

Universidad Autónoma Metropolitana – Azcapotzalco

División de Ciencias Básicas e Ingeniería

Licenciatura en Ingeniería en Computación

**Sistema de seguridad perimetral de una red con un firewall
FortiGate 60D**

Modalidad: Estancia Profesional

Trimestre 2017-Primavera

Nombre del alumno: Aarón López Vázquez

Matrícula: 208202129

Correo: aaronelv@icloud.com

Asesor:

M. en C. José Ignacio Vega Luna

Categoría: Titular C

Departamento de Electrónica

Correo: vlji@correo.azc.uam.mx

Jefe directo:

Ing. Mario Ernesto Gómez Romero

Coordinador del Área de Seguridad en Datos (T&B Talent S.A. de C.V.)

Correo: mario.gomez@tbtalent.com.mx

21 de julio de 2017

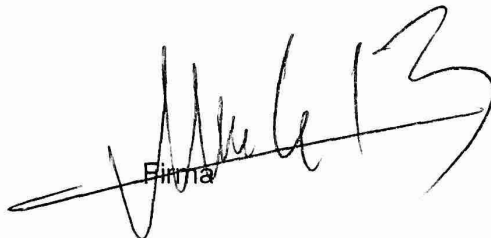
Declaratoria

Yo, José Ignacio Vega Luna, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Firma

Yo, Mario Ernesto Gómez Romero, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Firma

Yo, Aarón López Vázquez, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.



Firma

Resumen

El proyecto descrito en el presente documento, refiere a las actividades llevadas a cabo durante la estancia laboral en T&B Talent S.A. de C.V. , la cual es una empresa que ofrece asesoría y gestión de tecnologías de información como diseñar e implementar diversos esquemas de seguridad, que es el caso de su cliente Laboratorios OLAB, en donde, como se describe más adelante, se hace una implementación de un sistema de seguridad firewall FortiGate 60D, así como también se muestra su correcta administración, configurando políticas y creando perfiles de seguridad, así como también la creación de una VPN para su funcionamiento con Elastix para servicios de telefonía.

Para llegar a la configuración correcta del FortiGate 60D fue necesaria una inspección en Laboratorios OLAB para tener un diseño de la red y así hacer una correcta instalación, tal como se muestra más adelante en este reporte.

Tabla de contenido

1. Introducción	1
2. Antecedentes	1
3. Justificación	2
4. Objetivos	2
5. Marco teórico	3
5.1. Fortinet	3
5.2. FortiGate	3
5.3. FortiOS	4
5.4. Firewall	4
5.5. VPN	4
5.6. Elastix	5
6. Desarrollo del proyecto	8
6.1. Configuración y recursos del FortiGate60D	8
6.2. Configuración de interfaces	9
6.3. Configuración de rutas	10
6.4. Configuración de políticas	10
6.5. Configuración de VPN's	14
7. Resultados	17
8. Conclusiones	17
9. Bibliografía	18
10. Entregables	18

Índice de figuras

Figura1. Diagrama de red de laboratorios OLAB	8
Figura2. Validación de versión de firmware del FortiGate 60D	8
Figura3. Validación de recursos del FortiGate 60D	9
Figura4. Configuración de interfaces	9
Figura5. Configuración de rutas	10
Figura6. Política dmz (PACS) – wan1 (Maxcom)	10
Figura7. Política Internal1 (LAN_Del Valle) – Internal2 (LAN_WiFi)	11

Figura8. Política Internal1 (LAN_Del Valle) – VPN_Elastix	11
Figura9. Política Internal1 (LAN_Del Valle) – Wan 1 (Maxcom)	12
Figura10. Política Internal1 (LAN_WiFi) – Internal1 (LAN_Del Valle)	12
Figura11. Política Internal1 (LAN_WiFi) – Wan 1 (Maxcom)	13
Figura12. Política VPN_Elastix - Internal 1 (LAN Del Valle)	14
Figura13. Política Wan1 (Maxcom) – Internal1 (LAN_Del Valle)	14
Figura14. Configuración fase 1 VPN_Elastix	15
Figura15. Configuración fase 2 VPN_Elastix	15
Figura16. Configuración fase 1 de VPN por SSL	16
Figura17. Configuración fase 2 de VPN por SSL	16

Índice de tablas

Tabla1. Política LAN_PACS	10
Tabla2. Política LAN_Del Valle – LAN_WiFi	11
Tabla3. Política LAN_Del Valle – Red_Elastix	11
Tabla4. Política LAN_Del Valle – Wan1 con Web Filter y Application Control	12
Tabla5. Política LAN_WiFi – LAN_Del Valle	12
Tabla6. Política LAN_WiFi – Wan 1 con Web Filter y Application Control	13
Tabla7. Política VPN_Elastix – LAN_Del Valle	13
Tabla8. Política Wan1 – LAN_Del Valle	14

1. Introducción

Actualmente, las redes se han vuelto una herramienta indispensable para la vida diaria y laboral. Desde el uso de impresoras, compartimiento de archivos y dispositivos hasta el acceso a internet para diversas tareas. Para esto, la seguridad ha sido una prioridad para las empresas, ya que requieren de la protección de sus datos, así como también el control de acceso a internet.

VPN o red privada virtual es una extensión segura de la red local sobre una infraestructura pública o no controlada, manteniendo los recursos y facultades de una red local tradicional. A su vez, una VPN tiene como objetivo la interconexión entre sucursales de alguna empresa o entre oficinas independientes [1].

