



UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN ELECTRÓNICA DIGITAL Y TELECOMUNICACIONES

**TEMA: ELABORACIÓN DE UN MÓDULO PARA PRÁCTICAS DE LABORATORIO
DE GESTIÓN UNIFICADA DE AMENAZAS EN LA UNIVERSIDAD ISRAEL**

AUTOR/ A: JORGE ANÍBAL PICHUCHO BOMBÓN

**TUTOR/ A: Mg FRANCISCO JURADO PRUNA
TUTOR TÉCNICO: Mg. TANNIA MAYORGA JÁCOME**

AÑO: 2017

DECLARACIÓN

Yo, Pichucho Bombón Jorge Aníbal, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Tecnológica Israel, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido en su reglamento y por la normatividad institucional vigente.

Pichucho Bombón Jorge Aníbal

CERTIFICACIÓN DEL TUTOR

Certifico que el presente trabajo fue desarrollado por Pichucho Bombón Jorge Aníbal, bajo mi supervisión.

Ing. Tannia Mayorga Mg.
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Agradezco a Dios por permitirme vivir y bendecir cada uno de mis pasos.

A la memoria de mi padre quien a pesar de no estar presente, dejo en mí sus enseñanzas, perseverancia, valores y constante lucha por conseguir cada uno de los objetivos propuestos.

A mi madre quien con su amor y sacrificio logro darme fortaleza y fuerza para seguir adelante siendo un gran ejemplo para mí.

A mi amor, mi esposa Patty, quien me ha acompañado incondicionalmente en cada meta propuesta, regalándome cada momento de su tiempo, cuando lo necesite y brindarme la alegría de ser padre de dos hijos maravillosos.

A mis familiares por su apoyo incondicional.

A mis profesores, por el conocimiento transmitido en todo este tiempo como estudiante y en especial a mis tutores por su apoyo y tiempo dedicado a la elaboración de mi tesis.

Jorge Pichucho

DEDICATORIA

A mi esposa Patty, por el apoyo incondicional y el amor brindando a lo largo de estos años, siendo antes que mi esposa mi mejor amiga. Gracias por regalarme la alegría de ser padre y formar una familia con unos hijos maravillosos Julian y Jetzabel, quienes de igual forma han sido mi fuente de inspiración y también dedico este logro.

INDICE

1. INTRODUCCIÓN.....	3
1.1. ANTECEDENTES.....	3
1.2. EL PROBLEMA	4
1.2.1. Problema principal.....	4
1.3. JUSTIFICACIÓN.....	4
1.4. OBJETIVOS.....	4
1.4.1. Objetivo General	4
1.4.2. Objetivos Específicos	4
2. FUNDAMENTACIÓN TEÓRICA	5
2.1. INFRAESTRUCTURA DE RED Y COMUNICACIONES	5
2.1.1 Tecnologías de redes	5
2.1.2 Red de computadoras.....	5
2.1.3 Elementos de Red	6
2.1.3.1 El Switch	6
2.1.3.2 El Router	6
2.1.3.3 Protocolos de comunicación.....	7
2.1.3.4 Servidor.....	8
2.1.3.5 Estaciones de Trabajo.....	8
2.1.3.6 Cableado.....	8
2.1.3.7 Hub o Concentrador	9
2.1.3.8 Punto de acceso inalámbrico (Wireless Access Point)	9
2.1.3.9 Firewall.....	9
2.2. SEGURIDAD INFORMÁTICA	10
2.2.1 Definición de Seguridad Informática	10
2.2.2 Seguridad de la Información	10
2.2.3 Seguridad Perimetral	10
2.2.3.1 Para qué sirve la seguridad perimetral?	11
2.2.4 Protagonistas de ataques informáticos	11
2.2.4.1 Hacker.....	12
2.2.4.2 Cracker	12
2.2.4.3 Phreaker	13
2.2.4.4 Script Kiddies	13
2.2.4.5 Hacktivistas	14

2.2.4.6	Newbie o Neophyte	14
2.2.4.7	Lammer	15
2.2.5	Amenazas y tipos de ataques en la red	15
2.2.5.1	Malware	15
2.2.5.2	Virus	16
2.2.5.3	Gusano	16
2.2.5.4	Troyano	16
2.2.5.5	Man in the middle	16
2.2.5.6	DoS (Denegación de Servicio)	16
2.2.5.7	DDoS (Denegación Distribuida de Servicio)	17
2.2.5.8	Ransomware	17
3.	COMPARACIÓN CON OTROS FABRICANTES Y DISEÑO DEL SISTEMA DE GESTIÓN UNIFICADO DE AMENAZAS	19
3.1.	UNIFIED THREAT MANAGEMENT (UTM) O GESTIÓN UNIFICADA DE AMENAZAS	19
3.1.1	Componentes de un Sistema UTM:	20
3.2.	PRINCIPALES REQUERIMIENTOS DEL CLIENTE	22
3.3.	ANÁLISIS SOLUCIÓN FORTINET	22
3.3.1	Tecnología FORTIASIC	23
3.3.1.1	Content Processor	23
3.3.1.2	Network Processor	23
3.3.1.3	System-on-chip	23
3.3.2	Sistema Operativo FortiOS	24
3.3.3	Servicios Fortinet	26
3.3.3.1	Fortiguard	26
3.3.3.2	Forticare	26
3.4.	ANÁLISIS SOLUCIÓN CISCO ASA FIREPOWER	26
3.4.1	Tecnología Cisco ASA Firepower	27
3.4.2	Servicios y funciones de Cisco ASA Firepower	27
3.5.	COMPARACIÓN DE TECNOLOGÍAS UTM: FORTINET Y CISCO ASA FIREPOWER	28
3.6.	DISEÑO DEL MÓDULO PARA PRÁCTICAS DE LABORATORIO DE GESTIÓN UNIFICADA DE AMENAZAS EN LA UNIVERSIDAD ISRAEL	29
3.6.1	Alcance	30
3.6.2	Criterios del diseño y dimensionamiento del equipo	30
3.6.3	Análisis del dispositivo UTM	31

3.6.3.1	FORTINET	31
3.6.3.2	CISCO.....	33
3.6.3.3	Análisis de los Dispositivos UTM presentados.	35
3.6.4	Análisis de costos	37
3.6.4.1	Costo de la solución FORTINET	37
3.6.4.2	Costo de la solución CISCO	38
3.7.	ESPECIFICACIONES TÉCNICAS DEL UTM A IMPLEMENTARSE	38
3.7.1	Hardware	38
3.7.2	Software y Rendimiento.....	39
4.	IMPLEMENTACIÓN DEL MÓDULO Y ELABORACIÓN DE GUÍAS DE PRACTICA DE LABORATORIO.....	42
4.1.	Elementos necesarios para la implementación del UTM.....	42
4.1.1	Fortiwifi 30D.....	42
4.1.2	Cable de poder	43
4.1.3	Cable Ethernet.....	43
4.1.4	Adaptador USB a Serial.....	43
4.1.5	Cable DB9 a RJ-45.....	44
4.1.6	Laptop o PC.....	44
4.2.	Conexiones Básicas y Administración web con cable ethernet	44
4.3.	Configuración básica de Fortigate.....	46
4.4.	PRÁCTICAS DE LABORATORIO.....	54
4.4.1	Práctica N.-1 Inicialización UTM Fortigate	54
4.4.2	Práctica N.-2 Configuración Básica.....	62
4.4.3	Práctica N.-3 Respaldo de Configuraciones.....	71
4.4.4	Práctica N.-4 Configuración de objetos y políticas	76
4.4.5	Práctica N.-5 Configuración de perfiles de seguridad.....	81
4.4.6	Práctica N.-6 Antivirus	90
5.	CONCLUSIONES Y RECOMENDACIONES	96
6.	BIBLIOGRAFÍA.....	97
	ANEXOS.....	101

INDICE DE FIGURAS

Figura 1: Switch marca Fortinet 224D-POE (Fortinet, 2017)	6
Figura 2: Router marca Cisco (Cisco, 2016).....	7
Figura 3: Capas del Modelo OSI (Mikrotik, 2017)	7
Figura 4: Capas del Modelo TCP/IP (Netacad, 2017).....	8
Figura 5: Categoría de cableado (Krugel, 2013).....	8
Figura 6: Access Point marca Fortinet (Fortinet, 2017)	9
Figura 7: Firewall (Aportavalor, 2013).....	9
Figura 8: El muro simboliza la seguridad perimetral del cliente (Guardnet, 2011)	11
Figura 9: Diferencia Hacker y Cracker (Greenetics, 2016).....	13
Figura 10: Jhon Draper, alias “Cap’n Crunch (Hacker.NET, 2017).....	13
Figura 11: Script Kiddie (Geekistuff, 2014)	14
Figura 12: Grupos Hacktivistas Wikileaks y Anonymous (Reyes, 2013).....	14
Figura 13: Características de un Newbie (Greenetics, 2016)	15
Figura 14: Malware (Forospyware, 2009)	16
Figura 15: Ataque hombre en el medio (Cisco Networking Academy, 2016).....	17
Figura 16 Principales monedas digitales (Fortinet, 2017)	18
Figura 17: Ataque de Denegación de servicio (Seguridadweb20, 2015).....	18
Figura 18: Componentes de Sistema UTM (Fortinet, 2017)	19
Figura 19: La superficie de ataque se ha expandido (Fortinet, 2017)	20
Figura 20: Certificaciones Fortinet (Fortinet, 2017)	22
Figura 21: Hardware Sistemas Fortinet (Fortinet, 2017).....	23
Figura 22: Ingeniería de Hardware de Fortinet (Fortinet, 2017).	24
Figura 23: Comparación en pruebas realizadas NSS Labs (Fortinet, 2017).....	24
Figura 24: Evolución FortiOS y Módulos de Fortigate (Fortinet, 2017)	25
Figura 25: Servicios de Cisco ASA con Firepower (Cisco, 2016)	28
Figura 26: Firewall Multifunción en Small Medium Bussiness (Gartner, 2017).....	29
Figura 27: Especificaciones Técnicas del Dispositivo Fortinet (FortinetDocs, 2013).....	32
Figura 28: Características de Seguridad del Dispositivo Fortinet (FortinetDocs, 2013)	33
Figura 29: Especificaciones Técnicas del Dispositivo Cisco (Cisco, 2016)	35
Figura 30: Especificaciones de Hardware Fortiwifi 30D (FortinetDocs, 2013)	39
Figura 31: FortiOS versión 5.4 visualización de aplicaciones (FortinetDocs, 2013)	40
Figura 32: Especificaciones técnicas del rendimiento del equipo (FortinetDocs, 2013).....	40
Figura 33: Especificaciones adicionales Fortiwifi 30D (FortinetDocs, 2013)	40
Figura 34: Especificaciones Wireless (FortinetDocs, 2013).....	41
Figura 35: Diagrama de Red de Laboratorio de Redes (Elaboración Propia, 2017).....	42
Figura 36: Fortiwifi 30D (FortinetDocs, 2013).....	43
Figura 37: Cable de poder (FortinetDocs, 2013).....	43
Figura 38: Cable RJ-45 a RJ-45 (FortinetDocs, 2013).....	43
Figura 39: Adaptador SUB a Serial (Trendnet, 2017)	43
Figura 40: Cable RJ45 a DB9 hembra (Aliexpres, 2017).....	44
Figura 41: Conexión a través de cable Ethernet (FortinetDocs, 2013)	44
Figura 42: Conexión física desde laptop personal a Fortiwifi 30D (Elaboración Propia, 2017)...	44

Figura 43: Comando ipconfig desde CMD de Laptop Usuario (Elaboración Propia, 2017).....	45
Figura 44: Acceso vía browser a https://192.168.1.99 (Elaboración Propia, 2017)	45
Figura 45: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)	46
Figura 46 Menú Dashboard de equipo Fortiwifi 30D (Elaboración Propia, 2017).....	46
Figura 47: Vista Web del sistema (Elaboración Propia, 2017)	47
Figura 48: Configuración de Interfaz LAN del cliente (Elaboración Propia, 2017)	47
Figura 49: Configuración de Interfaz salida WAN hacia proveedor Internet (Elaboración Propia, 2017)	48
Figura 50: Configuración de ruta por defecto para salida a internet (Elaboración Propia, 2017).....	48
Figura 51: Configuración de política para salida a Internet (Elaboración Propia, 2017)	49
Figura 52: Prueba de ping al DNS de Google (Elaboración Propia, 2017).....	49
Figura 53: Prueba de salida al internet desde el PC (Elaboración Propia, 2017).....	50
Figura 54: Política de acceso a internet (Elaboración Propia, 2017).....	50
Figura 55: Opciones de Proxy (Elaboración Propia, 2017)	51
Figura 56: Configuración por defecto de Fortiwifi 30D (Elaboración Propia, 2017)	51
Figura 57: Cambio de parámetros de default a personalizados (Elaboración Propia, 2017)	52
Figura 58: Se despliega la red Wireless Laboratorio (Elaboración Propia, 2017)	52
Figura 59: Ingresamos el password laboratorio2017 (Elaboración Propia, 2017).....	52
Figura 60 Conexión al SSID Laboratorio sin inconveniente (Elaboración Propia, 2017)	53
Figura 61: Comando ipconfig para revisar dirección IP asignada (Elaboración Propia, 2017) ...	53
Figura 62: Conexión a Fortiwifi a través de Wireless (Elaboración Propia, 2017).....	53
Figura 63: Conexión básica a través del puerto USB de Administración Fortigate (Elaboración Propia, 2017).....	54
Figura 64: Cable USB (FortinetDocs, 2013)	55
Figura 65: Software Fortiexplorer (Elaboración Propia, 2017).....	56
Figura 66: Software Fortiexplorer verificando el equipo conectado vía USB (Elaboración Propia, 2017)	57
Figura 67: Ventana principal una vez activado el Setup Wizard (Elaboración Propia, 2017).....	57
Figura 68: Opciones del setup wizard (Elaboración Propia, 2017)	58
Figura 69: Configuración Zona Horaria del equipo (Elaboración Propia, 2017)	58
Figura 70: Configuración del direccionamiento IP y red del equipo (Elaboración Propia, 2017) ..	59
Figura 71: Configurar modo NAT del equipo, horario de navegación y VPN Remota (Elaboración Propia, 2017)	59
Figura 72: Resumen de los cambios realizados y aplicar los cambios (Elaboración Propia, 2017)	60
Figura 73: Aplicar y Finalizar el Wizard del Fortigate (Elaboración Propia, 2017)	60
Figura 74: Finalización del proceso Wizard (Elaboración Propia, 2017).....	61
Figura 75: Verificar cambio de dirección IP en Interfaz Lan del equipo luego del Wizard (Elaboración Propia, 2017)	61
Figura 76: Topología para administrar Fortigate (Elaboración Propia, 2017)	62
Figura 77: Comando ping desde CMD de Laptop Usuario (Elaboración Propia, 2017)	63
Figura 78: Acceso vía browser a https://192.168.1.1 (Elaboración Propia, 2017).....	64
Figura 79: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)	64
Figura 80: Menú Opciones administración Fortigate (Elaboración Propia, 2017)	64
Figura 81: Cambio de nombre del equipo (Elaboración Propia, 2017)	65

Figura 82: Nombre del equipo (Elaboración Propia, 2017)	66
Figura 83: Cambiar hora y fecha del sistema (Elaboración Propia, 2017)	66
Figura 84: Interfaces de red de Fortigate 30D (Elaboración Propia, 2017)	67
Figura 85: Configuración interfaz WAN acceso a internet del equipo (Elaboración Propia, 2017)	67
Figura 86: Configuración interfaz LAN acceso a red interna del cliente (Elaboración Propia, 2017)	68
Figura 87: Configuración de una ruta estática (Elaboración Propia, 2017)	68
Figura 88: Crear una ruta estática por defecto (Elaboración Propia, 2017)	69
Figura 89: Interfaz CLI del Equipo (Elaboración Propia, 2017)	69
Figura 90: Verificar configuración interfaz WAN (Elaboración Propia, 2017).....	69
Figura 91: Verificar configuración interfaz LAN (Elaboración Propia, 2017)	70
Figura 92: Verificar ruta estática (Elaboración Propia, 2017)	70
Figura 93: Cambio de password del sistema (Elaboración Propia, 2017)	70
Figura 94: Verificar acceso a internet desde Fortigate (Elaboración Propia, 2017).....	71
Figura 95: Topología para administrar Fortigate (Elaboración Propia, 2017)	71
Figura 96: Acceso vía browser a https://192.168.1.1 (Elaboración Propia, 2017).....	72
Figura 97: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)	73
Figura 98: Realizar un backup de configuración del equipo (Elaboración Propia, 2017).....	73
Figura 99: Backup a PC local del usuario sin encriptación (Elaboración Propia, 2017).....	73
Figura 100: Nombre del archivo por defecto del backup de configuración (Elaboración Propia, 2017)	74
Figura 101: Realizar un backup de configuración del equipo (Elaboración Propia, 2017).....	74
Figura 102: Backup a PC local del usuario con encriptación (Elaboración Propia, 2017)	74
Figura 103: Nombre del archivo por defecto del backup de configuración (Elaboración Propia, 2017)	75
Figura 104: Comparación archivos de backup del sistema sin y con encriptación (Elaboración Propia, 2017).....	75
Figura 105: Realizar una Restauración de configuración del equipo (Elaboración Propia, 2017)	76
Figura 106: Restaurar el sistema con archivo de backup (Elaboración Propia, 2017)	76
Figura 107: Topología para administrar Fortigate (Elaboración Propia, 2017)	77
Figura 108: Acceso vía browser a https://192.168.1.1 (Elaboración Propia, 2017)	78
Figura 109: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)	78
Figura 110: Crear la dirección IP de la PC como objeto.....	79
Figura 111: Crear política de navegación a internet a PC_Estudiante.....	80
Figura 112: Prueba de salida a internet desde PC Estudiante (Elaboración Propia, 2017)	80
Figura 113: Revisión de logs de tráfico desde la PC Estudiante 192.168.1.11	80
Figura 114: Topología para administrar Fortigate (Elaboración Propia, 2017)	81
Figura 115: Acceso vía browser a https://192.168.1.1 (Elaboración Propia, 2017)	82
Figura 116: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)	82
Figura 117: Verificar navegación a internet (Elaboración Propia, 2017).....	83
Figura 118: Verificar funcionamiento de aplicación Team Viewer (Elaboración Propia, 2017) ...	83
Figura 119: Crear un perfil de control aplicaciones (Elaboración Propia, 2017).....	84
Figura 120: Crear un perfil de control aplicaciones (Elaboración Propia, 2017).....	84

Figura 121: Escoger filtro de categorías (Elaboración Propia, 2017)	85
Figura 122: Elegir categoría Name (Elaboración Propia, 2017)	85
Figura 123: Digitar TeamViewer, aparece todos los nombres que coinciden (Elaboración Propia, 2017)	86
Figura 124: Escoger las aplicaciones seleccionadas (Elaboración Propia, 2017)	86
Figura 125: Agregar aplicaciones seleccionadas, verificar action Block y guardar (Elaboración Propia, 2017).....	86
Figura 126: Aplicar el perfil de seguridad en la política de navegación a internet (Elaboración Propia, 2017).....	87
Figura 127: Aplicación de Team Viewer bloqueada (Elaboración Propia, 2017).....	87
Figura 128: Agregar perfil de Filtrado Web (Elaboración Propia, 2017).....	88
Figura 129: Crear perfil de filtrado web para bloquear acceso a www.fortinet.com (Elaboración Propia, 2017).....	88
Figura 130: Aplicar el perfil de seguridad en la política de navegación a internet (Elaboración Propia, 2017).....	89
Figura 131: Mensaje de página bloqueada (Elaboración Propia, 2017)	89
Figura 132: Revisión de logs Fortigate (Elaboración Propia, 2017).....	90
Figura 133: Topología para administrar Fortigate (Elaboración Propia, 2017)	91
Figura 134: Acceso vía browser a https://192.168.1.1 (Elaboración Propia, 2017)	92
Figura 135: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)	92
Figura 136: Crear perfil de antivirus para bloquear ataques de antivirus (Elaboración Propia, 2017)	93
Figura 137: Aplicar el perfil de seguridad en la política de navegación a internet (Elaboración Propia, 2017).....	93
Figura 138: Ingresar a la página web www.eicar.org (Elaboración Propia, 2017).....	94
Figura 139: Descargar el archivo eicar.com (Elaboración Propia, 2017).....	94
Figura 140: Bloqueo al descargar archivo infectado con virus (Elaboración Propia, 2017)	95
Figura 141: Combinación de teclas (Elaboración Propia, 2017)	103
Figura 142: Comando de Windows (Elaboración Propia, 2017).....	103
Figura 143: Seleccionar interfaz de red (Elaboración Propia, 2017)	103
Figura 144: Protocolo IPv4 (Elaboración Propia, 2017).....	104
Figura 145: Ingreso de dirección IPv4 (Elaboración Propia, 2017).....	104
Figura 146: Archivo ejecutable de Fortiexplorer (Elaboración Propia, 2017)	105
Figura 147: Instalación de Fortiexplorer (Elaboración Propia, 2017).....	105
Figura 148: Ejecutar el programa Fortiexplorer (Elaboración Propia, 2017)	106
Figura 149: Ejecutar el programa Fortiexplorer (Elaboración Propia, 2017)	106
Figura 150: Conexión básica (FortinetDocs, 2013)	107
Figura 151: Ingreso al equipo vía browser (FortinetDocs, 2013)	107
Figura 152: Puertos y componentes del Fortiwifi 30D (FortinetDocs, 2013)	108

INDICE DE TABLAS

Tabla 1: Tabla de datos para dimensionamiento de equipos UTM.....	31
Tabla 2: Cuadro comparativo Fortinet y Cisco (Elaboración Propia, 2017).....	36
Tabla 3: Presupuesto Referencial Solución FORTINET	37
Tabla 4: Presupuesto Referencial Solución CISCO	38
Tabla 5: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)	62
Tabla 6: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)	72
Tabla 7: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)	77
Tabla 8: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)	81
Tabla 9: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)	91

RESUMEN

Para la elaboración del presente proyecto, inicialmente se investigaron los conceptos tanto de redes, como de seguridad perimetral y se menciona los principales ataques que existen en la actualidad; además se realiza un análisis tanto técnico como de costos de las soluciones propuestas, para luego proceder con la elaboración del módulo para prácticas de Gestión Unificada de Amenazas orientada a los estudiantes de la Universidad Tecnológica Israel ubicada en Quito con la finalidad de que tengan una guía de trabajo orientada al ámbito de seguridad informática.

La Universidad Israel actualmente no cuenta con un equipo de gestión unificada de amenazas con el cual se pueda elaborar prácticas que ayuden a los estudiantes a asimilar los conocimientos pedagógicos y ponerlos en práctica. De allí nace la necesidad de elaborar una guía de prácticas de laboratorio, con conceptos básicos, para lograr mejorar los conocimientos de los futuros profesionales

El documento se encuentra estructurado por 4 capítulos, de los cuáles el capítulo 1 es la introducción y justificación del problema, el capítulo 2 se basará en la descripción y conceptos teóricos de cada uno de los elementos que forman parte de este proyecto, en el capítulo 3 se realiza la comparación con otras marcas y diseño del sistema de gestión unificado de amenazas, el capítulo 4 se realiza la implementación del módulo y elaboración de las prácticas y al final se presentan las conclusiones y recomendaciones respectivas.

Palabras Claves: Guía, UTM, seguridad, prácticas

ABSTRACT

For the preparation of the present project, the concepts of both networks and perimeter security were investigated and the principal attacks that exist are mentioned; In addition, a technical and cost analysis of the proposed solutions is carried out, to proceed with the elaboration of the module for Unified Threat Management practices aimed at the students of the Technological University Israel located in Quito with the purpose of having a guide of work oriented to the field of computer security.

The Israel University does not currently have a Unified Threat Management team with which practices can be developed to help students assimilate and implement pedagogical knowledge. From there arises the need to develop a guide to laboratory practices, with basic concepts, to improve the knowledge of future professionals

The document is structured by 4 chapters, of which chapter 1 is the introduction and justification of the problem, chapter 2 will be based on the description and theoretical concepts of each of the elements that are part of this project, chapter 3 the comparison with other brands and design of the unified threat management system is carried out, chapter 4 is carried out the implementation of the module and elaboration of the practices and at the end the conclusions and recommendations are presented.

Keywords: Guide, UTM, security, practices

1. INTRODUCCIÓN

Debido al incremento en los ataques de seguridad informática a las diferentes entidades ya sean estas privadas o de gobierno, se ha creado la necesidad de poseer redes seguras ante un posible ataque para prevenir el robo de información o pérdida de la misma que en cualquier entidad es el bien máspreciado, entre algunos de los ataques a la seguridad de la información se puede mencionar el *ransomware* Wannacry que se extendió a 150 países y unas 200.000 víctimas encriptando todos los datos almacenados en los dispositivos electrónicos (Hirschberger, 2017). Las empresas enfocadas en seguridad han desarrollado diferentes plataformas que permiten controlar el tráfico de los usuarios, prevenir ataques internos o externos y que se acceda a recursos internos de la entidad desde cualquier parte del mundo.

Fortinet es uno de los fabricantes de equipos para seguridad de la información que existen en el mercado, ofrece soluciones completas que permiten proteger la información, sin la instalación de equipos servidores.

En el presente proyecto se mostrará la forma adecuada de configurar un equipo de gestión unificada de amenazas de marca Fortinet, demostrando las funciones principales del equipo mediante el desarrollo de prácticas de laboratorio que permitan comprender los conceptos de seguridad perimetral y vulnerabilidades de las cuáles se puede ser víctima.

1.1. ANTECEDENTES

En los últimos años, con el constante desarrollo de la tecnología, la era digital, el Internet de las cosas, las empresas cada día dependen más de la tecnología, por lo que deben estar actualizados en esta área, de allí que es indispensable mantener un conocimiento actualizado en estos temas, más aún si desempeña una profesión en el ámbito de redes o informática.

Actualmente la Universidad Tecnológica Israel, cuenta con un laboratorio de redes, el cual no dispone con un equipo dedicado para desarrollar prácticas relacionadas con la seguridad de la información *Unified Threat Management* (UTM) Sistema Gestión Unificada de Amenazas, por lo tanto no existe una guía de laboratorio para que los estudiantes practiquen los fundamentos de prevención de seguridad informática en equipos de propósito específico para esta tarea.

Con la implementación del UTM Fortinet, se tendrá 6 prácticas para configurar equipos Fortigate, que servirán para la formación del estudiante.

1.2. EL PROBLEMA

1.2.1. Problema principal

El laboratorio dedicado a redes de la Universidad Israel no dispone de dispositivos de laboratorio para la gestión unificada de amenazas que permita controlar y administrar la red, ni de una guía de laboratorio para que los estudiantes practiquen los fundamentos de prevención de seguridad informática en equipos de gestión unificada de amenazas.

1.3. JUSTIFICACIÓN

Este proyecto tiene como finalidad elaborar un módulo para prácticas de laboratorio de gestión unificada de amenazas en la Universidad Israel, con fines educativos sobre seguridad, que permita proteger, controlar y administrar la gestión de una red a través de un sistema de gestión unificada de amenazas marca Fortinet. Con esta guía se logrará proporcionar al estudiante las herramientas para minimizar los riesgos de seguridad a los cuáles está expuesta la red interna de las empresas e instituciones, a través de control de accesos, denegación de servicios y protocolos de comunicación.

1.4. OBJETIVOS

1.4.1. Objetivo General

Elaborar un módulo de prácticas para programación básica de un sistema de gestión unificada de amenazas para el laboratorio de redes de la Universidad Tecnológica Israel.

1.4.2. Objetivos Específicos

- Analizar las tecnologías UTM Fortinet en la implementación de un sistema de gestión de amenazas.
- Determinar el equipamiento necesario para el desarrollo de las prácticas a ser propuestas.
- Diseñar varias prácticas con varios tópicos, que permitan ejercitarse en situaciones reales a las cuales se enfrentan en la vida laboral.
- Elaborar guías de laboratorio para estudiantes, que permitan desarrollar las destrezas y habilidades para configurar y poner en producción sistemas de gestión unificada de amenazas marca Fortinet.
- Realizar *troubleshooting* con problemas reales de experiencias adquiridas con la marca.
- Desarrollar la memoria técnica de la implementación del sistema.

2. FUNDAMENTACIÓN TEÓRICA

En este capítulo, nos introduciremos en el mundo de la seguridad informática, atravesaremos diferentes temáticas. Entre otras cosas, se abordará la nomenclatura y los conceptos básicos de redes de datos y seguridad informática basados en autores como Benchimol y fabricantes especialistas en tecnología de redes y seguridad informática tales como Cisco, Fortinet, Mikrotik, los cuales se describen a continuación:

2.1. INFRAESTRUCTURA DE RED Y COMUNICACIONES

Infraestructura de red son todos los componentes básicos y necesarios para cualquier institución pública o privada para el correcto funcionamiento de la plataforma informática. Es imprescindible un buen diseño de la misma para que el rendimiento de toda la plataforma sea el adecuado ya que es el medio físico desde donde se puede conectar los ordenadores y equipos de trabajo (NBcomunicaciones, 2017).

A continuación mencionaremos los principales conceptos y equipos que forma parte de una red de comunicaciones:

2.1.1 Tecnologías de redes

En la actualidad las telecomunicaciones utilizan diferentes tecnologías de redes para comunicar equipos entre ambientes de red LAN (*Local Area Network*) y WAN (*Wide Area Network*). Se puede utilizar una combinación de tecnologías para obtener la mejor relación costo-beneficio y la máxima eficacia del diseño de la red.

Según (León, 2006, p. 1), indica que hay muchas tecnologías de redes disponibles, entre las que se encuentran:

- *Ethernet*.
- *Token Ring*.
- Modo de transferencia asíncrona (*Asynchronous Transfer Mode, ATM*).
- Interfaz de datos distribuidos por fibra (*Fiber Distributed Data Interface, FDDI*).
- *Frame Relay*.

2.1.2 Red de computadoras

Una red de computadoras, se la denomina también red de telecomunicaciones, es un conjunto de equipos de red que se encuentran conectados entre ellos a través de equipos de *networking* tal es el caso de *switches*, *routers*, *access points*, entre otros, que brindan su

hardware para el transporte de datos, con la finalidad de compartir y transportar información multimedia (Michel, 2013)

A continuación describiremos los principales elementos que forman parte de una red.

2.1.3 Elementos de Red

Tal como lo mencionamos en una red de computadoras existen varios elementos que son necesarios para la comunicación de un dispositivo a otro, entre los principales elementos tenemos los siguientes:

2.1.3.1 El Switch

Es uno de los equipos de *networking*, conocido como conmutador de red su función principal es la de interconectar dispositivos dentro de una misma red LAN para resolver problemas de congestión, un *switch* puede interconectar equipos tales como servidores, impresoras, cámaras, controladoras *Wireless*, *firewall* entre otros, funcionando como controlador de red permitiendo a los dispositivos compartir todo tipo de información multimedia desde el origen al destino.

Existen *switches* no administrables y administrables. Los *switches* no administrables son conmutadores automáticos y no permiten realizar ningún tipo de configuración, a diferencia los *switches* administrables que permiten realizar varios tipos de configuración (Sergio Untiveros, 2016)

En la figura 1 se observa un *switch* marca Fortinet, capa 3 *Power over Ethernet* (POE).



Figura 1: Switch marca Fortinet 224D-POE (Fortinet, 2017)

2.1.3.2 El Router

Es un dispositivo conocido como enrutador, el cual permite asegurar el enrutamiento de paquetes entre diferentes redes o proporcionar el mejor camino que debe tomar el paquete de datos (Ecured, 2017). En la figura 2 se observa un *router* para empresas medianas marca Cisco.



Figura 2: Router marca Cisco (Cisco, 2016)

2.1.3.3 Protocolos de comunicación

Modelo OSI

El Modelo *Open System Interconnection* (Modelo OSI) Interconexión de Sistemas Abiertos, se encarga de analizar los distintos niveles o capas, desde que el mensaje es enviado del origen hacia el destino, además realiza un análisis jerárquico donde la capa inferior sirve a la capa superior. En la figura 3 se observa las siete capas que compone el modelo OSI.

El modelo de Interconexión de Sistemas Abiertos fue lanzado en 1984 como un modelo de red descriptivo. (Mikrotik, 2017)



Figura 3: Capas del Modelo OSI (Mikrotik, 2017)

Modelo TCP/IP

El modelo *Transmission Control Protocol / Internet Protocol* (TCP/IP) es un protocolo de red que fue desarrollado en los años 70, se utilizó en la red *Advanced Research Project Agency* (ARPANET) la primera WAN (Portatiles, 2014).

Este modelo es utilizado para comunicaciones en redes, que permite conectividad de extremo a extremo. En la figura 4 se pueden observar las cuatro capas del modelo TCP/IP.

El modelo TCP/IP es un protocolo más confiable de extremo a extremo en comparación al modelo OSI.

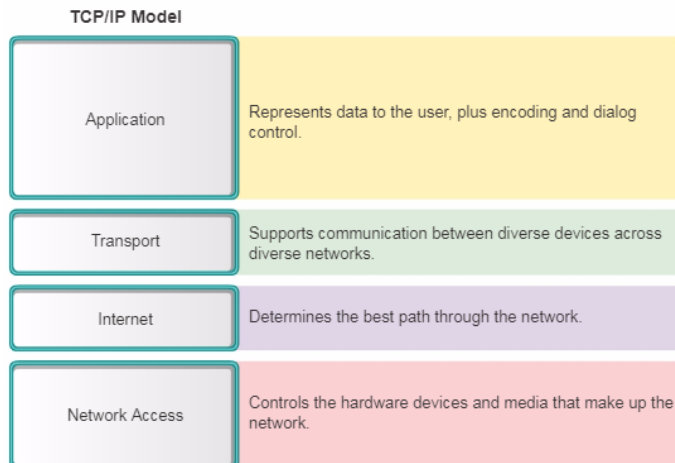


Figura 4: Capas del Modelo TCP/IP (Netacad, 2017)

2.1.3.4 Servidor

Es el elemento principal, capaz de compartir diferentes servicios o recursos para el resto de usuarios dentro de la empresa. Muchas veces es el servidor de las impresoras, control de acceso, servidor FTP (File Transfer Protocol), etc.

2.1.3.5 Estaciones de Trabajo

Es cada uno de los computadores o dispositivos conectados a la red, ya sea vía cableada o inalámbrica.

2.1.3.6 Cableado

La red LAN debe tener un sistema de cableado, que puede ser estándar de categoría 5e, 6, 6A, 7 o 7A. Este sirve para la conexión entre estaciones de trabajo y los servidores de archivos o periféricos (Valdez, 2013).

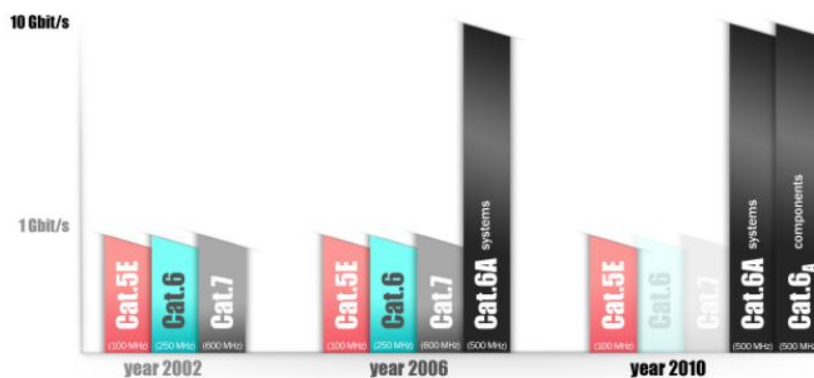


Figura 5: Categoría de cableado (Krugel, 2013)

2.1.3.7 Hub o Concentrador

Es un equipo que permite conectar entre sí los dispositivos de red, su principal desventaja es que generan demasiadas colisiones ya que retransmite los paquetes de datos hacia todos los puertos, razón por la cual ya no se utiliza actualmente (Valdez, 2013).

2.1.3.8 Punto de acceso inalámbrico (Wireless Access Point)

Un *Access Point* es un dispositivo que crea un *Wireless Local Area Network* (WLAN) en una oficina o edificio. Se conecta vía cable a un *router*, *switch* o *hub* y despliega una red inalámbrica a un área específica (Linksys, 2017).



Figura 6: Access Point marca Fortinet (Fortinet, 2017)

2.1.3.9 Firewall

Es un dispositivo de seguridad que permite proteger una computadora o una red de computadoras de amenazas externas específicamente provenientes del Internet.

El *firewall* se ha utilizado como protección de red, sin embargo las herramientas para realizar un ataque se han vuelto más especializadas y avanzadas, por lo que hoy en día un *firewall* puede ayudar a mitigar pero no proteger este tipo de amenazas (Cisco, 2016) .

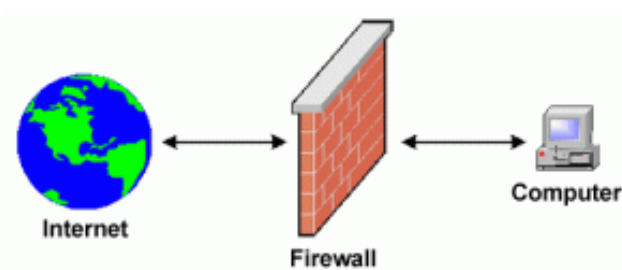


Figura 7: Firewall (Aportavalor, 2013)

2.2. SEGURIDAD INFORMÁTICA

A continuación se presentaran los términos más utilizados y conceptos relacionados que nos ayuden a entender a qué se refiere la seguridad informática.

2.2.1 Definición de Seguridad Informática

Es el estudio y aplicación de métodos y medios de protección para los sistemas de información y comunicación, al fin de prevenir el robo, destrucción o publicación de información confidencial (Benchimol, 2011) .

