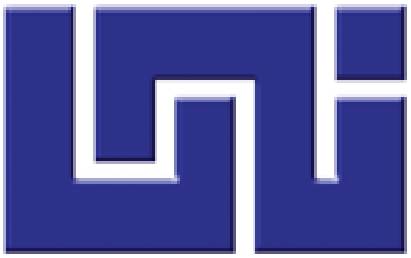
Universidad Nacional de Ingeniería

Facultad de Electrotecnia y Computación



Trabajo Monográfico:

Implementación de una herramienta de detección de intrusiones en la red de área local del Sistema Nacional de Inversión Pública (SNIP).

Presentado por:

Br. Karen Lisseth Sáenz Sánchez.

(2008-24040)

Br. Karen Aleyda Martínez Domínguez

(2008-24186)

Para optar por el título de:

Ingeniero en Computación.

Tutor:

Ing. Néstor Traña Obando.

Managua, Nicaragua

Diciembre, 2018.

Agradecimientos

Gracias a Dios, que nos otorgó la sabiduría necesaria para llevar a cabo este trabajo monográfico.

Gracias a nuestros padres, porque debido a ellos y a su apoyo incondicional a lo largo de nuestra carrera, logramos llegar hasta el final de la jornada.

Gracias a nuestros amigos, que siempre nos han prestado un gran apoyo moral y humano, necesarios en los momentos difíciles que transcurrimos para culminar este trabajo.

Y gracias a nuestro tutor, el especialista en Seguridad de la Información***, Néstor Traña Obando***, por su paciencia, comprensión y solidaridad con este proyecto, por el tiempo que nos ha concedido. Sin su apoyo este trabajo nunca se habría escrito y, por eso, este trabajo es también el suyo.

Contenido

Índice de Ilustraciones

Índice de Diagramas de Casos de Uso

Índice de Tablas

Índice de Tablas Casos de Uso

I. INTRODUCCIÓN

Nicaragua se cataloga como una región de Centroamérica que "*está muy tierna en temas de seguridad de la información*", según expresó John Molina en una entrevista realizada por El Nuevo Diario el 23 de enero del 2013.

En las redes de computadoras la tendencia al crecimiento de aplicaciones y servicios ha sido un factor importante en los últimos años para el desarrollo de herramientas necesarias para la seguridad de la información. La dependencia que existe en los usuarios hacia estas nuevas tecnologías (aplicaciones y servicios desarrollados con el fin de optimizar tiempo laboral, por ejemplo: servicios de notas en línea, compras online, etc.) se ha convertido en una necesidad de manera que, de la estabilidad y seguridad de esas aplicaciones y servicios, depende el giro de la institución.

Dichas redes, demandan medidas de protección más elaboradas para garantizar una segura operación y dar continuidad a los servicios críticos. Estas medidas exigen e incluyen métodos de detección y respuestas a los intentos de intrusión en tiempo real.

De manera general, las intranets adolecen de herramientas que faciliten la detección de ataques en tiempo real basados en el análisis del tráfico hacia uno de los puntos más vulnerables, como son los servidores. John Molina afirma "*que el punto más débil de la seguridad es el ser humano y normalmente el 80% de la inseguridad informática en las empresas empieza por el personal interno, el 20% es externo, o sea que tenemos que empezar a culturizar a la gente de la empresa sobre qué significa la seguridad de la información, llevar controles y evitar que suceda algo anómalo. Hay que enseñarle a la gente qué puede ser peligroso y qué no lo es*". Estos ataques o anomalías pueden ser causados por personas con mala intención que buscan robar información, denegar servicios, etcétera, haciendo uso de aplicaciones especializadas diseñadas para estos fines.

SNORT

Los avances tecnológicos están cada vez más instrumentados, interconectados e inteligentes; de ahí radica la existencia de nuevas posibilidades más complejas en el ámbito informático por lo que se debe estar preparado sobre seguridad informática.

En Nicaragua, hay instituciones como el Sistema Nacional de Inversión Pública (SNIP) que hacen uso de redes de área local para el desarrollo de sus funciones dentro y fuera de la institución. Siendo una institución perteneciente al Estado, no está exenta de ataques a la red y servicios (correo electrónico institucional, aula virtual, sitio web, entre otros), tal como les ha sucedido en ciertas ocasiones según el director del SNIP, en las que algunos de sus servicios han sido vulnerados.

Existe una gran variedad de estándares de protocolos que implementan en alguna medida seguridad en las intranets. Hay consideraciones de seguridad, como los que cita T. Socolofsky, C. Kale. (1991) en el “Tutorial de TCP/IP”, dentro del conjunto de protocolo de TCP/IP. Para muchas personas estas consideraciones son serios problemas, para otros no; depende de los requerimientos del usuario.

También se cuenta con numerosas herramientas y aplicaciones que brindan seguridad a los principales servicios ofrecidos por las empresas (correo electrónico, sitios web y servicios FTP), sin embargo, la seguridad por estos medios no es suficiente, en ocasiones se necesita un seguimiento detallado del tráfico en la red para la detección temprana de la propagación de ataques de intrusos hacia los puntos más sensibles de la red.

Es por esto que se han desarrollado herramientas o sistemas de detección de intrusos para solventar la falta de registros de ataques que se realizan a las redes de instituciones que no cuentan con seguridad de la información. Tomando en cuenta los ataques sufridos por el SNIP, se recomienda implementar una herramienta de Detector de Intrusos en su red de área local, para un mejor desempeño en sus servicios. Esto incluye un registro de ataques en tiempo real, control estadísticos de tráfico en la red, entre otras funciones.

SNORT

II. ANTECEDENTES

"*La información se ha convertido para toda empresa u organización en un activo de mucha importancia, a tal punto que el negocio en sí depende en gran parte de esta para poder subsistir.*

En el mundo actual, donde gran parte de la información es manejada por sistemas computarizados y de telecomunicaciones, es difícil poder afirmar que la información está 100% protegida. En base a eso, muchas de las empresas u organizaciones optan por utilizar mecanismos de protección adicionales, como un Intrusion Detection and Protection System (IDS/IPS), en sus infraestructuras de red. Estas empresas buscan cómo protegerse de las amenazas que existen en el internet." (El Nuevo Diario. (2014). Sistemas de Prevención de Intrusos de Nueva Generación. El Nuevo Diario.)

El Sistema Nacional de Inversión Pública (SNIP) de Nicaragua, surge con la visión de asegurar la calidad de las inversiones y su coherencia con las prioridades del desarrollo nacional, contribuyendo así al bienestar de todos los y las nicaragüenses. Cuenta con una red interna donde los usuarios hacen uso de servicios tales como: Correo Electrónico, Sitio Web, entre otros.

El SNIP en aras de fortalecer la seguridad de la información dentro de su entorno laboral ha implementado ciertas medidas de seguridad informática, lo que no ha tenido mucho efecto debido a que a pesar de esto han sufrido intrusiones a ciertos servicios con los que cuenta como institución (entre ello se destaca el ataque al servicio de Correo Electrónico), siendo estas intrusiones detectadas no en tiempo real, sino hasta que la intrusión es completada y observada en los servicios finales.

Con el fin de mitigar esta vulnerabilidad en la red, la institución decidió trabajar con una herramienta llamada Fortigate, (sistema de seguridad desarrollado por Fortinet, que se basa en software libre y funciona como detector de amenazas), intentando así llevar un registro de las posibles intrusiones detectables, sin embargo esta herramienta está implementada solo en la parte externa de la red dejando

SNORT

vulnerable la parte interna, agregando a esto el hecho de que la institución no es directamente quien está evaluando dichos registros generados por la aplicación ya que el riesgo es trasladado a un agente externo y en consideración esta herramienta no brinda la protección suficiente y requerida.

Otro aspecto importante que ha venido tomando en cuenta la institución, es la ralentización de la Intranet debido a posibles ataques informáticos y/o al uso de servicios Streaming (distribución digital de multimedia a través de una red de computadoras) que pueden estar provocando reducción del ancho de banda.

SNORT

III. JUSTIFICACIÓN

La seguridad de la información de las empresas es un tema que cada vez cobra mayor fuerza en el mundo de los negocios, ya que las empresas dependen mayoritariamente del flujo de información, si esta información se distorsiona (por intrusiones no autorizadas) puede afectar significativamente la reputación de la empresa, el giro o resultados del negocio.

En nuestro país, la seguridad informática es un tema que ha sido adoptado recientemente por las empresas, según publicación de La Prensa “hasta el 14 de octubre del año 2014, empezaba a generarse cierto nivel de preocupación en las pequeñas empresas e instituciones sobre la seguridad informática“, limitándose en la mayoría de los casos, a la protección de los equipos informáticos finales (End Point), haciendo uso de los Firewall o cortafuegos, antivirus y proxys, lo cual deja por fuera la infraestructura de red (router, switch, servidores, etcétera).

Existen personas mal intencionadas (tanto fuera, como dentro de las empresas) que intentan acceder de forma no autorizada a los datos sensibles de las empresas, dicho acceso no autorizado a una red informática, puede ocasionar en su mayoría problemas graves como perdida de información, suplantación de identidad, fraude, falsificaciones, etcétera; lo cual implica un delito informático según el documento “Delitos Informáticos del 2005, de la CORTE SUPREMA DE JUSTICIA NICARAGUA”.

El SNIP ha notado desde hace algún tiempo ralentización a la hora de navegar en el internet con el que trabajan, esto conlleva a dos posibles causas, primero que la red está sufriendo ataques internos o externos y segundo que el ancho de banda está siendo mal utilizado. Debido a esto la Institución SNIP requiere un mecanismo para detectar intrusiones en su red de área local. Por lo anterior descrito se propone la implementación de una herramienta de detección de intrusos que sirva como analizador de paquetes que provienen de agentes externos e internos, para lograr

detectar ataques a la entidad. Así mismo esta herramienta debe de registrar y llevar un control estadístico del tráfico en la red.

SNORT

IV. OBJETIVO GENERAL

Proporcionar a la Institución Sistema Nacional de Inversión Pública una herramienta administrativa de red en tiempo real, que facilite la detección de intrusiones mediante mecanismos de alertas y generación de ficheros de registros de incidencias.

V. OBJETIVOS ESPECÍFICOS

- Analizar la topología de red existente a fin de identificar la posición óptima dentro de la red, para la puesta en marcha de una herramienta de detección de intrusiones.

- Implementar una herramienta de detección de intrusiones sobre la topología de red física existente, que cumpla con los requerimientos de seguridad y reglas solicitadas por el SNIP.

- Desarrollar un caso de prueba a fin de verificar el cumplimiento de las funcionalidades y evaluar la efectividad de la herramienta de detección de intrusiones.

VI. MARCO TEÓRICO

La seguridad informática se enfoca en reducir el factor de riesgo al que se exponen los sistemas de información (sistemas de cómputo y de comunicación) que integran una red. Esta disciplina ha creado mecanismos de seguridad para mejorar las debilidades que se encuentran en la red, errores de diseño y errores de programación los cuales pueden ser aprovechados para acceder a la información confidencial de la empresa. Se debe tener en cuenta que un sistema de información se encuentra comprometido cuando presenta deficiencia física o de diseño en su estructura, exponiéndolo a un riesgo de ser dañado o vulnerado por una persona ajena al sistema.

SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS)

Los sistemas de detección de intrusos representan un mecanismo de defensa ante los intentos de intrusiones, sean estos desde el interior o exterior de una red. Se clasifican de acuerdo al modo de operación, técnica de análisis, tecnología de implementación, velocidad de respuesta y otras características. La importancia de los IDS se basa en prevenir que la información se vea comprometida, es decir, su función es la detección oportuna y temprana de las acciones ilegales o extrañas que indiquen una posible intrusión a una aplicación (software) o equipo de cómputo (hardware) en una red.

Los IDS están integrados por módulos que trabajan en forma conjunta y con funciones específicas recolectando y analizando datos de las actividades humanas o procesos que se efectúan en un sistema, genera alertas y según sea el caso acciona respuestas de tipo pasivos, activos o proactivos; citando a Alfon (2003) "*Los IDS pasivos son aquellos que notifican mediante alertas al administrador de la red pero no actúan y los IDS activos o proactivos generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en nuestra configuración*" (Sistemas de detección de

SNORT

Intrusos y SNORT. 2015, de Maestros del Web Sitio web: http://www.maestrosdelweb.com/snort/).

TIPOS DE IDS

Existen tres tipos de IDS:

1. HIDS (Host IDS)

Este actúa de forma local, es decir, sobre un único host con el objetivo principal de protegerlo, recopilando información de ficheros, recursos o logs, para posteriormente analizarlos y encontrar posibles hechos que atenten contra la información. Este tipo de IDS ofrece una gran ventaja y es que el procesamiento es mucho menor comparado con un NIDS.

2. NIDS (Net IDS)

Este tipo de IDS, actúa en una red de igual manera que HIDS capturando todo el tráfico de una red al igual como lo puede hacer un Sniffer (este es una herramienta, programa o un dispositivo de red que captura los paquetes que viajan por la red de datos), para luego analizar los paquetes capturados y así detectar primeras fases de posibles ataques a las redes. Por ejemplo, ataques de denegación de servicios, escanear puertos o intentos de entrar en un equipo de cómputo, analizando el tráfico de la red en tiempo real.

3. DIDS (Distributed IDS)

Parecido a un NIDS, pero los sensores están distribuidos en diferentes puntos de la red y envían las alertas a un sistema centralizado donde el operador podría analizarlas.

SNORT

ARQUITECTURA DE UN IDS

Aunque no es un estándar generado por alguna entidad certificadora, la arquitectura de IDS se compone de los siguientes parámetros:

1. Recolección de datos: A través de los logs de registro de los dispositivos de red se pueden recopilar datos.

2. Parámetros**:** Configuración de las reglas que determinan acciones particulares de amenazas o fallas de seguridad en la red.

3. Filtros**:** Comparan datos obtenidos en la parte de recolección de datos con los parámetros.

4. Detector de eventos**:** Función del IDS para alertar al administrador sobre actos inusuales en el tráfico de la red.

5. Dispositivo generador de alarmas**:** Según la configuración que el administrador le proporcione al IDS este está en capacidad de alertar mediante correo electrónico o vía SMS.

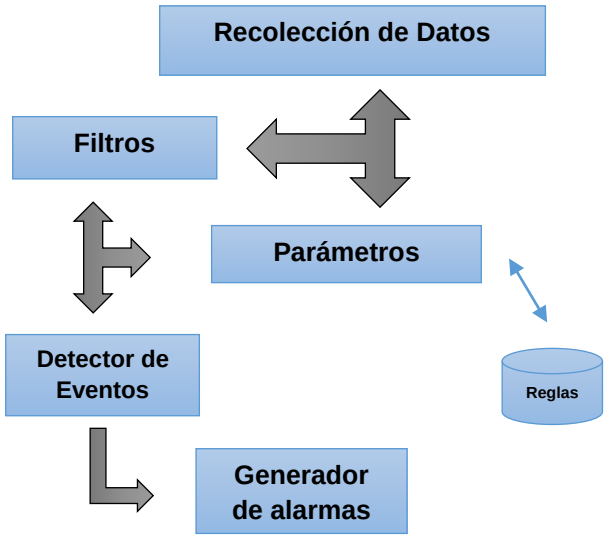


Ilustración 1 Arquitectura de un IDS.Fuente: creación propia.

FUNCIONAMIENTO DE IDS

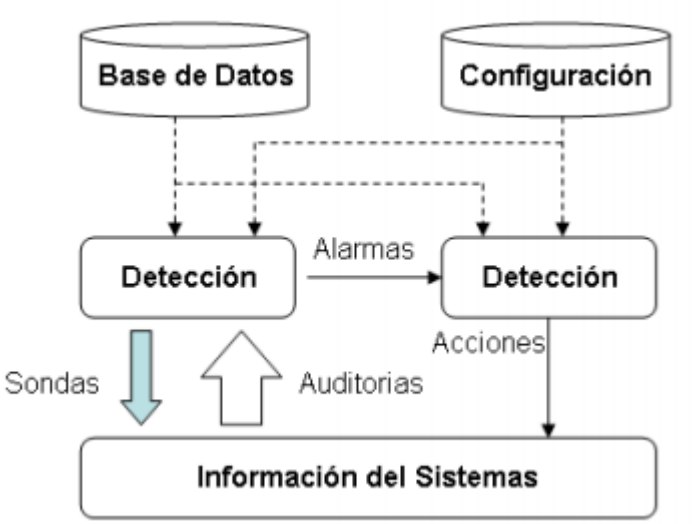


Ilustración 2 Funcionamiento de un IDS. Fuente: underc0de.org

El proceso de detección de intrusos, se lo define de la siguiente manera:

- ✓ Una base de datos con una recopilación de ataques anteriores.
- ✓ Un sistema actual debidamente configurado.
- ✓ Estado actual, referente en términos de comunicación y procesos.

SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS)

Este sistema fue desarrollado en 1990, fue diseñado para monitorear el tráfico de una red, en tiempo real y prevenir que se filtre cualquier actividad maliciosa conocida como intrusión en la misma, cuando se produce la caída de un paquete o éste pasa dañado o incompleto, en una transmisión de información, inmediatamente la red bloquea la transmisión por prevenir un posible ataque o deformaciones en la transferencia de datos, es considerado una mejora con respecto a los Firewalls, su diseño es una evolución de los IDS (Sistema de Detección de Intrusos).

A diferencia de los IDS esta nueva tecnología no se limita solo a escuchar el tráfico de la red y a mandar alertas en una consola, después de que ocurre una intrusión, el IPS funciona a nivel de la capa 7 tiene la capacidad de descifrar protocolos como

SNORT

HTTP, FTP y SMTP, algunos IPS permiten establecer reglas como se lo hace en los Firewalls.

La tecnología IPS ofrece una visión más profunda de las operaciones de la red proporcionando información sobre actividades maliciosas, malas conexiones, el contenido inapropiado de la red y muchas otras funciones de la capa de Aplicación, utiliza menos recursos que un IDS, siendo una solución ideal que contribuye a la seguridad de la información que se transmite por una red y disminución de costos, para una empresa que opta por adquirir sistemas o herramientas de este tipo para preservar los datos que posee.

El IPS no utiliza dirección IP como lo hace un firewall, ni funciona igual que uno. Permite poner normas y restringir acceso a usuarios, aplicaciones y a host, siempre y cuando se detecten que estos están teniendo actividades mal intencionadas o código malicioso en el tráfico de la red.

Ventajas

- Protección preventiva antes de que ocurra el ataque
- Defensa completa (Vulnerabilidades del Sistema Operativo, Puertos, Trafico de IP, códigos maliciosos e intrusos)
- Maximiza la seguridad y aumenta la eficiencia en la prevención de intrusiones o ataques a la red de una empresa.
- Fácil instalación, configuración y administración
- Es escalable y permite la actualización de dispositivos a medida que crece la empresa

No requiere tanta dedicación como un IDS tradicional; esto en consecuencia requeriría menos inversión en recursos para administrar y operar estos sistemas (en comparación con un IDS)

SNORT

TIPOS DE IPS

IPS basados en host (HIPS)

Esta aplicación de prevención de intrusiones reside en la dirección IP específica de un solo equipo, permite prevenir posibles ataques en los nodos débiles de una red es decir los host.

