DISEÑO DE SEGURIDAD DE FIREWALL PERIMETRAL PARA LA ORGANIZACIÓN CLINICA BARRAQUER

PAULA LEON RIVEROS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
PROYECTO DE SEGURIDAD INFORMATICA II
BOGOTA D.C.
2018

DISEÑO DE SEGURIDAD DE FIREWALL PERIMETRAL PARA LA ORGANIZACIÓN CLINICA BARRAQUER

PAULA LEON RIVEROS

Trabajo de grado presentado como requisito para optar al título de ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Directora

Yolima Mercado Palencia

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
PROYECTO DE SEGURIDAD INFORMATICA II
BOGOTA D.C.
2018

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá 13 de agosto de 2018

A Dios por otorgarme la fortaleza, sabiduría e inteligencia para poder desarrollar este proyecto, a él le debo todo lo que tengo y todo lo que soy.
A mi esposo que no solo ha sido mi compañero de vida sino mi amigo y un gran apoyo para el cumplimiento de mis metas.
A mi hermana y a mis padres porque han sido incontables los sacrificios que han hecho para ayudarme en cada paso de mi vida.

Todo el éxito que he logrado, es de ustedes también.

AGRADECIMIENTOS

Me gustaría expresar mi agradecimiento especial a mi tutora Yolima Mercado quien me brindó la oportunidad de oro para hacer este maravilloso proyecto sobre el tema de seguridad de firewall perimetral para la organización clínica Barraquer, lo cual también me ayudó a hacer muchas Investigaciones y llegué a conocer muchas cosas nuevas, estoy muy agradecida con ella.

En segundo lugar, también me gustaría agradecer a mis padres, a mi esposo y amigos que me ayudaron mucho a finalizar este proyecto dentro del marco de tiempo limitado.

Agradezco también a Clínica Barraquer por proporcionar la información necesaria con respecto al proyecto y también por su apoyo para completar el mismo.

CONTENIDO

pág.

ANEXOS

LISTA DE FIGURAS

Pag

LISTA DE TABLAS

pag

INTRODUCCIÓN

En este proyecto se consideran los diversos ambitos de la seguridad perimetral, la cual va adquiriendo y tomando fuerza con el incremento del volumen de información importante y sobre todo confidencial que se encuentra en los diversos sistemas de información de Clinica Barraquer.

Actualmente existe un sin número de posibilidades que permiten a un atacante aprovecharse de las debilidades de los sistemas de información de Clinica Barraquer y es allí en donde la labor de los administradores de sistemas de información, técnicos, analistas de informática etc., juega un papel fundamental ya que de ellos depende la labor de minimizar al máximo el nivel de exposición de los sistemas frente a las constantes amenazas que a nivel informático se presentan. Esta labor debe ser desarrollada con un elevado nivel de compromiso y con herramientas capaces de desarrollar ese nivel de proteccion, ya que el buen funcionamiento, tratamiento y gestión que se da a los sistemas de información de la organización, garantizará en gran medida que los objetivos del negocio se cumplan y la operación normal se lleve a cabo en un100%.

En gran parte de los sistemas puede llegar a ser muy fácil para un usuario acceder de forma no autorizada a información confidencial, lo cual se demuestra de diversas maneras en el presente flujo de pruebas y evidencias, a traves de la metodología de ethical hacking adoptada por el área de Seguridad de la Información, la cual tiene tiene como propósito definir y validar los niveles de exposición en que se encuentra la plataforma tecnológica de CLINICA BARRAQUER, frente a posibles ataques y/o accesos no autorizados por parte de delincuentes informáticos.

Hoy en día Clinica Barraquer es consciente que debe estar a la vanguardia de la innovación, ademas de que se debe disponer de la información siempre y de manera confiable, como un factor fundamental para la continuidad del negocio. El filtrado de elementos maliciosos, la detección oportuna de fallas y el monitoreo de los elementos en la red organizacional son fundamentales, de esto se deriva el diseño de un esquema capaz de suplir con estas necesidades fundamentales.

En este proyecto se propone el diseño de un sistema de seguridad perimetral en La Clínica Barraquer, que permitirá a la organización tener una mayor confianza, seguridad y efectividad en los procesos internos y externos.

1. TITULO DEL PROYECTO

“Diseño de seguridad de firewall perimetral para la organización clínica Barraquer”

2. DESCRIPCION DEL PROBLEMA

La seguridad en los sistemas de información es factor que se extiende más allá de la continuidad de un negocio, este va incluso sobre la capacidad y honorabilidad de la organización y sus colaboradores además de la eficiencia de sus procesos. Para llevar los riesgos de seguridad informática a su mínima expresión, es necesario un equipo especializado, que transforme la seguridad en un proceso continuo y dinámico.

En la actualidad la Clínica Barraquer, no cuenta con un nivel de seguridad perimetral, permitiendo que la organización sea vulnerable a ataques informáticos, de esta manera se realizará un análisis de la situación actual de la clínica en materia de seguridad informática, y así diseñar un sistema de seguridad perimetral considerando la infraestructura, los servicios, los protocolos, las aplicaciones, el acceso a Internet e Intranet.

El dìa 05 de diciembre del año 2017 hubo perdida de informacion en un equipo de un funcionario de la Clinica, que contenia informacion contable, debido a un ataque a traves de correo electronico que introdujo un troyano en un archivo pdf, ese dia estuvo en riesgo toda la organización porque se empezo a filtrar en parte de la red y afecto dos equipos mas del area asistencial.

La detección vulnerabilidades y el monitoreo de los sistemas de información son imprescindibles para el funcionamiento de la organización y sus usuarios. De esto la necesidad de diseñar un sistema que monitoree, recolecte, notifique y analice el tráfico desde y hacia la red privada de la organización.

3. FORMULACION DEL PROBLEMA

En la actualidad las amenazas y la creación de herramientas y software malicioso han avanzado en sus metodologías de afectación a las organizaciones en todo el mundo, tanto así que las pérdidas se han calificado como incuantificables, inclusive en algunos casos se realizan cifrados de información y se solicita dinero a cambio de recuperar algo de lo que abusivamente se cifro y guardo con fines de lucro.
Históricamente el recurso de firewall ha pasado por fases de evolución bastante contundentes ya que se ha tenido que invertir en un solución de nunca acabar, inicialmente porque las vulnerabilidades de los sistemas informáticos han ido en aumento con la intervención constante de intrusos y personas que practican un hacking destructivo todo el tiempo, es por ello que el trabajo se ha ido volviendo cada vez más arduo, a comparación de sus inicios en 1961, donde el conocimiento no era tan masivo como ahora.

Con lo anterior se hace más que necesario, obligatorio, el diseño de un sistema de seguridad de un firewall perimetral que valide los accesos custodie y evalué la información o las ejecuciones en tiempo real hacia nuestro sistema, bien sea desde internet o desde la misma red pública, evidenciándose estadísticamente que la mayoría de ataques a las organizaciones residen en la misma LAN.
El presente proyecto se pretende dar solución y aportar a la Clínica Barraquer en relación a la siguiente pregunta:

¿De qué manera el diseño de sistema de seguridad de un firewall perimetral ayuda a la compañía a minimizar los riesgos de acceso abusivo a la información, perjuicios económicos, sociales y daño a sistemas de información, hardware, entre otros?

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar un Sistema de seguridad perimetral, que permita una correcta administración del tráfico entrante y saliente a la red corporativa de la Clínica Barraquer, asistiendo al desarrollo de políticas de seguridad informática que contribuyan con la administración eficiente de los sistemas de Información.

4.2. OBJETIVOS ESPECIFICOS

- Realizar un proceso de recolección de información en cuanto a todo el ambiente virtual y físico de los servidores de la organización, switches, etc.
- Realizar el respectivo levantamiento de servicios informáticos, aplicaciones, redes y VLANS
- Indagar acerca de los tipos de ataques utilizados por intrusos y hackers en organizaciones del sector salud, las cuales manejan información muy sensible.
- Analizar las diferentes soluciones posibles a diseñar una red perimetral.
- Diseñar un esquema de seguridad perimetral para la Clínica Barraquer.
- Establecer políticas de seguridad capaces de estandarizar junto con los procesos transversales, la seguridad en cuanto acceso y permisos al personal de Clínica Barraquer.

5. JUSTIFICACIÓN

Las amenazas a la seguridad de los sistemas de información van en incremento día a día por lo que se necesita de soluciones para enfrentar dichas amenazas, es por esto que se debe buscar que solución es la que más se ajusta a la problemática de La Clínica. Estas tan indeseadas amenazas pueden ser controladas siempre y cuando se defina e implemente una solución de seguridad perimetral acorde a las políticas de seguridad establecidas.

La seguridad de los sistemas de información está ligada a amenazas a las que están expuestas, el acceso a Internet incrementa este riesgo de manera exponencial. El nivel de amenaza para la Clínica va dirigida a la información propia, de sus colaboradores y sus clientes, y cualquier acceso no autorizado o no detectado puede tener un impacto muy negativo en la organización.

De esta manera es indispensable diseñar mecanismos control y seguridad para proteger los sistemas de información de la organización. Generalmente se carece de recursos de seguridad informática dejando a la Institución expuesta a amenazas internas originadas desde el interior, como a amenazas, esto último debido a la interconexión con otras organizaciones o con la Internet; por lo que se pretende reforzar las políticas de seguridad de la entidad y disminuir los riesgos de seguridad para los recursos tecnológicos de la organización, fortaleciendo la protección perimetral de la infraestructura tecnológica frente a amenazas de seguridad, a través de un firewall, sistema de protección de intrusos, el control de la navegación de los usuarios al interior de la organización, control de aplicaciones y la prestación de servicios de acceso seguro a través de VPNs.

.

6. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Alcances:

- Se pretende diseñar un sistema de seguridad perimetral, que controle, monitoree y proteja los activos informáticos e información de Clínica Barraquer
- El presente proyecto se ha estudiado únicamente el sector del área de la salud para análisis y levantamiento de información.
- El proyecto abarcara todo el estudio minucioso de estado de seguridad actual, nuevas amenazas, y estado existente de la Clínica Barraquer conforme a los análisis de vulnerabilidades que se efectuaran, en cuanto a aplicativos, servidores de bases de datos, web, de archivos e historias clínicas.

7. METODOLOGIA DE DESARROLLO

7.1. POBLACIÓN Y MUESTRA

En consecución del proyecto se realizará el análisis de documentación actual, encuestas y entrevistas a profesionales del área de la seguridad informática y de la información, en donde se detallen las experiencias y los puntos de vista que han surgido en cuanto a herramientas de firewall perimetral, creación de políticas de seguridad, segmentación de red, esquemas y demás parámetros capaces de dar un valor a cada variable investigativa; para lo anterior se escogerán al menos quince (15) ingenieros de infraestructura y redes de seguridad, de empresas del sector salud y cinco (5) del sector bancario, con el fin de tener un esquema paralelo en la actividad actual del negocio y otra totalmente diferente pero de mayor exigencia. Así mismo se realizarán encuestas a al menos veinte (20) usuarios finales que identifiquen el conocimiento y la importancia de la seguridad informática en el sector salud el cual es el área de ejercicio de Clínica Barraquer.

7.2. PROCEDIMIENTO DE EJECUCION DEL PROYECTO – METODOLOGIA DEL DESARROLLO

Hace referencia a la necesidad de ejecutar controles de seguridad que contribuyan a la estabilidad y disponibilidad de los servicios de Clínica Barraquer, a fin de prevenir todo tipo de incidente que cause algún tipo de perjuicio a la organización y/o a sus empleados.

Para ello en el margen de los objetivos del presente proyecto se pretenden ejecutar una serie de actividades que contribuyan a la consecución de la misión y visión de un adecuado diseño seguridad informática respaldado en herramientas informáticas capaces de solventar las necesidades y actividades del proyecto.

- ***Objetivo No. 1*:** Realizar un proceso de recolección de información en cuanto a todo el ambiente virtual y físico de los servidores de la organización, switches, etc.

Realizar reuniones con los dueños de los respectivos procesos, para poder determinar una definición de funcionamiento, a fin de obtener el conocimiento necesario para poder establecer un diagrama de todo el ambiente físico y la emulación, si aplica a ambientes virtualizados, sus interacciones con la infraestructura de red, de tal manera que con el esquema global claro se ejerza una comprensión más lógica de la función del negocio.

• ***Objetivo No. 2*****:** Establecer políticas de seguridad capaces de estandarizar junto con los procesos transversales, la seguridad en cuanto accesos y permisos al personal de Clínica Barraquer

Se ejecutarán por escrito las políticas de seguridad las cuales deberán ser avaladas por el director de TI, el oficial de seguridad y la gerencia general, posterior a ello se procederá con la socialización al personal de Clínica Barraquer, a fin de crear conciencia de los riesgos a los cuales se están expuestos en el ámbito de seguridad informática

• ***Objetivo No. 3:*** Indagar acerca de los tipos de ataques utilizados por intrusos y hackers

Ejecutar un análisis del entorno de seguridad mundial, explorando en actualización de nuevos ataques a los sistemas informáticos con el fin de encontrar la manera de resistirlos y no permitir que penetren a la infraestructura tecnológica de Clínica Barraquer

• ***Objetivo No. 4:*** Analizar las diferentes soluciones posibles a diseñar una red perimetral.

Verificar la manera más óptima y de acuerdo con los conocimientos de la infraestructura actual de Clínica Barraquer, para implementar el sistema de firewall perimetral de tal manera que se generen varios filtros de seguridad antes de llegar a la red de las aplicaciones y usuarios, las cuales van a manejarse de manera independiente.

• ***Objetivo No. 5:*** Diseñar un esquema de seguridad perimetral para la Clínica Barraquer.

