

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

MAESTRÍA EN SEGURIDAD INFORMÁTICA APLICADA

“IMPLEMENTACIÓN DE UN RADIUS SERVER COMO MÉTODO DE AUTENTICACIÓN PARA TRABAJADORES CON ACCESO INALÁMBRICO DE UNA EMPRESA STARTUP UTILIZANDO RASPBERRY COMO PLATAFORMA PARA HARDWARE”

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

JOFRE JAVIER HARO BULGARIN

GUAYAQUIL – ECUADOR

2016

AGRADECIMIENTO

A Dios por darme apoyo cada día.

DEDICATORIA

Dedico el presente trabajo mi abuela Maria
por su apoyo incondicional.

TRIBUNAL DE SUSTENTACIÓN

RESUMEN

En el Capítulo 1 se presenta visión general de la situación actual de la empresa startup situada en la ciudad de Guayaquil en cuanto a la falta de un esquema de autenticación para sus trabajadores para acceder los recursos informáticos de la empresa y la solución propuesta.

En el Capítulo 2 se revisará la metodología del desarrollo de la solución del sistema de autenticación analizando la plataforma y metodología de autenticación seleccionada, de igual manera el software como aplicativo como mejor opción para aplicarse y las pruebas respectivas.

En el Capítulo 3 se analizará los resultados de las pruebas de lo recopilados en el capítulo 1 como análisis comparativo para confirmar las mejoras en el método de autenticación de esta empresa.

ÍNDICE GENERAL

AGRADECIMIENTO.....	ii
DEDICATORIA.....	iii
RESUMEN.....	v
ÍNDICE GENERAL.....	vi
ÍNDICE DE FIGURAS.....	viii
INTRODUCCIÓN.....	ix
CAPÍTULO 1.....	11
GENERALIDADES.....	11
1.1. Antecedentes.....	11
1.2. Descripción del problema.....	12
1.3. Solución Propuesta.....	14
CAPÍTULO 2.....	19
METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN.....	19
2.1. Modelos y protocolos de autenticación.....	19
2.2. Servidor de aplicaciones de autenticación.....	20
2.3. Desarrollo de Radius Server como plataforma de autenticación.....	22
2.4. Pruebas del sistema de autenticación con Radius Server.....	30
CAPÍTULO 3.....	33
ANÁLISIS DE RESULTADOS.....	33
3.1. Análisis comparativo.....	33
3.2. Análisis de los resultados obtenidos.....	35

CONCLUSIONES Y RECOMENDACIONES	36
BIBLIOGRAFÍA	40

ÍNDICE DE FIGURAS

Figura 1.1 Situación actual de la empresa	13
Figura 1.2 Solución propuesta para la autenticación con Radius Server.....	18
Figura 2.1 Flujo de comunicación del protocolo Radius Server.....	20
Figura 2.2 Distribución de Linux usada en plataforma Raspberry Pi.....	21
Figura 2.3 Capacidad y distribución en Raspberry con Raspbian.....	22
Figura 2.4 Update en librerías de Raspbian	23
Figura 2.5 Instalación de Apache	24
Figura 2.6 PHP fase 1.....	25
Figura 2.7 PHP fase 2.....	26
Figura 2.8 Instalación de MySQL	27
Figura 2.9 Configuración de IP estática para Radius Server en Router	28
Figura 3.1 Interface gráfica daloRADIUS	34

INTRODUCCIÓN

En la actualidad se tiene plena conciencia de los procesos de seguridad informáticos relacionados con los recursos informáticos y en especial con el contenido que estos poseen y que son de gran valor para las empresas del cual depende su funcionamiento y continuidad del negocio. [1]

La ISO/IEC 17799:2005 fue creada con el objetivo de poder llevar un mejor control de los recursos informáticos de una organización no importan la naturaleza del negocio que esta esté prestando a la sociedad. En este standard se da claramente reglas de cómo preservar la información así como la confidencialidad, la fiabilidad, autenticidad, fiabilidad y el no repudio. [1]

La sociedad en general debe proteger su información tanto personal como empresarial la cual puede ser usada para beneficios ajenos y como resultado afectara la continuidad del negocio afectando o no solo servicios privados sino también servicios gubernamentales que podría acarrear problemas como la falta de servicios de importancia fundamental para la generación de ingreso a los estados. [1]

El trabajo que presento detalla la situación actual de una empresa que inicia sus actividades con bajo presupuesto y que maneja información valiosa para su funcionamiento la misma está al alcance de sus empleados de manera continua, pero con un sistema de autenticación básico el cual hace notar la vulnerabilidad que esta empresa posee para manejar su sistema de información.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

Una empresa dedicada a la venta de insumos textiles domiciliada en la ciudad de Guayaquil ha iniciado sus operaciones la misma posee un presupuesto reducido y en especial lo asignado para su sistema de información, sus actividades las inicio en agosto del 2016 iniciando con un reducido personal de ventas el cual tiene contacto directo con el cliente final el cual se clasifica al por mayor y al por mejor.

Esta empresa tiene desarrollado un método de autenticación básico para que los trabajadores accedan a los recursos informáticos y accedan vía inalámbrica para distintas tareas entre ellas revisión, control y venta de su inventario los cuales se basan en insumos textiles de alta calidad y un valor elevado lo cual hace que la empresa

tenga un método de autenticación considerable en función de proteger sus viene.

1.2. Descripción del problema

Debido al presupuesto limitado que tiene esta empresa startup la cual se dedica a la venta de materiales en la industria textil, decidió que su red de acceso sería solo tipo wireless. Esta empresa startup tiene una infraestructura básica y rudimentaria de Internet, con relación a la parte de autenticación de los trabajadores, estos acceden a la Internet de la empresa a través de tres access point los cuales poseen un único SSID. Los trabajadores en gran mayoría son asesores de ventas, personal administrativo y operativo.

Todo el personal de la empresa tiene equipos asignados para tener acceso directo a la base de datos del inventario que posee la empresa. En la figura 1.1 podemos observar la infraestructura de Internet que tiene la empresa. Esta empresa con poco tiempo en el mercado ha sufrido varias intrusiones de personas ajenas a la empresa debido que algún trabajador ha compartido las credenciales de acceso a la red wireless.

