SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

4.2.1.MF0489_3. Capítulo 3
Parte 2
Comunicaciones seguras

JOSÉ PABLO HERNÁNDEZ

4.2. SECURE SHELL (SSH)

Secure Shell (SSH) es un protocolo diseñado con los propósitos de ser simple y fácil de programar.

El propósito era reemplazar al popular protocolo TELNET y a otros esquemas que no proporcionaban seguridad.

4.2. SECURE SHELL (SSH)

SSH se compone de tres tipos de protocolos:

- **Protocolo de la capa de transporte,**
- **Protocolo de autenticación de usuarios y**
- **Protocolo de conexión.**

4.2. SECURE SHELL (SSH)

Protocolo de la capa de transporte

Este protocolo proporciona autenticación de las entidades y de los mensajes, confidencialidad e integridad de los datos.

Dentro de este protocolo se establecen las claves de los Host. La autenticación del servidor se realizar en base al par o pares de claves (público-privada) que dicho servidor posee.

4.2. SECURE SHELL (SSH)

Protocolo de la capa de transporte

Para autenticar al servidor, el cliente dispone de dos opciones de acuerdo a la especificación de la RFC 4251:

- El cliente puede mantener localmente una base de datos que asocie cada nombre de host con su clave pública.
- La asociación nombre de host-clave pública es certificada por una autoridad.

4.2. SECURE SHELL (SSH)

Protocolo de autenticación de usuarios

Este protocolo autentica a los usuarios frente al servidor y está pensado para ejecutarse sobre protocolos que proporcionen confidencialidad e integridad.

Métodos de autenticación:

- método de clave pública
- método de contraseña
- método hostbased

4.2. SECURE SHELL (SSH)

Protocolo de conexión

Funciona sobre el Protocolo de la capa de transporte y permite que una misma conexión pueda ser utilizada a la vez para distintos propósitos, conocidos como canales. Un canal puede servir, por ejemplo, para ejecutar órdenes en un ordenador remoto (canal de sesión) o para usar en remoto sus programas que utilizan representación gráfica (por ejemplo, ventanas en un sistema Windows) (canal x11).

4.2. SECURE SHELL (SSH)

Protocolo de conexión

Un canal pasa por tres estados distintos en función del momento de transmisión de datos:

- Apertura del canal.
- Transmisión de los datos.
- Cierre del canal.

5. SISTEMAS SSL VPN

SSL VPN es una forma de utilizar VPN en la que se utiliza el navegador web para establecer la conexión entre dos extremos.

Una de las características más relevantes es que en SSL VPN no se requiere instalación de ningún cliente en el ordenador del usuario final.

Un ejemplo de su utilización es la conexión desde el navegador de un ordenador personal al ordenador corporativo de la empresa, de modo que una vez establecida la VPN se consiga la misma seguridad que estando físicamente en el equipo.

5. SISTEMAS SSL VPN

Las SSL VPN presentan posibles riesgos:

- SSL VPN no requiere la instalación de ningún software en el cliente.
- Otro de los riesgos se asocia con la información almacenada en los historiales.
- Como no se requiere la instalación de ningún software en el cliente, cualquier usuario con acceso a la web puede acceder a una VPN SSL.

5.1. TIPOS DE SSL VPN

VPN SSL portal

Permiten a los usuarios establecer una única conexión SSL con un sitio web para poder acceder remotamente y de forma segura a distintos servicios de red.

