PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITULACIÓN ESPECIAL

TEMA:

"ANÁLISIS DE TRÁFICO PARA LA INFRAESTRUCTURA DE LA RED DE LA EMPRESA PUBLICA MUNICIPAL DE TRANSPORTE TERRESTRE, TRÁNSITO Y SEGURIDAD VIAL EPM PORTOVIAL, PARA OFRECER UN MODELO CON CALIDAD DE SERVICIOS (QoS) "

Ing. Oscar Eduardo Salazar Salazar

Quito - 2016

AUTORÍA

Yo, Oscar Eduardo Salazar Salazar, portador de la cédula de ciudadanía No.1310113277, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Oscar Eduardo Salazar Salazar

Contenido

Tablas

Figuras

Resumen.

La globalización y el crecimiento tecnológico de los últimos años, han llevado para que las comunicaciones y la informática se encuentren cada vez más ligadas a través de la plataforma de comunicación basada en el protocolo IP, es así que hoy en día las TIC (Tecnologías de la Información y Comunicación) son una parte fundamental en todas las pequeñas y grandes empresas, y son donde convergen la informática y las comunicaciones.

Para el óptimo desempeño de una red de datos en cualquier organización es necesario contar con personal capacitado que disponga de herramientas y los conocimientos suficientes para realizar un completo análisis de ésta. El gran inconveniente es que en muchas ocasiones no se dispone de las herramientas necesarias, pues pueden llegar a ser costosas y en ocasiones difíciles de manejar.

En el presente proyecto se realiza el análisis de tráfico de la infraestructura de la red de la Empresa Pública Municipal de Transporte Terrestre, Tránsito y Seguridad Vial EPM Portovial ofreciendo un modelo con calidad de servicio (QoS), cuyo objetivo es optimizar el uso de la red.

La Calidad de Servicio (QoS) se traduce como la capacidad de una red para entregar un servicio específico a un tipo concreto de tráfico, el soporte de la QoS puede dar lugar a la reserva de un ancho de banda, a un tráfico con prioridades, a una prevención de la congestión.

La red de la Empresa Pública Municipal EPM Portovial, luego del pasado terremoto del 16 de Abril del 2016 que afectó gran parte de la Provincia de Manabí inclusive el Cantón

Portoviejo, la red de datos con el transcurso de este tiempo ha tenido demandas de sus usuarios y debido a las exigencias de éstos en solicitar un cierto tipo de Servicio, como Internet, Enlace de Datos con la Agencia Nacional de Tránsito ANT y VoIP (Voz sobre IP), ha llevado a la modernización y actualización de sus equipos conforme a los avances tecnológicos en esta materia como lo es las redes y la telecomunicaciones.

Como solución, se plantea la implementación de Calidad de Servicio (QoS), que priorice los paquetes de Internet, Enlaces de datos y VoIP (Voz sobre IP), para que no se pierda la calidad en la trasmisión de Internet y a su vez siga la transmisión de datos y VoIP por el canal de comunicación sin que exista perdidas tampoco en estas transmisiones.

Abstract.

Globalization and technological growth in recent years, have led to communications and computing are increasingly linked through the communication platform based on IP protocol, so is that nowadays the ICT (Information and Communication) are a fundamental part in all small and large businesses, and are where converging computing and communications.

For optimal network performance data in any organization it is necessary to have trained personnel with sufficient knowledge and tools to perform a complete analysis of it. The big drawback is that often do not have the necessary tools, it can become expensive and sometimes difficult to handle.

In this project the analysis of traffic on the network infrastructure of the Municipal Public Enterprise Land Transportation, Traffic and safety is done Vial EPM Portovial offering a model with quality of service (QoS), which aims to optimize the use of the network.

Quality of Service (QoS) translates to the ability of a network to deliver a specific service to a specific type of traffic, support for QoS can lead to reserve bandwidth to a traffic priorities, to prevent congestion.

The network of the Public Enterprise Municipal EPM Portovial, after the last earthquake of April 16, 2016 that affected much of the province of Manabí including the Canton Portoviejo, network data over this time has demands of its users and because of the

demands of these to request a certain type of service, such as Internet, data Link with the National Transit Agency ANT and VoIP (Voice over IP), it has led to the modernization and upgrading its equipment as advances technology in this area as it is and telecommunications networks.

As a solution, the implementation of Quality of Service (QoS), which prioritizes Internet packages, Data Links and VoIP (Voice over IP), is proposed, so that the quality of Internet transmission is not lost and in turn follow the Transmission of data and VoIp by the communication channel without there being any losses in these transmissions.

1. Introducción.

En los últimos años, las Telecomunicaciones, en especial las tecnologías vinculadas a la Internet, han alcanzado un crecimiento y auge mayor al que se hubiese podido esperar en sus principios.

Con la globalización gradual de los procesos, el despliegue tecnológico de los últimos años, el crecimiento explosivo de Internet y la intensificación de la competencia entre operadores, las telecomunicaciones del siglo XXI han ingresado en un periodo de revolución tecnológica y de mercado, donde el principal referente será la convergencia basada en el protocolo IP. Esta convergencia forzará inevitablemente a los operadores del sector de las telecomunicaciones a acondicionar sus redes hacia esta tendencia como único camino de supervivencia y crecimiento.

La Internet actual funciona bajo el protocolo IPv4 el cual fue diseñado bajo el esquema Best Effort, en el cual se proporciona una mayor valorización por el servicio de acceso y distribución de contenidos más que por el servicio de transporte de datos.

Este esquema Best Effort se caracteriza por presentar un bajo nivel de rendimiento, el cual se refleja en la lentitud de las trasmisiones, pérdidas de información, pérdidas de conexión y graves casos de congestión. A pesar de que se proporciona a las aplicaciones y servicios clásicos (Telnet, FTP, Correo Electrónico, entre otros) un esquema en el que pueden funcionar de manera adecuada, es perjudicial para las nuevas aplicaciones ya que no permite proporcionar calidad de servicio necesario para su funcionamiento.

En la actualidad con la gran velocidad de los cambios tecnológicos, la mejora de servicios como también la prioridad de recursos dentro de una red, ha obligado a realizar tanto estudios, como implementaciones para la mejora de calidad de las conexiones tanto de datos como de vos, a esto se lo denomina como QoS.

Calidad de Servicio (QoS, Quality of Service), se lo toma como el desempeño de un servicio dentro de una red y el grado de satisfacción de un cliente a este. Si se desea que la red tenga un QoS extremos todos los miembros de una red deben tener un mecanismo QoS.

En un ejemplo práctico de falta QoS, se puede tomar el uso del Internet, puesto que el Internet no diferencia la prioridad de los dispositivos, en ese caso deberemos modificar la infraestructura para llegar a un rendimiento óptimo.

El presente caso de estudio permitirá a la Empresa Pública Municipal de Transporte Terrestre, Transito y Seguridad Vial EPM Portovial realizar el análisis de la situación actual sobre los servicios de la red LAN ofertados como es el Internet, Enlace de Datos y VoIP cuyo tráfico de red circula a través de la infraestructura con el interés de tomar decisiones de cómo mejorar su desempeño contrarrestando dificultades y optimizar los procesos que puedan estar presentando conflictos como retardos en la transmisión y por lo cual mal funcionamiento.

2. Justificación.

El avance continuo de la tecnología ha llevado al 100% de las empresas en el mundo a necesitar de ella para poder subsistir y mantenerse competitivas en el mercado. Las empresas que se mantienen a la vanguardia de la tecnología y hacen uso de ésta, son las que hoy en día se destacan y tienen una gran tendencia de expansión.

Actualmente el control y buen uso de estos recursos tecnológicos es muy bajo en muchas empresas o instituciones. Los peligros que se encuentran hoy en día en las redes de datos ya sean internas como las redes LAN (Red de Área Local) o externas (Internet) cada día van creciendo y se van expandiendo rápidamente ya sea por correos electrónicos o toda clase de descarga que se haga desde Internet.

A parte de estas amenazas tampoco se tiene un control de la utilización de los recursos ni equidad en la distribución del canal por el cual se tiene acceso a Internet y esto pasa principalmente en los sitios donde varios usuarios usan el recurso al mismo tiempo, ya que debido a la falta de control, algunos usuarios absorben todo el canal en actividades no permitidas por la organización y a los usuarios que realmente lo necesiten para algo importante, les quedará muy reducido y tendrán una notable demora en sus procesos.

La importancia de este caso de estudio se hace evidente cuando se empieza a comparar las diferentes soluciones para redes IP. Aunque el protocolo IPv4 nos da muchas funcionalidades y características que favorecen al envío del tráfico, estos no son suficientes para poder hacer un correcto uso de los recursos de la red.

En la actualidad la Empresa Pública Municipal de Transporte Terrestre, Transito y Seguridad Vial EPM Portovial, desde la fecha que entró a operar para los procesos de matriculación en enero del 2015, su Infraestructura de Red no posee un excelente diseño, teniendo inconvenientes en ciertas ocasiones como latencia retardo o jitter en cada uno de sus servicios, internet, datos y VoIP sobre una misma red LAN , todo esto provocado por la indisponibilidad de la red; ya que uno de los servicios antes mencionados es el enlace de datos que se tiene con la Agencia Nacional de Tránsito, el cual provee el Sistema Informático Unificado de Matriculación Axis 4.0 por medio de un túnel para cada uno de los procesos de matriculación vehicular, es decir que la Empresa Pública Municipal EPM Portovial en su Infraestructura de la red no ofrece Calidad de Servicio (QoS), por el contrario lo que se tiene en la actualidad es Best Effort.

La Calidad de Servicio (QoS) se caracteriza por ceder la mejora en los datos, donde la mayoría de los equipos de comunicación como los Routers, Firewalls y Switches permiten priorizar las aplicaciones más necesarias e importantes, todo esto en periodo real, con el objetivo de que puedan ser utilizadas antes que el resto de los datos.

El propósito de este caso de estudio es realizar un análisis sobre el tráfico actual que se presenta en la red de telecomunicaciones de la Empresa Pública Municipal EPM Portovial y plantear soluciones basadas en Calidad de Servicio (QoS) para optimizar el ancho del canal, monitorear y detectar problemas de tráfico no deseado en la red, tomar decisiones de control de ancho de banda, filtrado web y a su vez proveer la mejor seguridad perimetral a todos los equipos en la red LAN en cuanto a medios de transmisión, Infraestructura de red y Topologías de Red, acorde a los requerimientos de la red proyectándose a futuro.

3. Antecedentes

En la actualidad la Calidad de Servicio (QoS) encierra las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado. Además a ello QoS hace rferencia a las diversas tecnologías que garantizan una cierta caliadad para los distintos servicios de toda la red.

Es importante resaltar de acuerdo los hitos e investigaciones realizadas sobre este caso de estudio a la infraestructura de la red de la Empresa Pública Municipal de Transporte Terrestre, Tránsito y Seguridad Vial EPM Portovial, de que el tráfico de la red donde se encuentran los servicios como Internet, Datos y VoIP, están sobre una misma LAN, permitiendo en ciertos momentos congestión en la misma y a su vez provocando de que exista malestar por los usuarios que manejan uno de estos servicios antes mencionados.

Hoy en día es fundamental para cualquier empresa contar con un medio que garantice y facilite la comunicación de los servicios de Internet, Datos y VoIP, con el objetivo de entregar los datos de manera fiable, apoyado en el uso eficiente de los recursos de la red, otorgando seguridad y ahorro de tiempo al usuario final al momento de utilizar las aplicaciones.

Como solución a este caso de estudio se plantea implementar Calidad de Servicio (QoS) en toda la infraestructura de la red de la Empresa EPM Portovial, para lo cual se debe requerir de tres pasos fundamentales: Identificar el tráfico de la red y sus requerimientos Clasificar el tráfico y Establecer políticas a cada clase.

4. Objetivos.

Objetivo General.

Analizar el Tráfico de la Infraestructura de la Red de la Empresa Pública Municipal de Transporte Terrestre, Tránsito y Seguridad Vial EPM Portovial, ofreciendo un Modelo con Calidad de Servicios QoS.

Objetivos Específicos.

1. Realizar un estudio de la situación actual de la Infraestructura de la red de la Empresa Pública Municipal EPM Portovial con los enlaces existentes.

2. Investigar mediante estudio los Perfiles y Políticas de Seguridad de acuerdo a las vulnerabilidades que pueden estar expuestos los datos.

3. Realizar un análisis de tráfico Best Effort y con Calidad de Servicio (QoS).

4. Proponer como solución la implementación de QoS en toda la red de la Empresa Pública Municipal EPM Portovial.

5. Desarrollo Caso de Estudio

Uno de los factores de éxito de la Internet actual ([1]), está en la aceptación de los protocolos TCP/IP ([2]), como estándar de facto para todo tipo de servicio y aplicaciones. La Internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de pública del XXI.

Una carencia fundamental de la actual Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los diferentes tipos de aplicación de usuario. La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como Best Effort, existen diferentes arquitecturas de Calidad de Servicio, IntServ, ServDiff.

5.1 Estudio de la Situación Actual de la Infraestructura de la Red.

El 7 de marzo de 2013 se crea la Empresa Pública Municipal de Transporte Terrestre, Tránsito y Seguridad Vial EPM Portovial, la misma que se constituye como persona jurídica de derecho público.

Luego mediante Resolución N° 179-DE-ANT-2014, suscrita por el Abg. Héctor Solórzano, Director Ejecutivo de la ANT de fecha 29 de octubre de 2014, resuelve certificar que el Gobierno Autónomo Descentralizado Municipal del Cantón Portoviejo, empezará a ejecutar competencias de títulos habilitantes en el ámbito de jurisdicción a partir del 4 de noviembre del 2014 y de Matriculación y Revisión Técnica Vehicular a

partir del 16 de enero de 2015; conforme a la Ley Orgánica de Transporte Terrestre, Tránsito y Seguridad Vial y su Reglamento General.

La Empresa Pública Municipal EPM Portovial, está constituida por un directorio que lo preside el Señor Alcalde del GAD Portoviejo el Ing. Agustín Casanova, al frente de esta empresa se encuentra el Gerente General el Ing. Gustavo Barrera Plúa, además la empresa posee las áreas de Secretaria General, Jurídica, Comunicación, Planificación, Financiero, Talento Humano, Compras Públicas, Tesorería, Contabilidad, Tecnología, Dirección Técnica, Transporte y Tránsito, Semaforización, Seguridad Vial, Archivo Central, Matriculación y Revisión Técnica Vehicular.

