

Diseño de redes seguras.

Caso práctico



[Linux Screenshots \(CC BY\)](#)

Las necesidades de comunicación acuciantes de las que disponen los sistemas de control actuales, con multitud de dispositivos interconectados, incluyendo aquellos pertenecientes al IoT, traspasos de información continuos entre el mundo corporativo y el industrial, los servicios en la nube o los accesos de los fabricantes para mantenimientos o cambios de programación, han hecho que los diferentes dispositivos que componen la industria se hayan

conectado para favorecer estas funcionalidades. El problema surge porque estas conexiones se han realizado siguiendo criterios de necesidad, y no mediante un estudio completo de la red y las posibilidades de crecimiento. Ahora toca arreglar esos problemas, creando una arquitectura de red que sea segura, dimensionada y escalable para cada sistema de control, o reformando la actual para mejorarla y que cumpla con estas características.

Objetivos:

A lo largo de esta unidad, el alumno estudiará diferentes tipos de tecnologías y soluciones de seguridad que se han desarrollado para implementar confianza sobre redes inalámbricas o para establecer canales seguros desde redes inseguras como Internet.

Además se explicarán las soluciones IDS e IPS, enfocadas a identificar y contener amenazas tanto en las redes como en los sistemas.

1.- Seguridad en redes inalámbricas.

Caso práctico

Manuel y Loli viven en un chalé y desde hace unas cuantas semanas, notan que la conexión wifi les va muy lenta. Paco, un amigo que tiene conocimientos avanzados en informática les dice que les visitará próximamente y aprovechará para echar un vistazo. Cuando Paco accede al router, comprueba que el cifrado que usa la red wifi es WEP y además, tras ver los logs del router identifica conexiones de otros equipos que no son ni de Manuel ni de Loli. En definitiva, les estaban robando la conexión.



En los últimos 30 años, hemos pasado de comunicaciones casi exclusivamente a través de cable, a estar conectados a través de tecnologías inalámbricas. Sin duda, la comodidad de disponer de una posibilidad donde pueda eliminarse parte del medio físico como son los cables, dotan de gran versatilidad, comodidad y libertar a los usuarios. Hoy en día apenas se concibe llevar a cabo una comunicación con necesidad de un cable. Se puede decir que estamos en una época donde predomina lo “Wireless” (sin cable). Ya casi nadie imagina en su hogar la necesidad de implementar una LAN, para conectar dispositivos, de hecho los más jóvenes pensarán que es una locura. Hoy todo se conecta por el “aire”. Pero es esta característica lo que hace a las redes inalámbricas inseguras.

Pensemos que el canal por el que se transmite la información, está accesible a todo el mundo. Cualquiera con un dispositivo adecuado y los conocimientos necesarios, será capaz al menos de conectarse o inspeccionar la información de una red wifi o bluetooth, por ejemplo. Cuestiones un poco más específicas se necesitarían para vulnerar la seguridad del 4G o 5G, pero nada es imposible, y en ciberseguridad menos.

En este punto, nos centraremos en la seguridad de las redes inalámbricas y en particular, en las redes wifi sobre las que exploraremos la evolución en sus protocolos y los niveles de seguridad hasta nuestros días.

1.1.- Conceptos básicos.

Antes de conocer cuáles son los riesgos y cómo hacer frente a los problemas de las redes wifi, es necesario conocer algunos conceptos:

Cobertura, canales y SSID

Es importante saber que, en este tipo de redes, existe una limitación con el radio de cobertura. En interiores suele ser de unos 20 metros y esta distancia es mayor al aire libre que puede llegar a ser de cientos de metro si las condiciones lo permiten.

Otro elemento importante, es la potencia de la señal que en el caso de las redes wifi se va a medir en mili vatios. A mayor potencia, también mayor alcance. El tipo de receptor o antena que tengamos también influirá en la cobertura, incluso podemos usar antenas alimentadas eléctricamente para ganar varios kilómetros de cobertura.

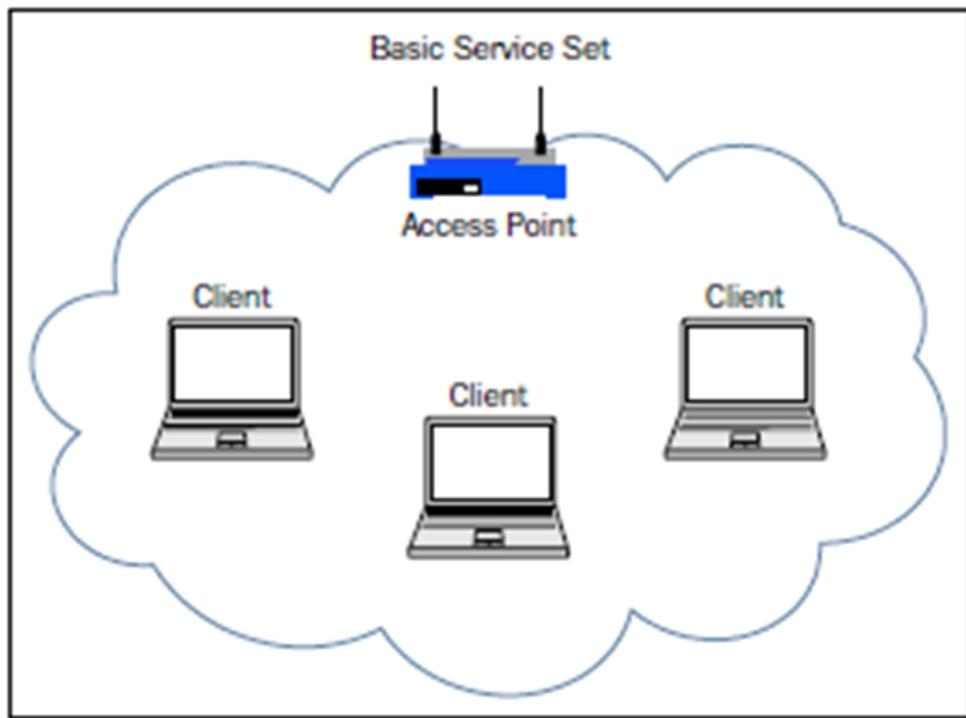
En interiores, si se usa la banda de 2,4 Ghz la señal wifi se extenderá más pero será menos veloz, y si usamos la de 5 Ghz, tendrá menos alcance pero la conexión será más rápida. En relación con esto, los puntos de acceso pueden ser configurados para que la señal wifi que se transmite se lleve a cabo a través de diferentes canales que pueden ir del 1 al 17 en función de las características del dispositivo. En realidad esta función es para mejorar la transmisión evitando contaminación por otros dispositivos o señales en las bandas que se estén usando.

