

# **IFCT0109. SEGURIDAD INFORMÁTICA MF0489\_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS**



## **UD03**

### **COMUNICACIONES SEGURAS**

# CONTENIDOS

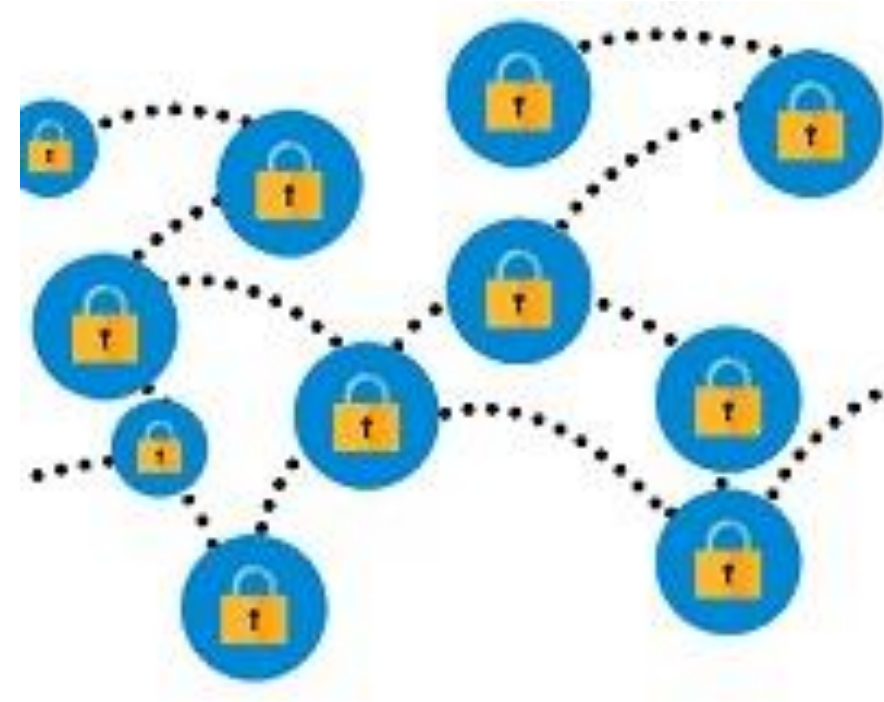
## 1. INTRODUCCIÓN

2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
5. SISTEMAS SSL VPN
6. TÚNELES CIFRADOS
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

# 1. INTRODUCCIÓN

UNA VEZ CONOCIDOS LOS ALGORITMOS CRIPTOGRÁFICOS, ASÍ COMO SU FUNCIONAMIENTO, EL SIGUIENTE PASO ES APLICARLOS.

UNO DE LOS USOS MÁS IMPORTANTES ES EL **ESTABLECIMIENTO DE COMUNICACIONES SEGURAS.**



# 1. INTRODUCCIÓN

UNA DE LAS CUESTIONES A RESOLVER ES CONOCER **CÓMO SE PUEDEN CONECTAR DOS ENTIDADES DE FORMA SEGURA USANDO UN CANAL DE COMUNICACIÓN INSEGURO.**

AQUÍ SURGE EL CONCEPTO DE **RED PRIVADA VIRTUAL (VPN)**, LA CUAL SERÁ DEFINIDA INDICANDO SUS FINALIDADES Y SUS FUNCIONALIDADES.

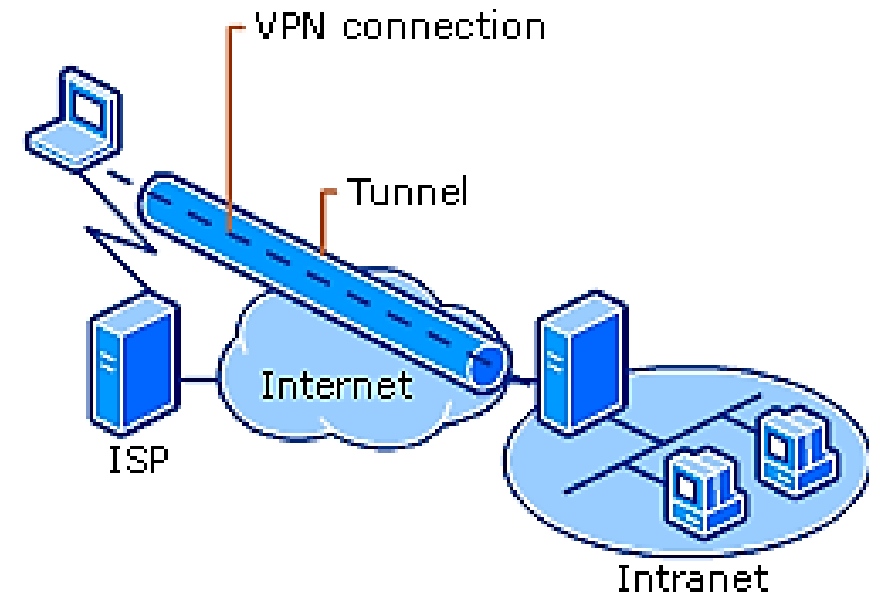


# 1. INTRODUCCIÓN

LAS VPN PUEDEN ESTABLECERSE HACIENDO USO DE **MÚLTIPLES PROTOCOLOS**.

EN PARTICULAR, EN ESTE CAPÍTULO SE DESCRIBEN LOS PROTOCOLOS **IPSEC, SSL Y SSH**, JUNTO CON OTROS BASADOS EN EL **ESTABLECIMIENTO DE TÚNELES CIFRADOS**.

FINALMENTE, SE PRESENTAN LAS VENTAJAS E INCONVENIENTES DE UTILIZAR DISTINTAS ALTERNATIVAS PARA LA CREACIÓN DE VPN.



# CONTENIDOS

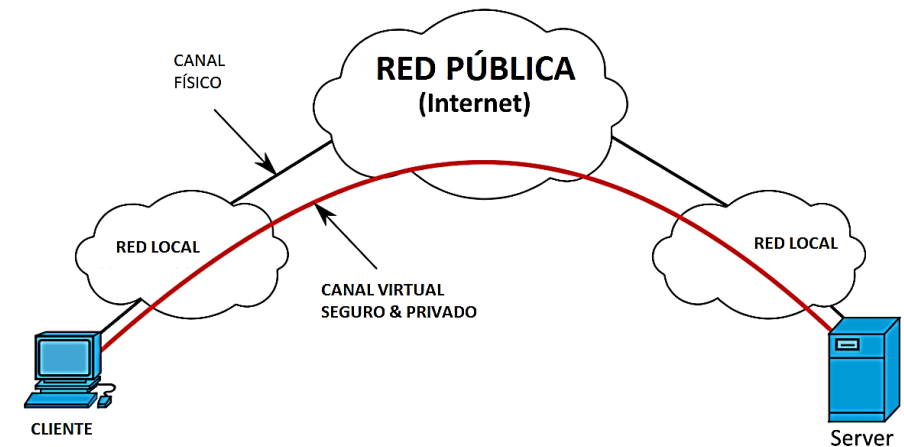
1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
5. SISTEMAS SSL VPN
6. TÚNELES CIFRADOS
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN



## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

LAS REDES PRIVADAS VIRTUALES, LLAMADAS VPN (VIRTUAL PRIVATE NETWORK) SON UN TIPO DE RED DE COMUNICACIONES QUE SE CONSTRUYE SOBRE OTRA YA EXISTENTE.

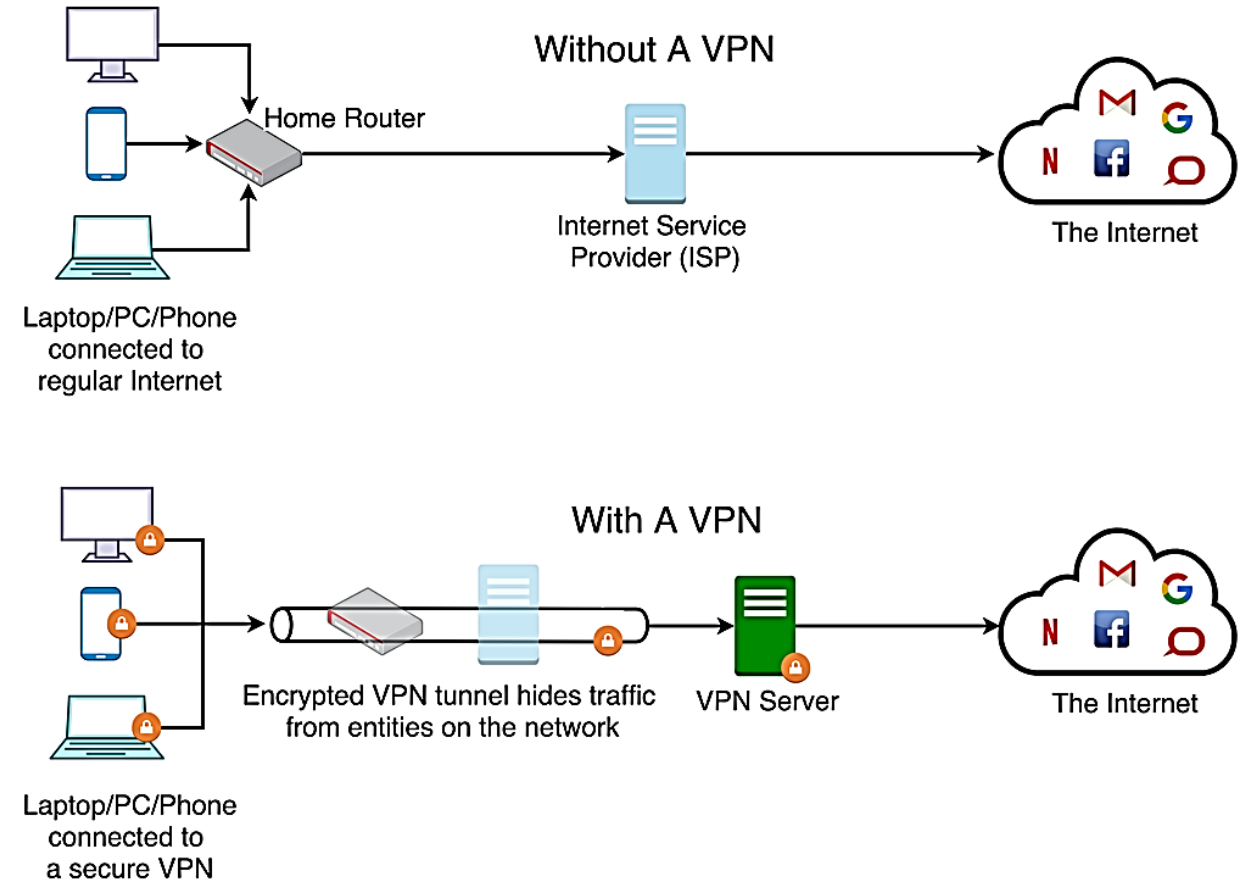
LA CARACTERÍSTICA FUNDAMENTAL ES QUE PUEDEN PERMITIR QUE DISTINTOS EQUIPOS EN DIVERSAS PARTES DEL MUNDO PUEDAN COMUNICARSE COMO SI ESTUVIESEN EN UNA RED DE ÁREA LOCAL.



## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

EL USO DE LAS VPN TIENE GRANDES VENTAJAS.

PARA COMPRENDER CÓMO ES ESTO POSIBLE ES IMPRESCINDIBLE INTRODUCIR LOS CONCEPTOS MÁS BÁSICOS DE REDES DE ORDENADORES.