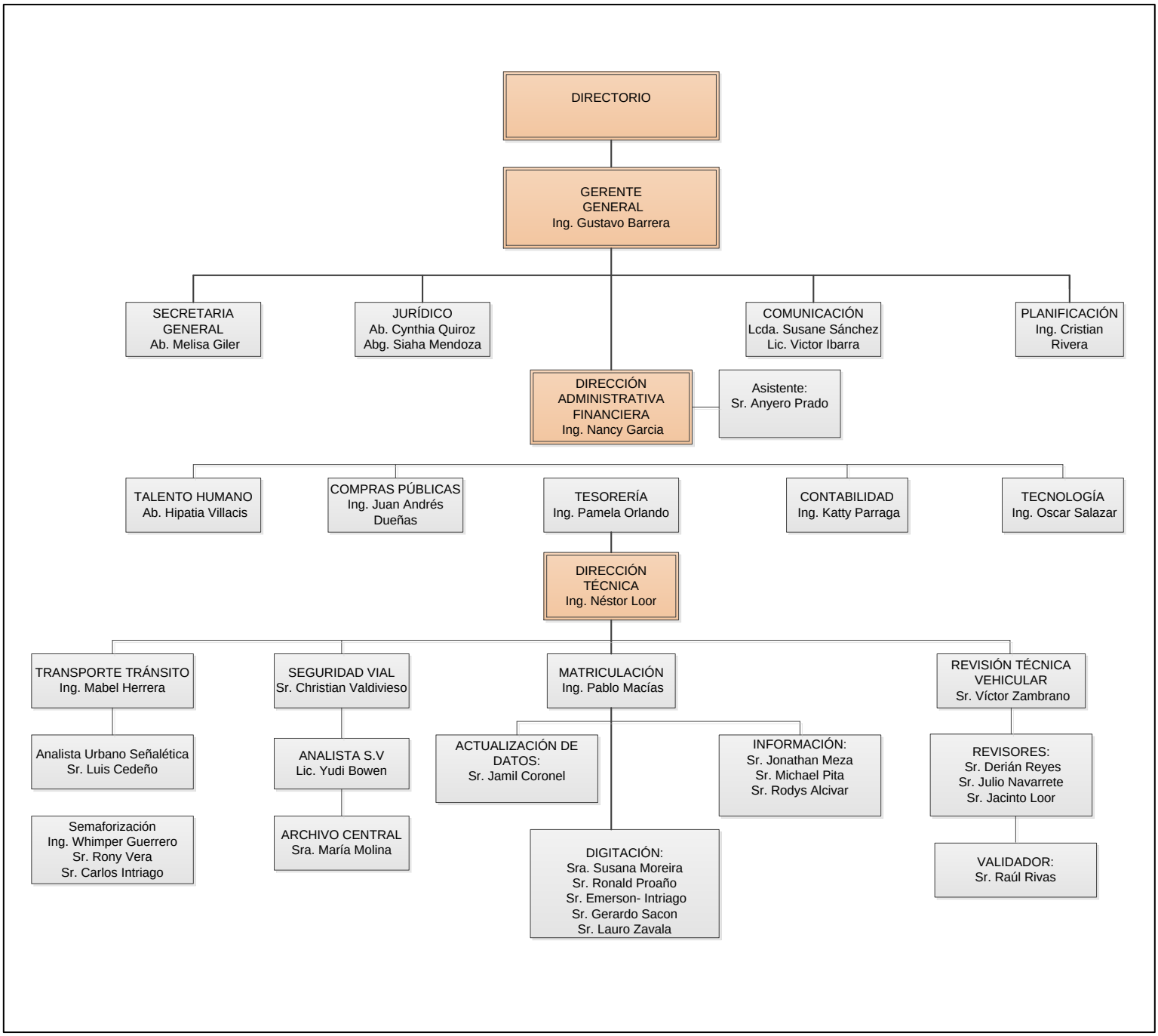


Figura 1. Organigrama Estructural de EPM Portovial. - Fuente: Área de Planificación de EPM Portovial.

A medida que fue creciendo la Empresa se incrementó personal y a su vez nació la necesidad de extender más puestos de trabajo, la infraestructura de red que se tenía en ese momento no garantizaba la demanda de tráfico de los datos de sus usuarios, ya que los

equipos de comunicación que se tenía en ese momento no eran equipos robustos, lo que provocaba la pérdida de paquetes por la falta de disponibilidad y a su vez haciéndola una red muy flexible y de poca seguridad. Además se presentaba encolamientos en toda la red y lentitud con el sistema de matriculación y otros servicios a nivel de internet.

Para realizar los procesos de matriculación vehicular se lo efectuaba mediante el sistema informático SITCON, el mismo que la ANT proporciona por medio de un enlace de datos mediante una red privada, hoy en día este sistema sólo se utiliza para realizar ciertas consultas a nivel de placas y usuarios.

Los servicios de comunicación con los que contaba en ese momento la empresa eran los siguientes:

- ✓ Internet (Ancho de Banda 2 Mb).
- ✓ Datos ANT (Ancho de Banda 2 Mb).

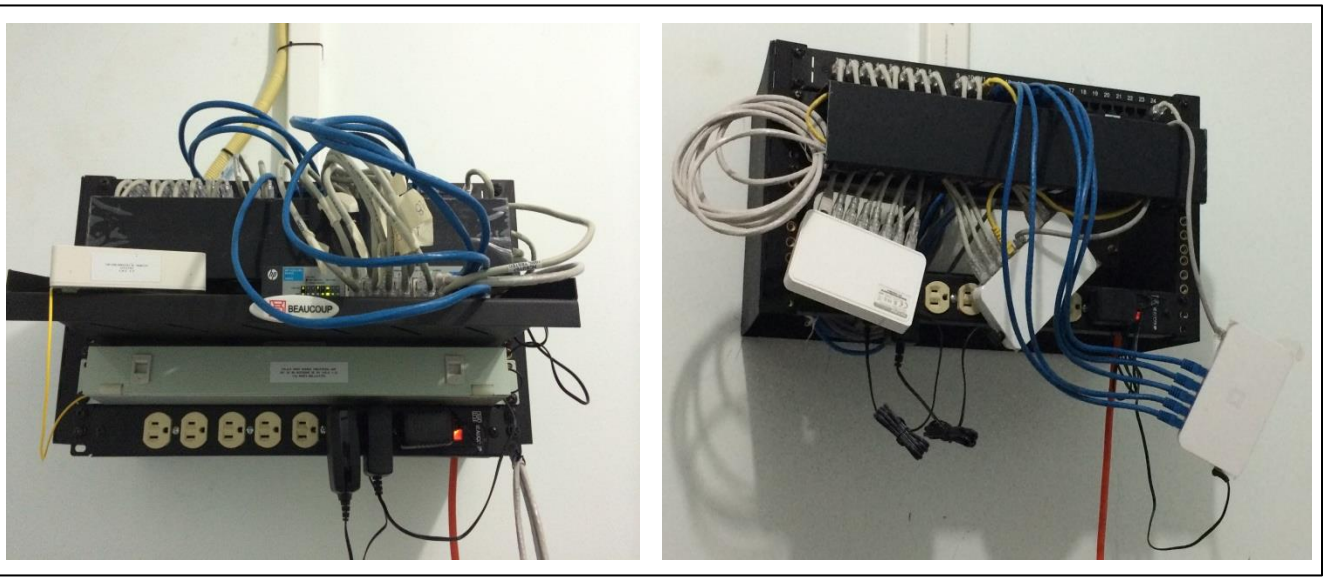


Figura 2. Antigua Infraestructura de la Red de EPM Portovial. - Fuente: Área de Tecnología de EPM Portovial.

El 15 de enero el año 2016 la Agencia Nacional de Tránsito – ANT implementa un nuevo Sistema Informático Unificado de Matriculación Axis 4.0, el mismo que consiste en unificar la Base de Datos de la Comisión de Tránsito del Ecuador con la del resto del país, con el objetivo de que los usuarios puedan realizar la matriculación de sus vehículos y motos en cualquier provincia o cantón del Ecuador evitando el mayor uso de documentos para los diferentes procesos de matriculación vehicular gracias a que este sistema permite escanear los documentos originales del usuario como cédula de identidad, certificado de votación, carta de compra – venta y otros, el peso de cada archivo al momento de subir al sistema es de hasta 500 Kb.

Luego la Empresa Pública Municipal EPM Portovial implementó en su primera fase una nueva infraestructura de red con equipos de comunicación desde Router, Firewall, Switches Administrables, Central Telefónica, Servidores, Cámaras Ip y NVR, los mismos que permiten garantizar el tráfico de los datos en la red Best Effort de aquellos usuarios que iban hacer uso de los servicios de Internet, Datos y VoIp; lo que llevó a incrementar el ancho de banda de los mencionados servicios de Internet y Datos de 2 a 4 Mb, también a ello se suma el uso de servicios vía web, como son:

- ✓ Correo Institucional https://mail.portoviejo.gob.ec/owa.
- ✓ Sistema de Control de Tramites Municipales https://online.portoviejo.gob.ec:8090/Principal.aspx
- ✓ Sistema de Alertas y Control Territorial https://online.portoviejo.gob.ec:8086/.
- ✓ Portal web de la empresa EPM Portovial http://www.portovial.gob.ec/epm/.

Las dificultades que actualmente presenta la red son las siguientes:

- ✓ Existe en ciertas ocasiones la red presenta pequeña lentitud lo que permite no tener alta disponibilidad para todos los servicios que se manejan en la empresa.
- ✓ La empresa posee un firewall como es el Fortinet - Fortigate 60D en el cual se tiene creada políticas y perfiles de seguridad a los usuarios que se encuentran en los grupos acceso total, acceso restringido, acceso de cámaras y acceso a celulares pero no una segmentación en la misma, además a ello si se tiene el control del ancho de banda a los grupos antes mencionados.
- ✓ No se tiene montado un Active Directory dentro de la red para los usuarios.
- ✓ Actualmente la red no posee segmentación por medio de Vlans para las áreas dentro de la empresa.
- ✓ No se cuenta con unidades de respaldos de almacenamiento para la información crítica.

Figura 3. Actual Infraestructura de la Red de EPM Portovial. - Fuente: Área de Tecnología de EPM Portovial.

5.1.1 Topología Física de la Red Actual.

Las tecnologías de Red en la actualidad se utilizan de una manera rápida y eficiente, gracias a esto se obtiene menor costo y mayor eficiencia.

Luego del pasado terremoto del 16 de Abril del 2016, el edificio donde funcionaba la Empresa Pública Municipal EPM Portovial colapsó y se tuvo que retomar las operaciones en contenedores, volviendo armar la misma Infraestructura de la Red con todos los equipos de transmisión y comunicación para el óptimo desempeño de los usuarios que utilizan actualmente los servicios de matriculación y otros.

El enlace que posee actualmente la Empresa es mediante un medio guiado con fibra óptica monomodo cuyo ISP es la Corporación Nacional de Telecomunicaciones ANT. Los equipos de comunicación y medios que conforman la Infraestructura de la Red de la Empresa son los siguientes:

Cantidad	**Descripción de Equipos de Transmisión y Comunicación**
1	**Router:** Cisco 800 Series
1	**Transceiver:** Optical Fiber Device 100Base-FX
1	**Bandeja ODF:** ODF-6-G. 652D
1	**Firewall:** Fortinet – Fortiget 60D
2	**Switch:** HP 1910 Web Admin Gb.
1	**Central Telefonica**: Hp Micro Server Gen8 G2020T Base NH PUS Svr.

1	**Teléfono GrandStream:** GXP2160 - Operadora
10	Teléfono GrandStream: GXP1625 - Usuarios
1	**Servidor de Aplicación:** HP ProLiant Micro Server Gen8 – WINDOWS SERVER 2008 R2
1	**NVR Hikvision Cámaras IPs:** 16 Canales IP (8 en HD) + 8 Puertos PoE: DS-7616NI-E2/8PI
8 **3** **3** **1**	**Cámaras Hikvision tipo POE - 1.3 Mp:** DS-2CD2010-I **Cámara Hikvision tipo POE - 1.3 Mp:** DS-2CD2010F-I **Cámara Hikvision tipo POE - 1.3 Mp:** DS-2CD1410F-I **Cámara Hikvision tipo POE - 1.3 Mp:** DS-2CD241F-I
1	**Cámara Hikvision PTZ 1.3 Mp:** DS-2DE5174
1	**Switch:** HP 1410 10/100/1000 Base-T (contenedor # 3)
1	**Switch:** Tplink 10/100 (Contenedor # 4)
3	**Access Point Ubiquiti:** 802.11n MIMO Unifi AP
3	**Cableado UTP par trenzado sólido**: Categoría 6

Tabla 1. Equipos de Transmisión y Comunicación - Fuente: Área de Tecnología de EPM Portovial.

A continuación se presenta la Topología Física de la Red de Datos de EPM Portovial.

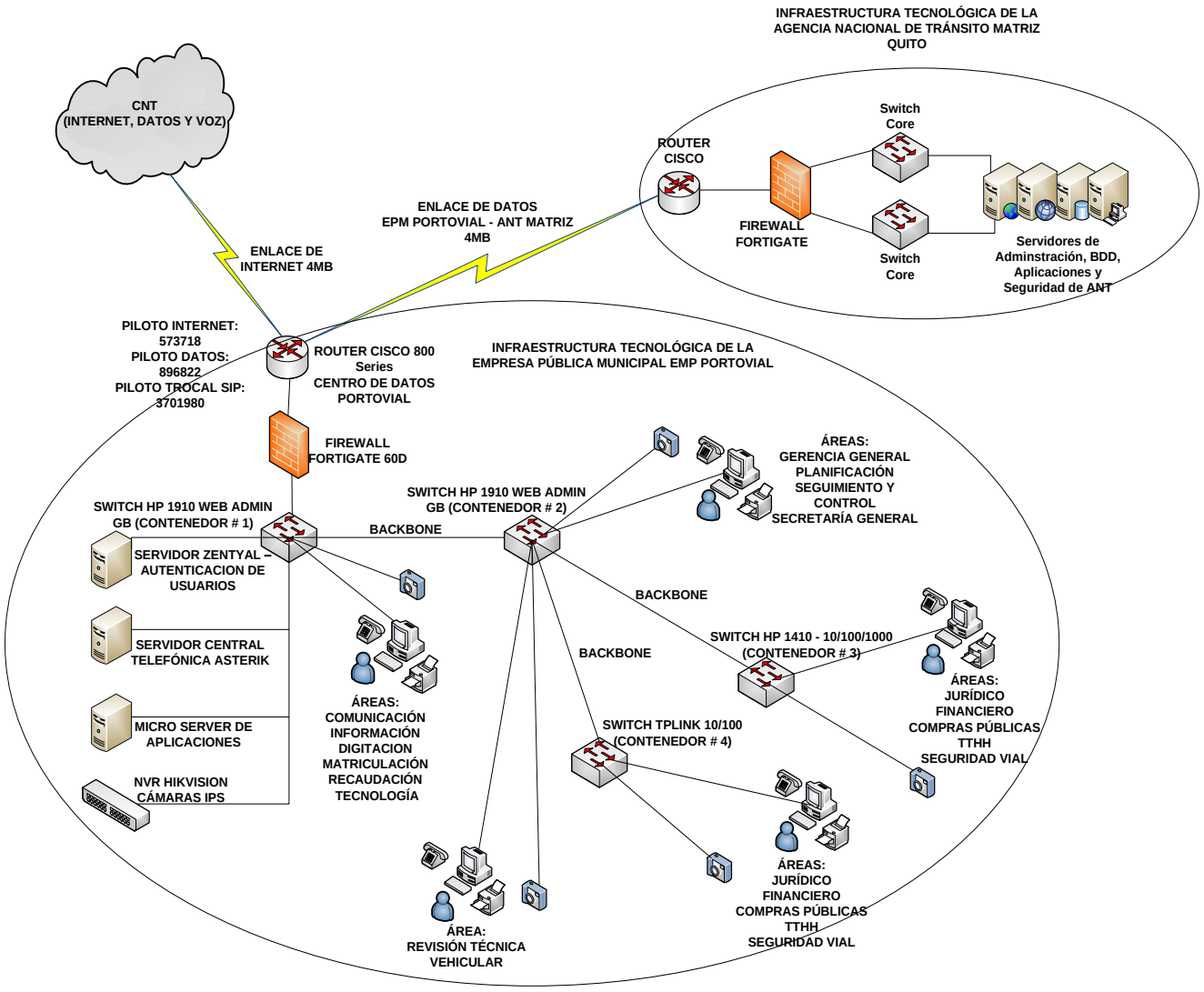


Figura 4. Topología Física de la Red de Datos - Fuente: Área de Tecnología de EPM Portovial.

5.1.2 Cuarto Principal de Comunicaciones EPM Portovial.

Actualmente el cuarto de comunicaciones se encuentra ubicado en el contenedor 1, que es allí donde se efectua toda la administración y control del flujo de la información y operación para los distintos procesos que se realiza a diario en la empresa.

