

UNIVERSIDAD NACIONAL DE INGENIERÍA RECINTO UNIVERSITARIO SIMÓN BOLIVAR FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN DEPARTAMENTO DE SISTEMAS DIGITALES Y TELECOMUNICACIONES.

MONOGRAFIA PARA OPTAR AL TÍTULO DE: INGENIERO ELECTRÓNICO

Título:

"Organizar Y Establecer Nuevas Soluciones de Seguridad en la Red de la Empresa Sistems Enterprise S.A."

Autores:

- Br. Herzan Francisco Carcache Huerta, Carnet: 2011-37268
- Br. Cristian Ulises Burgos Torres, Carnet: 2012-41142

Tutor: Ing. Luis Francisco López Bravo.

Managua, Nicaragua Octubre 2018

Dedicatoria:

Este esfuerzo especialmente lo queremos dedicar a todas aquellas personas que con su feroz espíritu de investigador dedicaron sus vidas para contribuir en el desarrollo pleno de la ciencia, teniendo en mente siempre como fin, el bienestar de la humanidad.

Les agradecemos profundamente por inspirarnos en el mundo del Networking todo lo que hemos aprendido y estamos por aprender, para cooperar al progreso del conocimiento científico en nuestra nación.

Muchas personas han contribuido indirecta o directamente en este estudio, razón que nos impulsa a dedicarlo también a todos los profesores de la Facultad de electrotecnia y computación nuestra universidad.

A todas las personas de nuestro país que realizan sus investigaciones para solucionar un problema que han hecho propio y que constantemente a través de cualquier medio científico intentan encontrarle una solución eficaz. Así mismo, a todas las personas que sufren las consecuencias de los pocos trabajos existentes en nuestra rama de seguridad de la información.

Por su incondicional y constante apoyo, a todos nuestros profesores, familiares y amigos, les ofrecemos este trabajo como muestra de cariño. Siempre nos inspiraron a continuar y seguir adelante hasta lograrlo ya que nunca perdimos de vista la siguiente máxima: "Si en algún momento dudas y crees que no lo logras, imagina la mirada de esperanza de aquellos que confían en ti".

En fin, este trabajo es para todos ustedes. Nos honra poder haber hecho algo que sabemos puede generar grandes beneficios. Estamos muy felices de formar parte de ese reducido pero incansable y tenaz grupo de investigadores.

Con mucho aprecio:

Cristhian Burgos y Herzan Carcache.

Agradecimientos:

En primer lugar a gracias a Dios por haberme guiado por el camino de la felicidad hasta ahora; en segundo lugar a cada uno de mi familia. Por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora. Agradeciéndole a mi compañero de tesis **Cristhian Burgos** por haberme ayudado en todo momento, a mis compañeros de Universidad porque en esta armonía grupal lo hemos logrado y a mi tutor monográfico quién nos ayudó en este proceso de formación, **Ing. Francisco López.**

Br. Herzan Francisco Carcache Huerta.

Primeramente, agradecerle principalmente a Dios por acompañarme a lo largo de mi carrera y guiarme a lo largo de mi aprendizaje, ayudarme en momentos de debilidad y darme la inteligencia necesaria para seguir adelante. Le doy gracias a mis padres **Héctor Burgos y Lucia Torres** por estar a mi lado y apoyarme en todo momento, por inculcarme los valores que tengo y por permitirme tener una excelente educación a lo largo de mi vida, y ser siempre el mejor ejemplo a seguir y salir adelante que tengo.

A mis hermanos **Héctor y Ana Lucia** por estar siempre a mi lado y brindarme su apoyo siempre que lo he necesitado, y ser un gran ejemplo de unidad familiar, a mis tíos **Luis y Maribel**, mis primos **Luis y Milton** por también ser una gran parte en mi vida, además de su gran apoyo en mi formación tanto como personal como profesional estando siempre presentes en todo momento y cuando más se necesitan.

A mi esposa **Meury Zamora**, la cual ha sido y será parte importante de mi vida, creyendo en mí y estando a mi lado en todo momento, demostrándome siempre su amor incondicional y paciencia. A **Herzan Carcache** por haber sido un excelente compañero de tesis y amigo, al igual que a nuestro tutor el **Ing. Francisco López** el cual siempre nos ayudó y motivo a lo largo de este camino lleno de obstáculos.

De igual manera, siempre teniendo en cuenta a una persona muy especial, que aunque ahora no está con nosotros, siempre estarás en mi mente cuando alcance grandes logros como este, Pedrito Valle.

Y por supuesto a la empresa **Sistems Enterprise S.A**, la cual nos permitió realizar esta monografía basándonos en sus instalaciones, compañeros actuales de trabajo los cuales siempre nos brindaron apoyo en momentos de duda y aprendizaje para realizar un buen trabajo monográfico.

Br. Cristhian Ulises Burgos Torres.

[&]quot;Organizar Y Establecer Nuevas Soluciones de Seguridad en la Red de la Empresa Sistems Enterprise S.A."

Abstract:

In the last years, information technologies have changed the world around us, as is the case with the Internet of Things, to such an extent that information security is important to protect the confidential or private information of any business system.

In the increasing boom of the different forms of penetration or security failures that present some technologies, attackers or intruders have several abilities to collapse the computer network and the theft of information in order to obtain money in return.

Our monograph tries to implement different security equipment to protect the computer network of the company Sistems Enterprise S, A. (SENCOM). With the following devices: a unified threat management that has different modules (Router, Firewall, VPN and Web Filter), an Intrusion Prevention System that acts on the basis of signatures and will be analyzing the traffic of the network towards the provider of Internet service, a Fortimail that is a mail server and at the same time is AntiSpam and finally a DNS Server.

Any type of computer threats put in risk and stability of the computer network but when implementing these security devices already mentioned, the probability that an intruder manages to steal information is significantly reduced by using the best security practices both in the entrance and in the exit.

SENCOM I need good management and administration of your resources this depends on the success of the business. Therefore, we take full advantage of all those elements that allow us to better manage the computational resources of the company and thus contribute to the achievement of the objectives we set ourselves.

This solution was viable because it allowed us to solve this problem in the company Sistems Enterprise S.A. to save money and share information between different areas, is an important factor in decision making.

Resumen:

En los últimos años las tecnologías de la información han cambiado el mundo que nos rodea como es el caso del internet de las cosas a tal punto que la seguridad informática es importante para resguardar la información confidencial o privada de cualquier sistema empresarial.

En la creciente forma de penetración o fallos de seguridad que presentan algunas tecnologías los atacantes o intrusos tienen varias habilidades para colapsar la red de computadoras con el fin del robo de la información con el fin de obtener dinero a cambio.

Nuestra monografía trata de implementar diferentes equipos de seguridad para proteger la red de computadoras de la empresa Sistems Enterprise S, A. (SENCOM). Con los siguientes dispositivos: un gestión unificada de amenaza que tiene diferentes módulos (Enrutador, Firewall, VPN y Web Filter), un Sistema de Prevención de Intrusos que actúa en base a firmas y estará analizando el tráfico de la red de cara al proveedor de servicio de internet, un Fortimail que es servidor de correo y al mismo tiempo es AntiSpam y por ultimo un Servidor DNS.

Cualquier tipo de amenazas informáticas ponen en riesgos y estabilidad de la red de computadora pero al implementar estos dispositivos de seguridad ya mencionado, la probabilidad de que un intruso logre robar información se reduce notablemente al usar las mejores prácticas de seguridad tanto en la entrada como en la salida.

SENCOM necesito de la buena gestión y administración de sus recursos de esto depende el éxito del negocio. Por lo cual aprovechamos al máximo todos aquellos elementos que nos permiten gestionar de una mejor manera los recursos computacionales de la empresa y de esta forma contribuir al logro de los objetivos que nos planteamos.

Esta solución nos resultó viable porque nos permitió resolver este problema en la empresa Sistems Enterprise S.A. para ahorrar dinero y Compartir información entre las distintas áreas, es un factor importante en la toma de decisión.

Tabla de llustraciones:

Fig. 1.2.1 Red de Computadora antes.	7
Fig. 1.2.2 Esquema de la Red después de utilizar el nuevo UTM.	7
Fig. 1.2.3 Configuración de los enlaces WAN y LAN	8
Fig. 1.2.4 Ingresando los DNS Público y DNS de Google.	8
Fig. 1.2.5 Configuración del Servidor de correo.	9
Fig. 1.3.1 Permisos del Servidor de Correo.	9
Fig. 1.3.2 Acceso a los protocolos HTTP, HTTPS y POP3	9
Fig. 1.3.3 Enrutamiento entre las distintas VLAN.	10
Fig. 1.3.4 Establecimiento del NAT Dinámico.	10
Fig. 1.3.5 Establecimiento del Network Time Protocol.	11
Fig. 1.3.6 NAT Estático en el servidor de tickets y el FTP.	11
Fig. 1.3.7 Restricción de categoría de sitios web usando Web Blocker	12
Fig. 2.2.1 Antes de la Implementación.	14
Fig. 2.2.2 Esquema de la implementación del sensor IPS NSP M-1450	14
Fig. 2.2.3 Preparación del sensor M-1450	15
Fig. 2.2.4 Conexión del sensor desde el puerto de consola.	15
Fig. 2.2.5 Configuración del sensor con el comando setup.	16
Fig. 2.2.6 Terminando de configurar con el comando setup.	16
Fig. 2.2.7 Establecer la llave compartida en la manager	.17
Fig. 2.2.8 Verificación de la llave compartida.	17
Fig. 2.2.9 Estableciendo la llave compartida en el sensor	18
Fig. 2.2.10 Verificando la relación entre el sensor y la manager.	18
Fig. 2.3.1 Elegir la versión a actualizar v descargar	19
Fig. 2.3.2 Actualizando la versión del IPS del NSP M-1450.	19
Fig. 2.3.3 Última versión disponible para el IPS NSP M-1450.	20
Fig. 2.3.4 Versión anterior del IPS	$\frac{20}{20}$
Fig. 2.3.5 Implementación del IPS con sus enlaces WAN LAN v AP	$\frac{20}{21}$
Fig. 2.4.1 Configuración de las políticas del IPS	$\frac{21}{21}$
Fig. 2.4.2 Asignación de las políticas a los puertos correspondientes	22
Fig. 2.4.3 Guardando las políticas del IPS	$\frac{22}{22}$
Fig. 2.4.4 Políticas de Firewall del IPS	23
Fig. 2.4.5 Antes de implementar el IPS	23
Fig. 2.4.6 Después de implementar el IPS	$\frac{23}{24}$
Fig. 3.1.1 Tipos de jerarguía para un servidor DNS	25
Fig. 3.1.2 Funcionamiento del Forwarders	25
Fig. 3.2.1 Selección del idioma de instalación en Linux	26
Fig. 3.2.2 Elección del tipo de teclado en el servidor	26
Fig. 3.2.3 Establecer las Credenciales de acceso	27
Fig. 3.2.4 Instalación del Sistema Operativo	27
Fig. 3.2.5 Ingreso de las Credenciales	28
Fig. 3.2.6 Elección de los módulos a instalar.	28
Fig. 3.2.7 Descarga e Instalación de los paquetes requeridos	29
Fig. 3.2.8 Configuración de la interfaz Externa.	29
Fig. 3.2.9 Aiuste del Nombre de Dominio	30
Fig. 3.2.10 Estableciendo las configuraciones realizadas	30
Fig. 3.2.11 Configurando la Dirección IP del Server.	31
Fig. 3.2.12 Guardando los Cambios Realizados.	31
Fig. 3.2.13 Verificación de los módulos activados en el server	32
Fig. 3.2.14 Habilitación de la cache del DNS transparente.	32
Fig. 3.2.15 Añadir los Forwarders de los DNS de Google.	33
Fig. 3.2.16 Configuración de nuestro dominio.	33
Fig. 3.3.1 Comprobando nuestra dirección IP en la PC	34
Fig. 3.3.2 Verificación del servidor DNS.	34
"One de la constante de la constan	
"Organizar Y Establecer Nuevas Soluciones de Seguridad en la	

Red de la Empresa Sistems Enterprise S.A."

Red de la Empresa Sistems Enterprise S A "	VII
Try. τ.υ.τ Continuation der Ferni de Contenno.	00
Fig. 4.8.7 Continuación del Perfil de contenido	00
rig. 4.8.6 Partil de Contanido de Entrado	03
Fig. 4.8.5 Política tanto entrante como soliente	05
Fig. 1.8.1 Partil de Salida dal Antispam	04
Fig. 4.8.3 Perfil del Antispam en la entrada	05 6/
Fig. 4.8.2 Configuración del perfil de Antispam	02
Fig. 4.8.1. Danel del Antispam	02
rig. 4.7.2 Creación de la política de sesión	01 60
rig. 4.7.1 Estableciendo el perill de sesión.	61
rig. 4.7.1 Establaciona al parfil da sosión	00
Fig. 4.6.1 Configuración de los porfilos	39 60
Fig. 4.5.15 Regresando con las nuevas credenciales y políticas establecida	38
Fig. 4.5.12 Finalizando la configuración del Wizard.	58
rig. 4.5.11 Estableciendo en la política de acceso y la acción a tomar de Relay.	57
FIG. 4.5.10 ESTADIECIENDO EL DOMINIO AL ANTISPAM.	56
Fig. 4.5.9 Ureacion de política principal de Acceso.	56
FIG. 4.5.8 Elección del nivel de Escaneo del Antispam.	33
Fig. 4.5.7 Configuración inicial del Antispam.	55
Fig. 4.5.6 Anadiendo nuestro dominio y el Gateway de la IP Privada	54
Fig. 4.5.5 Anadiendo los puertos de nuestro servidor de correo	54
Fig. 4.5.4 Contirmando las contiguraciones necesarias para el upgrade.	53
Fig. 4.5.3 Estableciendo la nueva contraseña de acceso.	53
Fig. 4.5.2 Contirmando el acceso al Wizard del Fortimail.	52
Fig. 4.5.1 Seleccionando el Wizard de la consola del Fortimail.	52
Fig. 4.4.5 Confirmacion de la actualización por medio del archivo de licencia.	51
FIG. 4.4.4 Subida del archivo de licencia a la consola.	51
rig. 4.4.3 busqueda del archivo en nuestro ordenador.	51
rig. 4.4.2 Eleccion del Archivo de Licencia para la consola.	50
FIG. 4.4.2 Elegatón del Archive de Licensia para la caracte	50
rig. 4.3.9 Acceso a la interiaz Granca del Fortimali.	49
rig. 4.3.0 ingresando las credenciales de administrador en la consola del Fortimali	48
Fig. 4.3.2 Upprocendo las excepción de segundad.	48
rig. 4.3.0 Entrando a la Internaz Granica desde el Navegador	4/
rig. 4.3.5 Estableciendo el direccionamiento de la privada de nuestra Empresa.	4/ 47
rig. 4.3.5 Estableciendo el direccionamiento de ID privada de nuestra Empresa	40
Fig. 4.3.4 Ingresando las Credenciales por defecto	40 //6
rig. τ.ο.2 πιταιτίζας με τα παγμίπα vitual del Fortintali Fig. 4.3.3 Autenticación del Fortimail	43 16
Fig. 4.3.2 Arrangue de la máquina virtual del Fortimail	4J 15
Fig. 4.3.1 Finalización del despliegue de la maquina virtual	44 15
Fig. 4.2.16 Porcentaie del despliegue de la máguina virtual del Fortimail	 44
Fig. 4 2 15 Tipo de Almacenamiento para el Fortimail	-
Fig. 4.2.13 Establecienco el annacenamiento de la mayuna virtual Fig. 4.2.14 Creación del disco virtual VMDK, reservando el espacio definido	43 43
Fig. 4.2.12 Computation del nombre de la maquina virtual	42 //2
Fig. 4.2.12 Configuración del nombre de la máquina virtual	42 12
Fig. 4.2.10 Especificación de la licencia	+1 //2
Fig. 4.2.0 Elección del archivo necesario del Fortimali.	+ 1 <u>/</u> 1
Fig. 4.2.9 Elección del archivo necesario del Fortimail	4 0 <u>4</u> 1
Fig. 4.2.8 Selección del Firmware para el desplieque del Fortimail	40
Fig. 4.2.7 Desplieque del OV/E del Entrimail para su debida instalación	<i>39</i> 40
Fig. 4.2.6 Selección del archivo a desplegar en puestro Hypervisor	39 20
Fig. 4.2.5 Descargando la versión 5.4 del Eartimail	3ð 20
Fig. 4.2.5 Election de la diffina version disponible del Fontimali.	38 20
rig. 4.2.2 Selección del producto el cual implementaremos	3/
rig. 4.2.2 Selección del producto el cuel implementarement	51
Fig. 4.1.1 Arquitectura de implementación del Fortimal.	36
	~ ~

Fig.	4.8.8 Finalización del Perfil de Contenido.	. 67
Fig.	4.8.9 Configuración del Antispam.	. 67
Fig.	4.8.10 Configuración de lista negra o blanca.	. 68
Fig.	4.8.11 Lista Blanca.	. 69
Fig.	4.8.12 Lista Negra	. 70
Fig.	4.9.1 Sitios Web con envíos de correo no deseado.	. 71
Fig.	5.1.1 Esquema de la Zona DMZ	. 72
Fig.	5.1.2 Esquema Antes de la implementación de la Zona DMZ	. 73
Fig.	5.1.3 Diagrama de red de SENCOM.	. 74
Fig.	5.1.4 Primeros Pasos para la creación de la interfaz en el ESXI.	. 76
Fig.	5.1.5 Procedimiento para la creación de la interfaz.	. 76
Fig.	5.1.6 Establecimiento de la interfaz de la zona DMZ.	. 77
Fig.	5.1.7 Creando la Interfaz de la zona DMZ.	. 77
Fig.	5.1.8 Configurando la zona DMZ	. 78
Fig.	5.1.9 Agregando la interfaz configurada al ESXI.	. 78
Fig.	5.1.10 Establecimiento de la interfaz del ESXI.	. 79
Fig.	5.2.1 Plataforma del UTM FortiGate 200 D para establecer la zona DMZ.	. 79
Fig.	5.3.1 Establecimiento de los puertos del UTM con sus direccionamiento IP Privado	. 80
Fig.	5.3.2 Configuración de la interfaz LAN de SENCOM.	. 80
Fig.	5.3.3 Configuración del Puerto del UTM para la Zona DMZ.	. 81
Fig.	5.3.4 Configuración del enlace WAN con su IP Publica.	. 81
Fig.	5.4.1 Integrando los Servidores Forwading del DNS de Google	. 82
Fig.	5.4.2 Establecimiento de los servidores de DNS de Google	. 82
Fig.	5.5.1 Ingresando el Enrutamiento Estático del enlace WAN.	. 83
Fig.	5.5.2 Configurando del Enrutamiento Estático por el enlace WAN	. 83
Fig.	5.5.3 Configuración del enlace WAN con su Enrutamiento Estático.	. 84
Fig.	5.6.1 Establecimientos de las distintas políticas de la red de la Empresa SENCOM.	. 84
Fig.	5.7.1 Establecimos la política de la Zona DMZ.	. 85
Fig.	5.7.2 Configurando las políticas del NAT	. 86
Fig.	5.7.3 Estableciendo el SNAT para la utilización de la Zona DMZ.	. 86
Fig.	5.7.4 Agregando el NAT a las políticas de la red	. 87
Fig.	5.8.1 Configuración del Fortimail de SENCOM.	. 88
Fig.	5.8.2 Modo de Operación del Fortimail.	. 89
⊢ıg.	5.8.3 Establecimiento del interfaz del Fortimali.	. 89
Fig.	5.8.4 Configurando la interfaz y permitiendo los distintos protocolos de red.	. 90
⊢ıg.	5.8.5 Estableciendo la interfaz del Fortimail.	. 90
⊢ıg.	5.8.6 Ingresando los Servidores DNS de Google.	. 91
⊢ıg.	5.9.1 Enrutamiento Estatico del Fortimail.	. 91
Fig.	5.9.2 Mostrando el enrutamiento del Fortimail.	. 92
⊢ıg.	5.9.3 Estableciendo las políticas del Fortimali	. 92
⊢ıg.	5.9.4 Establecimiento de la política de entrada del Fortimali.	. 93
⊢ıg.	5.9.5 Establecimiento de la política de salida del Fortimali.	. 93
⊢ıg.	1A.1 Diagrama de la red SENCOM	1

Lista de Acrónimos:

AP: Punto de Acceso Bandwidth: Ancho de Banda Brute Force Attack: Ataque a Fuerza Bruta **CSMA/CD:** Carrier Sense Multiple Access / Collition Detection **Domain:** Dominio **DHCP:** Dynamic Host Configuration Protocol **DoS:** Denial of Service **DDoS:** Distributed Denial of Service Attack **DNS:** Domain Name System **DMZ**: Demilitarized Zone Ethernet: Diseño de red de área local normalizado como IEEE 802.3 **Firewall:** Cortina de Fuego GUI Graphic User Interface: Interface Gráfico de Usuario Hacker: Experto en informática capaz de entrar en sistemas cuyo acceso es restringido **HTML:** HyperText Markup Language **HTTP:** Hypertext Transfer Protocol HTTPS: Hypertext Transport Protocol Secure Header: Cabecera **INTERNET:** Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red. **INTRANET:** Se llaman así a las redes tipo Internet pero que son de uso interno Institute of Electrical IEE: and **Electronics Engineers** ITU: International **Telecommunication Union ISO:** International Organization for Standardization

ISP: Internet Service Provider **IPS:** Intrusion Prevention System **IMAP:** Internet Message Access Protocol LAN: Local Area Network Shareware Linux: Versión y/o Freeware del conocido sistema operativo Unix Packet: Paquete Cantidad mínima de datos que se transmite en una red PING Packet Internet Groper: Rastreador de Paquetes Internet. Programa utilizado para comprobar si un Host está disponible **QoS:** Quality of Service **RAM:** Random Access Memory **ROM:** Read Only Memory **SMTP**: Simple Mail Transfer Protocol Sniffer: Pequeño programa que busca una cadena númerica o de caracteres en los paquetes que

atraviesan un nodo con objeto de conseguir alguna información. **Spam / Spammer:** Manda grandes cantidades de correo o mensajes

muy largos.

