

# ASIR

## Virtual Private Network

**OPENVPN™**



**FreeRADIUS**  
The world's most popular RADIUS Server

**OpenLDAP™**

# Introducción: Descripción del problema

---

La red de ASIR se trata de una red local que ofrece unos servicios determinados a los distintos usuarios, alumnos y profesores.

Al tratarse de una red local, los usuarios han de estar físicamente en el centro para poder hacer uso de estos servicios, como por ejemplo consultar la web donde se cuelgan los temarios y ejercicios.

Supongamos que por cualquier razón se hace necesario poder consultar dicha web sin estar físicamente en el centro, es decir, desde otra red como por ejemplo la de casa. En este caso la solución posible es pasar a través de internet.

Esto nos lleva a otro punto a tener en cuenta, la seguridad. Al tener que hacer uso de internet para conectar ambas redes, no tendremos el control sobre el tráfico una vez que los datos salgan al exterior desde un extremo y antes de que lleguen al otro extremo.

Por suerte existe una solución para tal situación, **crear una VPN**. Esto nos permitirá conectar dos o más puntos de manera segura.

Además, también será necesario controlar el acceso de usuarios, es decir, quienes se van a poder conectar a la VPN y quien no. Para esto vamos a necesitar hacer uso de algún protocolo de tipo AAA (Autenticación, Autorización y Auditoría) como puede ser RADIUS.

# Introducción: ¿Qué es una VPN?

---

Una VPN (Virtual Private Network), es una red privada que usa una red pública (normalmente Internet) para conectar dos o más puntos de manera segura.

Las conexiones VPN permiten a los usuarios acceder, desde casa o desde un punto remoto, al servidor de su organización a través de la infraestructura de encaminamiento que proveen las redes públicas.

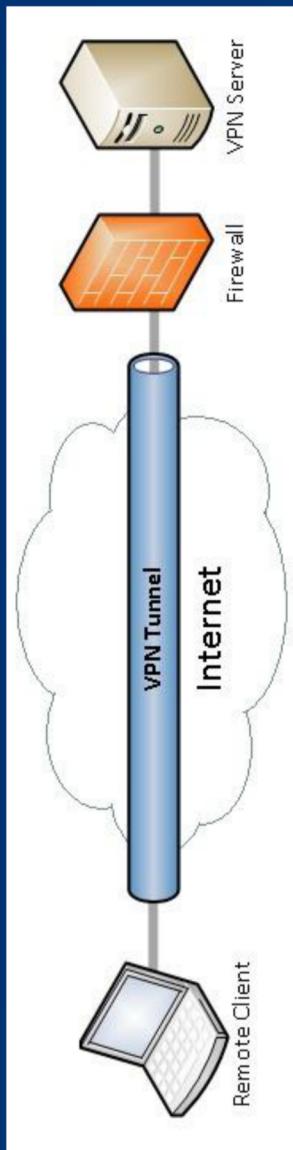
La privacidad se consigue mediante dos mecanismos:

- **La autenticación**, que asegura que sólo los usuarios autorizados accedan a un determinado servicio.
  - **El cifrado de datos**, que codifica la información enviada de modo que sólo el/los usuario(s) destino puedan descifrarla y por tanto comprenderla.
- A éstos dos hay que sumar otro aspecto fundamental en la construcción de una VPN:
- **La integridad de los datos**, garantía de que la información no pueda ser modificada en su camino hasta el receptor.

## Introducción: ¿Cómo funciona una VPN?

---

Una red privada virtual se basa en un protocolo denominado **protocolo de túnel**, es decir, un protocolo encargado de encapsular los paquetes cifrados que se transmiten desde un lado de la VPN hacia el otro.

