cpmb
centre professionnel
des métiers du bâtiment

VPN

cpmb
centre professionnel
des métiers du bâtiment

OBJECTIFS

- La sécurité en 3 points
- Définir les rôles du VPN
- Identifier les types de VPN
- Configuration d'un VPN

cpmb
centre professionnel
des métiers du bâtiment

LES POINTS ESSENTIELS EN SÉCURITÉ

- **Authentification**
  Identification des paires actifs dans l'établissement du réseau virtuel
- **Intégrité**
  Certification que les données n'ont pas été altérées par des tiers lors du transport de l'information
- **Confidentialité**
  Chiffrement des données pour assurées que les données ne pourront être interprétées

cpmb
centre professionnel
des métiers du bâtiment

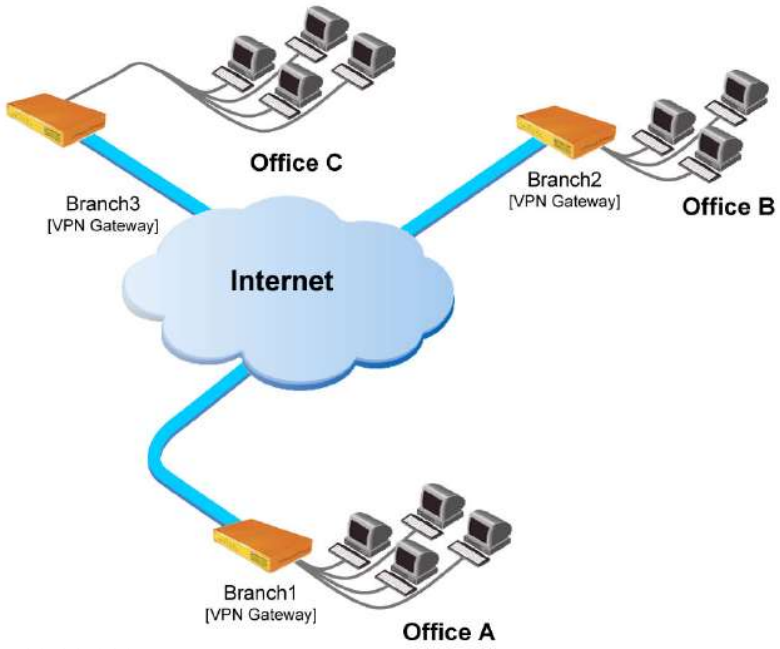
DÉFINITIONS ET PRINCIPES DE BASE

VPN est l'abréviation de Virtual Private Network

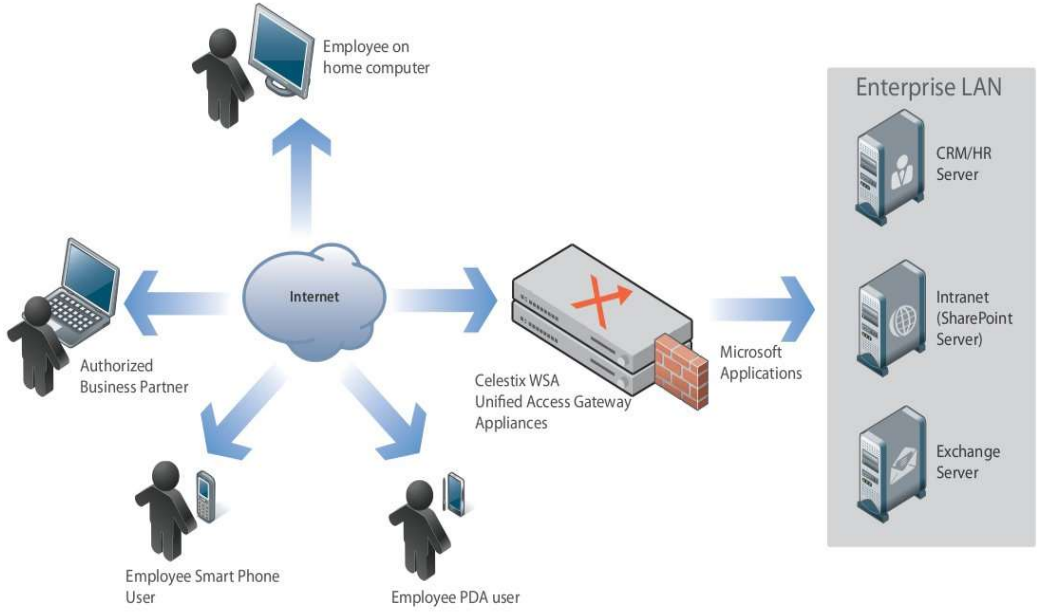
- Établissement d'une liaison sécurisée dans un environnement public mutualisé pour la transmission sécurisée des données, de la voix, …
- Sécurisation des données implique
  - Identification des participants de la transmission
  - Confidentialité de la transmission
- Les solutions VPN se basent sur un ensemble de protocoles de transport, d'authentification et de chiffrement des données