Los equipos que se encuentran en el cuarto principal de comunicaciones son los siguientes:

Descripción de Equipos de Transmisión y Comunicación
Router: Cisco 800 Series. (Pilotos Internet, Datos y Troncal SIP).
Transceiver: Optical Fiber Device 100Base-FX.
Bandeja ODF: ODF-6-G. 652D.
Firewall: Fortinet – Fortiget 60D.
Switch: HP 1910 Web Admin Gb. (Permite conectar al Backbone del contenedor 2).
Central Telefonica: Hp Micro Server Gen8 G2020T Base NH PUS Svr.
Servidor de Aplicación: HP ProLiant Micro Server Gen8 – WINDOWS SERVER 2008 R2
NVR Hikvision Cámaras IPs: 16 Canales IP (8 en HD) + 8 Puertos PoE: DS-7616NI-E2/8PI
Access Point Ubiquiti: 802.11n MIMO Unifi AP
Teléfono GrandStream: GXP1625 - Usuarios

Tabla 2. Equipos de Transmisión y Comunicación Cuarto Principal Contenedor 1 - Fuente: Área de Tecnología de EPM Portovial.

Los equipos que se encuentran en el contendedor 2 son los siguientes:

Switch: HP 1910 Web Admin Gb. (Permite conectar al Backbone del contenedor 1).

Access Point Ubiquiti: 802.11n MIMO Unifi AP
Teléfono GrandStream: GXP1625 - Usuarios

Tabla 3. Equipos de Transmisión y Comunicación Contenedor 2 - Fuente: Área de Tecnología de EPM Portovial.

Los equipos que se encuentran en el contendedor 3 son los siguientes:

Switch: HP 1410 10/100/1000 Base-T (contenedor # 3, permite conectar al Backbone del contenedor 2)
Teléfono GrandStream: GXP1625 – Usuarios

Tabla 4. Equipos de Transmisión y Comunicación Contenedor 3 - Fuente: Área de Tecnología de EPM Portovial.

Los equipos que se encuentran en el contendedor 4 son los siguientes:

Switch: Tplink 10/100 (Contenedor # 4, permite conectar al Backbone del contenedor 2)
Teléfono GrandStream: GXP1625 – Usuarios

Tabla 5. Equipos de Transmisión y Comunicación Contenedor 4 - Fuente: Área de Tecnología de EPM Portovial.

Los equipos que se encuentran en el Área de Revision Técnica Vehicular RTV son los siguientes:

Access Point Ubiquiti: 802.11n MIMO Unifi AP
Teléfono GrandStream: GXP1625 – Usuarios

Tabla 6. Equipos de Transmisión y Comunicación Área RTV - Fuente: Área de Tecnología de EPM Portovial.

5.1.3 Esquema Lógico de la Red Informática Actual.

La topología lógica en la que se encuentra la red de datos de la empresa Portovial está mediante el direccionamiento IP en una red de clase C 192.168.x.x, la misma que no posee segmentación en la actualidad, es decir es una red plana.

5.1.4 Red de Clase C.

El protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su dirección, que está compuesta por un número de 32 bits (cuatro octetos) y que es único para cada host.

El valor del primer byte, en estas direcciones, es de entre 192 y 223, utilizando los primeros tres bytes para el número de la red. El ultimo byte de la dirección, permitiendo un número máximo de 254 ordenadores.

A continuación se muestra el esquema lógico de la red datos de EPM Portovial.

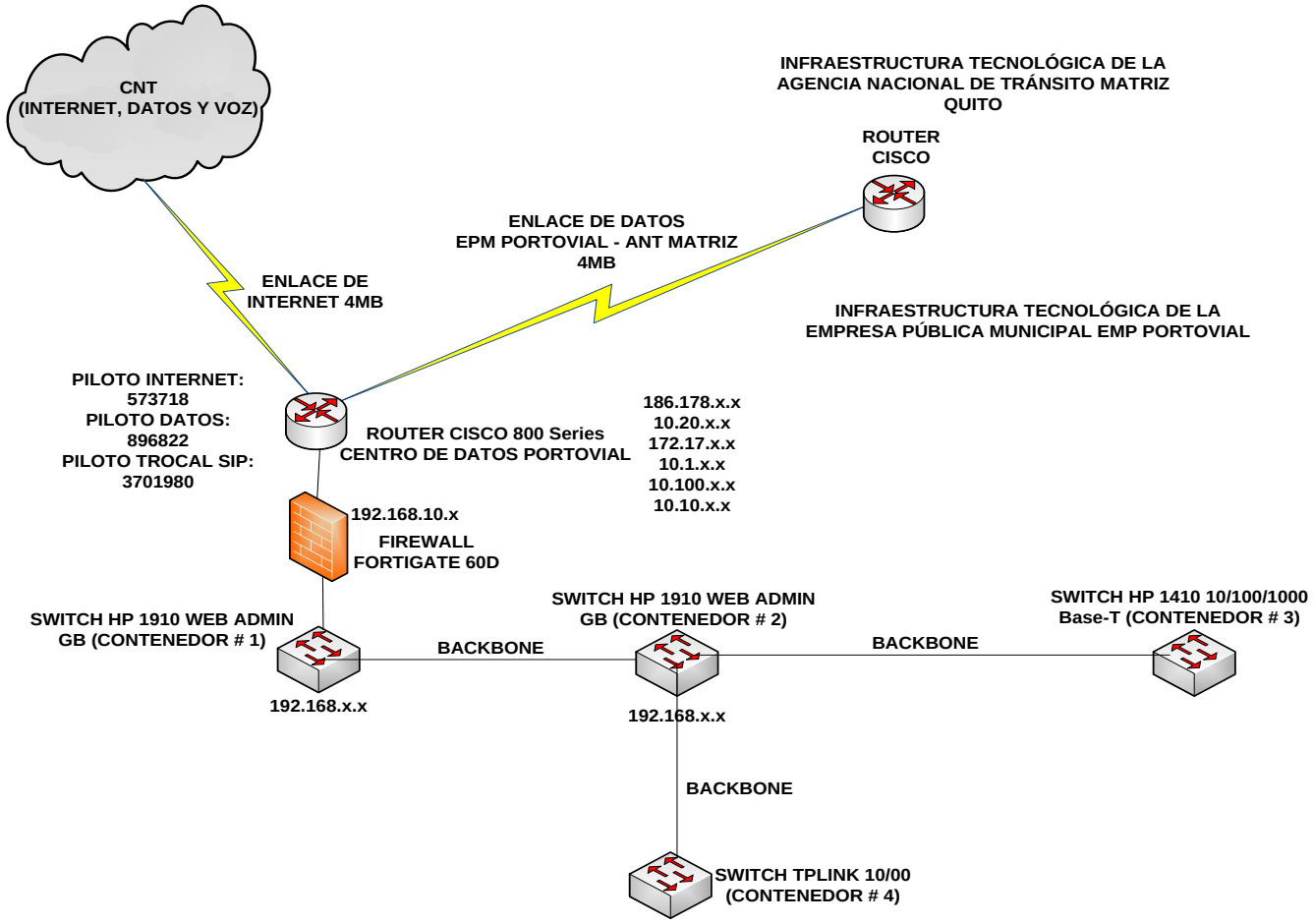


Figura 5. Esquema Lógico de la Red de Datos - Fuente: Área de Tecnología de EPM Portovial.

5.2 Estudio de los Perfiles y Políticas de Seguridad.

Hoy en día el uso de los servicios de Internet se encuentra en un proceso de aumento y evolución, esto ha llevado a las instituciones públicas y privadas a tomar decisiones en el control y protección de los datos, además a ello se suma el acceso a los sistemas de información desde cualquier lugar, permitiendo tener seguridad en toda la infraestructura de la red.

Las amenazas representan una acción dañina, mientras que la vulnerabilidad de los datos es el grado a la que se expone la información. Para que los datos de la empresa o las aplicaciones que corren en toda la red sean seguros se debe implantar perfiles o grupos de usuarios, los cuales estén sujetos a las políticas de seguridad que proteja toda la red, cuyo propósito es usar de manera correcta y eficiente los recursos para los cuales fueron creados.

Existen cinco características principales dentro de la seguridad que son las siguientes:

Integridad, Confidencialidad, Disponibilidad, No repudio y Autenticación.

5.2.1 Definición de Perfiles y Políticas de Seguridad.

En el presente documento se muestra los perfiles y las políticas de seguridad establecidas en el Firewall como un recurso para mitigar los riesgos a la red de datos de la empresa Portovial.

El equipo de telecomunicaciones con el que se cuenta es un Fortigate 60D de la marca Fortinet. Este equipo cuenta con la línea de procesadores de seguridad de red basados en tecnología ASIC.

El firewall con el que actualmente cuenta la empresa EPM Portovial es un FortiGate 60D, cuyo equipo es un dispositivo de seguridad de la red que monitorea el tráfico de la red tanto entrante como saliente y a su vez permite bloquear el tráfico específico en función al conjunto de las reglas de seguridad.

Este firewall posee grandes características de administración unificada de amenazas UTM, además a ello permite una inspección activa para la prevención de instrucciones y antivirus.

Características y beneficios

- ✓ Entrega un rendimiento líder en el mercado de 1.5 Gbps de performance de firewall con 7 puertos de switch de GbE, 1 puerto DMZ GbE y 2 puertos WAN GbE.
- ✓ FortiWiFi-60D ofrece capacidades de doble banda y soporta los estándares 802.11a/b/g/n asegurando la compatibilidad con la infraestructura de la red inalámbrica existente.
- ✓ Cuenta con un rico y completo set de características de protección de próxima generación con control de aplicaciones, rendimiento acelerado de IPS/AV, logueo local y refuerzo y cumplimiento de políticas de punto final.
- ✓ Una plataforma preparada para IPv6 con opciones de autenticación fuerte para el acceso a red seguro y cumplimientos de políticas de seguridad.
- ✓ Una consola de administración única, sencilla e intuitiva hace que sea fácil la implementación y administración.

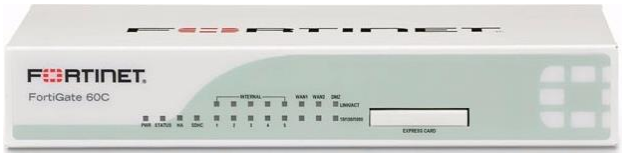
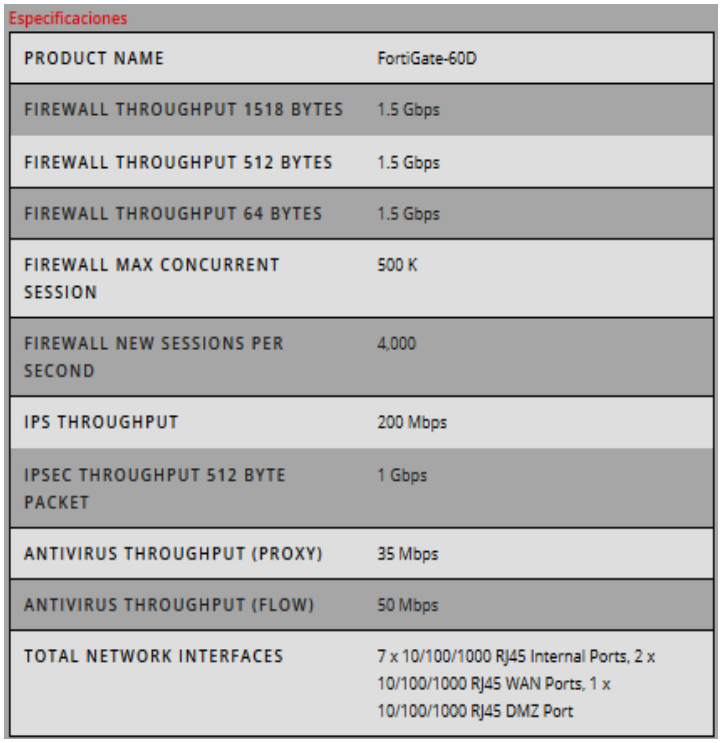


Figura 6. Equipo Fortigate 60D - Fuente: Fortinet.com



Especificaciones

PRODUCT NAME	FortiGate-60D
FIREWALL THROUGHPUT 1518 BYTES	1.5 Gbps
FIREWALL THROUGHPUT 512 BYTES	1.5 Gbps
FIREWALL THROUGHPUT 64 BYTES	1.5 Gbps
FIREWALL MAX CONCURRENT SESSION	500 K
FIREWALL NEW SESSIONS PER SECOND	4,000
IPS THROUGHPUT	200 Mbps
IPSEC THROUGHPUT 512 BYTE PACKET	1 Gbps
ANTIVIRUS THROUGHPUT (PROXY)	35 Mbps
ANTIVIRUS THROUGHPUT (FLOW)	50 Mbps
TOTAL NETWORK INTERFACES	7 x 10/100/1000 RJ45 Internal Ports, 2 x 10/100/1000 RJ45 WAN Ports, 1 x 10/100/1000 RJ45 DMZ Port

Figura 7. Especificaciones Técnicas del Fortigate 60D - Fuente: Fortinet.com, Redacción ZNET.

El tráfico de los enlaces de Internet y Datos pasa por el equipo Fortigate 60D, allí se controla el ancho de banda de toda la red y se aplica un control UTM a todo el tráfico que por allí circula. Este equipo se basa principalmente en políticas de firewall, cada política puede contener directrices de seguridad para los grupos creados como: acceso total, acceso restringido, cámaras Nvr Hikvision y acceso a celulares, además a ello se suma el control de las páginas web a las que pueden acceder las direcciones IP que están en esta política, control de antivirus, IPS, IDS, DoS, tipos de archivos que pueden descargar, registro de datos del tráfico de red, entre otras.

Como se puede observar en la figura 7 dentro de las políticas del firewall se encuentran configuradas las interfaces Internal 1 (Lan), Internal 2 (Datos) y Wan 2 (Internet), las mismas que hacen referencia a que grupo se encuentra ligada esta política.

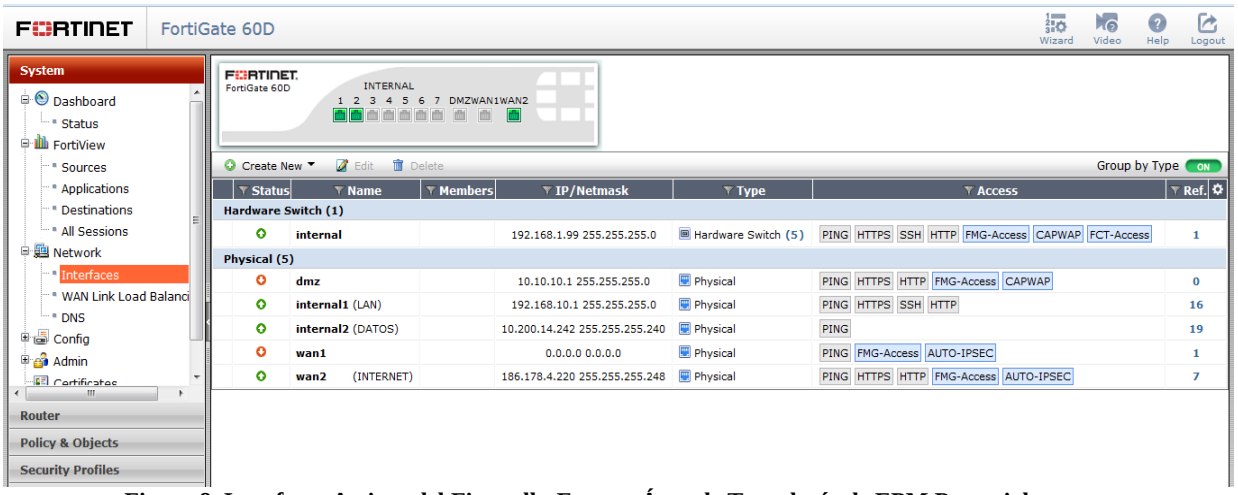


Figura 8. Interfaces Activas del Firewall - Fuente: Área de Tecnología de EPM Portovial.