La seguridad de la información tiene por objetivo prevenir 3 propiedades fundamentales de cualquier sistema informático, los cuales son:

- Confidencialidad
- Integridad
- Disponibilidad

2.2.2 Seguridad de la Información

Con el transcurso del tiempo la seguridad informática se ha ido extendiendo a otras áreas, razón por la cual no solo se enfoca a informática sino que nace un nuevo concepto denominado como seguridad de la información.

La seguridad de la información no solo contempla los procesos por equipos informáticos y sistemas, también abarca aquello que pensamos, algún escrito confidencial como por ejemplo: procesos de contingencia y continuidad del negocio, leyes, normas, procedimientos y políticas internas propias de cada empresa (Benchimol, 2011).

En definitiva los responsables en seguridad de redes, son los responsables de mantener la seguridad de los datos de una organización y garantizar la integridad y confidencialidad de la información.

2.2.3 Seguridad Perimetral

La seguridad perimetral es un método de defensa de red, que su objetivo es proteger el perímetro de la red, es decir proteger la red interna del cliente, del acceso de usuarios no autorizados que estén conectados desde cualquier sitio en el internet (Multicom, 2017).

La seguridad perimetral no es un componente aislado sino una estrategia para proteger los recursos de una red conectada a internet, adicional que condiciona la credibilidad de una organización en internet.

Por ejemplo: Si un Banco ha sufrido un ataque y este ataque fue conocido a nivel mundial, los clientes o usuarios finales, no tienen las garantías necesarias que aseguren que su dinero, cuentas e identificación personal estén aseguradas y protegidas (Guardnet, 2011).

En la figura 8 el muro hace referencia a la seguridad perimetral del cliente.

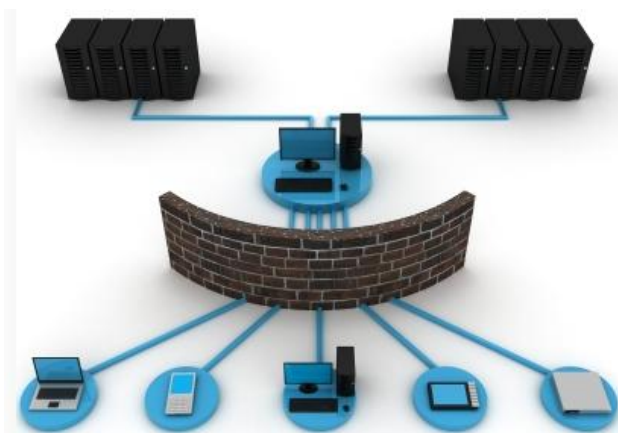


Figura 8: El muro simboliza la seguridad perimetral del cliente (Guardnet, 2011)

2.2.3.1 Para qué sirve la seguridad perimetral?

La seguridad perimetral sirve para cubrir los siguientes aspectos (Guardnet, 2011):

- Rechazar conexiones a servicios comprometidos
- Permitir sólo ciertos tipos de tráfico (p. ej. página web de la empresa) o entre ciertas sucursales
- Proporcionar un único punto de interconexión con el exterior (internet)
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet, es decir realizar un *Network Address Translation* (NAT)
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- Auditar el tráfico entre el exterior y el interior
- Ocultar información interna de la empresa

2.2.4 Protagonistas de ataques informáticos

Existen muchos términos que han sido mal utilizados por la sociedad, razón por lo cual vamos a mencionar cada uno de ellos y sus diferencias.

2.2.4.1 Hacker

El nombre hacker sirve para referirse a un experto (Gurú) en varias o algunas rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos (Cisco Networking Academy, 2016).

Cabe mencionar que un hacker es cualquier persona a la que le apasiona el conocimiento, le descubrimiento, el aprendizaje y el funcionamiento de las cosas.

El término hacker en el mundo profesional de seguridad informática es un honor ya que es una persona que ha logrado un gran conocimiento en una determinada actividad, de allí que el término es mal utilizado ya que no son piratas informáticos, ni cometen delitos.

Existen 3 tipos de Hacker:

- Black Hat Hacker.- Su principal desafío es romper reglas y para ello es necesario que aprenda muchas formas para cuidarse. Analizan un sistema como una caja cerrada y buscan todo lo que pueda ser vulnerable. Es necesario que deba pasar a ser un cracker sin hacer maldad.
- White Hat Hacker.- Tienen el conocimiento de la red del cliente y cuidan el medio interno de la red externa (Internet). Por lo general pueden estar en este grupo los especialistas u oficiales de seguridad de la institución.
- Gray Hat Hacker.- Es un hacker talentoso que algunas veces viola las leyes o estándares éticos, sin embargo lo usan para alertar a la empresa donde fue encontrada la vulnerabilidad para que puedan corregirla. Un ejemplo de este tipo de *hacker* es Chema Alonso que luego de ser un *Gray Hacker* pasó a trabajar a la empresa Telefónica.

2.2.4.2 Cracker

El nombre cracker proviene del inglés (crack = romper), que es una persona que viola la seguridad de un sistema similar a un *black* o *grey hacker*, sólo que a diferencia del hacker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo (Cisco Networking Academy, 2016).



Figura 9: Diferencia Hacker y Cracker (Greenetics, 2016)

2.2.4.3 Phreaker

Es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los sistemas telefónicos, telefonía móvil, tecnologías inalámbricas y el Voz sobre IP (VoIP) (Palacios, 2015).

Un ejemplo es Jhon Draper quien consiguió realizar llamadas gratuitas utilizando un pito de plástico, el cual emitía un tono a una frecuencia que utilizaba AT&T (*American Telephone and Telegraph*) para indicar que la línea telefónica estaba lista para rutear una llamada (Hacker.NET, 2017).

En la figura 10 se puede apreciar al primer Phreaker y el más famoso.



Figura 10: Jhon Draper, alias "Cap'n Crunch" (Hacker.NET, 2017)

2.2.4.4 Script Kiddies

Es quien utiliza programas creados por terceros sin conocer su funcionamiento, sin embargo están aprendiendo con libro en mano o capacitándose profesionalmente (Greenetics, 2016).



Figura 11: Script Kiddie (Geekistuff, 2014)

2.2.4.5 Hacktivistas

Son hackers o phreakers que utilizan o crean tecnología para conseguir un objetivo político o social. Para el país de los *United States* (EEUU) estas personas son un cracker.

Entre los principales grupos a nivel mundial se encuentran Wikileaks y Anonymous, quienes inclusive en el año 2012 llegaron a establecer una alianza entre ambos grupos (Norton, 2012).

En la figura 12 se observa los logos de ambos grupos:



Figura 12: Grupos Hacktivistas Wikileaks y Anonymous (Reyes, 2013)

2.2.4.6 Newbie o Neophyte

Significa principiante, es un joven de promedio entre 17 años, que intenta descargar algún software o aplicación para *hacking*, sin embargo no sabe ni cómo lograr instalarlo (Benchimol, 2011).

En la figura 13 se muestra las principales características que distinguen a un *newbie*.



Figura 13: Características de un Newbie (Greenetics, 2016)

2.2.4.7 Lammer

Son personas que presumen tener conocimientos que realmente no lo tienen, en otras palabras en un fanfarrón. Por lo general no son personas técnicas (Benchimol, 2011).

En resumen existen varios protagonistas en un ataque informático, que cuenta muchas veces con herramientas especializadas y diseñadas para un propósito específico.

Por el contrario no sucede con la persona encargada de la seguridad de la información en una institución sea pública o privada, que no cuenta con las herramientas adecuadas para contrarrestar estos ataques.

Adicional es indispensable ir actualizando los conocimientos para adquirir nuevas habilidades, ya que la velocidad con que avanza el mundo no espera y cada día existen ataques más especializados y complejos.

2.2.5 Amenazas y tipos de ataques en la red

Una amenaza es cualquier cosa que pueda alterar la operación, funcionalidad, disponibilidad o integridad de una red o sistema (Alulema, 2008).

Existen varios tipos de amenazas con diferentes técnicas cada vez más avanzadas y automatizadas, que pueden ser dirigidas al sistema operativo, a las aplicaciones, errores en configuraciones o errores en protocolos (Benchimol, 2011).

A continuación se describen las siguientes:

2.2.5.1 Malware

Con este nombre se conoce todo aquello que se cataloga como código malicioso (programas).

Generalmente, estas amenazas son detectadas por los antivirus, se trate de gusanos, spyware, troyanos, virus o scripts malintencionados (en rutina de tiempo o de ejecución).



Figura 14: Malware (Forospyware, 2009)

2.2.5.2 Virus

Es un software malicioso que se adjunta a otro programa para ejecutar una función indeseada específica en una computadora (Cisco Networking Academy, 2016).

2.2.5.3 Gusano

Malware que se multiplica explotando vulnerabilidades en las redes. Instala copias de sí mismo en la computadora infectada que luego infecta a otros hosts. Un gusano puede llevar un troyano (Cisco Networking Academy, 2016).

2.2.5.4 Troyano

Es un malware, que realiza operaciones maliciosas bajo el disfraz de una función.

2.2.5.5 Man in the middle

El atacante se ubica en medio de una comunicación válida entre dos equipos, logrando interceptar la misma.

Luego de comprometer la comunicación, el intercambio de datos entre estos dos equipos necesariamente deberá primero pasar por el atacante, logrando robo de accesos, *passwords* e inclusive robo de información.

En la figura 15 se puede apreciar cómo se realiza un ataque *man in the middle*.

2.2.5.6 DoS (Denegación de Servicio)

El ataque de DoS es un ataque de red que resulta en algún tipo de interrupción en el servicio a los usuarios, dispositivos o aplicaciones (Cisco Networking Academy, 2016).

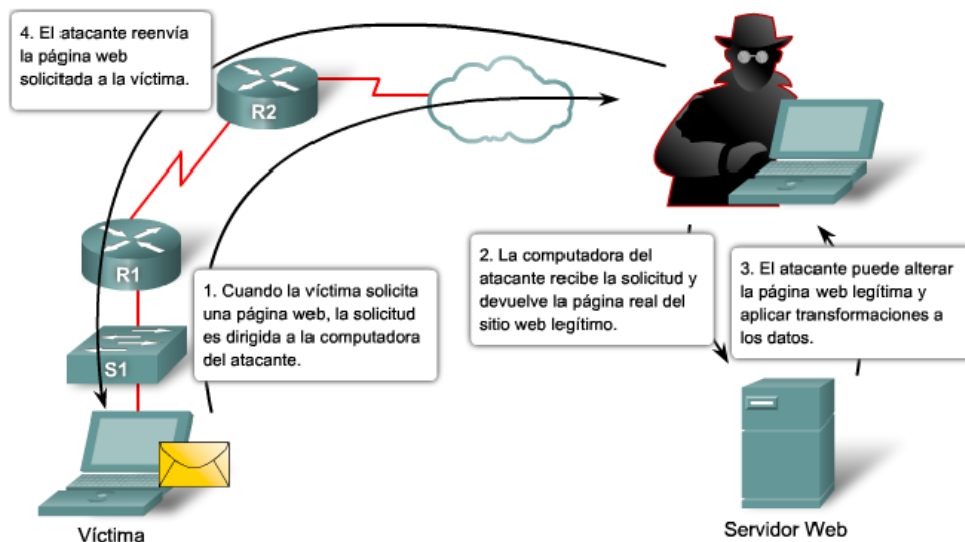


Figura 15: Ataque hombre en el medio (Cisco Networking Academy, 2016)

2.2.5.7 DDoS (Denegación Distribuida de Servicio)

Es similar en intención a un ataque DoS, excepto que un ataque DDoS se origina en múltiples fuentes coordinadas. Un ataque DDoS requiere al profesional de seguridad de red que identifique y detenga los ataques desde fuentes distribuidas a la vez que administra un incremento en el tráfico (Cisco Networking Academy, 2016).

En la figura 17 se puede observar un ataque DDoS, el cual muestra un ataque desde dos fuentes y varios dispositivos comprometidos llamados zombies realizando el ataque.

2.2.5.8 Ransomware

El *ransomware* es un tipo de ataque que encripta todos los datos de su víctima y pide un rescate a cambio de recuperar su información (Fortinet, 2017)

Esta encriptación es difícil de romper y descifrar.

Hoy en día es el tipo de ataque que es garantizado y rentable por los siguientes factores:

- Provee un retorno financiero inmediato, ya que sus víctimas pagan directamente y no necesitan vender información robada para hacer dinero.
- La moneda digital provee una vía fácil para pagos de *ransomware*, puesto que no existen transferencias ilegales y se desconoce el procedimiento de la transferencia y de la persona que recibe el pago.



Figura 16 Principales monedas digitales (Fortinet, 2017)

- Hay un cibercrimen por detrás de estos ataques, ya que hoy en día se puede comprar *ransomware* como servicio y existen algunas redes afiliadas creando este tipo de ataque (Fortinet, 2017) .

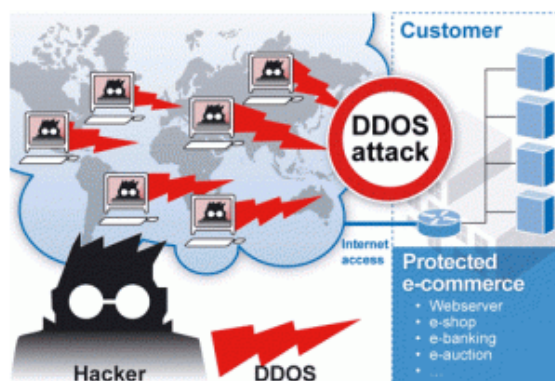


Figura 17: Ataque de Denegación de servicio (Seguridadweb20, 2015)

Con el objetivo de mitigar este tipo de ataques se crea empresas dedicadas a combatir el Cibercrimen en el mundo, innovando y creando dispositivos cada vez más inteligentes y a la vanguardia de la tecnología.

En el capítulo 3 se realiza un análisis comparativo entre dos fabricantes específicos que son viables para la implementación del sistema de gestión unificada de amenazas en la Universidad Israel y el Diseño del Sistema.

3. COMPARACIÓN CON OTROS FABRICANTES Y DISEÑO DEL SISTEMA DE GESTIÓN UNIFICADO DE AMENAZAS

Antes de realizar la comparación y análisis de las tecnologías utilizadas y el diseño del dispositivo adecuado, es importante entender (una vez revisado los protagonistas y los diferentes tipos de ataques) un concepto que ayudará a escoger que producto es el idóneo para este tipo de amenazas, para ello se revisara el concepto de UTM, que módulos forman parte del sistema y para que nos ayuda cada uno de los módulos.

3.1. UNIFIED THREAT MANAGEMENT (UTM) O GESTIÓN UNIFICADA DE AMENAZAS

Es un sistema de *hardware* y *software* específico para la seguridad informática en redes, el cual contiene una serie de módulos especializados para integrar seguridad inteligente en tiempo real, sin degradar su funcionamiento.

Los dispositivos UTM combinan las funciones de diferentes dispositivos de seguridad, administración y análisis en una sola plataforma (Fortinet, 2017) .

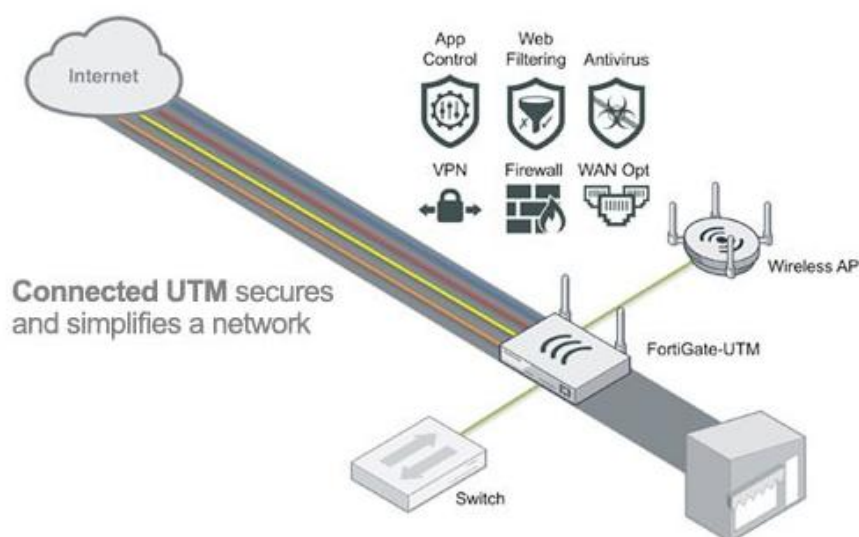


Figura 18: Componentes de Sistema UTM (Fortinet, 2017)

Luego del avance del internet fue necesario contar con una nueva tecnología de protección que sea menos compleja para administrar, más barata y más confiable.

El UTM existe porque resuelve 3 necesidades críticas:

1. Incrementar la seguridad.- Contar con políticas apropiadas, protección contra amenazas combinadas, contar con un tráfico limpio en la red.

2. Seguridad más eficiente.- Mayor performance y disponibilidad en la red, administrar el ancho de banda de la red del cliente, conseguir una mejor administración de mi sistema.
3. Rentabilidad.- Se tiene un retorno de la inversión, licencia única, bajos costos operacionales.

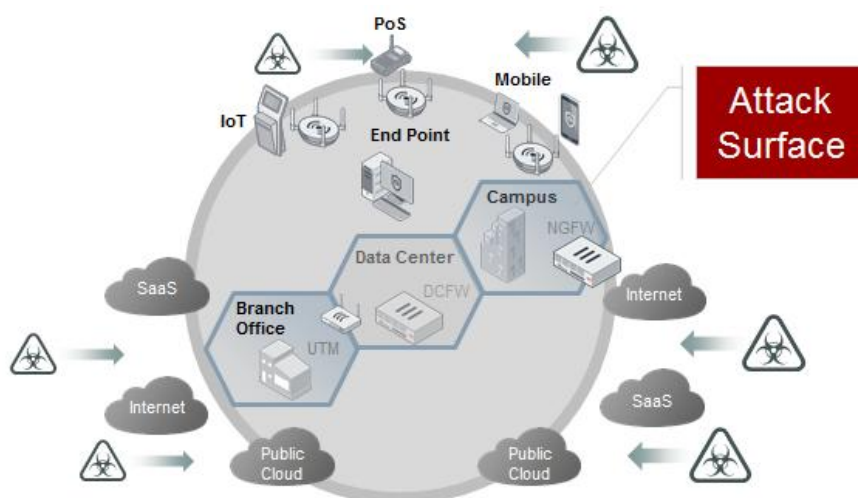


Figura 19: La superficie de ataque se ha expandido (Fortinet, 2017)

3.1.1 Componentes de un Sistema UTM:

Las empresas líderes en seguridad continuamente agregan funciones a los sistemas UTM y a la vez mantienen los principales componentes de otras soluciones enfocadas a la seguridad en la red como podemos mencionar las siguientes:

- Firewall

Es un dispositivo de seguridad que permite proteger una computadora o una red de computadoras de amenazas externas específicamente provenientes del Internet (Cisco, 2016).
- Intrusion Prevention System (IPS)

Su principal objetivo es identificar, registrar y bloquear ataques, evitando que tengan efecto (Ramos, 2011).
- Antivirus/Antispyware/Antimalware

Son sistemas que filtran contenido malicioso en canales de entrada a la red (Ramos, 2011).
- Antispam

Sistema que filtra contenido de correo basura o malicioso.

- Web Filtering
Permite el acceso y restricción de navegación vía browser a páginas web que utilicen los protocolos http (puerto 80) y https (puerto 443)
- Application Control
Permite el acceso y restricción de navegación y uso de aplicaciones que necesiten conexión a internet, por ejemplo *Teamviewer, Facebook, Spotify, Skype, etc.*
- Data Loss Prevention (DLP)
Son sistemas que ayudan a prevenir robo de información o contenido crítico de una entidad, se los usa por lo general en entidades bancarias o de gobierno.
- IPv6 Support
IPv6 es un protocolo de internet versión 6, diseñado para reemplazar al existente IPV4. Permitiendo que un mayor número de usuarios se comuniquen a internet o través de la red interna con una dirección IP que tiene mayor tamaño.
- IPSEC and SSL VPN
Redes privadas virtuales (*Virtual Private Network*), es un tipo de red que utiliza una infraestructura pública, por lo tanto no segura y creando un túnel virtual privado haciéndolo confiable.
- Traffic Shaping
Sistema que realiza control y restricción de ancho de banda.
- VoIP Support
Sistema que permite protección a la comunicación Voz sobre IP (VoIP)
- Routing
Router incorporado.
- WAN Optimization
Cache de navegación web cuando se usa navegación en modo proxy.
- DMZ
Zona Desmilitarizada. Es una red local ubicada entre la red interna y red externa que es utilizada para los servicios públicos que estarán expuestos al internet y por ende a los riesgos de seguridad.

Este tipo de tecnología ofrece una solución completa, sin afectar el rendimiento de la red interna del cliente, con bajo costo de operación y un buen retorno de capital.

Hoy en día es prioridad con los diferentes tipos de ataques contar con las herramientas adecuadas para evitar los mismos.

Adicional es importante conocer y entender los requerimientos del cliente antes de ofrecer una solución de seguridad.

3.2. PRINCIPALES REQUERIMIENTOS DEL CLIENTE

La mayoría de clientes necesita una solución completa y no varios equipos conectados a la vez, ya que esto implica más carga de trabajo al departamento de IT (*Information Technology*).

Es importante al momento de realizar el diseño, ofrecer una solución que cumpla con los siguientes parámetros:

- Agregar valor
- Confiabilidad
- Mejorar la seguridad
- Una buena integración con los servicios e infraestructura ya existente
- Que no afecte la experiencia del usuario final
- Demostrar ser la solución correcta.
- Un solo equipo de fácil administración

A continuación se realiza el análisis de dos soluciones planteadas en la Universidad Israel.

3.3. ANÁLISIS SOLUCIÓN FORTINET

Fortinet es una empresa multinacional de Estados Unidos con sede en Sunnyvale, California, es un líder en seguridad de la red a nivel mundial, fue fundada en el año 2000.

Su primer producto fue lanzado en el año 2002, desde entonces ha recibido más de 100 premios de industria como empresa y a sus productos.

Cuenta con varias certificaciones entre las que se puede mencionar ICSA (International Computer Security Association), NSS (Network Security Services), Certificaciones de Gobierno (FIPS-2 y Common Criteria EAL4+) e ISO 9001 (Fortinet, 2017).



Figura 20: Certificaciones Fortinet (Fortinet, 2017)

Los sistemas de seguridad Fortinet están basados sobre chips FortiASIC y sistema operativo FortiOS.

La tecnología FortiASIC acelera las funciones de red y seguridad, como escaneo de contenido, encriptación y procesamiento de paquetes de red, sin degradar el rendimiento de la red del cliente (Fortinet, 2017).

3.3.1 Tecnología FORTIASIC

Tal como mencionamos anteriormente, los sistemas de seguridad Fortinet, utilizan FortiASIC y constituyen hoy en día la nueva generación de red en tiempo real.

En la figura 20 se muestra la tecnología de hardware que usan los dispositivos Fortinet.

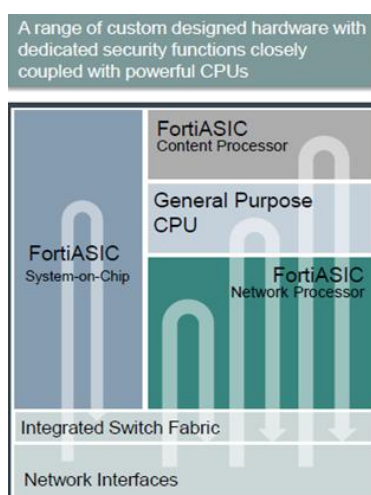


Figura 21: Hardware Sistemas Fortinet (Fortinet, 2017).

3.3.1.1 Content Processor

Acelera tareas intensivas de contenido y aplicación (IPS, AV)

3.3.1.2 Network Processor

Acelera tareas de seguridad (firewall, VPN)

3.3.1.3 System-on-chip

Une el FortiASIC-NP y FortiASIC-CP con CPU de propósito general, memoria e interfaces.

La tecnología FortiASIC ha ido evolucionando en el tiempo como se puede apreciar en la figura 20, partiendo en el año 2004 con una CP4 y hasta el 2015 el CP9.

En el año 2005 el NP1 y hoy en día contamos con el NP6.

En equipos de gama pequeña se encuentran los SoC 1 creado en el año 2010 hasta el SOC3 lanzado en el 2015.

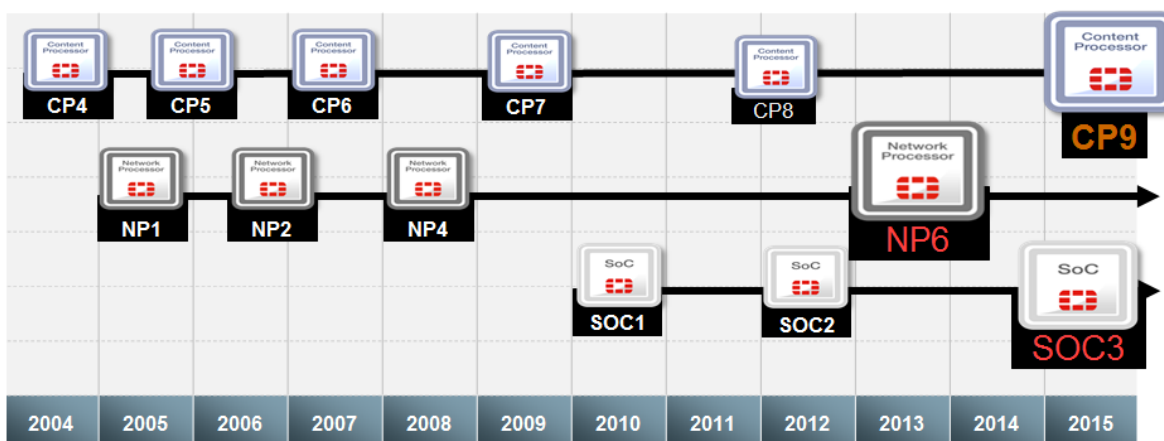


Figura 22: Ingeniería de Hardware de Fortinet (Fortinet, 2017).

La tecnología de FortiASIC logro catalogarlo en las pruebas de stress realizadas en el NSS Labs como el UTM más rápido del mundo.

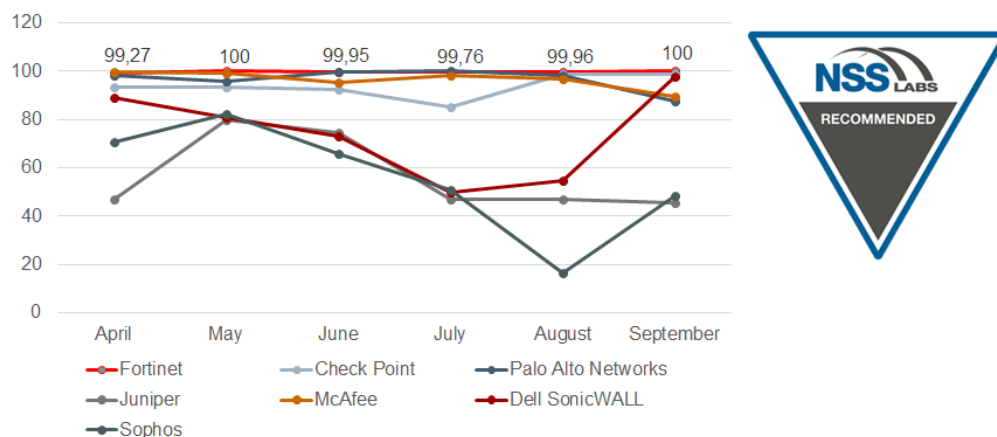


Figura 23: Comparación en pruebas realizadas NSS Labs (Fortinet, 2017).

3.3.2 Sistema Operativo FortiOS

Al igual que el hardware, el software de Fortinet se ha ido innovando y adaptándose a las nuevas tecnologías y funcionalidades.

Los dispositivos Fortinet pueden incluir los siguientes servicios:

- *Next Generation Firewall.*- Ofreciendo avanzada protección, detección y remediación de amenazas en un solo dispositivo.

- Prevención de Intrusos (IPS).- Mitigación de amenazas conocidas y desconocidas de ataques.
- Avanzada protección de antivirus y antispam.- Protección contra ataques dirigidos y persistentes provenientes de **malware**, el equipo logra detectar y bloquear el ataque.
- Control de Aplicación y filtrado URL.- Control de la capa de aplicación.
- Control de DLP (Data Loss Prevention). Prevenir el robo de información confidencial o crítica de una entidad. Soporta varias extensiones de documentos, por ejemplo Pdf, Word, Excel, etc.
- Routing.- Ruteo avanzado, NAT (Network Address Translation) y Alta disponibilidad y acceso vía VPN a través de Forticlient.
- Controladora Wireless.- Controladora de equipos propietarios Fortinet (FortiAP's)
- Conexión a Sanboxing.- Cuenta con integración a un equipo de sanboxing para prevenir ataques de día cero.
- Antimalware de dispositivos móviles.- Firmas especializadas para ataques de malware dirigidos y creados específicamente para dispositivos móviles
- Módulo WAF (Web Application Firewall).- Permite la protección exclusiva de servidores web contra determinados ataques, que un IPS o Firewall no puede proteger, por ejemplo: cross site scripting, sql injection.

En la siguiente figura se puede apreciar las bondades del Fortigate

Configuration	Log & Report	Diagnostics	Monitoring	Operation	Systems Integration	Central Mgmt. and Provisioning	Cloud & SDN Integration
					Visibility		
Policy Objects	Device Identification	SSL inspection	Actions	Policy and Control	AAA	Compliance	
Anti-Malware	IPS & DoS	Application Control	Web Filtering	Security	Advanced Threat Protection (ATP)		
Firewall	VPN	DLP	Email Filtering				
SD WAN	Explicit Proxy	IPv6	High Availability	Networking	Wireless Controller	Switch Controller	WAN Interface Manager
Routing/NAT	L2/Switching	Offline Inspection	Essential Network Services				
Physical Appliance (+SPU)	Virtual System	Hypervisor	Cloud	Platform Support	Security Fabric		

Figura 24: Evolución FortiOS y Módulos de Fortigate (Fortinet, 2017)

3.3.3 Servicios Fortinet

3.3.3.1 Fortiguard

Es un equipo de seguridad de ingenieros de Fortinet encargados de realizar las actualizaciones de todos los equipos Fortinet y todos los módulos de UTM, al igual que analizar los ataques de día cero y nuevas amenazas a nivel mundial.

Fortiguard de igual forma es la licencia de suscripción anual de UTM que incluye lo siguiente:

- Suscripción de *Antivirus*
- Suscripción de *Web Filter*
- Suscripción de *New Generation Firewall*
- Suscripción de *Antispam*

3.3.3.2 Forticare

Cubre la garantía de hardware del equipo y soporte de todos los productos Fortinet. Fortinet cuenta con un grupo de ingenieros de segundo nivel que pueden atender casos de soporte técnico sobre equipos Fortinet.

La licencia Forticare de igual forma permite actualizaciones de software de equipos Fortinet, mientras esté vigente la misma.

3.4. ANÁLISIS SOLUCIÓN CISCO ASA FIREPOWER

Cisco es una empresa global con sede en San José, California Estados Unidos, líder en lo que ha internet y dispositivos de red se refiere. La palabra Cisco proviene de la ciudad donde fue fundada en el año de 1984 (Cisco, 2017).

Su primer producto exitoso fue el *router* Cisco 12000 en el año de 1997, este fue su primer *router* en entregar equipos escalables, confiables y de alto rendimiento (Maestrosdelweb, 2007).

Cuenta con varias certificaciones y premios a nivel mundial en su área fuerte que es el *networking*.

En esta ocasión revisaremos la familia de sus productos *Next Generation Firewall*, el Cisco *Adaptive Security Appliance* (ASA) es un sistema operativo, el cual ofrece funcionalidades de firewall empresarial, adicional cuenta con un módulo de IPS y VPN.

Los sistemas ASA están basados en su software propietario IOS, sin embargo por aparición de ataques cada vez más sofisticados fue necesario la adquisición en el 2013 de Sourcefire un líder en soluciones inteligentes de ciberseguridad, creando su nuevo producto Cisco Firepower, pasando de ser un firewall a un UTM.

3.4.1 Tecnología Cisco ASA Firepower

Cisco en los últimos años ha demostrado innovación constante en sus productos adquiriendo Firepower y Meraki para brindar soluciones de UTM.

Firepower viene embedido como un componente adicional dentro del software ASA, para activarlo es necesario habilitarlo y dar de alta el servicio.

Entre las capacidades que ofrece la solución Cisco ASA con Firepower, tenemos las siguientes:

- VPN site to site y acceso remoto a través de VPN para brindar seguridad en las conexiones desde clientes que se conecten a la oficina principal.
- Granular visibilidad y control de aplicaciones de riesgo, cuenta con una base de datos de firmas de riesgo conocidas alrededor de 4000 aplicaciones.
- Provee alta efectividad en la prevención de riesgos y con una respuesta de autodefensa inteligente.
- Reputación y categorización de filtrado web, contando con más de 80 categorías
- *Advanced Malware Protection (AMP)* provee un efectivo *Sanboxing* que ayuda a descubrir, entender y bloquear malware (Cisco, 2016).

3.4.2 Servicios y funciones de Cisco ASA Firepower

Los dispositivos Cisco ASA pueden incluir los siguientes servicios:

- *Next Generation Firewall*.- Ofreciendo avanzada protección, detección y remediación de amenazas en un solo dispositivo.
- Prevención de Intrusos (IPS).- Con su módulo NGIPS (*Next Generation IPS*) de SourceFire logra una alta protección y mitigación de amenazas conocidas y desconocidas.
- Avanzada protección de malware.- Protección contra ataques dirigidos y persistentes provenientes de malware, el equipo logra detectar, bloquear, dar seguimiento, analizar y remediar el ataque.

- Incluye el firewall ASA.- Ruteo avanzado, NAT (Network Address Translation) y Alta disponibilidad y acceso vía VPN a través de Cisco AnyConnect VPN.
- Control de Aplicación y filtrado URL.- Control de la capa de aplicación.

En la figura 24 podemos observar los servicios que proporciona el Cisco ASA en conjunto con Firepower.



Figura 25: Servicios de Cisco ASA con Firepower (Cisco, 2016)

3.5. COMPARACIÓN DE TECNOLOGÍAS UTM: FORTINET Y CISCO ASA FIREPOWER

De acuerdo al estudio realizado de las tecnologías mencionadas se obtiene las siguientes características que la hacen la solución FORTINET sea la adecuada para el presente proyecto.

La tecnología ofrecida por FORTINET presenta la solución más apropiada en relación a UTM, ya que actualmente lidera el mercado de acuerdo a un estudio realizado por la empresa Gartner.

Gartner es una empresa de investigación y consultora especializada en Tecnologías de la Información (Gartner_Inc, 2017), quien año tras año evalúa todas las marcas líderes en el mercado, basándose en una medición de marketing y encuestas entre empresas líderes en tecnología.

De acuerdo a Gartner, en la siguiente figura se puede apreciar el reporte de las marcas líderes a nivel mundial con fecha a Junio del 2017. En la cual los tres primeros lugares en el cuadrante de Líderes lo ocupan:

1. - Fortinet
2. - Check Point

3. - Sophos



Figura 26: Firewall Multifunción en Small Medium Bussiness (Gartner, 2017)

Adicionalmente los equipos UTM de Fortinet, previenen ataques simultáneos, soportando aplicaciones exigentes, con su tecnología FortiASIC, logrando mantener el rendimiento de la red y el control en la seguridad perimetral.

La tecnología ofrecida por CISCO se encuentra aún innovando, por lo que al momento se presenta como una alternativa de conectividad más que de seguridad, aunque logro incorporar el módulo de Firepower, no cuenta aún con un enfoque exclusivo en seguridad perimetral, ni con todos los módulos que forman parte hoy en día de un UTM.

3.6. DISEÑO DEL MÓDULO PARA PRÁCTICAS DE LABORATORIO DE GESTIÓN UNIFICADA DE AMENAZAS EN LA UNIVERSIDAD ISRAEL

En esta parte se realizará el análisis técnico, beneficios y costos entre las dos soluciones, se logra definir la solución que cumpla con los requerimientos adecuados y que sea la más idónea para la elaboración del módulo para prácticas de laboratorio de gestión unificada de amenazas en la Universidad Israel.

Es necesaria una interfaz gráfica de administración ya que es mucho más fácil para el estudiante realizar las configuraciones y entender de manera adecuada las prácticas enfocadas a seguridad perimetral, que hoy en día es una de las ramas mejor pagadas en el área de tecnología.

3.6.1 Alcance

El diseño está basado en un equipo que ofrezca todas las funcionalidades de un UTM, de igual forma se realizará una guía de prácticas básicas aplicadas actualmente en la mayoría de clientes, basados en las mejores prácticas de acuerdo a la experiencia adquirida en el producto.

Adicionalmente se realizará la documentación de la red mediante diagramas e información de importancia.