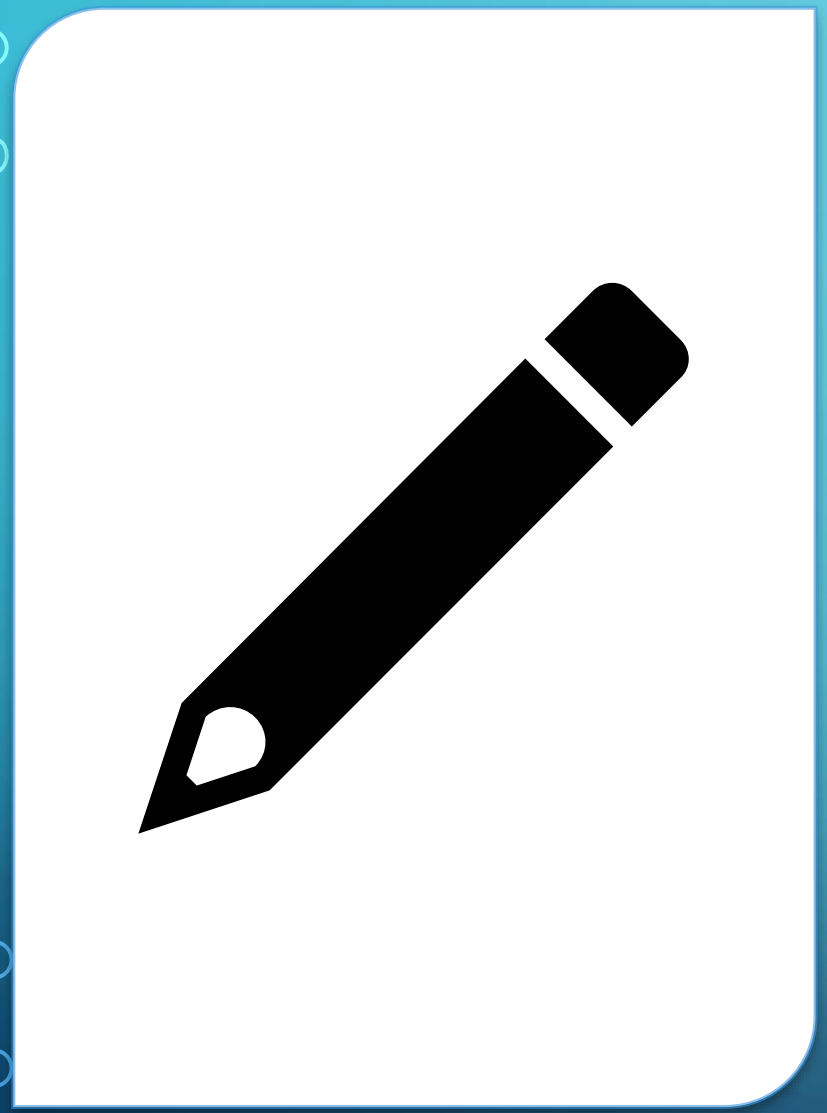
El funcionamiento es muy sencillo: el usuario accede a una página web, la cual es una puerta de entrada a los servicios, de ahí el nombre de portal.

Posteriormente, tras el acceso se produce la autenticación y, tras ello, dicha página web presenta los servicios a los que el usuario tiene acceso.

