ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD INFORMÁTICA A NIVEL LÓGICO Y FÍSICO EN LOS SERVIDORES EXPUESTOS A INTERNET DE UNA EMPRESA PRIVADA DE VENTA AL DETALLE"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

María Isabel Galarza Soledispa

GUAYAQUIL – ECUADOR

Año: 2016

AGRADECIMIENTO

Al Dios de Israel principalmente y de manera especial a mi madre Isabel, a mis hermanos José, Angélica y Silvana, a mi novio Andrés, a mis líderes espirituales Elkin y Leisa, a mi jefe directo, a mis amigos y a todos quienes me apoyaron en el desarrollo de este proyecto.

.

DEDICATORIA

A mi padre José Hitler Galarza Rodríguez,

cuyo sueño se cumple mediante este logro

aunque ya no está presente.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenín Freire

DIRECTOR MSIA

Mgs. Roky Barbosa	Mgs. Omar Maldonado
PROFESOR DELEGADO	PROFESOR DELEGADO
POR LA UNIDAD ACADÉMICA	POR LA UNIDAD ACADÉMICA

RESUMEN

El presente proyecto tiene como objetivo implementar mecanismos de seguridad en los servidores [3] expuestos a Internet de la compañía Intermediaria de Ventas que es una empresa de venta de ropa a nivel del Ecuador.

Básicamente se realizará la evaluación de la seguridad de los servidores de correo electrónico y facturación electrónica para identificar los riesgos y amenazas a los que están expuestos.

A nivel general se realiza el análisis de problemas presentados como saturación del ancho de banda y accesos remotos no autorizados producto de una inadecuada gestión de usuarios.

A través del uso de los mecanismos de seguridad, se podrá conseguir lo siguiente:

- Establecer medios de protección a la información contenida en los servidores.
- Se evitará el ingreso de usuarios no autorizados a la red de la organización.
- Uso equilibrado del ancho de banda.
- Los usuarios internos pueden acceder a cualquier sitio de internet bajo los filtros web adecuados.
- Implementación de medios de comunicación seguros para conexiones remotas.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

DNAT	Destination Network Address Translation(Traducción de dirección de red destino)
SNAT	Source Destination Address Translation (Traducción de dirección de red origen)
SSL	Secure Sockets Layer (Capa De Conexión Segura)
VPN	Virtual Private Network(Red Privada Virtual)

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad la seguridad informática se ha convertido en un pilar vital para las empresas, en especial cuando exponen sus servicios a través de Internet.

Un servidor en una red pública, se convierte en un objetivo para los atacantes conocidos como hackers. Por esta razón, es de suma importancia para el administrador fortalecer el sistema a nivel lógico y físico y establecer políticas de denegación de permisos para bloquear a usuarios no autorizados con el objetivo de proteger la información, el bien más importante de las organizaciones en la actualidad y al mismo tiempo proveer un desempeño adecuado de toda la red.

CAPÍTULO 1

GENERALIDADES

El presente capítulo tiene como objetivo conocer información de la empresa Fashion Style y la situación actual de los servidores de bases de datos, facturación electrónica y servidor de operaciones de sistemas con acceso a Internet y de la importancia que éstos representan al negocio.

1.1 Descripción general de la empresa

La empresa Fashion Style es una empresa comercial ecuatoriana establecida desde el 1 de diciembre de 1990 y está dedicada a la venta de ropa nacional e importada en las principales ciudades del país como son Guayaquil, Quito, Manta, Portoviejo, Machala, Santo Domingo y Quevedo. Cuenta con dieciséis sucursales, siendo su mayor presencia en las ciudades de Guayaquil y Quito.

Cuenta con un centro de distribución de mercadería ubicado en la matriz y maneja un personal de 1,000 empleados.

1.2 Visión

Lograr satisfacer las necesidades de vestimenta de todas las familias ecuatorianas.

1.3 Misión

Ser un canal entre el productor de confecciones y nuestros clientes finales, que permitan al primero conocer más a fondo las necesidades de sus consumidores, una expansión de sus productos en el mercado y una mejor rotación de su capital, y a los segundos adquirir productos de calidad a los mejores precios y la satisfacción en sus compras.

1.4 Infraestructura de la red actual.

La empresa actualmente cuenta con enlace de datos provisto por la empresa Telconet, con quien además se mantienen otros servicios Internet.

A través del enlace las sucursales se comunican hacia la matriz. Por motivos de seguridad, las sucursales no tienen habilitado el servicio de Internet, ya que la administración total de la empresa se encuentra centralizada en la ciudad de Guayaquil.

En la matriz la red LAN tiene las siguientes características:

- Ancho de banda de Internet: 8M
- Ancho de banda entre las sucursales: 2MB
- 1 RAC con 4 servidores físicos
- Equipos en alquiler por el proveedor:
    a. 1 Fortigate
    b. 1 Router para Internet
    c. 1 Router para datos

1.5 Descripción de servidores y bases de datos principales de la empresa.

La empresa cuenta con un Data Center ubicado en la matriz, donde existe un RAC con cuatro servidores físicos, dentro de los cuales existen servidores virtuales para las aplicaciones y bases de datos.

Los servidores se encuentran en la matriz y cada almacén dispone de su propio servidor y base de datos local para tener siempre activo el servicio de venta al público en caso de pérdida de comunicación.

