Universidad de Montemorelos

Facultad de Ingeniería y Tecnología

ESQUEMA SEGURO PARA LA RED INALÁMBRICA DE LA UNIVERSIDAD DE MONTEMORELOS

Trabajo de investigación

Presentada en cumplimiento parcial de los requisitos para el grado de:

Ingeniería en Electrónica y Telecomunicaciones

Por

Jonathan Gamaliel Roblero Martínez

Abril 2015

ESQUEMA SEGURO PARA LA RED INALÁMBRICA DE LA UNIVERSIDAD DE MONTEMORELOS

Trabajo de investigación

Presentada en cumplimiento parcial de los requisitos para el grado de:

Ingeniería en Electrónica y Telecomunicaciones

Por

Jonathan Gamaliel Roblero Martínez

APROBADA POR LA COMISIÓN

Asesor Principal: M.C. Carlos Emilio Hernández Rentería	Director de Facultad: M.C. Alejandro W. García Mendoza
Miembro:	Coordinador de Pregrado M.C. Jair Arody del Valle López
Miembro:	Fecha de aprobación

DE CONTENIDO

Esquema seguro para la red inalámbrica de la Universidad de Montemorelos

Jonathan Gamaliel Roblero Martínez,

Facultad de Ingeniería y Tecnología, Universidad de Montemorelos

Montemorelos, Nuevo León, México

1130686@alumno.um.edu.mx

M.C. Carlos Emilio Hernández Rentería

Facultad de Ingeniería y Tecnología, Universidad de Montemorelos

Montemorelos, Nuevo León, México

Carlos.hdz@um.edu.mx

***Resumen*— La seguridad es un punto importante dentro de las redes principalmente en las redes Wi-Fi, los problemas de seguridad para la red inalámbrica día a día han incrementado, mayormente en el robo de información que circula pura la red afectando empresas, escuelas, personas, etc. Por ello se realizó el diseño** de **esquema de seguridad en la capa de acceso de la red Wi-Fi de la UM, dado que no existe dentro de la UM un esquema de seguridad, una política de uso de la red para los usuarios y a petición del departamento de sistemas e infraestrucutra de la UM, una vez elaborado el proyectó se consiguieron los siguientes resultados: mayor seguridad en la red, un buen uso de red, administración de usuarios y sus actividades, se realizó una política de uso y privacidad para la red, cumpliendo cabalmente con lo que el departamento de sistemas pedía.**

Palabras claves: Red, Seguridad, Wi-fi.

I. INTRODUCCIÓN

A. Antecedentes

La seguridad de las redes inalámbricas es un aspecto primordial que no sólo se considera en el ámbito del cómputo, actualmente las organizaciones y sus sistemas de información se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes por medios tecnológicos, espionaje, sabotaje, vandalismo. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados [1].

Las redes Wi-Fi (Wireless Fidelity), basadas en estándares IEEE 802.11b/g se han hecho muy populares en los últimos tiempos. Muchos usuarios han instalado redes inalámbricas en sus hogares, empresas, escuelas, etc. Y así han ido colocando puntos de acceso para proporcionar una mejor comodidad en el acceso a los datos y servicios de la red. Estas redes han proporcionado a los hackers nuevas oportunidades para conseguir acceso no autorizado a los sistemas corporativos y sus datos, favorecido por las características específicas tanto del medio de transmisión como del tráfico que por la red circula [1].

Las redes Wi-fi conducen al desarrollo de nuevas soluciones de seguridad alternativas a la inicialmente existente *Wired Equivalent Privacy* (WEP) para proteger las redes Wi-Fi y proporcionar a los usuarios la garantía que necesitan para sus sistemas y datos [2]. El enorme interés que suscita, en general, el tema de seguridad y más específicamente en el ámbito de las redes Wi-Fi hacen que sea un área de gran actividad tanto investigadora como de aplicación.

En la Universidad de Montemorelos se consideran parte de los activos críticos los sistemas de conexión para el acceso al internet, no sólo porque alojan información sensible, sino también porque son parte importante del proceso de educación de

los alumnos, actualmente no se les da el suficiente resguardo por falta de un esquema seguro en la red.

Es en este marco de interés en el que se presenta este trabajo, se tiene como fin hacer una aportación importante al departamento de sistemas. Incluimos, en primer lugar, una breve descripción de dichas redes, también se hará una política de uso de la red Wi-fi, aplicaciones móviles basados en los principios de nuestra casa de estudio, culminando así con el esquema de seguridad para la red inalámbrica de la Universidad de Montemorelos.

B. Definición del problema

La poca seguridad en la red WLAN que tiene la Universidad de Montemorelos, es la principal motivación de este proyecto; existen deficiencias, la falta de un esquema de seguridad, la falta de equipos para realizar un esquema en la red WLAN de nuestra universidad haciendo de ella vulnerable ante los ataques que puedan presentarse para la red.

Actualmente la seguridad se ha convertido en uno de los problemas que presenta nuestra casa de estudio en el acceso a la red Wi-Fi, dado que solo cuenta con un esquema de seguridad que es un usuario contraseña para tener acceso a internet, en base a la petición del departamento de sistemas e infraestructura de la UM se va a realizar el proyecto para un esquema de seguridad de la red Wi-Fi para la UM.

Varios elementos han contribuido a la realización del proyecto, el hecho de que se utilice un medio de transmisión compartido con poco control de las personas o dispositivos con capacidad de acceso a dicho medio, la novedad de las redes sociales, y una política inexistente en la UM para el manejo y uso de la red inalámbrica, que ha primado su buen uso y ha dejado de lado aspectos relativos a su seguridad. Hoy en día se está realizando un gran esfuerzo en el desarrollo de estándares y tecnologías que eviten estos problemas de seguridad, manteniendo la filosofía de una conexión móvil.

C. Justificación

Las redes inalámbricas de área local, tienen un papel cada vez más importante en las comunicaciones del mundo. Debido a su facilidad de instalación y conexión, el avance de estas tecnologías inalámbricas para el área de redes ha ido creciendo a tal punto que es imposible dejar de lado el uso, instalación y estándares de las redes inalámbricas.

Considerando que día a día la mayoría de los servicios brindados por cualquier organización, estas se están migrando a entornos que involucran el uso de equipos de cómputo, servidores y redes de datos, en base a las tecnologías inalámbricas [2].

También se debe considerar los múltiples ataques que sufren las organizaciones, enfocados al robo de información, falsificación, modificación, denegaciones de servicio, suplantaciones, vulnerabilidades en sistemas, uso de equipos de cómputo para actividades maliciosas, entre muchas otras, debido a un descuido de manera intencional [3].

En la actualidad existen distintos sistemas de envío de datos de forma inalámbrica, por ello se hará referencia a la red Wi-Fi, la cual está basada en la tecnología inalámbrica fácilmente. Sin embargo un elevado porcentaje de redes inalámbricas instaladas por administradores de sistemas o de redes por su simplicidad de implementación, sin tener consideración la seguridad y por tanto han convertido la red en una red abierta, sin proteger el acceso a la información que por ellas circulan, haciendo que ésta sea vulnerable a los atacantes y que la información que circula en ella no esté totalmente protegida [4].

