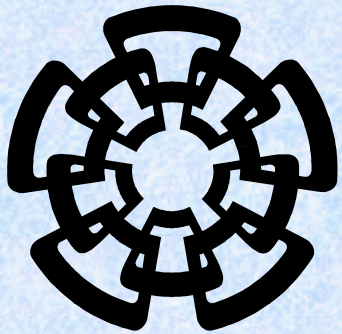


Internet y su Arquitectura de Seguridad

CINVESTAV-IPN

Departamento de Ingeniería Eléctrica

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

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

Resumen

Con el constante crecimiento de Internet (de su conectividad por supuesto), y con la aparición de nuevos servicios, la red internacional también ha dado a intrusos técnicamente avanzados la oportunidad de realizar una variedad de ataques, amenazando así la integridad de su infraestructura y violando la privacidad de los usuarios. No obstante que actualmente el entusiasmo ha sustituído a la inicial aversión de los usuarios de negocios y gubernamentales, el temor a los intrusos anónimos en Internet está forzando a la mayoría de las organizaciones a reclasificar soluciones radicales como puede ser la separación entre redes de datos privadas o Intranets y la Internet pública. La segmentación resultante se está constituyendo en un fuerte impedimento para lograrel concepto de una red Internet global. La seguridad criptográfica ofrece una alternativa viable con respecto a la segmentación, lo cual podría permitir mantener una conectividad fuertemente acoplada.

Resumen (cont.)

La organización 'Internet Engineering Task Force' (IETF), implementó mecanismos de seguridad criptográfica en varias capas del protocolo TCP/IP que permiten la protección lógica de las unidades de información transferidas sobre la red global y eliminan la necesidad de una segregación física del tráfico legitimo de ciertas porciones estratégicas de la red. Se espera que las nuevas medidas de seguridad criptográfica faciliten y simplifiquen las soluciones basadas en segmentación física y ofrezcan un medio práctico de comunicación segura sobre Internet. La segmentación usando 'firewalls' (¿cortafuegos?) y la separación física de las intranets permanecerá como una solución radical para la protección de redes corporativas contra el tráfico malicioso.
En nuestra conferencia presentamos una restropectiva acerca de las medidas de seguridad criptográfica disponibles para la infraestructura de Internet como una alternativa a la segregación física. Presentamos también la arquitectura de IPsec que incluye protocolos de seguridad en la capa de Internet, las propuestas relacionadas sobre administración de llaves, el protocolo de seguridad de la capa de transporte y puntos relativos a seguridad en el control y la administración de red.

Palabras claves: Internet; protocolos de seguridad; mecanismos criptográficos; seguridad en redes.

