

IPv6 et la sécurité: IPsec

Objectif:
Sécuriser ...

IPsec

- Toutes les implémentations conformes IPv6 doivent intégrer IPsec
- Services
 - Authentification mutuelle
 - Authentification de l'origine des données
 - Confidentialité des données
 - Confidentialité du flux des données
 - Intégrité des données
 - Prévention contre le rejeu des données
 - Non-répudiation
- Attaques
 - IP sniffing, spoofing, flooding
 - Écoute, usurpation de l'identité, inondation de messages

IETF IPsec

- IPsec exists below the Transport layer,
 - so its security services are transparently inherited by applications
- IPsec provides the protections of
 - data integrity,
 - data origin authentication,
 - data confidentiality,
 - and replay protection
 - without having to upgrade applications or train users.
- One of the great benefits of IPsec is the ability to protect against both internal and external attacks.

Orientations IETF

- Deux extensions IP de sécurité
 - Authentification: AH Authentication Header
 - Services d'authentification, intégrité des données
 - Optionnellement détection de rejeu et non-répudiation
 - Confidentialité: ESP Encapsulating Security Payload
 - Services de confidentialité, intégrité, authentification et détection de rejeu
 - Confidentialité du flux (au moins de façon limitée)
- Deux modes de protection
 - Transport
 - Tunnel

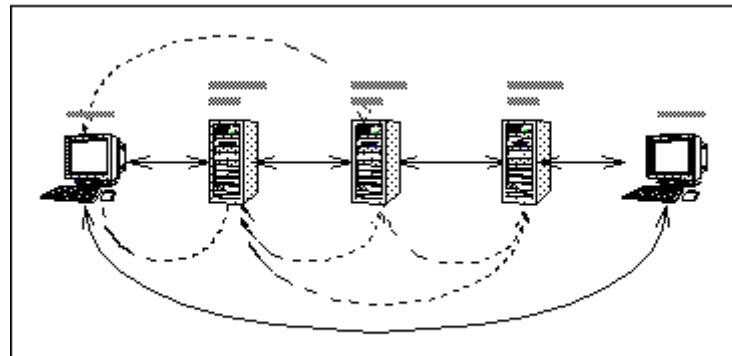


Figure 12-1. Différents modes de protection

Association de sécurité

- L'ensemble des services et mécanismes de sécurité choisis par les deux entités du réseau forme l'association de sécurité de la communication
- Unidirectionnelle
 - $A \rightarrow B$ et, éventuellement, $B \rightarrow A$
- identifiée par le triplet:
 - SPI Security Parameters Index
 - (SAID: Security Association Identifier)
 - Adresse du destinataire du paquet IP
 - Protocole de sécurité AH ou ESP

Contenu d'une association de sécurité

- AH:
 - Algorithme d'authentification, clés de chiffrement, ...
- ESP
 - Algorithme de chiffrement, clés de chiffrement,...
 - Algorithme d'authentification, clés de chiffrement
 - Si le service d'authentification est choisi
- Durée de vie
 - Pour éviter que les clés de chiffrement soient utilisées trop longtemps
- Mode du protocole IPsec
 - Transport
 - Tunnel
 - (Wildcard, c-à-d choisi par l'application)