Dentro de las políticas del Firewall que se encuentran creadas en el Fortigate 60D son las siguientes:

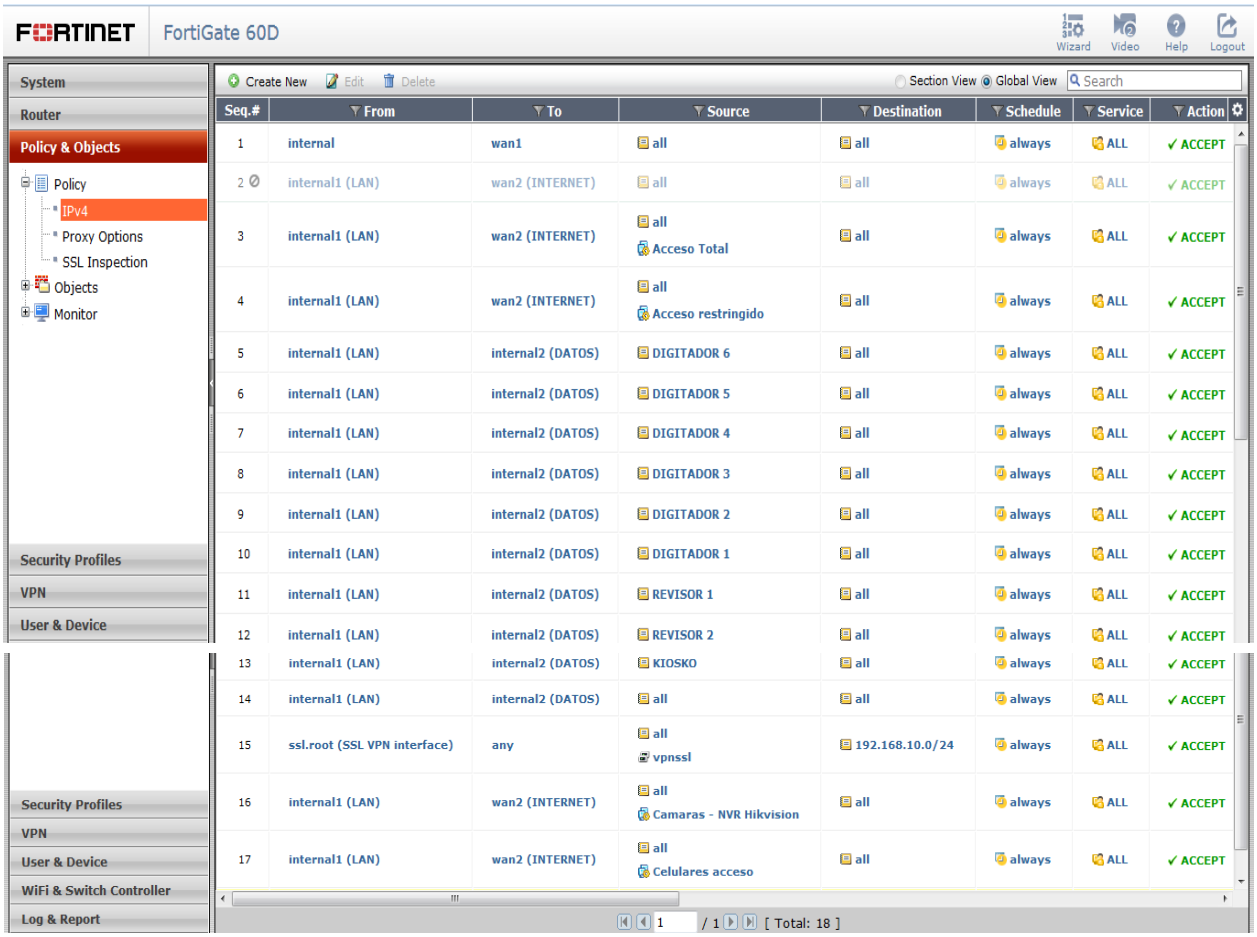


Figura 9. Politicas del Firewall Creadas para los Grupos - Fuente: Área de Tecnología de EPM Portovial.

Además a ello en la internal 1 (LAN) que hace referencia a la internal 2 (Datos), se encuentra configurado un NAT para el pools de IPs privada que otorgó la Agencia Nacional de Tránsito para aquellos usuarios que manejan procesos de matriculación y otros como son los digitadores, personal de RTV y la máquina del Kiosko para la emisión de los turnos, todo esto apuntando al Sistema de Matriculación Unificado Axis 4.0.

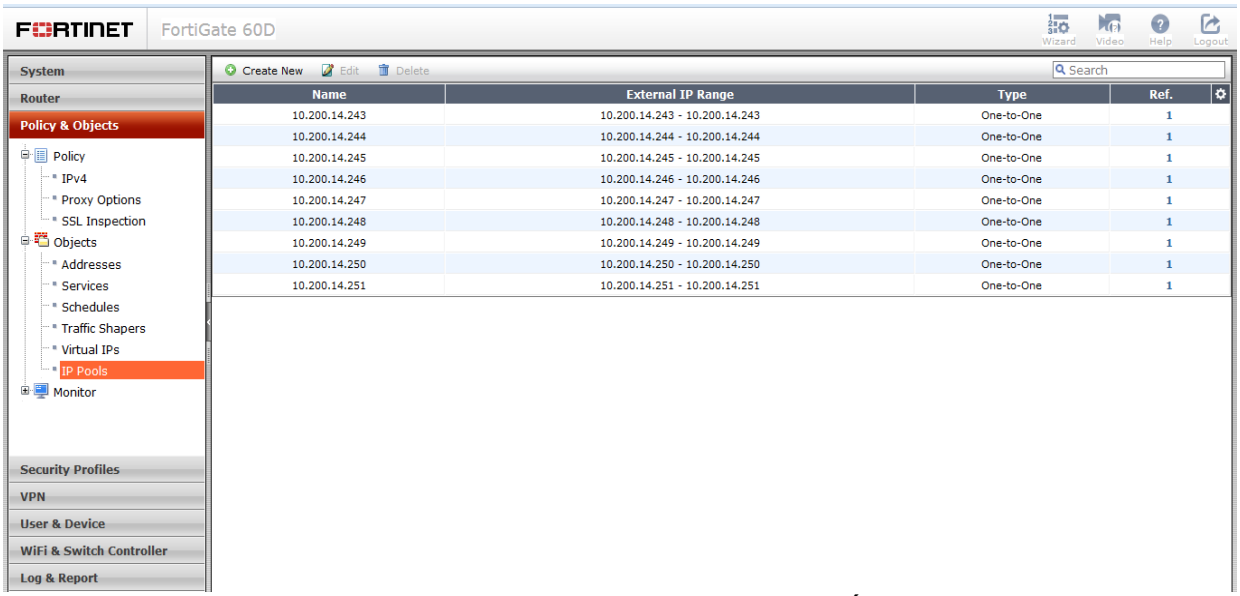


Figura 10. Pools de IPs de ANT Implementadas en el Firewall - Fuente: Área de Tecnología de EPM Portovial.

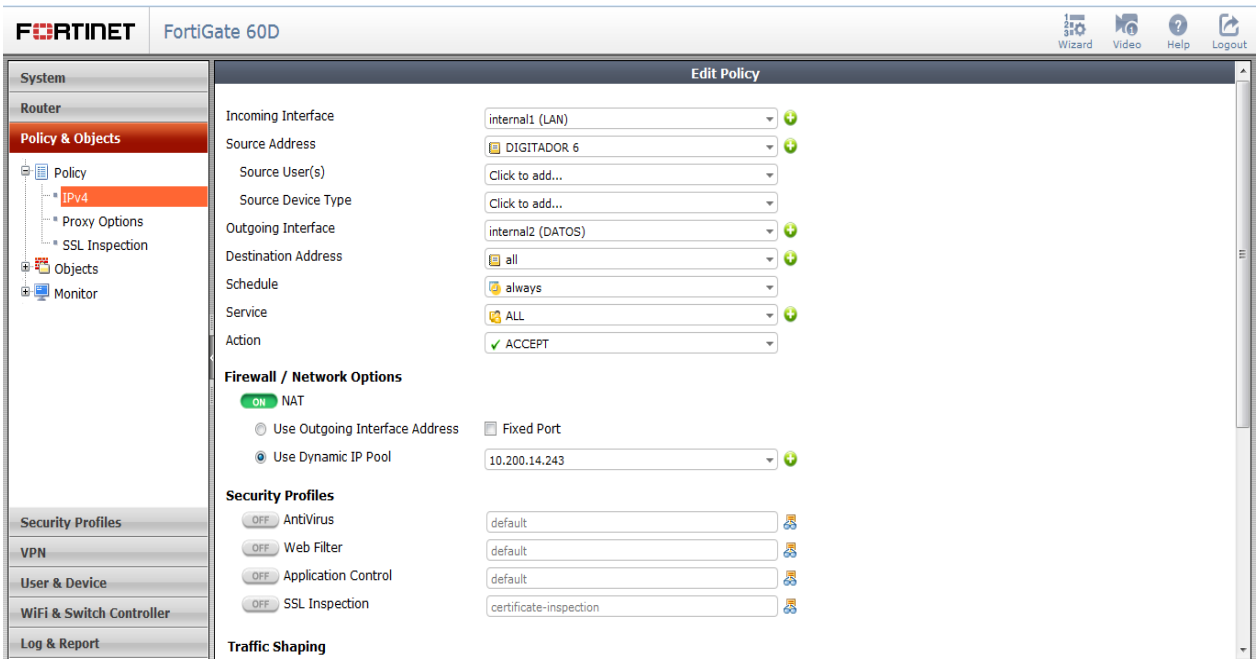


Figura 11. NAT en el Firewall - Fuente: Área de Tecnología de EPM Portovial.

5.2.1.1 Traffic Shapers del Fortigate 60D.

Conformado de tráfico (traffic shaping o packet shaping) es un mecanismo de control del tráfico inyectado a la red. Su objetivo es evitar la sobrecarga de la red con altas ráfagas de tráfico inyectado.

La conformación del tráfico, o la gestión del tráfico, controla el ancho de banda disponible y establece la prioridad del tráfico procesado, por la política para controlar el volumen de tráfico durante un período específico (estrangulación de ancho de banda) o tasa de tráfico.

La formación del tráfico intenta normalizar los picos y ráfagas de tráfico para priorizar ciertos flujos sobre otros. Pero hay una limitación física a la cantidad de datos que se pueden almacenar en memoria intermedia y la duración del tiempo. Una vez que estos

umbrales han sido superados, los marcos y paquetes se eliminarán, y las sesiones se verán afectadas de otras maneras.

Un enfoque básico de la conformación del tráfico es dar prioridad a ciertos flujos de tráfico sobre otros tráficos cuya pérdida potencial es menor desventajoso. Esto significa ciertos sacrificios en el rendimiento y la estabilidad en la baja prioridad del tráfico, para aumentar o garantizar el rendimiento y la estabilidad del tráfico de alta prioridad.

Hay que tomar en cuenta que la conformación del tráfico es efectiva para el tráfico IP normal a velocidades normales de tráfico. La conformación del tráfico no es efectiva durante los períodos en que el tráfico excede la capacidad de la unidad FortiGate debido a que los paquetes deben ser recibidos por el FortiGate antes de que estén sujetos a la conformación del tráfico, si la unidad FortiGate no puede procesar todo el tráfico recibe, entonces los paquetes perdidos, los retrasos, y la latencia son probables a ocurrir.

En la figura 11 se muestra el nombre de los grupos que se encuentran creados en el Traffic Shapers del Fortigate con las siguientes asignaciones:

- ✓ Acceso total con un Ancho de banda garantizado de 2048 (Kb/s), Ancho de banda máximo de 2097152 (Kb/s) y con prioridad alta.
- ✓ Acceso restrigido con un Ancho de banda garantizado de 2048 (Kb/s)correspondiente a 2 Mb, Ancho de banda máximo de 2097152 (Kb/s) y con prioridad alta.
- ✓ Cámaras Nvr Hikvision con un Ancho de banda garantizado de 100 (Kb/s) correspondiente a 0.09766 Mb, Ancho de banda máximo de 102400 (Kb/s) y con prioridad baja.

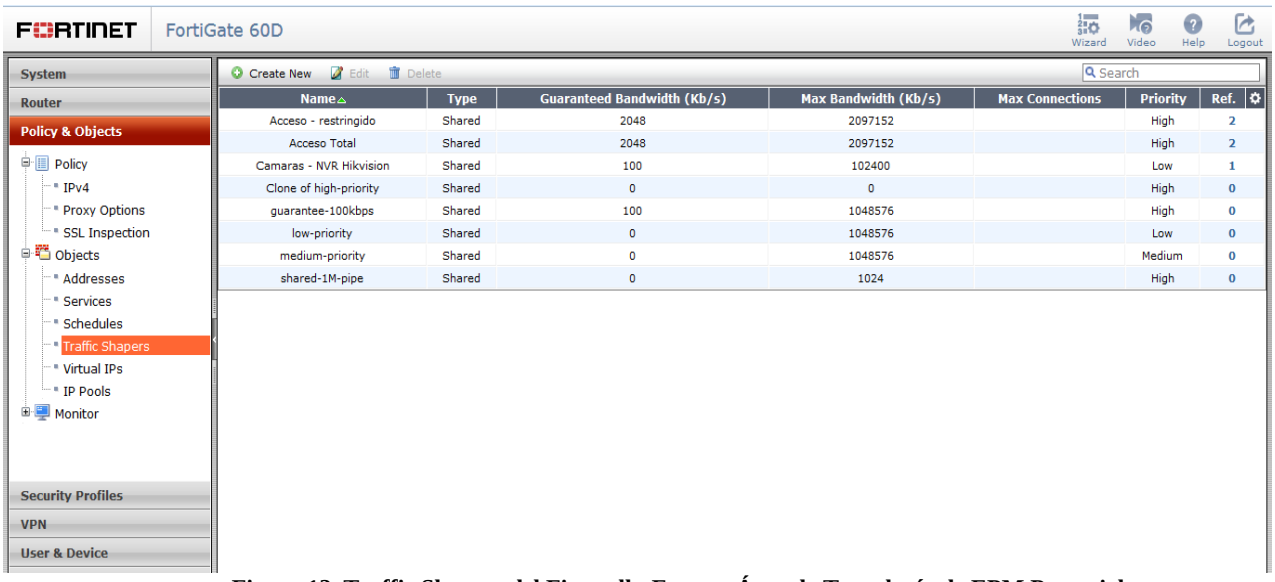


Figura 12. Traffic Shapers del Firewall - Fuente: Área de Tecnología de EPM Portovial.

A continuación se muestran todos los usuarios y dispositivos agregados a los diferentes grupos creados dentro de los perfiles del Firewall.

