COMUNICACIONES SEGURAS

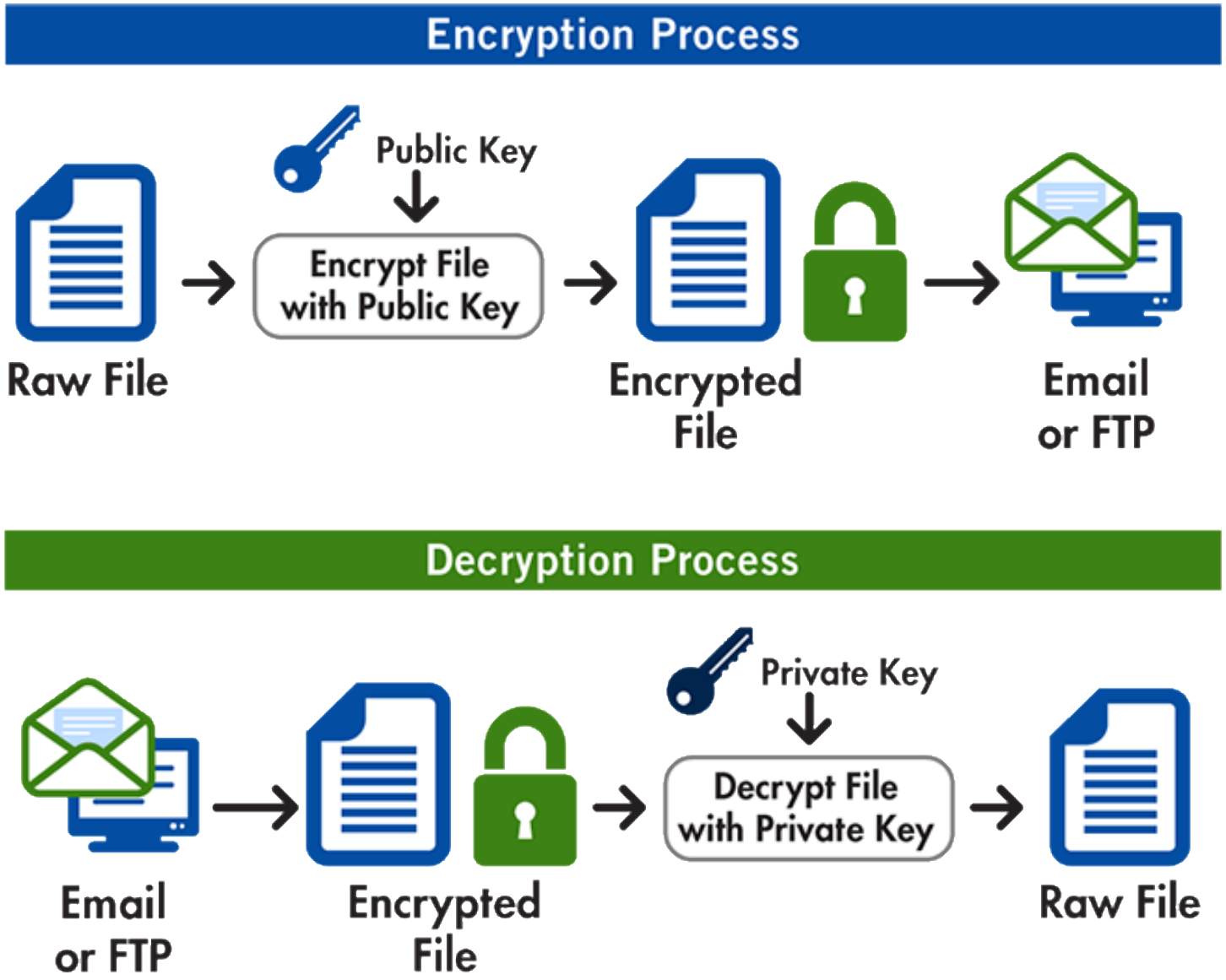
Fundamentos de SSH

- SSH fue diseñado para cerrar esta brecha de seguridad empleando técnicas de cifrado fuerte para todas las partes de la conexión de red.
- SSH encripta la contraseña y el intercambio de todas las transferencias de datos posteriores, por lo que es un protocolo mucho más seguro para el acceso remoto.
- Además de cifrado, SSH proporciona características de transferencia de archivos y la capacidad de tunelizar otros protocolos de red, es decir, permitir que los protocolos no encriptados puedan enviar sus datos a través de una conexión SSH.
- El principal inconveniente de SSH es que el cifrado y descifrado consumen tiempo de CPU.
- Este hecho retrasa las conexiones SSH en comparación con las conexiones directas y puede degradar el rendimiento global del sistema.

- Hay varios servidores SSH disponibles para Linux, pero el más popular con diferencia es el servidor OpenSSH (http://www.openssh.org).
- Este programa fue una de las primeras implementaciones abiertas del protocolo SSH, que fue desarrollado por SSH Communications Security (http://www.ssh.com), cuyo servidor se vende bajo el nombre de SSH Tectia.

Seguridad en los Datos

- Es posible que deseemos cifrar mensajes de correo electrónico o ficheros que se envíen a otra persona a través de otros medios. El E-mail nunca fue diseñado como una herramienta segura de transferencia de datos, y la mayoría de los mensajes de correo electrónico pasan a través de varios servidores de correo electrónico y routers. En cualquiera de estos puntos un cracker podría sniffar tráfico de correo electrónico y recopilar datos sensibles, como tarjetas de crédito o números de DNI.
- La herramienta habitual para la encriptación de correo electrónico es el paquete GNU Privacy Guard (GnuPG o GPG; http://www.gnupg.org).
- Este paquete es una re-implementación de código abierto del propietario Pretty Good Privacy (PGP).

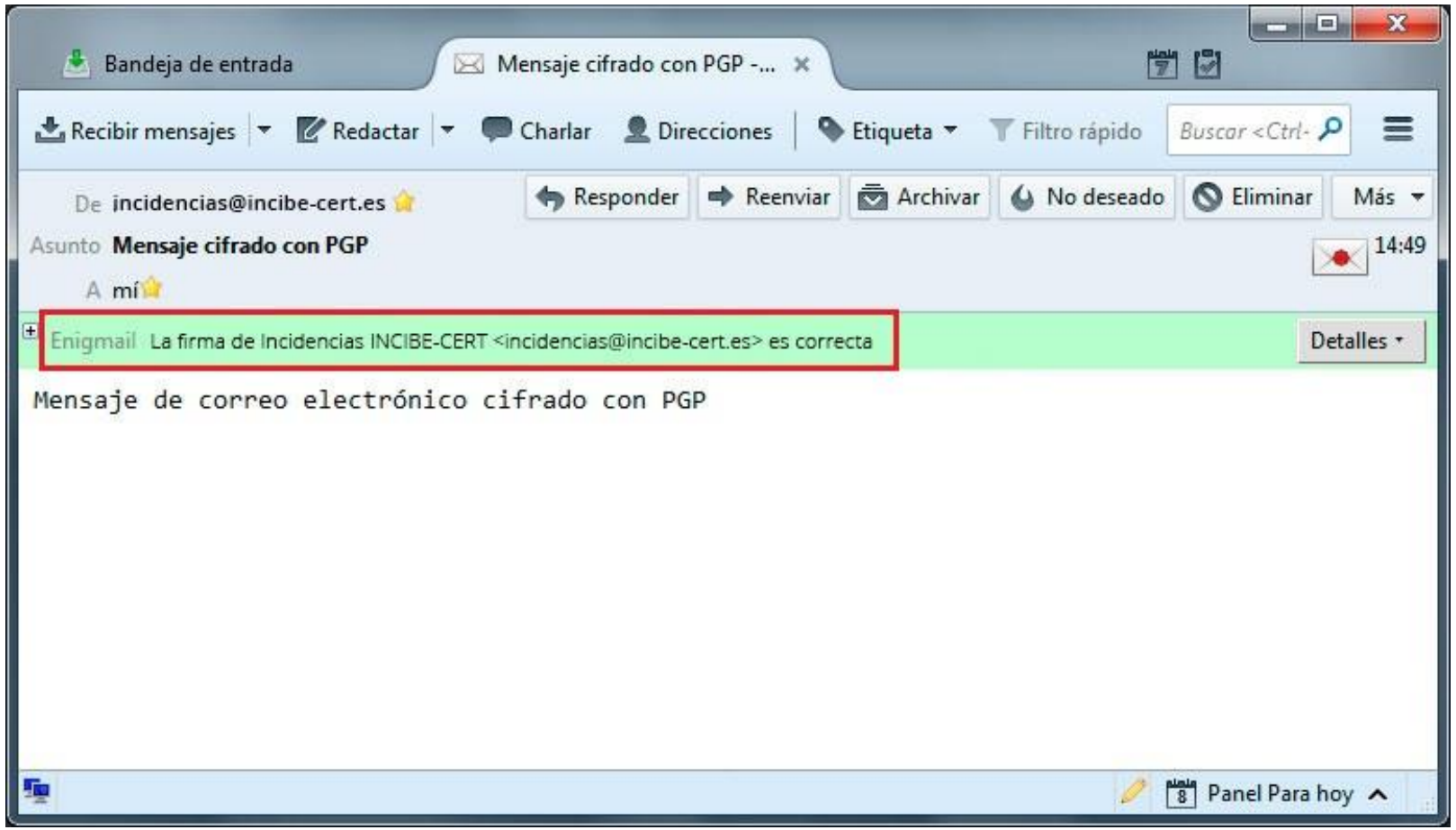

Encryption Process
Public Key
Encrypt File with Public Key
Raw File
Encrypted File
Email or FTP
Decryption Process
Private Key
Decrypt File with Private Key
Email or FTP
Encrypted File
Raw File

- Se puede utilizar OpenPGP mediante multitud de programas

- OpenPGP no solo se puede utilizar en clientes de correo, como los mencionados, sino que es posible utilizarlo en **clientes de correo vía web, como Gmail o Webmail**, por medio de extensiones para el navegador.

