UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Migración de la configuración de un Dispositivo de Gestión Unificada de Amenazas como Solución de Seguridad en Red

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A

José Carmen Hernández Padrón

ASESOR DE INFORME

Ing. Cruz Sergio Aguilar Díaz

Ciudad Universitaria, Cd. Mx., 2018

Índice

ÍNDICE DE ILUSTRACIONES

INTRODUCCIÓN

Introducción

La seguridad informática tiene por objetivo mantener la integridad, confidencialidad y disponibilidad de la información, por lo que es un tema de interés creciente en las organizaciones debido a la gran importancia que tiene la protección de la información.

Asimismo, existen un sinfín de soluciones de seguridad que le permiten a una organización proteger su información entre las cuales se cuenta con la seguridad perimetral.

La seguridad perimetral tiene por objetivo proteger de amenazas externas a todo sistema informático, utilizando para ello mecanismos de seguridad como lo son dispositivos de gestión unificada de amenazas (UTM, por sus siglas en inglés) que permiten fortalecer la seguridad, así como disponer de un monitoreo de la red. Dichos dispositivos UTM ofrecen una solución de seguridad integral en un solo punto de la red de una organización contra ataques externos.

La Coordinación de Seguridad de la Información (CSI) /UNAM-CERT, tiene implementada seguridad perimetral dentro de sus instalaciones haciendo uso de diversos dispositivos y soluciones de seguridad entre los cuales se encuentra un UTM el cual es una pieza fundamental para la protección de los sitios y servicios que administra.

Por lo anterior, el contenido del siguiente informe de Trabajo Profesional describe las actividades relativas a la migración de la configuración de un dispositivo UTM dentro de la CSI/UNAM-CERT.

CAPÍTULO 1

Descripción de la Organización

CAPÍTULO 1 – Descripción de la Coordinación de Seguridad de la Información/UNAM-CERT

La Coordinación de Seguridad de la Información (CSI)/UNAM-CERT, como parte de la Dirección de Sistemas y Servicios Institucionales dentro de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM, es un punto de encuentro al cual puede acudir la comunidad de cómputo para obtener información, asesorías y servicios de seguridad; así como para intercambiar experiencias y puntos de vista a través de seminarios, pláticas, investigaciones, logrando con ello, establecer políticas de seguridad adecuadas, disminuir la cantidad y gravedad de los problemas de seguridad y difundir la cultura de la seguridad en cómputo.

1.1 Misión

Contribuir al desarrollo de la UNAM, a través de la prestación de servicios especializados, la formación de capital humano y el fomento de la cultura de seguridad de la información.[1]

1.2 Visión

Consolidar a la UNAM como la entidad líder en materia de Seguridad de la Información en el país.

1.3 Objetivos

La CSI/UNAM-CERT tiene por objetivos[2] los siguientes puntos:

- Proporcionar servicios de seguridad de la información para la UNAM y otras organizaciones.
- Promover la cultura de seguridad de la información.
- Formar especialistas que desarrollen y apliquen estrategias de protección de la información.
- Difundir contenidos especializados en seguridad de la información.
- Colaborar con instituciones nacionales e internacionales en materia de detección y respuesta a incidentes.

[1] Seguridad UNAM (2018), Recuperado de: https://www.seguridad.unam.mx/mision-y-vision
[2] Seguridad UNAM (2018), Recuperado de: https://www.seguridad.unam.mx/objetivos

- Elaborar políticas y lineamientos de seguridad de la información para las dependencias y entidades académicas universitarias.

1.4 Historia

La historia de lo que hoy en día se conoce como Coordinación de Seguridad de la Información/UNAM-CERT se desarrolla desde hace más de 30 años como se muestra a continuación:

1975.- En una entrevista realizada al Sr. Rafael Durán, el entonces jefe de Departamento de Operación de DGSCA (Dirección General de Servicios de Cómputo Académico), por Diego Zamboni en 1995, se mencionaron los primeros problemas relacionados con la seguridad en cómputo en RED-UNAM. A continuación, se muestra un fragmento de la mencionada tesis de Diego Zamboni:

> *"Desde 1975 se tenían problemas de seguridad en cómputo. Estos eran con los sistemas Burroughs. Ya había en ese entonces en la Universidad gente con la capacidad y el interés de romper las barreras de seguridad impuestas por el sistema, por "el simple gusto de hacerlo". Contra estas violaciones de seguridad nunca fue posible tomar alguna acción formal debido a la falta de legislación al respecto, así como las fricciones y conveniencias políticas que, desgraciadamente, siempre han invadido los ámbitos académicos y científicos en nuestra Universidad".* [3]

1993.- La supercomputadora Cray Y-MP4/46, propiedad de la DGSCA, es vulnerada y ocurre una intrusión no autorizada, no fue hasta ese suceso que el personal directivo de la DGSCA se percata de la importancia de la seguridad en cómputo y decide crear el equipo de respuesta a incidentes que más adelante se convertiría en lo que hoy se conoce como Coordinación de Seguridad de la Información/UNAM-CERT.
Por lo anterior, la UNAM contacta por primera vez con el Coordination Center de Carnellie Mellon de Estados Unidos (CERT/CC), siendo este último el primer equipo de respuesta a incidentes de todo el mundo.

1994.- Se organiza la primera edición del Día Internacional en Cómputo (DISC) en México por parte del Área de Seguridad en Cómputo.

1995.- Se agrega el módulo de especialización "seguridad en cómputo" en el plan de becarios de supercómputo.

[3] ZAMBONI, Diego, Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix [en línea], Facultad de Ingeniería UNAM 1995. Formato PDF, Disponible en Internet: http://homes.cerias.purdue.edu/~zamboni/pubs/thesis-bs.pdf.

1999.- El Área de Seguridad en Cómputo se convierte en el Departamento de Seguridad en Cómputo gracias a la integración de Juan Carlos Guel como jefe, los recursos asignados a la organización aumentan, tanto en el ámbito material como en el del personal.
En ese mismo año el ingeniero Rubén Aquino Luna ingresa como becario en supercómputo con especialidad en seguridad en cómputo.

1999 – 2001.- Se tramita la acreditación ante FIRST (Forum of Incident Response Security Teams), acreditación que le permitió al equipo de respuesta a incidentes ser reconocido internacionalmente debido a que hasta ese momento no existía ningún equipo de respuesta a incidentes en México con reconocimiento internacional. La acreditación le permitió a UNAM-CERT tener presencia en grupos nacionales e internacionales.

2003.- Con la colaboración de la ANUIES (Asociación Nacional de Universidades e Instituciones de Educación Superior) se crea la iniciativa de extender la seguridad de la información a nivel nacional y nace la Red Nacional de Seguridad en Cómputo (RENASEC), albergando y distribuyendo acuerdos y noticias en materia de seguridad informática a más de 145 Instituciones de Educación Superior del país.

2010.- El Departamento de Seguridad en Cómputo se convierte en la Subdirección de Seguridad de la Información durante la dirección del Ing. Rubén Aquino Luna, en ese mismo año se obtiene la certificación ISO 27001:2005, estándar que específica los requisitos mínimos necesarios para implementar un sistema de gestión de la seguridad de la información.

2011.- Obtiene la recertificación del estándar ISO 27001:2005 en el proceso de atención y respuesta a incidentes.

2014.- La Subdirección de Seguridad de la Información se convirtió en la Coordinación de Seguridad de la Información o también conocida como CSI/UNAM-CERT.

2015.- Se obtiene la certificación de la actualización del estándar ISO 270001:2005 al ISO 270001:2013.

1.5 Servicios

La CSI/UNAM-CERT proporciona a la comunidad universitaria y externa servicios de información a través de portales web, como lo son seguridad.unam.mx, revista.seguridad.unam.mx, proyecto Honeynet, publicación de noticias y boletines

informativos, entre otros. Asimismo, resguarda información confidencial derivada de convenios con otras dependencias dentro y fuera de la misma Universidad Nacional Autónoma de México

Por otro lado, la CSI/UNAM-CERT cuenta con un Congreso de Seguridad en Cómputo y un Plan de Becarios en Seguridad Informática los cuales tienen por objetivo dar capacitación, tanto a personal interno como externo, en temas de seguridad.

1.6 Estructura organizacional

La CSI/UNAM-CERT como parte de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) tiene la siguiente estructura departamental (véase Ilustración 1.1):

- Auditoría y Nuevas Tecnologías
- Detección y Respuesta a Incidentes
- Operación Interna
- Seguridad en Sistemas
- Gestión de Proyectos y Capacitación

Cabe destacar que me desempeñé como “Especialista en Seguridad en Red” dentro del departamento de Operación Interna durante el periodo que comprende de septiembre de 2014 a marzo de 2016.

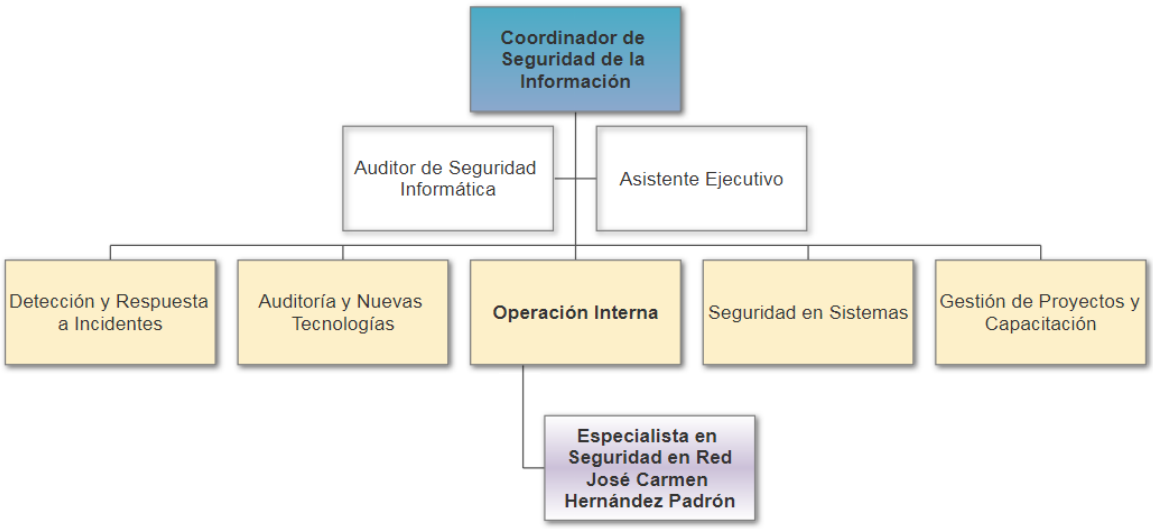

ILUSTRACIÓN 1.1 ORGANIGRAMA CSI/UNAM-CERT

CAPÍTULO 2

Descripción del Puesto de trabajo

CAPÍTULO 2 – Descripción del Puesto de Trabajo

2.1 Antecedente al puesto de trabajo

Durante mi último semestre de la carrera de Ingeniería en Computación, en el módulo de salida de redes y seguridad, ingrese a la octava generación del Plan de Becarios en Seguridad Informática de la CSI/UNAM-CERT, en el cual, haciendo uso de los conocimientos adquiridos en la ya mencionada carrera pude finalizarlo.

La CSI/UNAM-CERT buscaba personal con un perfil enfocado a la seguridad informática en temas de redes, por lo cual participé en el ingreso a dicho puesto, utilizando los conocimientos adquiridos durante la carrera, así como los adquiridos en el Plan de Becarios cumplí con las habilidades requeridas, siendo así, ingresé al puesto de Especialista en Seguridad en Red en septiembre de 2014 después de haber sido becario del Plan de Becarios en Seguridad Informática en su octava edición.

2.2 Funciones del puesto de Especialista en Seguridad en Red

Dentro del Departamento de Operación Interna el puesto de Especialista en Seguridad de Red tiene la siguiente función principal:

Implementación de procesos y dispositivos para la protección perimetral y monitoreo de redes.

Los conocimientos requeridos para el puesto ya enunciado son los siguientes:

- Manejo de sistema operativo linux.
- Conocimientos de administración de redes.
- Conocimientos de protección perimetral.
- Conocimientos de seguridad de la información.

Asimismo, la formación académica requerida para desempeñarse en el puesto es la siguiente:

- Licenciatura o estudiantes de los últimos semestres en Ingeniería en Computación, Ingeniería en Telecomunicaciones o carreras afines.

2.3 Actividades del puesto Especialista en Seguridad en Red

Mis principales actividades dentro de la CSI/UNAM-CERT como Especialista en Seguridad en Red fueron las siguientes:

- Evaluar, configurar y administrar dispositivos de protección perimetral, como lo son switches, routers, puntos de acceso, balanceadores de carga, firewalls y módems,

- Monitorear y administrar las cámaras de seguridad que resguardan las instalaciones de la CSI/UNAM-CERT,
- Configurar y administrar las reglas de firewall de la red interna,
- Asignación y revocación del acceso de equipos de cómputo a la red interna,
- Evaluar e instalar soluciones de red dentro de la infraestructura interna y
- Establecer los dispositivos y procesos que aseguren el monitoreo de red.

Lo anterior con el fin de mantener en un nivel aceptable la seguridad interna de la Red contra posibles ataques externos que pudieran suscitarse.

2.4 Formación Académica

A continuación, listo mi formación académica:

Fechas:	2010/2014
Estudios:	Ingeriría en Computación/Redes y Seguridad
Centro:	Ciudad Universitaria Facultad de Ingeniería
Fechas:	2013/2014
Estudios:	Seguridad Informática
Centro:	UNAM-CERT (Equipo de Respuesta a Incidentes de Seguridad en Cómputo)
Fechas:	Abril 2015
Estudios:	Curso: Fortigate Multi-Threat Security Systems I y Fortigate Multi-Threat Security Systems II
Centro:	Westcom
Fechas:	Abril 2015
Certificación:	CEH: Certified Ethical Hacking
Centro:	EC-Council
Fechas:	Julio 2015
Estudios:	Diplomado en tecnologías IP
Centro:	INTTELMEX
Fechas:	Febrero 2016
Certificación:	ITIL Foundations v3
Centro:	INTTELMEX
Fechas:	Julio 2016
Certificación:	Audito Líder ISO/IEC 27001:2013

- Sistema de Gestión de Seguridad de la Información 2.1
- Líder de Equipos de Auditoría 2.0
- Auditoría de Sistemas de Gestión 2.0

Centro: BSI Group México

2.5 Formación Profesional

A continuación, listo la formación profesional en la cual me he desempeñado a la fecha:

Fechas: Septiembre 2014 – Marzo 2016
Empresa: Coordinación de Seguridad de la Información/UNAM-CERT
Puesto: Especialista en Seguridad en Red
Descripción: Implementación de procesos y dispositivos para la protección perimetral y monitoreo de redes.
Evaluar tecnología de protección perimetral. Configurar y administrar dispositivos de protección perimetral. Establecer dispositivos y procesos para el monitoreo de red.