Como primera medida ha decidido que solo los equipos asignados a la nómina de los trabajadores deberían acceder a la red de la empresa, pero esta medida lo ha logrado de manera parcial debido que no tiene personal técnico que tenga conocimiento de acceder las MAC ADDRESS en los access point y los mismo tienen limitación en la cantidad de estas que puedan ser ingresadas.

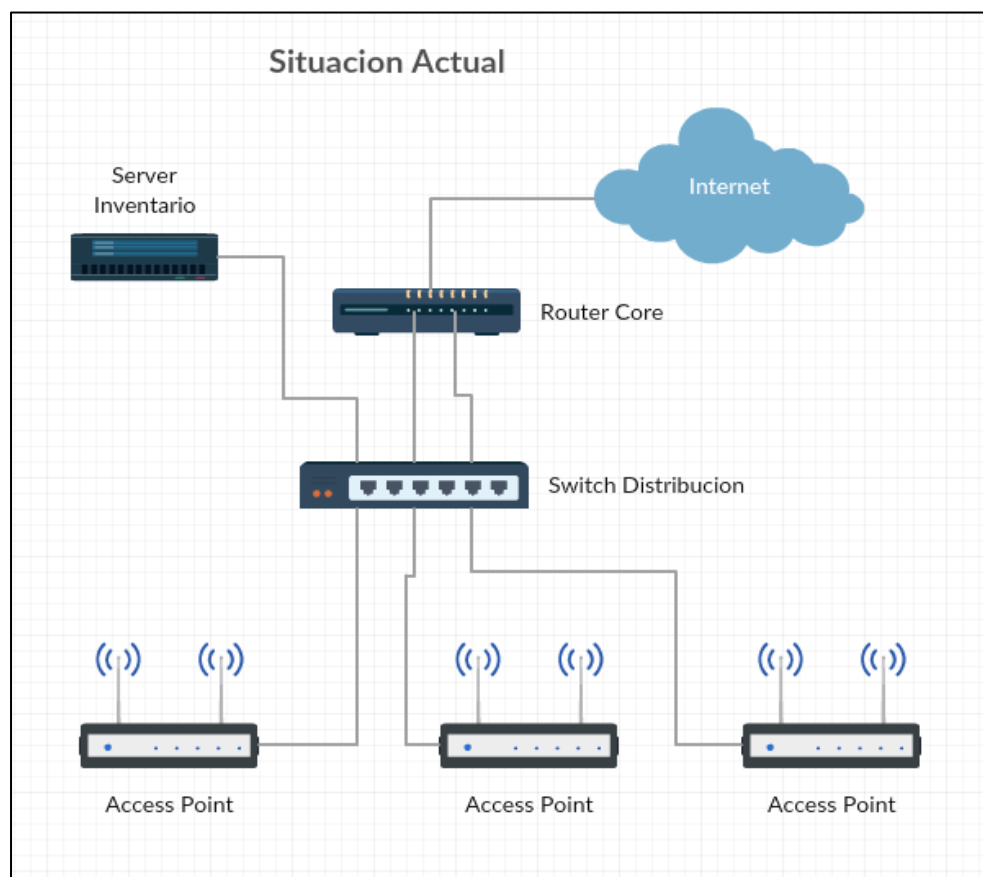


Figura 1.1 Situación actual de la empresa

La empresa tiene proyectado un considerable crecimiento, pero teme que sufra de alguna intrusión a su red y puedan sufrir pérdidas que puedan afectar de manera considerable su funcionamiento además

ha observado que los trabajadores usan la red de la empresa para access a Internet en sus momentos de descanso lo cual esta congestionando la comunicación con sus proveedores y demás.

En conclusión, esta empresa startup requiere llevar una auditoria en línea de los trabajadores que están accediendo a su Internet a través de la red de acceso wireless: cantidad de usuarios registrados, restringir por MAC ADDRESS, asignación de ancho de banda como registro, asignar a cada empleado única credencial, usuarios bloqueados por razones varias, usuarios dados de baja, disponibilidad de ancho de banda según la cantidad de usuarios registrados, asignación de ancho de banda ocupado según usuario registrados, respaldo del sistema de autenticación.

La empresa tiene limitado su presupuesto para implementar este sistema de autenticación para lo cual pide se proponga un sistema el cual se acople al dimensionamiento de su cantidad de trabajadores dejando un cuarenta por ciento de capacidad para incrementar su nómina con una plataforma económica y rentable.

1.3. Solución Propuesta

Tomando en cuenta que la empresa no tiene un sistema de autenticación que proteja su sistema de información se recomienda Implementar un sistema de autenticación capaz de proveer el servicio a los trabajadores que acceden vía wireless en los access point. La empresa tiene una nómina de cuarenta empleados los cuales deberán ser migrados al sistema de autenticación propuesto.

Se propone implementar el sistema de autenticación usando el modelo AAA (Authentication, Authorization and Accounting). Este modelo de autenticación tiene muchos años en funcionamiento el mismo ha sido usado ampliamente demostrado su capacidad para ser aplicados en sistemas de autenticación, este modelo este modelo AAA la primera etapa de autenticación es como su nombre lo indica, el usuario deberá demostrar quién es proporcionando su clave respectiva cuando el server lo requiera, es decir este paso es uno de los pilares para los sistemas de autenticación para poder acceder a la red que esta requiriendo. En el paso de autenticación hay diferente modelo como el normal, distribuido y roaming, dependiendo donde este el usuario haciendo este requerimiento.