Usos

- Entre los principales usos que se puede hacer de OpenPGP se encuentran:
- Comprobar la **autenticidad y la integridad de los correos** por medio de técnicas de cifrado. De esta manera se puede comprobar que quien envía la comunicación es quien dice ser y que esta no ha sido alterada antes de llegar a su destinatario.
- **Cifrar el contenido del correo**, incluidos los archivos adjuntos, para que éste sea solamente accesible por su destinatario. Si un tercero no autorizado se hace con el correo, no tendrá acceso a la información que contiene, incluido cualquier tipo de archivo adjunto.


Bandeja de entrada
Mensaje cifrado con PGP -...
Recibir mensajes
Redactar
Charlar
Direcciones
Etiqueta
Filtro rápido
Buscar <Ctrl-
De incidencias@incibe-cert.es
Responder
Reenviar
Archivar
No deseado
Eliminar
Más
Asunto Mensaje cifrado con PGP
14:49
A mí
Enigmail La firma de Incidencias INCIBE-CERT <incidencias@incibe-cert.es> es correcta
Detalles
Mensaje de correo electrónico cifrado con PGP
Panel Para hoy

VPN

RED PRIVADA VIRTUAL

CONCEPTO VPN

- DEFINICIÓN, QUE SE PUEDE HACER CON UN VPN

TIPOS DE VPN - ARQUITECTURA

- VPN ACCESO REMOTO, PUNTO A PUNTO, TUNNELING, OVER LAN

OBJETIVOS DE IMPLEMENTAR VPN

- FLEXIBILIDAD Y SEGURIDAD

FUNCIONAMIENTO BASICO DE UN VPN

- REQUERIMIENTO MÍNIMO, PROCEDIMIENTO

IMPLEMENTACIÓN DE UN VPN

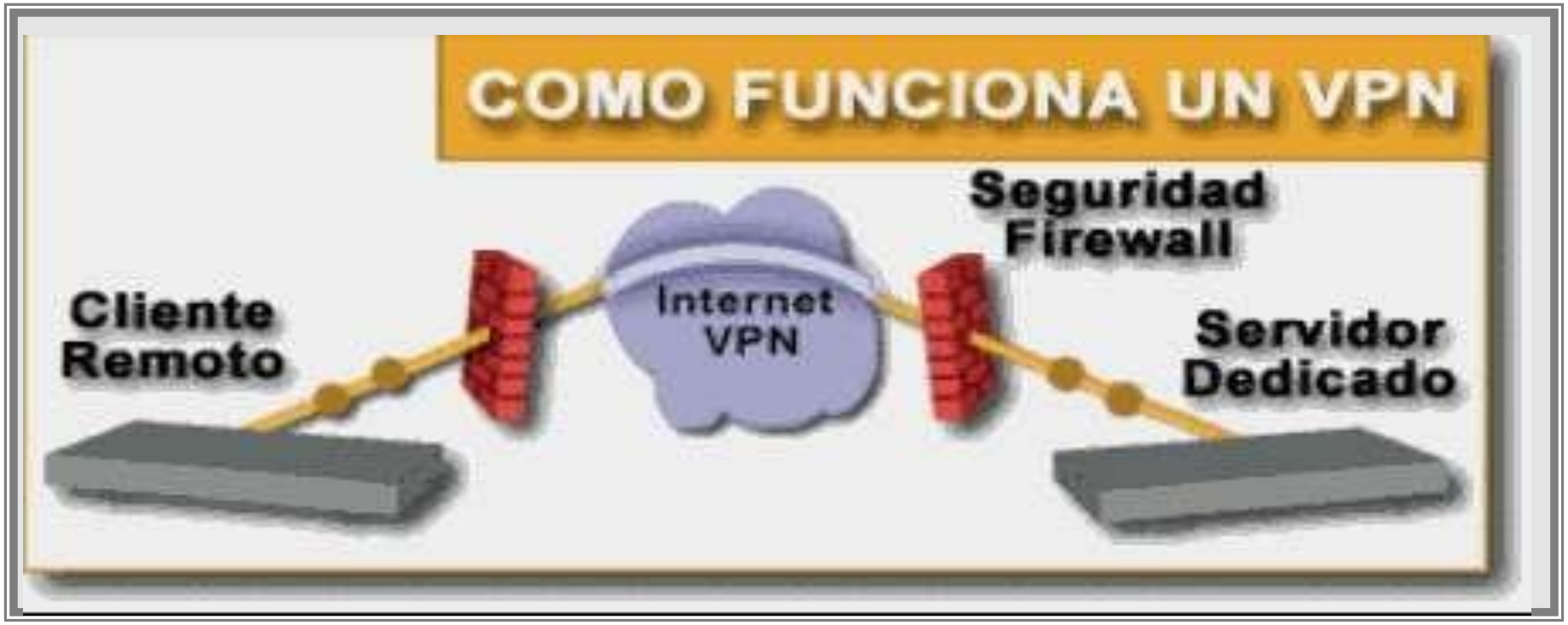
