SEGURIDAD EN SITIOS WEB

Septiembre 2001

Ing. Carlos Ormella Meyer

Seguridad en Sitios Web

- **Formas de diagnósticos de seguridad:**

⇒ **Evaluación de vulnerabilidades**

⇒ **Pruebas de penetración**

⇒ **Auditoría de seguridad**

Seguridad en Sitios Web

- Evaluación de vulnerabilidades:

⇒ Busca determinar las fallas de seguridad de un sistema.

⇒ Produce reportes del tipo, cantidad y grado de dichas fallas.

⇒ Permite establecer el status de seguridad en un momento determinado, aunque sin referirse a estándares específicos.

⇒ Permite tomar medidas **preventivas** para evitar que las fallas sean aprovechadas por un hacker.

Seguridad en Sitios Web

- **Formas de Escaneado:**

⇒ **Sniffer o Husmeador de Paquetes**

⇒ **Barridos con Pings**

⇒ **Escaneados TCP**

⇒ **Escaneados UDP**

⇒ **Identificación del Sistema Operativo**

⇒ **Escaneados de Cuentas**

Seguridad en Sitios Web

- **Factores que facilitan las intrusiones**

⇒ **Contraseñas**

⇒ **Protocolos**

⇒ **Uso Indebido de Comandos y Utilitarios**

⇒ **Fallas de Programas**

⇒ **Fallas de Configuración**

⇒ ***Conexiones y/o equipos remotos o móviles inseguros***

Seguridad en Sitios Web

- **Control de Acceso.**

• **Firewall**: Sistema que ejecuta una política de control de acceso entre redes y que por lo tanto no protege contra accesos internos indebidos.

» **Tipos de Firewalls:**

⇒ Filtros de Paquetes

⇒ Filtros dinámicos

⇒ Gateways de aplicación

• **IDS:** La aproximación más común compara el tráfico con patrones de ataques conocidos. Otra verifica la integridad de archivos no cambiantes.

Seguridad en Sitios Web

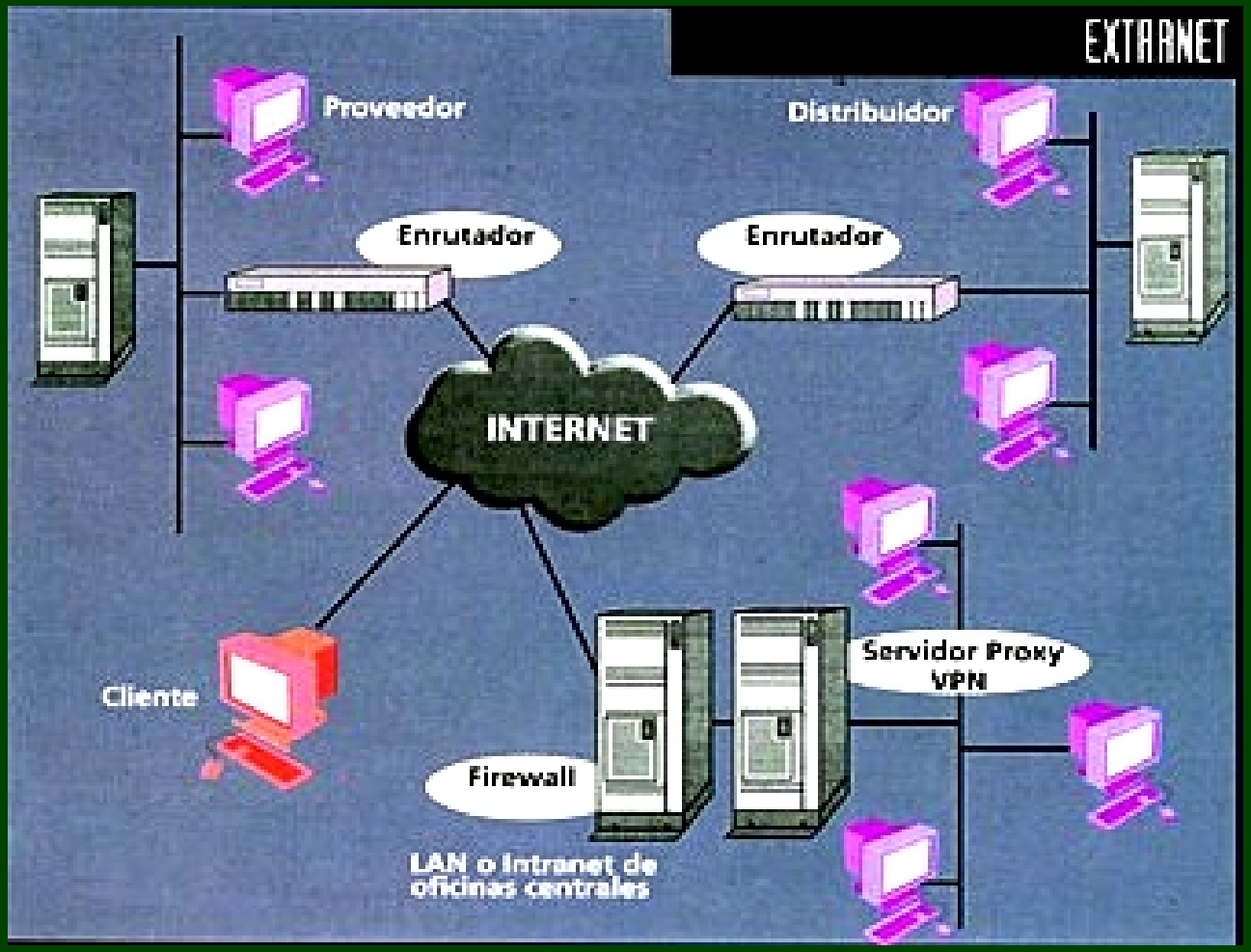
- **Comunicaciones remotas:** Se pueden usar líneas dedicadas o WANs como ISDN y Frame Relay, pero no son prácticas para usuarios móviles.
  - » Internet es un medio abierto que facilita las conexiones.
  - » Una VPN permite conexiones con seguridad.
- **VPN** es una ***Red Privada y Virtual.***
- **Tipos de VPN:**

