IMPLEMENTACIÓN DE POLÍTICAS TIPO BYOD BAJO ENFOQUE NAC BASADAS EN SOFTWARE LIBRE PARA LA GESTIÓN DE SEGURIDAD EN REDES DE DATOS

JOHANA YULIETH BOLAÑO CARRACEDO

GRUPO DE INVESTIGACIÓN EN TECNOLOGÍAS DE INFORMACIÓN

LÍNEA DE INVESTIGACIÓN: TELEMÁTICA

UNIVERSIDAD AUTONOMA DE BUCARAMANGA

FACULTAD DE INGENIERIA DE SISTEMAS

PROYECTO DE GRADO II

BUCARAMANGA, SANTANDER

2015

IMPLEMENTACIÓN DE POLÍTICAS TIPO BYOD BAJO ENFOQUE NAC BASADAS EN SOFTWARE LIBRE PARA LA GESTIÓN DE SEGURIDAD EN REDES DE DATOS

JOHANA YULIETH BOLAÑO CARRACEDO

Trabajo de tesis

JOSE GREGORIO HERNANDEZ S

Director trabajo de tesis

GRUPO DE INVESTIGACIÓN EN TECNOLOGÍAS DE INFORMACIÓN

LÍNEA DE INVESTIGACIÓN: TELEMÁTICA

UNIVERSIDAD AUTONOMA DE BUCARAMANGA

FACULTAD DE INGENIERIA DE SISTEMAS

PROYECTO DE GRADO II

BUCARAMANGA, SANTANDER

2015

NOTA DE ACEPTACION

Firma Director

Firma Evaluador

Firma Evaluador

Bucaramanga, Junio 22 de 2015

DEDICATORIA

Dedico este proyecto de grado, en primera instancia a Dios por todas las bendiciones que me ha dado, segundo a mis padres y a mis hermanos por el apoyo que me brindan y finalmente a todas las personas que me aconsejaron y me ayudaron en cada paso.

AGRADECIMIENTOS

Quiero agradecer la realización de este proyecto a mi familia, mi tutor José Gregorio Hernández por guiarme durante el trayecto y asesora Vicky Lozano por su colaboración y apoyo, al decano de la facultad Ingeniería de Sistemas Wilson Briceño por su comprensión y a todas aquellas personas que me colaboraron.

Tabla de contenido

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

CAPITULO I

1. INTRODUCCION

1.1 PROBLEMATIZACIÓN

Las funciones que antes eran realizadas solamente en la oficina, gracias a la mayor conectividad, están siendo desarrolladas a través de aplicaciones móviles durante los trayectos y/o en el hogar. Éste fenómeno ha generado cambios en la estructura organizacional de las empresas, dado que los departamentos de seguridad han debido adaptar sus sistemas de seguridad a los dispositivos móviles.

Las personas están llevando estos dispositivos a su trabajo para integrarlos en su flujo laboral diario. *Bring Your Own Device* (BYOD) podría tener profundas implicaciones para la forma en que las empresas administran sus redes, sus dispositivos móviles e incluso sus empleados, quienes están redefiniendo lo que significa estar “en la oficina” por esto, organizaciones deben ajustar sus mecanismos de control de acceso, autenticación, disponibilidad, identidad y capacidad de sus empleados y visitantes que llevan sus dispositivos móviles a sus redes para ofrecer sus servicios sin verse vulnerados en esos aspectos.

Los dispositivos móviles se han destacado en los últimos tiempos por ser un elemento indispensable para el diario vivir de las personas. El rápido crecimiento en ventas de los dispositivos ha provocado que los consumidores integren el uso de las aplicaciones en su rutina diaria. Estos potentes dispositivos tienen interfaces de usuario intuitivas, vienen equipados y pueden acceder a cientos de miles de aplicaciones, no solo para entretenimiento, sino también para fines productivos.

A nivel mundial, Latinoamérica se ha transformado en el mercado de mayor crecimiento en el volumen de ventas de dispositivos móviles, tanto de los mercados de Smartphone como de tabletas. De acuerdo a *Euromonitor International*, las ventas crecieron 61% y 414% respectivamente durante el 2011, fruto del escenario económico positivo vivido por la mayor parte de los países analizados. El crecimiento promedio del PIB de 4,5% observado en la región, afectó directamente el consumo privado por bienes de consumo durable, a diferencia de los mercados desarrollados quienes se han visto seriamente afectados por la incertidumbre en el panorama internacional. [1]

1.1.1 Antecedentes

1.1.2 Definición de Problema de investigación

En primer lugar se tiene que, en Mayo de 2011 fue presentado en el Departamento de Ingeniería de la información y las Comunicaciones de la Universidad De Murcia, el trabajo especial de Doctorado **Diseño de un sistema de control de acceso en redes heterogéneas con privacidad basado en Kerberos** por Fernando Pereñíquez García.

Esta tesis doctoral aborda el problema de la definición de movimientos rápidos sin interrupciones (*seamless handoffs*) en redes heterogéneas de próxima generación (NGNs) mediante definición de un proceso de distribución de claves seguro, que habilite un proceso de re-autenticación rápida a la vez que un acceso autenticado anónimo y que no se pueda trazar. Concretamente, el sistema de control de acceso desarrollado ofrece un conjunto de características que, hasta la fecha, no han confluido en una misma solución: (1) aplicable a las futuras redes NGN basadas en EAP; (2) reducción de la latencia introducida por el proceso de autenticación en entornos móviles, con independencia del tipo de *handoff* realizado por el usuario; (3) que el proceso cumpla fuertes requisitos de seguridad; (4) fácil despliegue en redes existentes; (5) compatibilidad con las actuales tecnologías estandarizadas; y (6) soporte de protección de privacidad del usuario. [2].

También se consultó el trabajo especial de grado que en Octubre de 2012, fue presentado por Julia Targelia Jiménez Orellana y Blanca Inés Rumipulla Castillo como requisito para optar el título de Ingeniero de Sistemas, el trabajo es titulado **Análisis de Soluciones de Acceso Seguro a la Red, e Implementación de un Proyecto Piloto para la Unidad Educativa "Técnico Salesiano".**

Este trabajo establece la importancia de la seguridad que ha adquirido incremento de las cambiantes condiciones. La posibilidad de interconectarse a través de redes, ha abierto nuevos espacios que permiten investigar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados como son que las organizaciones dependen de la presencia de internet, que es uno de los principales motivos que provocan riesgos de seguridad, porque permite acceder a la información y a los recursos de manera no autorizada.

Al analizar esta vulnerabilidad es necesario implementar medidas y técnica de seguridad en redes para proteger la información y recursos, estas deben ser proporcionales a lo que se intenta proteger como son: servidores web, servidores de correo, base de datos o cualquier tipo de red. [3]

En esta misma labor de investigación y consulta, se encontró el trabajo de María Luisa Cortez Caballero, Ana María Escalier Britos, Luis Fernando Rocha Guaraná

y José De la Cruz Condo **titulado Diplomado en Seguridad Informática "Control de Acceso a la Red"** en la Universidad Autónoma "Gabriel Rene Moreno", Facultad Integral del Chaco Carrera de Ingeniería Informática. El trabajo tiene como objetivo estudiar la importancia del control de acceso a redes puede encontrarse porque las empresas cada vez tienen redes más distribuidas, con oficinas y centros de negocios repartidos en distintas ubicaciones geográficas (sucursales), todos con la necesidad de acceso a la red y sistemas de la compañía utilizando distintos medios de acceso desde tecnologías inalámbricas, Internet, VPN, etc. Este entorno de interconexión tan complejo unido a la mayor criticidad de los datos que poseen las empresas y organizaciones, y a la necesidad de acceso a los datos desde cualquier dispositivo y ubicación, todo ello sin comprometer la integridad y confidencialidad de la información, ha provocado la aparición de innumerables y nuevos puntos débiles de acceso.

Estas circunstancias implican nuevos riesgos y amenazas ante los cuales las empresas demandan nuevas soluciones para solventarlas. En respuesta a esta demanda surgen iniciativas y tecnologías para resolverlas que se engloban dentro de lo que se conoce como Control de Acceso a la Red. Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos. Las reglas de acceso a la red a través de los puertos, están basadas en la premisa todo está restringido, a menos que este expresamente permitido. [4]

También continuando con el estudio y la investigación encontramos el proyecto de Olvido Nicolás Melero Titulado **Estudio sobre la implantación de las políticas de BYOD para el uso de dispositivos móviles personales en las comunicaciones de empresa** del año (2014)**,** ante la Universidad Politécnica de Valencia, Escuela Técnica Superior de Ingenieros de Telecomunicación, como Proyecto de grado. Esta tesis se orienta a profundizar sobre como poco a poco, esta corriente se ha ido trasladando a las empresas y organizaciones.

Sus empleados quieren utilizar en su entorno laboral aquellas tecnologías (dispositivos, aplicaciones y servicios) que están usando en su entorno personal y con las que dicen poder ser más productivos. Esto ha dado lugar a diferentes tendencias en el entorno empresarial. La más importante, el BYOD ("*Bring Your Own Device*") o "use su propio dispositivo", hace referencia al uso de dispositivos personales (Smartphone, tabletas, portátiles, discos USB) en el trabajo.

El fenómeno BYOD, es cada vez más común en la mayoría de las geografías a nivel mundial. Para las organizaciones, es una puerta de entrada para potenciales mejoras en la satisfacción y compromiso de los empleados, incremento de la

productividad y desarrollo de la innovación, habilitando nuevos negocios o innovando en los procesos de negocios existentes. [5]

1.2 JUSTIFICACIÓN

Existe una tendencia en el campo de los negocios y es que, más del 90% de los empleados utilizan sus propios dispositivos en muchos casos para acceder a la información de la empresa [6]. Esto les trae muchas preocupaciones a los directivos de las empresas sobre donde puede terminar la información que se consultó si por ejemplo el dispositivo es robado. BYOD utiliza protocolos de seguridad que permiten tener el control de la información que consultan los dispositivos conectados a una red con políticas de este tipo de control de acceso (cifrado de información en tránsito, autenticidad de usuario y autenticidad de red) [7].

Habitualmente los usuarios finales no tienen en consideración la seguridad cuando hacen uso de un sistema o red de comunicaciones, ya que, frecuentemente se ignoran los aspectos relacionados con la seguridad. De igual forma, estos aspectos a veces pueden considerarse una molestia, ya que la seguridad suele ir en el sentido opuesto de la comodidad y facilidad de uso en cuanto al diseño de un sistema. Es por esto que los usuarios a veces puedan tener una imagen negativa de la seguridad, por considerarlo algo molesto y que interrumpe su capacidad de realización de un trabajo determinado. En un entorno seguro, un usuario se encuentra con tareas que le pueden resultar incómodas (como por ejemplo, recordar contraseñas, cambiarlas periódicamente, restricciones de conexiones, imposibilidad de instalar software, entre otras) y que pueden limitar las operaciones que puede realizar así como los recursos a los que se le permite acceder. Sin embargo, la seguridad es fundamental a la hora de afrontar tareas que se realizan en sistemas informáticos ya que son las únicas medidas que pueden garantizar que éstas se realicen con una serie de garantías que se dan por sentado en el mundo físico [8].

El control de acceso a la red es un concepto de ordenador en red y conjunto de protocolos implementados para definir como asegurar los nodos de la red antes de que estos accedan a la red. NAC ofrece mecanismos de control que permiten hacer una validación de normas o políticas prestablecidas antes de conceder el acceso a la red. Permitiendo a la infraestructura de red como routers, switches, firewalls trabajar en conjunto con el back office y el equipamiento informático del usuario final para asegurar que el sistema de información está operando de manera segura antes de permitir el acceso a la red. Control de acceso a la red es

exactamente lo que su nombre indica, controlar el acceso a la red con políticas que incluyen pre-admisión y post admisión.

En el mundo intangible de la informática, tan cerca de un servidor están sus usuarios legítimos como los usuarios que hacen uso de la misma red de comunicaciones. Es más, estos usuarios, en el caso de una red global, se cuentan por millones. Algunos serán “buenos vecinos” pero otros serán agentes hostiles.

Para implementar este tipo de controles de acceso y políticas de seguridad con aplicaciones comerciales las organizaciones deben tener un presupuesto alto de inversión dado los costos de estos sistemas, es por esto que como alternativa se tiene el software libre para aquellas organizaciones cuyos presupuestos no alcanzan para hacer esta inversiones fuertes pero que deben solventar los requerimientos de seguridad que demandan las nuevas tecnologías.

El control de acceso se puede llegar a implementar mediante software libre que puede ser configurado para establecer este tipo de políticas. El software libre es aquel programa o conjunto de ellos de los que el usuario puede disponer del código fuente, sin restricciones, y el cual puede modificar y redistribuir también sin restricciones. Estas libertades garantizadas al usuario del software (o a aquel que lo recibe) no son contrarias a los derechos legítimos del autor del programa, es decir, éste no tiene que perder sus derechos sobre el mismo.

Para que las libertades de hacer modificaciones y de publicar versiones mejoradas tengan sentido, se debe tener acceso al código fuente del programa. Por lo tanto, la posibilidad de acceder al código fuente es una condición necesaria para el software libre. Ciertos tipos de reglas sobre la manera de distribuir software libre, son aceptables mientras no entren en conflicto con las libertades centrales. Por ejemplo, *copyleft* es la regla que implica que, cuando se redistribuya el programa, no se pueden agregar restricciones para denegar a otras personas las libertades centrales. Esta regla no entra en conflicto con las libertades centrales, sino que más bien las protege.

Con esto el propósito de este proyecto es mostrar las bondades del uso del software libre de la mano con el enfoque de seguridad de control de acceso a la red (NAC) que permita la implementación de la política empresarial BYOD. NAC (*Network Access Control*), en español (Control de Acceso a la Red)

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Implementar políticas tipo BYOD bajo enfoque NAC basadas en Software Libre, para la gestión de seguridad en redes de datos.

1.3.2 OBJETIVOS ESPECIFICOS

- Elaborar un estado del arte sobre políticas tipo BYOD y herramientas de Control de Acceso a la Red (NAC) de tipo propietario y Software Libre existentes en el mercado actual, como alternativas para la gestión de seguridad en redes de datos.
- Diseñar una red de laboratorio de pruebas que incluya políticas tipo BYOD y una solución NAC de Software Libre para la gestión de seguridad
- Validar la implementación de las políticas en la red de laboratorio de pruebas que incorpora políticas tipo BYOD y una solución NAC de Software Libre para la gestión de seguridad

1.4 MARCO TEORICO

En el contexto de la informática y los sistemas de información basados en aplicativos existe un mundo de requerimientos y necesidades. Dada que toda investigación realizada con un propósito llamado solución, es necesario que el investigador indague conceptos o referencias anteriores frente a su caso.

Teniendo en cuenta todos los aspectos que involucran la seguridad en redes autenticación, autorización, disponibilidad, confidencialidad, integridad y seguridad de equipos, servicios y datos.

1.4.1 Fundamentos de Seguridad Informática

La Seguridad Informática (S.I) es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

De acuerdo con la referencia de Purificación Aguilera en el libro de la Seguridad Informática explica los conceptos de la siguiente manera:

- **La Integridad:** Es la que se encarga de garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática.

- **La Disponibilidad u Operatividad:** Se encarga de garantizar el cumplimiento de sus objetivos, ya que se debe diseñar un sistema lo suficientemente robusto frente a ataques e interferencias como para garantizar su correcto funcionamiento, de manera que pueda estar permanentemente a disposición de los usuarios que deseen acceder a sus servicios.

- **La Privacidad** Es la necesidad de garantizar que cada mensaje transmitido o almacenado en un sistema informático solo podrá ser leído por su legítimo destinatario. Si dicho mensaje cae en manos de terceras personas, estas no podrán acceder al contenido del mensaje original. Por lo tanto este mensaje pretende garantizar la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de Backup y/o de los datos transmitidos a través de redes de comunicaciones.
- **Confidencialidad:** La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus directrices para la seguridad de los sistemas de Información define la confidencialidad como el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada. Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién puede acceder, a qué parte del sistema, en qué momento y para realizar qué tipo de operaciones.

- **El Control:** Permite asegurar que solo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma

- **La Autenticidad:** Garantiza que la identidad del creador de un mensaje o documento es legítima, es decir, gracias a esta función, el destinatario de un mensaje podrá estar seguro de que su creador es la persona que figura como remitente de dicho mensaje. [9] Adicionalmente pueden considerarse algunos aspectos, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- **Protección a la Replica:** Mediante la cual se asegura que una transacción solo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

- **No Repudio:** Mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

- **Consistencia:** Se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.

- **Aislamiento:** Este aspecto, íntimamente relacionado con la **Confidencialidad**, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

- **Auditoria:** Es las capacidad de determinar qué acciones o procesos se están llevando a cabo el sistema, así como quien y cuando las realiza.

1.4.2 Seguridad Física

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos tratados a continuación se prevén, otros, como la detección de un atacante interno a la empresa que intenta a acceder físicamente a una sala de operaciones de la misma, no.

Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

1.4.3 Seguridad Lógica

Luego de ver como nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

1. Restringir el acceso a los programas y archivos.
2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
5. Que la información recibida sea la misma que ha sido transmitida.
6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

1.4.4 Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el *National Institute for Standars and Technology* (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

- Identificación y Autentificación.
- Roles
  El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.
  Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.
- Transacciones
  También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.
- Limitaciones a los Servicios
  Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.
  Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.
- Ubicación y Horario
  El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

1.4.5 Definición de Seguridad en Redes de Datos

La definición que nos ofrecen las mejores prácticas como COBIT es: “Garantizar que se utilizan técnicas de seguridad y procedimientos de administración

asociados (por ejemplo, Firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes”

La definición que nos ofrece ISO 17799 es: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los limites organizacionales, requiere de la cuidadosa consideración del flujo de data, implicancias legales, monitoreo y protección. También se puede requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas [10].

Como conclusión: La seguridad en redes es un nivel que garantiza que el funcionamiento de todos los ordenadores de una red sea optimo y que todos los usuarios de estas máquinas posean los derechos que les han concedidos así como también asegurarse de que se utilicen técnicas y procedimientos de administración para el buen funcionamiento de dichas redes [11].

Se puede concluir:

1. Evitar que personas no autorizadas intervengan en el sistema con fines malignos.
2. Evitar que los usuarios realicen operaciones involuntarias que pueden dañar el sistema.
3. Asegurar los datos mediante la prevención de fallas.
4. Garantizar que no se interrumpan los servicios [12].

1.4.6 Importancia de la Seguridad

La seguridad de redes ha evolucionado durante la última década a partir de su concepto inicial, basado en soluciones puntuales como por ejemplo Firewalls y mecanismos de encriptación, dando pie a una nueva generación de tecnologías que son principales para identificar, prevenir y proteger todo tipo de vulnerabilidades posibles dentro de la red.

Este llamado tecnológico ha sido beneficioso como el medio más adecuado y eficiente para la propagación del acceso indebido a la información o realización de transacciones licitas.

Debido al aumento de la capacidad y complejidad de las redes de información y de las organizaciones que las usan, las limitaciones de las soluciones puntuales para la seguridad de las distintas herramientas informáticas son incapaces de satisfacer las necesidades de la mayor parte de los entornos corporativos, así como de muchos de los usuarios domésticos.

También la disponibilidad, continuidad y escalabilidad de la masiva explosión de las redes han ampliado y agilizado enormemente las capacidades de millones de usuarios y corporaciones.

1.4.7 CONTROL DE ACCESO A LA RED (NAC)

Control de acceso a la red (del inglés *Network Access Control*, NAC) es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades), usuario o sistema de autenticación y reforzar la seguridad de la red de acceso. [13]

Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos, recursos lógicos o recursos digitales. El objetivo del control de acceso es realizar exactamente lo que su nombre implica, es decir, controlar el acceso a la red con políticas, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final y controles post-admisión sobre los recursos y dispositivos a los que pueden acceder los usuarios y verificar lo que pueden hacer en la red.

Las soluciones de control de acceso se utilizan para proteger los datos y sistemas de las empresas, asegurar el cumplimiento de las políticas legales y empresariales, y bloquear los equipos desconocidos o no autorizados. Al mismo tiempo, deben ser compatibles con las necesidades de acceso ininterrumpido a la red de los usuarios legítimos. Una solución NAC efectiva reduce el riesgo y los costos de la seguridad, identificando e impidiendo las amenazas y vulnerabilidades. Por medio de una evaluación constante de todos los equipos con respecto a las políticas definidas, el control de acceso a la red puede verificar, por ejemplo, que los parches de seguridad están instalados y que no se utilizan aplicaciones no permitidas. Los objetivos generales que persigue un NAC son:

- Reducción del riesgo de ataques desconocidos. El punto clave de las soluciones del NAC es la habilidad de prevenir el acceso a la red de equipos terminales que no posean software antivirus, parches de seguridad, o software de prevención de intrusión al equipo, evitando así poner en riesgo los demás equipos de la red contra contaminación de gusanos, virus o código malicioso.
- Ejecución de políticas de seguridad. Las soluciones NAC permiten a los administradores de red definir políticas, tales como cuáles tipos de computadoras, o cuáles perfiles de usuarios deben tener acceso a determinadas áreas de la red, y forzar su ejecución a través de switches o routers.

- Manejo de identidad y acceso. Mientras las redes IP convencionales ejecutan sus políticas de seguridad y acceso en base a direcciones IP, un NAC lo hace basándose en identidades autenticadas, al menos para equipos terminales de usuarios.

Para llevar a cabo un adecuado control de acceso se debe realizar una autenticación, es decir, identificar a los usuarios validos que puedan acceder a los sistemas informáticos. Además, se debe realizar una correcta asignación de privilegios a dichos usuarios. Y por último un registro de las operaciones ejecutadas en el sistema.

