FACULTAD DE INGENIERÍAS Y CIENCIAS APLICADAS

DISEÑO E IMPLEMENTACION DEL SISTEMA DE PREVENCION Y DETECCION DE INTRUSIONES EN LA EMPRESA PROAUTO C.A.

AUTORES

HERNANDEZ ORTIZ DANIEL ALEJANDRO

SANTANA BARRIONUEVO ALBERTO CARLOS

AÑO

2018

FACULTAD DE INGENIERÍAS Y CIENCIAS APLICADAS

DISEÑO E IMPLEMENTACION DEL SISTEMA DE PREVENCION Y DETECCION DE INTRUSIONES EN LA EMPRESA PROAUTO C.A.

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingenieros en Redes y Telecomunicaciones

Profesor Guía

Msc. Milton Neptalí Román Cañizares

Autores

Daniel Alejandro Hernández Ortiz.

Alberto Carlos Santana Barrionuevo.

Año

2018

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido el trabajo, **Diseño e implementación del sistema de prevención y detección de intrusiones en la empresa PROAUTO C.A.,** a través de reuniones periódicas con los estudiantes **Daniel Alejandro Hernández Ortiz y Alberto Carlos Santana Barrionuevo**, en el semestre **2018-2**, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación."

_____

Milton Neptalí Román Cañizares

Magister en Gerencia de Redes y Telecomunicaciones

CC: 050216344-7

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado, **Diseño e implementación del sistema de prevención y detección de intrusiones en la empresa PROAUTO C.A.** de **Daniel Alejandro Hernández Ortiz y Alberto Carlos Santana Barrionuevo**, en el semestre **2018-2**, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Iván Patricio Ortiz Garcés

Magister en Redes de Comunicaciones

CC: 060235677-6

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Daniel Alejandro Hernández Ortiz.	Alberto Carlos Santana Barrionuevo.
CC: 172128461-8	CC: 172025887-8

AGRADECIMIENTOS

Quiero dar mis más sinceros agradecimientos a mi Tía Dra. Dora Ortiz T. por el cariño y la confianza que me ha brindado en mi vida.

Por último, quiero agradecer de manera especial a mis amigos Edison y Alberto y a todas las personas que de alguna forma colaboraron con el desarrollo de este proyecto de titulación.

Daniel H.

DEDICATORIA

Dedico este logro con mucho cariño a mis Padres Willan y Celia quienes son y serán los pilares fundamentales en mi vida. Gracias por su apoyo, confianza, cariño y entrega incondicional, sin ustedes nada de esto fuera posible.

De igual manera a mis hijos: Santiago y Danilo, por haber sido el mejor regalo que me ha brindado la vida y convirtiéndose en la inspiración para poder salir adelante.

Por último. A mi amada esposa. Carolina R, por su comprensión y compañía en la ejecución de este proyecto.

Daniel H.

AGRADECIMIENTOS

Yo; Alberto Carlos Santana Barrionuevo, quiero agradecer de manera especial a mi madre ya que con su apoyo y sus enseñanzas inculcadas hacia mi persona dieron como resultado la consecución de este proyecto.

A mi amada esposa quien con su apoyo incondicional fue parte importante de la culminación de este proyecto.

A mis amigos Gabriel y Daniel por su gran apoyo en el desarrollo y consecución del proyecto.

Alberto S.

DEDICATORIA

Este proyecto está dedicado a mi madre y mi abuelo, quienes inculcaron en mis valores y objetivos los mismos que dieron como resultado la finalización de este proyecto.

A mi amada esposa Mélida, quien siempre estuvo a mi lado con su incondicional apoyo.

A mis primos que con sus consejos y apoyo continuo permitieron sea posible la realización de este proyecto.

Alberto S.

RESUMEN

El presente documento detalla la implementación de un sistema de prevención y detección de intrusiones en la empresa PROAUTO C.A, capaz de prevenir el robo de información y detectar comportamientos anormales en la red de datos a través de la implementación de una solución de software libre basado en la distribución conocida con el nombre de SURICATA IPS-IDS.

Esta solución contiene algoritmos, conforme a los lineamientos de la norma ISO 27001, así como las pruebas de funcionamiento y operatividad del sistema acorde al fundamento teórico en temas de seguridad de la información, tipos, métodos contingentes y riesgos.

Por medio del software Suricata se realizará la implementación de sensores virtuales o sniffers que actuarán de manera granular en toda la red de datos para posteriormente con los resultados obtenidos del análisis inicial realizar la creación de reglas ACL's (Access Control List) basadas en algoritmos de inteligencia artificial.

En base al estudio efectuado y su respectiva documentación, el administrador de la red podrá obtener información que le facilite la toma de decisiones frente a las vulnerabilidades detectadas en la empresa. La solución presentará los datos de una manera estadística y cronológica, denotando irregularidades en el comportamiento de la red.

El sistema de prevención y detección de intrusiones estará alineado a la norma de seguridad de la Información ISO 27001, garantizando que la solución sea actualizable y permita la creación de políticas de seguridad en base a los riesgos detectados.

ABSTRACT

This document details the implementation of a system of prevention and detection of intrusions in the company PROAUTO CA, capable of preventing the theft of information and the behavior of abnormal behavior in the data network through the implementation of a software solution free based on the distribution known as SURICATA IPS-IDS.

This solution contains algorithms, in accordance with the guidelines of the ISO 27001 standard, as well as the tests of operation and functioning of the system according to the theoretical foundation on issues of information security, types, contingent methods and risks.

Through Suricata software, the implementation of virtual sensors or sniffers that granularly perform all the information in the access list of ACL (Access Control List) in artificial intelligence algorithms.

Based on the study carried out and its respective documentation, the network administrator can obtain information that will help him to make decisions regarding the vulnerabilities detected in the company. The solution presents the data in a statistical and chronological manner, denoting irregularities in the behavior of the network.

The system of prevention and detection of intrusions will be aligned with the security standard of the Information ISO 27001, guaranteeing that the solution is updatable and allows the creation of security policies based on the detected risks.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN.

El siguiente trabajo consiste en proveer a la empresa PROAUTO C.A. un sistema de prevención y detección de intrusiones el cuál permita prevenir, identificar y registrar eventos de seguridad que tengan lugar en la red corporativa.

PROAUTO C.A. inició sus actividades en el año de 1989 en la ciudad de Quito con la importación de camiones. En 1992 inicia la comercialización de vehículos livianos, venta de repuestos y servicios de taller, operaciones que mantiene hasta la actualidad categorizadas en dos ramas principales: venta de vehículos y taller mecánico tanto para *retail* como para flotas; siendo la venta de flotas y vehículos livianos las líneas más importantes del negocio. (PROAUTO C.A, s.f.)

Es un concesionario autorizado por General Motors para comercializar los vehículos de la marca Chevrolet en la provincia de Pichincha, zona en la que ocupa un índice importante de ventas de la marca. (PROAUTO C.A, s.f.)

La empresa pretende mantener o superar sus procesos de comercialización de vehículos, repuestos partes y accesorios anualmente, reduciendo los plazos de entrega a sus clientes siendo más eficaces y eficientes cuyo factor hacen que PROAUTO C.A este entre los principales concesionarios Chevrolet a nivel nacional. (PROAUTO C.A, s.f.)

En lo referente a su proceso operativo la empresa PROAUTO C.A. cuenta con el departamento de sistemas, el mismo que al momento no dispone de un sistema de detección de intrusiones, así como de la infraestructura física y lógica necesaria que permita la detección, análisis y prevención de los mismos en la red, siendo por lo tanto de vital importancia contar con un sistema que permita la prevención y detección de intrusiones para asegurar la confidencialidad de la información, ya que al ser esta un activo empresarial es imprescindible su seguridad ante posibles ataques informáticos que hoy en día son el común denominador en el ámbito de TI.

Figura 1. Valores Corporativos PROAUTO C.A

Adaptado de: (PROAUTO C.A, 2013)

Alcance.

El presente sistema de prevención y detección de intrusiones se diseña e implementa para la empresa PROAUTO C.A., los mismos que servirán para garantizar la confidencialidad de la información en la organización evitando los accesos no autorizados una red o host basándose en *sniffer* que actúa como sensor para analizar el tráfico de red determinando si es un indicio de ataque o falsa alarma.

Justificación.

A pesar del desarrollo de tecnología que se mantiene en la actualidad la Empresa PROAUTO C.A ha venido manteniendo problemas de ataques informáticos no identificados y ya que la seguridad perimetral de la cual esta provista la infraestructura de la organización no es suficiente para detectar y analizar si es susceptible a ingresos no autorizados a sistemas propios es necesaria una implementación de esta tecnología, que si bien puede venir incluida es sistemas UTM no existe una solución *open source* puesta en marcha en el ámbito empresarial.

El aporte a nuestra institución educativa se encuentra dado en que el presente trabajo de titulación es implementado en base a estándares de software libre,

que permiten tener datos de un escenario corporativo actual, en el cual se podrá evidenciar un escenario de ataques informáticos reales y su contingencia.

Objetivo General

Implementar un sistema de detección y prevención de intrusiones IPS-IDS en base al algoritmo del software SURICATA que controle el acceso a la información y sistemas de la empresa PROAUTO C.A

Objetivos específicos

- Analizar el escenario actual de seguridad de la información de la empresa PROAUTO C.A.
- Diseñar un sistema de prevención y detección de intrusiones que permita identificar y proteger la red de datos de la empresa.
- Implementar el sistema de prevención y detección de intrusiones.
- Validar la implementación del sistema de prevención y detección de intrusiones y su funcionalidad en la empresa.

1. Capítulo I. Marco Teórico

En este capítulo se describe a detalle los conceptos y elementos que conforman el sistema de detección y prevención de intrusiones. Por otra parte, se incluyen los lineamientos utilizados para la creación de las reglas fundamentadas en el algoritmo de inteligencia artificial.

Finalmente se abarcará un análisis de la solución propuesta frente a los diversos mecanismos basados en software libre para la prevención y detección de intrusiones.

1.1 Seguridad De La Información.

En retrospectiva la seguridad de la información es un conjunto de procedimientos que tienen como objetivo el proteger la integridad y privacidad de la información ante cualquier tipo de amenaza con el objetivo primordial de minimizar tanto los riesgos físicos como lógicos. En el caso de que se presente la filtración a las

seguridades se procurará el restablecimiento de la información garantizando la integridad de la misma. (Urbina, Introducción a la seguridad informática, 2016).

1.1.1 Definición de Riesgo.

El riesgo es la posibilidad que exista una amenaza, la cual se puede producir por medio de una vulnerabilidad. Sin embargo, un riesgo no siempre puede ser catalogado como una amenaza ya que para ser considerada como tal esta debe estar acompañada de una vulnerabilidad. (López, 2010)

Se puede obtener un gran número de amenazas cuando los sistemas informáticos presentan varias vulnerabilidades para lo cual se emplea la siguiente fórmula la misma que permite interpretar el análisis de riesgo en un sistema.

Ecuación de análisis de riegos (Ecuación 1)

$$B > P \times L$$

Dónde:

B: Es el gasto que significa la prevención de una pérdida específica debido a una vulnerabilidad.

P: Es la probabilidad de que por medio de la vulnerabilidad ocurra una pérdida específica.

L: Es el impacto total que ocasiona la pérdida específica por medio de la vulnerabilidad (Aguirre, 2006)

Cabe mencionar que los riesgos generalmente se clasifican en:

- Riesgos Internos;
- Riesgos Externos;
- Riesgos Físicos; y,
- Riesgos Lógicos.

1.1.1.2 Riesgo Externo. - Se entiende por riesgo externo a la infección que se produce por virus, malware o ataques globales que se produzcan en la red. A todo este grupo se lo denomina con el nombre de ataques no dirigidos.

1.1.1.3 Riesgos Físicos. - Es aquel que en el cual se contempla el robo o destrucción de la información.

1.1.1.4 Riesgos Lógicos. - Son aquellos que comprenden el acceso de intrusos a servicios o información propios de la empresa dentro de los cuales se incluyen los ataques dirigidos (Carpentier, 2016).

1.1.1.5 Riesgo Interno. - El riesgo interno se relaciona directamente con los recursos propios de la empresa siendo estos los siguientes:

- Ordenadores portátiles;
- Tabletas;
- Teléfonos Inteligentes;
- Infraestructura; y,
- Servicios y aplicaciones.

Adicionalmente a esta clasificación, el no contar con un plan de contingencia o reparación se encuentra definido como un tipo de riesgo interno. (Carpentier, 2016)

1.2 Clasificación De La Seguridad De La Información.

La Seguridad de la Información se clasifica en: seguridad activa, pasiva, física y lógica.

1.2.1 Seguridad Activa.

La seguridad activa consiste en el conjunto de medidas que se utilizan con el fin de detectar amenas siendo estos por ejemplo el uso de antivirus, firewall, además de la implementación de contraseñas complejas que dentro de sus parámetros se encuentran compuestas por un conjunto de letras mayúsculas, minúsculas, números y caracteres especiales (Alegre Ramos & García Cervigón Hurtado, 2011).

1.2.1.1 Firewall

Es un dispositivo de hardware o software utilizado para gestionar y principalmente filtrar el tráfico entre dos redes y comúnmente entre internet y una red privada LAN (Joan, 2013).

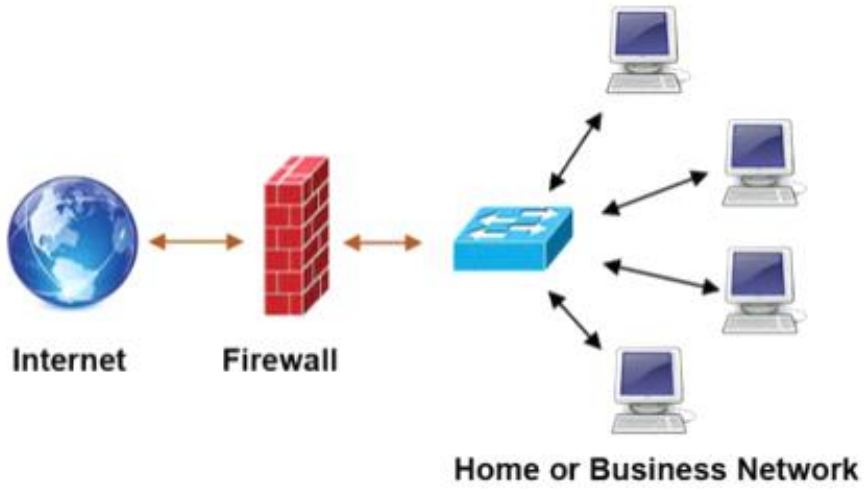

Figura 2. Firewall

Tomado de (Pattel, 2016)

Dentro de las principales funciones de un firewall según (MO, 2012) tenemos:

- Garantizar la seguridad y privacidad de una red de datos;
- Proteger la red de datos empresarial;
- Preservar la integridad de la información guarda dentro de la red LAN;
- Evitar el acceso de usuarios no deseados de manera bidireccional;
- Evitar ataques de tipo DOS; y,
- Permitir o denegar el acceso a aplicaciones de manera segura.

1.2.1.1.1 Firewall por Hardware

Este tipo de firewall depende de un dispositivo físico con cpu, memoria, disco, interfaces de red y sistema operativo. En algunos casos puede venir incluido como una función de un router de acceso a internet, su configuración y uso es complejo ya que requiere de conocimientos específicos.

Generalmente se utiliza para la protección de redes corporativas y en la mayoría de casos se comercializan como *Appliance* que consisten en una integración de software y hardware para una sola solución que incluye funciones adicionales como *web filtering* entre otras.

1.2.1.1.2 Firewall por Software

Actualmente con el desarrollo de las tecnologías de la información dentro de estos tipos de firewalls podemos mencionar aquellos que vienen incluidos con los sistemas operativos, en el caso de Windows el denominado Firewall de Windows y para Linux Iptables en versiones antiguas y firewalld para versiones recientes.

Las soluciones de antivirus como Eset o Kaspersky dependiendo del licenciamiento incorporan un módulo dedicado de firewall adicional a los módulos de antivirus. Por otra parte, con el avance de la virtualización de hardware, los firewalls también se pueden montar en ambientes de hardware virtual siendo instalados o funcionando como "*software as a hardware*".

1.2.2 Seguridad Pasiva

Se entiende como seguridad pasiva al conjunto de procedimientos o herramientas utilizadas para la recuperación de la infraestructura tecnológica ante una vulneración de seguridad. Su objetivo principal es minimizar al máximo el impacto que un evento de seguridad tenga sobre una organización. (Alegre Ramos & García Cervigón Hurtado, 2011)

1.2.3 Seguridad Física.

La seguridad física es el conjunto de procedimientos que se utilizan para proteger a los sistemas ante una manipulación provocada por el hombre de manera accidental o voluntaria pudiendo ser también ocasionado por factores naturales. (Alegre Ramos & García Cervigón Hurtado, 2011)

1.2.4 Seguridad Lógica.

La seguridad lógica son aquellos mecanismos de protección de los sistemas cuyo objetivo principal es el asegurar los datos y controlar el ingreso autorizado

a los sistemas o servicios que se mantengan. (Alegre Ramos & García Cervigón Hurtado, 2011)

1.2.4.1 Puertos

Un puerto se puede definir como un dispositivo físico o lógico que utiliza un sistema informático ya sea para conectarse con otros sistemas o dispositivos periféricos. (MO, 2012).

1.2.4.1.1 Puerto Físico

Es aquel que agrupa todos los conectores integrados en tarjetas o en la tarjeta madre de los equipos informáticos estos se utilizan para interconectar una gran gama de dispositivos externos o periféricos (MO, 2012).

Dentro de esta clase de puertos podemos mencionar los siguientes (MO, 2012):

- Ethernet
    - RJ-45
    - BNC
- Telefónico
    - Rj-11
- Conectores de Fibra
    - ST
    - SC
    - LC
    - FC
    - MTRJ
- USB
- LPT1
- RS232
- SERIAL
- VGA
- HDMI
- SATA
- PCI

- PCIe
- SLOT
- SOCKET
- AGP
- IDE

1.2.4.1.2 Puerto Lógico

Es el método por el cual un cliente interactúa con un servidor a través de una misma dirección de red. Los puertos lógicos suelen estar numerados entre 0 y 65535 permitiendo de esta forma identificar que aplicación lo utilizará. Inicialmente estos números de puerto se utilizaron con los protocolos de internet TCP/UDP que están dentro de la capa transporte del modelo OSI y actualmente también se utilizan en DCCP (Protocolo de Control de Congestión de Datagramas) y SCTP (*Stream Control Transmision Protocol*) (MO, 2012).

Existen tres categorías definidas por la entidad de control IANA (*Internet Assigned Numbers Authority*) mismas que se detallan a continuación:

Puertos Conocidos. - Son los que van desde el número 0 hasta el 1023 que son utilizados por el sistema operativo y servicios conocidos como por ejemplo HTTP, POP3/IMAP, TELNET, SSH, FTP, RDP entre otros (MO, 2012).

Puertos Registrados. - Son aquellos que van desde el 1024 al 49151 y están registrados por la IANA para su uso en cualquier servicio u aplicación (MO, 2012).

Puertos Privados. - Son los que están entre el rango de 49152 al 65535 y cuyo uso se lo realiza en aplicaciones *peer to peer* (MO, 2012).

Listado de Puertos más Utilizados

En el anexo A se muestra el listado de puertos con mayor uso.

1.2.4.2 Sniffer de Red

Es un programa que permite el análisis de redes, paquetes y protocolos del tráfico transmitido de una localización a otra. Un *Sniffer* captura un paquete de

información lo codifica y luego da a su propietario la habilidad de ver su contenido como se muestra en la Figura 3 (Kiguolis, 2016).

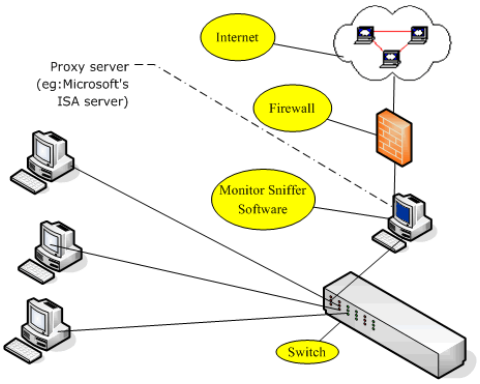

Figura 3. *Sniffer* de Red

Tomado de (Culturación, s.f.)

Los *sniffers* pueden ser utilizados con fines de monitoreo y análisis de problemas en la red siendo aprovechados por personas maliciosas con el fin de robo de información transmitida a través de la red de datos (Kiguolis, 2016).

Los *sniffers* se pueden dividir en aplicaciones legítimas y herramientas diseñadas por delincuentes informáticos con fines de robo de información ambos tipos de *sniffers* son programas afines con la única diferencia que los de tipo maliciosos poseen herramientas especializadas con características no estandarizadas (Kiguolis, 2016).

Uno de los *hábitats* de los *sniffers* son las redes LAN, cada vez que una computadora quiere transmitir un dato lo hace a través de un *switch* al cual están conectados todos los ordenadores, permitiendo la visualización de la información transmitida en un determinado instante, exceptuando si se realiza alguna configuración adicional dentro en el *switch* de distribución o acceso (Untiveros, 2004).

Las interfaces Ethernet o tarjetas de red están construidas de tal manera que en modo normal capturen paquetes dirigidos hacia ellas y no a los demás equipos de red por lo que para el uso de un *sniffer* es necesario colocar dicha tarjeta en modo promiscuo (Untiveros, 2004).

Modo Promiscuo

El modo promiscuo de una interfaz de red es aquel que permite capturar o analizar todos los paquetes que pasan por una red a la cual está conectada (Untiveros, 2004).

1.3 Sistemas De Detección Y Prevención De Intrusos

1.3.1 Sistemas de detección de intrusos

Las siglas IDS significan *Intrusion Detection System* que en español se traduce como *Sistema de Detección de Intrusos*. En el ámbito de las tecnologías de la información es un método utilizado para identificar situaciones o eventos no comunes en el tráfico de una red de datos como se lo puede evidenciar en la Figura 4 (Commons, 2018).

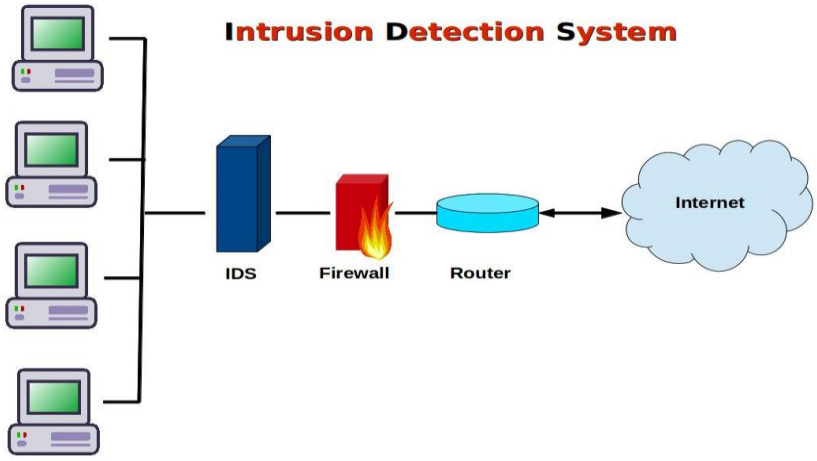

Figura 4. IDS

Tomado de (Mitra, 2015)

1.3.1.1 Clasificación de los IDS

Los sistemas de detección de intrusos se dividen en dos grupos que son los de red N-IDS y de host H-IDS.

1.3.1.1.1 N-IDS

Conocido también como IDS basados en red, su función principal es el analizar los paquetes y segmentos de la red con el fin de encontrar coincidencias con patrones definidos como sospechosos.

Los N-IDS se encuentran compuestos por:

- Analizadores;
- Interfaces de usuarios; y,
- Sensores.

Los sensores son distribuidos de una manera estratégica por toda la red con el fin de obtener un análisis granular de toda la infraestructura como se puede evidenciar en la Figura 5 (Policía Nacional, 2017).

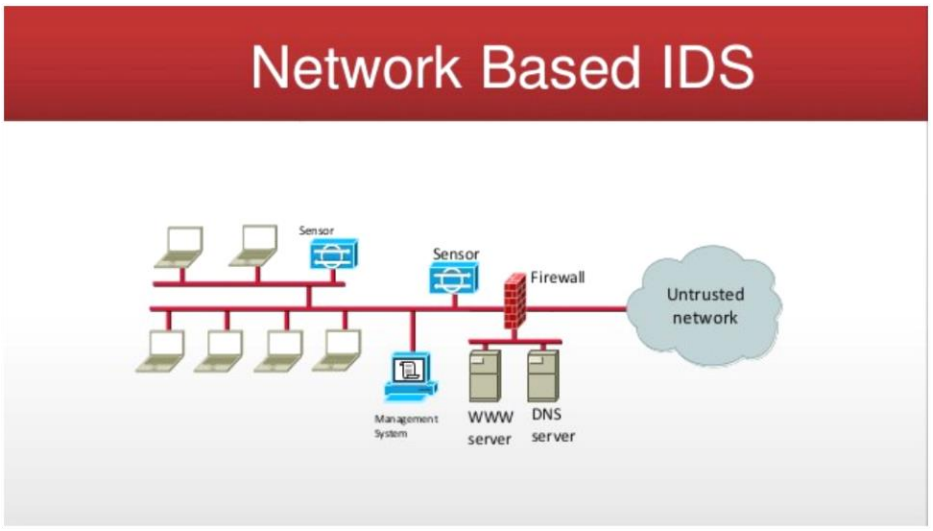

Figura 5. Estructura de un N-IDS

Tomado de (Balanji, 2017)

1.3.1.1.2 H-IDS

Es un tipo de IDS que realiza su función de seguridad en el host, son comunes en los programas antivirus, su estructura se puede evidenciar de una mejor manera en la Figura 6 (Commons, 2018).

