

Universidad Autónoma Metropolitana Unidad Azcapotzalco
División de Ciencias Básicas e Ingeniería
Licenciatura en Ingeniería en Computación

**Análisis e implementación de mecanismos de seguridad
para una red corporativa**

Reporte de Proyecto de Integración
que presenta:
Pérez Bonilla Leticia

Modalidad:
Estancia profesional

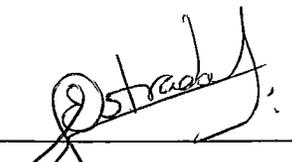
Asesores de proyecto:
M. en C. José Alfredo Estrada Soto
Ing. Mario Ernesto Gómez Romero

Trimestre:
14-0

Diciembre 2014

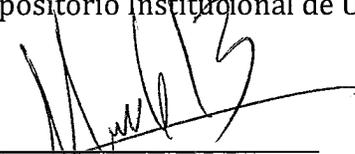
Declaratoria

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



M. en C. José Alfredo Estrada Soto

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



Ing. Mario Ernesto Gómez Romero

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



Leticia Pérez Bonilla

Resumen

La seguridad en redes de computadoras es un punto muy importante ya que busca garantizar que el material y los recursos de software de una organización se usen únicamente para los propósitos para los que fueron creados y dentro del marco previsto. Generalmente, esta se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autenticación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado. Esto nos llevó a plantear y configurar en la empresa políticas de seguridad, las cuales comprenden todas las reglas de seguridad que se siguen en la misma.

Durante la realización de este proyecto se brindan los servicios de seguridad haciendo uso del equipo FortiGate¹ tomando en cuenta el tipo y tamaño de la red; FortiGate es un producto de Fortinet² en una red corporativa. Para lidiar con vulnerabilidades en cuestión de seguridad de datos, se propone una metodología con base en el empleo de algoritmos complejos de seguridad, previo análisis de posibles amenazas a la red. Se generan e implementan políticas de protección contra ataques informáticos tales como la autenticación de usuarios por VPN, se aplican y configuran técnicas de priorización de tráfico y Calidad de Servicio (QoS) con el fin de reservar ancho de banda para aquellas aplicaciones que son más sensibles a los retardos, o bien para limitar el ancho de banda de aquellas aplicaciones que hacen un uso intensivo de los recursos de la red.

En este reporte encontraremos un recuento de las actividades que se llevaron a cabo para la elaboración del proyecto de estancia en la empresa TBT & TALENT.

-
1. Es un dispositivo para la protección de redes.
 2. Es el proveedor mundial en dispositivos de seguridad de red y líder en gestión unificada de amenazas (UTM)

Índice

Resumen.....	3
Capítulo 1	
Introducción	
1.1 Objetivo.....	6
1.2 Introducción.....	6
1.3 Antecedentes.....	7
1.4 Justificación.....	7
1.5 Organización del proyecto.....	8
Capítulo 2	
Análisis de la red de la empresa	
2.1 Características de la empresa.....	9
2.2 Características del equipo Fortigate 200B con el que cuenta la empresa.....	10
Capítulo 3	
Desarrollo	
3.1 Accediendo al equipo FORTIGATE-200B vía WEB.....	12
3.2 Interfaces.....	13
3.3 Dominiosvirtuales y Routing.....	14
3.4 Policy Route.....	15
3.5 Firewall.....	16
3.6 Antivirus.....	18
3.7 Filtrado Web.....	20
3.8 Calidad de servicio.....	22
3.9 Creación de políticas de seguridad.....	23
Capítulo 4	
Resultados y conclusiones	
4.1 Resultados.....	25
4.2 Conclusión.....	26
Capítulo 5	
Bibliografía y anexos	
5.1 Bibliografía.....	27
5.2 Anexos.....	28

Índices de figuras

Figura 1. Diagrama de red de la Empresa.....	10
Figura 2. Accediendo al Fortigate 200B.....	12
Figura 3. Información del Sistema Fortigate 200B.....	13
Figura 4. Interfaces.....	14
Figura 5. Ruta estática.....	15
Figura 6. Políticas de ruta.....	16
Figura 7. Agregando dirección de usuario al Firewall.....	17
Figura 8. Lista de direcciones agregadas al Firewall Objects.....	17
Figura 9. Grupos de usuarios en el Firewall Objects.....	18
Figura 10. Perfil AV_Orion de Antivirus.....	19
Figura 11. Perfil AV_flow de Antivirus.....	19
Figura 12. Perfil FW_ORION_M del Filtrado WEB.....	21
Figura 13. Perfil FW_Orion del Filtrado WEB.....	21
Figura 14. Perfil FW_total del Filtrado WEB.....	22
Figura 15. Políticas de seguridad.....	24
Figura 16. Campos de la configuración de cada política.....	24
Figura 17. Organización de nuestros usuarios	26
Figura 18. Rack en malas condiciones.....	28
Figura 19. Rack en malas condiciones.....	28
Figura 20. Rack ordenado.....	29

Capítulo 1

Introducción

1.1 Objetivo

General

Crear e implementar mecanismos de seguridad para una red corporativa.

Específicos

- Analizar las posibles amenazas a una red corporativa.
- Crear dominios virtuales.
- Crear y manejar routing.
- Implementar la funcionalidad Policy Routing
- Implementar un firewall
- Generar e implementar políticas de seguridad vía FortiGate.
- Aplicar técnicas de priorización de tráfico y calidad de servicio (QoS).
- Configurar y administrar un servidor VPN.
- Configurar servicios de acceso remoto.
- Implementar el filtrado de Tráfico Web (URL Web Filtering)

1.2 Introducción

Una red corporativa está compuesta por redes de área local propia de una entidad (empresa, firma, organismo, etc.) y unida mediante enlaces privados o públicos, que contiene a nivel de su red las prestaciones de la red pública y las de la misma red. En este tipo de empresas se debe dar mucha importancia a la seguridad en la red ya que es vulnerable a amenazas y ataques, ya sean internos o externos.

La seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y

equipos físicos, tales como las mismas computadoras. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización a organización.

En esta estancia profesional se participará en un proyecto que busca analizar posibles amenazas a una red corporativa y brindar así servicios de seguridad. Para ello se implementarán servidores VPN¹, firewalls, entre otros y se crearán políticas de protección contra ataques informáticos; todo ello con el fin de obtener una mayor seguridad en la empresa.

Es importante resaltar que se buscará prevenir ataques minimizando o eliminando los efectos de los ataques de forma continua y en tiempo real.