⇒ **Acceso Remoto**

⇒ **Intranet Extendida**

⇒ **Extranet**

Seguridad en Sitios Web

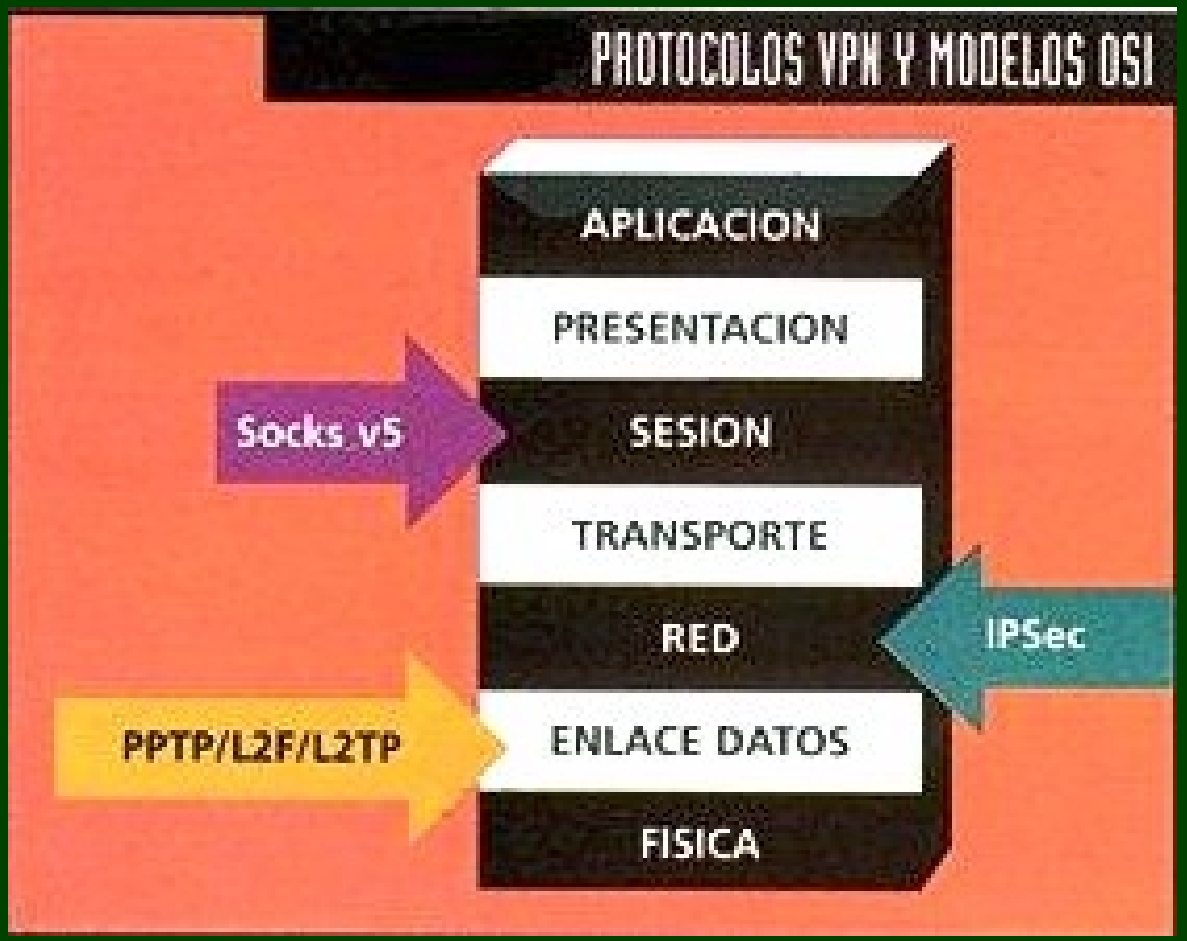


Seguridad en Sitios Web

- **Túnel:** Trayectoria virtual por la que viajan los paquetes de un punto a otro de Internet.
- La tunelización es básicamente un encapsulado con un protocolo adecuado, de modo que el paquete original se puede encriptar o autenticar el origen.
- **Gateway o servidor VPN:** dispositivo que encapsula los paquetes que recibe de una LAN o intranet local hacia Internet, y desencapsula los que recibe de Internet y los envía a su destino interno.

» Un túnel se establece entre un gateway y otro o bien con una máquina bajo VPN conectada a Internet.

Seguridad en Sitios Web



Seguridad en Sitios Web

- **Tunelización de Capa 2:** Permite interconectar plataformas similares IP, IPX y NetBEUI.

» Los protocolos de tunelización de Capa 2 son:

⇒ **PPTP**

⇒ **L2F**

⇒ **L2TP**

- Estos protocolos derivan del **PPP** que encapsula paquetes IP, IPX o NetBEUI en conexiones discadas o dedicadas punto a punto, y permite **autenticación del usuario** por medio de CHAP, PAP o MS-CHAP.

Seguridad en Sitios Web

- **PPTP*:*** Encripta con MPPE (basado en RC4) y permite compresión con protocolo MPPC de Microsoft.
- **L2F:** Original de Cisco. Sólo autentica, no encripta.
- **L2TP:** Norma del IETF que puede manejar tráfico IP, IPX o NetBEUI y enviarlo por cualquier medio basado en IP (incluyendo Internet), Frame Relay, ATM y X.25. Sólo autentica; no encripta.

Seguridad en Sitios Web

- **IPSec o Seguridad IP**

⇒ **Autenticación:** Identifica la ***máquina*** de origen, pero NO al usuario. Para autenticarlo hay que recurrir o a un protocolo de capa 2 como L2TP, bajo la forma **L2TP over IPSec**, o bien a un protocolo de capas superiores como **SSL**.

⇒ **Integridad de los datos:** Detecta modificaciones de los datos.

⇒ **Privacidad:** Encripta para impedir la lectura del mensaje por parte de un destinatario indebido.

Seguridad en Sitios Web

- **Modos de Operación de IPSec:**

⇒ **Túnel:** Entre los dispositivos de borde de Internet. Agrega un nuevo encabezamiento IP externo.