5.1. TIPOS DE SSL VPN

SSL VPN túnel

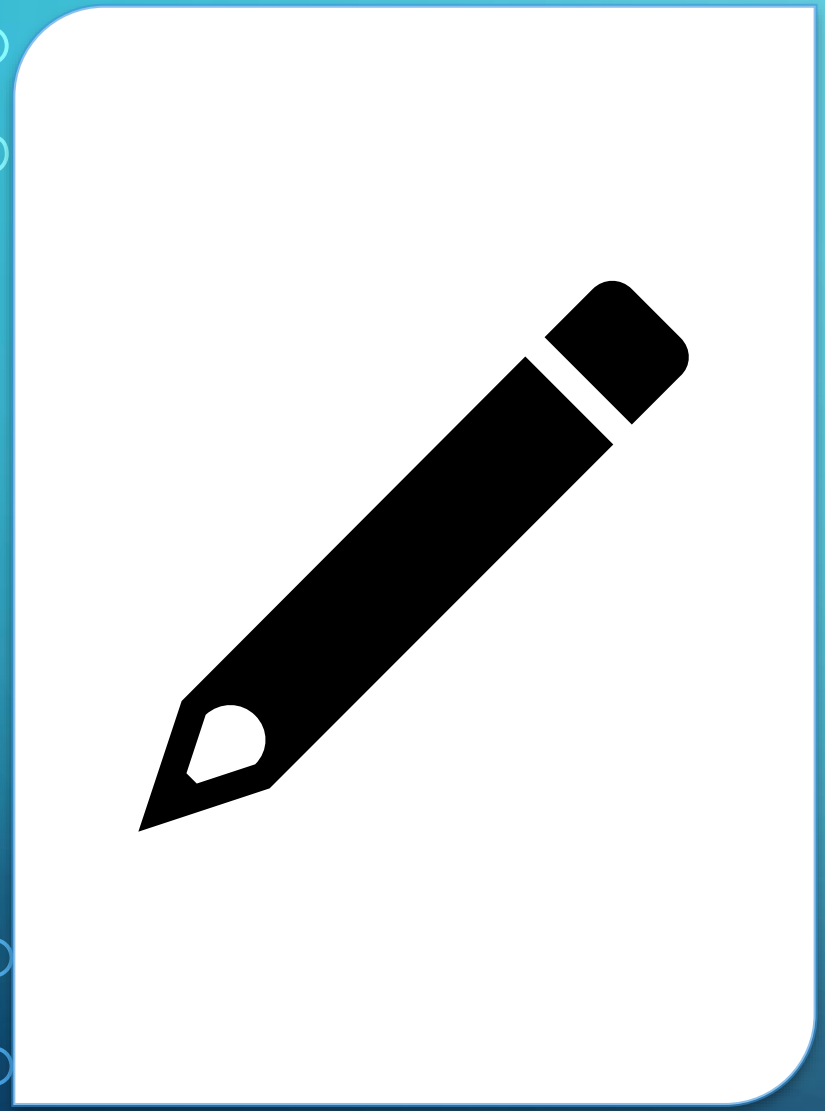
Permite a los usuarios usar un navegador web para acceder de forma remota y segura a múltiples servicios web utilizando un túnel que hace uso de SSL. En este caso, se necesita que el navegador soporte, entre otros, el uso de Java, JavaScript, ActiveX, aplicaciones Flash o plugins.



Ejemplo.

UNA GRAVERA DESEA EXTERNALIZAR SU SERVICIO DE CUSTODIA DE DOCUMENTOS DIGITALES. PARA ELLO, CONTRATAN UN SERVICIO DE GESTIÓN DOCUMENTAL ELECTRÓNICA, SGDELEC, QUE PERMITE QUE LA GRAVERA PUEDA TRANSFERIR SUS FACTURAS AL SERVIDOR DE SGDELEC. DADA LA SITUACIÓN ECONÓMICA, SGDELEC TIENE SU OFERTA DE BAJO COSTE, EN EL QUE SU SERVIDOR NO DISPONE DE UN CERTIFICADO ELECTRÓNICO PARA AUTENTICARSE.

EL DIRECTOR DE TI DE LA GRAVERA CONSULTA CON NEREA CUÁL DE LAS PRINCIPALES OPCIONES DE COMUNICACIÓN SEGURA ES MÁS ADECUADA: IPSEC, SSL O SSH. ¿CUÁL CREE QUE ES LA RECOMENDACIÓN DE NEREA?



Ejemplo. Solución.

EN EL ENTORNO DESCRITO, EXISTE LA NECESIDAD DE ESTABLECER UNA COMUNICACIÓN SEGURA ENTRE EMPRESAS QUE SON DISTINTAS E INDEPENDIENTES, SOLO UNIDAS POR UN CONTRATO DE PRESTACIÓN DE SERVICIOS. ESTA SITUACIÓN ES MUY DISTINTA DEL ESCENARIO DE APLICACIÓN HABITUAL DE IPSEC, DONDE SE BUSCA UNIR LÓGICAMENTE DOMINIOS O EQUIPOS DISTINTOS QUE ESTÁN GESTIONADOS POR UNA MISMA ENTIDAD.

