



**TOPNET**  
*Fournisseur de Services Internet*

**LES DOMAINES D'APPLICATIONS DES TECHNOLOGIES VPN :**

**Interconnexion de réseaux à faible coût et  
à fort niveau de sécurité**

**AUTEUR : BOUBAKER NOBEL EL HOSSINE**

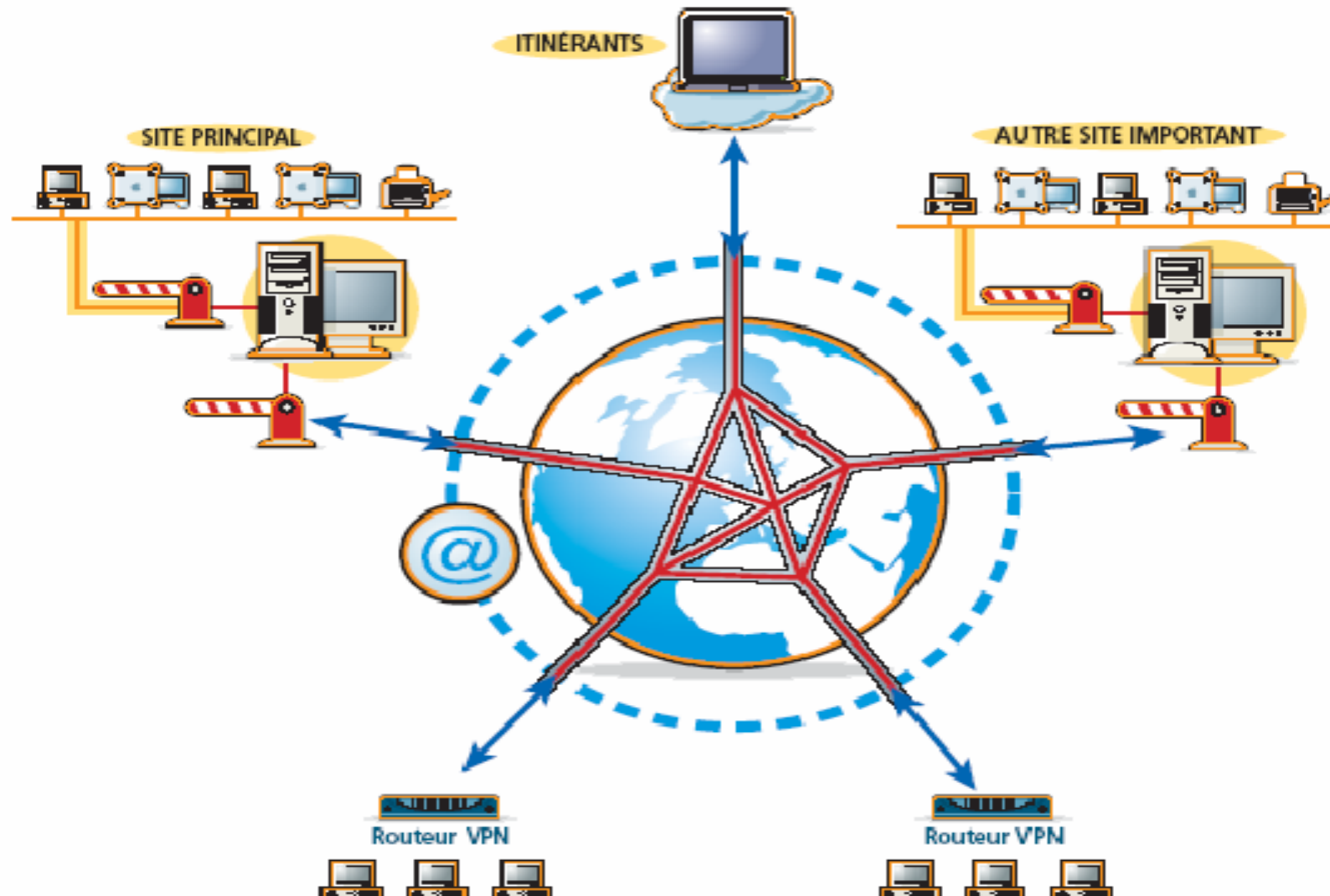
# Interconnexion de réseaux à faible coût et à fort niveau de sécurité : VPN

- **Qu'est ce que le VPN ?**
- **Quelle Sécurité pour le VPN ?**
- **Quel Coût pour le VPN ?**
- **Quel futur pour le VPN ?**

# Qu'est ce que Le VPN ?

- Le **VPN** est l'abréviation pour **Virtual Private Network** : Un **Réseau Privé Virtuel** (RPV),
- C'est une solution technique permettant à une entreprise de **connecter à distance** et en toute **sécurité**, les **réseaux informatiques** de ses différents établissements, filiales et éventuellement, ses collaborateurs nomades géographiquement éloignées via **Internet** .

