**WPA2 es inseguro en alguno de estos casos:**

Contraseña débil

Las claves de autenticación de WPA y WPA2 son vulnerables a password cracking por fuerza bruta, por lo que se recomienda siempre claves de alrededor de 20 caracteres.

Spoofing de tráfico WPA y descifrado

Mathy Vanhoef, quien además descubrió recientemente el ataque KRACK de octubre de 2017, junto con Frank Piessens, demostraron que, mediante un port scanner apuntado a un cliente que utilice WPA-TKIP, es posible inyectar en su conexión paquetes arbitrarios con al menos 112B de payload, y demostraron cómo descifrar paquetes arbitrarios, lo que puede ser utilizado para robar sesiones TCP de la víctima, permitiendo al atacante inyectar, por ejemplo, código javascript malicioso.

MS-CHAPv2

Este protocolo de autenticación de Microsoft cuenta con un amplio repertorio de vulnerabilidades graves, entre las que se encuentran el acceso a las contraseñas por fuerza bruta. Con decir que en el 2012 la seguridad de MS-CHAPv2 se redujo a romper una sola clave DES (Data Encryption Standard), un algoritmo de cifrado simétrico de bloques ya obsoleto.

Hole196

Esta es una vulnerabilidad del protocolo WPA2 que abusa de la GTK. Ella puede ser utilizada para conducir a ataques de MITM (Man In The Middle) y DoS (Denial of Service). No obstante, se asume que el atacante ya está autenticado contra el AP y así puede acceder a la GTK generada.

Lack of forward secrecy

WPA no provee PFS (Perfect Forward Secrecy), lo que significa que si un atacante descubre el PSK, puede descifrar todos los paquetes WIFI cifrados, tanto los futuros, como los pasados, que hayan sido recolectados por el atacante con un sniffer. WPA solo protege a los usuarios de atacantes que no tienen acceso a la contraseña de autenticación, no protege a un usuario de un ataque proveniente de otro usuario de la red WiFi. Es recomendable, por este punto, siempre utilizar SSL/TLS en las comunicaciones, o VPN.

Predictable Group Temporal Key (GTK)

En el 2016 se demostró que WPA y WPA2 contienen un generador numérico aleatorio inseguro. Los investigadores mostraron que, si un fabricante implementa un generador random determinado, un atacante será capaz de predecir el GTK que se supone que es generado aleatoriamente por el AP.

**4-way handshake**

El handshake de 4 caminos está diseñado de modo que el AP, o authenticator, y el cliente inalámbrico, o supplicant, puedan independientemente proveer al otro la clave que conocen para el PSK/PMK, sin comprometerla, por supuesto.

En vez de enviar la clave al otro nodo, el AP y el cliente cifran un mensaje para el otro, que solo puede ser descifrado con la PMK que han compartido, y si el mensaje puede ser descifrado satisfactoriamente, esto provee información de la PMK.

El handshake de 4-way es crítico para la protección de la PMK de APs maliciosos, por ejemplo, un atacante que intente falsear el SSID del AP original… de modo que el cliente nunca le «dice» al AP su PMK.

La PMK es generada luego de toda la sesión, y debería ser expuesta lo menos posible al medio. No obstante, las claves para cifrar el tráfico sí deben ser enviadas. El handshake de 4-way es utilizado para establecer otra clave, llamada PTK (pairwise Transient Key). La PTK es generada por concatenación de algunos atributos:

La PMK

* Un número de un solo uso (NONCE) del AP: Anonce.
* Un número de un solo uso del cliente: Cnonce.
* La dirección MAC del AP
* La dirección MAC del cliente.
* El producto se utiliza como entrada a una función pseudo-random.

Además, el handshake de 4 caminos también produce una clave temporal de grupo, llamada GTK (Group Temporal key), utilizada para descifrar mensajes broadcast y multicast.

El intercambio real del 4-way handshake son los siguientes, y todos viajan en forma de tramas EAPOL-key:

El AP envía un valor nonce al cliente. Este valor se llama Anonce. El cliente genera su propio nonce, llamado Cnonce, y ahora tiene todos los atributos para construir la PTK.

El cliente envía su propio Cnonce al AP junto con un código de integridad de mensaje, o MIC, que permite verificar la autenticidad. Es, en realidad, un HMAC (Hash message authentication code) o, específicamente aquí, MAIC (message authentication and integrity code).

