WifiSafe

WIFI-HOTSPOT PARA HOTELES

"Lo que la ley obliga a día de hoy"

2018 - WifiSafe

Ante las centenares de dudas que últimamente nos llegan, vamos a intentar resumir qué debe de hacer un hotel/restaurante/comercio/clínica, cualquier establecimiento o empresa que ofrezca servicio WiFi gratuito a sus clientes o invitados. Con lo que estos requerimientos son de obligatorio cumplimiento para todas las WiFi tanto gratis como de pago que no sean internas de la empresa, ósea el 100% de las WiFi-Públicas.

Punto a tener en cuenta.

La red WiFi debe de estar acotada en la empresa, ósea debemos de ofrecer el servicio WiFi a nuestros clientes, no a cualquiera que pase por la calle, entendiendo esto último como que no vale eso de mira, como delante tengo una plaza o a la competencia, voy a poner equipos WiFi que cubran esa área o zona y les voy a ofrecer WiFi para intentar captarlos como clientes ¡NO! Esto no es válido, ni legal, debéis de limitaros a los clientes de vuestra empresa comprendiendo también que la WiFi, no se puede evitar que salga de las cuatro paredes, no va a pasar nada porque alguien que esté en la puerta y no sea cliente, se conecte a una WiFi de cortesía (limitada en tiempo y caudal) pero desistir de dar cobertura a zonas o áreas públicas (o no) que no sean estrictamente las vuestras, aunque sean por motivos comerciales o de marketing.

Lo primero, es que todo este servicio que garantiza por ambas partes, cliente y empresa, el acceso a la red WiFi, debe de ser realizado con un equipo al efecto (un HotSpot) que es el que nos proporcionara todas las funciones que precisaremos.

Para que no hayan equivocaciones, un HotSpot, NO es el típico controlador de puntos de acceso que comercializan la mayoría de fabricantes, es más, en todas las instalaciones profesionales hay un controlador más un HotSpot, o en el mejor de los casos un HotSpot con controlador, como sucede con los equipos de 4ipnet.

Tampoco un HotSpot es un equipo de bajo coste al cual instalamos un software o aplicación para que emule. Un HotSpot con controlador, está debidamente dimensionados para garantizar la carga de trabajo, volumen de usuarios, control de clientes, servicios, paquetes, etc.

¿Qué servicios mínimos ha de tener obligatoriamente mi HotSpot?

Debe de tener un PORTAL CAUTIVO:

Un portal cautivo es una página de inicio personalizada, a la cual, accede el cliente cuando abre por primera vez su explorador (lógicamente, previamente debe de haber seleccionado la red WiFi a la que quería asociarse en su dispositivo).

Lo primero que debe de aparecer en el Portal Cautivo, es un Disclaimer de responsabilidades.

En este disclaimer (a ser posible supervisado previamente por un departamento legal) la empresa deberá de dejar claro, cuál es el objeto del servicio, sus responsabilidades del mismo, y las aceptaciones legales que el cliente acepta.

Además, indicar que se realiza un traceo de comunicaciones y que éste puede ser guardado (indicando el tiempo) para el objeto que sea (entre ellos para entregar a las fuerzas de seguridad, si en un momento fueran solicitados) y que en el caso que pidamos datos, como correo email o cualquier otro dato personal, el cliente , tiene a su disposición un email de contacto, (que debe quedar claro y completo) o por otros medios que la empresa considere, donde el cliente pueda pedir que sus datos personales puedan ser modificados o borrados.

La empresa también puede en ese disclaimer indicar que los datos del cliente, si es el caso, pueden ser utilizados para campañas de marketing, o inclusos facilitados a terceros, si así fuera.

Osea podéis/debéis de poner todo lo que queréis hacer con la información del cliente, si es que vais a hacer algo con ella, pues en este caso, las normas, las ponéis vosotros, por eso y para eso, ofrecéis un servicio gratuito y que el cliente, es libre de aceptar o no, pero no se le obliga en ningún caso.