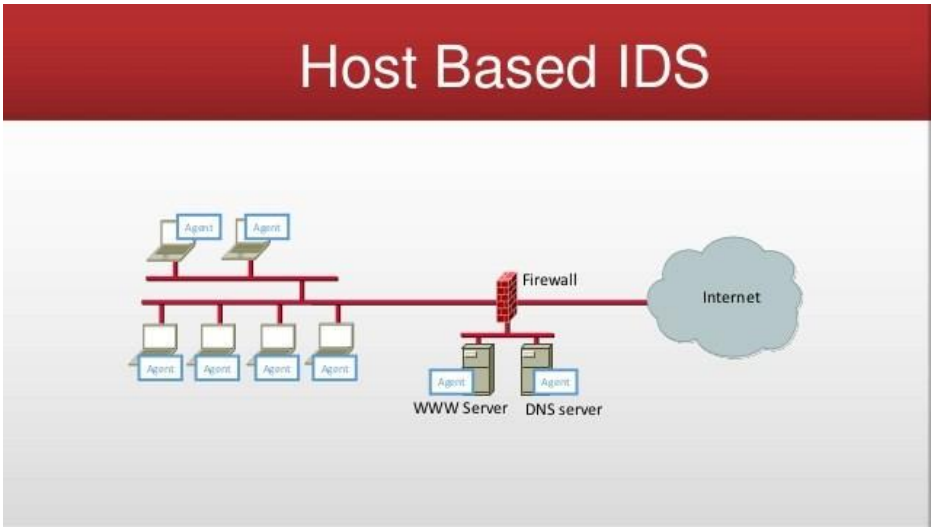

Figura 6. Estructura de un H-IDS

Tomado de (Balanji, 2017)

1.3.1.2 Técnicas para Detectar Intrusiones.

Dentro de las técnicas utilizadas para la detección de intrusiones en una red se puede mencionar las siguientes (Commons, 2018):

- Verificación de la lista de protocolo;
- Revisión de protocolos en la capa de aplicación; y,
- Reconocimiento de ataques de comparación de patrones.

1.3.1.3 Métodos para bloquear intrusiones

Entre los métodos más importantes podemos mencionar los siguientes:

Reconfiguración de dispositivos externos. - En este método se trata de reconfigurar por parte del N-IDS a firewalls que mediante el envío de datos en la cabecera del paquete explique la alerta (Commons, 2018).

Envío de trampas SNMP a un hipervisor externo. - Para este caso se realiza el envío de un datagrama SNMP a una interfaz de administración externa por ejemplo: HP Open View, Tivoli, Spectrum, etc (Commons, 2018).

Notificaciones por correo electrónico a uno o más usuarios. - Consiste en las notificaciones a través del envío de un correo electrónico al administrador con el fin de notificar una intrusión seria (Commons, 2018).

Registro del ataque. - Como su nombre lo indica es un listado con los eventos dentro de la cual se incorpora la dirección IP del atacante, dirección IP de destino, que protocolo se ha utilizado y su carga útil, parámetros relevantes para la gestión de seguridad (Commons, 2018).

Almacenamiento de paquetes sospechosos. - Es el almacenamiento de los paquetes originales capturados y/o los paquetes identificados que encendieron la alerta (Commons, 2018).

Apertura de una aplicación. - Con la utilización de un software externo se puede ejecutar acciones específicas entre ellas notificaciones por SMS o alertas sonoras (Commons, 2018).

Envío de un ResetKill.- Consiste en la construcción de un paquete de alerta TCP que forza el término de una conexión únicamente funcional con el fin de evitar intrusiones con técnicas que emplean el protocolo TCP (Commons, 2018).

Alertas Visuales. - Se refiere al despliegue de una alerta grafica o pop-up en la consola de administración que notifica un ataque (Commons, 2018).

1.3.2 Sistema de Prevención de Intrusos

Las siglas IPS significan *Intrusion Prevention System* que en español se traduce como *Sistema de Prevención de Intrusiones* cuyo desarrollo se origina en comienzos de 1990 con el fin de prevenir cualquier tipo de ingreso no autorizado a la red mediante mecanismos de identificación de paquetes, analizando si estos se encuentran dañados o incompletos para posteriormente bloquear su transmisión y así prevenir un posible ataque. Adicionalmente, permite proteger la red ante vulnerabilidades, tráfico o intrusiones obteniendo así una optimización de la seguridad y la eficiencia ante el ataque (Chicada, 2014).

Cabe recalcar que los IPS son sistemas escalables siendo estos una evolución de los sistemas IDS por cuanto dentro de sus características más relevantes tenemos las siguientes (Chicada, 2014):

- Capacidad de respuesta automática en cuanto se produce un ataque;
- Implementación de nuevos controles en medida de nuevos ataques;

- Disminución de falsos positivos en la red;
- Bloqueo y detección de ataques en la red en tiempo real; y,
- Garantiza el rendimiento del tráfico en la red mediante un bloqueo automático de los ataques.

1.3.2.1 Clasificación de los IPS

Los sistemas de prevención de intrusos se encuentran clasificados de acuerdo a la manera en la que detectan un comportamiento inusual en el tráfico de red de la siguiente manera:

- Detección basada en firmas;
- Detección basada en políticas;
- Detección basada en anomalía; y,
- Detección *honey pot.*

1.3.2.1.1 Detección basada en firmas.

Este método opera mediante una serie de patrones de bytes de referencia lo que le permite tener la capacidad de reconocer y comparar la cadena de bytes origen contra la cadena de bits que contiene la firma de no encontrar ninguna alteración en esta no se presenta ningún bloqueo sin embargo, en el caso de que exista un intruso que mantenga un patrón de bits que es desconocida por el IPS este no podrá detectar tal ataque razón por la cual es importante que la base de firmas se mantenga siempre actualizada (Urbina, Introducción a la seguridad informática, 2016).

1.3.2.1.2 Detección basada en políticas.

El segundo método de funcionamiento de un IPS se basa en lineamientos realizados por el administrador de red quien por medio de una política delimita el acceso de un host a una o varias redes bloqueando todo aquello que no esté dentro de este parámetro y siendo catalogado como acceso no autorizado (Urbina, Introducción a la seguridad informática, 2016).

1.3.2.1.3 Detección basada en anomalías.

El tercer método de funcionamiento de un IPS se basa en la detección de anomalías las cuales son consideradas en base a patrones de comportamiento

de tráfico en la red estructuradas por el IPS todo lo que se encuentra fuera del patrón en mención será considerado como una anomalía (Urbina, Introducción a la seguridad informática, 2016).

1.3.2.1.4 Detección basada en honey pot.

El cuarto método de funcionamiento de un IPS se basa en simular escenario de ataque con el fin de obtener información del método utilizado para el mismo, así como también la información del atacante como se muestra en la Figura 7 (wikipedia, 2014).

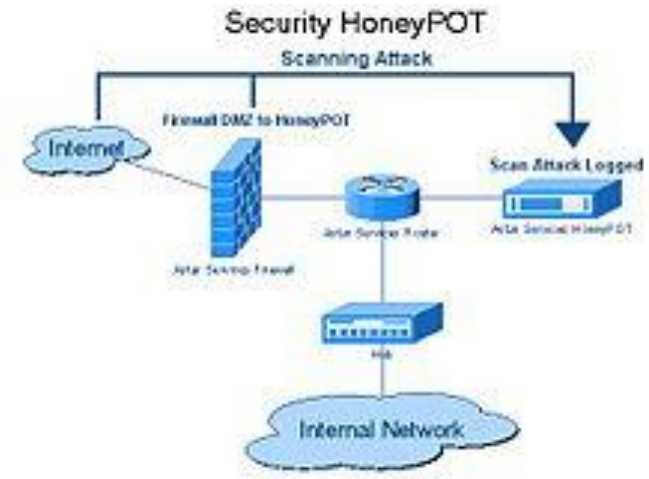

Figura 7. Diagrama de un *Honeypot*

Tomado de (wikipedia, 2014)

1.3.2.2 Clasificación de intrusiones

1.3.2.2.1 Acceso No Autorizado

Se puede definir como el acceso indebido, sin autorización o contra derecho a un sistema de tratamiento de la información con el objeto de obtener un logro de carácter intelectual por el desciframiento de códigos de acceso o contraseñas, sin causar daños inmediatos y tangibles en la victima (Huerta & Libano, 1996).

1.3.2.2.2 Ataque dirigido.

El método ATP *Advanced Persistent Threat* realiza un ataque dirigido a un host el cual mantiene información relevante e importante, esto se realiza mediante el

uso de la ingeniera social o *spear phishing* que permite a los hackers entrar a la red y apoderarse de la información (Kasperskylab, 2013).

1.3.2.2.3 Ataque Web.

Para medir el grado de impacto de un ataque web se toma en cuenta los siguientes objetivos:

- El interrumpir la operación de un sitio;
- La modificación de la información que se encuentra publicada;
- El obtener información no autorizada referente a la organización o de forma personal; y,
- Realizar ataques a la infraestructura interna y alcanzar un control de varios servicios y sistemas (ACISSI, 2015).

1.3.2.2.4 Botnet

Botnet es una red de *bots* su principal función es albergar toda la información enviada por los hosts infectados los cuales responden a las órdenes del o los hackers, siendo estas el robo de información, envío de denegación de servicio, envío de spam y virus. El funcionamiento y efectos de una red de bots dentro de una *botnet,* lo podemos observar en el Figura 8 (Aguilera, 2010).

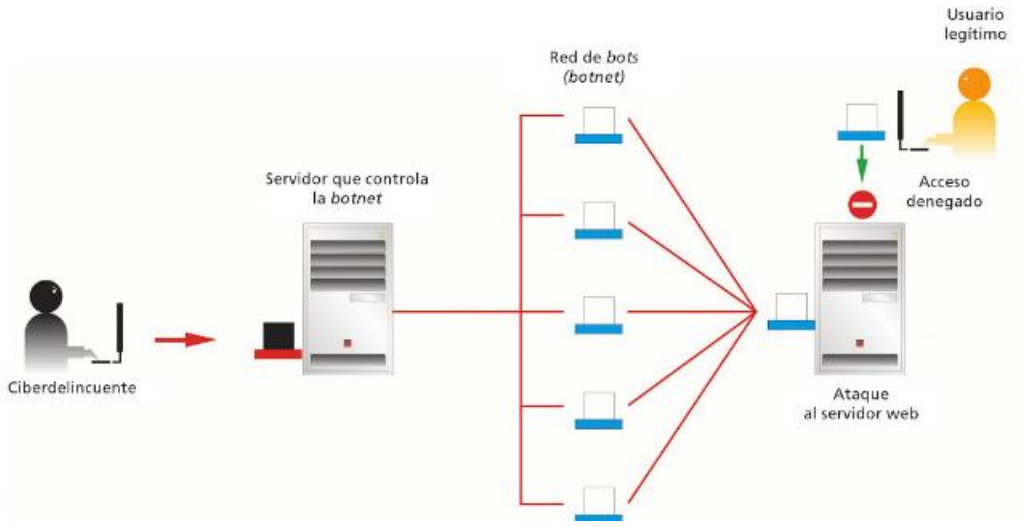

Figura 8. Funcionamientos y efectos de una botnet

Tomado de **(Aguilera, 2010)**

1.4 Inteligencia Artificial

1.4.1 Definición

Se define como el diseño de procesos que al ejecutarse en conjunto sobre una arquitectura física producen resultados que maximizan una cierta medida de rendimiento. Estos procesos son basados en secuencias de entradas que son percibidas y almacenadas por la arquitectura física (Pérez Porto & Gardey, 2014).

Los distintos dispositivos que cuentan con inteligencia artificial son capaces de ejecutar distintos procesos análogos al comportamiento humano, es decir; devolver una respuesta por cada entrada o la búsqueda de un estado entre todos los posibles mediante el uso de una lógica formal (Pérez Porto & Gardey, 2014).

La inteligencia artificial es la responsable de que los equipos o dispositivos inanimados entre ellos: computadores, dispositivos móviles, robots y software, sean capaces de resolver problemas facilitando las tareas de la vida humana (Culturación, s.f.).

1.4.2 Tipos de Inteligencia Artificial

1.4.2.1 Sistemas que piensan como humanos. - Aquellos que emulan al detalle el pensamiento humano (Culturación, s.f.). Un ejemplo de ello es el proyecto de IBM *Deep* QA llamado “Watson” que es capaz de responder a varias preguntas en lenguaje natural emulando de cierta manera el pensamiento humano por el amplio conocimiento que demuestra (Gonçalves, 2012).

1.4.2.2 Sistemas que actúan como humanos. - Son los que emulan y copian el comportamiento humano (Culturación, s.f.). Dentro de este tipo podemos mencionar los avances tecnológicos en cuanto a robótica se refiere especialmente en los robots que imitan gestos y movimientos de los seres humanos. Un claro ejemplo de ello es el robot HRP-4C creado por el Instituto Nacional de Ciencias Avanzadas y Tecnología(AIST) el cual es capaz de realizar movimientos y gesticulaciones faciales similares a la de un rostro humano en este caso femenino (CSCAZORLA, 2011).

1.4.2.3 Sistemas que piensan racionalmente. - Se pueden definir como los que tienden a pensar lógicamente imitando al cerebro humano (Culturación, s.f.). Como se mencionó en el punto 1.3.2.1 “Watson” de IBM es un claro ejemplo de esto ya que adicional a la interacción a través del lenguaje natural es capaz de realizar una recuperación de información de forma lógica (Gonçalves, 2012).

1.4.2.4 Sistemas que actúan racionalmente. - Estos emulan de manera racional el comportamiento humano (Culturación, s.f.). Es un campo de igual forma competente a la robótica actual un claro ejemplo de este tipo de inteligencia es el robot desarrollado por Honda llamado “asimo” el cual camina y corre a un máximo de 9km/h, salta en una o dos piernas y predice la dirección en la cual caminará otra persona para evitar tropezar con ella estas características de cierta forma le da un comportamiento lógico al interactuar con los seres humanos (Honda, 2011).

1.4.2.5 Inteligencia artificial Convencional (Simbólica-deductiva). - Es aquella que se basa en un análisis formal y estadístico del comportamiento del ser humano ante diferentes tipos de problemas o situaciones (Culturación, s.f.). Un referente de este tipo de inteligencia artificial es el análisis de datos a grande escala conocido en la actualidad como *Big Data*, responsable de monitorear las preferencias y gustos de los seres humanos en base a la cantidad de visitas y/o búsquedas a determinados sitios como por ejemplo *youtube* o los buscadores como *yahoo y google* definiendo las tendencias especialmente en redes sociales y generando un gran impacto en los usuarios.

1.4.2.6 Inteligencia Computacional (Simbólica-Inductiva). - Concentra su desarrollo de habilidades y mecánicas de pensamiento humano mediante la interacción progresiva con el ser humano (Culturación, s.f.). Los asistentes personales que incorporan fabricantes como Apple o Samsung son un tipo de Inteligencia Computacional Simbólica Inductiva ya que a través de la interacción con el usuario permite que de cierta forma conozca o se familiarice con las preferencias y gustos. Los aplicativos más relevantes en la actualidad son SIRI, *Bixby y Google Assistant*.

1.4.3 Algoritmo

Se define como un conjunto ordenado de instrucciones que representan un modelo de solución para un determinado tipo de problemas o eventos (UNNE, 2006).

En el ámbito del software un algoritmo es independiente del lenguaje en que se programe, es decir que se puede escribir y ejecutarse posteriormente en un lenguaje diferente.

1.4.3.1 Características Principales de los Algoritmos

Entre las principales se tiene (UNNE, 2006):

- Deben ser precisos;
- Definidos ya que si utiliza varias veces debe obtenerse el mismo resultado;
- Son finitos;
- Siempre deben producir un resultado; y,
- Los elementos de entrada pueden ser cero o más.

1.4.3.2 Clasificación de los Algoritmos

Los algoritmos se clasifican en:

- **Algoritmos Cualitativos. -** Son aquellos que no involucran cálculos numéricos y únicamente detallan los pasos o instrucciones en su secuencia (UNNE, 2006).
- **Algoritmos Cuantitativos. -** Se definen como algoritmos cuantitativos aquellos que involucran cálculos matemáticos (UNNE, 2006).

Técnicas de Representación

Dentro de las principales técnicas están (UNNE, 2006):

- Diagramas de flujo;
- Pseudocódigo;
- Lenguaje Natural; y,
- Fórmulas Matemáticas.

1.5 Open Source O Software Libre

Es aquel software que tiene la característica de poseer el código abierto a modificaciones y alteraciones, adicionalmente se puede descargar y distribuir de manera gratuita permitiendo de esta manera que la comunidad de programadores contribuya con su desarrollo y mejora continua (Pérez Porto & Gardey, 2014).

1.6 Herramientas De Software IPS-IDS

Actualmente existen varias opciones dentro de la comunidad de software libre con características IPS-IDS de las cuales las más relevantes en la actualidad son:

- Snort;
- Suricata;
- Bro; y,
- Kismet

1.6.1. Snort

Es un software que se ha convertido en un estándar debido a su longevidad en el mercado ya que está vigente desde el año 1998. Este software ha ido evolucionando en sus capacidades de IPS-IDS gracias al desarrollo continuo de la comunidad de software libre a pesar de que tiene algunas desventajas respecto a sus competidores como por ejemplo el no incorporar un entorno gráfico para su administración (Alejandro, 2017).

1.6.2. Suricata

Este software IPS-IDS utiliza firmas similares a Snort diferenciándose en la versatilidad y potencia que brinda gracias a la compatibilidad con el hardware y la capacidad de procesamiento múltiple hilo. Adicionalmente a estas ventajas es capaz de integrarse con plataformas de software de gestión y estadística de eventos.

1.6.3 Bro-IDS

Es un sistema basado en anomalías y firmas que poseen su propio lenguaje de administración llamado bro-script que vienen a ser su propio intérprete, lo cual lo hace complejo para la administración y configuración (Alejandro, 2017).

1.6.4 Kismet

Es un software IDS orientado netamente al monitoreo de eventos en una red inalámbrica el cual no posee mayores características de análisis de paquetes por lo que en algunas incidencias se realizan falsas detecciones (Alejandro, 2017).

Tomando en cuenta las características descritas en los puntos anteriores, se denota que el software con mayor capacidad de análisis, integración y administración es Suricata.

1.7 Suricata vs Otros Softwares

Actualmente Suricata es uno de los *softwares open source* con mayores ventajas implantando grandes mejoras sobre su competidor director snort como se puede evidenciar en la Tabla 1 (Alejandro, 2017).

Tabla 1.

Comparación entre Suricata y Snort

SURICATA	**SNORT**
Soporte de multiprocesador	Soporte para un procesador
Interfaz gráfica	Sin interfaz gráfica por defecto
Fácil administración	Administración Compleja
Análisis de certificados, solicitudes, peticiones	Análisis Únicamente de paquetes
Integración con Aplicaciones graficas de monitoreo.	
Integración con aplicaciones de análisis de logs, análisis de incidencias y reportes estadísticos.	

Tomado de (Alejandro, 2017).

Nota: las características descritas hacen referencia a las ventajas que posee suricata vs snort.

1.7.1 Software Suricata

Es un software *open source,* con capacidades de detección de intrusiones en tiempo real, prevención de intrusiones en línea, monitoreo de la red y procesamiento de PCAP (interfaz de una aplicación de programación para captura de paquetes) fuera de línea.

Suricata. - Consiste en el análisis del tráfico de red basándose en reglas potentes y extensas con un fuerte soporte de secuencia de comandos para la detección de amenazas complejas (Suricata, s.f.). El proyecto suricata y su código son propiedad de la OISF (*Open Information Security Foundation)* que es una fundación sin fines de lucro comprometida con el desarrollo del software libre (Suricata, s.f.).

2. Capítulo II. Análisis de la Situación Actual de la Empresa PROAUTO C.A.

2.1. Antecedentes

El concesionario PROAUTO C.A inicia su operación hace más de 20 años, iniciando sus actividades como taller de reparación de vehículos y venta de vehículos usados para posteriormente conseguir el aval de Colmotores y vender vehículos pesados de 4 toneladas y tracto mulas. En el año 1992 General Motors concede al concesionario la distribución de vehículos livianos fabricados por GM (PROAUTO C.A, s.f.).

En la actualidad PROAUTO C.A se encarga de la venta y posventa de vehículos livianos y pesados de la marca Chevrolet tanto para clientes *retail* como para flotas, con una representación importante en el mercado entre los distribuidores de la marcas de GM en Ecuador y contando con más de 200 colaboradores distribuidos en cinco agencias, cuatro en Quito y una en Cayambe (PROAUTO C.A, s.f.).

A medida del desarrollo tecnológico y el avance en sistemas de vulneración de seguridad informática PROAUTO C.A presenta la necesidad de contar con un sistema informático el cual permita prevenir e identificar un ataque de seguridad a los sistemas en ambientes de producción ya que los mismos contienen información detallada de clientes como índices de solvencia, cantidad de flotas adquiridas, cupo de renovación, etc.

En los últimos años los servicios de producción han sido objeto de varios intentos de vulneración de seguridad, sin embargo, estos no han podido ser identificados de una manera técnica desconociendo su origen, destino, grado de afectación y concurrencia convirtiéndose en un problema para los servicios que mantiene la empresa, así como también para el personal de TI.

2.2 Infraestructura Tecnológica

La empresa en mención cuenta con una infraestructura tecnológica tanto a nivel de red cableada como de red inalámbrica, éstas se encuentran concentradas en la agencia matriz, ya que a través de estas se brindan los accesos a internet y servicios propios de la compañía. A pesar de que la empresa cuenta con una solución perimetral de firewall, esta no posee un sistema de seguridad que permita monitorear en tiempo real y prevenir ataques a la red de datos e infraestructura que cumpla la normativa ISO 27001.

2.2.1 Red de Acceso

La red de acceso corporativa esta provista por tecnología de fibra FTTH (*Fiber to the Home*) para el acceso a internet y por una red hibrida de cobre y fibra para su red local como se muestra en la Figura 9

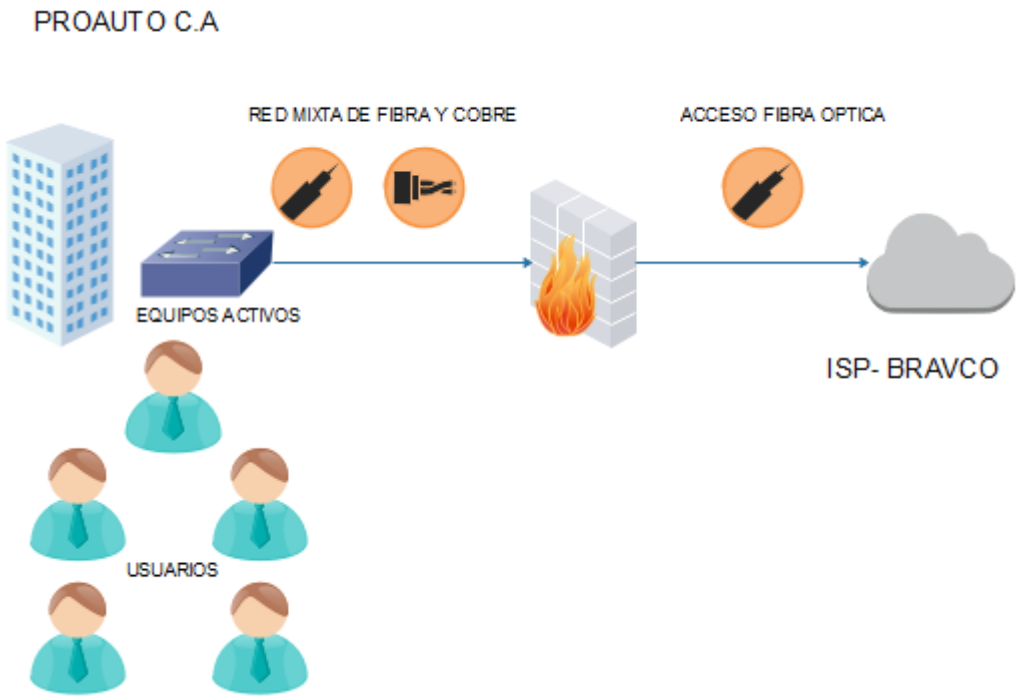

Figura 9. Red de Acceso Empresarial

2.2.1.1 Red Pasiva

La estructura de la red pasiva se encuentra compuesta por un sistema de cableado estructurado de categoría 5e, así como también los *patchpanels*, *jacks* de conexión y patchcords los cuales mantienen una longitud de 2 metros desde la estación de trabajo al punto de red.

Para el cableado vertical o de *backbone* se dispone de enlaces de fibra óptica con fibra multimodo situados en locaciones que superan los 100 metros para la conectividad inter-agencias y de acceso a internet.

El proveedor *ISP* tiene instalado una infraestructura sobre fibra monomodo que maneja los anchos de banda descritos en la tabla 2.

Tabla 2.

Anchos de Banda

Agencia	**Capacidad en Mbps**
Matriz	10Mbps para Internet
Monteserrín	6Mbps con Matriz
Carapungo	6Mbps con Matriz
Condado	6Mbps con Matriz
Cayambe	4Mbps con Matriz

Nota: Los Anchos de Banda descritos son con un canal dedicado

2.2.1.2 Red Activa

La red activa comprende los equipos que realizan algún tipo de procesamiento de información o son responsables de la gestión de las comunicaciones de una organización.

Dentro de los equipos activos de red para acceso tenemos los Intermediarios y los Terminales.

2.2.1.2.1 Equipos de red Intermediarios.

En este listado se incluyen los equipos que permiten la conectividad de red

- Switch Cisco sg300 de 52 puertos
- Switches de 24 puertos en marca huawei de la serie quidway 3000 sin *stack*
- Switches cisco sg200 de 26 puertos
- Equipos d-link DES3028.
- Routers Cisco Serie 2600.
- Router cisco 860.
- Access Point Ubiquiti i-mesh.
- Access Point Ubiquiti AC-PRO.

- Access Point Ubiquiti Nano loco m2.
- Equipos Linksys e2700.
- Equipo tplink.
- Central Telefónica Híbrida Siemens Hipath 3800

2.2.1.2.2 Equipos de red Terminales.

Los equipos terminales de usuarios en su totalidad se encuentran operando bajo la plataforma Windows para los computadores de escritorio y portátiles, adicionalmente existen un número limitado teléfonos IP siemens que trabajan en conjunto con una central híbrida de la misma marca.

La cantidad de equipos se detalla en la Tabla 3.

Tabla 3.

Cantidad de Equipos Terminales PROAUTO C.A

Agencia	**Número de Computadores**	**Número de Teléfonos IP**	**Número de Impresoras IP**
Matriz	89	1	12
Monteserrín	22	20	3
Carapungo	36	0	7
Condado	19	7	3
Cayambe	11	0	2

Nota: La cantidad puede variar debido al cambio y/o rotación de personal según requiera la organización.

2.2.2 Servidores

Dentro de los equipos utilizados para la infraestructura de hardware de cómputo en *datacenter* se tiene los siguientes servidores:

- Hp BladeSystem c3000;
- Blade server bl 460 gen 8;
- Dos blade server bl 460 gen 6;
- Server hp ml 350 gen 9;
- Server hp dl360 gen 9;
- Supermicro server core i3;
- Server hp dl360 gen 5;
- Network Attached Storage ctera C-200; y,
- Equipo HP de Torre core i5.