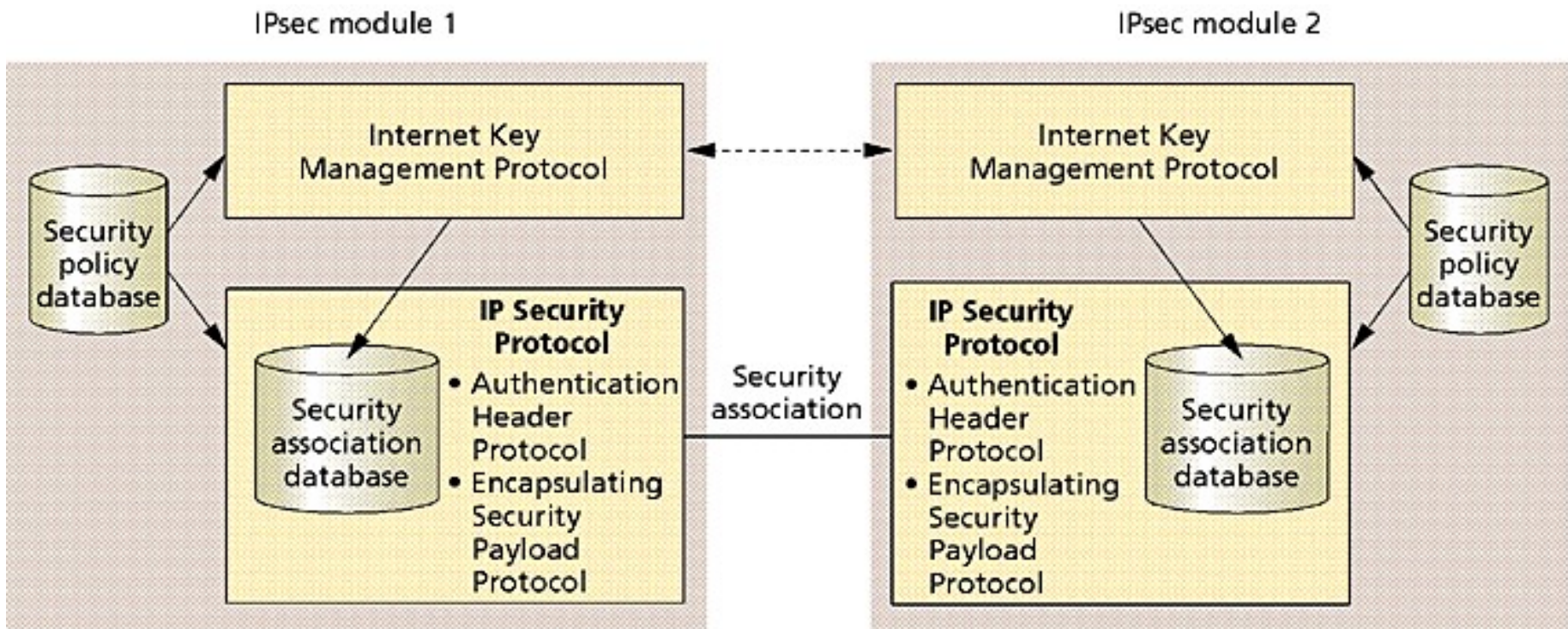
Choix d'une association de sécurité

- Choix, au niveau station émettrice ou passerelle de sécurité, dépend des paramètres suivants (sélecteurs):
 - Adresse IP de la source
 - Identité de l'utilisateur
 - Identité de l'équipement
 - Numéros de ports source et destination
 - Protocole de niveau transport
 - Adresse IP de l'équipement distant
 - Niveau de sensibilité des données
 - RFC 1108 <http://www.ietf.org/rfc/rfc1108.txt>
- En général on utilise
 - Adresse IP de destination
 - Numéro de protocole
 - Numéros de port

Bases de données

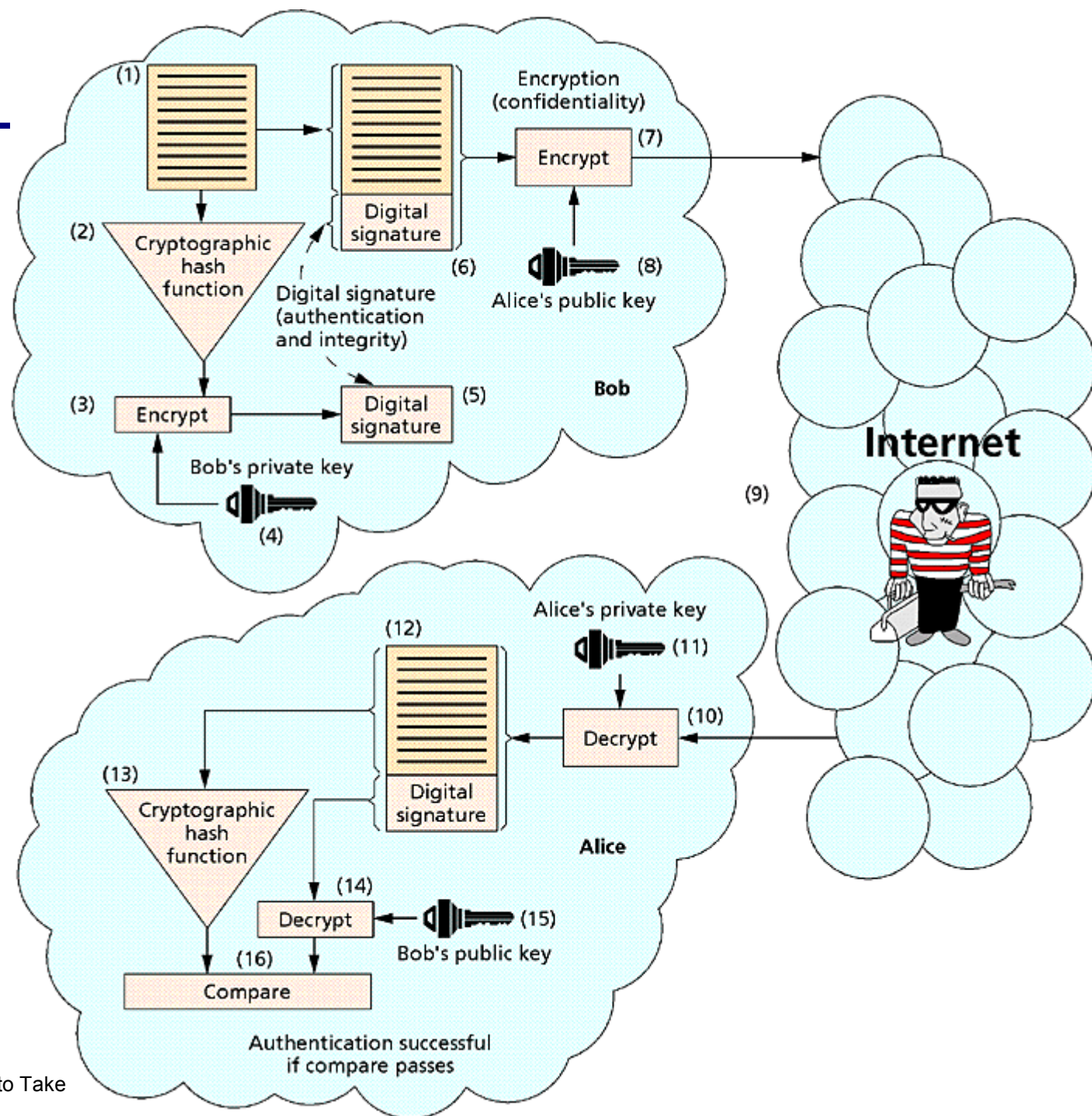
- IETF conseille deux BD
 - Security Policy DB (SPD)
 - En fonction du sélecteur
 - Discard
 - Bypass IPsec
 - Apply IPsec

- Security Association DB (SAD)
 - Services et mécanismes à appliquer
 - RFC 2401 → 2401bis
 - <http://www.ietf.org/rfc/rfc2401.txt>



PGP

- Pretty Good Privacy
 - Zimmerman, MIT



Source: P. Dowd et al., "Network Security: It's Time to Take It Seriously", IEEE Computer, Sep. 1998, pp. 24-28

