UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE GUAYAQUIL

CARRERA DE INGENIERÍA ELECTRÓNICA

"DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS PARA SIMULACIÓN DE ADMINISTRACIÓN Y SEGURIDAD PERIMETRAL PARA REDES LOCALES Y WAN'S UTILIZANDO SOFTWARE LIBRE A TRAVÉS DE GNS3"

Trabajo de titulación previo a la obtención del

Título de INGENIERO ELECTRÓNICO

AUTOR: Alvaro Adrián Manzano Angulo

TUTOR: Ing. Diego Freire Quiroga MSc.

GUAYAQUIL – ECUADOR

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Yo, Manzano Angulo Álvaro Adrián con documento de identificación N° 0924982424 manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 19 de septiembre de 2023

Atentamente,

Manzano Angulo Álvaro
CI: 0924982424

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, Manzano Angulo Álvaro Adrián con documento de identificación Nro. 0924982424, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del proyecto de titulación: "DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS PARA SIMULACIÓN DE ADMINISTRACIÓN Y SEGURIDAD PERIMETRAL PARA REDES LOCALES Y WAN'S UTILIZANDO SOFTWARE LIBRE A TRAVÉS DE GNS3.", el cual ha sido desarrollado para optar por el título de:" INGENIERO ELECTRÓNICO", en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 19 de septiembre de 2023

Atentamente,

Manzano Angulo Álvaro
CI: 0924982424

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Diego Roberto Freire Quiroga, con documento de identificación N° 0917208084, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: "DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS PARA SIMULACIÓN DE ADMINISTRACIÓN Y SEGURIDAD PERIMETRAL PARA REDES LOCALES Y WAN'S UTILIZANDO SOFTWARE LIBRE A TRAVÉS DE GNS3", realizado por Álvaro Adrián Manzano Angulo con documento de identificación N° 0924982424 obteniendo como resultado final el trabajo de titulación bajo la opción proyecto técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 19 de septiembre de 2023

Atentamente,

Ing. Diego Roberto Freire Quiroga, MSc.
CI: 0917208084

DEDICATORIA

"Dedico este trabajo de tesis a Dios y a mi madre, quienes han sido mi constante fuente de inspiración y apoyo a lo largo de este viaje académico. Tu guía y aliento han sido fundamentales en cada paso que he dado. Gracias por creer en mí y por ser mi fuente de fortaleza. Este logro también es tuyo."

AGRADECIMIENTO

A nuestros estimados profesores, cuya experiencia y conocimientos compartidos fueron invaluablemente enriquecedores para nuestro desarrollo académico y la creación de este trabajo. Sus orientaciones críticas y valiosos consejos guiaron nuestro camino hacia la excelencia

A nuestros compañeros de estudios, cuyo intercambio de ideas y debates constructivos generaron un ambiente de aprendizaje dinámico y enriquecedor. Sus perspectivas únicas contribuyeron a moldear nuestras ideas y a fortalecer nuestras conclusiones.

A nuestras familias, quienes nos brindaron su inquebrantable apoyo emocional y logístico. Sus ánimos y comprensión durante las jornadas de estudio y trabajo, impulsando así a superar obstáculos y alcanzar este logro con éxito.

Este trabajo no hubiera sido posible sin la colaboración y respaldo de cada uno de ustedes. Extendiendo nuestro más profundo agradecimiento por ser parte fundamental en esta etapa de nuestras vidas."

RESUMEN

El contenido del trabajo se estructura en capítulos que detallan la selección de tecnologías y herramientas, así como la configuración de topologías de red específicas y la simulación de amenazas y ataques. Se ilustra cómo el banco de pruebas puede emplearse mediante casos de estudio, comprobando asi su aplicabilidad en situaciones del mundo real. El objetivo fundamental de esta investigación es abordar los desafíos actuales en la administración y seguridad de redes mediante la creación de un banco de pruebas innovador y realista, empleando herramientas de software libre disponibles en la plataforma GNS3. La elección del software libre como base se fundamenta en su accesibilidad y capacidad para ofrecer soluciones económicamente viables.

Este proyecto de titulación muestra, un estudio y análisis de seguridad perimetral concerniente a la seguridad de redes con la finalidad que los estudiantes aprendan diferentes tipos de tecnología al momento de implementar estos diversos softwares de seguridad perimetral firewall basado a código libre, se procedió con la instalación de GNS3 de manera local en las computadoras del laboratorio de flexible, se descargó el IOS de Pfsense para las prácticas donde se realizó esquema de la red, configuraciones de la reglas y niveles de seguridad del firewall.

Con la simulación del banco de prueba de seguridad perimetral se consiguieron resultados en cuanto a la seguridad de la red LAN y WAN facilitando el control y protección de los datos, bloqueo y monitoreo de ataques informáticos, administración y navegación de las páginas WEB, aplicando diversas herramientas que ofrece PFsense para proteger la red.

La utilización de software de seguridad perimetral ayuda con la disminución de costos en las empresas pequeñas y medianas con un alcance para 100 a 200 usuarios o dispositivos finales de la red, se hace mención que no hay métodos para conservar la seguridad de la red total, pero se puede realizar reglas para mantenerla lo más segura a los posibles ataques cibernéticos que vaya surgiendo a través de los tiempos con la finalidad que muestra información no se encuentre vulnerable y tenga una conexión a internet confiable donde los datos no vayan a ser expuestos.

Palabras claves: PFsense, Red LAN, Red WAN, GNS3, Firewall

ABSTRACT

In this thesis we will discuss the implementation of a test bench using free software with firewall operating system such as Pfsense for simulation and administration of perimeter security for local LAN networks and WAN wide area networks, where methods will be applied to counter different cyber-attacks for the security of users when browsing the Internet.

This degree project shows, a study and analysis of perimeter security concerning network security in order for students to learn different types of technology when implementing this various perimeter security firewall software based on open source, proceeded with the installation of GNS3 locally on the computers of the flexible laboratory, the Pfsense IOS was downloaded for practices where network schema, rule configurations and firewall security levels were performed.

With the simulation of the perimeter security test bench, results were achieved in terms of the security of the LAN and WAN network, facilitating the control and protection of data, blocking and monitoring of computer attacks, administration, and navigation of web pages, applying various tools offered by Pfsense to protect the network.

The use of perimeter security software helps with the reduction of costs in small and medium-sized companies with a scope for 100 to 200 users or end devices of the network, it is mentioned that there are no methods to preserve the security of the total network, but rules can be made to keep it as safe as possible cyber-attacks that arise over time in order to shows information that is not vulnerable and has a reliable internet connection where our data will not be exposed.

KEYBOARDS: PFsense, Red LAN, Red WAN, GNS3, Firewall

TABLA DE CONTENIDO

INDICE DE FIGURAS

INTRODUCCIÓN

La constante evolución de las tecnologías de redes y seguridad ha dado lugar a un entorno digital cada vez más complejo y dinámico. En este contexto, la administración y seguridad perimetral se han convertido en aspectos críticos para garantizar el funcionamiento óptimo y la integridad de las redes locales (LAN) y de área amplia (WAN). La simulación de estos entornos de red es esencial para comprender y abordar los desafíos que surgen en la implementación de soluciones eficaces.

En este contexto, el presente trabajo titulado "Diseño e Implementación de un Banco de Pruebas para Simulación de Administración y Seguridad Perimetral para Redes Locales y Wan's utilizando Software Libre a través de GNS3" aborda la necesidad de contar con herramientas efectivas para simular y evaluar estrategias de administración y seguridad en redes. Para abordar este objetivo, el enfoque en el uso de GNS3, una plataforma de software libre ampliamente reconocida para la emulación de redes, que permite crear entornos virtuales que replican topologías de red reales.

En esta investigación, se explorará la creación de un banco de pruebas que permita simular escenarios reales de administración y seguridad perimetral, proporcionando un entorno seguro y controlado para el desarrollo, prueba y análisis de soluciones. A lo largo de este documento, se examinará en detalle los componentes clave de este diseño, desde la selección de herramientas de software libre hasta la configuración de topologías de red que imiten situaciones del mundo real.

Los capítulos subsiguientes de este trabajo abordan los aspectos técnicos y conceptuales del diseño e implementación del banco de pruebas, incluida la selección de tecnologías y herramientas, la configuración de topologías de red específicas y la simulación de amenazas y ataques. Además, estarán presente casos de estudio que ilustran la utilidad y aplicabilidad del banco de pruebas en escenarios del mundo real.

En última instancia, este trabajo busca contribuir al campo de la administración y seguridad de redes al proporcionar una herramienta valiosa para la evaluación de estrategias de seguridad y administración, permitiendo a los profesionales de TI y estudiantes explorar y poner en práctica enfoques efectivos en un entorno virtual controlado. Se espera que este trabajo sea un recurso útil y perspicaz para aquellos interesados en mejorar la resiliencia y seguridad de las redes en un mundo cada vez más interconectado y propenso a amenazas cibernéticas.

I EL PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA

Las empresas, instituciones públicas y privadas, colegios, universidades y bancos dependen de servidores y bases de datos enfrentando riegos a ciber-ataques que pueden causar daño importante en sus sistemas de información poniendo en peligro los datos relevantes de sus sistemas a través del Internet, causando que los profesionales de las TI empiecen a diseñar soluciones de seguridad de perimetral en sus redes, implementado herramientas de monitoreo en las WAN,LAN,DMZ y administración de Proxys teniendo como efecto control a los ataques cibernético dentro y afuera de la red.

Los alumnos de la carrera de Ingeniería en Electronica con mención en Telecomunicaciones, Ingenieria en Telecomunicaciones e Ingeniería en Computación necesitan estar preparados para estos retos que se presentan en el día a día en las empresas e instituciones pudiendo implementar diversas soluciones a los problemas que se presenten en el futuro.

La Universidad Politécnica Salesiana con sede Guayaquil no cuenta con un banco de pruebas para diseñar e implementar soluciones con seguridad perimetral con software en Open Source para solventar los conocimientos técnicos donde podrán elegir las diferentes tecnologías en firewall y enrutadores en código abierto.

1.2. ANTECEDENTES

Las amenazas y vulnerabilidades que afrontan hoy en día las redes de datos y telecomunicaciones poseen un porcentaje alto, llevando a neutralizar una extensa gama de amenazas que son producidas dentro y afuera de la red identificando el tipo de ataque que se presenta garantizando la seguridad y disponibilidad de los servicios e información.

Con los conocimientos que se obtengan en el banco de pruebas de seguridad perimetral con Open Source los alumnos pueden fortalecer sus destrezas en el momento de implementación de diversos softwares de firewall de código abierto atreves de una red simulada para mejorar y prevenir los ataques dentro y afuera red, políticas de navegación, enrutamientos de las redes Wan’s, IPsec, Aplicación Control Y IPS.

Este proyecto tendrá como resultado mostrar diferentes métodos de defensas de una red, permitiendo medir los niveles de confianza en la hora de la navegación hacia el internet, el cual entregará un gran interés en el funcionamiento de una red informática.

1.3. IMPORTANCIA Y ALCANCE

Este proyecto tiene alcance tecnológico por que los estudiantes podrán implementar diversas maneras de proteger una red utilizando diferentes softwares para la implementación sea de código privado o abierto, es importante en una empresa e institución la seguridad de la información es lo primordial debe estar salvaguarda.

1.4. DELIMITACION

1.4.1. Espacial

El proyecto de titulación para la obtención del título de “Ingeniero Electrónico”, fue realizado en la Universidad Politécnica Salesiana sede Guayaquil en el laboratorio de flexible.

1.4.2. Académica

Enfocado a las materias de redes, como Redes de Computadoras I, Redes de Computadoras II y Redes de Comunicaciones.

1.4.3. Temporal

El proyecto se desarrolló en los meses de mayo 2023 a agosto del 2023

1.5. OBJETIVOS

1.5.1. OBJETIVO GENERAL

Diseñar e implementar un banco de pruebas para simulación de administración y seguridad perimetral para redes locales y WAN'S utilizando software libre a través de GNS3."

1.5.2. OBJETIVOS ESPECÍFICOS

- Comparar los diferentes tipos de software Open Source para seguridad perimetral.
- Utilizar protocolos de enrutamiento para simular los enlaces WAN y redes locales.
- Diseñar e implementar diez prácticas con diversos métodos de administración y seguridad informática que serán emuladas en máquinas virtuales para ser utilizadas en GNS3.

II MARCO TEÓRICO

2.1. SEGURIDAD INFORMÁTICA

La seguridad informática incluye asegurar que los recursos de los sistemas de información de su organización se utilicen de una manera determinada y que sólo las personas autorizadas y dentro de sus límites tengan acceso a la información contenida en los mismos, así como autorización para modificarla: ejemplificando. A continuación de mejor manera con la siguiente imagen.

Ilustración 1. Robo de información
(Jesús Costas Santos, 2011)

2.2. PRINCIPIOS DE SEGURIDAD INFORMÁTICA

Si bien la mayoría de los expertos están de acuerdo en que ningún sistema es completamente seguro y 100 % libre de errores, debe tratar de proteger la información y los sistemas que la usan para brindarles a los usuarios un nivel razonable de seguridad, de modo que para que un sistema se considere razonablemente seguro, se debe garantizar el cumplimiento Fundamentos de Seguridad Informática: integridad, confidencialidad y disponibilidad (Gema, 2013).

Integridad. - Este es un principio fundamental de la seguridad informática, incluida la garantía de que la información solo puede ser modificada por personal autorizado o usuarios legítimos. Las violaciones de integridad tienen diferentes significados dependiendo de si ocurren en una computadora o en una red de comunicación.

- **Equipo de trabajo.** Se produce a la violación de la integridad cuando un usuario no legitimo modifica la información del sistema sin tener autorización para ello.

- **Red de comunicación.** Existe violación de la integridad cuando un atacante actúa como intermediario en una comunicación, recibe los datos enviados por un usuario, los modifica y se los envía al receptor (ataques man-in-the-middle.). A continuación, una imagen ilustrativa.

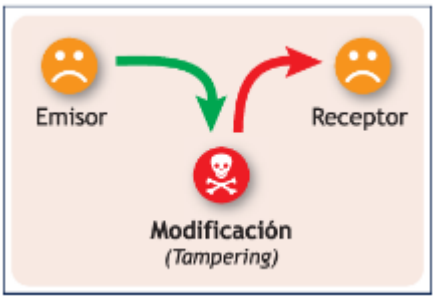


Ilustración 2. Violación de Integridad
(Gema Escrivá, 2013)

Confidencialidad. – Este es otro principio fundamental de la seguridad informática, que garantiza que la información sólo pueda ser accedida e interpretada por personas o sistemas autorizado (Gema, 2013).

La vulneración de la confidencialidad también afecta de forma diferente a equipos y redes:

- **Equipo de trabajo.** Se produce a una violación de la confidencialidad cuando un atacante consigue acceso a un equipo sin autorización, controlando sus recursos.

- **Red de comunicación.** Se vulnera la confidencialidad de una red cuando un atacante accede a los mensajes que circulan por ella sin tener autorización, existen mecanismo que permiten protegerse frente este tipo de ataques como el cifrado de la información o el uso de protocolos de comunicación, de mejor manera. A continuación, una imagen como ejemplo.

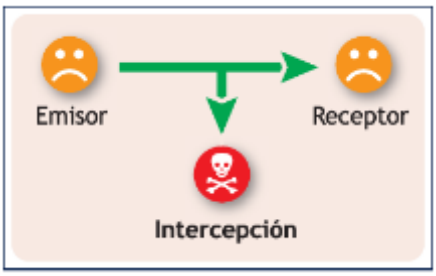


Ilustración 3. Violación de Confidencialidad
(Gema Escrivá, 2013)

Disponibilidad. - Es el tercer pilar básico de un sistema seguro es la disponibilidad, esto es, asegurar que la información es accesible en el momento adecuado para los usuarios legítimos (Gema, 2013).

La violación de la disponibilidad también se da de forma distinta en equipos y redes:

- **Equipos informáticos.** Se vulnera la disponibilidad de un equipo cuando los usuarios que tienen acceso a él no pueden utilizarlo. Por ejemplo, podría ser un virus que ha paralizado el sistema.

- **Redes de comunicación.** Se produce un ataque contra la disponibilidad cuando se consigue que un recurso deje de estar disponible para otros usuarios que acceden a él a través de la red. Existen una gran variedad de ataques que atentan contra la disponibilidad de un recurso en una red, como los ataques de denegación de servicios.

Estos ataques, así como las técnicas que se podrán utilizar para proteger las redes. A continuación, una imagen.

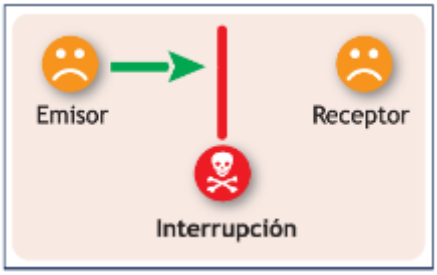


Ilustración 4. Violación de Disponibilidad
(Gema Escrivá, 2013)

2.3. SEGURIDAD FÍSICA

La seguridad física adquiere una importancia vital a la hora de preservar tanto los datos que poseen las empresas, como los equipos y dispositivos encargados de su tratamiento y almacenamiento, por tanto, definir la seguridad física como el conjunto de medidas de prevención y detección destinadas a evitar los daños físicos a los sistemas informáticos y proteger los datos almacenados en ellos (Gema, 2013).

2.4. SEGURIDAD LÓGICA

La seguridad lógica es el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como a garantizar el acceso a la información únicamente por las personas autorizadas (Gema, 2013).

Políticas de seguridad corporativa

La primera medida de seguridad lógica que debe adoptar una empresa es establecer unas normas claras en las que se indique qué se puede y qué no se puede hacer al operar con un sistema informático. El conjunto de normas que definen las medidas de seguridad y los protocolos de actuación a seguir en la operativa del sistema reciben el nombre de políticas de seguridad corporativa en materia informática.

.

Entre las políticas de seguridad relacionadas con la seguridad informática se tendrian las siguientes:

- Instalación, mantenimiento y actualización de los equipos.
- Control de acceso a áreas críticas de la empresa y a recursos críticos del sistema.
- Mantenimiento de las redes
- Autenticación de usuarios.
- Contraseñas.
- Privacidad de la información.
- Utilización de recursos de las redes informáticas.

Políticas de seguridad en materia de contraseñas

Para evitar que las amenazas descritas en el apartado anterior sean efectivas y evitar que usuarios maliciosos accedan a los datos de un sistema informático, los usuarios y las empresas deben establecer políticas de seguridad en materia de contraseñas (Gema, 2013).

Con el fin de evitar que las amenazas expuestas en el apartado anterior sean efectivas y que un usuario malintencionado pueda acceder a los datos de un sistema informático, es esencial que los usuarios y empresas establezcan unas políticas de seguridad relativas a las contraseñas.

Establecimiento de las contraseñas

Las contraseñas deben elegirse en función de su idoneidad para proteger la información, no en función de su facilidad para ser recordadas por el usuario. Como se adelantó en la página anterior, una adecuada política de seguridad prestará atención en fijar unas normas para la elección de contraseñas que dificulten los ataques por diccionario o por fuerza bruta. Para ello, las normas básicas son las siguientes (Gema, 2013):

- No deben ser o contener palabras usuales ni relacionadas con el entorno del usuario, como, por ejemplo: nombres de mascotas, fechas de cumpleaños, número del DNI, etc.
- No deben ser palabras con significado, por ejemplo, alimento. La contraseña debería ser una combinación de mayúsculas, minúsculas, números y otros caracteres, por ejemplo: aX4t$5#.
- La longitud de la contraseña debería ser de ocho caracteres como mínimo.
- Hay que evitar que el usuario utilice la misma contraseña en varios sitios, por ejemplo, que se utilice la misma contraseña para entrar a las aplicaciones de la empresa, al correo y a redes sociales.
- Se deben cambiar las contraseñas proporcionadas por defecto al registrarse por Internet en cualquier servicio. A continuación, una imagen ilustrando la explicación:

Ilustración 5. Contraseñas
(Gema Escrivá, 2013)

2.5. SEGURIDAD EN REDES

Las telecomunicaciones permiten que una persona juegue en línea con otra persona en el otro lado del mundo, use su teléfono móvil para navegar en Internet e incluso administre su hogar a través de aplicaciones de domótica. Todo gracias a la comunicación en red (Gema, 2013).

Ya sea por cable o inalámbrica, las redes informáticas se están volviendo cada vez más importantes para las actividades cotidianas. Las personas y las organizaciones confían en sus computadoras y redes para funciones como el correo electrónico, la contabilidad, la organización y la gestión de documentos. La intrusión personal no autorizada puede resultar en cortes de red costosos y pérdida de empleos. Los ataques a las redes pueden ser devastadores y pueden resultar en pérdida de tiempo y dinero debido al daño o robo de información o activos vitales (Jesús, 2015).

Por lo general, a los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se los denomina piratas informáticos.

Una vez que el pirata informático obtiene acceso a la red, pueden surgir cuatro tipos de amenazas:

- Robo de información.
- Robo de identidad.
- Perdida y manipulación de datos.
- Interrupción del servicio.

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa.

- **Amenazas externas:** las amenazas externas provienen de personas que trabajan fuera de una organización. Estas personas no tienen autorización para acceder al sistema o a la red de la computadora.
- **Amenazas internas:** las amenazas internas se originan cuando una persona cuenta con acceso autorizado a la red a través de una cuenta de usuario o tiene acceso físico al equipo de la red.

Para un intruso, una de las formas más fáciles de obtener acceso, ya sea interno o externo, es el aprovechamiento de las conductas humanas. Uno de los métodos más comunes de explotación de las debilidades humanas se denomina ingeniería social.

Ingeniería social: ingeniería social es un término que hace referencia a la capacidad de algo o alguien para influenciar la conducta de un grupo de personas. En el contexto de la seguridad de computadoras y redes, la ingeniería social hace referencia a una serie de técnicas utilizadas para engañar a los usuarios internos a fin de que realicen acciones específicas o revelen información confidencial. A continuación, una imagen:

Ilustración 6. Ingeniería Social
(Sánchez Rubio, 2015)

Con la evolución de los tipos de amenazas, ataques y explotaciones, se han acuñado varios términos para describir a las personas involucradas. Estos son algunos de los términos más comunes:

- **Hacker:** es un término general que se ha utilizado históricamente para describir a un experto en programación. Recientemente, este término se ha utilizado con frecuencia con un sentido negativo, para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa (Jesús, 2015).

- **Hacker de sombrero blanco:** una persona que busca vulnerabilidades en los sistemas o en las redes y, a continuación, informa estas vulnerabilidades a los propietarios del sistema para que las arreglen. Son éticamente opuestos al abuso de los sistemas informáticos. Por lo general, un hacker de sombrero blanco se concentra en proporcionar seguridad a los sistemas informáticos, mientras que a un hacker de sombrero negro (el opuesto) le gustaría entrar por la fuerza en ellos. La imagen siguiente ilustrará la explicación.

Ilustración 7. Hacker sombrero blanco
(Sánchez Rubio)

- **Hacker de sombrero negro:** otro término que se aplica a las personas que utilizan su conocimiento de las redes o los sistemas informáticos que no están autorizados a utilizar, generalmente para beneficio personal o económico. Un cracker es un ejemplo de hacker de sombrero negro. Encontrará una imagen ilustrativa.

Ilustración 8. Hacker sombrero negro
(Sánchez Rubio)

- **Cracker:** es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa, se imaginará mejor la explicación con la siguiente imagen.

Ilustración 9. Cracker
(Sánchez Rubio, 2015)

- **Phreaker:** una persona que manipula la red telefónica para que realice una función que no está permitida. Un objetivo común del phreaking es ingresar en la red telefónica, por lo general a través de un teléfono público, para realizar llamadas de larga distancia gratuitas .Una imagen ilustrativa a continuación:

Ilustración 10. Phreaker
(Sánchez Rubio, 2015)

- **Spammer:** persona que envía grandes cantidades de mensajes de correo electrónico no solicitado. Por lo general, los spammers utilizan virus para tomar control de computadoras domésticas y utilizarlas para enviar sus mensajes masivos.
- **Estafador:** utiliza el correo electrónico u otro medio para engañar a otras personas para que brinden información confidencial, como números de tarjetas de crédito o contraseñas. Un estafador se hace pasar por una persona de confianza que tendría una necesidad legítima de obtener información confidencial.

Hay diversos tipos de ataques informáticos en redes. Algunos son:

- **Ataque de denegación de servicio**, también llamado ataque DoS (Deny of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, normalmente provocando la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. A continuación, una imagen ilustrativa.

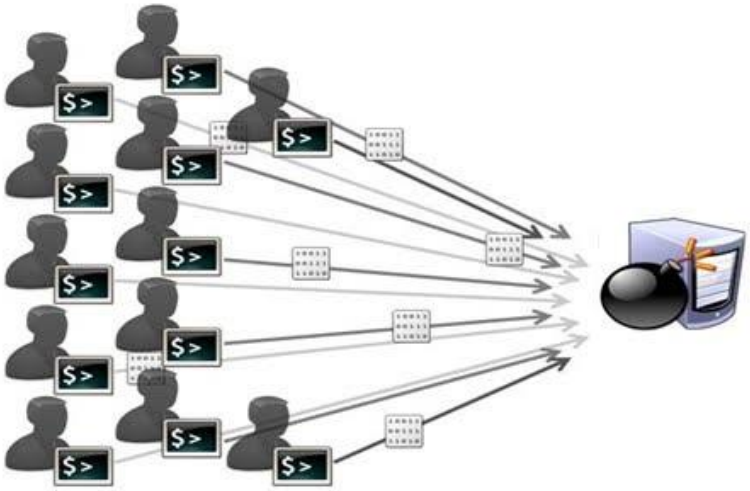


Ilustración 11. Ataque de denegación de servicio
(Sánchez Rubio, 2015)

- **Man in the middle**, a veces abreviado MitM, es una situación donde un atacante supervisa (generalmente mediante un rastreador de puertos) una comunicación entre dos partes y falsifica los intercambios para hacerse pasar por una de ellas, de mejor manera a continuación una imagen como ejemplo:

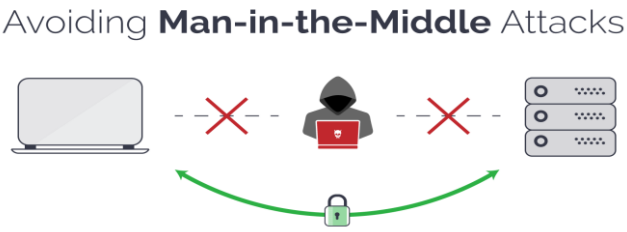


Ilustración 12. Man in the middle attack
(Sánchez Rubio, 2015)

- **Ataques de REPLAY**, una forma de ataque de red, en el cual una transmisión de datos válida es maliciosa o fraudulentamente repetida o retardada. Es llevada a cabo por el autor o por un adversario que intercepta la información y la retransmite, posiblemente como parte de un ataque enmascarado.

2.6. TÉCNICAS DE PROTECCIÓN

En una red de ordenadores en la que varios equipos comparten información, se comunican entre sí y ac- ceden a otras redes o a Internet, el impacto producido por un ataque sobre la red es más grave que el producido sobre un equipo, por lo que conviene establecer medidas específicas que protejan a los usuarios de la red (Gema, 2013).

Entre las técnicas de protección más utilizadas en redes se destaca los cortafuegos, sistemas de detección de intrusos, proxies, sistemas de gestión unificada de amenazas, VPN, sistemas centralizados de autenticación y zonas desmilitarizadas. Algunas ya se han estudiado en unidades anteriores, como los firewalls, por lo que se centrará en cómo utilizarlas en redes, mientras que otras técnicas son nuevas y conviene conocerlas (Gema, 2013).

2.6.1. CORTAFUEGOS

En una red de ordenadores, el cortafuegos se ubica en el límite de la red para poder analizar todo el tráfico que entra o sale de la misma. En algunas redes, algunos dispositivos de red (routers) hacen las funciones de firewall, mientras que en otras existe un equipo que dispone de dos tarjetas de red y analiza todo el tráfico (Gema, 2013).

Un cortafuego permite o deniega el tráfico en función de parámetros de- finidos en reglas. Si se cumplen las condiciones establecidas en una regla se aplicará la misma, aceptando o rechazando el paquete, y dejará de comprobarse el resto. Cuando no existe ninguna regla que coincida con las características del paquete recibido se aplicará la política por defecto para el paquete que entra al sistema o sale de él. Ejemplificando a continuación de mejor manera con la siguiente imagen.

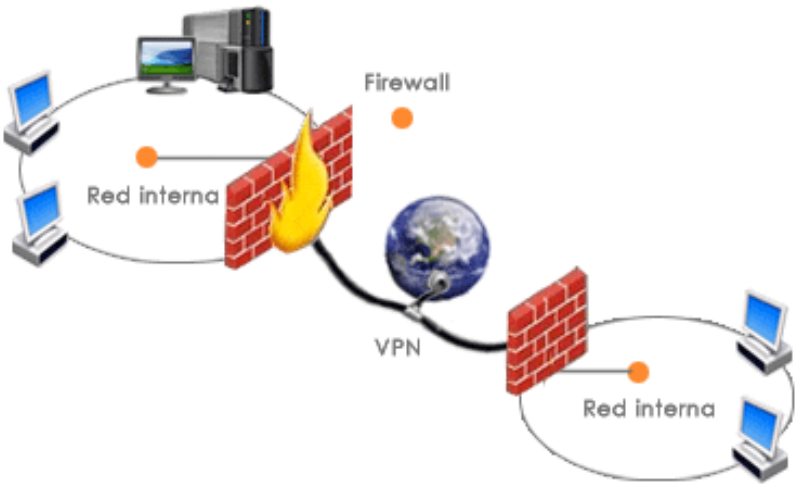


Ilustración 13. Cortafuegos
(Gema Escrivá, 2013)

- **Política restrictiva**, donde se rechaza todo el tráfico por defecto y solo se permite el paso de los paquetes aceptados de forma explícita.

- **Política permisiva**, en la que se acepta todo el tráfico, excepto aquellos paquetes especificados en las reglas, que serán rechazados.

2.6.2. ZONAS DESMILITARIZADAS

Una zona desmilitarizada o DMZ (DeMilitarized Zone, en inglés) es una red que suele albergar servidores que ofrecen algún servicio en Internet y que, generalmente, actúa como intermediaria entre la red interna de una empresa y la red externa, incrementando la seguridad de las redes internas.

La red interna y la externa pueden establecer conexiones con la DMZ, pero desde la DMZ solo se permite establecer conexiones con la red externa, denegando conexiones de entrada a la red interna.

De esta forma, los equipos de la DMZ pueden iniciar conexiones con equipos externos de forma legítima como, por ejemplo, el servidor de antivirus corporativo que se descarga regularmente las firmas y actualizaciones de los virus.

Es importante remarcar que no se permiten conexiones desde la DMZ a la red interna porque se trata de una red con un nivel de seguridad relativamente bajo, con lo que podría darse el caso de que un atacante controlase alguno de los servidores que hay dentro de la DMZ y tratase de establecer conexiones con los equipos de la red. De mejor manera a continuación una imagen como ejemplo:

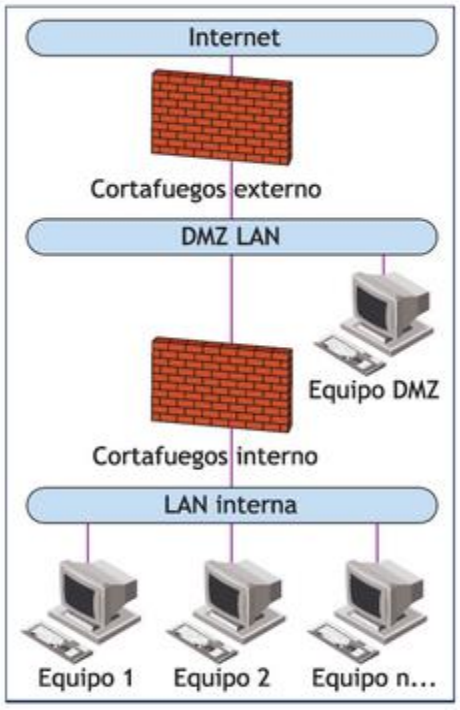


Ilustración 14. Esquema DMZ
(Gema Escrivá, 2013)

2.6.3. DETECCIÓN DE INTRUSOS

Este tipo de sistemas está formado por un dispositivo o software que monitoriza, alerta y/o elimina ataques a la red o a los equipos informáticos. Dentro de este tipo de técnicas distinguimos entre sistemas detectores de intrusos y sistemas de prevención de intrusos (Gema, 2013):

Sistemas detectores de intrusos, o IDS (Intrusion Detection System, en inglés), son un elemento pasivo que detecta ataques, pero no los elimina. Distinguimos tres tipos de IDS:

- HIDS (Host IDS), que monitoriza y protege un equipo.
- NIDS (Network IDS), que monitoriza y protege una red.

- DIDS (Distributed IDS), donde se dispone de NIDS distribuidos y gestionados por una consola.

Sistemas de prevención de intrusos o IPS (Intrusion Prevention System, en inglés), son un elemento activo que trata de neutralizar el ataque, adaptándose a él. Suelen estar formados por un IDS y un cortafuegos que modifica sus reglas dinámicamente para evitar accesos no autoriza- dos a la red (Gema, 2013).

2.6.4. PROXIES

Un proxy o intermediario de red es un servicio, normalmente instalado en un servidor o dispositivo dedicado, que realiza la función de intermediario entre él y los clientes que solicitan un determinado servicio, como por ejemplo HTTP. Un proxy web por tanto es un dispositivo que trabaja en el nivel de aplicación de OSI (Gema, 2013).

El uso más habitual de un servidor proxy es permitir el acceso a Internet a los equipos de una organización cuando solo se puede disponer de un único equipo conectado, que es el propio proxy. Este permite a los clientes conectarse a una red (generalmente Internet) de forma indirecta a través de él, proporcionando de esta forma una capa adicional de seguridad.

Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado de la petición al cliente.

Algunas de las ventajas de usar un proxy son las siguientes:

- La navegación puede ser más rápida si se usa la caché y esta es suficientemente grande.
- Proporciona seguridad al proteger a los equipos cliente de la red externa.
- Posibilita definir filtros de contenidos y listas de control de acceso para permitir a las organizaciones realizar un control del servicio que se está usando. De mejor manera a continuación una imagen como ejemplo:

Ilustración 15. Software Squid Proxy
(Gema Escrivá, 2013)

2.6.5. GESTIÓN UNIFICADAS DE AMENAZAS (UTM)

Los dispositivos conocidos como UTM (Unified Threat Management, en inglés) o gestión unificada de amenazas, combinan distintas técnicas de protección de redes como cortafuegos, antivirus, antispam, filtro de contenidos, detección y prevención de intrusos redes privadas virtuales y servidor proxy, todo ello en un único aparato (Gema, 2013).

Son la tendencia actual, sobre todo en pequeñas empresas, donde el ahorro de costes es crítico y no es posible invertir mucho dinero en soluciones de seguridad de varios.

No obstante, hay que tener en cuenta que el hecho de que todos los sistemas de protección estén integrados en un solo dispositivo puede pre- sentar problemas de rendimiento, escalabilidad y disponibilidad. Por ejemplo, un fallo completo en el dispositivo implica un fallo en todos los sistemas de protección de la red. Detallamos con una imagen esta explicación.

Ilustración 16. UTM SOPHOS
(Sophos, 2013)

2.7. REDES INFORMÁTICAS

Una red de comunicación es un sistema que permite la comunicación entre los ordenadores que se encuentran conectados a ella. La red está formada por los siguientes elementos: los

terminales (ordenadores), el medio de transmisión, los elementos de interconexión, los adaptadores de comunicación y los protocolos que funcionan en ellos (José, 2015).

Una red de comunicación ofrece una serie de servicios, es decir, pone a disposición de los usuarios un conjunto de funciones que pueden utilizar. Así mismo, esos servicios se basan en una serie de protocolos, que son las normas que se deben seguir para que las comunicaciones se realicen correctamente.

Todas las redes de comunicación se clasifican atendiendo al territorio que abarcan: redes locales (limitadas a uno o varios edificios), redes de área metropolitana (limitadas a una ciudad) y redes de área extensa (que abarcan territorios extensos como estados, continentes o incluso todo el planeta). Detallamos con una imagen esta explicación.

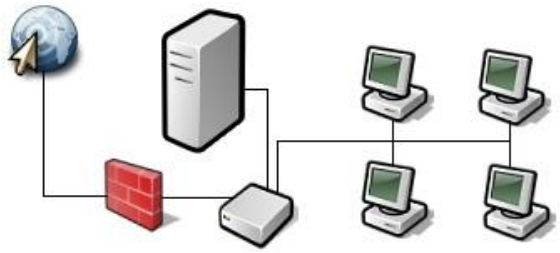


Ilustración 17. Red informática
(Cisco, 2010)

2.7.1. REDES DE ÁREA LOCAL

Una red de área local (LAN, Local Área Network), es un conjunto de elementos físicos y lógicos que proporcionan interconexión entre dispositivos en un área privada y restringida. La red de área local tiene entre otras, las siguientes características (Domingo, 2013):

- Una restricción geográfica: el ámbito de una oficina, de la planta de un edificio y depende de la tecnología con que esté construida.
- La velocidad de transmisión debe ser relativamente elevada.
- La red de área debe ser privada, toda la red debe pertenecer a la misma organización.
- Fiabilidad en las transmisiones, la tasa de error en una red de área local debe ser baja. Imagen ilustrativa como referencia, a continuación.

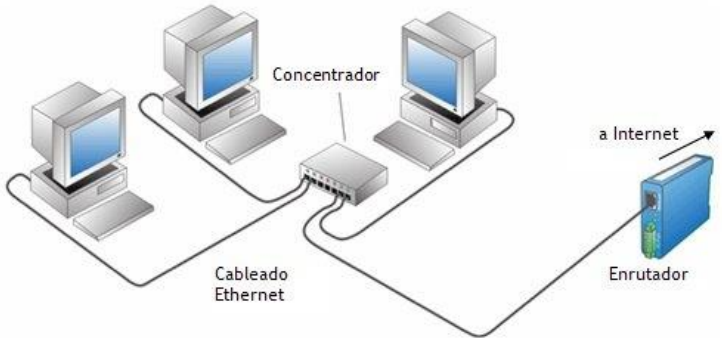


Ilustración 18. Red de área local (LAN)
(CISCO, 2014)

2.7.2. REDES DE ÁREA EXTENSA

Una red de área extensa o extendida (WAN, Wide Área Network) es una red que intercomunica equipos en un área geográfica muy amplia.

Las transmisiones en una WAN se realizan a través de líneas públicas. La capacidad de transmisión de estas líneas suele ser menor que las utilizadas en las redes de área local. Además, son compartidas por muchos usuarios a la vez, lo que exige un acuerdo en los modos de transmisión y en las normas de interconexión a la red (Domingo, 2013).

Las tasas de error en las transmisiones en las redes de área extensas son mayores unas mil veces superior que su equivalente en las redes de área local.

Las posibilidades de las redes de área extendidas son enormes: distintos tipos de redes de área local que interconectan, equipamientos de diversos fabricantes, multitud de protocolos de comunicación, posibilidad de diferentes líneas de transmisión. Imagen ilustrativa como referencia.

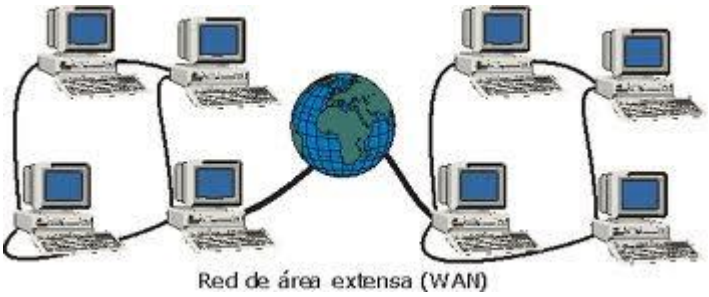


Ilustración 19. Red de área extensa (WAN)
(CISCO, 2014)

2.7.3. REDES DE ÁREA METROPOLITANAS, REDES DE ÁREA PERSONAL Y REDES INALÁMBRICAS

Los siguientes epígrafes se dedicarán a explicar brevemente las características de otras redes: las redes metropolitanas (MAN), redes de área personal (PAN) y las redes de área local inalámbricas (WLAN).

– **Redes metropolitanas**

Una red metropolitana es una red de distribución de datos para un área geográfica en el entorno de una ciudad. Este tipo de redes es apropiado, por ejemplo, para la distribución de televisión por cable en el ámbito de la población sobre lo que se entiende geográficamente la red. Imagen ilustrativa como referencia.

