ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EVALUACIÓN DE TECNOLOGÍAS UTM (UNIFIED THREATMENT MANAGEMENT) Y NGFW (NEXT GENERATION FIREWALL) PARA DETECCIÓN DE VULNERABILIDADES EN LA RED

DIEGO OLIVO SILVA LASCANO

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGISTER EN INTERCONECTIVIDAD DE REDES

RIOBAMBA – ECUADOR

Enero, 2020

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado ***"EVALUACIÓN DE TECNOLOGÍAS UTM (UNIFIED THREATMENT MANAGEMENT) Y NGFW (NEXT GENERATION FIREWALL) PARA DETECCIÓN DE VULNERABILIDADES EN LA RED"***, de responsabilidad del Ing. DIEGO OLIVO SILVA LASCANO, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ing. Marco Vinicio Ramos Valencia; Mg. **PRESIDENTE**	_____ FIRMA
Ing. David Omar Guevara Aulestia; Mg. **DIRECTOR**	_____ FIRMA
Ing. Ricardo Xavier Proaño Alulema; Mg **MIEMBRO**	_____ FIRMA
Ing. Germanía del Rocío Veloz Remache; Mg **MIEMBRO**	_____ FIRMA

Riobamba, Enero 2020

DERECHOS INTELECTUALES

Yo, Diego Olivo Silva Lascano, con cédula de identidad 1804153649, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, y que el patrimonio intelectual generado por el mismo pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

DIEGO OLIVO SILVA LASCANO

C.C.: 1804153649

DECLARACIÓN DE AUTENTICIDAD

Yo, Diego Olivo Silva Lascano, declaro que el presente proyecto de investigación es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

DIEGO OLIVO SILVA LASCANO

C.C.: 1804153649

DEDICATORIA

A mis padres Olivo y Cecilia por su apoyo incondicional en mi superación personal y profesional, a mis hijos Dustin, Diego y Rose por ser mi motor y motivo.

Diego Olivo Silva Lascano

AGRADECIMIENTO

A la Escuela Superior Politécnica de Chimborazo, al Instituto de Postgrado y Educación Continua, a los miembros del tribunal, a la coordinación del programa de maestría de Interconectividad de Redes, por haber sido entes fundamentales en el transcurso de la maestría. Al Hospital General Ambato, por abrirme las puertas para la realización de este trabajo investigativo en tan prestigiosa casa de Salud.

Diego Olivo Silva Lascano

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

LISTADO DE ANEXOS

RESUMEN

Las técnicas de ataques mediante vulnerabilidades de red han mantenido una evolución constante, por lo que es necesario la identificación y protección de intrusiones para evitar un posible riesgo de la información y la caída de servicios que repercuten en la atención a pacientes de hospitalización, emergencia y consulta externa. Se han desarrollado tecnologías para un mejor aseguramiento de la red como son los servidores UTM (Unified Threatment Management) y NGFW (Next Generation Firewall), que ofrecen un conjunto de herramientas para la protección de una red. En la investigación se propone determinar la mejor opción para la detección y protección de vulnerabilidades entre estas dos tecnologías. Se implementan los escenarios en la red y se realizan pruebas para medir los indicadores propuestos. Se determinan valores para: productividad, utilización, disponibilidad, tiempo de respuesta, exactitud. Se toman muestras a las mismas horas del día de cada escenario, se establecen pruebas estadísticas de acuerdo a la investigación y el número de datos; se aplica la distribución t de student con Shapiro-Wilk para comprobación de hipótesis, se plantea un Diagrama de Likert para evaluar de manera cualitativa las variables y se obtienen los indicadores: Productividad Servidor de Red 0% VS NGFW 77% VS UTM 65%, Utilización Servidor de Red 56% VS NGFW 69% VS UTM 58%, Tiempo de Respuesta Servidor de Red -141% VS NGFW 90% VS UTM 70%; en los indicadores de Disponibilidad y Exactitud las dos tecnologías mantienen un valor en el rango muy bueno, sobre un rango de muy deficiente del Servidor del Hospital Ambato. Esto permite determinar la mejora en la disponibilidad de la red con la aplicación de las tecnologías propuestas. Se determina además que de las tecnologías aplicadas el Next Generation Firewall ofrece mejores prestaciones, por lo cual se establece una guía para su implementación en escenarios similares.

Palabras clave: <NEXT GENERATION FIREWALL (NGFW)>, <UNIFIED THREATMENT MANAGEMENT (UTM)>, <VULNERABILIDADES DE RED>, <DETECCIÓN PROTECCIÓN INTRUSIONES>, <FIREWALL>.

ABSTRACT

Attack techniques through network vulnerabilities have maintained a costly evolution, so it is necessary to identify and protect intrusions to avoid a possible risk of information and the fall of services that have an impact on hospitalization, emergency, and hospitalization. External consultation technologies have been developed for better network security such as UTM (Unified Treatment Management) and NGFW (Next-Generation Firewall) servers, which offer a set of tools for the protection of a network. In the investigation, it is proposed to determine the best option for the detection and protection of vulnerabilities between these two technologies. The scenarios are implemented in the network, and tests are carried out to measure the proposed indicators. Values are determined for productivity, utilization, availability, response time, accuracy. Samples are taken at the same times the day of each scenario, statistical tests are established according to the investigation, and the data number. The student t distribution with Shapiro-Wilk is applied for hypothesis testing, a Likert Diagram is proposed to evaluate the variables qualitatively, and the indicators are obtained: Network Server Productivity 0% VS NGFW 77% VS UTM 65%, Use Network Server 56% VS NGFW 69% VS UTM 58%, Response Time Network Server -141% VS NGFW 90% VS UTM 70%; In the Availability and Accuracy indicators the two technologies maintain an outstanding value, over an inferior range of the Ambato Hospital Server. This allows us to determine the improvement in the availability of the network using the application of the proposed technologies. It is also determined that of the techniques applied, the Next Generation Firewall offers better performance, so a guide is established for its implementation in similar scenarios.

Keywords: <NEXT GENERATION FIREWALL (NGFW)>, <UNIFIED TREATMENT MANAGEMENT (UTM)>, <NETWORK VULNERABILITIES>, <INTRUSION PROTECTION DETECTION>, <FIREWALL>.

CAPÍTULO I

1. INTRODUCCIÓN

Según el estudio titulado Estado de la banda ancha en América Latina y el Caribe 2016 realizado por CEPAL; la expansión de redes sociales y la popularidad de mensajería instantánea en Latinoamérica han provocado que el 53 % de la población utilice internet a través de cualquier dispositivo. Ese porcentaje supone un crecimiento del 15% en los últimos tres años, periodo en el que Bolivia y Ecuador fueron los países que más crecieron en acceso a la red, según el estudio. Además, de los más de 300 millones de personas que acceden a internet, un 39% lo hace desde un teléfono móvil. (Cepal, 2016)

El Router que es el dispositivo intermediario entre una red interna y el internet; es el encargado de direccionar los diferentes paquetes a su destino estableciendo el mejor camino mediante la aplicación de un protocolo (Huitema, 2000). Y es aquí el punto crítico en el que sin una adecuada administración se pueden producir vulnerabilidades y poner en riesgo la información en tránsito.

Las instituciones públicas y privadas mantienen el reto de entender el flujo de información generado internamente y con el resto del mundo a través del internet; se deben identificar los riesgos más relevantes para poder neutralizarlos y evitar la interrupción de un proceso manteniendo a salvo la información.

Los NGFW (Next Generation Firewall) son básicamente un cortafuegos que ha incorporado otras funcionalidades de seguridad como antivirus, antispam, antispyware, sistemas de detección de intrusos, entre otras soluciones que permiten minimizar y detectar riesgos, amenazas o cualquier otro problema de seguridad. (S.L., 2018)

El UTM (Unified Threat Management) es un servidor que ha evolucionado de un firewall y ahora posee otros sistemas de seguridad similares a los NGFW, pero este inserta la identidad del usuario en las reglas de firewall establecidas, lo que permite la configuración de políticas sabiendo que usuario se conecta a través de qué dirección IP. Es un firewall de hardware que proporciona un análisis profundo de paquetes que protege a las corporaciones de posibles amenazas. (Agham, 2016)

Cada tecnología con sus prestaciones aporta a la detección de vulnerabilidades, mitigando posibles amenazas; minimizando de esta manera el riesgo de pérdida o alteración de la información sensible de la institución. La aplicación de la presente investigación pretende contribuir directamente a la solución del problema identificado estableciendo una guía a aplicar para la administración de la red.

1.1 Planteamiento del Problema

Los ciberataques son un problema que afecta a la población mundial, a tal punto que se han generado ciberguerras y acusaciones entre gobiernos por intento de robo o de desestabilización de gobiernos. Económicamente se han propagado ataques que comprometen la información pidiendo un rescate a cambio de su recuperación. (País, 2018)

Un estudio realizado por Kaspersky determina al menos 12 ataques de programas maliciosos por segundo en Latinoamérica en un estudio realizado el último año. Este promedio está por detrás de África y Asia y algunos países Europeos. En Ecuador existe un porcentaje del 36,1% de intentos de ataque por usuario conectado; lo que quiere decir que alrededor de 4 de cada 10 usuarios conectados han recibido algún tipo de ataque. (BBC, 2016)

La Dirección Nacional de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública tiene definidas las políticas de acceso y uso de recursos tecnológicos. La ausencia en la aplicación de todas o parte de estas políticas deja a una red y la información de la institución vulnerable.

El Hospital Provincial Docente Ambato brinda acceso a internet a sus usuarios que pueden ser personal administrativo, técnico e invitados. La red queda vulnerable ante la posibilidad de acceso a documentos de los equipos conectados; por parte de los mismos funcionarios, personal técnico, o incluso vecinos que pueden llegar a conectarse. La alteración en la información puede tener severas consecuencias en el desarrollo de las actividades desarrolladas en esta casa de salud.

El entorno hospitalario abarca varios tipos de usuarios que utilizan diferentes aplicaciones. El área administrativa generalmente utiliza el sistema de gestión documental, correo electrónico, aplicaciones del sistema financiero, almacenamiento en la nube. La vulneración de seguridad y posible robo de cuentas electrónicas a estos servicios, pueden ocasionar pérdidas económicas, falsificación de información oficial, perdida de datos. El área técnica que abarca: Consulta Externa, Hospitalización, Farmacia, Imagenología, Laboratorio consume servicios que brinda el mismo hospital con servidores de resultados de laboratorio, imágenes, agendamiento de citas

médicas y acceso a Sistema de registro de Atenciones Médicas que provee el Ministerio de Salud Pública; la vulneración de esta información puede poner en riesgo la salud del paciente de esta casa de salud.

Existen diferentes ataques cibernéticos que afectan a la integridad, la disponibilidad o la confidencialidad de la información. Estos ataques buscan las vulnerabilidades de un sistema y pueden ser a través de virus, robo de información, configuraciones por defecto de los sistemas o accesos no autorizados por parte de usuarios mal intencionados o hackers.(Mieres, 2009)

Los accesos no autorizados a la red pueden permitir robo, modificación o eliminación de la información que viaja a través de ella y la que reposa en los equipos conectados a la red; así como también existe la posibilidad de afectar a servicios inhabilitándolos, afectando a todos los usuarios.

La ausencia de un sistema de detección de vulnerabilidades ha permitido intentos de conexiones no deseadas desde el internet, que han sido identificados luego de caídas de la red y se ha procedido a bloquear direcciones IP a medida que han sido encontradas y a realizar bloqueo de puertos en firewall al encontrarse con una política de aceptar todo por defecto.

Se ha detectado un promedio diario de 50000 alertas en su mayoría con intentos fallidos de conexión hacía los servidores que tienen acceso a través de una IP pública, intentos de denegación de servicio, conexiones a través de equipos zombies, intentos de acceso por parte de usuarios no autorizados a recursos no permitidos dentro de la LAN. Los ataques recibidos son con el protocolo SSH y Telnet a través de puertos aleatorios, con una cadena de conexión en donde se puede identificar el origen de estos paquetes, y el nombre de usuario con el que se intenta obtener acceso al sistema.

Administrativamente se ha detectado que la navegación por parte de los usuarios incluye redes sociales, música en línea, videos, descarga de películas; acaparando todo el ancho de banda y dejando a otros usuarios sin la capacidad de poder realizar sus tareas habituales como investigación y carga de archivos. Se pueden aplicar alternativas de seguridad para protección de la red de los problemas identificados; la tendencia en la evolución tecnológica destaca la aplicación de Firewalls de siguiente generación (NGFW) y de Servidores Unificados de detección de amenazas (UTM). La aplicación de estas tecnologías de detección de vulnerabilidades permite la administración de los accesos y la aplicación de políticas de seguridad y navegación.

1.2 Formulación del Problema

¿La Evaluación de las tecnologías UTM (Unified Threatment Management) y NGFW (Next Generation Firewall) permite elegir la mejor tecnología para la detección de vulnerabilidades?

1.3 Sistematización del problema

- ¿Cuál es la mejor opción para administrar la red en segmentos?
- ¿Qué configuraciones se deben aplicar en el servidor UTM y en el NGFW para asegurar la red y detectar vulnerabilidades?
- ¿Qué pruebas de rendimiento se puede realizar en los entornos propuestos con cada una de las opciones de detección de vulnerabilidades?
- ¿Qué tecnología es la de mejor rendimiento para ser implementada en el Hospital Provincial Docente Ambato?

1.4 Justificación de la investigación

La aplicación de Servidores de Red Firewall, en la actualidad carecen de la capacidad de proteger de una manera integral a la red LAN que se encuentra expuesta a través de la navegación a internet. Se han desarrollado soluciones tecnológicas que integran más servicios de seguridad y una mejor administración de las conexiones ofreciendo una protección adecuada al entorno empresarial. Los servidores UTM y los NGFW, se han venido desarrollando a la par y evolucionando igual que las aplicaciones que se conectan a internet de diferentes formas. Estos trabajan ya no solo en capa de Red como un firewall tradicional, sino que llegan a identificar conexiones en la capa de aplicación administrando de mejor manera el acceso. Por este motivo un análisis entre las dos tecnologías permite determinar la opción que más se ajuste al entorno hospitalario y ofrezca las prestaciones requeridas.

La implementación de dos tecnologías para detección de vulnerabilidades y aseguramiento de la red como son UTM (Unified Threat Management) y NGFW (Next Generation Firewall) permitirán determinar la mejor opción en base a un análisis comparativo de los indicadores de prestación orientados al servicio como: la disponibilidad, el tiempo de respuesta, la exactitud; e indicadores orientados a la eficiencia como son: de productividad y utilización. Los beneficiarios directos todos los usuarios de la red del Hospital Provincial Docente Ambato estableciendo un

nivel de seguridad tanto en la información transmitida como la información almacenada en sus equipos o dispositivos.

Con la aplicación de la propuesta mejorará la disponibilidad del servicio de la red institucional mediante la aplicación de un sistema de detección de vulnerabilidades. Entre las diferentes Unidades Operativas y Hospitales que conforman la Zona 3 de Salud, no existe una administración similar a la propuesta. Al finalizar la investigación se establecerán los lineamientos y políticas que permitan la aplicación de buenas prácticas en cuanto a la administración y uso de la red. Se puede sugerir la réplica entre las diferentes instancias de esta Coordinación Zonal.

1.5 Objetivos de la investigación

1.5.1 Objetivo General

Evaluar las tecnologías UTM (Unified Threatment Management) y NGFW (Next Generation Firewall) para determinar la mejor opción en detección de vulnerabilidades en la red del Hospital General Ambato.

1.5.2 Objetivos Específicos

- Analizar las ventajas y desventajas de las tecnologías UTM (Unified Threatment Management) y NGFW (Next Generation Firewall) para determinar la mejor opción de detección de vulnerabilidades en la red.

- Diseñar los escenarios de prueba tomando en cuenta las políticas de uso de recursos tecnológicos que rige en el Ministerio de Salud Pública del Ecuador para obtener los datos que permitan medir los indicadores de evaluación de cada tecnología.

- Implementar los servidores NGFW y UTM como control de red perimetral para realizar la medición de indicadores de prestación orientados al servicio y de eficiencia.

- Establecer una guía para la implementación de un Sistema de detección de vulnerabilidades, su administración y monitoreo.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes del problema

Se han encontrado un trabajo de investigación antecedente relacionado al presente, a continuación, se detalla lo más relevante.

En el repositorio de la Escuela Superior Politécnica del Litoral, reposa la Tesis de Titulación *"Desarrollo del esquema de seguridad, plan de recuperación ante desastres informáticos y solución para el nivel de exposición de amenazas y vulnerabilidades aplicada a los servidores y equipos de comunicación del centro de datos de la municipalidad de la ciudad del este"* elaborado por el Lsi. Daniel Iván Quirumbay Yagual en el año 2015.

(Quirumbay Yagual, 2015) Realiza un análisis de las Aplicaciones y de los fabricantes más afectados por las vulnerabilidades. Además, enlista herramientas utilizadas para detectar vulnerabilidades. El trabajo concluye que se deben aplicar análisis de vulnerabilidades periódicas a la Infraestructura Tecnológica, principalmente en los servicios que se encuentran expuestos a internet.

2.2 Vulnerabilidades en la red

La vulnerabilidad es considerada como un punto débil, un hueco de seguridad que deja expuesta una red ante posibles ataques cibernéticos poniendo en peligro la seguridad de un sistema. Aunque una sola vulnerabilidad aparente no ser importante una combinación de ellas permitiría a un atacante alcanzar recursos críticos de la red y atentar la integridad de la misma. (Jajodia, Noel, & O'Berry, 2005)

Un atacante puede explotar todas las vulnerabilidades identificadas con el objetivo de atentar la seguridad de una red. Cuantificar los riesgos existentes en una red es muy complicado. Un sistema de análisis de riesgos y vulnerabilidades debe estar en la capacidad de modelar todos los aspectos dinámicos de la red, identificar niveles de ataque, ataques simultáneos, controles de acceso entre otros. (Ammann, Wijesekera, & Kaushik, 2002)

2.3 Ataques de Red

Un ataque de red se puede definir como el intento de acceso a un equipo remoto a través de una vulnerabilidad detectada. Un delincuente cibernético busca tomar control sobre el equipo remoto pudiendo anular servicios, atentar contra la integridad de la información inhabilitando el sistema o dejándolo inhabilitado. (Mieres, 2009)

2.3.1 Tipos de Ataques

Existen un sinnúmero de ataques clasificados en diferente bibliografía, se ha tomado en cuenta los ataques más comunes a los que está expuesta una red informática.

2.3.1.1 Acceso no autorizado

Se da cuando existen intentos de acceso a equipos y servicios a los cuales no se tiene permiso. Se trata de utilizar cuentas predeterminadas de ciertas aplicaciones que no han sido correctamente configuradas o utilizando claves aleatorias. Esto se puede evitar denegando todo y permitiendo solo a ciertos usuarios.(Vieites, 2013)

2.3.1.2 Aprovechamiento de vulnerabilidades conocidas de un programa

Existen varios programas y servicios de red que fueron diseñados sin tomar en cuenta el nivel de seguridad. Un atacante se aprovecha de estas vulnerabilidades que son conocidas para obtener acceso.(Vieites, 2013)

2.3.1.3 Denegación de Servicio

Este tipo de ataques buscan dar de baja el servicio o impiden que otros usuarios tengan acceso al servicio atacado. Se realizan a nivel de la capa de red a través del envío de datagramas elaborados de tal forma que causen daño en las conexiones y estas fallen. También se lo hace en la capa de aplicación enviando instrucciones que afecten al servicio de tal manera que pase muy ocupado o afecte el funcionamiento.(Stallings, 2004)

2.3.1.4 Suplantación de identidad

Un equipo simula las acciones de otro, haciéndose pasar por un equipo perteneciente a la red y con privilegios de acceso. El atacante sigue el rastro de las direcciones IP contenidas en los paquetes. Para protección de estos ataques es necesario verificar la autenticidad y el origen de los paquetes.(Molina, 2012)

2.3.1.5 Eavesdropping

Se trata del fisgoneo en el cual un equipo se configura para escuchar todas las conexiones y capturar datos que no están destinado a él. Una vez conseguidos estos datos se puede obtener muy sensible e importante como nombres de usuario y contraseñas de diferentes aplicaciones. (Vieites, 2013)

2.4 Seguridad de Redes

La seguridad de redes tiene como objetivo mantener la integridad, disponibilidad, privacidad, vigilancia y legitimidad de la información que es manejada mediante un computador, a través de procedimientos que prácticamente se basan en una política de seguridad, la cual permitirá un control adecuado. (Bustamante Sánchez, 2013)

2.5 Gestión de Usuarios

La gestión de usuarios se encuentra definida en la norma ISO 27002. Básicamente, se debe garantizar a los usuarios autorizados un acceso seguro e impedir el acceso a usuarios no autorizados. Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Los procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información. Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema. (ISO, 2008)

El administrador del sistema debe definir un procedimiento de registro de usuarios para otorgar y revocar accesos. Se deben utilizar identificadores de usuario únicos y se concederán permisos de acuerdo al rol que este usuario cumple. Al momento que un usuario cambia sus funciones dentro de la empresa, inmediatamente hay que establecer los nuevos permisos. Adicional a esto se deben incluir cláusulas en los contratos que permitan establecer sanciones si el personal intenta accesos no autorizados. (Dordoigne, 2015)

2.5.1 Pasos para un control de acceso

- **La identificación**. Cada usuario siempre tiene una identificación como un nombre de usuario, un ID, una tarjeta de identificación; que indica quienes son en un sistema. Este paso se lo realiza generalmente al iniciar sesión.

- **La autenticación**. Este es el segundo paso para el control de acceso, existen diferentes formas de verificación siendo la más básica la contraseña, sin embargo, también se cuenta con escáneres biométricos, reconocimiento de voz, entre otros. El objetivo de la autenticación es verificar la identidad del usuario del sistema.
- **La autorización.** Una vez que el usuario se autentica es autorizado para manejar utilizar un sistema. A un usuario generalmente se le da autorización para el uso de únicamente una parte de los recursos del sistema en función de sus tareas asignadas dentro de una organización.

  (Aguilera, 2011)

2.5.2 Control de accesos en red

- Política de uso de los servicios de red. Es necesario que la organización tenga definidas las políticas de acceso y uso de la red de tal forma que sean aplicables.

- Autenticación para conexiones externas. Se pueden establecer conexiones fuera de la red de área local de la institución. Una vez cumplidos los pasos para el control de acceso de usuario se le permiten determinadas conexiones establecidas para el desarrollo de sus actividades.

- Identificación de equipos en la red. Cada dispositivo de la red debe estar plenamente identificado, se lo puede realizar a través de la MAC de cada equipo para un control de quien accede y hacia donde desea acceder.

- Control de enrutamiento en la red. Según las necesidades y las reglas de negocio, un usuario deberá poder salir hacia otra red de tal forma que esto sea transparente.

  (Forouzan, 2007)

2.6 Gestión de Redes

Es un conjunto de tareas que abarcan muchos aspectos como el despliegue, la coordinación y la integración del hardware y el software con el fin de monitorear, probar, sondear, configurar, controlar y evaluar los recursos de una red para garantizar el servicio.(Forouzan, 2007)

Una red de comunicaciones consta de dos elementos básicos: los Elementos de Red que son todos los equipos que pueden ser gestionados y los Elementos de Gestión que son los encargados del monitoreo y control de los elementos de red.

Con la evolución de las redes de datos, estas se han vuelto más complejas y difíciles de administrar; están más expuestas a sufrir fallos y dejar de funcionar en ciertos segmentos. La falta de gestión en los equipos administrables hace más difícil la tarea de encontrar errores y retrasa tiempos valiosos en el flujo de la información. Cada equipo puede tener un sistema de gestión y dependiendo la marca la administración difiere, por lo tanto, sería necesario mantener distintas configuraciones. La gestión de red busca unificar en un solo sistema toda la administración.(Bertolín, 2008)

2.7 Monitoreo de redes

El monitoreo o monitorización de redes se refiere a la observación y el análisis del estado y comportamiento de cada equipo que compone la red a través de un sistema de gestión; este sistema se encuentra en constante ejecución en busca de errores por componentes defectuosos o lentos y emite algún tipo de alerta al administrador de la red. (Maiwald & Miguel, 2005)

2.8 Indicadores de prestación

Como resultado del monitoreo en la red se obtienen indicadores de prestación; hay que saber tomar la decisión de qué indicadores seleccionar para medir la calidad y eficiencia de la red. Los indicadores obtenidos pueden ser demasiados y con datos de difícil comprensión; así como también pueden existir indicadores que maneja una marca específica de equipos.

Existen dos categorías de prestaciones:

- **Orientados al servicio.** Miden el grado de satisfacción del usuario frente al servicio recibido.
    a. Disponibilidad. Porcentaje de tiempo en que un sistema de red está activo
    b. Tiempo de respuesta. El tiempo que tarda una respuesta después de una petición por parte de un usuario.
    c. Exactitud. Porcentaje del tiempo en el cual no hay errores en la transmisión y entrega de datos.
- **Orientado a la eficiencia.** Mide el costo para alcanzar el servicio hasta que llegue al usuario.
    a. Productividad. Tasa con la que ocurren eventos orientados a la aplicación
    b. Utilización. Porcentaje de uso de un recurso; sirve para eliminar cuellos de botella.

    (Maiwald & Miguel, 2005)

2.9 Servidor UTM

UTM (Unified Treath Management), es un software que trabaja más allá de ser un simple firewall que bloquea o permite conexiones. Este no solo protege de la intrusión, sino también de filtrado de contenido, spam, detección de intrusiones, equilibrio de carga, prevención de robo de datos y funciones antivirus, gestionadas por múltiples sistemas. (Moreno, 2010)

Un UTM inserta identidad al usuario que está accediendo a través del firewall, y permite identificar a un usuario por su nombre en lugar de una dirección IP; protege de este modo la falsificación de direcciones IP para acceder a un sistema y trabaja en el nivel de aplicación. (Martínez, 2017)

2.9.1 Ventajas de UTM

- Menor Complejidad: Integra varios productos en uno.
- Facilidad de Implementación: Se puede instalar de forma remota
- Sinergias con software de alta gama: Se puede administrar de forma remota sin necesidad de la presencia de personal de seguridad en sitio.
- Baja interacción del operador: El sistema se encarga de la detección de vulnerabilidades minimizando el mantenimiento y mejorando la seguridad.
- Fácil solución de problemas: Cuando una tecnología falla es más fácil intercambiar con soluciones en línea rápidas.

(Agham, 2016)

2.10 Servidor NGFW

Los firewalls de nueva generación, Next-Generation Firewall (NGFW), surgieron para revolucionar la seguridad de la red tal y como la conocíamos hasta ahora. Los firewalls tradicionales se limitan a la inspección de paquetes por estado y a reglas de control de acceso, pero a medida que los hackers se hacen más sofisticados, las amenazas son más avanzadas y este sistema ha dejado de ser eficaz. Con el fin de proteger un negocio de amenazas en constante evolución, el Firewall de Nueva Generación debe ser capaz de ofrecer un nivel más profundo de seguridad de red**.** (Benjumea Ospino, 2016)

2.10.1 Ventajas de NGFW

- Escaneo del tráfico de aplicaciones: Escanea todo el tráfico en la capa de red y capa de aplicación
- Categorización y Visualización: Permite analizar y visualizar todo el tráfico por medio de la identificación y categorización del tráfico
- Política de control granular: Permite crear e implementar políticas sobre la aplicación brindando completo control sobre el tráfico
- Gestión de ancho de banda: Prioriza el ancho de banda de acuerdo a la aplicación
- Bloqueo de Malware: Implementa detección y bloqueo de malware
- Control de aplicaciones distribuidas: Aplica el control y la política en cualquier sitio distribuido.
- Proporcionar rendimiento óptimo: Controla las aplicaciones sin perder las capacidades del tráfico de la red.

(Martínez, 2017)

2.11 Análisis Comparativo entre Tecnologías UTM y NGFW

El UTM nace de la idea de integrar en un solo servidor las soluciones disponibles de seguridad existente, el NGFW busca agregar a las funciones de firewall un control sobre el tráfico generado por las aplicaciones y la implementación en la detección/protección de intrusiones. En un concepto muy general las dos tecnologías buscan y logran el mismo objetivo que es la protección de amenazas ante las posibles vulnerabilidades que puede presentar la red. En la siguiente tabla se muestra las integraciones que posee cada tecnología.

Tabla 1-2: Integración de Tecnologías de NGFW y UTM

Parámetro	UTM	NGFW
Inspección con estado	Soporta	Soporta
Cliente	Pequeña y Mediana Empresa	Empresarial
Rendimiento	Inferior a NGFW	Superior a UTM
Filtrado de tráfico	Soporta	Soporta
NAT	Soporta	Soporta
VPN	Soporta	Soporta
Filtrado de contenido web	Soporta	Soporta
Conciencia de nivel de aplicación	Soporta	Soporta
Servicios de reputación e identidad	Soporta	Soporta
Administración de ancho de banda	Soporta	Soporta
IPS	Soporta	Soporta
Antivirus y antispam	Soporta	No soporta
Seguridad de e-mail	Soporta	No soporta
Prevención de pérdida de datos	Soporta	No soporta

Realizado por: Diego Silva, 2019

El enfoque de cada tecnología va dirigido dependiendo sus objetivos comerciales, de este modo el UTM es comercializado para pequeñas y medianas empresas, mientras que el NGFW para entornos empresariales grandes con gran manejo de usuarios. Mientras el UTM integra más servicios el rendimiento disminuye, pues dependiendo del entorno a aplicarse es probable que no necesite todos los paquetes de seguridad instalados, disminuyendo el rendimiento con servicios no requeridos.(S.L., 2018)

A pesar de ser términos muy diferentes, las empresas que ofertan soluciones de seguridad permiten elegir en un mismo equipo la instalación de Firewall, UTM o NGFW, básicamente el cliente elige el tipo de paquetes a ser integrados en el mismo dispositivo.

El término UTM aparece en el año 2004 integrando las soluciones de seguridad disponibles, pero los requerimientos cada vez son más exigentes y no todos los equipos pueden soportar está integración. Es aquí cuando las grandes empresas de seguridad de redes dan origen a los Firewall de Siguiente Generación con la capacidad de gestionar tráfico en capa 7. (Martínez, 2017)

Tomando como referencia el análisis de tecnologías Firewall del 2015 presentado en el cuadrante de Gartner (Empresa consultora y de investigación de tecnologías de la información con sede en

Stanford Connecticut, Estados Unidos), Se observa cuáles son las tecnologías que están como líderes del sector en lo referente a firewall de próxima generación para empresas. Según lo analizado en Gartner menos de un 40% de las empresas con conexión a Internet tienen en cuenta los Firewall de próxima generación y para el año 2018 esta cifra aumenta en un 85% debido a que las empresas se están dando cuenta de los beneficios de implementación para aplicaciones y el control de los usuarios. (S.L., 2018)

El mercado de los Firewall sigue evolucionando en productos de nueva generación, con nuevas características para mejorar el cumplimiento de las políticas (aplicaciones y usuarios), detectar nuevas amenazas mediante los sistemas de prevención de intrusiones (IPS), el uso de las VPN (Redes privadas virtuales), manejo de servicios web o transferencias de datos seguros o cifrados mediante la utilización del protocolo Secure Sockets Layer (SSL), que en gran medida están en las funcionalidades de los Firewalls. Sin embargo, los Firewall de próxima generación no integran todas las funcionalidades de seguridad de red en un solo equipo o todo en uno como los productos UTM; equipos o tecnología adecuada para pequeñas y medianas empresas. (Moreno, 2010)

La tecnología NGFW se destaca por las siguientes funcionalidades: Detección y decodificación de protocolos de aplicaciones; el firewall NGFW decodifica las aplicaciones codificada en la capa de socket seguro SSL, si la regla de política está definida para permitir el tráfico, este se codifica nuevamente y se transmite hacia su destino. Ejemplo Facebook.com Filtrado URL: basado en listas negras actualizadas el firewall NGFW puede restringir o dejar pasar URLs según las reglas definidas de filtrado, pero adicionalmente se puede personalizar las reglas de filtrado de URLs permitiendo accesos a sitios restringidos a usuarios con contraseñas. Descifrado de protocolos de aplicaciones y firmas de aplicaciones: con el descifrado de aplicaciones el firewall NGFW puede establecer si se está aplicando conexiones seguras o no y puede aplicar firmas o certificados digitales para aplicaciones seguras.(Martínez, 2017)

Análisis heurísticos o de comportamiento: cuando se combina las técnicas de identificación de aplicaciones con descifrado de protocolos y firmas digitales es posibles bloquear múltiples amenazas y además tener un buen control de uso de aplicaciones web. Prevención de amenazas: El firewall realiza la detección y bloqueos de amenazas, virus, spyware o exploits mediante la utilización de un motor de bases de datos de prevención en tiempo real. Es decir, el equipo ofrece gran velocidad de procesamiento que no afecta los tiempos de respuestas aun haciendo el análisis de datos de manera granular.

Presenta una interfaz gráfica que facilita la configuración, la gestión de seguridad y el monitoreo del tráfico de la red de una manera eficiente. Control y filtrado de archivos y datos los

administradores de TI o de seguridad informática pueden aplicar políticas para reducción de riesgos asociados a transferencias de archivos, por tipo de archivos, transferencias de tramas de datos confidenciales y control de transferencias.

Cumple las funcionalidades de túneles SSL, VPN extremo a extremo de usuarios y VPN site-to-site; para establecimiento de conexiones seguras con validación de usuario y contraseñas. La tecnología de NGFW cuenta con la protección total para IPv6. Posee un generador de reportes de análisis de amenazas y vulnerabilidades en tiempo real, facilitando la gestión unificada de amenazas. La tecnología permite establecer políticas basado en aplicaciones, que permiten la aplicabilidad de las políticas para los siguientes controles:

- Denegar acceso a la red de determinados tipos de aplicaciones, como por ejemplo peer-to-peer y servicios proxy.
- Permitir accesos a usuarios como se establece en directorio activo.
- Aplicar políticas de uso de aplicaciones Web mail y de mensajería instantánea; inspeccionando virus, spyware y exploits de vulnerabilidades, todo en una sola norma de política.
- Identificar transferencias de información confidencial y bloquear, permitir o enviar alertas acerca de quienes transfieren los datos.
- Aplicar políticas de filtrado Web, además informándole al usuario sobre la opción de continuar navegando en un sitio no seguro.
- Aplicar reglas de filtrado de cortafuegos basadas en el puertos entrantes y salientes combinadas con reglas de filtrado basadas en aplicaciones para facilitar la transición a cortafuegos de última generación.

(Stallings, 2007)

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Tipo y Diseño de Investigación

La presente investigación es de tipo cuasi-experimental, no se basa solamente en la descripción de conceptos porque se llevarán a cabo pruebas posteriores a la implementación de escenarios tanto con el Servidor UTM como con el servidor NGFW para la detección de vulnerabilidades y así determinar la mejor opción en base a los resultados obtenidos de los indicadores de cada variable para una adecuada administración de la red.

3.2 Métodos de Investigación

- ***Método deductivo*** Permite llegar a partir de las pruebas realizadas sobre los escenarios tanto con NGFW como con UTM a determinar mediante indicadores específicos la mejor opción para la aplicación y administración de la red institucional.

- ***Método inductivo***, al realizar el análisis de los escenarios de prueba implementados, además de las políticas establecidas por el MSP; se llega a establecer políticas específicas de aplicación de las diferentes opciones para cada caso de estudio.

- ***Método analítico***, al aplicar este proceso se podrá realizar el estudio del escenario con NGFW y con UTM y se puede comparar cada ítem llegando a determinar la mejor opción para cada caso.

3.3 Enfoque de la Investigación

El trabajo de investigación está orientado con un enfoque cuantitativo netamente, porque se obtendrán valores numéricos exactos de cada uno de los ítems establecidos para medir la prestación de las dos tecnologías propuestas; permite realizar la evaluación para determinar la mejor opción a ser elegida según el caso de estudio.

3.4 Alcance de la Investigación

Se realiza una investigación correlacional porque se establecerá una comparación entre las dos variables además de las tecnologías propuestas que serán medidas mediante indicadores que establecen la relación directa en la aplicación.