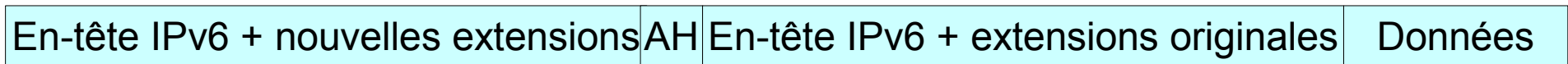
Digests et Signatures numériques

- Digest
 - Condensé (condensat, empreinte) d'un document obtenu avec une fonction mathématique de hachage (Hash function)
 - ex. "message" → "msg"
- Digital Signature
 - Le fait d'encrypter un condensé avec la clef privée d'un utilisateur produit une signature numérique
 - elle garantit à la fois:
 - l'identité de l'auteur (authentification)
 - l'intégrité du message
 - l'impossibilité pour l'auteur de "répudier" son message
- Applications typiques
 - Echange de documents, téléchargement de programmes
 - Courrier Electronique

Positionnement de l'extension d'authentification



Mode transport



Mode tunnel

Authentication Header Protocol

- Authentification et intégrité
- Trois niveaux de clefs
 - host-oriented keying
 - user-oriented keying
 - session-unique keying



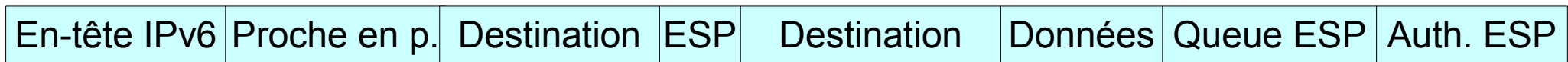
Contenu de l'extension d'authentification

32

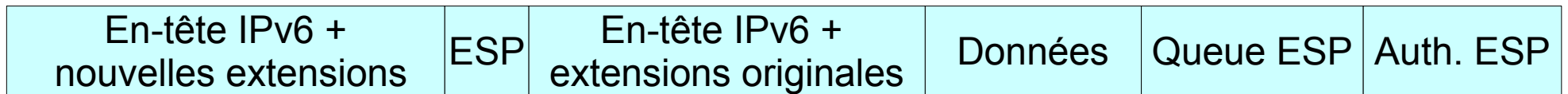
En-tête suiv.	Lg. extension	Réservé
Indice des paramètres de sécurité (SPI)		
Numéro de séquence		
Authenticateur (nombre variable de mots de 32 bits)		

Confidentialite

Les deux modes de protection



Mode transport



Mode tunnel



Encapsulating Security Payload Protocol

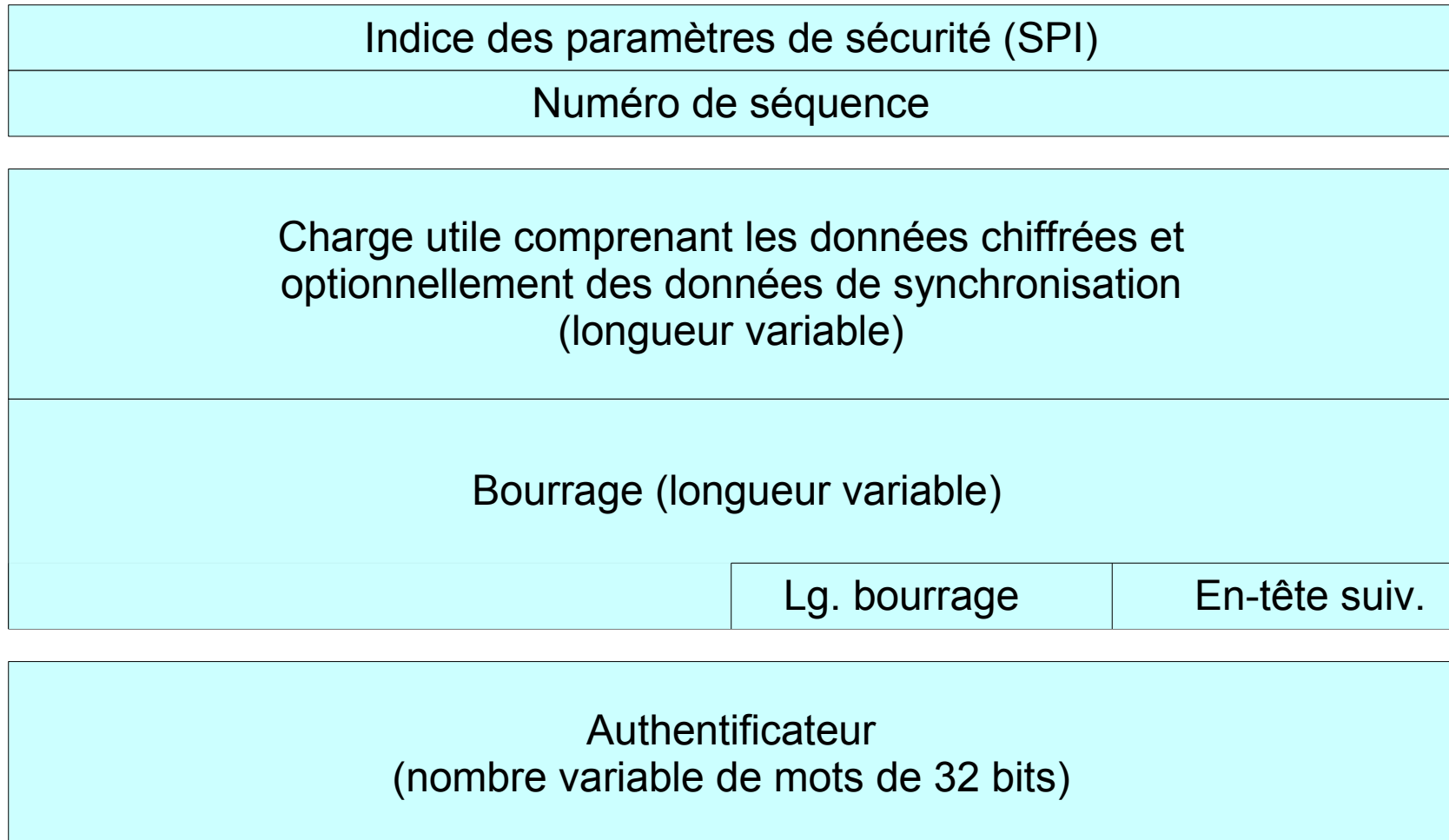
- Confidentialité
- Deux modes
 - Transport : le contenu du paquet
 - Tunnel : tout le paquet IP y compris l'en-tête