1.4.7.1 Tipos de Control de Acceso a la Red

Existen diferentes tipos de control de acceso a una red los cuales se explican a continuación:

- Basado en hardware. Tanto si es "*in-line*" o "*out-of-band*", esta opción necesita habitualmente de un equipo que tendrá que estar instalado en casi cualquier ubicación donde sea preciso contar con un NAC.
- Basados en agentes software. El siguiente paso es el basado en pequeños programas residentes en los ordenadores y dispositivos, instalándose estos agentes en cada uno de los sistemas que deban ser controlados por el NAC. Dichos agentes escanean y monitorizan el dispositivo, generalmente enviando los resultados a un servidor central. Los sistemas que no cumplen con los requisitos no tendrán autorización a la red, y a menudo se les envían algún tipo de medida correctora para que cumplan las directivas de seguridad.
- Sin agentes software. NAC sin agentes es otra de las variantes, y consiste en partes software que se ejecutan puntualmente. Con esta configuración, la idea es que un agente temporal (generalmente algún tipo de control ActiveX) escanee el cliente periódicamente en búsqueda de vulnerabilidades o incumplimientos en la política de seguridad. Los resultados del escaneo son enviados al servidor central de políticas, y se ejecuta una acción si es necesario en caso de que el sistema no cumpla con los requerimientos. Cuando el proceso se completa, el agente se descarga.
- NAC dinámico. El NAC dinámico, que utiliza agentes solo en un porcentaje determinado de equipos. También se conoce como NAC *peer-to-peer*,

siendo una opción que no requiere cambios a nivel de red o software que deba ser instalado en cada equipo. Los agentes, que en ocasiones pueden llegar a ser obligatorios, son instalados en sistemas seguros [14].

1.4.7.2 Elementos de un Control de Acceso a la Red

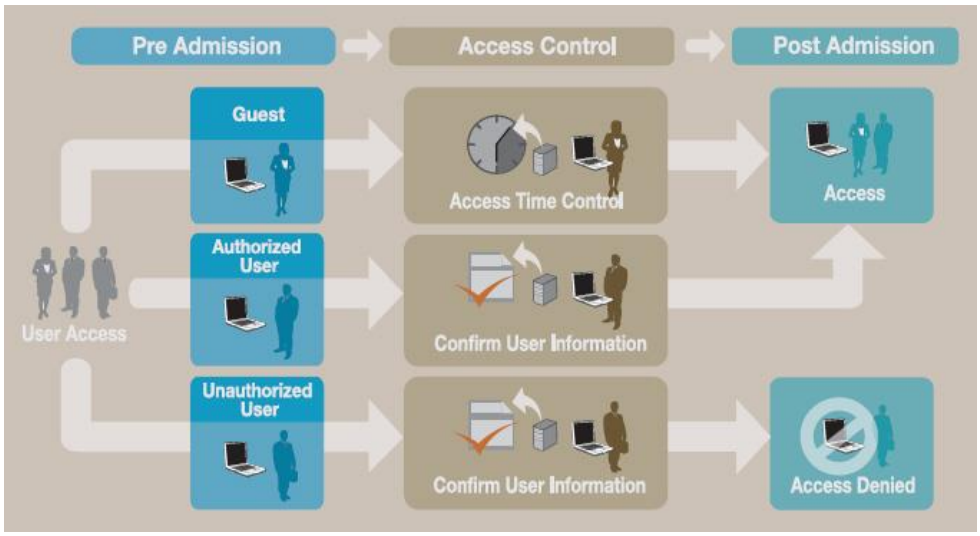


Ilustración 1 Elementos de NAC

Fuente Instituto Politécnico Nacional, 2010

Los elementos que integran un control NAC son los siguientes:

- Equipo cliente. En una red, los equipos clientes son empleados por los usuarios de una red tales como PC's, impresoras, servidores, entre otros.

- Autenticador. Entidad en un extremo de un segmento punto a punto de una LAN que facilita la autenticación de la entidad conectada al otro extremo del enlace.
- Nac Gateway. Es un dispositivo que se encuentra entre el servidor de autenticación y el equipo de usuario final. Este dispositivo permite controlar las acciones de autenticación y autorización mediante la manipulación de los atributos que entrega el servidor de autenticación, a fin de indicar al autenticador la acción a seguir.
- Servidor de autenticación. Entidad que facilita servicio de autenticación al autenticador. [15]

NAC impide el acceso de dispositivos no autorizados de forma automática y protege el riesgo de una falla en la red gracias a la política de administración integrada.

1.4.7.3 Conceptos de NAC

- **Pre-admisión y Post-admisión**: Basadas en políticas de ayuda antes de ganar acceso a la red de diseño predominante en NAC. En la pre-admisión que es el primer caso, las estaciones finales son controladas antes de autorizar el acceso a la red. Puede ser el caso de prevenir que los equipos que no tienen antivirus actualizados se conectaran a servidores sensibles.
  En el NAC post-admisión establece decisiones de refuerzo basada en acciones de usuario después de que a estos usuarios se les haya otorgado a la red.
- **Con agente vs sin agente:** En la tecnología de NAC, su idea fundamental es admitir a la red tomar decisiones de control de acceso basados en la inteligencia de los sistemas finales es una decisión de diseño clave. Los sistemas NAC pueden requerir agentes software para informar de las características de los equipos finales, o si por el contrario utilizan técnicas de escaneo e inventariado para discernir esas características remotamente.
- **Cuarentena y portal cautivo:** Las redes y los administradores de sistemas extienden productos NAC. Por ello las soluciones NAC requieren de un proceso para remediar el problema del usuario final que le ha sido denegado el acceso a la red.
  Existen dos estrategias para este remedio son portales cautivos y redes de cuarentena.
  Portales Cautivos: Restringen a los usuarios a una aplicación web, interceptando el acceso HTTP, que proporciona herramientas e

instrucciones para la actualización del computador. Cuando el equipo pasa la inspección automatizada, sin uso de la red.

Los portales cautivos externos permiten descargar a las organizaciones controladores inalámbricos. Una forma de consolidar los procesos de políticas de gestión, es cuando un portal único externo que ofrece un dispositivo NAC elimina la necesidad de crear varios portales para la autenticación inalámbrica.

Cuarentena: Provee a los usuarios acceso encaminado solo a determinados hosts y aplicaciones. La cuarentena a menudo empleado en la asignación de VLAN's, cuando un producto NAC decide que un usuario final no cumple con las políticas de seguridad, el puerto switch se asigna a una VLAN que va solo a los servidores de actualización y revisión, pero no al resto de la red. Para evitar la sobrecarga de la gestión de VLAN de cuarentena se pueden utilizar otras soluciones técnicas de gestión, como ARP (*Address Resolution Protocol*) o NDP (*Neighbor Discovery Protocol*).

- **Detección e identificación de nuevos dispositivos:** Se realiza a través de los switches donde los dispositivos están conectados recibiendo las peticiones de autenticación de los clientes.
- **Remediación para equipos con problemas de cumplimiento de políticas de seguridad:** Si algún dispositivo o equipo es trasladado a la zona de aislamiento, deben resolver los problemas de seguridad para lograr acceder a la red, como guía general se enseñan mensajes con los problemas que se han identificados y la forma de solucionarlos.

BYOD

Bring Your Own Device (BYOD), en español "trae tu propio equipo", es una política empresarial donde los empleados llevan sus propios dispositivos a su lugar de trabajo para tener acceso a recursos de la empresa como por ejemplo: correos electrónicos, bases de datos y archivos en servidores así como datos y aplicaciones personales. [9]Y en la práctica significa que los empleados de la empresa pueden aprovechar sus dispositivos inteligentes para llevar consigo la información y herramientas que necesitan para trabajar.

Gracias a las funcionalidades que presentan los Smartphone, así como la irrupción de tabletas que con su gran capacidad almacenamiento de datos, la conectividad y la estructura y diseño práctica para el trabajo con programas profesionales, ha posibilitado el surgimiento de una nueva cultura empresarial que los expertos vaticinan redefinirá la forma de trabajar en las corporaciones.

Adaptar los dispositivos de los trabajadores para su uso profesional aporta grandes oportunidades: aumento del rendimiento, flexibilización de la jornada laboral, movilidad total para trabajar desde cualquier parte del mundo.

Para el sector informático en concreto, el fenómeno BYOD presenta un gran reto: cómo gestionar y realizar un buen seguimiento de la información a la que se le da acceso a los empleados.

Aprovechar estas herramientas tan potentes que podemos llevarlas en nuestro bolsillo, maletín o bolso, para el ámbito profesional puede ser un gran paso hacia el aumento de la productividad y motivación de los empleados, pero podría convertirse en una gran problema si no se lleva un adecuado control de la información confidencial de la empresa. Ilustración 2.

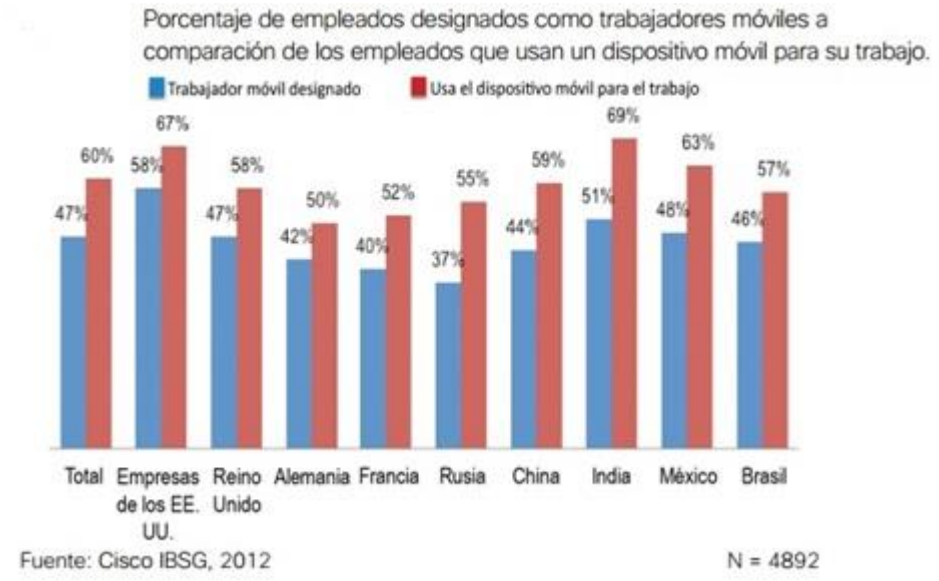


Ilustración 2 Comparación Cisco IBSG

El concepto de movilidad, que implica trabajar lejos de un entorno de oficina tradicional o de un lugar fijo, se ha convertido en un requisito común para el trabajador del conocimiento actualmente. El 47% de los empleados en las empresas están designados oficialmente como “trabajadores móviles”. Pero el 60% de los empleados usan un dispositivo móvil para su trabajo, un 13% más que quienes están considerados oficialmente como “trabajadores móviles” (consulte la Ilustración 2).

En su mayoría, estos dispositivos adicionales son el resultado de una iniciativa de los empleados: aun cuando “oficialmente” no necesitan dispositivos móviles para hacer su trabajo, integran la movilidad a su modo de trabajo, en forma cotidiana. Y los departamentos de TI corporativos les hacen el favor. Las empresas segmentan

a los trabajadores móviles, el 36% afirmó que otorgan privilegios de movilidad según la solicitud del empleado.

1.4.8 Ventajas del software libre

- Económico
- Libertad de uso y redistribución
- Independencia tecnológica
- Fomento de la libre competencia al basarse en servicios y no licencias
- Corrección más rápida y eficiente de fallos
- Métodos simples y unificados de gestión de software

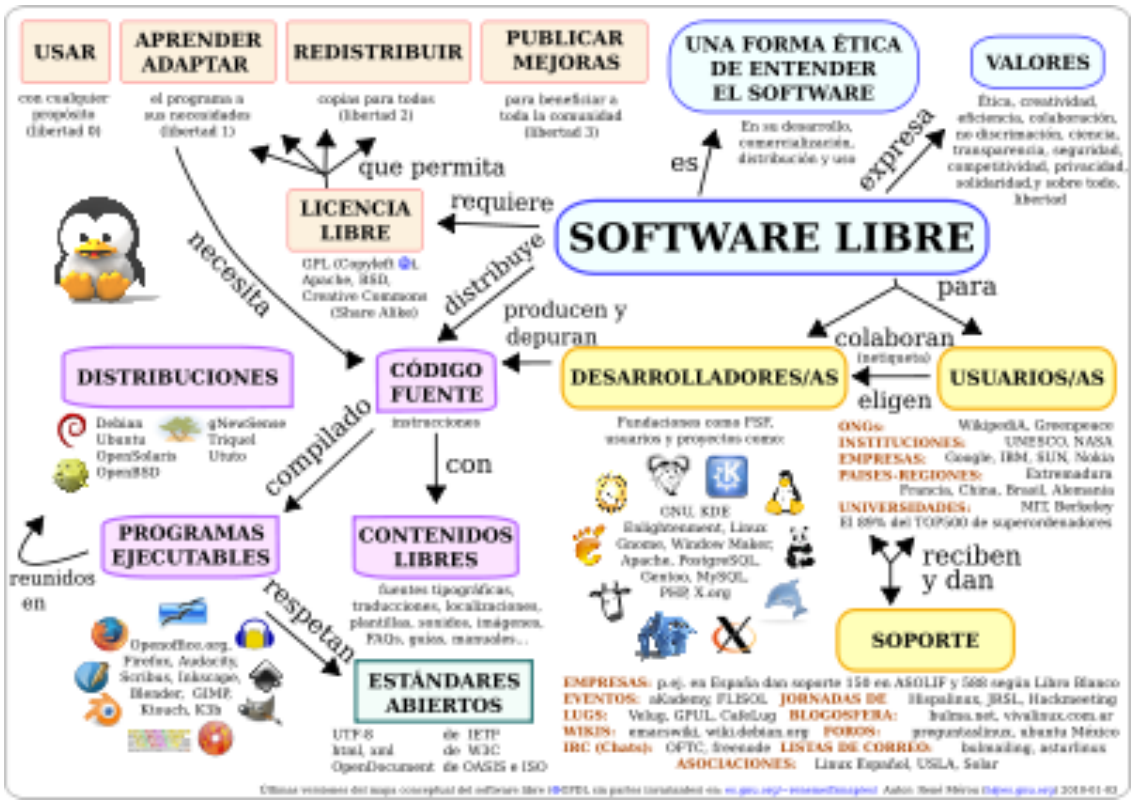


Ilustración 3 Ventajas Software Libre *[16]*

CAPITULO II

2. ESTADO DEL ARTE

En este capítulo se realiza una revisión de algunos trabajos de investigación existentes en el área de BYOD, que implementaciones tiene a nivel mundial, también se hace síntesis mediante un cuadro de las herramientas tanto propietarias y OpenSource de NAC, para seleccionar una herramienta mediante la tabla de comparación, posteriormente se definen las características del aplicativo seleccionado.

Trabajos de Investigación BYOD	
Título	**Descripción**
Investigación hecha por Cisco "El impacto financiero de BYOD, un modelo de los beneficios de BYOD para las empresas globales"	Análisis, diseñado para ayudar a las empresas a entender los costos y beneficios financieros de la implementación de BYOD. [17]
Artículo BYOD "*The results and the future"*	Este documento da a conocer los resultados de los programas de BYOD maduros e identifica las mejores practicas [18]
Analysis os Security Controls for BYOD	Este trabajo investiga sobre impacto de BYOD para la seguridad de la organización, identifica también las áreas clave en las que las organizaciones pueden implementar la seguridad. [19]
Technology Overview for emerging mobile device management services in Asia/Pacific	Este articulo trata sobre la administración de dispositivos móviles y la tecnología general para los nuevos servicios, teniendo en cuenta la importancia de las políticas BYOD. [20]

Tabla 1 Trabajos de Investigación BYOD

De acuerdo con los trabajos de investigación de BYOD, los administradores de TI en el mundo están anticipando los mismos beneficios de productividad en las redes móviles. A nivel de las instituciones no se encuentran muchos informes o artículos de aplicaciones y políticas de BYOD por lo nuevo de la tendencia y por los costos que pueden representar la implementación de soluciones comerciales. Como conclusión de este análisis de las investigaciones revisadas, se puede determinar que antes de poder realizar una implementación de políticas BYOD a una red, es recomendable considerar algunos retos vinculados al control de acceso a la red (NAC). Por otra parte este proyecto pretende mostrar como alternativa a las soluciones comerciales, como las soluciones de software libre pueden lograr ofrecer soluciones tan completas como las comerciales y cuyos costos de licenciamiento de software son de menor cuantía y asequibles para pequeñas y medianas instituciones.

2.1 ANÁLISIS DE SOLUCIONES NAC PROPIETARIAS Y OPENSOURCE

Este tema se encamina a estudiar las distintas soluciones NAC en el mercado, con sus diferentes fabricantes. Algunas soluciones propietarias con versiones

avanzadas que solicitan de licenciamiento, por lo que representa una inversión económica superior para adquirirla, por lo que las soluciones OpenSource están cada vez mejor posicionadas en este aspecto. En la siguiente tabla se ven algunas soluciones propietarias en el mercado, su fabricante y características.

2.1.1 Soluciones Propietarias

Producto	Descripción de la Solución	Fabricantes/Desarrolladores	URL
Cisco NAC Framework	Iniciativa propietaria de Cisco basada en la implantación de control de acceso dentro de la infraestructura de red.	Cisco NAC	http://www.cisco.com/c/en/us/solutions/enterprise-networks/network-admission-control-nac-framework/index.html
Cisco NAC Appliance	Equipos Cisco que permiten una rápida implantación de políticas de control de acceso a la red sin realizar cambios en switches y routers.	Cisco NAC	http://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html
ConSentry LANShield	Solución NAC de alto rendimiento pensada para ser desplegada de forma perimetral. Control de acceso basado en identidad, políticas y datos del usuario.	Basada en dispositivos propios, appliances creados por ConSentry	http://www.infoworld.com/article/2651128/security/network-security-review--consentry-lanshield-switch.html
Elemental Security Plataform	Sistema diseñado para monitorizar dispositivos de red, configuraciones, actividad de los usuarios, implementando políticas de seguridad basada en roles.	Propietaria, basada en un modelo de servidores y software de agentes	http://www.elementalsecurity.com/
ENDFORCE Enterpris	Solución basada en software, diseñada para redes	Basada en estándares, compatible con C-NAC, NAP y TNC	http://searchsecurity.techtarget.com/magazineContent

e	heterogéneas, con la capacidad de extender las funcionalidades ofrecidas por las arquitecturas NAC, NAP y TNC.		/Network-Access-Control-Endforces-Enterprise-25
FireEye NAC Appliance	Basada en appliances que implanta el control de acceso basándose en la inspección del tráfico de los dispositivos de la red, y por tanto en la detección de tráfico peligroso o dañino.	Propietaria, basada en dispositivos propios junto con la tecnología FACT	http://www.computerworld.com/article/2555111/security0/fireeye-debuts-with--virtual-machine--security.html
Juniper Networks Unified Access Control (UAC)	El Control de acceso unificado 2.0 incluye varios elementos: Infranet Controller, agente UAC y puntos de aplicación de la política de seguridad. Funciona en gran variedad de entornos, incluyendo aquellos con 802.1X.	Compatible con la arquitectura TNC	http://www.juniper.net/us/en/local/pdf/datasheets/1000137-en.pdf
Symantec Network Access Control	Ofrece una solución que permite aplicar control de acceso para dispositivos que se conecten a través de SSL VPNs, switches inalámbricos, aplicaciones basadas en Web, usando 802.1X, y casi cualquier infraestructura LAN o inalámbrica.	Compatible con la arquitectura Cisco NAC	https://support.symantec.com/en_US/article.HOWTO95154.html
Microsoft NAP	Iniciativa propietaria de Microsoft	Microsoft NAC	https://msdn.microsoft.com/en-us/library/windows/desktop/aa369712(v=vs.85).aspx

HP Procurve Networking Adaptative EDGE	Arquitectura que permite construir redes con inteligencia perimetral, que pone la inteligencia en el punto de conexión del usuario, permitiendo realizar en ese punto funciones como la priorización de tráfico, autenticación, reserva de ancho de banda y aplicación de políticas.	Arquitectura propietaria	http://www.hp.com/rnd/pdf_html/edge_architecture_whitepaper.htm

Tabla 2 Soluciones Propietarias

De la tabla anterior en donde se relacionan las diferentes soluciones que se pueden encontrar a nivel comercial para la implementación de NAC y BYOD se destacan las de la empresa Cisco que son líderes de la industria y ofrecen una solución modular y robusta para su implementación. Los otros fabricantes ofrecen soluciones que se enfocan más al control de acceso y otros se podrían utilizar más como complemento para la implementación de políticas BYOD. Todas las anteriores se caracterizan por sus altos costos de adquisición y modelos de licenciamiento que están relacionadas directamente con la cantidad de dispositivos que se van a gestionar, lo cual hace que a mayor tamaño del parque computacional de una organización mayor su costo de licenciamiento, razón por la cual esto hace inviable en pequeñas y medianas organizaciones su implementación.

2.1.2 Soluciones NAC OpenSource

Herramienta	Descripción de la Solución
FreeNAc	Proporciona una solución transparente para el manejo dinámico de redes virtuales, a la vez limita la conectividad a la red. Reduce la carga de gestión para equipos de red y brinda un nivel de seguridad alta centrada en los clientes que acceden. [21]
PacketFence	Totalmente confiable, compatible y libre. Incluye un conjunto de funciones que incorpora un portal para el registro y la rehabilitación de cable e

	inalámbrica, puede utilizarse efectiva redes de seguridad. [22]
OpenNac	Código abierto de control de acceso de red para entornos LAN/WAN corporativa. Permite la autenticación, autorización y auditoria de políticas basadas en todos los accesos de red. [23]

Tabla 3 Soluciones OpenSource

La tabla anterior resume las tres (3) soluciones OpenSource que cumplen con la mayor cantidad de opciones que demanda una infraestructura de NAC en una red de datos y la posibilidad de implementar políticas tipo BYOD a dispositivos móviles que se conecten.

De las tres soluciones se ha seleccionado PacketFence por cumplir con la mayoría de los componentes de una infraestructura NAC según sus principios de diseño y por incluir la posibilidad de implementar políticas tipo BYOD en redes inalámbricas que soportan la mayoría de equipos móviles que se conectan.

2.2 COMPARACIÓN Y SELECCIÓN DE HERRAMIENTA DE SOFTWARE LIBRE PARA IMPLEMENTAR NAC Y POLÍTICAS BYOD

2.2.1 Tipos de NAC

Soluciones Comerciales

- *Network Admisión Control NAC Cisco*
- *Network Access Protection NAP Microsoft*
- *Unified Access Control UAC Juniper*
- *Trusted Network Connect TNC Trusted Computing Group*

Soluciones OpenSource

- *Opennac OpenSource* NAC Solution
- *PacketFence*
- *NAC Take control of your LAN*

2.2.2 Tabla comparativa de elección de PacketFence respecto a otras soluciones NAC

Actualmente en el mercado hay múltiples posibilidades de soluciones NAC, en este caso se realiza la comparación de una solución comercial y dos soluciones OpenSource para los requerimientos de implementación de presente proyecto considerando las funcionalidades.