Si el cliente quiere WiFi, debe de aceptar las condiciones de uso que vuestra empresa y departamento legal estimen oportunos. Si no las acepta, pues tendrá que tirar de su plan de datos móviles. si los tiene.

Lógicamente, podéis detallar que al tratarse de una red pública no garantizáis la seguridad de la misma o de la integridad de los datos, ni de la veracidad de los servicios que contrate con empresas terceras a través de vuestra red, etc. Podéis ser tan creativos como queráis.

Pero... lo más importante, es que el cliente debe de marcar INEQUÍVOCAMENTE, la aceptación de estas cláusulas que vuestra empresa pone, o que legalmente os imponen y traspasáis las responsabilidades del usuario final, al usuario propiamente dicho, vuestro cliente. Y por lo tanto, no valen las opciones de un disclaimer con la opción pre-marcada de aceptación del servicio.

Para que el cliente acepte estas condiciones (que es lo primero que verá), basta con poner una casilla (que no un botón), donde deba marcar claramente que acepta las condiciones del servicio. Una vez lo marca y acepta, en ese momento el portal cautivo puede o bien darle acceso directo a la navegación web, o bien abrir un segundo portal de bienvenida a vuestra empresa y ahí, si así lo deseáis, hacerle ingresar los datos que queráis.

Por ejemplo, un usuario y password que s eutiliza mucho si estáis en un hotel y dependiendo de su estancia, lo que determina una conexión de x días determinada por su cheking, o bien, solicitar datos para marketing en un formulario. También puedes ofrecerle una WiFi-Premiun de pago, o lo que queráis , hay un mundo de opciones que podemos personalizarlos a gusto y necesidades de cada empresa.

No olvidéis que el diseño de la página que va a ver el cliente, también dice mucho del nivel de detalle, seriedad, profesionalidad de vuestra empresa, con lo que nuestro consejo, es que se medite bien y que se contrate un servicio de diseño para garantizar que la imagen de vuestra empresa este a la altura de lo que esperáis.

Guardar logs de conexiones (no, pero si):

Aunque en ningún momento (y por ahora) hay obligatoriedad de guardar datos de las comunicaciones de vuestros clientes, es recomendable, pues existe una recomendación europea que recoge que esto sea realizado, pero a día de hoy, que yo recuerde, sólo 3 países de la comunidad europea se han acogido a esta recomendación y lo han hecho obligatorio en sus respectivos países, en el caso de España, hasta la fecha de este escrito, no se había acogido a ella.

Mi consejo es que el equipo HotSpot que compréis, tenga esta posibilidad, pues ya sabemos que las leyes pueden ser obligatorias en cualquier momento. Por supuesto, este log de conexiones , donde podremos guardar desde la mac del dispositivo, ips, rutas etc, etc, no deben ser entregados a cualquiera, y mucho menos, por petición oral, lo que incluye también a las fuerzas de seguridad del estado que no estáis obligados a no ser que exista una petición judicial a dicho efecto.

En dicho log, no se guardan datos personales del usuario del dispositivo (persona física), ni tampoco datos de números de cuentas, ni correos, ni ningún otro tipo de comunicación que no sea estrictamente legal, ni tampoco estáis autorizados a poner un equipo que snife las comunicaciones, ni de clientes, ni empleados, es más, esto último está penalizado judicialmente.

¿A qué no estáis obligados?

No , NO estáis obligados a identificar persona/dispositivo, me llegan muchas preguntas de perconas mal asesoradas que dicen que su asesor de ley de protección de datos le obliga a identificar con nombre y apellidos e incluso documento de identidad al usuario.

Rotundamente NO, no estáis obligados y en el caso que lo hicierais, (algo que no es simple, ni económico) entonces deberéis de tener una persona en la empresa dedicada a tratar la confidencialidad de dichos datos.

Con lo que mi consejo, es que ni os lo planteéis, porque ¿Cómo vas a identificar a un cliente temporal de la cafetería, salón de congresos, etc, fehacientemente? Si quieres que el registro lo haga el propio cliente, puede éste inventarse todos los datos y poner un documento falso, con lo que vuestra captura sería totalmente irreal y no serviría de nada.

