Módulo WI-FI

Punto de acceso inalámbrico seguro.

por ALBA Software

1. Introducción

Las redes inalámbricas están de moda, y han venido para quedarse. La comodidad que supone estar conectado a la red de la empresa sin necesidad de cables junto con la proliferación y adopción dispositivos móviles como portátiles, PDAs, cámaras, etc. hacen de esta tecnología una herramienta de productividad muy beneficiosa para las empresas.

Wi-Fi es una tecnología similar a Ethernet, que nos permite conectar equipos separados físicamente sin necesidad de cables.

Se trata de una tecnología rápida. De hecho, es más veloz que la versión cable módem más rápida existente hoy en día.

Ofrece la posibilidad de conectarse a una red en cualquier lugar en el que exista un acceso Wi-Fi, como aeropuertos, hoteles o incluso parques.

Supone un ahorro de costes con respecto a las tecnologías de cables, y en el ámbito corporativo permiten extender las redes Ethernet a otras áreas más públicas como pueden ser salas de ventas, conferencias, almacenes, etc. Y también suele usarse Wi-Fi para interconectar edificios.

De hecho muchas empresas con aplicaciones de control de almacenes, hace tiempo que utilizan estas redes para conectar los terminales de captura de datos con el servidor de gestión y así poder manejar información on-line sobre los productos que están manipulando.

Pero cuidado, un acceso inalámbrico significa que nuestros dispositivos utilizan el "aire" para comunicarse, y que cualquier dispositivo de este tipo puede escuchar las transmisiones de los

Copyright © 2003 ALBA Software (www.albasoft.com) All rights reserved.

otros. Por decirlo de alguna manera, es el medio menos privado que existe.

Pero antes de alarmarnos veamos cómo funciona la seguridad en WI-FI, qué problemas tiene y cómo solucionarlos.

2. Funcionamiento

Un dispositivo Wi-Fi tiene la capacidad de descubrir las redes inalámbricas que tiene a su alrededor.

Una red inalámbrica utiliza las ondas de radio como nivel físico de transporte y pueden atravesar paredes y suelos.

De esto deducimos que es un medio público al cual todo el mundo puede tener acceso y que es una red, en principio, independiente de la que montamos en la empresa. Esto suena a Internet.

El problema es que cuando conectamos la red WI-FI a la red de la empresa estamos ofreciendo tomas de nuestra red a cualquiera que se encuentre a una distancia de enlace. Es decir, que cualquiera con cobertura puede escuchar el tráfico que circula por el medio y puede intentar una conexión al mismo.

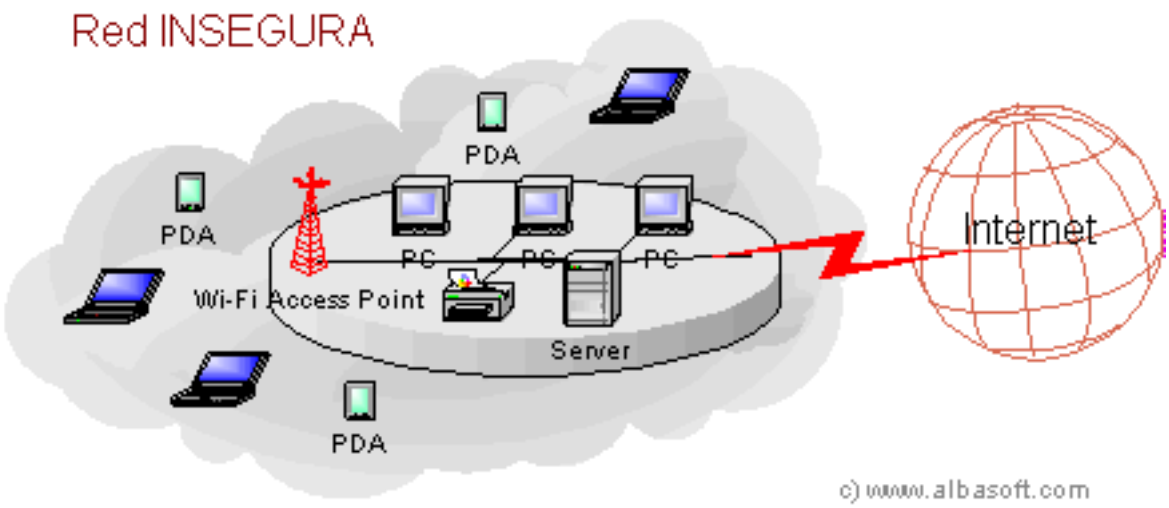
En principio existe una limitación de distancia para poder conectarse a buena velocidad a una de estas redes. Si, el parking de enfrente de su oficina suele tener cobertura. Pero el curioso que solo necesita escuchar la red puede encontrarse a kilómetros de distancia con antenas directivas y con programas de dominio público que cazan y guardan los correos electrónicos en carpetas, buscan tramas de autenticación y guardan los passwords, y demás simpáticas "utilidades".

Alerta:

¿Cuantas empresas en un radio de 10 kilómetros, podrían estar interesadas en tener acceso a toda la información de su empresa?