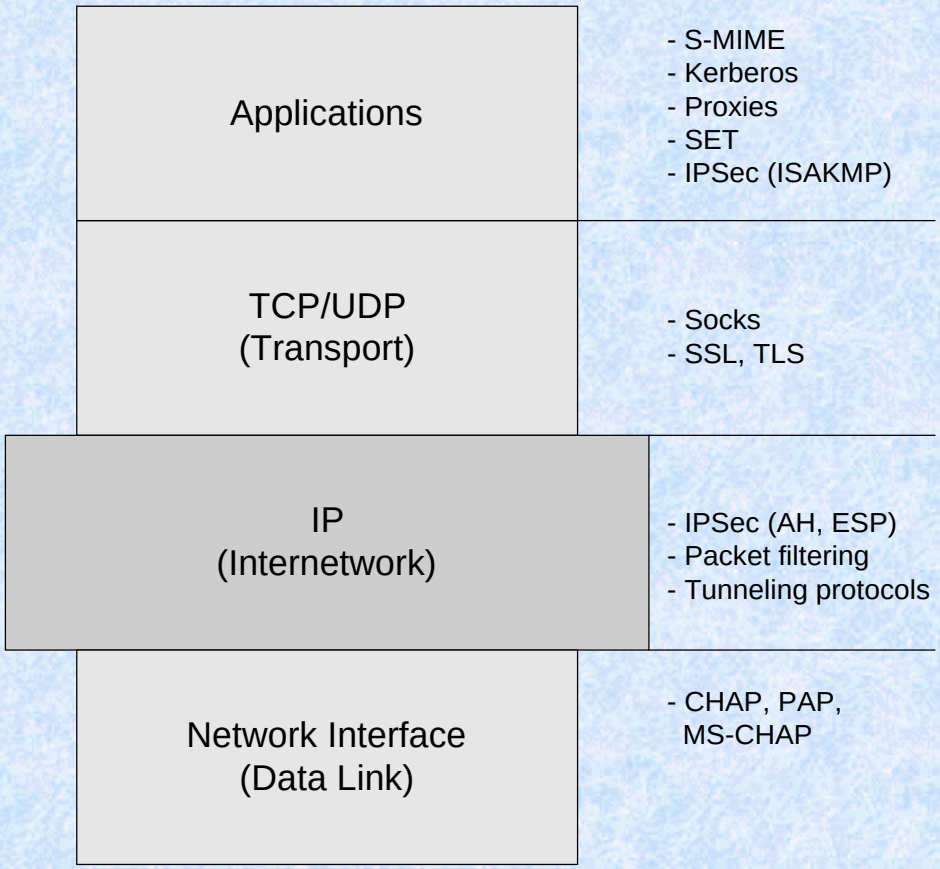
Ataques comunes

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

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

Esquemas de seguridad en las capas de TCP/IP



Arquitectura 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 un componente obligatorio en IPv6.

Conceptos IPSec

- Asociaciones de seguridad, el concepto de Security Association es una simple conexión lógica entre dos sistemas IPSec.
- Encapsulación, es una técnica común usada en redes conmutadas de paquetes, en donde una trama se transforma en una nueva

Algoritmos que usa IPSec

- Se basa en el algoritmo de Diffie-Hellman y/o RSA para intercambio de llaves.
- Encriptación asimétrica se realiza con DES y Triple-DES.
- En sistuaciones donde se requiere una mayor seguridad se usa RC5.
- Para hashing se usa el algoritmo SHA1 y MD5.