Fechas: Abril 2016 – Diciembre 2016
Empresa: Coordinación de Seguridad de la Información/UNAM-CERT
Puesto: Auditor de Seguridad Informática
Descripción: Evaluar controles de seguridad existentes.
Identificar las nuevas amenazas y realizar las observaciones correspondientes.
Realizar auditorías de seguridad informática. Analizar nuevos controles de seguridad de la información. Evaluar mejores prácticas de seguridad y su relación con el ISO/IEC 27001:2013.

Fechas: Enero 2017 – Diciembre 2017
Empresa: Instituto Nacional Electoral (INE) – Unidad Técnica de Servicios de Informática (UNICOM)
Puesto: Ingeniero Especialista en Seguridad Informática A5
Descripción: Coordinar y actualizar los estándares internos en materia de seguridad informática que permitan robustecer el esquema de protección de los servicios e infraestructura de Tecnologías de la Información.

Apoyar en la creación de estrategias de protección para los sistemas y servicios informáticos y gestionar las actividades que deriven de la misma.
Establecer la planeación y verificación para la realización de escaneos de vulnerabilidades y pruebas de penetración a equipos críticos de forma periódica o a petición de otras áreas.
Investigar las tendencias respecto a los nuevos tipos de ataques informáticos a efecto de identificar las nuevas amenazas y determinar un plan de respuesta apropiado.
Integrar y dar seguimiento a los planes de implementación de los mecanismos de seguridad que permitan tener un nivel óptimo de protección para los sistemas y servicios informáticos.

Atender la promoción de la cultura de la seguridad a todas las áreas del Instituto Nacional Electoral.

Fechas: Enero 2018 – a la fecha

Empresa: Instituto Nacional Electoral (INE) – Unidad Técnica de Servicios de Informática (UNICOM)

Puesto: Ingeniero Especialista en Seguridad Informática C

Descripción: Coordinar y actualizar los estándares internos en materia de seguridad informática que permitan robustecer el esquema de protección de los servicios e infraestructura de Tecnologías de la Información.

Apoyar en la creación de estrategias de protección para los sistemas y servicios informáticos y gestionar las actividades que deriven de la misma.

Establecer la planeación y verificación para la realización de escaneos de vulnerabilidades y pruebas de penetración a equipos críticos de forma periódica o a petición de otras áreas.

Investigar las tendencias respecto a los nuevos tipos de ataques informáticos a efecto de identificar las nuevas amenazas y determinar un plan de respuesta apropiado.

Integrar y dar seguimiento a los planes de implementación de los mecanismos de seguridad que permitan tener un nivel óptimo de protección para los sistemas y servicios informáticos.

Atender la promoción de la cultura de la seguridad a todas las áreas del Instituto Nacional Electoral.

CAPÍTULO 3

Proyecto Migración de la configuración de un Dispositivo de UTM como Solución de Seguridad perimetral en la Red de la CSI/UNAM-CERT

Capítulo 3 – Proyecto Migración de la configuración de un Dispositivo de UTM como Solución de Seguridad perimetral en la Red de la CSI/UNAM-CERT

3.1 Antecedentes

La CSI/UNAM-CERT proporciona a la comunidad universitaria y externa servicios de información a través de portales web, como lo son seguridad.unam.mx, revista.seguridad.unam.mx, proyecto Honeynet, publicación de noticias y boletines informativos, entre otros. Asimismo, resguarda información confidencial derivada de convenios con otras dependencias dentro y fuera de la misma Universidad Nacional Autónoma de México.

El fortalecimiento de la seguridad en la red dentro de la CSI/UNAM-CERT es importante para mantener la disponibilidad, integridad y confidencialidad de los servicios de información, tanto públicos como internos, que administra, por tal motivo se adquirió un dispositivo de Gestión Unificada de Amenazas que da soporte y protección a dichos servicios. Sin embargo, el dispositivo UTM se encuentra en las últimas etapas de soporte, por lo que se solicitó la adquisición de un nuevo dispositivo que permita dar continuidad a la protección de los servicios de información, la red interna y externa, así como contar con la detección y prevención de amenazas de manera oportuna.

3.2 Necesidades

Las características necesarias con los que debe contar el UTM que reemplazará al actual deberán ser por lo menos las siguientes:

- Filtrado de datos basado en reglas y políticas de firewall que permitan y excluyan el flujo de datos.
- Filtrado de sitios web que bloquee o permita la carga del contenido de los sitios mediante el uso de listas negras y blancas para bloquear y permitir.
- Configuración de una red privada virtual para la conexión segura desde una red pública.
- Detección y prevención de intrusos, así como la gestión de tráfico hacia la red interna.

- Catalogación del tráfico en la red interna que permita asignar ancho de banda a las conexiones desde y hacia afuera de la red interna.
- Configuración de perfiles lectura y escritura para la administración del UTM.

3.3 Problemática y objetivo

La CSI/UNAM-CERT requería que la configuración del nuevo dispositivo UTM fuera compatible con la estructura de la red interna, en este sentido las configuraciones del dispositivo UTM que fue reemplazado se modificaron, actualizaron y/o eliminaron para que se amoldarán a las nuevas características del nuevo dispositivo, tanto de software como de hardware.

3.3.1 Objetivo General

Reemplazar el dispositivo UTM con el que contaba la CSI/UNAM-CERT mediante la instalación y configuración de un nuevo dispositivo UTM en la red interna de manera satisfactoria, correcta y segura, tomando como base la configuración existente del dispositivo UTM que fue remplazado, con el objeto preservar la seguridad perimetral.

3.3.2 Objetivos Particulares

A continuación, se listan los objetivos específicos respecto a la realización de las actividades para llevar el proyecto de migración de manera satisfactoria.

- Reconocimiento de las necesidades de la CSI/UNAM-CERT para instalar un nuevo dispositivo UTM.
- Migrar de manera eficiente las configuraciones del UTM que se reemplazó al nuevo UTM.
- Instalación y puesta a punto del nuevo UTM en la red interna de la CSI/UNAM-CERT.

3.4 Desarrollo del proyecto

Las actividades que realicé de migración, configuración e instalación del nuevo dispositivo UTM las llevé a cabo entre julio y agosto de 2015.

3.4.1 Características principales del dispositivo UTM

Para dar cumplimiento al objetivo, tuve que investigar y conocer aspectos más específicos de las configuraciones y del hardware de los dispositivos UTM. A continuación, mencionó los aspectos relevantes que tomé en cuenta respecto a las configuraciones.

Los principales modos de configuración de los dispositivos UTM son los siguientes:

- Firewall: Sistema diseñado para el filtro de datos entre la red interna y externa, basándose en reglas y políticas para permitir y excluir el flujo de los datos.
- Filtrado de contenido: Controla el contenido de los sitios web que puede visitar un cliente, para esto utiliza dos listas, una lista blanca donde se encuentran los sitios permitidos y una lista negra en donde se encuentran los sitios bloqueados.
- VPN: La Red Privada Virtual es una infraestructura segura que trabaja sobre una red pública, como lo es internet, para conectar usuarios a la red interna a través de un acceso público.
- Antivirus: Software para la detección de virus con la capacidad de neutralizar sus efectos.
- Anti-spam: Método de prevención contra el correo basura.
- Detección y prevención de intrusos y gestor de tráfico: La detección de intrusos es una técnica que analiza la actividad de los servicios y de la red en busca de comportamientos anómalos para así poder emitir una alerta, por otro lado, la prevención de intrusos al encontrar un comportamiento anómalo tiene la capacidad de analizarlo y bloquearlo, asimismo, la gestión del tráfico permite analizar y caracterizar el tráfico de red.
- Balanceo de carga: Sistema que permite asignar la entrada de solicitudes, mediante un algoritmo, de los clientes entre los servidores existentes con el fin de minimizar tiempos de carga y evitar la saturación de dichos servicios.
- Alertas por e-mail: Sistema que permite el envío de alertas de seguridad a través de un correo electrónico.

Uno de los puntos más importantes que tomé en cuenta fueron las características de configuración de las políticas de Firewall las cuales permiten bloquear y/o dar acceso a los distintos tipos de tráficos de red, a continuación, mencionó los puntos para su creación:

- Interfaz entrante (Incoming Interface)
- Dirección de origen (Source Address)
- Usuario(s) origen (Source User(s))
- Tipo de dispositivo origen (Source Device Type)
- Interfaz de salida (Outgoing Interface)
- Dirección de destino (Destination Address)

- Horario (Schedule)
- Servicio (Service)
- Acción (Action)

Perfiles de seguridad (Security Profiles).

- Filtrado Web (Web Filter)
- Control de Aplicaciones (Application Control)
- IPS (Por sus siglas en inglés, Sistema de Prevención de Instrusos)
- Filtrado de correo electrónico (Email Filter)
- Inspección SSL/SSH (SSL/SSH Inspection)

Catalogación de tráfico.

- Shared Shaper. - Permite asignar ancho de banda a las conexiones hacia afuera de la red
- Reverse Shaper. - Permite asignar ancho de banda a las conexiones hacia adentro de la red
- Per-IP Shaper. - Permite asignar ancho de banda a las direcciones IP de origen

Opciones de registro.

- Eventos de seguridad (Security Events)
- Todas las sesiones (All Sessions)

En la Ilustración 3.1 se muestra la interfaz del dispositivo UTM en la cual se configuran las políticas.

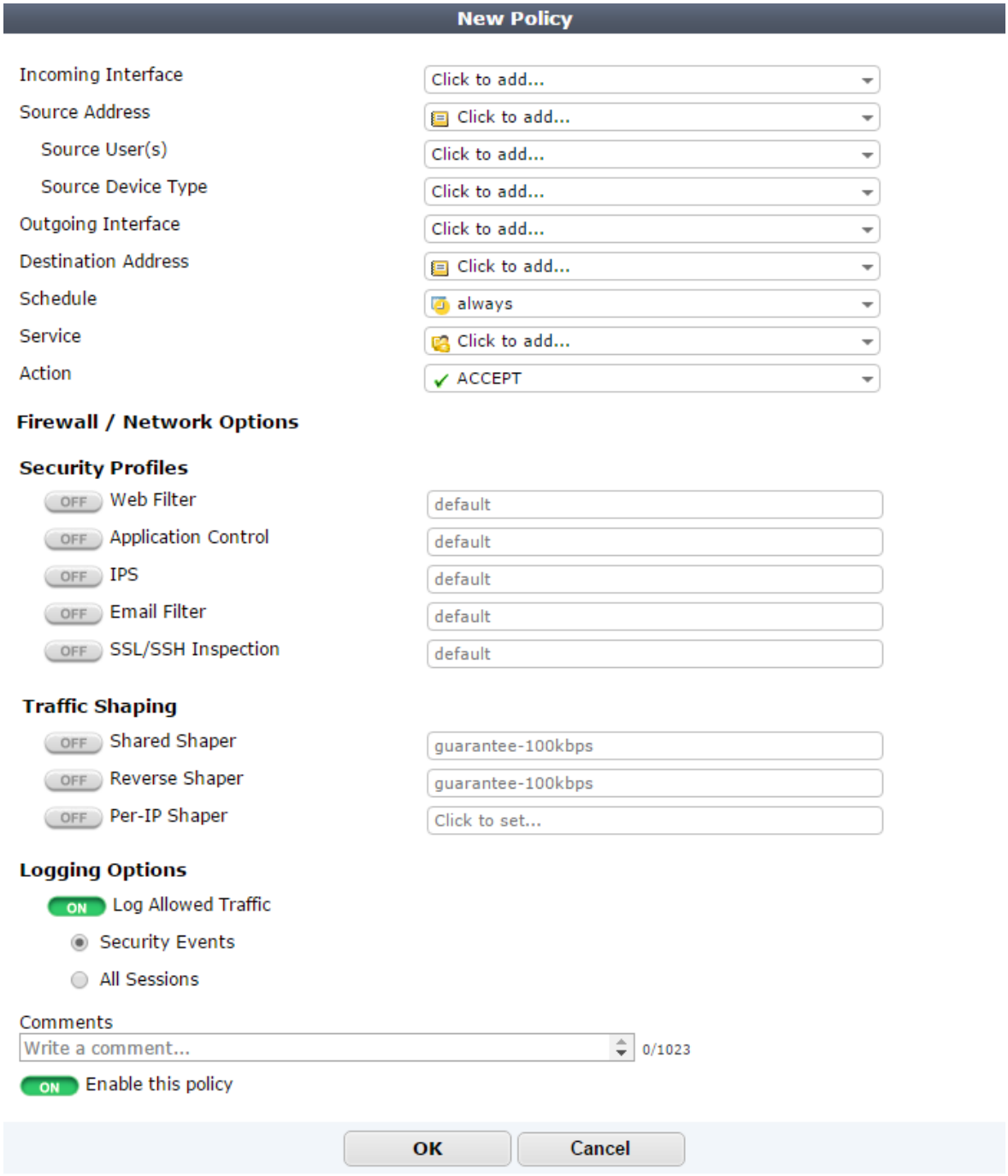

ILUSTRACIÓN 3.1 INTERFAZ PARA LA CREACIÓN DE UNA NUEVA POLÍTICA

3.4.1 Consideraciones iniciales para la migración de la configuración

Las consideraciones que tomé en cuenta para dar inicio con las actividades de migración fueron las siguientes:

- Los cambios significativos entre el dispositivo UTM que fue reemplazado y el nuevo son que cambiaron las interfaces de salida y entrada del hardware, asimismo, se añadieron características nuevas de configuración las cuales no impactan en gran medida la migración de las configuraciones debido a que hasta el momento del cambio no se utilizaban.
- La configuración del nuevo dispositivo UTM la realicé fuera de línea, cuando aún no se encontraba conectado a la red, gracias a un software del fabricante que me permite entrar como administrador en una sesión web del dispositivo.

3.4.2 Migración lógica

Backup de la configuración.