Contenu de l'extension de confidentialité

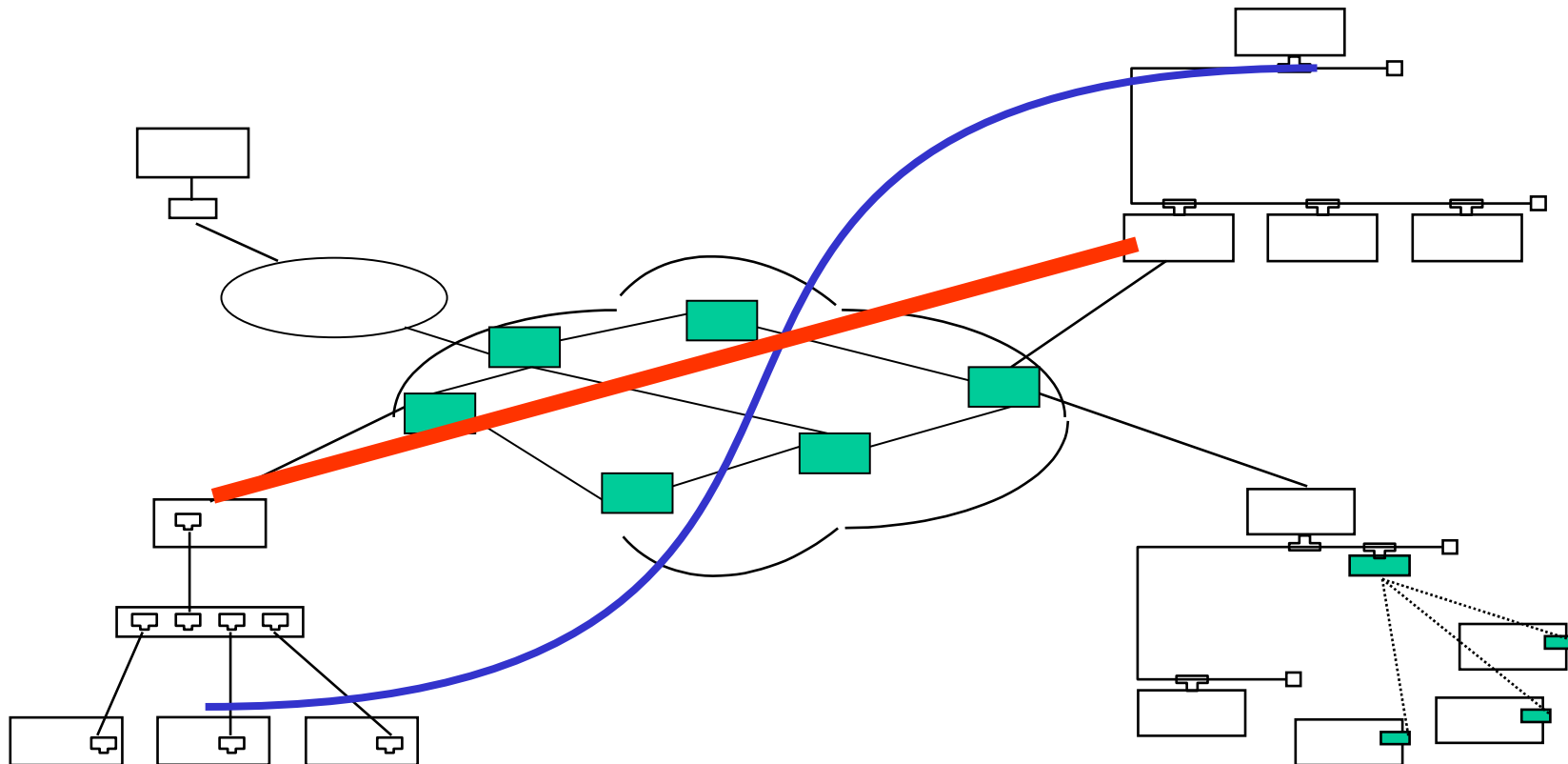
1

32



Modes d'opération

- Deux modes d'opération
 - transport mode
 - adresses source et destination en clair
 - tunnel mode
 - adresses source et destination cachées



Références

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

Internal and External Attacks

- Firewalls, secure routers, and
- strong authentication of remote access connections
- are examples of attempts to defend against external threats.
- But strengthening a network's perimeter does nothing to protect against attacks mounted from within.
- An organization can lose a great deal of sensitive information from internal attacks mounted by employees, supporting staff members, or contractors.
- Edge devices such as firewalls offer no protection against internal threats.