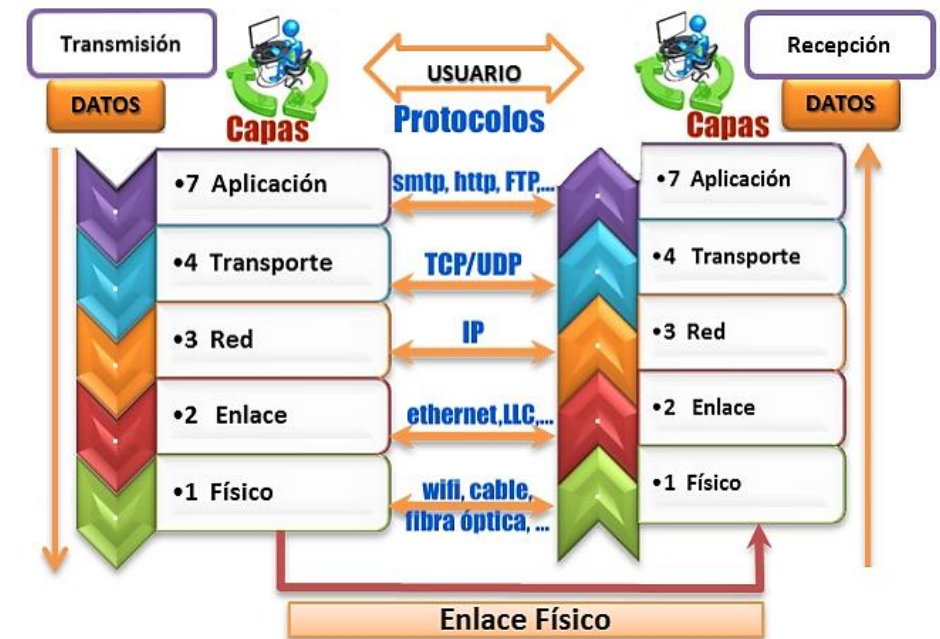




## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### CONCEPTOS PREVIOS. EL MODELO OSI

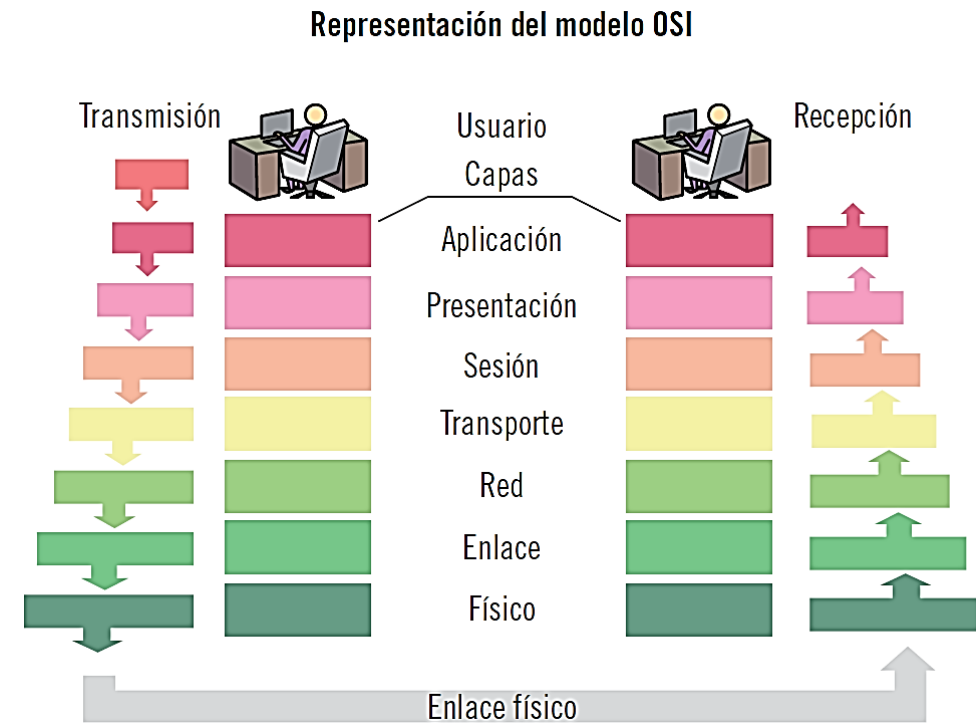
LA COMUNICACIÓN ENTRE DISTINTOS EQUIPOS PUEDE PLANTEARSE COMO UN CONJUNTO DE CAPAS SUCESIVAS ENTRE LAS QUE SE INTERCAMBIAN PAQUETES Y CADA UNA DE LAS CUALES TIENE UNA MISIÓN PARTICULAR.



## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### CONCEPTOS PREVIOS. EL MODELO OSI

EL MODELO MÁS COMÚNMENTE CONOCIDO ES EL **MODELO OSI**, EN EL QUE LAS CAPAS SE INTERRELACIONAN DE FORMA QUE APROVECHAN LAS CAPACIDADES DE LAS CAPAS INFERIORES Y OFRECEN SERVICIOS A LAS SUPERIORES.



## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### CONCEPTOS PREVIOS. EL MODELO OSI

EL MODELO OSI SE COMPONE DE **SIETE CAPAS**:

- **NIVEL FÍSICO (CAPA 1).** SE ENCARGA DE TRANSMITIR LOS DATOS FÍSICAMENTE POR EL CANAL DE COMUNICACIÓN (EL CABLE DE RED).
- **NIVEL DE ENLACE (CAPA 2).** PERMITE ESTABLECER EL CONCEPTO DE RED LOCAL, ES DECIR, QUÉ EQUIPOS ESTÁN DIRECTAMENTE CONECTADOS ENTRE SÍ. PARA ELLO, SE UTILIZAN LAS **DIRECCIONES MAC**, QUE SON LAS QUE LOS FABRICANTES PROPORCIONAN A LAS TARJETAS DE RED.
- **NIVEL DE RED (CAPA 3).** PERMITE QUE EQUIPOS DE DISTINTAS REDES PUEDAN COMUNICARSE ENTRE SÍ, GRACIAS AL ESTABLECIMIENTO DE UNA **DIRECCIÓN DE RED**.

## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### CONCEPTOS PREVIOS. EL MODELO OSI

- **NIVEL DE TRANSPORTE (CAPA 4).** HACE POSIBLE QUE EL CANAL DE COMUNICACIÓN PUEDA SER USADO POR DISTINTOS PROGRAMAS AL MISMO TIEMPO. PARA ELLO, SE INTRODUCE EL CONCEPTO DE **PUERTO**. ALGUNOS PROTOCOLOS DE ESTA CAPA OFRECEN LA POSIBILIDAD DE GESTIONAR LA ENTREGA DE INFORMACIÓN HACIENDO FRENTE A EVENTUALES PÉRDIDAS DE PAQUETES. EN ESTA CAPA, PROTOCOLOS COMO **TCP** HACEN FRENTE A ESTA SITUACIÓN. NO OBSTANTE, TAMBIÉN EXISTEN OTROS (COMO **UDP**) QUE NO OFRECEN ESTE SERVICIO.

## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### CONCEPTOS PREVIOS. EL MODELO OSI

- **NIVELES DE SESIÓN (CAPA 5) Y PRESENTACIÓN (CAPA 6).** LA CAPA 5 CREA EL CONCEPTO DE **SESIÓN ENTRE DOS APLICACIONES**. POR SU PARTE, LA CAPA 6 SE ENCARGA DE ASEGURAR QUE, AUNQUE LA **REPRESENTACIÓN DE LA INFORMACIÓN** SEA DISTINTA ENTRE DOS ORDENADORES (POR EJEMPLO, PORQUE LOS BITS SE ORDENAN DE FORMA DISTINTA), ESTO NO AFECTE AL FUNCIONAMIENTO.
- **NIVEL DE APLICACIÓN (CAPA 7).** AQUÍ SE DEFINEN LOS **PROTOCOLOS QUE SIGUEN LOS PROGRAMAS (HTTP, FTP, ETC.)**. UN PROTOCOLO ESPECIFICA QUÉ DATOS SE INTERCAMBIAN Y CUÁNDO SE TIENE QUE HACER.

## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### CONCEPTOS PREVIOS. EL MODELO OSI

LA COMUNICACIÓN ENTRE DISTINTOS ORDENADORES SE HACE DE LA SIGUIENTE MANERA:

EL PROGRAMA EMISOR PREPARA EL PAQUETE QUE QUIERE ENVIAR (**CAPA 7**) Y LO ENVÍA A LAS CAPAS INFERIORES. DEJANDO DE LADO LAS **CAPAS 6 Y 5** (PARA NO ENTRAR EN DETALLES).

LA **CAPA 4** AÑADE EL *PUERTO DE ORIGEN*, ASÍ COMO EL *DE DESTINO*.

LA **CAPA 3** RECIBE TODA ESTA INFORMACIÓN Y AÑADE LA *DIRECCIÓN IP DE ORIGEN Y LA DE DESTINO*.

## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### CONCEPTOS PREVIOS. EL MODELO OSI

LA **CAPA 2** ANALIZA: ¿ESTÁ EL DESTINO DENTRO DE LA MISMA RED?

- SI ES ASÍ, SE LE PUEDE ENVIAR DIRECTAMENTE, SIN SALIR DE LA RED LOCAL. LA CAPA 2 AÑADE LA *DIRECCIÓN MAC DEL ORDENADOR DESTINO*.
- SI NO ES ASÍ, ES NECESARIO ENVIARLO FUERA DE LA RED PARA ENCAMINARLO. LA CAPA 2 AÑADE LA *DIRECCIÓN MAC DEL ENCAMINADOR O ROUTER*, QUE SE ENCARGARÁ DE ENVIARLO A LA RED DEL DESTINATARIO.

FINALMENTE, TODA LA INFORMACIÓN DE LAS CAPAS ANTERIORES SE ENVÍA A TRAVÉS DEL MEDIO DE COMUNICACIÓN (EL CABLE O EL AIRE) GRACIAS A LA **CAPA 1**.



## **2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES**

### **CONCEPTOS PREVIOS. EL MODELO OSI**

TAL CUAL SE HA DESCRITO HASTA AHORA, NO HAY FORMA DE QUE DOS ORDENADORES EN DISTINTAS REDES PUEDAN ALCANZARSE DIRECTAMENTE, SIN AYUDA DE UN ENCAMINADOR (ROUTER).

PARA CONSEGUIR QUE UN EQUIPO DE UNA RED SE COMPORTE COMO SI FUESE DE OTRA, PARECE CLARO QUE ES NECESARIO INTRODUCIR ELEMENTOS EN DIFERENTES PARTES DE ESTE MODELO.

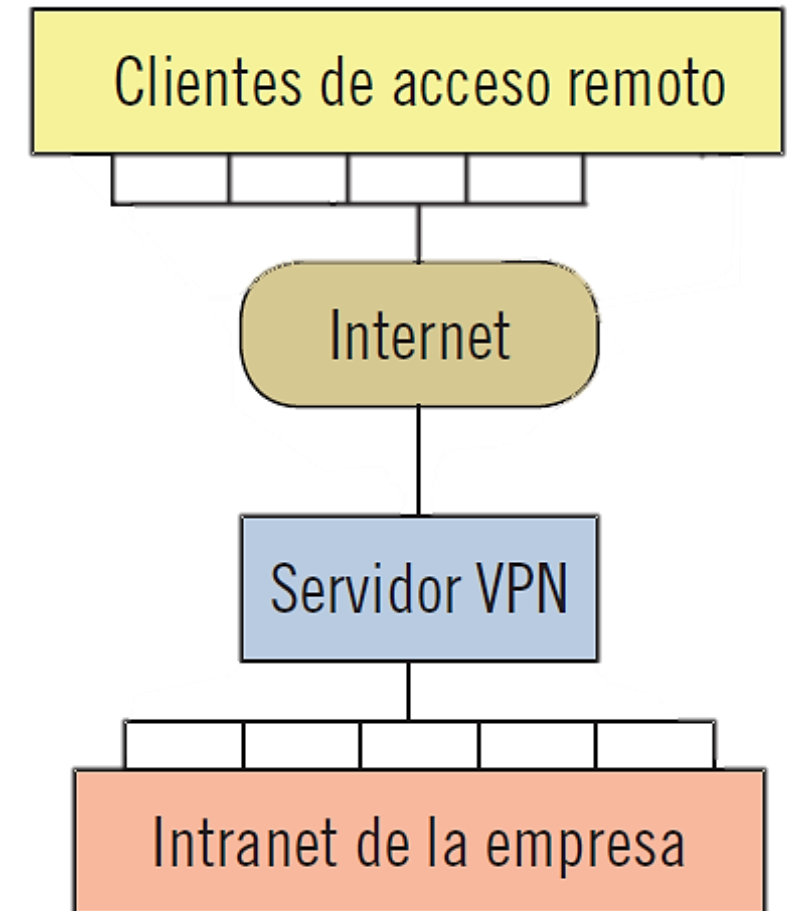
PARTICULARMENTE, UNA DE LAS TÉCNICAS MÁS HABITUALES ES EL **ENCAPSULADO DE PROTOCOLOS**.

## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### DESCRIPCIÓN DE LAS VPN

**LAS VPN PERMITEN QUE EQUIPOS FÍSICAMENTE DISTANTES SE COMPORTEN COMO SI ESTUVIERAN DENTRO DEL MISMO DOMINIO DE SEGURIDAD, ES DECIR, EN LA MISMA RED.**

ESTO TIENE ESPECIAL RELEVANCIA DE CARA A PERMITIR EL ACCESO A DETERMINADOS RECURSOS, COMO UN SERVIDOR DE DATOS.

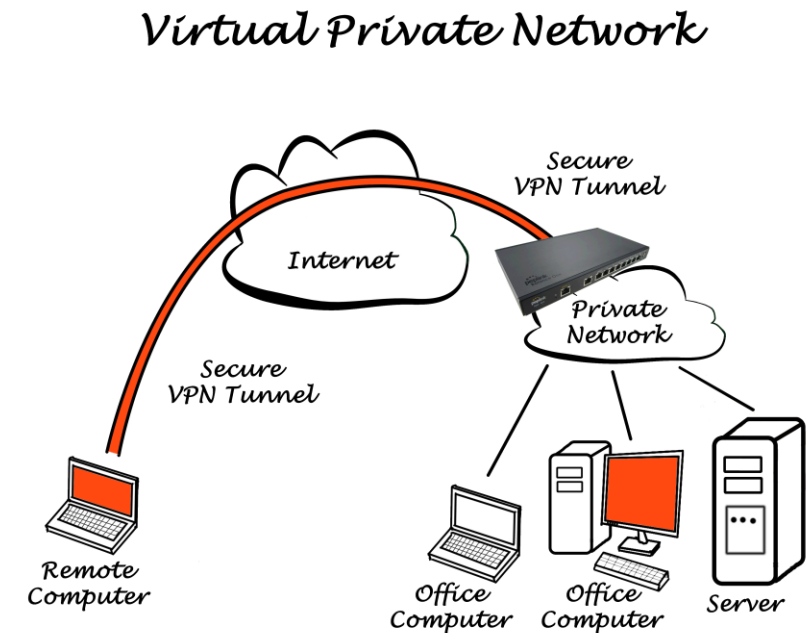


## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### DESCRIPCIÓN DE LAS VPN

UNA POLÍTICA DE SEGURIDAD ADECUADA DEBERÍA ESTABLECER LOS MECANISMOS DE PROTECCIÓN QUE ASEGUREN QUE SOLO LOS EQUIPOS QUE ESTÁN EN UNA RED PUEDAN TENER ACCESO A LOS RECURSOS.

