Servicio de Acceso Remoto Seguro para Terminales GSM y GPRS

Jaime Pérez Crespo

jperezc@rct.urjc.es

Febrero 2005

Contenidos

- Introducción
- ¿En qué consiste el servicio?.
- ¿Cómo se implementa?.
- Objetivos.
- Tecnologías.
- Conclusiones y trabajos futuros.
- Temas aprendidos.

Introducción

- Trabajo parte de una beca de colaboración con la URJC.
- Proyecto conjunto con Telefónica.
- Administración y mantenimiento de sistemas y redes.
- Construcción de una maqueta de un terminador de túneles.

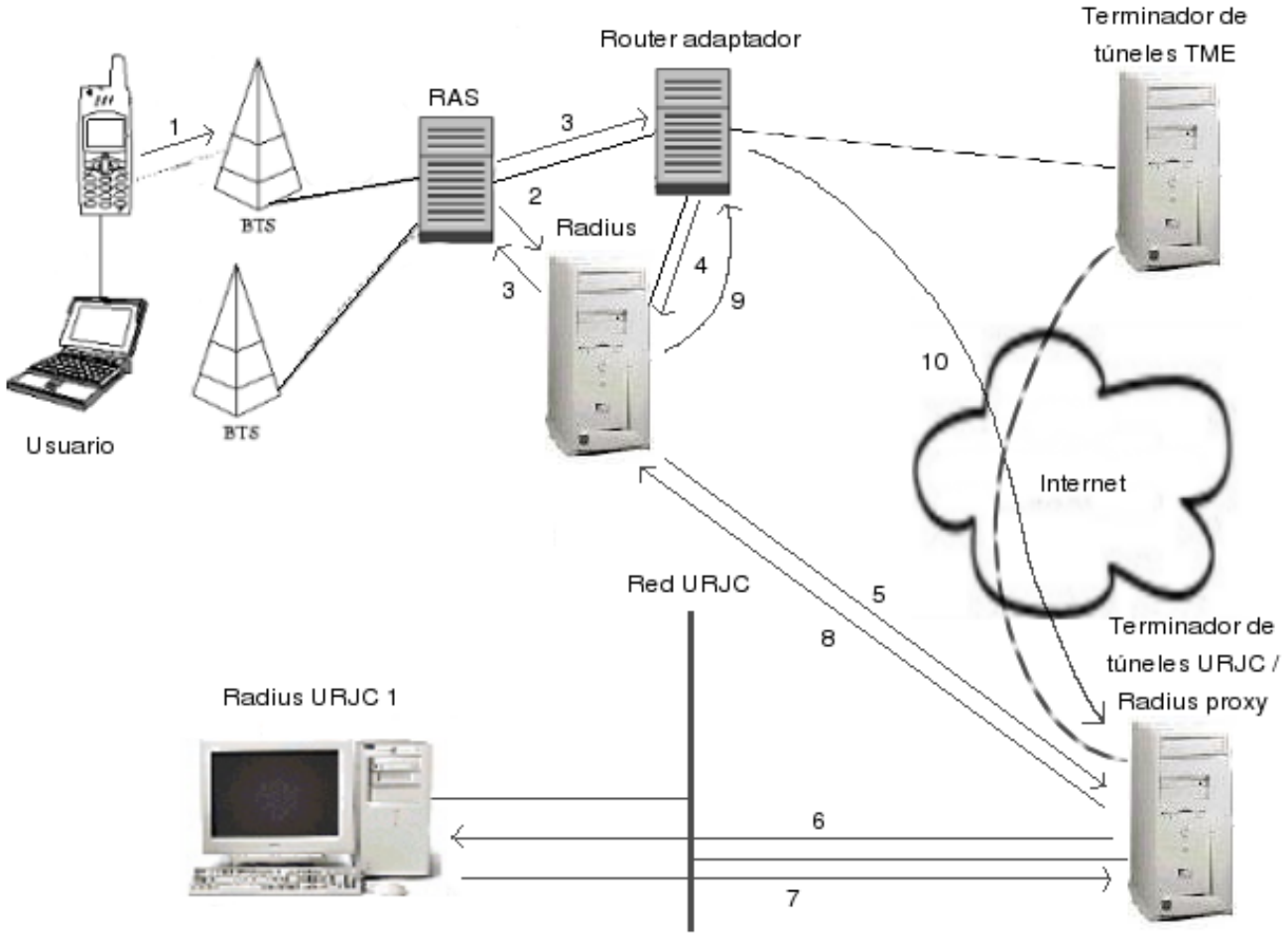
Descripción del servicio

- Teléfono móvil GSM o GPRS.
- Ordenador portátil.
- Tarjeta con extensión de la universidad.
- Servicios privados de la universidad.
- ¿Cómo juntarlo todo?.