IPS basada en red (PIN)

Esta aplicación IPS es en hardware y cualquier acción tomada para prevenir una intrusión en una red específica de host (s) se hace de una máquina con otra dirección IP en la red (esto podría ser en un front-end de cortafuegos).

SNORT

Dentro del ámbito de seguridad informática existen gran cantidad de IDS que se podrían implementar al SNIP, por esto, se realizó un estudio de comparación entre los más destacados y reconocidos evaluando sus características y facilidad de implementación para dar a la institución una herramienta que cumpla con los requerimientos y de soluciones acorde a su problemática.

Tabla 1 Comparativa para determinar el IDS más factible para la implementación al SNIP.

Características	**Endian Snort**	**Security Onion**	**Tripwire Opensource**	**BroIDS**
Desarrollado bajo Open source.	✓	✓	✓	✓
Análisis de tráfico en tiempo real.	✓	X	✓	
Logueo del tráfico malicioso en archivos o bases de datos.	✓	✓	✓	✓
Fácil de administrar.	✓	X	X	X
Su compatibilidad es únicamente con Linux.	*X	X	✓	X
Analizador de tráfico de red pasivo.	✓	X	X	✓
Licencia Gratuita.	✓	✓	X	✓
Gráficos detallados de las interfaces de red.	✓	X	X	✓
Antivirus y filtrado de contenido. Antivirus y Anti spam para el correo electrónico.	✓	X	X	X
Manejo de redes inalámbricas seguras.	✓	X	X	X
Enrutamiento.	✓	X	X	X
Alta Disponibilidad.	✓	X	X	X

SNORT

Manejo de Proxy.	✓	X	X	X
Establecimiento de reglas Firewall de entrada y salida.	✓	X	X	X

*no está desarrollado únicamente para Linux, tiene disponibilidad de ser utilizado en cualquier sistema Operativo.

Con esta tabla comparativa se determina que la herramienta a utilizar para el desarrollo de este trabajo monográfico según las características requeridas es ***ENDIAN SNORT***, debido a que cumple con las expectativas de solución a la situación de la institución.

Ilustración 3 Logo de Snort. Herramienta que se utilizará para la ejecución de este modelo monográfico.

SNORT

ENDIAN

Un firewall basado en una distribución de Linux llamada Endian, el cual se muestra la oportunidad no solo de montar un firewall sino también de implementar otros servicios como por ejemplo proxy, vpns, entre otros.

Además si se tiene una estructura de red con DMZ (zona desmilitarizada) brinda la posibilidad de hacerlo más sencillo, asimismo de poder administrarlo por vía Web dando más facilidad en el momento de implementar las reglas o políticas en el firewall.

La mayoría de los administradores, están en constante movimiento, por lo general no están en contacto directo con la maquina a administrar, lo que requieren herramientas que le brinden la posibilidad de administración remota por vía Web, ssh, telnet.

Endian cumple este requisito, permitiendo desde cualquier máquina de nuestra red acceder remotamente vía Web y administrar nuestro firewall, ahorrando que se desplace hacia la propia maquina física.

La expectativa que se pretende lograr implementando este firewall es tener más conocimiento de herramientas OpenSource, que no solo existe iptables, sino que hay muchas herramientas que pueden ser más sencillas de configurar y administrar tanto por vía Web como por la Shell del sistema.

La implementación de esta herramienta es totalmente gratuita, ya que es una distribución GNU/LINUX, se descarga una ISO () desde el sitio web oficial (www.endian.com), no requiere mucha capacidad física en la maquina donde se implementa. Endian es un firewall con nivel de aplicación.

HMailServer

HMailServer es un servidor de correo electrónico de Microsoft Windows. Permite manejar todo el correo electrónico sin tener que depender de un proveedor de

SNORT

servicios de Internet. Así mismo es una herramienta gratuita y de código abierto, muy fácil de instalar y configurar. HMailServer añade flexibilidad y seguridad y da control total sobre la protección contra el spam.

Características

- Soporta los protocolos POP3, SMTP e IMAP.
- Admite dominios virtuales.
- Integra copias de seguridad.
- Incluye cifrado SSL
- Integra filtros anti-spam y anti-virus.
- Permite la creación de scripts.
- Admite las reglas del servidor.
- Es multilingüe, incluyendo el idioma español.
- Soporta el enrutamiento de paquetes.
- Admite la copia de seguridad MX.
- Soporta la administración web.

Webmail

Es una aplicación que permite leer/enviar correo directamente desde el servidor, desde cualquier ordenador conectado a Internet. Cabe mencionar que está trabajando directamente en el servidor y, por defecto, los correos leídos no son borrados, por lo que de nuevo la PC los bajará y los volverá a leer a no ser que los borre).

SNORT

Ventajas de Webmail

- Los mensajes pueden leerse, escribirse y enviarse desde cualquier lugar con un explorador y conexión a Internet.
- Los mensajes no tienen que descargarse al ordenador.
- Las cuentas de correo pueden crearse fácilmente, lo que permite crear cuentas para uso anónimo fácilmente.

Joomla

Es un sistema de gestión de contenidos (o CMS, por las siglas en inglés, Content Management System) que permite desarrollar sitios web dinámicos e interactivos. Permite crear, modificar o eliminar contenido de un sitio web de manera sencilla a través de un "panel de administración". Además es uno de los más populares paquetes de software usado para crear, organizar, administrar y publicar contenido para sitios web, blogs, intranets y aplicaciones móviles.

Moodle

(Modular Object Oriented Dynamic Learning Environment -Entorno de Aprendizaje Modular Orientado a Objetos-) es una plataforma virtual de aprendizaje dentro de los sistemas de gestión de procesos de enseñanza – aprendizaje a través de la creación de cursos en línea, pues permite el levantamiento de un centro capaz de gestionar distintos cursos a la vez a través de la red, que se caracteriza por poseer una estructura modular y estar construida bajo la concepción constructivista de aprendizaje.

SNORT

Snort es un sistema para la prevención y detección de intrusiones en la red (IDS / IPS) desarrollado por Sourcere. Es una herramienta de seguridad muy utilizada en Linux, con la cual podemos asegurar nuestro equipo o nuestra red. Ofrece muchas posibilidades, un ejemplo es la detección de escaneo de puertos.

Nos ofrece de forma muy clara las ips que han intentado escanear nuestro equipo, así como la hora del escaneo y detalles sobre los paquetes empleados. Brinda varias opciones para la *prevención y detección de intrusos*. Los tres modos principales para la prevención de intrusiones son el filtrado integrado, la cooperación con un cortafuegos existente basado en iptables y el modo TCP-RST.

Snort como IDS o Sistema de detección de intrusiones basado en la red (NIDS), implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos de aprovechar alguna vulnerabilidad, análisis de protocolos, etc. Todo esto en tiempo real.

Un Sistema Snort como IPS (Intrusion Prevention System) es un sistema que permite prevenir las intrusiones. Se trata de un tipo de sistema que permite ir paso a paso más allá de los IDS, ya que puede bloquear determinados tipos de ataques antes de que estos tengan éxito.

Cuando Snort trabaja para la prevención de intrusos como filtro integrado, todo el tráfico debe pasar a través del sistema con Snort antes de que llegue a la red interna.
Si el tráfico dispara una regla de Snort, se desechan los paquetes que la activaron.

Se trata de un sistema basado en red que monitoriza todo un dominio de colisión y funciona detectando usos indebidos. Estos usos indebidos (o sospechosos) se reflejan en una base de datos formada por patrones de ataques.

Dicha base de datos se puede descargar también desde la propia página web de Snort, donde además se pueden generar bases de patrones "a medida" de diferentes entornos (por ejemplo, ataques contra servidores web, intentos de negaciones de servicio, exploits...). Es usual utilizarlo en combinación con herramientas del tipo Honeyput con el fin de monitorizar e interpretar ataques reales en un escenario controlado.

COMO FUNCIONA SNORT

Ilustración 4 Esquema de SNORT. Fuente: Snortudenar

Módulo de **captura del tráfico** (paquetes). Es el encargado de capturar todos los ataques de la red utilizando la librería libpcap. Aprovechando al máximo los recursos de procesamiento y minimizando por tanto la pérdida de paquetes a tasas de inyección elevadas.

Decodificador. Se encarga de formar las estructuras de datos con los paquetes capturados e identificar los protocolos de enlace, de red, etc. Snort posee capacidades de decodificación para protocolos Ethernet, SLIP y PPP. Se encarga de tomar los paquetes que recoge el libpcap y almacenarlos en una estructura de datos en la que se apoyan el resto de capas.

En cuanto los paquetes han sido capturados, Snort debe descifrar los elementos de protocolo específicos para cada paquete. El decodificador de paquetes es en realidad una serie de decodificadores, de forma que cada uno descifra elementos de protocolos específicos.

Funciona sobre la pila de protocolos de Red, que comienza con el nivel más bajo: protocolos de la capa de Enlace de Datos, descifrando cada protocolo conforme asciende en la pila de protocolos de red.

Preprocesadores. Como Snort tiene que leer todo el tráfico de la red e interpretarlo también tiene que llevar un control de los paquetes que se envían por la red y así poder darle forma a la información. Por ejemplo, escucha todo el tráfico que tiene como destino una dirección y puertos determinados para ensamblar los datos y así poder interpretarlos.

Estos se encargan de coger la información que viaja por la red de una manera caótica y darle forma para que pueda ser interpretada. De esta forma una vez que tenemos los datos ordenados que viajan por la red aplicaremos las reglas (rules) para buscar un determinado ataque.

La arquitectura de preprocesadores de Snort consiste en pequeños programas C que toman decisiones sobre qué hacer con el paquete. Estos pequeños programas C se compilan junto a Snort en forma de librería. Estos preprocesadores son llamados justo después que Snort realice la Decodificación, y posteriormente se llama al Motor de Detección.

Motor de Detección. Analiza los paquetes en base a las reglas definidas para detectar los ataques. El motor de detección es la parte más importante de Snort. Su

responsabilidad es descubrir cualquier actividad de intrusión existente en un paquete. Para ello, el motor de detección emplea las reglas de Snort. Las reglas son leídas en estructuras de datos internas o cadenas donde son comparadas con cada paquete. Si un paquete empareja con cualquier regla, se realiza la acción apropiada. De lo contrario el paquete es descartado. Las acciones apropiadas pueden ser registrar el paquete o generar alarmas.

Dependiendo que detecte el motor dentro de un paquete, el sistema de alerta, se encarga de loguear o generar una alerta.

Reglas. Definen el conjunto de reglas que regirán el análisis de los paquetes detectados. Las reglas de Snort son utilizadas por el motor de detección para comparar los paquetes recibidos y generar las alertas en caso de existir coincidencia entre el contenido de los paquetes y las firmas.

El archivo snort.conf permite añadir o eliminar clases enteras de reglas. En la parte final del archivo se pueden ver todos los conjuntos de reglas de alertas.

Ilustración 5 Estructura Reglas Snort. Fuente Snortudenar

Cabecera de una regla

La cabecera permite establecer el origen y destino de la comunicación, y sobre dicha información realizar una determinada acción. La cabecera contiene algunos criterios para unir la regla con un paquete y dictar qué acción debe tomar una regla. Su estructura es:

<acción> <protocolo> <red origen> <puerto origen> <dirección> <red destino><puerto destino>

Tabla 3-2: Estructura de la Cabecera de una regla Snort

Acción	Protocolo	Red Origen	Puerto Origen	Dirección	Red Destino	Puerto Destino
alert	tcp	$EXTERNAL_NET	any	→	$HOME_NET	53

Ilustración 6 Estructura de la regla / alerta Snort. Fuente :Snortudenar

Acción: Permite indicar la acción que se debe realizar sobre dicho paquete. Los posibles valores son:

alert: Genera una alerta usando el método de alerta seleccionado y posteriormente loggea el paquete.

log: Comprueba el paquete.

pass: Ignora el paquete.

activate: Alerta y luego activa otra regla dinámica.

dynamic: Permanece ocioso hasta que se active una regla, entonces actua como un inspector de reglas.

Protocolo: Permite establecer el protocolo de comunicaciones que se va a utilizar. Los posibles valores son: TCP, UDP, IP e ICMP.

Red de origen y red de destino. Permite establecer el origen y el destino de la comunicación.

Puerto de origen y destino. Permite establecer los puertos origen y destino de la comunicación. Indica el número de puerto o el rango de puertos aplicado a la dirección de red que le precede.

Dirección. Permite establecer el sentido de la comunicación. Las posibles opciones son: ->, <- y <>.

Plugins de salida (Modulos de salida). Permiten definir qué, cómo y dónde se guardan las alertas y los correspondientes paquetes de red que las generaron. Pueden ser archivos de texto, bases de datos, servidor syslog, etc.

Plugins de detección. Partes del software que son compilados con Snort y se usan para modificar el motor de detección.

VII. DISEÑO METODOLÓGICO

La metodología a utilizar en esta monografía es de tipo intervención y evaluación. El aspecto intervención se debe a que se realizarán pruebas intrusivas y no intrusivas a la infraestructura de red de SNIP teniendo en cuenta aspectos técnicos, operacionales y metodológicos de todos los elementos que la conforman.

El segundo aspecto a utilizar es de tipo evaluación para poder valorar la eficacia de la seguridad implementada, calidad, eficiencia de la red y el impacto de las vulnerabilidades que se encuentren.

Este trabajo monográfico se desarrolló en cuatro etapas, las que se llevaron a cabo con diversas técnicas y herramientas para la recaudación y análisis de la información.

SNORT

Etapa 1: Levantamiento de la información (Reconocimiento).
Se llevaron a cabo visitas para recaudar información pertinente para el desarrollo de esta monografía.

En primera instancia se levantaron datos visuales sobre las instalaciones de la institución ubicando la distribución de infraestructura de red. Se ejecutaron entrevistas con los directivos para que dieran a conocer cuál es la problemática que sufren con los servicios con los que cuentan en la institución.

Entrevista.

1- ¿Cuantos servidores tienen?

2- ¿Qué tipo de seguridad informática utilizan?

3- ¿Cuentan con un detector de intrusos?

4- ¿Cómo está estructurada la red?

5- ¿Cómo saben si están siendo atacados?

6- ¿De qué manera detectan/notan la vulnerabilidad en la red?

7- ¿Cuál de los servicios que tienen como institución es el más vulnerable a ataques?

8- ¿Hay firewall en la red de la institución?

9- ¿Qué provocó que implementaran Fortinet?

10- ¿Cómo se encargan de evaluar los registros obtenidos?

11- ¿Qué medidas toman para reducir o minimizar los ataques registrados?

SNORT

De acuerdo a la técnica implementada para el levantamiento de información que se llevó a cabo con los directivos, se obtuvo lo que se detalla a continuación.

Mencionaron que notan lentitud en la red, por lo que ellos, consideran se deben al mal uso de ancho de banda y a los ataques internos y externos que sufren como institución. No dejaron de mencionar el uso de Streaming por parte de los usuarios, lo que consideran hace aporte al hecho de la ralentización de la intranet.

Los directivos mencionan que no cuentan con un detector de invasiones (detector de intrusos) que lleve registros de ataques internos, detallaron que habían adquirido los servicios de Fortigate para evaluar qué acciones llevar a cabo ante un ataque externo. Pero no les ha sido de gran utilidad debido a que esta herramienta es manipulada por un tercero y no les reporta ningún análisis instantáneo; por lo consiguiente para ellos está siendo una herramienta sin ningún provecho.

En la entrevista realizada se les solicitó que especificaran que servicios prestan como institución a lo que contestaron que a lo inmediato solo contaban con correo institucional y su sitio web, pero pretendían implementar Aulas Virtuales implementando Moodle a lo que también querrían agregarle protección debido a los datos que se almacenarían sobre los usuarios. Se les hizo la solicitud de información sobre sus trabajadores que incluía nombres, direcciones de correo institucional de los empleados y cargos que desempeñan en la institución.

SNORT

Etapa 2: Análisis De Topología De Red.

Al realizar la segunda visita a la institución, se hizo levantamiento de topología de red, una solicitud a los directivos de revelar la ubicación exacta de los dispositivos con los que cuentan para distribuir el acceso a Internet en la institución.

Dispositivo	Descripción
UTM Fortigate (Fortinet)	Funciones de seguridad como firewalls, prevención de intrusiones, filtrado web y protección frente a malware o correo no deseado.
Servidor PowerEdge (Web, Apps, Smart) Dell 2650	Maximiza las velocidades de procesamiento y ofrece un gran ancho de banda de memoria y entrada/salida (E/S) de datos.
2 Router Cisco 800	CiscoSystems Inc. Router de 8 puertos con switch integrado, producto 128 Mb instalados, 384 Mb máximo Memoria Dram 32 Mb instalado Máximo 128 Mb Memoria Flash Se basa en Ethernet y fast Ethernet.
2 Switchs Dell 5324	Incrementar en los servidores el ancho de banda disponible. Redes virtuales (VLAN) 802.1q. Capacidad tope de fábrica de 48 Gbps y una tasa de reenvío de 35.6 millones de paquetes por segundo.

SNORT

1 Switch Capa 3 3560	Switch Administrable Capa 3, 24 LAN Port Gigabit PoE+ (30W/435W), Memoria Ram 256MB, Memoria Flash 64MB, Power 715W, VLAN.

Tabla 2 Resultados del Análisis de topología de red SNIP

SNORT

La institución hace uso de red LAN para la conexión entre los trabajadores de la institución, de igual manera al acceso de Internet, lo que vendría a ser la parte que está protegida por la herramienta Fortigate. La conexión entre los trabajadores está dada según el cargo que tienen dentro de los diferentes departamentos de la institución.

