

IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE
INTRUSOS PARA LA EMPRESA DISTRIBUIDORA DE CEMENTOS DE
OCCIDENTE SEDE DOSQUEBRADAS

WILMER JAVIER PEREZ GUERRERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACION EN SEGURIDAD INFORMATICA
PEREIRA RISARALDA
2018

IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE
INTRUSOS PARA LA EMPRESA DISTRIBUIDORA DE CEMENTOS DE
OCCIDENTE SEDE DOSQUEBRADAS

WILMER JAVIER PEREZ GUERRERO

Trabajo de grado para optar al título de especialista en Seguridad Informática

JOSE ALFAIR MORALES BARRERA
DIRECTOR DE PROYECTO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
PEREIRA RISARALDA
2018

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Pereira, 8 de marzo de 2018

Dedicada a Gaby y Diana, por hacer de mi mundo, un universo.

AGRADECIMIENTOS

En primer lugar a mi familia, por darme el apoyo y perdonarme el tiempo que no he estado con ellos, a mis compañeros de trabajo y en especial a aquellos que de una u otra forma colaboraron para finalizar este ciclo.

CONTENIDO

	Pág.
INTRODUCCIÓN	9
1. PLANTEAMIENTO DEL PROBLEMA	10
1.1. DEFINICIÓN DEL PROBLEMA	10
1.2. FORMULACION DEL PROBLEMA	11
2. JUSTIFICACIÓN	12
3. ALCANCE Y DELIMITACIÓN.....	14
4. OBJETIVOS.....	16
4.1. OBJETIVO GENERAL.....	16
4.2. OBJETIVOS ESPECÍFICOS.....	16
5. MARCO REFERENCIAL	17
5.1. MARCO HISTORICO	17
5.2. MARCO TEORICO	19
5.3. ESTADO DEL ARTE	22
5.4. MARCO CONCEPTUAL	25
5.5. MARCO LEGAL.....	26
6. DISEÑO METODOLOGICO.....	28
6.2. TÉCNICAS DE RECOLECCION DE DATOS	28
6.3. TÉCNICAS DE PROCESAMIENTO DE DATOS	28
6.4. METODOLOGIA DE DESARROLLO	29
6.4.1. Etapa de análisis de debilidades y recolección de información.....	29
6.4.2. Etapa de procesamiento y tratamiento de la data recogida.....	29
6.4.3. Etapa de desarrollo y ajustes del sistema	29

7.	ESTADO DE LA RED DE DATOS.....	31
7.1.	SITUACION INICIAL.....	31
7.2.	DIAGRAMA DE LA RED	32
7.3.	POLÍTICAS DE ADMINISTRACIÓN INICIALES	33
8.	RESULTADOS.....	34
8.1.	RESULTADOS INICIALES	34
8.1.1.	Riesgos hallados	34
8.1.2.	Sistema de filtrado de contenidos y conexiones.....	36
8.1.3.	Creación de Lista de chequeo para PC.....	38
8.1.4.	Conexión inalámbrica.....	38
8.2.	RESULTADOS INTERMEDIOS.....	39
8.2.1.	Implementación de proxy	41
8.2.2.	Aplicación de políticas internas	42
8.2.3.	Administración de carpetas compartidas.....	42
8.2.4.	Resultados de verificación de vulnerabilidades.....	42
8.3.	ENTREGA FINAL	44
8.3.1.	Diagrama de la Red de datos.....	44
8.3.2.	Políticas y autorizaciones del firewall	46
8.3.3.	Funcionamiento del IDS	48
9.	DIVULGACION	51
10.	CONCLUSIONES	52
	BIBLIOGRAFÍA	53

LISTADO DE IMAGENES

	Pág.
Imagen 1. Estado Inicial de la red de datos.....	32
Imagen 2. Puertos Abiertos	35
Imagen 3. Configuración Proxy no transparente.....	41
Imagen 4. Escaneo de puertos abiertos	43
Imagen 5. Detecciones del IPS en el Hacking Ético	43
Imagen 6. Red de datos.....	44
Imagen 7. Usuarios OpenVPN.....	45
Imagen 8. Configuración Firewall salida	47
Imagen 9. Bloqueo de Paginas sociales	47
Imagen 10. Configuración Firewall ingreso.....	48
Imagen 11. Actualización Reglas IPS.....	49
Imagen 12. Conexiones activas en la UTM	49
Imagen 13. Detecciones en el IDS.....	50
Imagen 14. Zonas y Redes en la UTM	50

LISTADO DE ANEXOS

	Pág.
ANEXO A. Listado de Chequeo para equipos	55
ANEXO B. Lista de chequeo para servidores	56
ANEXO C. Formato inclusión WiFi	57
ANEXO D. Formato Instalación Proxy	58
ANEXO E. Instalación de la UTM Endian	59
ANEXO F. Configuración de UTM Endian	62

GLOSARIO

ACCES POINT (Punto de Acceso): se usa para permitir la conexión inalámbrica en una red.

DHCP (Dynamic host Configuration protocol): usado para asignar direccionamiento IP dentro de una red.

HACKERS: término usado para relacionar a aquellas personas con amplios conocimientos en el área de informática, sin embargo también es usado para identificar personajes hostiles que acceden de forma no autorizada a un computador, haciendo uso de distintas técnicas.

IP: equivale a un número que identifica al dispositivo informático dentro de una red. Puede ser fijo o dinámico, este valor lo determina el administrador de una red.

ISP (Internet Service Provider): corresponde a la empresa que se encarga de proveer el servicio de internet a una empresa o colectividad.

IT (Information technology): Tecnología de la Información (TI), es equivalente al conjunto de hardware y software que permiten almacenar, distribuir y procesar información. También se suele utilizar para describir al equipo humano que establece las operaciones de funcionamiento informático en las empresas.

NAT (Network Address Traslator): consiste en el re direccionamiento de datos desde una red externa hacia un equipo dentro de la red, para proveer un servicio específico.

P2P (Peer to Peer): es una red, en la cual no existe un administrador o servidor principal, tampoco depende de los clientes que se conectan, funciona con los dispositivos que estén en línea y habilitados para tal fin.

PROXY: cumple la función de ser un intermediario entre el proveedor de internet y el equipo que usara la conexión a internet. Suele usarse para restringir el acceso a diversos sitios.

PUERTO: es la forma de interconexión lógica o física para la transmisión de datos entre computadores.

RED INFORMÁTICA: se usa para mencionar, el enlace entre dos o más dispositivos informáticos, en la cual se puedan compartir servicios y funciones.

ROUTER: dispositivo usado para permitir conectividad entre dos redes.

SERVIDOR: generalmente, es quien centraliza la información en una entidad, suele ser el equipo informático máspreciado, por los datos allí contenidos, sin embargo hay varios tipos de servidores.

SERVICIO: son funciones que provee a nivel informático un equipo de cómputo. Existen de varios tipos y funciones, cada una configurada dependiendo de las necesidades puntuales.

SSH (Secure Shell): equivale a un protocolo y un programa de interconexión entre equipos, muy usado para la administración de servidores Linux.

VPN (Virtual Private Network): Red Privada Virtual, es la configuración de una conexión, haciendo uso de otras redes, tales como internet para conectarse a una

red empresarial, permitiendo hacer uso de los recursos disponibles como si estuviera conectado localmente.

WAN (Wide Area Network): Red de área extensa, se refiere a una red que por su cubrimiento, puede alcanzar una vasta región geográfica. En sistemas también se utiliza para determinar una conexión a internet.

WiFi: es la forma más extendida de las comunicaciones actuales, comprende conexiones inalámbricas que cumplen con un estándar (802.11)

RESUMEN

El desarrollo de este trabajo, busca ayudar a disminuir los problemas de seguridad informática, que se presentan en la empresa Distribuidora de Cementos de Occidente, aplicando los métodos que permitan verificar estas falencias, con la consecuente búsqueda de alternativas para la implementación de la solución y disminución de errores de seguridad.

Dentro del proceso de búsqueda de soluciones para la citada empresa, se realizó la instalación, configuración y puesta en marcha de una solución que incorpora división de zonas de conexión, protección mediante firewall y Snort para la prevención de ataques informáticos.

PALABRAS CLAVE: Seguridad informática, Ethical Hacking, software libre, UTM.

TITULO DEL PROYECTO

IMPLEMENTACIÓN DE UN SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS PARA LA EMPRESA DISTRIBUIDORA DE CEMENTOS DE OCCIDENTE SEDE DOSQUEBRADAS

INTRODUCCIÓN

Según la ley 1581 del 2012, toda empresa es responsable de la información digital que contenga datos personales o que se encuentra en sus bases de datos, por ende, cada empresa debe proteger esta data, sabiendo en primer lugar, que es el activo más valioso, y segundo, porque una alteración en la misma, puede conllevar a consecuencias legales entre las cuales se aplica la ley 1273 del 2009, la cual estipula la creación de un nuevo bien jurídico, nombrado “de la protección de la información y de los datos”¹.

Dentro del desarrollo del trabajo, se revisan los inconvenientes técnicos que se poseen en la Distribuidora de Cementos de Occidente sede Dosquebradas. Como tal, se espera encontrar la mejor forma de proteger los datos, y de buscar que aspectos se están descuidando desde la parte administrativa u operativa.

El proyecto abarca la investigación de las posibles causas que vayan en detrimento de las condiciones mínimas de seguridad informática, para un desempeño sin contratiempos, en el área de sistemas de la empresa.

¹

Encabezado de la Ley N°1273 de 2009.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. DEFINICIÓN DEL PROBLEMA

En los últimos años, y debido al auge de las comunicaciones, cada empresa está más presta a la interconexión a través del internet. Sin embargo esta misma interconexión ha aumentado el riesgo de tener inconvenientes con los datos que las empresas han atesorado durante toda su existencia. Sin embargo frente a este panorama se han venido implementando soluciones que conllevan a mejorar la seguridad y que tienden a proteger los datos existentes en la empresa.

La empresa Distribuidora de Cementos de Occidente, ubicada en la ciudad de Dosquebradas, actualmente está sufriendo inconvenientes con la administración de los recursos que se prestan en su red de datos. Estos inconvenientes están relacionados con la indisponibilidad de recursos, fallas en la conectividad, caídas o bloqueos del sistema, pérdida de información y como una consecuencia de las anteriores se considera que ha habido pérdidas de oportunidad de negocio.

Estas fallas se presentan por la falta de personal, ya sea externo o interno que pueda proveer una adecuada asesoría para la implementación de los distintos servicios que se están prestando, también porque la parte administrativa no contemplaba la seguridad informática como una necesidad de la entidad, hasta que se convence de los riesgos a los que se expone la empresa, por la falta de políticas de prevención en el área de sistemas. Dichas pérdidas de información

pueden poner en riesgo la continuidad del negocio, tal como lo afirma Kaspersky Labs en el estudio realizado a más de 5.500 empresas en más de 26 países².

En vista de lo anterior, se ha propuesto buscar alternativas que ayuden a resolver esta situación, y es en este momento, donde se ingresa a analizar los distintos problemas que existen y buscar las alternativas de solución para los mismos.

1.2. FORMULACION DEL PROBLEMA

¿Cómo garantizar la seguridad informática al interior de la organización mediante el uso de un IDS en la empresa Distribuidora de Cementos de occidente?

² El coste real de la pérdida de datos en la empresa.

2. JUSTIFICACIÓN

Toda empresa debe propender por la protección de la información, que se genera dentro de ella, por varias razones, la primera sería la legal, puesto que la ley de Habeas Data o Ley 1581 de 2012, expone que la información que se almacena y que pueda contener datos personales de terceros, debe ser respaldada y protegida. Para preservarla, deben implementarse controles sobre los diversos dispositivos a los que se les está permitiendo el ingreso o si estas conexiones son de alguna forma validadas por el personal de sistemas de la empresa.

Los ataques a la información, pueden provenir tanto de ataques internos como externos, y la combinación de estos dos elementos, pueden ser extremadamente peligrosos, por lo tanto es requisito, protegerse en todos los aspectos. Un aspecto a considerar será como blindar nuestra información, empezando con el establecimiento de políticas de administración y manejo de los datos, las cuales corresponden a protocolos o lineamientos enfocados en ayudar a la protección informática. Dichas políticas se encargan del aseguramiento de la información para que la mencionada data esté protegida, tanto ante una pérdida provocada por daños en el hardware de los equipos, por software, el cual puede ser provocado por virus o software malicioso, así como de una extracción de información, valiéndose de técnicas informáticas abusivas.

El desconocimiento de los posibles riesgos, no son excusa para no protegerlos, además se estaría incumpliendo los dictámenes de ley, los cuales pueden ser puestos a prueba, en el caso de un requerimiento por las entidades de control estatales, en la presentación de información solicitada por ellas, inclusive los mismos socios de negocio o directivos de la entidad, pueden requerir datos que hayan estado involucrados en alguna pérdida de información. En el caso de una extracción de datos, existe la posibilidad de divulgarse información sensible y que comprometa la continuidad de negocio. Adicionalmente las empresas son

responsables legalmente de los datos que se almacenan, y estas bases de datos, están protegidas por la Ley 1268 de 2008. Estos datos deberán ser protegidos y en caso de fugas, la entidad deberá responder legalmente ante la información filtrada y que comprometa datos de terceros.