Para proteger la disponibilidad de los servicios del UTM llevé a cabo el respaldo de las configuraciones del dispositivo UTM que fue reemplazado de la siguiente manera.

La recopilación de la configuración la llevé a cabo utilizando la función Backup que poseen los dispositivos UTM, esto me garantizó que en caso de tener algún inconveniente durante la migración de dichas configuraciones pudiera regresar a la configuración anterior. Para crearlo seleccioné **Dashboard**, **Status** y **Backup** como se muestra en la Ilustración 3.2.

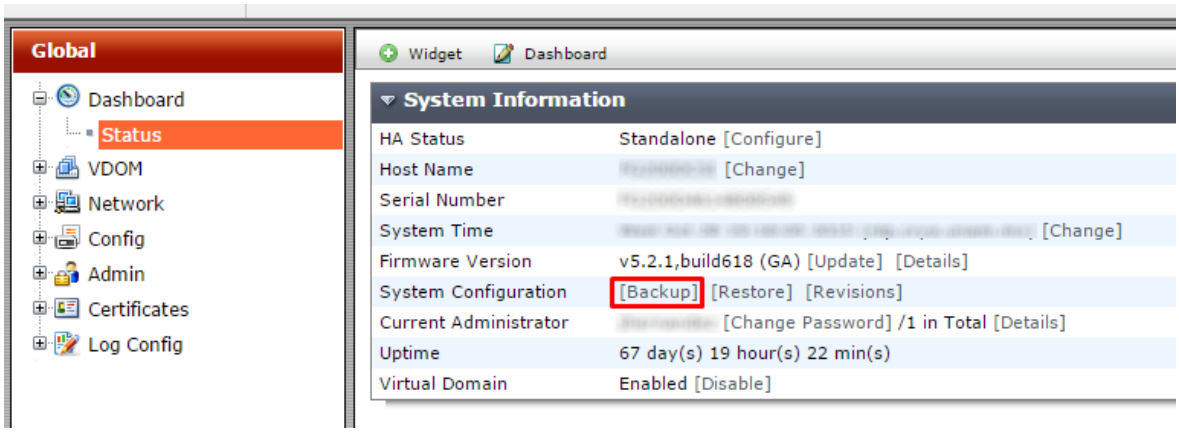

ILUSTRACIÓN 4.2 INTERFAZ GLOBAL

En seguida apareció la siguiente ventana que se muestra en la Ilustración 3.3, en la cual seleccioné **Full Config** para obtener las configuraciones completas y después seleccioné **Backup** para descargar dicha configuración en la PC local.

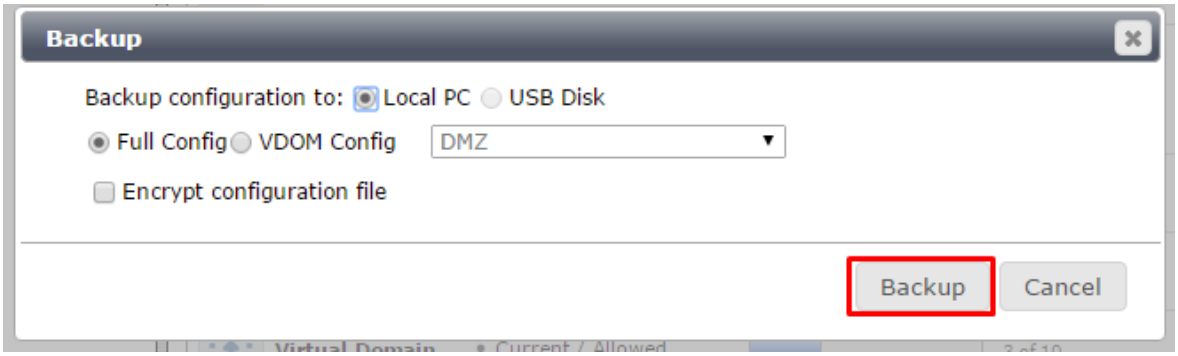

ILUSTRACIÓN 3.3 BACKUP DE CONFIGURACIÓN

Migración de la configuración de las VDOMs

La primera configuración que migré, después de generar el backup, fue la configuración de los dominios virtuales, los cuales permiten dividir de forma lógica una red y que esta pueda operar de formas diferentes en el mismo Hardware, en el caso del nuevo dispositivo UTM generé los siguientes dominios virtuales existentes en el UTM que fue reemplazado:

- DMZ: Dominio virtual para la zona desmilitarizada, la cual es utilizada cuando se requiere tener servicios de la red interna que deben ser accesibles desde la red pública y es necesario el uso de una nueva interfaz que separara los servicios que deben de ser visibles desde la red interna y externa sin poner en riesgo la seguridad de la red interna.
- LAN: Dominio virtual para la red de área local, la cual es utilizada para la conexión entre equipos pertenecientes a una misma organización.
- Root: Dominio virtual desde el cual se permite gestionar los demás dominios creados, dicho dominio se crea automáticamente cuando se habilitan el uso de las VDOMs en el dispositivo UTM.

La forma en la cual llevé a cabo dicha actividad fue la siguiente: Habilité el uso de VDOMs en el nuevo UTM, lo que crea por defecto una VDOM llamada root como se muestra en la Ilustración 3.4.

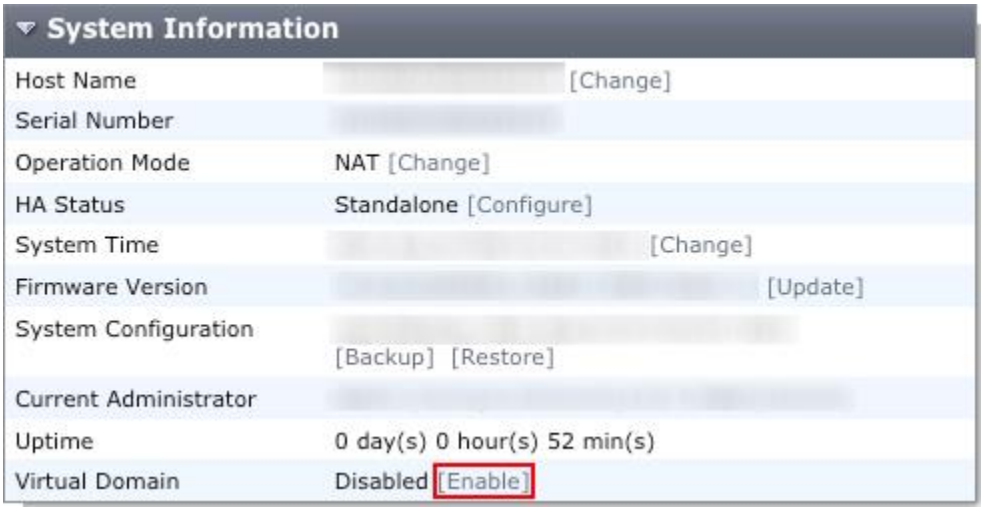

ILUSTRACIÓN 3.4 HABILITACIÓN DE LAS VDOMS

Datos necesarios para la migración de las VDOMs

La información que migré para la creación y configuración de las VDOMs fue la siguiente:

- Nombre de las VDOMs
- Modo de operación transparente: Esté modo de operación permite a las VDOMs comunicarse entre sí y también permite que la VDOM root pueda comunicarse con ellas
- IP y mascara de red
- Puerta de enlace

Actividades realizadas

Una vez obtenidos los datos necesarios de las VDOMs del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Creé y configuré las VDOMs, iniciando por acceder al menú de ***VDOM*** en el menú ***Global*** y dando clic en ***Create New*** como se muestra en la Ilustración 3.5.

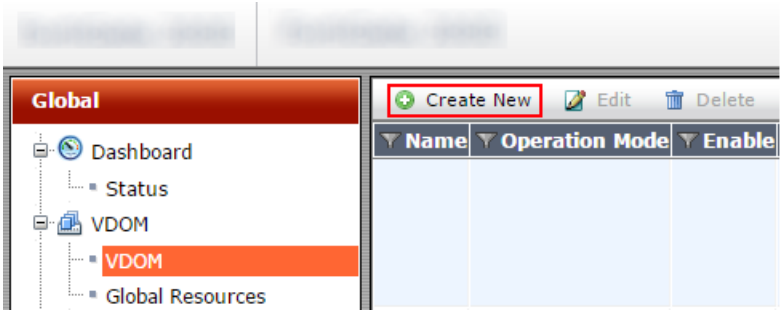

ILUSTRACIÓN 3.5 CREACIÓN DE UNA VDOM

2. Utilizando la información ya mencionada de las VDOMs configuré la nueva VDOM en modo transparente como se muestra en la Ilustración 3.6.

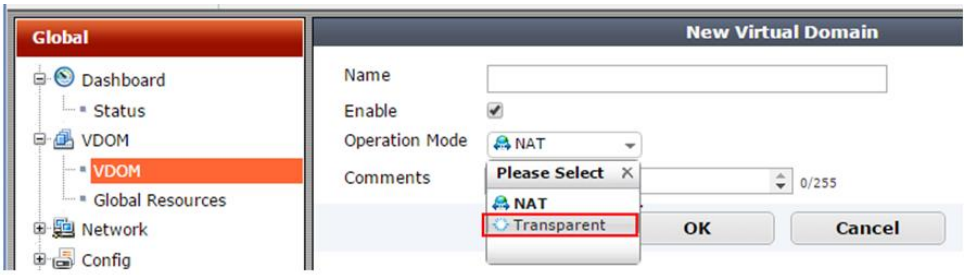

ILUSTRACIÓN 3.6 VDOM EN MODO TRANSPARENTE

3. Asimismo, configuré la IP, máscara de red y la puerta de enlace, dando clic en ***OK*** para finalizar la creación de la VDOM como se muestra en la Ilustración 3.7.

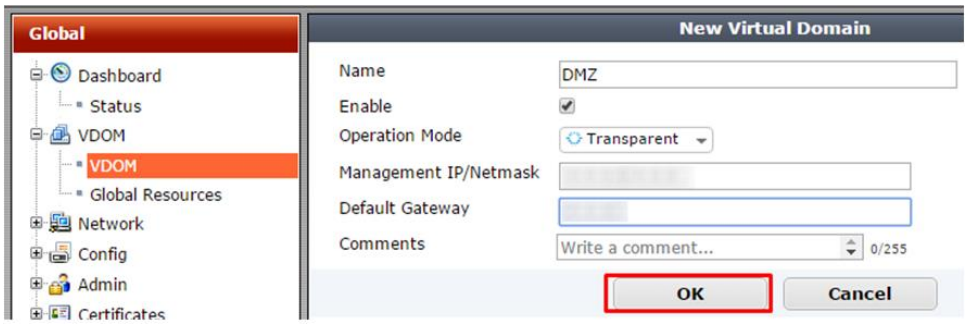

ILUSTRACIÓN 3.7 CONFIGURACIÓN DE UNA VDOM

La configuración para la VDOM LAN la realicé siguiendo los mismos pasos para la creación de la DMZ, quedando las siguientes VDOMs creadas como se muestra en la Ilustración 3.8.

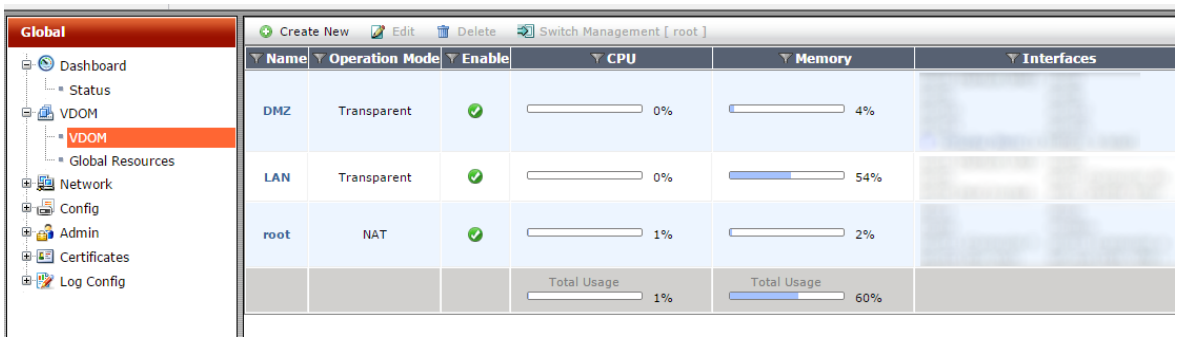

ILUSTRACIÓN 3.8 VDOMS

Migración de la red

Datos necesarios para la migración de las Interfaces

Las interfaces de red del dispositivo UTM se asocian con las VDOMs creadas con la finalidad de darles funcionalidad en la separación de la red. La información que migré para la configuración de las interfaces fue la siguiente:

- Nombre de la interface
- Tipo de interface
- Interface
- VLAN ID
- Dominio virtual
- Modo de direccionamiento
    - Manual
    - DHCP
    - PPPoE (Protocolo Punto a Punto sobre Ethernet)
    - Dirección IP y mascara de red
- Acceso administrativo
    - HTTPS PING HTTP FMG-Access
    - CAPWAP
    - SSH
    - SNMP
- Servidor DHCP
- Modo de Seguridad
- Administración de dispositivos
- Escucha para RADIUS Accounting Messages
- IP secundaría

Actividades realizadas

Una vez obtenidos los datos necesarios de las interfaces del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Interfaces*** en la configuración de ***Network*** y di clic en ***Create New***, como se muestra en la Ilustración 3.9.

ILUSTRACIÓN 3.9 NUEVA INTERFAZ

2. A continuación, se abrió la interfaz mostrada en la Ilustración 3.10 en la cual llevé a cabo la configuración de cada una de las interfaces con las que contaba el dispositivo UTM reemplazado, para finalmente dar clic en ***OK*** para su creación.