⇒ **Transporte:** Entre las máquinas que se conectan.

- **Protocolos IPSec:**

⇒ **AH:** Verifica ***integridad*** del paquete y ***autenticación*** de origen.

⇒ **ESP:** Provee ***privacidad*** de datos y opcionalmente ***autenticación*** de origen.

⇒ **IKE*:*** Negocia protocolos, algoritmos y claves.

Seguridad en Sitios Web

- Con IPSec sólo se pueden usar claves precompartidas o certificados digitales.
- Para certificados digitales se puede usar:

⇒ Un servicio CA de terceros (como Verisign).

⇒ Un PKI propio (software de Entrust o Xcert).

⇒ El software propio de algunos gateways VPN que permite crear y revocar certificados digitales propios.

- IKE no permite trabajar con sistemas de autenticación de una sola vía tales como Radius o Tacacs+, así como tampoco autenticación fuerte como token u OTP. Siguen algunas soluciones.

Seguridad en Sitios Web

⇒ **XAUTH:** Extensión de IKE que intercala un intercambio apropiado entre sus dos fases operativas (establecimiento de parámetros de seguridad y protocolos IPSec a usar). Pero no permite autenticación fuerte cuando los usuarios remotos reciben asignación dinámica de direcciones.

⇒ **Autenticación Híbrida:** Primero el gateway se autentica a sí mismo conforme IKE, y lo mismo hace el host cliente. Luego se sigue el proceso Xauth para autenticar al usuario.

⇒ **L2TP Sobre IPSec:** Soluciones propietarias.

Seguridad en Sitios Web

- **NAT:** Al cambiar la dirección IP de origen permite separar direcciones internas privadas de una o más direcciones registradas a la salida.

» NAT tendría que preceder al IPSec, porque al cambiar la dirección IP regenera el checksum TCP.

⇒ **AH:** Fallará de autenticar al verdadero origen.

⇒ **ESP:** En el modo transporte no autentica el verdadero origen.

» Algunos ISP de banda ancha requieren que se use NAT en la periferia quedando atrás el cliente IPSec.

Seguridad en Sitios Web

» Hay soluciones propietarias que permiten que el tráfico IPSec atraviese (modo ***Traversal***) un firewall o enrutador que realice NAT, generalmente encapsulando en UDP el paquete IPSec.

» Para el uso de claves precompartidas IKE requiere que no se cambien las direcciones IP de cada extremo durante el establecimiento de algoritmos y método de intercambio de claves. Se puede trabajar con otro tipo de identificador, por ejemplo la ID del usuario o el nombre del dominio (como con Win 2000).

Seguridad en Sitios Web

- **Análisis del Ambiente de Trabajo Remoto**

⇒ *Aumento sostenido de las comunicaciones remotas* a una empresa.

⇒ *Mayores velocidades*.

⇒ Las soluciones de banda ancha generalmente son conexiones permanentes (***always-on***), es decir se mantiene una dirección IP, e incluso hasta pueden ser compartidas.

- Los túneles VPN pasan en forma transparente a través del firewall de la empresa.

Seguridad en Sitios Web

- **Análisis del Ambiente de Trabajo Remoto**

⇒ **Firewall personal:** Debe permitir que se impongan políticas de seguridad desde un servidor central.

