SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

4.2.1.MF0489_3. Capítulo 3
Parte 1
Comunicaciones seguras

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Uno de los usos más importantes de los algoritmos criptográficos es el establecimiento de comunicaciones seguras.

Red Privada Virtual (VPN).

Protocolos:

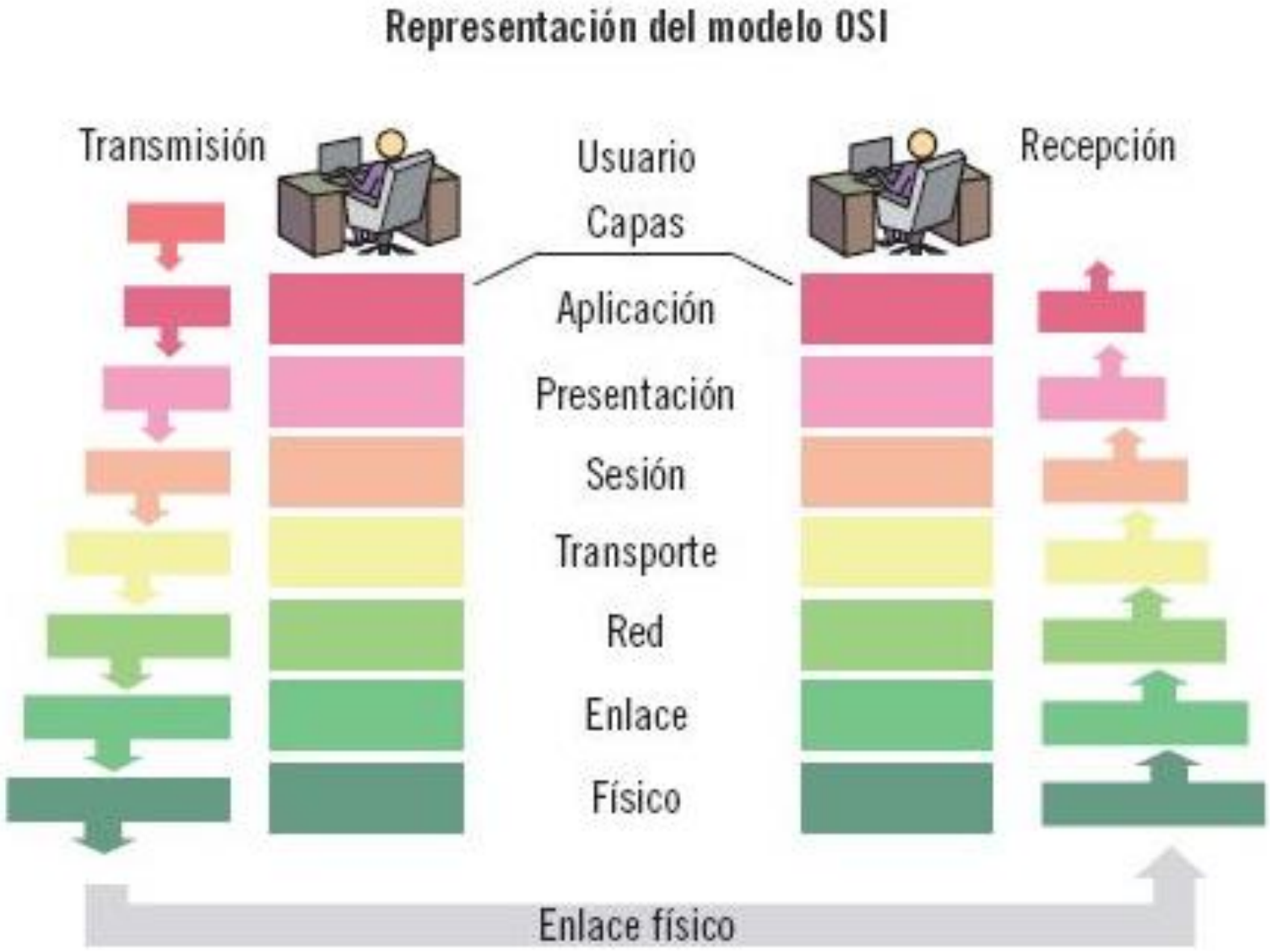
- **IPSec**
- **SSL**
- **SSH**

2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE VPN

Las redes privadas virtuales, habitualmente llamadas VPN (del inglés Virtual Private Network), son un tipo de red de comunicaciones que se construye sobre otra física ya existente.