- BASADA EN HARDWARE O EN SOFTWARE

ETAPAS PARA UNA CONEXIÓN VPN

TUNELAMIENTO PROTOCOLOS

VPN

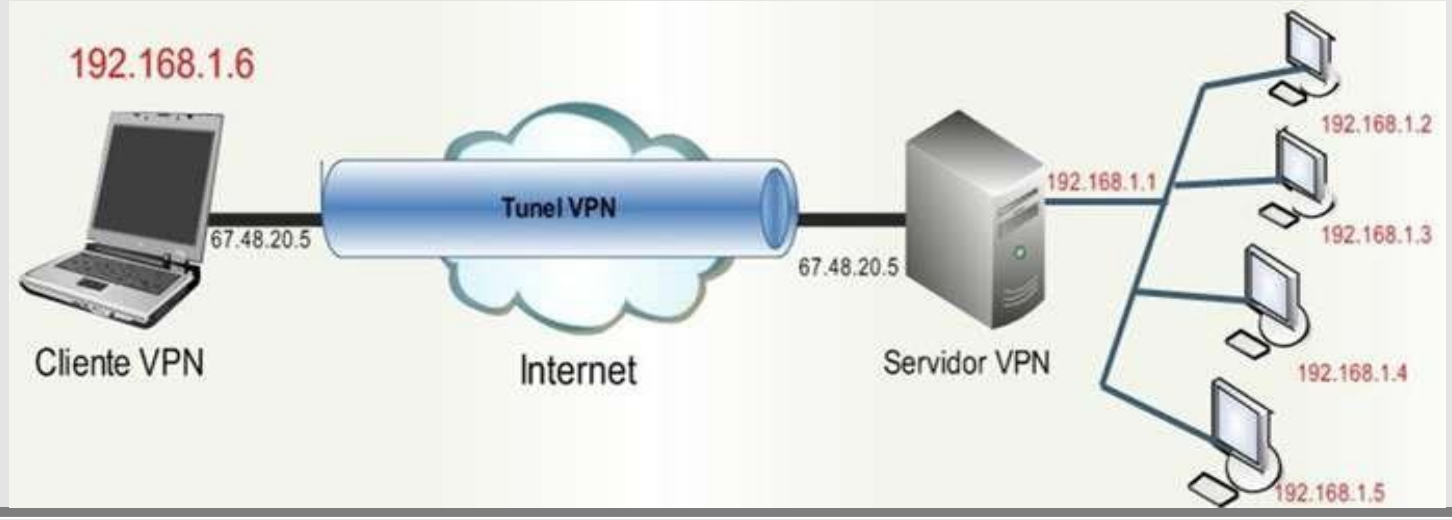
- PPTP, P2F, L2TP, IPSEC, SSL



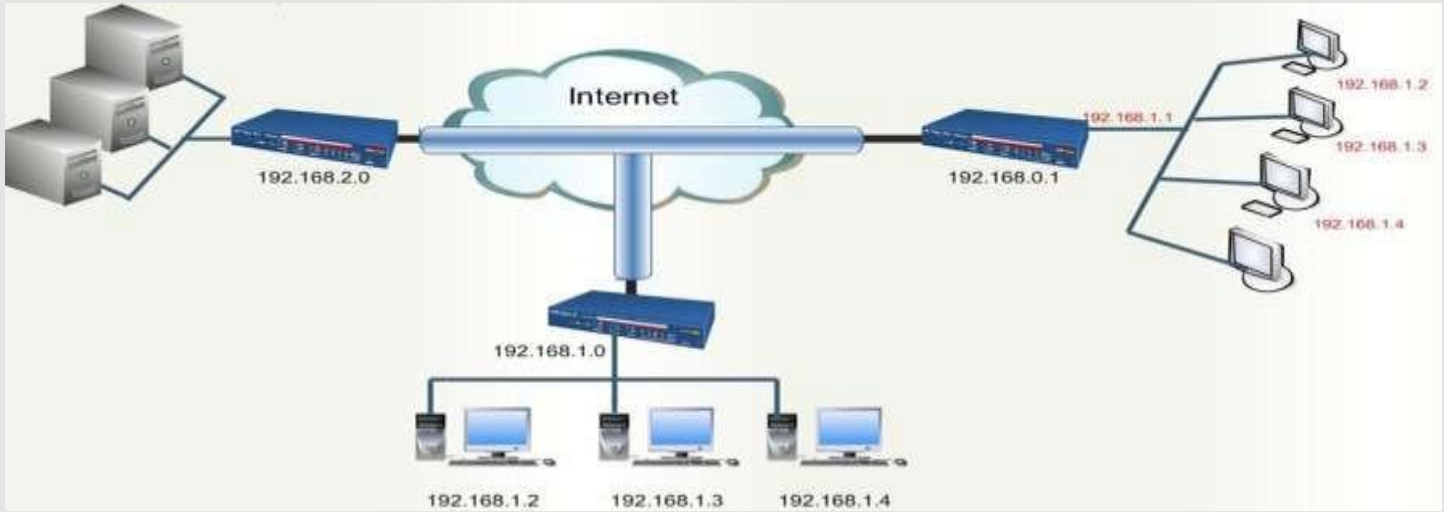
DEFINICIÓN:

- VPN ES UN CONCEPTO QUE PERMITE CONECTAR VARIAS LAN´s O ESTACIONES REMOTAS ENTRE SI
- IMPLEMENTA CONEXIONES DE FORMA SEGURA Y CONFIDENCIAL, A TRAVÉS DE UN MEDIO INSEGURO COMO INTERNET
- MEDIANTE EL USO DE AUTENTICACIÓN, ENCRIPTACIÓN Y TUNELES PARA LAS CONEXIONES

1) Conectar un Usuario Remoto a una LAN Corporativa



2) Conectar dos o más LAN´s Distintas

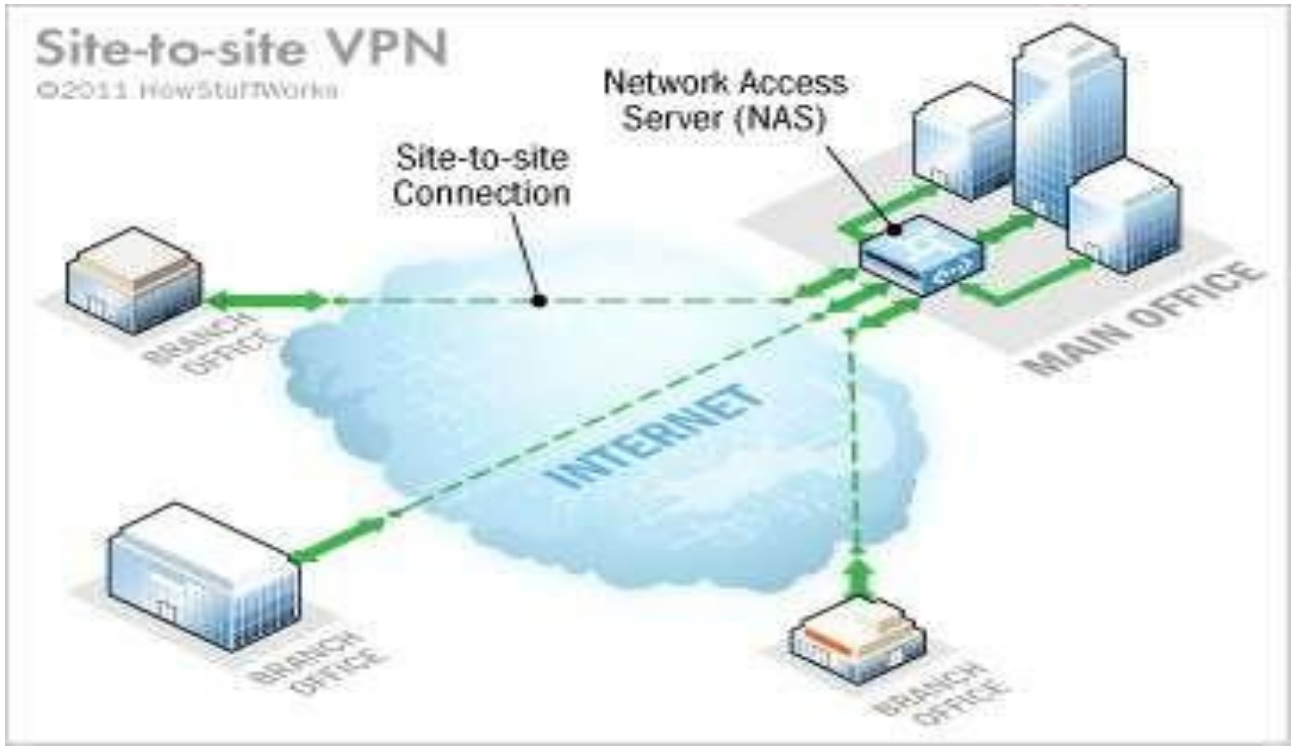


CONCEPTO VPN - ¿Qué puedo hacer con una VPN?

VPN DE ACCESO REMOTO:

- ❑ USUARIO O PROVEEDORES SE CONECTAN A UNA EMPRESA DESDE SITIOS REMOTOS UTUILIZANDO EL INTERNET COMO VÍNCULO DE ACCESO.
- ❑ REQUIEREN SER AUTENTICADOS Y TIENEN UN NIVEL DE ACCESO SIMILAR AL QUE TIENEN EN LA RED LOCAL.
- ❑ LAS EMPRESAS REEMPLAZAN CON ESTA TECNOLOGÍA SU INFRAESTRUCTURA DIAL-UP (MODEMS Y LÍNEAS TELEFÓNICAS)

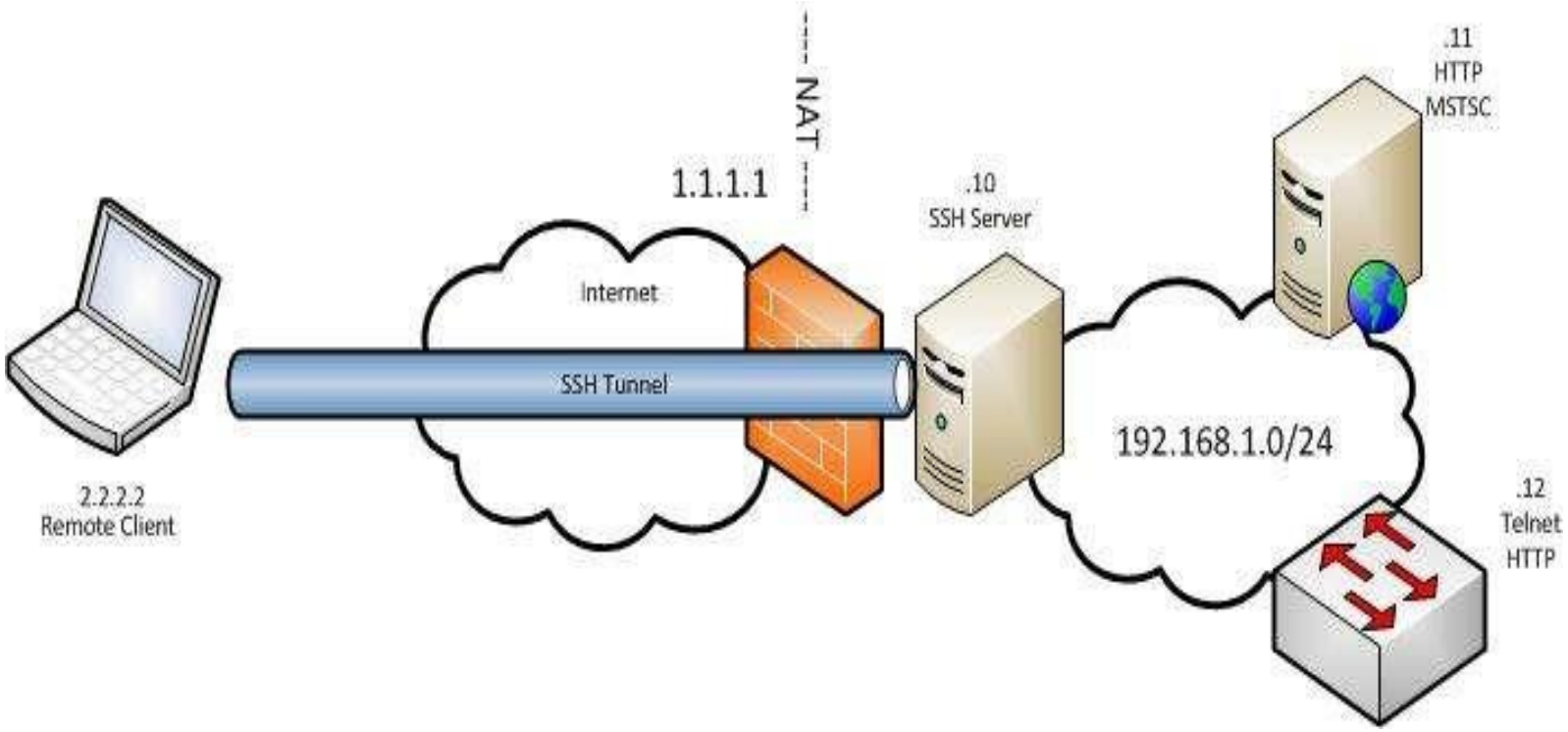
TIPOS DE VPN (ARQUITECTURA)– VPN Acceso Remoto



VPN PUNTO A PUNTO:

- ❑ OFICINAS REMOTAS SE CONECTAN A LA CENTRAL DE LA ORGANIZACIÓN.
- ❑ EL SERVIDOR VPN POSEE UN VINCULO PERMANENTE A INTERNET, ACEPTA LAS CONEXIONES PROVENIENTES DE LAS OFICINAS Y ESTABLECE EL TUNEL VPN.
- ❑ LAS OFICINAS SE CONECTAN A INTERNET CON EL ISP LOCAL.

