UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN

CARRERA: INGENIERÍA EN SISTEMAS INFORMÁTICOS

TEMA: Implementación e integración de solución aplicativa NAC para la administración y control de políticas de seguridad de acceso a red de dispositivos inalámbricos y alámbricos

AUTOR: **Luis Álvaro Pérez Rivera**

TUTOR: **Mg. Ing. Franz del Pozo**

D.M. Quito, marzo del 2015

AGRADECIMIENTO

Principalmente a Dios Todo Poderoso, sin su cuidado no habría podido culminar con este y el resto de mis proyectos de vida. Mateo 6:25-34. "Por nada estéis afanosos sino sean conocidas vuestras peticiones delante de Dios en toda oración y ruego, con acción de gracias."

A mi Esposa Gabriela y mis Hijas Fernanda y Valeria, a quienes agradezco su comprensión y paciencia en todo momento, quienes con su amor y apoyo hacen que cada día se renueve mi ánimo.

A mi Madre y mis Suegros con sus consejos oportunos han orientado y guiado, encaminado a un mejor porvenir.

A los Profesores, Autoridades y la Universidad que me han permitido continuar con los estudios, quienes han sido guías inherentes en el desarrollo de los proyectos, anhelo que se ha cumplido gracias al esfuerzo personal.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO 1

1.1 INTRODUCCIÓN

En el presente mundo globalizado la información constituye una pieza clave, en el ámbito empresarial y laboral, está en constante evolución permitiendo una mayor independencia por parte del empleado, con mayor flexibilidad en horarios, donde el empleado puede trabajar desde su casa u otra ubicación externa a la empresa. Esta evolución contribuye a la movilidad, pro-actividad y autonomía en el desarrollo de su trabajo; exige un manejo adecuado, acceso y entrega de información, comunicación inmediata y efectiva.

Se espera que la conectividad de smartphone / tablets rebase a la tecnología de computadoras portátiles y fijas. No es ninguna sorpresa que estos dispositivos móviles se están insertando cada vez más a los lugares de trabajo y se están utilizando para realizar tanto funciones críticas para los negocios como tareas privadas del usuario.

Ahora, el usuario en una empresa tiene entre 2 y 4 dispositivos móviles, la mayoría requiriendo conectividad inalámbrica y este número continúa aumentando. Junto con el rediseño y la actualización de la infraestructura inalámbrica para admitir estos dispositivos; algunas organizaciones empresariales han comenzado a desarrollar aplicaciones para empleados y para tiendas de aplicaciones personalizadas. (FLUKE Network)

El Diario Ti.com reveló un informe de la encuesta “Data Security Report“, en el cual sostiene que el aumento de dispositivos móviles personales y sus aplicaciones que se mezclan con la red corporativa están obligando a los expertos en TI a diseñar nuevas estrategias para resolver problemas de seguridad. El mismo también informa que un 82% de los encuestados señaló que los empleados de sus organizaciones están utilizando más dispositivos y aplicaciones para el trabajo personal. Sin embargo, sólo el 32% de estas empresas investigadas, han llevado a cabo auditorías de seguridad de las aplicaciones afectadas por estos dispositivos móviles. Pero aún, un 90% de los encuestados aseguró que su compañía no cuenta con tecnología para impedir que

estos dispositivos accedan por su propia cuenta a los sistemas corporativos, vulnerando la seguridad de la red… (BYOD Problemas de seguridad en redes corporativas)

La tendencia Bring Your Own Device (BYOD) significa la política de permitir a los empleados traer dispositivos móviles (laptops, tablets, y smartphones) a su lugar de trabajo y usar esos dispositivos para acceder a información y aplicativos de la empresa. (Rodriguez, 2013)

El verdadero reto para las organizaciones es como adoptar una práctica inevitable reduciendo al mínimo sus riesgos. BYOD en estos tiempos representa un signo claro de que los límites entre la vida personal y la profesional se están acercando, el modelo de trabajo tradicional de 8 horas se está desplazando al requerimiento de que un empleado preste servicios fuera de su horario de trabajo, pasando a vivir un entorno global de servicios 24horas/7dias a la semana, en el cual el empleado está pendiente de recibir información mientras esta en gozo de su horario familiar o de descanso.

Por esta razón existe la necesidad de plantear la propuesta de investigar acerca de aplicaciones para la administración control y acceso de equipos móviles y fijos a la infraestructura de red, utilizando una herramienta OpenSource NAC (Network Access Control) que permite implementar políticas y control para el acceso a información; control que es imprescindible en el resguardo de información crítica, contribuyendo a la disponibilidad de información, y confidencialidad de acceso a datos de manera segura y efectiva.

El control de acceso a la red NAC es usado para definir como asegurar la infraestructura de red antes de que usuarios accedan a ésta; el mecanismo de protección abarca varias tecnologías que permiten a las empresas garantizar la imposición de las políticas de seguridad corporativas a los puntos finales conectados a sus redes.

Las ventajas importantes de la tendencia BYOD y NAC es que el usuario o empleado puede coordinar mejor su vida laboral con su vida familiar, también permite el ahorro económico, evitando la adquisición del nuevo software como es la adquisición de licencias en sistemas operativos de PCs.

Para implementar un proyecto de BYOD hay que asegurar los mecanismos de conexión a la red y establecer políticas de uso aceptable donde se especifiquen los alcances en cuanto a propiedad de la información, soporte técnico sobre los dispositivos, y la seguridad de la información.

Esta tendencia crea una brecha de seguridad importante para las redes de una institución u empresa puesto que por intermedio de estos equipos se puede ingresar a servicios sensibles como servidores, además de poder tener acceso para realizar ataques interno (hackers, virus informáticos) y capturar los datos críticos de sistemas y servicios de la red; las empresas en la actualidad se encuentran conectadas a redes distribuidas en el resto del país por lo cual pueden tener acceso a red corporativas comprometiendo aún más la seguridad.

Razón por la cual se define el problema principal referente a BYOD y NAC sobre empresas o instituciones, como el no tener las herramientas necesarias para administrar un grupo de dispositivos móviles y fijos con diferentes versiones de sistemas operativos, con niveles diferentes de seguridad, con múltiples tipos de aplicaciones, programas; y que además pudieran funcionar para tener acceso a todos los recursos de una empresa de forma móvil sin control y seguridad alguna que al final comprometería la seguridad de información sensible.

1.2 JUSTIFICACIÓN

El concepto NAC realiza exactamente el control de acceso a una infraestructura de red con políticas de seguridad, incluyendo pre-admisión, chequeo de políticas de seguridad en el usuario final, controles post-admisión sobre los recursos a los que pueden acceder en la red tanto los usuarios, dispositivos y además que pueden hacer o comprometer dentro de la red.

Podemos ver diferentes tipos de usuarios que acceden a las redes de dominio privado e internet. Por lo antes expuesto, es necesario la implementación de políticas de control, acceso y seguridad, las mismas que nos garanticen que la infraestructura de red no sea comprometida o perjudicada al conectar nuevos dispositivos; impidiendo ataques e incluso robo de información confidencial o problemas inherentes a aplicativos que degradan los servicios de red.

Gracias a la integración e implementación de este aplicativo NAC OpenSource PacketFence es posible aislar y controlar el acceso a la infraestructura de red, garantizando un nivel de seguridad definido previamente mediante el establecimiento de parámetros de autenticación; asegurando se cumpla las políticas asignadas a los usuarios y dispositivos, facilitando con esto la gestión y administración.

1.3 OBJETIVO DE ESTUDIO

1.3.1 Objetivo general

Mejorar la administración de dispositivos alámbricos e inalámbricos, estableciendo políticas de seguridad, compatibilidad, confiabilidad para el control de acceso a la infraestructura de red a equipos móviles BYOD invitados y propios de la empresa.

1.3.2 Objetivos específicos

- Determinar las políticas de seguridad que se deben aplicar para asegurar el ambiente de red.

- Investigar un aplicativo NAC OpenSource para el control de acceso a la red mejorando la administración, operación y seguridad en dispositivos BYOD de la infraestructura de red.

- Implementar un caso de estudio, realizando ambientes de instalación, configuración, pruebas de funcionamiento del aplicativo.

1.4 HIPÓTESIS

- Estableciendo las políticas de seguridad, confiabilidad para el control de acceso a la infraestructura de red, se garantizará la seguridad de la información sensible de la empresa. La autentificación, registro, admisión de dispositivos y usuarios facilitará el acceso, uso de recursos restringidos, compartidos o públicos. La administración, seguimiento, gestión del aplicativo NAC y admisión a sus clientes contribuirá a cumplir con el objetivo general planteado.

CAPITULO 2

2. FUNDAMENTACION TEÓRICO

2.1 ANTECEDENTES

El fenómeno de la movilidad es uno de los impulsores de la tecnología en la actualidad. Hasta hace pocos años, la conexión inalámbrica era tan solo una cómoda opción para ofrecer conectividad en salas de conferencias y en campus específicos.

Con la llegada de todo tipo de dispositivos inalámbricos, el requisito de la movilidad y la conexión inalámbrica en movimiento, así como la ausencia de puertos Ethernet físicos en estos dispositivos, ha provocado que la conexión inalámbrica haya pasado de ser una simple comodidad a convertirse en una necesidad primaria de acceso para la conectividad de redes. (Aeroibe, 2013)

Ante esta movilidad inalámbrica en el lugar de trabajo, los administradores de tecnología de la información (IT) se enfrentan a más desafíos, como: ¿cuánto ancho de banda será suficiente? ¿Qué tipo de dispositivos surgirán en el futuro? ¿Qué ocurrirá el año que viene? La pregunta es cómo puede prepararse un administrador informático para un conjunto desconocido de dispositivos, con requisitos de ancho de banda y conectividad desconocidos, con el mismo número de recursos y, al mismo tiempo, tener la seguridad de que su red será segura, ofrecerá un alto rendimiento y estará listo para la siguiente ola de nueva tecnología, sobre todo la Gigabit Wifi. (Aeroibe, 2013)

Uno de los requisitos prioritarios que un administrador de red debe tener en cuenta para evaluar una solución de proveedor de redes es disponer de un modo de conectar y supervisar los dispositivos tanto administrados como los no administrados. Sin embargo, una vez que acceden a la red, ¿qué hacer con ellos? ¿Qué características o funcionalidades se deben buscar para garantizar la seguridad, la privacidad y la

productividad una vez que se permite a los usuarios conectar sus dispositivos? El verdadero problema de los recursos informáticos nunca ha sido la introducción de los dispositivos en la red, sino qué hacer con ellos una vez que estos acceden a la red.

Los principales factores que hay que tener en cuenta para una implementación con éxito son notificar el cumplimiento de normas de seguridad, garantizar que los dispositivos pueden usar los servicios y los activos disponibles al tiempo que se les impide el acceso a aquellos servicios y activos a los que no deben acceder, y garantizar que los dispositivos no saturarán los recursos de red que hay disponibles.

La normativa a aplicar en BYOD y NAC es identificar los tipos de usuarios que la institución va a proporcionar acceso a la red, estos pueden ser: empleados, funcionarios, estudiantes visitantes, invitados; todos los grupos indicados que deberán tener acceso a aplicaciones para realizar su trabajo (tarea) de manera cotidiana. Por este intermedio identificando quien va a tener acceso y a que información. Accesos por tipo de dispositivo. Determinar grupos de usuarios con características similares y permitir el acceso a determinadas funciones. Reglas de control de acceso, misma seguridad que resultará imprescindible para ayuda al resguardo de información privada.

Es muy importante la autentificación en el tema de infraestructura local, esto es todos los dispositivos móviles deben conectarse a la red a través de un método de autentificación seguro, basado en certificados 802.1x + Aut MAC Bypass (MAB); o evaluando con el departamento de IT de la institución una solución que ofrezca una conexión de manera automática proporcionando credenciales de autentificación a los diferentes dispositivos móviles. Este factor es esencial en BYOD.

Como control de acceso a red (NAC) es un enfoque de seguridad en redes de computadoras que intenta unificar las tecnologías de seguridad (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades, etc.) en los equipos finales, usuarios o sistemas de autenticación, reforzando la seguridad de la red.

Esta aplicación permitirá cancelar el acceso del dispositivo a la red si es el caso sin eliminar los derechos de ID del usuario sino del dispositivo especifico, esto por MAC Address, con esto el usuario podría trabajar con otro equipo móvil sin presentar dificultad en el acceso a la red NAC.

Para solucionar este tema de seguridad se ha planteado analizar y aplicar la tecnología NAC con herramientas OpenSource en plataforma Linux, de lo cual la propuesta es implementar la herramienta adecuada para poder controlar el acceso a los recursos de la infraestructura de red.

2.2 LA CONSUMERIZACIÓN DE LA IT

Tradicionalmente, los dispositivos que las empresas ponen a disposición de sus empleados, como computadores de escritorio, portátiles o teléfonos móviles, son con frecuencia los más avanzados a los que aquellos tienen acceso. La proliferación de dispositivos de consumo como portátiles, tablets, notebooks, smartphones, etc., ha facilitado que los empleados dispongan en muchos casos de herramientas de productividad más avanzadas para su uso personal.

Por este motivo, a medida que la tecnología desempeña una función cada vez más importante en sus vidas personales, los empleados se acostumbran a la potencia y comodidad de los nuevos servicios (intercambio de datos con almacenamiento en la nube, correo web, conectividad permanente, etc.) consultas al casillero de correo electrónico mediante smartphones y otros dispositivos móviles que también permiten almacenar y acceder a datos corporativos.

Desde el punto de vista del empleado, este prefiere trabajar con una Pc portátil, tablet o smartphone elegido por él, que adaptar sus necesidades y preferencias a un

dispositivo seleccionado para cumplir los requisitos de una parte de la organización; lo mismo ocurre con las aplicaciones y servicios.

La consumerización hace referencia a la tendencia actual, en el área de IT, por la cual la tecnología y los servicios orientados al usuario común, utilizados de manera privada, (como redes sociales, almacenamiento en la nube, webmail, smartphones, portátiles o tablets), están pasando a formar parte de la tecnología empleada por las empresas y sus empleados para llevar a cabo sus obligaciones profesionales. Mediante la consumerización, los empleados de una empresa utilizan sus propios dispositivos y aplicaciones particulares para realizar su trabajo. (Defensa, 2013)

Este término es empleado para referirse al conjunto de nuevas tecnologías y servicios externos a una empresa determinada que permite a los usuarios trabajar en cualquier momento y lugar. Debido a este movimiento, el modo de trabajar de empleados y empresas se está viendo transformado a gran velocidad. A pesar de no ser un término ampliamente extendido, la mayoría de los departamentos de IT se han enfrentado ya a alguno de los retos que presenta esta consumerización. Las implicaciones de la extensa utilización de dispositivos personales en el lugar de trabajo están forzando el cambio en las filosofías de trabajo y las prácticas de los profesionales de IT. La consumerización tiene un importante impacto en el modo en que los departamentos de TI de las empresas protegen sus puestos de trabajo y los datos corporativos.

La primera señal de que una empresa está aceptando la consumerización de la IT es la aplicación de programas «trae tu propio dispositivo» (ya referido anteriormente como BYOD). El BYOD se ha convertido en uno de los fenómenos que más incidencia ha tenido o tendrá en las organizaciones de IT. La tendencia BYOD permite que los empleados usen sus propios dispositivos, como computadores portátiles, tablets o smartphones, para acceder a los recursos de la empresa, así como aplicaciones móviles que habilitan el acceso a servicios corporativos.

Por tanto, el término BYOD se utiliza para referirse a una gran corriente actual que permite a los empleados conectarse a la red de su empresa y acceder a sus datos mediante la utilización de sus dispositivos personales. Requiere, por consiguiente, la introducción de algunos cambios para adaptarse al empleo de nuevos dispositivos en el entorno laboral. (Defensa, 2013)

Vulnerabilidad	Amenaza	Riesgo
La información viaja a través de redes inalámbricas que normalmente son menos seguras que aquellas cableadas.	Numerosos ataques documentados sobre redes inalámbricas.	Interceptación de información con el resultado de acceso a información sensible. Daño a la imagen de la empresa.
La movilidad proporciona la oportunidad de extender la zona de trabajo más allá de los límites físicos de las instalaciones de la empresa, por lo tanto, determinadas medidas y controles de seguridad no tienen efecto.	Los dispositivos de usuarios pueden contener *malware*, que podría ser más fácilmente introducido en las redes y sistemas de la organización.	Propagación de *malware*. Fuga de datos. La integridad, disponibilidad y confidencialidad de los datos pueden verse afectadas.
Muchos usuarios utilizan la tecnología *Bluetooth* para conectar dispositivos manos libres; sin embargo, no lo deshabilitan cuando no se está utilizando.	El dispositivo es visible para *hackers*, pudiendo lanzar un ataque.	Corrupción del dispositivo. Pérdida de datos. Exposición de información sensible.
El dispositivo almacena información no cifrada.	En el caso de pérdida o robo del dispositivo, la información almacenada en él estaría en claro y sería accesible a terceros.	Exposición de información sensible.
La pérdida de datos puede afectar a la productividad del empleado.	Debido a la portabilidad, los dispositivos pueden sufrir pérdidas o robos, y con ellos toda la información que almacenan.	Fuga de información.
La organización no gestiona los dispositivos.	Si no existe una estrategia de dispositivos móviles, el empleado puede conectar fácilmente sus dispositivos inseguros a la infraestructura de red de la empresa.	Fuga de información. Propagación de *malware*. Pérdida de control de la ubicación y accesos a la información.
El dispositivo permite la instalación de aplicaciones de terceras partes.	Las aplicaciones pueden contener *malware*, troyanos o virus.	Propagación de *malware*. Fuga de información. Puertas traseras en la red de la empresa.

Tabla 1: Principales vulnerabilidades de BYOD

La tabla muestra algunos ejemplos de las principales vulnerabilidades y los riesgos asociados a los que se enfrentan las empresas con las nuevas tendencias de consumerización.

|

Los programas BYOD revelan que las empresas no solo toleran el uso de dispositivos responsabilidad y propiedad del usuario sino que también lo incentivan y lo promueven. Por lo tanto considerando todos los aspectos que enfrenta una infraestructura de red es importante conceptualizar todos los términos involucrados en el uso y puesta en producción del servicio BYOD y NAC en el ámbito de tecnología de información.

2.3 SEGURIDAD INFORMÁTICA

La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de información, para que un sistema, aplicativo o información se considere segura deberá estar libre de peligro, riesgo o daño.

La seguridad informática debe establecer normas que minimicen (no existe seguridad al 100%) los riesgos de la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática, minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de la información de manera responsable.

La seguridad informática consiste en asegurar que los recursos del sistema informático de la organización estén disponibles y sean utilizados de la forma definida para su correcto uso, además de que su acceso y modificación estén limitados a las personas autorizadas. (Seguridad de la Información, 2011)

La seguridad informática debe garantizar:

- **La Disponibilidad de los sistemas de información:** Es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. El objetivo es que debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

- **La Integridad de la información:** busca mantener los datos libres de modificaciones no autorizadas, es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

- **La confidencialidad de la información:** Es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. Asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

La seguridad informática ha adquirido una gran importancia en los últimos tiempos, sobre todo para empresas. Esta situación se debe al constante avance tecnológico y al aumento de la dependencia digital a la hora de tratar la información, aumentando considerablemente los delitos informáticos para obtener beneficio.

Estos problemas están presentes en la mayoría de la infraestructura que no tiene definido un esquema de seguridad eficiente, el cual proteja los recursos de las actuales amenazas a las que esté expuesto.

Es este aspecto de la seguridad informática que tiene como objetivo la protección de los recursos informáticos contra daños, destrucción, uso no autorizado robo además

de mantener la integridad de los datos y permitir el uso eficiente de los recursos tecnológicos.

Comprende también aspectos relacionados con estándares, políticas, mejores prácticas, valores de riesgos y otros elementos necesarios para el correcto funcionamiento y administración de los recursos.

2.4 REDES DE AUTODEFENSA

Es un conjunto de sistemas estratégicos para la seguridad, que utiliza la red para identificar, impedir y adaptarse a las amenazas que provienen de fuentes internas y externas. Una red de autodefensa simplifica el entorno de seguridad a través de una estrecha integración, una completa seguridad, una mayor visibilidad de extremo a extremo y un mejor coste total de propiedad. Todos los componentes de la red (la plataforma de red segura, los servicios y tecnologías avanzadas, la administración operativa y el control de políticas de seguridad) juegan un papel importante en la seguridad del entorno de red. (Cisco, 2013)

2.5 CONTROL DE ACCESO A LA RED (NAC) - ATAQUES Y AMENAZAS

El marco de *Control de Acceso en Red* ayuda a las organizaciones a protegerse de las amenazas como spyware, virus, gusanos que intenten acceder a la red corporativa a través de cada vez una mayor variedad de dispositivos y terminales computacionales.

El control de acceso a red representa una categoría emergente en área de seguridad, su definición es controvertida y está en constante evolución. Los objetivos principales de este concepto se pueden resumir en:

- **Mitigar ataques de día cero:** El propósito clave de una solución NAC es la habilidad de prevenir en los equipos finales la falta de antivirus, parches o software malicioso, la prevención de intrusión de hosts, acceder a la red poniendo en riesgo a otros equipos de posible contaminación y expansión de gusanos informáticos.

- **Refuerzo de políticas:** La solución NAC permite a los operadores de red definir políticas, tales como tipos de dispositivos o roles de usuarios con acceso permitido a ciertas áreas de la red, forzarlos y controlarlos en switches y/o access point.

- **Administración de acceso e identidad:** Donde las redes IPs convencionales refuerzan las políticas de acceso con base en el direccionamiento IP, los dispositivos NAC lo realizan basándose en identidades de usuarios autenticados, para usuarios finales de equipos portátiles y fijos.

Un ataque informático es un método por el cual un individuo intenta explotar las vulnerabilidades del sistema para tomar el control, desestabilizar el sistema o robar información. Según la recomendación X.800 y la RFC 2828 los ataques pueden clasificarse en los siguientes tipos:

- **Ataques Pasivos:** Consisten en la observación de transmisiones sin afectar a los recursos, ni alterar la comunicación para obtener datos.

  Ejemplos: Eavesdropping, Sniffers, etc.

- **Ataques Activos:** Consisten en interferir flujos de comunicaciones y aprovechar vulnerabilidades del sistema para tomar el control.

  Ejemplos: Suplantación de identidad, exploits, etc. (Cerón)

2.6 CONTROLES DE SEGURIDAD

Para poder proporcionar controles de seguridad, es necesario implantar un control de acceso, el cual se encargue de limitar el paso a los recursos, mediante la autenticación de los usuarios y la autorización pertinente para acceder al recurso.

- **Controles Físicos:** Aquí están incluidos los sistemas biométricos, cámaras de vigilancia, alarmas térmicas, puertas de seguridad, etc.

- **Controles Técnicos:** Hay de dos tipos basados en red, ejemplos: Firewall, IDS, IPS; y basados en host, como antivirus, antiespias, antispam.

- **Controles Administrativos:** Son la definición de accesos, recursos y políticas de seguridad, del tipo de quien tiene acceso al recurso y por cuanto tiempo. (Cerón)

2.7 HERRAMIENTAS NAC

El significado de NAC es, el control de acceso a la red (Network Access Control), que es un conjunto de tecnologías y soluciones basadas en una iniciativa de la industria patrocinada por Cisco, utiliza la infraestructura de la red para hacer y cumplir la política de seguridad en todos los dispositivos que pretenden acceder a los recursos informáticos de la red, limitando así el daño causado por amenazas emergentes contra la seguridad. Los clientes (empresas) que usan NAC tienen la capacidad de permitir que accedan a la red sólo dispositivos de punto terminal (por ejemplo computadores alámbricos o inalámbricos, servidores, agendas PDA, etc.) confiables que cumplan con las políticas de seguridad y pueden limitar el acceso de los dispositivos que no las cumplen. (CISCO)

En este aspecto es necesario definir a PacketFence como una solución NAC OpenSource preparada para desplegar un sistema de control de acceso a red y proporcionar un completo sistema de control de acceso a redes.

2.7.1 Tipos de NAC

Dentro de esta clasificación tenemos:

- **NAC basado en Hardware:** Se basa en la instalación de un dispositivo físico apilable, encargado de procesar el tráfico de la red y ejecutar las políticas definidas.

- **NAC basado en Agente:** Se basa en el uso de programas instalados en los dispositivos clientes, los cuales recogen información para enviarla al servidor a la hora de acceder a la red. Esta opción es la que menos afecta a la red debido al procesado de los paquetes por parte del cliente.

- **NAC sin Agente:** Este modelo se basa en la ejecución de software desde un servidor hacia los clientes ejecutando escaneos en busca de incumplimiento en las políticas de seguridad. Este método presenta mayor congestión en la red.

- **NAC Dinámica:** En este modo se instalan varios agentes en servidores seguros encargados del cumplimiento de las políticas de seguridad, distribuyendo la carga de red y del sistema mediante los diferentes nodos donde se han instalados los agentes. (Cerón)

2.7.2 Elementos de un NAC.

- **Equipos cliente:** Dispositivo que solicita el acceso mediante un suplicante.

- **Autenticador:** Entidad que facilita la autenticación del cliente conectado al enlace, como puede ser un switch.

- **NAC Gateway:** Dispositivo que se encarga de gestionar los accesos, políticas de seguridad y la comunicación con el servidor de autenticación, por ejemplo software Open Source PacketFence.

- **Servidor de Autenticación:** Entidad que responde a las solicitudes de autenticación y valida el acceso usando protocolos de autenticación tales como 802.1X, EAP-MSCHAP, MAC, ejemplo servidor FreeRADIUS.

- **Servidor de Remediación:** Permite notificar y enviar al cliente las acciones necesarias para obtener acceso a la red en caso del incumplimiento de alguna política de seguridad.

2.7.3 Modos de operación de un NAC

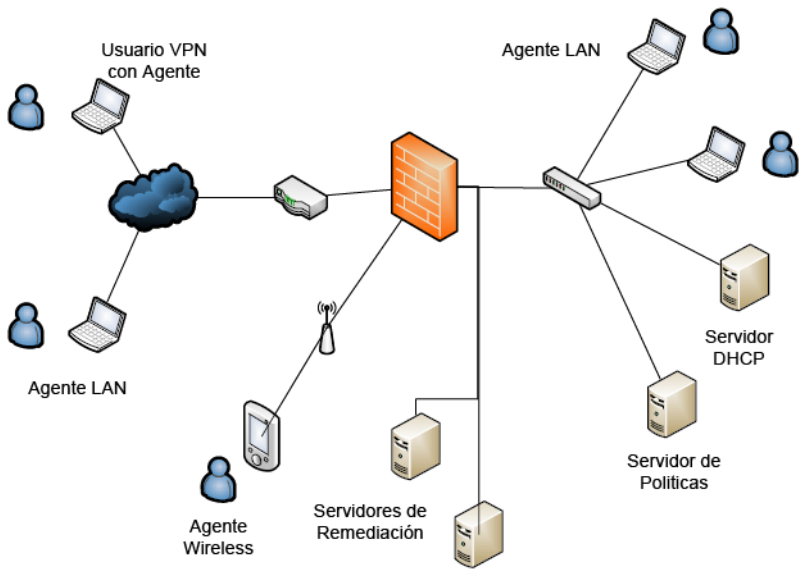


FIGURA 1: Elementos y Modos de Operación de la NAC

- Detección e identificación de nuevos dispositivos en la red.
- Autenticación de usuarios y dispositivos.
- Evaluación del sistema en cumplimiento de las políticas de seguridad.
- Autorización para acceder a la red.
- Remediación para equipos que no obtienen acceso

2.7.4 Controles de NAC

- **Pre-admisión y Post-admisión.-** Existen dos filosofías de diseño predominantes en NAC, basadas en políticas de refuerzo antes de ganar acceso a la red o después de hacerlo. En el primer caso denominado NAC pre-admisión, las estaciones finales son inspeccionadas antes de permitirles el acceso a la red. Un caso típico de NAC pre-admisión sería el prevenir que equipos con antivirus no actualizados pudieran conectarse a servidores sensibles. Alternativamente, el NAC post-admisión crea decisiones de refuerzo basadas en acciones de usuario después de que a estos usuarios se les haya proporcionado el acceso a la red.

- **Con agente vs sin agente.-** La idea fundamental de la tecnología NAC es permitir a la red tomar decisiones de control de acceso basadas en inteligencia sobre los sistemas finales, por lo que la manera en que la red es informada sobre los sistemas finales es una decisión de diseño clave. Una diferencia entre los sistemas de control de acceso (NAC) es si requieren 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.

- **Solución, cuarentena y portal cautivo.-** Los administradores de sistemas y redes despliegan productos NAC con la esperanza de que a algunos clientes legítimos se les denegará el acceso a la red (si los usuarios nunca tuvieron antivirus desactualizados y sus sistemas están siempre actualizados, NAC no sería necesario). Por ello las soluciones NAC requieren de un mecanismo para remediar el problema del usuario final que le ha sido denegado el acceso a la red.

Las dos estrategias comunes para denegar el acceso a las redes, son redes de en cuarentena y portales cautivos.

- **Red en cuarentena:** Es una red IP restringida que proporciona a los usuarios acceso encaminado sólo a determinados hosts y aplicaciones. La cuarentena es a menudo aplicado en términos de asignación de VLAN's, y cuando un producto NAC determina que un usuario final no cumple con las políticas de seguridad, su puerto de switch se asigna a una VLAN que se dirige sólo a los servidores de revisión y actualización, pero no con el resto de la red. Otras soluciones también usan técnicas de gestión direcciones (por ejemplo, Address Resolution Protocol (ARP) o Neighbor Discovery Protocol (NDP)) para la cuarentena, evitando la sobrecarga de la gestión de VLAN de cuarentena.

- **Portal cautivo:** Intercepta el acceso HTTP a páginas web, redirigiendo a los usuarios a una aplicación web que proporciona instrucciones y herramientas para la actualización de su computador. Hasta que su equipo pasa la inspección automatizada, sin uso de la red.

- **Portales cautivos externos:** Permiten a las organizaciones descargar controladores inalámbricos e intercambiadores de portales web de los hostting. Un portal único externo ofrecido por un dispositivo NAC para la autenticación inalámbrica y por cable, elimina la necesidad de crear varios portales, y consolida los procesos de políticas de gestión.

2.7.5 Características de NAC.

La primera tarea de NAC es a qué clientes se autoriza a acceder y permanecer en la red. Los criterios para tomar estas decisiones pueden variar ampliamente, en función de múltiples parámetros de la máquina cliente, como disponer de un software antivirus debidamente actualizado, un sistema operativo con los parches adecuados o un cortafuego configurado apropiadamente, por citar sólo algunos.

El objetivo es prevenir que los dispositivos que hayan sido contaminados en otras redes accedan a la red corporativa. Los dispositivos móviles y los utilizados por visitantes o socios comerciales que acceden a los recursos de la empresa son buenos ejemplos de clientes potencialmente peligrosos.

NAC puede también volver a ejecutar periódicamente los chequeos de seguridad mientras los clientes permanecen conectados a la red para cerciorarse de su buen comportamiento. Asimismo, algunos equipos comprueban si los dispositivos intentan explotar recursos no autorizados, restringiendo el acceso cuando violan las políticas.

Pese a sus ventajas, la adopción de NAC está lejos de ser agresiva, ni en número de despliegues ni en sus primeras aplicaciones en los negocios. Según Nemertes Research, en la mayoría de los casos, el uso del control de accesos se limita a las conexiones VPN; sólo una minoría emplea hoy NAC en las LAN corporativas.