Se realizará un diagrama en el cual se detallará no solo la solución de firewall sino los filtros perimetrales adicionales, de tal manera que se podrá efectuar un esquema lo suficientemente comprensible para futuras implementaciones sobre el mismo diagrama.

• ***Objetivo No. 6:*** Realizar el respectivo levantamiento de servicios informáticos, aplicaciones, redes y VLANS

Inmediatamente se tengan creadas las redes principales se dará lugar a crear las VLANS con las cuales se facilitará en orden de las políticas de acceso a los usuarios de clínica Barraquer, en misión de ingresar a las aplicaciones, internet, Wifi y demás, con el fin de llevar una administración más ordenada y por ende más controlada de los accesos, los puertos permitidos y demás.

8. MARCO REFERENCIAL

Fortigate – IP de Fábrica y configuración de las interfaces por consola.

En el artículo se detalla paso a paso la configuración de un Fortigate desde ceros, indicando el direccionamiento de entrada, las ips asignadas por puerto, las cuales son default para todos los fortigates. Igualmente indica la manera de configurar los dns e ip a entregar como administrativa del firewall

Esta referencia permite tener claridad en el tema de configuración y puesta en marcha de un fortigate traído directamente desde fábrica, desde ceros, por lo que se considera muy importante ya que es con ello que arranca la implementación.

Tutorial cómo definir y configurar las Políticas de Firewall en Fortigate.

Se explica de manera detallada los filtros de la creación de una política de seguridad en un firewall fortinet, detallan desde el origen al destino, puertos, NAT, etc.

Con esta referencia se podrán obtener los conocimientos plenos a la hora de configurar una política de seguridad para todo el tema de entrada y salida dentro de la LAN hacia internet, hacia las aplicaciones o viceversa

Propuesta de diseño de políticas de seguridad

Se presenta un modelo de diseño de políticas de seguridad implementadas en la Clínica Los Nogales, teniendo en cuenta los requerimientos de la dirección de IT y de la infraestructura tecnológica.

Esta referencia permitirá partir de un esquema de diseño de políticas de seguridad implementadas en una organización con una lógica de negocio parecida a Clínica Barraquer, con el fin de estandarizar las políticas de seguridad.

Propuesta de segmentación de Vlans y red en general

Se refiere a un esquema de segmentación de red apropiado para un diseño de delegación de permisos de acuerdo a la necesidad de servicios informáticos ofrecidos por Clínica Barraquer.

Ayudará a entender cómo debe diseñarse un esquema de red, de acuerdo a la necesidad y a estándares de buenas prácticas en diseño de red.

Diseño de una VPN

Determina las características de configuración para un tipo de VPN SSL, orientado a poder gestionar acceso remoto seguro desde internet hacia la red privada.

Con esta referencia se ejemplifica el diseño de una VPN para que los colaboradores, proveedores, etc. Autorizados de Clínica Barraquer puedan acceder a la red privada desde internet de manera segura, controlados a través del firewall perimetral.

Enrutamiento estático

Se muestra la manera de cómo debe diseñarse un enrutamiento estático, lo anterior para implementar proveedores de servicio de internet, controlados a través del firewall.

Esta referencia ayudara a tener una dimensión y explicación acerca de cómo deben configurarse los canales de internet dedicados contratados por Clínica Barraquer.

Esquema de monitoreo y recolección de logs de seguridad

La presente referencia describe la funcionalidad de la herramienta anexa a fortinet, llamada forticloud, la cual permite realizar un debido correlaciona miento de logs, entregando estadísticas referentes a ataques, spam, virus, entre otros

Con forticloud se permite tener un esquema de monitoreo amigable y centralizado del estado de seguridad de Clínica Barraquer, para lo cual esta referencia será vital en el diseño de esta interfaz.

Propuesta de esquema de alta disponibilidad

Indica un esquema de alta disponibilidad de dos fortigate en stack o HA.

Se pretende diseñar un esquema de alta disponibilidad de seguridad y red, con dos fortigates 300 c en HA (alta disponibilidad) para garantizar la disponibilidad del servicio dado el evento se caiga y/o sufra daños alguno de los firewall configurados.

Tutorial cómo definir y configurar las Políticas de Firewall en Fortigate

Se evidencia el paso a paso de configuración de una política de acceso de una red a otra, determinando puertos, direcciones ip especificas entre otras.

Es conveniente que de acuerdo al diseño de políticas de seguridad informática y de las validaciones del área de IT con las gerencias de Clínica Barraquer se establezcan políticas de entrada y salida entre Vlans o redes independientes, lo anterior para otorgar los permisos más convenientes.

Configurando un clúster dos o más Fortigate

En este procedimiento se expone cómo establecer dos firewalls Fortigate en modo clúster, en alta disponibilidad. Es preciso que los dos firewalls tengan la misma versión de firmware. En este caso los dos tienen una versión 3.

Esta referencia indica un procedimiento de configuración de un clúster de fortigates en HA pasivo- activo, la cual servirá para cumplir el mismo objetivo en Clínica Barraquer.

Installing a FortiGate in NAT/Route mode

En este ejemplo, aprenderá a conectar y configurar una nueva unidad FortiGate en modo NAT / Route para conectar de forma segura una red privada a Internet.
En el modo NAT / Ruta, se instala una unidad FortiGate como puerta de enlace o enrutador entre dos redes tal como lo especifica en su artículo de instalación Fortinet cookbook.[1] En la mayoría de los casos, se utiliza entre una red privada e Internet.

[1] The Fortinet cookbook. *Installing a FortiGate in NAT/Route mode.* [En Línea], Julio de 2014. Disponible en: <https://cookbook.fortinet.com/installing-fortigate-nat-route-mode/>

Esto permite al FortiGate ocultar las direcciones IP de la red privada mediante la traducción de direcciones de red NAT

Clínica Barraquer requiere de un diseño de seguridad fortigate en modo NAT/Route, para tener un mejor esquema de seguridad, enmascarando las ips privadas para mayor seguridad.

Fortinet mejora la seguridad de las redes Wifi con FortiCloud

Fortigate pretende robustecer sus inversiones y posicionamiento en el mercado de seguridad en redes inalámbricas. Los puntos de acceso inalámbricos (WLAN) de la serie FortiAP-S son los dispositivos Wifi gestionados en la nube más seguros del mercado para un entorno empresarial, al ejecutar la tecnología de ciberseguridad de Fortinet en el propio AP y disponer de las últimas actualizaciones de seguridad proporcionadas por el equipo de inteligencia de amenazas FortiGuard Labs.

Se pretende que Clínica Barraquer en el diseño de seguridad de red inalámbrica con FortiAPS, haga uso de un servicio anexo a Fortinet, que permitirá tener de manera centralizada y por ende controlada de todos los dispositivos access points proveedores de red wifi.

Fortinet quiere administrar el wi-fi más fácil desde la nube

Fortigate lanza una nueva mejora en el diseño de FortiAPS ofreciendo una administración más sencilla y segura a través de la nube.

Es conveniente validar con Clínica Barraquer, de acuerdo con la estabilidad en canales de internet dedicados que tengan, velocidad, ancho de banda, etc., lo anterior para poder validar si es procedente realizar el diseño y esquema de seguridad en la nube o si es más viable instalar una appliance en la red privada para tener control de manera local y no desde internet.

Fortinet lanza los primeros puntos de acceso inalámbricos universales de la industria

Se evidencia un proceso de investigación de Fortinet acerca de la creación de sus primeros dispositivos inalámbricos proveedores de wifi, administrados desde el Fortigate

Esta referencia es de carácter investigativo y netamente informativo para Clínica Barraquer, lo anterior para tener un dimensionamiento del crecimiento de Fortinet en los últimos años, referenciado hacia proveer servicios seguros de wifi como lo evidencia ebizlatam en su artículo de FortiAP [2]

FortiGuard Labs de Fortinet

Los nuevos servicios de sandboxing basados en cloud y reputación IP de FortiGuard mejoran la protección de las plataformas FortiGate, FortiCloud, FortiWeb, FortiDDoS y FortiDNS como lo ilustra Arrow [3] en su artículo.

Esta referencia establece para Clínica Barraquer los avances de Fortinet en materia de nuevos servicios de seguridad para todas las aplicaciones anexas de Fortinet, permitiendo indagar más acerca del diseño estable de seguridad con el cual contara Clínica Barraquer.

2 Ebizlatam. * Fortinet lanza los primeros puntos de acceso inalámbricos universales de la industria*. [En Línea], septiembre de 2016. Disponible en: <http://www.ebizlatam.com/fortinet-lanza-los-primeros-puntos-acceso-inalambricos-universales-la-industria >

3 Arrow. * FortiGuard Labs de Fortinet*. [En Línea], marzo de 2013. Disponible en:<http://www.arrowecs.es/news/fortiguard_labs_de_fortinet>

9. MARCO DE ANTECEDENTES

Como antecedentes se tienen los siguientes proyectos:

"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN LA OFICINA DE SISTEMAS DE INFORMACIÓN Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE CÓRDOBA como registra Dorita en su proyecto de diseño.[4]

El presente proyecto tiene como finalidad diseñar un Sistema de Gestión de la Seguridad de la Información para la oficina de Sistemas y Telecomunicaciones de la Universidad de Córdoba que sirva como punto de partida para su implementación mediante un análisis de la situación actual de los dominios, objetivos de control y controles que sugiere la norma ISO 27001, la selección de una metodología de evaluación de riesgos informáticos, el establecimiento de una política de seguridad informática institucional que sea liderada por la alta gerencia, además de generar la documentación respectiva para los Planes de Continuidad de Negocio con el fin de mantener y/o restaurar los servicios críticos y el análisis y selección de un modelo de Gobierno de Tecnología Informática que se ajuste a las necesidades institucionales.

Para lograr los objetivos propuestos y generar la documentación respectiva, es necesario realizar las actividades expuestas en el estándar ISO/IEC27001:2013

Tiene como objetivo diseñar o planear un Sistema de Gestión de la Seguridad de la Información mediante el estándar ISO/IEC 27001:2013

[4] Doria C., Andrés. Diseño De Un Sistema De Gestión De Seguridad De La Información Mediante La Aplicación De La Norma Internacional Iso/Iec 27001:2013 En La Oficina De Sistemas De Información Y Telecomunicaciones De La Universidad De Córdoba. En: UNAD. 2015. p. 1-65

“DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BELISARIO LTDA. DE LA CIUDAD DE BOGOTÁ D.C.” tal como lo ilustra en su proyecto, Botero[5]

Su propósito principal es ayudar a disminuir la pérdida de información y mejorar la seguridad informática mediante el diseño de un sistema de gestión de seguridad informática y de la información SGSI en la empresa Belisario Ltda.

La metodología de análisis y gestión de riesgos MAGERIT, permite identificar los activos a proteger y que hacen parte fundamental en la ejecución de los diferentes procesos organizacionales, además permite determinar el impacto y riesgo derivado de la posible materialización de amenazas, obteniendo como resultado la declaración de aplicabilidad, que expone una relación de mecanismos y controles aplicables a la organización.

Ayuda a disminuir la pérdida de información y mejora la seguridad informática mediante el diseño de un sistema de gestión de seguridad informática y de la información SGSI en la empresa Belisario Ltda.

“IMPLEMENTACIÓN DE UN FIREWALL GNU/LINUX EN UN ENTORNO ESCOLAR”

Tiene como objetivo representar unos análisis de implementación de software perimetral open zurce con el fin de realizar filtrado de contenido de los usuarios y poder otorgar una seguridad confiable a la red local, apoyando el objetivo del colegio en su labor educativa y asi es como Posada apoya el area tecnològica en su colegio a travès de este proyecto. [6]

[5] Botero V., David. Diseño Del Sistema De Gestión De Seguridad Informática Y De La Información (Sgsi) Para La Empresa Belisario Ltda. De La Ciudad De Bogotá D.C. En: UNAD.2016.p.1-182.
[6] Posada S. Olga, Garzón V. Hernando. Implementación De Un Firewall Gnu/Linux En Un Entorno Escolar. En: Monografias.2008.p.1-78.

10. DISEÑO DE SEGURIDAD DEL FIREWALL

13.1. FASE I

Se gestiona el correspondiente levantamiento de información proporcionada a servidores, equipos de cómputo y switches, para analizar y elaborar el esquema de red correspondiente, y poder gestionar la segmentación de VLANS de acuerdo a los tipos de aplicaciones y de servicios de informática, encontrando lo siguiente:

- 24 servidores virtualizados en VMware, los cuales están desplegados bajo ambiente Ubuntu y Windows
- 210 estaciones de trabajo con sistema operativo Windows
- 15 estaciones de trabajo con sistema operativo IOS
- 10 switches
- 7 servidores físicos

El presente proyecto establece como resultado una herramienta de firewall perimetral completamente configurada, de acuerdo con las necesidades de la Clínica Barraquer, como solución de seguridad informática, prevención de intrusos y control de accesos no autorizados a personal interno, pacientes, etc., con lo anterior el ingreso a la red wifi también estará de manera centralizada con lo cual se podrán también dictar políticas de seguridad para la solución Wireless actual de la Clinica.

13.2. FASE II

Se realiza el levantamiento de aplicaciones y VLANS pre configuradas en la red, arrojando lo siguiente:

- Dos aplicaciones core de negocio SIBA (Software de facturación, agendamiento, inventarios) e Historia clínica desarrolladas en lenguaje de programación Visual Studio, con motor de base de datos SQL Server 2008 R2

- Aplicación contable SIIMED desarrollada en Visual Studio con motor de base de datos SQL Server 2012.
- Las siguientes VLANS pre configuradas:

Tabla 1. *Estado actual de segmentación de la red de Clínica Barraquer.*

LAN (Admin_Vlan, 2 Members)	Aggregate
G_DIRECTIVOS	VLAN
G_OPERATIVO_1	VLAN
G_OPERATIVO_2	VLAN
G_RESIDENTES	VLAN
IMPRESORAS	VLAN
INVITADOS	VLAN
USUARIOS	VLAN
VLAN_VOZ	VLAN
WIFI_RESIDENTES	VLAN
WIFI_VIP	VLAN

Fuente: ECOMIL S.A.S. Propuesta de diseño de políticas de seguridad. Bogotá D.C.: Documentación de SGSI Ecomil S.A.S. 2015.p.43.