3.6.2 Criterios del diseño y dimensionamiento del equipo

La tecnología UTM deberá satisfacer las diferentes necesidades de seguridad que existen en la actualidad, adicional en un equipo de seguridad perimetral es importante su dimensionamiento, para ello se deben tomar en cuenta los siguientes requerimientos descritos en la tabla 1:

Dimensionamiento Fortigate					
1. ¿Poseen Uds. algún sistema o appliance de seguridad para su red interna? Si la respuesta es sí, especifique.					
SI		NO	X	COMENTARIOS:	
2. ¿Cuántas conexiones concurrentes tiene, especificar en el caso más alto?					
N/A					
3. ¿Cuántos enlaces de datos o internet dispone su empresa y capacidad de cada uno de los enlaces?					
SI	x	NO		COMENTARIOS:	1 Enlace de Internet
4. ¿De cuántos usuarios está compuesta su red? (Incluir hosts alámbricos e inalámbricos, invitados y otros dispositivos de red con acceso a sus enlaces de datos o a internet, todo dispositivo que tenga una IP)					
SI	X	NO		COMENTARIOS:	20 hosts
5. ¿Requiere de alta disponibilidad?					
SI		NO	X	COMENTARIOS:	
6. ¿El cliente requiere redundancia en fuentes de poder?					
SI		NO	X	COMENTARIOS:	
7. ¿Crecimiento en número de usuarios en 3 años?					
SI		NO	X	COMENTARIOS:	
8. ¿Tienen usuarios que se conectan a su red mediante medios externos como VPNs?					
SI		NO	X	COMENTARIOS:	
9. Si la respuesta es sí, especifique el número y tipo de VPN.					
SI		NO	X	COMENTARIOS:	
10. ¿Tienen algún sistema de autenticación para sus usuarios? Si la respuesta es afirmativa, especifique.					
SI		NO	X	COMENTARIOS:	

11. ¿Desea que este sistema de autenticación se conecte al dispositivo de seguridad de su red para dar acceso a sus usuarios?					
SI		NO	X	COMENTARIOS:	
12. ¿Su empresa tiene sucursales? Si la respuesta es sí se desearía incluirlas en la solución de seguridad?. La salida hacia en internet es desde la matriz?					
SI		NO	X	COMENTARIOS:	
13. ¿Los servidores de correo electrónico son administrados por Uds?					
SI		NO	X	COMENTARIOS:	
14. ¿Poseen Uds. problemas de SPAM en sus cuentas de correo electrónico corporativo?					
SI	X	NO		COMENTARIOS:	
15. ¿Qué funcionalidades desea incluir en su sistema de seguridad perimetral(Firewall, Filtrado WEB, control de aplicaciones, IPS/IDS, Antivirus, Prevención de fuga de información, AntiSpam)?. Especifique.					
SI	X	NO		COMENTARIOS:	Todos
16. ¿Le gustaría incluir en la solución de seguridad perimetral un sistema de análisis de bitácoras (Logs) que permita crear reportes personalizados?					
SI		NO	X	COMENTARIOS:	
17. Detallar el tipo y cantidad de interfaces de red que se requeriría en el equipo de seguridad, como por ejemplo Ethernet 10/100 - 10/100/1000, Fibra Óptica, etc.					
SI	X	NO		COMENTARIOS:	10/100/1000 .Al menos 4 interfaces
18. Tipo de soporte requerido (8x5 o 24x7)					
8X5					
19. Periodo de licenciamiento?					
1 año					

Tabla 1: Tabla de datos para dimensionamiento de equipos UTM

De acuerdo a la información obtenida en la Tabla 1, ya que el laboratorio de redes tiene una capacidad máxima de 20 estudiantes, se define las capacidades necesarias con respecto a hardware y software que cubran la necesidad del cliente.

Se toma en consideración la hoja de especificaciones de cada fabricante y el modelo ideal que cumpla con las expectativas del mismo.

Como la cantidad de usuarios no va a ser mayor a 20 usuarios tomaremos en cuenta un modelo de equipo por cada marca mencionada anteriormente.

De acuerdo a las especificaciones técnicas requeridas, existen dos modelos a escoger los cuales son el Cisco ASA 5506W-X y Fortiwifi 30D.

Una vez dimensionado el equipo, se realiza el análisis tanto de capacidades, como de costos de las dos marcas escogidas.

3.6.3 Análisis del dispositivo UTM

3.6.3.1 FORTINET

El Fortiwifi 30D es un equipo dedicado para oficinas y hogares pequeños, el cual es un equipo fácil de implementar y se configura a través de una sola interfaz GUI (*Graphical User Interface*).

Las especificaciones técnicas del Fortiwifi 30D son las que se muestran a continuación:

	FORTIGATE 30D	FORTIWIFI 30D	FORTIGATE 30D-POE	FORTIWIFI 30D-POE
Hardware Specifications				
GE RJ45 WAN Ports	1	1	1	1
GE RJ45 Switch Ports	4	4	3	3
GE RJ45 PoE Ports	–	–	1	1
Wireless Interface	–	802.11 a/b/g/n	–	802.11 a/b/g/n
USB Ports (Client / Server)	–	–	1 / 1	–
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)				800 / 800 / 800 Mbps
Firewall Latency (64 byte UDP packets)				8 μ s
Firewall Throughput (Packets Per Second)				1.2 Mpps
Concurrent Sessions (TCP)				200,000
New Sessions/Second (TCP)				3,500
Firewall Policies				5,000
IPsec VPN Throughput (512 byte packets)				350 Mbps
Gateway-to-Gateway IPsec VPN Tunnels				20
Client-to-Gateway IPsec VPN Tunnels				250
SSL-VPN Throughput				25 Mbps
Concurrent SSL-VPN Users (Recommended Maximum)				80
IPS Throughput (HTTP / Enterprise Mix)				150 / 35 Mbps
SSL Inspection Throughput				30 Mbps
NGFW Throughput				18 Mbps
Maximum Number of FortiAPs (Total / Tunnel Mode)				2 / 2
Maximum Number of FortiTokens				20
Maximum Number of Registered FortiClients				10
Dimensions				
Height x Width x Length (inches / mm)	1.38 x 7.17 x 5.24 inches (35 x 182 x 133 mm)			
Weight	0.7 lbs (0.3 kg)			
Form Factor	Desktop			
Environment				
Power Required	100–240VAC, 50–60 Hz			
Maximum Current	110 V / 1.0A, 220 V / 0.5 A		110 V / 1.0A, 220 V / 0.5 A	
Total Available PoE Power Budget*	15.4 W		15.4 W	
Power Consumption (Average / Maximum)	16.2 / 25.6 W		18.7 / 28.6 W	
Heat Dissipation	87 BTU/h		98 BTU/h	
Operating / Storage Temperature	32–104°F (0–40°C) / -31–158°F (-35–70°C)			
Humidity	10–90% non-condensing			
Operating Altitude	Up to 7,400 ft (2,250 m)			
Compliance				
Safety	FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB			
Certifications				
ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN				

Figura 27: Especificaciones Técnicas del Dispositivo Fortinet (FortinetDocs, 2013).

FG/FWF-30D Series	
Systems	
VDOM Support	
High Availability (HA)	CLI
FortiCarrier License Upgrade	
Networking	
Link Aggregation/Redundant Ports for HA	
VLAN	CLI (20 max)
VLAN Switch Mode	
DNS Server	
WAN Optimization, Web Caching	
Explicit Proxy	CLI
Dynamic Routing/ Policy Routing	•
Switch Controller	
Wireless Controller	CLI
Firewall	
Traffic Shaping	•
Server Load Balancing	
SSL Content Inspection	•
SSL Offloading	
SSH Proxy	
User/Device based Policies	•
FSSO/ Remote Authentication Services	•
UTM	
AV Quarantine	
IPS Extended DB	•
DoS Protection	CLI
DLP Fingerprinting	
Vulnerability Scan	
Endpoint Control	•
VPN	
L2TP client	CLI
SSL VPN	•
ARIA-SEED IPsec support	
Log & Reporting	
Memory Logging	CLI
Disk Logging	
Local Reporting	
FortiView Historical Data	

Figura 28: Características de Seguridad del Dispositivo Fortinet (FortinetDocs, 2013)

3.6.3.2 CISCO

El Cisco ASA 5506W-X es un equipo dedicado para pequeñas empresas. Cuenta con una interfaz para el ASA y es necesario levantar la interfaz de Firepower para acceder a los servicios de UTM.

La administración se realiza a través del Software ASDM de Cisco ASA.

High availability ⁴	Requires Security Plus License; Active/ Standby	Requires Security Plus License; Active/ Standby	Active/ Standby	Active/ Active and Active/ Standby	Active/ Active and Active/ Standby	Requires Security Plus License; Active/ Active and Active/ Standby	Active/ Active and Active/ Standby	Active/ Active and Active/ Standby
Integrated Wireless Access Point (See Cisco AP 702 datasheet for WiFi technical details)	N/A	Wireless Bands a/b/g/n; Max n wifi throughput 54 Mbps; internal antenna only; local management or centralized via Cisco WLC	N/A	N/A	N/A	N/A	N/A	N/A
Expansion slot	N/A	N/A	N/A	N/A	N/A	1 interface card	1 interface card	1 interface card
User-accessible Flash slot	No	No	No	No	No	No	No	0
USB 2.0 ports	USB port type 'A', High Speed 2.0	USB port type 'A', High Speed 2.0	USB port type 'A', High Speed 2.0	USB port type 'A', High Speed 2.0	USB port type 'A', High Speed 2.0	2	2	2
Integrated I/O	8 x 1 Gigabit Ethernet (GE)	8 x 1GE	4 x 1GE	8 x 1GE	8 x 1GE	6 GE copper	6 GE copper	8 GE copper

Dedicated management port	Yes (To be shared with FirePOWER Services), 10/100/1000	Yes (To be shared with FirePOWER Services), 10/100/1000	Yes (To be shared with FirePOWER Services), 10/100/1000	Yes (To be shared with FirePOWER Services), 10/100/1000	Yes (To be shared with FirePOWER Services), 10/100/1000	Yes (1 GE)	Yes (1 GE)	Yes (1 GE)
Serial ports	1 RJ-45 and Mini USB console	1 RJ-45 and Mini USB console	1 RJ-45 and Mini USB console	1 RJ-45 and Mini USB console	1 RJ-45 and Mini USB console	1 RJ-45 console	1 RJ-45 console	1 RJ-45 console
Solid-state drive	50 GB mSata ⁶	50 GB mSata ⁶	50 GB mSata tested for heat	80 GB mSata ⁶	100 GB mSata ⁶	1 slot, 120 GB multiline configurator self-encrypting drive (MLC SED)	1 slot, 120 GB MLC SED	1 slot, 120 GB MLC SED
Memory	4 GB	4 GB	4 GB	8 GB	8 GB	4 GB	8 GB	8 GB

Operating Parameters								
Temperature	32 to 104°F (0 to 40 °C)	32 to 104°F (0 to 40 °C)	-4 to 140°F (-20 to 60 °C)	32 to 104°F (0 to 40 °C)	32 to 104°F (0 to 40 °C)	23 to 104°F (-5 to 40°C)	23 to 104°F (-5 to 40°C)	23 to 104°F (-5 to 40°C)
Relative humidity	90 percent noncondensing	90 percent noncondensing	95 percent noncondensing	10 to 90 percent noncondensing	10 to 90 percent noncondensing	10 to 90 percent noncondensing	10 to 90 percent noncondensing	90 percent
Altitude	Designed and tested for 0 to 10,000 ft (3048 m)	Designed and tested for 0 to 10,000 ft (3048 m)	Designed and tested for 0 to 10,000 ft (3050 m)	Designed and tested for 0 to 10,000 ft (3048 m)	Designed and tested for 0 to 10,000 ft (3048 m)	Designed and tested for 0 to 15,000 ft (4572 m)	Designed and tested for 0 to 15,000 ft (4572 m)	Designed and tested for 0 to 10,000 ft (3050 m)
Acoustic noise	Fanless 0 dBA	Fanless 0 dBA	Fanless 0 dBA	41.6 A-weighted decibels (dBA) type	41.6 dBA type	64.2 dBA max	64.2 dBA max	64.2 dBA max
				67.2 dBA max	67.2 dBA max			

Figura 29: Especificaciones Técnicas del Dispositivo Cisco (Cisco, 2016)

3.6.3.3 Análisis de los Dispositivos UTM presentados.

A continuación se realiza un cuadro comparativo y de evaluación tanto del producto Fortinet como Cisco, para ver si cumplen con las especificaciones técnicas basándose en los requerimientos necesarios de la Tabla 1.

	FORTIWIFI 30D	CISCO ASA 5506-W
Características Mínimas	Características Ofrecidas	Características Ofrecidas
Características Generales		
Interfaces al menos 4	5 Interfaces GE	8 Interfaces GE
Manejo de ancho de banda	Si	Si

Conexiones Simultaneas mínimo 50000	200000	50000
Nuevas Conexiones por segundo mínimo 3500	3500	5000
Servicio para 20 usuarios	20	Indefinido
Soporte de acceso seguro (SSH,HTTPS)	Si	Si
Soporte para VLANs	Si	Si
Características de seguridad		
Throughput Firewall mínimo 700 Mbps	800 Mbps	750 Mbps
Throughput Antivirus mínimo 30 Mbps	30 Mbps	No aplica
Throughput IPS mínimo de 100 Mbps	150 Mbps	125 Mbps
Throughput VPN mínimo de 100 Mbps	350 Mbps	100 Mbps
Soporte de Proxy	Si	Si
Filtrado Web	Si	Si
Control de Aplicaciones	Si	Si
Antispam	Si	No aplica
Antivirus	Si	No aplica
Data Loss Prevention	Si	No aplica
Wireless Controller	Si	No aplica
Web Application Firewall	Si	No aplica
Interfaz Wireless 802.11 a/b/g/n	Si	Si
Licencia UTM de 1 año	Si	Si

Tabla 2: Cuadro comparativo Fortinet y Cisco (Elaboración Propia, 2017)

Los dispositivos analizados cumplen con los requerimientos necesarios, sin embargo existe cierta diferencia en los siguientes aspectos:

- Conexiones simultáneas Fortinet cuenta con 200000 conexiones a comparación de Cisco con 50000, lo cual representa a futuro podría presentar una degradación de rendimiento de la red con el equipo Cisco.
- La capacidad de usuarios conectados a internet cumple con ambos dispositivos, con Fortinet cumple la capacidad mínima de 20 usuarios en full UTM, sin embargo si no se realiza este tipo de navegación esto puede soportar hasta 30 usuarios. Cisco no tiene especificado de acuerdo a su hoja de especificaciones técnicas.
- En relación a un resumen de throughput de los diferentes servicios, podemos notar que Fortinet logra un mejor rendimiento en comparación a Cisco, gracias a su tecnología dedicada de procesadores FortASIC.
- Cisco no cuenta con los módulos de *Antispam*, *Antivirus*, *Data Loss Prevention*, *Web Application Firewall*, que Fortinet los tiene incorporado sin pagar suscripción adicional, ni equipos adicionales.

Por lo tanto se concluye que la mejor propuesta técnica se encuentra en este orden:

1.- Fortinet.

2.- Cisco.

3.6.4 Análisis de costos

El análisis de costos que se presenta a continuación contiene el detalle del precio relacionado tanto a Hardware, Software, Garantía y Suscripción Anual (licencias) de las soluciones estudiadas y ofertadas en el presente proyecto, para poder comparar aspectos como precio, funcionalidad y viabilidad, de esta forma finalmente se puede recomendar la mejor solución de seguridad tanto en precios, como en características técnicas.

3.6.4.1 Costo de la solución FORTINET



IMAGEN	DESCRIPCIÓN DE LOS EQUIPOS	CANT	V. UNITARIO	V.TOTAL (USD)
	FORTIGATE 30-D Hardware plus 1 year 8x5 Forticare and Fortiguard UTM Bundle	1	\$ 1100	\$ 1100
	PATCH-CORD CATEGORIA 6-E	2	\$ 5	\$10
SUBTOTAL				\$1110
+ 12%				143,2
TOTAL				1253,20

Tabla 3: Presupuesto Referencial Solución FORTINET

3.6.4.2 Costo de la solución CISCO

IMAGEN	DESCRIPCIÓN DE LOS EQUIPOS	CANT	V. UNITARIO	V.TOTAL (USD)
	CISCO ASA 5506W-X Wifi Chassis + 1 year Subscriber Bundle	1	\$ 2300	\$ 2300
	PATCH-CORD CATEGORIA 6-E	2	\$ 5	\$10
			SUBTOTAL	\$2310
			+ 12%	\$277,20
			TOTAL	2587,20

Tabla 4: Presupuesto Referencial Solución CISCO

Luego de revisar los alcances, garantías, servicios y funciones de los equipos, vemos que ambas tecnologías se ajustan a los objetivos de este proyecto, sin embargo por funcionalidades y costo del equipo, quedaría descartada la solución de Cisco, por lo que se recomienda optar por la solución de FORTINET.

3.7. ESPECIFICACIONES TÉCNICAS DEL UTM A IMPLEMENTARSE

De acuerdo a los datos obtenidos como capacidad de usuarios, ancho de banda, sesiones concurrentes y *throughput*, se dimensiona el modelo de UTM necesario para la implementación en el laboratorio de redes de la Universidad Israel.

El equipo a implementarse es el UTM marca Fortinet, modelo Fortiwifi 30D, que cuenta con una interfaz Wireless permitiendo lograr de una manera más fácil la conexión y el acceso al equipo.

3.7.1 Hardware

Las especificaciones técnicas de hardware del equipo son las siguientes:



Figura 30: Especificaciones de Hardware Fortiwifi 30D (FortinetDocs, 2013)

Como podemos observar en la figura anterior el equipo cuenta con (FortinetDocs, 2013):

- 4 Puertos RJ45 10/100/1000 en modo Switch
- 1 Puerto RJ45 10/100/100 para WAN
- Interfaz Wireless que soporta protocolo 802.11 a/b/g/n
- FostiASIC SPU SOC2
- Puerto USB, para conexión de un Modem 3G/4G vía USB compatible con el equipo, para proveer opcional redundancia de internet
- Puerto USB-MGMT para administración vía USB con programa Fortiexplorer
- Botón de reset
- Entrada para fuente de poder
- Leds de status

3.7.2 Software y Rendimiento

El equipo cuenta con un software propietario llamado FortiOS el cual nos permite controlar toda la seguridad y capacidad de la red, que está cruzando sobre el sistema con un software fácil de administrar y con visualización efectiva.

El sistema FortiOS cuenta con una plataforma consolidada que contiene toda la administración tanto del firewall como del servicio UTM en una sola interfaz a diferencia de otros fabricantes que necesitan múltiples accesos para controlar cada una de sus aplicaciones.

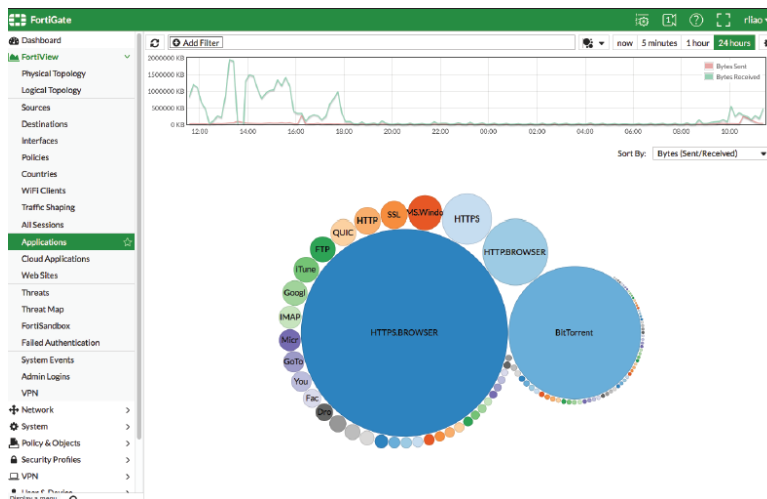


Figura 31: FortiOS versión 5.4 visualización de aplicaciones (FortinetDocs, 2013)

En la siguiente figura podemos observar las capacidades del Fortiwifi 30D en relación a rendimiento del hardware.

Hardware Performance			
Firewall Throughput (1518/512/64)	800 / 800 / 800 Mbps	IPS Throughput	150 Mbps
Firewall Latency	8 μs	Antivirus Throughput (Proxy Based)	30 Mbps
Concurrent Sessions	200 K	Virtual Domains (Default / Max)	-
New Sessions/Sec	3.5 K	Max Number of FortiAPs (Total/Tunnel)	2/2
Firewall Policies	200	Max Number of FortiTokens	20
IPSec VPN Throughput	350 Mbps	Client-to-Gateway IPSec VPN Tunnels	250
SSL-VPN Throughput	25 Mbps	Concurrent SSL-VPN Users (Recommended Max)	80

Figura 32: Especificaciones técnicas del rendimiento del equipo (FortinetDocs, 2013)

	FG-30D
Storage	-
WiFi Variant	✓
POE Variant	(1x GE)
Firewall & VPN Performance	✓✓
UTM Performance	✓
Port Density	✓✓
Ideal Use Cases	Small branch offices , Kiosks
	Site-Site VPN
	limited UTM & features, central logging

Figura 33: Especificaciones adicionales Fortiwifi 30D (FortinetDocs, 2013)

	FWF30D
Thick AP	✓
Wireless Controller	Yes (CLI)
#of WiFi radios	1
Supported Std	a/b/g/n
802.11n	2x2 MIMO
Max wireless association rate total	300Mbps
SSID's (incl. reserved)	8
Max FortiAP (Total/ Local Bridge)	2 / 2

Figura 34: Especificaciones Wireless (FortinetDocs, 2013)

4. IMPLEMENTACIÓN DEL MÓDULO Y ELABORACIÓN DE GUÍAS DE PRACTICA DE LABORATORIO.

Luego de realizar el diseño del módulo y escoger el equipo marca Fortinet, modelo Fortigate 30D, para elaborar el módulo, se instala el mismo en el laboratorio de redes de la UISRAEL, se realiza la configuración básica de acuerdo al siguiente diagrama de red propuesto, adicional se prueba la conexión al sistema vía Wireless desde una laptop de un usuario final, simulando la conexión de un alumno al equipo.

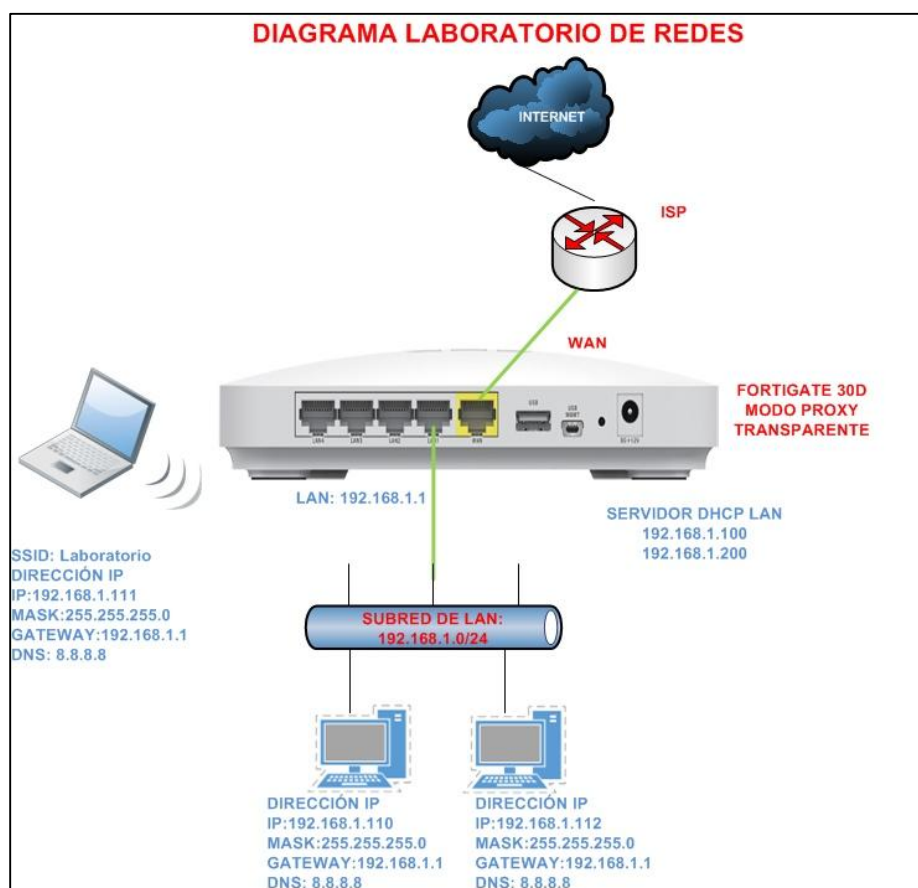


Figura 35: Diagrama de Red de Laboratorio de Redes (Elaboración Propia, 2017).

4.1. Elementos necesarios para la implementación del UTM

Para realizar la configuración inicial del sistema se necesita los siguientes elementos:

4.1.1 Fortiwifi 30D

Equipo Fortiwifi 30D, el cual tiene un FortiASIC SoC2 e incorporado una interfaz *wireless* que funciona en la banda a/b/g/n.

En la siguiente figura se puede observar la imagen de un Fortiwifi modelo 30D.

FortiWiFi 30D



Figura 36: Fortiwifi 30D (FortinetDocs, 2013)

Está formado por 4 puertos RJ45 en modo switch, 1 puerto para WAN (Conexión al proveedor de internet), 1 puerto USB y un puerto USB para administración de equipo con Fortiexplorer.

4.1.2 Cable de poder



Figura 37: Cable de poder (FortinetDocs, 2013)

4.1.3 Cable Ethernet



Figura 38: Cable RJ-45 a RJ-45 (FortinetDocs, 2013)

4.1.4 Adaptador USB a Serial



Figura 39: Adaptador SUB a Serial (Trendnet, 2017)

4.1.5 Cable DB9 a RJ-45



Figura 40: Cable RJ45 a DB9 hembra (Aliexpress, 2017)

4.1.6 Laptop o PC

Necesaria para conexión al equipo vía browser.

4.2. Conexiones Básicas y Administración web con cable ethernet

Es necesario conectar el equipo al adaptador de red y el cable de red *Ethernet* entre el puerto LAN 4 del Fortigate y el adaptador de red de la computadora.

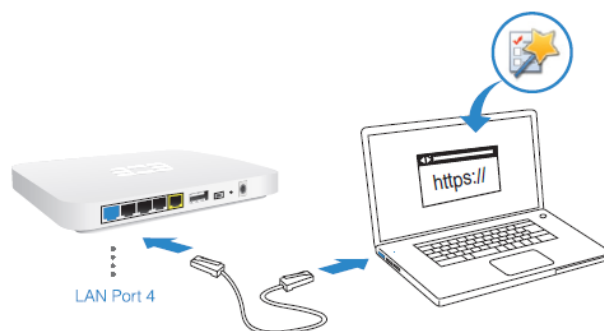


Figura 41: Conexión a través de cable Ethernet (FortinetDocs, 2013)

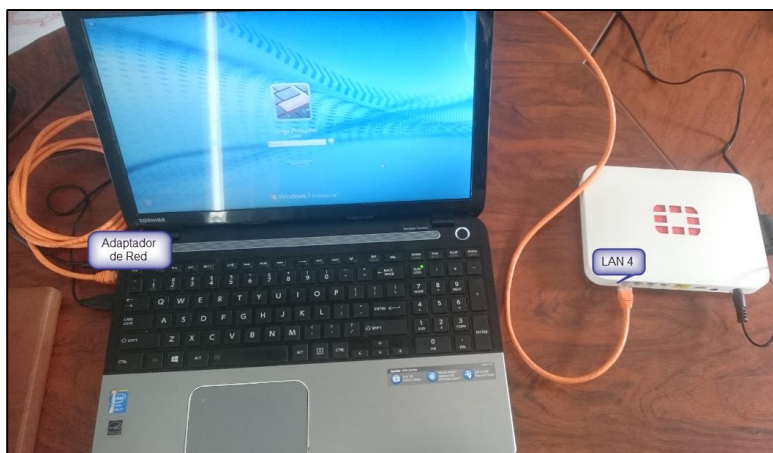
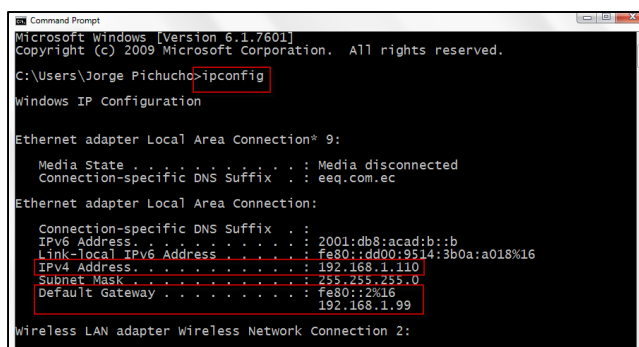


Figura 42: Conexión física desde laptop personal a Fortiwifi 30D (Elaboración Propia, 2017)

Al encender el equipo (Fortigate), en la laptop, automáticamente se asigna una dirección IP dentro de la subred 192.168.1.0/24 puesto que el Fortigate de fábrica viene configurado como servidor DHCP.

Para verificar que dirección IP obtuvimos en la Laptop o PC, ingresar al símbolo del sistema de Windows y ejecutar la siguiente sentencia **ipconfig**, verificar que se asignó la dirección IP: 192.168.1.110 con Máscara de Red: 255.255.255.0 y Gateway 192.168.1.99, tal como se muestra en la siguiente figura.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Jorge Fichucho>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : eeq.com.ec

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IPv6 Address . . . . . : 2001:db8:acad:b::b
    Link-local IPv6 Address . . . . . : fe80::dd00:9514:3b0a:a018%16
    IPv4 Address . . . . . : 192.168.1.110
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::2%16
                               192.168.1.99

