Universidad Tecnológica de El Salvador

FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS
TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

TEMA:

"ELABORACIÓN DE GUÍAS DE ADMINISTRACIÓN Y CONFIGURACIÓN DE FIREWALL FORTINET,

PARA FORTALECER LAS COMPETENCIAS SOBRE SEGURIDAD,

DE LA ASIGNATURA ADMINISTRACIÓN DE REDES DE LA UNIVERSIDAD TECNOLÓGICA DE EL SALVADOR".

TRABAJO DE GRADUACIÓN PRESENTADO POR:

Gerardo Benjamín Tobar Hernández

Hairo Rizzieri Flores Hernández

Moisés Arnulfo Escobar Castillo

PARA OPTAR AL GRADO:

TECNICO EN INGENIERIA DE REDES COMPUTACIONALES

ABRIL, 2014.

SAN SALVADOR, EL SALVADOR.

PÁGINA DE AUTORIDADES

ING NELSON ZÁRATE SÁNCHEZ
RECTOR

LIC. JOSE MODESTO VENTURA
VICERRECTOR ACADÉMICO

ING FRANCISCO ARMANDO ZEPEDA
DECANO

JURADO EXAMINADOR

ING. NOE RODRIGUEZ ELIAS MERLOS
PRESIDENTE

LIC. JUAN PABLO ORTIZ CINCO
PRIMER VOCAL

TEC. JUAN CARLOS AGUILAR SOLORZANO
SEGUNDO VOCAL

ABRIL, 2014

SAN SALVADOR, EL SALVADOR.

Universidad Tecnológica de El Salvador

ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Lic. Juan Pablo Ortiz Cinco, Tec. Juan Carlos Aguilar Solorzano, Ing. Noé Elías Rodriguez Merlos
a las 12:30pm. del día Viernes, 5 de diciembre de dos mil trece.
Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

1-Moises Arnulfo Escobar Castillo	CARNET 26-2984-2011
2-Gerardo Benjamín Tobar Hernández	CARNET 26-2254-2008
3-Hairo Rizzieri Flores Fernández	CARNET 26-2189-2007

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:
"Elaboración de guías de administración y configuración de Firewall Fortinett, para fortalecer las competencias sobre seguridad, de la asignatura administración de redes de la Universidad Tecnológica de El Salvador"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

APROBADO

YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 5 de diciembre de dos mil trece.

F. _____
PRIMER VOCAL
Lic. Juan Pablo Ortiz Cinco

F. _____
SEGUNDO VOCAL
Tec. Juan Carlos Aguilar Solorzano

F. _____
PRESIDENTE
Ing. Noé Elías Rodriguez Merlos

AGRADECIMIENTOS.

Agradezco de manera especial a Dios, al que es digno de toda honra y honor, por haberme otorgado mucha la sabiduría y fortaleza en el momento que lo necesitaba. Estaré, eternamente agradecido.

A mis padres: por apoyarme incondicionalmente, por su comprensión, su paciencia y sobre todo por haber creído en mí.

A nuestro asesor: Tec. Juan Carlos Aguilar, por dedicarnos gran parte de su valioso tiempo, para darnos su apoyo desde el primer momento en la redacción y corrección del trabajo de graduación.

A mis compañeros: Gerardo Benjamín y Hairo Rizzieri, doy las gracias por su amistad y compañerismo, por haberse mantenido constantes durante toda la realización de este trabajo de graduación.

Moisés Arnulfo Escobar Castillo.

AGRADECIMIENTOS

A DIOS: Sobre todas las cosas por haberme dado la sabiduría y la fortaleza para que fuera posible llegar hasta esta etapa de mi vida.

A MI FAMILIA: Por su cariño sin límites, su apoyo incondicional, su dedicación y empeño por ayudarme a ser una persona mejor cada día.

A MI ASESOR DE TESIS: Tec. Juan Carlos Aguilar por darnos su apoyo, ideas y correcciones en el proceso de realizar nuestra tesis y cumplir de una excelente manera su rol como asesor.

A MIS COMPAÑEROS DE TESIS: Moisés Escobar y Hairo Rizzieri por brindarme su amistad, su apoyo en todo momento y aportar su conocimiento junto al mío para lograr cumplir este reto.

A MIS AMIGOS Y COMPAÑEROS Y A UNA PERSONA MUY ESPECIAL: Que de una u otra manera estuvieron pendientes a lo largo de este proceso, brindado su apoyo.

Gerardo Benjamín Tobar Hernández.

AGRADECIMIENTOS

A MI PADRE ETERNO: Gracias a mi Dios quien me otorgo la vida, salud, sabiduría y los recursos necesarios para culminar esta carrera.

A MIS PADRES: Gracias a mi Madre Celestina Hernández y mi Padre Juan Antonio Flores. Por la educación y consejos que me brindaron y el apoyo económico que gracias a Dios han logrados los frutos esperados.

A MI ESPOSA: Vanessa de Flores Por ser el motor y la inspiración que me ayudaron a culminar este proceso.

NUESTRO ASESOR: Tec. Juan Carlos Aguilar, Quien nos guio por este largo proceso nos brindó de su sabiduría y consejos para terminar de la mejor manera nuestro proyecto de tesis.

COMPAÑEROS: Benjamín Tobar y Moisés Escobar. Gracias brindarme su amistad y Por darme la oportunidad de elaborar el proyecto de tesis junto a ellos. A demás de darme su respaldo y compartir sus conocimientos.

Hairo Rizzieri Flores

INDICE

INTRODUCCIÓN.

El crecimiento exponencial de internet y la constante evolución de sus vulnerabilidades hace que los especialistas en seguridad y gestión de riesgos en las redes se encuentren entre los más buscados por las organizaciones de todo el mundo y la demanda sigue en aumento.

La escases de candidatos calificados con el conocimiento especializado y habilidades necesarias para administrar dispositivos y aplicaciones en una infraestructura segura, hace que este estudio sea de provecho para el Docente y los nuevos estudiantes de la carrera Técnico en Ingeniería de Redes Computacionales.

Las vulnerabilidades en las redes de datos está presente, principalmente en los Campus Universitarios es por eso que este trabajo contiene, guías de configuración y administración básicas del dispositivo de seguridad Firewall Fortinet FortiGate 40-C, las cuales facilitarán el aprendizaje en las prácticas de seguridad en el laboratorio de redes y permitirá la implementación de una red segura en la Universidad Tecnológica de El Salvador.

CAPITULO I

SITUACION ACTUAL

1.1 Situación Problemática.

En la Universidad Tecnológica de El Salvador, una de las carreras impartidas es: Técnico en Ingeniería de Redes Computacionales, en la cual los estudiantes cursan la asignatura de: Administración de Redes, que contiene como uno de sus temas principales la seguridad informática.

La facultad de Informática y Ciencias Aplicadas, ha adquirido nuevos equipos firewall con la finalidad que estos sean utilizados para realizar prácticas en el laboratorio de redes. Con dicha adquisición se realizó una consulta en la Biblioteca, en la cual se determinó: que existen libros que proporcionan la información acerca de temas de seguridad dentro de una red, pero no existe material didáctico que brinde a los docentes y el alumnado los conocimientos necesarios para la administración e implementación para realizar prácticas con dichos equipos. Por lo consiguiente proponemos: la realización de guías didácticas para el conocimiento y aprendizaje básico que será puesto a disponibilidad de docentes y alumnos. Dicho material servirá para que puedan tomarlo como referencia en el momento que necesiten implementarlo, encontraran desde puntos básicos hasta soluciones empresariales.

Los estudiantes serán beneficiados porque contaran con material didáctico el cual se elaborará las guías tomando como referencia el diseño instruccional para que esto permita realizar prácticas que fortalecerán los conocimientos y habilidades de estudiantes de la asignatura administración de redes como a todos aquellos que deseen aprender sobre la temática de seguridad basada en firewall Fortinet.

Es importante destacar la importancia que tiene la administración de una red, por los datos que en ella circulan por ello incorporar conocimientos sobre cómo dar seguridad a una red computacional es vital. Con la culminación de este trabajo esperamos ayudar a futuros estudiantes los cuales tendrán a disposición este material de apoyo.

Se Desarrollara un manual de puntos claves que incorporan la seguridad en redes, esto permitirá tener una referencia importante tanto a nivel teórico como practico donde se detallaran la aplicación de administración y configuración del firewall Fortinet para que pueda ser usada por los estudiantes de la Universidad Tecnológica de El Salvador.

1.2 Justificación.

Esta guía será un beneficio que obtendrán los estudiantes de la asignatura Administración de Redes, de la carrera Técnico en Ingeniería de Redes Computacionales de la Universidad Tecnológica de El Salvador. Para obtener información didáctica y poder contribuir al fortalecimiento de competencias y aplicar todos los conocimientos para estar a la vanguardia de la tecnología en seguridad de redes informáticas, ya que es un tema es bastante complejo y se ha convertido en una de las principales preocupaciones de las empresas e instituciones que utilizan Internet como su medio de publicidad, distribución de información, comunicación en general, telefonía y video conferencias. También, influir en la formación profesional de cada uno de los estudiantes ya que actualmente la misión de todo administrador de redes, es considerar las nuevas vulnerabilidades existentes y así lograr el aporte de soluciones para disminuir riesgos.

Los estudiantes de la Universidad Tecnológica de El Salvador tendrán la oportunidad de acceder a la guía didáctica que se encontrará disponible en la Biblioteca de La Universidad.

1.3 Objetivos

1.3.1 General

Elaborar material de apoyo didáctico que desarrolle habilidades y competencias en los estudiantes de la Universidad Tecnológica de El salvador. Donde se integren las áreas básicas de seguridad de una red: Instalación, implementación, configuración, y administración básica de la seguridad en una red de datos utilizando el equipo firewall Fortinet fortigate-40C.

De este modo alcanzar el aprendizaje necesario a través de guías prácticas estructuradas de forma comprensiva.

1.3.2 Específicos

I. Realizar un documento donde el estudiante pueda apoyarse para desarrollar un proceso de aprendizaje autónomo o colaborativo, y orientarse a las funcionalidades de equipos firewall.

II. Presentar guías prácticas comprensivas sobre configuración de Firewall Fortinet FortiGate-40C con seguimiento sistematizado (Paso a Paso), el cual

facilite a los estudiantes La compresión y ejecución de las actividades planteadas en cada una de ellas

1.4 Alcances

1. Identificar el equipo físicamente. conexiones, puertos utilizados para preparar el equipo para su respectiva configuración. A demás instruiremos paso a paso como configurar el equipo Firewall Fortinet FortiGate-40C a través guías prácticas que muestran como ejecutar del asistente de instalación, establecer conexión con la red, donde se aplicara seguridad en parámetros esenciales en una empresa.

2. Un documento con guías prácticas de apoyo a los docentes y estudiantes. Que serán de utilidad para fomentar el desarrollo de las competencias en seguridad realizar las prácticas sobre Firewall en el laboratorio de redes.

1.5 Estudio de Factibilidad

1.5.1 Factibilidad Técnica

El proyecto es factible ya que el equipo Fortinet FortiGate-40C, proporciona un conjunto integrado de seguridad básica y los servicios de redes, es un equipo fácil de manejar y de alto rendimiento que es capaz de soportar una amplia gama de escenarios de implementación, permite mejorar la visibilidad de la red y aumentar el control sobre los usuarios, aplicaciones y datos. Los dispositivos ofrecen una protección en tiempo real, esto simplifica el diseño del aparato y proporciona un extraordinario rendimiento para redes más pequeñas, siendo utilizado por empresas, oficinas y centros educativos.

La Universidad adquirió 6 de estos equipos, por consiguiente se pueden desarrollar las competencias de: instalación, configuración y administración las cuales se podrán desarrollar realizando los planteamientos expuestos en las guías con el apoyo del docente.

A continuación se detalla la ficha técnica de los equipos de cómputo que actualmente posee el laboratorio de redes en la Universidad Tecnológica de El Salvador para el desarrollo de las guías didácticas.

Cuadro 1: Estudio de Factibilidad Técnica

Interface	Tipo	Protocolo	Descripción
Puertos Ethernet 1-5	RJ-45	Gigabit Ethernet	FortiASIC aceleró puerto Ethernet conmutados para la conexión a la red
WAN 1,2	RJ-45	Gigabit Ethernet	FortiASIC aceleró puerto Ethernet
USB	USB-A	USB 2.0	Puerto del servidor USB para llave memoria flash, módem o para realizar funciones de gestión.
USB MGMT	USB-B	USB 2.0	Puerto USB cliente para funciones de gestión.
Consola	RJ-45	RS-232 serial	Conexión opcional al equipo de gestión

Especificación de Hardware	Descripción
CPU	FortiASIC SoC
Almacenamiento Interno	No extraíble, 4gb de múltiples niveles de células NAND flash para optimización WAN
Memoria	512 MB (DDR 2)
Energía AC	100-240V, 50-60HZ
Consumo de energía	12.3W / 14.8W
Disipación de calor	50.5BTU/h
Montaje en pared	Sí
Ranura de seguridad Kensington	Ranura de seguridad antirrobo
Botón de reinicio	Presionar durante 5 segundos para restablecer el FortiGate al ajuste de fábrica

1.2 Requerimientos mínimos del PC

Procesador, sistema operativo y memoria	
Sistema operativo	Genuine Windows Xp Professional.
Procesador	Intel ® Pentium ® de doble núcleo E2140. 1.60 GHz 1Mb de cache L2 800 MHz FSB.
Chipset	Intel 963Q Expreso.
Memoria serie	2X512 Mb.
Tipo de memoria	PC2-530 (DDR2 667).
Las ranuras de memoria	4 DIMM.
Actualización de la memoria	Ampliable a 4 Gb.
Unidades internas	
Disco duro	80 Gb
Velocidad de la unidad	7200 rpm
Bahías de unidad externa	2 externos de 5,25 pulgadas, 1 externo de 3,5 pulgadas
Bahía interna de unidad	2 internos de 3,5 pulgadas
CD ROM y DVD	48X/32X Combo
Controlador de disco duro	SATA 3.0 Gb/s

1.5.2 Factibilidad Económica

El proyecto es económicamente factible debido a que se cuenta con el software y hardware del equipo firewall marca Fortinet modelo FortiGate-40C, los cuales están disponibles en el laboratorio de redes de La Universidad Tecnológica de El Salvador. Por tanto no se incurrirá en gasto adicional para el desarrollo de este proyecto denominado Elaboración de Guías de administración y configuración de firewall Fortinet, para fortalecer las competencias sobre seguridad, de la asignatura Administración de Redes.

Cuadro 2: Herramientas necesarias para la elaboración de las guías didácticas y realización de prácticas.

Producto	Costo
Hardware: Fortinet Fortigate-40c	$0.00 (Adquirido y proporcionado por la universidad.)
Software	$0.00 (incluido con el equipo.)
Hardware: Computadora	$0.00 (El lab. de redes cuenta con 40 computadoras a disposición para las prácticas.)

1.5.3 Factibilidad operativa

Cuadro 3: especificaciones de las realizaciones de prácticas

Temas	Nombres de las practicas	Duración
Conocimiento de la interfaz gráfica GUI	Comandos básicos de configuración	90 min
Configuración básica a través del Setup Wizard	Administración y configuraciones básicas a nivel de consola	90 min
Comandos básicos por medio de CLI	Filtrado de contenido WEB	90 min
Creación de backup y procedimiento de restauración	Administración asistida por software Fortinet	90 min

1.6 Carta de Aceptación

San Salvador 08 de Marzo 2013

Universidad Tecnológica de El Salvador
Presente:

Por este medio hacemos constar que estamos desarrollando el proyecto titulado "Elaboración de Guías de administración y configuración de firewall Fortinet, para fortalecer las competencias sobre seguridad, de la asignatura Administración de Redes de la Universidad Tecnológica de El Salvador" Dicho proyecto tendrá una duración de 5 meses desde Agosto a Diciembre del presente año.

El personal involucrado para el desarrollo de este proyecto es:

_____	_____
Gerardo Benjamín Tobar Hernández	Moisés Arnulfo Escobar Castillo
Alumno	Alumno
_____	_____
Hairo Rizzieri Flores Hernández	Tec. Juan Carlos Aguilar Solórzano
Alumno	Asesor

_____
Lic. Juan Pablo Ortiz Cinco
Coordinador Cátedra de Redes

CAPITULO II

FUNDAMENTOS DE SEGURIDAD EN LAS REDES

2.1 Principios de una red segura

Mantener una red segura garantiza la seguridad de los usuarios y protege los intereses comerciales. Esto requiere vigilancia de parte de profesionales de seguridad en redes quienes deberán estar constantemente al tanto de las nuevas y evolucionadas amenazas y ataques a las redes, así como también de las vulnerabilidades de los dispositivos y aplicaciones. La mayor motivación de la seguridad en redes es el esfuerzo por mantenerse un paso más delante de los hacker mal intencionados.

Diversas organizaciones han creado dominios que subdividen el mundo de la seguridad de redes en segmentos fácilmente manejables. Estas organizaciones establecen estándares, fomentan la colaboración y proveen oportunidades de desarrollo para los profesionales de la seguridad.

Tal como la seguridad en redes está compuesta de dominios, los ataques a las redes son clasificados, para hacer más fácil aprender de ellos y abordarlos apropiadamente. Los virus, gusanos y troyanos son tipos específicos de ataque a las redes. Generalmente los ataques a las redes se clasifican como ataques

de reconocimiento, de acceso o de denegación de servicio. Los profesionales de la seguridad en redes son responsables de crear y mantener la política de seguridad de red. Todas las prácticas de seguridad en redes están relacionadas con y guiadas por la política de seguridad en redes

2.1.1 Evolución de la seguridad en redes

Hoy en día internet es una red muy diferente a la que era en sus comienzos en los años sesenta. El trabajo de un profesional en redes incluye asegurarse de que el personal apropiado este muy versado en herramientas, procesos, técnicas, protocolos y tecnologías de seguridad en redes. Es crítico que los profesionales de seguridad en redes mantengan una paranoia saludable para manejar la colección de amenazas a las redes en constante evolución.

2.1.2 Dominios de seguridad en las redes

Los dominios proveen un marco organizado para facilitar el aprendizaje sobre la seguridad en redes. Es importante entender el funcionamiento de cada uno de estos dominios de la seguridad de redes.

Existen 12 dominios de seguridad descritos por **ISO/IEC27002** que sirven para organizar a alto nivel la información dentro de la seguridad en redes. Estos dominios tienen algunos paralelismos significativos con los dominios definidos por la certificación CISSP. Los 12 dominios están diseñados para servir como base común para desarrollar los estándares de seguridad en las organizaciones y las prácticas de administración de seguridad efectiva, así como también para ayudar a construir confianza en las actividades que tienen como lugar dentro de la organización

Los dominios de la seguridad en redes proveen una separación conveniente para los elementos de la seguridad en redes. Estos 12 dominios sirven como referencia útil para avanzar en el trabajo como profesional de la seguridad en redes.

1. **Evaluación de Riesgos:** es el primer paso en el proceso de administración de riesgos. Determina el valor cuantitativo y cualitativo del riesgo relacionado con una amenaza reconocida o situación determinada
2. **Política de seguridad:** es un documento que trata de las restricciones y comportamientos de los miembros de una organización y generalmente especifica cómo se puede acceder a los datos y quien puede hacerlo
3. **Organización de la seguridad de la información:** Es el modelo de gobierno establecido por una organización para la seguridad de la información

4. **Administración de los bienes:** es un inventario y esquema de clasificación para los bienes
5. **Seguridad de los recursos humanos:** trata de sobre los procedimientos de seguridad que guardan relación con los empleados de una organización que entran, se mueven en ella
6. **Seguridad física y ambiental:** describe la protección de las instalaciones reales de los ordenadores dentro de una organización
7. **Administración de las comunicaciones y las operaciones:** describe la administración de los controles técnicos de seguridad en sistemas y redes
8. **Control de acceso:** describe la restricciones derechos a redes sistemas, aplicaciones, funciones de datos
9. **Adquisición, desarrollo y mantenimiento de los sistemas de información:** describe la integración de seguridad a las aplicaciones
10. **Administración de incidentes de seguridad de la información:** describe como anticipar y responder a las fisuras de seguridad de la información
11. **Administración de la continuidad de los negocios:** describe la protección , mantenimiento y recuperación de procesos y sistemas críticos para los negocios
12. **Conformidad:** describe el proceso de asegurar la conformidad con las regulaciones, los estándares y las políticas de la seguridad, de la información

2.2 Políticas de seguridad en redes

Uno de los dominios más importantes es el de las políticas de seguridad una política de seguridad es una declaración formal de las reglas a las cuales deberán atender las personas que tienen acceso a los bienes tecnológicos y de información de una organización. La conceptualización, el desarrollo y la aplicación de una política de seguridad tienen un rol significativo en mantener a la organización segura. Es responsabilidad del profesional de la seguridad en redes hacer cumplir las políticas de seguridad en todos los aspectos de las operaciones de negocios en la organización.

La política de seguridad en redes es un documento amplio diseñado para ser claramente aplicable a las operaciones de una organización. Por su amplitud de cobertura e impacto, generalmente es un comité el que lo compila. Es un documento complejo que está diseñado para gobernar temas como accesos a los datos, navegación en la web, uso de las contraseñas, criptografía y adjuntos de correo electrónico.

La política de seguridad en redes traza las reglas de acceso a la red determina como se harán cumplir las políticas y describe la arquitectura básica del ambiente básico de seguridad de la información de la empresa

Antes de crear una política de seguridad debe entenderse que servicios están disponibles para que usuarios. La política de seguridad de red establece una

jerarquía de permisos y accesos y da a los empleados solo el acceso mínimo necesario para realizar sus tareas.

La política de seguridad de la red establece que bienes deben ser protegidos y da pautas sobre cómo deben ser protegidos. Esto será luego usado para determinar los dispositivos de seguridad y las estrategias y procedimientos de mitigación que deberán ser implementados en la red. Una posible orientación que los administradores pueden utilizar en el desarrollo de la política de seguridad y la determinación de distintas estrategias de mitigación es la incorporación de hardware o software necesarios para mantener una red segura basándonos en el tipo de rubro y magnitud de una empresa.

2.3 Principales técnicas de ataque

2.3.1 Engaño IP (Spoofing)

Una máquina suplanta la identidad de otra, Se usa para persuadir a un sistema que acepte datos como si vinieran de la fuente original o bien para recibir datos que debería ir a la máquina suplantada. Esta debilidad se debe a que los Routers solo miran la dirección de destino del paquete.

2.3.2 Husmeando en la red (Sniffing)

Una maquina intermedia entre el receptor y el transmisor, escucha os paquetes. En redes de medio compartido como Ethernet, las tarjetas de red tienen un segmento de hardware encargado de acceder a todos los datos que viajan por el medio.

2.4 Servicios de Red

Cuando abrimos un navegador de Internet e ingresamos una URL, accedemos a un servicio de red. La URL específica, entre otras cosas, la dirección remota de un equipo al que queremos acceder. Esta dirección remota (bajo una red TCP/IP) se denomina dirección IP.

El protocolo del servicio, que pertenece a la capa 7 o a la aplicación del modelo de referencia OSI, establecer las pautas sobre la comunicación entre la aplicación cliente y servidor.

Cuadro 1. Algunos de los protocolos más conocidos y sus puertos son los siguientes:

Servicio	PUERTO TCP PREDETERMINADO
HTTP	80
SMTP	25
POP 3	110
IMAP	143
HTTPS	443
TELNET	23
FTP	21
SSH	22
DNS	53
IRC	¿6667 o 194?

2.5 Modelo de referencia OSI

El **modelo de referencia OSI** (*open System* interconnection, interconexión de sistemas abiertos) lo desarrolló la ISO (*international standard organisation*, organización internacional de normalización) como una guía para definir un conjunto de protocolos abiertos. Su finalidad es proporcionar una base común para la coordinación en el desarrollo de normas destinadas a la interconexión de sistemas, permitiendo a la vez situar las normas existentes en la perspectiva del

modelo de referencia global. Tiene también como finalidad identificar los campos en los que se requiere la elaboración y el perfeccionamiento de normas, así como mantener la coherencia de todas las normas dentro de un marco común.

Cuadro 2 Capas del modelo OSI.