Sin embargo, la preocupación ante los problemas legales, o las diversas implicaciones que una pérdida o filtración de datos pueda conllevar, pueden ser solucionadas, si existen planes tendientes a que la información este protegida.

Estas razones han motivado a que dentro de la empresa Distribuidora de Cementos de Occidente, se logre la implementación de algún mecanismo que ayude a proteger toda la data que se maneja, pues en la actualidad se está presentando una problemática relativa a la seguridad informática y se precisa una solución que conlleve a resguardar la preciada información.

3. ALCANCE Y DELIMITACIÓN

El alcance del proyecto es la implementación de un sistema que ayude a solucionar la problemática de conectividad que se presenta en la entidad, así como garantizar que las conexiones que se realicen, estén de alguna forma controladas.

Este proyecto estará restringido al análisis de la seguridad perimetral de la entidad, excluyendo las bases de datos de la entidad tales como los programas contables, de inventario, de gestión humana y demás aplicaciones en los que la entidad base su funcionamiento. Se vinculará la parte de conectividad WiFi, puesto que se retirara la conexión existente, y cambiando su punto de acceso existente, al crear una red alterna que permita aislar las conexiones de los dispositivos móviles tanto foráneos como propios.

La solución está enfocada en la atenuación de posibles ataques externos, mediante la implementación de una aplicación IDS/IPS, la cual verificara las conexiones desde y hacia la entidad.

La sede principal está en el desarrollo del proyecto y solo se vinculan la sede alterna y los agentes comerciales, para el caso de las diversas conexiones a que haya lugar y que requieran acceso haciendo el uso de enlaces a través de la VPN o soluciones en las que se facilite la conectividad a través de la red WAN.

El tiempo estimado para la aplicación del proyecto es de aproximadamente 2 meses, tiempo en el que se desarrollaran las pruebas preliminares para la

obtención de los datos requeridos en la formulación de las diversas reglas que se necesitan para la adecuación final del sistema.

Paralelamente a la creación de este documento se llevan a cabo las actividades necesarias para la ejecución de la solución final.

Se excluye dentro del tratamiento del análisis de seguridad la página web y el correo, puesto que estos se encuentran externos a la entidad y no se permite la realización de pruebas de penetración por el proveedor del servicio.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Implementar un IDS/IPS como mecanismo de control de seguridad informática haciendo uso de software libre, en la empresa Distribuidora de Cementos de Occidente sede Dosquebradas.

4.2. OBJETIVOS ESPECÍFICOS

Levantar información del estado actual de la red de datos de la empresa Distribuidora de Cementos de Occidente buscando encontrar las posibles vulnerabilidades en el ámbito de la seguridad informática.

Hacer uso de ethical hacking para realizar un diagnóstico del estado actual de seguridad de la red de datos de la empresa Distribuidora de Cementos de Occidente sede Dosquebradas

Implementar una herramienta informática que ayuden en la protección de la información, en la red de datos de Distribuidora de Cementos de Occidente sede Dosquebradas

5. MARCO REFERENCIAL

5.1. MARCO HISTORICO

Desde los inicios de la era informática, se han venido presentando violaciones a los diferentes servicios de sistemas, en busca de portales que permitan acceder y en algunos casos, tomar el control de los mismos. Estos agujeros de seguridad, al principio eran subsanados por el personal de TI, posterior al encontrarse el daño, sin embargo con la creciente conectividad, cada vez es mayor la cantidad de ataques a los sistemas. Como una medida de prevención en las empresas, fueron instalados dispositivos de control, basado en reglas de permisos, si algo no estaba prohibido, estaba autorizado. Estos dispositivos fueron los firewall. Este elemento ha cumplido su tarea relativamente bien, sin embargo, al presentarse ataques, lo que realiza el equipo de TI es endurecer las reglas, pero siempre quedan brechas faltantes por cubrir, y cada día, surgen nuevas vulnerabilidades en los programas que a diario utilizamos.

Las constantes intromisiones a los sistemas, hicieron pensar a analistas de seguridad como Dorothy Denning y Peter Neumann, quienes durante los años 1984 a 1986, buscaron y desarrollaron el primer modelo de IDS denominado IDES - Intrusion Detection Expert System, basado en reglas orientadas a determinar el origen de los ataques. Este primer acercamiento a la detección de la actividad maliciosa, fue el origen de un continuo avance para frenar o disminuir el volumen de ataques a las redes actuales.

Según empresas como ESET Latinoamérica y Frontech Ltda, dedicadas a evaluar el riesgo informático, y quienes presentaron un informe³ relativo a la seguridad informática en el nivel corporativo, en el cual se especifica que en Latinoamérica existe un alto porcentaje de ataques y que estos puedan provocar pérdidas informáticas. En el mismo informe, se menciona que al menos un 20% de las empresas han recibido algún tipo de ataque, especialmente fraudes. Como tal, las empresas, han decidido invertir en la seguridad informática, sin embargo, el ritmo de inversión es muy lento comparado con el nivel de aumento de los posibles ataques a nivel mundial, tal como lo describe Kaspersky Labs⁴ en su informe del año 2016. Algo que en Latinoamérica, se aprecia mucho por el concepto errado, de suponer que a las empresas pequeñas nunca le atacaran los hackers o que simplemente, no serían blancos de ataques⁵.

Sin embargo, los recientes estudios demuestran que las empresas pequeñas, son el nuevo blanco de los ataques, basados en la sencilla razón que invierten menos en la seguridad, tal como lo muestra Inc.com en su publicación “The Big Business of Hacking Small Businesses”, en la cual mencionan que el nuevo destino de los ataques son las empresas con menos de 100 empleados, y así también lo muestra The New York Times, en su publicación del 26 de enero del 2016, “Las empresas pequeñas tampoco se salvan de los ‘hackers’⁶”

Como tal, la seguridad informática, se ha vuelto un requisito indispensable dentro del departamento de TI de las entidades. Y esa ha sido una de las razones para que en la actualidad, existan varios proyectos en desarrollo, tales como Fortinet,

³ ¿Cómo está Latinoamérica en temas de seguridad informática? <https://arandasoft.com/como-esta-latinoamerica-en-temas-de-seguridad-informatica/>

⁴ Kaspersky Labs rastrea más de 100 campañas maliciosas complejas contra organizaciones comerciales y gubernamentales alrededor del mundo. https://latam.kaspersky.com/about/press-releases/2016_kaspersky-lab-rastrea-mas-de-100-campanas-maliciosas-complejas-contra-organizaciones-comerciales-y-gubernamentales-alrededor-del-mundo

⁵ ¿Por qué los hackers quieren atacar tu pequeño negocio? <https://einformatico.com/los-hackers-quieren-atacar-pequeno-negocio/>

⁶ Las empresas pequeñas tampoco se salvan de los 'hackers'. <https://www.nytimes.com/es/2016/01/28/las-empresas-pequenas-tambien-pueden-ser-hackeadas/>

Snort, Endian, IpCop, SmothWall, PfSense y otros más, que buscan resolver estos inconvenientes de seguridad, cada uno inicialmente enfocado en desarrollar soluciones haciendo uso de software libre y luego convirtiéndose al sector privado como es el caso de Endian, el cual maneja la opción de software libre dando soporte a través de la comunidad que lo desarrollo o la versión Pro, la cual incluye un soporte especializado junto con la adquisición de la solución. Otro caso es SimpleWall, el cual permite hacer uso de su solución de una forma libre, sin embargo el soporte tiene un costo por hora de US\$35.

5.2. MARCO TEORICO

Cuando se habla de proteger los datos, se tiende a confundir dos expresiones: seguridad de la información y la seguridad informática.

En sí, la seguridad informática se dedica a disminuir los posibles riesgos de pérdida o alteración de la información almacenada en equipo electrónico, mientras la seguridad de la información cubre toda la información de la compañía.

Como tal, el proceso que nos interesa es proteger la información almacenada en dispositivos electrónicos, así que se requiere determinar los medios o procesos utilizados para alcanzar esta meta.

Dentro de los dispositivos asociados a la protección, y que son un punto inicial para detener los ataques o prevenirlos, están los firewall, los cuales son un conjunto de reglas que permiten o restringen la conexión desde o hacia los equipos protegidos por este dispositivo.

Un firewall, en su configuración estándar, permitirá todo el tráfico que exista en la red, sin embargo bloqueara solo lo que dentro de sus reglas este acordado. Junto a este dispositivo se requerirán otros elementos que ayuden a proteger los datos, como tal, el firewall es un excelente defensor, sin embargo no es el dispositivo final que protegerá una red de datos.

Para ayudar en esta gestión se requiere de dispositivos como el IDS (Intrusion Detection Systems), el cual analiza los datos que fluyen por la red y determina si son considerados amenazas o tráfico normal. El IDS genera informes, relacionando estas amenazas y queda a disposición del equipo de TI, la aplicación de políticas necesarias para disminuir o frenar estos procesos.

La ventaja de instalar un IDS, es que a diferencia del firewall, este analiza el comportamiento de la red, y dado que actualmente se tiene conectividad para cualquier dispositivo en las empresas, puede introducir un gusano informático y propiciar una infección, este tipo de inconveniente no podría ser resuelto por un firewall, ya que este solo se encarga del filtrado de datos en el ingreso, una vez dentro de la red, el firewall es inservible.

Ante estos eventos, la detección de las incidencias en la red, empieza a cobrar más importancia, pues no solamente se precisa custodiar el ingreso de datos desde el exterior, sino también los posibles riesgos que puedan causar los equipos foráneos que ingresan a la red, o inclusive los equipos propios en los cuales se pueda filtrar un software maligno. Sin embargo la detección solamente no es importante, se requiere la acción para generar la protección informática. Esta demora en la implementación de la solución, podría ser considerada una desventaja, sin embargo, la acción se haría sobre un problema puntual, favoreciendo la fluidez de los datos.

Una solución más agresiva en el control de amenazas es un IPS (Intrusion Prevention Systems), esta reacciona ante los diferentes comportamientos en la red, aplicando reglas que bloquean estos eventos detectados como amenazas.

Los IPS funcionan de varias formas, una de ellas es por detección de comportamiento irregular, es decir, supervisan la red en espera de posibles escaneos de puertos, u otras actividades que no se consideren normales en una red, aunque aparentemente es la forma ideal, puede generar inconvenientes al detectar muchas actividades como posibles ataques, en esta forma de operación se puede manejar en modo aprendizaje para que el IPS, reconozca el modo normal basado en estadísticas, o con patrón establecido por el administrador de TI.

Una segunda forma de operación, es similar al funcionamiento de los antivirus, es decir con cadenas reconocidas de ataques, denominadas firmas, las cuales serán buscadas por el IPS y generarán las contramedidas necesarias.

Por último, la configuración del dispositivo puede ser por políticas, en este caso, las reglas deberán ser muy específicas para permitir la conexión con los diferentes dispositivos en la red, de lo contrario serán rechazadas y tratadas como amenazas.

Aunque la opción aparentemente recomendable sería la implementación de un IPS, se debe tener en cuenta que este tipo de solución, va a detectar los denominados falsos positivos, es decir detectar tráfico legítimo como tráfico maligno y viceversa (denominados falsos negativos). También, es preciso establecer un buen equipo y que opere dentro de las mismas velocidades de la conexión de la red, de lo contrario, este se convertiría en el cuello de botella, al estar analizando el tráfico y congestionando la red.

5.3. ESTADO DEL ARTE

La empresa de hoy en día, esta de una u otra forma viviendo en la era digital, por ende, su información más valiosa comienza a residir en los computadores y sus sistemas de información, los cuales, son usados para el desarrollo de su actividad comercial. Estos datos, que pueden ser desde archivos contables hasta ofimáticos, son igualmente importantes, y requieren de igual atención, ya que en caso de pérdida, se deberán realizar nuevamente, con el consiguiente costo de tiempo y retrasando o paralizando otros procesos.

La seguridad de la información consiste básicamente en respaldar o resguardar la información que se maneja al interior de una empresa o de un particular, las formas de protección van desde copias hasta medidas de evitar que personal no autorizado haga uso de ellas. Asegurar la información es equivalente a evitar su deterioro, ya sea por mal uso, por falta o no aplicación de políticas que se encarguen de gestionar el correcto uso de la data. Dice la asociación española para la calidad (s.f.) que “La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.”

La información que se resguarda es toda la producida en la empresa, ya sea física o lógica que exista en ella. En la seguridad de la información, los principios fundamentales precisan que la información esté disponible, de forma íntegra y confidencial, por lo tanto, se requiere que haya mecanismos de protección, tanto lógicos como físicos. Dentro de las protecciones lógicas, está la encriptación que ayuda a mantener un poco más segura la información.

Esta protección también incluye restricciones físicas a los centros donde se

almacena la información, y que este lugar también se encuentre asegurado contra fallas energéticas, inundaciones y demás posibles acciones que puedan corromper su contenido como los desastres naturales.