En el paso de autorización se revisa los privilegios que tiene estos usuarios, pero tomando como referencia quien es, en este paso se le proporcionara los privilegios específicos que él solicita lo cuales ya fueron cargados en la base de datos donde ha sido creado el usuario. Cabe indicar que estas autorizaciones también se basan en las restricciones que tendrá este usuario según como ha sido creado en la base de datos por la organización y esto lo podrá limitar a los niveles de acceso que tendrá. Algo muy importante que realiza esta fase también es controlar los accesos simultáneos que podría intentar realizar el usuario. Los permisos a los cuales se les da a un usuario están dados en función de lo que permite los diferentes departamentos de una organización y no de lo que usuario desea acceder. Por ejemplo, para controlar los servicios que el usuario tendrá accesos podrían basarse en el rango de IP que se le pueda asignar y también parámetros de QoS.

El otro paso es la contabilización como parte del modelo AAA, esta fue creada para llevar estadística de consumo de recursos en la red por los usuarios que han podido validar su identidad. Para los ISP, organización y pequeñas pymes es de mucha importancia debido que esto les puede servir para llevar estadísticas y poder así dimensionar su red informática de mejor manera en caso que sea

necesario. El modelo AAA permite llevar la contabilización en tiempo real en caso que alguna organice lo requiera todo dependiendo como sea configurada.

El protocolo RadiusServer que usa este modelo AAA es de código abierto lo cual garantiza ser de mucha ayuda a empresa de baja escala para ser implementada en su organización, según se muestra en la figura 1.2 sobre este Radius Server estará corriendo FreeRadius, daloRadius, MySQL, PHP y Apache. [3]

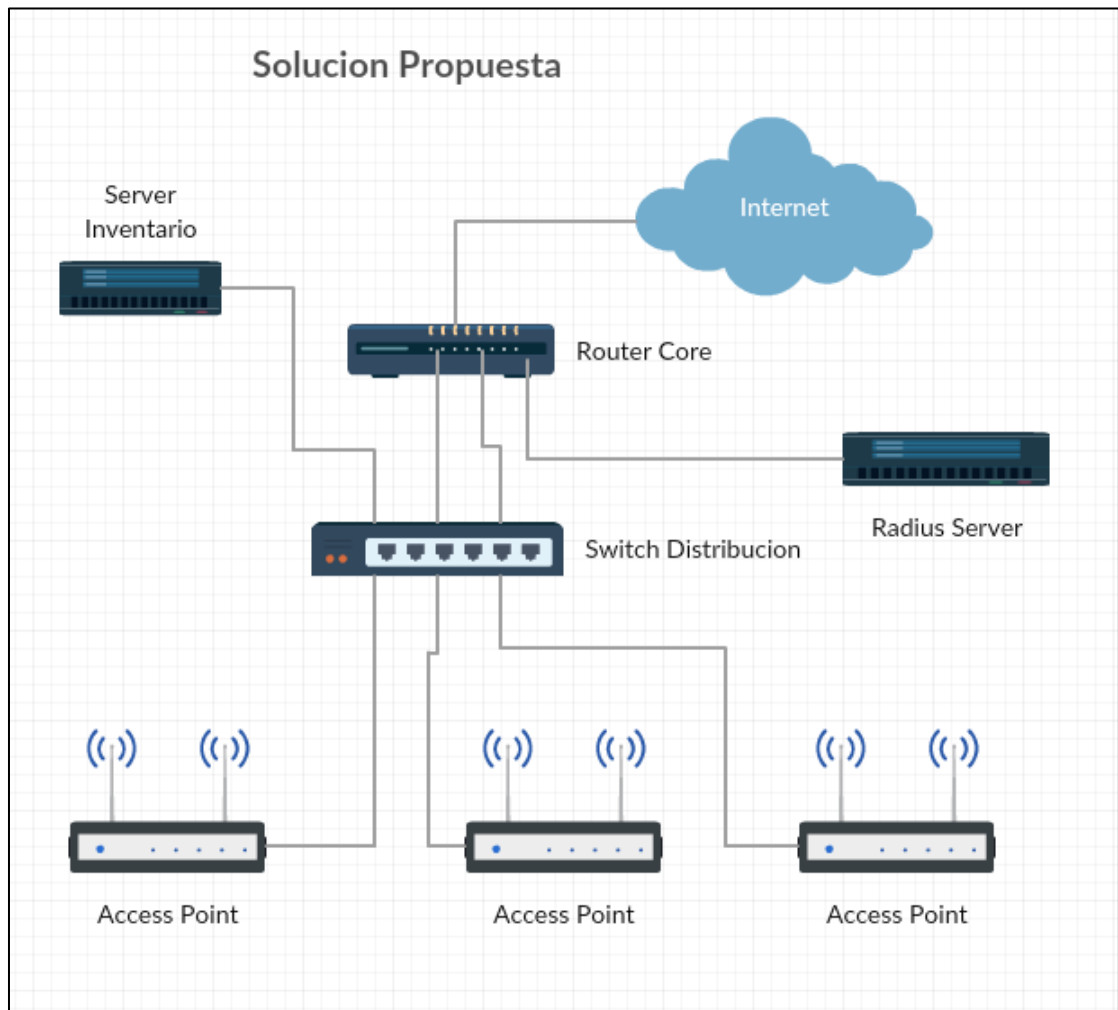


Figura 1.2 Solución propuesta para la autenticación con Radius Server

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1. Modelo y protocolo de autenticación

El protocolo de aplicación Radius Server funciona sobre UDP a diferencia del protocolo Diameter que trabaja sobre TCP. La diferencia entre estos dos protocolos de autenticación es el control de congestión que posee Diameter lo cual es una de las debilidades de Radius Server. A continuación, se muestra el esquema de cómo trabaja Radius Server método de autenticación elegido como solución para esta empresa.

En la figura 2.1 se puede observar un flujo básico de cómo trabaja Radius Server, la interacción con el cliente en este caso con los usuarios finales será de vital importancia que esté funcionando en toda su capacidad para brindar un óptimo servicio.