TYPES DE VPN

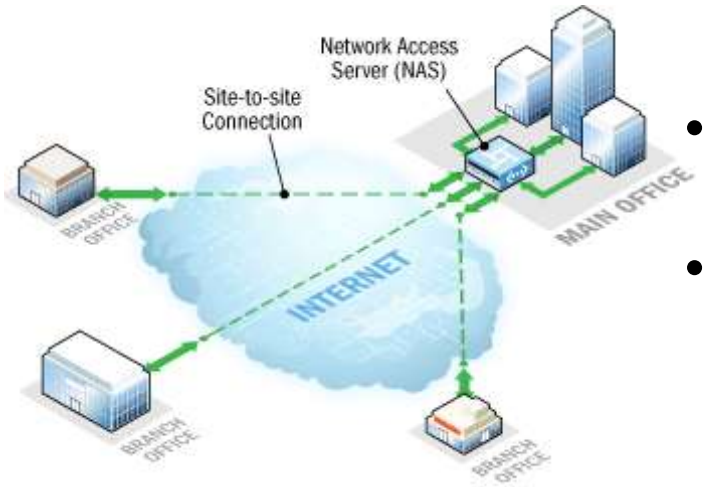
Site à site



Utilisateur nomade à site



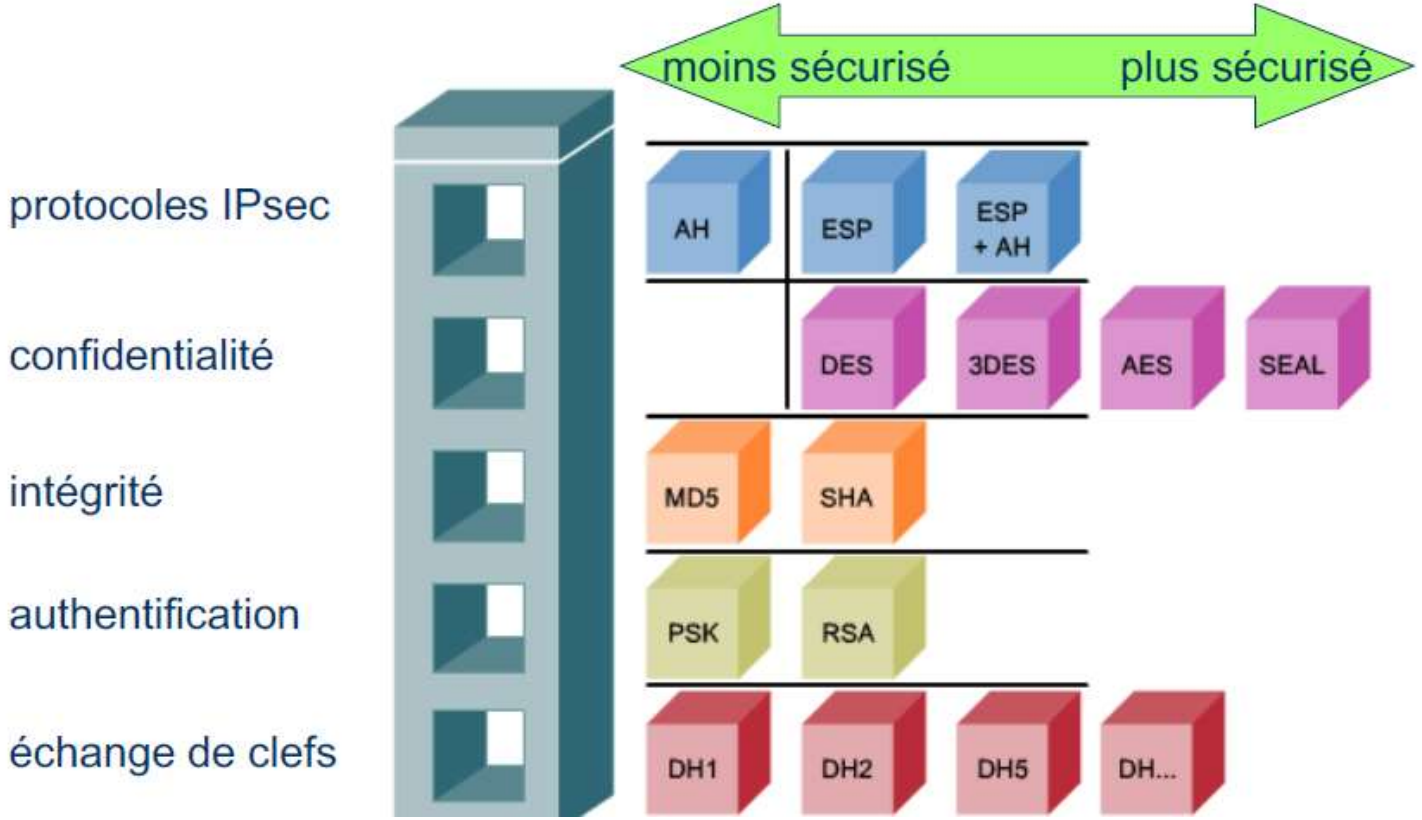
VPN SITE À SITE



- Permet de mettre en relation 2 ou plusieurs réseaux IP privés
- Une sonde sur le réseau Internet ne peut ‘voir’ que des paquets transmis entre les routeurs