Existen 2 tipos de VPN, VPN de acceso sitio-a-sitio, la cual se crea cuando se conoce la configuración de VPN en ambos lados de la conexión, y la VPN de acceso remoto, para este tipo de configuración se conocen dos métodos principales: Capa de sockets seguros (SSL) y seguridad IP (Ipsec) . El método utilizado dependerá de los requisitos de acceso de los usuarios y de los procesos llevados a cabo en la organización en la que se encuentre [2].

Elastix es una aplicación la cual sirve, para crear sistemas VoIP, que configurado con una VPN, permite dar acceso a los equipos que se encuentran dentro de la red interna.

Un firewall es un sistema de seguridad o de protección contra intrusiones de otras redes, que permite el monitoreo del tráfico de la red (datos entrantes y salientes) y la administración de la misma [3].

Un firewall puede ser un software instalado en una computadora que esté dentro de la red local o bien, puede ser un hardware conectado de la red local hacia la red externa. Este segundo, es el caso del sistema indicado en el presente reporte, el firewall FortiGate 60D.

El proyecto descrito en este documento muestra una metodología para la implementación de un sistema de seguridad firewall con el FortiGate 60D mediante el uso de políticas y perfiles de seguridad, además de la creación de una VPN con servicio de telefonía mediante Elastix.

2. Antecedentes

En Laboratorios OLAB, se requirió de un sistema de seguridad firewall dentro de su red en el cual se pudiesen establecer políticas de seguridad, en este caso se usó un firewall de la marca Fortinet modelo FortiGate 60D, el cual funciona con un sistema operativo FortiOS 5.0 que permite configurar y establecer filtrado web, antivirus, antispymware, antimailware, antispam, IPsec/SSL VPN, prevención de intrusiones, entre otras funciones, con la finalidad de responder con las necesidades de Laboratorios OLAB.

Junto con la implementación de este firewall, se requirió de la creación de una VPN que bien puede funcionar con servicios de telefonía, esto con ayuda de Elastix.

3. Justificación

Hoy en día, la seguridad informática es un tema de mucha importancia, ya que los ataques y amenazas han ido en incremento, mismos que comprometen información relevante de la empresa.

Está comprobado, que la mayoría de los ataques, amenazas o accesos indebidos son ocasionados en un gran porcentaje desde la red interna de las empresas. Por este motivo, T&B Talent S.A. de C.V. ha ofrecido a laboratorios OLAB un sistema de filtrado de contenido y bloqueo de sitios, además de la implementación de VPN's con servicios de telefonía por medio del ya citado FortiGate 60D.

A continuación, se dará una descripción breve de la importancia del problema a resolver.

Es indispensable tomar en cuenta las necesidades y las pérdidas económicas que pudiera tener la empresa sin un sistema de seguridad para la red, en este caso, laboratorios OLAB, y atender dichas necesidades con la creación de políticas, grupos, perfiles de seguridad y demás herramientas que ofrece el FortiGate 60D, para así garantizar una navegación segura, un control del tráfico entrante y saliente en la red, además de establecer seguridad por medio de VPN's en la comunicación que tendrá OLAB con la red Elastix para el servicio de telefonía.

FortiGate 60D ofrece la posibilidad de un monitoreo constante y en tiempo real para detectar y eliminar intrusiones, así como también admite configurar el mismo para bloqueo de puertos y limitar el acceso a la web.

4. Objetivos

Objetivo general:

Diseñar e implantar un sistema de seguridad de una red de datos usando un firewall FortiGate 60D.

Objetivos específicos:

- Diseñar e implantar un mecanismo de filtrado de contenido y bloqueo de sitios web para contar con seguridad perimetral con un firewall FortiGate 60D en las sucursales de Laboratorios OLAB.
- Diseñar e implantar una VPN con el servicio de telefonía Elastix en las sucursales de Laboratorios OLAB para establecer seguridad durante la comunicación.

5. Marco Teórico

5.1. Fortinet

Fortinet es una empresa de Estados Unidos con sede en Sunnyvale, California dedicada al desarrollo y comercialización de plataformas de seguridad de más alto rendimiento para asegurar y simplificar una infraestructura de IT. Fortinet tiene una amplia base de clientes, entre los cuales se encuentran operadores, centros de procesamiento de datos o empresas.

Fortinet también dirige el equipo de investigación de seguridad interna “FortiGuard Labs”, el cual cuenta con cuatro centros de investigación y desarrollo en Asia, así como otros en Estados Unidos, Canadá y Francia. Además, organiza un programa de certificación y formación con ocho niveles de certificación NSE

Los requerimientos actuales de las áreas de Tecnologías de Información se concentran en integrar sus soluciones de seguridad, buscan acelerar tareas de procesamiento para mantener seguras sus redes corporativas y, por otra parte, necesitan el respaldo de un esquema riguroso de investigación y soporte que les permita cumplir sus objetivos ante un ambiente global de amenazas. [5]

Bajo este panorama, Fortinet se consolida como la principal solución innovadora de alto desempeño para la seguridad de redes orientada a resolver problemas fundamentales que surgen en los entornos de redes de uso intensivo de ancho de banda donde las amenazas informáticas son cada vez más sofisticadas.

Fortinet es la compañía pionera en integrar varias funciones juntas en una sola plataforma -Unified Threat Management (UTM)- incluyendo firewall, VPN, control de aplicaciones, prevención de intrusos y filtrado web, ofreciendo protección total de contenidos.

5.2. FortiGate 60D

FortiGate 60D de Fortinet es un equipo compacto que posee todas las grandes características de una UTM. Ideal para pequeños negocios, conexión remota, equipo local de cliente (CPE) y redes de retail. Además, ofrece altos estándares de seguridad de redes y conectividad.

