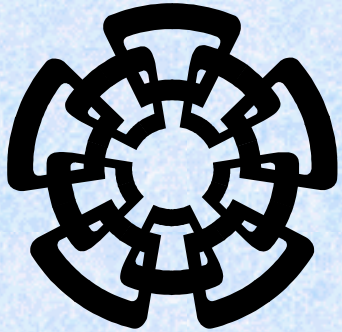


Una arquitectura de seguridad para IP

Rafael Espinosa García (respinosa@cs.cinvestav.mx)

Guillermo Morales Luna (gmorales@cs.cinvestav.mx)

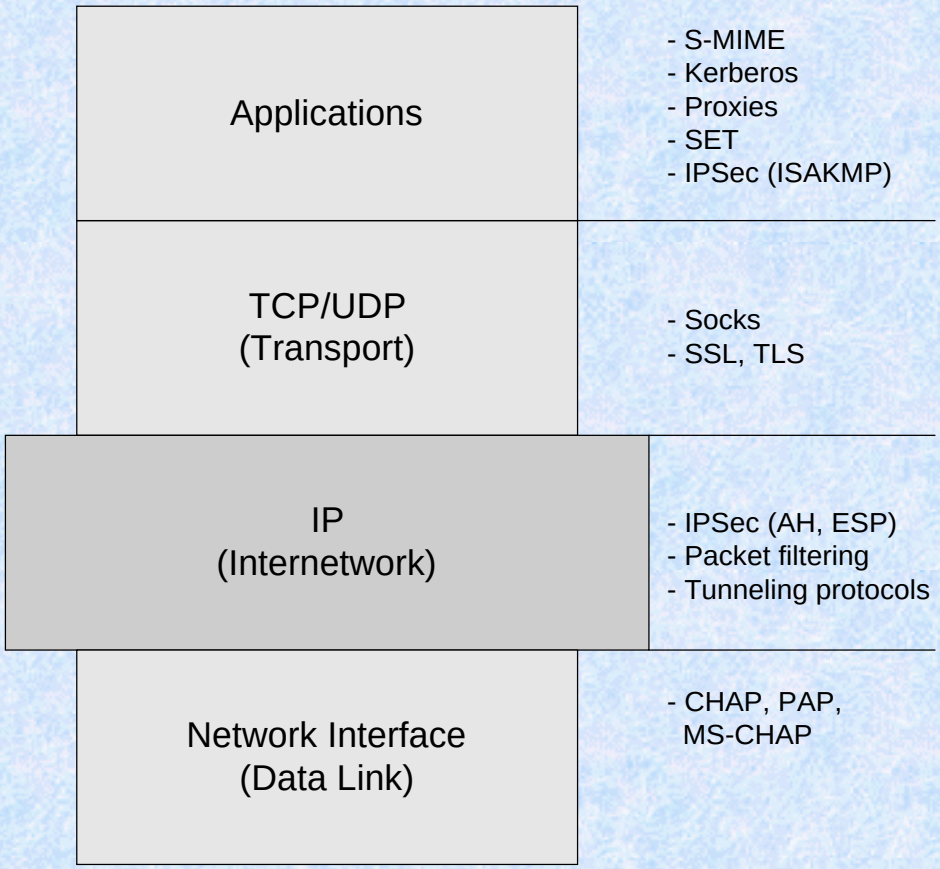
CINVESTAV-IPN

Departamento de Ingeniería Eléctrica

Problemas comunes

- Conexión al cable
- Imitación
- Negación de un servicio
- Contestación de mensajes en tránsito
- Suposición de *passwords*
- Suposición de llaves
- Virus

Esquemas de seguridad en las capas de TCP/IP



Protocolos de seguridad

- **CDPD** Cellular Digital Packet Data
- **DNSSEC** Domain Name System Security Extensions
- **DOCSIS** Data Over Cable Service Interface Specification
- **IEEE 802.11**
- **IPSec** IP Security Protocol
- **PPTP** Point to Point Tunneling Protocol
- **SET** Secure Electronic Transactions
- **S-MIME** Secure MIME
- **SSH** Secure Shell
- **SSL** & **TLS** Secure Sockets Layer & Transport Layer Security