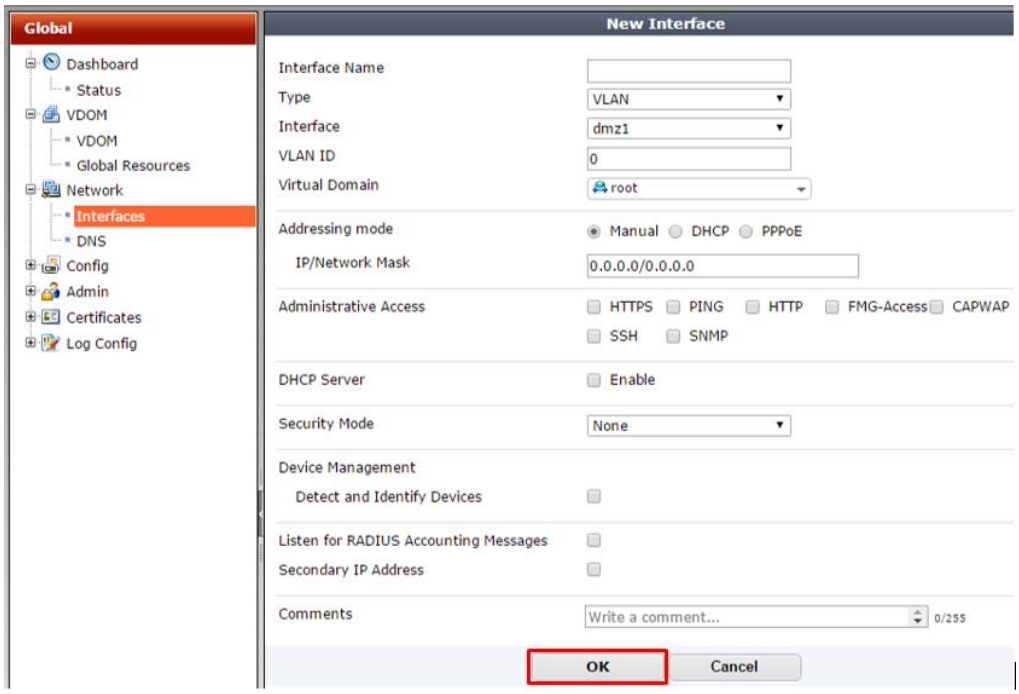

ILUSTRACIÓN 3.10 CONFIGURACIÓN DE INTERFACES DE RED

3. Configuré los DNS primario y secundario, como se muestra en la Ilustración 3.11, utilizado los mismos datos con los que contaba el dispositivo UTM reemplazado, el nombre del dominio local fue seguridad.unam.mx, finalmente di clic en ***Apply*** para que se guardara y aplicara la configuración.

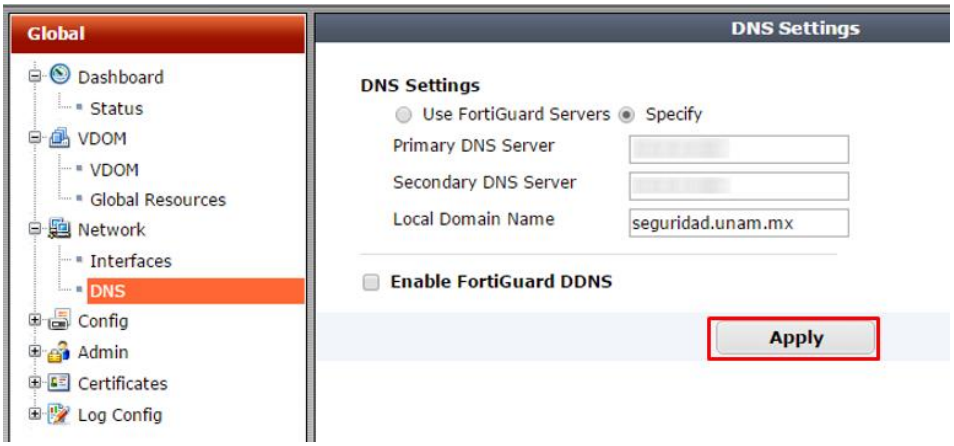

ILUSTRACIÓN 3.11 CONFIGURACIÓN DEL DNS

Una vez llevada a cabo la configuración de las interfaces y de los DNS finalicé la configuración de la red del nuevo dispositivo UTM.

Migración de la configuración de la administración del dispositivo UTM

Datos necesarios para la migración de los perfiles de administración

Los perfiles de administración permiten el control de acceso de las cuentas de administración, los permisos que se pueden configurar son de solo escritura, lectura y escritura o sin permisos de los siguientes servicios:

- System Configuration (configuración del sistema)
- Network Configuration (configuración de la red)
- Administrator Users (administración de usuarios)
- FortiGuard Update (actualización de FortiGuard)
- Maintenance (mantenimiento)
- Router Configuration (configuración del ruteo)
- Firewall Configuration (acceso a la configuración del firewall)
- Security Profile Configuration (configuración de los perfiles de seguridad)
- VPN Configuration (configuración de la VPN)
- User & Device (acceso a los usuarios y al dispositivo)
- WAN opt & Cache (optimización y chaching de la WAN)
- Endpoint Security
- WiFi Controller (controlador del WiFi)
- Log & Report (acceso a los logs y reportes)

Actividades realizadas

Una vez obtenidos los datos de los perfiles de administración del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Admin Profiles*** en la configuración de ***Admin*** y di clic en ***Create New***, como se muestra en la Ilustración 3.12.

ILUSTRACIÓN 3.12 NUEVO PERFIL DE ADMINISTRADOR

2. A continuación, se abrió la interfaz mostrada en la Ilustración 3.13 en la cual llevé a cabo la configuración de cada uno de los perfiles para la administración de usuarios, los cuales serán usados en el siguiente paso para la migración de las cuentas de administración del dispositivo UTM, para finalmente dar clic en ***OK*** para su creación.

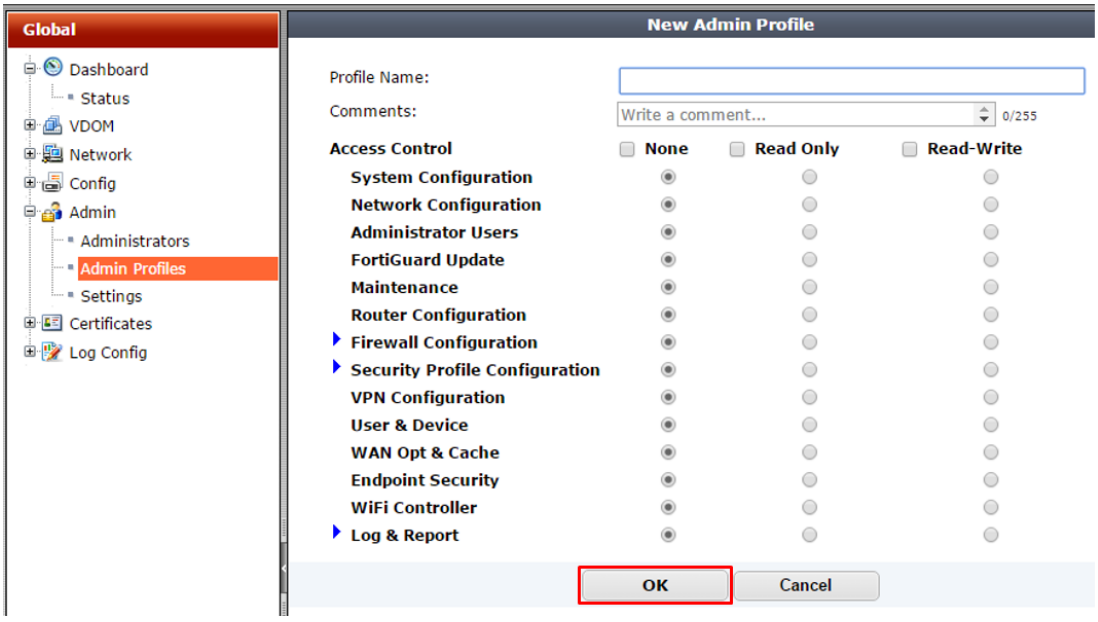

ILUSTRACIÓN 3.13 CONFIGURACIÓN DE LOS PERFILES DE ADMINISTRACIÓN

Datos necesarios para la migración de las cuentas de administración

La información que recabé del dispositivo UTM que fue reemplazado fue la siguiente:

- Nombre de la cuenta de administrador
- Tipo de cuenta
  - Regular
  - Remoto
  - PKI
- Contraseña de la cuenta (la contraseña la ingreso el personal de la CSI/UNAM-CERT que contaba con un acceso de administrador en el dispositivo UTM que fue reemplazado)
- Perfil del administrador (dichos perfiles de administración se mencionarán más adelante)
- Dominio virtual a administrar
- Hosts de confianza (Hosts desde los cuales se conectarán los usuarios con cuenta de administración)

Actividades realizadas

A partir de dicha información obtenida del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Administrators*** en la configuración de ***Admin*** y di clic en ***Create New***, como se muestra en la Ilustración 3.14.

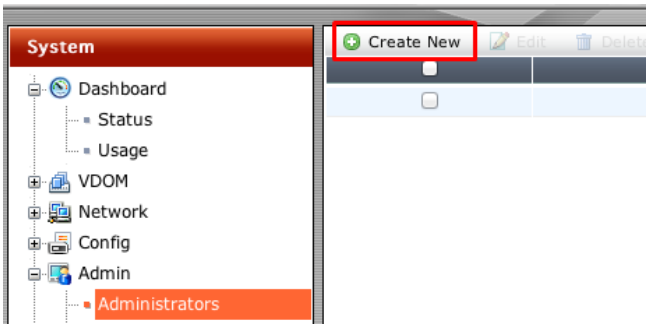

ILUSTRACIÓN 3.14 NUEVO ADMINISTRADOR

2. A continuación, se abrió la interfaz mostrada en la Ilustración 3.15 en la cual llevé a cabo la configuración de cada una de las cuentas de administrador con las que contaba el dispositivo UTM reemplazado, para la configuración de las contraseñas (***Password***) me apoyó el personal de la CSI/UNAM-CERT que contaba con una cuenta de administración, para finalmente dar clic en ***OK*** para su creación.

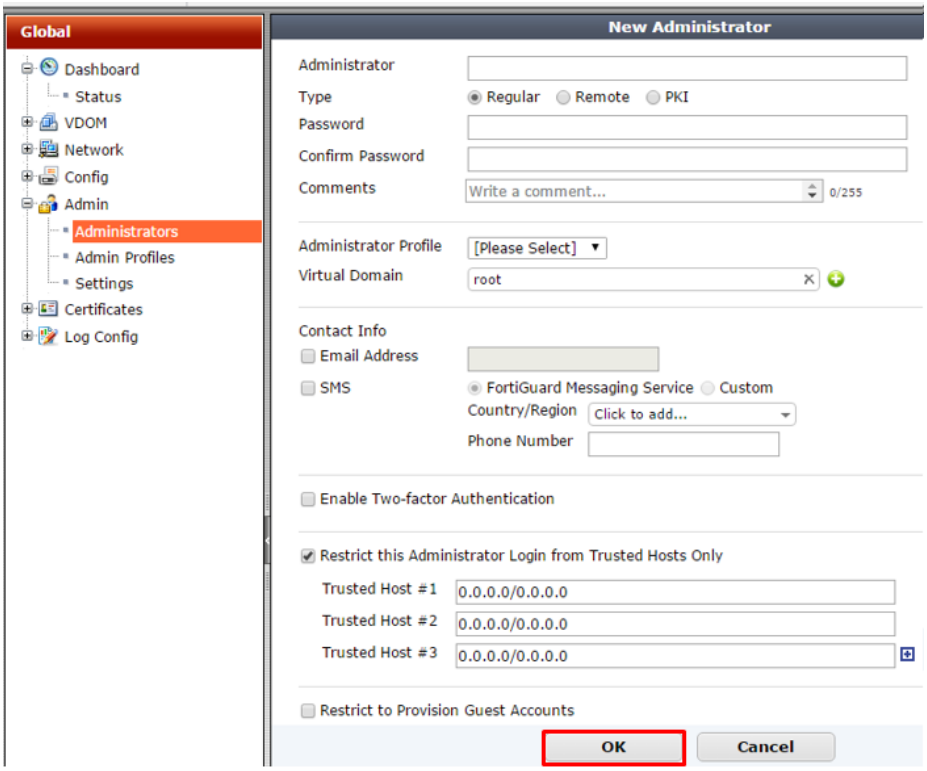

ILUSTRACIÓN 3.15 CONFIGURACIÓN DE LAS CUENTAS DE ADMINISTRACIÓN

Datos necesarios para la migración de los ajustes de administración

La información que recabé del dispositivo UTM que fue reemplazado para la configuración de los ajustes de administración de dicho dispositivo fueron los siguientes protocolos:

- Puerto HTTP
- Puerto HTTPS
- Puerto Telnet
- Puerto SSH
- Tiempo de inactividad

Actividades realizadas

Una vez obtenidos los datos de los ajustes de administración del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Settings*** en la configuración de ***Admin*** y se abrió la interfaz mostrada en la Ilustración 3.16 en la cual llevé a cabo la configuración de los ajustes de administración del dispositivo UTM, para finalmente dar clic en ***Apply*** para aplicar la configuración.