A continuación podemos ver un esquema de una red con acceso a internet y un punto de acceso WI-FI.

Copyright © 2003 ALBA Software (www.albasoft.com) All rights reserved.



Conexión incorrecta del punto de acceso WI-FI

En rojo podemos ver los puntos de acceso no controlados de esta red. Todos sabemos los problemas que conlleva un acceso a Internet no protegido, de ello se han encargado los distintos gusanos y robots que circulan por Internet, pero el problema de seguridad que más ha afectado desde Internet, en general, son los virus.

En una red Wi-Fi el atacante no va a ser un programa anónimo que realiza sus maldades sin importarle quienes somos, los posibles intrusos buscan nuestros datos para utilizarlos o destruirlos, esto sin eliminar la posibilidad de que el equipo del atacante esté infectado y nos invada la red de virus sin querer.

El problema de la seguridad no se ciñe a una tecnología en concreto, afecta a toda la arquitectura de comunicaciones de la empresa, y las soluciones de seguridad deben plantearse con una visión de conjunto.

3. Una solución segura.

El mecanismo que se encarga de asegurar la confidencialidad de las redes inalámbricas que se conoce como WEP (Wired Equivalent Privacy) tiene serios problemas de seguridad. Para solucionarlos se está trabajando en una revisión del protocolo llamado WPA (Wi-Fi Protected Access).

Estas tecnologías pretenden que los protocolos de conexión a las redes Wi-Fi sean más seguros, y esto se consigue asegurando que el que se está conectando es quien dice ser, y encriptando la información que circula por el medio.

Copyright © 2003 ALBA Software (www.albasoft.com) All rights reserved.

La autenticación puede realizarse mediante password o mediante MAC. Todos los dispositivos de red disponen de una referencia única que los identifica, de forma que cuando se establece la comunicación se le pregunta al dispositivo su nº de MAC y si no se encuentra en la lista de invitados no pasa.

Esto es tan fácil de saltar como escuchar un rato la red con un equipo que tenga instaladas herramientas de adminisrtación, y cuando una mac deje de generar tráfico entrar en la red suplantando este dispositivo.

La palabra clave es la misma en todos los dispositivos conectados, sin comentarios, pero además existen programas de dominio público que son capaces de romper este tipo de claves en muy poco tiempo.

El tema de la encriptación solo es realmente seguro si trabajamos con claves llamadas públicas. Sin entrar en detalles, es lo que se utiliza en los certificados digitales.

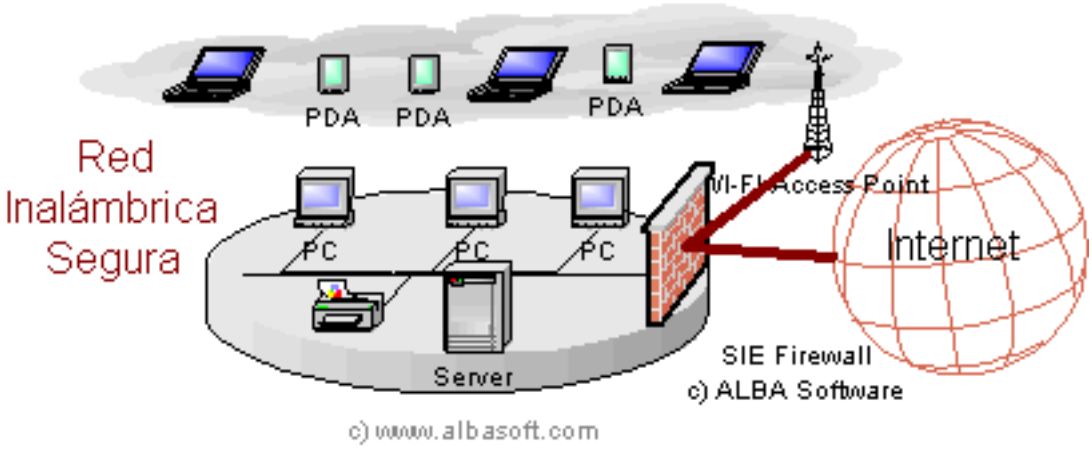
Cualquier avance en seguridad a la hora de conectarnos a una red Wi-Fi será bien venido, pero realmente ya existen mecanismos de autenticación, encriptación y control de acceso seguros y más que probados. Se utilizan en lo que conocemos como VPN y solucionan los mismos problemas que tenemos en las redes WI-FI.

Lo que necesitamos de los dispositivos WI-FI es la capacidad de acceso al medio, no podemos confiar toda la seguridad de nuestros datos a la implementación que se haya hecho para una u otra tarjeta. ¿Qué pasa con los dispositivos PDA que tenemos con el protocolo 802.11b que utilizan WEP como mecanismo de seguridad?, ¿Los tiramos y nos compramos otro? ¿Cuánto tiempo tardará hasta que nuestro dispositivo vuelva a ser inseguro?

