Arquitecturas de seguridad

[6.1] ¿Cómo estudiar este tema?

[6.2] Arquitecturas de seguridad tradicionales

[6.3] Secure Socket Layer: SSL

[6.4] Protocolo SSH

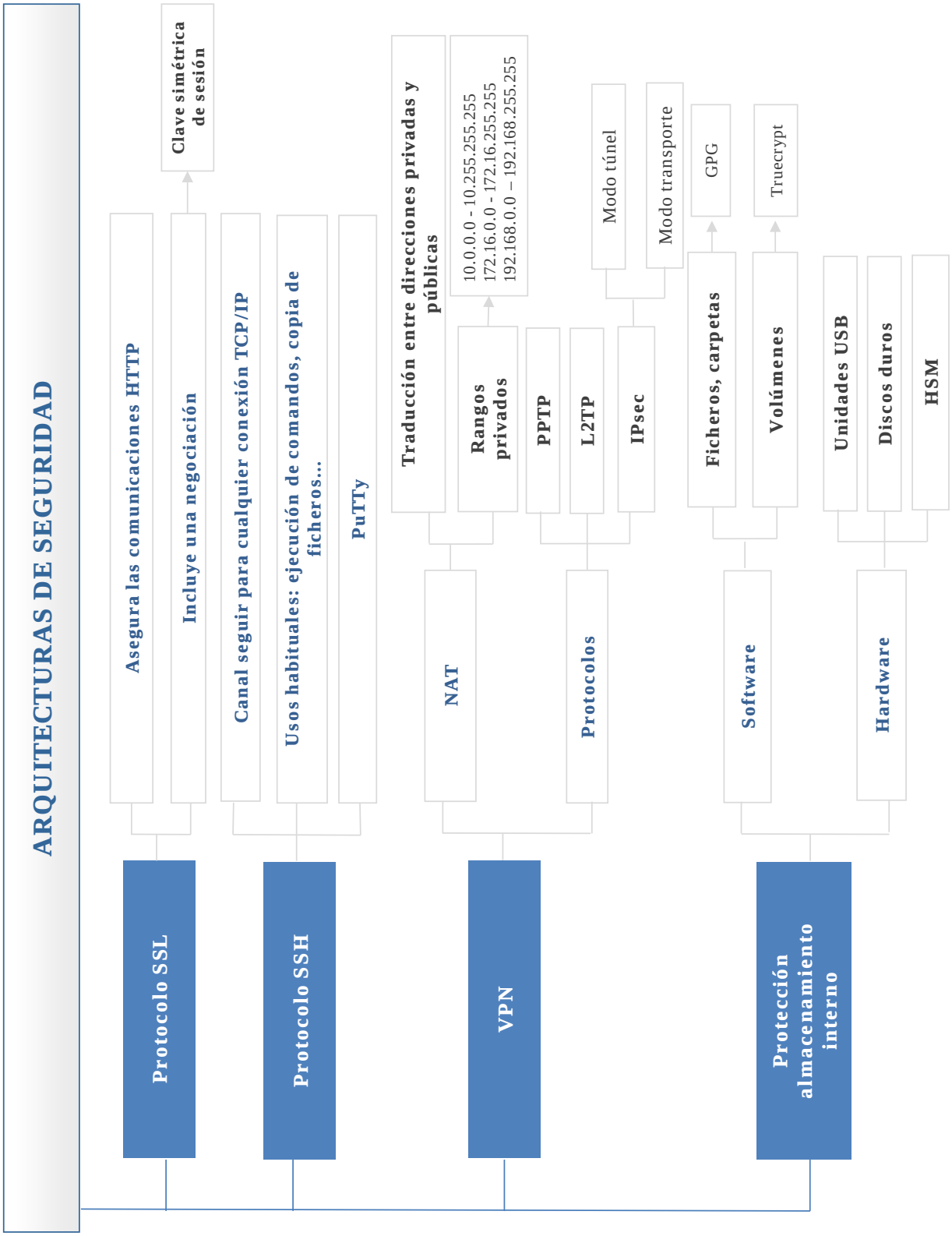
[6.5] Redes Privadas Virtuales (VPNs)

[6.6] Mecanismos de protección de unidades de almacenamiento externo

[6.7] Mecanismos de protección hardware

TEMA 6

Esquema


ARQUITECTURAS DE SEGURIDAD
Protocolo SSL
Asegura las comunicaciones HTTP
Incluye una negociación
Clave simétrica de sesión
Protocolo SSH
Canal seguir para cualquier conexión TCP/IP
Usos habituales: ejecución de comandos, copia de ficheros...
PuTTy
VPN
NAT
Traducción entre direcciones privadas y públicas
Rangos privados
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.16.255.255
192.168.0.0 – 192.168.255.255
Protocolos
PPTP
L2TP
IPsec
Modo túnel
Modo transporte
Protección almacenamiento interno
Software
Ficheros, carpetas
GPG
Volúmenes
Truecrypt
Hardware
Unidades USB
Discos duros
HSM

Ideas clave

6.1. ¿Cómo estudiar este tema?

El estudio de este tema se realiza a través de los contenidos desarrollados en las **Ideas clave** expuestas a continuación.
Para estudiar el apartado **6.5** te recomendados también el texto **páginas 2-12:** Fernández, J.; Alonso, J.L.; Figueroa, C. & Zazo, A. (2006). *Redes Privadas Virtuales.* Informe Técnico-Rechnical Report. DPTOIA-IT-2006/004. Septiembre 2006. Recuperado el 3 de noviembre de 2014 en:
http://eprints.rclis.org/13992/1/fernandez2006redes.pdf

En este tema veremos SSL como una capa de seguridad independiente con funciones de hacer posible la transmisión de datos críticos sobre Internet, usando una combinación de criptografía asimétrica y simétrica. VPN´s y NAT, como uno de los grandes problemas del sistema de direccionamiento de IPv4, y protección de dispositivos de almacenamiento seguro para guardar información confidencial.

En este tema realizaremos una primera aproximación a la **seguridad de las redes** de la mejor manera posible: **«aprendiendo a atacarlas»**. Comenzaremos estudiando una taxonomía completa de los **tipos de ataques**, sus **características** y **principales contramedidas**.

En la sección dedicada a las Redes Privadas Virtuales, no olvides consultar el siguiente Informe Técnico, páginas 2-12:

6.2. Arquitecturas de seguridad tradicionales

En el primer tema, en el apartado *1.2 La seguridad informática: perspectiva histórica* citamos como nació Internet, la búsqueda de un sistema capaz de reaccionar frente a adversarios que vinieran fuera de la red. Expliquemos al alumno un ejemplo de la importancia de este tema, vinculado al apartado anterior.

Una vez desarrollado Internet, el funcionamiento era idóneo, reacionaba bien a los ataques externos. Uno de los grandes problemas, era si el «enemigo» se encontraba conectado desde dentro, y el otro... era inimaginable: elegido un sistema de direccionamiento de 32 bits, implicaba la existencia de más de cuatro mil millones de direcciones IP´s, ¿cómo pensar en su agotamiento?, pues así fue. *Parches* a estos problemas han ido extendiendo la vida de IPv4, hasta la llegada total de IPv6. Uno de esos parches fue, y es NAT. Desde este tema, expondremos la importancia de VPN y NAT.