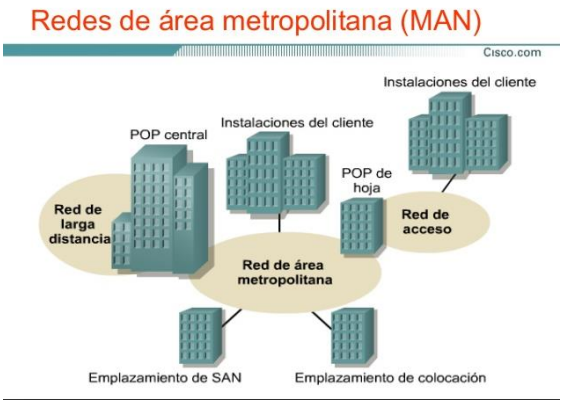


Ilustración 20. Red de área metropolitana (MAN)
(goconqr, 2012)

– **Redes de área personal**

Las redes PAN tienen algunas características que las hacen peculiar. A continuación se mencionan aquí algunas de ellas:

– Configuración de acceso a la red debe ser muy sencilla o incluso automática.

– Trasmisión por excelencia.
– El radio de acción de la red debe ser geográficamente muy limitado. Una imagen ilustrativa como referencia.

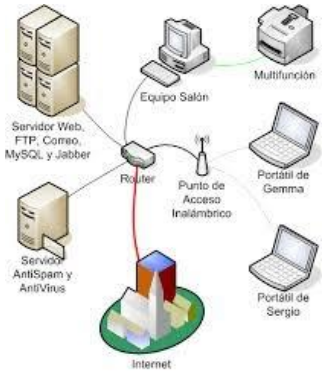


Ilustración 21. Red PAN
(CISCO, 2014)

– **Redes de inalámbricas**

Es una red sin cables junto con el descenso significativo de los costes de fabricación ha redundado en un importante auge de las comunicaciones telemáticas inalámbricas. Imagen ilustrativa como referencia, a continuación.

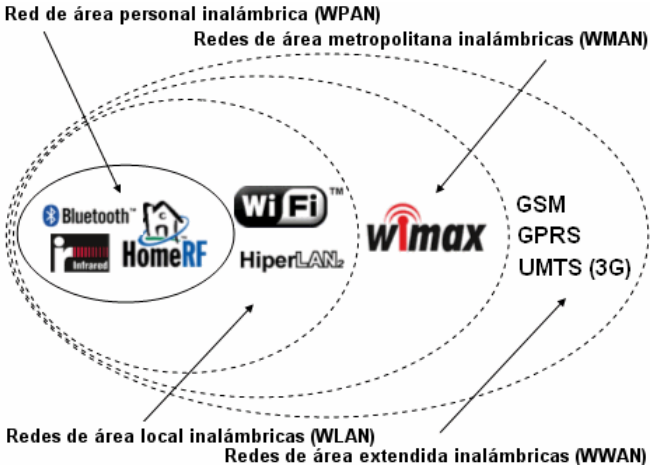


Ilustración 22. Red inalámbrica
(CISCO, 2014)

2.8. GNS3

Es un simulador de red redes que permite diseñar redes y correr simulaciones sobre las topologías creadas. Es de carácter gratuito y es parte de la empresa GNS3 Tecnologies.

Cuenta con una gran cantidad de usuarios, y es compatible con la mayoría de binarios de los equipos del mercado, como por ejemplo con los ISO de la empresa Cisco, de tal forma que se podria simular sus routers, switches y firewall dentro de la red. Imagen ilustrativa como referencia.

Ilustración 23. GNS3 LOGO
(GNS3, 2015)

2.8.1. REQUISITOS MINIMOS

Los siguientes son los requisitos mínimos para un entorno Windows en GNS3. A continuación, un cuadro ilustrativo.

Ítem	Requerimientos mínimos
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	2 o más núcleos lógicos
Virtualización	Se requieren extensión de virtualización. Es posible que se deba esto a través del BIOS de la computadora.
Memoria	4GB RAM
Espacio en disco	1GB de espacio disponible

Tabla 1. Requisitos Mínimos para GNS3
(Rosero, 2020)

2.8.2. REQUISITOS RECOMENDADOS

Los siguientes son los requisitos recomendados para un entorno Windows en GNS3. A continuación, un cuadro ilustrativo:

Ítem	Requerimientos mínimos
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	4 o más núcleos lógicos – AMD-V / RVI Series o Intel VT-X / EPT
Virtualización	Se requieren extensión de virtualización. Es posible que se deba esto a través del BIOS de la computadora.
Memoria	16GB RAM
Espacio en disco	Disco de Estado Sólido (SSD) 35GB de espacio disponible

Tabla 2. Requisitos Requerido para GNS3
(Rosero, 2020)

2.9. PFSENSE

Es un software de código abierto cuyas principales funcionalidades son actuar como router y firewall. Está basado en FreeBSD y por ello se puede instalar en gran cantidad de servidores y equipos. Cuenta con una interfaz WEB para configurar y monitorizar la red y las normas del firewall, a través de la cual se puede administrar todo el sistema (Álvaro, 2017)

Pfsense es una aplicación que se instala como un sistema operativo ya que tiene varias funcionalidades entre estos servicios de redes LAN y WAN, con detalle estos servicios son los siguientes:

- Firewall: Pfsense se puede configurar como un cortafuego permitiendo y denegando determinado tráfico de redes tanto entrante como saliente a partir de una dirección ya sea de red o de host de origen y de destino, también haciendo filtrado avanzado de paquetes por protocolo y puerto.

- Servidor VPN: Pfsense puede configurar como un servidor VPN usando protocolos de tunneling tales como IPSec, PPTP, entre otras

- Servidor de Balanceo de Carga: Pfsense puede ser configurado como servidor de balanceo de carga tanto entrante como saliente, esta característica es usada comúnmente en servidores web, de correo, de DNS.

- Portal Cautivo: Este servicio consiste en forzar la autenticación de usuarios en una página web especial de autenticación, para aceptar los términos de uso o para poder tener acceso a la red.

- Servidor DNS y reenviador de cache DNS: Pfsense se puede configurar como un servidor DNS primario y reenviador de consultas de DNS.

- Servidor DHCP: También funciona como servidor de DHCP, se puede también implementar VLAN desde Pfsense.

- Enrutamiento estático: Pfsense funciona como un enrutador ya que entrega direccionamiento IP y hace el nateo hacia afuera.

- Reportes Y Monitoreo: A través de los gráficos RDD Pfsense muestra el estado de los siguientes componentes: Utilización de CPU y rendimiento total, estado del Firewall, rendimiento individual por cada interfaz, paquetes enviados y recibidos por cada interfaz, manejo de tráfico y ancho de banda.

Por otra parte, establecen que para la instalación de Pfsense los requerimientos de hardware son los siguientes (Delgado Zambrano & Loor Loor, 2017).

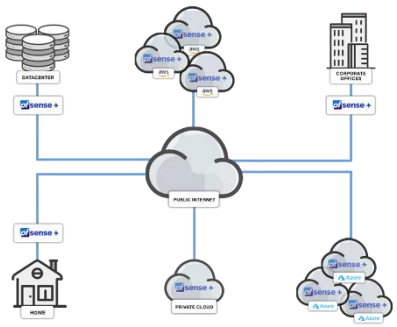
- Procesador Intel Pentium III, hasta un Intel Xeon, nada de AMD.

- Memoria RAM desde 256 Mb hasta 3 Gb.

- Disco Duro de 2 Gb hasta 80 Gb, IDE, SCSI, SATA Y SAS-SATA.

- Tarjetas de red cableadas Intel y Realtek (la red inalámbrica solamente funcionan las tarjetas de red marca Atheros).

Imagen ilustrativa como referencia, a continuación.



lustración 24. PfSense
(Pfsense, 2015)

III DISEÑO E IMPLEMENTACIÓN DEL BANCO DE PRUEBAS

3.1. FINALIDAD DEL DISEÑO

La intención del diseño e implementación del banco de pruebas es que los estudiantes conozcan de las diversas formas de asegurar una red de informática o de telecomunicaciones de los ataques de los hackers utilizando software libre.

En este tema esta centralizado para la administración control de red en tiempo real a través de simulaciones que se pueden implementar en la vida real en un empresa, universidad o colegio sin la necesidad de comprar equipos físicos de seguridad en estos tiempos las empresas que elaboran software dan los ISOS de forma gratuitamente a que los estudiantes e ingenieros pueden desarrollar habilidades en el momento que dar una solución.

El banco de prueba se implementó para proveer la simulación a las computadoras que se encuentran en el laboratorio de comunicaciones ópticas además los estudiantes pueden llevar sus laptops para realizar estas prácticas, los softwares que se utilizaran son de código abierto no se requiere ningún tipo de licencia

La siguiente figura describe la topología de red y las conexiones de comunicación del banco de pruebas:

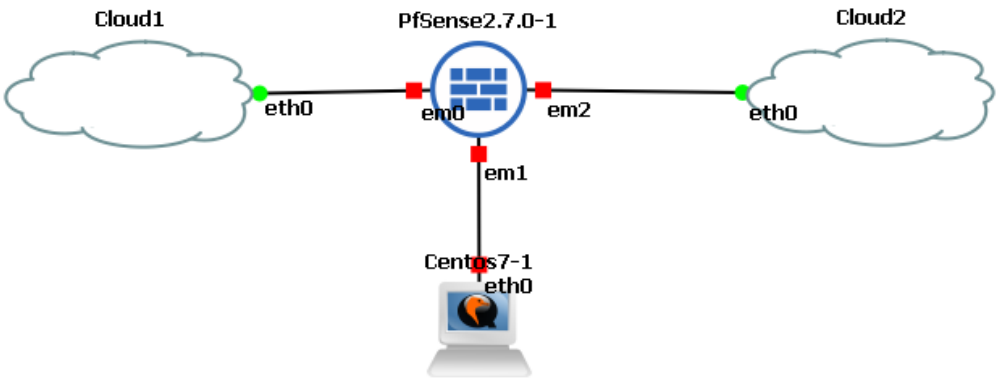


Ilustración 25. Diagrama del banco de pruebas
(Jesús Costas Santos, 2011)

3.2. ELABORACIÓN DEL BANCO DE PRUEBAS

Para la implementación y desarrollo del banco de pruebas se realizó en los siguientes pasos:

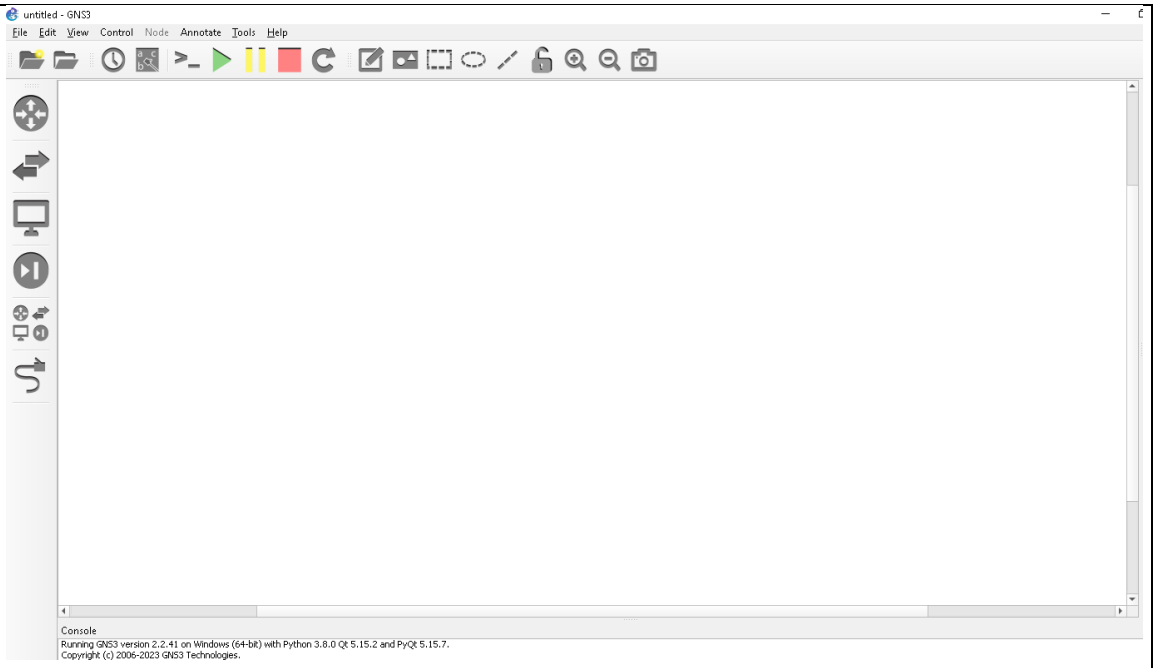
- Instalación de GNS3
- Instalación de la máquina virtual de VM-GNS3 mediante VMware.
- Configuración de GNS3 con la máquina virtual VM-GNS3
- Instalación de Pfsense en GNS3
- Instalación de OPNSense en GNS3
- Instalación de Mozilla Firefox en GNS3
- Instalación de Centos7 en GNS3
- Instalación de Ubuntu en GNS3

Para cada práctica se usará uno o varios elementos antes mencionados para poder profundizar en cada concepto necesario para profundizar en los conocimientos de administración y seguridad para redes LAN y WAN.

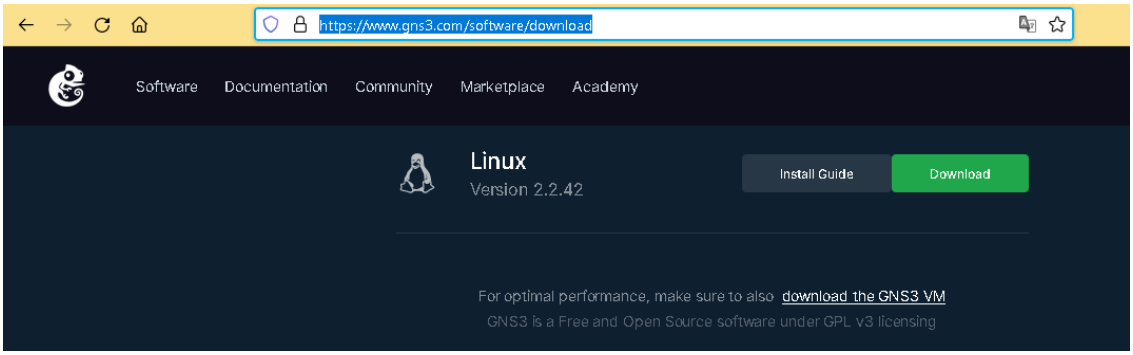
IV PRÁCTICAS DEL BANCO DE PRUEBAS

4.1. PRÁCTICA # 1

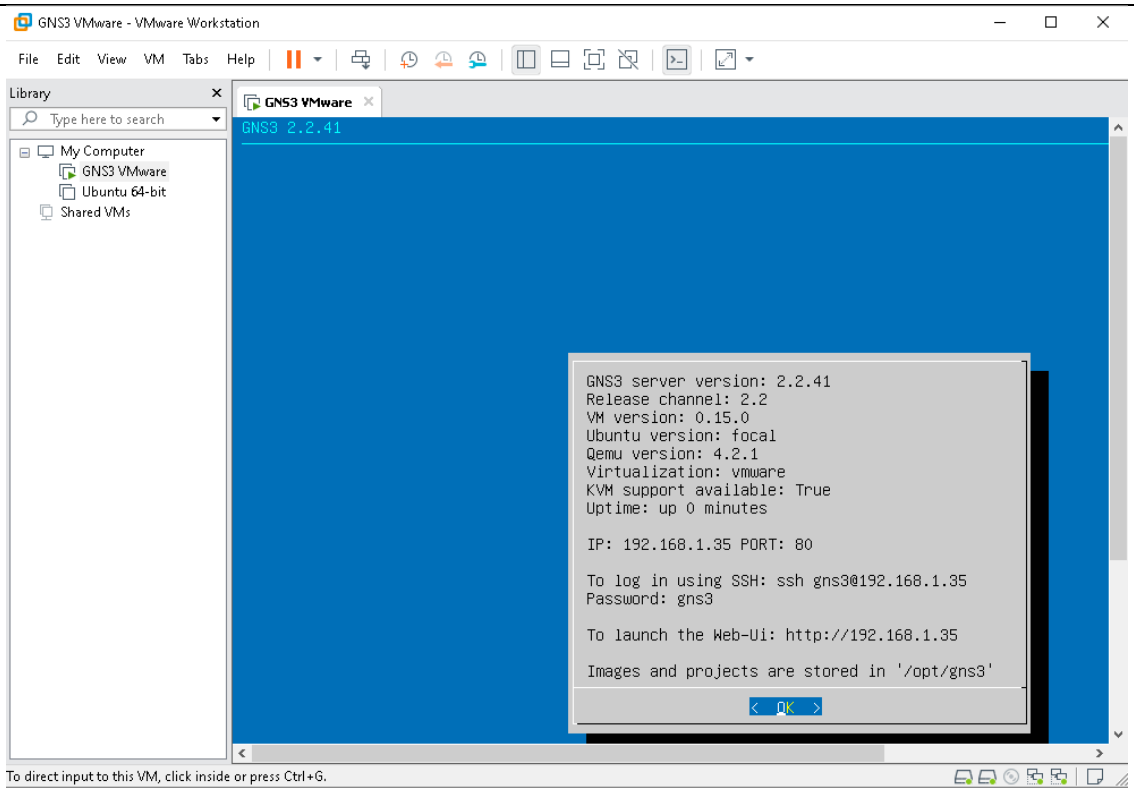
<table>
<tr><td colspan="2"> 
FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>Carrera: Ingeniería Electrónica</td><td>Asignatura: Redes de Computadoras</td></tr>
<tr><td>NRO. Práctica: 1</td><td>Título Práctica:
Configuración ambiente de GNS3 para el banco de pruebas.</td></tr>
<tr><td colspan="2">OBJETIVO:
• Objetivo General
Configurar el ambiente de prueba de GNS3 para banco de pruebas de seguridad y administración de redes LAN y WAN.</td></tr>
<tr><td>INSTRUCCIONES:</td><td>1. Cargar las imágenes de los diferentes softwares para que estén disponibles para el desarrollo de las prácticas.
2. Subir al AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta de la práctica realizada en clase.</td></tr>
<tr><td colspan="2">ACTIVIDADES POR DESARROLLAR</td></tr>
<tr><td colspan="2">1. Instalar GNS3 en los computadores o laptops. Bajar los instaladores desde: https://www.gns3.com/software/download puede ser para Linux como para Windows, la instalacion es sencilla, todo debe de ser siguiente y finalizar.</td></tr>
</table>



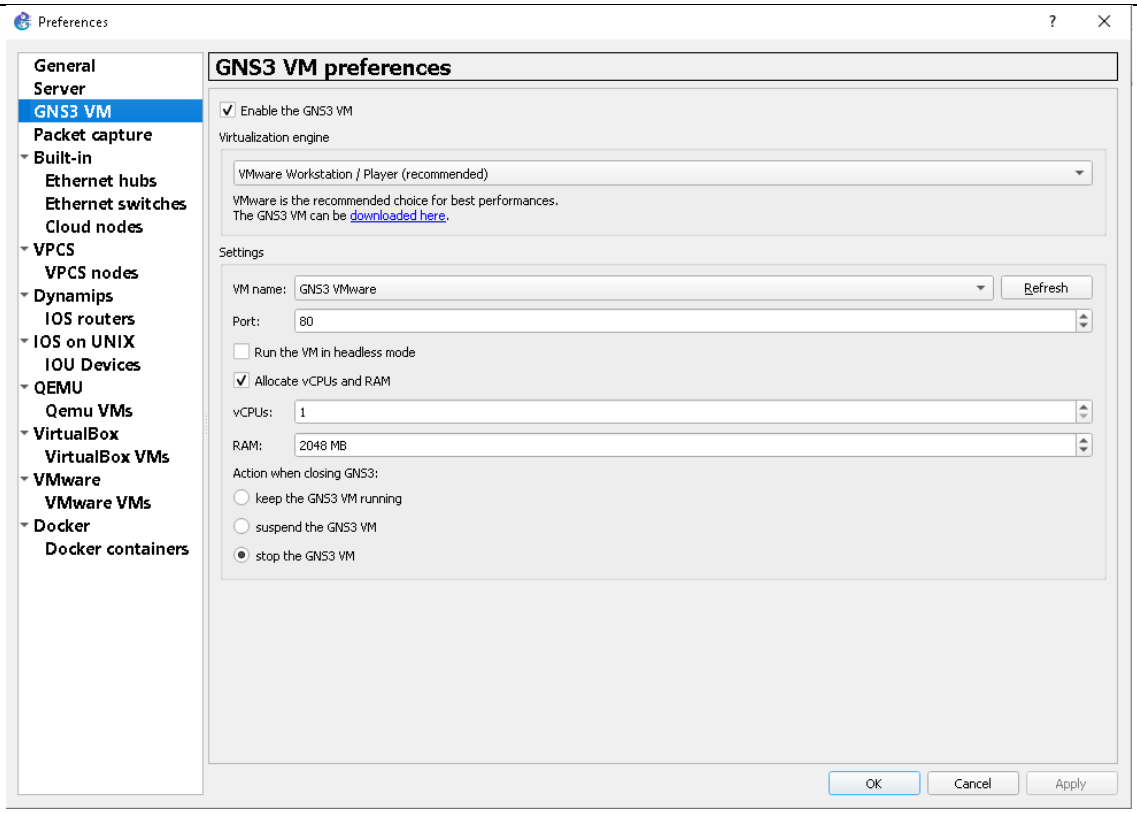
2. Bajar la GNS3 VM la misma que se instalará en VMWare.



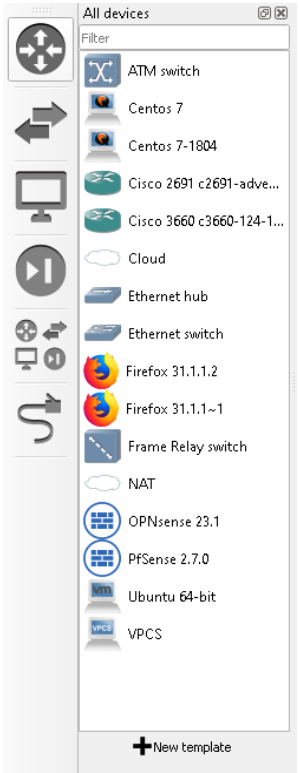
3. Una vez bajada se debe subir en el virtualizador para que se asigne la dirección IP y configurar la carga operativa de los diferentes software en la máquina virtual GNS3VM



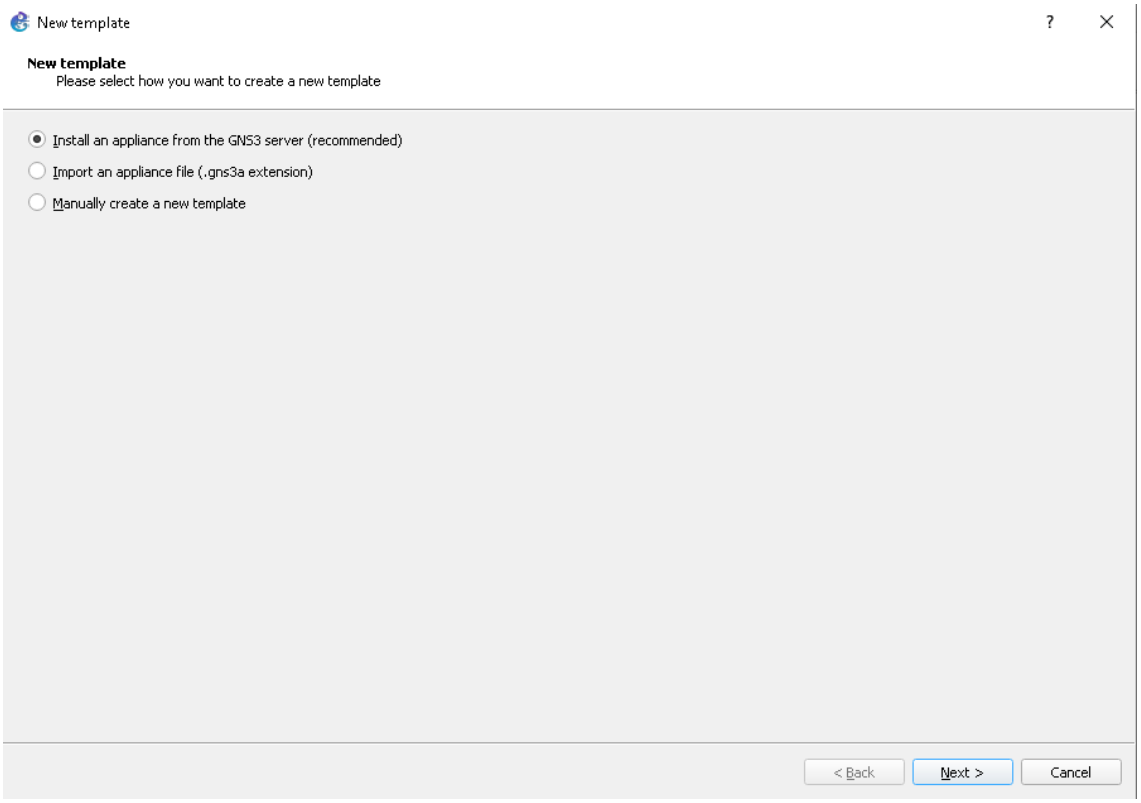
4. Debe dirigirse a Edit – Preference y en la sección de GNS3 VM escoger el virtualizador que esta usando para que exista relación entre el software GNS3 y la máquina virtual.

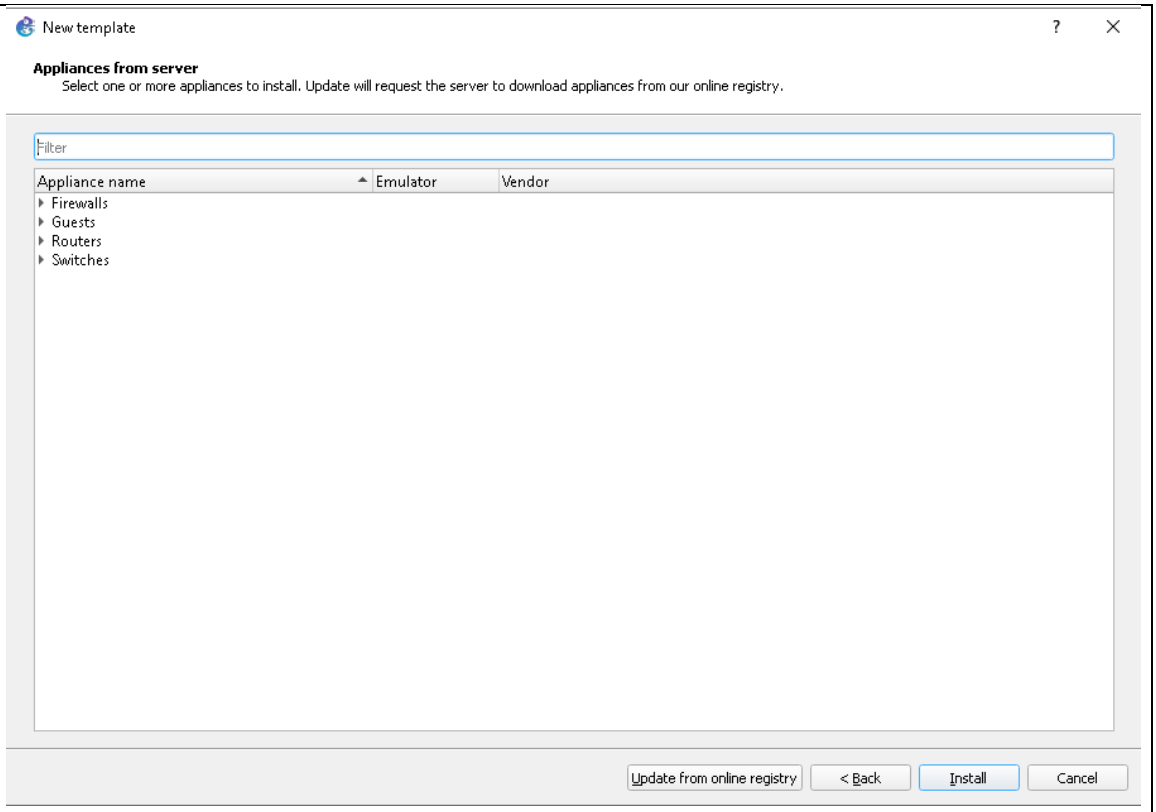


5. En el panel principal, dirigirse a la opción de Browse all device y se debe dirigir a NEW Template.



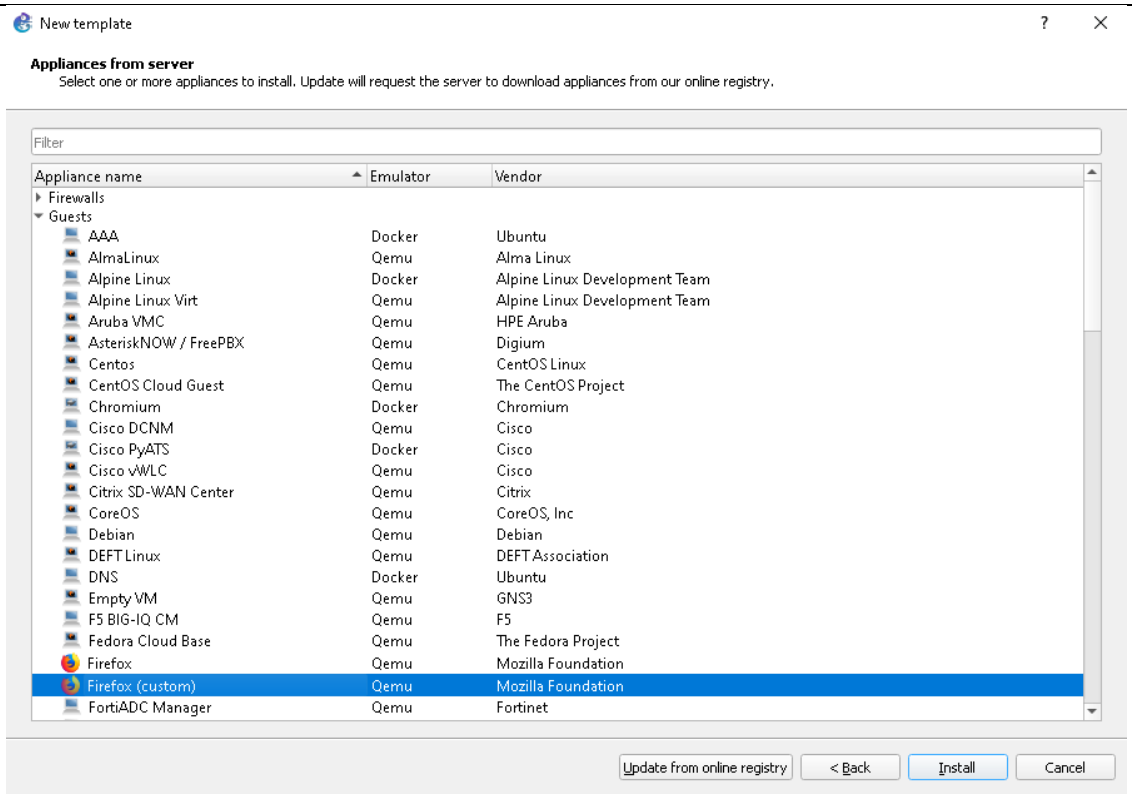
6. Se abre la opción de New Template, se deja por defecto la opción que aparece, se da siguiente y en la pantalla que aparece se escoge el software que se va a instalar. Se desarrollara un ejemplo debido a que todos los demas contienen el mismo procedimiento.



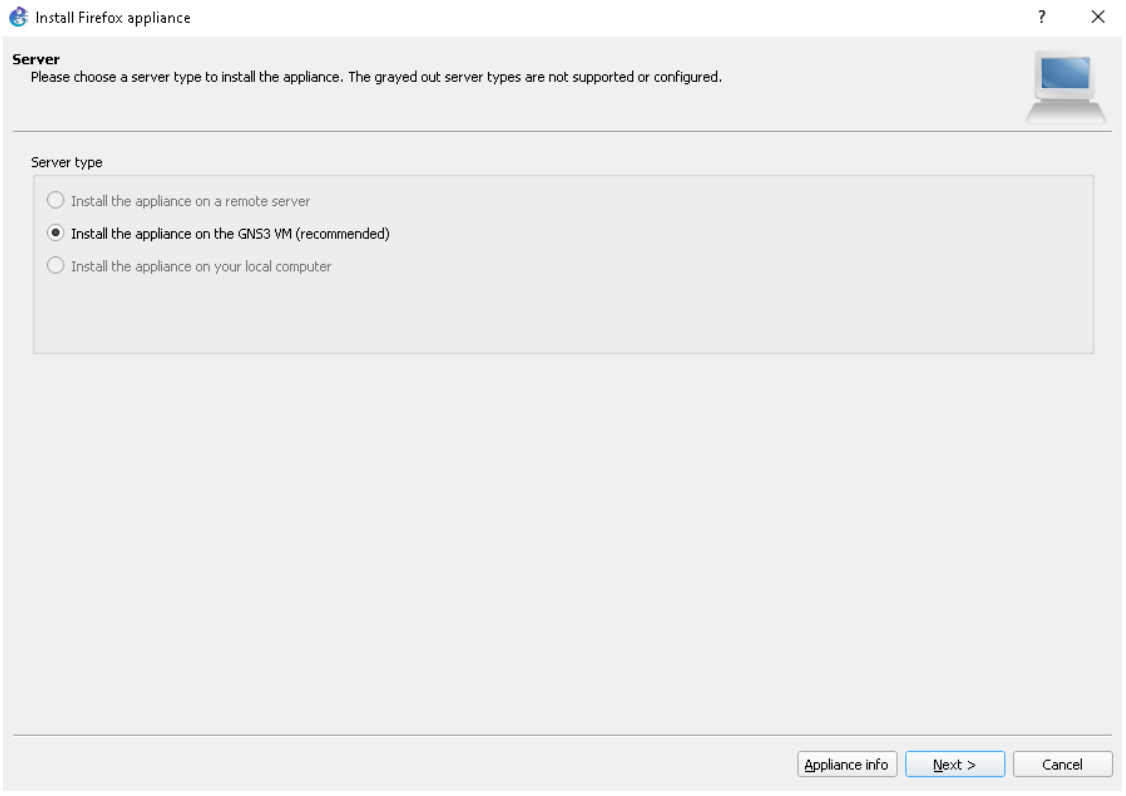


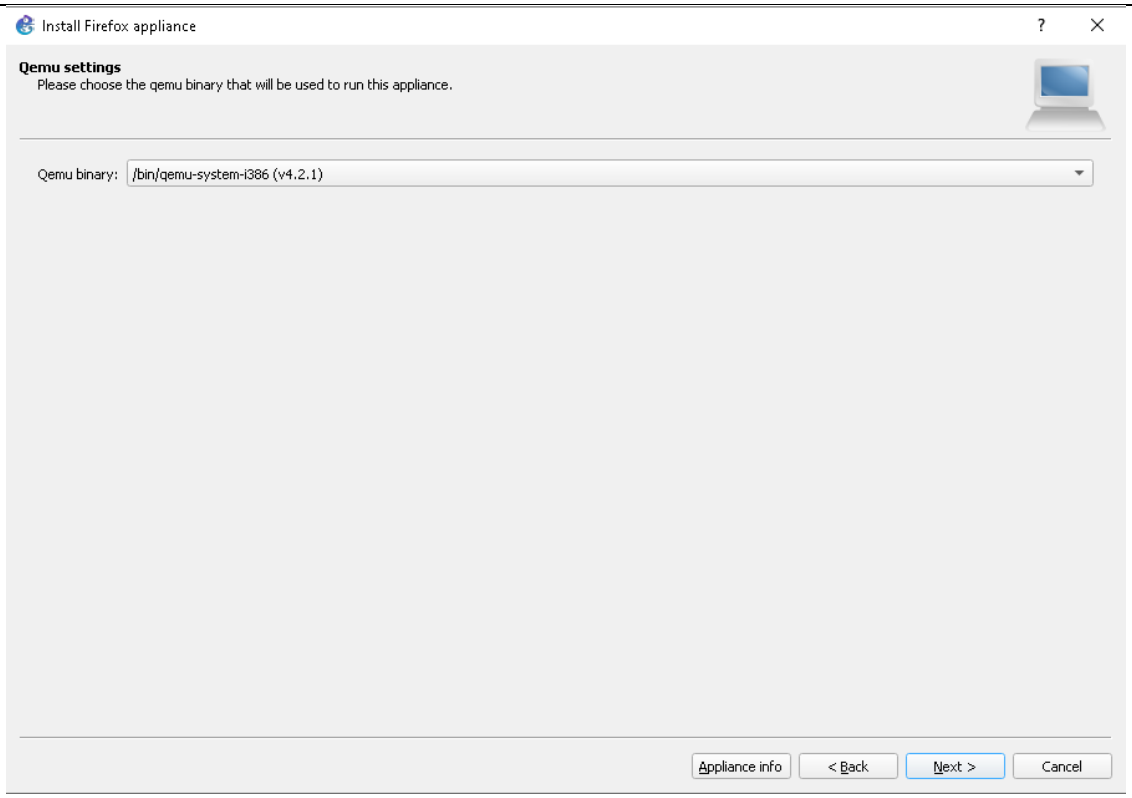
7. En la imagen anterior se puede ver que se puede instalar diferentes software para la emulación de los sistemas operativos como por ejemplo Firewall de diferentes marcas, router, switch e invitados.

   Se procederá a bajar la aplicación Firefox (custom), para dar un ejemplo de proceso para instalar una appliances.



8. Se presiona en Install, y se deja por defecto la opción presentada.

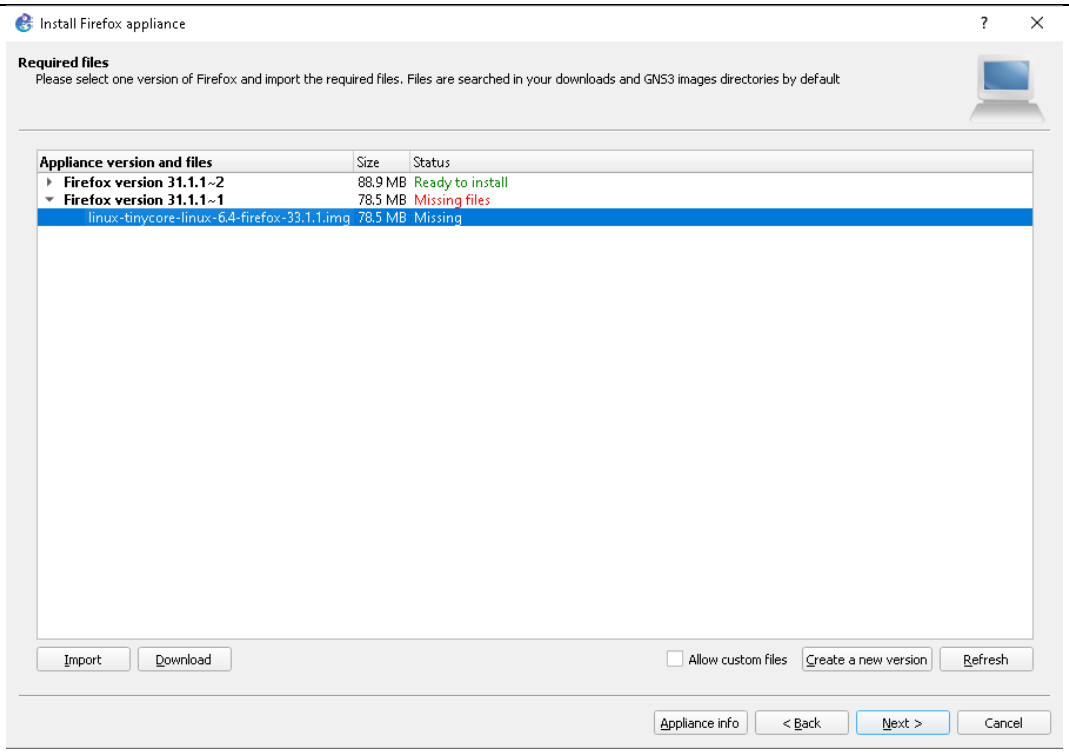




9. En la pantalla de Required files, se selecciona la versión del software que se usa en el banco de pruebas.

   Una vez seleccionado, se presiona la opción de Download, se direcciona a la página oficial o un repositorio seguro para descargar la imagen.

   Realizada la descarga se debe proceder a cargar mediante el boton IMPORT, donde se seleccionaron el archivo recien descargado.