CAPAS DEL MODELO OSI		
7 - Aplicación	→	Procesos de red a aplicaciones
6 - Presentación	→	Representación de datos
5 - Sesión	→	Comunicación entre Host
4 - Transporte	→	Conexión de extremo a extremo
3 - Red	→	Direccionamiento y mejor ruta
2 - Enlace de datos	→	Acceso a los medios
1 - Física	→	Transmisión binaria

2.5.1 La capa de transporte

La capa de transporte establece las reglas para conectar dos dispositivos remotos. Permite que las estaciones finales ensamblen y re ensamblen múltiples segmentos del mismo flujo de datos. Esto se hace por medio de identificadores que en protocolos TCP, UDP y SCTP reciben el nombre de **números de puerto**.

En la capa de transporte los datos pueden ser transmitidos de forma: **Fiable**

2.6 Protocolo TCP (Transmission Control Protocol)

Orientado a conexión con un saludo previo de tres vías antes de enviar los datos.

Permite además el transporte fiable entre los sistemas.

Asegura que los segmentos de datos distribuidos serán confirmados.

Proporciona la retransmisión de los segmentos no confirmados.

Coloca de nuevo los segmentos recibidos en su orden.

Proporciona control de flujo regulando el tráfico de datos.

2.7 Protocolo UDP (User Datagram Protocol)

No orientado a conexión, solo se establece un saludo de dos vías antes de enviar los datos. Transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones de datos. Algunos de los números de puertos utilizados por TCP, UDP y SCTP-rango **1** al **1023.**

2.7.1 Puertos más conocidos

1–255 puertos públicos

256–1023 puertos asignados a empresas

Rango **1024** al **49151**-asignados por **IANA** a específicas aplicaciones

Rango **49152** al **65535**-puertos dinámicos y privados

Cuadro 3 Puertos más comunes.

PUERTOS MAS COMUNES				
Nº	**TCP**	**UDP**	**SCTP**	**PROTOCOLO**
7	✓	✓	×	Echo
9	✓	✓	✓	Discard
13	✓	✓	×	Daytime
19	✓	✓	×	Character generator
20	✓	✓	✓	FTP data transfer
21	✓	✓	✓	FTP command
22	✓	✓	✓	SSH
23	✓	✓	×	Telnet
25	✓	✓	×	SMTP
37	✓	✓	×	Time
43	✓	✓	×	WHOIS
52	✓	✓	×	XNS
53	✓	✓	×	DNS
67	✓	✓	×	DHCP Server
68	✓	✓	×	DHCP Client
69	✓	✓	×	TFTP
70	✓	✓	×	Godher
79	✓	✓	×	Finger
80	✓	✓	✓	HTTP
101	✓	✓	×	NIC host name
109	✓	✓	×	POP2
110	✓	✓	×	POP3
119	✓	✓	×	NNTP
123	✓	✓	×	NTP
161	✓	✓	×	SNTP

2.8 Arquitectura y teoría de Firewall

Los filtros de paquetes, son una forma eficaz de control de tráfico que entra y sale de la red. La gran ventaja es que al trabajar sobre las capas IP y TCP/IP, no deben hacer cambios a nivel de la aplicación. Es también la gran desventaja, el número de reglas puede ser muy limitado, así que se requieren reglas adicionales.

2.9 Firewall.

El Firewall surge como un instrumento principal para ejecutar la política de seguridad de una organización. Al trabajar en todas las capas del modelo son complementarios a los filtros de paquete.

2.9.1 Firewall e Internet

El Firewall se instala entre la conexión de la red interna y el enlace a internet. Todo el tráfico que viene y sale a Internet pasa por el Firewall, su configuración, debe de estar en concordancia con la política de seguridad definida. Hoy en día una red conectada a Internet sin un Firewall es altamente riesgosa.

2.9.2 Que puede hacer un firewall

Ser una fuente de decisiones de seguridad. Permite concentrar las medidas de seguridad en un solo punto de red. Refuerza las políticas de seguridad. La mayoría de los servicios que los usuarios demandan de Internet, son inseguros. Por ejemplo, el uso de NFS desde fuera de la organización.

Almacenar su relación con Internet. Por ser "cuello de botella". Es factible registrar lo que ocurre entre la red protegida y la externa.

Limitar la exposición. Se puede usar un Firewall interno, es decir, dentro de la misma organización.

2.9.3 Que no puede hacer un Firewall

Proteger contra personas maliciosas internas en la red.

Proteger las conexiones que no pasan por él.

Proteger contra amenazas desprotegidas, pero es factible reconfigurarlo ante la nueva situación.

¿Proteger contra virus? No olvidar la interrogante.

2.10 Tipos de Firewall

2.10.1 Hardware

Este tipo de sistema es colocado sobre los dispositivos usados para ingresar a Internet, los llamados “routers”. Frecuentemente la instalación ya se encuentra realizada cuando compramos el router. En caso contrario es muy recomendable realizar la instalación. La colocación del firewall en este caso es muy compleja, es hecha gracias a un navegador que tiene acceso a Internet.

Host de base dual: este tipo de equipo utiliza dos tarjetas, una de las tarjetas conecta el equipo con una red interna y la otra con la externa.

Host de bastión: Se trata de un computador con una sola tarjeta de red. Un router de selección de filtro de paquetes, se interpone entre la red externa y el bastión. De esta forma se introduce un nivel adicional de seguridad al momento de tratar de penetrar las redes.

2.10.2 Software

Pueden ser distinguidos dos tipos de estos firewalls, el primero es el **gratuito:** también conocido bajo el nombre de software firewall, que puede ser usado con total libertad y de manera totalmente gratuita como su nombre indica. Su objetivo es rastrear y no permitir acceso a ciertos datos a las computadoras personales. Hoy en día la mayoría de las PC ya tienen el firewall colocado. Este sistema es caracterizado por su fácil instalación, al que pueden ser sumados otros sistemas para asegurar la computadora, cuando deja de funcionar, es la misma PC quien se encarga de avisarlo, no es requerido un sistema de Hardware para colocarlo y generalmente son utilizado en una sola computadora.

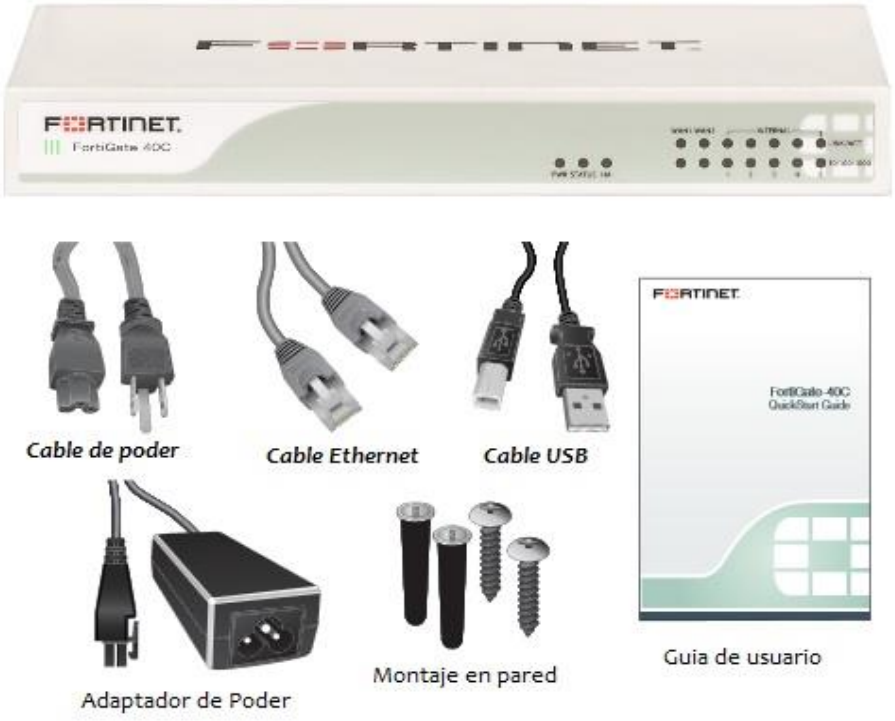
2.11 Sistema de gestión unificada de amenazas FortiGate-40C

FortiGate-40C es gestión unificada de amenazas, que incluye firewall, control de aplicaciones, IPS, antivirus, anti-spyware, anti-spam, VPN, filtrado web, control de aplicaciones, prevención de fuga de datos para una protección completa. Son ideales para las pequeñas empresas, oficinas pequeñas sucursales y puntos de venta que requieren todas las funciones de seguridad de red de grandes dispositivos.

2.11.1Características y ventajas

- ✓ 200 Mbps de rendimiento ofrece un rendimiento rápido para implementaciones de alto ancho de banda.
- ✓ Protección, incluyendo firewall, control de aplicaciones, IPS, antivirus, antispyware, anti-spam, VPN, filtrado web, control de aplicaciones, prevención de fuga de datos para la protección integral de las pequeñas empresas, tiendas minoristas y entornos de sucursales múltiples amenazas.
- ✓ Dos interfaces WAN y cinco puertos de switch internos ofrecen dos zonas de seguridad para la aplicación de políticas en los sitios remotos
- ✓ Licencias de usuarios ilimitados minimiza los costos de operación y se asegura que los cambios en el número de usuarios no interfieren con la disponibilidad de la red
- ✓ Disponible FortiManager y electrodomésticos FortiAnalyzer simplificar la gestión de la seguridad y reducir los gastos operativos en múltiples implementaciones
- ✓ Servicios de Suscripción FortiGuard entregar, protección hasta al día automatizada en tiempo real contra las amenazas de seguridad y vulnerabilidades.

2.12 Componentes incluidos en el paquete de un Fortinet FortiGate 40-C



2.13 Conectando el equipo

Asegúrese de que la unidad de FortiGate se coloca sobre una superficie estable antes de la primera configuración e instalación.

Precaución:

La descarga electrostática (ESD) puede dañar el equipo Fortinet.

No coloque objetos pesados sobre la unidad.

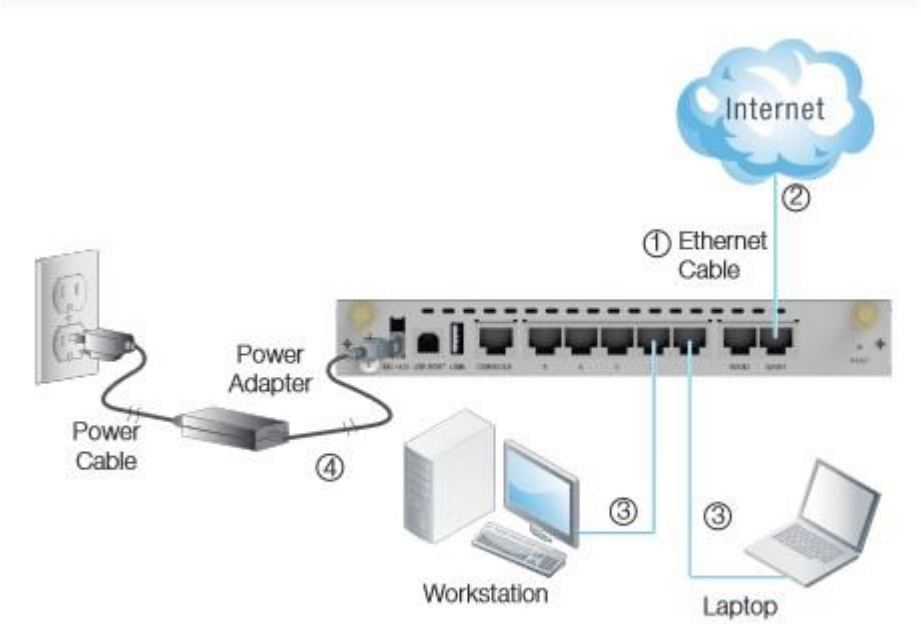
2.14 Conexión de dispositivos

1. Conecte el cable Ethernet al puerto WAN1.

2. Conecte el otro extremo del cable Ethernet a su red o Conexión a Internet.

3. Conecte un cable Ethernet para cada equipo que desee conectar a la unidad de FortiGate.

4. Conecte el adaptador de alimentación a la unidad de FortiGate y enchufe el cable de alimentación a una toma de corriente eléctrica.



2.14 GUIA 1

CONOCIENDO LA INTERFAZ GRAFICA DE USUARIO (GUI) DEL FORTIEXPLORER

1. Conociendo la interfaz gráfica de usuario (GUI) de FortiExplorer.

FortiExplorer es el software que acompaña a cualquier dispositivo Fortinet. Permite instalar, configurar fácil y rápidamente plataformas FortiGate.

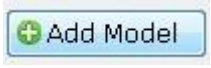
Proporciona instrucciones fáciles de seguir para la configuración básica. Como configurar la contraseña de administrador, las redes WAN y LAN, de igual manera nos permite de una forma fácil el registro del dispositivo.

Antes de iniciar las configuraciones, es necesario que FortiExplorer reconozca nuestro dispositivo.

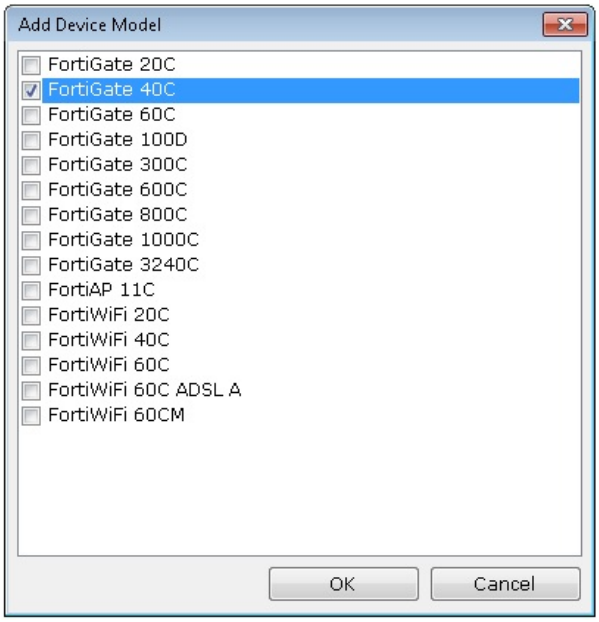
Para que el reconocimiento del equipo se realice correctamente, debemos de tomar en cuenta los siguientes pasos.

1- Seleccionar la opción

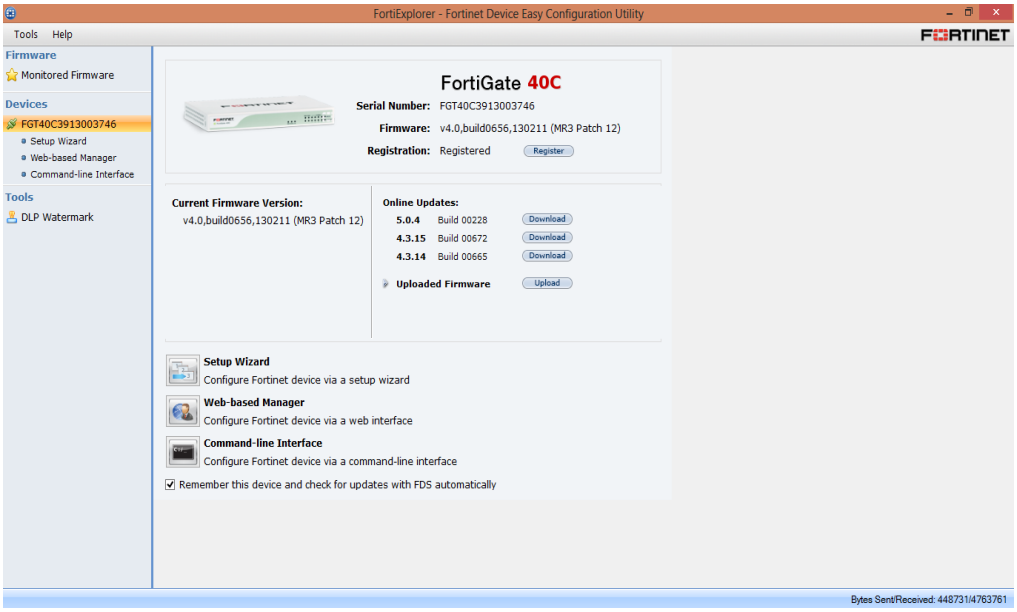
2- A continuación seleccionamos la opción



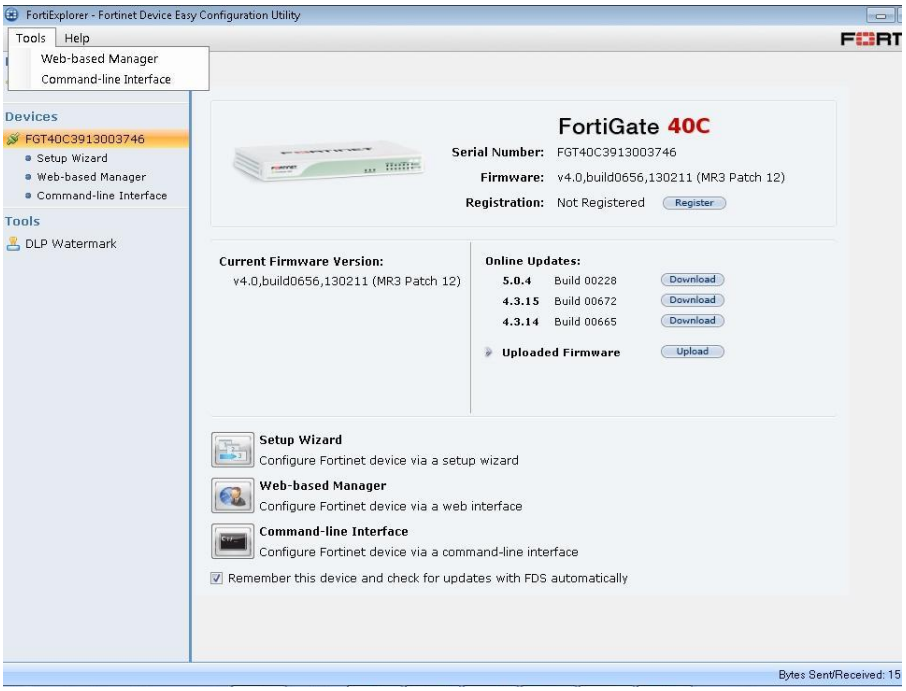
3- Aparece una lista con los dispositivos que podemos agregar en nuestro caso “FortiGate 40-C” damos clic en la opción ok.



4- Ahora podemos iniciar a explorar las opciones de FortiExplorer.



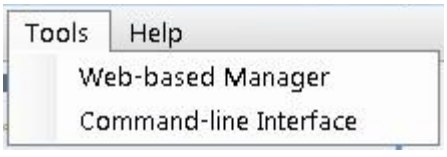
Opciones para la administración del Firewall.



1- Menú Tools (Herramientas)

Esta opcion nos brinda dos posiblidades para configurar nuestro firewall

Web-based Manager: Visualizar Confuguraciones y monitor atraves de la GUI (interfaz grafica de usuario)



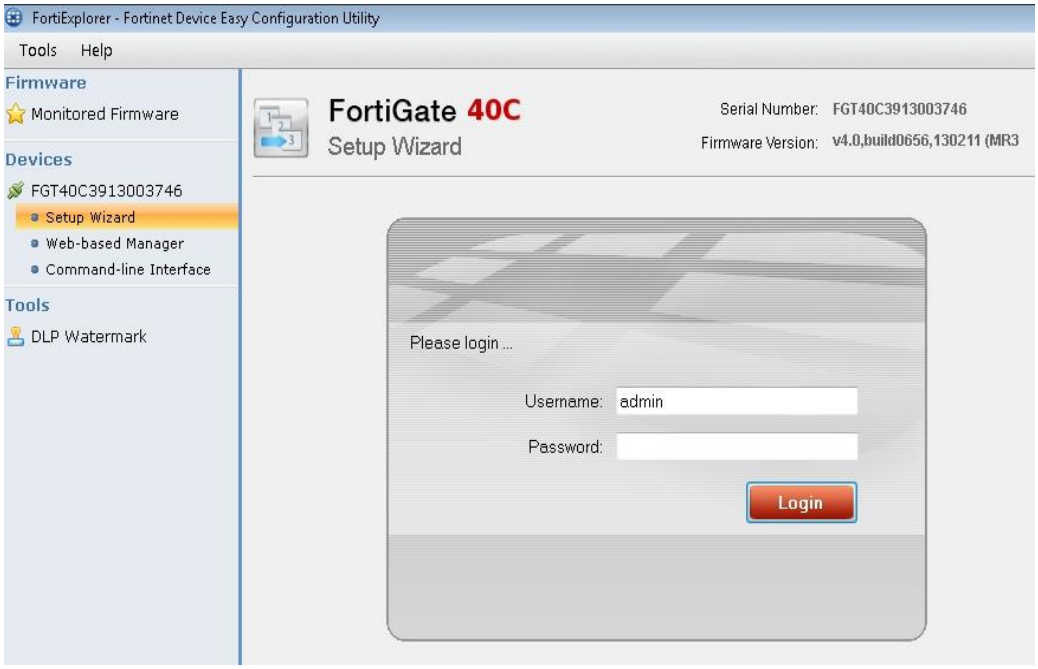
Command-line Interface: Confugurar atra ves de cosola utilizando lineas de comandos.

2- Menú Help: (Ayuda)

En esta opción podemos buscar ayuda en línea y más información acerca de nuestro dispositivo.

3- Setup Wizard:

Configurar a través de la interfaz gráfica. En un inicio antes de configurar nuestro FortiGate nos solicitará una contraseña. Por defecto el FortiGate no tiene contraseña establecida así que solo damos clic en login.



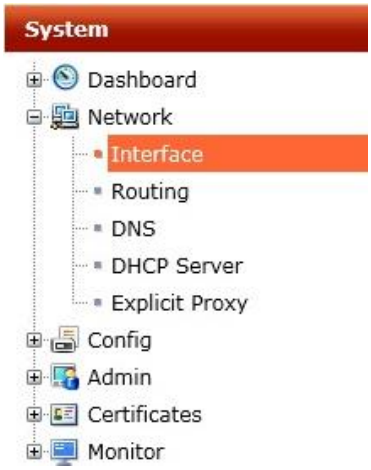
En esta opción podemos definir las configuraciones del sistema como:

- la contraseña de administración.
- Zona Horaria.
- Configurar la topología WAN
- Establecer redes WAN primarias.
- Configurar las redes LAN
- Configurar la seguridad
- Ver un sumario de las configuraciones del sistema.

4- Web-based Manager

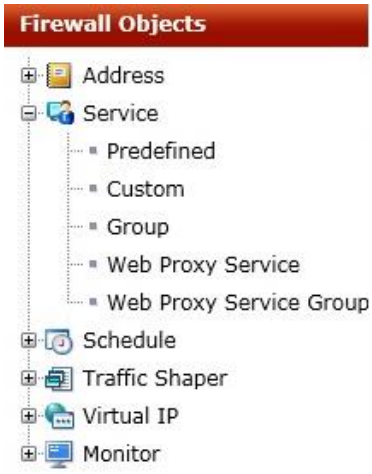
Contiene las opciones para monitorear lo que ocurre en la red y hacer ajustes en las configuraciones.

- *Sistema (System):* Contiene las configuraciones básicas del sistema. Permite ver el estado en general de nuestro dispositivo. Configurar interfaces, realizar rutas, configurar DNS, DHCP y puertos proxy.



- *Pollicy (Políticas)*: Configurar y monitorear las políticas de seguridad a implementar en la red

- *Firewall Objects:* Administrar filtrar y monitorear el trafico de la red,



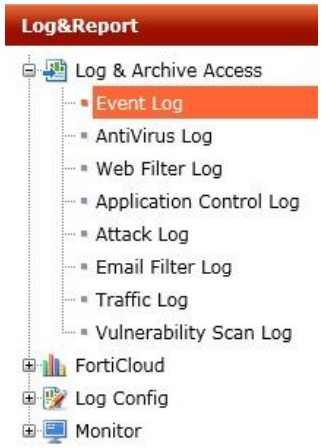
- UTM Profiles: Monitorear amenazas a la red, aplicar políticas para la seguridad de la red, configurar los protocolos y los filtros para sitios web.

- VPN: Configurar y monitorear las VPN en nuestra red

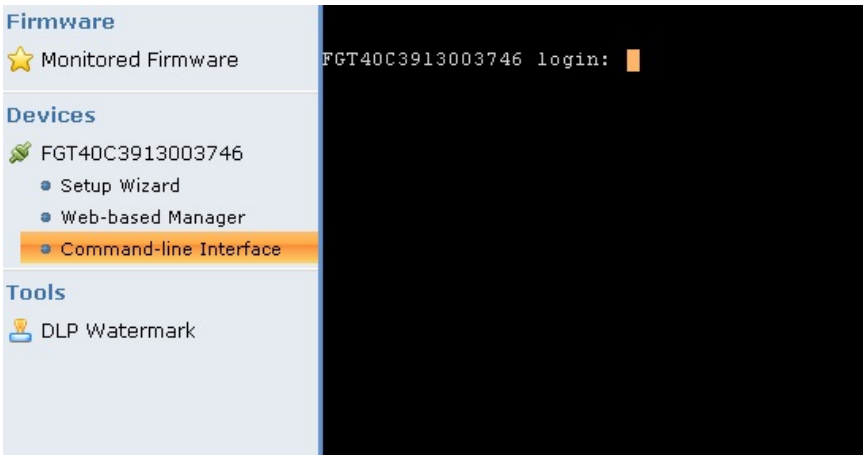
- USER: Gestionar y administrar usuarios y grupos.

