3.9 Configuraciones básicas

SEGURIDAD EN REDES INALÁMBRICAS

Las redes inalámbricas deben tener una protección especial por cuestiones de seguridad. Dependiendo de la seguridad de las redes se puede diferenciar en:

A) REDES ABIERTAS

Son las redes sin protección, por lo que cualquier usuario que tenga acceso a la red se puede conectar a ella sin necesidad de autentificación.

B) REDES CON SEGURIDAD

Para proveer de seguridad a la red inalámbrica existen varios protocolos de cifrado de datos:

SEGURIDAD EN REDES INALÁMBRICAS II

- **WEP** (**W**ired **E**quivalent **P**rivacy). Sistema de cifrado simple presente desde la primera versión del estándar **IEEE 802.11.** Utiliza una clave estática de 68 o 128 bits. El emisor debe escribir la clave para cifrar la información y el receptor también debe introducirla para descifrarla. Se considera **obsoleto** y se desaconseja su uso, ya que se puede "romper" en pocos minutos.
- **WPA** (**W**ifi **P**rotected **A**ccess). Dentro de WPA se distinguen estos tipos: WPA personal o WPA PSK (Pre-Shared Key) y WPA Enterprise o empresarial. Mejora la gestión de las claves del anterior, utilizando una clave de 256 bits que cambia dinámicamente en cada paquete que se transmita. También incluye la comprobación de la integridad de la información, para comprobar que llegue correctamente y no haya sido manipulada. Tampoco es considerado seguro. Utiliza el cifrado TKIP. Considerado **obsoleto**.

SEGURIDAD EN REDES INALÁMBRICAS III

- **WPA2 (W**ifi **P**rotect **A**ccess **2).** Es una versión mejorada del anterior, ya que utiliza un algoritmo de cifrado más avanzado (**AES**), mientras que el anterior usaba TKIP. Ha sido reemplazado por el siguiente, aunque se sigue utilizando ampliamente. Algunos routers pueden permitir usar Wpa2-tkip por cuestiones de compatabilidad. Aunque es aconsejable utilizar AES ya que TKIP está considerado obsoleto.

- **WPA3 (W**ifi **P**rotect **A**ccess **3)** utiliza un cifrado **SAE**, más robusto que el anterior, pues el cifrado de datos es individual y ofrece una mayor protección ante los ataques. Es el protocolo de seguridad más reciente y seguro para las redes Wi-Fi.

SEGURIDAD EN REDES INALÁMBRICAS IV

Además de los protocolos de cifrado de datos, existen una serie de medidas que pueden adoptarse para aumentar la seguridad de la red:

- **Filtrado de MAC**. También denominado filtrado por hardware. Con esta técnica solo se permite el acceso a la red a aquellos dispositivos que tengan una dirección MAC concreta que previamente se ha almacenado como dirección autorizada.
- **Desactivar la difusión del SSID.** El SSID es el identificador o nombre de la red wifi propia. Desactivando su difusión no podrá ser visto por otros usuarios.
- **Cambiar el SSID y la contraseña** que vengan por defecto en el router o añadir una contraseña si viene sin ella.

SEGURIDAD EN REDES INALÁMBRICAS V

- **Desactivar el WPS (W**ifi **P**rotected **S**etup**).** Es una función que se utiliza para conectarse al router de forma fácil y rápida, normalmente a través de un PIN. Puede activarse accediendo a la configuración del router o mediante un botón. Si bien es cierto que los equipos que instalan algunas ISP (empresas proveedoras de servicios de Internet) ya no traen esta función o la traen deshabilitada por defecto, es altamente recomendable anularla debido a la inseguridad de la misma.
- **Red de invitados.** Existen modelos de routers que crean una red inalámbrica separada de la red local y conocida como red de invitados. De esta manera, evitaremos que se tenga acceso a la red local, así como a los datos que aquí se albergan, evitando potenciales infecciones mediante la propagación de virus, malware o una fuga de información.

SEGURIDAD EN REDES INALÁMBRICAS VI

- **Deshabilitar UPnP (U**niversal **P**lug a**n**d **P**lay**).** Esto le permite a los dispositivos en la red como ordenadores, impresoras, y otros dispositivos, descubrirse entre ellos mismos dentro de la red. Esto puede introducir riesgos de seguridad, y puede deshabilitarse si la opción está presente.

- **Configurar el firewall.** Tener abiertos únicamente los puertos necesarios.

Además de estas medidas, se puede mejorar la seguridad con sistemas IDS, IPS o SIEM. Aunque es importante la seguridad, no debe complicarse hasta hacer tedioso su uso. Se debe buscar un equilibrio entre seguridad y facilidad de uso, utilizando correctamente los sistemas de autenticación y configuración de equipos de red.

SEGURIDAD EN REDES INALÁMBRICAS VII

ENLACES DE INTERÉS

- Simulador configuración router asus
- Simuladores de configuración productos linksys
- Simuladores de configuración productos tp-link

REDES WAN

Como vimos en sesiones anteriores, las redes WAN son redes que abarcan grandes distancias, ciudades, países o continentes. Pueden ser de escala mundial y conectar otras redes, como las LAN y las MAN.

Los protocolos utilizados en este tipo de redes han evolucionado con el tiempo. Antiguamente se utilizaban protocolos como **X.25, Frame Relay y ATM**, pero estos han sido en gran medida reemplazados por tecnologías más modernas como **MPLS** y Ethernet por fibra óptica.

Las redes WAN pueden ser públicas, como las que se utilizan para acceder a internet, o privadas utilizadas por grandes empresas y corporaciones. Ejemplos de redes son internet, las redes de los bancos, las de grandes empresas multinacionales, las redes militares, etc. Se utilizan también para ofrecer servicios en la nube.

CONFIGURACIÓN ACCESO INTERNET

Para configurar el acceso a Internet en un Router, es esencial navegar hasta el apartado denominado WAN. En España, los tipos de conexión WAN más comunes utilizados por los ISP son **PPPoE** e **IPoE**.

- **PPPoE** (**P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet). Requiere un nombre de usuario y una contraseña proporcionados por el proveedor de servicios de Internet.
- **IPoE** (**I**nternet **P**rotocol **o**ver **E**thernet). Más moderno que PPPoE, no requiere autenticación. La conexión se establece automáticamente, lo que facilita la configuración.

CONFIGURACIÓN ACCESO INTERNET II