VPN IPSEC

Les différents types de VPN

- VPN SSL :

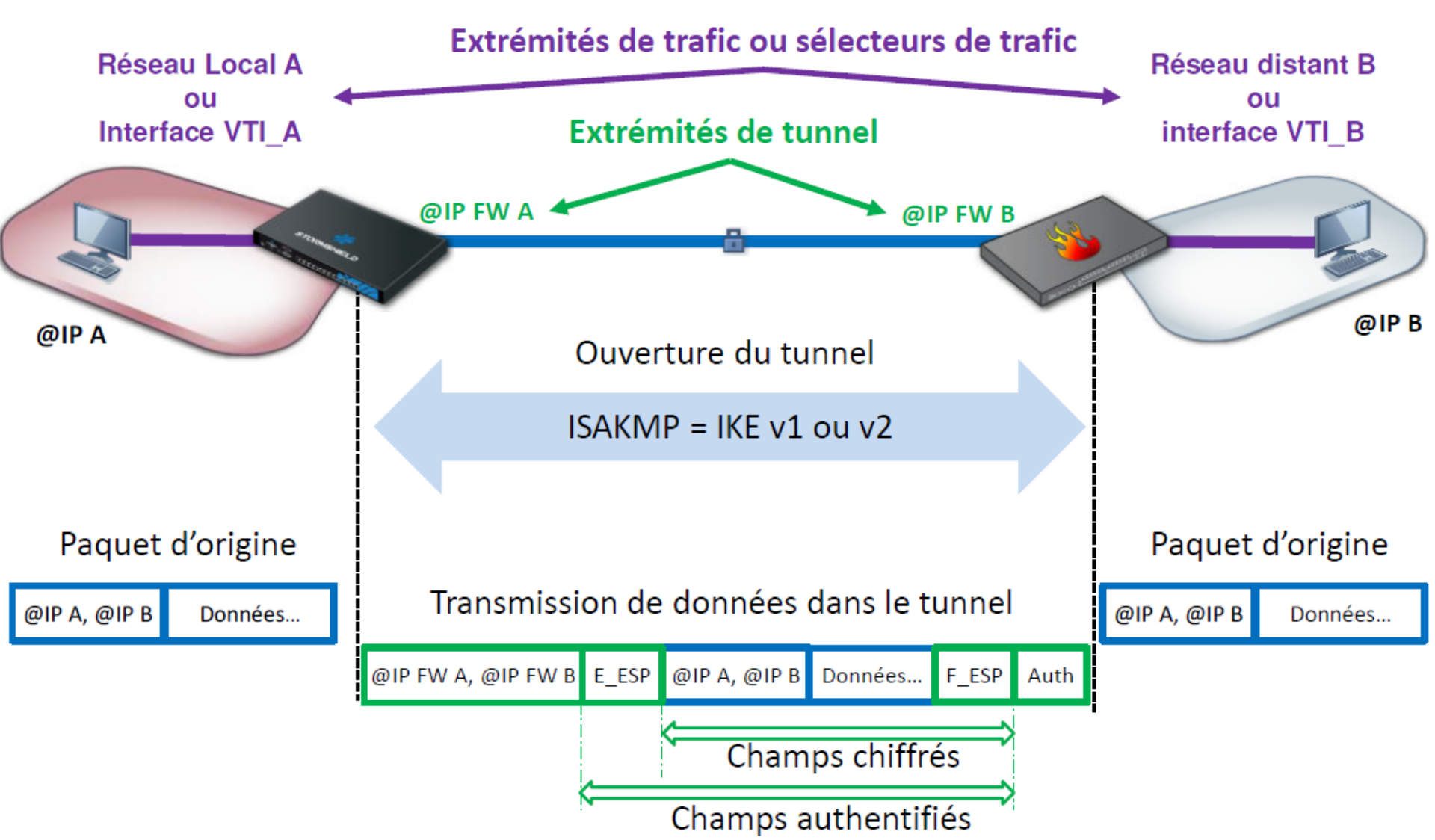
  clients nomades uniquement

- VPN IPsec (Internet Protocol Security) :

  tunnels site-à-site ou clients nomades

- GRE / GRETAP :