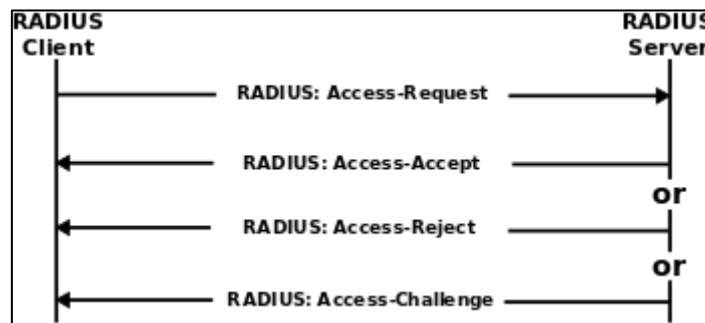


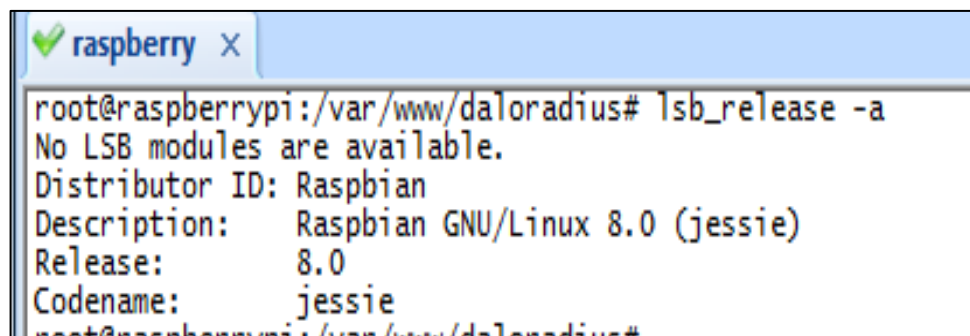
Figura 2.1 Flujo de comunicación del protocolo Radius Server [2]

El cliente Radius realiza un requerimiento al Radius Server para poder autenticarse y acceder a los servicios informáticos, pero antes deben pasar alguna prueba de confianza el cliente, para la solución propuesta al cliente se creará un usuario para cada empleado el mismo que será de absoluta responsabilidad de este.

2.2. Servidor de aplicaciones de autenticación

La limitante del cliente era el presupuesto destinado para esta solución se optó por un Raspberry modelo 2 B el cual tiene un costo muy asequible para este tipo de empresa, en el cual está instalado Debian(Raspbian) esta distribución de Linux es proporcionada por la empresa que crea los módulos de Raspberry. En la figura 2.2 podemos observar más detalles acerca de la version de Debian

usada por esta plataforma.

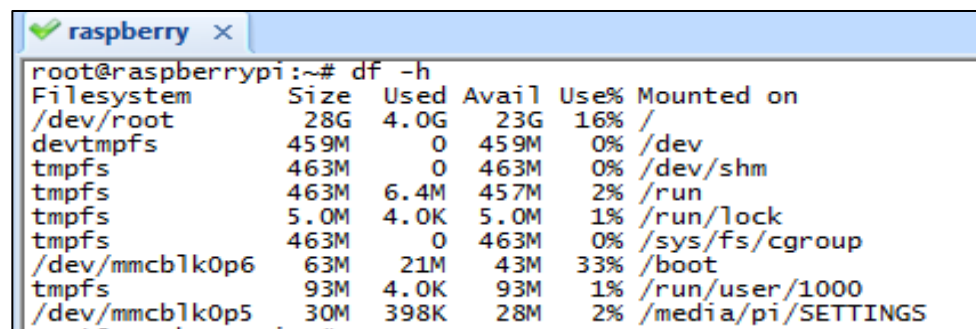


```
root@raspberrypi:/var/www/daloradius# lsb_release -a
No LSB modules are available.
Distributor ID: Raspbian
Description:   Raspbian GNU/Linux 8.0 (jessie)
Release:      8.0
Codename:     jessie
root@raspberrypi:/var/www/daloradius#
```

Figura 2.2 Distribución de Linux usada en plataforma Raspberry Pi

Este Raspberry requiere de una alimentación de 5V y 1A DC tipo mini USB, tiene cuatro puertos USB 2.0 capaces de proporcionar acceso a dispositivos externos como memorias para expansión y demás, tiene un puerto ethernet el cual proporcionar conectividad LAN, en el procesador de este Raspberry. El procesador brinda la solución de wifi y bluetooth de manera integrada, para esta solución no la utilizaremos debido que su alto procesamiento interferirá con el rendimiento para el óptimo funcionamiento del Radius Server, este Raspberry posee un mini slot para integrar una memory stick hasta 64 GB de capacidad, para esta solución se adquirió una memoria de 32 GB en el cual estará alojada el sistema operativo la base de datos

MySQL, y los demás servicios, en la figura 2.3 se puede observar la calidad que tiene el Raspberry y la usada donde ya está instalado todos los servicios con la base de datos creada con MySQL. [4]



```

root@raspberrypi:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       28G   4.0G   23G  16% /
devtmpfs        459M   0    459M   0% /dev
tmpfs           463M   0    463M   0% /dev/shm
tmpfs           463M   6.4M   457M   2% /run
tmpfs           5.0M   4.0K   5.0M   1% /run/lock
tmpfs           463M   0    463M   0% /sys/fs/cgroup
/dev/mmcblk0p6  63M   21M   43M  33% /boot
tmpfs           93M   4.0K   93M   1% /run/user/1000
/dev/mmcblk0p5  30M   398K   28M   2% /media/pi/SETTINGS

```

Figura 2.3 Capacidad y distribución en Raspberry con Raspbian

2.3. Desarrollo de Radius Server como plataforma de autenticación

Como paso previo para iniciar la instalación del Radius Server se procedió con la instalación del sistema operativo Raspbian 8.0 el cual está alojado en una memoria con capacidad de 32 GB, ahora se procederá con la instalación según se va indicando paso a paso, instalaremos y configuraremos un server Apache, MySQL y PHP con lo cual tendremos un LAMP Server.