1.3 Antecedentes

Inicialmente la seguridad de la información de una empresa se conseguía fundamentalmente por medios físicos y administrativos, ya sea utilizando cajas fuertes donde se guardaban los documentos o procedimientos de investigación de personal durante la fase de contratación. La introducción de las computadoras hizo evidente la necesidad de utilizar herramientas automáticas para proteger los archivos y otras informaciones almacenadas. Este es el caso de los sistemas multiusuarios, y más relevante para los sistemas en los que el acceso se puede hacer desde teléfonos públicos o redes de datos.

La utilización de facilidades de comunicación para transportar datos entre computadoras o entre redes ha generado un nuevo reto para la seguridad. Las medidas de seguridad en red son necesarias para proteger los datos durante su transmisión y garantizar que los datos que se han transmitido son auténticos.

1.4 Justificación

En la actualidad la seguridad en redes está compuesta por protocolos, tecnologías, dispositivos, herramientas y técnicas que protegen los datos y disminuyen las amenazas. La protección de la seguridad en muchas empresas se ha convertido en una confusión de herramientas y políticas puntuales. Mantenerse al ritmo de los hackers se ha convertido en una actividad altamente especializada, por lo tanto mantener la seguridad hoy en día en una red no se considera nada sencillo.

Los equipos de seguridad constituyen una nueva generación de dispositivos de seguridad de muy alto rendimiento que garantizan la protección completa de sistemas en tiempo real. Hoy en día, diversas plataformas de seguridad proveen una solución integrada de seguridad compuesta por las funcionalidades más necesarias para tener una protección completa de las comunicaciones como son: firewall, VPN, antivirus, filtrado web, control de aplicaciones, entre otros.

Para llevar a cabo este proyecto se requieren de conocimientos un tanto especializados en redes; sólo por mencionar algunos tenemos: la configuración de un switch, un router, métodos de seguridad, protocolos de red, algoritmos de cifrado, entre muchos más. Es importante mencionar que muchos de estos conocimientos fueron adquiridos en el área de concentración.

1.5 Organización del proyecto

Este proyecto consta de 5 capítulos los cuales están ordenados de la siguiente manera. En capítulo 1 encontramos una breve introducción, antecedentes y la justificación de ese proyecto. En el capítulo 2 se habla del análisis de la red de la empresa y así mismo las características del dispositivo FortiGate con el que cuenta la empresa. En el capítulo 3 se encuentra el desarrollo de todas las actividades que se llevaron a cabo en la empresa y las cuales se plantearon en los objetivos. En el capítulo 4 encontramos los resultados y las conclusiones y por último en el capítulo 5 encontramos los resultados y la conclusión del proyecto.

Capítulo 2

Análisis de la red de la empresa

2.1 Características de la empresa

Existen muchas empresas que se encargan de dar soporte y así mismo soluciones a problemas a los que se enfrenta una red corporativa, tal es el caso de la empresa TBT.

TBT es una empresa 100% mexicana, conformada por profesionales especializados en tecnologías de la información, diseño e implementación de soluciones de internet para todo tipo de negocio. Brinda diferentes servicios tales como consultoría en infraestructura de redes inalámbricas, integración de soluciones de seguridad informática, análisis de vulnerabilidades, soluciones de correo electrónico y web.

La empresa cliente de TBT en la cual se llevaron a cabo los objetivos mencionados anteriormente cuenta con una red organizada de la siguiente manera:

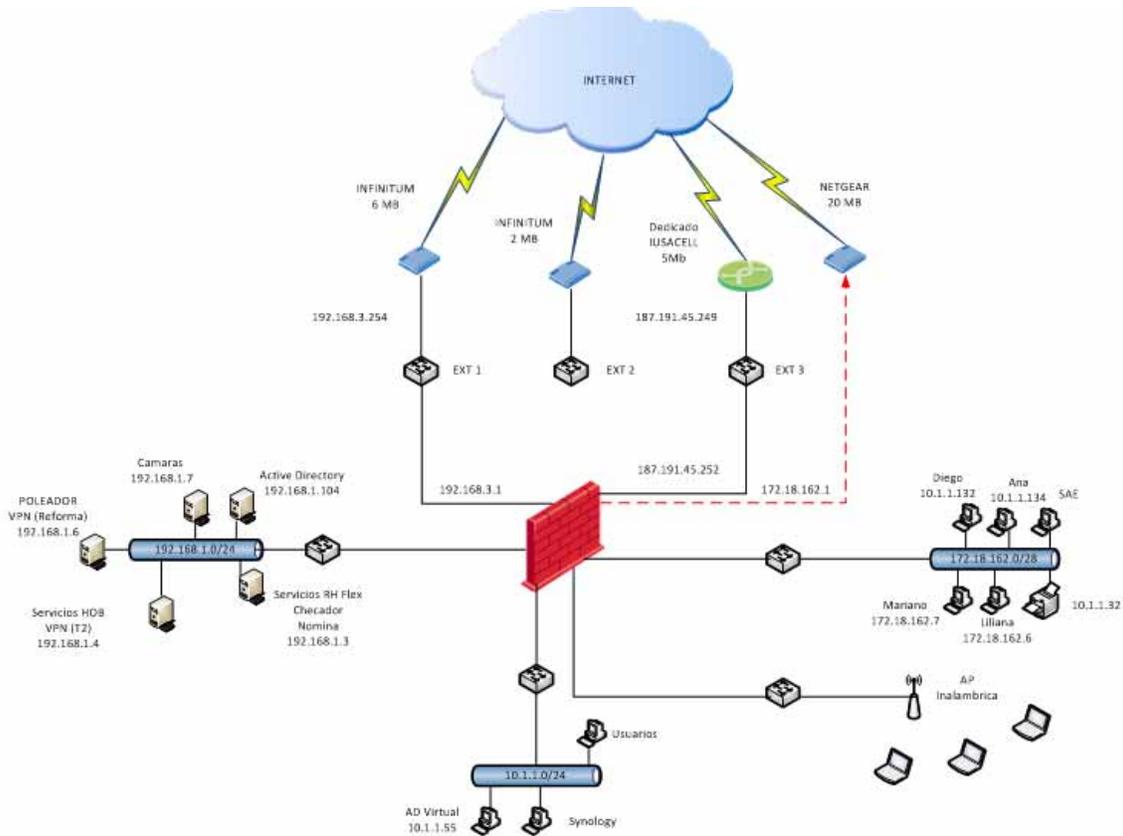


Figura 1. Diagrama de red de la Empresa

La empresa cliente llamada Grupo Orion brinda soluciones a empresas tales como administración del capital humano, capacitación empresarial, consultoría y coaching, entre otras, le trabaja a empresas tales como Iberia, Air France, Aeromexico, American Airlines, Banamex, British Airways, Capital Estratégico, Continental Airlines, entre muchas otras empresas importantes, es por ello que la seguridad en la red de la empresa es de vital importancia.