La característica fundamental es que pueden permitir que distintos equipos en diversas partes del mundo puedan comunicarse como si estuviesen en una red de área local.

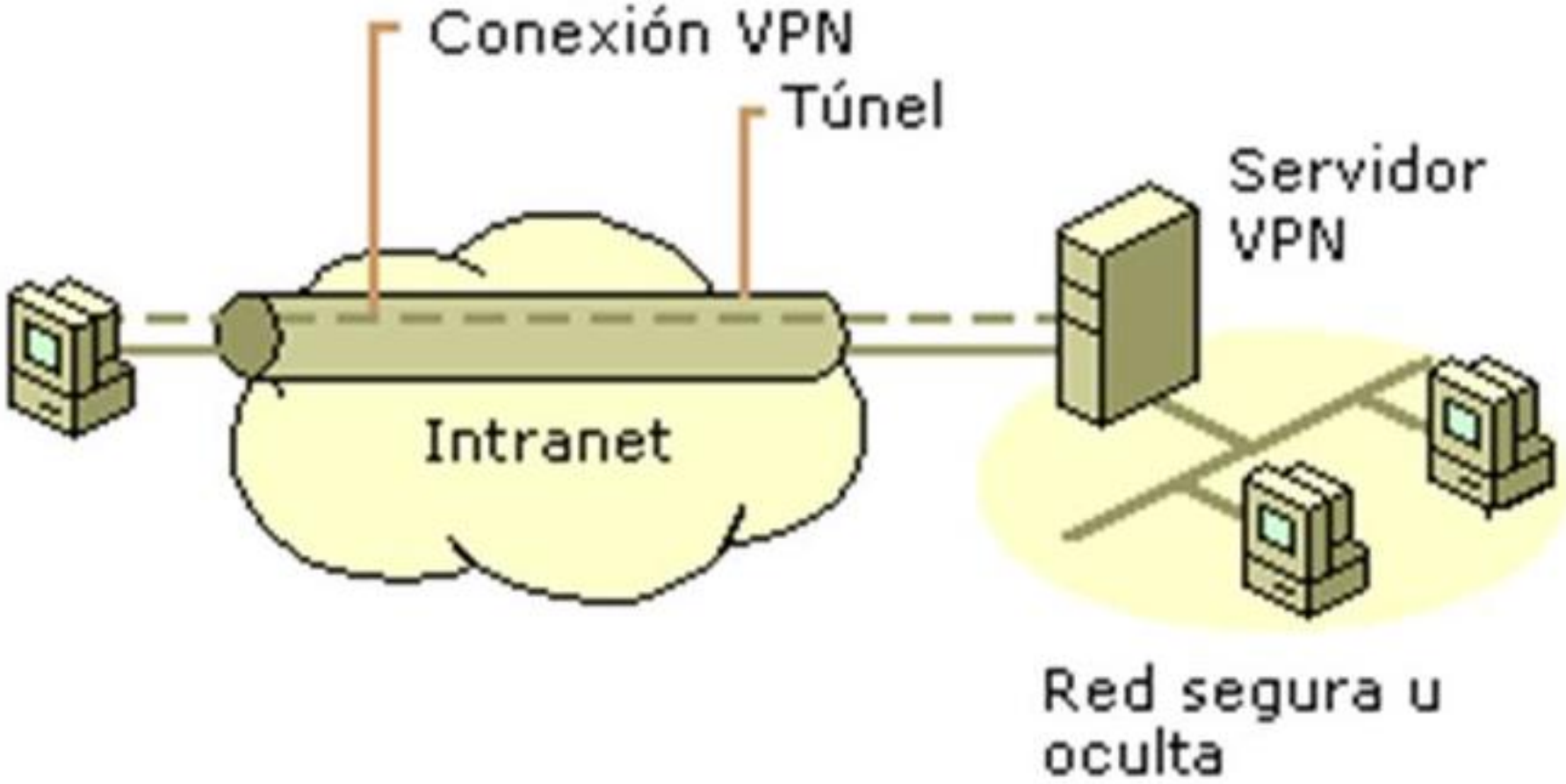
2.1. CONCEPTOS PREVIOS. EL MODELO OSI



2.1. CONCEPTOS PREVIOS. EL MODELO OSI

Para conseguir que un equipo de una red se comporte como si fuese de otra, una de las técnicas utilizadas más habituales es el encapsulado de protocolos.