FortiGate, además cuenta con un Throughput (rendimiento) de 1.5 Gbps el cual garantiza que su seguridad de conexión no sufra “cuellos de botella”, un Switch integrado y opciones para PoE que simplifican su infraestructura de red y puertos WAN de hasta 2x, LAN 7x y una interfaz DMZ (2 puertos Power over Ethernet en los modelos PoE).

La serie FortiGate 60D ofrece protección integral. Esta fue desarrollada por SPU SoC2 y combina una CPU basada en RISC con el contenido de la Unidad de Procesamiento de Seguridad (SPU) de Fortinet y procesadores de red para un rendimiento sin igual.

Proporciona aceleración de firewall en todos los tamaños de paquetes, aceleración de procesamiento de contenido UTM, acceso remoto seguro y VPN de alta velocidad para un rendimiento y protección superior.

5.3. FortiOS 5

FortiOS 5.0, el sistema operativo de seguridad más poderoso del mundo es la base para todas las plataformas de seguridad integrada Fortinet FortiGate. Ofrece mayor seguridad, inteligencia y control para ayudar a las empresas a estar más protegidos contra las amenazas avanzadas de hoy y permitir ambientes [BYOD] más seguros.

5.4. Firewall

Un firewall o también llamado corta-fuego, es un sistema que permite proteger a una o varias computadoras dentro de una red, de intrusiones o amenazas.

Existen dos tipos de firewall, el firewall por software que pueden ser gratuitos o comerciales, y el firewall por hardware.

El firewall por software gratuito puede ser usado con toda libertad por el usuario y tiene por objetivo rastrear y denegar el acceso a ciertos datos. Actualmente, la mayoría de las computadoras tienen instalado un firewall de este tipo y no requieren de algún hardware adicional.

El firewall por software comercial, al igual que el gratuito, tiene por objetivo rastrear y denegar el acceso a ciertos datos, pero con mayores niveles de control y protección. Para mayor eficiencia al proteger una computadora, son vendidos con algún sistema de antivirus.

El firewall por hardware es un sistema de seguridad instalado en una red, normalmente se colocan entre el router y la conexión a Internet.

Al ser dispositivos dedicados de seguridad, se encuentran optimizados para realizar la función de firewall, y además no consumen los recursos de los sistemas personales.

Su mayor inconveniente es el mantenimiento, ya que son difíciles de actualizar y de configurar correctamente.

5.5. VPN

VPN o red privada virtual, permite crear una extensión privada sobre una red pública, esto mediante un proceso de encapsulación y en algún caso de encriptación, desde los paquetes de datos a diferentes puntos remotos, mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por un túnel definido en la red pública.

En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignando a su ordenador remoto las direcciones y privilegios de esta, aunque la conexión la haya realizado mediante un acceso público a Internet.

5.6. Elastix

Elastix es un software de servidor de comunicaciones unificadas disponible para los PBX basados en Asterisk en una única interfaz fácil de usar.

Elastix tiene múltiples características y funcionalidades:

PBX

- Grabación de llamada
- Centro de conferencias con salas virtuales
- Mensaje de voz
- Soporte SIP y IAX, entre otros
- Funcionalidad correo de voz a correo electrónico
- Códecs compatibles: ADPCM, G.711 (A-Law y μ -Law), G.722, G.723.1 (pasar), G.726, G.728, G.729, GSM, iLBC (opcional) entre otros.
- IVR flexible y configurable
- Soporte para interfaces analógicas como FXS / FXO (PSTN / POTS)
- Soporte de síntesis de voz
- Soporte para interfaces digitales (E1 / T1 / J1) a través de protocolos PRI / BRI / R2
- Herramienta de configuración de lote de terminal IP
- Identificador de llamadas
- Cancelador de eco integrado por software
- Soporte para múltiples troncales
- Configurador de punto final
- Rutas entrantes y salientes con compatibilidad para coincidencia de marcación
- Soporte para video-teléfonos
- Soporte para follow-me
- Interfaz de detección de hardware
- Soporte para grupos de timbres
- Servidor DHCP para IP dinámico
- Soporte para paginación e intercomunicación
- Panel de operador basado en web
- Soporte para las condiciones de tiempo
- Llamar al estacionamiento
- Soporte para juegos de PIN
- Registro de detalle de llamada (CDR)
- Acceso directo al sistema interno (DISA)
- Informe de facturación y consumo
- Soporte de devolución de llamada
- Informes de uso del canal
- Soporte para interfaces bluetooth a través de teléfonos celulares (chan_mobile)
- Soporte para colas de llamadas
- Elastix Operator Panel (EOP)
- Plan de marcación distribuida con dundi
- Configuración de Voip Provider
- Asterisco Tiempo real
- Plan de marcación distribuida con dundi
- Configuración de Voip Provider
- Asterisco Tiempo real

FAX

- Servidor de fax basado en HylaFax
- Personalización del fax al correo electrónico
- Visor de fax con archivos PDF descargados
- Control de acceso para clientes de fax
- Aplicación de fax a correo electrónico
- Se puede integrar con Winprint Hylafax
- Módulo SendFax
- Envío de fax a través de la Interfaz Web
- Módulo SendFax - Envío de fax a través de la Interfaz Web