Wireless LAN adapter Wireless Network Connection 2:
```

Figura 43: Comando ipconfig desde CMD de Laptop Usuario (Elaboración Propia, 2017)

Los equipos Fortigate vienen con defecto con la dirección IP: 192.168.1.99.

Mediante un navegador Google Chrome o Firefox ingresar vía browser y digitar la siguiente dirección: <https://192.168.1.99>, aparece una advertencia de certificado, dar click en *advanced* y proceder a validar la advertencia.

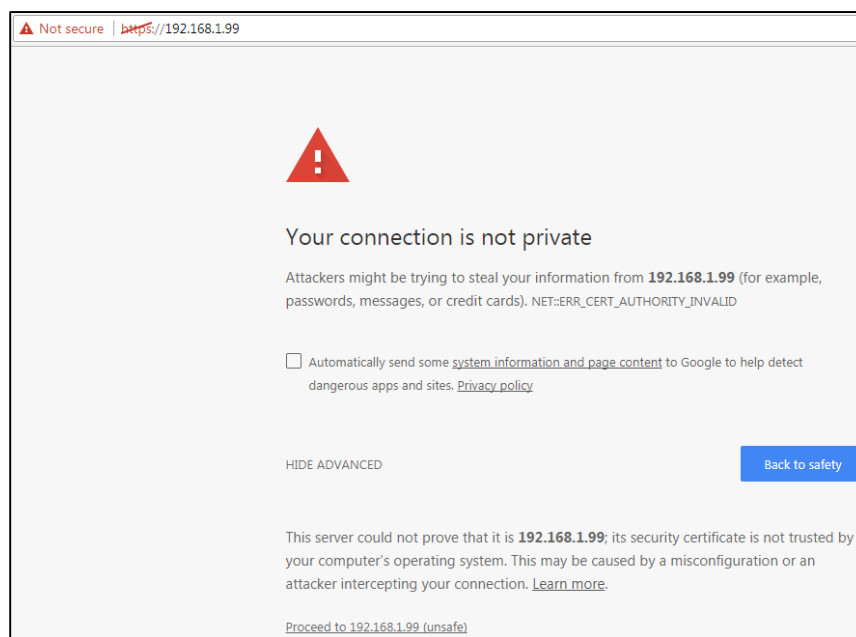


Figura 44: Acceso vía browser a <https://192.168.1.99> (Elaboración Propia, 2017)

Ingresar al equipo con el usuario: admin y sin password.

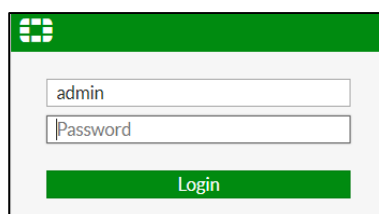


Figura 45: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)

Una vez ingresado al sistema se puede revisar el Dashboard y realizar el registro de la cuenta de usuario a la cual se atará el equipo Fortigate.

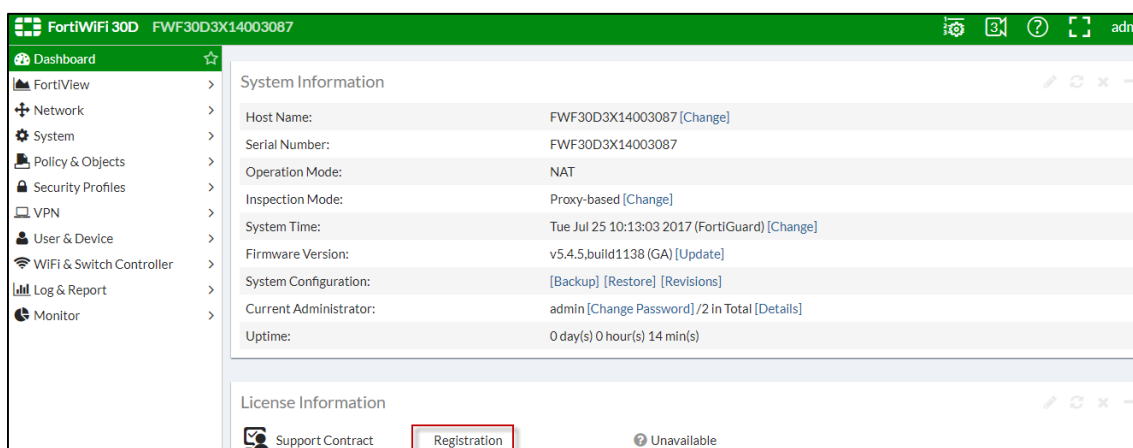


Figura 46 Menú Dashboard de equipo Fortiwifi 30D (Elaboración Propia, 2017)

4.3. Configuración básica de Fortigate

Se pondrá en funcionamiento al equipo Fortigate de acuerdo al diagrama de red propuesto en el laboratorio de redes.

En la interfaz gráfica se puede apreciar algunas características importantes del equipo, como muestra el widget de información del sistema, en el cual observamos el *firmware* del equipo, el número de serie del equipo, la creación de dominios virtuales o fortigates virtuales, etc.

En la columna izquierda se puede apreciar de acuerdo al modelo, los diferentes links para acceder a la configuración del sistema. En el link *System*, verificación de licencias y sincronización con Fortiguard, el modo de operación del equipo (*Stand-alone, active, passive*), entre otras. Otros links importantes son *Network*, se encuentran las interfaces, el servidor DHCP, el servidor DNS en el cual se puede configurar rutas estáticas, enrutamiento dinámico RIP, OSPF, BGP, Balanceo de carga. El link *Security Profiles* en el cual se declara las aplicaciones, url, antivirus, antispam, IPS, a ser bloqueados o permitidos, con el uso de políticas configuradas con el link *Policy & Object*. Adicionalmente, se puede observar otros links

como son el de VPN server, el link *User & Device* que se puede enlazar a un *Active Directory*, *Wifi-controller* para controlar *Access point* de Fortinet, reportes y monitoreo entre otros.

En este punto cabe acotar, que en la vista web no muestra todos los parámetros de configuración que soporta el equipo, para un propósito más avanzado usar la CLI del sistema.

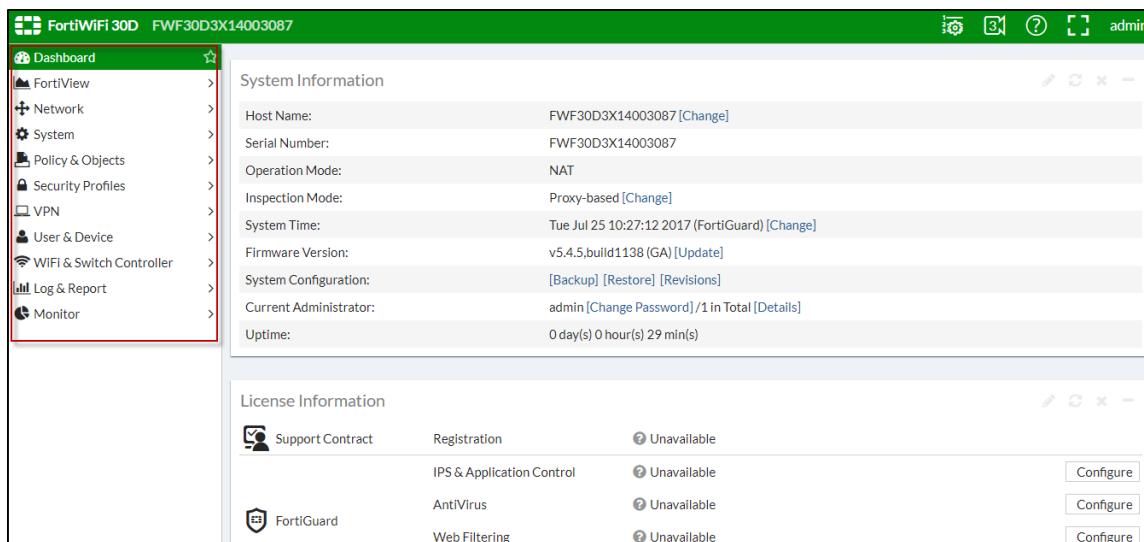


Figura 47: Vista Web del sistema (Elaboración Propia, 2017)

Ingresar en *Network*, interfaces, Internal y configurar la IP del interfaz de la red interna que servirá de Gateway a las computadoras conectadas localmente para acceso a internet.

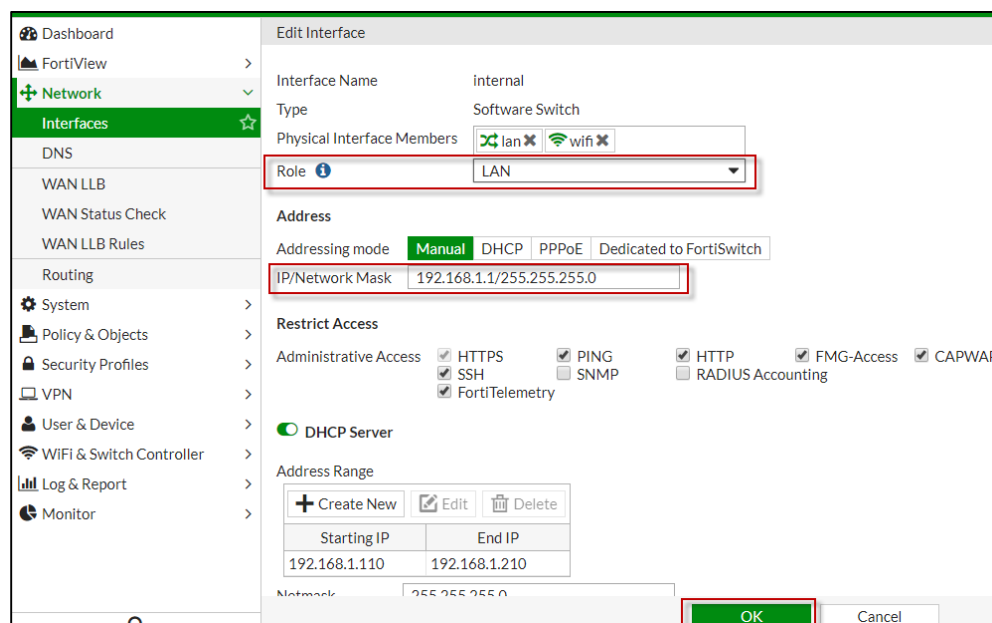


Figura 48: Configuración de Interfaz LAN del cliente (Elaboración Propia, 2017)

De acuerdo a la topología planteada, vamos a proveer de internet a la red interna. En este caso, se configurará una ruta por defecto con salto a la interfaz del router del ISP.

Ingresa en *Network*, interfaces, WAN y configura la IP del interfaz de salida hacia el internet.

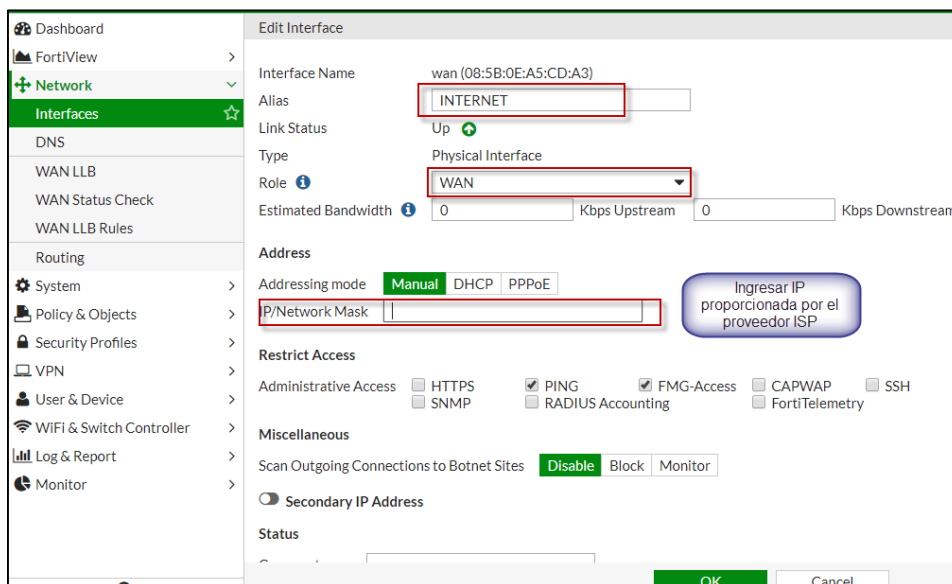


Figura 49: Configuración de Interfaz salida WAN hacia proveedor Internet (Elaboración Propia, 2017)

Hacer click en *Routing*, *static routes*, *create new* y crear la ruta hacia cualquier destino: 0.0.0.0/0.0.0.0, con siguiente salto que será la IP pública del *router* del proveedor de servicios.

Se puede apreciar en este link, que se puede configurar la distancia administrativa y prioridad de ruta frente a otras.

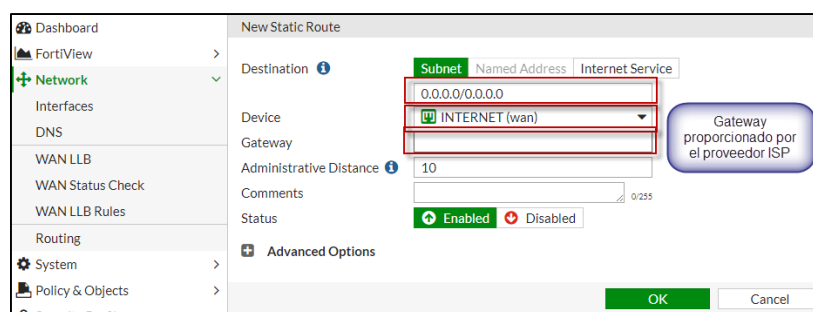


Figura 50: Configuración de ruta por defecto para salida a internet (Elaboración Propia, 2017)

Para proveer de internet a la red interna, configura la siguiente política en *Policy & Object*, *IPv4 Policy*, *create new* y coloca los siguientes parámetros:

Incoming Interface: Internal (LAN interna)

Outgoing Interface: INTERNET (Wan)

Source: all

Destination Address: all

Schedule: always

Service: all

Action: Accept

Enable NAT.

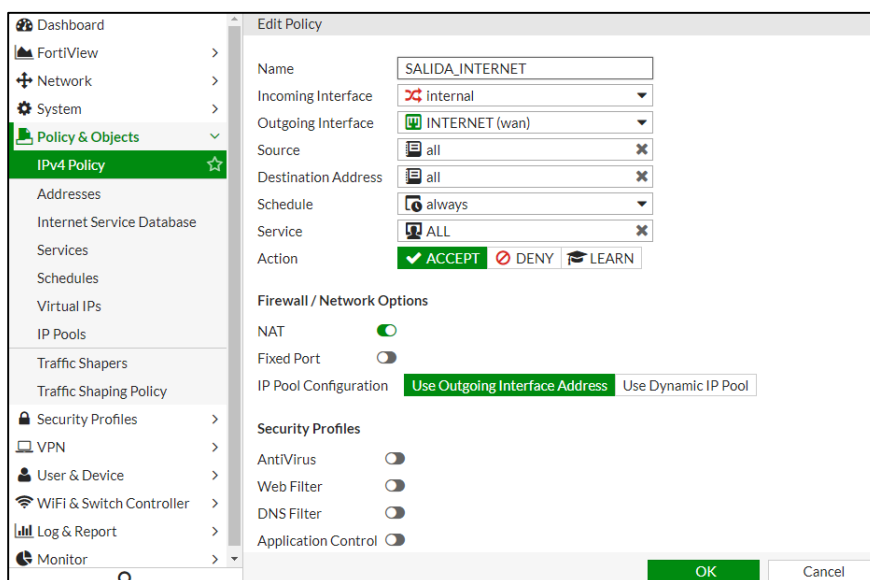


Figura 51: Configuración de política para salida a Internet (Elaboración Propia, 2017)

En este punto en la línea de comandos de Fortinet, hacer un ping al DNS de Google.

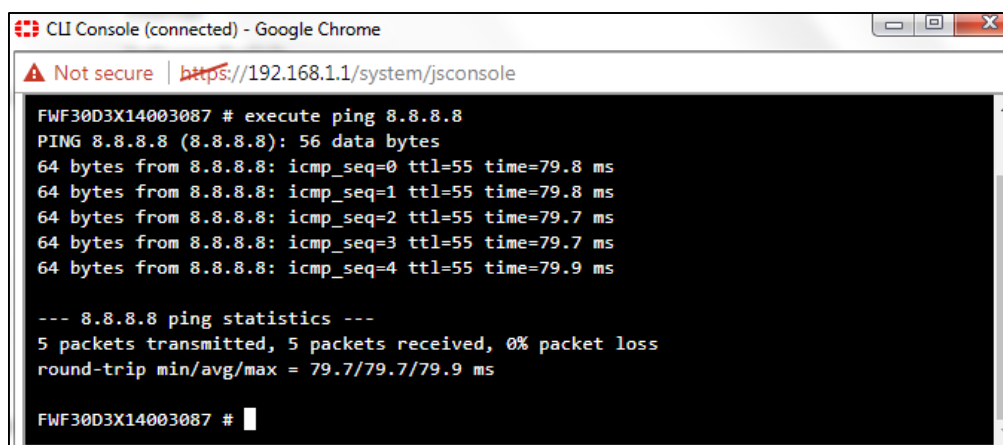
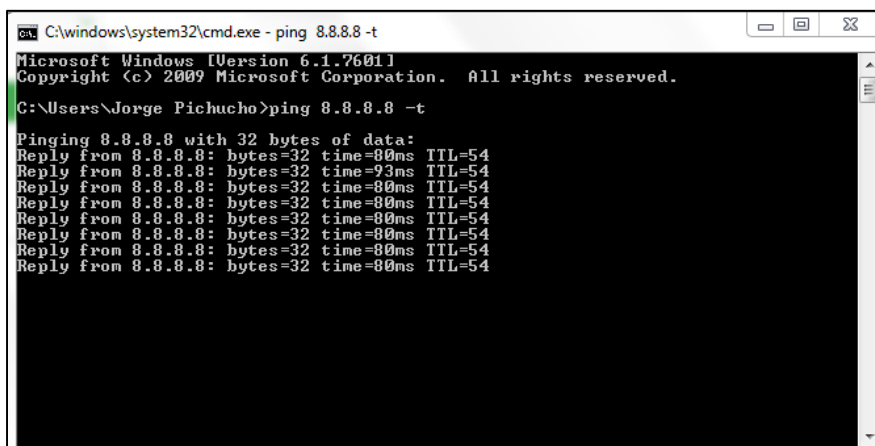


Figura 52: Prueba de ping al DNS de Google (Elaboración Propia, 2017)

Desde el PC, probar la conexión hacia el internet, realizando un ping al DNS de google.



```

C:\windows\system32\cmd.exe - ping 8.8.8.8 -t
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Jorge Pichucho>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=93ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54

```

Figura 53: Prueba de salida al internet desde el PC (Elaboración Propia, 2017)

A partir de estos parámetros configurados, se pueden crear grupos de usuarios, y crear otras reglas que sean más específicas para bloqueo o permiso del tráfico desde la WAN hacia la red.

Notar que las reglas específicas se configuran sobre la regla general, con esto si el PC realiza alguna petición hacia el internet, el paquete será comparado con las políticas para finalmente ser enrutado.

Así mismo se pueden apreciar algunos *features*, como son las opciones de proxy y la inspección SSL, en los cuales se encuentran especificados los puertos de los protocolos HTTP, SMTP, etc.

Otras Opciones son los logs, y captura de paquetes, que son guardados en disco, memoria o en la nube de Fortinet, según el caso, para presentar estadísticas del uso de la información en la organización. De igual forma existe la aplicación de los perfiles de seguridad que serán expuestos en la guía de prácticas.

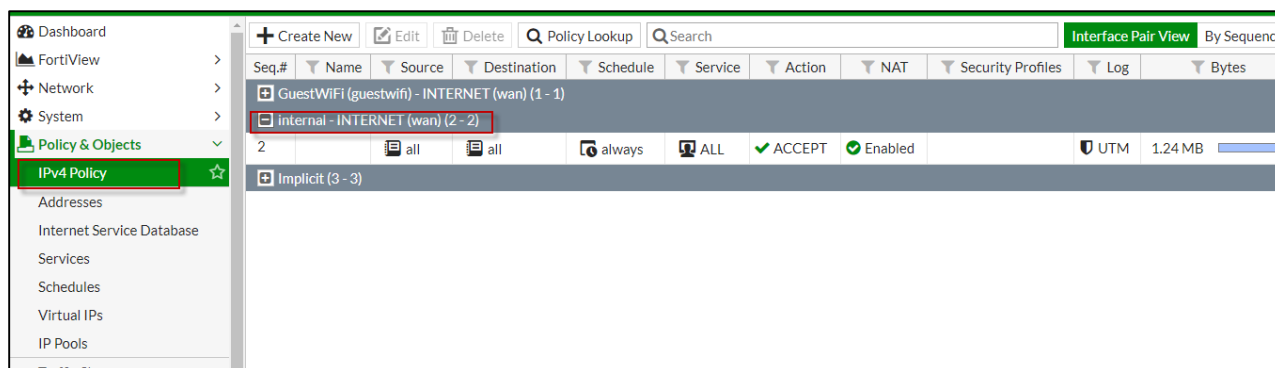


Figura 54: Política de acceso a internet (Elaboración Propia, 2017)

Se recomienda dejar los valores por defecto en las opciones de Proxy.

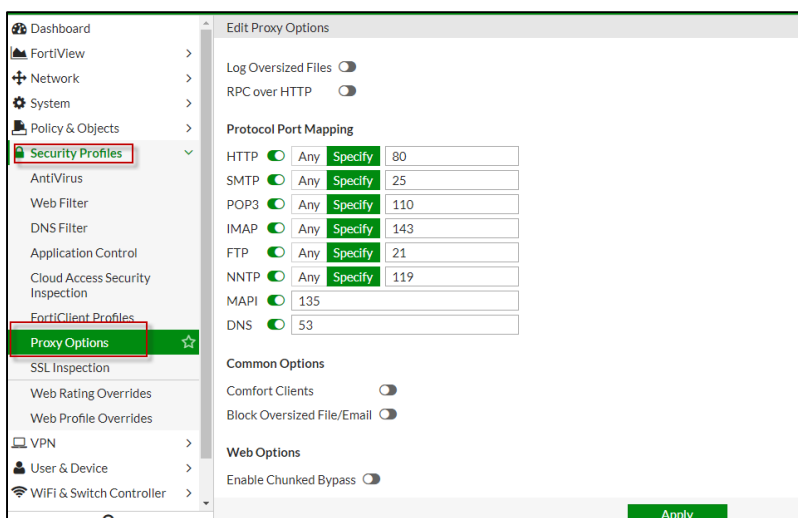


Figura 55: Opciones de Proxy (Elaboración Propia, 2017)

Como se mencionó el equipo cuenta con una interfaz vía Wireless que soporta la banda a/b/g/n. Se va a configurar un SSID (Service Set Identifier) con el nombre **Laboratorio**.

Para ello se ingresa a la opción Wifi & Switch Controller, SSID, el equipo por defecto tiene preconfigurado un SSID llamado fortinet, sin embargo es necesario cambiarlo por seguridad.

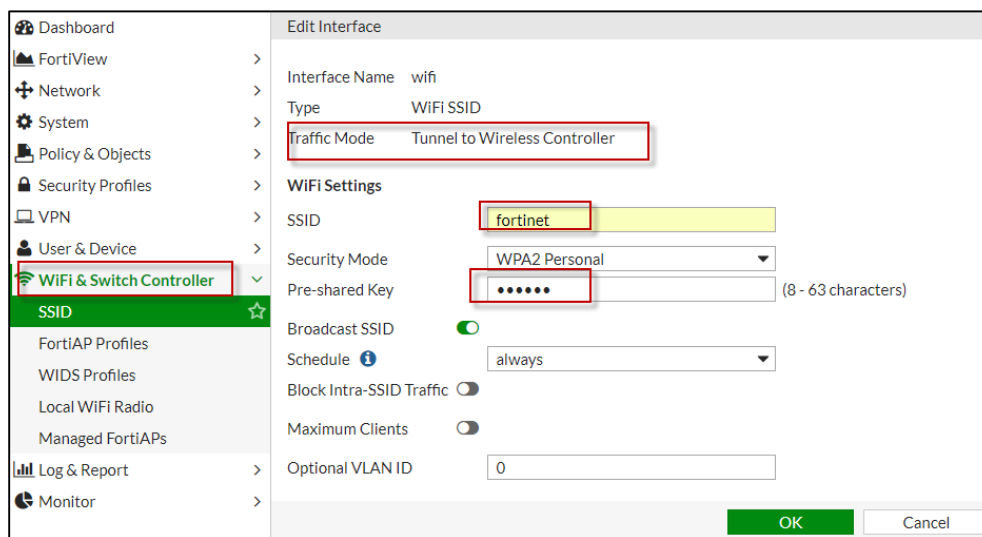


Figura 56: Configuración por defecto de Fortiwifi 30D (Elaboración Propia, 2017)

Se modifica el nombre del SSID a **Laboratorio**, la autenticación se la deja en WPA personal y el Pre-shared Key se digita **laboratorio2017** y se aplica los cambios.

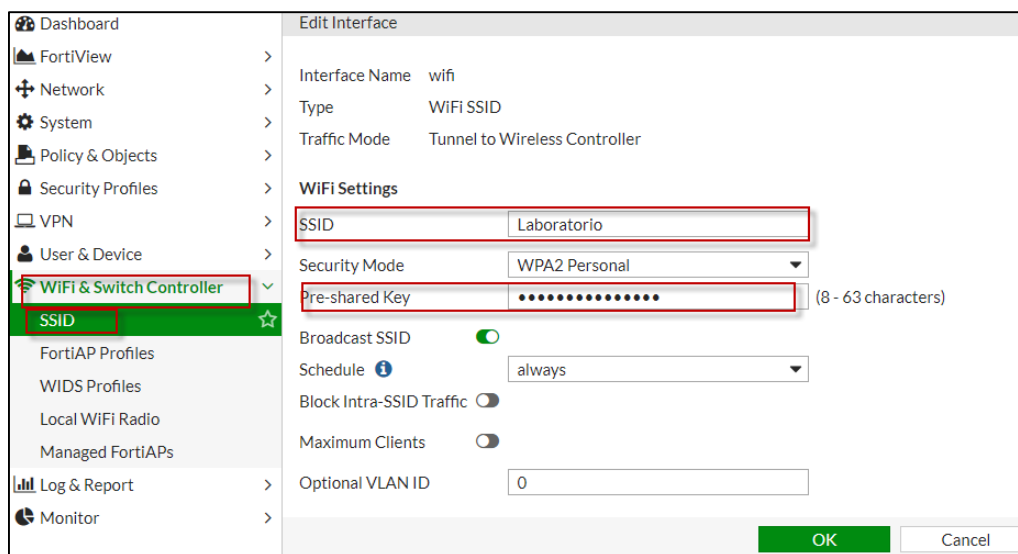


Figura 57: Cambio de parámetros de default a personalizados (Elaboración Propia, 2017)

Desde la PC se puede observar un SSID llamado Laboratorio, se da click en Connect, nos solicita un password.



Figura 58: Se despliega la red Wireless Laboratorio (Elaboración Propia, 2017)

El password es el descrito anteriormente **laboratorio2017**

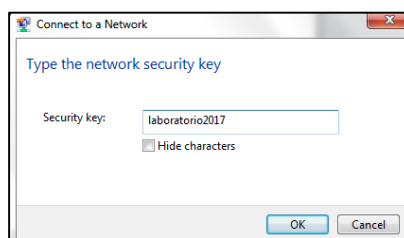


Figura 59: Ingresamos el password laboratorio2017 (Elaboración Propia, 2017)

Se logra realizar la conexión del acceso a la red Wireless sin problema.



Figura 60 Conexión al SSID Laboratorio sin inconveniente (Elaboración Propia, 2017)

Desde el PC, se revisa el direccionamiento IP, máscara y Gateway una vez logrado la conexión a la red Wireless.

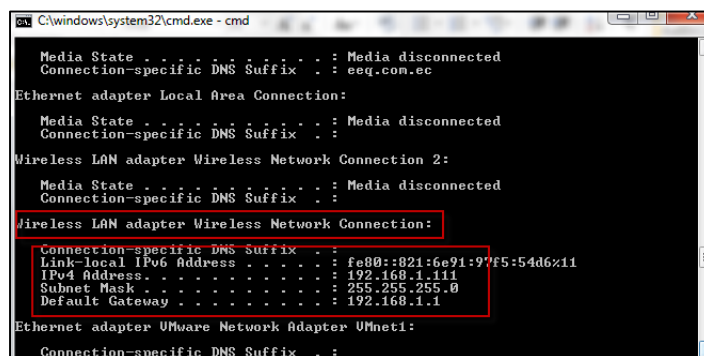


Figura 61: Comando ipconfig para revisar dirección IP asignada (Elaboración Propia, 2017)

Para comprobar la conexión, se ingresa al Fortigate vía browser, pero esta vez a través de la red Wireless.

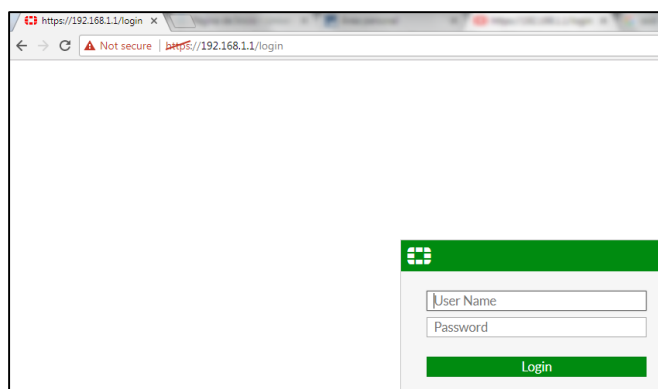


Figura 62: Conexión a Fortiwifi a través de Wireless (Elaboración Propia, 2017)

De esta forma queda configurado y funcionando el Módulo para prácticas de laboratorio de Gestión Unificada de Amenazas en la Universidad Israel.

Finalmente se realiza la instalación física del mismo en el Laboratorio y a continuación se elabora una guía de prácticas de laboratorio para los estudiantes.

4.4. PRÁCTICAS DE LABORATORIO

4.4.1 Práctica N.-1 Inicialización UTM Fortigate

Objetivos:

- Conocer el software Fortiexplorer para ingresar al equipo.
- Realizar la configuración inicial del Equipo.

Escenario:

En la figura 62 se observa la conexión básica vía cable USB, donde el estudiante deberá instalar en su Computadora el Software Fortiexplorer propiedad de Fortinet, cuyo procedimiento de instalación se encuentra en la parte de anexos.

Esto se lo realizará una sola vez y servirá para verificar las configuraciones por defecto del equipo.

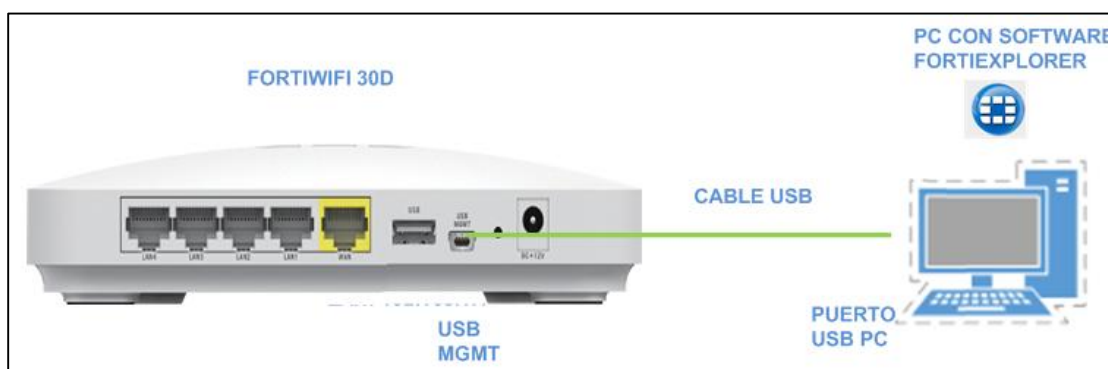


Figura 63: Conexión básica a través del puerto USB de Administración Fortigate (Elaboración Propia, 2017)

Materiales a utilizar en la práctica:

- Un Fortiwifi 30D
- Una computadora
- Un adaptador de consola USB propiedad de Fortinet
- Software Fortiexplorer instalado en la computadora del estudiante

Tiempo estimado:

Una hora aproximadamente

Desarrollo de la práctica:

Inicialmente todos los equipos Fortigate para pequeñas empresas, pueden configurarse a través de un puerto de consola para cable USB propiedad de Fortigate o a través de un puerto de consola RJ-45.

En este caso el equipo Fortigate modelo 30 no cuenta con un puerto de consola RJ-45, por lo cual la configuración inicial debe ser realizada a través de la conexión USB y del puerto que se encuentra en la parte posterior del equipo. La figura 63 muestra un cable USB para la conexión entre el Fortigate y la Computadora.



USB Cable

Figura 64: Cable USB (FortinetDocs, 2013)

Paso 1:

Descargar e instalar el software Fortiexplorer del siguiente link: <https://www.fortinet.com/support-and-training/support/product-downloads.html>

Paso 2:

Conecte el cable USB y abra el software Fortiexplorer si este no aparece automáticamente, para lo cual debe ir a Inicio → All Programs → FortiExplorer y ejecutar el programa Fortiexplorer, debe aparecer una ventana similar a la de la figura 64.

Si el cable USB entre el equipo y la computadora se encontraba previamente conectado la ventana del programa Fortiexplorer debería cambiar y ser mostrada como en la figura 65, puesto que debería reconocer el equipo conectado.

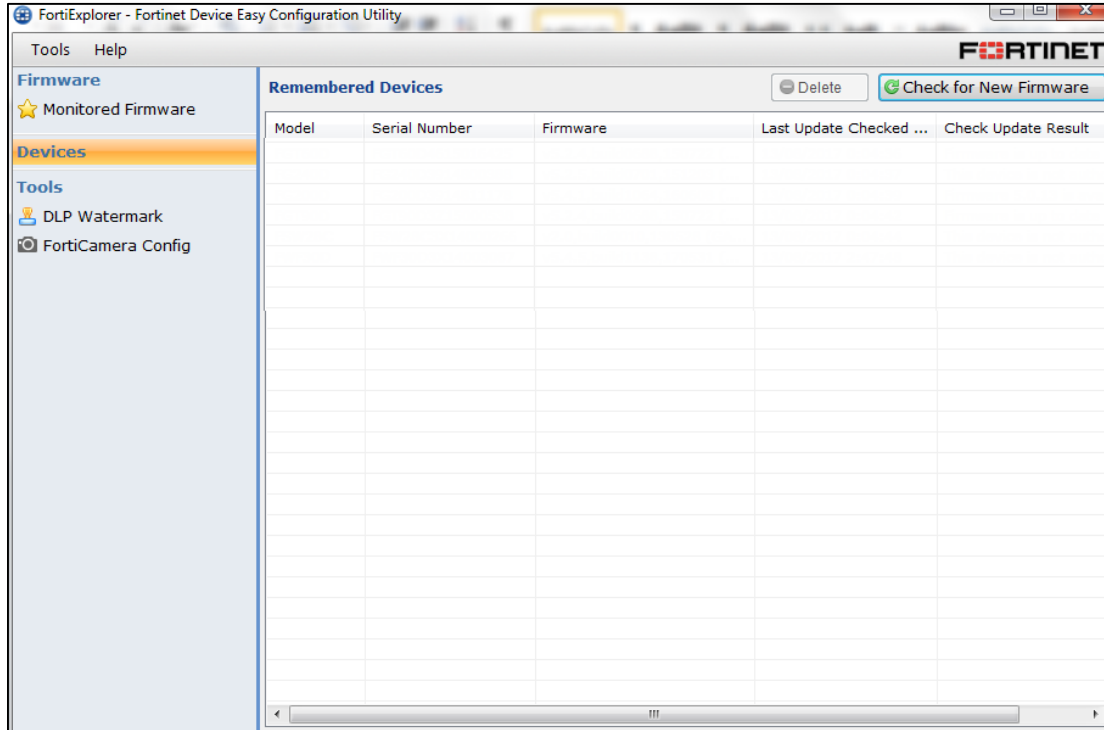


Figura 65: Software Fortiexplorer (Elaboración Propia, 2017)

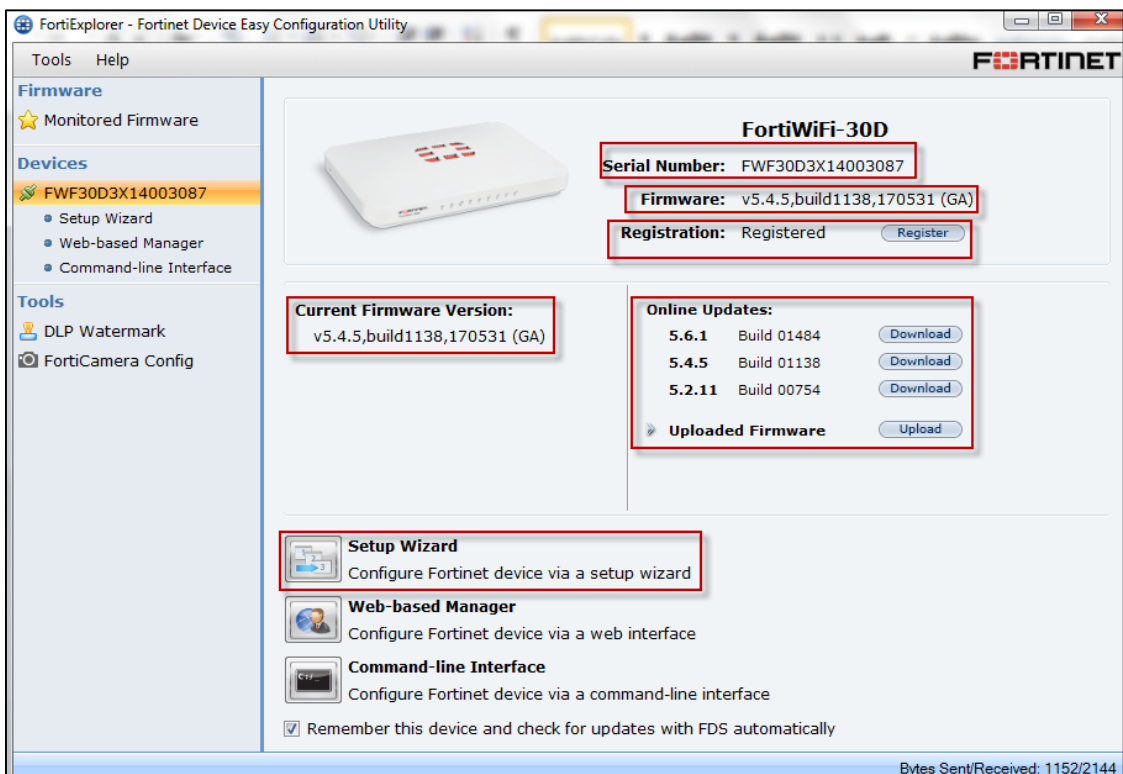


Figura 66: Software Fortiexplorer verificando el equipo conectado vía USB (Elaboración Propia, 2017)

La información que nos muestra el gráfico es el siguiente:

Modelo del Equipo: FortiWifi 30D

Número de Serie del mismo: FWF30D3X14003087

Versión de Firmware instalado: La versión de Firmware es 5.4.5

Registro: El equipo ya se encuentra registrado.

Paso 3:

Setup Wizard

Se puede configurar el Fortigate a través de un Wizard de una manera fácil, sin embargo la mejor práctica es realizarlo manualmente.

A continuación se revisan las opciones que pueden ser configurables en el Setup Wizard;

Ir a *Setup Wizard* y aparece ingresar usuario y password.

El usuario por defecto es **admin** y su contraseña está en blanco.

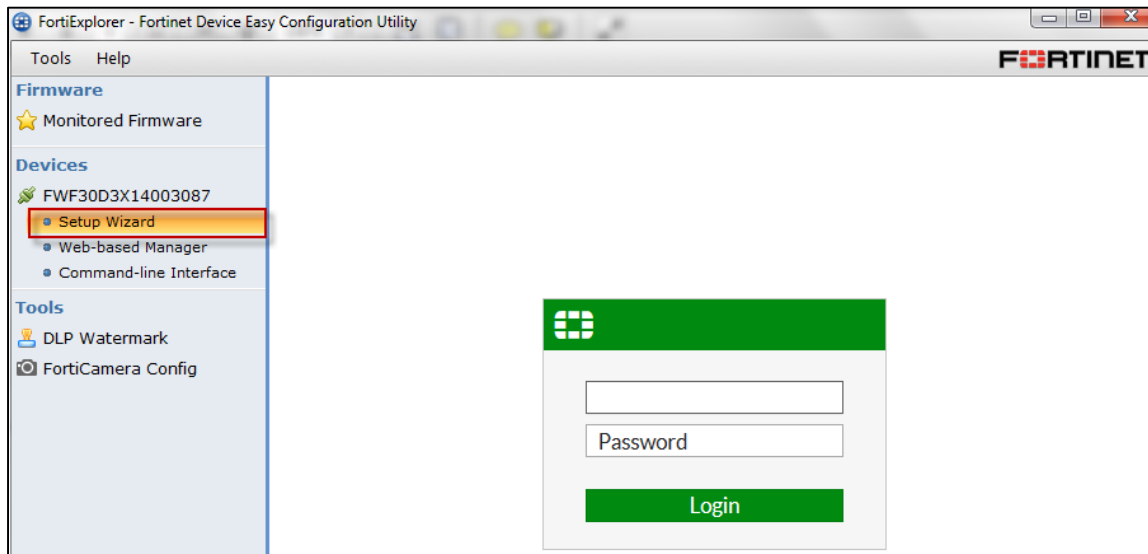


Figura 67: Ventana principal una vez activado el Setup Wizard (Elaboración Propia, 2017)

El primer cambio es realizar el cambio de la contraseña del usuario admin

El propósito de la práctica es revisar los pasos y configuraciones por defecto que tiene el equipo, dar click en Next.

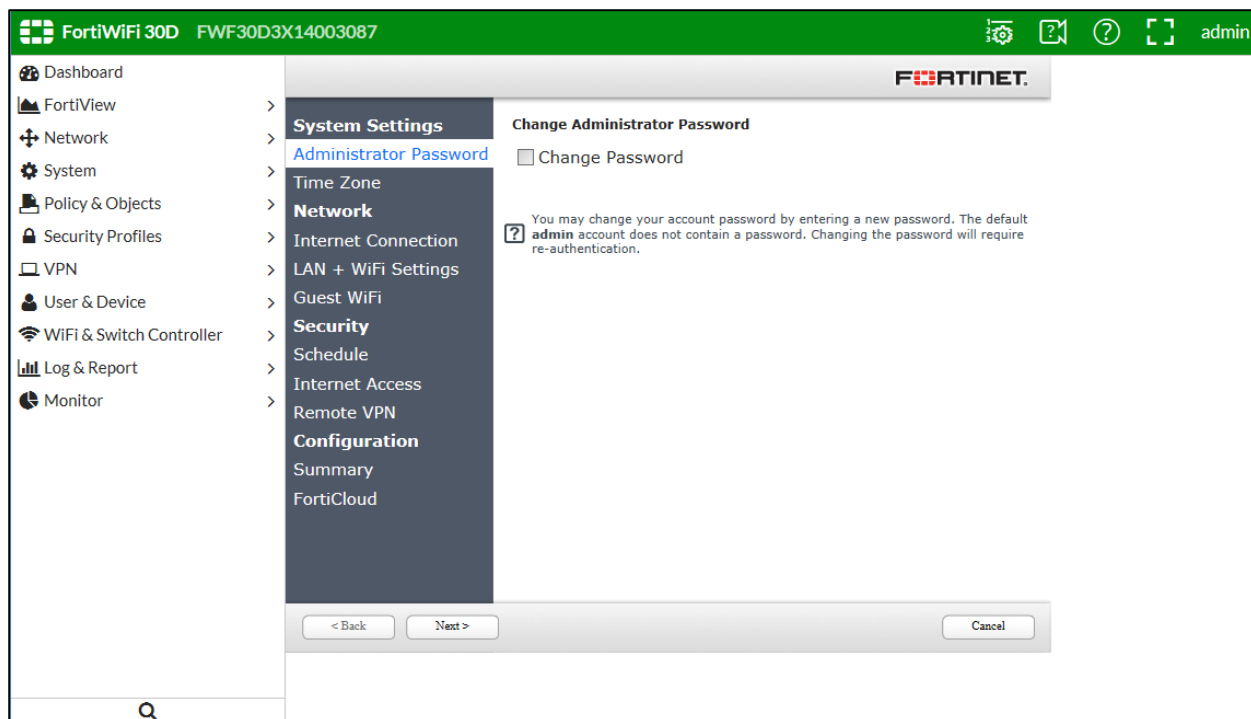


Figura 68: Opciones del setup wizard (Elaboración Propia, 2017)

Time Zone: Configurar la zona horaria del equipo, para el caso de Ecuador GMT-5

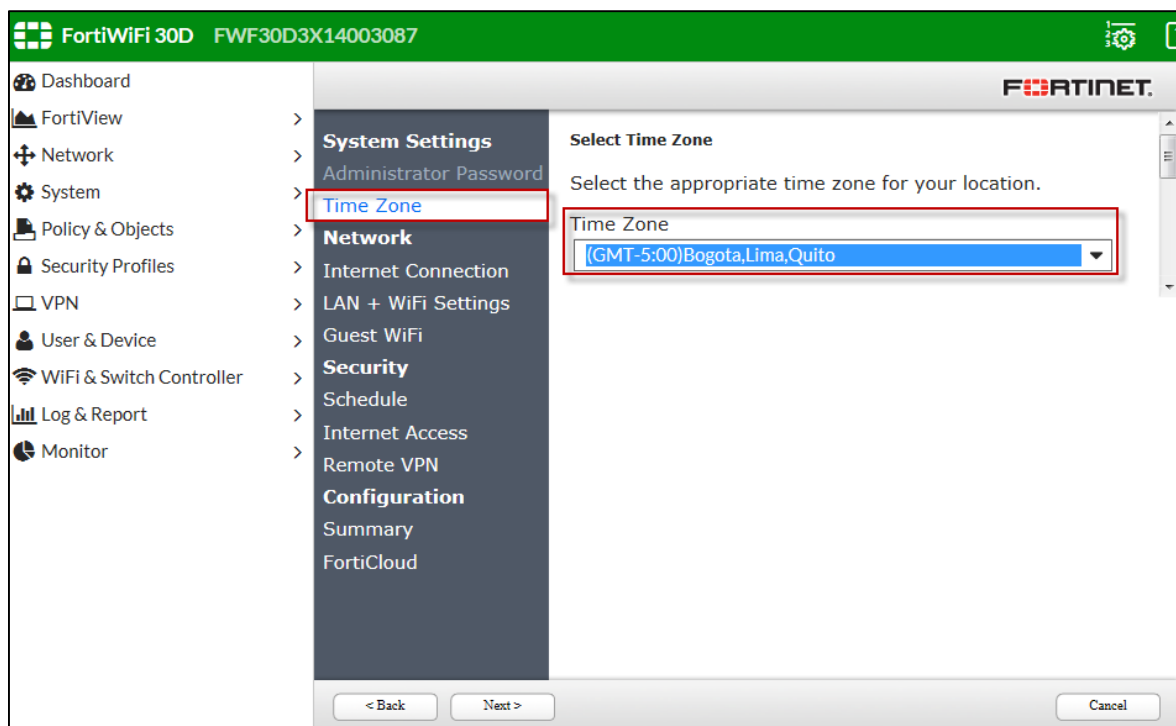


Figura 69: Configuración Zona Horaria del equipo (Elaboración Propia, 2017)

Network: Se puede configurar la dirección IP de la WAN, la red LAN y el SSID del acceso Wireless.

Para comprobar su funcionamiento se configura la IP de la Lan del equipo con 192.168.1.1/24.

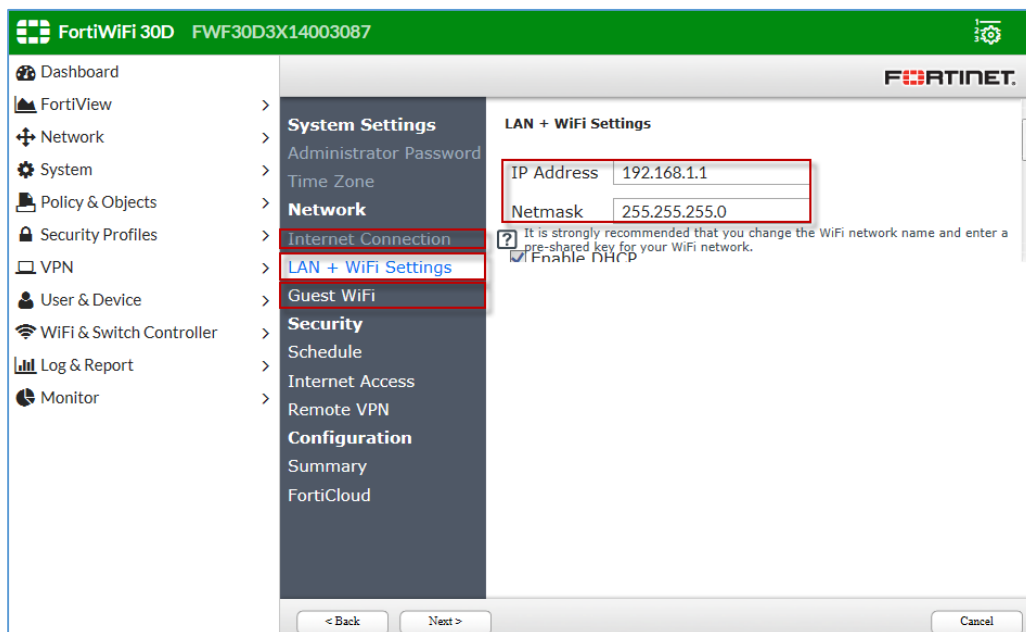


Figura 70: Configuración del direccionamiento IP y red del equipo (Elaboración Propia, 2017)

Security: Se configura el horario de navegación de los usuarios a internet, que trabaje en modo NAT el equipo para poder navegar a internet y si es el caso configurar una VPN.

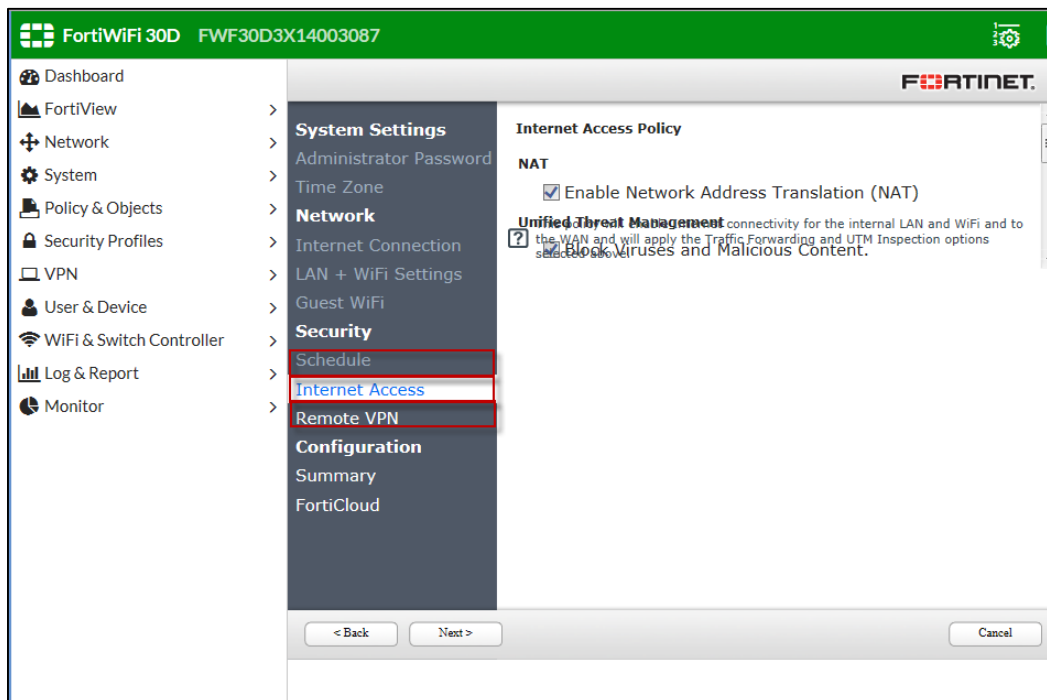


Figura 71: Configurar modo NAT del equipo, horario de navegación y VPN Remota (Elaboración Propia, 2017)

Por último se tiene un resumen de las configuraciones realizadas en el *Wizard* y se aplican las mismas en la opción de **Configure**.

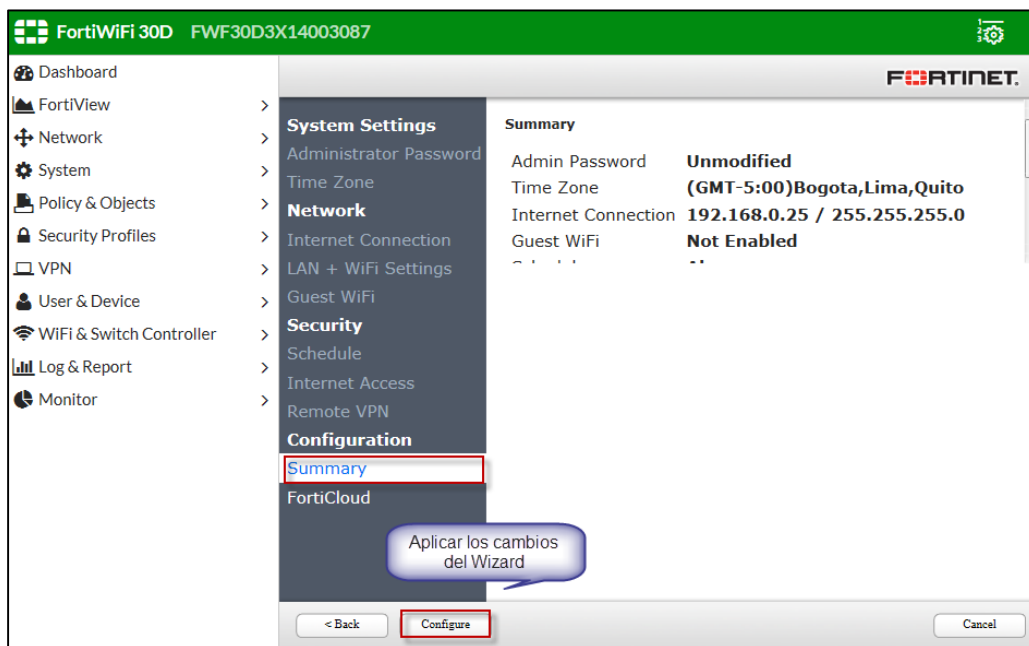


Figura 72: Resumen de los cambios realizados y aplicar los cambios (Elaboración Propia, 2017)

Una vez realizada la configuración elegida en el *Wizard*, aparece el siguiente mensaje que señala que los cambios fueron realizados con éxito y debemos escoger la opción **Done**

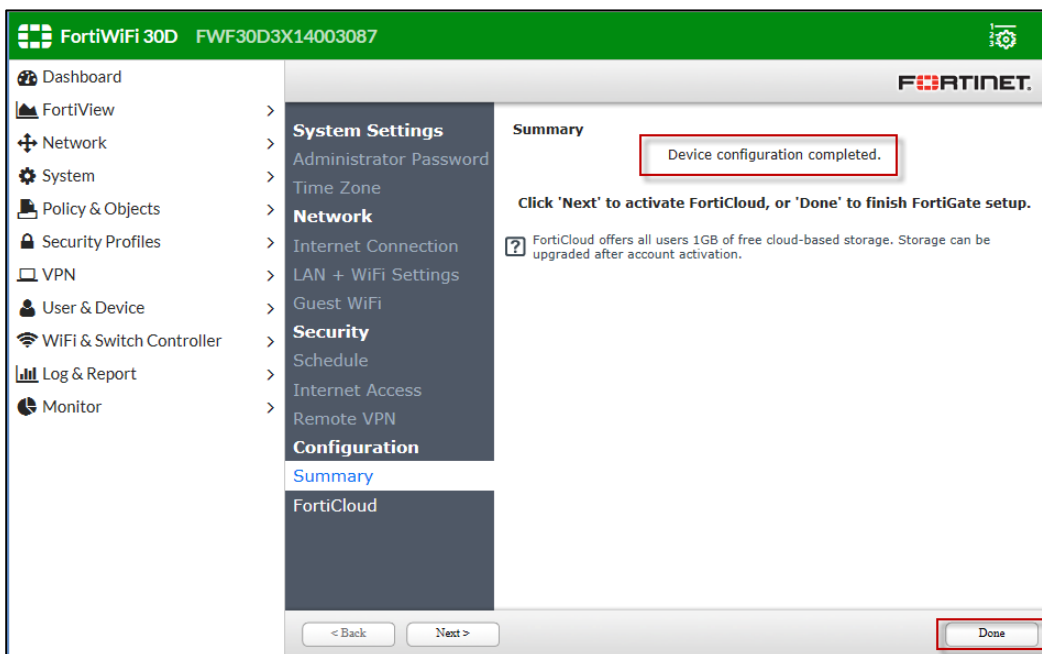


Figura 73: Aplicar y Finalizar el Wizard del Fortigate (Elaboración Propia, 2017)

Una vez aplicado y terminado el proceso de Wizard, el equipo nuevamente mostrará ingresar el usuario y la contraseña.

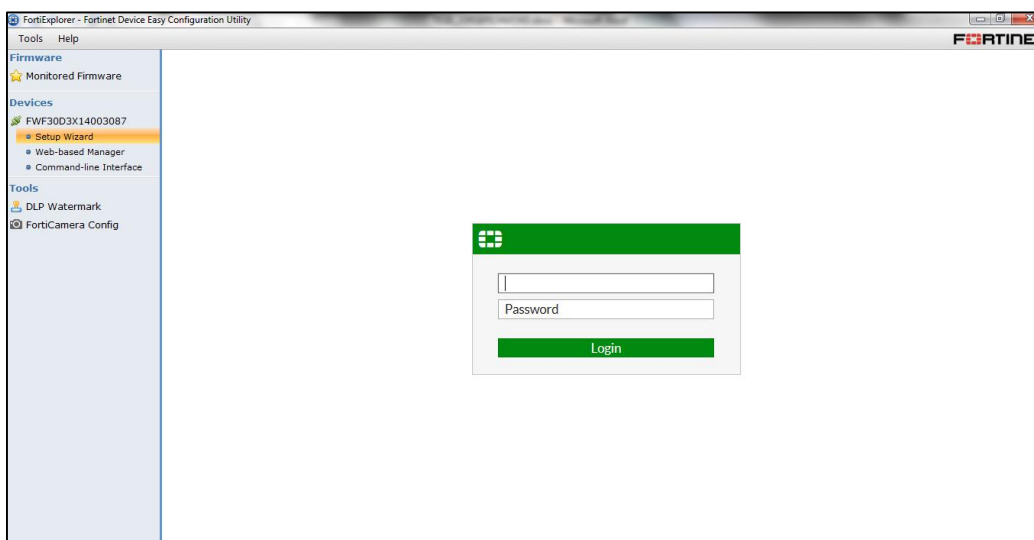


Figura 74: Finalización del proceso Wizard (Elaboración Propia, 2017)

Paso 4:

Verificar los cambios luego del proceso Wizard.

Se escoge la Opción Web-based Manager, en este caso el usuario y password se encuentran por defecto ya que no fue realizado ningún cambio y se ingresa las credenciales del equipo.

Aparece el siguiente Menú el cual es el Menú de administración del Fortigate y para revisar si los cambios fueron realizados satisfactoriamente se ingresa a Network → Interfaces → Internal y verificar que se encuentra configurada la dirección IP 192.168.1.1/24.

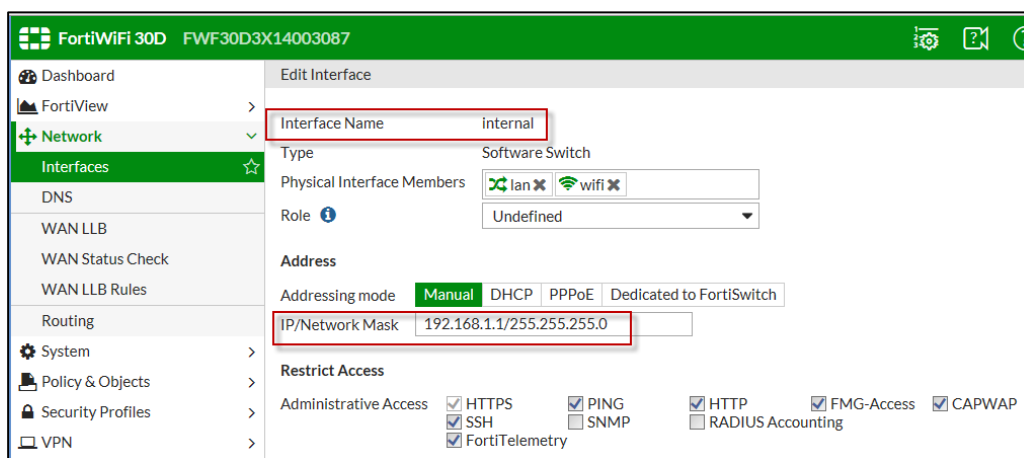


Figura 75: Verificar cambio de dirección IP en Interfaz Lan del equipo luego del Wizard (Elaboración Propia, 2017)

Resultados:

A pesar de utilizar el proceso *Setup Wizard* y configurar aspectos básicos para la administración, es importante una vez realizado este proceso ya no utilizar el Fortiexplorer, ya que la administración se la puede realizar vía browser a través de la dirección IP 192.168.1.1 que se realizará en la práctica 2.

4.4.2 Práctica N.-2 Configuración Básica

Objetivos:

- Realizar la configuración básica de equipo
- Revisar los componentes del Menú de administración

Escenario:

En la figura 75, se muestra una topología básica donde el estudiante debe simular y realizar las configuraciones básicas, indicadas en la práctica.

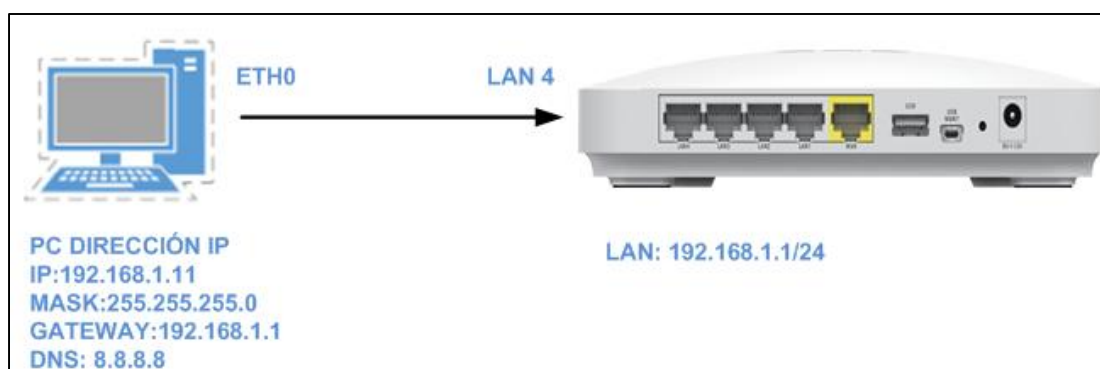


Figura 76: Topología para administrar Fortigate (Elaboración Propia, 2017)

Dispositivo	Nombre	Contraseña	Direccionamiento	
			Interfaz	IP
PC	NA	NA	NA	192.168.1.11/24
Fortigate 30D	admin		LAN 4	192.168.1.1/24

Tabla 5: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)

Materiales a utilizar en la práctica:

- Un Fortiwifi 30D
- Una computadora
- Un cable de red

Tiempo estimado:

Una hora aproximadamente

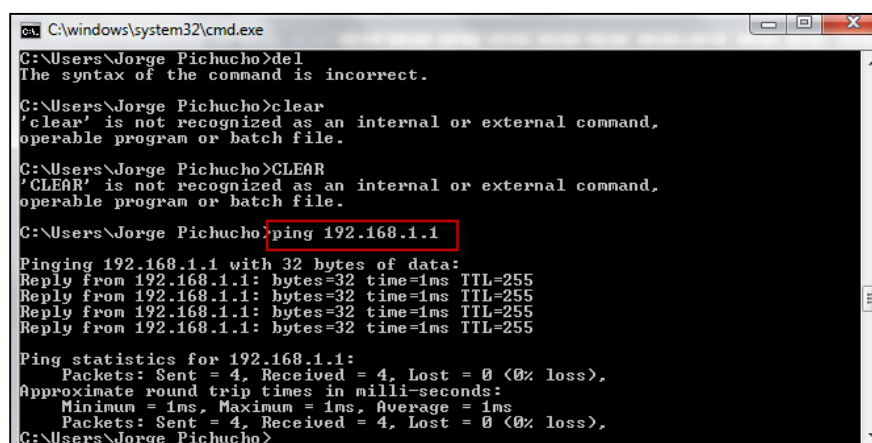
Desarrollo de la práctica:

Una vez inicializado el equipo, se puede realizar la administración del equipo vía Ethernet a través de un cable de red y vía browser ingresar la dirección IP del equipo en esta caso en la práctica 1 la dirección IPV4 del Fortigate es 192.168.1.1.

Antes de esto se realiza el cambio de dirección IP de la computadora de acuerdo a la tabla 5. En el Anexo 3 se describe como realizar el cambio de direccionamiento IP.

Paso 1:

Ingresar al símbolo del sistema de Windows y ejecutar un **ping** hacia la ip 192.168.1.1 para verificar que se tiene conexión a la IP: 192.168.1.1 tal como se muestra en la siguiente figura.