LAS **VPN** PERMITEN QUE LOS EQUIPOS CONECTADOS A ELLA SE COMPORTAN COMO SI ESTUVIESEN EN DICHA RED.

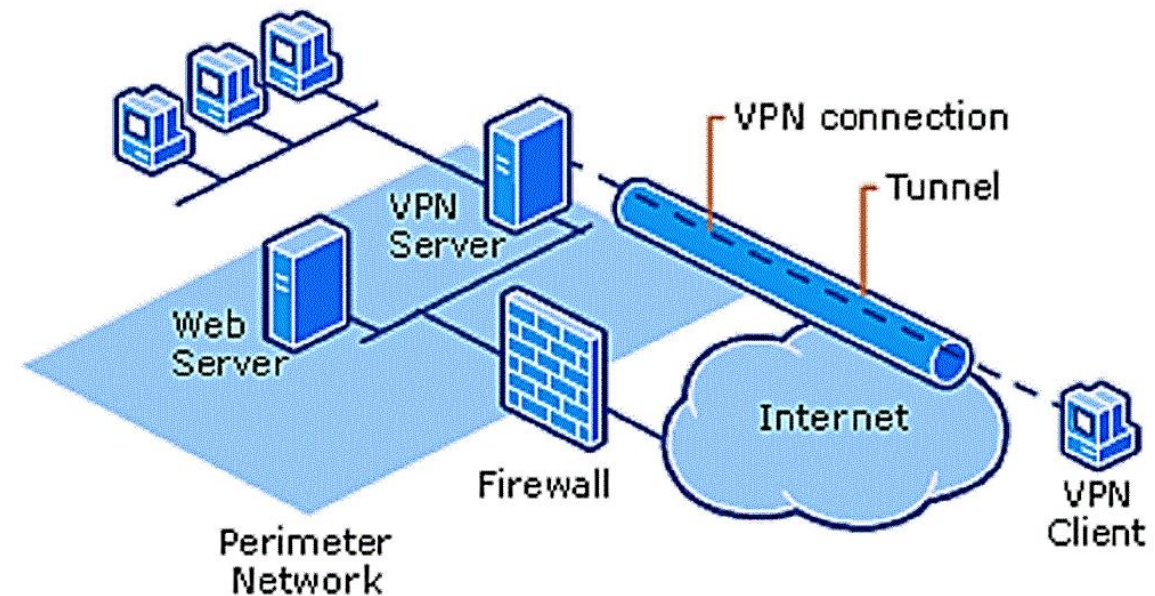


## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### DESCRIPCIÓN DE LAS VPN

**LAS VPN GARANTIZAN LA CONFIDENCIALIDAD DE LA INFORMACIÓN INTERCAMBIADA.**

**DE ESTA MANERA, SE PUEDE DECIR QUE LAS VPN PERMITEN CREAR UNA RED PRIVADA A PARTIR DE UNA RED PÚBLICA TÍPICAMENTE INSEGURA, COMO INTERNET.**



## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### DESCRIPCIÓN DE LAS VPN

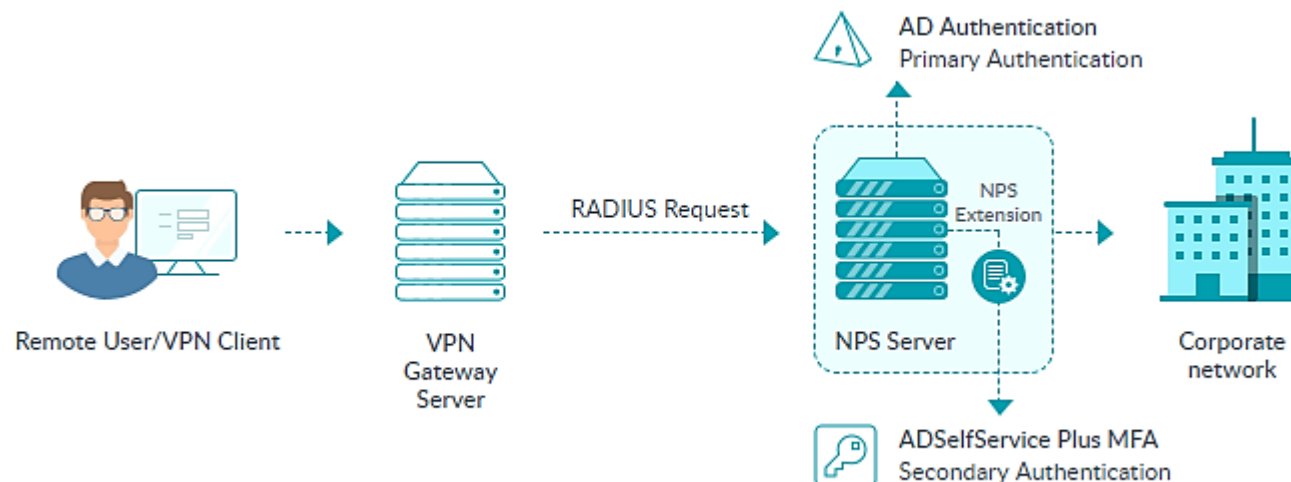
ESTA CIRCUNSTANCIA, JUNTO CON EL HECHO DE QUE EL USUARIO TENGA LA PERCEPCIÓN DE QUE PUEDE EMPLEAR SU EQUIPO COMO SI ESTUVIESE EN SU RED HABITUAL, DA LUGAR A LA DENOMINACIÓN DE **RED VIRTUAL** (PUES NO EXISTE FÍSICAMENTE) Y **PRIVADA**.



## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### DESCRIPCIÓN DE LAS VPN

LAS VPN SUELEN PROPORCIONAR **AUTENTICACIÓN** DE ORIGEN (PARA EVITAR QUE TERCEROS NO AUTORIZADOS ENTREN EN LA RED) E **INTEGRIDAD** DE LOS DATOS (ASEGURANDO QUE ESTOS NO SON ALTERADOS DURANTE LA COMUNICACIÓN).



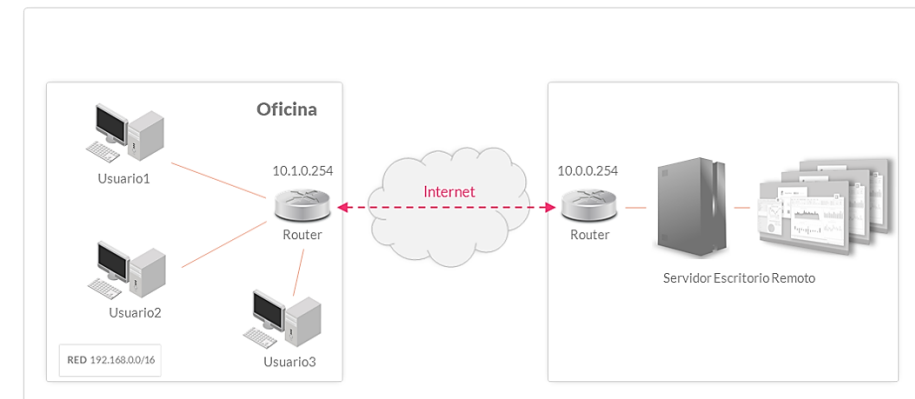
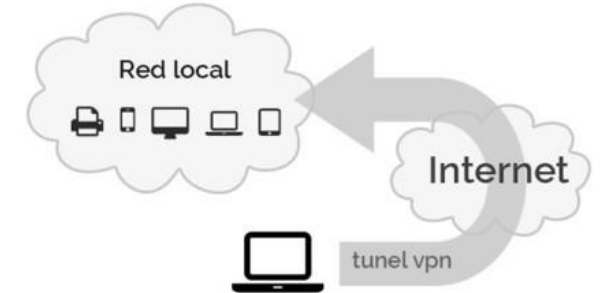


## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### DESCRIPCIÓN DE LAS VPN

LAS VPN PUEDEN SERVIR PARA:

- UN ACCESO DESDE UNA UBICACIÓN A LA RED DE LA OFICINA. ESTE TIPO SERÍA **CONEXIÓN ORDENADOR-A-RED**.
- DOS O MÁS REDES SE COMPORTEN COMO UNA ÚNICA RED. ESTO SERÍA **CONEXIONES SITIO-A-SITIO**.





## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### DESCRIPCIÓN DE LAS VPN

LAS VPN UTILIZAN PROTOCOLOS DE TUNELADO. LOS PRINCIPALES PROTOCOLOS 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)

**LAS OPCIONES MÁS EXTENDIDAS SON LAS BASADAS EN SSL E IPSEC**

## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### VENTAJAS Y DESVENTAJAS DE LAS VPN

#### VENTAJAS

- **BAJO COSTE DE DESPLIEGUE:** REDES FÍSICAMENTE SEPARADAS PUEDEN CONECTARSE SIN LA NECESIDAD DE ESTABLECER UNA RED DEDICADA.
- **TRANSPARENCIA DE COMUNICACIÓN:** LOS USUARIOS TIENEN LA SENSACIÓN DE USO DE LA RED COMO SI ESTUVIERAN FÍSICAMENTE CONECTADOS A ELLA.
- **SEGURIDAD EN LOS SISTEMAS:** SE CREA UNA CAPA ADICIONAL DE SEGURIDAD SOBRE EL ACCESO A INFORMACIÓN SENSIBLE.
- **SIMPLICIDAD ADMINISTRATIVA:** LAS DECISIONES DE A QUÉ ORDENADORES SE PERMITE ACCEDER A QUÉ RECURSOS SON AHORA MÁS FÁCILES, PUES TODOS PUEDEN ESTAR EN UNA MISMA RED.

## 2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES

### VENTAJAS Y DESVENTAJAS DE LAS VPN

#### DESVENTAJAS

- **FIABILIDAD DE LA RED:** LAS VPN SE CONSTRUYEN SOBRE INTERNET Y PUEDEN PRODUCIRSE FALLOS QUE IMPOSIBILITEN LA COMUNICACIÓN.
- **VELOCIDAD DE ACCESO:** LA VELOCIDAD DE ACCESO ES MENOR DEBIDO A LAS CAPAS DE SEGURIDAD QUE SE APLICAN (EJ. CIFRADO).
- **CONFIANZA DE LAS ENTIDADES:** SI UN EQUIPO ES COMPROMETIDO, LOS DEMÁS EQUIPOS PODRÍAN SER ATACADOS A PARTIR DEL PRIMERO.
- **INCOMPATIBILIDAD DE LAS REDES:** CADA FABRICANTE DE EQUIPOS DE COMUNICACIÓN TIENE SU PROPIA TECNOLOGÍA PARA CREAR LA VPN.

# CONTENIDOS

1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
5. SISTEMAS SSL VPN
6. TÚNELES CIFRADOS
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

### 3. PROTOCOLO IPSEC

**IPSEC (INTERNET PROTOCOL SECURITY) ES UN CONJUNTO DE PROTOCOLOS PARA CONFIGURAR CONEXIONES SEGURAS A TRAVÉS DE UNA RED.**

EL PROTOCOLO DE INTERNET (IP) ES EL ESTÁNDAR COMÚN QUE DETERMINA CÓMO VIAJAN LOS DATOS POR INTERNET.