Existen una serie de ideas generalizadas respecto a la seguridad de los sistemas en general, y perfectamente aplicable a las redes WIFI, que suelen resultar fatales a corto o medio plazo, tales como: “nadie conoce el sistema”, o “nadie tiene interés en el sistema”, así pues ¿para qué gastar recursos y tiempo en protegerlo?. Por desgracia, la experiencia demuestra que ninguno de ambos razonamientos resulta cierto, y que efectivamente hay más personas de las que en un principio parece que conocen de la existencia de ese sistema, y además, tienen intereses en él. Las consecuencias más comunes de ataques a redes WIFI son [5]:

1) Consumo de ancho de banda: Ahora mismo resulta sorprendentemente sencillo conseguir una conexión a una de las muchas redes inalámbricas desprotegidas, y sólo un poco más difícil a alguna de las protegidas con algún tipo de medida mínima. Como consecuencia de este tipo de acceso no autorizado, el ancho de banda

de las correspondientes redes WIFI se ve claramente mermado, más aún si éstas son utilizadas como medio de acceso a conexiones de tipo ADSL, cable módem, etc.

2) Acceso no autorizado a equipos: En general, las protecciones frente a equipos externos a la red local suelen ser más fuertes que aquellas que se aplican frente a equipos que pertenecen a la misma red local. De ahí, que en el momento que un equipo no autorizado se conecta a la red inalámbrica, los equipos que se encuentran conectados a dicha red y los que se encuentran en la misma LAN, suelen ser muy vulnerables. Las consecuencias de un acceso no autorizado a un equipo, puede provocar: el robo o destrucción de datos almacenados en dicho equipo, el robo de claves y contraseñas de acceso a cuentas bancarias, certificados personales, etc.

3) Responsabilidades legales: Como se ha comentado anteriormente, la instrucción en la red inalámbrica suele hacer mucho más vulnerables a los equipos de esa misma LAN, lo que facilita el acceso no autorizado. A partir de aquí, un equipo atacado puede servir como equipo atacante de sistemas remotos, esto podría dar lugar a responsabilidades legales si se considera que el propietario de la red WIFI o la persona que la ha instalado lo ha hecho de manera descontrolada y sin tener en cuenta ningún tipo de medida de seguridad preventiva.

Dada la situación de la falta de un esquema de seguridad en la UM, se debe realizar uno basado en las necesidades de sus servicios y objetivos. No olvidando que se debe contar con una política para el uso de la red Wi-Fi de la UM.

Sabiendo que la UM no cuenta con un registro de ataques a la red Wi-fi, tampoco con un esquema de seguridad establecido en la oficina encargada (Sistemas) y no existiendo una política escrita dentro de la reglamentación del estudiante para el uso de la red Wi-fi, se considera realizar este proyecto para cubrir esas deficiencias.

D. Objetivos

- Diseñar un esquema de seguridad en capa de acceso para la red inalámbrica de la Universidad de Montemorelos.
- Administrar los datos y promover un buen uso de la red.
- Realizar una política de uso de red y aplicaciones para los estudiantes, de acuerdo a la filosofía de la universidad.

E. Hipótesis

Es posible hacer un esquema de seguridad que permita resguardar la información de los usuarios de la Universidad de Montemorelos cayendo en los registros escolares, base de datos de sus trabajadores, inventario, nómina, publicaciones educativas, así como garantizar la disponibilidad de los servicios tanto para académicos, administrativos y alumnos.

Buscando limitar las actividades que no tengan ninguna relación con la finalidad de la institución, tanto actividades de usuarios internos o visitas que tengan acceso a la red de la UM.

II. FUNDAMENTOS TEÓRICOS

A. Marco Teórico.

La seguridad es una de las principales preocupaciones de las empresas que están interesadas en implementar redes inalámbricas [5]. Afortunadamente, tanto el conocimiento de los usuarios sobre la seguridad como las soluciones ofrecidas por los proveedores de tecnología están mejorando, cuando estas redes cuentan con una protección adecuada, las compañías pueden aprovechar con confianza las ventajas que ofrecen [6]. "Los proveedores están haciendo un gran trabajo para mejorar las funciones de seguridad, y los usuarios están obteniendo conocimiento de la seguridad inalámbrica", afirma Richard Webb [6], analista de orientación para redes de área local inalámbricas (LAN) de Infonetics Research.

De hecho, la seguridad es el principal obstáculo para la adopción de redes LAN inalámbricas. Y esta preocupación no es exclusiva de las compañías grandes. En lo que respecta a la conexión de redes inalámbricas, "la seguridad sigue siendo la preocupación nº 1 de las compañías de todos los tamaños", afirma Julie Ask, directora de investigaciones de Jupiter Research [6].

Cuando se habla de seguridad para una red Wi-Fi es bueno mencionar que existen distintos tipos de ataques hacia la misma, dentro de las que se mencionarán las más comunes. Tipos de ataques comunes:

1) Phishing

Conocido también como suplantación de marca, el ataque de phishing consiste en suplantar a una persona u organización con el fin de obtener información de una víctima que esté relacionada con la entidad suplantada. Ésta permite obtener correos, código de páginas que incluyan el dominio y hostings de un determinado dominio [7].

2) Cross-Site scripting (XSS)

Los datos se incluyen en el contenido dinámico que se envía a un usuario de la web sin ser validado por código malicioso.

El contenido malicioso enviado al navegador web a menudo toma la forma de un segmento de Java Script, pero también puede incluir HTML, Flash o cualquier otro tipo de código que el navegador puede ejecutar. La variedad de los ataques basados en XSS es casi ilimitada, pero normalmente incluyen la transmisión de datos privados, como las galletas o cualquier otra información de sesiones a la atacante, la reorientación de la víctima a la página web controlado por el atacante, o la realización de otras operaciones maliciosos en la máquina del usuario en la apariencia del sitio vulnerable [7].

3) Session Hijacking

Un secuestro de sesiones se da cuando un atacante logra colocarse entre dos máquinas, y apoderarse de la sesión establecida entre ambas. Los atacantes pueden hacerse de nuestras cuentas capturando las contraseñas que viajan por el aire, tanto en texto plano como encriptados, la comunicación sucede en tiempos diferidos.

De esta forma, el cliente envía una petición, el servidor la recibe y envía una respuesta con las cabeceras**HTTP.** Los ordenadores no sólo sirven para procesar información almacenada en soportes físicos en cualquier formato digital, sino también como herramienta para acceder a información, a recursos y servicios prestados por ordenadores remotos, como sistema de publicación y difusión de la información [7].

4) HeartBleed

El fallo Heartbleed es una vulnerabilidad importante de la librería de software criptográfico OpenSSL. OpenSSL es una implementación del protocolo de cifrado SSL/TLS utilizado para proteger la privacidad de las comunicaciones en Internet. OpenSSL se utiliza en muchos sitios Web y en otras aplicaciones como el correo electrónico, la mensajería instantánea o las redes VPN.

La vulnerabilidad Heartbleed permite a un atacante leer la memoria de los sistemas mediante determinadas versiones de OpenSSL, con lo que potencialmente le facilita el acceso a los nombres de usuario, las contraseñas o incluso a las claves criptográficas secretas del servidor utilizado por SSL. Al obtener estas claves, los usuarios maliciosos podrían observar todas las comunicaciones de ese sistema, lo que les permitiría explotar más vulnerabilidades [7].

Cuando se habla de ataques también se puede mencionar que existe distintas tecnologías que se puede analizar cuidadosamente para poder definir cuál es la que nos aporta más para obtener la seguridad que se busca en la red Wi-fi de la universidad.