3.5 Población de Estudio

La población de estudio de la presente investigación está conformada por el universo de paquetes recibidos tanto en el servidor del Hospital General Ambato, como en las implementaciones de servidores UTM y NGFW, los mismos que deben ser analizados para la detección de vulnerabilidades por la una y la otra tecnología. El número de paquetes es muy variable durante el día, se ha realizado el monitoreo de la red durante el período de 7 días obteniendo un promedio diario de 18’541.440 paquetes; por lo cual se considera que existe una población infinita.

Además, para el análisis de los indicadores de productividad el universo comprende el número de alertas de detección de vulnerabilidades de cada tecnología, en las pruebas realizadas al servidor instalado para el control de red en el Hospital General Ambato, los logs diarios de intentos de acceso fallidos sobrepasan los 30200 registros; lo cual también se considera un universo infinito.

3.6 Unidad de Análisis

La unidad de análisis está conformada por el número de paquetes de datos a ser analizados, y las detecciones de vulnerabilidades.

3.7 Muestra

La muestra tomada, es una muestra no probabilística, pues la captura de los paquetes para la muestra, se lo va a realizar en dos intervalos con carga de usuarios a partir de las 11:30 que es la hora pico de uso de la conexión de red y a las 23:30 sin carga de usuarios hasta obtener el número de paquetes requeridos por la muestra en un período de 30 días.

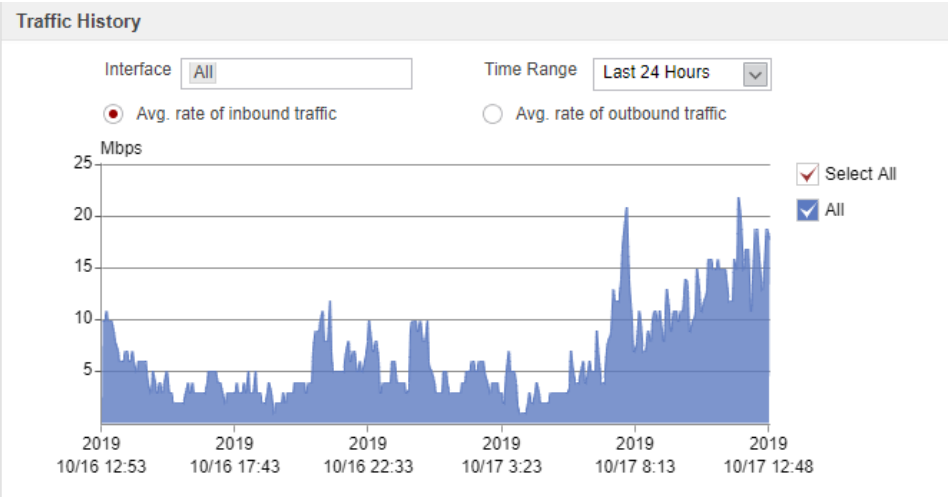


Figura 1-3: Uso de Red de Datos del Hospital General Ambato

Realizado por: Diego Silva, 2019

Se cuenta con una población infinita, por lo cual se debe aplicar la fórmula:

$$n = \frac{Z^2.p.q}{e^2}$$

Dónde:

Z = Nivel de confianza = 95% = 1,96

p = Porcentaje de la población que tiene el atributo deseado = 0,5

q = Porcentaje de la población que no tiene el atributo deseado (1-p) = 0,5

e = Error de estimación máximo aceptado 5%

n = Tamaño de la muestra

$$n = \frac{1{,}96^2.0{,}5.0{,}5}{0{,}05^2}$$

$$n = 384{,}16 \text{ paquetes}$$

Se tomarán 384 paquetes diarios o detecciones de vulnerabilidades según el caso durante el lapso de 30 días por cada escenario para obtener información confiable.

3.8 Técnica de Recolección de Datos

Observación directa. Al ser un trabajo experimental la observación directa es la mejor técnica de recolección de datos, pues de esta forma se pueden recopilar los resultados obtenidos mediante las herramientas utilizadas para la medición de cada ítem evaluado.

3.9 Instrumentos de Recolección de Datos Primarios y Secundarios

Para la variable independiente se utiliza el software de monitoreo propio instalado y configurado en los servidores NGFW y UTM, permitiendo así evaluar los indicadores planteados. Esta herramienta permite a través del protocolo SNMP recoger la información necesaria para la evaluación de diferentes ítems y presenta la información en forma gráfica.

En cuanto a la variable dependiente se usan herramientas para recolección como el ping, el mismo que sirve para realizar análisis paquetes y determinar los parámetros requeridos y ayuda en la toma de decisiones.

3.10 Instrumentos para Procesar Datos Recopilados

Procesamiento Electrónico de Datos. Los datos recopilados se realizan su procesamiento en un software estadístico para facilitar la obtención de resultados.

3.11 Implementación de Escenarios de Prueba

A continuación, se muestra la topología de la red de datos implementada en el Hospital General Ambato, sobre la cual se implementarán los escenarios reales de prueba tanto para el Servidor UTM, como para el NGFW. La aplicación en un escenario real permite la toma de muestras que reflejarán resultados fiables.

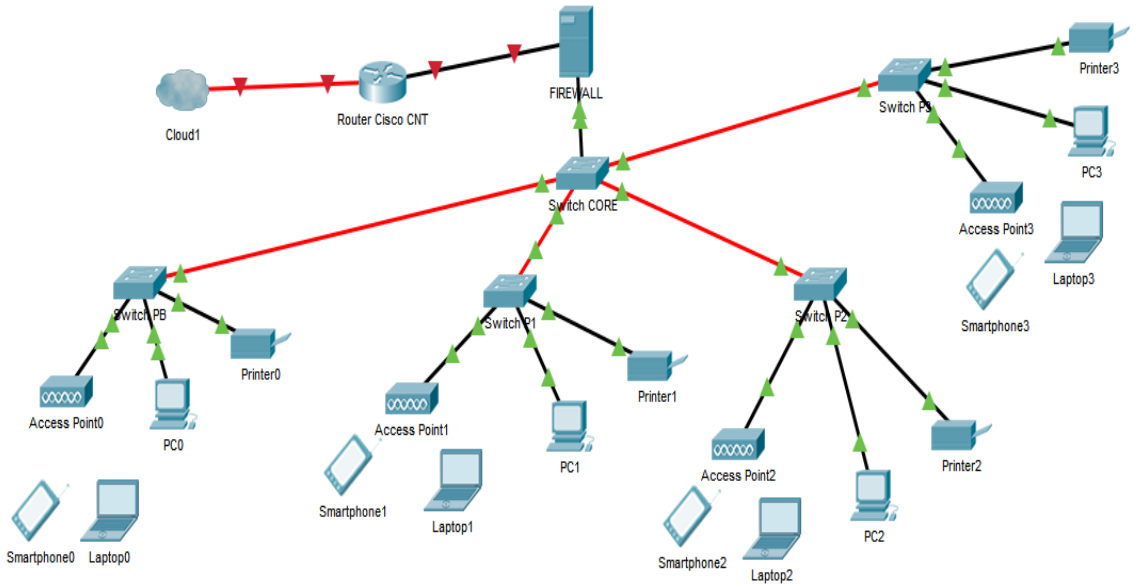


Figura 2-3: Esquema de Red de Datos del Hospital General Ambato

Realizado por: Diego Silva, 2019

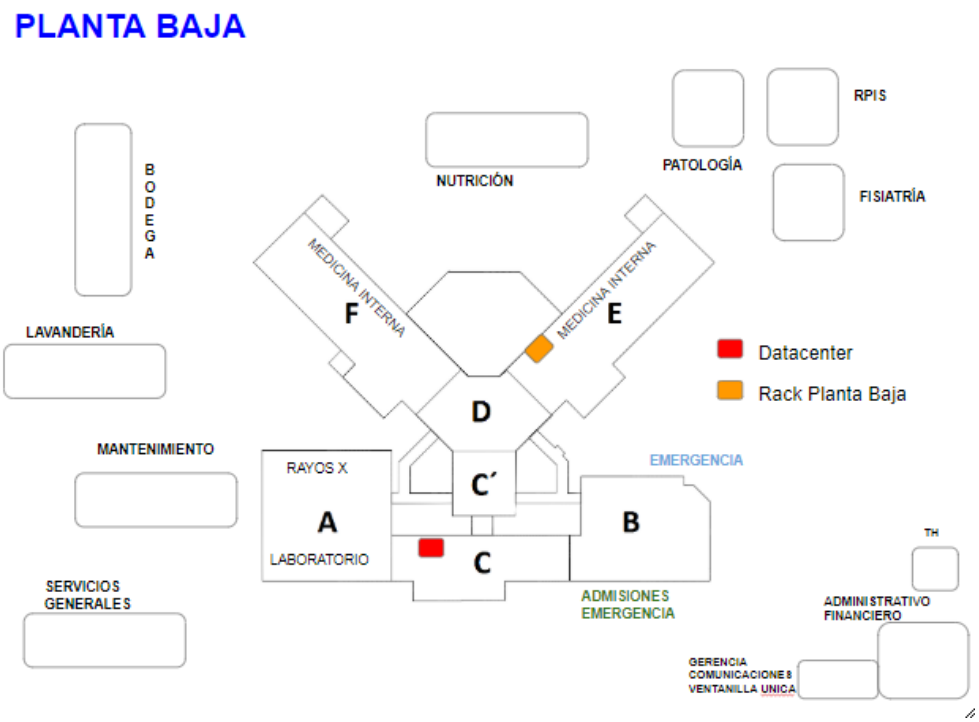


Figura 3-3: Distribución de áreas Planta Baja

Realizado por: Diego Silva, 2019

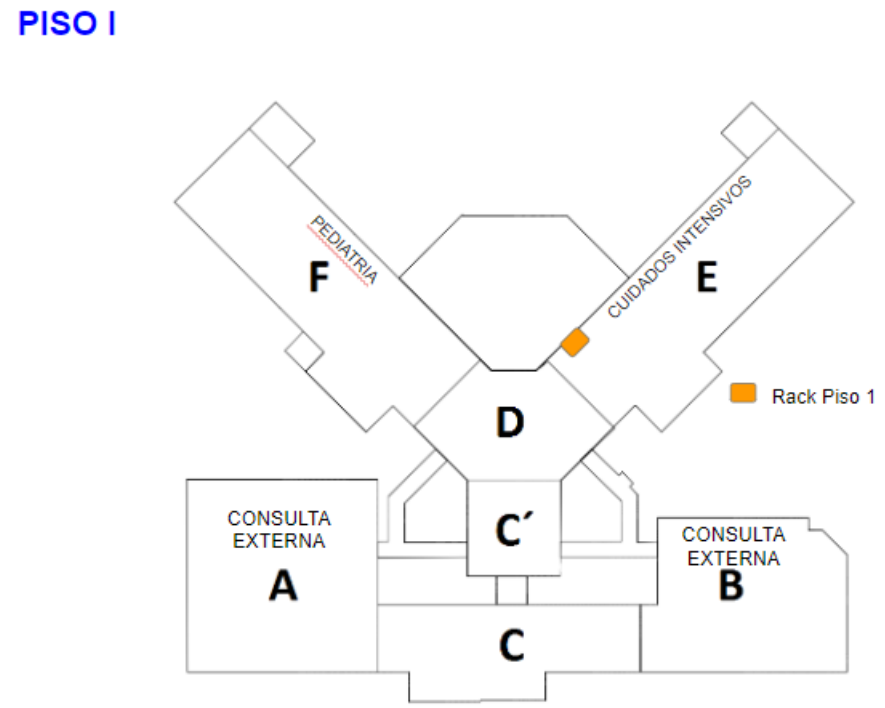


Figura 4-3: Distribución de áreas Piso 1

Realizado por: Diego Silva, 2019

PISO II

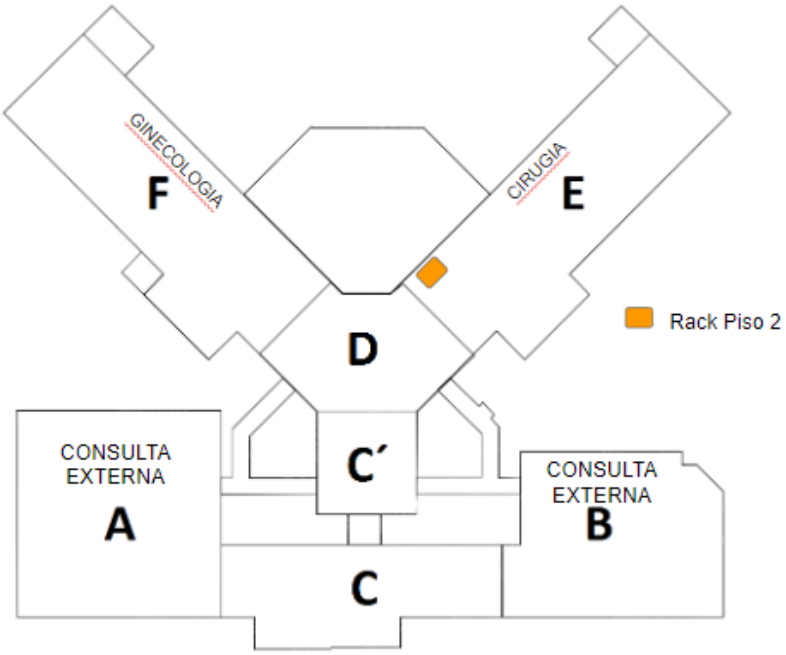


Figura 5-3: Distribución de áreas Piso 2

Realizado por: Diego Silva, 2019

PISO III

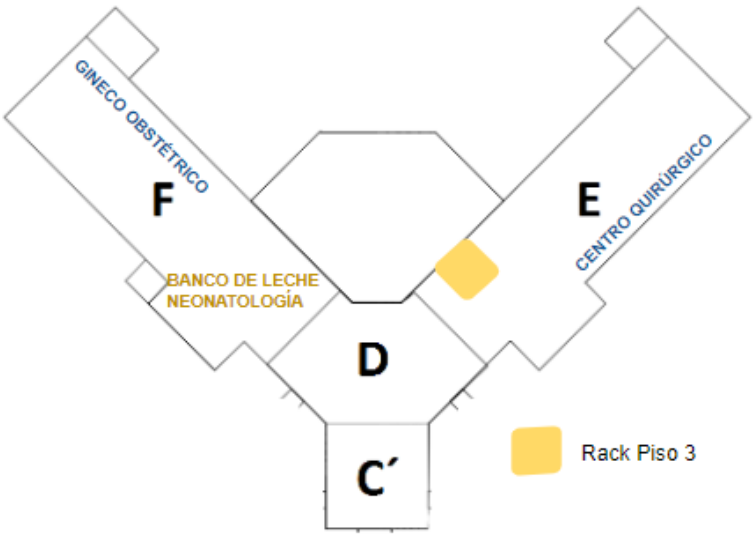


Figura 6-3: Distribución de áreas Piso 3

Realizado por: Diego Silva, 2019

3.11.1 Especificaciones Técnicas de los Equipos de Conexión Instalados

Tabla 1-3: Especificaciones Técnicas de Equipos de Conexión

EQUIPO	**MARCA / MODELO**	**ESPECIFICACIONES TÉCNICAS**
Servidor UTM	Acer / Veriton	Procesador: Intel Core I7 3.4 GHz Memoria: 8GB Disco Duro: 1 TB
Servidor NGFW	Huawei / USG 6300	Dimensiones (H x W x D) mm 44,4 x 442 x 421 Interfaces fijas 8 x GE (RJ45) + 4 x GE (SFP) Puerto USB2.0 2 x puertos USB Ranura de expansión 2 WSIC Expansión de E / S WSIC: 2 x 10 GE (SFP +) + 8 x GE (RJ45), 8 x GE (RJ45), 8 x GE (SFP), 4 x GE (RJ45) BYPASS Almacenamiento local Opcional. Admite un disco duro de 300 GB o 600 GB (el disco duro es intercambiable en caliente, pero la tarjeta de disco duro no lo es). Fuente de alimentación de corriente alterna 100V a 240V, 50 / 60Hz
Switchs	Huawei / C12800	Capacidad de conmutación 30/258 Tbit / s Reenvío de rendimiento 17,280 Mpps Ranuras de servicio 4 Diseño de flujo de aire Diseño estricto de flujo de aire de adelante hacia atrás Virtualización de dispositivos VS (virtualización 1:16) Cluster Switch System (CSS) 2 Virtualización de red M-LAG VXLAN y VXLAN puente BGP EVPN QinQ acceso VXLAN
Controladora Wifi	Huawei / AC 6605	Puerto 20 x GE + 4 x GE Combo + 2 x 10GE PoE PoE de 24 puertos Fuente de alimentación 1 + 1 CA o 1 + 1 CC Capacidad de reenvío 10 Gbit/s Cantidad máxima de AP gestionados 1024 Cantidad máxima de usuarios con acceso 10 000 Redes AP-AC Redes de capa 2 o capa 3

		Modos de transmisión Transmisión directa (transmisión local) o transmisión por túneles (o transmisión centralizada) Modos activo/standby del controlador de acceso 1 + 1 HSB o redundancia N + 1 Protocolos de radio 802.11a/b/g/n/ac/ac Wave 2
Access Point	Huawei / AP6050DN	Dimensiones (altura x ancho x profundidad) 53 mm x 220 mm x 220 mm Entrada de alimentación 12 V CC ±10 % Alimentación PoE: cumple con la norma 802.3at del IEEE. Consumo máximo de potencia 22,9 W (sin incluir la potencia de salida del puerto USB) Temperatura de funcionamiento −10 °C a 50 °C Tipo de antena AP6050DN: Antena integrada omnidireccional y de dos bandas AP6150DN: Antena externa omnidireccional y de dos bandas Cantidad máxima de usuarios simultáneos ≤ 512 Potencia máxima de transmisión 2,4 GHz: 26 dBm (potencia combinada) 5 GHz: 25 dBm (potencia combinada) Notas: La potencia de transmisión real depende de las leyes y normativas locales. La potencia de transmisión se puede ajustar de un puerto de radio de 2,4 G o 5 G a 1 dBm, en incrementos de 1 dB. MIMO: Secuencias espaciales 4 x 4:4 (SU-MIMO) 4 x 4:3 (MU-MIMO) Protocolos de radio 802.11a/b/g/n/ac/ac Wave 2 Velocidad máxima 2,53 Gbit/s

Fuente: Manuales de Equipos
Realizado por: Diego Silva, 2019

3.11.2 Distribución de Red

Tabla 2-3: Distribución de Puntos de Red

GRUPO	UBICACIÓN	PUNTOS DE RED
Emergencia	Planta Baja – Fase 2	58
Admisiones, Atención al Usuario	Planta Baja – Fase 2	35

Administrativo, Laboratorio, Rayos X	Área de Contingencia	128
Consulta Externa	Piso 1 - Fase 2 Piso 2 - Fase 2	47 49
Hospitalización	Planta Baja, Piso 1 – Fase 2 Piso 2 – Fase 2 Piso 3 – Fase 2	60 60 60 60
Administración de Servidores	Data Center – Fase2	48
Administración de Firewalls	Data Center – Fase2	48

Fuente: Planos del Hospital General Ambato
Realizado por: Diego Silva, 2019

3.11.3 Configuraciones a aplicarse en los Escenarios de Prueba

Se toma en cuenta que la implementación de los escenarios de prueba está dirigida a la detección de vulnerabilidades, por lo tanto, se aplican las configuraciones para seguridad perimetral. La administración de Direccionamiento IP, Control de Acceso a la red, definición de VLANS se encuentra administrado en el Switch de Core y en los Switchs de cada cuarto de datos.

Las principales configuraciones tomadas en cuenta para el escenario de prueba son:

1. Configuración de Interfaz Externa (Internet)
2. Configuración de Interfaz Interna (LAN)
3. Definición de objetos de red
4. Configuración de Cortafuegos
5. Configuración de Filtrado de paquetes
6. Configuración de Sistema de Detección de Intrusos IDS, y de Protección de Intrusos IPS.

3.11.4 Implementación Servidor UTM

Un Unified Threat Management se considera la evolución de los firewalls, y básicamente consiste en combinar varias funciones como antivirus, antispyware, antispam, firewall de red, filtrado de contenidos, detección y protección de intrusos. (Kolodgy, 2004)

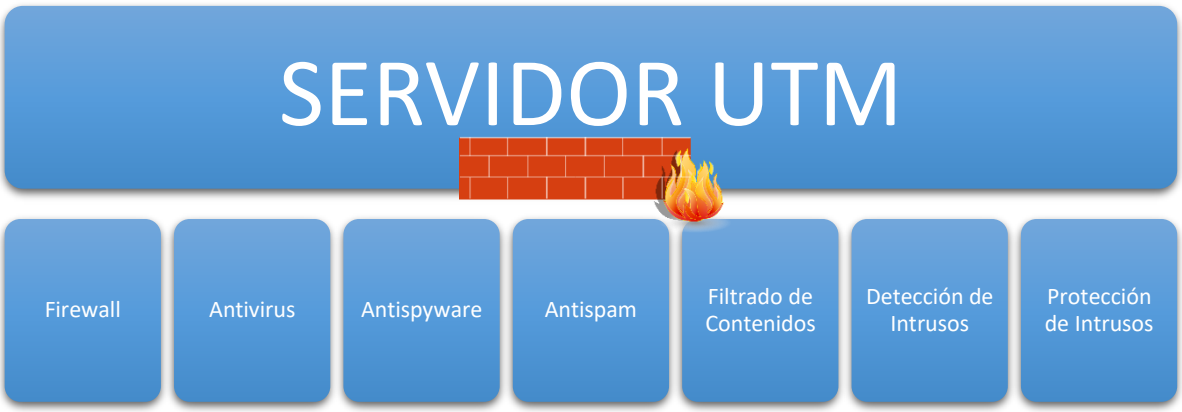


Figura 7-3: Descripción de Servidor UTM

Realizado por: Diego Silva, 2019.

Entre las múltiples opciones que existen de servidores UTM, se pueden listar: ClearOS, Zentyal, Endian, Astaro entre los más conocidos; tienen los mismos requerimientos de instalación; sin embargo, ClearOS, Endian y Astaro tienen una mayor parte de módulos licenciados. Zentyal a pesar de tener módulos licenciados permite la aplicación de la configuración requerida para el escenario de pruebas.

3.11.4.1 Instalación de Zentyal

Link de descarga de Imagen ISO: http://download.zentyal.com/zentyal-6.0-development-amd64.iso

- ✓ Una vez iniciada la instalación proceder con la elección del idioma.
- ✓ Se elige el tipo de Instalación, para este caso particular MODO EXPERTO.
- ✓ Elección de Ubicación Geográfica.
- ✓ Elegir si se desea realizar una detección del teclado.
- ✓ Se identifica la disposición del teclado luego de una serie de preguntas y continuar.
- ✓ Se inicia la carga de componentes necesarios adicionales para la instalación.
- ✓ Inicia la configuración de la red con la configuración del Nombre de la Máquina.
- ✓ Registrar el nombre de usuario del Sistema.
- ✓ Configurar Contraseña.
- ✓ Confirmar contraseña.
- ✓ El instalador inicia la búsqueda de configuración del reloj a través de la red.
- ✓ La detección indica la ubicación del huso horario y se acepta.

- ✓ Tomando en consideración que la instalación del sistema ocupará todo el espacio en disco porque se está instalando un equipo para este fin elegir particionado Guiado con la utilización de todo el disco.
- ✓ Se procede a elegir el único disco disponible para aplicar el particionado.
- ✓ Aceptar la advertencia de escritura en los discos, los cambios son irrevocables.
- ✓ Elegir administración remota, de este modo se minimiza el uso de recursos de una interfaz gráfica tanto de procesador como de memoria.
- ✓ Se inicia la instalación del sistema y la copia de los archivos al disco duro.
- ✓ En caso se requiera una conexión a través de un proxy, se debe establecer.
- ✓ Aceptar la instalación del GRUB en el registro principal de arranque.
- ✓ Aceptar la configuración del reloj en hora UTC.
- ✓ Aceptar la confirmación de terminación de configuración.
- ✓ Primer Inicio del servidor Zentyal.
- ✓ Una vez iniciado el sistema se puede apreciar la versión sobre la cual está instalado el servidor y el logueo.
- ✓ Después de acceder con las credenciales registradas en la instalación, se aprecia información importante para la administración del servidor.
- ✓ Configuración inicial posterior a la instalación. Se accede a través de un navegador web a mediante la ip configurada en la instalación y el siguiente puerto 192.168.125.1:8443. Se accede a la interfaz del Servidor Zentyal y solicita las credenciales de acceso.
- ✓ Después de haber iniciado sesión, aparece la pantalla que indica la Configuración Inicial.
- ✓ Se debe elegir los paquetes que se van a instalar, para el caso de estudio son necesarios los servicios de: DNS(Domain Name System), DHCP(Dynamic Host Configuration Protocol), Firewall, Antivirus, Proxy, FTP(File Transfer Protocol), IPsec(Internet Protocol Security), IPS (Intrussion Prevention System), los mismos que serán configurados posteriormente.
- ✓ Se muestra el resumen de los paquetes a instalar.
- ✓ Se muestra la descarga e instalación de paquetes necesarios y actualizados.
- ✓ Una vez concluido la descarga e instalación aparece la ventana de configuración inicial de red.
- ✓ Se elige la interfaz que se va a conectar a internet y la interfaz que se conecta a la red interna; al realizar esto se aplican automáticamente configuraciones predeterminadas de red para establecer un primer nivel de seguridad en la red. Se advierte que la interfaz configurada como externa no permitirá conexiones para configuración del servidor.

- ✓ Posteriormente se procede a configurar las direcciones IP que serán utilizadas en cada interfaz de red.
- ✓ Se determina el nombre del dominio y se indica si va a trabajar como servidor de dominio principal o adicional.
- ✓ Al aceptar los cambios se indica una advertencia de los cambios a ser aplicados por el cambio de nombre de Dominio.
- ✓ Al finalizar la configuración inicial se proceden a aplicar los cambios requeridos en el sistema.
- ✓ Una vez aplicados los cambios, se muestra la confirmación de instalación exitosa.
- ✓ Una vez concluido el proceso se puede acceder al Dashboard que muestra un resumen del funcionamiento del servidor Zentyal.

3.11.4.2 Configuración de Firewall Zentyal

Zentyal actúa como cortafuegos entre la red interna y el internet. La interfaz de red conectada al router del proveedor ISP, se debe marcar como externa; de esta manera se aplican ciertas políticas por defecto, como es denegar todo intento de conexión hacia la interfaz externa. Las conexiones internas se encuentran denegadas a excepción de los servicios ya definidos y configurados, cada servicio añade su propia excepción, pero puede ser modificada en cualquier momento por el administrador del sistema.

Objetos de red.- El Servidor UTM, implementa el tipo de administración mediante el uso de objetos de red, los mismos que deben ser definidos para ser utilizados más adelante en la configuración de los servicios tomando al objeto y concediendo permisos o eligiendo el comportamiento del mismo.

- ✓ Después de haber creado el nuevo objeto, se despliega la lista de objetos existentes; cada objeto tiene la opción de agregar miembros y de ejecutar las acciones de eliminar, actualizar o clonar un objeto.
- ✓ Al dar clic en el botón de configuración de miembros, se despliega la lista de miembros de este objeto.
- ✓ Dar clic en añadir nuevo y definir el nombre del rango de miembros que se está creando.
- ✓ En el menú de cortafuegos se encuentran los 4 tipos de filtrado de paquetes que controla Zentyal: desde las redes internas, desde las redes externas, para las redes internas, para el tráfico saliente de Zentyal.

- ✓ Verificar en el primer módulo de configuración los servicios a los cuáles pueden acceder los miembros de la red local al Servidor UTM.
- ✓ El acceso desde redes externas esta denegado por completo.
- ✓ La configuración del tráfico de las redes internas permanece abierta, posteriormente se verificará si es necesario limitarlo.
- ✓ El tráfico saliente de Zentyal, está abierto, para una libre navegación y conexión a servicios requeridos.

3.11.4.3 Configuración de Servidor Proxy

- ✓ En el menú de la parte izquierda, elegir Proxy, determinar el puerto 3128 y habilitar como Proxy Transparente, establecer el tamaño de la memoria cache en 100 MB que se considera el almacenamiento suficiente para las páginas habitualmente accedidas por los usuarios como son: registro de atenciones médicas, exámenes de laboratorio, documentos en línea, sistema de agendamiento, correo electrónico, las mismas que no demandan mayor almacenamiento por su contenido mínimo en multimedia.
- ✓ Añadir un perfil de filtrado con el nombre Todos_los_Usuarios.
- ✓ Dar clic en configuración para establecer los permisos del perfil de filtrado. Se muestra la primera pestaña, establecer el umbral en Medio y activar la casilla de Usar Antivirus, el módulo de antivirus debe estar activo.
- ✓ En la siguiente pestaña de Reglas de dominios y URLs, agregar las excepciones de los sitios a los cuales se va a denegar el acceso. Elegir la opción *Bloquear tráfico HTTPS por dominio.*
- ✓ Descargar de la siguiente dirección http://www.shallalist.de/Downloads/shallalist.tar.gz la lista para cargarla y poder discriminar por categorías de dominios y administrar de mejor manera el contenido accesible. Cargar el archivo en la opción *Listas por categorías*
- ✓ Volver a los perfiles de filtrado de todos los usuarios, ahora es visible un listado de categorías, y elegir el bloqueo básico de anuncios, sitios pornográficos, redes sociales, radio y televisión por web.
- ✓ La configuración en cuanto a los archivos MIME se conserva activada para todos los tipos, tomando en cuenta que la investigación busca determinar y disminuir las vulnerabilidades de red con todo el tráfico entrante y saliente.
- ✓ La última pestaña a configurar en el perfil es la de *Extensiones de archivo.* Es necesario evitar la descarga de ciertos tipos de archivo que pueden afectar con virus a los equipos de la red. Desactivar extensiones: adp, bat, bin.

- ✓ La definición de reglas de acceso generales hasta poder establecer las políticas en la propuesta, son de libre acceso para determinar los valores de los indicadores establecidos. Se permite sin restricción de horario al objeto Red_Local y se le asigna el perfil de filtrado Todos_los_Usuarios.

3.11.4.4 Sistema de Detección / Prevención de Intrusiones

- ✓ En el menú de la configuración IDS / IPS, elegir el interfaz que va a ser sujeto de aplicación del sistema de detección y prevención de Intrusiones. Para este caso aplicado es la interfaz eth0.
- ✓ Determinar las reglas a aplicarse, se puede registrar el suceso o denegar. Todas las actividades serán registradas y se bloquearán el acceso: ddos, dns, exploit, p2p, smtp, telnet, virus, web-attacks.

3.11.5 Implementación de Next Generation Firewall (NGFW)

Para restablecer a los firewalls como base universal de la seguridad en redes, los NGFW buscan solucionar los problemas de las conexiones desde el núcleo. Clasifican el tráfico según el tipo de aplicación y permiten el control de esta incluyendo la Web 2.0, Enterprise 2.0 y aplicaciones legacy. El firewall de siguiente generación debe tener la capacidad de: identificar aplicaciones independientemente del puerto, ver y controlar en base a políticas identificar usuarios y usar la identidad como atributo para el control de políticas, proporcionar en tiempo real protección contra las amenazas hasta la capa de aplicación, integrar el firewall con la prevención de intrusiones de red, admitir gran cantidad de datos con mínima degradación del rendimiento. (Miller, 2011)

3.11.5.1 NGFW Huawei USG6630

Dentro del entorno empresarial se encuentra instalado el Firewall de siguiente generación de marca Huawei modelo USG6300, el mismo que ofrece soluciones completas para la infraestructura de red mediana instalada. Las funciones de firewall, prevención de intrusiones, antivirus y prevención de perdida de datos permiten el manejo de un gran caudal de datos, su nombre se debe a que identifica más de 6300 aplicaciones, mediante el análisis del tráfico de servicio en 6 dimensiones; genera la aplicación de políticas de seguridad automáticamente. (Huawei Technologies Co., 2019)

Este equipo se encuentra instalado en el Data Center del Hospital General Ambato y se requiere la configuración establecido para el entorno de pruebas.

- ✓ Para obtener acceso al servidor digitar su dirección predefinida en el navegador y las credenciales de acceso.
- ✓ Al iniciar sesión se muestra el Dashboard del NGFW y muestra un resumen de la información más relevante del funcionamiento del firewall.

3.11.5.2 Configuración inicial, interfaces de red.

- ✓ Iniciar al Asistente de Configuración desde el Menú *System, Startup Wizard.*
- ✓ En la siguiente pantalla, definir el nombre de host
- ✓ Establecer la configuración de la hora
- ✓ Establecer el tipo de conexión que usará la interfaz WAN
- ✓ Establecer la ip pública, máscara de red, puerta de enlace y servidores DNS del proveedor ISP.
- ✓ Establecer la dirección de la Interfaz LAN, y la máscara.
- ✓ Establecer la configuración de Direccionamiento Dinámico DHCP
- ✓ En la pantalla final se muestra el resumen de la configuración de las interfaces de red, aplicar y guardar los cambios.
- ✓ En el menú *Object – Address – Address* Se procede con la creación del objeto de red con el nombre Red_LAN y se especifica la dirección de la red interna 192.168.210.0/24
- ✓ En el menú *Policy – Security Policy*, se añade una nueva política con el nombre *Negados_Red_LAN*; la zona de origen es *trust*, zona de destino *untrust*, la región de origen se elige la *Red_LAN* hacia *cualquier* destino, al igual que usuario, modo de acceso, dispositivo y servicio. Un módulo importante es el filtrado por aplicación, se eligen las mismas configuraciones aplicadas en el servidor UTM como son: bloqueo de redes sociales, youtube, sitios pornográficos, streaming de audio y video, sitios de recreación y los mismos deben ser elegidos en las categorías URL. Es necesario recalcar que las políticas se aplican en el orden listadas.
- ✓ Después de establecer los sitios y aplicaciones negadas, se procede con la creación de la política de acceso al resto de sitios de internet.
- ✓ Se define la regla de NAT para establecer la salida enmascarada a Internet, es decir que todas las conexiones sean a través de la IP pública.

3.11.5.3 Sistema de Detección / Prevención de Intrusiones.

- ✓ Para la configuración de este parámetro en el menú *Policies – Security Protection – Atack Defense.* Elegir en el modo de defensa *Detectar y Limpiar; a*gregar la interfaz GE1/0/7

que es la que se encuentra conectada a la WAN, establecer los parámetros de aprendizaje, y habilitar todas las reglas de aprendizaje.

- ✓ En la siguiente pestaña se muestra la configuración de ataques por paquetes únicos. Habilitar la acción descartar y habilitar las opciones existentes para protección de todos los tipos de ataques.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1 Operacionalización de Variables

Tabla 1-4: Operacionalización de Variables

Hipótesis	**Variables**	**Conceptualización**
La aplicación de un sistema de detección de vulnerabilidades UTM (Unified Threatment Management) o NGFW (Next Generation Firewall) mejorará la disponibilidad de la red institucional.	**Variable Independiente:** Sistema de detección de vulnerabilidades UTM (Unified Threatment Management) o NGFW (Next Generation Firewall)	• UTM (Unified Threat Management) Es un software de firewall que se encarga de la detección de amenazas y vulnerabilidades de la red. • NGFW (Next Generation Firewall) Es un firewall que incorpora herramientas de seguridad a medida que las necesidades han ido apareciendo
	Variable Dependiente: Disponibilidad de la red	• Tiempo en el que un sistema es capaz de realizar las transacciones para las que fue diseñado

Realizado por: Diego Silva, 2019

4.2 Matriz de Consistencia

Tabla 2-4: Matriz de Consistencia.