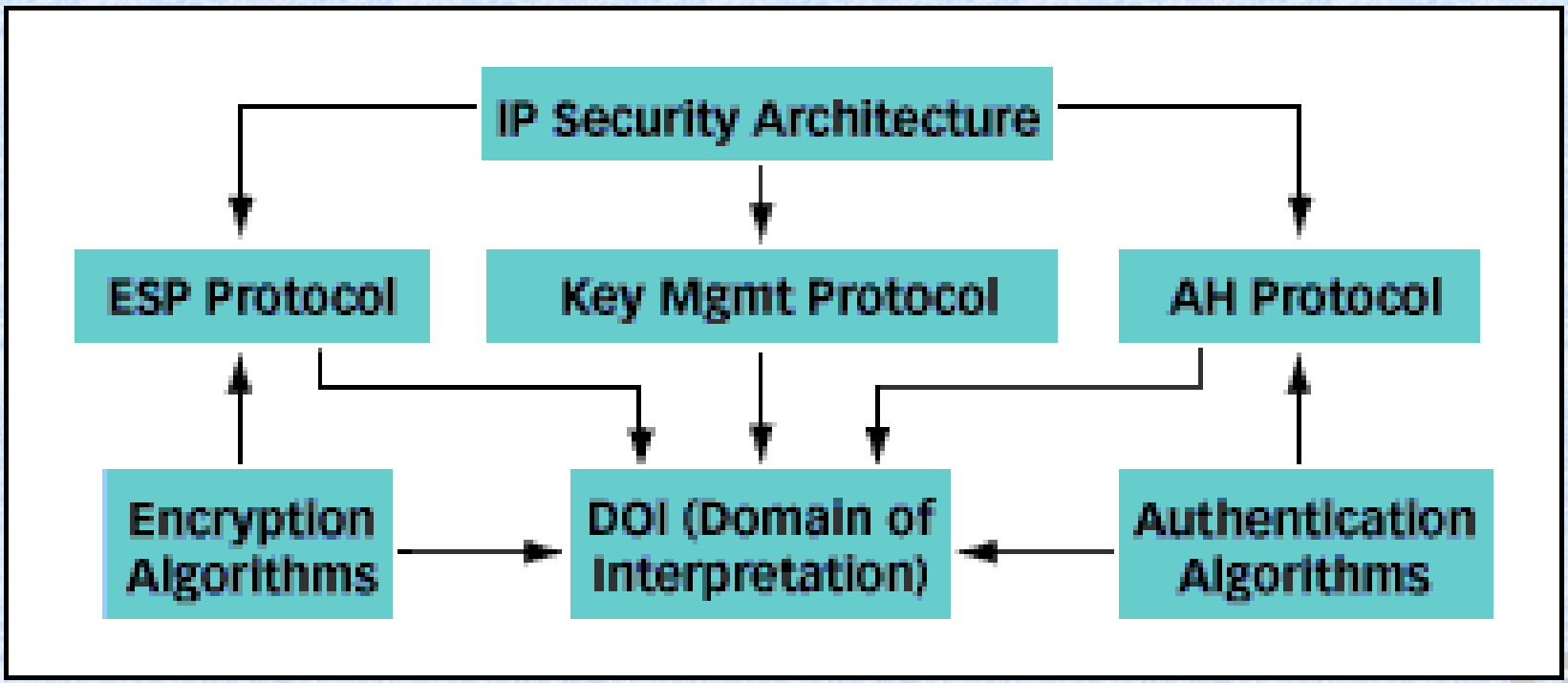
¿Qué es IPSec?

- Es un conjunto de estándares abiertos desarrollados por el *Internet Engineering Task Force* (IETF).
- Ofrece protección en la transmisión de información sensible sobre redes inseguras tal como es la propia Internet.
- IPSec actúa en la capa *de red*, protegiendo y autentificando paquetes IP entre los dispositivos participantes.

Estructura de IPSec

- IPSec tiene tres componentes principales:
  - *Authentication Header* (AH)
  - *Encapsulating Security Payload* (ESP)
  - *Internet Key Exchange* (IKE)
- Interoperabilidad.
- Independiente de algoritmos criptográficos actuales.
- Soporta tanto IPv4 como IPv6.
- Es una componente obligada en IPv6.

