

IPSec VPNs



IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Jesús Moreno León
Alberto Molina Coballes

Redes de Área Local

Junio 2009

¿Qué es IPSec?

Es un conjunto de protocolos cuyo objetivo es asegurar las comunicaciones IP:

- Autenticación
- Integridad
- Confidencialidad
- Protección frente ataques de Replay

Trabaja a nivel 3, por lo que puede usarse para proteger tráfico de cualquier aplicación.

Las aplicaciones no necesitan ser diseñadas para usar IPSec.



Los bloques que componen IPSec

- Protocolo de negociación:
 - ISAKMP/IKE
- Protocolo de seguridad:
 - AH, ESP
 - Cifrado:
 - DES, 3DES, AES
 - Hash:
 - MD5, SHA1
 - Protección:
 - DH, DH2, DH5...



Modos de funcionamiento

- Modo Transporte

Sólo se cifra y autentica el payload (los datos que se transmiten), dejando la cabecera IP intacta. Se usa en comunicaciones host-to-host

- Modo Túnel

Todo el datagrama IP es cifrado y autenticado, y se encapsula dentro de un nuevo datagrama IP con su nueva cabecera. Se usa para crear VPNs site-to-site o de acceso remoto.



Autenticación de dispositivos en IPSec VPN

- PreShared-Key
- Certificados
- Usuario/Contraseña. Biometría.
- Contraseñas de un sólo uso



Tipos de claves criptográficas

Simétricas

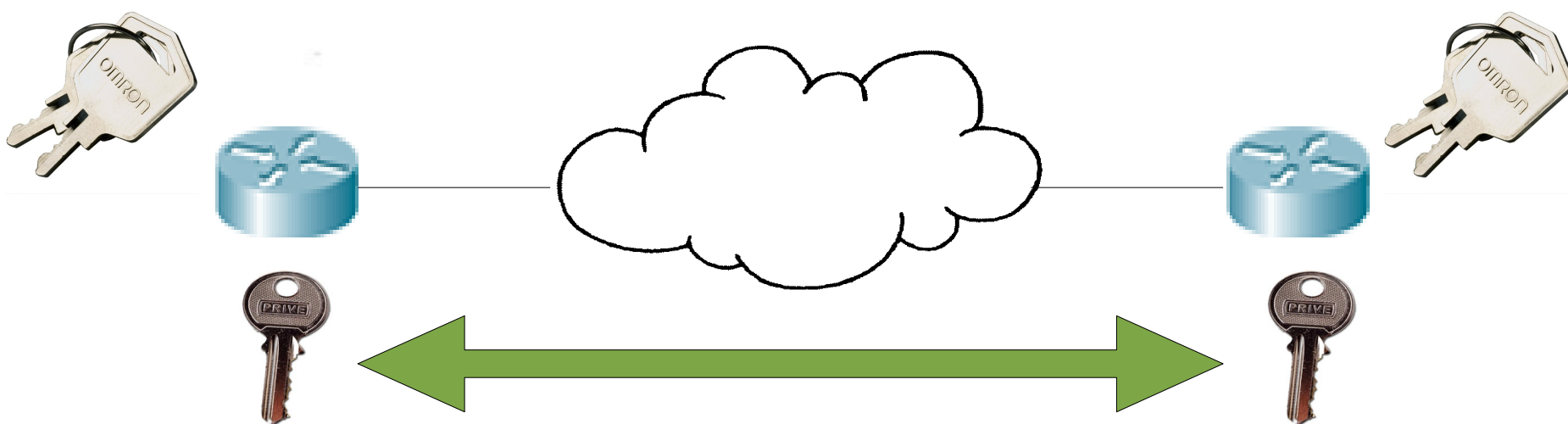


Asimétricas



¿Seguridad en una red pública? ¿Es posible?

Combinación de ambas técnicas:



Intercambiando las claves públicas, los dispositivos pueden generar e intercambiar una clave simétrica con la que cifrar toda la comunicación de esa sesión.

Algoritmos de cifrado

- DES

Creado por IBM. 56-bit key.

- 3DES


Ampliamente utilizado. Usa 3DES keys sobre cada bloque de datos. 168-bit key.