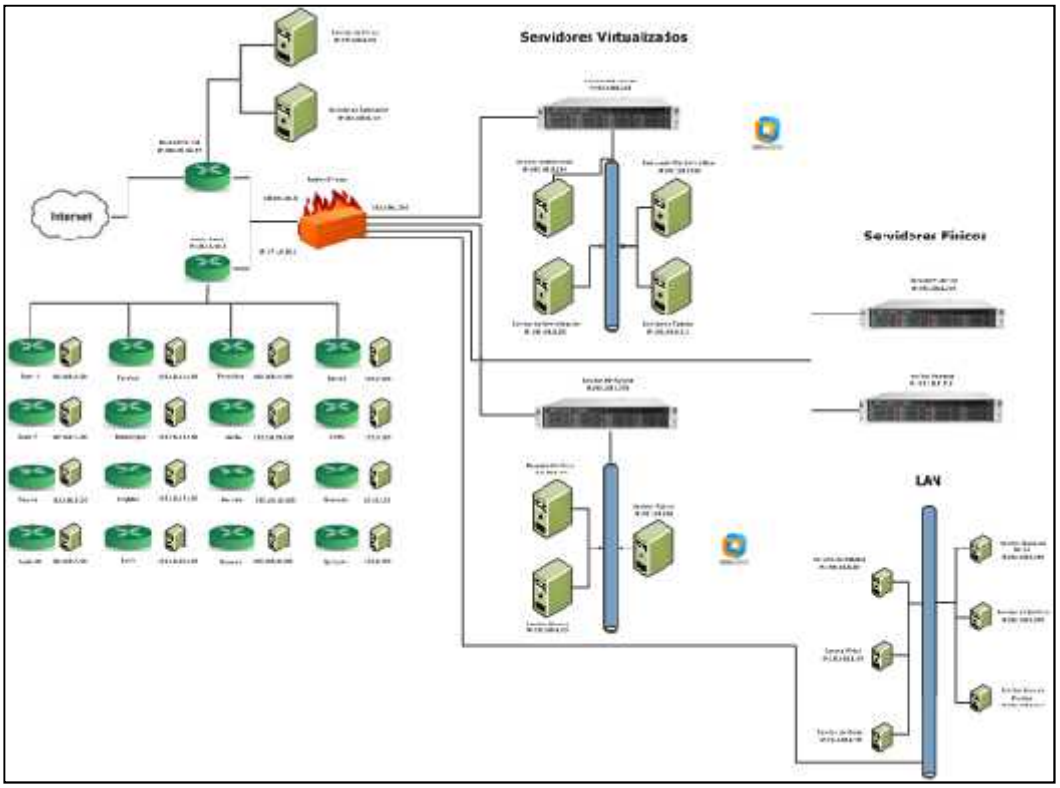

FIGURA 1. 1 Diagrama de Red de la organización

CAPÍTULO 2

ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

Actualmente, a nivel externo los servidores que interactúan como con Internet son: Correo electrónico, Operador de procesos y el de Facturación Electrónica, los cuales están directamente conectados al router de Internet del ISP por lo que todo el tráfico externo es permitido por estos equipos con el riesgo de sufrir algún ataque y la exposición a amenazas externas.

A nivel interno uno de los grandes problemas que existe es que usuarios del área administrativa de la empresa disponen de acceso total a Internet a tal punto que se encontró que algunos de ellos usan herramientas de acceso remoto como

Teamviewer sin la respectiva autorización. Esto a la vez, genera lentitud en el servicio de Internet y saturación del ancho de banda disponible.

2.1 Políticas y mecanismos de control utilizados para proveer seguridad a los servidores.

La empresa cuenta con varios controles que ayudan a prevenir acceso de personas autorizadas entre los cuales podemos mencionar:

1. Ningún usuario puede ser creado por los administradores de las sucursales. No disponen de las herramientas para hacerlo.
2. Las sucursales no disponen de acceso a Internet.
3. Existe un administrador responsable del manejo de los permisos a los servidores, quien solo crea los usuarios y correos electrónicos con la autorización respectiva.
4. Todos los cambios en las aplicaciones de la organización tienen la autorización de la gerencia.
5. Se dispone de un Data Center ubicado en un espacio separado del Dpto. de Sistemas.

No obstante, se requiere implementar nuevos mecanismos de seguridad para proteger la información de la empresa.

2.2 Administración de la red.

La administración de la red es desconocida parcialmente porque no existe documentación detallada sobre las políticas de seguridad aplicadas. Así

mismo se dispone de un equipo [2] Fortigate 200B que no es usado en su total potencialidad.

A nivel de la estructura de red, podemos notar que en el gráfico los servidores que interactúan con el Internet (Correo y Portal Web Facturación Electrónica) están directamente conectados al Router de Internet del ISP; por lo tanto, todo el tráfico externo es permitido por estos equipos. Cada uno de ellos consta con dos NIC, una para su direccionamiento LAN y otra interfaz para su direccionamiento público.

2.3 Identificación de los usuarios, clientes, proveedores que tienen acceso.

Actualmente las claves son generadas bajo un patrón estándar muy sencillo y fácil de descifrar; por lo tanto muchos usuarios podrían ingresar a cualquier equipo remotamente dentro de la misma red.

Los servidores cuentan con contraseñas que solo son conocidas por el personal de sistemas responsable. Sin embargo, algunas no han sido renovadas a medida que ha salido personal del área de sistemas.

2.4 Gestión actual de otorgación y denegación de permisos.

La gestión de usuarios se realiza de manera muy sencilla. Por lo general, se efectúa mediante un correo electrónico y se da acceso de nivel de usuario administrador para los usuarios que acceden a los servidores.

2.5 Identificación de servicios y aplicaciones expuestos a Internet en los servidores

Actualmente, los siguientes servidores no tienen restricción alguna:

- Correo Electrónico
- Facturación Electrónica
- Aplicaciones Web

2.6 Definición de problemas que afectan al ancho de banda.

No existen restricciones a sitios no permitidos: Los permisos que tienen los usuarios con acceso Internet es total. Es decir, no existen grupos o niveles de usuario para una correcta administración de permisos ni bloqueos por contenido de páginas web.

Lentitud en el servicio de Internet: Es un problema que se presenta como consecuencia de una apertura total a Internet a todos los usuarios del área administrativa. Otro de los inconvenientes que se dan es que los usuarios pueden acceder a YouTube, por el cual descargan películas, lo cual genera latencia en los servicios propios de la empresa.

Saturación del ancho de banda: Se ocasiona debido a que por el mismo canal, se transmiten los registros de vídeo vigilancia de todas las sucursales. Como podemos observar en el siguiente gráfico, el servicio de 8MB disponible de ancho de banda que tiene la empresa se usa su capacidad total por lo que existe saturación del mismo.