2.7.6 Arquitectura general de NAC.

Tres componentes básicos se encuentran en todos los productos NAC:

- El solicitante de acceso (Access Requestor o AR)
- La política de Punto de Decisión (Policy Decision Point o PDP)
- El punto de aplicación de políticas (The Policy Enforcement Point o PEP).

Las funciones individuales de la PDP y el PEP pueden estar contenidas en un servidor o propagarse a través de múltiples servidores, dependiendo de la implementación de los proveedores, pero en general, las peticiones de acceso AR, el PDP asigna una política, y el PEP hace cumplir la política.

La AR es el nodo que está intentando acceder a la red y puede ser cualquier dispositivo que se gestiona por el sistema NAC, incluyendo estaciones de trabajo, servidores, impresoras, cámaras y otros dispositivos habilitados para IP.

La AR puede llevar a cabo su evaluación propia de host, o algún otro sistema puede evaluar el host. In either case, the AR's assessment is sent to the PDP. En cualquier caso, la evaluación de la AR se envía al PDP. Sobre la base de la postura del AR y la definición de políticas de una empresa, el PDP determina cual acceso debería permitirse.

En muchos casos, el sistema de gestión del producto NAC puede funcionar como el PDP. El PDP se basa a menudo en los sistemas back-end, incluyendo antivirus, gestión de parches o directorios de usuarios, para ayudar a determinar la condición del host.

Una vez que el PDP determina la política a aplicar, esta comunica al control de acceso la decisión para la PEP realice su ejecución. El PEP puede ser un dispositivo de red, como un switch, firewall o router, un dispositivo fuera de la banda que maneje DHCP o ARP, o un agente del propio AR.

2.7.7 Ciclo de NAC

Cuando un host intenta conectarse a una red habilitada para NAC, normalmente hay tres fases: pre-admisión o la evaluación posterior a la admisión, la selección de políticas y aplicación de políticas. Los criterios que rigen cada paso se basan en la política de su empresa y las capacidades de su sistema de NAC.

FIGURA 2: Ciclo de NAC

Antes de seleccionar un producto, determine con exactitud cuáles son los objetivos de su empresa. Por ejemplo, ¿Qué tan lejos fuera de la fecha puede un host tener parches o firmas de antivirus antes de que ya no pueda acceder a la red? ¿Cuál es la condición aceptable antes de que un host invitado pueda tener acceso? ¿Quiere acceso a la base con un ID de usuario o no?

El ciclo de NAC comienza y termina con la evaluación. La evaluación de pre-ingreso se produce antes de que conceda un acceso total a la red. La evaluación posterior a la admisión después de que el acceso ha sido concedido; permite al host re-evaluarlo periódicamente para asegurarse de que no representa una amenaza.

La evaluación de host recopila información como los sistemas operativos de los hosts, niveles de los parches, aplicaciones que se ejecutan o se instalan, la postura de seguridad, la configuración del sistema, la conexión del usuario, y más; y lo pasa a un PDP. La información que recopila es una función de las políticas definidas y las capacidades del producto NAC.

2.7.8 NAC métodos de evaluación

La evaluación de host es una parte fundamental de determinar el estado de éste y el tipo de acceso que debe recibir. Estos son los métodos de evaluación más comunes usados hoy en día. Muchos proveedores de NAC soportan al menos dos de éstos métodos.

Las evaluaciones pueden utilizar un agente de instalación permanente, comúnmente en host basados en NAC, o agentes disolubles más probablemente, llamada así porque se basan en Java o ActiveX y desaparecen después de ser utilizados. Los agentes disolubles a veces se llaman NAC sin agente, pero este método implica de hecho que los agentes deben ser descargados e instalados en el computador del host.

El problema es que los modelos de seguridad en Windows, Mac OS X y Linux a menudo requieren agentes, ya sean permanentes o disolubles, y para esto debemos tener derechos de administrador local para ejecutarlos.

Esto se convierte en un problema en las organizaciones que (sabiamente) no permiten que los computadores portátiles y de escritorio se ejecuten con privilegios de administrador local. En algunos casos, los agentes pueden necesitar privilegios de administrador sólo la primera vez que es instalado, esto puede permitir trabajar evitando esta limitación.

Pero ¿qué pasa si no puede poner un agente en un sistema? En ese caso, las evaluaciones se llevan a cabo sin agente remoto a través de métodos de exploración o análisis, como ejecutar un escaneo de vulnerabilidades, o utilizando RPC (Remote Procedure Call) o WMI (Windows Management Instrumentation) para consultar un host. Por otra parte, el escaneo pasivo, mediante la detección de intrusiones y detección de anomalías de red, busca hosts maliciosos basados en el tráfico actual de la red. Una evaluación, incluso se podría definir como obligar a un usuario establecerse en una política de uso aceptable (Acceptable Use Policy) antes de ser concedido el acceso a la red.

Reevaluaciones posteriores a la conexión se producen después de que se concede el acceso al host. Estos se pasan por alto a su cuenta y riesgo, porque la condición de un hosts puede cambiar mientras se está conectado. Un gusano puede ser activado, o un usuario malintencionado podría empezar a atacar. La evaluación posterior a la conexión puede iniciarse automáticamente después de establecer un período de tiempo, por un administrador, según sea necesario, o basado en un cambio en el host, como un cortafuego de escritorio o el antivirus este deshabilitado. Nuevas evaluaciones se comparan con la política actual, y se toman acciones definidas.

Un giro interesante a las evaluaciones posterior a la conexión son los productos que utilizan la red de vigilancia pasiva, ya sea dentro del sistema de NAC o mediante la

integración con un sistema de detección de intrusiones existentes o un sistema de la red de detección de anomalías, para alertar sobre la actividad maliciosa. Estos monitores externos alertan sobre el tráfico de red y pueden detectar problemas de pérdidas por las evaluaciones basadas en host.

2.8 HERRAMIENTA NAC PACKETFENCE

Es totalmente compatible, confiable, libre y de código abierto que brinda apoyo en el control de acceso de red (NAC). Con un impresionante conjunto de funciones que incluyen un portal cautivo para el registro y la habilitación de usuarios, la gestión centralizada de redes cableadas e inalámbricas de soporte 802.1X, y aislamiento de dispositivos problemáticos, integración con el IDS Snort y el escáner de vulnerabilidades Nessus; PacketFence se puede utilizar con eficacia en seguridad de redes desde pequeñas a grandes redes.

Principalmente desarrollado en Perl con un poco de PHP, Web (HTML / CSS / JavaScript) y SQL, PacketFence aprovecha los componentes de los famosos proyectos de código abierto como Snort, Apache HTTPD, el Net-SNMP FreeRADIUS, mod_perl, MySQL, dhcpd, Bind (nombre), OpenVAS y mucho más.

2.8.1 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 discreta que trabaja con equipos de muchas marcas, tal como detallamos a continuación: 3Com, Aerohive, Allied Telesis, Aruba, Cisco, Dell, Enterasys, ExtremeNetworks, Extricom, Fundición / Brocade, Hewlett-Packard, Intel, Juniper Networks, LG-Ericsson EE.UU., Meru Networks, Motorola, Nortel / Avaya, Ruckus y Xirrus. Puede utilizarse en redes de:

- Bancos, Empresas de ingeniería y Fábricas
- Colegios y universidades
- Centros de convenciones y exposiciones
- Hospitales, centros médicos
- Hoteles

2.8.2 Componentes arquitectura PacketFence

Los componentes de PacketFence se ven representados en la siguiente imagen.

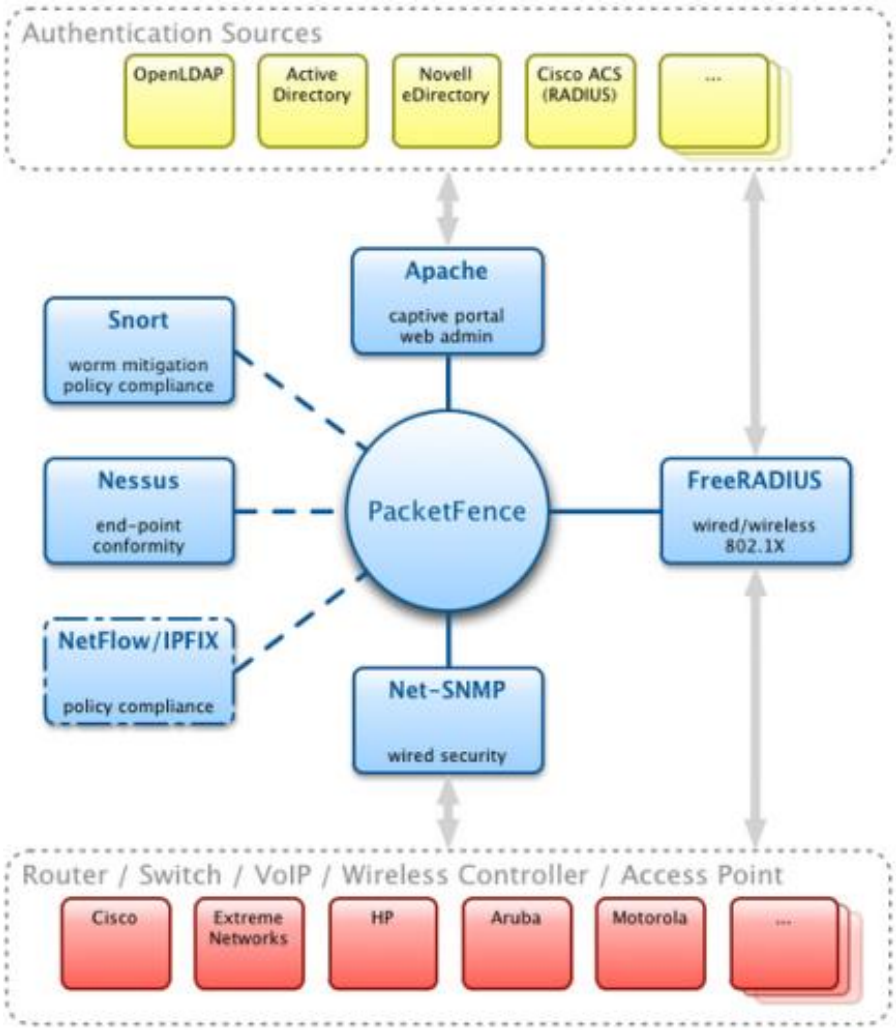


FIGURA 3: Arquitectura de PacketFence

2.8.3 Características generales

El modo Online es compatible con equipos alámbricos o inalámbrica, también se puede lograr una integración muy rápida, junto con un despliegue externo de una gran variedad de dispositivos.

- **Soporte 802.1X:** inalámbrico y alámbrico se apoya a través del módulo de FreeRADIUS [externo] que se incluye en el aplicativo.

- **Voz sobre IP (VoIP) Apoyo:** También llamada de telefonía IP (IPT), VoIP es totalmente compatible (incluso en entornos heterogéneos) con múltiples fabricantes de switches (Cisco, Edge-Core, HP, Linksys, Nortel Networks y muchos más).

- **Integración Wireless (inalámbrico):** Se integra perfectamente con las redes inalámbricas a través de un módulo de FreeRADIUS [externo].

Esto le permite asegurar sus redes alámbricas e inalámbricas de la misma forma utilizando la misma base de datos de usuario y el mismo portal cautivo, proporcionando una experiencia de usuario consistente. Permite la mezcla de puntos de acceso (AP Access Point) varias marcas de los controladores inalámbricos.

- ✓ **Registro de Dispositivos**

Apoya un mecanismo de registro opcional similar a soluciones portal cautivo. Al contrario de la mayoría de soluciones de portal cautivo, recuerda a los usuarios que previamente registrados y automáticamente se les dará acceso sin otra autenticación. Por supuesto, esto es configurable. Una política de uso se puede especificar de forma que los usuarios no pueden habilitar el acceso de red sin haberlo aceptado.

- ✓ **Detección de actividades de red anormales**

Actividades anormales de red (virus informáticos, gusanos, spyware, tráfico denegado por el establecimiento de política) pueden ser detectadas usando sensores Snort sean locales o remotos. Más allá de permite aplicar sus propias alertas y la supresión del mecanismo en cada tipo de alerta. Un conjunto de acciones configurables está disponible para los administradores.

- ✓ **Estado de Salud**

Mientras realiza una autenticación de usuario 802.1X, puede realizar una evaluación completa del dispositivo conectado utilizando la declaración (TNC) de protocolo de la Salud. Por ejemplo, puede verificar si se ha instalado un antivirus y la fecha de instalación, si los parches del sistema operativo están aplicados y mucho más; todo sin ningún agente instalado en el dispositivo final.

- ✓ **Escaneos de vulnerabilidades proactiva**

El análisis de vulnerabilidad Nessus o OpenVAS se pueden realizar en el registro del dispositivo, sea programado o sobre una base ad-hoc, correlaciona los ID de vulnerabilidad de cada exploración a la configuración de violación, retornando páginas web con el contenido específico informando sobre la vulnerabilidad que puede tener el huésped.

- ✓ **Remediación a través de un portal cautivo**

Una vez atrapado el tráfico de red, el flujo se determina con el aplicativo PacketFence. Con base en el estado de los nodos actuales (violación abierta, no registrado, etc.), se redirige al usuario a la URL correspondiente. En el caso de una violación, al usuario se le presenta instrucciones para la situación particular en la que se encuentre, reduce la intervención costosa del departamento de Help Desk.

- ✓ **Aislamiento de dispositivos problemáticos**

PacketFence soporta varias técnicas de aislamiento, incluido el aislamiento VLAN con soporte VoIP de múltiples fabricantes de switches.

- ✓ **De línea de comandos y gestión basada en la Web**

Proporciona pantallas basadas en Web y línea de comandos para todas las tareas de gestión. La administración basada en la Web es compatible con diferentes niveles de permisos para los usuarios y la autenticación de usuarios contra LDAP o Microsoft Active Directory (AD).

2.8.4 Funciones avanzadas de gestión de red

- ✓ **Gestión VLAN flexible y control de acceso basado en roles**

La solución se basa en el concepto de aislamiento de la red a través de la asignación de VLAN. Debido a su larga experiencia y varios despliegues, la administración de la VLAN de PacketFence llegó a ser muy flexible con el transcurso del tiempo. La topología VLAN privada se puede mantener, sin embargo PacketFence debe añadir dos nuevas VLAN a lo largo de su red, que son:

- VLAN de registro
- El aislamiento de la VLAN.

VLAN y los roles se pueden asignar utilizando los diversos medios:

- Por switch (con VLAN por defecto)
- Por categoría de cliente (predeterminado para los roles)

- ✓ **Acceso de invitados (BYOD) traiga su propio dispositivo**

La mayoría de las organizaciones integra una gran cantidad de consultores externos de diversas empresas, 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. Adicionalmente que rara vez se requiere que tengan acceso a la infraestructura corporativa interna, evitando carga administrativa (gestión por puerto VLAN).

- ✓ **Administración del acceso a invitados**

PacketFence admite una VLAN de invitados, esta VLAN de invitados se configura en su red solamente para tener acceso y salida hacia internet; el registro de VLAN y el portal cautivo son los componentes que se utilizan para explicar al cliente cómo registrarse para tener acceso y cómo funciona su acceso. Esto generalmente se marca por la organización que ofrece el acceso. Existen varios medios de registro para los huéspedes estos pueden ser:

- Registro manual de los huéspedes
- Contraseña del día
- El registro automático (con o sin credenciales)
- Acceso para invitados por patrocinador (empleado que de fe de un invitado)
- Acceso para invitados, activado por correo electrónico de confirmación
- Acceso para invitados, activado por la confirmación del teléfono móvil (mediante SMS)

También soporta creaciones el acceso de invitados e importaciones de los mismos. Se integra con la solución de facturación en línea, como Authorize.net. Con el uso de esta integración se puede manejar los pagos en línea, necesarios para obtener acceso de red correcta.

- ✓ **Administración de más tipos de violación**

PacketFence bloquea automáticamente los equipos de particulares en la red, además de usar Snort, OpenVAS Nessus como fuente de información, puede combinar los siguientes mecanismos de detección para bloquear efectivamente acceso a la red de estos dispositivos no deseados:

- ✓ **DHCP de huellas dactilares**

Puede bloquear los dispositivos basados en su huella digital DHCP. Casi todos los sistemas operativos tienen una huella digital única. PacketFence puede hacer uso de esta información y bloquear el acceso a la red de esos dispositivos; sobre la base de las huellas dactilares de DHCP se puede bloquear de forma automática, por ejemplo:

- Dispositivos PlayStation o cualquier otra consola de juegos.
- Puntos de acceso inalámbrico (WAP)
- Teléfonos VoIP
- Dispositivos de Apple iPod o iPhone
- Versiones antiguas de IE

- ✓ **User-Agent**

PacketFence puede bloquear los dispositivos basados en el User-Agent que se activa cuando estos dispositivos realizan actividades de red utilizando su navegador web incorporado.

- ✓ **Direcciones MAC**

Permite el bloqueo 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.

- ✓ **Registro automático**

Debido a que la mayoría de las redes en producción ya son muy grandes y complejas, ofrece varios medios para registrar automáticamente un cliente o dispositivo.

- **Por dispositivo de red:** Un dispositivo de red (Switch, AP, Wireless) se puede utilizar para registrar automáticamente todas las direcciones

MAC que solicite de acceso a la red. Muy útil para la agregar equipos a la red.

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

- **Por dirección MAC del vendedor:** La similitud por marca o proveedor se puede utilizar para registrar automáticamente los dispositivos de un proveedor específico. Por ejemplo, todos los productos de Apple pueden ser registrados de forma automática utilizando una norma de este tipo.

✓ **Vencimiento**

La duración del acceso a la red puede ser controlado con los parámetros de configuración. Se puede configurar por fecha absoluta (Jue 04 de agosto 2014 20:00:00 EST "), o por un periodo determinado de tiempo (cuatro semanas desde el primer acceso de la red) o tan pronto como el dispositivo pasa a estar inactiva. Dispositivos registrados sin actividad se convierten en no registrado. Con poca personalización también es posible hacer esto sobre una categoría de dispositivos. EL vencimiento también se puede editar manualmente en función de cada nodo.

✓ **Administración de ancho de banda**

PacketFence puede rastrear automáticamente la cantidad de ancho de banda que los dispositivos consumen en la red. Usando para esto su compatibilidad integrada, se puede poner en cuarentena o cambiar el nivel de acceso de los dispositivos que consumen demasiado ancho de banda durante un periodo de tiempo particular. Provee también informes sobre el consumo de ancho de banda.

- ✓ **Administración de dispositivos flotantes en la red**

Un dispositivo de red flotante es un Switch o Punto de Acceso (AP) que se puede mover alrededor de su red y que está conectado a los puertos de acceso. Una vez configurado correctamente, PacketFence reconoce los dispositivos de red flotante y configurará los puertos de acceso que permiten múltiples VLAN y adicionalmente más direcciones MAC. Una vez que el dispositivo se desconecta, retornará la configurar a su estado anterior.

- ✓ **Autenticación flexible**

Puede autenticar a los usuarios que utilizan varios protocolos / normas. Esto le permite integrarse en su entorno, sin necesidad de que los usuarios tengan que recordar su nombre de usuario y contraseña. También puede utilizar su base de datos SQL interna para autenticar a los usuarios a nivel local creados. Fuentes de autenticación soportados son:

- ➢ Microsoft Active Directory
- ➢ Novell eDirectory
- ➢ Open LDAP
- ➢ Cisco ACS
- ➢ RADIUS (FreeRADIUS, radiador, etc.)
- ➢ Archivo de usuario local

- ✓ **Redes enrutadas**

La arquitectura de PacketFence le permite trabajar a través de redes enrutadas. El servidor puede estar ubicado en el centro de datos y las sucursales pueden acceder de manera eficaz al server.

- ✓ **Implementación gradual**

Debido a la naturaleza intrusiva de control de acceso a la red, PacketFence viene con controles detallados a la hora de la implementación. Puede automáticamente pre-registrarse, pero también puede controlar niveles por switch, por puerto o no; cumpliendo sus funciones. Esto le permite implementar a la velocidad que desee sea por switch, por piso, por ubicación, etc.

- ✓ **Pass-Through (De Paso)**

Puede ser configurado para permitir el acceso a los recursos especificados incluso cuando el nodo está en aislamiento. Esto le permite dar acceso a las herramientas o parches específicos a través del portal cautivo.

- ✓ **De alta disponibilidad**

Se desarrolla con alta disponibilidad. Todos los despliegues se realizan utilizando activo-pasivo de alta disponibilidad, por lo que la solución se ha demostrado en este sentido.

- ✓ **Hardware soportado**

Soporta hardware de varios proveedores de red, y trabaja con estas tecnologías de forma integrada.

- ✓ **Basada en estándares**

Está construido utilizando estándares abiertos para evitar la dependencia de un proveedor. Entre las normas que permite, se encuentran:

- 802.1X
- Protocolo simple de administración de redes (SNMP)

- Gestión estándar de información:
  - SNMP(MIB)
  - BRIDGE-MIB
  - Q-BRIDGE-MIB
  - IF-MIB
  - IEEE8021- PAE-MIB
  - RADIUS Netflow / IPFIX
- Wireless ISP Roaming (WISPR)

✓ **Extensible / Fácilmente personalizable**

PacketFence tiene un par de puntos de extensión donde se puede anular el comportamiento predeterminado con un poco de código Perl. El API se ha diseñado para ser fácil de entender. También, cuando se actualiza, no reemplaza los archivos en los puntos de extensiones, de esta manera se mantiene su configuración libre de las modificaciones en las actualizaciones del paquete. Las plantillas de portal cautivo también son fácilmente personalizables conociendo HTML y CSS.

2.9 COMPARATIVO HERRAMIENTAS NAC.

En el mercado existe multitud de soluciones NAC, debido a los requerimientos para la implementación de presente proyecto, aprovechamiento de la infraestructura de red existente y cero gasto económico se da a conocer una tabla comparativa de tres soluciones NAC, considerando para esto las funcionalidades y el factor económico.

- Solución Comercial "Cisco Clean Access"
- Solución OpenSource "FreeNac"
- Solución OpenSource "PacketFence"

	Políticas Dinámicas	Políticas por puerto	Integración otros fabricantes	Integración Directorio Activo	Soporte Máquinas Virtuales	Edición de módulos e interfaz	Detección de dispositivos	Soporte actualizado	Vlans Dinámicas	Agente	Costo Económico
FreeNAC	√	√	√	√	no	no	no	no	√	no	Cero Dólares
PacketFence	√	√	√	√	√	√	√	√	√	no	Cero Dólares
Cisco	√	no	no	√	√	no	no	√	no	√	> a $ 10000

Tabla 2: Comparativo soluciones NAC

La solución Cisco trabaja con una arquitectura appliance basada en hardware para autenticaciones y para conceder acceso a los dispositivos finales, un agente que recopila los datos en el dispositivo y un gestor para administrar las políticas, esta solución sería recomendable para redes con dispositivos CISCO ya que no presentaría problemas de incompatibilidad con la electrónica de red siendo toda del mismo fabricante. El punto de fallo en esta solución suele ser si tenemos una red dispersa geográficamente necesitamos varios appliance en cada ubicación aumentando más el costo del proyecto. Esta solución basada en hardware podría ser ideal para una entidad bancaria que necesite revisar continuamente el tráfico en la red y conocer que usuarios hacen uso de ella para detectar códigos maliciosos, virus, fallas en la seguridad, etc.

La solución FreeNAC para poder disponer de todas sus opciones deberíamos adquirir una licencia comercial, en esta comparación hemos considerado la versión gratuita. Actualmente esta solución fue publicada bajo licencia GNU Public eliminando la versión comercial, pero siendo su última revisión en junio del 2008 y congelándose el proyecto en el 2010. Esta solución podría ser útil para una pequeña red que no necesita alta disponibilidad, ni una gestión por parte de los administradores de TI, ya que reduce la carga de gestión para equipos de red y nos ofrece un nivel de seguridad alta centrada en los clientes que acceden. Un ejemplo donde implantar esta solución

podría ser una empresa pyme con una red pequeña y que necesite un mínimo de seguridad.

La solución definitiva planteada PacketFence es la que mejor se adapta a nuestras necesidades ya que nos aporta un portal cautivo para identificar los usuarios, no debemos instalar ningún agente en un gran número de equipos desplegados, nos permite configuración de Vlans dinámicas (VMPS), es capaz de detectar el tipo de dispositivo que intenta acceder a la red, integración con detección de intrusos y detección de vulnerabilidades con una inversión en el aplicativo en cero.

En resumen es preciso encontrar un equilibrio entre el coste de la solución y la gestión administrativa, junto al nivel de seguridad deseado para el acceso a nuestra red, es decir equilibrio entre seguridad y usabilidad, Proporcionando mayor seguridad a nivel de trafico de red una solución basada en hardware pero con un alto coste administrativo y económico, mientras que una solución basada en software facilita bastante la gestión administrativa renunciando a un análisis exhaustivo de la red.

CAPÍTULO 3

3.1 ANÁLISIS INFRAESTRUCTURA Y DESCRIPCIÓN DEL PROBLEMA

La Empresa de carácter comercial CH para brindar un mejor servicio a los usuarios de su red local (LAN) y su red extendida cuenta con sistemas y bases de datos que necesitan ser replicadas con frecuencia si no a diario por las características del negocio; estos sistemas utilizan la infraestructura de red para transmisión de toda la información, transacciones comerciales, servicios a todos los locales en el país; además de poseer servicios de correo empresarial, páginas web de servicios de cobro, crédito, compras, marketing; que son actualizadas permanentemente.

En algunas ocasiones la red de la empresa ha sufrido congestión de servicios y en aplicaciones debido al gran número de usuarios que utilizan los sistemas y las aplicaciones, que son de carácter laboral; para mejorar el control y la administración de la institución se desea implementar la tecnología NAC con herramientas OpenSource.

Aunque parece no haber registro de algún ataque externo o interno a los servicios o datos de la empresa nunca está por demás prevenir cualquier problema en el futuro sobre todo cuando se trata de seguridad informática.

La empresa no ha realizado estudios referentes al uso de herramientas de administración y control de la red; la tendencia actual apuntan a que los sistemas de seguridad para redes se constituyen en una parte esencial de la arquitectura de red empresarial, al contar con varias aplicaciones que utilizan servicios de red, hace que su administración sea una pieza clave para garantizar la disponibilidad y el grado de servicio requerido para la red.

En este sentido, se realizará el Análisis e Implementación de Herramientas NAC OpenSource para la administración y control de acceso a la red Lan-Wan, que servirá para controlar y asegurar los dispositivos de red, dando seguimiento a todos los eventos ocurridos en los dispositivos de red, garantizando así la explotación eficiente de los recursos de la institución y así lograr mejorar el servicio.

Para elegir la herramienta NAC OpenSource adecuada se plantea realizar un ambiente de pruebas. Se creerá una VLAN especifica donde se realizará las pruebas de la herramienta en la red de la empresa, los datos tomados serán los más cercanos a la realidad puesto que al tener una VLAN dentro de la red institucional se podrá usar sistemas y equipos propios de la institución, además de utilizar los recursos de la red, sin interferir con el trabajo diario de los empleados.

Actualmente se carece de una forma eficaz de detectar o prevenir fallas de seguridad que puedan ocurrir dentro de la red interna, el fallo se detecta cuando se recibe la notificación de un usuario o por algún control realizado por los administradores del departamento de sistemas; ante esta situación y por la necesidad de detectar y prevenir fallas de seguridad en la red, de forma más rápida y segura surge la necesidad de implementar una solución que prevenga y detecte automáticamente las fallas de seguridad dentro de toda la red y notifique a los administradores las ocurrencias. Esta solución consiste en la instalación de una herramienta que monitoree, identifique problemas y notifique a las personas indicadas para su respectiva solución.

3.1.1 Infraestructura de red de la empresa

La infraestructura de red con la que actualmente cuenta la empresa y que está relacionada con el proyecto se compone de los siguientes elementos.

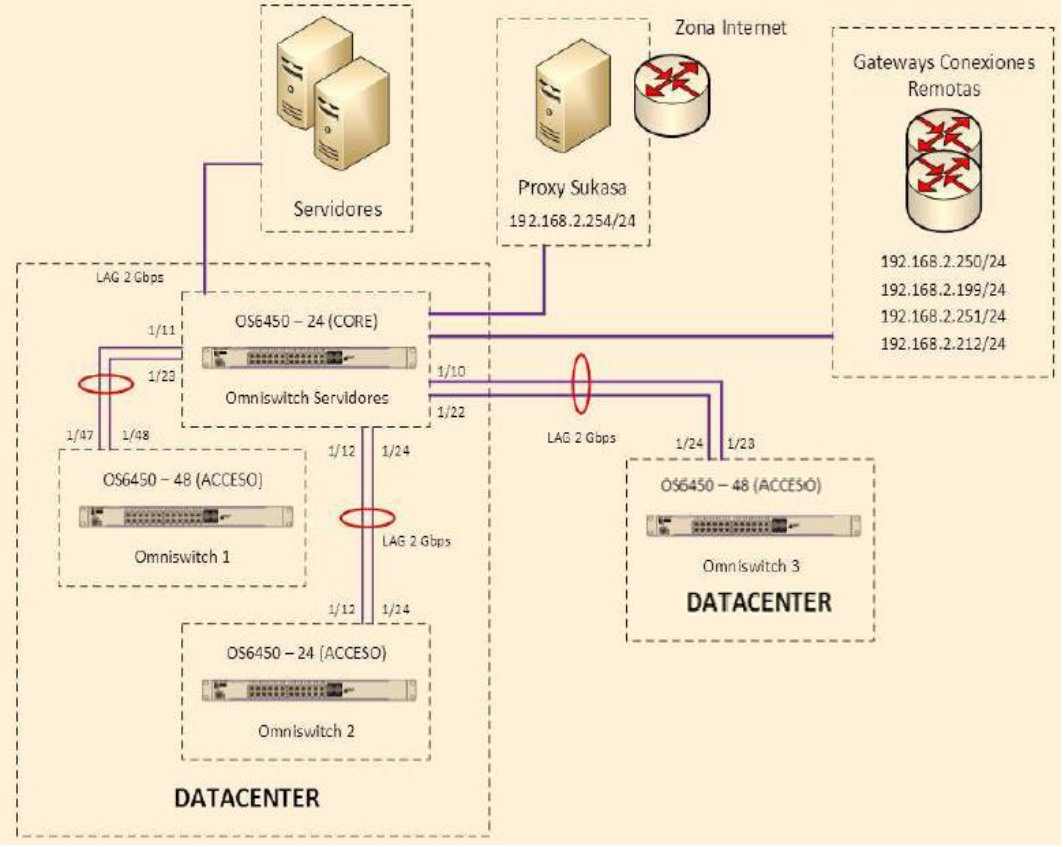


FIGURA 4: Diagrama de red que incluye servidores

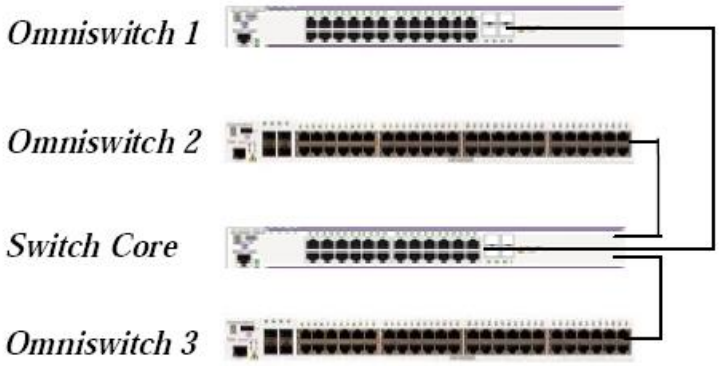


FIGURA 5: Organización de Switchs Empresa

SWITCH	MODELO	VELOCIDAD	FUNCION
Switch Omniswitch 1	6560 de 24 puertos	10/100/1000 Mbps	
Switch Omniswitch 2	6560 de 48 puertos	10/100/1000 Mbps	
Switch Omniswitch 3	6560 de 24 puertos	10/100/1000 Mbps	CORE (Principal)
Switch Omniswitch 4	6560 de 24 puertos	10/100/1000 Mbps	

Tabla 3: Características de Switches Empresa

3.1.2 Características de equipos de Networking

La familia de Switch OmniSwitch 6450 dispone de seguridad integrada, robustez y características mejoradas de OA&M, por lo que resultan ideales para cualquier entorno de red. Productos de Alcatel-Lucent que soportan las funcionalidades del sistema operativo Alcatel-Lucent (AOS) que facilita el despliegue y ofrece funciones ampliadas.

