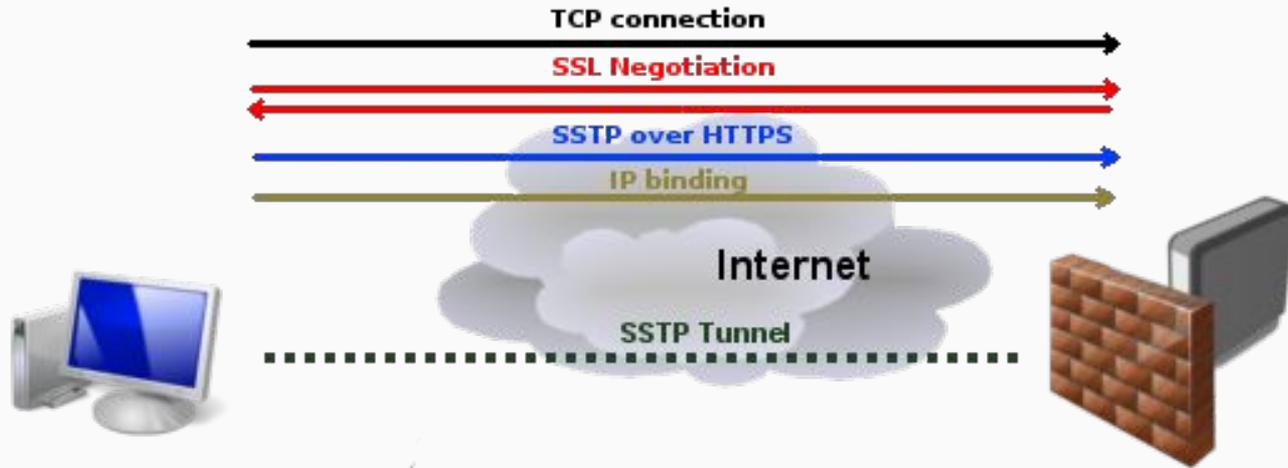


OpenSSL





¿Qué es OpenSSL?

OpenSSL es un proyecto de software libre basado en *SSL* *Leay*, desarrollado por Eric Young y Tim Hudson.

Consiste en un robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como *OpenSSH* y navegadores web (para acceso seguro a sitios HTTPS).

Estas herramientas ayudan al sistema a implementar el *Secure Sockets Layer (SSL)*, así como otros protocolos relacionados con la seguridad, como el *Transport Layer Security (TLS)*. *OpenSSL* también permite crear certificados digitales que pueden aplicarse a un servidor, por ejemplo *Apache*.

Los siguientes algoritmos de criptografía son soportados por la herramienta:

- **Para cifrado**

AES, Blowfish, Camellia, SEED, CAST-128, DES, IDEA, RC2, RC4, RC5, Triple DES, GOST 28147-89³

- **Funciones HASH**

MD5, MD4, MD2, SHA-1, SHA-2, RIPEMD-160, MDC-2, GOST R 34.11-94⁴

- **Clave pública**

RSA, DSA, Intercambio de claves Diffie–Hellman, curvas elípticas

Vamos a ingresar a la página y ver los detalles

OpenSSL

Cryptography and SSL/TLS Toolkit

Telecomunicaciones de voz y Data

Stevenson Canó