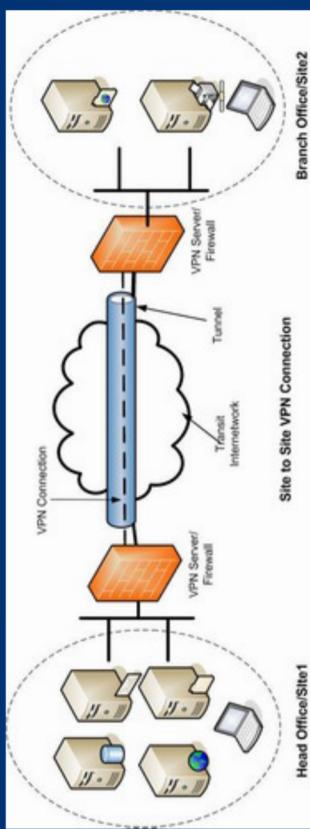


La palabra "túnel" se usa para simbolizar el hecho que los datos están cifrados desde el momento que entran a la VPN hasta que salen de ella, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN.

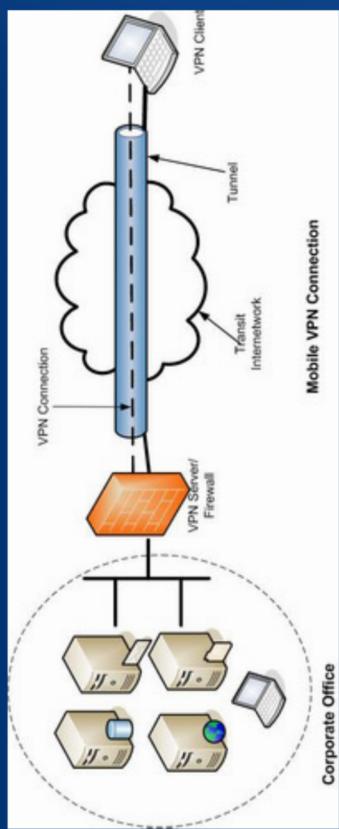
Esto quiere decir que además de protocolos de tunelizado, una VPN implementa mecanismos de seguridad para el cifrado de datos como puede ser por ejemplo **TLS/SSL**.

# Introducción: Topologías de una VPN

**VPN Punto a Punto:** Este tipo de VPN consiste en proporcionar un “túnel” para la conexión de puntos remotos entre sí. Permite interconectar dos redes LAN geográficamente distantes a través de Internet de manera segura. Este tipo de configuración es ideal para interconectar sucursales de una compañía separadas geográficamente.



**VPN de Acceso Remoto:** Es quizás el modelo más usado actualmente y consiste en varios usuarios que se conectan a un servidor remoto utilizando Internet como vínculo de acceso. El cliente se autentica al servidor de acceso remoto, y el servidor se autentica ante el cliente. Una vez autenticados, los clientes tienen un nivel de acceso muy similar al que tendrían si estuvieran conectados a la propia red local donde se encuentra el servidor VPN.



# **Introducción: Ventajas y desventajas de una VPN**

---

## **Ventajas**

- Posibilidad de conectar redes físicamente separadas sin necesidad de usar una red dedicada, si no a través de Internet.
- Acceso a los recursos de la red a la cual se conecta el cliente de forma remota.
- La integridad, confidencialidad y seguridad de los datos. Los datos viajan seguros de un extremo a otro de la VPN.

## **Desventajas**

- La velocidad de acceso es generalmente menor a la de una conexión tradicional.
- Es necesario ciertos conocimientos para implementar una conexión VPN.
- Una brecha de seguridad del equipo cliente puede poner en riesgo los recursos de la red a la que se conecta.

# Introducción: RADIUS

---

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autenticación, autorización y auditoría (AAA) para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

La autenticación gestionada por este protocolo se realiza a través del ingreso de un nombre de usuario y una clave de acceso. Esta información es procesada por un dispositivo NAS (Network Access Server) siendo posteriormente validada por un servidor RADIUS a través del protocolo correspondiente valiéndose de diversos mecanismos de autenticación y permitiendo el acceso al sistema.

# Introducción: LDAP

---

LDAP son las siglas de Lightweight Directory Access Protocol (en español Protocolo Ligero/Simplificado de Acceso a Directorios) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

Está basado en el estándar X.500 para compartir directorios, pero es menos complejo. Como X.500, LDAP organiza la información en un modo jerárquico usando directorios. Estos directorios pueden almacenar una gran variedad de información.

La mayor ventaja de LDAP es que se puede consolidar información para toda una organización dentro de un repositorio central. Por ejemplo, en vez de administrar listas de usuarios para cada grupo dentro de una organización, puede usar LDAP como directorio central, accesible desde cualquier parte de la red.