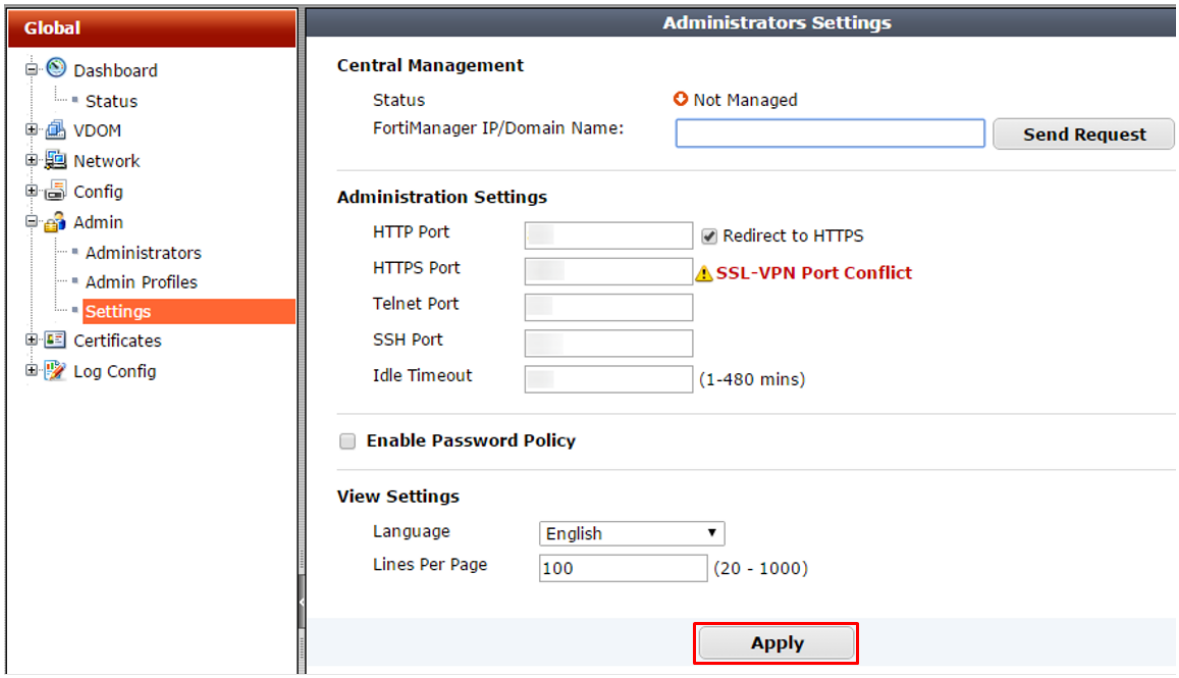

ILUSTRACIÓN 3.16 CONFIGURACIÓN DE LOS AJUSTES DE ADMINISTRACIÓN

Migración de la configuración de los certificados

Datos necesarios para la CA certificadora

Una CA certificadora o también conocida como autoridad certificadora expide los certificados digitales los cuales sirven como identificadores únicos para los servicios, dentro de la CSI/UNAM-CERT se cuenta con una CA certificadora de manera interna. Los datos que recabé para la migración de la CA fueron los siguientes:

- URL del servidor que contiene la CA certificadora
- Identificador de la CA

Actividades realizadas

Una vez obtenidos los datos de la CA certificadora del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***CA Certificates*** en la configuración de ***Certificates*** y se abrió la interfaz mostrada en la Ilustración 3.17 en la cual llevé a cabo la configuración para la importación de la CA certificadora que usa el dispositivo UTM, para finalmente dar clic en ***OK*** para aplicar la configuración.

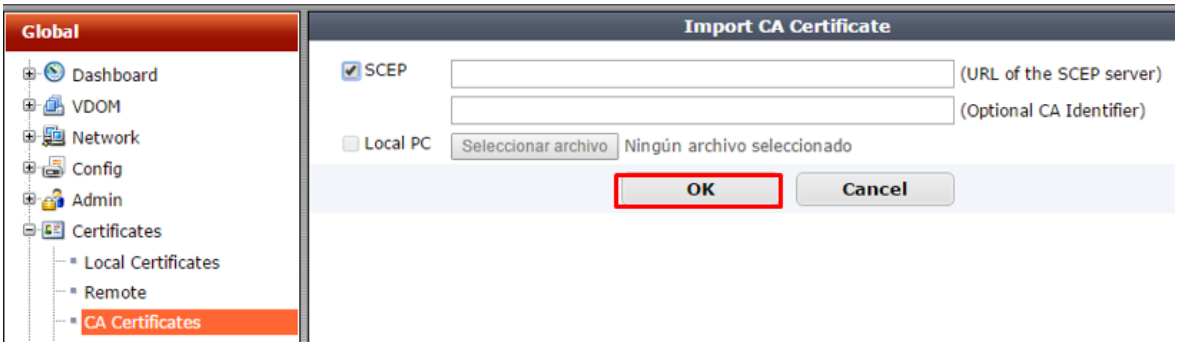

ILUSTRACIÓN 3.17 IMPORTACIÓN DE LA CA CERTIFICADORA

Migración de la configuración interna de las VDOMs

La función de las VDOMs es la de separar la red por lo cual dependiendo de la finalidad de cada una se crean y configuran políticas de firewall las cuales se aplican a los siguientes objetos:

- Direcciones de red
- Servicios de red
- Perfiles de horarios (horarios en los cuales funcionarán las políticas)

Por lo cual antes de migrar la configuración de las políticas, migre y depure los objetos del dispositivo UTM reemplazado.

Datos necesarios para migrar las direcciones de red

La información que recabé del dispositivo UTM que fue reemplazado para la configuración de las direcciones de red fue la siguiente:

- Nombre del objeto
- Tipo: rango de IPs o IP
- Rango de IPs o IP
- Interfaz
- Visibilidad del objeto

Actividades realizadas

Una vez obtenidos los datos de las direcciones de red del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Addresses*** que se encuentra en ***DMZ*** (DMZ, es el nombre de la VDOM que creé), ***Policy & Objects*** y ***Objects*** en donde llevé a cabo la configuración de los

objetos de red del dispositivo UTM como se muestra en la Ilustración 3.18, para finalmente dar clic en **OK** para guardar la configuración de los objetos de red.

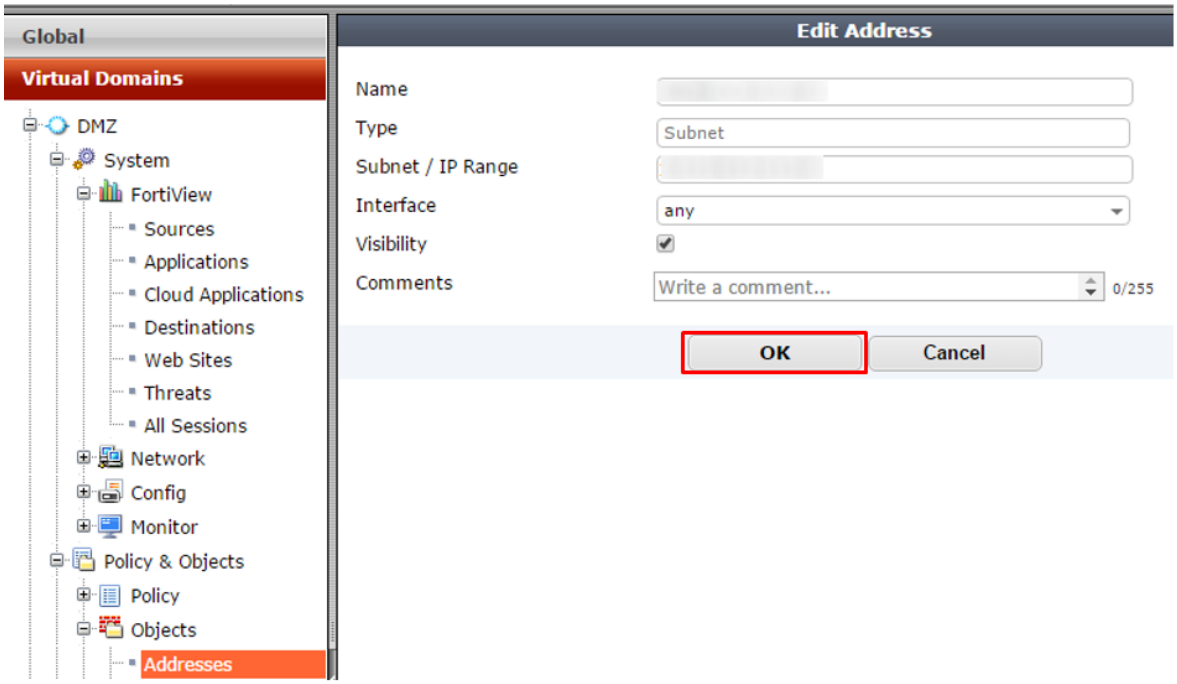

ILUSTRACIÓN 3.18 CONFIGURACIÓN DE LOS OBJETOS DE RED

Datos necesarios para migrar los servicios de red

La información que recabé del dispositivo UTM que fue reemplazado para la configuración de los servicios de red fue la siguiente:

- Nombre
- Categoría:
  - Sin categoría
  - General
  - Acceso web
  - Acceso a archivos
  - Email
  - Servicios de red
  - Autenticación
  - Acceso remoto
  - Tunneling
  - VoIP
  - Proxy web
- Tipo de protocolo:

- TCP/UDP/SCTP
- ICMP
- ICMP6
- IP

- Protocolo
  - TCP
  - UDP
  - Rango de puertos

Actividades realizadas

Una vez obtenidos los datos de los servicios de red del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Services*** que se encuentra en ***DMZ, Policy & Objects*** y ***Objects*** en donde llevé a cabo la configuración de los objetos de servicios de red del dispositivo UTM como se muestra en la Ilustración 3.19, para finalmente dar clic en ***OK*** para guardar la configuración de los objetos de servicios.

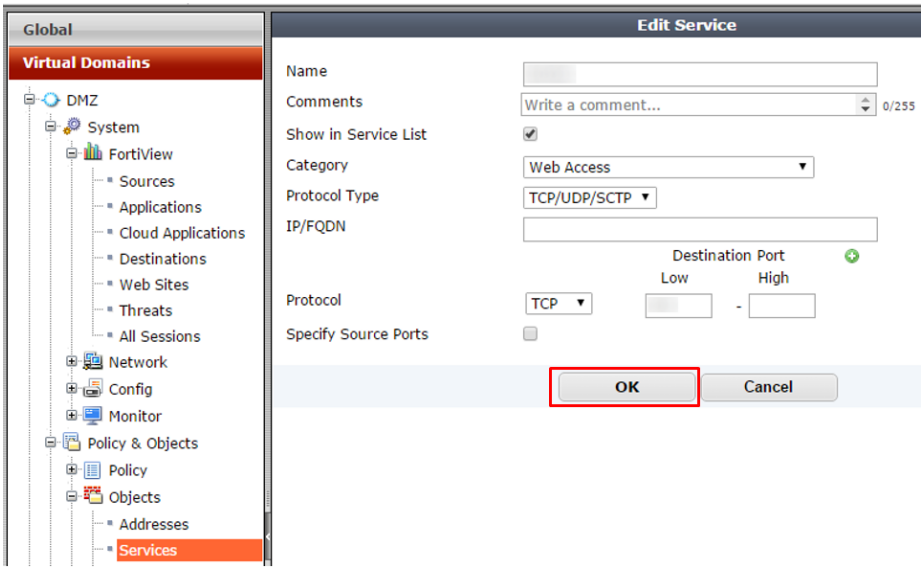

ILUSTRACIÓN 3.19 CONFIGURACIÓN DE LOS SERVICIOS DE RED

Datos necesarios para migrar los perfiles de horarios

La información que recabé del dispositivo UTM que fue reemplazado para la configuración de los perfiles de horarios fue la siguiente:

- Tipo:
  - Recurrente
  - Una sola vez

- Nombre del perfil
- Días de la semana
- Hora de inicio
- Hora de finalización

Actividades realizadas

Una vez obtenidos los datos de los perfiles de horarios del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Schedules*** que se encuentra en ***DMZ, Policy & Objects*** y ***Objects*** en donde llevé a cabo la configuración de los objetos de perfiles de horarios del dispositivo UTM como se muestra en la Ilustración 3.20, para finalmente dar clic en ***OK*** para guardar la configuración de dichos objetos.

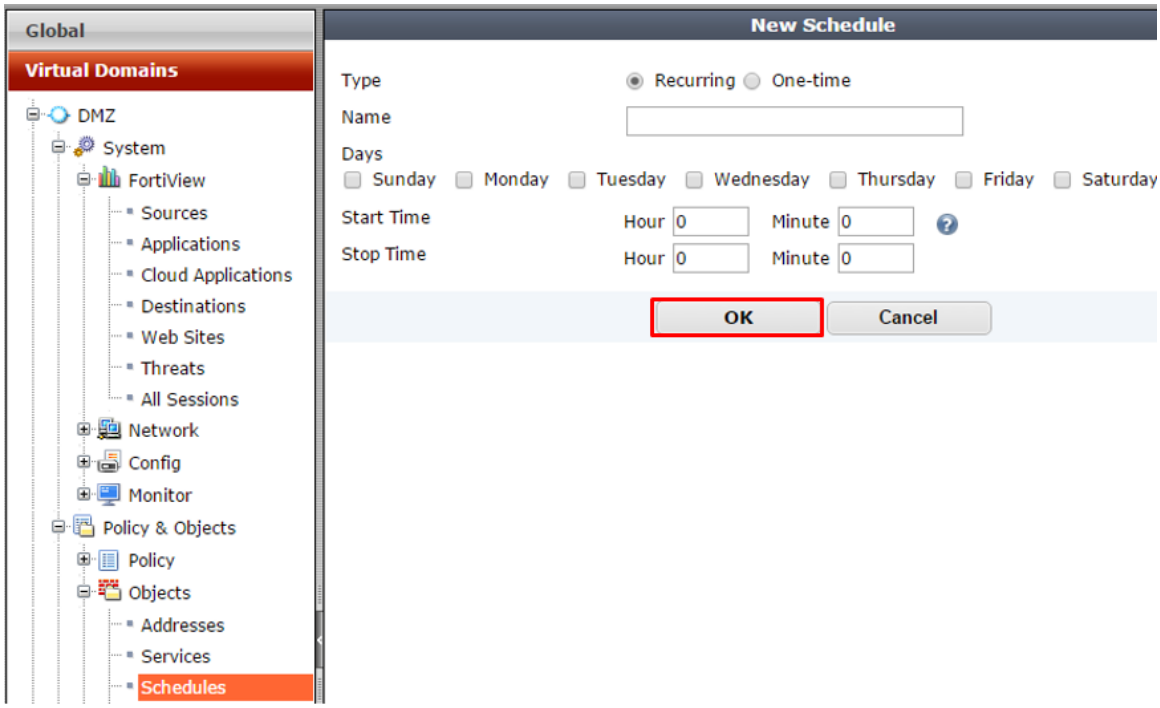

ILUSTRACIÓN 3.20 CONFIGURACIÓN DE LOS PERFILES DE HORARIO

Migración de la configuración de las políticas de las VDOMs

En este punto revisé todas las políticas del dispositivo UTM reemplazado para depurarlas, para esto tomé en cuenta los siguientes puntos:

- Políticas relacionadas a servicios que no existen
- Políticas relacionadas a objetos que ya no se usan
- Políticas relacionadas creadas para pruebas de servicios temporales

- Políticas específicas cuyas características pueden ser reemplazadas por políticas generales

Asimismo, modifiqué todas las políticas considerando que el nuevo dispositivo UTM tiene diferencias en las interfaces físicas respecto al dispositivo UTM que fue reemplazado.