- Wifi Contoller: Monitorear redes Wifi, realizar configuraciones gestionar puntos de Access Points (Puntos de Acceso).

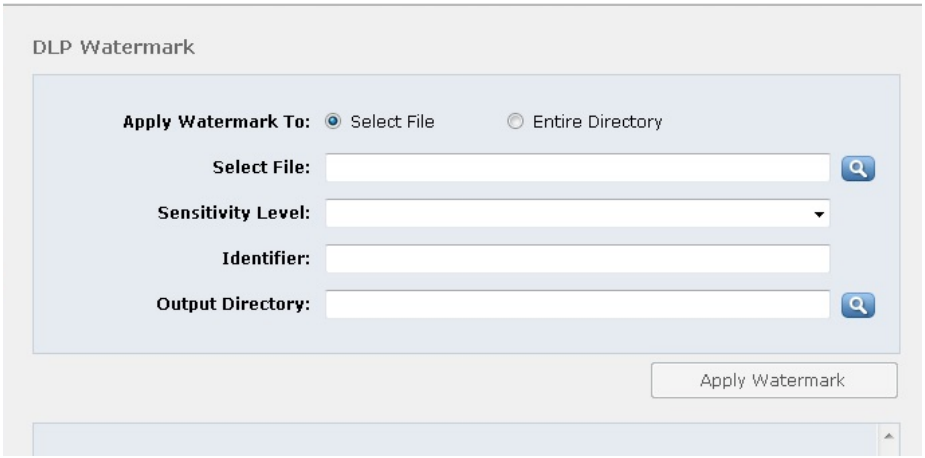
- *Log&Report*: Ver resúmenes y reportes del tráfico de la red, contenido filtrado y bloqueado.



5- **Command-line Interface:** Consola para administrar el dispositivo por línea de comando.



6- **DLP Watermark:** Añadir y editar un archivo que se visualizara como contenido en marca de agua.



2.15 GUIA 2

CONFIGURACION BASICA A TRAVES DEL SET-UP WIZARD DEL FORTIEXPLORER

Guía de configuración básica a través del set-up Wizard del FortiExplorer.

El asistente de configuración FortiExplorer ayuda a configurar el FortiGate de manera básica. Cuando seleccione el asistente de configuración, cada paso de la configuración básica son claramente establecidos y si es necesario volver a un paso anterior, se encuentra la opción de regresar.

El asistente de configuración le ayudará a configurar:

• una contraseña de administrador

• Zona de tiempo

• WAN y configuración de LAN

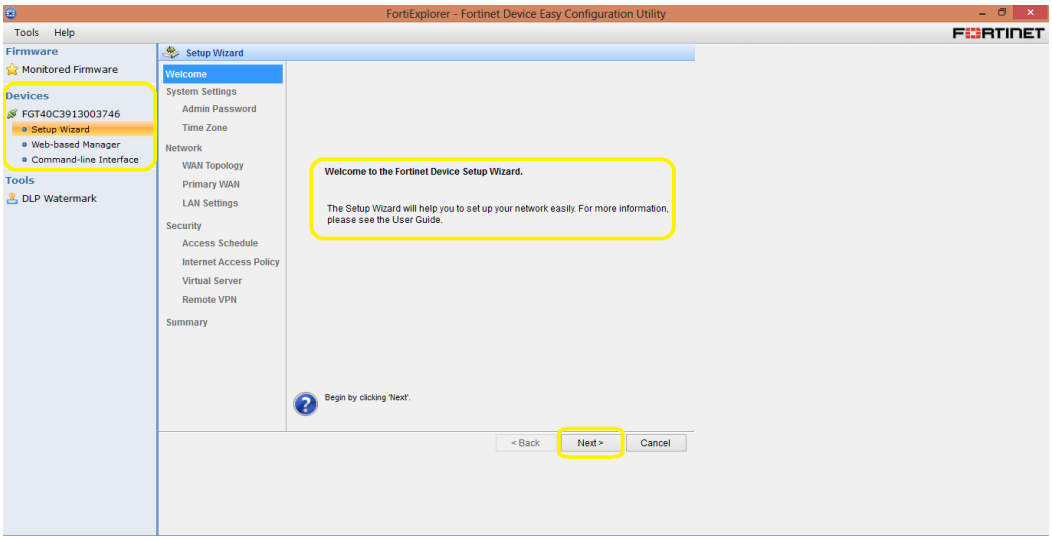
• Acceso a Internet

• un programa de acceso

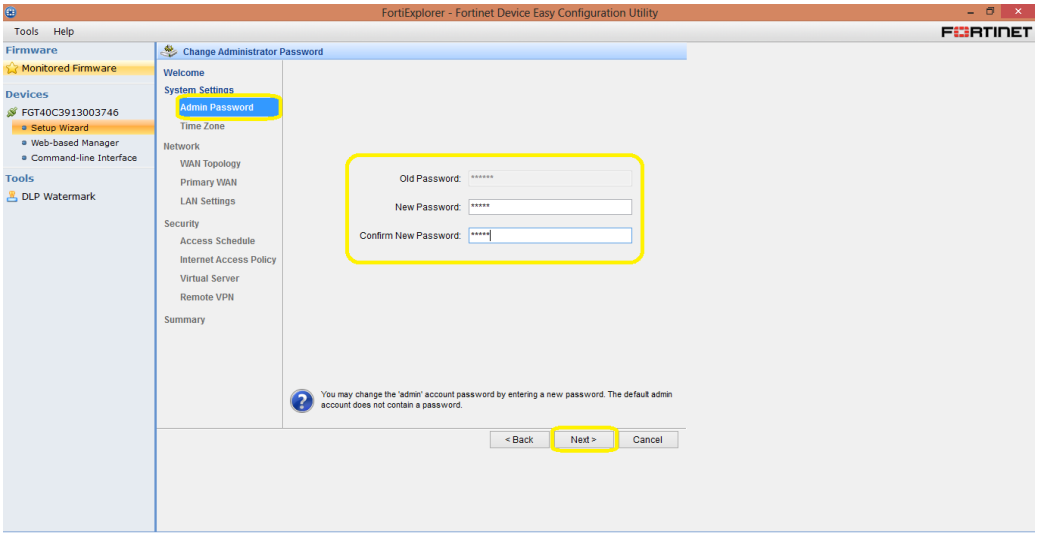
• un servidor virtual o VPN remoto

Una vez completados todos los pasos, puede revisar los nuevos ajustes del dispositivo en la página de resumen. La página de resumen le ayuda a verificar la configuración para asegurarse de que todo es correcto antes de actualizar el dispositivo con la nueva configuración.

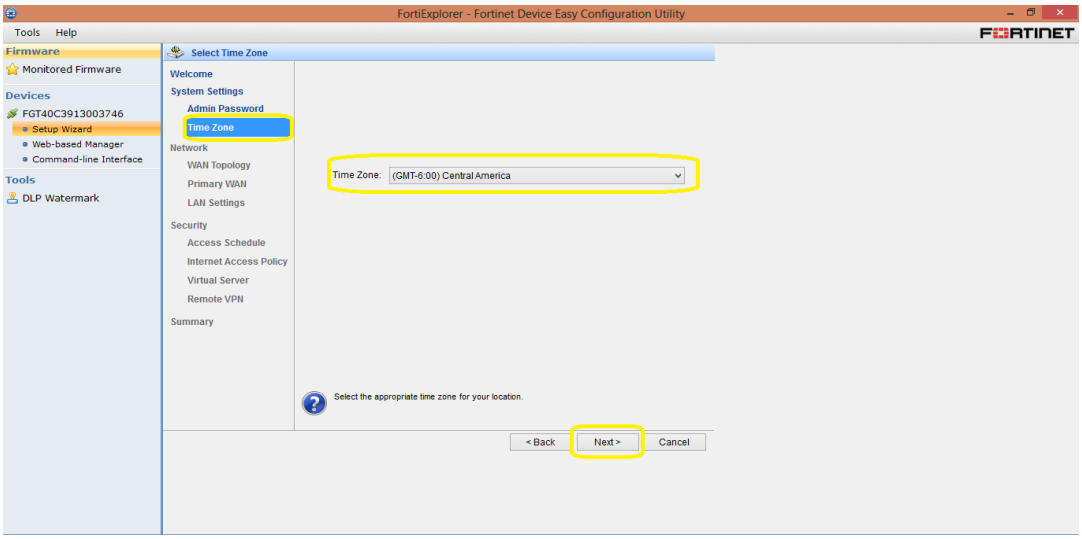
1. Para iniciar el asistente de configuración nos ubicaremos en el menú de la izquierda y daremos clic en la opción de “set-up wizard” en la sección de “devices” nos mostrara una breve descripción de lo que se va a realizar. Luego damos clic en “next”.



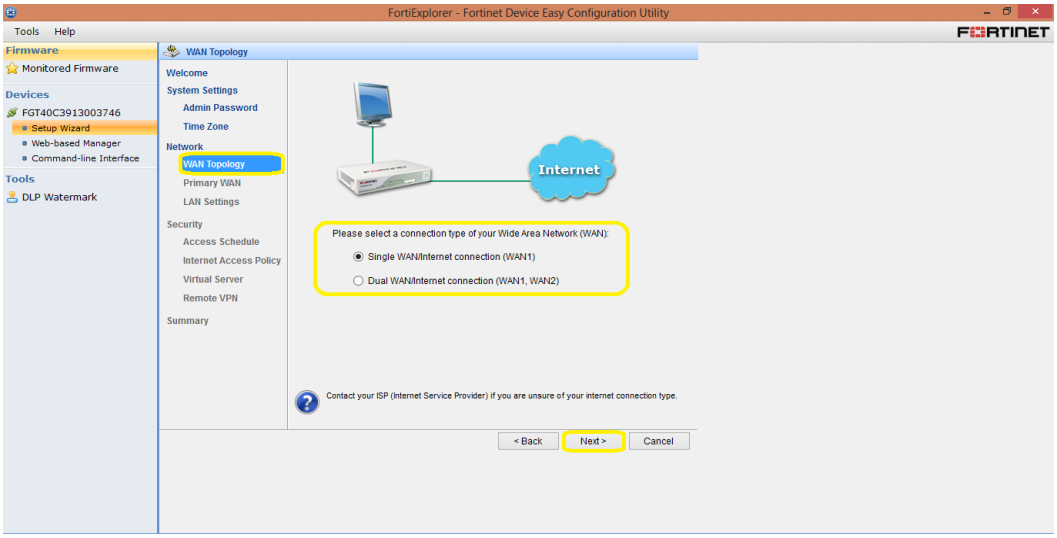
2. En esta sección cambiaremos la contraseña de administrador y luego pasamos al siguiente paso haciendo clic izquierdo en “next”.



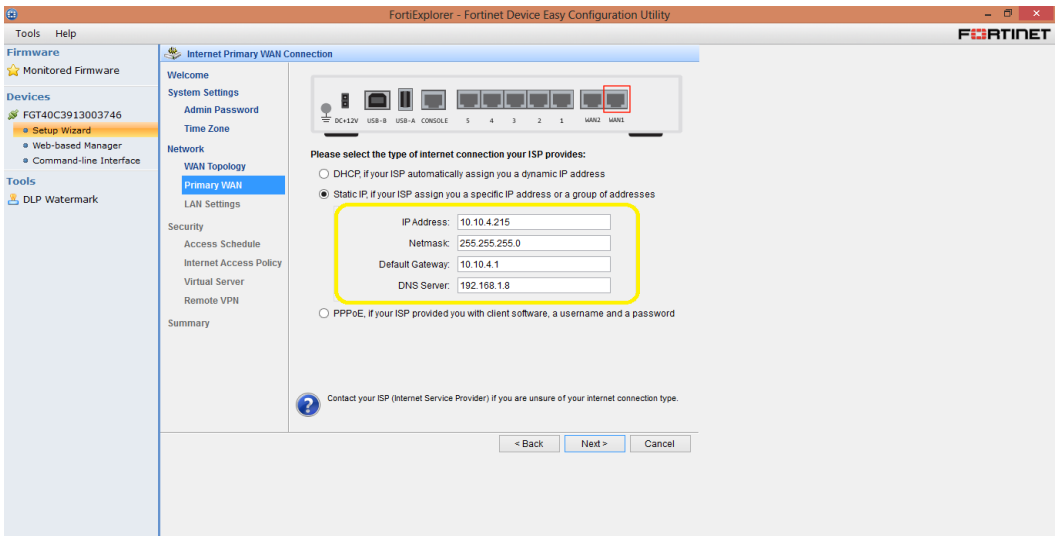
3. Acá configuraremos la zona horaria de nuestra región y damos clic izquierdo en “next” para pasar al siguiente paso.



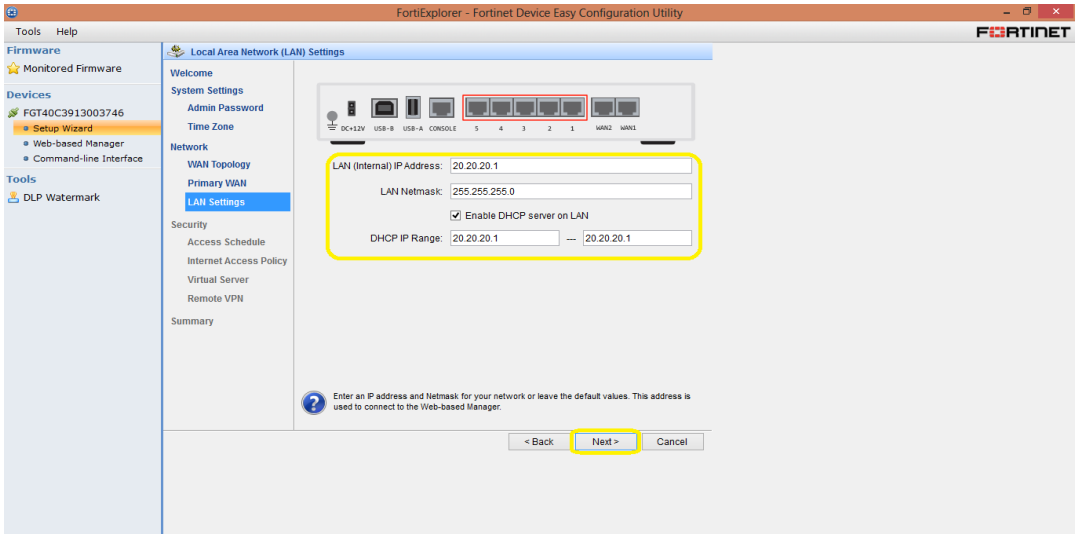
4. En este paso seleccionamos la topología con la que trabajaremos. Y daremos clic en “next”.



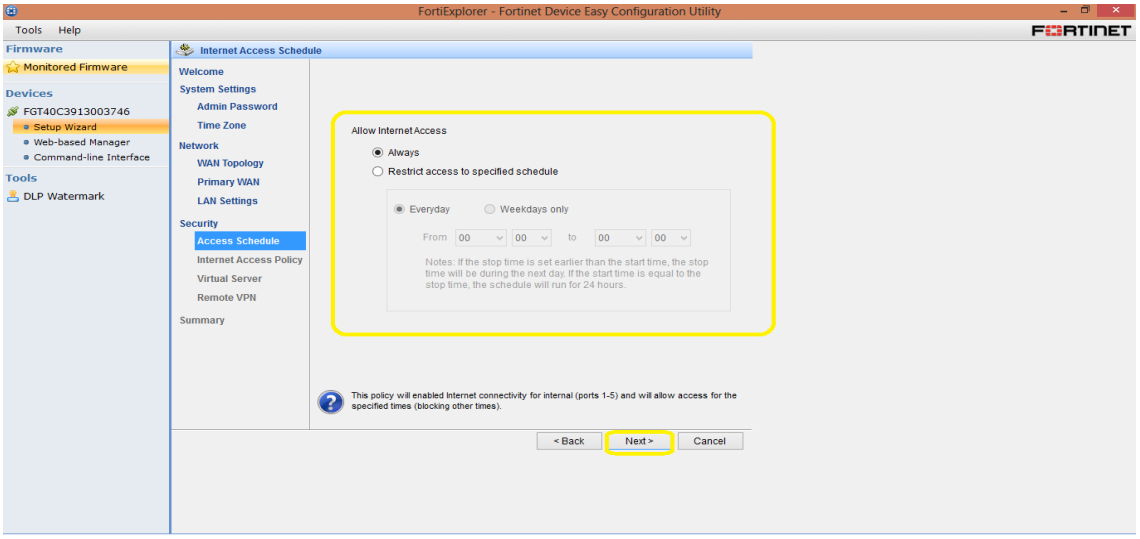
5. Configuramos nuestra WAN con los detalles proveídos por nuestro ISP en caso de ser IP estática o seleccionamos dinámica en caso contrario.



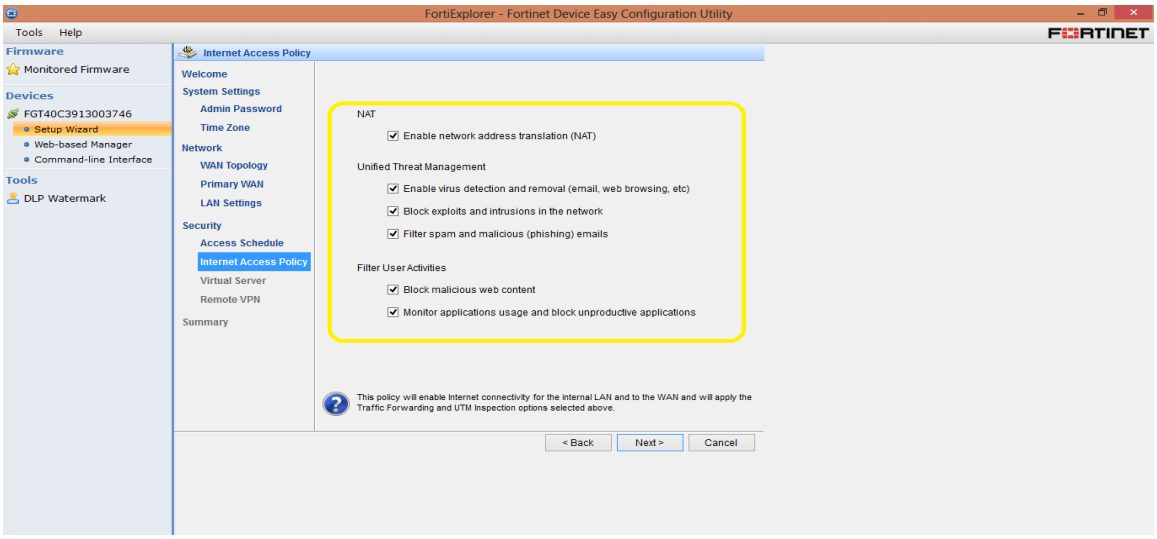
6. Configuramos la LAN con los parámetros de red que trabajaremos.



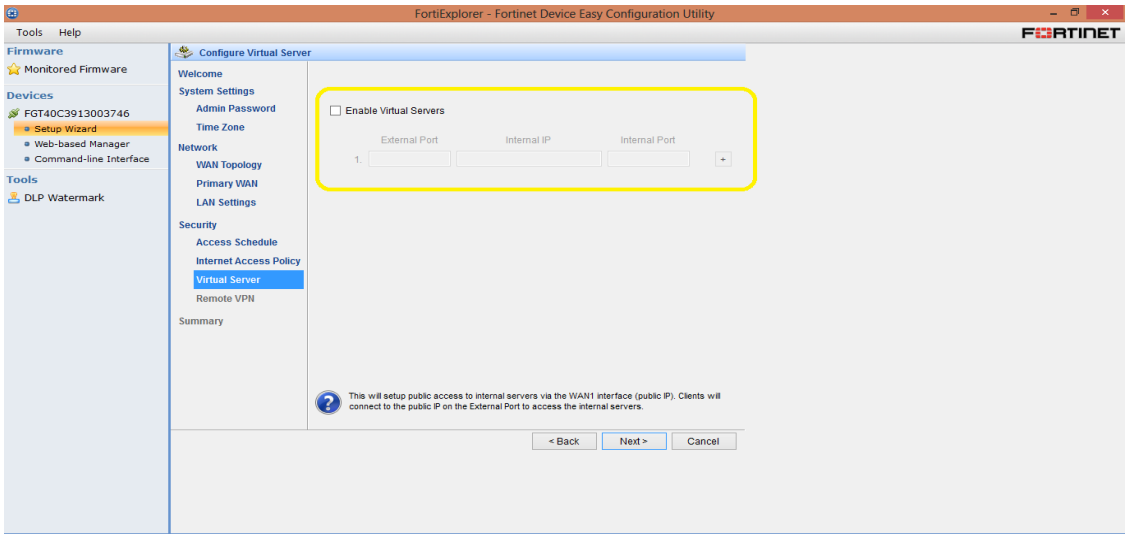
7. Configuramos el horario de acceso a internet o lo dejamos habilitado siempre.



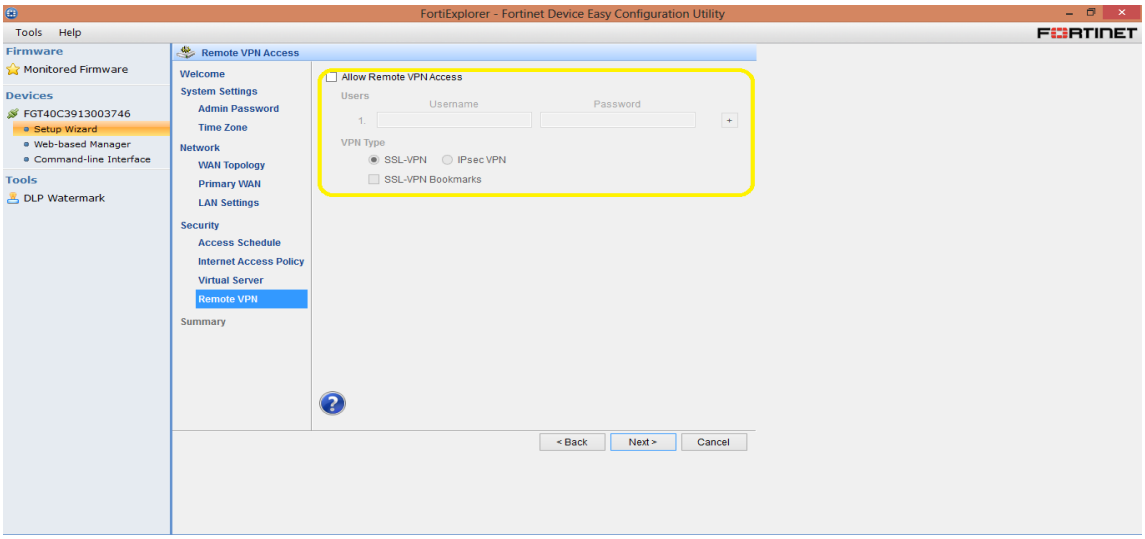
8. Seleccionamos las políticas que creamos necesarias para la conectividad de la LAN interna y de la WAN.



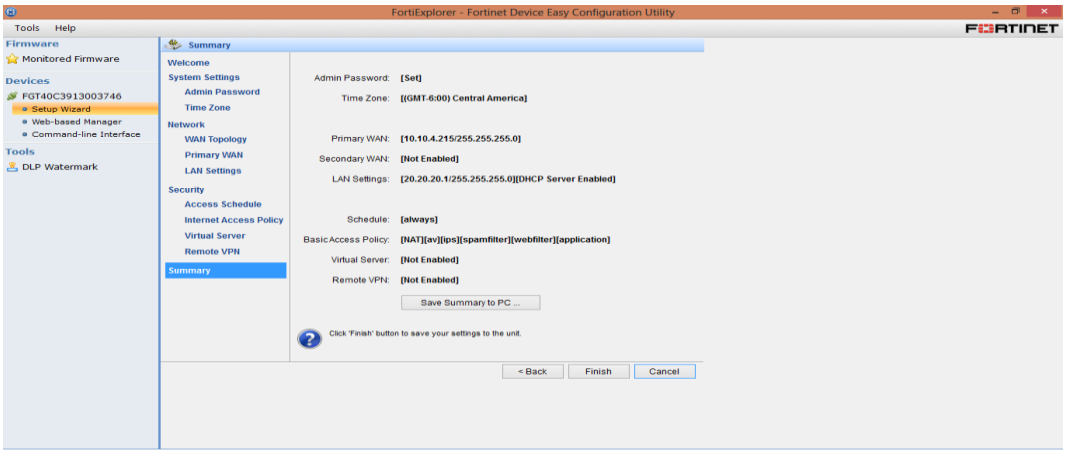
9. Agregamos servidores virtuales en caso de poseerlos para que puedan acceder a ellos desde un IP pública o puertos externos.