Además, en el caso de un hotel, por ejemplo, es común ofrecer un único usuario y password para los 2,3,4 dispositivos que pueda utilizar un cliente en su habitación, pero en ningún momento serías capaz de identificar si el usuario del dispositivo nº1, es el cliente o su pareja, o su hijo.

Independientemente, y si aún sigues pensando que debes hacerlo, quién te garantiza que tu cliente una vez logueado, no deja su dispositivo a un amigo, mientras queél se pega un chapuzón en la piscina o está en el spa?

Más recomendaciones a futuro.

Para nuevas instalaciones de puntos de acceso, es recomendable que siempre utilicéis equipos de última generación, con los últimos estándares actuales. En este caso, equipos que cumplan con Wave2, pues en el caso que hagáis compras de equipos con estándares más obsoletos, por ejemplo 802.11n, en cuanto la marca deje de fabricar el último modelo, (que no de comercializar) solo dispondréis de 5 años, en el cual, el fabricante está obligado por ley a actualizaciones de firmware, y por lo tanto, a tapar y evitar agujeros de seguridad en vuestras redes internas y las de vuestros clientes.

Huir de marcas domésticas que os llamen la atención por su bonito diseño o bajo precio, cuanto más "masivo" es un producto, más ataques vais a recibir, y por lo tanto, deberéis de estar más al tanto de la seguridad de vuestra red.

Elegir marcas no sólo reconocidas porque salgan en muchos foros o porque las encontréis muy fácilmente referenciadas en Internet. Elegir aquellos profesionales, empresas y fabricantes que están especializados en soluciones WiFi para vuestro sector.

El mayor número de fracasos de redes WiFi, un 99%, se dan por utilizar equipos de bajo coste y para el sector consumo.

Utilizar siempre switches gestionables, con POE 803.at (mejor que 803.af) pues os dará más flexibilidad y mejor gestión.

El corazón del éxito de una instalación hotelera es el HotSpot, por lo tanto, os doy un consejo, eviten comprar un equipo de gestión como es un HotSpot cuando veas que te lo venden por menos precio que el smarthpone que llevas en tu bolsillo, no es lógico, a contrario, es estúpido pensar que algo de poco valor, y por lo tanto, con una electrónica dedicada de bajo coste, poca memoria, poca cpu, etc, va a ser capaz de gestionar los millones de paquetes que son capaces de negociar los 50/100/200 /xxx clientes que tengas en tu hotel.

Si ya ves que tu pc, cuando abres muchas aplicaciones se vuelve mas lento e inestable, ¿crees que una cajita de pocos cientos de euros va a tener unas especificaciones técnicas razonables? Si piensas que te vas a comprar 20 puntos de acceso y el HotSpot te va costar (el hardware) lo que valen 2/3/4 Aps, te están vendiendo una moto...o lo que es peor, vas a tener malas valoraciones de tu establecimiento por ahorrarte en el corazón de tu red y confiar la gestión a algo que no es capaz.

¿Qué mínimo has de pedir a un HotSpot?

- Que sea capaz de tener varios portales cautivos diferenciados

Por ponerte un ejemplo, un hotel medio, tiene varias áreas o zonas diferenciadas para sus clientes. Tenemos el hotel, donde están los huéspedes, pero también tenemos una cafetería o restaurante donde vienen clientes externos, además de los huéspedes, también solemos tener salones de actos, reuniones o para eventos o celebraciones, sin contar las zonas privadas propias de la empresa, o para conectar vía WiFi los PDA,s comanderos del restaurante, o la propia administración del hotel, cada una de estas zonas de servicio, puede tener mútiples tipos de clientes.

Ejemplo, en un hotel que tiene, Huespedes, Cafeteria, Salones de alquiler

Puede darse el caso de que un día en concreto, coincidan en la cafetería clientes eventuales que van a desayunar, los huéspedes y un grupo de personas que alquila el salón para una convención comercial.