Prácticamente cualquier empresa, agencia gubernamental o corporación en general cuenta ahora con uno o varios sitios Web. «Quien no esté en Internet, no existe», literalmente. Este es un «pastel», por supuesto, demasiado irresistible para un atacante.

Una aplicación Web puede atacarse en varios puntos:

- En la propia lógica de la aplicación, **a través de ataques de inyección SQL, XSS y otros muchos**.
- **A través del navegador del usuario**.
- **Interceptando el tráfico entre el navegador y el servidor Web.**

Analizaremos las amenazas primera y segunda en profundidad en próximos temas de esta asignatura, por lo que en éste nos centraremos sobre todo en la tercera.

Así pues, en este tema analizaremos las arquitecturas de seguridad existentes cuyo **objetivo principal es proteger las comunicaciones entre distintos elementos**, un servidor Web, por ejemplo, aunque no tenemos porqué limitarnos a eso. Por ejemplo, estudiaremos también el ***protocolo SSH***, que aporta seguridad a una consola tradicional de red.

Existen **diversas aproximaciones al problema en función de en qué lugar de la pila TCP/IP decidimos situar el mecanismo de protección**. Cada lugar tiene sus ventajas e inconvenientes, que puedes observar en la **Figura 1**. Por ejemplo, una forma de proteger las comunicaciones es utilizar **IPSec**, un protocolo que se sitúa a nivel de red (Figura 1.a). La ventaja en este caso es que resulta transparente para los usuarios finales y aplicaciones y proporciona una solución de propósito general, que sirve para cualquier protocolo superior.

En la imagen vemos cómo podría proteger a HTTP, FTP, SMTP o cualquier otro protocolo de aplicación igualmente bien. El precio que hay que pagar para esta versatilidad es que el mecanismo se vuelve muy complejo en su configuración.

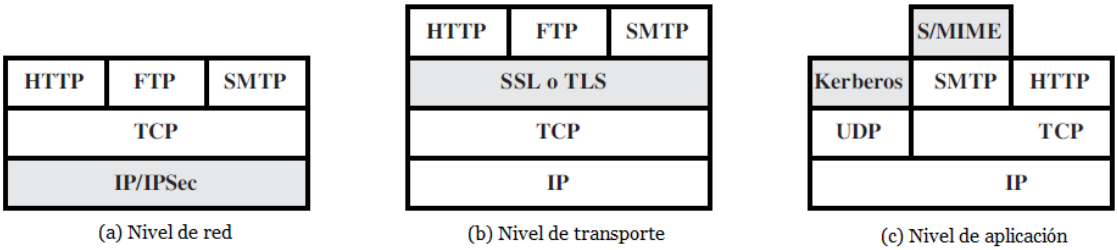


Figura 1. Diferentes arquitecturas de seguridad y su localización en la pila TCP/IP

Otra forma de abordar el problema es entonces «escalar» en la pila para y situarnos justo encima del nivel de transporte, normalmente con el protocolo TCP (Figura 1.b). Perderemos generalidad, puesto que ahora estamos atados a TCP, pero el protocolo se volverá más sencillo. Este es el enfoque utilizado, por ejemplo, por SSL, un conocidísimo mecanismo de seguridad que analizaremos en este tema.

6.3. Secure Socket Layer: SSL

El **protocolo SSL** fue desarrollado por la empresa *Netscape* en 1994 para garantizar la seguridad en el intercambio de datos entre un navegador y un servidor Web, siendo en la actualidad el más utilizado para realizar transacciones y comerciales en Internet. **SSL permite garantizar la confidencialidad, la autenticación y la integridad de los mensajes intercambiados.**

Como se trata de un protocolo relativamente viejo ya para un mundo tecnológico, su sucesor se denomina **TLS (Transport Layer Security)**, y es una nueva propuesta que nace como una evolución de SSL. Ambos protocolos son protocolos de nivel de transporte, por lo que podrían ser utilizados para el cifrado de protocolos de aplicación como Telnet, FTP, SMTP, IMAP o el propio HTTP. Se ubican, por tanto, entre el protocolo TCP y la capa de aplicación.

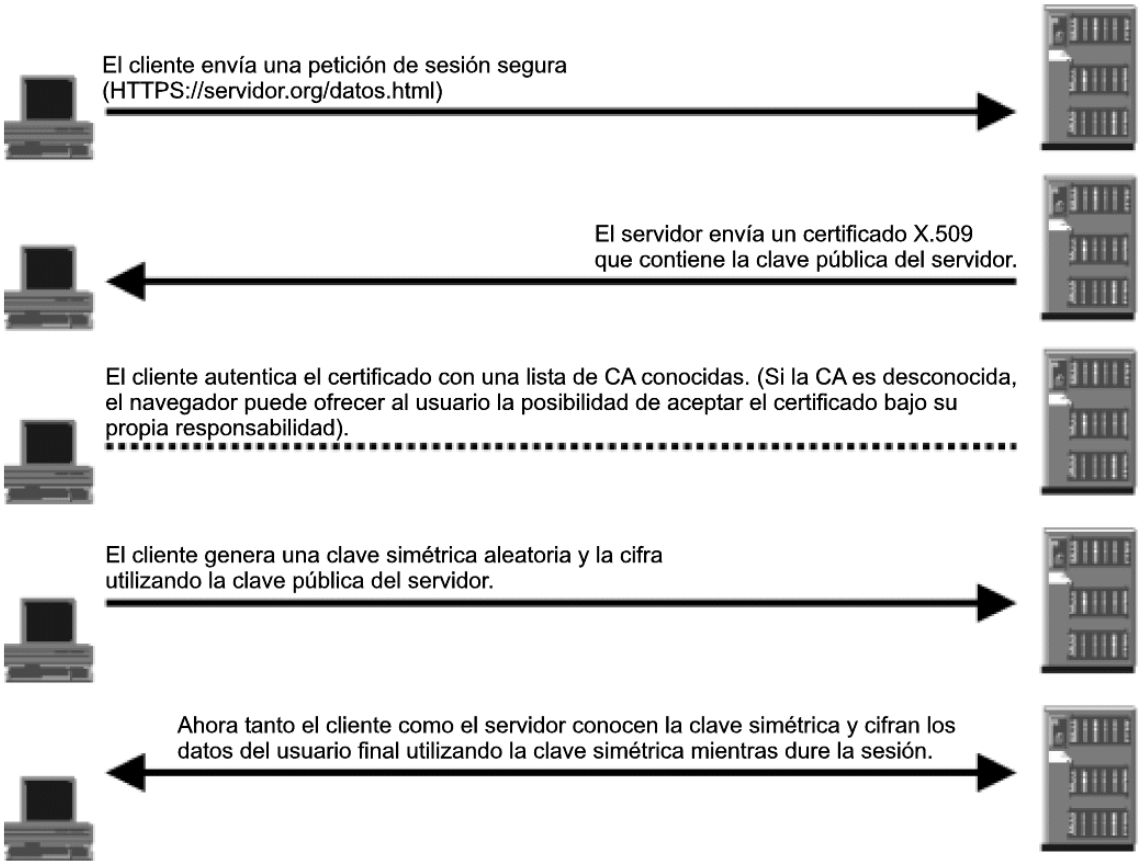


Figura 1. Esquema simplificado de una negociación SSL. (Fuente: publib.boulder.ibm.com)