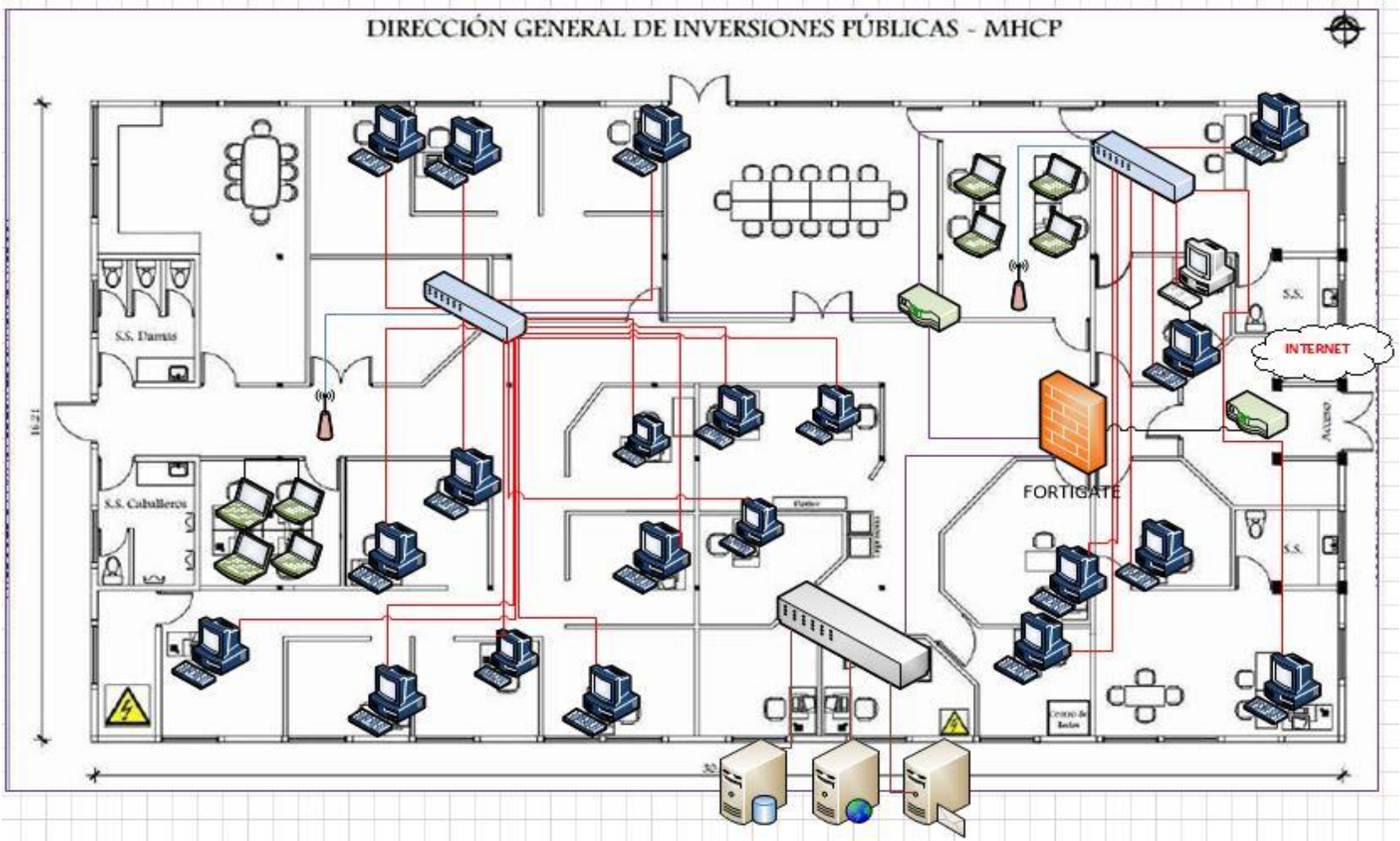


Ilustración 7 Distribución Administrativa del SNIP, imagen brindada por la institución. Diseño de la topología creada según lo recopilado de la entrevista.

Teniendo esto en cuenta y lo detallado en la entrevista realizada con anterioridad, se propone a los directivos implementar Snort en la zona desmilitarizada del servidor web, a lo que ellos como institución sugirieron también se haga en la red LAN, para que les ayude a la prevención de ataques internos.

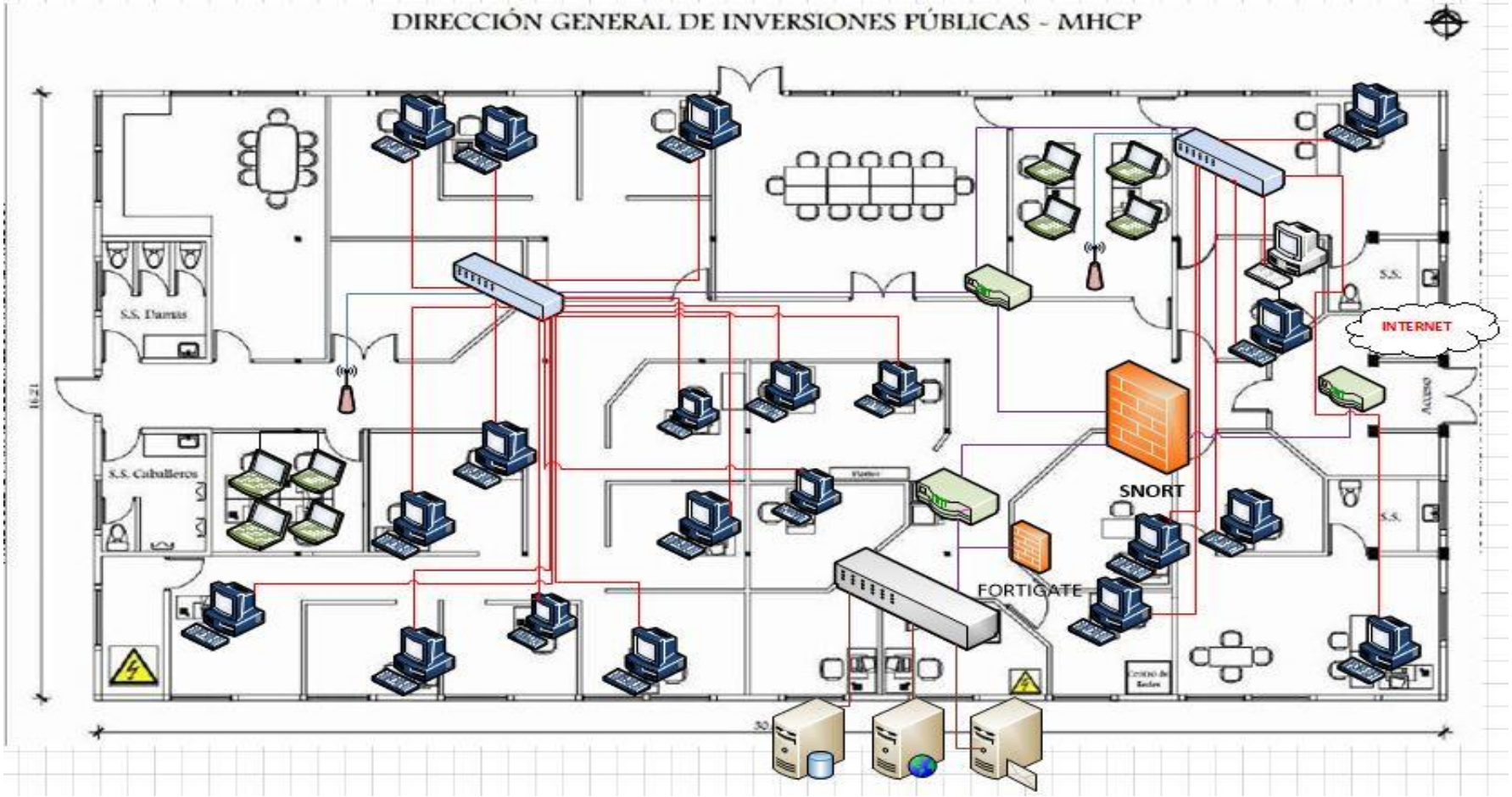


Ilustración 8 Distribución Administrativa del SNIP, imagen brindada por la institución. Diseño de la topología creada según lo recopilado de la entrevista.

SNORT

La topología lógica de la red de la institución correspondería a lo que se muestra en la ilustración 8.

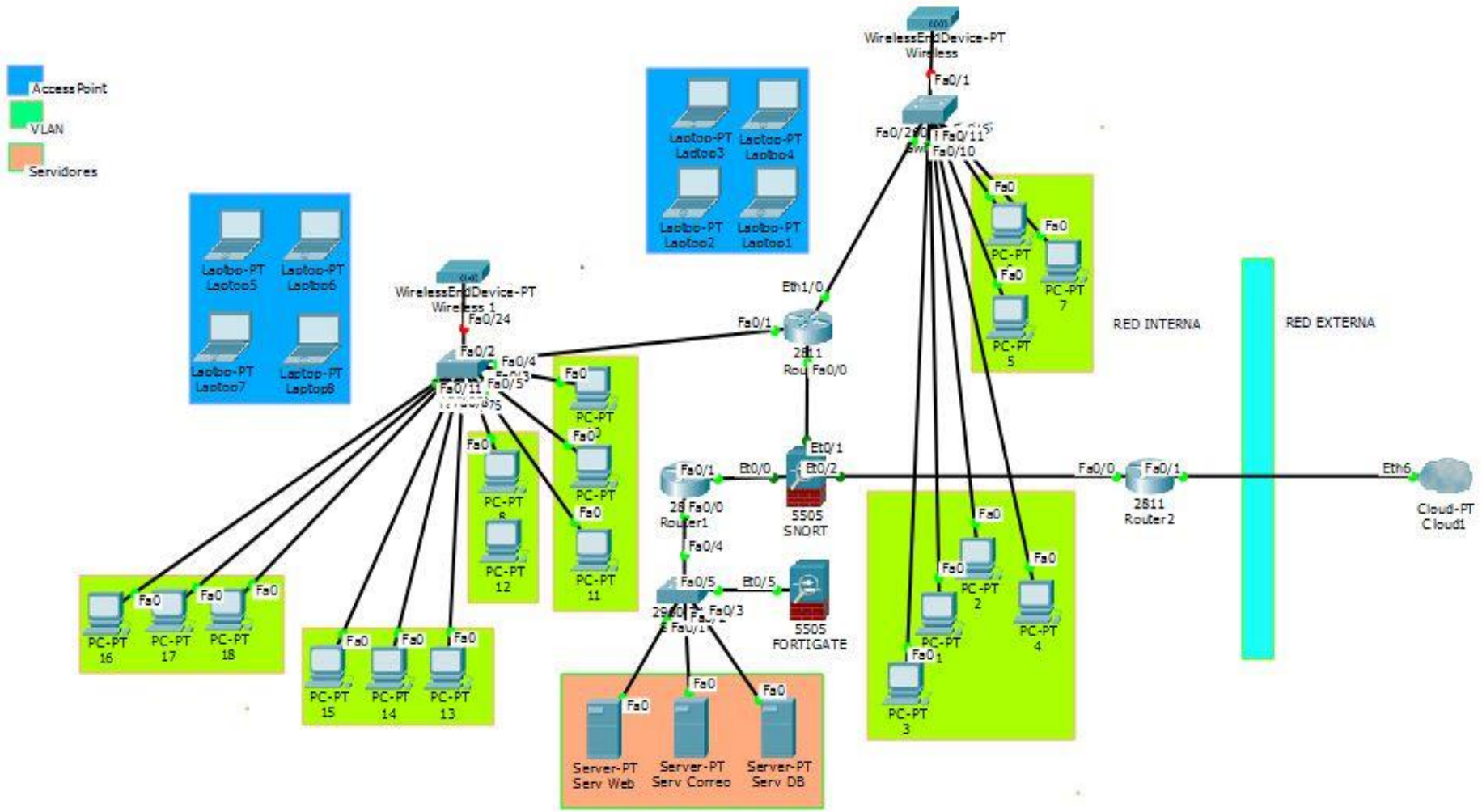


Ilustración 9 Topología Lógica de Snip.

SNORT

Etapa 3: Implementación de la herramienta SNORT como IDS.

Esta etapa encapsula la importancia de este trabajo monográfico, ya que al tener todos los datos necesarios se procederá a la implementación del SNORT, según se haya definido el lugar en la red. Este proceso incluye la configuración, activaciones de reglas, aprendizaje del SNORT como Sniffer, entre otras configuraciones.

Dentro de esta etapa se deben contemplar todas las tareas relacionadas con:

- La preparación de la infraestructura necesaria para la incorporación de la herramienta al entorno de red.
- La capacitación necesaria para la puesta en marcha dirigida al equipo de trabajo que se encargará de realizar el uso de la herramienta implementada.

Configuración de SNORT

SNORT puede funcionar en:

- **Modo IPS**, en el que se monitoriza por pantalla, toda la actividad de la red a través de un fichero de configuración en el que se especifican las reglas y patrones a filtrar y toma acciones sobre los ataques.
- **Modo IDS**, en el que se monitoriza por pantalla, toda la actividad de la red a través de un fichero de configuración en el que se especifican las reglas y patrones a filtrar para estudiar los posibles ataques.

En este caso se configurará SNORT en modo IDS. En la pestaña de Servicios vamos a “Prevención de Intrusos” ahí encontramos la configuración para SNORT.

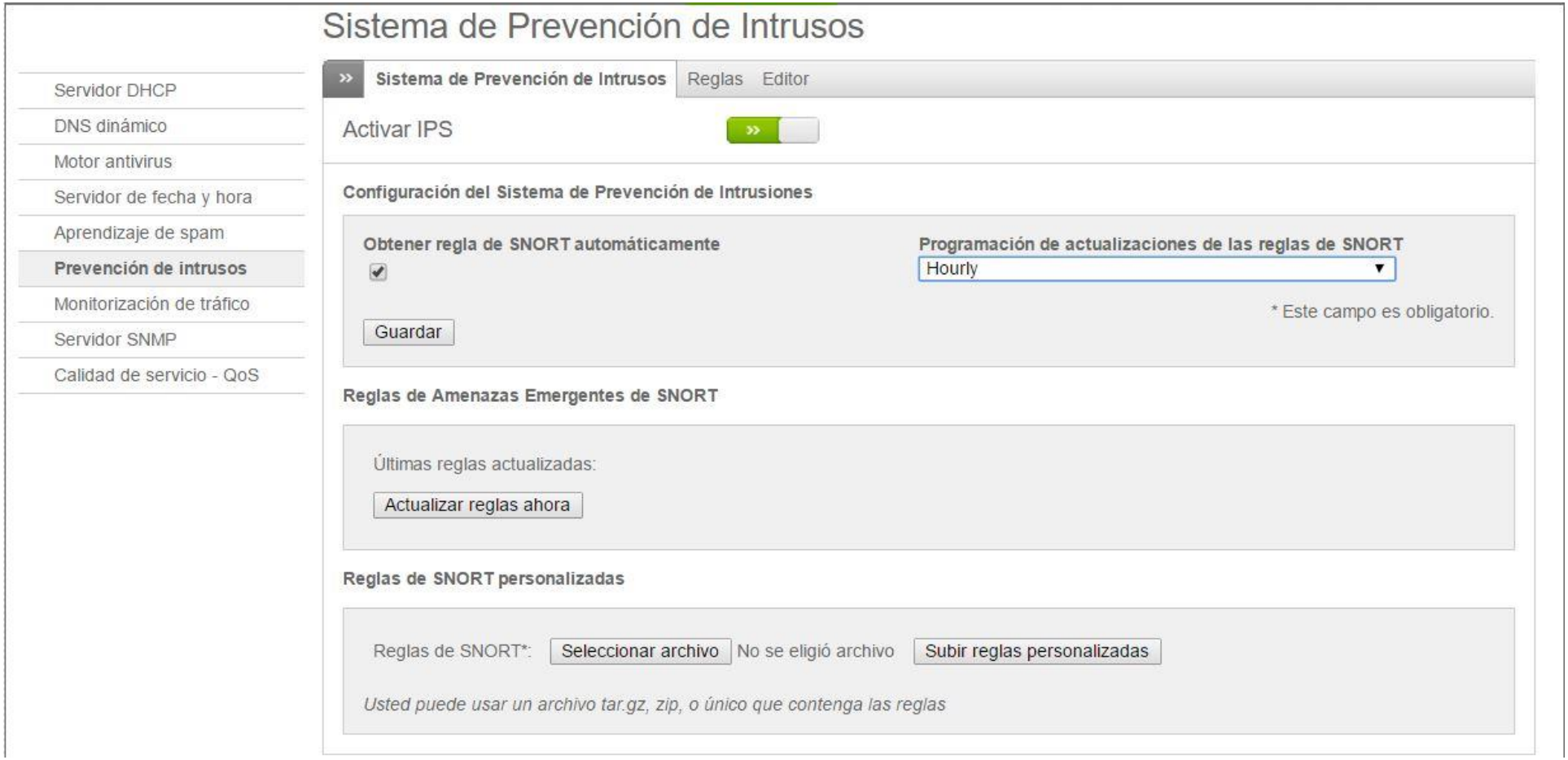


Ilustración 10 Configuración de Snort.

SNORT

Las opciones son sencillas, solo se habilita, y se le indica cada que tiempo se actualizarán las reglas desde los servidores de SNORT.

Ilustración 11 Activación y manipulación de alertas / reglas de Snort.

El sistema descargará las Reglas de Amenazas Emergentes para mantener actualizadas la lista que se crea gracias al código abierto.

En la sección de Reglas Personalizadas, SNORT permite crear reglas propias acordes a la necesidad de la institución y de lo que se desee realizar y analizar en la red de la misma. Partiendo del archivo que se descarga desde el sitio oficial de Snort.

En esta pestaña están las reglas que por defecto se activan de Snort, se listan según lo requerido por el usuario. La función de estas va en dependencia de la política que esté activado, nótese en la Ilustración 11 que la política activada es de ***Advertencia*** solamente. Para este trabajo monográfico la institución ha solicitado que solo se generen alertas de las intrusiones a los servidores con los que cuentan por lo que no hay una regla en estado activo de bloqueo para las intrusiones.

Al utilizar SNORT como IDS, no es necesario activar políticas de bloqueos, ya que lo que se pretende es tenerlo como sniffer y alertar una intrusión para que al ser analizados por al administrador de la herramienta y los respectivos directivos, tomen las decisiones que consideren pertinentes.

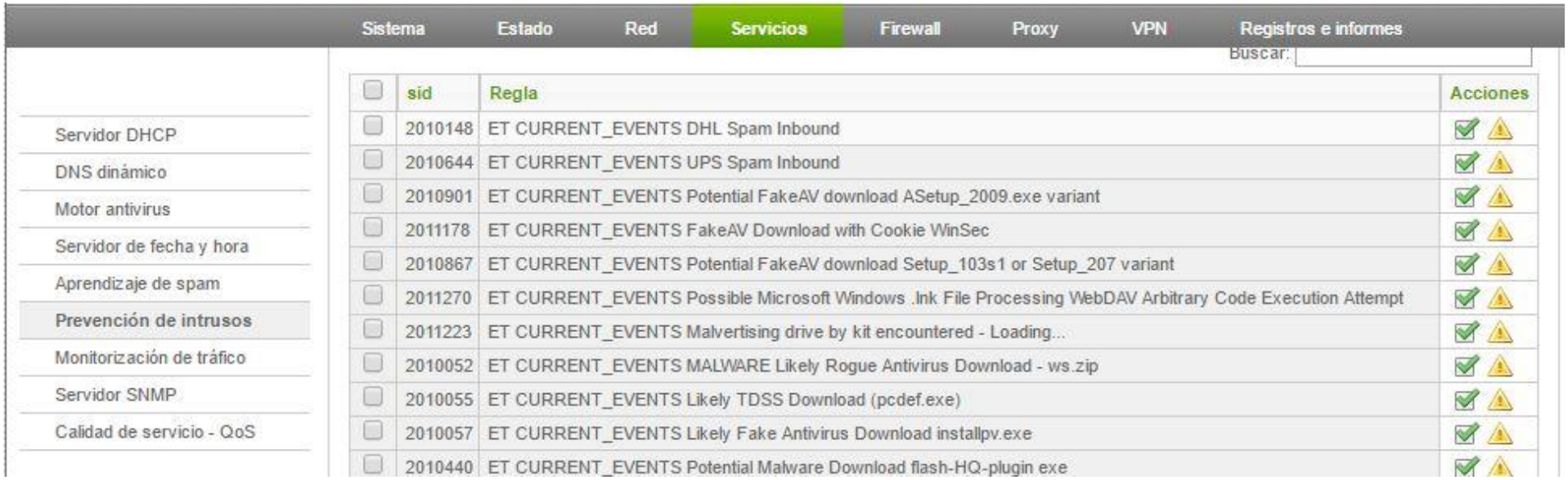


Ilustración 12 Muestra de la política activada para las reglas / alertas de Snort.