Es lógico que la zona de cafetería pueda tener estos tres tipos de clientes simultáneamente, pero qué pasa si los tres tipos de clientes se acercan (porque están al lado del espacio alquilado. Si están en la puerta de ese espacio, en el cual, hay una actividad privada, no podemos permitir que un huésped o un cliente eventual de cafetería esté haciendo uso del punto de acceso de dicho espacio, pues puede saturar el equipo.. como tampoco podemos aceptar que el huésped que tiene su habitación justo encima del espacio, haga uso del punto de acceso dedicado a otro grupo de clientes y viceversa.

Además, este tipo de clientes debería tener unas políticas de acceso diferenciadas.

El huésped tendrá conectividad 24h al día, durante toda su estancia, y con un caudal de acceso a Internet de, por ejemplo, 2 megas de subida y 1 de bajada.

Sin embargo, también tenemos huéspedes VIP, o porque son asiduos, o bien porque se hospedan en las Suite y queremos agasajarlos con una conectividad más alta, 5Megas de subida y 2 de bajada.

También tenemos la empresa que alquila el salón para 100 usuarios, a cada usuario queremos ofrecerle porque es una convención de informática, 10megas de bajada y 3 de subida. Pero tenemos a los oradores o a los que presentan el evento que precisan realizar una vídeo conferencia con 20megas de bajada y 10 de subida, considerando una VPN directamente a sus oficinas centrales de Suiza.

En el evento y el salón, solo van a estar utilizados 3 días de 10:00am a 17:00, con lo que una vez finalizado el horario del evento, no queremos que se queden usuarios dentro y queremos liberar el ancho de banda garantizado por contrato de dicho evento para uso del resto de huéspedes del hotel, ya que el hotel, tiene su máxima carga de trabajo precisamente por las noches y queremos disponer de dicho caudal disponible.

Por supuesto, los clientes eventuales de la cafetería tienen otro trato diferente, sólo pueden conectarse 30 minutos, y no pueden volver a conectarse hasta al cabo de 3 horas y a estos les pedimos en un formulario en el portal cautivo que indiquen su edad y nacionalidad.

Con estos ejemplos, os cuento tareas más que obvias... volviendo al caso del hotel que ya dispone como mínimo de 4 zonas diferenciadas con 4 Vlans, pero que sucede si queremos más zonas porque tengamos un segundo espacio o salón de actos, o bien un centro Gimnasio que ofrece servicios a clientes externos, y los cuales, cuando corren en las cintas quieren estar escuchando Spotify con calidad, o bien, cuando queremos meter en la misma red nuestras cámaras de viedeovigilancia inalámbricas, o los PDA comanderos, o el personal de la propia empresa...

Pues que esas 4VLANS se nos quedan insuficientes y no podemos ofrecer y securizar los servicios adecuadamente.

También cada vez más, el sector hotelero intenta integrar los servicios en su PMS, obteniendo más información de sus clientes y ofreciendo más servicios conociendo sus gustos. Con lo que el HotSpot debe de estar totalmente preparado para conectarse al PMS hotelero de forma sencilla y sin tener que modificar para nada los costosos programas PMS hoteleros.

También debemos ser capaces de enrutar adecuadamente a cada servicio, los caudales adecuados en cada momento, tener flexibilidad a la hora de jugar con más de una conexión a Internet balanceando cargas de trabajo, tener los criterios claros de reglas de firewall que queremos ofrecer a nuestros clientes, poder dar calidad de servicio en las comunicaciones de voz sobre IP, garantizar la prioridad en sistemas de video para que el Netflix se siga viendo bien en cualquier dispositivo, o incluso, anular el servicio de streaming si el caudal de acceso que nos llega del operador de turno es limitado y escaso

Todo esto, NO LO HACE un controlador de APS, todo esto no lo hace un HotSpot Cloud, todo esto y mucho más lo hace un HotSpot de la marca 4ipnet. ¿Aún no tienes el tuyo? Consúltame y te ayudaremos y te contaremos más diferenciaciones respecto a la competencia.

En WifiSafe puedes obtener más información, ponte en contacto con el Departamento de Soporte 807 450 005 o el Departamento de Pedidos 902 506 100 o envía un correo electrónico a info@wifisafe.com