```
C:\windows\system32\cmd.exe
C:\Users\Jorge Pichuco>del
The syntax of the command is incorrect.

C:\Users\Jorge Pichuco>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Jorge Pichuco>CLEAR
'CLEAR' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Jorge Pichuco>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\Jorge Pichuco>
```

Figura 77: Comando ping desde CMD de Laptop Usuario (Elaboración Propia, 2017)

Mediante un navegador Google Chrome o Firefox ingresar vía browser y digitar la siguiente dirección: <https://192.168.1.1> , aparece una advertencia de certificado, dar click en *advanced* y proceder a validar la advertencia.

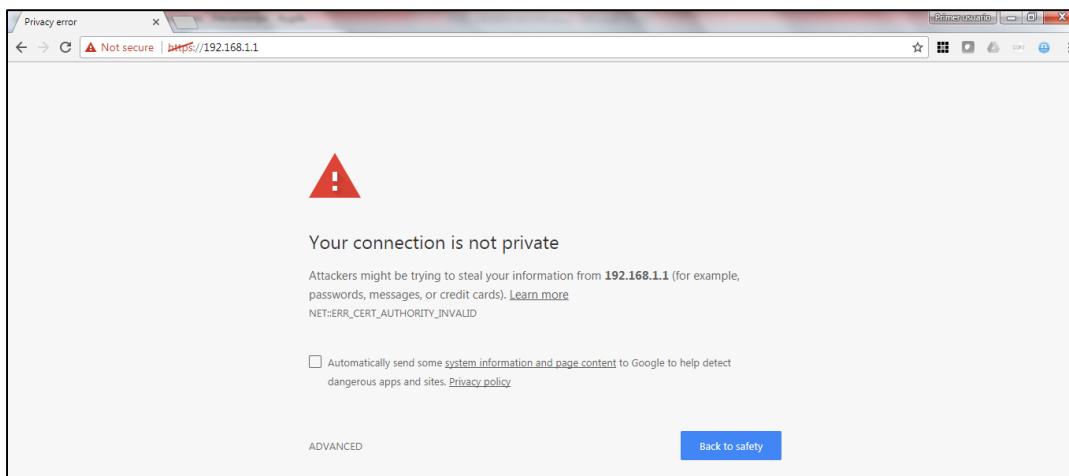


Figura 78: Acceso vía browser a <https://192.168.1.1> (Elaboración Propia, 2017)

Ingresa al equipo con el usuario: admin y sin password.

Figura 79: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)

Paso 2:

Revisión del Menú Opciones Fortigate

Se Ingresa al Menú principal de configuración del equipo.

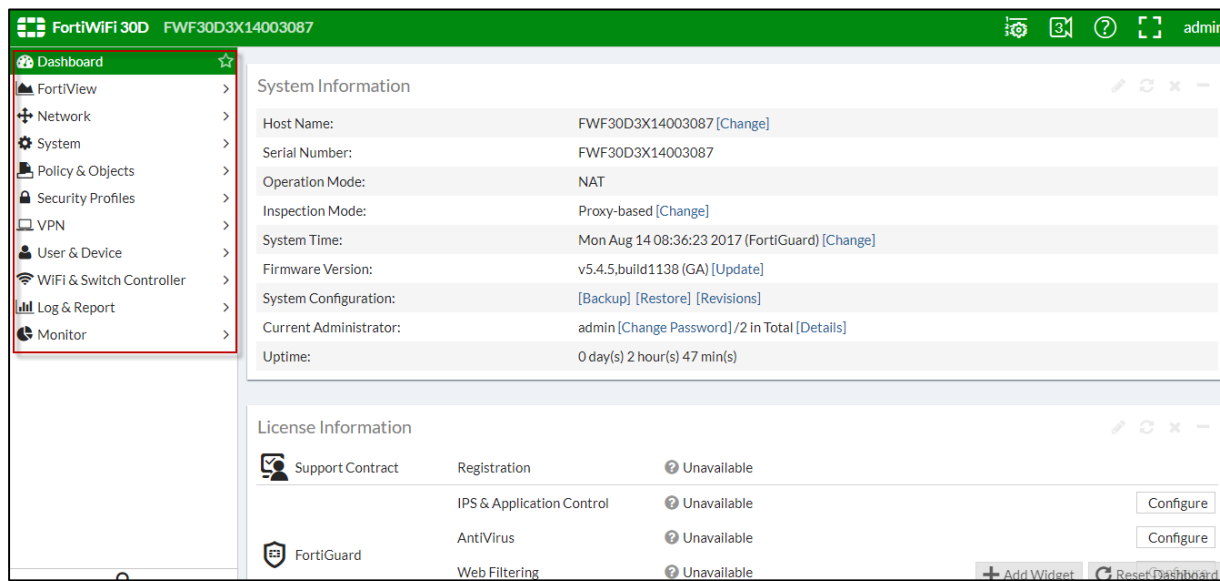


Figura 80: Menú Opciones administración Fortigate (Elaboración Propia, 2017)

En la interfaz gráfica se puede apreciar algunas características importantes del equipo, como muestra el widget de información del sistema, en el cual observamos el *firmware* del equipo, el número de serie del equipo, nombre del equipo, etc.

En la columna izquierda se puede apreciar de acuerdo al modelo, los diferentes links para acceder a la configuración del sistema.

FortiView, se puede apreciar los logs del sistema y muy importante al momento de monitorear el comportamiento del equipo.

Network, se encuentran las interfaces de red del equipo, el servidor DHCP, el servidor DNS, configuración de rutas estáticas, enrutamiento dinámico RIP, OSPF, BGP, Balanceo de carga

System, verificación de licencias y sincronización con Fortiguard, el modo de operación del equipo (*Stand-alone, active, passive*), entre otras.

Security Profiles, Se declaran las aplicaciones, url, antivirus, antispam, IPS, a ser bloqueados o permitidos, con el uso de políticas configuradas en el **Policy & Object**.

Adicionalmente, se pueden observar otros links como son el de **VPN**, para acceso remoto a la oficina.

User & Device, que se puede crear usuarios locales, grupos de usuarios, conexión a un *Active Directory*, LDAP o servidor Radius. Estos son usados tanto para navegación como para VPN.

Wifi-controller, para controlar *Access point* de Fortinet.

Log and Report, se revisan los logs del sistema y monitoreo de las diferentes aplicaciones.

Paso 3:

Cambiar el nombre del host del Fortigate.

Ir a Dashboard → Hostname y Change como se muestra en la figura 80.

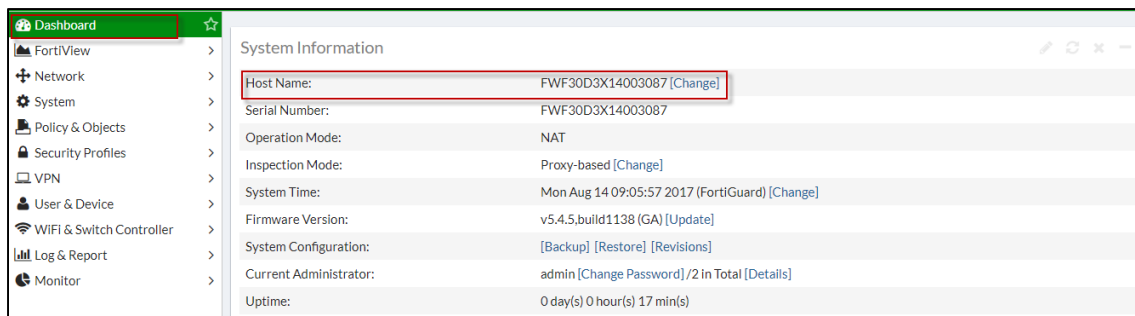


Figura 81: Cambio de nombre del equipo (Elaboración Propia, 2017)

Digitamos el nuevo nombre del equipo.



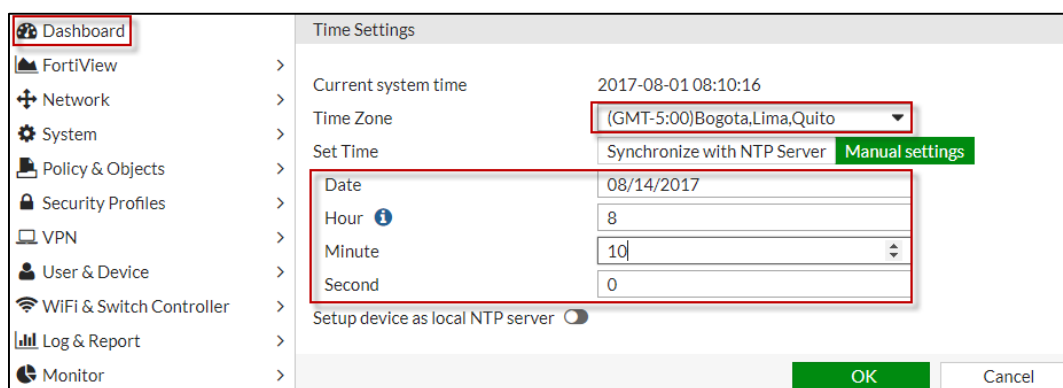
Dialog box titled "Edit Host Name". The "Host name" field contains the text "FWF30D_LABORATORIO". Below the field are two buttons: "OK" (highlighted in green) and "Cancel".

Figura 82: Nombre del equipo (Elaboración Propia, 2017)

Paso 4:

Configurar fecha y hora del sistema.

Ir a Dashboard → System Information → System Time y change, escoger el huso horario en nuestro caso GMT-5 y hora y fecha como se muestra en la siguiente figura y aplicamos. Es muy importante ya que sirve para revisión de logs del sistema y de seguridad.



Screenshot of the "Time Settings" configuration page. The left sidebar shows the navigation menu with "Dashboard" highlighted. The main content area shows the following settings:

- Current system time: 2017-08-01 08:10:16
- Time Zone: (GMT-5:00)Bogota,Lima,Quito
- Set Time: Synchronize with NTP Server (Manual settings button is highlighted in green)
- Date: 08/14/2017
- Hour: 8
- Minute: 10
- Second: 0
- Setup device as local NTP server:

At the bottom right, there are "OK" (highlighted in green) and "Cancel" buttons.

Figura 83: Cambiar hora y fecha del sistema (Elaboración Propia, 2017)

Paso 5:

Configurar interfaces de red del equipo WAN (Acceso a internet) y LAN (Acceso a la Red interna).

En este laboratorio, la dirección IP de la red LAN del Fortiwifi se debe configurar manualmente habilitar el servidor DHCP en la misma y la red WAN como cliente DHCP.

Ir a Dashboard → Network → Interfaces, se muestra la interfaz WAN del Fortigate 30D y la interfaz LAN que es identificada como Internal en el Fortigate.

La red Internal por defecto viene configurada en modo switch (configuración por software) desde los puertos LAN 1 a LAN 4, y adicional ya está configurada la dirección IP 192.168.1.1 que se realizó en la práctica 1.

En la figura 83 se observa el menú de Interfaces de Red del equipo Fortigate.

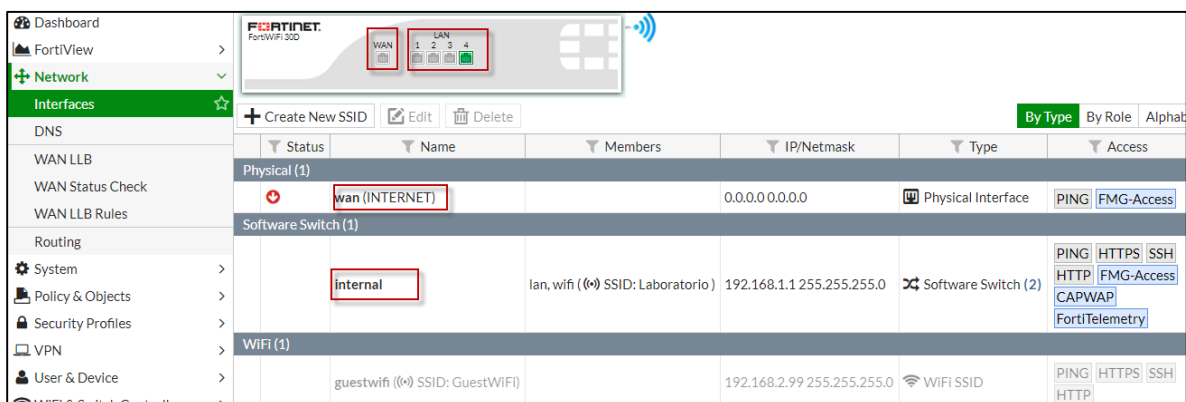


Figura 84: Interfaces de red de Fortigate 30D (Elaboración Propia, 2017)

Para configurar la red WAN como cliente DHCP se debe Ir a Dashboard → Network → Interfaces, doble click sobre interfaz WAN y se ingresa a la configuración de la misma, se pone un nombre a la interfaz, en este caso INTERNET y en Address se escoge el modo DHCP, ya que el proveedor de internet provee una dirección IP automáticamente y se aplican los cambios.

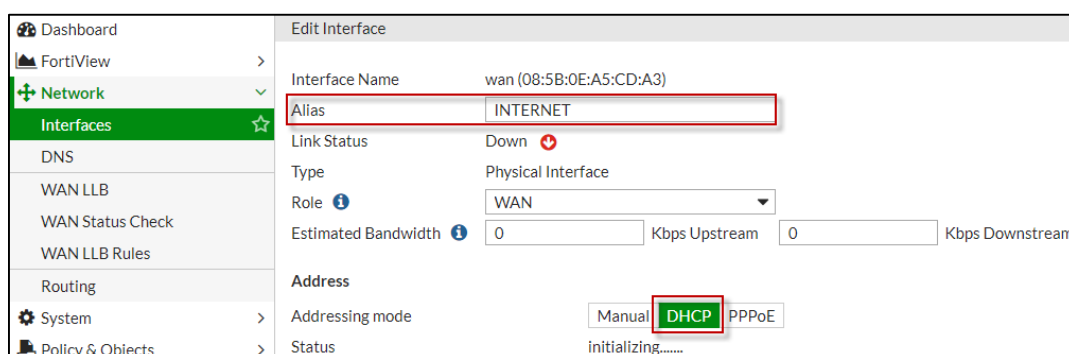


Figura 85: Configuración interfaz WAN acceso a internet del equipo (Elaboración Propia, 2017)

Para configurar la red LAN y configurar como servidor DHCP se debe ir a Dashboard → Network → Interfaces, doble click sobre interfaz LAN y se ingresa a la configuración de la misma. Se observa que en Address Mode está configurado Manual, ya que se debe configurar una IP fija 192.168.1.1/24.

Habilitar la opción DHCP Server y colocar el rango de direcciones IP, desde la 192.168.1.110 hasta la 192.168.1.210, esta configuración sirve para el acceso vía inalámbrica o red cableada al equipo y aplicar la configuración.

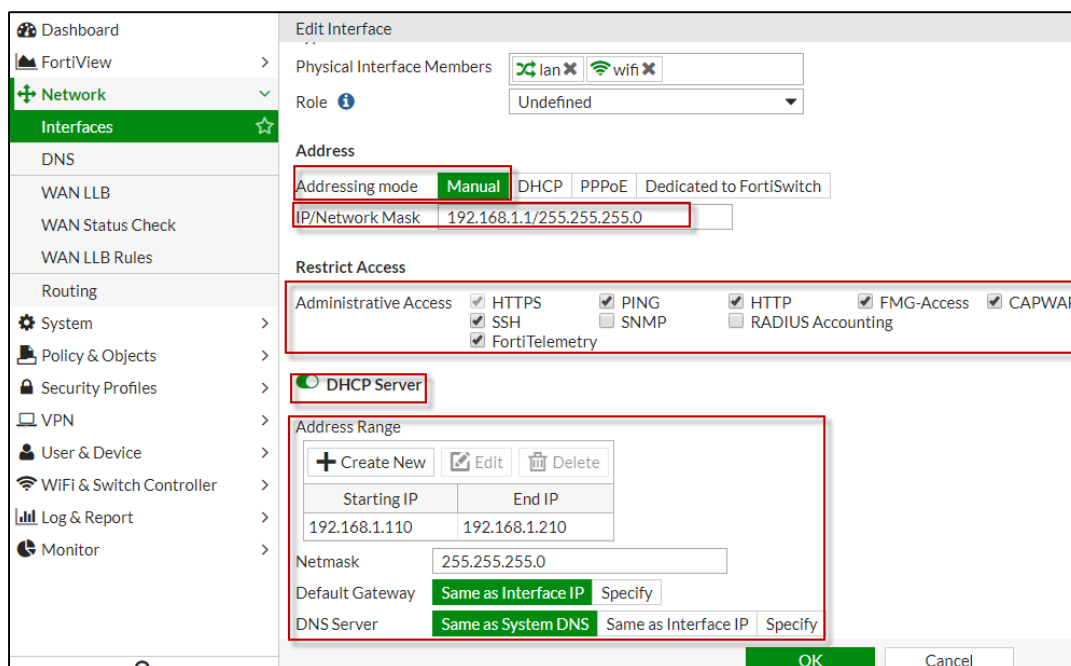


Figura 86: Configuración interfaz LAN acceso a red interna del cliente (Elaboración Propia, 2017)

Paso 6:

Crear una ruta estática, en la mayoría de casos es necesario, en este laboratorio al estar la red WAN obteniendo una dirección IP por medio de DHCP no es necesaria esta configuración.

Ir a Dashboard → Network → Routing y bajo Static Route se da click en Create New.

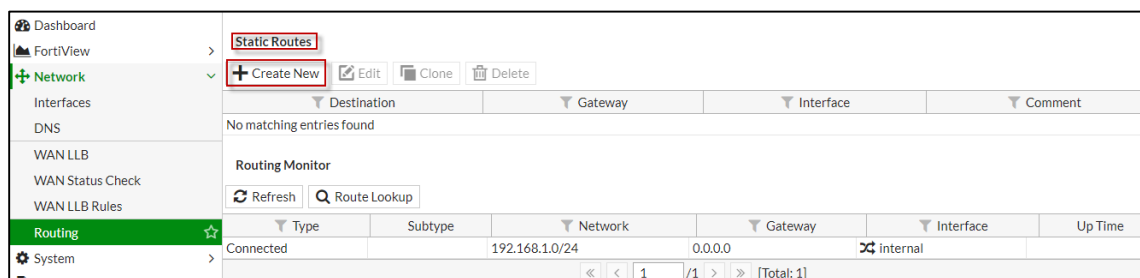


Figura 87: Configuración de una ruta estática (Elaboración Propia, 2017)

Se despliegan las siguientes opciones y se crea una ruta por defecto para salida a internet en caso de tener una dirección IP estática en la WAN, como se muestra en la figura 87.

Una ruta por defecto contiene en *Subnet* la dirección IP 0.0.0.0/0.0.0.0.

Device, la interfaz de salida del próximo salto, en este caso WAN

Gateway, la dirección IP del router del proveedor de internet, en este caso 192.168.0.1 y aplicar.

New Static Route

Destination **Subnet** Named Address Internet Service

0.0.0.0/0.0.0.0

Device INTERNET (wan)

Gateway 192.168.0.1

Administrative Distance 10

Comments

Status **Enabled** Disabled

Advanced Options

OK Cancel

Figura 88: Crear una ruta estática por defecto (Elaboración Propia, 2017)

Paso 7:

Ingresa los siguientes comandos para verificar los cambios en la interfaz CLI del Equipo.



Figura 89: Interfaz CLI del Equipo (Elaboración Propia, 2017)

Ir a Dashboard → CLI Console y dentro de esta interfaz digitar los siguientes comandos:

show system interface

En la figura 89 y 90 se verifica la configuración de red de la interfaz LAN y WAN del equipo.