Hipótesis	**Variables**	**Indicadores**	**Índices**	**Técnicas**	**Instrumentos**
La aplicación de un sistema de detección de vulnerabilidades UTM (Unified Threatment Management) o NGFW (Next Generation Firewall) mejorará la disponibilidad de la red institucional	**Variable Independiente:** Sistema de detección de vulnerabilidades UTM (Unified Threatment Management) o NGFW (Next Generation Firewall)	• Productividad	• $Tasa\ de\ ocurrencia\ de\ eventos = \frac{Total\ de\ Vulnerabilidades\ detectadas}{Total\ de\ Vulnerabilidades\ estimadas}$	• Observación	Software
		• Utilización	• $Porcentaje\ de\ utilización\ del\ medio = \frac{Ancho\ de\ banda\ utilizado}{Ancho\ de\ banda\ existente}$	• Observación	Software
	Variable Dependiente: Disponibilidad de la red	• Disponibilidad	• $Porcentaje\ de\ tiempo\ activo = \frac{Horas\ Totales - Horas\ paradas\ programadas}{Horas\ Totales} x100$	• Observación	Software
		• Tiempo de Respuesta	• $Porcentaje\ de\ Tiempo\ de\ Respuesta = \frac{Tiempo\ de\ respuesta\ desde\ la\ petición\ de\ usuario}{Tiempo\ de\ respuesta\ esperado}$	• Observación	Software
		• Exactitud	• $Porcentaje\ de\ tiempo\ libre\ de\ errores = \frac{Tiempo\ total\ prueba - (Tiempo\ respuesta * Paquetes\ perdidos)}{Tiempo\ total\ prueba}$	• Observación	Software

Realizado por: Diego Silva, 2019

4.3 Elección de la Prueba Estadística

Para efectuar el análisis de los indicadores propuestos de productividad, utilización, disponibilidad, tiempo de respuesta y exactitud, es necesario la aplicación de un proceso estadístico para cada indicador. Por esto se requiere identificar el método que mejor se ajuste con los datos obtenidos.

El caso de estudio compara dos tecnologías distintas para detección de vulnerabilidades: UTM y NGFW. Los valores han sido tomados bajo las mismas condiciones para evitar sesgo en la información. Se trata de un estudio transversal por que se están analizando estas tecnologías en el mismo momento. Se comparan dos grupos independientes y son variables paramétricas numéricas (cuantitativas) por lo cual según la siguiente tabla se debe aplicar la prueba t-student

Tabla 3-4: Tabla para selección de prueba estadística.

SELECCIÓN DE UNA PRUEBA ESTADÍSTICA

		DEMOSTRAR DIFERENCIAS		MOSTRAR RELACIÓN	PREDECIR UNA VARIABLE
Tipo de Variable	Tipo de Muestra	Dos Grupos	Tres Grupos	Dos Variables	Variable desenlace
Cuantitativa (distribución normal)	No Relacionada	t de student (muestras independientes)	Anova 1 factor	Pearson	Regresión Lineal
	Relacionadas	t de student (muestras relcionadas)	Anova 1 factor		
Cualitativa ordinal (libre distribución)	No Relacionadas	*U* Mann-Whitney	Kruskal-Wallis	Spearman	
	Relacionadas	Wilcoxon	Friedman		
Cualitativa dicotómica	No Relacionadas	X^2 (o prueba exacta de Fisher)	X^2 (de tendencia lineal)	Coeficiente phi	Regresión logística
	Relacionada	McNemar	Q de Cochran	Curvas de supervivencia	

Fuente: SlidePlayer.es, 2019

4.4 Determinación del valor alfa (α)

Para los cálculos de la prueba t-student es necesario conocer el nivel alfa, que es el porcentaje de error que se está dispuesto a correr, en el cálculo de la muestra se utilizó un valor del 5% por lo que para los cálculos de debe utilizar el mismo valor.

Alfa= α=5%=0,05

4.5 Software estadístico utilizado

El software escogido es IBM SPSS, un programa estadístico informático que ofrece IMB (International Business Machines Corporation). Es el acrónimo de Producto de Estadística y Solución de Servicio (SPSS), utilizado para realizar la captura y análisis de datos para crear tablas y gráficas con data compleja. El SPSS es conocido por su capacidad de gestionar grandes volúmenes de datos y es capaz de llevar a cabo análisis de texto entre otros formatos más.

4.6 Pruebas de los escenarios implementados con t-student y Análisis de Resultados.

La prueba t-student se la realiza en el software IBM SPSS. Una vez ingresados los valores obtenidos de cada variable se calcula el P-valor de la prueba T student para muestras independientes, el valor P es el nivel de significancia más pequeño que conduce al rechazo de la hipótesis nula Ho. Para corroborar la prueba, en cada indicador se debe aplicar la prueba de normalidad y de igualdad de varianzas.

Para poder establecer una comparación entre los indicadores de las variables independiente y dependiente, es necesario también incluir los resultados obtenidos del servidor de red instalado en la casa de salud objeto de estudio; sin embargo, estos valores no son tomados en cuenta al momento de la ejecución de la prueba en el software estadístico.

4.6.1 Productividad

La medición del índice de Productividad se calcula en base a la tasa de ocurrencia de eventos determinada por las vulnerabilidades detectadas. Se toman en cuenta las detecciones validas, puesto que existen falsos positivos como: ataques icmp al enviar un ping para prueba de conexión, cambios de estado del servidor DNS; y se toman en cuenta las detecciones capturadas por intentos de acceso a través de protocolos TELNET, SSH, Proxy, intentos de acceso en busca de Bases de datos entre los principales.

La herramienta utilizada son los logs del sistema.

- **Servidor Hospital Ambato**

Este índice se mantiene en cero, el Servidor no tiene un instalado un sistema de detección ni protección contra vulnerabilidades.

- **UTM**

Acceder a través del menú *Registros ->Consulta de Registros -> IPS.*

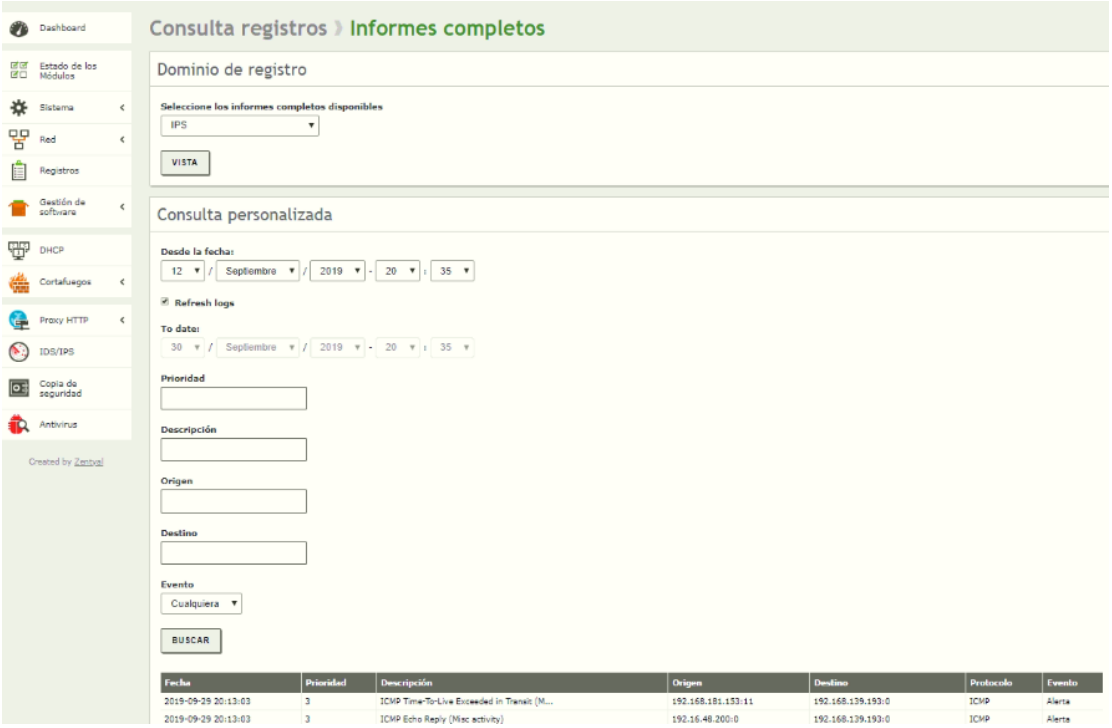


Figura 1-4: Informe de logs IPS - NGFW

Realizado por: Diego Silva, 2019

- **NGFW**

En el menú *Monitor -> System Log* despliega la información de los intentos fallidos de acceso

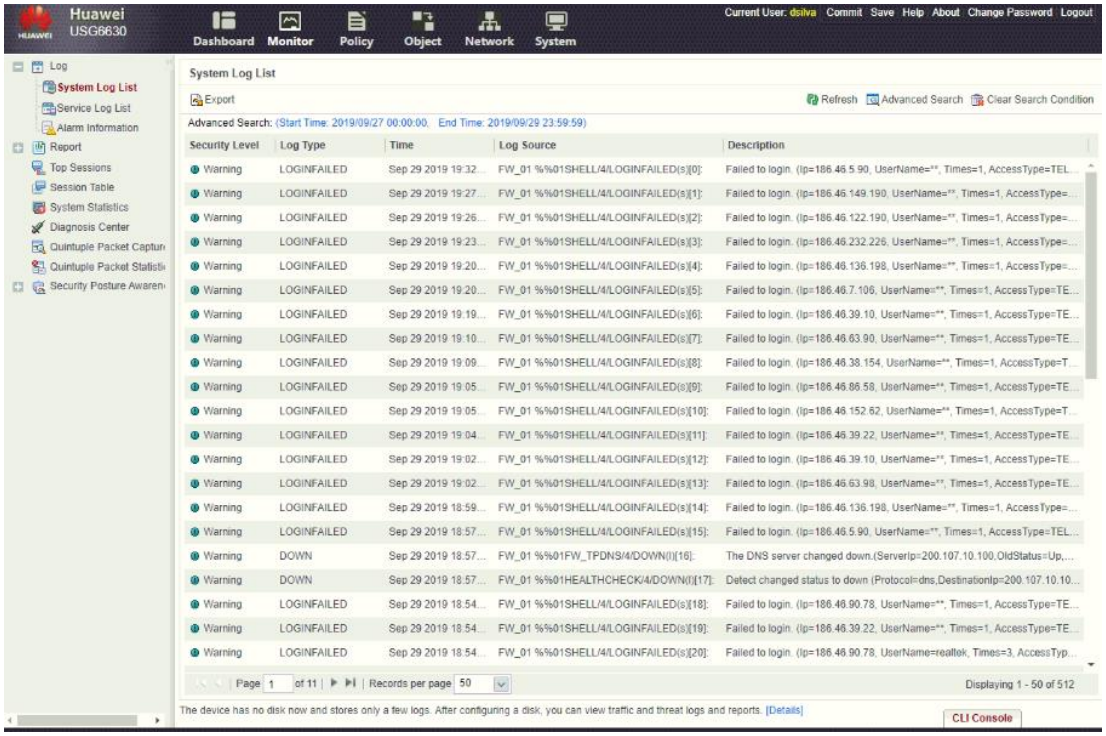


Figura 2-4: Informe de Logs IPS - NGFW

Realizado por: Diego Silva, 2019

Después de haber realizado el análisis de los logs de detección de vulnerabilidades se toman según lo indica la muestra 384 detecciones de los archivos de log, se identifica que se muestran muchas alertas, las cuales se consideran falsos positivos, como por ejemplo las peticiones recurrentes de DNS, o avisos de cambio de estado en un servidor.

Se obtienen las siguientes muestras:

Tabla 4-4: Detecciones Válidas

Día de la toma	DETECCIONES VALIDAS	
	UTM	NGFW
Día 1	222	301
Día 2	227	277
Día 3	256	276
Día 4	242	289
Día 5	249	259
Día 6	250	311
Día 7	256	313
Día 8	223	298
Día 9	233	277

Día 10	251	314
Día 11	276	251
Día 12	223	254
Día 13	272	354
Día 14	267	352
Día 15	226	299
Día 16	277	318
Día 17	276	341
Día 18	260	292
Día 19	228	239
Día 20	258	276

Realizado por: Diego Silva, 2019

4.6.1.1 Prueba de Normalidad

Para poder aplicar la prueba t-student es necesario que los valores se comporten normalmente, es decir que los valores obtenidos cumplan con la distribución normal. Para ello se utiliza el siguiente criterio:

- P-valor ≥α Rechazar H_o: Los datos provienen de una distribución normal.
- P-valor <α No rechazar H_o: Los datos no provienen de una distribución normal.

La comprobación de normalidad se realiza en el software estadístico SPSS. Después de ingresados los datos de las variables en la "vista de datos" se obtienen los resultados.

Tabla 5-4: Prueba de Normalidad del indicador Productividad

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Tecnologías	Estadístico	Gl	Sig.	Estadístico	gl	Sig.
Detecciones Válidas	UTM	,154	20	,200*	,909	30	,060
	NGFW	,106	20	,200*	,967	30	,686

Realizado por: Diego Silva, 2019

Se observa el nivel de significancia en la prueba de Shapiro Wilk debido a que es para muestras pequeñas (menor o igual a 30) que es el caso de este estudio. En la tabla se observan los valores del nivel de significancia para poder compararlos con el nivel alfa como se observa a continuación:

P-valor (UTM)=0,060 > α = 0,05

P-valor (NGFW)=0,686> α = 0,05

Dado que P-valor es mayor que alfa se rechaza Ho: Los datos provienen de una distribución normal. Es decir, la variable "productividad" en las dos tecnologías se comporta normalmente y se cumple una de las condiciones para realizar la prueba t-student.

4.6.1.2 Igualdad de varianzas

Otra condición para aplicar la prueba t-student es corroborar la igualdad de varianza entre los grupos. Si se cumple el criterio de que las varianzas son iguales además de haber cumplido con la prueba de normalidad, se puede proceder a realizar la prueba t-student para el análisis de hipótesis. Se utiliza el siguiente criterio:

- P-valor ≥α; Rechazar H_o: Las varianzas son iguales
- P-valor <α No rechazar H_o: Existe diferencia significativa en las varianzas

Además de los valores ya ingresados, se requiere ingresar el valor del intervalo de confianza, debido a que el porcentaje de error (α) es del 5%, el intervalo de confianza será de 95%, que sumados son 100%

Tabla 6-4: Prueba de igualdad de varianzas del indicador Productividad

		Prueba de Levene de igualdad de varianzas	
		F	Sig.
Detecciones Válidas	Se asumen varianzas iguales	3,641	,064
	No se asumen varianzas iguales		

Realizado por: Diego Silva, 2019

La igualdad de varianza se corrobora mediante la "Prueba de Levene para la igualdad de varianzas", se observa el nivel de significancia, que en este caso es de 0,064

P-valor=0,064 > α=0.05

- P-valor ≥α; Rechazar Ho: Las varianzas son iguales
- P-valor <α No rechazar Ho: Existe diferencia significativa en las varianzas

Debido a que el nivel de significancia es mayor que alfa se rechaza Ho, es decir: Las varianzas son iguales.

4.6.1.3 Resultados de la prueba t-student

Se utiliza el siguiente criterio para la decisión estadística:

Si P-valor ≤ α se rechaza Ho

Si P-valor > α no se rechaza Ho

H1: **Existe** una diferencia significativa entre la media de los valores de productividad con la tecnología UTM y la media de los valores de productividad con la tecnología NGFW.

$$H1: \mu a \neq \mu b$$

Ho: **No existe** una diferencia significativa entre la media de los valores de productividad con la tecnología UTM y la media de los valores de productividad con la tecnología NGFW.

$$Ho: \mu a = \mu b$$

En el software IBM SPSS se analizan los resultados, se toma el valor de la significancia bilateral de la prueba t-student. Como se han asumido varianzas iguales se toma el valor correspondiente a tal característica a pesar de que en este caso son valores iguales, pero es necesario aclararlo. El valor es de 0,00 como se aprecia en la Tabla 8-4.

Tabla 7-4: Resultados estadísticos del indicador Productividad

Estadísticas de grupo

	Tecnologías	N	Media	Desviación estándar	Media de error estándar
Detecciones Válidas	UTM	20	248,60	19,516	4,364
	NGFW	20	294,55	32,312	7,225

Realizado por: Diego Silva, 2019

Tabla 8-4: Resultados de la prueba t-student del indicador Productividad

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	T	Gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Detecciones Válidas	Se asumen varianzas iguales	3,641	,064	-5,444	38	,000	-45,950	8,441	-63,037	-28,863
	No se asumen varianzas iguales			-5,444	31,235	,000	-45,950	8,441	-63,160	-28,740

Realizado por: Diego Silva, 2019

P-valor=0,00 ≤ α=0.05

Debido a que P-valor es menor que alfa se rechaza H_o, es decir, **H_1:** Existe una diferencia significativa entre la media de los valores de productividad con la tecnología UTM y la media de los valores de productividad con la tecnología NGFW.

Descriptivamente la diferencia entre las medias de ambas tecnologías. La media para la tecnología UTM es de 249 detecciones válidas y 295 detecciones válidas para la tecnología NGFW.

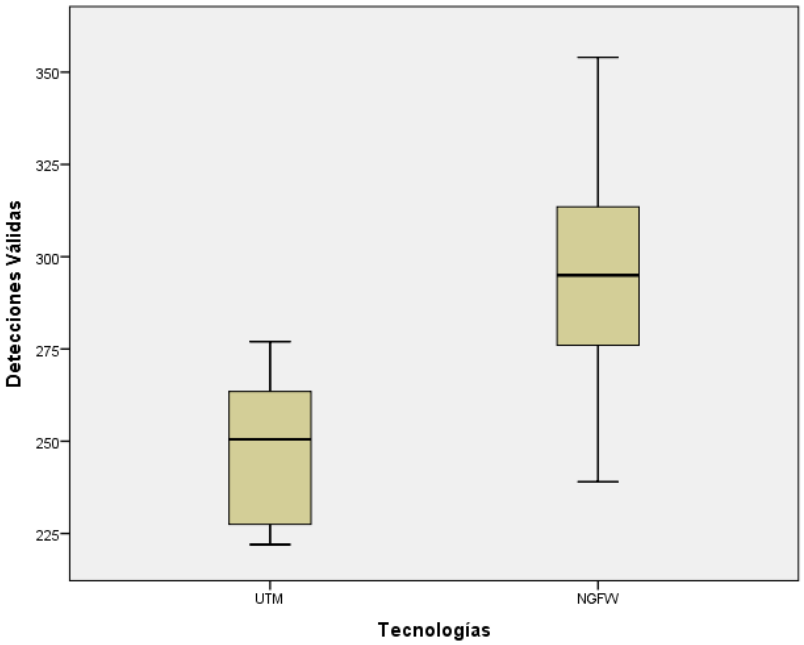


Figura 3-4: Medias de los valores de productividad de las tecnologías UTM y NGFW

Realizado por: Diego Silva, 2019

4.6.1.4 Decisión Estadística

Después de realizada la prueba t-student para la variable "productividad" se concluye que existe una diferencia significativa entre la media de los valores de detecciones válidas con la tecnología UTM y NGFW. Esto quiere decir que a más de observar que la media de los valores con tecnología UTM es menor, la prueba t-student indica que es significativamente menor, lo que indica que se puede asegurar que en cuanto a la variable productividad, la tecnología NGFW tiene una gran ventaja frente a UTM, ya que los valores de detecciones válidas son superiores lo cual significa un incremento en la productividad del servidor.

4.6.2 Utilización

El índice de Utilización está determinado por el ancho de banda utilizado sobre el ancho de banda contratado. Se obtiene información que permite identificar el porcentaje de utilización del medio.

Se realizan dos comprobaciones diarias con carga de usuarios y sin carga de usuarios a la misma hora del día.

- **Servidor Hospital Ambato**

Figura 4-4: Ancho de banda sin carga de usuarios – Servidor Hospital Ambato

Realizado por: Diego Silva, 2019

Figura 5-4: Ancho de banda con carga de usuarios – Servidor Hospital Ambato

Realizado por: Diego Silva, 2019

- **UTM**

Figura 6-4: Ancho de banda sin carga de usuarios - Zentyal

Realizado por: Diego Silva, 2019

Figura 7-4: Ancho de banda con carga de usuarios - Zentyal

Realizado por: Diego Silva, 2019

- **NGFW**

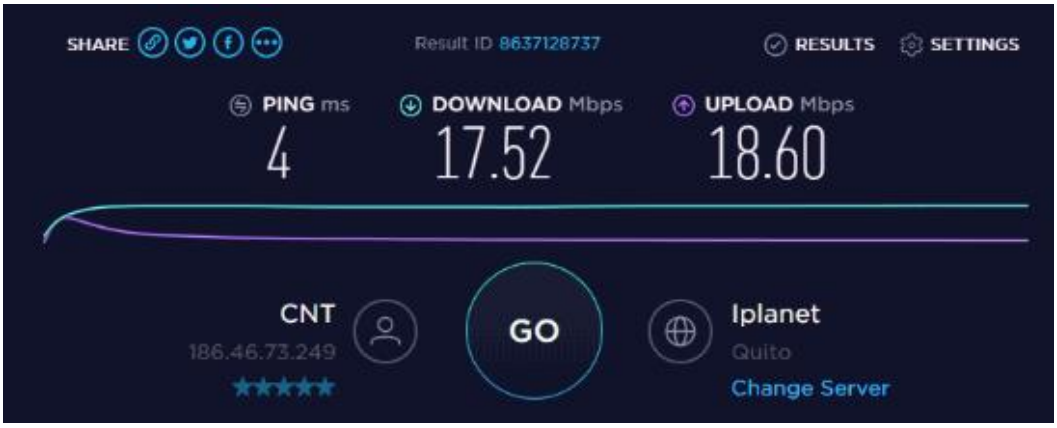


Figura 8-4: Ancho de banda sin carga de usuarios - NGFW

Realizado por: Diego Silva, 2019

Figura 9-4: Ancho de banda con carga de usuarios - NGFW

Realizado por: Diego Silva, 2019

Tabla 9-4: Medición de Ancho de banda

Días	MEDICIÓN DE ANCHO DE BANDA DE DESCARGA					
	Servidor Hospital Ambato		**UTM**		**NGFW**	
	Sin carga de usuario	**Con carga de usuarios**	**Sin carga de usuario**	**Con carga de usuarios**	**Sin carga de usuario**	**Con carga de usuarios**
Día 1	10,59	9,93	13,88	10,65	17,52	13,38
Día 2	10,87	10,01	14,25	11,38	16,63	11,94
Día 3	11,03	9,85	12,11	9,84	18,01	12,72
Día 4	10,96	10,13	13,54	9,27	15,63	13,49
Día 5	11,78	9,88	11,03	10,73	17,82	14,33
Día 6	13,51	11,72	13,79	11,40	17,36	14,83
Día 7	10,08	10,24	14,38	11,30	16,26	13,87
Día 8	11,24	9,24	12,70	10,68	18,78	13,91
Día 9	10,25	10,55	12,30	11,39	17,74	13,89
Día 10	12,51	10,90	13,58	10,27	15,03	14,30
Día 11	10,30	11,48	13,66	11,74	16,68	14,32
Día 12	10,96	11,95	13,26	11,21	17,94	13,93
Día 13	13,97	11,09	13,57	10,74	18,69	12,76
Día 14	11,37	10,32	14,79	12,23	15,20	14,07
Día 15	11,56	11,56	12,06	11,76	15,04	11,28
Día 16	12,44	12,88	12,36	11,24	18,61	13,71
Día 17	11,81	10,17	12,14	11,04	15,14	13,42
Día 18	13,61	10,97	12,75	11,36	17,44	11,31
Día 19	10,59	10,77	14,77	11,14	15,10	14,36
Día 20	12,36	9,95	14,94	11,67	15,50	13,91

Realizado por: Diego Silva, 2019

4.6.2.1 Prueba de Normalidad

Para poder aplicar la prueba t-student es necesario que los valores se comporten normalmente, es decir que los valores obtenidos cumplan con la distribución normal. Para ello se utiliza el siguiente criterio:

- P-valor $\geq \alpha$ Rechazar H_o: Los datos provienen de una distribución normal.
- P-valor $< \alpha$ No rechazar H_o: Los datos no provienen de una distribución normal.

La comprobación de normalidad se realiza en el software estadístico SPSS. Después de ingresados los datos de las variables en la "vista de datos" se obtienen los resultados.

Tabla 10-4: Prueba de Normalidad del indicador Utilización

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Tecnologías	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Ancho de Banda sin carga	UTM	,141	20	,200*	,958	20	,511
	NGFW	,133	20	,200*	,937	20	,210
Ancho de Banda con carga	UTM	,151	20	,200*	,935	20	,192
	NGFW	,149	20	,200*	,937	20	,212

Realizado por: Diego Silva, 2019

Se observa el nivel de significancia en la prueba de Shapiro Wilk debido a que es para muestras pequeñas (menor o igual a 30) que es el caso de este estudio. En la tabla se observan los valores del nivel de significancia para poder compararlos con el nivel alfa como se observa a continuación:

Sin carga de Usuarios

P-valor (UTM)=0,511 > $\alpha = 0,05$

P-valor (NGFW)=0,210> $\alpha = 0,05$

Sin carga de Usuarios

P-valor (UTM)=0,192 > $\alpha = 0,05$

P-valor (NGFW)=0,212> $\alpha = 0,05$

Dado que P-valor es mayor que alfa se rechaza Ho: Los datos provienen de una distribución normal. Es decir, la variable "utilización" en las dos tecnologías se comporta normalmente y se cumple una de las condiciones para realizar la prueba t-student.

4.6.2.2 Igualdad de varianzas

Otra condición para aplicar la prueba t-student es corroborar la igualdad de varianza entre los grupos. Si se cumple el criterio de que las varianzas son iguales además de haber cumplido con la prueba de normalidad, se puede proceder a realizar la prueba t-student para el análisis de hipótesis. Se utiliza el siguiente criterio:

- P-valor $\geq\alpha$; Rechazar H_o: Las varianzas son iguales
- P-valor $<\alpha$ No rechazar H_O: Existe diferencia significativa en las varianzas

Además de los valores ya ingresados, se requiere ingresar el valor del intervalo de confianza, debido a que el porcentaje de error (α) es del 5%, el intervalo de confianza será de 95%, que sumados son 100%

Tabla 11-4: Prueba de igualdad de varianzas del indicador Utilización

		Prueba de Levene de igualdad de varianzas	
		F	Sig.
Ancho de Banda sin carga	Se asumen varianzas iguales	,086	,771
	No se asumen varianzas iguales		
Ancho de Banda con carga	Se asumen varianzas iguales	1,142	,292
	No se asumen varianzas iguales		

Realizado por: Diego Silva, 2019

La igualdad de varianza se corrobora mediante la "Prueba de Levene para la igualdad de varianzas", se observa el nivel de significancia, que en este caso es

Sin carga de Usuarios

P-valor=0,771 > α=0.05

Con carga de Usuarios

P-valor=0,292 > α=0.05

- P-valor ≥α; Rechazar Ho: Las varianzas son iguales
- P-valor <α No rechazar Ho: Existe diferencia significativa en las varianzas

Debido a que el nivel de significancia es mayor que alfa se rechaza Ho, es decir: Las varianzas son iguales.

4.6.2.3 Resultados de la prueba t-student

Se utiliza el siguiente criterio para la decisión estadística:

Si P-valor ≤ α se rechaza Ho

Si P-valor > α no se rechaza Ho

H1: **Existe** una diferencia significativa entre la media de los valores de utilización con la tecnología UTM y la media de los valores de utilización con la tecnología NGFW.

$H1$: $\mu a \neq \mu b$

Ho: **No existe** una diferencia significativa entre la media de los valores de utilización con la tecnología UTM y la media de los valores de utilización con la tecnología NGFW.

Ho: $\mu a = \mu b$

En el software IBM SPSS se analizan los resultados, se toma el valor de la significancia bilateral de la prueba t-student. Como se han asumido varianzas iguales se toma el valor correspondiente a tal característica a pesar de que en este caso son valores iguales, pero es necesario aclararlo. El valor es de 0,00 como se aprecia en la Tabla 13-4.

Tabla 12-4: Resultados estadísticos del indicador Utilización

Estadísticas de grupo

	Tecnologías	N	Media	Desviación estándar	Media de error estándar
Ancho de Banda sin carga	UTM	20	13,2930	1,07736	,24091
	NGFW	20	17,2355	1,08564	,24276
Ancho de Banda con carga	UTM	20	11,0520	,69087	,15448
	NGFW	20	13,1330	,79361	,17746

Realizado por: Diego Silva, 2019

Tabla 13-4: Resultados de la prueba t-student del indicador Utilización

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	T	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Ancho de Banda sin carga	Se asumen varianzas iguales	,086	,771	-11,528	38	,000	-3,94250	,34200	-4,63485	-3,25015
	No se asumen varianzas iguales			-11,528	37,998	,000	-3,94250	,34200	-4,63485	-3,25015
Ancho de Banda con carga	Se asumen varianzas iguales	1,142	,292	-8,845	38	,000	-2,08100	,23528	-2,55729	-1,60471
	No se asumen varianzas iguales			-8,845	37,292	,000	-2,08100	,23528	-2,55759	-1,60441

Realizado por: Diego Silva, 2019

P-valor=0,00 ≤ α=0.05

Debido a que P-valor es menor que alfa se rechaza H_o, es decir, **H_1:** Existe una diferencia significativa entre la media de los valores de utilización con la tecnología UTM y la media de los valores de utilización con la tecnología NGFW.

Descriptivamente la diferencia entre las medias de ambas tecnologías sin carga de usuarios. La media para la tecnología UTM es de 13,29 Mbps y 17,23 Mbps para la tecnología NGFW.

La diferencia entre las medias de ambas tecnologías con carga de usuarios. La media para la tecnología UTM es de 11,05 Mbps y 13,13 Mbps para la tecnología NGFW.

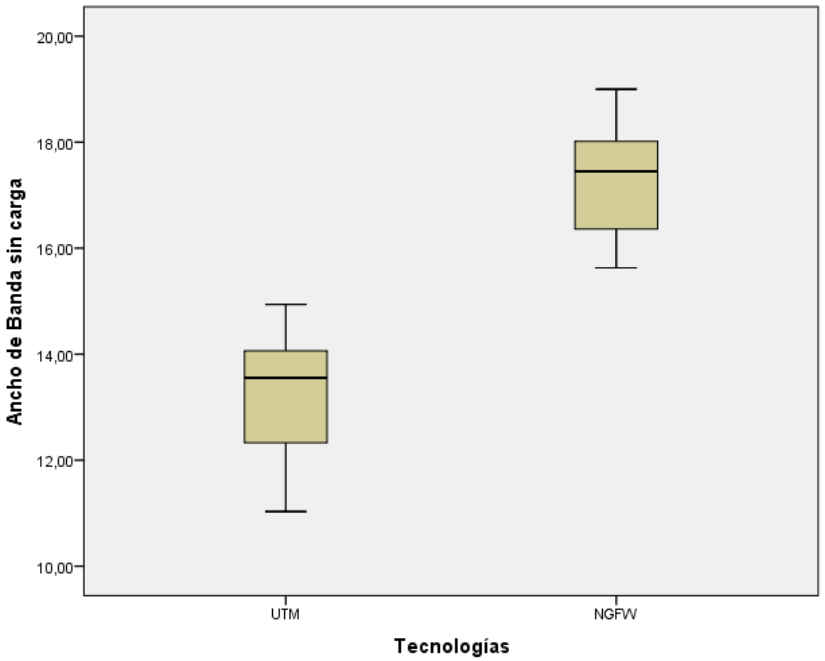


Figura 10-4: Medias de productividad UTM y NGFW sin carga de Usuarios.

Realizado por: Diego Silva, 2019

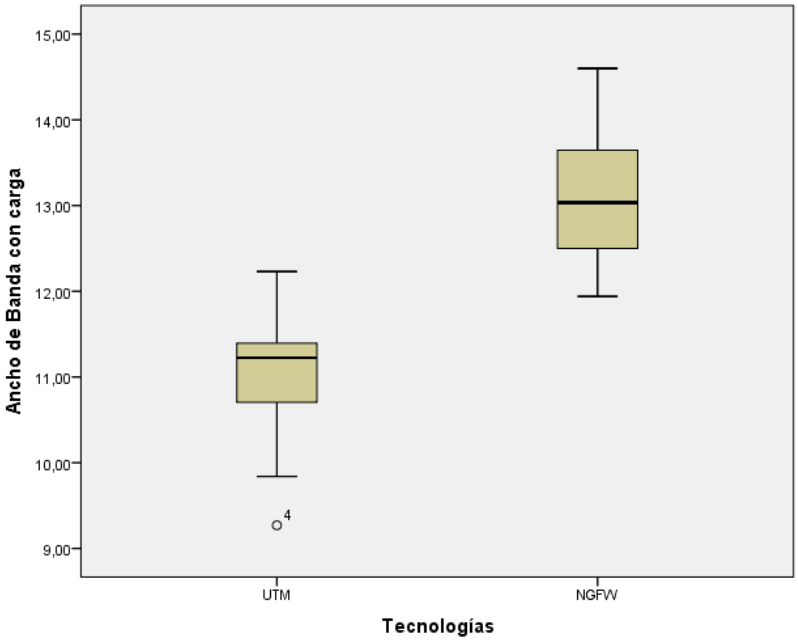


Figura 11-4: Medias de productividad de UTM y NGFW con carga de Usuarios.

Realizado por: Diego Silva, 2019

4.6.2.4 Decisión Estadística

Después de realizada la prueba t-student para la variable "utilización" se concluye que existe una diferencia significativa entre la media de los valores de detecciones válidas con la tecnología UTM y NGFW. Esto quiere decir que a más de observar que la media de los valores con tecnología UTM es menor, la prueba t-student indica que es significativamente menor, lo que indica que se puede asegurar que en cuanto a la variable productividad, la tecnología NGFW tiene una gran ventaja frente a UTM, ya que los valores de Ancho de banda con y sin carga de usuarios son superiores lo cual significa un incremento en la utilización del servidor.

4.6.3 Disponibilidad

Con este indicador se pretende determinar el porcentaje de disponibilidad de cada uno de los sistemas. Durante las pruebas realizadas en un tiempo total de 120 horas, ninguno de los servidores ha presentado caídas o fallas en su funcionamiento manteniéndose en un 100% de disponibilidad

4.6.4 Tiempo de respuesta

Se ha utilizado la herramienta ping para esta prueba, se ha podido obtener el tiempo de respuesta promedio de la población de 384 peticiones generadas a través del comando *ping*

www.google.com – n 384. El tiempo de respuesta promedio en un equipo conectado directo a internet es de 59,87 ms

- **Servidor Hospital Ambato**

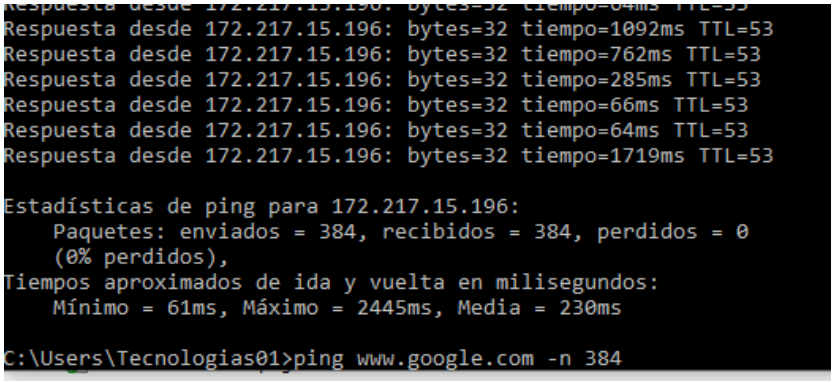


Figura 12-4: Pruebas de ping – Servidor Hospital Ambato

Realizado por: Diego Silva, 2019

- **UTM**

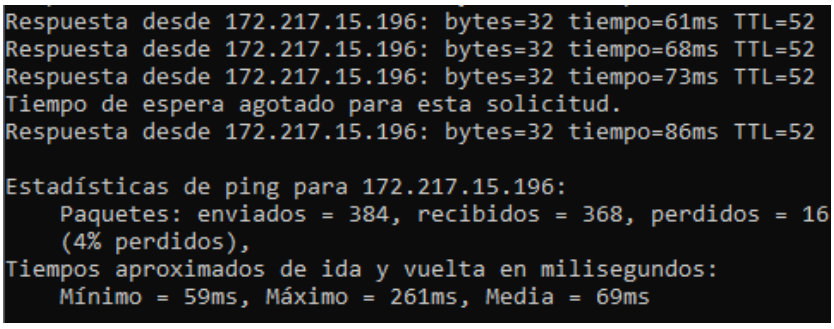


Figura 13-4: Pruebas de ping - Zentyal

Realizado por: Diego Silva, 2019

- **NGFW**

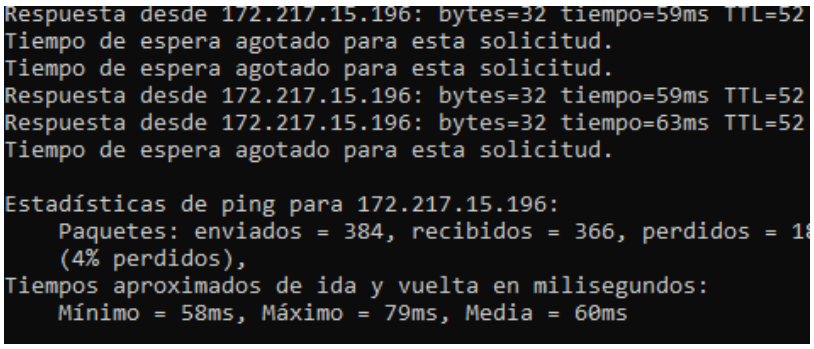


Figura 14-4: Pruebas de ping - NGFW

Realizado por: Diego Silva, 2019

En la siguiente tabla se muestra los resultados de las pruebas realizadas.