2.2. DESCRIPCIÓN DE LAS VPN



2.2. DESCRIPCIÓN DE LAS VPN

Para poner en marcha una VPN se utilizan protocolos de tunelado.

Los principales protocolos a través de los cuales se puede establecer una VPN son los siguientes:

- **IPSec (Internet Protocol Security).**
- **SSL (Secure Socket Layer).**
- **SSH (Secure Shell).**
- **PPTP (Point-to-Point Tunnelling Protocol).**
- **L2TP (Layer 2 Tunnelling Protocol).**
- **DTLS (Datagram Transport Layer Security).**

2.3. VENTAJAS Y DESVENTAJAS DE LAS VPN

Ventajas:

- **Bajo coste de despliegue.**
- **Transparencia de comunicación.**
- **Seguridad en los sistemas.**
- **Simplicidad administrativa.**

2.3. VENTAJAS Y DESVENTAJAS DE LAS VPN

Inconvenientes:

- **Fiabilidad de la red.**
- **Velocidad de acceso.**
- **Confianza de las entidades.**
- **Incompatibilidad de las redes.**

3. PROTOCOLO IPSEC

IPSec (Internet Protocol Security) es un conjunto de protocolos habitualmente usados para crear VPN.

Actúa en el nivel de red (nivel 3 del modelo OSI).

Protocolos que forman IPSec:

- **Internet Key Exchange (IKE).**
- **Encapsulating Security Payload (ESP).**
- **Authenticated Header (AH). Obsoleto.**

3.1. INTERNET KEY EXCHANGE (IKE)

Este protocolo permite establecer una asociación de seguridad entre las dos partes comunicantes.

La asociación de seguridad establece los parámetros que permitirán a las dos entidades comunicarse de forma segura.

Se determina el algoritmo criptográfico a utilizar y su modo de operación junto con la clave de cifrado para los datos que se intercambien.

3.1. INTERNET KEY EXCHANGE (IKE)

En IKE, los intercambios de mensajes entre las partes se realizan por pares, de forma que a un envío (“pregunta”) de una entidad le sigue otro (“respuesta”) de su contraria.

En el caso de que no se reciba respuesta, es responsabilidad del emisor repetir la pregunta o, en su caso, abandonar el protocolo.

3.1. INTERNET KEY EXCHANGE (IKE)

Habitualmente se producen dos intercambios:

IKE_SA_INIT: se intercambian valores aleatorios y ejecutan el algoritmo Diffie-Hellman para establecer una clave compartida. Esa clave se toma como base (denominada semilla) para derivar de ella otras dos claves: una para cifrar y otra para autenticar los mensajes haciendo uso de funciones hash con clave.

Este intercambio es muy simple: el emisor propone una serie de algoritmos criptográficos y el receptor contesta escogiendo uno de ellos (o devolviendo un error, si ninguno de ellos es adecuado).

IKE_AUTH: en esta fase se autentican mutuamente los comunicantes y se establece la asociación de seguridad que se utilizará en ESP.