2.2.3 Servicios y Aplicaciones

El principal servicio que tiene disponible dentro de la red privada la compañía es un ERP denominado Kairós, el mismo que emplea un aplicativo *forms* de *Oracle* que utiliza una base de datos del mismo fabricante de software, además de este aplicativo existe un servicio web destinado para agendamientos de citas del taller de vehículos.

Las aplicaciones en ambiente de producción y utilizadas en la organización son las siguientes:

- Eset Remote Console versión 6 y sus clientes;
- Windows server 2008 R2 Enterprise;
- SQL server 2008;
- Centos 7;
- Centos 4.8;
- Oracle Linux 5;
- Vmware Esxi versión 4-6;
- Kernel Virtual Machine;
- Paquetes de Office;
- Windows Profesional 7;
- Windows Profesional 8.1;
- Windows Profesional 10; y,
- Controladora de Access Point ubiquiti.

2.3 Seguridad

En cuanto a sistemas de seguridad la organización cuenta con un equipo firewall perimetral y un software de antivirus el cual sincroniza sus actualizaciones y vacunas por medio de una consola de antivirus centralizada.

A nivel de organización jerárquica y en cuanto a los terminales no se encuentra implementado un Directorio Activo, únicamente se dispone de un usuario Administrador y el usuario estándar en los equipos.

A nivel de políticas de usuarios para accesos a internet y la red se tiene *webfiltering* a sitios de redes sociales, sitios de *streaming*, *clouds* públicas y cuentas de mail personales.

2.3.1 Firewall

El equipo firewall se compone a nivel de hardware de un Supermicro y como software mantiene una distribución de centos 5 modificado basado en la funcionalidad de *iptables*.

2.3.2 Antivirus

Actualmente la compañía mantiene la versión 6.5 del software antivirus del fabricante eset para su consola en tanto que para los clientes cuenta con la versión de Eset Endpoint Antivirus 6.6 la misma que no posee el módulo de firewall o IPS-IDS para el host.

2.3.3 Eventos de Riesgo de Seguridad en la Red

La empresa PROAUTO C.A carece de un sistema de seguridad en su red de datos que le permita el monitoreo de eventos, prevención e identificación de ataques poniendo en alto riesgo la información que la empresa mantiene.

Dentro de las brechas de seguridad detectadas por medio de la consola de antivirus se puede evidenciar: botnets, troyanos las cuales en su momento ocasionaron encriptamiento de archivos en formato (. zepto), ocultamiento de archivos y directorios, ataques ICMP, inconvenientes con las colas de impresión, entre otros. El problema más relevante de lo descrito anteriormente es la eliminación de usuarios en un servidor que cuenta con licencias CAL para

conexión de escritorio remoto lo que impidió que los usuarios se puedan conectar remotamente a los servicios alojados en dicho servidor.

Hasta la fecha se desconoce si se logró ejecutar un *keylogger* para identificar la pulsación de teclas, intrusiones de *coinminer's* para *adware*, *retefe.t, Bondat.E* que se encargan de atacar el java de los navegadores y así descargar automáticamente programas maliciosos entre otros.

Adicionalmente a la problemática descrita anteriormente en la actualidad no se cuenta con una política de seguridad que cumpla un estándar bajo la normativa ISO 27001.

2.4 Diagramas De Red

Las cinco agencias están interconectadas a través de fibra óptica provista por el ISP de telecomunicaciones Bravco, el cual facilita tanto el acceso de datos como el de internet.

2.4.1 Diagrama General

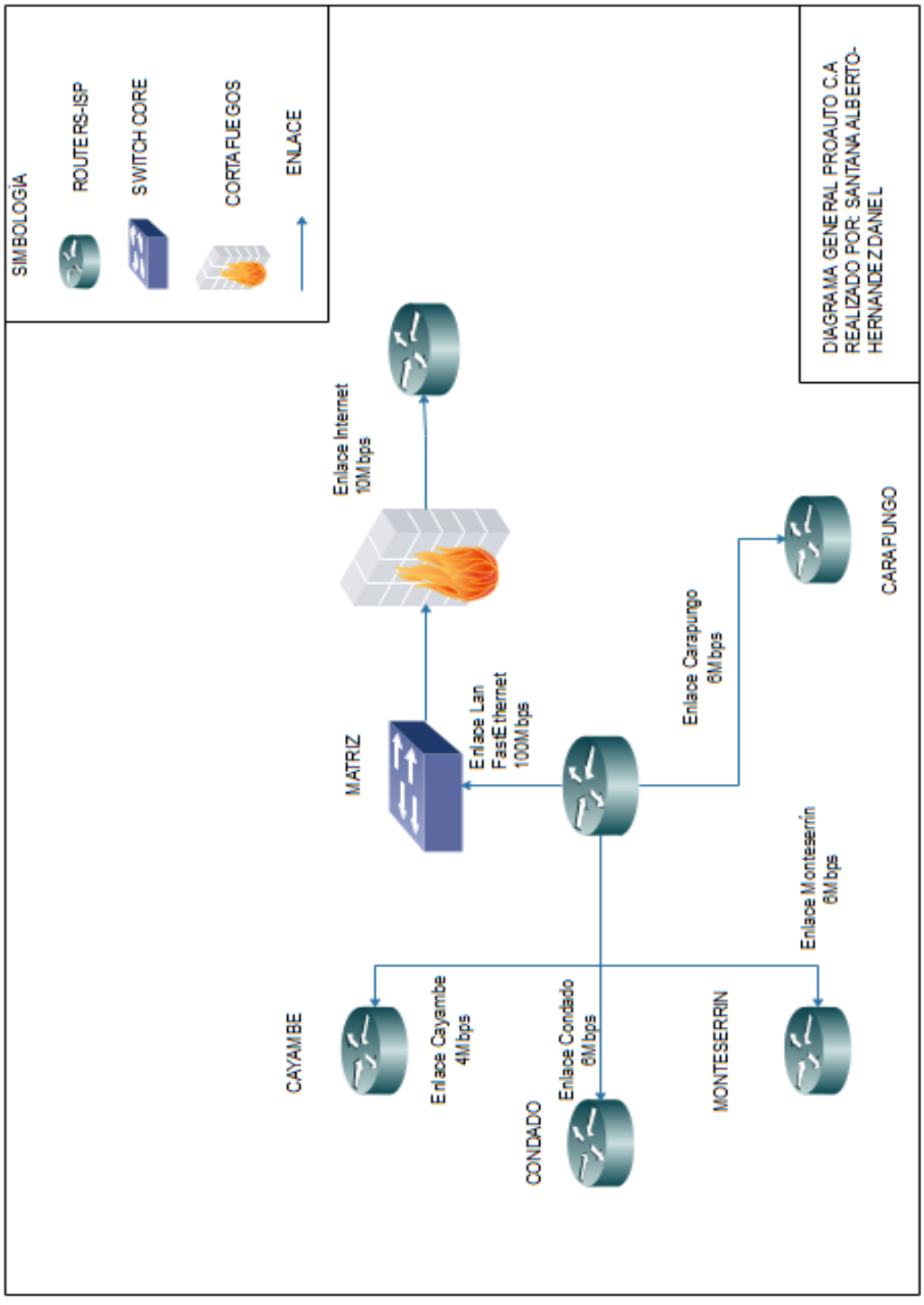

Figura 10. Diagrama General PROAUTO C.A

2.4.2 Diagrama Lógico

En este diagrama se detallan la cantidad de hosts activos y Access Point en cada punto de venta.

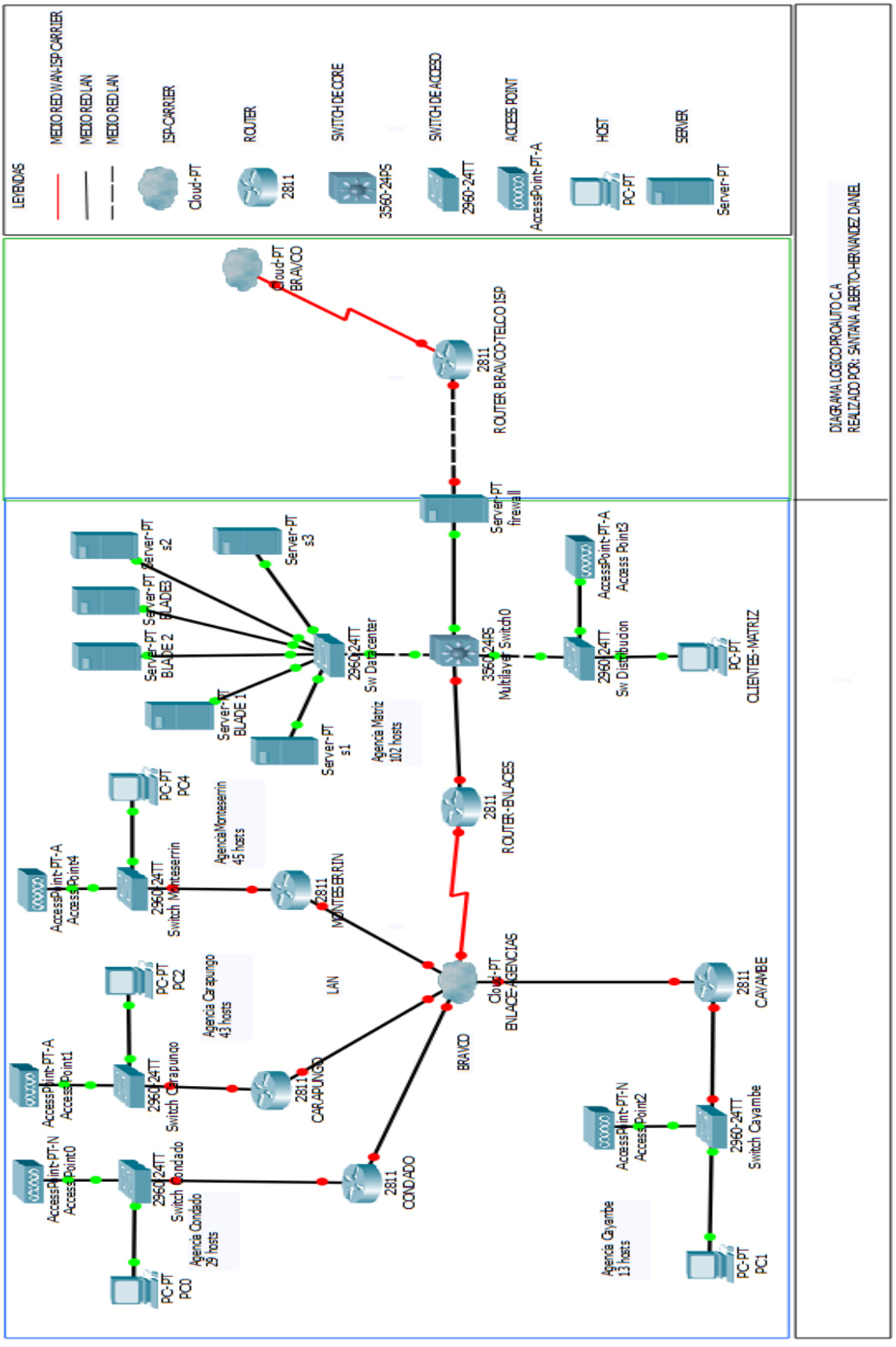

Figura 11. Diagrama Lógico de Red PROAUTO C.A.

2.4.3 Diagrama Físico

En este diagrama se detallan los equipos físicamente colocados en cada sucursal y sobretodo en el datacenter.

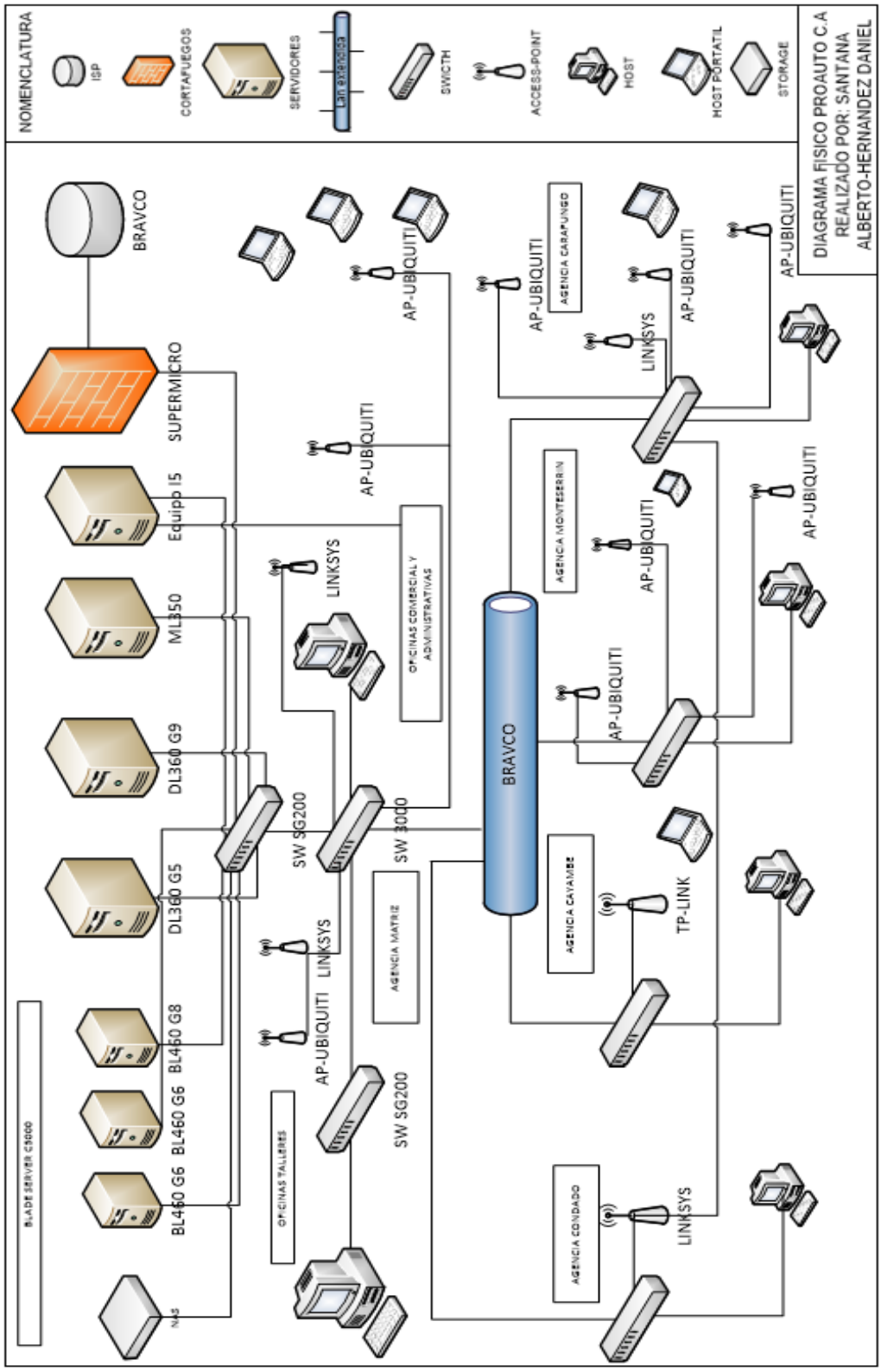

Figura 12. Diagrama Físico de Red PROAUTO C.A.

3. Capítulo III. Diseño del Sistemas IPS IDS.

En el presente capítulo se describe el diseño basado en la situación y problemática actual de la empresa PROAUTO C.A por lo que sus consideraciones se desprenden del capítulo anterior. Por otra parte, el presente diseño considera las herramientas de software apropiadas y en medida a los requerimientos de la empresa de tal manera que no incurran en gastos de licenciamiento de software.

Al ser un sistema de software libre bajo licenciamiento GPL, el *End of Life* de esta solución está proyectado a un tiempo mínimo de 3 años y máximo de 5 años acorde a las políticas internas sobre sistemas informáticos que mantiene actualmente la empresa PROAUTO C.A.

3.1 Diagramas de lógico del Sistema de Prevención y Detección de Intrusiones Proauto C.A.

Con el fin de brindar una solución de seguridad global para la empresa PROAUTO C.A el diseño del sistema de prevención y detección de intrusos se realiza en consideración a la infraestructura tecnológica, así como también a los requerimientos propios de la empresa como se puede observar en la (Figura 13).

La solución en mención se encuentra estructurada de tal manera que los datos y tráfico generados en la red principal y sucursales sean analizados en primera instancia por el sistema de prevención y detección de intrusiones, de manera preventiva y correctiva consecuentemente en base a las buenas prácticas de los sistemas de seguridad informática deberá contar con una sub-red que será de uso exclusivo para la administración y apartada de la red LAN.

De conformidad con la norma ISO 27001, se inicia el proceso de implementación y análisis de amenazas para posteriormente proceder a la identificación y planificación de los posibles riesgos que se pudieren presentar por cualquiera de las causas sean estas técnicas o humanas con el fin de garantizar una adecuada gestión de riesgos que permita conocer las vulnerabilidades de la información.

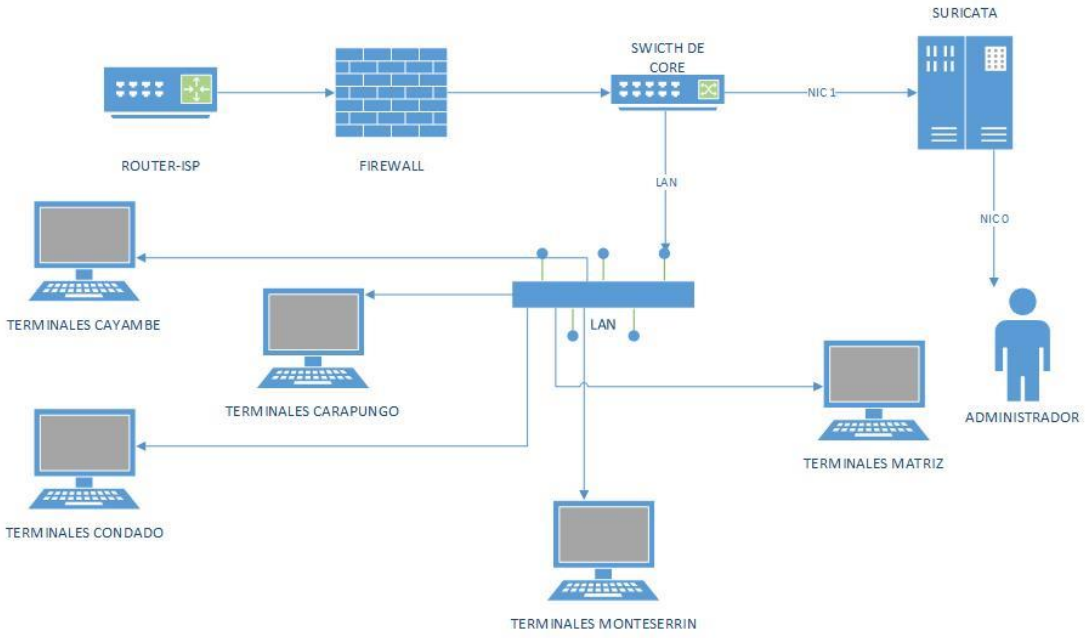

Figura 13. Diagrama físico de Solución IPS-IDS

3.2 Requerimientos Funcionales y Operatividad del Sistema de Prevención y Detección de Intrusos.

3.2.1 Requerimientos Funcionales.

Los requerimientos funcionales del sistema de prevención y detección de intrusos abarcan el detalle de los siguientes puntos:

- Motor de búsqueda;
- Soporte del sistema operativo;
- Motores tcp/ip y http;
- Motor de detección, salidas, filtrado de alertas, adquisición de paquetes;
- Reputación IP; y,
- Multi Threading.

3.2.1.1 Motor de búsqueda

El motor de búsqueda es aquel que permite realizar búsquedas de una manera automatizada al sistema como se muestra a continuación en la Tabla 4 en la que se observa los lineamientos del motor del sistema.

Tabla 4.

Detalle de motor de sistema Suricata.

Motor del Sistema	
Nombre	**Función**
NIDS	Motor de sistema que se encarga estrictamente de la detección de intrusiones en la red.
NIPS	Motor de sistema que se encarga estrictamente de la prevención de intrusiones en la red.
NSM	Motor de monitoreo de la seguridad de red.
PCAP	Motor de captura de paquetes que permite el procesamiento *offline*
Socket Unix	Procesamiento automatizado de archivos PCAP
Firewall	Integración con firewall Netfilter de Linux.

Tomado de: (Suricata, s.f.)

3.2.1.2 Compatibilidad con Sistema Operativo.

Al ser un sistema de seguridad informática este mantiene una compatibilidad multiplataforma con lo cual se garantiza la disponibilidad y factibilidad de migración de una plataforma a otra.

3.2.1.3 Motores TCP/IP- HTTP

Todo proceso que involucre seguridad de datos lleva al análisis y la decodificación de paquetes así como también la decodificación de la capa de

aplicación de HTTP, SSL, SMTP SSH entre otros, en la tabla 5 como se desprende a detalle en las características a cumplir del sistema (Suricata, s.f.).

Tabla 5.

Detalle de motores TCP/IP - HTTP

Motores TCP/IP	
Nombre	**Función**
TCP/IP	Motor de soporte escalable con soporte IPV6. Decodificación de túnel teredo Ipv6-Ipv4 IP-IP.
	Motor de secuencia TCP, sesiones de seguimiento, reensamblaje de corriente reensamblaje de la secuencia basada en objetivos, Motor IP *Defrag*, reensamblaje basado en objetivos
HTTP	Analizador de HTTP con estado incorporado en *libhtp*
	Registrador de solicitudes HTTP
	Analizador de palabras clave para hacer coincidir los almacenamientos intermedios

Tomado de: (Suricata, s.f.)

3.2.1.4 Motor de Detección

El motor de detección trabaja realizando búsquedas de palabras clave por protocolo lo que permite identificar una infección acompañada de perfiles de reglas, estos mecanismos cuentan con la estructura de algoritmos de Matcher encontrando todas las similitudes de un patrón en un campo determinado (Suricata, s.f.).

3.2.1.5 Filtrado de alerta / evento.

El filtrado de alerta o evento consiste en el control, prevención e identificación de una vulneración de seguridad, por lo que se debe mantener alertas o filtros

mismos que servirán para informar la ocurrencia de los hechos antes mencionados pudiendo ser estos por:

- Filtro de alerta de regla y umbralización;
- Filtrado de alerta global y umbralización, o por umbral de subred / host; y,
- Configuración de limitación de velocidad (Suricata, s.f.).

3.2.1.6 Adquisición de Paquetes.

Para realizar una correcta identificación de amenazas, se procede a la utilización de diferentes métodos de captura de paquetes como son:

- La captura de alto rendimiento por medio de AF_PACKET, PF_RING y NETMAP;
- Captura estándar que se realiza por medio de PCAP, NFLOG (integración netfilter);
- Modo IPS Netfilter basado en Linux (nfqueue) con soporte fallido abierto ipfw basado en FreeBSD y NetBSD; y,
- El AF_PACKET basado en Linux NETMAP (Suricata, s.f.).

3.2.1.7 Reputación IP.

La reputación se considera como una opinión relacionada con algo o alguien por lo que cuando se habla de Reputación IP, se refiere al prestigio o fama acerca de una dirección IP Pública ya sea esta de un sitio web, correo electrónico o servicio.

Los sistemas de reputación se convirtieron en el principal método de filtrado *spam* mediante el *score* de la dirección IP, por lo que la reputación IP es el mecanismo por el cual se detecta si el correo electrónico debe dirigirse a la bandeja de entrada o a la bandeja de *spam*.

En la actualidad los *botnets* al ser un conjunto de ordenadores infectados cuya principal función es el difundir malware a través de internet requieren de una gran cantidad de IP’s con una buena reputación siendo este un requisito esencial para que el ataque sea satisfactorio frente a la evolución y eficacia de los sistemas de detección.

En conclusión, podemos decir qué grupos legales e ilegales lideran una batalla para conseguir IPS con reputación limpia, lo cual hoy en día es difícil obtener. (Kasperskylab, 2013)

3.2.1.8 Multi-Hilo.

Este componente permite que sea una solución estable de seguridad ya que es precisamente el procesamiento multi-hilo el que al trabajar con grandes cantidades de datos busca patrones que permitan una vulnerabilidad de seguridad razón por lo cual al contar con un procesamiento óptimo se puede distribuir los procesos para poder transformarlos en operaciones atómicas y de bloques pequeños logrando un adecuado rendimiento del sistema. (Suricata, s.f.).

3.2.2 Operatividad del IPS

El sistema de prevención de intrusiones por medio de algoritmos es capaz de detectar y defender ataques como denegación de servicios "*DDoS"* o "SQL Inyección". Adicionalmente podrá discriminar el contenido del tráfico que se produzca vía web por lo que al detectar un evento en el que considere positivo la intrusión se interrumpe y todos los paquetes que contenga el mismo patrón serán clasificados de la misma manera.

