Acceso remoto y redes privadas virtuales

El acceso a la red local de una ubicación desde el exterior, para el teletrabajo o para la interconexión entre dos sitios, por ejemplo, requiere la instalación de soluciones específicas.

Estos accesos remotos utilizan la modalidad punto a punto entre dos terminales localizables por medio de una dirección (como una IP pública) o un número de teléfono.

1. Utilización y evolución

Estos servicios se pueden clasificar en dos categorías.

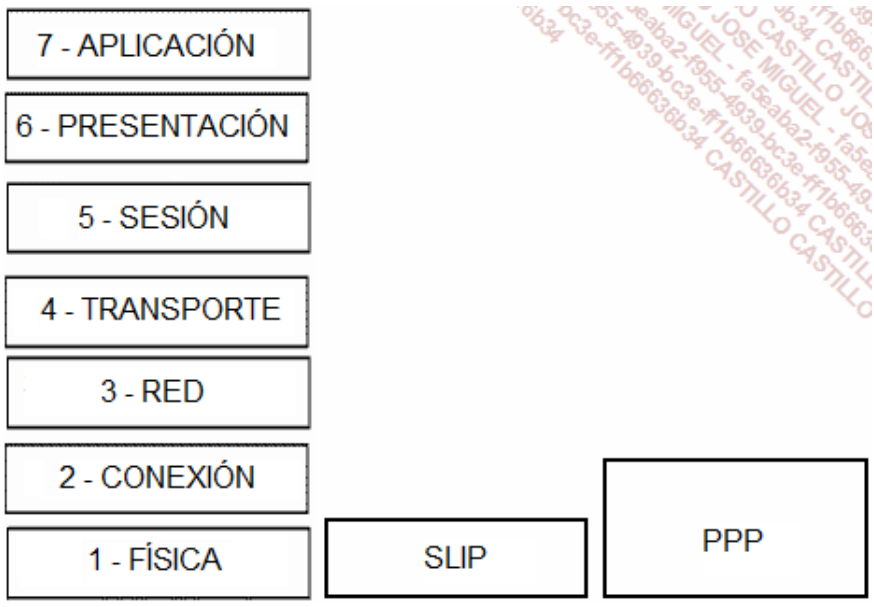
Si el acceso directo se realiza a través de un protocolo WAN, se habla de servicios de acceso remoto (RAS - *Remote Access Service*). A menudo se utiliza una solución por módem, con una facturación de la comunicación según tiempo y distancia.

Con la democratización de la conexión a Internet, las comunicaciones por acceso remoto con un módem analógico son poco comunes. Hoy en día lo normal es privatizar la comunicación en la red pública Internet. Para esto, se crea un túnel de aislamiento virtual y la comunicación cifrada se produce entre dos terminales, conectados a la red. Se habla de red privada virtual (RPV o VPN - *Virtual Private Network*).

La reducción de coste que implica la adopción de VPN ha generalizado su uso, tanto en la comunicación permanente entre lugares distantes como para accesos específicos de un puesto de trabajo en una empresa.

2. Protocolo de acceso remoto

El protocolo de nivel físico *Serial Line IP* (SLIP), que no era seguro, tiene su sucesor en el *Point to Point Protocol* (PPP) que cubre las dos capas bajas del modelo OSI.



Comparación de los modelos OSI, SLIP y PPP

PPP dispone de funcionalidades complementarias, como el control de errores y la seguridad. Soporta diferentes protocolos LAN de la capa de red.

3. Red privada virtual

Esta comunicación también es punto a punto entre un cliente y su servidor. El protocolo PPP se utiliza para el transporte.

a. Establecimiento de la conexión

Para poner en marcha la sesión VPN, en primer lugar se debe establecer una conexión a la red desde los dos extremos de la comunicación.

Tanto el cliente como el servidor deben soportar los diferentes protocolos que se utilizarán, a nivel de la comunicación, de la autentificación y del cifrado.

b. Autentificación

Cuando el cliente VPN pide acceso a su servidor, se exige, sobre todo, la autentificación del usuario.

La transferencia, la información de identificación y la contraseña se controlan de manera más o menos segura a través de una serie de protocolos estandarizados mediante PPP:

- *Password Authentication Protocol* (PAP) es poco recomendable, ya que la contraseña circula sin cifrarse.
- *Challenge Handshake Authentication Protocol* (CHAP) solo transmite una parte de la contraseña. Es un método más seguro que el anterior, pero aún es muy vulnerable en términos de seguridad.
- Microsoft CHAP versión 1 (MS-CHAPv1) y versión 2 (MS-CHAPv2) son versiones mejoradas de la anterior.

La verdadera confirmación de la seguridad llega con el mecanismo *Extensible Authentication Protocol* (EAP), que permite diferentes medios de autentificación, incluso el uso de un soporte físico o de la biometría.

c. El cifrado

Una vez que se supera la etapa de autentificación, se puede establecer el túnel de comunicación a distintos niveles del modelo OSI:

- Capa 2, con *Layer 2 Transport Protocol* (L2TP).
- Capa 3, con *Point To Point Tunneling Protocol* (PPTP) o *IP Security* (IPsec).
- Capas superiores con, por ejemplo, SSL/TLS.

Los dos protocolos PPTP y L2TP utilizan PPP para transportar los datos. L2TP reduce los encabezados, con una

compresión de 4 bytes en lugar de 6.

El protocolo *Microsoft Point to Point Encryption* (MPPE) proporciona el cifrado en PPTP, utilizando el algoritmo RC4. Se pueden utilizar contraseñas de 40, 56 o 128 bits. La autentificación, por ejemplo, se puede asegurar con MS-CHAPv1 o MS-CHAPv2. La solución PPTP/MPPE es la más antigua y tiende a utilizarse cada vez menos.

Si es necesaria la confidencialidad de la información transmitida por L2TP, el estándar de capa 3 IPsec garantiza la seguridad. Actualmente se recomienda la utilización de L2TP/IPsec para la realización de un túnel VPN en las capas 2 y 3.

Recientemente han aparecido nuevos tipos de red VPN. Considerando que todos los equipos de trabajo pueden interpretar las tramas SSL/TLS, por ejemplo gracias a los navegadores, la VPN-SSL favorece una solución sin despliegue ni instalación de cliente (*client less*). Además, el tráfico seguro por este método utiliza un puerto generalmente abierto en los cortafuegos, el TCP 443, correspondiente a HTTPS.

4. Clientes sencillos y acceso remoto

La banda ancha necesaria para las comunicaciones de acceso remoto o en una VPN se puede reducir por el uso de soluciones de tipo terminal, en las cuales el tráfico se reduce a:

- La transmisión de imágenes de pantalla en un sentido.
- La transmisión de las pulsaciones sobre el teclado y los movimientos del ratón.

Estas soluciones se utilizan también para redes locales, sobre las que aportan racionalización de los costes y facilidad de gestión.

Por ejemplo, un servidor Windows que incorpora la funcionalidad Servicios de escritorio remoto (RDS) puede unirse gracias al «Escritorio remoto», en lado del cliente, a través de una VPN o no. El protocolo de transmisión utilizado en las capas altas es *Remote Desktop Protocol* (RDP).

La empresa Citrix ofrece una solución similar con el servidor Xen App (p. ej., Presentation Server, el propio Metaframe). El protocolo que se utiliza es *Independent Computing Architecture* (ICA) y se debe instalar el cliente. El software de enlace *Citrix Secure Gateway* (CSG) se puede añadir en la empresa para una comunicación de terminal a través de una red privada virtual e Internet.

Existen también otras soluciones.