Fabricante	Políticas Dinámicas	Política por puerto	Integración otros fabricantes	Integración Directorio Activo	Soporte Máq. Virtuales	Edición de módulos e interfaz	Detección Dispositivos	Soporte Actualizado	VLANs Dinámicas.	Agente
Cisco	✓	X	X	✓	✓	X	X	✓	X	✓
FreeNac	✓	✓	✓	✓	X	X	X	X	✓	X
PacketFence	✓	✓	✓	✓	✓	✓	✓	✓	✓	X

Tabla 4 Comparación Soluciones NAC

La solución de Cisco sería aconsejable para redes homogéneas con dispositivo Cisco ya que no presentara problemas de incompatibilidad con la red siendo toda del mismo fabricante. Esta solución trabaja con un appliance apoyada en hardware para autenticar y conceder acceso a dispositivos finales, un agente recopila los datos en el dispositivo y un gestor para administración de políticas

La solución FreeNac podría ser utilizada para una pequeña red que necesite el mínimo de seguridad y que no requiere alta disponibilidad, ya que este tipo de NAC que es basada en software disminuye la carga de gestión para equipos de red y brinda un nivel alto de seguridad centrado en los clientes que aceptan.

La solución PacketFence es la que mayor se adapta a las necesidades, ya que es capaz de detectar el tipo de dispositivo que intenta acceder a la red, detección de intrusos y detección de vulnerabilidades. Esta solución aporta un portal cautivo, permite la configuración de Vlans dinámicas. Una solución basada en software facilita la gestión administrativa de la red sin necesidad de un análisis exhaustivo de esta. [24]

Como se puede observar en la tabla anterior de comparación de soluciones NAC, PacketFence fue seleccionado porque es la que mejor cumple con las necesidades con respecto a las otras soluciones, proporciona una mayor seguridad basada en software que facilita la gestión de administración de la red y cuenta con documentación técnica, guía de instalación que facilitan la

implementación, cuando los usuarios se registran a la red, los sistemas deben ser revisados para tener un nivel de fiabilidad adecuado, según las políticas de seguridad interna de la red, además por ser OpenSource no tiene ningún costo para obtenerlo. La forma en la que las diferentes soluciones realizan el trabajo depende de si son basadas en hardware, en línea, con agente o sin él pueden hacerlas un poco más complejas.

A continuación una tabla del porcentaje del cumplimiento de los parámetros en la comparación de soluciones NAC.

Solución	**Porcentaje**
PacketFence	90 %
FreeNac	50 %
Cisco	50 %

2.3 PACKETFENCE

PacketFence es una solución OpenSource confiable, libre, compatible y ampliamente soportada. Puede ser empleado para asegurar redes desde pequeñas a grandes de forma efectiva.

PacketFence tiene un conjunto de características entre las que están un portal cautivo para registro, administración para redes cableadas e inalámbricas, aislamiento de capa 2 para equipos que tienen problemas, soporte 802,1X, integración con Snort IDS y scanner de vulnerabilidades Nessus.

2.3.1 Modo de operación PacketFence

PacketFence es una solución a escala geográfica amplia y resistente a fallos. Cuando se utiliza la tecnología adecuada (como la seguridad de puerto) un único servidor puede ser usado para controlar cientos de interruptores (switchs) y en múltiples nodos.

Es una solución que puede utilizarse en redes de:

- Bancos, Empresas de ingeniería y Fábricas

- Colegios y universidades

- Centras de convenciones y exposiciones

- Hospitales, centros médicos

- Hoteles

Dentro de la arquitectura están los componentes

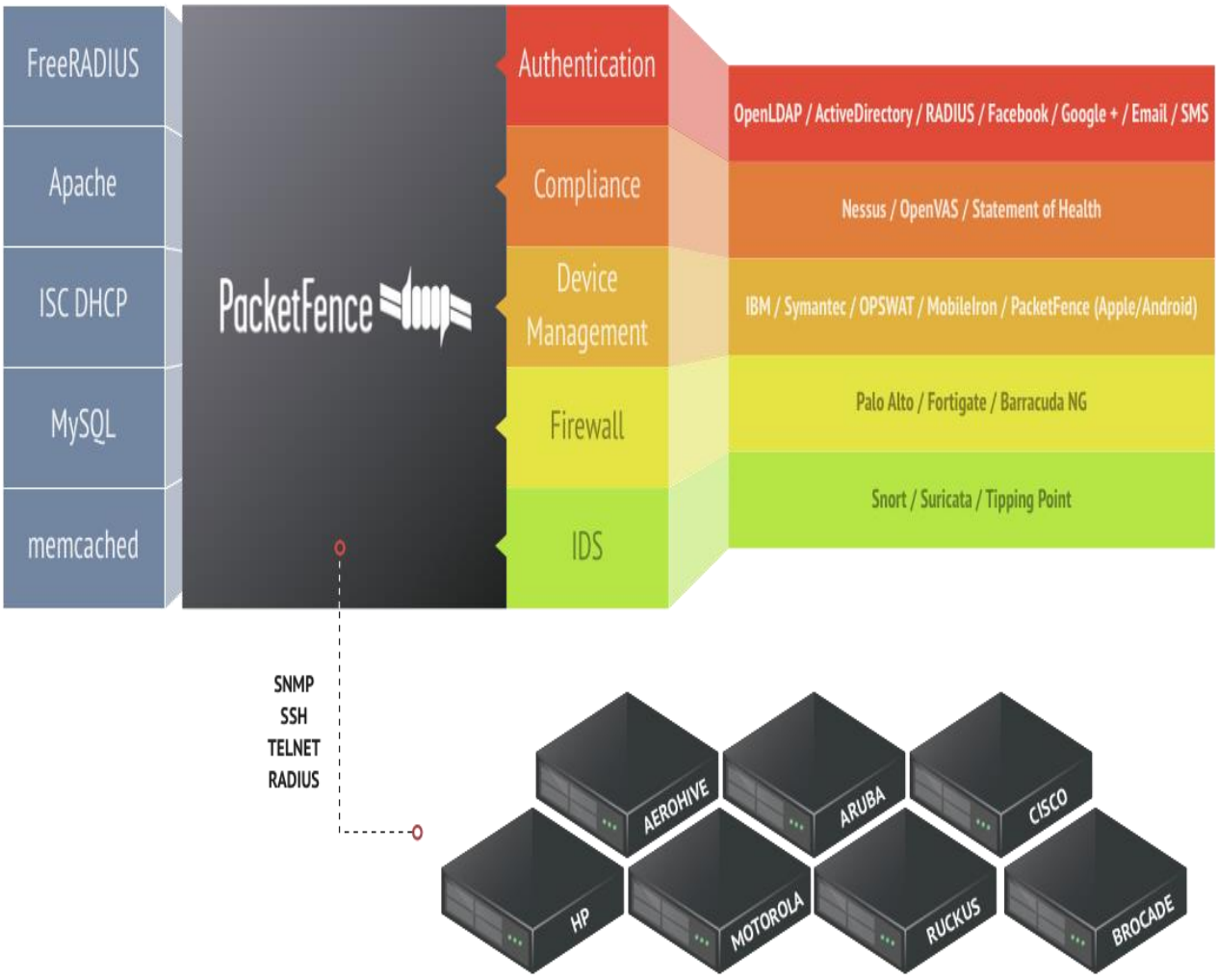


Ilustración 4 Componentes PacketFence

2.3.2 Autenticación y registro

- **Soporte 802.1X:** inalámbrico y cableado se apoya por un FreeRADIUS módulo que se incluye en PacketFence.

- **Integración inalámbrica:** integra perfectamente con las redes inalámbricas a través de una FreeRADIUS modulo. Esto le admite asegurar las redes cableadas e inalámbricas de la misma manera utilizando la misma base de datos del usuario y utilizando el mismo portal cautivo, proporcionando una experiencia de usuario consistente. Mezcla de puntos de acceso (AP) proveedores y controladores inalámbricos es compatible.
- **Voz sobre IP:** Es también llamada de telefonía IP, VoIP es totalmente compatible para diversos proveedores de conmutación.

- **Registro de dispositivos**: defiende un mecanismo de registro opcional similar a soluciones "portal cautivo". A diferencia de las otras soluciones de portal cautivo, PacketFence recuerda a los usuarios que previamente registrados y automáticamente les da el acceso sin otra autenticación. También es configurable. Una política de uso aceptable se puede especificar de forma que los usuarios no pueden permitir el acceso a la red sin antes aceptarla.

2.3.3 Detección de vulnerabilidad

- **Detección de actividades anormales de red:** Actividades de la red anormales (virus informáticos, gusanos, spyware, tráfico denegado por la política de establecimiento, etc.) pueden ser detectados utilizando local y remota Snort. Más allá de la detección simple, capas PacketFence su propia alerta y la supresión del mecanismo en cada tipo de alerta. Un conjunto de acciones configurables para cada violación, está disponible para los administradores.

- **Scans de vulnerabilidad proactivas:** Nessus u OpenVAS vulnerabilidad exploraciones se pueden realizar en el registro, programadas o sobre una base ad-hoc. PacketFence correlaciona los ID de la vulnerabilidad de cada uno de exploración a la configuración violación Nessus / OpenVAS, volviendo el contenido de páginas web específicas sobre las que la vulnerabilidad del huésped pueda tener.

- **Declaración de Salud:** Mientras que hace una autenticación de usuario 802.1X, PacketFence puede realizar una evaluación de la postura completa del dispositivo de conexión con el TNC Declaración de protocolo de la Salud. Por ejemplo, PacketFence puede verificar si se ha instalado un antivirus y hasta a la fecha, si los parches del sistema operativo son todos aplicada y mucho más, todo sin ningún agente instalado en el dispositivo de punto final.

2.3.4 Portal Cautivo

- **Remediación A través de un portal cautivo:** Una vez atrapado, todo el tráfico de la red se termina por el sistema PacketFence. En base a la situación actual de los nodos (no registrado, violación abierta, etc.), el usuario es redirigido a la URL correspondiente. En el caso de una violación, el usuario será presentado con las instrucciones para la situación particular que él / ella está en, reduciendo la intervención costosa mesa de ayuda.

- **El aislamiento de los dispositivos problemáticos:** PacketFence soporta varias técnicas de aislamiento, como el aislamiento de VLAN con soporte VoIP (incluso en entornos heterogéneos) para varios fabricantes de switches.

2.3.5 Administración

- **De línea de comandos y gestión basada en Web:** Interfaces basadas en Web y de línea de comandos para todas las tareas de gestión. Administración basada en Web es compatible con diferentes niveles de permisos para usuarios y la autenticación de usuarios contra LDAP o *Microsoft Active Directory*. (PacketFence)

2.3.6 Características avanzadas

El nodo se utiliza para referirse a un dispositivo de red consciente de que es controlado y supervisado por PacketFence. Puede ser un PC, ordenador portátil, impresora, teléfono IP, etc.

- **Gestión VLAN flexible y control de acceso basado en roles**:
  VLAN y los roles se pueden asignar utilizando los diversos medios:
- Por interruptor (por defecto para VLAN)
- Por categoría de cliente (por defecto para papeles)
- Por cliente

- **El acceso de invitados - Traiga su propio dispositivo (BYOD):** Hoy en día, la mayoría de las organizaciones se ocupan de una gran cantidad de

consultores de diversas empresas en las instalaciones que requieren acceso a Internet para su trabajo. En la mayoría de los casos, un acceso a la red corporativa se da con poca o ninguna auditoría de la persona o dispositivo. Además, rara vez se requiere que tengan acceso a la infraestructura corporativa interna, que se hace de esa manera para evitar (administración de VLAN por puerto) carga administrativa.

Si utiliza una VLAN de invitados, configurar la red para que la VLAN de invitados solamente sale a la Internet y la VLAN de registro y el portal cautivo son los componentes que se utilizan para explicar a los invitados cómo registrarse para el acceso y cómo sus obras de acceso. Esto normalmente se marca por la organización que ofrece el acceso a la red. Son posibles varios medios de huéspedes para:

- Registro manual de los huéspedes
- Contraseña del día
- Auto-inscripción (con o sin credenciales)
- Acceso para patrocinar invitados (empleado que dé fe de un huésped)
- Acceso para invitados activado por correo electrónico de confirmación
- Acceso para invitados activado por la confirmación de teléfono móvil (mediante SMS)
- Acceso para invitados activado a través de una autenticación de Facebook / Google / GitHub

PacketFence también soporta el acceso para invitados creaciones a granel y las importaciones. PacketFence también se integra con la solución de facturación en línea, como Authorize.net. El uso de esta integración, que puede manejar los pagos en línea, necesarios para obtener acceso a la red adecuada.

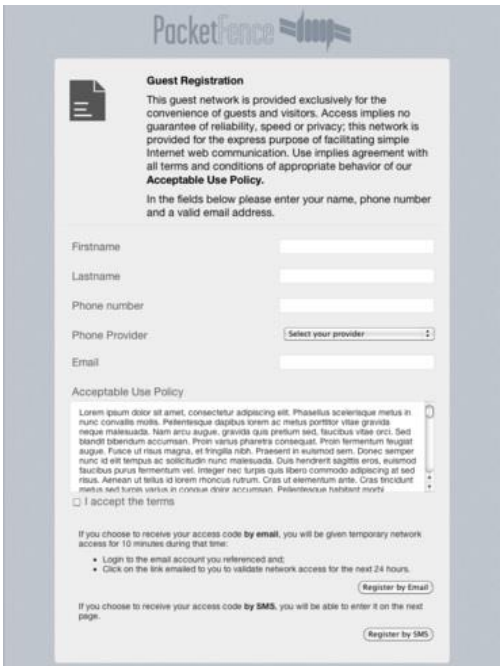


Ilustración 5 Acceso a invitados

Modos de funcionamiento

Puede ser desplegado en 3 modos de funcionamiento

- **Out-Of-Band:** en este modo el servidor de PacketFence se encarga de realizar las comprobaciones de políticas, acceso a la red, consulta a servidores de autenticación, este modo es el más usado siendo el método más escalable, resistente a fallos y es utilizado en las redes que soportan Vlans.
- **In-Band:** utilizado en redes con switchs antiguos. Desde la versión 3.0 de PacketFence se implementa el modo “In-Line” donde el servidor PacketFence se convierte en la puerta de enlace de la red, donde se conectan todos los dispositivos incompatibles.
  Este modo tiene varias limitaciones que pueden ser:
  a. Todos los dispositivos de la red están en la misma LAN de capa 2, donde se ve afectado por temas de broadcast en el caso de muchos dispositivos.
  b. Todos los paquetes enviados por los dispositivos deben pasar por el servidor de PacketFence, por lo que aumenta la carga de trabajo en el servidor.
  c. Dispositivos de red sin autenticar

- **Modo Hibrido:** soporta el modo de autenticación 802.1x y autenticación por MAC, es posible autenticar dispositivos por medio de RADIUS a través de 802.1x o autenticación por Mac desde la versión 3.6 de PacketFence.

Perfiles del Portal

PacketFence apoya el concepto de perfiles del portal. Un perfil de portal define el flujo de trabajo de registro que se utilizará, junto con las páginas de registro y regularización.

User – Agent

PacketFence puede bloquear dispositivos basados en el User-Agent proporcionado cuando esos dispositivos particulares realizan actividad de la red utilizando su navegador web incorporado.

Direcciones MAC

PacketFence puede bloquear el acceso de red a dispositivos que tienen un patrón específico de direcciones MAC. Usando esto, se podía bloquear de forma automática, por ejemplo, todos los dispositivos de un proveedor de red específica.

Inscripción automática

Porque la mayoría de las redes de producción ya son muy grandes y complejos, PacketFence ofrece varios medios para registrar automáticamente un cliente o dispositivo.

- Por dispositivo de red:
  Un dispositivo de red (Switch, AP, mando inalámbrico) se puede configurar para registrar automáticamente todas las direcciones MAC que la solicitud de acceso a la red. Muy útil para la transición a la producción.

- Por DHCP toma de huellas dactilares:
  Huellas dactilares DHCP se puede utilizar para registrar automáticamente los tipos específicos de dispositivos (por ejemplo. Los teléfonos VoIP, impresoras).

- Por dirección MAC del vendedor:
  La parte del proveedor de una dirección MAC se puede utilizar para registrar automáticamente los dispositivos de un proveedor. Por

ejemplo, todos los productos de Apple podrían ser registrados de forma automática utilizando una norma de este tipo.

Caducidad

La duración acceso a la red puede ser controlada con los parámetros de configuración. Puede ser una fecha absoluta, una ventana cuando el dispositivo se vuelve inactiva (por ejemplo. "Cuatro semanas desde el primer acceso a la red") o. Vencido dispositivos registrados se convierten en no registrado. Con poca personalización también es posible hacer esto en una base categoría de dispositivo. Vencimiento también se puede editar manualmente en función de cada nodo.

Auditoria de Ancho de banda

PacketFence puede rastrear automáticamente la cantidad de ancho de banda consumen dispositivos en la red. Con su apoyo violaciones incorporados, se puede poner en cuarentena o cambiar el nivel de acceso de los dispositivos que consumen demasiado ancho de banda durante una ventana de tiempo en particular. PacketFence también tiene informes sobre el consumo de ancho de banda. [25]

CAPITULO III

3. DISEÑO DEL PROTOTIPO PARA LA IMPLEMENTACIÓN DE NAC POR MEDIO DE SOFTWARE LIBRE PARA CREAR POLÍTICAS BYOD

3.1 DESCRIPCIÓN DE LA INFRAESTRUCTURA UTILIZADA EN EL PROTOTIPO

Para hacer uso de la herramienta PacketFence OpenSource seleccionada se habilita un escenario de pruebas para tener una visión global del sistema.

Los equipos clientes se conectan a la red con un conjunto de credenciales que proporciona y validan para autorizar el nivel apropiado de acceso a la red, dentro de las credenciales puede ir la identificación del usuario. Según el tipo de autenticación ya sea por el portal cautivo o 802.1x el switch envía los datos del

cliente para conectarse con el servidor de PacketFence y verificar si el usuario cumple con las reglas que se establecen.

3.2 DIAGRAMA DE RED

3.2.1 Diseño físico

La topología física utilizada para las pruebas en la red está conformada por un portátil que actúa como servidor para el uso de toda la configuración de PacketFence, equipos móviles como portátiles y smartphones como invitados, un switch para la conectividad cableada y para la prueba inalámbrica un router inalámbrico. A continuación el diseño de la red de laboratorio de pruebas propuesto.

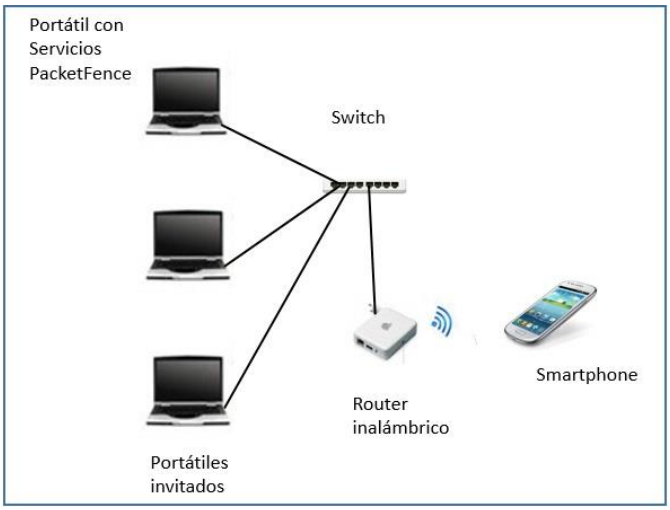
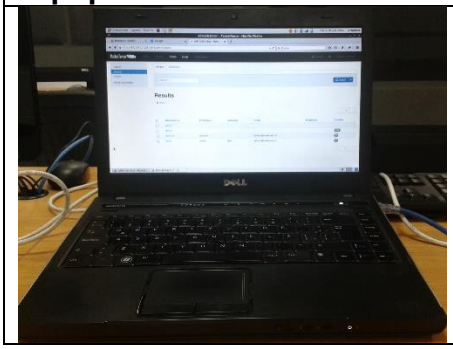


Ilustración 6 Diseño Físico de la red

Especificaciones equipos utilizados en pruebas de laboratorio

Equipos	Especificaciones
	*Dell Vostro 3360 (Core i5-3317U)* Este es el equipo donde está instalado el sistema operativo CentOS y configurado el servidor de PacketFence.

	*D-Link GO-SW-8E Switch 10/100 8 Puertos* Switch utilizado para hacer las conexiones del diagrama de red.
	*LENOVO ThinkPad X230 Laptop* Portátil utilizado como usuario invitado para las pruebas de los servicios de PacketFence.
	*Router Inalámbrico Apple AirPort Express Base Station Pequeña* Router inalámbrico utilizado en las pruebas para conectar dispositivos móviles como el Smartphone.
	*Smartphone S3 mini Sistema Operativo Android* Dispositivo utilizado para las pruebas con conexión inalámbrica.

Tabla 5 Equipos de pruebas

3.3 REQUISITOS DEL SISTEMA

PacketFence se apoya en diferentes componentes para un adecuado funcionamiento por lo que se deben tener instalado los siguientes componentes:

- Servidor DHCP
- Servidor Radius
- Servidor web Apache
- Base de Datos MySql

- IPS Suricata, IDS Snort

3.3.1 Requisitos mínimos de Hardware

- Intel o AMD CPU 3 GHz
- 100 Gb de espacio libre en disco
- 1 tarjeta de red

Opcionales

- 1 tarjeta para alta disponibilidad
- 1 tarjeta para detección de intrusos

3.3.2 Requisitos mínimos de sistema operativo

- Red Hat Enterprise Linux 6.x
- CentOS 6.x
- Debian 7.0
- Ubuntu 12.04 LTS

La herramienta PacketFence reutiliza muchos componentes y requiere los siguientes:

- Base de Datos del servidor
- Servidor web

Depende de la configuración pueden haber componentes adicionales:

- Servidor DHCP
- Servidor DNS
- Servidor RADIUS
- NIDS (Snort / Suricata)

Estos componentes se ejecutan en un mismo servidor en el cual PacketFence se instala.

