Protección a nivel de red (IPSec)
Protección a nivel de transporte (SSL / TLS / WTLS)
Redes Privadas Virtuales (VPN)

Ávila Santos Alex
Trejo Chávez Konrad
Ramos Grados Luis
Gerald Palomino Monge

Introducción

- IPsec es un conjunto de protocolos que proporcionan servicios de seguridad en la capa de red del modelo OSI, tanto en TCP como en UDP.
- Ipsec asegura las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos y también incluye protocolos para establecer claves de cifrado.
- SSL,TLS,WTLS es un estándar que permite dar seguridad a la comunicación cliente servidor valiéndose de encriptamiento de la información.
- Las VPN nos permiten extender de forma segura nuestra LAN sobre un red pública o no controlada como internet, permite que un computadora en la red envíe y reciba datos en redes públicas o compartidas como si fuera una red privada de forma segura con toda la funcionalidad, seguridad y políticas de gestión.

Protección a nivel de red (IPSec)

- Es un conjunto de protocolos que cumplen con asegurar las comunicaciones sobre el protocolo de Internet (IP) cifrando y/o autenticando cada paquete IP en el flujo de datos.
- Los protocolos actúan en la capa de red (capa 3 del modelo OSI).
- Para que una aplicación pueda usar Ipsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar sus códigos.
- Ipsec está implementado sobre un conjunto de protocolos criptográficos. Para asegurar el flujo de paquetes, garantizar la autenticación mutua y establecer parámetros criptográficos.

Aplicaciones de IPSec

- Conexión de dos oficinas por medio del Internet.
- Acceso Remoto seguro sobre el Internet
- Establecer conexiones Intranet + Extranet con socios comerciales.
- Mejorando la seguridad del comercio electrónico.

Componentes del IPSec

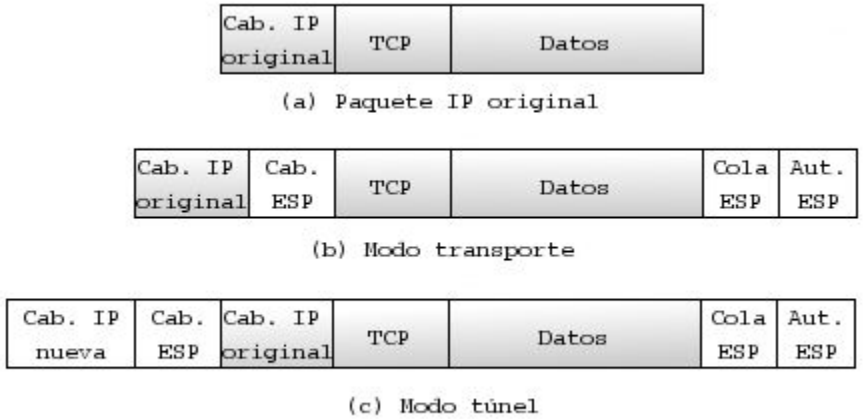
- Un protocolo de seguridad de claves.
  - Intercambio de llaves de internet.
- Dos protocolos de seguridad.
  - Carga de seguridad de encapsulado (ESP)

    Proporciona integridad de datos, encriptación, autenticación y anti reproducción.
  - Autentificación de cabecera IP (AH)

    También proporciona integridad de datos , autenticación y anti reproducción pero no cifrado.

Modos de funcionamiento (IPSec)

- Modo transporte
  - En este modo, solo la carga útil del paquete IP es autenticada y/o cifrada.
- Modo túnel
  - En este modo, todo el paquete IP es autenticado y/o cifrado



Archivos de configuración del servidor IPsec

- Archivo de configuración de StrongSwan Ipsec
  - /etc/ipsec.conf
    - ✓ **config setup** define parámetros de configuración generales
    - ✓ **conn <name>** define una conexión
    - ✓ **ca <name>** define una autoridad de certificación
- Archivo de secretos de StrongSwan Ipsec
  - /etc/ipsec.secrets contiene los tipos de secretos:
    - ✓ **RSA** define una clave privada RSA
    - ✓ **ECDSA** define una clave privada de ECDSA
    - ✓ **BLISS** define una clave privada BLISS (desde 5.2.2)
    - ✓ **P12** define un contenedor PKCS # 12 (desde 5.1.0)
    - ✓ **PSK** define una clave precompartida
    - ✓ **EAP** define las credenciales de EAP
    - ✓ **NTLM** define las credenciales NTLM
    - ✓ **XAUTH** define las credenciales de XAUTH
    - ✓ **PIN** define un PIN de tarjeta inteligente

SSL

Secure Sockets Layer (en español **capa de puertos seguros)** Es un estándar que brinda seguridad a la comunicación cliente servidor , a través del encriptado de sus datos. Para ello el cliente y el servidor deberán compartir una serie de parámetros a través de un certificado ssl .