Puesto que LDAP soporta la capa de conexión segura (SSL) y la seguridad de la capa de transporte (TLS), los datos confidenciales se pueden proteger de los curiosos.

# **ASIR VPN: Funciones y requisitos**

---

Los servicios que ofrecerá el sistema una vez implantado serán los siguientes:

1. Será posible acceder a la red de ASIR desde una red externa y hacer uso de sus servicios.
2. La conexión entre ambas redes se realizará a través de una VPN.
3. La conexión VPN se realizará de forma segura mediante cifrado, durante toda la sesión de trabajo entre el equipo cliente del usuario remoto y el servidor VPN implantado en la red de ASIR.
4. Los usuarios que podrán conectarse deberán existir en un servicio de directorio LDAP y además pertenecer a un grupo específico en LDAP, al que se le permitirá el acceso a la VPN.
5. Se hará uso de una autenticación de doble factor para realizar la conexión con la VPN:
  - a. Algo que el usuario posee: certificado digital y clave privada.
  - b. Algo que el usuario sabe: usuario/contraseña.
6. Un servidor VPN se encargará de validar los certificados.
7. Un servidor RADIUS será el encargado de la validación de las credenciales usuario/contraseña.

# ASIR VPN: Soluciones para servidor VPN

Como tecnologías VPN disponibles gratuitamente y más utilizadas en la actualidad, podemos elegir entre **PPTP, L2TP/IPsec y OpenVPN.**

PPTP	L2TP / IPsec	OpenVPN	OpenVPN / OpenSSL	OpenVPN / MPPE	OpenSSL / TLS/SSL	Native
Protocolo VPN propietario de Microsoft, muy básico basado en PPP.	Avanzado protocolo estandarizado formalmente y recomendado para reemplazar PPTP en plataformas donde se requieran cifrado seguro de datos.	Avanzada solución VPN de código abierto y que es ahora el estándar de facto en el campo de redes de código abierto.	OpenVPN / OpenSSL	<ul style="list-style-type: none"><li>- Se considera altamente seguro cuando utiliza el algoritmo de cifrado AES de 256 bits.</li><li>- Encapsula los datos dos veces.</li><li>- Si comprueba la integridad de los datos</li></ul>	<ul style="list-style-type: none"><li>- Se considera altamente seguro cuando utiliza el algoritmo de cifrado AES de 256 bits.</li><li>- Uso de certificados digitales con TLS/SSL.</li><li>- Si comprueba la integridad de los datos.</li></ul>	Compatible con una amplia gama de equipos de escritorio, dispositivos móviles y tabletas.
				<p>Tiene una sobrecarga ligeramente mayor a sus rivales debido al doble encapsulamiento que realiza.</p> <p>Es el que mayor velocidad tiene debido a la menor seguridad</p>		Ofrece un alto rendimiento. Es extremadamente rápido y fiable incluso en conexiones de alta latencia y grandes distancias.
						Nativo en una amplia gama de equipos de escritorio, dispositivos móviles y tabletas.

# ASIR VPN: Elección de solución VPN

---

OpenVPN es la mejor opción para todas las plataformas.

- Es extremadamente seguro, rápido,iable y altamente configurable.
- Utiliza tecnologías de código abierto como la biblioteca de cifrado OpenSSL.
- Puede ser configurado para usar cualquier puerto, lo que hace que sea difícil de bloquear por los cortafuegos.
- Es compatible con NAT, es decir, ambos extremos pueden ser redes NATeadas sin problemas.



Descartando PPTP completamente por su débil seguridad, entre L2TP/IPsec y OpenVPN, nos quedamos con OpenVPN ya que L2TP/IPsec es más lento debido a su doble encapsulamiento y además puede ser bloqueado con más facilidad debido a la dependencia de uso de puertos y protocolos fijos.

El único “inconveniente” de OpenVPN es la necesidad de instalar el software para el cliente, pero en la mayoría de las plataformas esto solo toma unos minutos.

