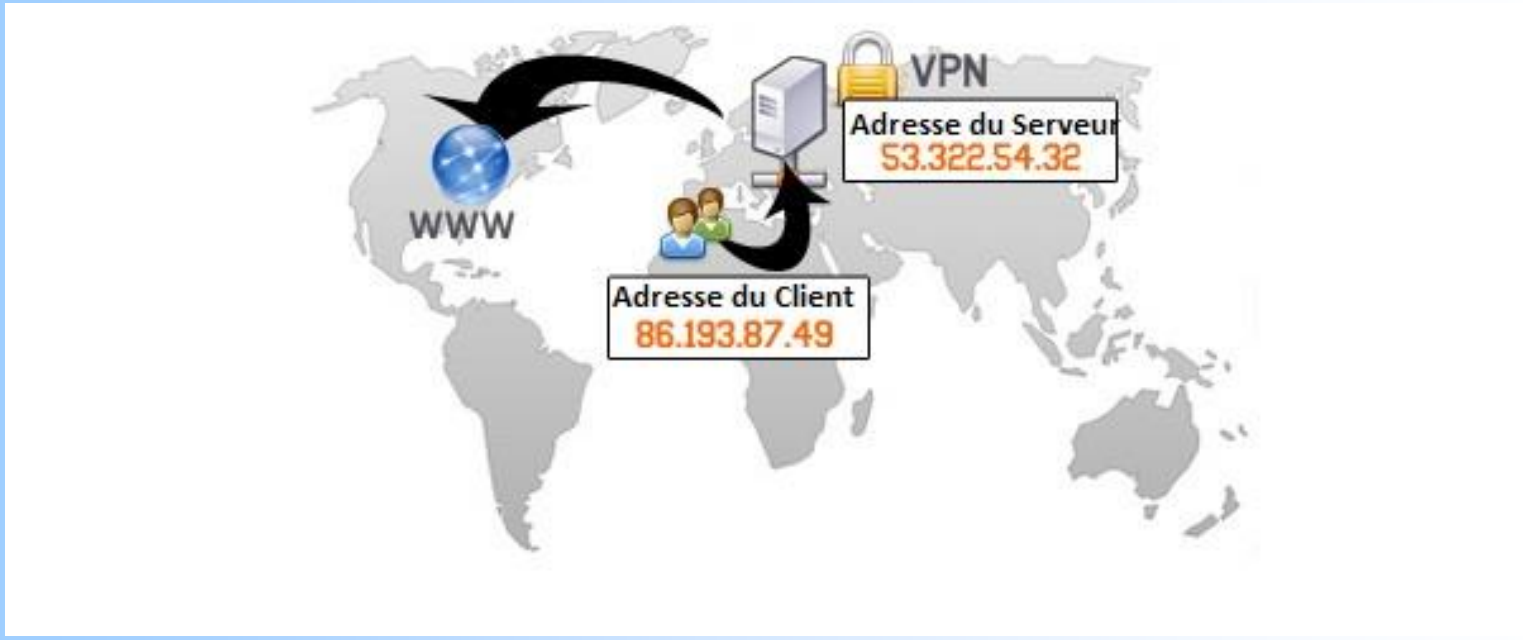
données du côté de l'organisation.

2. Fonctionnement

Dans les faits, nous établissons une connexion sécurisée avec le serveur qui nous propose le service VPN.

Ce serveur VPN nous connecte sur Internet en masquant notre adresse IP par son adresse IP.

Une communication VPN peut donc être de client à serveur mais il est à prendre en considération qu'elle peut aussi se faire de serveur à serveur.