13.3. FASE III

Se realiza un análisis de vulnerabilidades en todos los servicios informáticos de clínica Barraquer arrojando el siguiente resultado:

La metodología de ethical hacking adoptada por el área de Seguridad de la Información (ver Figura 1) tiene como propósito definir y validar los niveles de exposición en que se encuentra la plataforma tecnológica de CLINICA BARRAQUER, frente a posibles ataques y/o accesos no autorizados por parte de delincuentes informáticos.

***Figura 1**. Proceso de la Metodología Ethical Hacking*

Fuente: ROBERTO C. GONZÁLEZ. Capítulo 3 – Escaneo y Enumeración. México.: Ethical Hack.2017.p.5

A continuación se encuentra una descripción general de cada una de las fases contempladas dentro de la metodología de Ethical Hacking:

Anatomía de un ataque informático. Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque indicado en el artículo de ataques informáticos.[7]

Fase 1: Reconnaissance (Reconocimiento). El reconocimiento es probablemente la fase más larga, a veces dura semanas o meses con lo indica Fortinet en su artículo[8]. El sombrero negro usa una variedad de fuentes para aprender tanto como sea posible sobre el negocio objetivo y cómo opera, incluyendo

- Búsquedas en internet
- Ingeniería social
- Dumpster de buceo
- Servicios de búsqueda / gestión de nombres de dominio
- Escaneo de red no intrusivo

[7] Establece seguridad informática. “ATAQUES INFORMÀTICOS” [En Línea], septiembre 2016. Disponible en: <https://danacecyte2blog.wordpress.com/2016/09/14/ataques-informaticos-ramieluribe/>.
8 Tom. O. * The five phases of a successful network penetration*. [En Línea], diciembre de 2008. Disponible en: < https://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/> .p.1

Las actividades en esta fase no son fáciles de defenderse. La información sobre una organización encuentra su camino a Internet a través de varias rutas. Los empleados a menudo son fácilmente engañados para que entreguen fragmentos de información que, con el tiempo, actúan para completar una imagen completa de los procesos, la estructura de la organización y los puntos débiles potenciales.

Fase 2: Scanning (Exploración). Una vez que el atacante tiene suficiente información para entender cómo funciona la empresa y qué información de valor puede estar disponible, comienza el proceso de exploración del perímetro y de los dispositivos de red internos en busca de debilidades indicado en el artículo de Tom Olzak [9], incluyendo

- Puertos abiertos
- Servicios abiertos
- Aplicaciones vulnerables, incluidas los sistemas operativos
- Débil protección de datos en tránsito
- Marca y modelo de cada pieza de equipo LAN / WAN

Las exploraciones del perímetro y los dispositivos internos a menudo se pueden detectar con soluciones de detección de intrusión (IDS) o prevención (IPS), pero no siempre. Los sombreros negros veteranos saben cómo evitar estos controles. En cualquier caso, algunos pasos que puede tomar para frustrar los escaneos incluyen:

- Cerrar todos los puertos y servicios innecesarios
- Permitir que dispositivos críticos, o dispositivos que alojan o procesan información confidencial, respondan solo a dispositivos aprobados

Administre de cerca el diseño del sistema, resistiendo los intentos de permitir el acceso externo directo a los servidores, excepto en circunstancias especiales y restringido por las reglas de extremo a extremo definidas en las listas de control de acceso

Fase 3: Obtener acceso. Obtener acceso a los recursos es el objetivo de un ataque moderno. El objetivo habitual es extraer información de valor al atacante o utilizar la red como sitio de lanzamiento para ataques contra otros objetivos. En cualquier situación, el atacante debe obtener cierto nivel de acceso a uno o más dispositivos de red.

Además de los pasos defensivos descritos anteriormente, los administradores de seguridad deben hacer todos los esfuerzos posibles para garantizar que los usuarios no autenticados puedan acceder fácilmente a los dispositivos y servidores de los usuarios finales. Esto incluye negar el acceso del administrador local a los

9 Tom. O. * The five phases of a successful network penetration*. [En Línea], diciembre de 2008. Disponible en: < https://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/> .p.2

usuarios comerciales y monitorear de cerca el dominio y el acceso de administrador local a los servidores. Además, los controles de seguridad física deberían detectar intentos de ataque práctico y retrasar a un intruso el tiempo suficiente para permitir una respuesta humana interna o externa efectiva (es decir, guardias de seguridad o fuerzas del orden).
Alguna de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, denegación de servicio, DDoS, sesión hijacking, brute password.

Fase 4: Maintaining Access (Mantener el acceso). Habiendo obtenido acceso, un atacante debe mantener el acceso el tiempo suficiente para lograr sus objetivos. Aunque un atacante que llegue a esta fase ha eludido con éxito sus controles de seguridad, esta fase puede aumentar la vulnerabilidad del atacante a la detección así lo destaca Tom Olzak en su articulo [10]
.

Además de usar dispositivos IDS e IPS para detectar intrusiones, también puede usarlos para detectar extrusiones, lo cual incluye:

- Detectar y filtrar contenido de transferencia de archivos a sitios externos o dispositivos internos
- Evita / detecta la iniciación de sesión directa entre servidores de tu centro de datos y redes / sistemas que no están bajo tu control
- Busque conexiones a puertos impares o protocolos no estándar
- Detecta sesiones de duración inusual, frecuencia o cantidad de contenido
- Detecta el comportamiento anómalo de la red o del servidor, incluido la mezcla de tráfico por intervalo de tiempo.

Fase 5: Borrar huellas. Después de lograr sus objetivos, el atacante generalmente toma medidas para ocultar la intrusión y los posibles controles que quedan para futuras visitas. Alerte sobre cualquier actividad inusual, cualquier actividad no esperada en base a su conocimiento de cómo funciona la empresa. Para que esto funcione, los equipos de seguridad y de red deben tener al menos tanto conocimiento de la red como el atacante ha obtenido durante el proceso de ataque.

Evaluación Del Riesgo

Se definen cuatro niveles de riesgo para las vulnerabilidades, los cuales se utilizarán para la clasificación de cada una de ellas.

[10] Tom. O. * The five phases of a successful network penetration*. [En Línea], diciembre de 2008. Disponible en: < https://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/> .p.5

- **Nivel de riesgo Crítico:** Corresponde a la vulnerabilidad que permitiría a un atacante informático el ingreso total de la máquina violando todos los principios de seguridad de la información como confidencialidad, integridad y disponibilidad de toda la infraestructura.

- **Nivel de riesgo Alto:** corresponde vulnerabilidades por medio de las cuales fácilmente un intruso puede obtener control total del dispositivo, con posibilidades de comprometer la seguridad de toda la red. Las vulnerabilidades de este tipo incluyen la obtención de privilegios para leer y modificar archivos, ejecución remota de código, presencia de puertas traseras (Backdoors), entre otros.

- **Nivel de riesgo Medio:** corresponde a las vulnerabilidades por medio de las cuales es posible obtener acceso a información específica almacenada en los dispositivos, incluyendo configuraciones de seguridad. Las vulnerabilidades de este tipo incluye la divulgación de contenido de archivos, divulgación de reglas de filtrado y mecanismos de seguridad, uso de servicios sin autorización, entre otros.

- **Nivel de riesgo Bajo:** corresponde a las vulnerabilidades por medio de las cuales un intruso puede recolectar información de los dispositivos (Sistema Operativo, puertos abiertos, servicios, etc.), posiblemente se puede usar dicha información para buscar otras vulnerabilidades.

Tabla 2. *Representación de la evaluación de riesgos encontrados.*

Nivel de Riesgo	Representación
Crítico	
Alto	
Medio	
Bajo	

Fuente: *El autor*

Resumen De Hallazgos

A continuación se presenta el informe de la evaluación de seguridad realizada en Clínica Barraquer:

Tabla 3. *Tipo de vulnerabilidades encontradas en Clínica Barraquer, con el nivel de riesgo.*

Vulnerabilidad	Riesgo
Explotación de Vulnerabilidades	Crítico
Servicio FTP Descubierto	Alto
Visualización Interfaz Fortinet	Medio
Listado de Directorios	Medio
Autenticación por Defecto	Crítico
Vulnerabilidades Críticas	Crítico
Vulnerabilidades Medias	Medio
Vulnerabilidades Altas	Alto

Fuente*: El autor*

Resultados y Evidencias

La prueba se inicia con un ejercicio de caja negra sin ningún conocimiento de la red y partiendo de solo una conexión a un punto de red

Explotación De Vulnerabilidades

Riesgo Crítico

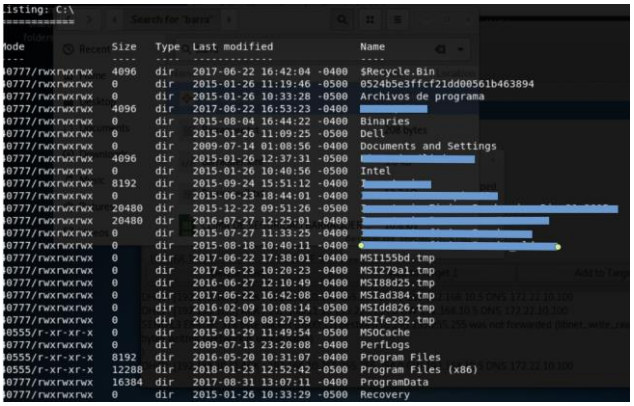
Descripción: Las vulnerabilidades intrusivas y de riesgo crítico que puede generar denegación de servicio en las máquinas afectadas.

Recomendación: Realizar el parcheo de todas las vulnerabilidades expuestas en el documento.

- **Red usuarios**

Se logro acceder a una direccion IP y se obtuvo acceso a todas las carpetas del equipo, las cuales se listan accediendo al equipo a traves del simbolo del sistema en la Figura 2:

Figura 2. *Acceso logrado a un equipo de la red de usuarios.*

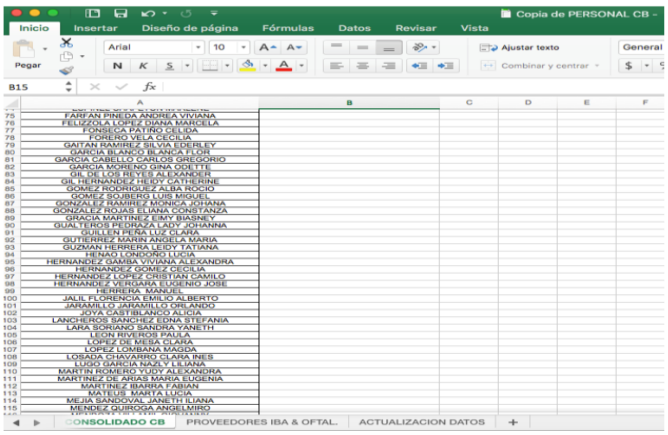


Fuente*: El autor*

Acceso a la información:

Se evidencia acceso a archivos de Excel con evidente información confidencial, en este caso y como se evidencia en la Figura 3 y en la Figura 4 se logró acceder a una base de datos de errores de códigos CUPS

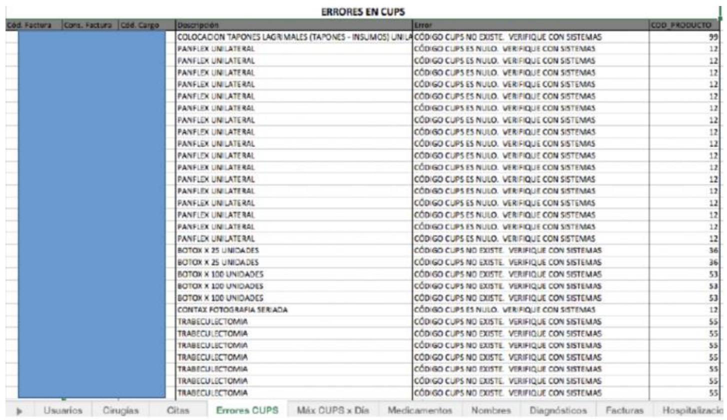
Figura 3. Acceso a base de datos de Excel de un equipo de la red de usuarios.



Fuente: *El autor*

Así mismo se logró acceder a diferentes reportes confidenciales donde se evidenciaba documentación de incidentes y eventos adversos, tal como lo evidencia la Figura 5.