**IPSEC AGREGA CIFRADO Y AUTENTICACIÓN PARA HACER QUE EL PROTOCOLO SEA MÁS SEGURO.**

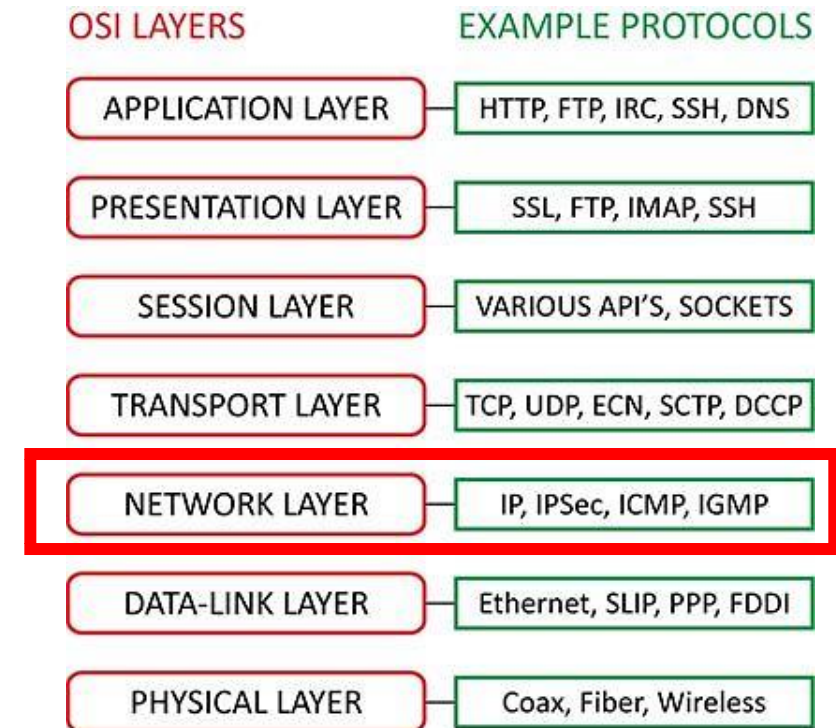
**IPSEC CODIFICA LOS DATOS EN EL ORIGEN Y LOS DESCODIFICA EN SU DESTINO. TAMBIÉN AUTENTICA EL ORIGEN DE LOS DATOS.**



### 3. PROTOCOLO IPSEC

**IPSEC ACTÚA EN EL NIVEL DE RED, A DIFERENCIA DE OTROS MECANISMOS QUE ACTÚAN EN CAPAS SUPERIORES.**

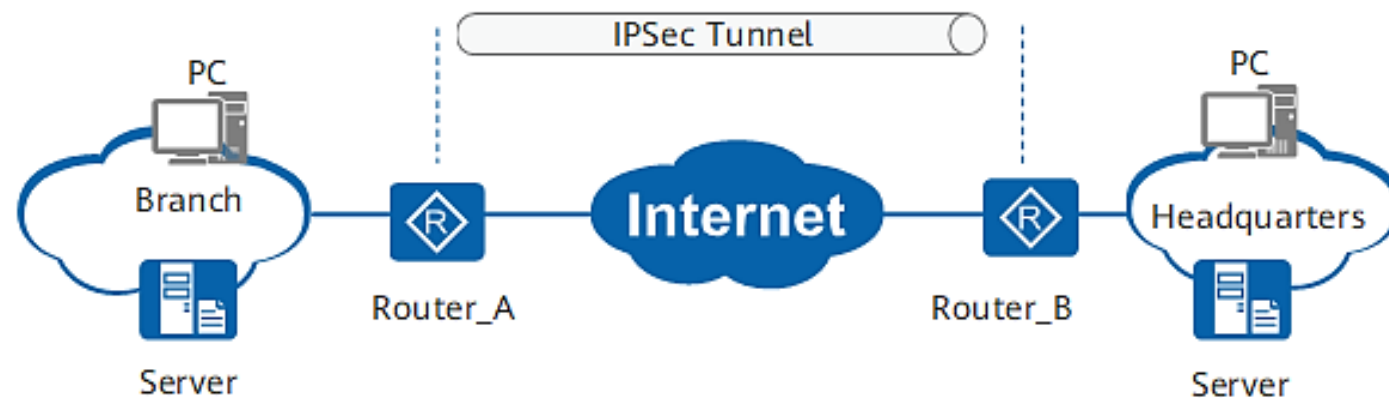
ESTA DIFERENCIA ES IMPORTANTE, PUES AL ESTAR SITUADO EN UN NIVEL INFERIOR, TODOS LOS PROGRAMAS Y SERVICIOS QUE SE SITÚEN POR ENCIMA PODRÍAN HACER USO DE IPSEC.



### 3. PROTOCOLO IPSEC

EL GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET DESARROLLÓ **IPSEC** EN LA DÉCADA DE 1990 **PARA GARANTIZAR LA CONFIDENCIALIDAD, INTEGRIDAD Y AUTENTICIDAD DE LOS DATOS CUANDO SE ACCEDE A LAS REDES PÚBLICAS.**

LOS USUARIOS SE CONECTAN A INTERNET CON UNA **VPN IPSEC** PARA ACCEDER A LOS ARCHIVOS DE LA EMPRESA DE FORMA REMOTA.





### 3. PROTOCOLO IPSEC

IPSEC SE PUEDE USAR PARA:

- PROPORCIONAR SEGURIDAD AL ENRUTADOR CUANDO SE ENVÍEN DATOS A TRAVÉS DE LA RED DE INTERNET PÚBLICA.
- CIFRAR LOS DATOS DE LA APLICACIÓN.
- AUTENTICAR RÁPIDAMENTE LOS DATOS SI PROCEDEN DE UN REMITENTE CONOCIDO.
- PROTEGER LOS DATOS DE LA RED ESTABLECIENDO CIRCUITOS CIFRADOS, LLAMADOS **TÚNELES IPSEC**, QUE CIFRAN TODOS LOS DATOS ENVIADOS ENTRE DOS PUNTOS DE CONEXIÓN.

### 3. PROTOCOLO IPSEC

EL CIFRADO **IPSEC** ES UNA FUNCIÓN DE SOFTWARE QUE CODIFICA LOS DATOS PARA PROTEGER SU CONTENIDO FRENTE A PARTES NO AUTORIZADAS.

**IPSEC** ADMITE VARIOS TIPOS DE CIFRADO, COMO **AES, BLOWFISH, TRIPLE DES, CHACHA Y DES-CBC**.

**IPSEC** UTILIZA EL **CIFRADO ASIMÉTRICO Y SIMÉTRICO** PARA PROPORCIONAR VELOCIDAD Y SEGURIDAD DURANTE LA TRANSFERENCIA DE DATOS.

**IPSEC** ESTABLECE UNA CONEXIÓN SEGURA CON **CIFRADO ASIMÉTRICO Y CAMBIA AL CIFRADO SIMÉTRICO PARA ACELERAR LA TRANSFERENCIA DE DATO**.

## 3. PROTOCOLO IPSEC

### ¿CÓMO FUNCIONA IPSEC?

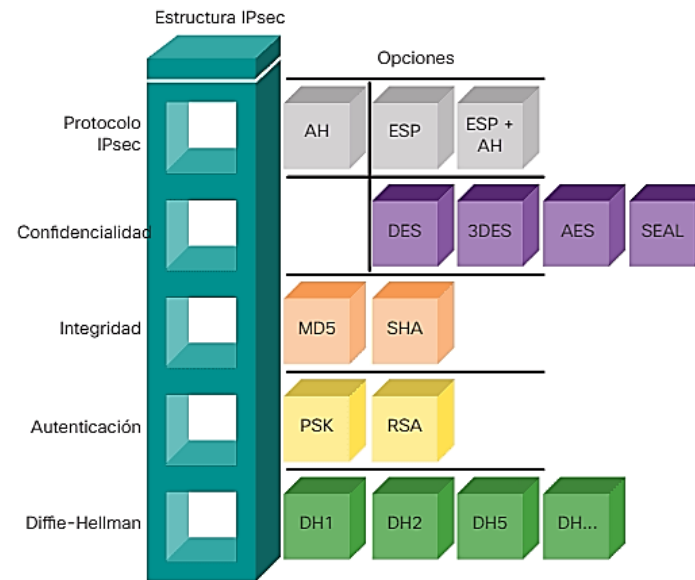
EL PROTOCOLO **IPSEC** SIGUE LOS SIGUIENTES PASOS:

- LA COMPUTADORA INICIA LA TRANSMISIÓN SEGURA **IPSEC** CON LA COMPUTADORA RECEPTORA.
- AMBAS COMPUTADORAS NEGOCIAN LOS REQUISITOS PARA ESTABLECER UNA CONEXIÓN SEGURA. ESTO INCLUYE ACORDAR MUTUAMENTE EL CIFRADO, LA AUTENTICACIÓN Y OTROS PARÁMETROS DE LA **ASOCIACIÓN DE SEGURIDAD (SA)**.
- LA COMPUTADORA ENVÍA Y RECIBE DATOS ENCRIPTADOS, Y VALIDA QUE PROVIENEN DE FUENTES CONFIABLES. REALIZA COMPROBACIONES PARA GARANTIZAR QUE EL CONTENIDO SUBYACENTE SEA FIABLE.
- UNA VEZ QUE LA TRANSMISIÓN SE COMPLETA O LA SESIÓN CONCLUYE, LA COMPUTADORA FINALIZA LA CONEXIÓN **IPSEC**.

### 3. PROTOCOLO IPSEC

LOS PROTOCOLOS QUE FORMAN IPSEC SON ESENCIALMENTE DOS:

- INTERNET KEY EXCHANGE (IKE)
- ENCAPSULATING SECURITY PAYLOAD (ESP)



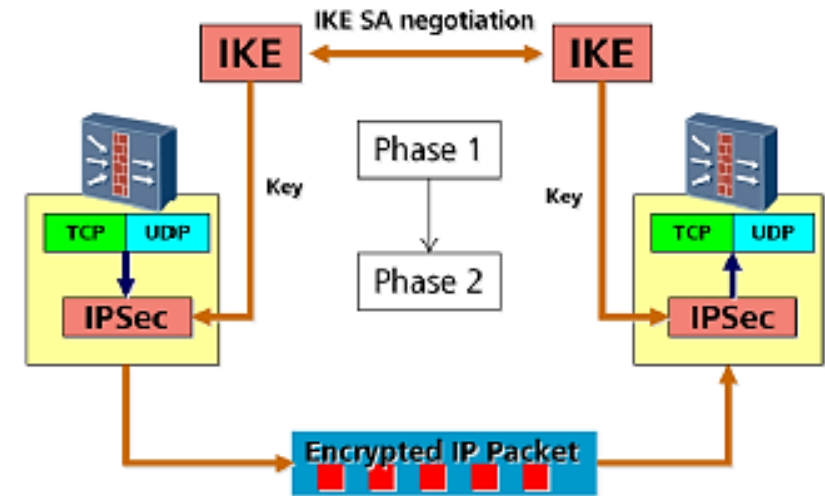
EXISTE UN TERCER PROTOCOLO (**AUTHENTICATED HEADER, AH**), PERO YA NO SE USA, PUES SU PRINCIPAL OBJETIVO DE SEGURIDAD (PROPORCIONAR AUTENTICACIÓN DEL MENSAJE) YA QUEDA CUBIERTO POR **ESP**.

### 3. PROTOCOLO IPSEC

#### 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. ASÍ, SE DETERMINA EL ALGORITMO CRIPTOGRÁFICO A UTILIZAR Y SU MODO DE OPERACIÓN JUNTO CON LA CLAVE DE CIFRADO PARA LOS DATOS QUE SE INTERCAMBIEN.

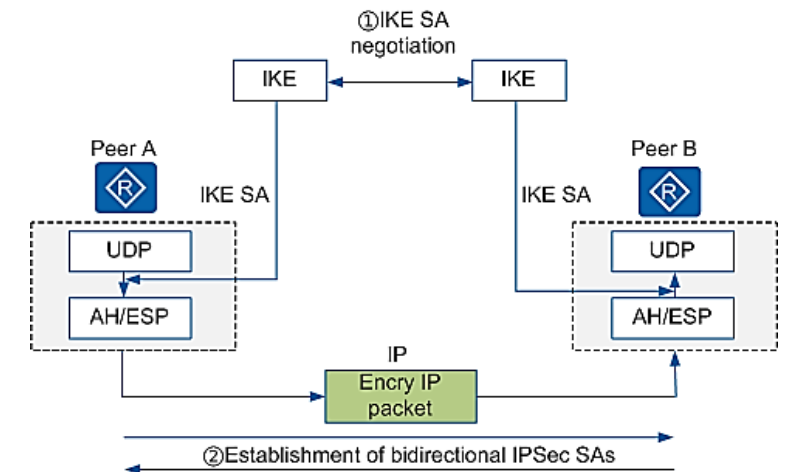


### 3. PROTOCOLO IPSEC

#### INTERNET KEY EXCHANGE (IKE)

GRACIAS A LA ASOCIACIÓN DE SEGURIDAD, LAS DOS PARTES DISPONEN DE UN *ESQUEMA DE FUNCIONAMIENTO* ACORDADO, QUE PODRÁ SER UTILIZADO EN EL PROTOCOLO **ESP**.

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.



### 3. PROTOCOLO IPSEC

#### INTERNET KEY EXCHANGE (IKE)

EN UNA EJECUCIÓN DEL PROTOCOLO HABITUALMENTE SE PRODUCEN DOS INTERCAMBIOS:

1. **IKE\_SA\_INIT:** ESTE INTERCAMBIO SE PRODUCE ANTES QUE CUALQUIERA DE LOS DEMÁS Y PERMITE NEGOCIAR ALGUNOS PARÁMETROS DE LA ASOCIACIÓN DE SEGURIDAD, INTERCAMBIAR VALORES ALEATORIOS Y EJECUTAR EL ALGORITMO DIFFIE-HELLMAN PARA ESTABLECER UNA CLAVE COMPARTIDA.

ESA CLAVE SE TOMA COMO BASE (*SEMILLA*) PARA DERIVAR DE ELLA OTRAS DOS CLAVES: *UNA PARA CIFRAR Y OTRA PARA AUTENTICAR* LOS MENSAJES HACIENDO USO DE FUNCIONES HASH CON CLAVE.