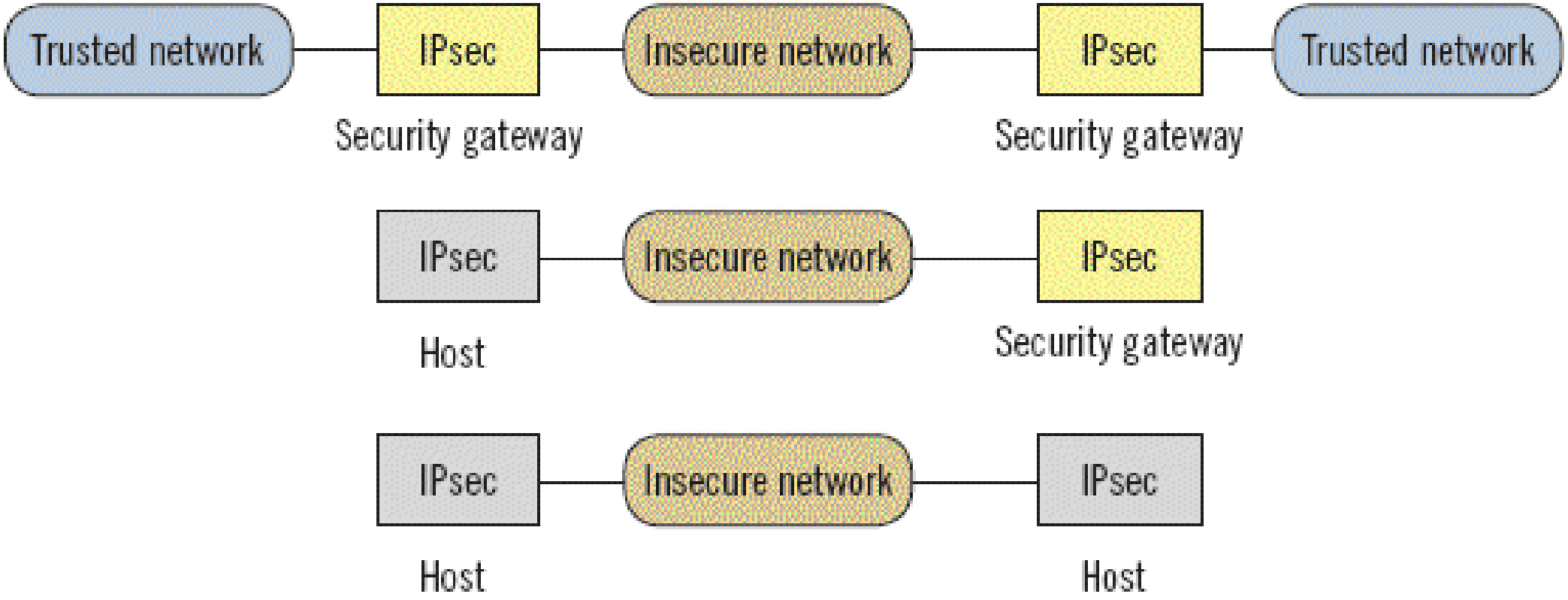
3.2. ESCENARIOS DE USO

Según la configuración física o el tipo de protección que se aplique, es posible establecer las siguientes clasificaciones acerca de los escenarios de uso de IPSec:

- Según la configuración física.
- Según el tipo de protección.