# Qu'est ce que Le VPN ?

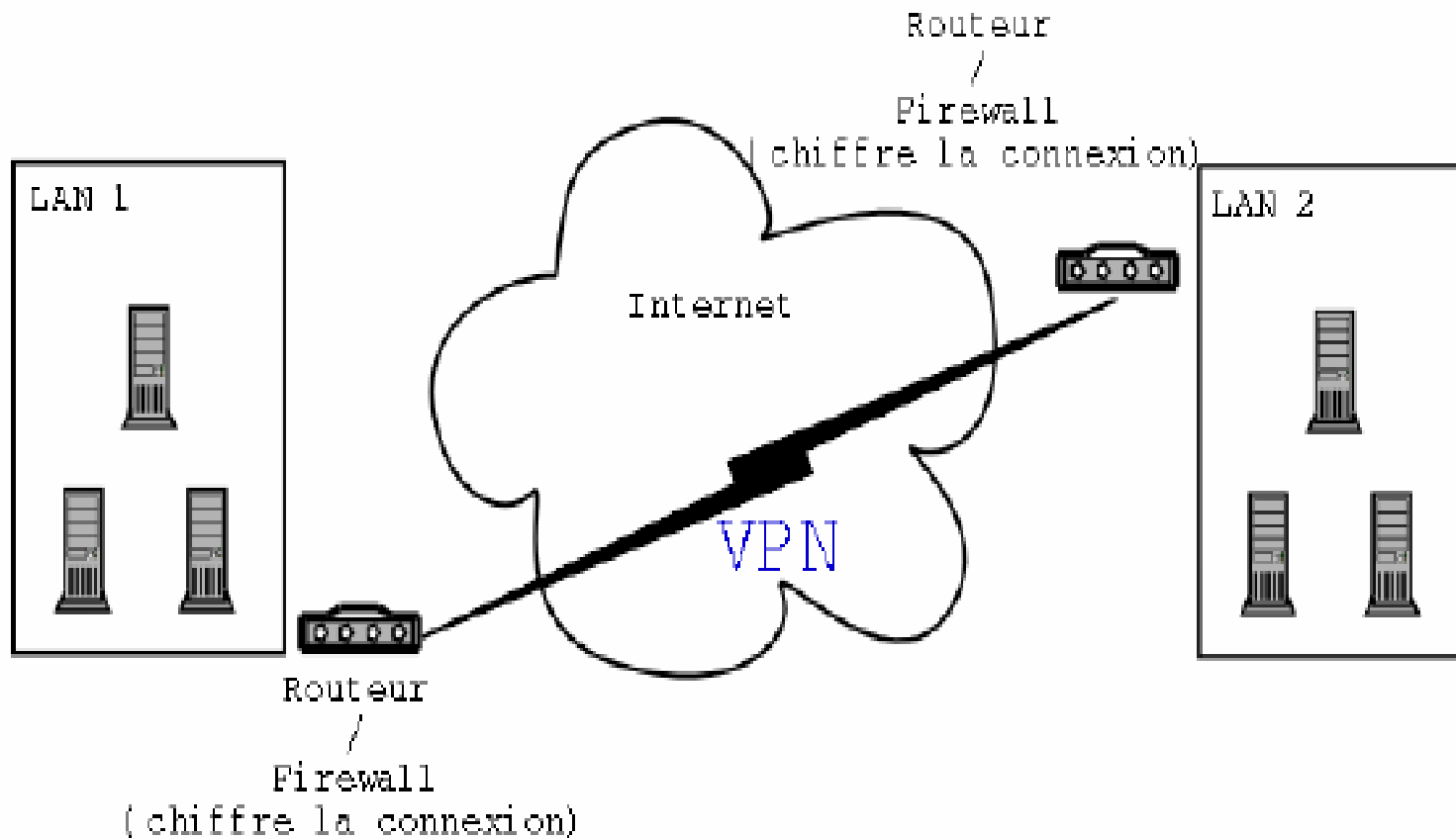


# Qu'est ce que Le VPN ?

- Un poste connecté par VPN est considéré comme faisant partie du **réseau interne** de l'entreprise et peut ainsi utiliser **sans restriction** toutes les ressources informatiques de l'**Intranet**.  
Indépendamment du Système :

- ❖ Windows
- ❖ MAC OSX
- ❖ Linux-Solaris

# Qu'est ce que Le VPN ?



# Quelle Sécurité pour le VPN ?

- Échange d'informations entre réseaux local
- Accès distant au réseaux local
- Informations internes qui circulent
- Informations stratégiques

A travers quoi ?