3.2.2.1 Estructura del Algoritmo de IA Suricata.

El algoritmo de inteligencia artificial (IA) en Suricata se encuentra estructurado de 3 componentes los mismos que se detallan a continuación y se observan en la Figura 14:

- Acción;
- Encabezamiento; y,
- Opciones de regla

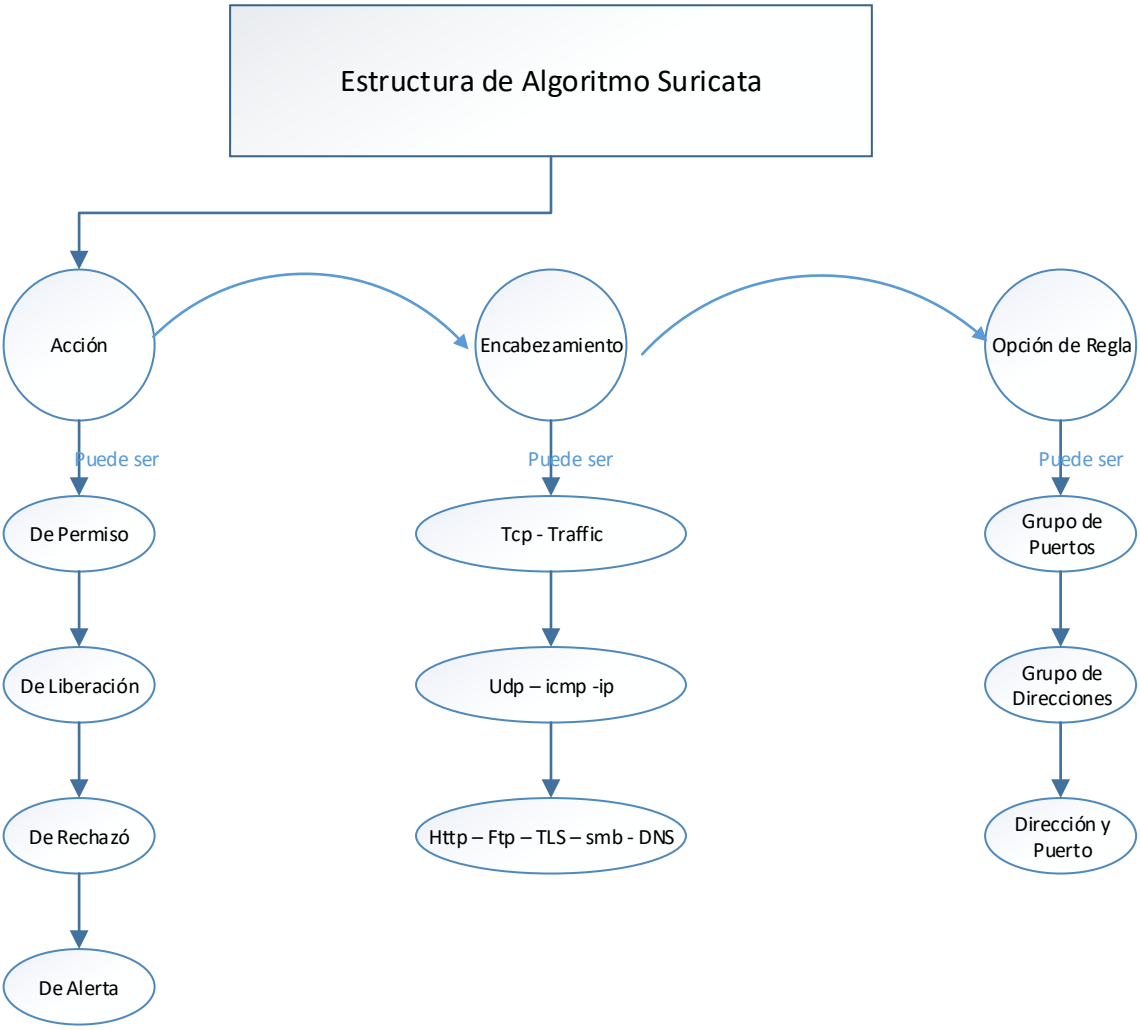

Figura 14. Estructura de Algoritmo Suricata

3.2.2.1.1 Acción

Esta propiedad permite establecer la operación que realiza cuando una acción coincide con el parámetro inicial del algoritmo para lo cual se encuentra clasificada en 4 grupos mismo que se detallaran a continuación:

- **Permitir.**

Si una acción coincide con el algoritmo planteado se realiza un *match* siempre y cuando este contenga autorización. Suricata deja de explorar el paquete y trasporta al final de todas las reglas, sin embargo, esta acción se realiza solo para ese paquete.

- **Liberar**

El algoritmo se encuentra estructurado de tal manera que se detendrá inmediatamente y el paquete no podrá ser enviado. Suricata realiza la generación de una alerta para este paquete para que el receptor no reciba al mismo.

- **Rechazar**

El algoritmo realiza la acción de rechazo permanente de un paquete siempre y cuando este coincida con la estructura que se mantiene. Al suceder este evento tanto el receptor como el emisor reciben un paquete de rechazo y Suricata genera una alerta.

- **Alerta**

Si el algoritmo coincide con una alerta, el paquete podrá transportarse sin ningún problema. Sin embargo; Suricata genera una alerta que solo visualizará el administrador del sistema.

3.2.2.1.2 Encabezamiento

El algoritmo que maneja Suricata dentro de sus parámetros se encuentra especificado por el protocolo de control de la regla, esto puede ser en primera instancia tcp que se utiliza para tráfico *tcp* sin discriminación.

En segunda instancia tenemos *udp, icmp e ip – ip* siendo este último el que engloba todos los protocolos de esta etapa. Finalmente tenemos los protocolos http, ftp, smtp, tls que incluyen *ssl*.

Por medio de estas fases Suricata discrimina en su algoritmo el protocolo analizado siendo esto un parámetro específico para su análisis.

3.2.2.1.3 Opción de regla.

Dentro de los diferentes parámetros que mantiene el algoritmo de Suricata se encuentra la estructura de la regla en donde se establecen lo siguiente:

- **Parámetros de origen y destino de puertos.** - Como se observa en las Figuras 15 y 16 se puede parametrizar uno o varios puertos siendo estos de origen o destino cuyo objetivo es el de discriminar el tráfico entrante y saliente.

```
 !  excepción / negación
: distancia
[] signos para aclarar qué partes pertenecen juntas
, separación
```

Figura 15. Instancias de configuración Puertos.

Tomado de (Suricata, 2016)

```
 [80, 81, 82] (puertos 80, 81 y 82)
[80: 82] (Rango de 80 a 82)
[1024:] (Desde 1024 hasta el número de puerto más alto)
! 80 (Todos los puertos, excepto 80)
[80: 100,! 99] (Rango de 80 a 100 pero 99 excluidos)
[1:80,! [2,4]]
[.... [.....]]
```

Figura 16. Parametrización de Puertos.

Tomado de (Suricata, 2016)

- **Dirección.** – En este punto se establece los lineamientos de comunicación fuente destino o destino fuente para ello se deberá contar con la estructura de la Figura 17.

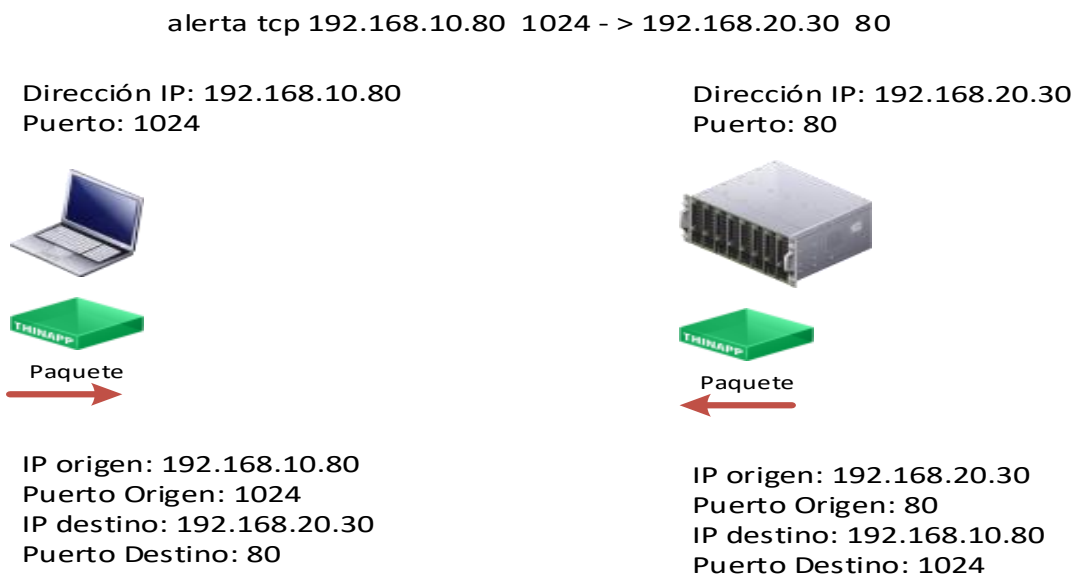

Figura 17. Estructura Fuente Destino

A continuación, se muestra en la Figura 18 un modelo de la estructura completa de algoritmo Suricata

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET
TROJAN Likely Bot
Nick in IRC (USA +..)"; flow:established,to_server;
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;
reference:url,doc.emergingthreats.net/2008124;
reference:url,www.emergingthreats.net/cgi-
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;
sid:2008124; rev:2;)
```

Figura 18. Estructura de Sintaxis de Suricata.

Tomado de (Suricata, 2016).

3.2.2.2.4 Estructura del Sensor IPS

El método de configuración de los sensores del sistema de prevención de intrusiones se encuentra conectado a un conmutador principal en cuyo caso la

interfaz debe estar configurada en modo *SPAN* (espejo) estableciendo los sensores de tal manera que se logre obtener los registros de todo el tráfico que se encuentre en la red como se puede observar en la Figura 19.

La función principal del conmutador de red es el compartir intrínsecamente los datos que se generen en sí mismo distribuyendo a todos los puertos y en base a la infraestructura propia de la empresa se realiza la segmentación de los sensores del IPS conforme a los lineamientos antes mencionados.

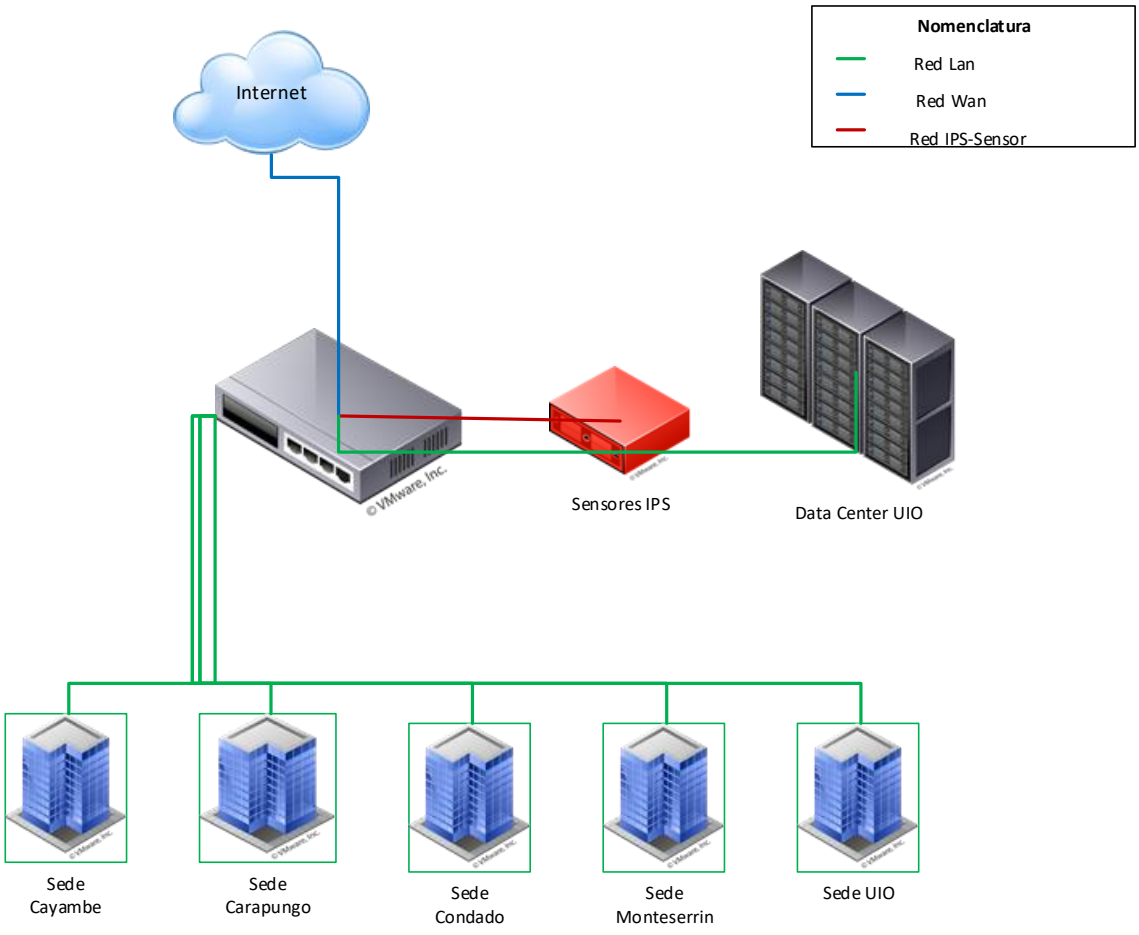

Figura 19. Esquema de Ubicación de Sensor IPS-IDS

3.2.3 Operatividad del IPS-IDS

El sistema de detección de intrusiones es capaz de identificar de una manera óptima las alertas que se generen en la red de datos de la empresa, para ello es importante que el sistema realice una categorización de eventos que permitan

obtener reportes de verdaderos positivos, verdaderos negativos y falsos positivos, como se puede visualizar en la Figura 20.

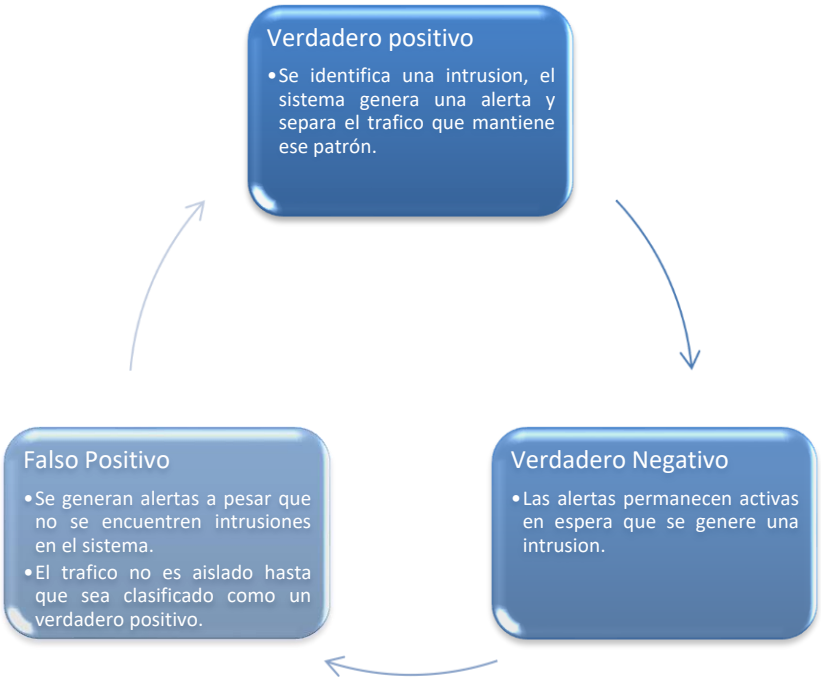

Figura 20. Ciclo de Operación de IPS-IDS

3.3 Requerimientos de Hardware y Software del Sistema de Prevención y Detección de Intrusos.

Es sistema de detección y prevención de intrusiones requiere de componentes de hardware y software de uso exclusivo de la plataforma destinada para este fin, por lo que es necesario que cumplan con las especificaciones detalladas a continuación:

3.3.1 Requerimiento de Hardware

Como requisitos mínimos el sistema de prevención y detección de intrusiones deberá cumplir a más de los requerimientos propios de la empresa con las siguientes características:

- Procesador de 2 núcleos x64 o superior. – Ya que se requiere que el sistema sea capaz de ejecutar múltiples hilos de procesamiento que soporten la generación de alertas y logs en *real time*, es esencial que el

procesador cuente con más de un núcleo para que pueda cubrir los requerimientos de multiprocesamiento del motor Suricata.

- Memoria RAM de 8 Gigabytes o superior. - Considerando que el sistema no requiere de un entorno gráfico el cual amerite un consumo de memoria elevado o superior a los 256MB, tomando en cuenta que las tareas de monitoreo y procesos de datos simultáneos ocupa el 33% del total de la memoria instalada. Se requiere un mínimo de memoria RAM de 2.64GB. Sin embargo, a medida del crecimiento de la información se requerirá mayor volumen de memoria. Adicionalmente considerando los 5 años de vida útil que tendrá el sistema se recomienda un mínimo de memoria RAM de 8GB.
- Tres interfaces de Red o tarjetas Ethernet. - Para su funcionamiento el sistema requiere de dos interfaces de red distribuidas de la siguiente forma una para la administración y otra que actuará de *sniffer* de red o sensor. A pesar de que con los parámetros físicos de hardware de red descritos anteriormente el sistema operaria sin problema se deberá considerar una tarjeta de red adicional con el fin de cubrir un eventual fallo de hardware.
- Un Disco duro de capacidad de 1Terabyte o superior. - Se requiere de la cantidad de almacenamiento detallada anteriormente, ya que por motivos de almacenamiento de logs del sistema éste almacenará los eventos que se produzcan en toda la red de datos de la empresa de manera incremental así tenemos:

  Almacenamiento diario

  $$Diaria = 492\ Mb$$

  Almacenamiento Semanal

  $$Semanal = 492\ Mb \times 7 = 3.4\ Gb$$

  Almacenamiento Mensual

  $$Mensual = 492\ Mb \times 30 = 14.76\ Gb$$

Almacenamiento Anual

$$Anual = \ 492\ Mb \times 365 = 179.58\ Gb$$

Proyección de capacidad a 5 años

$$Mensual = \ 179.58 \times 5 = 897.90\ Gb$$

Cabe mencionar que la empresa como requerimientos propios de hardware considera los siguientes:

- Equipo de cómputo Core i5 o superior;
- Almacenamiento de 1 Tb o superior; y,
- Memoria RAM 8 Gb o Superior.

3.3.2 Diagrama de Software

El sistema de detección y prevención de intrusiones deberá implementarse bajo la plataforma de GNU / LINUX con el fin de no incurrir en gastos de licenciamiento de software para la empresa a pesar de que el mismo es compatible tanto para arquitecturas Windows como Linux, dentro de esta última plataforma la compatibilidad del sistema se puede desarrollar bajo las siguientes distribuciones:

- Debian 8 o superior;
- Centos 6 o superior;
- Fedora 22 o superior;
- Ubuntu 11 o superior; y,
- OpenSuse 13.

El sistema operativo que se recomienda instalar es Debian en su versión 9 acompañado del software Suricata 4.0 para que la implementación cuente con las últimas actualizaciones tanto del sistema operativo como del sistema de prevención y detección de intrusiones conforme con la normativa de las buenas prácticas como lo indica el Apartado A-14 del Anexo A de la norma ISO 27001 literal .14.1.5.¨ Los planes de continuidad del negocio se probarán y actualizarán

regularmente para asegurarse que estén actualizados y sean efectivos.¨ (ISO, 2005)

3.3.2.1 Diagrama Estructural de Software

A continuación, en la Figura 21 se observa a nivel estructural las dependencias de software necesarias para el sistema de prevención y detección de intrusiones.

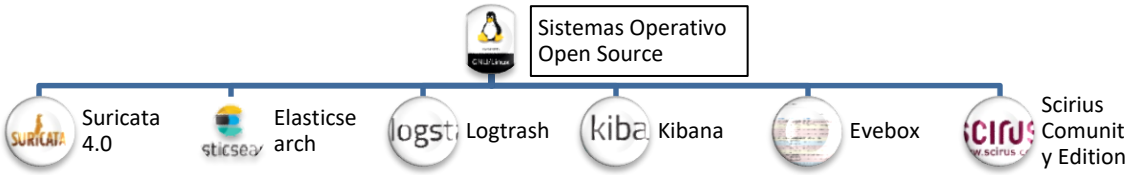

Figura 21. Estructura de Software

4. Capítulo IV. Implementación del Sistema de Prevención y Detección de Intrusiones.

Este capítulo trata de la instalación del hardware y software requerido para la puesta en marcha del sistema de prevención y detección de intrusiones en la empresa PROAUTO C.A., así como también se describe los lineamientos requeridos pre y post instalación de los paquetes de software necesarios para la puesta en marcha de la solución de IPS-IDS Suricata y su administración.

4.1 Paquetes de Software requeridos para la instalación

El sistema operativo en el cual se implementará la solución de prevención y detección de intrusos es Debían 9 ya que el mismo fue sometido a varias pruebas en conjunto con el motor de detección SURICATA 4.0 a esto se suma la facilidad de administración que presenta para infraestructuras en producción, así como en ambientes web, ya que es robusta y todas estas características suponen una ventaja frente a otros sistemas como Centos que está en su versión 7 que solo ha sido probado con suricata 3.1 (Suricata, s.f.).

Dentro de los paquetes de software complementarios que se necesitan adicionar sobre Debian 9 se listan los siguientes:

- Suricata versión 4.0.4;
- Elasticsearch;
- Logstash;
- Kibana;
- Paquetes *Scirius Comunity Edition; y,*
- EveBox

Estos paquetes son *opensource* al igual que Suricata, por lo cual no requieren de activación alguna o licenciamiento siendo fundamentales para que la solución IPS-IDS funcione adecuadamente.

4.2 Instalación

Una vez instalado el sistema operativo Linux en su versión Debian 9 se procede con la siguiente secuencia de instalación de los paquetes y dependencias descritos en la Figura 22.

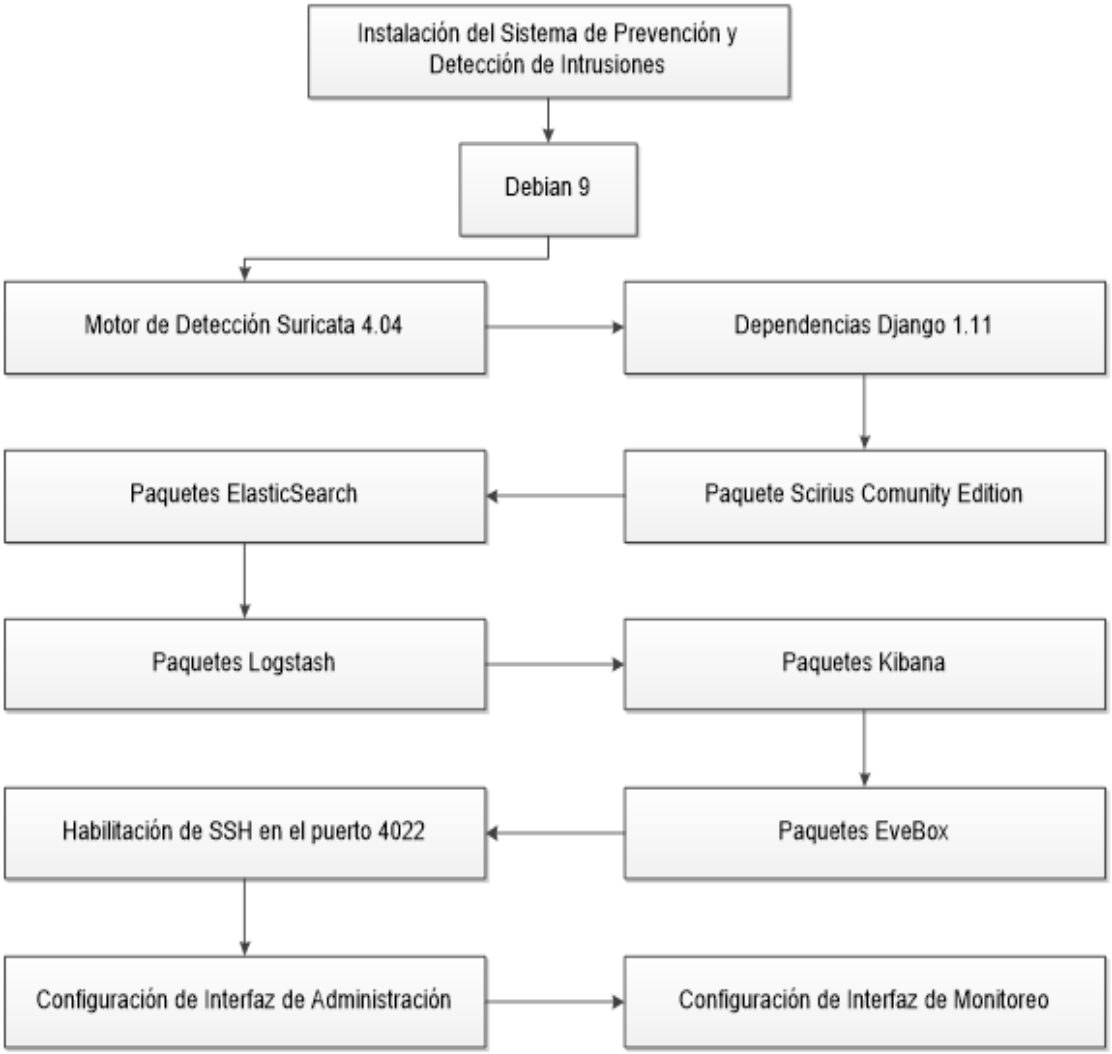

Figura 22. Diagrama de Instalación de Sistema de Prevención y Detección de Intrusiones.

- **Debian 9.-** Es un sistema Operativo Base, sobre el cual se instalarán las dependencias de Suricata que es una distribución compatible con las arquitecturas de procesadores i386, amd64 y arm64 entre las arquitecturas de procesadores más importantes. Este sistema operativo cuenta con mejoras y actualizaciones continúas previo a su liberación lo cual lo hace seguro, confiable y con una buena estabilidad por lo que es recomendado para aplicaciones de administración web o http excepto si se destina para levantamiento de servicios de *hosting* a través de cpanel.
- **Suricata 4.04.-** Es un motor de Detección de Intrusiones en su última Versión estable, actualmente está entre los mejores de detección y

prevención de intrusiones debido a sus características de multiprocesamiento, detección de protocolos, almacenamiento de eventos, etc.

- **Django1.11.-** Es un Software complementario requerido para la integración entre suricata y sus dependencias, convirtiéndose en un framework para la interacción del software complementario.
- **Scirius Comunity Edition.-** Es un gestor y administrador de reglas para Suricata, siendo el responsable de permitir al administrador gestionar de una forma sencilla, gráfica y eficiente las reglas del motor IPS-IDS
- **ElasticSearch.-** También es un gestor de la información obtenida de Suricata es decir, que es aquel que realiza una búsqueda de datos en tiempo real de alta escala y velocidad, así como también permite búsquedas múltiples y realiza una indexación de la data como se puede visualizar en la Figura 23.

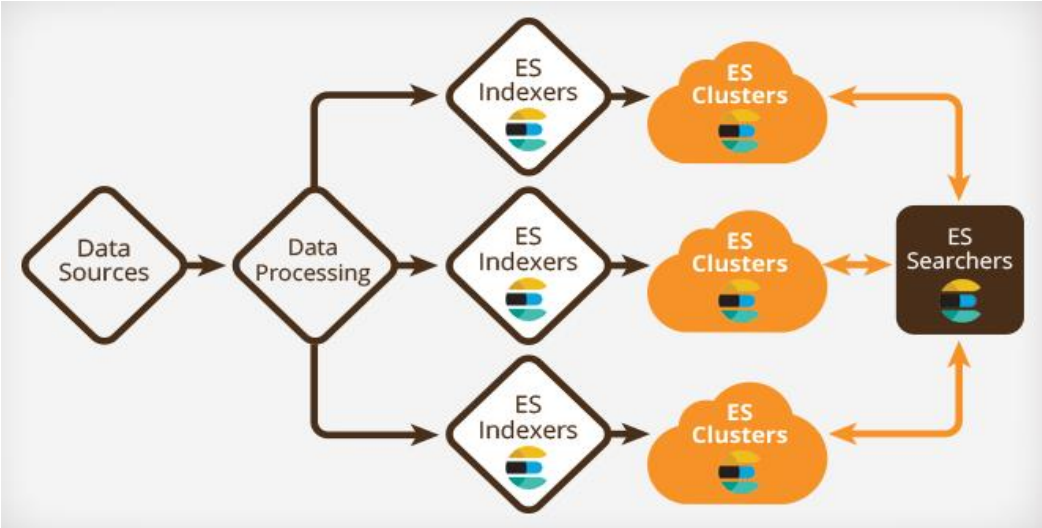

Figura 23. Estructura de ElasticSearch

Tomado de: (Krenn, 2017).

- **Logstash. -** Permite la interpretación de los logs generados por el motor suricata u otras plataformas como se puede visualizar en la Figura 24.

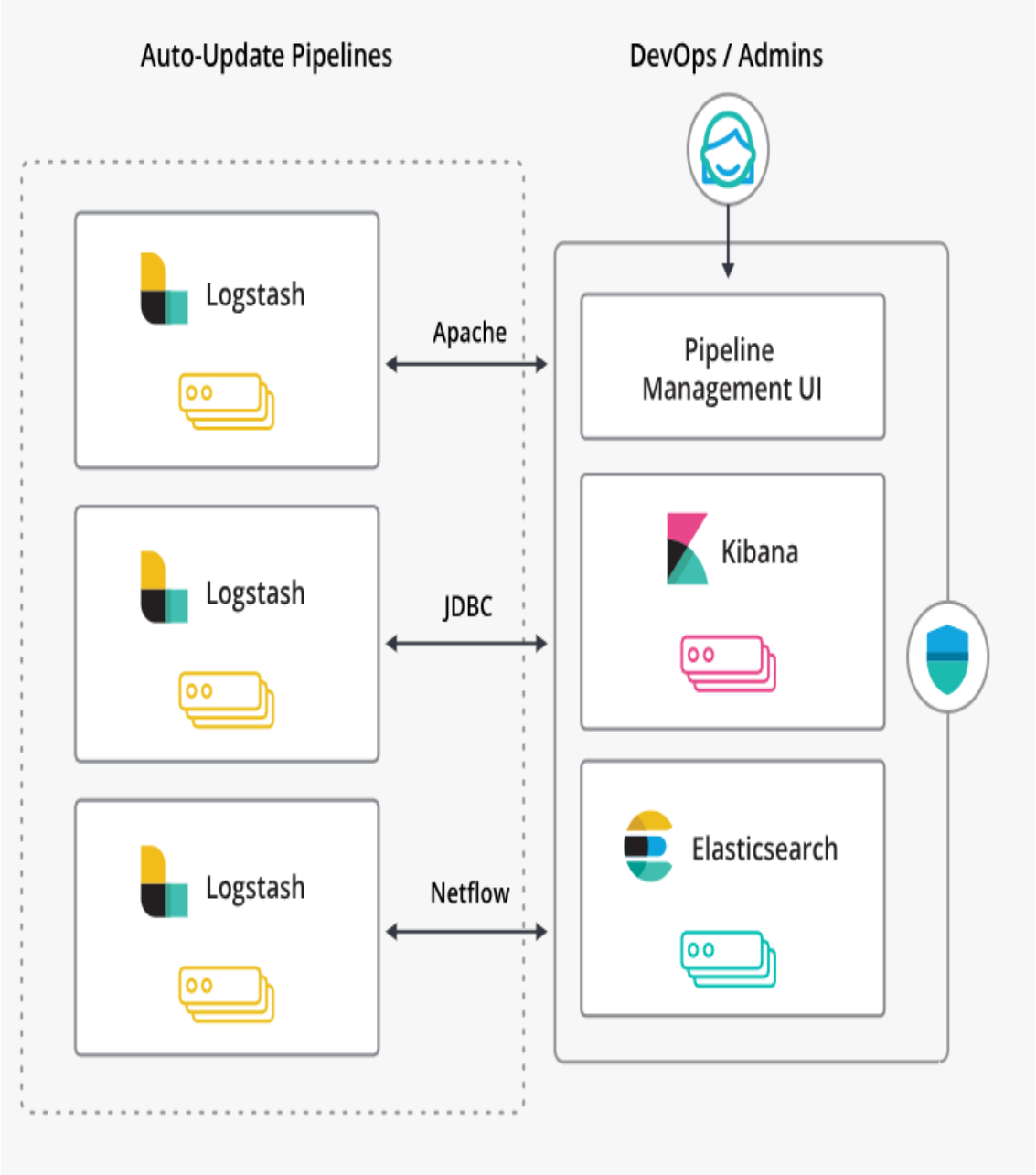

Figura 24. Estructura de Logstash

Tomado de: (Elastic, s.f.)

- **Kibana. -** Es el gestor de la interfaz gráfica para una visualización de la información generada por Suricata, permitiendo una mejor gestión y comparación de los resultados arrojados como se observa en la Figura 25.

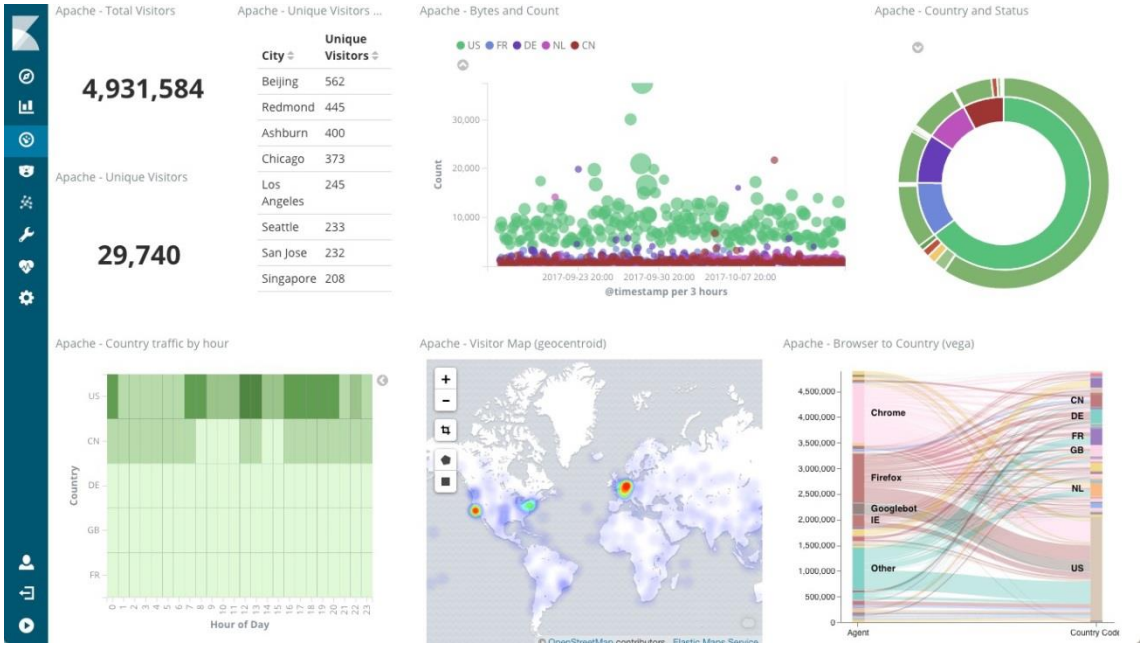

Figura 25. Kibana

Tomado de: (Elastic, s.f.)

- **EveBox:** Es el gestor de eventos generados por Suricata. Controla emite y administra las alertas provocadas por el motor de detección como consta en la Figura 26.

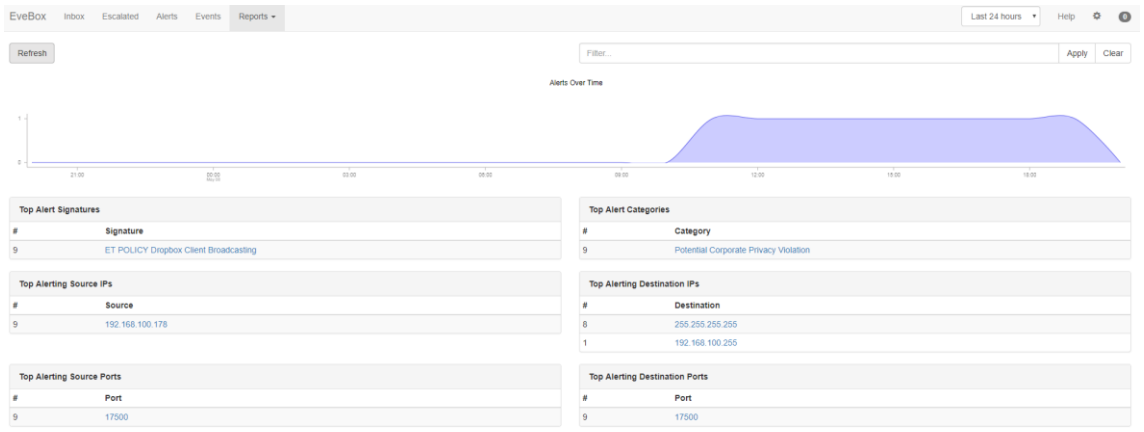

Figura 26. Panel Evebox

- **SSH. -** *Secure Shell* es el protocolo de administración remota del servidor Debian 9 cuyo puerto fue cambiado por seguridad al 4022 y se utiliza para

poder configurar o realizar cambios en los parámetros del sistema de una manera confiable.

- **Interfaz de Administración. -** Es el puerto físico y lógico que servirá como enlace para la gestión y administración del sistema IPS-IDS, ésta interfaz estará en otro segmento distinto a la de la red LAN empresarial para de esta forma precautelar la seguridad del sistema de prevención y detección de intrusiones.
- **Interfaz de Monitoreo. -** Es aquella interfaz que funciona en modo promiscuo o sniffer dedicada al monitoreo de intrusiones en la red de datos siendo responsable de capturar el tráfico malicioso que pudiese ingresar en el flujo de datos para que el motor de detección pueda realizar su trabajo.

4.2.1 Configuración Sistema Operativo Debian.

4.2.1.1 Parametrización del sistema operativo.

Una vez realizada la configuración de los parámetros básicos de instalación del sistema operativo, se realiza la parametrización de la tarjeta de red de administración como se muestra en la Figura 27**.**

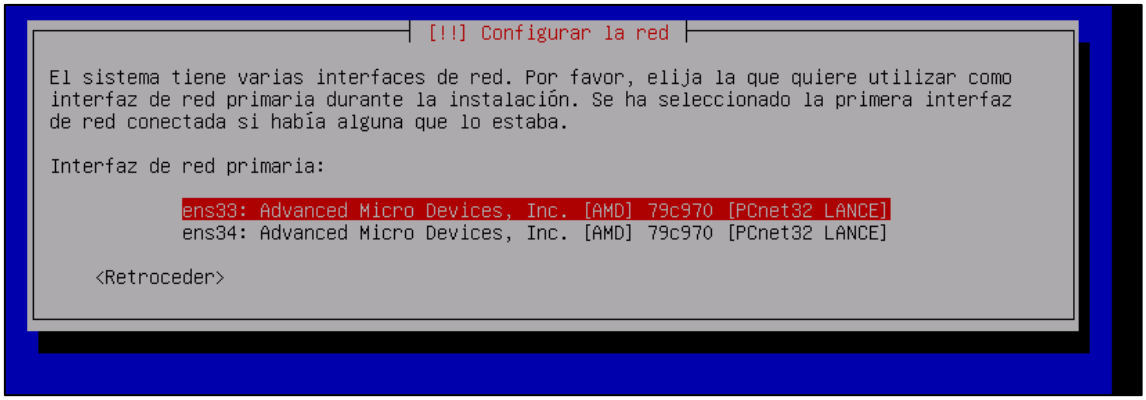

Figura 27. Pantalla de Instalación Debian Configuración de Interfaces

Al ser una interface de administración se configura mediante parámetros estáticos el cual contiene direccionamiento ip, mascará de red y puerta de enlace, como se muestra en la Figura 28 y 29.

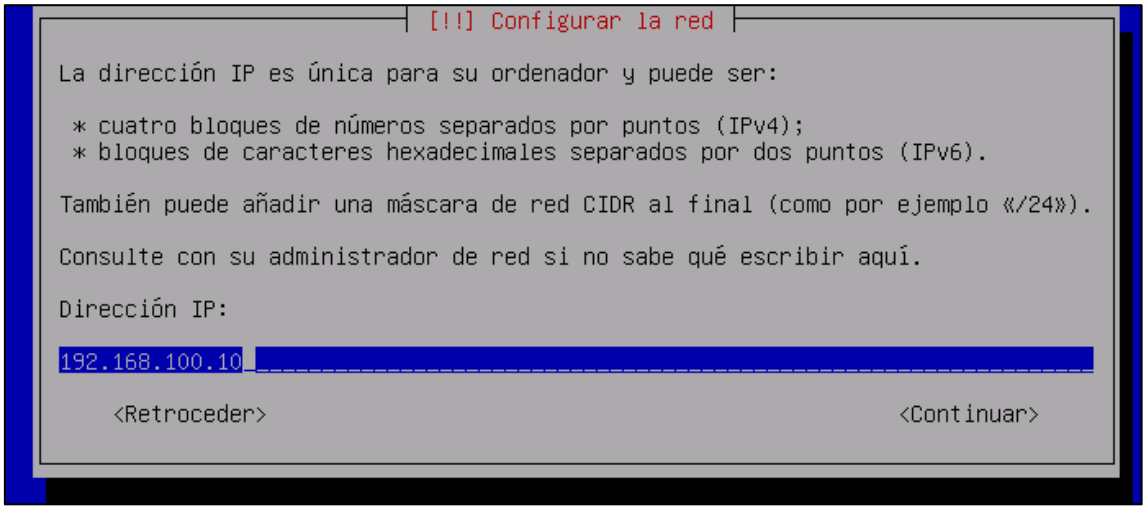

Figura 28. Asignación de Direccionamiento.

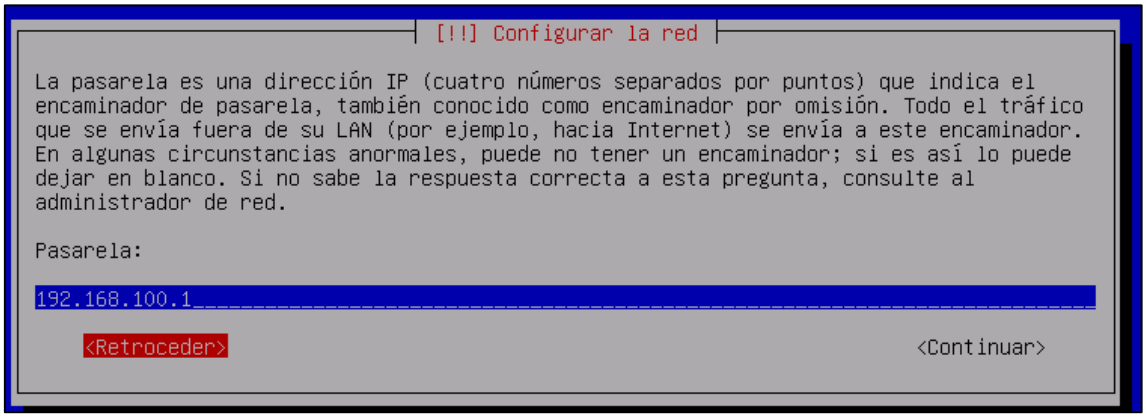

Figura 29. Asignación de puerta de Enlace.

Para la identificación del nombre del servidor se sigue la estructura del diagrama que se observa en la figura 30, según la normativa vigente para los servidores de la empresa.

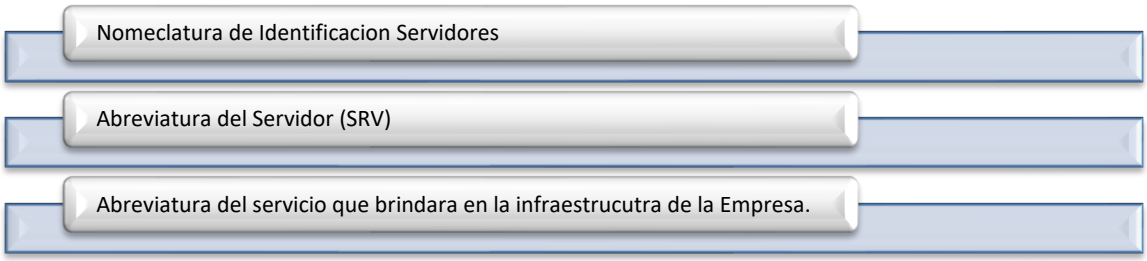

Figura 30. Esquema de Nomenclatura

En la Figura 31**,** se visualiza el esquema de nomenclatura de identificación destinado al servidor de producción.

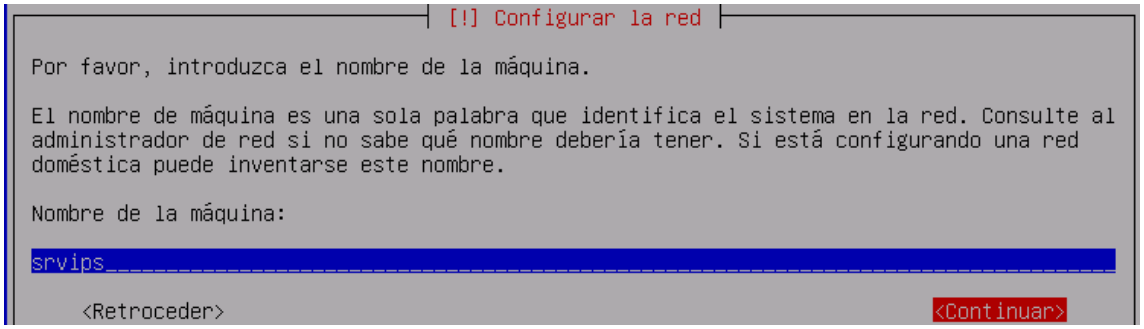

Figura 31. Pantalla de ingreso de nombre del host

4.2.2 Configuración Sistema de Prevención y Detección de Intrusiones Suricata.

4.2.2.1 Parametrización de Suricata.

Una vez realizada la configuración de los parámetros del sistema operativo, se realiza la parametrización de SURICATA con lo cual primero se configura el servicio de sshd con el fin de poder acceder al servidor de manera remota como se muestra en la Figura 32**.**