10. Una vez cargado el template en GNS3, esta listo para usar el mismo, cabe recordar que el template cargado de cualquier software o aplicación, al momento de llevarlo a la mesa de trabajo de GNS3 se inicia desde cero, sin ninguna configuracion existente.

RESULTADO(S) OBTENIDO(S):

El estudiante se familiariza con la aplicación mediante su instalación y configuración básica para iniciar en el proceso de configuración de appliance para la administración y seguridad de redes LAN y WAN.

CONCLUSIONES:

El estudiante genera destreza al gestionar desde cero el GNS3 y su máquina virtual GSN3 VM

RECOMENDACIONES:

Planificar el software a descargar y tener listo para gestionar el tiempo adecuadamente

Docente: _____

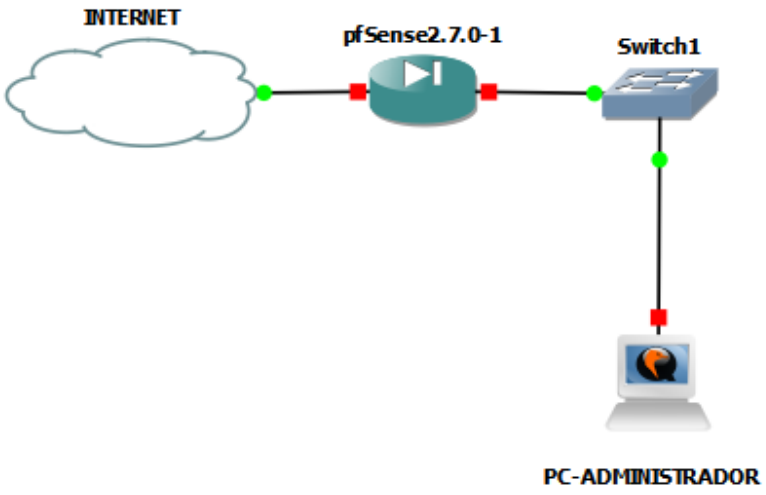
Firma: _____

4.2. PRÁCTICA # 2

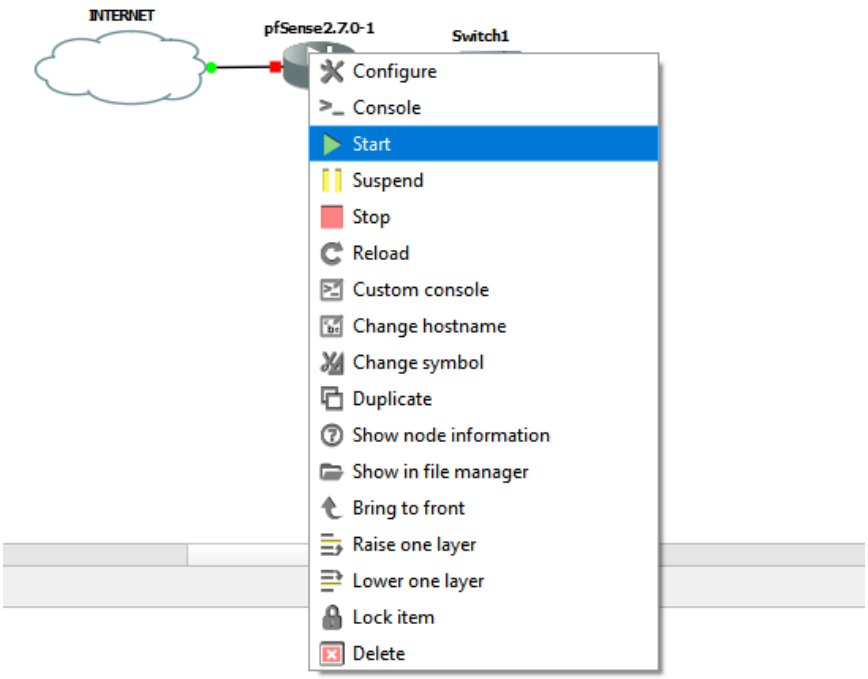
<table>
<tr><td colspan="2"> 
FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>Carrera: Ingeniería Electrónica</td><td>Asignatura: Redes de Computadoras</td></tr>
<tr><td>NRO. Práctica: 2</td><td>Título Práctica:
Configuración de una red LAN, asignación dinámica de direcciones IP (DHCP) y redirección de puertos (NAT) utilizando la solución de software de código abierto pfSense</td></tr>
<tr><td colspan="2">OBJETIVO:
• Objetivo General
Diseñar y configurar una red LAN (Local Área Network) utilizando la plataforma pfSense, junto con la implementación de la función de NAT (Network Address Translation)</td></tr>
<tr><td>INSTRUCCIONES:</td><td>1. Configurar las interfaces de red (WAN y LAN) con direcciones IP y máscaras de subred correspondientes.
2. Configurar la función de Network Address Translation (NAT) para permitir que los dispositivos de la red local accedan a Internet utilizando la dirección IP pública de la WAN.
3. Configurar un servidor DHCP para asignar automáticamente direcciones IP a los dispositivos en la red LAN
4. Subir al AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta de la práctica realizada en clase.</td></tr>
<tr><td colspan="2">ACTIVIDADES POR DESARROLLAR</td></tr>
</table>

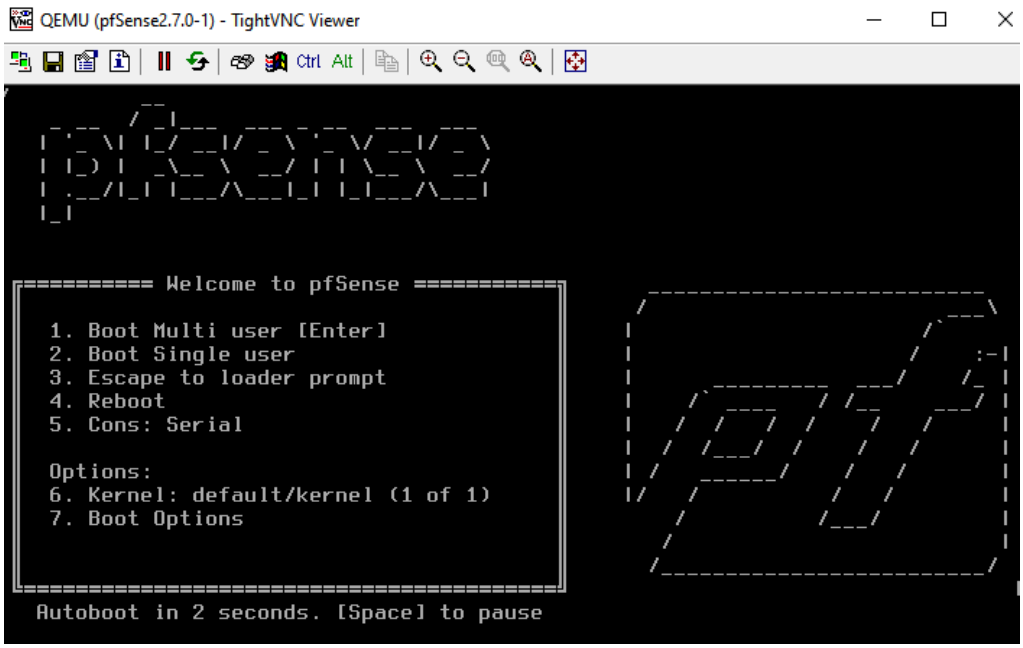
En esta práctica se trata de establecer una red local (LAN) al configurar automáticamente direcciones IP mediante DHCP y facilitar la redirección de puertos (NAT) utilizando el software de código abierto pfSense

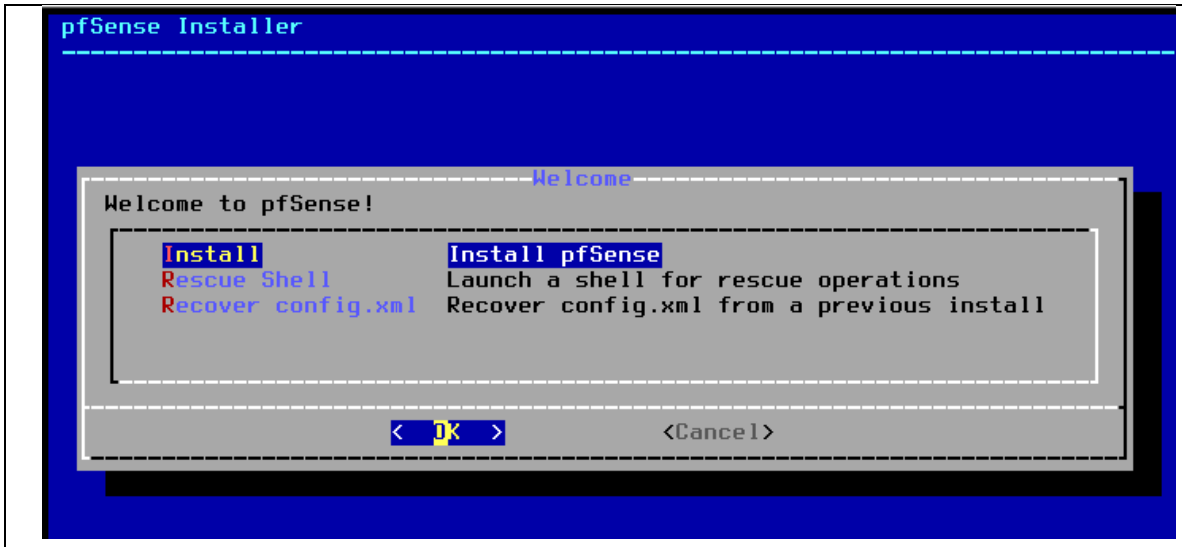
1. Realizar el siguiente esquema de red.

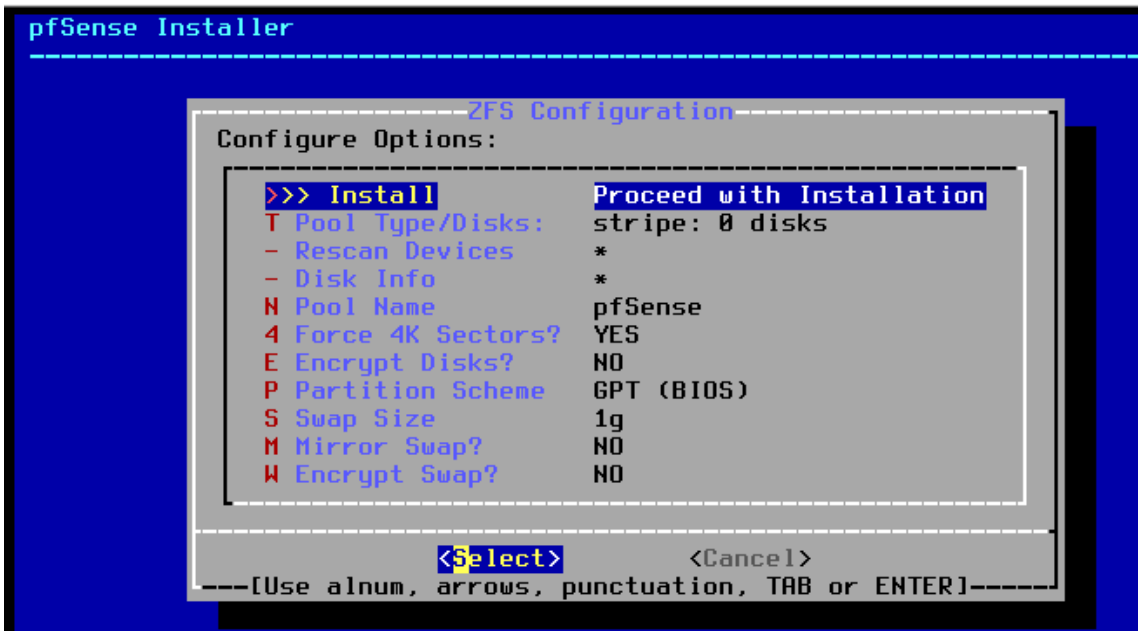


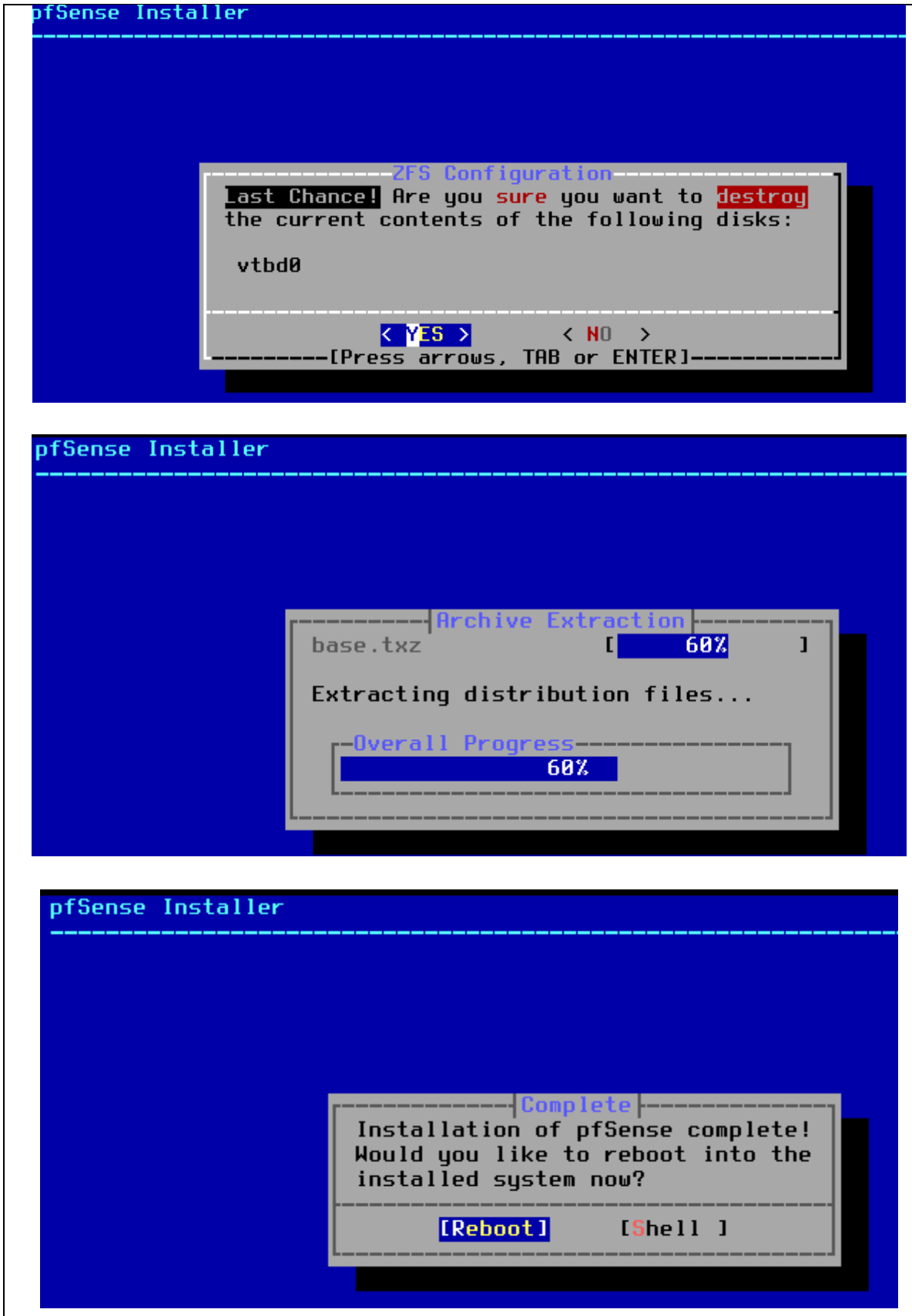
2. En esta práctica se hará uso de pfSense y Ubuntu 14.04 para llevar a cabo la configuración. Se comienza por instalar el software, y una vez finalizada la instalación, se desplegará la pantalla que contiene la configuración de las direcciones IP de la WAN y la red LAN. En esta etapa, se realiza modificaciones en todos los parámetros


INTERNET
pfSense2.7.0-1
Switch1
Configure
Console
Start
Suspend
Stop
Reload
Custom console
Change hostname
Change symbol
Duplicate
Show node information
Show in file manager
Bring to front
Raise one layer
Lower one layer
Lock item
Delete

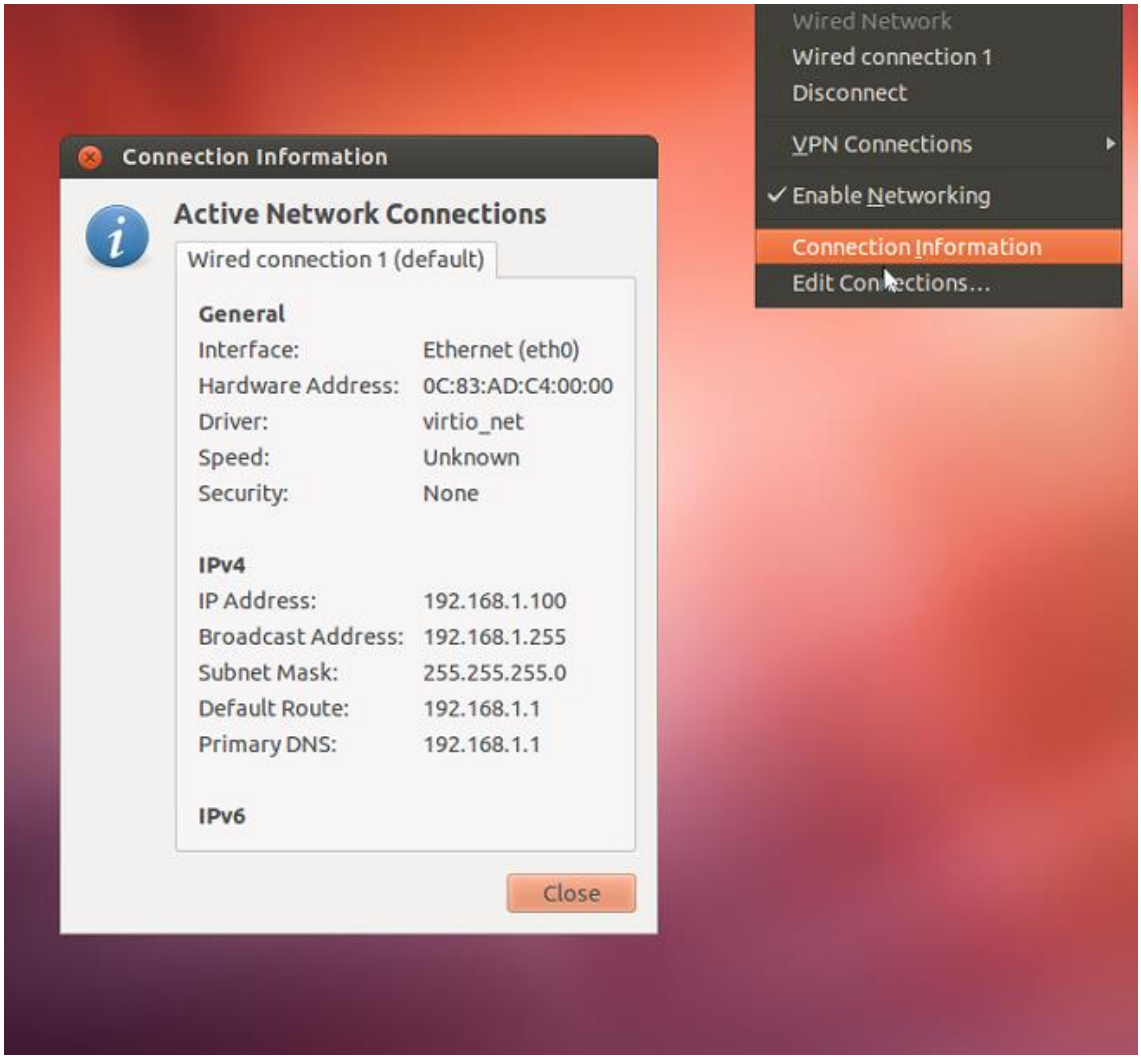

QEMU (pfSense2.7.0-1) - TightVNC Viewer
Ctrl
Alt
Welcome to pfSense
1. Boot Multi user [Enter]
2. Boot Single user
3. Escape to loader prompt
4. Reboot
5. Cons: Serial
Options:
6. Kernel: default/kernel (1 of 1)
7. Boot Options
Autoboot in 2 seconds. [Space] to pause


pfSense Installer
Welcome
Welcome to pfSense!
Install
Install pfSense
Rescue Shell
Launch a shell for rescue operations
Recover config.xml
Recover config.xml from a previous install
< OK >
<Cancel>

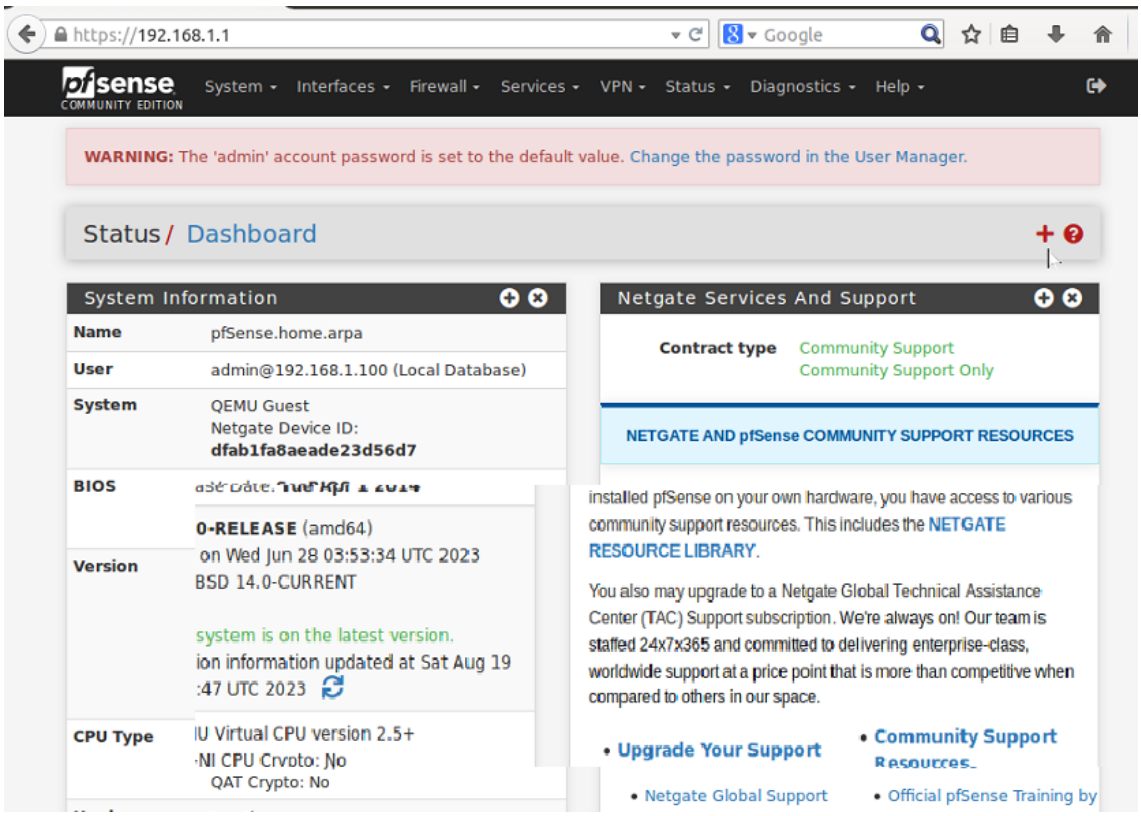

pfSense Installer
ZFS Configuration
Configure Options:
>>> Install
Proceed with Installation
T Pool Type/Disks:
stripe: 0 disks
- Rescan Devices
*
- Disk Info
*
N Pool Name
pfSense
4 Force 4K Sectors?
YES
E Encrypt Disks?
NO
P Partition Scheme
GPT (BIOS)
S Swap Size
1g
M Mirror Swap?
NO
W Encrypt Swap?
NO
<Select>
<Cancel>
[Use alnum, arrows, punctuation, TAB or ENTER]

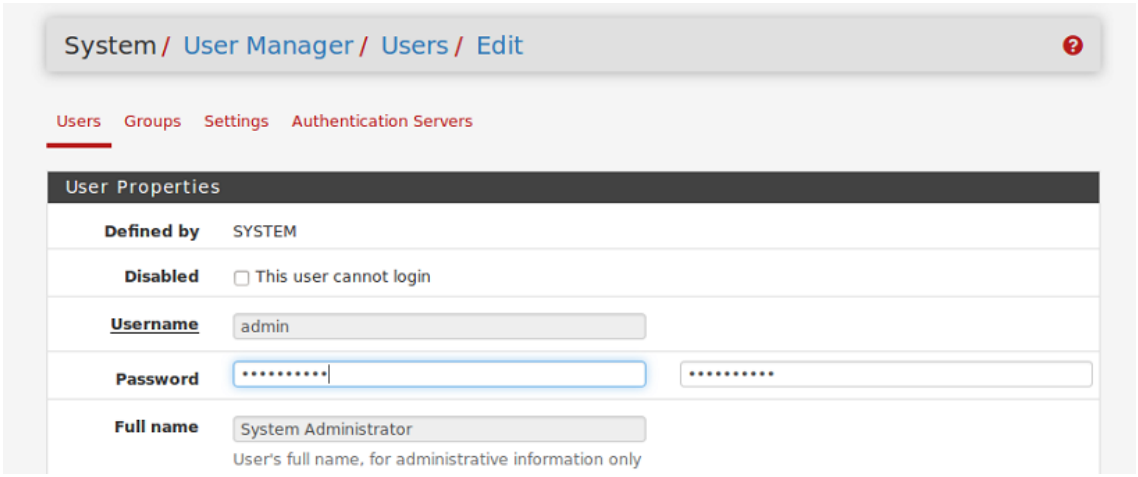

pfSense Installer
ZFS Configuration
Last Chance! Are you sure you want to destroy
the current contents of the following disks:
vtbd0
< YES >
< NO >
[Press arrows, TAB or ENTER]
pfSense Installer
Archive Extraction
base.txz
[60%]
Extracting distribution files...
Overall Progress
60%
pfSense Installer
Complete
Installation of pfSense complete!
Would you like to reboot into the
installed system now?
[Reboot]
[Shell]

3. Una vez finalizada la instalación del software pfSense, se observa la dirección IP WAN que posibilita el acceso a Internet. Se identifica la dirección IP LAN preestablecida, la cual se ajustará mas adelante a 192.168.20.20/24 para transformarla en la nueva dirección de administración. Estos ajustes se llevarán a cabo mediante la interfaz web. Cabe destacar que el software incluye de fábrica el protocolo DHCP, y se observará qué dirección asigna al PC



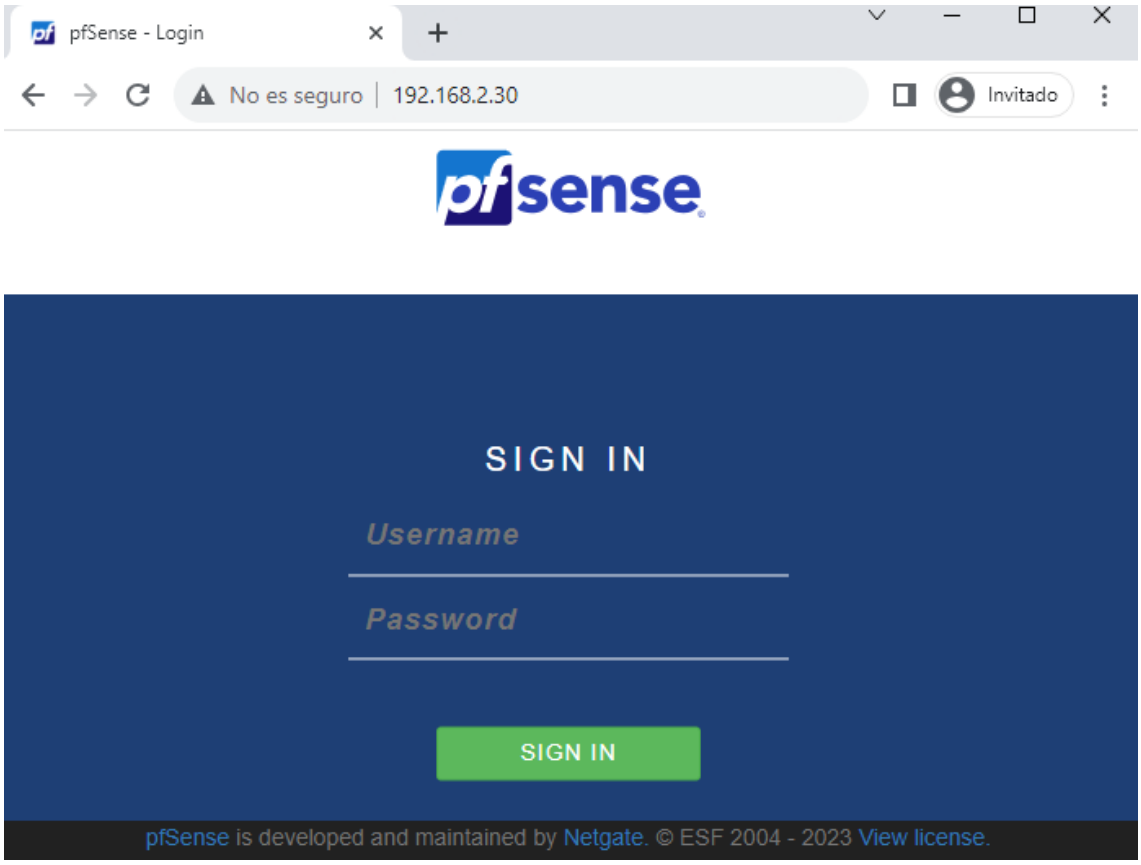
4. Se abre el navegador web y se digita la dirección 192.168.1.1, donde se procede a ajustar los parámetros de la red LAN, modificar la contraseña de administración del dispositivo y establecer la configuración del servidor DHCP , las credenciales para el ingreso son user: admin y contraseña: pfsense.



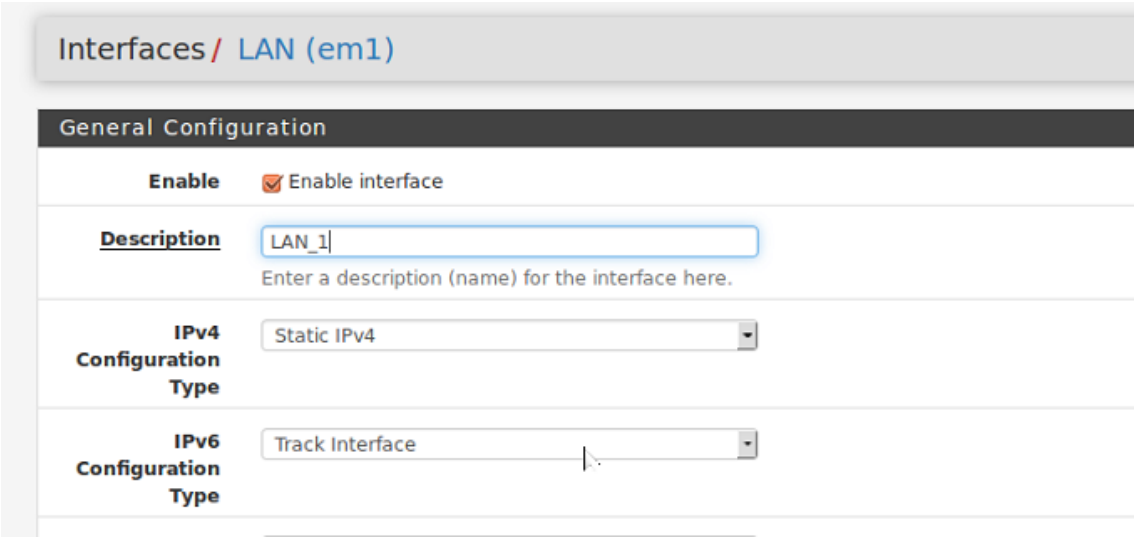


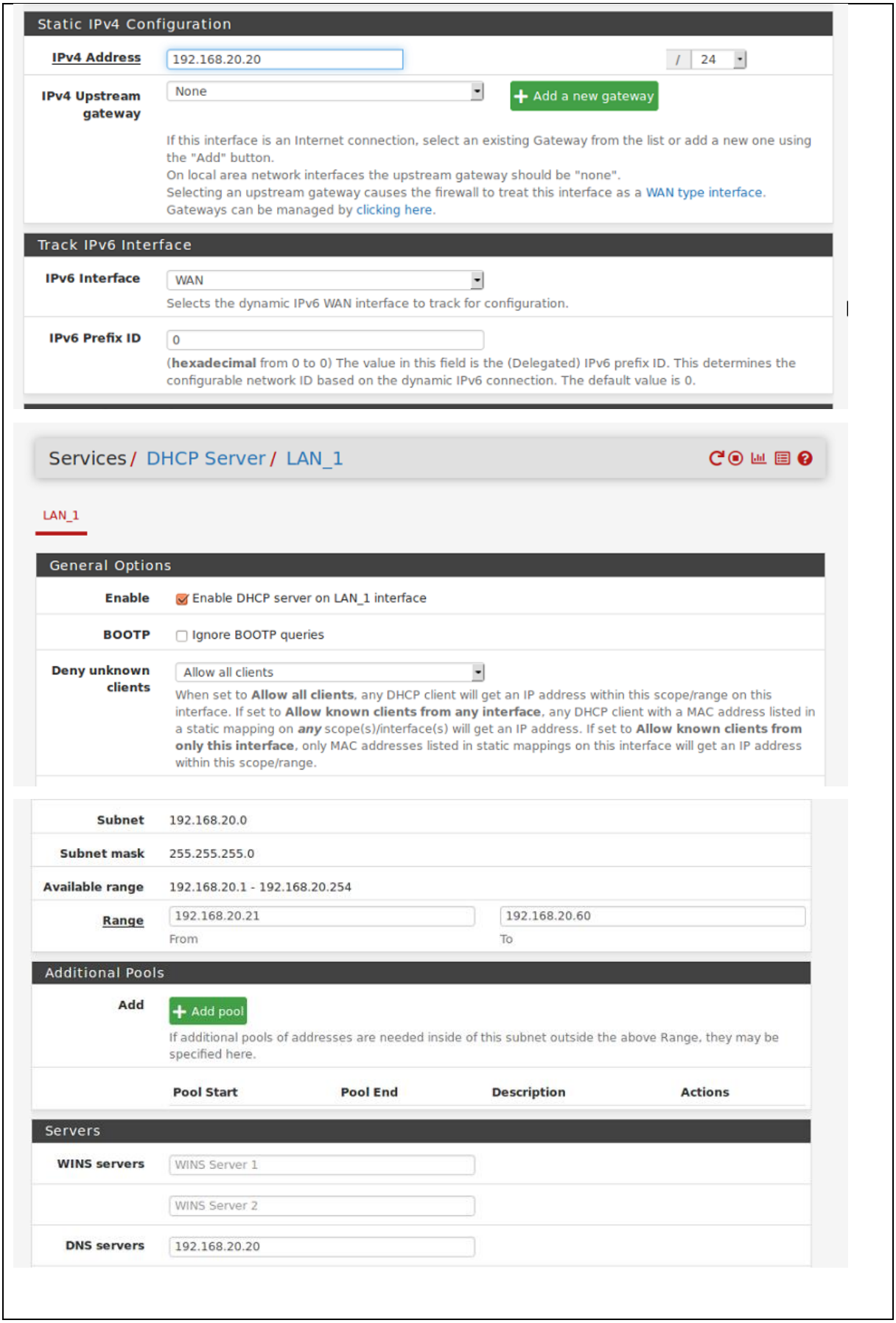
5. En este momento, se está preparado para dar inicio a las configuraciones correspondientes a la primera práctica. Para llevar a cabo esta tarea, se utiliza la dirección IP asignada por el servidor DHCP de pfSense, la cual es 192.168.2.30/24. Esta dirección permitirá administrar el equipo a través de su interfaz web mediante el

protocolo HTTP. Para acceder a la interfaz, basta con abrir cualquier navegador de su elección.

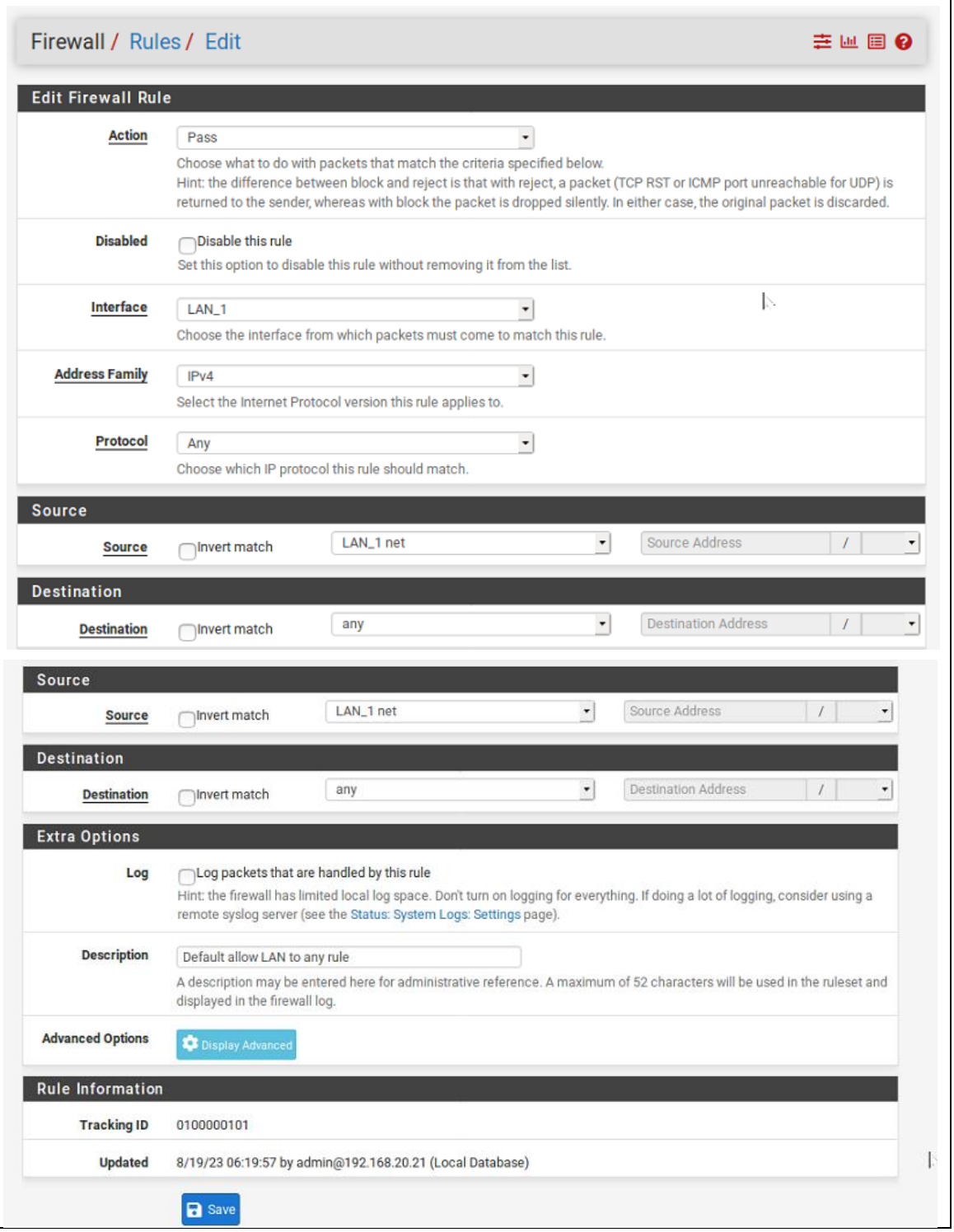


6. Seleccionar la sección "Interfaces" y eligir interfaz WAN. Verificar que esté configurada adecuadamente con la dirección IP y la máscara de subred proporcionadas por tu proveedor de servicios de Internet.