General

- Gestión centralizada de actualizaciones
- Monitor de recursos del sistema
- Soporte de copia de seguridad / restauración a través de la Web
- Configurador de red
- Desconexión del servidor desde la Web
- Fecha, hora y zona horaria configurables del servidor
- Control de acceso a la interfaz basada en ACL
- Copias de seguridad en un servidor FTP
- Módulos Elastix en RPMs
- Módulo de lista de clientes DHCP
- Restaurar copia de seguridad automática
- Validación de restauración de copia de seguridad
- DHCP por MAC
- Elastixwave
- Nuevo cuadro de mandos
- Elastix News Applet
- Mejora del detector de hardware
- Información de hardware de telefonía
- Applet de actividad de comunicación
- Applet de estado del proceso

Colaboración

- Calendario integrado con PBX con soporte para notificaciones de voz
- Libreta de teléfonos
- Dos productos CRM integrados a la interfaz (vTigerCRM y SugarCRM)
- Conferencia Web
- Nuevas funciones en el módulo de calendario

Extras

- Soporte de facturación con A2Billing

- CRM integrado: vTigerCRM y SugarCRM
- Módulo Addons

Mensajería instantánea

- Servidor de mensajería instantánea Openfire
- Informe de sesiones de usuario
- Las llamadas iniciadas por el cliente IM
- Soporte Jabber
- Gestión basada en Web para el servidor de mensajería instantánea
- Soporte de complementos
- Soporte de grupos de MI
- Soporte LDAP
- Soporte para otras pasarelas de mensajería instantánea como MSN, Yahoo Messenger, GTalk e ICQ
- Soporte de servidor a servidor

Email

- Servidor de correo con soporte multi-dominio
- Apoyo a cuotas
- Gestión basada en web
- Soporte Antispam
- Soporte para el relé de correo
- Basado en Postfix para un volumen de correo electrónico alto
- Cliente de correo electrónico basado en Web
- Gestión de listas de correo electrónico
- Módulo SMTP Remoto

Módulo de centro de llamadas

Elastix fue la primera distribución que incluyó un módulo de centro de llamadas con un marcador predictivo, liberado completamente como software libre. Este módulo se puede instalar desde la misma interfaz web Elastix a través de un cargador de módulos. El módulo del centro de llamadas puede manejar las campañas entrantes y salientes.

Elastix también es compatible con otras marcas de teléfonos gracias a los protocolos SIP11 y IAX12 que implementa Asterisk. El protocolo SIP es actualmente un estándar utilizado en su mayoría por los fabricantes de teléfonos IP y su funcionamiento es nativo para voz con Elastix, independientemente de alguna funcionalidad adicional que estos tengan.

6. Desarrollo del proyecto

En el siguiente diagrama de red (Figura1) se puede observar la forma en que está constituida la red de la sucursal Del Valle y la conexión que existe con la Red Elastix (comunicación por VPN).

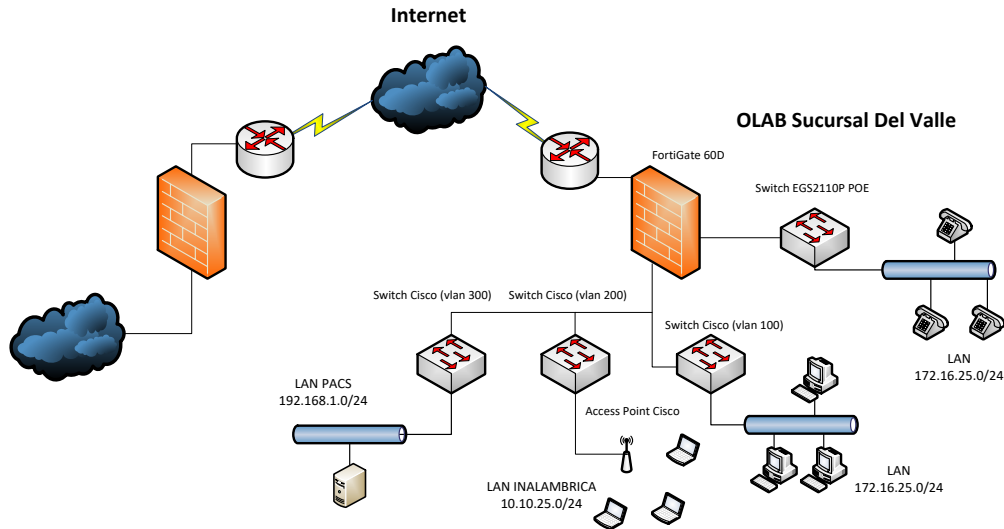


Figura1. Diagrama de red de laboratorios OLAB

A continuación, se hace una descripción de cada una de las fases realizadas para lograr la funcionalidad del equipo FortiGate 60D.

6.1. Configuración y recursos del FortiGate 60D

Desde la interfaz GUI del equipo FortiGate 60D, se valida la versión del firmware y los recursos utilizados.

System Information	
Host Name	FG_Del_Valle [Change]
Serial Number	FGT60D4613052040
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Tue Jan 6 14:59:51 2015 (FortiGuard) [Change]
Firmware Version	v5.0,build4317 (GA) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	0 day(s) 8 hour(s) 5 min(s)

Figura2. Validación de versión de firmware del FortiGate 60D

De la misma forma, desde de la interfaz se validan los recursos del FortiGate 60D.