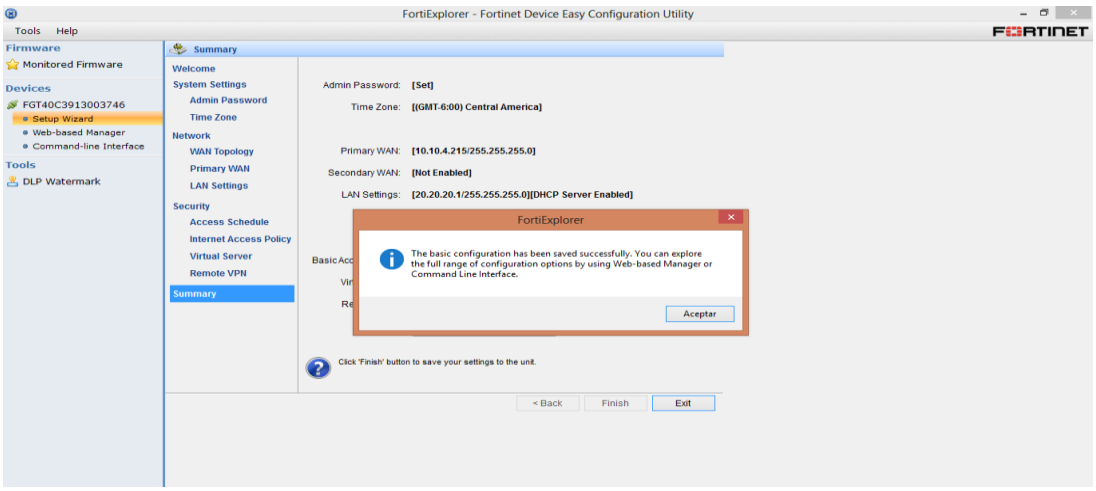
10. En esta sección configuraremos la VPN en caso sea que sea necesaria.



11. Una vez completados todos los pasos anteriores, puede revisar los nuevos ajustes del dispositivo en la página de resumen. La página de resumen le ayuda a verificar la configuración para asegurarse de que todo es correcto antes de actualizar el dispositivo con la nueva configuración. Damos clic en “finish” para cargar la configuración en nuestro dispositivo.



12. Esperamos a que finalice el proceso de actualización y que muestre el mensaje de confirmación que el procedimiento se ha realizado con éxito y ya tendremos nuestro equipo listo y con una configuración básica realizada.



2.16 GUIA 3

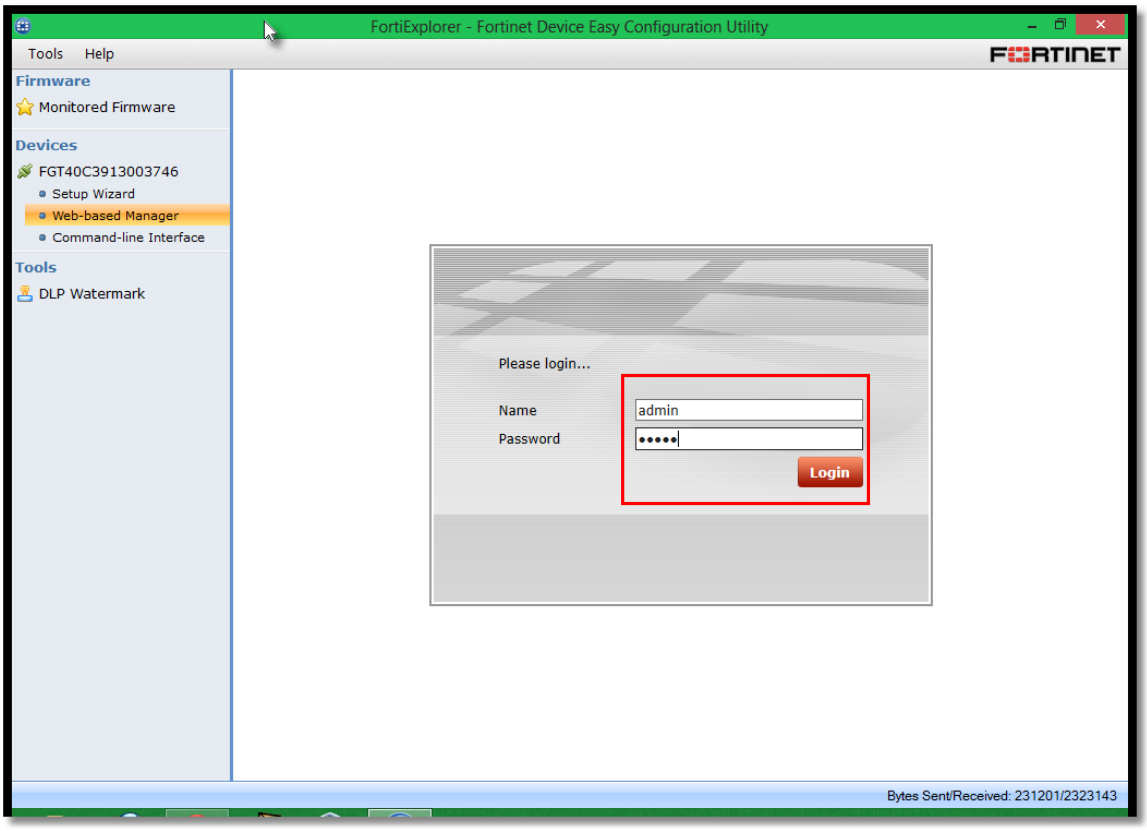
BLOQUEO DE EXTENCIONES

Contenido: Bloqueo de extensiones por medio de FortiExplorer.

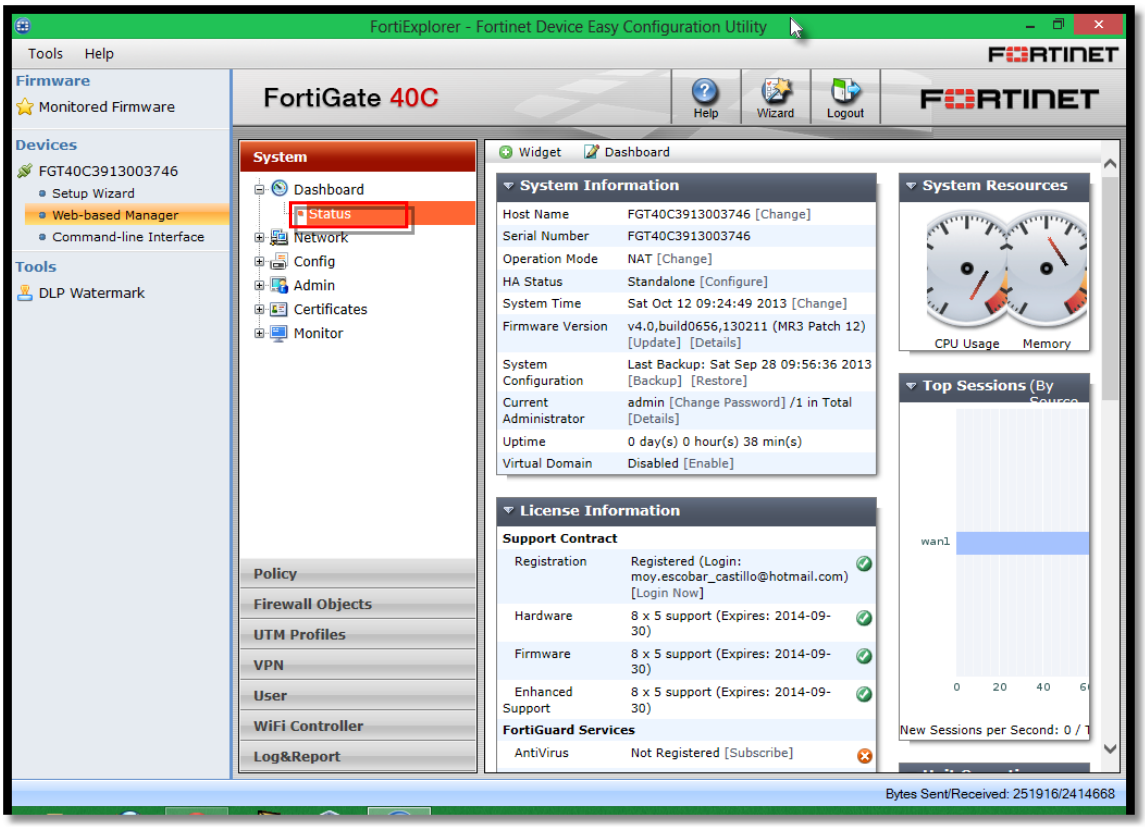
Objetivo: Establecer normas de seguridad a través del bloqueo de extensiones en una red.

Una de las funciones principales de un firewall es establecer límites a los usuarios, otorgar y limitar accesos a determinadas acciones.

1. Iniciamos FortiExplorer y presionaremos la opción *web-based* manager segundo pedirá la contraseña y el usuario que hemos configurado. Recordemos que por defecto el usuario y la contraseña es *admin.*



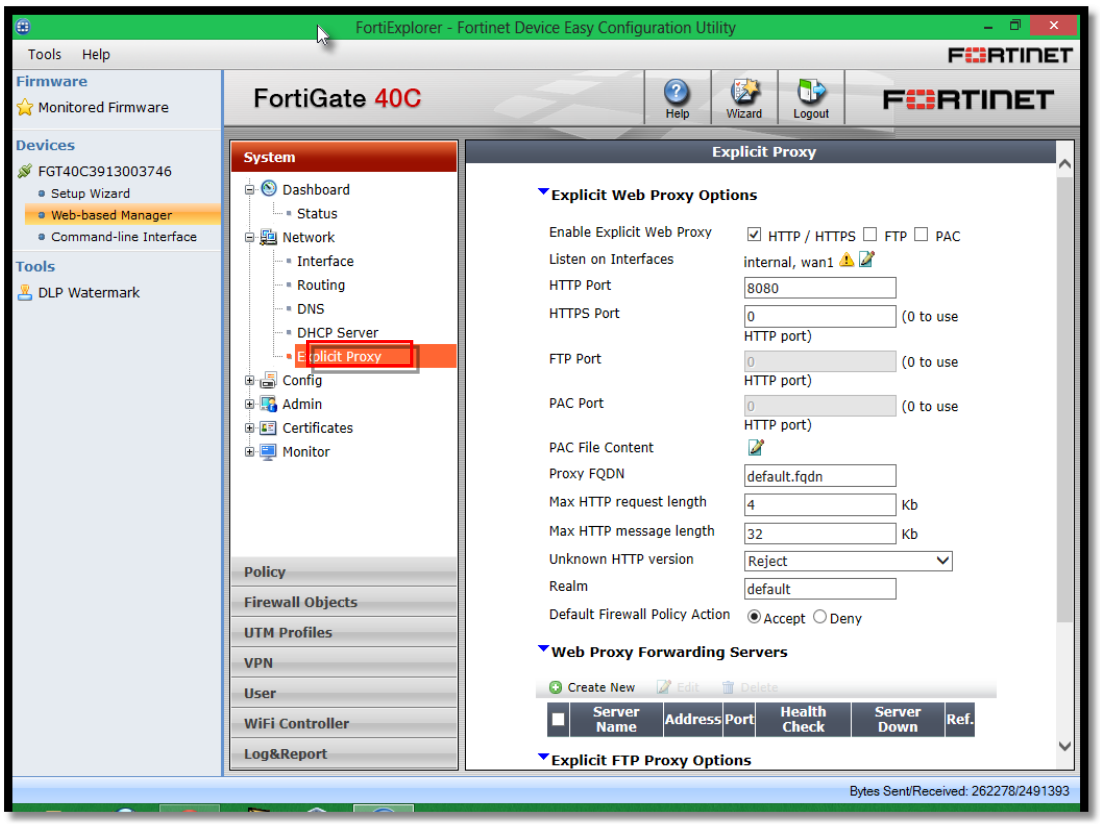
Luego de introducir los parámetros de seguridad saltara el siguiente recuadro.



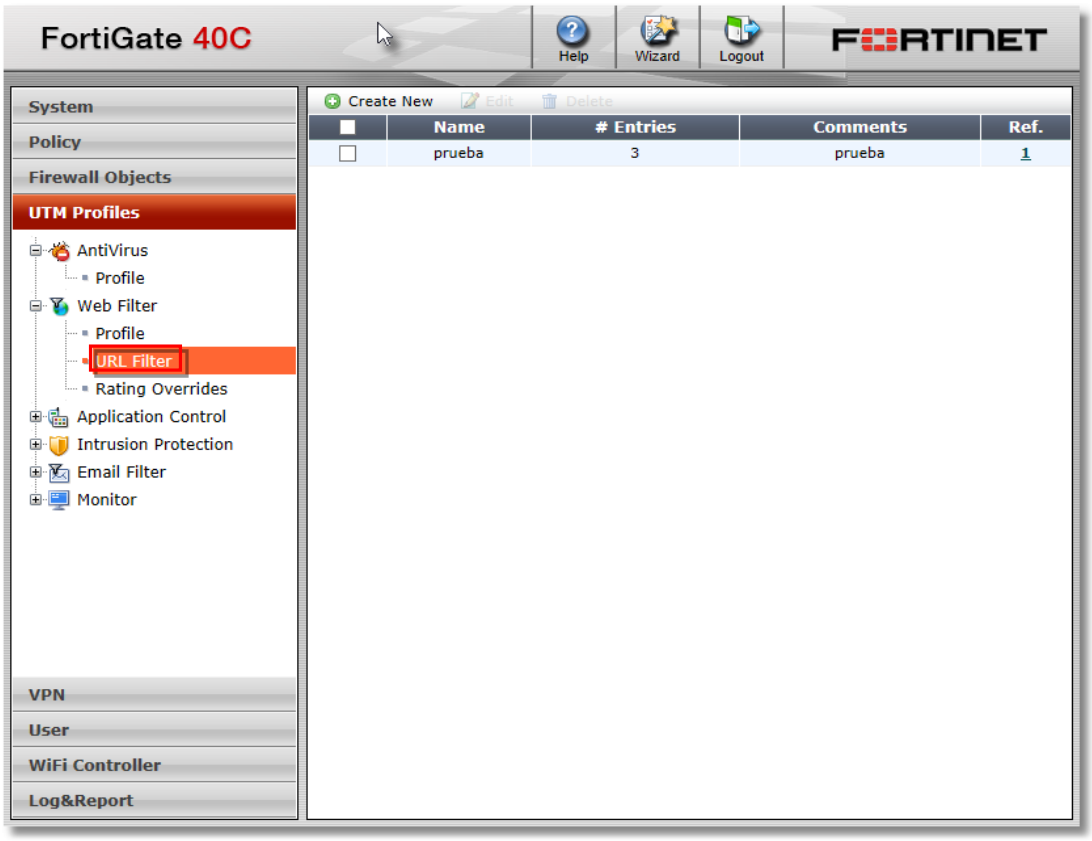
La opción *status*. Nos informa todos los recursos que tenemos, la información del sistema, los usuarios que se han conectado entre otras funciones.

2. ahora vamos a verificar la información por defecto configurada que está establecida en web proxy, esta configuración debe estar así.

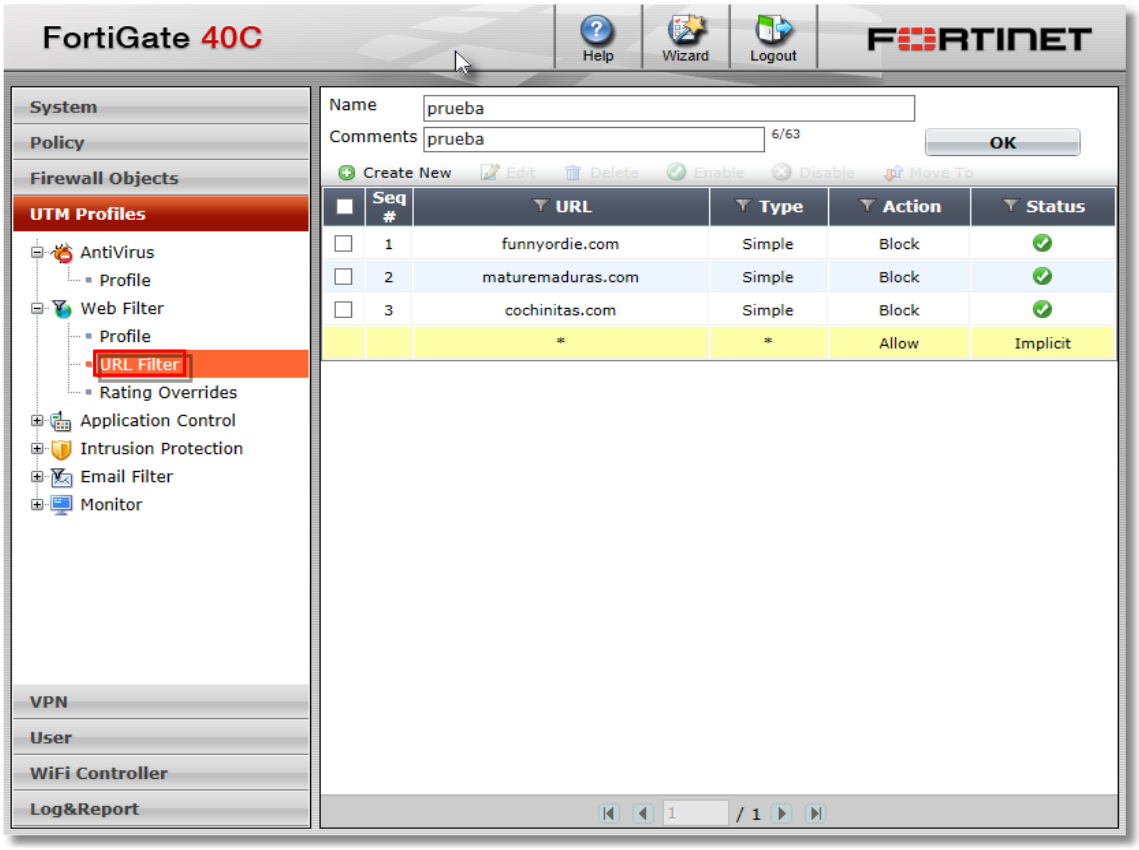
Nota: Si no está configurada de la manera que se está viendo en el siguiente recuadro debes configurarlo como se muestra.



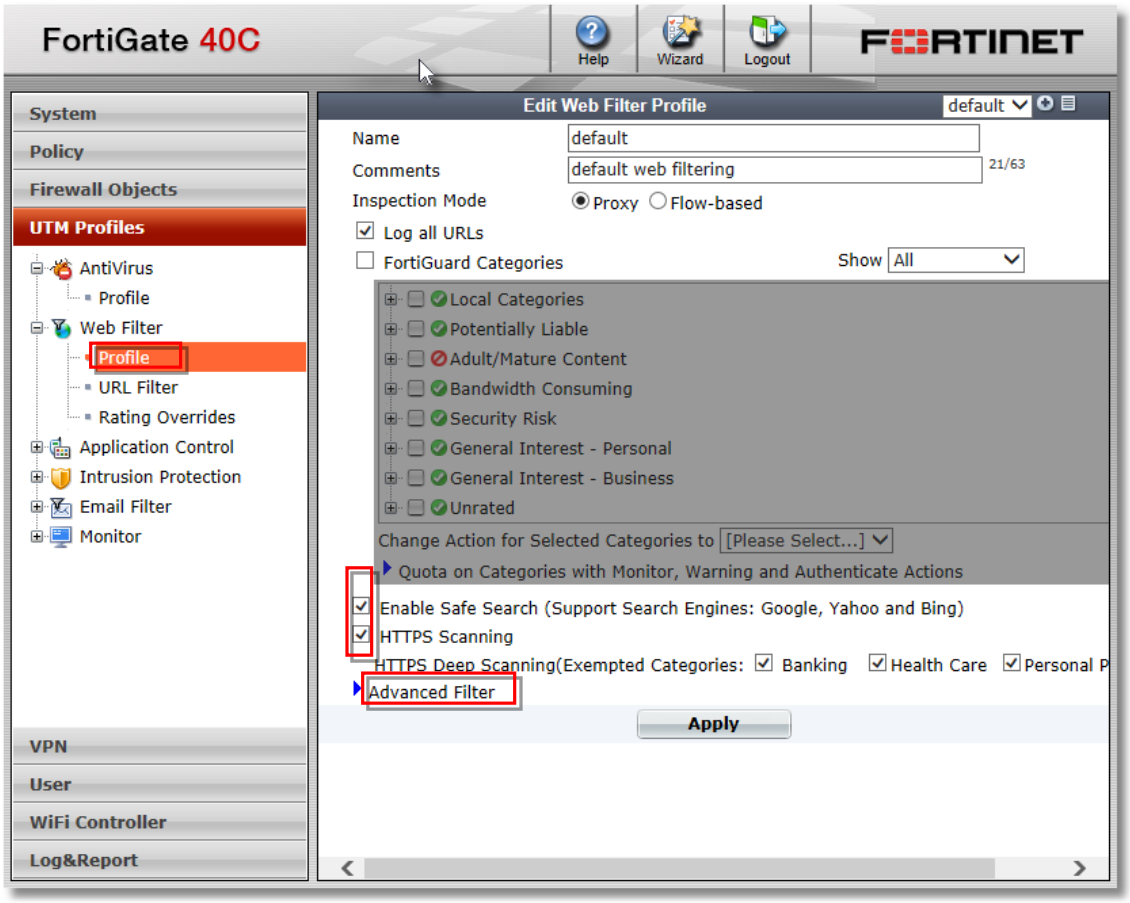
Luego de haber configurado Web Filter tendremos que crear un URL filtro presionamos la opción Create New y lo nombraremos “prueba”.



Dentro de este URL pondremos las páginas que deseamos que no sean una distracción ya sea para los usuarios o alumnos de dicho lugar. Agregaremos unas cuantas páginas no permitidas.



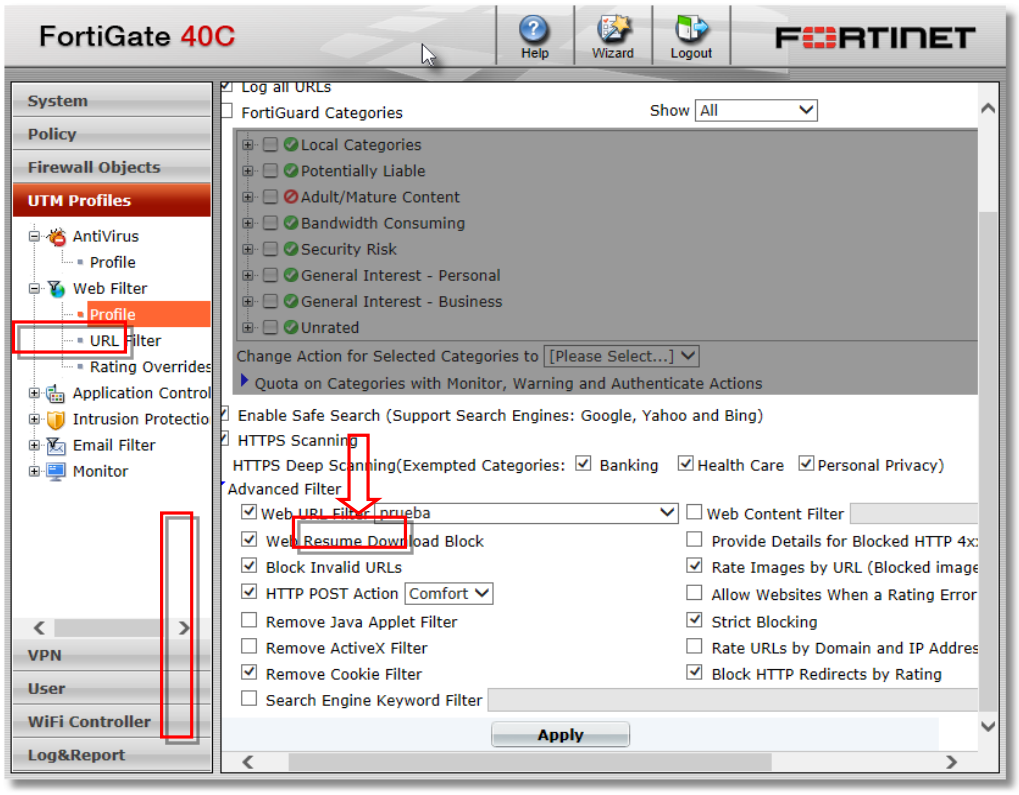
Después de haber agregado las paginas o URL que se bloquearan, comenzaremos a configurar la opción **Profile,** ahí podemos observar otras funciones que nos facilitan la administración, en ella podemos agregar filtros y clasificarlos por categorías.