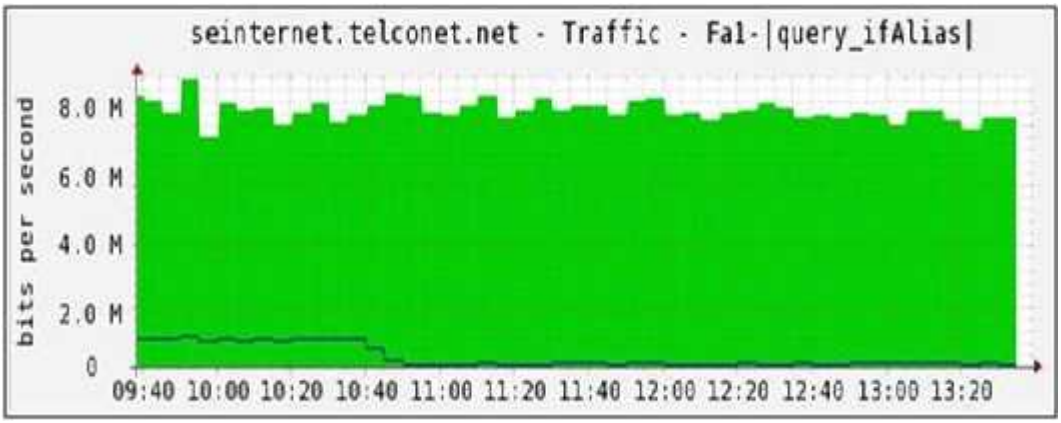

FIGURA 1. 2 Saturación del ancho de banda

CAPÍTULO 3

PLAN DE ACCIÓN DE IMPLEMENTACIÓN DE SEGURIDAD

A través del uso de los mecanismos de seguridad, se podrá establecer medios de protección a la información contenida en los servidores y se evitará el ingreso de usuarios no autorizados a la red de la organización.

3.1 Gestión adecuada de permisos y denegaciones para usuarios internos y externos

3.1.1 Administración del Equipo Fortigate 200B

Para una correcta organización de los usuarios hemos solicitado al proveedor Telconet ampliar el alcance de nuestra gestión en el equipo Fortigate 200B ya que la administración del equipo es compartida con

ellos y nuestro acceso no nos permite hacer una buena gestión a nivel de usuarios y administración del Firewall.

3.1.2 Gestión de Usuarios de Internet

Con el uso de las ventajas que nos ofrece el Fortigate, se definen perfiles y grupos de usuarios de Internet por Departamento de acuerdo a sus actividades diarias con el objetivo de obtener los siguientes resultados:

- Optimizar los recursos de ancho de banda
- Restringir todos accesos a Internet a las direcciones IP no autorizadas.

	Departamentos							
Web Filter	Contabilidad	RRHH	Compras	Publicidad	Gerencia	Mercadeo	Taller	Médico
Potentially Liable								
Drug Abuse	X	X	X	X	X	X	X	X
Hacking	X	X	X	X	X	X	X	X
Illegal or Unethical	X	X	X	X	X	X	X	X
Discrimination	X	X	X	X	X	X	X	X
Explicit Violence	X	X	X	X	X	X	X	X
Extremist Groups	X	X	X	X	X	X	X	X
Proxy Avoidance	X	X	X	X	X	X	X	X
Plagiarism	X	X	X	X	X	X	X	X
Child Abuse	X	X	X	X	X	X	X	X
Adult/Mature Content								
Alternative Beliefs	X	X	X	X	X	X	X	X
Abortion	X	X	X	X	X	X	X	√
Other Adult Materials	X	X	X	X	X	X	X	X
Advocacy Organizations	X	X	X	X	X	X	X	√
Gambling	X	X	X	X	X	X	X	X
Nudity and Risque	X	X	X	X	X	X	X	√
Pornography	X	X	X	X	X	X	X	X
Dating	X	X	X	X	X	X	X	X
Weapons (sales)	X	X	X	X	X	X	X	X
Marijuana	X	X	X	X	X	X	X	X
Sex Education	X	X	X	X	X	X	X	√
Alcohol	X	X	X	X	X	X	X	√

FIGURA 3. 1 Creación de grupos de usuarios

3.1.3 Creación de Filtros Web

Se definen filtros Web para crear restricciones a los grupos de usuarios cuando consulten información en la web. Esto nos ayudará a

no saturar el ancho de banda y evitar el acceso a sitios web que pueden representar un riesgo a la empresa.

FIGURA 3. 2 Creación de Filtros Web

3.2 Implementación de seguridad a nivel de servidor y de la red

3.2.1 Implementación de documentación de información de la red.

Se procedió a realizar la documentación de la empresa haciendo las inspecciones respectivas a nivel físico y posteriormente a nivel lógico, iniciando desde el diseño de la red. Dentro de la documentación que se realizó en la empresa se obtuvo:

- Informe de licenciamiento
- Diseño de la Red
- Gestión y procedimientos de seguridad

- Diseño de la Red LAN y equipos de la red con sus características de toda la empresa.
- Servidores con sus funciones y características.

3.2.2 Migración de Servidores Públicos detrás del Firewall Externo

A continuación se describe el diseño topológico lógico encontrado y a la vez, el nuevo diseño, el cual consiste en agregar el Servidor de Correo Electrónico detrás del Firewall [5] para evitar ataques e intrusiones externas.

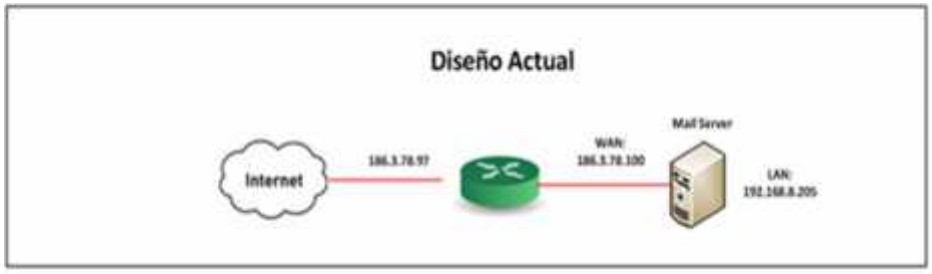

FIGURA 3. 3 Ubicación actual del servidor de correo

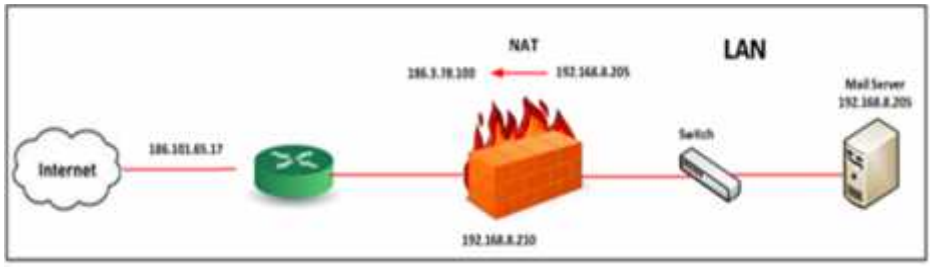

FIGURA 3. 4 Nueva ubicación del servidor de correo

Es necesario auditar las conexiones entrantes y salientes en el firewall. Para tal efecto, configuraremos un NAT [6] para que traduzca

nuestra IP interna 192.168.8.205 a su respectiva IP Pública 186.3.78.100 y de esta manera son redireccionadas las peticiones.