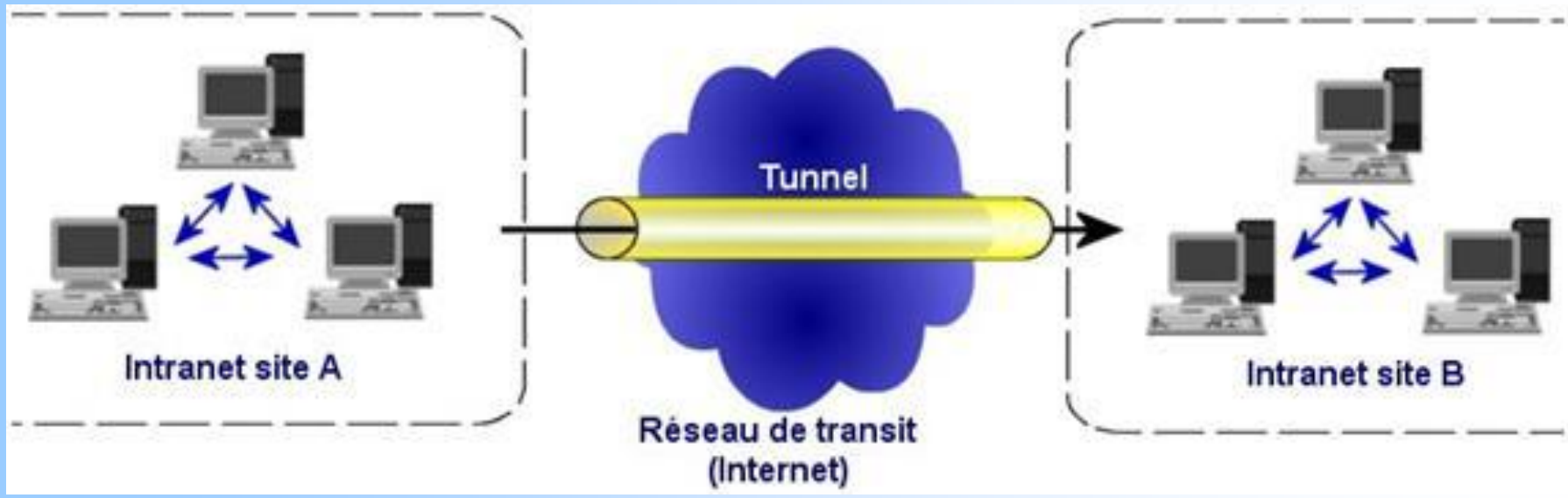
3. Divers types de VPN

Il existe d'autres types d'utilisation des VPN :

L'intranet VPN qui est utilisé pour relier deux intranets entre eux.

Ce type de VPN est utile pour les entreprises possédant plusieurs sites distants.

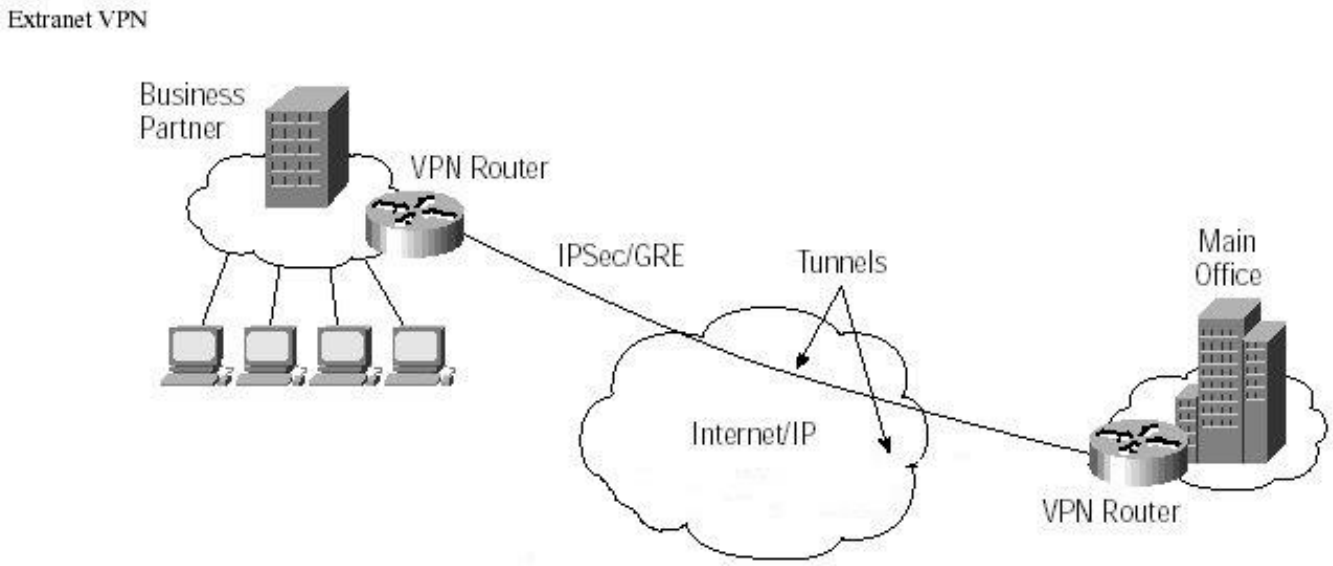
Le plus important avec ce type de VPN est de garantir la sécurité et l'intégrité des données.