Primero procedemos con la update de las librerías del Raspbian el cual servirá para descargar los diferentes servicios que usara Radius Server, la figura 2.4 nos muestra el update que sufre Raspbian antes de instalar los diferentes servicios.

```
root@raspberrypi:/home/pi# apt-get update
Get:1 http://mirrordirector.raspbian.org jessie InRelease [14.9 kB]
Get:2 http://archive.raspberrypi.org jessie InRelease [13.2 kB]
Get:3 http://mirrordirector.raspbian.org jessie/main armhf Packages [8,981 kB]
Get:4 http://archive.raspberrypi.org jessie/main armhf Packages [128 kB]
Get:5 http://archive.raspberrypi.org jessie/ui armhf Packages [53.6 kB]
Ign http://archive.raspberrypi.org jessie/main Translation-en_GB
Ign http://archive.raspberrypi.org jessie/main Translation-en
Ign http://archive.raspberrypi.org jessie/ui Translation-en_GB
Ign http://archive.raspberrypi.org jessie/ui Translation-en
Get:6 http://mirrordirector.raspbian.org jessie/contrib armhf Packages [37.5 kB]
Get:7 http://mirrordirector.raspbian.org jessie/non-free armhf Packages [70.3 kB]
Get:8 http://mirrordirector.raspbian.org jessie/rpi armhf Packages [1,356 B]
Ign http://mirrordirector.raspbian.org jessie/contrib Translation-en_GB
Ign http://mirrordirector.raspbian.org jessie/contrib Translation-en
Ign http://mirrordirector.raspbian.org jessie/main Translation-en_GB
Ign http://mirrordirector.raspbian.org jessie/main Translation-en
Ign http://mirrordirector.raspbian.org jessie/non-free Translation-en_GB
Ign http://mirrordirector.raspbian.org jessie/non-free Translation-en
Ign http://mirrordirector.raspbian.org jessie/rpi Translation-en_GB
Ign http://mirrordirector.raspbian.org jessie/rpi Translation-en
Fetched 9,300 kB in 16s (549 kB/s)
Reading package lists... Done
```

Figura 2.4 Update en librerías de Raspbian

Ahora se procede con la instalación de Apache con el siguiente comando: [7]

```
apt-get install apache2 apache2-doc apache2-utils
```

```

root@raspberrypi:/home/pi# apt-get install apache2 apache2-doc apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
 libasn1-8-heimdal libgssapi3-heimdal libcrypto4-heimdal libheimbase1-heimdal
 libheimntlm0-heimdal libhx509-5-heimdal libkrb5-26-heimdal libroken18-heimdal
 libwind0-heimdal libxfce4ui-1-0 pypy-upstream-doc wiringpi xfce-keyboard-shortcuts
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
 apache2-bin apache2-data libapr1 libaprutil1 libaprutil1-dbd-sqlite3
 libaprutil1-ldap liblua5.1-0 ssl-cert
Suggested packages:
 apache2-suexec-pristine apache2-suexec-custom openssl-blacklist
The following NEW packages will be installed:
 apache2 apache2-bin apache2-data apache2-doc apache2-utils libapr1 libaprutil1
 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0 ssl-cert
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,496 kB of archives.
After this operation, 25.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrordirector.raspbian.org/raspbian/ jessie/main libapr1 armhf 1.5.1-3 [77.1 kB]
Get:2 http://mirrordirector.raspbian.org/raspbian/ jessie/main libaprutil1 armhf 1.5.4-1 [75.9 kB]
Get:3 http://mirrordirector.raspbian.org/raspbian/ jessie/main libaprutil1-dbd-sqlite3 armhf 1.5.4-1 [17.7 kB]
Get:4 http://mirrordirector.raspbian.org/raspbian/ jessie/main libaprutil1-ldap armhf 1.5.4-1 [16.7 kB]
Get:5 http://mirrordirector.raspbian.org/raspbian/ jessie/main liblua5.1-0 armhf 5.1.5-7.1 [83.7 kB]
Get:6 http://mirrordirector.raspbian.org/raspbian/ jessie/main apache2-bin armhf 2.4.10-10+deb8u7 [893 kB]
Get:7 http://mirrordirector.raspbian.org/raspbian/ jessie/main apache2-utils armhf 2.4.10-10+deb8u7 [194 kB]
Get:8 http://mirrordirector.raspbian.org/raspbian/ jessie/main apache2-data all 2.4.10-10+deb8u7 [163 kB]
Get:9 http://mirrordirector.raspbian.org/raspbian/ jessie/main apache2 armhf 2.4.10-10+deb8u7 [207 kB]
Get:10 http://mirrordirector.raspbian.org/raspbian/ jessie/main apache2-doc all 2.4.10-10+deb8u7 [2,747 kB]
Get:11 http://mirrordirector.raspbian.org/raspbian/ jessie/main ssl-cert all 1.0.35 [20.9 kB]
Fetched 4,496 kB in 5s (797 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1:armhf.
(Reading database ... 120807 files and directories currently installed.)
Preparing to unpack .../libapr1_1.5.1-3_armhf.deb ...
Unpacking libapr1:armhf (1.5.1-3) ...
Selecting previously unselected package libaprutil1:armhf.
Preparing to unpack .../libaprutil1_1.5.4-1_armhf.deb ...
Unpacking libaprutil1:armhf (1.5.4-1) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:armhf.
Preparing to unpack .../libaprutil1-dbd-sqlite3_1.5.4-1_armhf.deb ...
Unpacking libaprutil1-dbd-sqlite3:armhf (1.5.4-1) ...
Selecting previously unselected package libaprutil1-ldap:armhf.
Preparing to unpack .../libaprutil1-ldap_1.5.4-1_armhf.deb ...
Unpacking libaprutil1-ldap:armhf (1.5.4-1) ...
Selecting previously unselected package liblua5.1-0:armhf.
Preparing to unpack .../liblua5.1-0_5.1.5-7.1_armhf.deb ...
Unpacking liblua5.1-0:armhf (5.1.5-7.1) ...
Selecting previously unselected package apache2-bin.
Preparing to unpack .../apache2-bin_2.4.10-10+deb8u7_armhf.deb ...
Unpacking apache2-bin (2.4.10-10+deb8u7) ...
Selecting previously unselected package apache2-utils.
Preparing to unpack .../apache2-utils_2.4.10-10+deb8u7_armhf.deb ...
Unpacking apache2-utils (2.4.10-10+deb8u7) ...
Selecting previously unselected package apache2-data.
Preparing to unpack .../apache2-data_2.4.10-10+deb8u7_all.deb ...
Unpacking apache2-data (2.4.10-10+deb8u7) ...
Selecting previously unselected package apache2.
Preparing to unpack .../apache2_2.4.10-10+deb8u7_armhf.deb ...
Unpacking apache2 (2.4.10-10+deb8u7) ...
Selecting previously unselected package apache2-doc.