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol **TFTP**: Trivial File Transfer Protocol

Time-out: Parámetro que indica a un programa el tiempo máximo de espera antes de abortar una tarea o función

TTL: Time To Live

UDP: User Datagram Protocol

UTM: Unified Threat Management

VoIP: Voice over IP

WAN: Wide Area Network

TABLA DE CONTENIDO

DEDICATORIA:	II
AGRADECIMIENTOS:	
ABSTRACT:	IV
RESUMEN:	V
TABLA DE ILUSTRACIONES:	VI
LISTA DE ACRÓNIMOS:	IX
TABLA DE CONTENIDO	X
INTRODUCCION:	1
OBJETIVOS:	2
OBJETIVO GENERAL:	2
OBJETIVOS ESPECÍFICOS:	2
ANTECEDENTES:	3
JUSTIFICACIÓN:	4
ESTRUCTURA DE CONTENIDO	5
CAPÍTULO 1	6
1 UTM	6
1. Teoría	0 6
1.2 Implementación [.]	7
1 3 Permisos en el servidor de Correo	9
CAPÍTULO 2	
2 IPS.	13
2.1 Rase Teórica	13
2.2. Implementación:	
2.2. Implementación del IDS:	
2.5. Actualization del IDS:	
3. SERVIDOR DNS:	
3.1. Teoría:	25
3.2. Implementación:	
3.3. Prueba del Servidor DNS:	
CAPÍTULO 4	
4. Fortimail:	
4.1. Implementación:	
4.2. Instalación del Fortimail	
4.3. Administracion de Fortimail	45
4.4. Aplicando licencia	
4.5. Configuración Inicial	52
4.6. Creando Perfiles del Fortimail	59
4.7. Perfil Session	60
4.8. Perfil Antispam	62
"Organizar Y Establecer Nuevas Soluciones de	

4.	9. SU	JRBI
CAPÍTU	JLO 5	
5.	DMZ	
5.	1. Te	20ría
5.	2. Fo	rtigate:
5.	3. Int	terfaces:
5.	4. Se	rvidores DNS:
5.	5. Ru	ıtas estáticas:
5.	6. Po	olíticas:
5.	7. Sa	ılida DMZ:
5.	8. Fo	rtimail:
5.	9. Ro	outing:
CONCL	USIONE	594
BIBLIO	GRAFÍA	:95
ANEXO	DS:	
ANEXO) 1. DIA	GRAMA FINAL DE SENCOMI
ANEXO) 2. TABI	LA DE COTIZACIONESII

INTRODUCCION:

La Empresa Sistems Enterprise S.A (SENCOM), ubicada en el KM 6.5 carretera norte especializada en áreas de telecomunicaciones y sistemas especiales o de bajo voltaje (centrales telefónicas, cableado estructurado, networking, seguridad electrónica, seguridad de la información, planta externa, centro de datos y energía), cuenta con una red interna protegida por un UTM (Unified Threat Management o Gestión de amenaza unificada) de cara a internet, el cual tiene módulos de IPS, Enrutador, FireWall, VPN y web filter, siendo este por el momento el único equipo en el perímetro, protegiendo los distintos servicios, aplicaciones y equipos localizados en la red interna de la empresa.

El siguiente protocolo tiene como objeto el organizar y establecer nuevas soluciones de seguridad en la red de la Empresa Sistems Enterprise S.A. con la finalidad de mejorar la seguridad informática. La Empresa cuenta con un dispositivo de seguridad en la red, pero implementaremos nuevos servicios por lo que es necesario estas nuevas soluciones de seguridad, requiriendo una seguridad informática más robusta capaz de defender la red de computadoras de cualquier amenaza informática. Se emplearán las mejores prácticas de seguridad informática en la red para estar en la vanguardia en las tecnologías de la información.

La protección de los distintos servicios y aplicaciones presentes en la empresa nos ayudara a la escalabilidad como protección de futuros servicios a implementar como son: antispam, DNS, de igual manera la implementación de una zona desmilitarizada (DMZ) aislada de nuestra red interna, finalmente organizar la estructura de la red de datos de acuerdo con las necesidades de la Empresa Sistems Enterprise S.A.

La Empresa Sistems Enterprise S.A. proporciona Soporte Técnico a diferentes empresas en el ámbito de seguridad informáticas, resguardando todo tipo de información confidencial, reduciendo riesgo de amenazas y complejidad en la red, dentro de las nuevas implementaciones interna es aumentar la eficiencia en la seguridad de nuestra red emplearemos un IPS del cual estará de cara a internet siendo el primer analizador de tráfico en nuestro perímetro comparando firmas.

El Antispam estará protegiendo nuestro servidor de correo, analizando e implementando políticas para el tráfico dirigido a este y por ultimo nuestra zona DMZ estará conectada a nuestro UTM y a la vez aislada de nuestra red interna.

Objetivos:

Objetivo General:

• Establecer las buenas prácticas de seguridad informática de la red de computadora de la Empresa Sistems Enterprise S.A.

Objetivos Específicos:

- Implementar el sistema de prevención de intrusos y gestión unificada de amenazas con sus debidas configuraciones para el bloqueo de las vulnerabilidades en el perímetro de la red.
- Instalar y configurar un servidor DNS.
- Implementar un analizador de correos Antispam "Fortimail" para la eliminación de correo no deseado para la Empresa Sistems Enterprise S.A.
- Emplear un sistema de red DMZ (Zona Desmilitarizada) en la empresa Sistems Enterprise S.A. (SENCOM).
- Establecer las buenas prácticas en la configuración de los dispositivos de seguridad (IPS, Antispam) con sus debidas políticas tanto de entrada como de salida.

Antecedentes:

En el transcurso de los años la Empresa Sistems Entreprise S.A. Ha constado con un UTM, resguardando la seguridad de la red funcionando de la mejor manera sin haber algún incidente, pero cabe destacar que se quiere añadir nuevos servicios como es el servidor DNS que anteriormente estaba tercerizado. Por lo tanto, estos servicios requieren protección de un sistema de prevención de intrusos que estará de cara al ISP (Proveedor de Servicios de Internet) y un Fortimail que actúa como antispam y servidor de correo previniendo el contenido de spam tanto de entrada como de salida de la red, de la misma manera protegiendo nuestro DNS el cual también será implementado y es una necesidad en proteger los activos de la Empresa.

Por eso la importancia en tener los dispositivos de seguridad en la red bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la Empresa Sistems Enterprise S.A. Vale la pena implementar dispositivos de seguridad si los recursos y la información merecen protegerse. En la red de nuestra empresa tenemos información delicada y documentos importantes en el área administrativa; esto debe protegerse del acceso indebido.

La tecnología va presentando mejoras significativas en dispositivos y soluciones. La empresa Sistems Enterprise S.A. cuenta con equipos cuyo acoplamiento a las nuevas tecnologías y estándares requieren mejorarse, por lo que encontramos como única solución, organizar y establecer soluciones de seguridad usando los equipos existentes junto con nuevos, lo que permitirá en tener un sistema de red con criterios técnicos de escalamiento, seguridad, disponibilidad e integridad de acuerdo a estándares establecidos.

Consideramos que en la Facultad de Electrotecnia y Computación de la Universidad Nacional de Ingeniería del Recinto Universitario Simón Bolívar no habido ningún tema monográfico relacionado al nuestro. Nosotros nos basamos en el libro: *Ataques en redes de datos IPV4 e IPV6*. De los autores: García Rambla, Juan Luis. Publicado en el año (2017). En España su tercera edición revisada y ampliada. En este documento se nos presenta los diferentes métodos de vulnerabilidad en el mundo del networking para establecer soluciones de seguridad.

[&]quot;Organizar Y Establecer Nuevas Soluciones de Seguridad en la Red de la Empresa Sistems Enterprise S.A."

Justificación:

Actualmente la Empresa Systems Enterprise, cuenta con una red alámbrica e inalámbrica que proporciona soporte técnico a diferentes empresas en el ámbito de seguridad informática. El personal de esas empresas usan el internet con fines de trabajo pero algunos hacen mal uso, ingresando a sitios web para descargar recursos de origen desconocidos que pueden ocasionar que un virus informático dañe los equipos o la red, esto provocaría que los encargados en brindar el soporte técnico tengan que estar continuamente dándole mantenimiento a los dispositivos. Además el ancho de banda se ve afectado. Sin embargo, la empresa Systems Enterprise requiere mejorar la infraestructura de la red (interna) para la calidad de sus servicios.

La Empresa SISTEMS ENTERPRISE S.A, ve necesario organizar y establecer nuevas soluciones de seguridad en la red en el perímetro interno como (IPS) y la nueva implementación de equipos de seguridad antispam (FORTIMAIL), de igual manera la nueva utilización de un servidor DNS.

De esta manera nosotros podemos dar solución a esta necesidad por separado:

- **Seguridad:** Al incorporar estos: IPS, Antispam, se tendrá una seguridad sólida en el perímetro de nuestra red, analizando todo tipo de tráfico entrante y saliente hacia el internet.
- Establecimiento: Los servicios actuales y los nuevos que implementaremos se ordenarán en una zona DMZ para aislar e intensificar la seguridad en el perímetro debido al contenido y reducir costos.

Esta solución, es viable porque nos permitirá resolver la problemática en nuestra empresa acerca de las vulnerabilidades de seguridad en la red informática. Lo que lleva al ahorro de dinero, a la facilidad de comunicación y poder compartir información de forma segura. Durante nuestra formación académica, asignaturas como Redes de Computadoras y Redes Telefónicas nos brindaron conocimientos sobre el amplio mundo de las tecnologías de la información y el Networking. También otras clases como metodología de la investigación, inglés, redacción técnica, Programación y Electrónica Digital. Todos estos conocimientos adquiridos en estas asignaturas nos serán útiles para el desarrollo de esta monografía.

Estructura de Contenido

Esta Monografía está estructurado de la siguiente manera. En el Capítulo 1, Implementaremos la gestión unificada de amenaza. En el Capítulo 2 abordaremos la implementación del Sistema de prevención de intruso con sus respectivas políticas, base teórica y la colocación de este dispositivo de seguridad en el Rack. En el Capítulo 3 implementaremos en una máquina virtual la instalación de un servidor DNS en Linux con sus debidas configuraciones para la traducción de los distintos nombres de dominios. En el Capítulo 4 Instalaremos un Fortimail luego de haber descargado desde la página oficial de Fortinet el sistema operativo lo desplegamos en nuestro ESXI, procedemos a instalar y configurar el Fortimail. En el Capítulo 5 Creación de una zona DMZ utilizando un UTM de la marca Fortinet con su modelo FortiGate 200D y esta zona implementaremos el Fortimail.

Capítulo 1

1. UTM

1.1. Teoría:

Gestión Unificada de Amenazas. Nuestro UTM tiene los siguientes módulos o funcionalidades como son:

- Función de un firewall.
- Función de VPN (para hacer túneles o redes privadas).
- Filtrado de contenidos (para el bloqueo de sitios no permitidos mediante categorías).
- Sistema de Prevención de Intrusos (IPS).
- Enrutador.

Web Filter o Filtrado de contenido: Es un software que examina páginas web para determinar partes o totalidad de información para mostrar al usuario. Este filtro comprueba el origen o el contenido de HTML (lenguaje de marcas de hipertexto) contra una lista de reglas proporcionadas por la empresa o persona que ha instalado el filtro Web. Un filtro permite a una empresa o usuario individual bloquear páginas de sitios Web que incluyan publicidad, contenido pornográfico, spyware, virus y etc. Los vendedores de filtros Web afirman que sus productos reducirán los lapsos de tiempos en la navegación recreativa por internet entre los empleados y protegerán las redes de varias amenazas que provienen de la Web.

VPN: Es una conexión cifrada entre redes privadas a través de una red pública, como Internet. En vez de usar una conexión dedicada de capa 2, como una línea arrendada, una VPN usa conexiones virtuales llamadas "túneles VPN", que se enrutan a través de Internet desde la red privada de la empresa hasta el host del sitio o del empleado remoto.

VPN de acceso remoto: Si se utiliza una VPN de sitio a sitio para conectar redes enteras, la VPN de acceso remoto admite las necesidades de los empleados a distancia, de los usuarios móviles y del tráfico de extranet de cliente a empresa. Una VPN de acceso remoto se crea cuando la información de VPN no se configura de forma estática, pero permite el intercambio dinámico de información y se puede habilitar y deshabilitar.

1.2. Implementación:

Anteriormente el UTM XTM-330 de la marca WatchGuard estaba resguardando la red de computadora ahora reemplazamos por una nueva versión del mismo fabricante UTM M200 de la misma Compañía, también en el capítulo 5 implementaremos otro UTM de la marca Fortinet la versión FortiGate 200 D para la creación de la zona DMZ usando un servidor Virtual un Fortimail.

En la Fig. 1.2.1, observamos cómo estaba nuestra red.



Fig. 1.2.1 Red de Computadora antes.

Después de haberse vencido el modelo XTM-330 que es una versión desfasada al modelo M200 con mejores requerimientos y características.

En la siguiente Fig.1.2.2, mostramos el esquema de la red después de utilizar el UTM.



Fig. 1.2.2 Esquema de la Red después de utilizar el nuevo UTM.

Para administrar el Watchguard tiene un método muy interesante que hay que descargar un software desde la página oficial del proveedor de ese modo se puede configurar este UTM. [1]

Ponemos nuestro Gateway por defecto en status las credenciales son readonly y de admin es readwrite, las credenciales de admin son para guardar los cambios hechos en el equipo. Después de cambiar las credenciales, entramos a la parte de Network y configuramos el enlace WAN e ingresamos nuestro Gateway que es 192.168.119.2.

En la Fig.1.2.3, presentamos la configuración de los enlaces WAN y LAN del UTM.

D:\Wat	tchguard\Saves\c	onfigs\WatchGuard-XTM	200_20180	108_1054.xml *-	Policy Manager	de Fireware	
Archivo E	Editar Ver Configu	urar Red FireCluster VPN	Servicios	de Suscripción A	yuda		
-	B . V +	X早老版目	1 2	🗓 🖉 🔗 🗖	. ?		
Firewall	Mobile VPN with IP.	Sec					
Orden /	Configuració	n de red		The second	n	_	
1 2	Interfaces			Contraction 1	Dodas Destancia		
3	mierraces A	gregacion de enlaces Pue	nte VLAN	Bucle invertido	prioge indiocola	WINS/DNS DNS d	inar
4	Seleccione la i	nterfaz que desea editar y o	iespués hao	a clic en Configu	rar. Para que el o	fispositivo XTM funci	one
5							0010
7	Configurar inte	erfaces en Modo de enruta	miento comb	anado			
8	Interfaz	Nombre (Alias)		Tipo	Dir	ección IPv4	
9	0	External		Externo	Di	reccion IP Publica.	
10	1	LANSENCOM		Confiable	15	92.168.119.2	
11	2	AP_102		VLAN			
13	3	AP100		VLAN			
14	4	Optional-3		Desactiva	do		
15	5	Optional-4		Desactiva	do		-
16	6	Optional-5		Confiable	Otro	Rango de Direccionam	nien
17	7	Internet MiltonHome		Confiable	Otro	Rango de Direccionam	nier
18		-					
19							

Fig. 1.2.3 Configuración de los enlaces WAN y LAN.

En la Fig.1.2.4, observamos el ingreso de los DNS Público y DNS de Google.



Fig. 1.2.4 Ingresando los DNS Público y DNS de Google.

En nuestro dispositivo de seguridad que es el WatchGuard establecemos la configuración del servidor de correo con su respectivo puerto como una lista de acceso. [3]

A continuación en la Fig.1.2.5, mostramos la configuración del servidor de correo.

0 🗉	InboundMailPop3S	InMailPop3S	External	Any-Trusted, Any-Optional	tcp:995

Fig. 1.2.5 Configuración del Servidor de correo.

1.3. Permisos en el servidor de Correo.

En la Fig.1.3.1, presentamos los permisos necesarios del servidor de correo.

TCP_587	TCP_587	Any-Trusted	IBW_mail_server	tcp:587

Fig. 1.3.1 Permisos del Servidor de Correo.

Después de permitir con una lista de acceso tanto el POP3 que almacena el correo en un servidor remoto, HTTPS y HTTP que son los Protocolo de navegación tanto segura con sus puertos 443 y 8080. [9]

En la Fig.1.3.2, mostramos el acceso de los distintos protocolos HTTP, HTTPS y POP3.

29	🔊 🔊 🕂 🔳 🕪	F HTTP-FB-Permitido	HTTP-proxy	Any-Trusted	Any-External	tcp:80
30	🔯 🔊 🖳 🛛 🧌	F HTTP-proxy-Sencom01	HTTP-proxy	Any-Trusted	Any-External	tcp:80
31	🗢 🖉 🖉 🖉	POP3-proxy-Sencom01	POP3-proxy	Any-Trusted, Any-Op	Any-External	tcp:110
32	IV 🔊 🕂 🖬 🗆 🍬	HTTPS-FB-Permitido	HTTPS-proxy	Any-Trusted	Any-External	tcp:443
33	🔊 🔎 🛄 🛛 🤌	HTTPS-proxy-Sencom01	HTTPS-proxy	Any-Trusted	Any-External	tcp:443

Fig. 1.3.2 Acceso a los protocolos HTTP, HTTPS y POP3.

Enrutar a	Puerta de enlace	Indicador	Interfaz	Agregar
10.0.5.4	10.0.5.1	0		Editar
0.57.56.0/24	192.168.119.109	1		Eliminar
192.168.1.0/24	192.168.119.109	1		Eiminar
192.168.200.0/24	192.168.119.220	1		Import
				Export
ou cannot import/export	routes for BOVPN interfaces			

En la Fig.1.3.3, observamos el enrutamiento entre las distintas VLAN.

Fig. 1.3.3 Enrutamiento entre las distintas VLAN.

En nuestro dispositivo de red utilizamos (NAT Dinámico) que es la traducción de direcciones de red por lo cual una IP pública es traducida a varias IP privadas como se ve en la Fig.1.3.4, [17]

K Configuración de NAT
Esas configuraciones de NAT sólo se aplican a las políticas de firewall.
La NAT Dinámica reescribe la IP de origen de los paquetes para usar la dirección IP de su interfaz de salida.
192.168.119.0/24 - Any-External
Arriba Abajo Agregar Eliminar
Aceptar Cancelar Ayuda

Fig. 1.3.4 Establecimiento del NAT Dinámico.

En la Fig. 1.3.5, presentamos el ingreso de nuestro protocolo de tiempo de red (NTP) al UTM para sincronizar los relojes de los sistemas informáticos.