Se han establecido un conjunto de criterios de evaluación basado en las tendencias empresariales y tecnológicas. Concretamente, se habrá examinado la capacidad que tiene cada proveedor de satisfacer los requisitos de precio-rendimiento, capacidad de recuperación, seguridad y capacidad de gestión que plantea la conectividad de red de campus emergente en función de los siguientes criterios:

- Garantizar un acceso de los usuarios sencillo, seguro y rentable
- Proporcionar ancho de banda y calidad de servicio adecuados
- Optimizar la implementación y las operaciones

- Ofrecer compatibilidad con los estándares y requisitos tecnológicos emergentes
- Ofrecer experiencia y valor a la empresa

Buscando una tecnología que nos permita poder cumplir con los requisitos básicos de seguridad para la universidad se realizó la siguiente comparativa:

Con las tecnologías de las marcas: HP, CISCO, RUCKUS Y ARUBA.

1) *Análisis de los proveedores HP:*

Acceso unificado cableado e inalámbrico: HP ofrece una cartera estrechamente integrada de soluciones de acceso cableadas e inalámbricas que incluyen hardware, un solo sistema operativo y gestión uniforme. El software Intelligent Management Console (IMC) de HP proporciona gestión multiproveedor desde una pantalla única para todos los productos de red cableada e inalámbrica de HP, que incluye la incorporación, el aprovisionamiento y la supervisión de dispositivos móviles. La incorporación se realiza en función de la identidad de los dispositivos (ubicación, hora y estado de seguridad del dispositivo) así como mediante el control de acceso a la red 802.1x. La cartera unificada elimina el coste y la complejidad administrativa, al tiempo que garantiza experiencias de usuario homogéneas y una conectividad sin interrupciones en toda la empresa [8].

Seguridad de red: HP ofrece sólidas funcionalidades de gestión de la identidad y seguridad de extremos. Los conmutadores de red cableada e inalámbrica unificada y los puntos de acceso de WLAN incluyen funcionalidades integradas de detección (WIDS) y prevención de intrusiones (WIPS), lo que amplía la seguridad hasta el extremo de la red, mientras elimina la necesidad de dispositivos IDS/IPS dedicados. Se admiten tres modos de implementación de IDS/IPS claramente diferenciados para satisfacer los requisitos de los clientes. El acceso seguro basado en identidad se simplifica gracias a la incorporación y el aprovisionamiento de los dispositivos utilizando el software IMC de HP [8].

2) *Análisis de los proveedores CISCO:*

Acceso unificado cableado e inalámbrico: Cisco ofrece una gama integrada de productos de acceso cableado e inalámbrico basado en las instalaciones. Comparten una misma plataforma de gestión, Prime, a través de la cual se gestionan todas las funciones de la conectividad de red. La incorporación de dispositivos cableados e inalámbricos requiere una plataforma independiente, ISE (Identity Services Engine). La solución de Cisco es exhaustiva, pero no está totalmente integrada, y por tanto requiere servidores y dispositivos adicionales para ofrecer una funcionalidad básica [8].

Cisco ofrece además soluciones inalámbricas Meraki gestionadas en la nube. Las soluciones Meraki no están integradas con el resto de la gama de productos de Cisco y no son compatibles con el acceso cableado e inalámbrico unificado [8].

Seguridad de red: La plataforma de gestión Prime de Cisco es compatible con funcionalidades WIDS/WIPS. La funcionalidad WIPS adaptativa proporciona una detección de intrusiones más sólida frente a una mayor variedad de amenazas, pero requiere un dispositivo Mobility Service Engine (MSE) adicional [8].

Los puntos de acceso son compatibles con supervisión sobre el aire superpuesta (overlay) y por intervalos (time-slicing). La incorporación segura de dispositivos se proporciona mediante un componente ISE (Identify Services Engine) independiente [8].

3) *Análisis de los proveedores RUCKUS:*

Acceso unificado cableado e inalámbrico: Ruckus es un proveedor exclusivamente de Wi-Fi que no ofrece productos de infraestructura cableada ni de gestión de políticas centralizadas.

Seguridad de red: Ruckus proporciona una funcionalidad WIDS limitada. La mitigación requiere la intervención manual de un administrador tras la detección del intruso. El enfoque de Ruckus de la incorporación y el aprovisionamiento seguro de nuevos dispositivos inalámbricos utiliza claves previamente compartidas dinámicas (DPSK, Dynamic Pre-Shared Keys). Cada clave se empareja con un dispositivo concreto para su gestión y supervisión. Este enfoque presenta limitaciones que pueden resultar complicadas de gestionar.

4) *Análisis de los proveedores ARUBA:*

*A*cceso unificado cableado e inalámbrico: Aruba está centrada principalmente en el mercado

de acceso a la LAN inalámbrica. La empresa ofrece dos aplicaciones de gestión de red diferenciadas. AirWave™ proporciona gestión FCAPS multiproveedor para infraestructura WLAN de campus (así como soporte limitado para infraestructuras cableadas). La aplicación independiente ClearPass proporciona control de acceso a la red y gestión de políticas para dispositivos/usuarios móviles [8].

a) Tecnología de controlador virtual

La tecnología de controlador virtual de Aruba Instant proporciona funciones de calidad empresarial, como calidad de servicio (QoS) automática, autenticación 802.1X, aplicación de normativas basadas en dispositivos y funciones, protección frente a conexiones pirata y Adaptive Radio Management™ (ARM™), lo que optimiza el funcionamiento del cliente Wi-Fi asegurándose de que los AP no sufran interferencias RF [9].

b) Facilidad de implantación

Aruba Instant está en funcionamiento en minutos. Desde un portátil, solo hay que establecer una conexión inalámbrica con una SSID para realizar la provisión inalámbrica en cuestión de minutos. Si desea ampliar la cobertura inalámbrica, solo tiene que instalar más AP Aruba Instant; las configuraciones se distribuyen automáticamente desde el controlador virtual [9].

c) Gestión y visibilidad

Se pueden gestionar varias redes Aruba Instant de forma segura y centralizada mediante AirWave, lo que permite a Aruba Instant funcionar en cientos de lugares distribuidos. Con AirWave, el departamento de TI dispone de una visibilidad en tiempo real de los usuarios, los dispositivos móviles, y la infraestructura con cable e inalámbrica, desde una única consola de gestión [9].

El Aruba Instant multifunción se puede configurar para ofrecer acceso WLAN con supervisión de la conexión a tiempo parcial, supervisión dedicada de la conexión para IPS inalámbrico, y análisis de espectro o función de malla empresarial segura [9].

d) Protección de la inversión

Puesto que los requisitos de las redes WLAN y de las aplicaciones cambian con el tiempo, Aruba Instant permite la migración a una arquitectura centralizada de controlador de movilidad con una capacidad de hasta 2048 AP.

e) Aplicación

AP de doble banda, radio única o doble 802.11n rentable para interiores, ideal para instalaciones de cualquier densidad, desde baja a extremadamente alta.

f) Seguridad de red:

Las funcionalidades WIDS/WIPS de Aruba permiten una sólida aplicación de la seguridad en el extremo de la red, que incluye la mitigación de acciones ilegales y la supervisión sobre el aire superpuesta (overlay) o por intervalos (time-slicing). Un módulo de software independiente en el controlador RFProtect® permite configurar y aplicar políticas de red/seguridad. ClearPass proporciona incorporación y aprovisionamiento seguro de dispositivos. [9]

g) Conclusión del análisis de tecnologías:

De los cuatro proveedores analizados en este informe, Cisco y HP ofrecen por lejos las más amplias carteras de redes de campus. Ambos ofrecen una amplia gama de soluciones de redes de campus, como los productos de acceso cableados/inalámbricos, los conmutadores L2/l3 de núcleo y de distribución y las aplicaciones de gestión unificada.

Cisco tiende a favorecer una solución de proveedor único, mientras que HP ofrece una cartera más abierta con capacidades de gestión de proveedores múltiples y un compromiso más fuerte con los estándares abiertos como OpenFlow. Ambos proveedores también ofrecen una amplia gama capacidades de distribución, consultoría y asistencia global, tanto directamente como a través de una vasta red de socios [10].