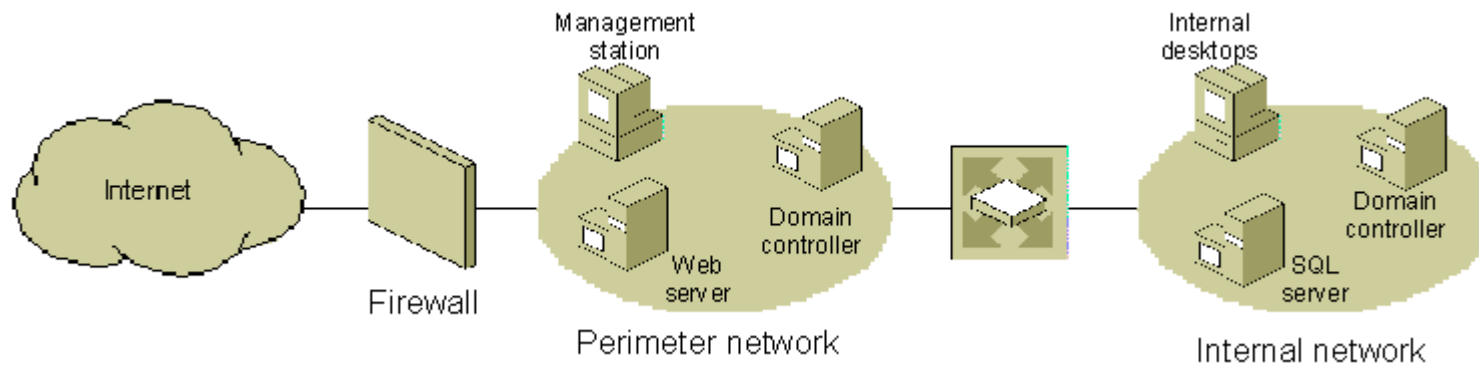
Benefits of IPsec

- IPsec provides network-level
- data integrity,
- data confidentiality,
- data origin authentication,
- and replay protection for IP-based traffic.
 - IPsec in Windows Server 2003 integrates with the inherent security of the Windows Server 2003 operating system to provide the ideal platform for protecting intranet and Internet communications.

IPsec in Windows

- Transparency of IPsec to users and applications
- Defense-in-depth against vulnerabilities in upper-layer protocols and applications
- Restricted access to servers
- Customizable security configuration
- Centralized IPsec policy administration through Active Directory
- Support for IETF standards
- Support for automatic cryptographic key management
- Hardware acceleration of IPsec cryptographic functions is supported by many network adapters