3. Divers types de VPN

L'extranet VPN est utilisé par les entreprises, car elles peuvent utiliser ce type de VPN pour communiquer avec ses clients.

L'extranet VPN ouvre son réseau local à ses clients ou à ses partenaires.



4. Les principaux protocoles de tunnelisation

Les principaux protocoles utilisés sont :

L2F (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva.

A noter qu'il est désormais obsolète.

PPTP (Point-to-Point Tunneling Protocol) est aussi un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.

L2TP (Layer Two Tunneling Protocol) est protocole de niveau 2 s'appuyant sur PPP, et qui fait converger les fonctionnalités de PPTP et L2F.

4. Les principaux protocoles de tunnelisation

GRE (Generic Routing Encapsulation) est développé par Cisco, mais qui est souvent remplacé par L2TP.

IPSec est un protocole de niveau 3, issu des travaux de l' IETF (Internet Engineering Task Force), groupe participant à l'élaboration des standards Internet).

Il permet de transporter des données chiffrées pour les réseaux IP.

SSL (Secure Sockets Layer) offre une très bonne solution de tunnelisation.

L'avantage de cette solution est de permettre l'utilisation d'un navigateur Web comme client VPN.

On peut accéder à ce type de VPN avec un navigateur web via «https».

Il permet aux utilisateurs de mettre en place une connexion sécurisée au réseau depuis n'importe quel navigateur Web.