- L’établissement et la transmission des données sont basée sur IPsec (Internet Protocol Security) qui est un ensemble de protocoles
  - IKE qui négocie l’authentification des participants et la manière de protéger les données
  - IPSec (protocoles) qui achemine les données entre les participants

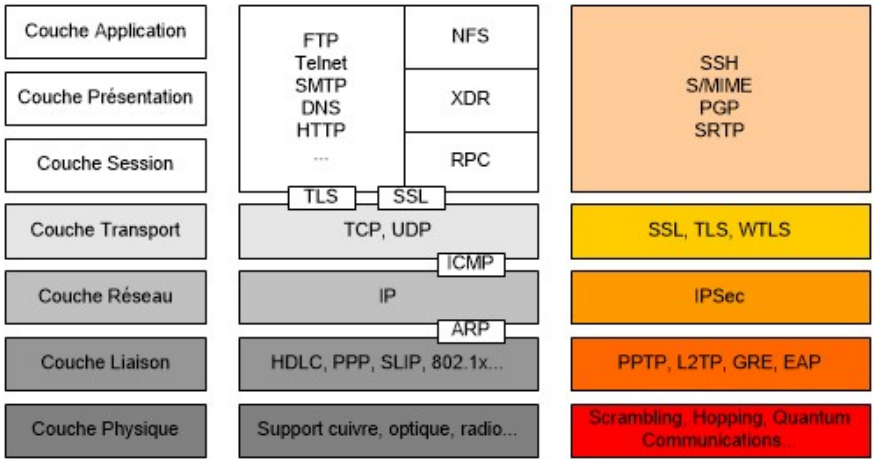
cpmb
centre professionnel
des métiers du bâtiment