```

Figura 2.5 Instalación de Apache

En la figura 2.5 podemos observar el proceso de instalación de Apache. Después de este primero paso instalaremos PHP con los siguientes comandos


```
apt-get install libapache2-mod-php5 php5 php-pear php5-xcache
```

```
apt-get install php5-mysql [7]
```

En la figura 2.6 y 2.7 podemos observar las fases de instalación de PHP.

```

root@raspberrypi:/home/pi# apt-get install apache2 apache2-doc apache2-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version.
apache2-doc is already the newest version.
apache2-utils is already the newest version.
The following packages were automatically installed and are no longer required:
 libasn1-8-heimdal libgssapi3-heimdal libhcrypto4-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhx509-5-heimdal
 libkrb5-26-heimdal libroken18-heimdal libwind0-heimdal libxfce4ui-1-0 pypy-upstream-doc wiringpi xfce-keyboard-shortcuts
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 52 not upgraded.
root@raspberrypi:/home/pi# apt-get install libapache2-mod-php5 php5 php-pear php5-xcache
Reading package lists... Done
Building dependency tree
Reading state information... Done
libapache2-mod-php5 is already the newest version.
php-pear is already the newest version.
php5 is already the newest version.
php5-xcache is already the newest version.
The following packages were automatically installed and are no longer required:
 libasn1-8-heimdal libgssapi3-heimdal libhcrypto4-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhx509-5-heimdal
 libkrb5-26-heimdal libroken18-heimdal libwind0-heimdal libxfce4ui-1-0 pypy-upstream-doc wiringpi xfce-keyboard-shortcuts
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 52 not upgraded.

```

Figura 2.6 PHP fase 1

```

root@raspberrypi1:/home/pi# apt-get install libapache2-mod-php5 php5 php-pear php5-xcacher
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
libasn1-8-heimdal libgsasl3-heimdal libhcrypto4-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhx509-5-
libkrb5-26-heimdal libroken18-heimdal libwind0-heimdal libxftc4ui-1-0 pypy-upstream-doc wiringpi
xfce-keyboard-shortcuts
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
libonig2 libperl4-corelibs-perl libqdbm14 libor php-curl php5-common php5-json php5-readline
Suggested packages:
php5-dev php5-user-cache
The following NEW packages will be installed:
libapache2-mod-php5 libonig2 libperl4-corelibs-perl libqdbm14 libor php-pear php5 php5-curl php5-common php5-jso
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,458 kB of archives.
After this operation, 21.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main libonig2 armhf 5.9.5-3.2 [101 kB]
Get:2 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main libperl4-corelibs-perl all 0.003-1 [43.6 kB]
Get:3 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main libor armhf 4.86-dfsg-1 [321 kB]
Get:4 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main php5-common armhf 5.6.27-dfsg-0-deb8u1 [716 kB]
Get:5 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main php5-xcacher armhf 3.2.0-1 [110 kB]
Get:6 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main libqdbm14 armhf 1.8.7-5-b1 [86.0 kB]
Get:7 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main php5-json armhf 1.3.6-1 [16.9 kB]
Get:8 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main php5-curl armhf 5.6.27-dfsg-0-deb8u1 [1,905 kB]
Get:9 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main php5 all 5.6.27-dfsg-0-deb8u1 [1,326 B]
Get:10 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main libapache2-mod-php5 armhf 5.6.27-dfsg-0-deb8u1 [
Get:11 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main php-pear all 5.6.27-dfsg-0-deb8u1 [268 kB]
Get:12 http://mirrors.ubuntu.com/mirrors.archive/ubuntu/ jessie/main php5-readline armhf 5.6.27-dfsg-0-deb8u1 [11.2

```

Figura 2.7 PHP fase 2

Como siguiente paso se procederá con la instalación de la base de datos MySQL con el siguiente comando

```
apt-get install mysql-server mysql-client [7]
```

En la figura 2.8 se puede observar el proceso de instalación de MySQL.

```

root@raspberrypi:/home/pi# apt-get install php5-mysql
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libbasn1-8-heimdal libgssapi3-heimdal libhcrypto4-heimdal libheimbase1-heimdal libheimntlm0-heimdal libhx509-5-heimdal libkrb5-3-heimdal libroken18-heimdal libwind0-heimdal libxfce4ui-1-0 pypy-upstream-doc wiringpi xfce-keyboard-shortcuts
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  libmysqlclient18 mysql-common
The following NEW packages will be installed:
  libmysqlclient18 mysql-common php5-mysql
0 upgraded, 3 newly installed, 0 to remove and 52 not upgraded.
Need to get 693 kB/745 kB of archives.
After this operation, 3,553 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrordirector.raspbian.org/raspbian/ jessie/main mysql-common all 5.5.53-0+deb8u1 [75.5 kB]
Get:2 http://mirrordirector.raspbian.org/raspbian/ jessie/main libmysqlclient18 armhf 5.5.53-0+deb8u1 [617 kB]
Fetched 693 kB in 1s (602 kB/s)
Selecting previously unselected package mysql-common.
(Reading database ... 124501 files and directories currently installed.)
Preparing to unpack .../mysql-common_5.5.53-0+deb8u1_all.deb ...
Unpacking mysql-common (5.5.53-0+deb8u1) ...
Selecting previously unselected package libmysqlclient18:armhf.
Preparing to unpack .../libmysqlclient18_5.5.53-0+deb8u1_armhf.deb ...
Unpacking libmysqlclient18:armhf (5.5.53-0+deb8u1) ...
Selecting previously unselected package php5-mysql.
Preparing to unpack .../php5-mysql_5.6.27+dfsg-0+deb8u1_armhf.deb ...
Unpacking php5-mysql (5.6.27+dfsg-0+deb8u1) ...
Processing triggers for libapache2-mod-php5 (5.6.27+dfsg-0+deb8u1) ...
Setting up mysql-common (5.5.53-0+deb8u1) ...
Setting up libmysqlclient18:armhf (5.5.53-0+deb8u1) ...