Arquitectura de IPSec



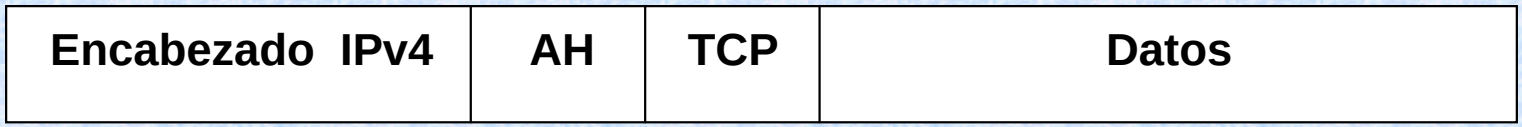
Servicios IPSec

	AH	ESP (sólo encriptación)	ESP (encriptación más autentificación)
Control en el acceso	√	√	√
Integridad sin conexión	√		√
Autentificación en el origen de datos	√		√
Rechazo de paquetes retocados	√	√	√
Confidencialidad		√	√
Confidencialidad limitada por el tráfico		√	√

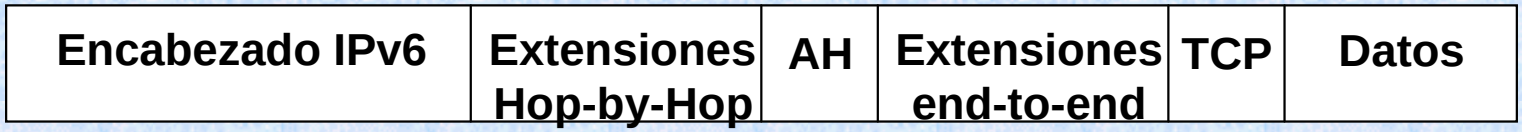
Beneficios

- Herencia de niveles de seguridad
- Transparencia en las aplicaciones
- Transparencia respecto a usuarios finales
- Seguridad a nivel individual

Autentificación



IPv4



IPv6

Encabezado de AH

Next Header	Length of Auth Data field	Reserved
Security Parameter Index (32 bit-value)		
Authentication Data (variable number of 32-bit words)		

Authentication Header

Encriptamiento

Encabezado IPv6	Extensiones Hop-by-Hop	Destinations Options	ESP Header	ESP Payload

Asociaciones de Seguridad (SA)

- Cada conexión IPSec puede realizar tareas de encriptamiento, de integridad y de autentificación.
- Cuando la seguridad, y sus niveles, queda convenida, los dos nodos participantes deben decidir cuáles algoritmos han de usar.
- Posteriormente, ambos participantes deben compartir una llave de seguridad.
- Una SA es una relación entre dos o más entidades que describen cómo es que las entidades usarán los servicios de seguridad para comunicarse con los niveles convenidos.

Formas de encapsulamiento

	Modo Transporte SA	Modo Túnel SA
AH	Auténtifica el campo Payload y selecciona porciones del encabezado IP y los encabezados de exntensión IPv6.	Auténtifica el paquete IP interno completo (el encabezado interno más el campo Payload) más porciones seleccionadas del encabezado IP exterior y los encabezados de extensión de IPv6.
ESP	Encripta el campo Payload del encabezado IP y cualquiera de los encabezados de extensión de IPv6 seguidos del encabezado ESP.	Encripta el paquete IP interno.
ESP con Auténtificación	Encripta el campo Payload del encabezado IP y cualquiera de los encabezados de extensión seguidos del encabezado ESP. Auténtifica el campo Payload pero no el encabezado IP.	Encripta el paquete IP interno. Autentificación el paquete interior IP.

Algoritmos utilizados en IPSec

- Se basa en el algoritmo de Diffie-Hellman y/o RSA para intercambio de llaves.
- Encriptamiento asimétrico realizado con DES-CBC y Triple-DES.
- En sistuaciones donde se requiere una mayor seguridad se utiliza RC5.
- Para *hashing* se utilizan los algoritmos SHA1 y HMAC-MD5.