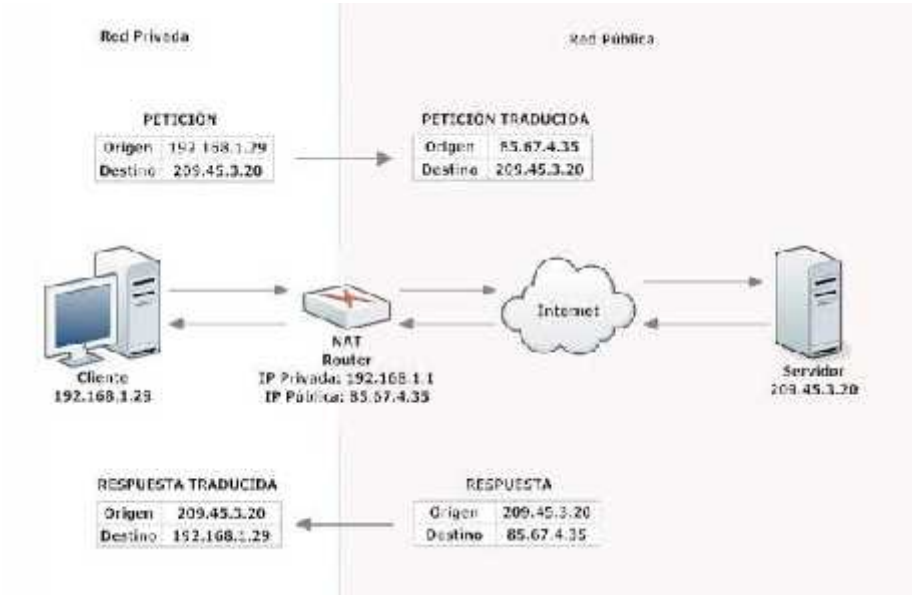

FIGURA 3. 5 Esquema de funcionamiento de NAT

Adicionalmente, eliminaremos por completo la tarjeta de red del servidor que se la utiliza actualmente para el direccionamiento público y realizar las restricciones que se consideren necesarias para aislar el server.

3.2.3 Creación de Objetos y Políticas de Firewall

Procedemos en primera instancia a crear los objetos, para esto necesitamos básicamente realizar tres procedimientos:

a. Crear un SNAT para el envío de correos mediante nuestra IP Pública.

FIGURA 3. 6 Creación de SNAT

b. Creamos un DNAT para que todo el tráfico que llegue a la interfaz pública 186.3.78.100 se traduzca internamente en nuestra interfaz LAN 192.168.8.205.

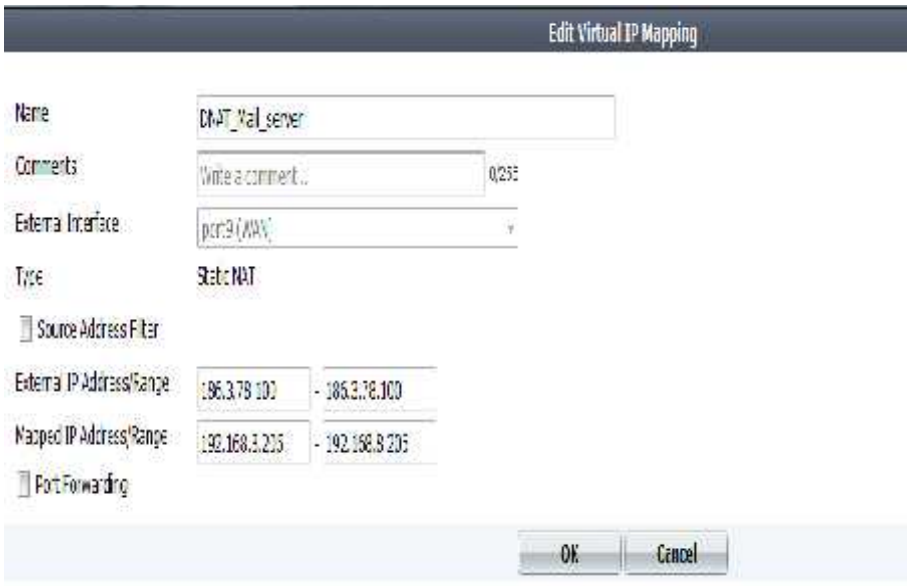

FIGURA 3. 7 Creación de DNAT

c. Crear las políticas de acceso en el Firewall desde la red LAN hacia la red WAN.

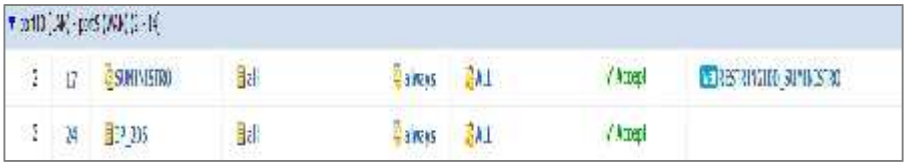

FIGURA 3. 8 Creación de políticas de acceso LAN-WAN

FIGURA 3. 9 Edición de políticas de acceso LAN-WAN

Se establecen políticas desde la red WAN hacia la red LAN. Solamente publicamos los puertos necesarios para el envío y recepción de correo electrónico.

FIGURA 3. 10 Edición de políticas de acceso WAN-LAN

FIGURA 3. 11 Edición de políticas de acceso WAN-LAN

3.3 Reestructuración lógica del Servidor de Facturación Electrónica

De la misma manera tal como publicamos los puertos necesarios del Servidor de Correo Electrónico, lo vamos a realizar con el Servidor de Facturación electrónica. Eliminamos la interfaz de red Pública y configuraremos un DNAT en nuestro Firewall.

Creamos un DNAT para que todo el tráfico que llegue a la interfaz pública 186.3.78.102 se traduzca internamente en nuestra interfaz LAN 192.168.8.213, solo publicamos el puerto 80.