Datos necesarios para la migración de las políticas

La información que recabé del dispositivo UTM que fue reemplazado para la configuración de las políticas fue la siguiente:

- Interfaz entrante (Incoming Interface)
- Dirección de origen (Source Address)
- Usuario(s) origen (Source User(s))
- Tipo de dispositivo origen (Source Device Type)
- Interfaz de salida (Outgoing Interface)
- Dirección de destino (Destination Address)
- Horario (Schedule)
- Servicio (Service)
- Acción (Action)

Perfiles de seguridad (Security Profiles)

- Filtrado Web (Web Filter)
- Control de Aplicaciones (Application Control)
- IPS
- Filtrado de correo electrónico (Email Filter)
- Inspección SSL/SSH (SSL/SSH Inspection)

Catalogación de tráfico

- Shared Shaper. - Permite asignar ancho de banda a las conexiones hacia afuera de la red
- Reverse Shaper.- Permite asignar ancho de banda a las conexiones hacia adentro de la red
- Per-IP Shaper.- Permite asignar ancho de banda a las direcciones IP de origen

Opciones de registro

- Eventos de seguridad (Security Events)
- Todas las sesiones (All Sessions)

Actividades realizadas

Una vez obtenidos los datos de las políticas del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***IPv4*** que se encuentra en ***DMZ, Policy & Objects*** *y* ***Policy*** y di clic en ***Create New***, como se muestra en la Ilustración 3.21.

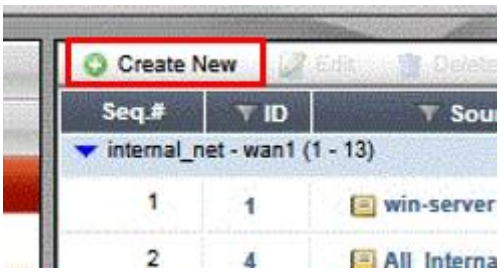

ILUSTRACIÓN 3.21 NUEVA POLÍTICA

2. A continuación, se abrió la interfaz mostrada en la Ilustración 3.22 en la cual llevé a cabo la configuración de cada una de las políticas con las que contaba el dispositivo UTM reemplazado, tomando en cuenta las consideraciones ya mencionadas, para finalmente dar clic en ***OK*** para su creación.

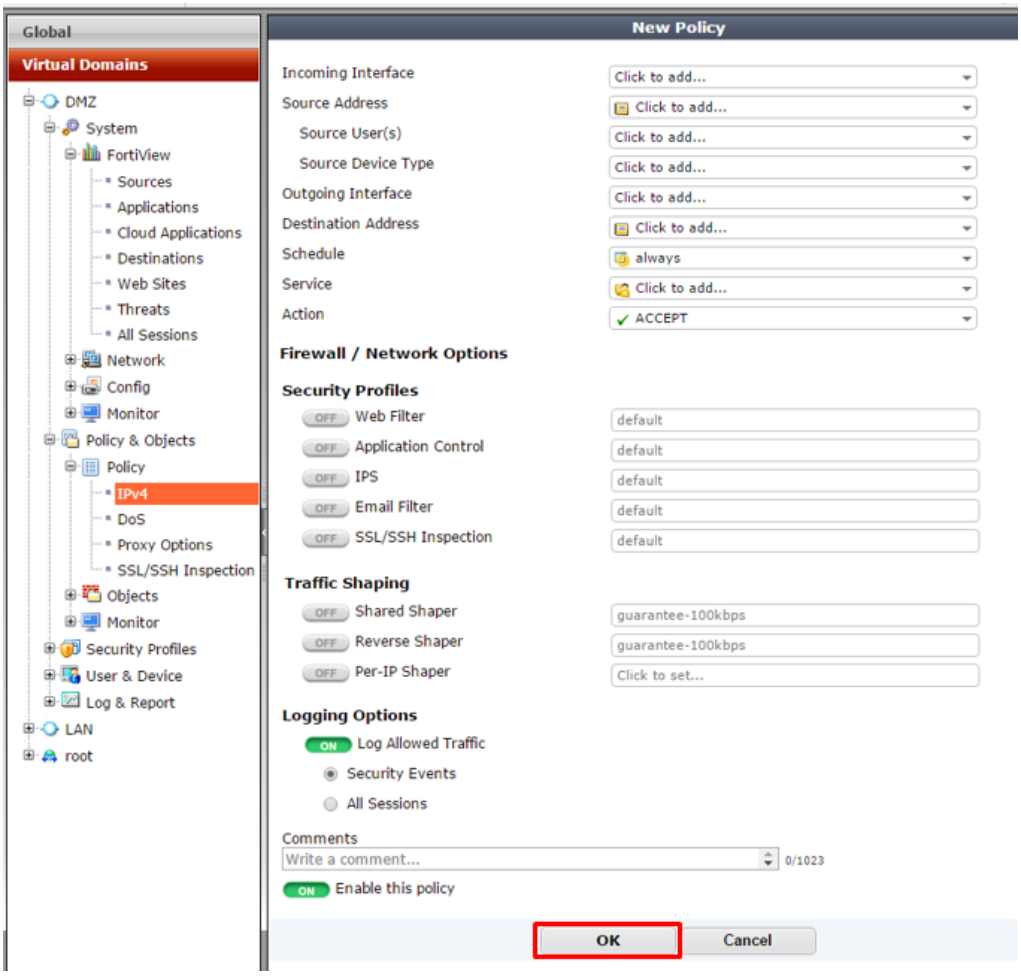

ILUSTRACIÓN 3.22 CONFIGURACIÓN DE LAS POLÍTICAS

Al finalizar todas las configuraciones, las políticas se mostraron como en la Ilustración 3.23.

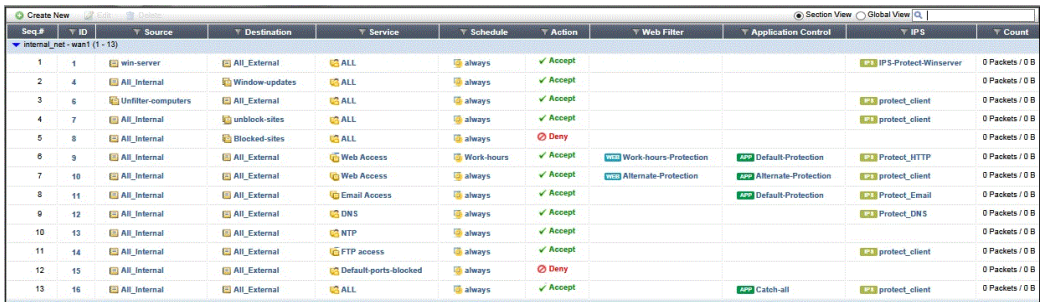

ILUSTRACIÓN 3.23 POLÍTICAS CONFIGURADAS

Migración de la configuración interna de la VDOM root

La VDOM root tiene funciones adicionales a las VDOM como lo son:

- Configuración del ruteo de paquetes
- Configuración de una conexión VPN
    - Portal web para VPN
    - Uso de LDAP para autenticación
    - Configuración de grupo de usuarios para el uso de la VPN

Datos necesarios para migrar la configuración del ruteo estático de paquetes

La información que recabé del dispositivo UTM que fue reemplazado para la configuración de las direcciones de red fue la siguiente:

- IP y marcara del destino
- Dispositivo
- Puerta de enlace
- Distancia
- Prioridad

Actividades realizadas

Una vez obtenidos los datos del ruteo estático del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Static Routes*****,** que se encuentra en ***root, Router*** *y* ***Static Objects*****,** en donde llevé a cabo la configuración de la ruta estática del dispositivo UTM como se muestra en la Ilustración 3.24, para finalmente dar clic en ***OK*** para guardar la configuración de ruteo estático.

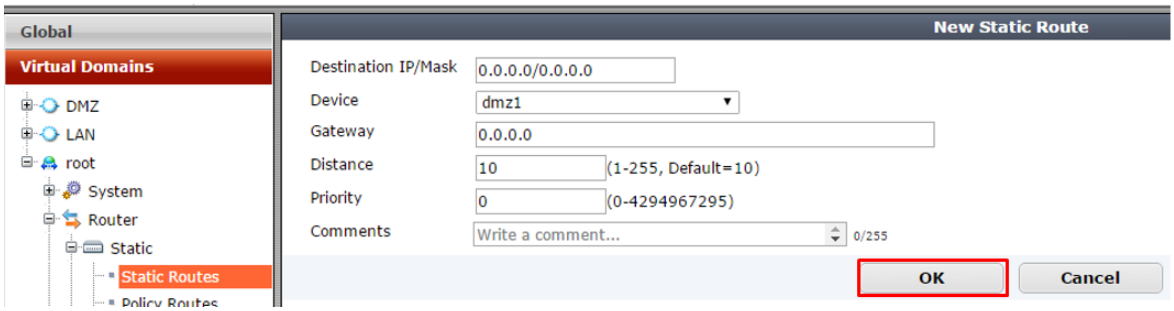

ILUSTRACIÓN 3.24 CONFIGURACIÓN DE RUTEO ESTÁTICO

Datos necesarios para migrar la configuración de VPN

Para la configuración de la VPN necesité la siguiente información del dispositivo UTM:

- Habilitar el modo Túnel
  - Conjunto de IPs fuente
  - Opciones para el cliente
    - Guardar contraseña
    - Auto conexión
    - Mantener la sesión activa
- Habilitar el Modo Web
  - Mensaje del portal
  - Tema
- Marcadores predefinidos
  - Categoría
  - Nombre
  - Tipo
    - HTTP/HTTPS
    - Citrix
    - FTP
    - Port forward
    - RDP
    - RDP nativo
    - SMB/CIFS
    - SSH
    - TELNET
    - VNC
  - URL
  - Descripción
  - Single Sign-On

- Deshabilitado
- Estático
- Automático

Actividades realizadas

Una vez obtenidos los datos de la configuración de VPN del dispositivo UTM reemplazado realicé los siguientes pasos:

2. Seleccioné ***Portals*** que se encuentra en ***root*** , ***VPN*** y ***SSL*** en donde llevé a cabo la configuración del portal web de la VPN como se muestra en la Ilustración 3.25, en la cual configuré los marcadores predefinidos para el acceso a la VPN dando clic en ***Create New***, para finalmente guardar la configuración del portal de la VPN.

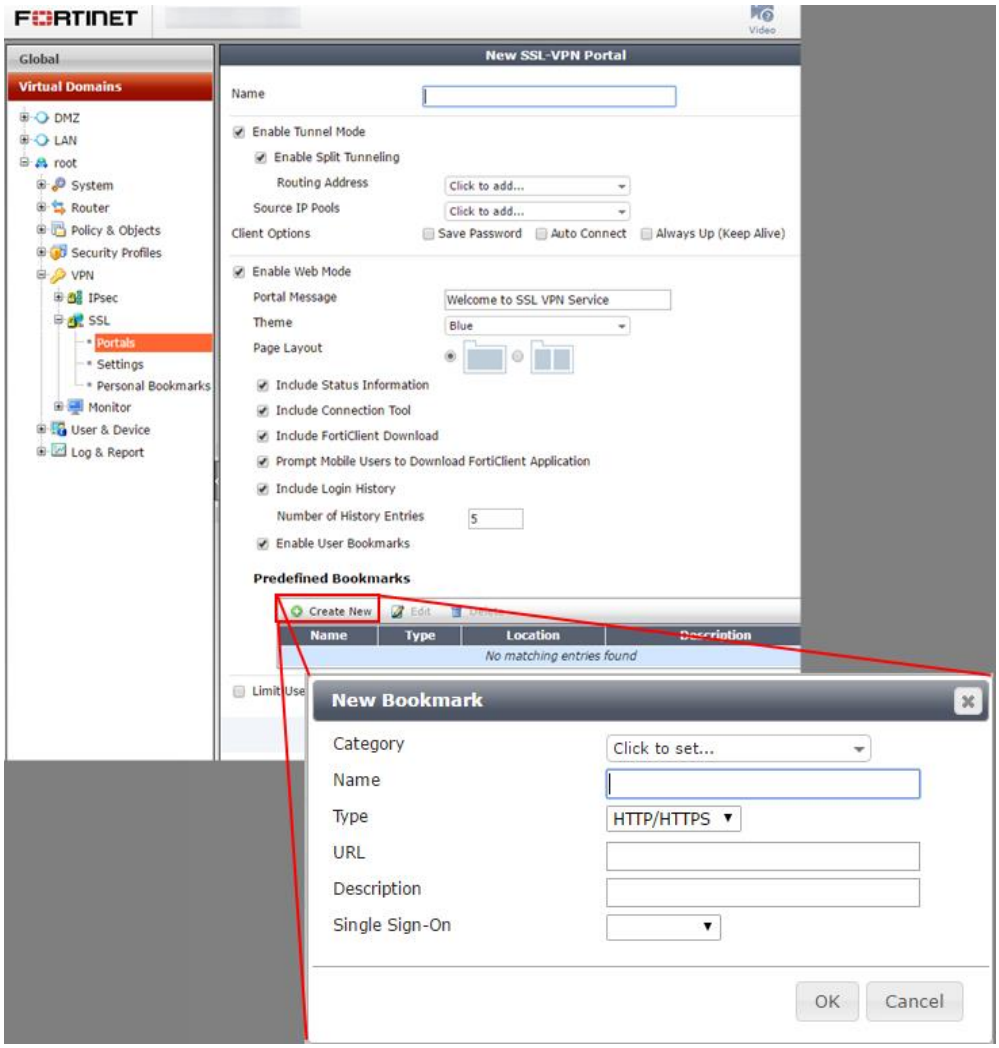

ILUSTRACIÓN 3.25 CONFIGURACIÓN DEL PORTAL DE LA VPN

Datos necesarios para migrar los ajustes de la VPN

La información que recabé del dispositivo UTM que fue reemplazado para la configuración de los ajustes de la VPN fue la siguiente:

- Interfaz de escucha (interfaz para la conexión de la VPN)
- Puerto de escucha (interfaz para el puerto por donde se conectará la VPN)
- Restricción de acceso a la VPN
- Servidores DNS

Actividades realizadas

Una vez obtenidos los datos de los ajustes de la VPN del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***Settings*** que se encuentra en ***root, VPN*** *y* ***SSL*** en donde llevé a cabo la configuración de los ajustes de la VPN como se muestra en la Ilustración 3.26, para finalmente dar clic en ***Apply*** para aplicar la configuración de los ajustes de la VPN.