Aruba y Ruckus están centrados más específicamente en el mercado de acceso inalámbrico. Por lo que la determinación de la tecnología se basó más en lo que buscamos que es seguridad inalámbrica wifi.

Aruba también ofrece una solución de gestión de proveedores múltiples escalable que mejora la administración de las redes mixtas

Un esquema de seguridad basada en la tecnología de ‘’ARUBA” puede complementar lo siguiente:

Con la ayuda de la tecnología de Aruba se podrá plantear un esquema que nos permita más seguridad en la red inalámbrica de la universidad dándonos los siguientes beneficios:

Acceso unificado cableado e inalámbrico: Aruba está centrada principalmente en el mercado de acceso a la LAN inalámbrica. La empresa ofrece dos aplicaciones de gestión de red diferenciadas. AirWave™ proporciona gestión FCAPS multiproveedor para infraestructura WLAN de campus (así como soporte limitado para infraestructuras cableadas). La aplicación independiente ClearPass proporciona control de acceso a la red y gestión de políticas para dispositivos/usuarios móviles. [11]

Aruba Instant™ virtualiza las funciones del controlador de movilidad de Aruba en puntos de acceso (AP) 802.11n, lo que crea una red LAN inalámbrica (WLAN) de nivel empresarial repleta de funciones con la asequibilidad y sencillez de configuración de una red Wi-Fi básica.

Gracias a su impresionante capacidad de ampliación, Aruba Instant se puede instalar en un único sitio o en varios lugares distribuidos geográficamente. Se puede gestionar un grupo de hasta 16 AP Aruba Instant mediante un AP único, designado como controlador virtual. Se pueden gestionar varias redes de controlador virtual mediante el sistema de gestión Aruba AirWave™.

Controladores de LAN inalámbrica: La función principal es el reenvío de paquetes de datos centralizado a través del controlador, aunque también admite el reenvío distribuido. La itinerancia rápida (menos de 50 mseg) de capa 3 y la tecnología Client Match garantizan un sólido rendimiento de la itinerancia. Se incluye también un paquete completo de características de gestión de recursos de radio así como una amplia variedad de configuraciones de alta disponibilidad. La plataforma de nube Meridian de Aruba admite servicios de ubicación tanto Wi-Fi como de balizas de Aruba [11].

En base a los distintos tipos de access point que la empresa de Aruba maneja se determinó que el más conveniente para el esquema es el: Aruba instant 205, el cual brinda de los siguientes beneficios únicos:

- Optimización de cliente Wi-Fi, brinda una señal óptima mientras los usuarios se desplazan.
- Reúne parámetros de rendimiento de sesiones desde dispositivos móviles.
- Si un dispositivo se aleja de un punto de acceso o si RF la interferencia impide el rendimiento, automáticamente brinda al dispositivo una mejor AP.
- Calidad de servicio para aplicaciones de comunicaciones unificadas.
- Un único punto de acceso se distribuye en la red, brinda una configuración única de puntos de acceso a la WLAN y su configuración es única desde el mismo access point.
- Configuración de seguridad desde su interfaz (controlador virtual).
- Configuración de restricción y bloqueo de páginas indebidas.
- Configuración de restricción y bloqueo de aplicaciones restringidas por políticas de la universidad.
- Monitoreo constante del acceso de usuarios y control de sus accesos.
- Monitoreo constante que permite ver cuando alguien quiere realizar una actividad prohibida dentro de la red.

B. Estado del arte

La elaboración de estudios acerca del conocimiento producido de la seguridad de las redes Wi-Fi es relativamente reciente. Se han manejado distintos métodos de esquemas de seguridad basados en los siguientes tipos:

1) Wardriving

Es un método para redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como una laptop o un PDA. El método es simple y consiste en que el atacante simplemente pasea con el dispositivo móvil y en el momento en que se detecta la existencia de una red, realiza un análisis de la misma ubicando los puntos de acceso con sus datos (SSID, WEP, direcciones MAC, entre otros).

Para realizar el wardriving se necesita pocos recursos. Los más habituales son una laptop con una tarjeta inalámbrica, un dispositivo GPS el cual es usado para ubicar el AP en un mapa de coordenadas, opcionalmente una antena direccional para re-

cibir el tráfico de la red desde una distancia considerable y software apropiados para verificar puntos de acceso como por ejemplo: AirSnort, Kismet, AirTools o NetStumber, entre otros [12].

2) Warchalking

Se trata de un lenguaje de símbolos utilizados para marcar sobre el terreno la información que fue recopilada en el Wardriving, es decir, difundir la existencia de redes inalámbricas; de forma que puedan ser utilizadas por aquellas personas interesadas que pasen por el lugar. Su simbología es la siguiente:

SSID
)(
Nodo Abierto
Ancho de banda

SSID
0
Nodo cerrado

SSID Contacto
(w)
Nodo WEP
Ancho de banda

Primeramente se identifica el nombre del nodo o el SSID, luego se identifica el tipo de red, bien sea abierta, cerrada o con WEP, y por último se especifica la velocidad máxima de la red [12].

3) Osa

Este mecanismo consiste en autenticar todas las peticiones de los usuarios. OSA consta de dos pasos; el primero consiste en que la estación que quiere autenticar con otra o con el AP (access point), le envía una una trama que contiene la identidad (SSID Service Set Identifier) de esta estación emisora. El segundo paso, la otra estación (receptora) o el APC envía a la estación emisora otra trama que indica si se reconoció o no la identidad proporcionada por ella, dada la figura 1 podemos observar su esquema.

El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de encriptación [12].

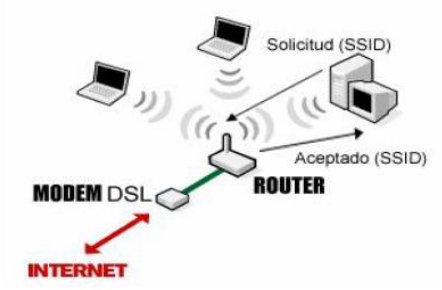


Figura 1. Esquema de seguridad del modelo OSA

4) SKA

Este mecanismo se basa en cada que estación debe poseer una clave compartida, la cual es recibida a través de un canal seguro e independiente de la red 802.11; por lo que cada estación que posea una clave va a poder autenticarse con otra por medio de un (secreto) compartido. WEP es el algoritmo de encriptación utilizado en este mecanismo. Dada la figura 2 podemos observar su esquema [12].

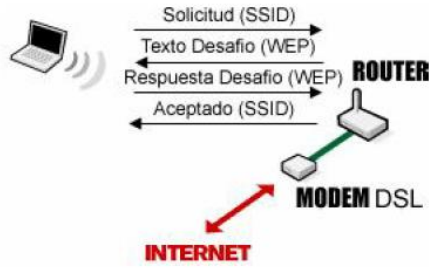


Figura 2. Esquema de seguridad del modelo SKA

5) Filtrado por direcciones MAC

Como parte del éstandar 802.11, cada interfaz de radio o dispositivo tiene una única dirección MAC asignada por el fabricante. Para incrementar la seguridad inalámbrica es posible configurar el AP (Access point) para que acepte solo ciertas direcciones MAC y bloquee todas las demás, es decir, se crea una lista de direcciones MAC que serán permitidas por el AP para conectarse. Esta técnica puede ser muy compleja si es implementada, por lo que se recomienda usar en redes pequeñas.