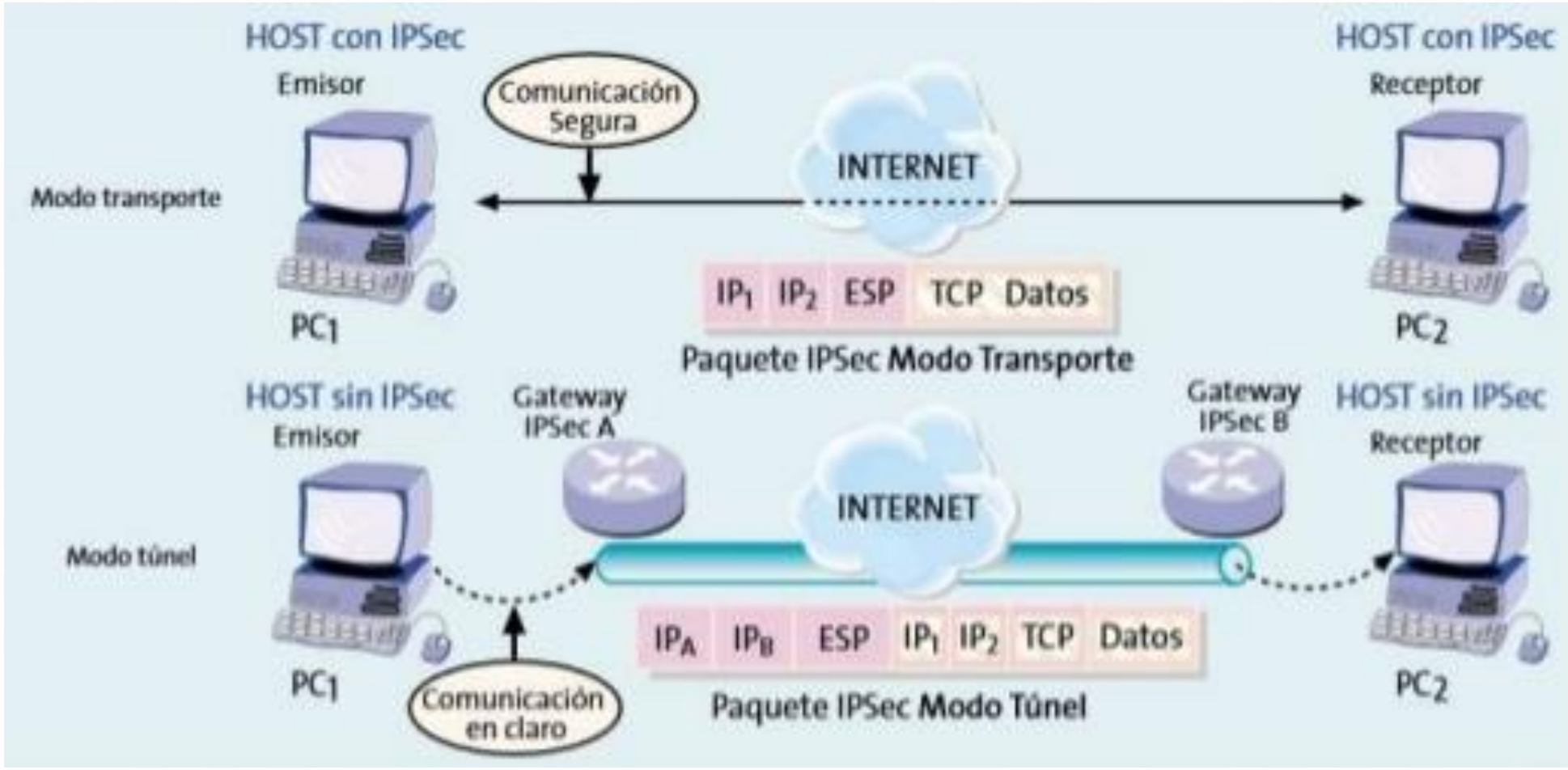
3.2. ESCENARIOS DE USO

Según la configuración física



3.2. ESCENARIOS DE USO

Según el tipo de protección



Ejemplo.

UNA MULTINACIONAL DEDICADA A LA GESTIÓN BANCARIA HA DECIDIDO QUE, POR CONTRATO, TODOS SUS EMPLEADOS TENDRÁN DERECHO A UN DÍA SEMANAL DE TRABAJO EN CASA. SIN EMBARGO, TODOS ELLOS HAN DE REALIZAR LAS MISMAS OPERACIONES QUE REALIZAN EN LA OFICINA. PARA ELLO, EL EQUIPO DE INFORMÁTICOS DE LA EMPRESA HA INDICADO LA NECESIDAD DE UTILIZAR EL PROTOCOLO IPSEC PARA QUE LOS USUARIOS PUEDAN CONECTARSE DESDE SU CASA A LA OFICINA. ADEMÁS, HAN INSTALADO UN EQUIPO INTERMEDIARIO EN LA SEDE BANCARIA PARA QUE TODOS SE CONECTEN A ÉL. ¿QUÉ CONFIGURACIÓN FÍSICA Y TIPO DE PROTECCIÓN SON MÁS ADECUADOS?

Ejemplo. Solución.

DADO QUE TODOS LOS EQUIPOS SE CONECTAN AL INTERMEDIARIO, LA CONFIGURACIÓN FÍSICA MÁS ADECUADA ES AQUELLA EN LA QUE UN EXTREMO ES EL EQUIPO FINAL (EL ORDENADOR DEL EMPLEADO) Y OTRO ES EL INTERMEDIARIO (EL EQUIPO DE LA EMPRESA).