3.4 DEFINICIÓN DE POLÍTICAS BYOD/NAC A IMPLEMENTAR

3.4.1 Políticas del aplicativo seleccionado

A continuación se relacionan las diferentes políticas que se definen para que se prueben en la red de laboratorio que se diseñó.

Parámetros	**PacketFence**
Requerimientos	
Política de Control de acceso	Los usuarios no pueden disponer el acceso a la red, sin estar autenticado anteriormente.

Tabla 6 Parámetros PacketFence

Gestión de acceso al usuario	
Registro de cliente	PacketFence ha creado una aplicación fácil para registrar los datos del usuario con sus contraseñas.
Gestión de privilegios	A los usuarios se les puede asignar un privilegio ya sea administrador o invitado. Un usuario no registrado no accede a la red.
Claves de los usuarios	Al registrar un usuario con su clave puede ser almacenado en OpenLdap, donde se guarda de manera cifrada para su seguridad.
Examinación de derechos para acceder a la red	Se hace revisión en la base de datos antes de que el usuario intente acceder a la red.

Tabla 7 Política: Gestión de acceso al usuario

Responsabilidades del usuario	
Empleo de claves	Para un cumplimiento de políticas de seguridad se recomienda a los usuarios el uso de claves, sin embargo cuando los usuarios ingresan los datos las contraseñas tienen una validación para un mínimo grado de seguridad.

Política de escritorio y pantalla limpia	Para este caso no cumple
Equipo de cliente desatendido	Cuando el usuario deja el equipo por un lapso de tiempo su acceso se bloquea y tendrá que autenticarse nuevamente.

Tabla 8 Política: Responsabilidades del usuario

Control de Acceso a la red	
Política sobre el uso de los servicios	Esta política es para cumplir la autenticación que todos los usuarios deben hacer.
Identificación de equipos en las redes	Los equipos ya autenticados se identificaran por la dirección MAC
Protección de puerto y configuración remota	NO
Segregación de redes	Las Vlans permiten la creación de redes lógicamente independientes dentro de una red física. PacketFence asigna la VLan a un dispositivo que puede ser una VLan especial donde PacketFence actúa como servidor DNS, DHCP, HTTP donde se ejecuta el portal cautivo.
Control de conexión a la red	El sistema de control de acceso basado en la norma 802.1x que permite la autenticación.
Control de enrutamiento a la red	No

Tabla 9 Política: Acceso a la red

Control de acceso al sistema operativo	
Procedimiento de un registro seguro	No
Identificación y autenticación de usuarios	Los usuarios para poder acceder a la red tienen un identificador único.
Sistema de gestión de contraseñas	Las contraseñas son guardadas en formatos de encriptación.
Limitación del tiempo de conexión	Se asigna un tiempo específico para la conexión

Tabla 10 Política: Control de acceso al sistema operativo

Las anteriores políticas que se han definido son las que serán validadas en la red de laboratorio de pruebas con la implementación del PacketFence y así demostrar su cumplimiento en un ambiente operativo controlado.

CAPITULO IV

4. IMPLEMENTACIÓN, PLAN DE PRUEBAS Y VALIDACION DEL PROTOTIPO IMPLEMENTADO

4.2 IMPLEMENTACIÓN PACKETFENCE

Instalación de PacketFence

Para iniciar las pruebas se basa en los manuales de PacketFence que se encuentran en

http://www.packetfence.org/documentation/guides.html

Se encuentra el manual de instalación de la herramienta por medio de la página de PacketFence en la siguiente dirección:

http://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Administration_Guide-4.0.6.pdf

Prueba con el sistema operativo Ubuntu 12.04

Para empezar con los requerimientos que necesita el aplicativo seleccionado se realizaron pruebas en el sistema Ubuntu 12.04 instalándolo y actualizando, se realizan las instrucciones del manual suministrado por el sitio oficial de PacketFence y por otros sitios encontrados pero el resultado es fallido ya que las dependencias de las librerías no encajan, el error generado es que las librerías requeridas por PacketFence son superiores a las del sistema operacional, aun cuando se descarga el paquete y no se instala con apt-get genera errores de dependencias, que aunque se tratan de corregir no se logra hacer funcionar.

Prueba con el sistema operativo CentOS 6

Se instala CentOS release 6.6 y se actualiza, se envía instalación de PacketFence y resulta exitosa la prueba, a continuación se describen los pasos seguidos para su instalación y configuración.

Se realizó una prueba con una versión empaquetada para deshacerse en una unidad o USB a base de CentOS 6.6, y funciona.

Se desactiva el Firewall, el complemento llamado Selinux

```
Yum update


disable firewall


-disable selinux


[root@proyecto ~]# sestatus | grep -i mode
Current mode:                enforcing
Mode from config file:          enforcing


[root@proyecto ~]# setenforce 0
[root@proyecto ~]# sestatus | grep -i mode
Current mode:                permissive
Mode from config file:          enforcing
```

Añadir el repositorio a través del yum que es una de las formas más fácil de instalar PacketFence y crear el archivo de depósito PacketFence en el directorio /***etc/yum.repos.d/PacketFence.repo*** con el siguiente contenido

```
[PacketFence] name=PacketFence Repository
baseurl=http://inverse.ca/downloads/PacketFence/RHEL$releasever/$basearchgp
gcheck=0
```

Luego se descarga el paquete de *rpmforge* para poder instalar PacketFence.

http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm

Hacer la descarga directa

http://packetfence.org/downloads/PacketFence/RHEL6/x86_64/RPMS/packetfence-release-1-1.el6.noarch.rpm

Y proceder a instalar donde se descarga una cantidad de paquetes necesarios.

```
yum -y install packetfence
```

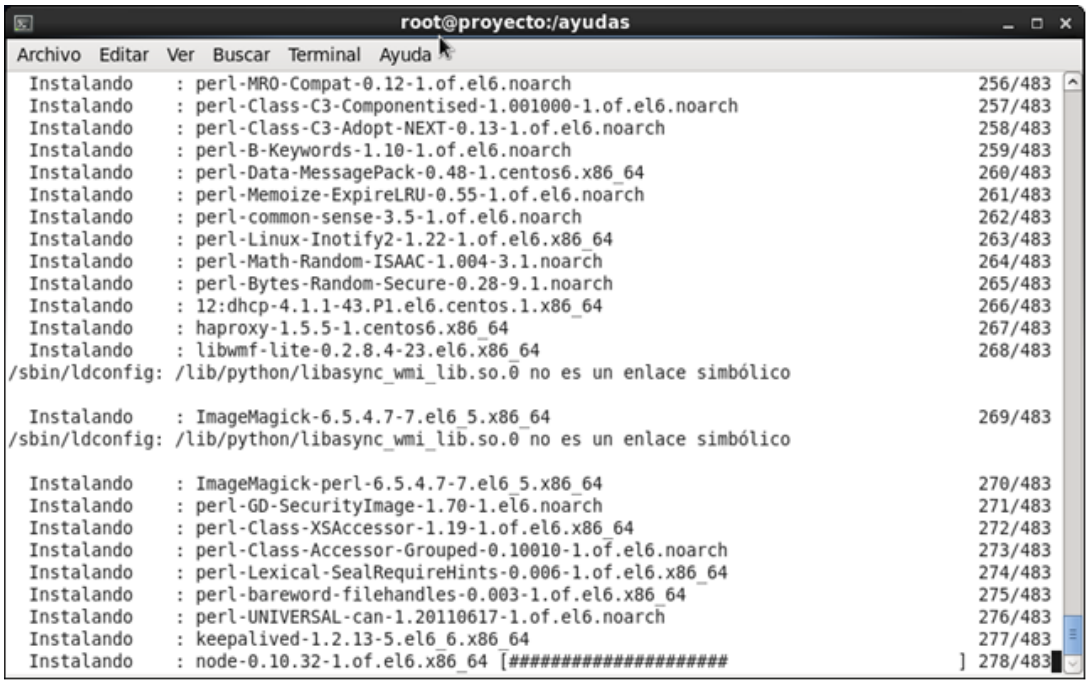


Ilustración 7 Instalación inicial PacketFence

Ilustración 8 Instalación finalizada

Puerto de configuración https://127.0.0.1:1443/

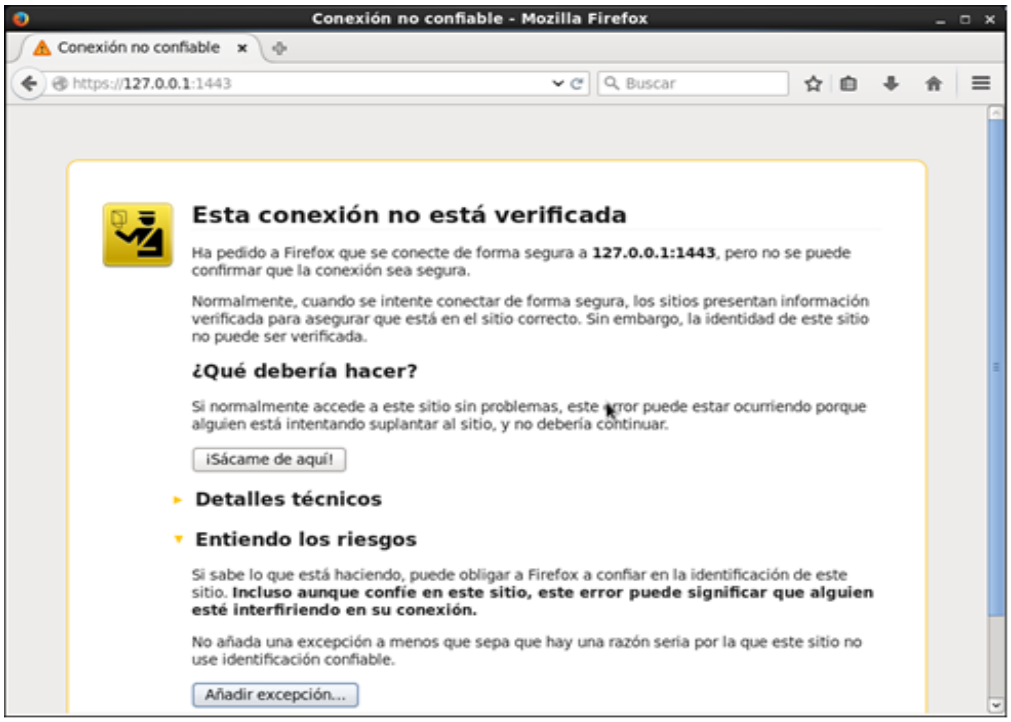


Ilustración 9 Conexión confiable

Ilustración 10 Excepción de Seguridad

Como se pudo observar con las pruebas de instalación la distribución de Linux que soporta la implementación de PacketFence es CentOS 6 que tiene los complementos a nivel de librerías válidos para su instalación y configuración.

Configuración Inicial PacketFence

Debemos hacer una configuración inicial que se realiza para que la herramienta PacketFence logre iniciar sus servicios dentro de la red. Estos servicios utilizados instalados por defecto desde el repositorio son: MySql, Apache, DHCP, FreeRadius.

PacketFence incorpora una aplicación basada en entorno web la cual permitirá paso a paso configurar NAC. El proceso de configuración se basa en diferentes pasos. [26]

- **Selección del método de funcionamiento**

En este paso se pide seleccionar un mecanismo de aplicación. Si se tienen dispositivos de red inmanejables se selecciona la opción de *Inline enforcement*, si son dispositivos de red manejables se escoge *VLAN enforcement*.

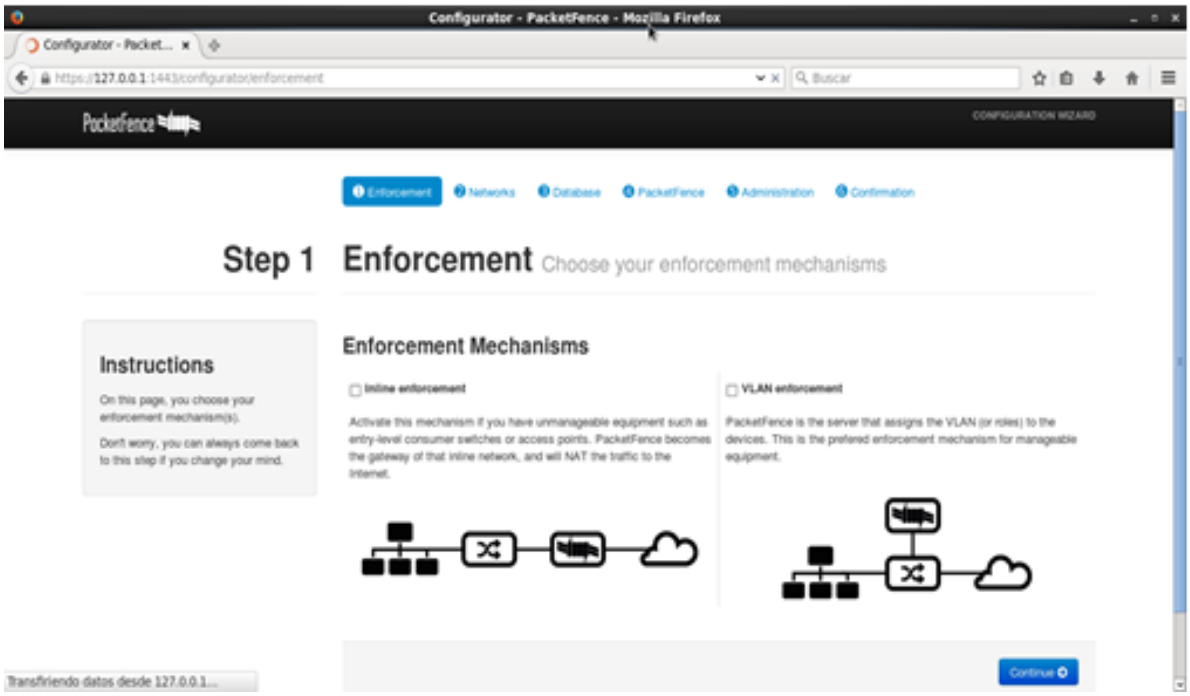


Ilustración 11 Selección del método de funcionamiento

Se requiere realizar la instalación del RADIUS y para que éste funcione correctamente una creación de base de datos por lo que instalamos MySql.

Instalación RADIUS

1. Se crea la base de datos radius

```
CREATE DATABASE radius;
```

2. Se asignan permisos al usuario radius, a la base de datos, a todas las tablas identificado con la clave “radpass”

```
GRANT ALL PRIVILEGES ON radius. * TO radius@localhost
IDENTIFIED BY “radpass”;
```

3. Se hace uso de la base de datos radius para luego proceder a deshacer el script que trae el esquema predefinido de la base de datos radius

```
use radius;
source/etc/raddb/sql/mysql/schema.sql
```

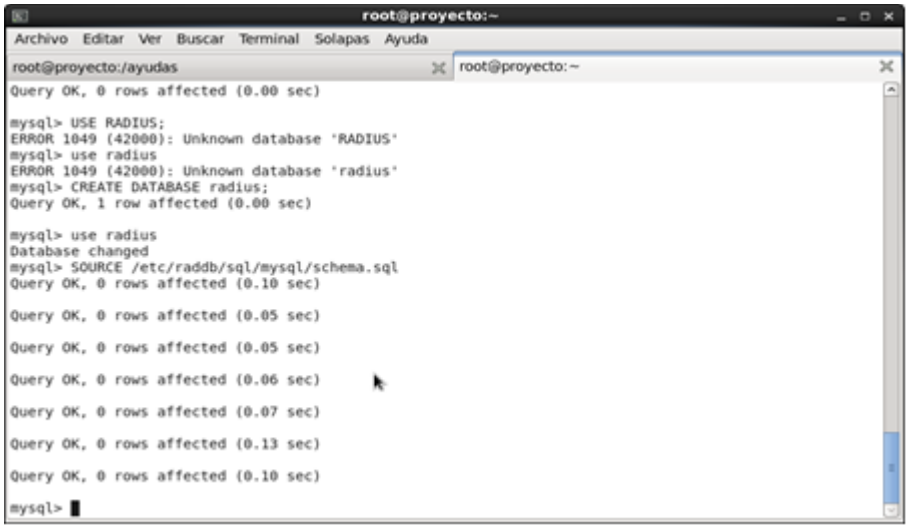


Ilustración 12 Base de datos de radius

4. Se revisa la configuración del archivo SQL de radius y que estén activas las siguientes líneas:

```
vi /etc/raddb/sql.conf
        # Connection info:
         server = "localhost"
        #port = 3306
        login = "radius"
        password = "radpass"
        # Database table configuration for everything except Oracle
        radius_db = "radius"
```

5. También se revisa la clave de radius para la autenticación de usuarios

```
vi /etc/raddb/clients.conf

secret = testing123
```

6. Se reinicia radius

```
service radius restart
```

Al reiniciar el servicio se genera el siguiente error

Error: Refusing to start with libssl version OpenSSL 1.0

El error se elimina cambiando el siguiente parámetro cambiándolo en

```
/etc/radb/radiusd.conf
allow_vulnerable_openssl = no a yes
```

7. Se realiza prueba de autenticación por radius, agregar un usuario para probar por base de datos mysql

```
mysql -u root -p

use radius;

INSERT INTO `radcheck` (`id`, `username`, `attribute`, `op`, `value`)
VALUES (1,'test','User-Password',':=','test');
```

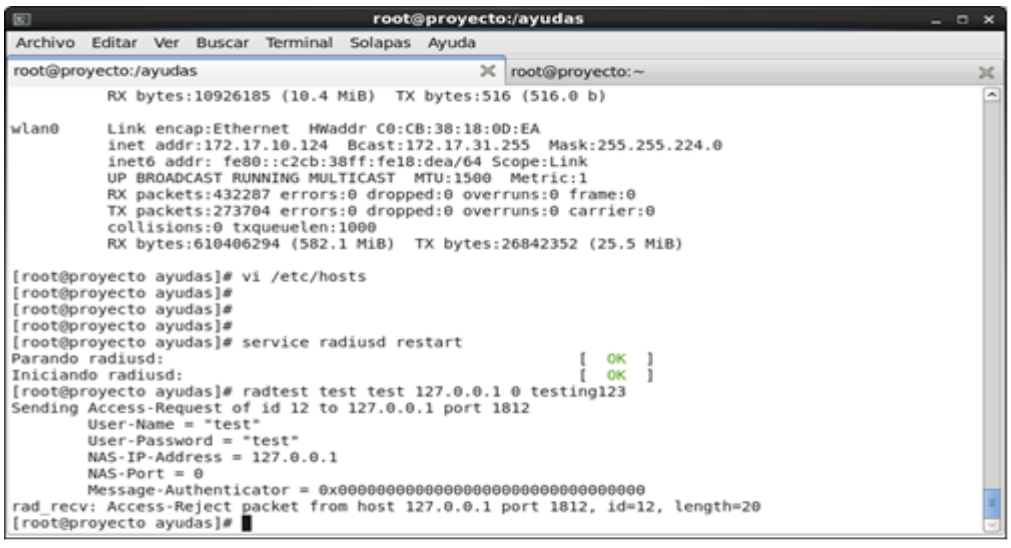


Ilustración 13 Insertar usuario

Revisar los errores en radius para autenticar

```
[root@proyecto ayudas]# radtest test localhost 0 testing123
radclient:: Failed to find IP address for proyecto
radclient: Nothing to send.
```

7.1 Revisar errores para la configuración de radius

```
radiusd -X
radiusd: #### Opening IP addresses and Ports ####
listen {
        type = "auth"
        ipaddr = *
        port = 0
Failed binding to authentication address * port 1812: Address already in use
/etc/raddb/radiusd.conf[273]: Error binding to port for 0.0.0.0 port 1812
```

Para arreglar el problema se colocan en el conf en la línea de ip 127.0.0.1 para remplazar el *

En el archivo /etc/hosts

Se adiciona a 127.0.0.1 el nombre proyecto

```
[root@proyecto ayudas]# radtest test test 127.0.0.1 0 testing123
Sending Access-Request of id 12 to 127.0.0.1 port 1812
        User-Name = "test"
        User-Password = "test"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 0
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=12, length=20
```

```
radtest dd9999 Abcd1234 localhost:18120 12 testing123
Sending Access-Request of id 54 to 127.0.0.1 port 18120
        User-Name = "dd9999"
        User-Password = "Abcd1234"
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 12
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 18120, id=54, length=2
```

Continuación Configuración PacketFence

- **Configuración de red**
  Se configuran las interfaces de red el servidor de PacketFence, a continuación el paso a paso donde tenemos una interfaz inalámbrica y la física.