El SSID (Service Set Identifier) es el nombre de la red wifi. Los puntos de acceso (routers inalámbricos) “anuncian” su red continuamente, permitiendo a los clientes listar las redes disponibles. Es posible encontrar redes “ocultas” que no anuncian de forma activa su SSID, pero hay que destacar que no es una medida de protección aunque antes así se pensara.

BSS

O Basic Service Set, se trata de la configuración normal/habitual. Un punto de acceso al que se conectan varios clientes. De cara a los que veremos posteriormente, en este tipo de configuraciones hay que tener en cuenta que están formadas por:

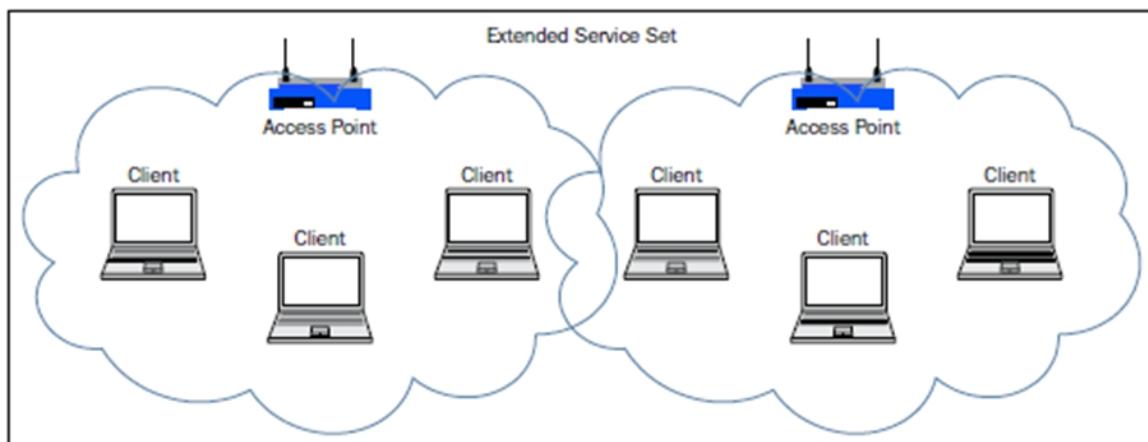
- El SSID: visto en el punto previo.
- El BSSID: O Basic SSID que es la [MAC](#), o dirección física del punto de acceso (AP).



BSSID (Dominio público)

ESS

O Extended Service Set: se trata de la configuración que contempla más de un punto de acceso para crear la conexión. En este tipo de configuraciones hay que tener en cuenta que existirá el ESSID (Extended SSID), similar al SSID pero con la diferencia de que puede haber varios puntos de acceso con diferentes SSID que forman parte del de este tipo de infraestructura. Este tipo de redes wifi son las que se despliegan en ciudades, universidades, aeropuertos, y en menor medida en empresas con gran extensión.



ESSID (Dominio público)

Modos

- **Infraestructura:** se trata del modo más común de implementación. Este tipo de red es generada por los propios router wifi o puntos de acceso. Es la que podemos encontrar en los hogares, empresas y ciudades.
- **Ad-hoc:** también se conoce como modo "peer-to-peer". Las redes ad-hoc no requieren un punto de acceso centralizado. En su lugar, los dispositivos de la red inalámbrica se conectan directamente entre sí. Hay dispositivos que son compatibles con este modo pero casi el 100% son compatibles con el modo infraestructura.

Frames

1. **Management frames:** conocidos como paquetes de gestión estos son responsables de mantener la comunicación que está presente entre el punto de acceso y el cliente asociado a él. Alguno de sus subtipos:
 - Beacon frame
 - ATIM frame
 - Probe response
 - Probe request
 - Disassociation frame
 - Association Request frame
 - Association Response frame
2. **Control frames:** paquetes de control, estos son responsables de un intercambio adecuado de información (Data) entre el punto de acceso y los clientes asociados. Tiene varios subtipos:
 - CTS: Clear to Send
 - RTS: Request to Send
 - ACK: Acknowledgement frame
3. **Data frames:** son paquetes con información. Son los más importantes cuando uno está tratando de descifrar la contraseña encriptada por algún tipo de cifrado en particular WEP, ya que dichos paquetes contienen toda la información que se envía a través de nuestra red wifi.

A la hora de llevar a cabo tanto una auditoría como un ataque a un red de estas características, hay que centrarse en los beacon frames, los probe request y los probe response. A través del análisis de estos paquetes se podrá obtener información como:

- SSID
- Tipo de cifrado
- Canal
- MAC
- Información del fabricante

Hasta que surgieron estas normas que se acaban de enumerar, se tomaba como referente la norma [RFC 3227](#): Directrices para la recopilación de evidencias y su almacenamiento. Dicha guía muestra las mejores prácticas para determinar la volatilidad de los datos, decidir qué recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados con la parte legal.

Es una guía que data del año 2002. A pesar de su antigüedad, de ella suele tenerse muy presente su apartado 2.1 sobre el orden de volatilidad.

AUTOEVALUACIÓN

Los dos modos de infraestructura que involucran puntos de acceso más habituales en las redes wifi son:

- BSSID y ESSID
- ESIDS y Ad-hoc
- Ad-hoc y BSIDS

1.2.- Debilidades en las redes wifi.



[inaara](#) (Dominio público)

Ya lo dejamos entrever al comienzo de este punto. En una infraestructura cableada, acceder a la red requiere de un acceso físico: es necesario conectarse mediante un cable Ethernet RJ-45. Esta seguridad física impide el acceso a personas no autorizadas. Con la aparición de las redes inalámbricas, surgió la necesidad de protegerse frente a accesos no autorizados: al no existir una protección física, cualquier persona que disponga de una antena Wi-Fi podría conectarse a la red.

