

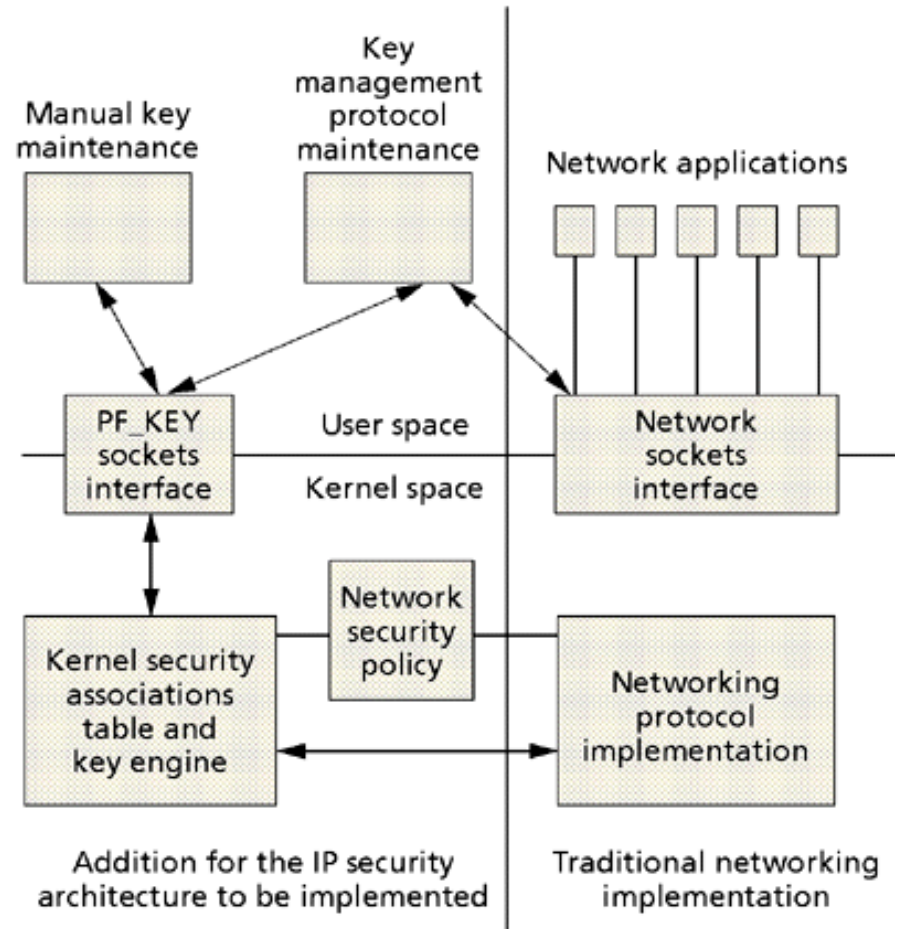
## IPv6 et la sécurité: Gestion des clés

Objectif:

Comment distribuer les clés

# Internet Key Management Protocol

- IPsec n'impose pas un algorithme donné
- Le protocole IKMP permet aux deux entités de négotier l'algorithme à utiliser en fonction des capacités respectives
- Dans les réseaux privés la gestion peut être manuelle



# Gestion des associations et des clés

- Deux approches
  - Gestion manuelle
    - Environnement de petite taille et statique (danger !)
  - Gestion automatique
    - Internet Security Association and Key management Protocol (ISAKMP)
      - Cadre générique pour la négociation, la modification et la destruction des SA  
RFC 2408  
<http://www.ietf.org/rfc/rfc2408.txt>
      - Indépendant du protocole d'échange de clés (et du protocole pour lequel on souhaite négotier une SA)
      - Associé aux protocoles d'échange de clés SKEME et Oakley
    - Internet Key Exchange (IKE)
      - RFC 2409  
<http://www.ietf.org/rfc/rfc2409.txt>
    - Domaine d'interprétation (DOI)
      - RFC 2407  
<http://www.ietf.org/rfc/rfc2407.txt>
    - Clés pour l'authentification mutuelle et préalable des équipements
      - Pre-shared key (PSK) ou Public Key Infrastructure (PKI)