Configuración de NTP
Los servidores NTP ayudan a sincronizar la hora Image: sincronizar la hora del sistema Nombres de Servidor/Direcciones IP del NTP:
0.pool.ntp.org 1.pool.ntp.org 2.pool.ntp.org
Agregar Eliminar Habilitar este dispositivo como un servidor NTP (Fireware OS v11.10 y superior)

Fig. 1.3.5 Establecimiento del Network Time Protocol.

El SNAT es cuando una laptop envía un paquete desde una red a un puerto en una interfaz externa u opcional, SNAT cambia la dirección IP de destino a una dirección IP y un puerto detrás del Firewall. Si una aplicación de software utiliza más de un puerto y los puertos se seleccionan en forma dinámica, debe usar 1 a 1 NAT o verificar si un proxy en el Firebox gestiona este tipo de tráfico. Esto implica que el NAT también opera sobre las conexiones desde las redes que su Firebox protege. [16]

En la Fig. 1.3.6, mostramos la configuración del NAT Estático (SNAT) para nuestro servidor de Tickets y el FTP.

	R SNAT	Editar SNAT
Editar SNAT Configurar uno o más miembros NAT para esta acción de SNAT. Nombre de SNAT: Descripción: NAT estático Balance de carga en el servidor Miembros de SNAT: PPUBLICA -> 192.168.119.213 Editar Eliminar Acceptar Cancelar	servidor. FTP_SNAT TicketServer Editar Eliminar	Configurar uno o más miembros NAT para esta acción de SNAT. Nombre de SNAT: FTP_SNAT Descripción: (a) NAT estático (b) Balance de carga en el servidor Miembros de SNAT: (c) Agregar Editar Eliminar Aceptar Cancelar
	Aceptar Cancelar Ayuda	

Fig. 1.3.6 NAT Estático en el servidor de tickets y el FTP.

Web blocker es el encargado de bloquear los sitios web por categoría. El objetivo es crear tantas listas negras de acceso prohibido y listas blancas de acceso permitido utilizando cualquier navegador: Internet Explorer, Mozilla Firefox, Chrome, Safari u Opera. Con el objetivo que nuestra red tenga mayor protección.

En la Fig. 1.3.7, observamos la restricción de categoría de sitios web en nuestro Web Blocker del UTM lo que deseamos bloquear en nuestra red para mayor seguridad en nuestro perímetro.



Fig. 1.3.7 Restricción de categoría de sitios web usando Web Blocker.

Capítulo 2

2. IPS:

2.1. Base Teórica:

Un sistema de prevención de intruso es el que examina los flujos de tráfico de la red para explotar las vulnerabilidades. Estas vulnerabilidades provienen en formas de entradas malintencionadas a una aplicación o servicio de destino que los atacantes usan para interrumpir para obtener el control de una PC. Después de un ataque exitoso el intruso puede deshabilitar la aplicación de destino, obtiene una conexión de extremo a extremo, resultando un estado de denegación de servicio, accediendo a todos los derechos y permisos disponibles.

Los IPS detectan el tráfico malintencionado en distintas formas:

Detección basada en firmas: funciona parecido como un antivirus y el administrador tiene que verificar que la firma este actualizado. Es decir la firma es capaz de reconocer una determinada cadena de bytes o patrón y a su vez manda una alerta.

Detección basada en políticas: el administrador de la red tiene que especificar que host tienen acceso a los recursos de la compañía por lo cual estas políticas de seguridad tienen que estar bien declaradas.

Detección basada en anomalías: este método consiste en el comportamiento anormal en nuestro sistema porque después de cierto tiempo de estar analizando el tráfico se genera un patrón luego cuando difiere activa las alarmas y esto tiende como un falso positivo.

2.2. Implementación:

Antes la Empresa Sistems Enterprise S.A. estaba estructurada de la siguiente manera:

En la Fig. 2.2.1, presentamos como estaba la red antes de implementar el IPS.



Fig. 2.2.1 Antes de la Implementación.

Procedimos a interceptar el tráfico entre el proveedor de servicios de internet y nuestro UTM WatchGuard modelo XTM 330 fue reemplazado por la versión M200 de la misma marca.



En la Fig. 2.2.2, mostramos el esquema que implementamos para el IPS.

Fig. 2.2.2 Esquema de la implementación del sensor IPS NSP M-1450

Primero el sensor M-1450 tenemos que establecer la conexión con la manager del IPS. Nosotros conectamos al puerto de consola del sensor con un adaptador DB9

a USB en una PC que está en la misma red y la manager es la interfaz gráfica del IPS que utiliza un sistema operativo llamado MLOS que está en el ESXI que es ambiente de virtualización por lo cual podemos configurar el equipo. [13]

En la Fig. 2.2.3, observamos la preparación de nuestro sensor IPS M-1450.



Fig. 2.2.3 Preparación del sensor M-1450.

Utilizamos el software Putty ya con el puerto identificado de nuestra pc COM5 y con el Baud-Rate 38400 ingresamos nuestras credenciales en el sensor M-1450 e ingresamos los siguientes comandos: **deinstall, **resetconfig

Estos comandos hacen que si el sensor borre la conexión de la manager y restaure los valores predeterminado del equipo, después con el comando setup estableceremos la conexión de la manager pero nos pedirá direcciones IP. [14]

En la Fig. 2.2.4, exhibimos la conexión del sensor desde el puerto de consola hacia la PC.



Fig. 2.2.4 Conexión del sensor desde el puerto de consola.

En el momento nos pedirá cambiar la contraseña del sensor y el nombre que deseemos.

En la Fig. 2.2.5, enseñamos la configuración del sensor con el comando setup.

COM5 - PUTTY × lease enter the sensor name 1: SENCOM Please enter the option for IP Type(IPV4=1 or IPV6=2 or BOTH=3) [IPV4=1]: y Error: IP Option is incorrect (Please ensure you enter corresponding numeral value 1,2 o 3). please enter it again or press CTRL-C/ESC to exit. lease enter the option for IP Type (IPV4=1 or IPV6=2 or BOTH=3) [IPV4=1]: 1 Please enter the sensor IP(A.B.C.D) [172.16.10.62]: Please enter the sensor subnet mask(A.B.C.D) [255.255.255.0]: 255.255.255.0 Sensor IP is already set, new IP will take effect after a reboot lease enter the manager primary IPv4 address(A.B.C.D): "You can set the Manager secondary IP in case the manager has two interfaces" Press Y to configure manager secondary IP address [N]: Y Please enter the manager secondary IPv4 (A.B.C.D): lease enter the sensor default gateway(A.B.C.D) [172.16.10.1]: lease enter management port configuration choice (a/m) [Auto]: There is no matched command. Please enter management port configuration choice(a/m) [Auto]: auto Error: Management port config choice is invalid, please enter it again or press CTRL-C/E C to exit.

Fig. 2.2.5 Configuración del sensor con el comando setup.

La dirección del sensor 192.168.1.221 y la máscara es: 255.255.255.0. Introducimos la dirección de la manager es 192.168.1.182. La primaria y la secundaria seria la misma sino hay otra y el default Gateway es 192.168.1.1 y le damos enter. [11]

En la Fig. 2.2.6, mostramos lo última configuración del comando setup:

Sensor configuration is almost complete. The final step is to establish a secure Management channel (trust) between the sensor and its Manager. This is accompli shed by a secret key that is shared by the Manager and this sensor. Please ensure that a shared secret key has already been defined on the Manager f or this sensor... Press Y to set shared secret key now or N to exit [Y]: _

Fig. 2.2.6 Terminando de configurar con el comando setup.

Y le damos N luego procederemos hacerlo.

Entramos a la manager con la dirección IP 192.168.1.182 en el Navegador introducimos las credenciales de acceso y nos vamos donde dice DEVICE en GLOBAL luego en New.

Ponemos el nombre que le pusimos desde la línea de comandos y la contraseña que va establecer la conexión del sensor con la manager.

Como se ve en la Fig.2.2.7, establecemos la llave compartida en la manager. [8]



Fig. 2.2.7 Establecer la llave compartida en la manager.

En la Fig. 2.2.8, verificamos la llave compartida en la manager.



Fig. 2.2.8 Verificación de la llave compartida.

Regresamos al software Putty e introducimos el comando <u>Shared Secret Ke</u>y y con la misma contraseña que habíamos puesto en la manager hacemos ahora desde la línea de comando

En la Fig.2.2.9, presentamos el establecimiento de la llave compartida en el sensor.

login as: admin
* * *
Authorized users only. Unauthorized users will be prosecuted
to the full extent of the law.
* * *
admin@ 's password:
Access denied
admin@ 's password:
Last login: Mon Mar 19 14:02:56 2018 from
Trying
Connected to
Escape character is '\377'.
Hello, this is zebra (version 0.92a).
Copyright 1996-2001 Kunihiro Ishiguro.
intrushell@SENCOM> set sensor sh
intruShell@SENCOM> set sensor sharedsecretkey

Fig. 2.2.9 Estableciendo la llave compartida en el sensor.

Ahora para ver que el sensor y la manager tiene la conexión establecida damos el siguiente comando status.

En la Fig. 2.2.10, verificamos la relación entre el sensor y la manager con el comando status en el sensor.

[Manager Communications]	
frust Established	yes (RSA 2048-bit with SHA2 support)
Alert Channel	up
Log Channel	up
Authentication Channel	up
Last Error	None
Alerts Sent	35510
Logs Sent	11396

Fig. 2.2.10 Verificando la relación entre el sensor y la manager.

2.3. Actualización del IPS:

En la manager nos vamos donde updating y en Download Device Software, nos muestra todos las actualizaciones para diferentes modelos buscamos nuestro sensor M-1450, seleccionamos la versión 9.1.3.6 y comenzamos el download.

En la Fig. 2.3.1, exhibimos la elección de la versión a actualizar y descargar.

McAfee Network Secur Version: 9.1.7.49	ity Manager	Dashboard	Analysis	Policy	Devices	Nanager	_	_
Domain: /Sencom 👻	/Sencom >	Updating > Dow	mload Device	Software				
 Updating Download Signature Sets Download Callback Detectors 	0				8.1.3.124 8.1.3.100 8.1.3.89			
Manual Import Messages from McAfee > Automatic Updating	O Hodel: H	1450			8.1.3.43			
 Users and Roles Setup Integration 	8	1450			9.1.3.6			
 Reporting Maintenance Troubleshooting 	0				8.3.3.37			
	0				8.3.3.35			
	0				8.3.3.9 8.3.3.4			
	0				8.1.3.130 8.1.3.124			
	0				8.1.3.100			
	0				8.1.3.43			

Fig. 2.3.1 Elegir la versión a actualizar y descargar

Ahora nos muestra desde la versión que tenemos y la versión que descargamos ahora damos click en Upgrade.

En la Fig. 2.3.2, presentamos la actualización del IPS.

McAfee Network Securi Version: 9.1.7.49	rity Manager 😥 Watager	4
Domain: /Sencom 💌	/Sencom > IPSM1450 > Maintenance > Deploy Device Software	?
Global Devices	Use this page to upgrade (or downgrade) the software running on this device.	
Device: IPSM1450 Y	Deploy Device Software	
Summary	Software Ready for Installation Running	oftware Version
 Setup Maintenance 	9.1.3.5	9.1.3.4
Deploy Device Software Import Configuration		Upgrade
Export Configuration Reboot Shut Down > Troubleshooting Deploy Pending Changes > IPS Interfaces		

Fig. 2.3.2 Actualizando la versión del IPS del NSP M-1450.

Para comprobar que hemos actualizado a la última versión nos vamos al software Putty para ver la actualización con el comando status. En la Fig. 2.3.3, mostramos la última versión disponible para el IPS.

PuTTY			<u> </u>	×
System Name	:	SENCOM		^
Date		1/30/2018 - 21:16:2 UTC		
System Uptime		05 min 45 secs		
System Type		M-1450		
Serial Number		S025350126		
Software Version		9.1.3.6		
Hardware Version		1.10		
MGMT Ethernet port		auto negotiated		
MGMT port Link Status		link up		

Fig. 2.3.3 Última versión disponible para el IPS NSP M-1450.

Y la versión que anteriormente es:

En la Fig. 2.3.4, observamos la versión anterior del II	PS.
---	-----

PuTTY		_	×
			^
Date	: 1/30/2018 - 21:28:1 UTC		
System Uptime	: 03 min 01 secs		
System Type	: M-1450		
Serial Number	: S025350152		
Software Version	: 9.1.3.4		
Hardware Version	: 1.10		
MGMT Ethernet port	: auto negotiated		
MGMT port Link Status	: link up		

Fig. 2.3.4 Versión anterior del IPS.

Después de tener la conexión con la manager y luego de haber actualizado el IPS procedimos a colocar el sensor en el Rack, para esto tuvimos que hacer cable RJ-45 categoría 6 y medimos la distancia que hay entre el ISP, UTM y el Switch de IP Privada.

Después de colocar los conectores desde la manager estaba en down lo cual lo encendimos y al final mostraremos como un antes y un después de haber implementado este equipo. Esto es en capa 2.

En la Fig. 2.3.5, revelamos la implementación del IPS los enlaces WAN, LAN y AP. En esta parte ya hemos colocado el dispositivo de red en el rack y podemos acceder desde SSH.

McAfee Network Securi Version: 9.2.7.9	ity Manage	Dashboard	Analysis	Policy Devices	Manager						
Domain: /Sencom 💌	/Sencom	> SENCOM > S	etup > Physical	Ports							
Global Devices	Use this p	this page to manage the physical ports on this device. (Changes made on this page take effect immediately.)									
Device: SENCOM V C	Monitori	ng Ports Res	ponse Ports Ma	nagement Port							
Summary	Use this	Use this tab to manage this device's monitoring ports.									
Setup	Death (Link	Connector	Cound	Operation						
IP Bindings	POPL	LINK	Туре	speed	Mode	Fail-Open Kit	Placement	Kesponse Port			
Name Resolution	1A	🔍 Up	RJ-45	1 Gbps / Full (auto-neg	In-line Fail Open - Passive (Paired	Built in	Outside Network	This Port			
Time Zone NTP	1B	🔍 Up	RJ-45	1 Gbps / Full (auto-neg	In-line Fail Open - Passive (Paired	Built in	Inside Network	This Port			
Proxy Server	2A	🔍 Up	RJ-45	1 Gbps / Full (auto-neg	In-line Fail Open - Passive (Paired	Built in	Outside Network	This Port			
ATD Integration NTBA Integration	2B	🔍 Up	RJ-45	1 Gbps / Full (auto-neg	In-line Fail Open - Passive (Paired	Built in	Inside Network	This Port			
Application Identification	ЗA	Ø Disabled	RJ-45	1 Gbps / Full (auto-neg	In-line Fail Open - Passive (Paired	🗕 Bypassi	Inside Network	This Port			
 Quarantine Logging 	3B	Ø Disabled	RJ-45	1 Gbps / Full (auto-neg	In-line Fail Open - Passive (Paired	Bypassi	Outside Network	This Port			
Remote Access	4A	🔍 Up	RJ-45	1 Gbps / Full (auto-neg	In-line Fail Open - Passive (Paired	Built in	Outside Network	This Port			
 Performance Monitoring Advanced 	4B	🔍 Up	RJ-45	1 Gbps / Full (auto-neg	In-line Fail Open - Passive (Paired	Built in	Inside Network	This Port			
 Maintenance Troubleshooting Deploy Pending Changes IPS Interfaces 								-			

Fig. 2.3.5 Implementación del IPS con sus enlaces WAN, LAN y AP.

2.4. Políticas del IPS:

Configuramos las políticas del IPS en la manager.

En la Fig.2.4.1, mostramos la configuración de las políticas del IPS.

Domain: /Sencom	/Sencom > Intrusion Prevention > Polic	y Types > IPS Policies								
Intrusion Prevention	IPS policies contain all IPS attack definitions, including exploits, malware, policy violations, Denial-of-Service and reconnaissance attacks. Use this page to define and assign IPS policies.									
Policy Manager	IPS Policies									
Policy Types IPS Policies				Ownership and Mi	alatus.					
Advanced Malware Policies Inspection Options Policies	me	Description A	Attack Set Profile	Owner Domain	Visibility	Editable Here				
Connection Limiting Policies	aster Attack Repository	Default settings for all attack definitions	Master Attack Repository	/Sencom	Owner and child domains	Yes				
Pirewaii Policies QoS Policies ▷ Exceptions ▷ Objects ▷ Advanced	Default Testing	All attacks (blocking disabled)	Default Testing	/Sencom	Owner and child domains	Yes				
	Default Exclude Informational	All attacks except informational-severity attacks (blocking disabled)	Default Exclude Informational	/Sencom	Owner and child domains	Yes				
	Sencom	Sencom perimetro	Default Prevention	/Sencom	Owner and child domains	Yes				
	Default Detection	The standard attack set (blocking disabled)	Default Detection	/Sencom	Owner and child domains	Yes				
	SENCOM_WANdetection_1A-1B	The standard attack set (blocking disabled)	Default Detection	/Sencom	Owner and child domains	Yes				
	SENCOM_LAN_Detection_2A-2B	The standard attack set (blocking disabled)	Default Detection	/Sencom	Owner and child domains	Yes				
	SENCOM_AP_Detection_4A-4B	The standard attack set (blocking disabled)	Default Detection	/Sencom	Owner and child domains	Yes				
	Default Prevention	The standard attack set (blocking enabled for RfSB attacks only)	Default Prevention	/Sencom	Owner and child domains	Yes				
	SENCOM_WANprevention_1A-1B	The standard attack set (blocking enabled for RfSB attacks only)	Default Prevention	/Sencom	Owner and child domains	Yes				
	SENCOM_LAN_Prevention_2A-2B	The standard attack set (blocking enabled for RfSB attacks only)	Default Prevention	/Sencom	Owner and child domains	Yes				
	SENCOM_AP_Prevention_4A-4B	The standard attack set (blocking enabled for RfSB attacks only)	Default Prevention	/Sencom	Owner and child domains	Yes				
	Default DoS and Reconnaissance Only	Threshold, learning and correlation-based attacks only (blocking disabled)	Default DoS and Reconnaissa	/Sencom	Owner and child domains	Yes				
	SENCOM_WAN-DoS_1A-1B	Threshold, learning and correlation-based attacks only (blocking disabled)	Default DoS and Reconnaissa	/Sencom	Owner and child domains	Yes				
	SENCOM_LAN_DoS_2A-2B	Threshold, learning and correlation-based attacks only (blocking disabled)	Default DoS and Reconnaissa	/Sencom	Owner and child domains	Yes				
	SENCOM_AP_DoS_4A-4B	Threshold, learning and correlation-based attacks only (blocking disabled)	Default DoS and Reconnaissa	/Sencom	Owner and child domains	Yes				

Fig. 2.4.1 Configuración de las políticas del IPS.

A continuación en la Fig.2.4.2, podemos observar la asignación de las políticas de prevención a cada puerto el 1A/1B es el enlace WAN. Así a los demás puertos 2A/2B es la LAN, 4A/4B es el AP.

McAfee Network Securi Version: 9.1.7.49	ty Manager Reference Analysis Policy Devices	Manager	
Domain: /Sencom	/Sencom > Intrusion Prevention > Policy Types > IPS Policies		?
Intrusion Prevention Policy Manager Policy Types IPS Policies Advanced Malware Policies Inspection Options Policies	Assign this policy to one or more interface. Note: Interfaces assigned to a policy group cannot be managed from this Assignments Search Interfaces	page. They can be managed from the <u>Policy I</u>	Manager-
Connection Limiting Policies	Available Interfaces	Current Policy	Selected Interface (Policy Group)
QoS Policies	/Sencom/SENCOM/2A-2B	SENCOM_LAN_Detection_2A-2B	/Sencom/SENCOM/1A-1B
Exceptions	/Sencom/SENCOM/3A-3B	Default Prevention	
 Objects Advanced 	/Sencom/SENCOM/4A-4B	SENCOM_AP_Detection_4A-4B	
		•	
		3 Objects	1 Object
			Reset
	SENCOM_WANdetection_1A-1B		Save Cancel

Fig. 2.4.2 Asignación de las políticas a los puertos correspondientes.

En la Fig. 2.4.3, guardamos las políticas del IPS.