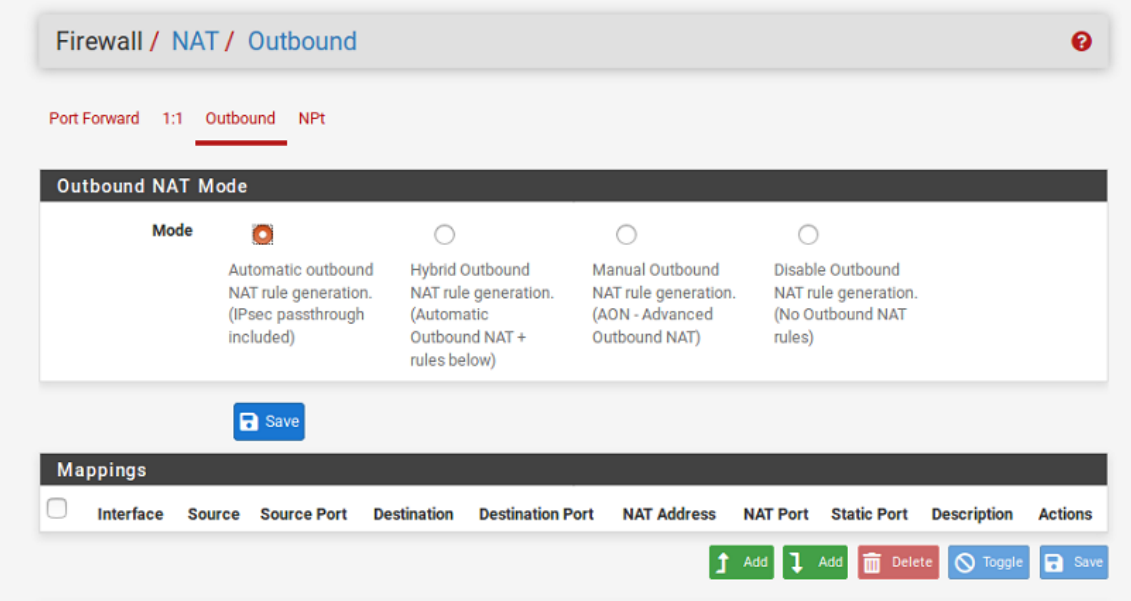



Static IPv4 Configuration
IPv4 Address
192.168.20.20
/ 24
IPv4 Upstream gateway
None
Add a new gateway
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.
Track IPv6 Interface
IPv6 Interface
WAN
Selects the dynamic IPv6 WAN interface to track for configuration.
IPv6 Prefix ID
0
(hexadecimal from 0 to 0) The value in this field is the (Delegated) IPv6 prefix ID. This determines the configurable network ID based on the dynamic IPv6 connection. The default value is 0.
Services / DHCP Server / LAN_1
LAN_1
General Options
Enable
Enable DHCP server on LAN_1 interface
BOOTP
Ignore BOOTP queries
Deny unknown clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Subnet
192.168.20.0
Subnet mask
255.255.255.0
Available range
192.168.20.1 - 192.168.20.254
Range
192.168.20.21
From
192.168.20.60
To
Additional Pools
Add
Add pool
If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.
Pool Start
Pool End
Description
Actions
Servers
WINS servers
WINS Server 1
WINS Server 2
DNS servers
192.168.20.20

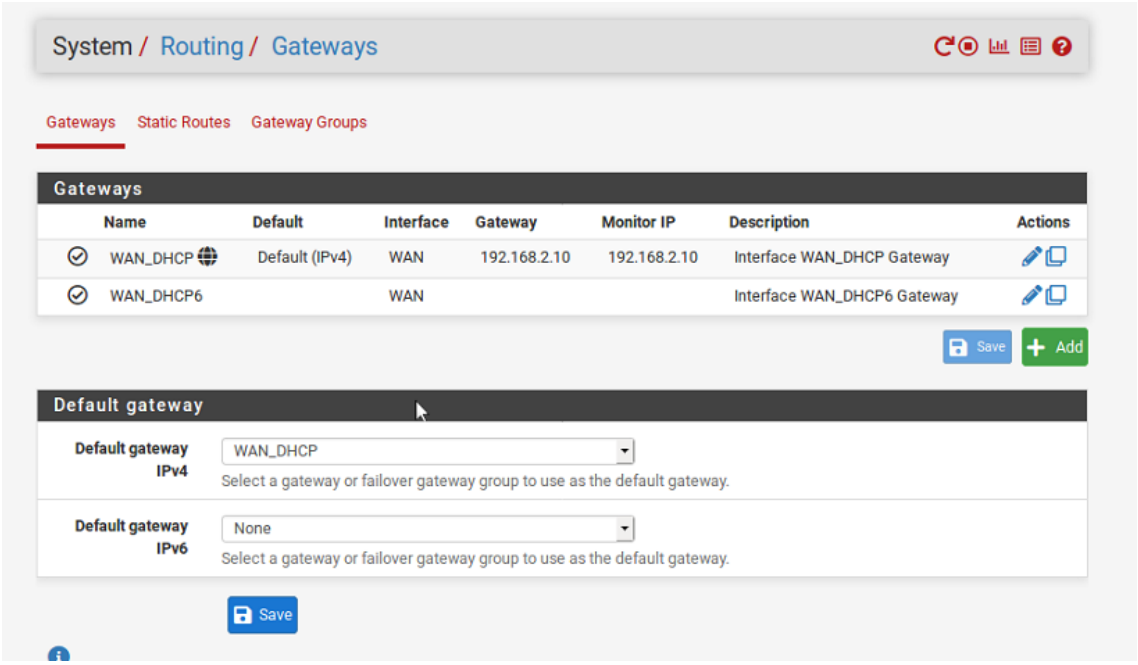
7. Ir a la sección "Firewall" y eligir "Rules". Asegúrarse de contar con una regla que permita el tráfico saliente (desde tu red LAN hacia cualquier destino) en la interfaz LAN. Esto facilitará que los dispositivos internos puedan conectarse a Internet. Además, puedes generar reglas extra de acuerdo con tus requerimientos para autorizar o restringir tráfico particular.

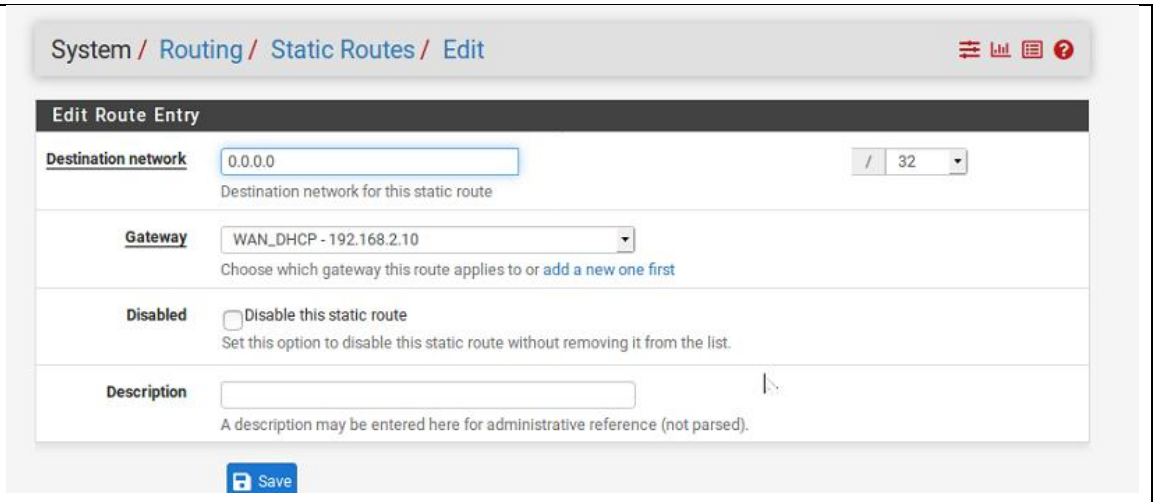


8. Ir a la sección "Firewall" y elegir la opción "NAT", luego seleccionar "Outbound" (Salida). En el campo "Mode" (Modo), optar por "Automatic outbound NAT rule generation" (Generación automática de reglas NAT de salida) en la mayoría de las situaciones. Sin embargo, si tiene requisitos particulares, tienes la opción de configurar manualmente las reglas de NAT.

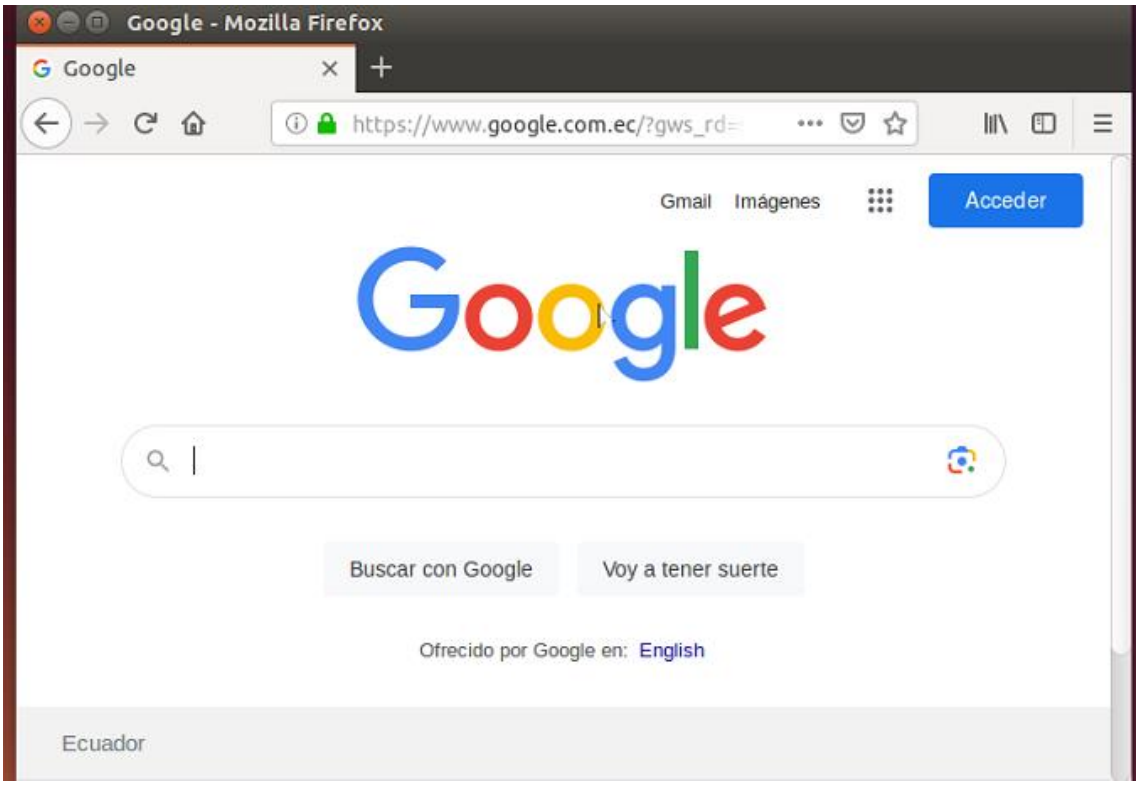


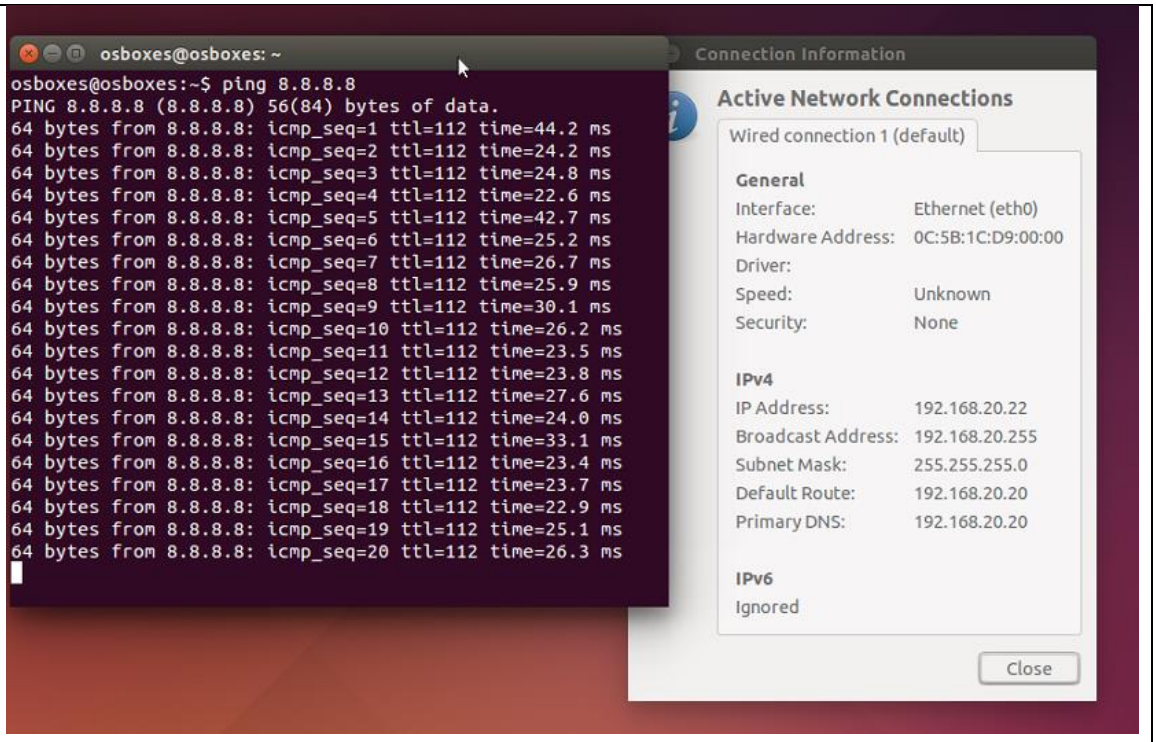
9. Una vez establecida las reglas, se procede a configurar la ruta estática y la puerta de enlace por donde se accederá a Internet.





10. Se realiza una prueba para confirmar que se haya asignado correctamente una dirección IP a través del protocolo DHCP en la red configurada. Luego, se llevará a cabo un ping y se navegará por Internet para verificar que todo esté operativo y funcionando.





RESULTADO(S) OBTENIDO(S):

El estudiante se familiariza con la implementación exitosa de estos servicios como es DHCP, Rutas Estáticas, Firewall componentes que garantiza una gestión efectiva de las direcciones IP, el enrutamiento y la seguridad de la red

CONCLUSIONES:

Se realiza la configuración de HCP, reglas de Firewall y pruebas de acceso a internet.

RECOMENDACIONES:

- Antes de implementar en producción, realiza pruebas exhaustivas para confirmar que la asignación de direcciones IP a través de DHCP y la conexión a Internet funcionan correctamente.
- Mantener un registro detallado de todas las configuraciones realizadas en PfSense, incluyendo direcciones IP, reglas de firewall y configuración DHCP

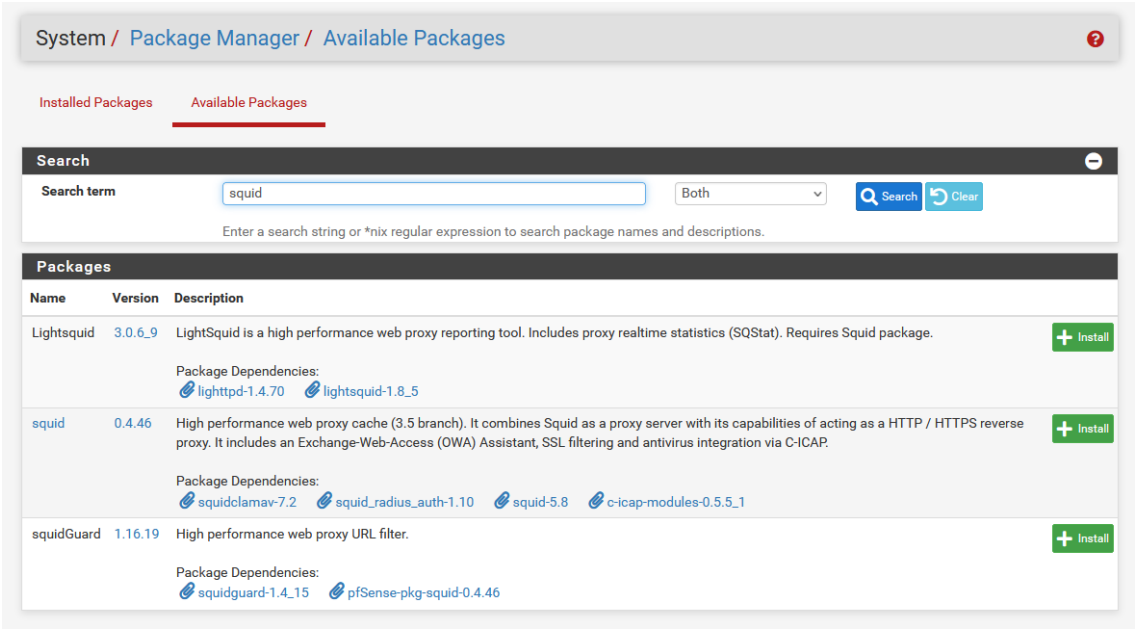
Docente: _____

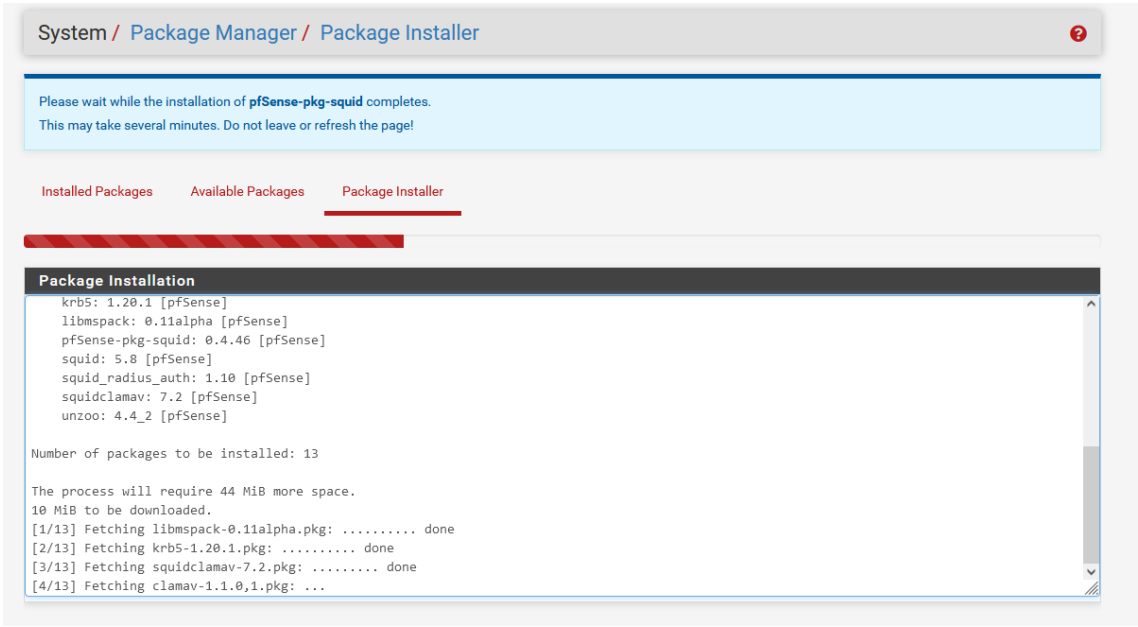
Firma: _____

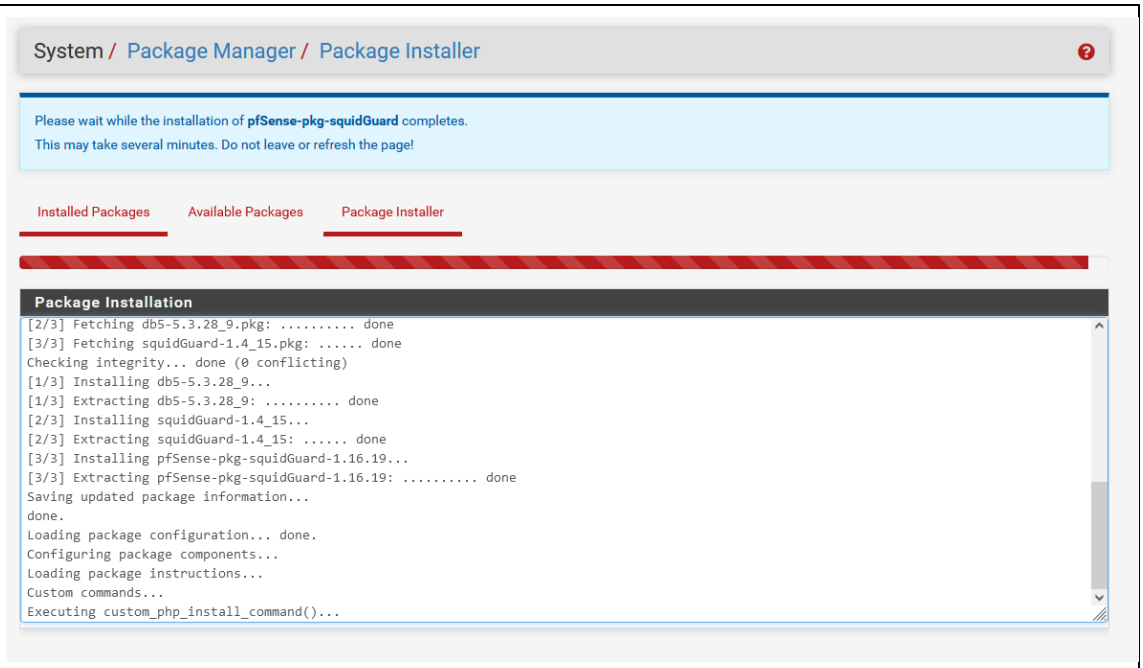
4.3. PRÁCTICA # 3

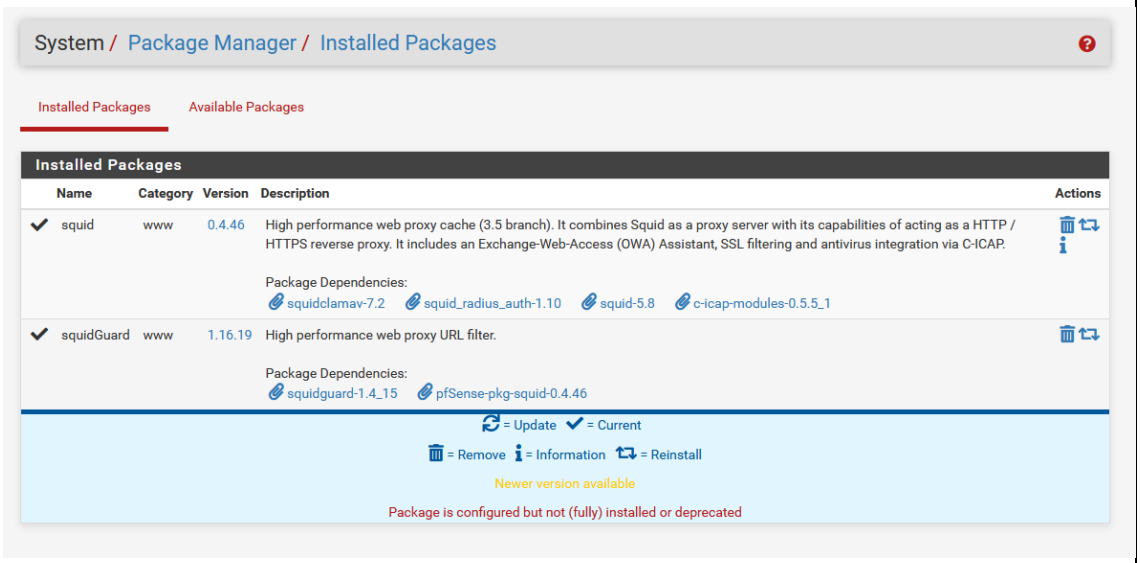
<table>
<tr><td colspan="2">FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>Carrera: Ingeniería Electrónica</td><td>Asignatura: Redes de Computadoras</td></tr>
<tr><td>NRO. Práctica: 3</td><td>Título Práctica:
Configurar un Sistema de Bloqueo de Páginas Web HTTPS con Certificado Utilizando pfSense con reglas de Squid proxy e Squid Guard"</td></tr>
<tr><td colspan="2">OBJETIVO:
• Objetivo General
Implementar un Sistema de Bloqueo de Sitios Web con Protocolo HTTPS Utilizando pfSense y Certificados"</td></tr>
<tr><td>INSTRUCCIONES:</td><td>1. Instalar y configurar pfSense en el entorno de red, asegurando una conexión estable y funcional.
2. Generar o adquirir certificados SSL/TLS válidos para permitir la inspección del tráfico HTTPS a través de Squid proxy.
3. Configurar el servicio Squid proxy en pfSense, habilitando la inspección SSL/TLS para el tráfico web seguro.
4. Implementar reglas de firewall que redirijan el tráfico HTTP y HTTPS hacia Squid proxy para su filtrado
5. Subir al AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta de la práctica realizada en clase.</td></tr>
<tr><td colspan="2">ACTIVIDADES POR DESARROLLAR</td></tr>
</table>

1. Instalar los paquetes en el pfsense de squid proxy y squid guard ingresando a su ip de administracion en este caso es la 192.168.20.20/24.



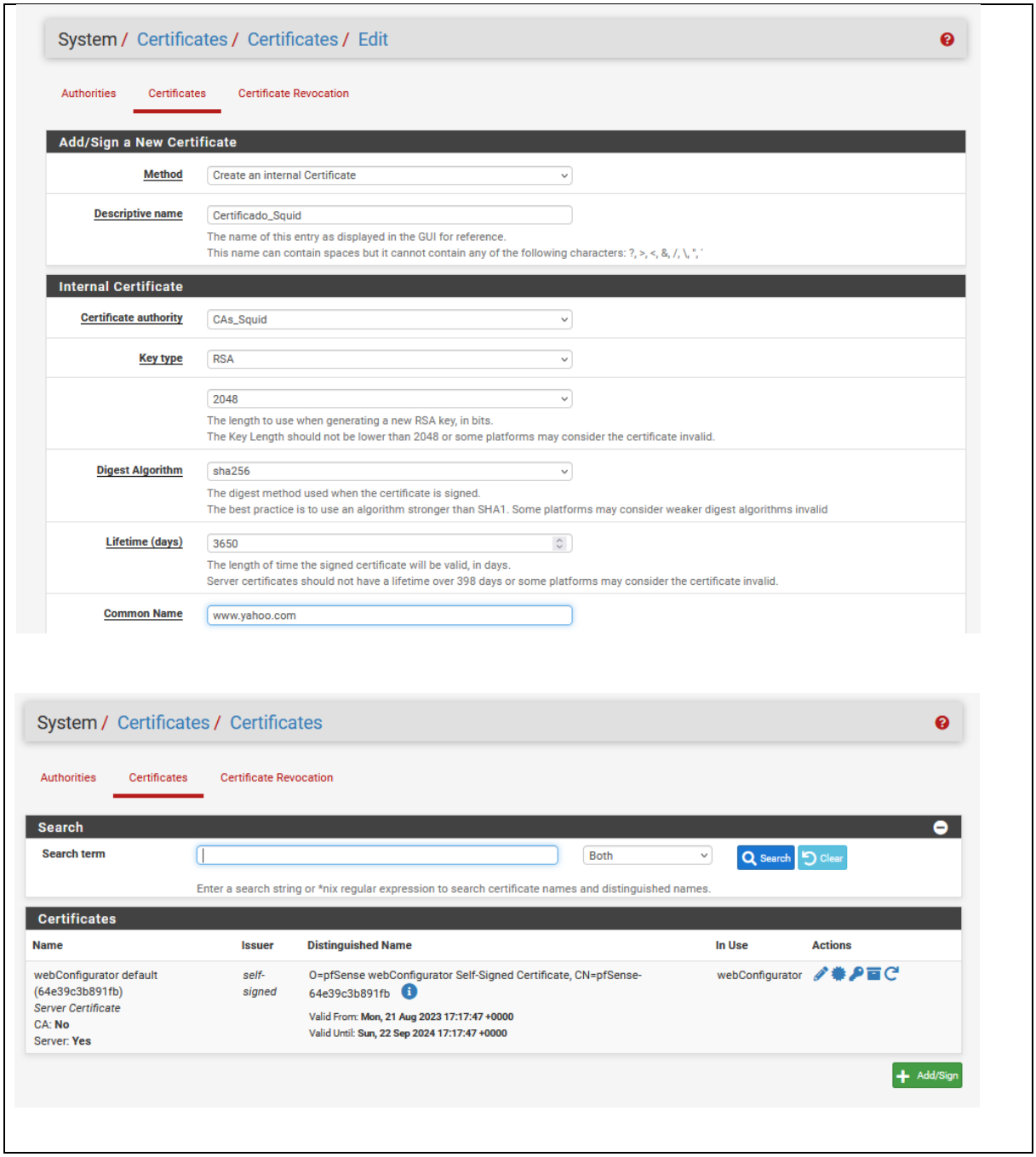


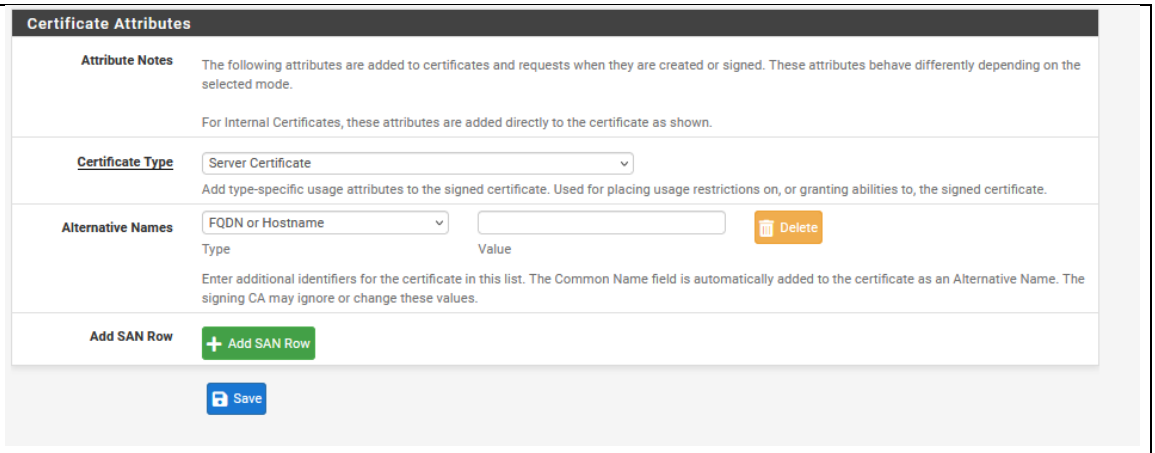




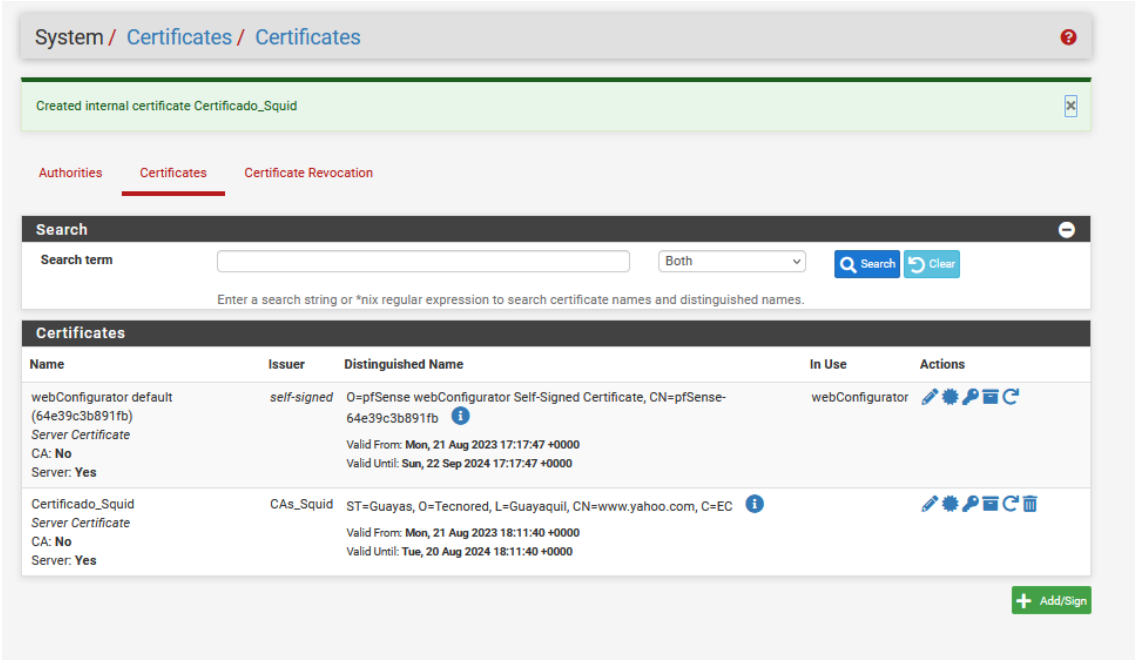
2. Generar los certificados CAs y cerficados que serán empleados en Squid para la navegación.

3. Creación de Certficados.

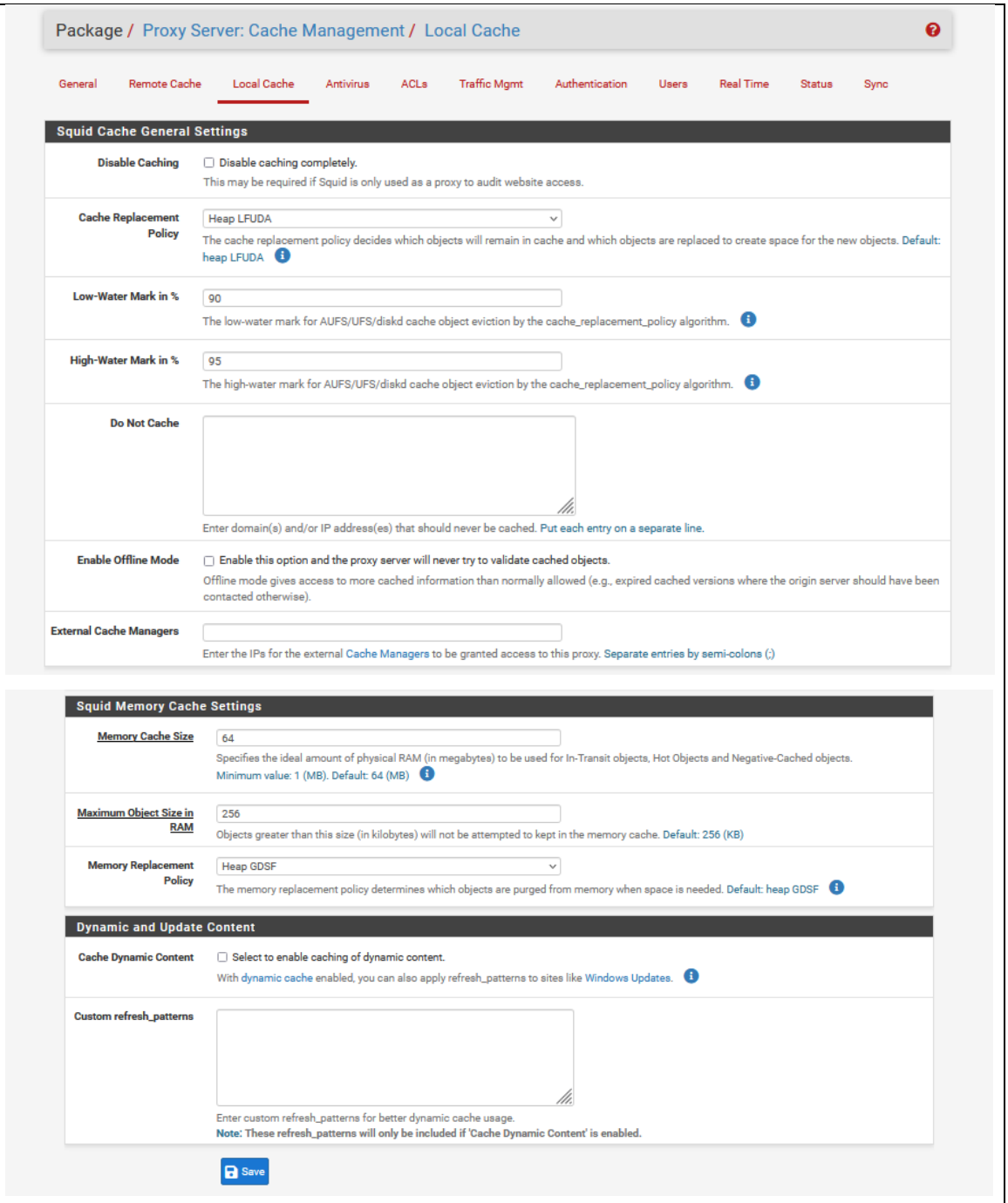

System / Certificates / Certificates / Edit
Authorities
Certificates
Certificate Revocation
Add/Sign a New Certificate
Method
Create an internal Certificate
Descriptive name
Certificado_Squid
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '
Internal Certificate
Certificate authority
CAs_Squid
Key type
RSA
2048
The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm
sha256
The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime (days)
3650
The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Common Name
www.yahoo.com
System / Certificates / Certificates
Authorities
Certificates
Certificate Revocation
Search
Search term
Both
Search
Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.
Certificates
Name
Issuer
Distinguished Name
In Use
Actions
webConfigurator default (64e39c3b891fb)
Server Certificate
CA: No
Server: Yes
self-signed
O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-64e39c3b891fb
Valid From: Mon, 21 Aug 2023 17:17:47 +0000
Valid Until: Sun, 22 Sep 2024 17:17:47 +0000
webConfigurator
Add/Sign



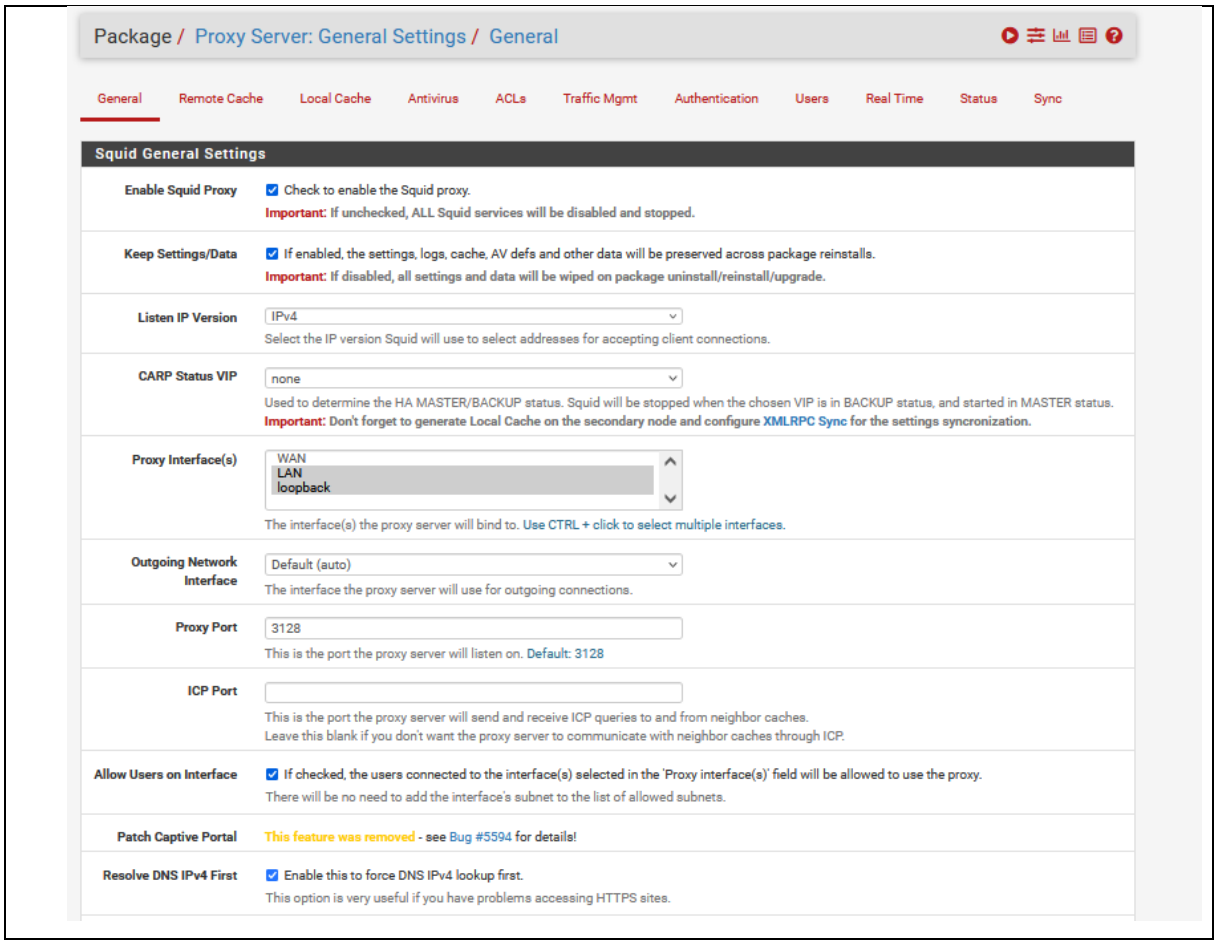
4. Se muestra que toda las configuración de los certificados que fueron creadas