Figura 4. *Acceso a base de datos de errores de códigos CUPS.*



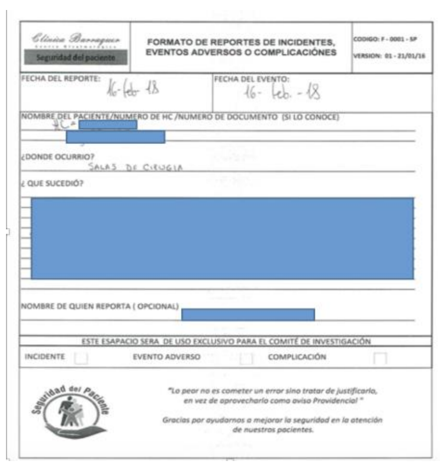
ERRORES EN CUPS

Cód. Factura	Cons. Factura	Cód. Cargo	Descripción	Error	COD_PRODUCTO
[redacted]			COLOCACION TAPONES LAGRIMALES (TAPONES - INSUMOS) UNILA	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	99
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			PANFLEX UNILATERAL	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			BOTOX X 25 UNIDADES	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	36
			BOTOX X 25 UNIDADES	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	36
			BOTOX X 100 UNIDADES	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	53
			BOTOX X 100 UNIDADES	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	53
			BOTOX X 100 UNIDADES	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	53
			CONTAX FOTOGRAFIA SERIADA	CÓDIGO CUPS ES NULO. VERIFIQUE CON SISTEMAS	12
			TRABECULECTOMIA	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	55
			TRABECULECTOMIA	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	55
			TRABECULECTOMIA	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	55
			TRABECULECTOMIA	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	55
			TRABECULECTOMIA	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	55
			TRABECULECTOMIA	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	55
			TRABECULECTOMIA	CÓDIGO CUPS NO EXISTE. VERIFIQUE CON SISTEMAS	55

Usuarios | Cirugías | Citas | Errores CUPS | Máx CUPS x Día | Medicamentos | Nombres | Diagnósticos | Facturas | Hospitalizacio

Fuente: *El autor*

Figura 5. *Acceso reportes de incidentes y eventos adversos del equipo de un usuario.*



Clínica Barraquer
Seguridad del paciente

FORMATO DE REPORTES DE INCIDENTES, EVENTOS ADVERSOS O COMPLICACIÓNES

CODIGO: F - 0001 - SP
VERSION: 01 - 21/01/16

FECHA DEL REPORTE: 16-feb-18

FECHA DEL EVENTO: 16- feb. - 18

NOMBRE DEL PACIENTE/NUMERO DE HC /NUMERO DE DOCUMENTO (SI LO CONOCE)
HC= [redacted]

¿DONDE OCURRIO?
SALAS DE CIRUGIA

¿ QUE SUCEDIÓ?
[redacted]

NOMBRE DE QUIEN REPORTA (OPCIONAL) [redacted]

ESTE ESAPACIO SERA DE USO EXCLUSIVO PARA EL COMITÉ DE INVESTIGACIÓN

INCIDENTE ☐ EVENTO ADVERSO ☐ COMPLICACIÓN ☐

Seguridad del Paciente

"Lo peor no es cometer un error sino tratar de justificarlo, en vez de aprovecharlo como aviso Providencial "

Gracias por ayudarnos a mejorar la seguridad en la atención de nuestros pacientes.

Fuente: *El autor*

Información sensible:

La información confidencial se refiere a la información privilegiada o patentada que solo ciertas personas pueden ver y que, por lo tanto, no es accesible para todos. Si la información confidencial se pierde o se utiliza de una manera diferente a la prevista, el resultado puede ser un daño grave para las personas u organizaciones a las que pertenece esa información.

La información sensible también se puede llamar un activo sensible.

Algunos ejemplos de información confidencial son los siguientes:

- Información personal, incluido el documento de identificación y las credenciales bancarias, tal como se evidencia en la Figura 6.
- Secretos comerciales
- Informes de vulnerabilidad del sistema
- Documentación de adquisición previa a la solicitud, incluidas las declaraciones de trabajo
- Informes de deficiencia de seguridad informática

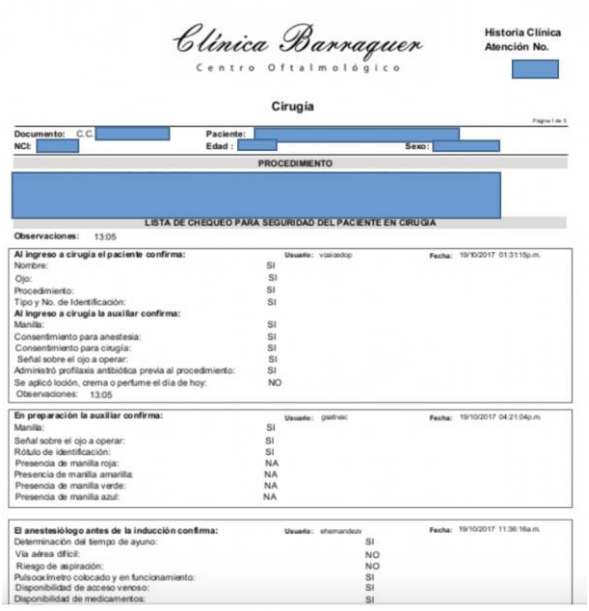
Figura 6. *Acceso a documento de identificación de un paciente de la clínica.*

Fuente: *El autor*

Se aseguró acceso a la historia clínica electrónica de los pacientes como verifica en la Figura 7, por lo que se evidencio que la confidencialidad requiere procedimientos y medidas para controlar el acceso físico y técnico a la información. Por ejemplo, mientras que la seguridad física limita la posibilidad de acceso físico no autorizado a la información (instalación, infraestructura de TI, etc.), la seguridad de TI controla el acceso a la información a través del sistema de TI. Los procedimientos destinados a preservar la confidencialidad de la información incluyen:

- Gestión de perfiles de usuario y derechos de acceso
- Clasificación de datos (tanto electrónicos como impresos)
- Política de escritorio limpio (política de lugar de trabajo limpio)
- Acuerdos de confidencialidad y no divulgación con empleados y contratistas
- Política de contraseñas
- Reglas y regulaciones para el uso de TI de los empleados

Figura 7. *Acceso a la historia electrónica de un paciente.*


Clínica Barraquer
Centro Oftalmológico

Historia Clínica
Atención No.

Cirugía

Documento: C.C. Paciente:
NCI: Edad : Sexo:

PROCEDIMIENTO

LISTA DE CHEQUEO PARA SEGURIDAD DEL PACIENTE EN CIRUGIA

Observaciones: 13:05

Al ingreso a cirugía el paciente confirma:		Usuario:	Fecha:
Nombre:	SI		
Ojo:	SI		
Procedimiento:	SI		
Tipo y No. de Identificación:	SI		
Al ingreso a cirugía la auxiliar confirma:			
Manilla:	SI		
Consentimiento para anestesia:	SI		
Consentimiento para cirugía:	SI		
Señal sobre el ojo a operar:	SI		
Administró profilaxis antibiótica previa al procedimiento:	SI		
Se aplicó loción, crema o perfume el día de hoy:	NO		
Observaciones: 13:05			

En preparación la auxiliar confirma:		Usuario:	Fecha:
Manilla:	SI		
Señal sobre el ojo a operar:	SI		
Rótulo de identificación:	SI		
Presencia de manilla roja:	NA		
Presencia de manilla amarilla:	NA		
Presencia de manilla verde:	NA		
Presencia de manilla azul:	NA		

El anestesiólogo antes de la inducción confirma:		Usuario:	Fecha:
Determinación del tiempo de ayuno:	SI		
Vía aérea difícil:	NO		
Riesgo de aspiración:	NO		
Pulsoxímetro colocado y en funcionamiento:	SI		
Disponibilidad de acceso venoso:	SI		
Disponibilidad de medicamentos:	SI		

Fuente: *El autor*

Servicio FTP Descubierto

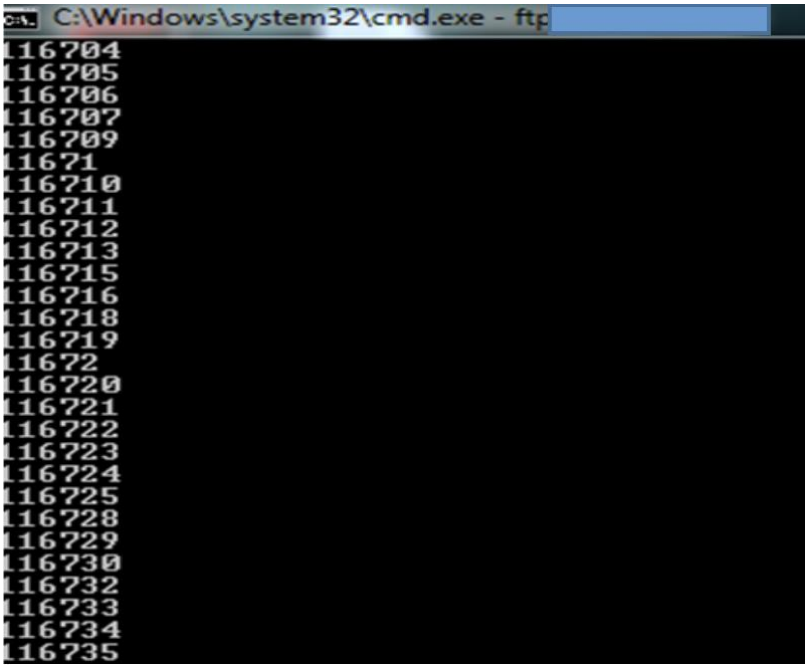
Riesgo Alto

Descripción: Se encuentra un servicio FTP, las credenciales de autenticación pueden ser vistas dado que la información no se transporta cifrada, ya que el servicio FTP no utiliza ningún método de encriptación de datos, esencialmente en la fase autenticación.

Recomendación: Retirar el servicio o aplicar SFTP, lo anterior debido a que es una versión segura de File Transfer Protocol (FTP), que facilita el acceso a los datos y la transferencia de datos a través de un flujo de datos Secure Shell (SSH). Es parte del protocolo SSH. Este término también se conoce como Protocolo de transferencia de archivos SSH.

En la Figura 8 se evidencia como el atacante logro ingresar al servidor FTP, se listan todas las carpetas de información concernientes a la historia clínica de los pacientes las cuales se almacenan eba través de la consola de comandos de Windows.

Figura 8. *Evidencia de acceso a FTP descubierto, listado de carpetas.*



Fuente: *El autor*

Vulnerabilidades Críticas

Riesgo Crítico

Descripción: Se encuentra vulnerabilidades en activos de Clinica Barraquer que puede permitir a un atacante informático utilizar exploits para lograr una intrusión, extraer información confidencial o realizar ataques de denegación de servicio.
Recomendación: Aplicar los parches de seguridad de acuerdo a las vulnerabilidades presentadas, lo anterior debido a que las encontradas hacen referencia a falta de proceso de actualización de Microsoft en los equipos relacionados en la tabla 4, tabla 5, tabla 6 y tabla 7

Tabla 4.*Vulnerabilidad de severidad critico detectadas en toda la red de usuarios y aplicaciones.*

Dirección IP	Severidad	Vulnerabilidad
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows XP Unsupported Installation Detection
	CRITICO	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Fuente: *El autor*

Tabla 5.*Vulnerabilidad de severidad critico detectadas en toda la red de usuarios y aplicaciones*

Dirección IP	Severidad	Vulnerabilidad
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	Microsoft Windows XP Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	Microsoft Windows XP Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows Vista Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Fuente: *El autor*

Tabla 6.*Vulnerabilidad de severidad critico detectadas en toda la red de usuarios y aplicaciones.*

Dirección IP	Severidad	Vulnerabilidad
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Fuente: *El autor*

Tabla 7.*Vulnerabilidad de severidad critico detectadas en toda la red de usuarios y aplicaciones*

Dirección IP	Severidad	Vulnerabilidad
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection

Fuente: *El autor*

Tabla 8.*Vulnerabilidad de severidad critico detectadas en toda la red de usuarios y aplicaciones*

Dirección IP	Severidad	Vulnerabilidad
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows 8 Unsupported Installation Detection
	CRITICO	Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows RCE
	CRITICO	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
	CRITICO	Microsoft Windows SMBv1 Multiple Vulnerabilities

Fuente: *El autor*

Vulnerabilidades Altas

Riesgo Alto

Descripción: Se visualiza una alta cantidad de vulnerabilidades en PHP y SSL, como se evidencia en la tabla 8 y tabla 9.

Recomendación: Aplicar los parches de seguridad para apache, PHP y SSL.

Tabla 9.*Vulnerabilidad de severidad alto detectadas en toda la red de usuarios y aplicaciones.*

Dirección IP	Severidad	Vulnerabilidad
	ALTO	SNMP Agent Default Community Name (public)
	ALTO	SNMP Agent Default Community Name (public)
	ALTO	PHP 5.6.x < 5.6.26 Multiple Vulnerabilities
	ALTO	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
	ALTO	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
	ALTO	PHP 5.6.x < 5.6.25 Multiple Vulnerabilities
	ALTO	PHP 5.6.x < 5.6.30 Multiple DoS
	ALTO	OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities
	ALTO	Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)
	ALTO	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities
	ALTO	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
	ALTO	Unsupported Web Server Detection
	ALTO	Unsupported Web Server Detection
	ALTO	Unsupported Web Server Detection
	ALTO	Unsupported Web Server Detection
	ALTO	Apache 2.2.x < 2.2.34 Multiple Vulnerabilities
	ALTO	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.28 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.28 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.25 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.25 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.12 FPM Unix Socket Insecure Permission Escalation
	ALTO	PHP 5.5.x < 5.5.12 FPM Unix Socket Insecure Permission Escalation
	ALTO	PHP 5.5.x < 5.5.33 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.33 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.18 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.18 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.35 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.35 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.14 Multiple Vulnerabilities

Fuente: *El autor*

Tabla 10.*Vulnerabilidad de severidad alto detectadas en toda la red de usuarios y aplicaciones.*

Dirección IP	Severidad	Vulnerabilidad
	ALTO	PHP 5.5.x < 5.5.14 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.20 'process_nested_data' RCE
	ALTO	PHP 5.5.x < 5.5.20 'process_nested_data' RCE
	ALTO	PHP 5.5.x < 5.5.21 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.21 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.23 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.23 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.30 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.30 Multiple Vulnerabilities
	ALTO	PHP 5.5.x < 5.5.38 Multiple Vulnerabilities (httpoxy)
	ALTO	PHP 5.5.x < 5.5.38 Multiple Vulnerabilities (httpoxy)
	ALTO	PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)
	ALTO	PHP 5.5.x < 5.5.22 Multiple Vulnerabilities (GHOST)
	ALTO	OpenSSL 1.0.1 < 1.0.1i Multiple Vulnerabilities
	ALTO	OpenSSL 1.0.1 < 1.0.1i Multiple Vulnerabilities
	ALTO	OpenSSL 1.0.1 < 1.0.1s Multiple Vulnerabilities (DROWN)
	ALTO	OpenSSL 1.0.1 < 1.0.1s Multiple Vulnerabilities (DROWN)
	ALTO	OpenSSL 1.0.1 < 1.0.1h Multiple Vulnerabilities
	ALTO	OpenSSL 1.0.1 < 1.0.1h Multiple Vulnerabilities
	ALTO	Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)
	ALTO	Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)
	ALTO	Apache 2.4.x < 2.4.10 Multiple Vulnerabilities
	ALTO	Apache 2.4.x < 2.4.10 Multiple Vulnerabilities
	ALTO	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities
	ALTO	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities
	ALTO	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
	ALTO	Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities
	ALTO	SNMP Agent Default Community Name (public)
	ALTO	SNMP Agent Default Community Name (public)

Fuente: *El autor*

Vulnerabilidades Medias

Riesgo Medio

Descripción: Se visualiza servicios con vulnerabilidades en Microsoft, Open SSL y vulnerabilidades en apache.