Una vez definida la importancia que se requiere dar a los datos, es menester determinar cómo protegerlos. Los archivos que están en los computadores de una empresa, son importantes por muchas razones: equivalen al trabajo desarrollado por las personas que laboran allí, son requeridos para conocer el avance de un proyecto, demuestran el estado de un convenio o contrato o son simplemente el resultado de una labor. Sea cual fuere su origen, estos datos serán requeridos en algún momento y deberán estar disponibles en el estado en que sus autores lo plasmaron. Si estos datos son plausibles de modificación o destrucción, el riesgo al que la empresa se enfrenta es muy alto y puede ocasionarle pérdidas tanto económicas por sanciones, la pérdida de oportunidad, o conducirla al cierre por la pérdida de información.

La Seguridad Informática en cambio, es los mecanismos que se implementan dentro de una organización para evitar el acceso de terceros no autorizados en la manipulación de los datos, aunque aparentemente son similares, el uno protege la información usando mecanismos y como ejemplo citaremos la creación de copias de respaldo, mientras que el segundo se encarga de velar por los procedimientos que aseguran esta data, es decir evitar que los datos a ser respaldados puedan ser alterados tanto en su parte original como en la copia.

Para conocer que tan frágil o robusta es la seguridad informática, se requieren hacer pruebas que permitirán establecer que tan factible puede ser comprometer la integridad de los datos que circulan en la red de una empresa. En estos casos

se hace uso de técnicas que dejan evidencia de las fallas a las que se está expuesta la entidad y que terminan por entregarle a la misma, una serie de recomendaciones y sugerencias para solventar este hecho.

Este mecanismo se denomina Ethical Hacking, y según la revista Enter.co "...es una herramienta de prevención y protección de datos..."⁷, en la que una empresa es verificada en sus posibles puntos débiles para buscar la seguridad de los datos y evitar inconvenientes informáticos.

Como tal el procedimiento se encarga de verificar que tan accesible podría estar la información para un tercero, que este en busca de falencias de seguridad, y que permitan explotar estas debilidades para obtener acceso a información sensible de la entidad. Dentro de las vulnerabilidades que se buscan son conexión de datos ya sea por redes inalámbricas, las cuales generalmente brindan acceso a toda la red; nombres de usuario y contraseñas que permitan tomar control de un servidor y dentro de este a los servicios que presta; equipos con fallas en antivirus, programas o sistemas operativos desactualizados que permitan explotar esas vulnerabilidades en busca de tomar el control y de esta forma llegar a los datos... en fin son varias las opciones que se pueden tener para acceder a la información de la entidad, la gran diferencia entre un hacking ético y una interrupción cibernética es que la primera será usada para descubrir los posibles errores de seguridad y solucionarlos antes que el segundo haga uso de los mismos problemas en detrimento de la empresa atacada.

7 El hacking ético y su importancia para las empresas, <http://www.enter.co/guias/tecnologias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/>

5.4. MARCO CONCEPTUAL

En la ejecución del proyecto se hará uso de diversos términos técnicos, los cuales se describen a continuación, para mejorar la comprensión del mismo.

Amenaza Informática: es toda posible acción u omisión que comprometa la seguridad de la información.

Firewall: Esquema de reglas o permisos que ayudan a proteger permitiendo o no el ingreso de paquetes de información a una red de computadoras.

Hacking: Acción de ingresar o de obtener privilegios especiales dentro de un sistema informático, valiéndose de técnicas de programación o buscando errores que permitan acceder u obtener estos permisos.

Hacking Ético: o Ethical Hacking, equivale a buscar, previa autorización de la empresa, las posibles vulnerabilidades que se tenga en el área de informática.

IDS: Sistema de detección de intrusos, utilizado como herramienta para determinar si existen comportamientos sospechosos dentro de las posibles amenazas informáticas a una red de computadores.

IPS: Sistema de prevención de intrusos, a diferencia del anterior, este dispositivo se encarga de tomar acciones frente a comportamientos sospechosos dentro de una red de computadoras.

Pruebas de Penetración o Pentesting: Procedimientos utilizados para averiguar qué tan frágil o endeble es la seguridad informática en una organización.

Red pública: Se entiende por las redes que existen disponibles en zonas de gran afluencia de personal que permiten conexión sin discriminación de seguridad. Cualquiera puede conectarse y usar la red.

Red Privada: Al contrario de la pública, en esta se requiere permiso para conectarse, ya sea de forma alámbrica o inalámbrica.

Seguridad de la información: Mecanismos que se encargan de salvaguardar la información que exista dentro de una entidad.

Seguridad Informática: Procedimientos establecidos para prevenir la alteración, divulgación o manipulación indebida de la información que puede pertenecer a una persona o entidad.

UTM: Unidad de tratamiento de Amenazas, es un compendio de diversas funciones, dispuestas de tal forma que proveen de varios servicios a una red, haciéndose todo esto desde un solo equipo.

VPN: Red Privada Virtual, es un mecanismo que facilita asegurar la información, para poderla transmitir haciendo uso de canales públicos como lo es el internet.

WAN: Red de área extensa, utilizada normalmente para definir la conexión hacia internet.

5.5. MARCO LEGAL

Dentro de las regulaciones que existen para el cuidado de la información, está la ley 1273 de 2009, la cual vincula dentro del código penal la identificación de los delitos contra la información y el tratamiento de datos, imponiendo penas privativas de la libertad, que van desde los 3 meses hasta los 6 años.

Dentro de esta ley, se tipifica el delito de “OBSTACULIZACION ILEGITIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACION”⁸, algo que se está evidenciando en la red, al tenerse problemas de comunicación y que se considera según los análisis realizados, puede ser consecuencia del descontrol por la popularidad de las claves del acceso inalámbrico.

Sin embargo, bajo el amparo de esta ley, de descubrirse el causante, es factible iniciar un proceso legal, lo que conlleva un largo proceso de recolección de pruebas y que en muchos casos terminan sin resolver, pues el atacante desaparece sin dejar mucho rastro.

También dentro de los datos que se requieren proteger, están las bases de datos que contienen listados de personas junto a sus datos más relevantes a nivel comercial, es por esto que la Ley 1581 de 2012 o habeas data, recomienda mantener salvaguardada esta información y evitar pérdidas de sus contenidos para que sean divulgados o vendidos.

8

Ley 1273 de 2009, artículo 269B.

6. DISEÑO METODOLOGICO

6.1. TIPO DE INVESTIGACION

La investigación a desarrollar será de tipo *aplicada*, puesto que se encuentra enfocada en lograr un objetivo único y con una clara definición de sus alcances.

6.2. TÉCNICAS DE RECOLECCION DE DATOS

Se realiza, previa autorización de la entidad, recolección de posibles inseguridades, haciendo uso de herramientas de penetración informática, así mismo, se levanta el estado actual de los equipos y su nivel de compromiso con la información de la entidad.

6.3. TÉCNICAS DE PROCESAMIENTO DE DATOS

La información recolectada es utilizada para crear los métodos de protección, establecer las políticas a ser implementadas y que dispositivos realmente son requeridos para la protección de la data en la entidad.

Los datos suministrados en la recolección de inseguridades, se usan para crear un listado de chequeo, el cual se ejecuta en cada equipo, para subsanar las dificultades. Con la información de las pruebas de penetración, se preparan las diversas reglas a ser introducidas en el firewall y/o en el IDS.

6.4. METODOLOGIA DE DESARROLLO

En este documento, se pretende identificar, seleccionar y poner en funcionamiento un sistema de seguridad informático que proteja los datos de posibles ataques. Para lograr complementar este objetivo, se requiere dividir el proceso en las siguientes etapas:

6.4.1. Etapa de análisis de debilidades y recolección de información.

En este periodo se requiere hacer una valoración frente a cuales podrían ser las diversas falencias, en las que se está incurriendo en la entidad.

6.4.2. Etapa de procesamiento y tratamiento de la data recogida

En este momento se precisa identificar, catalogar y valorar los diversos riesgos que tiene a nivel informático la entidad, así mismo se precisa determinar los puntos neurálgicos de la data.

6.4.3. Etapa de desarrollo y ajustes del sistema

Para esta etapa, se planea hacer la implementación y las correspondientes pruebas determinando si la solución planteada, sirve como solución a la problemática dada.

6.5. HIPÓTESIS

Es factible la implementación de un sistema de detección y prevención de intrusos para la empresa Distribuidora de Cementos de Occidente sede Dosquebradas?

7. ESTADO DE LA RED DE DATOS

7.1. SITUACION INICIAL

La entidad ha estado implementando soluciones en el área de comunicaciones, a medida que se ha ido requiriendo nuevas prestaciones; con el fin de solventar los inconvenientes en esta área, se ha colocado un router que a su vez presta los servicios de WiFi, para los equipos móviles del área comercial y demás dispositivos que precisen una conexión a internet; por la buena fe y prestos para que los funcionarios puedan hacer uso de esta conexión se ha divulgado la clave, logrando con esta medida que la clave de la red sobrepase los límites de la entidad y se haya convertido en una red WiFi publica, con el consiguiente riesgo de la violación de seguridad a los datos y la constante falla del servicio por la cantidad de equipos conectados a la misma y al alto uso de Streaming.

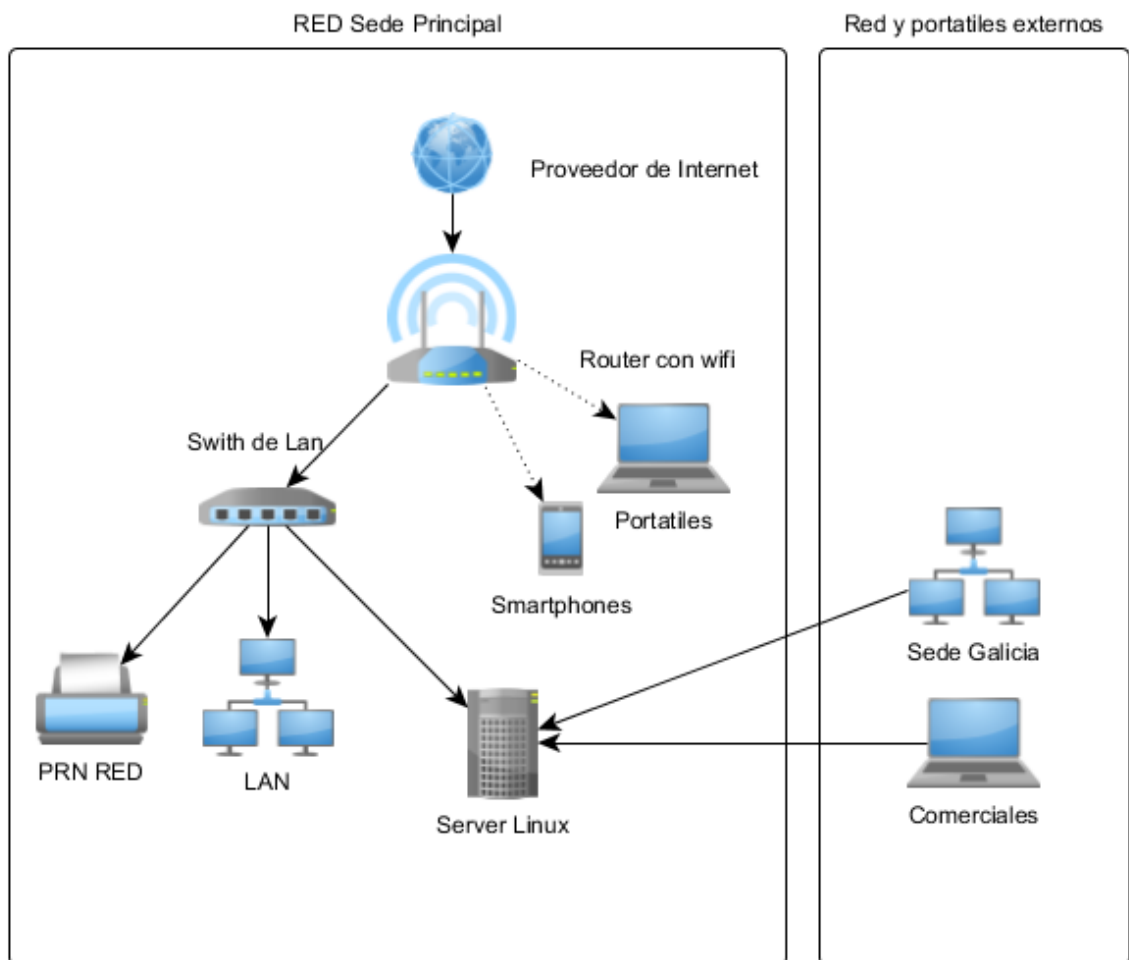
También por la instalación de una locación alterna, para atender los clientes de un sector en particular se estableció una sede adicional, esta sede requiere conexión con el servidor GNU-Linux, por lo que se habilito la apertura del puerto 22 en el router, direccionándolo hacia el servidor. Esta apertura del puerto permite la conexión del servidor con los clientes del programa contable, haciendo uso de SSH, desde la sede alterna y también para los comerciales que requieren hacer uso del software empresarial, sin embargo esta conexión está disponible para cualquier persona que conozca la dirección IP publica de la entidad, convirtiéndose en un factor de riesgo importante.

Por la misma necesidad de aprovechar la red, se comparten carpetas para que todos los usuarios puedan tener disponibles los datos que se requieran en cualquier momento. En algunos casos se encuentran compartidas las carpetas raíz para facilitar el acceso de toda la información almacenada en los

computadores. Riesgo considerado de alto impacto, al tener una conectividad de personal ajeno a la empresa.