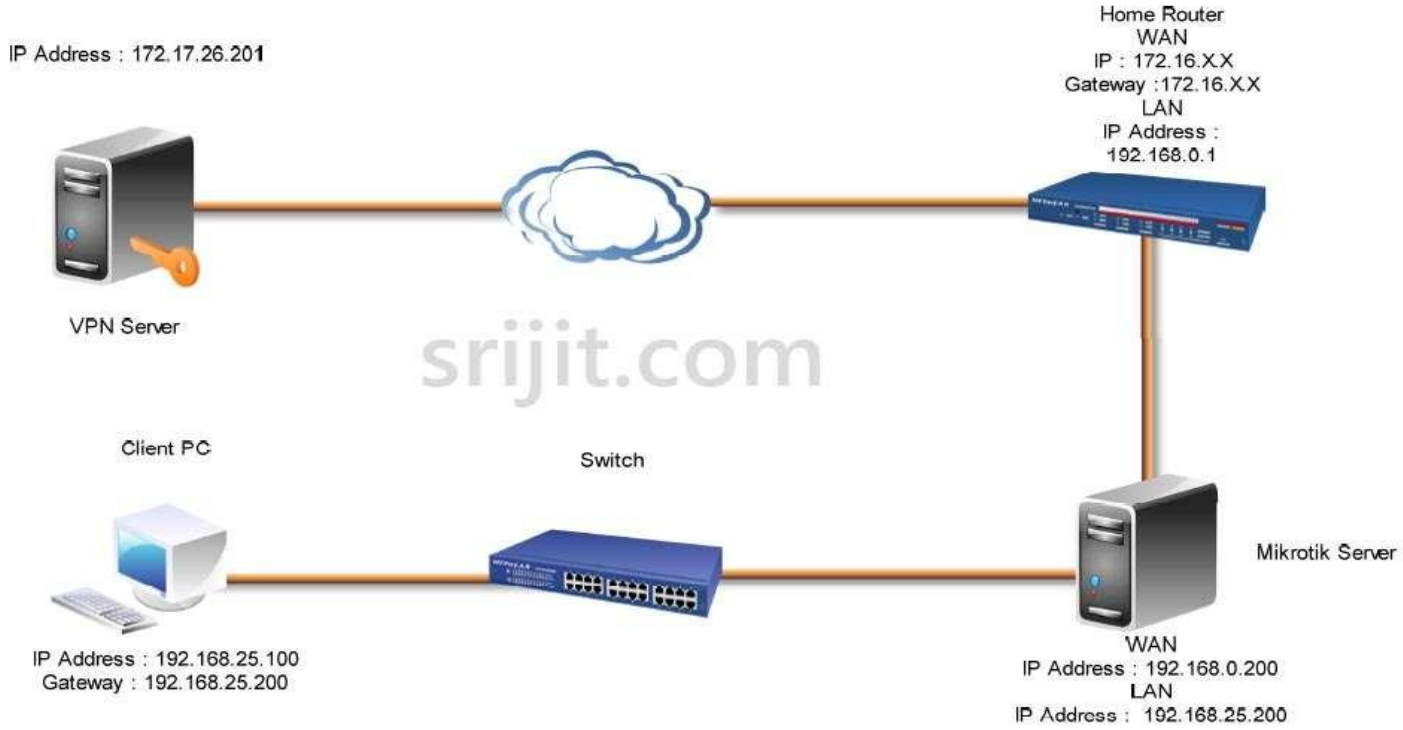
TIPOS DE VPN (ARQUITECTURA)– VPN Punto A Punto



VPN TUNNELING:

- CONSISTE EN ENCAPSULAR UN PROTOCOLO DE RED SOBRE OTRO CREANDO UN TUNEL DENTRO DE UNA RED DE COMPUTADORAS.
- EL TUNEL SE IMPLEMENTA INCLUYENDO UNA PDU DENTRO DE OTRA PDU CON EL OBJETO DE TRANSMITIRLA DE UN EXTREMO A OTRO DEL TUNEL REQUERIR INTERPRETACIÓN INTERMEDIA DE LA PDU ENCAPSULADA.
- UTILIZADO PARA REDIRECCIÓN DE TRÁFICO EN ESCENARIOS IP MOVIL.

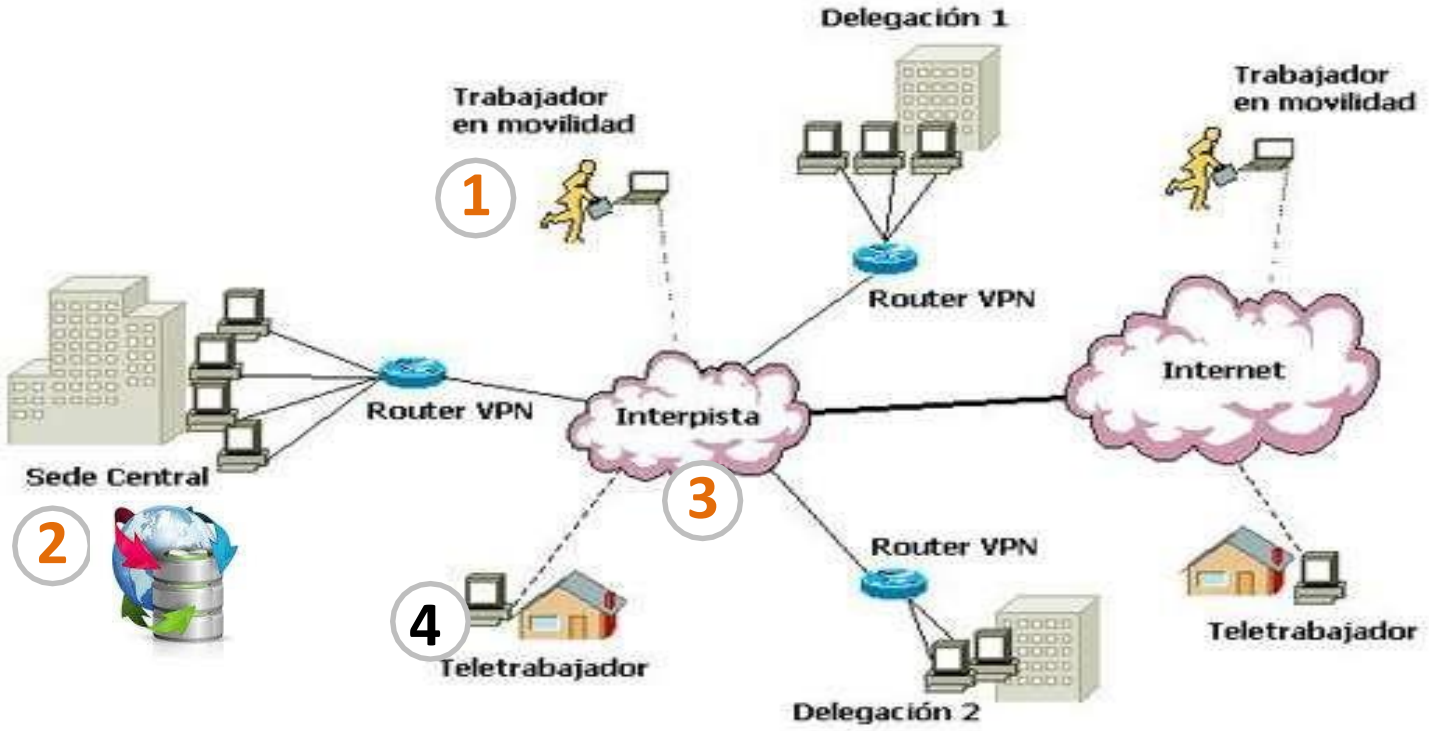
TIPOS DE VPN (ARQUITECTURA)– VPN Tunneling



VPN OVER LAN:

- ❑ MENOS DIFUNDIDO PERO MUY POTENTE.
- ❑ VARIANTE DEL ACCESO REMOTO, NO USA INTERNET SINO LA MISMA RED DE LA EMPRESA.
- ❑ PERMITE AISLAR ZONAS Y SERVICIOS DE LA RED INTERNA.
- ❑ MEJORA LA SEGURIDAD DE REDES INALAMBRICAS

TIPOS DE VPN (ARQUITECTURA)– VPN Over LAN

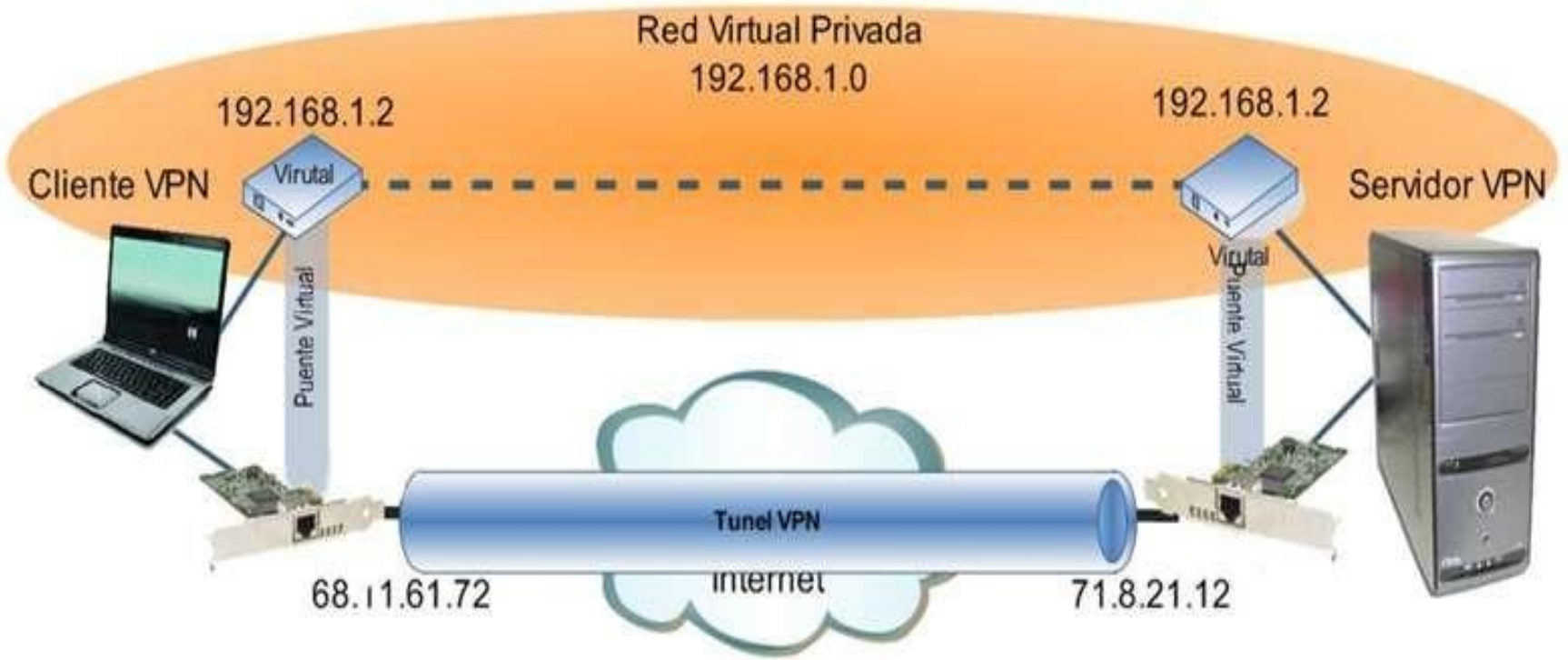


- ❑ PROPORCIONAR MOVILIDAD A LOS EMPLEADOS.
- ❑ ACCESO A LA BASE DE DATOS SIN UTILIZAR OPERADORES TELEFÓNICOS.
- ❑ INTERCAMBIO DE INFORMACIÓN EN TIEMPO REAL.
- ❑ TELETRABAJO
- ❑ CORREO ELECTRÓNICO CORPORATIVO.
- ❑ ESCONDE LOS DATOS DE NAVEGACIÓN
- ❑ BRINDAR SEGURIDAD MEDIANTE ENCRIPTACIÓN Y ENCAPSULACIÓN.

OBJETIVOS DE IMPLEMENTAR VPN

- TANTO EL CLIENTE COMO EL SERVIDOR CUENTAN, COMO MÍNIMO, CON LO SIGUIENTE:
  - ✓ UNA INTERFAZ DE RED FÍSICA PARA LA CONEXIÓN A INTERNET.
  - ✓ UNA INTERFAZ DE RED VIRTUAL PARA CONECTARSE A LA RED PRIVADA.
  - ✓ UN PUENTE VIRTUAL PARA CONECTAR AMBAS INTERFACES.

FUNCIONAMIENTO BÁSICO DE UN VPN



- PC REMOTA LLAMA A ISP LOCAL Y ESTABLECE UNA CONEXIÓN A INTERNET.
- SW CLIENTE VPN DE LA PC REMOTA RECONOCE UN DESTINO ESPECIFICADO Y NEGOCIA UNA SESION DE VPN.
- SERVIDOR VPN ACEPTA PETICIÓN DE CONEXIÓN, SE NEGOCIAN PARÁMETROS DE CONEXIÓN (ENCRIPTACIÓN, AUTENTICACIÓN) PIDE AL CLIENTE QUE SE VALIDE.
- CLIENTE VPN SE VALIDA ENVIANDO USUARIO Y CONTRASEÑA
- SERVIDOR VERIFICA USUARIO Y ENVÍA PARÁMETROS DE CONFIGURACIÓN DEL PROTOCOLO DE CAPA 3 ASIGNADOS POR MEDIO DE UN SERVIDOR DHCP
- SE ESTABLECE EL TUNEL DONDE TODO EL TRÁFICO ENTRE DOS PUNTOS ES ENCRIPTADO.

IP asignada: 192.168.1.2
Mascara de Subred: 255.255.255.0.
Puerta de Enlace: 192.168.1
Servidor DNS: 192.168.1.1

FUNCIONAMIENTO BÁSICO DE UN VPN

ZyXEL

ZyWALL USG 100

Con integración de tecnología VPN IPSec y SSL, es la solución ideal para aplicaciones VPN a través de redes distribuidas. Mayor conectividad de red con enlaces multi-ISP, tarjetas inalámbricas y 3G

- VPN híbrida (IPSec/SSL/L2TP)

ZyWALL OTP

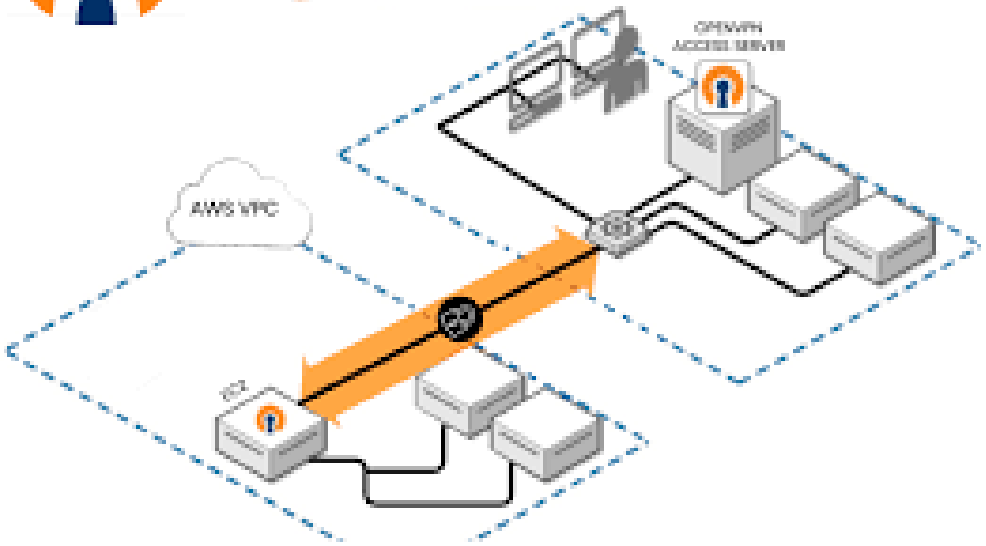
Generador de PINs

Un generador de PINs de 6 dígitos numéricos para ser utilizado junto con una contraseña en un proceso de autenticación robusto.

- ❑ UTILIZA EQUIPOS DEDICADOS QUE PUEDAN REALIZAR LA TAREA DE FORMA TRANSPARENTE.
- ❑ PROCESO DE ENCRIPTACIÓN SE REALIZA A NIVEL FÍSICO.
- ❑ GENERALMENTE SE UTILIZAN LOS ROUTERS CON VPN INCORPORADA QUE CUENTAN CON UN PROCESADOR Y ALGORITMOS DE ENCRIPTACIÓN.
- ❑ INSTALACIÓN SENCILLA, MANTENIMIENTO MÍNIMO, SISTEMA INDEPENDIENTE DE LAS MAQUINAS CONECTADAS A LA RED.
- ❑ FIRMWARE Y SISTEMAS DE ENCRIPTACIÓN CERRADO, SE DEPENDE DEL FABRICANTE.
- ❑ LA SEGURIDAD ESTA EN LOS EXTREMOS, SIENDO EL CAMINO INSEGURO DESDE EL ORDENADOR AL DISPOSITIVO VPN.