Tipos de formatos de alertas y Modos de alerta.

Snort genera dos tipos de alertas, que son:

Fast: El modo Alerta Rápida nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y puerto de origen y destino. Formato ASCII.

Full: El modo de Alerta Completa, nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y puerto de origen/destino e información completa de las cabeceras de los paquetes registrados. Formato ASCII. Las alertas de Snort se activarán según lo que detecte el IDS, estas se mantienen en modo advertencia porque están destinadas solo a *notificar* sucesos irregulares.

Especificación casos de uso.

Los casos de usos definen las diferentes funciones que serán realizadas por el IDS, mediante la interacción de este con cada uno de los tipos de usuarios, a los que se le denomina *actores.* Asi que la especificación de los casos de uso es de suma importancia, debido a que establece las funciones y responsabilidades que tiene cada actor con respecto al funcionamiento adecuado del IDS.

Tabla 3 Tabla 3 Actores del IDS

Actor	Descripción
Administrador	Este actor tiene los permisos para gestionar configuraciones dentro del IDS.
Usuario	Este actor no tiene permisos para gestionar configuraciones, pero hace uso del IDS a través del análisis de prevencion de intrusos en todo lo que transita por medio de la red LAN a la que está conectado en la institución.
Atacante	Este actor no tiene los permisos para estar dentro del IDS, pero hace uso del sistema al intentar conectarse a la red de la institución desde fuera de la red o de manera interna.

La tabla anterior muestra los actores principales y sus funciones dentro del sistema detector de intrusiones.

SNORT

Diagramas de casos de uso

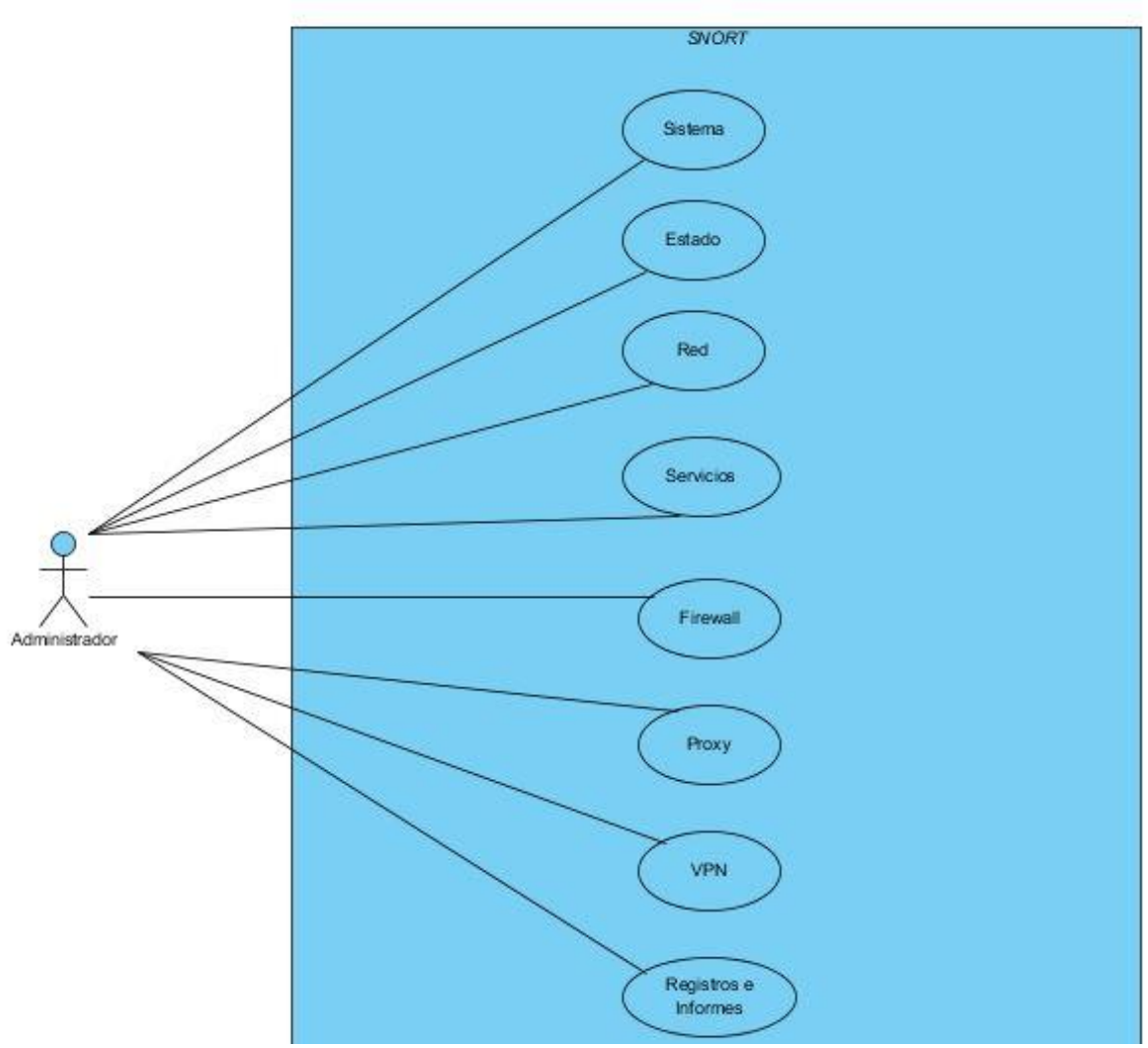


Diagrama CU 1 Sistema SNORT

Al especificar los principales actores del sistema, se deben crear diagramas UML, a fin de que se visualice el comportamiento del sistema detector de intrusos y su interacción con los diferentes usuarios.

SNORT

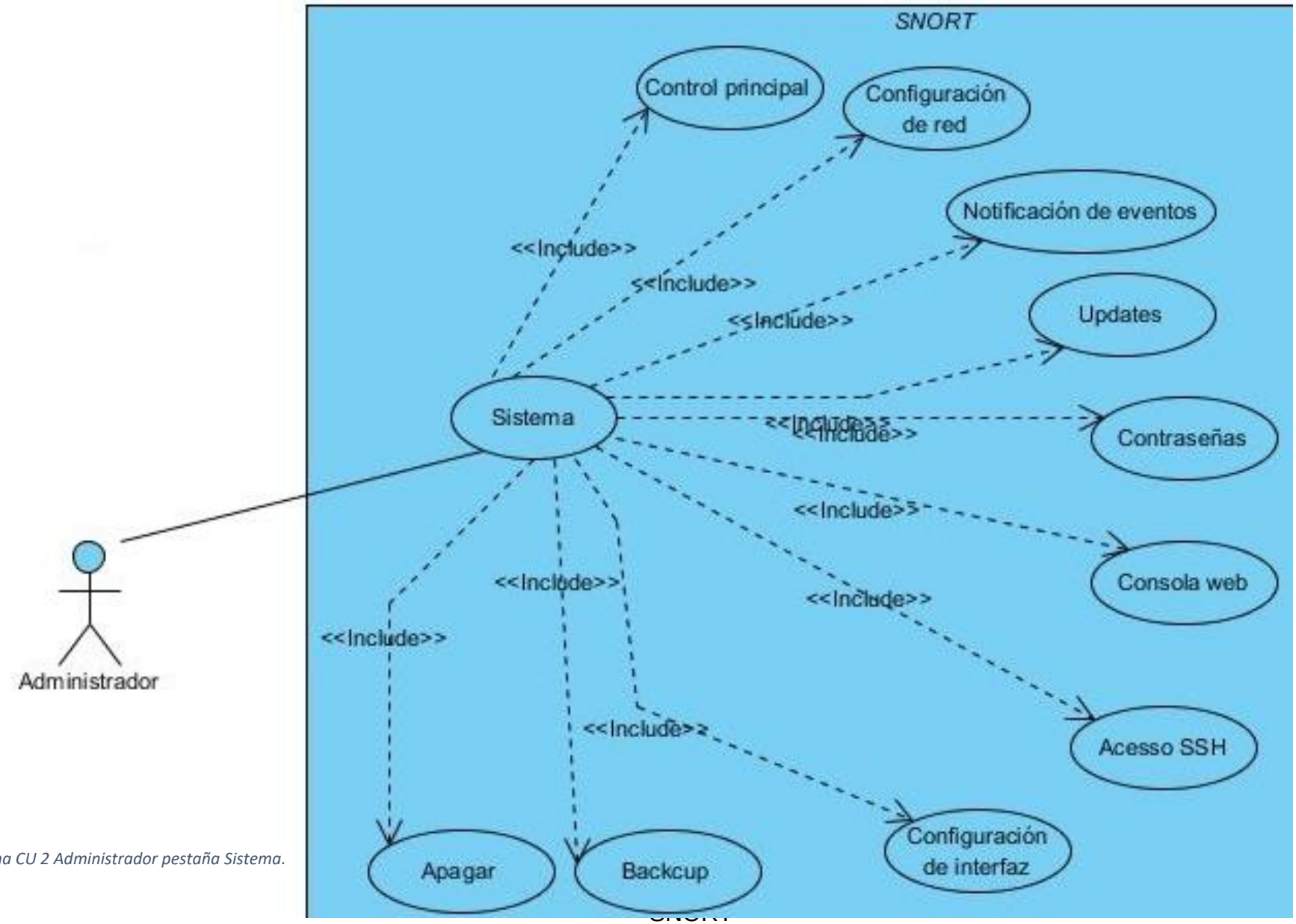


Diagrama CU 2 Administrador pestaña Sistema.

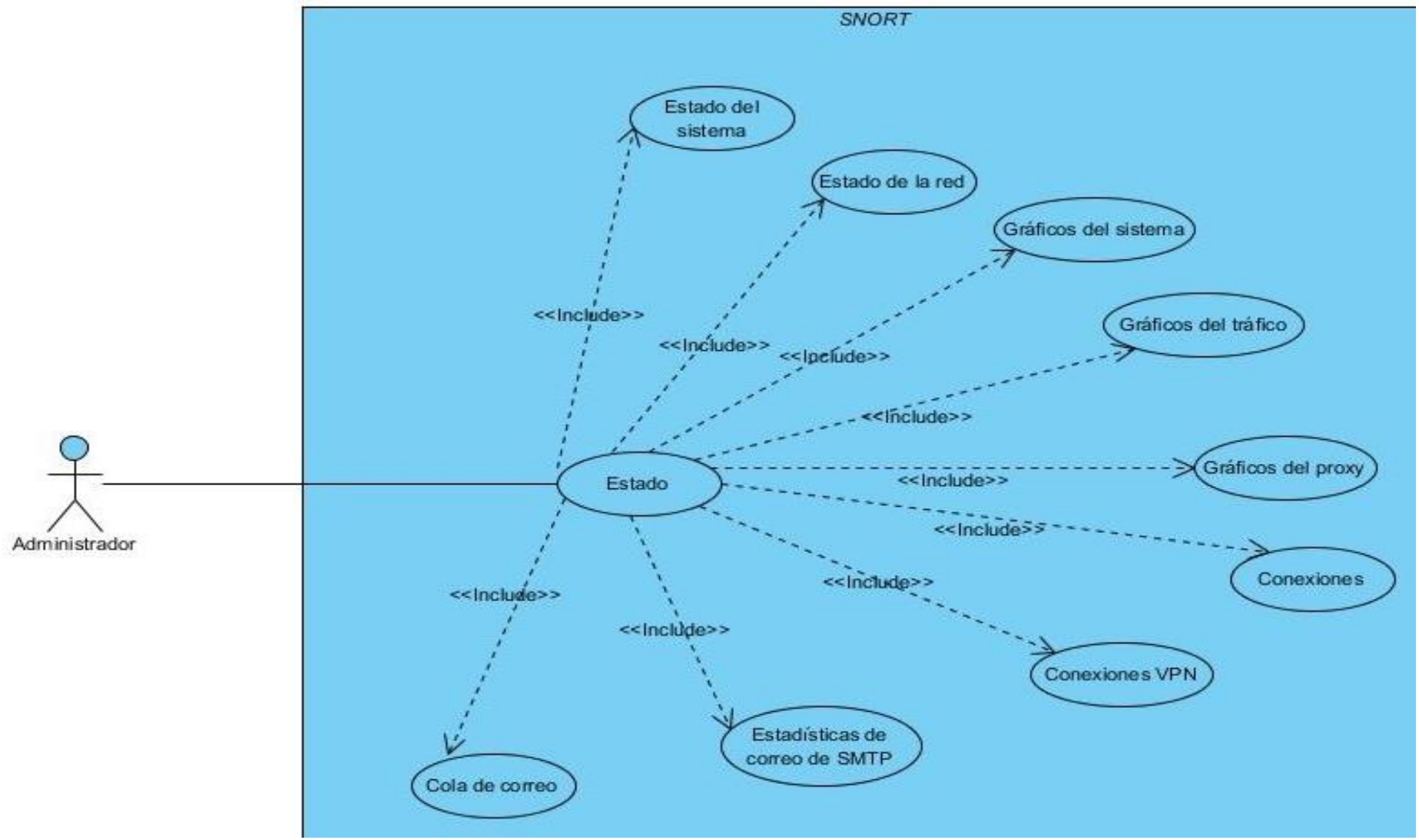


Diagrama CU 3Administrador pestaña Estado

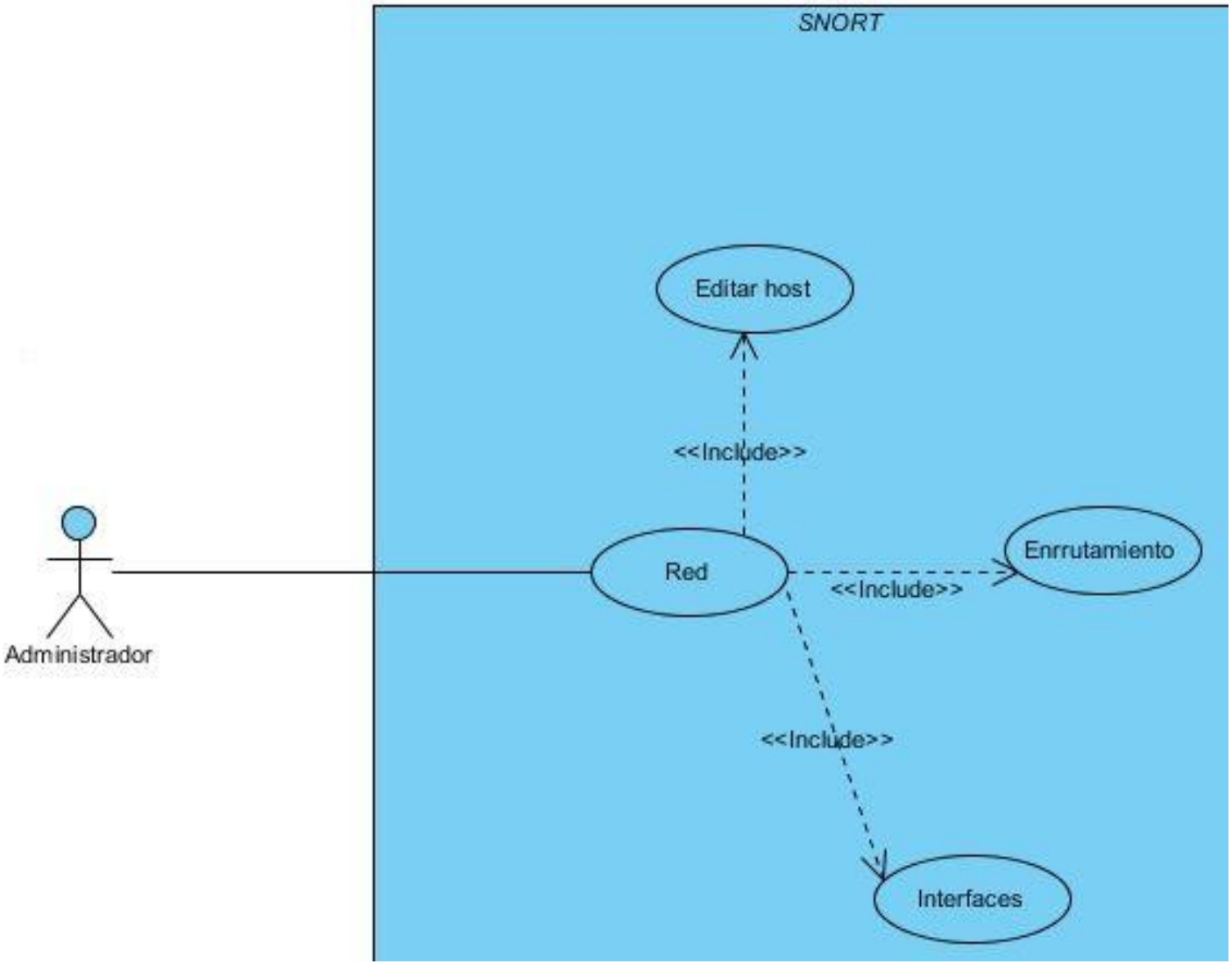


Diagrama CU 4 Administrador Pestaña Red.