El **funcionamiento básico de SSL** es sencillo:

1. Se produce un intecambio inicial de claves públicas entre cliente y servidor, utilizando para ello certificados digitales. La autenticación del servidor es obligatoria, pero no la del cliente, lo que podría generar algunos problemas de seguridad, como veremos a continuación.
2. Se negocian los parámetros del protocolo de cifrado simétrico, como el algoritmo de cifrado concreto o la longitud de clave, que se va a emplear en la sesión.
3. Se genera una clave simétrica aleatoria, que será sólo válida para esta sesión, por lo que la clave se denomina **clave de sesión**.
4. Se envía esta clave al servidor, cifrándola con su clave pública.
5. A partir de este momento todos los datos que se intercambien entre cliente y servidor se cifrarán con la clave de sesión.

El **principal problema** de este protocolo es el hecho comentado de que **la autenticación del cliente no es obligatoria**. Esto abre las puertas a ataques de tipo *man-in-the-middle*, como ya analizamos en el Tema 5 de la asignatura.

6.4. Protocolo SSH

El ***protocolo SSH*** es otra de las grandes arquitecturas de seguridad imprescindibles en la Internet moderna. En esencia, permite establecer una conexión segura a máquinas remotas, y fue diseñado para reemplazar servicios similares, pero inseguros, como Telnet, rlogin, rcp o FTP.

Este protocolo **utiliza un proceso seguro de autenticación del usuario**, ya que no se envía la contraseña *en claro* al servidor, como en los servicios habituales. Permite ejecutar comandos, copiar ficheros desde y hacia máquinas remotas y, en general, canalizar a través de un canal seguro cualquier conexión TCP/IP con una máquina remota.

El protocolo consta de **tres grandes bloques o partes fundamentales**:

- **Nivel de transporte:** se encarga de la autenticación del servidor, del establecimiento de un canal cifrado para garantizar la confidencialidad de la comunicación, de la comprobación de la integridad de los mensajes, así como de la generación de identificador único de sesión.
- **Nivel de autenticación de usuario:** el protocolo ofrece varios mecanismos de autenticación:
  - **Autenticación basada en el uso de criptografía de clave pública.** El usuario deberá disponer, por tanto, de un par de claves pública/privada para poder utilizar esta opción, sin duda la más segura.
  - **Autenticación tradicional basada en nombre de usuario y contraseña.** Esta contraseña se envía, en cualquier caso, cifrada.
  - **Autenticación basada en la procedencia (dirección IP de origen) de la conexión.** Esta opción no es segura y no debería utilizarse en entornos empresariales.
  - **Nivel de sesión:** se encarga de la asignación de identificadores de sesión, que permiten multiplexar varias comunicaciones distintas a través de un único «túnel» cifrado virtual.

Existen multitud de clientes SSH para diferentes sistemas operativos. Por ejemplo, *Linux* tiene el cliente integrado de forma nativa, por lo que sólo hay que lanzarlo con el comando «ssh». Para *Windows*, el cliente por excelencia quizás sea PuTTy, gratuito y ampliamente utilizado.

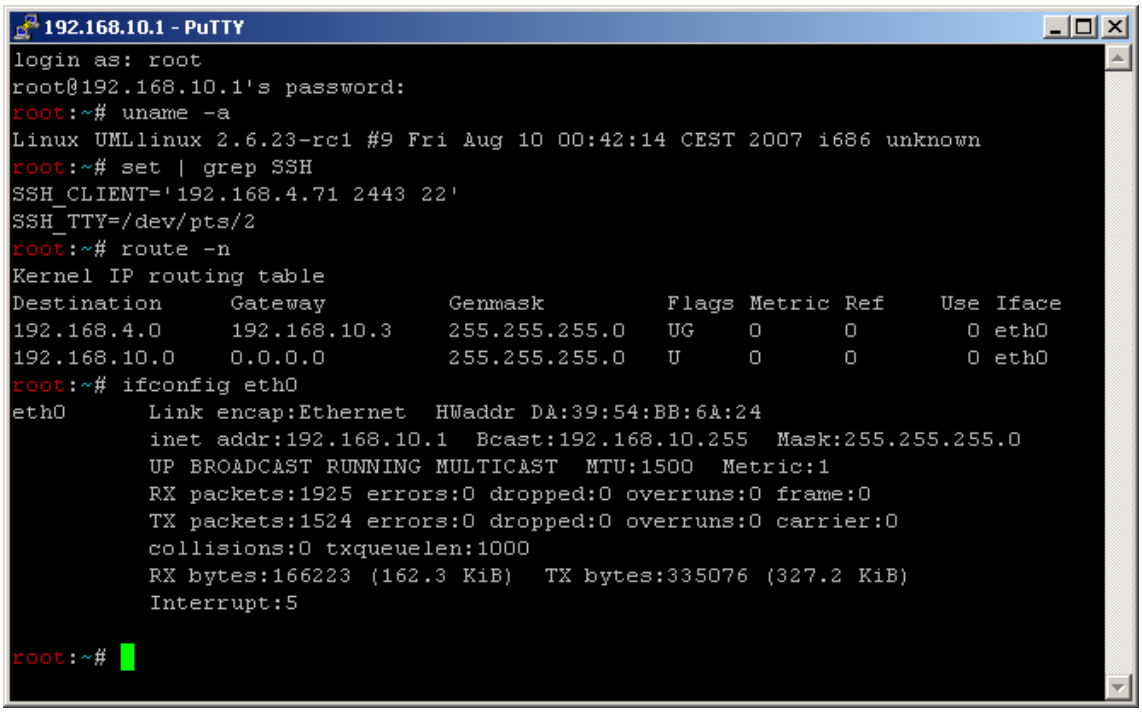


Figura 2. Sesión SSH activa

6.5. Redes Privadas Virtuales (VPNs)

Otra de las grandes arquitecturas de seguridad, imprescindibles en cualquier organización de tamaño medio o grande, son las denominadas **redes privadas virtuales** (VPN, en inglés, de *virtual private network*).

En pocas palabras, una VPN establece un enlace de comunicaciones segura entre dos nodos, utilizando para ello un método de encapsulamiento del tráfico que utiliza criptografía simétrica. A este enlace se le llama normalmente **túnel cifrado VPN**, o simplemente **túnel VPN**. En la **Figura 4** puedes encontrar un esquema general de una VPN.