Administración de llaves

- Existen dos mecanismos de administración:
  - Manual
  - Automático
- El protocolo ISAKMP/Oakley administra las llaves en forma automática

IPSec versus SSL

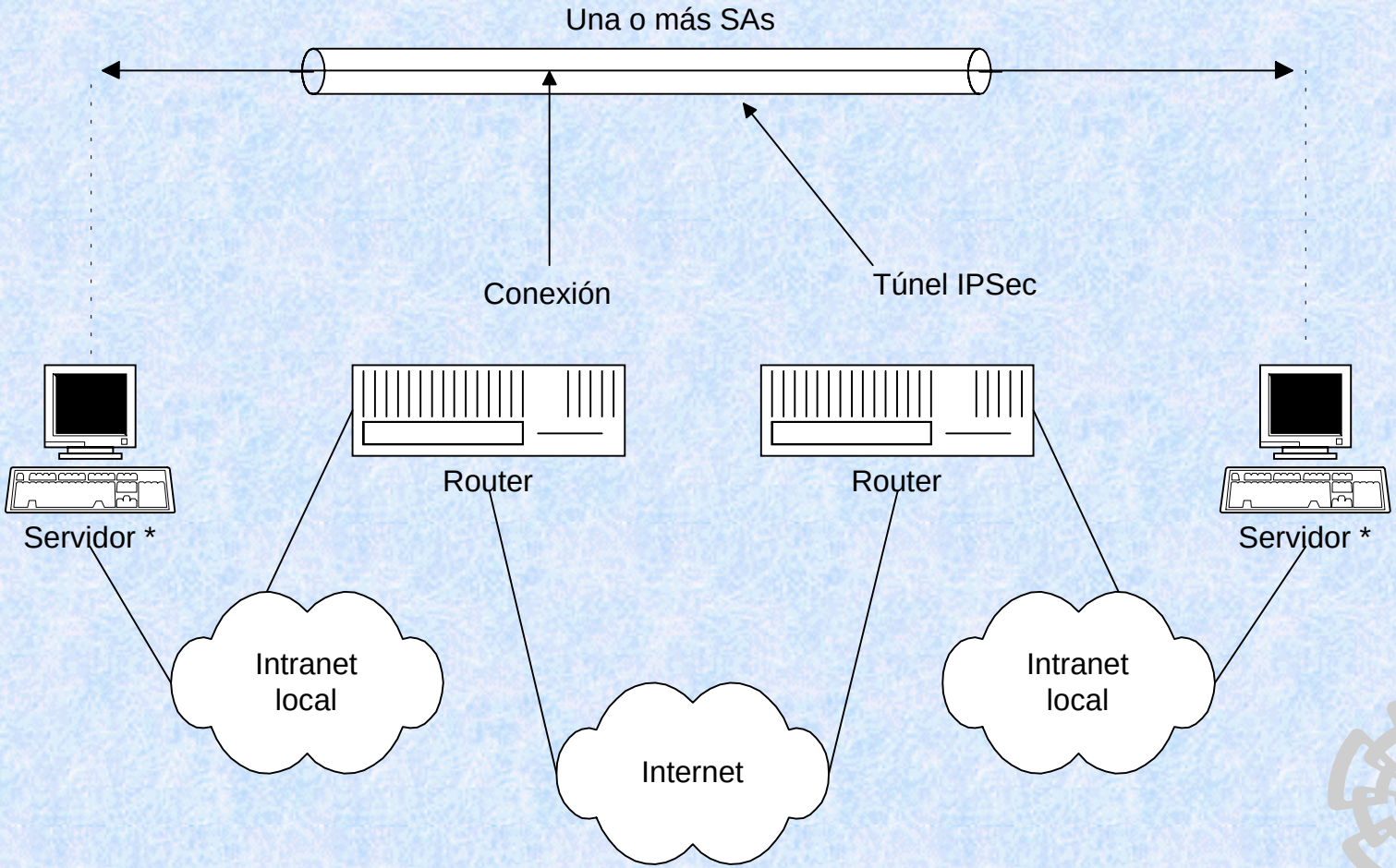
- Asegura paquetes de bajo nível creando redes seguras sobre canales inseguros.
- IPSec asegura una red completa.

* SSL opera en la capa de transporte y no necesita estar en la misma red segura.
* SSL asegura dos aplicaciones a través de una red pública.