SNORT

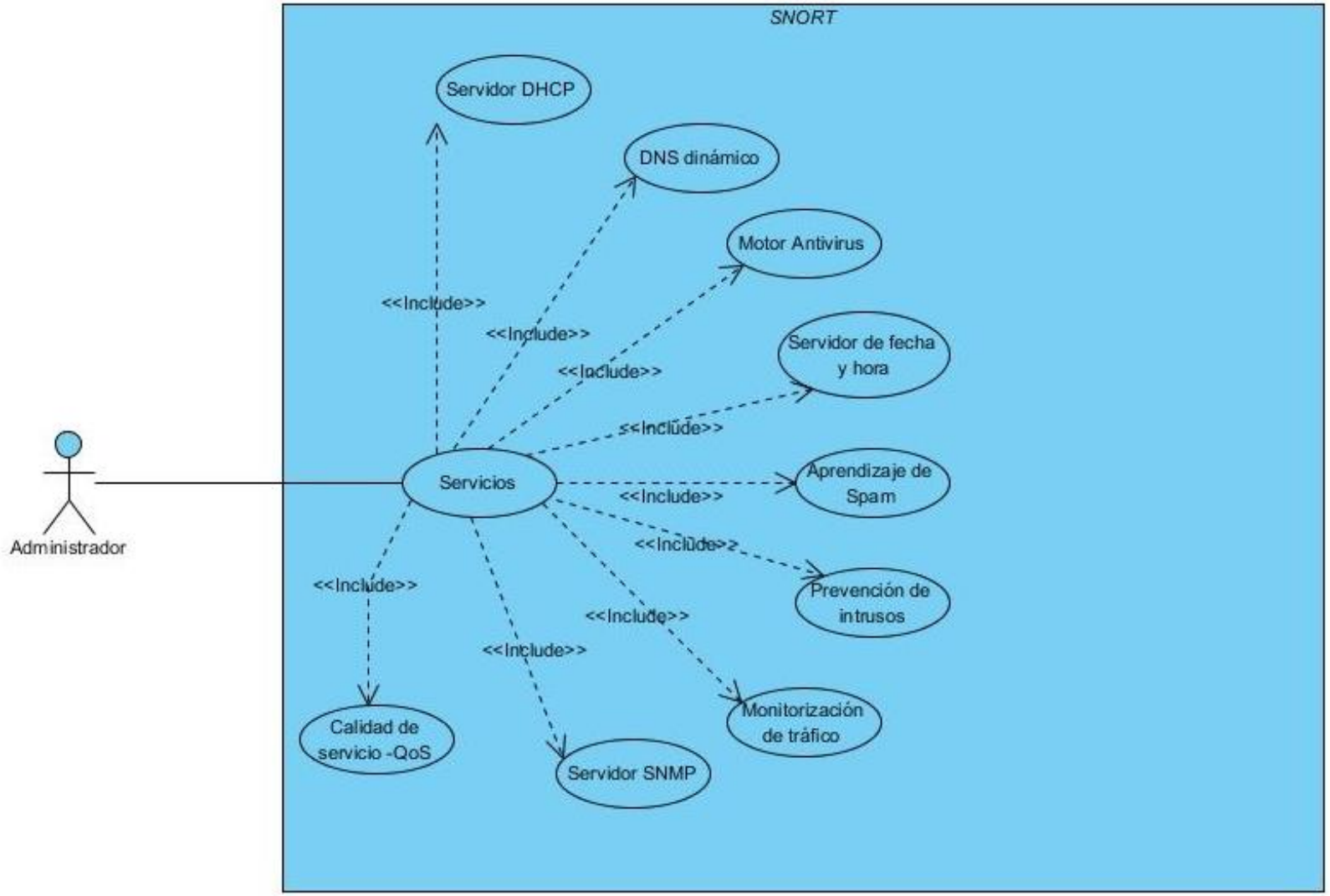


Diagrama CU 5 Administrador pestaña Servicios.