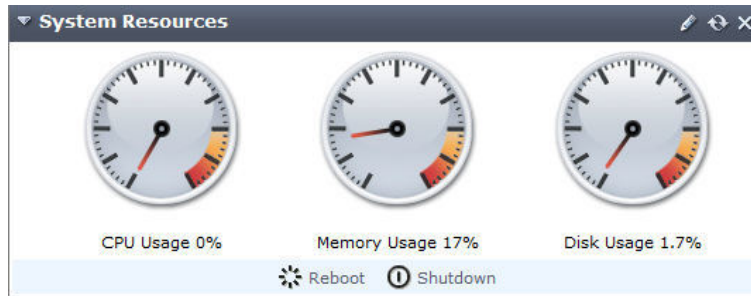


Figura3. Validación de recursos del FortiGate 60D

6.2. Configuración de interfaces

Dentro del menú **System** encontramos la opción **Network >> Interfaces** con la siguiente configuración.

- Wan1 (Maxcom): 201.161.8.178/255.255.255.248 PING, HTTPS, SSH. Interfaz del enlace dedicado, por el cual se configura el túnel de la VPN y brinda el servicio de internet.
- Dmz (PACS): 192.168.1.254/255.255.255.0 PING, HTTPS, SSH. Interfaz dmz, en donde se encuentran conectados los equipos con aplicaciones hacia el PACS, este segmento de red, cuenta con salida a internet.
- Internal1 (LAN_Del Valle): 172.16.25.254/255.255.255.0 PING, HTTPS, SSH. Interfaz LAN, segmento de red para los usuarios y dispositivos con conexión por cable Ethernet con salida a internet.
- Internal2 (LAN_WiFi): 10.10.25.254/255.255.255.0 PING, HTTPS. Interfaz WiFi, segmento de red para los usuarios y dispositivos con conexión inalámbrica con salida a internet.

	Name	Type	IP/Netmask	Access	Administrative Status	Link Status
<input type="checkbox"/>	dmz (PACS)	Physical Interface	192.168.1.254 / 255.255.255.0	HTTPS,PING,SSH	⬆	⬆ 100 Mbps/Full Duplex
<input checked="" type="checkbox"/>	wan1 (Maxcom)	Physical Interface	201.161.8.178 / 255.255.255.248	HTTPS,PING,SSH	⬆	⬆ 1000 Mbps/Full Duplex
<input type="checkbox"/>	VPN_Elastix	Tunnel Interface	0.0.0.0 / 0.0.0.0		⬆	
<input type="checkbox"/>	wan2	Physical Interface	0.0.0.0 / 0.0.0.0		⬆	⬆
<input type="checkbox"/>	mesh.root (SSID: fortinet.mesh.root)	WiFi	0.0.0.0 / 0.0.0.0		⬆	
<input type="checkbox"/>	internal1 (LAN_Dell Valle)	Physical Interface	172.16.25.254 / 255.255.255.0	HTTPS,PING,SSH	⬆	⬆ 100 Mbps/Full Duplex
<input type="checkbox"/>	internal2 (LAN_WiFi)	Physical Interface	10.10.25.254 / 255.255.255.0	HTTPS,PING	⬆	⬆ 100 Mbps/Full Duplex
<input type="checkbox"/>	internal3	Physical Interface	0.0.0.0 / 0.0.0.0		⬆	⬆
<input type="checkbox"/>	internal4	Physical Interface	0.0.0.0 / 0.0.0.0		⬆	⬆
<input type="checkbox"/>	internal5	Physical Interface	0.0.0.0 / 0.0.0.0		⬆	⬆
<input type="checkbox"/>	internal6	Physical Interface	0.0.0.0 / 0.0.0.0		⬆	⬆
<input type="checkbox"/>	internal7	Physical Interface	0.0.0.0 / 0.0.0.0		⬆	⬆

Figura4. Configuración de interfaces

6.3. Configuración de rutas

Dentro del menú **Router** en la opción **Static>>Static Route** observamos.

IP/Mask	Gateway	Device
0.0.0.0 0.0.0.0	201.161.8.177	wan1
192.168.90.0 255.255.255.0		VPN_Elastix
172.16.195.0 255.255.255.0		ssl.root

Figura5. Configuración de rutas

6.4. Configuración de políticas

Dentro del menú **Policy** en la opción **Policy >> Policy** tenemos las siguientes políticas.

I. Dmz (PACS) – Wan1 (Maxcom)

No. de Política	Origen	Destino
2	LAN_PACS	All

Tabla1. Política LAN_PACS

Seq.#	ID	Source	Destination	Schedule	Service	NAT	Action
▼ dmz (PACS) - wan1 (Maxcom) (1 - 1)							
1	2	LAN_PACS	all	always	ALL	✓	✓ Accept
▶ internal1 (LAN_Dell Valle) - internal2 (LAN_WiFi) (2 - 2)							
▶ internal1 (LAN_Dell Valle) - VPN_Elastix (3 - 3)							
▶ internal1 (LAN_Dell Valle) - wan1 (Maxcom) (4 - 4)							
▶ internal2 (LAN_WiFi) - internal1 (LAN_Dell Valle) (5 - 5)							
▶ internal2 (LAN_WiFi) - wan1 (Maxcom) (6 - 7)							
▶ VPN_Elastix - internal1 (LAN_Dell Valle) (8 - 8)							
▶ wan1 (Maxcom) - internal1 (LAN_Dell Valle) (9 - 10)							
▶ Implicit (11 - 11)							

Figura6. Política dmz (PACS) – wan1 (Maxcom)