7.2. DIAGRAMA DE LA RED

Imagen 1. Estado Inicial de la red de datos.



Fuente: El Autor

7.3. POLÍTICAS DE ADMINISTRACIÓN INICIALES

Las políticas para la administración de la información, son prácticamente inexistentes, debido a la permisividad con la que se trata la información en general. El exceso de confianza ha permitido que se haya perdido información, así como problemas con la conectividad y la estabilidad de la red, que es la razón de la implementación de una solución de red que involucre la administración en general y proporcione una estabilidad y tranquilidad para poder operar los equipos.

8. RESULTADOS

8.1. RESULTADOS INICIALES

Equipos que se conectan sin control, carpetas compartidas, contraseñas de uso público han permitido que la red de la entidad Distribuidora de Cementos de Occidente, se encuentre con fallas en la disponibilidad de recursos, bloqueos del sistema y fallas de conexión externa para la sede alterna y los equipos de los comerciales.

Como se muestra en la Imagen 1 (pág. 32), los equipos cableados se encuentran unidos con los equipos móviles, los cuales ingresan directamente a través del router entregado por el ISP y configurado con el NIT de la empresa como clave de acceso. La conexión para los equipos externos se hace a través del puerto 22, y este se encuentra direccionado al equipo servidor haciéndose uso de NAT.

Para el análisis de los riesgos, se procede con un levantamiento del estado actual de los equipos, y se hace un Hacking Ético inicial para confirmar los riesgos y detectar los posibles riesgos a los que se encuentran expuestos los diversos equipos que corresponden a la entidad.

8.1.1. Riesgos hallados

En la evaluación inicial se encuentran los siguientes problemas:

- Equipos no poseen antivirus o están desactualizados.
- El sistema operativo de varios equipos no se encuentra actualizado.
- Hay facilidad para la instalación de programas por cualquier usuario.
- Se comparten carpetas del sistema.

- Los equipos remotos acceden a través del puerto TCP 22 al servidor, por lo que el servidor se encuentra expuesto ante posibles ataques externos.
- La contraseña del ROOT, en el servidor, resulto estar dentro de un diccionario de ataque.
- Se encuentran programas para descargas por P2P en equipos que tienen privilegios para acceder al servidor.

Para la verificación de los puertos abiertos en la red, se hace uso de la página Whatsmyip.org, la cual, aparte de brindar la determinación de la IP publica, también presta el servicio de análisis de puertos que están accesibles desde el exterior.

Imagen 2. Puertos Abiertos

The screenshot shows the 'Server Port Test' interface. It features a sidebar with 'Networking Tools' and 'Text Related Tools'. The main area displays a progress bar at 100% and a 'Re-Scan' button. Below is a table of test results:

Application	Port	Status
FTP	21	Timed-Out
SSH	22	Open
Telnet	23	Timed-Out
Mail [SMTP]	25	Open
DNS	53	Timed-Out
Web Server [HTTP]	80	Timed-Out
Mail [POP]	110	Timed-Out
netbios	137	Timed-Out
netbios	138	Timed-Out
netbios	139	Timed-Out
Mail [IMAP]	143	Timed-Out
Web Server [HTTPS]	443	Timed-Out
Microsoft-DS Service	445	Timed-Out
Apple Filesharing Protocol	548	Timed-Out

Fuente: El Autor.

Se solicita a la entidad, la adquisición de un antivirus para sus equipos y la implementación urgente de un sistema de administración de conexiones. También se solicita la implementación de restricción de usuarios y la eliminación de los

programas no autorizados por la empresa y con los cuales no se tienen licencias de uso.

Como parte del trabajo de concientización en la seguridad informática empresarial, se realiza una capacitación a los usuarios, orientada hacia la minimización de los riesgos informáticos y ayudar a crear estrategias que conlleven a la implementación de políticas restrictivas consensuadas con los usuarios y evitar el caos por la instauración de las medidas de seguridad.

8.1.2. Sistema de filtrado de contenidos y conexiones

Dentro de los trabajos a ser entregados, se inicia con la implementación de una UTM, la cual contiene un firewall, servidor DHCP, servidor Proxy en modo transparente y un analizador de intrusiones dentro de sus varias funciones. Estas funciones servirán para poder disminuir los riesgos a los que se está exponiendo la empresa y filtrar los diversos riesgos hallados en la exploración de vulnerabilidades

La empresa Distribuidora de Cementos de Occidente, entrega una torre, la cual es utilizada para la implementación de la UTM, como primera instancia se usa Endian, al ser una solución completa en la parte de administración de conexión y por la facilidad de administración vía WEB, también porque involucra un IDS dentro de su configuración.

Se realiza la Instalación del dispositivo, la cual se encuentra detallada en el anexo E, igual la configuración básica se encuentra en el anexo F, y se crean los usuarios para las conexiones remotas, haciendo uso de OpenVPN. Los usuarios creados para las conexiones VPN, se listan en la Imagen 7 (Pág. 45 de este documento) En las máquinas que requieren conexión remota, se realiza la

conexión del cliente de OpenVPN, y se establecen las comunicaciones con el servidor adecuadamente.

Se cierran todos los puertos de entrada y salida, se habilita la navegación por el puerto 80 y 443, servidores de correo en los puertos 25 y 465, que son los utilizados por el proveedor del servidor de correo, y se restringe la salida del servidor que alberga el programa de contabilidad hacia internet para evitar posibles infecciones y ataques. Estas configuraciones del firewall, se encuentran detalladas en la Imagen 8 (pág. 47). Para la verificación del resultado correcto de estas configuraciones, se utilizó el servicio que provee la página web, en la cual se puede hacer un análisis de puertos. El resultado de este servicio se encuentra en la Imagen 4 (pág. 43)

Los resultados encontrados después de una semana de operación del firewall, son positivos, se ha reducido la desconexión de los equipos remotos hacia el servidor y por el momento la velocidad de operación ha sido satisfactoria. Cabe resaltar que se ha desactivado las conexiones inalámbricas mientras la entidad provea un Acces Point para administrar adecuadamente las conexiones por dispositivos móviles.

Como alternativa para la solución, es la inclusión de una tercera tarjeta de red y usar la UTM como administrador de conexiones inalámbricas. Los reportes de intrusiones que trae la UTM, se han saturado con los intentos de conexión de los diversos programas que buscan una conexión P2P o torrent. Se ha procedido de acuerdo a los resultados emitidos, a buscar las maquinas por la dirección IP y desinstalar los programas que causan estos inconvenientes.

8.1.3. Creación de Lista de chequeo para PC

Con la información recolectada, se procede a crear una serie de parámetros que deberán cumplir los computadores de la entidad. Este procedimiento se encuentra en los anexos y corresponde al anexo A.

En el caso de los servidores, también es preciso resolver algunos inconvenientes y por esta razón se creó una lista de chequeo similar, aunque es exclusiva para los servidores. Esta segunda lista se encuentra en el anexo B.

Con la aplicación de estas listas de chequeo se han reducido los reportes de intrusiones causados por software de descarga y los agentes de conexión para nubes públicas como Dropbox, Drive, Sky o Mega, los cuales son considerados como posibles violaciones a la seguridad corporativa por la posible facilidad para extraer datos de la entidad.

La entidad esta consiente de la necesidad de un antivirus para ayudar en la protección de los activos lógicos, y se están evaluando los diversos proveedores que suplirán esta necesidad.

8.1.4. Conexión inalámbrica

Debido a que varios de los empleados, especialmente el área comercial, hace uso de dispositivos móviles, es necesaria la implementación de algún medio que les permita la conexión de una forma segura, por lo que se plantean dos alternativas:

- a. Instalación de un portal cautivo: Como principal ventaja, está la asignación de usuarios y contraseñas, pudiéndose establecer el tiempo que duraran los mismos. Como desventaja, existe el hecho que se pueden filtrar los usuarios y contraseñas a terceros.

- b. Conexión por la UTM: aparte de la ventaja económica, la cual es el ahorro en la compra del equipo del portal cautivo, la ventaja en la seguridad, es que se puede filtrar la conexión de los dispositivos autorizados, haciéndose validación por MAC, ante esta validación, no importa si se filtra la clave de conexión, pues solo permite la conexión a dispositivos habilitados.

La opción tomada por la entidad es utilizar la administración de las conexiones inalámbricas a través de la UTM, la cual es marcada como la zona Azul. Dentro de esta zona se permite la conexión de las máquinas que previamente han sido registrados por el equipo de TI de la entidad, para los usuarios que requieren conexión hacia el servidor o Zona Verde se puede hacer de dos formas, habilitar reglas que permitan el tráfico de esa IP hacia el servidor o usar la VPN.

Como una forma de llevar el control de los equipos autorizados se diseñó una tabla donde se consignan los datos del usuario y del equipo que se planea incorporar. Este formato se incluye como anexo C.

Teniéndose en cuenta que el personal pueda ser retirado en temporada de vacaciones o cuando dejan el cargo, el formato involucra la opción de llevar el registro de aprobación o eliminación del listado de MAC autorizadas, validando el motivo a que haya lugar.

8.2. RESULTADOS INTERMEDIOS

Como parte de la implementación de la solución se realiza una segunda revisión para determinar si la solución provista está reduciendo los riesgos y mejorando la interconexión de la empresa y se obtienen los siguientes datos:

- La empresa ha implementado parcialmente la instalación de un antivirus, debido a una posible actualización de equipos.
- Por la misma actualización, aún se encuentran algunos equipos con sistemas operativos desactualizados y que se encuentran sin soporte por parte del fabricante del software.
- Se ha implementado la creación de usuarios administrativos y aplicación de políticas para los usuarios normales, con esto se disminuyó la instalación de software no licenciado, sin embargo, aún quedan algunos usuarios que han logrado burlar la seguridad impuesta, y han implementado la instalación de software portable.
- Dentro del software portable hallado, se encuentra ultrasurf, un programa para evadir el control del firewall.
- El uso de la carpeta publica general, se está convirtiendo en un problema a corto plazo, pues se almacena información sensible de la entidad, además que se utiliza para compartir archivos multimedia.

Debido a que algunos problemas encontrados, se refieren al comportamiento de los usuarios, se hace un llamado a la Gerencia para una nueva charla informativa con los empleados y evitar que se sigan presentando abusos por parte de los empleados, que pueden afectar la entidad.

8.2.1. Implementación de proxy

Ante los riesgos que se presentan por la utilización de herramientas informáticas que ayudan a evadir los controles, se cambia la configuración del proxy en modo no transparente, y de esta manera, bloquear los servicios de proxy anónimos. El puerto implementado es el 8083.

Se inicia el proceso de implementación del proxy, para lo cual se dispone de un formato de control en el que se anota el nombre del equipo y el usuario responsable. Este formato se incluye como Anexo D. Con la instalación del proxy configurado en modo no transparente se espera desestimular el uso de software no autorizado.

Imagen 3. Configuración Proxy no transparente

Proxy HTTP: Configuración

>> Configuración Política de acceso Autenticación Filtrado web Unirse al Active Directory Proxy HTTPS

Habilitar proxy HTTP >>

VERDE AZUL

no transparente no transparente

▼ Configuraciones de proxy ?

Puerto utilizado por el proxy *	Error de idioma *
8083	Inglés
Nombre de equipo visible usado por el proxy	Cuenta de correo electrónica usada para notificación (admin caché)
Tamaño máximo de descarga (entrante en KB) *	Tamaño máximo de carga (saliente en KB) *
0	0

Fuente: El Autor.

8.2.2. Aplicación de políticas internas

Debido a la negligencia de algunos usuarios, se solicita a la gerencia, para que a través de Gestión Humana, se realice los ajustes necesarios que ayuden a que los empleados colaboren con la aplicación de las políticas de seguridad informática.

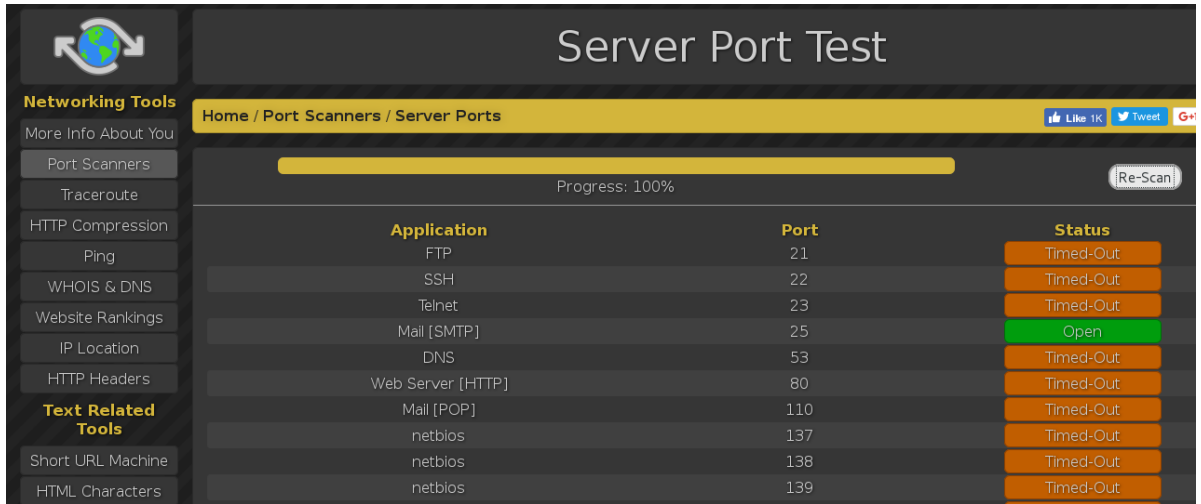
8.2.3. Administración de carpetas compartidas

Debido al volumen de información almacenado en la carpeta pública, y que en algunos casos se está manejando como almacén de información empresarial, se requiere una nueva capacitación que involucre la seguridad corporativa y los riesgos de la difusión de información que pueda atentar contra la estabilidad de la entidad. En esta charla se notifica que la información se borra todos los días en el horario nocturno, para evitar saturar el servidor con datos y explicar que la carpeta pública solo se utiliza para colocar información de la cual se tiene copia en su equipo local y que no sea calificada como sensible.