# ISAKMP

- Protocole niveau application
  - Paramètres IPsec , TLS, SSL
- Blocs
  - paramètres de sécurité à négocier
    - (bloc Security Association ou SA, Proposal ou P, Transform ou T)
  - clés de session à convenir (Key Exchange ou KE)
  - identités des entités (ID)
  - certificats (CERT, Certificate Request ou CERTREQ)
  - l'authentification (HASH, SIG, NONCE où NONCE contient un nombre généré aléatoirement utilisable une seule fois)
  - messages d'erreurs (notification ou N)
  - associations de sécurité à supprimer (Delete)
  - constructeur d'équipement/logiciel de sécurité (Vendor ID)

# Echanges ISAKMP/IKEv1

---

- Phase 1
  - SA ISAKMP bidirectionnelle
    - Attributs
    - Identités
    - Clés
  - Sert à protéger les échanges ISAKMP futurs en confidentialité et intégrité/authentification
- Phase 2
  - Négotiation des paramètres de sécurité pour une ou plusieurs SA
    - IPsec AH ESP
    - Autre protocole de sécurité (TLS, SSL)

# ISAKMP/IKEv1

---

- Quatre modes
  - Principal (Main mode) - phase 1
  - Agressif (Agressive mode) – phase 1
  - Rapide (Quick mode) – phase 2
  - Nouveau groupe (New Groupe mode)
    - Sert à convenir d'un nouveau groupe pour des futurs échanges Diffie-Hellman

# Intéractions entre IPsec et IKE

- Trafic entrant
- Trafic sortant

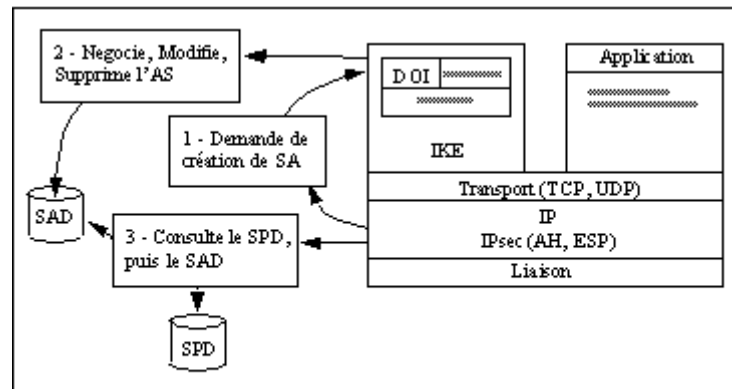


Figure 12-12. Interactions de IKEv1 avec IPsec

# SKEME et Oakley

---

# IKEv2

---

- Objectif de simplifier IKEv1
- [http://livre.point6.net/index.php/IKE\\_Version\\_2](http://livre.point6.net/index.php/IKE_Version_2)

# SPKI

---

# DNSSEC

---

- Domain Name System Security
- [http://livre.point6.net/index.php/CI%C3%A9s\\_publicues\\_:\\_infrastructures\\_et\\_certificats#DNSSEC\\_.28Domain\\_Name\\_System\\_9](http://livre.point6.net/index.php/CI%C3%A9s_publicues_:_infrastructures_et_certificats#DNSSEC_.28Domain_Name_System_9)

# Architectures de mise en oeuvre d'IPsec

- Trois cas typiques
  - Interconnexion de réseaux privés
    - VPN Virtual Private Networks
  - Nomadisme
    - Avant la norme 802.11i
- [http://livre.point6.net/index.php/Mise\\_en\\_place\\_d%27une\\_](http://livre.point6.net/index.php/Mise_en_place_d%27une_)