3.1.3 Funciones de seguridad de equipos de networking

- ✓ Auto detección en el control de acceso a la red (NAC) a través del marco de seguridad Access Guardian (IEEE 802.1X, MAC, reglas)
- ✓ Contención y cuarentena automáticas con Alcatel-Lucent OmniVista 2500 NMS Quarantine
- ✓ Manager™ integrado en el OmniVista 2500 NMS
- ✓ Calidad de servicio avanzada (QoS) y listas de control de acceso (ACL) para control del tráfico

3.1.4 Funciones de rendimiento y resistencia

- ✓ Función avanzada de capa 2 con enrutamiento básico de capa 3 para IPv4 e IPv6
- ✓ Interfaces de usuario de triple velocidad (10/100/1000) e interfaces Gigabit Ethernet de fibra (SFP) compatibles con transceptores ópticos 100BASE-X o 1000BASE-X

- ✓ Rendimiento de conmutación y enrutamiento a velocidad de cable
- ✓ Alta disponibilidad con concepto de chasis virtual, enlaces de apilamiento redundantes, recuperación en caso de fallo del módulo principal o secundario, opciones de fuentes de alimentación intercambiables en caliente y rollback de configuraciones.

3.1.5 Rangos de direccionamiento IP de la empresa (Subredes)

La red LAN de la empresa está conformada por varias subredes, distribuidas entre las diferentes dependencias de la institución. Los rangos de las subredes mencionadas son:

	NUM	DEPARTAMENTO	DIR IPs	GTW EN CORE
VLAN	1	Estándar	192.168.2.0/24	192.168.2.250
VLAN	100	Web	192.168.100.0/24	192.168.100.1
VLAN	101	Crédito	192.168.101.0/24	192.168.101.1
VLAN	102	Contabilidad	192.168.102.0/24	192.168.102.1
VLAN	103	Compras	192.168.103.0	192.168.103.1
VLAN	104	RRHH	192.168.104.0	192.168.104.1
VLAN	105	Marketing	192.168.105.0	192.168.105.1
VLAN	106	Sistemas	192.168.106.0	192.168.106.1
VLAN	107	Presidencia	192.168.107.0	192.168.107.1
VLAN	108	Bodega	192.168.108.0	192.168.108.1
VLAN	109	Wireless	192.168.109.0	192.168.109.1
VLAN	110	Servicio Técnico	192.168.110.0	192.168.110.1
VLAN	111	Auditoria	192.168.111.0	192.168.111.1
VLAN	112	Visitantes	192.168.112.0	192.168.112.1

Tabla 4: Direccionamiento IP Empresa

3.1.6 Equipos de la empresa

A continuación se detalla la información de los servidores y routers inalámbricos existentes en la empresa y que se encuentran ubicados en el Data Center a excepción de los routers y conectorizados al switch principal de CORE. (2 Web, 2013)

Equipos	DIRECCION IP	MASCARA
Servidor Proxi y Correo	192.168.2.254	255.255.255.0
Servidor Antivirus	192.168.2.225	255.255.255.0
Servidor IPS	192.168.2.178	255.255.255.0
Servidor de Monitoreo	192.168.2.10	255.255.255.0
Servidor Compras	192.168.2.249	255.255.255.0
Servidor Seg. Ocupacional	192.168.2.9	255.255.255.0
Servidor Bodega	192.168.2.102	255.255.255.0
Servidor Cobranzas	192.168.2.115	255.255.255.0
Servidor Doc Cobranzas	192.168.2.79.5	255.255.255.0
Wireless skbod01 Admin	192.168.2.151	255.255.255.0
Wireless skbod02 Admin	192.168.2.239	255.255.255.0
Wireless skbod03 Bodega	192.168.2.161	255.255.255.0

Tabla 5: Direccionamiento equipos Empresa

3.1.7 Políticas de seguridad de acceso a la red.

Actualmente la empresa cuenta con una política de seguridad de acceso a la red, la cual establece los requisitos que deben cumplir los usuarios para poder conectar un dispositivo a la red, estos requisitos son:

PARAMETRO	PERMITIDO
Sistema operativo	Windows Xp SP3, Win 7 Prof-Standard, Win 8, Dist. LINUX
Antivirus corporativo	Instalado y registrado al servidor
Actualización de Windows	Activadas
DHCP	No activo

Tabla 6: Políticas acceso a la red Empresa

3.1.8 Problemática detectada en la implementación

En la actualidad para controlar el acceso a la red se realiza un proceso manual por parte del departamento de soporte de sistemas y comunicaciones, entre las desventajas que se presentan son las siguientes:

- Mayor riesgo al efectuar una validación manual.
- Incremento horas soporte (HelpDesk) para validar los equipos.
- Únicamente se valida equipos al ingresar por primera vez.
- Dificultad en identificar vulnerabilidades por puertos abiertos.
- Dificultad en identificar aplicaciones no autorizadas.
- Los usuarios que se conectan a la red inalámbrica, mediantes equipos como laptops, tablets, teléfonos inteligentes, presentan otros problemas, ya que estos dispositivos sin gestión, ni control suelen tener problemas de virus informáticos que complican el tráfico en la red, por lo que resulta difícil conocer el estado de seguridad del dispositivo.

3.2 MACROAMBIENTE

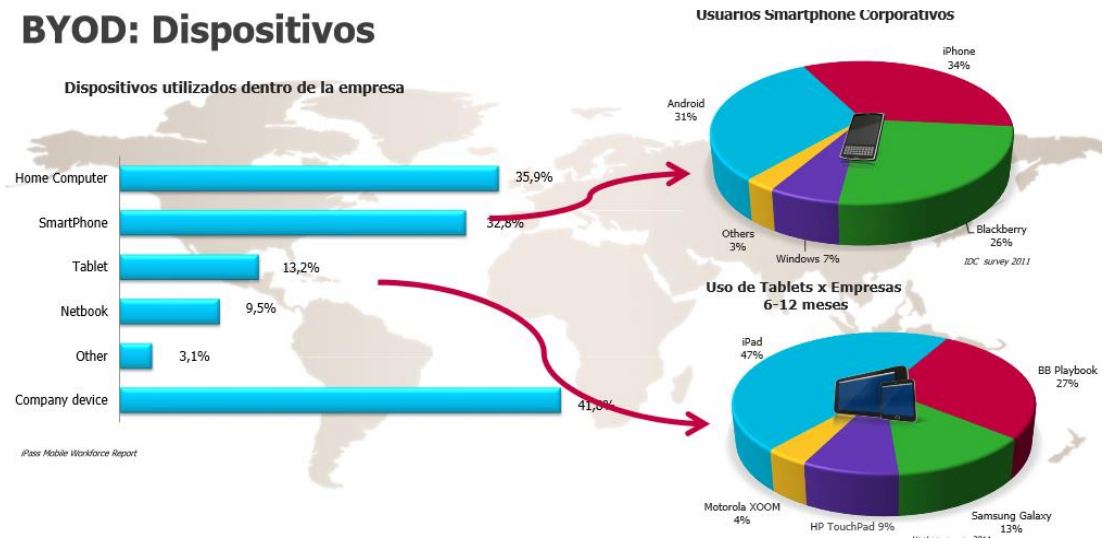


FIGURA 6: Dispositivos utilizados dentro de la empresa

En el Ecuador en los últimos años han aumentado la utilización de equipos electrónicos como teléfonos, tablets, laptops entre otros, los cuales se los utiliza con más frecuencia en el ámbito laboral, dando paso a la falta de seguridad de los sistemas de las empresas, ya que estos equipos electrónicos se conectan a la red sin los debidos controles en acceso, manejo, restricciones de información. Este fenómeno se da mucho en las grandes ciudades como Quito, Guayaquil y Cuenca.

3.3 MICROAMBIENTE

La solución aplicativa propuesta NAC OpenSource, se la aplicará en la empresa de carácter comercial CH, empresa que presta las características, problemática explicada, para su implementación y operación.

3.4 INVESTIGACIÓN BIBLIOGRÁFICA DOCUMENTAL

Según Hugo Cerda (CERDA, 1993) en su texto "Los elementos de la investigación" dice que "la investigación bibliográfica es el procedimiento cuya finalidad es obtener datos e información a partir de documentos y escritos".

A través de esta investigación se realizó una amplia exploración de información y documentos acerca de la utilización de equipos electrónicos en el ámbito laboral, y los temas que vienen relacionados dentro de este, como son la seguridad informática, las redes de autodefensa, control de admisión de red, ataques, defensas, controles en seguridad, características herramientas NAC, herramienta OpenSource PacketFence.

Se exploró de forma profunda lo descrito en la comunidad científica acerca del problema a investigarse; de tal manera que el material obtenido, fue indispensable para el aprendizaje y elaboración del marco teórico.

3.5 MÉTODO CIENTÍFICO

Para esta investigación se va a definir lo que es el método científico deductivo (Rojas, 2006) "El método científico deductivo es el que va de lo general a lo particular."

Dentro de esta investigación se ha planteado este método debido a que primero se analizó el problema general de la utilización de equipos electrónicos en el ámbito laborar y la falta de seguridad que esto genera en los sistemas de las empresas y posteriormente se dará la elaboración de la solución aplicativa NAC con el fin de obtener resultados para dar mejoras de seguridad en los sistemas informáticos de las empresas.

3.6 TÉCNICAS E INSTRUMENTOS

Análisis de datos

- Se realizó encuestas a los empleados de la empresa, con el objetivo de recabar el criterio acerca de las seguridades implementadas en cuanto al acceso a información mediante las redes alámbrica e inalámbrica.
- Tabulación de los resultados obtenidos de las encuestas.
- Análisis de resultados.

3.7 COMPROBACIÓN DE LA HIPÓTESIS

- En la actualidad si es imprescindible el acceso a información de carácter privado y público, cualquiera que sea el sitio o lugar, con el objetivo de acceder a información laboral, comercial, de negocios, tramites en sitios web; que permitan ser más eficientes en tiempo y pro actividad.
- El registro e identificación de usuarios, que acceden a la red empresarial dentro de la base de información del aplicativo propuesto contribuye a la restricción de acceso a información de carácter privado o público.

- Mantener el control de acceso y admisión a los recursos de red de diferentes equipos y tecnología alámbrica e inalámbrica contribuye a la seguridad de la información.

3.7.1 Población y Muestra

La encuesta (**ANEXO**) se la aplicó a todo el personal del departamento de sistemas de la Empresa CH, y al personal de otros departamentos que se encuentra a cargo de las jefaturas, gerencias, personal administrativo, siendo realizadas 20 encuestas en su totalidad.

3.7.2 Determinación de Variables

- Variable Independiente:

  La solución aplicativa NAC (Network Access Control) OpenSource

- Variable Dependiente:

  La administración y control de políticas de seguridad de acceso a red.

3.7.3 Operacionalización de variables

Variable	Concepto	Categoría	Indicadores	Técnicas	Fuentes de verificación
Independiente Herramientas NAC OpenSource	Proporcionar una forma de aplicar políticas de seguridad dentro de la red LAN - Detectar vulnerabilidades en los dispositivos escaneados	Requerimientos de utilización	Herramienta PacketFence Herramienta Snort Herramienta Nessus	Utilización directa Revisión de documentos	Internet Manuales Tutoriales
Dependiente Control de admisión a los recursos críticos de la red	Capacidad de controlar los dispositivos que ingresan a la red LAN		Violaciones de seguridad Vulnerabilidades de los dispositivos finales	Observación Comparación de violaciones y vulnerabilidades	Reportes Gráficos Estadísticos Aplicación de políticas de seguridad

Tabla 7 Operacionalización de variables

3.7.4 Comprobación y análisis de la hipótesis de investigación

H1: Mediante el análisis de la herramienta Network Access Control aplicado a la empresa CH mejorara el control de admisión a los recursos de red.

H0: Mediante el análisis de la herramienta Network Access Control aplicado a la empresa CH no mejorara el control de admisión a los recursos de la red.

3.7.4.1 Nivel de significación

El nivel de significancia, que en este análisis se utilizará es un nivel estadístico de **α = 0.05**, dado que es probable que la herramienta elegida en el análisis para la implementación no se pueda usar en toda la red LAN de la empresa.

3.7.4.2 Criterio

De acuerdo al análisis desarrollado en la presente investigación, se ha seleccionado como estadístico de prueba de hipótesis la técnica *"chi-cuadrado".* La fórmula que da el estadístico es la siguiente:

$$x^2 = \sum_i \frac{(observada_i - esperada_i)^2}{esperada_i}$$

Para conocer las frecuencias teóricas o esperadas, se calculan a través del producto de los totales marginales *(total del renglón x total de columna),* dividido por el número total de casos *(gran total).*

$$\textbf{\textit{fe}} = \frac{\textit{(Total del renglón) * (Total de la columna)}}{\textit{Gran total}}$$

En la *tabla* se pueden observar los resultados de los cálculos, tanto de la frecuencia esperada, como la del valor de " x^2*calculado*", luego de haber aplicado las fórmulas anteriores. Ahora es necesario determinar el criterio de decisión. Entonces se acepta **H0** cuando:

$$x^2 \ calculado < x^2 \ tabla \ ,$$

en caso contrario se rechaza **H0**

Donde el valor de x^2*tabla* representa el valor proporcionado por la tabla de "*distribución* x^2 ", según el nivel de significación elegido y los grados de libertad. El nivel de significancia adoptado para esta investigación es de ***α = 0,05***. Para la determinación de los grados de libertad ***(gl)*** se debe aplicar la siguiente fórmula:

$$\textbf{\textit{gl}} = (r - 1) * (k-1)$$

3.7.4.3 Cálculos

Los resultados de la investigación realizada se resumen en las tablas mostradas a continuación:

FACTIBILIDAD		
Pregunta	**Mejora**	**No mejora**
Pregunta 1	20	0
Pregunta 6	20	0
TOTAL	**40**	**0**

Tabla 8: Resultados de factibilidad

GESTION		
Pregunta	**Mejora**	**No mejora**
Pregunta 2	17	3
Pregunta 5	20	0
TOTAL	**37**	**3**

Tabla 9: Resultados de gestión

SEGURIDAD		
Pregunta	**Mejora**	**No mejora**
Pregunta 3	20	0
Pregunta 4	20	0
TOTAL	**40**	**0**

Tabla 10: Resultados de seguridad

PRODUCTIVIDAD		
Pregunta	**Mejora**	**No mejora**
Pregunta 3	20	0
TOTAL	**20**	**0**

Tabla 11: Resultados de productividad

USABILIDAD		
Pregunta	**Mejora**	**No mejora**
Pregunta 7	18	2
TOTAL	**18**	**2**

Tabla 12: Resultados de usabilidad

La matriz de los resultados obtenidos queda conformada de la siguiente manera:

Herramienta NAC OpenSource	**Control de admisión a los recursos de red**		
	MEJORA	**NO MEJORA**	**TOTAL**
FACTIBILIDAD	40	0	40
GESTION	37	3	40
USABILIDAD	18	2	20
SEGURIDAD	40	0	40
PRODUCTIVIDAD	20	0	20
TOTAL	155	5	160

Tabla 13 Matriz de resultados totales de la encuesta

De la tabla anterior se realiza el cálculo para el grado de libertad.

$$gl = (r - 1) * (k-1);$$

$$gl = (5-1) * (2-1);$$

***gl* =** (4) * (1);

gl = 4 grado de libertad

Consultando la tabla estadística de distribución de *chi-cuadrado*, tomando el *valor de significancia 0,05* y *grado de libertad 4*, el valor

$$x^2 \, tabla = 9.488$$

Herramienta NAC OpenSource	Control de admisión a los recursos de red		
	MEJORA	NO MEJORA	TOTAL
FACTIBILIDAD	37	3	40
GESTION	35	5	40
USABILIDAD	19	1	20
SEGURIDAD	38	2	40
PRODUCTIVIDAD	18	2	20
TOTAL	147	13	160

Tabla 14 Matriz de resultados esperados

Diseñamos la tabla para aplicar la fórmula de chi-cuadrado:

	fo	fe	(fo-fe)² /fe
El aplicativo NAC OpenSource mejora la factibilidad	40	37	0,24
El aplicativo NAC OpenSource mejora la gestión	37	35	0,11
El aplicativo NAC OpenSource mejora la usabilidad	18	19	0,05
El aplicativo NAC OpenSource mejora la seguridad	40	38	0,11
El aplicativo NAC OpenSource mejora la productividad	20	18	0,22
El aplicativo NAC OpenSource no mejora la factibilidad	0	3	3,00
El aplicativo NAC OpenSource no mejora la gestión	3	5	0,80
El aplicativo NAC OpenSource no mejora la usabilidad	2	1	1,00
El aplicativo NAC OpenSource no mejora la seguridad	0	2	2,00
El aplicativo NAC OpenSource no mejora la productividad	0	2	2,00
TOTALES	160	160	**9,54**

Tabla 15 Frecuencia observada sobre frecuencia esperada.

3.7.4.4 Demostración de la hipótesis

Como: x^2 *calculado* **= 9.54** y

x^2 *tabla* **= 9.488**

Entonces: x^2 *calculado* $>$ x^2 *tabla*

Por lo tanto se rechaza la hipótesis **H0** por cuanto x^2 *calculado* está en la zona de rechazo de la hipótesis nula y se acepta la investigación.

Por consiguiente:

Se acepta la hipótesis **H1** que dice, mediante el análisis de la herramienta Network Access Control aplicado a la empresa CH mejorará el control de admisión a los recursos de red.

3.8 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS ENCUESTA

	MEJORA	NO MEJORA
FACTIBILIDAD (%)	100	0
GESTION (%)	92,5	7,5
USABILIDAD (%)	45	5
SEGURIDAD (%)	100	0
PRODUCTIVIDAD (%)	50	0

Tabla 16 Tabla porcentual de resultados encuesta

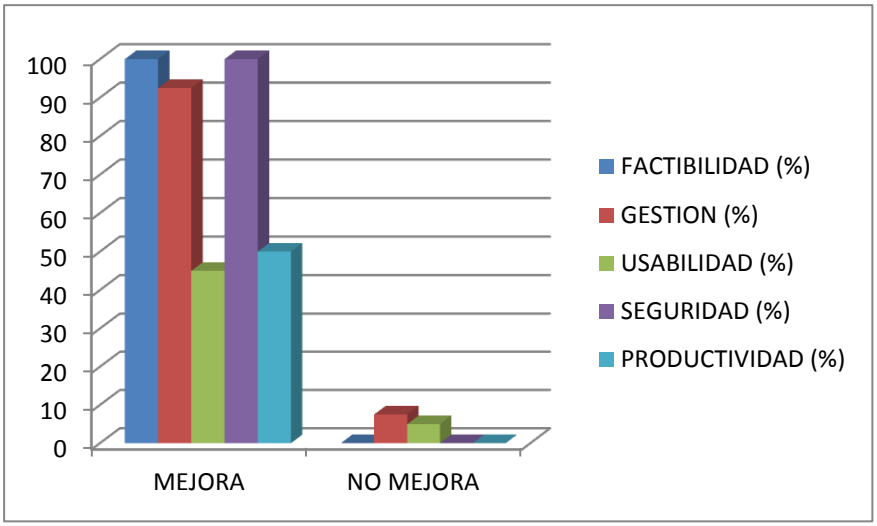


Tabla 17 Tabla estadística de resultados encuesta

Según la información y datos entregados en la encuentra planteada nos entrega los siguientes resultados.

- **MEJORA**: El mayor porcentaje de usuarios entrevistados plantea la respuesta de que toda solución implementada en el departamento de TI servirá como solución a los diferentes inconvenientes experimentados por los usuarios, permitiendo facilidades para las tareas normales y cotidianas en sus actividades.

- **NO MEJORA**: Un mínimo porcentaje informa que no mejora la situación actual de los problemas percibidos a nivel de la red interna, cabe considerar que estas observaciones no necesariamente son problemas inherentes a la solución al paradigma planteado, más bien va por problemas de falta de soporte técnico a problemas varios (Help-Desk) .

3.9 APORTE DE LA PROPUESTA DE INVESTIGACIÓN.

Al culminar el presente trabajo se cumplió principalmente con los objetivos propuestos:

- Se determinó claramente un modelo de políticas de seguridad, que se debe aplicar para asegurar el ambiente de red, estas políticas contribuyeron en la mejora de gestión del estado inicial de la red; solucionando en gran manera los problemas de organización en cuanto a ingreso a la red de nuevos dispositivos, la gestión en la solución a tráfico internos y a la saturación por problemas de virus informáticos y envió de correo electrónico.

- La investigación del aplicativo PacketFence y su integración al ambiente de red permitió mejorar la administración y operación de todos los dispositivos que ingresan en la red, esto implica una monitorización constante de actividades en la red.

- La experiencia ganada en la investigación y estudio de caso permitió entregar un documento que sirve como aporte a los nuevos procesos implementados en la empresa y a nivel educativo como guía para posibles casos a implementar en diferentes instituciones públicas o privadas.

- Según conclusiones expresadas por parte de la directiva de la empresa, el presente trabajo sirve como punto de inicio para posterior implementación, que el mismo aplicativo permitirá integrar y ser aplicado, por cuanto los nuevos servicios que se están entregando en las nuevas versiones del software PacketFence facilitará dar soluciones a otros problemas tecnológicos identificados como riesgos de seguridad que afectaría los servicios de red, importante considerar que el aplicativo es compatible con diferentes marcas de hardware, reduciendo costos de inversión en la implementación del caso.

CAPÍTULO 4

4.1 DESARROLLO DE LA PROPUESTA

Implementar la solución automatizada de control de acceso a la red (NAC). Esta necesidad es debido al continuo aumento de usuarios, visitantes, proveedores externos que necesitan acceso a la red para poder ejecutar sus tareas. Estos usuarios no pueden ser tratados del mismo modo ya que dependiendo del tipo de usuario que solicita el acceso deberá proporcionarse los recursos específicos, ninguno más que no esté permitido y aprobado por parte de la Dirección de Sistemas.

Se tendrá en cuenta las siguientes etapas para implementar la solución:

- ✓ Definición de características técnicas
- ✓ Selección de la solución

4.1.1 Definición de características técnicas

La definición de características técnicas se realiza en base a las necesidades de la empresa, además del aprovechamiento de la infraestructura tecnológica que dispone.

Requerimiento de características técnicas:

- ✓ Autentificación
- ✓ Asignación de políticas de control de tráfico por usuario sin importar el puerto físico o VLan.
- ✓ Capacidad de integrar y auto-configurar switch de la empresa.
- ✓ Autentificación vía servicio Radius
- ✓ Clasificación de usuarios con base a perfiles o políticas aplicadas
- ✓ Soporte de autentificación mediante el protocolo 802.1x
- ✓ Aplicar políticas de control sobre direcciones físicas (MAC)

4.1.2 Selección de la solución

PacketFence es una solución OpenSource con gran apoyo en la comunidad y en continuo desarrollo. Esta solución nos ofrece multitud de funcionalidades. En relación al tema de valor económico ofrece todas sus características y funcionalidades a un costo cero dólares (0 $). También ofrece soporte técnico comercial donde el precio varía dependiendo de la licencia adquirida por la empresa o responsable de implementación.

Teniendo en consideración la infraestructura de la empresa y el proceso manual para integrar y validar a los dispositivos de los usuarios en la red, se propone la solución basada en el aplicativo PacketFence OpenSource que automatice el procedimiento de validación y control de acceso de usuarios y dispositivos de la red.

4.1.3 Fases en el proceso de acceso a la red de la empresa.

- **Detección:** Se realiza por medio de peticiones entre el equipo cliente y el switch de acceso.

- **Autenticación:** De usuarios se realiza a través del protocolo 802.1x, el mismo que se validará en un servidor Radius.

- **Métodos de autentificación:** Los métodos a utilizarse en la fase serán:
    - 802.1x + MAC detection Bypass
    - Dirección MAC si el equipo no es compatible con 802.1X

- **Evaluación:** Para la evaluación de los equipos el servidor PacketFence se encarga de comprobar el rol asignado al usuario, y garantizar los recursos adecuados al cliente. Esta evaluación se realiza verificando que el cliente cumple todos los requisitos de seguridad sin tener que instalar ningún agente en el cliente, una vez evaluada se determinará la política asignada a su rol y la VLan que le corresponde.

- **Autorización:** Se realizará por medio del servidor PacketFence que dependiendo de los resultados obtenidos en la fase anterior se le asignará un rol de privilegios al equipo o usuario. Los perfiles son cuarentena, básico, avanzado.

PERFIL	DESCRIPCION	ROL
Cuarentena	Usuarios que no cumplan la validación	Ingreso a VLan en cuarentena
Básico	Usuarios con antivirus actualizado	Acceso a Internet
Avanzado	Validación completa	Acceso a Internet, Intranet y aplicaciones corp.

Tabla 18: Rol de privilegios de acceso a la red

- **Remediación:** En esta fase los usuarios que han sido trasladados a la VLan de cuarentena se le mostrará un mensaje enviado por el servidor PacketFence con los o el motivo por los que han sido denegado el acceso y las acciones a tomar para poder acceder a la red.

4.1.4 Ambiente de pruebas con la herramienta PacketFence

La herramienta Packetfence se puede administrar mediante una interfaz web. En nuestro ambiente de pruebas la dirección web del servidor es la siguiente https://192.168.10.20:1443/admin. Para ingresar al sitio de administración de la herramienta lo hacemos con el usuario admin y contraseña admin1 (adminsk).

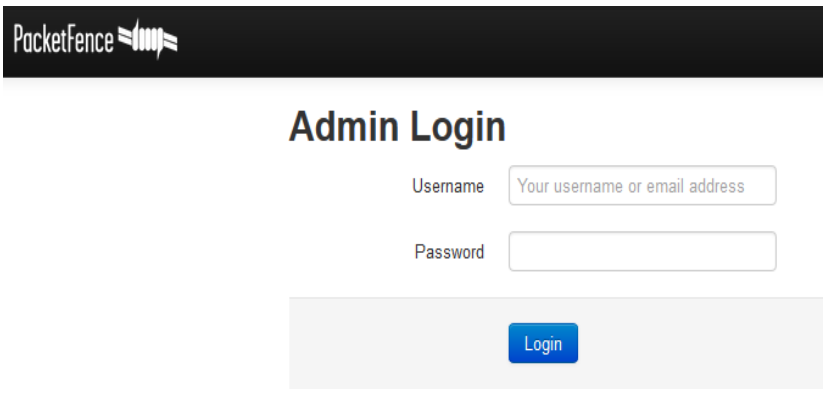


FIGURA 7: Solicitud de login aplicativo PacketFence

4.1.5 Configuración de PacketFence

Una vez iniciado el sistema y conectado el servidor al switch en modo TRUNK accedemos a la configuración de PacketFence, donde definiremos el modo de funcionamiento, las interfaces de red, contraseñas de administración y servicios a ejecutar.

- Primer paso: Seleccionamos el modo de funcionamiento, en nuestro caso probaremos solo el modo; "VLAN Enforcementent" ya que en el despliegue en producción solo aplicaremos la solución a dispositivos gestionables con 802.1x con soporte MAB (Mac Bypass).

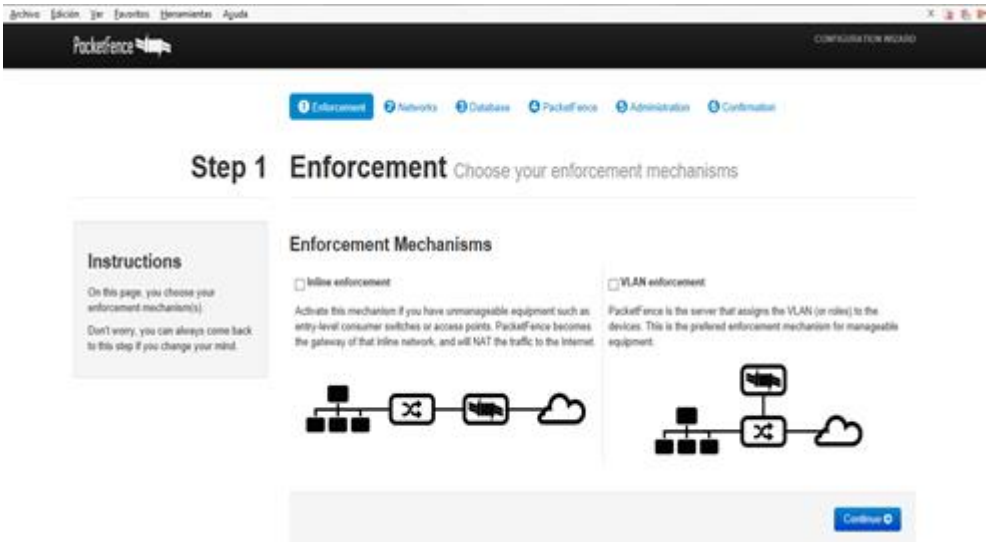


FIGURA 8: Pantalla de inicio PacketFence

- Segundo paso: Definiremos las direcciones de red y las interfaces del sistema donde el DHCP del servidor ofrecerá servicio para los dispositivos que deseen acceder a la red. Aplicaremos la configuración establecida en la tabla descrita a continuación.

Interface	Vlan	Red	Gateway	Descripción
eth0/0		192.168.10.0/24	192.168.10.254	Gestión
eth0/2	2	192.168.2.0/24	192.168.2.254	Registro
eth0/3	3	192.168.3.0/24	192.168.3.254	Cuarentena
eth0/4	4			Detección de MAC
eth0/5	30	192.168.30.10	192.168.30.254	Invitados

Tabla 19: Direccionamiento IPs - Vlans para Roles PacketFence

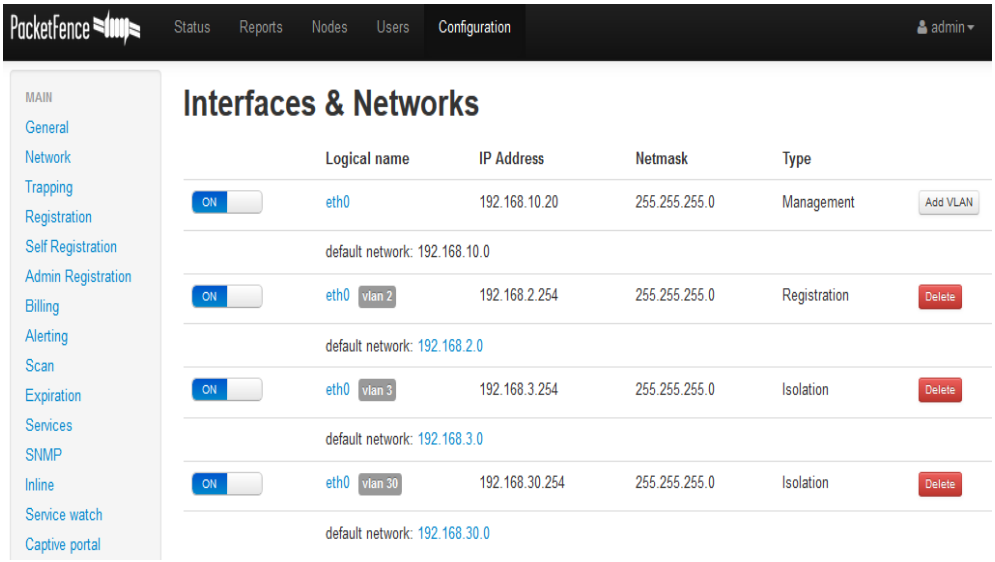


FIGURA 9: Configuración Vlans PacketFence

- Tercer paso: Crearemos el esquema de la base de datos y un usuario para que PacketFence realice conexiones.
- Cuarto paso: Definiremos el nombre del HOST el cual identificara al servidor este será "BYOD" para este caso.
- Quinto paso: Es el último paso, se iniciarán todos los servicios y accederemos a la interface de gestión.

