VPN (VIRTUAL PRIVATE NETWORK)

Las VPNs son redes virtuales que utilizan Internet para desplegarse, de tal forma que se puede crear una red entre dispositivos que se encuentran físicamente en redes diferentes. El funcionamiento de esa red es a efectos prácticos como el de una LAN.

En una red VPN el tráfico viaja cifrado, como en SSH. Sin embargo, no hay que confundir VPN con SSH. Por un lado, SSH es punto a punto y sirve para tomar el control de una única máquina. Por su parte, con VPN uno o varios equipos pueden trabajar como si fueran parte de una LAN en la que no están situados físicamente. Además, con VPN las IPs de origen reales, privadas, viajan en el PDU en todo momento, aunque ocultas. El potencial de las VPNs es enorme:

* Nos permiten conectar redes LAN remotas de manera exclusiva sin necesidad de tener un cable dedicado entre ellas, es decir, sin necesidad de una MacroLAN. Supongamos que tenemos una sede de nuestra empresa en Abando y otra en Zorrozaurre. Mediante VPN puedo conseguir que los trabajadores de la sede de Abando trabajen como si estuvieran en la de Zorrozaurre y/o viceversa. El ejemplo podría extenderse de tal manera que las sedes estuvieran mucho más alejadas: una en Nicaragua y otra en Grecia, por ejemplo.
* Nos permiten gestionar los privilegios y restricciones de la red virtual; por ejemplo, dar acceso específico a esa red virtual a una red (segmento) determinada de la empresa y a otras no. Esto se puede hacer mediante reglas de Firewall, por ejemplo. Supongamos que en una empresa hay 3 segmentos de red independientes: trabajadores, dirección y administración. Un empleado de la empresa podría conectarse a una red virtual (10.4.4.0/24, por ejemplo) desde su casa (IP de la tarjeta virtual del PC de su casa: 10.4.4.1, por ejemplo-). Puedo decirle al firewall que permita que las peticiones que lleguen desde la 10.4.4.1 puedan acceder sólo al segmento “trabajadores”. Así, ese empleado trabajaría desde casa como si estuviera en un equipo del segmento Trabajadores, pudiendo acceder a todos los recursos de red del segmento, pero no a los segmentos en los que no tiene privilegios. Es decir, se puede decir que prácticamente estaría trabajando como si estuviera en la oficina. De hecho, así es como la mayoría de las empresas de telecomunicaciones ha organizado la manera de trabajar de sus empleados durante la pandemia provocada por el COVID-19.

Así, en cuanto a su funcionalidad, podemos hablar de dos tipos de VPNs:

* VPNs site-to-site: también conocidas como Router-to-Router, las VPNs site-to-site pueden ser basadas en intranet o en extranet. Las primeras se crean dentro de las organizaciones, y suelen utilizarse en grandes compañías que quieren conectar las redes de sus oficinas de tal manera que estando en una de ellas se pueda trabajar como si se estuviera en otra; es decir, se despliegan aprovechando la intranet de la compañía. Las que son basadas en extranet funcionan de manera parecida, pero entre organizaciones diferentes, así que se despliegan en Internet.
* VPNs client-to-site: también conocidas como de acceso remoto. Permiten que un cliente con unas credenciales determinadas se conecte mediante VPN a una red y trabaje en ella como si estuviera in situ, aprovechando todos sus recursos. En el caso del teletrabajo motivado por el COVID-19, éste suele ser el modelo utilizado para llevarlo a cabo.

Entre otros, VPN puede usar el método IPSEC (Internet Protocol Security), que es un conjunto de protocolos criptográficos cuya función es asegurar las comunicaciones sobre IP; este método se compone de varios protocolos: AH, ESP e ISAKMP. Cada uno de esos protocolos utiliza algoritmos de cifrado como: DES, 3DES e IDEA. También se utilizan algoritmos de HASH: MD5, SHA...

IKE es uno de los medios para que dos extremos negocien cómo edificar las asociaciones IPSEC. Particularmente, ISAKMP lo hace en dos fases: en la primera, se crea el primer tíunel, que debe proteger los mensajes de negociación posteriores; en la fase 2, se crea el túnel que deberá proteger los datos.