Certificado ssl

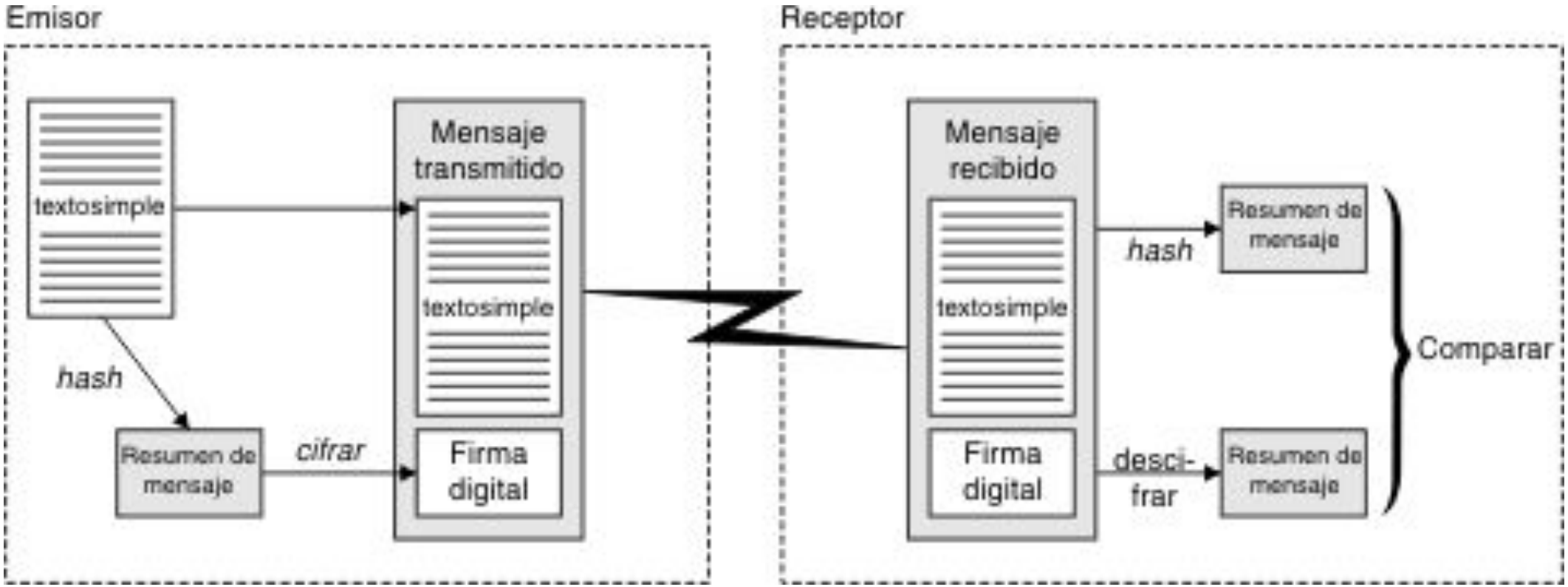
Para establecer la coneccion se instala un certificado ssl en el servidor este sirve como un "pasaporte" electrónico que establece las credenciales de una entidad en línea al hacer negocios en la Web

¿ Para qué sirve ?

- Autenticar la identidad del sitio web, garantizando a los visitantes que no están en un sitio falso.
- Información de inicio de sesión y contraseñas.
- Información financiera (como números de tarjetas de crédito y cuentas bancarias).
- Datos personales (como nombres, direcciones, números de seguridad social y fechas de nacimiento).
- Información patentada.
- Listas de clientes.

Estableciendo comunicación

Integridad del certificado



SSL vs TSL

El protocolo criptográfico TSL (seguridad de la capa de transporte) creado en 1999 es el sucesor de SSL ambos se trabajan de manera semejante sin embargo la encriptación pero el primero se caracteriza por tener una encriptación más fuerte que su antecesor.

Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.

Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES y AES (Advanced Encryption Standard).