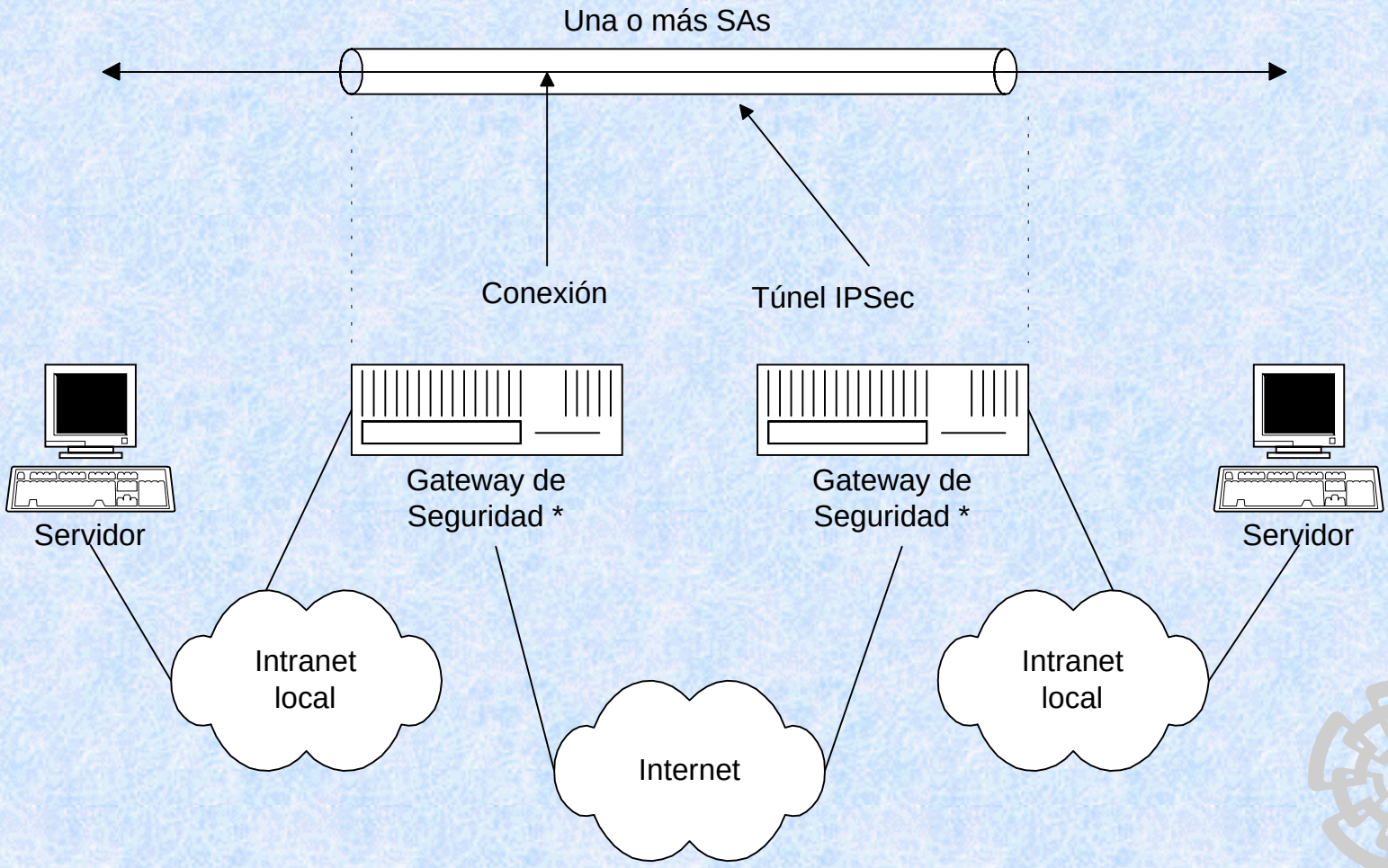
Aplicaciones

- IPSec brinda privacidad, integridad, y autentificación para el comercio electrónico.
- Satisface rigurosos requerimientos para la transmisión de información sensible en Internet.
- Al implementarse sobre las redes no se afecta a la base instalada.