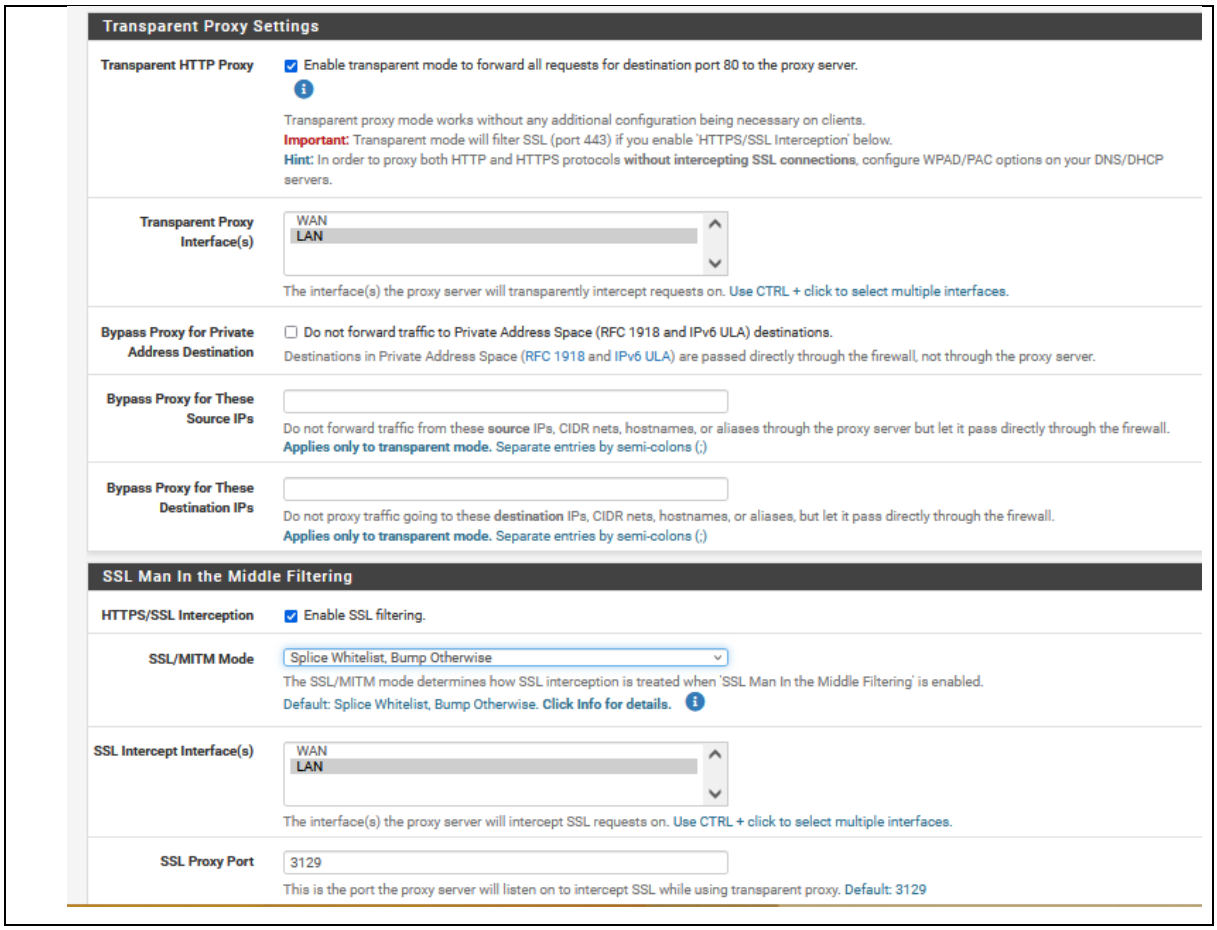


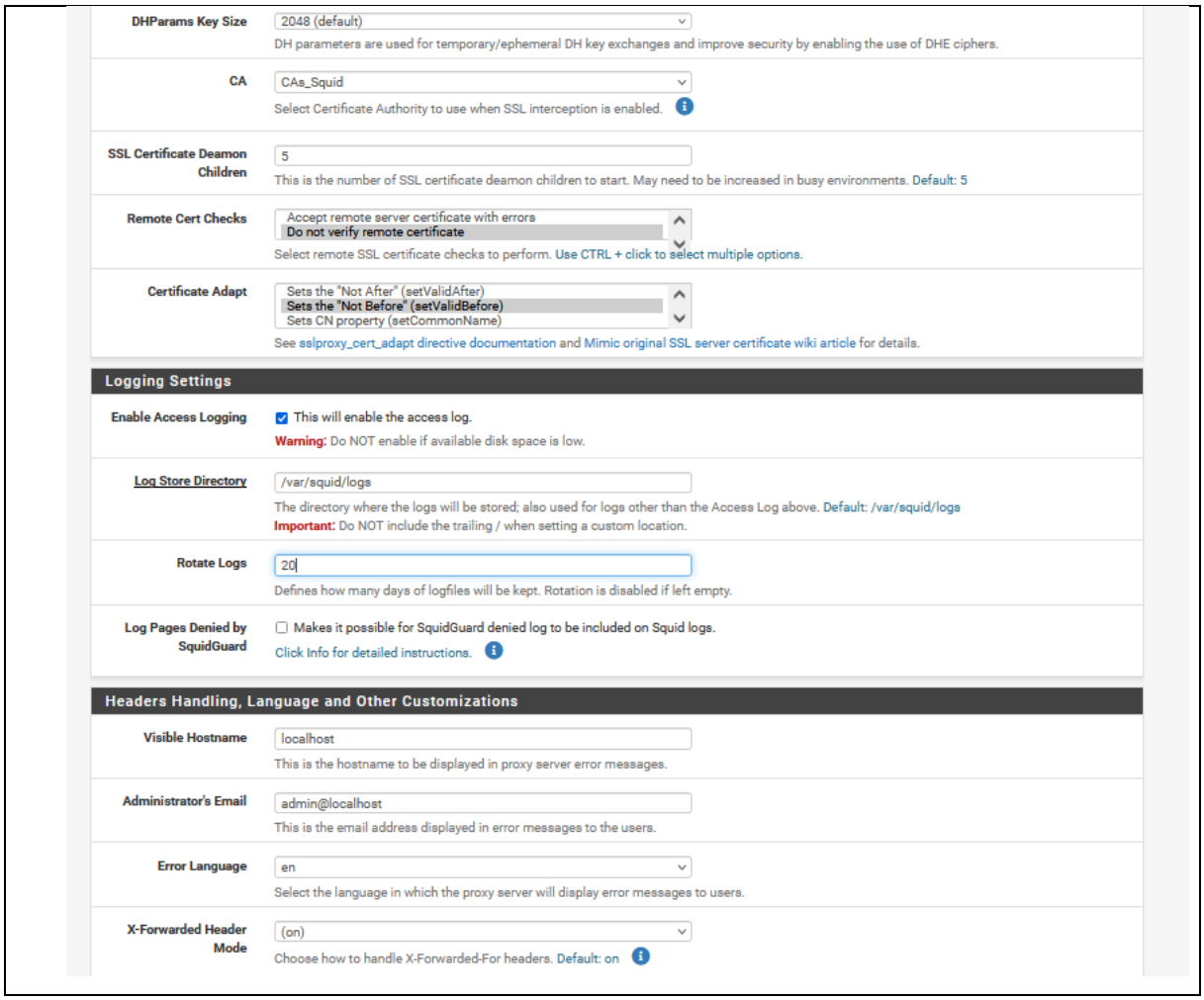
5. Antes de comenzar a configurar el Squid activar local cache solo le dará click en SAVE

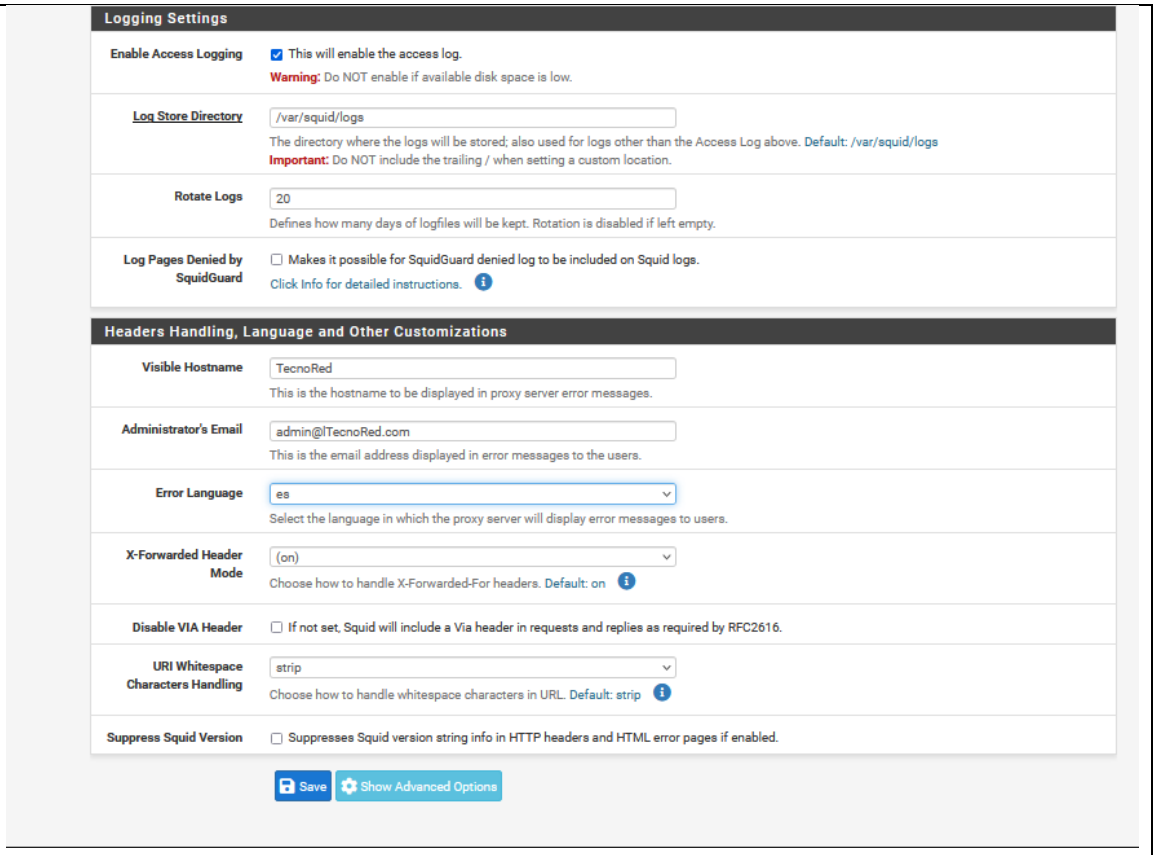


6. Configuracion del Squid proxy

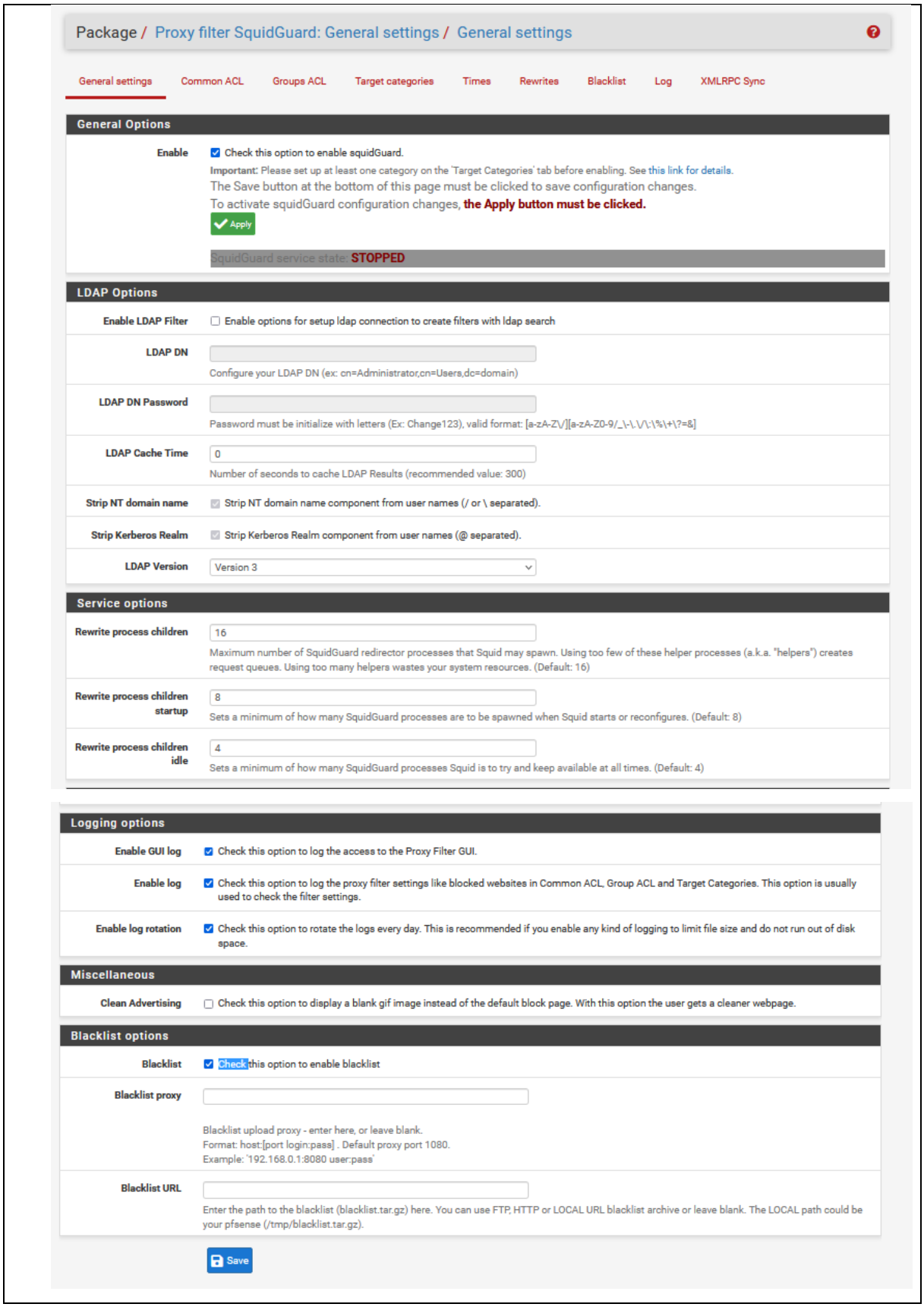

Package / Proxy Server: General Settings / General
General
Remote Cache
Local Cache
Antivirus
ACLs
Traffic Mgmt
Authentication
Users
Real Time
Status
Sync
Squid General Settings
Enable Squid Proxy
Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data
If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version
IPv4
Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP
none
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.
Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings syncronization.
Proxy Interface(s)
WAN
LAN
loopback
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface
Default (auto)
The interface the proxy server will use for outgoing connections.
Proxy Port
3128
This is the port the proxy server will listen on. Default: 3128
ICP Port
This is the port the proxy server will send and receive ICP queries to and from neighbor caches.
Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
Allow Users on Interface
If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.
There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal
This feature was removed - see Bug #5594 for details!
Resolve DNS IPv4 First
Enable this to force DNS IPv4 lookup first.
This option is very useful if you have problems accessing HTTPS sites.


Transparent Proxy Settings
Transparent HTTP Proxy
Enable transparent mode to forward all requests for destination port 80 to the proxy server.
Transparent proxy mode works without any additional configuration being necessary on clients.
Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections, configure WPAD/PAC options on your DNS/DHCP servers.
Transparent Proxy Interface(s)
WAN
LAN
The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.
Bypass Proxy for Private Address Destination
Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations.
Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.
Bypass Proxy for These Source IPs
Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.
Applies only to transparent mode. Separate entries by semi-colons (;)
Bypass Proxy for These Destination IPs
Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.
Applies only to transparent mode. Separate entries by semi-colons (;)
SSL Man In the Middle Filtering
HTTPS/SSL Interception
Enable SSL filtering.
SSL/MITM Mode
Splice Whitelist, Bump Otherwise
The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.
Default: Splice Whitelist, Bump Otherwise. Click Info for details.
SSL Intercept Interface(s)
WAN
LAN
The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.
SSL Proxy Port
3129
This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

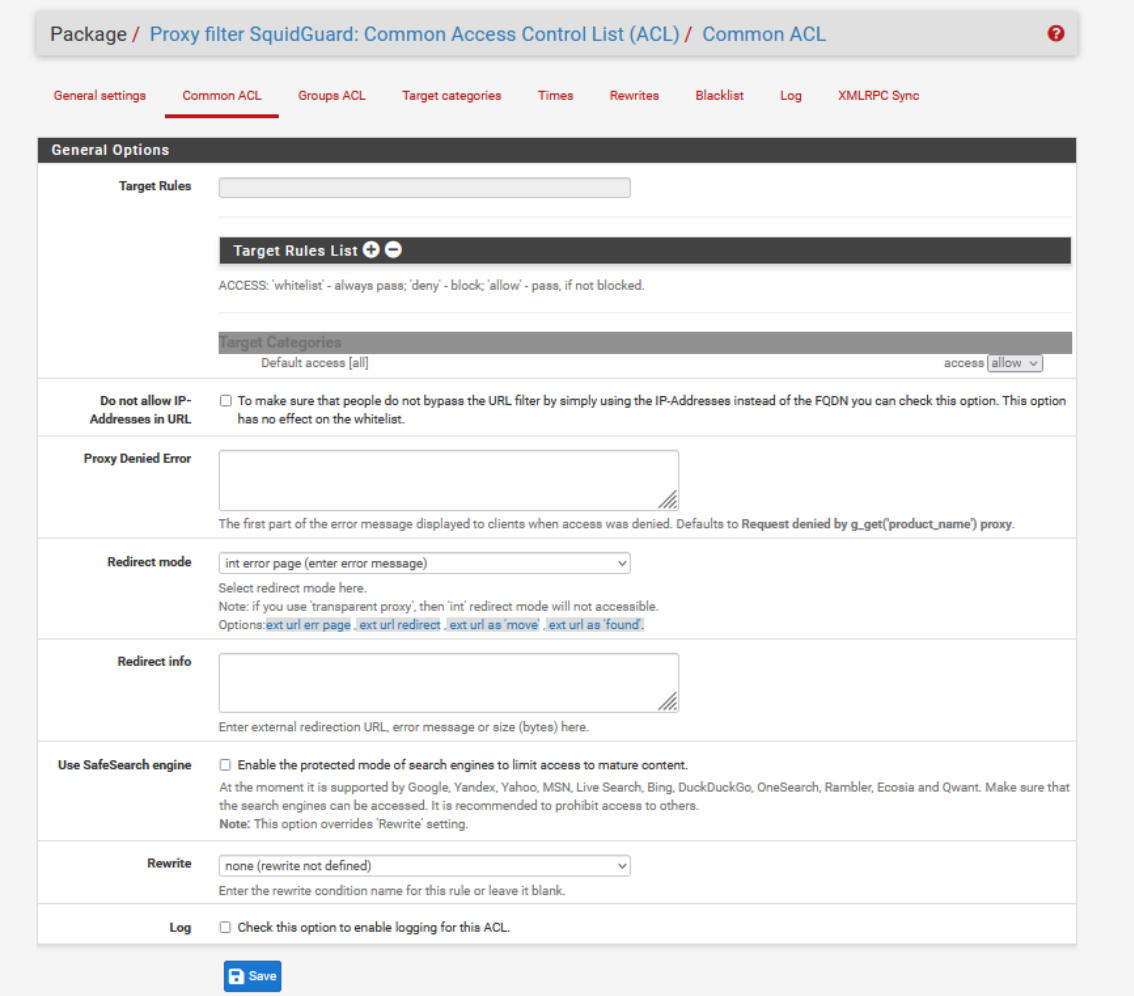

DHParams Key Size
2048 (default)
DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.
CA
CAs_Squid
Select Certificate Authority to use when SSL interception is enabled.
SSL Certificate Deamon Children
5
This is the number of SSL certificate deamon children to start. May need to be increased in busy environments. Default: 5
Remote Cert Checks
Accept remote server certificate with errors
Do not verify remote certificate
Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.
Certificate Adapt
Sets the "Not After" (setValidAfter)
Sets the "Not Before" (setValidBefore)
Sets CN property (setCommonName)
See sslproxy_cert_adapt directive documentation and Mimic original SSL server certificate wiki article for details.
Logging Settings
Enable Access Logging
This will enable the access log.
Warning: Do NOT enable if available disk space is low.
Log Store Directory
/var/squid/logs
The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.
Rotate Logs
20
Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Log Pages Denied by SquidGuard
Makes it possible for SquidGuard denied log to be included on Squid logs.
Click Info for detailed instructions.
Headers Handling, Language and Other Customizations
Visible Hostname
localhost
This is the hostname to be displayed in proxy server error messages.
Administrator's Email
admin@localhost
This is the email address displayed in error messages to the users.
Error Language
en
Select the language in which the proxy server will display error messages to users.
X-Forwarded Header Mode
(on)
Choose how to handle X-Forwarded-For headers. Default: on

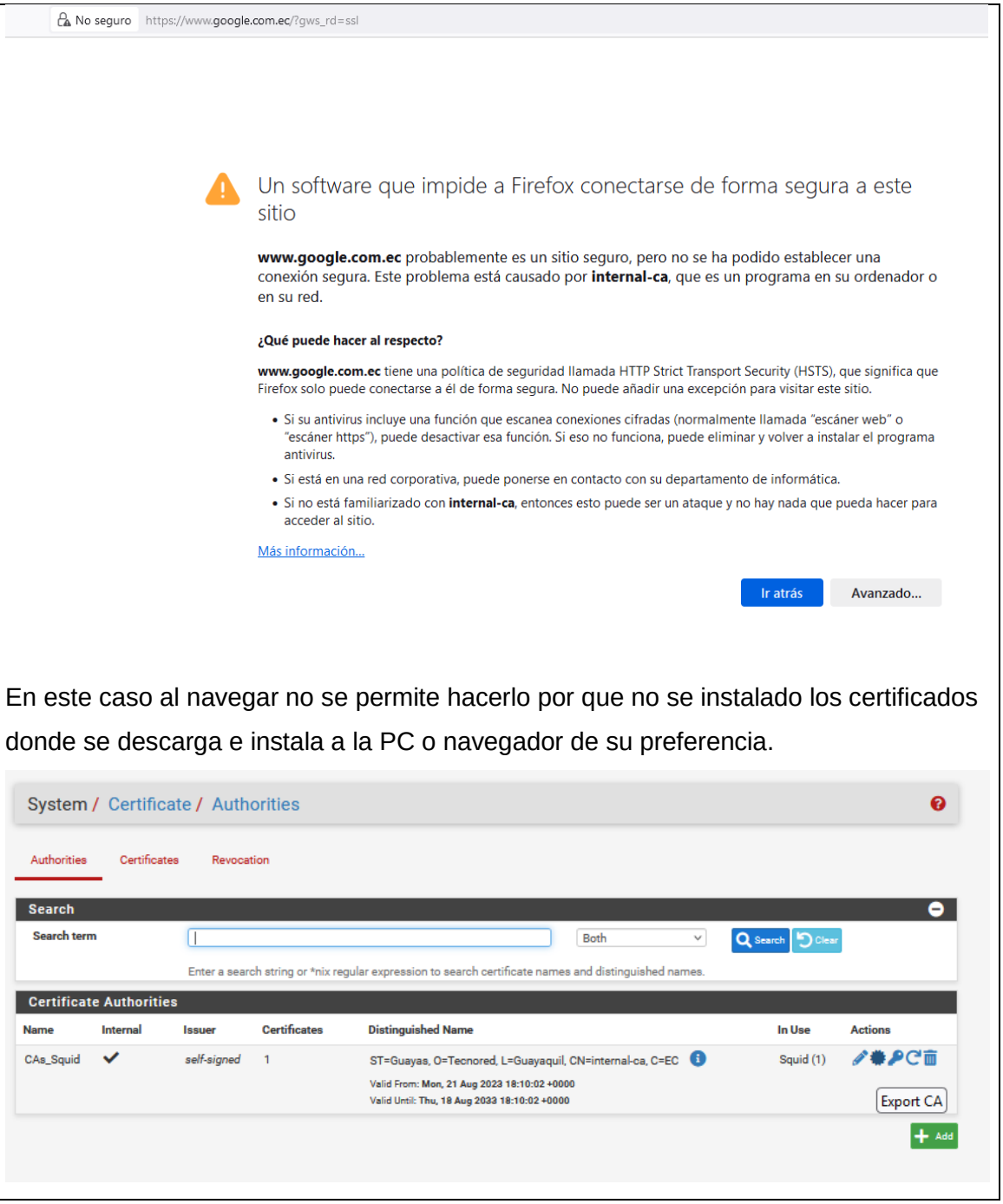


7. Configurar el squidguarden para lo que se aplicará en todo el la red y se activará a todos los logs y la blacklist.

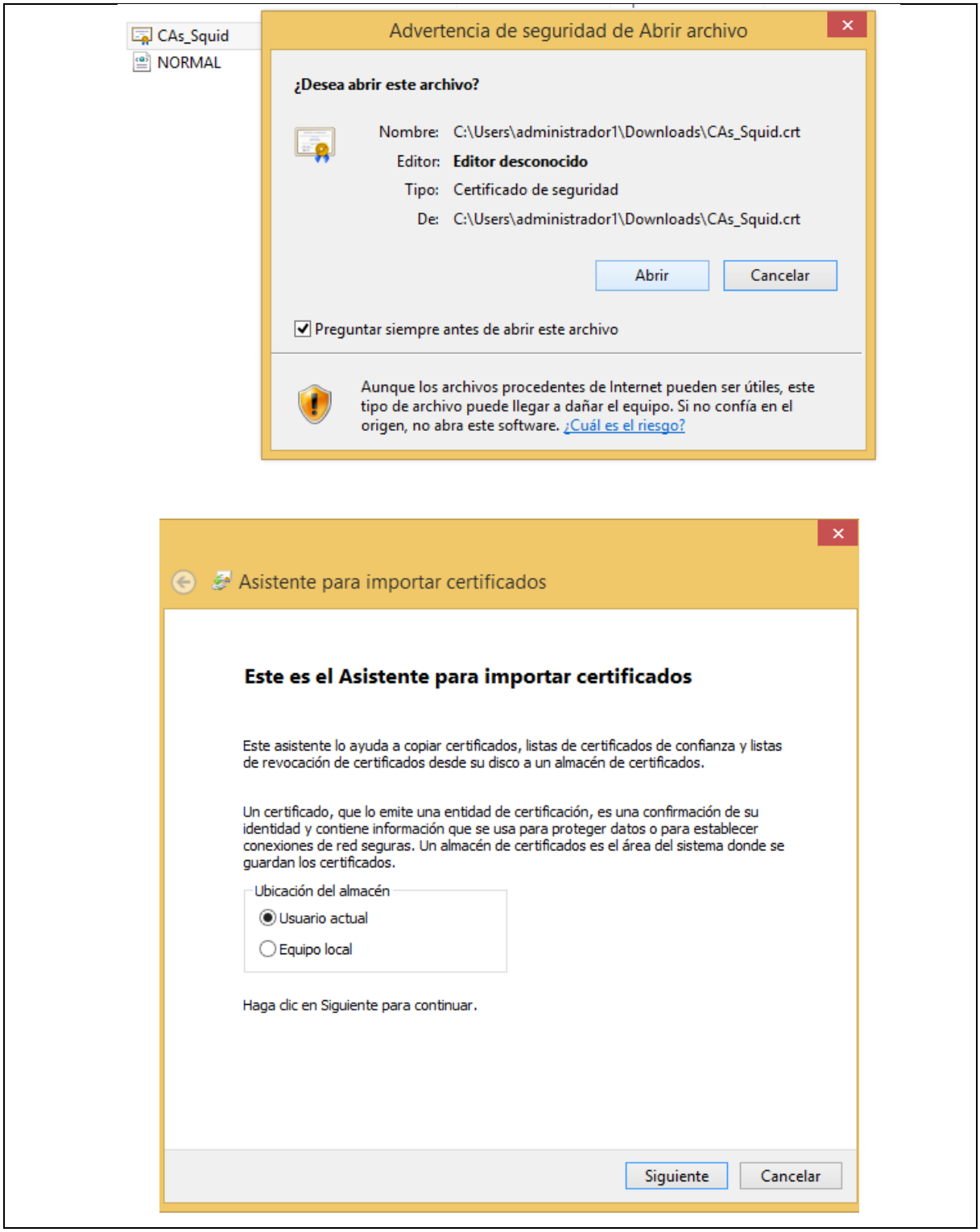

Package / Proxy filter SquidGuard: General settings / General settings
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
General Options
Enable
Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details.
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, the Apply button must be clicked.
Apply
SquidGuard service state: STOPPED
LDAP Options
Enable LDAP Filter
Enable options for setup ldap connection to create filters with ldap search
LDAP DN
Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)
LDAP DN Password
Password must be initialize with letters (Ex: Change123), valid format: [a-zA-Z\/][a-zA-Z0-9/_\-\.\/\:\%\+\?=&]
LDAP Cache Time
0
Number of seconds to cache LDAP Results (recommended value: 300)
Strip NT domain name
Strip NT domain name component from user names (/ or \ separated).
Strip Kerberos Realm
Strip Kerberos Realm component from user names (@ separated).
LDAP Version
Version 3
Service options
Rewrite process children
16
Maximum number of SquidGuard redirector processes that Squid may spawn. Using too few of these helper processes (a.k.a. "helpers") creates request queues. Using too many helpers wastes your system resources. (Default: 16)
Rewrite process children startup
8
Sets a minimum of how many SquidGuard processes are to be spawned when Squid starts or reconfigures. (Default: 8)
Rewrite process children idle
4
Sets a minimum of how many SquidGuard processes Squid is to try and keep available at all times. (Default: 4)
Logging options
Enable GUI log
Check this option to log the access to the Proxy Filter GUI.
Enable log
Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.
Enable log rotation
Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.
Miscellaneous
Clean Advertising
Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.
Blacklist options
Blacklist
Check this option to enable blacklist
Blacklist proxy
Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'
Blacklist URL
Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).
Save

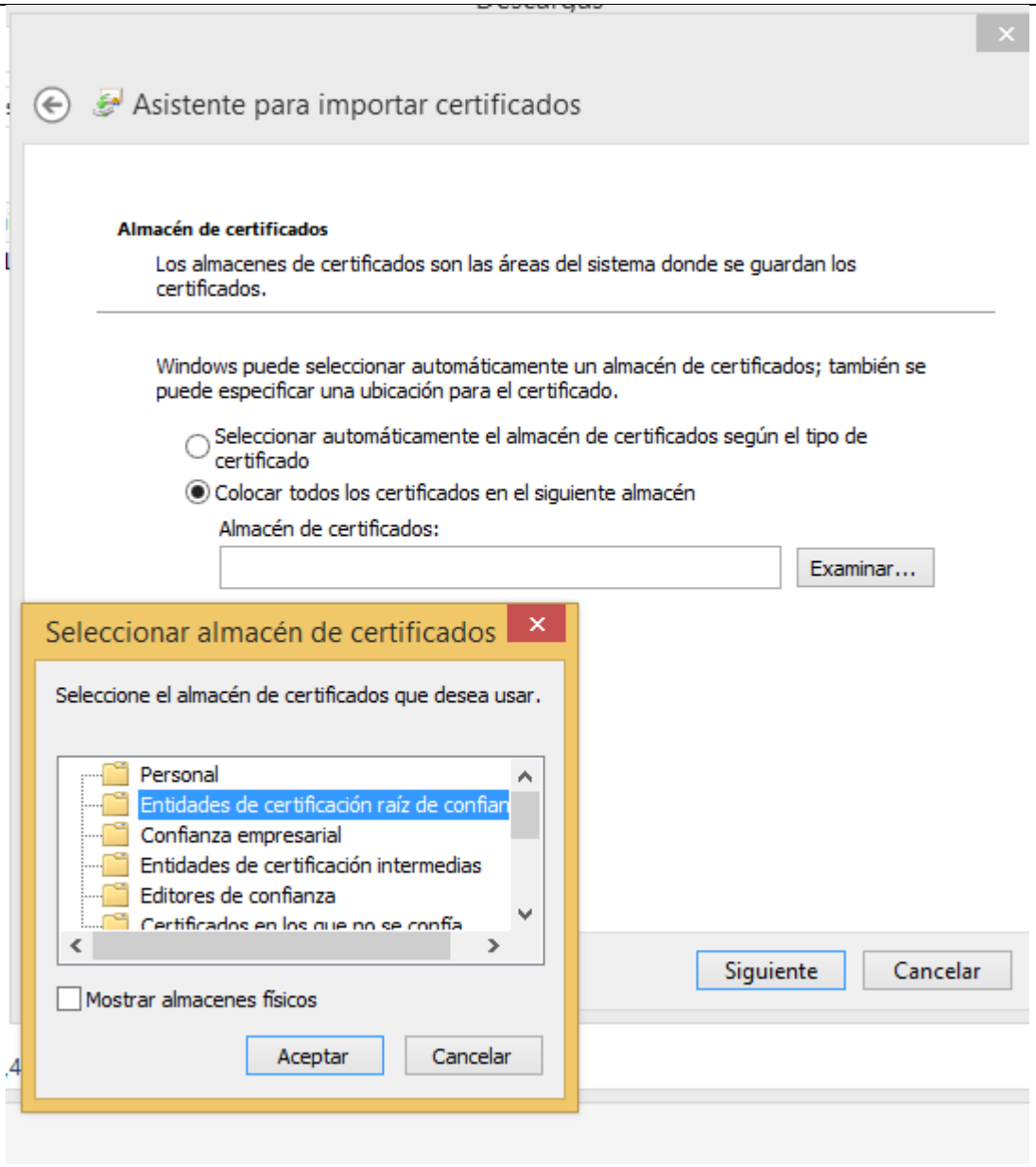
8. Se agrega un target en el common acl para realizar el primer bloqueo sin la instalación del certicado y se prueba navegación.



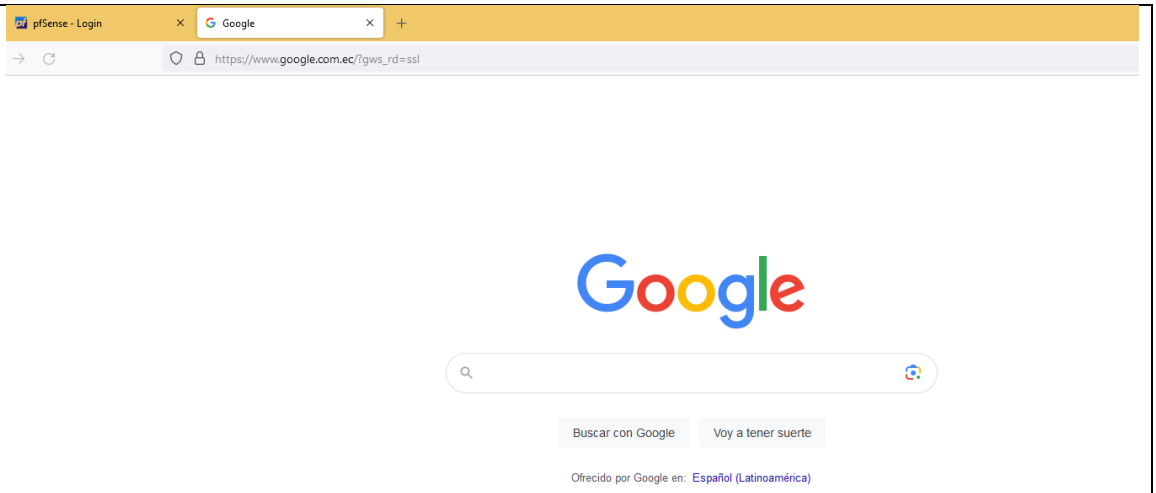


9. En este caso al navegar no se permite hacerlo por que no se instalado los certificados donde se descarga e instala a la PC o navegador de su preferencia.