Daremos clic en la opción Advanced Filtery con la cual vamos a establecer configuraciones avanzadas para el filtro que creamos anteriormente.

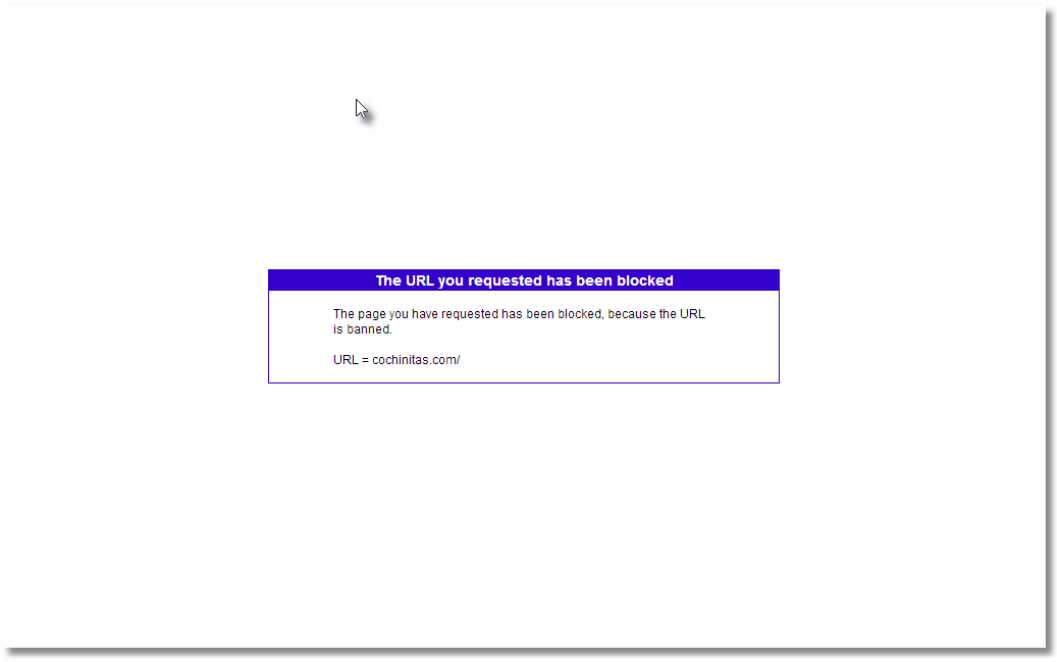
- Web URL Filter: Nos permite seleccionar el filtro que deseamos configurar.

- Web Resume Download Block: Bloquea las descargas de archivos.
- Block Invalid URL: Bloquea las URL invalidas.
- HTTP post Action: Permite seleccionar el mensaje que el usuario visualizará cuando intente acceder a una URL bloqueada.
- Remove Cookie Filter: No permite que las páginas bloqueadas almacenen cookies en el sistema.



Presionamos la opción Apply para guardar las configuraciones realizadas.

Ahora que realizamos correctamente las configuraciones pondremos en el navegador del cliente una de las direcciones que ha sido agregadas en la URL de bloqueo a continuación veremos el ejemplo.



Como se observa la página ha sido bloqueada por nuestro firewall.

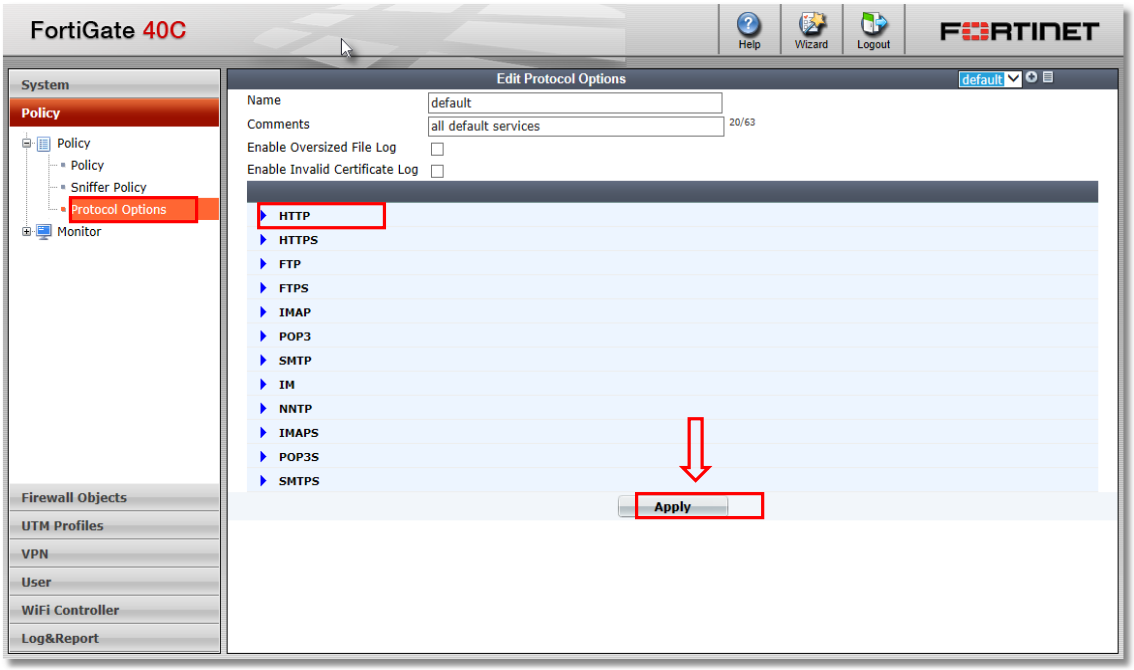
Bloqueo de extensión .exe

Una de los problemas más frecuentes en una red, es la descarga de aplicaciones que los usuarios realizan. Aplicaciones que luego utilizan para descargar contenido de internet. Esto nos trae como consecuencia la saturación en el ancho de banda, lo cual puede afectar negativamente la productividad de una empresa o centro de cómputo.

Esta guía nos explica el procedimiento a realizar para erradicar este problema.

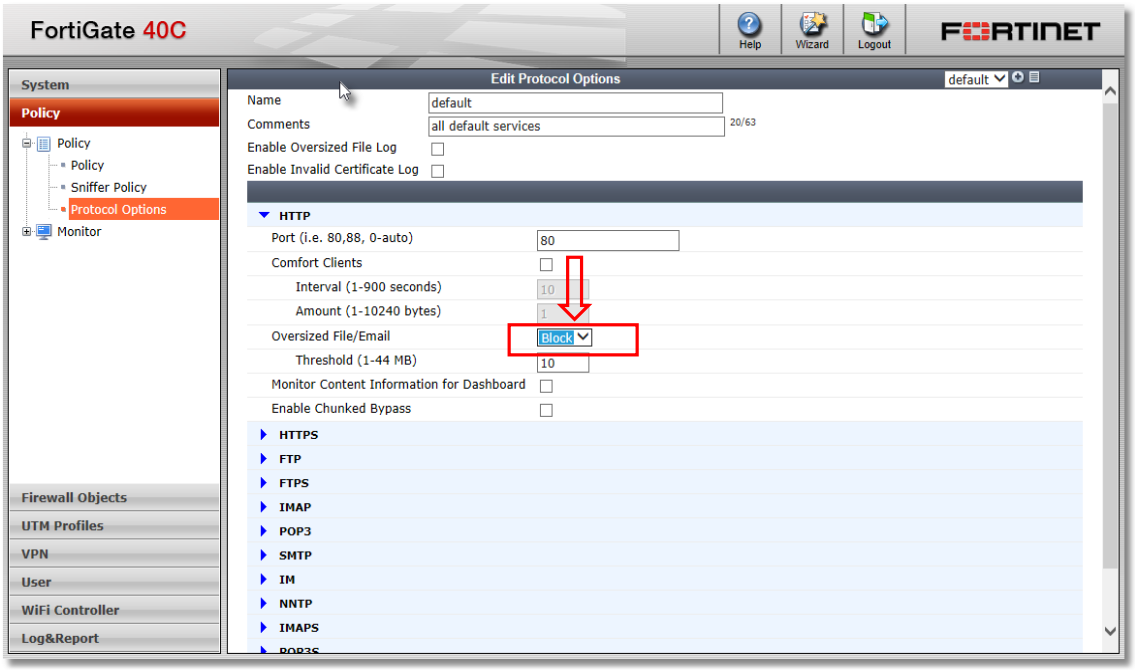
PASO 1:

Dentro de la opción Policy en el panel de Configuración, Presionaremos en Protocol Options, Aparecerá una lista de protocolos en la cual presionaremos la opción HTTP. La opción Name la dejaremos con “default”.



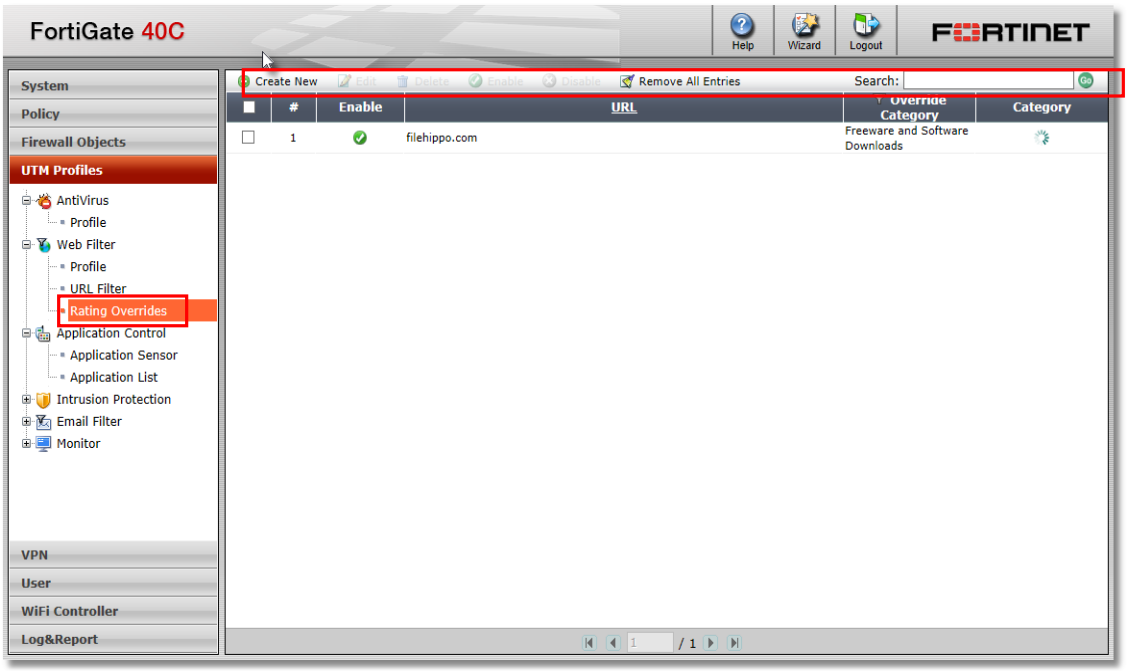
PASO 2:

Dentro de HTTP encontraremos la opción de Block y Pass en este caso necesitamos seleccionar la opción bloquear para poder bloquear extensiones.



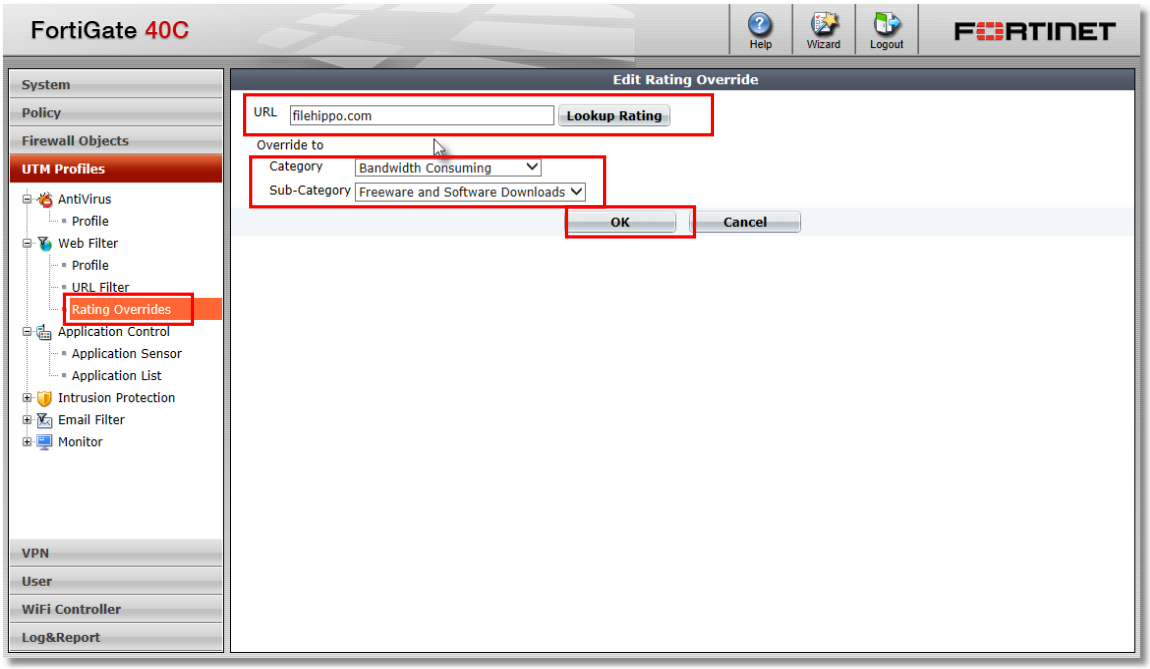
PASO 3:

Luego nos desplazaremos la categoría UTM profiles seleccionar la opción Rating Overrrides. y luego la opción Create New.



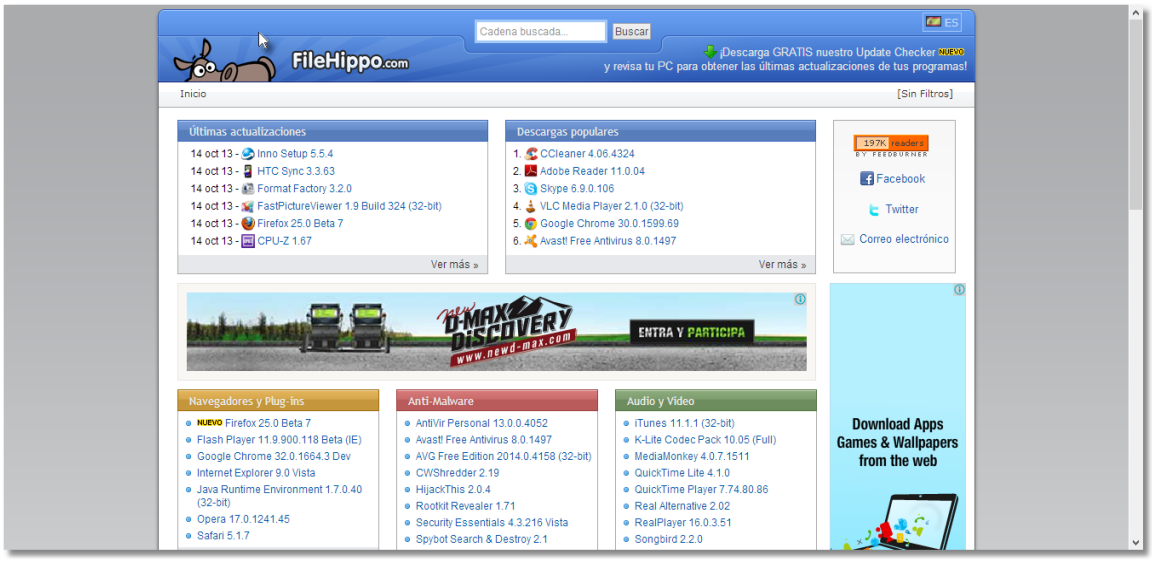
PASO 4:

Para ejemplada agregaremos la dirección filehippo.com (Web donde se descargan programas gratuitos). Ahora seleccionamos la dirección creada y presionamos la opción editar que nos aparecerá en la parte de arriba de la dirección.

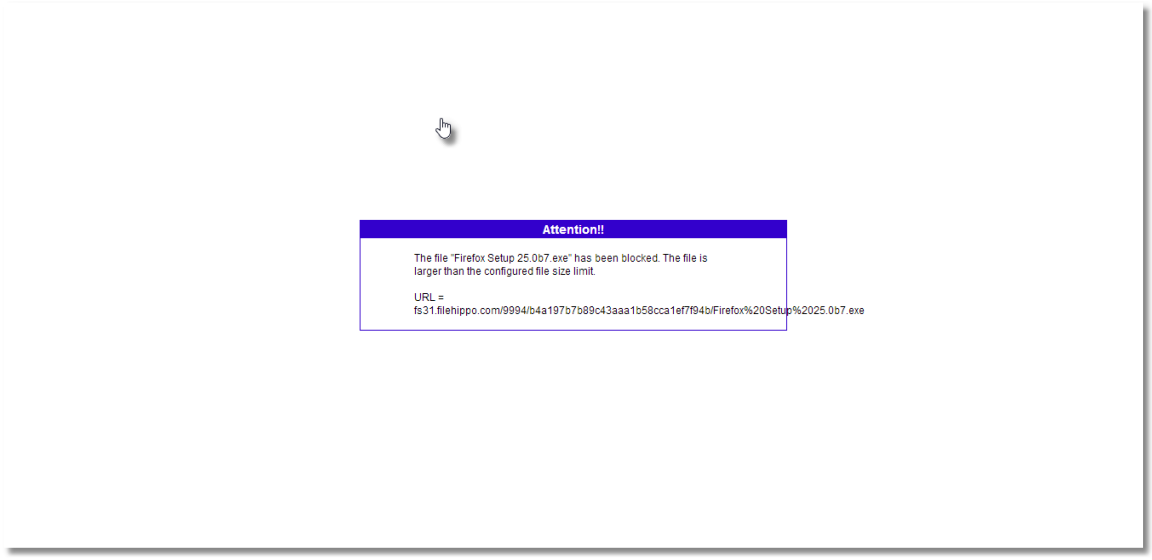


En la parte de las categorías pondremos el tipo de opción con la que lo queremos limitar y en la subcategoría decidiremos que no descargara aplicaciones.

Ahora para poder ver si es verdad que hemos hechos bien la configuración entramos a la página o la dirección.



Ahora seleccionamos uno de los programas y a continuación nos saldrá el mensaje de que ha sido bloqueada por el administrador.



2.17 GUIA 4

COMANDOS DE CONFIGURACION BASICOS POR MEDIO DE CLI

Comandos de configuración básicos por medio de CLI

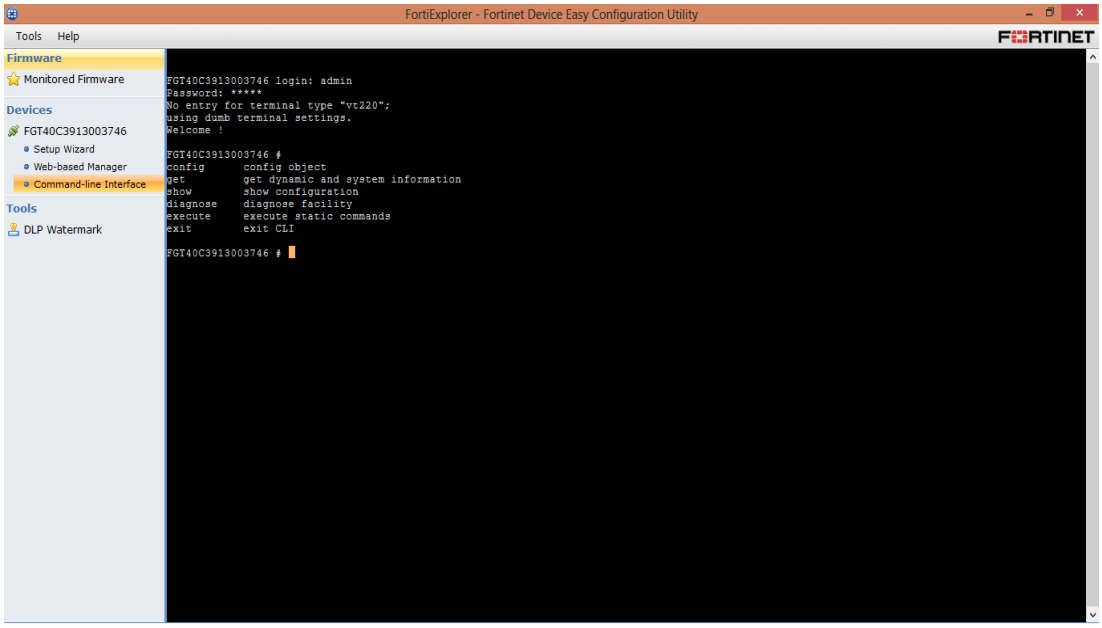
Existen diferentes tipos de conexión, para configurar el Firewall Fortinet FortiGate 40C por medio de la línea de comandos (CLI). Se puede conectar a través de Telnet o SSH desde cualquier red a la que esté conectado el equipo.

La forma más sencilla, es utilizando el cable de consola, el cual se conecta directamente desde el equipo a un ordenador a través del puerto RJ45 que ha sido asignado por el fabricante para dicha conexión.

Su funcionamiento es de una forma simple, la CLI muestra un prompt donde el administrador se logea por medio del usuario y contraseña, estos parámetros han sido previamente configurados.

Una vez obtenido el acceso a la CLI, se procede a digitar las órdenes utilizando los comandos específicos para cada configuración.

Cuadro1. Accediendo a la CLI con el usuario y contraseña de administrador.



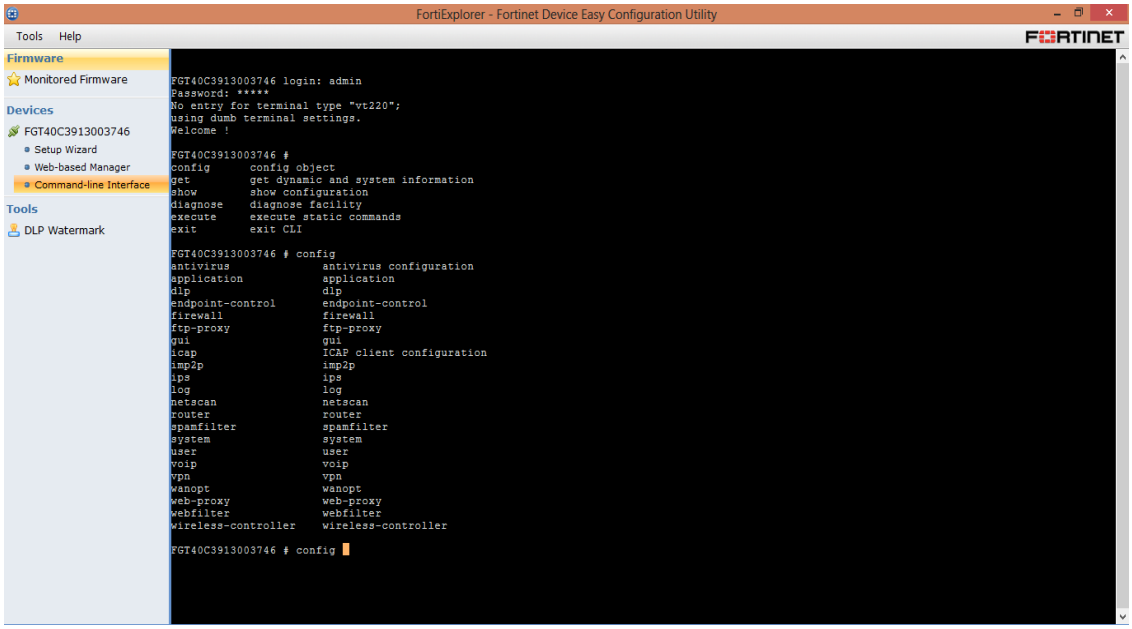
Al hablar de comandos hablamos de una serie de instrucciones proporcionadas por el usuario u administrador para interactuar con él en su mismo idioma, el cual generalmente está contenido en un archivo ejecutable.