POR OTRO LADO, EL SERVICIO DE BAJO COSTE NO PERMITE LA AUTENTICACIÓN DEL SERVIDOR USANDO UN CERTIFICADO DIGITAL. COMO SE DESCRIBIÓ EN SSL, EN EL PROTOCOLO DE SALUTACIÓN SE ENVÍA DICHO CERTIFICADO. ESTE HECHO DESACONSEJA EL USO DE SSL.

EN BASE A TODO LO ANTERIOR, Y REFORZADO POR EL HECHO DE QUE UNO DE LOS USOS HABITUALES DE SSH ES LA TRANSFERENCIA DE FICHEROS, EL CONSEJO DE NEREA ES UTILIZAR EL PROTOCOLO SSH.

6. TÚNELES CIFRADOS

Un túnel se define como la encapsulación de un protocolo de red en otro, de modo que las solicitudes puedan llegar de un origen a un destino. De esta forma, se permite la utilización de un protocolo en un entorno de red que no lo permitiría.

Los túneles se pueden considerar como la base sobre la que se asientan las VPN.

Para construirlos se utilizan los protocolos de tunelado.

6.1. POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

Point-to-Point Tunneling Protocol (PPTP) fue un protocolo desarrollado por Microsoft y normalizado por la IETF (RFC 2637).

PPTP hace uso de la seguridad de otro protocolo, llamado Point-to-Point (PPP), para realizar la comunicación en el túnel.

Así, se proporcionan los servicios de autenticación y confidencialidad haciendo uso de PPP.

6.1. POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

Respecto a la autenticación, es posible hacer uso de protocolos como:

- Password Authentication Protocol (PAP).
- Shiva Password Authentication Protocol (SPAP).
- Challenge Handshake Authentication Protocol (CHAP).
- Microsoft CHAP v1 (MS-CHAP v1).
- MS-CHAP v2.

6.1. POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

En relación con la confidencialidad, se hace uso del protocolo Microsoft Point-to-Point Encryption (MPPE) para cifrar los mensajes.

El cifrado se realiza a través del algoritmo de cifrado de flujo RC4.

6.1. POINT-TO-POINT TUNNELING PROTOCOL (PPTP)

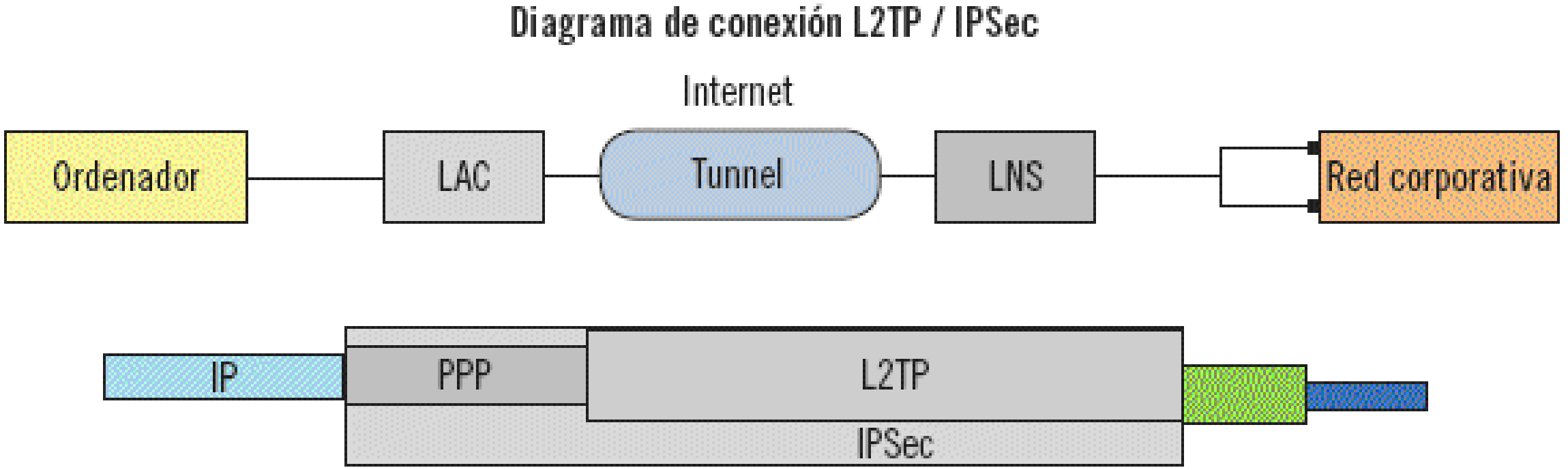
En cuanto a la comunicación por PPTP se pueden distinguir dos tipos:

- **De control se basa en controlar y gestionar la información que pasa por el canal.**
- **De datos consiste en realizar el encapsulado y transmisión de datos mediante el protocolo GRE**

6.2. LAYER 2 TUNNELLING PROTOCOL (L2TP)

El protocolo L2TP permite esencialmente construir túneles para que dos equipos o subredes puedan conectarse a través del protocolo PPP.

6.2. LAYER 2 TUNNELLING PROTOCOL (L2TP)



6.3. DATAGRAM TRANSPORT LAYER SECURITY (DTLS)

Datagram Transport Layer Security (DTLS) es un protocolo basado en TLS que proporciona comunicaciones seguras para la transmisión de datagramas.

7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS VPN

Las dos alternativas que más se emplean en la actualidad para la implementación de VPN son los sistemas basados en IPSec y aquellos basados en SSL.

7.1. PROS Y CONTRAS DE IPSEC VPN

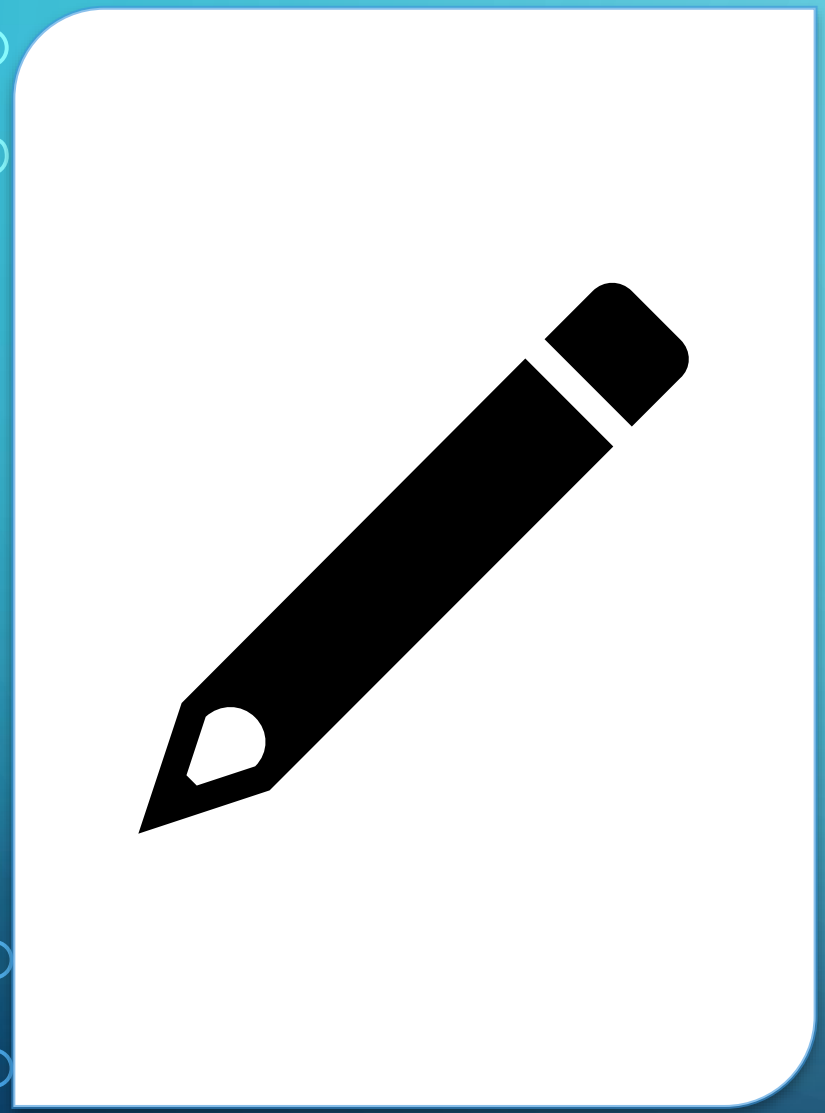
Ventajas de IPSec: está especialmente diseñada para aquellas situaciones en las que se quiere realizar una red privada estable a lo largo del tiempo.