```
root@srvips:~# vim /etc/ssh/sshd_config
```

Figura 32. Línea de Comando para Configuración de SSH en Debian 9

Para el ingreso mediante ssh usaremos el puerto de comunicación 4022 precautelando que el acceso a la administración del sistema no se lo realice por el puerto por defecto del servicio ssh como se visualiza en la Figura 33.

```
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Port 4022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Figura 33. Configuración de SSH

Adicionalmente como se indica en la Figura 33 se habilita el acceso como super usuario root.

4.2.2.1.2 Configuración de Interface Modo Promiscuo.

Para monitorear e identificar el tráfico que se produzca en la red el motor SURICATA debe mantener como parte de su configuración una tarjeta de red que se encuentre en modo promiscuo, este modo permite monitorear los paquetes que se transmitan a través de la red. El comando que permite listar e identificar los modos operación de las tarjetas de red es ifconfig –a como se observa en la Figura 34.

```
Last login: Tue May  8 21:48:56 2018 from 192.168.100.178
root@srvips:~# ifconfig -a
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.10  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::e269:95ff:fe2f:dbb  prefixlen 64  scopeid 0x20<link>
        inet6 2800:bf0:287:1025:e269:95ff:fe2f:dbb  prefixlen 64  scopeid 0x0<gl
obal>
        ether e0:69:95:2f:0d:bb  txqueuelen 1000  (Ethernet)
        RX packets 91208  bytes 48168429 (45.9 MiB)
        RX errors 0  dropped 49  overruns 0  frame 0
        TX packets 72202  bytes 28321388 (27.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 20  memory 0xfe500000-fe520000

enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::2e0:52ff:feb3:3537  prefixlen 64  scopeid 0x20<link>
        inet6 2800:bf0:287:1025:2e0:52ff:feb3:3537  prefixlen 64  scopeid 0x0<gl
obal>
        ether 00:e0:52:b3:35:37  txqueuelen 1000  (Ethernet)
        RX packets 35336  bytes 8003997 (7.6 MiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 488  bytes 40028 (39.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 640002  bytes 183410448 (174.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 640002  bytes 183410448 (174.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 34. Listado de Interfaces de Red

Mediante el detalle de configuración de las tarjetas de red como consta en la Figura 34**,** se indica que la tarjeta de red eno1 es destinada a la administración y la tarjeta enp1s0 es la que se encontrará en modo promiscuo.

Como segundo se le indica al motor Suricata cuál es la tarjeta de red que se encuentra en modo promiscuo debiendo modificar el archivo de configuración como se observa en la Figura 35.