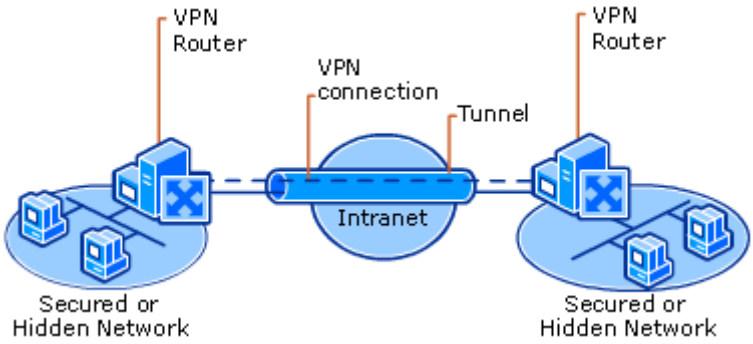


Figura 3. Esquema general de una VPN. Fuente: http://technet.microsoft.com/

NAT: Network Address Translation

El concepto de **traducción de direcciones**, más conocido por su acrónimo inglés NAT, es muy importante en el área de las redes de comunicaciones, de la seguridad en las mismas y de las VPN en particular.

Su principal aplicación es ocultar el direccionamiento IP interno de una red. La **IANA**, organismo internacional que se encarga de gestionar muchas cuestiones importantes respecto a la estructura de Internet, reservó en su momento **tres grandes bloques de direcciones IP** para su uso en redes privadas internas:

De la dirección 10.0.0.0 a la 10.255.255.255
De la dirección 172.16.0.0 a la 172.31.255.255
De la dirección 192.168.0.0 a las 192.168.255.255

Estas direcciones se conocen con el nombre de ***direcciones globales no-enrutables*** y significa que no pueden utilizarse como direcciones IP públicas, sino únicamente en el interior de redes «cerradas», privadas, que no son visibles desde Internet.

Es en este punto donde entra en juego el concepto de ***NAT***, que convierte estas direcciones privadas en direcciones IP «reales», públicas. Cualquier cortafuegos o router moderno incluye ya **capacidad NAT**, y se usa tanto como medida de seguridad (para ocultar información a un atacante), como para ahorrar costes (con una única dirección IP pública podemos tener muchas direcciones IP internas). En la **Figura 5** puedes encontrar un ejemplo de NAT.

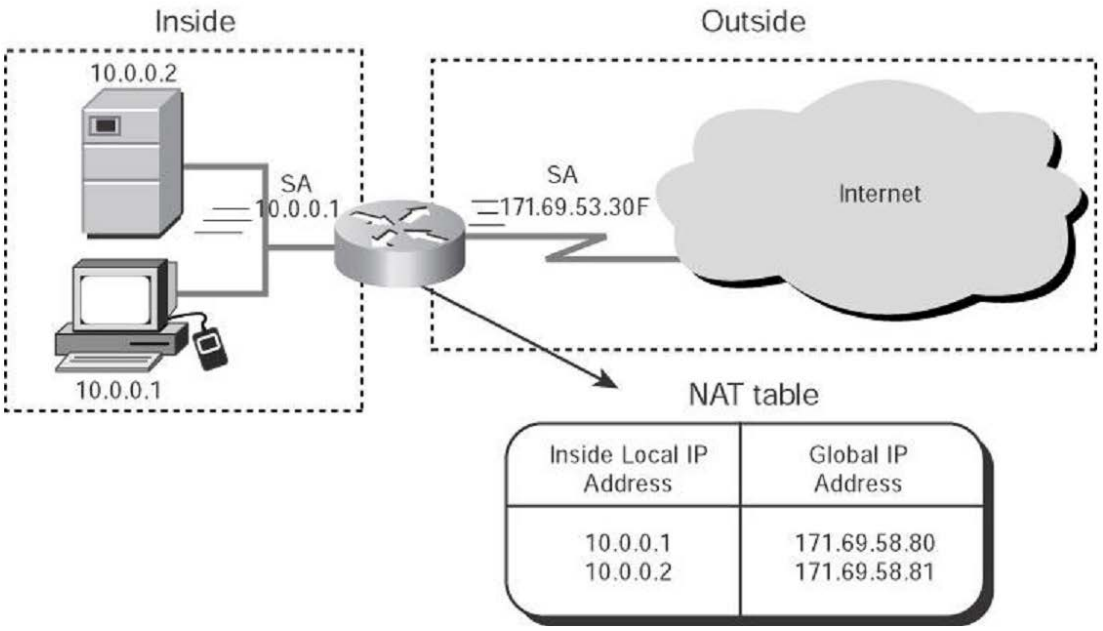


Figura 4. Ejemplo ilustrativo de proceso NAT

Protocolos VPN

El concepto genérico de VPN tiene que concretarse, por supuesto, en un protocolo que finalmente ordena la comunicación entre las partes. En el caso de VPN existen tres grandes tipos de protocolos actualmente en uso:

- **Point-to-Point Tunneling Protocol (PPTP).** Funciona a nivel de enlace del modelo OSI, y ha sido diseñado para conexiones sencillas, únicas entre cliente y servidor (no permiten conectar dos redes, por ejemplo). Este estándar es muy común en el entorno Microsoft, aunque va siendo sustituido paulatinamente por el siguiente protocolo, más moderno.
- **Layer 2 Tunneling Protocol (L2TP).** Este protocolo es una combinación del anterior, PPTP, y el antiguo Layer 2 Forwarding Protocol (L2F). Se ha convertido es un estándar, muy utilizado sobre todo en las conexiones de acceso a Internet vía telefónica (como las actuales ADSL).
- **IPSec**. Es el estándar más completo, pues permite todo tipo de conexiones, incluyendo túneles que conectan dos redes completas, en lugar de dos computadores. Esta versatilidad es también un inconveniente en ocasiones, pues puede llegar a ser difícil de configurar.

Dispositivos VPN

Los **dispositivos VPN** son e**lementos hardware o software que utilizan alguno o todos de los protocolos anteriores para crear túneles seguros**. Actualmente, la mayoría de los dispositivos con compatibles con IPSec, considerado el protocolo VPN más importante. IPSec tiene **dos grandes modos de operación**:

- **Modo túnel**, en el que todo el contenido del paquete se cifra (incluyendo, por ejemplo, cabeceras IP) y encapsula dentro de un paquete IPSec.
- **Modo de transporte**, en el que sólo los datos del paquete se cifran, dejando la cabecera IP visible e inalterada.

6.6. Mecanismos de protección de unidades de almacenamiento externo

Otra de las grandes arquitecturas de seguridad, a las que no se le suele prestar atención por no estar directamente relacionada con las redes, es **aquella dedicada a proteger el almacenamiento externo**, como discos duros, unidades USB extraíbles y cualquier otro medio.

Existen diferentes soluciones, tanto software como hardware, para solucionar este problema. Dentro del primero grupo podemos encontrar desde aplicaciones que aseguran determinados archivos o carpetas hasta protecciones a nivel de sistema de ficheros. En cuanto al hardware, el abanico de posibilidades es todavía más amplio, incluyendo unidades USB con capacidad de realizar determinadas operaciones criptográficas (ya sea mediante software o hardware), discos duros externos de gran capacidad, usados en entornos militares, o módulos de alta seguridad, muy utilizados en entornos bancarios, llamados **Hardware Security Modules (HSM)**.

Analizaremos estas soluciones con detalle a continuación.