2.2 Características del equipo Fortigate 200B con el que cuenta la empresa

El Fortigate 200B ofrece la administración integrada de amenazas en las redes internas cableadas e inalámbricas. El dispositivo provee hasta 5 Gbps de capacidad de procesamiento de Firewall, permitiéndote proteger las aplicaciones y la red sin afectar la disponibilidad y la performance.

Características

- Ofrece hasta 5 Gbps de firewall con 8 interfaces GbE.
- FortiGate-200B-POE potencias de hasta 8 puntos de acceso inalámbricos integrados con interfaces de POE.
- Preparado para IPv6 plataforma con opciones de autenticación fuerte para acceso de red seguro y el cumplimiento de la política de seguridad.
- La bahía de expansión FSM ofrece una mayor flexibilidad mediante el apoyo de almacenamiento localizado y presentación de informes de datos de eventos, y la optimización de la WAN.
- Administración centralizada y presentación de informes a través FortiManager y FortiAnalyzer simplificar el despliegue y la gestión de su infraestructura de seguridad.

FortiOS es el software, desarrollado por el fabricante Fortinet exclusivamente para la seguridad, el rendimiento y fiabilidad, es un sistema operativo que aprovecha el poder del contenido FortiASIC y procesadores de red. El software FortiOS permite un amplio conjunto de servicios de seguridad:

- Firewall
- VPN
- Intrusion Prevention
- Antivirus/Antispyware
- Antispam
- Web Filtering
- Application Control
- Data Loss Prevention
- End Point
- Network Access Control

Capítulo 3

Desarrollo

3.1 Accediendo al equipo FORTIGATE-200B vía WEB

Apuntando vía `https://` a la dirección **192.168.1.99** en el navegador. Nos muestra la pantalla de inicio del equipo. En donde nos pide, la siguiente información:

Name y Password

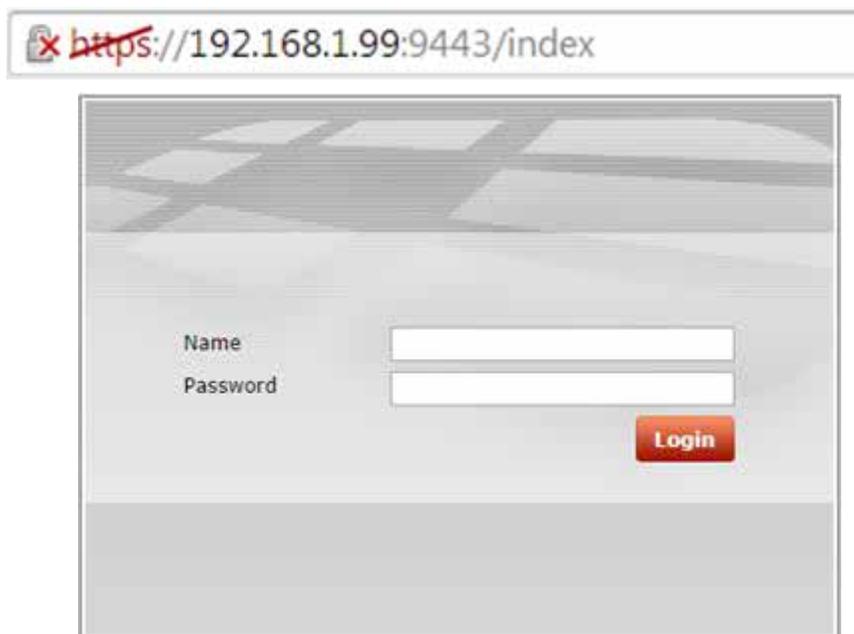


Figura 2. Accediendo al Fortigate 200B

Entrando con el nombre y contraseña correcta a nuestro Fortigate 200B podemos ver la información del sistema como se muestra en la imagen siguiente:



Figura 3. Información del Sistema Fortigate 200B

Aquí podemos observar:

Versión de Firmware :

V5.0, build0292 (GA Patch 9). La cual es última versión liberada por el fabricante Fortinet y la cual es estable.

Número de serie:

FG200B3912611300

Entre otras características, es importante resaltar que se debe de estar actualizando la versión del Firmware conforme vayan saliendo, ya que esto nos permite un mejor uso y rendimiento del dispositivo.

3.2 Interfaces

Para crear una interfaz dentro de Fortinet debemos seguir lo siguientes pasos:

1. Nos vamos a **System>Network>Interface** enseguida damos click en **Créate new**
2. Estando ahí ponemos el nombre, dirección ip y la máscara.

A continuación podemos observar en la Figura 4 las interfaces que se crearon:



Figura 4. Interfaces

Podemos observar el puerto así como las respectivas direcciones IP y máscaras.

3.3 Dominios virtuales y Routing

Los equipos FortiGate permiten la utilización de Dominios Virtuales, de modo que sobre una única plataforma física podemos configurar hasta 500 Equipos virtuales, completamente independientes entre sí y con todas las funcionalidades que posee cada plataforma física. Todos los equipos FortiGate disponen en su configuración básica de la capacidad de definición de hasta 10 dominios virtuales, siendo posible ampliar el número de éstos en los equipos de gama alta (a partir de la gama FG3000), llegando hasta 500 Dominios Virtuales.

Cada uno de estos dominios virtuales representan de forma lógica una máquina independiente del resto, asignándoles interfaces lógicas (VLAN's) o físicos con la posibilidad de trabajar en modo router o transparente, aplicar diferentes perfiles y políticas sobre cada máquina, etc.

Los equipos FortiGate pueden trabajar con enrutamiento dinámico, soportando RIP (v1 y v2), OSPF y BGP, así como con enrutamiento multicast (PIM sparse/dense mode), además de trabajar con enrutamiento estático y ofrecer la posibilidad de realizar *policy routing*.

Es necesario configurar una ruta predeterminada para cada interfaz e indique cuál es la ruta preferida mediante la especificación de la distancia. La distancia inferior se declara activa y se coloca en la tabla de enrutamiento.