CADRE GÉNÉRAL D'UN VPN IPSEC



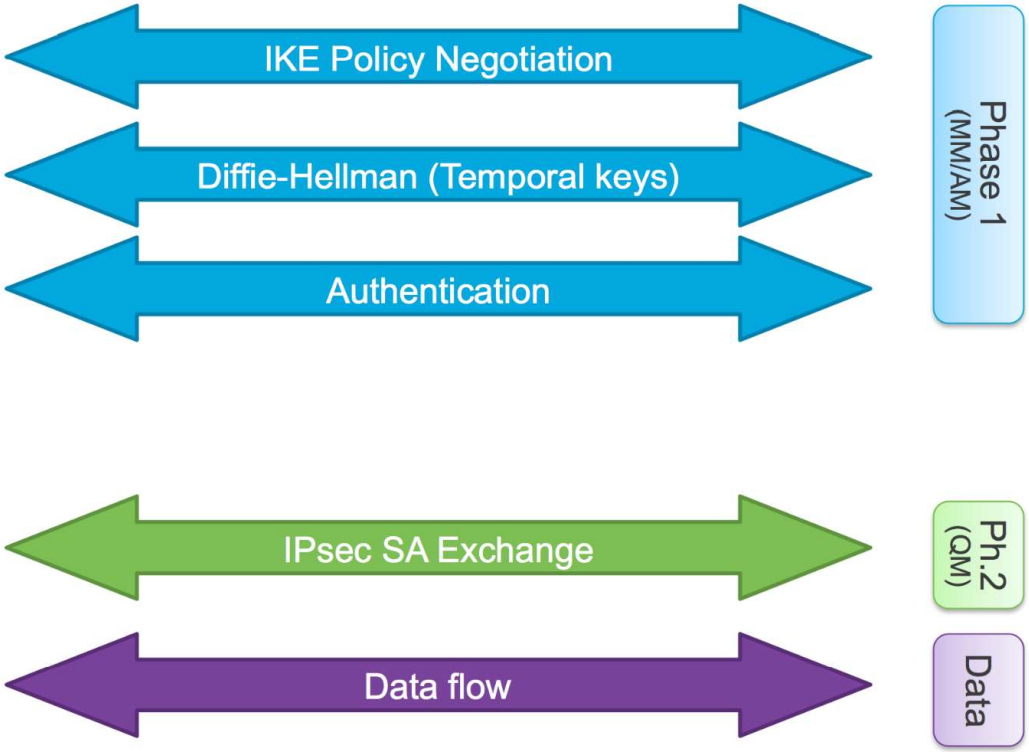
cpmb
centre professionnel
des métiers du bâtiment

CADRE GÉNÉRAL D'UN VPN IPSEC



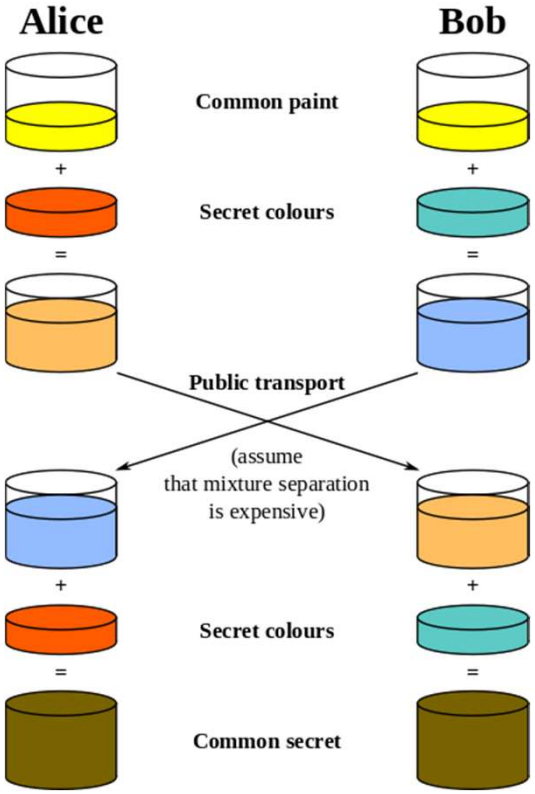
cpmb
centre professionnel
des métiers du bâtiment