El filtrado por MAC es una medida básica para evitar que el primero que se encuentre dentro del

área de captación del AP, pueda acceder a la red, lo cual resulta muy efectivo para prevenir accesos no autorizados.[13]

6) WPA-PSK Y WPA-Enterprise

WPA (Wireless Protected Access), es un sistema para proteger las redes inalámbricas Wi-Fi, creado para corregir las deficiencias del sistema previo WEP.

WPA usa un password maestro a través del cual el sistema genera claves para cifrar el tráfico de la red, que cambian continuamente usando el protocolo TKIP; además las claves nunca son rehusadas eliminando el riesgo de que puedan ser descubiertas. Incluye también los beneficios de autenticación del estándar 802.1x, lo que le permite al sistema checar quien se está registrando contra una base de datos central de usuarios conocidos. Este sistema ofrece dos métodos de autenticación de usuario y manejo de claves:

- WPA-PSK (WPA pre-shared key) normalmente usado en ambiente donde no se cuenta con servidores de autenticación. Se usan claves pre-compartidas estáticas a partir de las cuales se generan nuevas claves de encriptación usando protocolo TKIP. Con la autenticación PSK, los usuarios deben introducir la clave maestra manualmente en los puntos de acceso e introducir clave en cada dispositivo cliente que acceda a la red inalámbrica.
- WPA-Enterprise (WPA Empresarial): este caso se requiere de un servidor de autenticación como punto final y el uso de EAP, teniendo en cuenta que también usa TKIP.[14]

7) Servidor de autenticación de RADIUS

RADIUS (Remote Authentication Dial-UP User Service), es un servidor de punto final que es responsable de recibir solicitudes de conexión y de la autenticación de los usuarios para luego retomar toda la información de configuración necesaria para el cliente. Este servidor desempeña la autenticación utilizando EAP. Una de las características importantes es la capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, pudiendo utilizar estos valores para generar estadísticas. Como se muestra en la figura 3 se puede observar su esquema y función.

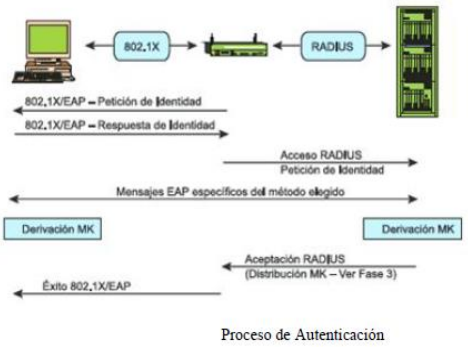


Figura 3. Esquema de seguridad del modelo RADIUS.

Actualmente existen muchos tipos de RADIUS, tanto comerciales como de código abierto [14].

III. RESULTADOS

A. Metodología.

Se realizó una entrevista con el Ing. Elifelet López, encargado del departamento de sistemas de la Universidad de Montemorelos, para saber acerca de la seguridad con la que se cuenta de forma interna.

Posteriormente al saber que la universidad no cuenta con dicha seguridad que pueda resguardar a los usuarios de la red Wi-Fi, teniendo nada más como seguridad el acceso al internet desde una usuario y contraseña. Después de conocer que la UM no cuenta con dicha seguridad se procede a realizar un esquema de seguridad, que permitirá a los usuarios estar protegidos en el uso de red Wi-Fi.

Se analizaron las tecnologías que actualmente existen en seguridad Wi-Fi y se compararon para ver cuál es la más conveniente de acuerdo a los requerimientos que pide la Universidad de Montemorelos, se analizaron las marcas líderes en el mercado como Cisco, Ruckus, Aruba, Hp y se tomaron en cuenta sus ventajas y desventajas que ofrecían para las necesidades del proyecto. Estas comparaciones se presentan en el marco teórico.

Una vez analizadas las tecnologías se apuesta por los ofrecimientos que da para la seguridad utilizar Aruba, se determina que el modelo Access

point 205-aruba es el ideal para realizar el esquema de seguridad.

Se procede a la configuración del Access point partiendo del acceso al controlador virtual que Aruba nos ofrece por default, en ese punto el Access point trae una dirección IP como se muestra en la figura 4.

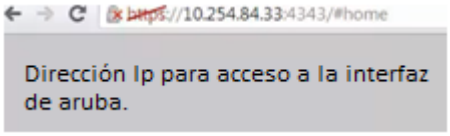


Figura 4. Dirección Ip para ingresar a la interfaz del AP.

Esta dirección una vez encontrada nos llevará a la página principal de la interfaz la cual se ve en la figura 5.

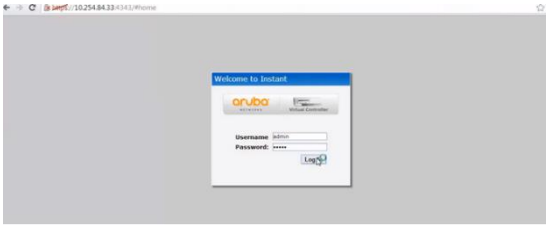


Figura 5. Login de acceso a la Interfaz AP.

Al ingresasr a la interfaz de Aruba se procede a crear un controlador virtual, ingresamos a donde dice: Virtual controller IP, una vez que se abre la ventana trae un cuadro para ingresar la dirección IP que nos proporciona el manual de Aruba y entonces poder activar el controlador.

Después de dicho proceso comenzamos con la configuración del Access point. Dentro de la interfaz se podrán observar, Access point conectados y al seleccionar el AP se podrá observar los usuarios conectados, también se podrá observar las redes que existen como se muestra en la figura 6, en este caso se haría por facultades y dentro de ellas distribuyendo los AP.

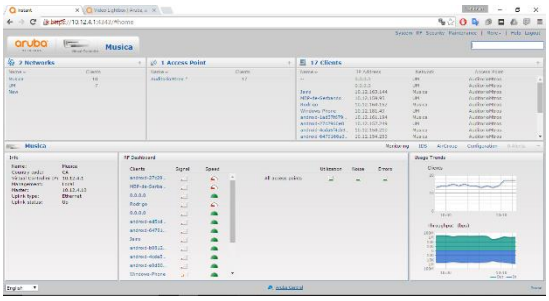


Figura 6. Interfaz AP.

En la configuración del Access point se procede a realizar los siguientes pasos:

Nos mostrará de inmediato todos los Access point que están conectados a la controladora virtual. Se selecciona un AP el cual tendrá un nombre y se selecciona para poder configurar. Así se muestra en la figura 7.

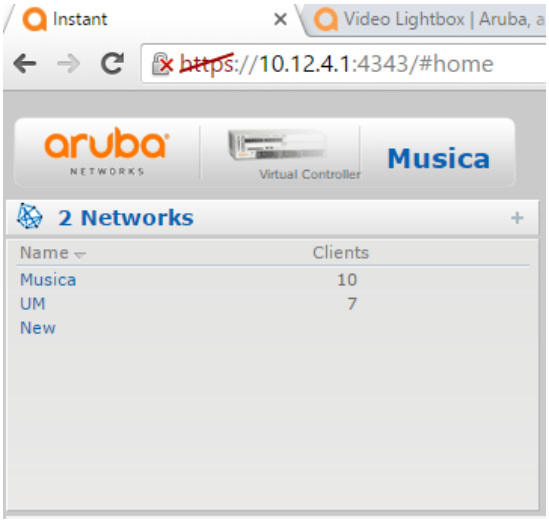


Figura 7. Access point contectados.

Una vez que se entre al “edit” del AP con “x” nombre tendremos que comenzar a configurar nuestro equipo, el cual está divido en 4 pasos: WLAN settings, VLAN, Security, Access.

