

**INTERCONNEXIONS DE SITES DISTANTS
(VPN)
SÉCURITÉ & PROTOCOLES**

SOMMAIRE

**1. LES DIFFÉRENTS BESOINS
EN RÉSEAUX PRIVÉS VIRTUELS**

**2. LES 2 PRINCIPAUX PROTOCOLES
DE TUNNELISATION**

**3. QUEL BESOIN EN RÉSEAU PRIVÉ VIRTUEL ?
QUEL PROTOCOLE DE TUNNELISATION ?**

1. LES DIFFÉRENTS BESOINS EN RÉSEAUX PRIVÉS VIRTUELS

1. UTILISATEUR NOMADE

(à partir d'un laptop à l'hôtel, dans un aéroport)

ont un accès aux ressources du réseau de l'entreprise)

C'est la cas d'un réseau privé virtuel à accès commuté

ou « VDPN » pour Virtual Dial-up Private Networking

2. TUNNEL SÉCURISÉ DE 2 SITES DISTANTS

**liaison au moyen d'un tunnel sécurisé
de deux sites distants**

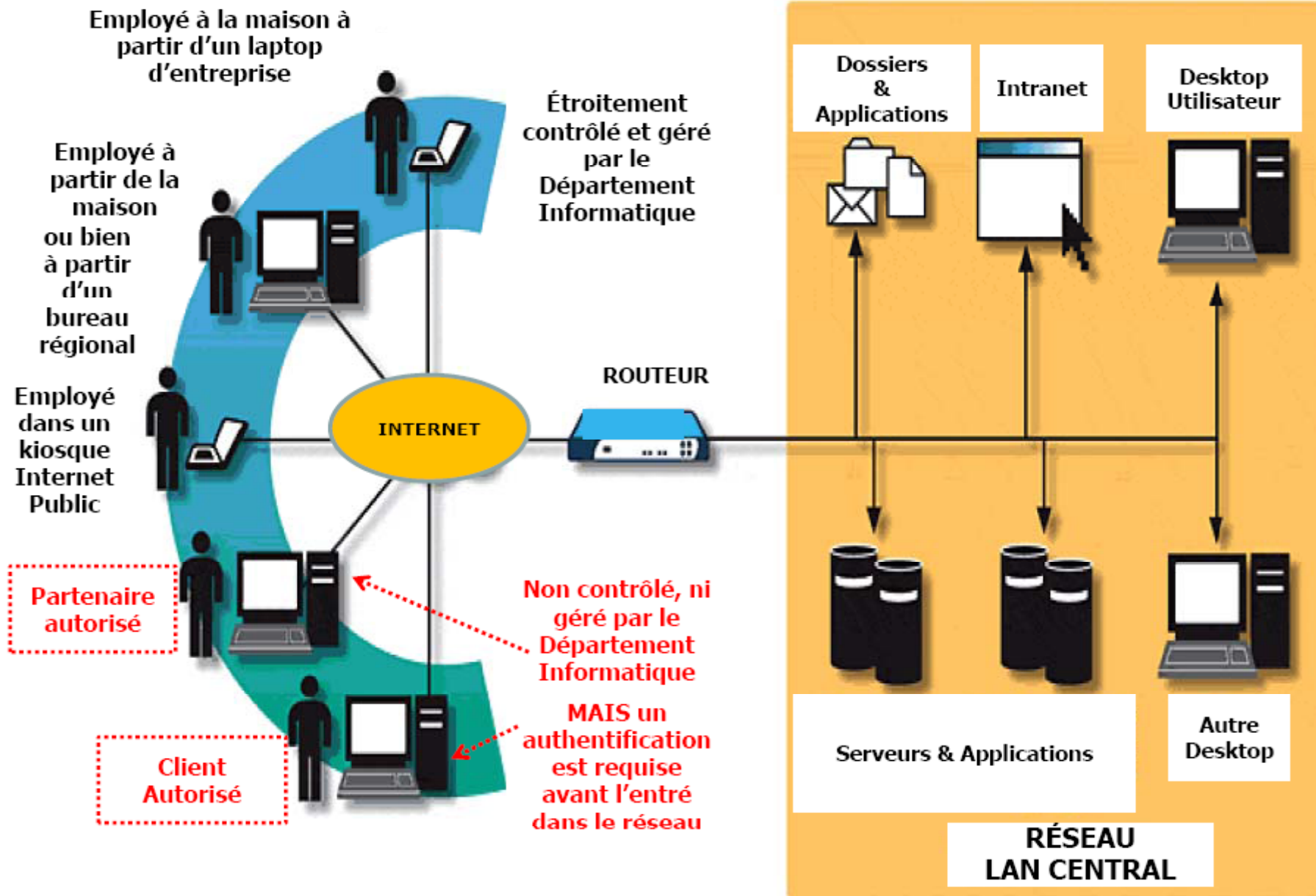
3. EXTRANET GLOBAL

permettant à un ensemble de sites distants

de communiquer via un réseau virtuel

auxquels ils sont raccordés

LES DIFFÉRENTS BESOINS EN RÉSEAUX PRIVÉS VIRTUELS



2. LES 3 PRINCIPAUX PROTOCOLES DE TUNNELISATION

Le principe de la tunnelisation

L'artifice utilisé = un protocole
d' « encapsulation »
("tunneling",
ou « tunnelisation »)

... encapsulant de façon
chiffrée les données à
transmettre

Le réseau est PRIVÉ ...

... seuls les ordinateurs des
sous-réseaux d'entreprise

...de part et d'autre du VPN ...

... de part et d'autre du VPN
peuvent "voir" les données ...

1. PPTP ou POINT TO POINT TUNNELING PROTOCOL

Transport des données :

ASSURÉ

Flux de contrôle du tunnel :

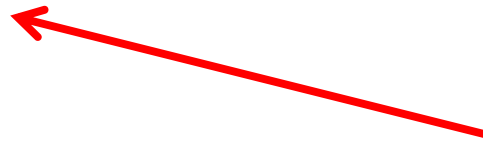
ASSURÉ

Chiffrement des données véhiculées :

ASSURÉ

Contrôle d'intégrité des paquets de données envoyés :

PPTP N'OFFRE AUCUN MÉCANISME



2. IPSEC ou IP SECURITY

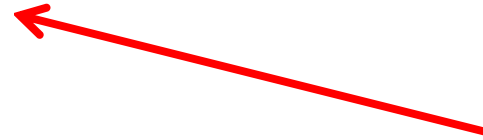
En un mot :

Le protocole IPSEC permet