Tabla 14-4: Tiempo de respuesta

Días	TIEMPO DE RESPUESTA		
	Servidor Hospital Ambato	**Zentyal**	**Huawei USG 6630**
Día 1	230 ms	69 ms	63 ms
Día 2	186 ms	67 ms	61 ms
Día 3	197 ms	70 ms	62 ms
Día 4	213 ms	69 ms	59 ms
Día 5	191 ms	68 ms	60 ms
Día 6	211 ms	65 ms	61 ms
Día 7	221 ms	72 ms	63 ms
Día 8	221 ms	70 ms	63 ms
Día 9	201 ms	69 ms	60 ms
Día 10	200 ms	65 ms	65 ms
Día 11	214 ms	73 ms	63 ms
Día 12	224 ms	65 ms	61 ms
Día 13	177 ms	65 ms	62 ms
Día 14	223 ms	72 ms	60 ms
Día 15	190 ms	69 ms	59 ms
Día 16	201 ms	73 ms	65 ms
Día 17	210 ms	67 ms	59 ms
Día 18	170 ms	73 ms	65 ms
Día 19	211 ms	70 ms	63 ms
Día 20	198 ms	67 ms	58 ms

Realizado por: Diego Silva, 2019

4.6.4.1 Prueba de Normalidad

Para poder aplicar la prueba t-student es necesario que los valores se comporten normalmente, es decir que los valores obtenidos cumplan con la distribución normal. Para ello se utiliza el siguiente criterio:

- P-valor $\geq \alpha$ Rechazar H_o: Los datos provienen de una distribución normal.
- P-valor $< \alpha$ No rechazar H_o: Los datos no provienen de una distribución normal.

La comprobación de normalidad se realiza en el software estadístico SPSS. Después de ingresados los datos de las variables en la “vista de datos” se obtienen los resultados.

Tabla 15-4: Prueba de Normalidad del indicador Tiempo de Respuesta

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Tecnologías	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Tiempo de Respuesta	UTM	,120	20	,200*	,916	20	,082
	NGFW	,144	20	,200*	,938	20	,216

Realizado por: Diego Silva, 2019

Se observa el nivel de significancia en la prueba de Shapiro Wilk debido a que es para muestras pequeñas (menor o igual a 30) que es el caso de este estudio. En la tabla se observan los valores del nivel de significancia para poder compararlos con el nivel alfa como se observa a continuación:

P-valor (UTM)=0,082 > $\alpha = 0,05$

P-valor (NGFW)=0,216> $\alpha = 0,05$

Dado que P-valor es mayor que alfa se rechaza Ho: Los datos provienen de una distribución normal. Es decir, la variable "tiempo de respuesta" en las dos tecnologías se comporta normalmente y se cumple una de las condiciones para realizar la prueba t-student.

4.6.4.2 Igualdad de varianzas

Otra condición para aplicar la prueba t-student es corroborar la igualdad de varianza entre los grupos. Si se cumple el criterio de que las varianzas son iguales además de haber cumplido con la prueba de normalidad, se puede proceder a realizar la prueba t-student para el análisis de hipótesis. Se utiliza el siguiente criterio:

- P-valor $\geq\alpha$; Rechazar H_o: Las varianzas son iguales
- P-valor $<\alpha$ No rechazar H_O: Existe diferencia significativa en las varianzas

Además de los valores ya ingresados, se requiere ingresar el valor del intervalo de confianza, debido a que el porcentaje de error (α) es del 5%, el intervalo de confianza será de 95%, que sumados son 100%.

Tabla 16-4: Prueba de igualdad de varianzas del indicador Productividad

		Prueba de Levene de igualdad de varianzas	
		F	Sig.
Tiempo de Respuesta	Se asumen varianzas iguales	,968	,331
	No se asumen varianzas iguales		

Realizado por: Diego Silva, 2019

La igualdad de varianza se corrobora mediante la "Prueba de Levene para la igualdad de varianzas", se observa el nivel de significancia, que en este caso es de 0,331
P-valor=0,331 > α=0.05

- P-valor ≥α; Rechazar Ho: Las varianzas son iguales
- P-valor <α No rechazar Ho: Existe diferencia significativa en las varianzas

Debido a que el nivel de significancia es mayor que alfa se rechaza Ho, es decir: Las varianzas son iguales.

4.6.4.3 Resultados de la prueba t-student

Se utiliza el siguiente criterio para la decisión estadística:

Si P-valor ≤ α se rechaza Ho

Si P-valor > α no se rechaza Ho

H1: **Existe** una diferencia significativa entre la media de los valores de tiempo de respuesta con la tecnología UTM y la media de los valores de tiempo de respuesta con la tecnología NGFW.

$H1$: $\mu a \neq \mu b$

Ho: **No existe** una diferencia significativa entre la media de los valores de tiempo de respuesta con la tecnología UTM y la media de los valores de tiempo de respuesta con la tecnología NGFW.

Ho: $\mu a = \mu b$

En el software IBM SPSS se analizan los resultados, se toma el valor de la significancia bilateral de la prueba t-student. Como se han asumido varianzas iguales se toma el valor correspondiente a tal característica a pesar de que en este caso son valores iguales, pero es necesario aclararlo. El valor es de 0,00 como se aprecia en la Tabla 18-4.

Tabla 17-4: Resultados estadísticos del indicador Productividad

Estadísticas de grupo

	Tecnologías	N	Media	Desviación estándar	Media de error estándar
Tiempo de Respuesta	UTM	20	68,9000	2,77014	,61942
	NGFW	20	61,6000	2,13739	,47793

Realizado por: Diego Silva, 2019

Tabla 18-4: Resultados de la prueba t-student del indicador Tiempo de Respuesta

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Tiempo de Respuesta	Se asumen varianzas iguales	,968	,331	9,331	38	,000	7,30000	,78237	5,71617	8,88383
	No se asumen varianzas iguales			9,331	35,703	,000	7,30000	,78237	5,71282	8,88718

Realizado por: Diego Silva, 2019

$$\text{P-valor}=0{,}00 \leq \alpha=0.05$$

Debido a que P-valor es menor que alfa se rechaza H_o, es decir, **H_1:** Existe una diferencia significativa entre la media de los valores de Tiempo de Respuesta con la tecnología UTM y la media de los valores de Tiempo de Respuesta con la tecnología NGFW.

Descriptivamente la diferencia entre las medias de ambas tecnologías. La media para la tecnología UTM es de 68,9 ms y 61,6 ms para la tecnología NGFW.

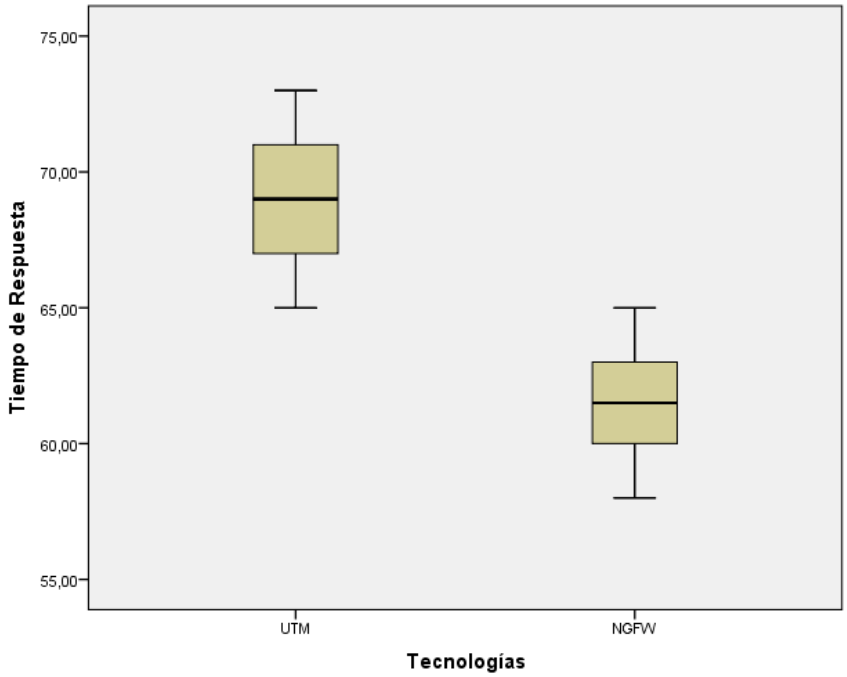


Figura 15-4: *Medias de Tiempo de Respuesta de UTM y NGFW*

Realizado por: Diego Silva, 2019

4.6.4.4 Decisión Estadística

Después de realizada la prueba t-student para la variable "tiempo de respuesta" se concluye que existe una diferencia significativa entre la media de los valores de tiempo de respuesta en milisegundos con la tecnología UTM y NGFW. Esto quiere decir que a más de observar que la media de los valores con tecnología UTM es mayor, la prueba t-student indica que es significativamente mayor, lo que indica que se puede asegurar que en cuanto a la variable tiempo de respuesta, la tecnología NGFW tiene una gran ventaja frente a UTM, ya que los valores de tiempo de respuesta son inferiores lo cual significa un incremento en la disponibilidad del servidor.

4.6.5 Exactitud

A través de las pruebas de ping con una carga de 64 bytes en un sistema Linux con el comando *ping www.google.com -c 384 -D.* Se toman muestras del tiempo promedio de respuesta, los paquetes perdidos en esta prueba y el tiempo total de la prueba; y se obtiene el tiempo con errores en la transmisión y el porcentaje de tiempo libre de errores.

Se aplica la siguiente fórmula para obtener el porcentaje libre de errores:

Porcentaje de Tiempo libre de errores

$$= \frac{Tiempo\ total\ de\ la\ prueba - (Tiempo\ de\ respuesta * Paquetes\ perdidos)}{Tiempo\ total\ de\ la\ prueba}$$

- **Servidor del Hospital Ambato**

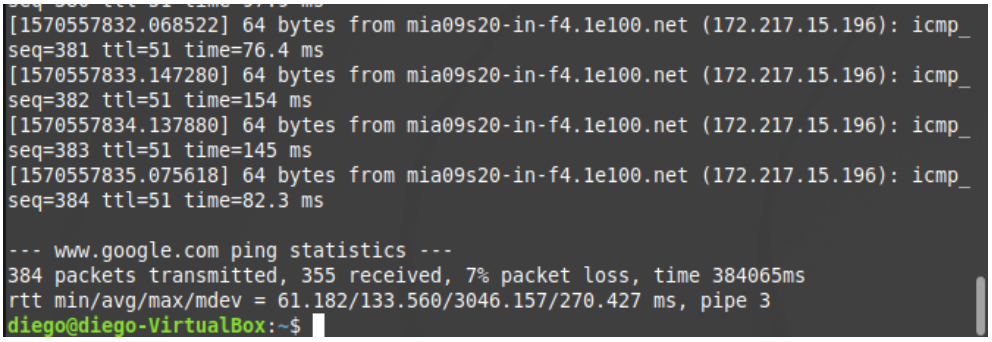


Figura 16-4: Pruebas de ping para pérdidas – Servidor del Hospital Ambato

Realizado por: Diego Silva, 2019

Tabla 19-4: Porcentaje de pérdidas – Servidor Hospital Ambato.

Día	Tiempo de respuesta (ms)	Paquetes perdidos	Tiempo con errores de transmisión (ms)	Tiempo total de la prueba (ms)	Porcentaje de Tiempo libre de errores
Día 1	133,56	29	3873,24	384065	0,989915
Día 2	137,54	21	2888,34	384654	0,992491
Día 3	132,45	24	3178,8	384174	0,991726
Día 4	131,27	31	4069,37	385523	0,989445
Día 5	128,99	15	1934,85	384255	0,994965
Día 6	139,447271	16	2231,15633	384972	0,99420437
Día 7	134,021448	34	4556,72924	384613	0,98815243
Día 8	127,05282	22	2795,16204	384954	0,99273897
Día 9	129,343461	25	3233,58653	384895	0,99159878
Día 10	126,755013	25	3168,87533	385163	0,99177264
Día 11	131,808181	22	2899,77999	384723	0,99246268
Día 12	139,150354	37	5148,56308	384783	0,98661957
Día 13	138,45027	27	3738,15729	384914	0,99028833
Día 14	131,402841	35	4599,09945	385497	0,98806969
Día 15	133,391087	15	2000,86631	384309	0,9947936
Día 16	138,649388	40	5545,97553	384406	0,98557261
Día 17	127,834017	16	2045,34427	385070	0,99468838
Día 18	130,400832	15	1956,01248	385133	0,9949212
Día 19	137,121677	18	2468,19019	384416	0,99357938
Día 20	131,480091	31	4075,88281	384837	0,98940881

Realizado por: Diego Silva, 2019

- **UTM**

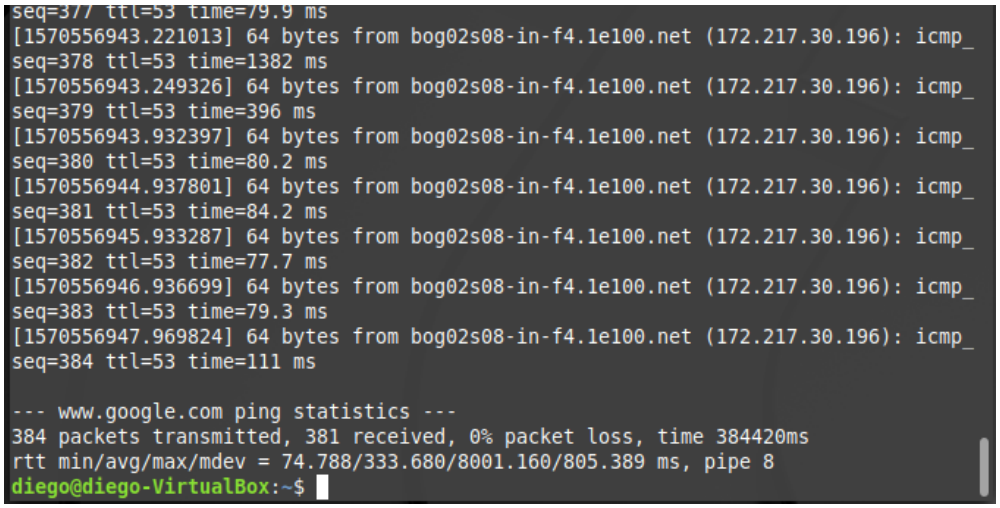


Figura 17-4: Pruebas de ping para pérdidas - Zentyal

Realizado por: Diego Silva, 2019

Tabla 20-4: Porcentaje de pérdidas – UTM.

Día	Tiempo de respuesta (ms)	Paquetes perdidos	Tiempo con errores de transmisión (ms)	Tiempo total de la prueba (ms)	Porcentaje de Tiempo libre de errores (ms)
Día 1	139,571816	4	558,287265	384420	0,99854772
Día 2	137,805662	5	689,028312	384152	0,99820637
Día 3	127,570877	11	1403,27964	384156	0,99634711
Día 4	130,194737	10	1301,94737	383985	0,99660938
Día 5	139,785395	11	1537,63935	385041	0,99600656
Día 6	128,200848	11	1410,20933	385016	0,99633727
Día 7	132,500678	12	1590,00814	385055	0,9958707
Día 8	137,08133	3	411,24399	384538	0,99893055
Día 9	139,082704	7	973,578927	384477	0,99746778
Día 10	130,953211	11	1440,48532	384387	0,99625251
Día 11	127,457452	1	127,457452	384922	0,99966887
Día 12	131,551068	7	920,857476	384708	0,99760635
Día 13	137,074993	9	1233,67493	384852	0,99679442
Día 14	134,659704	3	403,979111	384041	0,99894808
Día 15	131,893888	7	923,257219	384786	0,9976006
Día 16	128,991437	1	128,991437	384542	0,99966456
Día 17	139,723079	2	279,446157	384409	0,99927305
Día 18	134,271915	7	939,903406	384768	0,99755722
Día 19	130,565263	3	391,69579	384757	0,99898197
Día 20	129,13708	2	258,274159	384241	0,99932783

Realizado por: Diego Silva, 2019

- **NGFW**

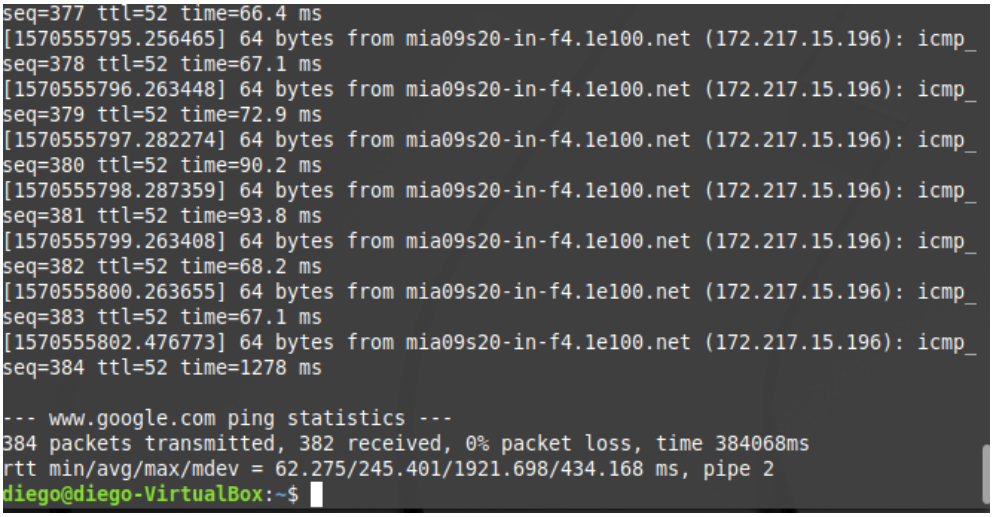


Figura 18-4: Pruebas de ping para pérdidas - NGFW

Realizado por: Diego Silva, 2019

Tabla 21-4: Porcentaje de pérdidas – NGFW.

Día	Tiempo de respuesta (ms)	Paquetes perdidos	Tiempo con errores de transmisión (ms)	Tiempo total de la prueba (ms)	Porcentaje de Tiempo libre de errores (ms)
Día 1	134,766686	2	290,8	384548	0,999243
Día 2	143,957357	7	135,47	384199	0,999647
Día 3	141,400362	1	275,14	384886	0,999284
Día 4	137,074752	9	423,69	384607	0,998896
Día 5	139,218911	2	143,25	384086	0,999627
Día 6	143,759213	8	1150,0737	384661	0,99701016
Día 7	143,786781	6	862,720687	384492	0,99775621
Día 8	131,608462	9	1184,47616	384231	0,99691728
Día 9	130,671379	4	522,685517	384199	0,99863954
Día 10	134,221104	5	671,10552	385053	0,99825711
Día 11	142,311988	5	711,55994	384269	0,99814828
Día 12	134,024415	10	1340,24415	384442	0,99651379
Día 13	143,55551	4	574,222041	384504	0,99850659
Día 14	143,592905	9	1292,33615	384750	0,9966411
Día 15	144,96129	9	1304,65161	384830	0,9966098
Día 16	130,737127	10	1307,37127	384761	0,99660212
Día 17	139,821337	4	559,28535	384335	0,9985448
Día 18	138,78393	4	555,13572	384572	0,99855648
Día 19	142,36646	7	996,565219	385059	0,99741192
Día 20	144,695229	2	289,390458	384001	0,99924638

Realizado por: Diego Silva, 2019

A continuación, se muestra un resumen de los resultados obtenidos en las pruebas de exactitud realizadas en el Servidor instalado del Hospital Ambato y las implementaciones con los escenarios con servidores UTM y NGFW.

Tabla 22-4: Porcentaje de pérdidas comparativo.

Porcentaje de tiempo libre de errores			
Días	**Servidor Hospital Ambato**	**UTM**	**NGFW**
Día 1	98,9915%	99,8548%	99,9243%
Día 2	99,2491%	99,8206%	99,9647%
Día 3	99,1726%	99,6347%	99,9284%
Día 4	98,9445%	99,6609%	99,8896%
Día 5	99,4965%	99,6007%	99,9627%
Día 6	99,4204%	99,6337%	99,7010%
Día 7	98,8152%	99,5871%	99,7756%
Día 8	99,2739%	99,8931%	99,6917%
Día 9	99,1599%	99,7468%	99,8640%
Día 10	99,1773%	99,6253%	99,8257%
Día 11	99,2463%	99,9669%	99,8148%
Día 12	98,6620%	99,7606%	99,6514%
Día 13	99,0288%	99,6794%	99,8507%
Día 14	98,8070%	99,8948%	99,6641%
Día 15	99,4794%	99,7601%	99,6610%
Día 16	98,5573%	99,9665%	99,6602%
Día 17	99,4688%	99,9273%	99,8545%
Día 18	99,4921%	99,7557%	99,8556%
Día 19	99,3579%	99,8982%	99,7412%
Día 20	98,9409%	99,9328%	99,9246%
Promedio	99,1371%	99,7800%	99,8103%

Realizado por: Diego Silva, 2019

4.6.5.1 Prueba de Normalidad

Para poder aplicar la prueba t-student es necesario que los valores se comporten normalmente, es decir que los valores obtenidos cumplan con la distribución normal. Para ello se utiliza el siguiente criterio:

- P-valor $\geq \alpha$ Rechazar H_o: Los datos provienen de una distribución normal.
- P-valor $< \alpha$ No rechazar H_o: Los datos no provienen de una distribución normal.

La comprobación de normalidad se realiza en el software estadístico SPSS. Después de ingresados los datos de las variables en la "vista de datos" se obtienen los resultados.

Tabla 23-4: Prueba de Normalidad del indicador Exactitud

Pruebas de normalidad

		Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Tecnologías	Estadístico	Gl	Sig.	Estadístico	gl	Sig.
Exactitud	UTM	,157	20	,200*	,916	20	,081
	NGFW	,144	20	,200*	,909	20	,062

Realizado por: Diego Silva, 2019

Se observa el nivel de significancia en la prueba de Shapiro Wilk debido a que es para muestras pequeñas (menor o igual a 30) que es el caso de este estudio. En la tabla se observan los valores del nivel de significancia para poder compararlos con el nivel alfa como se observa a continuación:

P-valor (UTM)=0,081 > $\alpha = 0,05$

P-valor (NGFW)=0,062> $\alpha = 0,05$

Dado que P-valor es mayor que alfa se rechaza Ho: Los datos provienen de una distribución normal. Es decir, la variable "exactitud" en las dos tecnologías se comporta normalmente y se cumple una de las condiciones para realizar la prueba t-student.

4.6.5.2 Igualdad de varianzas

Otra condición para aplicar la prueba t-student es corroborar la igualdad de varianza entre los grupos. Si se cumple el criterio de que las varianzas son iguales además de haber cumplido con la prueba de normalidad, se puede proceder a realizar la prueba t-student para el análisis de hipótesis. Se utiliza el siguiente criterio:

- P-valor $\geq\alpha$; Rechazar H_o: Las varianzas son iguales
- P-valor $<\alpha$ No rechazar H_O: Existe diferencia significativa en las varianzas

Además de los valores ya ingresados, se requiere ingresar el valor del intervalo de confianza, debido a que el porcentaje de error (α) es del 5%, el intervalo de confianza será de 95%, que sumados son 100%.

Tabla 24-4: Prueba de igualdad de varianzas del indicador Exactitud

		Prueba de Levene de igualdad de varianzas	
		F	Sig.
Exactitud	Se asumen varianzas iguales	1,282	,431
	No se asumen varianzas iguales		

Realizado por: Diego Silva, 2019

La igualdad de varianza se corrobora mediante la "Prueba de Levene para la igualdad de varianzas", se observa el nivel de significancia, que en este caso es de 0,431
P-valor=0,431 > α=0.05

- P-valor ≥α; Rechazar Ho: Las varianzas son iguales
- P-valor <α No rechazar Ho: Existe diferencia significativa en las varianzas

Debido a que el nivel de significancia es mayor que alfa se rechaza Ho, es decir: Las varianzas son iguales.

4.6.5.3 Resultados de la prueba t-student

Se utiliza el siguiente criterio para la decisión estadística:

Si P-valor ≤ α se rechaza Ho

Si P-valor > α no se rechaza Ho

H1: **Existe** una diferencia significativa entre la media de los valores de exactitud con la tecnología UTM y la media de los valores de exactitud con la tecnología NGFW.

$H1$: $\mu a \neq \mu b$

Ho: **No existe** una diferencia significativa entre la media de los valores de exactitud con la tecnología UTM y la media de los valores de exactitud con la tecnología NGFW.

Ho: $\mu a = \mu b$

En el software IBM SPSS se analizan los resultados, se toma el valor de la significancia bilateral de la prueba t-student. Como se han asumido varianzas iguales se toma el valor correspondiente a tal característica a pesar de que en este caso son valores iguales, pero es necesario aclararlo. El valor es de 0,431 como se aprecia en la Tabla 26-4.

Tabla 25-4: Resultados estadísticos del indicador Productividad

Estadísticas de grupo

	Tecnologías	N	Media	Desviación estándar	Media de error estándar
Exactitud	UTM	20	,99779994	,001306866	,000292224
	NGFW	20	,99810293	,001089605	,000243643

Realizado por: Diego Silva, 2019

Tabla 26-4: Resultados de la prueba t-student del indicador Exactitud

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	T	Gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Exactitud	Se asumen varianzas iguales	1,282	,265	-,796	38	,431	-,000302984	,000380469	-,001073204	,000467236
	No se asumen varianzas iguales			-,796	36,809	,431	-,000302984	,000380469	-,001074022	,000468055

Realizado por: Diego Silva, 2019

P-valor=0,431 ≥ α=0.05

Debido a que P-valor es mayor que alfa se acepta H_o, es decir, **Ho: NO Existe** una diferencia significativa entre la media de los valores de exactitud con la tecnología UTM y la media de los valores de exactitud con la tecnología NGFW.

Descriptivamente la diferencia entre las medias de ambas tecnologías. La media para la tecnología UTM es de 99,77% y 99,81% para la tecnología NGFW.

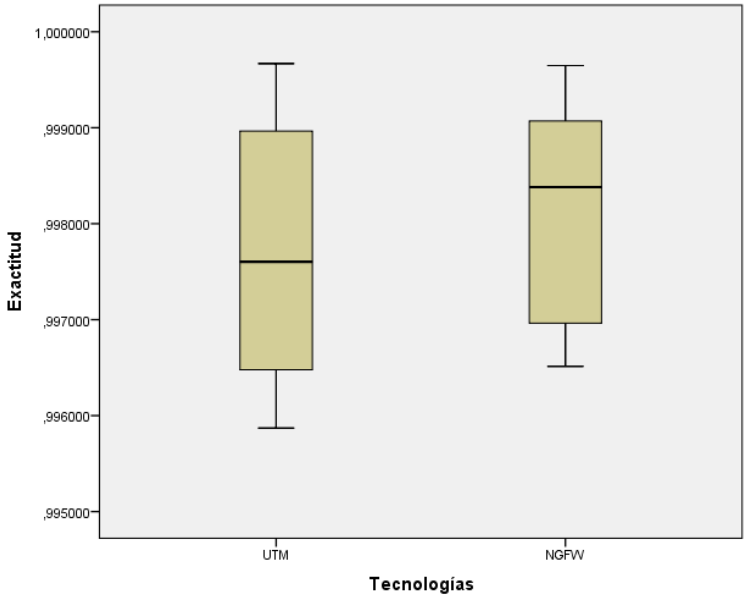


Figura 19-4: Medias de los valores de Exactitud de las tecnologías UTM y NGFW

Realizado por: Diego Silva, 2019

4.6.5.4 Decisión Estadística

Después de realizada la prueba t-student para la variable "exactitud" se concluye que **no existe** una diferencia significativa entre la media de los valores de porcentaje de exactitud con la tecnología UTM y NGFW. Esto quiere decir que a más de observar que la media de los valores con tecnología UTM es menor con muy poco, la prueba t-student indica que no es significativamente menor, lo que indica que se puede asegurar que en cuanto a la variable exactitud, la tecnología NGFW no tiene ventaja frente a UTM, ya que los valores de porcentaje de exactitud son muy aproximados, entendiéndose de esta manera que las dos tecnologías manejan un porcentaje muy bueno aproximándose al 100%

4.7 Medición de indicadores

Tabla 27-4: Medición de indicadores.

Indicadores	Índices	Servidor del Hospital Ambato	Servidor UTM	Servidor NGFW
• Productividad	• $Tasa\ de\ ocurrencia\ de\ eventos = \frac{Total\ de\ Vulnerabilidades\ detectadas}{Total\ de\ Vulnerabilidades\ estimadas}$	$TOE = \frac{0}{0}$ $TOE = 0$	$TOE = \frac{248,6}{384}$ $TOE = 65\%$	$TOE = \frac{294}{384}$ $TOE = 77\%$
• Utilización	• $Porcentaje\ de\ utilización\ del\ medio$ • $Con\ carga\ de\ usuario = \frac{Ancho\ de\ banda\ utilizado}{Ancho\ de\ banda\ existente}$ • $Sin\ carga\ de\ usuario = \frac{Ancho\ de\ banda\ utilizado}{Ancho\ de\ banda\ existente}$	• $PUCC = \frac{10,68}{19} = 56\%$ • $PUSC = \frac{11,59}{19} = 61\%$	• $PUCC = \frac{11,05}{19} = 58\%$ • $PUSC = \frac{13,29}{19} = 70\%$	• $PUCC = \frac{13,13}{19} = 69\%$ • $PUSC = \frac{17,23}{19} = 90\%$
• Disponibilidad	• $Porcentaje\ de\ tiempo\ activo = \frac{Horas\ Totales - Horas\ paradas\ programadas}{Horas\ Totales} x100$	100%	100%	100%
• Tiempo de respuesta	• $Tiempo\ de\ Respuesta = \frac{TRE-(TRU-TRE)}{TRE}$ • Dónde: • TRU = Tiempo de respuesta desde la petición de usuario • TRE = Tiempo de respuesta esperado	• $TR = = \frac{59,87-(204-59,87)}{59,87}$ $TR = -141\%$	• $TR = = \frac{59,87-(68,9-59,87)}{59,87}$ $TR = 85\%$	• $TR = = \frac{59,87-(61,6-59,87)}{59,87}$ $TR = 97\%$
• Exactitud	• $Porcentaje\ de\ tiempo\ libre\ de\ errores = \frac{Tiempo\ total\ de\ la\ prueba-(Tiempo\ de\ respuesta*Paquetes\ perdidos)}{Tiempo\ total\ de\ la\ prueba}$	99,1371 %	99,78 %	99,8103 %

Realizado por: *Diego Silva, 2019*

4.8 Análisis Comparativo para determinar la mejor opción a ser aplicada

Se ha realizado un análisis estadístico que ha permitido comprobar hipótesis individuales de cada indicador de las tecnologías estudiadas y se obtiene un valor porcentual de cada uno. Se requiere establecer una tabla comparativa que evidencie los resultados obtenidos y permita determinar la mejora con la aplicación de las tecnologías y cual de ellas es la mejor para ser aplicada. Para esto se emplea el diagrama de Likert ajustado al estudio actual dando un enfoque cualitativo a los datos obtenidos. Se asignan puntajes a cada ítem con el fin de que se reflejen actitudes positivas o negativas.

Tabla 28-4: Diagrama de Likert – Indicadores Hospital General Ambato

SERVIDOR HOSPITAL AMBATO

	Muy Deficiente	**Deficiente**	**Regular**	**Bueno**	**Muy Bueno**
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Productividad	X				
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Utilización					
Con carga de Usuario			X		
Sin carga de Usuario				X	
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Disponibilidad					X
	< 60 %	60% - 70%	70% - 80%	80% - 90%	> 90%
Tiempo de respuesta	X				
	<99,4%	99,4% - 99,5	99,5% - 99,6%	99,6% - 99,75%	> 99,75%
Exactitud	X				

Realizado por: Diego Silva, 2019

Tabla 29-4: Diagrama de Likert – Indicadores UTM.

TECNOLOGÍA UTM

	Muy Deficiente	**Deficiente**	**Regular**	**Bueno**	**Muy Bueno**
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Productividad				X	
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Utilización					
Con carga de Usuario			X		

Sin carga de Usuario				X	
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Disponibilidad					X
	< 60 %	60% - 70%	70% - 80%	80% - 90%	> 90%
Tiempo de respuesta				X	
	<99,4%	99,4% - 99,5	99,5% - 99,6%	99,6% - 99,75%	> 99,75%
Exactitud					X

Realizado por: Diego Silva, 2019

Tabla 30-4: Diagrama de Likert – Indicadores Hospital General Ambato.

TECNOLOGÍA NGFW

	Muy Deficiente	**Deficiente**	**Regular**	**Bueno**	**Muy Bueno**
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Productividad					X
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Utilización					
Con carga de Usuario				X	
Sin carga de Usuario					X
	< 40 %	40% - 50%	50% - 60%	60% - 75%	> 75%
Disponibilidad					X
	< 60 %	60% - 70%	70% - 80%	80% - 90%	> 90%
Tiempo de respuesta					X
	<99,4%	99,4% - 99,5	99,5% - 99,6%	99,6% - 99,75%	> 99,75%
Exactitud					X

Realizado por: Diego Silva, 2019

Tabla 31-4: Matriz de Contingencia de Valores Observados en Diagramas de Likert.

MATRIZ DE CONTINGENCIA DE VALORES OBSERVADOS

	Muy Deficiente	**Deficiente**	**Regular**	**Bueno**	**Muy Bueno**
SERVIDOR HGA	2	0	1	1	1
UTM	0	0	1	3	1
NGFW	0	0	0	1	4

Realizado por: Diego Silva, 2019

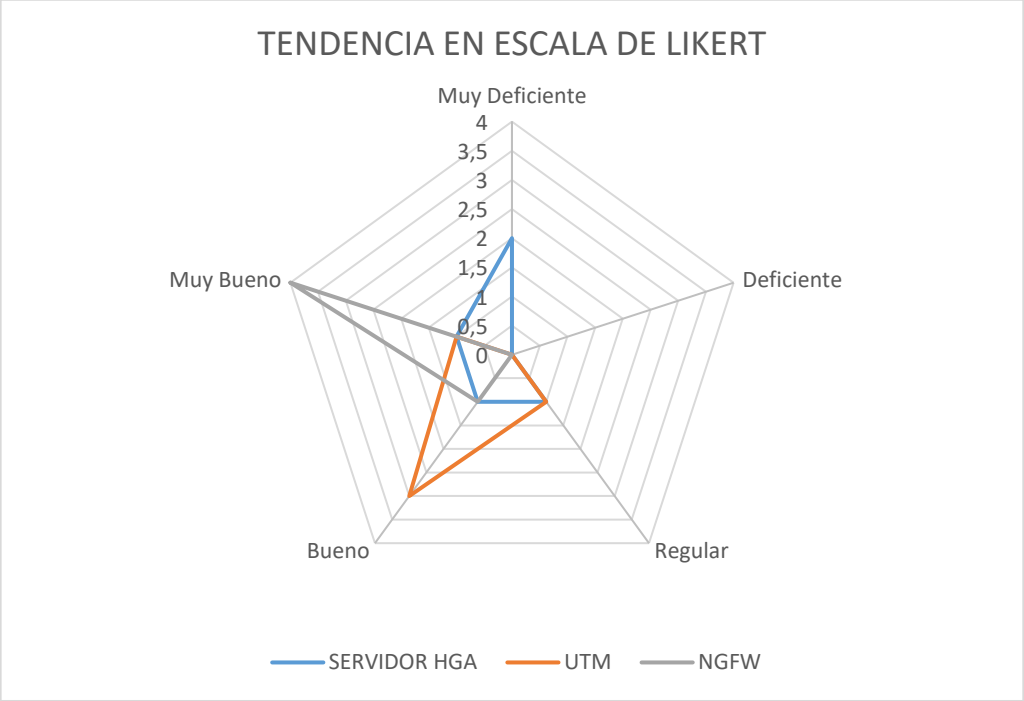


Figura 20-4: Tendencia de Tecnologías en Escala de Likert

Realizado por: Diego Silva, 2019

En la Figura anterior se puede apreciar la tendencia de cada tecnología aplicada, incluyendo al servidor de red del Hospital General Ambato, la cual permite identificar claramente de manera cualitativa que la tecnología NGFW tiene tendencia a MUY BUENO, mientras que la tecnología UTM tiende a BUENO, por último, se puede apreciar el contraste con el Servidor del HGA el mismo que tiende a una calificación de regular.