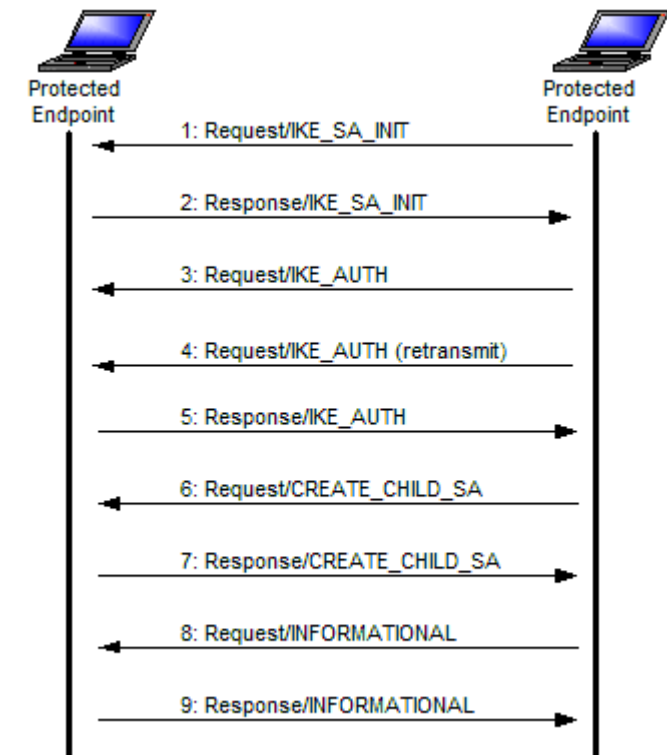


### 3. PROTOCOLO IPSEC

#### INTERNET KEY EXCHANGE (IKE)

2. **IKE\_AUTH:** EN ESTA FASE SE AUTENTICAN MUTUAMENTE LOS COMUNICANTES Y SE ESTABLECE LA ASOCIACIÓN DE SEGURIDAD QUE SE UTILIZARÁ EN **ESP**.

PARTE DE LOS MENSAJES QUE SE INTERCAMBIAN AQUÍ ESTÁN CIFRADOS UTILIZANDO LA CLAVE NEGOCIADA EN EL INTERCAMBIO ANTERIOR.



### 3. PROTOCOLO IPSEC

#### ENCAPSULATING SECURITY PAYLOAD (ESP)

EL PROTOCOLO **ESP** SE ENCARGA DE PROPORCIONAR ***CONFIDENCIALIDAD, AUTENTICACIÓN E INTEGRIDAD*** DE LA INFORMACIÓN EN TRÁNSITO.

PARA ELLO, **ESP** INTRODUCE ESA INFORMACIÓN EN OTRO PAQUETE, SOBRE EL QUE SE APLICAN LOS MECANISMOS DE SEGURIDAD.

LOS MECANISMOS QUE SE ELIGEN Y CÓMO SE APLICAN SE BASAN EN LA ASOCIACIÓN DE SEGURIDAD ESTABLECIDA TRAS **IKE**.

### **3. PROTOCOLO IPSEC**

#### **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. PROTOCOLO IPSEC**

#### **ESCENARIOS DE USO**

#### **SEGÚN LA CONFIGURACIÓN FÍSICA**

SE REFIERE A SI LOS PARTICIPANTES EN **IPSEC** SON ORDENADORES DE USUARIO O EQUIPOS INTERMEDIOS QUE ESPECÍFICAMENTE SE DEDICAN A ESTABLECER ESTE TIPO DE CONEXIONES. SE IDENTIFICAN **TRES ESCENARIOS** POSIBLES:

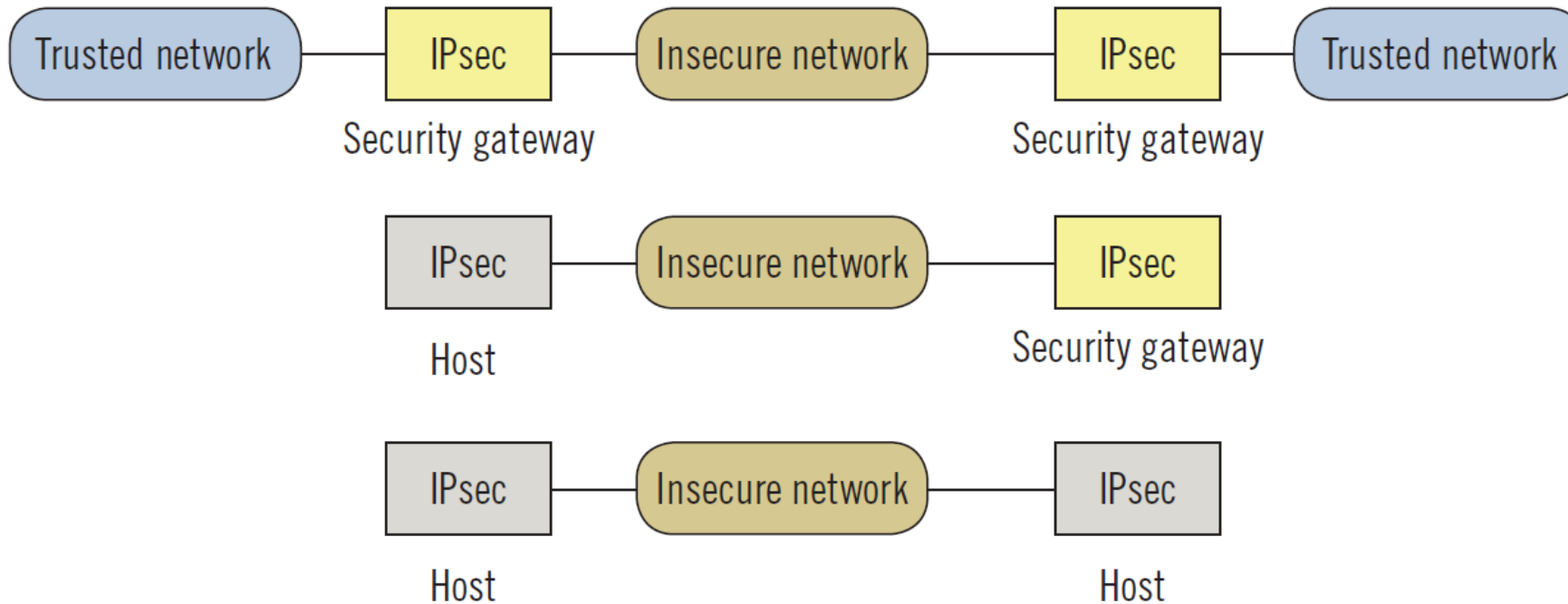
- **LOS EQUIPOS FINALES SE CONECTAN A LOS CITADOS EQUIPOS INTERMEDIOS.**
- **SOLO UNO DE LOS EXTREMOS ES UN EQUIPO FINAL, EXISTIENDO UN INTERMEDIARIO EN EL OTRO EXTREMO.**
- **AMBOS EQUIPOS FINALES SÍ IMPLEMENTAN IPSEC, POR LO QUE NO EXISTEN INTERMEDIARIOS.**

# 3. PROTOCOLO IPSEC

## ESCENARIOS DE USO

### SEGÚN LA CONFIGURACIÓN FÍSICA

Ejemplos de configuraciones físicas de IPSec



### **3. PROTOCOLO IPSEC**

#### **ESCENARIOS DE USO**

#### **SEGÚN EL TIPO DE PROTECCIÓN**

DE ACUERDO AL TIPO DE PROTECCIÓN APLICADA, SE ESPECIFICAN DOS POSIBLES MODOS DE USO:

- **MODOS TRANSPORTE**
- **MODOS TÚNEL**

## 3. PROTOCOLO IPSEC

### ESCENARIOS DE USO

#### SEGÚN EL TIPO DE PROTECCIÓN

- EN EL **MODO TRANSPORTE**, SOLO SE PROTEGE LA CARGA ÚTIL DE CADA UNO DE LOS PAQUETES QUE SE ENVÍAN. DE ESTA MANERA, NO SE MODIFICA LA CABECERA DEL PAQUETE (QUE CONTIENE, ENTRE OTRAS COSAS, LAS DIRECCIONES ORIGEN Y DESTINO). ESTE MODO DE USO ES ADECUADO PARA LA CONFIGURACIÓN ENTRE EQUIPOS FINALES.
- EN EL **MODO TÚNEL**, EL PAQUETE QUE CONTIENE LA INFORMACIÓN INTERCAMBIADA SE ENCAPSULA DENTRO DE OTRO PAQUETE. LA PRINCIPAL VENTAJA ES QUE DE ESTA FORMA EL ORIGINAL PUEDE PROTEGERSE COMPLETAMENTE, INCLUYENDO SU CABECERA. ESTE MODO ES EL IDÓNEO CUANDO ALGUNO DE LOS COMUNICANTES NO ES UN EQUIPO FINAL, SINO UN INTERMEDIARIO.



# CONTENIDOS

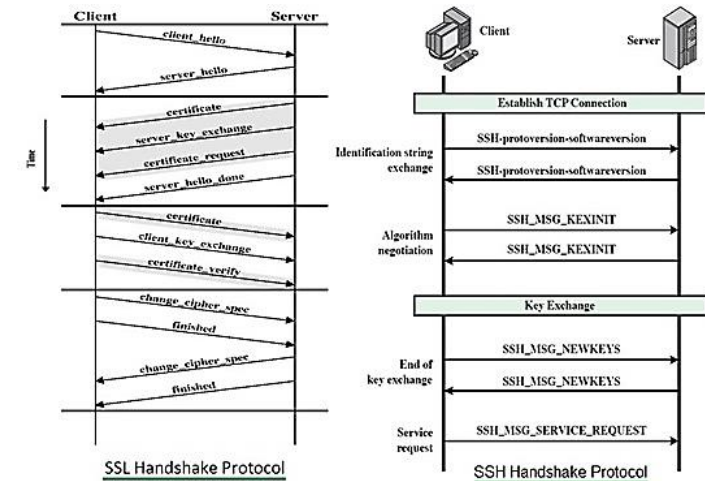
1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
- 4. PROTOCOLOS SSL Y SSH**
5. SISTEMAS SSL VPN
6. TÚNELES CIFRADOS
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

## 4. PROTOCOLOS SSL Y SSH

LOS PROTOCOLOS **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.

HAY DIFERENCIAS ENTRE AMBOS:

- EN **SSH** LO MÁS HABITUAL ES QUE LA AUTENTICACIÓN SE REALICE UTILIZANDO USUARIO Y CONTRASEÑA
- EN **SSL** SE UTILIZAN CERTIFICADOS.



## 4. PROTOCOLOS SSL Y SSH

**SSL** ES UTILIZADO FRECUENTEMENTE EN APLICACIONES EN LAS QUE SE HACE USO DE DATOS SENSIBLES, POR EJEMPLO, EN APLICACIONES BANCARIAS.

**SSH** ES UTILIZADO HABITUALMENTE PARA ENVIAR ÓRDENES O COMANDOS A OTRO ORDENADOR A TRAVÉS DE INTERNET.

SSH	SSL/TLS
Secure shell	Secure Socket Layer/Transport Socket Layer
Runs on port 22	Runs on port 443
SSH is made for securely executing commands on a server	Used for securely communicating personal information
Uses a username and password authentication system to establish a secure connection	Typically uses X.509 digital certificates for client and server authentication
Based on network tunnels	Based on digital certificates
A remote protocol	A security protocol
Made to reduce security threats for remote server login	Created to allow secure transition of data between a server and the browser
It follows the authentication process by a server's verification that is done by the client, a session key and a client's authentication	It follows the authentication process by the exchange of digital certificate

## 4. PROTOCOLOS SSL Y SSH

### SECURE SOCKETS LAYER (SSL)

EL PROTOCOLO **SSL** FUE DISEÑADO ORIGINALMENTE POR NETSCAPE.

LA PRIMERA VERSIÓN NUNCA LLEGÓ A ENTREGARSE, EN LA SEGUNDA SE DETECTARON ERRORES DE SEGURIDAD IMPORTANTES Y EN 1996 SE PRESENTÓ LA VERSIÓN SSL 3.0.

CUANDO SE LLEGÓ A UN CONSENSO SOBRE SU ESPECIFICACIÓN, SE PUBLICÓ BAJO EL NOMBRE DE **TLS (TRANSPORT SECURITY LAYER)**, LO QUE SE PUEDE CONSIDERAR COMO LA SIGUIENTE VERSIÓN DE **SSL**.

EL PROTOCOLO **SSL TRABAJA POR ENCIMA DEL NIVEL DE TRANSPORTE (NIVEL 4 OSI), PROPORCIONANDO SEGURIDAD A CUALQUIER SERVICIO A NIVEL DE APLICACIÓN (NIVEL 5 OSI).**

## 4. PROTOCOLOS SSL Y SSH

### SECURE SOCKETS LAYER (SSL)

SE CARACTERIZA POR SOPORTAR **COMPRESIÓN** (OPCIONAL), **HACER USO DE CERTIFICADOS X.509** Y PROPORCIONAR LOS SERVICIOS DE SEGURIDAD DE **AUTENTICACIÓN EN SERVIDOR** (OBLIGATORIA), **AUTENTICACIÓN EN CLIENTE** (OPCIONAL), **INTEGRIDAD**, **CONFIDENCIALIDAD** Y **NO REPUDIO DEL CLIENTE** (OPCIONAL).