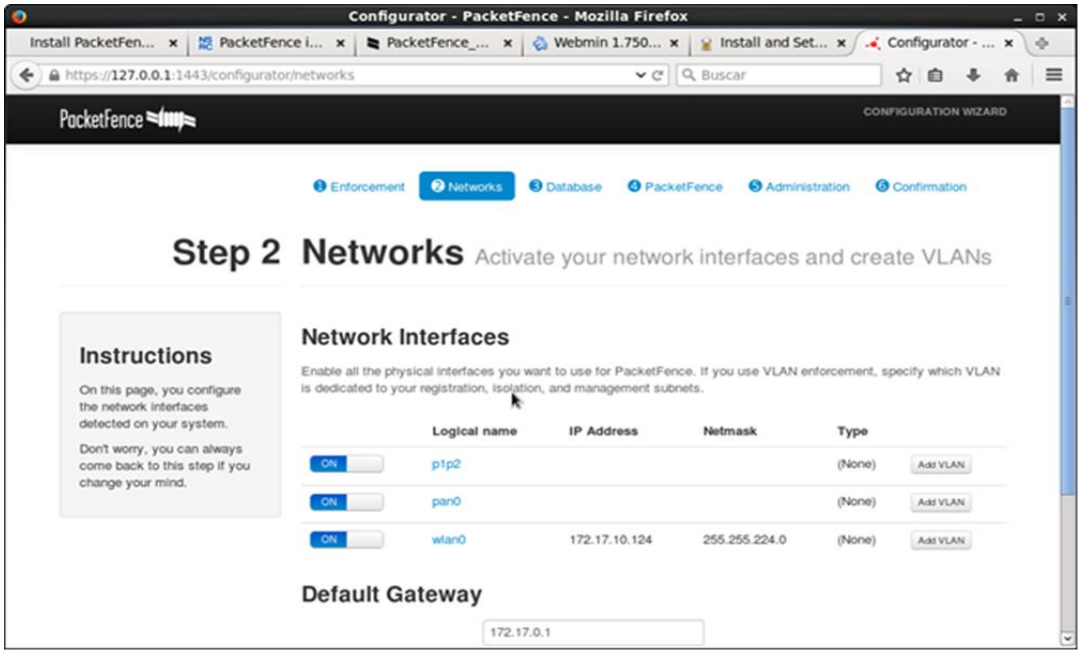


Ilustración 14 Configuración de Red, paso 1

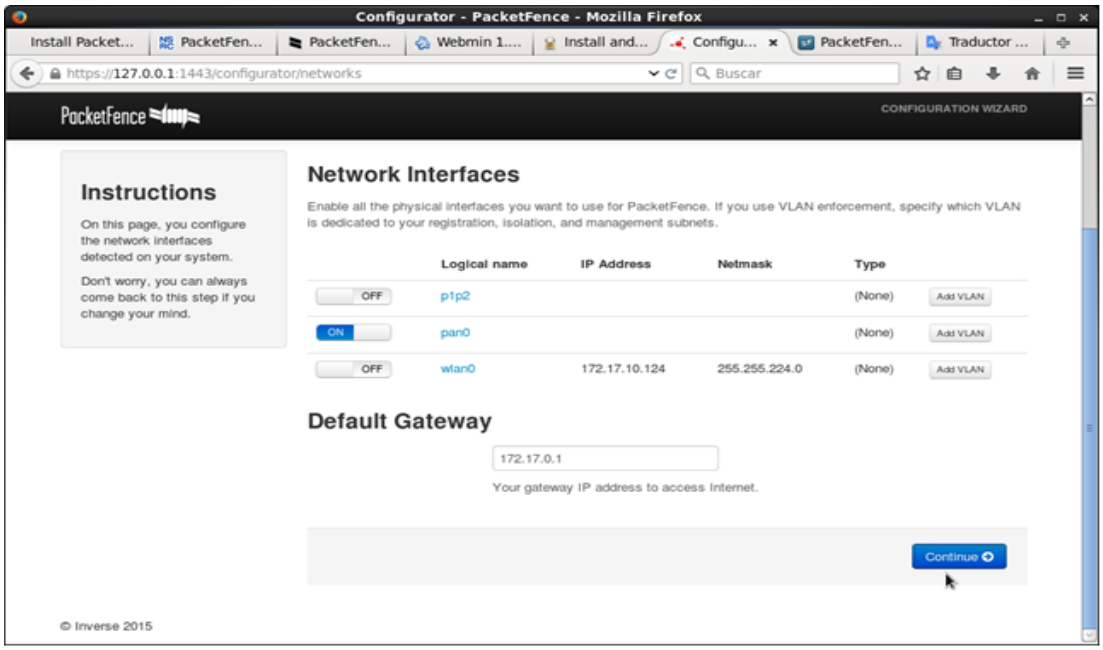


Ilustración 15 Configuración de Red, paso 2

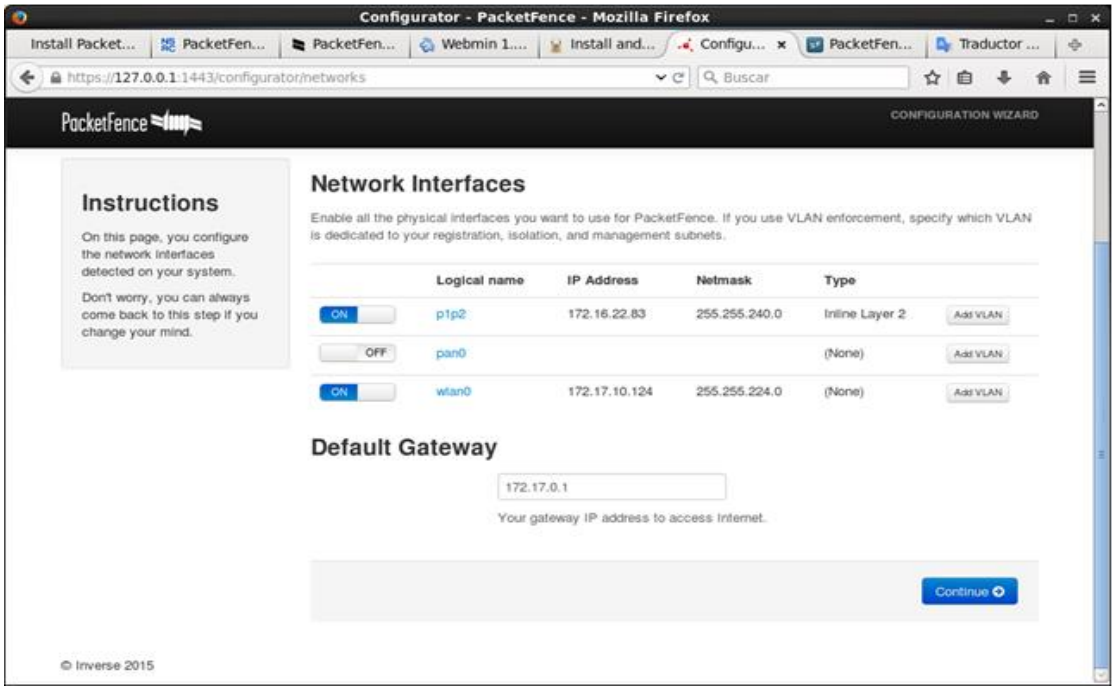


Ilustración 16 Configuración de Red, paso 3

Pide escoger una interfaz tipo “Management” para la administración y otra para prestar los servicios que llamamos Layer 2

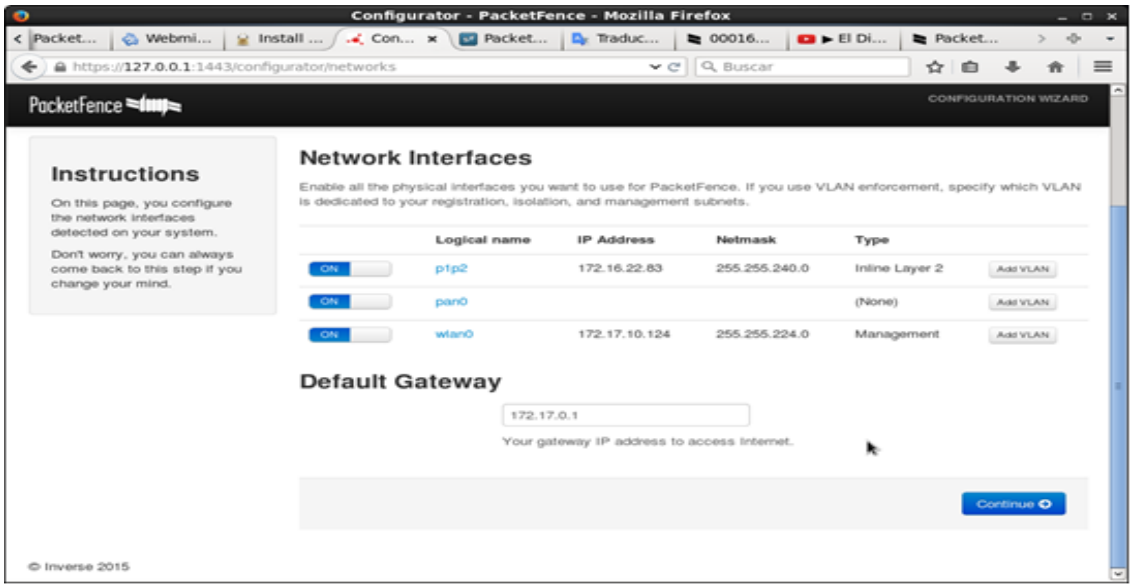


Ilustración 17 Configuración de Red, paso 4

Cuando se configure la interfaz pide el DNS y una ip adicional para generar interfaz virtual, también si se quiere habilitar el DHCP y si se quiere hacer NAT a todo lo que llegue para dar internet automáticamente.

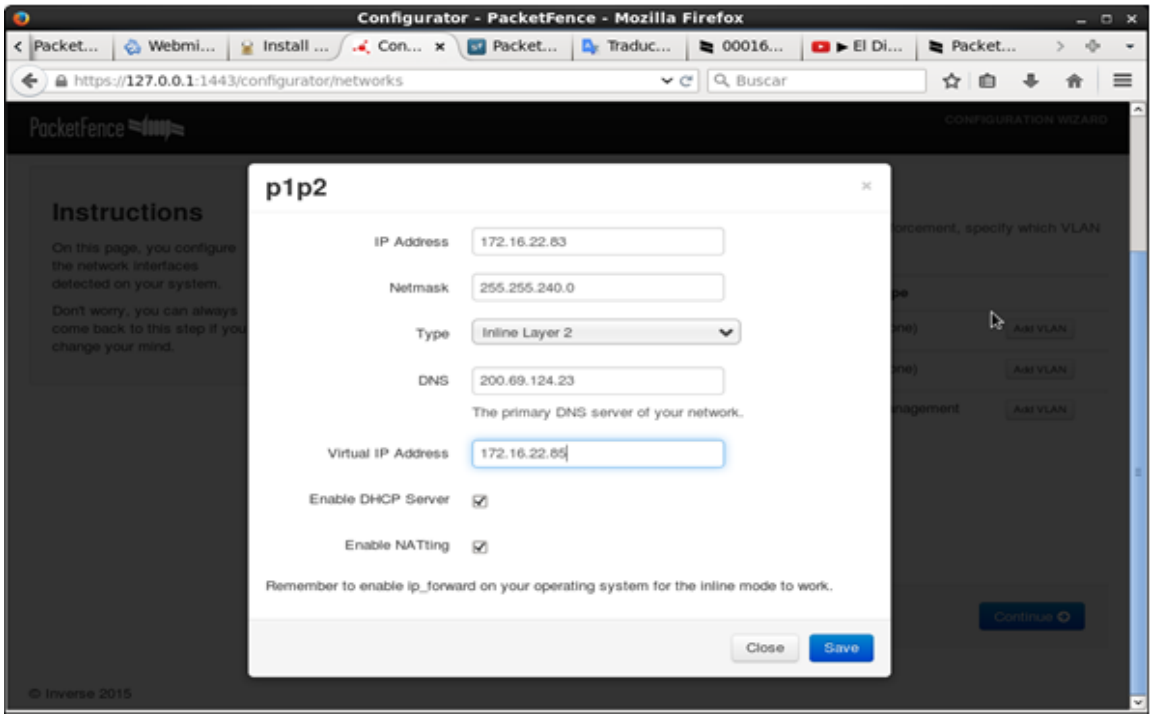


Ilustración 18 Configuración de Red, paso 5

- **Base de Datos**
  Luego se procede introduciendo una contraseña de usuario de MySQL para crear una nueva base de datos y usuario para PacketFence, donde la herramienta crea la estructura correcta de tablas.

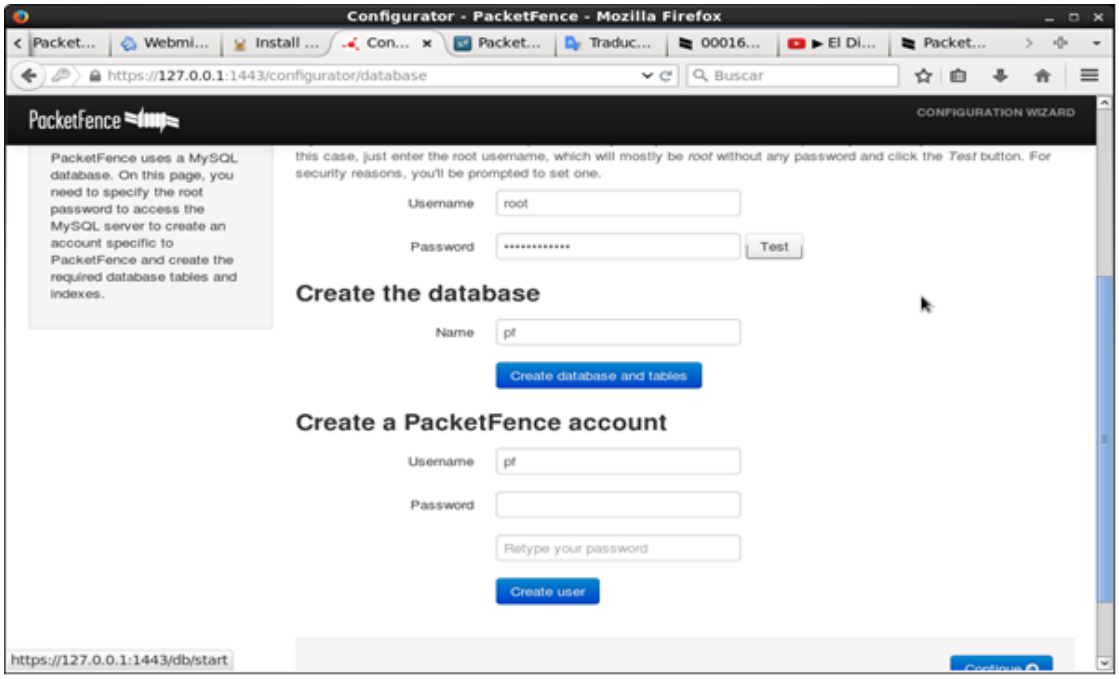


Ilustración 19 Creación base de datos

Luego de creada la base de datos pide crear un usuario para añadirlo a la misma.

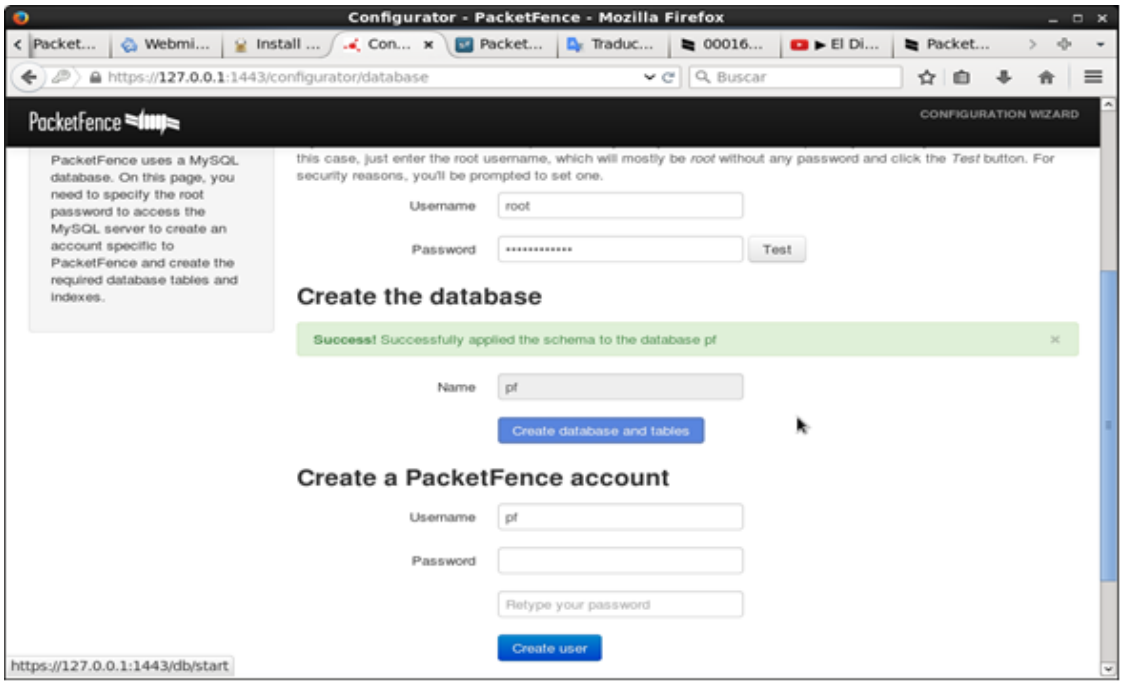


Ilustración 20 Creación base de datos exitosa

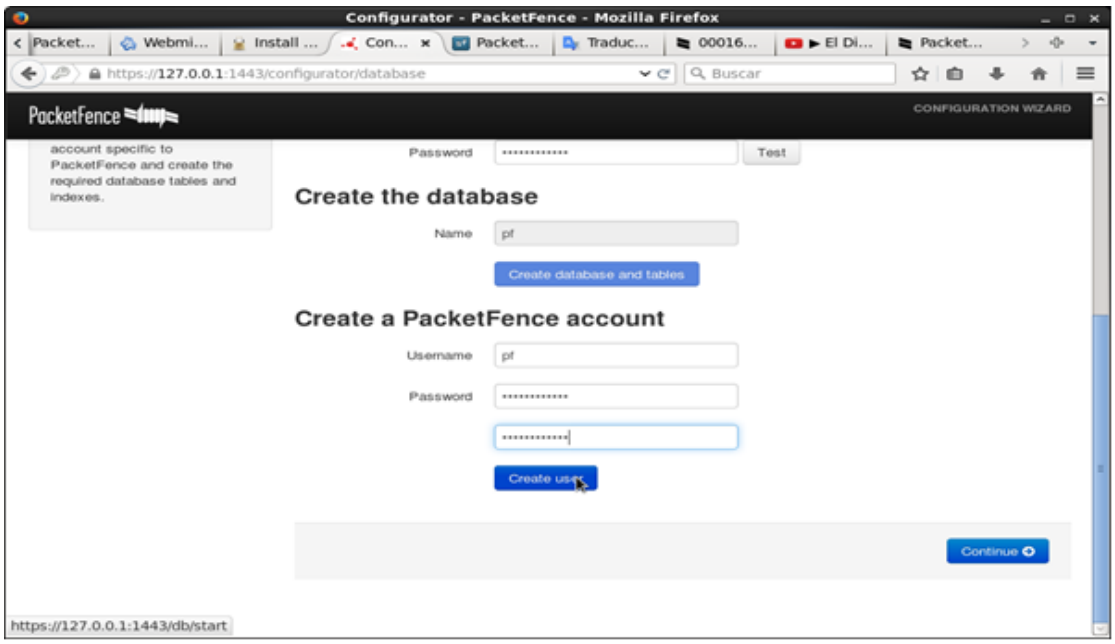


Ilustración 21 Creación de usuario a la base de datos

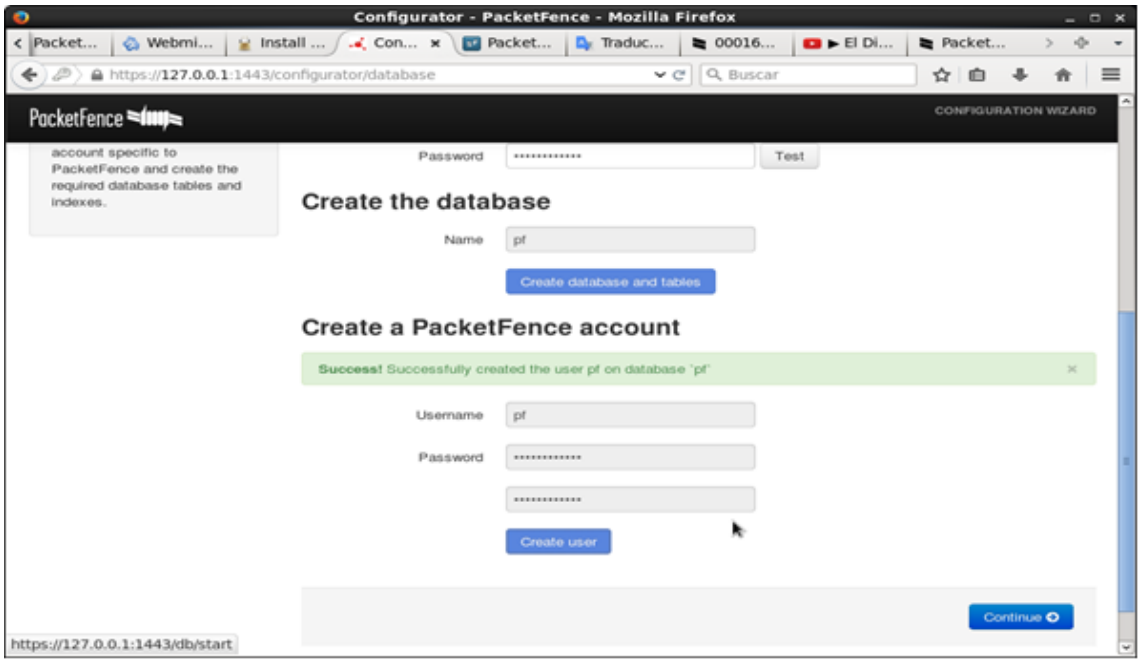


Ilustración 22 Creación usuario exitosa

- **Configuración General**

  En esta parte, se realiza una configuración básica necesitamos introducir un dominio, el nombre del host, dirección IP del servidor DHCP.

Ilustración 23 Configuración general PacketFence

- **Administración**

  Este paso es para establecer el administrador PacketFence donde se introduce una contraseña. Por último se da clic en Start PacketFence para iniciar todos los servicios.