La medición de indicadores y su representación cualitativa y gráfica permite determinar que la mejor opción para ser aplicada es la tecnología NGFW, la cual en las pruebas realizadas ha demostrado estadísticamente ser mejor en casi todos los aspectos. Como apoyo para la toma de decisión la figura muestra la tendencia individual.

4.9 Comprobación de Hipótesis

Tabla 32-4: Tabla comparativa de indicadores.

Hipótesis	**Variables**	**Indicadores**	**Servidor Hospital Ambato**	**UTM**	**NGFW**
La aplicación de un sistema de detección de vulnerabilidades UTM (Unified Threatment Management) o NGFW (Next Generation Firewall) mejorará la disponibilidad de la red institucional	**Variable Independiente:** Sistema de detección de vulnerabilidades UTM (Unified Threatment Management) o NGFW (Next Generation Firewall)	• Productividad	• 0	• 65%	• 77%
		• Utilización con usuarios	• 56%	• 58%	• 69%
		• Utilización sin usuarios	• 61%	• 70%	• 90%
	Variable Dependiente: Disponibilidad de la red	• Disponibilidad	• 100%	• 100%	• 100%
		• Tiempo de Respuesta	• -141%	• 85%	• 97%
		• Exactitud	• 99,1371%	• 99,78	• 99,8103

Realizado por: Diego Silva, 2019

Para establecer la comprobación de hipótesis se han determinado indicadores tanto de la variable independiente como la variable dependiente, los mismos que han sido tratados estadísticamente de forma individual con la prueba t-student; se generan diagramas de Likert para tratar de forma cualitativa a los indicadores y poderlos representar gráficamente; finalmente se establece una tabla comparativa entre los indicadores.

Los resultados obtenidos en las pruebas aplicadas para cada indicador, muestran de manera clara que la aplicación de un sistema de detección de vulnerabilidades UTM (Unified Threatment Management) o NGFW (Next Generation Firewall) mejora la disponibilidad de la red institucional de manera significativa por lo cual se comprueba la hipótesis planteada.

Se comprueba además que la tecnología Next Generation Firewall para detección de vulnerabilidades es la mejor opción para ser aplicada en el Hospital General Ambato; pues ha superado al servidor UTM en todos los indicadores propuestos en la presente investigación.

CAPÍTULO V

5. PROPUESTA

5.1 Definición de Políticas

El Hospital General Ambato, cuenta con una infraestructura nueva con los servicios de Emergencia, Consulta Externa, Hospitalización, Laboratorio, Imagenología, Farmacia, Admisiones, Atención al Usuario en el área de atención al usuario externo. El área Administrativa se encuentra distribuida en espacios independientes de Gerencia, Administrativo Financiero, Talento Humano, Bodega.

Se cuenta con cableado estructurado con dos racks de datos por piso en fase 2 (consulta externa) y dos racks por piso en fase 3 (hospitalización); el cableado horizontal está instalado con cable UTP categoría 6, la conexión desde los racks hacía el Data Center es mediante fibra óptica multimodo. Se cuenta con dos Switch de Core configurados con balanceo de carga con capacidad de 20 Gbps cada uno ofreciendo una capacidad total de 40 Gbps en la Red de Área Local.

Se determina la subdivisión en Redes Virtuales para tener una mejor administración de los segmentos de red de acuerdo a la distribución del edificio. Se debe aplicar además las políticas establecidas por la Dirección Nacional de TICS del Ministerio de Salud Pública del Ecuador.

Entre otras se describen las políticas aplicables en el Next Generation Firewall:

- Establecer un control a nivel tecnológico para que los equipos informáticos de escritorio que no sean propiedad del MSP no se puedan conectar a la red institucional, ya sea por conexión alámbrica o inalámbrica, ya que constituye grave riesgo de seguridad. La infracción deberá ser reportada al Oficial de Seguridad de la Información.

- Establecer un control a nivel tecnológico para que los equipos informáticos portátiles que no sean de propiedad del MSP y pertenezcan a terceros autorizados, se conecten a través de una conexión inalámbrica exclusiva para el efecto, los accesos serán limitados a los servicios de red y recursos informáticos autorizados y no podrán comunicarse entre sí, ni con equipos informáticos de escritorio y portátiles de funcionarios de la institución.

• Proporcionar los medios de conexión a los servicios de red institucionales a los equipos informáticos portátiles que no sea de propiedad del MSP y que pertenezcan a funcionarios de la institución, cuando haya sido solicitado por el Jerárquico Superior, revisado por el Responsable de Seguridad de Tecnologías de la Información y aprobado por el Oficial de Seguridad de la Información, en el caso de Planta Central y el responsable de la Unidad de Tecnología en caso de una unidad a nivel desconcentrado.

• Proporcionar los medios de conexión a los servicios de red institucionales a los dispositivos móviles que pertenezcan a los funcionarios del MSP, cuando haya sido solicitado por el Jerárquico Superior, revisado por el Responsable de Seguridad de Tecnologías de la Información y aprobado por el Oficial de Seguridad de la Información, en el caso de Planta Central y el responsable de la Unidad de Tecnología en caso de una unidad a nivel desconcentrado.

• Configurar redes inalámbricas institucionales para el uso de servicios de red mediante dispositivos móviles y establecer controles de acceso lógico a los servidores institucionales.

• Configurar redes inalámbricas aisladas de manera lógica para la ciudadanía que hace uso de los servicios institucionales y establecer controles de conexión a los servidores y aplicaciones internas.

• Establecer un control a nivel tecnológico para evitar la conexión a los servicios de red a los equipos informáticos de escritorio o portátiles de los funcionarios que hayan sido configurados como servidores de aplicaciones de propósito general o específico, o motores de bases de datos institucionales. Solo se permitirá utilizar para estos efectos equipos servidores que pertenezcan al parque tecnológico del Centro de Procesamiento de Datos institucional.

• Evitar que los equipos escritorio o portátiles de los funcionarios que ha sido asignados para realizar las actividades operativas, sean configurados también como servidores de aplicaciones de propósito general o específico, o motores de bases de datos institucionales. Solo se permitirá utilizar para estos efectos equipos servidores que pertenezcan al parque tecnológico del Centro de Procesamiento de Datos institucional.

• Proporcionar un medio de conexión temporal y aislado en una red lógica diferente a los servicios de red institucionales para los equipos informáticos diseñados para proporcionar aplicaciones de propósito general o específico o alojar un repositorio de información, para

ejecutar una demostración o prueba de concepto, cuando haya sido solicitado por el Jerárquico Superior, revisado y aprobado por el responsable de la Unidad de Tecnología en caso de una unidad a nivel desconcentrado.

• Usar los equipos informáticos del MSP para desarrollar las actividades propias de cada estructura organizacional, bajo ninguna circunstancia se utilizarán los recursos informáticos para realizar actividades prohibidas por la normativa legal vigente o por normas jurídicas nacionales o internacionales.

• Garantizar la continuidad de los servicios y comunicaciones del MSP, realizando un monitoreo continuo de los enlaces de comunicaciones, los servicios tecnológicos de esta Cartera de Estado.

• Usar el servicio de internet institucional para temas exclusivamente laborales.

• Administrar la infraestructura tecnológica del servicio de internet institucional y monitorear sus capacidades a fin de proporcionar un servicio óptimo.

• Configurar los permisos de navegación a páginas web externas cuando por necesidades institucionales haya sido solicitado por el Jerárquico Superior para los funcionarios a su cargo, revisado y probado por el responsable de la Unidad de Tecnología en caso de una unidad a nivel desconcentrado.

• Configurar el acceso al servicio de internet institucional para terceros autorizados cuando por necesidades institucionales requieran acceder a portales web externos, utilizando infraestructura tecnológica institucional y haya sido solicitado por el Jerárquico Superior, revisado y probado por el responsable de la Unidad de Tecnología en caso de una unidad a nivel desconcentrado.

• Realizar monitoreo de puertos o análisis de tráfico en la red del MSP, con el motivo de evaluar seguridades y vulnerabilidades. La DNTIC o su Unidad Tecnología a nivel desconcentrado son las únicas autorizadas para realizar estas actividades.

• Descargar o transmitir archivos digitales que no sean para fines laborales como música o videos desde Internet ya que estos violan los derechos de propiedad intelectual y hacen un consumo inadecuado de los servicios de red.

5.2 Definición de Redes y Subredes

DISTRIBUCIÓN DE VLANS

Las Redes Virtuales de Área Local por sus siglas en inglés VLAN (Virtual Local Area Networks), permiten obtener un mejor desempeño de la misma al implementarse como varias redes lógicas funcionando sobre una misma red física(Rabie, Aboul-Magd, & Mohan, 2013). Se puede aplicar en la infraestructura de red motivo de investigación, para segmentar la red y poder administrarla de mejor manera.

La siguiente tabla muestra la distribución de las VLANS en los diferentes espacios físicos.

Tabla 1-5: Distribución de VLANs.

Nro. VLAN	GRUPO	UBICACIÓN
10	Emergencia	Planta Baja – Fase 2
11	Admisiones, Atención al Usuario	Planta Baja – Fase 2
12	Administrativo, Laboratorio, Rayos X	Área de Contingencia
20	Consulta Externa	Piso 1, Piso 2 – Fase 2
30	Hospitalización	Planta Baja, Piso 1, Piso 2, Piso 3 – Fase 2
40	Red Inalámbrica Servicios HGA 1	Toda la Infraestructura (Administrativos de nivel jerárquico superior)
41	Red Inalámbrica Servicios HGA 2	Toda la Infraestructura (Administrativos de nivel jerárquico bajo)
42	Red Inalámbrica Equipos Médicos	Toda la Infraestructura (Conexión de Equipos Médicos Inalámbricos)
50	Administración de Dispositivos de conexión	Toda la Infraestructura
100	Telefonía IP	Toda la Infraestructura
200	Administración de Servidores	Data Center – Fase2
210	Administración de Firewalls	Data Center – Fase2

Realizado por: Diego Silva, 2019

5.3 Implementación del Servidor para detección de vulnerabilidades

Ya en la implementación de los escenarios de prueba, se establecieron las configuraciones básicas para el funcionamiento del NGFW Huawei USG6630 para funcionar con filtrado de paquetes, detección y protección de intrusiones; el mismo requiere el acondicionamiento para trabajar con

la segmentación de la red, y proveer el servicio con la aplicación de las políticas de acceso. Se procede a explicar las configuraciones necesarias para complementar el funcionamiento del sistema de detección de vulnerabilidades.

5.3.1 Definición de Objetos de Red

Se requiere la creación de los siguientes objetos para ser utilizados posteriormente

Tabla 2-5: Objetos de Red - NGFW.

Nombre	Descripción	Red
Equipos_Medicos	Red inalámbrica de equipos médicos	192.168.44.0/24
External_FW_PBX	Dirección IP de WAN de PBX telefónica	10.203.x.x/32
IP_Internet	IP pública utilizada para la conexión a internet	186.46.x.x/32
IP_DNS	IP de DNS de proveedor de Internet	200.107.10.100 200.107.10.105
IP_FW_TO_SW	IP para acceso de configuración	192.168.210.1/32
IP_PBX_Intranet	VLAN para telefonía	192.168.100.0/23
LAN_P1_F2	Red Piso 1 Fase 2	192.168.20.0/24
LAN_P1_F3	Red Piso 1 Fase 3	192.168.21.0/24
LAN_P2_F2	Red Piso 2 Fase 2	192.168.30.0/24
LAN_P2_F3	Red Piso 2 Fase 3	192.168.31.0/24
LAN_P3_F3	Red Piso 3 Fase 3	192.168.35.0/24
LAN_PB_BloqueA	Red Planta Baja Bloque A	192.168.10.0/24
LAN_PB_Emergencia	Red Planta Baja Emergencia	192.168.11.0/24
LAN_PB_Fase3	Red Planta Baja Fase 3	192.168.12.0/24
WLAN_HGA_Servicios1	Red Inalámbrica para personal médico	192.168.41.0/24
WLAN_HGA_Servicios2	Red Inalámbrica con privilegios	192.168.42.0/24
WLAN_Hospital_Ambato	Red Inalámbrica para conexión de usuario común	192.168.44.0/24

Realizado por: *Diego Silva, 2019*

Se deben aplicar los objetos en el sistema de administración del NGFW, ingresando en el menú *Object -> Address -> Address* opción *Add*

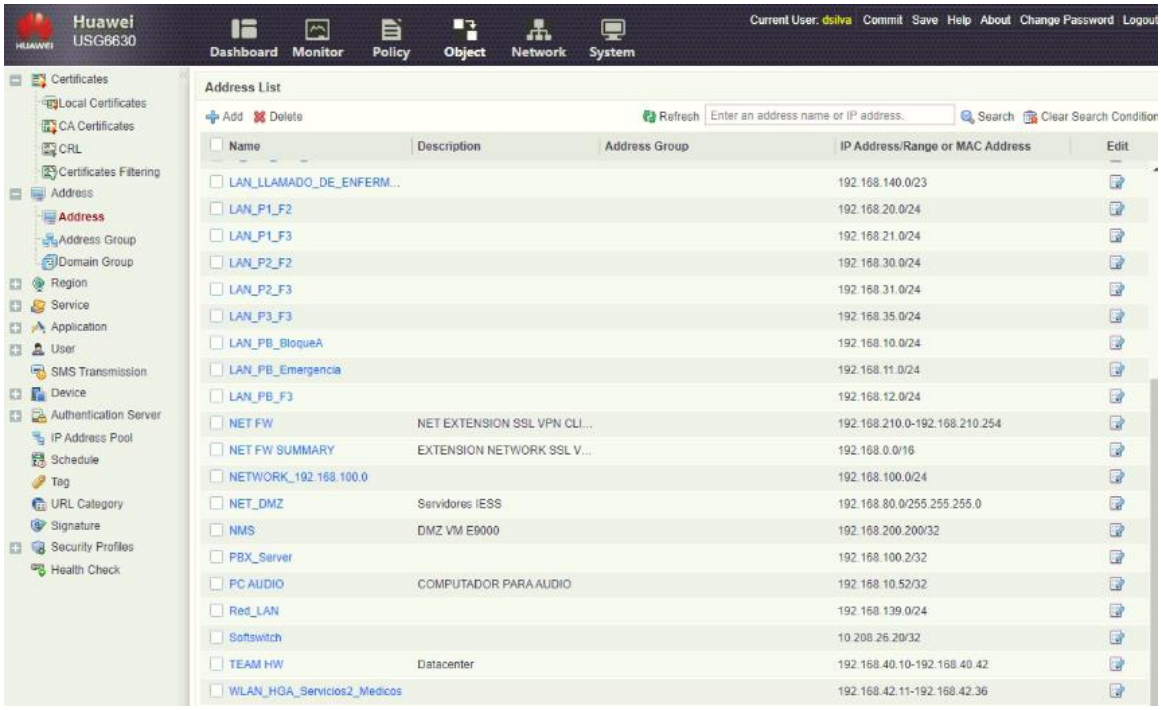


Figura 1-5: Definición de Objetos - NGFW

Realizado por: Diego Silva, 2019

5.3.2 Configuración NAT para conectividad de PBX

Se debe establecer una configuración NAT para enmascarar las conexiones hacia internet de la red LAN y que las peticiones puedan ser traducidas.

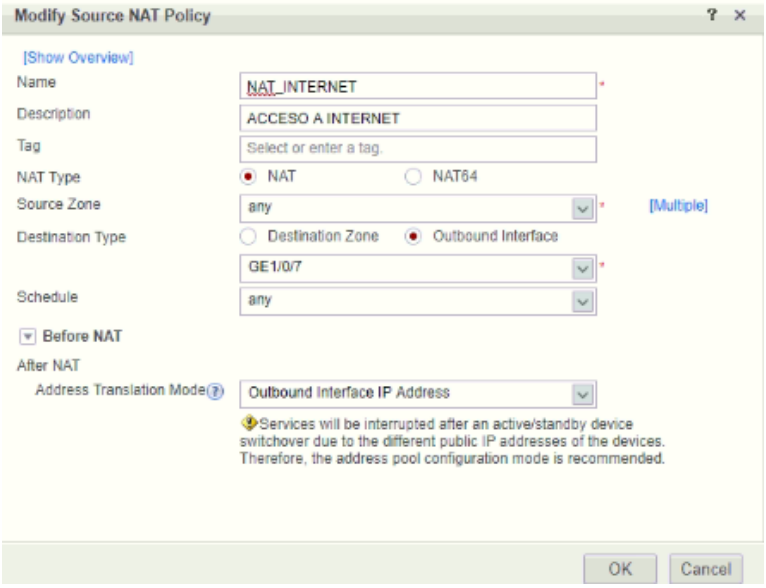


Figura 2-5: Definición de NAT para LAN - NGFW

Realizado por: Diego Silva, 2019

La conexión de la telefonía digital sale a través del firewall, es necesario establecer un NAT para indicar al NGFW como enmascarar estas conexiones de la VLAN de la Telefonía hacia la WAN del proveedor de internet.

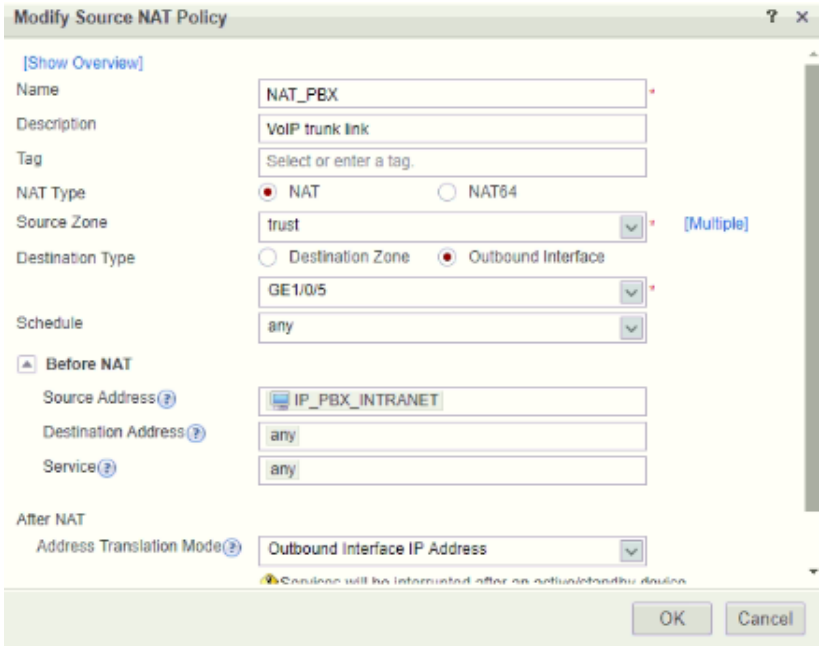


Figura 3-5: Definición de NAT para Telefonía - NGFW

Realizado por: Diego Silva, 2019

En resumen, las reglas de NAT quedan de la siguiente manera, tomando en cuenta que existe una definición por defecto establecida por el equipo.

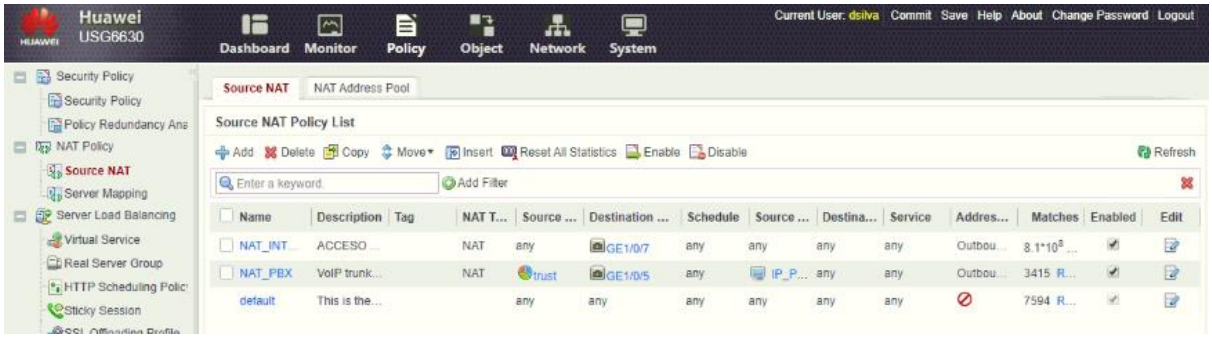


Figura 4-5: Definición de NAT - NGFW

Realizado por: Diego Silva, 2019

5.3.3 Definición de Políticas de Acceso en NGFW

A continuación, se listan las políticas implementadas tomando en cuenta que dependen del orden en las que se encuentran determinadas, se puede negar o permitir una acción que más abajo se haga lo contrario y no se ejecute. Es importante mencionar que la Licencia del NGFW mantiene

una base de datos actualizada de URLS y Aplicaciones que se pueden elegir dentro la declaración de cada regla de acceso.

Tabla 3-5: Definición de Políticas - NGFW.

Nombre	Zona Origen	Zona Destino	Dirección Origen	Dirección Destino	Aplicación	Acción
PBX (Permitir de una zona confiable a la PBX)	No confiable	Confiable	Cualquiera	192.168.100.0/24	Cualquiera	Permitir
SBC2PBX (Controlador de Sesión a PBX)	No confiable	Local	IP_SBC_VoIP_ISP 10.208.x.x/32	IP_PBX_TRUNK 10.203.x.0/30	Cualquiera	Permitir
VoIP_LAN_to_Internet (Permitir la salida de telefonía a Internet)	Confiable	No Confiable	PBX_Server 192.168.100.0/23	Cualquiera	Cualquiera	Permitir
LAN_Allow_Social (Redes Sociales en LAN)	Confiable	No Confiable	Cualquiera	Cualquiera	Compras Pornografía Juegos Netflix Loteria	Denegar
LAN1_TO_INTERNET (IPS privilegiados con restricción antecedente mínima)	Confiable	No Confiable	IP_Privilegiadas (Gerencia, Comunicación, jefes, TICS)	Cualquiera	Cualquiera	Permitir
ATENCION_USUARIO (Solo Whatsapp)	Confiable	No Confiable	192.168.40.0/24	Cualquiera	Whatsapp	Permitir
POLITICAS_URLS (URLS no permitidas)	Confiable	No Confiable	Cualquiera	Cualquiera	Proxies RadioOnline MercadoLibre OLX	Denegar
Deny_Social_Network (Listado de aplicaciones denegadas)	Confiable	No Confiable	Cualquiera	Cualquiera	Facebook Twitter Instagram Youtube Recreación Descarga de Software Compras Viajes Música Video	Denegar
LAN2_TO_INTERNET (IPS con restricción antecedente mínima)	Confiable	No Confiable	LAN_P1_F2 LAN_P1_F3 LAN_P2_F2 LAN_P2_F3 LAN_P3_F3	Cualquiera	Cualquiera	Permitir

			LAN_PB_BloqueA LAN_PB_Emergencia LAN_PB_Fase3 WLAN_HGA_Servicios1 WLAN_HGA_Servicios2			
IP_FW_INTRANET (Permitir conexión del firewall con intranet)	Local	Local Trust	Cualquiera	Cualquiera	Cualquiera	Permitir
DNS_TRAFFIC (Permitir Consultas a DNS)	Confiable	No Confiable	Cualquiera	IP_DNS	Cualquiera	Permitir
INTERNET_TO_FW (Actualización de Base de Datos de URLS y Aplicaciones)	No Confiable	Local	Cualquiera	IP_Internet	Cualquiera	Permitir
FW_OUT (Desde el Firewall a Internet)	Local	No Confiable	Cualquiera	Cualquiera	Cualquiera	Permitir
IP_FW_TO_SW_Core (Acceso desde SW a IP de configuración de NGFW)	Confiable	Local	Culaquiera	IP_FW_TO_SW	Cualquiera	Permitir

Realizado por: *Diego Silva, 2019*

En el menú *Policies -> Security Policy -> Security Policy* añadir las reglas definidas anteriormente.

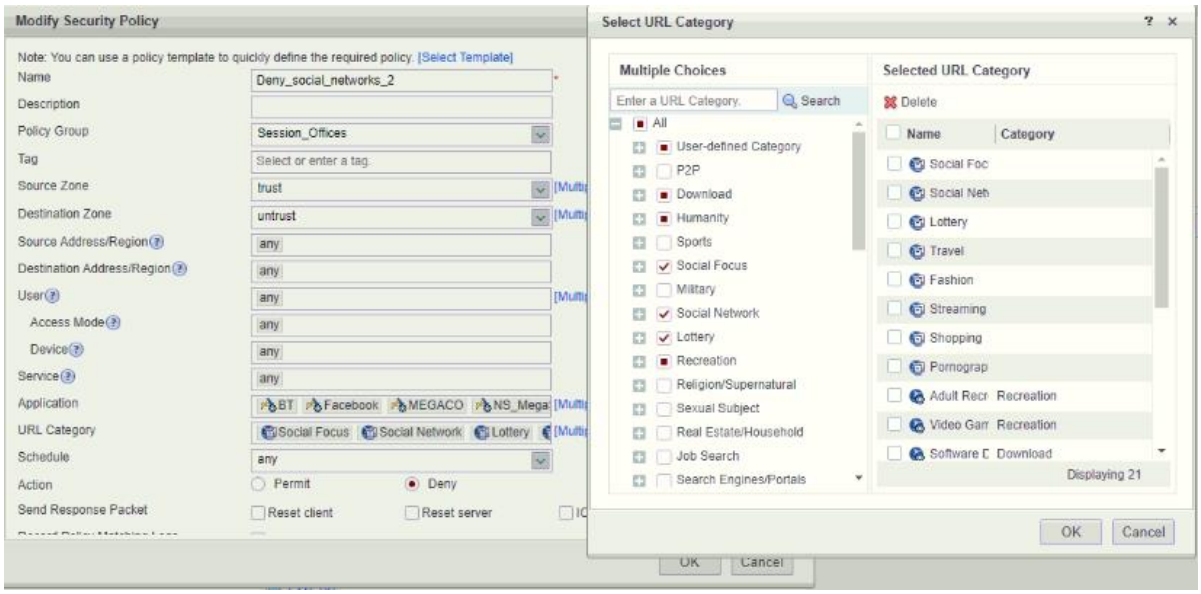


Figura 5-5: Definición de Políticas - NGFW

Realizado por: Diego Silva, 2019

5.3.4 Monitoreo de NGFW

Parte importante en la administración de una red es el constante monitoreo de las actividades que se están ejecutando en el servidor, alertas de intrusiones en el sistema, el consumo de ancho de banda el número de usuarios conectados, determinar que aplicación o que usuario está utilizando mayores recursos para poder realizar un análisis y tomar decisiones que impliquen políticas de acceso para un mejor desempeño de la red.

El NGFW de Huawei, incluye un Dashboard mostrado como página de inicio que despliega un resumen de las actividades ejecutadas por el servidor.

En la siguiente imagen se muestra las conexiones existentes, a través del puerto 5 el PBX, en el puerto 7 la IP pública, en los puertos 9 y 11 de fibra óptica las conexiones hasta el Switch de Core y su espejo

Figura 6-5: Información de Dispositivo - NGFW

Realizado por: Diego Silva, 2019

Se muestra un resumen del uso del CPU, de la Memoria y del almacenamiento interno, se observa que el almacenamiento está por llenarse con la información que almacena el NGFW, por lo que se puede considerar el incremento en almacenamiento. Además, muestra el número de conexiones por segundo, el consumo de ancho de banda, y los clientes conectados.

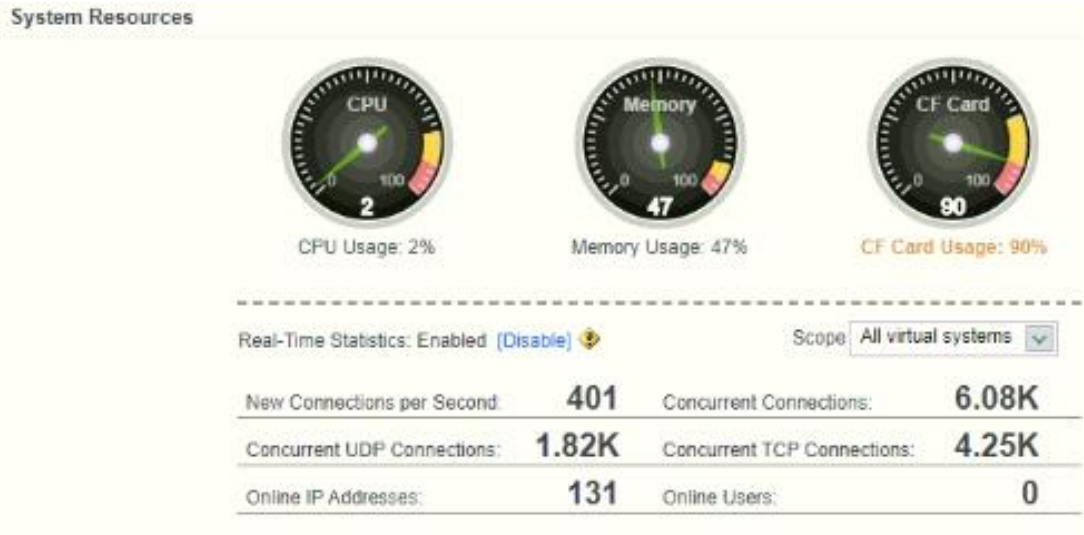


Figura 7-5: Recursos del Sistema - NGFW

Realizado por: Diego Silva, 2019

El consumo de ancho de banda se refleja en un período de 24 horas, y se puede determinar las horas pico de consumo de ancho banda.

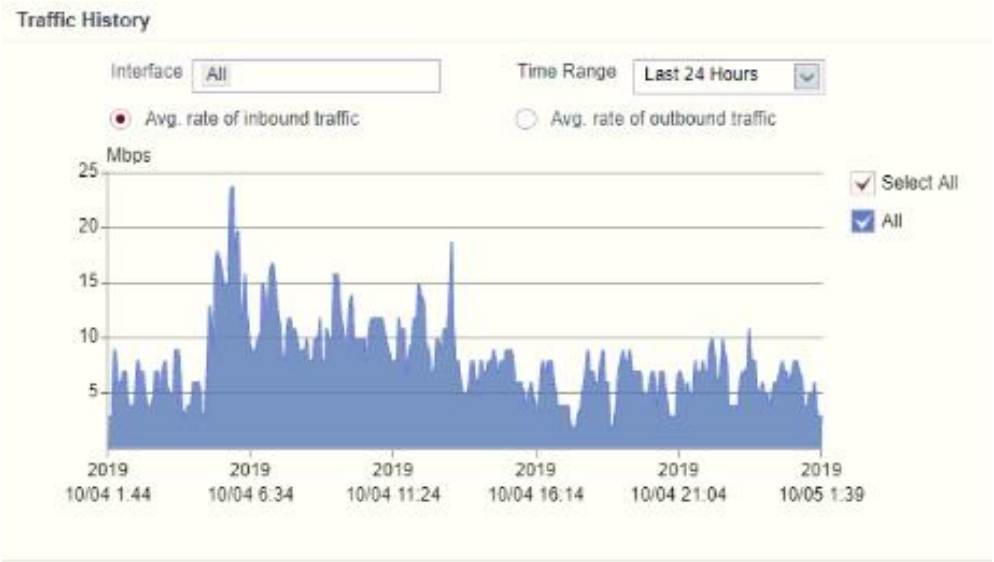


Figura 8-5: Consumo de ancho de banda - NGFW

Realizado por: Diego Silva, 2019

Se despliega también el Ranking en tiempo real de las direcciones IP que se encuentran consumiendo mayor ancho de banda.

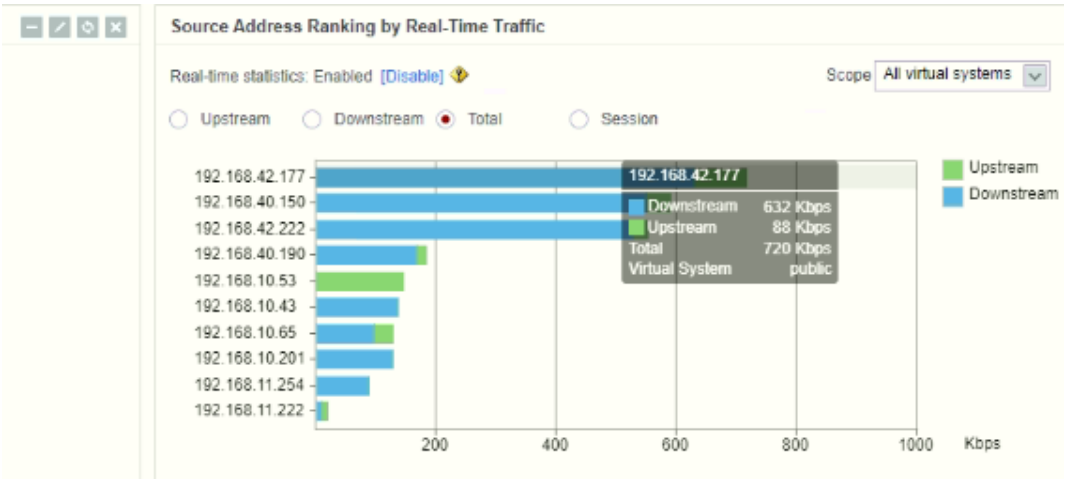


Figura 9-5: Ranking de Consumo de ancho de banda - NGFW

Realizado por: Diego Silva, 2019

El informe incluye también un ranking de las aplicaciones que se encuentran ocupando el medio de transmisión, se observa que aproximadamente 14 mbps están siendo utilizados por una descarga, seguido de conexiones HTTPS, Facebook al estar permitido en ciertos lugares y otras aplicaciones con menor consumo.

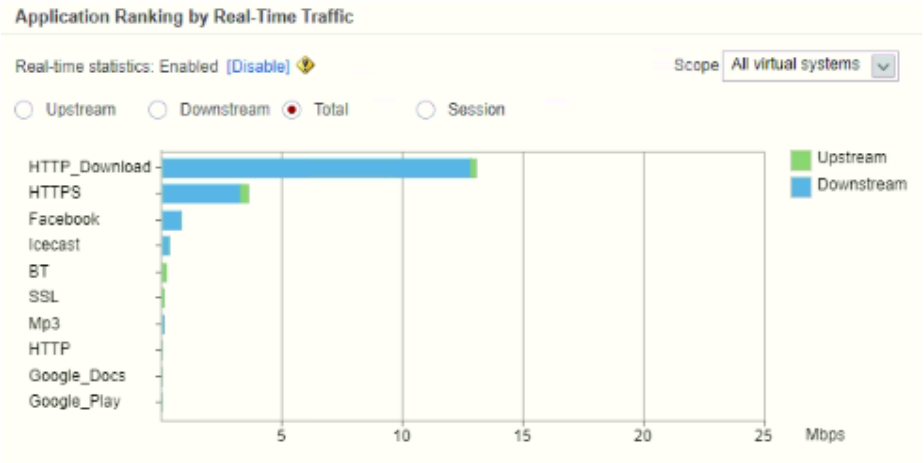


Figura 10-5: Ranking de aplicaciones con consumo de ancho de banda - NGFW

Realizado por: Diego Silva, 2019

Una de las partes esenciales es el log de las alarmas del sistema de protección de intrusiones el cual indica un informe detallado de cada una generada. Se observa que el sistema tiene constantemente intentos de conexión no deseados los que son identificados y neutralizados.