Normalmente, cuando se adquiere un router wifi o punto de acceso, es habitual encontrarse el dispositivo configurado sin cifrado (o con una configuración por defecto) y sin control de acceso a la red, lo cual podría ser totalmente inseguro.

Debemos contemplar desde el punto de vista de la seguridad tanto el cifrado empleado en el intercambio de información, como el control de acceso a la red inalámbrica. Además, cualquier usuario que se pueda conectar y autorizarse en una red wifi, podría espiar el tráfico que se genera en la misma.

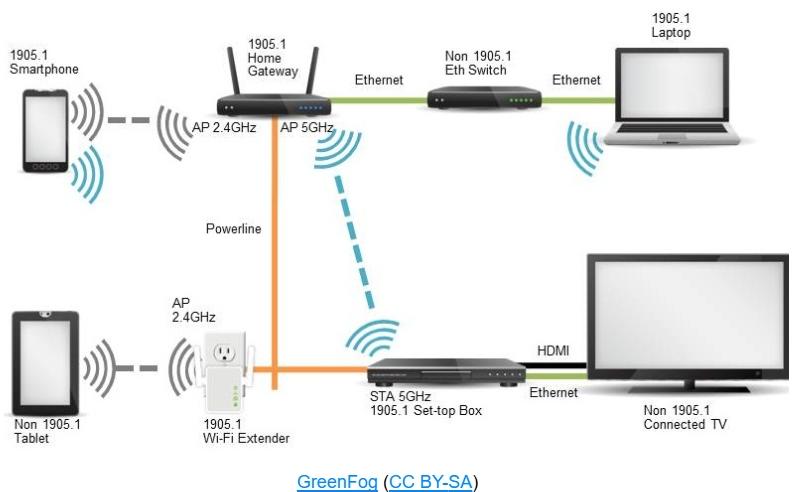
Desde sus inicios, una de las medidas más interesantes a la hora de establecer seguridad en una wifi, era el filtrado por MAC. En la actualidad y desde hace años, ese mecanismo, aunque recomendable su implementación, resulta ineficaz para “usuarios con conocimientos avanzados” ya que es posible evadirlo de una manera muy sencilla, simplemente modificando la MAC desde un sistema operativo Linux con la aplicación [macchanger](#).

1.3.- Vulnerabilidades en protocolos wifi.

Debido a la naturaleza de las redes inalámbricas, es fundamental que las comunicaciones se cifren. Si la comunicación se lleva a cabo en claro, cualquiera puede interceptar la comunicación y ni siquiera ser detectado. Existen varios protocolos de cifrado wifi, pero no todos ellos son seguros, algunos tienen debilidades conocidas y son fácilmente atacables.

Los protocolos de cifrado existentes son los siguientes:

- [WEP](#) (Wired Equivalent Privacy). (1999)
- [WPA](#) (Wi-Fi Protected Access). (2003)
- [WPA2](#) (Wi-Fi Protected Access 2). (2004)
- [WPA3](#) (Wi-Fi Protected Access 3). (2018)



[GreenFog \(CC BY-SA\)](#)

WEP

El objetivo del sistema Wired Equivalent Privacy (WEP, “Privacidad Equivalente a Cableado”) es proporcionar a una red inalámbrica una seguridad equivalente a la de una red cableada. Esto se consigue sustituyendo el componente de seguridad física por la necesidad de una contraseña. Es importante señalar que el sistema WEP no protege de escuchas de tráfico realizadas por usuarios ya conectados. Este hecho ya existe en una red cableada: un usuario malintencionado que consiga acceso físico a la red puede “esnifar” el tráfico de datos emitido por los otros usuarios si no existe ninguna medida de seguridad adicional.

Hoy en día, el cifrado WEP no se considera seguro al existir ataques sencillos que permiten obtener la clave rápidamente sin necesidad de emplear fuerza bruta. En cambio, WPA y WPA2/3 se consideran seguros al no existir todavía ataques criptográficos sencillos.

Para crackear una red de estas características basta con conseguir una cantidad suficiente de paquetes para obtener la contraseña.

WPA, WPA2 y WPA3

WPA (Wi-Fi Protected Access), a diferencia de WEP, utiliza un vector de inicialización de 48 bits y una clave de cifrado de 128 bits. Lo más importante, es que WPA, utiliza lo que se llama el Protocolo de integridad de clave temporal (TKIP). Considerando que WEP usa la misma clave para cifrar todos los paquetes que fluyen a través de la red, WPA con TKIP, cambia la clave de cifrado cada vez que un paquete se transmite.

WPA2 es la versión certificada del estándar de la IEEE de WPA con algunas actualizaciones como el uso de cifrado AES.

¿Que es TKIP y AES?

TKIP y AES son dos tipos diferentes de cifrado que pueden ser utilizados en una red WiFi. TKIP significa “Protocolo de integridad de clave temporal”. Fue un protocolo de encriptación provisional introducido con WPA para reemplazar el cifrado WEP, el cuál se veía muy afectado por la inseguridad en el momento, aunque TKIP es en realidad muy similar a WEP.

AES (Advanced Encryption Standard) es un protocolo de cifrado más seguro introducido con WPA2, que reemplazó el estándar WPA. AES no es una norma creada específicamente para redes Wi-Fi, es un estándar de cifrado usado globalmente. AES se considera generalmente muy seguro, y la principal debilidad sería un ataque de fuerza bruta, el cuál se puede impedir usando una contraseña muy segura.

El “PSK”, en ambos casos, significa “llave pre-compartida”, que es generalmente la frase de cifrado. Esto lo distingue de WPA-Enterprise, que utiliza un servidor RADIUS, que crea de forma aleatoria claves únicas en redes corporativas o gubernamentales, WiFi más grandes.

Para crackear la contraseña de una red WPA, será necesario utilizar un diccionario o llevar a cabo un ataque de fuerza bruta sobre la captura del paquete denominado [4wayHandshake](#). Si la contraseña es muy robusta, las probabilidades de éxito se verán notablemente reducidas.