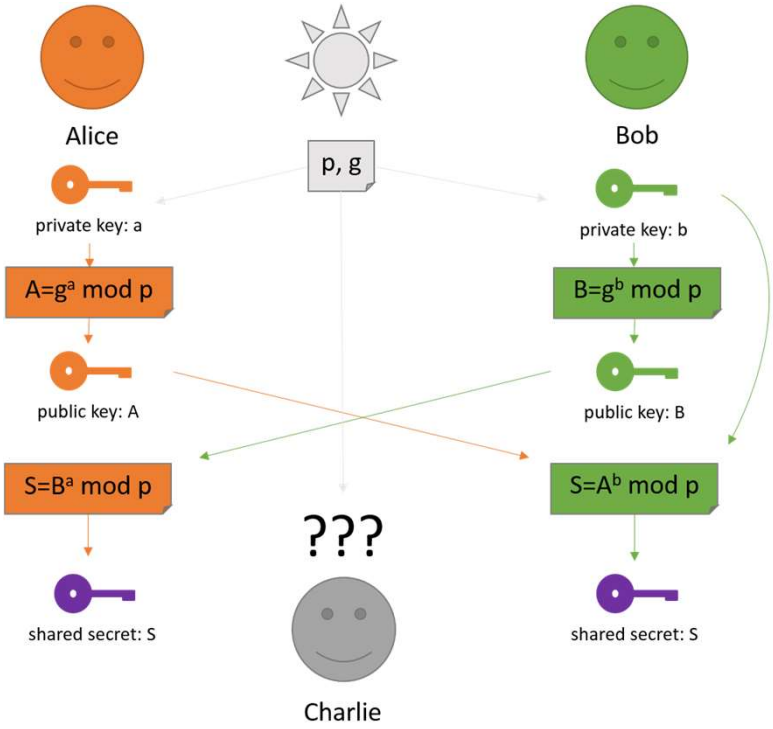
SCHÉMA DE MISE EN PLACE IPSEC



cpmb
centre professionnel
des métiers du bâtiment

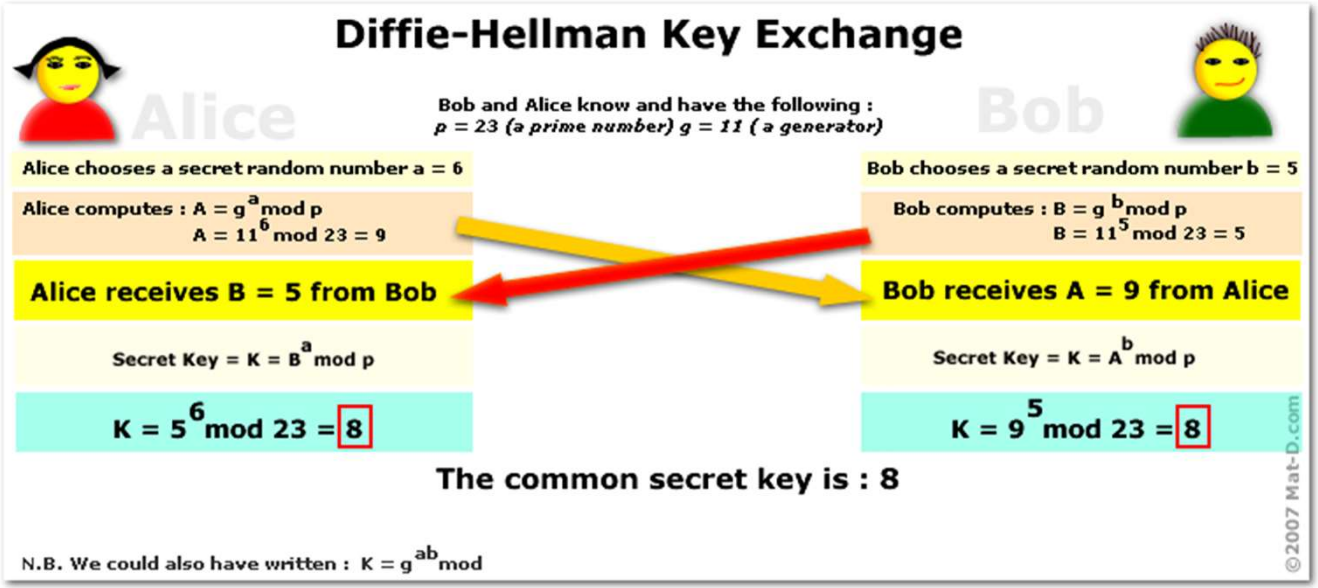
PRINCIPE DIFFIE-HELLMAN





cpmb
centre professionnel
des métiers du bâtiment

PRINCIPE DIFFIE-HELLMAN



cpmb
centre professionnel
des métiers du bâtiment

PRINCIPE DIFFIE-HELLMAN

Diffie-Hellman (DH) allows two devices to establish a shared secret over an unsecure network. In terms of VPN it is used in the in IKE or Phase1 part of setting up the VPN tunnel.
There are multiple Diffie-Hellman Groups that can be configured in an IKEv2 policy on a Cisco ASA running 9.1(3). In Nov 2016 ASA 9.6(x) is available and there are no new changes to the DH Groups.

Diffie-Hellman group 1 - 768 bit modulus - AVOID
Diffie-Hellman group 2 - 1024 bit modulus - AVOID
Diffie-Hellman group 5 - 1536 bit modulus - AVOID
Diffie-Hellman group 14 - 2048 bit modulus – MINIMUM ACCEPTABLE
Diffie-Hellman group 19 - 256 bit elliptic curve – ACCEPTABLE
Diffie-Hellman group 20 - 384 bit elliptic curve – Next Generation Encryption
Diffie-Hellman group 21 - 521 bit elliptic curve – Next Generation Encryption
Diffie-Hellman group 24 - modular exponentiation group with a 2048-bit modulus and 256-bit prime order subgroup – Next Generation Encryption

Algorithms marked as AVOID do not provide an adequate security level against modern threats and should not be used to protect sensitive information. It is recommended that these algorithms be replaced with stronger algorithms.
Next Generation Encryption (NGE) is expected to meet the security and scalability requirements of the next two decades.
If you are using encryption or authentication algorithms with a 128-bit key, use Diffie-Hellman groups 5, 14, 19, 20 or 24. If you are using encryption or authentication algorithms with a 256-bit key or higher, use Diffie-Hellman group 21 or 24.

cpmb
centre professionnel
des métiers du bâtiment

ETABLISSEMENT D'UN TUNNEL VPN

Phase 1 – authentification mutuelle

a) Négociation du chiffrement, de la fonction de hachage, méthode d'authentification et méthode d'échange de clés Diffie-Hellman (paramètres IKE)
b) Établissement du secret partagé en utilisant la méthode Diffie-Hellman convenue; du secret partagés seront dérivées les clés pour le chiffrement et le hachage négociés
c) Authentification mutuelle des participants en utilisant les méthodes et clés négociées dans les 2 premières phases