le transport de paquets IP au dessus du protocole IP

de la manière la plus sûre

et la plus efficace qui soit.



IPSEC ou IP SECURITY

Le mode tunnel :

permet la liaison de deux réseaux distants

Le mode transport :

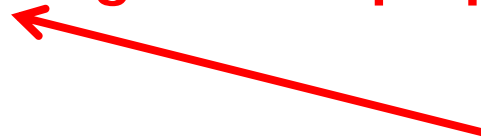
permet à deux hôtes de communiquer directement

Le protocole ISAKMP :

assure l'authentification sécurisée par mot de passe, par clé publique

Le protocole AH :

permet de contrôler l'intégrité des paquets IP complets réalisant le tunnel



**3. QUEL BESOIN EN RÉSEAU PRIVÉ VIRTUEL ?
QUEL PROTOCOLE DE TUNNELISATION ?**

1. POUR LE CAS DE L'UTILISATEUR NOMADE

PPTP ou Point to Point Tunneling Protocol ←

Microsoft offre le support PPTP en standard sur ses systèmes d'exploitation depuis Windows 98.

L'accès est totalement transparent.....

tant pour le client nomade.....

.... que pour le réseau auquel il se connecte

2. POUR LE CAS DU TUNNEL SÉCURISÉ DE 2 SITES DISTANTS

IPSEC ou IP Security ←

Le niveau de sécurité très élevé :

authentification

chiffrement

intégrité

renouvellement périodique des clés

3. POUR LE CAS DE L'EXTRANET GLOBAL

IPSEC ou IP Security ←

MAIS

La mise en œuvre n'est pas chose simple

Elle demande des procédés compliqués



CONTACT



DKB Solutions

Mr. Bertin DJAHA – Directeur Général

Siège : Abidjan – Cocody Riviera 3

En Face de l'Eglise Sainte Famille

Complexe Améthyste - Pavillon Cristal

Adresse: 17 B.P. 519 Abidjan 17

Tél : (225) 22 47 00 50, Fax : (225) 22 47 04 75

Hotline 24h/24 : (225) 07 84 46 95

Email: bertin.djaha@dkbsolutions.com



CONTACT



DKB Solutions

Mr. Guy AOUSOU – Marketing Manager

Hotline 24h/24 : (225) 07 18 07 88

Email: guy.aoussou@dkbsolutions.com



MERCI DE VOTRE ATTENTION