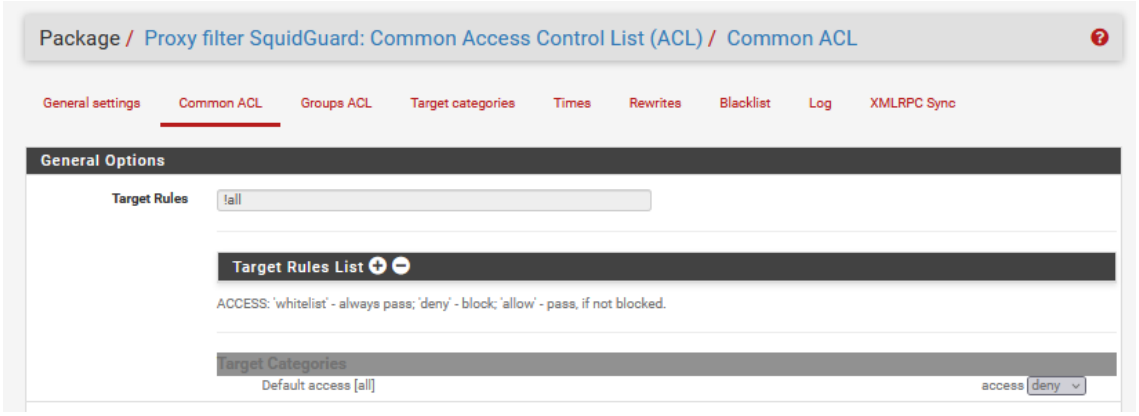

CAs_Squid
NORMAL
Advertencia de seguridad de Abrir archivo
¿Desea abrir este archivo?
Nombre: C:\Users\administrador1\Downloads\CAs_Squid.crt
Editor: Editor desconocido
Tipo: Certificado de seguridad
De: C:\Users\administrador1\Downloads\CAs_Squid.crt
Abrir
Cancelar
Preguntar siempre antes de abrir este archivo
Aunque los archivos procedentes de Internet pueden ser útiles, este tipo de archivo puede llegar a dañar el equipo. Si no confía en el origen, no abra este software. ¿Cuál es el riesgo?
Asistente para importar certificados
Este es el Asistente para importar certificados
Este asistente lo ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde su disco a un almacén de certificados.
Un certificado, que lo emite una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.
Ubicación del almacén
Usuario actual
Equipo local
Haga clic en Siguiente para continuar.
Siguiente
Cancelar

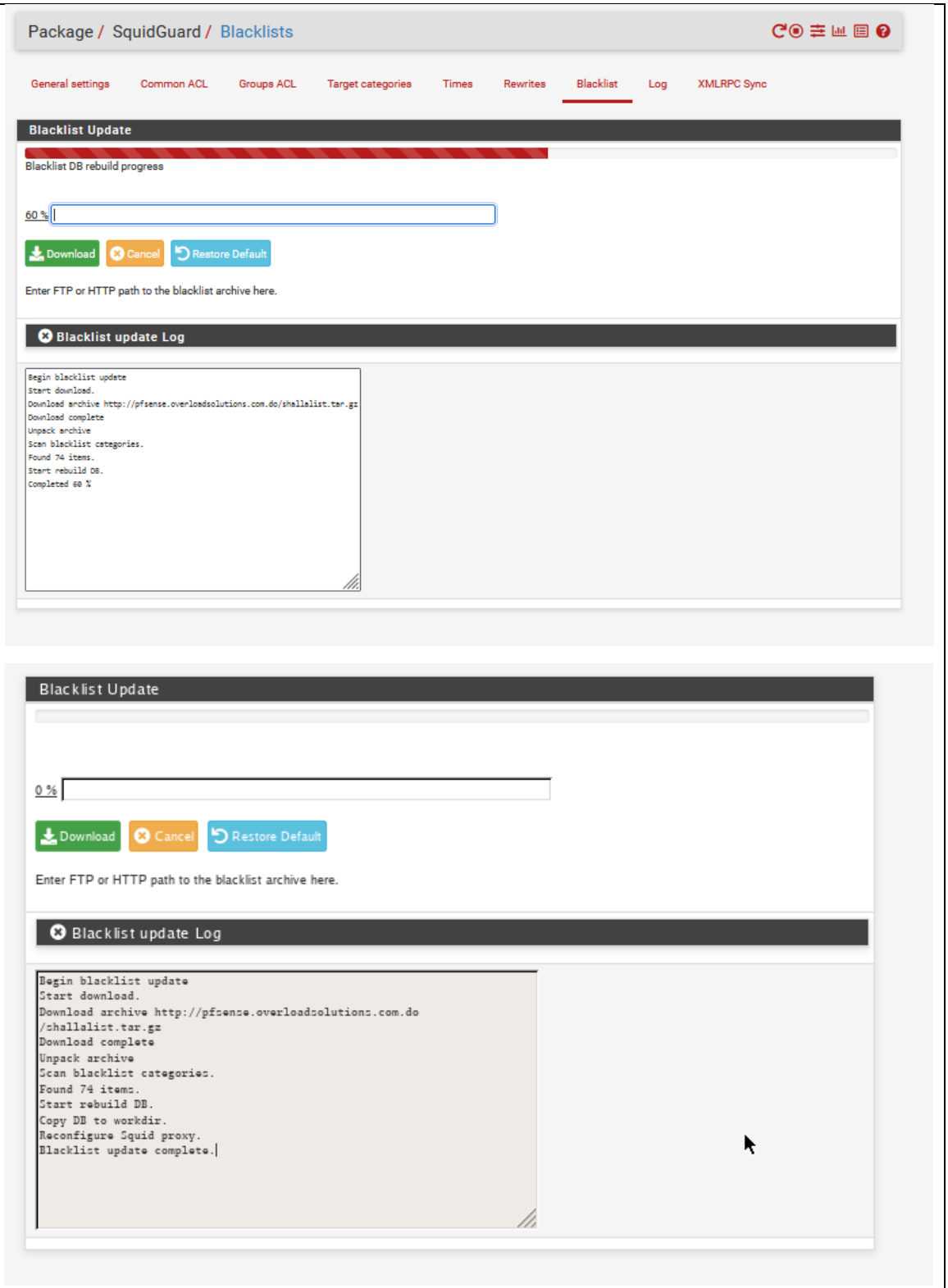


10. Una vez instalado el certificado del navegador y listo, comprobando que se dispondrá internet.

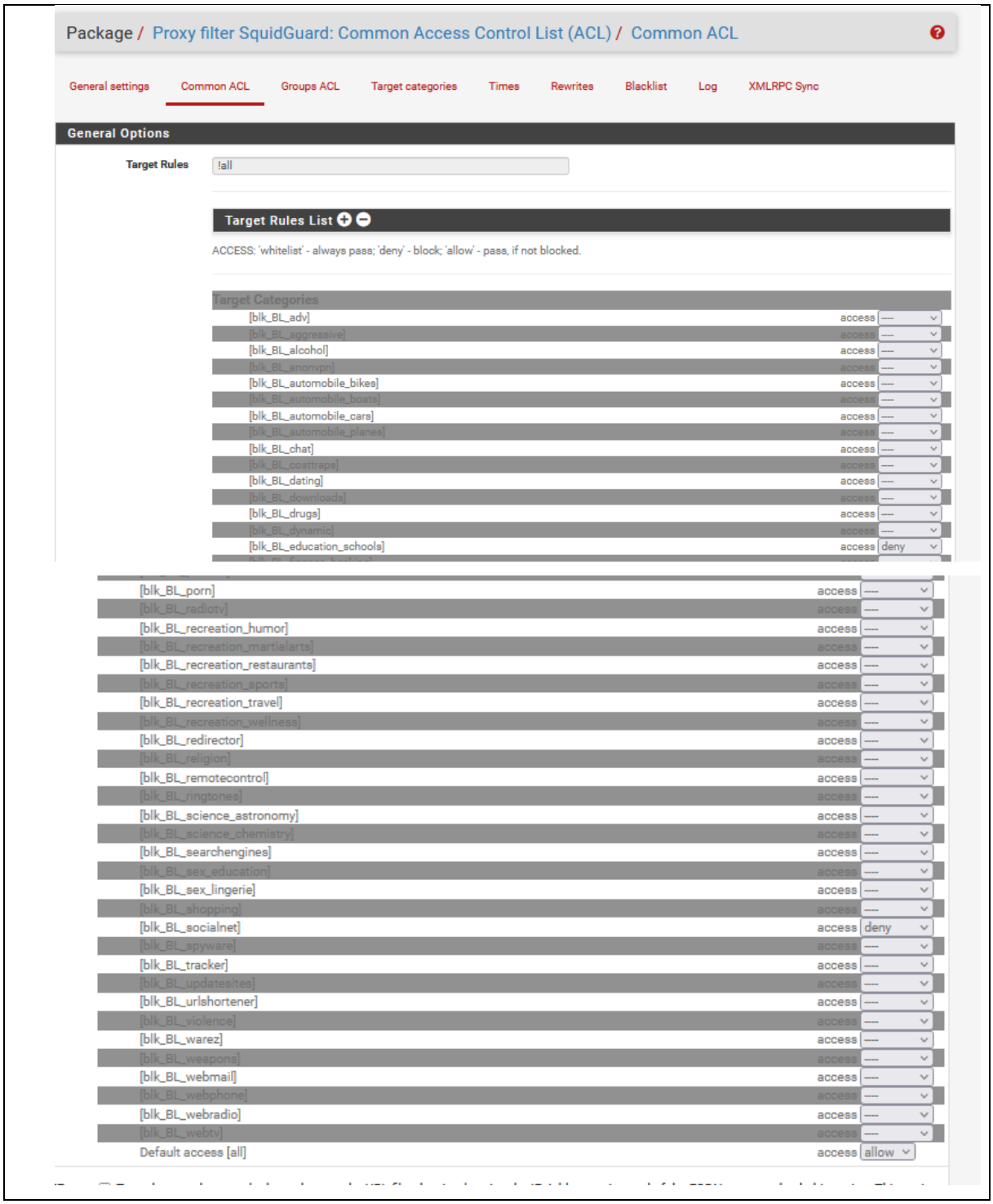


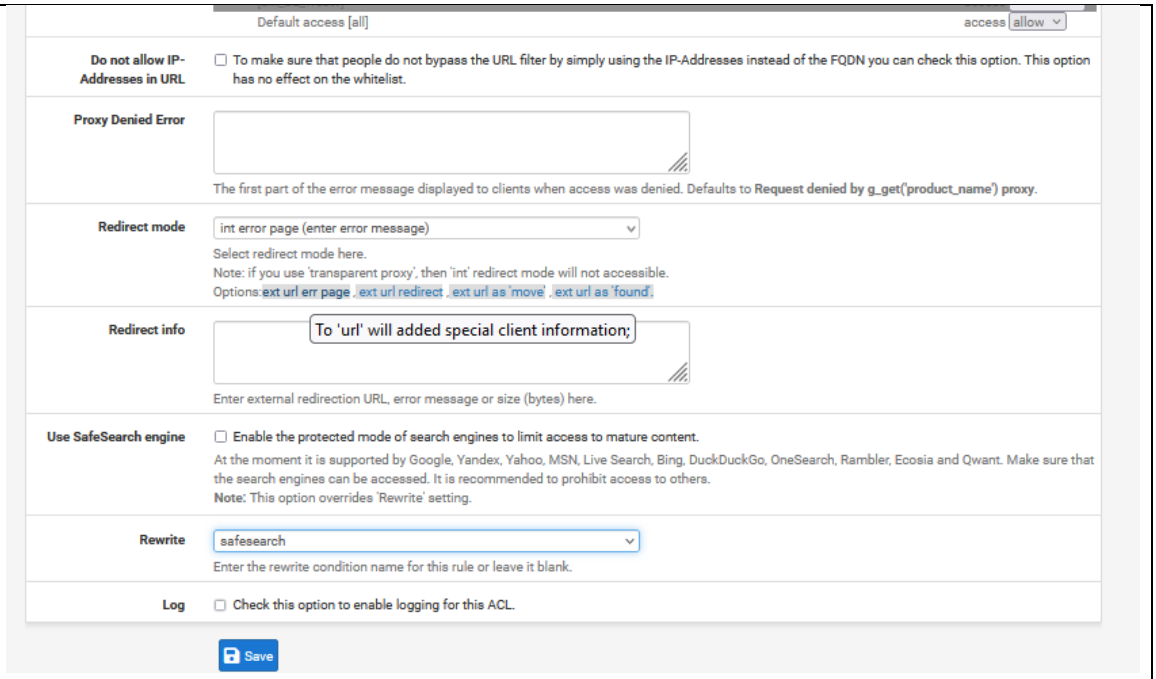
11. Se procede a paraer el servicio COMMON ACL para descargar la blacklist del siguiente enlace: http://pfsense.overloadsolutions.com.do/shallalist.tar.gz
12. Se instalará los bloqueos para las páginas web en todas las redes sociales, páginas educativas y donde de acuerdo a tus necesidades de tu red se irá bloqueando.



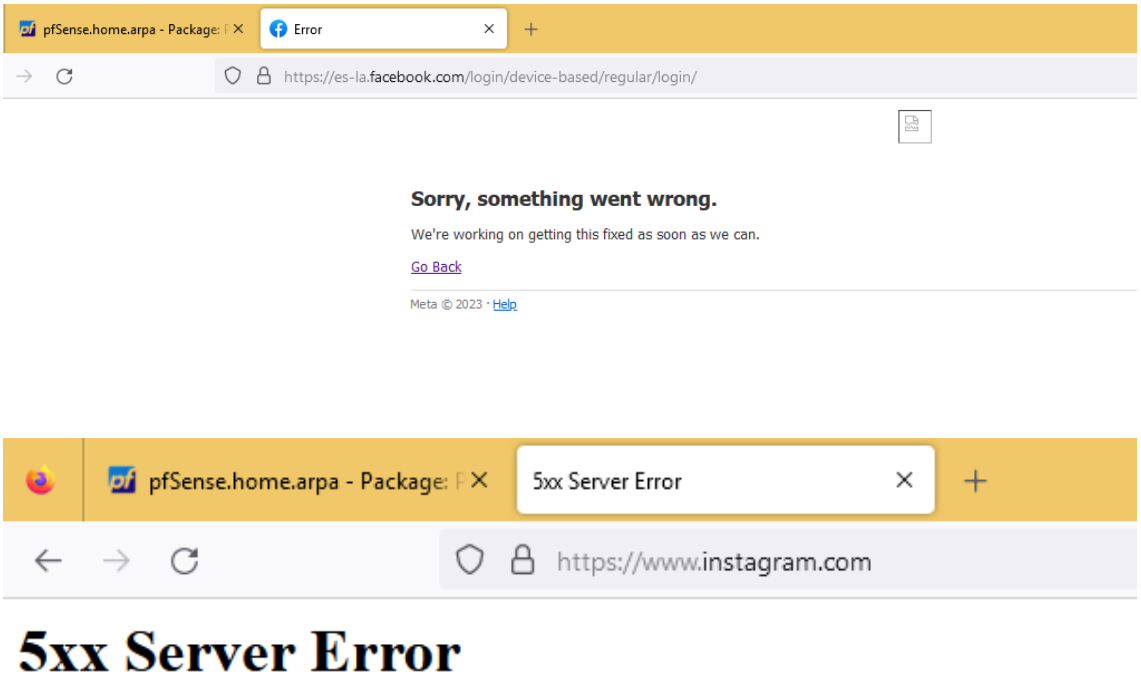


13. Una vez instalado se regresa a Comon ACL y saldrán todos los servicios que existen para bloque de páginas se gurada y se aplica los cambios.


Package / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL
General settings
Common ACL
Groups ACL
Target categories
Times
Rewrites
Blacklist
Log
XMLRPC Sync
General Options
Target Rules
!all
Target Rules List
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.
Target Categories
[blk_BL_adv] access ---
[blk_BL_aggressive] access ---
[blk_BL_alcohol] access ---
[blk_BL_anonvpn] access ---
[blk_BL_automobile_bikes] access ---
[blk_BL_automobile_boats] access ---
[blk_BL_automobile_cars] access ---
[blk_BL_automobile_planes] access ---
[blk_BL_chat] access ---
[blk_BL_costtraps] access ---
[blk_BL_dating] access ---
[blk_BL_downloads] access ---
[blk_BL_drugs] access ---
[blk_BL_dynamic] access ---
[blk_BL_education_schools] access deny
[blk_BL_porn] access ---
[blk_BL_radiotv] access ---
[blk_BL_recreation_humor] access ---
[blk_BL_recreation_martialarts] access ---
[blk_BL_recreation_restaurants] access ---
[blk_BL_recreation_sports] access ---
[blk_BL_recreation_travel] access ---
[blk_BL_recreation_wellness] access ---
[blk_BL_redirector] access ---
[blk_BL_religion] access ---
[blk_BL_remotecontrol] access ---
[blk_BL_ringtones] access ---
[blk_BL_science_astronomy] access ---
[blk_BL_science_chemistry] access ---
[blk_BL_searchengines] access ---
[blk_BL_sex_education] access ---
[blk_BL_sex_lingerie] access ---
[blk_BL_shopping] access ---
[blk_BL_socialnet] access deny
[blk_BL_spyware] access ---
[blk_BL_tracker] access ---
[blk_BL_updatesites] access ---
[blk_BL_urlshortener] access ---
[blk_BL_violence] access ---
[blk_BL_warez] access ---
[blk_BL_weapons] access ---
[blk_BL_webmail] access ---
[blk_BL_webphone] access ---
[blk_BL_webradio] access ---
[blk_BL_webtv] access ---
Default access [all] access allow



14. Una vez guardado se ingresa a las siguientes dirección Facebook, Instagram, twitter y páginas educativas recordar ir a general setting y darle clik en aplicar.



RESULTADO(S) OBTENIDO(S):

El estudiante se familiariza con la utilización de certificados HTTPS en el proceso de bloqueo ha permitido una mayor precisión en la identificación de los sitios web, incluso cuando se trata de conexiones seguras.

CONCLUSIONES:

El estudiante realiza la configuración de un sistema de bloqueo de páginas web HTTPS con certificado utilizando pfSense y las reglas de Squid Proxy y SquidGuard ha sido probado como una medida efectiva para controlar y gestionar el acceso a contenido web en una red.

RECOMENDACIONES:

Ejecutar varias configuraciones con páginas diferentes para el bloqueo de navegación y ejecutar destrezas.

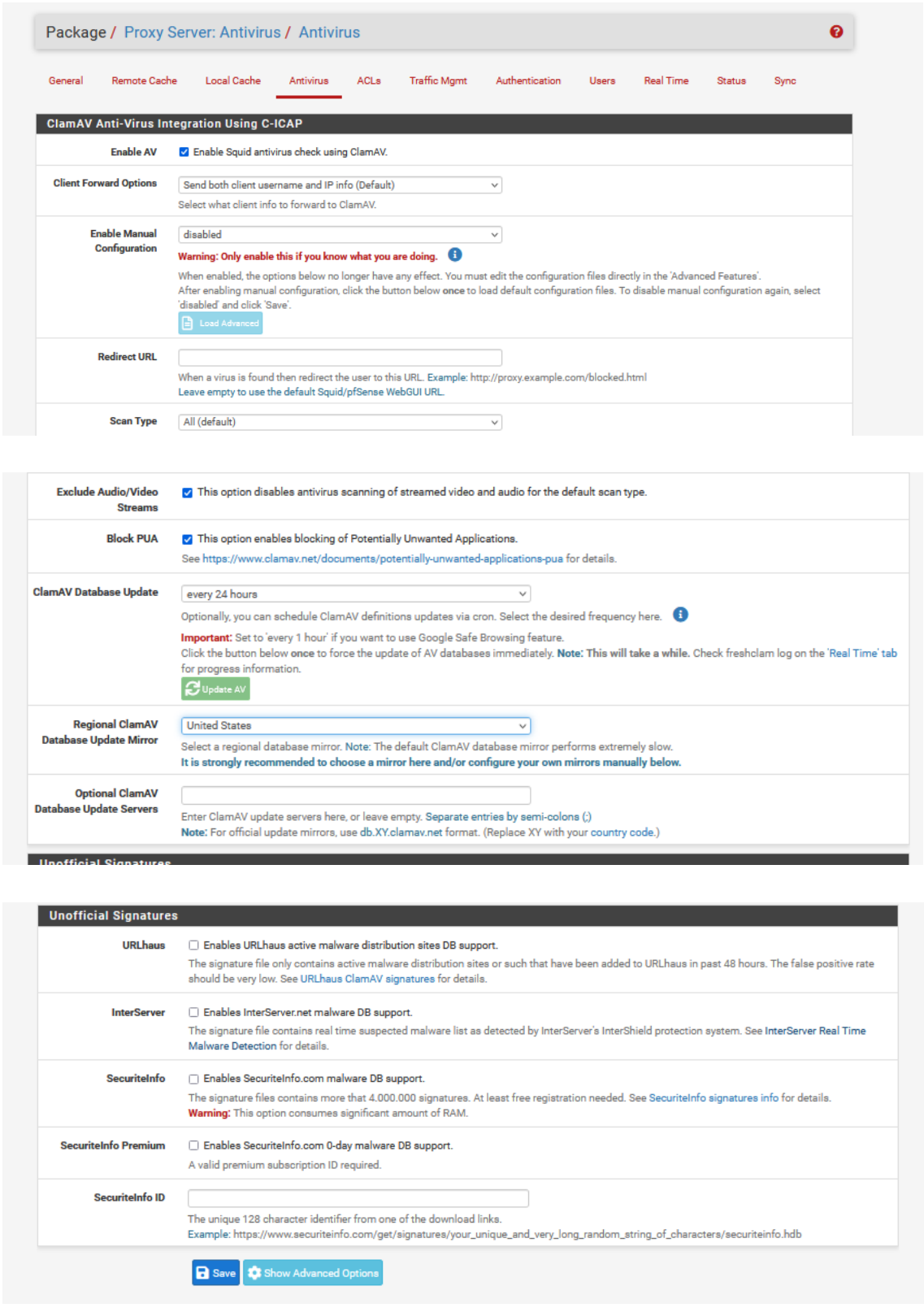
Docente: _____

Firma: _____

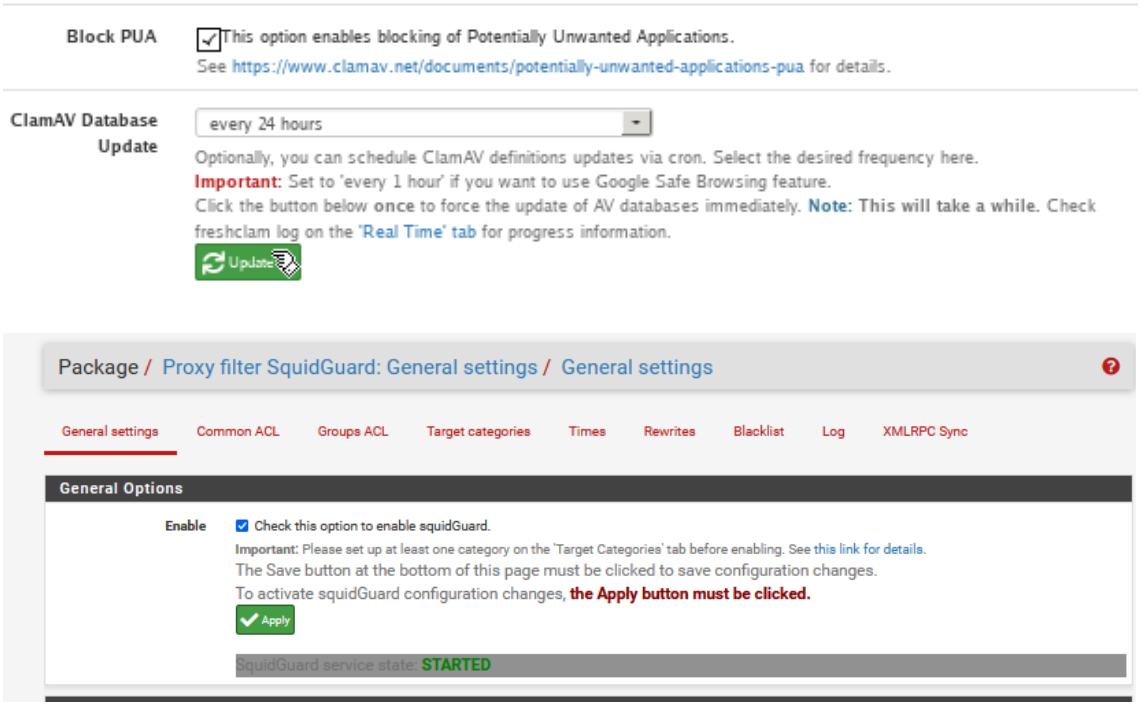
4.4. PRÁCTICA # 4

<table>
<tr><td colspan="2"> 
FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>Carrera: Ingeniería Electrónica</td><td>Asignatura: Redes de Computadoras</td></tr>
<tr><td>NRO. Práctica: 4</td><td>Título Práctica:
Configuración de un sistema antivirus para identificar la descarga de archivos comprometidos mediante el uso de un proxy Squid en pfSense</td></tr>
<tr><td colspan="2">OBJETIVO:
• Objetivo General
Configurar un sistema antivirus con el fin de detectar de manera efectiva la descarga de archivos infectados, utilizando un proxy Squid en la plataforma pfSense</td></tr>
<tr><td>INSTRUCCIONES:</td><td>1. Configurar e integrar el sistema antivirus seleccionado con el proxy Squid en pfSense, asegurando una comunicación fluida y segura.
2. Definir políticas y reglas de detección de archivos comprometidos en el sistema antivirus, considerando factores como tipo de archivos, extensiones y firmas maliciosas.
3. Establecer alertas y notificaciones para el equipo de administración de la red en caso de detección de descargas de archivos infectados.
4. Subir al AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta de la práctica realizada en clase.</td></tr>
<tr><td colspan="2">ACTIVIDADES POR DESARROLLAR</td></tr>
</table>

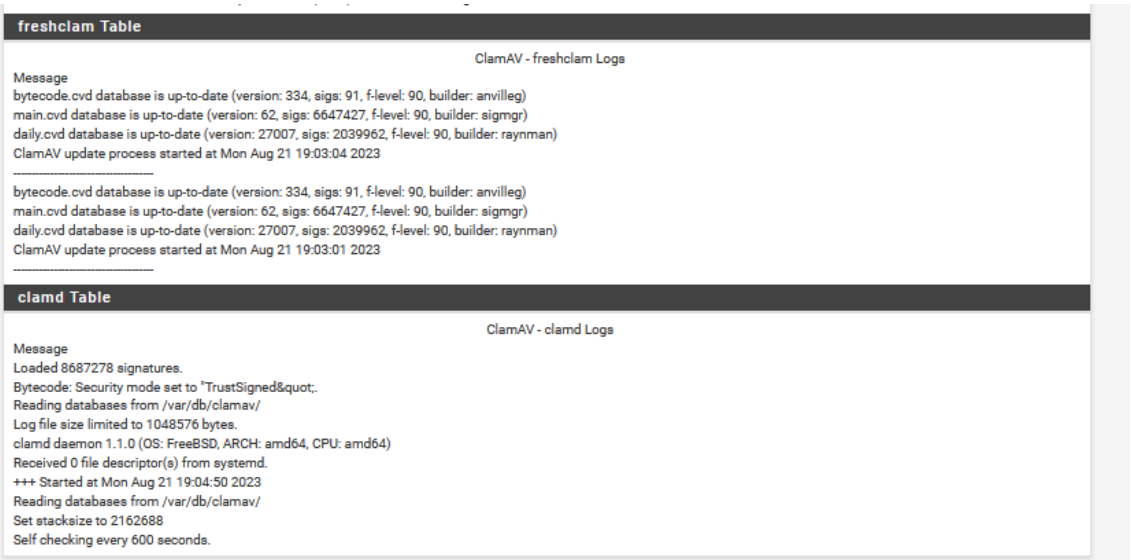
1. Para este práctica se usará el filtrado de antivuris donde el Pfsense detectará archivos que tengan algún malware.

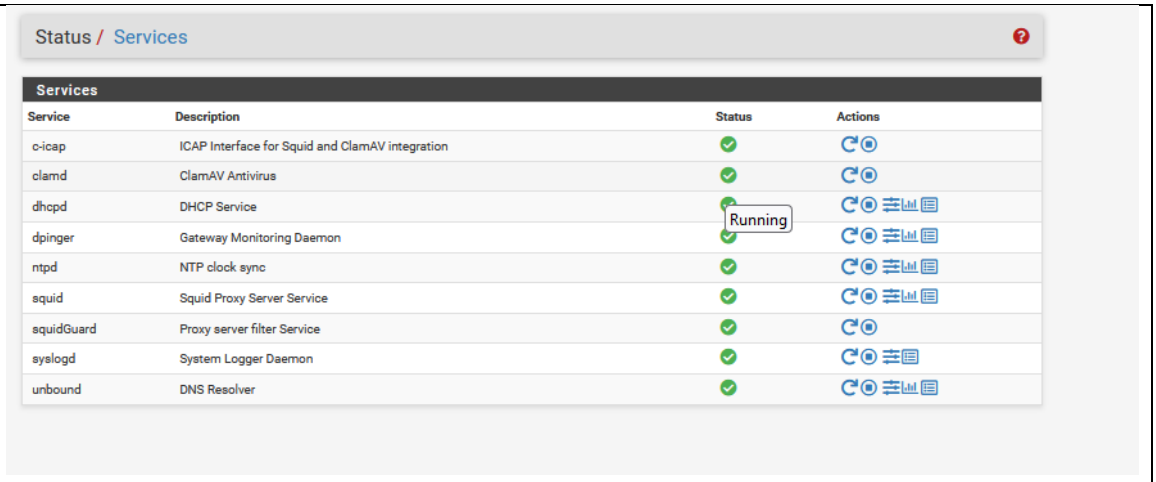


2. Una vez guardado se actualiza el ClamAv y otra vez en guardar y se regresa a general y le dando guardar dentro del Squid proxy y squidguard se ejectua aplicar para que lea el antivirus.

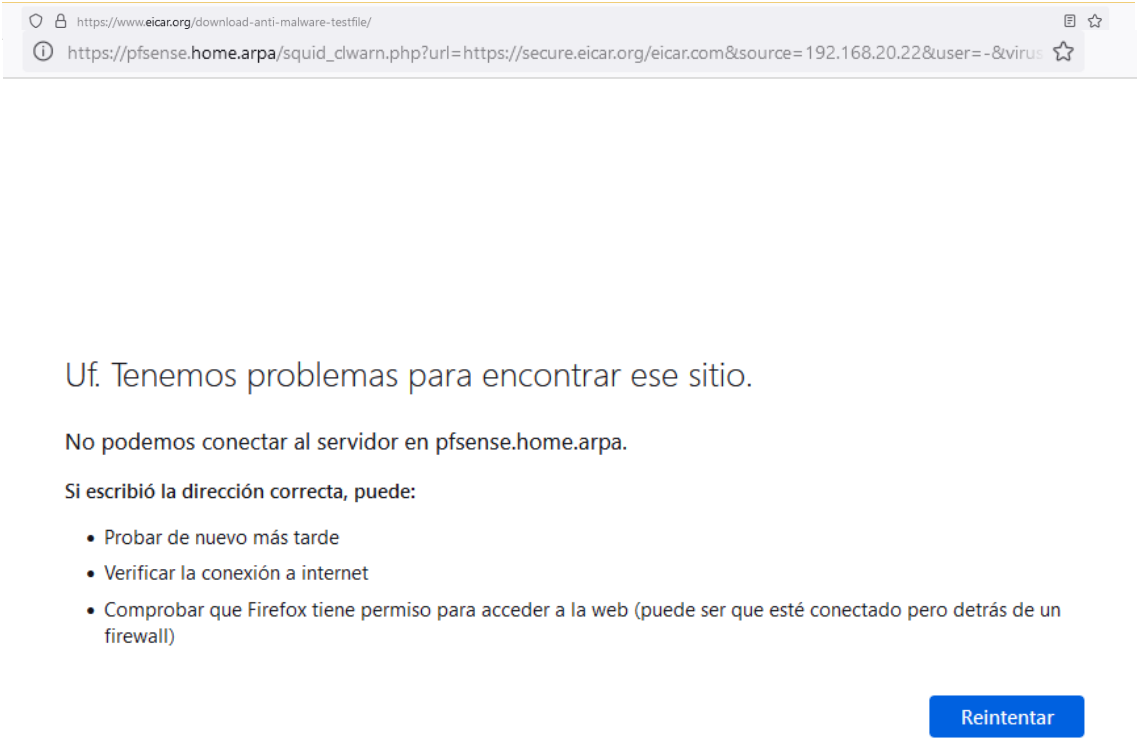


3. Ir a los estados de servicios para ver activo el servicio y podrecer a bajar un archivo que afecte a la red antes de realizar estos pasos se observará a realtime para ver si se ha actualizado la base.





4. Se ingresa a eicar test a traves del navegador y se selecciona cualquier malware y saltará el Pfsense avisando que se descargo un virus.



RESULTADO(S) OBTENIDO(S):

El estudiante configuró en pfSense un sistema antivirus para detectar de manera efectiva la descarga de archivos infectados.

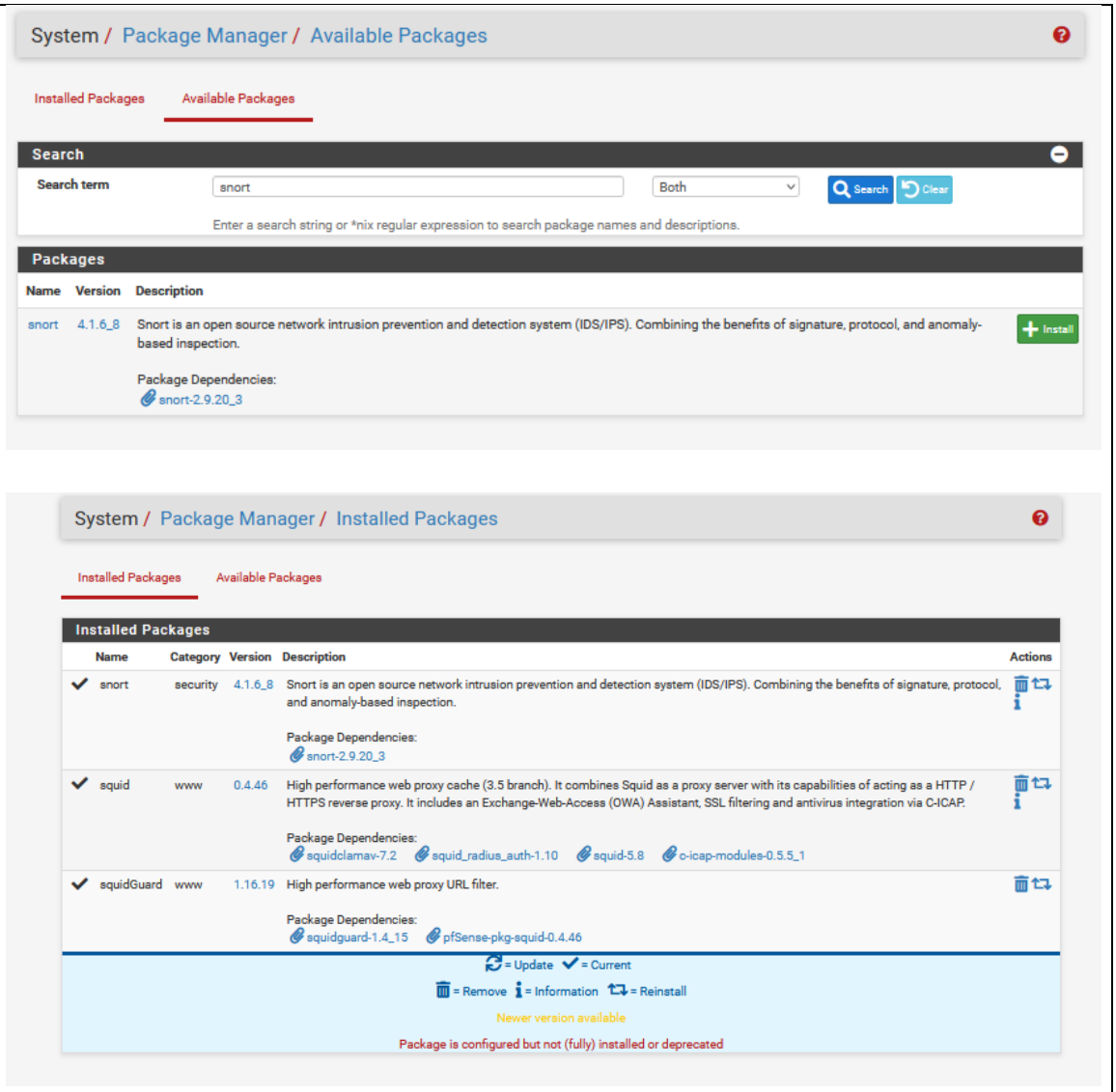
CONCLUSIONES:
E estudiante se familiariza con el sistema pfSense donde se configura el sistema antivirus para la detección de archivos maliciosos cuando se descarguen de la navegación que realice el usuario final.
RECOMENDACIONES:
Realiza pruebas exhaustivas en un entorno de laboratorio antes de implementar la solución en producción.

Docente: _____

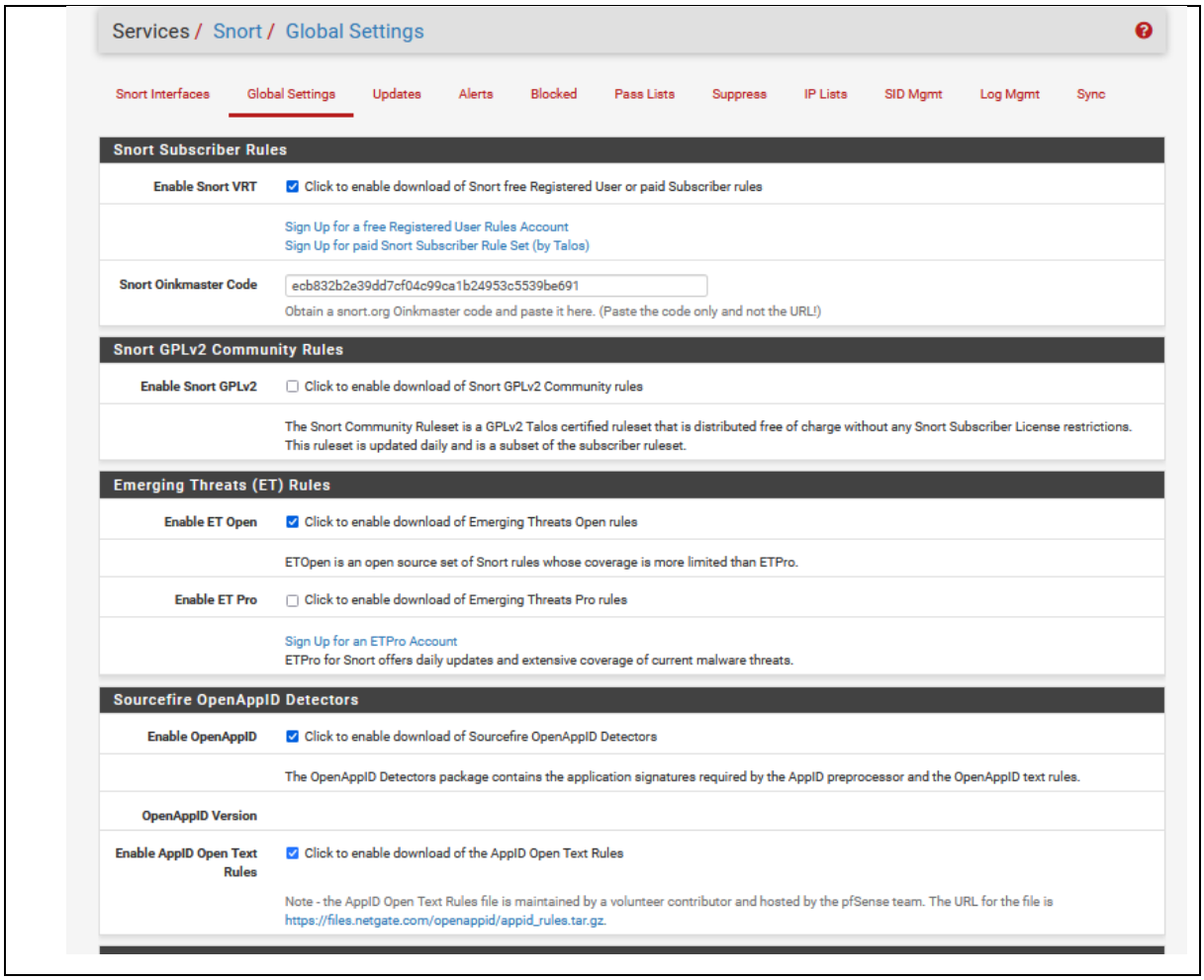
Firma: _____

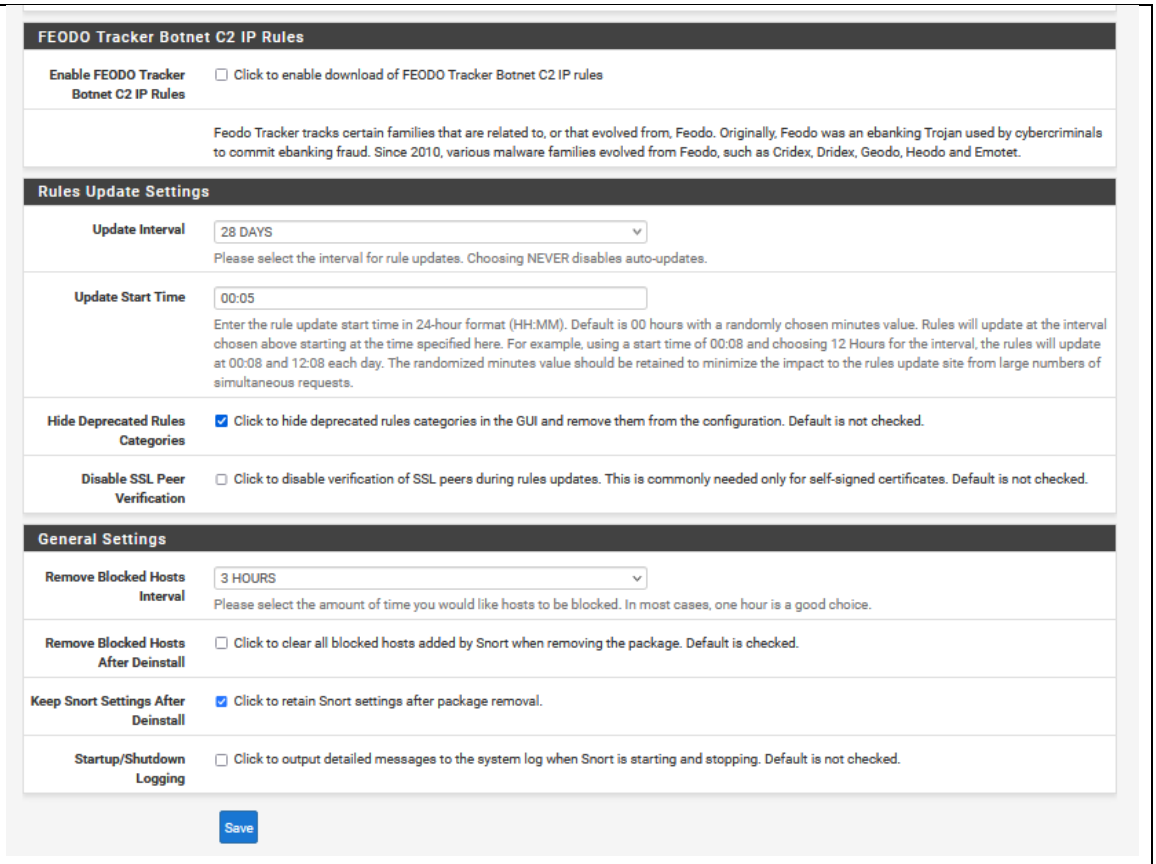
4.5. PRÁCTICA # 5

<table>
<tr><td colspan="2"> 
FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>Carrera: Ingeniería Electrónica</td><td>Asignatura: Redes de Computadoras</td></tr>
<tr><td>NRO. Práctica: 5</td><td>Título Práctica:
Implementación de un sistema de Detección y Prevención de Intrusiones (IDS/IPS) a través de la integración de Snort junto con la plataforma pfSense.</td></tr>
<tr><td colspan="2">OBJETIVO:
• Objetivo General
Identificar intrusiones y actividades anómalas en las primeras etapas, lo que permite una respuesta rápida para mitigar posibles amenazas.</td></tr>
<tr><td>INSTRUCCIONES:</td><td>1. Utilizar Snort para analizar el tráfico de red en tiempo real y detectar actividades maliciosas o sospechosas.
2. Configurar Snort para bloquear o alertar sobre actividades que coincidan con patrones de intrusión conocidos en la base de datos de reglas.
3. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.</td></tr>
<tr><td colspan="2">ACTIVIDADES POR DESARROLLAR</td></tr>
<tr><td colspan="2">1. Para la configuración de un sistema de detección de intruso se instalará los packages en el Pfsense.</td></tr>
</table>