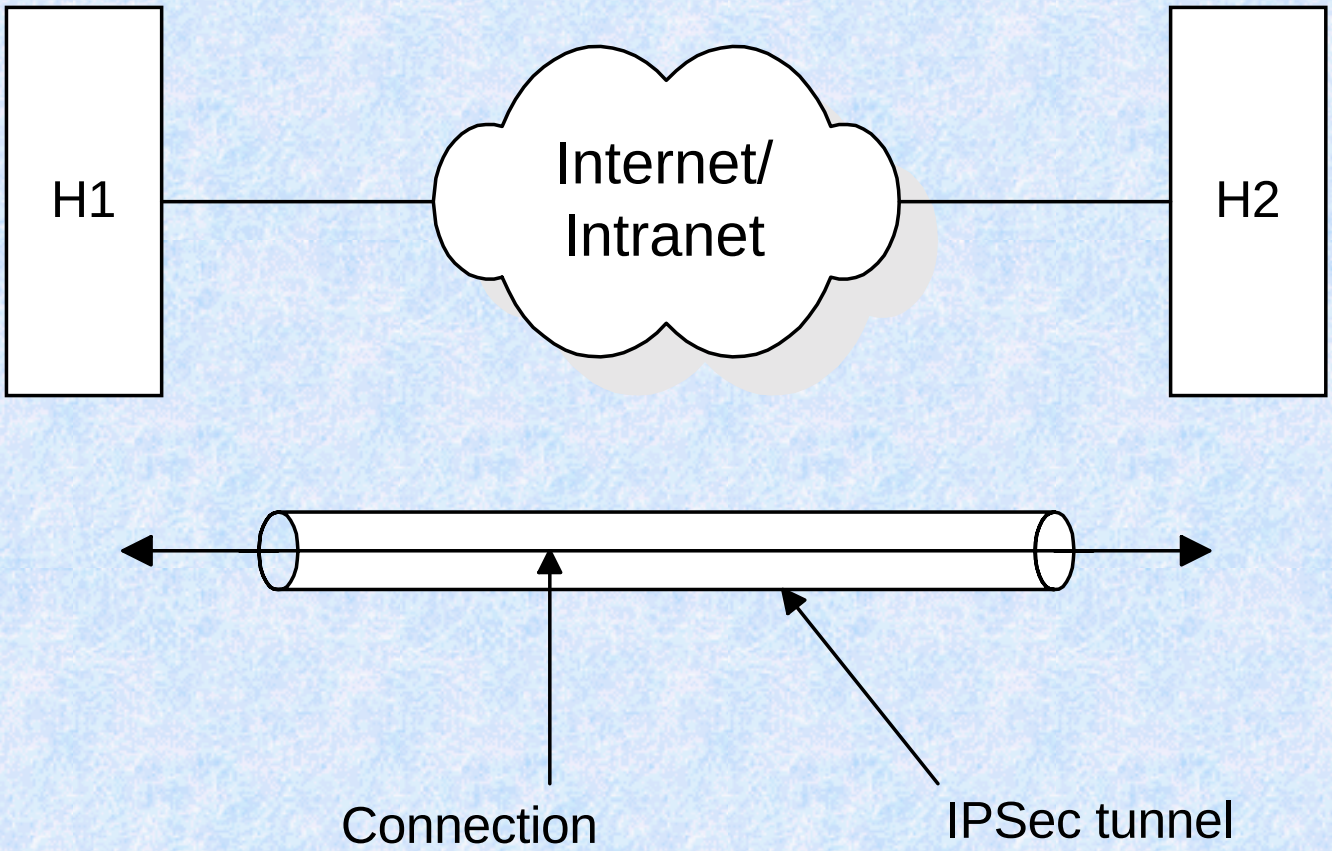
IPSec versus SSL

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

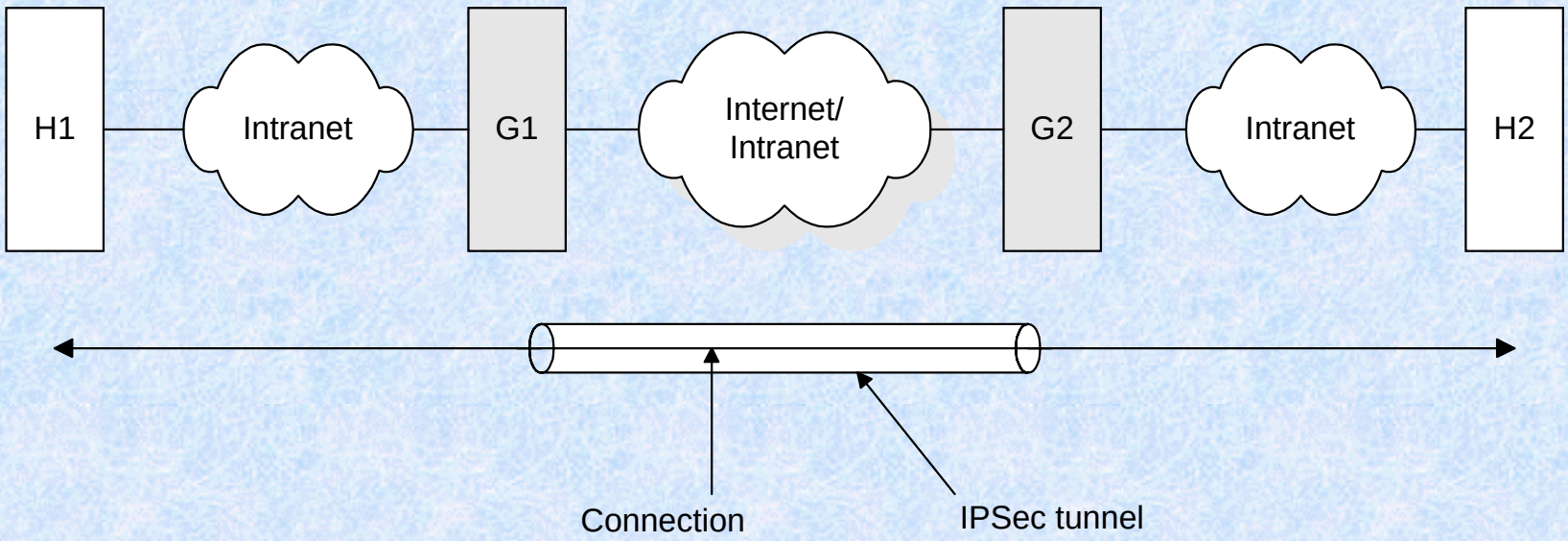
Aplicaciones

- IPSec es usado cuando es necesaria la comunicación segura sobre redes inseguras.
- Hardware y software para VPN.
- Hardware y software para acceso remoto
- Firewalls.