Le secret partagé est en général

Des certificats auto générés ou authentiques

Une clé partagée (ex. : a!jFtm$B+\4U3lrP+S\kbwqk9uq\QZA!Pu58W+JS#)

cpmb
centre professionnel
des métiers du bâtiment

ETABLISSEMENT D'UN TUNNEL VPN

Phase 2 – négociation des paramètres des réseaux et de la protection des données

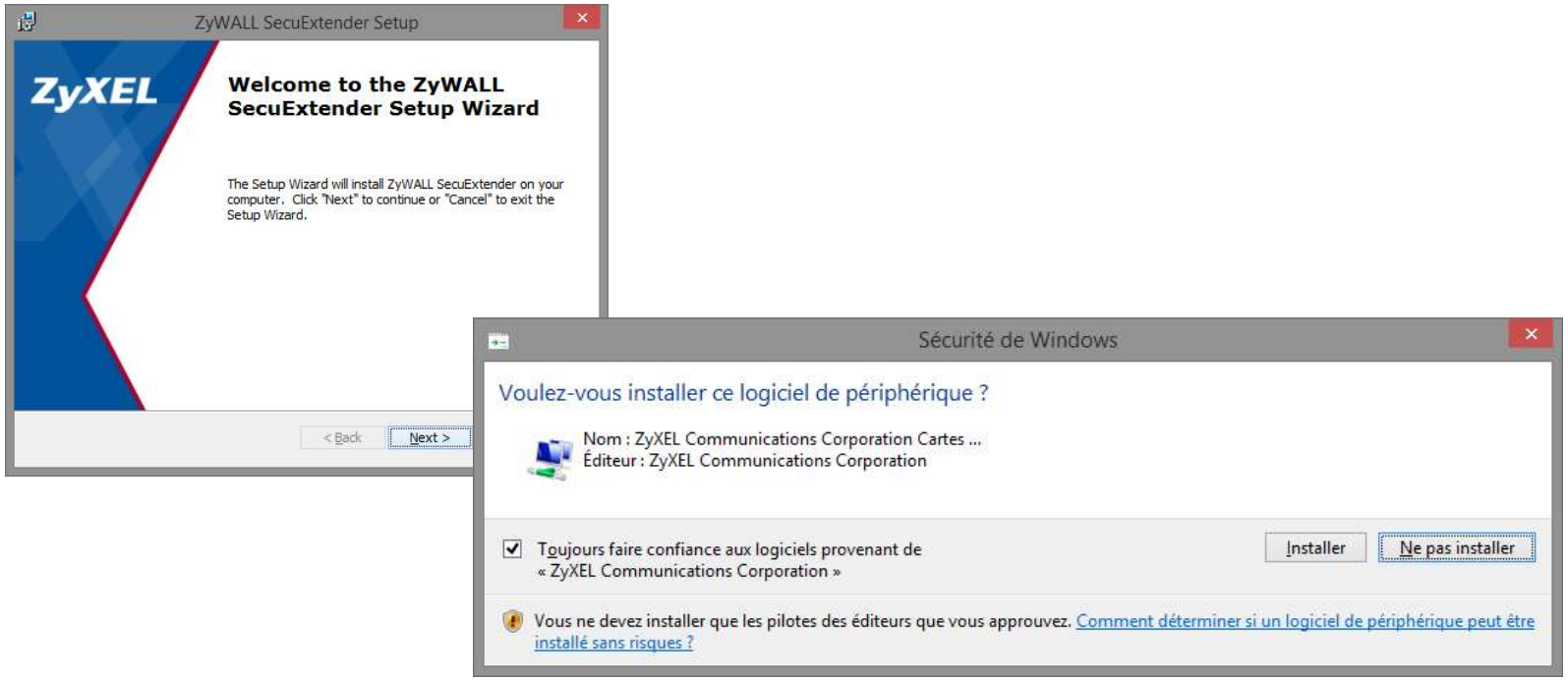
- A partir des clés et négociations générées dans la phase 1, création de clés pour le chiffrage des données
  1. Une deuxième itération Diffie-Hellman peut être utilisée pour le partage des clés (sécurité accrue)
  2. Une fois la phase 2 terminée, le tunnel est établi et les données peuvent transiter entre les sites
- Chaque phase génère des SA (Security Association) dont la durée de vie est limitée; une fois la période de validité échue, une nouvelle phase démarre
- Il est possible d'associer plusieurs réseaux par des 'Phase 2' différentes