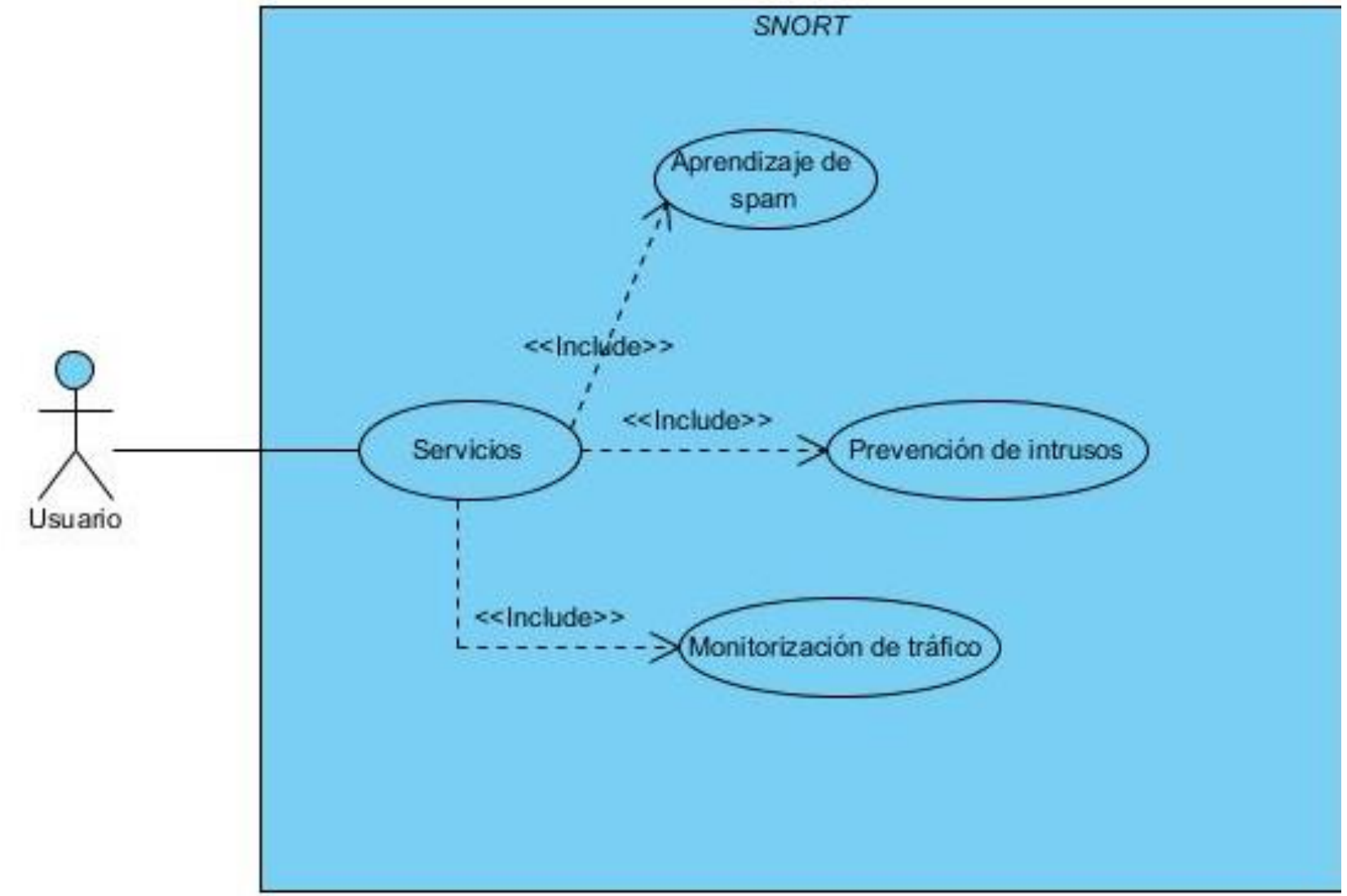


Diagrama CU 6 Usuario pestaña Servicios

SNORT

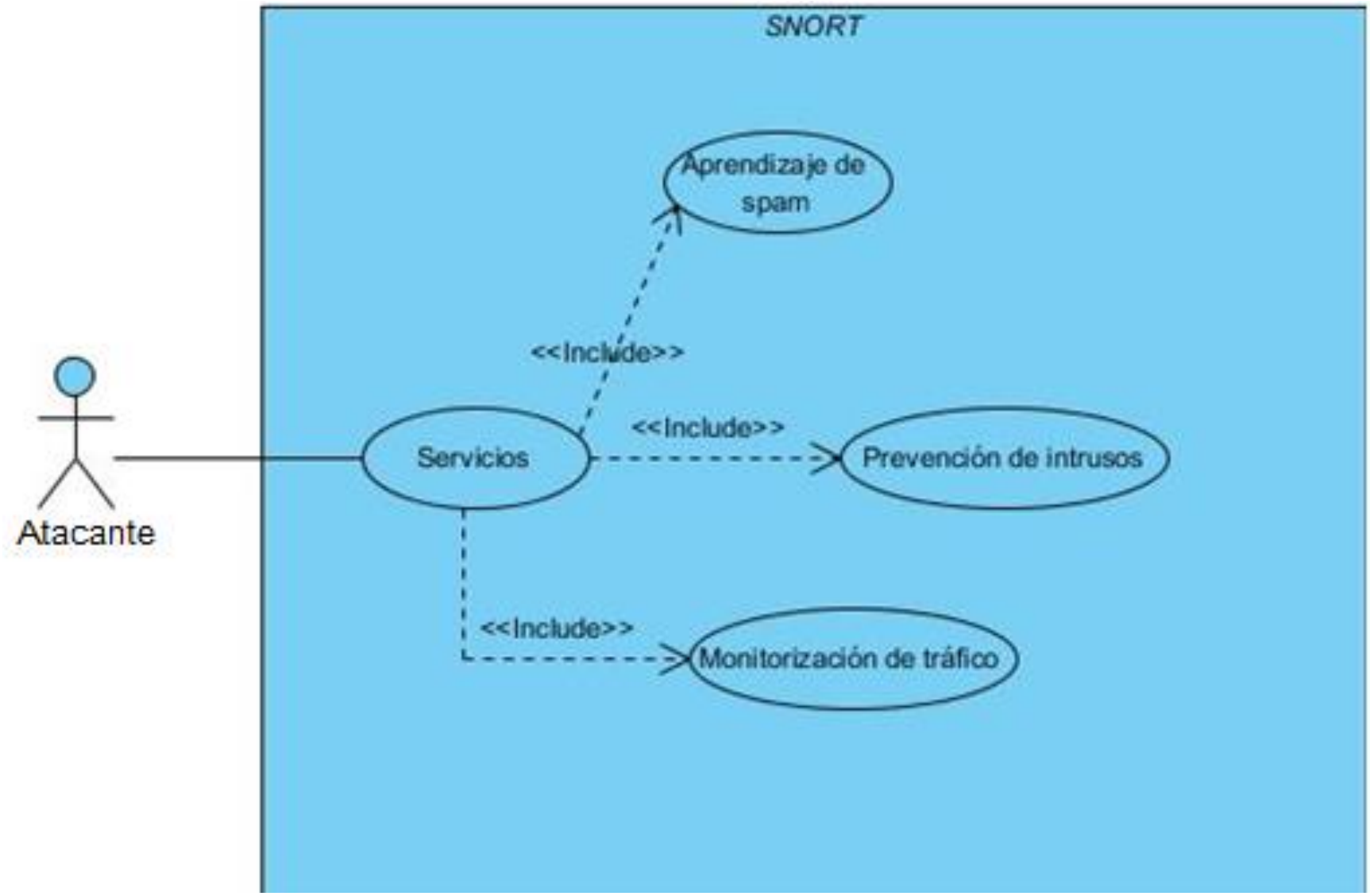


Diagrama CU 7 Atacante pestaña Servicios

SNORT

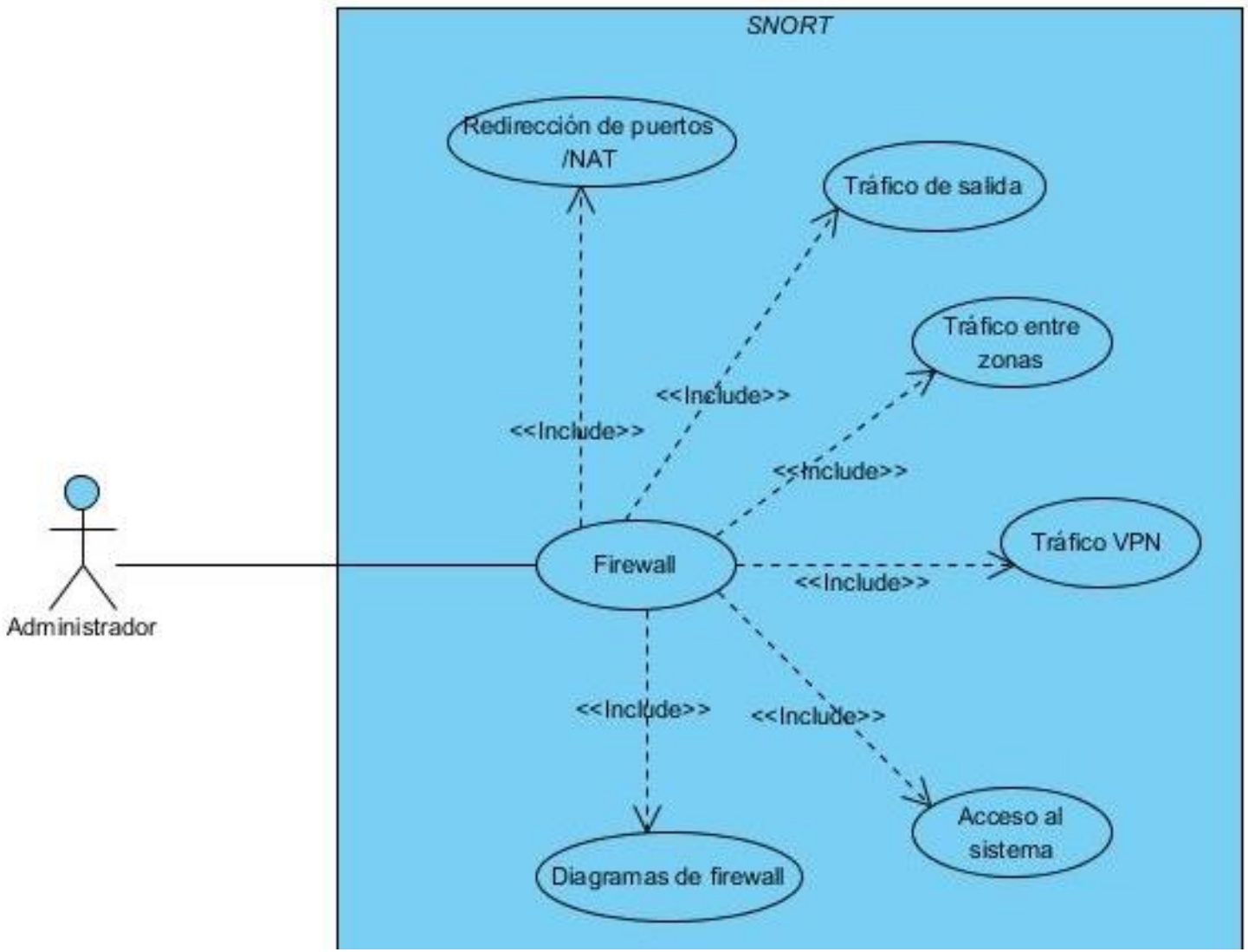


Diagrama CU 8 Administrador pestaña Firewall

SNORT

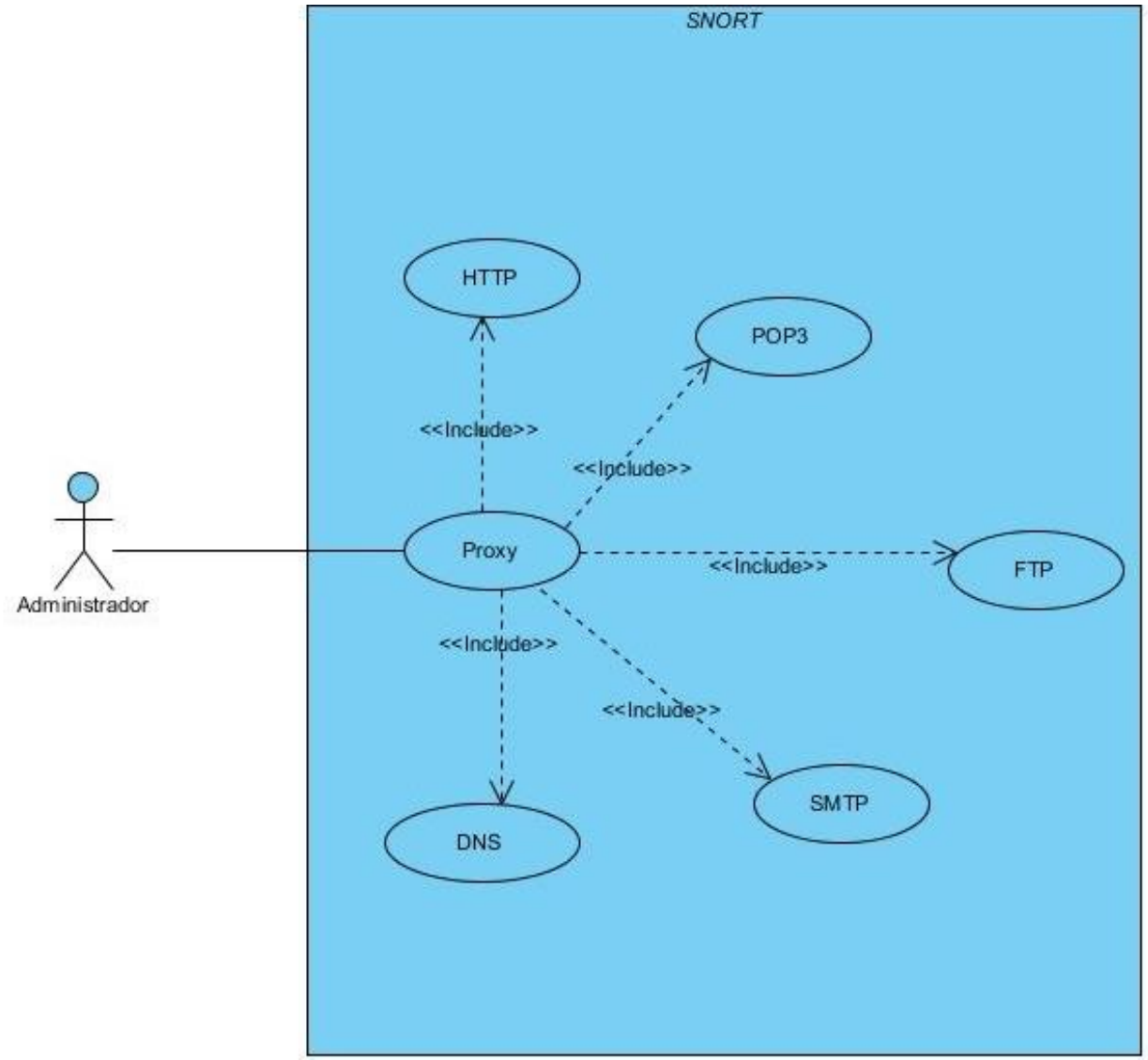


Diagrama CU 9 Administrador pestaña Proxy

SNORT

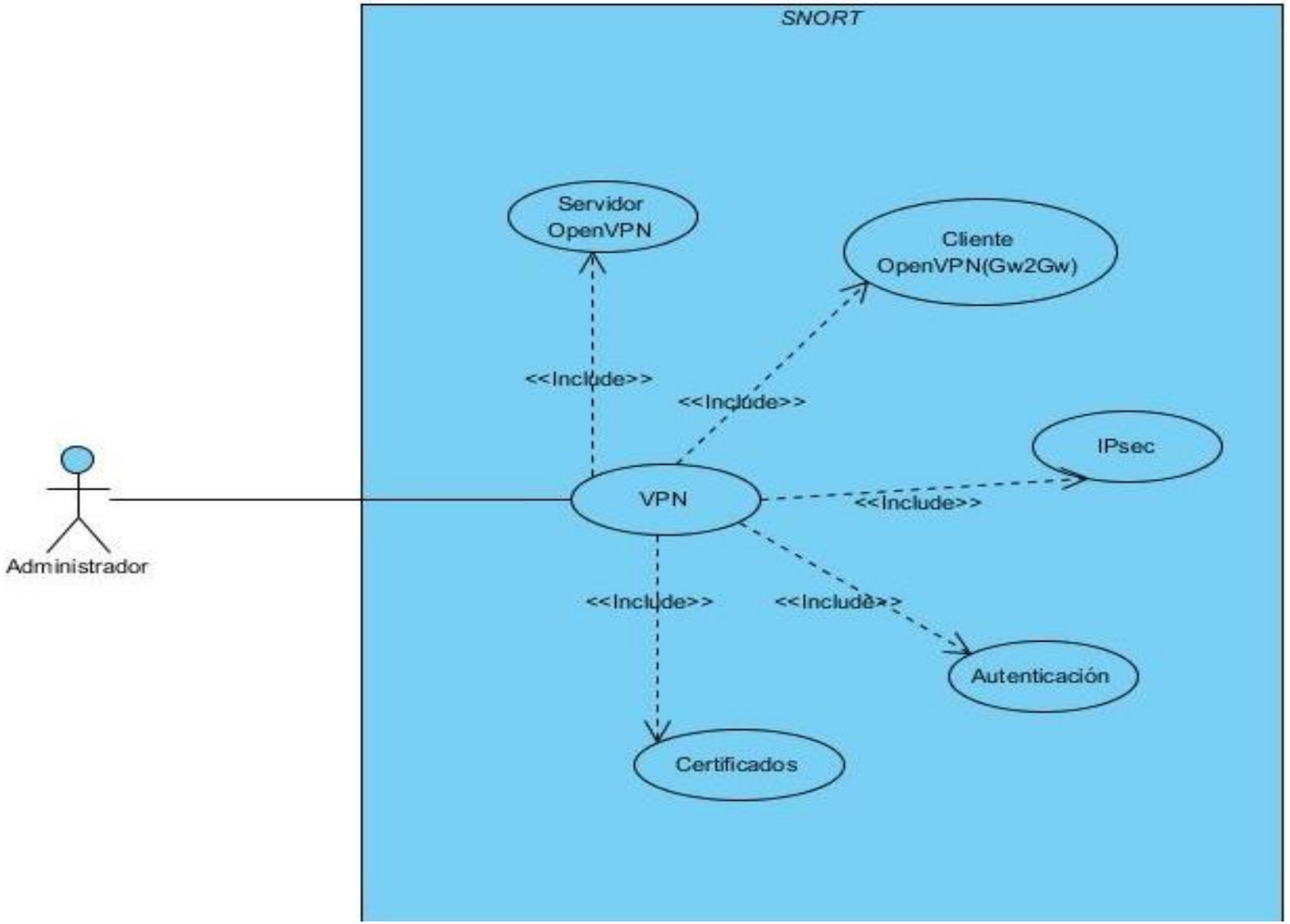


Diagrama CU 10 Administrador pestaña VPN

SNORT

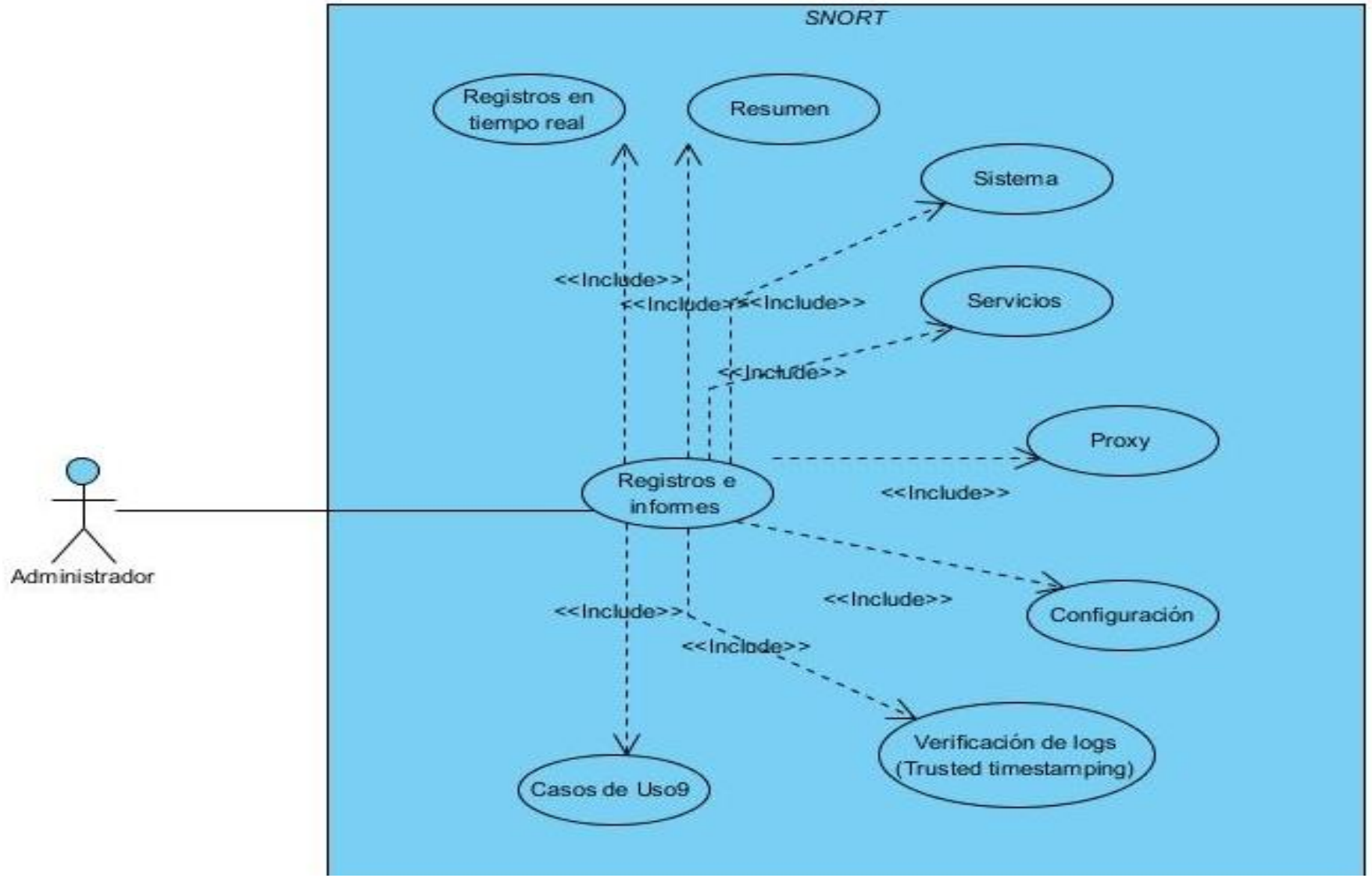


Diagrama CU 11 Administrador pestaña Registros e Informes.

SNORT

Detalle de Casos de Usos.

Esta plantilla de casos de usos es utilizada para el detalle y especificación de cada uno de estos

Tabla 4 Planilla Casos de uso

ID	CU1
Nombre	Nombre completo del caso de uso
Autor	Nombre del autor (autores) del caso de uso
Fecha	Fecha de creación del caso de uso
Actores	Especificación de los usuarios que interactúan con el caso de uso
Prioridad	Nivel de importancia de la realización del caso de uso
Frecuencia	Regularidad con la que se lleva a cabo el caso de uso
Descripción: Breve explicación del funcionamiento del caso de uso.	
Precondiciones: Establece las condiciones que deben cumplirse para la ejecución del caso de uso.	
Flujo Normal: Listado de las actividades necesarias para el correcto desarrollo del caso de uso.	
Flujo alternativo: Son las posibles salidas del sistema, en caso que el usuario decida no continuar con el flujo normal del caso de uso.	
Postcondiciones: Establece el estado del sistema cuando el caso de uso se realiza con éxito.	

SNORT

Niveles de prioridad y frecuencia.

Prioridad	Descripción
Baja	El caso de uso no afecta el funcionamiento de otros casos.
Media	Importante, no es necesaria la ejecución del caso de uso constantemente.
Alta	Obligatorio, el caso de uso afecta el funcionamiento de otros casos-

Tabla 5 Niveles de Prioridad

Frecuencia	Descripción
Baja	Raramente
Media	Algunas veces
Alta	Siempre

Tabla 6 Niveles de Frecuencia

Casos de uso del Sistema detector de Intrusión (IDS SNORT)

ID	CU1
Nombre	Administrar la pestaña Sistema
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite configuración de red ✓ Cambiar contraseñas ✓ Accede a la consola web, etc.	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador accede al control principal. ✓ El administrador realiza configuración de red. ✓ El administrador asigna contraseñas.	
Flujo alternativo: 1. Ninguno.	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 1 Administrador de pestaña Sistema

SNORT

ID	CU2
Nombre	Administrar la pestaña Estado
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Alta
Descripción: ✓ Permite acceder al estado del sistema.	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador visualiza los gráficos del tráfico.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 2 Administrar pestaña Estado

ID	CU3
Nombre	Administrar la pestaña Red
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite configuración de host ✓ Permite configuración de enrutamiento ✓ Permite configuración de interfaces	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador añade un nuevo host. ✓ El administrador añade una nueva ruta. ✓ El administrador crea un nuevo enlace.	
Flujo alternativo: 2. Ninguno.	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 3 Administrar pestaña Red

ID	CU4
Nombre	Administrar la pestaña Servicios
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite al administrador configurar el sistema de detección de intrusos.	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador activa y configura el IDS. ✓ El administrador activa, agrega y actualiza reglas.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 4 Administrar pestaña Servicios

ID	CU5
Nombre	Administrar la pestaña Firewall
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite agregar reglas de puerto NAT de destino ✓ Permite añadir una nueva regla al firewall ✓ Permite añadir una nueva regla de acceso al sistema	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador crea reglas NAT. ✓ El administrador añade nuevas reglas de acceso al sistema. ✓ El administrador visualiza los diagramas de firewall	
Flujo alternativo: 3. Ninguno.	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 5 Administrar pestaña Firewall

SNORT

ID	CU6
Nombre	Administrar la pestaña Proxy
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite habilitar el proxy ✓ Permite analizar proxy SMTP ✓ Permite configurar el proxy DNS	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador configura el proxy HTTP. ✓ El administrador configura políticas de acceso. ✓ El administrador realiza configuración general del POP3. ✓ El administrador realiza configuración general del proxy SMTP y del proxy DNS.	
Flujo alternativo: 4. Ninguno.	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 6 Administrar pestaña Proxy

SNORT

ID	CU7
Nombre	Administrar la pestaña VPN
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite habilitar servidor OpenVPN ✓ Permite activar redes privadas virtuales ✓ Permite añadir un nuevo usuario local	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador activa el servidor OpenVPN ✓ El administrador activa el IPsec ✓ El administrador añade un usuario local y añade un nuevo certificado	
Flujo alternativo: 5. Ninguno.	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 7 Administrar pestaña VPN

SNORT

ID	CU8
Nombre	Administrar la pestaña Registros e Informes
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite al administrador visualizar el informe en tiempo real.	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador analiza y guarda el informe en tiempo real.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 8 Administrar pestaña Registros e Informes

ID	CU9
Nombre	Control principal
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite visualizar la información de la información del hardware. ✓ Permite visualizar las interfaces de red.	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador tiene acceso a toda la información de Snort.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 9 Control principal

ID	CU10
Nombre	Configuración de red
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Realiza las configuraciones de red.	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El administrador selecciona el modo de red y un tipo de enlace ✓ Selecciona la zona de red ✓ Asigna preferencias de acceso a internet.	
Flujo alternativo: 2. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 10 Configuración de red

ID	CU11
Nombre	Notificación de eventos.
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Activa notificaciones de evento	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El actor activa las notificaciones de eventos ✓ El actor configura el correo electrónico.	
.Flujo alternativo: 3. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 11 Notificación de eventos.

ID	CU12
Nombre	Updates
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite realizar actualizaciones.	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El actor debe registrarse en la comunidad de Endian para recibir actualizaciones disponibles.	
Flujo alternativo: 4. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 12 Updates

ID	CU13
Nombre	Contraseñas
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Asigna contraseñas.	
Precondiciones: ✓ El administrador debe estar autenticado.	
Flujo Normal: ✓ El actor debe asignar las contraseñas de interfaz y del root.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 13 Contraseñas

ID	CU14
Nombre	Consola web
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Muestra la consola web	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor puede realizar configuraciones desde consola	
Flujo alternativo: 2. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 14 Consola web

ID	CU15
Nombre	Acceso SSH
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite al actor administrar las opciones de consola segura	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor puede activar el acceso a la seguridad en sistemas y técnicas hacking	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 15 Acceso SSH

ID	CU16
Nombre	Configuración de interfaz
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite seleccionar el idioma	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor selecciona el idioma	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 16 Configuración de interfaz

ID	CU17
Nombre	Backup
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite realizar Backup	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor crea soporte del contenido del sistema ✓ El actor importa el activo del backup	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 17 Backup

ID	CU18
Nombre	Apagar
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite apagar el sistema	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El administrador puede apagar el sistema	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 18 Apagar

ID	CU19
Nombre	Estado del sistema
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite ver la información del sistema	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor visualiza los servicios del sistema como usos de disco, tiempo de servicio y usuarios, módulos cargados y versión del kernel.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 19 Estado del sistema

ID	CU20
Nombre	Estado de red
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite visualizar las interfaces	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor visualiza el estado NIC, entradas de la tabla enrutamiento y entrada de la tabla ARP.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 20 Estado de red

ID	CU21
Nombre	Gráficos del sistema
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite obtener información acerca de los gráficos del sistema	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor observa los gráficos del CPU ✓ El actor observa los gráficos de la memoria y el gráfico de Swap	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 21 Gráficos del sistema

ID	CU22
Nombre	Gráficos del tráfico
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Muestra los gráficos de red	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor observa los tráficos de red y sus especificaciones	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 22 Gráficos del tráfico

ID	CU23
Nombre	Gráficos del proxy
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Representa los gráficos del acceso al proxy	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor visualiza los gráficos del tráfico del proxy por día y los grafico de la caché cada 5 minutos	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 23 Gráficos del proxy

ID	CU24
Nombre	Conexiones
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Muestra las conexiones	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor obtiene información de la conexiones LAN, INTERNTET, DMZ, RED INALAMBRICA, ENDIAN FIREWALL Y VPN	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 24 Conexiones

ID	CU25
Nombre	Conexiones VPN
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 25 Conexiones VPN

ID	CU26
Nombre	Estadísticas de correo de SMTP
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Muestra estadísticas de correo de SMTP	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor visualiza las gráficas del día, semana, mes y año	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 26 Estadísticas de correo de SMTP

ID	CU27
Nombre	Cola de correo
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Muestra información de correo	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor obtiene información del correo de proxy	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 27 Cola de correo

ID	CU28
Nombre	Editar host
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite configurar un host	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor puede configurar el host para servicios del sistema	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 28 Editar host

ID	CU29
Nombre	Enrutamiento
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite editar el enrutamiento	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor edita las entradas de enrutamiento actuales y la política de enrutamiento	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 29 Enrutamiento

ID	CU30
Nombre	Interfaces
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite administrar enlaces de internet	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor añade una nueva ruta y administra la política de enrutamiento ✓ El actor añade una nueva VLAN	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 30 Interfaces

ID	CU31
Nombre	Servidor DHCP
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite la configuración del servidor DHCP	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura el servidor ✓ Agrega una asignación fija y dinámicas	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente.	

Tabla CU 31 Servidor DHCP

SNORT

ID	CU32
Nombre	DNS Dinámico
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite agregar clientes DNS dinámicos	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor agrega host de DNS dinámicos ✓ El actor realiza forzado de actualización	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 32 DNS Dinámico

ID	CU33
Nombre	Motor Antivirus
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite configurar el antivirus	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura el antivirus ClamAV ✓ El actor programa la actualización de firmas ClamAV	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 33 Motor Antivirus

ID	CU34
Nombre	Servidor de fecha y hora
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite la configuración de fecha y hora	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura la hora manualmente o la sobrescribe con los servidores NTP predeterminados	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 34 Servidor de fecha y hora

ID	CU35
Nombre	Aprendizaje de spam
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite configurar el spam	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor edita la configuración predeterminada ✓ El actor añade fuente de aprendizaje de spam para IMAP ✓ El actor verifica las conexiones ✓ El actor inicia el aprendizaje y actualiza las reglas de spamAssassin	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 35 Aprendizaje de spam

ID	CU36
Nombre	Sistema de prevención de intrusos
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador , usuario, atacante
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite configurar el sistema de prevención de intrusos	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor puede activar o desactivar el IPS. ✓ El actor programa la actualización de reglas. ✓ El actor puede agregar reglas personalizadas.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 36 Sistema de prevención de intrusos

ID	CU37
Nombre	Monitorización de tráfico
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite analizar el tráfico monitoreado en la red	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor activa o desactiva la monitorización del tráfico. ✓ El actor debe guardar cambios.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 37 Monitorización de tráfico

ID	CU38
Nombre	Servidor SNMP
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite al administrador habilitar o deshabilitar el servidor SNMP	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura el servidor SNMP	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 38 Servidor SNMP

ID	CU39
Nombre	Calidad de Servicio QoS
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite al administrador agregar o eliminar dispositivos para la calidad de servicios	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor añadirá dispositivos especificando uso de ancho de banda de subida y de bajada. ✓ El actor modificará reglas de calidad de servicios.	
Flujo alternativo: 1. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 39 Calidad de Servicio QoS

SNORT

ID	CU40
Nombre	Redirección de Puertos
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite administrar reglas sobre reenvío de puerto	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor añade reglas de reenvío de puerto ✓ El actor puede ver las reglas del sistema	
Flujo alternativo: 5. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 40 Redirección de Puertos

ID	CU41
Nombre	NAT Fuente
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite agregar, activar o desactivar reglas de NAT	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor añade reglas de NAT origen ✓ El actor puede ver las reglas del sistema	
Flujo alternativo: 6. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 41 NAT Fuente

ID	CU42
Nombre	Tráfico enrutado de entrada
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite añadir regla al firewall	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor elige la red y los servicios a enrutar	
Flujo alternativo: 7. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 42 Tráfico enrutado de entrada

ID	CU43
Nombre	Tráfico de salida
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite configurar el firewall de salida	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor modifica las reglas actuales. ✓ El actor activa o desactiva el firewall de salida. ✓ El actor elige registrar conexiones salientes.	
Flujo alternativo: 8. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 43 Tráfico de salida

ID	CU44
Nombre	Trafico entre zonas
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor modifica las reglas actuales. ✓ El actor activa o desactiva el firewall de Inter-Zona. ✓ El actor elige registrar conexiones de Inter-Zona.	
Flujo alternativo: 9. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 44 Trafico entre zonas