```
auto enp1s0
iface enp1s0 inet manual
    pre-up ifconfig $IFACE up
    post-down ifconfig $IFACE down
    post-up /etc/network/if-up.d/idps-interface-tuneup_stamus
```

Figura 35. Parámetros de Configuración de Interfaz en modo Promiscuo Debian.

Una vez generado el registro de la tarjeta en modo promiscuo en el archivo de configuración del servidor se indica la parametrización de la tarjeta al servicio de stamus network para monitorear el tráfico por esa interface como se demuestra en la Figura 36.

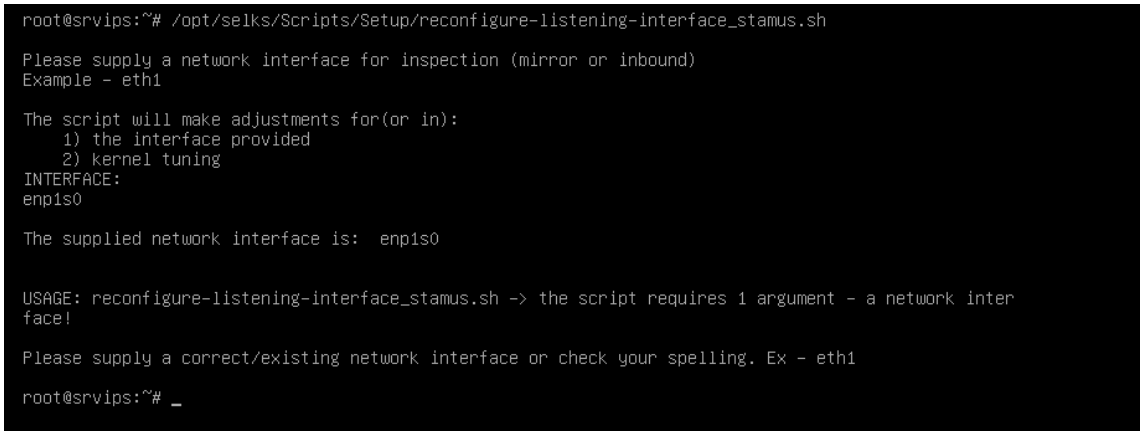

Figura 36. Definición de Tarjeta en Modo Promiscuo para paquetes Scirius.

A continuación, se modifica la línea 568 del archivo de configuración de Suricata en el cual se indica el nombre de la interface que se encuentra en modo promiscuo como se observa en las Figuras 37 y 38.

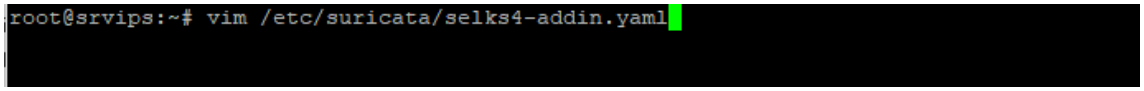

Figura 37. Parametrización de Interfaz en Suricata

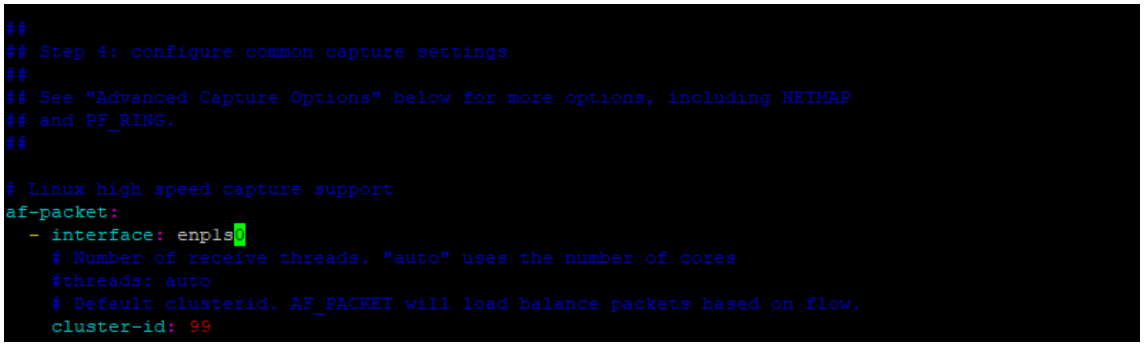

Figura 38. Configuración de Interfaz de Red Archivo de Parámetros Suricata

4.2.2.1.3 Validación de Motor de búsqueda Suricata.

Como procedimiento final, se realiza el monitoreo de la instalación y servicios del motor de búsqueda SURICATA para lo cual se ingresa al registro de operación en el cual se evidencia que se encuentra ejecutándose sin ningún error como consta en la Figura 39.

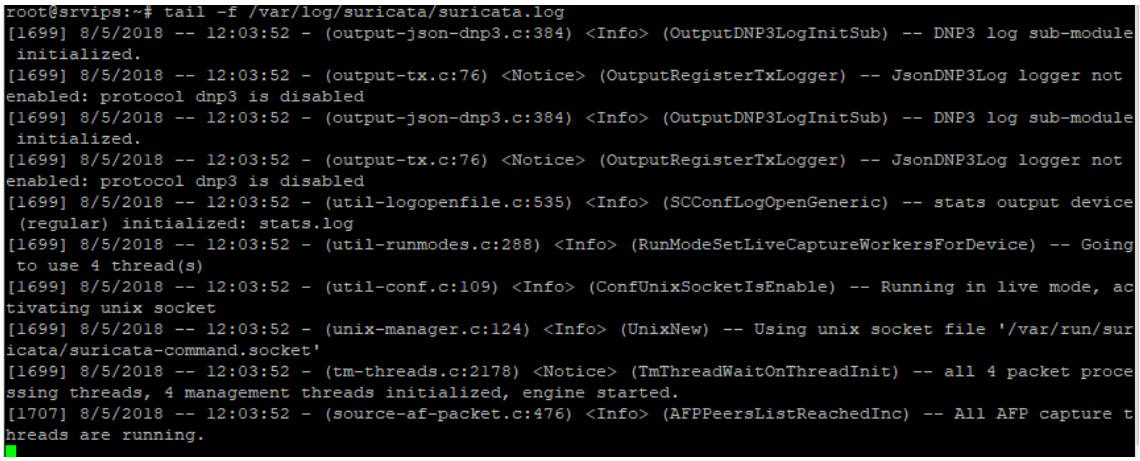

Figura 39. Archivo de log de Suricata.

4.2.3 Ingreso al Sistema de Prevención y Detección de Intrusiones.

4.2.3.1 Ingreso interface gráfica Scirius.

Para ingresar a la consola de administración se accede a través de un navegador a la dirección IP destinada como administración mediante el protocolo https. Como se evidencia en la Figura 40.

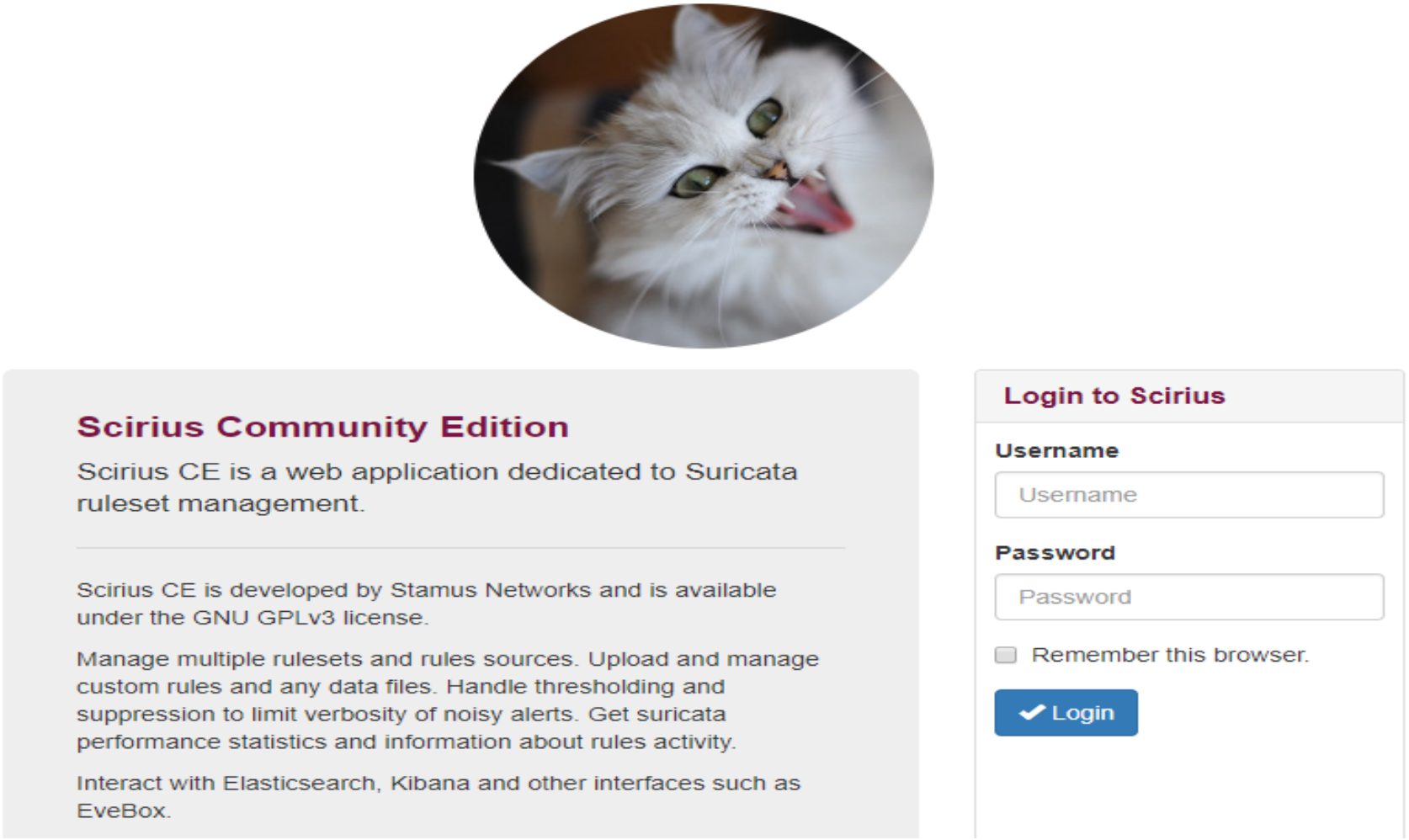

Figura 40. Pantalla de Login de Gestor de Administración Scirius para Suricata

En la interface gráfica del Sistema Suricata podemos observar las actividades de alerta, así como también las reglas, paquetes y uso de hardware en tiempo real como se indica en la Figura 41.

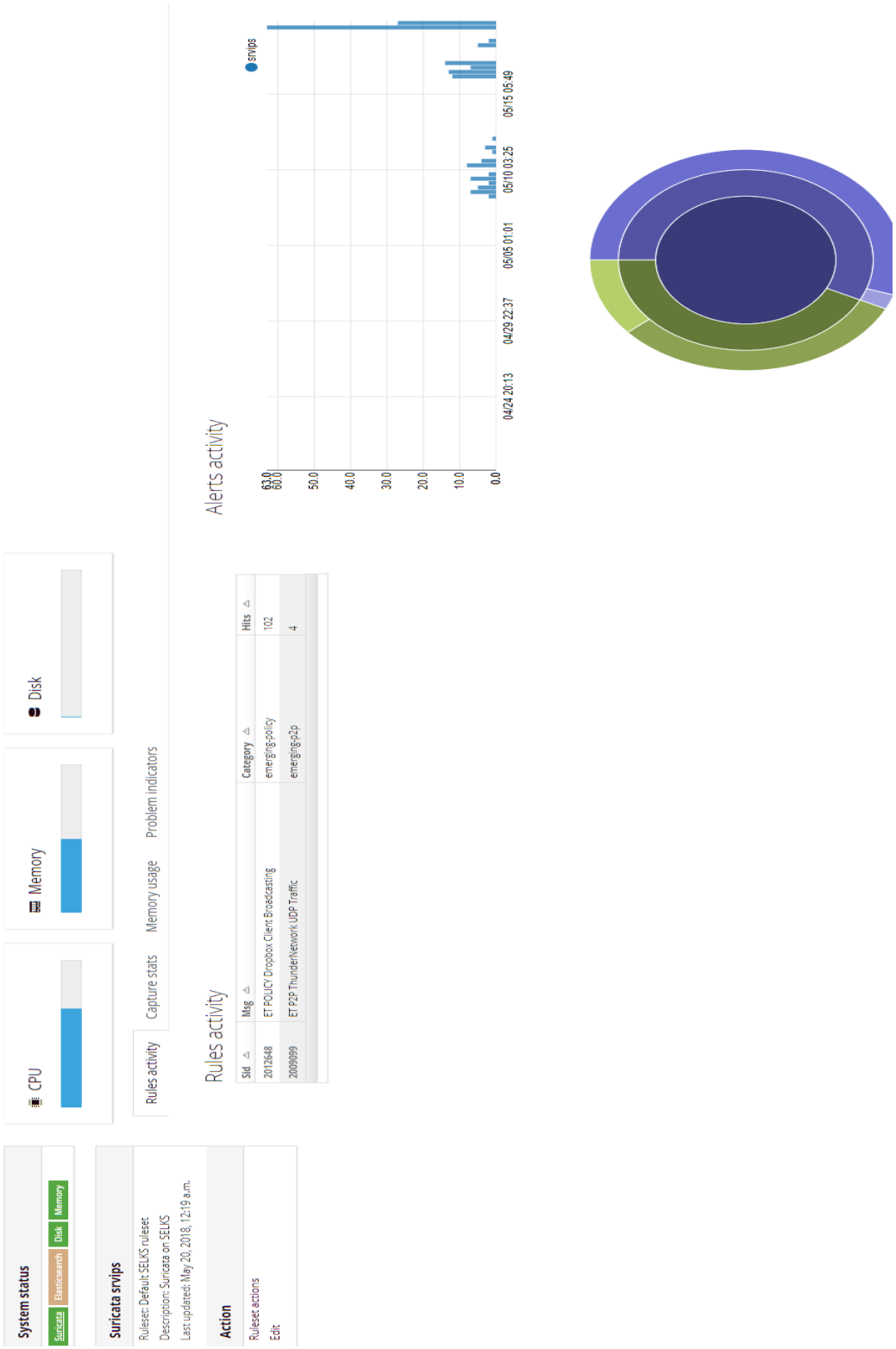

Figura 41. Pantalla Principal de Administración Scirius para Suricata

4.3 Actualización de Reglas

Una vez realizada la instalación de las herramientas de hardware y software es necesario realizar una actualización de Reglas de Suricata, lo cual garantiza que las reglas de la solución estén actualizadas con los últimos parches de seguridad el procedimiento se indica en la Tabla 6.

Tabla 6.

Actualización de Reglas para Suricata

Desde El panel de Administración	Suricata→Action→Update
Desde la Consola por Terminal	Python manage.py updatesuricata

4.4 Configuración de Reglas

Al estar el sistema IPS-IDS instalado de forma correcta en conjunto con los paquetes de gestión gráfica y de análisis se procede a configurar las reglas y políticas personalizadas creadas en el capítulo III, las mismas que se detallan en el Anexo C.

5. Capítulo V. Pruebas y Validación de la Solución IPS-IDS.

Este capítulo contiene la documentación probatoria de las alertas y bloqueos que el sistema de prevención y detección de intrusiones Suricata detecta en la red de la empresa PROAUTO.

5.1 Pruebas de Operación de la Implementación del Sistema de Prevención y Detección de Intrusiones.

5.1.1 Validación de Módulos Scirius para Suricata.

Para la validación del correcto funcionamiento de las dependencias que contemplan la plataforma Scirius se ingresa utilizando el browser de un navegador a la dirección ip asignada al servidor la misma que por su seguridad es confidencial visualizando posteriormente la Figura 42.

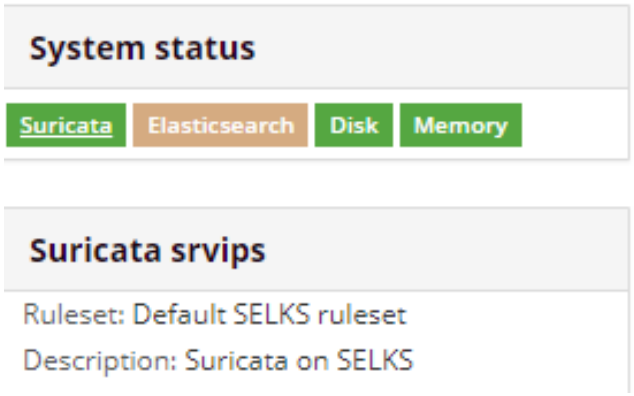

Figura 42. Estado de dependencias Scirius.

5.1.2 Prueba de Funcionamiento de Suricata

Para verificar el funcionamiento del motor Suricata en modo IDS se ejecuta el siguiente comando:

" tail -f /var/log/suricata/fast.log"

El resultado esperado es el que se muestra en la Figura 43, en donde se puede observar la fecha y hora del evento acompañado de una breve descripción de la política donde se indica el origen y destino de la incidencia en base al protocolo tcp/ip v4.

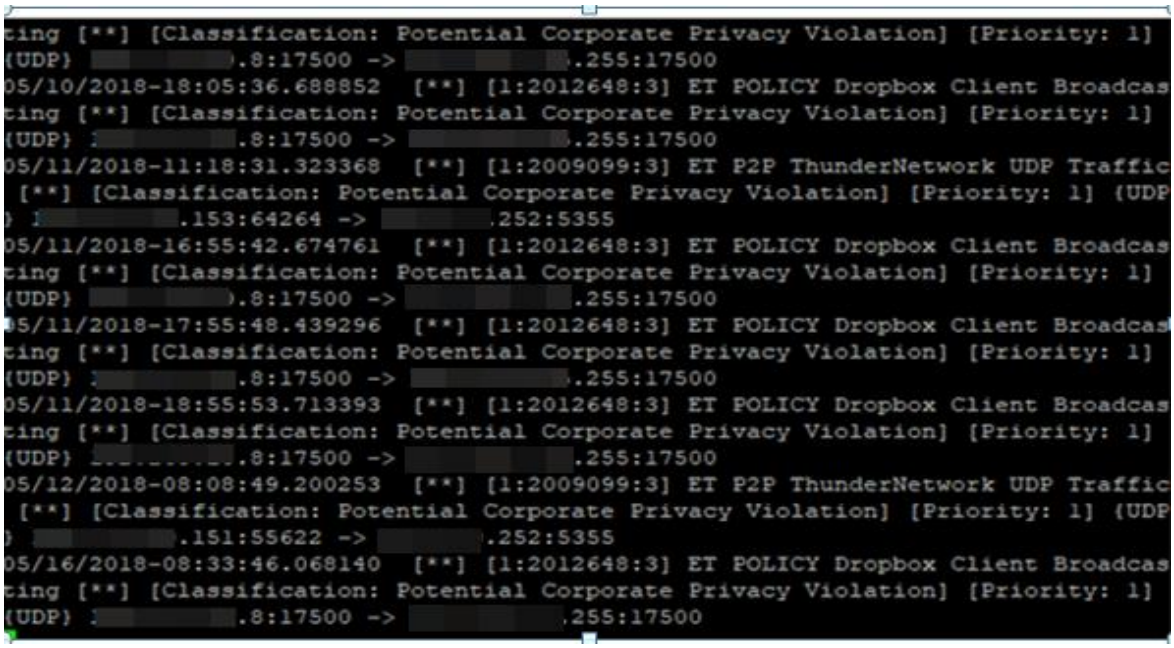

Figura 43. Log de Detección

5.1.3 Actualización de Módulos

Ya que el sistema de prevención y detección de intrusiones se encuentra alineado con la norma ISO 27001 se realiza la actualización y *upgrade* de toda la plataforma, así como de sus dependencias mediante el siguiente comando:

"apt-get update && apt-get upgrade"

En la Figura 44 se puede evidenciar que el sistema, así como también las dependencias se encuentran actualizadas y a la fecha no existen nuevas versiones de los módulos que contemplan esta solución.

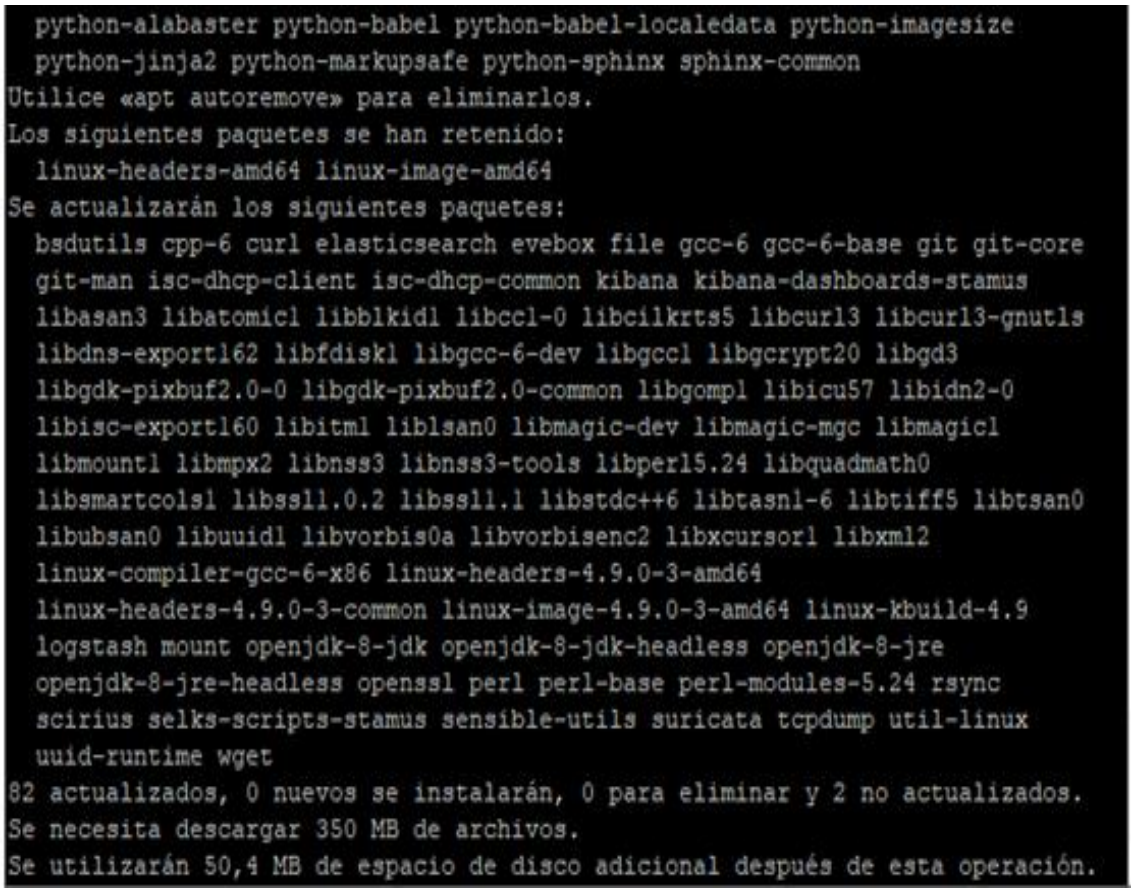

Figura 44. Promt de estado de actualización de módulos

5.2 Suricata como IDS

Para la validación del sistema de detección de intrusiones, se ha realizado la creación de dos reglas de incidencias siendo una la que notifique los intentos de acceso a una nube privada y la otra a las conexiones que se realicen en base al protocolo p2p desde los *hosts* como se puede evidenciar en la Figura 45.

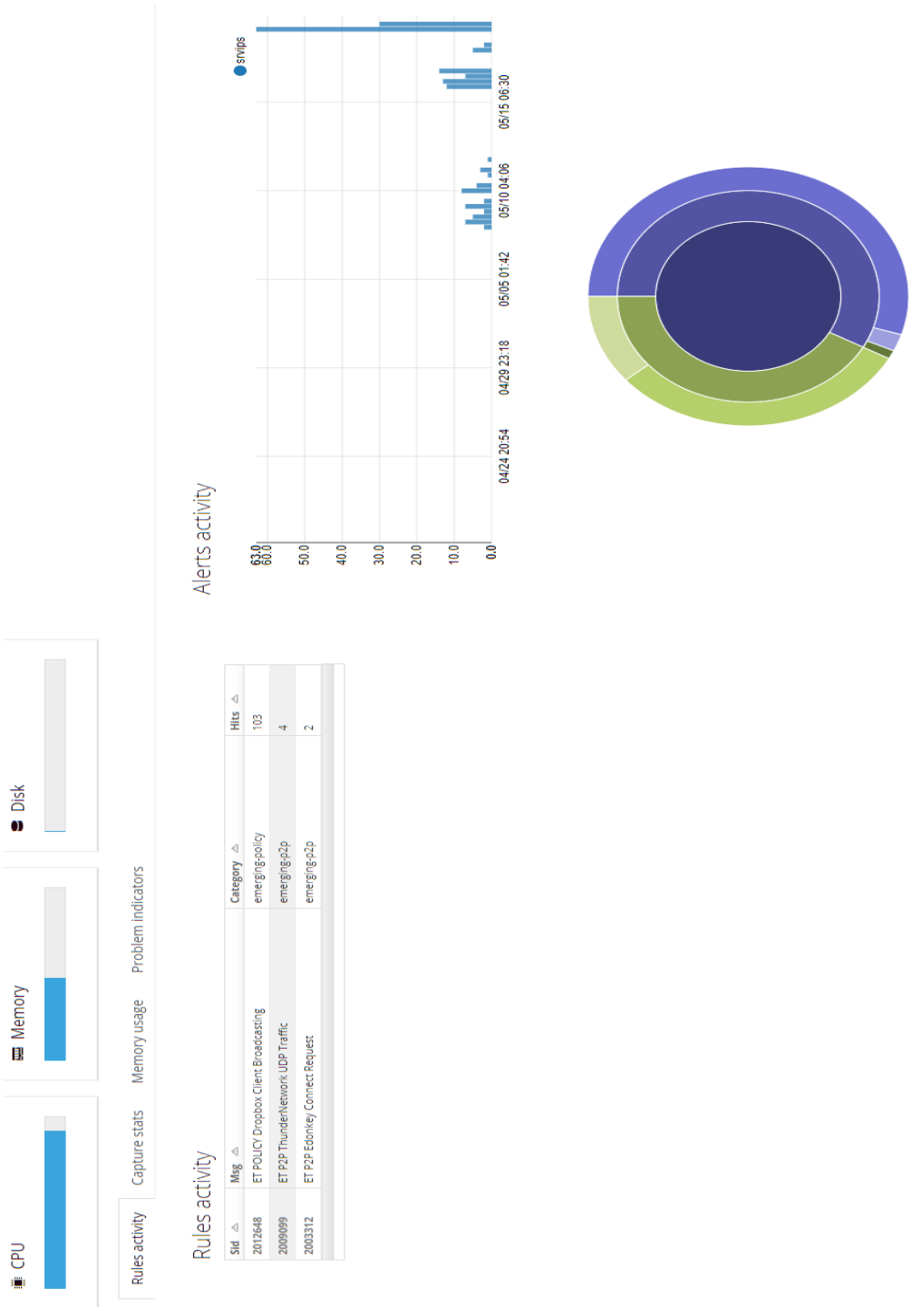

Figura 45. Reporte de funcionamiento IDS.

Como parte de la información que nos despliega el sistema se puede obtener el detalle del número de intentos de conexión por direccionamiento ip de origen, así como también; el destino que mantuvo la conexión como se evidencia en la Figura 46.

Figura 46 Reporte de incidencias IPS

Adicional a la información del IDS tenemos datos de geolocalización, lista de amenazas de conexiones y destino como se desprende de la Figura 47.

Figura 47. Reporte de conexión ONYPHE.

5.2.1 Visor de Gráficas Kibana

El paquete Kibana nos permite ver de manera gráfica una estadística de la cantidad de eventos vs las horas de los sucesos, lo que permite analizar cronológicamente las horas con mayor número de incidencias y cuáles de ellas se producen con mayor frecuencia y poseen mayor severidad para la seguridad como se demuestra en la Figura 48.

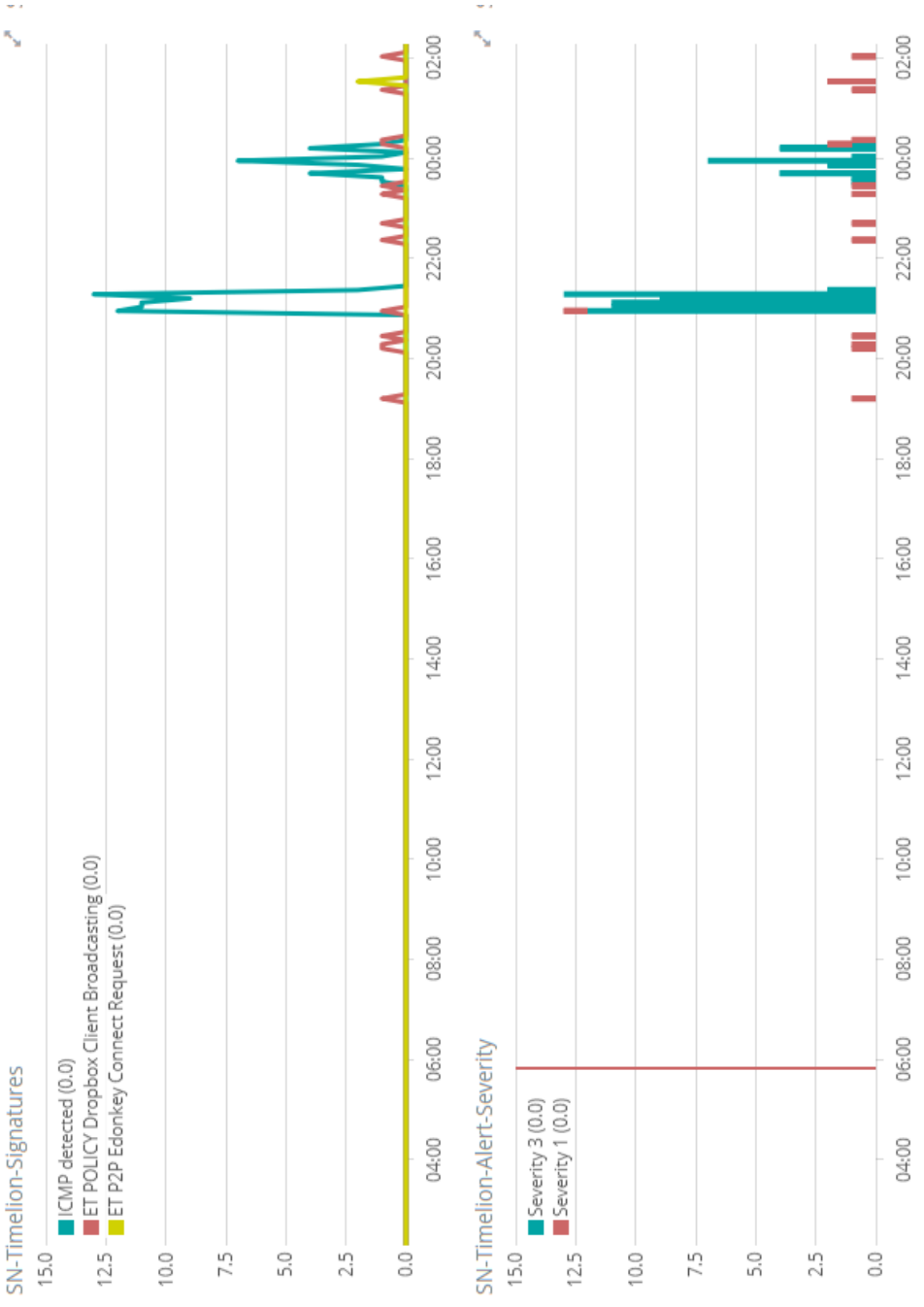

Figura 48. Reporte de funcionamiento IDS

5.2.2 Panel de Registros de Logstash

Como se visualiza en la Figura 49 y 50 el gestor de logs se encuentra funcionando correctamente. Adicionalmente se tiene la información relacionada a la cantidad de espacio ocupada por el archivo incremental de los registros.

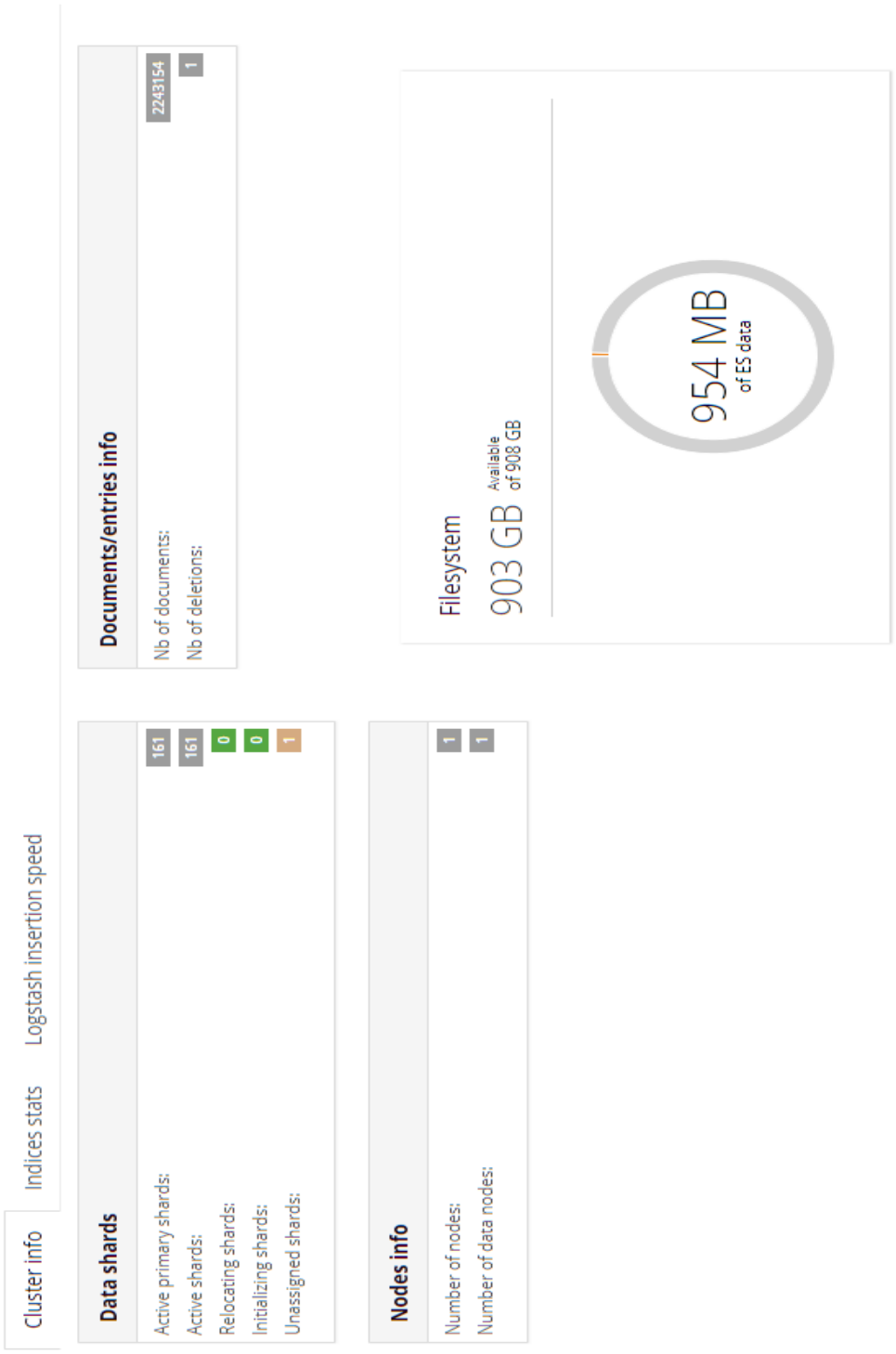

Figura 49. Dashboard de Logstash

Cluster info | Indices stats | Logstash insertion speed

Name	Count	Deleted
logstash-2018.05.17	18093	0
logstash-2018.05.12	13497	0
logstash-alert-2018.05.17	25	0
logstash-alert-2018.05.16	21	0
logstash-alert-2018.05.11	4	0
logstash-alert-2018.05.10	12	0
logstash-2018.05.09	12023	0
logstash-alert-2018.05.12	1	0
logstash-flow-2018.05.16	296036	0
logstash-flow-2018.05.17	269820	0
logstash-flow-2018.05.15	506	0
logstash-flow-2018.05.12	117194	0
logstash-alert-2018.05.18	7	0
logstash-flow-2018.05.10	405880	0
logstash-flow-2018.05.11	382859	0
logstash-2018.05.20	5029	0
logstash-2018.05.08	6787	0
logstash-dns-2018.05.16	4	0
logstash-flow-2018.05.18	198360	0
logstash-2018.05.18	18093	0
logstash-2018.05.19	13712	0
logstash-flow-2018.05.09	294116	0
logstash-2018.05.15	745	0
logstash-2018.05.16	7865	0
logstash-flow-2018.05.20	7199	0

Figura 50. Cantidad de Logs generados

5.2.3 Panel de Alertas de Evebox

El gestor de alertas nos indica de una forma detallada y segmentada por colores las incidencias de acuerdo al impacto de seguridad que tienen los eventos, siendo el color rojo para los eventos con un riesgo alto y el verde con uno menor o que aún no ha sido clasificado como alto como consta en la Figura 51.

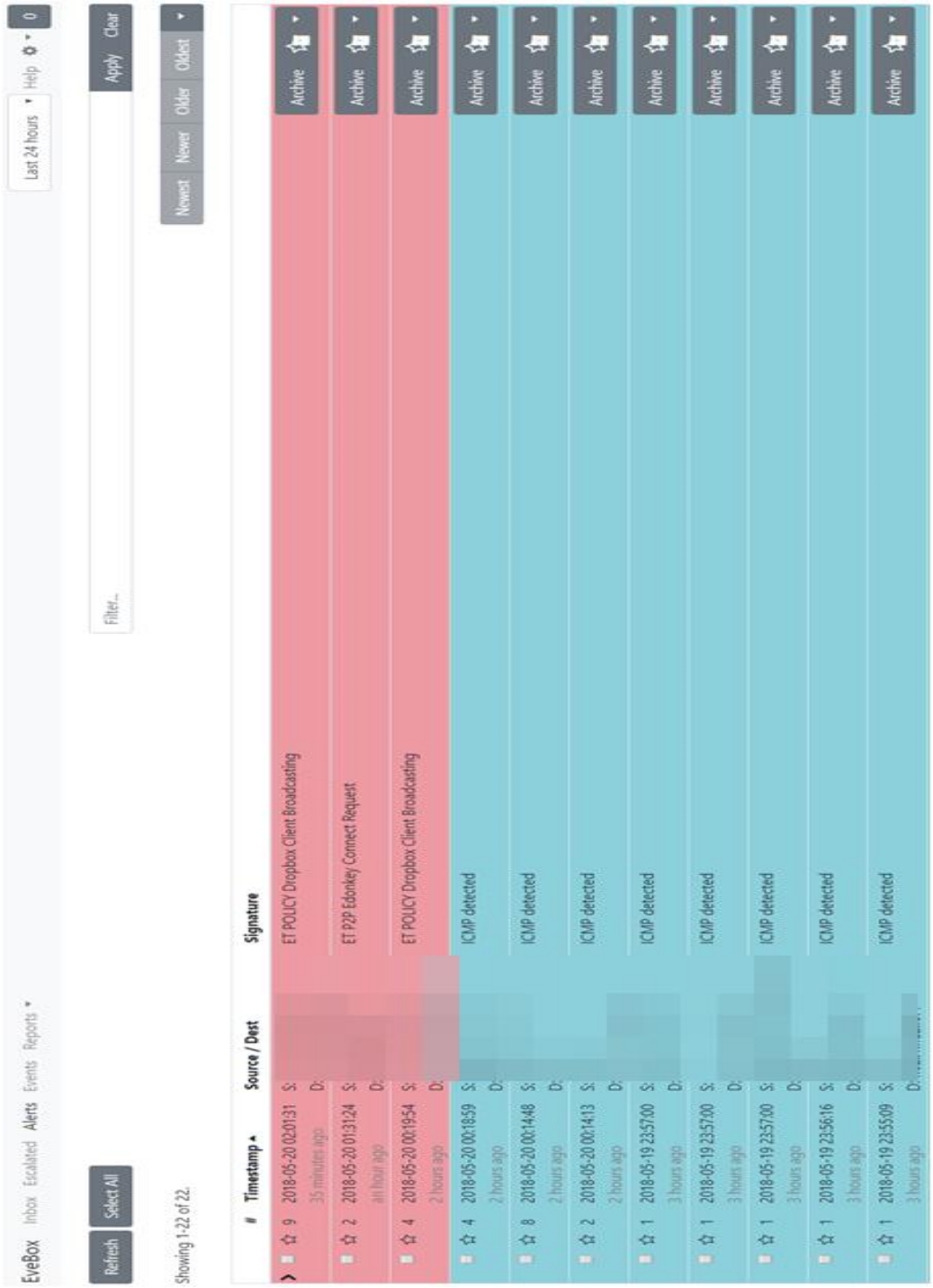

Figura 51. Panel de Alertas Evebox

5.3 Suricata como IPS

Para la validación del sistema de prevención de intrusiones se ha realizado la creación de una regla de incidencias la cual bloquea el acceso a una nube privada Figura 52.

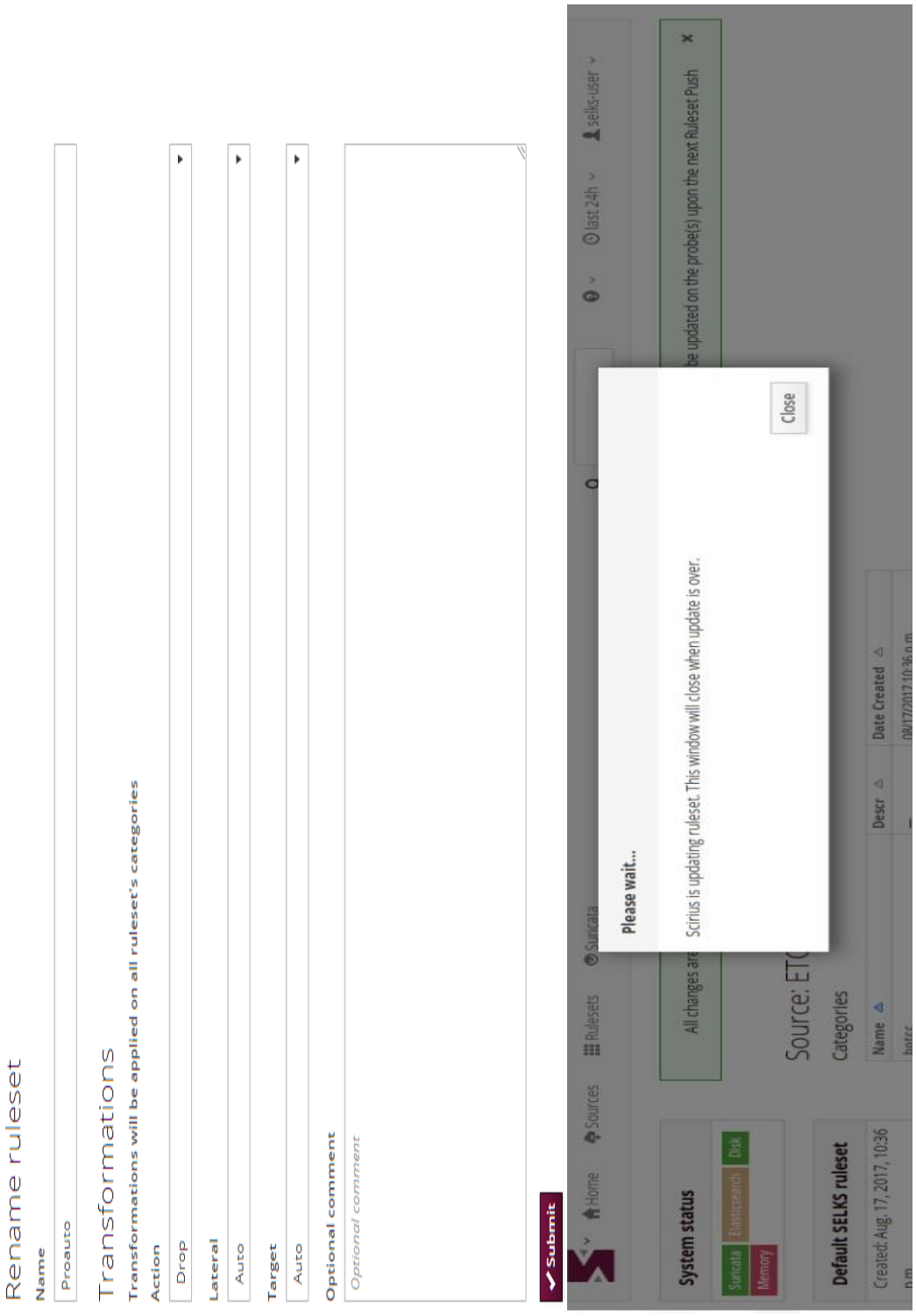

Figura 52. Activación módulo IPS

5.3.2 Fuente de Regla a modificar.

Para que el módulo de IPS pueda bloquear el tráfico no deseado primero se identifica la regla y posteriormente se cambia al estado de DROP como se evidencia en la Figura 53

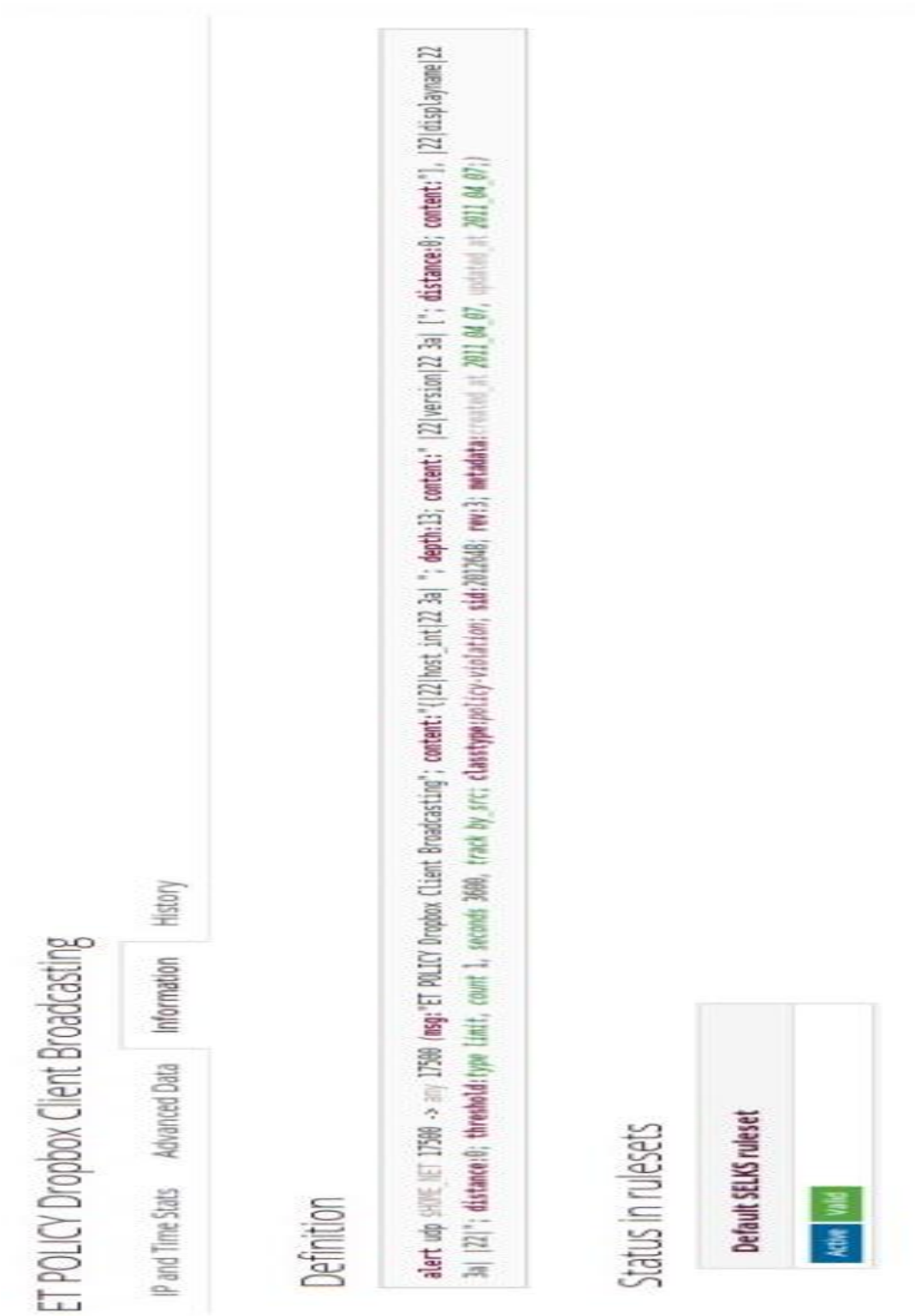

Figura 53 Verificación Fuente IPS.

5.3.1 Actualización de Fuente Suricata

Como parte del proceso de prevención de intrusiones se realiza la modificación de la regla en el módulo de SURICATA siendo en esencial la acción RULESET ACTION UPDATE. Figura 54.

Figura 54. Actualización Fuente IPS

5.3.2 Bloqueo de Acceso

Una vez aplicada la regla se realiza un intento de conexión desde el host de prueba, luego de lo cual se evidencia el bloqueo de acceso al servicio de la nube privada. Figura 55.

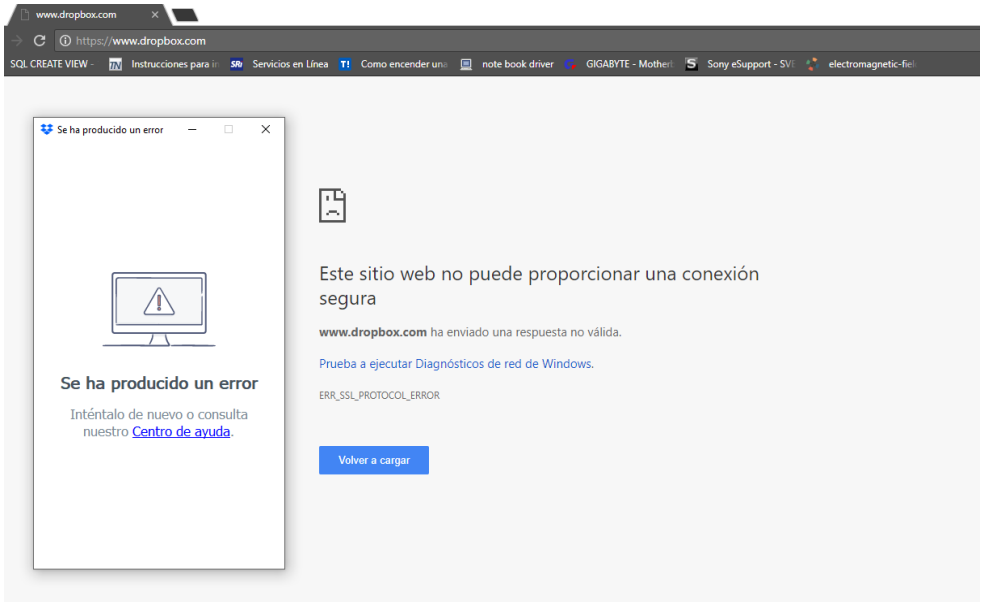

Figura 55. Bloqueo de acceso a servicio web

6. Conclusiones y Recomendaciones

6.1 Conclusiones

El sistema de Detección y Prevención de intrusiones permite garantizar la confidencialidad e integridad de la información de la empresa PROAUTO C.A.

La solución implementada se fundamenta en la norma ISO 27001 permitiendo evaluar los riesgos y tomar las acciones para la prevención y control de ataques a la información y a los sistemas que lo procesan en la empresa PROAUTO C.A.

La solución planteada presenta varias características importantes derivadas de su estructura de software libre. Entre las principales se tiene: Bajo costo, flexibilidad para adaptarse y mejorar de acuerdo a las necesidades de la empresa, independencia con respecto a determinados proveedores o marcas, etc.

Como resultado de la implementación del sistema propuesto se evidenció el uso de aplicaciones no autorizadas en diversos hosts dentro de la empresa logrando detectar una vulnerabilidad de posible fuga de información a través del uso no autorizado de nubes privadas a pesar de los controles de webfiltering que mantiene su seguridad perimetral.

Se consiguió un monitoreo constante de la red, permitiendo al administrador de la red tomar decisiones ante eventos y uso de aplicaciones no autorizadas.

Las pruebas realizadas utilizando el sistema propuesto, permitieron evidenciar su correcto funcionamiento tanto en hardware como en software y a la vez recibir una retroalimentación para mejorar y optimizar su funcionamiento.

Mediante el reporte del módulo de IDS se pudo obtener resultados de conexiones origen destino tanto en conteo de intentos de conexión como la cronología de estos.

Por medio de la creación de reglas aplicables en el módulo IPS se obtuvo el bloqueo a aplicaciones y sitios no autorizados luego de ser detectados por la funcionalidad IDS del sistema implementado.

Mediante la integración de SELKS el cual permite la interacción de suricata, kibana, logstash, evebox, sicirus y elasticsearch se pudo obtener una estadística de las horas con mayor incidencia de vulnerabilidades de acuerdo a las políticas de seguridad implementadas, así como también el índice de gravedad de la incidencia según el nivel de riesgo parametrizado en el algoritmo.

La solución planteada permite tener indicadores en tiempo real con entornos gráficos y cumpliendo con los requerimientos y necesidades de la empresa.

Esta solución constituye una herramienta de seguridad de la información para registrar las incidencias o eventos que se produzcan en la red.

6.2 Recomendaciones

El sistema debe estar en constante evolución y de acuerdo a los eventos con mayor número de incidencias se debe analizar el patrón de comportamiento para de esta manera crear nuevas reglas que permitan mitigar el uso de servicios no autorizados.

Crear políticas de seguridad informática para la empresa basadas en los lineamientos que deben seguir los hosts, aplicativos y servidores de acuerdo a la norma ISO 27001.

En base a la información obtenida del sistema se sugiere realizar revisiones periódicas y afinamientos en la seguridad perimetral ya que esta solución no remplaza las funciones o características que tiene un Firewall.

Con el fin de precautelar la disponibilidad de toda la infraestructura de la empresa es necesario implementar un *datacenter* alterno el cual permita mantener sistemas distribuidos ante un eventual fallo humano o desastre natural.

Se requiere fomentar mecanismos de educación, socialización y capacitación a todo el personal de la empresa referente a los procesos que contribuyan al uso, manejo adecuado y seguro de las herramientas tecnológicas e información de la misma.

Referencias

ACISSI. (2015). Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa (Tercera ed.). Barcelona: Epsilon.

Aguilera, P. (2010). Seguridad informática. Madrid: Editex S.A.

Aguirre, J. R. (2006). deic. Recuperado el 03 de Abril de 2018, de deic: http://deic.uab.es/material/26118-05GestionSeg.pdf

Alegre Ramos, M. D., & García Cervigón Hurtado, A. (2011). SEGURIDAD INFORMATICA (Primera ed.). Madrid: Paraninfo, SA.

Alejandro. (2017). Proteger Mi PC. Recuperado el 01 de abril de 2018, de Proteger Mi PC: https://protegermipc.net/2017/02/22/mejores-ids-opensource-deteccion-de-intrusiones/

Balanji, N. (2017). *GbHackers on Security*. Recuperado el 28 de marzo de 2018, de *GbHackers on Security*: https://gbhackers.com/intrusion-detection-system-ids-2/

Carpentier, J. F. (2016). La seguridad informática en la PYME: Situación actual y mejores prácticas (Vol. I). Barcelona, España: ENI.

Chicada, E. T. (2014). Gestión de incidentes de seguridad informática (Primera ed.). Málaga: IC Editorial.

Commons, C. (2018). CCM Enciclopedia. Recuperado el 29 de marzo de 2018, de CCM Enciclopedia: https://es.ccm.net/contents/162-sistema-de-deteccion-de-intrusiones-ids

CSCAZORLA. (2011). Xataka. Recuperado el 13 de Abril de 2018, de Xataka: https://www.xatakaciencia.com/robotica/hrp-4c-miim-el-robot-con-apariencia-humana

Culturación. (s.f.). Culturación. Recuperado el 03 de abril de 2018, de Culturación: http://culturacion.com/que-es-la-inteligencia-artificial/

Elastic. (s.f.). *Elastic Products*. Recuperado el 07 de 05 de 2018, de *Elastic Products*: https://www.elastic.co/products

Gonçalves, A. B. (2012). Máquinas que piensan como humanos. EL OBSERVADOR.

Honda. (2011). *World Honda*. Recuperado el 14 de Abril de 2018, de *World Honda*: http://world.honda.com/ASIMO/technology/2011

Huerta, M., & Libano, C. (1996). Delitos Informáticos. Santiago, Chile: Editorial Jurídica ConoSur.

Internet Society. (2014). *Internet Society* Capitulo República Dominicana. Recuperado el 01 de abril de 2018, de *Internet Society* Capitulo República Dominicana: https://isoc-rd.org.do/publicaciones/iana/

ISO. (2005). *Information technology — Security techniques — Information security management systems — Requirements* (Vol. I). Geneva, Switzerland : ISO copyright office.

Joan. (2013). *geekland*. Recuperado el 31 de marzo de 2018, de *geekland*: https://geekland.eu/que-es-y-para-que-sirve-un-firewall/

Kasperskylab. (2013). *Kasperskylab*. Recuperado el 3 de Abril de 2018, de *Kasperskylab*: https://www.kaspersky.es/blog/que-es-una-apt/966/

Kiguolis, L. (2016). LOSVIRUS. Recuperado el 02 de abril de 2018, de LOSVIRUS: https://losvirus.es/sniffers/

Krenn, P. (2017). *Software Engineering Daily*. Recuperado el 05 de 05 de 2018, de *Software Engineering Daily:* https://softwareengineeringdaily.com/2017/04/12/elasticsearch-with-philipp-krenn/

Lab, K. (2012). *Kaspersky Lab Daily*. Recuperado el 13 de Mayo de 2018, de https://www.kaspersky.es/blog/como-evadir-la-reputacion-de-las-direcciones-ips/272/

López, P. A. (2010). Seguridad Informática (Vol. I). Madrid: Editex S.A.

Mitra, A. (2015). *Computer Security and PGP*. Recuperado el 28 de marzo de 2018, de *Computer Security and PGP*: https://computersecuritypgp.blogspot.com/2015/09/what-is-intrusion-detection-system.html

MO, M. (2012). Con Ciencia y Conocimiento Libre. Recuperado el 31 de marzo de 2018, de Con Ciencia y Conocimiento Libre: http://cocolibre.blogspot.com/2012/10/clasificacion-de-puertos-de-red.html

Pattel, P. (2016). *Open source*. Recuperado el 31 de marzo de 2018, de *Open Source*: http://opensourceforu.com/2016/07/implementing-a-software-defined-network-sdn-based-firewall/

Pérez Porto, J., & Gardey, A. (2014). *Definicion.DE*. Recuperado el 02 de abril de 2018, de Definicion.DE: https://definicion.de

Policía Nacional. (2017). *Policía Nacional Escala Básica* (Vol. III). Madrid: CEP Editorial.

PROAUTO C.A. (2013). Valores. Quito, Pichincha, Ecuador.

PROAUTO C.A. (s.f.). PROAUTO C.A. Recuperado el 6 de Abril de 2018, de PROAUTO C.A Nosotros: https://proautochevrolet.com.ec/sobre-nosotros

Suricata. (2016). *Suricata/Docs*. Recuperado el 12 de mayo de 2018, de Suricata/Docs: http://suricata.readthedocs.io/en/suricata-4.0.4/

Suricata. (s.f.). *Open Source IDS / IPS / NSM engine*. Recuperado el 28 de marzo de 2018, de *Open Source IDS / IPS / NSM engine*: https://suricata-ids.org/

UNNE. (2006). Facultad de Ingenieria de la Universidad Nacional del Nordeste. Recuperado el 01 de abril de 2018, de Facultad de Ingenieria de la Universidad Nacional del Nordeste: http://ing.unne.edu.ar/pub/informatica/Alg_diag.pdf

Untiveros, S. (2004). AprendaRedes.com. Recuperado el 29 de marzo de 2018, de AprendaRedes.com: http://www.aprendaredes.com/dev/articulos/aprende-a-mirar-dentro-de-la-red-con-un-sniffer.htm

Urbina, G. B. (2016). Introducción a la seguridad informática (Primera ed.). México: Patria.

wikipedia. (2014). *wikipedia*. Recuperado el 03 de Abril de 2018, de wikipedia: https://es.wikipedia.org/wiki/Honeypot

Zuñiga, V. (2011). guiascursos. Recuperado el 31 de marzo de 2018, de guiascursos: https://guiascursos.files.wordpress.com/2011/10/puertos.pdf

ANEXOS

Anexo A

Tabla 1 Listado de Puertos con mayor uso.

Puerto/protocolo	Servicio / Descripción
n/d / GRE	GRE (protocolo IP 47) Enrutamiento y acceso remoto
n/d / ESP	IPSec ESP (protocolo IP 50) Enrutamiento y acceso remoto
n/d / AH	IPSec AH (protocolo IP 51) Enrutamiento y acceso remoto
1/tcp	Multiplexor TCP
7/tcp	Protocolo Echo (Eco) Responde con eco a llamadas remotas
7/udp	Protocolo Echo (Eco) Responde con eco a llamadas remotas
9/tcp	Protocolo Discard Elimina cualquier dato que recibe
9/udp	Protocolo Discard Elimina cualquier dato que recibe
13/tcp	Protocolo Daytime Fecha y hora actuales
17/tcp	Quote of the Day (Cita del Día)
19/tcp	Protocolo Chargen Generador de caracteres
19/udp	Protocolo Chargen Generador de caracteres
20/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - datos
21/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros) - control
22/tcp	SSH, scp, SFTP
23/tcp	Telnet manejo remoto de equipo, inseguro
25/tcp	SMTP Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)
37/tcp	time (comando)
43/tcp	nicname
53/tcp	DNS Domain Name System (Sistema de Nombres de Dominio)
53/udp	DNS Domain Name System (Sistema de Nombres de Dominio)
67/udp	BOOTP BootStrap Protocol (Server), también usado por DHCP

68/udp	BOOTP BootStrap Protocol (Client), también usado por DHCP
69/udp	TFTP Trivial File Transfer Protocol (Protocolo Trivial de Transferencia de Ficheros)
70/tcp	Gopher
79/tcp	Finger
80/tcp	HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (WWW)
88/tcp	Kerberos Agente de autenticación
110/tcp	POP3 Post Office Protocol (E-mail)
111/tcp	sunrpc
113/tcp	ident (auth) antiguo sistema de identificación
119/tcp	NNTP usado en los grupos de noticias de usenet
123/udp	NTP Protocolo de sincronización de tiempo
123/tcp	NTP Protocolo de sincronización de tiempo
135/tcp	epmap
137/tcp	NetBIOS Servicio de nombres
137/udp	NetBIOS Servicio de nombres
138/tcp	NetBIOS Servicio de envío de datagramas
138/udp	NetBIOS Servicio de envío de datagramas
139/tcp	NetBIOS Servicio de sesiones
139/udp	NetBIOS Servicio de sesiones
143/tcp	IMAP4 Internet Message Access Protocol (E-mail)
161/tcp	SNMP Simple Network Management Protocol
161/udp	SNMP Simple Network Management Protocol
162/tcp	SNMP-trap
162/udp	SNMP-trap
177/tcp	XDMCP Protocolo de gestión de displays en X11
177/udp	XDMCP Protocolo de gestión de displays en X11

389/tcp	LDAP Protocolo de acceso ligero a Bases de Datos
389/udp	LDAP Protocolo de acceso ligero a Bases de Datos
443/tcp	HTTPS/SSL usado para la transferencia segura de páginas web
445/tcp	Microsoft-DS (Active Directory, compartición en Windows, gusano Sasser, Agobot)
445/udp	Microsoft-DS compartición de ficheros
500/udp	IPSec ISAKMP, Autoridad de Seguridad Local
512/tcp	exec
513/tcp	login
514/udp	syslog usado para logs del sistema
520/udp	RIP
591/tcp	FileMaker 6.0 (alternativa para HTTP, ver puerto 80)
631/tcp	CUPS sistema de impresión de Unix
666/tcp	identificación de Doom para jugar sobre TCP
993/tcp	IMAP4 sobre SSL (E-mail)
995/tcp	POP3 sobre SSL (E-mail)
1080/tcp	SOCKS Proxy
1337/tcp	suele usarse en máquinas comprometidas o infectadas
1352/tcp	IBM Lotus Notes/Domino RCP
1433/tcp	Microsoft-SQL-Server
1434/tcp	Microsoft-SQL-Monitor
1434/udp	Microsoft-SQL-Monitor
1494/tcp	Citrix MetaFrame Cliente ICA
1512/tcp	WINS
1521/tcp	Oracle listener por defecto
1701/udp	Enrutamiento y Acceso Remoto para VPN con L2TP.
1720/udp	H323.
1723/tcp	Enrutamiento y Acceso Remoto para VPN con PPTP.

1761/tcp	Novell Zenworks Remote Control utility
1863/tcp	MSN Messenger
1935/???	FMS Flash Media Server
2049/tcp	NFS Archivos del sistema de red
2082/tcp	CPanel puerto por defecto
2086/tcp	Web Host Manager puerto por defecto
2427/udp	Cisco MGCP
3030/tcp	NetPanzer
3030/udp	NetPanzer
3074/tcp	Xbox Live
3074/udp	Xbox Live
3128/tcp	HTTP usado por web caches y por defecto en Squid cache
3128/tcp	NDL-AAS
3306/tcp	MySQL sistema de gestión de bases de datos
3389/tcp	RDP (Remote Desktop Protocol) Terminal Server
3396/tcp	Novell agente de impresión NDPS
3690/tcp	Subversion (sistema de control de versiones)
4662/tcp	eMule (aplicación de compartición de ficheros)
4672/udp	eMule (aplicación de compartición de ficheros)
4899/tcp	RAdmin (Remote Administrator), herramienta de administración remota (normalmente troyanos)
5000/tcp	Universal plug-and-play
5060/udp	Session Initiation Protocol (SIP)
5190/tcp	AOL y AOL Instant Messenger
5222/tcp	Jabber/XMPP conexión de cliente
5223/tcp	Jabber/XMPP puerto por defecto para conexiones de cliente SSL
5269/tcp	Jabber/XMPP conexión de servidor
5432/tcp	PostgreSQL sistema de gestión de bases de datos

5517/tcp	Setiqueue proyecto SETI@Home
5631/tcp	PC-Anywhere protocolo de escritorio remoto
5632/udp	PC-Anywhere protocolo de escritorio remoto
5400/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5500/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5600/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5700/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5800/tcp	VNC protocolo de escritorio remoto (usado sobre HTTP)
5900/tcp	VNC protocolo de escritorio remoto (conexión normal)
6000/tcp	X11 usado para X-windows
6112/udp	Blizzard
6129/tcp	Dameware Software conexión remota
6346/tcp	Gnutella compartición de ficheros (Limewire, etc.)
6347/udp	Gnutella
6348/udp	Gnutella
6349/udp	Gnutella
6350/udp	Gnutella
6355/udp	Gnutella
6667/tcp	IRC IRCU Internet Relay Chat
6881/tcp	BitTorrent puerto por defecto
6969/tcp	BitTorrent puerto de tracker
7100/tcp	Servidor de Fuentes X11
7100/udp	Servidor de Fuentes X11
8000/tcp	iRDMI por lo general, usado erróneamente en sustitución de 8080. También utilizado en el servidor streaming Shoutcast
8080/tcp	HTTP HTTP-ALT ver puerto 80. Tomcat lo usa como puerto por defecto.
8118/tcp	privoxy
9009/tcp	Pichat peer-to-peer chat server

9898/tcp	Gusano Dabber (troyano/virus)
10000/tcp	Webmin (Administración remota web)
19226/tcp	Panda SecurityPuerto de comunicaciones de Panda Agent.
12345/tcp	NetBus en:NetBus (troyano/virus)
31337/tcp	Back Orifice herramienta de administración remota (por lo caballos de troya)

Tomado de (Zuñiga, s.f)

Nota: En la tabla se muestra en la columna izquierda el número de puerto y que protocolo utiliza y en la derecha está su descripción.

Anexo B

Log de Instalación