# ASIR VPN: Solución para servidor RADIUS

---

La opción elegida para implantar un servidor RADIUS es **FreeRADIUS**:

- Se trata de uno de los servidores RADIUS más populares y de libre distribución.
  - Es simple y bastante flexible ya que puede interactuar con distintos almacenes de datos y ofrece soporte para diversos mecanismos de autenticación.
  - Cuenta con una gran comunidad que lo sustenta. Desde sus inicios, el proyecto ha crecido hasta incluir soporte para más tipos de autenticación que cualquier otro servidor de código abierto.
- Es decir, FreeRADIUS permite entre otras cosas, distintas formas de autenticación y entre ellas está **realizar la autenticación contra un servidor LDAP**. Además en un futuro lo podremos usar, aparte de para la VPN, para controlar el acceso Wifi en el centro mediante EAP-TLS.



The world's most popular RADIUS Server

# ASIR VPN: Solución para servidor LDAP

---

La opción elegida es **OpenLDAP**. Se trata de una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) que está respaldada por una gran comunidad.

OpenLDAP incluye un número de características importantes entre las que destacan:

- Soporte LDAPv3 — OpenLDAP soporta la Capa de autenticación y seguridad (SASL), la Seguridad de la capa de transporte (TLS) y la Capa de conexión segura (SSL), entre otras mejoras. Muchos de los cambios en el protocolo desde LDAPv2 han sido diseñados para hacer LDAP más seguro.
- Soporte IPv6 — OpenLDAP soporta la próxima generación del protocolo de Internet versión 6.



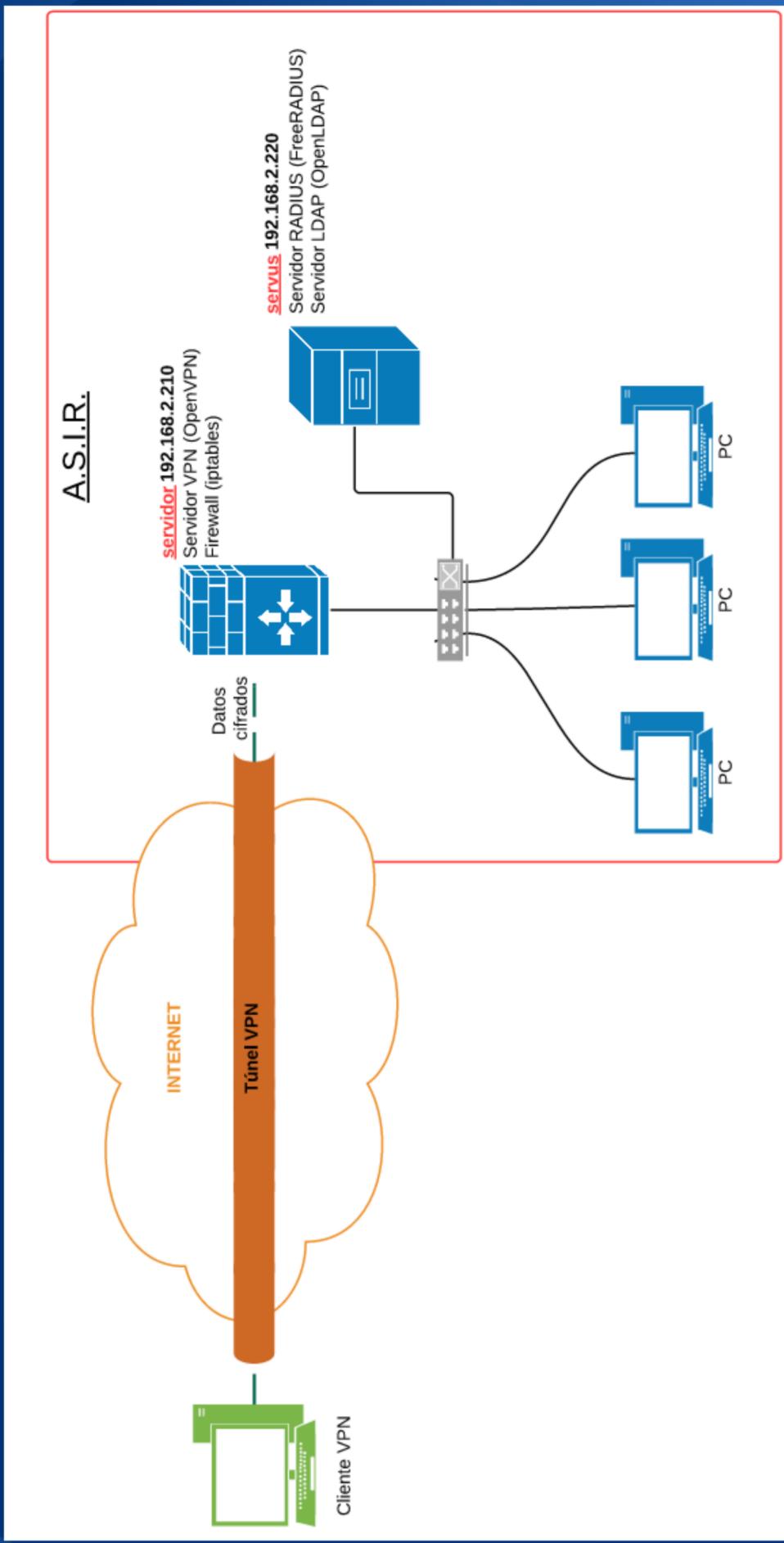
# **ASIR VPN: Modelado de la infraestructura**