McAfee Network Securi Version: 9.1.7.49	ty Manager Residual Analysis	Policy Devices	X Ianager		_	_		_	1			
Domain: /Sencom	/Sencom > Intrusion Prevention > Policy	Types > 1PS Policies							?			
✓ Intrusion Prevention	IPS policies contain all IPS attack definitions, including exploits, malware, policy violations, Denial-of-Service and reconnaissance attacks. Use this page to define and assign IPS policies.											
Policy Manager	1PS Policies											
Policy Types IPS Policies			Ownership and Vi	Auroanship and Visibility Last Hadatad								
Advanced Malware Policies Inspection Options Policies	*	Attack Set Profile	Owner Domain	Visibility	Editable Here	Active Revision	Time	By	Assignments			
Connection Limiting Policies	k definitions	Master Attack Repository	/Sencom	Owner and child domains	Yes	1	Feb 28, 2018 01:04:11	admin	n/a			
QoS Policies		Default Testing	/Sencom	Owner and child domains	Yes	1	Feb 28, 2018 01:04:12	admin	2			
Exceptions	-severity attacks (blocking disabled)	Default Exclude Informational	/Sencom	Owner and child domains	Yes	1	Feb 28, 2018 01:04:12	admin	2			
 Objects Advanced 		Default Prevention	/Sencom	Owner and child domains	Yes	Z	Feb 28, 2018 01:04:13	admin	٩			
	ng disabled)	Default Detection	/Sencom	Owner and child domains	Yes	1	Feb 28, 2018 01:04:11	admin	۵.			
	ng disabled)	Default Detection	/Sencom	Owner and child domains	Yes	3	Mar 02, 2018 15:03:36	admin	۵.			
	ng disabled)	Default Detection	/Sencom	Owner and child domains	Yes	1	Mar 02, 2018 15:35:07	admin	9			
	ng disabled)	Default Detection	/Sencom	Owner and child domains	Yes	1	Mar 02, 2018 15:39:57	admin	٩			
	ng enabled for RfSB attacks only)	Default Prevention	/Sencom	Owner and child domains	Yes	2	Feb 28, 2018 01:04:13	admin	1			
	ng enabled for RfSB attacks only)	Default Prevention	/Sencom	Owner and child domains	Yes	1	Mar 02, 2018 15:04:38	admin	1			
	ng enabled for RfSB attacks only)	Default Prevention	/Sencom	Owner and child domains	Yes	1	Mar 02, 2018 15:37:15	admin	1			
	ng enabled for RfSB attacks only)	Default Prevention	/Sencom	Owner and child domains	Yes	1	Mar 02, 2018 15:40:59	admin	1			
	tion-based attacks only (blocking disabled)	Default DoS and Reconnaissa	/Sencom	Owner and child domains	Yes	1	Feb 28, 2018 01:04:12	admin	2			
	tion-based attacks only (blocking disabled)	Default DoS and Reconnaissa	/Sencom	Owner and child domains	Yes	1	Mar 02, 2018 15:06:39	admin	2			
	tion-based attacks only (blocking disabled)	Default DoS and Reconnaissa	/Sencom	Owner and child domains	Yes	1	Mar 02, 2018 15:38:03	admin	۵.			
	tion-based attacks only (blocking disabled)	Default DoS and Reconnaissa	/Sencom	Owner and child domains	Yes	1	Mar 02, 2018 15:43:51	admin	۵.			
	Custom Attacks						Ner	Сору	Edit Delete			

Fig. 2.4.3 Guardando las políticas del IPS.

En la Fig.2.4.4, presentamos las políticas de Firewall para denegar el tráfico proveniente de Rusia y China.

Version: 9.1.7.49		er Dashboard	Analysis	Policy Devi	ces Manager	_	_	_	_	_		
Domain: /Sencom	/Sencom > Infrusion Prevention > Policy Types > Firewall Policies ?											
Intrusion Prevention Policy Hanager Velicy Types HS Policies Advanced Milware Policies Inspection Options Policies Connection Limiting Policies QeS Policies Dispects Dispects Advanced	Firewall policies control endpoint access (and inspection) based on source, destination, and application, etc. Use this page to define and assign firewall policies.											
	Properties Access Rules											
	Use this page to define access rules, which are evaluated from the top downward and respond on a first-matched basis. Important: Traffic that does not match an explicit access rule will be permitted.											
										Search		
		State	Description		Direction	Source Address	Source User	Destination Address	Application	Effective Time	Response	
	1	Enabled	Bloqueo Paises			China Russia	🙆 Any	Any	🔅 Any	🔯 Always	Drop	
										1 rule		
	Sencom	_FW							🛛 Prompt for a	assignment after save	Save Cancel	

Fig. 2.4.4 Políticas de Firewall del IPS.

En la Fig. 2.4.5, enseñamos como estaba la red de computadoras antes de la implementación del IPS.



Fig. 2.4.5 Antes de implementar el IPS.

En la Fig. 2.4.6, mostramos después de implementar el IPS nos quedó de la siguiente manera:



Fig. 2.4.6 Después de implementar el IPS.
Capítulo 3

3. Servidor DNS:

3.1. Teoría:

Proviene de las palabras (Domain Name System o Sistema de nombres de dominio) su función es que traduce nombres de dominio a IPs y viceversa. En las redes TCP/IP cada dispositivos final dispone de una dirección IP para la comunicación con el resto de PCs es como decir que es un identificador único que lo diferencia del resto de dispositivos. Durante el proceso de búsqueda de un nombre, funcionan como clientes DNS, Consultando otros servidores para resolver completamente el nombre buscado. Un diagrama jerárquico de cómo funciona un servidor DNS.





Fig. 3.1.1 Tipos de jerarquía para un servidor DNS.

Los Forwarders son los encargados de reenviar a los otros DNS internos para reenviar consultas y resolver nombres de dominios externos o fuera del sitio.



En la Fig. 3.1.2, indicamos el funcionamiento del Forwarders.

Fig. 3.1.2 Funcionamiento del Forwarders.

3.2. Implementación:

Después de preparar una máquina virtual en nuestro segmento de IP Privada con todas las características básicas en hardware y ya con el sistema operativo LINUX listo, Iniciamos la instalación. [18]

En la Fig. 3.2.1, evidenciamos la selección del idioma en la instalación del servidor DNS.

Choose the language also be the default	to be used for the inst language for the instal	all led	ation process. The system.	selected	language	will
Language:						
	C Albanian Arabic Arabic Asturian Basque Belarusian Buigarian Catalan Chinese (Simplified) Chinese (Graditional) Croatian Creatian Czech Danish Dutch Esperanto Estonian Finnish French Galician German Greek		No localization Shaip マンチ Asturianu Euskana Bosanski bahrapcxM Català 中文(間体) 中文(電体) 中文(電体) 中文(電体) 中文(電体) 中文(電体) 中文(電路) Experanto Essti Suomi Français Galego Deutsch Exhyruků			
<go back=""></go>						

Fig. 3.2.1 Selección del idioma de instalación en Linux.

En la Fig. 3.2.2, señalamos la elección del tipo de teclado en el servidor.



Fig. 3.2.2 Elección del tipo de teclado en el servidor

En el proceso de instalación del sistema operativo es necesario establecer el idioma en nuestro caso es en inglés y el tipo de teclado por los diferentes caracteres que son necesarios para programar.

En la Fig. 3.2.3, indicamos el establecimiento de las credenciales de acceso.



Fig. 3.2.3 Establecer las Credenciales de acceso.

En la Fig. 3.2.4, mostramos la instalación del sistema del servidor DNS.



Fig. 3.2.4 Instalación del Sistema Operativo.

En la Fig. 3.2.5, presentamos el ingreso de nuestras credenciales para después acceder a la plataforma del Zentyal. Esperamos que termine de configurar. [12]

c zentyal x + ← C Image: A straight of the stra	··· 🛛 🏠	III\ © ≡
	🛡 🏠	Ⅲ\ 🖾 🗏
Czentya		
O zentya		
Czentya		
	al	
Username		
herzan		
Password		
•••••		
	_	
ENTER		
Created by Zentval S.L.		
- C - C - Cantual Manilla Sizofau		

Fig. 3.2.5 Ingreso de las Credenciales.

Luego posteriormente descargamos archivos necesarios para la ejecución de nuestro Server procedimos a configurar nuestro servidor DNS.

En la Fig. 3.2.6, observamos la elección de los módulos a instalar en el Server.



Fig. 3.2.6 Elección de los módulos a instalar.

Al momento de seleccionar los módulos necesarios para nuestro servidor DNS va a instalar los paquetes en nuestra plataforma y en el servidor. De este modo podamos configurarlo.

En la Fig. 3.2.7, enseñamos la descarga e instalación de los paquetes requeridos.



Fig. 3.2.7 Descarga e Instalación de los paquetes requeridos.

En la Fig. 3.2.8, exponemos la configuración de la interfaz externa.



Fig. 3.2.8 Configuración de la interfaz Externa.

Establecemos el nombre del dominio por el cual nuestro servidor DNS estará traduciendo los diferentes sitios Web por nombres. Esperamos que se guarden los cambios hechos para acceder a la plataforma del Zentyal.

En la Fig. 3.2.9, revelamos los ajustes del Nombre de Dominio.



Fig. 3.2.9 Ajuste del Nombre de Dominio.

En la Fig. 3.2.10, observamos la configuración realizada.



Fig. 3.2.10 Estableciendo las configuraciones realizadas.

Asignamos nuestro direccionamiento de IP Privado en la plataforma como cualquier servidor es necesario que sea Estático y guardamos los cambios.

En la siguiente Fig. 3.2.11, enseñamos la configuración de la dirección IP del server.

Ozentyal Developme	nt Edition 5.0	Search
R Network	Name	
Interfaces	eth0	
Gateways	Method	
DNS	Static •	
Objects		
Services	External (WAN)	intual as a mateway and this interf
Static Routes	Internet router.	niyai as a gaceway and this intern
Tools	IP address	Netmask
Logs	192.168.119.129	255.255.255.0 •
Software Management <	CHANGE	

Fig. 3.2.11 Configurando la Dirección IP del Server.

En la Fig. 3.2.12, guardamos los cambios hechos en el server.



Fig. 3.2.12 Guardando los Cambios Realizados.

En la Fig. 3.2.13, verificamos los módulos activados en el servidor DNS.

Oz	zentyal Deve	lopi	nent Edition 5.0	Search	Q G
۲	Dashboard		Module Status (Configuratio	on
99	Module Status		Module	Depends	Status
*	System	<	Network		
망	Network	<	Firewall	Network	
	Logs		DNS DNS	Network	
	Software	<	Logs		
	Management		NTP		
!! !	Users and Computers	<	Domain Controller and File Sharing	Network, DNS, NTP	

Fig. 3.2.13 Verificación de los módulos activados en el server.

En la Fig. 3.2.14, podemos observar la habilitación de la cache del DNS transparente.



Fig. 3.2.14 Habilitación de la cache del DNS transparente.

[&]quot;Organizar Y Establecer Nuevas Soluciones de Seguridad en la Red de la Empresa Sistems Enterprise S.A."

En nuestro servidor DNS para que resuelva los nombres de los sitios Web con sus debidos servidores es necesario tener los reenviadores o Forwarders en nuestro caso añadimos a google.

Como se ve en la	Fig. 3.2.15.	añadimos los	Forwarders of	de los DNS de	Google.
	,				

O z	zentyal Deve	elopme	nt Edition 5.0			Search			۹ 🗗
1	Management	<							
*	Users and Computers	<	+ ADD NEW						Q
					Forwarder				Action
\diamond	Domain	<			8.8.8.8			6	3 🖉
	File Sharing				1	0 🗾	KK	Page 1	K
(IN CONTRACTOR OF INCOME IN CONTRACTOR OF INCOME I	DNS		Domains						
	Firewall	<	Domains						
Crea	ated by <u>Zentyal S.L</u>	-	+ ADD NEW						Q
			Domain [Domain IP Addresses	Hostnames	Mail Exchangers	Name Servers	TXT records	Services
			sencom.com.ni	*	*	*	*	*	*

Fig. 3.2.15 Añadir los Forwarders de los DNS de Google.

En la Fig. 3.2.16, presentamos la configuración de nuestro dominio lo cual añadimos nuestra dirección IP fija del Servidor y también nuestro Gateway.

0	zentyal Deve	elopn	ent Edition 5.0 Search	Q	•
۲	Dashboard		Domains > sencom.com.ni		?
র র	Module Status		IP address		
*	System	<	+ ADD NEW		Q,
망	Network	<	IP Address	Action	
	Logs		192.168.119.129	8]
1	Software Management	<	192.168.119.2	8]
	Users and		10 y K < P	age 1 >	К

Fig. 3.2.16 Configuración de nuestro dominio.

3.3. Prueba del Servidor DNS:

Ahora con el comando nslookup en una máquina virtual Windows 7 del mismo rango de red nos dispondremos a verificar si el Servidor DNS está funcionando debidamente.

En la Fig. 3.3.1, comprobamos nuestra dirección IP en la PC con el comando ipconfig desde el cmd.

C\Windows\system32\cmd.exe]
Microsoft Windows [Versión 6.1.7600] Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.	
C:\Users\CISCO>ipconfig	1
Configuración IP de Windows	
Adaptador de Ethernet Conexión de área local:	
Sufijo DNS específico para la conexión : localdomain Vínculo: dirección IPv6 local : fe80::5040:ed0a:4148:6623x11 Dirección IPv4 : 192.168.119.128 Máscara de subred : 255.255.255.0 Puerta de enlace predeterminada : 192.168.119.2	
Adaptador de túnel isatap.localdomain:	
Estado de los medios : medios desconectados Sufijo DNS específico para la conexión : localdomain	
C:\Users\CI\$C0>	
-	

Fig. 3.3.1 Comprobando nuestra dirección IP en la PC.

Como se ve en la Fig. 3.3.2, verificamos el servidor DNS.

C:\Windows\system32\cmd.exe - nslookup
> www.youtube.com
Servidor: ns.sencom.com.ni
Address: 192.168.119.129
Beenveets ne sutenitatius:
Nespuesta no autoritativa. Nombre: uoutube-ui l google com
Addresses: 2607:f8b0:4008:811::200e
216-58-192-46
172.217.2.78
216.58.192.110
172.217.2.206
172.217.0.174
172.217.8.110
216.58.219.78
172 217 8 142
216-58-219-142
172.217.3.78
172.217.15.206
Aliases: www.youtube.com
kuuu uni edu ni
Servidor: ns.sencom.com.ni
Address: 192.168.119.129
Respuesta no autoritativa:
Nombre: www.uni.edu.ni
Address: 165.98.144.15
> www.facebook.com
Servidor: ns.sencom.com.ni
Address: 192.168.119.129
Beenveets no suteritatius:
Nombue' stan-mini clûn facebook com
Addresses: 2a03:2880:f12c:183:face:b00c:0:25de
157.240.14.35
Aliases: www.facebook.com

Fig. 3.3.2 Verificación del servidor DNS.

Capítulo 4

4. Fortimail:

Consiste en un Antispam y servidor de correo. El usuario recibe un mensaje por cierta persona pero en el contenido del mensaje es enviado un enlace a otro sitio vulnerable y eso se conoce como phising.

Antispam: Es un método para no recibir correo basura, tanto para los usuarios finales como para los administradores de los sistemas de correos electrónicos usan diferentes técnicas contra ellos. Estas técnicas han sido incorporadas en distintos productos, servicios y software para aliviar la carga que cae sobre usuarios y administradores. No hay una forma perfecta para solucionar este problema de Spam, entre las múltiples unas funcionan mejor que otras, rechazando así en su totalidad y en algunos casos el correo deseado para eliminar completamente el Spam.

Detección de spam: Consiste en perder gran cantidad de correos electrónicos basura para reducir la cantidad de correos legítimos. Se basa en el contenido del mensaje del correo electrónico, ya sea por la detección de palabras clave como (Viagra) o por medios estadísticos. Los métodos antes mencionado pueden ser muy precisos cuando se sintoniza con los correos legítimos que la persona recibe, se puede cometer errores tales como él envió de contenido destinados a una dirección particular o más bien a una distribución masiva.

Existen sitios conocidos como listas negras, estos son direcciones IP de Spammers conocido, también están los spamtraps son direcciones de correo electrónico invalidas que no se utilizan durante mucho tiempo para recoger correos basura.

4.1. Implementación:

ARQUITECTURA.

La arquitectura de la solucion es bastante sencilla al implementar el Fortimail, en la cual tenemos una sola conexión (En este caso es Virtual). la arquitectura quedara asi:

En la Fig. 4.1.1, observamos la arquitectura de implementacion del Fortimail en SENCOM.



Fig. 4.1.1 Arquitectura de implementación del Fortimail.

4.2. Instalación del Fortimail.

El Fortimail al ser una maquina virtual se instalara sobre la plataforma VmWare, lo que se usa para instalar es una plantilla OVF que se descarga desde la pagina web de Fortinet con una cuenta previamente creada:

Primero accedemos al sitio:

<u>https://support.fortinet.com/Download/FirmwareImages.aspx</u> nos logueamos con el usuario y nos dara una pagina como esta, donde damos clic en "Download \rightarrow Firmware Images": [6]

En la Fig. 4.2.1, enseñamos como se descarga el Firmware desde la pagina oficial de Fortinet.

	DET SUPPORT Home	Asset	Assistance	Download Feedback	Cristhian Narva LOG OUT View All Accounts
Firmware Images	Fortinet Firmware images And Software Releases			Forbisuard Service Updates Firmware Images Firmware Image Checksums HQIP Images	

Fig. 4.2.1 Descarga del Firmware desde la página oficial de Fortinet.

En la siguiente Fig. 4.2.2, mostramos la selección del producto el cual implementaremos en nuestro caso es el Fortimail:

FortiGate	
FortiConverter FortiCore FortiDB	
FortiDDoS FortiDNS	
FortExtender	
FortiGate	
FortiGate-One	
FortiGateConnector	
FortiLog	
FortiMail	

Fig. 4.2.2 Selección del producto el cual implementaremos.

Luego de que hayamos seleccionado la ultima version disponible del Fortimail como se ve en la Fig. 4.2.3.

FortiMail			•	
Releas	e Notes Do	ownload		
mage File	Path			
/ <u>FortiMa</u>	Ш/			
mage Fold	ders/Files			
	Name	Size (KB)	Date Created	Date Modified
	Archives	Directory	2007-12-04 15:12:00	2007-12-04 15:12:00
	v2.8	Directory	2010-10-29 10:10:53	2010-10-29 10:10:53
	v3.00	Directory	2010-10-29 10:10:07	2010-10-29 10:10:07
	v4.00	Directory	2015-02-23 10:02:57	2015-02-23 10:02:57

Fig. 4.2.3 Elección de la última versión disponible del Fortimail.

En la siguiente Fig. 4.2.4, enseñamos el procedimiento para descargar la ultima version disponible del Firmware, esa es la imagen que vamos a descargar via HTTPS:

	FML_3000E-64-v54-build0692-FORTINET.out	93,642	2017-07-25 09:07:47	2017-07-25 09:07:47	HTTPS Checksum
	FML_3200E-64-v54-build0692-FORTINET.out	93,619	2017-07-25 09:07:28	2017-07-25 09:07:28	HTTPS Checksum
	FML_400E-v54-build0692-FORTINET.out	93,493	2017-07-25 09:07:41	2017-07-25 09:07:41	HTTPS Checksum
	FML_60D-v54-build0692-FORTINET.out	92,413	2017-07-25 09:07:02	2017-07-25 09:07:02	HTTPS Checksup
	FML_VM-64-v54-build0692-FORTINET.out	92,855	2017-07-25 09:07:06	2017-07-25 09:07:06	HTTPS D cksum
	FML_VM-64-v54-build0692-FORTINET.out.ovf.zip	178,856	2017-07-25 09:07:49	2017-07-25 09:07:49	HTTPS Checksum
D	THE REPORT OF A LOCAL PROPERTY OF	02.014	00 50 00 00 00 00 00	0047-07-05-00-07-00	UTTOC CI I

Fig. 4.2.4 Procediendo a descargar la última versión disponible del firmware.

En la Fig. 4.2.5, obsevamos como se descargara el archivo en formato Rar de esta forma:



Fig. 4.2.5 Descargando la versión 5.4 del Fortimail.