  Site-à-site -> transport paquets IP ou trame ethernet


Extrémités de trafic ou sélecteurs de trafic
Réseau Local A
ou
Interface VTI_A
Réseau distant B
ou
interface VTI_B
Extrémités de tunnel
@IP FW A
@IP FW B
@IP A
@IP B
Ouverture du tunnel
ISAKMP = IKE v1 ou v2
Paquet d'origine
@IP A, @IP B
Données...
Paquet d'origine
@IP A, @IP B
Données...
Transmission de données dans le tunnel
@IP FW A, @IP FW B
E_ESP
@IP A, @IP B
Données...
F_ESP
Auth
Champs chiffrés
Champs authentifiés

VPN IPSEC

- Tunnel VPN Ipsec site-à-site
- connecter deux réseaux privés via Internet
- Authentification des identités des deux extrémités de tunnel :
  - Soit clé pré-partagée (PSK : Pre-Shared key)
  - Soit certificats (PKI),
- Intégrité des données échangées :
  - algorithmes de hachage,
- Confidentialité
- Anti-rejeu : ignorer des anciens paquets déjà reçus, s'ils sont transmis à nouveau.

VPN IPSEC

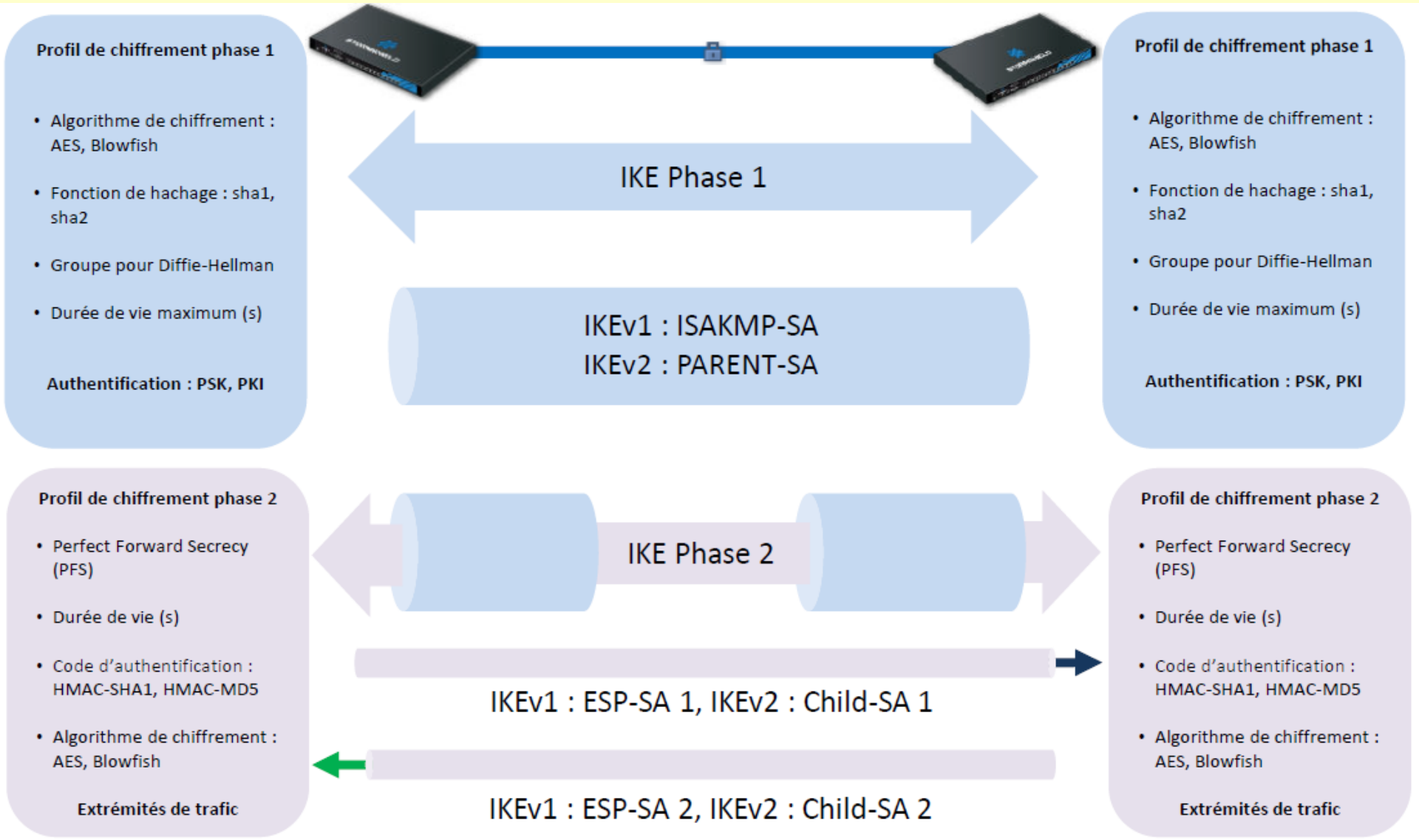
- Tunnel VPN IPsec site-à-site

- Négociation du tunnel :
  - entre les extrémités de tunnel :
    - @IP des équipements (@IP FW A et @IP FWB).
  - Protocole ISAKMP (Internet Security Association Key Management Protocol),
  - appelé également IKE (Internet Key Exchange),
  - deux versions V1 et V2
  - protocole IKE transmis via UDP sur le port 500

VPN IPSEC

- Tunnel VPN IPsec site-à-site

- Tunnel établi :
  - réseaux privés communiquent via le protocole ESP (Encapsulating Security Payload)
  - assure la confidentialité et l'intégrité des données.
  - encapsulé directement dans un paquet IP.
  - Deux modes de fonctionnement
    - Correspondance de politique
    - Virtual Tunneling Interface
  - Si une extrémité de tunnel est dans un réseau translaté, NAT-Traversal activé automatiquement :
    - protocole UDP sur le port 4500 utilisé pour finaliser la négociation IKE et transmettre les paquets ESP


Profil de chiffrement phase 1
• Algorithme de chiffrement : AES, Blowfish