Soluciones software

La ventaja de utilizar **soluciones software**, es que generalmente, se pueden utilizar tanto para unidades de almacenamiento externo, como USBs o discos duros externos, como para las unidades de almacenamiento propias de un ordenador.

Sin embargo, un inconveniente es que para poder utilizar estas funcionalidades será necesario **instalar dicho software en todos los ordenadores** desde los que se desee almacenar información «segura» y recuperarla.

A nivel de fichero o carpeta

Adoptando este tipo de soluciones software se puede cifrar el contenido determinados archivos o carpetas, tanto con criptografía de clave simétrica o asimétrica. Como ya sabemos, de forma muy esquemática y resumida, **en este modelo asimétrico es necesario el uso de dos claves**:

- **Clave pública:** esta clave puede ser difundida por un canal público o inseguro sin comprometer la seguridad. Cuando un extremo B consigue la clave pública de A (K_{pa}) utiliza la clave para cifrar la información hacia B.
- **Clave privada o secreta**: Como su nombre indica, esta clave debe guardarse en secreto y no darse a conocer. La clave privada es la inversa de la pública y puede descifrar información que hayan sido cifrados con la clave pública. Por lo que únicamente B, puede conseguir el contenido de los mensajes cifrados con su clave pública.

En la práctica, se suele escoger un modelo híbrido para realizar las operaciones de cifrado y descifrado. Para ello se genera una clave de sesión (K_s) que se utilizará para cifrar el contenido que se quiere proteger. Esa clave de sesión se cifrará con la clave pública del extremo al que se desea mandar la información. De esta manera, el único extremo que puede conseguir la clave de sesión es el destinatario (ver Figura 6).

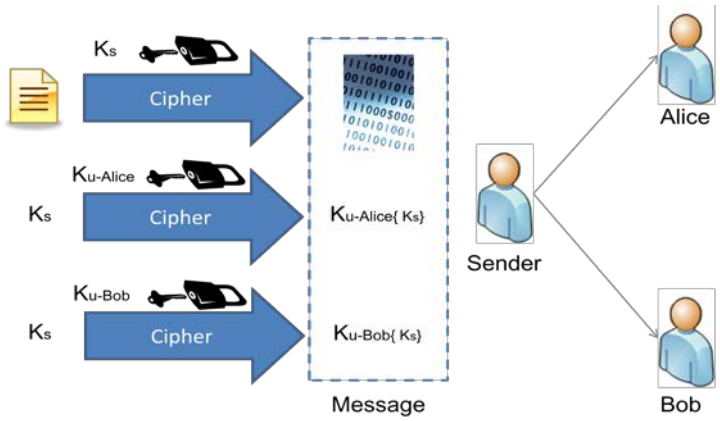


Figura 5. Esquema híbrido de envío o cifrado de ficheros

Una de las ventajas de este enfoque es que no es necesario cifrar el contenido a enviar varias veces en caso de que existan varios destinatarios, teniendo únicamente que cifrar la clave de sesión varias veces con las claves públicas de cada destinatario.

Con arquitecturas de clave pública, también se pueden utilizar servicios de **firma digital**, preservando no solo la confidencialidad de los datos sino también la integridad de los mismos. Un ejemplo de este tipo de soluciones es **GNU Privacy Guard**, también conocido como GPG.

GNU Privacy Guard

GNU Privacy Guard (GPG) es una herramienta capaz de proporcionar cifrado de la información y firma digital con licencia GPL. Podría considerarse, en cierta manera, la alternativa libre al conocido software PGP, que es propietario. El software en su versión nativa utiliza una interfaz de texto, aunque existen ya multitud de programas que utilizan GPG para proporcionar mecanismos de seguridad, como Thunderbird o SeaHorse.

Criptografía de clave pública

El modelo escogido por **GPG** para realizar el cifrado y descifrado de la información es el de criptografía de clave pública. Los comandos utilizados para realizar el cifrado y descifrado de la información son los siguientes:

Cifrado:

```
# gpg –r "key" –encrypt "document"
```

En este caso se generará un documento con extensión .asc, de la forma "document.asc" que habrá sido cifrado con la clave "key". Como se especificó anteriormente, "key" se debe corresponder con la clave pública del receptor.

Descifrado:

```
# gpg "document.asc"
```

En este caso, no hace falta especificar nada más, puesto que la operación que se intenta realizar es el descifrado y por tanto la clave que se debe utilizar es la privada o secreta.

Firma digital

Otra de las funciones que pueden realizarse mediante GPG es la **firma digital**, puesto que utiliza el método de clave pública. De esta manera, cuando se desea realizar una firma digital se utiliza la clave secreta para cifrar una determinada información.

Debido a que la clave secreta no es de dominio público, ninguna otra entidad puede haber «firmado» esa información. El extremo B que recibe la información firmada de A puede comprobar la firma mediante la clave pública A.

Firma:

```
# gpg –s "documentsigned"
```

Cuando se pretende realizar esta operación, debe introducirse una clave para acceder al contenedor de claves. Esta clave se especifica, por el usuario, en el momento de generar las claves públicas y privadas. Una vez introducida se generará el documento «documentsigned.asc» que contendrá la firma digital.

Verificación:

Al descifrar un determinado documento cifrado también se verifica la firma (si ha sido firmado) automáticamente, sin embargo es posible verificar únicamente la firma mediante este comando.

```
# gpg --verify "documentsigned.asc"
```

A nivel de volumen

En contraposición a las soluciones que acabamos de ver, que cifran archivos o carpetas individuales, existe otro tipo de software que cifra volúmenes o unidades de disco completas. Se puede incluso, crear volúmenes ocultos, o «secretos», que se pueden montar como unidades de almacenamiento lógico. Estos volúmenes son en realidad archivos que tienen su propio sistema de archivos y toda la información almacenada en el mismo será protegida.

El ejemplo más representativo de este tipo de software es, sin duda, **TrueCrypt**.

TrueCrypt

Es un software de código libre y gratuito **muy utilizado para cifrar volúmenes completos**. Aunque recientemente, en abril de 2014, se ha generado un gran revuelo tras el anuncio por parte de sus desarrolladores de que abandonaban el proyecto y de que uso ya no era seguro, la comunidad de software ha tomado el testigo y ya están en marcha varios proyectos que seguirán desarrollando este software tan útil y utilizado. A día de hoy, el mejor lugar para descargarlo es la siguiente dirección:

Accede al software a través del aula virtual o desde la siguiente dirección web:
https://www.grc.com/misc/truecrypt/truecrypt.htm

Truecrypt **es un software capaz de proporcionar mecanismos de autenticación y confidencialidad de manera transparente al usuario**. Una vez que se ha instalado el software, las claves utilizadas para cifrar y descifra la información se mantienen protegidas (mediante cifrado) para prevenir el acceso no deseado a las mismas.