Ejemplo práctico

1. Marcación del 553 en el terminal.
2. El RAS consulta a Radius Telefónica.
3. El Radius Telefónica indica que se establezca un Router Adaptador.
4. El Router Adaptador pide al Radius que autentique al usuario.
5. El Radius Telefónica escala la petición al Proxy Radius URJC.
6. El Proxy Radius URJC realiza la consulta a los Radius corporativos.
7. Los Radius corporativos URJC autentican al usuario.
8. El Proxy Radius URJC informa del resultado.
9. El Radius Telefónica recibe el resultado y en función de éste, asigna una IP.

Esquema del servicio



Implementación del servicio

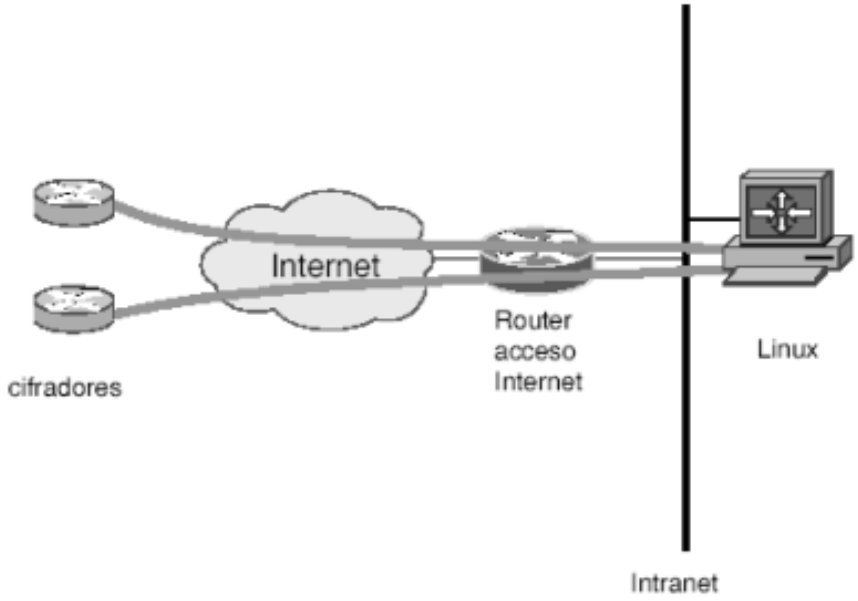
- Redes Privadas Virtuales (VPN). Independientes para cada cliente.
- Seguridad a nivel de red: `IPSec`.
- Protocolos de encaminamiento: `RIP`.
- Autenticación y autorización: `Radius`.

Objetivos

- Documentación. Libros, manuales, RFC's...
- Configuración de un terminador de túneles IPSec.
- Sencillez de montaje y mantenimiento.
- Coste reducido.
- Seguridad.
- Pruebas:
  - Seguridad y mantenimiento de la maqueta (URJC).
  - Funcionamiento correcto del servicio (Telefónica + URJC).

Tecnologías

- Sistema GNU/Linux.
  - Arquitectura loopback.