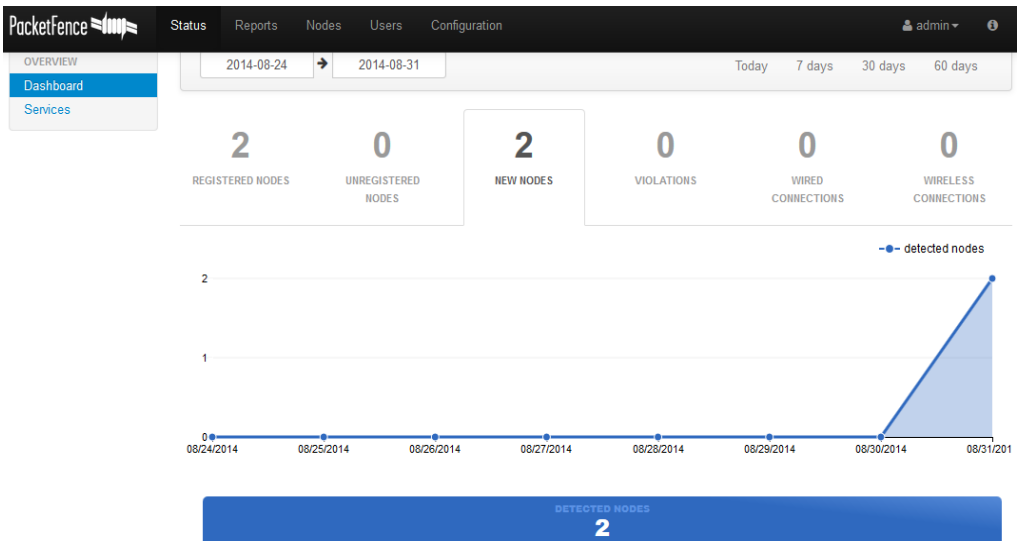


FIGURA 10: Puesta en pre-producción PacketFence

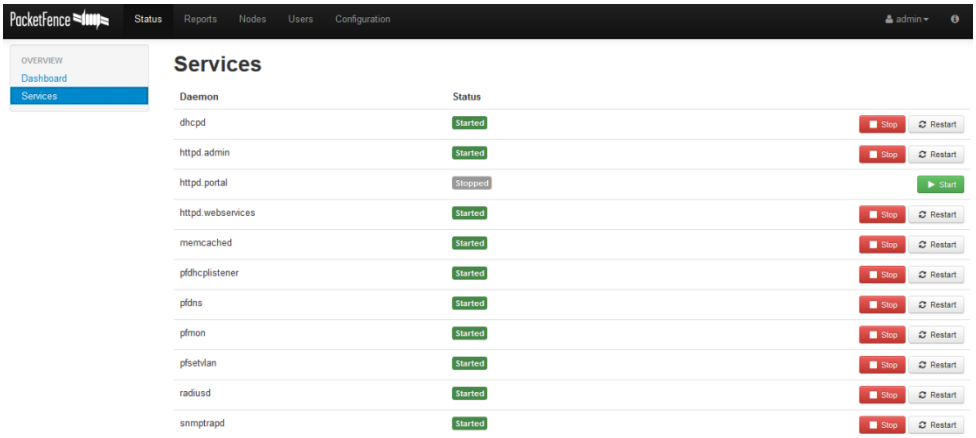


FIGURA 11: Servicios operativos en PacketFence

4.1.6 Puesta en pre-producción

Para la puesta en pre-producción desarrollaremos todas las configuraciones en la red de producción, sin aplicar la configuración a ningún switch de acceso, para esto solicitaríamos autorización y un periodo de tiempo de pruebas. Se creara las Vlans de registro y aislamiento, además de propagación en la infraestructura de red.

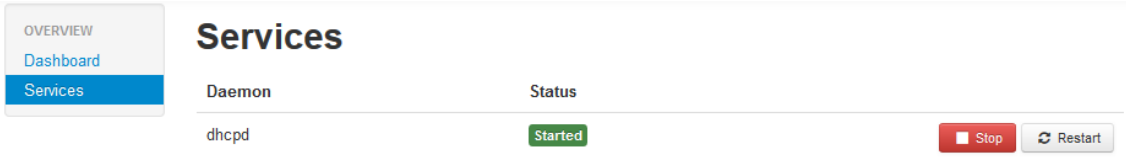
La implementación de autentificación mediante LDAP será de gran interés para facilitar la gestión administrativa de los usuarios, pudiéndose autenticar en el portal cautivo cada usuario que este dado de alta en la Empresa, con esto controlar también los accesos del usuario, en que dispositivos inicia sesión y aplicarle reglas de acceso en el caso que fuese necesario, un ejemplo un consumo excesivo de ancho de banda.

4.1.7 Puesta en producción

Levantamiento y puesta en producción de todos los servicios entre los que se encuentran:

- Dhcpd
- Httpd.admin
- Httpd.portal
- Httpd.webservices
- Iptables
- Memcached
- Pfdhcplistener
- Pfdns
- Pfmon
- Pfsetvlan
- Radiusd
- Snmptrapd

Servicios inicializados y operativos.



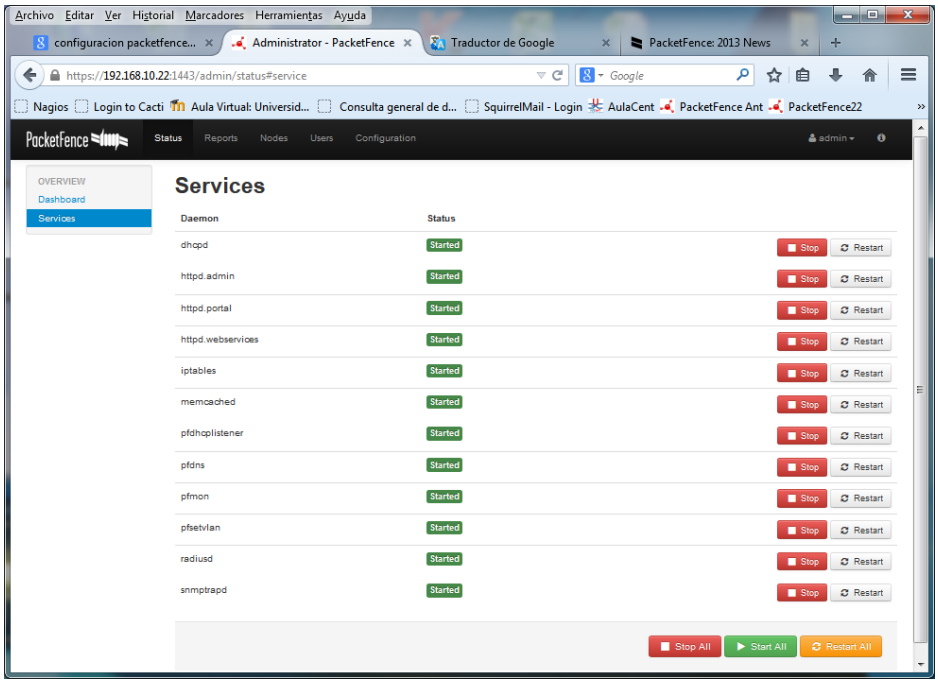


FIGURA 12: Servicios de PacketFence inicializados

4.1.8 Pruebas

Al momento se encuentran registrados 45 estaciones de trabajo (nodes).

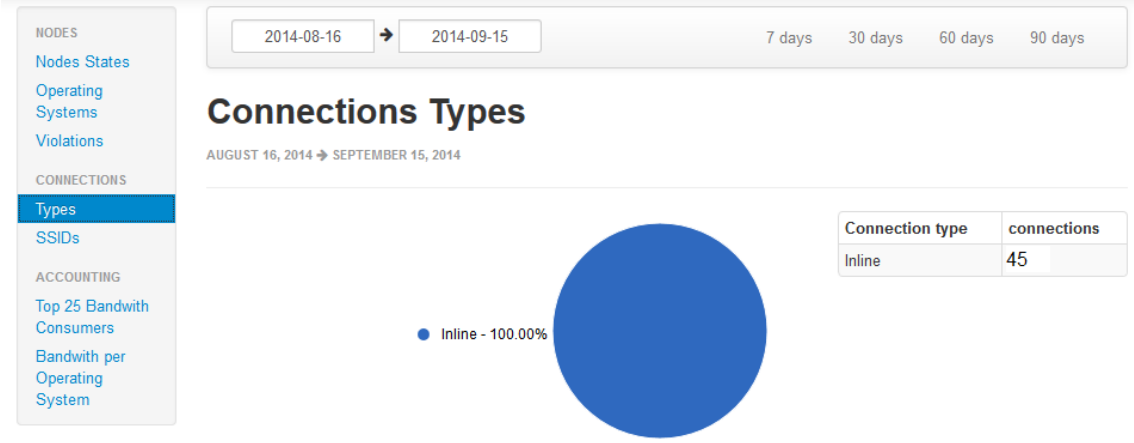


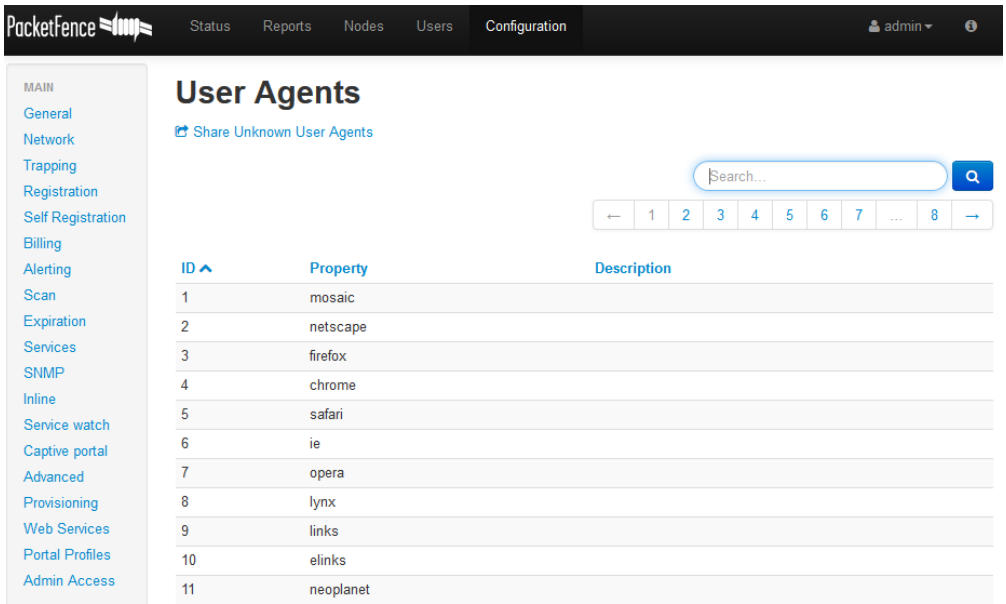
FIGURA 13: Nodes (Pcs) Inline

4.1.9 Resultados obtenidos

Muestra de escaneo de sistemas operativos de equipos (alámbricos e inalámbricos) y/o dispositivos registrados en PacketFence.

ID	OS Class ID	OS Class	Operating System	Fingerprint
100	1	Windows	Microsoft Windows XP (Version 5.1, 5.2)	1,15,3,6,44,46,47,31,33,121,249,43,200
100	1	Windows	Microsoft Windows XP (Version 5.1, 5.2)	1,15,3,6,44,46,47,31,33,249,43
100	1	Windows	Microsoft Windows XP (Version 5.1, 5.2)	1,15,3,6,44,46,47,31,33,249,43,252
100	1	Windows	Microsoft Windows XP (Version 5.1, 5.2)	1,15,3,6,44,46,47,31,33,249,43,252,12
100	1	Windows	Microsoft Windows XP (Version 5.1, 5.2)	15,3,6,44,46,47,31,33,249,43
100	1	Windows	Microsoft Windows XP (Version 5.1, 5.2)	15,3,6,44,46,47,31,33,249,43,252
100	1	Windows	Microsoft Windows XP (Version 5.1, 5.2)	15,3,6,44,46,47,31,33,249,43,252,12
100	1	Windows	Microsoft Windows XP (Version 5.1, 5.2)	28,2,3,15,6,12,44,47
101	1	Windows	Microsoft Windows 2000 (Version 5.0)	1,15,3,6,44,46,47,31,33,43
101	1	Windows	Microsoft Windows 2000 (Version 5.0)	1,15,3,6,44,46,47,31,33,43,252

FIGURA 14: Categorización de sistemas operativos



12	neoplanet2	
13	avantgo	
14	emacs	
15	mozilla	
16	konqueror	
17	r1	
18	netfront	
19	mobile_safari	
20	obigo	
100	device	Any device browser
101	iphone	iPhone
102	ipod	iPod
103	blackberry	BlackBerry
104	kindle	Amazon Kindle

← 1 2 3 4 5 6 7 ... 8 →

FIGURA 15: Agente operativo para detección de software

CAPÍTULO 5

5.1 CONCLUSIONES

- Identificados los problemas de seguridad en la red de la empresa se procedió con la gestión, detección y control de las vulnerabilidades, infracciones y violaciones en la red, entregando solución a cada uno de los casos presentados, permitiendo que la red trabaje bajo parámetros normales, y en este proceso reducir recursos y tiempo hombre en el servicio Help Desk.

- Las características del aplicativo y variedad ampliada de hardware compatible con el mismo, considerando los dispositivos y controladores alámbricos e inalámbricos de diferentes marcas y/o fabricantes, ayudó a disminuir el costo y adquisición de nueva tecnología para la infraestructura de red de la empresa.

- La investigación de la arquitectura y aplicativo, su integración, la experiencia adquirida en el caso de estudio permitió entregar un documento que sirve como aporte inicial para los nuevos y futuros procesos a implementarse en la empresa en la cual se aplicó, documento que también servirá como guía para posibles casos de estudio a nivel educativo y en diferentes instituciones privadas y públicas.

5.2 RECOMENDACIONES

- Actualización e implementación de políticas de seguridad de acuerdo a los nuevos requerimientos existentes siguiendo las normativa para acceso a la red; realizar mantenimiento y gestión de dispositivos con tiempo de caducidad, expiración, detección de infracciones en el uso de los servicios de la infraestructura de red.

- Muy importante la gestión del hardware de la infraestructura de red de la empresa que funciona integradamente con el aplicativo implementado, refiriéndome a la actualización del Firewall-IOS de los dispositivos de comunicación (hardware) según recomendaciones realizadas por el desarrollador del aplicativo, tarea que contribuirá a la seguridad de la red.

- Mantener actualizaciones del aplicativo PacketFence, capacitaciones de uso, controles de información detallada, referente al manejo de nuevos usuarios y dispositivos sin importar el medio de transmisión utilizado para la comunicación dentro de la red de la empresa.

BIBLIOGRAFÍA

2 Web. (14 de Oct de 2013). *Aumento del BYOD obliga a resolver problemas de seguridad en redes corporativas*. Recuperado el mayo de 2014, de Edicion 4113: http://diarioti.com/aumento-del-byod-obliga-a-resolver-problemas-de-seguridad-en-redes-corporativas/69615

Seguridad de la Información. (Julio de 2011). Obtenido de Wikipedia: http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Disponibilidad

4 Web. (2011). *La revista de Finanzas*. Recuperado el Junio de 14, de http://www.finanzasybanca.com/index.php/Apuntes/byod-plantea-un-nuevo-reto-de-seguridad-para-la-empresa.html

6 Web. (Sep de 2013). *La ciberdefensa un reto prioriotario*. Recuperado el Junio de 2014, de http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/137_NECESIDAD_DE_UNA_CONCIENCIA_NACIONAL_DE_CIBERSEGURIDAD_LA_CIBERDEFENSA_UN_RETO_PRIORITARIO.pdf

9 Web. (s.f.). *Descripciones NAC*. Recuperado el Julio de 2014, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28041/8/dgc59fTFC0114Presentaci%C3%B3n.pdf

BYOD Traiga su propio dispositivo (BYOD). (s.f.). Recuperado el Mayo de 2014, de BYOD Traiga su propio dispositivo (BYOD): http://es.flukenetworks.com/expertise/topic/byod

CERDA, H. (1993). Los elementos de la investigación . En H. CERDA, *Los elementos de la investigación* (pág. 439). Quito : ABYA AYALA .

Cerón, D. G. (s.f.). *Implantacion de control de acceso a la red*. Recuperado el Julio de 2014, de Daniel Gutierrez Cerón: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28041/8/dgc59fTFC0114Presentaci%C3%B3n.pdf

CISCO. (s.f.). *CISCO* . Obtenido de CISCO : http://www.cisco.com/web/LA/productos/destacado/nac.html

Defensa, E. d. (2013). Necesidad de una Conciencia Nacional deciberseguridad.

Network, A. (2013). Llevar los dispositivos moviles al trabajo . En A. Network, *Llevar los dispositivos moviles al trabajo* . EEUU.

Network, A. (s.f.). *Aerohive Network*. Recuperado el Junio de 2014, de Llevar los dispositivos móviles personales al trabajo: http://www.aerohive.com/pdfs/international/Aerohive-Whitepaper-BYOD-and-Beyond_Spanish.pdf

Problemas de seguridad en redes corporativas . (s.f.). Obtenido de http://diarioti.com/aumento-del-byod-obliga-a-resolver-problemas-de-seguridad-en-redes-corporativas/69615

Rodriguez, D. (2013). Tendencias, Problemas, Retos y Soluciones para BYOD. En D. Rodriguez, *David Rodriguez* .

Rojas, S. R. (10 de noviembre de 2006). Guia para realizar investigaciones sociales. En S. R. Rojas, *Guia para realizar investigaciones sociales* (pág. 439). México, Bogotá, Colombia: Plaza y Valdez.

Systems, C. (2006). Red de autodefensa de Cisco: sistemas estrategicos para la seguridad de la información . En C. Systems, *Red de autodefensa de Cisco: sistemas estrategicos para la seguridad de la información* . Cisco Systems .

ANEXOS

ANEXO 1: CASO DE ESTUDIO

Nombre de la Empresa: COMERCIALIZADORA HOGAR

Sector: Comercialización de artículos y electrodomésticos para el hogar.

de empleados: 310 aproximadamente

Proyecto: Permitir la conectividad de equipos y dispositivos alámbricos e inalámbricos a la red de la empresa bajo control y administración de políticas de seguridad implementadas con una herramienta de control de acceso a la red NAC.

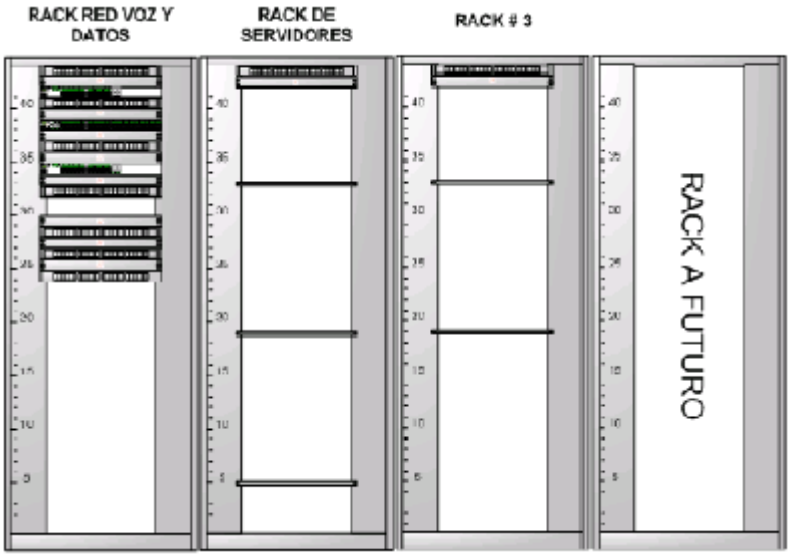
Solución: Implementación de políticas de seguridad en la red de la empresa CH utilizando la herramienta PacketFence.

Resultados: Control, seguimiento, capacidad para administrar el acceso de equipos alámbricos e inalámbricos a la infraestructura de red local y extendida.

INTRODUCCION

La Empresa CH dedicada a la comercialización de todo tipo de artículos, electrodomésticos, equipos para el hogar; con locales comerciales a nivel de todo el país, cuenta con un recurso humano de colaboradores de aproximadamente 330 personas, las mismas que están distribuidas en sus diferentes áreas tanto administrativa, operativa, de comercialización, etc.

Para mantener operativa su infraestructura de red principal ubicada cerca de la ciudad de Sangolquí, mantiene un centro de datos y equipos de networking (switchs, routers), servidores de base de datos, internet, antivirus, IPS, correo electrónico, software en general de servicios administrativos, etc.; en la misma ubicación.



En vista del creciente desarrollo de la empresa se ha visto en la necesidad de tomar acciones con el objeto de controlar la creciente demanda de todos los servicios informáticos a nivel nacional, estos servicios están siendo distribuidos desde matriz hacia cada uno de los puntos de comercialización.

Los servicios prestados por el área informática son diversos, ayudando al correcto flujo de información, permitiendo que toda esta información se actualice oportunamente, manteniendo prioridad en actualización de datos correspondientes a inventarios diarios, ventas de toda la mercadería importada y comercializada. Por esta razón

cuenta con servicios externos de proveedores de transmisión de datos e internet orientados a la conectividad con los diferentes locales comerciales y redes distribuidas.

La seguridad de la infraestructura de red de la empresa es de gran preocupación por cuanto cada día se evidencia nuevos requerimientos de tecnología de información en busca de ser analizados estudiados, y solucionados; con esto afianzar la seguridad confidencialidad e integridad de la información, que demanda el ascendente crecimiento de la empresa y sus diferentes servicios.

Los proveedores de servicios de internet y transmisión de datos no han podido ofrecer mayores características de seguridad para la red interna, refiriéndose a la autentificación de nuevos usuarios, restricciones de acceso a los servidores y su información, tampoco capacidad de personalización de los diferentes servicios de red de las redes distribuidas.

Al momento el personal se puede conectar a la red de trabajo con sus equipos asignados o personales sean estos alámbrico o inalámbrico (desktop, laptop, smartphone) en cualquier momento no existiendo ningún control tampoco seguridad en el acceso a la información de la empresa.

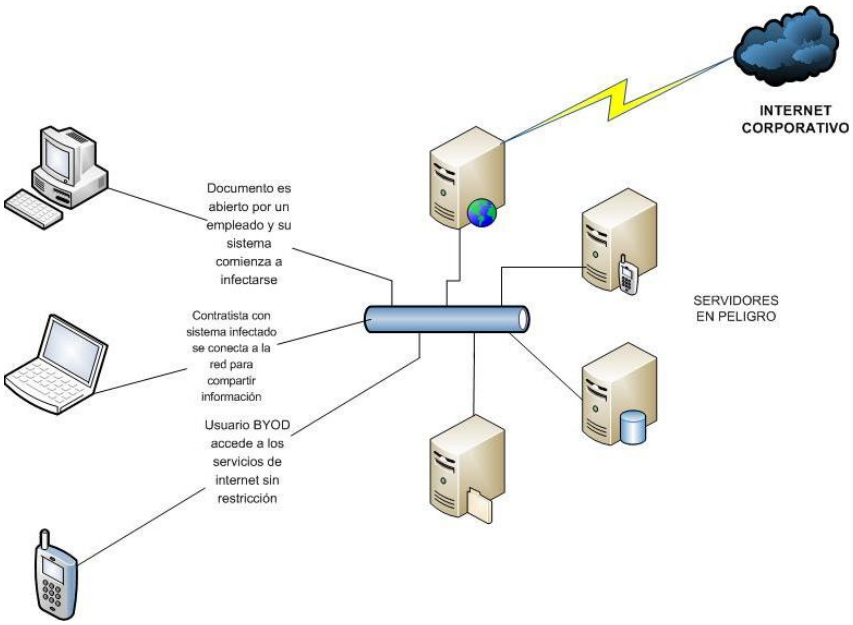
En vista de esta preocupación los directivos han visto la necesidad de buscar una solución al acceso de la información tomando como punto prioritario el control de acceso a la red (Nac), y resguardar la información que circula en la infraestructura de red, para acceso de nuevos usuarios, acceso a personal de nuevos proyectos, segmentación de red por departamentos, personalización de acceso a los diferentes servicios de red; con todo esto busca asegurar la información sensible y posible a ser modificada sin autorización, ocasionando pérdidas de carácter económico a la empresa.

SOLUCION

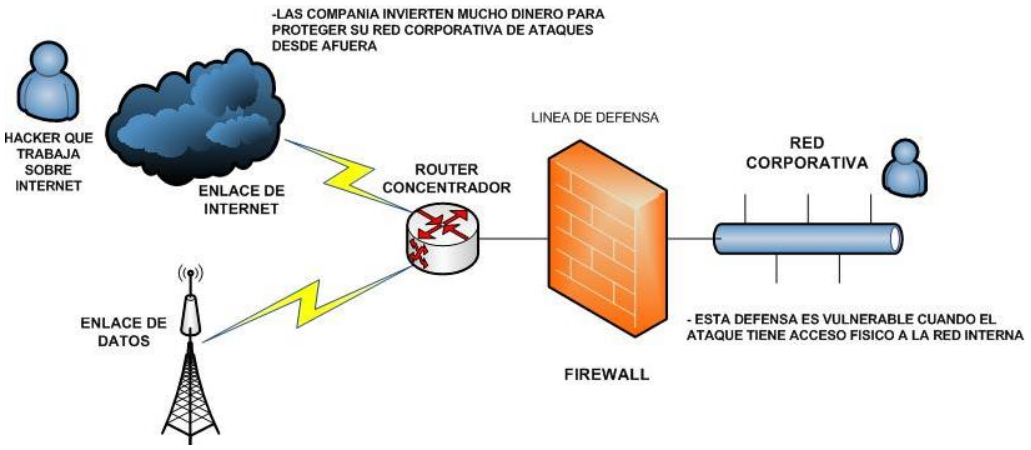
Para subsanar los diferentes problemas se ha tomado la decisión de implementar la herramienta PacketFence aplicativo de uso libre, ayudando a abordar problemas de rendimiento y control en la infraestructura de red.

Los directivos de la empresa han visto con buena expectativa la implementación del aplicativo considerando que.

- Se busca manejar eficientemente clientes en la red.
- Evitar posibles problemas con usuarios que sin control de acceso a la red, presentan problemas de gusanos y virus informáticos.



- Usuarios no autorizados podrían conectarse a la red sin conocimiento y permisos de los administradores de TI desde la red local.



IMPLEMENTANDO PACKETFENCE A LA INFRAESTRUCTURA DE RED

PacketFence es totalmente compatible, solución confiable, con un impresionante conjunto de características incluyendo un portal-cautivo para el registro y la remediación, la gestión centralizada para equipos fijos y móviles, potentes opciones de gestión de BYOD, apoyo 802.1X, el aislamiento a nivel de capa 2 (enlace) de los dispositivos problemáticos; aplicativo que permite asegurar de manera eficaz las redes.

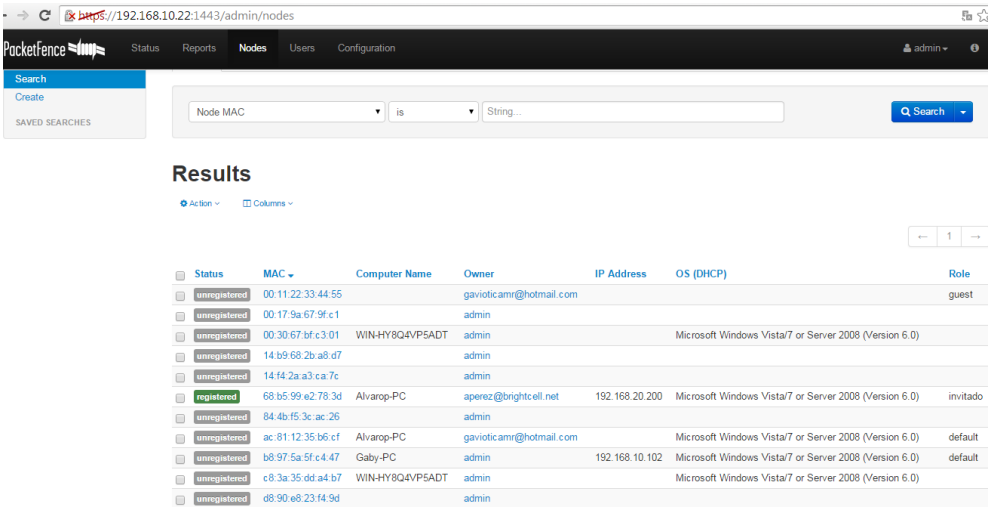
Esta solución de servicio está enfocada en políticas de seguridad automatizadas, previamente planteadas y analizadas, a ser implementadas en cada uno de los departamentos de la empresa, permitiendo el acceso bajo estas políticas a todos los usuarios antiguos y nuevos de la infraestructura de red.

Su función es garantizar la seguridad y estabilidad de la red mediante la personalización y la administración de los diferentes accesos a recursos y permitir tomar control de las diferentes novedades o violaciones de las políticas de seguridad, apoyando a un eficiente flujo de información segura y estable.

FUNCIONAMIENTO DEL PORTAL CAUTIVO

La identificación se realiza a través de un interface web; el ingreso a la red se la programa luego del registro del dispositivo, en caso determina o detecta alguna violación es re-direccionado a un URL que le informa del problema y da a conocer instrucciones para remediar la situación.