```

Connected
FWF30D_LABORATORIO # show system interface
config system interface
edit "wan"
set mode dhcp
set allowaccess ping fgfm
set type physical
set alias "INTERNET"
set role wan
set snmp-index 1
next
edit "modem"

```

Figura 90: Verificar configuración interfaz WAN (Elaboración Propia, 2017)

```

CLI Console Detach ✎ ✕ -
--More--      edit "internal"
--More--      set ip 192.168.1.1 255.255.255.0
--More--      set allowaccess ping https ssh http fgfm capwap
--More--      set type switch
--More--      set fortiheartbeat enable
--More--      set snmp-index 6
--More--      next
--More--      edit "lan"
--More--      set type hard-switch
--More--      set snmp-index 4
--More--      next
--More--      end
FWF30D_LABORATORIO #

```

Figura 91: Verificar configuración interfaz LAN (Elaboración Propia, 2017)

show router static

```

CLI Console Detach ✎ ✕ -
--More--      set type hard-switch
--More--      set snmp-index 4
--More--      next
--More--      end
FWF30D_LABORATORIO # show router static
config router static
edit 1
set gateway 192.168.0.1
set device "wan"
next
end
FWF30D_LABORATORIO #

```

Figura 92: Verificar ruta estática (Elaboración Propia, 2017)

Paso 8:

Por último se puede cambiar la clave de ingreso al sistema.

Ir a Dashboard → System Information y Current Administrator escoger Change Password.

System Information	
Host Name:	FWF30D_LABORATORIO [Change]
Serial Number:	FWF30D3X14003087
Operation Mode:	NAT
Inspection Mode:	Proxy-based [Change]
System Time:	Tue Aug 1 09:20:15 2017 [Change]
Firmware Version:	v5.4.5,build1138 (GA) [Update]
System Configuration:	[Backup] [Restore] [Revisions]
Current Administrator:	admin [Change Password]/1 in Total [Details]
Uptime:	0 day(s) 1 hour(s) 42 min(s)

Figura 93: Cambio de password del sistema (Elaboración Propia, 2017)

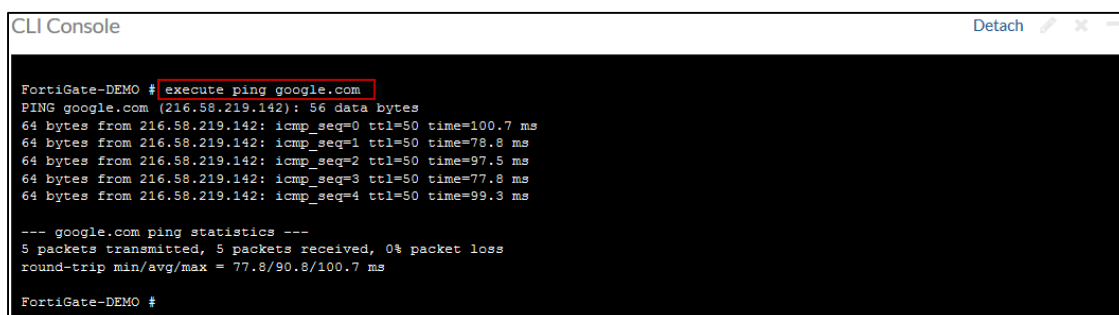
En esta práctica dejaremos el password por defecto. Es decir sin password de usuario admin.

Resultados:

Luego de realizar la configuración básica del equipo, el sistema debe ser capaz de tener navegación a internet.

Ir a Dashboard → CLI Console y ejecutar el comando:

execute ping google.com y el resultado es exitoso, tal como se muestra en la figura 93.



```

CLI Console
FortiGate-DEMO # execute ping google.com
PING google.com (216.58.219.142): 56 data bytes
64 bytes from 216.58.219.142: icmp_seq=0 ttl=50 time=100.7 ms
64 bytes from 216.58.219.142: icmp_seq=1 ttl=50 time=78.8 ms
64 bytes from 216.58.219.142: icmp_seq=2 ttl=50 time=97.5 ms
64 bytes from 216.58.219.142: icmp_seq=3 ttl=50 time=77.8 ms
64 bytes from 216.58.219.142: icmp_seq=4 ttl=50 time=99.3 ms

--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 77.8/90.8/100.7 ms
FortiGate-DEMO #
  
```

Figura 94: Verificar acceso a internet desde Fortigate (Elaboración Propia, 2017)

Al momento el equipo está listo y con acceso a internet.

4.4.3 Práctica N.-3 Respaldo de Configuraciones

Objetivos:

- Revisar los tipos de respaldos del equipo.
- Realizar respaldo del equipo

Escenario:

En la figura 94, se muestra una topología básica donde el estudiante debe simular y realizar el respaldo de configuración del equipo, indicadas en la práctica.

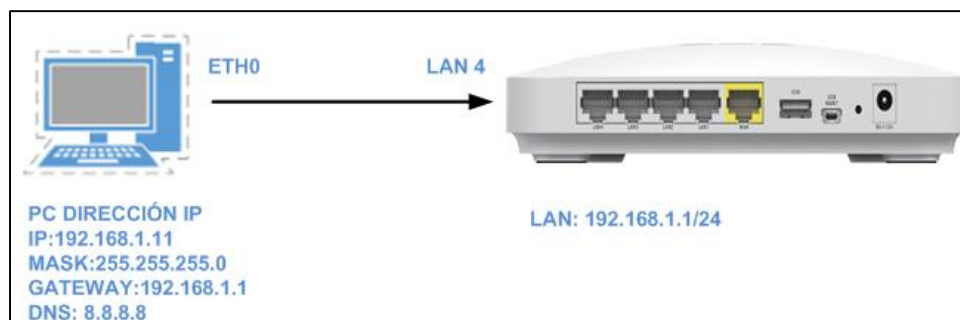


Figura 95: Topología para administrar Fortigate (Elaboración Propia, 2017)

Dispositivo	Nombre	Contraseña	Direccionamiento	
			Interfaz	IP
PC	NA	NA	NA	192.168.1.11/24
Fortigate 30D	admin		LAN 4	192.168.1.1/24

Tabla 6: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)

Materiales a utilizar en la práctica:

- Un Fortiwifi 30D
- Una computadora
- Un cable de red

Tiempo estimado:

Una hora aproximadamente

Desarrollo de la práctica:

Paso 1:

Ingreso al equipo.

Mediante un navegador Google Chrome o Firefox ingresar vía browser y digitar la siguiente dirección: <https://192.168.1.1> , aparece una advertencia de certificado, dar click en *advanced* y proceder a validar la advertencia.

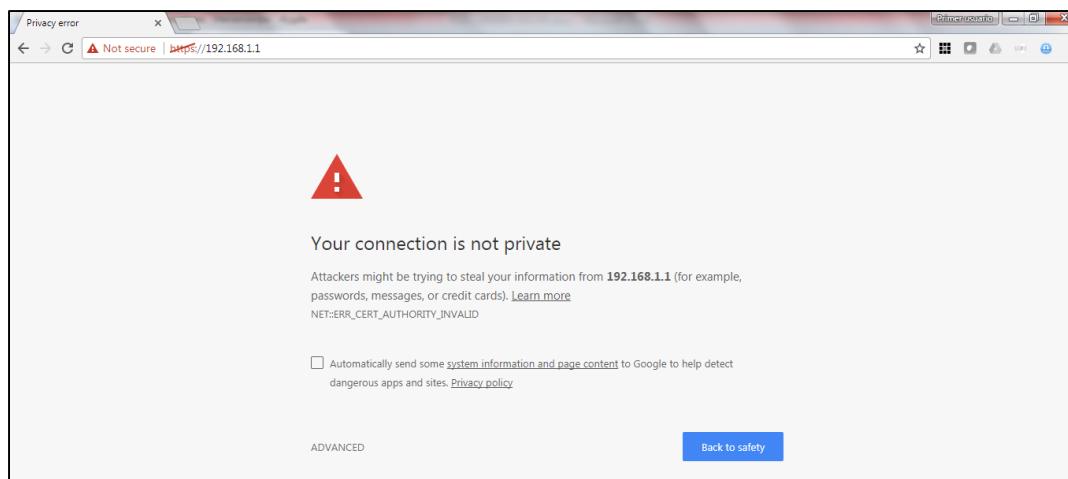


Figura 96: Acceso vía browser a <https://192.168.1.1> (Elaboración Propia, 2017)

Ingresar al equipo con el usuario: admin y sin password.

Figura 97: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)

Paso 2:

Backup de configuración del equipo sin encriptación

Ir a Dashboard → System Information → System Configuration y dar click en Backup.

System Information	
Host Name:	FWF30D_LABORATORIO [Change]
Serial Number:	FWF30D3X14003087
Operation Mode:	NAT
Inspection Mode:	Proxy-based [Change]
System Time:	Tue Aug 1 09:11:43 2017 [Change]
Firmware Version:	v5.4.5,build1138 (GA) [Update]
System Configuration:	[Backup] [Restore] [Revisions]
Current Administrator:	admin [Change Password] / 1 in Total [Details]
Uptime:	0 day(s) 1 hour(s) 34 min(s)

Figura 98: Realizar un backup de configuración del equipo (Elaboración Propia, 2017)

Escoger la opción backup a la PC local y OK.

Figura 99: Backup a PC local del usuario sin encriptación (Elaboración Propia, 2017)

Se descarga un archivo con el nombre del equipo, fecha y hora. Es recomendable cambiarlo de nombre para identificarlo de mejor manera.

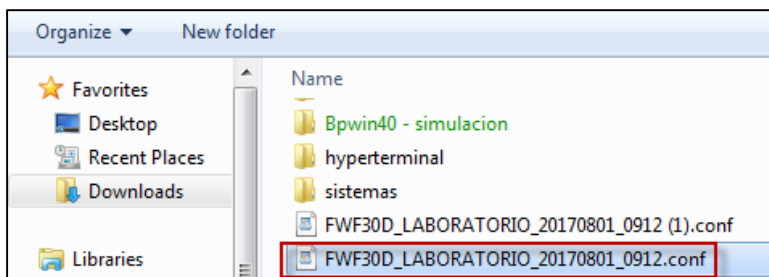


Figura 100: Nombre del archivo por defecto del backup de configuración (Elaboración Propia, 2017)

Paso 3:

Backup de configuración del equipo con encriptación

Ir a Dashboard → System Information → System Configuration y dar click en Backup.

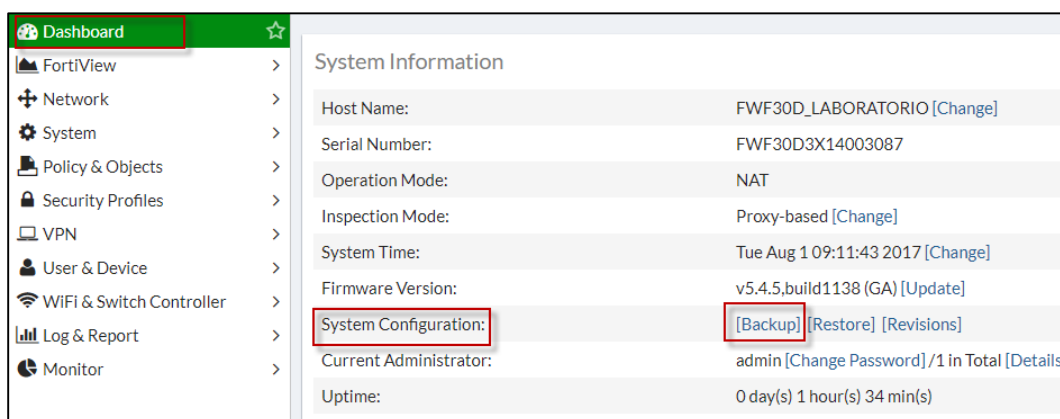


Figura 101: Realizar un backup de configuración del equipo (Elaboración Propia, 2017)

Escoger la opción backup a la PC local, habilitar la encriptación y digitar una contraseña, en este caso es **fortinet** y OK.

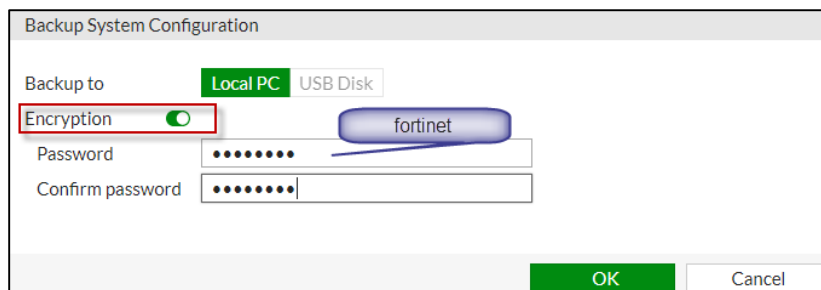


Figura 102: Backup a PC local del usuario con encriptación (Elaboración Propia, 2017)

Se descarga un archivo con el nombre del equipo, fecha y hora. Es recomendable cambiarlo de nombre para identificarlo de mejor manera.

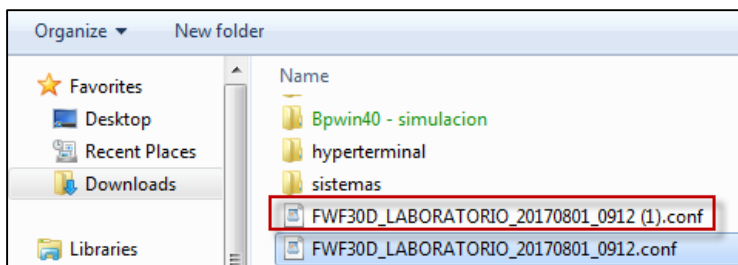


Figura 103: Nombre del archivo por defecto del backup de configuración (Elaboración Propia, 2017)

Paso 4:

Usar Wordpad o Notepad++ abra el archivo del backup con encriptación, en otra ventana el archivo sin encriptación y compare los detalles de ambos.

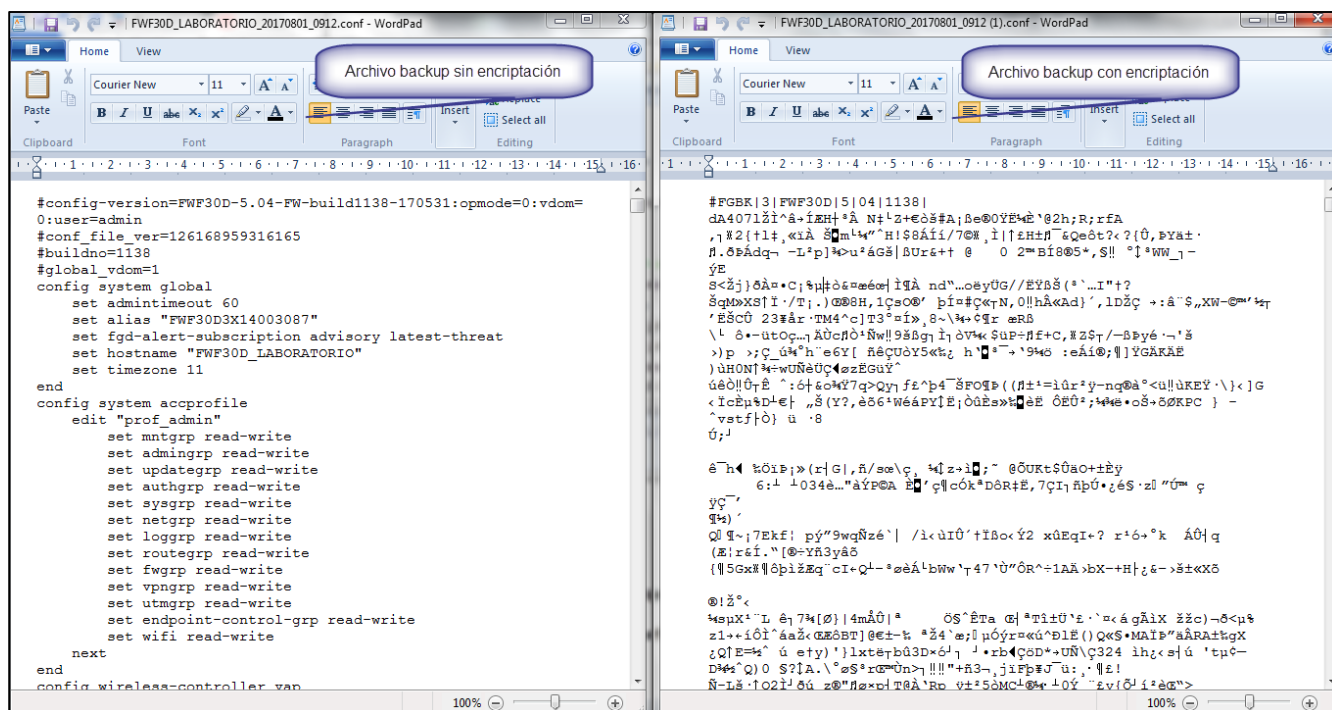


Figura 104: Comparación archivos de backup del sistema sin y con encriptación (Elaboración Propia, 2017)

Se puede observar que el archivo encriptado no es un archivo que se pueda leer, por ende la configuración está protegida.

Paso 5:

Restaurar un archivo de configuración.

De igual forma, como se realiza un backup del sistema, se puede realizar la restauración del mismo.

Ir a Dashboard → System Information → System Configuration y dar click en Restore.

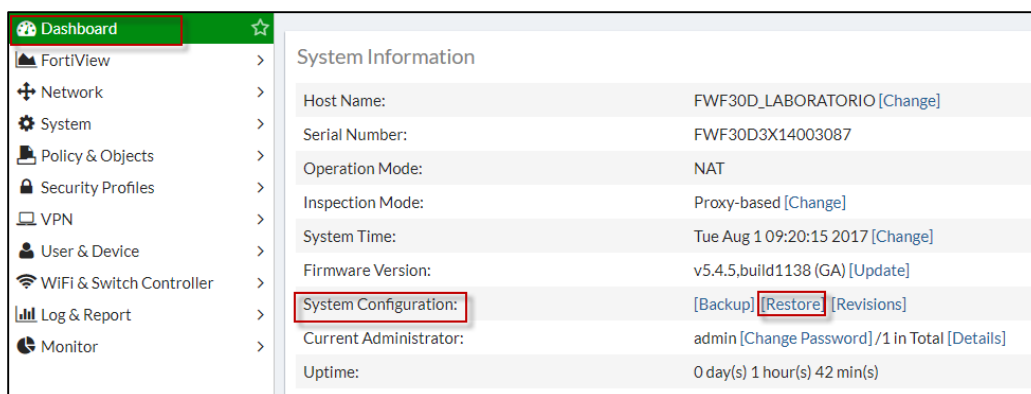


Figura 105: Realizar una Restauración de configuración del equipo (Elaboración Propia, 2017)

Escoger el archivo de configuración a restaurar, en caso de restaurar el archivo encriptado digitar la clave fortinet (si no está encriptado dejar en blanco el campo de *password*).



Figura 106: Restaurar el sistema con archivo de backup (Elaboración Propia, 2017)

El sistema se reinicia y sube la configuración que se encontraba en el *backup* respectivo.

Resultados

El *backup* puede ser realizado con y sin encriptación para una mayor seguridad, sin embargo al momento de realizar un *restore* se debe conocer la clave que fue digitada al momento de realizar el *backup*, caso contrario será invalido.

Se realiza la restauración del sistema sin problema.

4.4.4 Práctica N.-4 Configuración de objetos y políticas

Objetivos:

- Revisar los diferentes tipos de objetos que pueden ser configurados.
- Realizar política de navegación y dar acceso a internet a la PC de administración, simulando la red LAN del equipo.

Escenario:

En la figura 107, se muestra una topología básica donde el estudiante debe simularla y realizar la configuración para permitir el acceso a internet de los usuarios internos, indicadas en la práctica.

Al momento solo se tiene acceso a internet desde el equipo Fortigate, el objetivo es dar acceso a la PC que se encuentra configurada en la red LAN del cliente.

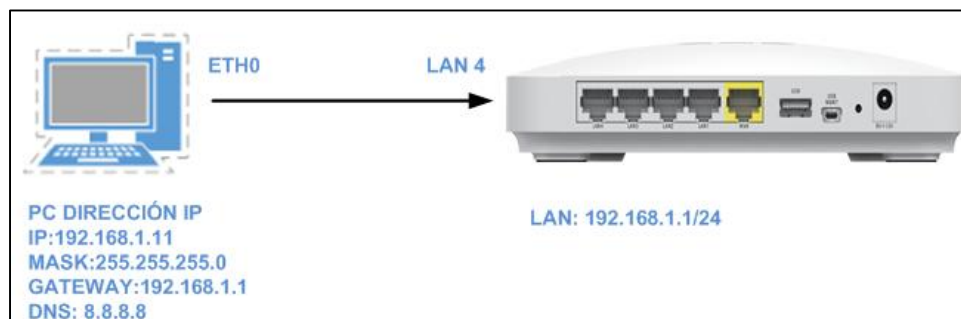


Figura 107: Topología para administrar Fortigate (Elaboración Propia, 2017)

Dispositivo	Nombre	Contraseña	Direccionamiento	
			Interfaz	IP
PC	NA	NA	NA	192.168.1.11/24
Fortigate 30D	admin		LAN 4	192.168.1.1/24

Tabla 7: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)

Materiales a utilizar en la práctica:

- Un Fortiwifi 30D
- Una computadora
- Un cable de red

Tiempo estimado:

Una hora aproximadamente

Desarrollo de la práctica:

Paso 1:

Ingreso al equipo.

Mediante un navegador Google Chrome o Firefox ingresar vía browser y digitar la siguiente dirección: <https://192.168.1.1> , aparece una advertencia de certificado, dar click en *advanced* y proceder a validar la advertencia.

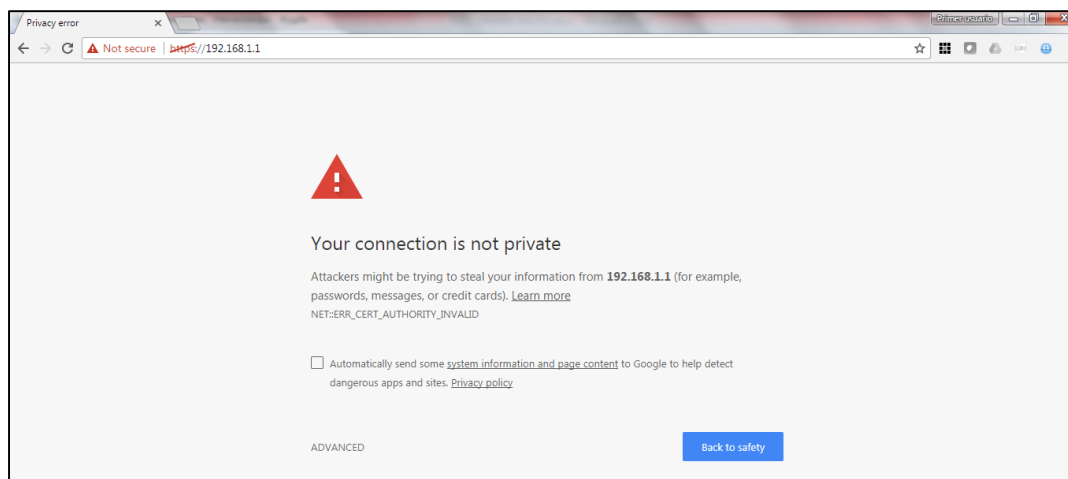


Figura 108: Acceso vía browser a <https://192.168.1.1> (Elaboración Propia, 2017)

Ingresar al equipo con el usuario: admin y sin password.

Figura 109: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)

Paso 2:

Crear la dirección IP de la PC como objeto.

Los objetos en Fortigate se refieren a direcciones IP's , rangos de IP's, FQDN (Fully Qualified Domain Name), grupo de direcciones IP públicas por países.

En este caso se crea la dirección IP de la PC que es la 192.168.1.1

Ir a Policy & Objects → Address.

Crear una nueva Address y setear :

Tipo: IP/Netmask,

Subnet/IP Range: la dirección IP que será asignada a la PC (192.168.1.11/32)

Interface a Any y guardar los cambios.

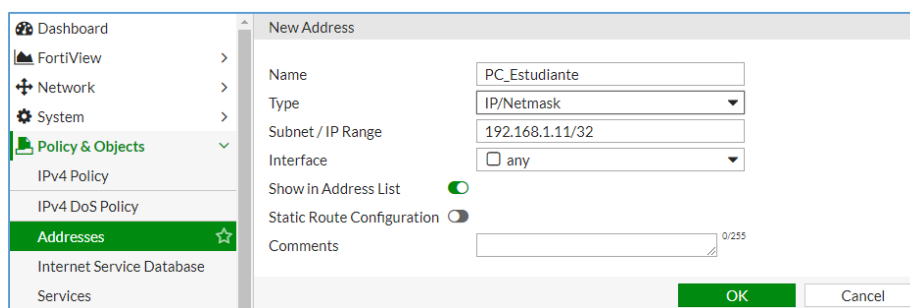


Figura 110: Crear la dirección IP de la PC como objeto

Paso 3

Crear la Política para acceso al internet.

Ir a Policy & Objects → IPv4 Policy, *Create new* y colocar los siguientes parámetros:

Incoming Interface: Internal (LAN interna)

Outgoing Interface: INTERNET (Wan)

Source: PC_Estudiante (el objeto que fue creado)

Destination Address: all

Schedule: always

Service: all

Action: Accept

Enable NAT.

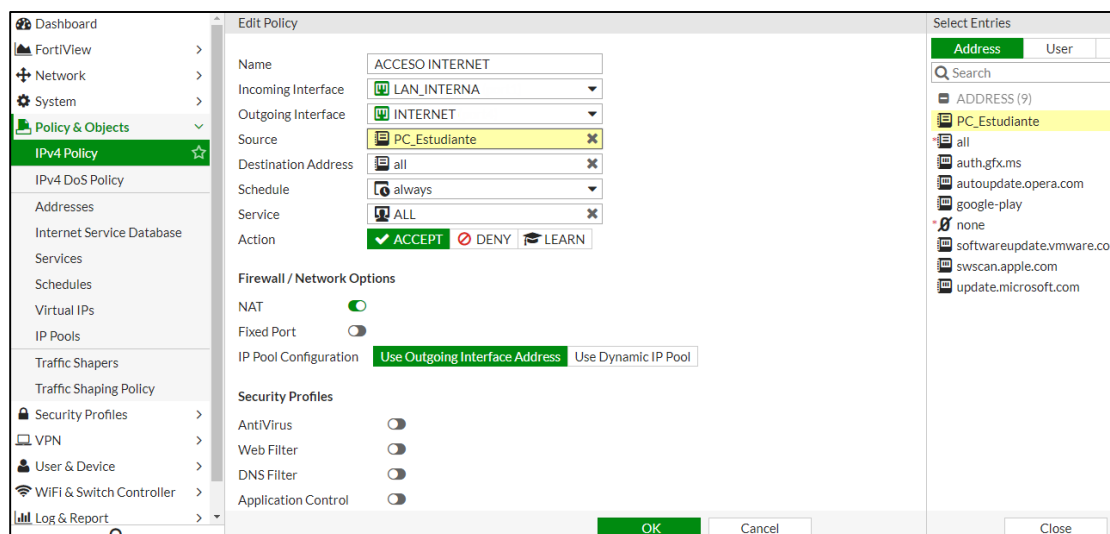
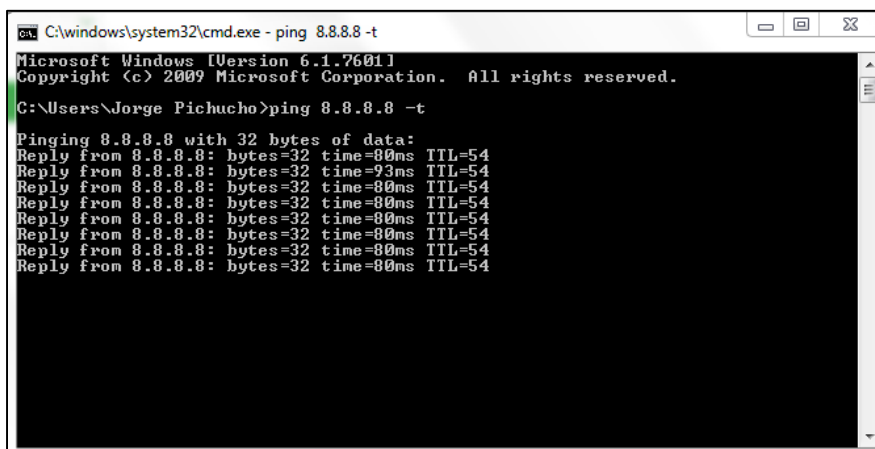


Figura 111: Crear política de navegación a internet a PC_Estudiante

Paso 4

Desde el PC, probar la conexión hacia el internet, realizando un ping al DNS de google.



```

C:\windows\system32\cmd.exe - ping 8.8.8.8 -t
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Jorge Pichucho>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=93ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54
Reply from 8.8.8.8: bytes=32 time=80ms TTL=54