8.2.4. Resultados de verificación de vulnerabilidades

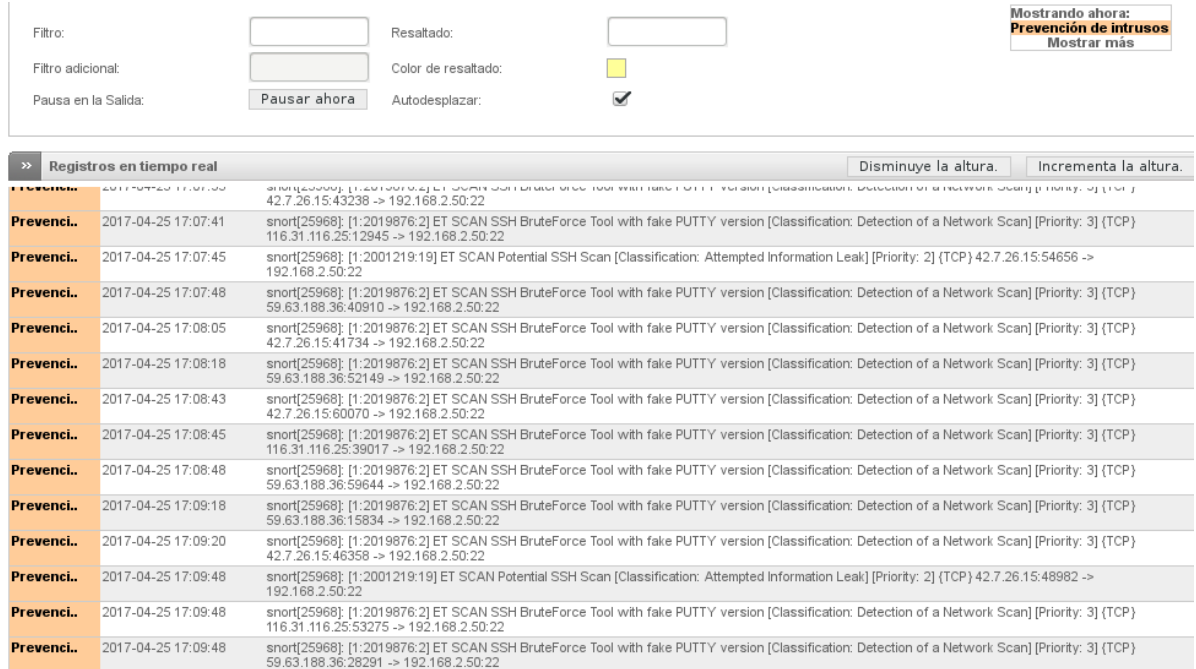
Los resultados de las vulnerabilidades, informa que se han cerrado la mayoría de vulnerabilidades, las que aún permanecen abiertas, corresponden a equipos que se planea cambiar. También como resultado de este resultado, se logra percatar que el IDS, detecta la presencia de un equipo haciendo numerosos llamados a los distintos equipos de la entidad. El equipo detectado corresponde al usado en las pruebas de penetración. Esta información la encontramos en las imágenes siguientes.

Imagen 4. Escaneo de puertos abiertos



Fuente: El Autor.

Imagen 5. Detecciones del IPS en el Hacking Ético



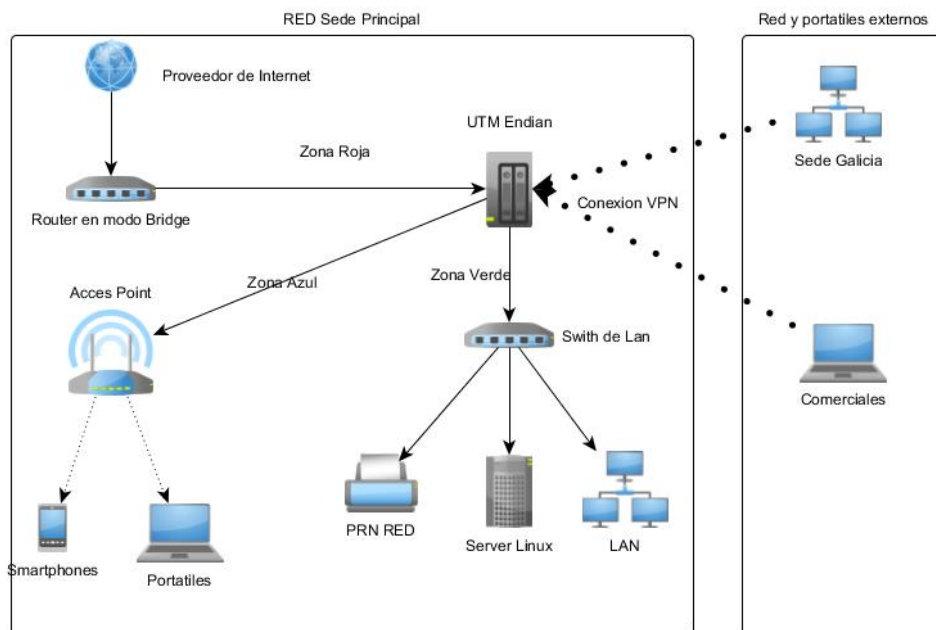
Fuente: El Autor.

8.3. ENTREGA FINAL

Con las capacitaciones, y las medidas adoptadas tanto por el departamento de Gestión Humana y el Área Técnica, se logra la aplicación de las medidas en el área informática tendientes a mejorar la seguridad de la misma.

8.3.1. Diagrama de la Red de datos

Imagen 6. Red de datos.



Fuente: El Autor

Como lo muestra la Imagen 6, la vinculación de la UTM Endian a la red, permite que esta sea la encargada de la administración de conexiones en la entidad, como primera parte se cambia la configuración del Router entregado por el ISP a modo bridge, cabe recordar que era este quien se encargaba de administrar la salida y entrada de información, así como la apertura de puertos, mismas funciones que serán asumidas por la UTM.

La UTM divide la red en Zonas: la Zona Roja equivale a las conexiones externas, la Zona Verde corresponde a los equipos que están conectados directamente al switch de LAN, también conocido como zona de confianza, y por último la Zona Azul en la que están conectados los equipos móviles.

Para los equipos externos así como para la interconexión de la red de la sede externa se utiliza OpenVPN, la cual provee el sistema de control de encapsulamiento de la información en dos formas TUN y TAP, para este caso se hará uso de TAP, puesto que permite vincular los equipos como si estuvieran en la misma red, facilitando el uso de los aplicativos de la entidad.

Como medida de funcionamiento, se requiere la creación de los usuarios, y su correspondiente configuración en los equipos cliente. El listado de usuarios se encuentra especificado en la figura 7. (Se oculta los nombres de usuarios por seguridad).

Imagen 7. Usuarios OpenVPN

Nombre	Observación	Acciones
come[redacted]	Equipo [redacted]	<input checked="" type="checkbox"/>
constr[redacted]	Local [redacted]	<input checked="" type="checkbox"/>
const[redacted]	Const [redacted]	<input checked="" type="checkbox"/>
constr[redacted]	Equipo auxiliar [redacted]	<input checked="" type="checkbox"/>
cont[redacted]	adria [redacted]	<input checked="" type="checkbox"/>
port[redacted]	equipo portatil inventarios	<input type="checkbox"/>
wit[redacted]	sistemas	<input checked="" type="checkbox"/>

Fuente: El Autor.

8.3.2. Políticas y autorizaciones del firewall

Para evitar salida de información no autorizada, se restringe puertos y se permite la salida hacia internet solo a los puertos 80 y 443 que corresponde a HTTP y HTTPS respectivamente, sin embargo, hay algunas aplicaciones de proveedores que requieren ingresar a puertos específicos y que el firewall por defecto bloquea. Estos son anexados a la lista de permitidos que se puede visualizar en la Imagen n° 8 (pág. 47). También se realiza el bloqueo de las páginas sociales que solicita la entidad, este bloqueo se encuentra en la Imagen 9 (pág. 47).

La configuración que se encuentra disponible en la Imagen 8, debido a la privacidad y seguridad de los datos de la entidad se ha borrado parcialmente la información que pueda servir para identificar una persona o la MAC de un equipo.

En la figura 10 (pág. 48), se encuentran los puertos que tienen permitido hacer una conexión directa con el servidor, bien sea porque presta un servicio concreto como el 5290 utilizado para la administración remota del servidor, el cual se mantiene desactivado para evitar posibles ataques al mismo. U otros como el 5222 que corresponde al servidor de mensajería en la entidad.

Imagen 8. Configuración Firewall salida
Configuración del firewall de salida

Reglas actuales						
#	Origen	Destino	Servicio	Política	Observación	Acciones
+ Añadir una nueva regla al firewall						
1	VERDE AZUL	ROJO	TCP/80	→	allow HTTP	↓ ✓ ✎ 🗑
2	VERDE	ROJO	TCP+UDP/2096 TCP+UDP/17500 TCP+UDP/2083 TCP+UDP/444 TCP+UDP/7005 TCP+UDP/5222	→	salida correo	↑ ↓ ✓ ✎ 🗑
3	██████████	ROJO	<CUALQUIERA>	→	permiso ██████████	↑ ↓ ✓ ✎ 🗑
4	VERDE	ROJO	TCP+UDP/465	→	allow SMTP thunderbird	↑ ↓ ✓ ✎ 🗑
5	VERDE	ROJO	TCP/993	→	allow IMAPs	↑ ↓ ✓ ✎ 🗑
6	VERDE AZUL	ROJO	TCP/443	→	allow HTTPS	↑ ↓ ✓ ✎ 🗑
7	VERDE	ROJO	TCP/995	→	allow POP3s	↑ ↓ ✓ ✎ 🗑
8	VERDE	ROJO	TCP+UDP/8282 TCP+UDP/7779 TCP+UDP/9080 TCP+UDP/8090	→	salida tributario	↑ ↓ ✓ ✎ 🗑
9	Interfaz 1	ROJO	TCP+UDP/8181	→	pagina ██████████	↑ ↓ ✓ ✎ 🗑
10	VERDE	ROJO	TCP+UDP/3389	→	salida para terminal server	↑ ↓ ✓ ✎ 🗑
11	Interfaz 1	ROJO	TCP+UDP/8080 TCP+UDP/8082 TCP+UDP/89	→	salida para ██████████	↑ ↓ ✓ ✎ 🗑
12	VERDE	ROJO	TCP/21	→	allow FTP	↑ ↓ ✓ ✎ 🗑
13	VERDE	ROJO	TCP/110	→	allow POP	↑ ↓ ✓ ✎ 🗑
14	VERDE	ROJO	TCP/143	→	allow IMAP	↑ ↓ ☐ ✎ 🗑
15	VERDE NARANJA AZUL	ROJO	TCP+UDP/53	→	allow DNS	↑ ↓ ✓ ✎ 🗑
16	VERDE	ROJO	TCP+UDP/1194	→	salida vpn	↑ ↓ ✓ ✎ 🗑
17	VERDE NARANJA AZUL	ROJO	ICMP/8 ICMP/30	→	allow PING	↑ ✓ ✎ 🗑

Fuente: El Autor.

Imagen 9. Bloqueo de Paginas sociales

19	192.168.1.0/24	50.76.50.112/28 65.201.208.24/29 65.204.104.128/28 66.93.78.176/29 66.92.180.48/28 66.199.37.136/29 66.220.144.0/20 67.200.105.48/30 69.63.176.0/20 69.171.224.0/19 74.119.76.0/22 173.252.64.0/18 204.15.20.0/22 75.125.225.163/20 31.13.73.129/20	<CUALQUIERA>	→	bloquear facebook	↑ ↓ ✓ ✎ 🗑
----	----------------	---	--------------	---	-------------------	-----------

Fuente: El Autor.