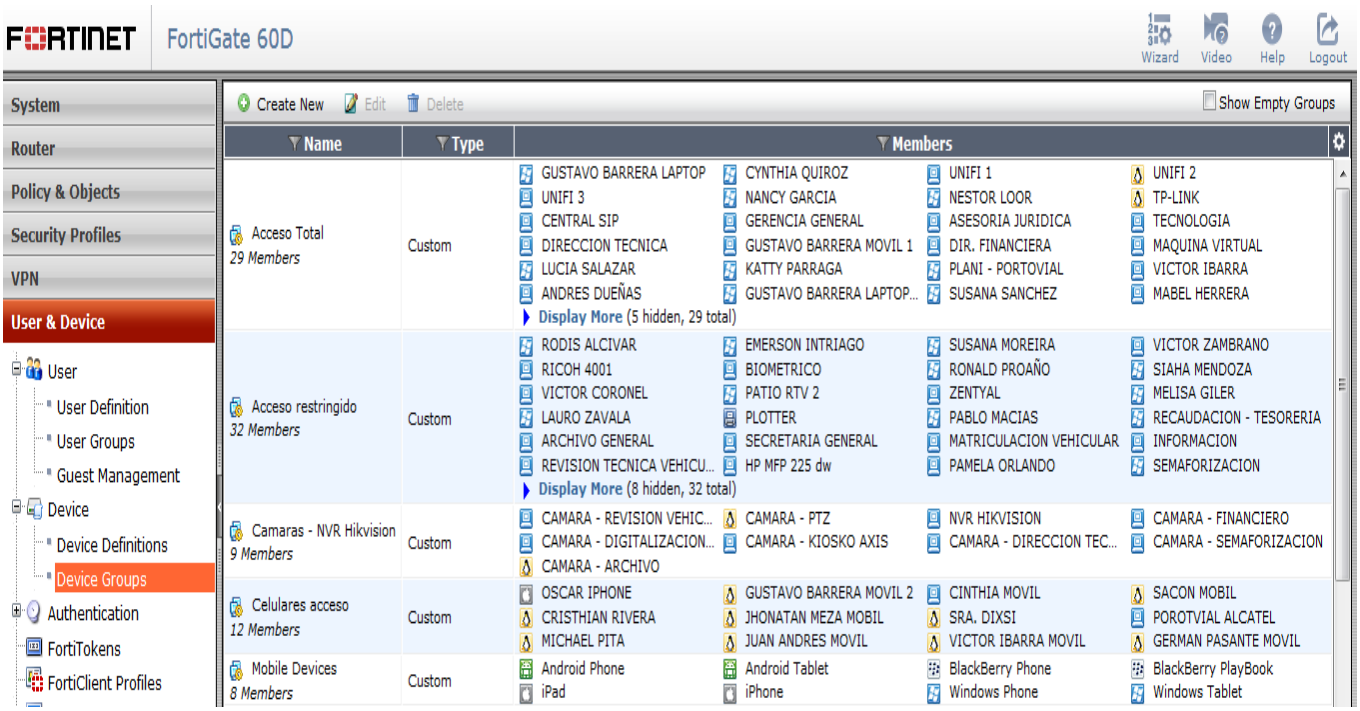


Figura 13. Grupos de Usuarios y Dispositivos del Firewall - Fuente: Área de Tecnología de EPM Portovial.

5.2.1.2 Filtrado Web del Fortigate 60D.

El Servicio de Filtrado Web de Fortinet entrega actualizaciones para regular actividades web. Con 75 categorías de contenidos web, más de 30 millones de sitios web nominales y más de dos mil millones de páginas web, el servicio de filtración de FortiGuard es uno de los servicios integrados más exacto de la industria.

La solución Fortiguard Web Filter consiste en dos partes, los Servidores Fortiguard y el sistema de seguridad multi amenaza FortiGate. Los servidores FortiGuard contienen una base de datos de posiciones que consiste en unos mil millones de direcciones de páginas web. El servicio de Filtración FortiGuard puede ser activado sobre todos los sistemas de seguridad FortiGate para regular y bloquear el acceso a los sitios web dañinos, inadecuados y peligrosos que pueden contener ataques de Phishing y/o malware como spyware. Las posibilidades de filtrado son múltiples:

- Filtrado de URL
    - ✓ Por direcciones IP.
    - ✓ URLs completas.
    - ✓ URLs definidas usando wildcards o regular expressions.
    - ✓ Posibilidad de importar listas de terceros.
- URL Exempt list
- Filtrado de contenido - Listas negras/blancas locales
- Filtrado de Scripts - Java applets, cookies, y activeX
- Administrador de Servicio filtrado de URL (FortiGuard).
    - ✓ Más de 25 millones de dominios categorizados.
    - ✓ 56 categorias.

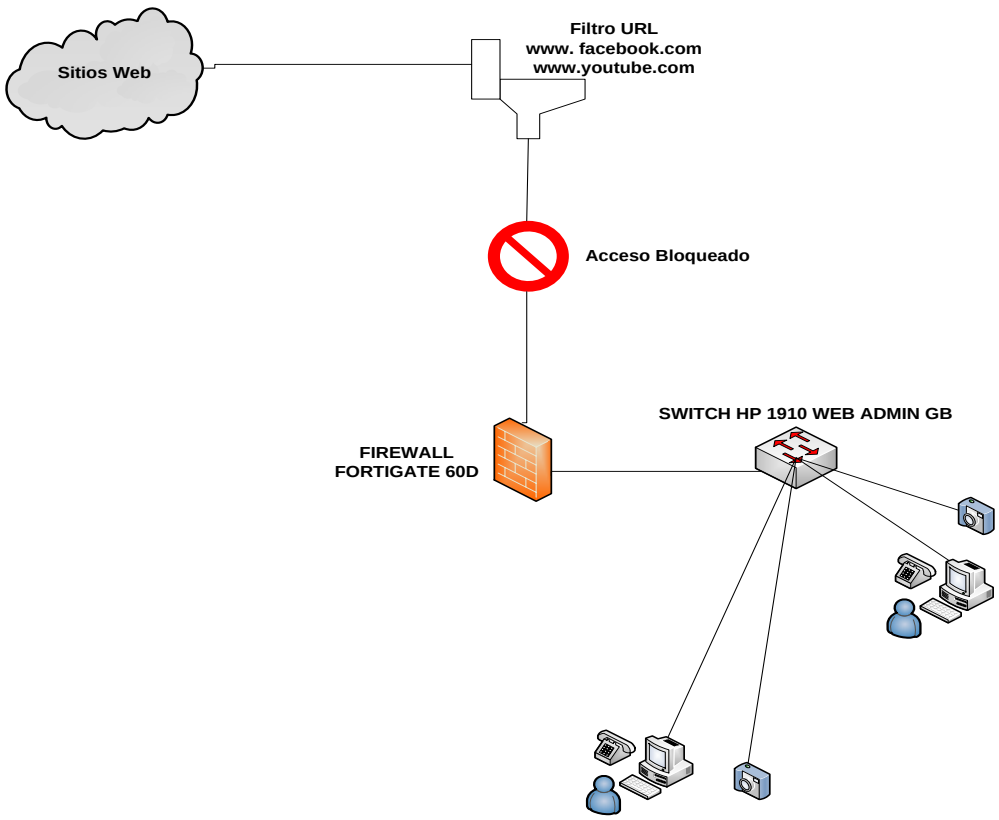


Figura 14. Esquema Lógico de las Políticas de Seguridad del Filtrado Web - Fuente: Área de Tecnología de EPM Portovial.

El filtrado web se maneja de manera similar, primero se crea un perfil de filtrado web, este perfil contará con todas las paginas que se quieran restringir, una característica importante de este equipo es que tiene una gran base de datos de sitios web, los cuales están separados por categorías, esto es de gran ayuda ya que no se tiene que bloquear pagina por pagina, sino que se puede bloquear un grupo completo de páginas que sean del mismo tipo.

Las categorías de filtrado web están organizadas en 8 grupos principales:

1. Categorías locales
2. Potencialmente responsable

3. Contenido adulto / maduro
4. Consumo de ancho de banda
5. Riesgo de seguridad
6. Interés general personal
7. Negocio de interés general
8. Sin clasificar

En la empresa EPM Portovial actualmente se encuentra establecido estas políticas de seguridad de los grupos de Acceso total, Acceso restringido, Cámaras Nvr Hikvision y Acceso a celulares en el uso de un filtro URL estático para bloquear el acceso a un sitio web específico.

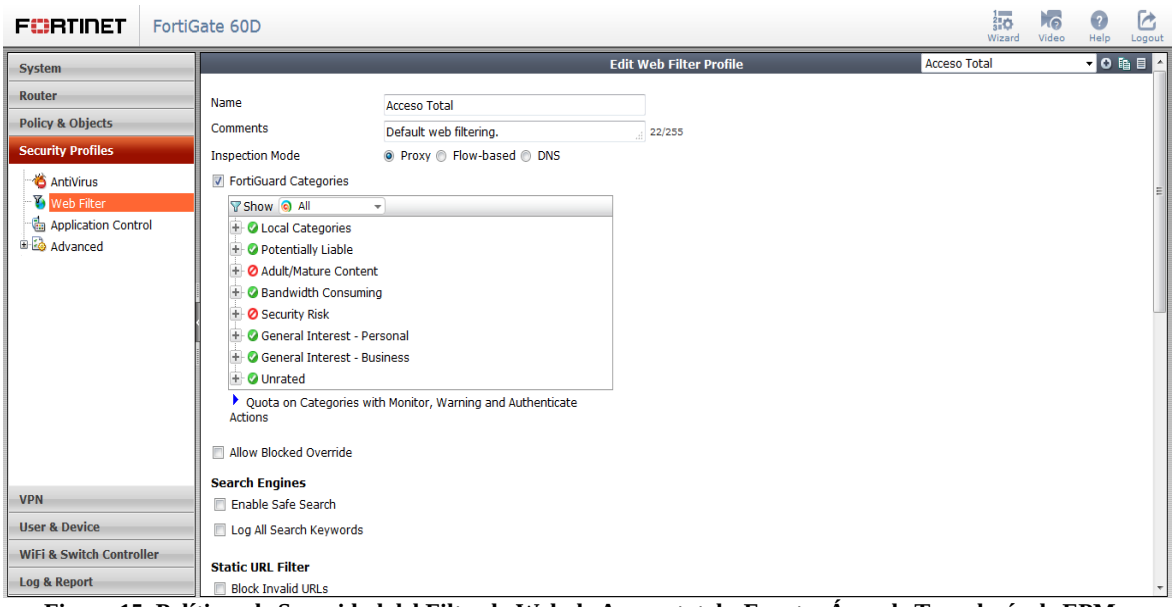


Figura 15. Políticas de Seguridad del Filtrado Web de Acceso total - Fuente: Área de Tecnología de EPM Portovial.

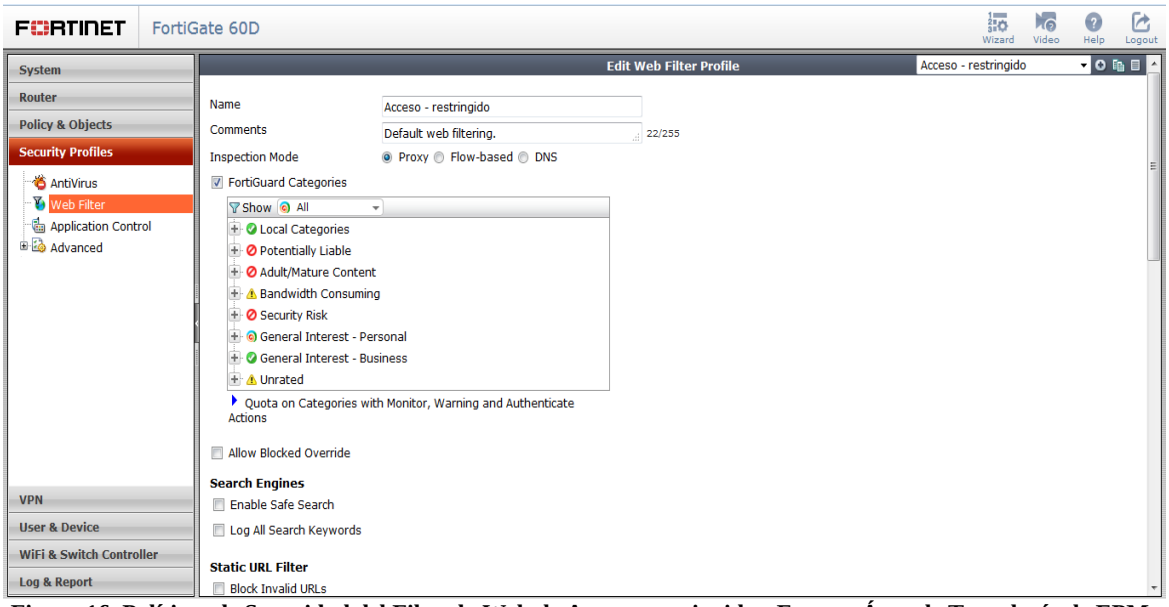


Figura 16. Políticas de Seguridad del Filtrado Web de Acceso restringido - Fuente: Área de Tecnología de EPM Portovial.

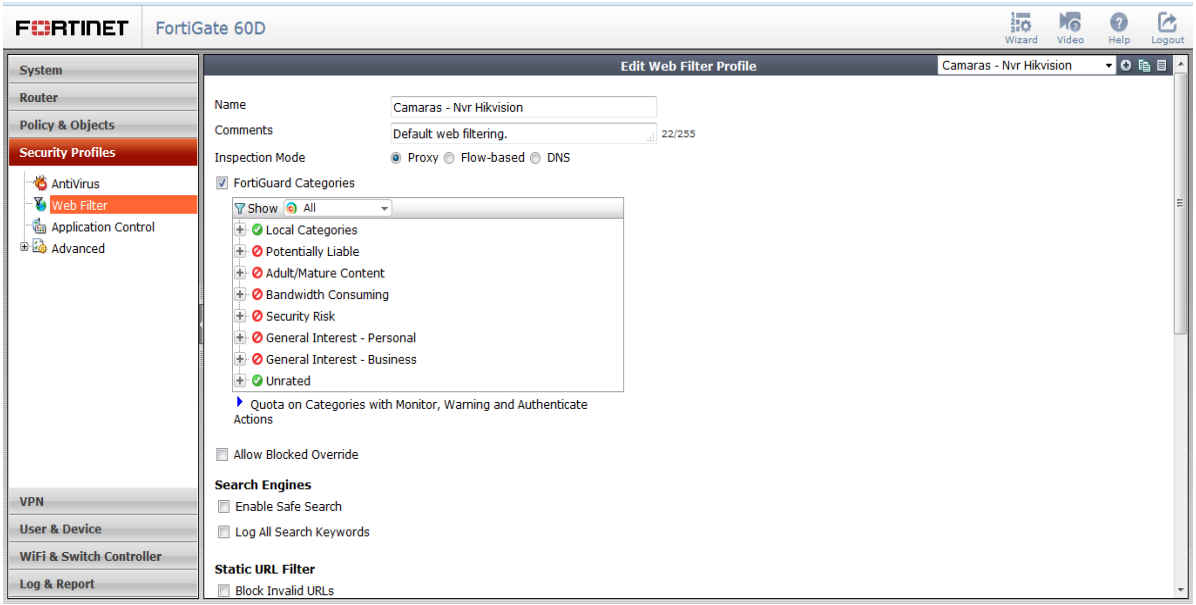


Figura 17. Políticas de Seguridad del Filtrado Web de Acceso Cámaras Nvr Hikvision - Fuente: Área de Tecnología de EPM Portovial.

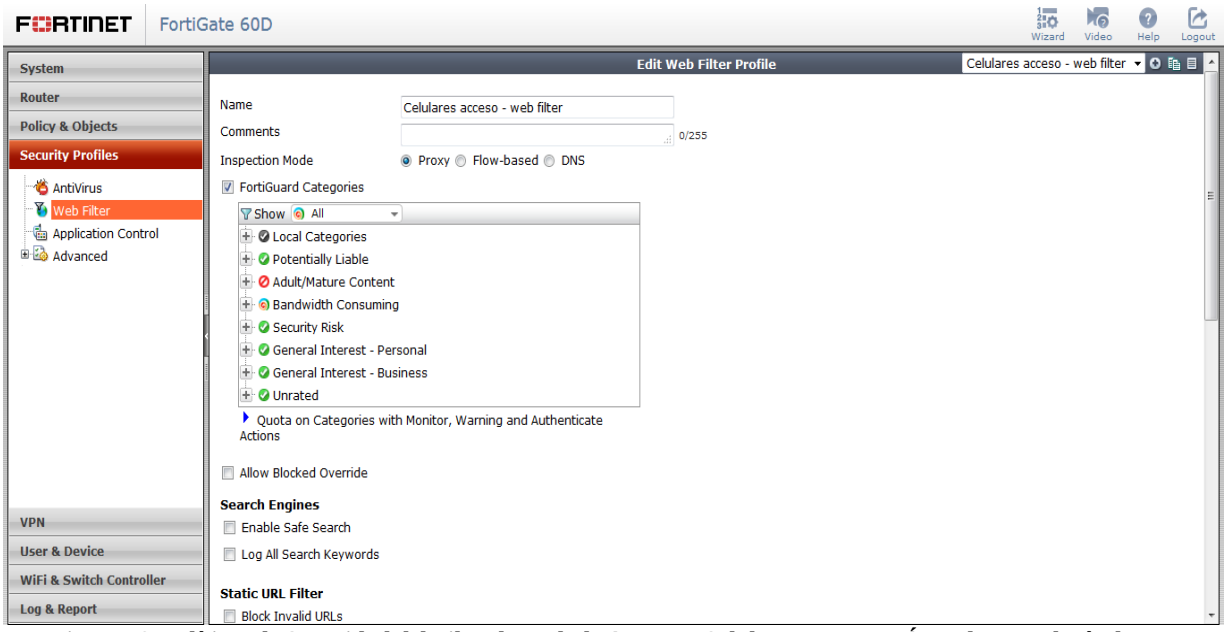


Figura 18. Políticas de Seguridad del Filtrado Web de Acceso a Celulares - Fuente: Área de Tecnología de EPM Portovial.