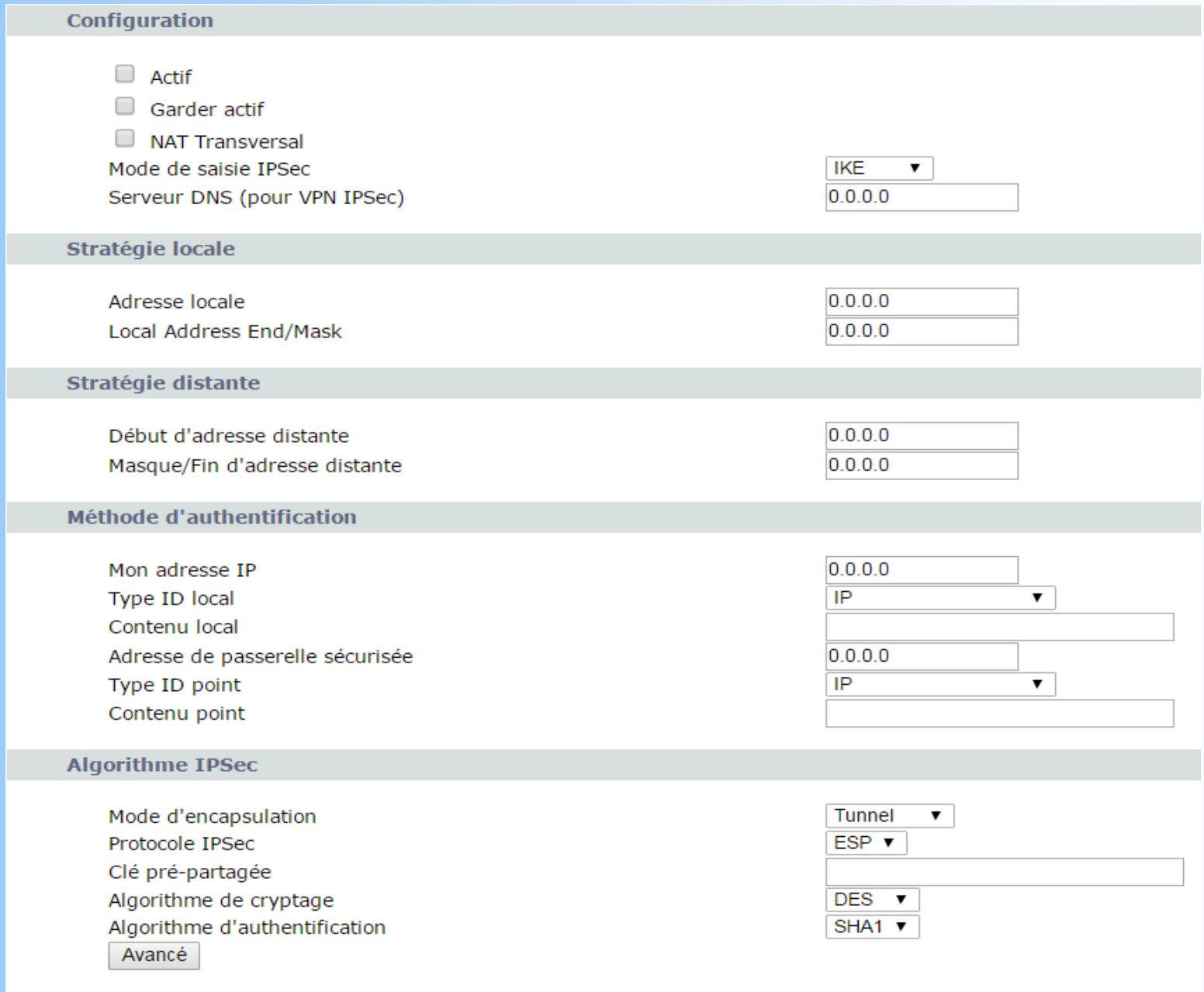
5. Le VPN avec le routeur Zyxel

Pour accéder au service VPN, allez dans …

Sécurité > VPN > configuration des règles

Pour configurer une règle, cliquez sur le bloc notes.

5. Le VPN avec le routeur Zyxel



5. Le VPN avec le routeur Zyxel

Quelques explications :

Actif : active la stratégie du VPN

NAT Transversal permet d'activer une connexion VPN quand il y a des routeurs entre les deux IpSec routeurs

IKE / Manuel : l'option **IKE** fournit plus de protection.

Manuel : Utilisé en cas de problème avec l'option **IKE**.

AH / ESP :

AH : Authentication Header, ce protocole permet d'assurer l'intégrité des données. Les algorithmes qui doivent être obligatoirement implémentés pour être conforme à la RFC sont SHA-1 et MD5.

5. Le VPN avec le routeur Zyxel

Quelques explications (suite) :

ESP : Encapsulating Security Payload, permet lui aussi d'assurer l'intégrité des données mais aussi leur confidentialité.

Pour l'authentification, un numéro de séquence est généré à partir de la clé secrète utilisée par les deux correspondants. Pour la confidentialité, l'implémentation de triple DES est obligatoire, mais d'autres techniques peuvent être utilisées comme DES, RC5, ou autres.

Avec le **NAT Transversal**, il faut utiliser **ESP** et non **AH**

DES / 3DES : Ce champ est applicable avec ESP dans le champ de Protocole IPSEC.

DES utilise une clé unique de 8 caractères.

3DES utilise une clé unique de 24 caractères.

5. Le VPN avec le routeur Zyxel

Quelques explications (Suite et fin) :

SHA1 / MD5 : Algorithmes de cryptage.

SHA1 est plus élevé que **MD5**, mais plus lent.