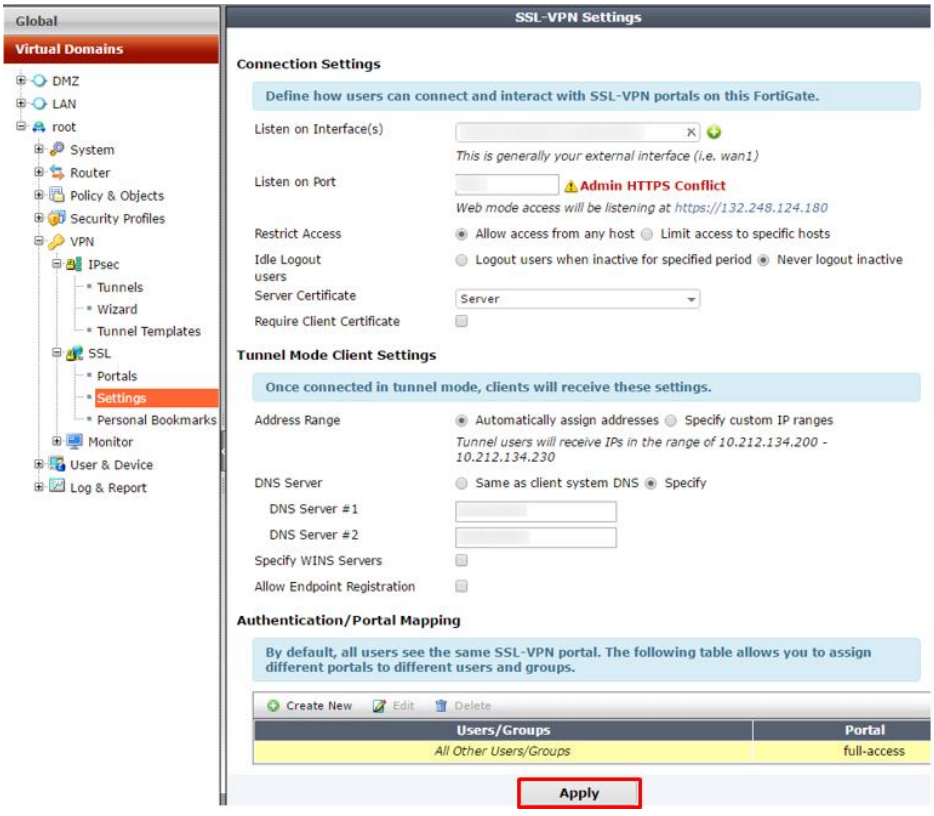

ILUSTRACIÓN 3.26 CONFIGURACIÓN DE LOS AJUSTES DE LA VPN

Datos necesarios para migrar los servicios de LDAP

El servicio de LDAP en el dispositivo UTM permite utilizar un método de autenticación que se encuentre en otro sitio de la red, la información que recabé del dispositivo UTM que fue reemplazado para la configuración del servicio de LDAP fue la siguiente:

- IP del Servidor
- Puerto del Servidor
- Identificador de Nombre Común
- Nombre Distinguido
- Usuario DN
- Contraseña
- Protocolo
    - LDAPS
    - STARTTLS
- Certificado

Actividades realizadas

Una vez obtenidos los datos de los servicios de LDAP del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné ***LDAP Servers*** que se encuentra en ***root, User & Device, y Authentication*** en donde llevé a cabo la configuración del LDAP como se muestra en la Ilustración 3.27, para finalmente dar clic en ***OK*** para aplicar la configuración.

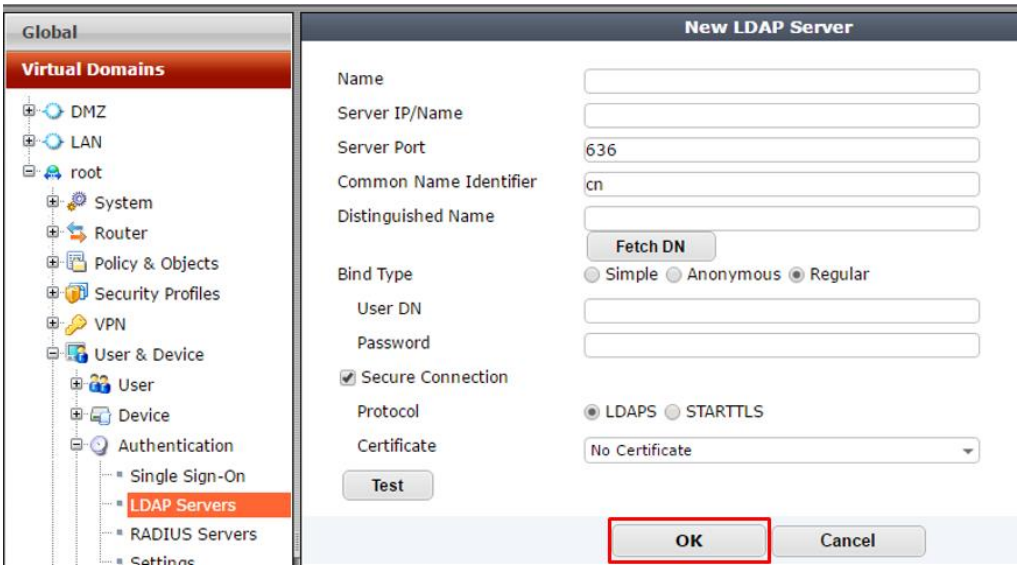

ILUSTRACIÓN 3.27 CONFIGURACIÓN DE LDAP

Datos necesarios para migrar los grupos de usuarios para el uso de la VPN

La información que recabé del dispositivo UTM que fue reemplazado para la configuración de los grupos fue la siguiente:

- Nombre
- Tipo
  - Firewall
  - Fortinet Single Sing-On
  - Guest
  - RADIUS Single Sing-On
- Grupos Remotos
  - Servidor Remoto
  - Grupos

Actividades realizadas

Una vez obtenidos los datos de los grupos de usuarios del dispositivo UTM reemplazado realicé los siguientes pasos:

1. Seleccioné **LDAP Servers** que se encuentra en **root** , **User & Device**, y **User** en donde llevé a cabo la configuración de los grupos de usuarios como se muestra en la Ilustración 3.28, para finalmente dar clic en **OK** para aplicar la configuración.

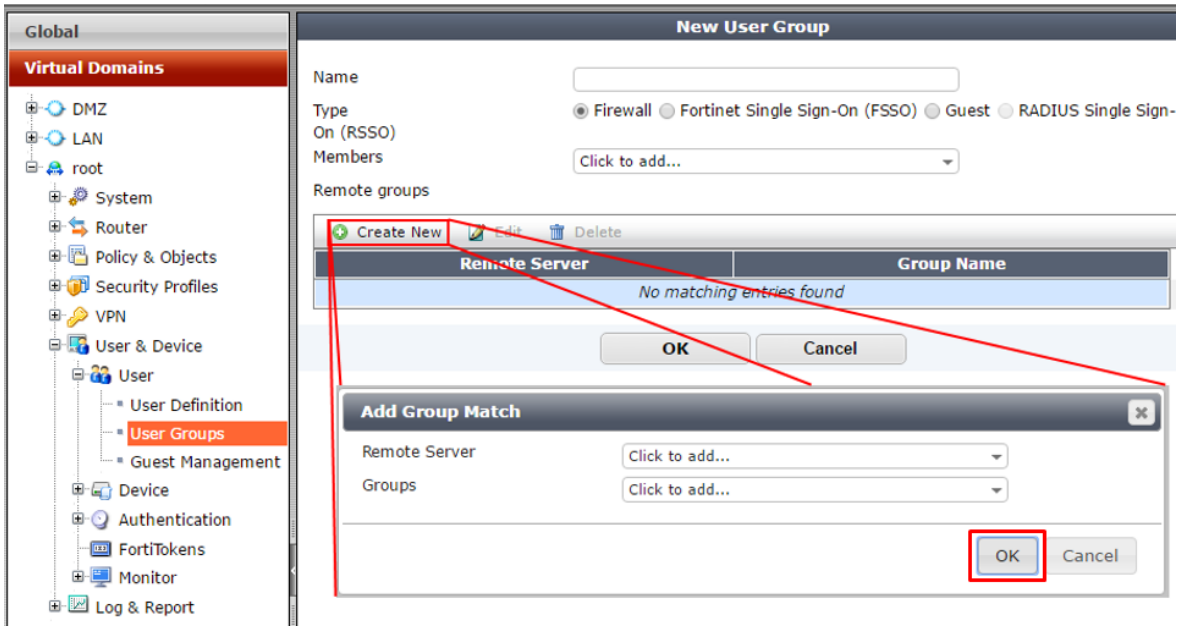

ILUSTRACIÓN 3.28 CONFIGURACIÓN DE LOS GRUPOS DE USUARIOS

3.4.3 Migración física

Para la migración e instalación física del nuevo dispositivo UTM tomé las siguientes consideraciones:

- El horario laborar ordinario de la CSI/UNAM-CERT comprende de las 10:00 h a las 20:00 h y el horario de salida a comer es de las 15:00 h a las 17:00 h de lunes a viernes.
- La ventana de servicio para la instalación del dispositivo UTM fue en el horario de comida, de las 15:00 h a las 17:00 h.
- Se envió un aviso de dichos cambios y de la interrupción de los servicios de red a todo el personal de la CSI/UNAM-CERT.

Actividades realizadas

Durante las dos horas disponibles, de 15:00 h a las 17:00 h, hice el cambio de los dispositivos UTM de la siguiente manera:

1. Apagué el UTM que fue reemplazado.

2. Desconecté la fuente de alimentación del dispositivo UTM que fue reemplazado.

3. Identifiqué y desconecté de cada cable de red conectado al dispositivo UTM que fue reemplazado.

4. Desmonté el dispositivo UTM reemplazado del rack retirando los tornillos que lo sostenían.

5. Coloqué el nuevo dispositivo UTM en la misma ubicación donde se encontraba el anterior colocándole los tornillos para fijarlo de manera segura.

6. Conecté la fuente de alimentación al nuevo dispositivo UTM instalado.

7. Conecté los cables de red en los puertos que corresponden en el nuevo dispositivo UTM.

8. Encendí el nuevo UTM.

9. Verifiqué que la conectividad en la red actuara normalmente con el nuevo dispositivo UTM accediendo a los servicios internos y externos que ofrece la CSI/UNAM-CERT de la siguiente manera:

a. Se accedió desde Internet a las páginas principales de la CSI/UNAM-CERT las cuales son:

   i. https://revista.seguridad.unam.mx/

   ii. https://www.seguridad.unam.mx/

   iii. https://www.seguridad.unam.mx/

   Y se tuvo acceso al contenido de los servicios web sin ningún inconveniente.

b. Comprobé el acceso a internet desde los equipos internos de cómputo, accediendo a un navegador web y buscando la palabra "UTM" el cual arrojo varios resultados, lo que valido el acceso a internet. Asimismo, al llevar a cabo dicha acción de valido el servicio de DNS y Gateway.
c. Validé el acceso a los perfiles de administración del nuevo UTM con el apoyo del personal de la CSI/UNAM-CERT, comprobando que cada uno tuviese el perfil correspondiente en función de sus atribuciones.
d. Comprobé el acceso mediante VPN a la red interna, conectándome desde una red pública utilizando mis credenciales asignadas y mediante el uso de la utilidad ping para así alcanzar la IP privada que tenía asignado mi equipo de cómputo.
e. Validé, con el apoyo del personal de la CSI/UNAM-CERT, la configuración de las políticas de firewall al intentar acceder, mediante los protocolos https, SSL, TCP y TELNET, a los servicios internos que dan soporte a la operación y actividades que se llevan a cabo de forma continua en la CSI/UNAM-CERT.
f. En los días subsecuentes a la instalación del nuevo UTM validé que no se registraran fallas y/o incidentes relacionados con la operación de dicho UTM, concluyendo así que su funciona de forma normal.

Físicamente la instalación del nuevo dispositivo UTM se llevó sin contratiempos y quedo instalado en el mismo sitio donde se encontraba el dispositivo UTM reemplazado.

A continuación, en la Ilustración 3.29, se muestra la consecución de los pasos del reemplazo físico ya descritos en los puntos del 1 al 8.

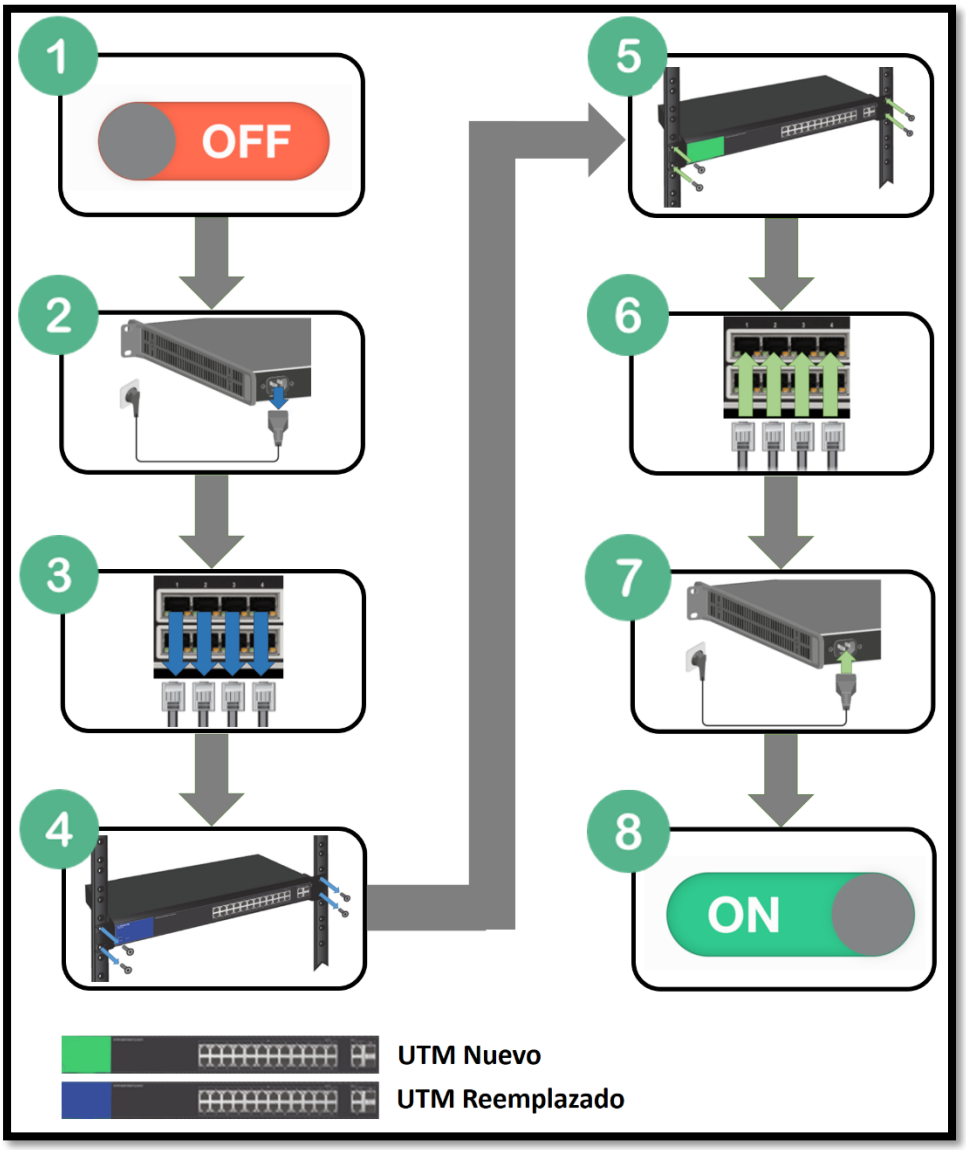

ILUSTRACIÓN 3.29 INSTALACIÓN DEL DISPOSITIVO UTM

Resultados

3.5 Resultados

Al realizar las actividades para el proyecto de migración del dispositivo UTM, tanto de manera lógica como física, y gracias al valioso apoyo por parte del personal de la CSI/UNAM-CERT que en todo momento estuvo disponible para la recolección de información en relación a las configuraciones que realice, así como su disponibilidad para realizar sus actividades durante la interrupción de los servicios al migrar físicamente el dispositivo UTM.