II. Internal1 (LAN_Del Valle) – Internal2 (LAN_WiFi)

No. de política	Origen	Destino
7	LAN_Del Valle	LAN_WiFi

Tabla2. Política LAN_Del Valle – LAN_WiFi

Seq.#	ID	Source	Destination	Schedule	Service	NAT	Action
▶ dmz (PACS) - wan1 (Maxcom) (1 - 1)							
▼ internal1 (LAN_Dell Valle) - internal2 (LAN_WiFi) (2 - 2)							
2	7	LAN_Del Valle	LAN_WiFi	always	ALL	⊗	✓ Accept
▶ internal1 (LAN_Dell Valle) - VPN_Elastix (3 - 3)							
▶ internal1 (LAN_Dell Valle) - wan1 (Maxcom) (4 - 4)							
▶ internal2 (LAN_WiFi) - internal1 (LAN_Dell Valle) (5 - 5)							
▶ internal2 (LAN_WiFi) - wan1 (Maxcom) (6 - 7)							
▶ VPN_Elastix - internal1 (LAN_Dell Valle) (8 - 8)							
▶ wan1 (Maxcom) - internal1 (LAN_Dell Valle) (9 - 10)							
▶ Implicit (11 - 11)							

Figura7. Política Internal1 (LAN_Del Valle) – Internal2 (LAN_WiFi)

Esta política permite la comunicación entre ambos segmentos de red, se tiene que desde la LAN Del Valle pueda tener acceso a la LAN WiFi, de igual modo se tiene que configurar otra política donde el flujo sea invertido (LAN_WiFi – LAN_Del Valle).

I. Internal1 (LAN_Del Valle) – VPN_Elastix

No. de política	Origen	Destino
6	LAN_Del Valle	Red_Elastix

Tabla3. Política LAN_Del Valle – Red_Elastix

Seq.#	ID	Source	Destination	Schedule	Service	NAT	Action
▶ dmz (PACS) - wan1 (Maxcom) (1 - 1)							
▶ internal1 (LAN_Dell Valle) - internal2 (LAN_WiFi) (2 - 2)							
▼ internal1 (LAN_Dell Valle) - VPN_Elastix (3 - 3)							
3	6	LAN_Del Valle	Red_Elastix	always	ALL	⊗	✓ Accept
▶ internal1 (LAN_Dell Valle) - wan1 (Maxcom) (4 - 4)							
▶ internal2 (LAN_WiFi) - internal1 (LAN_Dell Valle) (5 - 5)							
▶ internal2 (LAN_WiFi) - wan1 (Maxcom) (6 - 7)							
▶ VPN_Elastix - internal1 (LAN_Dell Valle) (8 - 8)							
▶ wan1 (Maxcom) - internal1 (LAN_Dell Valle) (9 - 10)							
▶ Implicit (11 - 11)							

Figura8. Política Internal1 (LAN_Del Valle) – VPN_Elastix

II. Internal1 (LAN_Del Valle) – Wan 1 (Maxcom)

No. de Política	Origen	Destino	Web Filter	Application Control
1	LAN_Del Valle	all	Sucursal_Del Valle	Sucursal_Del Valle

Tabla4. Política LAN_Del Valle – Wan1 con Web Filter y Application Control

Seq.#	ID	Source	Destination	Schedule	Service	NAT	Action	Web Filter	Application Control
▶ dmz (PACS) - wan1 (Maxcom) (1 - 1)									
▶ internal1 (LAN_Dell Valle) - internal2 (LAN_WiFi) (2 - 2)									
▶ internal1 (LAN_Dell Valle) - VPN_Elastix (3 - 3)									
▼ internal1 (LAN_Dell Valle) - wan1 (Maxcom) (4 - 4)									
4	3	LAN_Del Valle	all	always	ALL		Accept	Sucursal_Del Valle	Sucursal_Del Valle
▶ internal2 (LAN_WiFi) - internal1 (LAN_Dell Valle) (5 - 5)									
▶ internal2 (LAN_WiFi) - wan1 (Maxcom) (6 - 7)									
▶ VPN_Elastix - internal1 (LAN_Dell Valle) (8 - 8)									
▶ wan1 (Maxcom) - internal1 (LAN_Dell Valle) (9 - 10)									
▶ Implicit (11 - 11)									

Figura9. Política Internal1 (LAN_Del Valle) – Wan 1 (Maxcom)

Para las políticas con usuarios acceso a servicios de internet se activa la opción de Web Filter y Application Control.

III. Internal2 (LAN_WiFi) – Internal1 (LAN_Del Valle)

No. de política	Origen	Destino
8	LAN_WiFi	LAN_Del Valle

Tabla5. Política LAN_WiFi – LAN_Del Valle

Seq.#	ID	Source	Destination	Schedule	Service	NAT	Action
▶ dmz (PACS) - wan1 (Maxcom) (1 - 1)							
▶ internal1 (LAN_Dell Valle) - internal2 (LAN_WiFi) (2 - 2)							
▶ internal1 (LAN_Dell Valle) - VPN_Elastix (3 - 3)							
▶ internal1 (LAN_Dell Valle) - wan1 (Maxcom) (4 - 4)							
internal2 (LAN_WiFi) - internal1 (LAN_Dell Valle) (5 - 5)							
5	8	LAN_WiFi	LAN_Del Valle	always	ALL		Accept
▶ internal2 (LAN_WiFi) - wan1 (Maxcom) (6 - 7)							
▶ VPN_Elastix - internal1 (LAN_Dell Valle) (8 - 8)							
▶ wan1 (Maxcom) - internal1 (LAN_Dell Valle) (9 - 10)							
▶ Implicit (11 - 11)							

Figura10. Política Internal1 (LAN_WiFi) – Internal1 (LAN_Del Valle)

Política de regreso para que la LAN WiFi pueda tener comunicación con la LAN Del Valle.