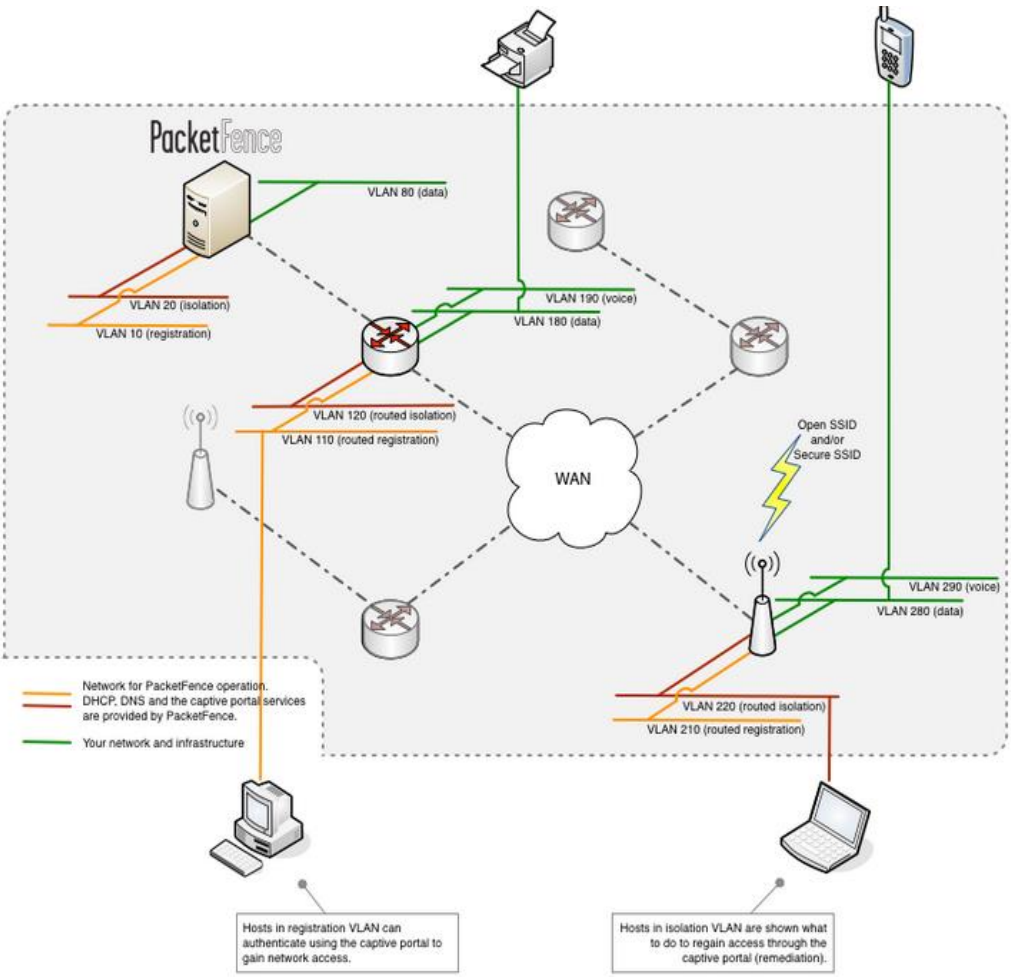
Son identificados en la red usuarios registrados y no-registrados, la pantalla del aplicativo a continuación informa el estado del dispositivo, la MAC address, nombre del dispositivo, tipo de usuario o patrocinador, dirección IP, tipo de sistema operativo características imprescindibles para la administración.



Para el acceso por primera vez a la red el servidor solicita datos informativos del usuario (nombre, dirección de correo electrónico, teléfono, etc.); para el permiso solicitado de acceso a la red el servidor informará que se ha enviado un mail a la dirección de correo registrada, solicita confirmar la información y posterior recibir un nombre de usuario y contraseña.

Características de funcionamiento de portal cautivo

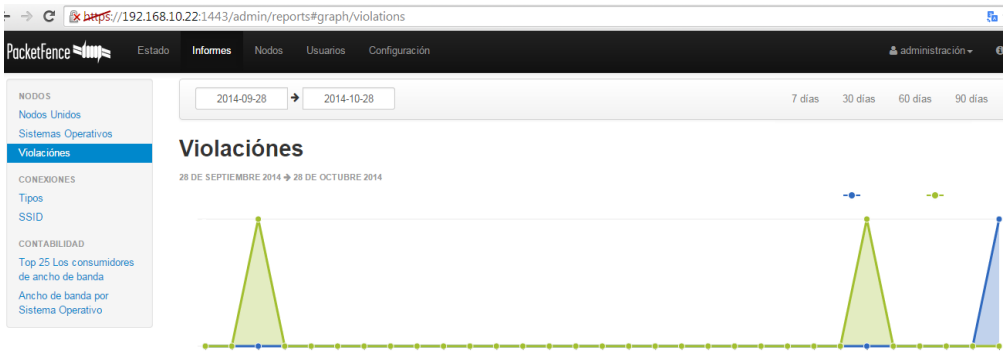
- Soporta varias técnicas de aislamiento, como el aislamiento a grupos de vlan o áreas segmentadas de red de trabajo.
- Actividades de red anómalas pueden ser detectadas utilizando un conjunto de acciones configuradas para cada violación, estas pueden ser problemas de virus informáticos, tráfico negado por las políticas establecidas, exploración de vulnerabilidades como parches del sistema operativo; en definitiva puede realizar una evaluación completa del dispositivo de conexión utilizando la declaración TNC de protocolo de salud.



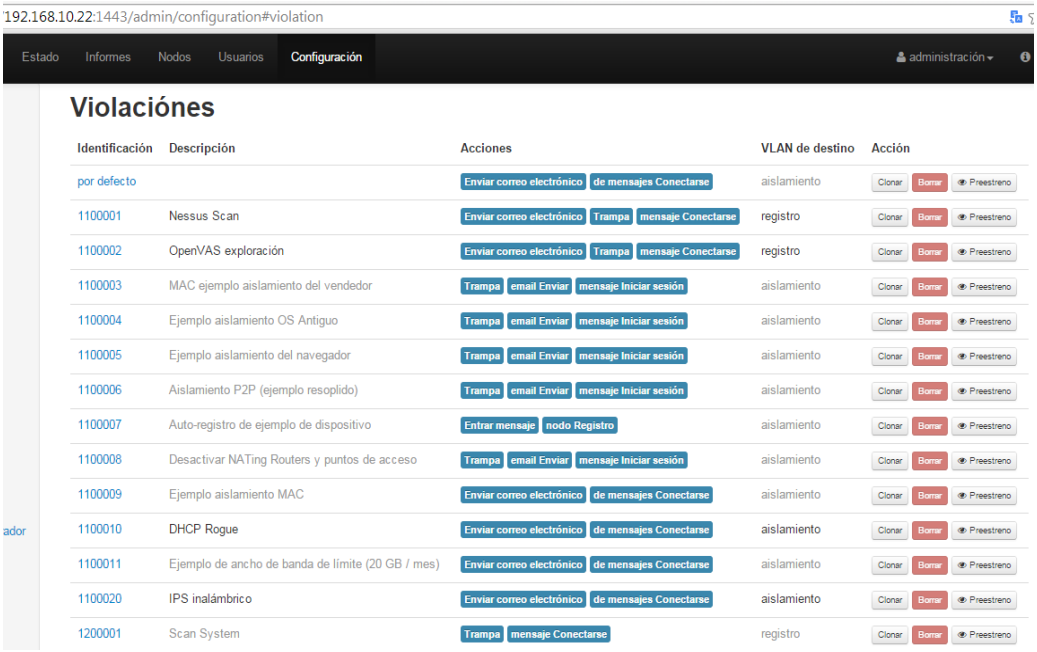
Como son autenticados los usuarios en la red.

- El usuario se conecta a la red corporativa, pero su sistema operativo es vulnerable.
- Su autenticación es validada, el sistema de control escanea el dispositivo que se conecta y encuentra que el sistema operativo es vulnerable, por infección de virus informáticos o falta de parches del sistema operativo.
- Esta vulnerabilidad es chequeada por el aplicativo y las políticas de seguridad y control.
- Si no cumple con lo estipulado sus credenciales no son aceptadas, por lo que su acceso no es otorgado y se lo re-direcciona a una zona (cuarentena) preparada para solucionar su situación, adicionalmente el aplicativo lo envía al portal cautivo donde se le informa al respecto y la posible remediación.
- El sistema es re-direccionado a un servidor de remediación, el mismo que actualiza el sistema operativo haciendo que el dispositivo cumpla las políticas.
- El dispositivo es nuevamente chequeado y ya remediado se le otorga las credenciales de acceso y el respectivo registro en el aplicativo.

El aplicativo muestra pantallas de reportes de violaciones e ingresos no autorizados a la red, información importante para tomar control de los posibles accesos no autorizados,



Diferentes tipos de violaciones y mensajes enviados para informar al cliente y procedimiento a seguir para su registro en el sistema.



RESULTADOS

La personalización del aplicativo ha logrado reducir el esfuerzo administrativo y el soporte Help Desk en cuanto a costos y esfuerzos costo-hombre del departamento de tecnología de información, con la ayuda de las diferentes características del aplicativo Nac como son:

- ✓ Autentificación e identificación de acceso a la red
- ✓ Cumpliendo la política de acceso, impidiendo o aislando a aquellos no permitidos
- ✓ Identificando a usuarios que no cumplan con las políticas de seguridad establecida
- ✓ Eliminando o mitigando las vulnerabilidades detectadas.

La organización de la infraestructura de red, y el acceso a nuevos equipos se establece con mayor control una vez implementado las políticas formales, permitiendo en gran manera facilitar el acceso de todo tipo de equipos fijos o móviles, esto en la actualidad ya no representa un problema de seguridad por cuanto los equipos son direccionados ha Vlans o redes segmentadas con carácter de invitados, donde se acoplan a las políticas automáticas de seguridad implementadas con anterioridad, las correspondientes Vlans son totalmente separadas de la red de datos a nivel de capa 3, todos los dispositivos deben ser registrados con el uso de su MAC Address o dirección física e ingreso al segmento de red correspondiente posterior a la autenticación.

El aplicativo ha logrado mejorar el rendimiento en mención de la productividad y acceso a la información a los servidores, y la creciente cantidad de usuario que necesitan el acceso u salida a Internet corporativo y sus diferentes servicios. Cabe recalcar que se ha logrado mejorar el rendimiento de los canales de comunicación evitando la saturación de los enlaces de datos punto a punto (PaP) y punto a multipunto (PmP) de los diferentes locales comerciales por los que se transmite servicios de acceso a los servidores y Internet distribuido, permitiendo un ahorro económico importante, y manteniendo canales libres para uso de transmisión de voz IP con la implementación de QoS en los mismos canales.

De positiva y mucha importancia para la empresa, el mejorar los retardos en el acceso a los recursos de red siendo estos más eficientes, mejorando los tiempos de respuesta a los servidores por lo que se ha evitado saturación de determinados canales por el consumo excesivo de internet por parte de usuarios no autorizados. Mejora sustentable del acceso remoto a las diferentes estaciones de trabajo para controlar entregar el debido soporte técnico help desk.

CONCLUSIONES

- La elección de una alternativa o aplicativo de código abierto es una solución que en general es aplicada en pymes y medianas empresas pero no tiene buena aceptación en grandes empresas, ya que se requiere cumplir y adoptar tecnologías provistas por partners tecnológicos y no tener que lidiar con soluciones en las que tengan que invertir horas en personal de TI o sus equipos de desarrollo; la adopción de un aplicativo con código abierto es mucho más complicada, ya que de una u otra manera la comunicación y soporte a problemas o errores de código es menos eficiente.
- Independientemente de lo antes expresado toda organización debe considerar que es imprescindible contar con un control de acceso a la infraestructura de red tanto externa como interna que cumpla políticas de acceso de usuarios y dispositivos.

PASOS FUTUROS

Ampliación de nuevas características permitidas en versiones superiores por el aplicativo Packetfence buscando mejorar y corrección de errores, añadir soporte para el firewall Barracuda, una nueva fuente de autentificación basada en Backhole, etc.

Implementación de nuevo aplicativo opensource para la entrega de estadísticas, monitoreo, comportamiento de los enlaces, permitiendo entregar información estadística de calidad de servicio SLA, con esto exigir a los proveedores se cumpla con las normativas de servicio al cliente, normativa que está bajo control de la Superintendencia de Telecomunicaciones-Supertel entidad que controla los servicios de telecomunicaciones en el país.

ANEXO 2: MANUAL DE USUARIO

Introducción

En el documento se detalla información de cómo los usuarios pueden autentificarse para acceder a la red de la institución considerando que la seguridad está siendo controlada por el aplicativo PacketFence NAC.

Para la autenticación se utiliza la herramienta PacketFence proceso de implementación que se detalló en documentos anteriores e incluidos en el CD de instaladores y documentación. Para lo indicado utilizaremos un nombre de usuario y contraseña, de esta manera tendríamos acceso mediante el aplicativo a la red de la institución.

El presente manual es apoyo para que los usuarios puedan acceder mediante la herramienta NAC, facilitando la configuración básica de nuevos o antiguos usuarios que no están familiarizados con el aplicativo con el acceso.

Objetivos

- ✓ Dar a conocer como configurar los equipos para permitir el acceso por intermedio de PacketFence.
- ✓ Servir como guía para el proceso de autenticación y registro de usuarios en el aplicativo.

Dirigido a

Todo el personal administrativo, directivos, usuario final, invitados, personal temporal, que están interactuando en la empresa para acceso a información pública y privada, cabe recalcar que el aplicativo toma control de todos los usuarios que ingresan a la red bajo las políticas de seguridad y control planteadas inicialmente.

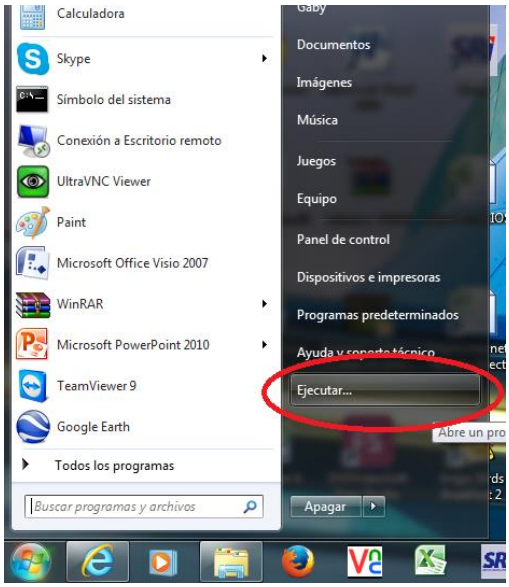
Especificaciones técnicas

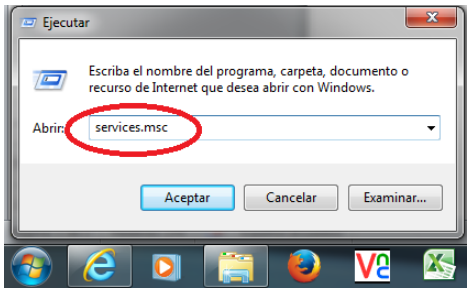
Para el acceso mediante el aplicativo PacketFence a la infraestructura de red de la empresa se debe considerar las siguientes instrucciones:

Se requiere seguir los siguientes pasos:

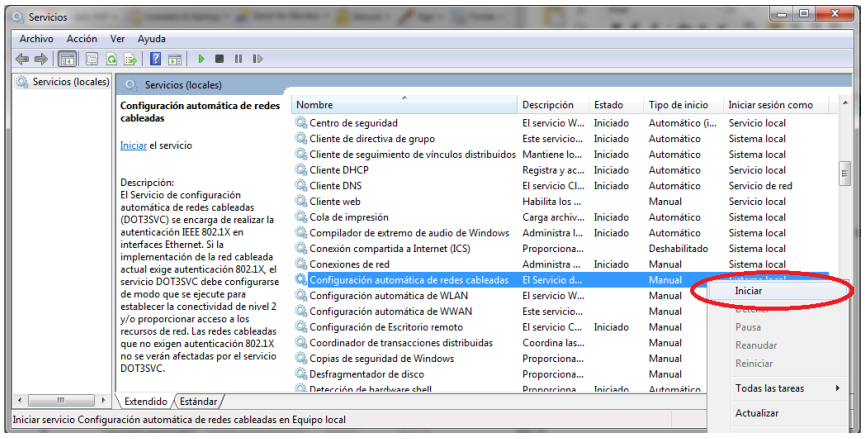
- **Habilitar 802.1x para redes cableadas**

Paso 1: Iniciar sesión como administrador. Clic en el botón inicio, opción ejecutar, e ingresar el siguiente comando services.msc.

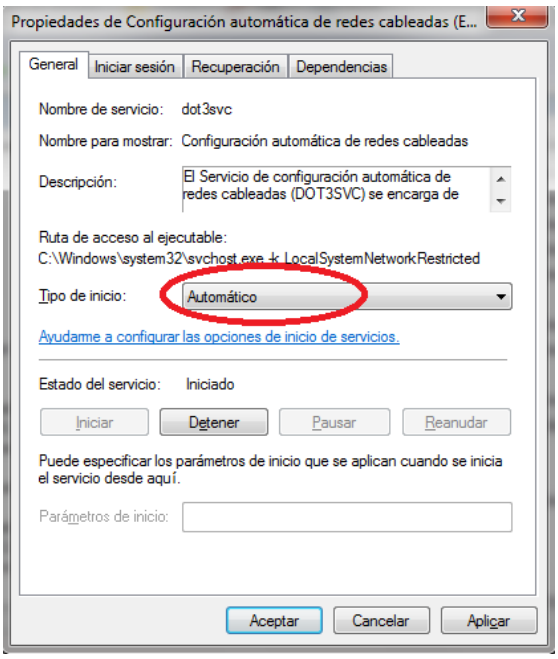




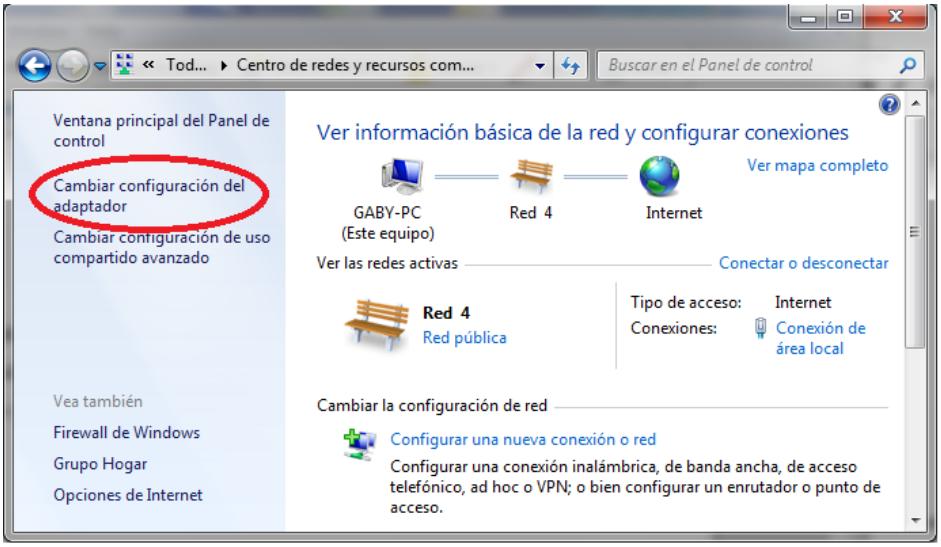
A continuación observamos la lista de servicio locales, habilitar el servicio "configuración automática de redes cableadas", hacer clic en iniciar.



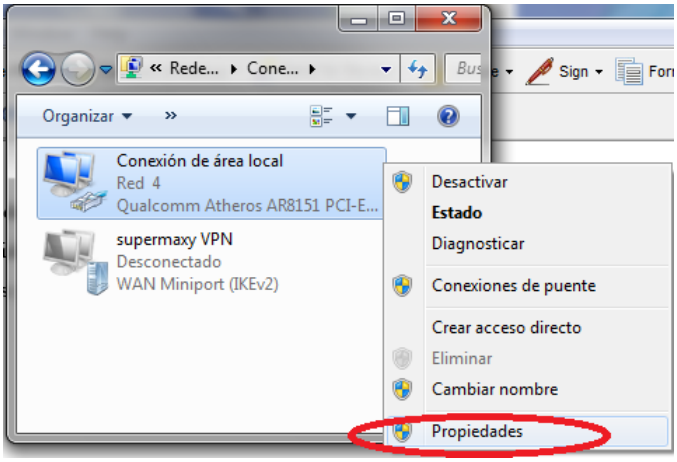
Clic derecho en propiedades y cambiamos en tipo de inicio "automático", aceptamos los cambios.



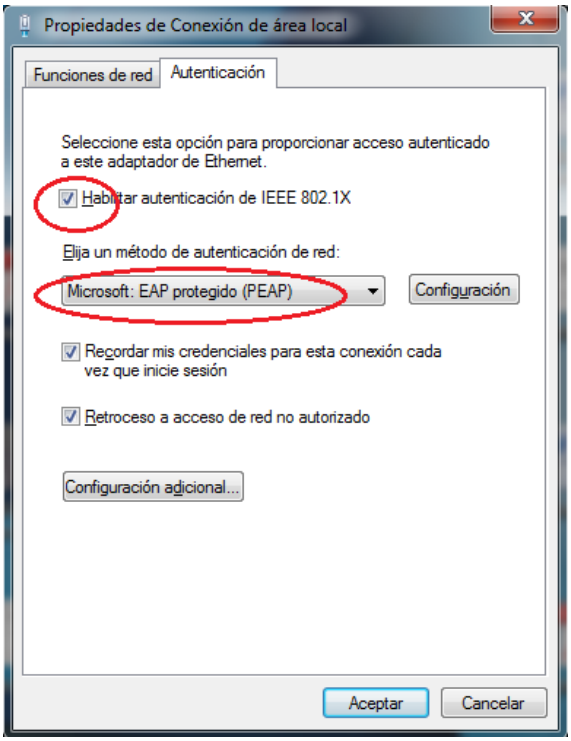
Paso 2: Para abrir la conexión de red, clic en "panel de control" - "centro de redes y recursos compartidos", clic en la opción cambiar configuración del adaptador.



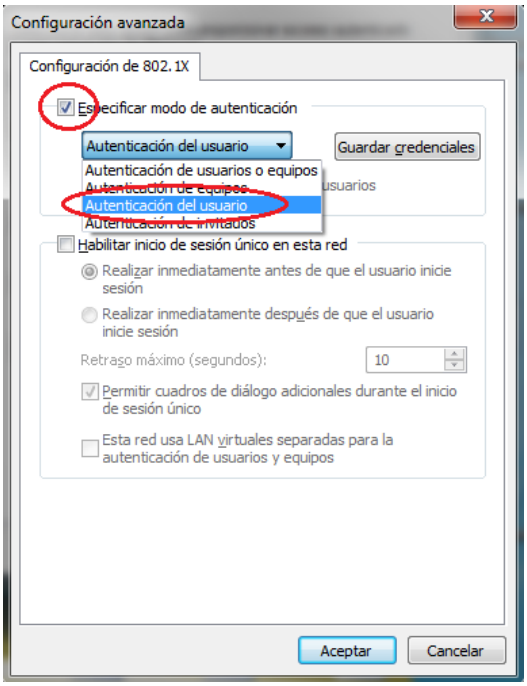
A continuación observamos los adaptadores de red, escogemos el adaptador correspondiente, clic derecho en "propiedades".



Se observa la ventana de propiedades del adaptador correspondiente, clic izquierdo en la pantalla de "autenticación". En la pestaña indicada habilitar la opción de "habilitar autenticación de IEEE 802.1X", en el método de autenticación de red se configura "Microsoft EAP protegido (PEAP)"

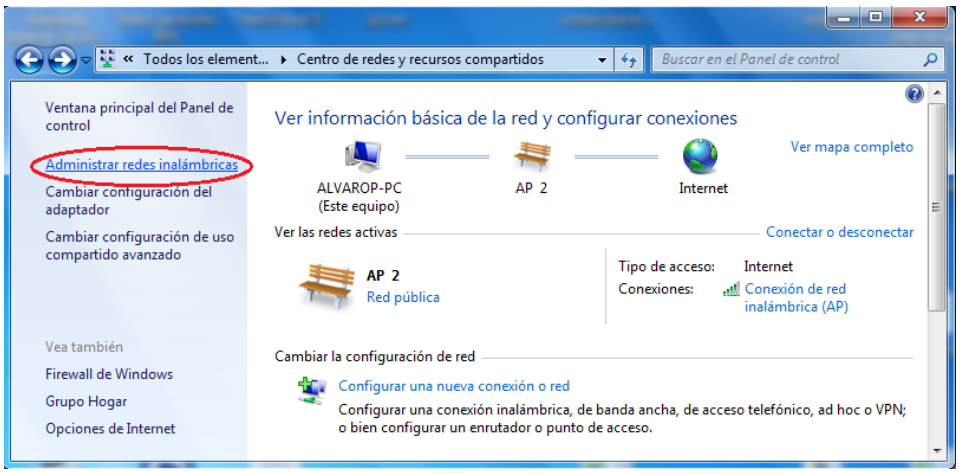


Para habilitar opciones adicionales, dar clic en "configuración adicional", habilitar la casilla "especificar modo de autenticación" elegir "autenticación del usuario", aceptar los cambios.

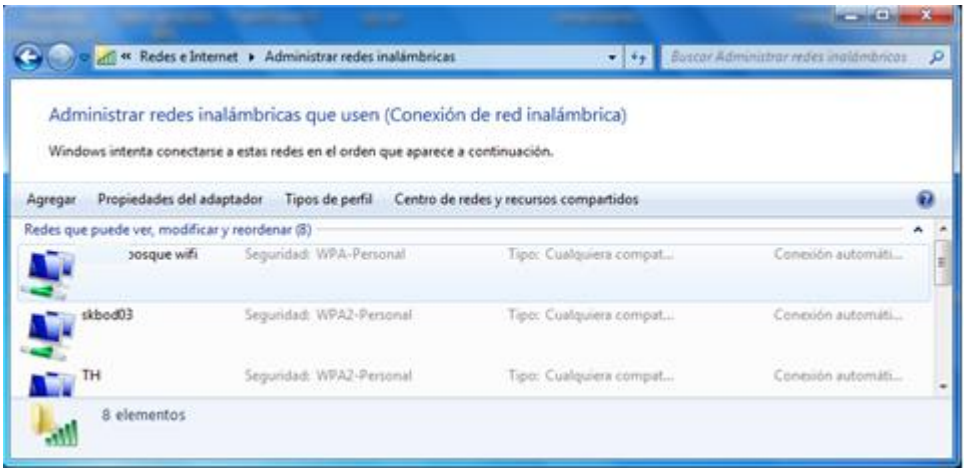


- **Habilitar 802.1x en una red inalámbrica.**

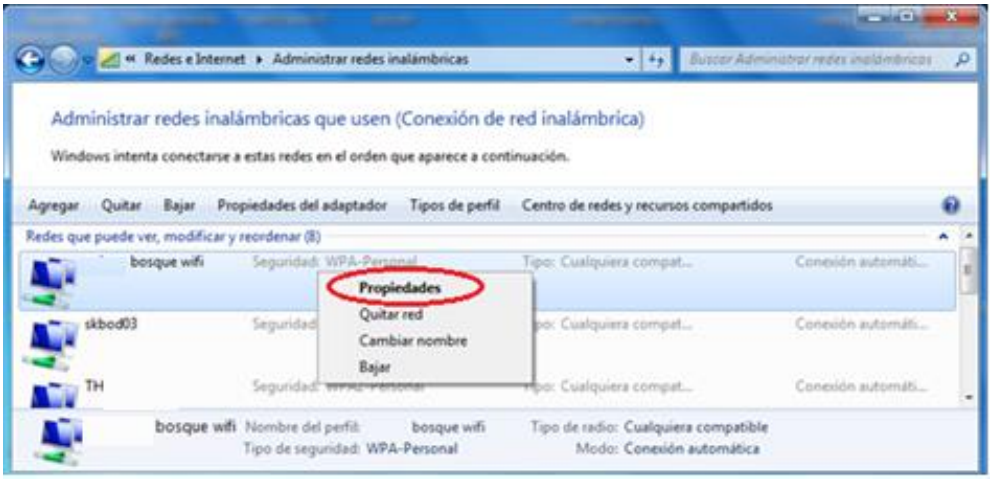
Paso 1: Para abrir la conexión de red, clic en "panel de control" - "centro de redes y recursos compartidos", clic en la opción "Administrar redes inalámbricas".



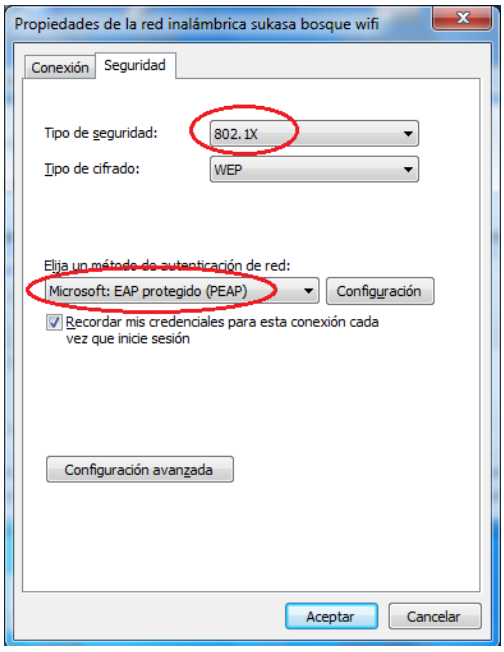
La ventana a continuacion muestra el listado de las redes inalambricas disponibles.

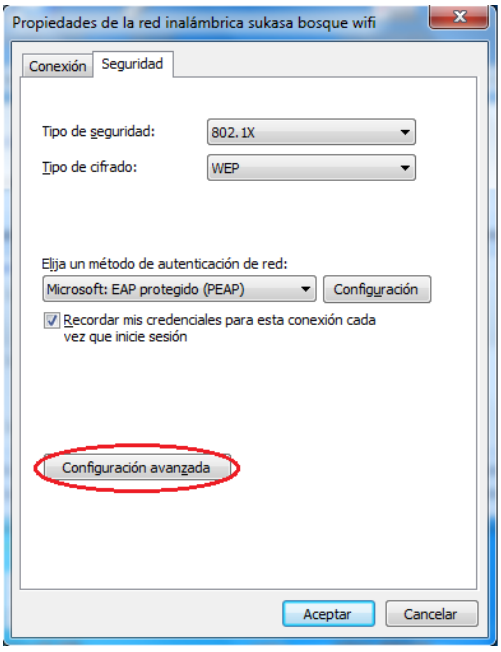


Escoger la red correspondiente en este caso la red de CH es "bosque Wifi ". Posterior clic derecho en propiedades, escoger la pestaña seguridad.

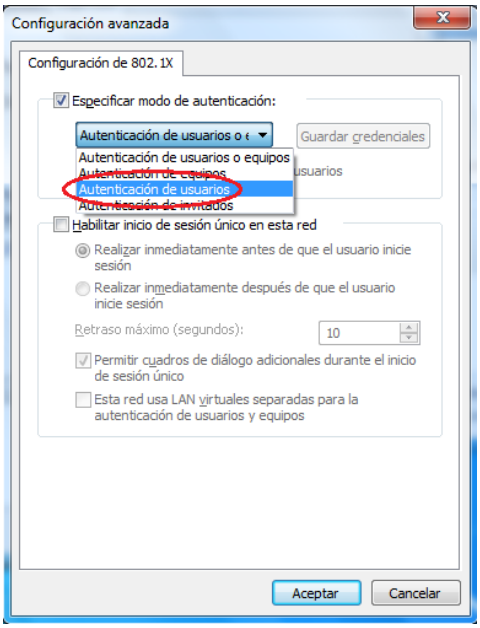


Hacer clic en tipo de seguridad "802.1X", elegir el metodo de autenticacion "Microsoft: EAP protegido (PEAP)"





Clic en "configuracion avanzada" habilitar la casilla "especificar modo de autenticacion" escoger "autenticacion de usuarios".