5.3 Análisis de Tráfico.

En la actualidad las redes de datos se han convertido en pieza fundamental en cualquier organización, y esta es la justificación principal del desarrollo del presente caso de estudio, ya que todas estas redes en algún momento se enfrentan a perdidas en el rendimiento por factores tanto internos como externos. También es de total conocimiento para cualquier administrador de red que no es fácil detectar estos problemas, pues en muchas ocasiones no es claro cuáles son los pasos a seguir y que herramientas utilizar, perdiendo mucho tiempo y dinero en personal externo calificado para realizar dicha labor y poder tener claras las causas del mal desempeño de la red.

El origen de la pérdida del rendimiento en una red de datos puede deberse a conflictos en direccionamiento IP, tormentas de broadcast, spanning-tree, flooding, enlaces redundantes, ataques hechos por terceros que intenten vulnerar la seguridad en algún

servidor usando ataques DoS (Denegación de Servicio), capturar tráfico con un envenenamiento ARP o infectar equipos para incluirlos en una red zombie.

Esta situación llevó a analizar la red, el tráfico que se genera a nivel de enlace, identificando toda la información que se transmite y la visualización de los paquetes, los bytes que transportan las tramas a nivel de enlace, volumen de tráfico cantidad de colisiones y ancho de banda utilizado.

Para este caso de estudio se utilizó un analizador de tráfico de red a nivel local como es el Wireshark, que proveerá toda la información del tráfico que se genere a nivel de la red LAN, mostrando en detalle cada una de las tramas IP que sean sospechosas de tráfico no deseado en una red al igual que su contenido para tomar decisiones de bloqueos.

Además a ello otra herramienta importante con que se contó para realizar este análisis de tráfico es la plataforma marca Fortinet – Fortigate 60D la cual está destinada a recolectar todos los datos que circulan desde la red LAN hacia Internet y enviarlas al dispositivo analizador de este tráfico. Desde esta plataforma podemos realizar controles con respecto al tráfico no deseado, además a ello se utilizó una herramienta adicional que se encuentra incorporada del Fortigate como es el FortiCloud que es un analizador de tráfico que proveerá informes detallados de tráfico web, estadísticas de acceso a Internet, cantidades de ancho de banda utilizado y otras estadísticas que se adjuntarán.

Best Effort: También conocido como QoS deficiente. Best effort es un servicio que presenta una conectividad básica pero sin garantía. Es caracterizado por colas tipo FIFO los cuales no presentan diferenciación entre flujos.

El crecimiento en el tráfico que circula por Internet así como la proliferación de servicios basados en ella han evidenciado las carencias del modelo Best-Effort. En este modelo, cualquier tráfico es tratado de la misma forma, es decir, no hay tráfico más prioritario que otro y la red solo se diseño para hacer lo mejor que pueda en hacer llegar un paquete a su destino, el cual resulta apropiado para aplicaciones clásicas de redes de datos como correo electrónico, la transferencia de archivos, la navegación en www y el comercio electrónico, que constituyen las aplicaciones Elásticas. Sin embargo, estas redes se utilizan cada vez más para transportar no sólo datos sino también flujos multimedia en difusión (por ejemplo, servicios de audio y video en streaming) e interactivos (por ejemplo, servicios de VoIP) conocidas como aplicaciones No Elásticas. ([3])

Calidad de Servicio (QoS): La Calidad de Servicio (QoS), se puede entender como la medida del comportamiento de la bondad de la red con respecto a ciertas características de los servicios definidos, o como la capacidad de una red para proveer mejor servicio para un determinado tipo de trafico. Los parámetros relacionados con QoS son: Ancho de Banda, nivel de retardo o latencia, variación del retardo o jitter, rendimiento o throughput, pérdida de paquetes. Una red debe garantizar; que puede ofrecer un cierto nivel de Calidad de Servicio para un nivel de tráfico con un conjunto especificado de parámetros.

La implementación de Políticas de Calidad de Servicio se puede enfocar en varios aspectos según los requerimientos de la red, los principales son:

- ✓ Determinar el ancho de banda de manera variada.
- ✓ Administrar y garantizar el flujo de los datos en la red.

- ✓ Aplicar preferencias al tipo de tráfico que esté cursando en ese momento.
- ✓ Permitir modelar el tráfico de toda la red. ([4])

En la actualidad la red de la Empresa Pública Municipal de Portovial no contempla estrategias de Calidad de Servicio; ya que el tráfico que pasa por ella, no posee un proceso diferencial, y lo que en si presenta la red es servicio de mejor esfuerzo para enviar y recibir los paquetes de la misma condición.

5.3.1 Herramientas Utilizadas para el Análisis de Tráfico de la Red Portovial

En base al mapeo inicial de la situación actual de la red de la Empresa Portovial, así como también al tamaño de la misma y a un sondeo de los principales protocolos y aplicaciones que se utilizan en la red se utilizaron herramientas de software que analicen el tráfico de tal manera que se pueda tener un patrón de comportamiento en base a los datos devueltos.

Wireshark: Anteriormente esta herramienta se la conocía como Ethereal, que es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos.

Para realizar este proceso del análisis del tráfico se utilizó una máquina conectada a la red LAN de la empresa donde se comenzó a capturar los datos de todos los protocolos durante horas laborales desde las 08:00 am hasta las 17:00 pm durante días intermedios teniendo los siguientes resultados.

En la figura 19 se muestran los diferentes protocolos capturados durante el análisis, ya que existen estaciones de trabajo que se encuentran iniciando sesiones y otros que ya lo han hecho, debido que a están enviando peticiones a direcciones de broadcast y spaningtree.

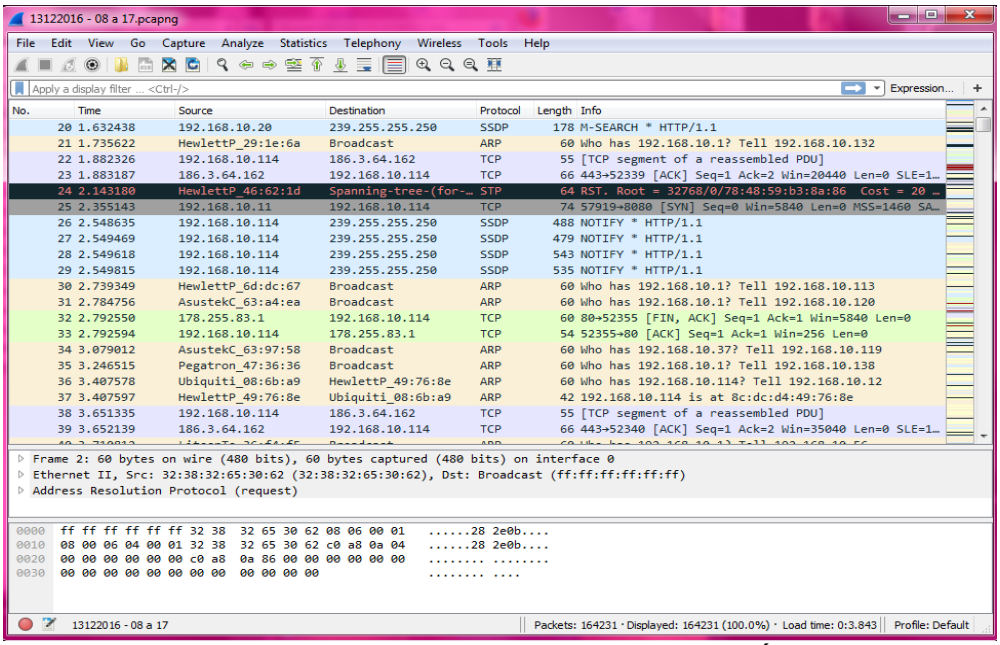


Figura 19. Análisis del Tráfico Mediante la Herramienta Wireshark - Fuente: Área de Tecnología de EPM Portovial.

Ahora en la figura 20 se muestra la opción I/O Graph de Wireshark, el tráfico de los equipos, en donde la línea negra corresponde a la cantidad de paquetes que pasan por el equipo. Es importante tener en cuenta que el eje vertical utiliza una escala logarítmica para facilitar visualizar la cantidad de paquetes en cada unidad de tiempo.

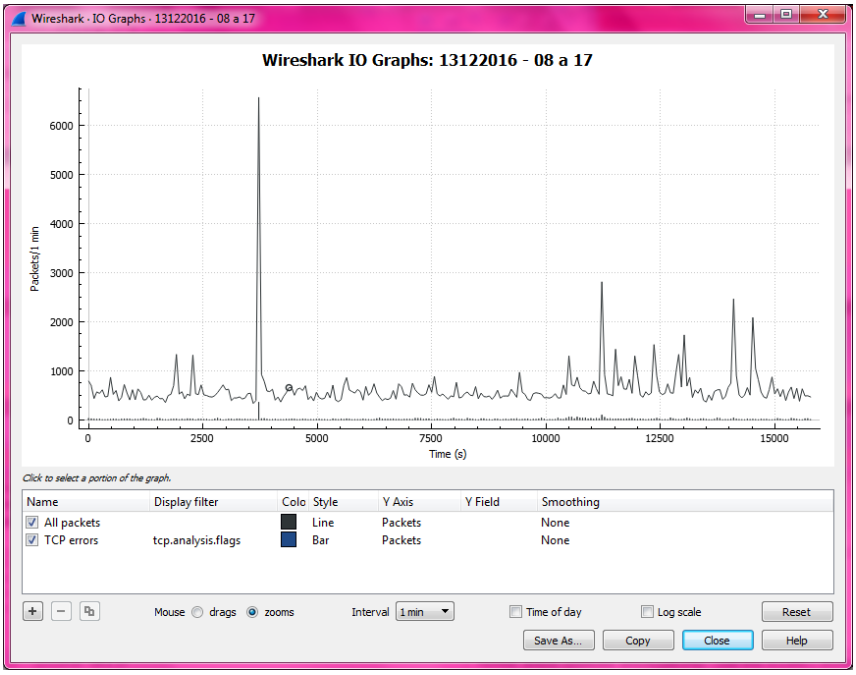


Figura 20. Análisis del Tráfico Mediante el I/O Graph- Fuente: Área de Tecnología de EPM Portovial.

Para respaldar la información realizada con el análisis en el Wireshark, esta vez utilizaremos el Firewall del Fortigate 60D.

Fortigate 60D: Para realizar el análisis del tráfico con esta herramienta se utilizó la opción Sistema de Log y Report donde permite realizar lo siguiente:

- ✓ Funcionalidades de gestión de logs y generación de informes. Proporciona un registro de eventos del funcionamiento antivirus, antispam, etc., así mismo posibilita la generación de informes a medida en diversas modalidades, como la personalizada y la planificada.
- ✓ Centralización de logs:

  Posibilidad de almacenar eventos en memoria, discos duros o envió de información a un sistema de FortiCloud.

- ✓ El archivado de contenidos permite guardar información relevante: SMTP, POP3, FTP, HTTP, IM.
- ✓ Espacio reservado para cuarentena de antivirus.
- ✓ Alertas por email para eventos críticos.

En la figura 21 se muestra la interfaz de la herramienta FortiCloud la mima que no va ayudar a realizar el análisis y consumo del ancho de banda de las diferentes interfaces y protocolos, el filtrado web, etc.

El FortiCloud es un servicio de retención de logs que nos ayuda a administrar la gestión de la seguridad de nuestros firewalls Fortigate de una manera más visual.

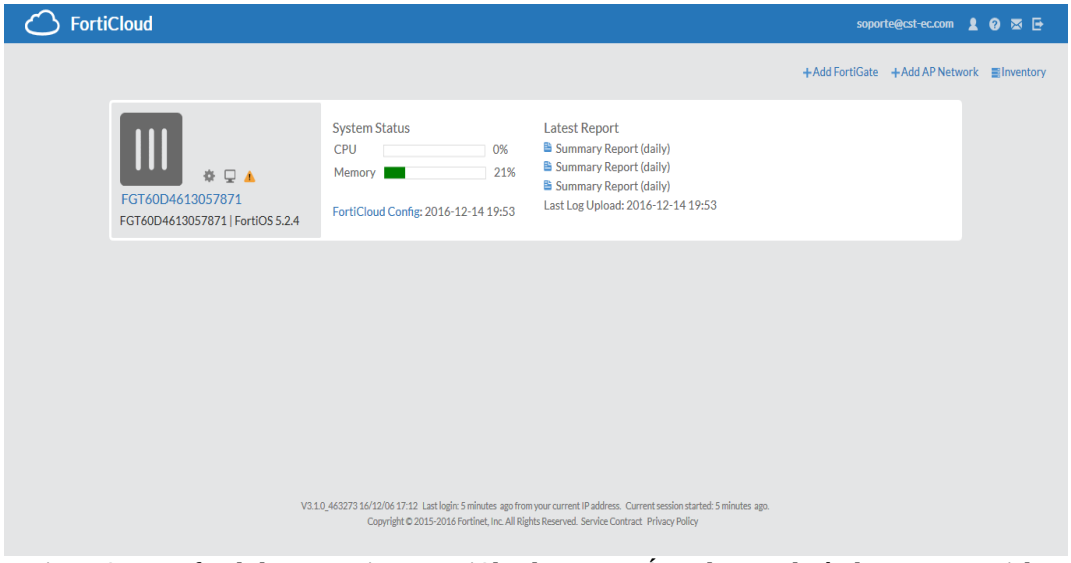


Figura 21. Interfaz de la Herramienta FortiCloud - Fuente: Área de Tecnología de EPM Portovial.

En la figura 22 se realizó un análisis desde la interfaz Internal 1 (LAN) hacia la interfaz de la Internal (Datos); cabe mencionar que este análisis se lo realizó en un periodo de

resumen de los últimos 7 días desde el 2016/12/07 00:00:00 hasta 2016/12/08 00:00:00, teniendo los siguientes resultados. (Tráfico superior por protocolo).