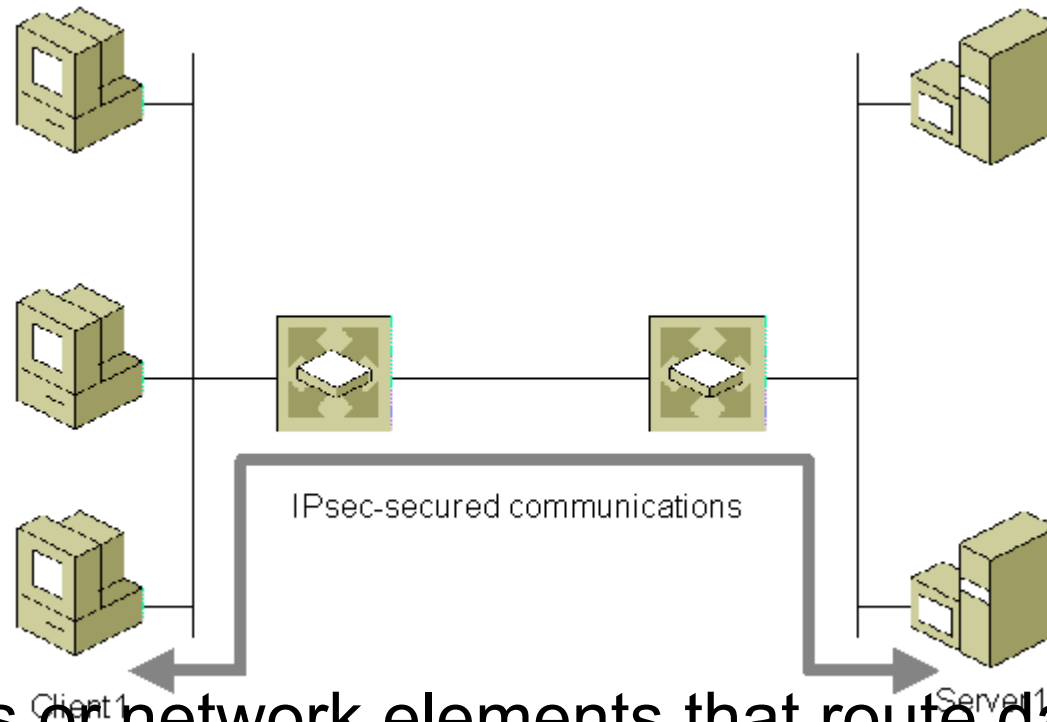
Packet Filtering



Support for IETF standards

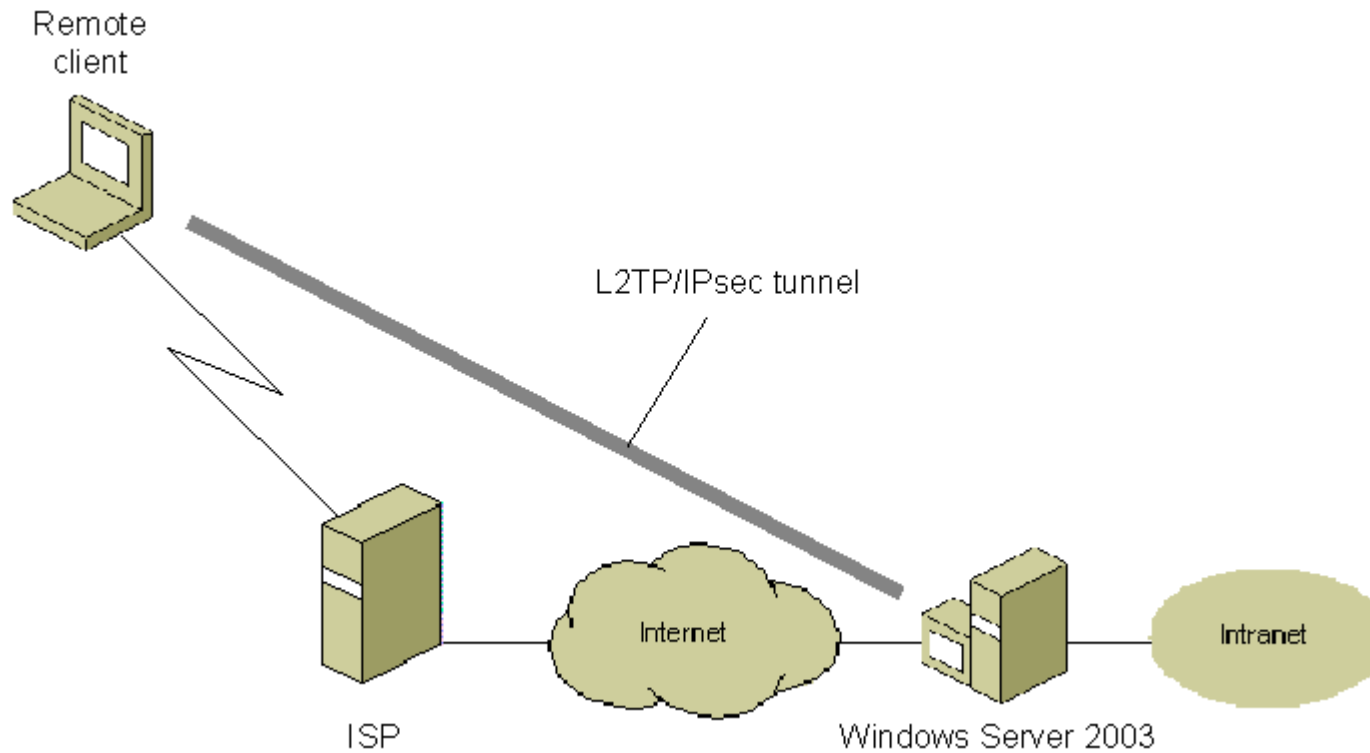
- RFC 1828: IP Authentication using Keyed MD5
- RFC 1829: The ESP DES-CBC Transform
- RFC 2085: HMAC-MD5 IP Authentication with Replay Prevention
- RFC 2104: HMAC: Keyed-Hashing for Message Authentication
- RFC 2401: Security Architecture for the Internet Protocol
- RFC 2402: IP Authentication Header
- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2406: IP Encapsulating Security Payload (ESP)
- RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2410: The NULL Encryption Algorithm and Its Use with IPsec
- RFC 2411: IP Security Document Roadmap
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- A GSS-API Authentication Method for IKE (draft-ietf-ipsec-isakmp-gss-auth-0x.txt)
- UDP Encapsulation of IPsec Packets (draft-ietf-ipsec-udp-encaps-02.txt)
- Negotiation of NAT-Traversal in the IKE (draft-ietf-ipsec-nat-t-ike-02.txt)

End-to-End Security

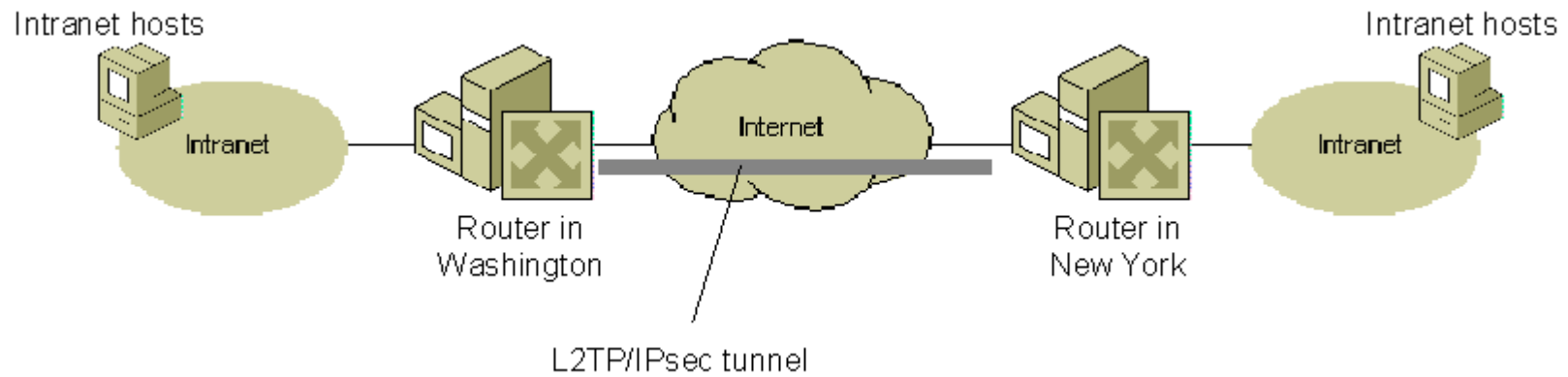


- Computers or network elements that route data from source to destination are not required to support IPsec.