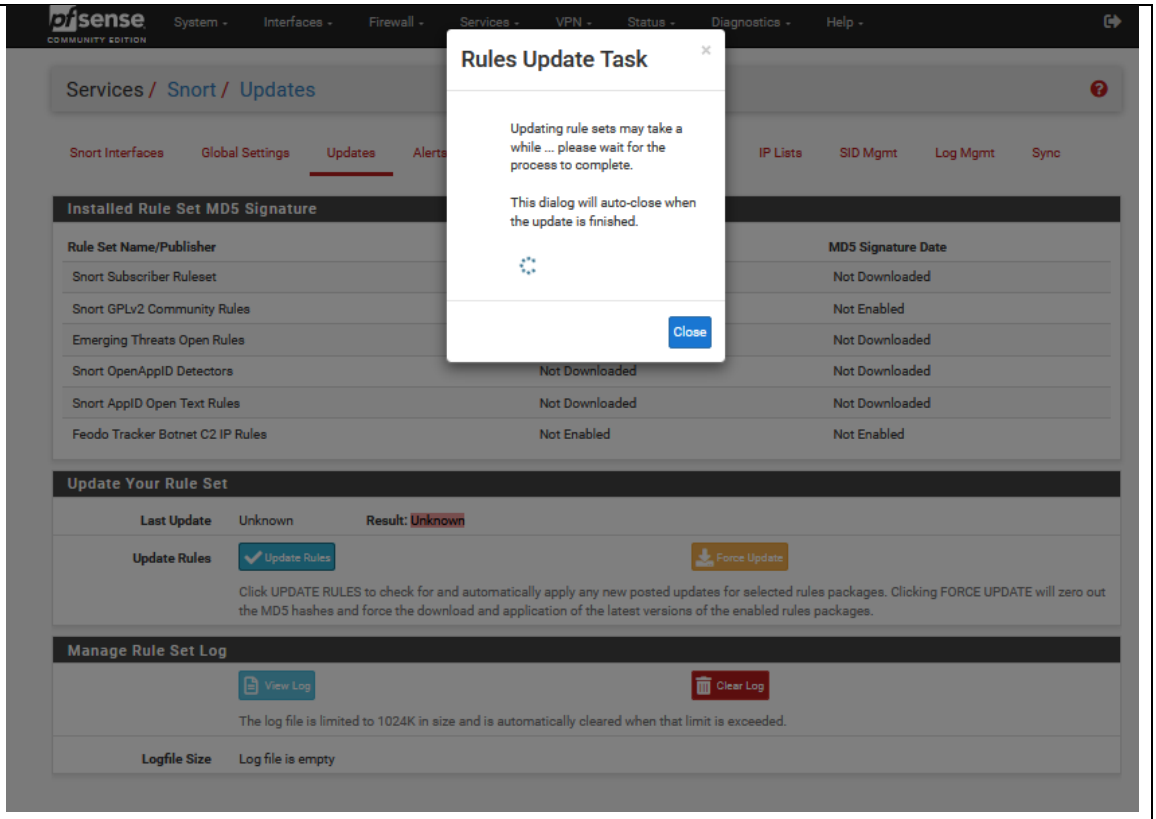


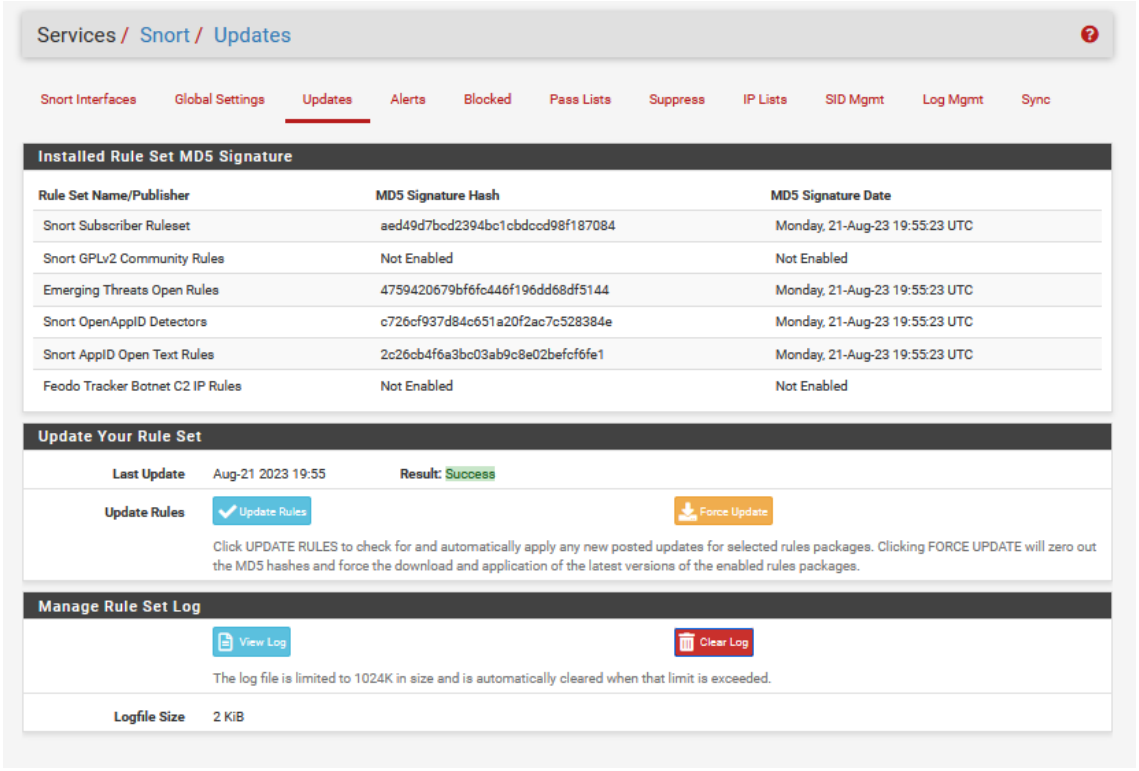
2. Una vez instalado, dirigirse a servicios snort en este caso se asigna a la interfaz Wan para la configuración debe elegir el snort Oikmaster registrándose en la página web de snort. En este caso el código es: ecb832b2e39dd7cf04c99ca1b24953c5539be691


Services / Snort / Global Settings
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Snort Subscriber Rules
Enable Snort VRT
Click to enable download of Snort free Registered User or paid Subscriber rules
Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)
Snort Oinkmaster Code
ecb832b2e39dd7cf04c99ca1b24953c5539be691
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)
Snort GPLv2 Community Rules
Enable Snort GPLv2
Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions.
This ruleset is updated daily and is a subset of the subscriber ruleset.
Emerging Threats (ET) Rules
Enable ET Open
Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
Enable ET Pro
Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.
Sourcefire OpenAppID Detectors
Enable OpenAppID
Click to enable download of Sourcefire OpenAppID Detectors
The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.
OpenAppID Version
Enable AppID Open Text Rules
Click to enable download of the AppID Open Text Rules
Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is
https://files.netgate.com/openappid/appid_rules.tar.gz.

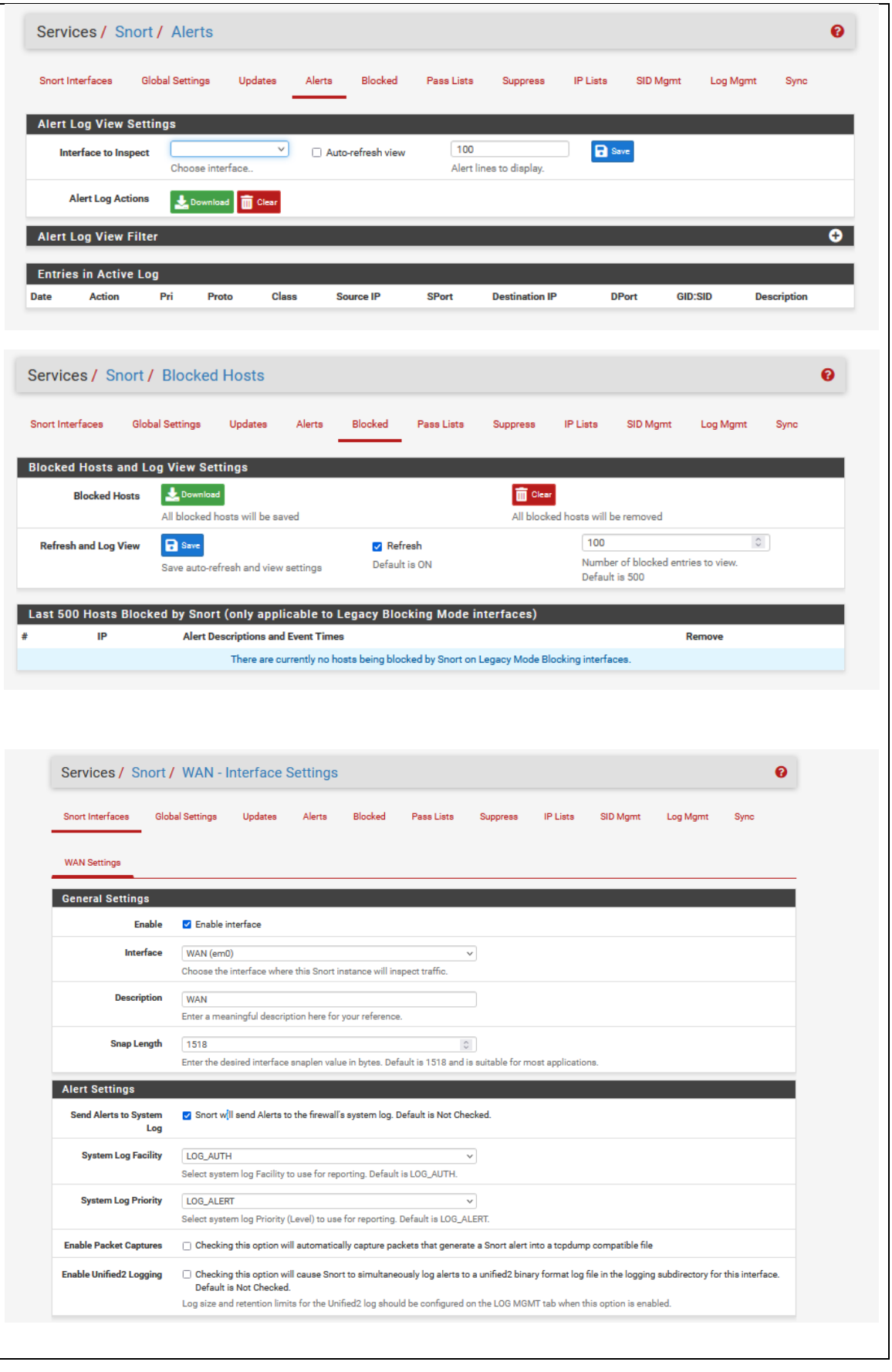


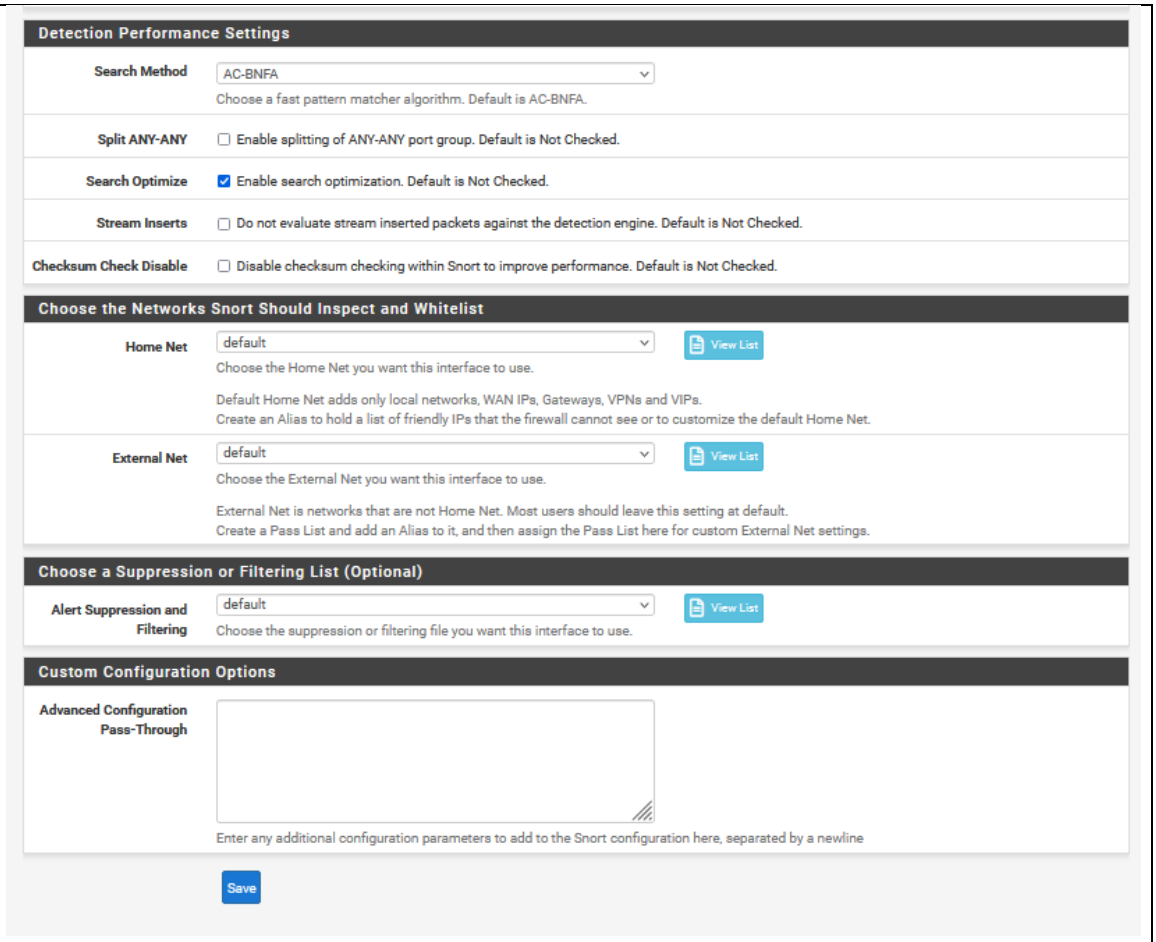
3. Dirigirse a Update para actualizar las reglas,



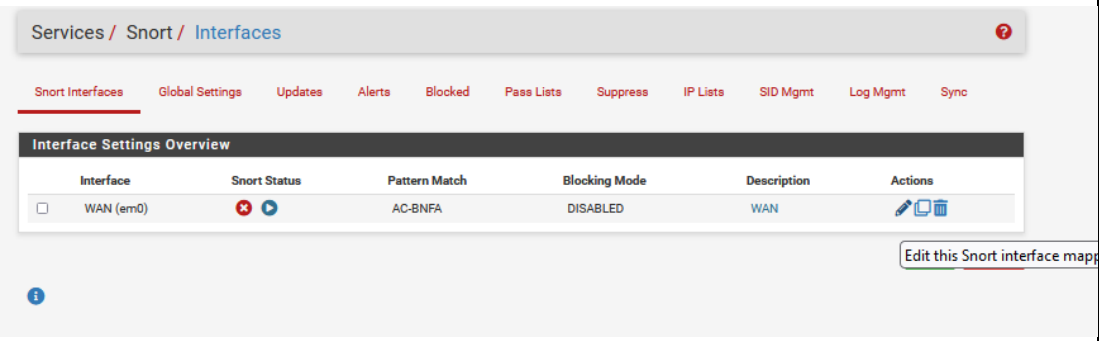


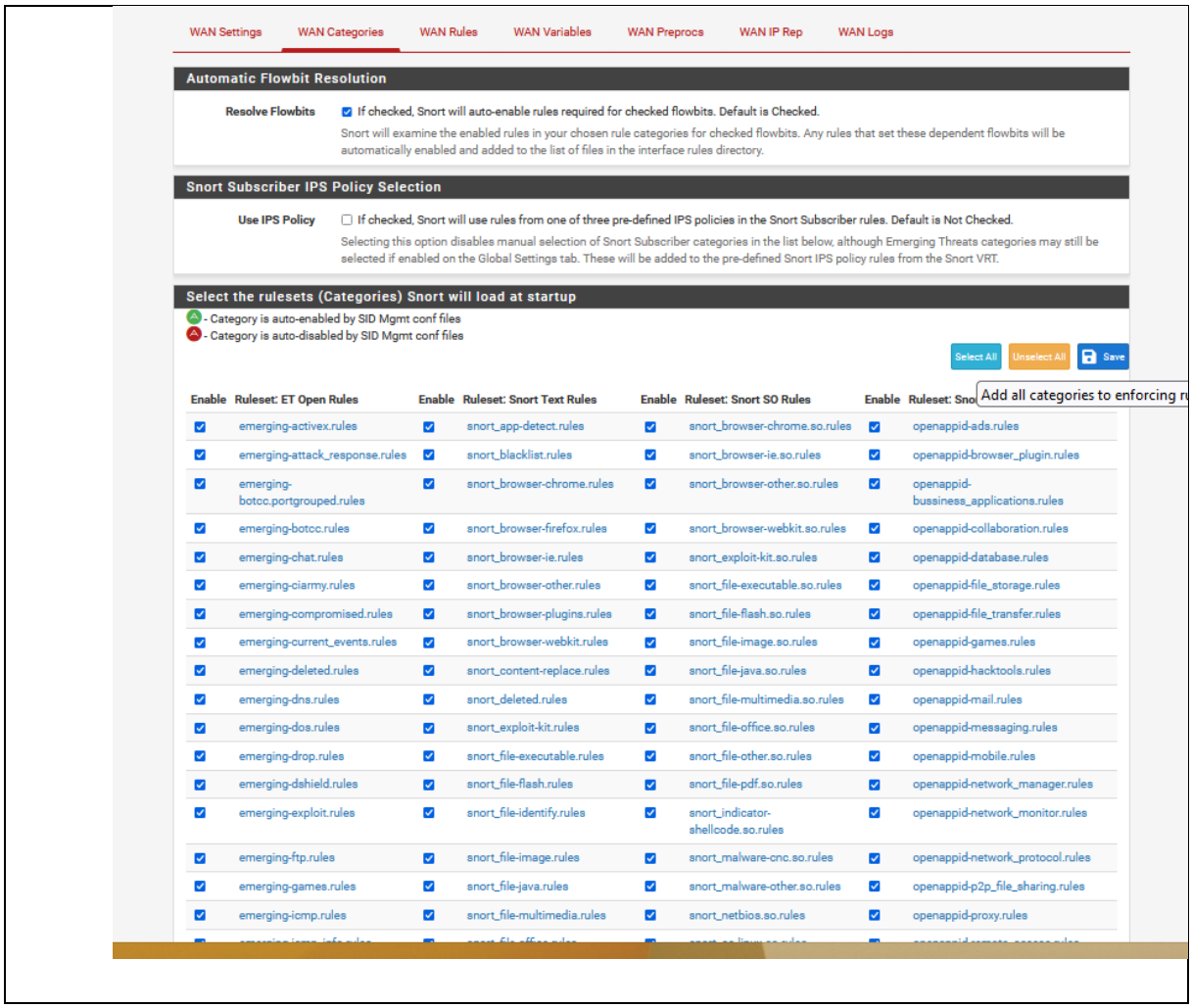
4. Se procede a configurar snort.

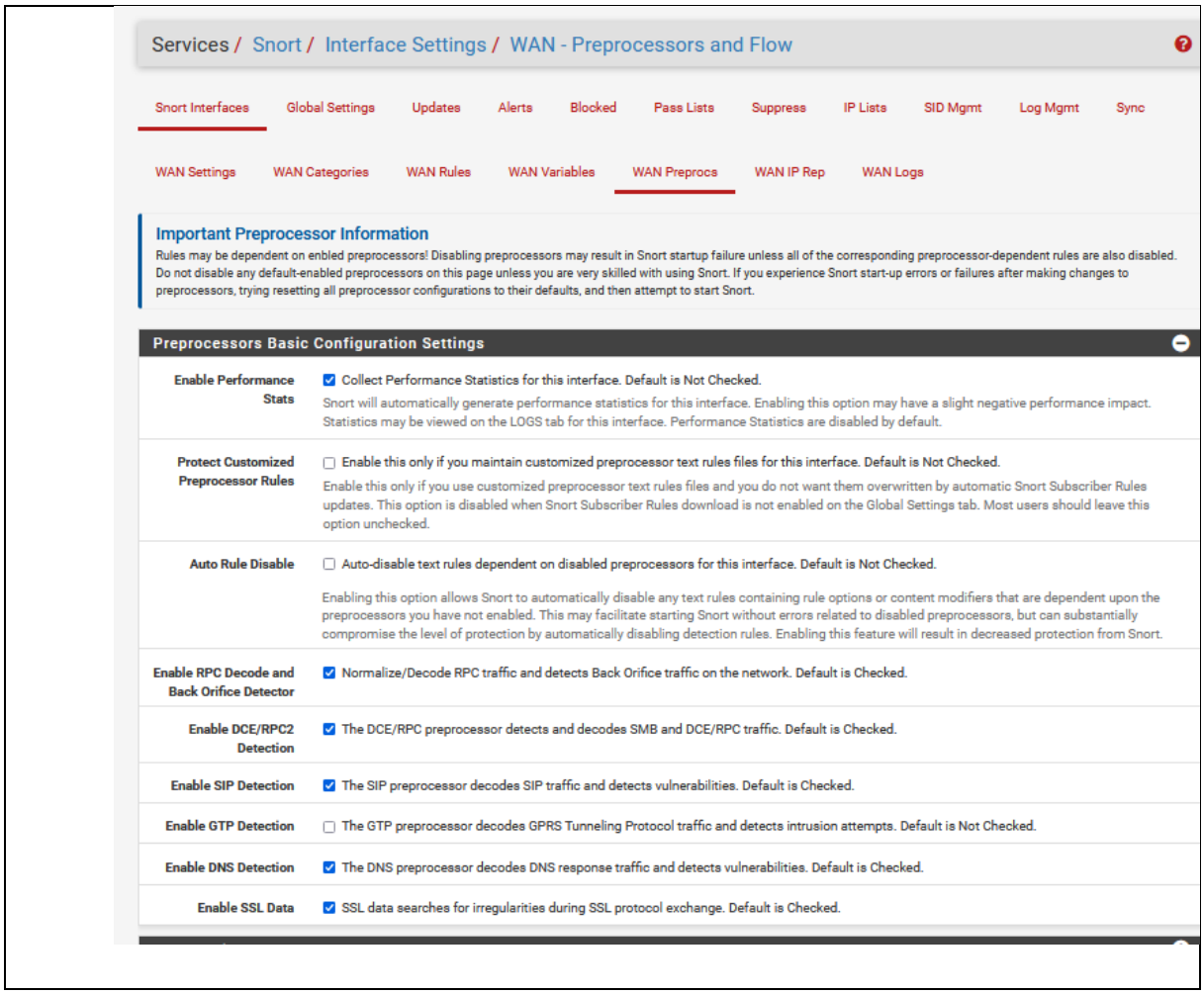

Services / Snort / Alerts
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Alert Log View Settings
Interface to Inspect
Choose interface..
Auto-refresh view
100
Alert lines to display.
Save
Alert Log Actions
Download
Clear
Alert Log View Filter
Entries in Active Log
Date
Action
Pri
Proto
Class
Source IP
SPort
Destination IP
DPort
GID:SID
Description
Services / Snort / Blocked Hosts
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Blocked Hosts and Log View Settings
Blocked Hosts
Download
All blocked hosts will be saved
Clear
All blocked hosts will be removed
Refresh and Log View
Save
Save auto-refresh and view settings
Refresh
Default is ON
100
Number of blocked entries to view.
Default is 500
Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)
#
IP
Alert Descriptions and Event Times
Remove
There are currently no hosts being blocked by Snort on Legacy Mode Blocking interfaces.
Services / Snort / WAN - Interface Settings
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
WAN Settings
General Settings
Enable
Enable interface
Interface
WAN (em0)
Choose the interface where this Snort instance will inspect traffic.
Description
WAN
Enter a meaningful description here for your reference.
Snap Length
1518
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.
Alert Settings
Send Alerts to System Log
Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility
LOG_AUTH
Select system log Facility to use for reporting. Default is LOG_AUTH.
System Log Priority
LOG_ALERT
Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Enable Packet Captures
Checking this option will automatically capture packets that generate a Snort alert into a topdump compatible file
Enable Unified2 Logging
Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

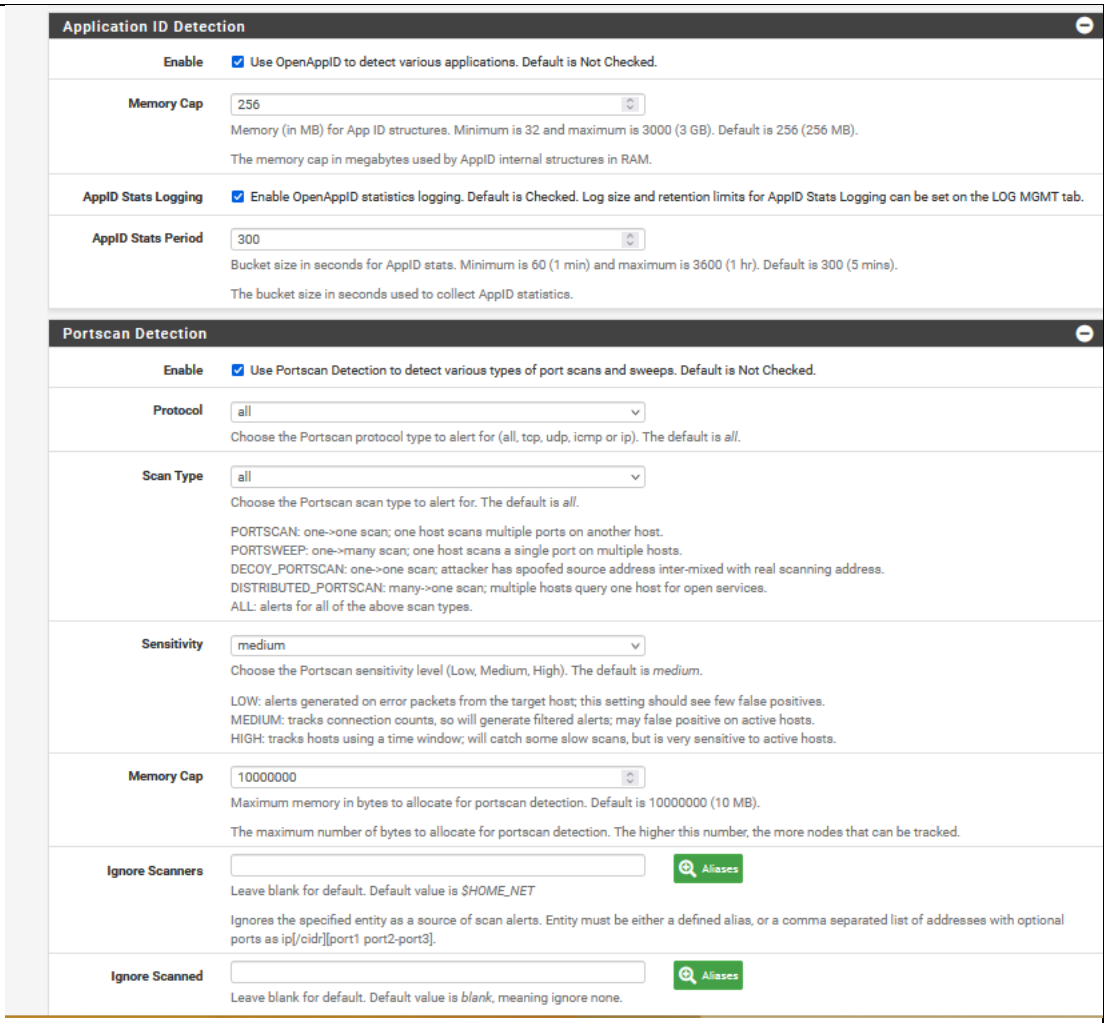


5. Una vez ya guardado, seleccionar en el lápiz para seguir configurando y seleccionando todas las reglas de categoria

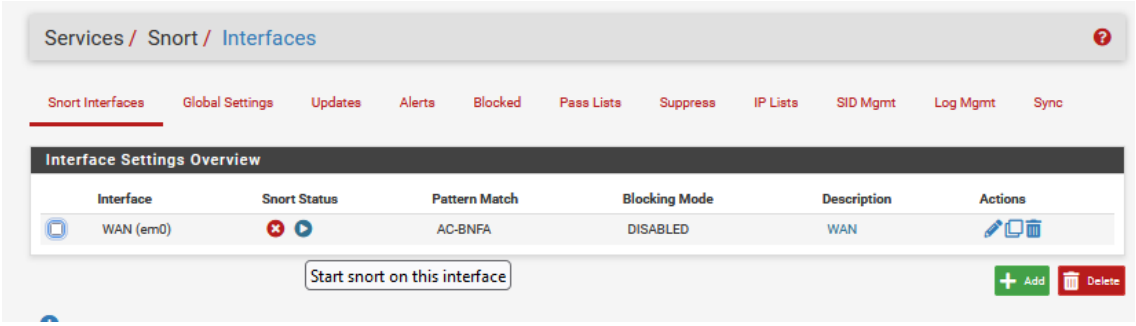


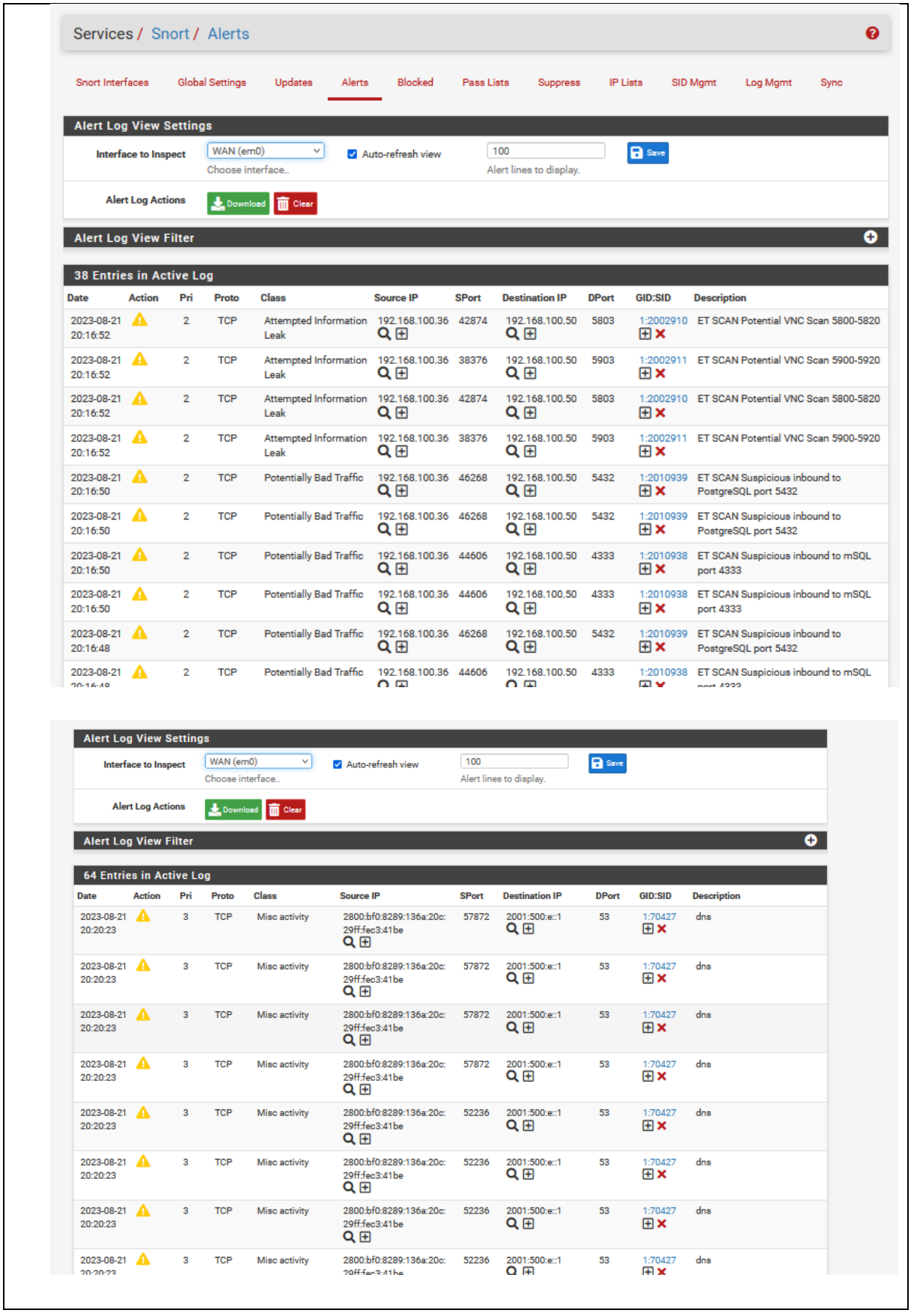

WAN Settings
WAN Categories
WAN Rules
WAN Variables
WAN Preprocs
WAN IP Rep
WAN Logs
Automatic Flowbit Resolution
Resolve Flowbits
If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.
Snort Subscriber IPS Policy Selection
Use IPS Policy
If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.
Select the rulesets (Categories) Snort will load at startup
- Category is auto-enabled by SID Mgmt conf files
- Category is auto-disabled by SID Mgmt conf files
Select All
Unselect All
Save
Add all categories to enforcing r
Enable
Ruleset: ET Open Rules
Enable
Ruleset: Snort Text Rules
Enable
Ruleset: Snort SO Rules
Enable
Ruleset: Sno
emerging-activex.rules
emerging-attack_response.rules
emerging-botcc.portgrouped.rules
emerging-botcc.rules
emerging-chat.rules
emerging-ciarmy.rules
emerging-compromised.rules
emerging-current_events.rules
emerging-deleted.rules
emerging-dns.rules
emerging-dos.rules
emerging-drop.rules
emerging-dshield.rules
emerging-exploit.rules
emerging-ftp.rules
emerging-games.rules
emerging-icmp.rules
snort_app-detect.rules
snort_blacklist.rules
snort_browser-chrome.rules
snort_browser-firefox.rules
snort_browser-ie.rules
snort_browser-other.rules
snort_browser-plugins.rules
snort_browser-webkit.rules
snort_content-replace.rules
snort_deleted.rules
snort_exploit-kit.rules
snort_file-executable.rules
snort_file-flash.rules
snort_file-identify.rules
snort_file-image.rules
snort_file-java.rules
snort_file-multimedia.rules
snort_browser-chrome.so.rules
snort_browser-ie.so.rules
snort_browser-other.so.rules
snort_browser-webkit.so.rules
snort_exploit-kit.so.rules
snort_file-executable.so.rules
snort_file-flash.so.rules
snort_file-image.so.rules
snort_file-java.so.rules
snort_file-multimedia.so.rules
snort_file-office.so.rules
snort_file-other.so.rules
snort_file-pdf.so.rules
snort_indicator-shellcode.so.rules
snort_malware-cnc.so.rules
snort_malware-other.so.rules
snort_netbios.so.rules
openappid-ads.rules
openappid-browser_plugin.rules
openappid-bussiness_applications.rules
openappid-collaboration.rules
openappid-database.rules
openappid-file_storage.rules
openappid-file_transfer.rules
openappid-games.rules
openappid-hacktools.rules
openappid-mail.rules
openappid-messaging.rules
openappid-mobile.rules
openappid-network_manager.rules
openappid-network_monitor.rules
openappid-network_protocol.rules
openappid-p2p_file_sharing.rules
openappid-proxy.rules


Services / Snort / Interface Settings / WAN - Preprocessors and Flow
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
WAN Settings
WAN Categories
WAN Rules
WAN Variables
WAN Preprocs
WAN IP Rep
WAN Logs
Important Preprocessor Information
Rules may be dependent on enbled preprocessors! Disabling preprocessors may result in Snort startup failure unless all of the corresponding preprocessor-dependent rules are also disabled. Do not disable any default-enabled preprocessors on this page unless you are very skilled with using Snort. If you experience Snort start-up errors or failures after making changes to preprocessors, trying resetting all preprocessor configurations to their defaults, and then attempt to start Snort.
Preprocessors Basic Configuration Settings
Enable Performance Stats
Collect Performance Statistics for this interface. Default is Not Checked.
Snort will automatically generate performance statistics for this interface. Enabling this option may have a slight negative performance impact. Statistics may be viewed on the LOGS tab for this interface. Performance Statistics are disabled by default.
Protect Customized Preprocessor Rules
Enable this only if you maintain customized preprocessor text rules files for this interface. Default is Not Checked.
Enable this only if you use customized preprocessor text rules files and you do not want them overwritten by automatic Snort Subscriber Rules updates. This option is disabled when Snort Subscriber Rules download is not enabled on the Global Settings tab. Most users should leave this option unchecked.
Auto Rule Disable
Auto-disable text rules dependent on disabled preprocessors for this interface. Default is Not Checked.
Enabling this option allows Snort to automatically disable any text rules containing rule options or content modifiers that are dependent upon the preprocessors you have not enabled. This may facilitate starting Snort without errors related to disabled preprocessors, but can substantially compromise the level of protection by automatically disabling detection rules. Enabling this feature will result in decreased protection from Snort.
Enable RPC Decode and Back Orifice Detector
Normalize/Decode RPC traffic and detects Back Orifice traffic on the network. Default is Checked.
Enable DCE/RPC2 Detection
The DCE/RPC preprocessor detects and decodes SMB and DCE/RPC traffic. Default is Checked.
Enable SIP Detection
The SIP preprocessor decodes SIP traffic and detects vulnerabilities. Default is Checked.
Enable GTP Detection
The GTP preprocessor decodes GPRS Tunneling Protocol traffic and detects intrusion attempts. Default is Not Checked.
Enable DNS Detection
The DNS preprocessor decodes DNS response traffic and detects vulnerabilities. Default is Checked.
Enable SSL Data
SSL data searches for irregularities during SSL protocol exchange. Default is Checked.

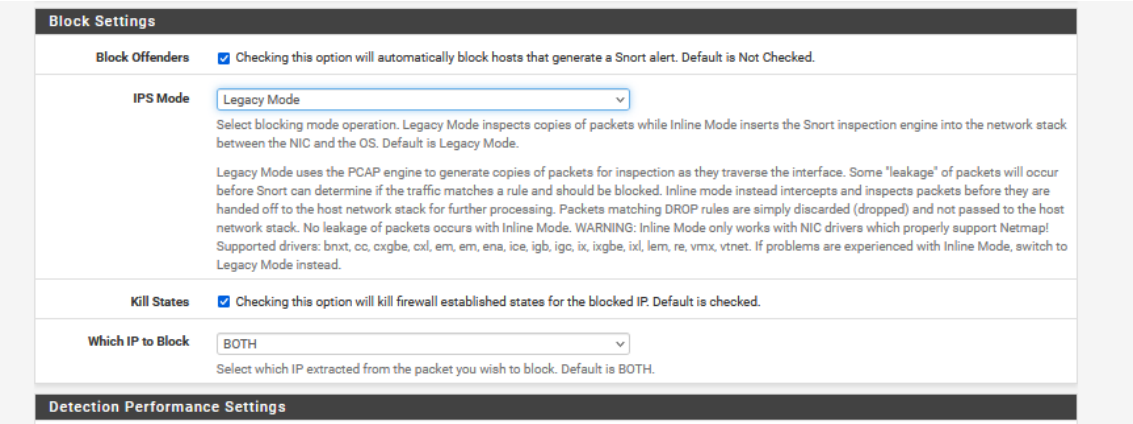


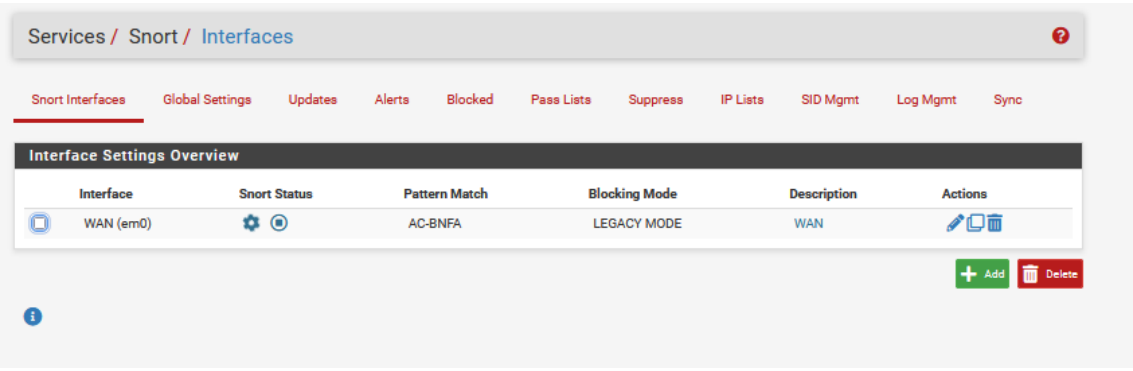
6. Ir a snort interfaces para darle iniciar y comienza a capturar ataques desde algun celular o pc, haciendo un escaneos de puerto.