## 4. PROTOCOLOS SSL Y SSH

### SECURE SOCKETS LAYER (SSL)

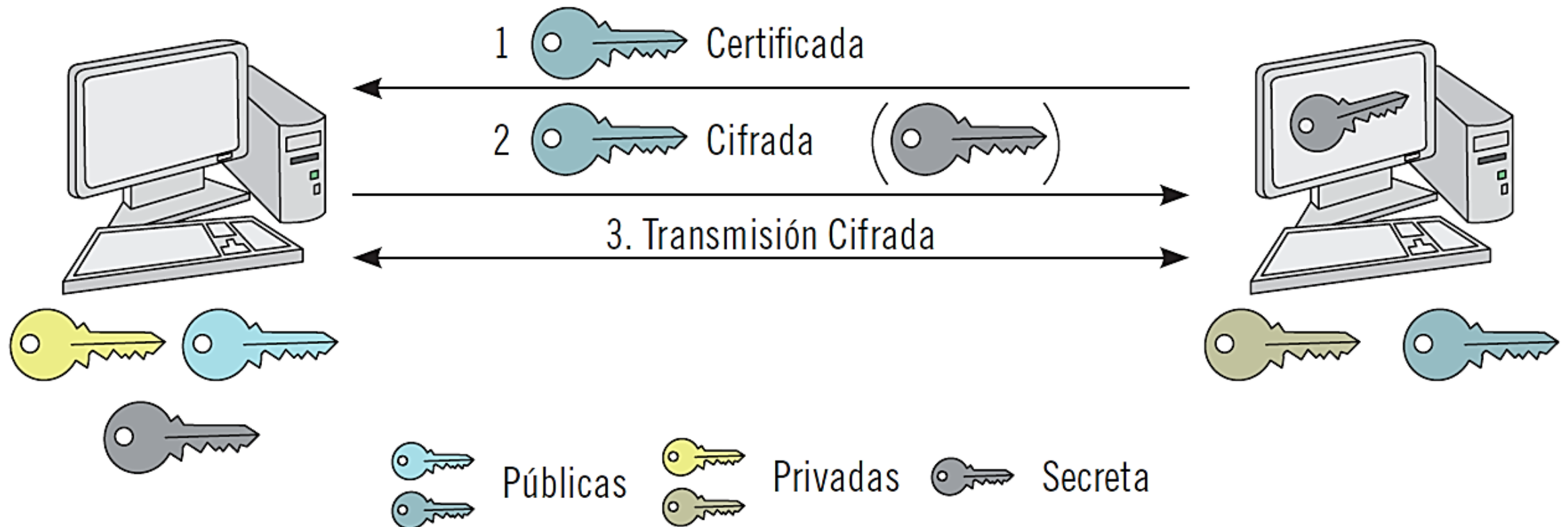
EL FUNCIONAMIENTO DEL PROTOCOLO SE PRESENTA EN LA SIGUIENTE FIGURA. CADA EXTREMO DE LA COMUNICACIÓN POSEE UN PAR DE CLAVES (JUNTO CON EL CERTIFICADO ASOCIADO Y CONSIDERANDO QUE EN EL CLIENTE ES OPCIONAL). SUPONIENDO QUE UN CLIENTE **A** QUIERE ESTABLECER COMUNICACIÓN CON UN SERVIDOR **B**.

- 1) **B** ENVÍA SU CLAVE PÚBLICA CERTIFICADA A **A**.
- 2) **A**, CREA UNA CLAVE SECRETA
- 3) SE LA ENVÍA A **B**
- 4) LA TRANSMISIÓN DE INFORMACIÓN COMIENZA, LA INFORMACIÓN SE TRANSMITIRÁ CIFRADA MEDIANTE LA CLAVE SECRETA INTERCAMBIADA.

## 4. PROTOCOLOS SSL Y SSH

### SECURE SOCKETS LAYER (SSL)

#### Funcionamiento genérico de SSL





## **4. PROTOCOLOS SSL Y SSH**

### **SECURE SOCKETS LAYER (SSL)**

**SSL ESTÁ FORMADO POR VARIOS SUB-PROTOCOLOS:**

- **PROTOCOLO DE SALUTACIÓN**
- **PROTOCOLO DE REGISTRO**
- **PROTOCOLO DE CAMBIO DE ESPECIFICACIÓN DE CIFRADO**
- **PROTOCOLO DE AVISO**

## **4. PROTOCOLOS SSL Y SSH**

### **SECURE SOCKETS LAYER (SSL)**

#### **PROTOCOLO DE SALUTACIÓN**

**SE EJECUTA ANTES DE TRANSMITIR LOS DATOS DE LA APLICACIÓN.**

**EN ESTE PROTOCOLO EL CLIENTE Y EL SERVIDOR ACUERDAN LOS ALGORITMOS QUE USARÁN PARA CIFRAR Y APLICAR CONTROL DE INTEGRIDAD SOBRE LOS DATOS QUE SE INTERCAMBIEN.**

**PARA ELLO, EL CLIENTE OFRECE LAS OPCIONES DISPONIBLES Y EL SERVIDOR SELECCIONA AQUELLA QUE MÁS LE CONVIENE.**

**EN ESTE PROTOCOLO EL SERVIDOR SE AUTENTICA FRENTE AL CLIENTE (ENVIÁNDOLE SU CERTIFICADO DE CLAVE PÚBLICA). OPCIONALMENTE, TAMBIÉN EL CLIENTE SE PUEDE AUTENTICAR.**

## **4. PROTOCOLOS SSL Y SSH**

### **SECURE SOCKETS LAYER (SSL)**

#### **PROTOCOLO DE REGISTRO**

**ESTE PROTOCOLO UTILIZA LOS ALGORITMOS DEFINIDOS POR EL DE SALUTACIÓN PARA CIFRAR Y APLICAR EL CONTROL DE INTEGRIDAD SOBRE LOS DATOS.**

**TAMBIÉN COMPRIME LOS DATOS, HACIENDO QUE LA TRANSMISIÓN SEA MÁS LIGERA.**

## **4. PROTOCOLOS SSL Y SSH**

### **SECURE SOCKETS LAYER (SSL)**

#### **PROTOCOLO DE CAMBIO DE ESPECIFICACIÓN DE CIFRADO.**

**SE EMPLEA PARA QUE UNA DE LAS PARTES ANUNCIE A LA OTRA QUE QUIERE CAMBIAR LA MANERA DE CIFRAR LA INFORMACIÓN.**

SOLO CONSISTE EN UN MENSAJE, QUE UNA PARTE ENVÍA A OTRA EN EL MOMENTO OPORTUNO. DE HECHO, EL PROTOCOLO DE SALUTACIÓN SIEMPRE FINALIZA CON ESE MENSAJE.

DE ESTA MANERA, LOS ACUERDOS DE ESE PROTOCOLO EMPIEZAN A UTILIZARSE.

## 4. PROTOCOLOS SSL Y SSH

### SECURE SOCKETS LAYER (SSL)

#### PROTOCOLO DE AVISO

TIENE COMO FUNCIÓN **AVISAR** A CUALQUIERA DE LOS PARTICIPANTES DE **ALGÚN TIPO DE INCIDENCIA OCURRIDA**.

PUEDE SER DEBIDA A UN ERROR FATAL O UNA ADVERTENCIA. SI EL NIVEL ES FATAL (POR EJEMPLO, SI NO HAY ACUERDO EN EL PROTOCOLO DE SALUTACIÓN) LA CONEXIÓN SSL ASOCIADA SE FINALIZA.

ENTRE LAS ADVERTENCIAS SE PUEDEN DESTACAR LA RECEPCIÓN DE UN CERTIFICADO EXPIRADO O EL HECHO DE QUE UNA DE LAS ENTIDADES NO DESEE MANDAR MÁS MENSAJES EN UNA DETERMINADA CONEXIÓN.

## 4. PROTOCOLOS SSL Y SSH

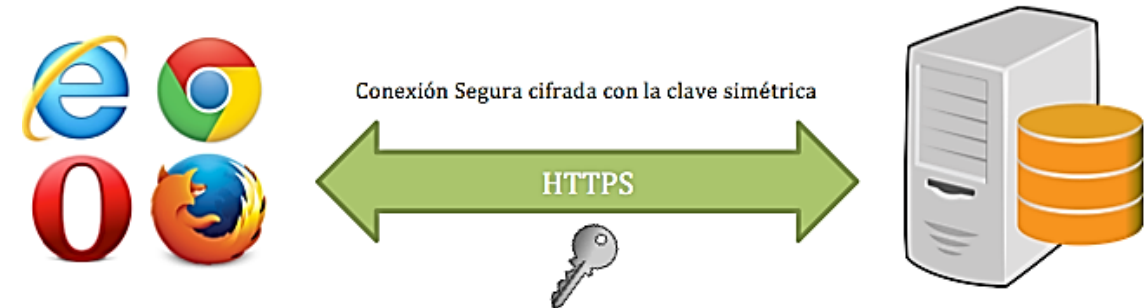
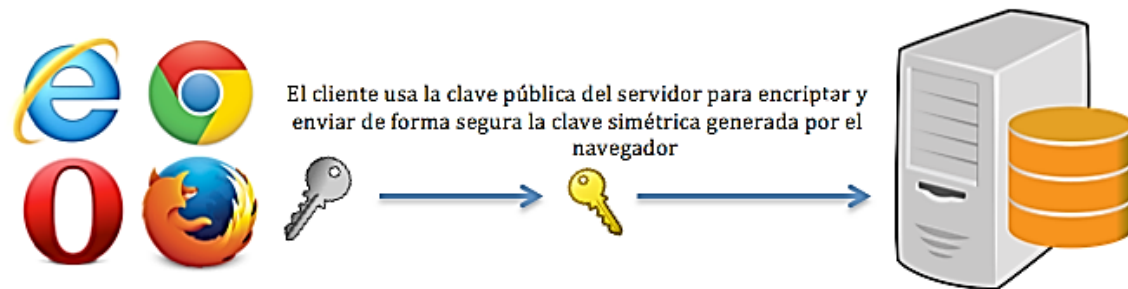
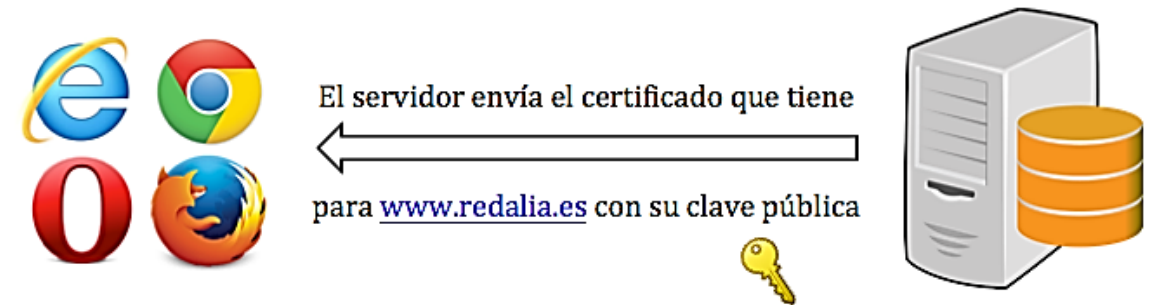
### SECURE SOCKETS LAYER (SSL)

VEAMOS LO QUE SUCEDERÍA CUANDO UN CLIENTE ACCEDERÍA A UN SITIO WEB DE UN SERVIDOR CON UN CERTIFICADO SSL A TRAVÉS DEL PROTOCOLO HTTPS:

1. **UN USUARIO REALIZA UNA PETICIÓN HTTP SEGURA A TRAVÉS DE UN NAVEGADOR A UN SITIO WEB.**
2. **EL SERVIDOR DONDE ESTÁ ALOJADO EL SITIO WEB ENVÍA EL CERTIFICADO QUE INCLUYE SU CLAVE PÚBLICA.**
3. **EL NAVEGADOR COMPRUEBA QUE LA CA SEA DE CONFIANZA.** EN CASO CONTRARIO, PEDIRÁ AL USUARIO QUE ACEPTAR EL CERTIFICADO BAJO SU RESPONSABILIDAD.
4. **EL NAVEGADOR GENERARÁ UNA CLAVE SIMÉTRICA, QUE SERÁ CIFRADA MEDIANTE LA CLAVE PÚBLICA DEL SERVIDOR PARA SER ENVIADA DE MANERA SEGURA AL MISMO.**
5. **LA COMUNICACIÓN YA SE HA ESTABLECIDO DE MANERA SEGURA, Y SERÁ CIFRADA EN AMBOS SENTIDOS.**

## 4. PROTOCOLOS SSL Y SSH

### SECURE SOCKETS LAYER (SSL)





## 4. PROTOCOLOS SSL Y SSH

### SECURE SHELL (SSH)

**SECURE SHELL (SSH)** ES UN PROTOCOLO DISEÑADO CON LOS PROPÓSITOS DE SER SIMPLE Y FÁCIL DE PROGRAMAR.

LA VERSIÓN INICIAL ESTABA PENSADA PARA **PERMITIR QUE UNA PERSONA PUDIESE ABRIR UNA SESIÓN EN UN ORDENADOR REMOTO.**

EL PROPÓSITO ERA **REEMPLAZAR AL PROTOCOLO TELNET Y A OTROS ESQUEMAS QUE NO PROPORCIONABAN SEGURIDAD.**

**SSH PUEDE SER UTILIZADO NO SOLO PARA EL PROPÓSITO ANTERIOR, SINO TAMBIÉN PARA FUNCIONES COMO *TRANSFERENCIAS DE FICHEROS O ENVÍOS DE CORREOS.***

## **4. PROTOCOLOS SSL Y SSH**

### **SECURE SHELL (SSH)**

ESTE PROTOCOLO ES UTILIZADO POR MÚLTIPLES APLICACIONES CLIENTE-SERVIDOR Y ESTÁ DISPONIBLE EN LA MAYORÍA DE LOS SISTEMAS OPERATIVOS.