ID	CU45
Nombre	Trafico VPN
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite configurar frewall de la VPN	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor activa o desactiva el firewall de la VPN	
Flujo alternativo: 10. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 45 Trafico VPN

ID	CU46
Nombre	Acceso al Sistema
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite la configuración al acceso del sistema	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor añade reglas de acceso al sistema ✓ El actor asigna políticas sobre los servicios de acceso al sistema	
Flujo alternativo: 11. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 46 Acceso al Sistema

ID	CU47
Nombre	Diagramas de Firewall
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite visualización de las configuraciones de los tráficos de red existentes	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor observa los diagramas de firewall y sus configuraciones.	
Flujo alternativo: 12. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 47 Diagramas de Firewall

ID	CU48
Nombre	HTTP Configuración
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite habilitar el proxy	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura el estado del proxy HTTP. ✓ El actor guarda los cambios realizados.	
Flujo alternativo: 13. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 48 HTTP Configuración

ID	CU49
Nombre	POP3
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite administrar configuración general de POP3	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor administra el detector de correo electrónico ✓ El actor guarda cambios realizados	
Flujo alternativo: 14. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 49 POP3

ID	CU50
Nombre	POP3 Filtro de Spam
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite analizar, aprobar o denegar envios o recibimiento de correos en lista.	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor lista los correos permitidos en “Lista Blanca” ✓ El actor lista los correos no permitidos en “Lista Negra” ✓ El actor etiqueta asunto del correo spam ✓ El actor establece valores al analizador de correo	
Flujo alternativo: 15. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 50 POP3 Filtro de Spam

SNORT

ID	CU51
Nombre	FTP
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite analizar virus FTP	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor habilita la red en la que desea analizar virus FTP ✓ El actor activa registros del firewall de conexiones salientes ✓ El actor agrega el proxy a evadir ✓ El actor guarda cambios realizados	
Flujo alternativo: 16. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 51 FTP

SNORT

ID	CU52
Nombre	Proxy SMTP
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite configurar proxy SMTP	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor activa o desactiva el Proxy SMTP	
Flujo alternativo: 17. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 52 Proxy SMTP

ID	CU53
Nombre	Proxy DNS
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite configurar el proxy, enrutar DNS y activar el spyware.	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura el proxy DNS ✓ El actor realiza enrutamiento de DNS ✓ El actor guarda los cambios realizados	
Flujo alternativo: 18. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 53 Proxy DNS

ID	CU54
Nombre	Servidor OpenVPN
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite configurar redes privadas virtuales	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor habilita o deshabilita el servidor OpenVPN	
Flujo alternativo: 19. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 54 Servidor OpenVPN

SNORT

ID	CU55
Nombre	IPSec
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite activar el IPSec del VPN	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor habilita o deshabilita la IPSec del VPN	
Flujo alternativo: 20. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 55 IPSec

ID	CU56
Nombre	Autenticación
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite crear usuarios locales del VPN	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor agrega usuarios al VPN	
Flujo alternativo: 21. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 56 Autenticación

ID	CU57
Nombre	Certificados
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite añadir certificados de VPN	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor añade certificados ✓ El actor especifica autoridad de certificados ✓ El actor lista certificados revocados	
Flujo alternativo: 22. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 57 Certificados

ID	CU58
Nombre	Registros en tiempo real
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite visualizar registros en tiempo real de los servicios contenidos	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor visualiza registros del Firewall ✓ El actor visualiza registros del Servidor Web ✓ El actor visualiza registros de OpenVPN ✓ El actor visualiza registros de Proxy SMTP ✓ El actor visualiza registros de Prevención de Intrusos ✓ El actor visualiza registros de Proxy HTTP ✓ El actor visualiza registros del Sistema ✓ El actor visualiza registros del Antivirus ClamAV	
Flujo alternativo: 23. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 58 Registros en tiempo real

SNORT

ID	CU59
Nombre	Resumen
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite visualizar resumen del registro en general	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor visualiza el resumen que se genera de los registros del dia anterior ✓ El actor puede exportar los registros ✓ El actor puede actualizar los registros	
Flujo alternativo: 24. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 59 Resumen

ID	CU60
Nombre	Visor del registro de Sistema
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite visualizar los registros del sistema	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor puede configurar lo que requiere visualizar según filtros, secciones o fecha ✓ El actor visualiza las acciones del sistema en el registro segundo a segundo	
Flujo alternativo: 25. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 60 Visor del registro de Sistema

ID	CU61
Nombre	Visor de registro de los servicios
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite visualizar los ataques en el firewall para el día específico	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura los filtros para visualizar los registros del IDS	
Flujo alternativo: 26. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 61 Visor de registro de los servicios

ID	CU62
Nombre	Visor de registro de servicio OpenVPN
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite visualizar los ataques en el firewall para el día específico	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura los filtros para visualizar los registros del VPN	
Flujo alternativo: 27. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 62 Visor de registro de servicio OpenVPN

ID	CU63
Nombre	Visor de registro de servicio ClamAV
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite visualizar los ataques en el firewall para el día específico	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura los filtros para visualizar los registros del ClamAV	
Flujo alternativo: 28. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 63 Visor de registro de servicio ClamAV

ID	CU64
Nombre	Visor del registro Firewall
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Alta
Frecuencia	Alta
Descripción: ✓ Permite visualizar los ataques en el firewall para el día específico	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura los filtros para visualizar los registros del firewall	
Flujo alternativo: 29. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 64 Visor del registro Firewall

ID	CU65
Nombre	Visor del registro del Proxy HTTP
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite visualizar los ataques en el firewall para el día específico	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura los filtros para visualizar los registros del Proxy HTTP ✓ El actor puede exportar los filtros ✓ El actor puede actualizar los filtros ✓ El actor especifica los IP de origen del que requiere el registro	
Flujo alternativo: 30. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 65 Visor del registro del Proxy HTTP

ID	CU66
Nombre	Informe de análisis del Proxy
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite generar informe de análisis de Proxy	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor debe activar el generador de informe de análisis Proxy ✓ El actor debe guardar los cambios ✓ El actor visualiza el informe de análisis Proxy	
Flujo alternativo: 31. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 66 Informe de análisis del Proxy

ID	CU67
Nombre	Visor del registro de SMTP
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite visualizar los ataques en el firewall para el día específico	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor configura los filtros para visualizar los registros de SMTP ✓ El actor puede exportar los registros ✓ El actor puede actualizar los registros ✓ El actor visualiza el registro de ataques en el firewall según el día específico	
Flujo alternativo: 32. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 67 Visor del registro de SMTP

SNORT

ID	CU68
Nombre	Configuración del registro
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Media
Frecuencia	Media
Descripción: ✓ Permite configurar el visor, resumen, registro remoto y registro de firewall	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor especifica las líneas a visualizar del registro ✓ El actor especifica la cantidad de días de los que se guardará registro ✓ El actor activa o desactiva el registro remoto ✓ El actor elige las acciones a seguir para el registro de Firewall ✓ El actor guarda los cambios realizados	
Flujo alternativo: 33. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 68 Configuración del registro

ID	CU69
Nombre	Verificación de sesión
Autor	Administrador
Fecha	20/09/2017
Actores	Administrador
Prioridad	Baja
Frecuencia	Baja
Descripción: ✓ Permite activar o desactivar verificación de inicio de sesión	
Precondiciones: ✓ El administrador debe estar autenticado	
Flujo Normal: ✓ El actor activa o desactiva la opción de verificar log	
Flujo alternativo: 34. Ninguno	
Postcondiciones: ✓ Los datos son guardados correctamente	

Tabla CU 69 Verificación de sesión

Estudio de Factibilidad

Implementar nuevos elementos en una institución implica realizar un estudio de viabilidad consecuente a lo que se pretende efectuar, a esto se le conoce como estudio de factibilidad, dentro de este se realizan diferentes actividades para recopilar datos que contribuyan a la toma de decisiones sobre lo que se requiere implementar. Este estudio de factibilidad está conformado de 3 aspectos: Técnico, Operativo y Económico.

1. Factibilidad Técnica.

En la actualidad la institución del Sistema de Inversión Pública cuenta con una variedad de computadoras asignadas al personal administrativo, estos a su vez están conectados a una LAN.

Cantidad	Descripción
21	PC Dell Optiplex Procesador Core i7 2,7 GHz Memoria Interna 8 GB DDR4 – SDRAM Almacenamiento total 1000 GB Puertos tipo A 1 3.0 Gen1 LAN 10,100,1000 Mbit/s
8	Laptop Pantalla LED 14 ‘‘ Intel Celeron N3000 series 1,1 GHz Memoria Interna 4 GB DDR3 – SDRAM Almacenamiento 500 GB

3	Routers Cisco 861 Interfaz WAN: 10/100 Mbps Fast Ethernet Interfaz de LAN: Conmutador gestionado 10/100 FE de 4 puertos
3	• 2 Switch Dell 5324 24 puertos. Algoritmo de encriptación SSL, SSL 3.0, SSL 2.0. Protocolo Ethernet. Método de autentificación: Secure Shell (SSH), RADIUS, TACACS + • 1 Switch Cisco Catalyst 3560G 24 puertos. Protocolo Ethernet. Método de autentificación: Kerberos, RADIUS, TACACS +, Secure Shell v.2 (SSH2)
1	Servidor Dell 2650, Almacenamiento interno máximo 730 GB (5 x 146 GB), Tarjeta de interfaz de red Dos tarjetas integradas Broadcom® Gigabit BaseT con soporte para recuperación tras fallos y distribución de carga. Software Microsoft® Windows® 2000 Server; Microsoft Windows 2000 Advanced Server; Red Hat® Linux® 7.2.

Tabla 7 Estudio de Factibilidad Técnica SNIP

SNORT

Sistema Operativo: **Endian**

Las nuevas adquisiciones para la implementación del Sistema Detector de Intrusos los requerimientos serán:

Cantidad	Descripción
1	Pc Dell UPC Core i5 Memoria 4 ranuras DIMM DDR3. Máx. capacidad de la memoria del sistema: 16GB BIOS 32Mb AMI UEFI Legal BIOS con soporte GUI Chipset Intel® H61 Disco Duro de 320GB - 2 puertos USB 3.1 Gen1 de ASMedia ASM1042, compatible con USB 1.0 / 2.0 / 3.0 hasta 5 Gb / s LAN PCI Gigabit x1 x 10/100/1000 Mb / s, 2 NEXT 10/100/1000 Mb / s.

Tabla 8 Propuesta de Adquisiciones

Este hardware requerido está dentro de la lista de los dispositivos con los que cuenta la institución, es decir que la institución no requerirá incurrir en gastos para la implementación del Sistema Detector de Intrusos.

SNORT

2. Factibilidad Operativa

Desde el punto de vista operativo el Sistema Detector de Intrusos, será de apoyo para la Institución y sus directivos en la realización del uso cotidiano de sus dispositivos dentro de la red en el SNIP, puesto que contribuirá en la seguridad interna y externa de la red con la que cuentan como institución.

Este sistema cuenta con una interfaz gráfica de fácil aprendizaje, con un alto nivel de interacción con el usuario, lo que lo convierte en una herramienta de gran utilidad para la institución. El administrador del sistema lo ejecutará según lo requiera la política de la institución.

El SNIP como tal acepta la implementación del Sistema detector de Intrusos, debido a que este le proporciona mayor seguridad y disminuye la ralentización de la red. La institución cuenta con personal capacitado, pero se anexará capacitaciones al personal que se encargue de la administración del sistema.

SNORT

3. Factibilidad Económica

Alternativa propuesta: ENDIAN LINUX

Se presenta el análisis de las cotizaciones para esta propuesta, en cuanto a costos de software, recursos humanos e insumos.

El software utilizado corresponde a Endian, distribución de LINUX, que se encuentra disponible para la descarga gratuita en el link http:// www.endian.com/news/endian-firewall-community-3-2-1/ que permite su distribución sin ningún costo de licencias.

- Recursos humanos

Cantidad	Personal	Salario x Mes	Total
1	Administrador	$280	$1680
1	Analista/Implementación	$300	$1800
			$3480

Tabla 9 Análisis de Cotizaciones HH

Nota:

- ❖ Se estima una duración de 6 meses para el desarrollo de este trabajo a la institución, para el cual se requiere un administrador con un salario de $280 y un analista con un salario de $300. Teniendo este proyecto un costo total de elaboración de $3480.
- ❖ El valor que se presenta anteriormente es el costo de la implementación y puesta en marcha de la alternativa propuesta a la institución, sin embargo, para el SNIP no tendrá valor alguno debido a que será un aporte de la Universidad para beneficio de la institución.

SNORT

- Insumos

Cantidad	Descripción	Precio
1	Pc Dell	$682.55

Tabla 10 Costos de Insumos

Los insumos mostrados representan el costo que la institución se ahorra al contar con el hardware que se requiere para implementar el detector de Intrusiones.

Conclusión del estudio de Factibilidad

Demostrado en los puntos anteriores, tanto los estudios de factibilidad técnica, operativa y económica resultan ser favorables para el proyecto. Lo que determina su viabilidad. El proyecto resulta ser una buena herramienta para la institución, además no implica que el SNIP incurra en gastos.

Etapa 4: Realización y análisis de pruebas de intrusión.

En esta etapa se realizaron las pruebas de intrusión a nivel de red local para validar el buen funcionamiento de las reglas y configuraciones realizadas en la etapa 3, lo cual por medio del análisis de estas pruebas conlleva a tomas de decisiones de mantener, mejorar o cambiar las reglas que ameriten configuraciones.

Antes de ejecutar los ataques pertinentes para esta etapa, se realizó un escaneo haciendo uso de la herramienta ZAP con el fin de detectar las vulnerabilidades de los servidores con los que cuentan en la institución.

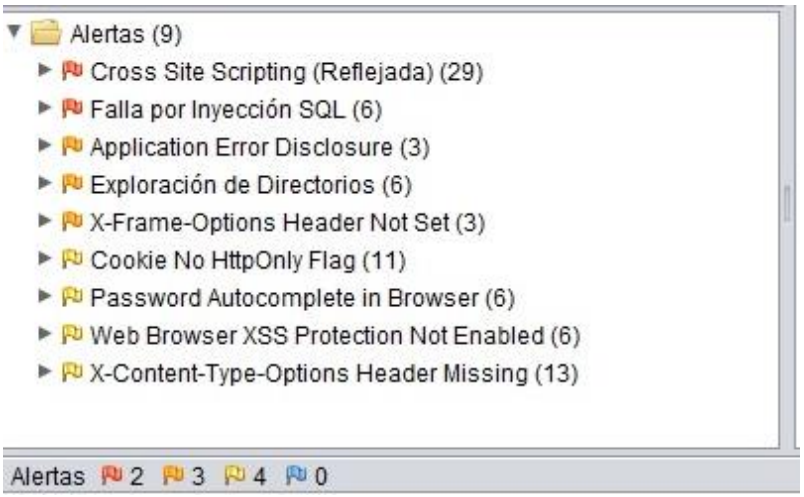


Ilustración 13 Reporte de Alertas de OWASP

Este escaneo muestra las alertas clasificadas en categorías por banderas. Los banderazos rojos están dentro de nivel de riesgo alto, las banderas naranjas en el nivel de riesgo medio y las amarillas en el nivel de riesgo bajo.

Al exportar los resultados del escaneo de esta herramienta, los expresa en formato HTML de manera que facilita su interpretación.

SNORT

Medium (Medium)	Exploración de Directorios
Description	Es posible ver el listado de directorios. La lista de directorios puede revelar scripts ocultos, incluyen archivos, copia de seguridad de los archivos de origen, etc, que se pueden acceder para leer información sensible.
URL	http://10.5.32.10/webmail/skins/Default/
Method	GET
Attack	Parent Directory
URL	http://10.5.32.10/webmail/static/
Method	GET
Attack	Parent Directory
URL	http://10.5.32.10/webmail/skins/
Method	GET
Attack	Parent Directory
URL	http://10.5.32.10/webmail/static/js/
Method	GET
Attack	Parent Directory
URL	http://10.5.32.10/webmail/static/css/
Method	GET
Attack	Parent Directory
URL	http://10.5.32.10/webmail/skins/Default/images/
Method	GET
Attack	Parent Directory
Instances	6
Solution	Desactivar la exploración de directorios. Si esto es necesario, asegúrese de que los archivos de la lista no induce riesgos.
Reference	http://httpd.apache.org/docs/mod/core.html#options http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html
CWE Id	548
WASC Id	48

Ilustración 14 Reporte HTML Ataque a Webmail Herramienta ZAP

1. Describe cual es la vulnerabilidad encontrada al momento de realizar el escaneo.
2. Muestra las direcciones que están vulnerables a ataques dentro de la red.
3. Cantidad de casos encontrados de vulnerabilidad.
4. Solución sugerida por la herramienta para solventar las vulnerabilidades encontradas.
5. Referencia a la solución sugerida.
6. Número de vulnerabilidad identificada, según la lista de tipos de debilidad del software, conocida como CWE (por sus siglas en inglés, Common Weakness Enumeration; en español Enumeración de debilidad común). Para este caso el número hace referencia en la lista a: Exposición a la información a través de la lista de directorios.
7. Numero en la lista de “The Web Application Security Consortium” (WASC) que hace referencia a Indexación Insegura.

SNORT

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://10.5.32.10/joomla/index.php/6-your-template
Method	GET
Parameter	X-Frame-Options
URL	http://10.5.32.10/joomla/index.php/log-out?view=remind
Method	GET
Parameter	X-Frame-Options
URL	http://10.5.32.10/joomla/index.php/acerca
Method	GET
Parameter	X-Frame-Options
URL	http://10.5.32.10/joomla/index.php/component/search/?Itemid=101&searchphrase=all&searchword
Method	GET
Parameter	X-Frame-Options
URL	http://10.5.32.10/webmail/
Method	GET
Parameter	X-Frame-Options
Instances	43
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15

Ilustración 15 Reporte HTML Ataque a Joomla Herramienta ZAP

SNORT

1. Describe cual es la vulnerabilidad encontrada al momento de realizar el escaneo.
2. Muestra las direcciones que están vulnerables a ataques dentro de la red.
3. Cantidad de casos encontrados de vulnerabilidad.
4. Solución sugerida por la herramienta para solventar las vulnerabilidades encontradas.
5. Referencia a la solución sugerida.
6. Número de vulnerabilidad identificada, según la lista de tipos de debilidad del software, conocida como CWE (por sus siglas en inglés, Common Weakness Enumeration; en español Enumeración de debilidad común). Para este caso el número hace referencia en la lista a: debilidad en la configuración del software.
7. Numero en la lista de “The Web Application Security Consortium” (WASC) que hace referencia a Debilidad, mala configuración de la aplicación.