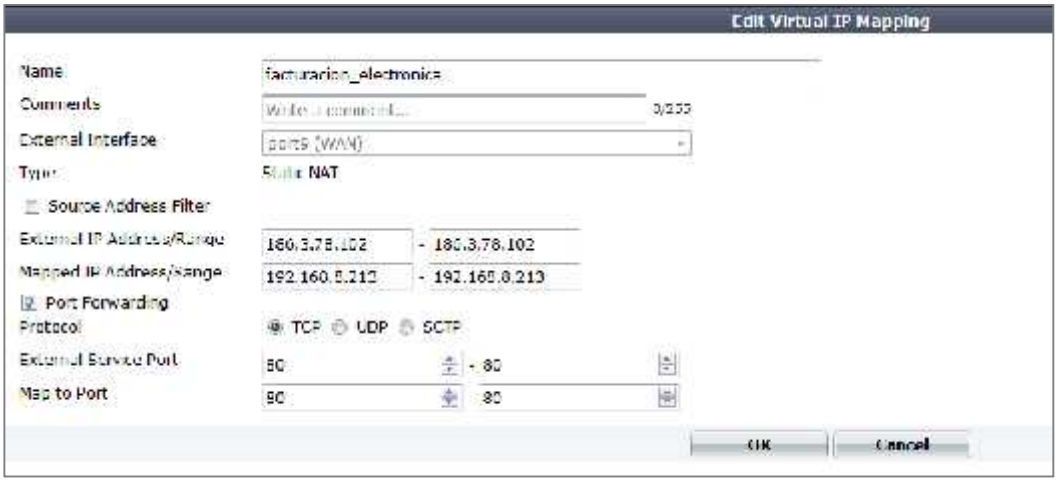

FIGURA 3. 12 Edición de políticas DNAT LAN-WAN

Por último creamos las políticas de acceso en el Firewall desde la red WAN hacia la red LAN.

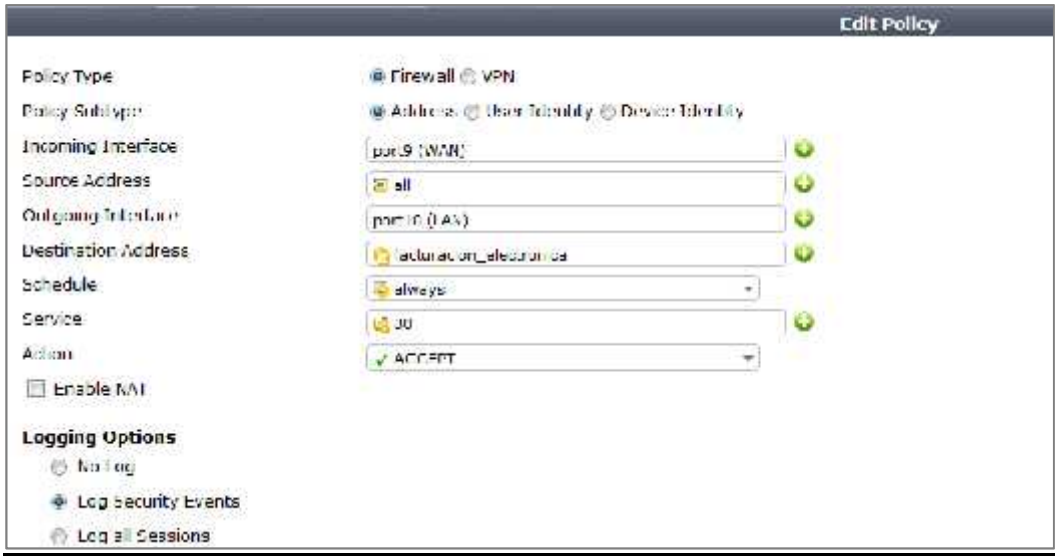

FIGURA 3. 13 Edición de políticas DNAT WAN-LAN

3.4 Implementación de servicios provistos por el proveedor de Internet

Proteger la red interna de la organización, separando los servicios privados como son servidor Base de Datos y servidor de aplicaciones de la red pública (Internet)

3.4.1 Implementación de FortiGate 200B en administración conjunta con el proveedor.

Las plataformas de seguridad FortiGate ofrecen un rendimiento sin igual, protección en tiempo real, y una simplificación de la red. El hardware y software de FortiGate ofrece la flexibilidad de implementación, alto rendimiento y protección integrada necesaria para estar al tanto del panorama de amenazas que ofrece una red dinámica, incluyendo:

- Firewall, VPN
- Intrusion Prevention System (IPS)

- Antivirus/Antispyware/Antimalware
- Application Control
- Vulnerability Management
- Web Filtering
- Antispam

3.5 Implementación de medios de comunicación seguros para conexiones remotas.

3.5.1 Implementación de App Control

Todas las PC que tengan acceso a Internet sin las debidas precauciones constituyen una amenaza constante a nuestra organización, es así que para evitar la fuga de información a través de los terminales de los usuarios se procederá al bloqueo de aplicaciones de acceso remoto a través de Application Control en nuestro firewall, básicamente se procederá con el bloqueo de las siguientes categorías a nivel de aplicaciones:

a. Social Media
b. Herramientas de acceso remoto
c. Audio/Vídeo

Para ello en la sección de Application Control – Application Sensors, procedemos con la creación del app control **SocialNetwork_Teamviewer**. Con esto se realizará bloqueo a las redes sociales y acceso remoto.