WPS

La seguridad de las redes inalámbricas ha evolucionado y mejorado mucho desde la implantación del cifrado WPA, y sobre todo, WPA2 y WPA3. Con WPA sabemos que nuestra red utiliza un método de cifrado seguro, pero... ¿quién no se ha visto en la siguiente situación?

Llegas a casa con tu portátil recién comprado y cuando lo estás configurando para que tenga acceso a tu red inalámbrica... no te acuerdas de cuál es la contraseña de acceso a la red. ¿Cuál era la contraseña? ¿La has cambiado últimamente? ¿La tienes apuntada en algún sitio? Y si no la recuerdas... ¿tienes la dirección IP del router y las credenciales para conectarte a su página de administración y averiguarla? Para esta cuestión, los routers inalámbricos han evolucionado con el objetivo de hacernos la vida más cómoda. Y con esta idea en mente, incorporan funcionalidad llamada WPS o WiFi Protected Setup. El WPS es un mecanismo creado para facilitar la conexión de dispositivos a nuestra WiFi. Existen varios métodos pero el más extendido y que a su vez es el que se usa en las redes domésticas, es el intercambio de PIN.

Si nuestro router tiene habilitada la funcionalidad WPS y queremos acceder a nuestra WiFi, simplemente tenemos que enviarle un código PIN de 8 dígitos para que el router nos permita acceder a la red inalámbrica. Inconveniente: el tiempo que un atacante necesita para averiguar un PIN de 8 dígitos es mucho menor que el que necesita para averiguar la contraseña WPA2/3 configurada en la red.

Existen aplicaciones como [reaver](#) que pueden llevar a cabo ataques contra este tipo de servicios pero también hay que señalar que muchos router cuentan con medidas de protección para evitarlo.

Para saber más

Puedes complementar esta información con la disponible en el seminario web de [seguridad wifi](#) de INCIBE.

1.4.- Ataques a redes wifi.

Como podemos inferir, atacar una red wifi es relativamente sencillo y si además el atacante está autorizado, podrá realizar más ataques. Los más interesantes:

- Man in The Middle: se trata de un tipo de ataque donde un usuario autorizado en la red podrá capturar el tráfico que discurre si no va cifrado. Las redes Wifi son un “caldo de cultivo” estupendo para poner a prueba las labores de auditoría o de ataque. Al igual que ocurre con las redes cableadas, las wifi están sujetas a este tipo de ataques pero además, gracias a que el canal es abierto, están mucho más expuestas a los usuarios. Derivados de este tipo de ataque, se pueden realizar suplantación de MAC, suplantación de servidor [DHCP](#) y un largo etcétera.
- Falsificación de puntos de acceso: del mismo modo que podemos suplantar la MAC de un cliente, es posible hacerlo de un router con las consecuencias que ello supone.
- Denegaciones de servicio: resulta realmente sencillo llevar a cabo un ataque de estas características sobre un punto de acceso que no tenga funcionalidades que protejan frente a este tipo de ataques.
- Deautenticación de usuarios: con diversas herramientas, es posible que usuarios que están conectados a un router wifi, sean desconectados por un atacante.



Andrés Rubio - Elaboración propia (Dominio público)

AUTOEVALUACIÓN

Los ataques que afectan a la funcionalidad WPS se llevan a cabo a través de qué aplicación:

- Reaver
- Pixie Power
- Ninguna. El protocolo es robusto ante cualquier ataque

2.- Soluciones DLP.

Caso práctico



[Richard Patterson \(CC BY\)](#)

Luis y Sara son los gerentes de una empresa que se dedica a producir galletas y productos derivados. Desde hace unos cuantos meses, llevan trabajando en un nuevo producto que creen que va a dar mucho que hablar. La sorpresa de ambos es mayúscula cuando han comprobado que una empresa de la competencia acaba de sacar al mercado, un bollo similar al que habían desarrollado ellos. ¿Qué es lo que ha ocurrido? ¿Algún empleado habrá robado la información?

Según la definición más extendida en Internet “*un DLP (prevención de pérdida de datos, por sus siglas en inglés) es el conjunto de herramientas y procesos utilizados para garantizar que los datos confidenciales de una empresa no se pierdan, se utilicen de forma inapropiada o puedan acceder a ellos usuarios no autorizados*”

Uno de los mayores riesgos de una organización es la pérdida de su información a través de las fugas de datos: empleados descontentos, extorsión, almacenamiento de la información fuera de la infraestructura de la organización, etc. Como se ha repetido por activa y por pasiva, la información en uno de los activos más importantes de las compañías, ya que es el valor que se genera con los proyectos de investigación y desarrollo entre otros. Además, en la actualidad con la gran cantidad de servicios para el almacenamiento en la nube existentes, puede ser relativamente fácil exfiltrarla si los administradores no han tomado las medidas adecuadas.

De ahí que muchas compañías clasifiquen su información por la importancia que tiene para ellos en función de su criticidad e impacto ante la pérdida de esta. Las herramientas para este propósito suelen estar basada en el marcaje de documentos conforme al nivel de clasificación de la información, pero esto representa un trabajo de partida elevado, y para su continuidad una colaboración de los usuarios en el marcaje de la información.



[OpenClipart](#) (Dominio público)

Otra herramienta complementaria es el IRM (Information Resource Management) en el que la información se puede gestionar en base a destinatarios, tiempo de vida o cuándo debe ser destruida que se puede complementar con la vigilancia de la información basada en comportamientos de los usuarios con respecto a los movimientos que realizan:

- Descargas masivas de documentos
- Permisos sobre nuevas carpetas
- Falta de recertificación de permisos en las carpetas.

Estas herramientas están basadas en la necesidad de conocer de los usuarios, revisión de permisos sobre la información (recertificación), mínimo privilegio, control y vigilancia. Como decíamos al comienzo, la difusión del perímetro a servicios en la nube ha incrementado estos riesgos, ya que muchos usuarios disponen de mecanismos para poder almacenar la información en repositorios que se encuentran en la nube, y a los dispositivos BYOD que permiten traspasar información entre ellos con las diferentes alternativas que tienen cada uno (wifi, usb, tarjetas de memoria, ...).