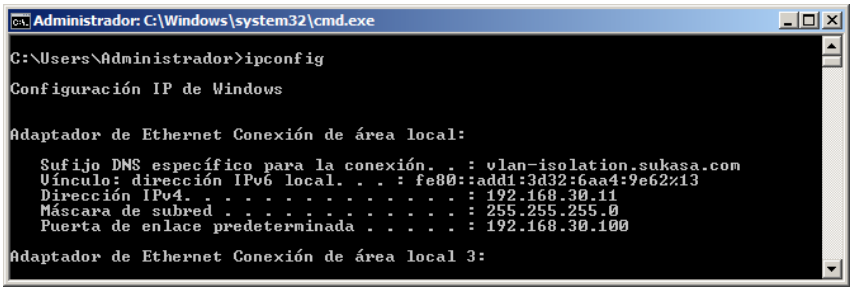


aceptar los cambios y podemos observar que la red escogida se encuentra habilitada la seguriudad de utenticacion 802.1X.

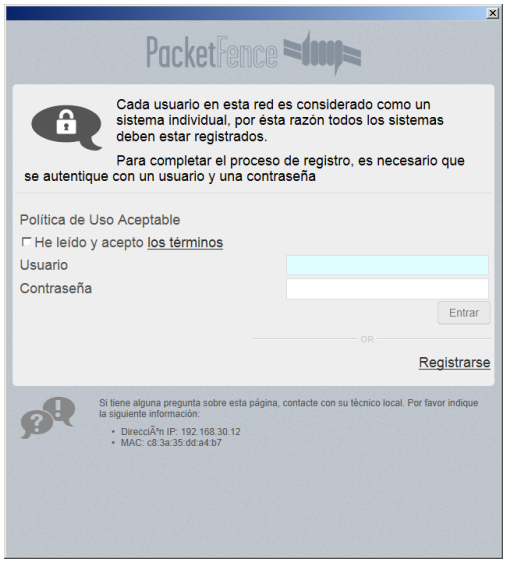
Registro de usuarios en la infraestructura de red

La identificación se realiza a través de la interface web mediante la utilización de navegadores (IE, Firefox, Google Chome), si un nuevo usuario requiere ingresar a la red deberá conectarse vía cableado o servicio inalámbrico, desde cualquier punto de acceso a la infraestructura de red.

Dentro de la red automáticamente será detectado por el servidor PacketFence y asignado a la Vlan de aislamiento (direccionamiento DHCP), la misma que validará el registro inicial, donde se re-direcciona al URL que le informa y solicita dados iniciales de identificación e instrucciones adicionales.



La pantalla a continuación nos informa: Cada usuario en la red es considerado como un sistema individual, por esta razón todos los sistemas deben estar registrados. Para completar el proceso de registro, es necesario que se autentifique con un usuario y contraseña. A continuación deberá aceptar las políticas e ingresar el usuario y contraseña.



Si el usuario se ha registrado previamente o con anterioridad deberá ingresa sus datos de identificación (usuario / password), de lo contrario continuar con el registro y solicitar las autorizaciones necesarios mediante las siguientes instrucciones.

- Registro mediante Sponsor o patrocinador
- Registro mediante uso de código de acceso enviado por correo electrónico
- Registro mediante envió de mensajes SMS

El registro mediante sponsor o patrocinador es provisto para la conveniencia de invitados y visitantes, el acceso no implica ninguna garantía de confiabilidad, velocidad en el servicio de transmisión de datos, o privacidad de información, la red esta provista para el propósito expreso de facilitar la comunicación hacia internet.

Si elige tener un acceso por promotor el sistema envía un mail a la dirección de correo electrónico del patrocinador, el mismo que tendrá que hacer clic en el enlace de confirmación enviado al mail y autenticarse con su usuario y password (sponsor) con el fin de aprobarlo. Mientras tanto el nuevo usuario se encuentra en zona de espera.

Para el acceso por este medio deberá registrar sus datos personales como son: nombre, apellido, empresa, número de teléfono, correo electrónico, correo electrónico del patrocinador (previamente registrado en el sistema) y aceptar las políticas de uso.

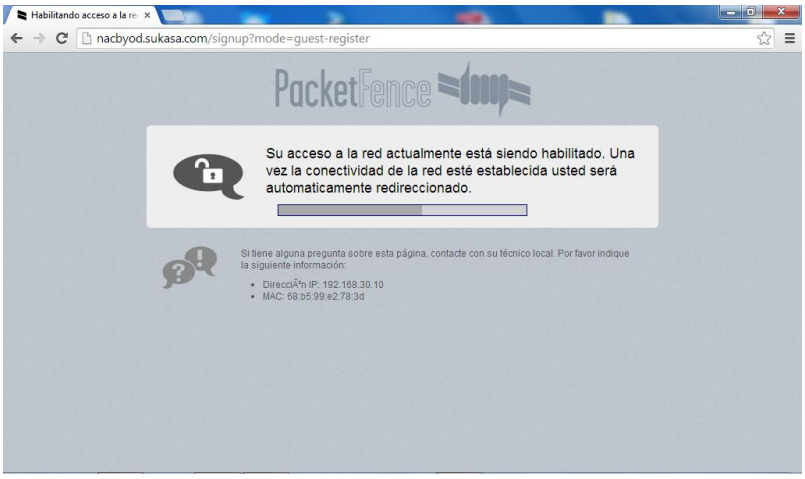
El registro mediante uso de código de acceso enviado por correo electrónico, solicita de igual manera datos personales para registro en el sistema; el procedimiento para autorización es ingresar en la dirección de correo electrónico referenciado (de nuevo usuario) hacer clic sobre el enlace que ha sido enviado para validar el acceso a la red por las próximas 24 horas.

Si el registro es por medio de envío de mensajes SMS, recibirá su código de acceso por este medio luego de lo cual estará habilitado para entrar en la próxima página.

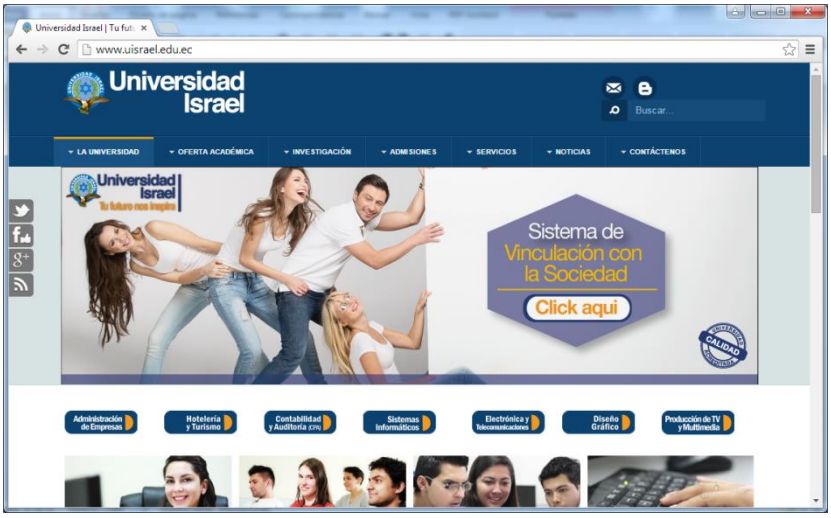
Para cada uno de los casos anteriormente explicados se solicita la confirmación por el mismo medio (mail o SMS); cabe indicar, si no se sigue el procedimiento claramente estipulado el acceso a la red no será autorizado, por lo tanto los dispositivos (Smartphone, Pcs) estarán en margen de espera para el acceso a la red

A continuación mensajes previos a la autorización definitiva del usuario.

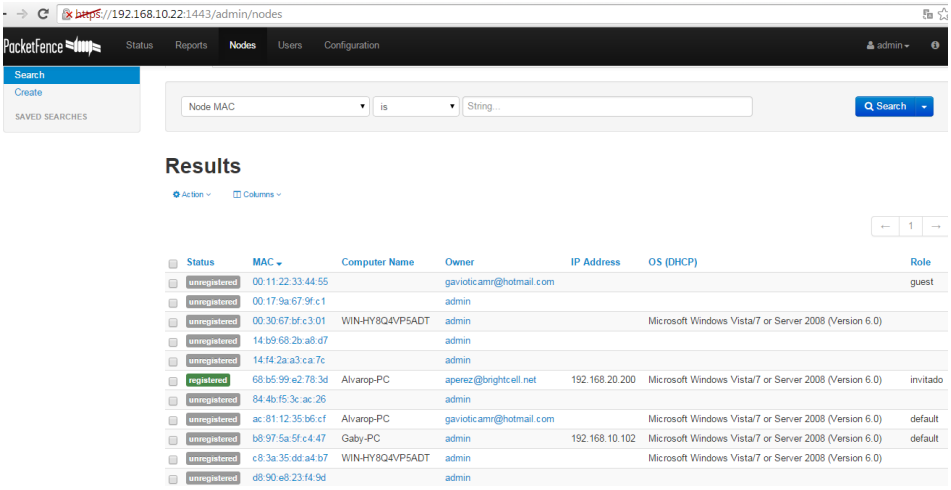
Mensajes explicativos: de que acceso a la red está por confirmarse.



Acceso definitivo a la red, muestra el permiso de navegación.



Todos los dispositivos que se encuentran dentro de la infraestructura de la red son registrados en el sistema (opciones Nodos y Usuarios) estos puede ser administrador por el personal responsable o encargado de dicha tarea, este usuario deberá tener permisos de administrador para proceder con la ejecución de la tarea.



A continuación acceso a las características de los usuarios ingresados en el aplicativo, sean estos registrados o no-registrados; en esta opción podemos observar datos de información del usuario características principales, opción de cambio de estatus de registro, roles de trabajo en la red, violaciones de políticas registradas por el usuario, y más características manipulables por el administrador.

ANEXO 3: MANUAL TECNICO CONFIGURACION PACKETFENCE

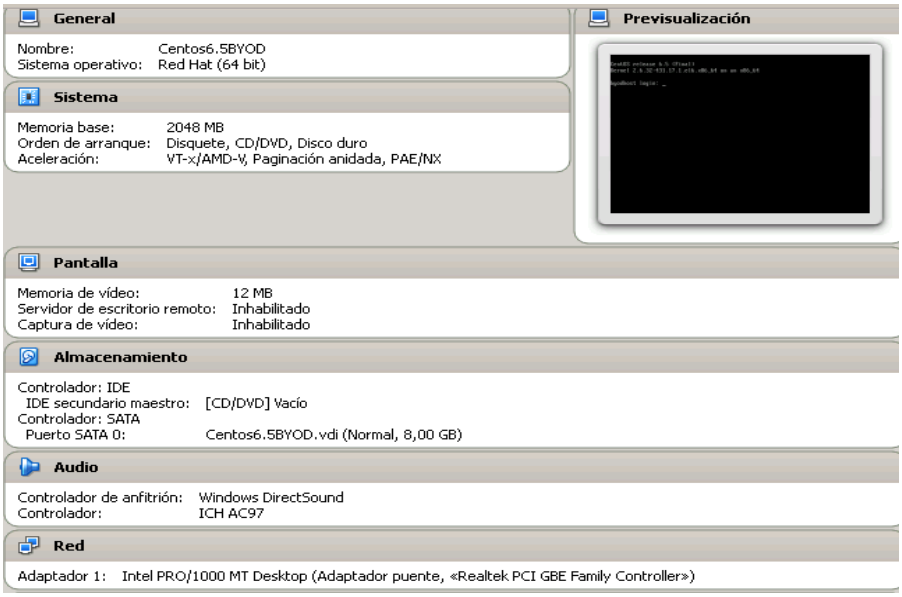
Para la implementación de la herramienta PacketFence se habilitó un escenario de pruebas para instalar y no interferir en el funcionamiento diario de la empresa. Para esto se utilizó un ambiente virtualizado con las siguientes características:

Software utilizado:

- Ambiente virtualizado con Oracle VirtualBox VM Versión 4.3.6
- Sistema Operativo CentOS reléase 6.5 (Final) Kernel 2.6.32-431.17.1 x86_64. Upgrade SO CentOS 6.6.

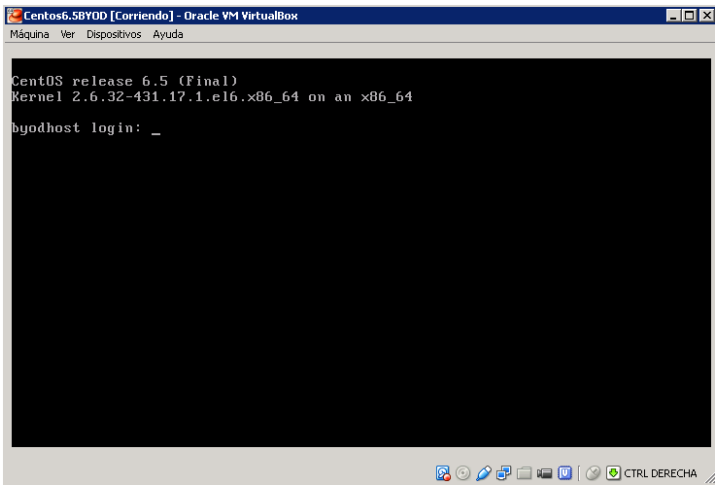
Hardware utilizado:

- Procesador Core I5
- Memoria Ram 2 Gb
- Unidad de DVD Rw
- Tarjeta de red Intel Pro/1000MT



Como anexo se adjunta video tutorial de la instalación del sistema operativo e instalación de Packetfence.

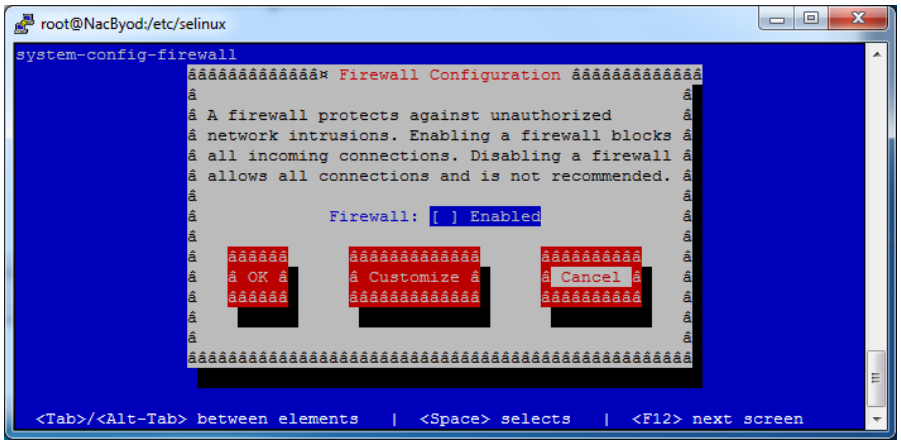
Se continuó con la instalación del sistema operativo CentOS el mismo que cumple con las características para iniciar con la instalación del aplicativo PacketFence. A continuación pantalla de inicio del sistema operativo CentOS ya instalado.



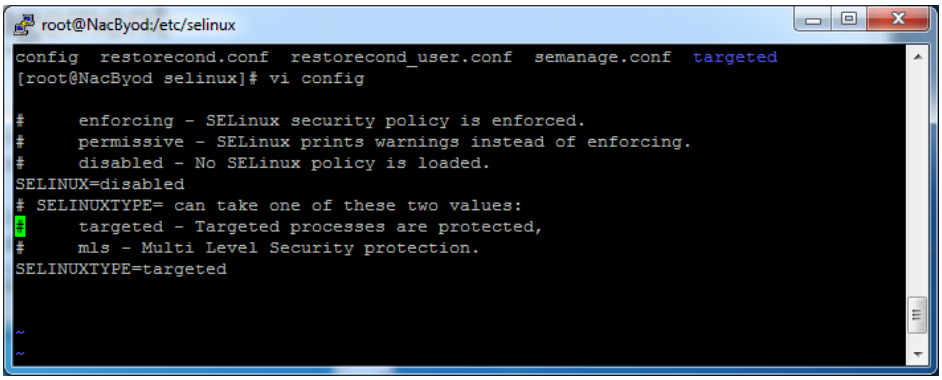
Proceso de instalación del aplicativo OpenSource PacketFence

Previo a la instalación del paquete se procede con la des-habilitación de los siguientes servicios correspondientes al sistema operativo:

- Disable Firewall
- Disable SELinux
- Disable resolvconf



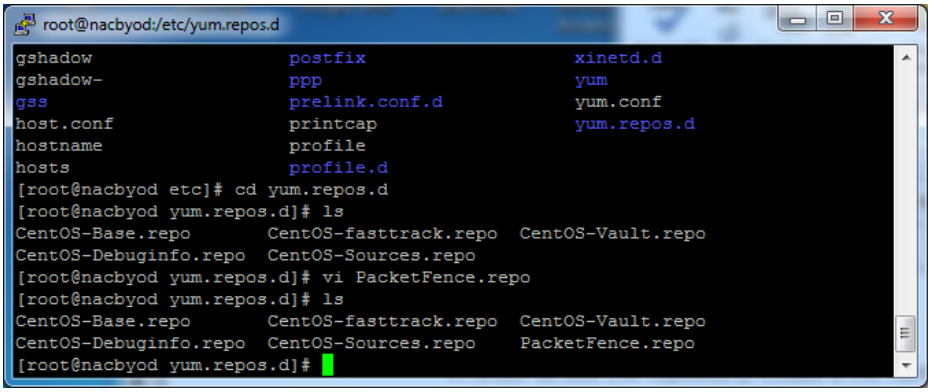
- Directorio del sistema operativo /etc/selinux/config



Para la instalación se procedió con la creación del repositorio desde el cual se iniciará el proceso.

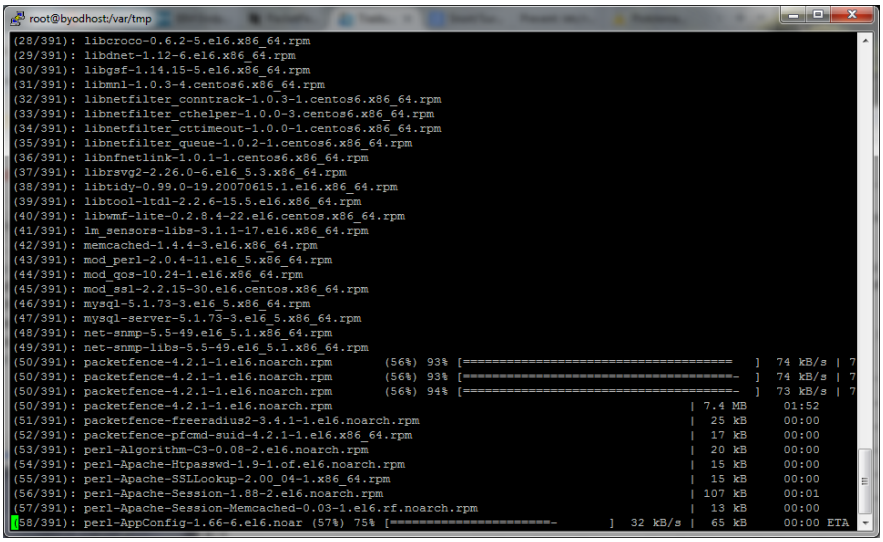
- La última versión de PacketFence es 4.5.1, que ha sido puesto en libertad el 10/11/2014. Esta versión se considera estable y se puede utilizar en entornos de producción.
- La forma más fácil de instalar PacketFence si utiliza una distribución equivalente a CentOS es mediante el uso de un repositorio. Para esto, basta con crear un archivo llamado /etc/yum.repos.d/PacketFence.repo con el siguiente contenido:

```
[PacketFence]
name=PacketFence Repository
baseurl=http://inverse.ca/downloads/PacketFence/RHEL$releasever/$base
arch
gpgcheck=0
```

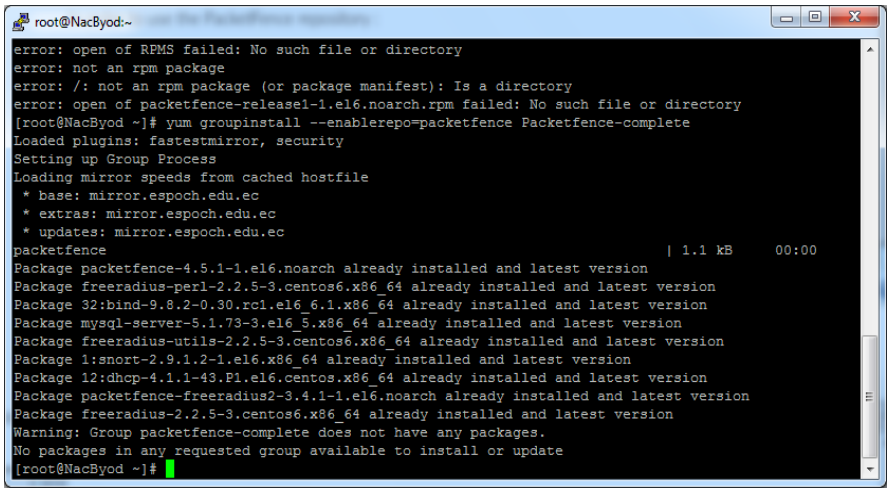


- Se ejecuta la línea de comando siguiente.

yum install PacketFence.repo
rpm -Uvh http://packetfence.org/downloads/PacketFence/RHEL6/`uname -i`/RPMS/packetfence-release-1-1.el6.noarch.rpm
yum groupinstall --enablerepo=packetfence Packetfence-complete



- Proceso de instalación de los paquetes que incluyen en PacketFence



- Proceso de actualización de los paquetes de PacketFence

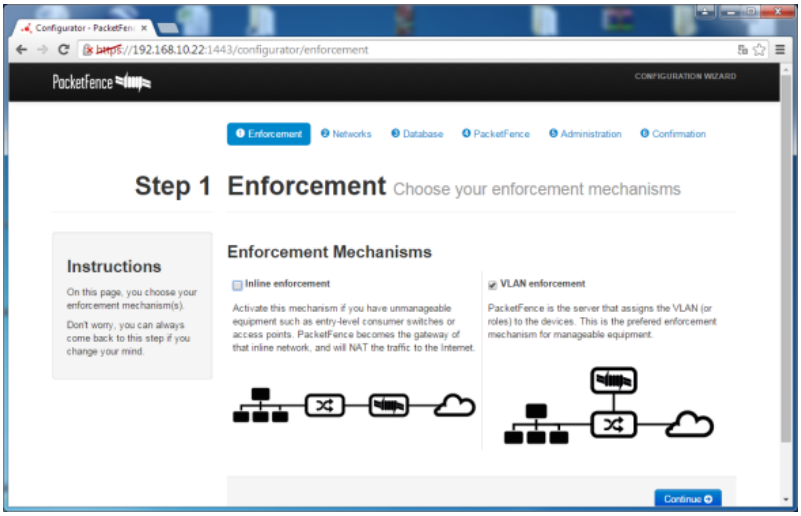
Inicio de configuración PacketFence primeros pasos

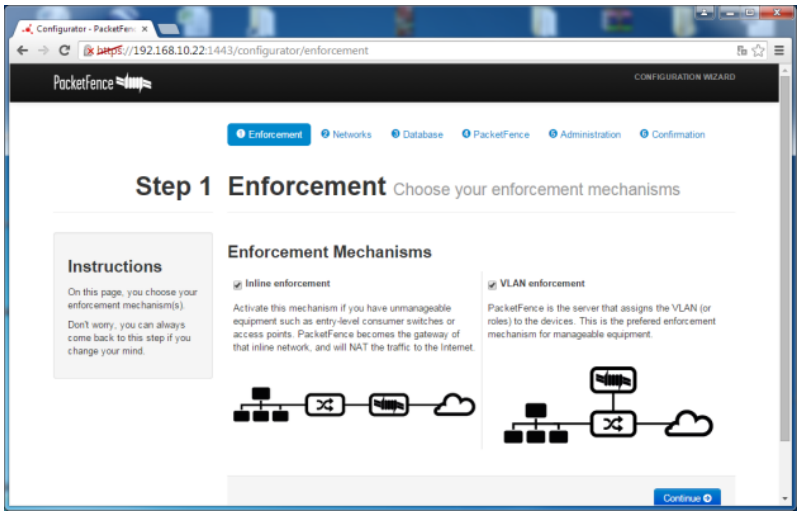
Con el uso de uno de los browser instalados en el PC, Internet Explorer, Firefox, Google Chome ingresamos mediante el link siguiente:

https://192.168.10.22:1443/configurator/enforcement

- **Paso 1: Ejecución (Enforcement)**

En el paso inicial se escoge el tipo de implementación que puede ser por InLine (en capa 2 de red) o Vlans. La opción seleccionada para este caso es Vlans ya que la implementación se realiza con equipos Capa 3 (Switch). Se adiciona también la configuración hibrida en caso de agregar equipos capa2 posteriormente.





- **Paso 2: Redes (Interfaces de red)**

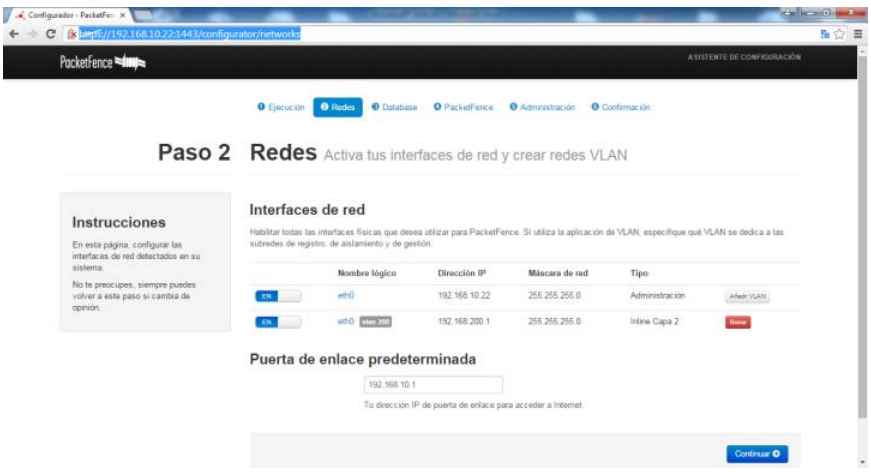
Configuración de la red, se configura las interfaces de red según la necesidad, asignando IPs estáticas según el proyecto propuesto y para cada uno de los tipos requeridos de la aplicación.

En esta opción se puede definir las interfaces a utilizar; éstas pueden ser:

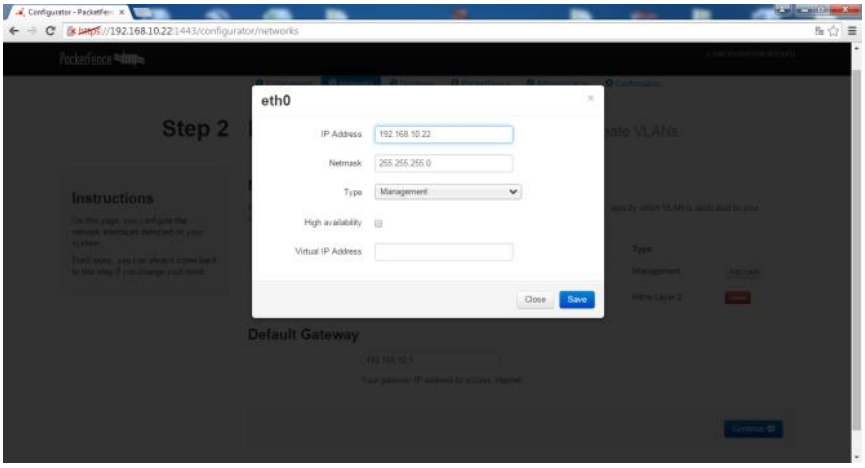
- Administración (Management)
- Registro (registration)
- Aislamiento (Isolation)

Seleccionamos una interface de mantenimiento destinado a la comunicación y administración con los equipos de red, una interface de registro para monitorear los usuarios conectados a la red inalámbrica. Se crea una Vlan restringida que adicionalmente fue creada en los Switch con el objetivo de albergar a los usuarios invitados de la red que permanecerán dentro de un corto periodo de tiempo en las instalaciones, cumple con la función de restringir el acceso a los usuarios invitados y piratas que se conectan ya sea por cable o inalámbrico, impidiendo que tengan comunicación con los diferentes equipos de la red o con los servidores, su única función es salida hacia internet, todos los equipos de esta Vlan están bajo control de PacketFence.

A continuación pantalla de configuración interfaces de red.



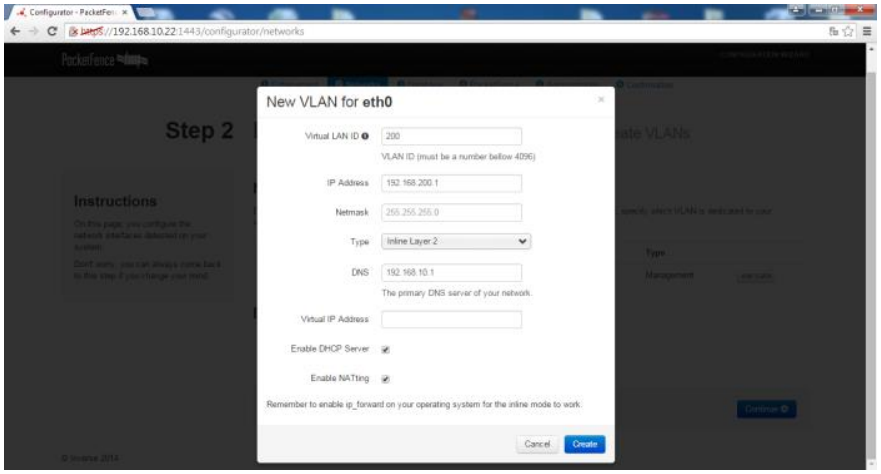
Configuración interface Ethernet 0, como interface para administración.



La Vlan de aislamiento es la encargada de ubicar a los equipos que infringen las políticas de seguridad como son: falta de antivirus, problemas con paquetes no instalados en los sistemas operativos, direcciones físicas MAC identificadas como restringidas, problemas con malware, etc.

La función principal de las Vlans indicas es registrar y monitorear usuarios alámbricos e inalámbricos invitados o no que se conectan a la red de la empresa.

Configuración Sub-interface VLan Ethernet 0, como interface InLine.