FIGURA 3. 14 Creación de App Control

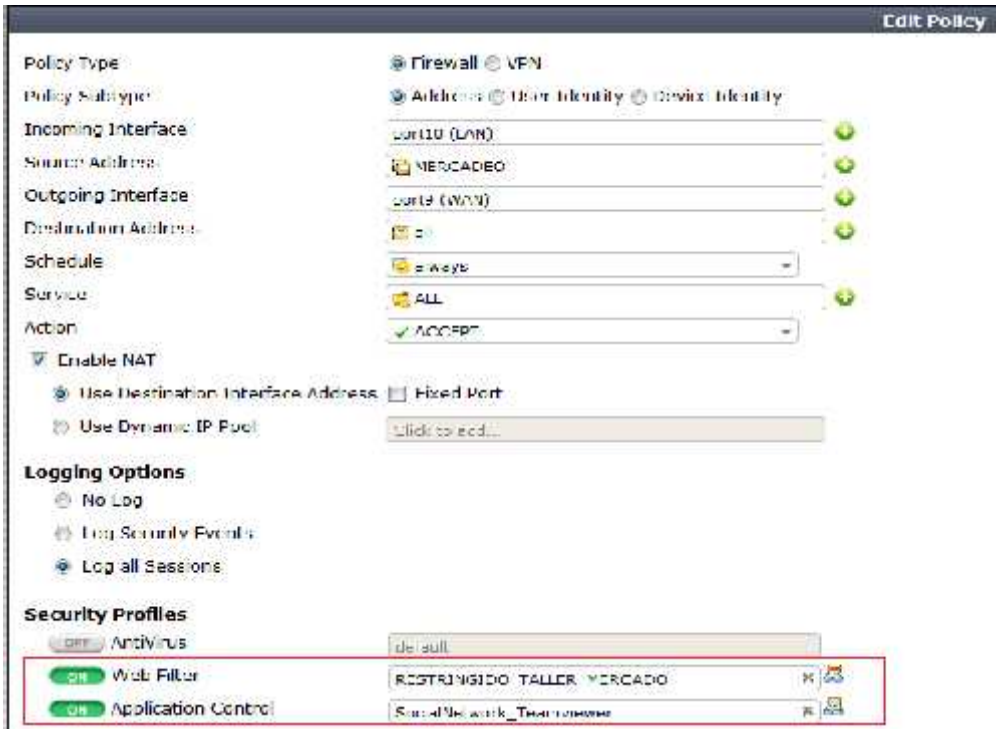

FIGURA 3. 15 Asignación del App Control a los grupos de Usuario

Así mismo se definen los permisos y configuración adecuada del correo electrónico.

3.5.2 Implementación Túnel VPN (Virtual Private Network)

VPN es una extensión de una red local que permite conectar dos o más puntos de manera segura a través de Internet.

Normalmente, VPN usa una tecnología denominada **tunneling** a la hora de establecer la comunicación entre dos puntos. El tunneling simplemente hace uso de un protocolo especial (normalmente **SSH**) para crear un “túnel” por el que circulan todos los datos desde un extremo a otro. Este “túnel” en realidad es la misma información que se manda pero encriptada por la acción del protocolo seguro de comunicación, lo cual hace que nuestros datos no puedan ser vistos por agentes externos.

Otro de los usos más extendidos de las VPN es para facilitar el acceso remoto a una red local. En este caso se lo implementará para dar acceso a los siguientes usuarios, quienes serán denominados Clientes VPN:

- Proveedor de facturación electrónica para realizar actualizaciones.
- Administrador de red en case de que se presente alguna caída del servicio fuera del horario normal de trabajo.

El cliente VPN debe tener instalado un programa cliente de VPN quien tras introducir siempre un usuario y un password, se conecta con un servidor VPN situado en las oficinas de la empresa y así tener acceso a toda la red de la misma.

A nivel de cliente VPN el usuario se conectará desde Internet y se establecerá el uso del software FortiClient como medio de acceso hacia el servidor de Bases de Datos.

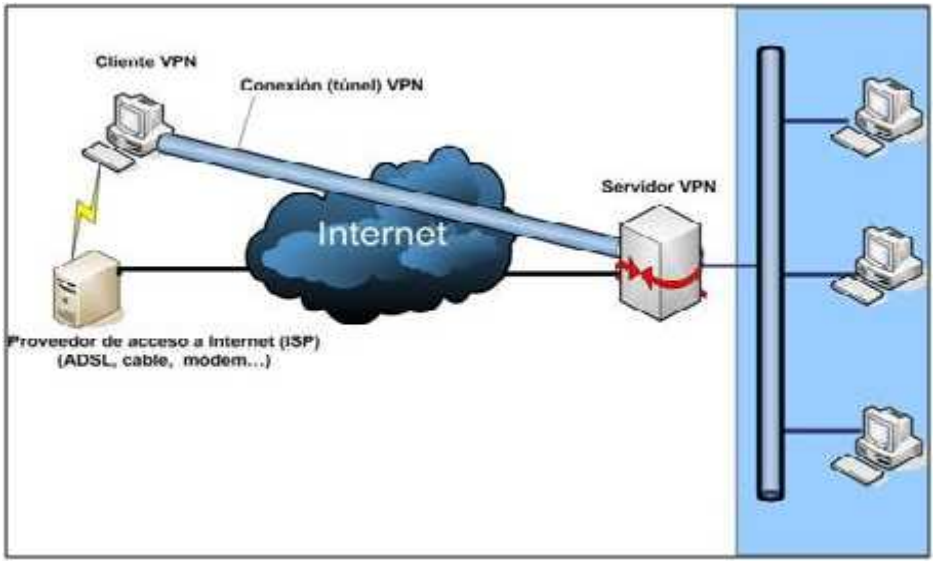

FIGURA 3. 16 Esquema de Red VPN

3.5.3 Configuración de la VPN en el firewall

Para la configuración del túnel VPN procedemos a crear el pool y definimos el puerto 10443 para conexiones remotas.

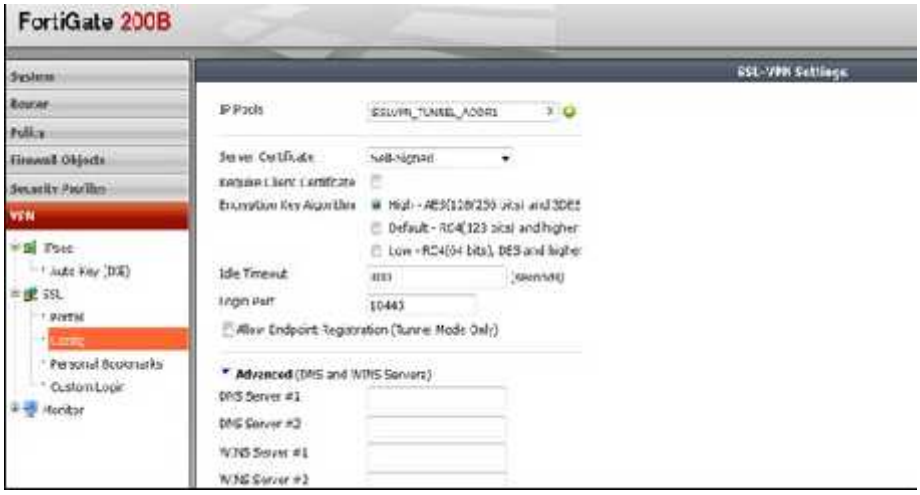

FIGURA 3. 17 Creación de VPN

Habilitamos el túnel VPN y especificamos los servicios que están permitidos para las sesiones remotas, tales como: SSH, HTTP, HTTPS, FTP, TELNET, etc.