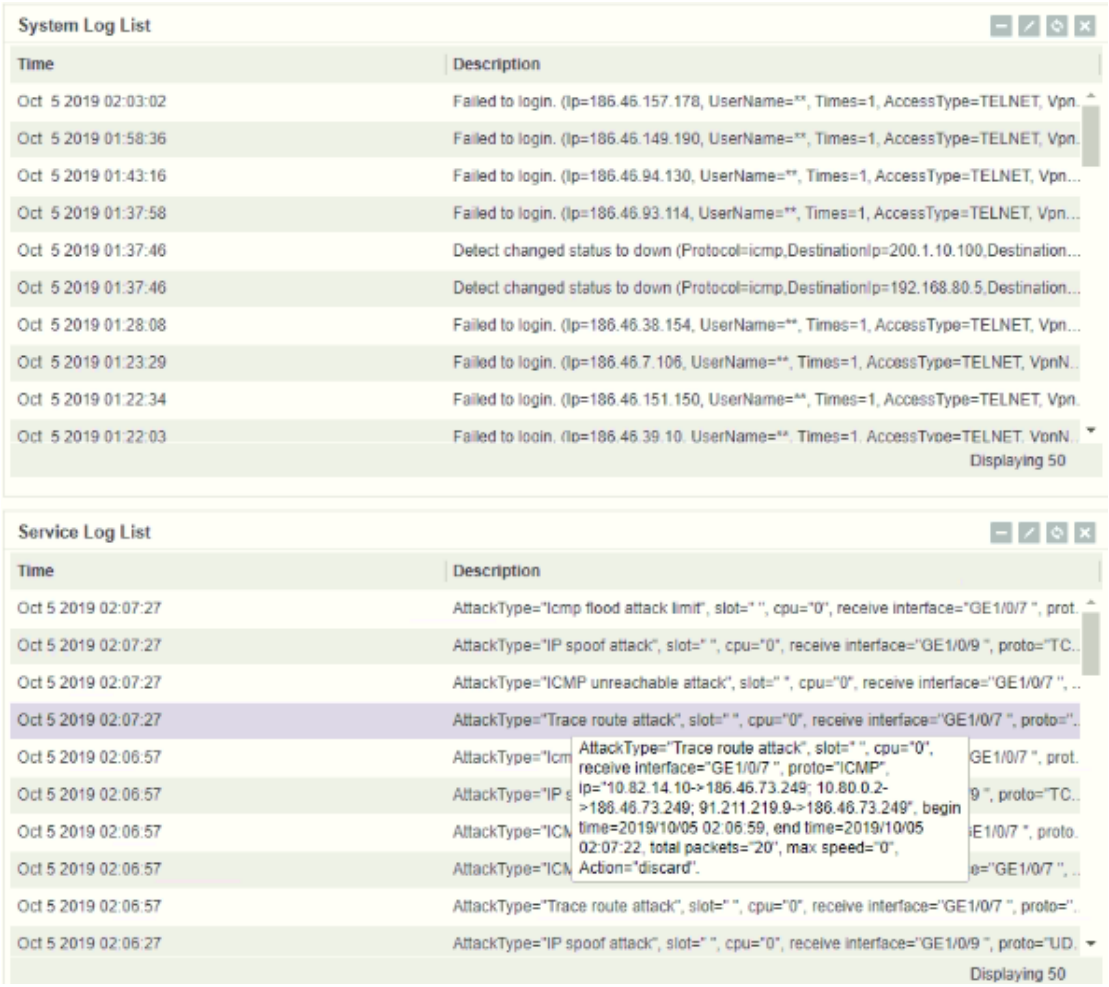


Figura 11-5: Logs del sistema de Detección/Protección de intrusos - NGFW

Realizado por: Diego Silva, 2019

CONCLUSIONES

- El Hospital Provincial General Docente Ambato ha prestado las facilidades necesarias para la aplicación de la investigación y posterior aplicación de un servidor que protege de las intrusiones detectadas. Además, se ha podido evaluar las tecnologías UTM (Unified Threatment Management) y NGFW (Next Generation Firewall) para la detección de vulnerabilidades en la red. El servidor de la casa de salud, carece de un sistema de detección/protección de intrusiones, con la implementación del servidor UTM se tiene un índice de productividad de 65% frente a 77% obtenido por el NGFW de detecciones efectivas de vulnerabilidades.

- Mediante la medición estadística cuantitativa y cualitativa, el análisis comparativo y gráfico de indicadores establecidos para comparar las dos tecnologías de detección y protección de vulnerabilidades se ha podido determinar que el servidor NGFW (Next Generation Firewall) es la mejor opción por haber superado al servidor UTM en los índices de la variable dependiente con un tiempo de respuesta de 85% (UTM) vs 97% (NGFW), el índice de exactitud de 99,78% (UTM) vs 99,81% (NGFW) y en el proceso de identificación/protección de intrusiones, filtrado de contenidos con una base de datos actualizada constantemente y que además ofrece un monitoreo de actividades en tiempo real que permite la toma de decisiones inmediata evitando afectar los servicios de red. Los indicadores obtenidos demuestran una mejora notable frente al servidor de red con el que se mantenía la administración en el Hospital General Ambato.

- Se ha diseñado e implementado los escenarios de prueba tomando en cuenta las políticas de uso de recursos tecnológicos que rige en el Ministerio de Salud Pública del Ecuador, de esta manera se han podido medir los indicadores propuestos y establecer políticas propias de red. Los resultados obtenidos se adaptan a entidades similares del sector salud, pues se ha realizado la investigación bajo condiciones propias de la naturaleza de su funcionamiento

- Con la información recopilada se ha establecido una guía para la implementación de un Sistema de Detección de Vulnerabilidades, su administración y Monitoreo. La guía indica de manera gráfica la creación y mantenimiento de las configuraciones inherentes a mantener la salud de la red.

RECOMENDACIONES

- Se han identificado intentos de accesos en forma reiterada al servidor a través de la IP pública, se recomienda mantener el sistema de Detección/Protección de Intrusos junto con la configuración establecida para evitar caída en los servicios de red prestados.

- Mantener las actualizaciones constantes del Sistema Operativo y de las Bases de Datos para la identificación de amenazas y el filtrado de reglas de filtrado de aplicaciones, para una eficiente administración combinada con el monitoreo de la red.

- Las políticas establecidas por la Dirección Nacional de TICS del MSP, establecen el uso de Software Libre, se puede implementar la opción del servidor UTM como controlador de Dominio y manejo de usuarios para un mejor control y administración de la red institucional.

- Los Manuales proporcionados resultantes de la presente investigación deben formar parte de la documentación de la Unidad de Tecnologías del Hospital General Ambato, para una recuperación inmediata ante una posible caída del Sistema.

BIBLIOGRAFÍA

Agham, V. (2016). Unified Threat Management. Obtenido de https://www.semanticscholar.org/paper/Unified-Threat-Management-Agham/f864e8730c699f63f7375f98d10f52f971111f70

Aguilera, P. (2011). *Redes seguras (Seguridad informática)*: Editex.

Ammann, P., Wijesekera, D., & Kaushik, S. (2002). *Scalable, graph-based network vulnerability analysis.* Paper presented at the Proceedings of the 9th ACM Conference on Computer and Communications Security.

BBC. (2016). 12 ataques por segundo: Cuáles son los países de América Latina más amenazados por malware.

Benjumea Ospino, C. M. (2016). Diseño de una guia de seguridad perimetral escalable y en alta disponibilidad con equipos firewall tipo NGFW.

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información*: Editorial Paraninfo.

Bustamante Sánchez, **R**. (2013). Seguridad en redes. Recuperado de http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/handle/231104/165

Cepal, **N.** (2016). Estado de la banda ancha en América Latina y el Caribe 2016. *Comisión Económica para América Latina y el Caribe*, 46. Recuperado de Estado de la banda ancha en América Latina y el Caribe 2016 Obtenido de: http://hdl.handle.net/11362/40528

Dordoigne, **J.** (2015). *Redes informáticas-Nociones fundamentales (5ª edición):(Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6...)*: Ediciones ENI.

Forouzan, B. A. B. A. (2007). *Transmisión de datos y redes de comunicaciones*: McGraw-Hill.

Huawei Technologies Co., L. (2019). Firewall de última generación de la serie USG6300. Retrieved 05/07/2019, 2019, Obtenido de: https://e.huawei.com/es/products/enterprise-networking/security/firewall-gateway/usg6300

Huitema, C. H. (2000). *Routing in the Internet*: Prentice-Hall.

ISO, N. (2008). 27002: 2008: Tecnología de la información. *Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información*.

Jajodia, S., Noel, S., & O'Berry, B. (2005). Topological analysis of network attack vulnerability *Managing Cyber Threats* (pp. 247-266): Springer.

Kolodgy, C. (2004). Worldwide Threat Management Security Appliances 2004-2008 Forecast and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance.

Maiwald, E., & Miguel, E. A. (2005). *Fundamentos de seguridad de redes*: McGraw-Hill.

Martínez, T. (2017). Diferencias entre UTM y NGFW, ¿las hay? , 2019, Obtenido de https://www.telequismo.com/2017/07/utm-ngfw.html/

Mieres, J. (2009). Ataques informáticos. *Debilidades de seguridad comúnmente explotadas).* Obtenido de *http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf*.

Miller, L. C. (2011). *Next-generation firewalls for dummies*: Wiley.

Molina, L. P. Z. (2012). Evaluación y mitigación de ataques reales a redes ip utilizando tecnologías de virtualización de libre distribución. *Ingenius*(8), 11-19.

Moreno, Y. C. (2010). UTM: Administración Unificada de Amenazas [UTM: Unified Threat Management]. *Ventana Informática*(22).

País, E. (2018). Noticias sobre ataques informáticos. Obtenido de https://elpais.com/tag/ataques_informaticos/a

Quirumbay Yagual, D. I. (2015). *Desarrollo del esquema de seguridad, plan de recuperación ante desastres informáticos y solución para el nivel de exposición de amenazas y vulnerabilidades aplicada a los servidores y equipos de comunicación del centro de datos de la municipalidad de la ciudad del este.* (Mastría), Escuela Superior Politécnica del Litoral, Guayaquil. Obtenido de http://www.dspace.espol.edu.ec/xmlui/handle/123456789/30025

Rabie, S., Aboul-Magd, O., & Mohan, D. (2013). VLAN support of differentiated services: Google Patents.

S.L., A. S. S. (2018). ABAST - Next Generation Firewalls. 2018, from http://www.abast.es/ciberseguridad/soluciones-de-seguridad-ti/next-generation-firewalls-ngfw/

Stallings, W. (2004). *Fundamentos de seguridad en redes: aplicaciones y estándares*: Pearson Educación.

Stallings, W. (2007). *Network security essentials: applications and standards*: Pearson Education India.

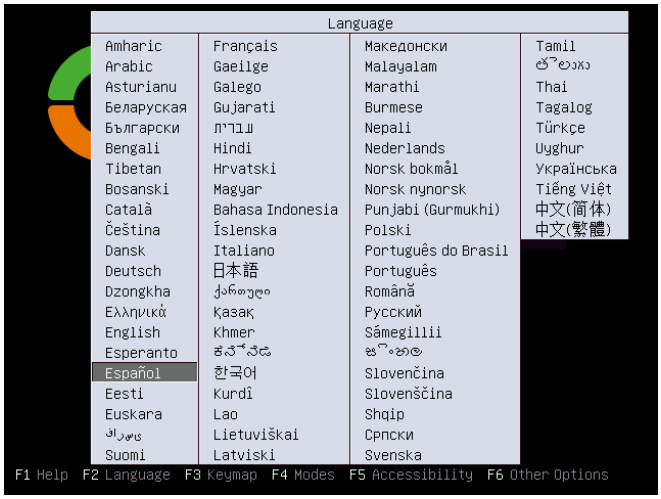
Vieites, A. G. (2013). Tipos de ataques e intrusos en las redes informáticas. Obtenido de https://www.edisa.com/wp-content/uploads/2019/08/ponencia_-_tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

ANEXOS

ANEXO A: INSTALACIÓN DE ZENTYAL

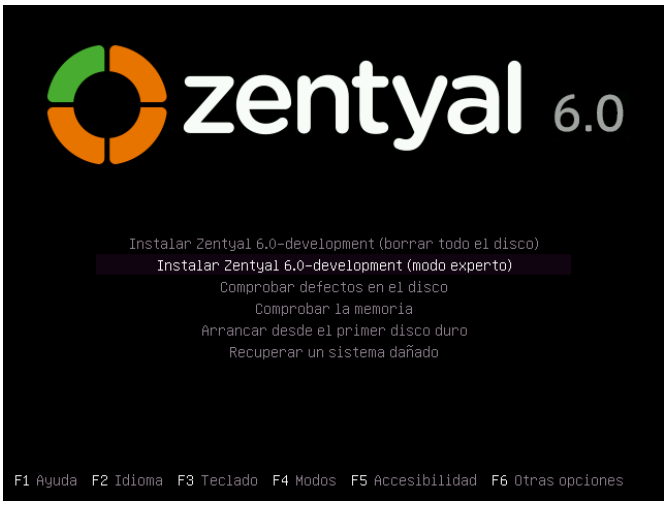
Link de descarga de Imagen ISO: http://download.zentyal.com/zentyal-6.0-development-amd64.iso

Una vez iniciada la instalación proceder con la elección del idioma



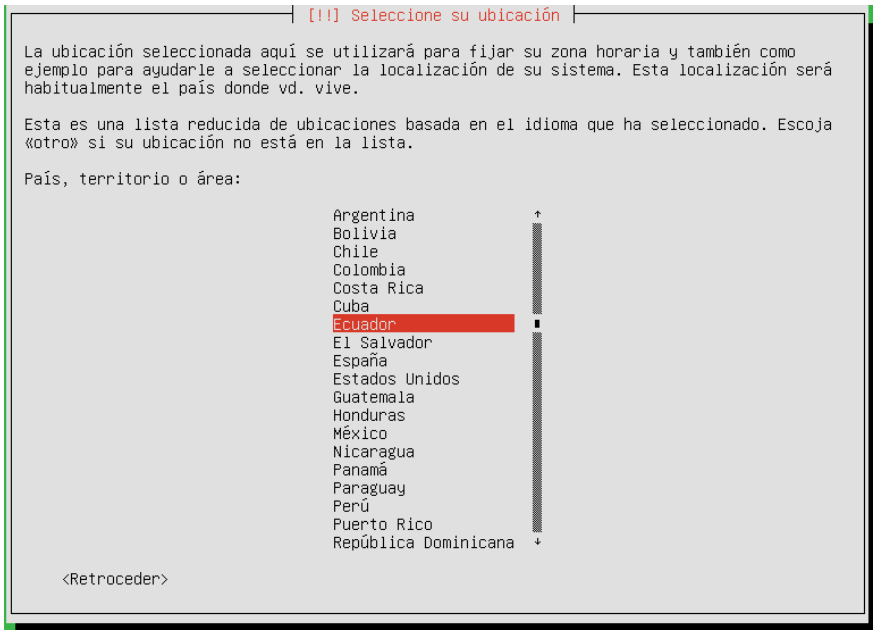
Realizado por: Diego Silva, 2019

Se elige el tipo de Instalación, para este caso particular MODO EXPERTO



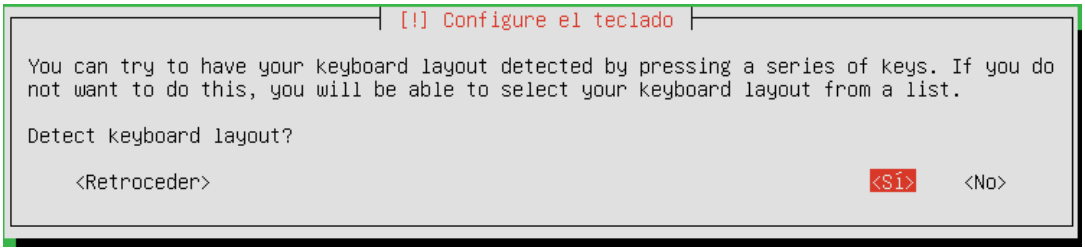
Realizado por: Diego Silva, 2019

Elección de Ubicación Geográfica



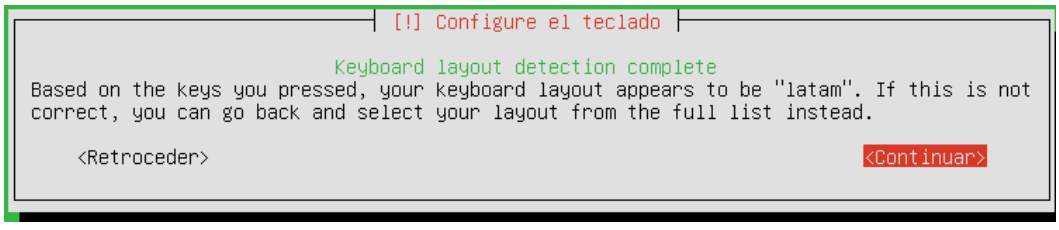
Realizado por: Diego Silva, 2019

Elegir si se desea realizar una detección del teclado



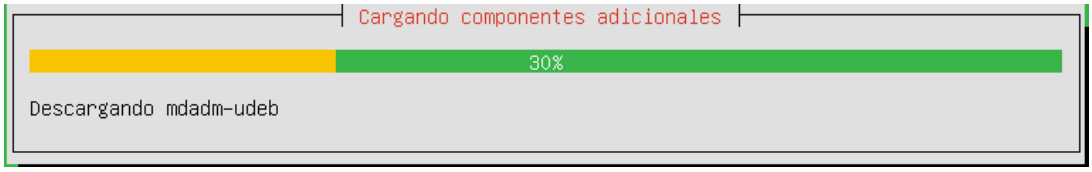
Realizado por: Diego Silva, 2019

Se identifica la disposición del teclado luego de una serie de preguntas y continuar



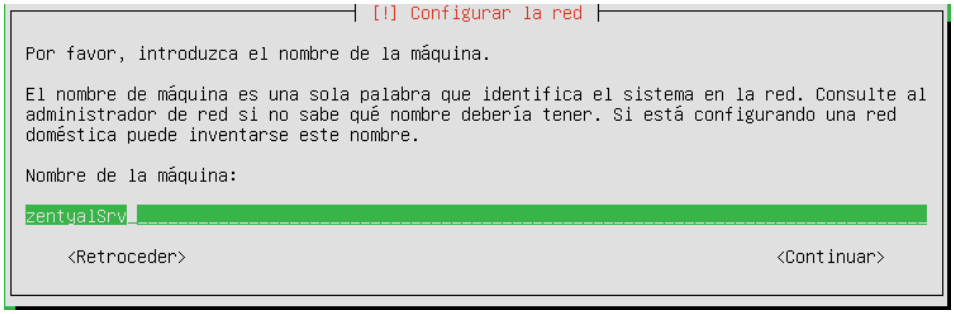
Realizado por: Diego Silva, 2019

Se inicia la carga de componentes necesarios adicionales para la instalación



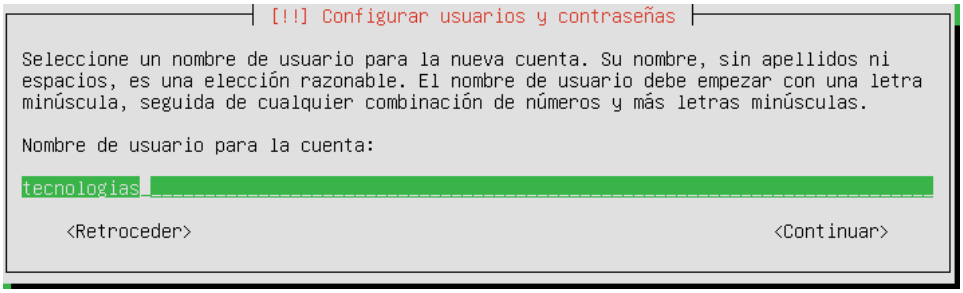
Realizado por: Diego Silva, 2019

Inicia la configuración de la red con la configuración del Nombre de la Máquina



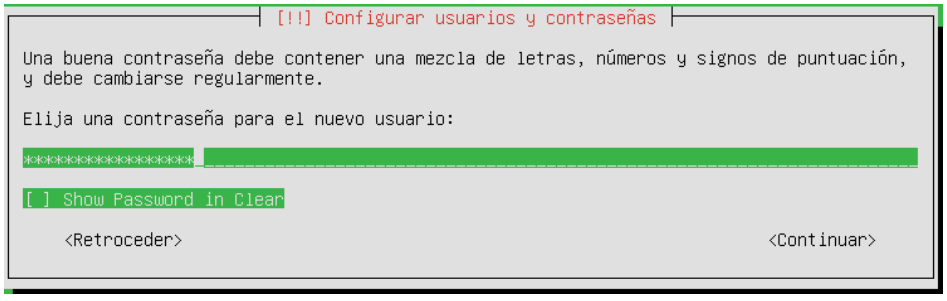
Realizado por: Diego Silva, 2019

Registrar el nombre de usuario del Sistema



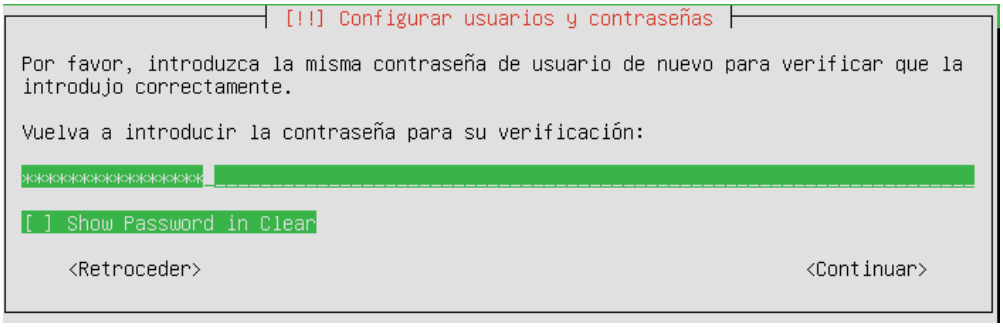
Realizado por: Diego Silva, 2019

Configurar Contraseña



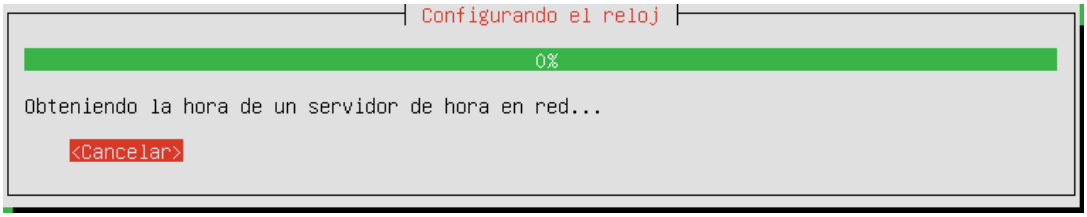
Realizado por: Diego Silva, 2019

Confirmar contraseña



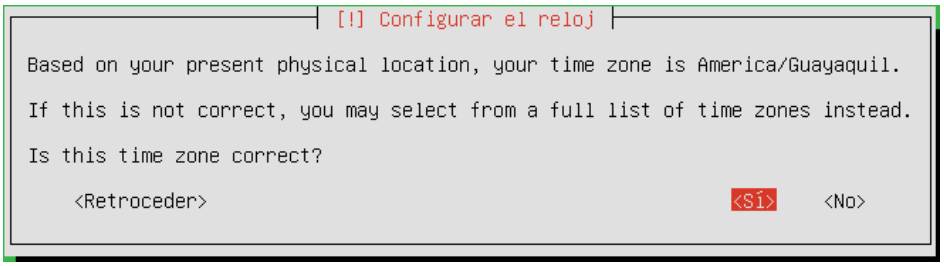
Realizado por: Diego Silva, 2019

El instalador inicia la búsqueda de configuración del reloj a través de la red



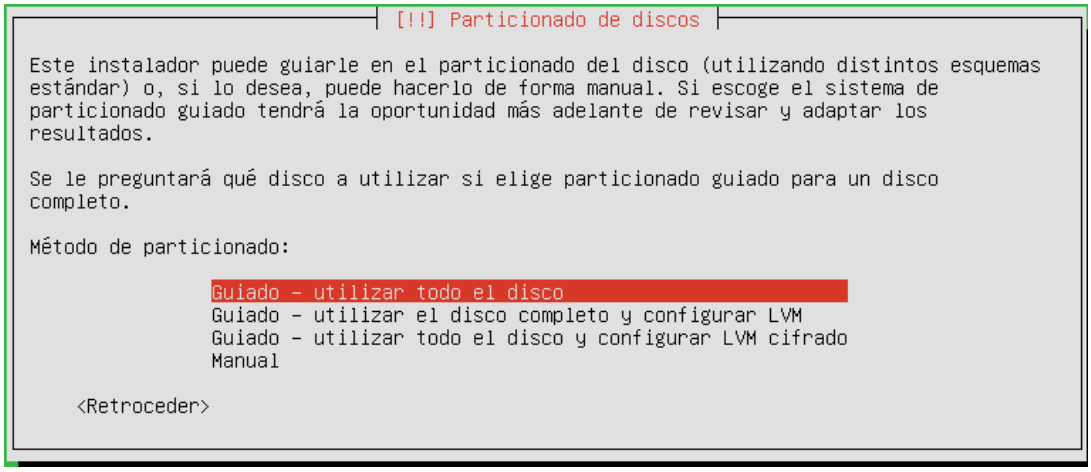
Realizado por: Diego Silva, 2019

La detección indica la ubicación del huso horario y se acepta



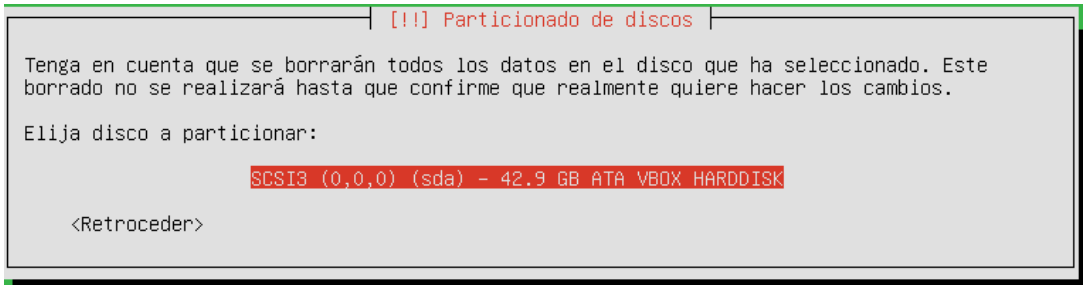
Realizado por: Diego Silva, 2019

Tomando en consideración que la instalación del sistema ocupará todo el espacio en disco porque se está instalando un equipo para este fin elegir particionado Guiado con la utilización de todo el disco.



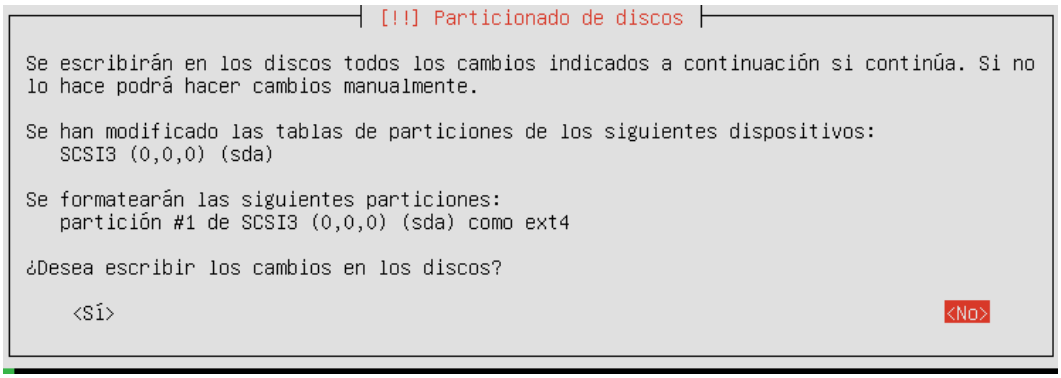
Realizado por: Diego Silva, 2019

Se procede a elegir el único disco disponible para aplicar el particionado



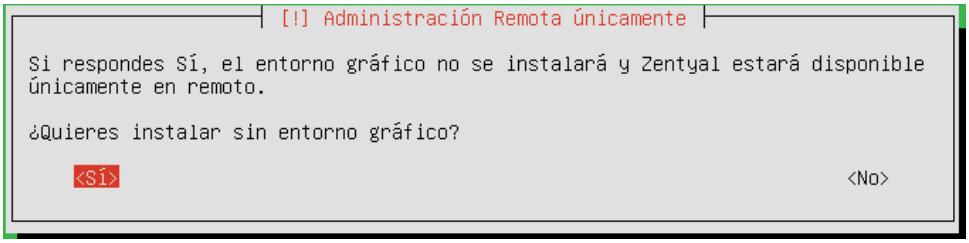
Realizado por: Diego Silva, 2019

Aceptar la advertencia de escritura en los discos, los cambios son irrevocables



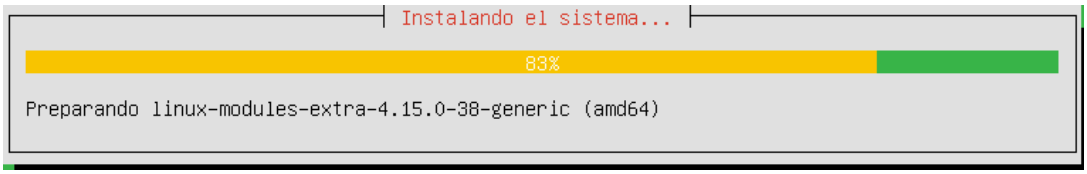
Realizado por: Diego Silva, 2019

Elegir administración remota, de este modo se minimiza el uso de recursos de una interfaz gráfica tanto de procesador como de memoria



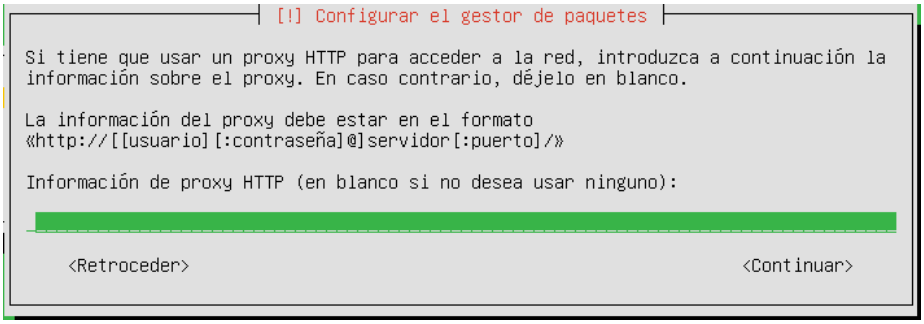
Realizado por: Diego Silva, 2019

Se inicia la instalación del sistema y la copia de los archivos al disco duro



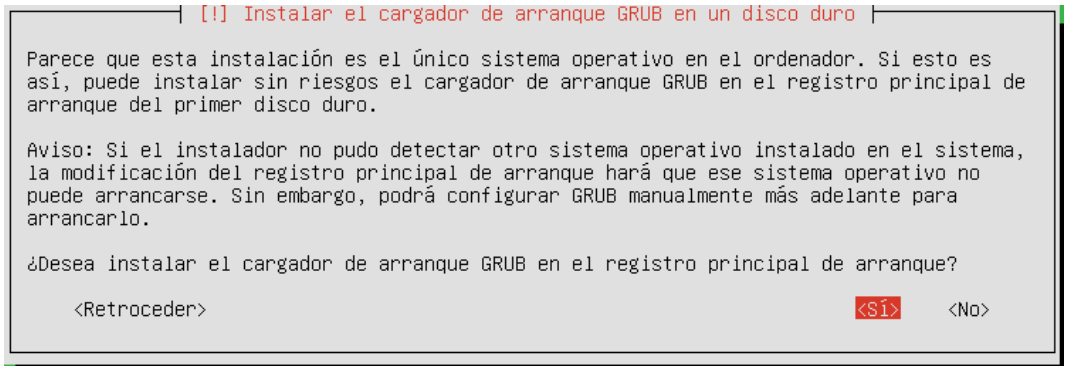
Realizado por: Diego Silva, 2019

En caso se requiera una conexión a través de un proxy, se debe establecer



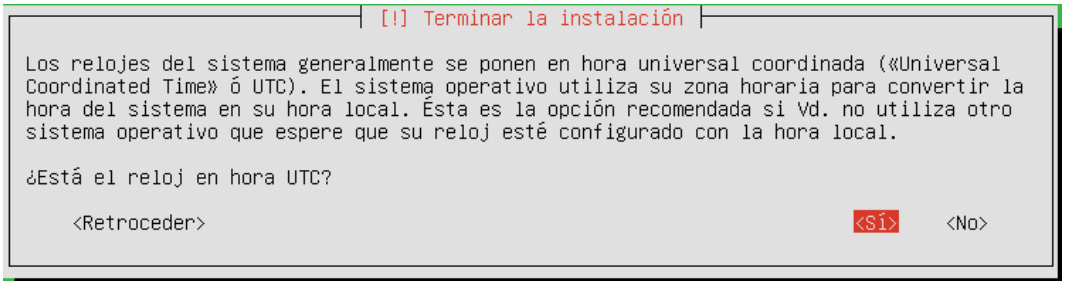
Realizado por: Diego Silva, 2019

Aceptar la instalación del GRUB en el registro principal de arranque



Realizado por: Diego Silva, 2019

Aceptar la configuración del reloj en hora UTC

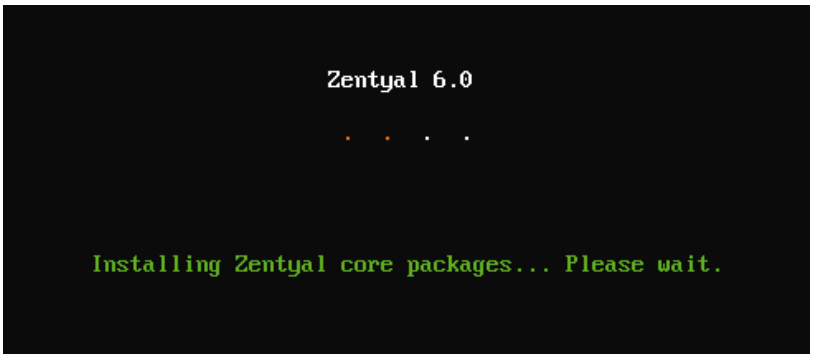


Realizado por: Diego Silva, 2019

Aceptar la confirmación de terminación de configuración

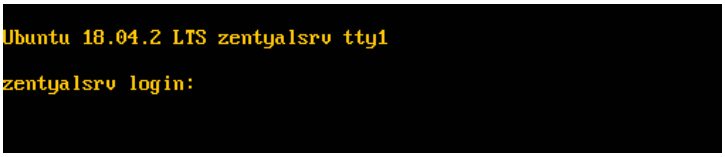
Realizado por: Diego Silva, 2019

Primer Inicio del servidor Zentyal



Realizado por: Diego Silva, 2019

Una vez iniciado el sistema se puede apreciar la versión sobre la cual está instalado el servidor y el logueo



Realizado por: Diego Silva, 2019

Después de acceder con las credenciales registradas en la instalación, se aprecia información importante para la administración del servidor

```
zentyalsrv login: tecnologias
Password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch



You can access the Zentyal Web Interface at:

 * https://your_server_ip:8443



Pueden actualizarse 8 paquetes.
3 actualizaciones son de seguridad.

*** Es necesario reiniciar el sistema ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

tecnologias@zentyalsrv:~$ _
```

Realizado por: Diego Silva, 2019

Configuración inicial posterior a la instalación. Se accede a través de un navegador web a mediante la ip configurada en la instalación y el siguiente puerto 192.168.125.1:8443. Se accede a la interfaz del Servidor Zentyal y solicita las credenciales de acceso.