Para configurar la ruta estática seguimos los pasos descritos a continuación:

1. Nos vamos a **Router > Static > Static Route** y seleccionamos **Create New**.
2. Seleccionamos **Destination IP/Mask to the address** y la **netmask** la ponemos a 0.0.0.0/0.0.0.0.
3. Seleccione el dispositivo para la conexión primaria, **WAN1**.
4. Escribimos el **Gateway address**.
5. Seleccionamos **Advanced**.
6. Escribimos la Distancia a 10.
7. Damos click en **OK**.
8. Repetimos los pasos del 1 al 7 para configurar el dispositivo WAN2 pero este con una distancia de 20.

En la Figura 5 podemos observar la ruta estática configurada:



The screenshot shows the FortiGate 200B configuration interface. On the left, a navigation tree is visible with 'Router' selected, and 'Static' > 'Static Routes' highlighted. The main area displays a table titled 'Create New' with the following data:

IP/Mask	Gateway	Device
0.0.0.0 0.0.0.0	187.174.218.65	port20
0.0.0.0 0.0.0.0	187.191.45.249	port9
192.168.200.0 255.255.255.0		ssl.root

Figura 5. Ruta estática

3.4 PolicyRoute

Ambos enlaces están disponibles para distribuir el tráfico de Internet a través de ambas rutas, si una de las interfaces falla, la unidad FortiGate continuará enviando tráfico a través de la otra interfaz activa. La configuración es similar a la configuración de interfaces redundantes, con la principal diferencia que las rutas configuradas deben tener los mismos ajustes de distancia.

Esto significa que ambas rutas permanecerán activas en la tabla de enrutamiento. Para hacer esto usamos una política de ruta por defecto para indicar la interfaz que se prefiere para acceder a Internet. Si el tráfico coincide con la política de seguridad, la política prevalece en la tabla de enrutamiento, incluyendo las rutas conectadas.

Para redirigir tráfico a través de la interfaz secundaria, se crea una política de ruta para dirigir tráfico sobre ella en vez de la interfaz principal. Al añadir una política de ruta, sólo debemos definir la interfaz de salida y dejar la puerta de entrada en blanco. Esto asegura que la política de ruta no será activada cuando el enlace está inactivo. En la Figura 6 se muestra las políticas de ruta configuradas:

#	Incoming	Outgoing	Source	Destination
20	ext-rog	port12	192.168.200.0/255.255.255.0	10.1.1.0/255.255.255.0
19	port12	port11	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0
8	port12	switch	10.1.1.0/255.255.255.0	192.168.1.0/255.255.255.0
16	port12	switch	172.18.162.0/255.255.255.240	192.168.1.0/255.255.255.0
17	port12	port12	172.18.162.0/255.255.255.240	10.1.1.0/255.255.255.0
18	switch	port13	192.168.1.0/255.255.255.0	172.18.162.0/255.255.255.240
7	switch	port12	192.168.1.0/255.255.255.0	10.1.1.0/255.255.255.0
19	port12	port13	10.1.1.0/255.255.255.0	172.18.162.0/255.255.255.240
21	Ag_Test	port12	10.10.10.0/255.255.255.0	10.1.1.0/255.255.255.0
23	port12	Ag_Test	10.1.1.0/255.255.255.0	10.10.10.0/255.255.255.0
10	switch	Ag_Test	192.168.1.0/255.255.255.0	10.10.10.0/255.255.255.0
9	Ag_Test	switch	10.10.10.0/255.255.255.0	192.168.1.0/255.255.255.0
14	port12	port11	10.1.1.0/255.255.255.0	0.0.0.0/0.0.0.0
6	Ag_Test	port11	10.10.10.0/255.255.255.0	0.0.0.0/0.0.0.0
11	port12	port11	172.18.162.0/255.255.255.240	0.0.0.0/0.0.0.0
12	switch	port11	192.168.1.0/255.255.255.0	0.0.0.0/0.0.0.0

Figura 6. Políticas de ruta

3.5 Firewall

Los equipos FortiGate poseen la funcionalidad de firewall basada en tecnología *Stateful Inspection Packet*. Esto le permite hacer un análisis exhaustivo de la cabecera de cada paquete, identificando la sesión a la que pertenece, chequeando el correcto orden de los paquetes y realizando control sobre el tráfico de la red.

Las políticas del firewall controlan todo el tráfico que atraviesa el equipo FortiGate. Cada vez que el Firewall recibe un nuevo paquete, analiza la cabecera de este para conocer las direcciones origen y destino, el servicio al que corresponde ese paquete, y determina si se trata de una nueva sesión o bien pertenece a una sesión ya establecida y llega en el orden correcto. Este análisis de la cabecera es acelerado mediante el Circuito Integrado de Aplicación Específica FortiASIC, lo que permite a las plataformas FortiGate alcanzar un rendimiento mayor y un número de nuevas sesiones por segundo superior al de cualquier solución basada en la utilización de una CPU de propósito general.

Lo primero que hicimos fue agregar a todas las direcciones de los objetos de nuestro Firewall, para esto sólo hay que seguir los siguientes pasos:

1. Nos vamos a **Firewall Objects > Address > Create New**
2. Llenamos los campos solicitados con la información correspondiente de cada uno de nuestros usuarios como se muestra en la Figura 7 y damos click en **OK**



Figura 7. Agregando dirección de usuario al Firewall

En la Figura 8 podemos ver la lista de algunas direcciones que se agregaron:

Name	Address/POOL	Interface	Type	Show in Address List
Fabiola Vargas	10.1.1.102	port12	Subnet	<input checked="" type="checkbox"/>
Fernando Hernández	10.1.1.127	port12	Subnet	<input checked="" type="checkbox"/>
Fernanda Ordo	10.1.1.111	port12	Subnet	<input checked="" type="checkbox"/>
Francisco Sánchez	10.1.1.120	port12	Subnet	<input checked="" type="checkbox"/>
Gabriela Heras	10.1.1.108	port12	Subnet	<input checked="" type="checkbox"/>
Georgina Espindole	10.1.1.104	port12	Subnet	<input checked="" type="checkbox"/>
Gloria Moran Naguel	10.1.1.127	port12	Subnet	<input checked="" type="checkbox"/>
MariBertha Torres	10.1.1.109	port12	Subnet	<input checked="" type="checkbox"/>
IPHONE TONY	192.168.1.207	evbnh	Subnet	<input checked="" type="checkbox"/>
Isabel	10.10.10.40	Ag_Fe01	Subnet	<input checked="" type="checkbox"/>
Isabel Flores	10.1.1.113	port12	Subnet	<input checked="" type="checkbox"/>
José Morales	10.1.1.111	port12	Subnet	<input checked="" type="checkbox"/>
Kania Flores	10.1.1.126	port12	Subnet	<input checked="" type="checkbox"/>
LAN	192.168.1.0/255.255.255.0	evbnh	Subnet	<input checked="" type="checkbox"/>
LAN2	10.1.1.0/255.255.255.0	port12	Subnet	<input checked="" type="checkbox"/>

Figura 8. Lista de direcciones agregadas al Firewall Objects

Lo siguiente que hicimos fue mandar a todas estas direcciones a diferentes grupos, esto con el fin de tener un mejor manejo de todos nuestros usuarios y así brindarles de manera grupal las políticas que más adelante se mencionan. En la Figura 9 podemos ver los grupos en lo que se separamos a todos los usuarios:



Figura 9. Grupos de usuarios en el Firewall Objects

3.6 Antivirus

Se configuraron los perfiles de seguridad para así aplicar las distintas políticas de acceso específico. Estos perfiles de seguridad cuentan con componentes como AntiVirus, Intrusion ProtectionSystem (IPS), WebFiltering, Email filtering, entre otros.