Incluso la pérdida de información puede estar asociada a delitos penales o sanciones administrativas, que pueden derivar en juicios. La prevención de fugas de información puede conseguirse en base a una herramienta como un DLP o en base a una serie de políticas de seguridad, pero sin ayuda de la tecnología, esta última medida podría ser insuficiente.

Ventajas de un DLP

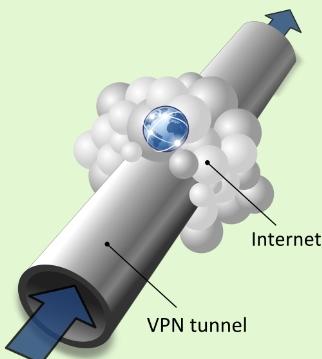
Sin duda este tipo de soluciones cuenta con una serie de características que les hacen ideales para proteger los datos entre otras cosas. Destacan:

- Identificación de amenazas tanto internas como externas: este tipo de herramientas actúa en ocasiones como una solución antimalware en compañía de un cortafuegos. A través de la configuración de directivas y políticas, es posible parametrizar estas herramientas para evitar tráfico no esperado o la exfiltración de información no autorizada.
- Se alinea con el cumplimiento normativo: en Europa y en España las organizaciones están sujetas a cumplir leyes relacionadas con la protección de datos de carácter personal. Estas herramientas a través de las soluciones que incorporan, facilitan dicha labor y proporcionan mecanismos de protección para garantizar la seguridad de ese tipo de datos.
- Segregación de roles para evitar el envío de información: un DLP no permitirá la transferencia de determinados tipos de archivos o documentación sin la autorización pertinente. Esto se consigue a través de la implementación de credenciales o sistemas que garanticen la autorización.

Habitualmente este tipo de soluciones son provistas por fabricantes desde una perspectiva comercial, no obstante, también es posible encontrar soluciones Open Source que, a pesar de no contar con toda la funcionalidad, pueden ser válidas para determinado tipo de empresas. Se puede encontrar un listado de estas en el siguiente enlace: <https://heimdalsecurity.com/blog/open-source-paid-data-loss-prevention-dlp-solutions/>

3.- Redes Privadas virtuales y túneles.

Caso práctico



[OpenClipart](#) (Dominio público)

Mari Carmen va a abrir una nueva oficina en una localidad próxima a donde tiene la sede central. Apenas la separan 23 kilómetros y la gustaría que ambas estuvieran conectadas a la red de tal modo que de manera lógica, pareciera una única infraestructura. Mari Carmen ha valorado la conectividad directa mediante enlace físico, pero se le va del presupuesto. Un compañero de carrera, le ha recomendado el uso de una VPN que además de mucho más barato, también es muy seguro.

Los problemas de seguridad derivados de la expansión de internet y la falta de implementación de medidas técnicas de seguridad en el desarrollo de los protocolos en el momento de su aparición han propiciado que a lo largo de las últimas décadas, se vengan evolucionando dichos protocolos o añadiendo funcionalidades que les doten de robustez frente a las posibles amenazas a las que se exponen.

Con la democratización de Internet, las soluciones que se empleaban y que tenían un coste elevado, fueron quedando relegadas en pro de tecnologías que surgían para dar respuesta a cuestiones relacionadas con la seguridad en las comunicaciones. Las organizaciones querían seguridad pero las conexiones de Internet no eran confiables. En este sentido las soluciones que aparecieron trataron de dar respuesta a este problema. El diseño era sencillo, usar un canal inseguro como es Internet para establecer un canal seguro por el mismo. Surge entonces el concepto de túneles y/o redes privadas virtuales (VPNs).

Qué es una VPN y para qué sirve

Tal y como se ha comentado en la introducción, se trata de la implementación de una red privada y segura sobre red pública y no segura que es Internet. Esto se consigue proporcionando o construyendo un túnel IP cifrado y/o encapsulado a través de la Red. El tipo de encapsulado que emplea, ha de estar permitido en la red pública, transportando por esta paquetes de la red privada y que en ningún caso serán accesibles por terceros salvo vulnerabilidad o problema con el certificado empleado.

Es importante que una vez que se establece la conexión con el servicio de VPN, el direccionamiento IP será independiente del de la red pública, pasando a formar parte del direccionamiento privado de la organización. Esta función permite a los clientes que se conecten ser un equipo más de la red corporativa, interna, o cualquiera para la que se ha implementado. La implementación de este tipo de redes conlleva un requerimiento de seguridad que habitualmente puede ser una encriptación con IPSec o protocolo más evolucionado.

Tal y como hemos avanzado anteriormente, se pueden hacer servir como una extranet de tal modo que podremos acceder a todos los servicios de la empresa para los que tengamos autorización. Es habitual que muchas organizaciones usen este tipo de conexiones para permitir el acceso a la red interna de aquellos empleados en itinerancia.

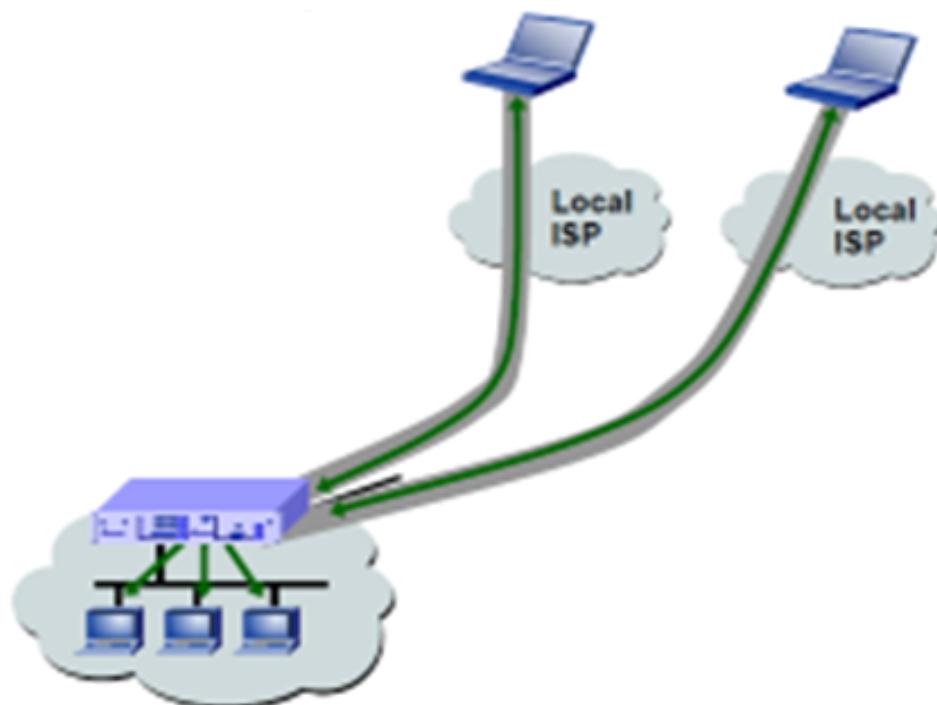
En función de cómo estén implementadas, se puede decir que son más seguras que una extranet convencional y permite conectar diferentes delegaciones o sedes de una empresa, simulando una red local de una manera transparente y económica, permitiendo el acceso a clientes, socios y consultores a los diferentes recursos de la red de forma remota.