Una de las facilidades que contienen las diferentes CLI, son los comandos de ayuda que nos permiten conocer que órdenes o comandos pueden ser ejecutados según la configuración que valla a realizarse.

En el modo de configuración global de la CLI se digita el signo de interrogación (?) al ser digitada esta orden automáticamente el resultado muestra los comandos que se pueden ejecutar en la rama de configuración actual.

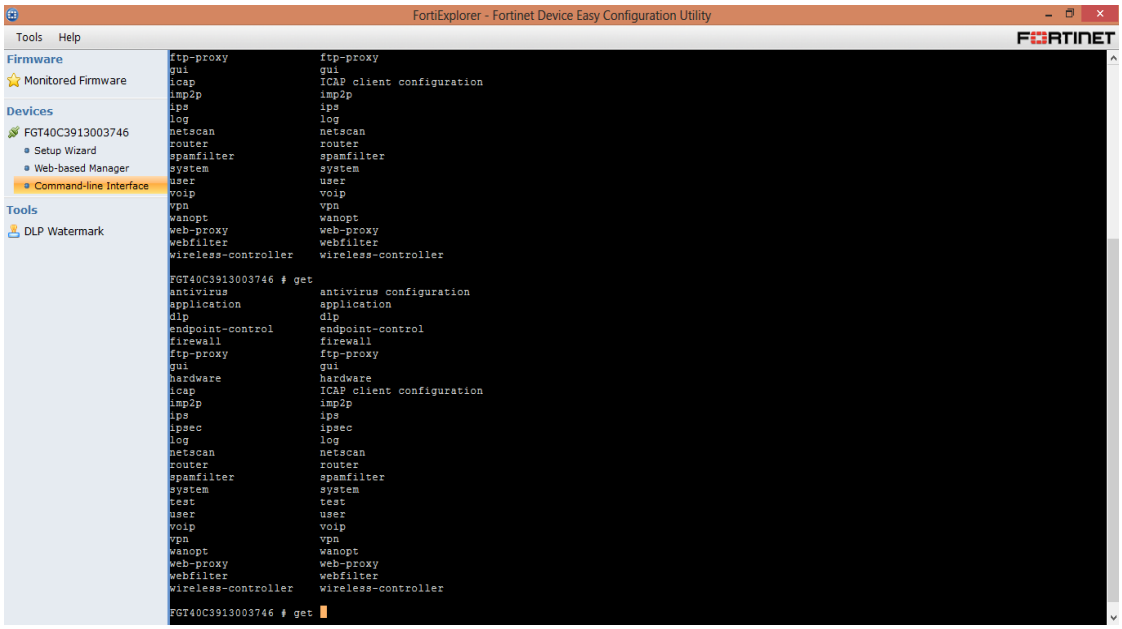
Cada una de las órdenes mostradas en la lista, nos permite realizar diferentes tareas, como la configuración del Wireless por medio del comando config.

Cuadro2. Ejecución del comando ayuda.



Con el comando config tenemos una larga lista de opciones que podemos utilizar para configurar el FortiGate, por ejemplo se puede configurar un WebFilter con el cual se puede denegar el acceso a ciertos sitios Web.

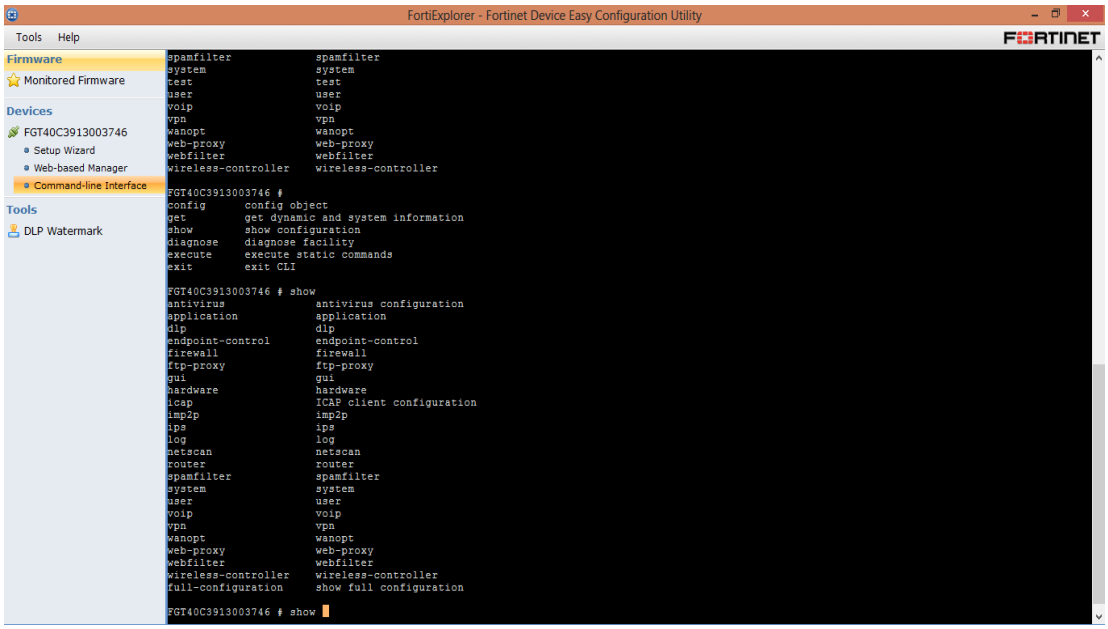
Cuadro3. Listado de ordenes utilizables por medio del comando config.



Todas las configuraciones realizadas mediante el CLI, son almacenadas en el HD del equipo. Pero ¿Cómo podemos ver, esas configuraciones almacenadas? Simple, con el comando show.

Se utiliza la opción de ayuda para el comando show, de igual forma con las ordenes anteriores se obtendrá un listado con las opciones que podemos ver mediante este comando.

Cuadro4. Listado de ordenes utilizables mediante el comando show



Los comandos de información permiten mostrar la información relativa al router. Todos comienzan con el prefijo show.

Por ejemplo, si queremos visualizar la configuración de antivirus utilizando la siguiente línea de comandos # show antivirus configuración.

Este comando es bastante útil, si el equipo muestra alguna falla en alguna de las ramas de configuración, siguiendo el caso del ejemplo, si en la red se obtienen problemas de virus se puede visualizar la configuración de Antivirus del equipo.

Otro de los comandos que podemos utilizar es el execute que permite entre otras opciones realizar una conexión a través de telnet o un Ping para verificar la conexión dentro de la red.

Imagen6. Comando execute

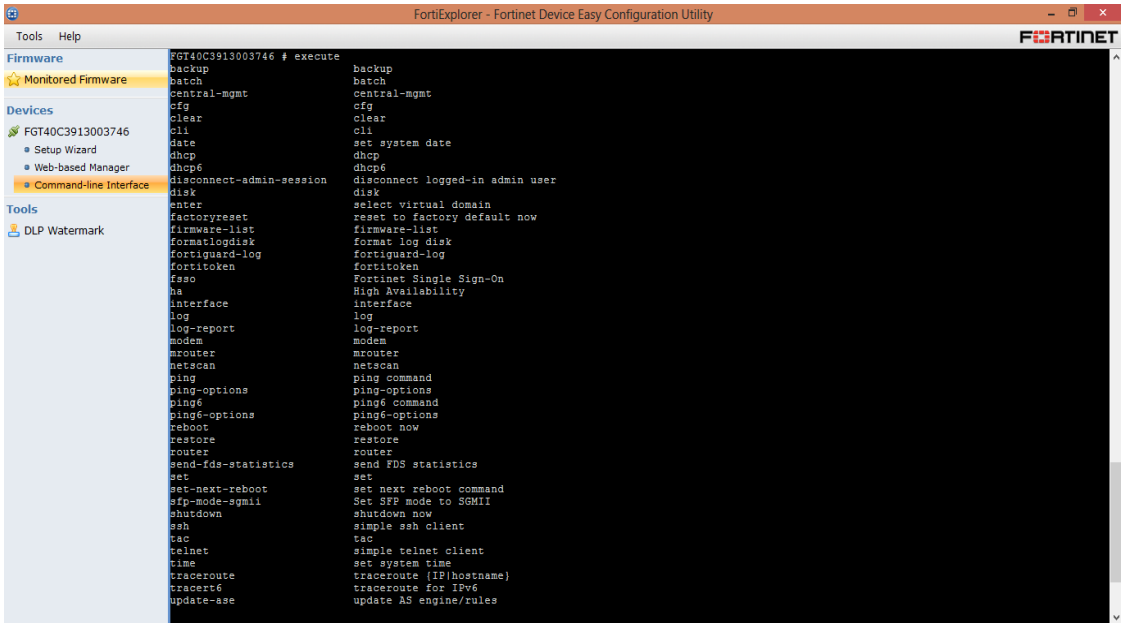
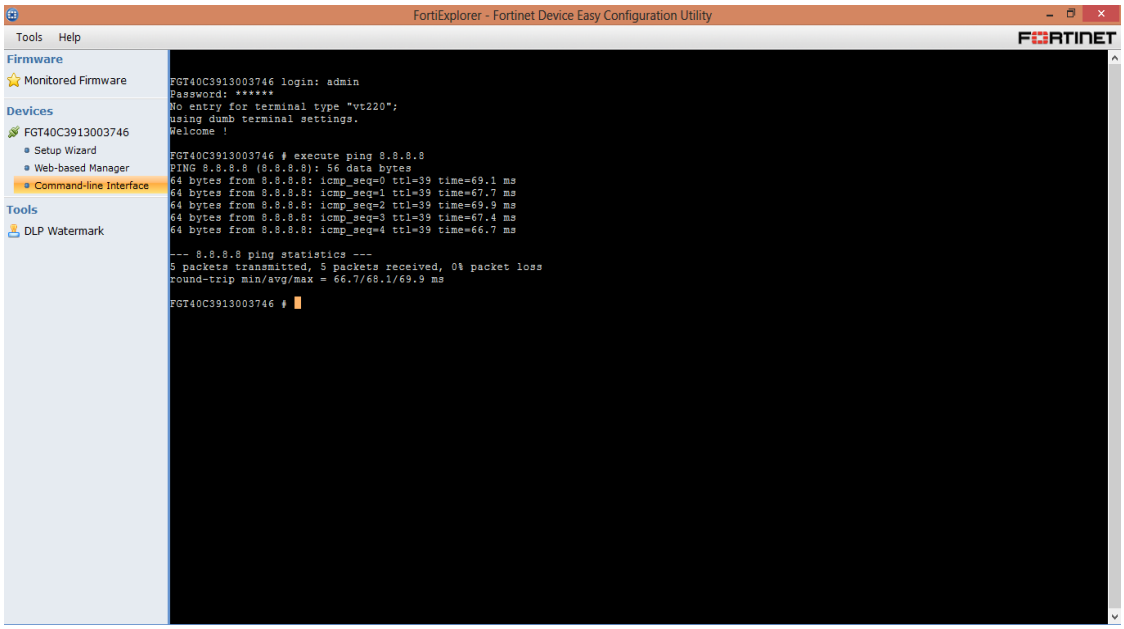


Imagen7. Ejecutando el comando ping



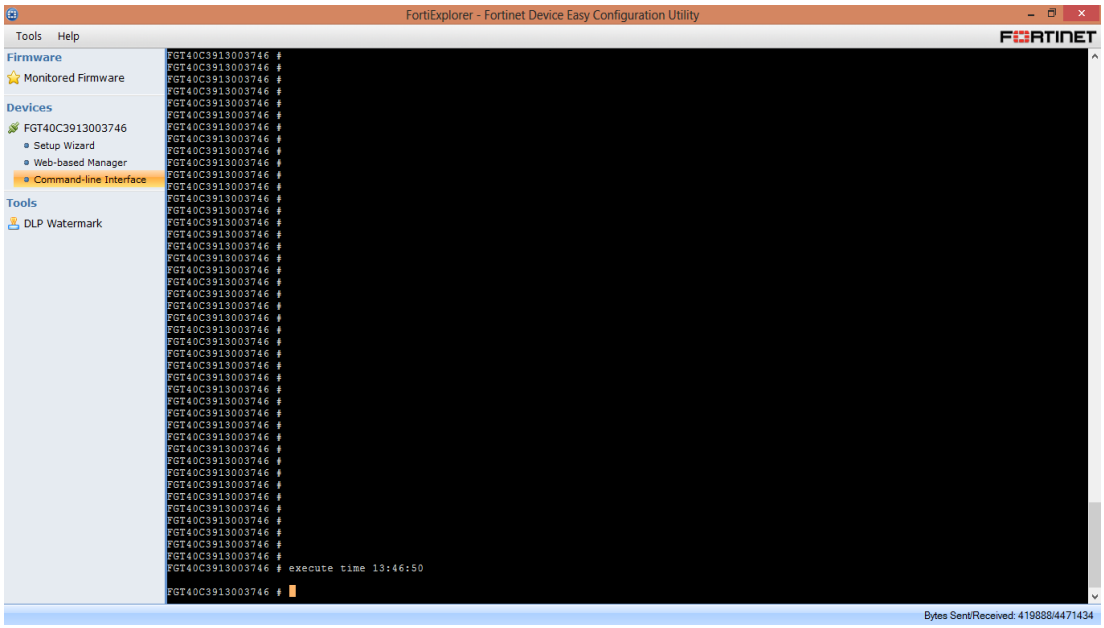
Una configuración simple pero muy importante que se puede realizar con el comando execute es la configuración de la hora y la fecha.

Utilizamos la siguiente línea de comandos:

execute time 13:46:50

execute date 2013-09-28

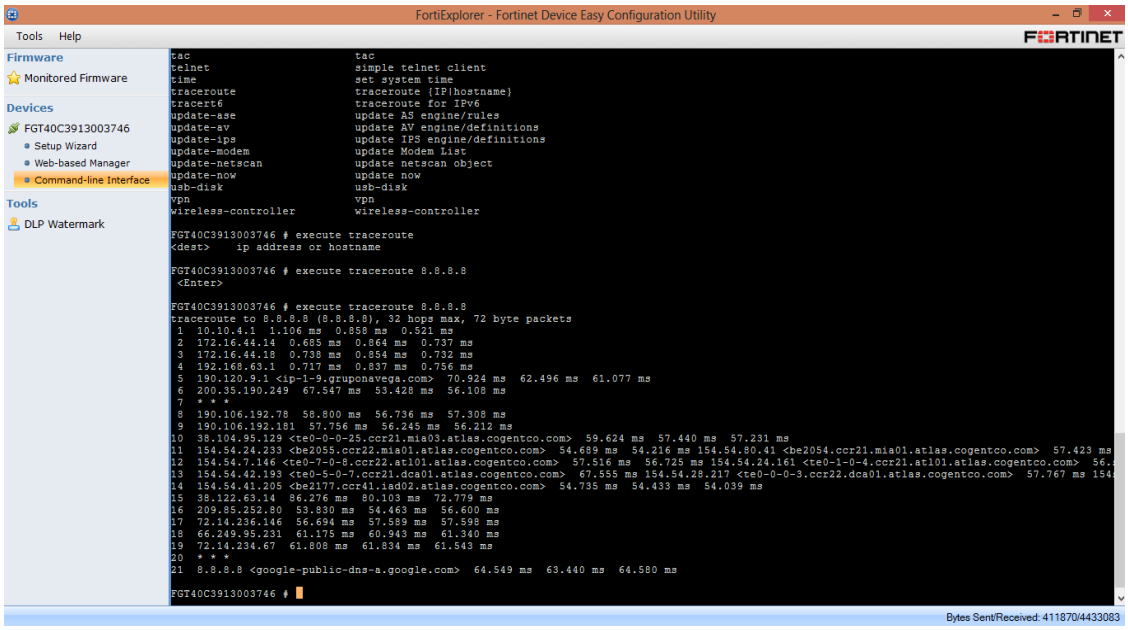
Imagen8. Configuración de hora.



Un comando que permite seguir la pista de los paquetes que vienen desde un host (punto de red) es el TracerRoute el cual obtiene además una estadística de la latencia de red de esos paquetes, lo que viene a ser una estimación de la distancia a la que están los extremos de la comunicación.

Línea de comandos para utilizar el tracerroute: # execute tracerroute 8.8.8.8

Imagen9. Utilización del comando tracerroute



Esta interfaz (CLI) existe casi desde los comienzos de la computación, superada en antigüedad solo por las tarjetas perforadas y mecanismos similares. Existen, para diversos programas y sistemas operativos, para diversos hardware, y con diferente funcionalidad.

Por ejemplo, las CLI son parte fundamental de los Shells o Emuladores de Terminal. Aparecen en todos los desktops (Gnome, KDE, Windows) como un método para ejecutar aplicaciones rápidamente. Aparecen como interfaz de lenguajes interpretados tales como Java, Python, Ruby o Perl. También se utilizan en aplicaciones cliente-servidor, en DBs (Postgres, MySQL, Oracle), en clientes FTP, etc. Las CLI son un elemento fundamental de aplicaciones de ingeniería tan importantes como Matlab y Autocad.

2.18 GUIA 5

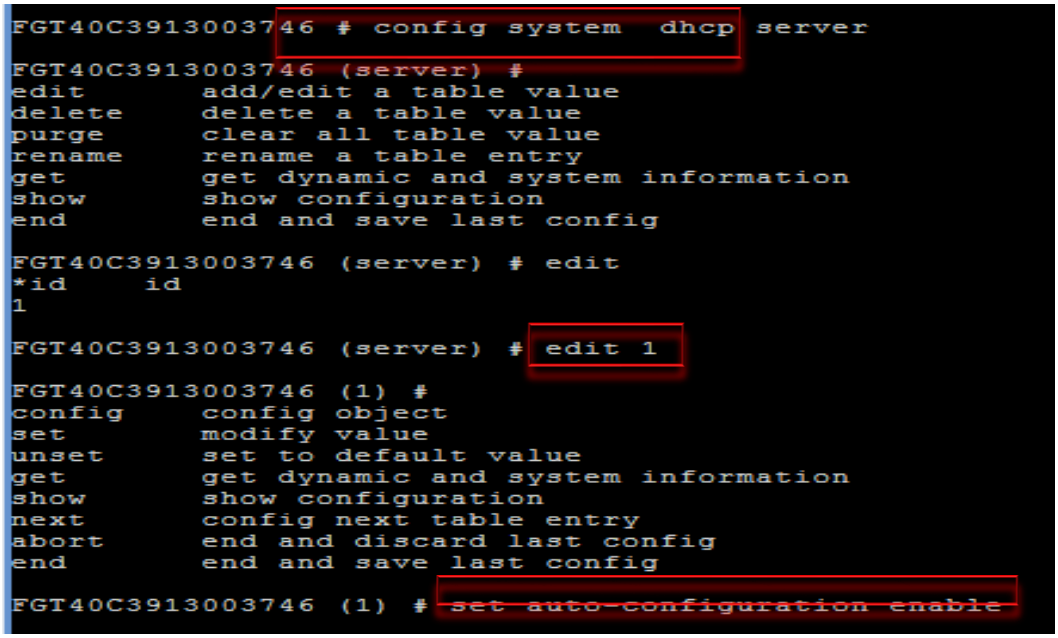
CREACION DE DHCP

Contenido: Configuración de DHCP a través del CLI en FORTINET.

Objetivo: Configurar DHCP por línea de comandos.

1. Primero tendremos verificar si DHCP esta configurado atraves del comando **config system dhcp server**

   En este caso el DHCP no esta configurado para ello tendremos que poner el comando **edit 1** para poder configurar .



2. Es importante configurar el tiempo para evitar conflictos de IP. Para ello realizamos la siguientes configuraciones:

```
FGT40C3913003746 (1) # set conflicted-ip-timeout 60
 <Enter>

FGT40C3913003746 (1) # set conflicted-ip-timeout 100

FGT40C3913003746 (1) # set default-gateway 10.10.10.1
```

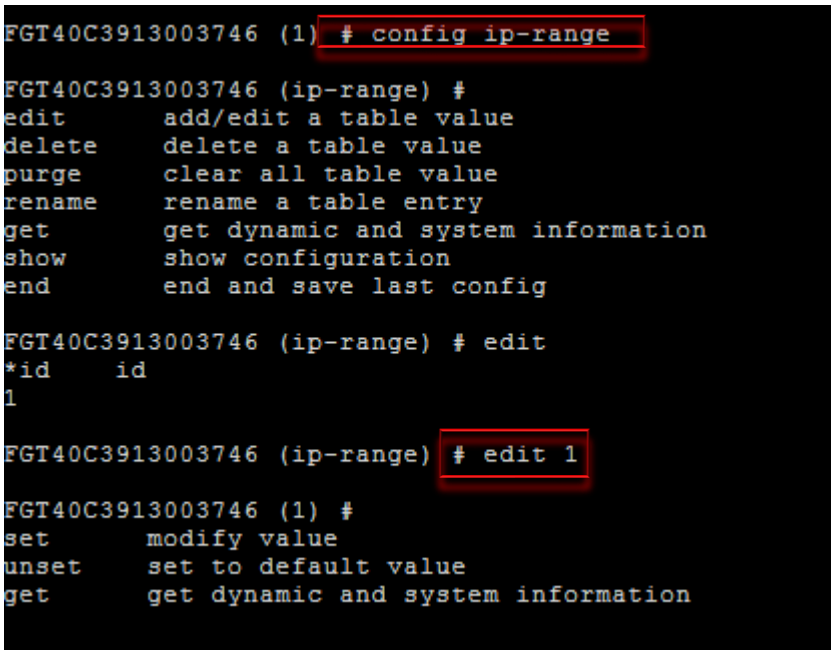
3. En este paso determina la interface por cual distribuirá el DHCP

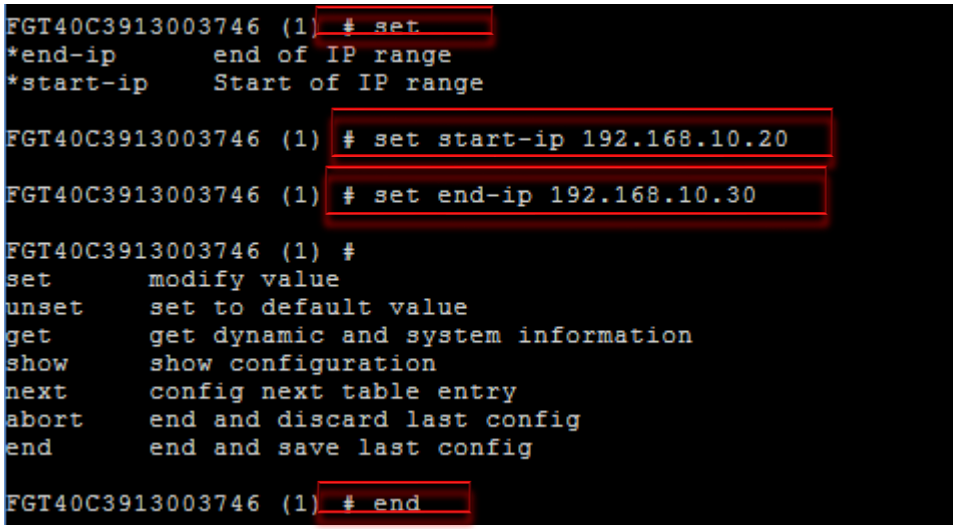
```
FGT40C3913003746 (1) # set interface
<string>    please input string value
internal ()interface
wan1 ()interface
wan2 ()interface

FGT40C3913003746 (1) # se interface wan2

FGT40C3913003746 (1) # set lease-time
<integer>    300 ~ 8640000 seconds (5 minutes ~ 100 days)
     0 for unlimited lease time


FGT40C3913003746 (1) # set lease-time 300

FGT40C3913003746 (1) # set netmask
<net_netmask>    Net netmask xxx.xxx.xxx.xxx

FGT40C3913003746 (1) # set netmask 255.255.255.0
```

4. Activaremos nuestro DHCP con el siguiente comando.

```
FGT40C3913003746 (1) # set enable enable
 <Enter>
```

5. Aquí vemos el comando para poder configurar el rango de IP que será asignado.

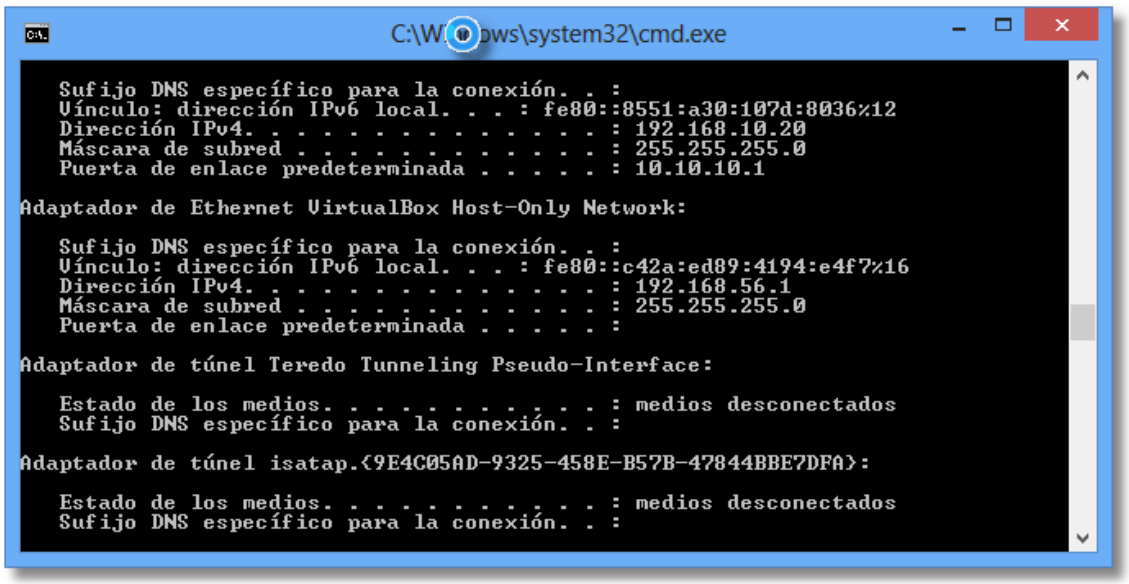




6. Como hemos visto ya está configurado el rango que será asignado para la configuración de IP, con el comando

   set start-ip 192.168.10.20- 192.168.10.30.