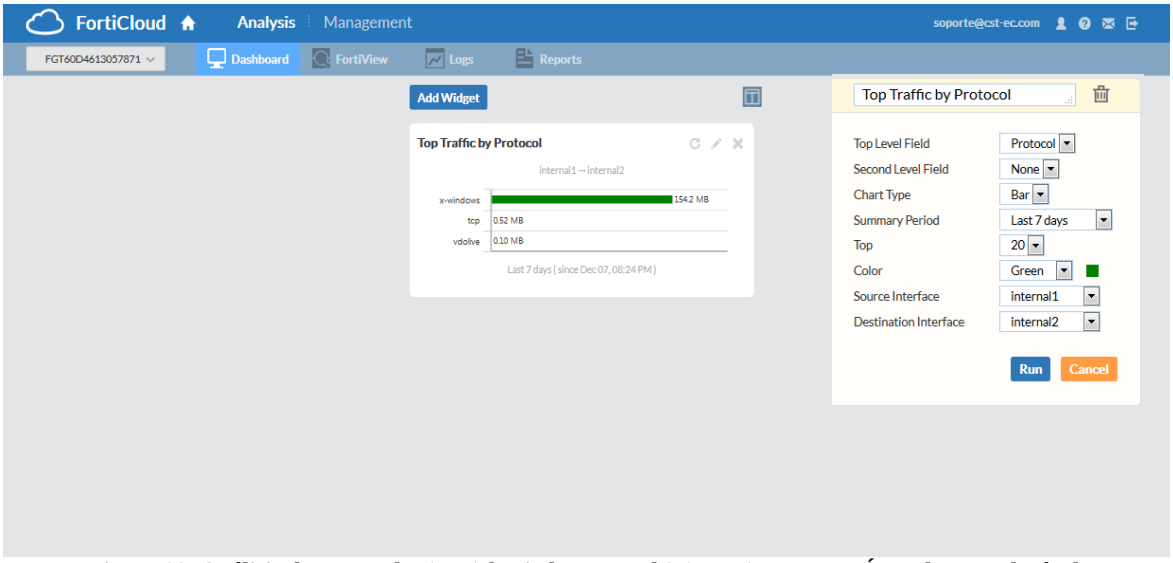


Figura 22. Análisis de Internal 1 (Lan) hacia la Internal 2 (Datos) - Fuente: Área de Tecnología de EPM Portovial.

Ahora analizaremos desde la interfaz de la Internal 1 (Lan) hacia la Interfaz de la Wan 2 (Internet), utilizando los últimos 7 días desde el 2016/12/07 00:00:00 hasta 2016/12/08 00:00:00.

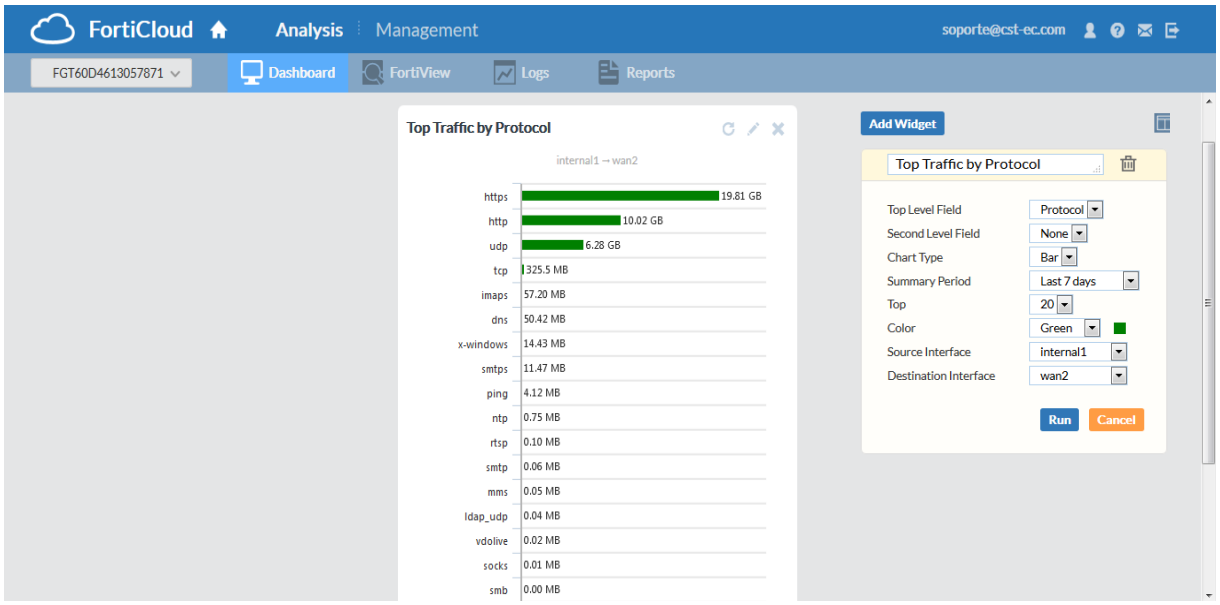


Figura 23. Análisis de Internal 1 (Lan) hacia la Wan 2 (Internet) - Fuente: Área de Tecnología de EPM Portovial

Luego vamos a realizar un análisis del historial de tráfico de las tres intefaces: Internal 1 (Lan), Intertnal 2 (Datos) y Wan 2 (Internet) de los últimos 7 días.

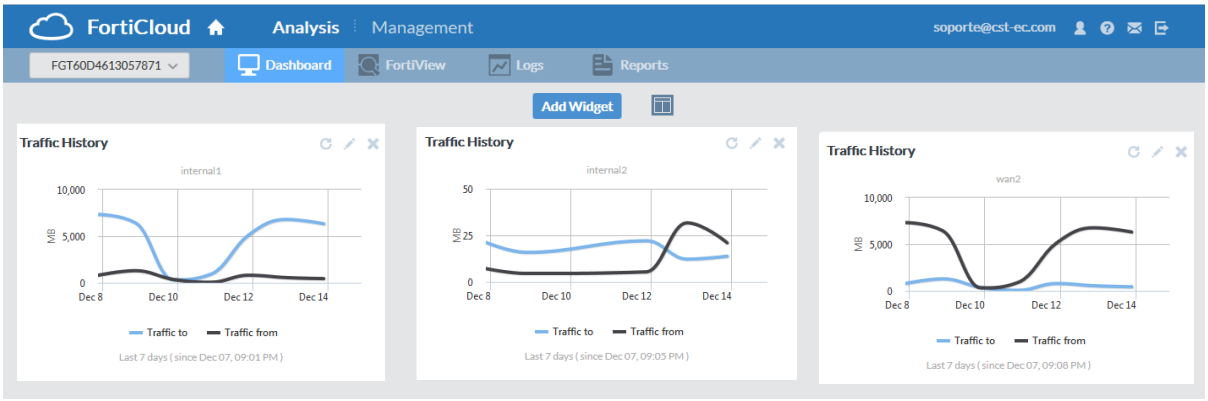


Figura 24. Análisis del Historial de Tráfico Internal 1 (Lan) Intertnal **2 (Datos) y Wan 2 (Internet). - Fuente: Área de Tecnología de EPM Portovial.**

Una vez obtenido el historial de tráfico realizaremos el siguiente análisis por los pprincipales sitios visitados por los usuarios de la red de Portovial durante los últimos 7 días.

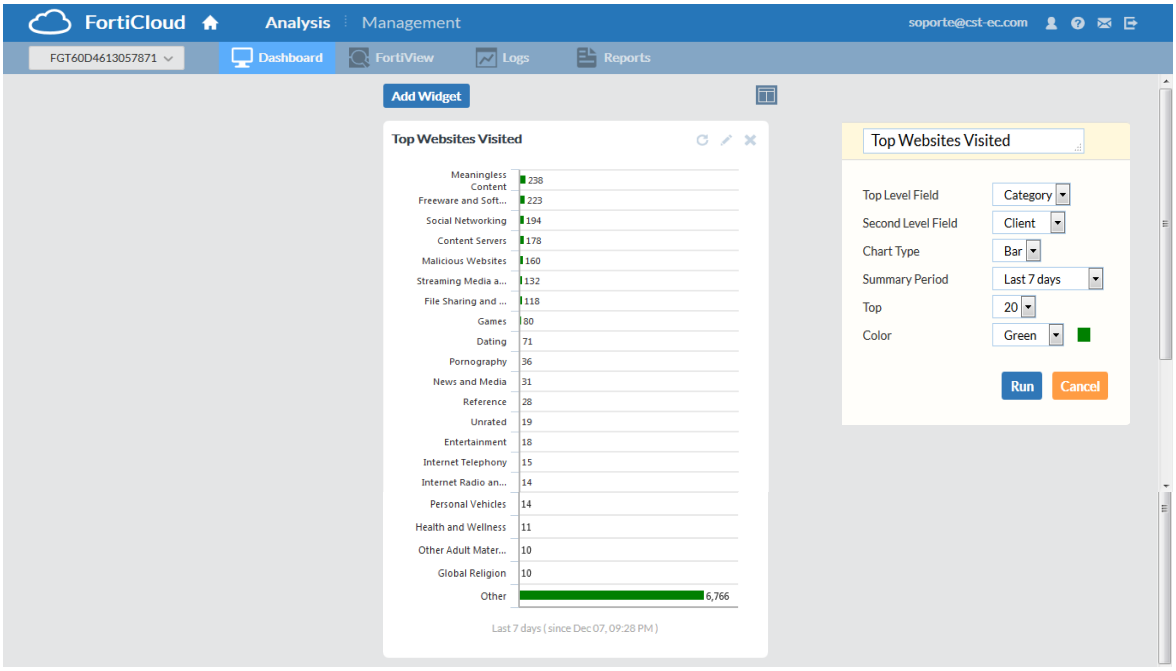
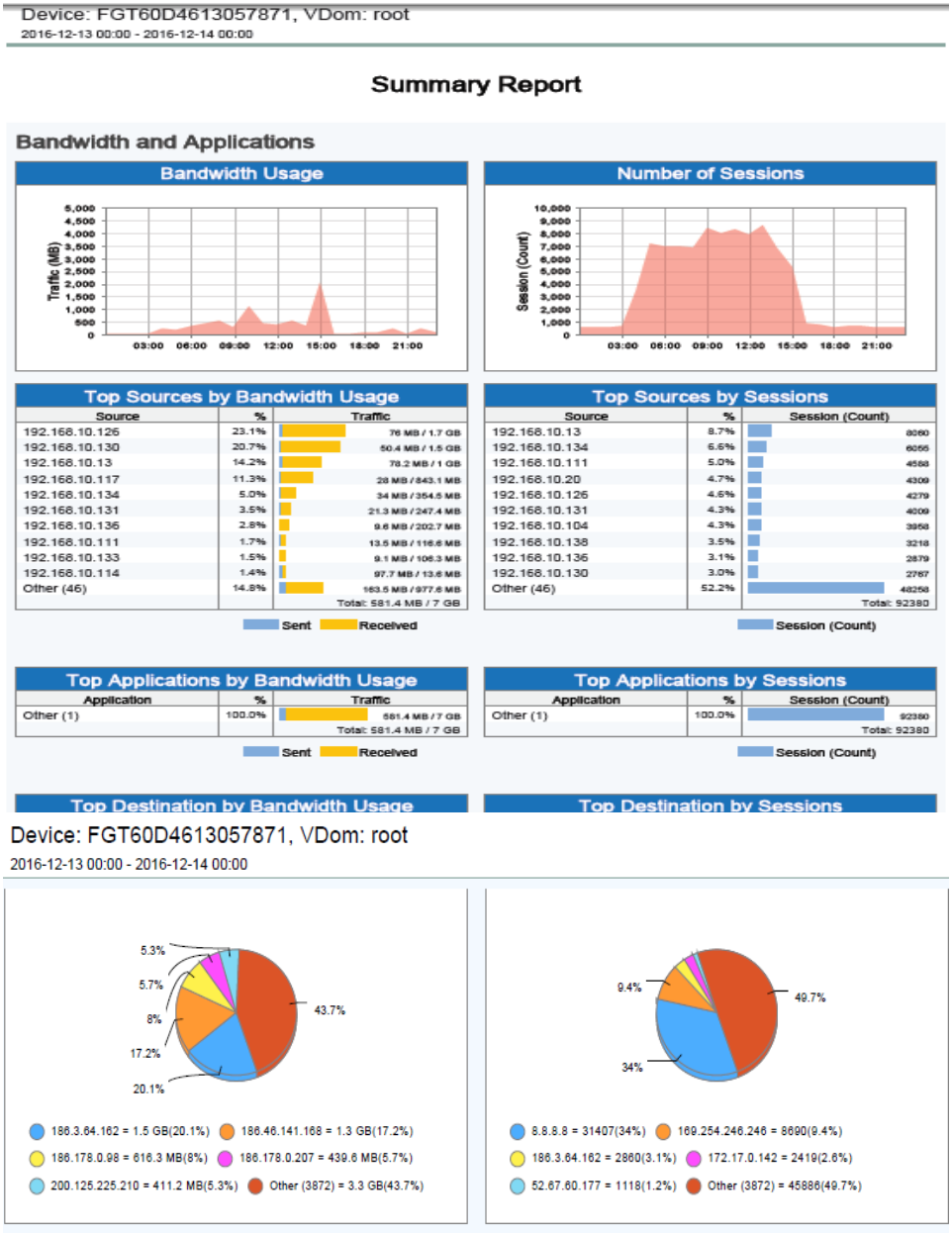


Figura 25. Análisis de los Principales Sitios Visitados por los Usuarios - Fuente: Área de Tecnología de EPM Portovial.

5.3.2 Resumen del Análisis de Tráfico de la Red Portovial.

Una vez realizado el análisis de tráfico de la red de Portovial por medio del Fortigate 60D y con la ayuda de la herramienta FortiCloud se tomaron en cuenta que se debían hacer cambios en los distintos grupos de acuerdo a los perfiles y políticas de seguridad para bajar el consumo del ancho de banda por parte de los usuarios, es por esta razón se muestra a continuación un resumen del análisis realizado.



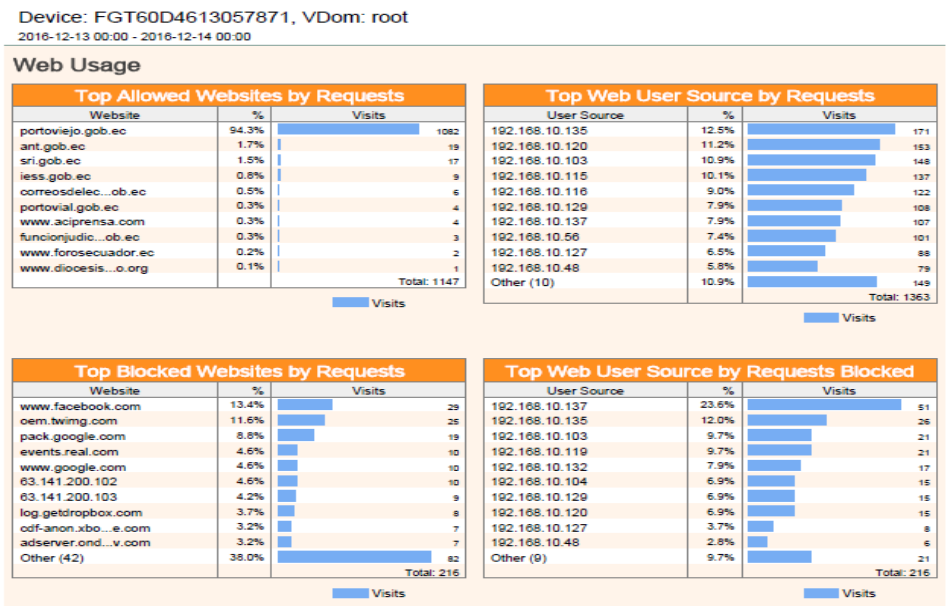


Figura 26. Resumen del Análisis de Tráfico Fortigate 60D - Fuente: Área de Tecnología de EPM Portovial.

5.4 Propuesta para la implementación de QoS.

5.4.1 Definición.

Para poder implementar QoS en una red es importante conocer el tipo de usuario que se tiene y saber cuáles serán las aplicaciones o servicios necesarios para realizar el trabajo de dichos usuarios, esto es con el fin de poder hacer una diferenciación de tráfico y así establecer prioridades. Además se debe valorar el sistema operativo en el cual se va a trabajar, tomando en cuenta sus ventajas y desventajas tanto como en su desempeño.

Dentro de una red convergente el propósito más importante de la Calidad de Servicio, son los datos, voz y video que cohabitan sin ocasionar inconvenientes en los parámetros de transmisión. Estos parámetros al momento de transmitir los datos son los que perjudican la Calidad del Servicio como la pérdida de paquetes, ancho de banda, demora, fiabilidad y la inestabilidad.