Lo decomprimos y veremos varios OVF y otros archivos que son parte de esos OVF, lo que los diferencian es el tamaño en disco que la plantilla tiene configurado en este caso seria la de **250 Gb.** [7]

Como se ve en la Fig. 4.2.6, seleccionamos el archivo a desplegar en nuestro Hypervisor.

lombre	Fecha de modifica	Tipo	Tamaño
FML VM-64-v53-build0634-FORTINET.out.ovf.zip	25/05/2017 08:40 a	Archivo WinRAR Z	153.838 KB
😡 fortimail-vm-64bit-250gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
👧 fortimail-vm-64bit-1024gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
😡 fortimail-vm-64bit-2048gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
👧 fortimail-vm-64bit-4096gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
👧 fortimail-vm-64bit-8192gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
🙀 fortimail-vm-64bit-12288gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
🚯 fortimail-vm-64bit-24576gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
🐣 fortimail-vm-disk1.vmdk	28/02/2017 07:50	VMware virtual dis	154,818 KB
🐣 fortimail-vm-disk2-250gb.vmdk	28/02/2017 07:50	VMware virtual dis	117 KB
🐣 fortimail-vm-disk2-1024gb.vmdk	28/02/2017 07:50	VMware virtual dis	244 KB
🐣 fortimail-vm-disk2-2048gb.vmdk	28/02/2017 07:50	VMware virtual dis	372 KB
🐣 fortimail-vm-disk2-4096gb.vmdk	28/02/2017 07:50	VMware virtual dis	628 KB
🐣 fortimail-vm-disk2-8192gb.vmdk	28/02/2017 07:50	VMware virtual dis	1,183 KB
🐣 fortimail-vm-disk2-12288gb.vmdk	28/02/2017 07:50	VMware virtual dis	1,678 KB
afortimail-vm-disk2-24576gb.vmdk	28/02/2017 07:50	VMware virtual dis	3,288 KB

Fig. 4.2.6 Selección del archivo a desplegar en nuestro Hypervisor

En la Fig. 4.2.7, presentamos el despliegue del OVF del Fortimail para su debida instalacion en el servidor ESXI para poder instalar la imagen, esta es un OVF asi que solo seguimos la ruta: **File** \rightarrow **Deploy OVF Template**.

rice.	calt view inventory Ad	rmanit	tration	1
	New	•	ntory	Þ
	Deploy OVF Template			
	Export	•		
	Report	•	local	əst
	Browse VA Marketplace		Getti	9 5
	Print Maps		l	L
	Exit		wn	r.
_		_	" A n	bst

Fig. 4.2.7 Despliegue del OVF del Fortimail para su debida instalación.

Como se ve en la Fig. 4.2.8, seleccionamos el Firmware para el despliegue del Fortimail.

🕜 Deploy OVF Template		<u>1995</u> 0		×
Source Select the source location.				
Source OVF Template Details Name and Location Storage Disk Format Ready to Complete	Deploy from a file or URL C: \Users\Lenovo\Documents\Fortimail\fortimail-vm-64bit-250 Brow Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive network share, or a CD/DVD drive.	vse]	

Fig. 4.2.8 Selección del Firmware para el despliegue del Fortimail.

En la Fig. 4.2.9, exponemos la eleccion del archivo necesario del Fortimail.

manizar 🔻 Nueva ca	irpeta		8	
,	Nombre	Fecha de modifica	Tino	Tamaño
🕈 Acceso rápido		r cente de modifica	ripo	Turnullu
Escritorio 💉	tortimail-vm-64bit-250gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
Deserves	😡 fortimail-vm-64bit-1024gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
	👧 fortimail-vm-64bit-2048gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
🛗 Documentos 🖈	👧 fortimail-vm-64bit-4096gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
📰 Imágenes 🛛 🖈	👧 fortimail-vm-64bit-8192gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
Aplicando Licen	👧 fortimail-vm-64bit-12288gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
Instalando el VIV	🐼 fortimail-vm-64bit-24576gb-hw7.ovf	28/02/2017 07:50	Open Virtualizatio	61 KB
OneDrive				
Este equipo				
CANM (G:)				
CANM (G:)				

Fig. 4.2.9 Elección del archivo necesario del Fortimail.

En la Fig. 4.2.10, observamos las especificaciones del requerimiento del Fortimail.

Source OVF Template Details End User License Agreement Name and Location Storage Disk Format Ready to Complete Publisher: No certificate present Download size: 151.3 MB Size on disk: 250.6 GB (thick provisioned) Description:	Source OVF Template Details End User License Agreement Storage Disk Format Ready to Complete Publisher: No certificate present Download size: 151.3 MB Size on disk: 164.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:	Deploy OVF Template OVF Template Details Verify OVF template details.				-	
OV Template Details Product: FortiMail-VM Forti User Licens Agreement. Version: Storage Version: Dick Format Vendor: Ready to Complete: Publisher: No certificate present. Download size: 151.3 MB Size on disk: 164.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:	OVF Template Details Product: FortiMail-VM Name and Location Version: Storage Version: Disk Format Vendor: Ready to Complete: Vendor: Download size: 151.3 MB Size on disk: 164.0 MB (thin provisioned) Size on disk: 164.0 MB (thin provisioned) Description: Version:	Source					
Version: Storage Version: Disk Format Vendor: Ready to Complete Publisher: No certificate present Download size: 151.3 MB Size on disk: 164.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:	Version: Storage Vendor: Publisher: No certificate present. Download size: 151.3 MB Size on disk: 164.0 MB (thin provisioned) 250.6 GB (thick provisioned)	OVF Template Details End User License Agreement	Product:	FortiMail-VM			
User Format Vendor: Ready to Complete: Publisher: No certificate present Download size: 151.3 MB Size on disk: 164.0 M8 (thin provisioned) 250.6 G8 (thick provisioned) Description:	User Format Vendor: Ready to Complete Publisher: No certificate present Download size: 151.3 MB Size on disk: 154.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:	Storage	Version:				
Publisher: No certificate present Download size: 151.3 MB Size on disk: 164.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:	Publisher: No certificate present Download size: 151.3 MB Size on disk: 164.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:	Disk Format Ready to Complete	Vendor:				
Download size: 151.3 MB Size on disk: 154.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:	Download size: 151.3 MB Size on disk: 164.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:		Publisher:	No certificate present			
Size on disk: 154.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:	Size on disk: 154.0 MB (thin provisioned) 250.6 GB (thick provisioned) Description:		Download size:	151.3 MB			
Description:	Description:		Size on disk:	164.0 MB (thin provisioned) 250.6 GB (thick provisioned)			
			Description:				
						21	
1	Ť	Help			< Back	Next >	Canc

Fig. 4.2.10 Especificaciones del requerimiento del Fortimail.

En la Fig. 4.2.11, evidenciamos la aceptación de la licencia.



Fig. 4.2.11 Aceptación de la licencia.

En la Fig. 4.2.12, presentamos la configuracion del nombre de la maquina virtual.

🕝 Deploy OVF Template	<u>10</u>	20		×
Name and Location				
Specify a name and location for the deployed template				
Source Name: OVE Template Details]
End User License Agreement The name can contain up to 80 characters and it must be	unique within the inventory fr	older		_
Name and Location Storage	andae want are inventory it	Juci .		
Disk Format Ready to Complete				
New y to complete				
	1			
	J.			
Heln	< Back Now + S	1	Com	cel
	V DOLK NEXT >		Can	

Fig. 4.2.12 Configuración del nombre de la máquina virtual.

En la Fig. 4.2.13, enseñamos el establecimiento del almacenamiento de la maquina virtual.

🕝 Deploy OVF Template							<u> </u>		×
Storage Where do you want to stor	e the vi	rtual machine files?							
Source	Select	a destination stora	ge for the virtu	al machine files:					
OVF Template Details End User License Agreement	Nam	ie 💊	Drive Type	Capacity	Provisioned	Free	Туре	Thin	Prov
Name and Location		Almacenamien	Non-SSD	7.27 TB	3.61 TB	4.67 TB	VMFS5	Supp	orte
Storage Disk Format Ready to Complete		HDD_Solid_SO	SSD	439.50 GB	282.59 GB	388.72 GB	VMFS5	Supp	orte
	< □ (Disable Storage DRS	5 for this virtual	machine					>
	Selec	t a datastore:							
	Nam	le	Drive Type	Capacity P	rovisioned	Free	Туре	Thin P	rovi
	¢					ſ			>
Help					< Back	Next	>	Cancel	

Fig. 4.2.13 Estableciendo el almacenamiento de la máquina virtual.

En la Fig. 4.2.14, observamos la creacion del disco virtual VMDK, reservando el espacio definido.

<u>urce</u> /F Template Details	When you click Finish, the dep	loyment task will be started.
d User License Agreeme	nt peployment settings:	
me and Location	OVF file:	C:\Users\Lenovo\Documents\Fortimail\Imagenes\fortima
prage	Download size:	151.3 MB
<u>ix Format</u>	Size on disk:	250.6 GB
eady to complete	Name:	FortiMail-VM-Sen-ON
	Host/Cluster:	localhost.
	Datastore:	Almacenamiento Interno (Arreglo)
	Disk provisioning:	Thick Provision Lazy Zeroed
	Network Mapping:	"Bridged" to "VM Network"

Fig. 4.2.14 Creación del disco virtual VMDK, reservando el espacio definido.

En la Fig. 4.2.15, mostramos el tipo de almacenamiento para el Fortimail.

Deploy OVF Template Disk Format In which format do you war	nt to store the virtual disks?		5		×
Source OVF Template Details End User License Acreement Name and Location Storage Disk Format Ready to Complete	Datastore: Available space (GB): Thick Provision Lazy Zer C Thick Provision Eager Ze C Thin Provision	Almacenamiento Interno (Arr 4779.4 oed oroed			
Help		< Back	Next >	Car	ncel

Fig. 4.2.15 Tipo de Almacenamiento para el Fortimail.

Como se ve en la Fig. 4.2.16, indicamos el porcentaje del despliegue de la maquina virtual del Fortimail.

7 - vSphere Client	
File Edit View Inventory Adminis	tration Plug-ins Help
D D one ball bue	ntery 👂 🎒 Inventary
	0000
Portugation NC Demonstra NC	Image: Image
<>	
Recent Tasks	
Name	Status Details Initiated by Requested Start Ti
Deproy OVP template	Completed Completed Completed Completed Completed

Fig. 4.2.16 Porcentaje del despliegue de la máquina virtual del Fortimail.

4.3. Administracion de Fortimail.

En la Fig. 4.3.1, presentamos la finalización del despliegue de la máquina virtual.



Fig. 4.3.1 Finalización del despliegue de la máquina virtual.

Por defecto el Fortimail tiene una IP que es la: "192.168.1.99" pero como esa IP no nos servira ya que el equipo es virtual, en cuando lo encendemos le cambiaremos la IP a la que necesitamos desde la consola del Esxi.

Por el tipo de implementacion y la arquitectura requerida, la interfaz que configuraremos aca recibira todo, desde la administracion hasta el envio y recepcion de correo, analisis, conexión a internet etc. [4]

En la Fig. 4.3.2, observamos el arranque de la maquina virtual del Fortimail.



Fig. 4.3.2 Arranque de la máquina virtual del Fortimail.

Luego nos autenticamos, en este punto "<u>el login es: admin y el password: no es</u> <u>nada</u>" como se ve en la Fig. 4.3.3.

98.88-15:39:21 ** new v+ image disk
88.88-15:39:25 *** Haiting for var
08.08-15:39:31 *** waiting for var
08.08-15:39:36 ** partitioning new vm system
enabling LVM
partitioning devices
creating volume group
creating logical devices
starting LVM subsystem
LVM created
08.08-15:39:52 ** formatting system
formatting partition /dev/vga/vga2 as reiserfs
successful
formatting partition /dev/vga/vga3 as reiserfs
successful
08.08-15:40:08 *** waiting for var
08.08-15:40:14 *** waiting for var
Initialize Database
Initialize Configuration
08.08-08:40:29 Parsing default configuration file!
FEUM8080808080 login:
FEUM888888888888888888 login: _

Fig. 4.3.3 Autenticación del Fortimail.





Fig. 4.3.4 Ingresando las Credenciales por defecto.

Luego ejecutamos el siguiente comando:

"<u>config system interface</u> <u>edit port 1</u> set ip x.x.x.x x.x.x.x"



FEVM808080808080 (interface) # set inter Parsing error at 'set'. err=1
FEUM808080808080 (interface) # edit add/edit atable value delete atable value purge clear all table value remame remame atable entry get get dynamic and system information show show configuration end and save last config FEUM80808080808080808080808080800 (interface) # end
FEUMARABARARAR = FEUMARABARARARAR = FEUMARABARARARAR =
FEUM00000000000 # config system interface FEUM000000000000 (interface) # edit port1 FEUM000000000000 (port1) # FEUM00000000000 (port1) # FEUM00000000000 (port1) # Set ip 0.0.0.0 0.0.0.0

Fig. 4.3.5 Estableciendo el direccionamiento de IP privada de nuestra Empresa.

Nota: El Fortimail virtual trae hasta 5 interfaces, la interfaz por defecto es la 1, por eso la configuramos aca, pero igual se puede configurar una interfaz de cada funcion incluso solo de administracion.

Luego de poner la IP, ponemos en el buscador la IP que configuramos con la siguiente direccion: <u>https://ip_fortimail/admin.</u>

Ahí tendremos que darle una excepcion al navegador por el certificado.

Nota: Para quitar ese mensaje podemos exportar el certificado del Fortimail e instalarlo en la PC desde donde se tenga que acceder.

En la Fig. 4.3.6, observamos como entramos en la interfaz gráfica desde el Navegador.



Fig. 4.3.6 Entrando a la Interfaz Gráfica desde el Navegador.

Universidad Nacional de Ingeniería Facultad de Electrotécnica y Computación

En la Fig. 4.3.7, exhibimos la confirmacion de la excepción de seguridad.

· End a sunda da al	anne stare identifier Finder attentio	
Esta a punto de a	terar como identifica Firerox este sitio.	
Los bancos, tiend	las y otros sitios públicos legítimos no le p	pedirán hacer esto.
Servidor		
Dirección:	admin	Qbtener certificado
Estado del certificado		
Este sitio intenta identifica	arse a sí mismo con información no válida	yer
Citio errineo		
Sitio erróneo		
Sitio erróneo El certificado pertenece a	un sitio diferente, lo que podría significar	que alquien estă intentando
Sitio erróneo El certificado pertenece a hacer pasar por este sitio.	un sitio diferente, lo que podría significar	que alquien estă intentando
Sitio erróneo El certificado pertenece a hacer pasar por este sitio. Identidad desconocida	un sitio diferente, lo que podría significar	que alquien estă intentando
Sitio erróneo El certificado pertenece a hacer pasar por este sitio. Identidad desconocida No se confía en el certific confiable usando una firm	un sitio diferente, lo que podría significar ado porque no ha sido verificado como en na segura.	que alquien está intentando nitido por una autoridad
Sitio erróneo El certificado pertenece a hacer pasar por este sitio. Identidad desconocida No se confía en el certific confiable usando una fim Guardar esta excepció	un sitio diferente, lo que podría significar ado porque no ha sido verificado como en na segura. In de manera permanente	que alquien estă intentando nitido por una autoridad

Fig. 4.3.7 Confirmando la excepción de seguridad.

Luego nos autenticamos, recordemos que todavía no tenemos configurado password, así que ese campo lo dejamos en blanco y accedemos a la herramienta.

En la Fig. 4.3.8, observamos el ingreso de las credenciales de administrador.



Fig. 4.3.8 Ingresando las credenciales de administrador en la consola del Fortimail.

C FortiMail	× \+										- o
🗲 🛛 💋 🗞 https://	1/admin/FEAdmin.html#SysStatusModulesCollection				C 9.8	Úscar				1	1 🗄 🕴 🐨
FortiMail VM	00					Basic Mode 3	2)	2		FORTIDE
Honitor	Status Hal Statistics Ses	sions Console									
System Status	Add Content*										
Mail Queue	Contain Information		000	Statution Mattern							00000
Quarantine	System and matching	FT: 84000000000	908	Statistics History		1					60086
Sender Reputation	Up time:	0 dav(s) 5 hour(s) 58 minute(s) 37 second(s)		Email History by Day	A.	L	Bar Cha	r 1	Castr	er Name	
Endpoint Reputation	System time:	Tue, 08 Aug 2017 14:37:49 PDT		100							8
Archive	Reboot time:	Tue, 08 Aug 2017 08:39:12 PDT		11 11 1							11 11 11 1
Log	Firmware version:	v5.3,build634,170228 (5.3.9 GA) [Update]		1 - 11 - 11 - 11 - 11 - 11 - 11 - 11 -							15 16 18
Report	Operation mode:	Server 👻		100 100							
Maintenance	Current administrator: HA mode:	admin / 1 in total [Details] Configured: off. Effective: off		17 AV 18							11 11 1
System	Log disk:	Capacity 49 GB, Used 33 MB (0.07%), Free 49 GB					-	. /			6 11 11
Encryption	Małbox disk: Email throushout:	Capacity 197 GB, Used 249 MB (0.13%) , Free 197 GB 0 messages per minute (last 1 minutes)		1 II I)			11 11 1
Mail Settings				10 10		Fate church est		debe ter	art-alized		18 AV 18
lices	License Information		888	10 10 1			Activer Adol	n Fish	See See See		
	Ant/Virus:	1.00001 (Unreachable)	0	5 A. M.			ncar actuals				10 10 10
Policy	AntiVirus definition:	1.00001 (Updated Never) Update] Trial (Evokas Universited)	0	11 11 1							
Profile	AntiSpam definition:	1.00001 (Updated Never)		F 10 10							11 11 11
AntiSpam	VH:	Trial license(Expire in 14 days 18 hours 5 mins) [Update]	0	1.10							
AntiVirus	FortiSandbox	Diabled [Configure]	8	17 AN 1							11 11 1
Email Archiving			-	100 100							1 1 1
Log and Report	System Resource		6008	100 AUR -	ANY - ANY						r - 10 - 10 - 1
Log and Report	CPU usage:	0%		Statistics Summir	ŝ						0000
	Memory usage:	14%		Managa directions			3				0086
	Lon dik uson:	0%		HERed ALL		100	8				
	and an endage			Messages	TotalTh	is Year This P	HonthThis	WeekTo	odayThis	HourThis	Minute
	Mail disk usage:	0%		Not Spam Classified BySi	ubtotal 0%	0%	0%	0%	0%	0%	0%
	System load:	3%		Soam Cassified By Si	o latotal	0	0	0	0	0	0
				and the second s	0%	0%	0%	0%	0%	0%	0.9%

En la Fig. 4.3.9, presentamos el acceso a la interfaz gráfica del Fortimail.

Fig. 4.3.9 Acceso a la interfaz Gráfica del Fortimail.

4.4. Aplicando licencia.

Los primeros 15 dias despues de instalado el equipo, tendremos una licencia "demo" puesto que no podremos actualizar las firmas, ni acceder a la red de Fortimail en la nube, otra caracteristica desactivada es el Sandbox.

Previamente tuvimos que haber creado una cuenta en la pagina de Fortinet (Cualquiera puede crear cuenta) y registrar el producto para obtener la licecnia.

Para actualizar seguimos la ruta: Monitor \rightarrow System Status \rightarrow Status \rightarrow VM \rightarrow Update

En la Fig. 4.4.1, observamos la interaccion con la plataforma del Fortimail.



Fig. 4.4.1 Interacción con la consola del Fortimail.

En la Fig. 4.4.2, enseñamos la eleccion del archivo de licencia:

- (VM License File				3
	Seleccionar ar	chivo	Ningún archivo seleccionad	o ·	
	Upload Car	ncel			
7-06-27					

Fig. 4.4.2 Elección del Archivo de Licencia para la consola.

En la Fig. 4.4.3, mostramos la busqueda del archivo en nuestro ordenador.

Abrir					×
← → → ↑ 📙 > Este equipo → Documentos → Fortimail → Licenci	as v	õ	Buscar en Licencia	s	P
Organizar 👻 Nueva carpeta				•	?
Acceso rápido Escritorio Descargas Documentos Imágenes Aplicando Licen ConeDrive Este equipo CANM (G:) CRIS HDD (E:)	Fecha de modifica. 08/08/2017 08:32 a.	T	ipo .rchivo WinRAR Z	Tamaño 77 KB	
Nombre de archivo: FML-VM02_6417231.zip		~	Todos los archivo Abrir	s Cancelar	×

Fig. 4.4.3 Búsqueda del archivo en nuestro ordenador.

En la Fig. 4.4.4, indicamos la subida del archivo de licencia a la consola.

	VM License File				×
	Seleccionar archivo	FML-VM02_6417231.zip	-		
017.05.07	Upload Cancel				
ed)	1			615	
17-06-27	4			30-	

Fig. 4.4.4 Subida del archivo de licencia a la consola.

En la Fig. 4.4.5, presentamos la confirmacion de la actualizacion por medio del archivo de licencia.



Fig. 4.4.5 Confirmación de la actualización por medio del archivo de licencia.