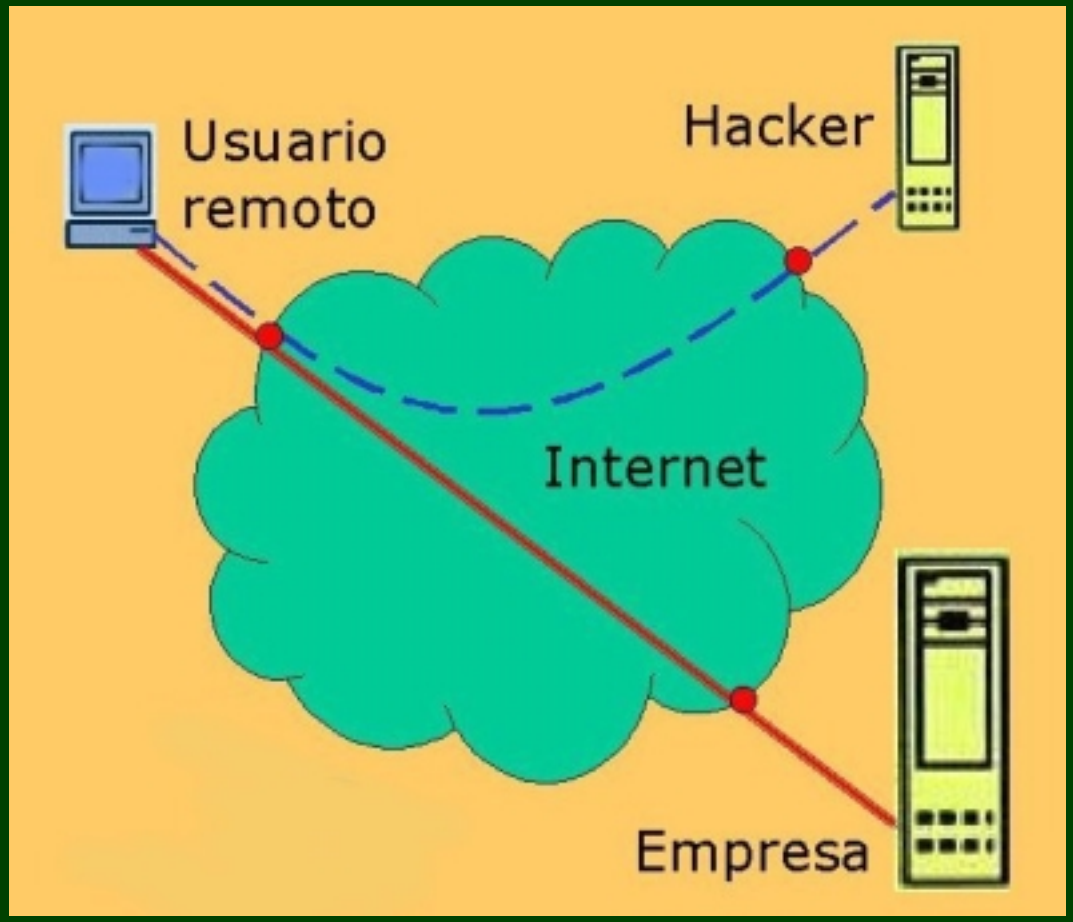
⇒ **Detector de intrusiones:** Debe poder enviar alertas en tiempo real al administrador de la red de la empresa.

⇒ **Antivirus:** Actualizado una vez al día como cliente administrado; filtros de contenido para evitar Caballos de Troya (tráfico saliente del remoto sólo de las aplicaciones conocidas).

⇒ **Encriptado de archivos.**

Seguridad en Sitios Web

Split Tunneling



Deshabilitación de túnel dividido.

Al registrarse identificar la o las tarjetas de red del usuario remoto mediante comandos SNMP o herramienta de inventariado (como el SMS de Microsoft).

Seguridad en Sitios Web

- **Análisis del Ambiente de Trabajo Móvil**

⇒ PDA, Palmtops, Pocket PC, handheld o laptop. Se conectan al **AP** de una LAN bajo el protocolo del IEEE 802.11b o Wi-Fi a 11 Mbps.

» El protocolo de encriptado **WEP** viene sin activar por default, es poco seguro (claves estáticas de 40 bits) y requiere la distribución física de la clave.

» Hay productos que trabajan con claves de 128 bits y que son dinámicas, cambiando con cada sesión.

» O bien un túnel VPN con IPSec. Pero necesitará un servidor VPN entre el AP y la LAN cableada.

Seguridad en Sitios Web

» Un producto VPN es movianVPN de Certicom que dialoga con los principales gateway VPN y viene en equipos como la serie Jornada 560 de HP.

» Sincronización por infrarrojo entre PDAs y PCs. Puede pasar datos sin verificar la PC.

- **Bluetooth.** Seguridad: FH con 1600 saltos por segundo; dirección única sin encriptar; inicialización con PIN de 4 dígitos en memoria o en disco; claves de encripción compartidas; sólo autentica dispositivos, no usuarios.