FortiGate ofrece el sistema antivirus perimetral de mayor rendimiento gracias a su optimizada arquitectura y configuración. Los componentes principales del sistema antivirus de FortiGate son:

- La arquitectura hardware basada en FortiASIC
- Su optimizado sistema operativo FortiOS
- La infraestructura FortiProtect, los laboratorios y centros de desarrollo distribuidos a lo largo de todo el mundo.

Si el sistema FortiGate detecta la existencia de un archivo infectado en una transmisión, el archivo es eliminado o guardado en cuarentena, y es sustituido por un mensaje de alerta configurable por el administrador. Además, el equipo FortiGate guarda un registro del ataque detectado, y puede configurarse el envío de un correo de alerta o un trap SNMP.

Para una protección extra, el motor antivirus es capaz de bloquear ficheros de un tipo específico (.bat, .exe, etc) que potencialmente sean contenedores de virus, o bien bloquear aquellos archivos adjuntos de correo electrónico que sean de un tamaño superior al límite de filtrado.

Aquí creamos diferentes perfiles, para crearlo seguimos los siguientes pasos:

1. Nos vamos a **Security Profiles>Antivirus>Profiles**
2. Estando ahí damos click en el icono 
3. Ahí agregamos un nombre para el perfil y las características que deseamos tenga.

En la Figura 10 y 11 podemos observar la configuración del perfil AV_Oriony AV-flow respectivamente que se crearon. Claramente podemos observar los distintos protocolos que se agregan a cada perfil, esto se debe a las distintas necesidades de los usuarios.

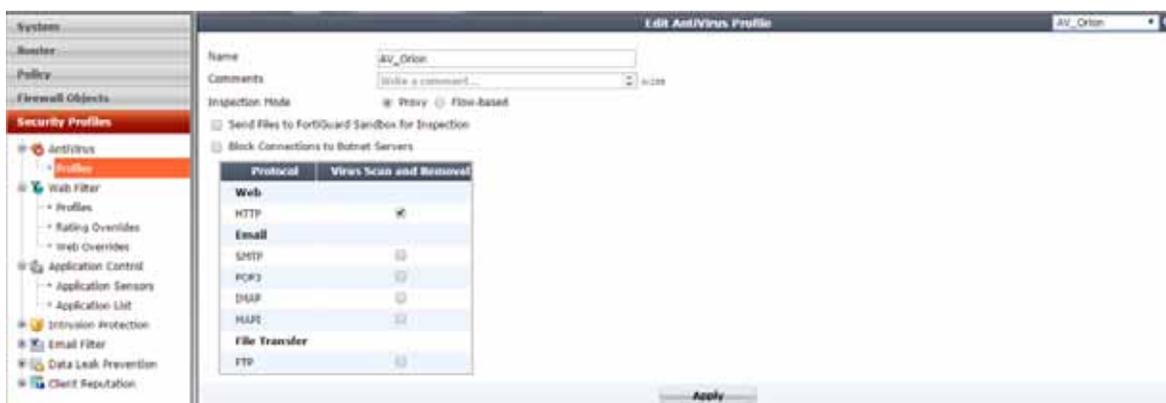


Figura 10. Perfil AV_Orion de Antivirus



Figura 11. Perfil AV_flow de Antivirus

3.7 Filtrado Web

La distribución y visualización de contenido no autorizado supone un riesgo importante para cualquier organización. Para las empresas, la monitorización del uso que sus empleados hacen de los accesos a Internet y la prevención de visualización de contenidos web inapropiados o no autorizados se ha convertido en algo necesario, justificado por los costes financieros y las implicaciones legales que conlleva la pasividad en este aspecto.

El servicio FortiGate web filtering puede ser configurado para escanear toda la cadena del contenido del protocolo http permitiéndonos filtrar direcciones URL potencialmente no asociadas al desarrollo de la normal actividad laboral, contenidos embebidos en las propias páginas web o scripts basados en java, activeX o cookies, contenidos potencialmente peligrosos.

Aquí creamos diferentes perfiles, muy parecido al caso anterior seguimos los siguientes pasos:

1. Nos vamos a **Security Profiles>Web filter>Profiles**
2. Estando ahí damos click en el icono 
3. Ahí agregamos un nombre para el perfil y las características que deseamos tenga.

Ahí agregamos un nombre para el perfil y las elegimos las categorías que queremos que sean bloqueadas. En la Figura 12, 13 y 14 podemos observar los perfiles configurados para nuestros usuarios.

Podemos observar que los dos primeros perfiles tienen las mismas características, con excepción de que en el perfil FW_Orion hacemos la excepción de una página, la cual es necesaria para algunos usuarios, en el tercer perfil que se configuró se bloquean prácticamente todas las categorías, esto con el fin de tener un mayor rendimiento.