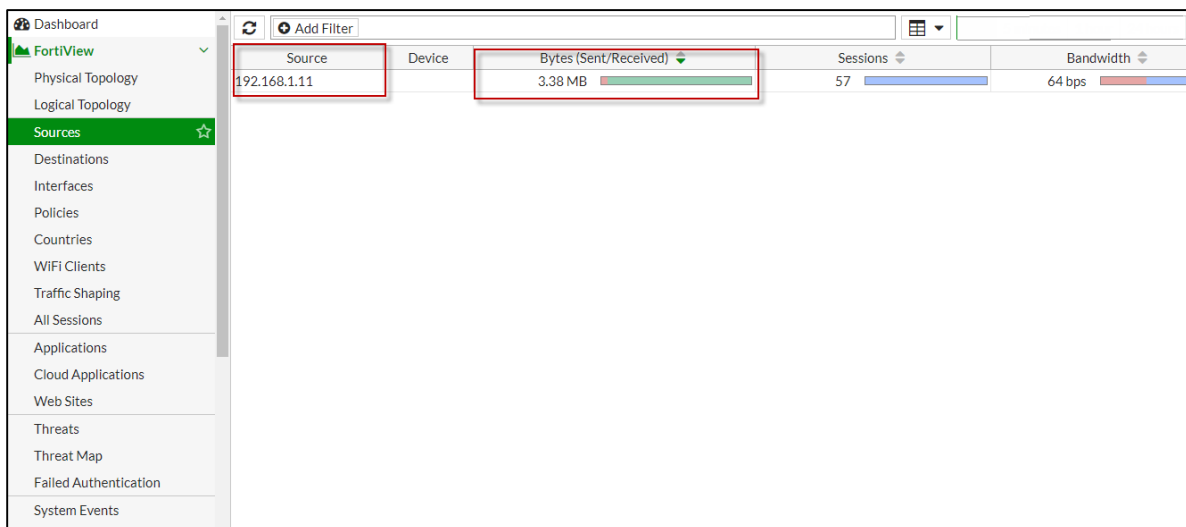
```

Figura 112: Prueba de salida a internet desde PC Estudiante (Elaboración Propia, 2017)

Resultados:

Se realiza navegación vía browser y se verifica en los logs de Fortigate que existe tráfico de salida a internet.

Ir a Fortiview → Source.



Source	Device	Bytes (Sent/Received)	Sessions	Bandwidth
192.168.1.11		3.38 MB	57	64 bps

Figura 113: Revisión de logs de tráfico desde la PC Estudiante 192.168.1.11

4.4.5 Práctica N.-5 Configuración de perfiles de seguridad

Objetivos:

- Revisar las diferentes funciones de seguridad que pueden ser configuradas.
- Crear un perfil de seguridad de aplicaciones y filtrado web
- Bloquear el acceso a cierta aplicación y página web

Escenario:

En la figura 114, se muestra una topología básica donde el estudiante debe simular y realizar la configuración de los perfiles de seguridad, indicados en la práctica.

Al momento se tiene acceso a internet desde la PC que se encuentra configurada en la red LAN del cliente, sin embargo se encuentra con navegación hacia el internet sin restricciones, el objetivo es bloquear cierto tráfico de internet y monitorear el mismo.

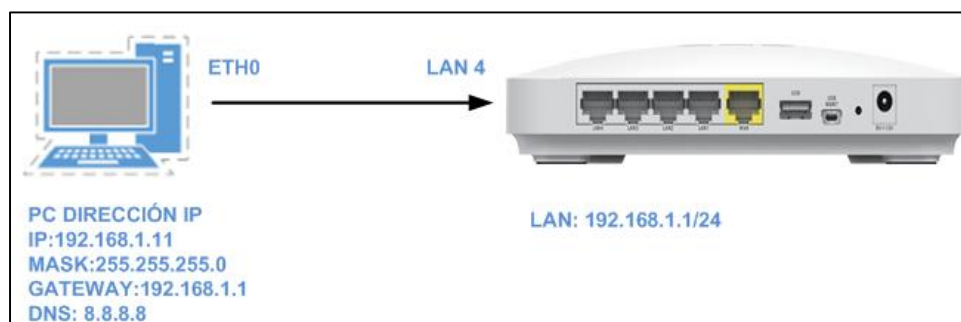


Figura 114: Topología para administrar Fortigate (Elaboración Propia, 2017)

Dispositivo	Nombre	Contraseña	Direccionamiento	
			Interfaz	IP
PC	NA	NA	NA	192.168.1.11/24
Fortigate 30D	admin		LAN 4	192.168.1.1/24

Tabla 8: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)

Materiales a utilizar en la práctica:

- Un Fortiwifi 30D

- Una computadora
- Un cable de red

Tiempo estimado:

Una hora aproximadamente

Desarrollo de la práctica:

Paso 1:

Ingreso al equipo.

Mediante un navegador Google Chrome o Firefox ingresar vía browser y digitar la siguiente dirección: <https://192.168.1.1> , aparece una advertencia de certificado, dar click en *advanced* y proceder a validar la advertencia.

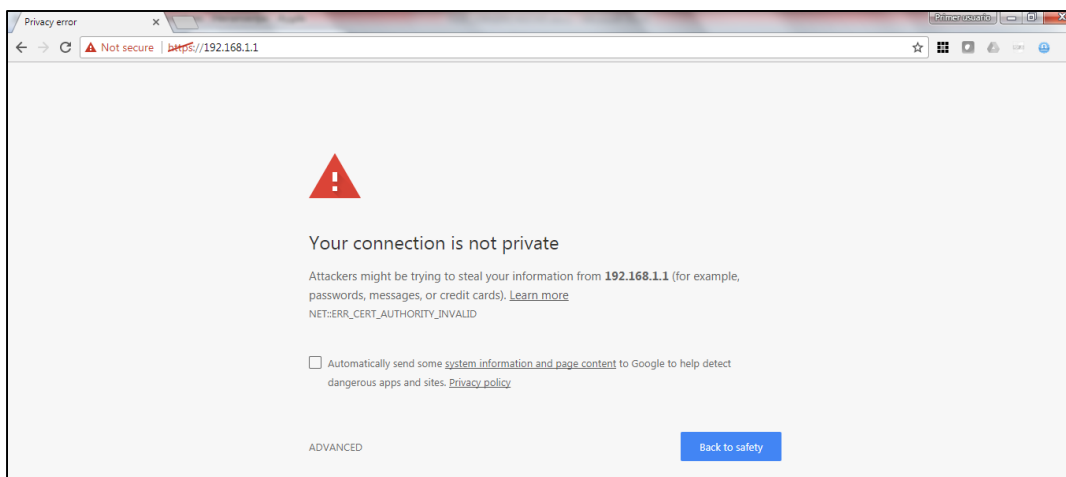


Figura 115: Acceso vía browser a <https://192.168.1.1> (Elaboración Propia, 2017)

Ingresar al equipo con el usuario: admin y sin password.

A screenshot of a login form with a green header. The form contains two input fields: the first is labeled "admin" and the second is labeled "Password". Below the fields is a green "Login" button.

Figura 116: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)

Paso 2:

Verificar en primer lugar el acceso a internet desde la PC (Práctica N.- 4) y comprobar que funcione sin problemas la aplicación TeamViewer

TeamViewer es una aplicación que nos permite conexión remota de un PC a otro, sin embargo puede servir para copiar información crítica de la PC del usuario y consumo de ancho de banda.

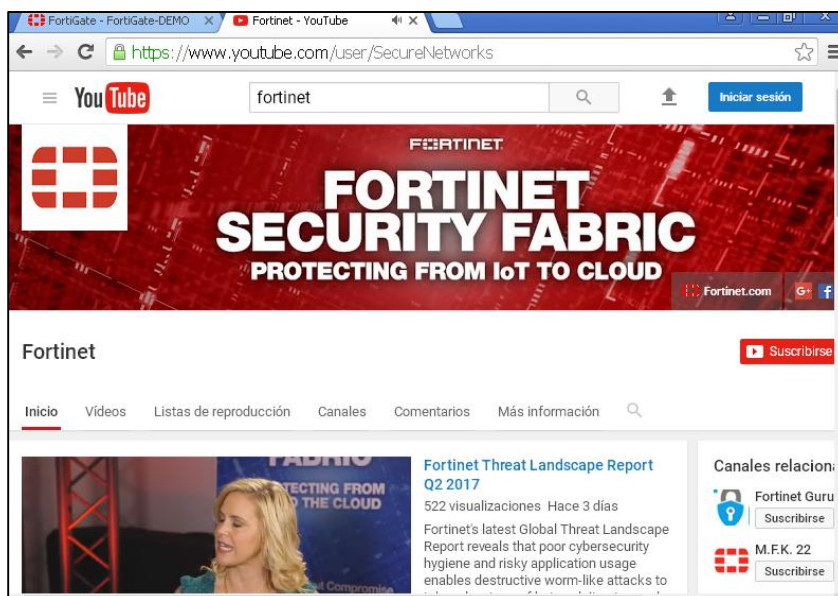


Figura 117: Verificar navegación a internet (Elaboración Propia, 2017).

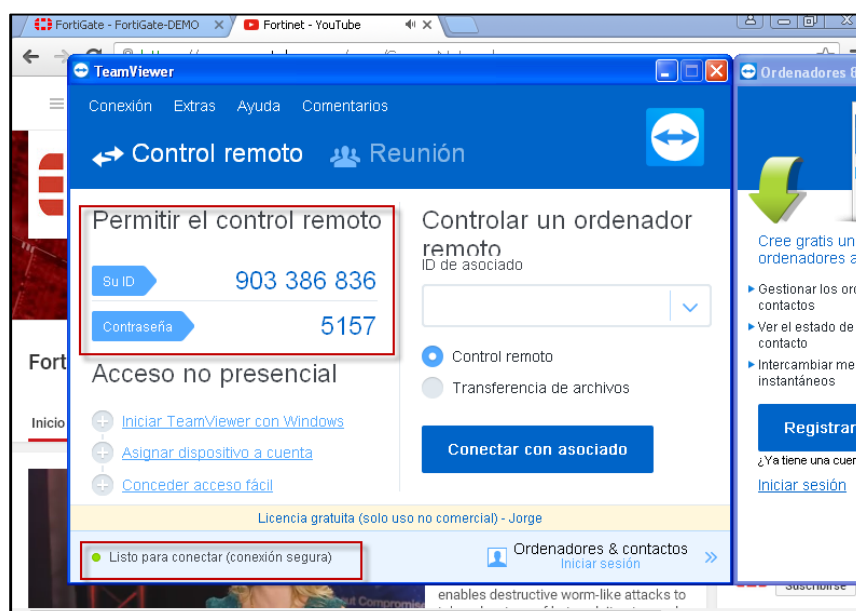


Figura 118: Verificar funcionamiento de aplicación Team Viewer (Elaboración Propia, 2017)

Una vez verificado el acceso a internet y correcto funcionamiento de TeamViewer, procedemos a bloquear la aplicación específica.

Paso 3:

Crear un perfil de seguridad de control de aplicaciones para bloquear la aplicación TeamViewer.

Ir a Security Profiles → Application Control → Application Sensor y crear un New Application Sensor para bloquear la aplicación TeamViewer.

Name: APP_BLOQUEO

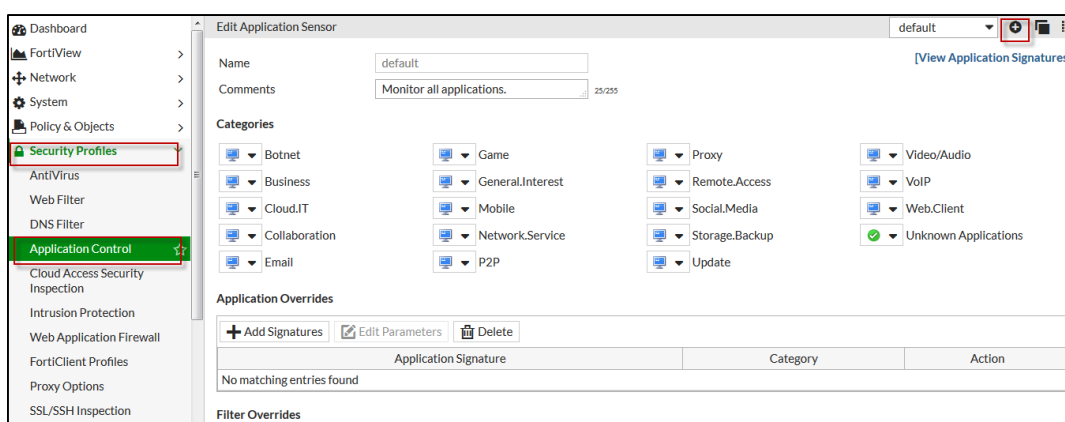


Figura 119: Crear un perfil de control aplicaciones (Elaboración Propia, 2017)

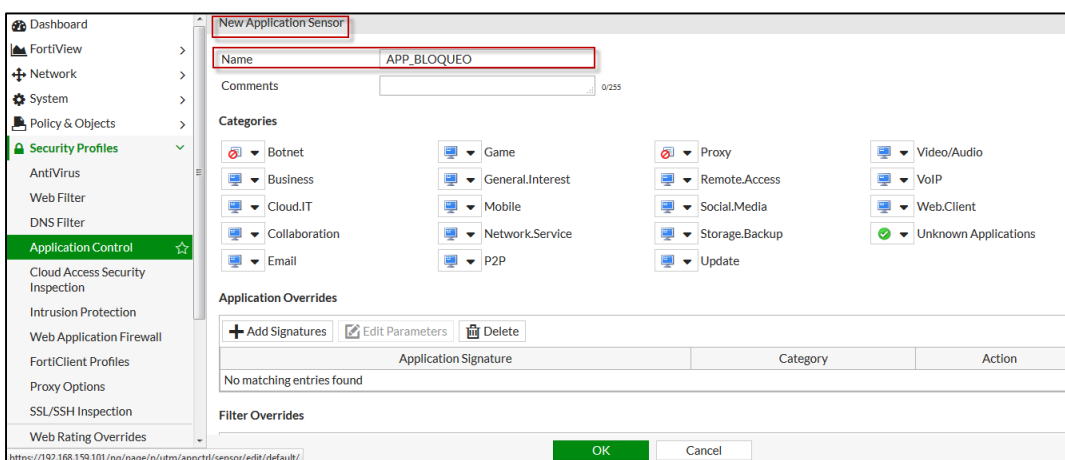


Figura 120: Crear un perfil de control aplicaciones (Elaboración Propia, 2017)

Seleccionar Add Signatures en Application Overrides.

En la lista de categorías, escoger el filtro name y buscar la aplicación TeamViewer, seleccionar la misma, escoger todas las opciones que aparecen en la lista y seleccionar User Selected Signature, por último OK para guardar el perfil.

Verificar que este configurada la Action a Block.

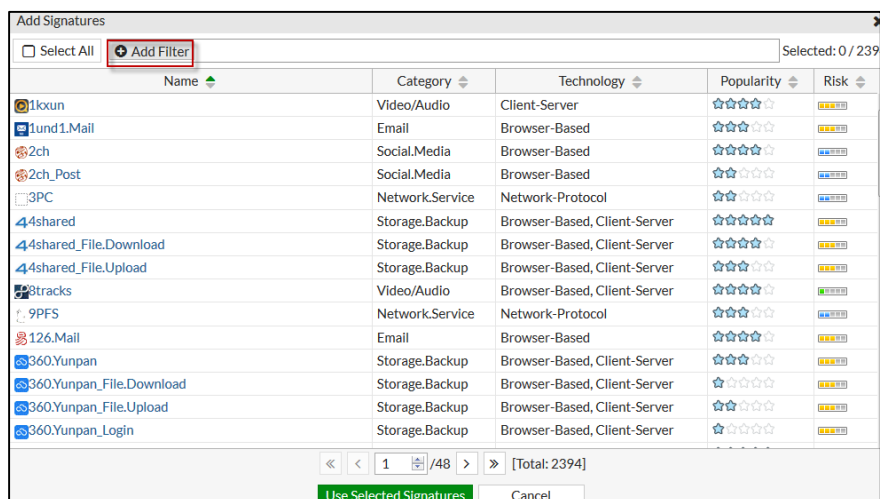


Figura 121: Escoger filtro de categorías (Elaboración Propia, 2017)

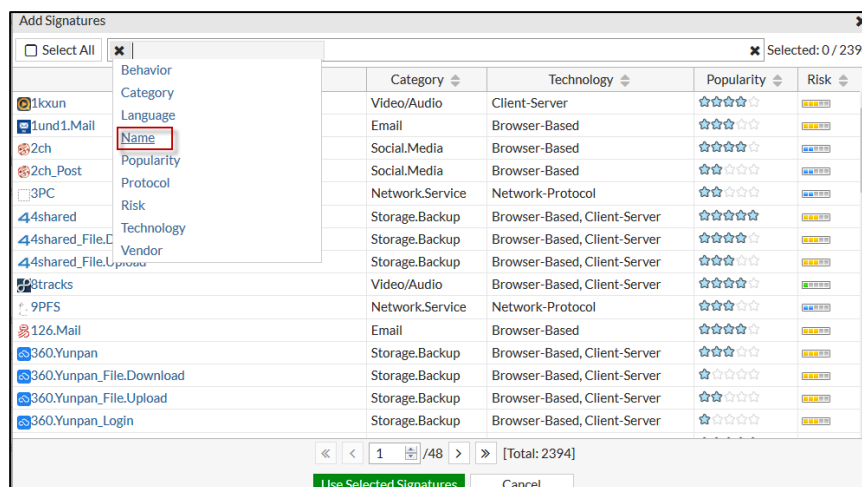


Figura 122: Elegir categoría Name (Elaboración Propia, 2017)

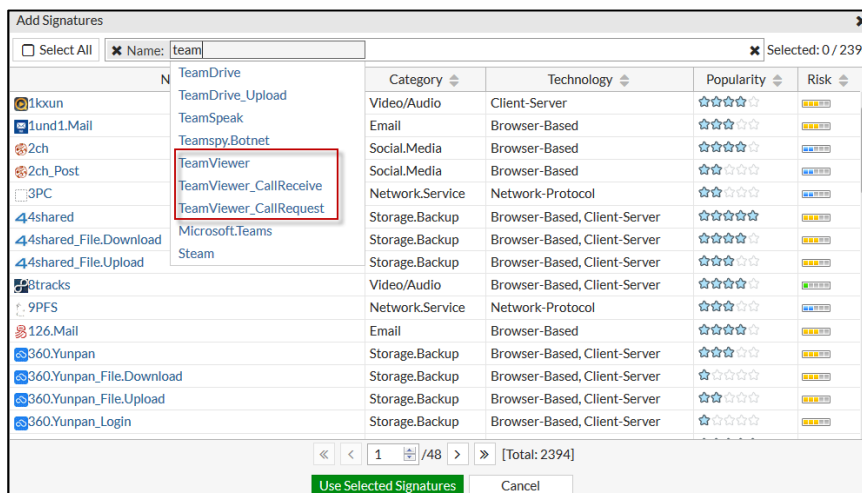


Figura 123: Digitar TeamViewer, aparece todos los nombres que coinciden (Elaboración Propia, 2017)

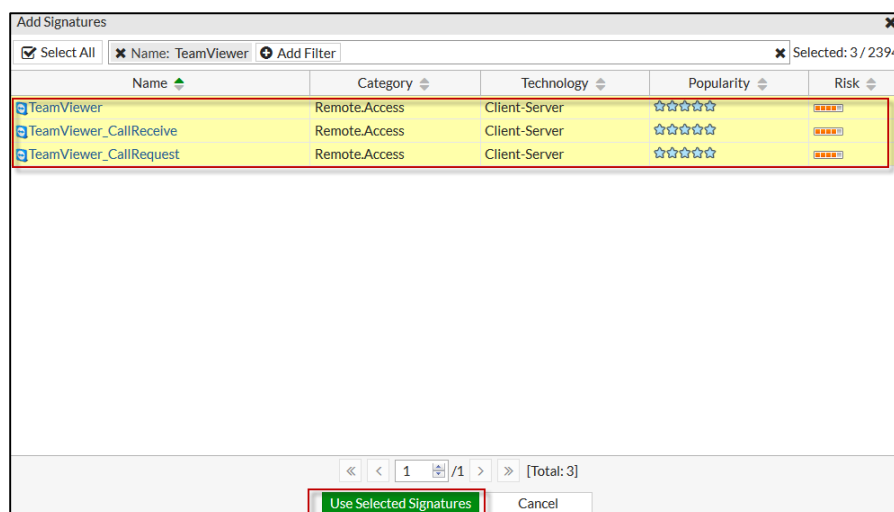


Figura 124: Escoger las aplicaciones seleccionadas (Elaboración Propia, 2017)

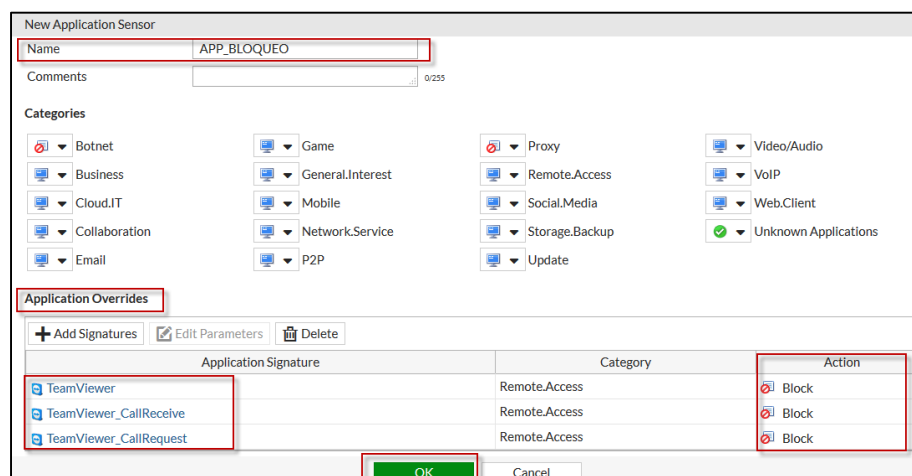


Figura 125: Agregar aplicaciones seleccionadas, verificar acción Block y guardar (Elaboración Propia, 2017)

Paso 4:

Agregar el perfil de control aplicaciones a la política de navegación creada en la práctica 4.

Ir a Policy&Objects → IPv4 Policy → Policy

Editar la política creada donde se permite la navegación de los usuarios internos hacia el internet.

Bajo Security Profiles, habilitar Application Control y configurar o escoger el perfil APP_BLOQUEO creado anteriormente y guardar los cambios.

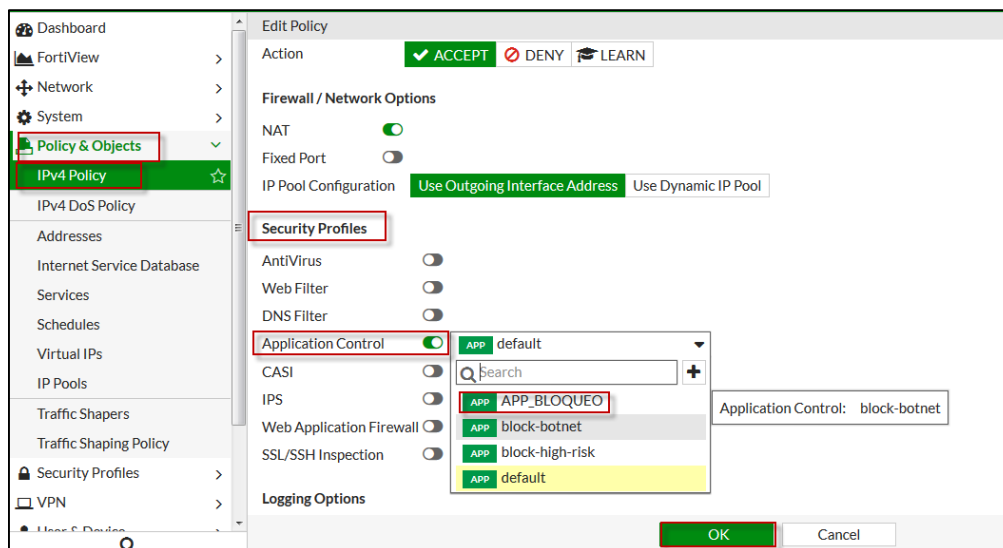


Figura 126: Aplicar el perfil de seguridad en la política de navegación a internet (Elaboración Propia, 2017)

Abrir nuevamente el Team Viewer, observar que no aparece ID, ni contraseña y se obtiene un mensaje que no está listo, compruebe su conexión. En este momento la aplicación fue bloqueada.

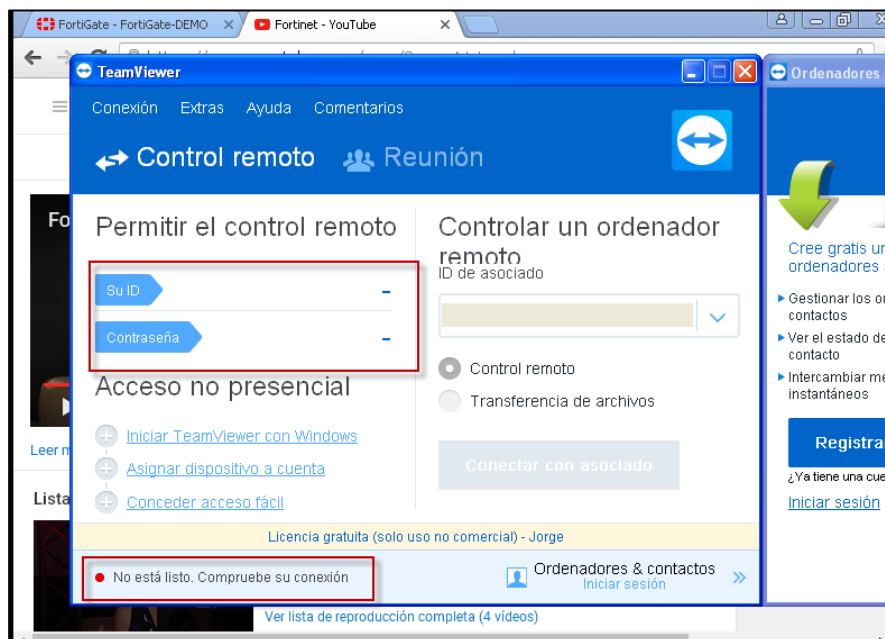


Figura 127: Aplicación de Team Viewer bloqueada (Elaboración Propia, 2017)

Paso 5:

Bloquear acceso a página web www.fortinet.com con módulo de Filtrado Web.

Ir a Security Profile → Web Filter → Agregar un nuevo perfil

Name: WEBFILTER_BLOQUEO

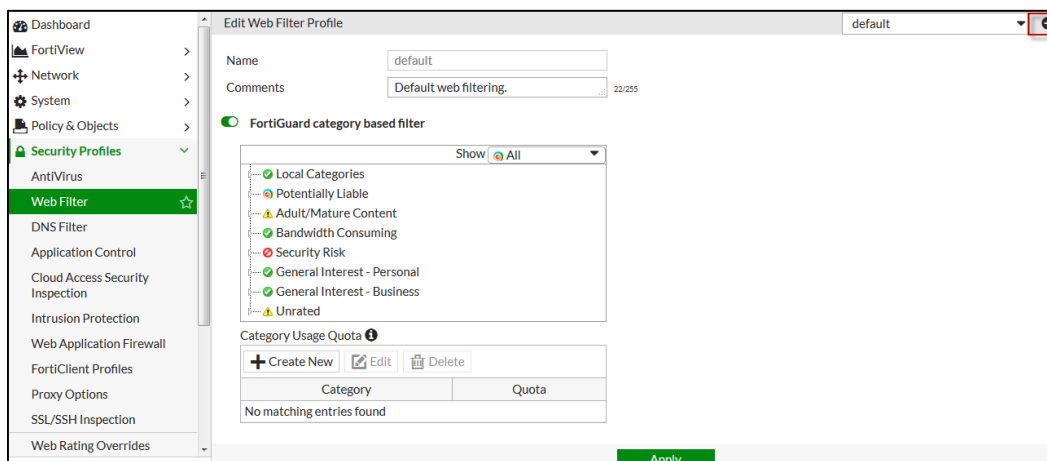


Figura 128: Agregar perfil de Filtrado Web (Elaboración Propia, 2017)

Ir a URL Filter y habilitarlo, crear un nuevo filtro con los siguientes campos:

URL: *.fortinet.com

Type: Wildcard

Action: Block

Status: Habilitar

Dar click en aplicar y se guarda el nuevo perfil creado de Filtrado WEB.

La configuración que se realizó, bloqueará la navegación vía browser a www.fortinet.com.

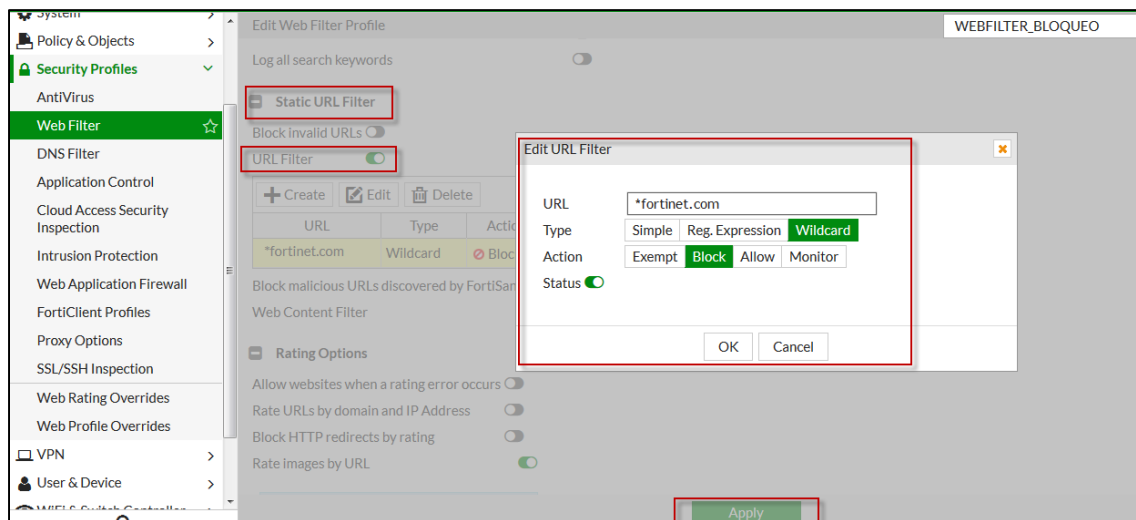


Figura 129: Crear perfil de filtrado web para bloquear acceso a www.fortinet.com (Elaboración Propia, 2017)

Paso 6:

Agregar el perfil de filtrado web a la política de navegación creada en la práctica 4.

Ir a Policy&Objects → IPv4 Policy → Policy

Editar la política creada donde se permite la navegación de los usuarios internos hacia el internet.

Bajo Security Profiles, habilitar Web Filter y configurar o escoger el perfil WEBFILTER_BLOQUEO creado anteriormente y guardar los cambios.

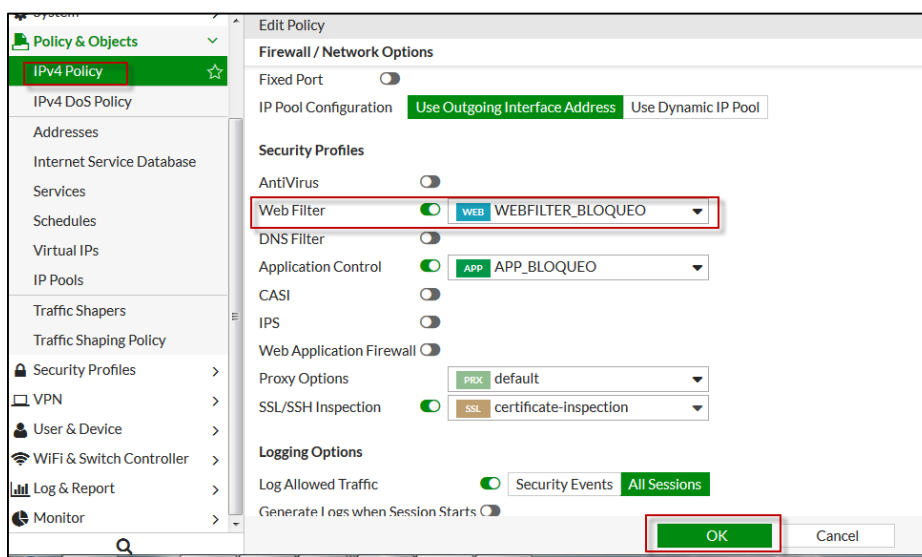


Figura 130: Aplicar el perfil de seguridad en la política de navegación a internet (Elaboración Propia, 2017)

Intentar navegar desde la PC del estudiante vía browser a www.fortinet.com, aparece que la página está bloqueada por Web Filtering.



Figura 131: Mensaje de página bloqueada (Elaboración Propia, 2017)

Resultados

Ir a FortiView → Applications → Escoger TeamViewer. Observar que el sensor está trabajando ya que se verifica que desde la dirección IP: 192.168.1.11 hay una sesión a TeamViewer sin embargo el ancho de banda es de 0bps, esto significa que no tiene conexión al servidor de TeamViewer.

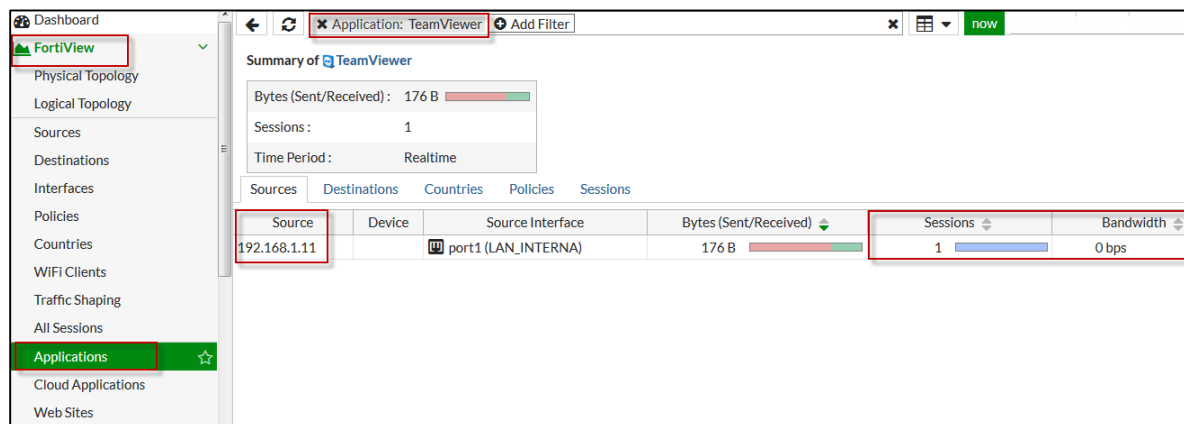


Figura 132: Revisión de logs Fortigate (Elaboración Propia, 2017)

4.4.6 Práctica N.-6 Antivirus

Objetivos:

- Configurar el módulo de antivirus.
- Crear un perfil de seguridad de antivirus
- Test de descarga de virus

Escenario:

En la figura 133, se muestra una topología básica donde el estudiante debe simularla y realizar la configuración del perfil de antivirus, indicadas en la práctica.

Al momento se tiene acceso a internet desde la PC que se encuentra configurada en la red LAN del cliente, sin embargo se encuentra con navegación hacia el internet sin restricciones, el objetivo es tratar de descargar un virus, simulando un ataque de este tipo y bloquear el mismo.

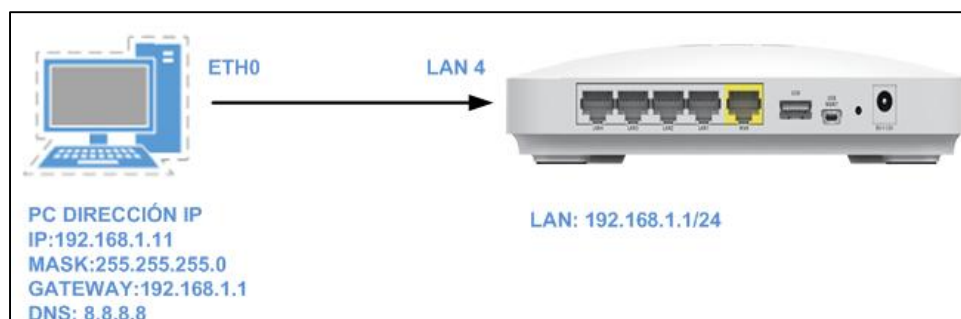


Figura 133: Topología para administrar Fortigate (Elaboración Propia, 2017)

Dispositivo	Nombre	Contraseña	Direccionamiento	
			Interfaz	IP
PC	NA	NA	NA	192.168.1.11/24
Fortigate 30D	admin		LAN 4	192.168.1.1/24

Tabla 9: Direccionamiento IPV4 para administración Fortigate (Elaboración Propia, 2017)

Materiales a utilizar en la práctica:

- Un Fortiwifi 30D
- Una computadora
- Un cable de red

Tiempo estimado:

Una hora aproximadamente

Desarrollo de la práctica:

Paso 1:

Ingreso al equipo.

Mediante un navegador Google Chrome o Firefox ingresar vía browser y digitar la siguiente dirección: <https://192.168.1.1> , aparece una advertencia de certificado, dar click en *advanced* y proceder a validar la advertencia.

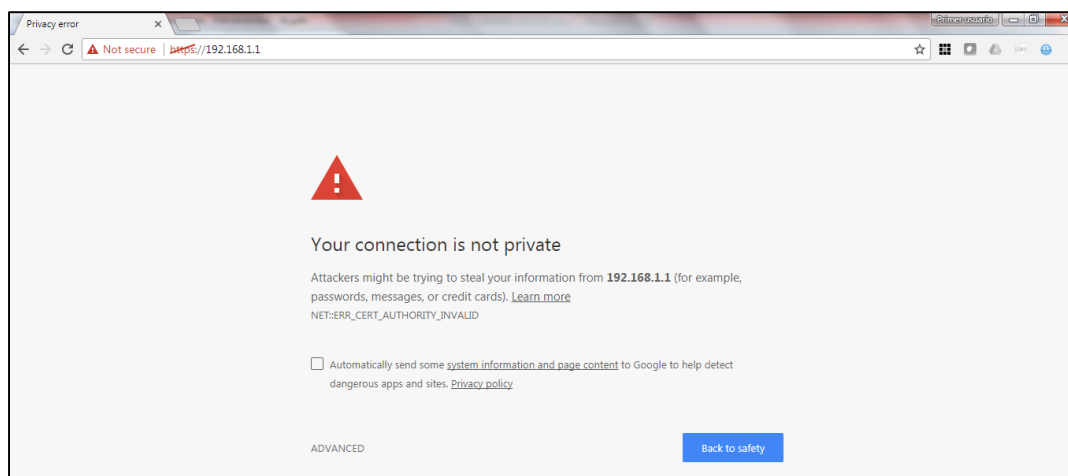


Figura 134: Acceso vía browser a <https://192.168.1.1> (Elaboración Propia, 2017)

Ingresar al equipo con el usuario: admin y sin password.

Figura 135: Ingreso de credenciales al equipo Fortigate (FortinetDocs, 2013)

Paso 2:

Verificar en primer lugar el acceso a internet desde la PC (Práctica N.- 4).

Paso 3:

Crear un perfil de seguridad de antivirus para bloquear ataques de virus.

Ir a Security Profiles → Antivirus → y crear un New Antivirus Profile para bloquear ataques de virus.

Name: ANTIVIRUS_GENERAL

Detect Viruses: Block

Inspected Protocols: Habilitar todos los protocolos.

Inspection Option: Dejar por default y aplicar los cambios.

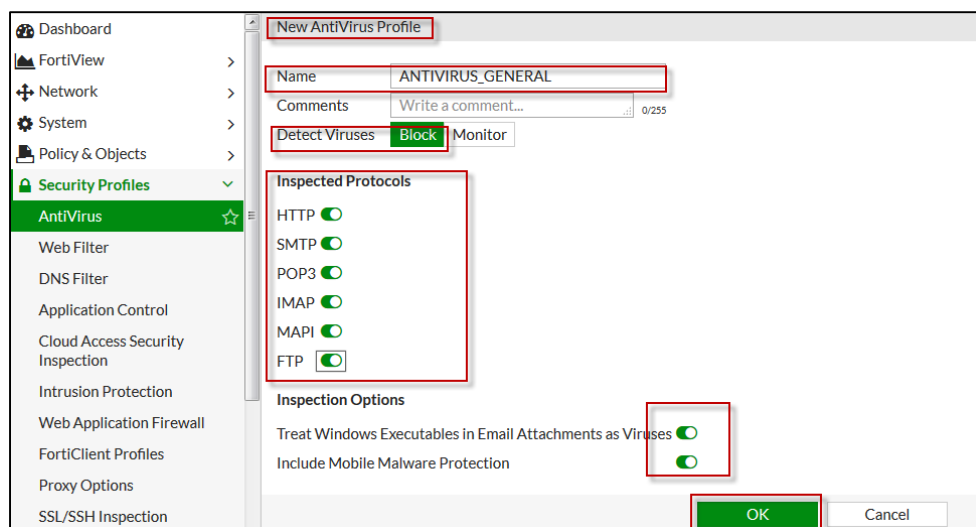


Figura 136: Crear perfil de antivirus para bloquear ataques de antivirus (Elaboración Propia, 2017)

Paso 4:

Agregar el perfil de antivirus a la política de navegación creada en la práctica 4.

Ir a Policy&Objects → IPv4 Policy → Policy

Editar la política creada donde se permite la navegación de los usuarios internos hacia el internet.

Bajo Security Profiles, habilitar Web Filter y configurar o escoger el perfil ANTIVIRUS_GENERAL creado anteriormente y guardar los cambios.

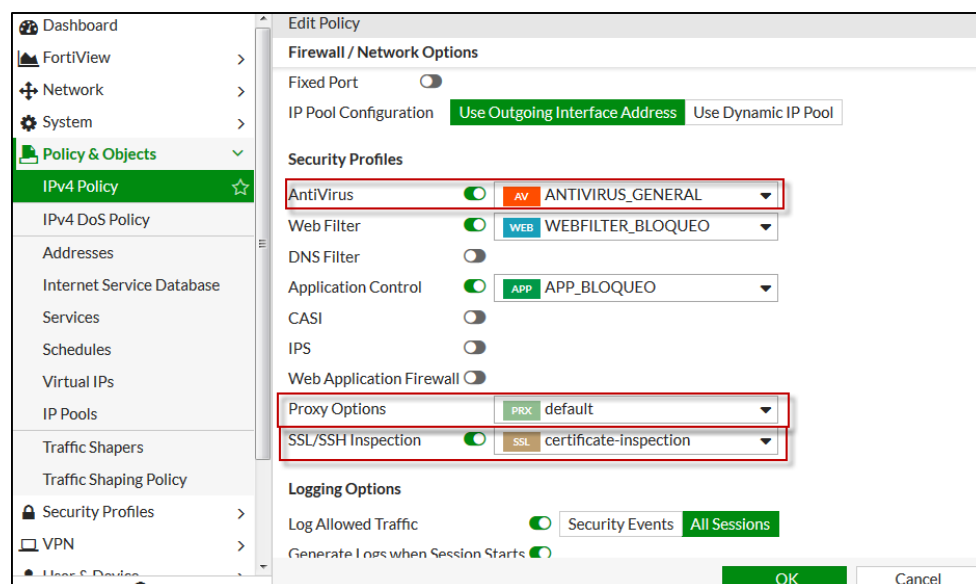


Figura 137: Aplicar el perfil de seguridad en la política de navegación a internet (Elaboración Propia, 2017)

Paso 5:

Desde la PC del estudiante ir a www.eicar.org → Download Anti Malware → Download y escoger eicar.com.

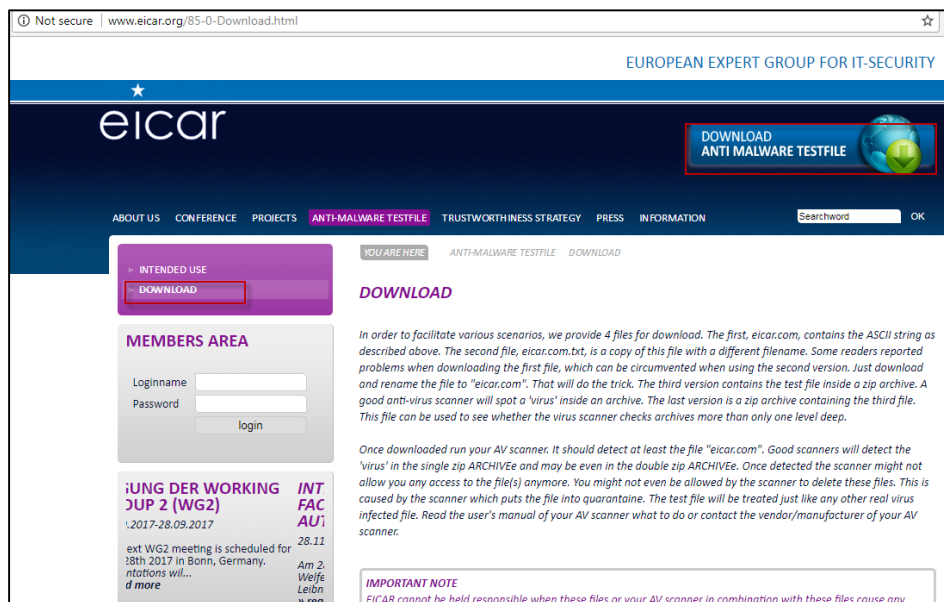


Figura 138: Ingresar a la página web www.eicar.org (Elaboración Propia, 2017)

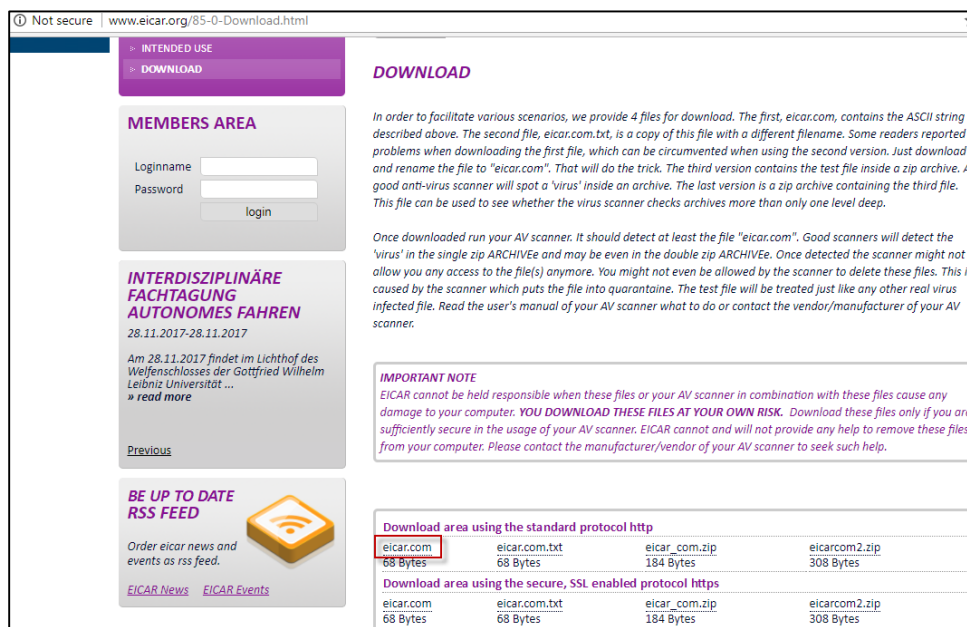


Figura 139: Descargar el archivo eicar.com (Elaboración Propia, 2017)

Resultados:

Al descargar el antivirus se muestra un mensaje que ha sido bloqueado y no puede ser descargado porque contiene virus.

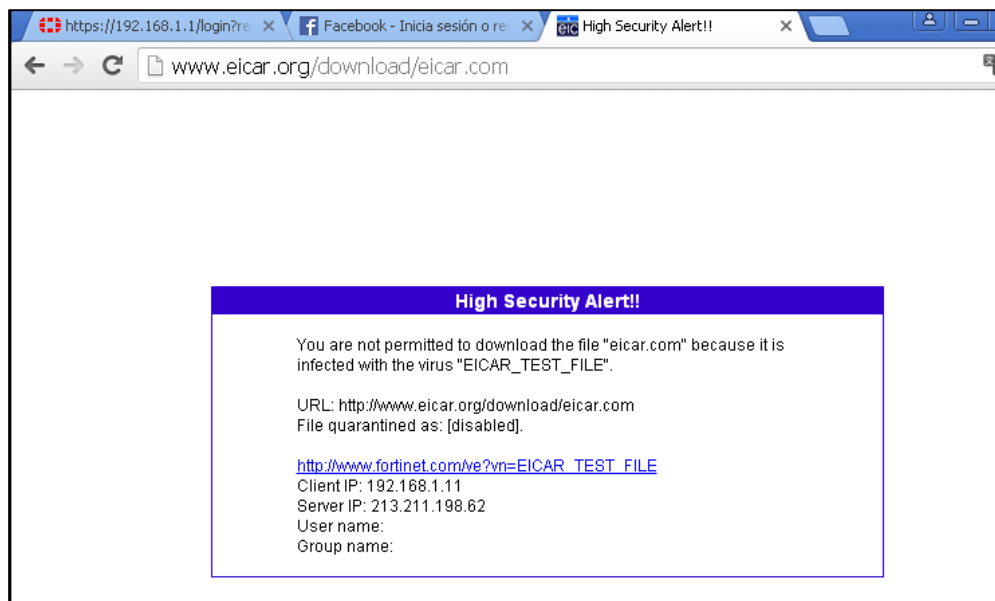


Figura 140: Bloqueo al descargar archivo infectado con virus (Elaboración Propia, 2017)

Ir a Fortiview → Threats y verificar los logs del virus y desde que dirección IP fueron generados. Es muy importante tomar en cuenta la dirección IP del usuario final, ya que puede tratarse de un malware y trate de infectar otros dispositivos, sin embargo el Fortigate lo aísla para que no se propague vía red el mismo.

5. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

En este proyecto se trató de dar a conocer lo que es seguridad perimetral y UTM, primero con fundamentación teórica, para posteriormente exponer las fases necesarias para la implementación de un sistema de Gestión Unificado de Amenazas en la Universidad Israel.

Con respecto al análisis de las tecnologías UTM, se llegó a la conclusión de que por arquitectura, diseño y costos, el equipo con mejor características fue del fabricante Fortinet.

En razón al equipamiento necesario, se optó por el modelo de equipo Fortiwifi 30D ya que cumple con el dimensionamiento necesario y logra cumplir el desarrollo de las prácticas.

Por otro lado el diseño de las prácticas fue elaborado de acuerdo a las recomendaciones y mejores prácticas sugeridas por el fabricante Fortinet.

Asimismo la elaboración de las prácticas de UTM, basadas en la guía de laboratorio realizada, generara un gran aporte, logrando que el estudiante conozca la tecnología y las funciones de un equipo de primera línea.

Además al realizar el troubleshooting con problemas reales y observar los resultados en cada una de las prácticas realizadas, ayudaran al estudiante a entender el comportamiento y manejo de logs y eventos de un dispositivo de seguridad perimetral.

Finalmente se desarrolla la memoria técnica de la implementación del sistema, con el propósito de que el personal que esté a cargo del módulo, tenga la información necesaria del mismo para ponerlo en producción y realizar las prácticas sin inconvenientes.

RECOMENDACIONES

Es importante utilizar el módulo para que el estudiante aproveche al máximo las capacidades y funciones que ofrece el equipo.

Se debería implementar otras prácticas adicionales, ya que el equipo cuenta con otros módulos adicionales incluidos, tales como Protección de Fuga de Información, VPN (*Virtual Private Network*), Portal Captivo, Dominios Virtuales, Navegación y autenticación de usuarios locales, que no pudieron ser realizadas debido a factor tiempo.

6. BIBLIOGRAFÍA

- Aliexpres. (2017). <https://es.aliexpress.com>. Obtenido de <https://es.aliexpress.com>:
<https://es.aliexpress.com/cheap/cheap-db9-female-rj45.html>
- Alulema, D. (Junio de 2008). Estudio y diseño de un sistema de seguridad perimetral para la red Quito Motors. *Tesis*. Quito, Pichincha, Ecuador.
- anica, blogspot. (01 de 03 de 2009). *blog, Modelos OSI y TCP/IP*. Obtenido de modelos-osi-y-tcp-ip-anica.blogspot.com:
<http://modelos-osi-y-tcp-ip-anica.blogspot.com/>
- Aportavalor. (Enero de 2013). <http://aportavalor.com>. Obtenido de
<http://aportavalor.com/glosario/firewall/>
- Benchimol, D. (2011). Hacking desde Cero. En D. Benchimol, *Hacking desde Cero* (págs. 14-30). Buenos Aires: Fox Andina.
- Books.google. (2017). <https://books.google.com.ec>. Obtenido de <https://books.google.com.ec>:
<https://books.google.com.ec/books?id=b753DQAAQBAJ&pg=PA350&lpq=PA350&dq=Permiten+controlar+las+conexiones+de+red+que+acepta+o+emite+un+dispositivo,+ya+sean+conexiones+a+trav%C3%A9s+de+Internet+o+de+otro+sistema&source=bl&ots=tEQQ4p1Eks&sig=kWDxXXBfgaululC>
- Cely, J. M. (2015). *Modelo TCP/IP*. Obtenido de <http://giret.ufps.edu.co/cisco>:
http://giret.ufps.edu.co/cisco/docs/material/ccna1_cap11b.pdf
- Cisco. (2016). www.cisco.com. Obtenido de www.cisco.com:
http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
- Cisco Networking Academy. (2016). *Cursos y certificaciones*. Obtenido de <https://www.netacad.com>:
<https://www.netacad.com/es/web/about-us/courses-and-certifications>
- Ecured. (Junio de 2017). <https://www.ecured.cu>. Obtenido de <https://www.ecured.cu>:
<https://www.ecured.cu/Router>
- EdwinRSV. (09 de Junio de 2011). <https://guardnet.wordpress.com>. Obtenido de
<https://guardnet.wordpress.com>: <https://guardnet.wordpress.com/2011/06/09/capa-de-seguridad-perimetral/>
- Fabian Frank. (18 de 06 de 2009). *Enrutamiento estático*. Obtenido de <http://www.monografias.com/>:
http://www.monografias.com/usuario/perfiles/fabian_frank/monografias
- filezilla-project.org. (2016). *filezilla free FTP*. Obtenido de <https://filezilla-project.org>: https://filezilla-project.org/download.php?show_all=1
- Forospyware. (Agosto de 2009). <http://www.forospyware.com>. Obtenido de
<http://www.forospyware.com>: <http://www.forospyware.com/t266312.html>
- Fortinet. (05 de 2017). <https://www.fortinet.com>. Obtenido de
https://www.fortinet.com/content/.../FortiSwitch_D_Series.pdf

- Fortinet. (2017). *www.fortinet.com*. Obtenido de www.fortinet.com:
<https://www.fortinet.com/solutions/small-business/connected-utm.html>
- FortinetDocs. (06 de Julio de 2013). *http://docs.fortinet.com*. Obtenido de <http://docs.fortinet.com>:
<http://docs.fortinet.com/fortigate/hardware/30d>
- Gartner. (20 de Junio de 2017). *https://www.gartner.com*. Obtenido de <https://www.gartner.com>:
<https://www.gartner.com/doc/reprints?id=1-43QT4Y6&ct=170621&st=sb&elqTrackId=E850DEA71AC725B0DF33D12317D64181&elq=95a39e4966014e6ba0849676c54a4590&elqaid=3226&elqat=1&elqCampaignId=>
- Gartner_Inc. (2017). *http://www.gartner.com*. Obtenido de <http://www.gartner.com>:
http://www.gartner.com/technology/why_gartner.jsp
- Geekistuff. (01 de Septiembre de 2014). *http://www.geekistuff.com*. Obtenido de <http://www.geekistuff.com>: <http://www.geekistuff.com/script-kiddie/>
- Gonzalez, M. S. (2016). *Redes telematicas*. Obtenido de <http://redestelematicas.com/>:
<http://redestelematicas.com/direccionamiento-ipv4/>
- Gonzalez, R. (2015). *Ventajas de las Vlans*. Obtenido de <https://sites.google.com/site>:
<https://sites.google.com/site/isaacivantorresgonzalezvlan/home/ventajas-de-las-vlan>
- Greenetics. (23 de 09 de 2016). *Curso de Hacking Ético Avanzado. Curso de Hacking Ético Avanzado*. Quito, Pichincha, Ecuador: Greenetics.
- Guardnet. (09 de Junio de 2011). *https://guardnet.wordpress.com*. Obtenido de <https://guardnet.wordpress.com>: <https://guardnet.wordpress.com/2011/06/09/capa-de-seguridad-perimetral/>
- Guevara, h. (2016). *modelo OSI y TCP*. Obtenido de <http://es.slideshare.net/wilbe>:
<http://es.slideshare.net/wilber147/3modelos-osi-y-tcpip-caractersticas-funciones-diferencias>
- Hacker.NET, E. (2017). *https://www.elhacker.net*. Obtenido de <https://www.elhacker.net>:
<https://www.elhacker.net/hackers-john-draper.html>
- Hirschberger, R. (14 de 05 de 2017). *RT*. Obtenido de SEPA MAS:
<https://actualidad.rt.com/actualidad/238431-europol-ciberataque-virus-wannacry-sin-precedentes>
- Internetworking Solutions S.A. (s.f.). *net solution*. Obtenido de http://www.netsolutions.com.mx/servicios/redes/que_es/que_es.html
- Jeffry Handal. (2013). *Redes Virtuales*. Obtenido de Network startup resource center:
https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjxtoeGkbvRAhVG4iYKH3OCGkQFggYMAA&url=https%3A%2F%2Fnsr.org%2Fworkshops%2F2013%2Fwalc%2Fcampus%2Fraw-attachment%2Fwiki%2Fagenda%2Fvlan.pdf&usq=AFQjCNELXF9qx4ZxZ_
- Krugel. (25 de Abril de 2013). *http://www.krugel.com.ar*. Obtenido de <http://www.krugel.com.ar>:
<http://www.krugel.com.ar/a/6/evolucion-del-cableado-estructurado>

- Leon, E. E. (2005). *Direccionamiento IPV4*. Obtenido de [http://isa.uniovi.es/docencia:
http://isa.uniovi.es/docencia/SIGC/pdf/direccionamiento-ip.pdf](http://isa.uniovi.es/docencia/http://isa.uniovi.es/docencia/SIGC/pdf/direccionamiento-ip.pdf)
- León, E. E. (01 de 02 de 2006). *Direccionamiento IP*. Obtenido de [http://www.monografias.com/:
http://www.monografias.com/trabajos29/direccionamiento-ip/direccionamiento-ip.shtml](http://www.monografias.com/http://www.monografias.com/trabajos29/direccionamiento-ip/direccionamiento-ip.shtml)
- León, E. E. (29 de 03 de 2006). *tecnologias de red*. Obtenido de [https://cecy09.wordpress.com:
https://cecy09.wordpress.com/tecnologias-de-red/](https://cecy09.wordpress.com/https://cecy09.wordpress.com/tecnologias-de-red/)
- Linksys. (2017). *http://www.linksys.com*. Obtenido de [http://www.linksys.com:
http://www.linksys.com/us/r/resource-center/what-is-a-wifi-access-point/](http://www.linksys.com/http://www.linksys.com/us/r/resource-center/what-is-a-wifi-access-point/)
- Maestrosdelweb. (Diciembre de 2007). *http://www.maestrosdelweb.com*. Obtenido de [http://www.maestrosdelweb.com:
http://www.maestrosdelweb.com/historia-de-cisco/](http://www.maestrosdelweb.com/http://www.maestrosdelweb.com/historia-de-cisco/)
- Michel. (21 de 11 de 2013). *Fundamentos de redes de datos y telecomunicaciones*. Obtenido de [http://www.monografias.com/:
http://www.monografias.com/trabajos98/fundamentos-redes-datos-y-telecomunicaciones/fundamentos-redes-datos-y-telecomunicaciones.shtml](http://www.monografias.com/http://www.monografias.com/trabajos98/fundamentos-redes-datos-y-telecomunicaciones/fundamentos-redes-datos-y-telecomunicaciones.shtml)
- Mikrotik. (2017). *mikrotikxperts*. Obtenido de [http://www.mikrotikxperts.com:
http://www.mikrotikxperts.com/index.php/informacion/conocimientos-basicos/14-modelo-osi-y-tcp-ip](http://www.mikrotikxperts.com/http://www.mikrotikxperts.com/index.php/informacion/conocimientos-basicos/14-modelo-osi-y-tcp-ip)
- Multicom. (2017). *http://multicomp.com.mx*. Obtenido de [http://multicomp.com.mx:
http://multicomp.com.mx/seguridad-informatica/seguridad-perimetral/](http://multicomp.com.mx/http://multicomp.com.mx/seguridad-informatica/seguridad-perimetral/)
- NBcomunicaciones. (2017). *http://nbcomunicaciones.com*. Obtenido de [http://nbcomunicaciones.com:
http://nbcomunicaciones.com/infraestructura-de-red.html](http://nbcomunicaciones.com/http://nbcomunicaciones.com/infraestructura-de-red.html)
- Netacad, C. (2017). *www.netacad.com*. Obtenido de [www.netacad.com:
https://210561797.netacad.com/courses/366977/modules](http://www.netacad.com/https://210561797.netacad.com/courses/366977/modules)
- Norton, Q. (26 de Febrero de 2012). *https://www.wired.com*. Obtenido de [https://www.wired.com:
https://www.wired.com/2012/02/wikileaks-anonymous-partners/](https://www.wired.com/https://www.wired.com/2012/02/wikileaks-anonymous-partners/)
- Olago, J. P. (2015). *Cisco_VLSM*. Obtenido de [http://giret.ufps.edu.co/:
http://giret.ufps.edu.co/cisco/descargas/Presentaciones/Modulo2_capitulo6.pdf](http://giret.ufps.edu.co/http://giret.ufps.edu.co/cisco/descargas/Presentaciones/Modulo2_capitulo6.pdf)
- Palacios, L. (13 de Octubre de 2015). *http://hackersenelmendo.blogspot.com*. Obtenido de [http://hackersenelmendo.blogspot.com:
http://hackersenelmendo.blogspot.com/2015/10/tipos-de-hackers.html](http://hackersenelmendo.blogspot.com/http://hackersenelmendo.blogspot.com/2015/10/tipos-de-hackers.html)
- Ramos, A. (Febrero de 2011). *www.criptored.upm.es*. Obtenido de [www.criptored.upm.es:
www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf](http://www.criptored.upm.es/www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf)
- Reyes, A. (30 de Julio de 2013). *http://www.clasesdeperiodismo.com*. Obtenido de [http://www.clasesdeperiodismo.com:
http://www.clasesdeperiodismo.com/2013/07/30/wikileaks-anonymous-y-el-periodismo/](http://www.clasesdeperiodismo.com/http://www.clasesdeperiodismo.com/2013/07/30/wikileaks-anonymous-y-el-periodismo/)
- Seguridadweb20. (2015). *http://www.seguridadweb20.es*. Obtenido de [http://www.seguridadweb20.es:
http://www.seguridadweb20.es/ataques-ddos/](http://www.seguridadweb20.es/http://www.seguridadweb20.es/ataques-ddos/)

Sergio Untiveros. (01 de 03 de 2016). *que es el switch*. Obtenido de AprendaRedes.com:
<http://www.aprendaredes.com/dev/articulos/que-es-el-switch.htm>

Trendnet. (2017). <https://www.trendnet.com>. Obtenido de <https://www.trendnet.com>:
<https://www.trendnet.com/langsp/products/USB-adapters/TU-S9>

Valdez, F. (18 de Marzo de 2013). <http://informaticks-technol0ogii.blogspot.com>. Obtenido de
<http://informaticks-technol0ogii.blogspot.com>: <http://informaticks-technol0ogii.blogspot.com/2013/03/elementos-que-conforman-una-red.html>

ANEXOS

ANEXO 1

PRESUPUESTO FORTIGATE 30D

IMAGEN	DESCRIPCIÓN DE LOS EQUIPOS	CANT.	V. UNITARIO	V.TOTAL (USD)
	FORTIGATE 30-D Hardware plus 1 year 8x5 Forticare and Fortiguard UTM Bundle	1	\$ 1100	\$ 1100
	PATCH-CORD CATEGORIA 6-E	2	\$ 5	\$10
			SUBTOTAL	\$1110
			+ 12%	143,2
			TOTAL	1253,20

OBSERVACIONES

Forma de pago: 80% de adelanto Y 20%
contraentrega

Validez de la oferta: 15 días

Garantía: Según Forticare adquirido

Tiempo de entrega del equipo: 45 días

ANEXO 2

PRESUPUESTO CISCO ASA FIREPOWER

IMAGEN	DESCRIPCIÓN DE LOS EQUIPOS	CANT.	V. UNITARIO	V.TOTAL (USD)
	CISCO ASA 5506W-X Wifi Chassis + 1 year Subscriber Bundle	1	\$ 2300	\$ 2300
	PATCH-CORD CATEGORIA 6-E	2	\$ 5	\$10
			SUBTOTAL	\$2310
			+ 12%	\$277,20
			TOTAL	2587,20

OBSERVACIONES

Forma de pago: 80% de adelanto y 20%
 contraentrega
Validez de la oferta: 15 días
Garantía: Según Suscripción adquirida
Tiempo de entrega del equipo: 45 días

ANEXO 3

CAMBIAR DIRECCIÓN IPV4 EN UNA COMPUTADORA

Paso 1: Presionar las teclas Windows + R (⊞ + R) y muestra el print de la figura.

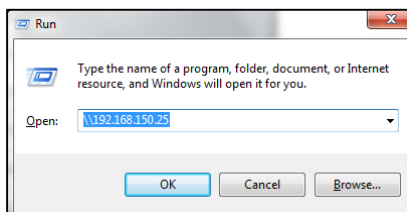


Figura 141: Combinación de teclas (Elaboración Propia, 2017)

Paso 2: Ejecutar el siguiente comando de Windows (ncpa.cpl) y OK

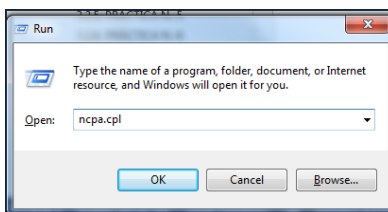


Figura 142: Comando de Windows (Elaboración Propia, 2017)

Paso 3: Seleccionar interface de red.

Posterior al comando ejecutado, muestra nuestras interfaces de red de la computadora, seleccionar la interfaz que se está trabajando generalmente tienen los nombres de (Ethernet local Connection - Local Área Connection)

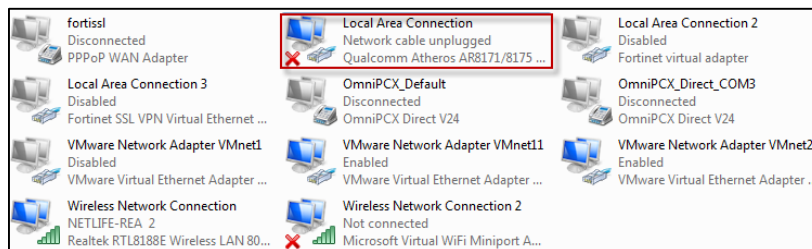


Figura 143: Seleccionar interfaz de red (Elaboración Propia, 2017)

Paso 4: Ingresar a la interfaz LAN con click derecho → Propiedades y elegir IPv4

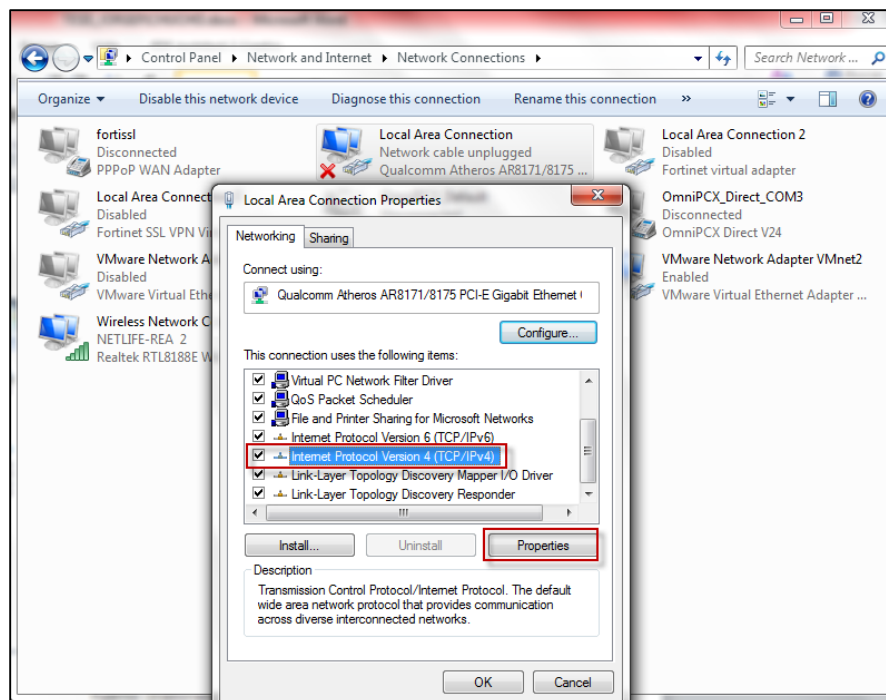


Figura 144: Protocolo IPv4 (Elaboración Propia, 2017)

Paso 5: Ingresar dirección IPv4 correspondiente a la práctica

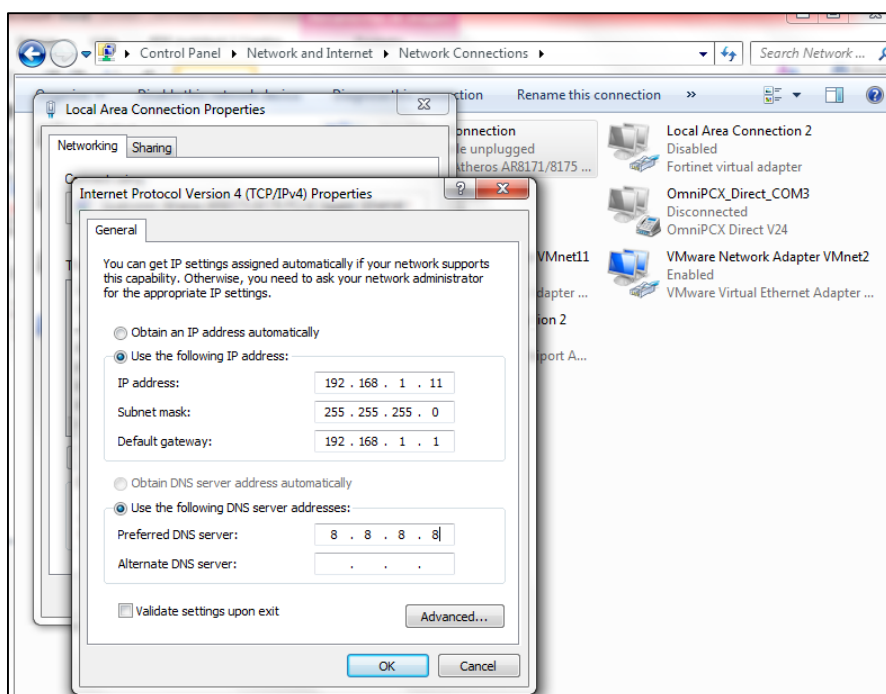


Figura 145: Ingreso de dirección IPv4 (Elaboración Propia, 2017)

ANEXO 4

INSTALACIÓN FORTIEXPLORER

Paso 1:

Descargar el software del siguiente link: https://1drv.ms/f/s!AkU_LNL4kcZ3jkJhmrLk07dcla7e

Paso 2:

Ubicar el archivo descargado cuyo nombre es FortiExplorerSetup_win_upgrade_2.6.1083.msi y realizar la instalación del mismo

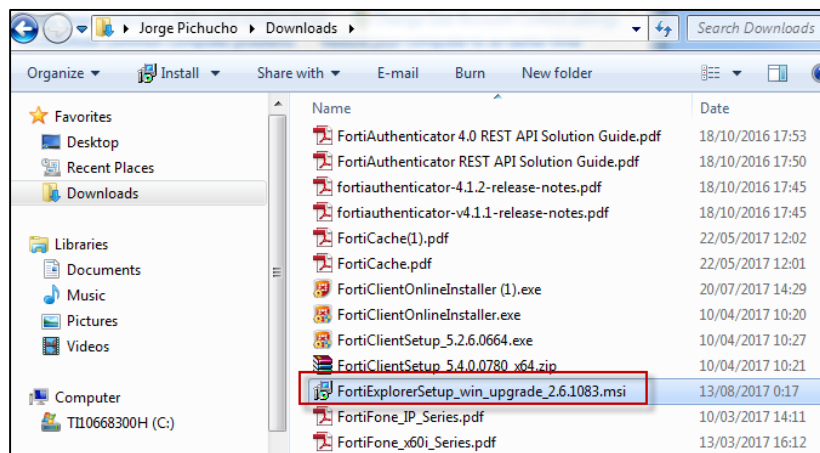


Figura 146: Archivo ejecutable de Fortiexplorer (Elaboración Propia, 2017)

Paso 3: Ejecutar como administrador y Next hasta terminar la instalación. La instalación se realiza por defecto.



Figura 147: Instalación de Fortiexplorer (Elaboración Propia, 2017)

Paso 4: Ejecutar el programa, el ejecutable es Fortiexplorer depende del sistema operativo de la PC del estudiante para ubicar el ejecutable.

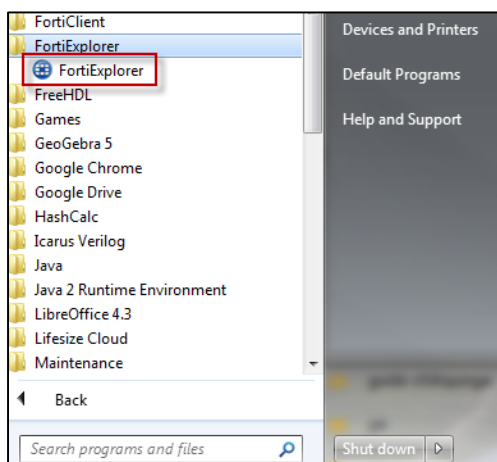


Figura 148: Ejecutar el programa Fortiexplorer (Elaboración Propia, 2017)

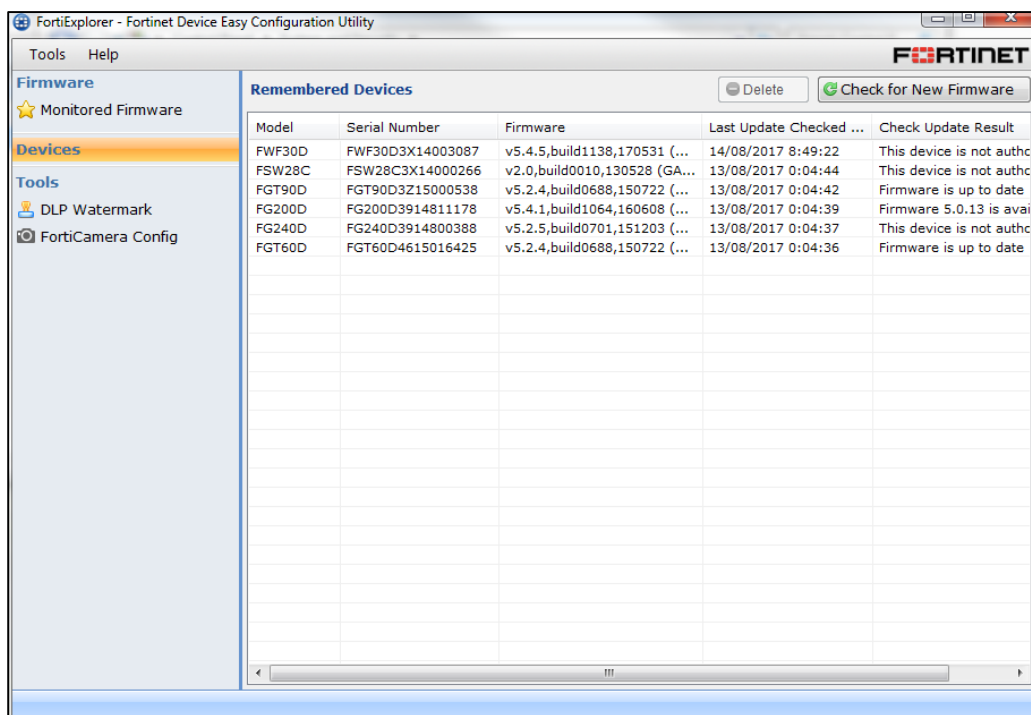


Figura 149: Ejecutar el programa Fortiexplorer (Elaboración Propia, 2017)

Paso 5: Conectar el cable USB que viene con el Fortigate , se instala el driver en la PC y ya puede ser utilizado el software para administración sin inconvenientes.

ANEXO 5

MANUAL DE CONFIGURACIÓN RÁPIDA DE FORTIWIFI

1) Conexiones básicas

Conecte el dispositivo a la toma eléctrica y a una conexión a internet. Por lo general es un modem o router, caso contrario puede ser otro dispositivo en la red.

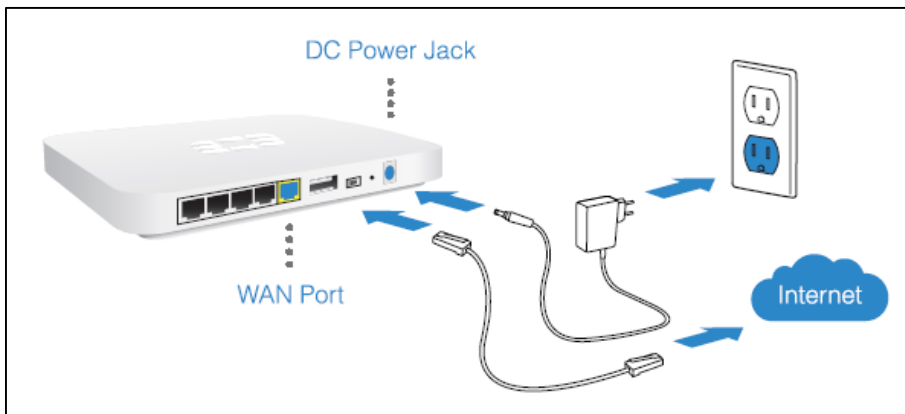


Figura 150: Conexión básica (FortinetDocs, 2013)

2) Ingreso vía browser a través de un cable Ethernet

- Conecte el cable Ethernet o de red
- Visitar 192.168.1.99 en su explorador
- Ingresar con usuario: admin y password: en blanco
- Click en Wizard ubicado en la esquina superior derecha
- Configure su equipo y guarde las configuraciones

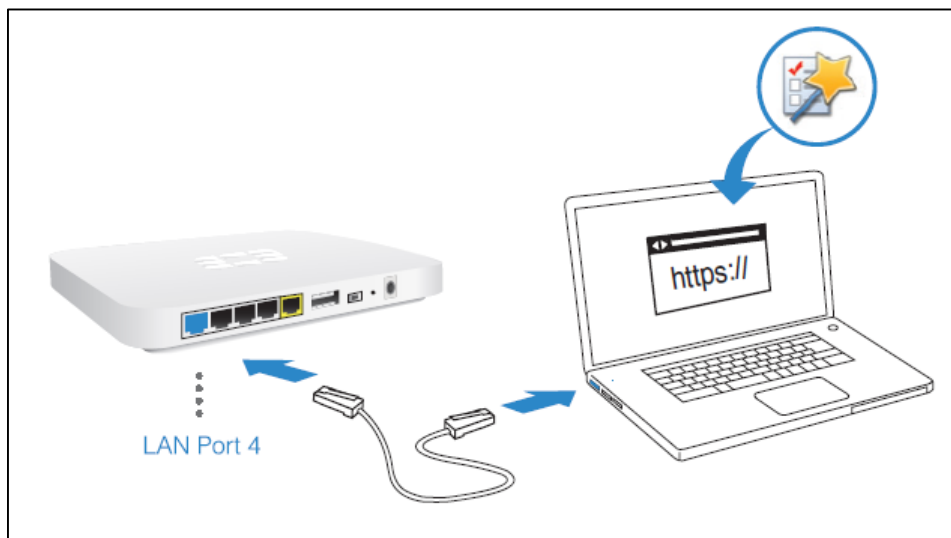


Figura 151: Ingreso al equipo vía browser (FortinetDocs, 2013)

3) Puertos y componentes del Fortiwifi 30D

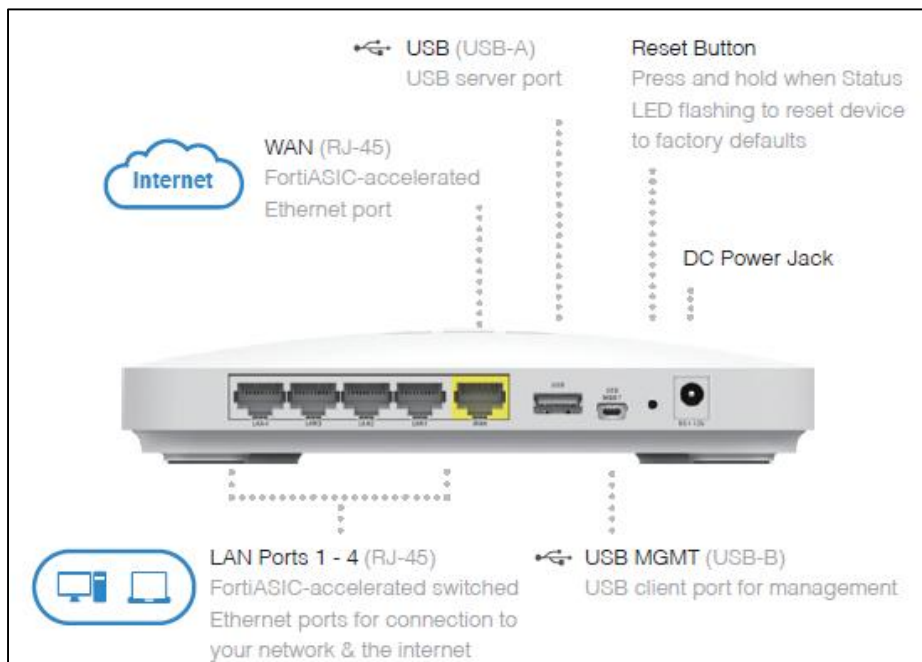









Figura 152: Puertos y componentes del Fortiwifi 30D (FortinetDocs, 2013)

ANEXO 6

CRONOGRAMA DE ACTIVIDADES

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1	 	Establecer los parámetros adecuados para el desarrollo del módulo para prácticas de laboratorio del sistema UTM	14 días	vie 19/05/17	mié 07/06/17
3		Realizar el dimensionamiento y adquisición del equipo adecuado	7 días	jue 08/06/17	vie 16/06/17
6		Elaborar el diseño de la guía de prácticas de laboratorio del sistema	20 días	sáb 17/06/17	jue 13/07/17
10		Implementar el equipo en el laboratorio de redes	5 días	vie 14/07/17	jue 20/07/17
13		Crear las guías de prácticas de laboratorio	15 días	vie 21/07/17	jue 10/08/17
16		Realizar pruebas de funcionamiento y validación de datos	8 días	vie 11/08/17	mar 22/08/17