4.5. Configuración Inicial.

Antes de configurar politica, tenemos que añadir el dominio a proteger, para esto se deben de tener los siguientes datos:

- IP de donde viene el correo (No precisamente el servidor de correo).
- IP del servidor de correo.
- Dominio.
- Puerto de correo.
- Protocolo de correo.

Cabe destecar que esto se puede hacer no precisamente de este Wizard pero es preferible hacerlo desde aca ya que para configurar las opciones que se necesitan hay que navegar por diferentes lugares del menu del Fortimail y aca estan reunidas y lineales.

En la Fig. 4.5.1, observamos la seleccion del Wizard desde la parte superior derecha:

C FortiMail	× +			- 0 ×
🗲 🛈 🛍 🗞 https://	/admin/FEAdmin.html#SysStatusModulesCollection	C Q. Buscar	0	☆ 🖻 🖡 👘 😇 🗏
FortiMail VI	MOO	Basic Mode >> 0	Waters	
Monitor	Status Mail Statistics Sessions Console		C	
Maintenance	Add Content •			
System	System Information	Statistics History		

Fig. 4.5.1 Seleccionando el Wizard de la consola del Fortimail.

Al ejecutar el Wizard nos da una advertencia que si lo ejecutamos borrara las configuraciones que tenga configuradas en esos momentos, como es la primera vez no le prestamos atencion pero hay que considerar que cada vez que corremos el Wizard borrara lo que tiene configurado, no se tiene que hacer en produccion bajo ninguna circunstancia y se tiene que tener respaldo de la configuracion.

En la Fig. 4.5.2, presentamos la confirmacion del acceso al Wizard del Fortimail.



Fig. 4.5.2 Confirmando el acceso al Wizard del Fortimail.

Quick Start Wizard:	1/7			×
-Edit Administrato	or Password			
Change password				
New password:	•••••			
Confirm password:	•••••			
		7		
				Nave
DOCK				Next
				\sim

En la Fig. 4.5.3, mostramos el establecimiento de la nueva contraseña de acceso.

Fig. 4.5.3 Estableciendo la nueva contraseña de acceso.

Luego reafirmamos la configuracion de Red, y la zona horaria del equipo, esto tiene que estar bien configurado para que la actualizacion de las firmas sea correcta.

En la Fig. 4.5.4, enseñamos la confirmacion de las configuraciones necesarias para el upgrade.

ck Start Wizard: 2/7
etwork Settings
ort1 IP: / 24
rimary DNS:
econdary DNS:
efault gateway:
ime Settings
ime zone: (<u>GMT-6:00)Central America</u>
) Set time Date: 08/08/17 🖪 Hour: 16:0 Y Minute: 52 Y Second: 0 Y
Avantatically synchronize system time using NTP server
NT Server name/IP: pool.ntp.org
× .
ck Rep

Fig. 4.5.4 Confirmando las configuraciones necesarias para el upgrade.

Luego se tiene que configurar el nombre del equipo, el nombre de dominio y los puertos de correo.

Como se ve en la Fig. 4.5.5, añadimos los puertos de nuestro servidor de correo.

Quick Start Wizard: 3/7	x
– Local Host Settings	
Host name:	AntispamFortimal
Local domain name:	
POP3 server port number:	110
SMTP server port number:	25
SMTP over SSL/TLS	
SMTP server port number:	465
Back	Next

Fig. 4.5.5 Añadiendo los puertos de nuestro servidor de correo.

A continuacion mostramos en la Fig. 4.5.6, añadimos el dominio y el gateway de la IP privada.

Quick Start Wizard: 4/7 Domain Configuration	×
Ell New Se Edit B Delete Domain Name Use MX Record - SMTP Server	
Back	Next

Fig. 4.5.6 Añadiendo nuestro dominio y el Gateway de la IP Privada.

Luego escogemos el nivel de Antispam y Antivirus del Fortimail, esto podemos modificarlo más adelante.

En la Fig. 4.5.7, mostramos la configuración del Antispam.

FortiMail		×
Do	main Settings	
Domain name:		
Use MX record:		
SMTP server:	Port: 25	
Create Cancel		
↑ <i>1</i>		

Fig. 4.5.7 Configuración inicial del Antispam.

En la Fig. 4.5.8, observamos la elección del nivel de escaneo del Antispam.



Fig. 4.5.8 Elección del nivel de Escaneo del Antispam.

Como se ve en la Fig. 4.5.9, creamos la política principal de acceso, en la que protegemos el dominio, de cualquier spoofing:

abled	0.0.0.0		/ 0
Sender pattern:	User Defined	~	
	*		Regular expression
ecipient pattern:	User Defined	~	
	*		Regular expression
ender IP/netmask:			
everse DNS pattern:	*		Regular expression
uthentication status:	Any	~	
Action:	Reject	~	

Fig. 4.5.9 Creación de política principal de Acceso.

En la Fig. 4.5.10, enseñamos el establecimiento del dominio del antispam e ingresamos la IP de donde nos vendrán los correos, igualmente establecemos el dominio del cual vamos a hacer relay y hacia dónde va el correo:

webled.		1 22
habled		/ 32
ender pattern:	User Defined	
		Regular expression
cipient pattern:	User Defined 🗸	
		Regular expression
ender IP/netmask:		
everse DNS pattern:	*	Regular expression
uthentication status:	Any	
ction:	Not Authenticated	
Second Sec. (Second	Authenticated	•
omments:	Any	

Fig. 4.5.10 Estableciendo el Dominio al Antispam.

En la Fig. 4.5.11, presentamos el establecimiento de la política de acceso y la acción a tomar de Relay. (Cabe destacar que si el correo es en saliente el estado de la autenticación es siempre "Authenticated" ya que si no es así, es que tenemos alguna PC Botnet o algún spoofing dentro del dominio.

babled			1	1 22
				1 32
Sender pattern:	User Defined		~	
		DOMINIO		Regular expression
Recipient pattern:	User Defined			
	*			Regular expression
Sender IP/netmask:				
Reverse DNS pattern:	*		Regular expression	
Authentication status:	Authenticated			
Action:	Reject		~	\leftarrow
	Discard			
Comments:	Reject			
	Relay		\supset	
	Safe			
Create Cancel	Safe & Relay			

Fig. 4.5.11 Estableciendo en la política de acceso y la acción a tomar de Relay.

La acción a tomar cuando encontremos esta comunicación debería ser "relay" si cumple con lo dispuesto antes, cabe destacar que podemos rechazar el correo en este caso, así mismo permitir otras direcciones especificas desde la cuales necesitemos enviar correos.

En la Fig. 4.5.12, observamos la finalización de la configuración del wizard.



Fig. 4.5.12 Finalizando la configuración del Wizard.

En la Fig. 4.5.13, mostramos el resumen general de la regla de la política de acceso.

Quick Start Wizard: 7/7	×
Network Settings	^
Port1 IP: Primary DNS: Secondary DNS: Default gateway:	
Time Settings	<u> </u>
Time zone: (GMT-6:00)Central America Set time: 08/08/2017 16:52:0	
Local Host Settings	
Host name: AntispamFortimal Local domain name:	
POP3 server port number: 110 SMTP server port number: 25	
Domain Configuration	
Domain Name Use MX Record SMTP Server	OK Cancel
Back	Next

Fig. 4.5.13 Resumen general de la regla de la política de acceso.

Al terminar nos dará un resumen de lo que hemos hecho:

Luego el wizard termina y entonces nos redirigirá a la pantalla de autenticación donde ingresaremos con la nueva contraseña configurada:

En la Fig. 4.5.14, presentamos la pantalla de autenticación del Fortimail con el cambio realizado.

Fig. 4.5.14 Regresando con las nuevas credenciales y políticas establecida.

4.6. Creando Perfiles del Fortimail.

Antes de las políticas debemos configurar los perfiles que se le aplicaran a las políticas, las políticas en general se componen de perfiles que se aplican a origendestino sin importar si las aplicamos por IP, dominio, usuario.

Los perfiles que podemos configurar vienen desde controlar detalles de las sesiones como los tamaños de correos, como grupos de IP y de correos para permisos especiales, en este documento solo mencionaremos los que se configuraron para Sencom.

Para configurar los perfiles, iremos a la siguiente ruta: Menú \rightarrow Profile:

En esta Fig. 4.6.1, observamos la configuración de los perfiles.



Fig. 4.6.1 Configuración de los perfiles.

Acá podemos elegir entre varios perfiles a configurar, los más importantes y los que ocuparemos por ahora serian:

- 1. Session
- 2. Antispam
- 3. Antivirus
- 4. Content
- 5. Notification

4.7. Perfil Session.

Este perfil se aplica a nivel de IP antes de que la conexión SMTP, esto quiere decir que aplica las políticas antes de podamos ver las cuentas de correo, dominio, asunto, etc. Lo que podremos ver en el log solo es la dirección IP y el nombre del servidor de correo de donde viene.

Por esta razón en esta parte solo configuramos el tamaño del correo, dependiendo de las necesidades de los usuarios y las políticas de la empresa, así que creamos un perfil nuevo:
Ponemos un nombre al perfil y configuramos el tamaño del correo en la siguiente dirección: *Profile → Session → New → SMTP Limits → Cap message size (KB) at*, al terminar damos clic en *Create*

En la siguiente Fig. 4.7.1, mostramos el establecimiento del perfil de sesión.

FortiMail VM00 FortiMail	
🚯 Dashboard	Session
Monitor >	
System >	
🛓 Domain & User 💦 📏	C « < 1 / 1 > » Records per page: 50 •
Policy >	Profile name
Profile V	Inbound_Session
Session	Outbound_Session

Fig. 4.7.1 Estableciendo el perfil de sesión.

Como se ve a continuación en la Fig. 4.7.2, la creación de la política de sesión.

Session Profile	
Profile name: Session_Domain	
Connection Settings	
Sender Reputation	
Endpoint Reputation	
Sender Validation	
Session Settings	
Unauthenticated Session Settings	
SMTP Limits	
Restrict number of EHLO/HELOs per session to:	3
Restrict number of email per session to:	10
Restrict number of recipients per email to:	500
Cap message size (KB) at:	10240
Cap header size (KB) at:	32
Maximum number of NOOPs allowed for each connection:	10
Maximum number of RSETs allowed for each connection:	20
Error Handling	
	Create Cancel

Fig. 4.7.2 Creación de la política de sesión.

Universidad Nacional de Ingeniería Facultad de Electrotécnica y Computación

En la Fig. 4.7.3, exponemos la confirmación de la política de sesión.

FortiMail VM00	FortiMail	
🚯 Dashboard		Session
C Monitor	>	→ New Clone Cone
🌣 System	>	
占 Domain & User	>	2 ≪ < 1 / 1 > ≫ Records per page: 50 ▼
Policy	>	Profile name
Profile	~	Inbound_Session
Session		Outbound Session
AntiSpam	(Session_Domain

Fig. 4.7.3 Confirmación de la política de sesión.

4.8. Perfil Antispam.

Este perfil es el que marca cómo será la inspección SMTP de los correos, esto puede ser de manera entrante y saliente.

En la Fig. 4.8.1, observamos el panel del antispam ya con la licencia.

FortiMail VM02 F	ortiMa					(0	23	SOG	
n Dashboard		Status Mail :	Statistics Session Console			+Manage Widget	(Res	et Wid	get
 Monitor System Domain & User Policy Profile Session Antt/Vius Content Resource Authentication LDAP Dictionary Security IP Pool Group Notification 	>	System Informa Serial number: Up time: System time: Reboot time: Firmware version: System configuratio Operation mode: Current administrat HA mode: Log disic Enail throughput: License Informa AntiVirus: AV definition: AV definition:	tion FUN000000104634 73 dary(s) 13 hour(s) 25 minute(s) 7 second(s) Wesk May 9, 2018 08:12:59 CST Sut, Feb 24, 2018 18:47:52 CST Conformation (Restorme) Suture Suture Conformation (Restorme) Conformation (Restorme) Usersed (Explicit Action (Restorme) Usersed (Explicit Action (Restorme) Usersed (Explicit Action (Restorme) Usersed (Explicit Action (Restorme) Version 50:00134 (Last update attempt: 2018-05-09) Usersion 50:00134 (Last update attempt: 2018-05-09)	$\mathcal{C} = \mathbf{x}$ resper minute $\mathcal{C} = \mathbf{x}$	Statistics History (By Day)	C / O = Newskitter (10.4%) 21%) Not Span (4 Not Span (4 0 0 0 0 0 0 0 0 0 0 0 0 0	ad \$ 2.78%)	-	×	
 Security Encryption Email Archiving Log & Report 	> > >	Virus outbreak: AntiSpam: AS definition: VM: FortiSandbox: FortiCloud:	Expired Licensed (2018-07-19) Version 7.00387 (Last update attempt: 2018-05-09) Registered [Bodatas_] Cloud (Licensed) [Configures_] Activated (infraestructura)[iniser.com.un)] [Launch Pertal_] [Log Out_]	0000	Not Sparm (24.0%) Sparm (76.0%	6) Vizus (0%)				
Q										

Fig. 4.8.1 Panel del Antispam.

En la Fig. 4.8.2, presentamos la configuración del perfil del antispam.



Fig. 4.8.2 Configuración del perfil de Antispam.

Creando los perfiles del Antispam, damos click en new y luego configuramos el perfil de entrada y salida.

Como se ve en la Fig. 4.8.3, creamos el perfil del antispam en la entrada.

omain	Sustam			
Drofile name:	Incoming Anticoam			
Default action:	Incoming Antispam	+ New	PS Edit	
Deraurt action.	incoming_Anospain	TIVEWas	E2 CUILia	
Scan Configu	urations			
C Fort	iGuard	Action:	Incoming_Antispam	*
C Gre	ylist			
SPF	check	Action:	Default	-
O DM	ARC check	Action:	Default	
C Beh	avior analysis	Action:	Incoming_Antispam	-
C Hea	der analysis	Action:	Incoming_Antispam	-
🖸 💽 Heu	ristic	Action:	Incoming_Antispam	
C SUR	RBL [Configuration]	Action:	Default	Ψ.
O DN	SBL [Configuration]	Action:	Default	-
C Ban	ned word [Configuration]	Action:	Default	•
C Safe	elist word [Configuration]			
Dict	ionary	Action:	Default	•
C O Imag	ge spam	Action:	Default	•
C O Baye	isian	Action:	Default	
C Sus	picious newsletter	Action:	Incoming_Antispam	-
Nev	vsletter	Action:	Incoming_Antispam	
Scan Option	5			
Max messa	ge size to scan: 600 🔄 KB (0 means no limi	its}		
Bypass	scan on SMTP authentication			
C Scan Pl	DF attachment			
Apply d	efault action without scan upon policy match			

Fig. 4.8.3 Perfil del Antispam en la entrada.

Universidad Nacional de Ingeniería Facultad de Electrotécnica y Computación

A continuación en la siguiente Fig. 4.8.4, observamos el perfil de salida del Antispam.

AntiSpam Profile					
Domain: Profile name: Default action:	System Antispam_Outgoing Outgoing	+ New	Edit		
Scan Configu	rations				
🗄 💽 Forti	Guard	Action:	Outgoing •]	
Grey	ylist				
SPF	check	Action:	Default]	
	ARC check	Action:	Default]	
Beha	avior analysis	Action:	Outgoing 👻]	
Head	der analysis	Action:	Outgoing -]	
🗄 💽 Heur	istic	Action:	Outgoing 🗸]	
SUR	BL [Configuration]	Action:	Default]	
	BL [Configuration]	Action:	Default]	
Banı Banı	ned word [Configuration]	Action:	Default]	
Safe	list word [Configuration]				
🗄 🕥 Dicti	onary	Action:	Default]	
🗄 🕥 Imag	e spam	Action:	Default]	
🗄 🕥 Baye	sian	Action:	Default]	
Susp	picious newsletter	Action:	Default]	
New	vsletter	Action:	Default]	
				ОК	Cancel

Fig. 4.8.4 Perfil de Salida del Antispam.

Como se ve en la Fig. 4.8.5, creación de las políticas tanto entrante como saliente.

FortiMail VM02 For	tiMai	1									0	53	SOC-
Dashboard		IP Policy											
C Monitor	>	+ New	56	Edit 🛱 Delete	Move -								
System	>		-			7							
🚨 Domain & User	>		1	1 > » Reco	ords per page: 50 💌	•					5	selected	:1/4
Policy	~	Enabled	ID	Source	Destination	Session	AntiSpam	AntiVirus	Content	IP Pool	Authentication	Excl	u
Access Control			4	0.0.0/0	0.0.0/0	Inbound			Content Incomin			0	^
IP Policy			3	0.0.0/0	0.0.0/0	Outgoing	Antispam Outgoi	AV Reject	Content Outgoin			0	
Recipient Policy			1	0.0.0/0	0.0.0/0	Inbound Session						0	
E Profile	>		2	::/0	::/0	Inbound Session						0	
Security	>												
Encryption	>												
 Email Archiving 	>												
🚹 Log & Report	>												



Al igual que el perfil del AntiSpam el perfil de contenido examina tambien el protocolo SMTP del correos para los distinstos archivos que son enviados.

En la Fig. 4.8.6, observamos el perfil de contenido de entrada.

Profile	name:	Content Incoming			
Action:	[Content_Incoming.	+ New	Edit	
Att	achment S	Scan Rules			
	+ New	🚺 Edit 🎁 Delete 🔺 Move 🔹	-		
	Enabled	File Filter	Operator	Action	
		executable_windows	Is	Default	^
		video	Is	Default	
		audio	Is	Default	
		image	Is	Default	
		archive	Is	Default	
		encrypted	Is	Default	
					~

Fig. 4.8.6 Perfil de Contenido de Entrada.

En la Fig. 4.8.7, enseñamos la continuación del perfil de contenido.

O Detect fragmented email
O Detect password protected Office document
Attempt to decrypt PDF document
O Detect embedded component
MS Office
Visual Basic for Application
C MS Visio
Open Office
PDF
Defer delivery of message on policy match
Defer delivery of message larger than 0 Image: KB
Maximum number of attachment 10
Maximum size message 10240 KB
Action:Default
Adult image analysis ()
Action:Default

Fig. 4.8.7 Continuación del Perfil de contenido.

Universidad Nacional de Ingeniería Facultad de Electrotécnica y Computación

Content Disarm and Reconstruction	
Action:Default	
HTML content Convert HTML to text	•
Remove URIs	
MS Office ()	
PDF 1	
Archive Handling	
Check archive content	
Detect on failure to decompress	
 Detect password protected archive 	
Attempt to decrypt archive	
Max level of compression	
File Password Decryption Options	
Words in email content	
Number of words to try: 5	
Built-in password list	
User-defined password list	

Е

Fig. 4.8.8 Finalización del Perfil de Contenido.

Bien al ser una interfaz virtual es necesario establecerlo con el dirección privado asignado.

Como se ve en la Fig. 4.8.9, configuramos el antispam.

FortiMail VM02 Forti	Mail						@ [] s	SOC.
Bashboard	Interface Link Monito	r Routing DNS	DDNS Port Forwarding	FortiGate Traffic Capture				
Monitor) 0 + New. [E Edit.	🖞 Delete					1	Fotal:
Network	Name	Type	IP/Netmask	iPvő/Netmask	Access	Status		
Administrator Configuration Mail Settings	port1	Physical		±/0	HTTPS_PING_SSH	0	•	

Fig. 4.8.9 Configuración del Antispam.

Ahora configuramos la lista negras son todos aquellos nombres de dominios, diferentes páginas web que envíen correos no deseado y las listas blancas son todos aquellos dominios que necesitamos acceso por correo.

A continuación veremos en la siguiente Fig. 4.8.10, configuramos las lista negra o blanca.

FortiMail VM02	FortiMai	I			
🚯 Dashboard		System	Domain	Personal	Blocklist Action
民 Monitor	>	Block List	Safelist		
🔅 System	>	DIOCKEISE	Jure Lise		
🛓 Domain & User	>				
📕 Policy	>				
Profile	>				
Security	~				
Quarantine					
Block/Safe List					

Fig. 4.8.10 Configuración de lista negra o blanca.

En la Fig. 4.8.11, observamos la lista blanca.

List Se	List Setting of System (Safe List)						
Safe L	Safe List: Email received from these addresses / domains / IPs will always be accepted						
C	C + New Im Delete Total: 41 / 4096						
1	*@agrisal.com						
2	*@albanisa.com.ni						
3	*@asamblea.gob.ni						
4	*@asamblea.gobni*						
5	*@bolsanic.com						
6	*@capesa.com.ni						
7	*@caseware.com						
8	*@consinter.com						
9	*@email.dropbox.com						
10	*@enabas.gob.ni						
11	*@enatrel.gob.ni						
12	*@getechnologiesmx.com						
13	*@invercasacorreduria.com						
14	*@latinoins.com						
15	*@list.ibw.com.ni v						
Back	Restore Close						

Fig. 4.8.11 Lista Blanca.