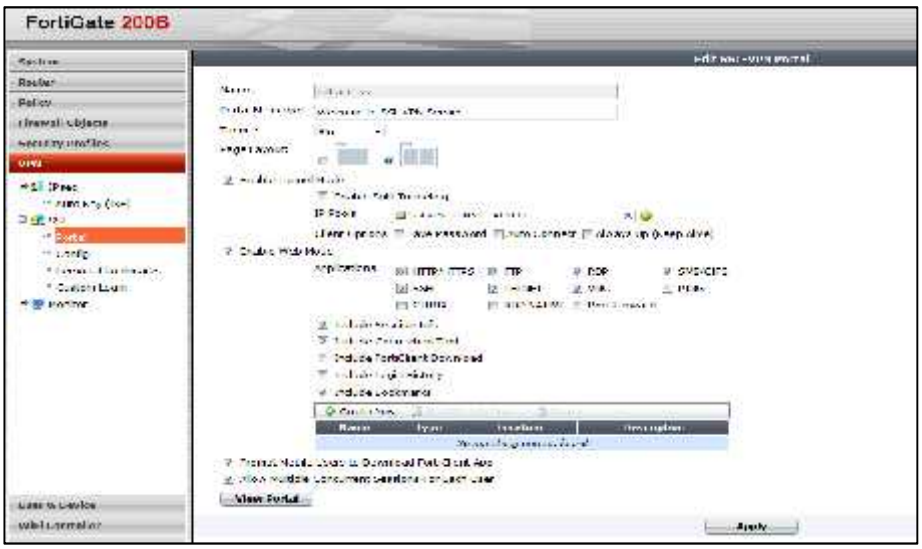

FIGURA 3.18 Restricciones y permisos de Servicios de VPN

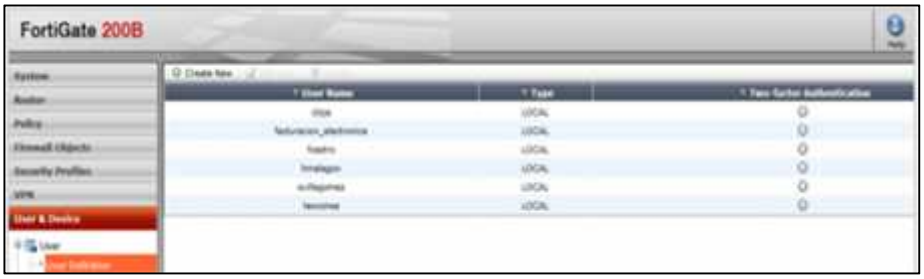

FIGURA 3. 19 Creación de usuarios locales para la conexión VPN

FIGURA 3. 20 Creación de la política WAN – LAN

Para la configuración en el cliente VPN utilizaremos el software FortiClient como medio de acceso hacia el servidor de Base de Datos. A continuación se describe el instructivo necesario para realizar la conexión VPN:

- Procedemos con la instalación del aplicativo SSL VPN Client de Fortinet, dando doble clic en el ejecutable FortiClientInstaller dentro de los instaladores proporcionados.

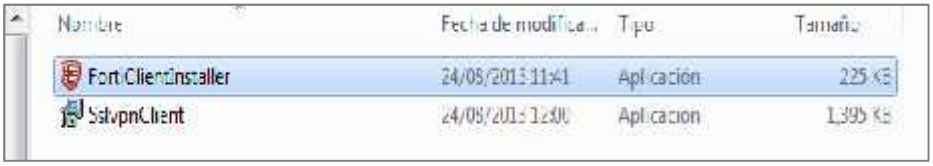

Figura 3.21 Instalación de FortiClient

- El instalador descarga la última versión del aplicativo (5.2.3) por lo que necesita tener una conexión activa a Internet.
- Una vez descargado el aplicativo, procedemos con la configuración del túnel VPN.

Figura 3.22 Configuración de VPN en el cliente

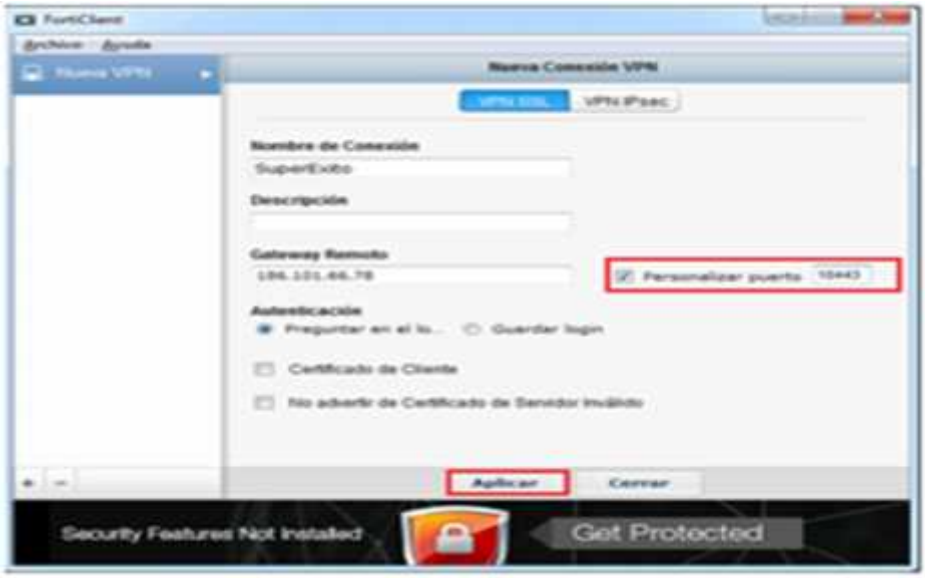

Figura 3.23 Opciones de configuración de VPN

Dentro de los parámetros de configuración se establece el nombre de conexión, el Gateway remoto que es el direccionamiento IP Público de nuestro Fortinet 186.101.66.78. El puerto es otro parámetro importante que viene desmarcado y por defecto es 443, el cual lo tenemos que modificar marcando la casilla y estableciendo el puerto 10443.