WTLS

Adaptación de TLS que provee autenticación para servicios wap , es decir para dispositivos móviles .

Está adaptado para la condiciones que este medio presenta es decir :

- Bajo ancho de banda
- Poder de procesamiento limitado
- Poca capacidad de memoria

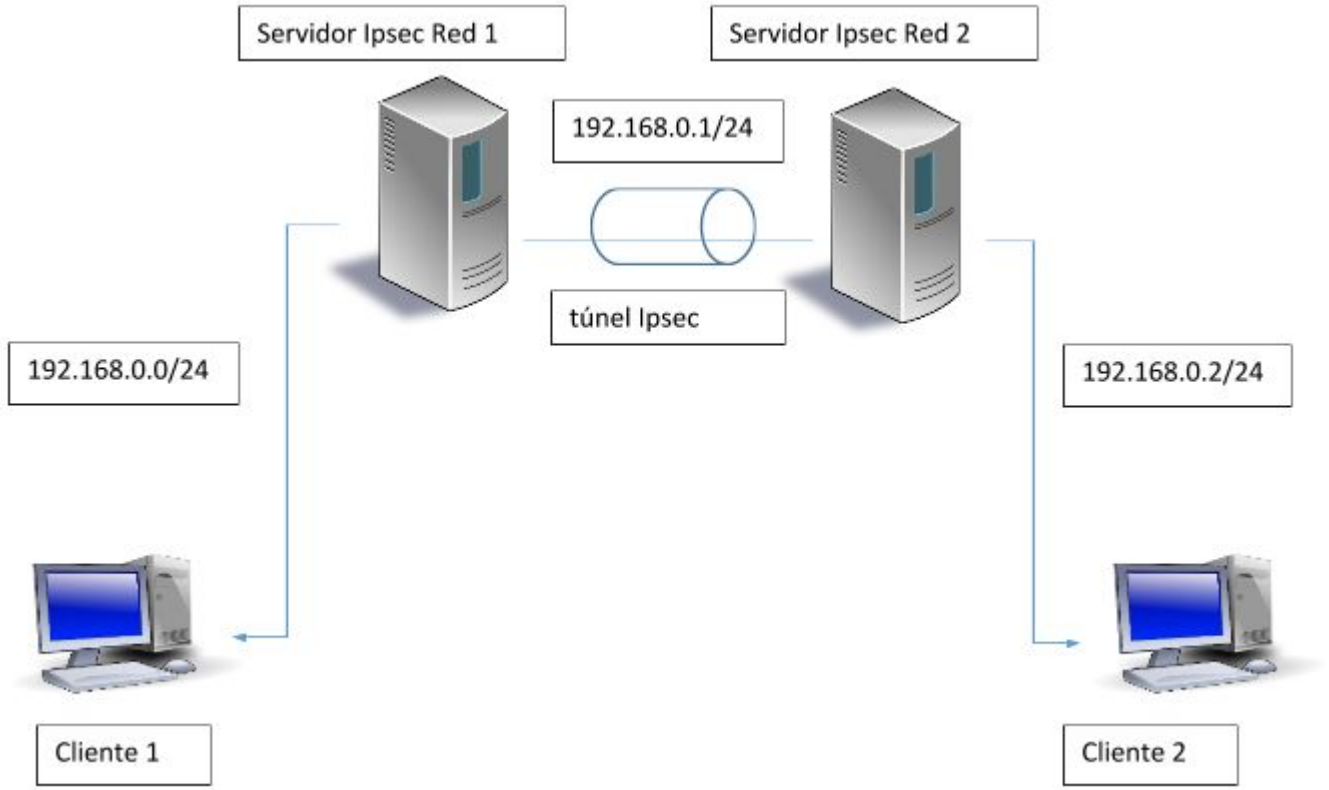
Redes Privadas Virtuales (VPN)

Las VPN nos permiten extender de forma segura nuestra LAN sobre un red pública o no controlada como internet, permite que un computadora en la red envíe y reciba datos en redes públicas o compartidas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

La conexión VPN a través de Internet es técnicamente una unión Wide Area Network (WAN) entre los sitios pero al usuario le parece como si fuera un enlace privado

Red IPSEC


Servidor Ipsec Red 1
Servidor Ipsec Red 2
192.168.0.1/24
túnel Ipsec
192.168.0.0/24
192.168.0.2/24
Cliente 1
Cliente 2

Red servidor SSL