En la Fig. 4.8.12, mostramos la lista Negra.

List Se	List Setting of System (Block List)						
Block	Block List: Email received from these addresses / domains / IPs will be discarded						
C	€ + New						
46	*@certesnetworks.com	^					
47	*@clear.net.nz						
48	*@clientesglobal.com						
49	*@cnvl11.info*						
50	*@cocoonhyaena.com						
51	*@confiancabr.com.br						
52	*@connect.com						
53	*@correos24.net						
54	*@cosekish.info						
55	*@cox.net						
56	*@ctezopen.com						
57	*@d210-197.icpnet.pl						
58	*@daum.net						
59	*@davdrkr.com						
60	*@densitionz.website	~					
Back	Restore Close	e					

Fig. 4.8.12 Lista Negra.

4.9. SURBI

SURBL (anteriormente conocido como Spam URI RBL) es una colección de listas URI DNSBL de hosts de Identificador uniforme de recursos (URI), generalmente dominios de sitios web, que aparecen en mensajes no solicitados. SURBL se puede utilizar para buscar cuerpos de mensajes de correo electrónico entrantes para enlaces de carga útil de correo no deseado para ayudar a evaluar si los mensajes no son solicitados.

En esta Fig. 4.9.1, presentamos los sitios web con envíos de correo no deseado.

SU	SURBL Configuration							
	➡ New Im Delete Total: 5							
		SURBL Server Address						
	1	psbl.surriel.com	*					
	2	bl.spamcop.net						
	3	zen.spamhaus.org						
	4	list.dsbl.org						
	5	b.barracudacentral.org						
			-					
		ОК	Cancel					

Fig. 4.9.1 Sitios Web con envíos de correo no deseado.

Capítulo 5

5. DMZ

5.1. Teoría

A como es de saber uno de los objetivos de nuestra monografía es la implementación de una zona DMZ (zona desmilitarizada) en la red de la empresa Sistems Enterprise S.A, primeramente discutiremos algunas preguntas introductorias como lo son:

¿Qué es una DMZ? Y para que nos servirá en nuestra red y en nuestra seguridad.

Una DMZ o zona desmilitarizada básicamente es una zona insegura en nuestra red, a la cual se debe tener acceso desde el internet (WAN) y nuestra zona segura (LAN), pero con la condición de que nuestros equipos en la zona DMZ no tengan acceso a nuestra LAN, por lo cual generalmente se tienen separadas, esto siempre con el objetivo de garantizar la mayor seguridad a nuestra LAN.

Esta zona desmilitarizada nos servirá para poder aislar nuestros servicios publicados o con acceso desde el Internet de nuestra red segura, y así poder evitar la posibilidad de que ataques destinados a estos servicios nos perjudiquen. [5]

En la Fig. 5.1.1 exhibimos el esquema de la zona DMZ.



Fig. 5.1.1 Esquema de la Zona DMZ.

Para poder entender mejor la implementación de nuestra zona DMZ se observaran dos diagramas, uno describirá como se tiene la red anteriormente a la propuesta, y luego como quedo la red después de nuestra implementación.

Nota: los diagramas que serán mostrados serán hechos superficialmente con el propósito del entendimiento de la estructuración de esta zona. [2]

En la Fig. 5.1.2, observamos el esquema antes de la implementación de la zona DMZ.



Diagrama sin zona DMZ.

Fig. 5.1.2 Esquema Antes de la implementación de la Zona DMZ.

"Organizar Y Establecer Nuevas Soluciones de Seguridad en la Red de la Empresa Sistems Enterprise S.A."

Universidad Nacional de Ingeniería Facultad de Electrotécnica y Computación

A como se puede observar la topología de red anterior nos muestra la estructura básica de nuestra red, en donde se ve nuestros watchguard administrando el tráfico proveniente de la LAN, siempre analizado por el IPS en cada una de las conexiones.

A continuación se les mostrara en la Fig. 5.1.3, el diagrama de red de SENCOM, después de la implementación de la zona DMZ.

Diagrama después de la implementación de la Zona DMZ.



A como se puede observar en la nueva topología de red, se utilizó un Fortigate (Fortigate 200D) para la nueva implementación el cual nos estará administrando nuestra zona DMZ.

Fortigate 200D es un next generation firewall (firewall de próxima generación) el cual utiliza procesadores de seguridad especialmente diseñados y servicios de seguridad de inteligencia de amenazas para ofrecer una protección de alto nivel y alto rendimiento, incluido el tráfico encriptado. Fortigate reduce la complejidad con la visibilidad automatizada de las aplicaciones, los usuarios y la red, y proporciona clasificaciones de seguridad para adoptar mejores prácticas en la seguridad.

Debajo de él se observa nuestro web/mail server el cual en este caso lo tenemos ubicado en nuestra zona DMZ. En este caso nuestro servidor de correos es un FORTIMAIL, el cual es el antispam de Fortinet, que nos garantiza una protección especializada y de alta calidad contra amenazas comunes y avanzadas el cual a la vez integra solidas capacidades de protección de datos para evitar la pérdida de estos.

Este Fortimail se encuentra en un ESXi el cual es un ambiente de virtualización que nos permite tener varios hypervisores y una cantidad de interfaces de red disponibles con la facilidad de ser divididas y manejar el tráfico de cada una de ellas por aparte.

Después de haber dejado claro y de describir un poco de los dispositivos de red a utilizar podemos proceder a mostrar el procedimiento seguido para poder crear nuestra DMZ.

Primeramente, se tuvo que crear un Vswitch en nuestro ESXI por donde circulara el tráfico de nuestra DMZ, para esto se siguió el siguiente procedimiento:

Se accedió a nuestro hypervisor, se pueden observar una cantidad de máquinas saliendo por la interfaz vmnic0, lo cual forma parte de nuestra LAN.





Fig. 5.1.4 Primeros Pasos para la creación de la interfaz en el ESXI.

Luego se procedió a la creación de nuestra interfaz como se ve en la siguiente Fig. 5.1.5.

Configuration	Local Users &	Groups Even	ts Permissions			
R Physical A Configuration	Remove Prop daptas vmnic2 vmnic0 100 Fu	ertes	ts Permissions		Refresh Add Networkin	g Properties
Dar	move Droper	tiac				~

Fig. 5.1.5 Procedimiento para la creación de la interfaz.

En la Fig. 5.1.6, presentamos el establecimiento de la interfaz de la zona DMZ.

Add Network Wizard	- 0)
Connection Type Networking hardware of	an be partitioned to accommodate each service that requires connectivity.	
Connection Type Network Access Connection Settings Summary	Connection Types Virtual Machine Add a labeled network to handle virtual machine network traffic. VMkernel The VMkernel TCP/IP stack handles traffic for the following ESXI services: vSphere vMotion, iSCSI, NFS, and host management.	
Hala I	Pade Newth Case	el

Fig. 5.1.6 Establecimiento de la interfaz de la zona DMZ.

En la Fig. 5.1.7, mostramos la creación de la interfaz de la zona DMZ.

rtual Machines - Netw	ork Access					
Virtual machines reach	networks through uplink adapters attached to vSphe	ere standard s	witches.			
						_
nnection Type	Select which vSphere standard switch will handle	e the network	traffic for this connection. You may also	o creat	e a new	
nection Settinas	vsphere standard switch using the unclaimed he	twork adapte	rs listed below.			٦
nmary	Create a vSphere standard switch	Speed	Networks			1
	Intel Corporation 1350 Gigabit Netv	vork Connec	tion			
	Vmnic3	Down	None			
	O Use vSwitch0	Speed	Networks			1
	Intel Corporation 1350 Gigabit Netv	vork Connec	tion			
	vmnic2	Down	None			
	vmnic0	100 Full	129.73.223.1-129.73.223.254			
	C Use vSwitch1	Speed	Networks			
	Intel Corporation I350 Gigabit Netv	vork Connec	tion			
	Preview:					
	Virtual Machine Port Group	Physical Adapte	15			-
	VM Network 2 👳 🔶	👝 🔛 vmni	G			
	1					_

Fig. 5.1.7 Creando la Interfaz de la zona DMZ.

"Organizar Y Establecer Nuevas Soluciones de Seguridad en la Red de la Empresa Sistems Enterprise S.A." Configurando la zona DMZ lo podemos ver en la siguiente Fig. 5.1.8.

🕝 Add Network Wizard				-		×
Virtual Machines - Connec Use network labels to ide	ction Settings entify migration compatible connection	ons common to two or more hosts.				
Connection Type Network Access Connection Settings Summary	Port Group Properties Network Label: VLAN ID (Optional): Preview: 	DMZ None (0) Physical Adapters Physical Adapters wmnic3	•			
Help			< Back Ne	ext >	Cano	el

Fig. 5.1.8 Configurando la zona DMZ.

En la Fig. 5.1.9, enseñamos la agregación la interfaz configurada al ESXI.

🕝 Add Network Wizard		-		×
Ready to Complete Verify that all new and m	odified vSphere standard switches are configured appropriately. \bigcup_{V}			
Connection Type Network Access Connection Settings Summary	Host networking will include the following new and modified standard switches: Preview: Virtual Machine Port Group Physical Adapters			
Help	< Back Fini	sh	Canc	el

Fig. 5.1.9 Agregando la interfaz configurada al ESXI.

Universidad Nacional de Ingeniería Facultad de Electrotécnica y Computación

En la Fig. 5.1.10, mostramos el establecimiento de la interfaz del ESXI.



Fig. 5.1.10 Establecimiento de la interfaz del ESXI.

De esta manera tenemos creado nuestro Vswitch, por donde pasará el tráfico de nuestra DMZ, en este servidor se desplegará nuestro Fortimail.

5.2. Fortigate:

A como se pudo ver en el grafico anterior el fortigate está conectado directamente a internet pero de igual manera tiene una conexión al swith LAN, por lo cual se le asignó una IP para administración, esta configuración podrá verse en la imagen relacionada con las interfaces de FORTIGATE. [15]

En la Fig. 5.2.1	, observamos la	plataforma de	I UTM FortiGate	200 D.
------------------	-----------------	---------------	-----------------	--------

III Aplicaciones 🕒 MX Lookup 1	bol - C 🛛 Uso de la herramier 💟 Supported plath	emi: [] Network Security Mii 💆 Müldes Partner Port: 🛞 Robot de tiempo de
FortiGate 2000 NFF	2000 Sencom	κ. () 🕬 Δ 🤒 soc.eburgu
Dashboard Main Security Fabric Forth/lew Network System Polycy & Objects Security Profiles VPN User & Device	System Information Sector NFR_2000_Sector Sector Number FG20004Q17801740 Firmane v6.0.2 build0163.(0A) Mode NAT/Flow-based System Time 2018/08/2108.5555 Upden 16:21:17-80 VolANIP	I Licenses (** 209.222.126.22) 0 I Fort/Cloud (Global) I Security Fabric Sencom I © FortSCare Support Statur © Activated Explored Explored IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
 WFI & Switch Controller Ing & Report Monitor 	Administrators B OHTTPS OF FordExplorer SOC_charges toper_admin admin super_admin	E CPU 1 minute 12 1 1005 199
	Memory' 2005	1 minute* [] I Sessions 1 minute* [] I
Q	704	

Fig. 5.2.1 Plataforma del UTM FortiGate 200 D para establecer la zona DMZ.

5.3. Interfaces:

A continuación estableceremos los puertos del UTM con el direccionamiento IP privado en la siguiente Fig. 5.3.1.

FortiGate 200D	NFR_200D	_Sencom					>_ [] @+ Д+ 🙆 soc_	cburgos 🕶
 Dashboard Security Fabric FortiView 	> ^ > >	🕄 FortiGa	te 200D MGMT WAN1 1 3 5 7 9	11 13 15 DMZ1				
+ Network	~		WAN2 2 4 6 8 10	0 12 14 16 DMZ2				
Interfaces	☆	+ Create Ne	w▼ 🖋 Edit 📋 Delete			VLAN	Switch Mode 💽 By Type By Role Alpha	abetically
DNS		T Status	T Name	T Members	T IP/Netmask	Т Туре	T Access	T Ref.
Packet Capture		Physical (10)						
SD-WAN		0	dmz1		10.10.10.1 255.255.255.0	Physical Interface	PING HTTPS HTTP FMG-Access CAPWAP	0
Performance SLA		0	dmz2		0.0.0.0 0.0.0.0	Physical Interface	PING FMG-Access CAPWAP	0
SD-WAN Rules		0	mgmt		192.168.1.99 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	1
Static Routes		0 0	port14 (1 Connected FortiSwitch(s))		Dedicated to FortiSwitch	Physical Interface	PING CAPWAP	4
Deline Reuter		•	port15 (Red SENCOM)		129.73.223.219 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FortiTelemetry	3
Policy Routes		0	port16 (DMZ Sencom)		172.16.30.1 255.255.255.248	Physical Interface	PING	2
RIP		0	wan1 (OUTSIDE_INTERNET)			Physical Interface	PING HTTPS HTTP FMG-Access	6
OSPF		0	wan2		0.0.0.0 0.0.0.0	Physical Interface	PING FMG-Access	0
BGP		VLAN Switch	(1)					
Multicast				1 3 5 7 9 11 13 15				
System	>		lan (VLAN ID: 0)		192.168.100.99 255.255.255.0	⊐ VLAN Switch (13)	PING HTTPS HTTP FMG-Access CAPWAP	2
Policy & Objects	>			2 4 6 8 10 12 14 16				
Security Profiles	>							
P VPN	>							
User & Device	>							
WiFi & Switch Controlle	er >							
Leg & Report	> .							

Fig. 5.3.1 Establecimiento de los puertos del UTM con sus direccionamiento IP Privado.

Se pueden observar las distintas interfaces etiquetadas con la dirección en donde apuntan, en este caso las que nos interesan son:

- Puerto 15 (Red SENCOM)
- Puerto 16 (Red DMZ)
- WAN1 (Outside_Internet)

A continuación se presentara en la Fig. 5.3.2, la configuración de la interfaz LAN de SENCOM.

Edit Interface					
Interface Name Alias	port15 (70:4C:A5:10:0 Red SENCOM	C:1B)			
Link Status	Up 📀				
Туре	Physical Interface				
Tags					
Role 1 Und	efined Add Tag Categor	▼ У		G	
Address					
Addressing mode	Manual DHCP F	PPoE			
IP/Network Mas	k				
Administrative A	ccess				
IPv4 V HTTP CAPW	S	 ✓ PING □ SNMP ✓ FortiTelemetr 	FMG-Access FTM y		
DHCP Server	r				
Networked Devi	ces				
Device Detection					
				ОК	Cancel

Fig. 5.3.2 Configuración de la interfaz LAN de SENCOM.

Universidad Nacional de Ingeniería Facultad de Electrotécnica y Computación

Estableciendo la configuracion del puerto del UTM para la zona DMZ en la Fig.

5.3.3.	Edit Interface
	Interface Name port16 (70:4C:A5:10:0C:1C) Alias DMZ Sencom Link Status Up o Type Physical Interface
	Tags Role 1 DMZ Add Tag Category
	Address Addressing mode Manual DHCP PPPoE IP/Network Mask 172.16.30.1/255.255.248
	IPv4 HTTPS HTTP 1 PING FMG-Access CAPWAP SSH SNMP FTM RADIUS Accounting FortiTelemetry
	Device Detection 🕥
	Miscellaneous
	Scan Outgoing Connections to Botnet Sites Disable Block Monitor OK Cancel

Fig. 5.3.3 Configuración del Puerto del UTM para la Zona DMZ.

Como se ve en la Fig. 5.3.4, la configuración del enlace WAN.

Edit Interface	
Interfree Name	wan1 (70:4C:A5:10:0C:0A)
Alias	OUTSIDE_INTERNET
Link Status	Up 📀
Туре	Physical Interface
Estimated Bandwidth 🕚	0 kbps Upstream 0 kbps Downstream
Tags	
Role 1 WAN	► Add Tag Category
Address	
Addressing mode Man IP/Network Mask	UUAL DHCP PPPoE
Administrative Access	
IPv4 VHTTPS CAPWAP RADIUS Accourt	HTTP FING FMG-Access SSH SNMP FTM fting Fort/Telemetry
Miscellaneous	
Scan Outgoing Connection	ns to Botnet Sites Disable Block Monitor
Enable Explicit Web Proxy	

Fig. 5.3.4 Configuración del enlace WAN con su IP Publica.

Después de la configuración de las interfaces podemos añadir las direcciones de servidores DNS para la navegación, en este caso a como se verá a continuación se utilizan los DNS de Google.

5.4. Servidores DNS:

En esta parte asignaremos los servidores DNS que ocuparemos se mostrara en la Fig. 5.4.1.

FortiGate 200D	NFR_200E	D_Sencom		
Dashboard	> 1	DNS Settings		
🔆 Security Fabric	>			
EortiView	>	DNS Servers	Use FortiGuard Servers Specify	
+ Network	~	Primary DNS Server	8.8.8.8	
Interfaces	_	Secondary DNS Server	8.8.4.4	
DNS	☆	Local Domain Name		
Packet Capture				
SD-WAN				Apply
Performance SLA				

Fig. 5.4.1 Integrando los Servidores Forwading del DNS de Google.

En esta Fig. 5.4.2, se observa los servidores DNS de Google.

DNS Settings		
DNS Servers	Use FortiGuard Servers	Specify
Primary DNS Server	8.8.8.8	
Secondary DNS Server	8.8.4.4	
Local Domain Name		

Fig. 5.4.2 Establecimiento de los servidores de DNS de Google.

Ya que tenemos las configuraciones básicas establecidas es hora de hacer nuestra primera configuración de routing, en la cual a como se espera es nuestras rutas de salida a internet

5.5. Rutas estáticas:

A continuación haremos el enrutamiento estático del enlace WAN en la siguiente Fig. 5.5.1.

Dashboard	>	+ Create New 🖋 Edit 「 Clone	🖻 Delete	
🔆 Security Fabric	>	Destination 🗢	▼ Gateway ≑	T Interfac
E FortiView	>	0.0.0/0 😫	129.73.223.1	Red SENCOM (port15)
🕂 Network	~	0.0.0/0		MOUTSIDE_INTERNET (wan1)
Interfaces				
DNS				
Packet Capture				
SD-WAN				
Performance SLA				
SD-WAN Rules				
Static Routes	☆			
Policy Routes				
RIP				
OSPF				
BGP				
Multicast				

Fig. 5.5.1 Ingresando el Enrutamiento Estático del enlace WAN.

A como se puede observar en nuestra imagen de rutas estáticas, existen dos, una para la salida a internet por nuestro Gateway el cual es directamente nuestra puerta de salida de IP publica (por motivos de seguridad no se presentan las IPs públicas.

En la Fig. 5.5.2, enseñamos la configuración el enrutamiento estático por el enlace WAN.

Edit Static Route	
Destination	Subnet Named Address Internet Service
	0.0.0.0/0.0.0
Gateway	
Interface	OUTSIDE_INTERNET (wan1)
Administrative Distance 🟮	10
Comments	0/255
Status	Enabled O Disabled
Advanced Options	
	OK Cancel

Fig. 5.5.2 Configurando del Enrutamiento Estático por el enlace WAN.

En la Fig. 5.5.3, observamos la configuración del enlace WAN con su enrutamiento estático.

Edit Static Route	
Destination	Subnet Named Address Internet Service
	0.0.0/0.0.0
Gateway	
Interface	🖷 Red SENCOM (port15) 👻
Administrative Distance 🜖	30
Comments	0/255
Status	Senabled Obisabled
Advanced Options	
	OK Cancel

Fig. 5.5.3 Configuración del enlace WAN con su Enrutamiento Estático.

Esta segunda imagen es de una ruta redundante, la cual utiliza el Gateway de nuestra LAN, a como se puede ver la distancia administrativa es mayor que nuestro primer enlace, lo cual significa que este actuara solamente si el primero pierde conexión. Debido a que es una DMZ solo lo dejaremos con un enlace y deshabilitamos el segundo con nuestra LAN. [10]

5.6. Políticas:

Después de haber realizado el direccionamiento y enrutamiento necesario, es tiempo de ejercer políticas de navegación y por supuesto lo más importante realizar la política que enrute nuestra DMZ con el internet.