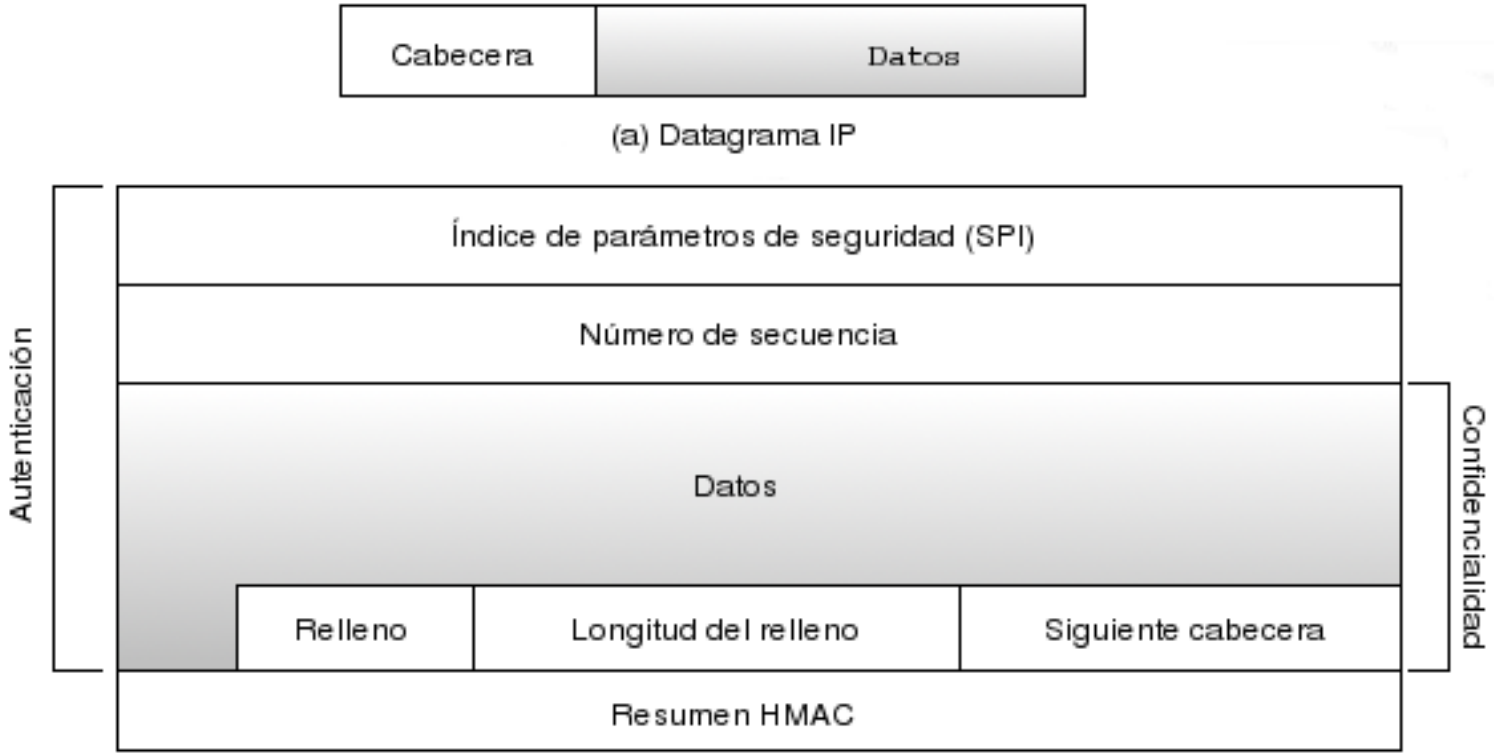


Tecnologías

- Redes Privadas Virtuales.
  - IPSec. Seguridad integrada en IPv4.
  - OpenSWAN + núcleo del sistema operativo.
  - Confidencialidad e integridad: 3DES + ESP.
  - Autenticación: SHA1 (¿roto?) + IKE.
  - Túneles IPIP.

Tecnologías

- Modo túnel IPIP, protocolo ESP.



Tecnologías

- RIP:
  - quagga.
  - Encaminamiento dinámico y sencillo.
- Radius:
  - GNU Radius está homologado, FreeRadius no.
  - Servidor delegado o proxy.
  - Se utilizan "realms" para ver quién autentica.
- Filtrado de paquetes con iptables.
  - No restrictivo con los usuarios del servicio.
  - Muy restrictivo para administración del propio terminador.

Conclusiones y trabajos futuros

- Terminador de túneles IPSec.
- Servidor Radius delegado o proxy.
- Encaminamiento dinámico mediante RIP.
- Sencillez de uso y administración.
- Pruebas pendientes con Telefónica.
- Mejorar la administración del servicio.
- Interfaz de monitorización del terminador.

Temas aprendidos

- Redes Privadas Virtuales: IPSec.
- Protocolos de encaminamiento: RIP.
- Autenticación, Autorización, Cuentas: Radius.
- Tecnologías móviles: GSM y GPRS.