Hoy en día también encontramos utilidad en los servicios de VPN con un propósito diferente y que nada tiene que ver con el profesional. Nos estamos refiriendo a saltarse las restricciones geográficas para el acceso a servicios que no están disponibles en nuestro país.

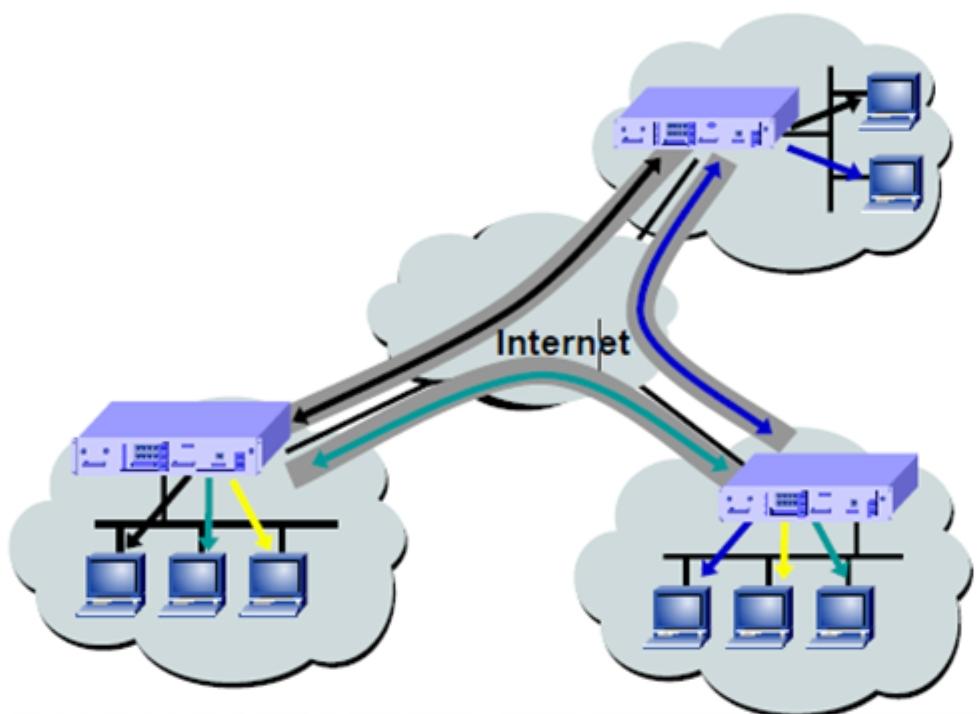
Tipos o modos de enlace

Existen dos modos principales para el establecimiento de las conexiones vía VPN:

- Enlace Cliente - Red: El cliente se conecta remotamente a una LAN. Se usa [PPP](#) para establecer una conexión entre el cliente y la LAN.
- Enlace Red – Red: Se encapsula el tráfico de una red local. Nos ahorraremos el paso PPP (el tráfico se encapsula directamente).



Cliente - Red (Dominio público)



Red- Red (Dominio público)

Aspectos técnicos (tunneling)

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red. El establecimiento de dicho túnel se implementa incluyendo un PDU (Unidad de datos de protocolo) dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera los paquetes de datos se transportan sobre Internet y nadie salvo el emisor y el receptor, serán capaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado que, entre otros, podría ser SSH, IPSec, etc.

Básicamente se añade una cabecera IP adicional (cabecera del protocolo de transporte) al paquete original para que éste pueda circular a través de Internet hasta el router de la empresa corporativa donde es eliminada. El router que permite accesos vía tunel a una red privada se denomina servidor de túneles.

IPSec

A nivel técnico, los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo [OSI](#). Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, que son los protocolos más usados. Una ventaja importante de IPsec frente a SSL y otros métodos que operan en capas superiores, es que 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 realizar modificaciones sobre su implementación.

IPSec es bastante flexible en tanto que permite seleccionar protocolos de seguridad, algoritmos que se van a utilizar y las claves requeridas para dar estos servicios. Algunos de los servicios de seguridad que proporciona:

- Control de acceso: incluso mediante infraestructura PKI.
- Integridad: a través del control del flujo de las transmisiones.
- Autentificación del origen de los datos
- Confidencialidad: mediante el encapsulado.

Un dato interesante es que la implementación de IPSec en el origen de IPv6 era obligatorio, pero tras el cambio en 2011 se convirtió en una característica recomendable pero opcional.

Ventajas e inconvenientes

Ventajas

- Ahorro en costes: al emplear Internet como canal, la economización para establecer conexiones privadas es muy económico.
- No se compromete la seguridad de la red empresarial al desarrollarse la comunicación por un canal completamente privado.
- El cliente remoto adquiere la condición de miembro de la red corporativa con todas las medidas de seguridad que conlleva: permisos, directivas de seguridad, políticas, etc.
- El cliente tiene acceso a todos los recursos ofrecidos en la red corporativa incluyendo servicios como impresoras, correo electrónico, base de datos, etc.
- Acceso desde cualquier punto del mundo siempre y cuando se tenga acceso a una conexión a Internet.