Primer paso: WLAN settings, Aquí se selecciona el uso principal que se le dará al AP, la cual cuenta con 3 opciones: employee, voice y guest. Por lo que se selecciona “employee” que es el modo empleado que se usará como el AP master que referenciará la misma configuración a los demás AP mediante el controlador virtual. Se puede observar en la figura 8 el acceso al WLAN setting.

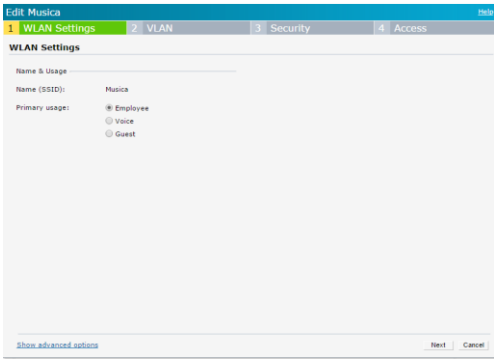


Figura 8. Cuadro de configuración del AP.

El segundo cuadro se presenta la configuración de las VLAN y asignaciones IP, se dan mediante una asignación por default pues el servidor que maneja la universidad es el encargado de realizar ese trabajo. Se puede observar el acceso en la figura 9.

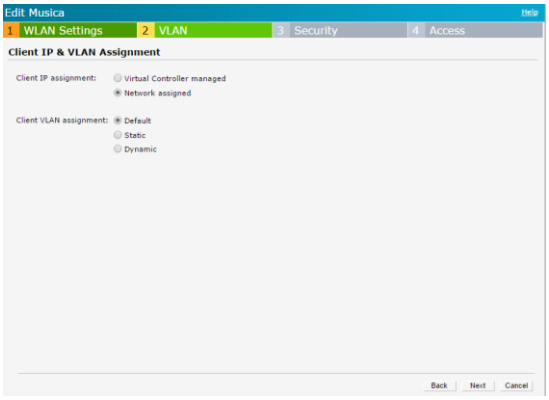


Figura 9. Configuración para direccionamiento.

En el tercer cuadro podremos configurar todo lo relacionado al tipo seguridad, desde ahí podremos elegir el tipo en 3 rangos que son los siguientes: open, personal y Enterprise, se selecciona el open puesto que es una red de acceso libre el que la universidad presenta, tomándose en cuenta que se tiene un login de usuario-contraseña se debe optar por dejar la red en open para no tener doble login al conectarse a la red Wi-fi..

En caso siguiente se procede a dejar en disabled que es incapacitar o que no actué el MAC authentication y blacklisting dado que todo se maneja y controla desde el servidor de la universidad

Posteriormente se procede a seleccionar el fast roaming que viene siendo el rango de alcance y velocidad por lo que se recomienda dejar en el 802.11r que adjudica a tener lo siguiente:

802.11r, también conocido como Fast BSS transition está enfocado a permitir la conexión continua a clientes en movimiento, pensando sobretodo en aplicaciones de VoIP. Ahora mismo, si nos alejamos de un punto acceso para entrar en otro, el proceso de reconexión puede ser automático, pero es lento, lo que no permite un uso fluido de la VoIP y provoca cortes de las comunicaciones.

Con la implementación de 802.11r se permitiría la transición entre distintos puntos de acceso de forma automática y rápida, con un tiempo de reconexión menor de 50 milisegundos, permitiendo a los clientes establecer la seguridad y la QoS que quieren usar en el nuevo punto antes de desconectarse del anterior. El acceso a esta configuración se ve en la imagen 10.

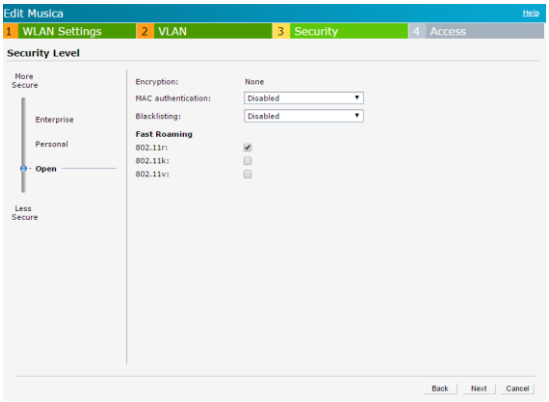


Figura 10. Niveles de seguridad.

El cuarto cuadro presenta la configuración de las reglas de acceso, cabe mencionar que ahí se procede a la restricción de las aplicaciones y bloqueo de páginas que nuestra casa de estudio prohíbe bajo el acuerdo de políticas de uso del internet que sostiene la hoja compromiso del estudiante.

Contiene 3 rangos de nivel de seguridad de acceso para el uso de aplicaciones y paginas indebidas las cuales se dividen en las siguientes: role based, networ based, unrestricted, en estos niveles se considera el uso de network based dado que es la opción recomendada en el esquema presentado por el departamento de sistemas en cuestiones de equipo, puesto que el rango alto que se presenta para configurar requiere de un esquema distinto

con equipos adecuados para ese tipo de configuración.

Una vez seleccionado el modo network-based se procede a entrar al recuadro donde se presenta el nombre de los AP, una vez seleccionado se ingresa al modo edit que es edición, posteriomente se mostrará el tipo de regla y servicio, donde se mostrarán las opciones de aplicación, categorías, reputación tanto de páginas web como de aplicaciones. Ahí se seleccionan las aplicaciones y páginas que la política restringe y bloquea, de acuerdo al uso de internet que presenta la universidad a los estudiantes, maestros y administradores.

Se seleccionan cuales se permiten y cuales se bloquean o restringen para realizar el buen uso de la red Wi-fi. Una vez seleccionado se procede a guardar la configuración. Se puede observar el ejemplo en la figura 11.

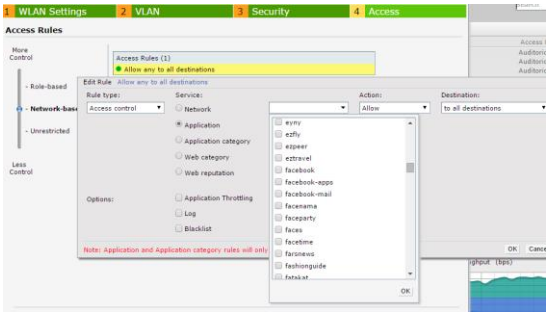


Figura 11. Configuración de bloqueo y restricción de páginas y aplicaciones.

Una vez realizado el bloqueo y restricciones se procede a verificar el orden jerárquico de las aplicaciones elegidas, se concluirá seleccionando “ok” y ahí quedará restringido todo lo seleccionado en base a la política que se realizó con vicerrectoría estudiantil. En la figurar 12 podemos ver claramente como se da el bloqueo y restricciones.

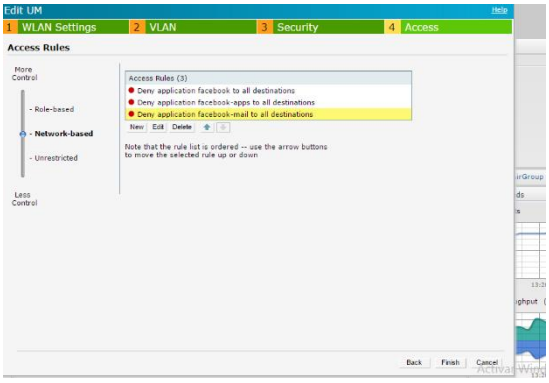


Figura 12. Listado de aplicaciones y páginas bloqueadas.