Demostraremos con una pc con un recuadro mostrando la ip



2.19 GUIA 6

CREACION DE BACKUP Y PROCEDIMIENTO DE RESTAURACION

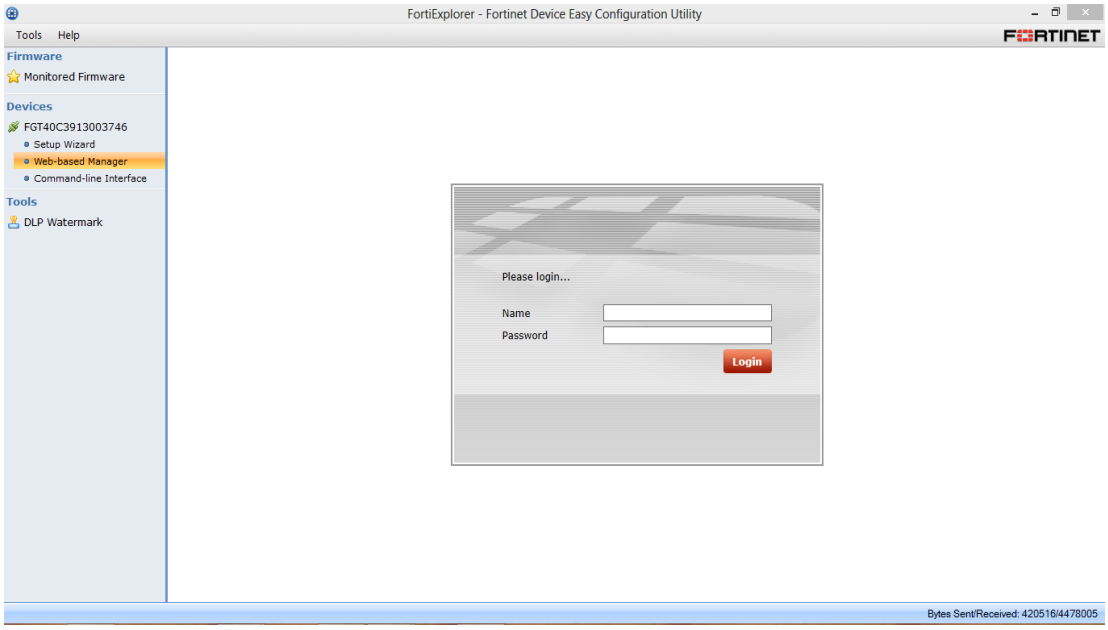
Guía de creación de backup y procedimiento de restauración.

Una copia de seguridad, copia de respaldo o *backup* (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrupto, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales; etc..

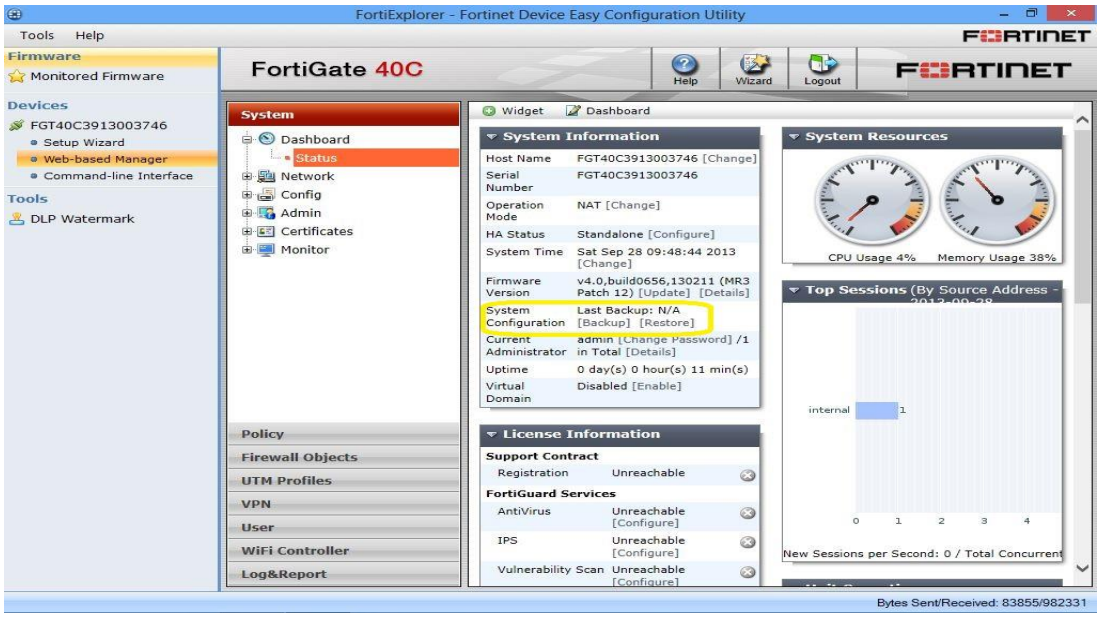
El proceso de copia de seguridad se complementa con otro conocido como restauración de los datos (en inglés *restore*), que es la acción de leer y grabar en la ubicación original u otra alternativa los datos requeridos.

Iniciamos con los pasos requeridos para la siguiente guía de creación de backup y procedimiento de restauración para la configuración del equipo firewall en este caso el Fortinet Fortigate-40c.

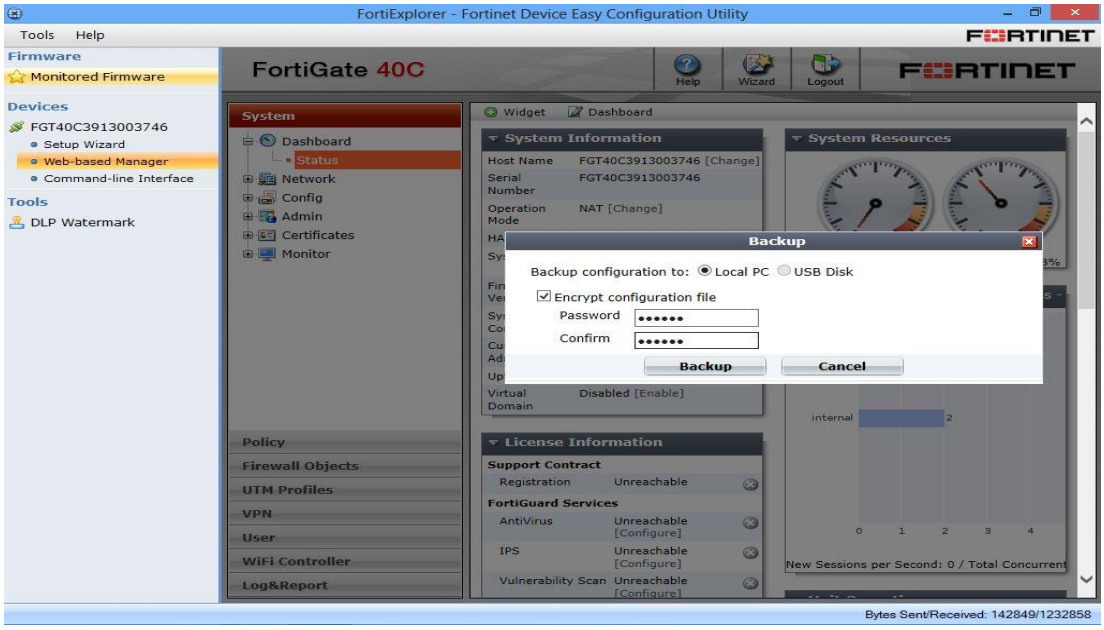
1. En el software FortiExplorer damos clic izquierdo en web-based manager y luego iniciamos sesión con nuestro usuario y contraseña.



2. En la siguiente pantalla nos ubicamos en el menú de “system” y damos clic en “Dashboard” y luego en “status”, y en el apartado de la información del sistema buscamos “System configuration” que nos indicaría el ultimo backup realizado en este caso no muestra ninguno y damos clic izquierdo en “backup”.

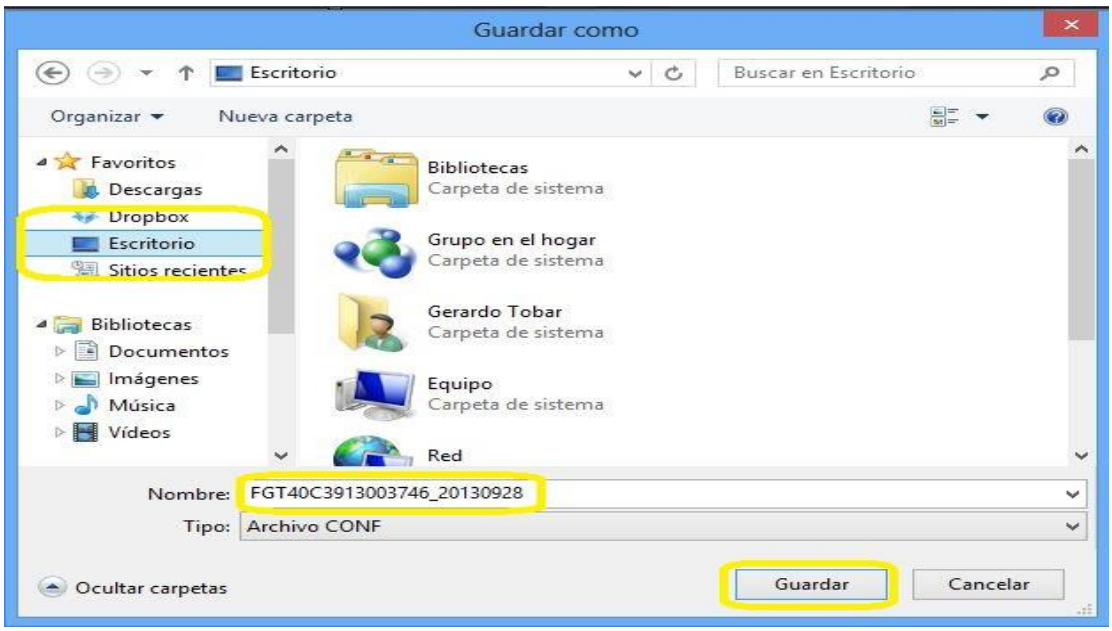


3. En la siguiente pantalla seleccionamos donde guardaremos el archivo de backup y seleccionamos la opción de “Encrypt configuration file” donde nos solicitara nuestra contraseña y damos clic izquierdo en “backup”.

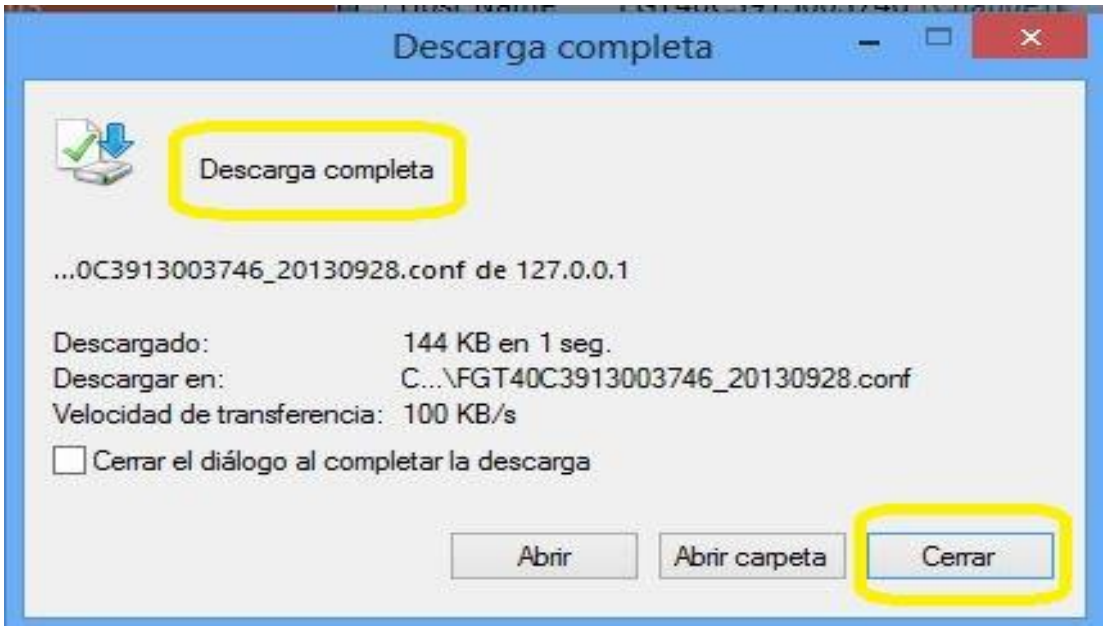


4. En la siguiente pantalla nos consulta si deseamos abrir o guardar el archivo de configuración en este caso daremos clic en “guardar”.

5. En el siguiente paso seleccionamos nuestra ruta o directorio en donde dejaremos el archivo guardado, si se necesita se puede cambiar el nombre del archivo para un mejor recordatorio, luego proceder a dar clic izquierdo en “guardar”.



6. En el siguiente paso esperaremos a que la descarga del archivo se complete y daremos un clic izquierdo en “cerrar y ya tendremos nuestro backup realizado.

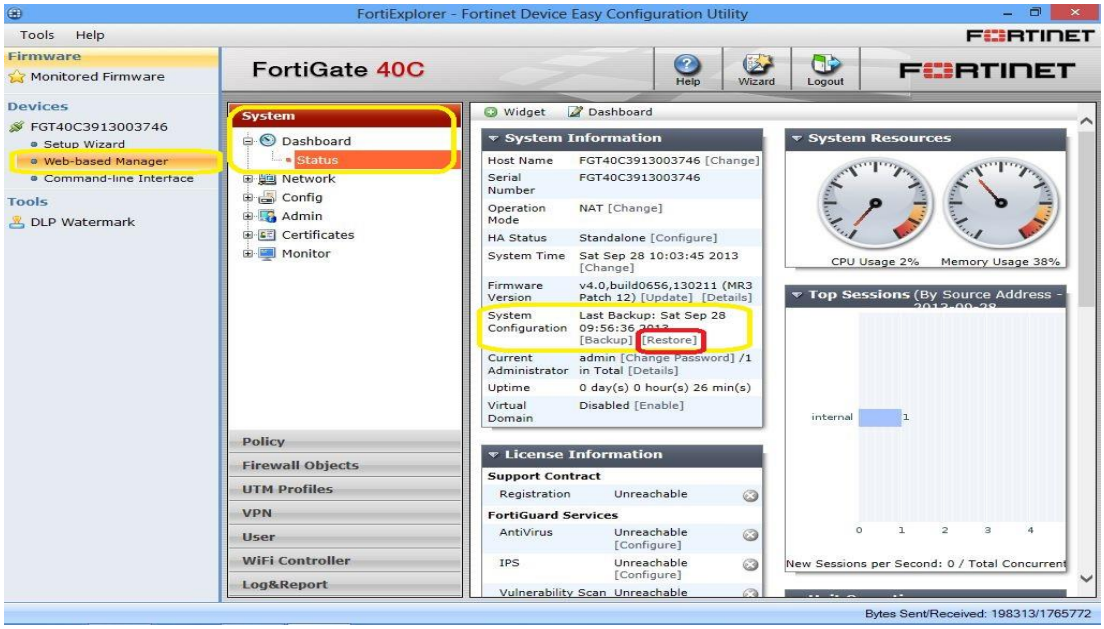


7. Si deseamos verificar si el procedimiento tuvo éxito nos dirigimos al directorio donde decidimos guardar nuestro archivo de configuración.

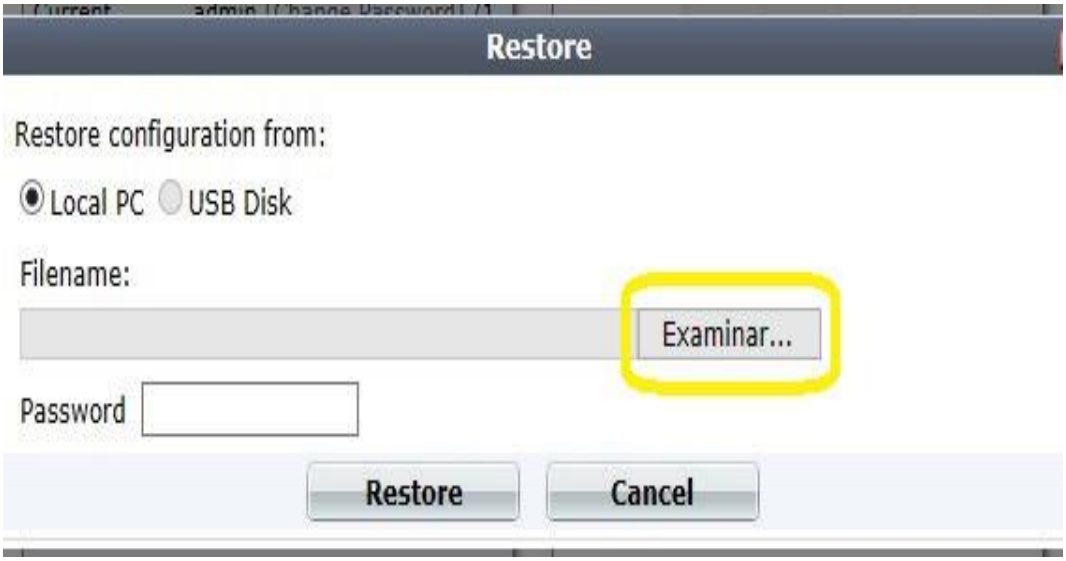
A continuación en la segunda parte de esta guía mostraremos como realizar el procedimiento de restauración para nuestro equipo cuando sea necesario o cuando tengamos algún tipo de falla o error.

1. En el software Fortiexplorer damos clic en “web-based manager” y nos ubicaremos en el menú “system” daremos otro clic en “dashboard” y luego en “status” y nos dirigimos al apartado de información del sistemas

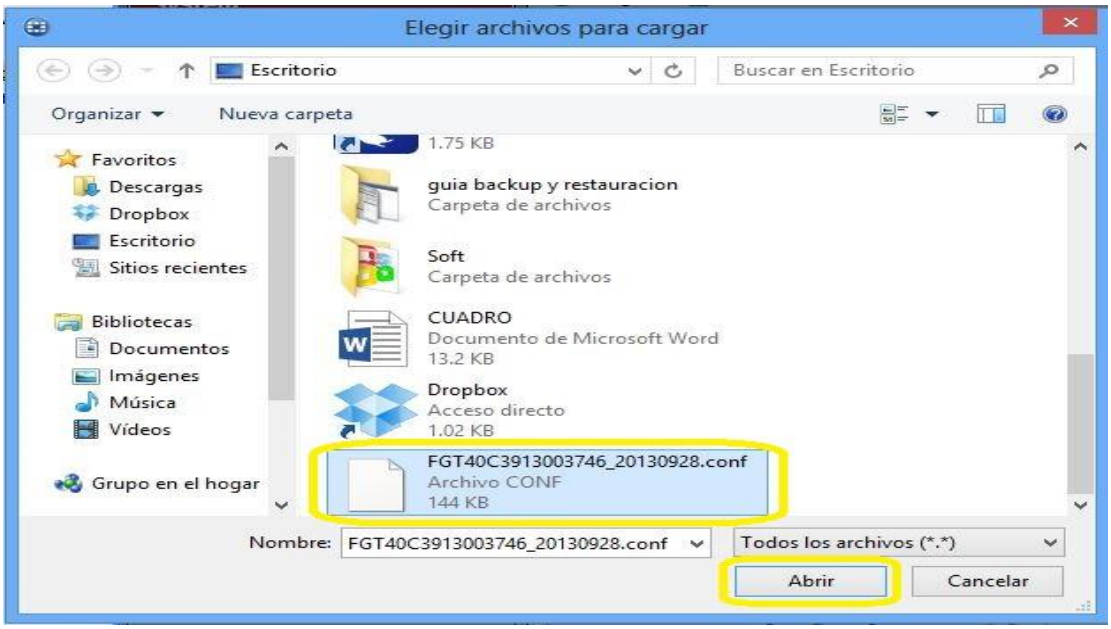
y en la sección de “system configuration” nos muestra el detalle de nuestro último backup, y daremos clic en “restore”.



2. En la siguiente ventana que se muestra daremos clic izquierdo para examinar nuestro archivo en el directorio que se encuentre guardado.



3. Seleccionamos nuestro archivo y damos clic izquierdo en “abrir”.



4. Después que tengamos nuestro archivo seleccionado ponemos nuestra contraseña y daremos clic izquierdo en “restore”.

5. Esperamos a que nos muestre el mensaje que el procedimiento se ha realizado con éxito (por motivos de la rapidez del procedimiento no se logró hacer la captura de pantalla del mensaje) y esperamos a que nuestro equipo se reinicie automáticamente y cargue nuevamente, y ya tendremos nuestra restauración realizada.

CAPÍTULO III

PROPUESTA DE LA SOLUCIÓN

3.1 Propuesta de solución

Efectuando una investigación en la Biblioteca de la Universidad Tecnológica de El Salvador se demostró, que no se cuenta con guías que expliquen paso a paso el funcionamiento y configuración de los equipos Fortinet FortiGate 40-C; Tomando en cuenta que la Catedra de Redes de la Universidad los ha adquirido recientemente. Estos equipos serán puestos a disposición de los docentes para la enseñanza en las prácticas de seguridad, tomando como base principal cada una de las guías que contiene este documento y estarán disponibles para su uso respectivo en la Biblioteca, de esta forma se ayudara a solventar los problemas que puedan tener los estudiantes de ciclos posteriores acerca de este tema ya que contarán con material didáctico del cual puedan apoyarse y además solventar alguna duda que respecte a la temática de Firewall, el cual está desarrollado ampliamente en este aporte bien documentado.

Las guías están basadas en un esquema básico funcional diseñado para el laboratorio de redes para que los resultados puedan ser satisfactorios.

Se han diseñado de tal manera que el estudiante no encuentre inconvenientes, en el proceso de desarrollo, haciendo más comprensivo el aprendizaje,

colocando capturas de pantalla con su correspondiente explicación en cada una de ellas.

Se incorporará este documento completo con contenido nuevo sobre el tema de seguridad con los equipos Fortinet FortiGate 40-C en formato digital e impreso a cada una de las bibliotecas de la Universidad Tecnológica de El Salvador, donde los bibliotecarios/as las podrán al alcance de los estudiantes que necesiten consultar esta temática, haciendo uso debido de este documento que será su material de apoyo y aprendizaje para llevar a cabo sus prácticas.