5.4.2 Parámetros de la Calidad de Servicio (QoS).

Tanto en el caso del tráfico que corresponden a aplicaciones elásticas y no elásticas, así a noción de QoS es muy importante y está definida como un conjunto de parámetros que representan las propiedades de los ([5])tráficos. En general existen los ([6]) siguientes parámetros:

- **Retardo (Delay):** Se refiere al tiempo que dura en transmitirse un bit desde su origen hasta su destino. Es un parámetro que se emplea para medir el máximo retardo en una red de extremo a extremo. El retardo es ocasionado por la distancia, errores en la transmisión (bits errados), las capacidades de procesamiento de los sistemas que están involucrados en la transmisión, y otros factores.
- **Variabilidad (Jitter):** Expresa la variación experimentada entre dos retardos consecutivos durante la transmisión y procesamiento de datos. El Jitter puede amortiguarse mediante el incremento de buffers (buffering) en los receptores lo que a su vez, incrementa el retardo extremo a extremo.

- **Pérdida de Paquetes o Fiabilidad (Reliability):** Está referida a la pérdida de paquetes y corrupciones de datos durante la transferencia de datos. Cuando ocurre congestión en una red, los paquetes tienden a caerse debido a un sobre flujo del buffer o debido al esfuerzo límite de retardo. Las pérdidas de paquetes afectan directamente la visión de la Calidad de Servicio en el lado del receptor extremo.

- **Ancho de Banda (Bandwidth):** Es la capacidad de transportar información a través de un canal de comunicación. Este canal puede ser analógico o digital. En la transmisión analógica tal como en telefonía, radiodifusión (AM o FM), es medido en ciclos por segundo (Hertz). En la transmisión digital (velocidad de transmisión) es medido en bits ([7]) por segundo. Para sistemas digitales, los términos Ancho de Banda (Bandwidth) o Capacidad (Capacity) se usan indistintamente.

- **Latencia (Latency):** Un método para medir la Latencia es ver cuánto tiempo se demora un dispositivo en procesar un paquete. Este dispositivo puede ser un router, un sistema completo de comunicaciones que incluye routers y enlaces, en muchos casos hablar de Latencia es sinónimo de Retardo (Delay).

Parámetro	Unidades	Significado
Ancho de Banda (bandwidth)	Kb/s	Indica el caudal máximo que se puede transmitir
Retardo (delay) o latencia (latency)	ms	El tiempo medio que tardan en llegar los paquetes
Jitter	ms	La fluctuación que se puede producir en el Retardo
Tasa de pérdidas (loss rate)	%	Proporción de paquetes perdidos respecto de los enviados

Tabla 7. Parámetros de QoS - Fuente: ([8])

5.4.3 Modelos para la Obtención de QoS.

QoS o calidad de servicio tienen diferentes modelos de implementación que se muestran a continuación que son los siguientes:

5.4.3.1 Best-Effort.

Este modelo se aplica al Internet y a las redes de datos que no tienen políticas explicitas. Esta no garantiza ningún tratamiento especial para los datos ni aplicaciones, las principales características del modelo son:

- ✓ Escalable.
- ✓ Fácil de configurar.
- ✓ No garantiza recursos, ni diferencia servicios. ([9])

5.4.3.2 IntServ.

Este modelo de implementación es bajo demanda. El objetivo fundamental es garantizar que los recursos estén disponibles en la ruta de una aplicación específica.

Cuando se inicia la sesión de la aplicación se señala la ruta para validar la disponibilidad de los recursos de la red de datos. Sus características son:

- ✓ Negocia las condiciones de QoS antes de que inicie la comunicación propia.
- ✓ Cuando se realiza la reserva, la aplicación utiliza los recursos reservados más allá de la situación de tráfico de la red.
- ✓ Se adecua a las demandas específicas y diferentes de cada tipo de aplicación.
- ✓ Reserva recursos para cada flujo de información.

- ✓ No es escalable en redes de gran tamaño.
- ✓ Usa servicios Resource Reservation Protocol. ([10])

5.4.3.3 DiffServ.

Este modelo garantiza el modo genérico y no por flujos. Garantiza diferentes condiciones de servicios para diferentes tipos de tráfico, modo Escalante y efectivo en la red.

- ✓ No requiere señalización.
- ✓ No garantiza condiciones de tráfico extremo a extremo.
- ✓ Flexible y Escalante.
- ✓ Divide el tráfico en función de los requerimientos de la organización.
- ✓ Cada paquete recibe el tratamiento especial y diferenciado.
- ✓ El mecanismo de implementación es complejo. ([11])

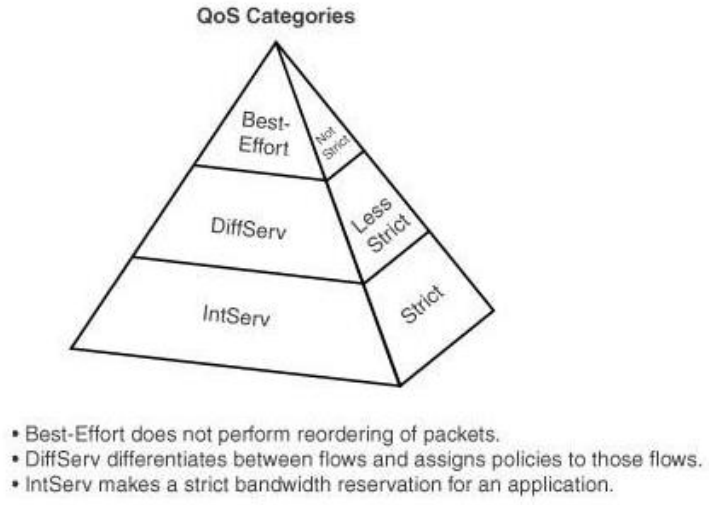


Figura 27. Modelo de QoS - Fuente: ([12])

5.4.4 Mecanismos de QoS.

Los mecanismos de QoS proporcionan a la red de datos la capacidad de asegurar; con un grado de fiabilidad, donde se deben cumplir los requisitos de tráfico necesario en términos de perfil y ancho de banda, con el objetivo de brindar y garantizar servicios útiles a toda la red.

A continuación se explicarán los siguientes mecanismos de QoS.

- **Mecanismos de Prioridad:** Se refiere a la capacidad de los diferentes tratamientos al retardo, es decir los paquetes de mayor prioridad son los primeros en liberarse antes de los de menor prioridad.
- **Mecanismos de Identificación de Tráfico:** Este proceso se lo hace mediante la dirección origen y dirección destino, identificando el número de puerto y tipos de protocolos como por ejemplo TCP y UDP.
- **Mecanismos de Marcado de Paquetes:** Se lo realiza diferenciando los tipos de tráfico empleando una etiqueta para sellar las varias formas de etiquetado, utilizando la cabecera de nivel 2 o nivel 3. ([13]) ([14])
- **Mecanismos de Ordenamiento de Paquetes:** Para realizar este procedimiento primero se debe preferir un paquete para la transmisión desde la cola de paquetes, luego este proceso continúa eligiendo que paquete y desde que cola y estación están establecidos para la transmisión dejando claro el periodo de tiempo.
- **Mecanismos de Control de Tráfico:** Controlan las sesiones de tráfico admitidos para que no violen las reglas de QoS, asegura que todo el tráfico que pase a través de este siga las reglas conforme a los parámetros del tráfico.

5.4.5 Herramientas de QoS.

Actualmente las herramientas disponibles para ofrecer QoS son los sistemas de colas y priorización de datos, los cuales tienen como objetivo hacer una distribución del tráfico para incrementar la eficiencia de la red. Las herramientas más conocidas para llevar a cabo son los siguientes:

- **Fifo (First In, First Out – Primero en entrar, primero en salir):** Los paquetes son enviados en el mismo orden en el que llegan a la interfaz, es el mecanismo con que se trabaja por default en una red IP.
- **PQ (Priority Queuing – Cola con Prioridad):** Se da la prioridad estricta al tráfico importante, se basa en la prioridad del tráfico de varios niveles el cual puede aportar el encabezado del paquete IP, estos niveles pueden ser alto, medio, normal y bajo.
- **CQ (Custom Queuing – Encolamiento Personalizado):** Garantiza el ancho de banda mediante una cola de espera programada, reserva un porcentaje del ancho de banda disponible para tipo de tráfico seleccionado.
- **RED (Random Early Detection, Gestión de la Congestión):** Evita congestión, se encarga de monitorear el tráfico al azar, si la congestión aumenta elimina paquetes, al darse cuenta que el tráfico sube, disminuye la velocidad de transmisión de paquetes.
- **GTS (Generic Traffic Shapping, Regulación del Ancho de Banda):** Retrasa el exceso de tráfico al usar buffers para modelar el flujo, con lo que reduce el tráfico saliente limitando el ancho de banda de cada tráfico específico y si excede el ancho de banda establecido es enviado a una cola de espera.

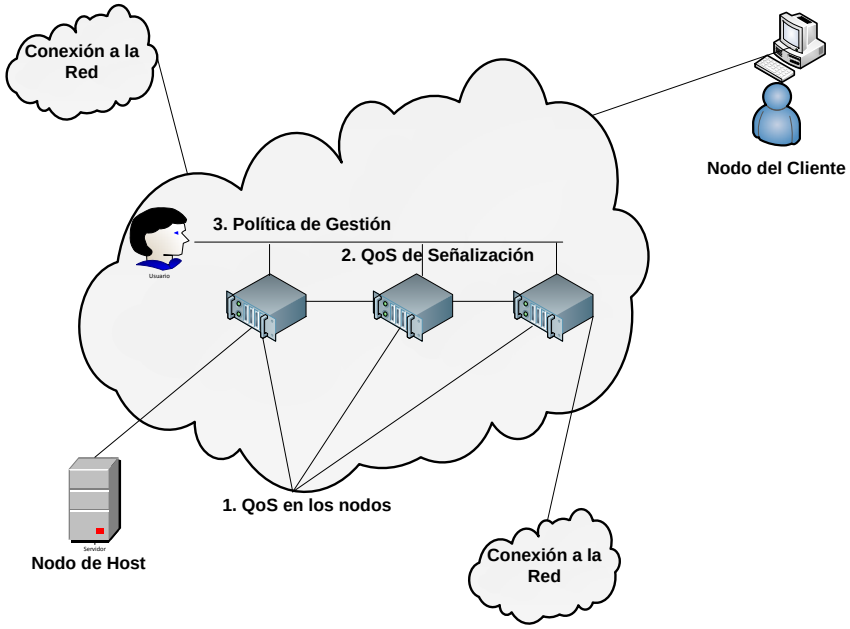


Figura 28. Arquitectura Básica de una Red con QoS. - Fuente: Área de Tecnología de EPM Portovial.

6. Conclusiones y Recomendaciones.

Luego de haber realizado el estudio con su respectivo análisis a la red de la Infraestructura de la red de Portovial, se identificaron los problemas actuales, los datos obtenidos en el instrumento de recolección de datos permitieron llegar a las siguientes conclusiones y recomendaciones:

6.1 Conclusiones.

- El análisis realizado a la Infraestructura de la red de la Empresa Portovial permitió conocer las necesidades e inconvenientes que presenta la misma al ser consciente de la importancia de tener un monitoreo periódico de la red y tener muy claros los conceptos básicos para analizar los datos que se capturen. Con estos conocimientos se pueden controlar los paquetes dañinos que circulan por la red sin control y así poder tener un mejor aprovechamiento del medio.

- El tener una herramienta muy eficaz como es el Fortigate 60D, este nos ayudó a determinar el consumo del ancho de banda de los diferentes interfaces implementadas en el equipo mediante el Traffic Shapers, así mismo poder colocar políticas de seguridad a cada uno de los grupos creados con el objetivo de cuidar la vulnerabilidad de los datos.
- Se queda demostrado que la topología de la red que se tiene actualmente en la empresa está dada Best Effort (mejor esfuerzo), por lo que no existe Calidad de Servicio (QoS), cuyo objetivo es permitir entender la medida del comportamiento de la red con respecto a ciertas características de los servicios definidos, o como la

capacidad de la red para proveer mejor servicio para un determinado tipo de tráfico.

- Existen varios mecanismos para la implementación de Calidad de Servicio en redes de datos, entre los cuales el método DiffServ es el más utilizado debido a que brinda versatilidad al no reservar previamente recursos de red ni introducir sobrecarga en la red para brindar Calidad de Servicio.
- Se concluye que el monitoreo continuo del tráfico de datos permite realizar una evaluación apropiada del comportamiento de la red en tiempo real. Entre los parámetros recomendados para evaluar están la cantidad de tráfico, el uso del ancho de banda y el porcentaje de utilización.

6.2 Recomendaciones.

- Las colisiones son una parte inherente del diseño y operación de una red LAN Ethernet IEEE 802.3, entre más nodos sean agregados a la red, la probabilidad de tener colisiones aumenta; agregando más nodos a la red, también se incrementa la utilización del ancho de banda. La forma más recomendable de lograr eficientemente altos promedios de utilización del ancho de banda, es por medio de la segmentación de la red con algún mecanismo que permita por ejemplo la utilización y el manejo de Vlans.
- Antes de aplicar QoS a cualquier red, se debe evaluar los terminales a configurar y las necesidades de la empresa a aplicar.
- Si en su momento la empresa Portovial llegase a implementar Calidad de Servicio se recomienda que el proceso de QoS se extienda hacia otras áreas ofreciendo

servicios integrados de internet, datos, VoIP y video, permitiendo tener mayores recursos en la red.

- Finalmente se recomienda restructurar las políticas de seguridad en el Fortigate 60D, ya que con esto se puede controlar el consumo del ancho de banda y el uso eficiente del internet, ya que un usuario no autorizado podría estar haciendo uso indiscriminado de los recursos de la red.

7. Bibliografía.

[1]. X. Xiao, L. Ni, “Internet QoS: ABig Picture” IEEE Network Magazine, 1999.

[2]. R. Branden, L. Zhang, S. Herzog, S. Jamin, “Resourse ReserVation Protocol (RSVP) – Version 1 Functional Specification “ IETF Standards Track RFC 2205, September.

[3]. Centro de Comunicaciones Avanzadas de Banda Ancha, “Internet 2 a Catalunya (I2CAT)”, Febrero 1999 http://www.ccaba.upc.es.

[4]. Cisco, “Internetworking Technology Handbook”, capitulo “Quality of Service (QoS)” Diciembre 2003.

[5]. Rec. I.350 “Aspectos generales de Calidad de Servicio y de Calidad de Funcionamiento en las Redes Digitales Incluidas las Redes Digitales de Servicos Integrados", ITU-T,1993.

[6]. Rec. E.800 “Terms and Definitions Related To The Quality of Telecommunications Services”, CCITT, 1988.

[7]. Tom Sheldon “ Encyclopedia of Networking and Telecommunications” Mc Graw Hill, 2001.

[8]. eslared.org.ve. (2012). www.eslared.org.ve. Recuperado el 2013, de www.eslared.org.ve: www.eslared.org.ve walcs walc2004 apc-aa archivos... Practica QoS.doc.

[9]. GEROMETTA, Oscar. “Modelos de implementación de QoS”. 2010.

[10]. GEROMETTA, Oscar. “Modelos de implementación de QoS”. 2010.

[11]. GEROMETTA, Oscar. “Modelos de implementación de QoS”. 2010.

[12]. Wallace., K. (2004, Noviembre 24). http://www.ciscopress.com. Retrieved 2013, fromhttp://www.ciscopress.com:http://www.ciscopress.com/articles/article.asp?p = 352991&seqNum=4.

[13]. Traffic Control HOWTO,http://www.tldp.org/HOWTO/Traffic-Control-HOWTO/sostware.html#s-IProute2.

[14]. Calidad de Servicio en Redes de Servicios Diferenciados, http://www.tid.es/presencia/publicaciones/comsid/esp/24aart5.pdf.

8. Anexos.

Anexo 1. Nuevas instalaciones de la Empresa Portovial

Anexo 2. Área de Matriculación Vehicular

Anexo 3. Área de Información Vehicular

Anexo 4. Área de Revisión Técnica Vehicular – RTV

Anexo 5. Área Administrativa