Inconvenientes

- No se garantiza disponibilidad. Si no tenemos conexión a internet no dispondremos del canal.
- No se garantiza el caudal y estaremos sujetos a la velocidad que provea el ISP.
- Gestión de claves de acceso y autenticación delicada y laboriosa.
- La fiabilidad es menor que en una línea dedicada al depender del ISP, aunque a día de hoy se pueden fijar acuerdos de nivel de servicio para determinados tipos de contratos.
- Mayor carga en el cliente VPN a cause del trabajo extra a la hora de encapsular y cifrar el tráfico.
- Mayor complejidad en la configuración del cliente para la confluencia de servicios como proxy, servidor de correo, etc.
- Una VPN se considera segura pero no hay que olvidar que viajamos por Internet con las amenazas sujetas a este tipo de canal y también que el compromiso de los certificados usados para el cifrado del tráfico podría comprometer a la organización.

4.- Herramientas de monitorización.

Caso práctico



[Snort \(CC0\)](#)

un encargo de consultoría, la empresa contratada le sugiere que instale un sistema de prevención de intrusos (IPS) para proteger su red.

Carlos acaba de informatizar toda su empresa ya que gran parte de los procesos productivos, han de estar informatizados. Por televisión ve frecuentemente noticias de incidentes de seguridad que paralizan las empresas y él no se lo puede permitir, necesita que su negocio esté activo 24/7. Lo que más le preocupa son las comunicaciones entre los diferentes elementos, no pueden fallar por lo que la red es un punto crítico. Tras

Con la democratización de Internet, la creación de nuevos servicios y la aparición de nuevas amenazas, se convertía en una necesidad el desarrollar herramientas en los ámbitos organizativos pudieran monitorizar las redes para evitar ataques o al menos informar de que algo no contemplado, estaba sucediendo. Fruto de esta necesidad surgen las herramientas de monitorización que veremos a lo largo de este punto.

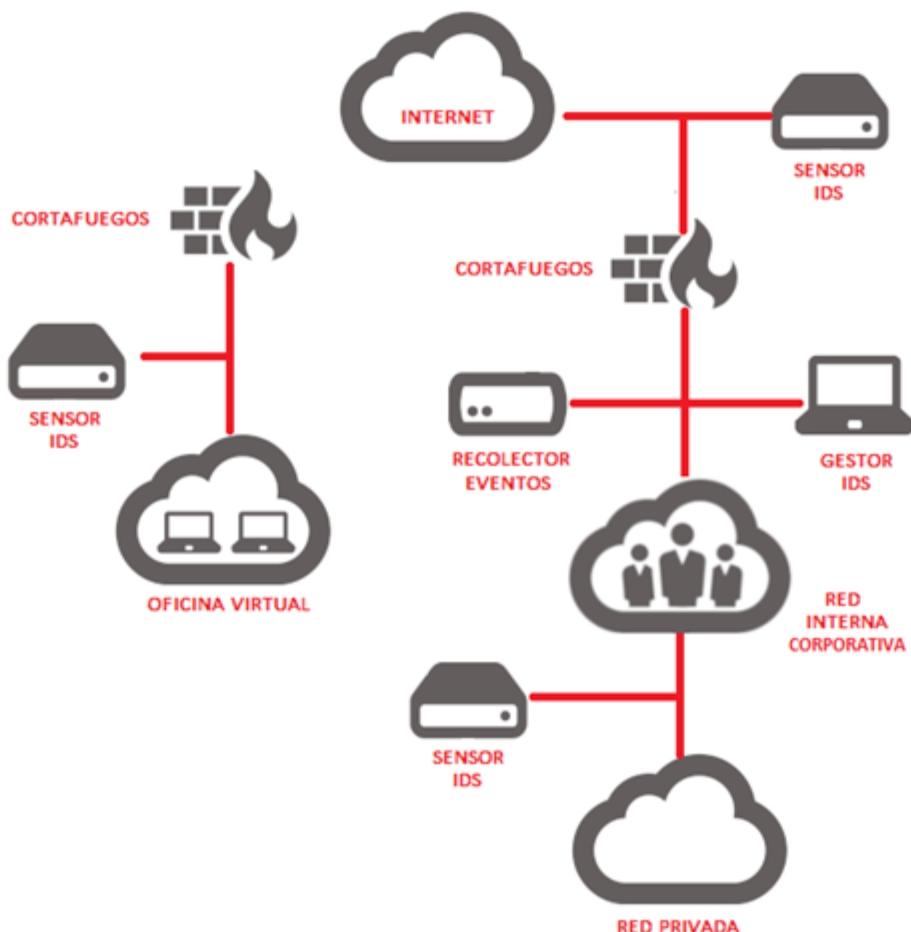
IDS

Los Sistemas de Detección de Intrusiones son soluciones empleadas para la detección de accesos no permitidos en una red o en un ordenador. Esta función la desarrollan monitorizando el tráfico entrante y comparándolo con determinadas reglas en su base de datos y que están asociadas a tipos de ataques. Estas aplicaciones si detectan algún tipo de comportamiento sospechoso en el segmento de red que están controlando, lanzarán una alerta a los operadores del servicio para que lleven a cabo las acciones pertinentes. La tipología de ataque puede ser muy variada y es en esta cuestión donde los IDS comerciales cuentan con ventaja frente a los gratuitos ya que cuentan con bases de datos y reglas más completas. Este tipo de solución tiene un comportamiento reactivo ya que no mitigan la intrusión, simplemente informan de ella.

IPS

Los Sistemas de Prevención de Intrusiones son un tipo de solución muy similar a los IDS pero tienen carácter preventivo. Es decir, en caso de que un incidente trate de afectar a un sistema y sea detectado, además de informar llevará a cabo una acción para contenerlo y si es posible, mitigarlo. Para ello analizan en tiempo real lo que transcurre por la red con el propósito de identificar anomalías, comportamientos extraños, etc. que tras el cotejo con las reglas de su base de datos podrá interactuar con la amenaza bloqueando la conexión descartando paquetes, cerrando puertos, etc.