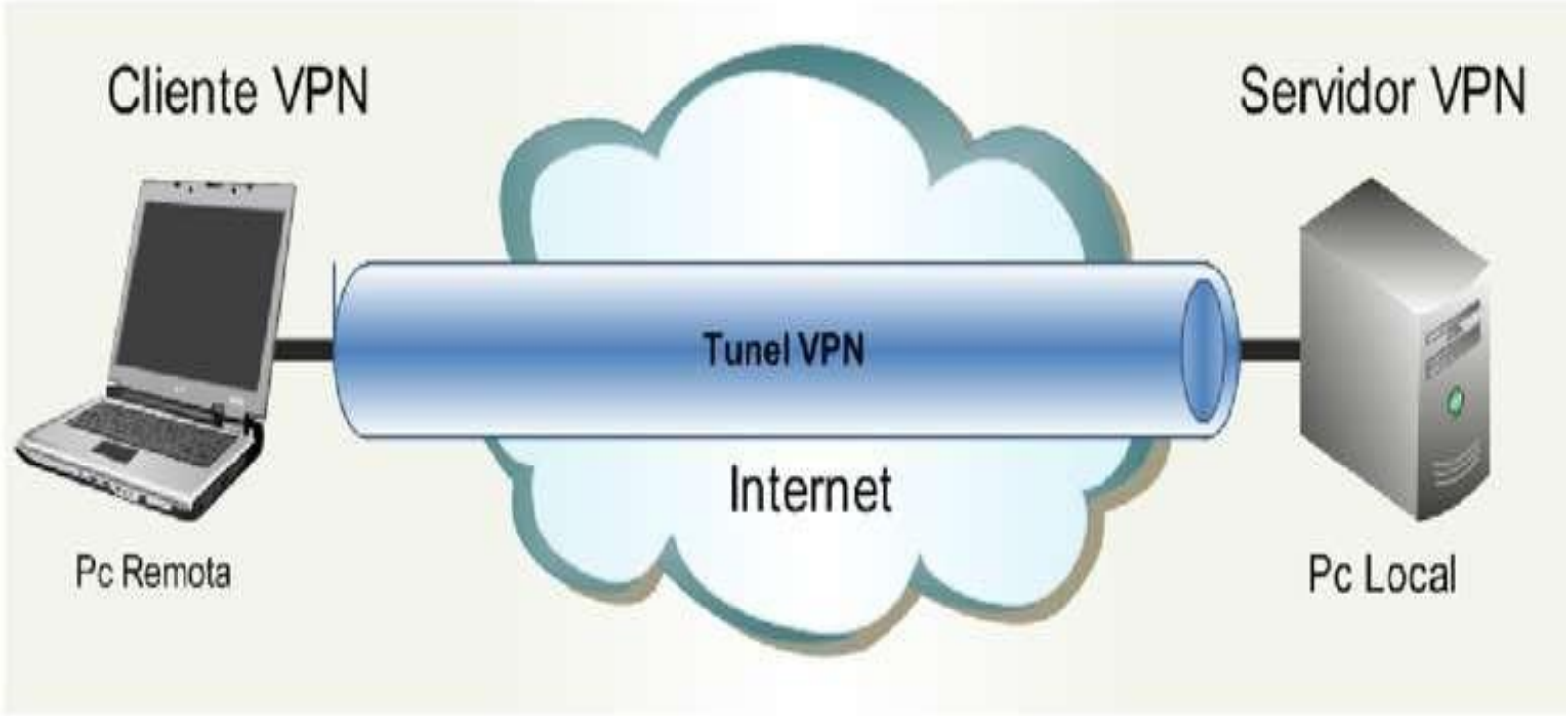
IMPLEMENTACIONES DE VPN – BASADA EN HARDWARE

OPENVPN



- VIENE SIENDO LA MAS UTILIZADA DADA LA NECESIDAD DE LOS MEDIANOS Y PEQUEÑOS USUARIOS DE IMPLEMENTAR SISTEMAS DE SEGURIDAD PARA EL ACCESO A SUS MÁQUINAS.
- ES MAS ECONÓMICO QUE LAS VPN BASADA EN HARDWARE.
- REQUIERE LA INSTALACIÓN DEL SW EN CADA MÁQUINA.
- EL SISTEMA DE CLAVES Y CERTIFICADOS ESTA EN MÁQUINAS POTENCIALMENTE INSEGURAS.
- PUEDEN DAR COBERTURA A REDES INTERNAS COMO EXTERNAS.
- LA SEGURIDAD SE PUEDE CUBRIR DE MAQUINA A MAQUINA.