Recomendación: Aplicar los parches de seguridad y configuraciones de seguridad requeridas para las vulnerabilidades presentadas.

Tabla 11.*Vulnerabilidad de severidad medio detectadas en toda la red de usuarios y aplicaciones.*

Dirección IP	Severidad	Vulnerabilidad
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Fuente*: El autor*

Tabla 12.*Vulnerabilidad de severidad medio detectadas en toda la red de usuarios y aplicaciones.*

Dirección IP	Severidad	Vulnerabilidad
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Fuente: *El autor*

Tabla 13.*Vulnerabilidad de severidad medio detectadas en toda la red de usuarios y aplicaciones.*

Dirección IP	Severidad	Vulnerabilidad
[redacted]	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
	MEDIO	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
	MEDIO	OpenSSL < 1.1.0 Default Weak 64-bit Block Cipher (SWEET32)
	MEDIO	OpenSSL 1.0.x < 1.0.2m RSA/DSA Unspecified Carry Issue

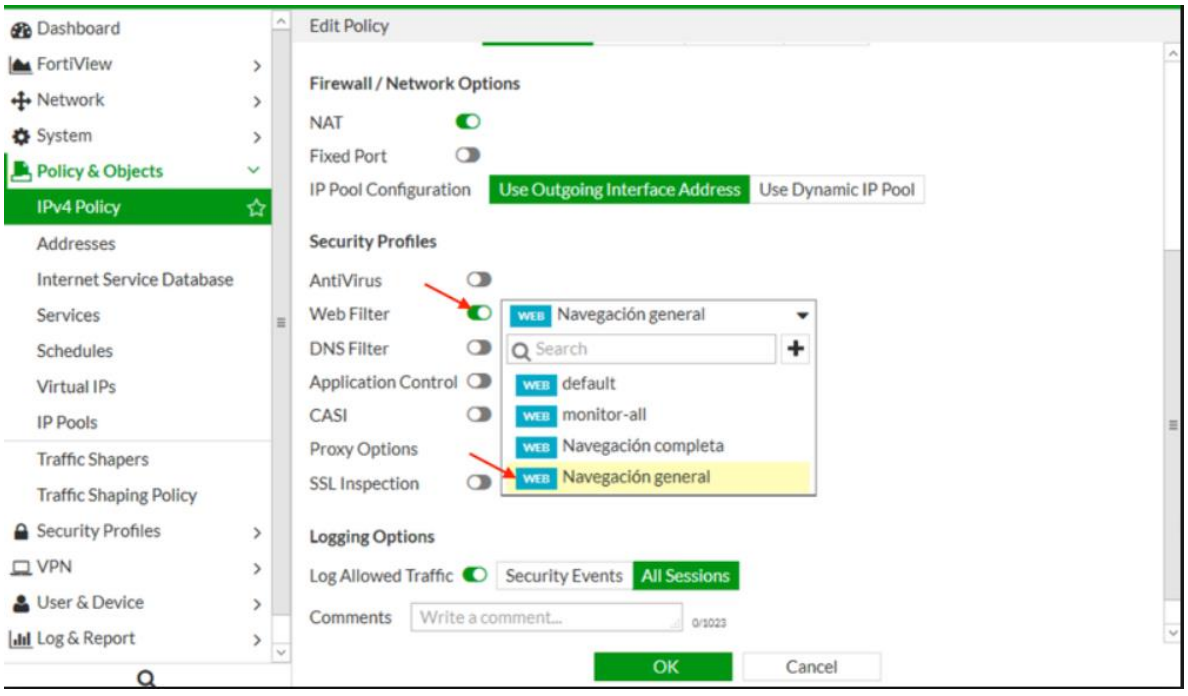
***Fuente**: El autor*

FASE IV

Verificar las funcionalidades del firewall a licenciar

Se establecerá como resultado una herramienta de firewall perimetral completamente configurada, de acuerdo con las necesidades de la Clínica Barraquer, como solución de seguridad informática, prevención de intrusos y control de accesos no autorizados a personal interno, pacientes, etc., con lo anterior el ingreso a la red wifi también estará de manera centralizada con lo cual se podrán también dictar políticas de seguridad para la solución Wireless actual de la Clínica.

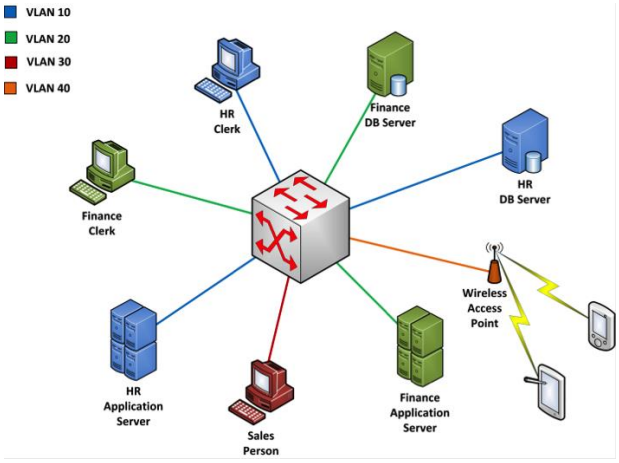
Figura 9.*Panel de creación de políticas de seguridad.*



Fuente: *NCORA. JOSEP. Configuracion de modulo Web Filter en Fortigate.España.:ncora.2017.p.4*

Así mismo se gestionan las redes segmentadas luego del levantamiento debido de información, de hardware, servidores, etc., lo cual facilitará a la Clínica Barraquer la administración de la herramienta luego de ser configurada.

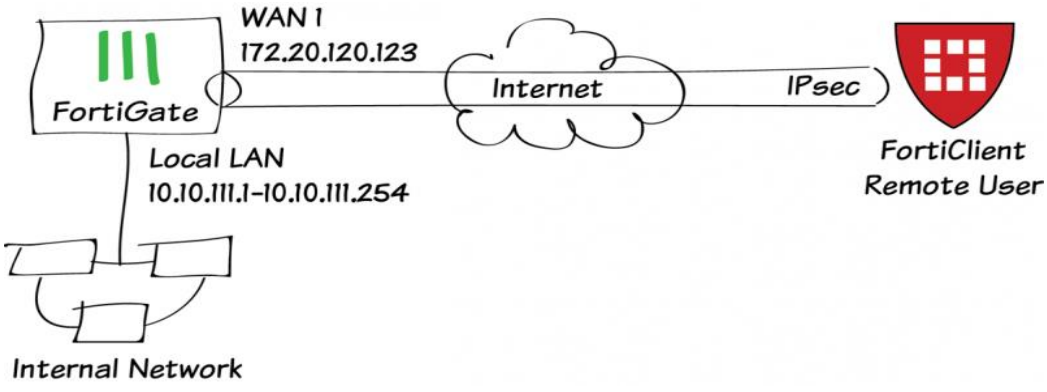
***Figura 10**. Propuesta de segmentación de red para Clínica Barraquer.*



Fuente: RAGASYS. Ejemplo básico I configuración VLANs.España.:2016.p.9

Se gestionan también las Bps tipo SSL, debidamente configuradas de acuerdo con la necesidad de la Clínica Barraquer, teniendo en cuenta políticas de seguridad de acceso a proveedores, empleados, etc., de acuerdo con su función.

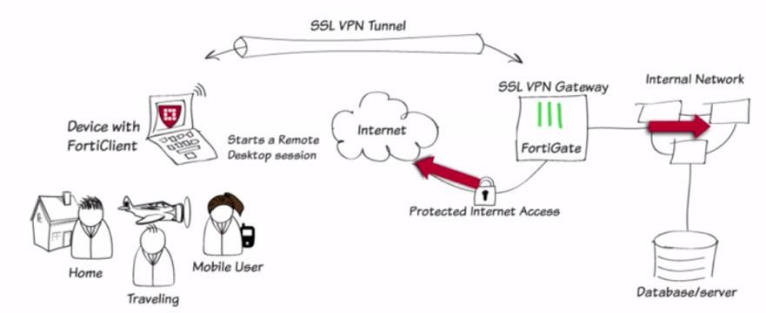
***Figura 11.** Diseño de una VPN en firewall Fortinet.*



Fuente: FORTINET TECHNICAL DOCUMENTATION. IPsec VPN with FortiClient. Estados Unidos.:2018.p.1

Con la configuración de un túnel de acceso VPN los usuarios autorizados podrán acceder desde otro lugar geográfico diferente a clínica Barraquer a la red interna, solo requieren una conexión a internet para poder efectuar dicha conexión remota.

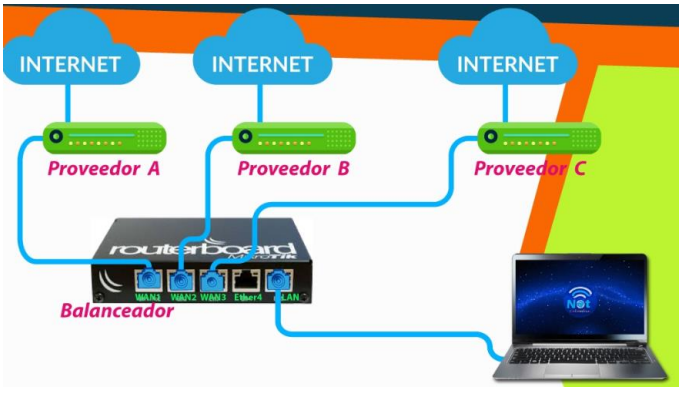
***Figura 12**. Diagrama de flujo de conexión remota desde internet hacia la red interna a través de VPN.*



***Fuente**: FORTINET TECHNICAL DOCUMENTATION. IPsec VPN with FortiClient. Estados Unidos.:2018. p.9*

Configuración de rutas estáticas para canales de internet, balanceo o prioridad:

***Figura 13.** Esquema de balanceo de canales de internet.*



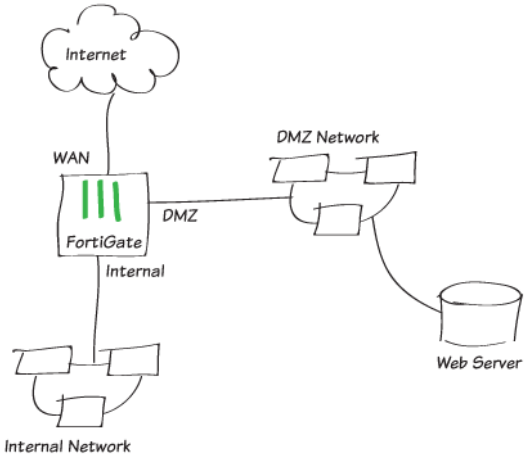
***Fuente**: RICHARDS. REYES. Balanceo de carga MikroTik Links de diferentes velocidades.Colombia.:2015.p.1*

Esquema DMZ propuesto:

En este sistema, se protegerán los servidor web conectándolos a la red DMZ de FortiGate *. Una red DMZ (del término 'zona desmilitarizada') es una red segura, protegida por FortiGate, que solo otorga acceso si se ha permitido explícitamente. Para clínica Barraquer la red DMZ utiliza una subred privada y permite el acceso a un servidor web utilizando diferentes direcciones para usuarios internos y externos, mientras que impide el acceso desde el servidor web a la red interna si el servidor web está en peligro, como se evidencia en la

Una política de cortafuegos WAN a DMZ con una IP virtual (VIP) usa NAT fuente para ocultar la dirección DMZ del servidor web, permitiendo a los usuarios externos acceder al servidor web utilizando una dirección IP pública .Una política de firewall interno a DMZ permite a los usuarios internos acceder al servidor web utilizando su dirección DMZ .Ambas políticas de firewall solo permiten el acceso al servidor web mediante HTTP y HTTPS. No se permite ningún otro acceso. *

Figura 14. *Esquema DMZ para clínica Barraquer*



Fuente: BILL DICKIE. Protecting a web server with DMZ. Estados Unidos.: 2016. p1

Reglas de filtrado Fortinet

Las comprobaciones realizadas por una unidad Fortigate se pueden resumir en cuatro niveles diferentes de control. Si se cumple algún paso dentro de las diferentes capas que contienen una regla de bloqueo, el paquete de datos se descartaría. Estos niveles son los siguientes:

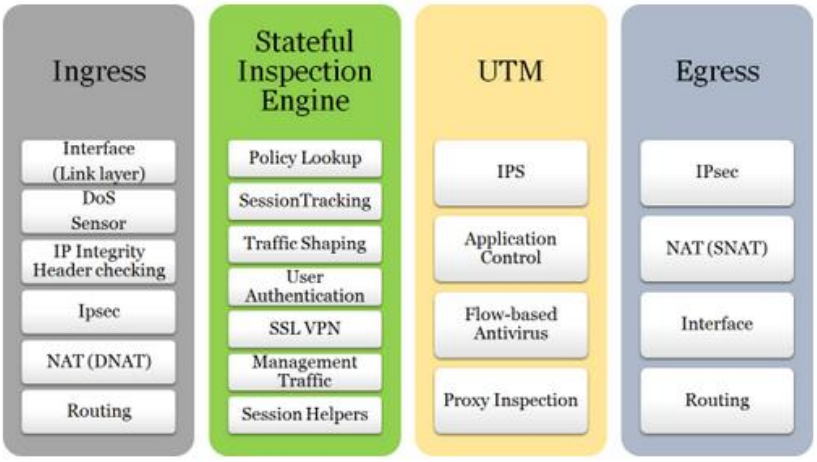
Ingreso: el filtrado de entrada controla el tráfico entrante para proteger la red de los riesgos de seguridad. Los controles relacionados con DOS (Denegación de servicio), el destino IPSEC (Seguridad IP) y el enrutamiento se realizan en el nivel de Ingreso.

