# Redes Seguras.

[Redes Seguras.](#_tvq6pj529v66)

[Introducción](#_7lp8e4piumrm)

# Introducción

La necesidad de interconexión entre los ordenadores crea, hoy en día un gran número de vulnerabilidades en la comunicación de la información entre ellos.

Ya sabemos que la seguridad informática es cuestión de equilibrio. Las medidas de seguridad deben estar acordes al valor de aquello que se debe proteger.

La configuración de redes siguiendo el esquema de **servidores** y **estaciones de trabajo** nos facilita la administración, pero también permite enfocar los esfuerzos en materias de seguridad.

En este tema, mencionaremos algunas de las medidas que nos ayudan cuando la información está en movimiento... es decir... a través de redes.

La comprensión de los entramados de comunicaciones es compleja, incluso para los especialistas y, lógicamente, queda fuera del alcance de éste tema. Tan solo resaltamos algunas de las medidas de seguridad en red que tenemos disponibles.

# Nivel Físico y enlace

## Redes cableadas

El cable puede ser interceptado físicamente (“pinchado”), y analizado mediante un analizador de tramas o “sniffer”. O bien, puede interponerse un switch y obtener acceso a la red.

En redes cableadas, para hacer esto es necesario acceder físicamente al cable, con lo que es sensato prestar atención al **control del acceso físico** a la red.

**Redes inalámbricas**

En redes inalámbricas, un Punto de Acceso (AP) introduce a las máquinas WiFi en la LAN. Sin embargo, las señales inalámbricas exceden los límites físicos de la organización, de tal manera que desde el exterior se podría acceder a datos de la red.

Hay un protocolo de autenticación, que decide quién puede formar parte de la red, que puede operar de dos maneras.

* **PSK**: Pre-Shared-Key (Clave PreCompartida): para acceder a la red se requiere el conocimiento de una contraseña, igual para cada posible ordenador en la red.
* **IEEE802.1x.** Identificación de cada usuario mediante un servidor **RADIUS** (*Remote Authentication Dial-In User Server)*. Es un servicio que se puede instalar en la red, y que dota a cada usuario de un login y un password para acceder a la red. El control es mucho mayor.

Hay un protocolo de encriptación, para que si se interceptan los paquetes sea difícil su examen.

* **WEP**: Wired Equivalent Privacy. Basado en el algoritmo RC4 con una clave generada a partir de la contraseña. Como ya sabemos, presentaba importantes vunerabilidades. Se puede desescriptar en pocos minutos con análisis criptográfico
* **WPA**: Wi-Fi Protected Access. Es una modificación de WEP, con un variaciones periódicas en la clave (TKIP Temporal Key Integrity Protocol)
* **WPA2**: Supone una solución más segura. Se basa, en principio, en el algoritmo AES, y es un protocolo extensible (preparado para admitir nuevos algoritmos sin modificar el protocolo)

# Nivel RED/TRANSPORTE

## Encriptación de red a red: Redes privadas virtuales.

Ya mencionamos el protocolo IPsec (*Internet Protocol security*). Se trata de un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

Actúa en el nivel de red, y se activa en los **enrutadores**, de tal manera que puede cifrarse toda una ruta entre dos redes, creando así un **tunel seguro** a nivel de red.

Si se activa el protocolo ipsec, toda comunicación de la ruta irá cifrada.

El protocolo IPsec sirve para crear **Redes Privadas Virtuales (VPN - Virtual Private Network).** Una VPN es un montaje en el cual se logra una red segura mediante cifrado, pero en la que realmente los paquetes viajan por una red insegura (como Internet).

El protocolo *de derecho* para lograr ésto es IPsec, pero, no obstante, existen otros que *de hecho* son muy populares, aunque se basan en conexiones de punto-a-punto. Quizá los más utilizados sean [PPTP](http://es.wikipedia.org/wiki/PPTP), y su sucesor, [L2TP](http://es.wikipedia.org/wiki/L2TP), promovidos por Microsoft y algunas otras importantes empresas de comunicaciones.

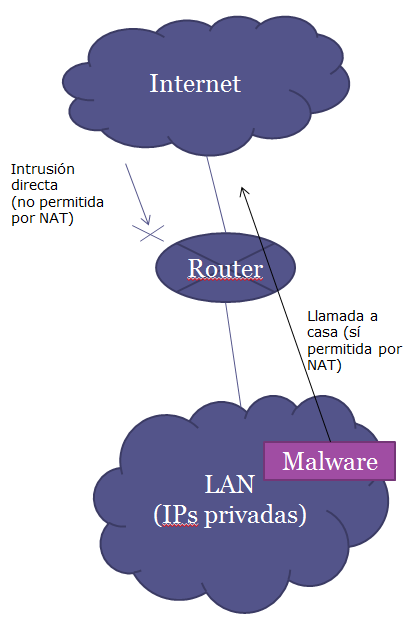
## Firewall

En una red local conectada a Internet a través de un router se produce un curioso fenómeno:

Debido a que las redes locales se montan con IPs privadas, y no es posible un rutado hacia una dirección IP privada desde el exterior (sin utilizar **NAT/PAT**), resulta que no es posible una intrusión desde Internet hacia una IP privada mediante TCP o UDP

El hecho de utilizar IPs privadas se debe al agotamiento de Ips públicas desde 1994.