Tal como se requiere configuración del firewall de salida, se hace lo mismo con el firewall de ingreso y el correspondiente re-direccionamiento de las NAT, para los

servicios como el de mensajería, que se precisan hacer llegar las peticiones, al servidor. Esta configuración se aprecia en la imagen 10 (pág. 48)

Imagen 10. Configuración Firewall ingreso

Redirección de puertos / NAT de destino

>> Redirección de puertos / NAT de destino NAT fuente Tráfico enrutado de entrada

>> Reglas actuales

[Agrega nueva regla de reenvío de puerto / NAT de destino](#)

#	Dirección IP de llegada	Servicio	Política	Traducir a	Observación	Acciones
1	201[REDACTED]	TCP/22		192.168.2.50 : 22	ssh linux	
	PERMITIR con IP desde:			<CUALQUIERA>		
2	201[REDACTED]	TCP+UDP/5290		192.168.2.50 : 5290	webmin	
	PERMITIR con IP desde:			<CUALQUIERA>		
3	201[REDACTED]	TCP+UDP/9090		192.168.2.50 : 9090	admin pidgin	
	PERMITIR con IP desde:			<CUALQUIERA>		
4	201[REDACTED]	TCP+UDP/5222		192.168.2.50 : 5222	pidgin	
	PERMITIR con IP desde:			<CUALQUIERA>		
5	const[REDACTED] (Usuario de OpenVPN)	<CUALQUIERA>		192.168.2.61	habilitacion vpn prueba	
	PERMITIR con IP desde:			<CUALQUIERA>		
6	const[REDACTED] (Usuario de OpenVPN)	<CUALQUIERA>		192.168.2.50	const[REDACTED] impresion	
	PERMITIR con IP desde:			<CUALQUIERA>		

Fuente: El Autor.

8.3.3. Funcionamiento del IDS

Mientras que en el firewall, las condiciones de trabajo están dadas por las políticas de bloqueos, en la IDS, se configura basado en las firmas. Estas firmas son provistas por los diseñadores de la UTM y son actualizadas periódicamente, por lo que se requiere, que la UTM esté buscando estas nuevas firmas en forma regular. Se programa que dicha actualización se realice de forma diaria.

Una presentación de la configuración para la actualización de las firmas correspondientes se encuentra en la Imagen 11 (pág. 49).

Imagen 11. Actualización Reglas IPS



Fuente: El Autor

Todas las conexiones pasan por la UTM, y esta se encarga de registrar cada una de ellas, informando el protocolo que usan y las direcciones tanto origen como destino.

Imagen 12. Conexiones activas en la UTM

Conexiones

Seguimiento de las conexiones de IPTables

Legenda: LAN INTERNET DMZ Red inalámbrica Endian Firewall VPN (IPsec)

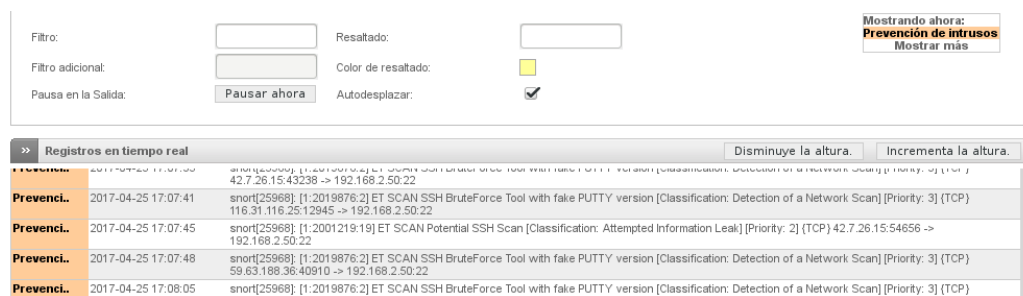
IP de origen	Puerto origen	IP destino	Puerto destino	Protocolo	Estado	Caduca
127.0.0.1	51017	127.0.0.1	6379	tcp	ESTABLISHED	119:59:59
192.168.0.101	2089	192.168.0.249	10443	tcp	ESTABLISHED	119:59:59
127.0.0.1	33745	127.0.0.1	3401	udp		0:02:57
192.168.43.194	123 (NTP)	201.49.148.135	123 (NTP)	udp		0:02:26
192.168.0.101	2088	192.168.0.249	10443	tcp	TIME_WAIT	0:01:59
192.168.0.101	2087	192.168.0.249	10443	tcp	TIME_WAIT	0:01:55
192.168.0.101	2086	192.168.0.249	10443	tcp	TIME_WAIT	0:01:54
192.168.0.101	2085	192.168.0.249	10443	tcp	TIME_WAIT	0:01:50
192.168.0.101	2084	192.168.0.249	10443	tcp	TIME_WAIT	0:01:49
10.0.0.1	4820	65.55.108.17	80 (HTTP)	tcp	SYN_SENT	0:01:48
192.168.0.101	2083	192.168.0.249	10443	tcp	TIME_WAIT	0:01:45
192.168.0.101	2082	192.168.0.249	10443	tcp	TIME_WAIT	0:01:44
192.168.0.101	2081	192.168.0.249	10443	tcp	TIME_WAIT	0:01:40
10.0.0.1	4819	65.55.2.26	80 (HTTP)	tcp	SYN_SENT	0:01:40
192.168.0.101	2080	192.168.0.249	10443	tcp	TIME_WAIT	0:01:39
192.168.0.101	2059	192.168.0.249	10443	tcp	TIME_WAIT	0:01:35
192.168.0.101	2058	192.168.0.249	10443	tcp	TIME_WAIT	0:01:34
192.168.0.101	2067	192.168.0.249	10443	tcp	TIME_WAIT	0:01:30
192.168.0.101	2066	192.168.0.249	10443	tcp	TIME_WAIT	0:01:29
192.168.0.101	2065	192.168.0.249	10443	tcp	TIME_WAIT	0:01:25
192.168.0.101	2064	192.168.0.249	10443	tcp	TIME_WAIT	0:01:24
10.0.0.1	4817	65.55.2.26	80 (HTTP)	tcp	SYN_SENT	0:01:24
192.168.0.101	2063	192.168.0.249	10443	tcp	TIME_WAIT	0:01:20
192.168.0.101	2062	192.168.0.249	10443	tcp	TIME_WAIT	0:01:19
10.0.0.1	4816	131.263.45.116	80 (HTTP)	tcp	SYN_SENT	0:01:19
192.168.0.101	2061	192.168.0.249	10443	tcp	TIME_WAIT	0:01:15

Fuente: El Autor

Así mismo, las posibles violaciones a la seguridad, quedan registradas en el IDS, advirtiendo el inconveniente y la posible causa, además de la dirección que está originando el problema.

En la Imagen 13 (pág. 50), se especifica un intento de ingreso utilizando una versión falsa de Putty (programa para acceso SSH en servidores Linux) usando la metodología de fuerza bruta.

Imagen 13. Detecciones en el IDS



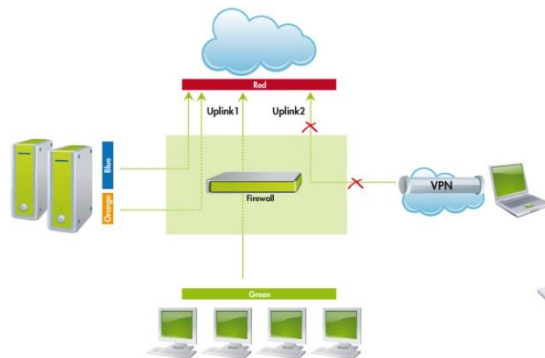
The screenshot shows an IDS interface with a search filter section at the top and a table of real-time logs below. The filter section includes fields for 'Filtro:', 'Filtro adicional:', 'Pausa en la Salida:', 'Resultado:', 'Color de resaltado:', and 'Autodesplazar:'. The table lists several intrusion events, all marked as 'Preveni.' (Prevention). The events are related to SSH brute force attacks using a fake PUTTY version.

Evento	Fecha y Hora	Detalle del Evento
Preveni.	2017-04-25 17:07:41	snort[25968]: [1:2019876:2] ET SCAN SSH BruteForce Tool with fake PUTTY version [Classification: Detection of a Network Scan] [Priority: 3] (TCP) 42.7.26.15:43238 -> 192.168.2.50:22
Preveni.	2017-04-25 17:07:45	snort[25968]: [1:2001219:19] ET SCAN Potential SSH Scan [Classification: Attempted Information Leak] [Priority: 2] (TCP) 116.31.116.25:12945 -> 192.168.2.50:22
Preveni.	2017-04-25 17:07:48	snort[25968]: [1:2019876:2] ET SCAN SSH BruteForce Tool with fake PUTTY version [Classification: Detection of a Network Scan] [Priority: 3] (TCP) 59.63.188.36:40910 -> 192.168.2.50:22
Preveni.	2017-04-25 17:08:05	snort[25968]: [1:2019876:2] ET SCAN SSH BruteForce Tool with fake PUTTY version [Classification: Detection of a Network Scan] [Priority: 3] (TCP) 42.7.26.15:44794 -> 192.168.2.50:22

Fuente: El Autor

La descripción de las distintas redes y zonas en las que se enmarca la nueva organización de la entidad, se puede apreciar en la Imagen 14.

Imagen 14. Zonas y Redes en la UTM



Fuente: Endian Firewall/ Configuración grafica de red.

9. DIVULGACION

El contenido del presente documento, junto con sus anexos, guías y resultados serán entregados de forma digital en primer lugar, a la Empresa Distribuidora de Cementos de Occidente, por facilitar la prestación de sus equipos y la aceptación de las diversas recomendaciones.

Como segunda instancia, serán entregados también de forma digital, a la Universidad Nacional Abierta y a distancia UNAD, con el propósito de ser almacenado dentro de sus repositorios para su divulgación y publicación.

10. CONCLUSIONES

- Es factible la instalación de un sistema de seguridad en la empresa Distribuidora de Cementos de Occidente Sede Dosquebradas. Como resultado del proceso se logró la implementación satisfactoria de una UTM que provee los servicios de Firewall, Proxy, Separación de Zonas de red, y un IDS.
- El levantamiento de información del estado inicial de la empresa, permitió establecer los requisitos adicionales a instaurar, como complemento de los sistemas automáticos de protección, pues el usuario es una parte importante dentro de la seguridad de la información en una entidad.
- Las metodologías usadas para determinar las falencias de seguridad, ayudaron para la generación de formatos que contribuyeron en la implementación satisfactoria de controles y políticas para la seguridad informática de la entidad.

BIBLIOGRAFÍA

Asociación Española para la Calidad (AEC). s.f. Seguridad de la información. [Citado el 10 de Noviembre de 2016]. Disponible en Internet: <<http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion>>

BRUNEAU, Guy. SANS Institute. 2001. The History and Evolution of Intrusion Detection. [Citado el 06 de Octubre de 2016]. Disponible en internet: <<https://www.sans.org/reading-room/whitepapers/detection/history-evolution-intrusion-detection-344>>

DEL CAMPO, Rubén. Nethive. 2015. El coste real de la pérdida de datos en la empresa. [Citado el 20 de marzo de 2017]. Disponible en internet <<https://nethive.es/blog/el-coste-real-de-la-perdida-de-datos-en-la-empresa/>>

El hacking ético y su importancia para las empresas. 28 de febrero de 2014. [Citado el 14 de Noviembre de 2016]. Disponible en Internet: <<http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/>>

CAMELO, Leonardo. Seguridad de la Información en Colombia. 23 de febrero de 2010. Marco legal de Seguridad de la Información en Colombia. [Citado el 26 de Noviembre de 2016]. Disponible en Internet: <<http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.html>>

GUSTKE, Constance. 2016. The New York Times. Las empresas pequeñas tampoco se salvan de los 'hackers'. [Citado el 23 de mayo de 2017]. Disponible en Internet: <<https://www.nytimes.com/es/2016/01/28/las-empresas-pequenas-tambien-pueden-ser-hackeadas/>>

PEREZ Porto, Julián y Merino, María. 2008. Definicion.de. Definición de seguridad informática - Qué es, Significado y Concepto. [Citado el 19 de septiembre de 2016]. Disponible en Internet: <<http://definicion.de/seguridad-informatica/#ixzz4PeQqEXnh>>

Rodriguez y Cairos, S.L., 2016. ¿Por qué los hackers quieren atacar tu pequeño negocio? [Citado el 14 de Agosto de 2017]. Disponible en Internet: <<https://einformatico.com/los-hackers-quieren-atacar-pequeno-negocio/>>

Universidad Nacional Abierta y a distancia. 2013. Legislación en Seguridad Informática en Colombia. Lección 30. [Citado el 10 de Noviembre de 2016]. Disponible en internet: <http://datateca.unad.edu.co/contenidos/233005/contenido%20en%20linea%20PELSI_I_2013/leccin_30_legislacin_en_seguridad_informtica_en_colombia.html>

Coltefinanciera S.A. s.f. ¿Qué es el Hábeas Data?. [Citado el 18 de octubre de 2016]. Disponible en internet: <<http://www.coltefinanciera.com.co/educacion-financiera/habeas-data>>

ANEXO A. Listado de Chequeo para equipos

Fecha de revisión _____

Consecutivo

Responsable _____

Nombre del PC _____

Dirección IP _____

Estado Actual	
Sistema Operativo _____	Service Pack _____
Actualizaciones activas _____	
Antivirus Instalado _____	Fecha de última actualización _____

Procedimiento para disminuir riesgos Informáticos			
Descripción	Realizado	Aplazado	Motivo de aplazamiento
Instalación de Actualizaciones en el sistema operativo			
Instalación o actualización del antivirus empresarial			
Eliminación de software no autorizado o no licenciado			
Eliminación de carpetas compartidas			
Redireccionamiento a carpeta pública (general)			
Creación de usuario administrativo			
Aplicación de política de permisos para usuario normal			

Observaciones

Firma Responsable Equipo

Firma Realizador Procedimiento

Fuente: El Autor

ANEXO B. Lista de chequeo para servidores

Fecha de revisión _____ Consecutivo

Responsable _____
 Nombre del servidor _____
 Direccion IP _____

Estado Actual	
Sistema Operativo _____	Subversion _____
Actualizaciones activas _____	
Antivirus Instalado _____	Fecha de ultima actualizacion _____

Procedimiento para disminuir riesgos Informáticos			
Descripción	Realizado	Aplazado	Motivo de aplazamiento
Instalación de Actualizaciones en el sistema operativo			
Instalacion o actualización del antivirus empresarial			
Revisión de carpetas compartidas			
Verificacion de Clave usuario administrador			
Verificacion de permisos usuarios regulares			
Bloqueo salida puertos WEB			
Bloqueo salida puertos no requeridos			
Verificacion de servicios adicionales			

Observaciones

Firma Responsable Equipo

Firma Realizador Procedimiento

Fuente: El Autor

ANEXO C. Formato inclusión WiFi

Fecha de solicitud _____ Consecutivo

Solicitante _____
 Cargo _____
 Identificación _____

Equipo Movil			
Sistema Operativo	_____	Service Pack	_____
Marca	_____	Modelo	_____
Serial	_____	MAC	_____

Aprobacion Red Inalambrica			
Fecha	inclusion/Retiro	Motivo	Firma de autorizacion

Observaciones

 Firma Responsable Equipo

Fuente: El Autor

ANEXO D. Formato Instalación Proxy

Fecha del procedimiento _____ consecutivo

Realizado por _____
Procedimiento a realizarse _____

motivo _____
Autorizado por _____

Usuario	Equipo	Realizado		Firma usuario
		si	no	

Observaciones

Firma Realizador Procedimiento

Firma autorizador Procedimiento

Fuente: El Autor.