```

Figura 2.8 Instalación de MySQL

El siguiente paso es configurar el Raspberry como IP estática, pero el Router Ubiquiti modelo EdgeMax que posee el cliente nos provee la opción de separar IP como estática y con chequeo de MAC ADDRESS lo cual se la mayor seguridad para separar una IP estática al Radius Server.

En la figura 2.9 se puede observar cómo se configura IP estática desde el Router lo cual no hace necesario configurar desde Radius Server.

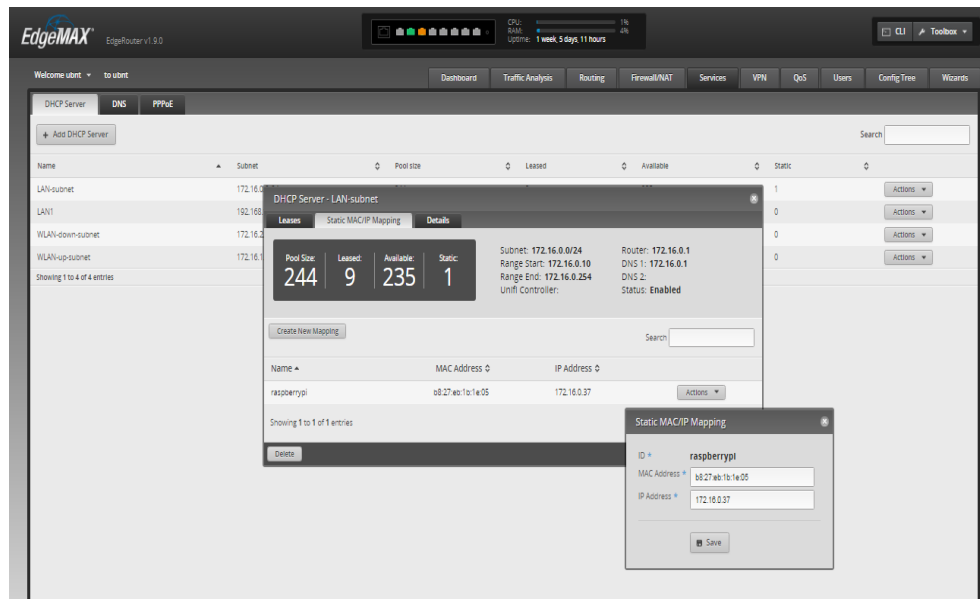


Figura 2.9 Configuración de IP estática para Radius Server desde el Router

Ahora procederemos con la instalación de FreeRadius en cual actuara como un GUI en conjunto con daloRADIUS para la interacción del Administrador del Radius Server de manera amigable, los siguientes comandos son para la instalación de FreeRadius:

```
sudo su
```

```
apt-get install freeradius freeradius-mysql php5-gd php-db
```

Instalamos daloRADIUS:

```
cd /usr/src
```

```
wget
```

```
http://downloads.sourceforge.net/project/daloradius/daloradius/daloradius0.9-9/daloradius-0.9-9.tar.gz
```

```
tar xvfz daloradius-0.9-9.tar.gz -C /var/www
```

```
mv /var/www/daloradius-0.9-9/ /var/www/daloradius
```

```
cd /var/www/daloradius [7]
```

Inicializamos la base de datos MySQL para FreeRADIUS con el siguiente procedimiento:

```
mysql -u root -p
```

```
CREATE DATABASE radiusdb ;
```

```
exit
```

```
mysql -u root -p radiusdb < /var/www/daloradius/contrib/db/fr2-mysql-daloradius-and-freeradius.sql
```

```
mysql -u root -p
```

```
CREATE USER 'radiususer'@'localhost' ;
```

```
SET PASSWORD FOR 'radiususer'@'localhost' =  
PASSWORD('radiuspass') ;
```

```
GRANT ALL ON radiusdb.* to 'radiususer'@'localhost' ;
```

```
exit
```

Editamos en daloRADIUS

var/www/daloradius/library/daloradius.conf.php lo cual permitirá que

daloRADIUS sea integrado en la base de datos MySQL

```
$configValues['CONFIG_DB_USER'] = 'radiususer' ;
```

```
$configValues['CONFIG_DB_PASS'] = 'radiuspass' ;
```

```
$configValues['CONFIG_DB_NAME'] = 'radiusdb' ;
```

Configuramos en FreeRADIUS con la creación de usuario y password

Se requiere editar /etc/freeradius/users

```
client 172.16.0.0/24 {
```

```
secret = prueba123
```

```
shortname = oficina-principal
```

```
} [7]
```

2.4. Pruebas del sistema de autenticación con Radius Server

Ahora procedemos con varias pruebas para verificar el correcto funcionamiento de Radius Server, procedemos con detener y reiniciar el servicio FreeRadius:

```
service freeradius stop
```

```
service freeradius start
```

Con el siguiente comando simulamos un requerimiento y si esta todo correctamente configurado obtendremos como respuesta "Access-Accept".

```
radtest "TEST" hello localhost 0 prueba123
```

Finalmente procedemos con la fase final de pruebas configurando FreeRADIUS en la base de datos MySQL, editamos en archivo de configuración `/etc/freeradius/radiusd.conf` removiendo "#" que esta como comentarios para podernos activar:

```
$INCLUDE sql.conf
```

```
$INCLUDE sql/mysql/counter.conf
```

Ahora editamos `/etc/freeradius/sql.conf` para que refleje lo siguiente:

```
server = "localhost"
```

```
login = "radiususer"
```

```
password = "radiuspass"
```

```
radius_db = "radiusdb"
```

Para finalizar debemos editar /etc/freeradius/sites-enabled/default

retirando "#" los comentarios para poder activar

```
"authorize"
```

```
"accounting"
```

```
"session"
```

```
"post-auth" [7]
```

Finalmente procedemos con el reinicio del Raspberry para verificar

su correcto funcionamiento:

```
reboot
```


CAPÍTULO 3

ANÁLISIS DE RESULTADOS

3.1. Análisis comparativo

Para realizar un análisis comparativo se procedió con la verificación después de la implementación de este sistema de autenticación algunas variables que la empresa puede manejar como percepción de los medios de autenticación, manejo seguro según el estándar ISO 27001 el cual proporciona buenas métodos de aseguramiento de la información.

