OpenVPN

OpenVPN es una solución de conectividad basada en software libre: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas IEEE 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre.

**Implementación de VPN**

Supongamos que se tienen dos sitios de una organización conectados a Internet. En ambos se contará con un equipo de conexión a la red de redes que cumplirá la función de ruteo hacia y desde Internet así como firewall para protegerse de accesos no autorizados. El software VPN debe estar instalado en ese firewall o algún dispositivo protegido por él. Uno de los sitios será el “servidor” y será el sitio que contiene la información y sistemas que queremos compartir, mientras que al otro lo llamaremos “cliente”. El servidor será entonces configurado para aceptar conexiones desde el cliente (y viceversa). Llegado este punto habremos logrado tener dos sitios comunicados como en una red directa real pero aún no es una VPN dado que falta implementar la “privacidad”, pues cualquier nodo intermedio de Internet puede leer la información que viaja sin protección. Lo que se debe hacer seguidamente es establecer mecanismos de cifrado que mediante uso de claves aseguren que solo equipos o personas dueños de esas claves puedan acceder a los datos enviados por la VPN. Todos los datos enviados del punto A al B deberán ser cifrados antes de ser enviados y descifrados en el otro extremo para posteriormente ser entregados normalmente a su destinatario final. Uno de los factores que diferencian a una implementación de VPN de otra, son los mecanismos que utilicen para cifrar y distribuir claves a todos los integrantes de dicha red.

**Protocolos**

Las soluciones de VPN pueden ser implementadas a diferentes niveles del modelo OSI de red.

**Implementaciones de capa 2 - Enlace**

El encapsulamiento a este nivel ofrece ciertas ventajas ya que permite transferencias sobre protocolos no-IP, como por ejemplo IPX4 de Netware Systems. Teóricamente, las tecnologías implementadas en capa 2 pueden tunelizar cualquier tipo de paquetes y en la mayoría de los casos lo que se hace es establecer un dispositivo virtual PPP5 con el cual se establece la conexión con el otro lado del túnel.

**Implementaciones de capa 3 - Red**

IPsec es la tecnología más aceptada en este punto y fue desarrollada como un estándar de seguridad de Internet en capa 3. IPsec se pude utilizar para encapsular cualquier tráfico de capa 3 pero no el tráfico de capas inferiores, por lo que no se podrá utilizar para protocolos no-IP como IPX o mensajes de broadcast. Su principal ventaja es que puede ser usado prácticamente en cualquier plataforma existiendo una gran variedad de soluciones tanto de software como de hardware.

**Implementaciones de capa 7 – Aplicación**

También es posible establecer túneles en la capa de aplicación y de hecho son ampliamente utilizados hoy en día siendo algunas aproximaciones soluciones como SSL6 y TLS7. El usuario accede a la VPN de la organización a través de un browser iniciando la conexión en un sitio web seguro (HTTPS-Secured website).

Además, existen otros productos como SSL-Explorer y otros que ofrecen una combinación de gran flexibilidad, seguridad fuerte y facilidad de configuración. La seguridad es lograda mediante cifrado del tráfico usando mecanismos SSL/TLS, los cuales han probado ser muy seguros y están siendo constantemente sometidos a mejoras y pruebas.

**Usos de las VPN**

**Las VPN se usan generalmente para:**

* Conexión entre diversos puntos de una organización a través de Internet.
* Conexiones de trabajadores domésticos o de campo con IP dinámicas.
* Soluciones extranet para clientes u organizaciones asociadas con los cuales se necesita intercambiar cierta información en forma privada pero no se les debe dar acceso al resto de la red interna.
* Además, brinda una excelente fiabilidad en la comunicación de usuarios móviles así como también al unir dos puntos distantes como agencias de una empresa dentro de una sola red unificada.

**Ventajas y Desventajas de OpenVPN**

Ventajas OpenVPN provee seguridad, estabilidad y comprobados mecanismos de cifrado sin sufrir la complejidad de otras soluciones VPN como las de Ipsec.

**Ventajas**

* Posibilidad de implementar dos modos básicos, en capa 2 o capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).
* Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización protegerá el laptop remoto aún cuando no es un equipo de la red local. Por otra parte, sólo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.
* Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.
* Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como cliente (iniciando conexiones).
* Sólo un puerto en el firewall debe ser abierto para permitir conexiones, dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.
* Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.
* Todos los conceptos de reglas, restricciones, reenvío y NAT10 pueden ser usados en túneles OpenVPN.
* Alta flexibilidad y posibilidades de extensión mediante scripting. OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.
* Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.
* Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.
* Instalación sencilla en cualquier plataforma. Tanto la instalación como su uso son muy simples.
* Diseño modular. Se basa en un excelente diseño modular con un alto grado de simplicidad tanto en seguridad como red.

**Desventajas**

* No tiene compatibilidad con IPsec que es el actual estándar para soluciones VPN.
* Carencia de masa crítica [cita requerida].
* Todavía son relativamente pocos los que saben cómo usar OpenVPN [cita requerida].
* A día de hoy mayormente se puede conectar a otras computadoras o dispositivos con IOS y Android [cita requerida]. Sin embargo, esto está cambiando, dado que existen compañías desarrollando dispositivos con clientes OpenVPN integrados y haciendo llegar esta tecnología a otros ámbitos como la automatización industrial (ver ejemplo en Panasonic).