3.1.1 Planteamiento del proyecto temático

Las fases planteadas en este capítulo permitirán conocer paso a paso el desarrollo del Documento Elaboración de Guías de administración y configuración de firewall Fortinet FortiGate 40-C. Para fortalecer los conocimientos en el área de seguridad de una red informática, de la asignatura Administración de Redes de la Universidad Tecnológica de El Salvador

Se realizan tres fases que darán la propuesta de solución del documento, las cuales son:

FASE 1: Investigación.

Se indago sobre los temas del documento en la Biblioteca de la Universidad Tecnológica de El Salvador y no se encontró información sobre el dispositivo FortiGate 40-C, en base a la investigación y tomando en cuenta que en la actualidad hay mayor demanda por parte de los empresarios, para la seguridad de la información que manejan sus empresas, solicitando personal capacitado en el área que solicitan, con ello se dispondrá de guías básicas donde se desarrollan temáticas básicas tanto de instalación como de configuración.

Se tomó en cuenta las características de los equipos que había en el Laboratorio de la Universidad para así al momento de implementar los Servidores no se produzca ningún error.

El nuevo material de estudio les facilitara las tareas de entendimiento básico de las características de seguridad que provee el firewall FortiGate 40-C con este se favorecerá el proceso aprendizaje y se reforzaran las competencias en entorno de seguridad.

FASE 2: Instalación y Configuración

Considerando los requerimientos mínimos para el uso de los equipos en un escenario básico de red, las funcionalidades para las cuales se ha desarrollado material didáctico son las siguientes:

- Conociendo la interfaz gráfica de usuario (GUI) de FortiExplorer.
- Configuración básica a través del set-up wizard de FortiExplorer.

- Comandos básicos por medio de CLI.
- Creación de backup y procedimiento de restauración de configuración.

Teniendo en cuenta que las siguientes funcionalidades son las que habitualmente un administrador deberá manejar y aplicar como seguridad básica en una red

FASE 3: Pruebas

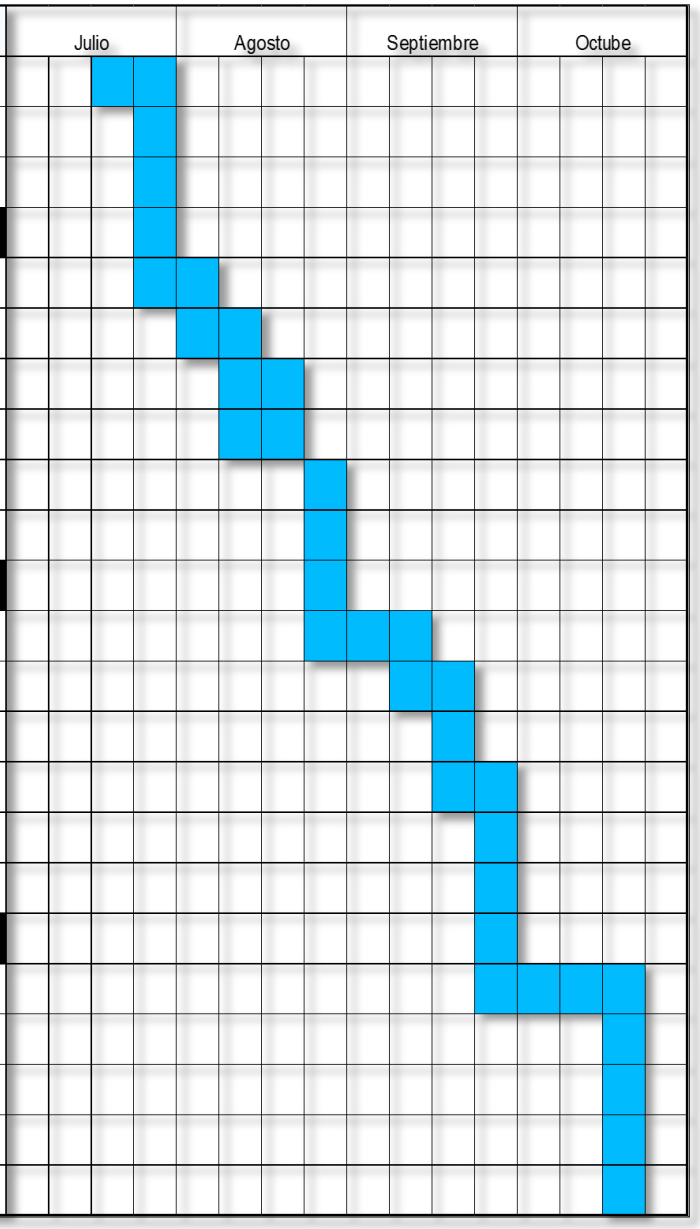
Para finalizar la propuesta de solución para la configuración del equipo FortiGate 40-C, se realizaron una serie de pruebas, que consistieron en verificar el buen funcionamiento de las políticas aplicadas, así como su comprobación.

Pruebas a realizar:

- ✓ Conectividad entre servidor y cliente
- ✓ Verificación de cada política creada

3.1.2 Cronograma de Actividades

Nombre de tarea	Fechas / 2013
Inscripción seminario de egresados	22-jul al 26-jul
Inicio del proceso de graduación	29-jul
asignación del asesor, inscripción de grupo y	29-jul al 31-jul
Primer Avance	
Desarrollo	30-jul al 05-agos
Investigación	06-agos al 12-agos
Organización de ideas y redacción	13-agos al 19-agos
Revisión de la propuesta	20-agos al 26-agos
Diseño de la propuesta	27-agos al 29-agos
Entrega	26-agos al 30-agos
Segundo Avance	
Desarrollo	31-agos al 11-sep
Búsqueda de información	12-sep al 18-sep
Capturas de pantalla	19-sep
Organización del documento	20-sep al 26-sep
Correcciones del proyecto de parte del	26-sep
Entrega	23-sep al 27-sep
Tercer Avance	
Desarrollo	28-sep al 18-oct
Reunión grupal para toma de decisiones	19-oct al 20-oct
Revisión del proyecto	21-oct al 22-oct
Reunión con el asesor	23-oct al 24-oct
Entrega	21-oct al 25-oct



3.2 Tecnologías y recursos seleccionados

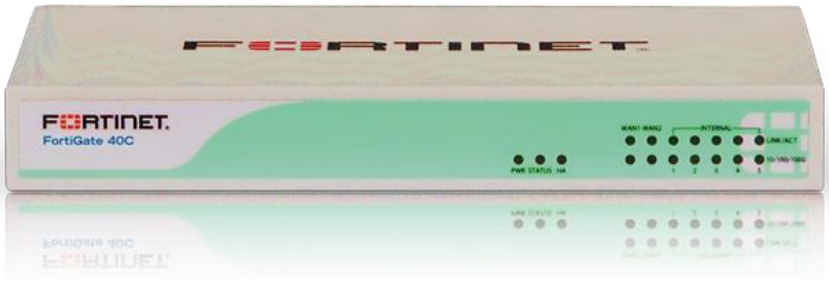


Figura 3.1 equipo FortiGate 40 C

FORTINET es el proveedor líder de Sistemas de Seguridad con Aceleración basada en ASIC. Nombrado por IDC como el Proveedor Líder en Sistemas Gerenciados de Amenaza Unificada (UTM).

FORTINET proporciona una solución completa de seguridad que provee seguridad de contenido verdadero a 360° en escaneo, registros, reportes, provisionamiento y manejo centralizado.

Los dispositivos Fortinet minimizan el esfuerzo requerido para monitorear y mantener políticas de uso aceptables, para identificar patrones de ataques y procesar al atacante y cumplir con las regulaciones gubernamentales relativo a la privacidad y descubrimiento de brechas de seguridad.

Estos aceptan y procesan una gran cantidad de registros log proporcionados por los sistemas FortiGate, incluyendo datos de tráfico, eventos, virus, ataque, filtrado de contenidos y filtrado de correo electrónico

Equipo adicional a FortiGate 40-C El sistema FortiManager es la piedra angular de la solución central de administración.

FortiManager es administración y monitoreo integrado que permite a la Empresa de cualquier tamaño administrar fácilmente los productos Fortinet.

Reduce el esfuerzo de administración requerido para desplegar, configurar, monitorear y mantener el rango completo de los productos Fortinet que provee en la seguridad de la red

El conjunto de soluciones de la familia Fortinet pueden proveer en conjunto todas las siguientes características

Funcionalidades de FortiGate

- ✓ Anti Virus (Gateway).
- ✓ Anti Spam.
- ✓ Filtrado de contenido Web. Ips
- ✓ Vpn
- ✓ Segmentación de ancho de banda

- ✓ Ruteo
- ✓ Firewall
- ✓ Prevención contra fuga de información (DLP)
- ✓ Seguridad inalámbrica centralizada.
- ✓ Optimización sobre WAN.
- ✓ Control de aplicaciones.

Tabla 3.3

Requerimientos mínimos de la pc del administrador:

Procesador, sistema operativo y memoria	
Sistema operativo	Genuine Windows Xp Professional.
Procesador	Intel ® Pentium ® de doble núcleo E2140. 1.60 GHz 1Mb de cache L2 800 MHz FSB.
Chipset	Intel 963Q Expreso.
Memoria serie	2X512 Mb.
Tipo de memoria	PC2-530 (DDR2 667).
Las ranuras de memoria	4 DIMM.
Actualización de la memoria	Ampliable a 4 Gb.
Unidades internas	
Disco duro	80 Gb
Velocidad de la unidad	7200 rpm
Bahías de unidad externa	2 externos de 5,25 pulgadas, 1 externo de 3,5 pulgadas
Bahía interna de unidad	2 internos de 3,5 pulgadas
CD ROM y DVD	48X/32X Combo
Controlador de disco duro	SATA 3.0 Gb/s

Tabla 3.4

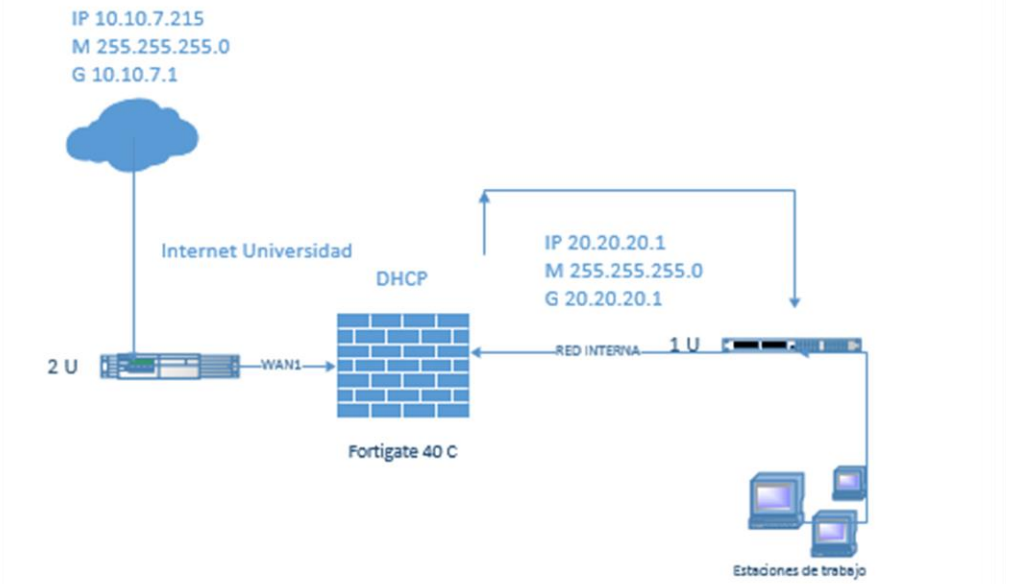
Descripción del equipo Fortinet

Interface	Tipo	Protocolo	Descripción
Puertos Ethernet 1-5	RJ-45	Gigabit Ethernet	FortiASIC aceleró puerto Ethernet conmutados para la conexión a la red
WAN 1,2	RJ-45	Gigabit Ethernet	FortiASIC aceleró puerto Ethernet
USB	USB-A	USB 2.0	Puerto del servidor USB para llave memoria flash, módem o para realizar funciones de gestión.
USB MGMT	USB-B	USB 2.0	Puerto USB cliente para funciones de gestión.
Consola	RJ-45	RS-232 serial	Conexión opcional al equipo de gestión

Especificación de Hardware	Descripción
CPU	FortiASIC SoC
Almacenamiento Interno	No extraíble, 4gb de múltiples niveles de células NAND flash para optimización WAN
Memoria	512 MB (DDR 2)
Energía AC	100-240V, 50-60HZ
Consumo de energía	12.3W / 14.8W
Disipación de calor	50.5BTU/h
Montaje en pared	Sí
Ranura de seguridad Kensington	Ranura de seguridad antirrobo
Botón de reinicio	Presionar durante 5 segundos para restablecer el FortiGate al ajuste de fábrica

3.3 Diseño de la propuesta

El esquema presentado a continuación es la topología básica con la cual se elaboró el contenido didáctico para el cual la persona que desee hacer uso de las guías desarrolladas deberá guiarse con la imagen presentada a continuación



Las solicitudes generadas por las estaciones de trabajo dependen de una interfaz denominada red interna la cual es a la que las políticas creadas en el equipo FortiGate 40-C establecerán los parámetros de accesos que podrán tener bajo dicha red. Se podrá notar que en el esquema aparece una interfaz llamada WAN 1 la cual es la que deberá poseer el direccionamiento permitido para que el dispositivo pueda proveer acceso a internet con ello todas las solicitudes que

lleguen a la interfaz de red interna, dependiendo de si el tráfico es permitido o denegado será direccionado a la interfaz WAN 1

3.4 Presentación de la propuesta

No se realizó ningún gasto económico

3.1.7 Evidencias del Proyecto

Figura 3.8

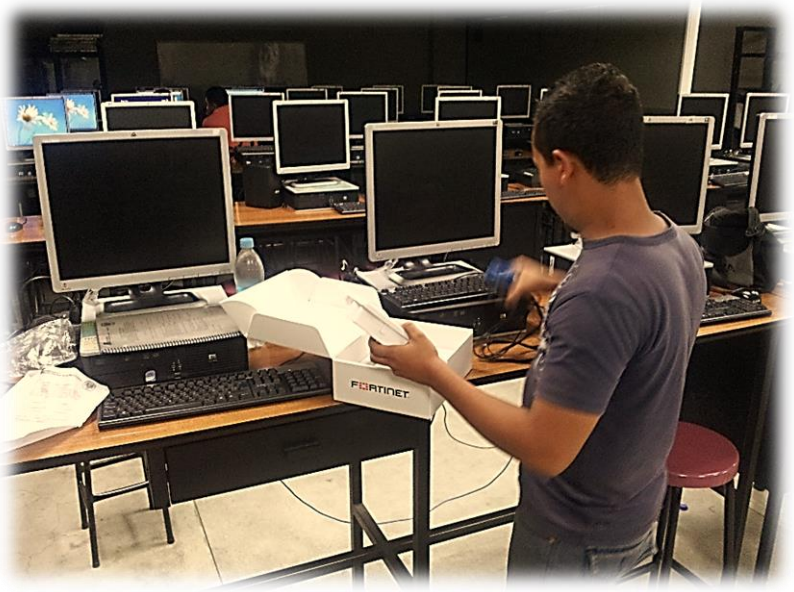


Figura 3.9

Figura 3.10

Figura 3.11

3.5 Conclusiones

Una investigación realizada en la Bibliotecas de la Universidad Tecnológica de El Salvador, en el área de Informática dio como resultado que: no existía material didáctico, que explique la funcionabilidad del equipo FortiGate 40-C; Por consiguiente, había la necesidad de elaborar guías de administración y configuración básicas para estos dispositivos de seguridad.

Las guías de administración y configuración del Firewall Fortinet, FortiGate 40-C, facilitará a los estudiantes de forma comprensiva el aprendizaje autónomo orientado a las funcionalidades de la seguridad en una red de datos.

El Firewall FortiGate 40-C, proporcionará la mayoría de las herramientas para complementar la seguridad en la red, mediante la imposición de políticas de seguridad, en el acceso a los recursos de la red.

De igual forma todo el documento servirá de apoyo tanto a docentes como estudiantes en el desarrollo básico del funcionamiento del equipo con lo cual se podrá ir mejorando con el tiempo hasta llegar a poseer material didáctico avanzado de estos temas.

3.6 Recomendaciones.

Se considera que algunos de los conocimientos más importantes, para todo administrador; son las políticas de seguridad dentro de una red, aplicando el contenido teórico practico que está descrito paso a paso en las guías de configuración básica del equipo Firewall Fortinet FortiGate 40-C. Dichas recomendaciones son las siguientes, esperando sean tomadas en cuenta para un desarrollo óptimo:

- ✓ El contenido desarrollado para el funcionamiento correcto de las guías se deberá respetar la topología.

- ✓ Entendimiento sobre interconexión de dispositivos facilitara el resultado de las guías.

3.7 Glosario de Términos:

A

- **Access Points:** Punto de acceso inalámbrico hacia una red.

- **Anti-spam:** Software que puede detectar y filtrar el spam. (Correo no deseado).

- **Anti-spyware:** Programa desarrollado para el ámbito de la seguridad informática, el cual protege a los usuarios de programas maliciosos, tales como el software espía, spywares, la publicidad no deseada en nuestro navegador, adwares, pérdida de control sobre nuestro equipo.

B

- **Backup:** Una copia de seguridad, copia de respaldo o backup en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

C

- **CISSP:** Es una certificación de alto nivel profesional otorgada por la (ISC)2, con el objetivo de ayudar a las empresas a reconocer a los profesionales con formación en el área de seguridad de la información.

- **CLI:** La infraestructura de lenguaje común (Common Language Infrastructure, CLI).

- **Consola:** Sistema o consola de comandos, un método que permite a las personas dar instrucciones a algún programa informático.

- **Criptografía:** La criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

D

- **DBs:** o Direct Broadcast Satellite es el servicio que distribuye una señal de audio, vídeo o datos sobre una extensa zona predeterminada.

- **DNS:** Domain Name System o DNS es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

- **Dominios:** Es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet.

E

- **Ethernet:** Ethernet es un estándar de redes de área local para computadores con acceso al medio por contienda.

F

- **Filtrado web:** Programa diseñado especialmente para restringir el acceso a ciertos materiales de la Web.

- **Firewall:** Un cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

- **Firmware:** El firmware es un bloque de instrucciones de máquina para propósitos específicos, grabado en una memoria, normalmente de lectura/escritura, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

- **FortiAnalyzer:** Es un sistema de logeo, analizador y de reporte de redes en tiempo real de forma segura, agregan y analizan la información logeada desde los dispositivos de seguridad FortiGate, permitiéndote cumplir con las regulaciones gubernamentales, relacionadas con privacidad.

- **FortiExplorer:** Software de administración de dispositivos Fortinet.

- **Fortigate-40C:** Firewall con funciones de seguridad administrables.

- **FortiGuard:** Filtro que se encarga de gestionar la seguridad y permisos en la web.

- **FortiManager:** El FortiManager suministra las herramientas necesarias para gestionar eficientemente cualquier tamaño de infraestructura de seguridad de Fortinet.

- **Fortinet:** Fortinet es una empresa privada estadounidense, situada en Sunnyvale (California), que se dedica especialmente al diseño y fabricación de componentes y dispositivos de seguridad para redes informáticas.

- **FTP:** FTP en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.

G

- **GUI**: Interfaz Gráfica de Usuario.
-

H

- **HTTP:** Hypertext Transfer Protocol o HTTP es el protocolo usado en cada transacción de la World Wide Web.

- **HTTPS**: Hypertext Transfer Protocol Secure, más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP.

I

- **IANA:** Internet Assigned Numbers Authority es la entidad que supervisa la asignación global de direcciones IP, sistemas autónomos, servidores raíz de nombres de dominio DNS y otros recursos relativos a los protocolos de Internet.

- **IMAP:** Internet Message Access Protocol, es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet.

- **IRC:** es un protocolo de comunicación en tiempo real basado en texto, que permite debates entre dos o más personas.

- **ISO/IEC27002:** Es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International

Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000.

L

- **Línea de comando:** Interfaz de Línea de Comandos, por su acrónimo en inglés de Command Line Interface, es un método que permite a las personas dar instrucciones a algún programa informático por medio de una línea de texto simple.

M

- **Matlab:** es una herramienta de software matemático que ofrece un entorno de desarrollo integrado con un lenguaje de programación propio.

- **Modelo de referencia OSI**: Modelo arquitectónico definido por ISO que está compuesto por siete capas o niveles: físico, enlace, red, transporte, sesión, presentación y aplicación.

N

- **NFS:** El Network File System, o NFS, es un protocolo de nivel de aplicación, según el Modelo OSI.
- **NIC:** El proceso de registro era hecho a través de la DDN-NIC en el Centro de Investigación de Stanford.

- **NNTP:** Network News Transport Protocol es un protocolo inicialmente creado para la lectura y publicación de artículos de noticias en Usenet.

- NTP: Network Time Protocol es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

P

- **POP3:** Post Office Protocol Es un protocolo de red que se utiliza en clientes locales de correo electrónico para obtener los mensajes de correo electrónico almacenados en un servidor remoto.

- **Puertos:** Un puerto de red es una interfaz para comunicarse con un programa a través de una red.

R

- **RJ-45:** Es una interfaz física comúnmente usada para conectar redes de cableado estructurado. Es parte del Código Federal de Regulaciones de Estados Unidos.

S

- **SCTP:** Stream Control Transmission Protocol es un protocolo de comunicación de capa de transporte que fue definido por el grupo SIGTRAN de IETF en el año 2000.

- **SMTP:** El Simple Mail Transfer Protocol, es un protocolo de la capa de aplicación. Protocolo de red basado en texto, utilizado para el intercambio de mensajes de correo electrónico

- **Sniffing:** Se trata de dispositivos que permiten al atacante “escuchar” las diversas comunicaciones que se establecen entre ordenadores a través de una red.

- **Spoofing:** Uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

- **SSH:** Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

T

- **Telnet:** Es el nombre de un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

- **TFTP:** Son las siglas de Trivial file transfer Protocol. Es un protocolo de transferencia muy simple semejante a una versión básica de FTP.

U

- **UDP:** User Datagram Protocol es un protocolo del nivel de transporte basado en el intercambio de datagramas.

- **URL:** Es una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación.

W

- **WHOIS:** es un protocolo TCP basado en petición/respuesta que se utiliza para efectuar consultas en una base de datos.

X

- **XNS:** Protocolo de comunicación de la firma Rank Xerox.

3.8 Referencias.

Cisco. (2013). *Seguridad en redes.* Recuperado de http://www.cisco.com/web/ES/solutions/smb/products/security/security_primer.html

Fundación Wikimedia, Inc. (2013). *Cortafuegos Informática.* Recuperado de http://es.wikipedia.org/wiki/Cortafuegos_(informática)

Fundación Wikimedia, Inc. (2013). *Técnica de ataque Spoofing.* Recuperado de http://es.wikipedia.org/wiki/Spoofing

Fundación Wikimedia, Inc. (2013). *Protocolo SMTP.* Recuperado de http://es.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Fortinet. (2013). *Network Security Appliance Fortinet.* Recuperado de http://www.fortinet.com/products/fortigate/40C.html

Fortinet. (2013). *Download Software FortiExplorer.* Recuperado de http://www.fortinet.com/resource_center/fortiexplorer_product_download.html

FortiForo. (2013). *Foro no oficial de soporte en español.* Recuperado de http://www.fortigate.es/

Microsoft. (2005). *Introducción a TCP/IP.* Recuperado de http://technet.microsoft.com/es-es/library/cc786900(WS.10).aspx

Microsoft. (2005). *Protocolo UDP.* Recuperado de http://technet.microsoft.com/es-es/library/cc785220(v=ws.10).aspx

Microsoft. (2013). *Que es un firewall.* Recuperado de http://windows.microsoft.com/es-co/windows/what-is-firewall#1TC=windows-7

Slideshare. (2010). *Modelo de referencia OSI.* Recuperado de http://www.slideshare.net/SuperFonso/modelo-de-referencia-osi-3009986

Slideshare. (2012). *Tipos de Firewall.* Recuperado de http://www.slideshare.net/CathaGuzman/tipos-de-firewall

Ulbrich Cesar, & Valle Della. (2011). *Universidad Hacker.* Recuperado de http://es.scribd.com/doc/63912618/202/Husmeando-en-la-red-Sniffing