En general, existen **dos grandes formas de utilizar este software**:

- **Unidades virtuales:** generadas por el programa, bajo demanda del usuario, con el fin de gestionar la información que se debe almacenar y recuperar de forma segura. Estas unidades virtuales se comportan exactamente igual que los discos duros y pueden ser montadas y desmontadas por el usuario.
- **Contenedor:** los contenedores son un tipo de fichero creado por el programa que pueden ser accedidos a través de una unidad virtual, es decir, «residen» en las unidades virtuales. Esto contenedores almacenan la información de manera cifrada. Cada uno de estos contenedores tiene una clave asociada que deben ser introducida para recuperar la información.

Funcionamiento de Truecrypt

Cuando se realiza una determinada **operación de I/O,** el driver de Truecrypt captura primero todas las peticiones, y decide después si alguna afecta a la unidad virtual cifrada. Si es así, toma el control y lleva a cabo el cifrado o descifrado correspondiente. Si no, deja que sea el sistema operativo quien la realice, sin ningún tipo de intervención por parte de Truecrypt. En la **Figura 7** puedes encontrar un esquema de su funcionamiento.

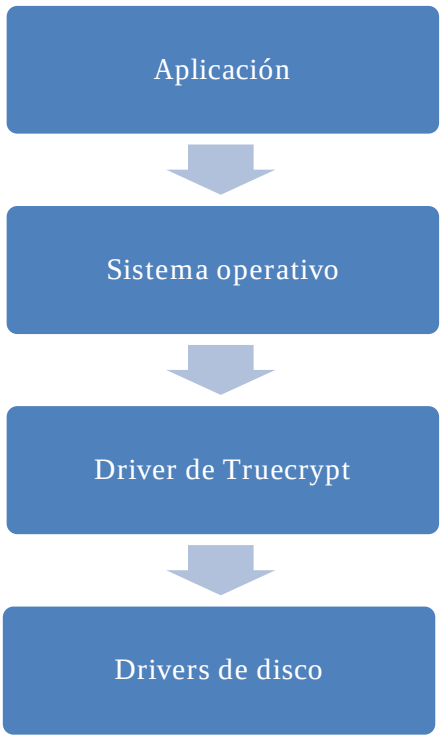


Figura 6. Funcionamiento de Truecrypt

Modo de cifrado XTS

Truecrypt dispone de muchas funciones avanzadas, y una de ellas es el modo especial de cifrado que utiliza por defecto. Se denomina **XTS**, siglas de **XEX-TBC-Stealing**, y fue aprobado en el estándar IEEE 1619 para la protección criptográfica de datos en dispositivos de almacenamiento de bloque en diciembre de 2007.

Está diseñado de forma que permite procesar de manera eficiente bloques consecutivos de información. Su nombre proviene de **Xor-Encrypt-Xor**, ya que su manera de funcionar es mediante dos operaciones Xor. Muy sucintamente, su modo de operación es el siguiente:

$$C_i = E_{k1}(P \,\hat{}\, (E_{k2}(n) \otimes a^i)) \,\hat{}\, (E_{k2}(n) \otimes a^i)$$

Donde:

⊗ Significa la multiplicación de dos polinomios sobre un campo `GF(2) módulo` $X^{128} + X^7 + X^2 + X + 1$

`K1` es la clave de cifrado

`K2` es la clave de cifrado secundaria

`i` es el índice del bloque cifrado

`n` es el índice de la unidad de datos; para la primera unidad de datos, n = 0

`a` es un elemento primitivo del campo de Galois (2^{128}) que se corresponde al polinomio `X`

Los algoritmos que proporciona TrueCrypt para realizar el cifrado de la información son los siguientes:

Algoritmo	Tamaño de clave
AES	256-bit
Twofish	256-bit
Serpent	256-bit
AES-Twofish-Serpent	256-bit; 256-bit; 256-bit
Serpent-AES	256-bit; 256-bit
Serpent-Twofish-AES	256-bit; 256-bit; 256-bit
Twofish-Serpent	256-bit; 256-bit

Pre-Boot Authentication

Otra de las funcionalidades útiles de Truecrypt consiste en que **permite realizar el cifrado de todo el volumen en el que se encuentra un sistema instalado**, como la partición en la que reside el propio sistema operativo. Utilizando esta funcionalidad se puede conseguir un alto nivel de seguridad ya que todos los archivos del sistema, como temporales, ficheros de hibernación, información sobre las aplicaciones ejecutadas, nombres y localizaciones de ficheros, etc., también se mantienen en el sistema protegidos.

Cuando un usuario desea acceder a una máquina asegurada con esta funcionalidad debe teclear la contraseña adecuada antes de que el sistema de carga de *Windows* arranque. Para conseguir esto, TrueCrypt utiliza su propio *Boot Loader*.

Hidden Volume

Como mecanismo de protección adicional, se pueden utilizar los denominados ***volúmenes ocultos***. Este tipo de volúmenes residen dentro de volúmenes convencionales, de forma que a simple vista no pueden ser detectados.

Cuando se crea un volumen, TrueCrypt rellena su espacio con información aleatoria, que posteriormente se irá sobrescribiendo con los datos que se deseen guardar. De esta manera, si se crea un volumen escondido no será posible detectarlo, pues no se sabe dónde acaban los datos y comienza el siguiente volumen.

La clave utilizada para este segundo volumen escondido debe ser completamente diferente a la utilizada para el volumen convencional. Así, si la clave del primero ha sido comprometida, por cualquir motivo, no será posible acceder al segundo.

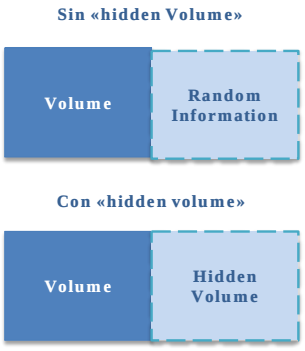


Figura 7. Volúmenes ocultos de Truecrypt

Cifrado de la unidad de intercambio con CryptoSwap

Otra herramienta con una funcionalidad interesante es ***CryptoSwap***, que es **capaz de cifrar la partición de intercambio de *Windows***. La memoria de intercambio es un espacio de memoria reservado para alojar aquellos procesos que no están activos en el sistema o están siendo poco utilizados, para liberar parte de la memoria primaria.

De esta manera, se optimiza el uso de la memoria física para aquellos procesos que realmente la necesitan y el sistema operativo cuenta con una mayor cantidad de memoria, sin embargo, en contrapartida, se pierde velocidad ya que las memorias de intercambio utilizadas son las de almacenamiento (que son mucho más lentas que las primarias o RAM).

Cuando uno de estos procesos es movido a esta zona de memoria, se pueden copiar a su vez parte o la totalidad de determinados documentos sensibles. De esta manera, aunque los documentos se estén almacenando de una manera segura, a la hora de editarlos o leerlos, se pueden estar copiando temporalmente en una región del ordenador que no está protegida y por tanto que es susceptible de ataques.