  User= admin
  Pass= proyecto2015

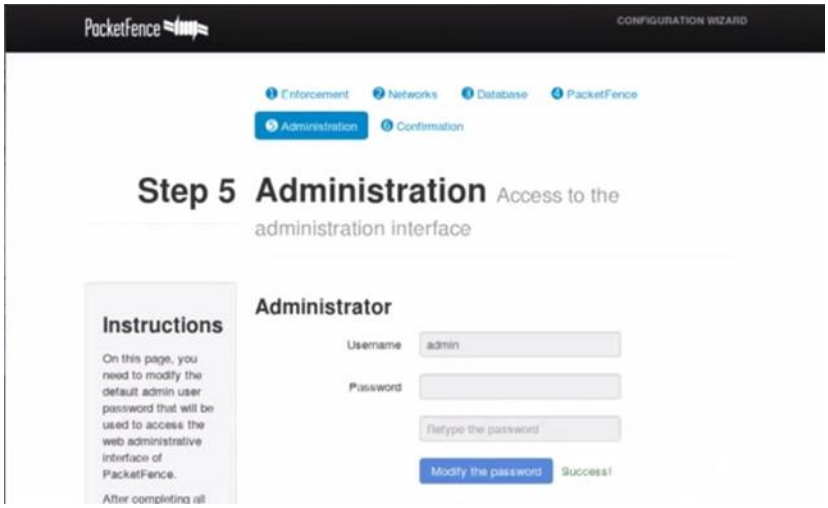


Ilustración 24 Administración

- **Inicio de servicios**

  Y finalmente se inician todos los servicios que se observan, estos servicios aseguran la configuración básica de PacketFence

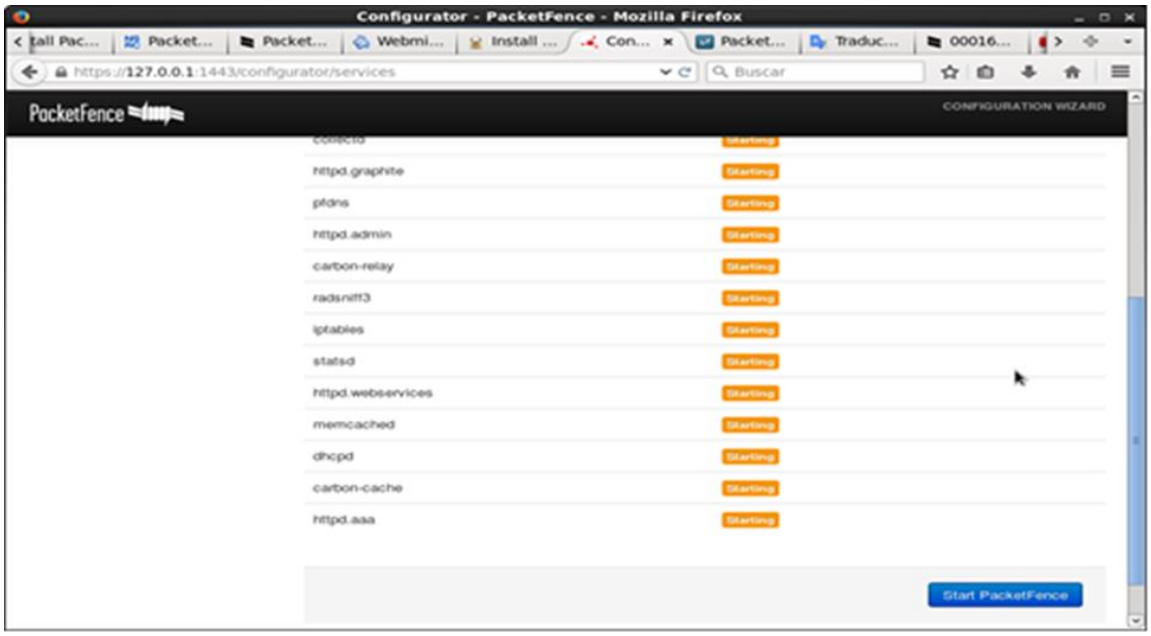


Ilustración 25 Ventana inicio de Servicios

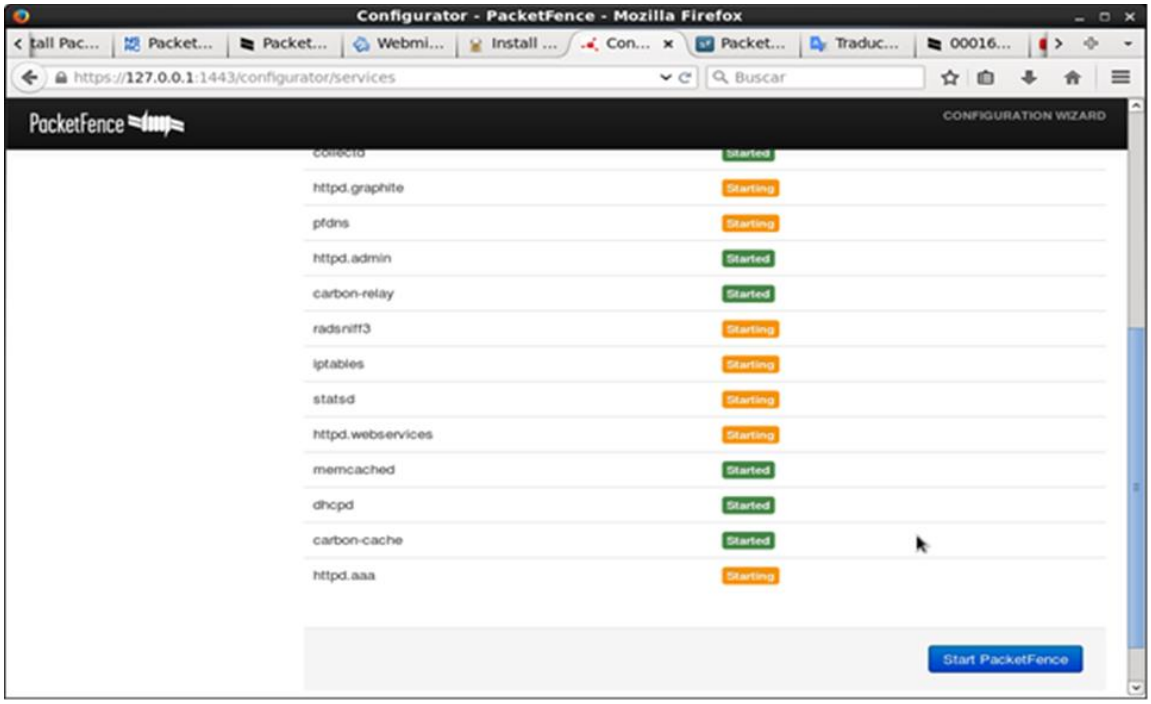


Ilustración 26 Servicios iniciando

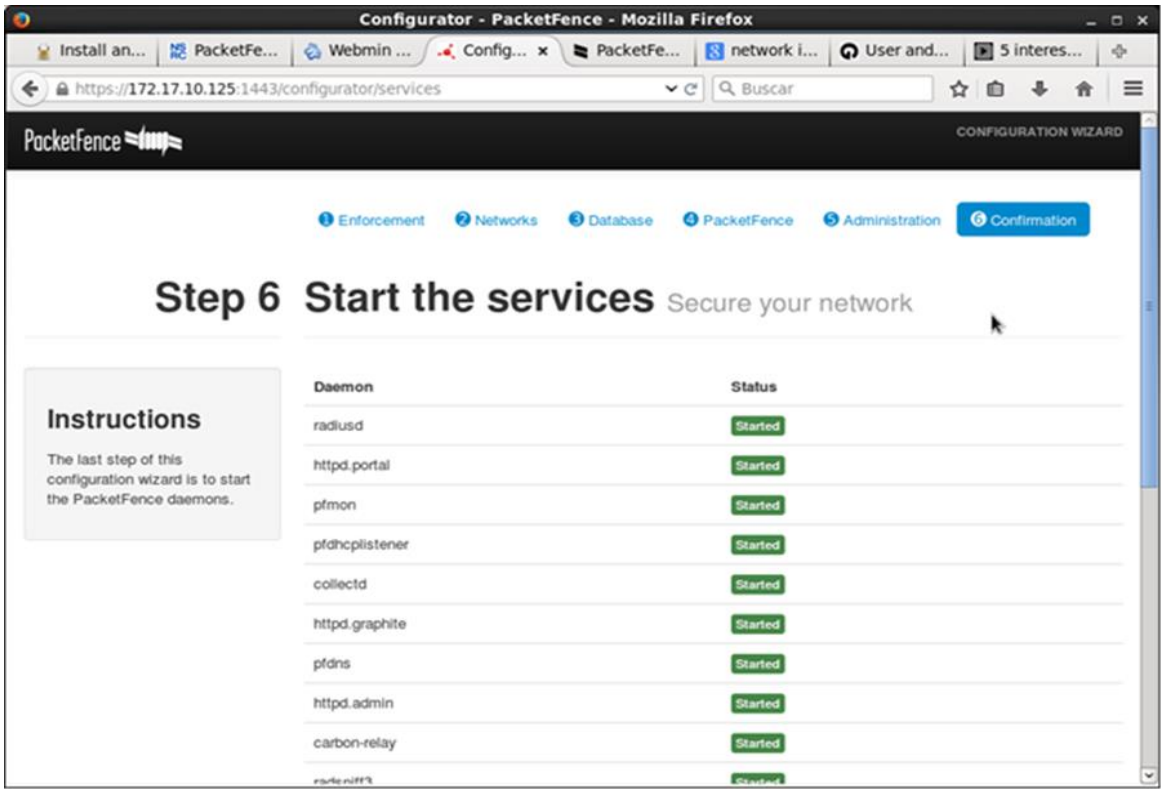


Ilustración 27 Servicios iniciados exitosamente

CONFIGURACION EN SERVIDOR DHCP
Ámbito configurado.

NETWORK 172.16.16.0
RANGO 172.16.16.20 172.16.16.240

Mysql
Usuario= root
Password= proyecto2015

Sistema operativo CentOS
Usuario=root
Password= proyecto2015

Usuario=proyecto
Password=proyecto2015

conf1.png
conf2.png

```
root@proyecto sites-enabled]# /usr/local/pf/bin/pfcmd service radiusd start
service|command
memcached|already started
httpd.admin|already started
Checking configuration sanity...
WARNING - inline mode needs ip_forward enabled to work properly. Refer to the administration guide to enable ip_forward.
radiusd|start
```

4.3 PARAMETRIZACIÓN DEL APLICATIVO SELECCIONADO

La herramienta PacketFence ofrece una interfaz web para su administración en un ambiente de pruebas utilizamos la dirección web del servidor https://172.17.10.125:1443/ que nos muestra la siguiente imagen para entrar el nombre del administrador y su contraseña.

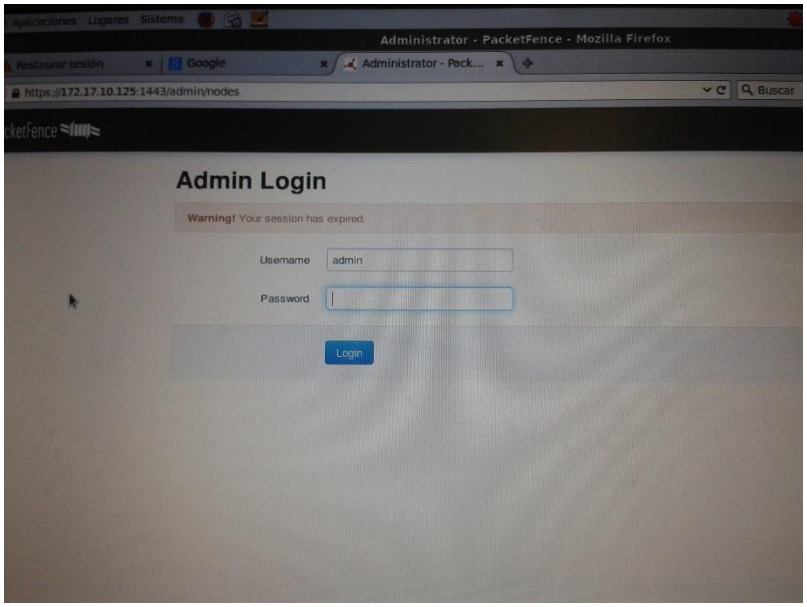


Ilustración 28 admin/login

4.3.1 Definición del plan de pruebas

Este apartado contiene las pruebas implementadas sobre el prototipo de laboratorio y sobre las cuales se validará el cumplimiento de las políticas tipo BYOD.

Para la implementación se necesita un escenario de red con los equipos descritos anteriormente, para simular los principales servicios.

Red Física e inalámbrica de pruebas para implementación

El laboratorio montado cuenta con el portátil donde fue instalado el sistema operativo CentOS y la herramienta PacketFence, un equipo de pruebas de la red cableada, el switch y router inalámbrico. Los equipos de red se interconectan entre sí mediante cableado estructurado de categoría 6 de acuerdo a las velocidades de transmisión soportadas por los puertos.

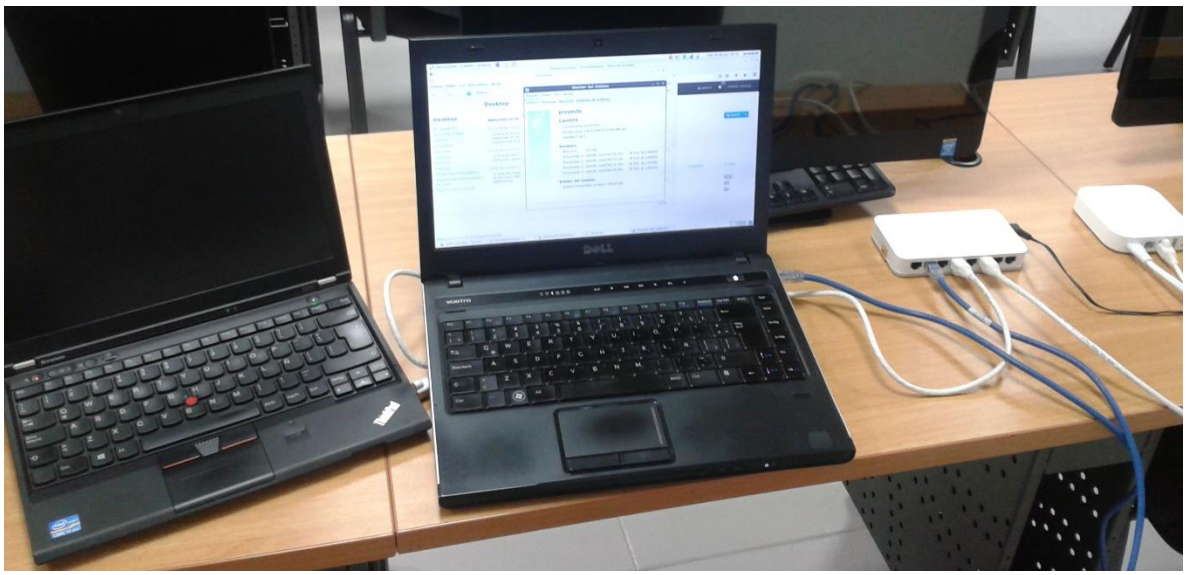


Ilustración 29 Equipos de red del laboratorio

PRUEBAS RED CABLEADA

- **Creando un nuevo usuario**

  En la siguiente imagen podemos ver en la pestaña “Users”/ “Create” la creación de un nuevo usuario local con algunas propiedades según lo requiera, por motivos de seguridad con el usuario y contraseña.

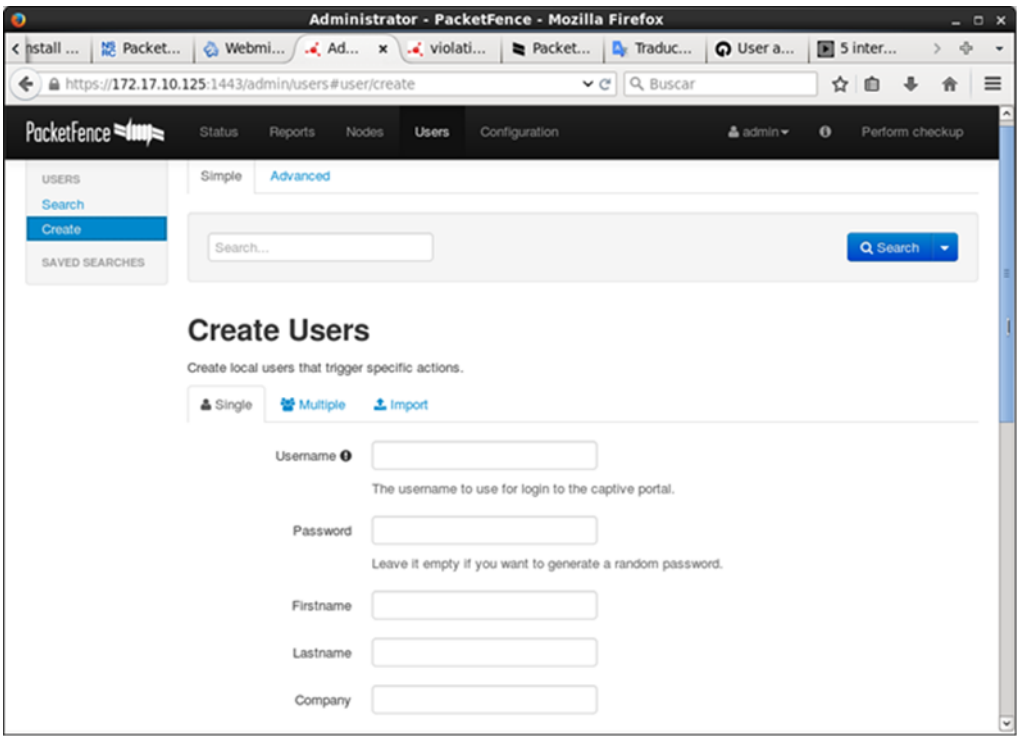


Ilustración 30 Creación usuario PacketFence

Luego de llenar los datos requeridos el usuario es creado exitosamente.

- **Búsqueda de Nodos**

  En esta imagen visualizamos los nodos que va tomando pero no están registrados.

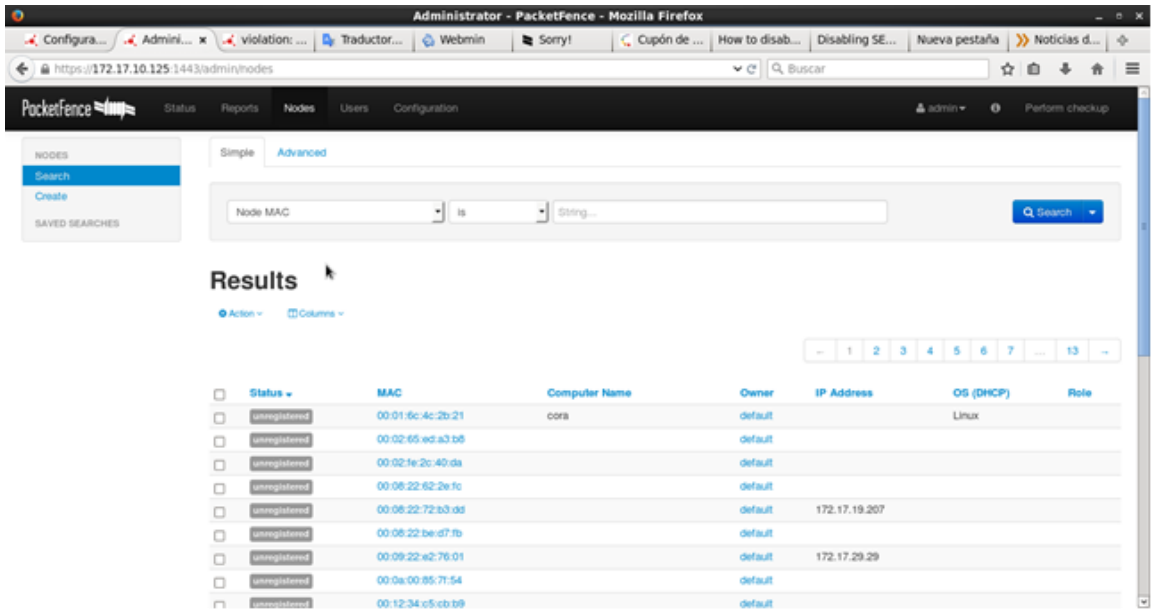


Ilustración 31 Nodos encontrados

Cada nodo puede ser configurado para su registro, igualmente aparecen las direcciones MAC de los equipos de los usuarios que se hayan creado pero que no aparecen registrados.

En la ilustración anterior se puede ver enlistados de forma exitosa todos los nodos encontrados con su respectiva dirección MAC, donde se pueden configurar.

Para realizar un registro completo se configura la fecha de registro y hasta cuando se dan los servicios, donde el resultado de esta prueba es exitosa para llevar al siguiente paso.

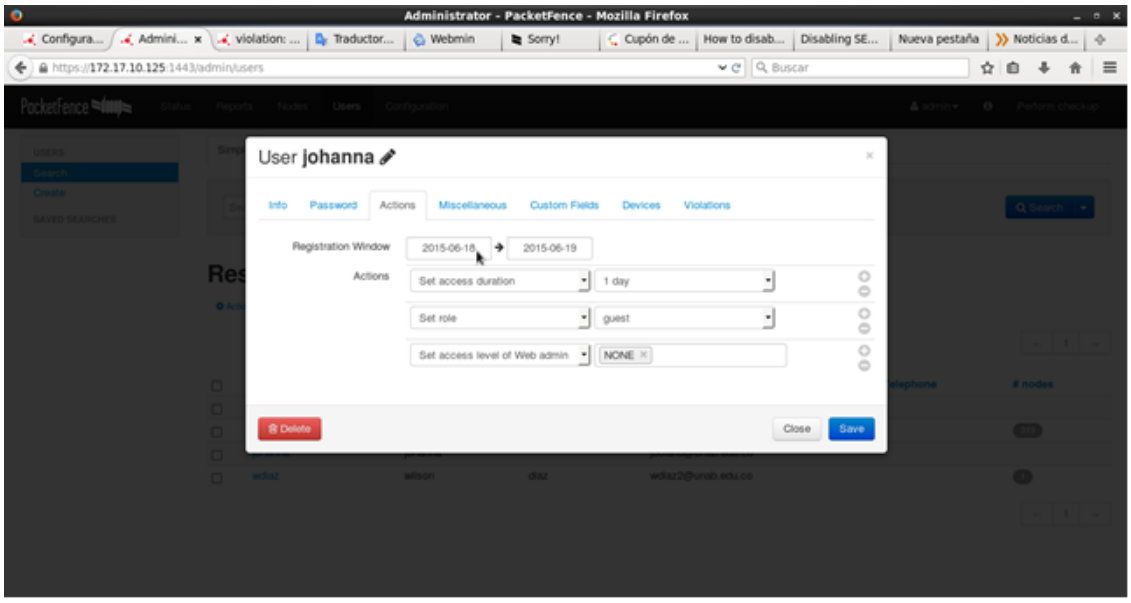


Ilustración 32 Configuración Nodo

Luego se ve como es detectado por el sistema y pasa de "*Unregistered*" a "*Registered*" informa el estado del dispositivo, la dirección MAC, el nombre, tipo de usuario, dirección IP y tipo de sistema operativo.