El AP construye y envía al cliente la GTK o clave de grupo, y una secuencia de números acompañada de con otro MIC. Esta secuencia de números será utilizada en la siguiente trama broadcast o multicast, de modo que, al recibirla, el cliente puede ejecutar una detección básica de replay.

El cliente envía finalmente una confirmación, o acknowledge (ACK) al AP.

Generación de otras claves

La Pairwise Transient Key o PTK, de 64 bytes de longitud, se divide en cinco claves distintas:

16B de la clave de confirmación EAPOL-Key (KCK – EAPOL-Key Confirmation Key), utilizada para calcular el MIC en mensaje EAPOL-Key de WPA.

16B de la clave de cifrado del EAPOL-Key (KEK – EAPOL-Key Encryption Key), utilizada por el AP para cifrar los datos adicionales enviados al cliente, por ejemplo, el RSN o la GTK.

16B de la clave temporal (TK – Temporal Key), utilizada para cifrar o descifrar paquetes de datos unicast.

8B para la clave de autenticación del MIC para los paquetes enviados desde el AP al cliente.

8B para la clave de autenticación del MIC para los paquetes enviados desde el cliente al AP.

La Group Temporal key o GTK, de 32B, se divide en tres claves separadas:

16B para la clave de cifrado GTK, utilizada para cifrar y descifrar tráfico de datos multicast y broadcast.

8B para la clave de autenticación del MIC para los paquetes enviados desde el AP en multicast/broadcast.

8B para la clave de autenticación del MIC para los paquetes recibidos por el AP en multicast/broadcast.

Cabe aclarar que las claves MIC de autenticación para tráfico saliente y entrante del AP solo se usan si la red está utilizando cifrado de datos TKIP.

**Group key handshake**

La GTK utilizada en la red podría necesitar actualizarse luego de un tiempo de expiración. Cuando un dispositivo deja la red, la GTK también necesita actualizarse. Esto es para evitar que el dispositivo siga recibiendo tráfico multicast y broadcast desde el AP.

Para manejar esta actualización de la GTK, el estándar 802.11i define el Group Key Handshake, que consiste en un handshake de 2 pasos (2-way handshake):

El AP envía la nueva GTK a cada cliente en la red. La GTK es cifrada usando la KEK asignada al cliente, y protege los datos de modificaciones utilizando el MIC.

El cliente envía al AP un acuse de recibo / ACK por la nueva clave GTK recibida.

**Proxy**

Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos. Siendo tú el cliente, esto quiere decir que el proxy recibe tus peticiones de acceder a una u otra página, y se encarga de transmitírselas al servidor de la web para que esta no sepa que lo estás haciendo tú.  
  
De esta manera, cuando vayas a visitar una página web, en vez de establecer una conexión directa entre tu navegador y ella puedes dar un rodeo y enviar y recibir los datos a través de este proxy. La página que visites no sabrá tu IP sino la del proxy, y podrás hacerte pasar por un internauta de otro país distinto al tuyo.  
  
Los proxys son utilizados muy a menudo para acceder a servicios que tienen bloqueado su contenido en determinado país. Por ejemplo, si una web no ofrece determinado contenido en tu país pero sí en otro, haciéndote pasar por un internauta de ese otro país puedes acceder a él.  
  
Como muchos de estos servicios de proxy bloquean también cookies, scripts y otros objetos que están alojados en las webs, también son útiles para poder navegar de una manera mucho más privada y anónima.  
  
Aun así, tampoco te tienes que lanzar de cabeza a los miles de proxys gratuitos que hay por la red. Ten en cuenta que todos nuestros datos pasarán por sus servidores, por lo que el anonimato que se les supone no siempre se cumple. Lo mejor es desconfiar de los proxys web que no pertenezcan a empresas de seguridad o que muestren demasiada publicidad.  
  
Por último, ten en cuenta que lo único que hace un servidor proxy es esconder tu IP. Esto quiere decir que no suelen eliminar ningún otro tipo de identificador adicional que pueda revelar tu identidad, por lo que aunque tu IP esté oculta, alguien con acceso a tu red y los datos que transmites podría espiar tu tráfico.