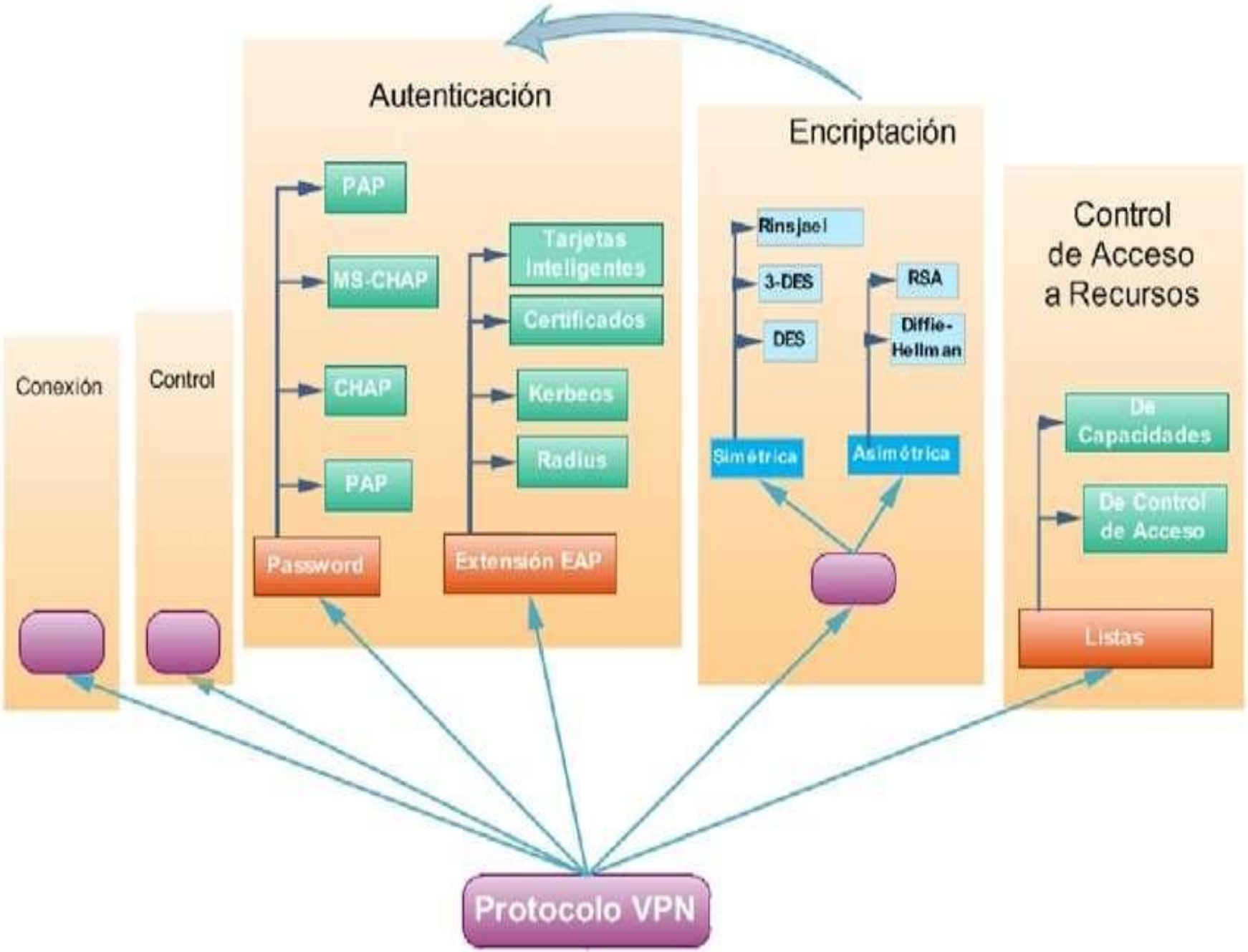
IMPLEMENTACIONES DE VPN – BASADA EN SOFTWARE



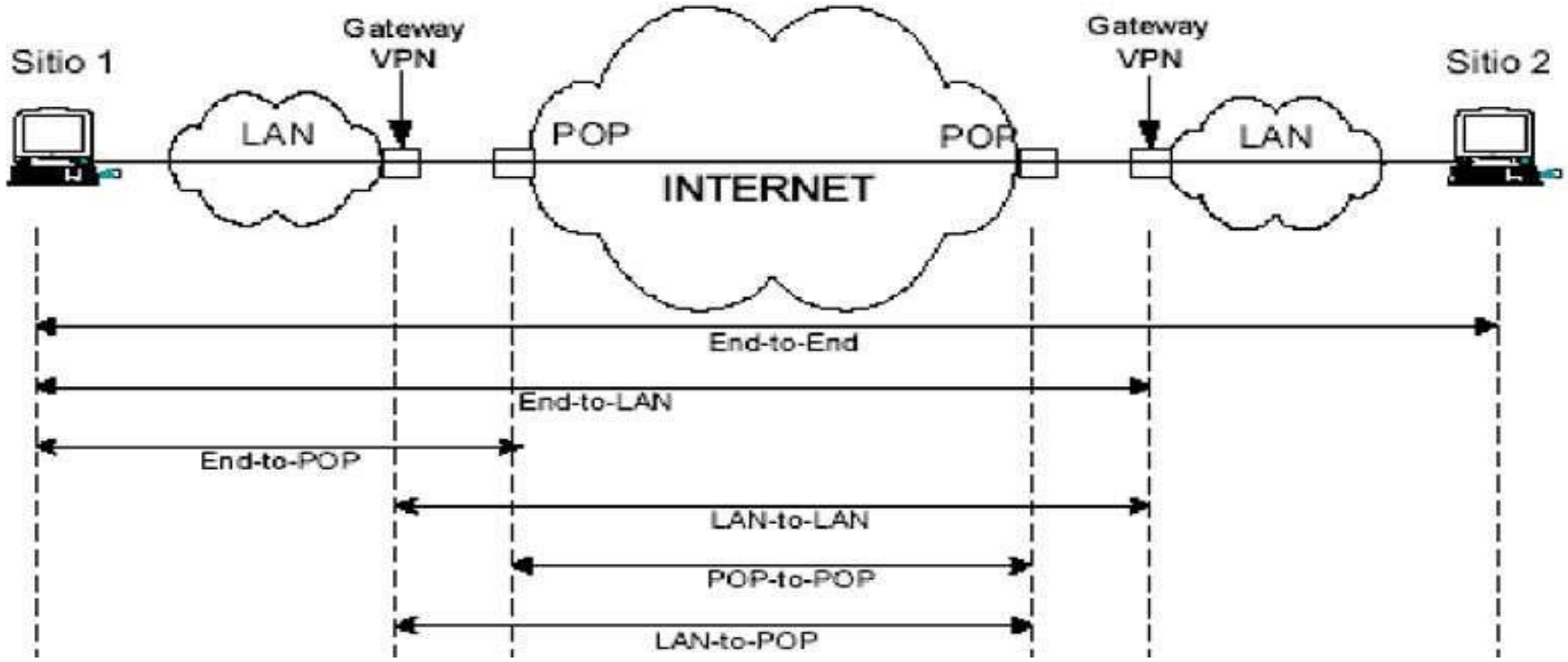
- FUE LA PRIMERA APLICACIÓN QUE SE LE DIO A LA TECNOLOGÍA VPN.
- NACIO DE LA NECESIDAD DE ACCEDER A LA RED CORPORATIVA DESDE CUALQUIER UBICACIÓN, INCLUSO A NIVEL MUNDIAL.
- CON EL ACCESO REMOTO VPN, LOS RAS CORPORATIVOS QUEDARON OLVIDADOS, PUES SU MANTENIMIENTO ERA COSTOSO Y LAS CONEXIONES REMOTAS ERAN COSTOSAS

ARQUITECTURA VPN – ACCESO REMOTO

ETAPAS NECESARIAS PARA UNA CONEXIÓN VPN



- CONEXIÓN: VPN DE ACCESO REMOTO / VPN DE ENRUTADOR A ENRUTADOR
- CONTROL DE CONEXIÓN: MANTIENE LA CONEXIÓN ESTABLE.
- AUTENTICACIÓN: EL USUARIO ENVIA PARAMETROS DE AUTENTICACIÓN DEFINIDOS Y EL SERVIDOR VERIFICA QUE LOS DATOS SEAN CORRECTOS (CLAVES, FIRMA DIGITAL).
- CIFRADO: OCULTA LA INFORMACIÓN MEDIANTE UN CONJUNTO DE REGLAS APLICADAS EN EL EMISOR Y EL RECEPTOR.
- CONTROL DE ACCESO: POLITICAS PARA EL ACCESO AUTORIZADO A DETERMINADOS RECURSOS.

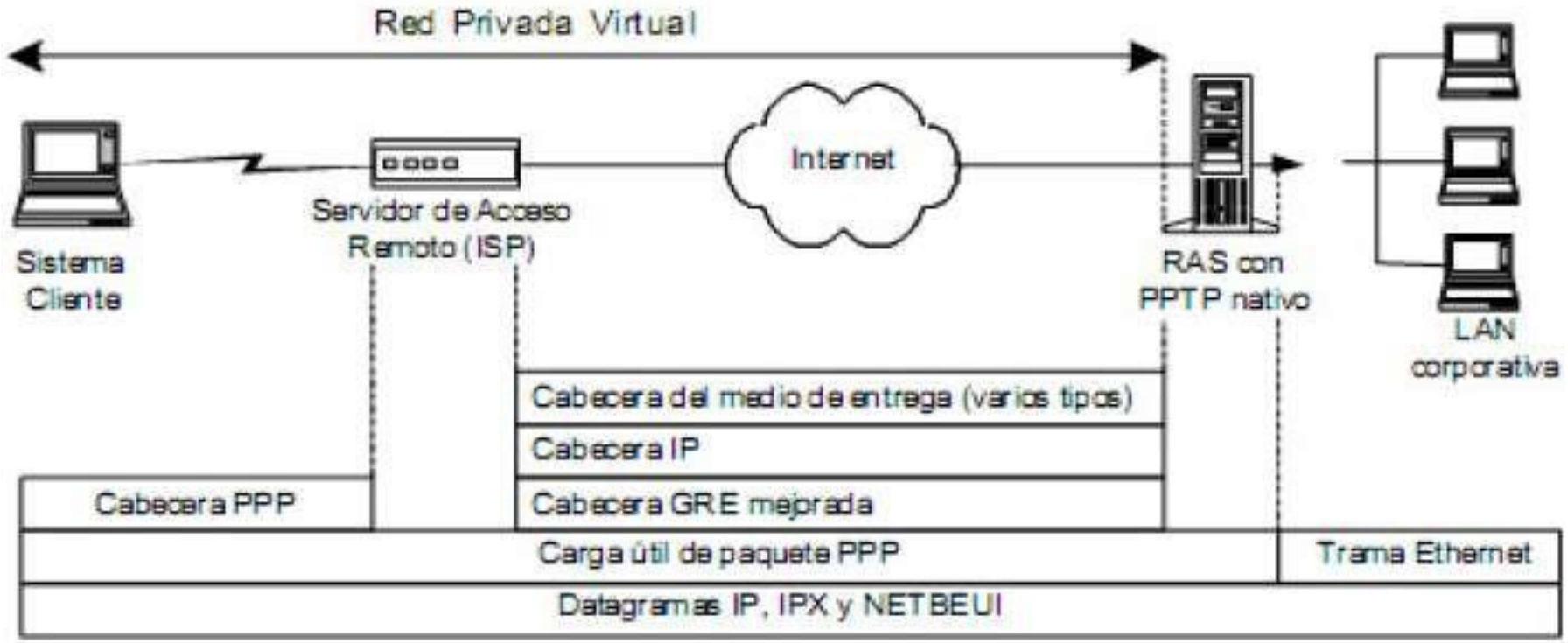


- TECNICA QUE USA UNA INFRAESTRUCTURA ENTRE REDES PARA TRANSFERIR DATOS DE UNA RED A OTRA.
- LOS DATOS PUEDEN SER TRANSFERIDOS COMO TRAMAS DE OTRO PROTOCOLO.
- EL PROTOCOLO ENCAPSULA LAS TRAMAS CON UNA CABECERA ADICIONAL , EN LUGAR DE ENVIARLA COMO LA PRODUJO EL NODO ORIGINAL.
- LA TECNOLOGÍA DE TUNEL SE PUEDE BASAR EN EL PROTOCOLO DEL TUNEL DE NIVEL 2, NIVEL 3, O NIVELES INTERMEDIOS (NIVELES DEL MODELO DE REFERENCIA DE INTERCONEXIÓN DE SISTEMAS ABIERTOS – OSI)

TUNELAMIENTO – MODELOS DE SEGURIDAD

- PPTP: PROTOCOLO DE TUNEL PUNTO A PUNTO
- L2TP: PROTOCOLO DE TUNEL DE CAPA 2.
- IPSEC: PROTOCOLO DE SEGURIDAD DE INTERNET.
- SSL: SECURE SOCKET LAYERS
- SSTP: SECURE SOCKET TUNNELING PROTOCOL