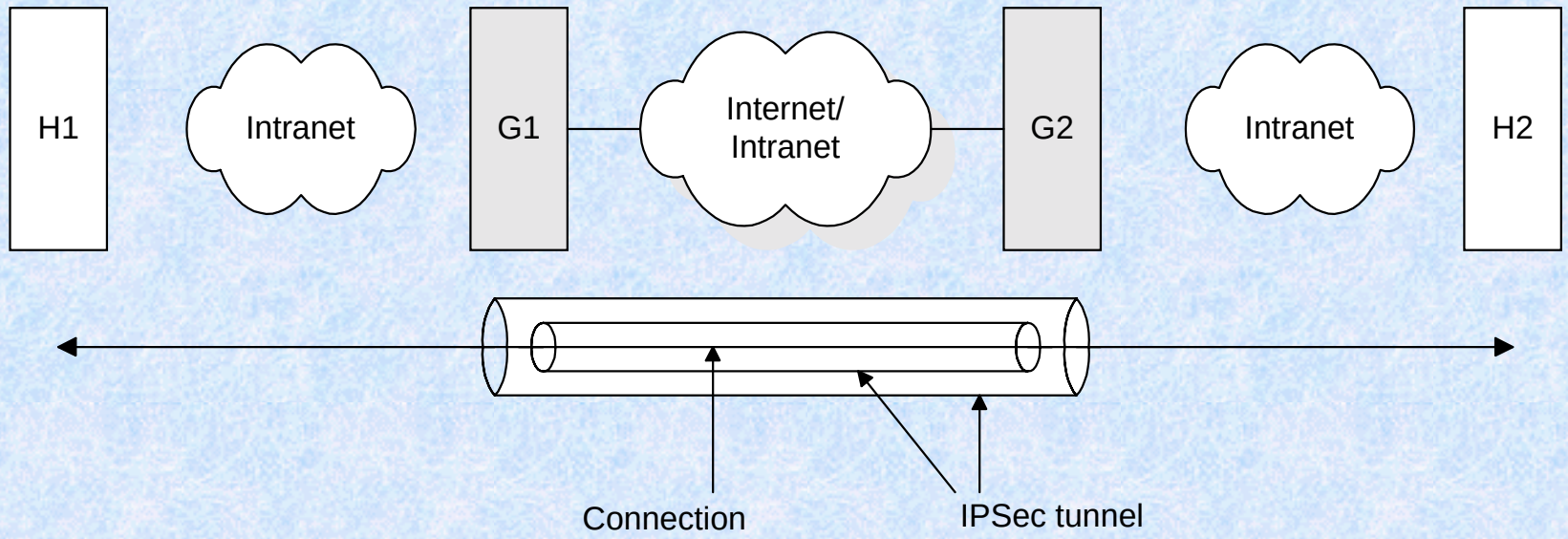
Seguridad nodo a nodo caso 1



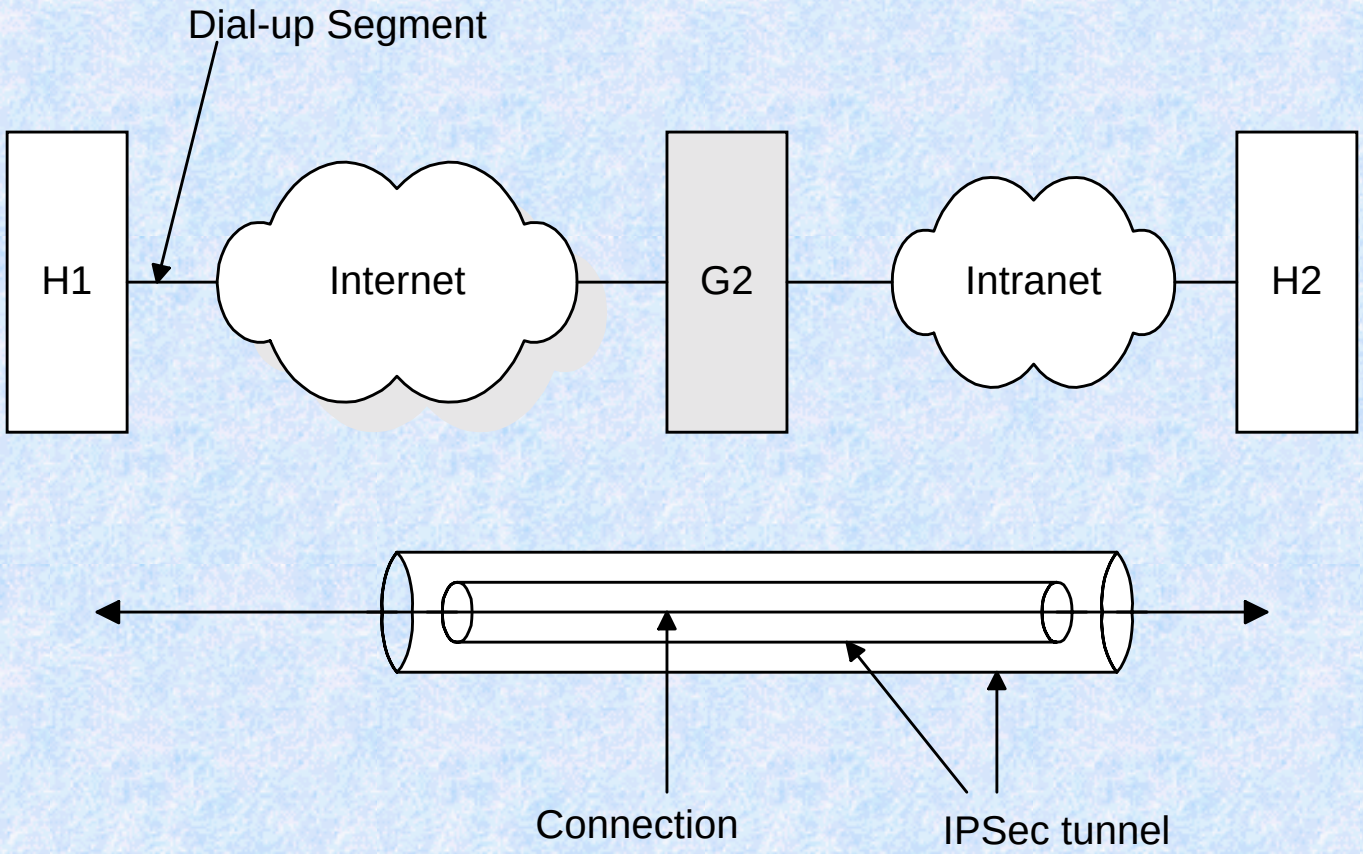
Soporte básico VPN caso 2



Seguridad nodo a nodo con soporte VPN caso 3



Acceso remoto
caso 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.
- Corporaciones como CISCO, 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.