EL TIPO DE PROTECCIÓN MÁS ADECUADO EN ESTOS CASOS ES EL MODO TÚNEL.

3.3. ENCAPSULATING SECURITY PAYLOAD (ESP)

El protocolo ESP se encarga de proporcionar confidencialidad, autenticación e integridad de la información en tránsito.

- **identificador de la asociación de seguridad**
- **número de secuencia**
- **vector de inicialización (si se requiere)**
- **carga útil (más relleno)**

4. PROTOCOLOS SSL Y SSH

SSH y SSL permiten construir un túnel confidencial por el que enviar los datos de forma segura, además de verificar la integridad de los datos transmitidos.

En SSH lo más habitual es que la autenticación se realice utilizando usuario y contraseña y en SSL se utilicen certificados.

4.1. SECURE SOCKETS LAYER (SSL)

El protocolo SSL fue diseñado originalmente por Netscape. (https://es.wikipedia.org/wiki/Netscape_Communications_Corporation)

1996 SSL 3.0. Primera versión comercial (TLS)

4.1. SECURE SOCKETS LAYER (SSL)

El protocolo SSL trabaja por encima del nivel de transporte (nivel 4 del modelo OSI).

Soporta compresión (aunque es opcional) y hace uso de certificados X.509 v3.

Proporciona los servicios de seguridad de autenticación en servidor (obligatoria), autenticación en cliente (opcional), integridad, confidencialidad y no repudio del cliente (opcional).

4.1. SECURE SOCKETS LAYER (SSL)

4.1. SECURE SOCKETS LAYER (SSL)

SSL está formado por varios subprotocolos:

- **Protocolo de salutación**
- **Protocolo de registro.**
- **Protocolo de cambio de especificación de cifrado.**
- **Protocolo de aviso.**

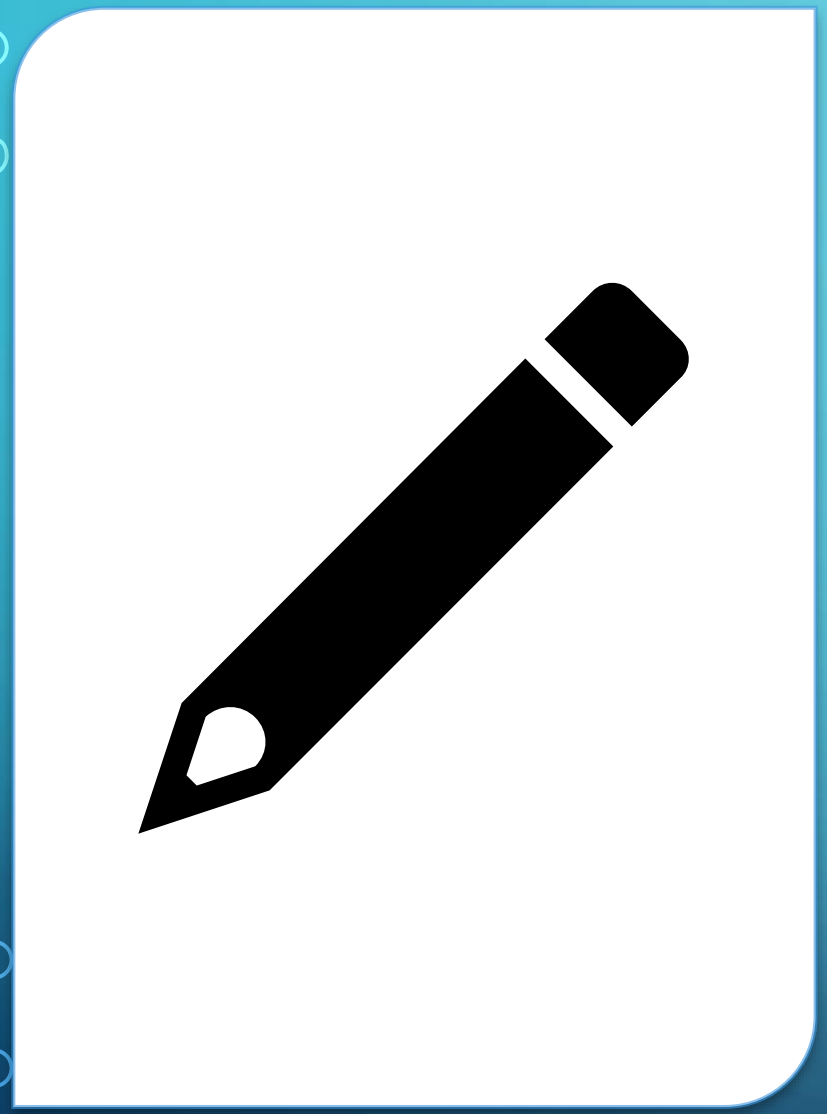
4.1. SECURE SOCKETS LAYER (SSL)