```
 [root@localhost suricata-4.0.0]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.66.128  netmask 255.255.255.0  broadcast 192.168.66.255
        inet6 fe80::8e23:a3c:3ba7:9e56  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:43:9a:b1  txqueuelen 1000  (Ethernet)
        RX packets 51779  bytes 70619069 (67.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18210  bytes 1600228 (1.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost suricata-4.0.0]# ip add
```

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid_lft forever preferred_lft forever

inet6 ::1/128 scope host

valid_lft forever preferred_lft forever

2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP q

link/ether 00:0c:29:43:9a:b1 brd ff:ff:ff:ff:ff:ff

inet 192.168.66.128/24 brd 192.168.66.255 scope global dynamic ens33

valid_lft 1714sec preferred_lft 1714sec

inet6 fe80::8e23:a3c:3ba7:9e56/64 scope link

valid_lft forever preferred_lft forever

[root@localhost suricata-4.0.0]# /usr/bin/suricata -c /etc/suricata//suricata.ya

/usr/bin/suricata: error while loading shared libraries: libhtp.so.2: cannot ope

[root@localhost suricata-4.0.0]# nano /etc/suricata/suricata.yaml

-bash: nano: no se encontró la orden

[root@localhost suricata-4.0.0]# vi /etc/suricata/suricata.yaml

[root@localhost suricata-4.0.0]# tail -f /var/log/suricata/fast.log

tail: no se puede abrir «/var/log/suricata/fast.log» para lectura: No existe el

tail: no queda ningún fichero