SNORT

Luego de realizar el escaneo se procedió a llevar a cabo los ataques. Estos se ejecutaron para evaluar las condiciones en las que trabaja SNORT. Se hizo uso de la herramienta JOOMSCAN para realizar ataques al Sitio Web de la institución.

Ilustración 16 Aplicación utilizada para llevar a cabo los ataques.

El comando que se utiliza para escanear un objetivo y encontrar las vulnerabilidades del sitio web utiliza la siguiente sintaxis: **joomscan.pl –u url de destino;** para este caso será:

joomscan –u http://10.5.32.10/joomla

SNORT

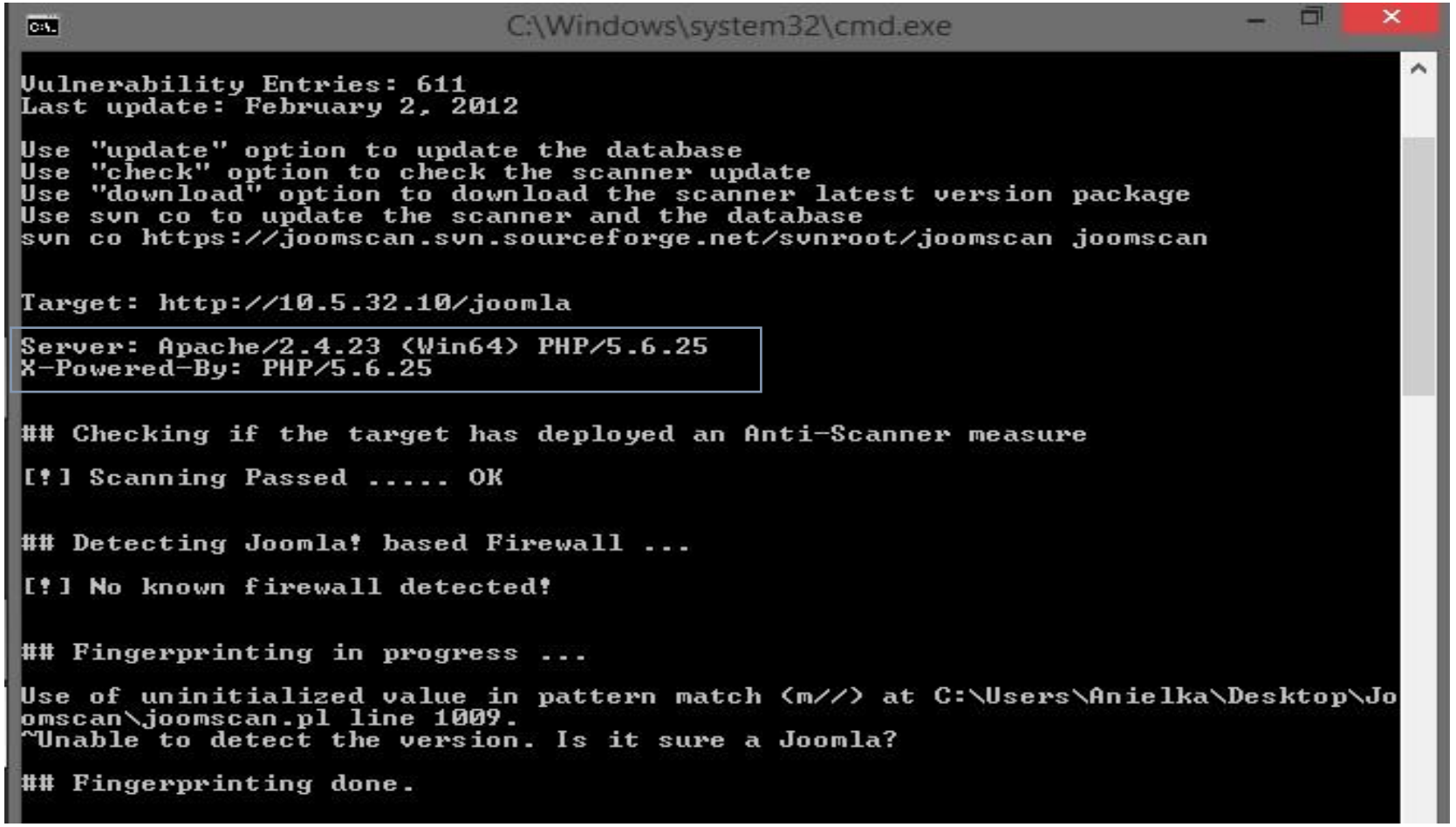


Ilustración 17 Resultados del escaneo

En la *ilustración 17* se muestra que el escaneo se ha iniciado y está mostrando la información del servidor web.

SNORT

Ilustración 18 Resultados del escaneo

La ilustración 18 muestra las Vulnerabilidades descubiertas. Al final de cada resultado expresa el valor de la vulnerabilidad. Si su valor es "*Yes*" como se resalta en la imagen significa que el sitio web es vulnerable en esas direcciones.

SNORT

Ilustración 19 Resultado del Scaneo

Al finalizar el escaneo, Joomscan muestra el total de posibles entradas encontradas y el total de entradas vulnerables que contiene el sitio web. Muestra también el tiempo de ejecución del escaneo.

Para estos ataques realizados se evaluó el monitoreo que realizó SNORT como detector de intrusos. Los resultados obtenidos se basan en las configuraciones que se realizaron para que funcionara como sniffer, es decir, al llevar a cabo la detección no ejecutó ninguna acción ya que es lo que se pretende al tenerlo de aprendiz. SNORT alertó sobre el ataque que se realizó con Joomscan.

SNORT

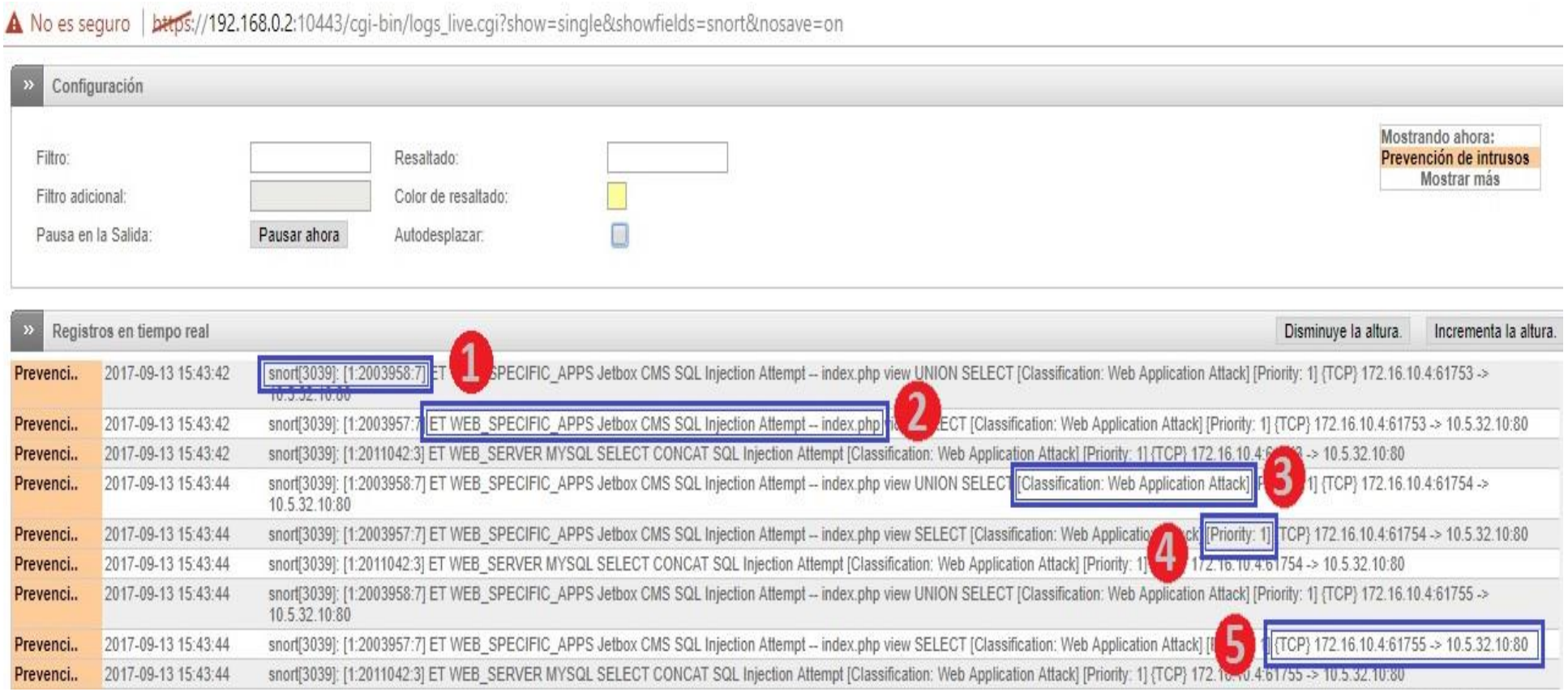


Ilustración 20 Reporte generado por SNORT. Ataque al Servidor Web.

La ilustración 20 muestra el reporte que genera Snort al detectar una posible intrusión en el servidor web.

Este reporte detalla:

1. El número de alerta contenido en el fichero de SNORT al que hace referencia la intrusión.
2. El tipo de ataque que se está intentando realiza

SNORT

3. La clasificación de a qué servicio se le está realizando el ataque, en este caso expresa que fue dirigido al Servidor Web.
4. Nivel de prioridad de la alerta.
5. Dirección desde donde se realizó el ataque y dirección a la que está dirigido el ataque.

La siguiente ilustración detalla:

1. El número de alerta contenido en el fichero de SNORT al que hace referencia la intrusión.
2. El tipo de ataque que se está intentando realizar.
3. La clasificación de a qué servicio se le está realizando el ataque, en este caso expresa que fue dirigido al Servidor Web con la herramienta SqlMap.
4. Nivel de prioridad de la alerta.
5. Dirección desde donde se realizó el ataque y dirección a la que está dirigido el ataq

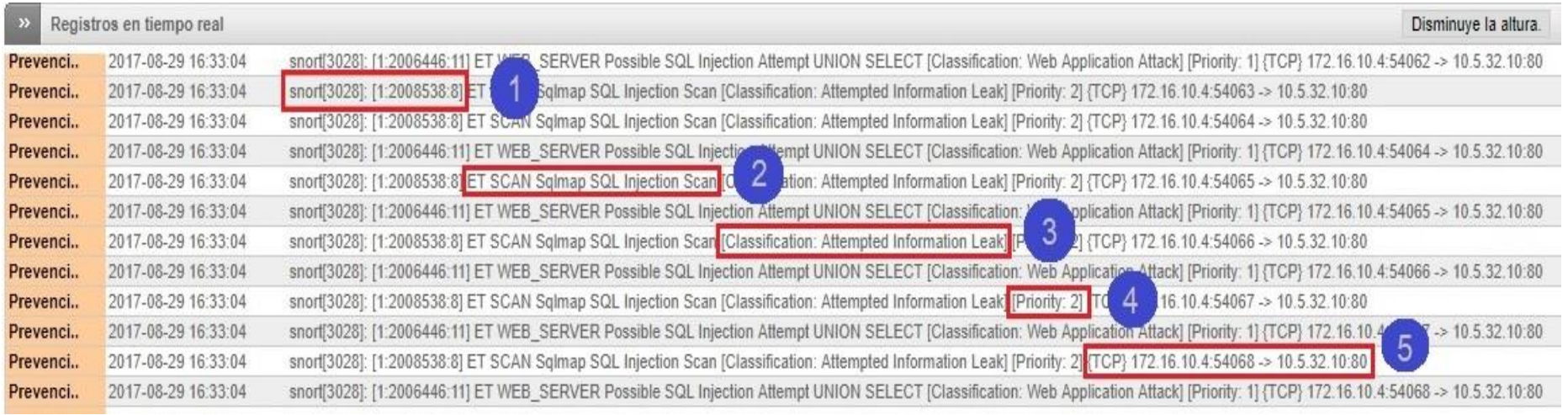


Ilustración 21 Reporte generado por SNORT. Ataque al Servidor de Correo.

SNORT

La siguiente tabla muestra el listado de reglas que contiene SNORT activadas según las categorías de ataques que se realicen

Tabla 11 Resumen de reglas activadas según los ataques realizados.

Regla	Clasificación	Función	Dirigido
auto/emerging activex.rulex	Analiza el comportamiento del tráfico de datos en la red interna	Sniffer (Oyente)	Red en general de la institución.
Exploit	Contiene diferentes categorías de servicios de Exploits (aprovechamiento de vulnerabilidad) que no están especificados en las reglas.	Detector ataques SQL	Servidor web. Correo electrónico y Aulas virtuales.
SQL	Reglas para ataques de vulnerabilidades. Incluye reglas que detectan la actividad básica del protocolo para fines de registro.	Detector ataques SQL	Correo electrónico y Aulas virtuales.
Web Server	Reglas para ataques y vulnerabilidades contra el servidor web.	Detector ataques servidores web.	Servidor web.
DNS	Reglas para ataques y vulnerabilidades con respecto a DNS.	Detector ataques ataques sevidores web.	Servidor web.

Herramienta de ataque	Servidor a atacar	Ataque	Clasificación de ataque	Sintáxis
Joomscan	Sitio Web (Joomscan)	Prueba de SQL Injection, divulgación de ruta completa	Intento de escape de información	Joomscan.pl –u http://10.5.32.10/joomla
SQLMap	Servidor de correo (Webmail)	Prueba de SQL Injection	Intento de escape de información	sqlmap.py –u Http://10.5.32.10/webmail
SQLMap	Servidor de Bases de datos (Moodle)	Prueba de SQL Injection	Intento de escape de información	sqlmap.py –u Http://10.5.32.10/moodle

Tabla 12 Lista de ataques realizados.

La tabla anterior contiene en resumen el listado de los ataques realizados para las pruebas de intrusión dirigidos a los servidores con los que trabajan en la institución.

SNORT

Conclusión.

El análisis de topología de red sirvió para determinar la posición óptima de la herramienta IDS, lo que nos hizo ubicarlo en un punto clave entre la red interna d la institución, los servidores y la red externa.

La implementación de esta herramienta servirá para el análisis de tráfico de datos y evaluación de consumo de ancho de banda, gracias a los reportes obtenidos que genera la herramienta; lo que conlleva a un mejor uso y distribución de ancho de banda.

Con la ejecución de ataques a los servicios de la institución se demuestra la funcionalidad de la herramienta cumpliendo así con lo requerido por los directivos.

Con este desarrollo monográfico se concluye que, con la implementación de la herramienta SNORT los directivos del SNIP estarán en capacidad de tomas de decisiones en dependencia de los resultados obtenidos de los reportes de ataque del Snort, según vayan siendo analizados, ya que, el hecho de usar ip segmentados les facilita la identificación del intruso.

Recomendaciones

Al momento de llevar a cabo la implementación de este desarrollo monográfico los directivos deberán decidir si poner las reglas de la herramienta SNORT en modo detección o prevención, designar un encargado de la administración de la herramienta para que puedan mantenerse informados a través de los registros en tiempo real que les brinda la herramienta SNORT.

VIII. GLOSARIO

1. Exploit: nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad del sistema. El fin de este puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.
2. Fortigate: Sistema de seguridad desarrollado por Fortinet, software libre y funciona como detector de amenazas.
3. IDS (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusiones.
4. Intruso: Persona que intenta acceder a un sistema informático sin autorización.
5. Libpcap: es una librería open source escrita en C que ofrece al programador una interfaz desde la que capturar paquetes en la capa de red, además Libpcap es perfectamente portable entre un gran número de SO's.
6. OpenSource: es el término con el que se conoce al software distribuido y desarrollado libremente. El código abierto tiene un punto de vista más orientado a los beneficios prácticos de compartir el código que a las cuestiones éticas y morales las cuales destacan en el llamado software libre.
7. Servicios FTP: "File Transfer Protocol", Protocolo para la Transferencia de Archivos. Los servicios FTP, son programas especiales que se ejecutan en un servidor conectado normalmente en Internet (aunque puede estar conectado en otros tipos de redes, LAN, MAN, etc.). La función del mismo es permitir el desplazamiento de datos entre diferentes servidores/ordenadores.
8. Sniffers: son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet.

9. Streaming: la tecnología streaming permite que un servidor se conecte con una computadora y se establezca una comunicación en la que los datos fluyen de forma continua, sin interrupciones.
10. TCP-RST: conjunto de protocolo activado con el flag RST (Reset): Este bit se utiliza para reiniciar una conexión debido a paquetes corrompidos.

IX. BIBLIOGRAFÍA

Alfon. (2003). Sistemas de detección de Intrusos y SNORT. 2015, de Maestros del Web http://www.maestrosdelweb.com/snort/

Álvarez Oliva, Alberto. (2013). Seguridad en Redes y Sistemas, Detección de Intrusiones con SNORT. Junio, 2015, de Universidad Oberta de Catalunya http://openaccess.uoc.edu/webapps/o2/bitstream/10609/22909/5/lalvarezoTFM0613memoria.pdf

Andrés Acosta, Leonardo Rodríguez M. (Dic. 2008). Snort Como herramienta Administrativa. Marzo, 2015, de Inventum http://biblioteca.uniminuto.edu/ojs/index.php/Inventum/article/viewFile/64/63

Chavarría, Pereira, Dávila. (2005). Delitos Informáticos 2015, de CORTE SUPREMA DE JUSTICIA NICARAGUA http://www.ictparliament.org/sites/default/files/delitosinformaticos.pdf

El Nuevo Diario. (2014). Sistemas de Prevención de Intrusos de Nueva Generación. El Nuevo Diario. http://www.elnuevodiario.com.ni/economia/332250-sistemas-prevencion-intrusos-nueva-generacion/

http://www.elnuevodiario.com.ni/economia/288521-no-hay-negocio-o-empresa-que-no-dependa-tecnologia/

http://www.snip.gob.ni/snip

Joan. (2014). Tu propio IDS con Snort y Snorby en Linux. Julio, 2015, de Joan Escorihuela http://www.joanemarti.com/tu-propio-ids-con-snort-y-snorby-en-linux-debian-7/

Jorge Mieres. (Enero 2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas. Septiembre 2016, de evilfingers Sitio web: *https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf*

José Manuel García. La ética como asignatura en los estudios de informática. Septiembre 2015, Universidad de Murcia.

Liliana Gordillo. (2008). Módulo de Seguridad Informática. Marzo, 2015, de Cybsec http://www.cybsec.com/upload/ESPE_IDS_vs_IPS.pdf

Massiell Largaespada E. (Octubre 2013). Empresas deben mejorar seguridad informática. Junio, 2015, de El Nuevo Diario http://www.elnuevodiario.com.ni/economia/300475-empresas-deben-mejorar-seguridad-informatica/

Sistema nacional de inversión pública de Nicaragua. *http://www.snip.gob.ni/snip*

T. Socolofsky, C. Kale. (1991). Tutorial de TCP/IP 2015, de Spider Systems Limited Sitio web: http://www.rfc-es.org/rfc/rfc1180-es.txt