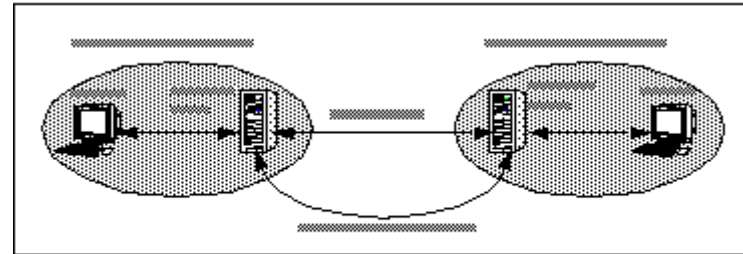


Figure 12-14 . Architecture VPN : Interconnexion de réseaux locaux

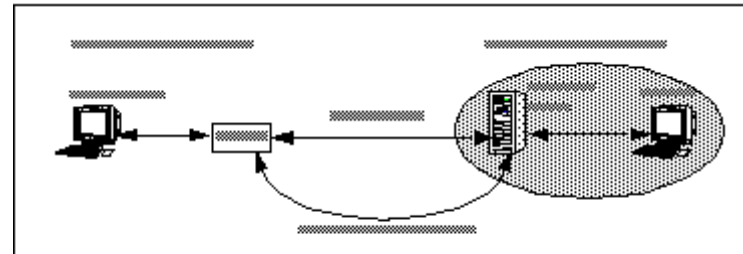


Figure 12-15 . Architecture VPN : nomadisme

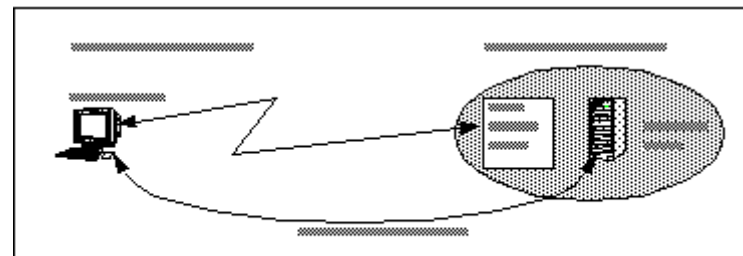


Figure 12-16 . Architecture VPN : protection de l'accès Wi-Fi

# Critique de IPsec

---

- [http://livre.point6.net/index.php/Critique\\_des\\_IPsec](http://livre.point6.net/index.php/Critique_des_IPsec)

# Comparaison entre VPN IPsec et VPN SSL

---

- [http://livre.point6.net/index.php/Comparaison\\_entre\\_VPN\\_IPsec\\_et\\_VPN\\_SSL](http://livre.point6.net/index.php/Comparaison_entre_VPN_IPsec_et_VPN_SSL)