PROTOCOLOS VPN

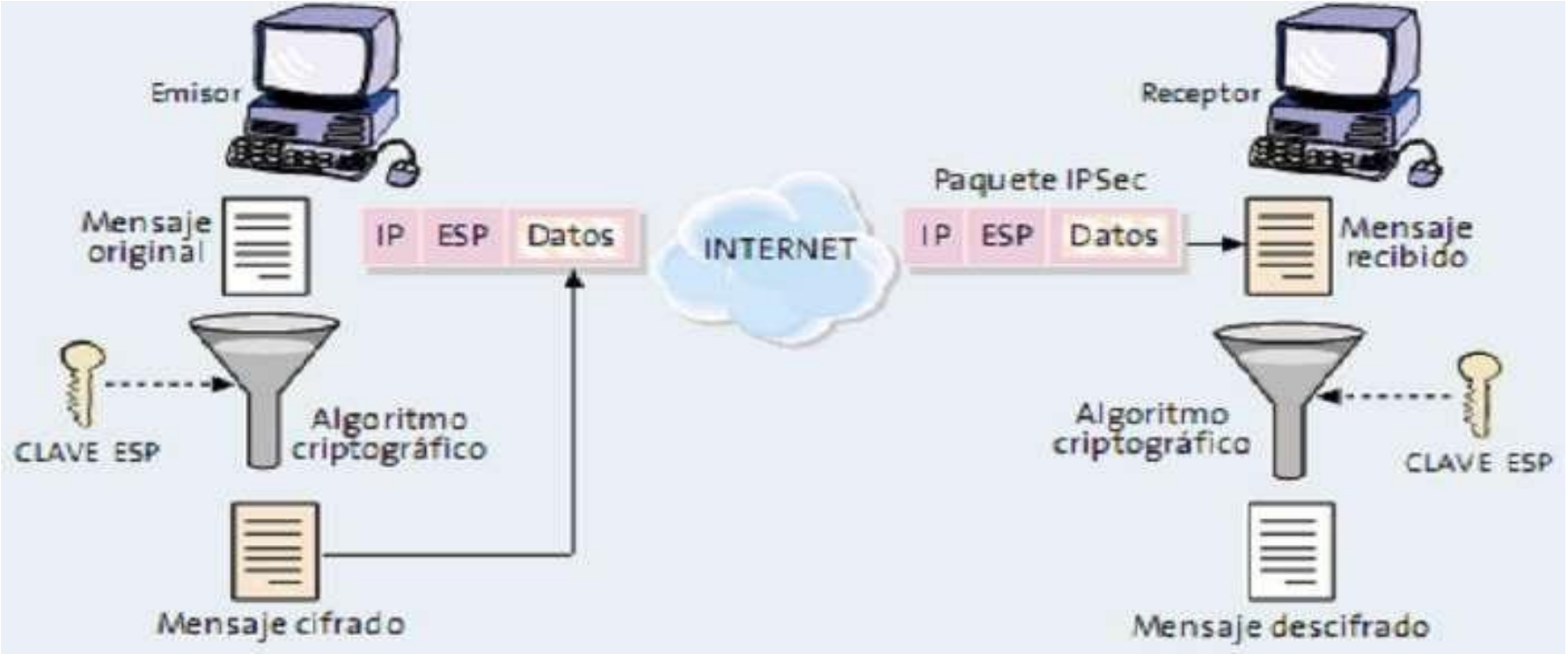


- USADO, EN GENERAL, POR PEQUEÑAS EMPRESAS PARA REALIZAR SUS VPN EN TOPOLOGÍAS LAN TO LAN Y ACCESO REMOTO, PARA TELETRABAJO.
- PPTP ENCAPSULA PAQUETES PPP.
- ES CAPAZ DE ENCAPSULAR PAQUETES IP, IPX y NETBEUI.
- PPTP ENCAPSULA PAQUETES PPP USANDO UNA VERSION MODIFICADA DEL PROTOCOLO DE ENCAPSULAMIENTO RUTEADO GENERICO - GRE

PROTOCOLOS DE TUNEL - PPTP

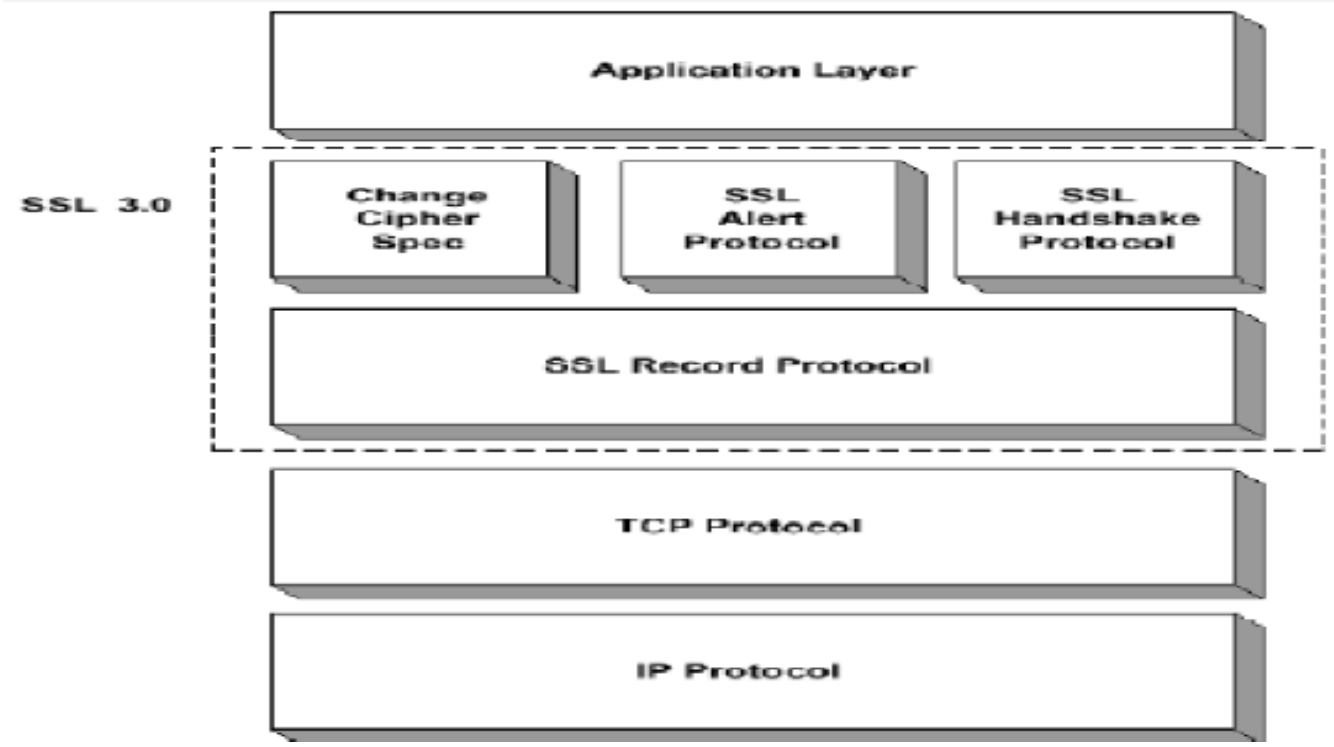
- CREADO COMO SUCESOR DE PPTP (MICROSOFT) Y L2F (CISCO), PROTOCOLO CAPA 2.
- SOPORTA MULTIPROTOCOLO.
- PERMITE QUE UN UNICO TUNEL SOPORTE MAS DE UNA CONEXIÓN
- L2TP NO CIFRA EL TRAFICO DE DATOS DEL USUARIO, LO CUAL DA PROBLEMAS PARA MANTENER LA CONFIDENCIALIDAD.

PROTOCOLOS DE TUNEL – L2TP



- IPSEC: CONJUNTO DE PROTOCOLOS DISEÑADOS PARA PROVEER UNA SEGURIDAD BASADA EN CRIPTOGRAFÍA ROBUSTA PARA IPV4 E IPV6.
- SERVICIOS DE SEGURIDAD INCLUYE: CONTROL DE ACCESO, INTEGRIDAD DE DATOS,AUTENTICACIÓN DEL ORIGEN DE DATOS, PROTECCIÓN ANTIREPETICIÓN Y CONFIDENCIALIDAD DE DATOS.
- PROTOCOLO MODULAR QUE NO DEPENDE DE UN ALGORITMO CRIPTOGRÁFICO.
- TRABAJA EN LA CAPA 3 DEL MODELO OSI, INDEPENDIENTE DEL NIVEL DE TRANSPORTE Y DE LA INFRAESTRUCTURA DE LA RED.

PROTOCOLOS DE TUNEL – IPSEC



- BASADO EN UN CIFRADO DE CLAVE PUBLICA QUE GARANTIZA LA SEGURIDAD DE LOS DATOS QUE SE ENVÍAN A TRAVÉS DE INTERNET.
- ESTABLECE UN CANAL SEGURO DE COMUNICACIÓN LUEGO DE UNA AUTENTICACIÓN.
- FUE RENOMBRADO A TLS – TRANSPORT LAYER SECURITY.
- ES INDEPENDIENTE DEL PROTOCOLO UTILIZADO , ASEGURA TRANSACCIONES EN LA WEB CON HTTP Y TAMBIEN CONEXIONES FTP, POP, IMAP.
- SE UBICA ENTRE LA CAPA DE APLICACIÓN Y LA CAPA DE TRANSPORTE
- EL CLIENTE NO NECESITA INSTALACIÓN.

PROTOCOLOS DE TUNEL – SSL