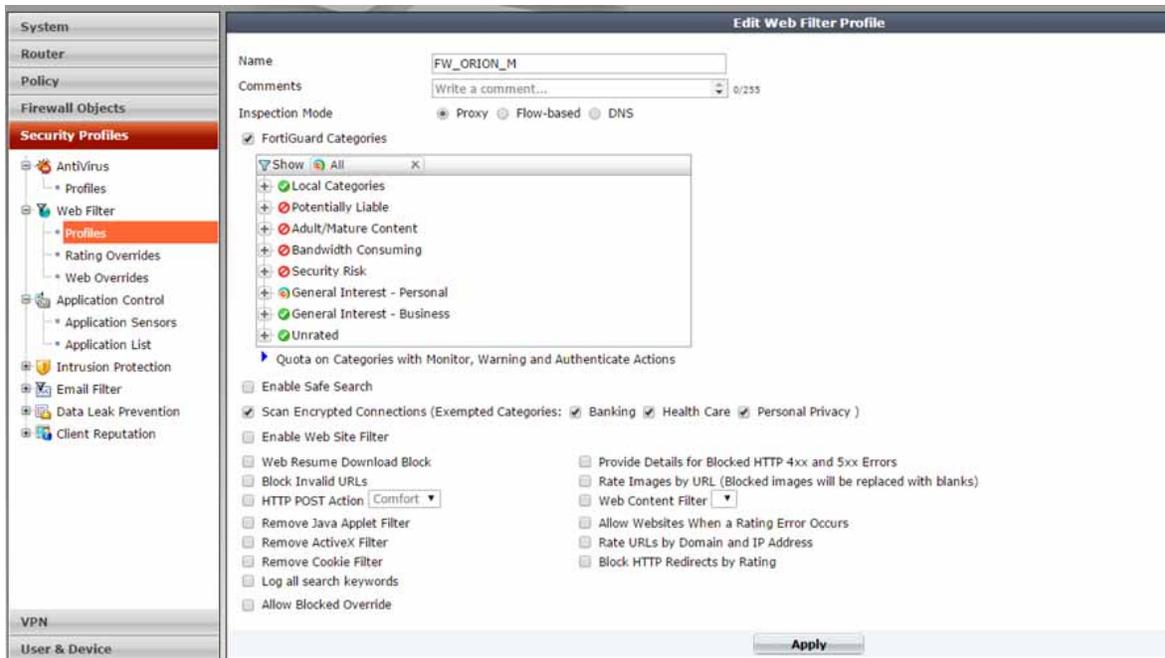


Figura 12. Perfil FW_ORION_M del Filtrado WEB

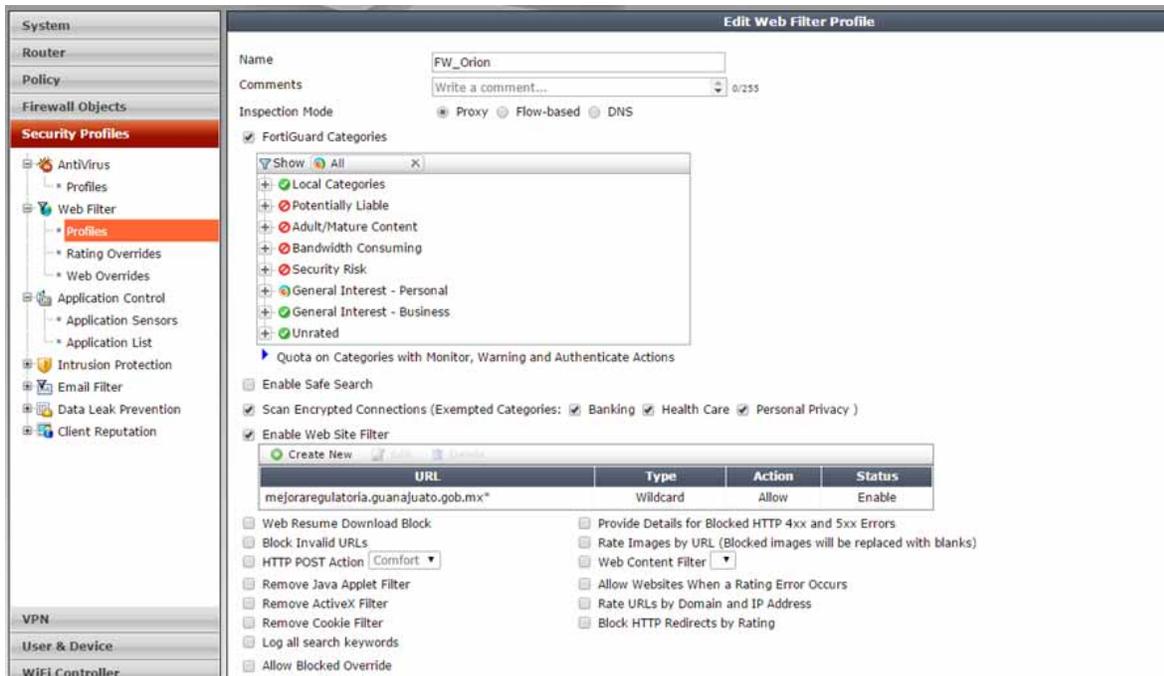


Figura 13. Perfil FW_Orion del Filtrado WEB

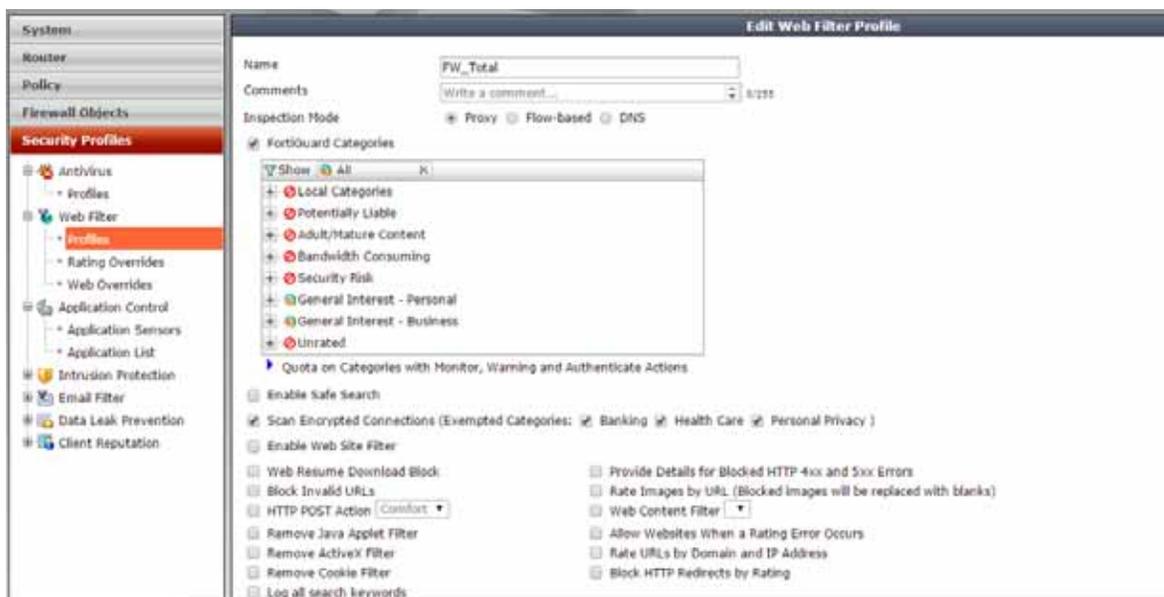


Figura 14. Perfil FW_total del Filtrado WEB

3.8 Calidad de servicio

Mediante la aplicación de técnicas de Calidad de Servicio la red provee un servicio prioritario sobre el tráfico más sensible al retardo. Los equipos FortiGate permiten aplicar técnicas de priorización de tráfico y Calidad de Servicio (QoS), reservar ancho de banda para aquellas aplicaciones que sean más sensibles al retardo, o bien limitar el ancho de banda de aquellas aplicaciones que hagan un uso intensivo de los recursos de la red.