**¿Para qué sirve un proxy?**  
  
Un proxy no tiene por qué usarse necesariamente para navegar por Internet a través del navegador; esto es sólo un tipo de los proxys que existen, el denominado proxy de web. También tenemos el denominado proxy caché, cuyo cometido principal es precargar el contenido de una web para así, acelerar la respuesta web en futuras peticiones. En definitiva, podríamos resumir los usos de un proxy en:  
  
Servidor proxy de web. A través de un proxy accedemos a una página web garantizando así el anonimato de nuestro ordenador en la visita a esa página web. La página web no sabrá cuál es la IP que la ha visitado ni los detalles de nuestro ordenador. Sólo sabrá aquellos del proxy que utilicemos. A través de este tipo de proxy podemos hacer otras muchas cosas: modificar los datos del proxy que proporciona a la web, aligerar la carga de la página web, acceder a páginas web que sólo están disponibles para IP’s de un determinado país, etc.  
  
Servidor proxy de FTP. El funcionamiento es bastante similar al servidor proxy de web, sólo que en lugar de acceder a una página web, estamos accediendo a un FTP. Es difícil encontrar un proxy que sea rápido y, generalmente, cuando conectamos a un FTP es con la firme intención de descargar archivos de gran tamaño por lo que puede acabar resultando un proceso eterno.  
  
Si quieres una seguridad mayor tendrás que ir a por [una VPN](https://www.xataka.com/seguridad/guia-de-compras-de-vpn-nueve-servicios-a-considerar-para-navegar-de-forma-mas-segura). Las VPN o redes privadas virtuales se diferencian de los proxys sobre todo en que cifran todo el tráfico que pasa a través de ellas, algo que un proxy no hace. Por lo tanto, al cifrar los datos, aunque tus comunicaciones fuesen interceptadas por una agencia gubernamental u operadora no sería tan fácil obtener tus datos de navegación. Aunque claro, [la eficacia de la VPN](https://www.xataka.com/seguridad/como-evitar-que-tu-operadora-sepa-a-donde-navegas-vpn-dns-y-paginas-con-https) depende también de cual tengamos.

**Entonces, ¿Qué hace un VPN que no hace un Proxy?**

Simple: **Un VPN cifra todo el tráfico que pasa a través de él, un Proxy no hace esto.**

**Lo único que hace un servidor proxy es esconder tu IP**. Usualmente no se deshacen de ningún tipo de identificador adicional que puede revelar tu identidad. Esto quiere decir que cualquiera con acceso a los datos que transmites a través de tu red podría espiar tu tráfico: el gobierno, tu ISP, cualquiera conectado a la misma red Wi-Fi, software malicioso en tu navegador, etc.

**Un VPN en cambio es un asunto completamente diferente**. Sí, un VPN también sirve para enmascarar tu IP y hacer creer a un sitio web que estás en otro lugar, pero el concepto va más allá de simplemente eso.

Una **Red Privada Virtual** te permite crear una conexión segura a otra red y todo el tráfico que pasa por ella está asegurado y protegido. El VPN captura todo el tráfico del dispositivo donde esté instalado y al contrario de un proxy que solo actúa como intermediario entre una aplicación única, el VPN cifrará todo lo que se transmita desde tu ordenador.

Es como si se creara un túnel completamente privado entre tu ordenador y una red remota que a su vez te conectará con el resto de Internet.

En conclusión, si lo único que necesitas es ocultar tu IP o hacer creer a un sitio web que estás en otro lugar, con un Proxy te basta y sobra. Pero si buscas seguridad, privacidad y anonimato, necesitas un VPN. Los primeros no tienen ningún costo de ancho de banda, pero el VPN sí, y es por ello que no conseguirás ninguno que te ofrezca un servicio ilimitado completamente gratuito. Mientras mejor sea el cifrado y mientras más rápido funcione, más costoso será.

**Honeypot**

Un honeypot puede ser tan sumamente sencillo como un equipo informático cualesquiera que analice el tráfico entrante y saliente hacia Internet. Pero es importante «habilitar» o no sanear alguna vulnerabilidad del S.O, en algún protocolo, programa o cualquier otro elemento para así atraer más fácilmente a un atacante o atacantes.

Pero, por otra parte, un honeypot puede ser bastante complejo. Puede funcionar como una red de ordenadores, funcionando con diversos sistemas, y con infinidad de servicios. Con esto, cuando uno de los equipos es atacado inmediatamente es informado el administrador de sistemas.

Una de las opciones más utilizadas es usar un honeypot en forma de programa. Hay honeypots que simulan ser una red local de múltiples equipos, ips falsas, directorios inventados, equipos no presentes, etc… para crear gran confusión al atacante y/o para detectar nuevos métodos de ataque y poder aplicar defensas a nuestra red real.

También pueden guardar usuario y contraseña que el atacante introduce, bien manualmente, o por medio de diccionarios para así poder excluir todos esos caracteres alfanuméricos o no de contraseñas en nuestra red real.