La seguridad es un problema de barreras, cuantas más coloquemos más seguro estará el sistema, y el coste de la puerta debe estar en concordancia con el valor de los datos que se protege. Además, no toda la información que circula por nuestra red tiene el mismo grado de privacidad.

Por eso desde ALBA Software proponemos una solución de seguridad por capas, creando distintos escenarios y aislando las redes para poder controlar el tráfico.

Copyright © 2003 ALBA Software (www.albasoft.com) All rights reserved.



Red WI-FI controlada por SIE-Firewall

En la plataforma de comunicaciones SIE las capas son módulos estándar de conectividad, servicios de red y seguridad. No sólo nos sirven para controlar las comunicaciones WI-FI, sino para asignar políticas de seguridad a todas las comunicaciones de nuestra red corporativa, incluyendo las comunicaciones Internet.

- **Módulo Firewall:** separación de redes y políticas de filtrado.
- **Módulo DHCP:** para asignar direcciones dinámicas o fijas según el dispositivo que se conecta.
- **Módulo Proxy:** para controlar los accesos a Internet.
- **Módulo VPN access:** que permite un acceso completo a la red interna sólo a aquellos usuarios a los que el administrador de la red haya suministrado un certificado digital. Todas las comunicaciones van encriptadas y utiliza el estándar IP-SEC.

El módulo WI-FI de SIE cumple con todos los estandares de la norma y mejora sus características de seguridad al centralizar la administración de toda la gestión de la red.

De esta forma aunque todos los dispositivos comparten el medio, cada uno tiene un nivel de seguridad y puede acceder a ciertas redes o servicios según sus privilegios.

Por ejemplo, si tenemos servidores de bases de datos con información confidencial conectados mediante Wi-Fi el acceso a estos equipos debería ser únicamente sobre VPN (IP-SEC), mientras que los PDAs que quieran salir a Internet les daremos paso a través del proxy, el cual nos pedirá una simple autenticación mediante usuario y password.

4. Creación de redes y conexión de centros.

Los dispositivos Wi-Fi se conectan con las redes físicas a través de los llamados *puntos de*

Copyright © 2003 ALBA Software (www.albasoft.com) All rights reserved.

acceso. Un punto de acceso es una tarjeta de red Wi-Fi con características especiales y un software que le permite establecer conexiones con distintas tarjetas Wi-Fi y enrutar el trafico entre ellas y hacia otras redes. Físicamente se parecen a los routers pero con una antena.

El punto de acceso de SIE Firewall es una tarjeta instalada en el equipo que proporciona una cobertura entre 60 m (a 54 Mbps) y 300 m (a 10 Mbps).

Para crear redes de mayor cobertura se dispersan puntos de acceso 'hardware' por la zona a cubrir de forma que se vean entre ellos formando una red que puede llegar a cubrir una ciudad entera. Uno de estos puntos de acceso es SIE-Firewall que enlaza la red Wi-Fi con la red física de la empresa y donde se encuentran los mecanismos de gestión y control de las comunicaciones.

Si ya tenemos punto de acceso Wi-Fi en nuestras instalaciones podemos conectarlo a una entrada ethernet de SIE Firewall o podemos utilizarlo para ampliar la cobertura de nuestra red Wi-Fi.

Red WI-FI controlada por SIE-Firewall

Además SIE Firewall puede gestionar una segunda interface WI-FI que utiliza antenas directivas para conectar centros que pueden estar a varios kilometros de distancia, siempre que tengan visión directa.

Al utilizar SIE Firewall los centros se conectan mediante VPN Node, con todas las características de seguridad, escalabilidad y redundancia de las que dispone este módulo.

5. Características técnicas

- Estándar IEEE 802.11g y cumple con el 802.11b.
- Alta tasa de transmisión hasta 54Mbps, con ajuste automático a 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48.

Copyright © 2003 ALBA Software (www.albasoft.com) All rights reserved.

- Rango de operación de hasta 350 m.
- Banda de frecuencia de 2.4GHz, 2.400MHz - 2.4835MHz.
- Tecnología de multiplexación por división en frecuencias ortogonales (OFDM).
- Encriptación WEP de 64/128-bits.
- Todas las características técnicas de SIE Firewall y su capacidad de crecimiento modular.

6. Artículos de interés

- HP alerta sobre el bajo nivel de seguridad de las redes 'wireless'
  http://www.computing-spain.com/Actualidad/Noticias/Infraestructuras/Soluciones/20031201051
- Efectivos d seguridad declaran q el Wi-Fi no será apto para los juegos d Atenas
  http://www.terrassawireless.net/modules.php?op=modload&name=News&file=article&sid=188
- Wi-Fi se consolida como una tecnología madura
  http://www.computing-spain.com/Actualidad/Noticias/Infraestructuras/Soluciones/20031119030
- Un estudio cuestiona WPA, el nuevo estándar de seguridad para Wi-Fi
  http://www.computing-spain.com/Actualidad/Noticias/Seguridad/Vulnerabilidades/20031112001

Módulo de SIE Firewall.

Copyright © 2003 ALBA Software (www.albasoft.com) All rights reserved.