Antes esta empresa solo requería compartir la única clave de los access point a los empleados los cuales a su vez la usaban para acceder a los diferentes recursos informáticos de la empresa y no existía un control estricto de quien y a que recursos informativos cada empleado ingresaba.

Ahora la empresa maneja de maneja estricta los accesos y uso de los recursos informativos de cada empleado gracias al modelo AAAA, nótese que la empresa está en capacidad de llevar un auditoria en línea de cada empleado mientras estén autenticados en la red. Según se muestra en la figura 3.1 daloRADIUS es muy rico en la información del comportamiento de cada usuario



Figura 3.1 Interface gráfica daloRADIUS

3.2. Análisis de los resultados obtenidos

Notamos la mejoría en relación al control de acceso que tiene la empresa de cada empleado en tiempo real y no solo compartiendo la única clave con todos ellos. Observamos una resistencia natural de los empleados para aceptar el nuevo método de autenticación, pero se procedió con la socialización del uso de este método el cual traerá muchos beneficios para la empresa y para todos los empleados debido que la empresa ya no tendrá comprometida la continuidad del negocio, ahora el control de acceso se dará a cada empleado según su rango y departamento que pertenezca.

El dueño de esta empresa comprendió después de ver los resultados con el nuevo método de autenticación los beneficios que ha obtenido cuando fue instalado Radius Server, siempre aplicando normas de seguridad, aunque eso implique inversiones desde cientos de dólares hasta millones siempre conlleva beneficios para el aseguramiento de los sistemas informáticos de las empresas.

CONCLUSIONES Y RECOMENDACIONES

1. Cuando finalice este trabajo y luego de haber implementado este sistema de autenticación en una empresa que inicio sus actividades como proveedor de insumos para textiles teniendo que mejorar la manera como sus empleados se deberían autenticar para acceder a los recursos informáticos, se concluye que:
2. Cuando se realizó el levantamiento de información acerca de cómo esta empresa tenía implementado el sistema de autenticación para sus empleados se concluye que esa extremadamente básica sin ningún tipo de cuidado al permitir que los empleados conocían la única clave de la red wireless para acceder a la red no garantizaba la seguridad de la red.
3. El incremento paulatino de los empleados que eran contratados por esta empresa hacia caóticos el control de acceso de cada uno

de estos a los recursos informáticos he incrementaba algún tipo de ataque informático a la red debido que el método de autenticación era conocido por todos y fácilmente podrían ser compartidos con personas ajenas a la empresa.

4. Se requería establecer de manera diaria el cambio de clave para que todos los empleados se puedan autenticar en la red así como realizar actualización de enrutamiento debido a la congestión de la red LAN debido que la mayor parte de los empleados usaban de manera indebida la red para acceder a INTERNET para lo cual no fue creada la red de esta empresa.

5. La falta de socialización a los empleados por parte de la empresa permite que extraños a la empresa puedan tener acceso a los recursos informáticos en inicio como medio para acceder a INTERNET, pero este podría llevar a comprometer con el acceso a sus recursos informáticos que son de vital importancia para su funcionamiento.

6. Al finalizar este trabajo y luego de haber implementado un esquema de autenticación para una empresa proveedora de insumos textiles se recomienda que:

7. Se conversó con el dueño de esta empresa y se recomendó cuando tenga el presupuesto necesario fortalezca el sistema de autenticación con un segundo Radius Server como método de respaldo en caso que el primero falle, esto protegerá la continuidad del negocio de esta empresa.

8. Se puede seguir utilizando como base de datos MySQL el cual es instalado en el Raspberry hasta cuando se detecte una alta carga de CPU lo cual nos indicara que el cliente deberá una otro dispositivo donde deberá alojar esta base de datos, al momento de realizar esta implementacion no se logró un stress de la plataforma para confirmar la máxima transacciones que podría soportar esta plataforma.

9. Para poder garantizar la continuidad del negocio de esta empresa requiere de manera oportuna se integre un segundo Raspberry para poder tenerlo como respaldo, de igual manera esta empresa debido que su principal recurso es el manejo de su inventario se implemente de manera oportuna un respaldo de la base de datos de sus empleados en la parte de autenticación se aloje en otro lugar físico para garantizar en caso de afectación total de sitio esta plataforma de autenticación pueda ser restablecida en el menor tiempo usando esta respaldo remoto que fue recomendado.

10. Se realice socialización y capacitaciones de manera continua para los empleados pueden administrar sus credenciales de manera responsables y tener conocimiento de los riesgos en casos de compartir esta información con otros empleados o extraños a la empresa.

BIBLIOGRAFÍA

[1] ISO/IEC 17799:2005, Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.

[2] Protocolo AAA, https://es.wikipedia.org/wiki/Protocolo_AAA

[3] Modelo de flujo de Radius Server, <https://en.wikipedia.org/wiki/RADIUS>

[4] ISO/IEC 27001:2011 Tecnología de la Información – Técnica de seguridad – Sistema de Gestión de la Seguridad de la Información (SGSI).

[5] Raspberry Organización, <https://www.raspberrypi.org>

[6] Raspberry FreeRadius,

<http://www.binaryheartbeat.net/2013/12/raspberry-pi-based-freeradius-server.html>

[7] RADIUS Server,

<https://www.globalknowledge.com/us-en/resources/resource-library/white-papers/building-installing-and-configuring-a-radius-server/>