Eso previene (de manera accidental) ciertos tipos de intrusiones. La situación no será así con IPv6, y NAT/PAT no será necesario. En ese contexto, la participación de los firewall será imprescindible.

Sin embargo, volviendo a la situación actual, sí es posible que desde una IP privada se inicie una conexión TCP o UDP hacia una IP pública.

Así, parte de las intrusiones se basan en la acción previa de MALWARE, que se instale en cualquier equipo de una red, y que realice una llamada a casa.

Un **firewall** es un filtro de comunicaciones. Opera en el nivel de red y de transporte. Es decir, se basa en definir una serie de reglas, que suelen estar basadas en:

* **Direccion IP** del paquete, bien de origen o bien de destino
* **Puerto** del paquete, bien de origen o bien de destino

Existen básicamente dos tipos:

* **En los routers** (cada router tiene el suyo propio). Tambien se les llama “firewall hardware”)
* **En los equipos de usuario** (como el firewall de Windows, o fabricado por otros, como Agnitum, Ashampoo, Symantec, etc.). También se les llama “firewall software”.

Los firewall pueden tener, básicamente, dos modos de funcionamiento:

* En el modo llamado **lista blanca**, en el que NADA se permite, excepto lo que se ponga en la “lista blanca”. Es decir, el firewall impide el paso de cualquier paquete, a menos que cumpla alguna las condiciones que se ponen en la lista blanca.
* En el modo **lista negra**, en el que TODO se permite, excepto lo que se ponga en la “lista negra. Es decir, el firewall permite el rutado de cualquier paquete, a menos que cumpla alguna de las condiciones de la lista negra.

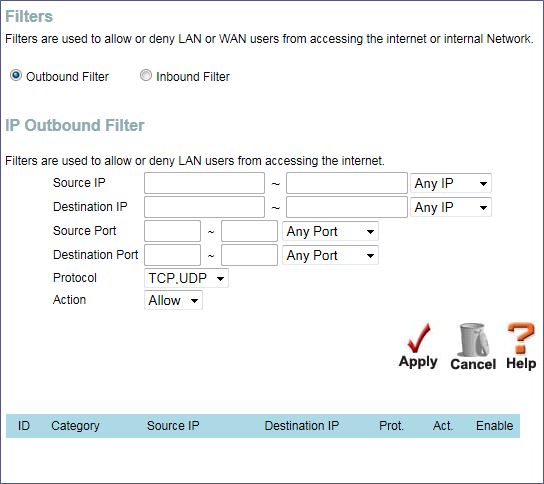
Aunque la mayoría de los routers proporcionan una flexible combinación de listas blancas y listas negras, no todos tienen ambos modos.

### Firewall en router (“por hardware”)

Cada router tiene su propia configuración de firewall. Básicamente, consiste en elaborar una lista blanca o una lista negra basándose en:

* IP de origen o de destino
* Puerto de origen o de destino
* Tráfico entrante o tráfico saliente

La ilustración que sigue es una captura de la configuración de la lista de un router. Se trata de un modo de funcionamiento flexible, en el que se pueden combinar listas blancas y negras. El último desplegable, permite seleccionar las palabras “Allow”, “Deny” (permitir/denegar), y crear listas flexibles.



### Firewall en equipo. (“por software”)

Los firewall en equipo suelen funcionar en modo “lista blanca”. Funcionan por proceso. Eso significa que además de poder establecer un filtrado por IP o puerto, podemos decidir qué procesos (programas) pueden realizar conexiones salientes o aceptar conexiones entrantes.

Cuando tenemos un firewall en el equipo, cualquier conexión saliente o entrante será interceptada por el firewall, que preguntará al usuario si se permite, mediante un diálogo emergente. El firewall recuerda la decisión del usuario.

Algunos firewall no permiten que el usuario tome esa decisión a menos que tenga privilegios de administrador

Éstos firewall están completamente orientados a la utilización de un único equipo, tanto a evitar comunicaciones salientes descontroladas, como a intentos de intrusión desde la misma red.

# Nivel TRANSPORTE/APLICACIÓN

## Protocolo TLS/SSL

Es uno de los más importantes protocolos de seguridad de hoy en día. Ya comentamos su funcionamiento en temas anteriores.

Proporciona transportes seguros entre aplicaciones, basándose en cifrado.

Se utiliza para las versiones *seguras* de protocolos ya conocidos como http (https), ftp (ftps), telnet (ssh), smtp...

La implementación debe estar en los propios clientes y servidores.

El más popular en este momento, es sin duda, https, basado en certificados x509, y la verificación de identidades mediante la PKI.