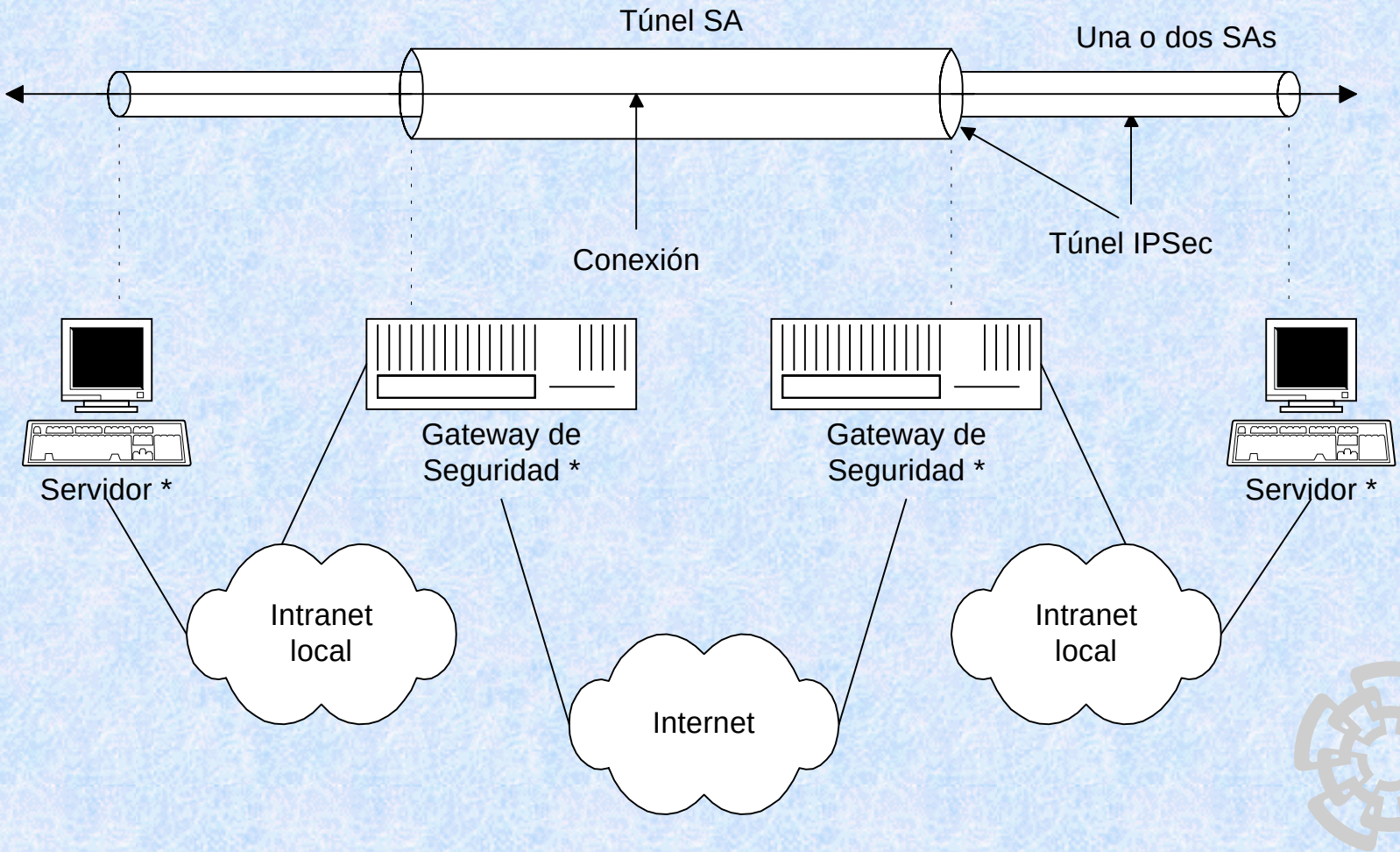
Seguridad nodo a nodo (escenario 1)