• Fonction de hachage : sha1, sha2
• Groupe pour Diffie-Hellman
• Durée de vie maximum (s)
Authentification : PSK, PKI
IKE Phase 1
IKEv1 : ISAKMP-SA
IKEv2 : PARENT-SA
Profil de chiffrement phase 1
• Algorithme de chiffrement : AES, Blowfish
• Fonction de hachage : sha1, sha2
• Groupe pour Diffie-Hellman
• Durée de vie maximum (s)
Authentification : PSK, PKI
Profil de chiffrement phase 2
• Perfect Forward Secrecy (PFS)
• Durée de vie (s)
• Code d'authentification : HMAC-SHA1, HMAC-MD5
• Algorithme de chiffrement : AES, Blowfish
Extrémités de trafic
IKE Phase 2
IKEv1 : ESP-SA 1, IKEv2 : Child-SA 1
IKEv1 : ESP-SA 2, IKEv2 : Child-SA 2
Profil de chiffrement phase 2
• Perfect Forward Secrecy (PFS)
• Durée de vie (s)
• Code d'authentification : HMAC-SHA1, HMAC-MD5
• Algorithme de chiffrement : AES, Blowfish
Extrémités de trafic

VPN IPSEC

- Phase 1

- Négociation d’un profil de chiffrement phase 1
  - algorithmes de chiffrement/authentification.
  - Authentification avec une clé pré-partagée ou certificats.
  - dialogue d'application chiffré PARENT-SA dans IKEv2 établi entre les deux extrémités.
  - permet la négociation de la phase 2 qui sera entièrement chiffrée grâce à la clé de phase 1 PARENT-SA

VPN IPSEC

- Phase 2

- Négociation du profil de chiffrement phase 2
- Communication des extrémités de trafic via le tunnel VPN IPsec.
- Deux canaux ouverts pour la transmission des données (un dans chaque direction).
- Chaque canal utilise sa propre clé de chiffrement.
- appelées CHILD-SA1 et CHILD-SA2 en IKEv2.
- Chaque extrémité possède deux clés symétriques :
  - une pour chiffrer les données transmises
  - une déchiffrer les données reçues.

VPN IPSEC

- Vie du tunnel

- Négociation du tunnel déclenchée par le correspondant dont le réseau local a initié du trafic vers le réseau distant.
- Si aucun trafic entre les réseaux :
  - le tunnel ne sera pas ouvert.