Después de la configuración del AP se regresa a la página principal donde nos enfocaremos al monitoreo del uso de aplicaciones, acciones indebidas, intensidad de señal, usuarios conectados y accesos, rendimiento, en lo que el principal objetivo es monitorear los ataques o accesos restringidos a las aplicaciones o paginas indebidas.

El acceso a lo que se restringe en la configuración nos mostrará inmediatamente la alerta, en base a los ataques o ingresos indebidos será el número de alerta, el AP tendrá la capacidad de bloquear ese canal de enlace para no permitir seguir conectado al internet. Dada la tecnología que usa el AP es una de las ventajas que este equipo y marca tecnológica nos permite realizar. En la figura 13 vemos el circulo donde se ven el número de ataques.

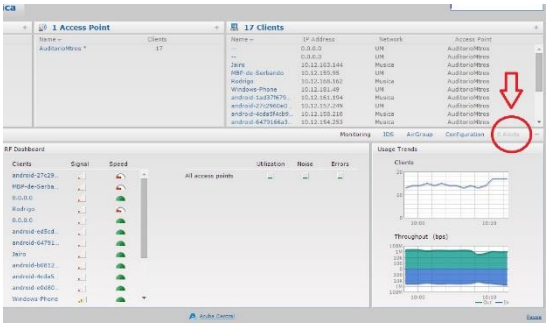


Figura 13. Círculo rojo, detección de ataques y violaciones a la configuración.

Dentro de sus características que se manejó en la configuración y lo que Aruba nos ofrece en sus AP, cabe mencionar que existen otras herramientas alternativas que pueden ayudar a la mejora de la seguridad, consiste en las siguientes:

1) *Perfiles de uso*

En esta parte se pueden realizar perfiles de acuerdo a las jerarquías en el control de acceso a la web y uso de aplicaciones, podemos definir los perfiles en 4 tipos siendo los siguientes: Administrador, maestros, alumnos e invitados. Dándoles a cada uno distintos tipos de acceso para proteger más nuestra red.

2) *Blacklist*

Conforme los usuarios vayan realizando uso indebido de la red Wi-Fi, podría castigarse de cierta manera poniéndolo en la blacklist que es la lista negra de usuarios que hacen actividades indebidas dentro de la red. En esta lista puede configurarse de tal modo que el acceso a ciertos usuarios sea limitado, siendo esta una herramienta importante del AP. En la figura 14 se puede observar la blacklist.

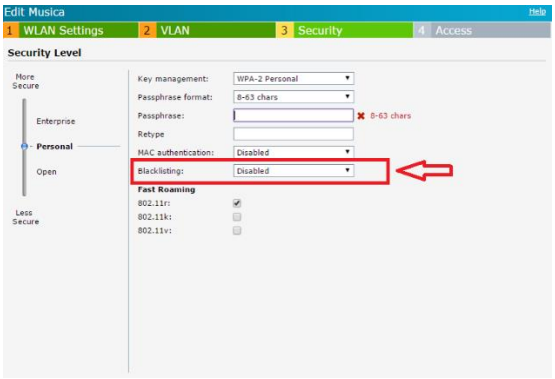


Figura 14. Blacklist

3) *Determinar plataformas usadas*

En esta herramienta se puede ver el sistema operativo con el que los usuarios están conectados a la red, esto nos ayuda para poder identificar ciertos huecos en la seguridad, haciendo de ello una herramienta para tener una lista de los huecos que puedan causar errores en nuestra seguridad.

4) *Graficas de uso*

Las gráficas de uso nos ayudan a saber características con la que los usuarios trabajan dentro de la red, podemos tomar en cuenta la velocidad con la que trabajan, el rendimiento de la red en el usuario, números de clientes conectados a la red con una actualización cada 10 minutos.

B. Presentación de los resultados.

Los resultados se dieron de acuerdo a los objetivos propuestos, como punto principal fue la realización del esquema de seguridad para la red Wi-Fi de la UM, basándonos en la capa de acceso. En la figura 15 observamos el esquema de seguridad.

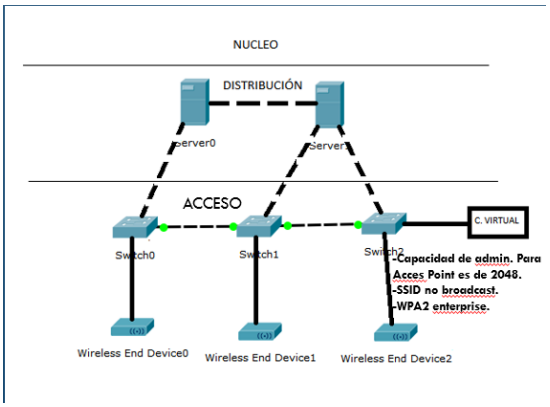


Figura 15. Esquema de seguridad de la red Wi-Fi UM.

Cuando se configuraron los AP se hicieron algunas pruebas de bloqueo a algunas páginas web, una de ellas fue a Facebook, tomando en cuenta que esta página estará bloqueada de acuerdo a la pólitica de privacidad que se entregó a Vicerrectoria estudiantil. Tomando en cuenta que la red Wi-Fi con acceso al internet es totalmente para el desarrollo profesional del estuidante. En la figura 16 vemos un claro ejemplo de el bloqueo de páginas.

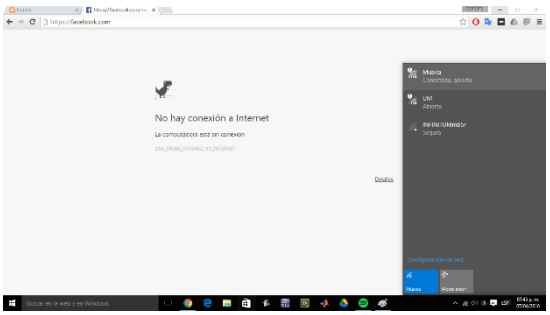


Figura 16. Conexión al AP aruba que tiene como nombre “música”.

Una vez conectado al AP correspondiente se comenzó el bloqueo de aplicaciones y páginas web que están dentro de los parámetros que la política de uso de la red en la UM se estableció. Véase figura 17.

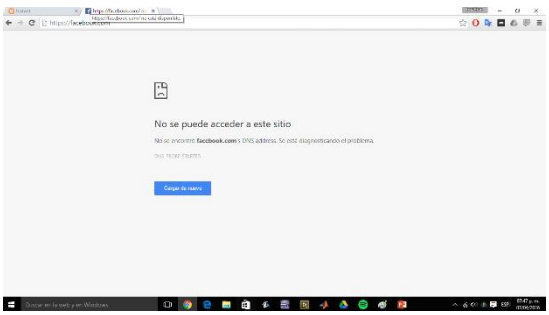


Figura 17. Acceso blqueado a Facebook.

De acuerdo a uno de los objetivos que se propuso se pudo administrar la red en cuestiones del ancho de banda para poder tener un acceso óptimo a las páginas educativas y de búsqueda para realizar tareas que son priorodad dentro de la política de uso de red para el estudiante. Se puede obervar en la figura 18.

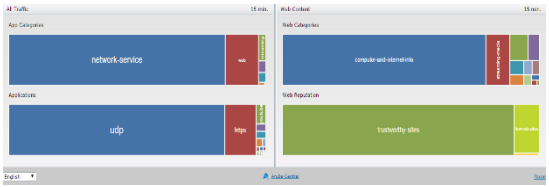


Figura 18. Control de manejo de ancho de banda.

A petición del departamento de vicerrectoría estudiantil, se elaboró una política de uso y privacidad para el uso de la red tomando como base la carta de compromiso que el estudiante firma cada semestre al ingresar. Tomando los siguientes puntos que corresponden al uso del tiempo y tecnología en la carta de compromiso.