La Calidad de Servicio es una funcionalidad fundamental para poder gestionar el tráfico generado por la transmisión de voz y las aplicaciones multimedia. Estos tipos de tráfico son enormemente sensibles al retardo y a la variación del mismo (jitter).

La configuración de calidad de servicio que hicimos nos permitió la utilización de aplicaciones sin recurrir a una ampliación innecesaria del ancho de banda de la red, y así pudimos reservar el ancho de banda necesario para cada aplicación. Dimos prioridad a este tipo de tráfico ante otros menos sensibles al retardo como fueron el correo o el tráfico ftp.

Los equipos FortiGate proveen calidad de servicio para todos los servicios soportados, incluyendo H.323, SIP, TCP, UDP, ICMP o ESP. La Calidad de Servicio es implementada en las plataformas FortiGate del siguiente modo:

La gestión de ancho de banda se realizó mediante la utilización de buffers que permitieron regular los diferentes flujos de tráfico en base a la velocidad de transmisión de los paquetes. Lo que logramos fue evitar que los paquetes sean descartados, haciendo que se almacenen en el buffer hasta su transmisión, retrasando su envío hasta que sea posible. En este caso activamos la técnica *TokenBucket* para garantizar y limitar el ancho de banda, esto en la parte de Firewall.

- La bufferización se realizó en función de la prioridad asignada a cada flujo, pudiendo variar entre prioridad alta, media o baja. Como el ancho de banda no era suficiente para el envío de todos los paquetes almacenados, se transmitieron en primer lugar los de prioridad alta.
- La tecnología *DiffServ* permitió modificar los parámetros DSCP, siguiendo las normas RFC 2474 y 2475. Así, aquellos componentes de la red compatibles con *DiffServ*, fueron capaces de interpretar la prioridad de los paquetes transmitidos inspeccionando las cabeceras de los paquetes y clasificando, marcando, y gestionando el tráfico en base a esta información.

3.9 Creación de políticas de seguridad

La política define la acción a tomar con aquellos paquetes que cumplan los criterios definidos. Entre las acciones a realizar están:

- Permitir la conexión
- Denegar la conexión
- Requerir autenticación antes de permitir la conexión. La validación de usuario puede realizarse contra usuarios registrados en local, o bien haciendo uso de servidores externos que pueden ser RADIUS, LDAP y/o Directorio Activo.
- Procesar el paquete como perteneciente a una conexión tunelizada mediante IPSec
- Realizar traducción de direcciones
- Aplicar reglas de gestión de ancho de banda
- Analizar el tráfico mediante funcionalidades adicionales de seguridad, como Antivirus, AntiSpam, Detección/Prevención de Intrusiones, filtrado Web, etc. mediante la definición de un perfil de protección

A cada política se le puede definir un horario, tanto único como recursivo, que permite acotar la aplicación de la regla a un espacio temporal determinado en función de la hora, el día de la semana, mes o año.

Cada política permite realizar traducción de direcciones mediante NAT, permitiendo realizar una traducción estática de direcciones, o bien utilizar grupos de direcciones con objeto de realizar NAT dinámico, y así mismo definir traducciones de puertos (PAT). En cada política se puede habilitar el seguimiento de aquellas conexiones que atraviesan el firewall de acuerdo a la política definida, con objeto de poder hacer un registro de las conexiones establecidas a través del equipo.

Creamos varias políticas de seguridad, apoyadas en lo que ya habíamos configurado anteriormente como son los perfiles de antivirus y los de filtrado web.

En la Figura 15, podemos observar varias políticas que fueron creadas. Podemos ver que hacemos uso del perfil de antivirus que creamos llamado AV_Orion y del perfil del filtrado web que llamamos FW_ORION y que se mencionan con anterioridad.

Seq.#	Source	Destination	Schedule	Service	Authentication	Action	AV	Web Filter
Ap_Test (SSID: Orion Wireless) - port11 (INFINITUM6MB) (1 - 2)								
1	AP_ORION	all	always	ALL		Accept	AV_Orion	FW_Orion
2	all	all	always	ALL		Accept	AV_Orion	FW_Orion
Ap_Test (SSID: Orion Wireless) - port12 (Usuarios) (3 - 3)								
3	all	all	always	ALL		Accept		
Ap_Test (SSID: Orion Wireless) - switch (LAN) (4 - 4)								
4	all	all	always	ALL		Accept	AV_Orion	FW_Orion
port10 (TELMEX_DEDICADO) - switch (LAN) (5 - 6)								
5	ATAQUE	all	always	ALL		Deny		
	ATAQUE2							
	ATAQUE3							
	ATAQUE4							
	ATAQUE5							
	ATAQUE6							
6	all	VPN192.168.1.6				SSL-VPN		
port12 (Usuarios) - Ap_Test (SSID: Orion Wireless) (7 - 7)								
7	all	all	always	ALL		Accept		
port12 (Usuarios) - port11 (INFINITUM6MB) (8 - 12)								
8	WEBSNFSE	all	always	ALL		Deny		
9	Filtrado total	all	always	ALL		Accept	AV_Orion	FW_Orion
10	Filtrado_Lan10	all	always	ALL		Accept	AV_Orion	FW_Orion
11	Sin filtrado_LAN 10	all	always	ALL		Accept		
12	all	all	always	ALL		Accept	AV-flow	FW_Orion

Figura 15. Políticas de seguridad.

Para poder crear cada política llenamos cada campo que se muestra en la Figura 16.

Edit Policy

Policy Type: Firewall (selected) | VPN

Policy Subtype: Address (selected) | User Identity | Device Identity

Incoming Interface: port12 (Usuarios)

Source Address: Brian Lap 209

Outgoing Interface: port15 (TESTNETGEAR)

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Enable NAT

- Use Destination Interface Address
- Use Dynamic IP Pool

Fixed Port

Click to add...