Variante de SSL. SSL Extended Validation (EV-SSL)

Validar correctamente el certificado digital.

EV-SSL es exactamente igual a SSL en sus fases y funcionamiento, pero impone restricciones adicionales sobre los certificados. Particularmente, se destacan las siguientes:

- Las Autoridades de Certificación están obligadas a pasar una auditoría periódica, que verifique el rigor del proceso de emisión de certificados.
- Para los certificados que se emiten a páginas web, solo se emiten si lo solicita la persona responsable del dominio o con control exclusivo sobre él.
- Las Autoridades de Certificación deben implementar el protocolo OCSP, de forma que el navegador pueda comprobar inmediatamente la vigencia del certificado.
- Los certificados se emiten con una política de certificación distinta que permite a los navegadores reconocer este tipo de certificados.



Ejemplo.

LUCÍA ES CONTRATADA POR UNA EMPRESA DE ALOJAMIENTO DE PÁGINAS WEB. EN DICHA EMPRESA HAN INSTALADO UN NUEVO SERVIDOR QUE HACE USO DEL PROTOCOLO SSL.

LA MISIÓN DE LUCÍA ES DETERMINAR SI SSL PERMITE RESOLVER TRES NECESIDADES DE LA EMPRESA:

(1) ¿SE PODRÁ AHORA PERMITIR QUE LOS CLIENTES ACCEDAN A LAS PÁGINAS ESTANDO SEGUROS DE QUE NADIE PUEDE ESPIAR LOS DATOS QUE INTERCAMBIAN?

(2) ¿PODREMOS ESTAR SEGUROS DE QUIÉN ACCEDE AL PORTAL?

(3) SI UNA DE ESAS PÁGINAS ES UN BANCO, ¿SE PUEDE GARANTIZAR QUE SI SE ORDENA UNA TRANSFERENCIA, NADIE HA MANIPULADO LA CANTIDAD INDICADA POR EL CLIENTE?

¿PODRÍA AYUDAR A LUCÍA A DETERMINAR SI SE CUMPLEN O NO ESTAS NECESIDADES?

Ejemplo. Solución.

LA PRIMERA NECESIDAD QUEDA CUBIERTA POR SSL, PUES EL INTERCAMBIO DE INFORMACIÓN SE REALIZA CIFRADO ENTRE EL CLIENTE Y EL SERVIDOR. ASÍ, NO HAY POSIBILIDAD DE QUE NADIE ESPÍE EL CONTENIDO DE LA COMUNICACIÓN.

LA SEGUNDA NECESIDAD PUEDE CUMPLIRSE SI EN LA EMPRESA CONFIGURAN SSL PARA QUE AUTENTIQUE AL CLIENTE. DEBE RECORDARSE QUE ESTO ES UNA CUESTIÓN OPCIONAL EN SSL, POR LO QUE, AUNQUE ESTÁ PERMITIDO, SE OFRECE SOLO SI ASÍ SE INDICA.

FINALMENTE, LA TERCERA NECESIDAD TAMBIÉN QUEDA CUBIERTA. COMO SE DIJO ANTERIORMENTE, EL PROTOCOLO DE SALUTACIÓN PERMITE ACORDAR LA FUNCIÓN DE CONTROL DE INTEGRIDAD QUE DEBE APLICARSE. DE ESTA MANERA SE PREVIENEN MANIPULACIONES DE LA INFORMACIÓN TRANSMITIDA.