Desventajas de IPSec: la complejidad de su administración y configuración.

7.2. PROS Y CONTRAS DE SSL VPN

Ventajas de SSL: para establecer una red privada virtual constituye una alternativa sencilla.

Desventajas de SSL: tecnología es más adecuada cuando las aplicaciones se ejecutan en el navegador web, algo que no siempre ocurre. Además, dado que SSL se sitúa en el nivel de transporte del Modelo OSI, no permite que todas las aplicaciones se aprovechen de la existencia de la red privada virtual.



Ejemplo.

ALBERTO JIMÉNEZ Y BEATRIZ HERNÁNDEZ ACABAN DE LICENCIARSE COMO INGENIEROS INFORMÁTICOS. SON GRANDES EMPRENDEDORES Y HAN DECIDIDO CREAR UNA EMPRESA DE DESARROLLO DE APLICACIONES MÓVILES. HAN ALQUILADO UN LOCAL Y LO HAN ESTABLECIDO COMO LA SEDE DE LA EMPRESA, EN LA QUE ALMACENAR LA BASE DE DATOS DE CLIENTES Y TODO EL SISTEMA NECESARIO. ACTUALMENTE SOLO TIENEN 5 CLIENTES Y, POR ELLO, ADEMÁS DE DESARROLLAR APLICACIONES PARA DICHOS CLIENTES HAN DE VIAJAR CON FRECUENCIA PARA HACER NUEVOS CONTACTOS. LOS VIAJES TIENEN QUE APROVECHARLOS PARA TRABAJAR, CONSULTANDO DE VEZ EN CUANDO DATOS ALMACENADOS EN LA BASE DE DATOS SITUADA EN LA SEDE DE LA EMPRESA, POR EJEMPLO LAS DIRECCIONES DE CORREO DE SUS CLIENTES. DISCUTA QUÉ TIPO DE VPN (SSL O IPSEC) SERÍA MÁS ADECUADA PARA ESTA EMPRESA.

Ejemplo. Solución.

IPSEC OFRECE UNAS CARACTERÍSTICAS DE SEGURIDAD SUPERIORES A SSL, ENTRE ELLOS ESTÁ EL ALGORITMO DE CIFRADO (3DES) O LA AUTENTICACIÓN DE LAS PARTES. EN IPSEC TANTO CLIENTE COMO SERVIDOR HAN DE AUTENTICARSE, MIENTRAS QUE EN SSL LA AUTENTICACIÓN DEL CLIENTE ES OPCIONAL. ASIMISMO, LOS COSTES DE GESTIÓN DE IPSEC SON MÁS ELEVADOS Y SE REQUIERE UN MAYOR CONOCIMIENTO.