# Support IPsec Windows XP

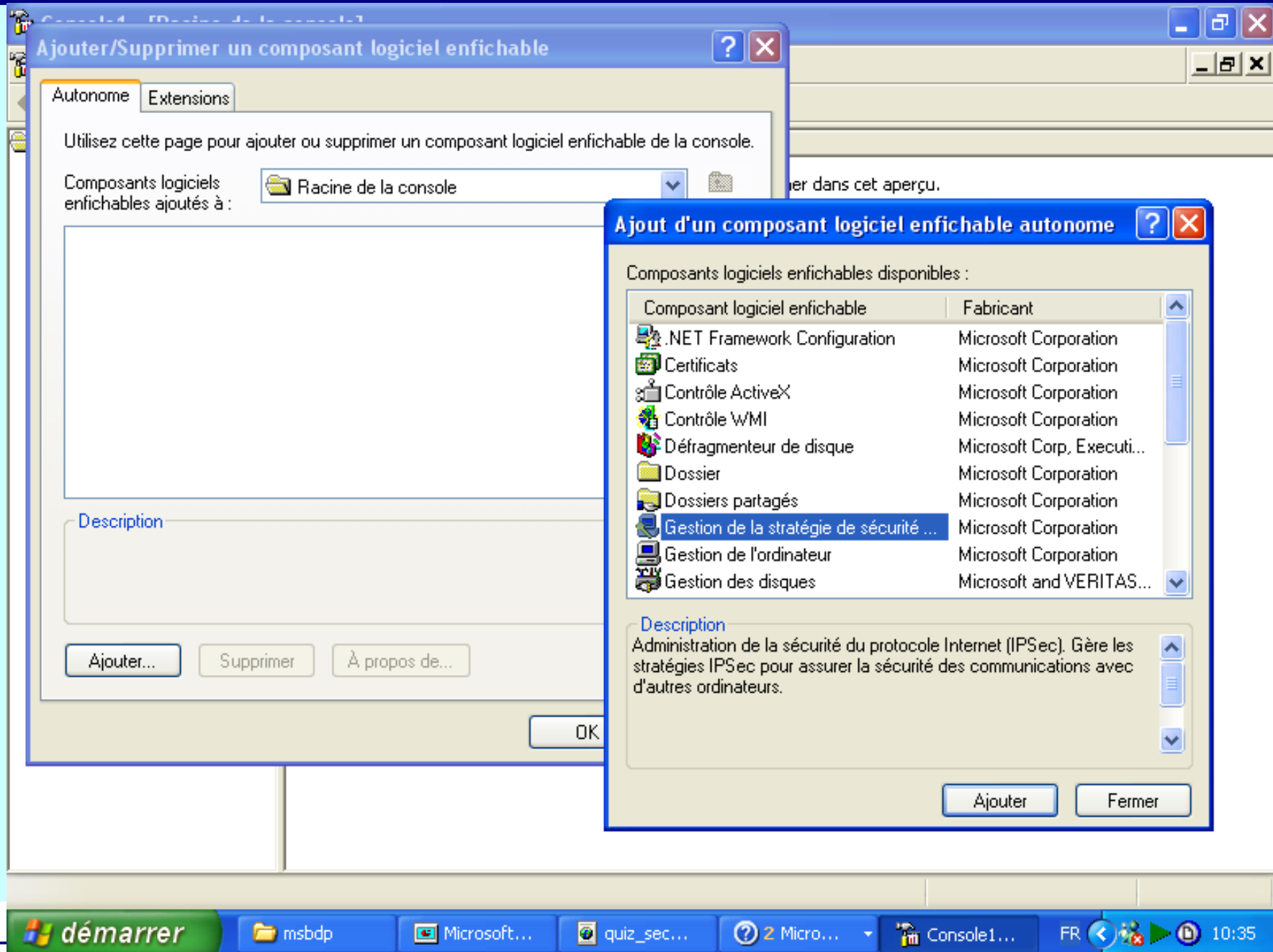
Centre d'aide et de support

← Précédent   →   Ajouter aux Favoris   Modifier l'affichage   Imprimer...   Rechercher dans le sommaire

## Aide-mémoire : Définition des stratégies IPsec

Étape	Référence
<input type="checkbox"/> Établissez un plan de sécurité.	<a href="#">Établissement d'un plan de sécurité IPsec</a>
<input type="checkbox"/> Analysez les concepts de la stratégie de sécurité IP (Internet Protocol) ou IPsec.	<a href="#">Description d'une stratégie IPsec</a>
<input type="checkbox"/> Démarrez le composant logiciel enfichable Stratégies de sécurité IP.	<a href="#">Pour démarrer le composant logiciel enfichable Stratégies de sécurité IP</a>
<input type="checkbox"/> Définissez une stratégie IPsec pour chaque scénario du plan de sécurité de votre entreprise.	<a href="#">Définir des stratégies IPsec</a>
<input type="checkbox"/> Attribuez des stratégies IPsec.	<a href="#">Attribuer une stratégie IPsec</a>

# MMC Microsoft Management Console



# Questions

---

- 1 -
- 2 -
- 3 -
- Vos questions
- 
- 
-

# Références

---

- IPv6 Théorie et Pratique, chapitre Sécurité
  - <http://livre.point6.net/index.php/S%C3%A9curit%C3%A9>