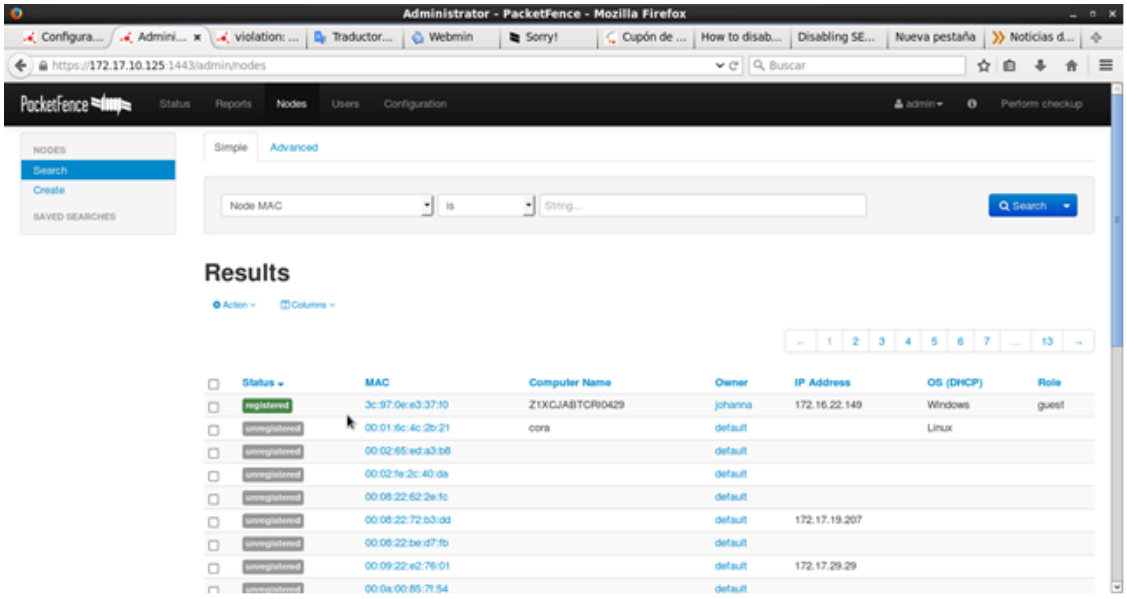


Ilustración 33 Nodo registrado

- **Información del Nodo**

Se procede a ver la información del nodo, opción del cambio de estado, roles de la red, violaciones de políticas que se registran y otras características que pueden ser manipulables por el administrador.

Aquí se visualiza las características del nodo registrado

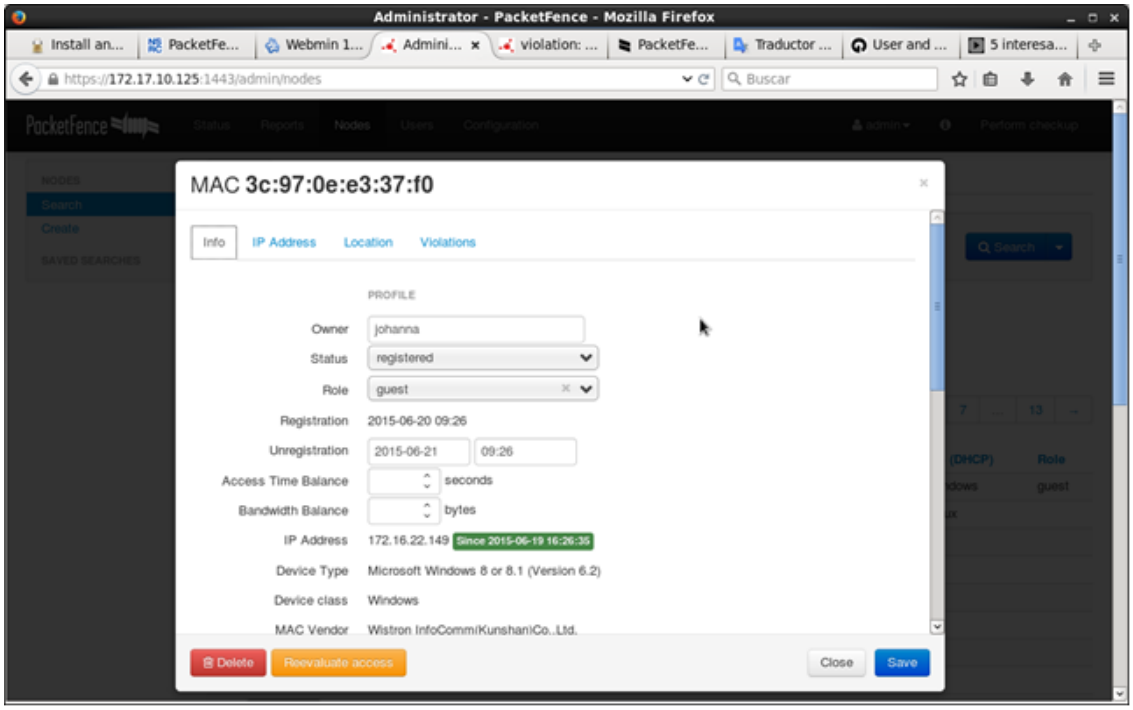


Ilustración 34 Pestaña Información General del Nodo

Pestaña IP Address, donde se ve la IP que ha tomado, el tiempo de inicio y final de acuerdo a los permisos dados y resulta correcto.

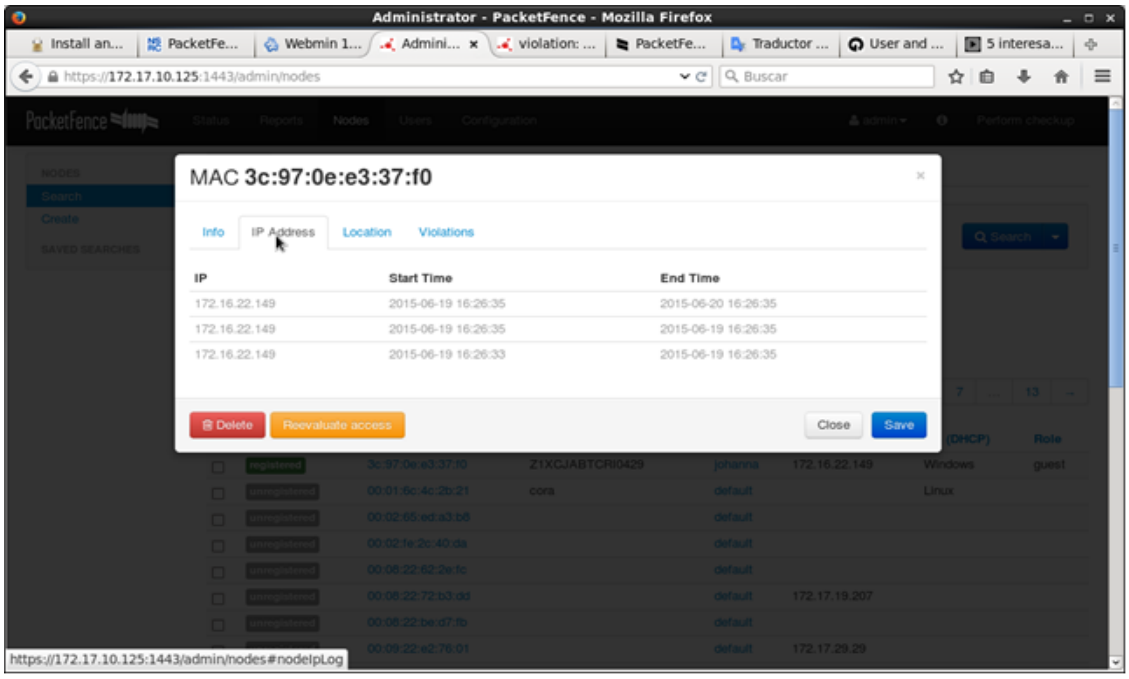


Ilustración 35 Pestaña IP Address

Pestaña “Location” se observa el tipo de conexión que utiliza PacketFence.

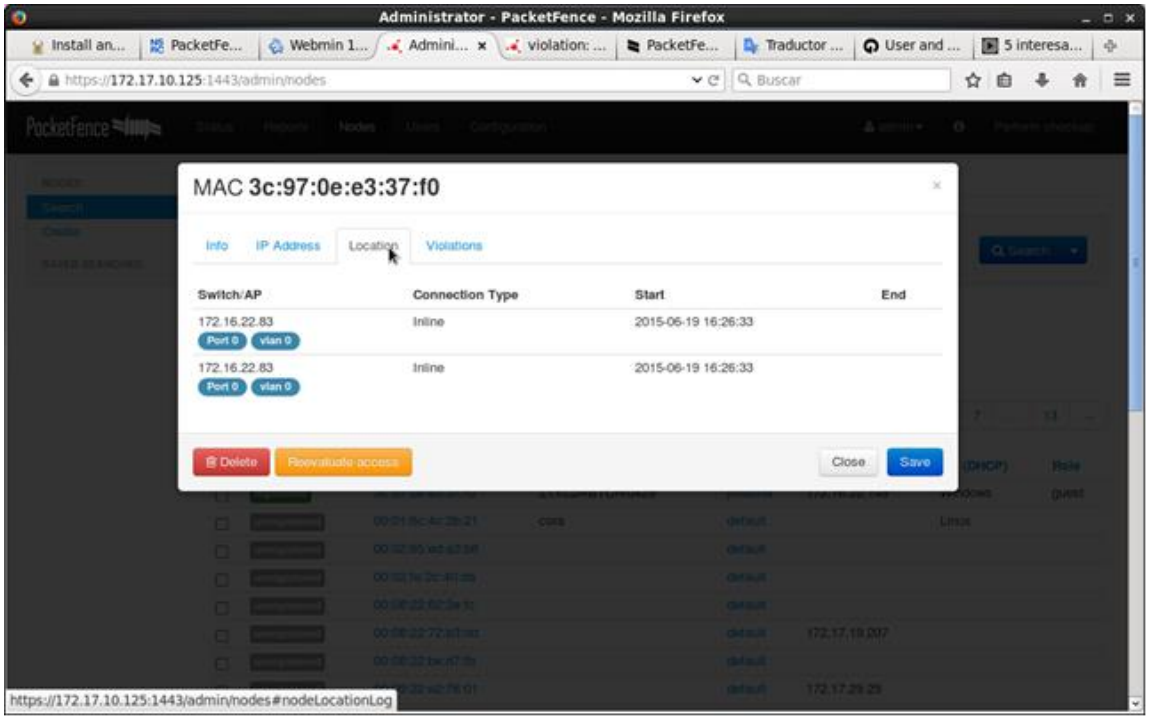


Ilustración 36 Pestaña Location

Pestaña “Violations” Donde se ve los escaneos que la herramienta ha realizado de forma correcta.

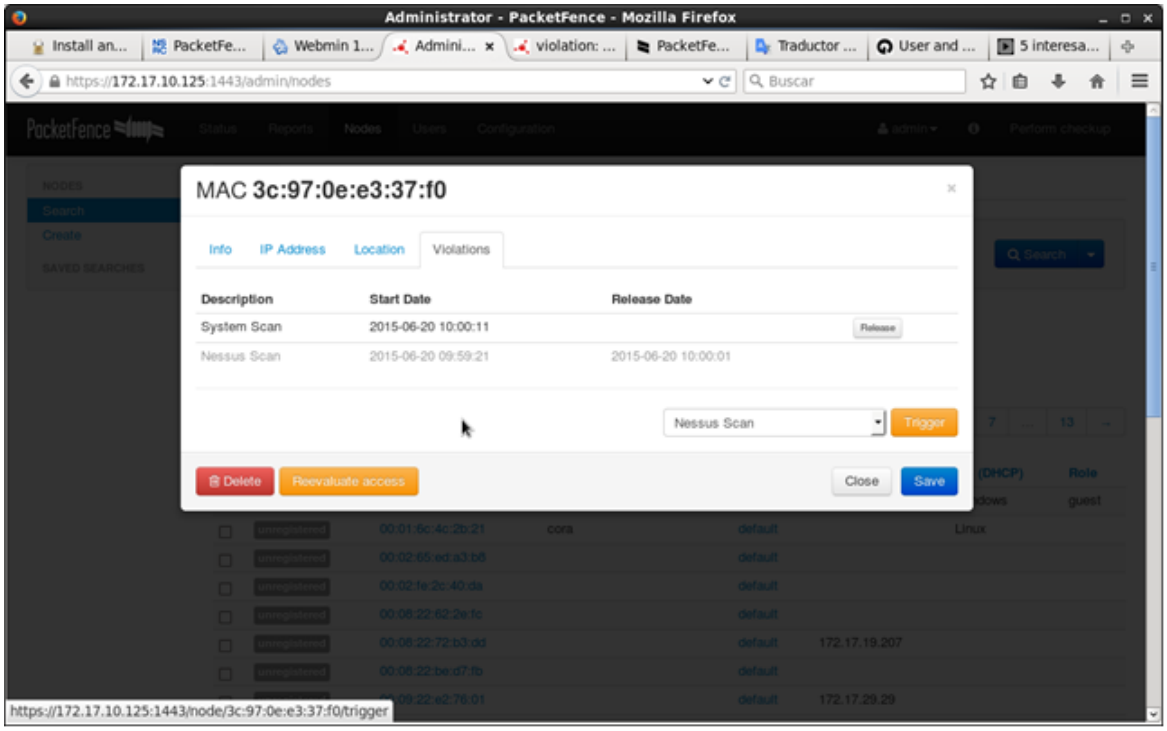


Ilustración 37 Pestaña Violations

- **Prueba de navegación**

Se realizó una prueba para la navegación en equipos distintos y se observa que el equipo deniega la conexión y se visualiza el nombre del equipo para el proyecto “packet.proyecto.edu”.

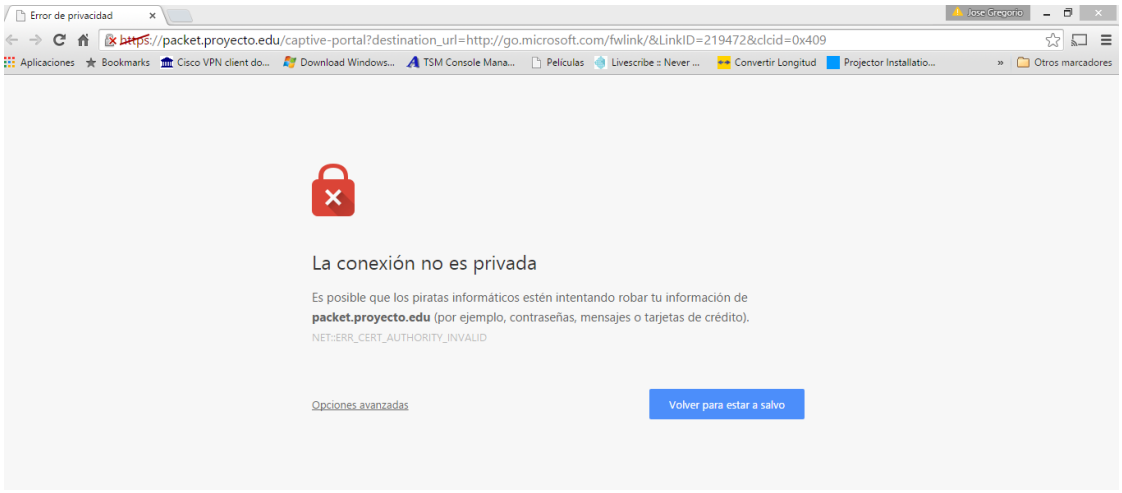


Ilustración 38 Error de privacidad

En la siguiente prueba se comprueba que PacketFence interrumpe la navegación del portal cautivo a través de un interfaz web; para que el usuario se registre para poder acceder, en tal caso de una violación informa el problema y que hacer para poder remediarlo.

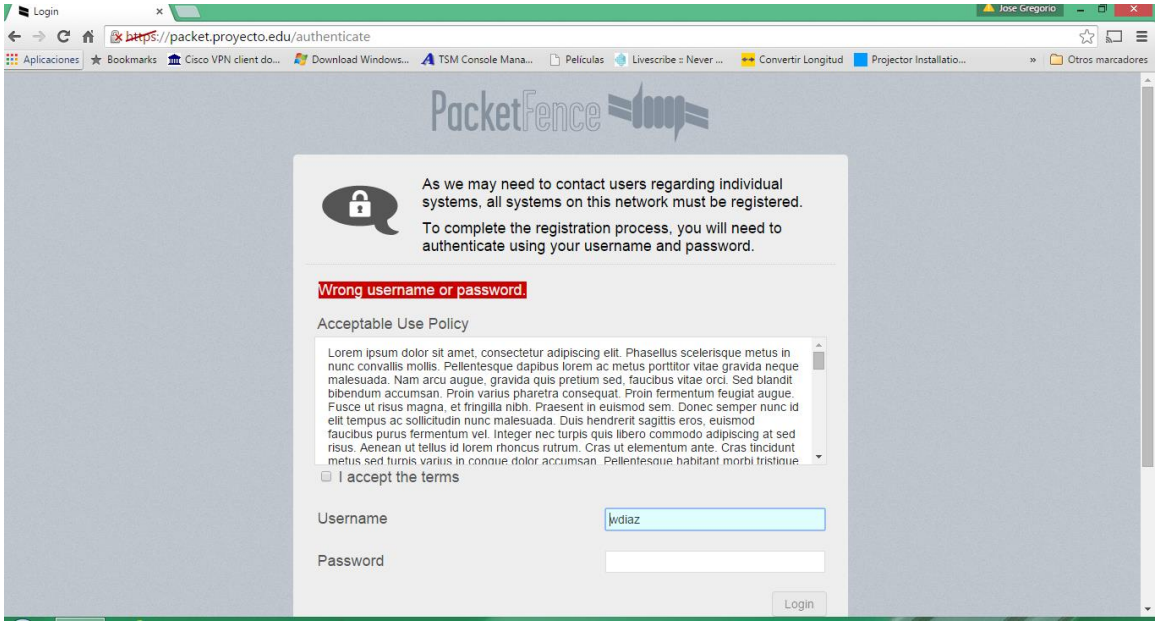


Ilustración 39 Login

Después se ingresan los datos de usuario, contraseña y aceptar términos.

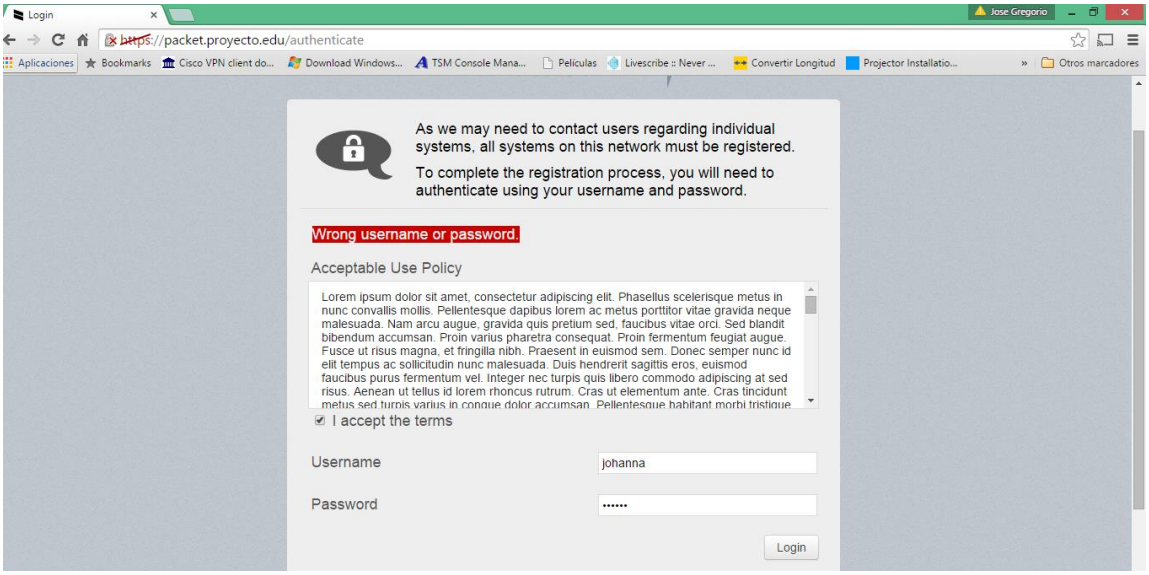


Ilustración 40 Ingreso de datos

Luego de llenado los datos, se da clic al botón “login” y se ve la siguiente pantalla. Aparece el mensaje que dice que se está actualmente habilitando el acceso a la red. Una vez establecida la conexión a la red se le redirigirá automáticamente.

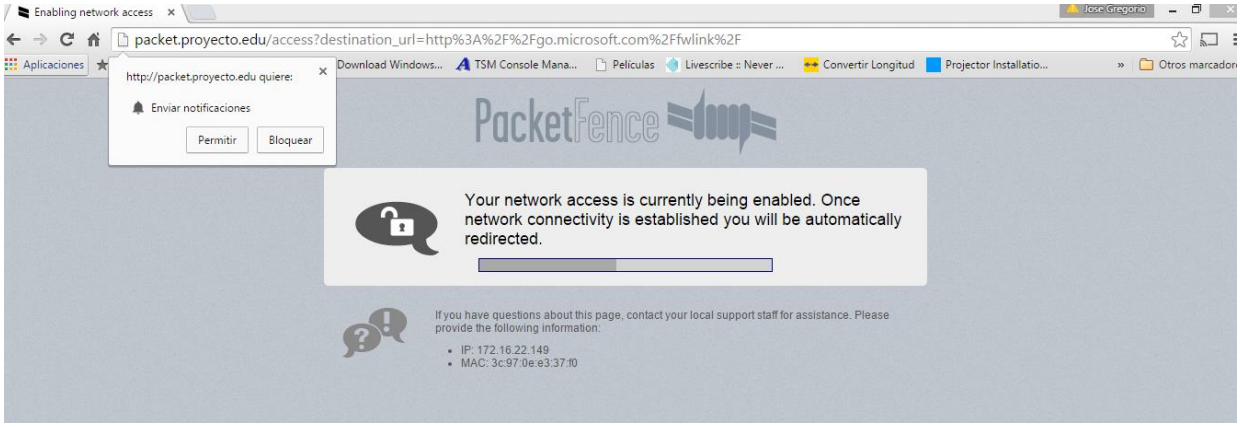


Ilustración 41 Permitir acceso

Pero cuando se termina el proceso no accede de forma correcta, ya que se presenta un problema de “DNS” y todavía no deja navegar.