Realizado por: Diego Silva, 2019

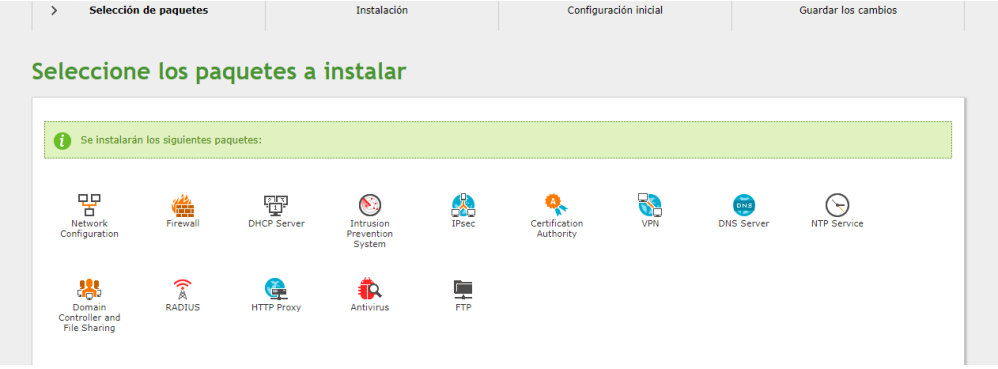
Después de haber iniciado sesión, aparece la pantalla que indica la Configuración Inicial

Realizado por: Diego Silva, 2019

Se debe elegir los paquetes que se van a instalar, para el caso de estudio son necesarios los servicios de: DNS(Domain Name System), DHCP(Dynamic Host Configuration Protocol), Firewall, Antivirus, Proxy, FTP(File Transfer Protocol), IPsec(Internet Protocol Security), IPS (Intrussion Prevention System), los mismos que serán configurados posteriormente.

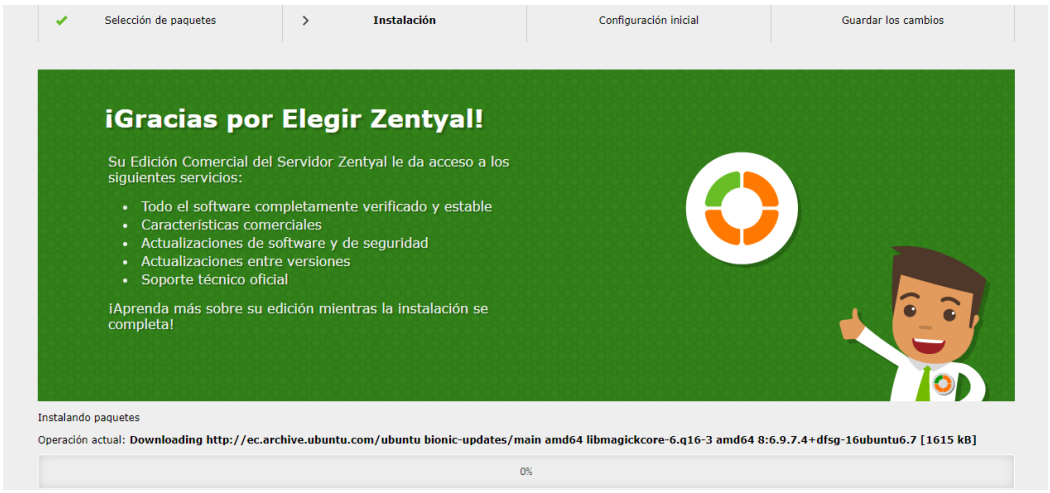
Realizado por: Diego Silva, 2019

Se muestra el resumen de los paquetes a instalar



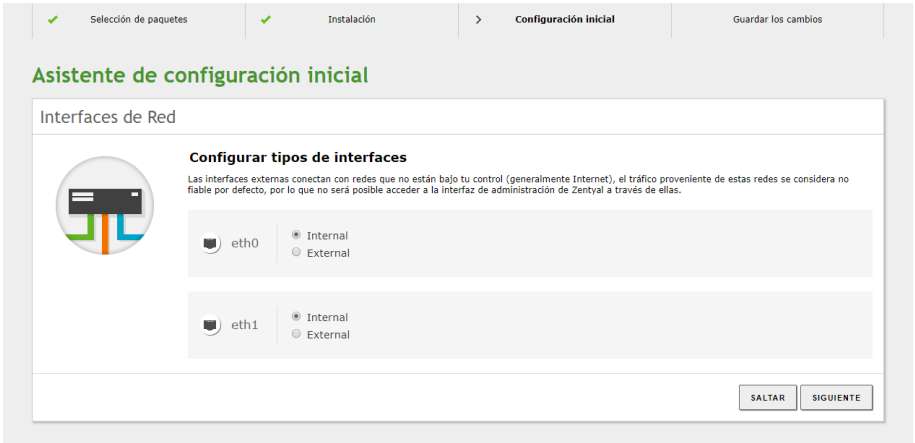
Realizado por: Diego Silva, 2019

Se muestra la descarga e instalación de paquetes necesarios y actualizados



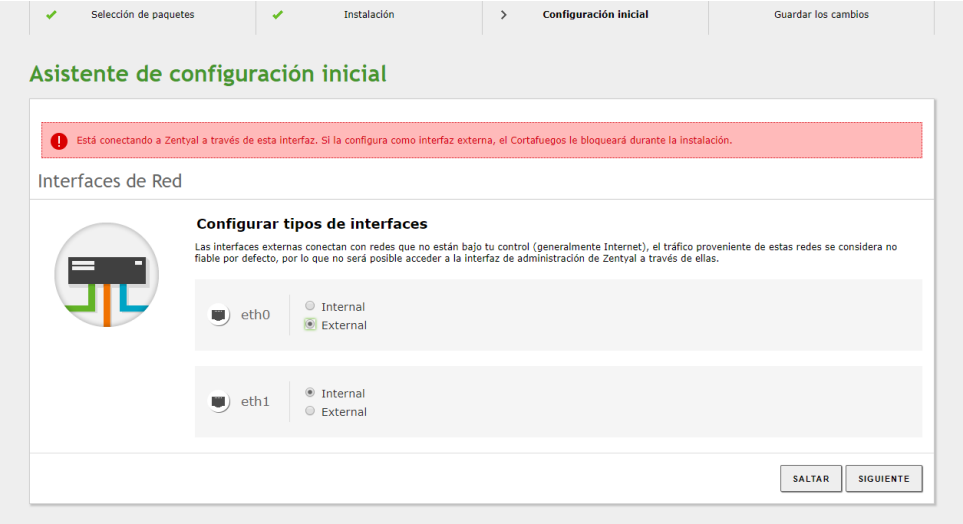
Realizado por: Diego Silva, 2019

Una vez concluido la descarga e instalación aparece la ventana de configuración inicial de red



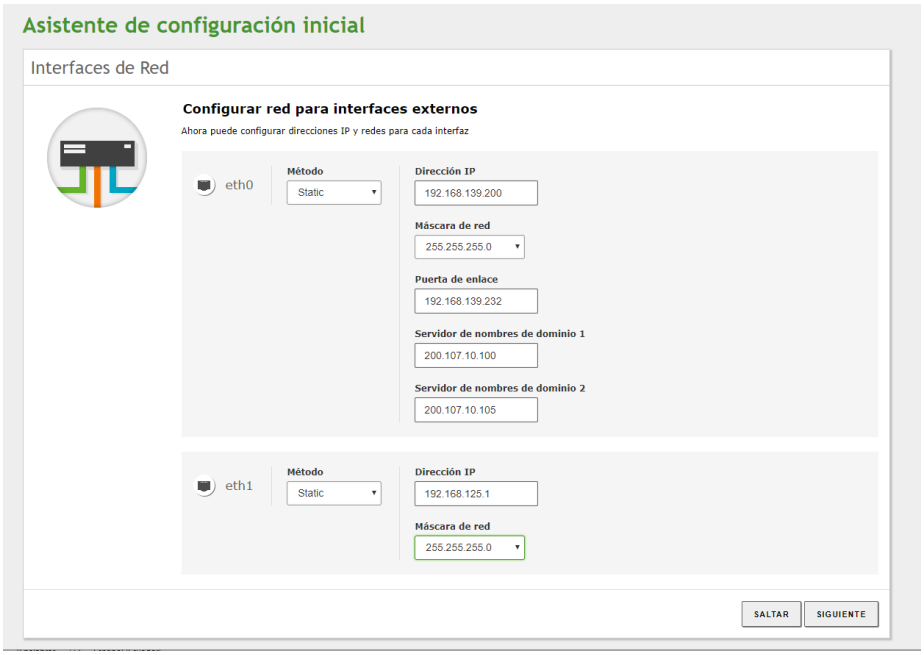
Realizado por: Diego Silva, 2019

Se elige la interfaz que se va a conectar a internet y la interfaz que se conecta a la red interna; al realizar esto se aplican automáticamente configuraciones predeterminadas de red para establecer un primer nivel de seguridad en la red. Se advierte que la interfaz configurada como externa no permitirá conexiones para configuración del servidor.



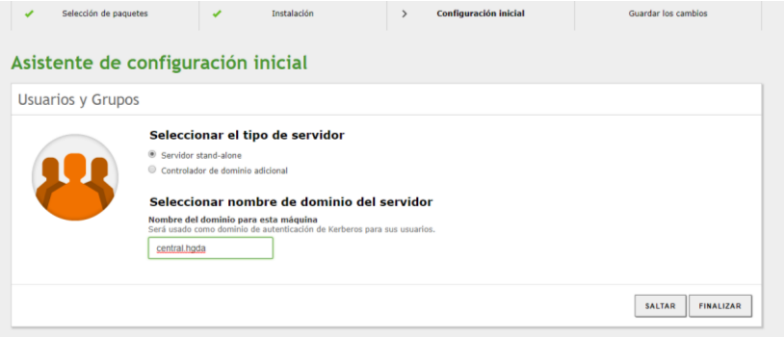
Realizado por: Diego Silva, 2019

Posteriormente se procede a configurar las direcciones IP que serán utilizadas en cada interfaz de red



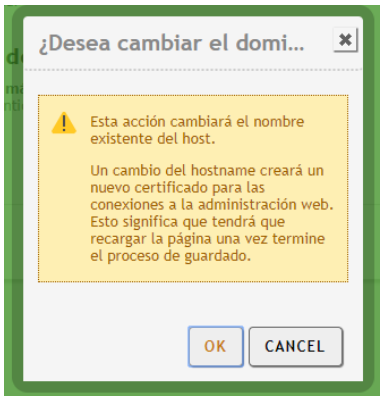
Realizado por: Diego Silva, 2019

Se determina el nombre del dominio y se indica si va a trabajar como servidor de dominio principal o adicional.



Realizado por: Diego Silva, 2019

Al aceptar los cambios se indica una advertencia de los cambios a ser aplicados por el cambio de nombre de Dominio.

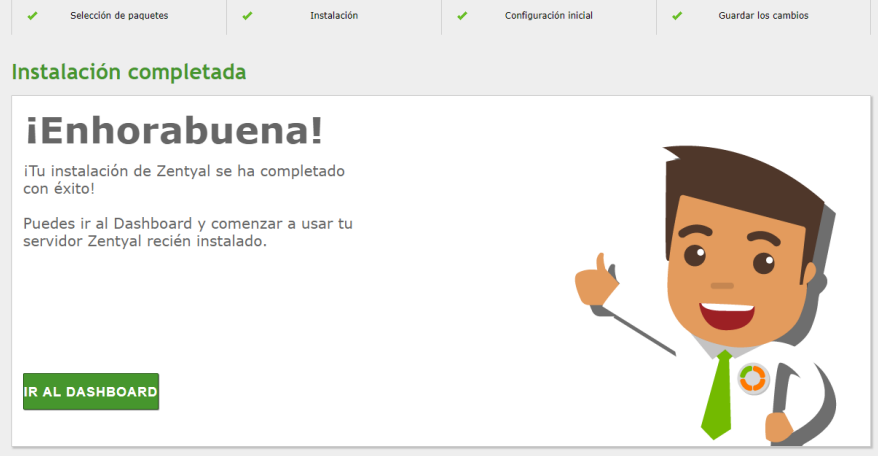


Realizado por: Diego Silva, 2019

Al finalizar la configuración inicial se proceden a aplicar los cambios requeridos en el sistema

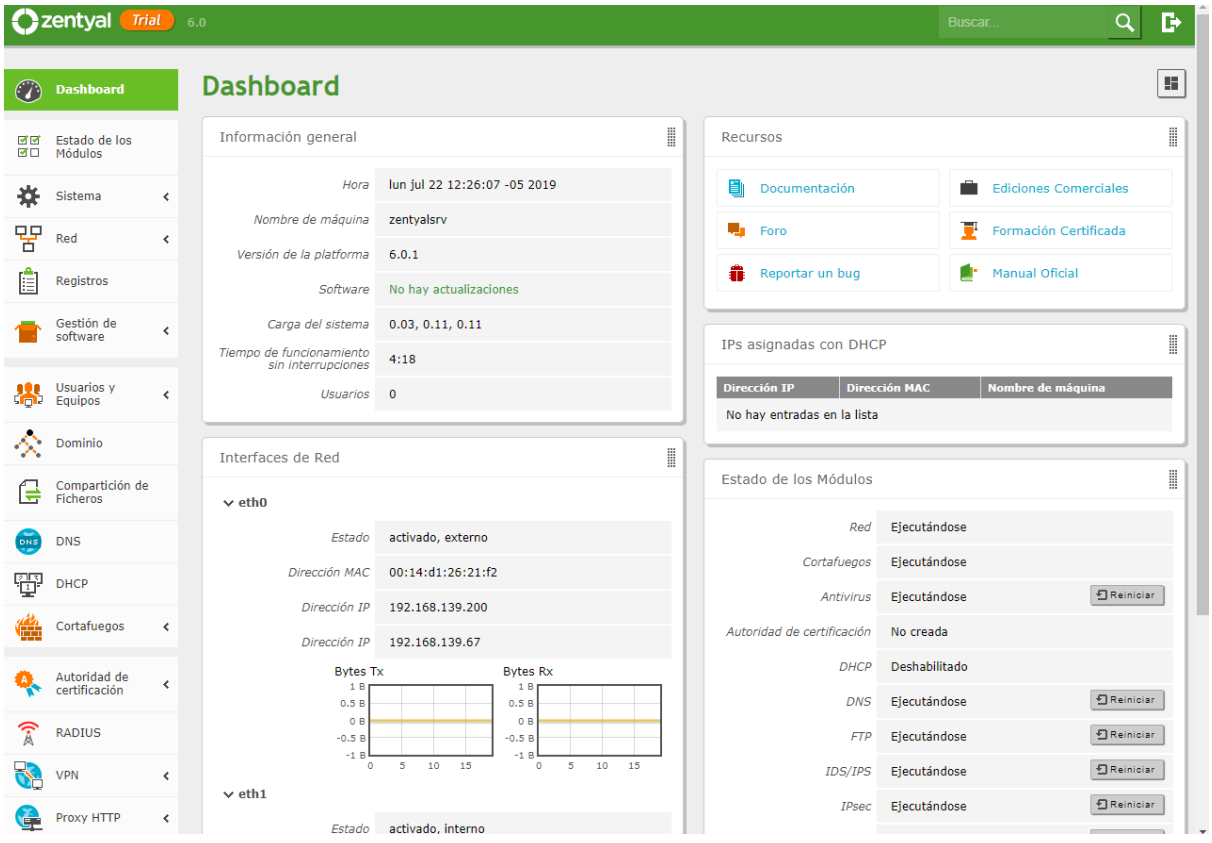
Realizado por: Diego Silva, 2019

Una vez aplicados los cambios, se muestra la confirmación de instalación exitosa.



Realizado por: Diego Silva, 2019

Una vez concluido el proceso se puede acceder al Dashboard que muestra un resumen del funcionamiento del servidor Zentyal.



Realizado por: Diego Silva, 2019

CONFIGURACIÓN DE FIREWALL ZENTYAL

Zentyal actúa como cortafuegos entre la red interna y el internet. La interfaz de red conectada al router del proveedor ISP, se debe marcar como externa; de esta manera se aplican ciertas políticas por defecto, como es denegar todo intento de conexión hacia la interfaz externa. Las conexiones internas se encuentran denegadas a excepción de los servicios ya definidos y configurados, cada servicio añade su propia excepción pero puede ser modificada en cualquier momento por el administrador del sistema.

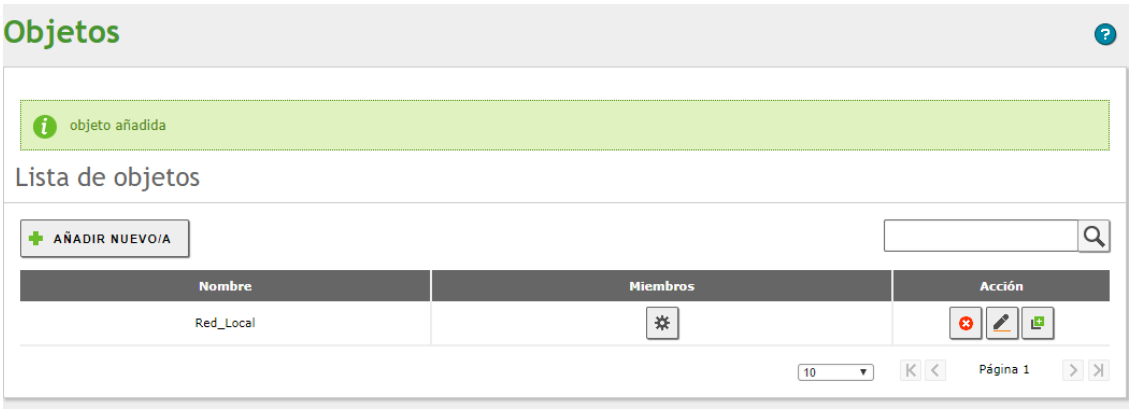
Realizado por: Diego Silva, 2019

Objetos de red

El Servidor UTM, implementa el tipo de administración mediante el uso de objetos de red, los mismos que deben ser definidos para ser utilizados más adelante en la configuración de los servicios tomando al objeto y concediendo permisos o eligiendo el comportamiento del mismo.

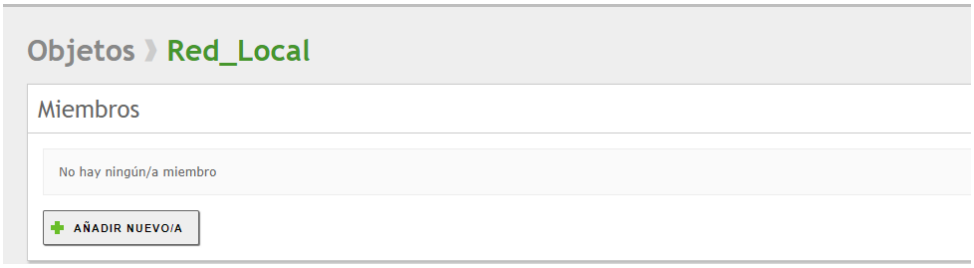
Realizado por: Diego Silva, 2019

Después de haber creado el nuevo objeto, se despliega la lista de objetos existentes; cada objeto tiene la opción de agregar miembros y de ejecutar las acciones de eliminar, actualizar o clonar un objeto.



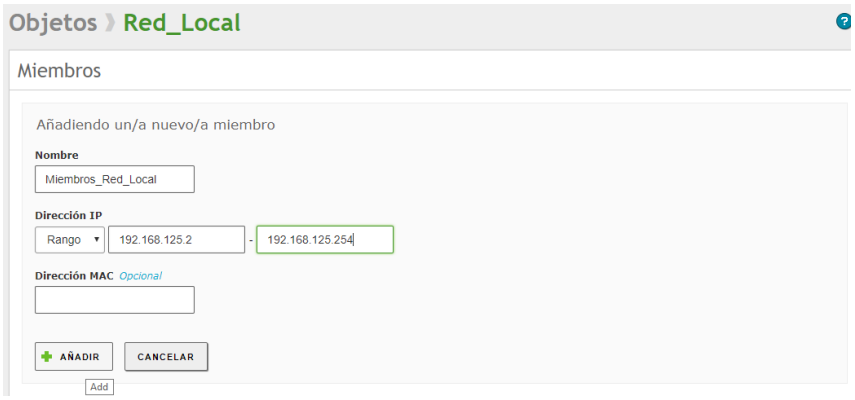
Realizado por: Diego Silva, 2019

Al dar clic en el botón de configuración de miembros, se despliega la lista de miembros de este objeto



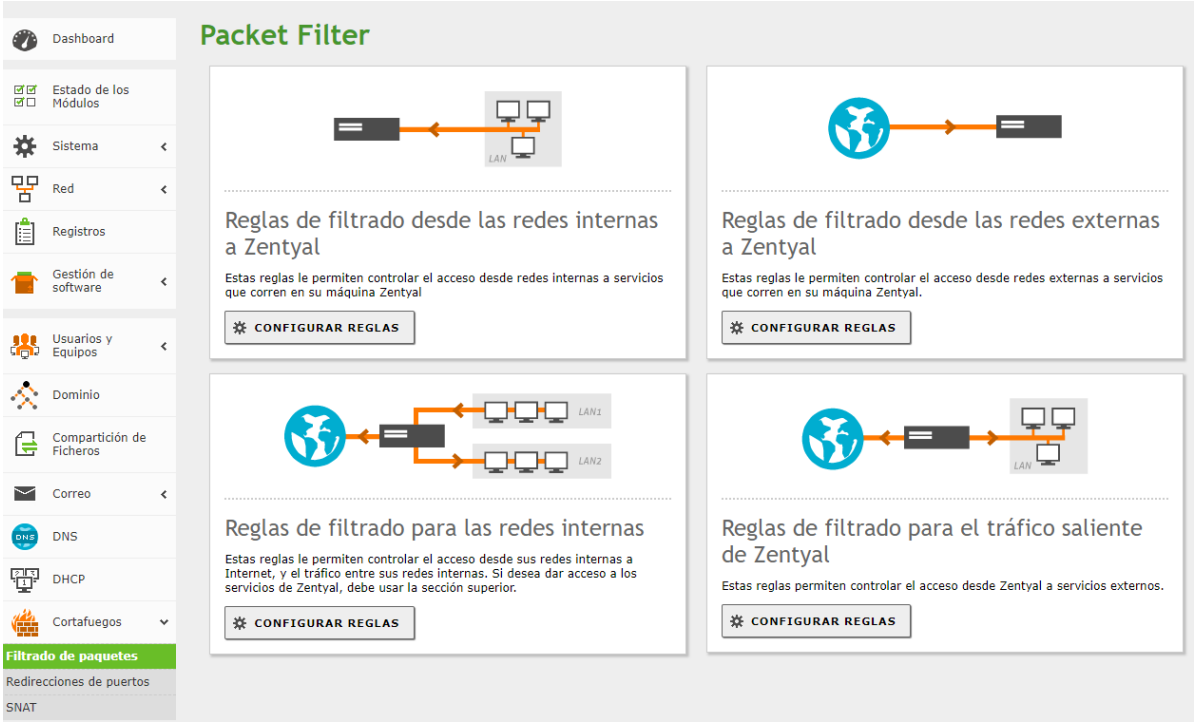
Realizado por: Diego Silva, 2019

Dar clic en añadir nuevo y definir el nombre del rango de miembros que se está creando.



Realizado por: Diego Silva, 2019

En el menú de cortafuegos se encuentran los 4 tipos de filtrado de paquetes que controla Zentyal: desde las redes internas, desde las redes externas, para las redes internas, para el tráfico saliente de Zentyal



Realizado por: Diego Silva, 2019

Verificar en el primer módulo de configuración los servicios a los cuáles pueden acceder los miembros de la red local al Servidor UTM.

Realizado por: Diego Silva, 2019

El acceso desde redes externas esta denegado por completo.

Realizado por: Diego Silva, 2019

La configuración del tráfico de las redes internas permanece abierta, posteriormente se verificará si es necesario limitarlo

Realizado por: Diego Silva, 2019

El tráfico saliente de Zentyal, está abierto, para una libre navegación y conexión a servicios requeridos

Realizado por: Diego Silva, 2019

Configuración de Servidor Proxy

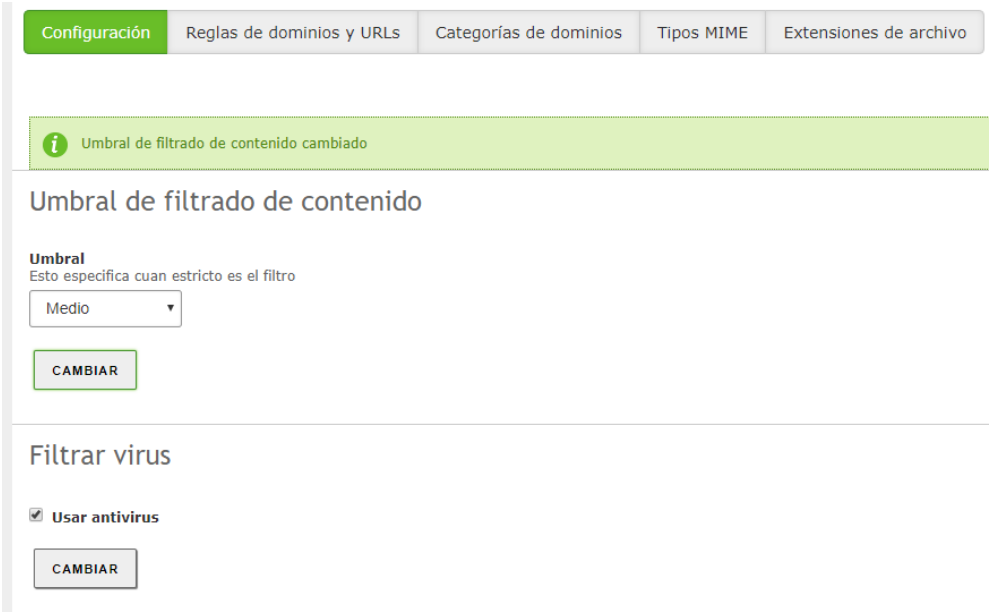
En el menú de la parte izquierda, elegir Proxy, determinar el puerto 3128 y habilitar como Proxy Transparente, establecer el tamaño de la memoria cache en 100 MB que se considera el almacenamiento suficiente para las páginas habitualmente accedidas por los usuarios como son: registro de atenciones médicas, exámenes de laboratorio, documentos en línea, sistema de agendamiento, correo electrónico, las mismas que no demandan mayor almacenamiento por su contenido mínimo en multimedia.

Realizado por: Diego Silva, 2019

Añadir un perfil de filtrado con el nombre Todos_los_Usuarios

Realizado por: Diego Silva, 2019

Dar clic en configuración para establecer los permisos del perfil de filtrado. Se muestra la primera pestaña, establecer el umbral en Medio y activar la casilla de Usar Antivirus, el módulo de antivirus debe estar activo.



Realizado por: Diego Silva, 2019

En la siguiente pestaña de Reglas de dominios y URLs, agregar las excepciones de los sitios a los cuales se va a denegar el acceso. Elegir la opción *Bloquear tráfico HTTPS por dominio.*

Realizado por: Diego Silva, 2019

Descargar de la siguiente dirección http://www.shallalist.de/Downloads/shallalist.tar.gz la lista para cargarla y poder discriminar por categorías de dominios y administrar de mejor manera el contenido accesible. Cargar el archivo en la opción *Listas por categorías*

Realizado por: Diego Silva, 2019

Volver a los perfiles de filtrado de todos los usuarios, ahora es visible un listado de categorías, y elegir el bloqueo básico de anuncios, sitios pornográficos, redes sociales, radio y televisión por web.

Realizado por: Diego Silva, 2019

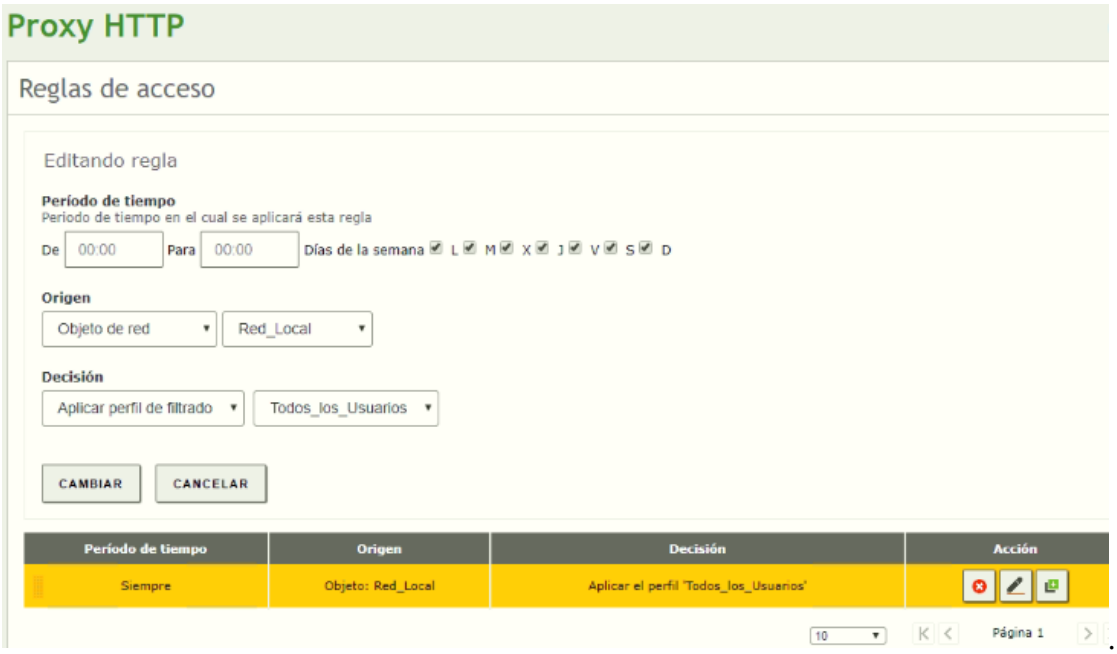
La configuración en cuanto a los archivos MIME se conserva activada para todos los tipos, tomando en cuenta que la investigación busca determinar y disminuir las vulnerabilidades de red con todo el tráfico entrante y saliente.

Realizado por: Diego Silva, 2019

La última pestaña a configurar en el perfil es la de *Extensiones de archivo.* Es necesario evitar la descarga de ciertos tipos de archivo que pueden afectar con virus a los equipos de la red. Desactivar extensiones: adp, bat, bin.

Realizado por: Diego Silva, 2019

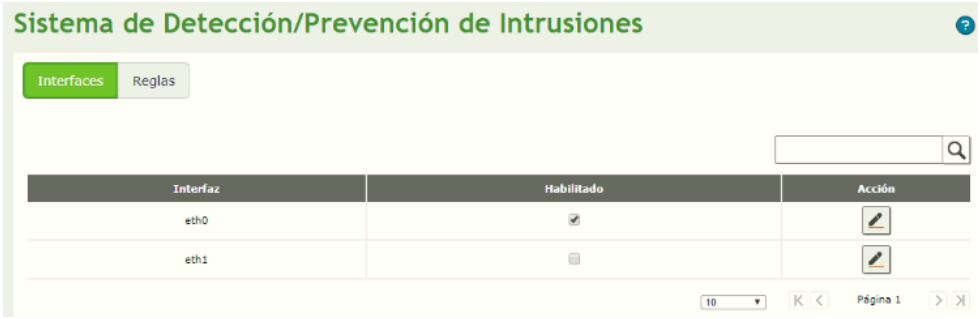
La definición de reglas de acceso generales hasta poder establecer las políticas en la propuesta, son de libre acceso para determinar los valores de los indicadores establecidos. Se permite sin restricción de horario al objeto Red_Local y se le asigna el perfil de filtrado Todos_los_Usuarios



Realizado por: Diego Silva, 2019

Sistema de Detección / Prevención de Intrusiones

En el menú de la configuración IDS / IPS, elegir el interfaz que va a ser sujeto de aplicación del sistema de detección y prevención de Intrusiones. Para este caso aplicado es la interfaz eth0.



Realizado por: Diego Silva, 2019

Determinar las reglas a aplicarse, se puede registrar el suceso o denegar. Todas las actividades serán registradas y se bloquearán el acceso: ddos, dns, exploit, p2p, smtp, telnet, virus, web-attacks.

Realizado por: Diego Silva, 2019

ANEXO B: IMPLEMENTACIÓN DE NEXT GENERATION FIREWALL (NGFW)

Para restablecer a los firewalls como base universal de la seguridad en redes, los NGFW buscan solucionar los problemas de las conexiones desde el núcleo. Clasifican el tráfico según el tipo de aplicación y permiten el control de esta incluyendo la Web 2.0, Enterprise 2.0 y aplicaciones legacy. El firewall de siguiente generación debe tener la capacidad de: identificar aplicaciones independientemente del puerto, ver y controlar en base a políticas identificar usuarios y usar la identidad como atributo para el control de políticas, proporcionar en tiempo real protección contra las amenazas hasta la capa de aplicación, integrar el firewall con la prevención de intrusiones de red, admitir gran cantidad de datos con mínima degradación del rendimiento. (Miller, 2011)

NGFW HUAWEI USG6630

Dentro del entorno empresarial se encuentra instalado el Firewall de siguiente generación de marca Huawei modelo USG6300, el mismo que ofrece soluciones completas para la infraestructura de red mediana instalada. Las funciones de firewall, prevención de intrusiones, antivirus y prevención de perdida de datos permiten el manejo de un gran caudal de datos, su nombre se debe a que identifica más de 6300 aplicaciones, mediante el análisis del tráfico de servicio en 6 dimensiones; genera la aplicación de políticas de seguridad automáticamente. (Huawei Technologies Co., 2019)

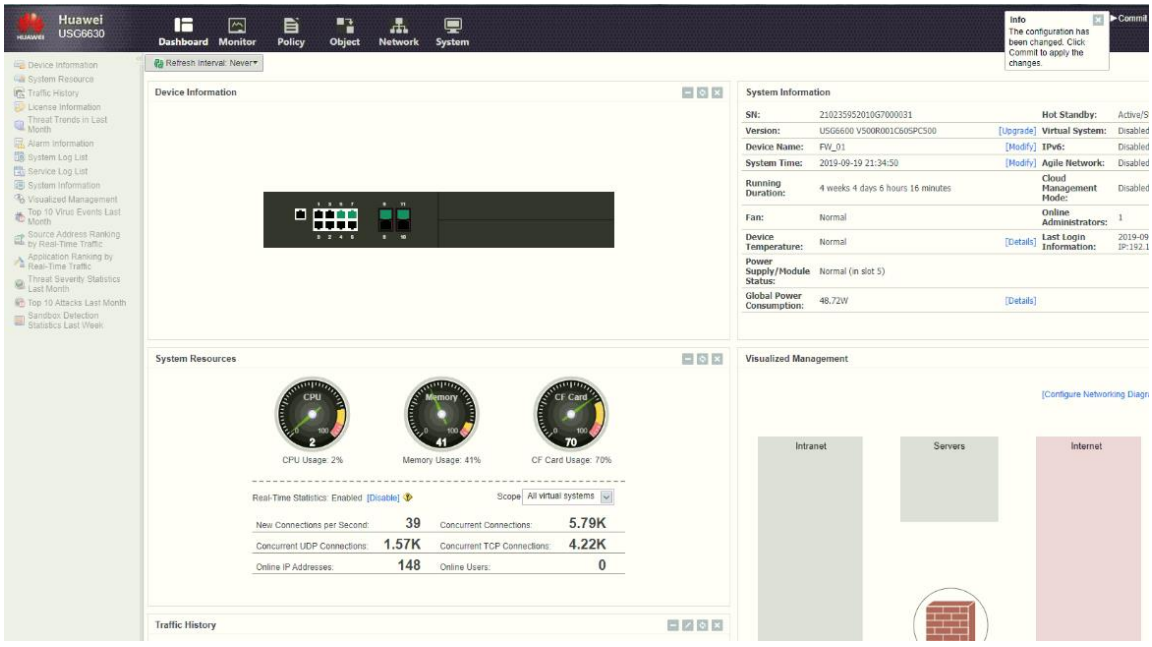
Fuente: (Huawei Technologies Co., 2019)

Este equipo se encuentra instalado en el Data Center del Hospital General Ambato y se requiere la configuración establecido para el entorno de pruebas.