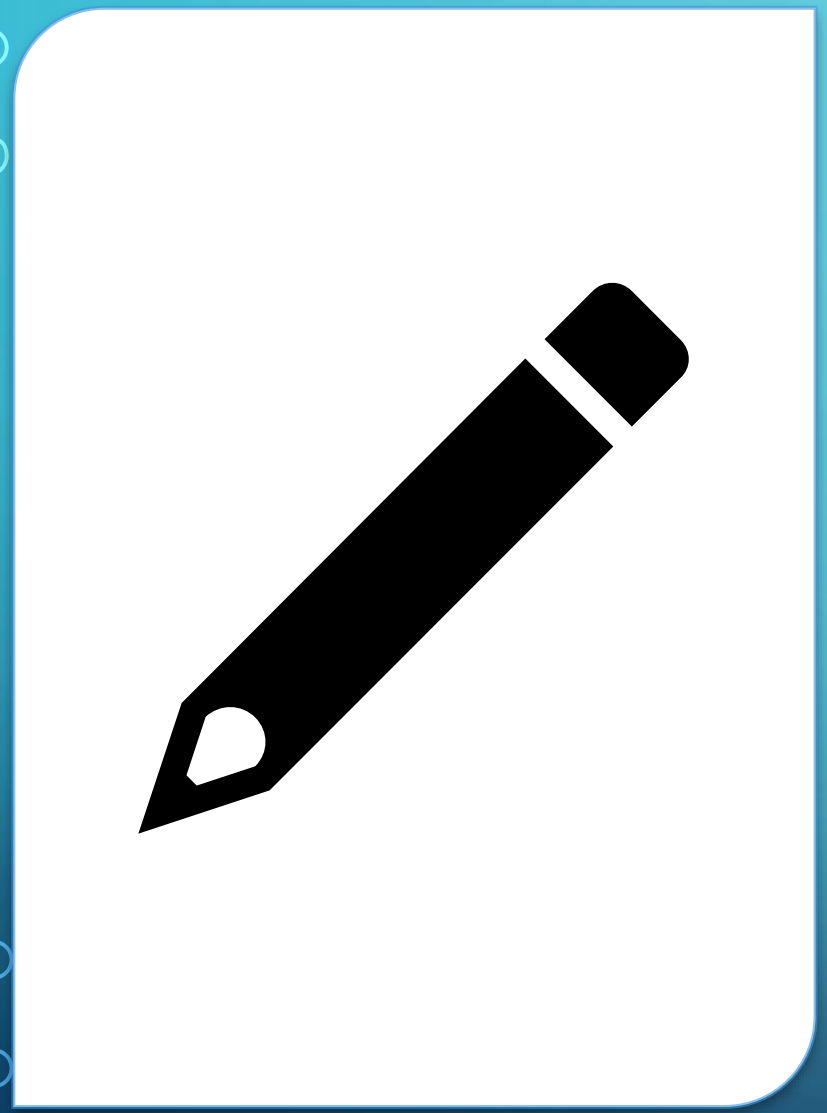
POR UN LADO, HAY QUE TENER PRESENTE QUE ALBERTO Y BEATRIZ ACABAN DE LICENCIARSE Y, POR ELLO, AUNQUE TENGAN LOS CONOCIMIENTOS, ES POSIBLE QUE LA ADMINISTRACIÓN Y EL ESTABLECIMIENTO ADECUADO DE IPSEC SEA UN PROCESO QUE REQUIERE ALGO MÁS DE EXPERIENCIA. ADEMÁS, TENIENDO EN CUENTA QUE AMBOS VAN A VIAJAR CON FRECUENCIA, CONECTÁNDOSE A LA BASE DE DATOS DE LA EMPRESA CON POCA ASIDUIDAD Y SIN TENER IMPUESTA NINGUNA RESTRICCIÓN DE SEGURIDAD, LO MÁS ADECUADO SERÍA HACER USO DE SSL VPN. DE ESTE MODO, VÍA WEB AMBOS USUARIOS PODRÍAN ACCEDER DESDE SUS PORTÁTILES, CON SEGURIDAD (AUNQUE NO TAN ELEVADA COMO CON IPSEC) Y DE FORMA SENCILLA. ASIMISMO, LA ADECUACIÓN DE UTILIZAR SSL VPN TAMBIÉN SE JUSTIFICA POR EL HECHO DE QUE SE HA DE PROPORCIONAR SERVICIO PARA ACCEDER A UN ÚNICO SERVICIO, ES DECIR, A LA BASE DE DATOS SITUADA EN LA SEDE.

7.3. ANÁLISIS DE COSTES

Ambas soluciones necesitan algún equipamiento de red que permita utilizarlo en el entorno corporativo.

Puesta en funcionamiento de todos los programas que deben poder ejecutarse a través de la VPN.

Ejercicios.



4.3.100.1.MF0489_3_EJERCICIOSCAPITULO_3.DOCX