Como alumno de la universidad de Montemorelos me comprometo a:

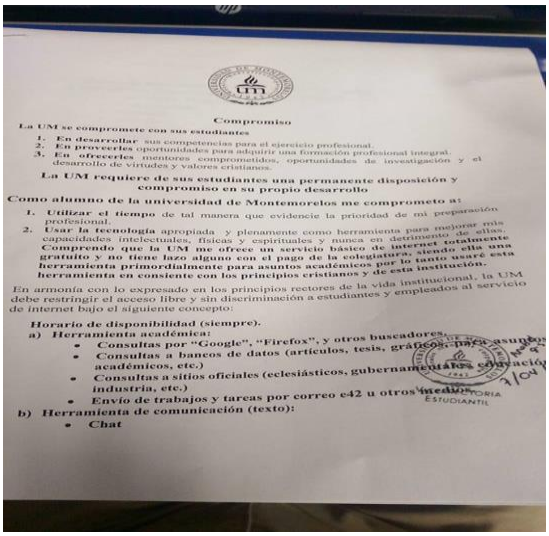
1) Utilizar el tiempo de tal manera que evidencie la prioridad de mi preparación profesional.
2) Usar la tecnología apropiada y plenamente como herramienta para mejorar mis capacidades intelectuales, físicas y espirituales y nunca en detrimento de ellas. Comprendo que la UM me ofrece un servicio básico de internet totalmente gratuito y no tiene lazo alguno con el pago de la colegiatura, siendo ella una herramienta primordialmente para asuntos académicos por lo tanto usaré esta herramienta en consiente con los principios cristianos y de esta institución.

En armonía con lo expresado en los principios rectores de la vida institucional, la UM debe restringir el acceso libre y sin discriminación a estudiantes y empleados al servicio de internet bajo el siguiente concepto:

Horario de disponibilidad (siempre).

a) Herramienta académica:
   - Consultas por “Google”, “Firefox”, y otros buscadores.
   - Consultas a bancos de datos (artículos, tesis, gráficos, para asuntos académicos, etc.)
   - Consultas a sitios oficiales (eclesiásticos, gubernamentales, educación, industria, etc.)
   - Envío de trabajos y tareas por correo e42 u otros medios.
b) Herramienta de comunicación (texto):
   - Chat
   - Correo electrónicos

   Horario de disponibilidad (3:00am-7:00am/ 7pm-11pm)
c) Herramienta de comunicación (video, voz y sonido):
   - Voz (Skype, Magic Jack, etc)
   - Video y sonido
   - Facebook
   - Youtube
d) Herramienta de entretenimiento
   - Juegos
   - Tv
   - Películas
   - Radio
   - Otros medios



Compromiso

La UM se compromete con sus estudiantes

1. **En desarrollar** sus competencias para el ejercicio profesional.
2. **En proveerles** oportunidades para adquirir una formación profesional integral.
3. **En ofrecerles** mentores comprometidos, oportunidades de investigación y el desarrollo de virtudes y valores cristianos.

La UM requiere de sus estudiantes una permanente disposición y compromiso en su propio desarrollo

Como alumno de la universidad de Montemorelos me comprometo a:

1. **Utilizar el tiempo** de tal manera que evidencie la prioridad de mi preparación profesional.
2. **Usar la tecnología** apropiada y plenamente como herramienta para mejorar mis capacidades intelectuales, físicas y espirituales y nunca en detrimento de ellas. **Comprendo que la UM me ofrece un servicio básico de internet totalmente gratuito y no tiene lazo alguno con el pago de la colegiatura, siendo ella una herramienta primordialmente para asuntos académicos por lo tanto usaré esta herramienta en consistente con los principios cristianos y de esta institución.**

En armonía con lo expresado en los principios rectores de la vida institucional, la UM debe restringir el acceso libre y sin discriminación a estudiantes y empleados al servicio de internet bajo el siguiente concepto:

Horario de disponibilidad (siempre).

a) **Herramienta académica:**
   - **Consultas por "Google", "Firefox", y otros buscadores.**
   - **Consultas a bancos de datos (artículos, tesis, gráficos, info. asuntos académicos, etc.)**
   - **Consultas a sitios oficiales (eclesiásticos, gubernamentales, corporación industria, etc.)**
   - **Envío de trabajos y tareas por correo e42 u otros medios.**

b) **Herramienta de comunicación (texto):**
   - **Chat**

Figura 19. Aceptación de la política de uso de la red.

C. Discusión.

Dentro del marco de investigación se encontró que se pretendía realizar el esquema de seguridad bajo una política inexistente de la UM, una vez que se presentó este problema con el Prof. Ekel Collins, el departamento de vicerrecotoria estudiantil hace la petición para que se pueda hacer una política de uso de la red.

En comparación con otros esquemas de seguridad podemos aclarar que en base a lo que existe se pudo aportar una innovación al esquema de seguridad para la capa de acceso debido que no se encontró información alguna donde hayan utilizado un esquema en base a la tecnología Aruba.

Muchos han implementado esquemas desde otras capas en la red, debido a las necesidad de su empresa, escuela u oficina, en este marco de investigación se realizó el esquema en base a la capa de acceso debido que es donde radica el problema principal en la UM.

El esquema de seguridad basado en la tecnología de Aruba hace diferencia de trabajos que se han realizado anteriormente, dada las características que esta presenta y mencionadas anteriormente. Podemos confirmar que este esquema cumple con los requerimientos establecidos.

En los trabajos a futuro podemos establecer los siguientes puntos:

- Instalación de los Access point Aruba instant 205 en toda la universidad.
- Comprar una controladora física para que evitar sobrecarga de trabajo al servidor actual.
- Realizar la instalación de la controladora y hacer el esquema a nivel “campus”.

REFERENCIAS

[1] Guzmán Mendoza Lovani, Medina García Alfredo, "Diseño de esquema de seguridad para la red inalámbrica de la empresa ACSA" 17 de mayo 2007.

[2] "Wi-Fi Alliance," Wi-Fi Alliance, [Online]. Available: http://www.wi-fi.org/. [Accessed 13 Septiembre 2015].

[3] Oscar Delgado Moatar "Protocolos y esquema de seguridad para redes Ad-hoc móviles inalámbricas. Leganés, España, Universdidad Carlos De Madrid, Nomviembre 2010.

[4] José Antonio Flores Torres, "Las tecnologías aplicadas en redes de computadores" Estudio de implementación de seguridad en la red WI-FI.

[5] García, F. T. Ética y Seguridad en la red.

[6] Aruba Case Study, Islamic University in madinah deploys, wireless network for students and staff.

[7] Ramírez Ascencio, E. (2014). *Vulnerabilidades en los sistemas académicos y sitios web de la Universidad de Montemorelos* (Doctoral dissertation).

[8] Aruba Networks, For T.G.I. Friday´s.

[8] Redes de campus convergentes, Comparación de las soluciones de Aruba Networks®, Cisco®, HP® y Ruckus Wireless®, Febrero de 2015

[9] Aruba Network, "La oficina completamente inalámbrica al alcance de las empresas: El uso de 802.11n Como Red Principal.

[10] Aruba Network, Red Aruba centrada en el usuario para la educación superior. **www.arubanetworks.com**

[11] http://www.networkworld.es/wifi/aruba-presenta-una-solucion-cloud-wifi-avanzada

[12] http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf Seguridad de las redes inalámbricas: Wardriving y Warchalking

[13] http://www.une.edu.ve/inproasune/esquema_tesis.htm

[14] http://www.une.edu.ve/inproasune/esquema_tesis.htm