Motor Stateful Inspection: la inspección de estado permite que el firewall FortiGate mantenga el contexto con las sesiones activas. Si un paquete es parte de una sesión existente, el paquete atravesará el dispositivo sin control adicional. Si un paquete no coincide con una conexión existente, se evaluará de acuerdo con las reglas del firewall. El motor Stateful Inspection incluye autenticación de usuario, configuración de tráfico, seguimiento de sesión y búsqueda de política.

Escaneo UTM: las unidades FortiGate están pre configuradas con los llamados perfiles UTM. Los perfiles de seguridad de UTM incluyen antivirus, filtrado web, protección contra intrusos (IPS), filtrado de correo electrónico y DataLeakPrevention (DLP). Las unidades FortiGate están pre configuradas con varios perfiles UTM predeterminados, por lo que podemos utilizar los perfiles predeterminados o crear perfiles personalizados para que coincidan con las necesidades de nuestra empresa. Podemos utilizar la información de los perfiles de contenido predeterminados de fábrica de nuestro FortiGate para saber más sobre el perfil predeterminado disponible para un modelo específico.

Egreso: Egreso se realiza en paquetes de datos existentes de la unidad FortiGate. Este tipo de filtrado puede ayudar a contener actividades de botnet y realiza comprobaciones de seguridad en fuentes NAT, I.PSEC y enrutamiento. También se aplican límites máximos de uso de ancho de banda en el nivel de egreso. El siguiente diagrama muestra un esquema que contiene todos estos pasos:

Figura 15. *Esquema de niveles de filtrado.*



Fuente: *FABRIZIO. FortiGate Filters, FortiGate Policies y FortiGate Endpoint Security.Estados Unidos.2014.p2*

Dependiendo de la configuración de seguridad y la configuración de UTM, un paquete podría fluir directamente desde el motor de Inspección de estado a la capa de Egreso.

Dentro de la capa UTM, Proxy Inspection es un paso opcional que contiene controles de Inspección VoIP, Antivirus, Protocolo de Adaptación de Contenido de Internet (ICAP), Filtro Web, Filtro de Correo Electrónico y Prevención de Filtración de Datos. Durante este capítulo, nos centraremos en el motor de Inspección de estado y en las capas de UTM.

Características del firewall

El uso principal de una unidad FortiGate es proteger nuestras redes de ataques con sus características de firewall. Las políticas de seguridad definirán el tráfico de red permitido.

Planificaciones de las políticas de seguridad

Una política de firewall FortiGate también requiere que establezcamos explícitamente un marco de tiempo en el cual la regla mencionada estará activa. El valor predeterminado es Siempre (lo que significa que siempre está activo). Los dos tipos de programas admitidos por FortiGate son los siguientes:

Recurrente: nos permite activar la regla en un día específico de la semana, en un rango específico de días, etc.

Una sola vez: se aplica generalmente para probar políticas o políticas que queremos que sean efectivas bajo demanda por un número limitado de ocurrencias

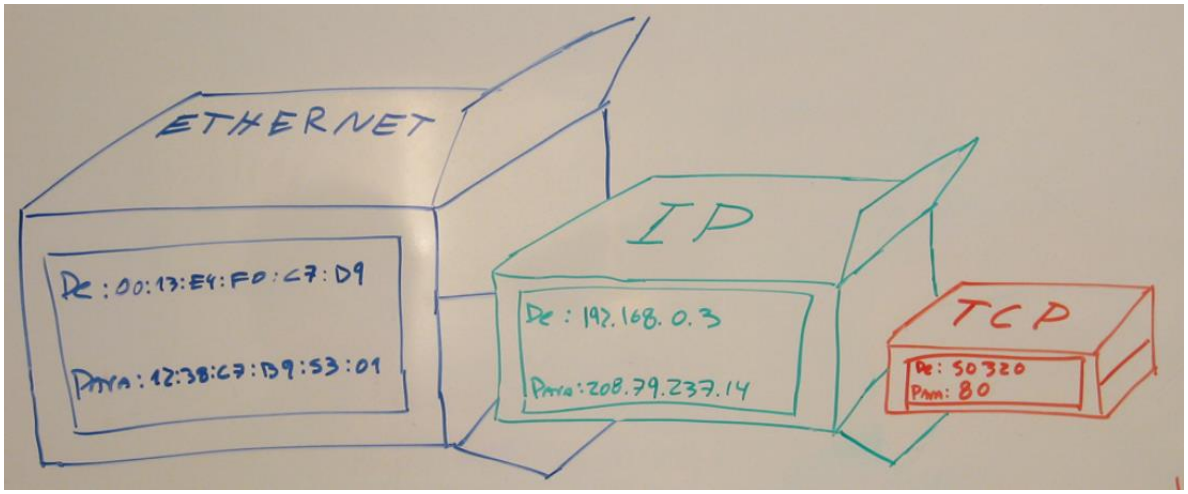
Anatomía de un paquete de red

Un paquete es un contenedor o caja que transporta datos a través de una red TCP / IP. Un paquete es el arbitraje lógico más fundamental de los datos que se pasan a través de una red.

Un paquete normalmente representa la cantidad más pequeña de datos que puede atravesar una red a la vez. Un paquete de red TCP / IP contiene varios elementos de información, incluidos los datos que transporta, direcciones IP de destino de origen y otras restricciones necesarias para la calidad de servicio y el manejo de paquetes.
Cada vez que un nodo en una red envía algunos datos a través de la red, pasa el marco de datos al conmutador y luego al enrutador. El enrutador, después de mirar las direcciones IP de destino, encapsula los datos y los dirige hacia el destinatario. Estos datos encapsulados son el paquete que se reenvía a través de la red.

Los paquetes contienen dos tipos distintos de información para llegar al destino completa y correctamente, a saber, la información de control y los datos que está transmitiendo. La información de control incluye direcciones de destino de origen, formato de secuencia, detección de errores y mecanismos de corrección, todo lo cual ayuda a garantizar la entrega óptima de datos. La información de control generalmente reside en el encabezado y el avance, encapsulando los datos del usuario entre ellos.

***Figura 16**. Anatomía de un paquete.*



***Fuente:** ROMANO. Cosas a saber para montar una red.:Colombia.2009.p1*

Configuración de forticloud para correlacionamiento de logs:

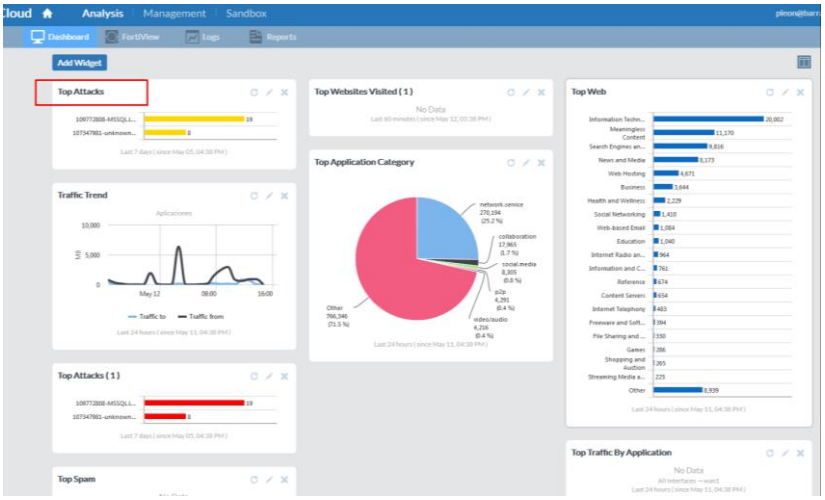
FortiCloud es una plataforma de administración basada en la nube para Fortigate, FortiWiFi y FortiAP que permiten una configuración de dispositivo sencilla y visibilidad para preparar, prevenir, detectar y responder a las amenazas de la red, tal como se evidencia en la figura 17.

Beneficios incluidos:

- Gestión simple y eficiente
- Identificación de amenazas previamente desconocidas
- Análisis de seguridad y visibilidad

Foricloud ofrece una gama de administración y servicios en Fortinet Firewalls y puntos de acceso. FortiCloud ofrece implementación de cero toques, administración de configuración, informes y análisis, espacio aislado para la protección contra amenazas de día cero y los indicadores de compromiso servicio que utiliza el análisis Big Data para identificar las amenazas ya presentes en los dispositivos del cliente.

Figura 17. *Esquema de monitoreo y recolección de logs de seguridad.*

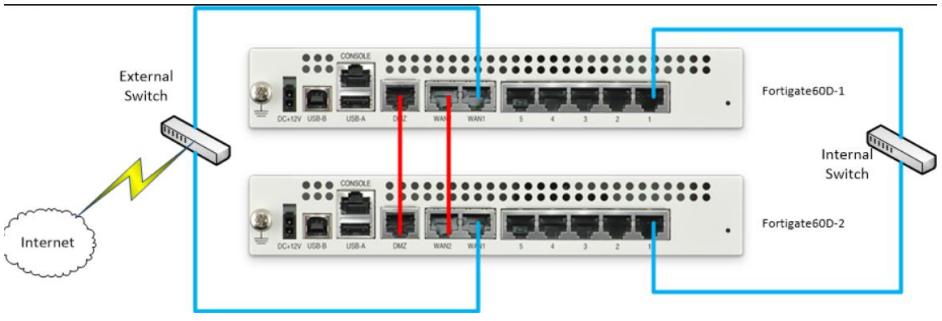


Fuente: *El autor*

Configuración de fortigate en HA (alta disponibilidad)

Para llevar a término esta configuración es conveniente poder efectuar la conexión puerto a puerto entre los dos firewalls, para Clínica Barraquer se tendrá en cuenta un clúster activo – pasivo, para lo cual deberá licenciarse un único Firewall, lo anterior para reducir costos y de acuerdo a la necesidad de clínica Barraquer, quedando configurado como se evidencia en la Figura 18.

Figura 18*. Propuesta de esquema de alta disponibilidad.*



Fuente*: FORTINET TECHNICAL DOCUMENTATION. IPsec VPN with FortiClient. Estados Unidos.:2018. p.16*

La línea FortiGate combina el sistema operativo de seguridad FortiOSTM y las últimas tecnologías de hardware para proporcionar una gama completa y de alto rendimiento de funciones de seguridad y redes.

Las plataformas FortiGate incorporan funciones de red sofisticadas, como alta disponibilidad para el máximo tiempo de actividad de la red y capacidades de dominio virtual (VDOM) para separar varias redes que requieren diferentes políticas de seguridad.

En el corazón de estas funciones de seguridad de redes, están las políticas de firewall. Las políticas de firewall controlan todo el tráfico que intenta pasar a través de la unidad FortiGate, entre interfaces, zonas y subinterfaces de VLAN de FortiGate. Se trata de instrucciones que usan la unidad FortiGate para decidir la aceptación de la conexión y el procesamiento de paquetes para el tráfico que intenta atravesar. En el momento que el firewall recoge un paquete de conexión, considera la dirección de origen, de destino y el servicio del paquete (por número de puerto) e intenta hallar una política de firewall que concuerde con el paquete.

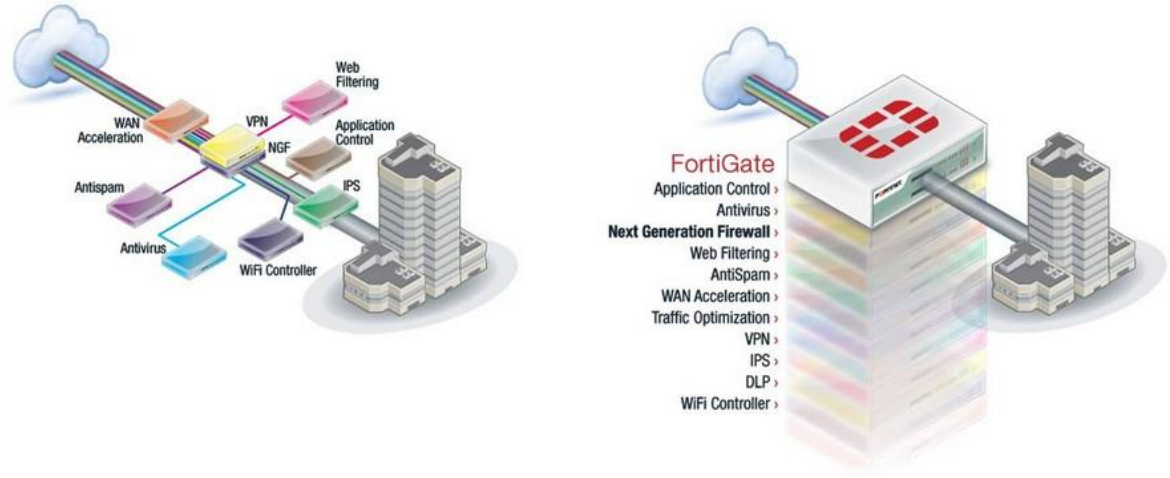
Las políticas de firewall pueden contener muchas instrucciones para que la unidad FortiGate siga cuando recibe paquetes coincidentes. Se requieren algunas instrucciones, como dejar caer o aceptar y procesar los paquetes, mientras que otras instrucciones, como el registro y la autenticación, son opcionales. Es a través de estas políticas que la unidad FortiGate otorga o niega los paquetes y la información dentro o fuera de la red, quién tiene prioridad (ancho de banda) sobre otros usuarios y cuándo pueden obtenerse los paquetes.