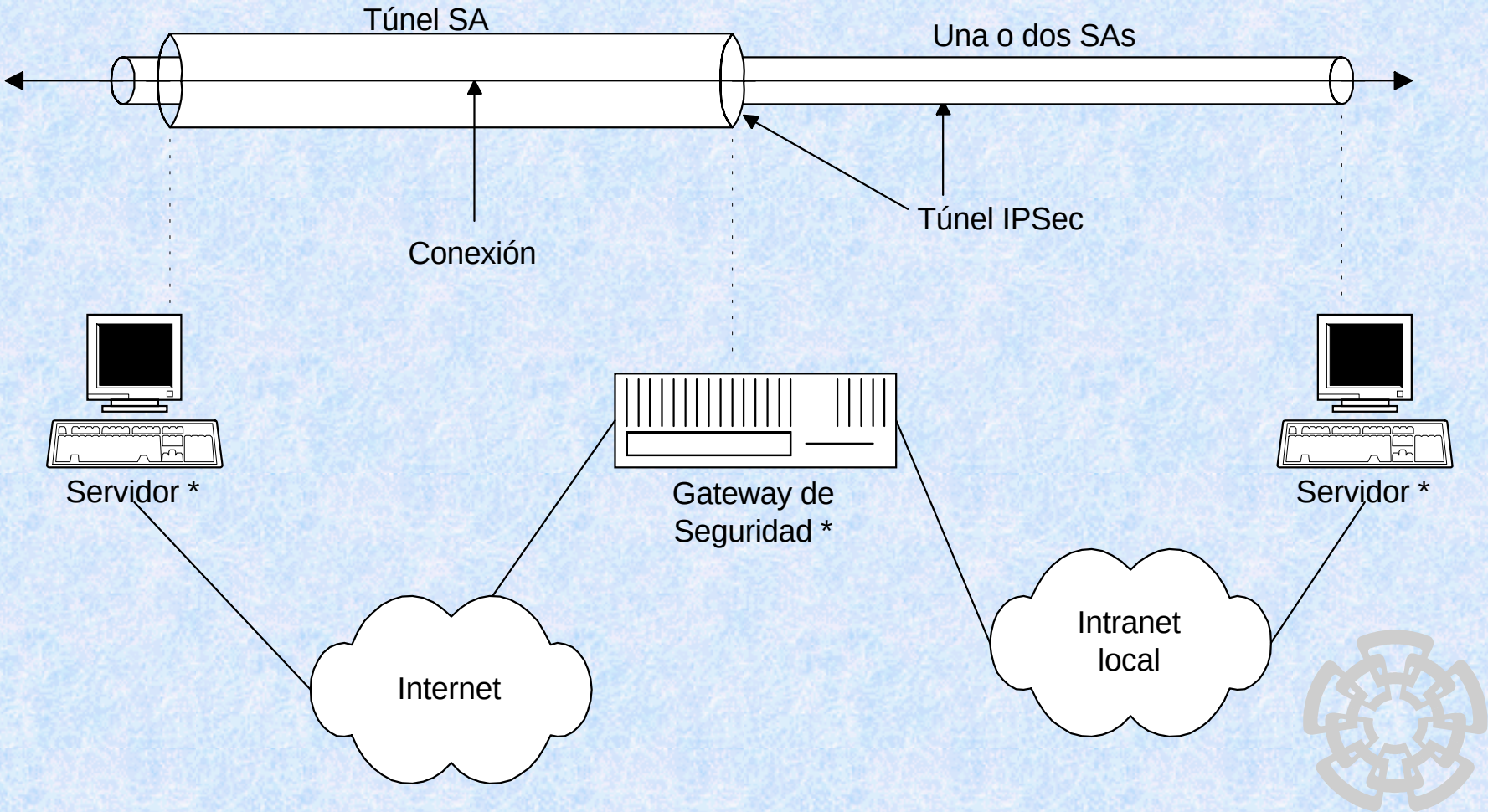
Soporte básico VPN (escenario 2)



Seguridad nodo a nodo con soporte VPN (escenario 3)



Acceso remoto (escenario 4)

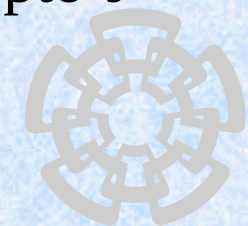


Productos

- RSA BSAFE Crypto-C y RSA BSAFE Crypto-J son productos que ofrecen un núcleo criptográfico necesario para implementar sistemas IPSec y VPN.

- CET (*Cisco Encryption Technology*) de Cisco ofrece características similares a las de IPSec.

- Corporaciones como Nortel, IBM, Raptor y Secure Computing tienen incorporados componentes de seguridad IPSec y RSA BSAFE Crypto-C o RSA BSAFE Crypto-J en sus productos.