Para obtener acceso al servidor digitar su dirección predefinida en el navegador y las credenciales de acceso.

Realizado por: Diego Silva, 2019

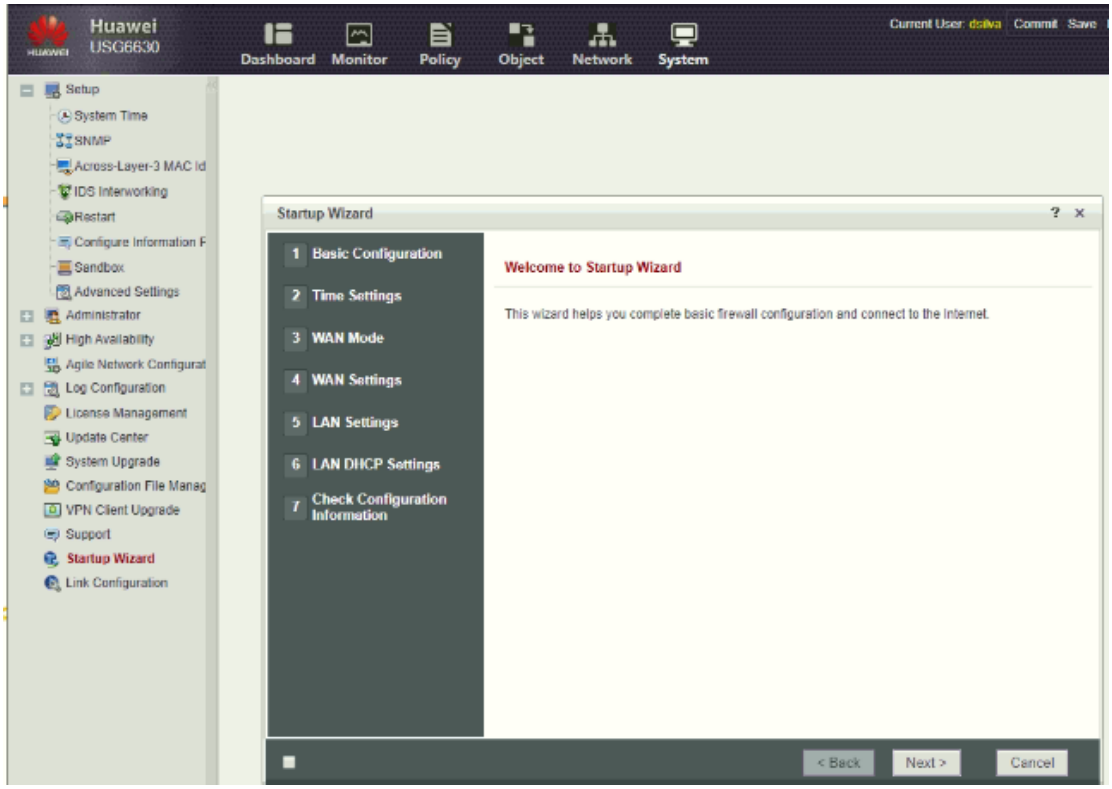
Al iniciar sesión se muestra el Dashboard del NGFW y muestra un resumen de la información más relevante del funcionamiento del firewall.



Realizado por: *Diego Silva, 2019*

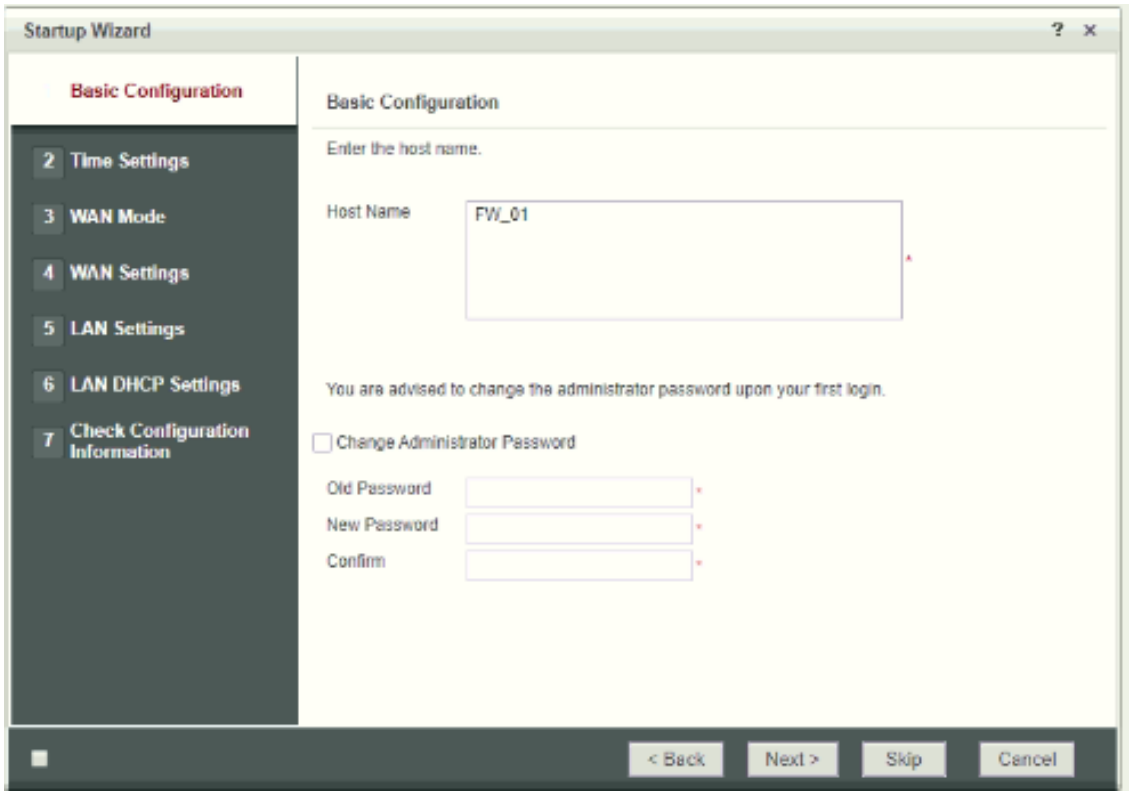
Configuración inicial, interfaces de red.

Iniciar al Asistente de Configuración desde el Menú *System*, *Startup Wizard.*



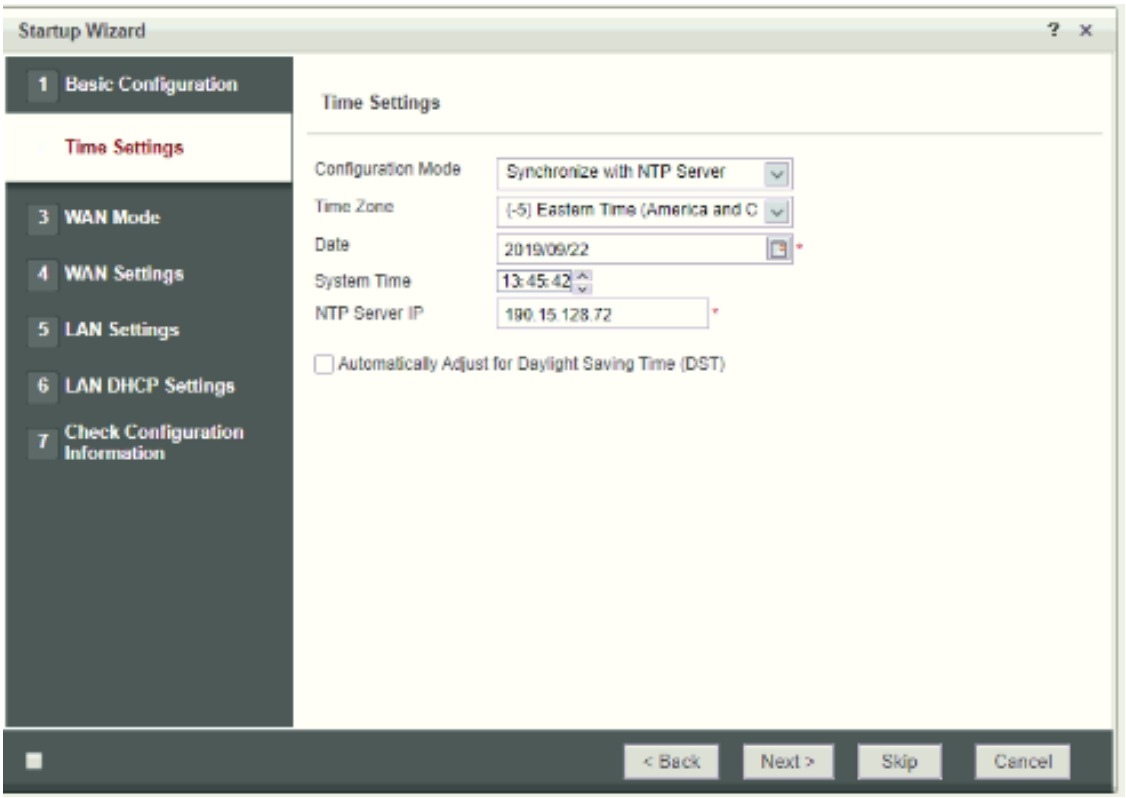
Realizado por: Diego Silva, 2019

En la siguiente pantalla, definir el nombre de host



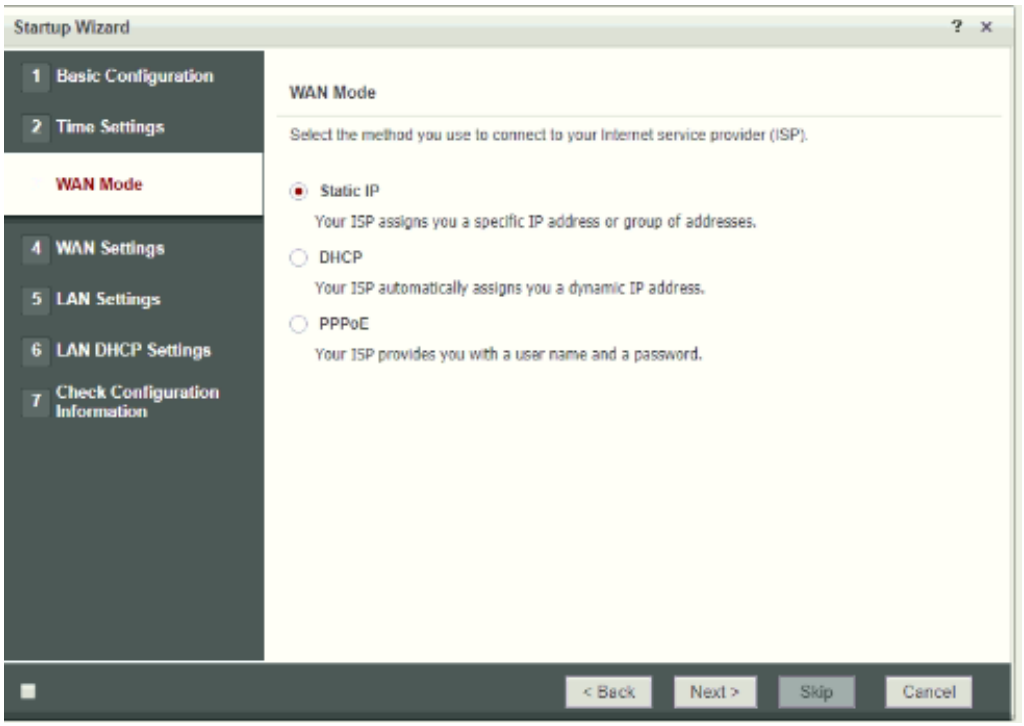
Realizado por: Diego Silva, 2019

Establecer la configuración de la hora



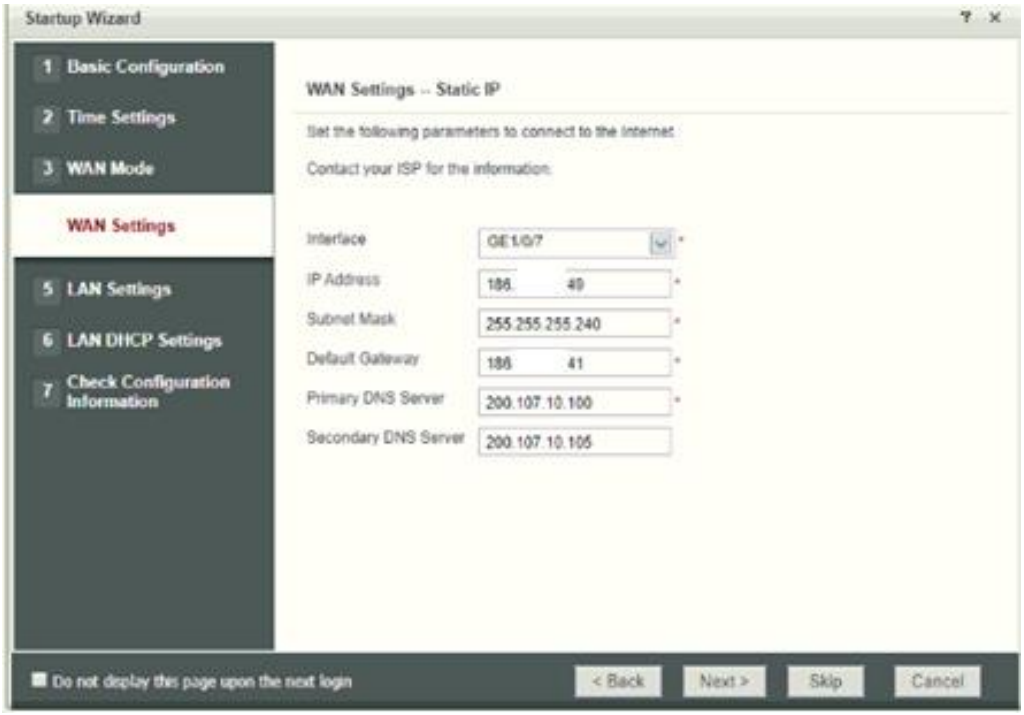
Realizado por: Diego Silva, 2019

Establecer el tipo de conexión que usará la interfaz WAN



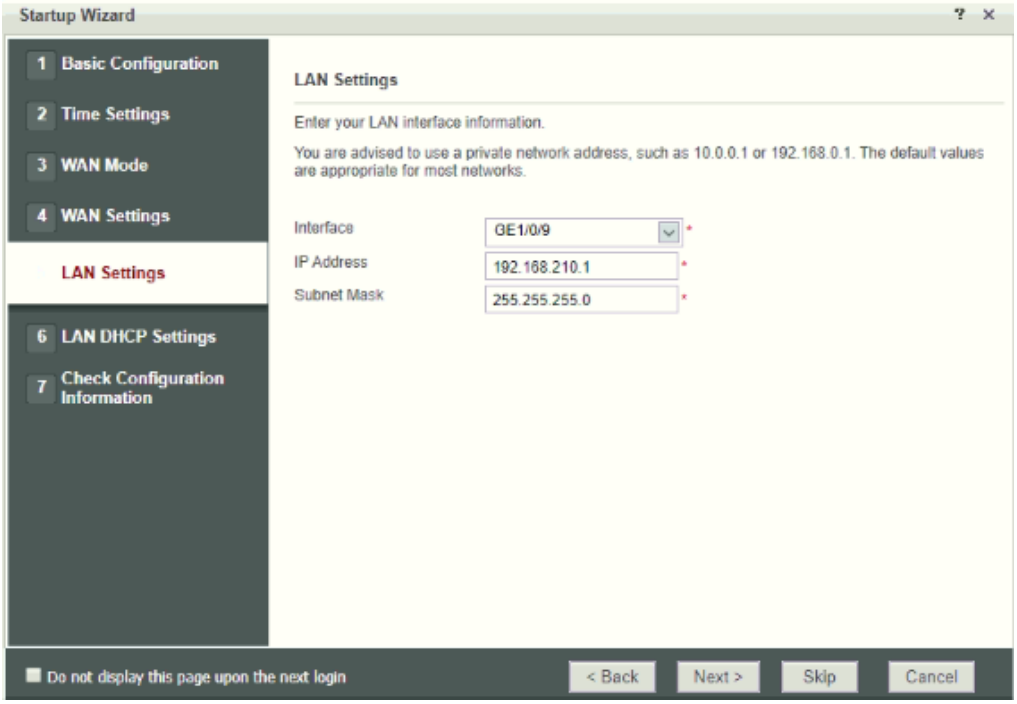
Realizado por: Diego Silva, 2019

Establecer la ip pública, máscara de red, puerta de enlace y servidores DNS del proveedor ISP.



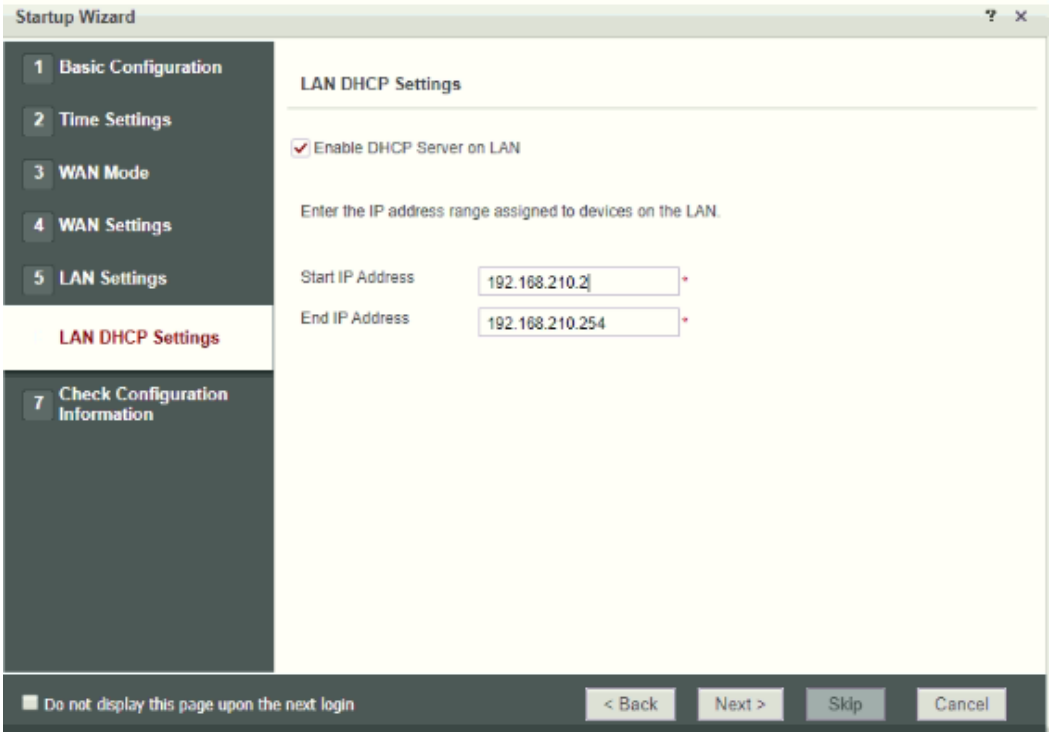
Realizado por: Diego Silva, 2019

Establecer la dirección de la Interfaz LAN, y la máscara.



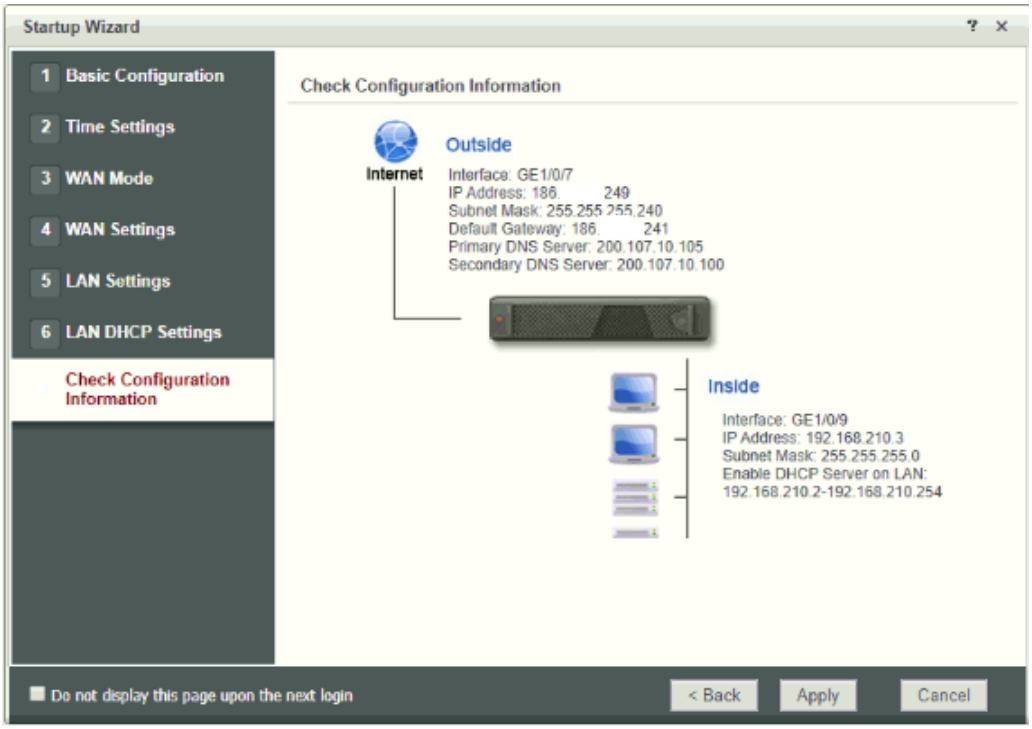
Realizado por: Diego Silva, 2019

Establecer la configuración de Direccionamiento Dinámico DHCP



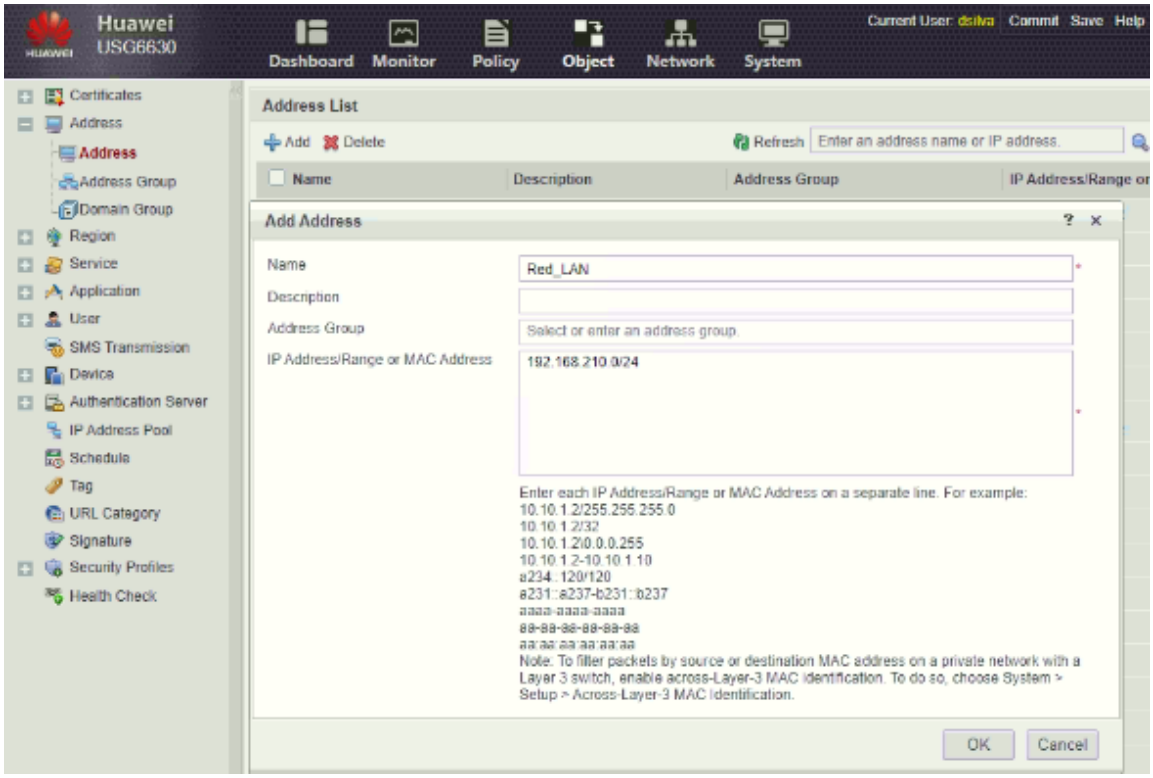
Realizado por: Diego Silva, 2019

En la pantalla final se muestra el resumen de la configuración de las interfaces de red, aplicar y guardar los cambios.



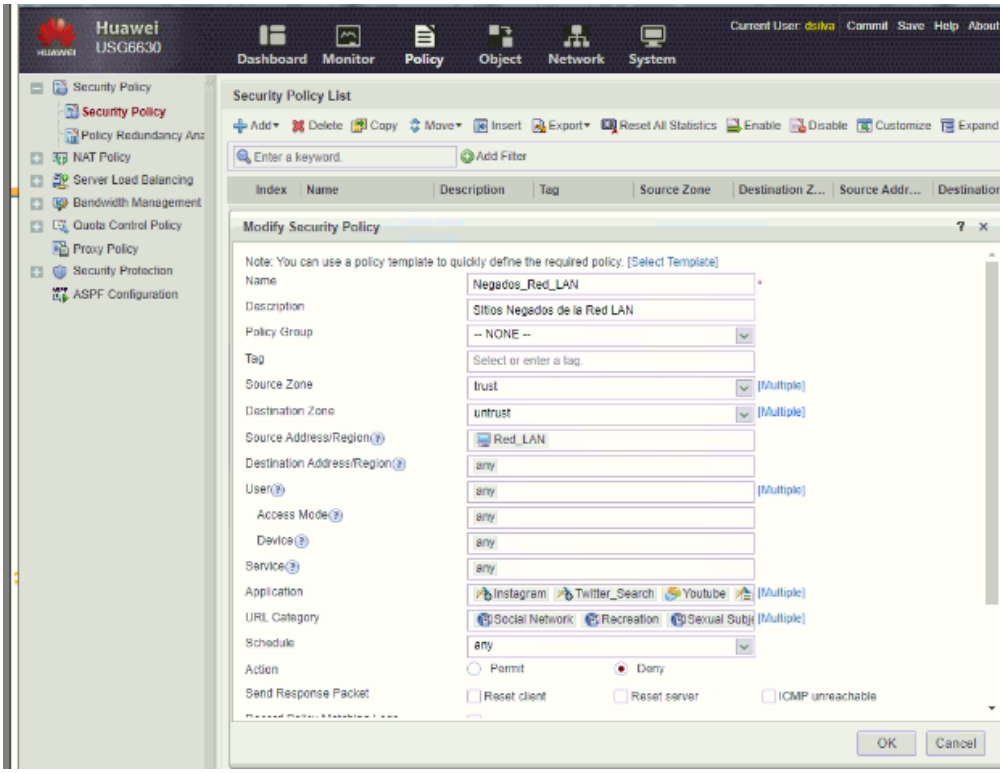
Realizado por: Diego Silva, 2019

En el menú *Object – Address – Address* Se procede con la creación del objeto de red con el nombre Red_LAN y se especifica la dirección de la red interna 192.168.210.0/24



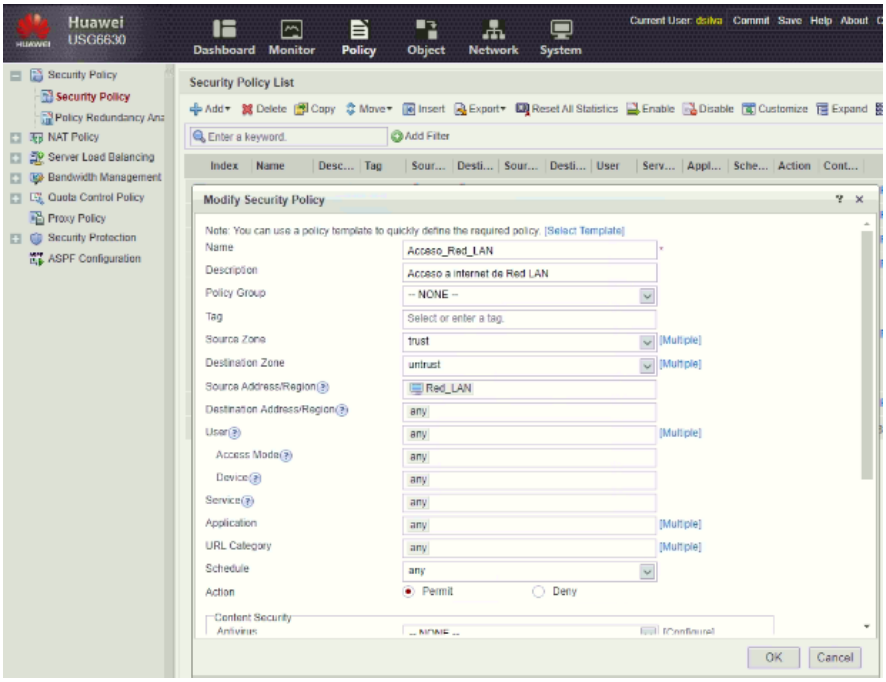
Realizado por: Diego Silva, 2019

En el menú *Policy – Security Policy*, se añade una nueva política con el nombre *Negados_Red_LAN*; la zona de origen es *trust*, zona de destino *untrust*, la región de origen se elige la *Red_LAN* hacia *cualquier* destino, al igual que usuario, modo de acceso, dispositivo y servicio. Un módulo importante es el filtrado por aplicación, se eligen las mismas configuraciones aplicadas en el servidor UTM como son: bloqueo de redes sociales, youtube, sitios pornográficos, streaming de audio y video, sitios de recreación y los mismos deben ser elegidos en las categorías URL. Es necesario recalcar que las políticas se aplican en el orden listadas.



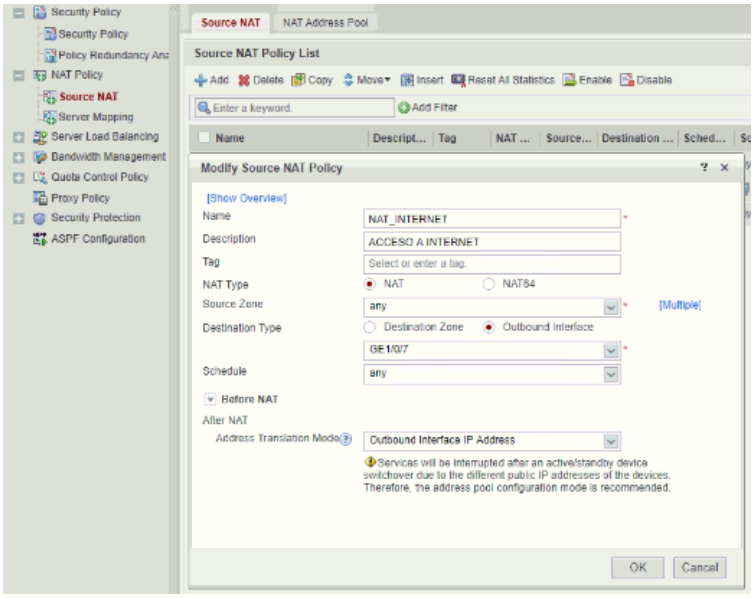
Realizado por: Diego Silva, 2019

Después de establecer los sitios y aplicaciones negadas, se procede con la creación de la política de acceso al resto de sitios de internet.



Realizado por: Diego Silva, 2019

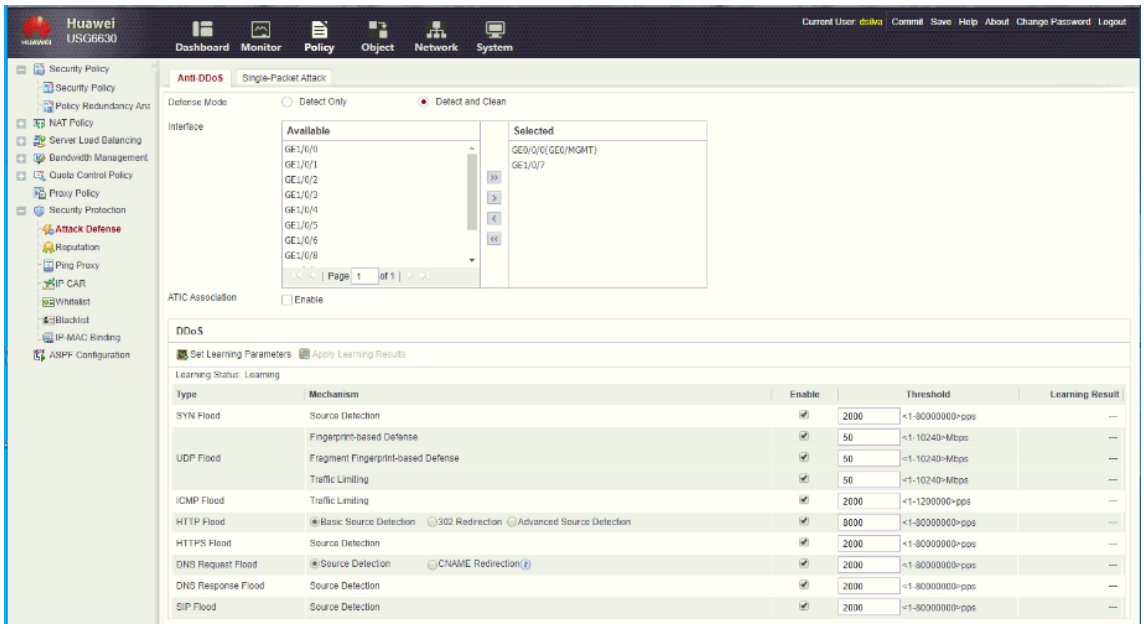
Se define la regla de NAT para establecer la salida enmascarada a Internet, es decir que todas las conexiones sean a través de la IP pública.



Realizado por: Diego Silva, 2019

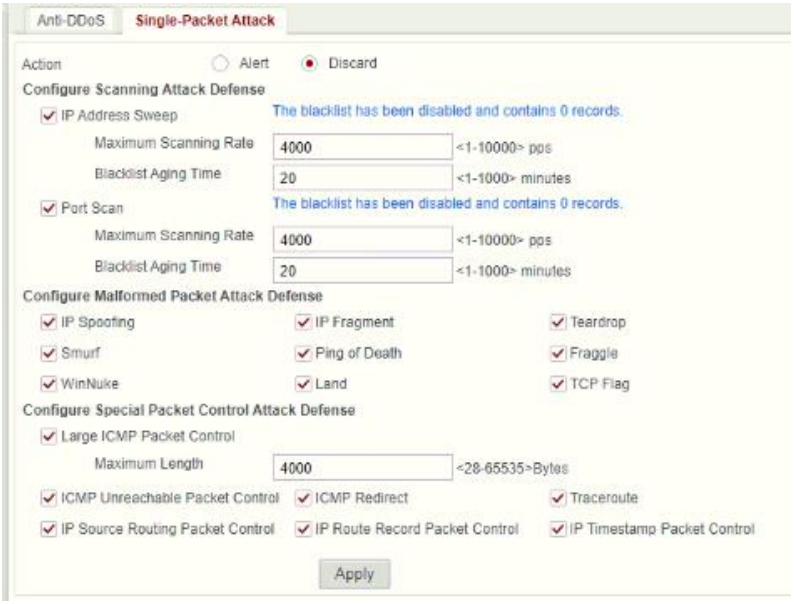
Sistema de Detección / Prevención de Intrusiones.

Para la configuración de este parámetro en el menú *Policies – Security Protection – Atack Defense.* Elegir en el modo de defensa *Detectar y Limpiar; a*gregar la interfaz GE1/0/7 que es la q se encuentra conectada a la WAN, establecer los parámetros de aprendizaje, y habilitar todas las reglas de aprendizaje.



Realizado por: Diego Silva, 2019

En la siguiente pestaña se muestra la configuración de ataques por paquetes únicos. Habilitar la acción descartar y habilitar las opciones existentes para protección de todos los tipos de ataques.



Realizado por: Diego Silva, 2019