Logging Options

- No Log
- Log Security Events
- Log all Sessions

Security Profiles

- AntiVirus: AV_Orion
- Web Filter: default
- Application Control: default
- IPS: default
- Email Filter: default
- DLP Sensor: default
- Proxy Options: default
- SSL/SSH Inspection: default

Figura 16. Campos de la configuración de cada política

Capítulo 4

Resultados y conclusiones

4.1 Resultados

El principal objetivo de este proyecto fue la seguridad de la red corporativa, con todas las implementaciones y configuraciones logramos cumplir este objetivo. Ahora todos los usuarios de la red en la empresa Grupo Orion se encuentran organizados de mejor manera y así mismo cuentan con una mayor seguridad en su red, esto debido a los antivirus que se activaron, a los perfiles creados para los diferentes tipos de usuarios, así como el tráfico WEB. Con este último que se llevó a cabo tenemos mayor rendimiento laboral por parte de los usuarios, ya que se encuentran limitados de ver diferentes categorías de páginas.

Con todo el trabajo realizado logramos tener en Grupo Orion los siguientes 3 puntos:

- 1) Seguridad completa y consolidada
- 2) Alto Rendimiento
- 3) Alerta contra amenazas

Al organizar a nuestros usuarios en grupos, ahora es más fácil atender ciertos problemas y verificar desde el FortiGate que todo marche bien. En el caso de un usuario necesite revisar una página que se encuentra bloqueada, sólo basta que lo diga para que desde el FortiGate podamos darle acceso a dicha página, esto claro conociendo su dirección IP.

Con la creación de las VLAN'S para los enlaces y la red interna se logró distinguir la ubicación de manera más sencilla, con la creación de la VPN a través de Fortinet se logró ahorrar comprar la licencia de la herramienta HOB, así mismo mejora el redimiendo del usuario hacia el servidor.

En la Figura 17 podemos observar la manera en que nuestros usuarios se encuentran organizados:

Group Name	Members			
AP_ORION 4 Members	Brian Wireless	Isabel	Lic. Pacheco	Pablo_AP
Aplicativos 1 Members	104			
Filtrado total 1 Members	Fernando Hernández			
Filtrado_Lan10 21 Members	Alejandra Serrano Archivo_PC2 Fernando Ortiz José Morales Mauricio Castillo Veronica Grupo Urban	Ana Elia Perez Diego Santiago Francisco Sánchez Lilia León Noe Grupo Urban	Ana Perez Erika Johana Gabriela Marin Liliana Hernandez Ricardo Moreno	Archivo_PC1 Fabiola Vargas Georgina Espindola Lucia Morales Tonatuu Alfaro
Sin filtrado_LAN 10 14 Members	Ale Salas LapTop Brian Lap 209 Kania Flores Rocio	Alejandra Rodriguez Carmen Geronimo Lic.Tere Rocha Sistemas_PC	Alejandra Salas Gloria Moran Moguel Patricia Fuentes	Bernardino Pacheco Isabel Flores Pedro de Santiago
VPN_Network 2 Members	VPN192.168.1.0	VPN_10.1.1.0		
VPN_SSL 1 Members	VPN192.168.1.0			
WEBSense 4 Members	53	60	149	Synology

Figura 17. Organización de nuestros usuarios.

4.2 Conclusiones

Como hemos visto la seguridad en las redes se ha convertido en un factor importante en el diseño e implementación de las redes. El administrador de la red debe estar constantemente implementando medidas de seguridad en la red con el fin de tener una red confiable y estable. Como ya sabemos, las amenazas informáticas ponen en riesgo nuestra red y la integridad de la información. Es por eso, que se tomaron medidas tales como la configuración del firewall, la creación de perfiles, la creación de políticas de seguridad, entre otras.

Crear los perfiles en el equipo FortiGate nos fue de gran ayuda ya que pudimos manejar la red de manera más ordenada y con esto obtuvimos un mayor rendimiento; el definir distintos segmentos de red, aislados de la mayoría de los usuarios y con pocos privilegios, nos permitió tener un control más preciso para estos tipos de usuarios.

Con base en lo anterior, es posible concluir que la seguridad debe ser contemplada de un modo global, protegiendo a la red de cualquier tipo de ataque y del uso indebido o el desaprovechamiento de los recursos.

Finalmente, la elaboración de este proyecto ha sido una experiencia que ha permitido ampliar mi nivel de conocimientos, y reafirmar mi interés, en el campo de las redes de computadoras.

Capítulo 5

Bibliografía y anexos

4.1 Bibliografía

Zhihu Wang. "Design and realization of computer network security perception control system" Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, pp. 482-487, noviembre 2011.

Andrew S. Tanenbaum. "Redes de computadoras" Pearson Educación, pp. 891, 2003.

FortiGate Cookbook "A practical Guide to Getting the best from Your FortiGate", Fortios 5.0, May 2014.

4.2 Anexos

Una de las actividades extras que se hicieron en este proyecto y que considero importante mencionar fue el cambio de cableado que se hizo en la red de la empresa, a continuación se muestro los detalles:

Objetivo general

- Cambiar el cableado estructurado en el rack

Objetivos específicos

- Ubicar los nodos de los enlaces, los usuarios y los servidores.
- Identificar a cada usuario.

Resulta más frecuente de lo que parece encontrar racks con todos los cables puestos de cualquier manera. Este tipo de racks suelen presentar problemas precisamente por su caos. Por un lado los servidores se calientan más por el menor flujo de aire, por lo que los componentes se estropean antes.

Por otro lado si se desea hacer algún cambio es más probable que la persona que lo haga toque sin querer algún cable y desconecte algún equipo, ya sea la alimentación o la red.

El rack se encontraba en las siguientes condiciones:



Figura 18. Rack en malas condiciones



Figura 19. Rack en malas condiciones

En la Figura 18 y 19 se puede apreciar como los cables de red se han colocado de cualquier manera.

Para evitar todas estas complicaciones y tener un mayor rendimiento en la red se modificó el cableado y se identificaron los enlaces, los servidores y los usuarios. Al reordenar el rack se facilitó tanto la refrigeración como la facilidad de operación de los servidores, así como también la ubicación de cada uno de los usuarios.

En la Figura 20 se muestra como quedó el rack después de reordenarlo:



Es importante mencionar las siguientes observaciones:

Para identificar de manera más sencilla se usaron cables de red de diferente color:

- Los cables de color rojo identifican a los usuarios.
- Los cables de color azul identifican los servidores.
- Los cables de color amarillo son tesorería.
- Los cables de color blanco son enlaces.