Por lo anterior, realicé de manera correcta y eficiente la migración de las configuraciones y puesta a punto del nuevo dispositivo UTM cumpliendo así el objetivo general y particulares del proyecto.

Asimismo, el nuevo dispositivo UTM cubre la necesidad que requiere el constante cambio de las amenazas de seguridad, y por lo cual los mecanismos de seguridad deben ir un paso adelante para proteger la información de las organizaciones.

CONCLUSIONES

3.6 Conclusiones

La migración de las configuraciones del dispositivo UTM reemplazado al nuevo dispositivo UTM cumplió con las necesidades requeridas por la CSI/UNAM-CERT, asimismo, se cumplieron los objetivos generales y particulares del proyecto.

Personalmente el haber sido parte de la realización de las actividades para el proyecto me aportaron los siguientes conocimientos en el desarrollo de un proyecto:

- El contexto de la organización, en este caso la CSI/UNAM-CERT, es un tema importante que se debe revisar con el objetivo de un buen desarrollo en el proyecto.
- El apoyo de la alta gerencia para llevar a cabo el proyecto es parte fundamental para la factibilidad de este, sin el apoyo de la alta gerencia difícilmente se podría finalizar en tiempo y forma un proyecto.
- Informar a las áreas interesadas a las cuales el proyecto afecta es un punto importante para la asignación de actividades respecto a las atribuciones específicas del personal involucrado en el proyecto.

Por otra parte, los conocimientos técnicos obtenidos fueron los siguientes:

- Instalación física de un dispositivo UTM, en un centro de datos y los factores que son importantes como lo son; la disponibilidad de espacio, la instalación del cableado estructurado y las medidas de seguridad necesarias para su correcto funcionamiento dentro del centro de datos.
- Análisis de la ficha técnica (datasheet) de los dispositivos UTM en donde se resume el funcionamiento y características de los dispositivos con la finalidad de revisar la factibilidad de migración de un dispositivo a otro.

Por lo anterior, puedo decir con toda razón que dicho proyecto me aportó un crecimiento laboral en los ámbitos de:

- Conocimientos especializados: Manejo especifico en el uso de nuevas tecnologías.
- Habilidades organizativas: Toma de decisiones y análisis de ideas claves para la resolución de problemas.
- Habilidades relacionales: Trabajo en equipo y una buena comunicación.

Los conocimientos que obtuve a lo largo de mi vida académica en la Facultad de Ingeniería, como lo son la capacidad de analizar, diseñar, planear, observar y producir soluciones para solventar problemas fueron esenciales para llevar a cabo, y de manera satisfactoria, el presente proyecto.

3.7 Glosario

Alertas por e-mail	Sistema que permite el envío de alertas de seguridad a través de un correo electrónico.
Antispam	Método de prevención contra el correo basura.
Antivirus	Software para la detección de virus con la capacidad de neutralizar sus efectos.
Balanceo de carga	Sistema que permite asignar la entrada de solicitudes, mediante un algoritmo, de los clientes entre los servidores existentes con el fin de minimizar tiempos de cara y evitar la saturación de dichos servicios.
CAPWAP	(Control And Provisioning of Wireless Access Points) es un protocolo de red estándar e interoperable que permite que un Controlador de Acceso de LAN Inalámbrica Central (AC) administre una colección de Puntos de Terminación Inalámbrica (WTP) , más comúnmente conocidos como Puntos de Acceso Inalámbricos.
CERT	(Por sus siglas en inglés Computer Emergency Response Team) Equipo de Respuesta a Incidentes de Seguridad en Cómputo
Detección y prevención de intrusos y gestor de tráfico	La detección de intrusos es una técnica que analiza la actividad de los servicios y de la red en busca de comportamientos anómalos para así poder emitir una alerta, por otro lado, la prevención de intrusos al encontrar un comportamiento anómalo tiene la capacidad de analizarlo y bloquearlo, asimismo, la gestión del tráfico permite analizar y caracterizar el tráfico de red.
DHCP	(Protocolo de configuración dinámica de host): Protocolo que permite a un dispositivo de una red, conocido como servidor DHCP, asignar direcciones IP temporales a otros dispositivos de red, normalmente equipos.
Dirección IP	Dirección que se utiliza para identificar un equipo o dispositivo en una red.
DMZ	(Zona desmilitarizada) Se refiere a la zona ubicada entre la red interna e Internet, permitiendo que los servicios que se encuentren en ella puedan ser alcanzados desde Internet.

DNS	(Servidor de nombres de dominio): La dirección IP de su servidor ISP, que traduce los nombres de los sitios Web a direcciones IP.
Enrutador	Dispositivo de red que dirige o enruta paquetes a través de las redes. Un enrutador funciona con una dirección de mensajes IP, a fin de determinar la mejor ruta hacia su destino.
Enrutamiento	Proceso utilizado para determinar la mejor ruta y hacer avanzar la información a lo largo de esa ruta, a partir de una red fuente o segmento de red, hacia una dirección de red de destino.
Filtrado de contenido	Controla el contenido de los sitios web que puede visitar un cliente, para esto utiliza dos listas, una lista blanca donde se encuentran los sitios permitidos y una lista negra en donde se encuentran los sitios bloqueados.
Firewall	Sistema diseñado para el filtro de datos entre la red interna y externa, basándose en reglas y políticas para permitir y excluir el flujo de los datos.
FMG-Access	Acceso a FortiManager, una herramienta para ingresar al dispositivo UTM para su administración.
FTP	Acrónimo de File Transfer Protocol, protocolo de transferencia de archivos. La transferencia se realiza de un servidor FTP a través del navegador o un programa utilitario de FTP.
HTTP	Protocolo de transferencia de hipertexto, un protocolo de red que se usa para recuperar páginas web desde un servidor web.
HTTPS	(Hypertext Transfer Protocol Secure) es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la Internet.
ICMP	(Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).
Interfaz	Manera con la que el usuario se comunica con un dispositivo informático.
Internet	Apócope de International Net, soporte de comunicación entre computadoras (net = red).
Intranet	Red de acceso restringido mediante password.

LAN (Local Area Network)	Red de área local que consiste en dos o más nodos, generalmente en un área relativamente pequeña (local). Las estaciones de trabajo de una LAN se conectan con el propósito principal de compartir información y recursos locales. Típicamente, una red casera es una LAN, así como la red de una oficina pequeña o la red de una planta manufacturera.
LDAP	(Por sus siglas en inglés, Protocolo de Acceso Ligero a Directorio) Protocolo que permite acceder a información guardada de forma centralizada a través de la red.
PPPoE	(Point-to-Point Protocol over Ethernet o Protocolo Punto a Punto sobre Ethernet) es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet.
ISP	(Internet Service Provider): Servidor conectado directamente a Internet y que le permite a sus usuarios el acceso o entrada a dicha red.
Proxy (servidor proxy)	Componente de un firewall que maneja el tráfico de una LAN desde y hacia Internet. Permite la descarga más rápida de documentos o páginas Web de uso frecuente y el control de acceso.
Puerto	Son vías que permiten a una PC el intercambio de datos, su salida y entrada.
Puertos TCP o UDP	Son números de puertos que habilitan paquetes de IP para ser enviados de una computadora a Internet. Algunos son asignados permanentemente (ej: para e-mail por SMTP es el 25) otros son efímeros y desaparecen al terminar una sesión de comunicación. Hay disponibles 65 535 puertos para TCP y UDP.
RADIUS	(Remote Authentication Dial-In User Service). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.
RDP	(Remote Desktop Protocol) es un protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre una terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows

SMB (Server Message Block) es un protocolo de red que permite compartir archivos, impresoras, etcétera, entre nodos de una red de computadoras que usan el sistema operativo Microsoft Windows.

SMTP Acrónimo de Simple Mail Transfer Protocol, protocolo de enlace entre clientes y servidores para enviar correo electrónico.

Snifer Herramienta que permite capturar y analizar el tráfico de una red.

SNMP Acrónimo de Simple Network Management Protocol. Protocolo estándar para la administración de red en Internet. Prácticamente todos los sistemas operativos, routers, switches, módems cable o ADSL módem, firewalls, etc. se ofrecen con este servicio.

SSH Protocolo similar a "telnet", pero en el que ambos extremos de la conexión se autentifican mutuamente y la conexión en sí va protegida criptográficamente.

SSL (Secure Sockets Layer) Protocolo que permitir que las aplicaciones transmitan información de ida y de manera segura hacia atrás.

STARTTLS Es una extensión a los protocolos de comunicación de texto plano, que ofrece una forma de mejorar desde una conexión de texto plano a una conexión cifrada (TLS o SSL) en lugar de utilizar un puerto diferente para la comunicación cifrada.

Telnet (Telecommunication Network) Se trata del nombre de un protocolo de red que se utiliza para acceder a una computadora y manejarla de forma remota. El término también permite nombrar al programa informático que implementa el cliente.

TCP/IP Acrónimo de Transmission Control Protocol/ Internet Protocol. Protocolo desarrollado para la comunicación entre computadoras. Es el estándard de la transmisión de datos por redes, incluida Internet.

TCP Acrónimo de Transmission Control Protocol. Protocolo que dirige la ruptura de los mensajes en paquetes para su envío vía IP y el reensamblaje y verificación de los mensajes recibidos en paquetes vía IP.

UDP	Acrónimo de User Datagram Protocol. Protocolo dentro del TCP/IP que convierte mensajes de datos en paquetes para su envío vía IP pero no verifica que hayan sido entregados correctamente
URL	Es una secuencia de caracteres que se utiliza para nombrar y localizar recursos, documentos e imágenes en Internet. URL significa "Uniform Resource Locator", o bien, "Localizador Uniforme de Recursos".
UTM	Gestión unificada de amenazas el cual incluye funciones como antivirus, antispyware, antispam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas.
VDOM	Dominio Virtual que permite dividir una red local de forma lógica para su administración.
VNC	(Virtual Network Computing) Programa de software libre basado en una estructura cliente-servidor que permite observar las acciones de un servidor de forma remotamente a través de un equipo cliente.
VoIP	(Voice Over Internet Protocol) Acrónimo de Voz sobre Protocolo de Internet, el cual por sí mismo significa voz a través de internet. Es una tecnología que proporciona la comunicación de voz y sesiones multimedia (tales como vídeo) sobre Protocolo de Internet (IP).
VPN	La Red Privada Virtual es una infraestructura segura que trabaja sobre una red pública, como lo es internet, para conectar usuarios a la red interna a través de un acceso público.
WAN	Red que interconecta dos o más LAN utilizando alguna forma de línea de telecomunicaciones, como las líneas telefónicas o dedicadas de alta velocidad

3.8 Referencias Electrónicas

DISC2013. (15 del 10 de 2017). DISC2013. Obtenido de ¿Qué es el DISC?: http://www.disc.unam.mx/2013/espanol/

Gómez, E. T. (21 del 10 de 2017). Ponencia "seguridad perimetral". Obtenido de Mundo Internet 2005: http://aui.es/IMG/pdf/spam.pdf

José Miguel Baltazar Gález, J. C. (22 del 10 de 2017). Diseño e implementación de un esquema de seguridad perimetral para redes de datos. Obtenido de Caso práctico: Dirección General de Colegio de Ciencias y Humanidades: http://132.248.9.195/ptb2011/mayo/0669103/0669103_A1.pdf

KASPERSKY. (20 del 10 de 2017). ¿Qué es la gestión unificada de amenazas (UTM)? Obtenido de http://latam.kaspersky.com/mx/internet-security-center/definitions/utm

Technet Microsoft. (27 del 10 de 2017). Windows Server. Obtenido de ¿En qué consiste NAT?: https://technet.microsoft.com/es-mx/library/cc753373(v=ws.10).aspx

UNAM/CERT. (14 del 10 de 2017). Acerca de: Misión - CSI -. Obtenido de Misión: http://www.seguridad.unam.mx/acerca/mision.dsc

UNAM/CERT. (14 del 10 de 2017). Acerca de: Objetivos - CSI -. Obtenido de Objetivos: http://www.seguridad.unam.mx/acerca/objetivo.dsc

UNAM/CERT. (14 del 10 de 2017). Acerca de: Visión - CSI -. Obtenido de Visión: http://www.seguridad.unam.mx/acerca/vision.dsc

UNAM/CERT. (15 del 10 de 2017). Coordinación de Seguridad de la Información - CSI -. Obtenido de http://www.seguridad.unam.mx

Martín Zamboni. (20 del 10 de 2017). *D. Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix.* http://homes.cerias.purdue.edu/~zamboni/pubs/thesis-bs.pdf