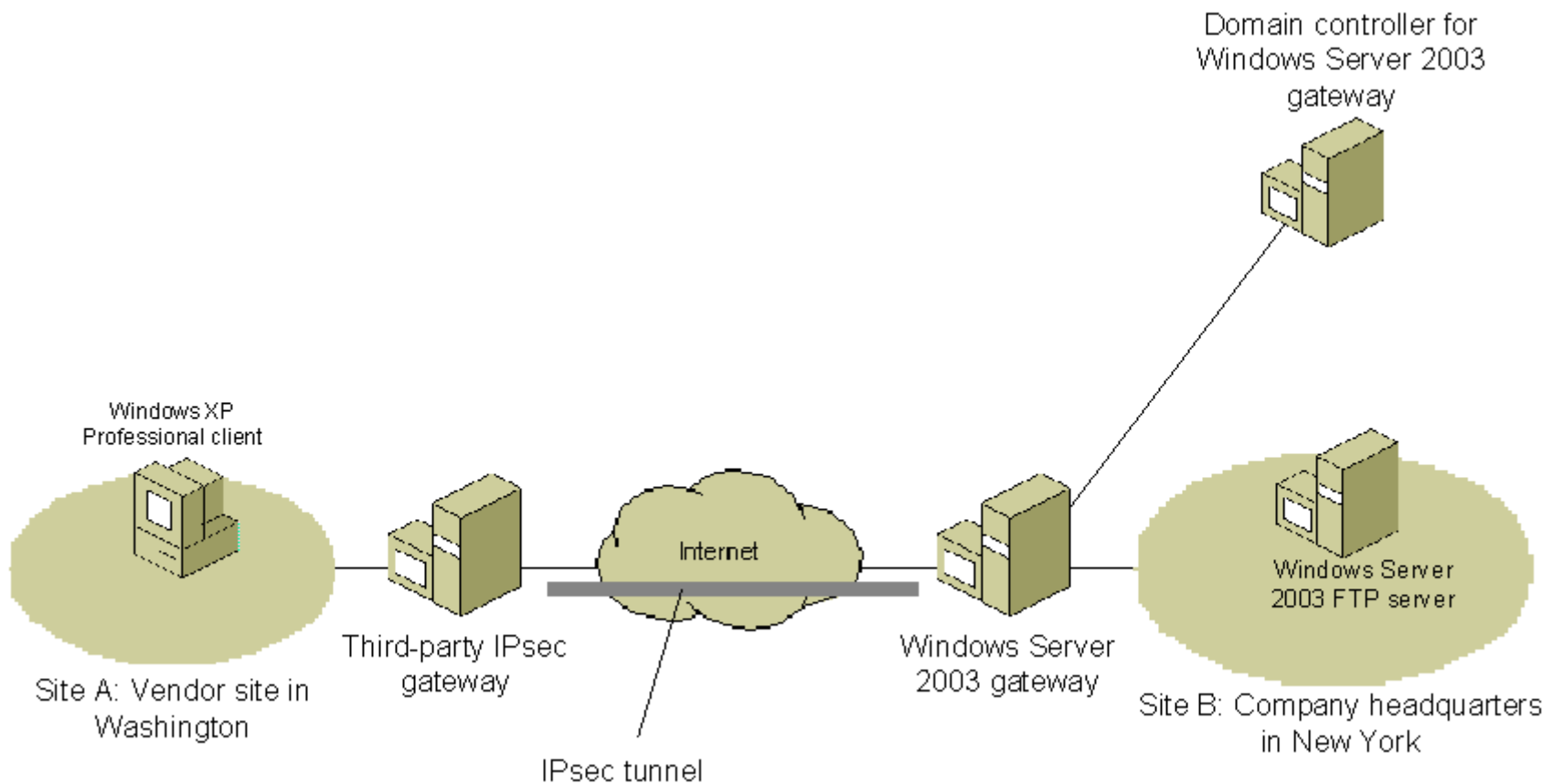
L2TP/IPsec for Remote Access



Site-to-Site VPN Connection



Gateway-to-Gateway Tunneling



Creating IPsec Policies

- General IPsec policy settings
 - Settings that determine the name of the policy, its description, key exchange settings, and key exchange methods. General IPsec policy settings apply regardless of which rules are configured.
- Rules
 - One or more IPsec rules that determine which traffic IPsec examines, how that traffic is secured and encrypted, and how IPsec peers are authenticated.

Defining IPsec Policy Rules

- Filter list
 - A single filter list is selected that contains one or more predefined packet filters that describe the types of traffic to which the configured filter action for this rule is applied.
- Filter action
 - A single filter action is selected that includes the type of action required (permit, block, or secure) for packets that match the filter list.
 - For the secure filter action, the negotiation data contains one or more security methods that are used (in order of preference) during IKE negotiations and other IPsec settings.
 - Each security method determines the security protocol (such as AH or ESP), the specific cryptographic algorithms, and session key regeneration settings.

Defining IPsec Policy Rules (2)

- Authentication methods
 - One or more authentication methods are configured (in order of preference) and used for authentication of IPsec peers during main mode negotiations.
 - The available authentication methods are
 - the Kerberos V5 protocol (used in Active Directory environments),
 - use of a certificate issued from a specified certification authority (CA), or
 - a preshared key.