---

La infraestructura que se va a implantar para dotar de una VPN a la red de ASIR depende principalmente de las siguientes soluciones:

- **OpenVPN**: encargado de crear una VPN y además, será el encargado de validar mediante TLS/SSL el primer factor necesario para la autenticación: certificados y claves privadas.
- **FreeRADIUS**: encargado de validar el segundo factor de la autenticación para poder permitir el acceso de usuarios a la VPN: usuario/contraseña contra LDAP.
- **OpenLDAP**: encargado de almacenar y gestionar una base de datos centralizada que guardará, entre otras, cosas las credenciales de los usuarios que deberán ser validadas y podrán conectarse a la VPN.

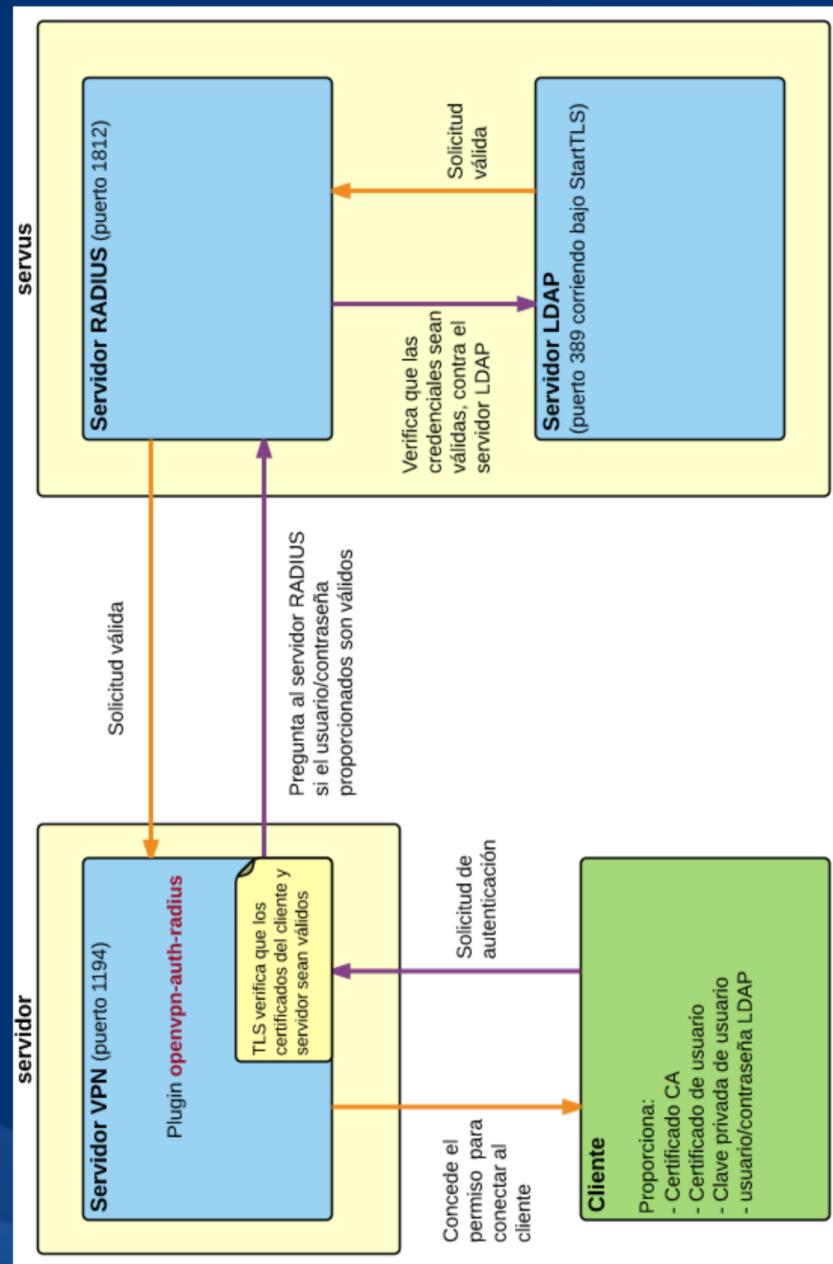
# ASIR VPN: Esquema de la infraestructura