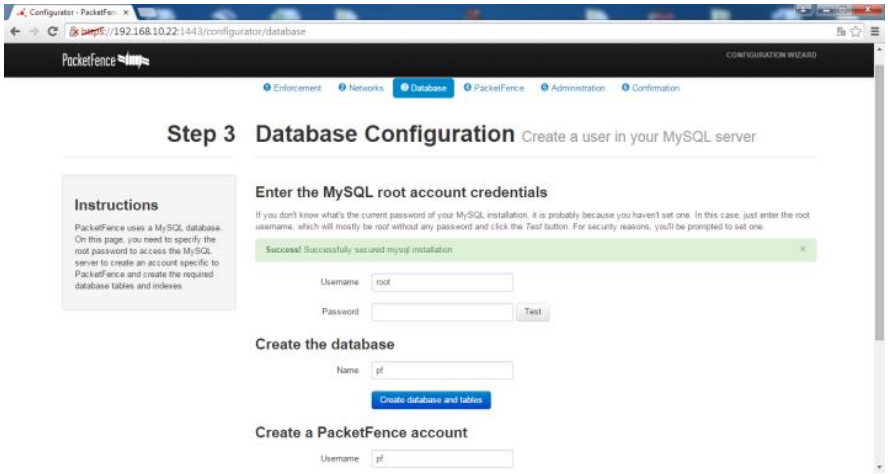


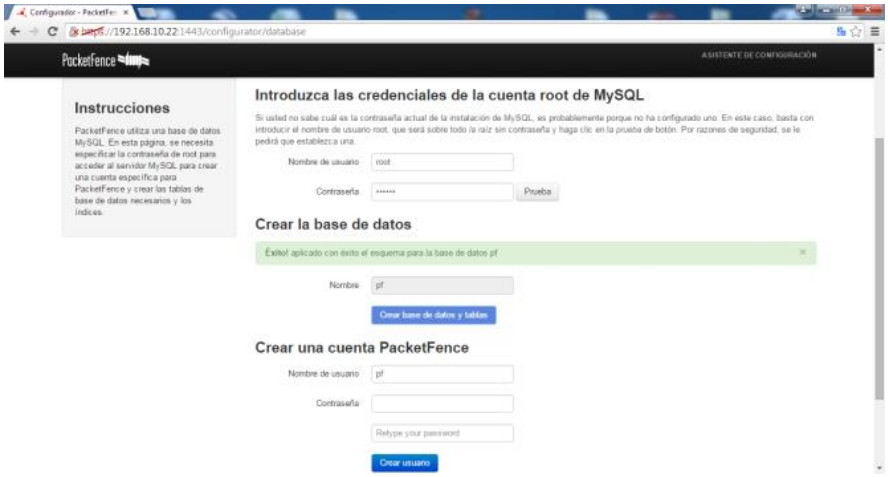
- **Paso 3: Configuración Base de Datos.**

Configuración de base de datos, es creada automáticamente por el aplicativo; en este paso se va a crear la base de datos de PacketFence y organizarla de acuerdo a la estructura correcta. Un usuario para MySQL también será creado y asignado a la base de datos de nueva creación.

El usuario para crear las credenciales de MySQL es root con el password admin1, el nombre que lleva la BDD es pf adicional una cuenta para PacketFence nivel usuario pf con password admin1 (pf1).

Si los datos ingresados son correctos, permite continuar con el siguiente paso.



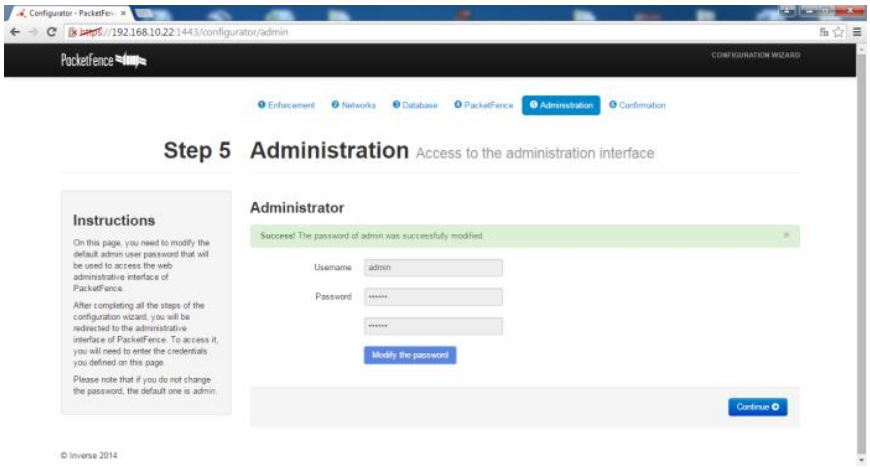


- **Paso 4: Configuración PacketFence**

Configuración general, aquí se deberá configurar parámetros básicos como son: el dominio, nombre del host (nombre asignado al servidor), la dirección IP de las redes en las cuales el servidor PacketFence asignará direccionamiento IP dinámico, esto es en las redes de registro, aislamiento, y/o cuarentena.

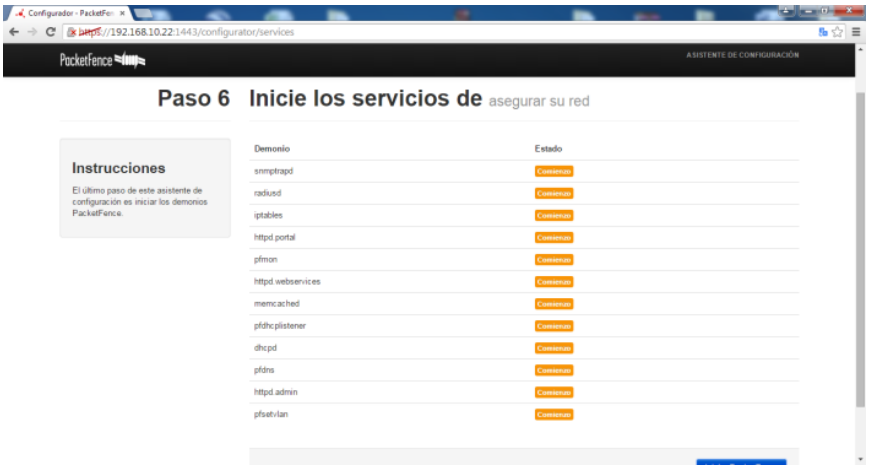
- **Paso 5: Administración**

Creación del usuario administrador, en este paso se solicita la creación de un usuario administrador el mismo que tendrá acceso vía Web por medio de cualquier navegador una vez el aplicativo este funcional. Usuario admin con password admin1 (adminsk).

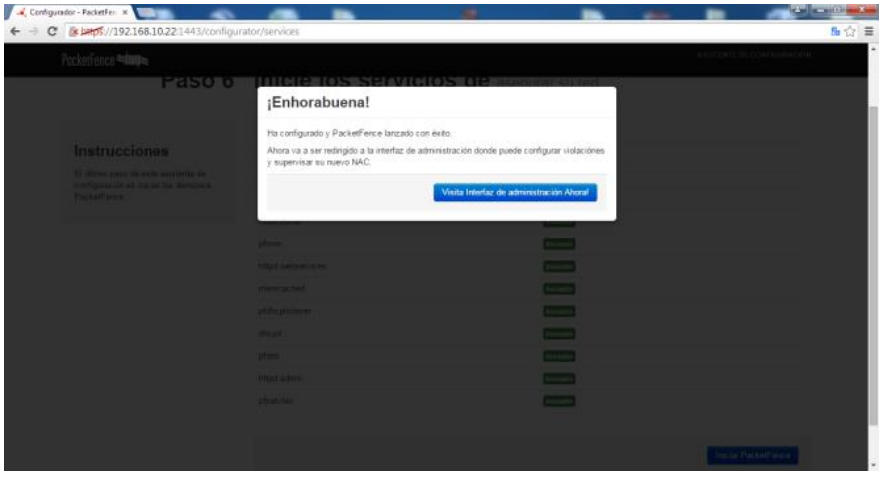


- **Paso 6: Inicio de servicios de PacketFence**

En esta pantalla se puede observar todos los servicios que se iniciarán tan pronto accedamos a la configuración de PacketFence, todos estos servicios deberán estar operativos para garantizar el funcionamiento inicial del aplicativo.



Una vez terminado este proceso nos muestra la siguiente pantalla de bienvenida.

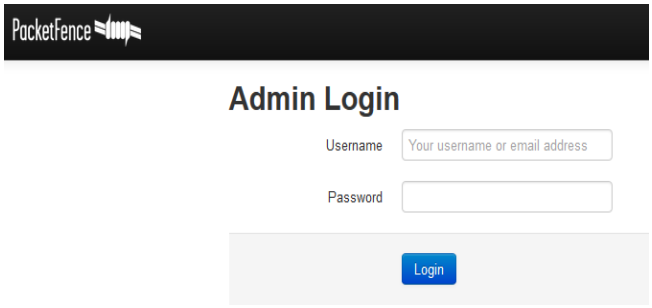


Ingreso por primera vez a PacketFence

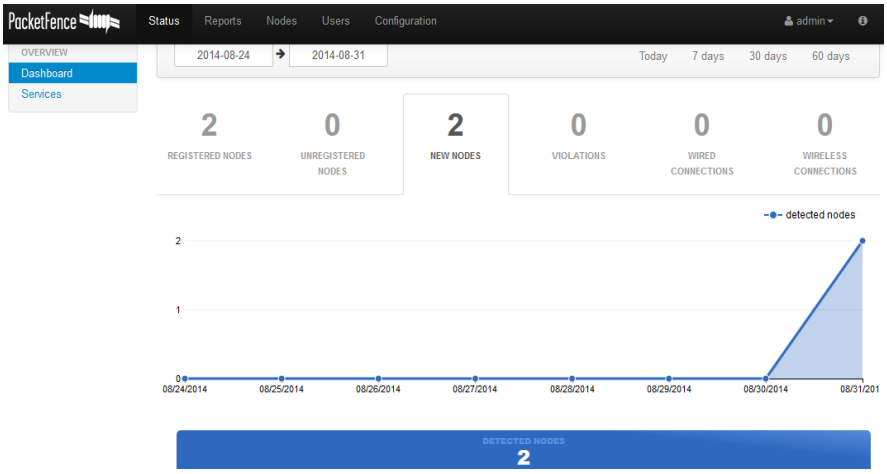
La herramienta Packetfence se puede administrar mediante una interfaz web. En nuestro ambiente de pruebas la dirección web del servidor es la siguiente.

https://192.168.10.22:1443/admin

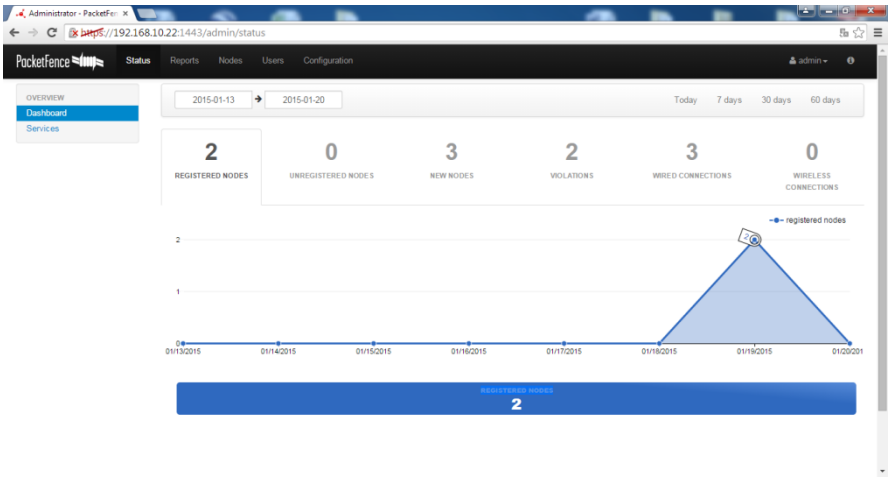
Para ingresar al sitio de administración de la herramienta ingresamos con el usuario admin y contraseña admin1 (adminsk).



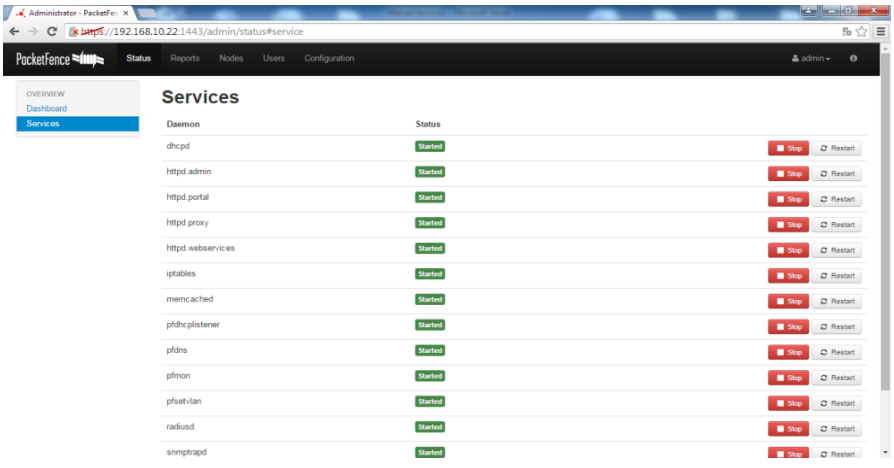
Una vez ingresado al sitio de administración se presenta la pantalla inicial que trata sobre el estado actual del servidor, dentro de lo que podemos observar (nodos se refiere a dispositivos o equipos conectados): los nodos registrados, nodos no registrados, nodos nuevos conectados, nodos que infringen y establecen violaciones, conexiones por medio de cable, conexiones por medio inalámbrico.

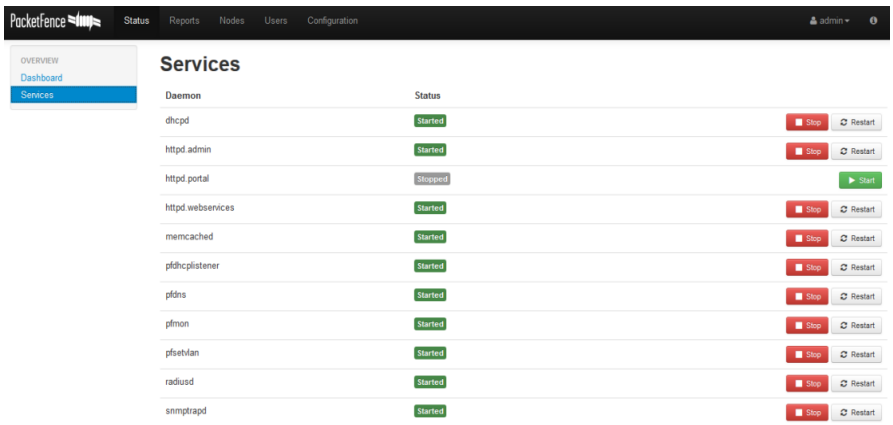


Estado de conexión de nodos (dispositivos) o reporte de los nodos en el servidor PacketFence

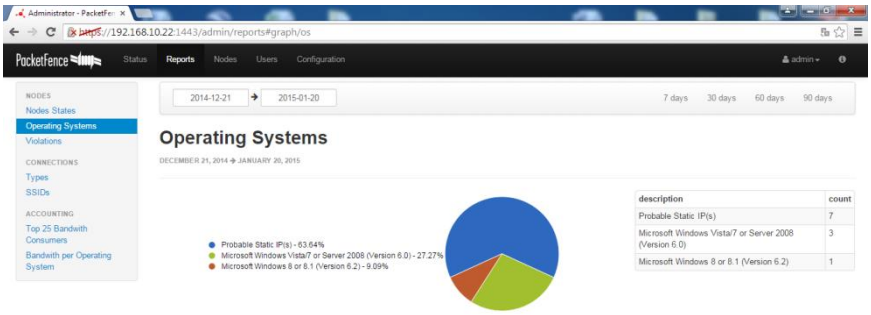


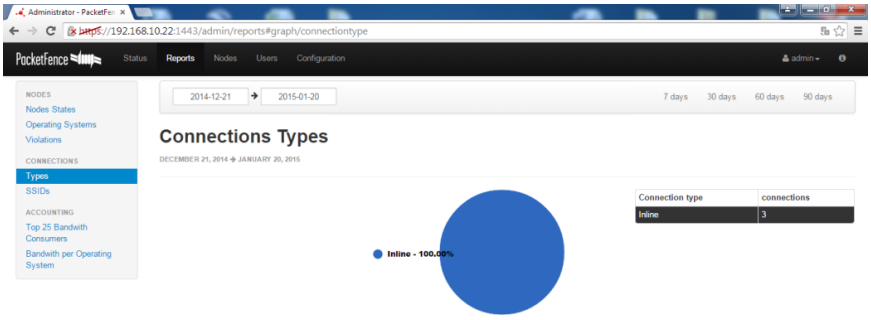
Dentro de estatus es posible observar también los servicios operativos del aplicativo, los mismos que puedes ser reiniciados o parados según la función entregada.





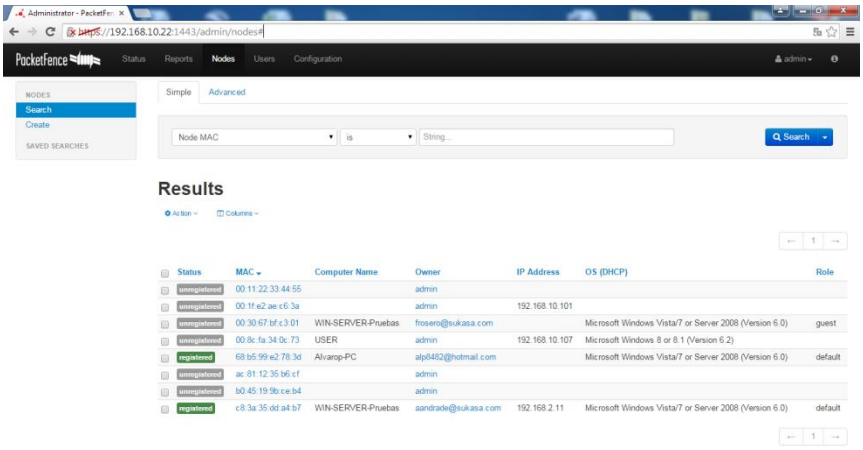
Se continúa con el menú reportes, se puede observar con mayor detalle los reportes sobre los eventos suscitados, detalla reportes de nodos, reporte por tipo sistemas operativos de nodos, conexiones que se muestras con gráficos estadísticos, violaciones, tipos de conexiones, uso ancho de banda por consumidor o por sistema operativo.



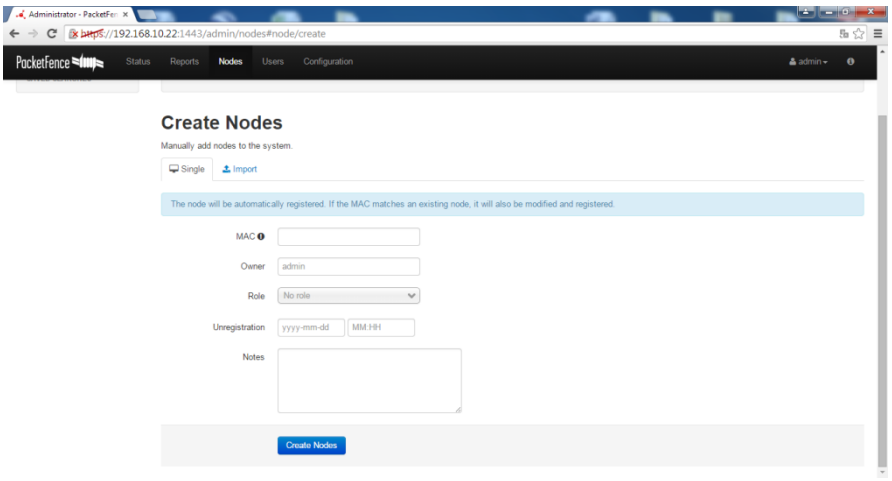


El menú a continuación es de importancia, se lleva el control de todos los nodos (dispositivos) conectados, son identificados por medio de su MAC address; una vez sea identificado el dispositivo y su MAC el administrador puede decidir qué control de acceso o privilegio entregar. Si existe nodos no identificados el administrador puede tomar la decisión de no registrar (Unregistered) y no les permitirá el acceso a la red.

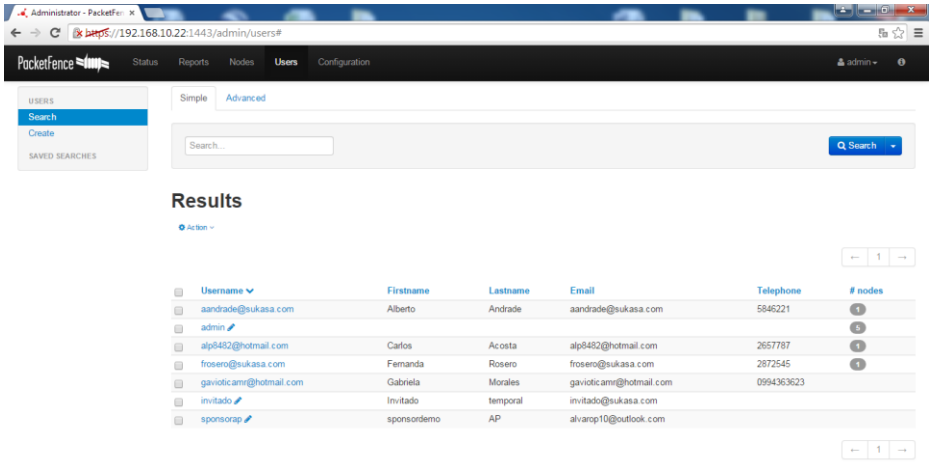
Dentro de la información que este menú entrega esta: el estatus de cada dispositivo (registrado/no-registrado), dirección física MAC, nombre del dispositivo, identificación propietario, dirección IP asignada por DHCP, tipo de sistema operativo, rol asignado para los privilegios respectivos.



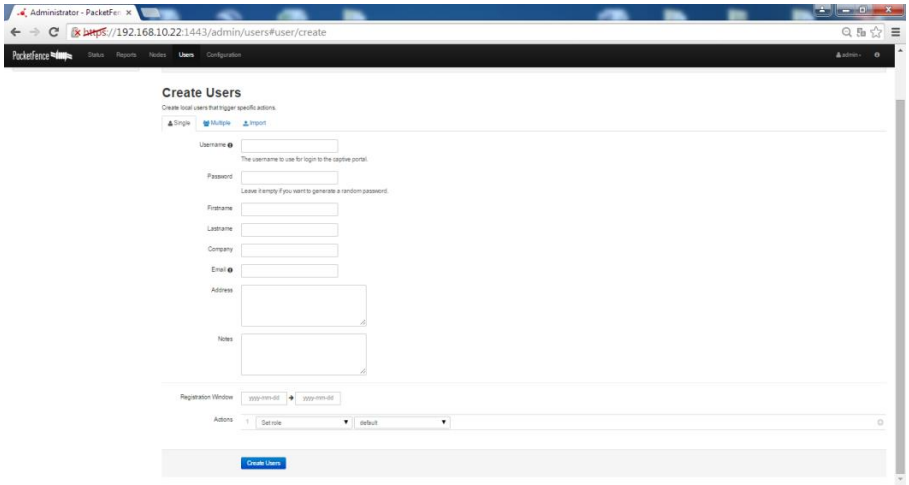
En el presente menú también podemos crear permisos para nuevos nodos o dispositivos, con la opción de Create Nodes, ingresamos toda la información solicitada para nuevos usuarios y lo agregamos al aplicativo.



El menú Usuarios muestra información de reportes de nombre de usuario como identificador principal (más características), correo electrónico, teléfono, número de nodo asignado al usuario; dentro las características de Usuario podemos identificar las violaciones los equipos asignados al usuario y más. A continuación detalle de las pantallas.



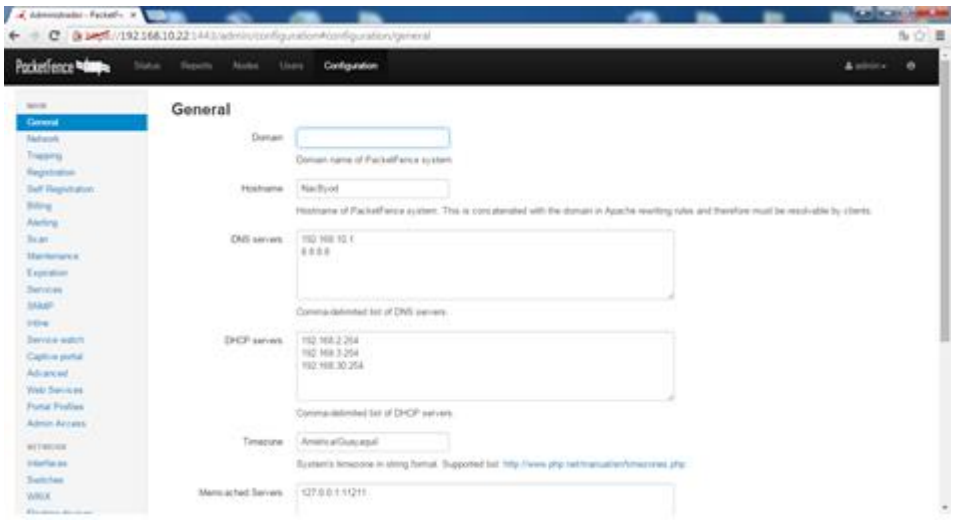
Adjunto a este menú se observa la opción de creación de usuarios locales con propiedades y acciones específicas, personalización según el requerimiento.



Menú de configuración principal, se detalla las diferentes opciones de configuración entre las que tenemos:

- General: Datos generales de configuración aplicativo PF (Dominio, hostname, Servidores Dns, Servidores Dhcp, zona horaria mundial).
- Red: Detector servicios DHCP, detector de violaciones Dhcp.
- Captura: Ingreso de rangos de direcciones IP para supervisar, opción de registro de nodos por primera vez, listado de MAC address que podrían ser inmunes al control, detección de gusanos en la red, características de uso de proxy para acceso a la red.
- Registro: Activar o desactivar la posibilidad de registrar un dispositivo de juego utilizando la página del portal cautivo, papel por default de registro del dispositivo (invitado, juego, por default).
- Auto-Registro: Al habilitar esta opción permite a los huéspedes solicitar su acceso por adelantado el registro es por MAIL, SMS, e ingreso de correo electrónico del patrocinador (SPONSOR) autorizador para el ingreso del usuario a la red.
- Facturación: Procedimiento de pago y autorización de pago de servicio en caso sea necesario, mediante la herramienta Autorize.net.
- Alertas: Información para el envío de notificaciones de Alertas, a los usuarios y administradores.
- Scan: Configuración de escaneo para el cumplimiento de políticas del lado del cliente. Conexiones 802.1.X y puertos.
- Mantenimiento: Configuración intervalos de mantenimiento (nodos, sesiones, violaciones, autorizaciones).
- Caducidad: Configuración caducidad de sesiones en el portal cautivo, sesiones de administrador, registros nodos.
- Servicios: Habilitación o des-habilitación de servicios de PacketFence (Dhcpd, pfdns, snort, suricata, radiusd, iptables, memcached, pfbandwidthd, httpd.admin, httpd.portal, httpd.webservices, httpd.proxy, pfsetvlan, snmptrapd, pfmon, pfdhcplistener); ubicación de los directorios de los servicios.
- SNMP: Configuración de la detección de servicios SNMP.
- InLine: Detección, registro, auditoria, redirección de puertos y dispositivos que se conectan al sistema por InLine.

- Reloj de Servicio: Detección y reanudación de servicios que no se están ejecutando.
- Portal Cautivo: Activar la función de detección automática de la red para su registro el re-direccionamiento automático. Portal seguro.
- Avanzado: Evaluación del estado de una VLAN, nodo y volver a asignar o cambiar las reglas de iptables.
- Servicios Web: Datos de acceso servidor y usuario Webservice.
- Perfiles del Portal: Características para presentar un portal cautivo diferente según el SSID, la VLAN, o el conmutador IP que se conecta el cliente.
- Administrador de acceso: Definir los roles con los derechos de acceso específicos a la interfaz de administración Web. Los roles se asignan a los usuarios en función de su fuente de autenticación.



- RED:
  - Interfaces: Información de las interfaces de red del servidor, Vlans (Direccionamiento IP).
  - Switches: Agregar y configurar dispositivos de red (Switch, Access point)
  - Floating devices: Agregar y configurar dispositivos inalámbricos a la red.
  - Firewall: Control y habilitación de un firewall opcional.

- USUARIOS
    - Roles: Definir las funciones que se aplicarán a todos los dispositivos de la red.
    - Duración de acceso: Este es el valor de duración de acceso predeterminado para los roles de los dispositivos.
    - Sources (Fuentes): Definir las fuentes de autenticación para que los usuarios accedan al portal cautivo o la interfaz de administración Web. Cada perfil de portal debe estar asociado con uno o múltiples fuentes de autenticación mientras que las conexiones 802.1x la ordenaron fuentes internas para determinar qué papel va a utilizar.

- COMPLIANCE
    - Violaciones: Tabla de reporte de las violaciones por su identificador, descripción, acciones, Vlan a la que se aplica y acción.
    - Declaración de salud: Definir los filtros que se aplicarán a todos los clientes compatibles con NAP que producen un estado de salud (informe de mantenimiento).

IMPLEMENTANDO PACKETFENCE A LA INFRAESTRUCTURA DE RED

Configuración de PacketFence - Caso de Uso

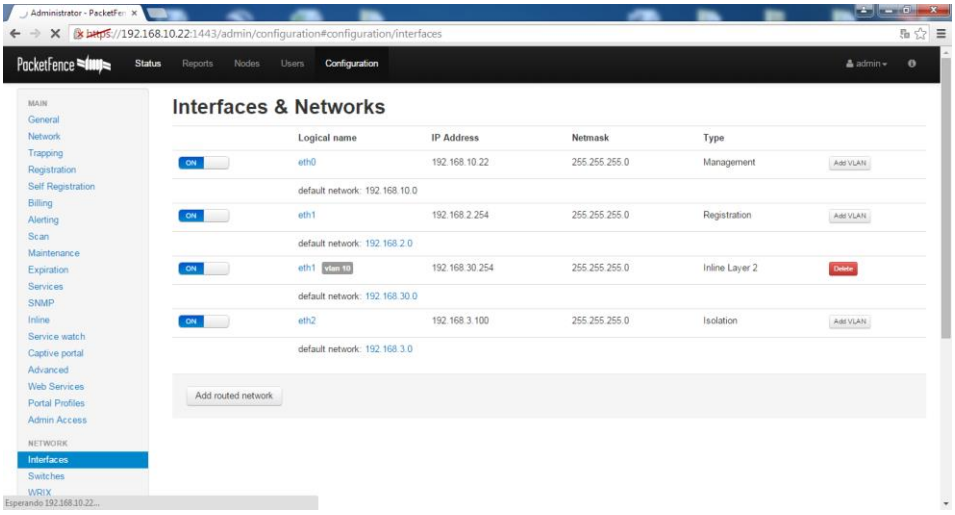
Una vez iniciado el sistema y conectado el servidor al switch en modo TRUNK accedemos a la configuración de PacketFence, donde definiremos o corregiremos el modo de funcionamiento, las interfaces de red, contraseñas de administración y características a configurar según sea el requerimiento y topología de red.

- Seleccionamos el modo de funcionamiento, en nuestro caso probaremos solo el modo; "VLAN Enforcement" ya que en el despliegue en producción solo aplicaremos la solución a dispositivos gestionables con 802.1x con soporte MAB (Mac Bypass).

- Se define las direcciones de red y las interfaces del sistema donde el DHCP del servidor ofrecerá servicio para los dispositivos que deseen acceder a la red.

- Se aplica la configuración establecida en la tabla descrita a continuación, esta configuración se apega a la configuración establecida para el caso de estudio.

Interface	Vlan	Red	Gateway	Descripción
eth0/0		192.168.10.0/24	192.168.10.254	Gestión
eth0/2	2	192.168.2.0/24	192.168.2.254	Registro
eth0/3	3	192.168.3.0/24	192.168.3.254	Cuarentena
eth0/4	4			Detección de MAC
eth0/5	30	192.168.30.10	192.168.30.254	Invitados

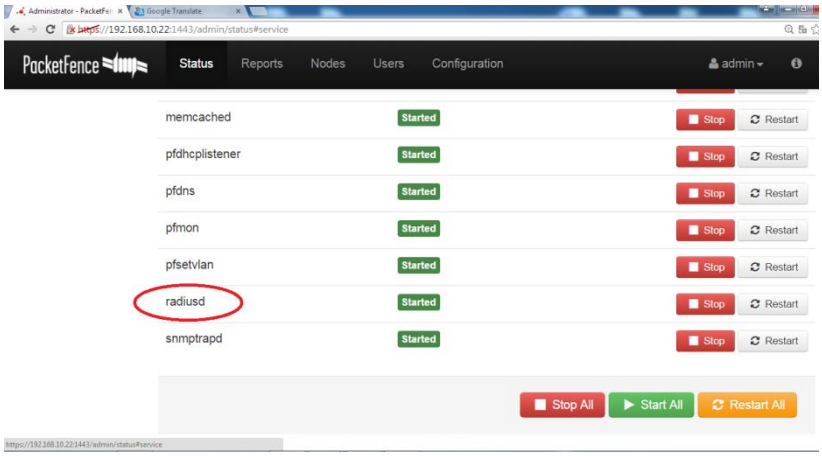


Configuración para la infraestructura de red del caso de estudio.