## Proxy de red

La palabra *proxy*, en informática, es un trozo de software que hace algo en nombre de otro. Refiriéndonos a las comunicaciones, un [PROXY](http://es.wikipedia.org/wiki/Proxy) es un servicio, que, instalado en un ordenador de una LAN permite hacer algo en nombre de otro ordenador de la red. Es una especie de servicio intermediario

Los proxys de red son programas que actúan en el **nivel de aplicación.** Eso significa que conocen y entienden los protocolos de aplicación.

Un determinado producto de tipo proxy maneja una serie de protocolos. Los típicos son:

* HTTP
* FTP
* SMTP
* POP3
* IMAP

Los proxy son un invento del pasado, que no acaba de desaparecer ni acaba de encontrar del todo un lugar permanente.

Incialmente nacieron para acelerar en acceso a las redes. Cuando las redes eran lentas y las páginas web estáticas, ocurria que muchos usuarios de una LAN solicitaban exactamente las mismas páginas. A alguien se le ocurrió que si se pusiera un intermediario en la red que almacenase en un caché las páginas más populares, podría acelerarse en mucho el servicio. Así nacieron los proxy-cache



Los navegadores se configuraban para pedir las páginas al proxy-chache. El proxy, buscaba a ver si tenía la página en su caché, y si era así, la servía localmente. Si no, la pedía al sitio original y la guardaba en su caché durante un tiempo.

Posteriormente, extendiendo la idea del proxy-cache, se crearon otros tipos de proxys:

* proxys que entendían diversos protocolos de aplicación
* proxys que tenían todo tipo de filtros de contenidos
* proxys que discriminaban usuarios, permitiendo que algunos accedieran a unos contenidos y otros no
* proxys con reglas de acceso complejas, basadas en IP, en nombres de dominio, puertos, usuarios...
* proxys que *auditaban* el acceso, registrando los movimientos de cada usuario
* etc, etc, etc.

No obstante, nunca fueron productos con un éxito arrasador. Poco a poco, las empresas que los fabricaban fueron dejando de hacerlo, hasta que hoy en día quedan pocos productos de éste estilo.

### 

### Red con bastión host

Cuando se instala un proxy, es frecuente combinarlo con un firewall, ya que si no es así, pierde parte de su seguridad.

La configuración con *bastión host*, típica de seguridad en LAN pasa por la activación del firewall de router y la instalación de un servidor proxy en la red:

* Se instala el servicio proxy en un servidor.
* En el firewall del router se prohibe la salida desde cualquier IP de la LAN, excepto de la IP del servidor del proxy.
* Se configuran los clientes en las estaciones de trabajo para que utilicen el proxy.
* Con ésta configuración, cualquier petición de una estación de trabajo será dirigida al proxy.
* El proxy la realiza en su nombre y devuelve los resultados.
* Se pueden establecer controles adicionales de seguridad en el proxy.

Esta combinación, permite un control casi total sobre las comunicaciones salientes, ya que todas deben pasar por el PROXY.

Tiene varias utilizaciones típicas:

* Se desea control sobre las comunicaciones salientes
* Se desea registrar (auditar) el acceso a las comunicaciones
* **Evita la llamada a casa del malware.**



#### Single-homed bastion host

Es un dispositivo con una interfaz única de red, frecuentemente se utiliza para una puerta de enlace (gateway)en el nivel de aplicación. El router externo está configurado para enviar los datos al Bastion Host y los clientes internos enviar los datos de salida al host. Finalmente el host evaluará los datos según las directrices de seguridad.

#### Dual-homed bastión host

Es un dispositivo que tiene al menos dos interfaces de red. Sirve como puerta de enlace al nivel de aplicación y como filtro de paquetes. La ventaja de usar este host es crear una ruptura entre las red externa e interna, lo que permite que todo el tráfico de entrada y salida pase por el host. Este host evitará que un atacante intente acceder a un dispositivo interno.

### 

### 

### 

### El protocolo SOCKS

En aquellas redes en las cuales se instala un proxy, es posible que algunos programas no utilicen un protocolo estándar, y sin embargo, queramos que sobrepasen el proxy.

Por ejemplo, los programas de chat y/o comunicaciones, como Live Messenger o Skype son un ejemplo típico: utilizan protocolos de aplicación propios, que ningún proxy puede implementar.

Para que estos programas puedan utilizar un proxy el protocolo genérico de proxy: SOCKS, siempre y cuando el cliente y el proxy lo soporten.

SOCKS es un protocolo de encapsulación... permite enviar paquetes al proxy dirigidos a un servidor del exterior, junto con instrucciones para el proxy, de cómo enviarlos a su destinatario y cómo recoger la respuesta.

Más: SOCKS en wikipedia... [en inglés](http://en.wikipedia.org/wiki/SOCKS), y [en español (muy escueto)](http://es.wikipedia.org/wiki/SOCKS)

### Red con Zona Desmilitarizada (DMZ / Red perimetral)

En seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ solo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de correo electrónico, Web y DNS. Y es precisamente estos servicios alojados en estos servidores los únicos que pueden establecer tráfico de datos entre el DMZ y la red interna, por ejemplo, una conexión de datos entre el servidor web y una base de datos protegida situada en la red interna.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall).