A continuación, se describe las características del firewall FortiGate que ayudan a proteger la red, y las políticas de firewall que son las instrucciones para la unidad FortiGate.

Funciones del Firewall

La unidad FortiGate incluye un amplio conjunto de funciones para proteger la red de ataques no deseados. A continuación se proporciona una descripción general de lo que la unidad FortiGate puede proteger. Cada uno de estos elementos se configura y se agregan a las políticas del firewall como un medio de instruir a la unidad FortiGate sobre qué hacer cuando se encuentra con una amenaza a la seguridad.

***Figura 19**. Funciones de firewall fortinet.*



Fuente: ANONIMO.Fortinet Real Time Network Protection.Mexico.2013. p.1

- **Antivirus**

Antivirus es un grupo de características que están diseñadas para evitar que los archivos no deseados y potencialmente maliciosos ingresen a su red. Todas estas características funcionan de diferentes maneras, ya sea mediante el control de un tamaño de archivo, nombre, tipo o la presencia de una firma de virus o grayware.

Las rutinas de exploración de antivirus utilizadas están diseñadas para compartir el acceso al tráfico de la red. De esta forma, cada característica individual no tiene que examinar el tráfico de la red como una operación separada, lo que reduce significativamente los gastos generales. Por ejemplo, si habilita el filtrado de archivos y el análisis de virus, los recursos utilizados para completar estas tareas son solo un poco mayores que la activación del análisis de virus solo. Dos características no requieren el doble de recursos.

La función de escaneo antivirus incluye varios módulos y motores que realizan tareas separadas. La unidad FortiGate realiza el procesamiento antivirus en el siguiente orden:

- Tamaño del archivo

- Patrón de archivo
- Tipo de archivo
- Búsqueda de virus
- Grayware
- Heurística

Si un archivo falla alguna de las tareas del análisis antivirus, no se realizan más escaneos. Por ejemplo, si el archivo "fakefile.exe" se reconoce como un patrón bloqueado, la unidad FortiGate enviará un mensaje al destinatario informándole que el mensaje original tenía un virus, y el archivo se eliminará o se pondrá en cuarentena. El escaneo de virus, grayware, heurística y escaneos de tipo de archivo no se realizarán ya que el archivo ya se ha determinado como una amenaza y se ha solucionado.

- **Filtrado web**

El filtrado web es un medio para controlar el contenido que un usuario de Internet puede ver. Con la popularidad de las aplicaciones web, la necesidad de monitorear y controlar el acceso web se está convirtiendo en un componente clave de los sistemas Secure Content Management que emplean antivirus, filtrado web y seguridad de mensajes. Las razones importantes para controlar el contenido web incluyen:

- Perdió productividad porque los empleados están accediendo a la web por razones no comerciales.
- Congestión de la red: el ancho de banda valioso se utiliza para fines no comerciales y las aplicaciones empresariales legítimas sufren.
- Pérdida o exposición de información confidencial a través de sitios de chat, sistemas de correo electrónico no aprobados, mensajería instantánea y uso compartido de archivos de igual a igual.
- Mayor exposición a amenazas basadas en la web a medida que los empleados navegan por sitios web no relacionados con negocios.
- Responsabilidad legal cuando los empleados acceden / descargan material inapropiado y ofensivo.
- Infracción de derechos de autor causada por empleados que descargan y / o distribuyen material protegido por derechos de autor.

A medida que el número y la gravedad de las amenazas aumentan en la web, el potencial de riesgo también aumenta dentro de la red de la empresa. La navegación web casual no comercial ha causado a muchas empresas innumerables horas de litigios legales, ya que los empleados que descargan y visualizan contenido ofensivo han creado entornos hostiles. Los ataques y amenazas basados en la web también

se vuelven cada vez más sofisticados. Las nuevas amenazas y las aplicaciones basadas en web que están causando problemas adicionales para las corporaciones incluyen:

- Spyware / Grayware
- Suplantación de identidad
- Mensajería instantánea
- Compartición de archivos punto a punto
- Streaming Media
- Ataques de red combinados

- **Filtro antispam / correo electrónico**

La unidad FortiGate realiza el filtrado de correo electrónico (anteriormente llamado antispam) para correo electrónico IMAP, POP3 y SMTP. El filtrado de correo electrónico incluye filtrado de spam y filtrado de las palabras o archivos que no desea permitir en los mensajes de correo electrónico. Si su unidad FortiGate admite el análisis e inspección de contenido SSL, también puede configurar el filtrado de correo no deseado para el tráfico de correo electrónico IMAPS, POP3S y SMTPS.
Puede configurar la unidad FortiGate solicitada mediante la detección e identificación de mensajes no deseados de servidores de spam conocidos o sospechosos. FortiGuard Antispam Service utiliza una base de datos de reputación de IP de remitente y una base de datos de firmas de correo no deseado, junto con sofisticadas herramientas de filtrado de correo no deseado, para detectar y bloquear una amplia gama de mensajes de correo no deseado. Utilizando la configuración del perfil de protección Antispam de FortiGuard puede habilitar la verificación de la dirección IP, la comprobación de URL, la verificación de la suma de comprobación del correo electrónico y el envío de correo no deseado. Las actualizaciones de las bases de datos de reputación de IP y firmas de spam se proporcionan continuamente a través de la red de distribución global de FortiGuard.

Desde la página del Servicio Antispam de FortiGuard en el centro FortiGuard puede usar IP y búsqueda de firmas para verificar si una dirección IP está en la lista negra en la base de datos de reputación IP antispam FortiGuard, o si una URL o dirección de correo electrónico está en la base de firmas.

- **Técnicas de filtro de correo electrónico**

La unidad FortiGate tiene una serie de técnicas disponibles para ayudar a detectar el correo no deseado. Algunos usan el servicio FortiGuard AntiSpam, que requiere una suscripción. El resto usa sus servidores DNS, o listas que debe mantener.
La unidad FortiGate consulta el servicio FortiGuard Antispam para determinar si la dirección IP del cliente que entrega el correo electrónico está en la lista negra. Una coincidencia hará que la unidad FortiGate trate los mensajes entregados como correo no deseado. Si está habilitado, la unidad FortiGate verificará todas las direcciones IP en el encabezado del correo electrónico SMTP contra el servicio FortiGuard Antispam.

La unidad FortiGate consulta el servicio FortiGuard Antispam para determinar si alguna URL en el cuerpo del mensaje está asociada con el correo no deseado. Si alguna URL está en la lista negra, la unidad FortiGate determina que el mensaje de correo electrónico es correo no deseado.

La unidad FortiGate envía un hash de un correo electrónico al servidor FortiGuard Antispam que compara el hash con los hashes de los mensajes spam conocidos almacenados en la base de datos FortiGuard Antispam. Si los resultados hash coinciden, el correo electrónico se marca como correo no deseado.

La unidad FortiGate compara la dirección IP del cliente que entrega el correo electrónico a las direcciones en la lista negra / blanca de la dirección IP especificada en el perfil de protección. Si se encuentra una coincidencia, la unidad FortiGate tomará la acción configurada para la entrada correspondiente de la lista negra / blanca contra todos los correos electrónicos entregados.

La unidad FortiGate toma el nombre de dominio especificado por el cliente en el saludo HELO enviado al iniciar la sesión SMTP, y hace una búsqueda de DNS para determinar si el dominio existe. Si la búsqueda falla, la unidad FortiGate determina que los mensajes entregados durante la sesión SMTP son spam.

La unidad FortiGate compara la dirección de correo electrónico del remitente, como se muestra en el sobre del mensaje MAIL FROM, a las direcciones en la lista negra / blanca de la dirección de correo electrónico especificada en el perfil de protección. Si se encuentra una coincidencia, la unidad FortiGate tomará la acción configurada para la entrada correspondiente de la lista negra / blanca.

La unidad FortiGate realiza una búsqueda de DNS en el dominio de respuesta para ver si hay un registro A o MX. Si no existe tal registro, el mensaje se trata como spam.

La unidad FortiGate bloqueará los mensajes de correo electrónico basados en la coincidencia del contenido del mensaje con las palabras o patrones en la lista de palabras prohibidas del filtro de spam seleccionado.

- **Protección contra intrusos**

El sistema FortiGate Intrusion Protection combina detección y prevención de firmas con baja latencia y excelente fiabilidad. Con Protección contra intrusos, puede crear múltiples sensores IPS, cada uno con una configuración completa basada en firmas. Luego, puede aplicar cualquier sensor IPS a cada perfil de protección. El sistema de protección contra intrusos FortiGate protege su red de ataques externos. Tu unidad FortiGate tiene dos técnicas para lidiar con estos ataques.

La defensa basada en anomalías se usa cuando el tráfico de red se usa como arma. Un host puede verse inundado con mucho más tráfico de lo que puede manejar, haciendo que el host sea inaccesible. El ejemplo más común es el ataque de denegación de servicio, en el cual un atacante dirige una gran cantidad de computadoras para intentar el acceso normal al sistema de destino. Si se realizan suficientes intentos de acceso, el objetivo se ve abrumado y no puede dar servicio a usuarios genuinos. El atacante no obtiene acceso al sistema de destino, pero no es accesible para nadie más. La función DoS de la unidad FortiGate bloqueará el tráfico sobre un cierto umbral del atacante, permitiendo conexiones de otros usuarios legítimos.

La defensa basada en firmas se usa contra ataques conocidos o vulnerabilidades de vulnerabilidades. A menudo, estos involucran a un atacante que intenta obtener acceso a su red. El atacante debe comunicarse con el host en un intento de obtener acceso, y esta comunicación incluirá comandos particulares o secuencias de comandos y variables. Las firmas IPS incluyen estas secuencias de comandos, lo que permite a la unidad FortiGate detectar y detener el ataque.

La base de la protección contra intrusiones basada en firmas son las propias firmas IPS. Cada ataque puede reducirse a una cadena de comandos en particular o una secuencia de comandos y variables. Las firmas incluyen esta información para que su unidad FortiGate sepa qué buscar en el tráfico de la red.

Las firmas también incluyen características sobre el ataque que describe. Estas características incluyen el protocolo de red en el que aparecerá, el sistema operativo vulnerable y la aplicación vulnerable.

Antes de examinar el tráfico de red para detectar ataques, FortiGate identificará cada protocolo que aparezca en el tráfico. Los ataques son específicos del protocolo, por lo que su unidad FortiGate conserva recursos al buscar ataques solo

en los protocolos utilizados para transmitirlos. Por ejemplo, la unidad FortiGate solo examinará el tráfico HTTP para detectar la presencia de una firma que describa un ataque HTTP. Una vez que los decodificadores de protocolo separan el tráfico de red por protocolo, el motor de IPS examina el tráfico de red para las firmas de ataque.

Sin embargo, el motor de IPS no examina el tráfico de red para todas las firmas. Primero debe crear un sensor IPS y especificar qué firmas se incluyen. Sin embargo, no tiene que elegir cada firma que desee incluir individualmente. En cambio, los filtros se utilizan para definir las firmas incluidas.

Los sensores IPS contienen uno o más filtros IPS. Un filtro es simplemente una colección de atributos de firma que usted especifica. Las firmas que tienen todos los atributos especificados en un filtro se incluyen en la firma IPS.

Por ejemplo, si su unidad FortiGate protege un servidor Linux que ejecuta el software del servidor web Apache, puede crear un nuevo filtro para protegerlo. Configure OS en Linux, y Application to Apache y el filtro incluirá solo las firmas aplicables tanto a Linux como a Apache. Si desea buscar todas las firmas de Linux y todas las firmas de Apache, debe crear dos filtros, uno para cada uno.

- **Traffic Shaping**

La configuración del tráfico, cuando se incluye en una política de firewall, vigila el ancho de banda favorable e instaura la prioridad del tráfico procesado por la política. La configuración del tráfico permite controlar qué políticas tienen la mayor prioridad cuando se mueven grandes cantidades de datos a través de la unidad FortiGate. Por ejemplo, la política para el servidor web corporativo podría tener mayor prioridad que las políticas para la mayoría de las computadoras de los empleados. Un empleado que necesita acceso a Internet de alta velocidad adicional podría tener una política de salida especial configurada con mayor ancho de banda.

La configuración del tráfico está disponible para las políticas de firewall cuya Acción es ACCEPT, IPSEC o SSLVPN. También está disponible para todos los servicios compatibles, incluidos H.323, TCP, UDP, ICMP y ESP.

La configuración del tráfico no puede aumentar la cantidad total de ancho de banda disponible, pero puede usarla para mejorar la calidad del tráfico intensivo en ancho de banda.

El ancho de banda disponible para el tráfico establecido en un modelador de tráfico se usa para controlar las sesiones de datos para el tráfico en ambas direcciones. Por ejemplo, si se aplica ancho de banda garantizado a una política de FTP interna

y externa, y un usuario en una red interna usa FTP para colocar y obtener archivos, tanto las sesiones de envío como las de reparto comparten el ancho de banda disponible para el tráfico controlado por la política.