- AES

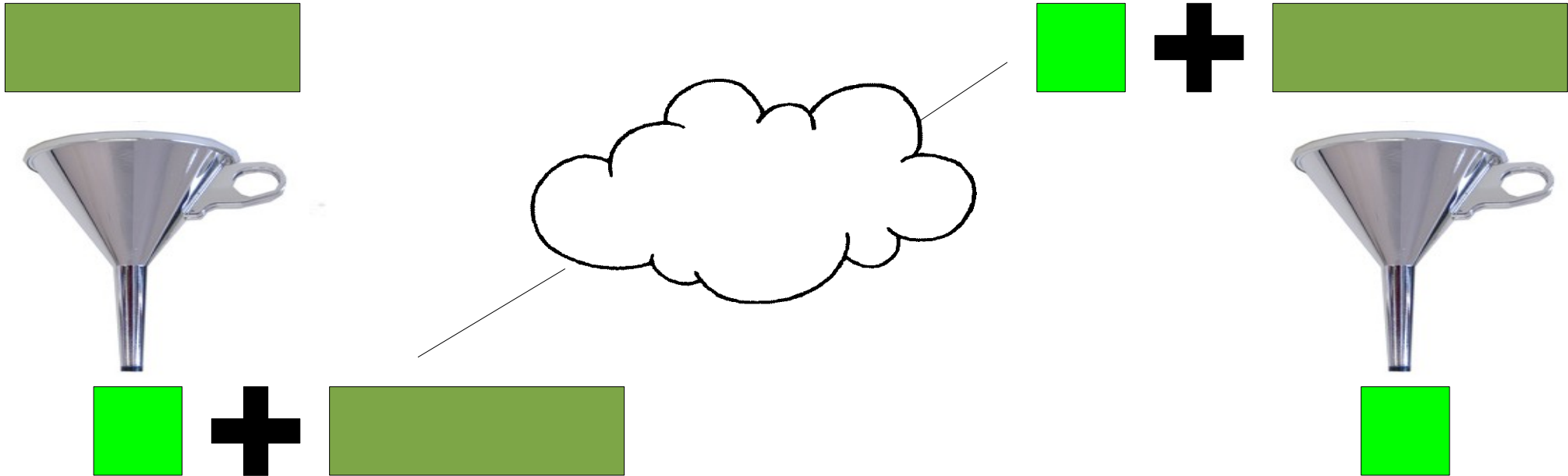
Más moderno y eficiente. 128, 192 y 256-bit key.

- RSA

Rivest, Shamir and Adleman. Primer algoritmo capaz de cifrar y firmar. Gran avance para la criptografía de clave pública. 512, 1024 bit key.



Integridad



Algoritmos de Hash

- MD5
- SHA-1



IKE Fase 1

IKE: Internet Key Exchange, es el protocolo que se usa para establecer una Asociación de Seguridad (SA).

El objetivo de la Fase 1 es establecer un canal seguro de comunicaciones para poder intercambiar una clave simétrica con la que cifrar la sesión.



Mensaje 1: Negociación de la política

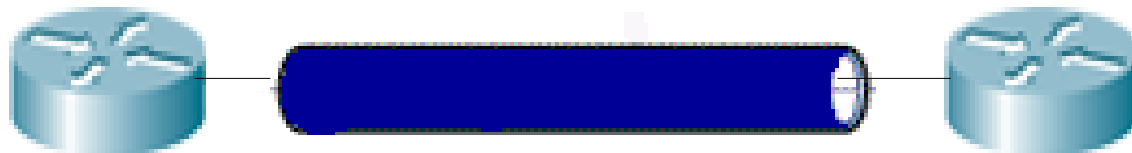
Mensaje 2: Intercambio de DH Keys (RSA).

Mensaje 3: Verificación de la identidad (shared secret o certificados)

IKE Fase 2

Las claves simétricas IPSec son negociadas e intercambiadas.

Ya tenemos formada la Asociación de Seguridad (SA).



IKE Fase 1.5

XAuth – Extended Authentication

RADIUS, Controlador de Dominio

Mode Config

Configuración IP...