IV. Internal1 (LAN_WiFi) – Wan 1 (Maxcom)

No. de Política	Origen	Destino	Web Filter	Application Control
11	VIP_OLAB	all	VIP_OLAB	VIP_OLAB
4	LAN_WiFi	all	Sucursal_Del Valle	Sucursal_Del Valle

Tabla6. Política LAN_WiFi – Wan 1 con Web Filter y Application Control

Seq.#	ID	Source	Destination	Schedule	Service	NAT	Action	Web Filter	Application Control
▶ dmz (PACS) - wan1 (Maxcom) (1 - 1)									
▶ internal1 (LAN_Dell Valle) - internal2 (LAN_WiFi) (2 - 2)									
▶ internal1 (LAN_Dell Valle) - VPN_Elastix (3 - 3)									
▶ internal1 (LAN_Dell Valle) - wan1 (Maxcom) (4 - 4)									
▶ internal2 (LAN_WiFi) - internal1 (LAN_Dell Valle) (5 - 5)									
▼ internal2 (LAN_WiFi) - wan1 (Maxcom) (6 - 7)									
6	11	VIP_OLAB	all	always	ALL	✓	✓ Accept	VIP_OLAB	VIP_OLAB
7	4	LAN_WiFi	all	always	ALL	✓	✓ Accept	Sucursal_Del Valle	Sucursal_Del Valle
▶ VPN_Elastix - internal1 (LAN_Dell Valle) (8 - 8)									
▶ wan1 (Maxcom) - internal1 (LAN_Dell Valle) (9 - 10)									
▶ Implicit (11 - 11)									

Figura11. Política Internal1 (LAN_WiFi) – Wan 1 (Maxcom)

Para las políticas con usuarios acceso a servicios de internet se activa la opción de Web Filter y Application Control.

V. VPN_Elastix – Internal1 (LAN_Del Valle)

No. de política	Origen	Destino
6	Red_Elastix	LAN_Del Valle

Tabla7. Política VPN_Elastix – LAN_Del Valle

Seq.#	ID	Source	Destination	Schedule	Service	NAT	Action
▶ dmz (PACS) - wan1 (Maxcom) (1 - 1)							
▶ internal1 (LAN_Dell Valle) - internal2 (LAN_WiFi) (2 - 2)							
▶ internal1 (LAN_Dell Valle) - VPN_Elastix (3 - 3)							
▶ internal1 (LAN_Dell Valle) - wan1 (Maxcom) (4 - 4)							
▶ internal2 (LAN_WiFi) - internal1 (LAN_Dell Valle) (5 - 5)							
▶ internal2 (LAN_WiFi) - wan1 (Maxcom) (6 - 7)							
▼ VPN_Elastix - internal1 (LAN_Dell Valle) (8 - 8)							
8	5	Red_Elastix	LAN_Del Valle	always	ALL	⊗	✓ Accept
▶ wan1 (Maxcom) - internal1 (LAN_Dell Valle) (9 - 10)							
▶ Implicit (11 - 11)							

Figura12. Política VPN_Elastix - Internal 1 (LAN Del Valle)

VI. Wan1 (Maxcom) – Internal1 (LAN_Del Valle)

No. de Políticas	Origen	Destino
9	all	Camaras Checador
10	all	LAN_Del Valle Soporte (Usuarios)

Tabla8. Política Wan1 – LAN_Del Valle

Seq.#	ID	Source	Destination	Schedule	Service	NAT	Action	Web Filter	Application Control	Authentication
▶ dmz (PACS) - wan1 (Maxcom) (1 - 1)										
▶ internal1 (LAN_Dell Valle) - internal2 (LAN_WiFi) (2 - 2)										
▶ internal1 (LAN_Dell Valle) - VPN_Elastix (3 - 3)										
▶ internal1 (LAN_Dell Valle) - wan1 (Maxcom) (4 - 4)										
▶ internal2 (LAN_WiFi) - internal1 (LAN_Dell Valle) (5 - 5)										
▶ internal2 (LAN_WiFi) - wan1 (Maxcom) (6 - 7)										
▶ VPN_Elastix - internal1 (LAN_Dell Valle) (8 - 8)										
▼ wan1 (Maxcom) - internal1 (LAN_Dell Valle) (9 - 10)										
9	9	all	Camaras Checador	always	ALL	⊗	✓ Accept			
10	10	all	LAN_Del Valle			⊗				
10.1				always	ALL		✓ Accept			SOPORTE
▶ Implicit (11 - 11)										

Figura13. Política Wan1 (Maxcom) – Internal1 (LAN_Del Valle)

En estas políticas se pueden tener acceso a los servicios con un nat publicado (cámaras y checador), además se tiene una política para el acceso a la VPN por SSL.

6.5. Configuración de VPNs

- I. Dentro del menú **VPN** en la opción **IPsec>>Auto key (IKE)** se tiene la configuración **VPN_Elastix**.

Name: VPN_Elastix

Comments: Write a comment... 0/255

Remote Gateway: Static IP Address

IP Address: 201.157.45.50

Local Interface: wan1 (Maxcom)

Mode: Aggressive Main (ID protection)

Authentication Method: Preshared Key

Pre-shared Key:

Peer Options

Accept any peer ID

Enable IPsec Interface Mode

IKE Version: 1 2

Mode Config:

Local Gateway IP: Main Interface IP Specify 0.0.0.0

P1 Proposal

1 - Encryption: AES128 Authentication: SHA1

DH Group: 1 2 5 14

Keylife: 28800 (120-172800 seconds)

Local ID: (optional)

XAUTH

Disable Enable as Client Enable as Server

NAT Traversal: Enable

Keepalive Frequency: 10 (10-900 seconds)

Dead Peer Detection Enable

OK Cancel

Figura14. Configuración fase 1 VPN_Elastix

Name: P2_Elastix

Comments: Write a comment... 0/255

Phase 1: VPN_Elastix

Advanced...