En la siguiente Fig. 5.6.1, revelamos el establecimiento de las distintas políticas de red de la empresa SENCOM.

FortiGate 200D	NFR_200	D_Sencom					>_	C) @• A• 😣	SOC_cburgos •
Dashboard	> ^	+ Creat	e New 🖋 Edit 📋 Dele	e Q Policy Lookup Search		Q		Interface Pair View	By Sequence
🔆 Security Fabric	>	ID	Name	From	То	Source	Destination	Schedule	Service
🖿 FortiView	>	8	Permisos Web 2				ল আ	Control Partrictivo	
Network	>	Ľ		C VENIX_ENIX (VSW.pol (14)		EANT SW	i an	Control Nestrictivo	T ALL
System	>								
Policy & Objects	~								
IPv4 Policy	☆								
IPv4 DoS Policy		1	Permisos Web 1	VLAN_LAN (vsw.port14)	R OUTSIDE_INTERNET (wan1)	LAN FSW	all 🗐	o Control de Salida	🖳 ALL
Addresses									
Wildcard FQDN Addresses									
Internet Service Databa	se	7	NAT de Correo	OUTSIDE INTERNET (wan1)	MZ Sencom (port16)	🕮 all	😤 Mail Service	always	E Email Ac
Services						-	-		- Web Acc
Schedules									
Virtual IPs		1	Callel DMZ						-
IP Pools		°	Salida DIVIZ	DMZ Sencom (port16)	OUTSIDE_INTERNET (wan1)	📕 all	📱 all	L o always	LE ALL
Traffic Shapers									
Traffic Shaping Policy									
Security Profiles	>	2	Acceso VPN	SSL-VPN tunnel interface (ssl.root)	🗮 Red SENCOM (port15)	🔳 all	🔳 all	Lo always	🛛 ALL
I VPN	>					SSL-vpn-user			
🛔 User & Device	>	5 🖸 🔺	RED_SENCOM_RED_LAN	層 Red SENCOM (port15)	⊐‡ lan	🔳 all	🗐 all	Lo always	🛛 ALL
♥ WiFi & Switch Controlle	r >	0	Implicit Denv	□ anv	C any	লি আ	ান আ	To alwave	
🔟 Log & Report	>	<u> </u>		C any	U any	i an	dii	og arways	W ALL
Monitor	, •								7

Fig. 5.6.1 Establecimientos de las distintas políticas de la red de la Empresa SENCOM.

5.7. Salida DMZ:

Edit Policy				
			ID	
Name 📵	Salida DMZ		6	
Incoming Interface	DMZ Sencom (port16) +		Last used 23 minute(s) ago	
Outgoing Interface	OUTSIDE_INTERNET (wan1) *		First used	
Source	🗐 all 🗙 🕇		Hit count	
Destination	all X		433	
Schedule	T always		Active sessions 3	
Service	ALL ×		2 minutals) and	
Action	✓ ACCEPT ⊘ DENY ≉ LEARN		2 minute(s) ago	now
Firewall / Network O	ptions		•	0
NAT	Ο		2 minute(s) ago	now
IP Pool Configuration	Use Outgoing Interface Address Use Dyna	mic IP Pool	3	
Security Profiles			2 minute(s) ago	now
AntiVirus Web Filter	● AV_Sencom ▼	,	Jatol kutas	
DNS Filter				0
Application Control			2 minute(s) ago	now
IPS SSL Inspection	IPS_Sencom ssl_certificate-inspection	,	Total bytes 820.82 kB	
Logging Options			Current bandwidth	
Log Allowed Traffic	Security Events All Sessions		0.070	
Capture Packets				
Comments Write	a comment		┛ Online Help 🖸	
Enable this policy 🤇)			

En la siguiente Fig. 5.7.1, mostraremos el establecimiento de la política de la zona DMZ.

Fig. 5.7.1 Establecimos la política de la Zona DMZ.

A continuación en la Fig. 5.7.2, observamos la configuración de la política de NAT, en este caso su utilizara un SNAT para después agregarlo a una política.

A Dashboard	× *			2		
We Dashboard		+ Create New • Fdit	Clone Delete Search	ŭ		
Security Fabric	· · ·	Name ≑	Details 🗢	Interfaces ≑	Services ≑	Ref. ≑
FortiView	>					
Network	>					
System	>	Mail Service	> 172.16.30.2 (TCP: 11443> 443)			1
🛎 Policy & Objects	~		\triangleright			
IPv4 Policy			<i>u</i> 0			
IPv4 DoS Policy						
Addresses						
Wildcard FQDN Addresses						
Internet Service Databa	se					
Services						
Schedules						
Virtual IPs	☆					
IP Pools						

Fig. 5.7.2 Configurando las políticas del NAT

Aquí se hará la configuración necesaria para garantizar el acceso a nuestro servidor desde fuera de nuestra LAN, en donde se especifican la IP externa con la IP que será dirigido y el puerto que se utilizara para el acceso a este servicio, en este caso se destinó el puerto 11443 como externo y será redirigido al puerto 443 el cual pertenece a HTTPS.

En la Fig. 5.7.3	, presentamos el establecimiento del SNAT	para la zona DMZ.
------------------	---	-------------------

Edit Virtual IP
Name Mail Service Comments NAT de Correo Color Change
Network
Interface any
Type Static NAT
External IP Address/Range -
Mapped IP Address/Range 172.16.30.2 - 172.16.30.2
Optional Filters 🛈
Port Forwarding
Protocol TCP UDP SCTP ICMP
External Service Port 11443 - 11443
Map to Port 443 - 443
OK Cancel

Fig. 5.7.3 Estableciendo el SNAT para la utilización de la Zona DMZ.

Universidad Nacional de Ingeniería Facultad de Electrotécnica y Computación

dit Policy			
			ID
Name 📵	NAT de Correo		/
Incoming Interface	MOUTSIDE_INTERNET (wan1)		Last used
	+		32 minute(s) ago
Outgoing Interface	🗎 DMZ Sencom (port16) 🛛 🗙		First used
	+		2 day(s) ago
Source	🗉 all 🛛 🗙		
	+		Hit count
Destination	Ail Service X		/0
Calcadada			Active sessions
Schedule	Lo aiways		0
Service	Le Mail Access		
	• vveb Access		2 minute(s) ago now
Action			0
Action	V ACCELL V DENT P LEANN		0
Firewall / Network O	ptions		2 minute(s) ago now
NAT 🔿			
			2 minute(s) ago now
Security Profiles			
AntiVirus	■ default ▼	1	2 minute(s) ago now
Web Filter			0
DNC Filter			0
DINSFILLER			
Application Control			2 minute(s) ago now
IPS	protect_email_server	ø	Total bytes
SSL Inspection	ss. certificate-inspection	<i>a</i> *	1.44 MB
			Current handwidth
Logging Options			0 B/s
Log Allowed Traffic	Security Events All Sessions		
Capture Packets			
Comments Write	a comment		🗐 Online Help 🖸
	20		
Enable this policy			
. ,			

Luego podemos agregar nuestro NAT a nuestra política como se ve en la Fig. 5.7.4.

Fig. 5.7.4 Agregando el NAT a las políticas de la red.

5.8. Fortimail:

Después de haber mostrado toda la configuración necesaria en nuestro enrutador de perímetro (Fortigate), nos falta la instalación y configuración de parte de nuestros servidor que estará localizado en nuestra DMZ.

A continuación se ve en la Fig. 5.8.1, la configuración del Fortimail de SENCOM.



Fig. 5.8.1 Configuración del Fortimail de SENCOM.

A como se había mencionado anteriormente, el modo en el cual operaremos nuestro Fortimail será el modo server, ya que consta con las características necesarias que satisfacen el fin requerido. Este Servidor Fortimail está en el capítulo anterior todas las configuraciones debidas.

Status Consol	9		➡Manage Widget	C Reset Wid
System Informatio	on 2 - x	Statistics History (Count, By Day)	3 ≠ 0 ≓ 🔟	≑ − ×
Serial number:	FEVM00000000000			
Up time:	2 day(s) 1 hour(s) 7 minute(s) 53 second(s)	Bypass Scan On Auth [10	0%]	
System time:	Fri, Aug 31, 2018 10:03:27 CST			
Reboot time:	Wed, Aug 29, 2018 08:55:34 CST			
Firmware version:	v6.0,build108,180731 (6.0.2 GA) [Update]	8		
System configuration:	[Backup] [Restore]			
Operation mode:	Server 💌	6		
Current administrator	: admin (4 in total) [Details]			
HA mode:	Configured: off, Effective: off	4		
Log disk:	Capacity 49 GB, Used 32 MB (0.07%), Free 49 GB			
Mailbox disk:	Capacity 198 GB, Used 245 MB (0.13%), Free 198 GB			
Email throughput:	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute	2		
License Informatio	on 2 - x			
AntiVirus:	No license ()	0	26	- 21
AV definition:	Version 1.00001 [Update]	08.11 08.10 08.10 08.10 08.51 08.57 08.50 08.50 08.50 08.	re 08.11. 08.10 08.10 08.10	08.2 .
AV engine:	Version 1.00001			
Virus outbreak:	Expired 📀	Statistics Summary (Today)	2 / 0	≓ - ×
AntiSpam:	Expired 📀	No data!		
AS definition:	Version 1.00001			
VM:	Trial license(Expire in 12 days 1 hour 26 mins) [Update]	Statistics Summary	C hu	≓ - ×
FortiSandbox:	Disabled [Configure]	,	~	
FortiCloud:	Not Activated [Activate]	Messages Total This This	This Today This	This

En la Fig. 5.8.2, veremos el modo de operación del Fortimail.

Fig. 5.8.2 Modo de Operación del Fortimail.

Es necesaria la configuración de interfaces en el fortimail:

Algo antes no mencionado es de que este servidor tendrá dos interfaces de red, una de ellas será con su IP de web server el cual estará localizado en la DMZ y la otra será una IP administrativa la cual se conectara a nuestro switch LAN (esto se puede observar en nuestro diagrama final de red DMZ).

En la Fig. 5.8.3, observamos el establecimiento del interfaz del Fortimail.

Selection Select							
Link Status	Name	Туре	IP/Netmask	IPv6/Netmask	Access	•	
•	port1	Physical	129.73.223.225/24	::/0	HTTPS,PING,SSH	• *	
•	port2	Physical	172.16.30.2/29	::/0	HTTPS,PING	•	

Fig. 5.8.3 Establecimiento del interfaz del Fortimail.

En la siguiente Fig. 5.8.4, mostramos la configuración de la interfaz con los distintos protocolos de red.

Bdit Interf	ace					
Interf Link s	ace name: por tatus: 📀	t1 (00:0c:29:17:34	4:2c)			
Add Ma IP/N IPv	Iressing Mode anual DHCP Netmask: 6/Netmask:	129.73.223.2	25 / 2	4		
Adv Acc	vanced Setting ess: D HTTPS D SNMP	PING HTTP	SSH			
We Ma	b access: D Admin I access: D POP3	WebmailIMAP	POP3S	IMAPS		
MT Adr	U: 1500 ninistrative stat	us: Up Down				OK Cancel

Fig. 5.8.4 Configurando la interfaz y permitiendo los distintos protocolos de red.

En la Fig. 5.8.5, enseñamos el establecimiento de la interfaz del Fortimail.

Edit Interface 새라						
Interface name: por Link status:	t2 (00:0c:29:17:	34:36)				
Addressing Mode Manual DHCP IP/Netmask:	172.16.30.2	/ 29				
Advanced Setting Access:		SSH				
SNMP Web access:	HTTPWebmail	TELNET				
Mail access: POP3 MTU: 1500	C IMAP	C POP3S C IN	ЛАРS			
Administrative stat	tus: Up Down					
Fig. 5.8.5 Esta	ableciend	lo la interfaz de	I Fortimail.	C	Cancel	



De igual manera se tendrán que configurar servidor DNS en nuestro FORTIMAIL, usaremos los de Google.

En la Fig. 5.8.6, observamos el ingreso de los servidores DNS en el Fortimail.

FortiMail VM00	FortiMai	I							
🚯 Dashboard		Interface	Link Monitor	Routing	DNS	DDNS	Port Forwarding	FortiGate	Traffic Capture
FortiView	>			45					
C Monitor	>	Network S	etting						
🔅 System	~	Primary DN	NS server:	8.8.8.8					
Network		Secondary	DNS server:	8.8.4.4					
Administrator								A	Canad
Configuration								Арріу	Cancel
Mail Settings									
Customization									

Fig. 5.8.6 Ingresando los Servidores DNS de Google.

5.9. Routing:

En nuestro Fortimail será necesario realizar la configuración de dos rutas estáticas, una para la comunicación con la administración del mail server y la otra para la salida por medio de su Gateway.

En la Fig. 5.9.1, presentamos el enrutamiento estático del Fortimail.

FortiMail VM00	FortiMa	il 📐				
2 Dashboard		Interface Link Monitor Routing (ONS DDNS Port	Forwarding FortiGate	Traffic Capture	
FortiView	>	C + New Edit Delete				
Monitor	>					
System	~	Destination IP/Netmask	Gate	eway		Interface
Network		0.0.0.0/0	172.	.16.30.1		port2
Administrator		172.16.20.0/24				port1
Configuration						
Mail Settings						

Fig. 5.9.1 Enrutamiento Estático del Fortimail.

Lin la rig. 5.3, mostramo		
EdivRouting Entry		
Destination IP/netmask:	0.0.0.0	/ 0
Interface:	port2 💌	
Gateway:	172.16.30.1	
	ОК	Cancel

En la Fig. 5.9, mostramos el enrutamiento del Fortimail.

Fig. 5.9.2 Mostrando el enrutamiento del Fortimail.

A continuación podremos ver la configuración de políticas por default de nuestro servidor, en esta parte no se ha editado nada ya que son configuraciones empresariales adaptables al entorno y las necesidades, en donde son necesarias políticas de seguridad y el monitoreo de la entrada y salida de correo.

En esta Fig. 5.9.3, observamos el establecimiento de las políticas del Fortimail.

FortiNail VM00	FortiMa	il					
🚯 Dashboard		IP Policy					
FortiView	>	- Nour		Edit 📅 Delete	t Maya =		
C Monitor	>	T New.		Edit Delete	∎ Move ▼		
System	>		<	1 / 1 > » Re	ecords per page: 50	-	
💄 Domain & User	>	Enabled	ID	Source	Destination	Session	
Policy	~		1	0.0.0/0	0.0.0/0	Inbound Session	
Access Control			2	::/0	::/0	Inbound Session	
IP Policy							_
Recipient Policy							

Fig. 5.9.3 Estableciendo las políticas del Fortimail.

En la Fig. 5.9.4, enseñamos establecimiento de la politica de entrada del Fortimail.

Inbound	Ou	tbound							
+ New.		Edit 🛅 Delete 🔺 N	Nove 💌 🔍 Policy Looku	ıp					
2 « •	Image: Contract of the second seco								
Enabled	ID	Domain Name	Sender Pattern	Recipient Pattern	AntiSpam	AntiVirus	Content	Resource	
	1	system	*@*	*@*	AS Inbound	AV SysQuarantine	CF Inbound	Res Default	

Fig. 5.9.4 Establecimiento de la política de entrada del Fortimail.

En esta Fig. 5.9.5, exhibimos el establecimiento de la política de salida del Fortimail.

Inbound	Ou	tbound								
+ New.	+ New Image: Delete									
C «	2 « < 1 / 1 > » Records per page: 50 V Domain:All V Show system policy Totals									
Enabled	Enabled ID Domain Name Sender Pattern Recipient Pattern AntiSpam AntiVirus Content									
	2	system	*@*	*@*	AS Outbound	<u>AV Reject</u>	CF Outbound			

Fig. 5.9.5 Establecimiento de la política de salida del Fortimail.

De esta manera se tiene configurada nuestra DMZ, alejada de nuestra red LAN e inclusive con otro direccionamiento de salida, para poder tener acceso a nuestro servicio desde internet es necesario digitar: <u>https://<ip_externa>:1433</u> (puerto establecido en nuestra configuración al igual que el protocolo https)

Por los momentos es de uso interno empresarial por lo cual los usuarios añadidos tienen credenciales específicas para la utilización del servicio.

Conclusiones.

En esta monografía aplicamos toda la base teórica y práctica precisamente para tener una mayor seguridad en la red de la compañía Sistems Enterprise S.A. Durante todo el proceso de instalación y configuración de: (IPS, UTM, DNS, Fortimail y una Zona DMZ). Obtuvimos los resultados satisfactorios cumpliendo con los objetivos planteados en cada uno de estas implementaciones antes mencionadas.

Concluimos que es necesario implementar estas soluciones de seguridad con sus mejores prácticas y políticas en una organización porque los ataques cibernéticos están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso son los usuarios, se trata de uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de nosotros los administradores de red. Esta solución integral busca proteger, solucionar y evitar las distintas vulnerabilidades. Esto fue nuestra meta principal de este documento en organizar y establecer nuevas soluciones de seguridad en la red de la empresa Sistems Enterprise S.A.

Nosotros recomendamos estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su red o equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible. Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. No ingresar datos personales y contraseñas en cualquier página Web. También no abrir correos remitentes desconocidos porque dentro del contenido puede llevar un enlace para ser redirigido, Cambiar las contraseñas más frecuentemente y tener un doble patrón de autenticación en sus cuentas personales. Otro punto es encriptar todos los discos duros de las computadoras con el objetivo de prevenir las pérdidas de datos.

Bibliografía:

- [1] A.FOROUZAN, B. ((2002)). TRANSMISION DE DATOS Y REDES DE COMUNICACIONES. Madrid: McGrawHill.
- [2] Andina, F. (2014). REDES ADMINISTRACION DE SERVIDORES. Buenos Aires.
- [3] B., K. A. (2013). Hacking Etico 101.
- Barker, K. &. (s.f.). CCNA Security 640-554. 800 East 96 th Street Indianapolis, IN 46240: Pearson Education, Inc.
- [5] CISCO. (2018). Curricula de CCNA del Modulo 1-4.
- [6] Fortinet. (s.f.). *Download Firmware*. Obtenido de https://support.fortinet.com/Download/FirmwareImages.aspx
- [7] Fortinet. (s.f.). Recurso de Fortimail. Obtenido de https://docs.fortinet.com/fortigate/adminguides
- [8] Garcia Rambla, J. L. (2017). *Ataques en redes de datos IPV4 e IPV6.* España, tercera edición revisada y ampliada.
- [9] Huerta, A. V. (Julio, 2002). SEGURIDAD EN UNIX Y REDES.
- [10] James O. Coplien, R. C. (2012). Código Limpio. Madrid, España.: ANAYA.
- [11] M Carling, S. D. (s.f.). *Guia Avanzada Administracion de Sistemas Linux.* Madrid, Mexico: Prentice Hall.
- [12] Marchionni, E. A. (s.f.). ADMINISTRADOR DE SERVIDORES. USERS.
- [13] McAfee. (s.f.). McAfee Network Security Platform. Obtenido de https://community.mcafee.com/t5/Network-Security-Platform-NSP/bd-p/network-securityplatform-expert-center
- [14] Syed M.Sarwar, R. K. (s.f.). El Libro de Unix. Madrid: Addison Wesley.
- [15] TANENBAUM, A. S. (2012). Redes de Computadoras. Mexico: PEARSON.
- [16] Tori, C. (2008). Hacking Etico. Buenos Aires, Argentina.
- [17] Zemánek, J. (2004). CRACKING SIN SECRETOS. RA~MA.
- [18] Zentyal. (s.f.). Zentyal.org Documentacion para el servidor DNS. Obtenido de https://doc.zentyal.org/es/

Anexos:

Anexo 1. Diagrama Final de SENCOM

En la Fig. 1A.1 observamos el diagrama de la red de computadora de la empresa SENCOM al completar todos nuestros objetivos.



Fig. 1A.1 Diagrama de la red SENCOM
ANEXO 2. Tabla de Cotizaciones

Marca	Precio en Dólares.
UTM Fortinet Fortigate 200 D	\$ 3,837.32
UTM WatchGuard M-200	\$ 6,500
8 PATCHCORD 7FT CAT 5E GRIS	\$ 2.29
Sensor del IPS M-1450	\$2,000
Total	\$12,355.64

En esta tabla se observan todos los equipos de red que utilizamos para llevar a cabo este proyecto de organización y estructuración de la red que la Empresa SENCOM nos facilitó para hacer esta monografía. Estos precios vienen incluido con IVA y Envió desde el lugar del fabricante.