Referencias

- Molva, Refik, Internet security architecture, *Computer Networks*, Vol. 31, No. 8, april 1999, Elsevier.
- Stallings, William, IP Security, *The Internet Protocol Journal*, Vol. 3, No. 1, march 2000, CISCO.
- Cheng, P.C., Garay, J.A., Herzberg, A. and Krawczyk, H., *A security architecture for the Internet Protocol*, IBM System Journal, Vol. 37, No. 1, 1998, IBM.
- Murhammer, M.W., Atakan, O., Bretz, S., Pugh, L.R., Suzuki, K., and Wood, D.H., *TCP/IP Tutorial and Technical Overview*, october 1998, IBM.
- Allard, J., and Nygren, S., IPSec Safety First and interoperability, *Data Communications*, june 1999, CMP.

Bibliografía reciente

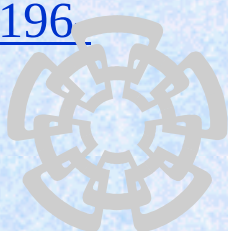
- *IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks*, Naganand Doraswamy, july 1999, Prentice-Hall,.
- *Big Book of IPSec RFCs: Ip Security Architecture*, Pete Loshin, 1999, Morgan Kaufmann, .
- *Implementing IPSec: Making Security Work on VPNs, Intranets, and Extranets (Networking Council)*, Elizabeth Kaufman, 1999, John Wiley.
- *A Technical Guide to IPSec Virtual Private Networks*, Jim S. Tiller, James s. Tiller, December 2000, Auerbach.

Recursos y vínculos relacionados

- **Para un seguimiento del estado actual del estándar IPSec**
  - The IPSec Working Group home page
    http://www.ietf.org/html.charters/ipsec-charter.html
- **Para un panorama de IPSec y de su estructura**
  - ID *IP Security Document Roadmap*
    http://www.ietf.org/internet-drafts/draft-ietf-ipsec-doc-roadmap-02.txt
  - ID *Security Architecture for the Internet Protocol*, updated May 1998
    http://www.ietf.org/internet-drafts/draft-ietf-ipsec-arch-sec-05.txt

Recursos y vínculos relacionados

- **Para informarse sobre AH y sus algoritmos**
  - ID *IP Authentication Header*, updated May 1998 http://www.ietf.org/internet-drafts/draft-ietf-ipsec-auth-header-06.txt
  - RFC 2104, *HMAC: Keyed-Hashing for Message Authentication* ftp://ftp.isi.edu/in-notes/rfc2104.txt
  - ID *The Use of HMAC-MD5-96 within ESP and AH*, updated February 1998 http://www.ietf.org/internet-drafts/draft-ietf-ipsec-auth-hmac-md5-96-03.txt
  - ID *The Use of HMAC-SHA1-96 within ESP and AH*, updated February 1998 http://www.ietf.org/internet-drafts/draft-ietf-ipsec-auth-hmac-sha196-03.txt



Recursos y vínculos relacionados

- **Para informarse sobre ESP y sus transformadas relativas**
  - RFC 1827, *IP Encapsulating Security Payload*, updated August 1995 ftp://ftp.isi.edu/in-notes/rfc1827.txt
  - ID *The ESP DES-CBC Transform*, updated July 1997 http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ciph-des-derived-01.txt

Recursos y vínculos relacionados

- **Para informarse sobre ISAKMP, Oakley, e IPSec DOI**
  - ID *Internet Security Association and Key Management Protocol (ISAKMP)*, updated March 1998 http://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-09.txt
  - ID *Revised SA negotiation mode for ISAKMP/Oakley*, updated November 1997 http://www.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-SA-revised-00.txt
  - ID *The OAKLEY Key Determination Protocol*, updated July 1997 http://www.ietf.org/internet-drafts/draft-ietf-ipsec-oakley-02.txt
  - ID *The Internet IP Security Domain of Interpretation for ISAKMP*, updated May 1998 http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ipsec-doi-09.txt

Recursos y vínculos relacionados

- **Para informarse sobre usuarios, pruebas y certificaciones**
  - The Automotive Exchange Network (ANX) http://www.aiag.org/anx
  - NIST IPSec Web-Based interoperability tester http://ipng17.ipng.nist.gov/ipsecdoc
  - The ISCA IPSec certification program

    http://www.icsa.net

Preguntas y respuestas

¡¡Gracias por su asistencia!!

Rafael Espinosa García (respinosa@cs.cinvestav.mx)

Guillermo Morales Luna (gmorales@cs.cinvestav.mx)