P2 Proposal

1- Encryption: AES128 Authentication: SHA1

Enable replay detection

Enable perfect forward secrecy (PFS).

DH Group: 1 2 5 14

Keylife: Seconds 1800 (Seconds) 5120 (KBytes)

Autokey Keep Alive: Enable

Auto-negotiate: Enable

Quick Mode Selector

Source address: Specify 172.16.25.0/24 Select -----Address-----

Source port: 0

Destination address: Specify 192.168.90.0/24 Select -----Address-----

Destination port: 0

Protocol: 0

OK Cancel

Figura15. Configuración fase 2 VPN_Elastix

II. Dentro del menú **VPN** en la opción **SSL** se configuró el perfil VPN por SSL.

Esta VPN permite dar acceso a los equipos que se encuentran dentro de la red interna además de poder atender las necesidades de los dispositivos que requieran algún soporte desde cualquier lugar que cuente con una conexión a internet.

Name:

Portal Message:

Theme:

Page Layout:

Enable Tunnel Mode

Enable Split Tunneling

IP Pools:

Client Options: Save Password Auto Connect Always Up (Keep Alive)

Enable Web Mode

Applications: HTTP/HTTPS FTP RDP SMB/CIFS
 SSH TELNET VNC PING
 CITRIX RDP NATIVE Port Forward

Include Session Info

Include Connection Tool

Include FortiClient Download

Include Bookmarks

Name	Type	Location	Description
No matching entries found			

Prompt Mobile Users to Download FortiClient App

Allow Multiple Concurrent Sessions For Each User

Figura16. Configuración fase 1 de VPN por SSL

IP Pools:

Server Certificate:

Require Client Certificate:

Encryption Key Algorithm: High - AES(128/256 bits) and 3DES
 Default - RC4(128 bits) and higher
 Low - RC4(64 bits), DES and higher

Idle Timeout: (seconds)

Login Port:

Allow Endpoint Registration (Tunnel Mode Only)

Advanced (DNS and WINS Servers)

Figura17. Configuración fase 2 de VPN por SSL

7. Resultados

Con la realización del proyecto de estancia aquí descrito, se obtuvo una implantación de la seguridad de la red de datos de Laboratorios OLAB a través de la configuración de un firewall para filtrar y bloquear sitios web de acuerdo a las políticas solicitadas y acordadas, así como la puesta en marcha de una VPN para la comunicación segura de información.

De esta manera, fue posible llevar un mejor control de cada usuario y así poder asignar los recursos necesarios para poder llevar a cabo sus actividades de manera segura. Además establecer comunicación de forma segura con Elastix a través de VPN's creadas y mejorar el flujo de datos en la red a través de rutas establecidas.

Una vez cumplidos los objetivos, teniendo buenos resultados al brindar una correcta configuración al FortiGate 60D fue posible elaborar un manual de configuración para futuras actualizaciones.

8. Conclusiones

Con la realización de este proyecto fue posible llevar a la práctica los conocimientos obtenidos en la Universidad sobre redes y seguridad.

El problema a resolver se logró solucionar en forma y tiempo, y así cumplir los objetivos al diseñar e implantar un sistema de seguridad de una red de datos usando un firewall FortiGate 60D creando perfiles de seguridad y usando herramientas que son necesarias para la empresas para poder cubrir sus necesidades tal como lo es Elastix.

De este manera, también fue posible adquirir otros conocimientos al usar equipos de la marca Fortinet en especial con el modelo FortiGate 60D, que bien puedo concluir que además de ser un sistema innovador por trabajar con sistemas de seguridad UTM, FortiGate 60D es capaz de mantener la seguridad de una empresa.

9. Bibliografía

- [1] Enredajo.blogspot.mx (2009). *Qué es una VPN y tipos de VPN* [online]. Disponible en: <http://enredajo.blogspot.mx/2009/03/que-es-una-vpn-y-tipos-de-vpn.html>
- [2] Universidad Autónoma de Guerrero, Cisco Networking Academy (2011). *Capítulo 7: Seguridad de la conectividad Site-to-Site* [online]. Disponible en: <http://ecovi.uagro.mx/ccna4/course/module7/#7.0.1.1>
- [3] Cisco (2008). *¿Qué es un Firewall?* [online]. Disponible en: http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
- [4] FortiGate-600C, F. (2016). *Fortinet FortiGate-600C - Neuronet*. [online] Disponible en: <http://www.neuronet.cl/producto/fortinet-fortigate-60/>
- [5] Asc (2016). *Antivirus Fortinet – ASC* [online]. Disponible en: www.asc.com.mx/hs-soluciones-de-seguridad/antivirus-fortinet/

10. Entregables

De acuerdo con el cronograma de actividades propuesto, se entregó de forma semanal al jefe directo un reporte con las actividades realizadas durante la estancia en T&B Talent S.A. de C.V. que incluyen reportes con los archivos de configuración de la creación de interfaces, rutas, políticas, grupos, objetos y VPN's, esto para tener un control y evaluar los resultados que se iban obteniendo a lo largo del proyecto.

Al finalizar, se hizo entrega de un manual de configuración del equipo FortiGate 60D que engloban las configuraciones antes mencionadas para futuras actualizaciones o adecuaciones que se requieran.