Una vez incluido en una política de firewall, el ancho de banda garantizada y máxima es el ancho de banda total disponible para todo el tráfico controlado por la política. Si varios usuarios inician varias sesiones de comunicación utilizando la misma política, todas estas sesiones de comunicaciones deben compartir el ancho de banda disponible para la política como lo indica Roberto en su boletín[11].

Sin embargo, la disponibilidad de ancho de banda no se comparte entre varias instancias de uso del mismo servicio si estas múltiples instancias están controladas por diferentes políticas. Por ejemplo, puede crear una política FTP para limitar la cantidad de ancho de banda disponible para FTP para una dirección de red y crear otra política FTP con una disponibilidad de ancho de banda diferente para otra dirección de red.

La configuración del tráfico intenta "normalizar" los picos / ráfagas de tráfico para priorizar ciertos flujos sobre otros. Pero hay una limitación física a la cantidad de datos que pueden almacenarse en búfer y al período de tiempo. Una vez superados estos umbrales, se eliminarán los marcos y paquetes, y las sesiones se verán afectadas de otras maneras. Por ejemplo, configuraciones de configuración de tráfico incorrectas pueden en realidad degradar aún más ciertos flujos de red, ya que el descarte excesivo de paquetes puede crear una sobrecarga adicional en las capas superiores que puede estar intentando recuperarse de estos errores.

Un enfoque básico de configuración del tráfico es priorizar ciertos flujos de tráfico sobre otro tráfico cuyo posible descarte es menos ventajoso. Esto significaría que acepta sacrificar cierto rendimiento y estabilidad en el tráfico de baja prioridad, para aumentar o garantizar el rendimiento y la estabilidad del tráfico de alta prioridad.

Si, por ejemplo, está aplicando limitaciones de ancho de banda a ciertos flujos, debe aceptar el hecho de que estas sesiones pueden ser limitadas y, por lo tanto, tener un impacto negativo. La configuración del tráfico aplicada a una política de firewall se aplica para el tráfico que puede fluir en cualquier dirección. Por lo tanto, una sesión que puede ser configurada por un servidor interno a uno externo, a través de una política de interno a externo, tendrá una configuración de tráfico aplicada incluso si el flujo de datos fluye de externo a interno. Un ejemplo puede ser un "get" de FTP o un servidor SMTP conectándose a uno externo, para recuperar el correo electrónico.

[11] HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Boletín de Política Informática N° 2. Página 7. España. 2000.

La configuración del tráfico es efectiva para el tráfico IP normal a las tasas de tráfico normales. La configuración del tráfico no es efectiva durante los períodos en que el tráfico excede la capacidad de la unidad FortiGate. Dado que los paquetes deben ser recibidos por la unidad FortiGate antes de que estén sujetos a la configuración del tráfico, si la unidad FortiGate no puede procesar todo el tráfico que recibe, es probable que se produzcan paquetes perdidos, retrasos y latencia.

Modo de Ejecución NAT

En el modo NAT, la unidad FortiGate es visible para la red a la que está conectada. Todas sus interfaces están en diferentes subredes. Cada interfaz que está conectada a una red debe configurarse con una dirección IP que sea válida para esa subred.

Por lo general, utilizará el modo NAT cuando la unidad FortiGate se implementa como una puerta de enlace entre redes privadas y públicas. En su configuración predeterminada de modo NAT, la unidad FortiGate funciona como un firewall. Las políticas de firewall controlan las comunicaciones a través de la unidad FortiGate tanto a Internet como a las redes internas. En el modo NAT, la unidad FortiGate realiza la traducción de direcciones de red antes de que los paquetes IP se envíen a la red de destino. Por ejemplo, una empresa tiene una unidad FortiGate como su interfaz a Internet. La unidad FortiGate también actúa como un enrutador para múltiples subredes dentro de la compañía como lo ilustra Roberto en su boletín[12].

- **Cómo funciona la traducción de direcciones**

En el modo NAT, las políticas de firewall realizan la traducción de direcciones entre las interfaces internas y externas. Cuando un usuario accede a un sitio web, por ejemplo, el sitio web solo conoce la solicitud mediante la interfaz externa de la unidad FortiGate, en este ejemplo, wan1.

Por ejemplo, un usuario navega a un servidor web (dirección IP XXX.XXX.XX.XX). La PC del usuario tiene una dirección IP de XX.XX.XX.X en la interfaz interna. La unidad FortiGate recibe la solicitud del usuario para ir al servidor web. La interfaz externa de la unidad FortiGate para enviar y recibir información es want 1 (XXX.XXX.XX.XX). La unidad FortiGate analiza las políticas del firewall para determinar a dónde debe ir la solicitud, en este caso, la interfaz externa.

La unidad FortiGate cambia la información del paquete de la dirección de retorno a su interfaz externa, mientras realiza un seguimiento de la solicitud del usuario de

[12] HERNÁNDEZ, Roberto. Firewalls: Seguridad en las redes e Internet. Boletín de Política Informática N° 2. Página 10. España. 2000.

origen y la dirección de PC de origen. Una vez modificada, la unidad FortiGate envía la información del paquete al servidor web.

Cuando el servidor web envía la respuesta, la envía a lo que cree que es la dirección de origen, la dirección Fort1Gate wan1, XXX.XXX.XX.XX. Cuando la unidad FortiGate recibe la información, determina dónde debe ir mirando su información de sesión. Al usar políticas de firewall, determina que la información debe dirigirse al usuario de origen en XX.XX.XX.X El FortiGate cambia la IP de destino al usuario correcto y entrega el paquete.

A lo largo de este intercambio, que se produce en nanosegundos, y debido a la tracción de direcciones de red, el servidor web no sabe que la dirección de origen es realmente XX.XX.XX.X, sino XXX.XXX.XX.XX.

- **Tabla NAT central**

La tabla NAT central le permite definir y controlar con mayor detalle la traducción de direcciones realizada por la unidad FortiGate. Con la tabla NAT, puede definir las reglas que dictan la dirección de origen o el grupo de direcciones y qué grupo de IP usa la dirección de destino.

La tabla NAT también funciona de la misma manera que la tabla de políticas del firewall. Es decir, la unidad FortiGate lee las reglas NAT en una metodología de arriba hacia abajo, hasta que alcanza una regla de coincidencia para la dirección entrante. Esto le permite crear múltiples políticas de NAT que dictan qué grupo de IP se usa en función de la dirección de origen. Las políticas NAT también se pueden reorganizar dentro de la lista de políticas, del mismo modo que las políticas de firewall.

11. RECURSOS NECESARIOS PARA EL DESARROLLO

Se indican a continuación los recursos tanto humanos como de infraestructura que se requieren para llevar a término el proyecto:

14.1. Recurso humano:

- **Oficial de seguridad informática:** El cual se encarga de realizar el levantamiento de las políticas de seguridad, de acuerdo a la necesidad de la Clínica Barraquer y del análisis de vulnerabilidades efectuado.

- **Ingeniero de redes e infraestructura:** Se encargara de realizar todo el tema de levantamiento de información acerca de servidores, aplicaciones, redes, hardware y software.

14.2. Recursos físicos

- Dos firewall HW Fortigate 300 C
- 1 equipo de cómputo, Core I3, 4GB de memoria RAM, PUTTY instalado.
- Cable serial
- 7 metros de Cable RJ45 categoría

12. PRESUPUESTO

Tabla 14.*Relación de presupuesto de proyecto.*

RECURSO	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Oficial de seguridad informática	1	$ 4.500.000	$ 4.500.000
Ingeniero de redes e infraestructura	1	$ 3.700.000	$ 3.700.000
Equipo de computo	1	$ 2.000.000	$ 2.000.000
FW fortigate 300 C	2	$ 7.200.000	$ 14.400.000
Cable serial	1	$ 25.000	$ 25.000
Metro de cable RJ45	7	$ 7.000	$ 49.000
TOTAL			**$ 24.674.000**

Fuente: *El autor*

13. CONCLUSIONES

Se examinaron varios diseños de firewall centrados en Internet en un intento de cumplir con los requisitos de seguridad y rendimiento de las aplicaciones de varios niveles. En todos los escenarios, los servidores que alojan los componentes de las aplicaciones se separaron de la red corporativa de la compañía utilizada para realizar negocios internos, como un paso inicial para segregar recursos con diferentes requisitos de seguridad. Para controlar estrechamente las interacciones entre los niveles de la aplicación, se analizaron los niveles de alojamiento de la aplicación en subredes dedicadas. Al implementar firewall, se pudo aumentar significativamente la dificultad de obtener acceso no autorizado a recursos sensibles de Internet.

Se realizó el respectivo levantamiento de información de la red, de servicios informáticos y aplicaciones, con lo anterior se pudo tener un esquema general del estado del diseño previo, lo cual ayudo a un mejor análisis de implementación acotando los servicios actuales de Clinica Barraquer.

Se identifica una serie de vulnerabilidades críticas que es de inmediata atención para evitar que un atacante informático pueda explotarlas, adicional se indago acerca de los ataques más utilizados por hackers e intrusos en el sector salud, entre los cuales se encuentran, correo electrónico malicioso, phising, ataque por logueo de fuerza bruta, Wannacry – Ramsonware y troyanos.

En este proyecto, se indica que al diseñar la red, se deben considerar otros componentes del perímetro, tales como sistemas de detección de intrusos, enrutadores y VPN, todos los anteriores están inmersos en la solución presentada y se garantiza que no habrá afectación de la infraestructura y se selecciona un diseño que coincide con la arquitectura de las aplicaciones y las necesidades comerciales de clínica Barraquer

Se gestiona la creación de políticas de seguridad en el firewall categorizadas por acceso a puertos específicos, a páginas y aplicaciones estrictamente garantizadas para la gestión básica de cada usuario, paciente y empleado, con lo cual se establecen controles de acceso y jerarquías de permisos para poder limitar los accesos.

14. RECOMENDACIONES

Cada fuente de información de los departamentos de gestión de Clínica Barraquer en el margen de los procesos alineados al sistema de gestión de seguridad informática, es muy importante para definir los parámetros de configuración de políticas de seguridad perimetral, así mismo la capacitación y concientización del personal de la organización en cuanto a temas se seguridad informática y de la información.

Es importante contemplar factores exógenos al diseño de seguridad del firewall perimetral, para prevenir afectaciones del servicio de aplicaciones y demás factores que deban interactuar con el firewall.

Es importante que se aplique una regla de firewall de tal manera que la red de usuarios no pueda llegar con facilidad a la red de servidores.

Se recomienda extender un sistema de gestión de seguridad de la información en todos los procesos de la Clínica Barraquer.

Es recomendable implementar un sistema de control de acceso a la red dado que cualquier persona que se conecte a la red va a tomar una dirección IP y navegación a internet.

BIBLIOGRAFIA

BROBECK, Casi. Firewall: Historia. En: Ostec. Julio, 2017. Vol. 1, no. 1, p. 1-2.

CLARENC, Hernán. Tutorial cómo definir y configurar las Políticas de Firewall en Fortigate. En: ZTNet. Agosto, 2013. Vol. 1, no. 1, p. 1-2.

CLARENC, Hernán. Tutorial cómo definir y configurar las Políticas de Firewall en Fortigate. En: ZTNet. Agosto, 2013. Vol. 1, no. 1, p. 1-2.

HERRERO, Héctor. Configurando un clúster dos o más Fortigate. En: Bujarra. Octubre, 2008. Vol. 1, no. 1, p. 1-2.

JORGE. Fortigate – IP de Fábrica y configuración de las interfaces por consola. En: NKSistemas. Mayo, 2012. Vol. 1, no. 1, p. 1-2.

MARTIN, Victoria. Installing a FortiGate in NAT/Route mode. En: Cookbook. Julio, 2014. Vol. 1, no. 1, p. 1-2.

SANTILLAN. Hugo. Fortinet quiere administrar el wi-fi más fácil desde la nube. En: SiliconWeek. Agosto, 2015. Vol. 1, no. 1, p. 1-2.

SIN INFORMACION. Fortinet lanza los primeros puntos de acceso inalámbricos universales de la industria. En: NeoDigital. Julio, 2016. Vol. 1, no. 1, p. 1-2.

SIN INFORMACION. FortiGuard Labs de Fortinet. En: Arrowecs. Octubre, 2016. Vol. 1, no. 1, p. 1-2.

VERDU, Marga. Fortinet mejora la seguridad de las redes Wifi con FortiCloud. En: ComputerWorld. Septiembre, 2015. Vol. 28, no. 1, p. 1-2.

ANEXO A

AUTORIZACION PARA EJECUCION DE PROYECTO

Clínica Barraquer
Centro Oftalmológico

Bogotá, 06 de junio de 2018

Señores:
OFTALMOS S.A
Gerencia de TI (Tecnología informática)
Bogotá

Asunto: Solicitud de autorización implementación de firewall Fortinet

Reciba un cordial saludo,

Mediante el presente documento solicito su aval para poder gestionar la implementación del firewall perimetral Fortinet 300 C, orientado a establecer un control de seguridad a nivel de la red interna de Clinica Barraquer.

Muchas gracias.

Sls,

Nombre: Paula León R
D.I: C.C 1023880317
Empresa: ***OFTALMOS S.A***

OFTALMOS S.A.
860.004.676-8
DEPARTAMENTO DE TECNOLOGÍA
06 JUN 2018
REVISADO

Dirección: Av. 100 No. 18a-51 Bogotá D.C., Colombia • Teléfonos: (+57)(+1) 218 7077 - (+57)(+1) 644 9555 • Fax (+57)(+1) 610 4406
Web. www.barraquer.com.co