```
[root@localhost suricata-4.0.0]# /usr/bin/suricata -c /etc/suricata//suricata.ya
/usr/bin/suricata: error while loading shared libraries: libhtp.so.2: cannot ope
[root@localhost suricata-4.0.0]# /usr/bin/suricata -c /etc/suricata//suricata.ya
/usr/bin/suricata: error while loading shared libraries: libhtp.so.2: cannot ope
[root@localhost suricata-4.0.0]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.66.128  netmask 255.255.255.0  broadcast 192.168.66.255
        inet6 fe80::8e23:a3c:3ba7:9e56  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:43:9a:b1  txqueuelen 1000  (Ethernet)
        RX packets 52321  bytes 70677321 (67.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18670  bytes 1677763 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
[root@localhost suricata-4.0.0]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.66.128  netmask 255.255.255.0  broadcast 192.168.66.255
        inet6 fe80::8e23:a3c:3ba7:9e56  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:43:9a:b1  txqueuelen 1000  (Ethernet)
        RX packets 52325  bytes 70677677 (67.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18673  bytes 1679077 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost suricata-4.0.0]# /usr/bin/suricata -c /etc/suricata//suricata.ya
/usr/bin/suricata: error while loading shared libraries: libhtp.so.2: cannot ope
```

[root@localhost suricata-4.0.0]# echo "/ usr / local / lib" >> /etc/ld.so.conf

[root@localhost suricata-4.0.0]# ldconfig

[root@localhost suricata-4.0.0]# /usr/bin/suricata -c /etc/suricata//suricata.yaml -i ens33

30/9/2017 -- 19:45:35 - <Notice> - This is Suricata version 4.0.0 RELEASE

^C30/9/2017 -- 19:45:48 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.

30/9/2017 -- 19:45:48 - <Notice> - Signal Received. Stopping engine.

30/9/2017 -- 19:45:49 - <Notice> - Stats for 'ens33': pkts: 1, drop: 0 (0.00%), invalid chksum: 0

[root@localhost suricata-4.0.0]# /usr/bin/suricata -c /etc/suricata//suricata.yaml -i ens33

30/9/2017 -- 19:45:55 - <Notice> - This is Suricata version 4.0.0 RELEASE

30/9/2017 -- 19:46:08 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.

^C30/9/2017 -- 19:51:41 - <Notice> - Signal Received. Stopping engine.

30/9/2017 -- 19:51:41 - <Notice> - Stats for 'ens33': pkts: 5354, drop: 0 (0.00%), invalid chksum: 0

[root@localhost suricata-4.0.0]# /usr/bin/suricata -c /etc/suricata//suricata.yaml -i ens33 -D

30/9/2017 -- 19:51:50 - <Notice> - This is Suricata version 4.0.0 RELEASE

[root@localhost suricata-4.0.0]# /usr/bin/suricata -c /etc/suricata//suricata.yaml -i ens33 --init-errors-fatal

30/9/2017 -- 19:56:11 - <Notice> - This is Suricata version 4.0.0 RELEASE

30/9/2017 -- 19:56:25 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.

Anexo C

Estructura de Reglas.

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Parameter Problem undefined Code"; icode:>2; itype:12; classtype:misc-activity; sid:2100428; rev:8; metadata:created_at 2010_09_23, update$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Photuris Reserved"; icode:0; itype:40; classtype:misc-activity; sid:2100429; rev:7; metadata:created_at 2010_09_23, updated_at 2010_09_23;)

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Photuris Unknown Security Parameters Index"; icode:1; itype:40; classtype:misc-activity; sid:2100430; rev:7; metadata:created_at 2010_09_2$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Photuris Valid Security Parameters, But Authentication Failed"; icode:2; itype:40; classtype:misc-activity; sid:2100431; rev:7; metadata:c$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Photuris Valid Security Parameters, But Decryption Failed"; icode:3; itype:40; classtype:misc-activity; sid:2100432; rev:7; metadata:creat$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Photuris undefined code!"; icode:>3; itype:40; classtype:misc-activity; sid:2100433; rev:9; metadata:created_at 2010_09_23, updated_at 201$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Redirect undefined code"; icode:>3; itype:5; classtype:misc-activity; sid:2100438; rev:10; metadata:created_at 2010_09_23, updated_at 2010$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Reserved for Security Type 19 undefined code"; icode:>0; itype:19; classtype:misc-activity; sid:2100440; rev:8; metadata:created_at 2010_0$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Reserved for Security Type 19"; icode:0; itype:19; classtype:misc-activity; sid:2100439; rev:7; metadata:created_at 2010_09_23, updated_at$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP SKIP undefined code"; icode:>0; itype:39; classtype:misc-activity; sid:2100446; rev:8; metadata:created_at 2010_09_23, updated_at 2010_09_$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Source Quench undefined code"; icode:>0; itype:4; classtype:misc-activity; sid:2100448; rev:8; metadata:created_at 2010_09_23, updated_at $

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Timestamp Reply undefined code"; icode:>0; itype:14; classtype:misc-activity; sid:2100452; rev:8; metadata:created_at 2010_09_23, updated_$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Timestamp Request undefined code"; icode:>0; itype:13; classtype:misc-activity; sid:2100454; rev:8; metadata:created_at 2010_09_23, update$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP Traceroute undefined code"; icode:>0; itype:30; classtype:misc-activity; sid:2100457; rev:8; metadata:created_at 2010_09_23, updated_at 20$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP unassigned type 1 undefined code"; itype:1; classtype:misc-activity; sid:2100459; rev:8; metadata:created_at 2010_09_23, updated_at 2010_0$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP unassigned type 2 undefined code"; itype:2; classtype:misc-activity; sid:2100461; rev:8; metadata:created_at 2010_09_23, updated_at 2010_0$

#alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"GPL ICMP unassigned type 7 undefined code"; itype:7; classtype:misc-activity; sid:2100463; rev:8; metadata:created_at 2010_09_23, updated_at 2010_0$

#alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"GPL ICMP Information Reply undefined code"; icode:>0; itype:16; classtype:misc-activity; sid:2100416; rev:8; metadata:created_at 2010_09_23, update$

#alert icmp $HOME_NET any -> $EXTERNAL_NET any (msg:"GPL ICMP Time-To-Live Exceeded in Transit undefined code"; icode:>1; itype:11; classtype:misc-activity; sid:2100450; rev:9; metadata:created_at 201$

2100363 || GPL ICMP_INFO IRDP router advertisement || cve,1999-0875 || bugtraq,578 || arachnids,173

2100364 || GPL ICMP_INFO IRDP router selection || cve,1999-0875 || bugtraq,578 || arachnids,174

alert tls [108.160.162.0/24,108.160.165.0/24,108.160.166.0/24] 443 -> $HOME_NET any (msg:"ET POLICY Dropbox.com Offsite File Backup in Use"; flow:established,from_server; content:"|55 04 03|"; content:"|0d|*.dropbox.com"; distance:1; wi$

alert udp $HOME_NET 17500 -> any 17500 (msg:"ET POLICY Dropbox Client Broadcasting"; content:"{|22|host_int|22 3a| "; depth:13; content:" |22|version|22 3a| ["; distance:0; content:"], |22|displayname|22 3a| |22|"; distance:0; threshold$

2100365 || GPL ICMP PING undefined code

2100366 || GPL ICMP_INFO PING *NIX

2100368 || GPL ICMP_INFO PING BSDtype || arachnids,152

2100369 || GPL ICMP_INFO PING BayRS Router || arachnids,444 || arachnids,438

2100370 || GPL ICMP_INFO PING BeOS4.x || arachnids,151

2100371 || GPL ICMP_INFO PING Cisco Type.x || arachnids,153

2100372 || GPL SCAN PING Delphi-Piette Windows || arachnids,155

2100373 || GPL ICMP_INFO PING Flowpoint2200 or Network Management Software || arachnids,156

2100374 || GPL ICMP_INFO PING IP NetMonitor Macintosh || arachnids,157

2100375 || GPL ICMP_INFO PING LINUX/*BSD || arachnids,447

2100376 || GPL ICMP_INFO PING Microsoft Windows || arachnids,159

2100377 || GPL ICMP_INFO PING Network Toolbox 3 Windows || arachnids,161

2100378 || GPL ICMP_INFO PING Ping-O-MeterWindows || arachnids,164

2100379 || GPL ICMP_INFO PING Pinger Windows || arachnids,163

2100380 || GPL ICMP_INFO PING Seer Windows || arachnids,166

2100381 || GPL ICMP_INFO PING Sun Solaris || arachnids,448

2100382 || GPL ICMP_INFO PING Windows || arachnids,169

2100384 || GPL ICMP_INFO PING

2100385 || GPL ICMP_INFO traceroute || arachnids,118

2100386 || GPL ICMP_INFO Address Mask Reply

2100387 || GPL ICMP Address Mask Reply undefined code

2100388 || GPL ICMP_INFO Address Mask Request

2100389 || GPL ICMP Address Mask Request undefined code

2100390 || GPL ICMP_INFO Alternate Host Address

2100391 || GPL ICMP Alternate Host Address undefined code

2100392 || GPL ICMP Datagram Conversion Error

2100393 || GPL ICMP Datagram Conversion Error undefined code

2100394 || GPL ICMP_INFO Destination Unreachable Destination Host Unknown

2100395 || GPL ICMP_INFO Destination Unreachable Destination Network Unknown

2100396 || GPL ICMP_INFO Destination Unreachable Fragmentation Needed and DF bit was set

2100397 || GPL ICMP_INFO Destination Unreachable Host Precedence Violation

2100398 || GPL ICMP_INFO Destination Unreachable Host Unreachable for Type of Service

2100399 || GPL ICMP_INFO Destination Unreachable Host Unreachable

2100400 || GPL ICMP_INFO Destination Unreachable Network Unreachable for Type of Service

2100401 || GPL ICMP_INFO Destination Unreachable Network Unreachable

2100402 || GPL ICMP_INFO Destination Unreachable Port Unreachable

2100403 || GPL ICMP_INFO Destination Unreachable Precedence Cutoff in effect

2100404 || GPL ICMP_INFO Destination Unreachable Protocol Unreachable

2100405 || GPL ICMP_INFO Destination Unreachable Source Host Isolated

2100406 || GPL ICMP_INFO Destination Unreachable Source Route Failed

2100407 || GPL ICMP Destination Unreachable undefined code

2100408 || GPL ICMP_INFO Echo Reply

2100409 || GPL ICMP Echo Reply undefined code

2100410 || GPL ICMP_INFO Fragment Reassembly Time Exceeded

2100411 || GPL ICMP_INFO IPV6 I-Am-Here

2100412 || GPL ICMP IPV6 I-Am-Here undefined code

2100413 || GPL ICMP_INFO IPV6 Where-Are-You

2100414 || GPL ICMP IPV6 Where-Are-You undefined code

2100415 || GPL ICMP_INFO Information Reply

2100416 || GPL ICMP Information Reply undefined code

2100417 || GPL ICMP_INFO Information Request

2100418 || GPL ICMP Information Request undefined code

2100419 || GPL ICMP_INFO Mobile Host Redirect

2100420 || GPL ICMP Mobile Host Redirect undefined code

2100421 || GPL ICMP_INFO Mobile Registration Reply

2100422 || GPL ICMP Mobile Registration Reply undefined code

2100423 || GPL ICMP_INFO Mobile Registration Request

2100424 || GPL ICMP Mobile Registration Request undefined code

2100425 || GPL ICMP Parameter Problem Bad Length

2100426 || GPL ICMP Parameter Problem Missing a Required Option

2100427 || GPL ICMP Parameter Problem Unspecified Error

2100428 || GPL ICMP Parameter Problem undefined Code

2100429 || GPL ICMP Photuris Reserved

2100430 || GPL ICMP Photuris Unknown Security Parameters Index

2100431 || GPL ICMP Photuris Valid Security Parameters, But Authentication Failed

2100432 || GPL ICMP Photuris Valid Security Parameters, But Decryption Failed

2100433 || GPL ICMP Photuris undefined code!

2100436 || GPL ICMP_INFO Redirect for TOS and Host

2100437 || GPL ICMP_INFO Redirect for TOS and Network

2100438 || GPL ICMP Redirect undefined code

2100439 || GPL ICMP Reserved for Security Type 19

2100440 || GPL ICMP Reserved for Security Type 19 undefined code

2100441 || GPL ICMP_INFO Router Advertisement || arachnids,173

2100443 || GPL ICMP_INFO Router Selection || arachnids,174

2100445 || GPL ICMP_INFO SKIP

2100446 || GPL ICMP SKIP undefined code

2100448 || GPL ICMP Source Quench undefined code

2100449 || GPL MISC Time-To-Live Exceeded in Transit

2100450 || GPL ICMP Time-To-Live Exceeded in Transit undefined code

2100451 || GPL ICMP_INFO Timestamp Reply

2100452 || GPL ICMP Timestamp Reply undefined code

2100453 || GPL ICMP_INFO Timestamp Request

2100454 || GPL ICMP Timestamp Request undefined code

2100455 || GPL ICMP_INFO Traceroute ipopts || arachnids,238

2100456 || GPL ICMP_INFO Traceroute

2100457 || GPL ICMP Traceroute undefined code

2100458 || GPL ICMP_INFO unassigned type 1

2100459 || GPL ICMP unassigned type 1 undefined code

2100460 || GPL ICMP_INFO unassigned type 2

2100461 || GPL ICMP unassigned type 2 undefined code

2100462 || GPL ICMP_INFO unassigned type 7

2100463 || GPL ICMP unassigned type 7 undefined code

2100465 || GPL SCAN ISS Pinger || arachnids,158

2100466 || GPL ICMP L3retriever Ping || arachnids,311

2100467 || GPL SCAN Nemesis v1.1 Echo || arachnids,449

2100469 || GPL SCAN PING NMAP || arachnids,162

2100471 || GPL SCAN icmpenum v1.1.1 || arachnids,450

2100472 || GPL ICMP_INFO redirect host || cve,1999-0265 || arachnids,135

2100473 || GPL ICMP_INFO redirect net || cve,1999-0265 || arachnids,199

2100474 || GPL SCAN superscan echo

2100475 || GPL ICMP_INFO traceroute ipopts || arachnids,238

2100476 || GPL SCAN webtrends scanner || arachnids,307

2100477 || GPL ICMP_INFO Source Quench

2100478 || GPL SCAN Broadscan Smurf Scanner

2100480 || GPL ICMP_INFO PING speedera

2100481 || GPL ICMP_INFO TJPingPro1.1Build 2 Windows || arachnids,167

2100482 || GPL ICMP_INFO PING WhatsupGold Windows || arachnids,168

2100483 || GPL SCAN PING CyberKit 2.2 Windows || arachnids,154

2100484 || GPL SCAN PING Sniffer Pro/NetXRay network scan

2100485 || GPL ICMP_INFO Destination Unreachable Communication Administratively Prohibited

2100486 || GPL ICMP_INFO Destination Unreachable Communication with Destination Host is Administratively Prohibited

2100487 || GPL ICMP_INFO Destination Unreachable Communication with Destination Network is Administratively Prohibited

2012647 || ET POLICY Dropbox.com Offsite File Backup in Use || url,dereknewton.com/2011/04/dropbox-authentication-static-host-ids/ || url,www.dropbox.com

2012648 || ET POLICY Dropbox Client Broadcasting