# **ASIR VPN: Paquetes necesarios**

<u>Servus</u>	<u>Servidor</u>	<u>Cliente</u>
	<ul style="list-style-type: none"><li>• OpenLDAP:<ul style="list-style-type: none"><li>○ slapd</li><li>○ ldap-utils</li><li>○ libnss-ldap</li><li>○ libpam-ldap</li><li>○ gnutls-bin</li></ul></li><li>• OpenVPN:<ul style="list-style-type: none"><li>○ openvpn</li><li>○ openvpn-auth-radius</li><li>○ easy-rsa</li><li>○ freeradius-utils</li></ul></li><li>• FreeRADIUS:<ul style="list-style-type: none"><li>○ freeradius</li><li>○ freeradius-ldap</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Administrador de red GUI:<ul style="list-style-type: none"><li>○ network-manager-openvpn</li></ul></li></ul>

# ASIR VPN: Funcionamiento de la infraestructura



1. El cliente le manda una solicitud de autenticación a OpenVPN proporcionándole los certificados y usuario/contraseña.
2. OpenVPN a través de TLS, verifica que los certificados sean válidos y a través del plugin openvpn-auth-radius, le pregunta al FreeRADIUS si el usuario/contraseña que el cliente le ha proporcionado son válidos.
3. FreeRADIUS recoge la solicitud y verifica las credenciales contra OpenLDAP, a través de una conexión segura al puerto 389 bajo TLS.
4. OpenLDAP le envía una respuesta a FreeRADIUS validando la solicitud.
5. FreeRADIUS le envía una respuesta a OpenVPN validando la solicitud.
6. OpenVPN le concede el permiso al cliente de conectarse a la VPN.
7. Se inician los pasos de funcionamiento de OpenVPN descritos arriba.

## **ASIR VPN: Pruebas en directo**

---

- Creación de certificados para un usuario.
- Conexión a la VPN con dicho usuario.
- Intento de conexión a la VPN con credenciales falsas.
- Intento de conexión a la VPN con usuario no existente en el grupo de LDAP permitido.
- Ping a máquinas que están en la misma red que el servidor VPN.
- Revocación de certificado a un usuario.
- Intento de conexión con el usuario al que se le ha revocado el certificado.

## **ASIR VPN: Dificultades encontradas**

---

1. Escasa documentación sobre la infraestructura creada, OpenVPN + FreeRADIUS + OpenLDAP, como conjunto en sí.
2. Intento de uso de EAP-TLS como método de autenticación.
3. Uso correcto de certificados.

# ASIR VPN: Propuestas de modificaciones o ampliaciones

---

1. Implantar la VPN con IPsec ya que con la llegada de IPv6 no será necesario tener las redes NATeadas, además IPsec, mediante plugins parece ser que puede delegar el sistema de autenticación y autorización a un servidor RADIUS, cosa que con OpenVPN no se puede.
2. La creación de una infraestructura para el manejo de los certificados de los usuarios (creación, almacenamiento, revocación, etc) un poco más elaborada.