cpmb
centre professionnel
des métiers du bâtiment

VPN SSL POUR UTILISATEUR NOMADE

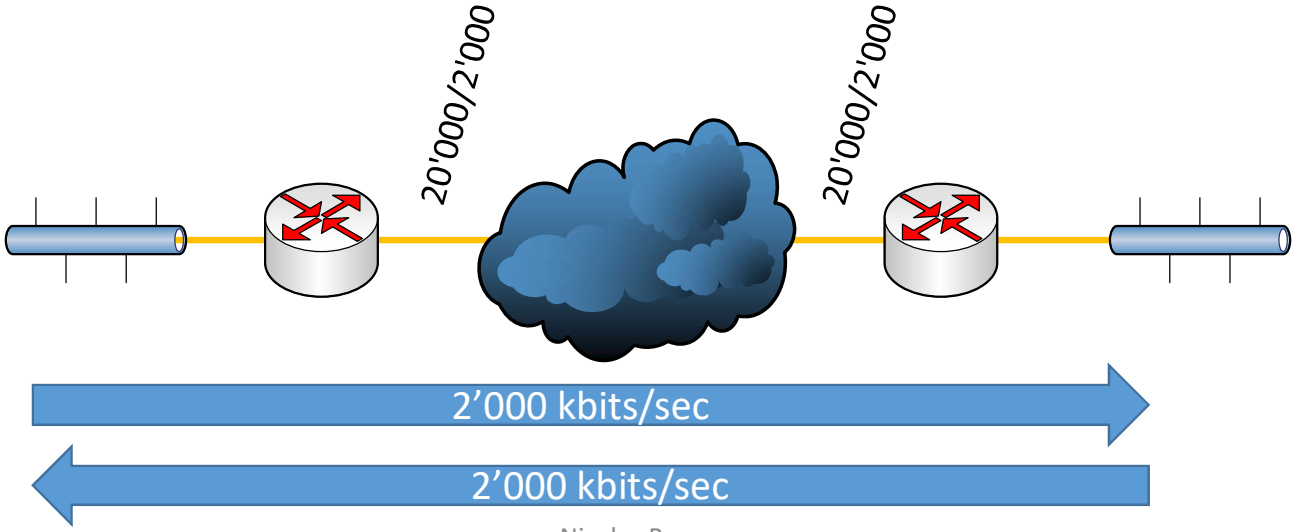
- Permet de mettre en relation un utilisateur nomade avec l'infrastructure de l'entreprise
- Tout comme pour les connexions VPN site à site, la communication est sécurisée
- Installation à la volée du client VPN sur le poste nomade si nécessaire
- Une fois la connexion établie, accès aux données et applications 'identique' à une connexion locale

INSTALLATION DU CLIENT



REMARQUES IMPORTANTES

- Le débit montant est souvent le point faible des liaisons VPN établies sur des liaisons de type DSL



cpmb
centre professionnel
des métiers du bâtiment

REMARQUES IMPORTANTES

VPN et applications VoIP

- Attention à la qualité de service à propager de bout en bout de la connexion
- Il faut gérer attentivement la bande passante montante
- La transmission de la voix est réalisée de terminal à terminal
- Le réseau VPN entre les différents sites doit être entièrement maillé ou …
- Prévoir des liaisons montantes suffisamment importantes et configurer explicitement le routage pour transiter par un point central du réseau

REMARQUES IMPORTANTES