INTERNET ???? Donc quelle sécurité .....

# Quelle Sécurité pour le VPN ?

## Principe:

Établir un tunnel sécurisé site à site ou site à client distant via un réseau de transit.

## Méthodes :

- Tunneling
- Authentification
- Chiffrement
- Contrôle de l'intégrité des données



# Quelle Sécurité pour le VPN ?

## Tunneling :

L'établissement d'une connexion VPN consiste tout d'abord à encapsuler vos données de telle manière à créer un tunnel entre les deux extrémités de votre liaison. L'encapsulation affecte un en-tête aux données privées pour pouvoir traverser le réseau de transit.

Cette méthode permet le transport d'un protocole à l'intérieur d'un autre protocole.

# Quelle Sécurité pour le VPN ?

## Authentification :

Afin de sécuriser l'accès au tunnel préalablement établi plusieurs niveaux d'authentifications pourront être utilisés:

- Authentification des utilisateurs en mode client / serveur
- Authentification mutuelle des machines par échange d'identité
- Authentification des paquets combinée au contrôle d'intégrité des données l'intérieur d'un autre protocole.

# Quelle Sécurité pour le VPN ?

## Chiffrement:

Application d'un algorithme cryptographique aux données privées afin d'obtenir un texte chiffré souvent appelé «Ciphertexte».

Il existe deux types de chiffrement :

- Chiffrement symétrique utilisé par les algorithmes DES
- Chiffrement asymétrique ou par clé publique (PKI) pouvant inclure des signatures numériques RSA RC4 .

# Quelle Sécurité pour le VPN ?

## Contrôle de l'intégrité des données :

Service de sécurité qui consiste à permettre la détection de l'altération des Données durant le transfert. On distingue deux types d'intégrité:

- **L'intégrité en mode non connecté** permet de détecter de modifications d'un datagramme individuel mais pas sur l'ordre du datagramme.

- **L'intégrité en mode connecté** permet en plus de détecter la perte de paquets ou leur réordonnancement.

Ce service est très lié à l'authentification de l'origine des données et sont souvent fournis conjointement.

# Quelle Sécurité pour le VPN ?

**Le déploiement d'un VPN implique la prise en compte de plusieurs éléments:**

- Intégration dans la politique de sécurité en place dans l'entreprise
- Type de Connexion : site à site / via passerelle / logiciel client
- Choix du protocole et de l'authentification Interopérabilité des matériels de communication
- Adresses publiques fixes pour le sites VPN
- Affectation des adresses dynamiques
- Prise en charge multiprotocole
- Nombre de tunnels à ouvrir
- Translation d'adresse
- Administration et contrôle des accès VPN

# Quel Coût pour le VPN ?

**Le Coût d'un VPN est un avantage pour différentes raisons:**

- Pas de liaisons physiques comme les LAN
- Pas de point d'accès Comme les Wireless
- Les différents LAN d'une VPN sont connectés sur Internet mais selon le cas de l'entreprise et de sa taille : ADSL, LS, RTC, RNIS = Donc pas de problème de Budgétisation
- Passage de l'entreprise à une phase de gestion dynamique, collaborative et en temps réel : Donc plus fiable et constructive.

# Quel futur pour le VPN ?

Une étude du cabinet Frost et Sullivan estime ainsi que le CA des solutions VPN basées sur IP devrait passer de 658 M\$ en 1999 à 14,5 Md\$ en 2006 sur le seul marché EMEA (Europe, Moyen-Orient et Afrique).

«Les dernières prévisions annoncent une croissance moins forte que prévu pour 2001. Ce sont les RPV qui désormais font l'objet des spéculations les plus fortes : un marché de 32 milliards de dollars en 2003»

selon Infonetics Research. Dans la même étude Infonetics Research prévoit une croissance de 606% des dépenses liées au VPN dans le monde entier

**Merci**  
**pour votre Lecture**



# Pour Plus d'informations ?

**TUNIS** : Immeuble Pacha Centre, Bloc A, 6ème étage, 81 avenue Kheireddine Pacha 1073  
Tunis

**Tél** : 71 950 415 - **Fax** : 71 951 031

**SOUSSE** : 22, Immeuble Gloulou, Boulevard Mohamed Mâarouf 4000 Sousse

**Tél** : 73 215 355 - **Fax** : 73 215 356

**Site Web** : [www.topnet.tn](http://www.topnet.tn)

**Adresse email** : [commercial@topnet.tn](mailto:commercial@topnet.tn)