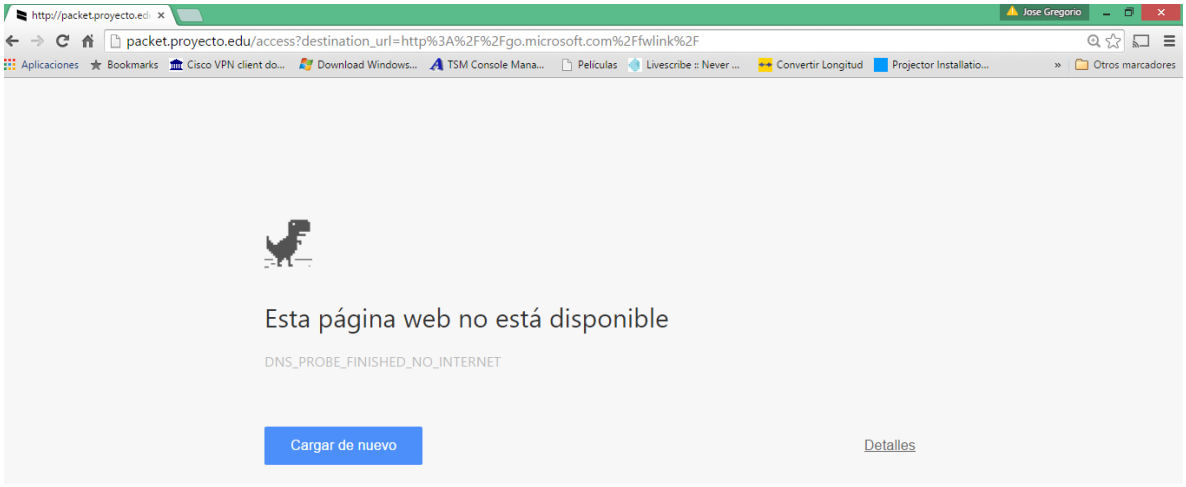


Ilustración 42 Error conexión

PRUEBA RED INALAMBRICA

PacketFence no requiere de parámetros adicionales de personalización, por lo tanto se enfoca en el ejemplo de funcionamiento del servidor con el registro de equipos inalámbricos.

Equipo utilizado para la prueba un Smartphone Samsung S3 mini. El nombre de la red es Unab_Eventos hacemos conexión con la clave “Wifi2015”. En la siguiente imagen el celular obteniendo la dirección IP.

Ilustración 43 Conexión Inalámbrica

Si el ingreso de la contraseña es exitoso se conecta a la red y se visualiza como se asigna la dirección IP 172.16.23.137 obtenida dentro del rango.

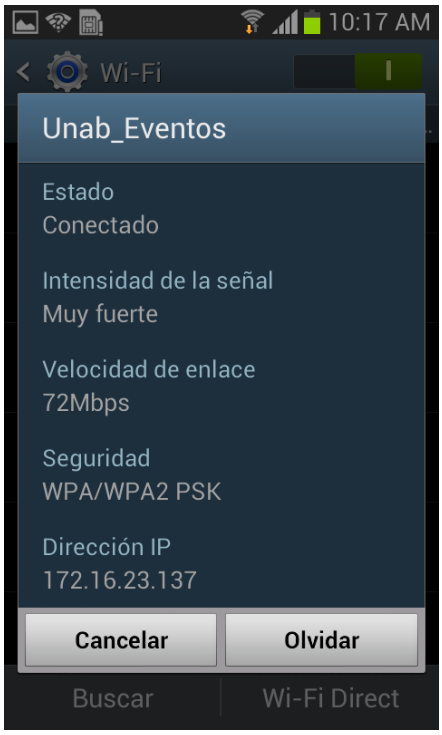


Ilustración 44 Obtención dirección IP

- **Prueba de navegación**

Se abre un navegador en el equipo y muestra que no es permitida la conexión ya que el usuario no se ha registrado

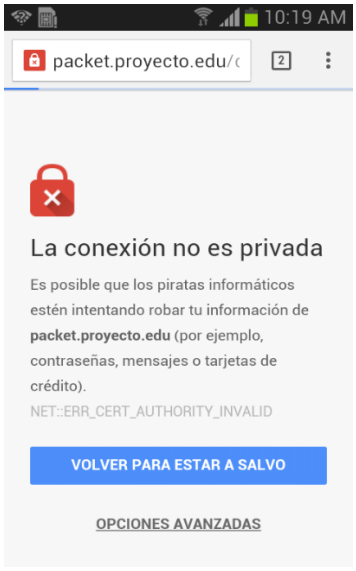


Ilustración 45 Conexión no privada

Se da clic a *"acceder a packet.proyecto.edu"*

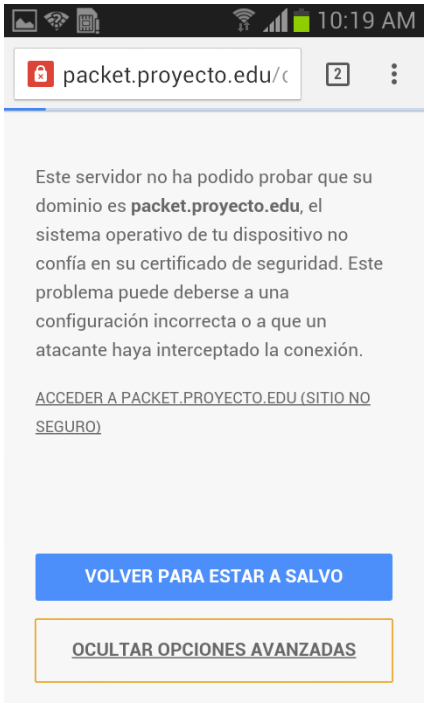


Ilustración 46 Acceso al usuario

Pasa a la página para hacer acceso del usuario

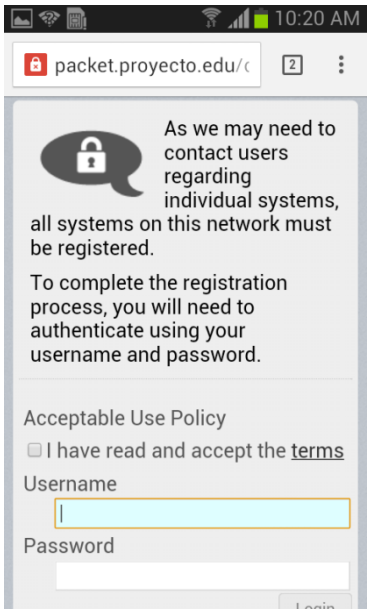


Ilustración 47 Insertar datos

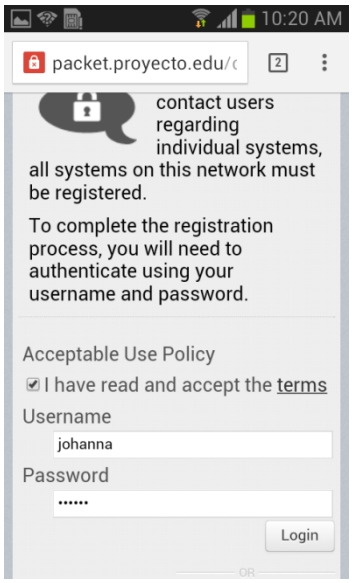


Ilustración 48 Insertar datos (2)

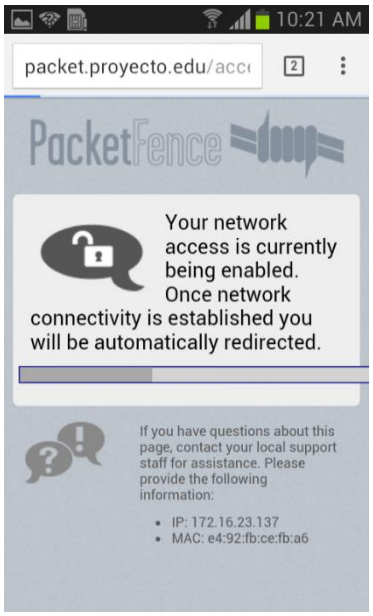


Ilustración 49 Página de cargando

La administración de equipos se realiza por medio del portal web del servidor, al ingresar a la pestaña *"Nodes"* donde se lleva el control de los usuarios se identifica la dirección MAC del equipo (e4:92:fb:ce:fb:a6).

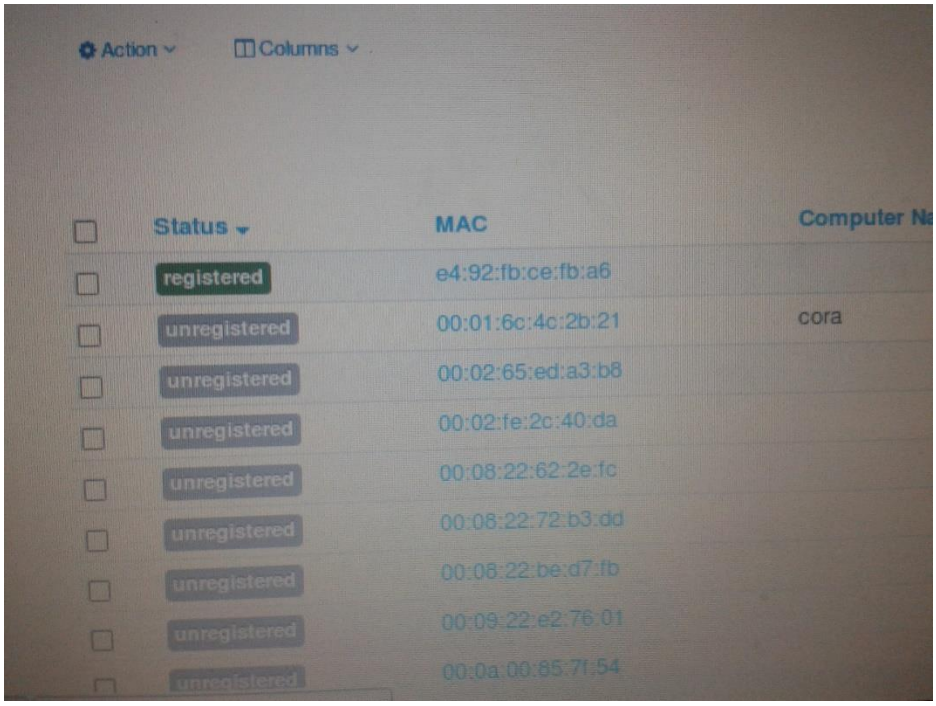


Ilustración 50 Estado Nodo inalámbrico

En el siguiente paso, muestra un aviso de que no deja acceder a la navegación y luego al reiniciar el equipo permite la navegación normal.

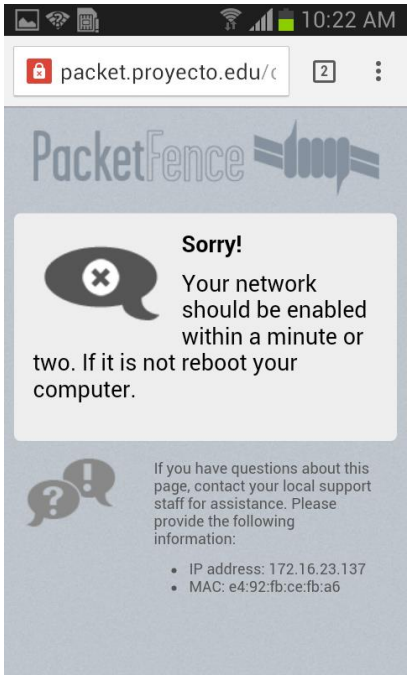


Ilustración 51 Aviso

Resultados de Pruebas

La herramienta ayuda con las diferentes características de NAC como son:

- Acceso a nuevos equipos, con mayor control de políticas.
- Mejora el rendimiento de productividad y acceso a servidores.
- Más eficiencia de los recursos de la red.
- Identificación y autenticación de acceso a la red.
- Aislamiento e identificación de usuarios no permitidos

Las pruebas realizadas en el ambiente de red del laboratorio diseñado, a pesar de contar con los elementos básicos, permitieron realizar la validación de las políticas definidas sobre las cuales a continuación se revelan los hallazgos encontrados.

4.4 VALIDACIÓN DEL CUMPLIMIENTO DE POLÍTICAS NAC Y BYOD IMPLEMENTADAS

Posterior a las pruebas con la herramienta PacketFence se validará el cumplimiento de las políticas tipo BYOD.

4.4.1 Análisis y matriz de cumplimiento

Requerimientos	Si	No
- Política control de acceso	✓	
Gestión de acceso al usuario		
- Registro de cliente	✓	
- Gestión de Privilegios	✓	
- Claves de los usuarios	✓	
- Examinación de derechos para acceder a la red	✓	
Responsabilidades del usuario		
- Empleo de claves	✓	
- Política de escritorio y pantalla limpia		**X**
- Equipo cliente desatendido	✓	
Control de acceso a la red		
- Política sobre el uso de los servicios	✓	
- Identificación de equipos en las redes	✓	
- Protección de puerto		**X**
- Segregación de redes	✓	
- Control de conexión a la red	✓	
- Control de enrutamiento a la red		**X**
Control de acceso al sistema operativo		
- Procedimiento de un registro seguro		**X**
- Identificación y autenticación de usuarios	✓	
- Sistema de gestión de contraseñas	✓	
- Limitación del tiempo de conexión	✓	

Tabla 11 Validación de cumplimiento

Como se puede observar en la matriz de cumplimiento, las características que se pretendían evaluar del aplicativo PacketFence seleccionado como aplicativo OpenSource para la implementación de control de acceso y políticas tipo BYOD cumple en un 77.77% en su funcionalidad, y el 22.23 % restante no se pudo comprobar dado el alcance y recursos con los cuales se contó para desarrollar el laboratorio propuesto, aspectos tales como contar con un switch para solo conectividad y no contar con un Switch Core Capa 3 que permitiera el manejo de VLANs para probar su alcance con este tipo de redes segmentadas; a nivel inalámbrico solo se contó con un router inalámbrico que permite actuar como bridge de la red cableado y no con una controladora y Access Points donde se pudiera validar otros criterios de autenticación.

¿Cómo contribuye el trabajo de investigación al tema de estudio BYOD y NAC para la gestión de redes seguras?

El presente trabajo de investigación contribuye a la gestión de redes seguras, presentando una opción alternativa para implementar control de acceso (NAC) y políticas tipo BYOD para redes cableadas e inalámbricas, utilizando software con licenciamiento Opensource.

Presupuesto aproximado de la solución:

Se parte del hecho que la institución ya tiene su infraestructura de red cableada e inalámbrica implementada, así que la inversión para la instalación y configuración del PacketFence será:

Item	Valor
Servidor	$ 15.000.000.oo
Horas Profesionales (80 Horas)	$ 8.000.000.oo
Total Inversión	$ 23.000.000.oo

CAPITULO V

5. CONCLUSIONES Y RECOMEDACIONDES

5.2 Conclusiones

- Con las pruebas realizadas con la herramienta PacketFence se puede decir que cumple en un 78% con los requerimientos de una solución para implementar control de acceso a una red LAN y WLAN y políticas tipo BYOD siendo una solución OpenSource que puede facilitar su implementación en instituciones con pequeñas y medianas infraestructuras tecnológicas y presupuestos reducidos de inversión.
- Para un trabajo futuro con la implementación de NAC en una organización o empresa se requeriría una investigación dedicada a establecer las políticas necesarias para controlar los diferentes niveles de acceso y personal dedicado a su implementación.

- Al ser una herramienta *OpenSource* su implementación es más asequible dado que sus componentes son de libre distribución, lo cual no implica que su nivel de implementación sea sencilla, pues se requiere de un alto nivel de conocimientos a nivel de plataforma de sistemas operativos, servicios de red, conocimientos en seguridad informática y *networking*.
- Las soluciones comerciales que se pudieron evaluar permiten una administración más sencilla para su implementación y gestión, lo cual se traduce igualmente en un mayor valor comercial, lo cual debería evaluar una empresa u organización al momento de tomar la decisión de implementar una solución tecnológica de este tipo.

5.3 Recomendaciones

- Es necesario contar con plataformas de administración de redes con soporte para todo tipo de dispositivos, de manera que la información de la empresa no pueda ser vista desde el exterior de la red local y no queden así vulnerables a intrusiones o ataques informáticos a través de Internet.
- Las políticas sobre la información deben acompañarse con un sistema de credenciales de acceso que coadyuven en el aseguramiento de la misma.
- Una estrategia BYOD implica analizar los costos, los riesgos e involucrar a los recursos humanos y la gestión jurídica.
- Realizar auditorías específicas para monitorizar cómo estos nuevos elementos afectan a la red. Los sistemas de redes autodefinidas por software o SDN (Software Defined Networks, por sus siglas en inglés) permitirán reconocer los roles de cada usuario y/o dispositivo que accede a la red, mecanismos de automatización para que la red se reconfigure por sí sola respondiendo a actividades identificadas, crearán una administración y aplicación automática de perfiles de seguridad.
- Tener un control de todos los dispositivos que se conecten a la red de la empresa. Para ello existen soluciones del tipo "*Endpoint Protection Platforms*" (auditoría de hardware y software, gestión de parches y vulnerabilidades, control de aplicaciones) que permiten tener inventariados todos los dispositivos, los cuales tiene Packetfence.
- Gestionar las contraseñas. Las políticas de contraseñas para dispositivos BYOD no deberían ser diferentes de los requisitos que se deben cumplir para establecer contraseñas seguras para los activos de TI tradicionales como ordenadores portátiles o equipos de escritorio.
- Aplicar la política a una red segmentada: los datos confidenciales deben residir siempre en una red distinta a la que está abierta a invitados, contratistas u otras personas que no son empleados. Packetfence permite este tipo de manejo por medio de VLANs.

- Las herramientas MDM (Mobile Device Management) son soluciones diseñadas para ayudar a las compañías en la administración de todo lo que tiene que ver con el ámbito móvil: dispositivos, aplicaciones y contenido. En cuanto al BYOD, los sistemas MDM aportan herramientas para gestionar toda la plataforma de dispositivos móviles, pertenezcan o no al empleado. [27]
- La Universidad Autónoma de Bucaramanga podría realizar la implementación de PacketFence por medio de un proyecto de grado de la facultad de ingeniería de sistemas que se encargará de realizar el estudio de requerimientos para el control de acceso y la definición de políticas tipo BYOD para su red inalámbrica, y posteriormente la implementación en su infraestructura de red.

BIBLIOGRAFIA

[1] «Cisco,» 2012. [En línea]. Available: http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD_Horizons-Global_LAS.pdf.

[2] F. Pereñiquez Garcia, «Universidad de Murcia,» 2011. [En línea]. Available: http://www.tdx.cat/handle/10803/32055.

[3] J. J. y. B. Rumipulla, Octubre 2012. [En línea]. Available: http://dspace.ups.edu.ec/bitstream/123456789/4282/1/UPS-CT002616.pdf.

[4] L. R. J. d. l. C. Ana Escalier. [En línea]. Available: http://es.slideshare.net/marlucoca/control-de-acceso-a-red. [Último acceso: 2014].

[5] O. Melero, 2014. [En línea]. Available: http://riunet.upv.es/bitstream/handle/10251/38257/NicolasMelero_M%C2%AAOlvidoMEMORIAerasmus.pdf?sequence=1&isAllowed=y.

[6] QuinStreet, «Webpedia,» 2015. [En línea]. Available: http://www.webopedia.com/TERM/B/BYOD.html.

[7] IBM. [En línea]. Available: http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html. [Último acceso: 14 Mayo 2015].

[8] CIO, «CIO,» 25 junio 2014. [En línea]. Available: http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html.

[9] A. López, Seguridad Informática, Infomática y Comunicaciones, Editex, S.A, 2010.

[10] «ISO,» [En línea]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=39612. [Último acceso: 3 Junio 2015].

[11] «CQR,» Septiembre 2013. [En línea]. Available: https://www.crq.gov.co/Documentos/NORMAS_SEGUIRIDAD_CRQ.pdf.

[12] «WatchGuard,» [En línea]. Available: http://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp_es.pdf. [Último acceso: 26 Junio 2015].

[13] «Wikipedia,» [En línea]. Available: http://es.wikipedia.org/wiki/Control_de_acceso_a_red. [Último acceso: 2014].

[1 «Siliconweek,» [En línea]. Available: http://www.siliconweek.es/e-enterprise/como-elegir-la-

4] mejor-solucion-de-control-de-acceso-a-la-red-nac-751. [Último acceso: Junio 25 2015].

[1 A. T. Cordoba, «Instituto Politecnico Nacional,» Abril 2010. [En línea]. Available:
5] http://tesis.ipn.mx/bitstream/handle/123456789/6823/ESIME-RADIUS.pdf?sequence=1.

[1 «wikipedia,» [En línea]. Available: http://es.wikipedia.org/wiki/Software_libre. [Último acceso:
6] 8 Noviembre 2014].

[1 C. IBSG, «Cisco,» [En línea]. Available:
7] https://www.cisco.com/web/about/ac79/docs/re/byod/BYOD-Economics_Presentation_ES-XL.pdf. [Último acceso: 2015].

[1 I. Gartner, «Bing your Own Device: The Results and the future,» 2014.
8]

[1 G. G. P. P. S. M. David Rivera, «Analysis of Security Controls for BYOD,» 2015.
9]

[2 «Gartner,» [En línea]. Available: https://www.gartner.com/doc/2638216/technology-overview-
0] emerging-mobile-device. [Último acceso: 11 Mayo 2015].

[2 C. M. P. Cevallos, «Space,» 2012. [En línea]. Available:
1] http://dspace.espoch.edu.ec/bitstream/123456789/2429/1/18T00505.pdf.

[2 «Openaccess,» [En línea]. Available:
2] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28041/3/dgc59f_TFC_Memoria_0901.pdf. [Último acceso: 5 Marzo 2015].

[2 «Opennac,» [En línea]. Available: http://www.opennac.org/opennac/en/about/what-is-
3] opennac.html. [Último acceso: 12 Marzo 2015].

[2 [En línea]. Available:
4] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28041/3/dgc59f_TFC_Memoria_0901.pdf. [Último acceso: 3 Mayo 2015].

[2 «PacketFence,» 2008. [En línea]. Available:
5] http://www.packetfence.org/about/advanced_features.html.

[2 «openaccess,» [En línea]. Available:
6] http://openaccess.uoc.edu/webapps/o2/bitstream/10609/27941/8/bsimomTFM1213mem%C3%B2ria.pdf. [Último acceso: 4 Abril 2015].

[2 TRC. [En línea]. Available: http://www.trc.es/documentacion/integracion/TRC_BYOD.pdf.
7] [Último acceso: 16 Junio 2015].

[2 «PackeFence,» [En línea]. Available: http://packetfence.org/. [Último acceso: 15 Abril 2015].
8]