ANEXO E. Instalación de la UTM Endian

En este anexo se relaciona el paso a paso de la instalación de una UTM.

Se inicia con la inserción del CD que contiene el instalador. Al arrancar muestra la selección del idioma de la instalación:



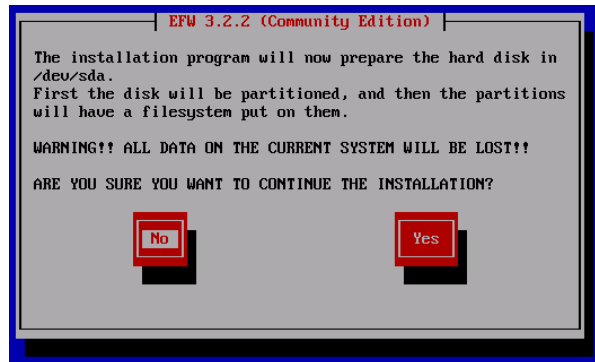
Selección de Idioma para la instalación. Fuente: El autor

Posteriormente informa que se iniciara la instalación, pero si se desea cancelarla, solo hay que seleccionar “cancelar” en cualquiera de las pantallas siguientes:



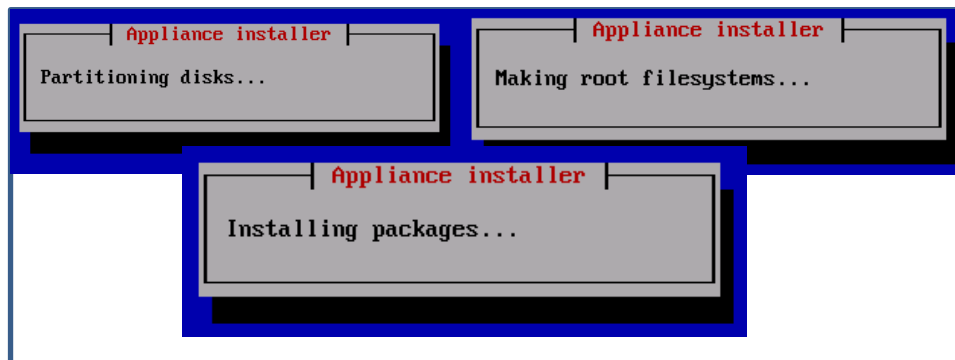
Aceptación de la instalación. Fuente: El Autor

Como consecuencia de esta instalación, se perderá toda la información existente en el disco duro. Para poder continuar se requiere la confirmación de esto:



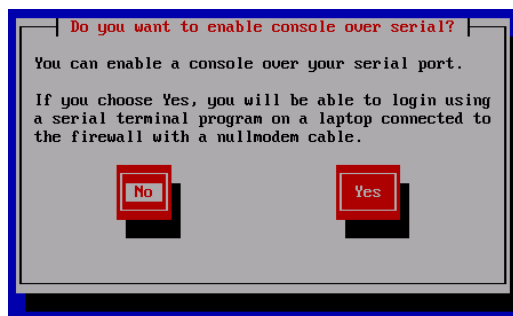
Confirmación del borrado del disco duro. Fuente: El Autor

Las pantallas siguientes informan que se están dividiendo los discos, y estableciendo la configuración necesaria para la instalación de los paquetes que hacen funcionar la UTM:



Preparación del disco y copiado de los programas necesarios. Fuente: El Autor

Dentro de la instalación, pregunta si se desea activar el acceso por SSH desde el puerto serial de la máquina. En esta ocasión se seleccionó "No".



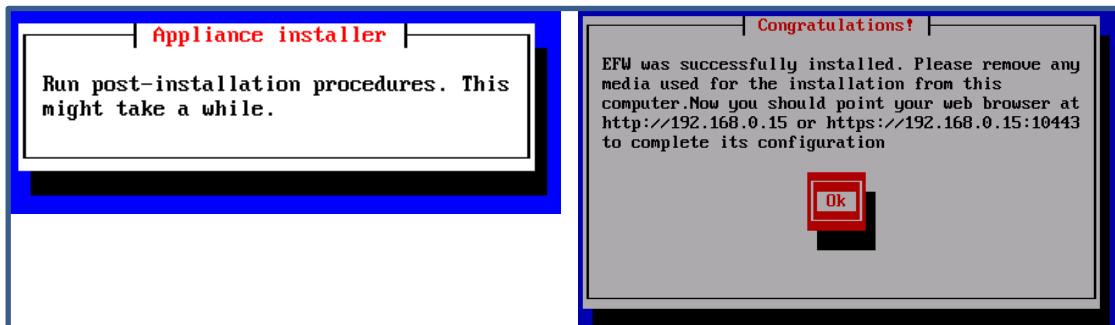
Activación puerto serial para consola. Fuente: El Autor

La configuración inicial del equipo se hace en la dirección 192.168.0.15, la cual viene pre-configurada, sin embargo en este punto es posible cambiarla por la dirección en la que trabajara la UTM, aunque se recomienda finalizar la configuración fuera de la red de trabajo para evitar trastornos operativos.



Dirección IP de acceso. Fuente: El Autor.

La Instalación ha concluido. Los pantallazos siguientes confirman esta operación y solo resta esperar que la maquina reinicie para realizar la configuración desde un terminal Web en modo grafico



Finalización de la instalación de la UTM. Fuente: El Autor.

ANEXO F. Configuración de UTM Endian

A continuación, se describirá el proceso de configuración de una UTM Endian. En primera instancia, se enciende la máquina, la cual tiene dos opciones, dentro de las cuales, se selecciona automáticamente la opción resaltada en la imagen:

```
GNU GRUB version 2.00

Endian Firewall Community release 3.2.2
Advanced options for Endian Firewall Community release 3.2.2

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
The highlighted entry will be executed automatically in 3s.
```

Pantalla de arranque de Endian. Fuente: El Autor.

Al terminar el proceso de arranque de la máquina, mostrara los datos relacionados con la dirección IP de ingreso (zona verde) y la conexión al proveedor ISP (zona roja).

```
Release: Endian Firewall Community release 3.2.2
Product: Community (64 bit)
Hostname: efw-31aa8191e1

GREEN Zone
Management URL: https://192.168.0.15:10443
IPs: 192.168.0.15/24
Devices: eth0 [UP]

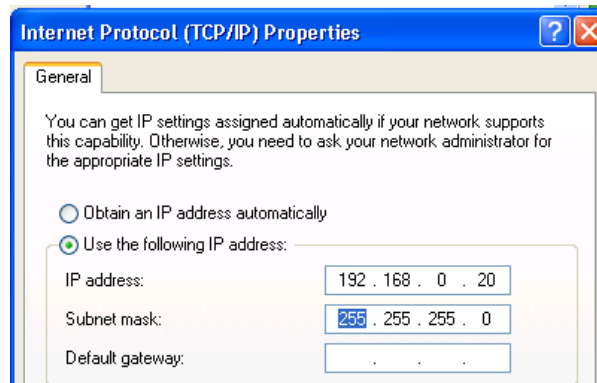
Uplink - Main [ACTIVE]
IPs: 192.168.0.15 [DHCP]
Device: eth1 [UP]

0 Shell
1 Reboot
2 Change Root Password
3 Change Admin Password
4 Restore Factory Defaults
5 Network Configuration Wizard

Choice: _
```

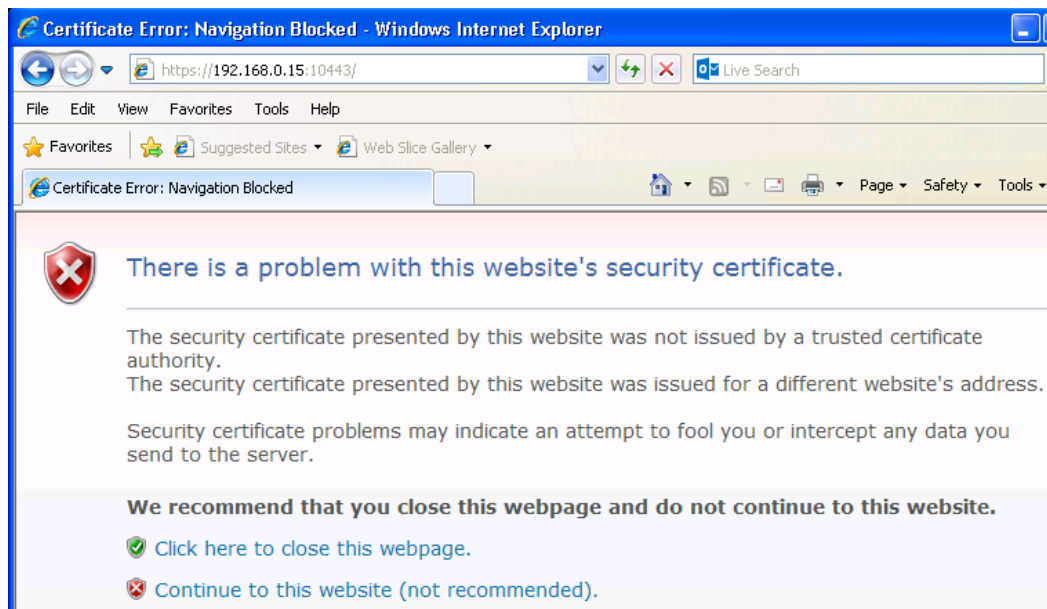
UTM lista para ser operada desde un navegador. Fuente el Autor.

Para poder acceder a la UTM, se requiere un equipo que este en el mismo segmento de red de ella, para lo cual, se configura un pc, en la red 192.168.0.0/24, y así poder gestionar toda la configuración.

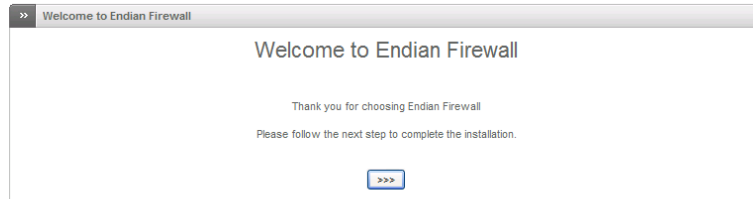


Dirección IP del equipo configurador. Fuente: El autor.

Con la dirección provista por la UTM y el equipo en el mismo segmento de red, se ingresa la dirección en un navegador web y se procede a la configuración inicial. Cabe aclarar que debido a que es una página que usa el puerto 443, se genera un error de seguridad por el certificado, puesto que la maquina Endian es el certificador de un sitio seguro, se requiere pulsar en Continuar al sitio web.



Una vez se acepta el ingreso al sitio Web, muestra la pantalla de bienvenida.



Endian Firewall Community release 3.2.2 (c) Endian

Página de bienvenida de Endian: Fuente: El Autor

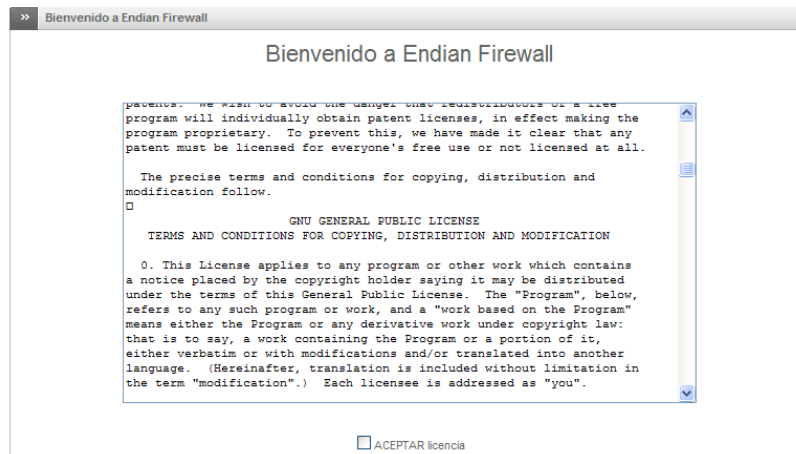
Posterior a la bienvenida, se escoge el Idioma que se va a manejar en la interface.