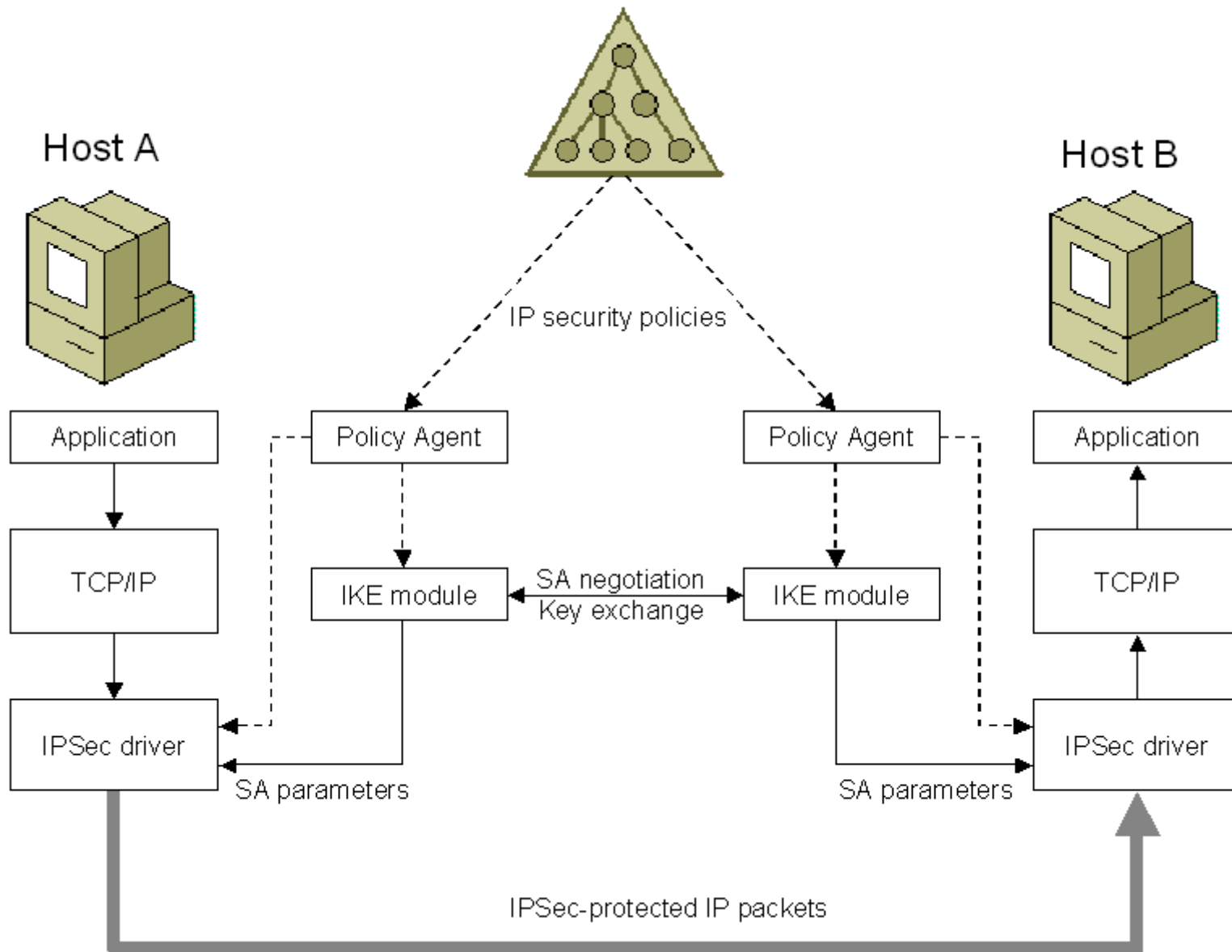
Example of Configuring an IPsec Policy

- As an example of how to configure IPsec policies, consider an organization with a centralized legal department. The network administrators have decided that communications within the legal department have to be authentic and unmodified, but not encrypted. Additionally, communications between the legal department and other departments within the organization must be authentic, unmodified, and encrypted.
- IPsec applies the appropriate security policy based on the characteristics of IP packets. For our example, if the communication is between a computer in the legal department and a computer outside the legal department, IPsec for Windows Server 2003 must enforce data origin authentication, data integrity, and data confidentiality. If the communication is between computers inside the legal department, IPsec must enforce data origin authentication and data integrity.
- To implement IPsec for the legal department, the administrator would perform the following steps:
- Create an organizational unit for the legal department named "Legal" and place all of the computer accounts of the legal department within it.
- Using the IP Security Policies extension within the Group Policy Editor snap-in (available under Computer Configuration\Security Settings), create an IPsec policy named "Communication for the Legal Department" with the following settings:
 - A filter list named "Legal intra-department traffic" that specifies that the destination address of packets must match an address on the IP subnets of the legal department and the source address of packets must match an address on the IP subnets of the legal department.
- A filter list named "All IP traffic" that specifies any IP traffic.
- A filter action named "Secure traffic within the Legal department" that specifies data authenticity and integrity.
- A filter action named "Secure traffic outside the Legal department" that specifies data authenticity, integrity, and confidentiality.
-

Example of Configuring an IPsec Policy (2)

- A rule named "Legal intra-department communications" which uses the "Legal intra-department traffic" filter list, the "Secure traffic within the Legal department" filter action, and Kerberos authentication.
- A rule named "Inter-department communications" which uses the "All IP traffic" filter list, the "Secure traffic outside the Legal department" filter action, and Kerberos authentication.
- Assign the IPsec policy named "Communication for the Legal Department" to the "Legal" organizational unit.
-
- After the IPsec policy is assigned and all computers within the legal department update their Computer Configuration Group Policy settings, IPsec-secured communications is enforced for all communication of the computers in the legal department.
- For example, when a computer in the legal department sends a packet to computer in another department, the packet matches the "All IP traffic" filter list, which is associated with the "Inter-department communications" rule, which enforces the use of Kerberos authentication and data origin authentication, integrity, and confidentiality.
- When a computer in the legal department sends a packet to another computer in the legal department, the packet matches the "Legal intra-department traffic" filter list, which is associated with the "Legal intra-department communications" rule, which enforces the use of Kerberos authentication and data origin authentication and integrity.
- Notice that for intra-department communication, the packets also match the "All IP traffic" filter list. However, the match to the "Legal intra-department traffic" filter list is more specific, and it is chosen over the "All IP traffic" filter list.

IPsec Components



How IPsec Works

- The user on Computer A sends a message to the user on Computer B. The message is passed to TCP/IP and is intercepted by the IPsec driver on Computer A.
- The IPsec driver on Computer A checks its outbound IPsec filter list and determines that the message should be secured.
- The action is to negotiate security, so the IPsec driver notifies IKE module to begin negotiations.
- The two computers use IKE to authenticate each other and determine secret keying material, the type of protection for future IKE traffic, and the type of protection for the message that is being sent.
- The sets of parameters that determine the protection, known as security associations (SAs), are sent to the IPsec driver. The IPsec driver uses SA information to protect the message.
- The IPsec-protected message is forwarded to Computer B.
- The IPsec driver on Computer B receives the IPsec-protected message.
- The IPsec driver on Computer B validates authentication and integrity and, if required, decrypts the message.
- The IPsec driver passes the validated and decrypted message to the TCP/IP driver, which passes it to the receiving application on Computer B.

Questions

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

Références

- IPv6 Théorie et Pratique, Chapitre Sécurité
 - <http://livre.point6.net/index.php/S%C3%A9curit%C3%A9>
- Microsoft IP Security for Windows
 - <http://technet.microsoft.com/en-us/network/bb531150.aspx>