DE HECHO, SE HA CONVERTIDO EN EL **MÉTODO HABITUAL PARA REALIZAR INICIO DE SESIÓN REMOTA Y ESTABLECIMIENTO DE TÚNELES.**

**SSH SE COMPONE DE TRES TIPOS DE PROTOCOLOS:**

- **EL PROTOCOLO DE LA CAPA DE TRANSPORTE**
- **EL PROTOCOLO DE AUTENTICACIÓN DE USUARIOS**
- **EL PROTOCOLO DE CONEXIÓN**

## **4. PROTOCOLOS SSL Y SSH**

### **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. SE EJECUTA EN LA CAPA DE TRANSPORTE (NIVEL 4 DEL MODELO OSI).**

**DENTRO DE ESTE PROTOCOLO SE ESTABLECEN LAS CLAVES DE LOS HOST.**

**LA AUTENTICACIÓN DEL SERVIDOR SE REALIZA EN BASE AL PAR O PARES DE CLAVES (PÚBLICO-PRIVADA) QUE DICHO SERVIDOR POSEE.**

## **4. PROTOCOLOS SSL Y SSH**

### **SECURE SHELL (SSH)**

#### **PROTOCOLO DE LA CAPA DE TRANSPORTE**

**PARA AUTENTICAR AL SERVIDOR, EL CLIENTE DISPONE DE DOS OPCIONES:**

- 1. EL CLIENTE PUEDE MANTENER LOCALMENTE UNA BASE DE DATOS QUE ASOCIE CADA NOMBRE DE HOST CON SU CLAVE PÚBLICA. EVITA LA NECESIDAD DE UNA ADMINISTRACIÓN CENTRALIZADA, ASÍ COMO EL USO DE UN TERCERO DE CONFIANZA PARA REALIZAR LA COORDINACIÓN. EL MANTENIMIENTO PUEDE SER COSTOSO.**
- 2. LA ASOCIACIÓN NOMBRE DE HOST-CLAVE PÚBLICA ES CERTIFICADA POR UNA AUTORIDAD. EL CLIENTE PUEDE VERIFICAR LA VALIDEZ DE LAS CLAVES PROPORCIONADAS POR DETERMINADAS AUTORIDADES, UTILIZADO LA CLAVE DE LA AUTORIDAD RAÍZ. SE DISMINUYEN LOS PROBLEMAS DE GESTIÓN PORQUE EL CLIENTE SOLO HA DE ALMACENAR DE FORMA SEGURA LA CLAVE DE UNA AUTORIDAD. TODAS LAS CLAVES DE LOS HOSTS TIENEN QUE SER CERTIFICADAS POR UNA AUTORIDAD.**

## **4. PROTOCOLOS SSL Y SSH**

### **SECURE SHELL (SSH)**

#### **PROTOCOLO DE LA CAPA DE TRANSPORTE**

TRAS ESTA AUTENTICACIÓN, SE PROCEDE A REALIZAR LOS INTERCAMBIOS DE PAQUETES. PARA ELLO, EL CLIENTE Y EL SERVIDOR ESTABLECEN UNA CONEXIÓN Y COMIENZA EL INTERCAMBIO DE DATOS.

ESTOS PAQUETES CONTIENEN LA CARGA ÚTIL, A LA QUE SE APLICA COMPRESIÓN, CIFRADO Y CONTROL DE INTEGRIDAD UTILIZANDO UN CÓDIGO MAC.

LOS ALGORITMOS DE CIFRADO, CONTROL DE INTEGRIDAD Y COMPRESIÓN SON NEGOCIADOS EN ESTE PROTOCOLO, ANTES DE QUE SE PRODUZCA EL INTERCAMBIO.

## **4. PROTOCOLOS SSL Y SSH**

### **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**

**EN CUANTO A LOS MÉTODOS DE AUTENTICACIÓN, ES POSIBLE INDICAR:**

- **EL MÉTODO DE CLAVE PÚBLICA**
- **EL MÉTODO DE CONTRASEÑA**
- **EL MÉTODO HOSTBASED**

## **4. PROTOCOLOS SSL Y SSH**

### **SECURE SHELL (SSH)**

#### **PROTOCOLO DE AUTENTICACIÓN DE USUARIOS**

##### **MÉTODO DE CLAVE PÚBLICA,**

EN EL QUE EL CLIENTE ENVÍA AL SERVIDOR SU CLAVE PÚBLICA FIRMADA PARA QUE LA VERIFIQUE.

##### **MÉTODO DE CONTRASEÑA**

EN EL QUE EL CLIENTE ENVÍA UNA CONTRASEÑA AL SERVIDOR.

##### **MÉTODO HOSTBASED**

EN EL QUE EL CLIENTE ENVÍA UNA FIRMA AL SERVIDOR HACIENDO USO DE LA CLAVE DE SU HOST, CONSIGUIENDO QUE EL SERVIDOR CONFÍE EN EL HOST CUANDO ÉSTE INDIQUE QUE EL USUARIO SE HA AUTENTICADO.



## **4. PROTOCOLOS SSL Y SSH**

### **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 PARA EJECUTAR ÓRDENES EN UN ORDENADOR REMOTO (CANAL DE SESIÓN) O PARA USAR EN REMOTO SUS PROGRAMAS QUE UTILIZAN REPRESENTACIÓN GRÁFICA (CANAL X11).**

## 4. PROTOCOLOS SSL Y SSH

### SECURE SHELL (SSH)

#### PROTOCOLO DE CONEXIÓN

UN CANAL PASA POR TRES ESTADOS DISTINTOS EN FUNCIÓN DEL MOMENTO DE TRANSMISIÓN DE DATOS:

- **APERTURA DEL CANAL**, INDICANDO ESENCIALMENTE EL TIPO DE CANAL, EL TAMAÑO DE DATOS A ENVIAR Y EL TAMAÑO MÁXIMO DE LOS PAQUETES.
- **TRANSMISIÓN DE LOS DATOS**, ES DECIR, EL USO PROPIAMENTE DICHO DEL CANAL.
- **CIERRE DEL CANAL**, PARA CONCLUIR LA COMUNICACIÓN POR PARTE DE CUALQUIERA DE LOS PARTICIPANTES.

## 4. PROTOCOLOS SSL Y SSH

### SECURE SHELL (SSH)

UNA CARACTERÍSTICA MUY IMPORTANTE DE **SSH** ES LA **POSIBILIDAD DE REALIZAR REDIRECCIÓN DE PUERTOS**, TANTO DEL CLIENTE COMO DEL SERVIDOR.

ESTO PERMITE ESTABLECER LA CONEXIÓN **SSH** USANDO UNOS PUERTOS Y QUE CADA UNO DE LOS EXTREMOS LO REENVÍE A OTRO DE SUS PUERTOS.

ESTO ES ESPECIALMENTE **ÚTIL CUANDO EXISTEN MECANISMOS DE PROTECCIÓN, COMO CORTAFUEGOS**, QUE IMPIDEN QUE CIERTOS PUERTOS PUEDAN SER USADOS PARA RECIBIR DATOS DESDE OTROS ORDENADORES.

GRACIAS A LA REDIRECCIÓN, SE PUEDEN RECIBIR DATOS POR UN PUERTO (PERMITIDO POR EL CORTAFUEGOS) Y REENVIARLOS A OTRO DONDE REALMENTE ESTÉ ESPERANDO EL PROGRAMA QUE MANEJA LA CONEXIÓN **SSH**.

# CONTENIDOS

1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
- 5. SISTEMAS SSL VPN**
6. TÚNELES CIFRADOS
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

## 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.

LA UTILIZACIÓN DE ESTE TIPO DE **SSL** SE PUEDE CONSIDERAR MUY SENCILLA PARA LOS USUARIOS.

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** CONTRA LA SEGURIDAD:

- NO REQUIERE LA INSTALACIÓN DE NINGÚN SOFTWARE EN **EL CLIENTE**. ÉSTE **PUEDE ESTAR INFECTADO** CON ALGÚN TIPO MALWARE, DE FORMA QUE DICHO PROGRAMA PODRÍA INFECTAR A LA ENTIDAD DONDE SE CONECTA.

PARA RESOLVER ESTE PROBLEMA, LAS ENTIDADES CON LAS QUE SE ESTABLECE LA VPN FUERZAN LA VERIFICACIÓN DE INTEGRIDAD EN EL CLIENTE, **RECHAZANDO LAS CONEXIONES** EN CASO DE **NO DISPONER DE CIERTAS MEDIDAS DE SEGURIDAD ESTABLECIDAS EN UNA POLÍTICA**, POR EJEMPLO, INSTALACIÓN DE ANTIVIRUS O DE UN CORTAFUEGOS.

## 5. SISTEMAS SSL VPN

- OTRO DE LOS RIESGOS SE ASOCIA CON LA **INFORMACIÓN ALMACENADA EN LOS HISTORIALES**. CUANDO SE REALIZA UNA CONEXIÓN CON UN NAVEGADOR, SE DEJAN RASTROS INDICANDO DÓNDE Y PARA QUÉ FUERON UTILIZADOS (COOKIES, HISTORIAL DE URL, ETC.). EL PROBLEMA SE AGRAVA SI LA COMUNICACIÓN SE ESTABLECE DESDE UN ORDENADOR PÚBLICO, YA QUE LA INFORMACIÓN ALMACENADA PUEDE QUEDAR A DISPOSICIÓN DE TERCEROS NO AUTORIZADOS (POR EJEMPLO, OTROS USUARIOS DE UN CIBERCAFÉ). POR ELLO, **EL EXTREMO AL QUE SE ESTABLECE LA CONEXIÓN VPN SSL SUELE INCLUIR FUNCIONES PARA ELIMINAR LA INFORMACIÓN CREADA EN CADA SESIÓN.**



## 5. SISTEMAS SSL VPN

- 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**. ESTO FACILITA LA EXISTENCIA DE ATAQUES REMOTOS DE DESCUBRIMIENTO DE CONTRASEÑAS. UN MODO DE SOLUCIONARLO SERÍA **UTILIZAR MÉTODOS ROBUSTOS DE AUTENTICACIÓN, COMO ES LA AUTENTICACIÓN DE DOS FACTORES**.

# CONTENIDOS

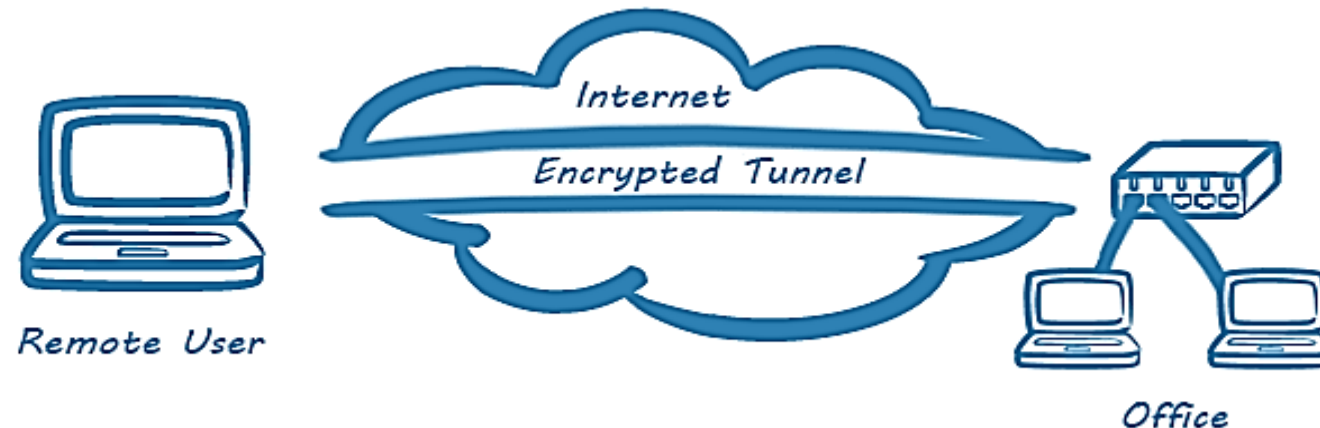
1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
5. SISTEMAS SSL VPN
- 6. TÚNELES CIFRADOS**
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

## 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.



## 6. TÚNELES CIFRADOS

PARA CONSTRUIRLOS SE UTILIZAN LOS **PROTOCOLOS DE TUNELADO**. A CONTINUACIÓN, SE REVISAN LOS PROTOCOLOS MÁS HABITUALES QUE CUMPLEN CON ESTE OBJETIVO:

- **OPENVPN**
- **WIREGUARD**
- **PPTP**
- **IKEV2/IPSEC**
- **L2TP/IPSEC**
- **SSTP**
- **SOFTETHER**

## 6. TÚNELES CIFRADOS

### OPENVPN: EL PROTOCOLO VPN N.º 1

#### PROS

- COMPATIBILIDAD NATIVA CON CASI TODOS LOS SERVICIOS DE VPN
- CÓDIGO ABIERTO
- PROBADO EXHAUSTIVAMENTE DURANTE UN LARGO PERIODO DE TIEMPO
- NO SE CONOCEN VULNERABILIDADES
- LOS USUARIOS PUEDEN ELEGIR ENTRE LAS VERSIONES UDP Y TCP
- COMPATIBLE CON UNA AMPLIA GAMA DE CIFRADOS, INCLUIDO AES-256
- COMPATIBLE CON PERFECT FORWARD SECRECY (PFS)
- PROTOCOLO POR EXCELENCIA DURANTE LAS ÚLTIMAS DOS DÉCADAS

## 6. TÚNELES CIFRADOS

### OPENVPN: EL PROTOCOLO VPN N.º 1

#### CONTRAS

- ALTO CONSUMO DE ANCHO DE BANDA
- NO ES EL PROTOCOLO VPN MÁS RÁPIDO QUE EXISTE
- GRAN BASE DE CÓDIGO

## 6. TÚNELES CIFRADOS

### WIREGUARD: UN PROTOCOLO NUEVO IMPRESIONANTE

#### PROS

- BASE DE CÓDIGO MUY LIGERA
- VELOCIDADES EXTREMADAMENTE RÁPIDAS
- CÓDIGO ABIERTO
- CONSUMO DE DATOS LIMITADO
- NO SE CONOCEN PROBLEMAS DE SEGURIDAD
- BUENO EN LA GESTIÓN DE CAMBIOS DE RED
- COMPATIBLE CON SECRETO PERFECTO DIRECTO
- CONFIGURACIÓN MANUAL MUY SENCILLA



## 6. TÚNELES CIFRADOS

### WIREGUARD: UN PROTOCOLO NUEVO IMPRESIONANTE

#### CONTRAS

- PROBLEMAS DE PRIVACIDAD CON LA CONFIGURACIÓN PREDETERMINADA
- NO ES COMPATIBLE CON TODOS LOS SERVICIOS DE VPN
- HACE FALTA MÁS TIEMPO PARA PROBARLO Y ANALIZARLO DE FORMA EXHAUSTIVA
- SOLO SE PUEDE UTILIZAR CON UDP

## 6. TÚNELES CIFRADOS

### PPTP: DESFASADO E INSEGURO

#### PROS

- VELOCIDADES MUY ALTAS
- COMPATIBILIDAD NATIVA CON CASI TODAS LAS PLATAFORMAS
- FÁCIL DE CONFIGURAR

#### CONTRAS

- SE HAN DETECTADO VULNERABILIDADES DE SEGURIDAD
- NO ES COMPATIBLE CON LAS CLAVES DE CIFRADO DE 256 BITS
- NO PUEDE SORTEAR LA CENSURA
- HA SIDO DESCIFRADO POR LA NSA
- NO ES EFICAZ COMO HERRAMIENTA DE SEGURIDAD

## 6. TÚNELES CIFRADOS

### IKEV2/IPSEC: UN GRAN PROTOCOLO PARA USUARIOS MÓVILES

#### PROS

- PROPORCIONA UNA CONEXIÓN MUY ESTABLE
- OFRECE VELOCIDADES RÁPIDAS
- COMPATIBLE CON UNA AMPLIA GAMA DE CIFRADOS, INCLUIDO AES-256
- BUENO EN LA GESTIÓN DE CAMBIOS DE RED
- COMPATIBLE CON SECRETO PERFECTO DIRECT

#### CONTRAS

- CÓDIGO CERRADO (EXCEPTO PARA LINUX)
- ES PROBABLE QUE ESTÉ COMPROMETIDO POR LA NSA
- POCO FIABLE PARA SORTEAR CORTAFUEGOS

## 6. TÚNELES CIFRADOS

### L2TP/IPSEC: ES LENTO Y NO MERECE LA PENA UTILIZARLO

#### PROS

- EL ENCAPSULAMIENTO DOBLE OFRECE MÁS SEGURIDAD
- COMPATIBILIDAD NATIVA CON LA MAYORÍA DE LAS PLATAFORMAS
- COMPATIBLE CON UNA AMPLIA GAMA DE CIFRADOS, INCLUIDO AES-256

#### CONTRAS

- ES PROBABLE QUE ESTÉ COMPROMETIDO POR LA NSA
- MÁS LENTO QUE OTROS PROTOCOLOS VPN
- SUSCEPTIBLE DE SUFRIR ATAQUES DE INTERMEDIARIO

## 6. TÚNELES CIFRADOS

### SSTP: CÓDIGO CERRADO CON POSIBLES RIESGOS

#### PROS

- BUENO PARA SALTARSE CORTAFUEGOS
- FÁCIL DE CONFIGURAR EN WINDOWS
- USA UN FUERTE CIFRADO AES-256

#### CONTRAS

- CÓDIGO CERRADO
- PUEDE SER SUSCEPTIBLE DE SUFRIR ATAQUES DE INTERMEDIARIO
- PREOCUPANTES VÍNCULOS CON LA NSA

## 6. TÚNELES CIFRADOS

### SOFTETHER: UNA BUENA OPCIÓN PARA ELUDIR LA CENSURA
























#### PROS

- CÓDIGO ABIERTO
- VELOCIDADES MUY ALTAS
- COMPATIBLE CON UNA AMPLIA GAMA DE CIFRADOS, INCLUIDO AES-256
- BUENO PARA SALTARSE CORTAFUEGOS

#### CONTRAS

- HAY QUE CONFIGURARLO MANUALMENTE PARA QUE SEA SEGURO
- NO OFRECE COMPATIBILIDAD NATIVA CON NINGÚN SISTEMA OPERATIVO
- SOLO ES COMPATIBLE CON ALGUNOS SERVICIOS VPN

## 6. TÚNELES CIFRADOS

No es Nada Seguro 	Algunos Problemas de Seguridad 	Muy Seguro 	El Más Seguro 
<b>PPTP</b>  Anticuado  Fácil de hackear	<b>L2TP/IPSec</b>  Seguro cuando se usa con AES  Vulnerable a ataques MITM cuando se usa con llave compartida  Puede haber sido interferido por la NASA	<b>IKEv2/IPSec</b>  Muy rápido  Funciona bien en dispositivos móviles  Código cerrado	<b>OpenVPN</b>  De código abierto  Protocolo estándar  Rápido
	<b>SSTP</b>  Vulnerable a ataques MITM Poodle  De código cerrado	<b>Wireguard</b>  Código abierto  Rápido y seguro  Relativamente nuevo	
		<b>SoftEther</b>  Muy rápido  Ideal para eludir la censura  Require configuración manual para ser seguro	



## 6. TÚNELES CIFRADOS

Protocolo	Cifrado	Velocidad	Fiabilidad	Puntos débiles
OpenVPN TCP	256 bits	Moderada	Muy alta	No se conocen
OpenVPN UDP	256 bits	Rápida	Alta	No se conocen
PPTP	128 bits	Muy rápida	Moderada	Conocidos
L2TP/IPSec	256 bits	Moderada	Moderada	Se sospechan
SSTP	256 bits	Rápida	Muy alta	Se sospechan
SoftEther	256 bits	Muy rápida	Muy alta	Necesita arreglos
IKEv2/IPSec	256 bits	Muy rápida	Alta	Se sospechan
WireGuard	256 bits	Muy rápida	Alta	No se conocen

# CONTENIDOS

1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
5. SISTEMAS SSL VPN
6. TÚNELES CIFRADOS
7. **VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN**

## 7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

**OPENVPN** ES EL PROTOCOLO VPN MÁS SEGURO QUE EXISTE.

ES LA MEJOR OPCIÓN CUANDO LA PRIVACIDAD Y LA SEGURIDAD SON FUNDAMENTALES Y NO TE IMPORTA PERDER UN POCO DE VELOCIDAD Y FLEXIBILIDAD.

DEBERÍAS USAR **OPENVPN** PARA ACCEDER A INTERNET GRATIS EN PAÍSES CON UN ALTO NIVEL DE CENSURA O PARA USAR TORRENTS.

SI **OPENVPN** NO ESTÁ DISPONIBLE, **SOFTETHER** ES UNA BUENA ALTERNATIVA PARA EVITAR LA CENSURA.

## 7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

**WIREGUARD** ES EL PROTOCOLO VPN MÁS RÁPIDO. PARECE SER EXTREMADAMENTE SEGURO, PERO SU CORTA VIDA HACE QUE SIGAMOS PREFIRIENDO **OPENVPN** PARA ACTIVIDADES ALTAMENTE SENSIBLES.

UTILIZA **WIREGUARD** PARA LAS ACTIVIDADES EN LAS QUE LA VELOCIDAD SEA CRUCIAL, COMO LOS **JUEGOS** Y EL **STREAMING**.

**WIREGUARD** ES TAMBIÉN EL PROTOCOLO VPN MÁS EFICIENTE EN CUANTO AL USO DE DATOS. SI USAS UNA VPN EN EL TELÉFONO MÓVIL Y TE PREOCUPA EL CONSUMO DE DATOS, USA **WIREGUARD**. EL CONSUMO DE DATOS SERÁ MÍNIMO.

## 7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

**IKEV2 ES OTRO BUEN PROTOCOLO PARA LOS USUARIOS DE VPN MÓVILES, YA QUE SU PROTOCOLO MOBIKE HACE QUE SEA EL MEJOR PARA GESTIONAR LOS CAMBIOS DE RED FRECUENTES Y REPENTINOS (POR EJEMPLO, ENTRE REDES WI-FI Y DATOS MÓVILES).**

**EL CONSUMO DE DATOS DE IKEV2 NO ES TAN BAJO COMO EL DE WIREGUARD, PERO ES MUCHO MÁS EFICIENTE QUE OTROS PROTOCOLOS COMO OPENVPN.**

# CONTENIDOS

1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
5. SISTEMAS SSL VPN
6. TÚNELES CIFRADOS
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

## RESUMEN

EL ESTABLECIMIENTO DE CANALES SEGUROS DE COMUNICACIÓN ES FUNDAMENTAL PARA EL INTERCAMBIO DE DATOS.

**LAS REDES PRIVADAS VIRTUALES (VPN) Y LOS TÚNELES DE CIFRADO SON ELEMENTOS ESENCIALES.**

GRACIAS A ELLOS ES POSIBLE ESTABLECER COMUNICACIONES SEGURAS ENTRE DOS ENTIDADES O USUARIOS, ELIMINANDO LA NECESIDAD DE TENER QUE ESTAR FÍSICAMENTE EN LA MISMA RED. Y NO SOLO ESO: PERMITEN CREAR UNA COMUNICACIÓN SEGURA UTILIZANDO UN CANAL INSEGURO, COMO PUEDE SER INTERNET.

HAY MÚLTIPLES PROTOCOLOS QUE PERMITEN SU ESTABLECIMIENTO. ENTRE ELLOS CABE DESTACAR **IPSEC, SSL Y SSH.**



## RESUMEN

**IPSEC** ES UN PROTOCOLO QUE ACTÚA EN LA CAPA DE RED Y ESTÁ COMPUESTO ESENCIALMENTE DE LOS PROTOCOLOS DE **INTERNET KEY EXCHANGE (IKE)** Y **ENCAPSULATING SECURITY PAYLOAD (ESP)**.

**SSL** ACTÚA EN UNA CAPA SUPERIOR, EN LA CAPA DE TRANSPORTE, Y SE COMPONE DE LOS PROTOCOLOS DE REGISTRO, SALUTACIÓN, CAMBIO DE ESPECIFICACIÓN DE CIFRADO Y AVISO.

TAMBIÉN EJECUTÁNDOSE EN LA CAPA DE TRANSPORTE, **SSH** ES UN PROTOCOLO DE AUTENTICACIÓN REMOTA COMPUESTO POR LOS PROTOCOLOS DE CAPA DE TRANSPORTE, AUTENTICACIÓN DE USUARIOS Y CONEXIÓN.

## RESUMEN

FINALMENTE, CABE DESTACAR DOS DE LAS ALTERNATIVAS DE **VPN** MÁS EXTENDIDAS: **VPN SSL** Y **VPN IPSEC**.

LA ELECCIÓN ENTRE UNA U OTRA TECNOLOGÍA PARA IMPLEMENTAR UNA VPN DEBE PARTIR, NECESARIAMENTE, DEL ESTUDIO DETALLADO DEL CONTEXTO Y DE LAS NECESIDADES DE LOS USUARIOS.

LAS **VPN SSL** SON INTERESANTES PORQUE PASAN DESAPERCIBIDAS PARA LOS USUARIOS Y SE BASAN EN UTILIZAR EL NAVEGADOR WEB PARA ESTABLECER UNA COMUNICACIÓN ENTRE DOS EXTREMOS.