Una vez realizadas las configuraciones damos clic en aplicar y esperamos unos segundos hasta que guarde los cambios, luego damos clic en cerrar.

Con esta ya hemos realizado las configuraciones necesarias y solo restaría acceder con el usuario asignado.

Una vez conectado a la VPN, para acceder a cualquier computador de la empresa bastaría con hacer escritorio remoto a la IP interna de los servidores de la LAN.

Sin embargo, los accesos están limitados por usuarios por motivos de seguridad.

Figura 3.24 Acceso desde el cliente VPN

CAPÍTULO 4

ANÁLISIS DE RESULTADOS

Determinar los recursos e inversión monetaria necesaria para la implementación del proyecto. Conocer los mecanismos de mejoras con los cambios implementados.

4.1 Requerimiento de recursos

Un administrador de infraestructura calificado con los siguientes conocimientos:

- Seguridad Informática
- Redes
- CCNA
- Administración de servidores

4.2 Análisis financiero

Inversión en Servicios del proveedor de enlace de datos e Internet

Tabla 1 Servicios contratados

Servicio	Periodicidad	Modalidad	Valor
Fortimail	Mensual	Servicio	$150.00
Fortigate	Mensual	Alquiler	$200.00
Total	**Mensual**		**$350.00**

4.3 Cronograma de trabajo

Para realizar la implementación se estima un mes debido a que no se cuenta con la documentación de la red ni información alguna de las características de los servidores y servicios.

Tabla 2 Cronograma de Implementación

Tarea	Días estimados
Levantamiento de información	1 semana
Análisis de la red LAN	1 semana
Documentación de la red actual, servidores, equipos de comunicación y servicios recibidos	1 semana 1 semana
Diseño de nuevo modelo de red	
Solicitud de nuevos servicios de seguridad	1 día1

Cambio al nuevo modelo de red	1 día
Configuración de la red y Fortigate	
Creación de grupos de usuarios	
Creación de Web Filters	
Configuración de VPN	

4.4 Informes de resultados positivos de la seguridad implementada mediante gráficos.

Luego de la aplicación de los web filters a cada uno de los Departamentos de la empresa hemos optimizado este recurso y ahora se observan los siguientes consumos como resultado positivo que del total disponible (8MB) solamente estamos consumiendo 3.55 MB, se han realizado pruebas de rendimiento con el Internet y ha mejorado considerablemente.

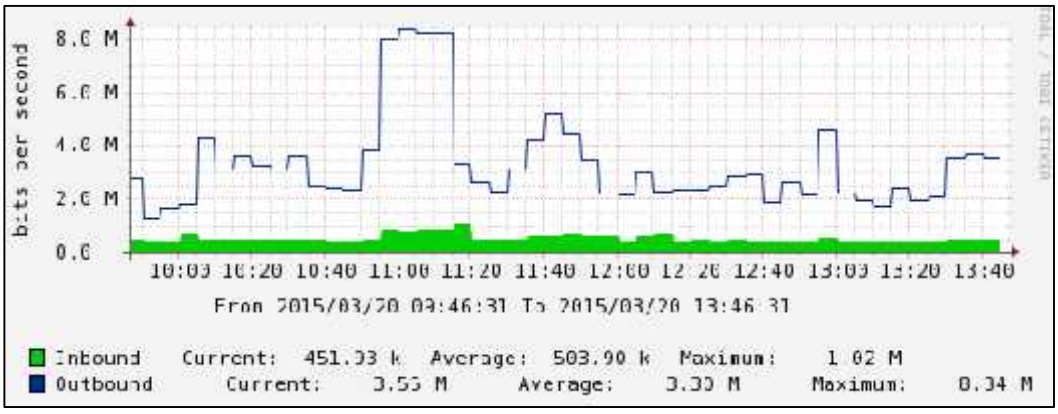

Figura 4. 1 Uso del ancho de banda de Internet después de la implementación.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. La seguridad informática tiene un punto de importancia vital para las empresas, sin importar el tamaño.

2. El buen uso de los mecanismos de seguridad proveerá a la empresa una adecuada protección frente a las amenazas que a diario se presentan a través de Internet.

RECOMENDACIONES

1. Es importante contar con personal capacitado en la seguridad de la información para evitar el acceso de usuarios no autorizados a la información y bases de datos de la empresa.

2. Elaborar informes periódicos de auditoría de seguridad de la información.

3. Realización de un Ethical Hacking [1] y pruebas de intrusión una vez realizada la implementación de los mecanismos de seguridad. El test de penetración o pruebas de intrusión y el Ethical hacking ayudan a detectar problemas
4. desconocidos que no pueden ser encontrados durante una revisión de configuración.

GLOSARIO

FortiGate: Es un Firewall basado en hardware desarrollado por Fortinet. El sistema de FortiGate es el único sistema que puede detectar y eliminar virus, gusanos y otras amenazas basadas en contenido, sin afectar al rendimiento de la red, incluso para aplicaciones en tiempo real como la navegación Web. Las soluciones de FortiGate también incluyen: Firewall, filtrado de contenido, VPN, antivirus, antispam, detección y prevención de intrusos y gestor de tráfico, balanceo de carga, alertas por e-mail.

FortiMail: Es una plataforma de seguridad de correo electrónico completa de la empresa Fortinet que sirve para proteger contra los ataques entrantes, así como las amenazas de salida y la pérdida de datos mediante antispam, antiphishing, antimalware, la prevención de fuga de datos, identity based encryption (IBE), archivado de mensajes, motores de filtrado entrantes de FortiMail, bloqueador de spam y malware.

BIBLIOGRAFÍA

[1] Karina Astudillo, Hacking Ético 101. Cómo hackear profesionalmente en 21 días o menos, 2013.

[2] Fortigate http://www.exclusive-networks.es/portfolio-item/fortinet/ fecha de consulta enero de 2016

[3] Seguridad de servidores http://www.segu-info.com.ar/proteccion/proteccion.htm fecha de consulta enero de 2016

[4] Concepto VPN http://www.anexom.es/tecnologia/mi-conexion/vpn-%C2%BFque-es-y-para-que-sirve/ fecha de consulta enero de 2016

[5] Concepto de Firewall https://www.masadelante.com/faqs/cortafuegos fecha de consulta enero de 2016

[6] NAT redes http://www.xatakaon.com/tecnologia-de-redes/nat-network-address-translation-que-es-y-como-funciona fecha de consulta enero de 2016