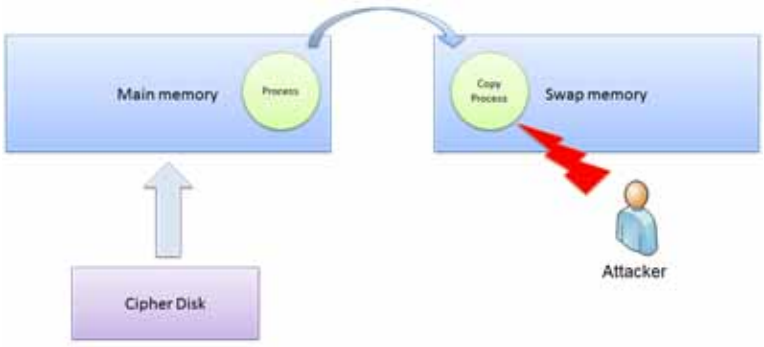


Figura 8. Funcionamiento esquemático de CryptoSwap

Utilizando esta funcionalidad, después de la carga de la memoria de intercambio del sistema operativo, se genera una clave «aleatoria» de cifrado que es única para cada sesión. Esta clave no se almacena y cambia con cada reinicio de la computadora.

6.7. Mecanismos de protección hardware

Las **soluciones hardware** para la protección del almacenamiento externo tienen una ventaja clara, y es su **mayor nivel de seguridad**, **a cambio de un coste mayor**, obviamente. Otra diferencia importante es que generalmente no necesitan de ninguna instalación, ya que se conectan como unidades de almacenamiento convencionales. En contrapartida es una solución menos flexible, ya que el software puede ser instalado en distintos tipos de dispositivos.

Existen diferentes medios de «habilitar» las funciones de cifrado/descifrado de este tipo de dispositivos, por ejemplo mediante contraseñas, USB tokens, Smart Cards, Certificados, etc. Actualmente existe una amplia oferta de dispositivos de almacenamiento que pueden realizar operaciones criptográficas.

Unidades USBs con capacidades criptográficas

Actualmente algunos **dispositivos USB** incorporan **hardware criptográfico y un almacén de claves** para poder almacenar información de manera confidencial. De esta manera, introduciendo algún tipo de credencial, como una contraseña a través de un programa embebido en el USB, se habilita al dispositivo para que acceda a su almacén de claves y cifre/descifre la información que está alojada en el mismo.

Así, las claves utilizadas para realizar las operaciones no son las mismas que para acceder al almacén de claves y se aumentan el nivel de seguridad de la información contenida en el dispositivo (ya que las claves escogidas por los usuarios suelen ser menos robustas que las escogidas por los fabricantes). Los algoritmos y modos utilizados para asegurar la información dependen de cada fabricante.

IronKey

Un ejemplo de unidad USB con capacidades criptográficas es **IronKey**. Utiliza el algoritmo de cifrado AES en modo CBC y tiene un chip especializado en realizar operaciones criptográficas.

Cuando se intenta realizar una manipulación física del dispositivo, éste borra sus propias claves para que los intrusos no puedan acceder a la información alojada en él.

Igualmente, para evitar los ataques de fuerza bruta el dispositivo borra su contenido, de manera segura, cuando se realizan diez intentos fallidos de autenticación.

Figura 9. Unidad USB criptográfica Ironkey

Discos duros con capacidades criptográficas

Al igual que con los USBs, algunos **discos duros** también tiene la capacidad de realizar operaciones criptográficas para almacenar la información de manera segura. De nuevo, el usuario debe autenticarse al disco duro mediante alguna credencial, normalmente una contraseña o token USB.

Existen versiones de discos duros con capacidades criptográficas tanto internos como externos. Veamos algún ejemplo:

- **ArticSoft DiskAssurity.** Se conecta como un disco externo USB. Toda la información que es almacenada en este dispositivo es cifrada de manera transparente al usuario. De igual modo se realiza la recuperación de la información.

  Para poder acceder al contenido del disco, se utiliza un token USB que contiene la clave de desbloqueo del dispositivo (no la clave de cifrado y descifrado).

Figura 10 DiskAssurity

Hardware Security Modules

De todos los dispositivos hardware, los que mayor seguridad ofrecen son los denominados ***Hardware Security Modules*** **(HSM)**. Este tipo de dispositivos no sólo proporcionan seguridad a nivel lógico ante accesos no autorizados, sino que proporcionan un alto nivel de seguridad física.

Figura 11 CryptoSec de la empresa española RealSec

Esto hace que sean muy utilizados en entornos bancarios, como en los sistemas de pagos de con tarjeta. Estos módulos se integran en los cajeros automáticos para cifrar el PIN introducido por el usuario y para realizar las tareas de autorización, como comparar que el **PIN introducido (cifrado)** es correcto frente al mantenido por la entidad bancaria.

Por su parte, las Autoridades de certificación, en entornos de PKI, suelen utilizar este tipo de dispositivos a la hora de generar las claves y almacenarlas.

Por último, también son utilizados para ejecutar determinados módulos que necesitan de un entorno seguro y controlado. Esto módulos pueden ser implementados, por lo general, en lenguajes de alto nivel como .NET, Java o C.

FIPS 140-2

Una de las normas utilizadas para definir cuál es el nivel de seguridad de un determinado dispositivo de almacenamiento es la **FIPS 140-2**, que ha sido especificada por el National Institute of Standards and Technology (NIST) y el Communications Security Establishment (CSE).

Consta de cuatro niveles, siendo el primero el menos exigente y el cuarto el máximo. Los niveles superiores contienen a los inferiores, por lo que extienden las exigencias de éstos:

Nivel 1. Es el nivel de seguridad más bajo. En este nivel únicamente es necesario especificar en el dispositivo algún módulo criptográfico, es decir que proporcione algún algoritmo criptográfico (aprobado por el NIST y el CSE).
Nivel 2: En este nivel, se exige que existan evidencias de intentos de manipulación indebidas. Para ello, se pueden utilizar sellos o revestimientos que deberán ser rotos para acceder físicamente al dispositivo.
Nivel 3. Los dispositivos que cumplen el nivel 3 de protección, son capaces de detectar que están siendo manipulados físicamente y responden ante este tipo de ataques modificando su módulo criptográfico. Por ejemplo borrando sus claves o deshabilitando sus circuitos criptográficos.
Nivel 4. El nivel 4 de seguridad en dispositivos de almacenamiento seguro, no sólo proporciona todas las medidas anteriores, sino que protege su módulo criptográfico ante cambios de las condiciones ambientales normales, como cambios en la temperatura, voltajes, perturbaciones electromagnéticas, etc. Este tipo de dispositivos son útiles cuando se necesitan un altísimo grado de seguridad y el entorno disponible de operación no lo es.

Lo + recomendado

No dejes de leer...

The State of SSL Security

En este documento se explica la importancia de los certificados de seguridad SSL.