Hay que mencionar que casi la totalidad de las soluciones hoy en día tienen funcionalidad de IPS que además se suele combinar con aplicaciones tipo  UTM.



[Incibe \(CC0\)](#)

Debes conocer

Si quieres conocer más acerca de la firma electrónica, puedes visitar la siguiente [entrada del Blog de Protege tu Empresa de INCIBE](#).

AUTOEVALUACIÓN

La diferencia esencial entre un IDS y un IPS es:

- El IDS previene frente a las intrusiones.
- El IPS únicamente detecta.
- El IDS es de reactivo y el IPS preventivo.

4.1.- Tecnologías.

Ambas soluciones cuentan con posibilidad de ser implementados en diferentes tipos de activos en función de cuál sea su función. De esta manera podemos encontrar

1. Basados en Red (o Network IDS/IPS):
 1. Monitorizan la actividad de un segmento de red.
2. Basados en Host (Host IDS/IPS)
 1. Monitorizan la actividad y comportamiento de un host que puede ser un servidor o un puesto de trabajo.
3. Híbridos
 1. Son IDS/IPS basados en host con capacidades de detectar eventos en la red.



Richard Patterson (CC BY)

Network IDS/IPS NIPS/NIDS

Este tipo de soluciones, al estar desplegadas en un segmento de red van a ser capaces de proteger varios sistemas al mismo tiempo. Su funcionamiento se basa en “escuchar” el tráfico en la red (sin alterarlo), tal como un monitor pasivo de la red (IDS), pero si se produce algún tipo de evento no contemplado o alerta, llevará a cabo una acción de contención (IPS).

De manera inicial, no interfiere con los sistemas y es totalmente transparente. Los IDS/IPS de red pueden interpretar todas las opciones y contenido o información que pudiera llevar un paquete TCP, UDP o ICMP y de otros tipos. Pueden detectar intentos repetidos de un evento (portscan, uso de herramientas conocidas, etc.). Además pueden colocarse en modo “invisible/monitor” con una interfaz que solo escucha.

Qué pueden detectar

- Paquetes con piezas de código o payload maliciosos.
- Sesiones no permitidas (intentos de ftp, telnet, etc.)
- Secuencia de paquetes que sigue un tipo de ataque conocido.

Inconvenientes

Por la naturaleza de la solución, requiere una configuración especial en switches o la electrónica de red para que el equipo donde está instalado el IDS/IPS pueda escuchar el tráfico de todo un segmento. Esto supone:

- Requieren una configuración inicial y parametrización que puede ser más o menos compleja.
- Pueden tener muchos “falsos positivos” y “falsos negativos”.
- Su funcionamiento es inútil en conexiones cifradas (SSL, VPN, SSH).

Host IDS/IPS (HIDS/HIPS)

Este tipo de soluciones se instalan directamente en servidores que soportan aplicaciones específicas (BBDD, www, DNS, etc.) o puestos críticos como los utilizados para la administración de los sistemas. Aunque el nombre quizás pueda confundir, además de detectar ataques locales, también tienen la posibilidad de detectar anomalías en la red.

Uno de los mayores inconvenientes es que al formar parte del sistema operativo, consumen recursos de este además de ser intrusivos ya que se tienen que instalar y en ocasiones pueden interferir con otras aplicaciones o servicios. Para que funcionen correctamente es necesario que el registro de logs esté habilitado ofreciendo de este modo un gran nivel de detalle de auditoría muy interesante para la investigación de los incidentes.

Una de las características más interesantes es que, ante un determinado evento, pueden permitir una reconfiguración dinámica del sistema para contenerlo o bloquearlo. No obstante, algunos de los tipos de respuesta que ofrecen son:

- Suspensión o bloqueo de cuentas de usuario
- Bloqueo del ataque
- Registro de eventos para análisis posterior
- Notificación de eventos (alarma, e-mail)
- Ejecución de scripts

Otros problemas y conclusiones

Hemos visto algunos problemas en puntos previos relacionados con cuestiones asociadas a la propia solución como:

- Si vamos a disponer de varios IDS/IPS, la administración de eventos se vuelve compleja,
- Vamos a tener el problema de convergencia entre la aparición de un ataque nuevo y la aparición de la firma para el IDS/IPS. Puede existir una ventana de oportunidad para los atacantes.
- Existencia de falsos Positivos/falsos negativos. Mientras que los primeros redundarán en una tarea extra de parametrización y afinado, los segundos supondrán un problema grave, pues la solución no será capaz de detectar amenazas reales.

Métodos de evasión

A los problemas anteriores, hemos de añadir aquellos que se crean específicamente para evitar ser detectados por estas herramientas. Algunos de los más importantes:

- **Ataques de inserción:**
 - Mediante la inyección de paquetes especialmente manipulados.
 - Disminuir el tamaño de paquetes para pasar desapercibidos.
 - Ocultar verdadera información a través de “covert channels”.
- **Evasión:**
 - Fragmentación de los paquetes para que estos no sean inspeccionados.
 - Spoofing o falsificación para hacer creer a los IDS/IPS que se trata de paquetes legítimos
 - Modificación de la secuencia y/o payload de paquetes de un ataque conocido para que la regla no sea capaz de detectarlo.
- **Denegación de servicio (DoS):**
 - Ataques falsos a HIDS para que deshabiliten cuentas y servicios de manera automática.
 - Ataques a gran escala para llenar bases de datos con registros de log.
 - Ataques dirigidos a las soluciones de manera específica para provocar sobrecarga y que dejen de actuar. Esto no lo hemos comentado, pero es posible configurar estas herramientas para que en caso de mal funcionamiento, se desconecten y no interfieran con el resto de sistemas, pero puede ser una opción arriesgada.

Conclusiones

Sobra decir que tanto los IDS como los IPS son piezas claves en la atención e investigación de incidentes de seguridad además de ser soluciones para la prevención de determinado tipo de amenazas. En un entorno donde la ciberseguridad cada día cobra más importancia, estas soluciones mejoran la administración de la seguridad informática pero no son una solución general, son una pieza más.

Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.



MINISTERIO
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL



Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

Historial de actualizaciones

Versión: 01.00.00

Fecha de actualización: 28/06/23

Versión inicial de los materiales.