- PacketFence configuración FreeRADIUS (Authentication 802.1X or MAC)
- PacketFence Dirección IP: 192.168.10.22
- VLan Gestión: 1
- VLan Registration: 2
- VLan Isolation: 3
- VLan Detección MAC: 4
- VLan Guest VLAN: 30
- Usar SNMP v2c
    - SNMP Read community: public
    - SNMP Write community: private
    - SNMP Trap community: public
- RADIUS Secret: frasesecreta

La autenticación y registro

Consiste en comprobar la identidad de un usuario o dispositivo, para posterior autorizar el acceso a los recursos permitidos, para esto se ha configurado la Vlan correspondiente. Es soportado para las redes cableadas e inalámbricas, a través del servicio Radiusd inhibido en el servidor PacketFence bajo la versión 4.5.1 instalada.

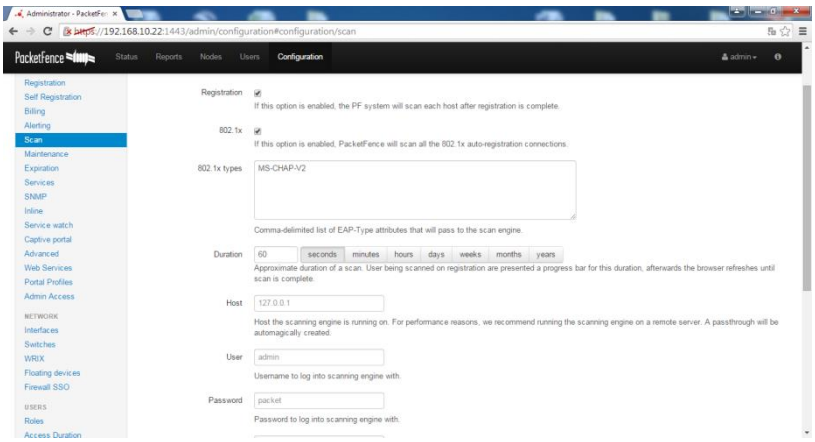


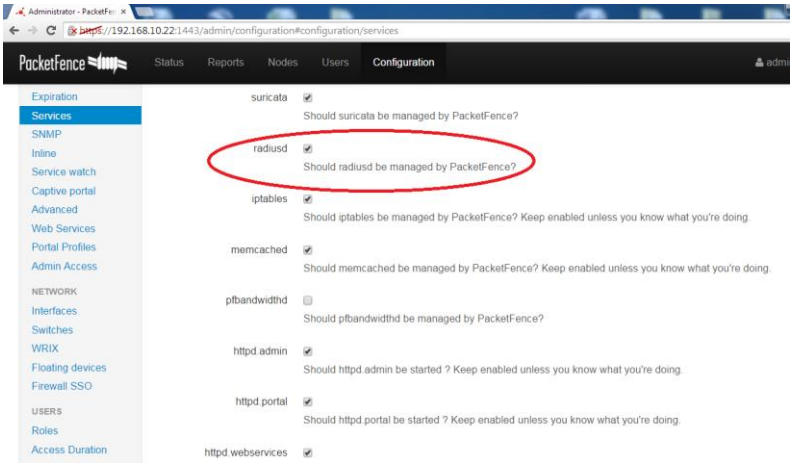
Se integra a la infraestructura de red atreves del servicio indicado (radiusd), permitiendo asegurar la red (soporta 802.1X) usando para esto la misma base de datos de usuarios del aplicativo PF y el portal cautivo.

La autenticación 802.1X es uno de los métodos más seguros ya que permite la detección de sistemas finales en el puerto del switch mediante autenticación. Su fundamente se basa en el concepto de puerto siendo este el puerto donde se puede conceder el acceso de un dispositivo a la red. Inicialmente todos los puertos están desautorizados, excepto uno que es el puerto de acceso que se utiliza para comunicarse con el cliente permitiéndole únicamente tráfico (comunicación). Cuando un nuevo cliente solicita la interconexión, le pasa al autorizador (PacketFence-servicio radiusd) información sobre la autenticación, cuando este contesta y resuelve el permiso (autoriza), permite el uso de un puerto al nuevo cliente; si es un cliente inalámbrico se le redirección a la Vlan de usuarios registrados previo a la autenticación mediante el protocolo EAP-MSCHAP.

El procedimiento seguido es:

- Autenticación
- Acceso a la red mediante perfiles de usuario / Radius (proto 802.1X)
- Asignación de políticas de control, sin importar el puerto físico.
- Clasificación de usuarios con base a perfiles o políticas.
- Aplicación de políticas de control sobre direcciones físicas (MAC) por PF.

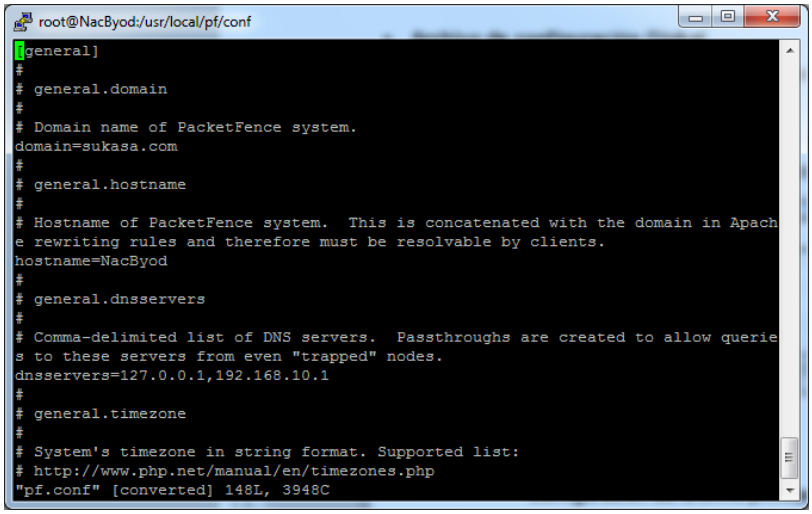




Configuración del archivo principal pf.conf de Packetfence.

En este archivo se agrega parámetros importantes del aplicativo, esta configuración se encuentra dentro del directorio /usr/local/pf/conf/pf.conf.

El archivo es posible abrir utilizando el comando vi (edición de archivos) más el nombre del archivo y extensión. Cualquier cambio se reflejará de inmediato en el aplicativo.



El contenido del archivo a continuación.

```
[general]
#
# general.domain
# Domain name of PacketFence system.
domain=CH.com
# general.hostname
# Hostname of PacketFence system.  This is concatenated with the domain in Apache rewriting rules and
therefore must be resolvable by clients.
hostname=NacByod
# general.dnsservers
# Comma-delimited list of DNS servers.  Passthroughs are created to allow queries to these servers from
even "trapped" nodes.
dnsservers=192.168.10.1,8.8.8.8
# general.dhcpservers
# Comma-delimited list of DHCP servers.  Passthroughs are created to allow DHCP transactions from even
"trapped" nodes.
dhcpservers=192.168.2.254,192.168.3.254,192.168.30.254
# general.timezone
# System's timezone in string format. Supported list:
# http://www.php.net/manual/en/timezones.php
[trapping]
# trapping.range
# Comma-delimited list of address ranges/CIDR blocks that PacketFence will monitor/detect/trap on.
Gateway, network, and
# broadcast addresses are ignored.
range=192.168.0.0/24,192.168.10.0/24,192.168.2.0/24,192.168.3.0/24
# trapping.redirtimer
# How long to display the progress bar during trap release. Default value is
# based on VLAN enforcement techniques. Inline enforcement only users could
# lower the value.
redirtimer=20m
# trapping.wait_for_redirect
# How many seconds should the WebAPI sleep before actually triggering the VLAN change.
# This is meant to give the device enough time to fetch the redirection page before
# switching VLAN.
wait_for_redirect=5
# trapping.interception_proxy
# When enabled, packetfence will intercept proxy request to somes specified port
interception_proxy=enabled

[registration]
# registration.button_text
button_text=Registrar
# registration.device_registration
# Enable or Disable the ability to register a gaming device using the specific portal page designed to do it
device_registration=enabled
# registration.device_registration_role
# The role to assign to gaming devices. If none is specified, the role of the registrant is used.
device_registration_role=guest

[guests_self_registration]
# guests_self_registration.sponsorship_cc
# Sponsors requesting access and access confirmation emails are CC'ed to this
# address. Multiple destinations can be comma separated.
sponsorship_cc=alvarop10@outlook.com

[alerting]
# alerting.emailaddr
# Email address to which notifications of rogue DHCP servers, violations with an action of "email", or any
other
# PacketFence-related message goes to.
emailaddr=alp8482@hotmail.com
# alerting.fromaddr
# Source email address for email notifications. Empty means root@<server-domain-name>.
fromaddr=pf@localhost
# alerting.subjectprefix
#Subject prefix for email notifications of rogue DHCP servers, violations with an action of "email", or any other
#PacketFence-related message.
subjectprefix=Alerta PF:

[scan]
# scan.engine
```

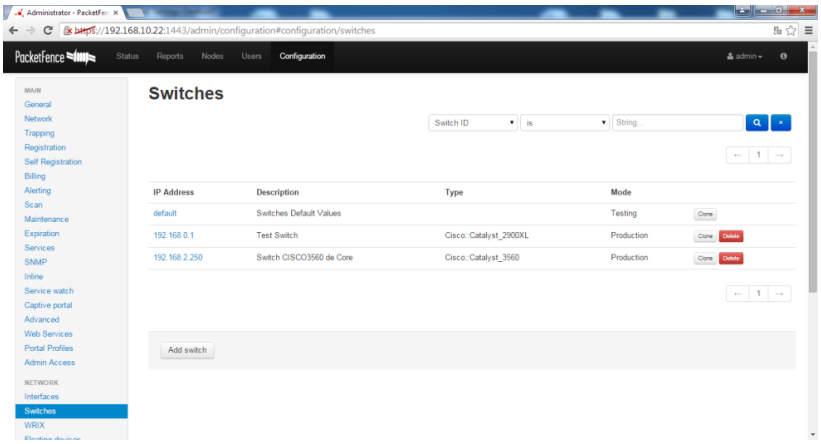
```
# Which scan engine to use to perform client-side policy compliance.
engine=nessus

[database]
# database.pass
# Password for the mysql database used by PacketFence.
pass=pf1

[captive_portal]
# captive_portal.network_detection_ip
# This IP is used as the webserver who hosts the common/network-access-detection.gif which is used to detect if network
# access was enabled.
# It cannot be a domain name since it is used in registration or quarantine where DNS is blackholed.
# It is recommended that you allow your users to reach your packetfence server and put your LAN's PacketFence IP.
# By default we will make this reach PacketFence's website as an easy solution.
network_detection_ip=192.168.20.100
# captive_portal.secure_redirect
# If secure_redirect is enabled, the captive portal uses HTTPS when redirecting
# captured clients. This is the default behavior.
secure_redirect=disabled

[interface eth0]
ip=192.168.10.22
type=management
mask=255.255.255.0

[interface eth1]
enforcement=vlan
ip=192.168.2.254
type=internal
mask=255.255.255.0

[interface eth2]
enforcement=vlan
ip=192.168.3.100
type=internal
mask=255.255.255.0

[interface eth1.10]
enforcement=inlinel2
ip=192.168.30.254
type=internal
mask=255.255.255.0
```

Configuración de dispositivos de red en switches.conf

En este archivo se almacena la información relacionada con los dispositivos de red que van a ser configurados para trabajar en conjunto con Packetfence, el aplicativo necesita conocer que dispositivos van a ser administrados, dentro de los cuales están switch capa 3 (red), Access point (wireless), esta información se almacena en el directorio /usr/local/pf/conf/ en el archivo switches.conf.

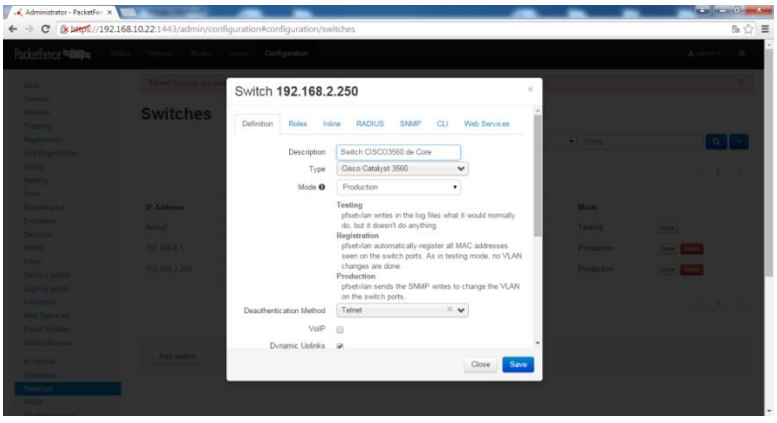
Dentro del menú configuration ubicamos el sub-grupo Network opción Switch: donde procedemos a ingresar la configuración requerida para el equipo (switch) que entrará en producción.

A continuación muestra de las pantallas de configuración.

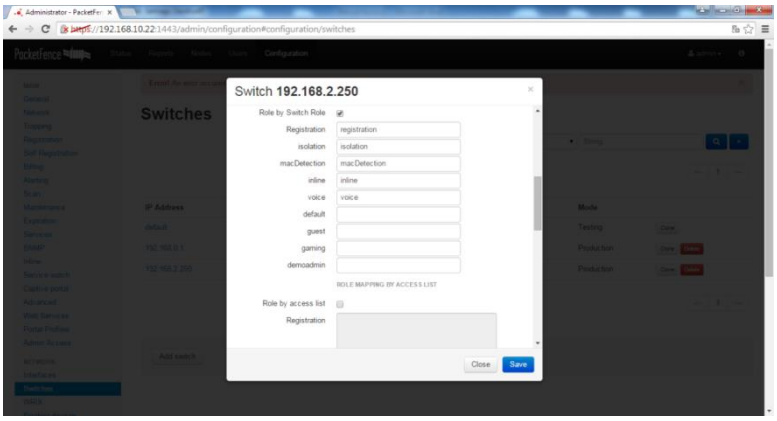


Agregar el dispositivo (switch) con la opción ADD Switch, donde permite el acceso al resto de configuraciones y parámetros, estos datos solicitados deben estar en concordancia a los parámetros solicitados para el estudio de caso; el Switch tiene las siguientes características:

- Switch Catalyst Series 2900
- Catalyst 2960 IOS versión 12
- Port 24 puertos FastEthernet
- Dirección IP 192.168.2.250 Vlans de Registro.



El Switch entrará directamente en producción por lo tanto pfsetvlan envía el SNMP registrando para cambiar la VLAN en los puertos del switch. La siguiente pestaña es Roles en donde se agrega las Vlans necesarias para el funcionamiento del servidor.



En la misma pantalla se detalla el ajuste del modo InLine, frase secreta de Radius, configuración de la versión del protocolo de comunicación SNMP y seguridades, usuario y contraseña de comunicación (telnet) con el dispositivo (switch), características acceso web en caso sea necesario.

Configuración de SNMP:

Accediendo al switch (192.168.2.251) al que se conectará PacketFence y en modo de configuración realizamos lo siguiente:

```
snmp-server community nac RW 10
snmp-server enable traps port-security
snmp-server enable traps port-security trap-rate 1
snmp-server host 192.168.10.22 version 2c nac port-security
```

Configurando las Interfaces:

Para administrar las interfaces de cada switch se necesita port security en cada interfaz.

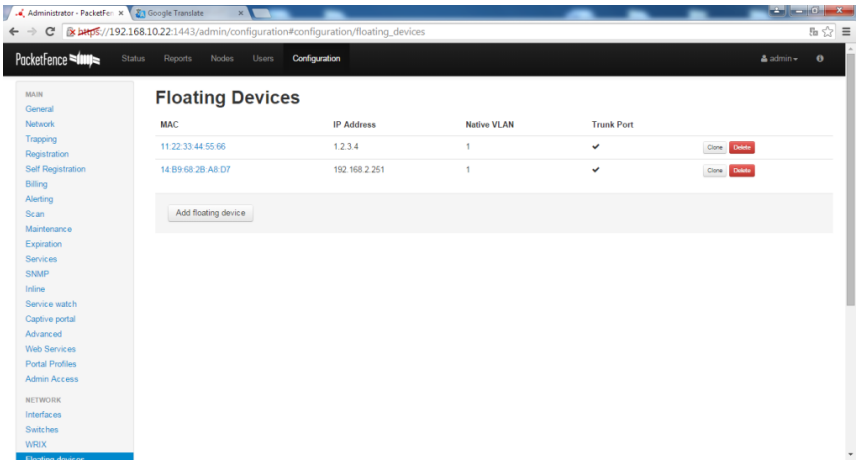
```
interface FastEthernet0/23
switchport access vlan 2
switchport mode access
switchport port-security maximum 1 vlan access
```

switchport port-security
switchport port-security violation restrict
switchport port-security mac-address 0200.000X.XXX
speed 100
duplex full

Nota. X.XXX es el número de ifindex de la interfaz, en este caso seria 1.0023 por la interfaz F 0/23

Configuración de dispositivos Floating-Devices equipos inalámbricos (Access point)

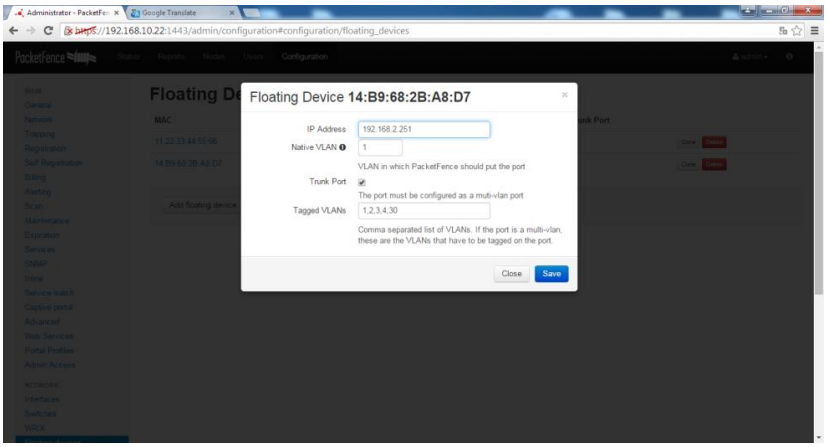
Floating-Devices: Agregar y configurar dispositivos inalámbricos a la red pueden ser puntos de acceso inalámbrico locales y de amplia extensión. Todo dispositivo inalámbrico debe ser identificado. A esta opción ingresamos por Configuration grupo Network opción Floating Devices.



Los dispositivos deben ser identificados utilizando su dirección física MAC Address. En el caso presente se entregara servicio inalámbrico a equipos locales como a equipos (dispositivos) de usuario invitados temporales o por periodos de tiempo. Para eso se utiliza el Access point DWL-3200AP dentro de la infraestructura de red de la empresa. Se detalla las configuraciones requeridas para acceso al servidor.

- PacketFence configuración FreeRADIUS
- PacketFence Dirección IP: 192.168.10.22
- Dirección IP Floating: 192.168.2.251
- VLan Gestión: 1
- VLan Registration: 2
- VLan Isolation: 3
- VLan Detección MAC : 4
- VLan Guest VLAN: 30
- Usar SNMP v2c
    - SNMP community: public
    - RADIUS Secret: Frasesecreta1
    - Open SSID: PF-Public
    - WPA-Enterprise SSID: PF-Secure

El acceso a la infraestructura de red es autorizado por medio de una cuenta de usuario y clave que previamente fue ingresado en el servidor PF de igual manera están bajo el control y políticas de seguridad de PF. A continuación se muestra la configuración ingresada al dispositivo Floating (Access Point).



ANEXO 4: ENCUESTA

OBJETIVO: Determinar si la seguridad de la red LAN de la Empresa CH, mejorará con la implementación de la herramienta de control y seguridad de acceso a la red NAC.

CUESTIONARIO

1. ¿Cree usted que es útil el controlar el acceso a la red local de información de la empresa?

SI___ NO___

2. ¿Cuándo se presenta un acceso indebido de seguridad a la red local podría Usted determinar donde se genera el problema?

SI___ NO___

3. ¿Con la implementación de la herramienta Network Access Control cree Usted que se podría controlar la vulnerabilidad y fallas de seguridad de la red de la empresa, garantizando así la seguridad de la red local?

SI___ NO___

4. ¿Considera Usted que con la implementación de un aplicativo se logrará mejorar el control de acceso a los recursos de red?

SI___ NO___

5. ¿Piensa Usted que el tener la administración y monitoreo de la red para la detección de vulnerabilidades y fallas de seguridad, favorecerá de alguna manera la tarea del administrador de la red local de la empresa?

MUCHO___ POCO___ NADA___

6. ¿La herramienta implementada permitirá obtener información detallada y en tiempo real del estado actual de los dispositivos que conforman la red?

SIEMPRE _____ CASI SIEMPRE_____ NUNCA_____

7. ¿Cree usted que la implementación de esta herramienta ayudará al desarrollo de la Infraestructura de red de la empresa?

SI___ NO___

ANEXO 5: POLITICAS DE CONTROL DE ACCESO

CUMPLIMIENTO DE POLITICAS DE CONTROL DE ACCESO A LA RED PARA DISPOSITIVOS INALAMBRICOS Y ALAMBRICOS QUE NECESITAN ACCESO A LA RED DE LA ORGANIZACIÓN.

Resumen

El movimiento de traer su propio dispositivo a la empresa para uso dentro en la misma (BYOD), ha ayudado a simplificar las operaciones de TI, permitiendo a los empleados y visitantes conectar dispositivos personales, tales como computadores portátiles, teléfonos inteligentes (Smartphone) y tablets a los recursos de la organización. Por supuesto, esta flexibilidad ha adicionado otro tipo de factor que es: la necesidad de establecer pautas adecuadas para el uso y control de estos dispositivos, así como lo que el usuario se le permite introducir o acceder a la red.

Dado que los empleados utilizan sus dispositivos para actividades personales y/o recreativas, esta puede plantear más riesgos para la organización que el uso exclusivo de los dispositivos propiedad de la empresa.

Esta política describe los pasos que la empresa sus empleados y usuarios visitantes deben seguir al conectar dispositivos personales a los sistemas y red de la organización.

Propósito

El propósito de esta política es proporcionar los requisitos para el uso adecuado de los recursos de red y establecer los pasos que tanto los usuarios y el departamento de TI debe seguir para inicializar, apoyar y quitar dispositivos que acceden a la red de la empresa. Los requerimientos se deben seguir como se los ha documentado, con el fin de proteger los sistemas de la empresa y datos, de acceso no autorizado; todo esto por evitar el mal uso de la información y recursos de red.

Cobertura

Todo empleado a tiempo completo, trabajadores contratados, consultores, personal a tiempo parcial, trabajadores temporales, visitantes y otro personal que se conceda el

acceso a los sistemas de organización, redes, software y/o datos están cubiertos por esta política.

Los equipos cubiertos incluye (pero no se limita a): Computadores de escritorio, portátiles, tablets, Smartphones (definido como cualquier teléfono celular que se conecta a Internet a través de Wi-Fi de la empresa).

Unidades memory-flash, discos duros externos, iPods, dispositivos de entretenimiento y música portátiles o similares que se conectan a las redes WiFi. De entretenimiento y consolas de videojuegos (Xbox, PS3, Wii, etc.) que se conectan a la red WiFi, mismos que se utilizan para acceder a servicios de correo electrónico y sistemas de organización.

Orientación general de las políticas

Todos los usuarios deben conocer que cada vez que un dispositivo está conectado a la red de la empresa, a los sistemas, o computadoras (servidores), existen oportunidad para: introducir virus, spyware, malware y otros programas que causan malestar y daño.

Como resultado de cualquier circunstancia, un usuario que conecta su propio dispositivo para uso de los recursos de la organización, sistemas o redes podría interrumpir las operaciones del negocio, causar fuga de información, publicar datos de la organización, de clientes y/o socios, en sitios web sin ninguna autorización. En el peor de los casos, se procederá con sanciones civiles y/o penales para el usuario que infrinja esta reglamentación, adicional a costos/gastos que ocasionará el aspecto legal y/o administrativo.

La lista de verificación y la forma de aprobación (ver más abajo) deben ser utilizados para identificar las necesidades de los empleados previo a su aprobación de acceso, este control debe ser ejecutado antes que cualquier dispositivo personal sea ingresado (interconectado) a la redes de la empresa.

Ningún usuario miembro de la empresa, visitante o personal de TI podrá autorizar el acceso a la red sin previo consentimiento y aprobación por parte de Gerencia de TI de la organización o personal autorizado para esta acción.

Responsabilidades del Departamento de TI

El departamento de TI se asegurará de los siguientes puntos, para facilitar el acceso conforme a lo solicitado por cada usuario que solicita el acceso a la red:

- ✓ El dispositivo no debe tener una dirección IP estática que podría ocasionar conflictos (de direccionamiento IP) en la red.
- ✓ El dispositivo no debe contener virus informáticos, software espía o infección por malware. Debe estar correctamente protegido contra virus informáticos evitando la propagación de software malicioso y otras amenazas que puedan hacer que la red de la organización sea vulnerable.
- ✓ El dispositivo no tiene ningún software de terceros o aplicaciones que suponen una amenaza para los sistemas de la empresa y red de información, o que pudiera ser incompatible con las aplicaciones que se encuentran en producción, el departamento de TI debe verificar y si es el caso remover tales aplicaciones.
- ✓ El departamento de TI se reserva el derecho de la evaluación y análisis, en cuanto a las aplicaciones (actuales o futuros) que son apropiados para los dispositivos asociados con la organización y sus departamentos de sistemas, información, y redes.
- ✓ El departamento de TI se reserva el derecho de autorizar el acceso a la red información con el uso de autentificaciones y autorización vía mail o SMS según permita los aplicativos internos de la organización.
- ✓ Si se trata de un dispositivo móvil como laptops, smartphone o tablet, que necesariamente se asocie con los sistemas de la empresa, se debe levantar una política de seguridad (ejemplo, acceso a bases de datos); para este efecto se debe cumplir con el acceso mediantes nombre de usuario y contraseña, factor que asegura el acceso a la red; siendo el caso de un no correcto ingreso de la identificación no se permitirá el ingreso a los sistemas de información y se registrará las características del dispositivo.
- ✓ El dispositivo cuenta con todos los parches de seguridad críticos del sistema operativo instalados.
- ✓ El dispositivo está configurado correctamente para permitir el acceso remoto para posible soporte y ayuda por parte del departamento de TI.

- ✓ El dispositivo debe prestar las facilidades para levantar una conexión VPN si así se lo requiere.
- ✓ El departamento de TI se reserva el derecho para evaluar, borrar información de forma presencial o remota en caso de que el empleado ha sido despedido o situaciones similares que causen que el dispositivo ya no preste servicio y no use los recursos de la red. Este punto contempla todo tipo de información y software.

Responsabilidades del usuario

El usuario no debe tratar de cambiar o desactivar la configuración de seguridad aplicada al dispositivo por parte del Departamento de TI.

- ✓ En caso que un usuario disponga de un dispositivo de propiedad personal y que esté previamente autorizado a conectarse a los recursos de red, los sistemas de la organización; y que exista la suposición de que podría estar infectado con un virus informáticos, spyware u otra amenaza o de alguna manera podría estar comprometido con algún problema; él propietario del dispositivo debe notificar inmediatamente al departamento de TI del potencial riesgo de seguridad.
- ✓ En caso de que un usuario pierda un dispositivo de propiedad personal y que esté autorizado para conectarse a los recursos de la organización, sistemas y redes, él propietario debe notificar inmediatamente al departamento de TI, del potencial riesgo de seguridad para el que el departamento indicado tome las acciones necesarias al respecto.
- ✓ Cada vez que un usuario deja de usar los recursos de red de la organización por un período de tiempo, o deja de usar definitivamente el dispositivo personal en la infraestructura de red, previamente autorizado para su uso en la organización; el usuario debe notificar al departamento de TI que el dispositivo ya no se utilizará para conectarse a los recursos de la organización, sistemas y redes.
- ✓ Los usuarios no pueden descartar los dispositivos previamente autorizados hasta que el departamento de TI le confirme la eliminación del dispositivo de los registros ingresados en la bitácora de servicio.

Datos requeridos para la verificación y aprobación de dispositivos

Este documento debe llenarse antes que todo dispositivo de propiedad personal, vaya a ser ingresado a la red de la organización en calidad de nuevo usuario o equipo. Previo a la autorización debe ser revisado y firmado por el Gerente del Departamento de TI o Responsable a cargo del procedimiento.

Reconocimiento de la política

Este formulario se utiliza para acusar recibo de, y el cumplimiento de la política de cesantía del dispositivo en la organización.

Procedimiento y aceptación de la política

Complete los siguientes pasos:

1. Lea completo la política.
2. Firmar y fechar en los espacios provistos.
3. Devuelva una copia de este documento firmado al departamento de TI.

Firma: …….

CI: ……
Fecha: ……..

Su firma implica que está de acuerdo con los siguientes términos:

I. He recibido y leído la política, entiendo y estoy de acuerdo con el mismo.
II. Entiendo que la organización puede controlar las aplicaciones (software) y el cumplimiento de la presente política para garantizar seguridad en la red.
III. Entiendo que violaciones de la presente política podrían resultar en la terminación de contrato laboral y acciones legales contra mí persona.

FORMULARIO INGRESO DE NUEVOS DISPOSITIVOS PARA ACCESO A LA RED DE LA ORGANIZACION

Fecha de solicitud: ……..
Nombre completo (Usuario): ……
Área laboral (Usuario): …….
Teléfono trabajo (Usuario): …….
Teléfono móvil (Usuario): ……..……
Teléfono domicilio (Usuario): ……
Dirección correo electrónico (Usuario):……
Cargo que desempeña (Usuario):…….
Qué tipo de dispositivo va a conectar a la red: ……..
El usuario quiere conectarse a recursos de la organización, sistemas o redes:
……
Recursos, sistemas o redes de organización a la que el usuario desea conectarse:
……
Objetivo (tarea) de la petición: ……..

…….. …….

Firma **Firma**

Aprobación Gerente de TI. **Aprobación Responsable de proceso:**

ELIMINACION DEL REGISTRO DE USUARIO O DISPOSITIVO

Fecha solicitud de eliminación de registro (usuario): ……..
Fecha dispositivo fuera de servicio (Dept. de TI): ……

Método utilizado para descartar el usuario o dispositivo (disociar / eliminar los sistemas de la empresa, mantenimiento del sistema operativo, destrucción física, etc.):

……
.....

ANEXO 6: DVD INFORMACION

INFORMACION: Adjunta información documentos magnéticos del caso de estudio manual de usuario, manual técnico, instaladores (software) utilizados para la implementación del aplicativo PacketFence, video tutorial, imagen virtual del aplicativo en una pen-drive.