Podemos decir, que un honeypot es un gran aliado para defender tu red, aunque el concepto sea atraer ataques, la mejor táctica para defenderse es saber cómo actúa el enemigo y que mejor que ponerle un cebo el cual no supondrá un riesgo para nuestra red, y nos ayudará a saber cómo incide el ataque y de qué manera.

Los honeypots más conocidos son: honeyd, kippo(ssh), Valhalla, Specter, honeynet

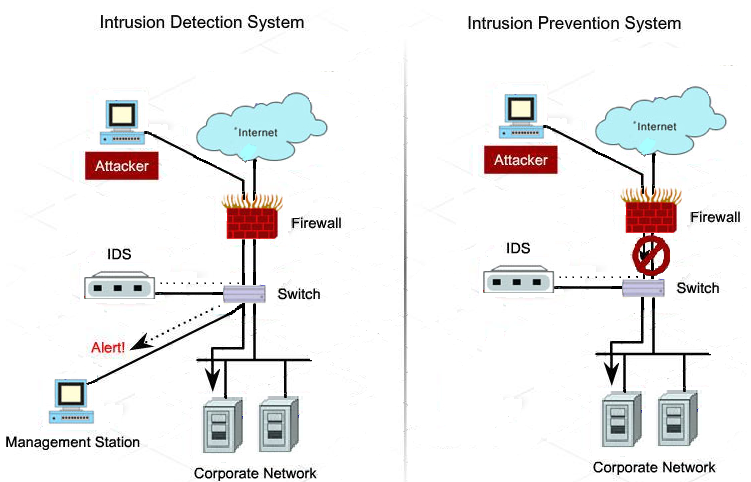
IDS

Un sistema de detección y prevención de intrusos resulta fundamental para ayudar a los profesionales de seguridad en la detección y pronta respuesta ante ataques y anomalías, además que les permite estudiar el origen y estructura de los ataques cibernéticos para crear herramientas y procesos mejorados que permitan contrarrestar futuros ataques.

Entonces, ¿Qué es un sistema de detección y prevención de intrusos?

Es una de las herramientas utilizadas para proteger las infraestructuras de manejo de información. Denning (1987) define de forma clara a estos sistemas como: “los elementos que detectan, identifican y responden a actividades no autorizadas o anormales”.

Los sistemas de detección de intrusos (IDS) fueron los primeros en aparecer, estos se encargan de monitorear y detectar comportamientos y eventos sospechosos tanto en host como en red, en tiempo real, luego, estos sistemas evolucionaron a sistemas de prevención de intrusos (IPS), que adoptan un enfoque de prevención y rápida respuesta ante los eventos sospechosos que ocurran, además de que sus análisis suelen ser de mayor complejidad. Al día de hoy, se siguen encontrando estos sistemas IDS e IPS por separado o combinados (IDS/IPS), dependiendo de la implementación que se requiera.



Al implementarse en host, pueden monitorear todo el tráfico dirigido a un equipo específico y los comportamientos inusuales que ocurran en el sistema. Cuando se implementan en red, monitorean todo el tráfico de ésta y permanecen ocultos ante los atacantes, a la vez que ejecutan acciones predefinidas ante los ataques. También existen otras categorías para estos sistemas, como los Wireless IDS/IPS que son implementados en entornos inalámbricos y los Virtual IDS/IPS que se implementan en un entorno virtual. Los IDS/IPS basan su funcionamiento detectando eventos que coincidan con los registrados en archivos de reglas definidas previamente o buscando patrones de comportamiento inusuales a partir de datos aprendidos de lo que se consideran las actividades normales realizadas en la red o host, es decir, cuando detecte una actividad que no se suele realizar normalmente o que un usuario que se conecta durante el día de pronto se conecte a horas de la madrugada, lo tomará como un comportamiento inusual o sospechoso.

¿Por qué utilizar un IDS/IPS?

Un IDS/IPS nos permite tener una supervisión completa del flujo y estado de los componentes la red o sistema, permite mantener un control en caso de que se detecten ataques o anomalías, incluyendo aquellas que se originen desde la porción segura de la red, ya que sin necesidad de estar presentes en el momento que ocurra algún ataque, el IDS/IPS estará configurado para actuar en respuesta automática ante el evento presentado, y nos permitirá tener un registro de todo lo ocurrido para posterior análisis y mejoramiento de la seguridad de la infraestructura.