Endian Firewall Community release 3.2.2 (c) Endian

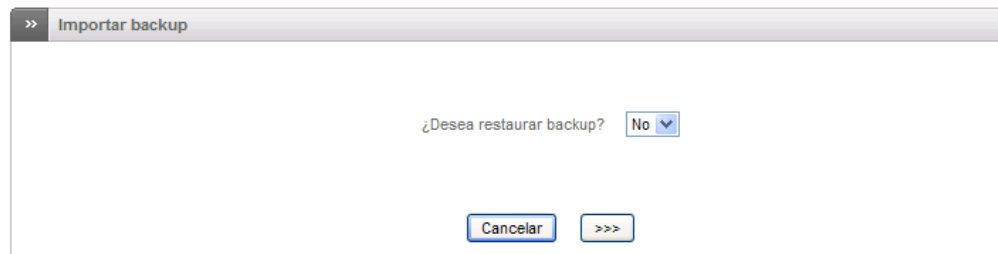
Selección de idioma. Fuente: El Autor

Como todo software, se requiere la aceptación de los términos de la licencia otorgada, posterior a su lectura, se acepta para continuar con la configuración.



Términos de licencia de Endian. Fuente: El Autor

Una vez aceptada la licencia, el asistente de configuración consulta si se desea restaurar una copia anterior, debido a que es una instalación nueva, no se tiene.



Endian Firewall Community release 3.2.2 (c) Endian

Restauración de copias de seguridad. Fuente: El Autor.

Uno de los pasos iniciales es la creación de las contraseñas de administración y root, para lo cual se deben ingresar en los recuadros adecuados. Estas contraseñas deberán ser guardadas y protegidas, evitando su publicación.

>> cambiar la contraseña por defecto

<p>Contraseña (admin) de la interfaz Web</p> <p>Contraseña *</p> <input type="password" value="••••••"/> <p>Confirmar contraseña *</p> <input type="password" value="••••••"/>	<p>Contraseña SSH (root)</p> <p>Contraseña *</p> <input type="password" value="••••••"/> <p>Confirmar contraseña *</p> <input type="password" value="••••••"/>
<input type="button" value="Cancelar"/>	<input type="button" value=">>>"/>

Asignación de contraseñas. Fuente: El Autor.

Ahora se determinaran las tarjetas de red, que administraran las diferentes zonas de la red, se empieza con la interface Roja, la cual será la conexión con el ISP.

>> Asistente de configuración de red

Paso 1/8: Seleccione el modo de red y un tipo de enlace

Modos de red

Enrutamiento
 Con puente
 Sin enlace

Enrutamiento
 Este es el modo de funcionamiento estándar. Aquí se pueden configurar enlaces de los tipos siguientes: Ethernet por DHCP, Ethernet estático, Banda ancha móvil (3G/4G), PPPoE, Módem ANALÓGICO

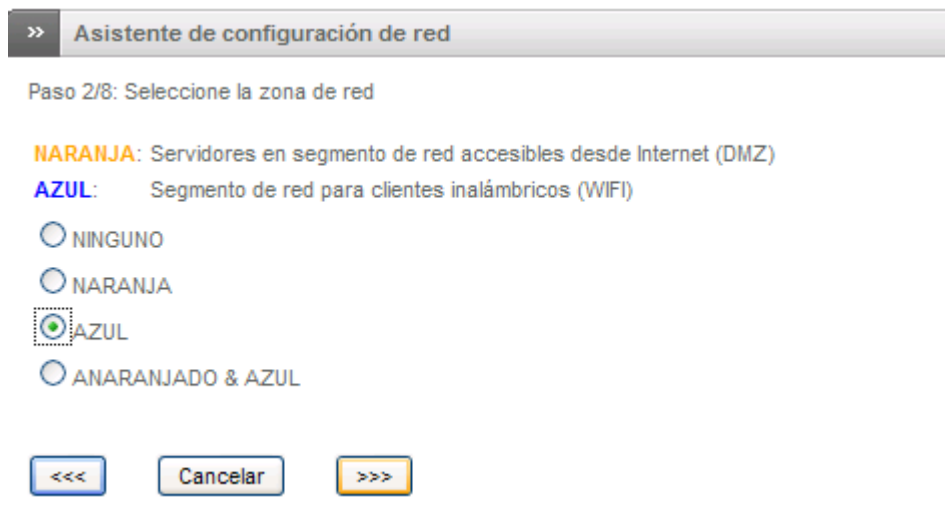
Tipo de enlace (zona ROJA)

Ethernet por DHCP
 Ethernet estático
 Banda ancha móvil (3G/4G)
 PPPoE
 Módem ANALÓGICO

Información del hardware	
Número de interfaces	3

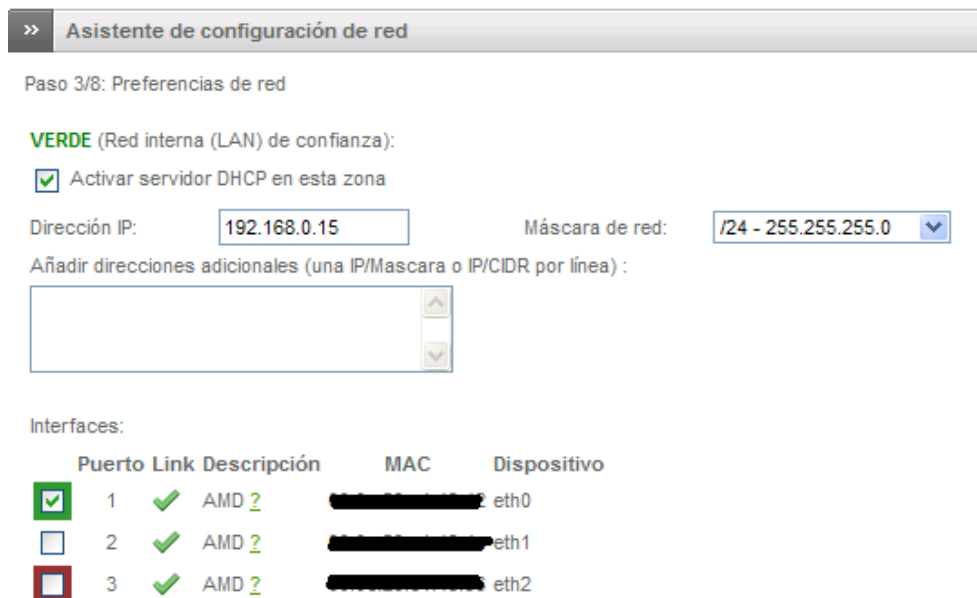
Configuración Zona Roja. Fuente: El Autor.

La siguiente zona en ser configurada es la Azul, que será asignada a los dispositivos inalámbricos.



Configuración Zona Azul. Fuente: El Autor.

Ahora se realiza la configuración de las distintas zonas y la asignación de tarjetas para cada zona. Por cuestiones de no interferir con la red, se sigue trabajando en un segmento diferente. (Las direcciones MAC se ocultan por seguridad informática)



Asignación de interface para la zona verde. Fuente: El Autor.

AZUL (Segmento de red para clientes inalámbricos (WiFi)):

Dirección IP: Máscara de red:

Añadir direcciones adicionales (una IP/Máscara o IP/CIDR por línea):

Interfaces:

	Puerto	Link	Descripción	MAC	Dispositivo
<input type="checkbox"/>	1	✓	AMD ?	██████████	eth0
<input checked="" type="checkbox"/>	2	✓	AMD ?	██████████	eth1
<input type="checkbox"/>	3	✓	AMD ?	██████████	eth2

Nombre del host:

Nombre del dominio:

Asignación de interface para la zona Azul. Fuente: El Autor.

>> Asistente de configuración de red

Paso 4/8: Preferencias de acceso a Internet

ROJO (Conexión a Internet (WAN), no fiable):

Interfaces:

	Puerto	Link	Descripción	MAC	Dispositivo
<input type="checkbox"/>	1	✓	AMD ?	██████████	eth0
<input checked="" type="checkbox"/>	2	✓	AMD ?	██████████	eth1
<input type="checkbox"/>	3	✓	AMD ?	██████████	eth2

MTU:

Ocultar la dirección MAC con:

DNS: automático manual

Este campo puede dejarse en blanco.

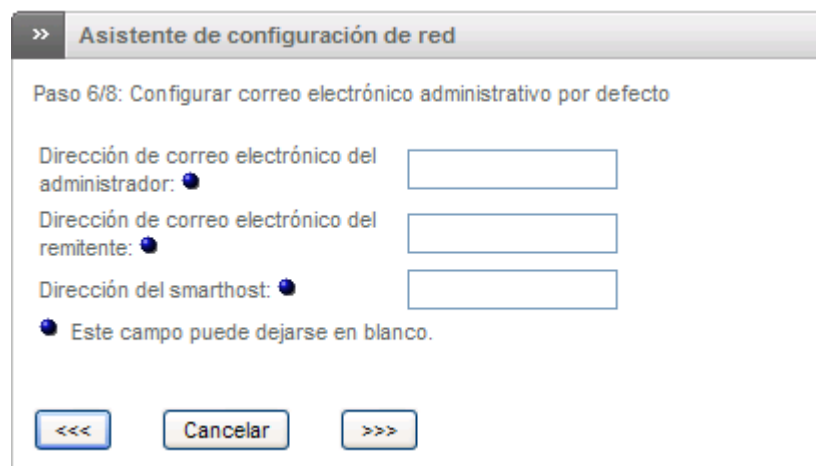
Asignación de interface para la zona Roja. Fuente: El Autor.

Para culminar la configuración, se requiere hacer la configuración de los DNS, los cuales, para el caso presente, equivale a un servicio automático, provisto por el ISP.



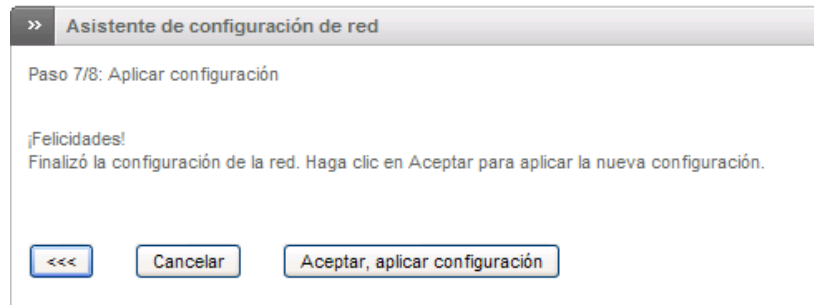
Configuración DNS Automático. Fuente: El Autor.

De requerirse, se puede configurar un correo electrónico para que el administrador pueda recibir las alertas en el correo. Sin embargo, esta función se puede configurar después, en caso de ser requerida.

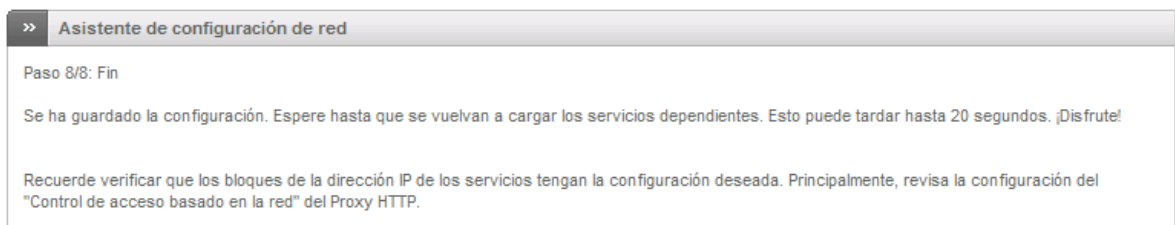


Configuración del correo de alertas. Fuente: El Autor.

Como paso final, se requiere aceptar la configuración que se ha dado y reiniciar la máquina.

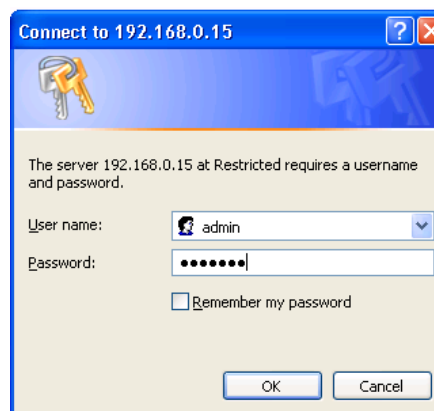


Configuración inicial concluida. Fuente: El Autor.



Reinicio del equipo con los datos ingresados. Fuente: El Autor.

Una vez el equipo ha reiniciado, se ingresa digitando las credenciales necesarias.



Ingreso al portal Web de administración. Fuente: El Autor.