Accede al mapa a través del aula virtual o desde la siguiente dirección web:
https://www.nextsense.com/content/Datasheets%20SSL/Whitepaper_The%20State%20of%20SSL%20Security.pdf

El apocalipsis zombi: Heartbleed

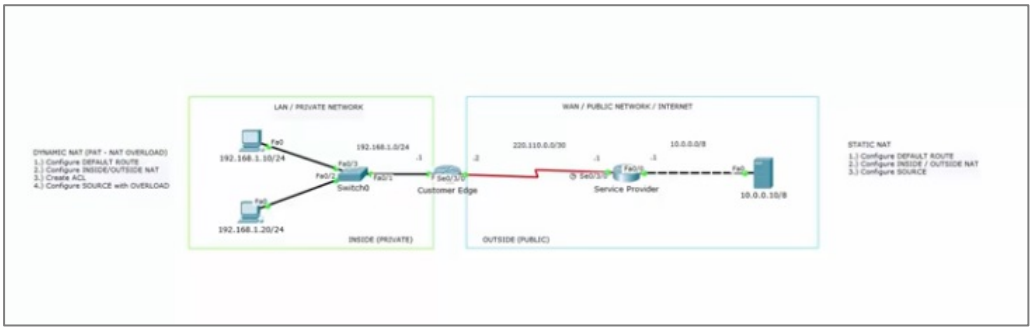
Cualquier persona mínimamente relacionada con la tecnología se haría eco del fallo de seguridad de la librería OpenSSL publicado en Abril de 2014. Aunque no es una vulnerabilidad del propio protocolo SSL, prácticamente todas las implementaciones del mundo hacían uso, en mayor o menor medida, de dicha librería. Lee el siguiente blog que pertenece a INCIBE (Instituto Nacional de Ciberseguridad) y analiza cómo evolucionó el fallo y cómo empezó a corregirse.

Accede al documento a través del aula virtual o desde la siguiente dirección web:
http://www.inteco.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/heartbleed_desmitificado

No dejes de ver...

How to configure NAT in Packet Tracer

En este vídeo se presenta cómo configurar NAT con el software de CISCO Packet Tracer.



Accede al vídeo a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=hGyNiveOlUs

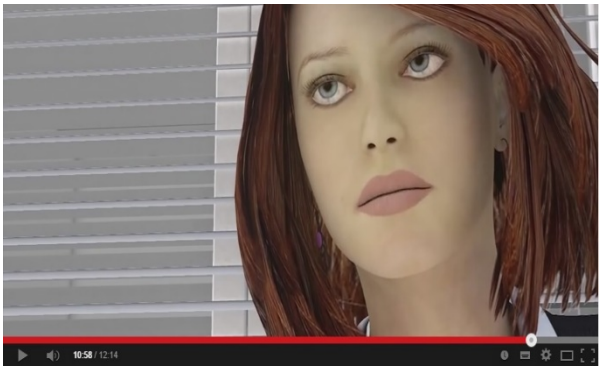
SSL

En esta lección de la Intypedia se presenta una buena introducción, en forma de vídeo, al funcionamiento del protocolo SSL. No dejes de verla como repaso, o para comprobar que realmente has entendido los principales conceptos estudiados en nuestro tema. Además, en el segundo enlace podrás encontrar también de forma visual algunos de los principales ataques a dicho protocolo.

Accede al vídeo 1 a través del aula virtual o desde la siguiente dirección web:
http://www.criptored.upm.es/intypedia/video.php?id=introduccion-ssl&lang=es
Accede al vídeo 2 a través del aula virtual o desde la siguiente dirección web:
http://www.criptored.upm.es/intypedia/video.php?id=ataques-ssl&lang=es

Gestión de claves y tecnología HSM

En este interesante video se analiza otro de los pilares que hemos estudiado en el tema: los HSM. Se presenta el problema de la gestión de claves, presentando un ejemplo real de un HSM llamado *CryptoSign Server* de la empresa española Realsec.



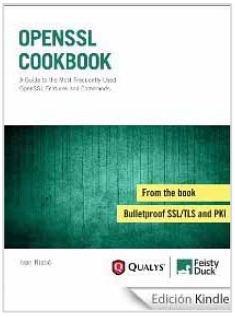
Accede al vídeo 1 a través del aula virtual o desde la siguiente dirección web:
https://www.youtube.com/watch?v=sdgGJ_INIno

+ Información

A fondo

OpenSSL Cookbook

John Viega, J.; Messier, M. & Chandra, P. (2013). *OpenSSL Cookbook*. Feisty Duck. ISBN: 978-1907117053.



Este libro, escrito por el conocido especialista Ivan Ristic, es una descripción exhaustiva de la instalación, configuración y gestión de claves y certificados utilizando la famosa herramienta *OpenSSL*. Incluye además, una guía de buenas prácticas para el desarrollo de aplicaciones que hagan uso de SSL.

Test

1. ¿Qué características tiene la clave criptográfica con la que se cifra la información en el protocolo SSL?

A. Es una clave simétrica fija, que se genera una única vez

B. Es una clave simétrica aleatoria, diferente para cada sesión SSL

C. Se denomina clave de sesión, y es una clave asimétrica aleatoria, diferente para cada sesión SSL

D. Es la clave pública del destinatario

2. ¿Para qué sirve esencialmente el protocolo SSH?

A. Únicamente para ejecutar comandos remotos de forma segura

B. Únicamente para transferir ficheros de forma segura (es una especie de FTP seguro)

C. Habitualmente para ejecutar comandos o copiar ficheros, pero permite canalizar cualquier conexión TCP/IP a través de un canal seguro

D. Para establecer conexiones seguras con un servidor Web remoto

3. Existe una herramienta muy conocida para ejecutar un cliente SSH en entornos Windows. ¿Cómo se llama?

A. Nmap

B. WinSSH

C. PuTTy

D. WinSCP

4. NAT es un mecanismo que sirve para:

A. Es parte del protocolo VPN

B. Traducir direcciones privadas en públicas y viceversa

C. Es el mecanismo encargado del cifrado en las redes privadas virtuales

D. Negociar los parámetros del túnel VPN

5. ¿Puedes asignar la dirección IP 192.168.1.1 a una interfaz pública de un router?

A. No, para una interfaz pública solo se puede asignar 127.0.0.1

B. Sí, si es del rango de la IP asignada por mi ISP

C. Sí, siempre que se utilice NAT en dicho interfaz.

D. No, porque se trata de una dirección pública reservada para uso interno.

6. ¿Cuáles de los siguientes protocolos son de VPN?

A. SSH, PPTP, L2TP e IPSec

B. NAT e IPSec

C. PPTP, NAT e IPSec

D. PPTP, L2TP e IPSec

7. Los protocolos de cifrado de archivos, para su posterior intercambio, ¿qué tipo de esquemas de cifrado suelen utilizar?

A. Esquema de claves simétricas

B. Esquema de claves asimétricas

C. Un esquema híbrido, en el que se genera una clave de sesión simétrica que se cifra con la clave pública del destinatario

D. Un esquema híbrido, en el que se genera una clave de sesión asimétrica que se cifra con la clave simétrica del destinatario

8. GPG es una herramienta de:

A. Cifrado de archivos y carpetas

B. Traducción de direcciones

C. Exclusivamente de firma digital

D. Escaneo de direcciones IP

9. Un HSM es un dispositivo:

A. Software de alta seguridad para el cifrado de archivos

B. Hardware de alta seguridad para el cifrado de archivos

C. Es un disco duro externo con capacidades criptográficas

D. Es un token USB de autenticación

10. Existe una herramienta muy conocida para el cifrado de volúmenes y unidades de disco. ¿Puedes identificarla?

A. GPG

B. CryptoSwap

C. Truecrypt

D. PGP