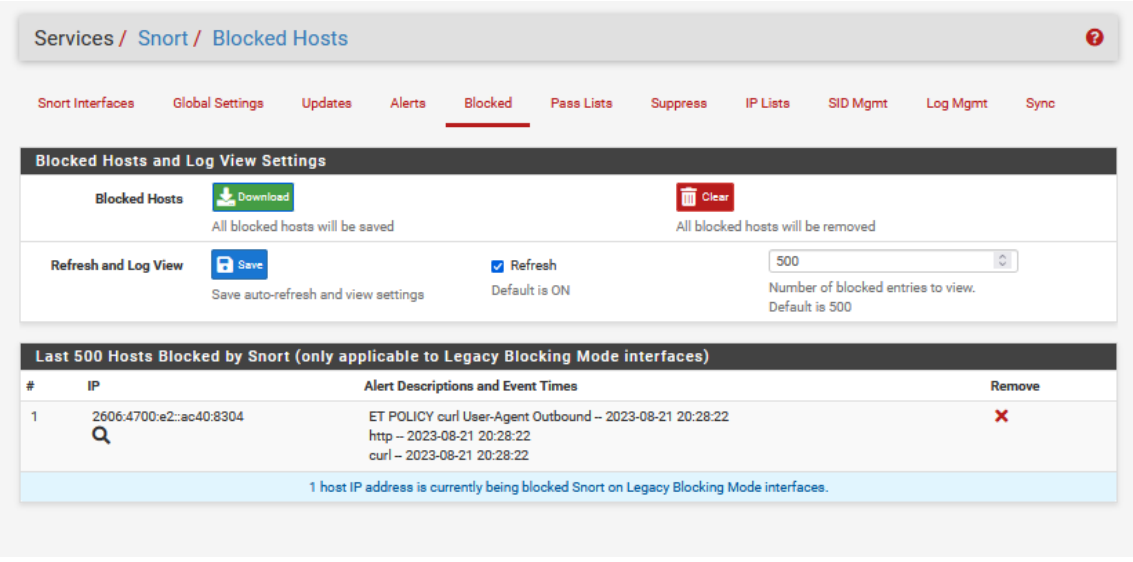



Services / Snort / Alerts
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Alert Log View Settings
Interface to Inspect
WAN (em0)
Choose interface..
Auto-refresh view
100
Alert lines to display.
Save
Alert Log Actions
Download
Clear
Alert Log View Filter
38 Entries in Active Log
Date Action Pri Proto Class Source IP SPort Destination IP DPort GID:SID Description
2023-08-21 20:16:52 2 TCP Attempted Information Leak 192.168.100.36 42874 192.168.100.50 5803 1:2002910 ET SCAN Potential VNC Scan 5800-5820
2023-08-21 20:16:52 2 TCP Attempted Information Leak 192.168.100.36 38376 192.168.100.50 5903 1:2002911 ET SCAN Potential VNC Scan 5900-5920
2023-08-21 20:16:52 2 TCP Attempted Information Leak 192.168.100.36 42874 192.168.100.50 5803 1:2002910 ET SCAN Potential VNC Scan 5800-5820
2023-08-21 20:16:52 2 TCP Attempted Information Leak 192.168.100.36 38376 192.168.100.50 5903 1:2002911 ET SCAN Potential VNC Scan 5900-5920
2023-08-21 20:16:50 2 TCP Potentially Bad Traffic 192.168.100.36 46268 192.168.100.50 5432 1:2010939 ET SCAN Suspicious inbound to PostgreSQL port 5432
2023-08-21 20:16:50 2 TCP Potentially Bad Traffic 192.168.100.36 46268 192.168.100.50 5432 1:2010939 ET SCAN Suspicious inbound to PostgreSQL port 5432
2023-08-21 20:16:50 2 TCP Potentially Bad Traffic 192.168.100.36 44606 192.168.100.50 4333 1:2010938 ET SCAN Suspicious inbound to mSQL port 4333
2023-08-21 20:16:50 2 TCP Potentially Bad Traffic 192.168.100.36 44606 192.168.100.50 4333 1:2010938 ET SCAN Suspicious inbound to mSQL port 4333
2023-08-21 20:16:48 2 TCP Potentially Bad Traffic 192.168.100.36 46268 192.168.100.50 5432 1:2010939 ET SCAN Suspicious inbound to PostgreSQL port 5432
2023-08-21 2 TCP Potentially Bad Traffic 192.168.100.36 44606 192.168.100.50 4333 1:2010938 ET SCAN Suspicious inbound to mSQL
Alert Log View Settings
Interface to Inspect
WAN (em0)
Choose interface..
Auto-refresh view
100
Alert lines to display.
Save
Alert Log Actions
Download
Clear
Alert Log View Filter
64 Entries in Active Log
Date Action Pri Proto Class Source IP SPort Destination IP DPort GID:SID Description
2023-08-21 20:20:23 3 TCP Misc activity 2800:bf0:8289:136a:20c:29ff:fec3:41be 57872 2001:500:e::1 53 1:70427 dns
2023-08-21 20:20:23 3 TCP Misc activity 2800:bf0:8289:136a:20c:29ff:fec3:41be 57872 2001:500:e::1 53 1:70427 dns
2023-08-21 20:20:23 3 TCP Misc activity 2800:bf0:8289:136a:20c:29ff:fec3:41be 57872 2001:500:e::1 53 1:70427 dns
2023-08-21 20:20:23 3 TCP Misc activity 2800:bf0:8289:136a:20c:29ff:fec3:41be 57872 2001:500:e::1 53 1:70427 dns
2023-08-21 20:20:23 3 TCP Misc activity 2800:bf0:8289:136a:20c:29ff:fec3:41be 52236 2001:500:e::1 53 1:70427 dns
2023-08-21 20:20:23 3 TCP Misc activity 2800:bf0:8289:136a:20c:29ff:fec3:41be 52236 2001:500:e::1 53 1:70427 dns
2023-08-21 20:20:23 3 TCP Misc activity 2800:bf0:8289:136a:20c:29ff:fec3:41be 52236 2001:500:e::1 53 1:70427 dns
2023-08-21 3 TCP Misc activity 2800:bf0:8289:136a:20c: 52236 2001:500:e::1 53 1:70427 dns

7. Entonces se bloquea todas las alertas y se activará el blocking mode donde en blacklist aparacerá blocked.







RESULTADO(S) OBTENIDO(S):

El estudiante realiza la configuración y el ajuste de un IDS/IPS implican comprender tanto las reglas de detección como las características de tu red

CONCLUSIONES:
Le estudiante configuró el sistema Snort para la detección de intrusos.
RECOMENDACIONES:
Debe monitorear regularmente los registros de Snort, analizar los eventos detectados y ajustar las reglas según los patrones de tráfico observados**.**

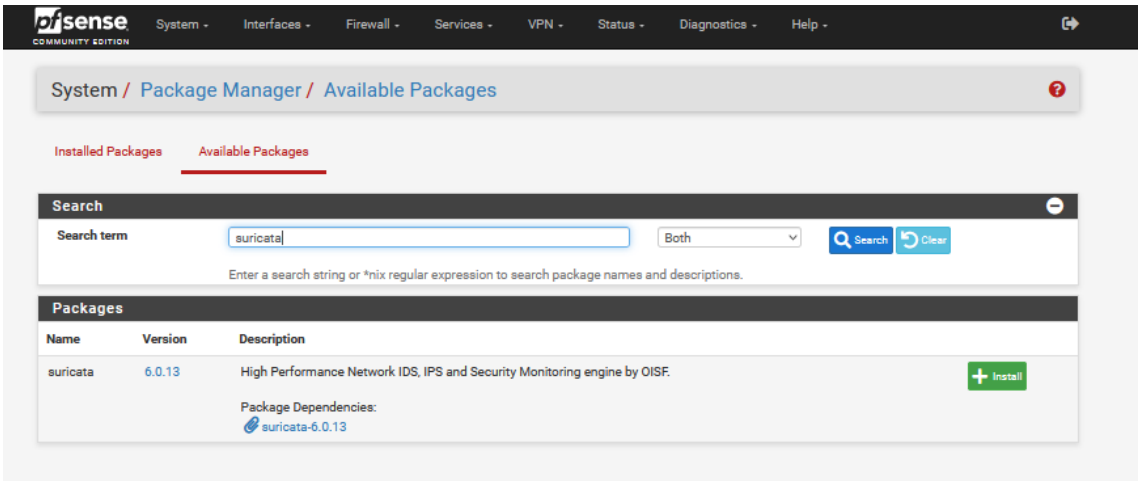
Docente: **_____**

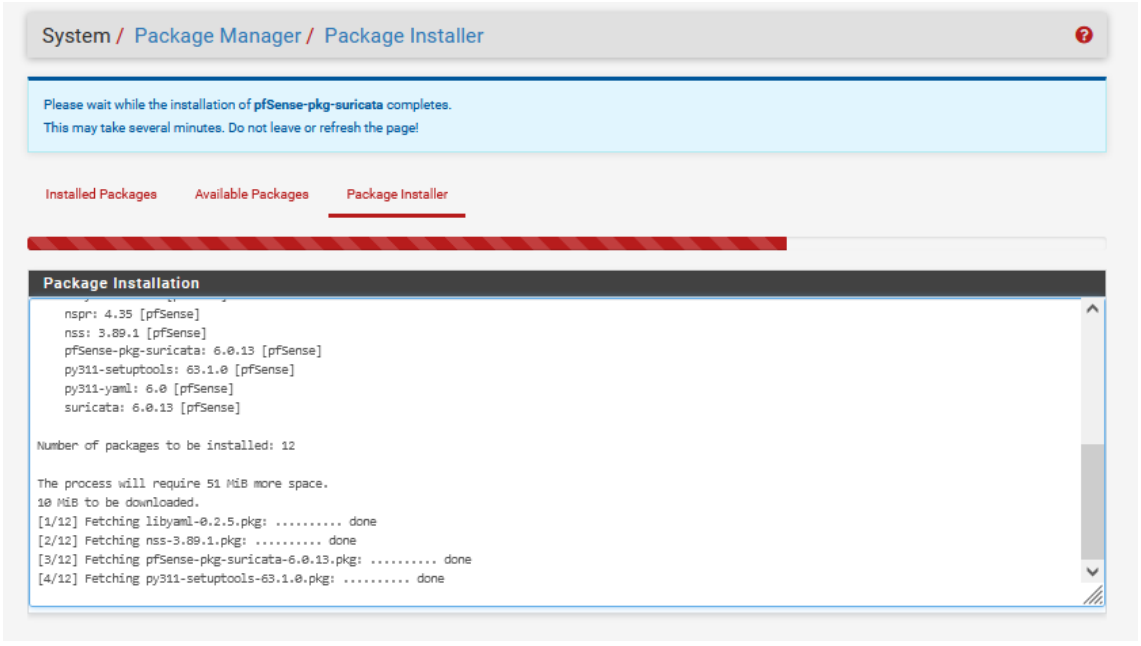
Firma: **_____**

4.6. PRÁCTICA # 6

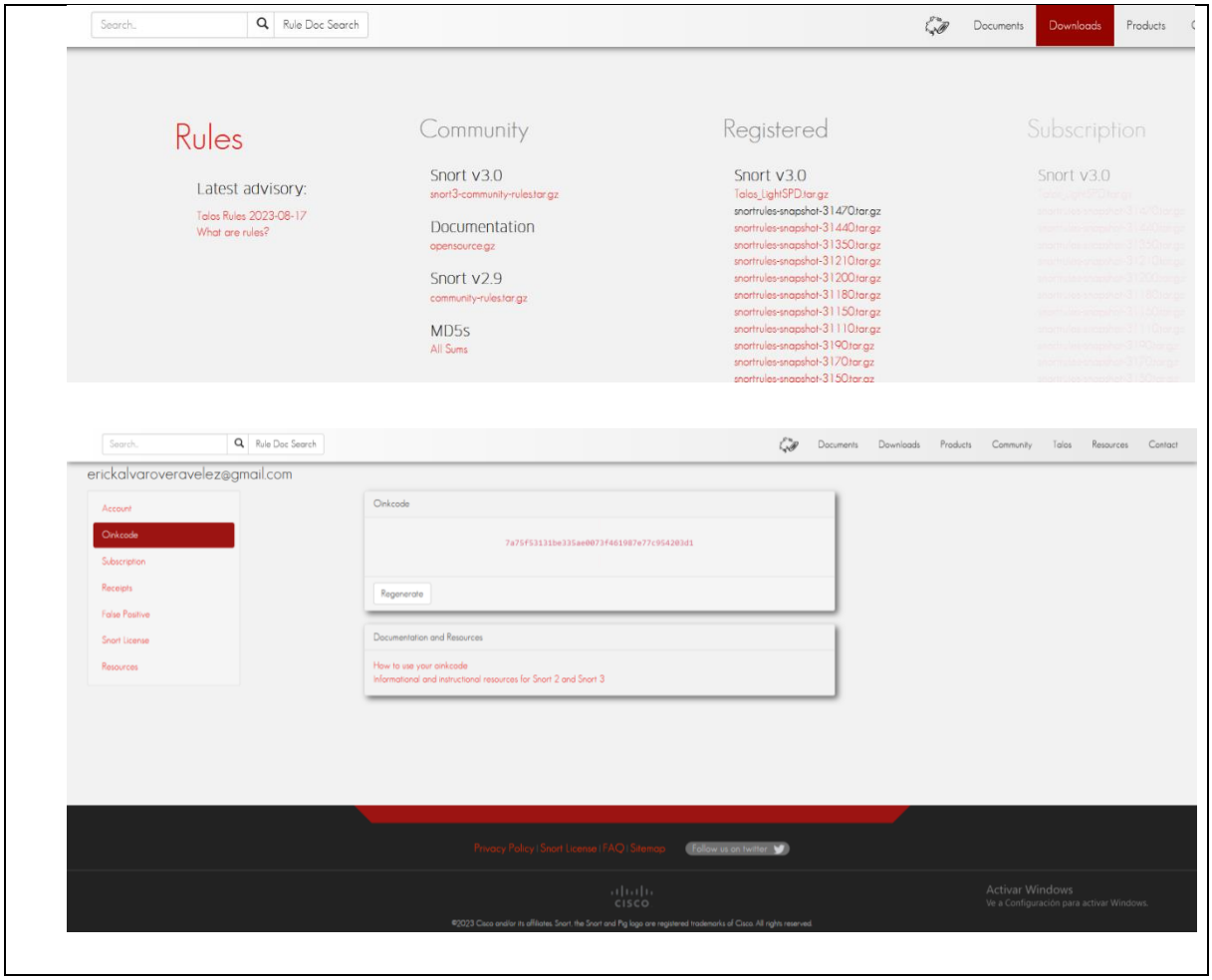
<table>
<tr><td colspan="2"> 
FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>Carrera: Ingeniería Electrónica</td><td>Asignatura: Redes de Computadoras</td></tr>
<tr><td>NRO. Práctica: 6</td><td>Título Práctica:
Implementación de IPS con Suricata en pfSense: Reforzando la Seguridad de la Red para la red LAN y WAN</td></tr>
<tr><td colspan="2">OBJETIVO:
• Objetivo General
Fortalecer y mejorar de manera significativa la seguridad de la red, permitiendo la identificación y prevención proactiva de posibles intrusiones y amenazas en ambos segmentos de la red</td></tr>
<tr><td>INSTRUCCIONES:</td><td>1. Configurar y optimizar pfSense en los segmentos de red LAN y WAN para admitir la implementación de Suricata como Sistema de Prevención de Intrusiones (IPS) en ambos entornos.
2. Definir reglas de detección personalizadas en Suricata para abordar los perfiles de amenazas y los patrones de tráfico relevantes para cada segmento de red (LAN y WAN).
3. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.</td></tr>
<tr><td colspan="2">ACTIVIDADES POR DESARROLLAR</td></tr>
</table>

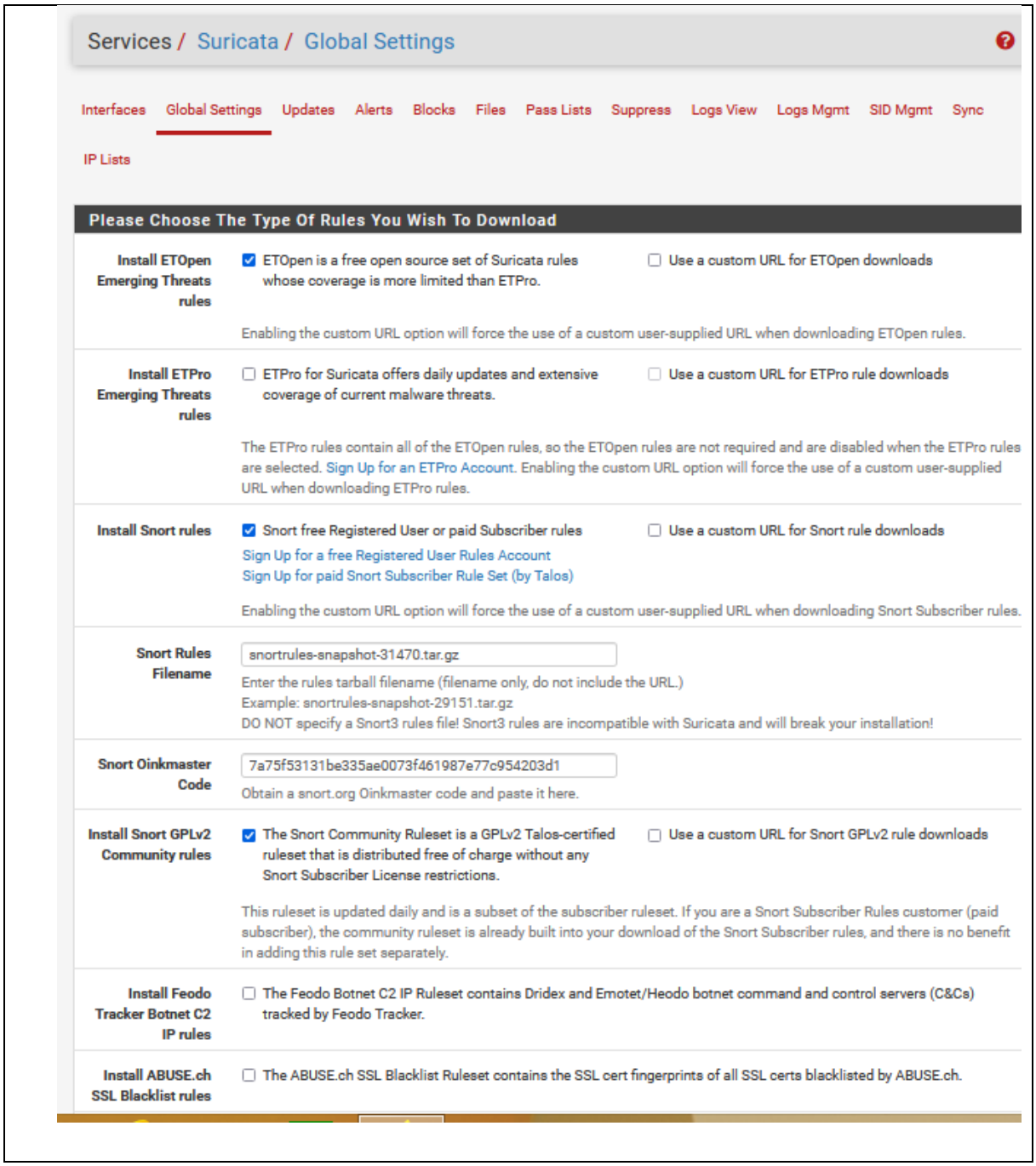
1. Para la configuración de un sistema de detección de intruso se deberá instalar los packages en el pfSense, en este caso puntual Suricata:

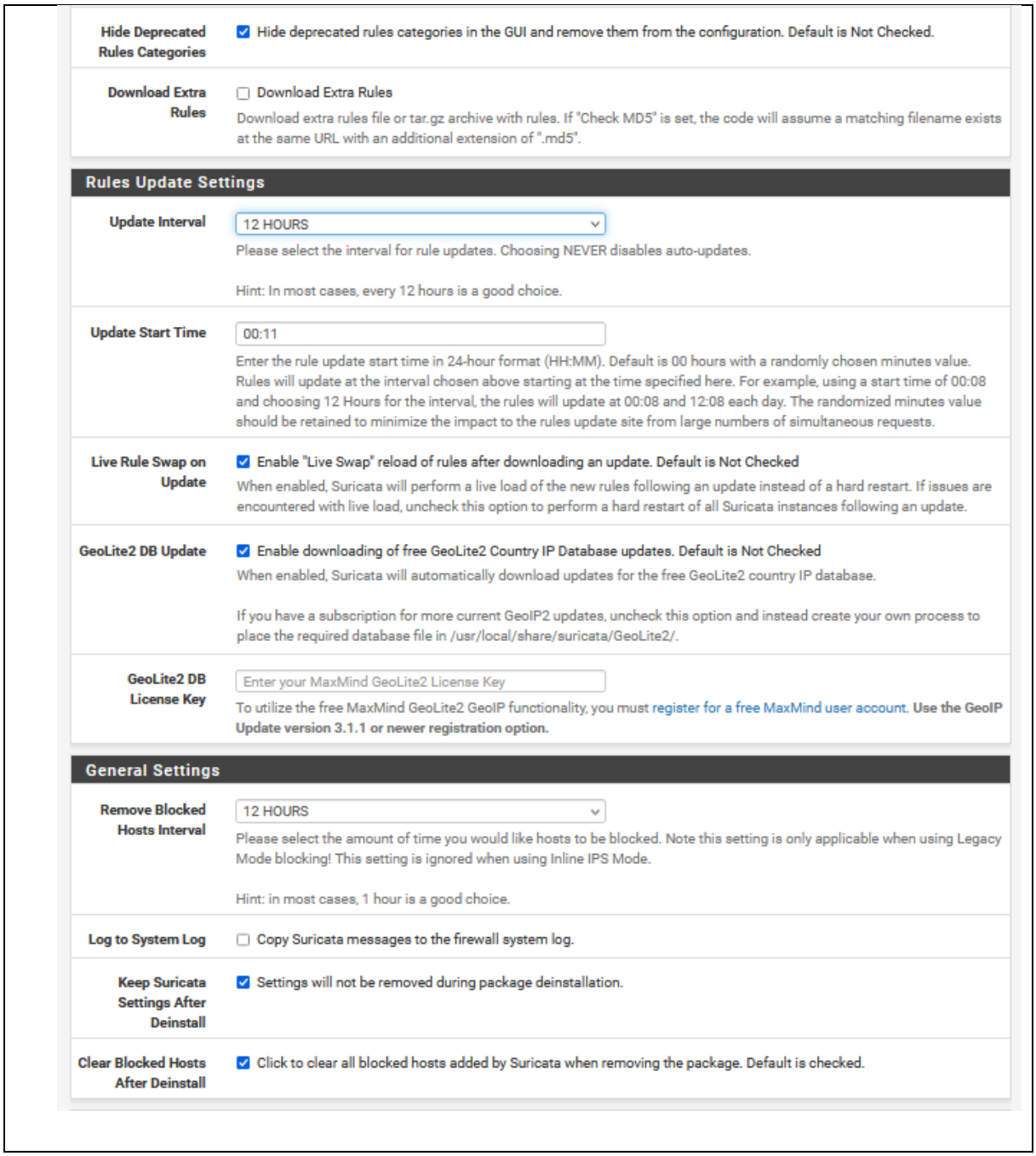


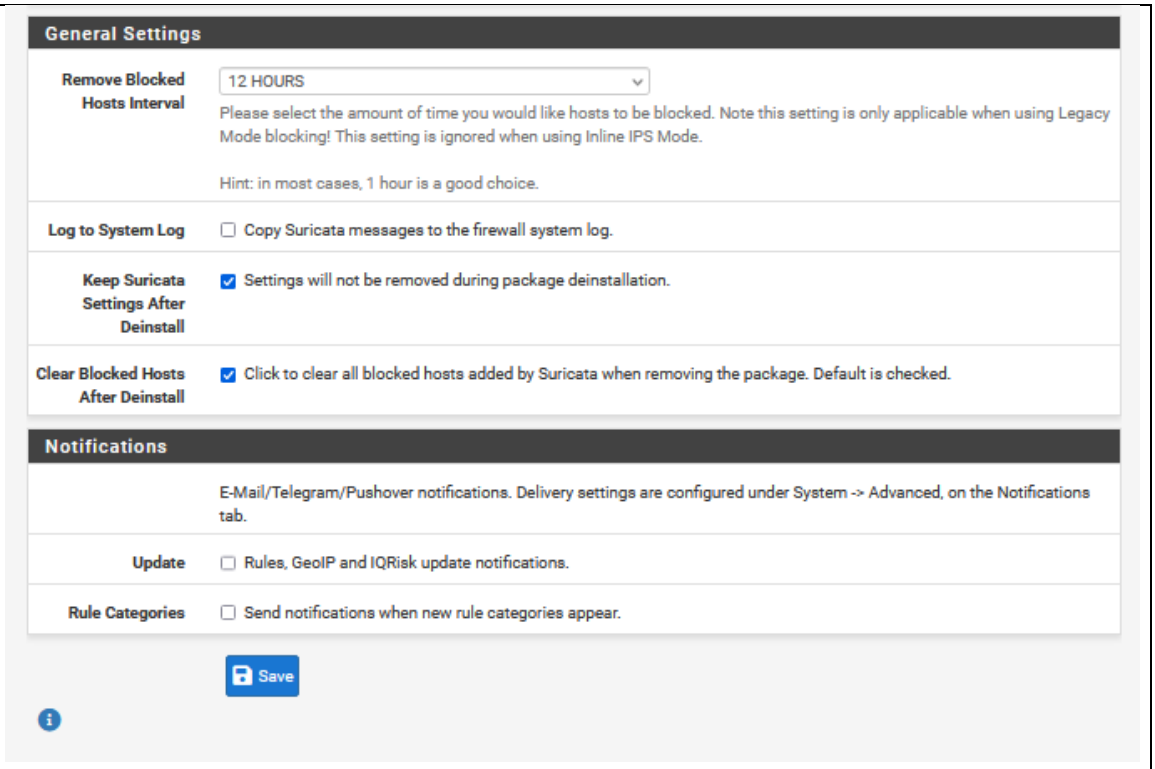


2. Para esta practica se activa suricata para la red lan y wan, se debe estar estar registrado en snort he instalar sus reglas y el oikmaster

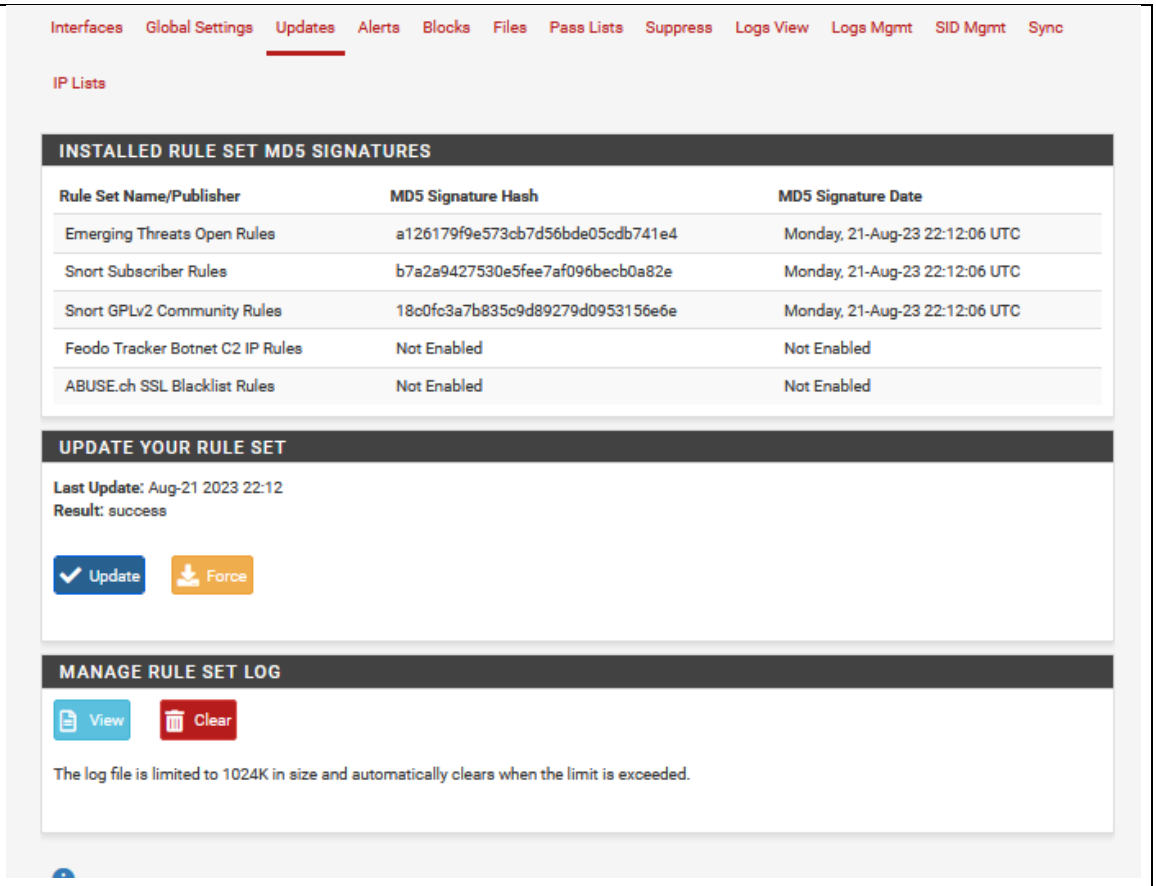

Search..
Rule Doc Search
Documents
Downloads
Products
Rules
Latest advisory:
Talos Rules 2023-08-17
What are rules?
Community
Snort v3.0
snort3-community-rules.tar.gz
Documentation
opensource.gz
Snort v2.9
community-rules.tar.gz
MD5s
All Sums
Registered
Snort v3.0
Talos_LightSPD.tar.gz
snortrules-snapshot-31470.tar.gz
snortrules-snapshot-31440.tar.gz
snortrules-snapshot-31350.tar.gz
snortrules-snapshot-31210.tar.gz
snortrules-snapshot-31200.tar.gz
snortrules-snapshot-31180.tar.gz
snortrules-snapshot-31150.tar.gz
snortrules-snapshot-31110.tar.gz
snortrules-snapshot-3190.tar.gz
snortrules-snapshot-3170.tar.gz
snortrules-snapshot-3150.tar.gz
Subscription
Snort v3.0
Search..
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
erickalvaroveravelez@gmail.com
Account
Oinkcode
Subscription
Receipts
False Positive
Snort License
Resources
Oinkcode
7a75f53131be335ae0073f461987e77c954203d1
Regenerate
Documentation and Resources
How to use your oinkcode
Informational and instructional resources for Snort 2 and Snort 3
Privacy Policy | Snort License | FAQ | Sitemap
Follow us on twitter
cisco
©2023 Cisco and/or its affiliates. Snort, the Snort and Pig logo are registered trademarks of Cisco. All rights reserved.
Activar Windows
Ve a Configuración para activar Windows.


Services / Suricata / Global Settings
Interfaces
Global Settings
Updates
Alerts
Blocks
Files
Pass Lists
Suppress
Logs View
Logs Mgmt
SID Mgmt
Sync
IP Lists
Please Choose The Type Of Rules You Wish To Download
Install ETOpen Emerging Threats rules
ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro.
Use a custom URL for ETOpen downloads
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.
Install ETPro Emerging Threats rules
ETPro for Suricata offers daily updates and extensive coverage of current malware threats.
Use a custom URL for ETPro rule downloads
The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. Sign Up for an ETPro Account. Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.
Install Snort rules
Snort free Registered User or paid Subscriber rules
Use a custom URL for Snort rule downloads
Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.
Snort Rules Filename
snortrules-snapshot-31470.tar.gz
Enter the rules tarball filename (filename only, do not include the URL.)
Example: snortrules-snapshot-29151.tar.gz
DO NOT specify a Snort3 rules file! Snort3 rules are incompatible with Suricata and will break your installation!
Snort Oinkmaster Code
7a75f53131be335ae0073f461987e77c954203d1
Obtain a snort.org Oinkmaster code and paste it here.
Install Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions.
Use a custom URL for Snort GPLv2 rule downloads
This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.
Install Feodo Tracker Botnet C2 IP rules
The Feodo Botnet C2 IP Ruleset contains Dridex and Emotet/Heodo botnet command and control servers (C&Cs) tracked by Feodo Tracker.
Install ABUSE.ch SSL Blacklist rules
The ABUSE.ch SSL Blacklist Ruleset contains the SSL cert fingerprints of all SSL certs blacklisted by ABUSE.ch.


Hide Deprecated Rules Categories
Hide deprecated rules categories in the GUI and remove them from the configuration. Default is Not Checked.
Download Extra Rules
Download Extra Rules
Download extra rules file or tar.gz archive with rules. If "Check MD5" is set, the code will assume a matching filename exists at the same URL with an additional extension of ".md5".
Rules Update Settings
Update Interval
12 HOURS
Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Hint: In most cases, every 12 hours is a good choice.
Update Start Time
00:11
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.
Live Rule Swap on Update
Enable "Live Swap" reload of rules after downloading an update. Default is Not Checked
When enabled, Suricata will perform a live load of the new rules following an update instead of a hard restart. If issues are encountered with live load, uncheck this option to perform a hard restart of all Suricata instances following an update.
GeoLite2 DB Update
Enable downloading of free GeoLite2 Country IP Database updates. Default is Not Checked
When enabled, Suricata will automatically download updates for the free GeoLite2 country IP database.
If you have a subscription for more current GeoIP2 updates, uncheck this option and instead create your own process to place the required database file in /usr/local/share/suricata/GeoLite2/.
GeoLite2 DB License Key
Enter your MaxMind GeoLite2 License Key
To utilize the free MaxMind GeoLite2 GeoIP functionality, you must register for a free MaxMind user account. Use the GeoIP Update version 3.1.1 or newer registration option.
General Settings
Remove Blocked Hosts Interval
12 HOURS
Please select the amount of time you would like hosts to be blocked. Note this setting is only applicable when using Legacy Mode blocking! This setting is ignored when using Inline IPS Mode.
Hint: in most cases, 1 hour is a good choice.
Log to System Log
Copy Suricata messages to the firewall system log.
Keep Suricata Settings After Deinstall
Settings will not be removed during package deinstallation.
Clear Blocked Hosts After Deinstall
Click to clear all blocked hosts added by Suricata when removing the package. Default is checked.

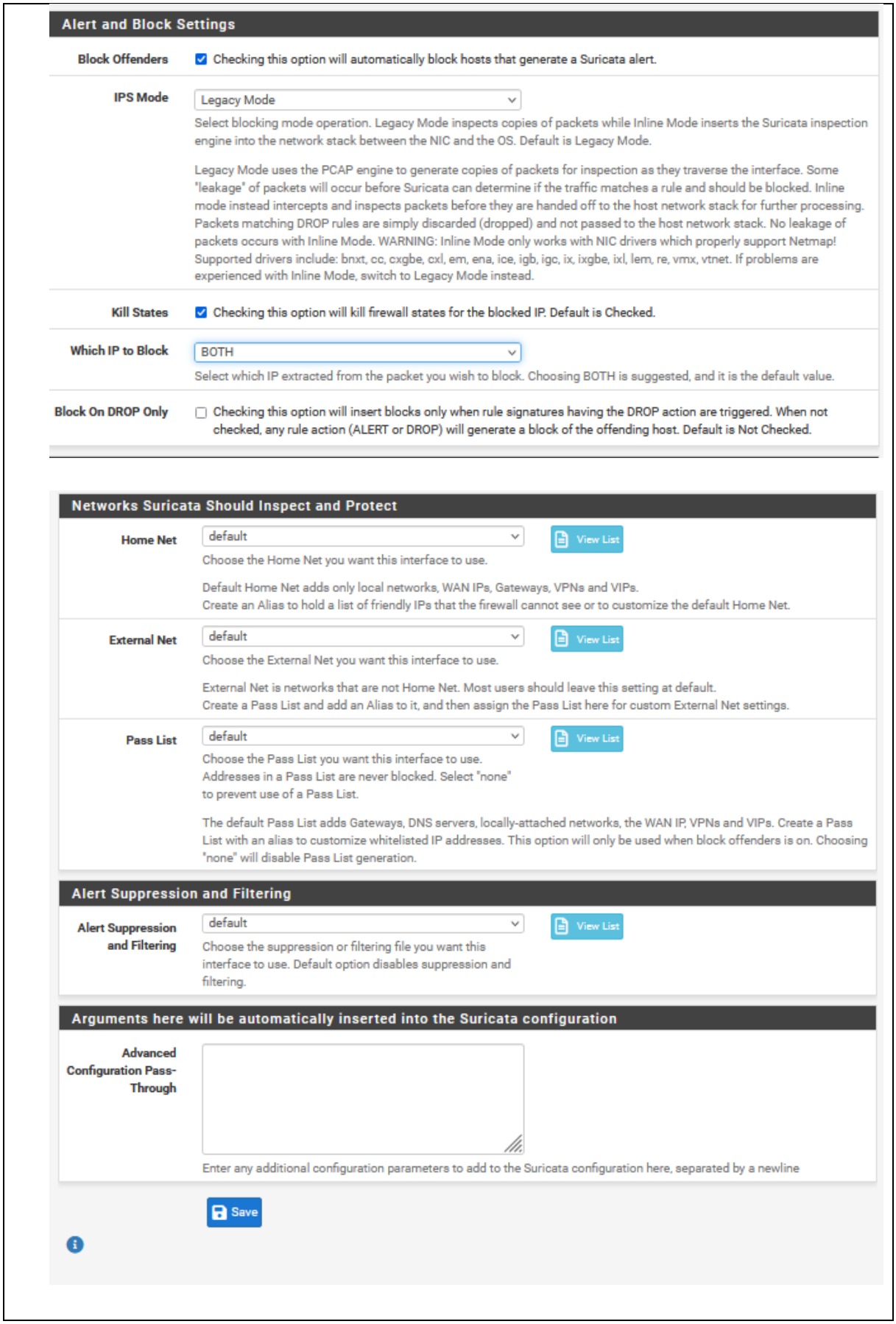


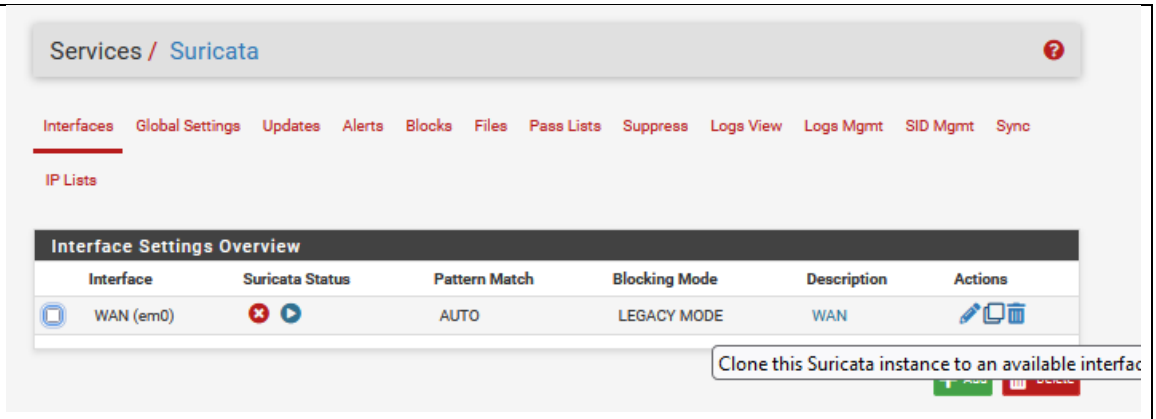
3. Actualizar Reglas



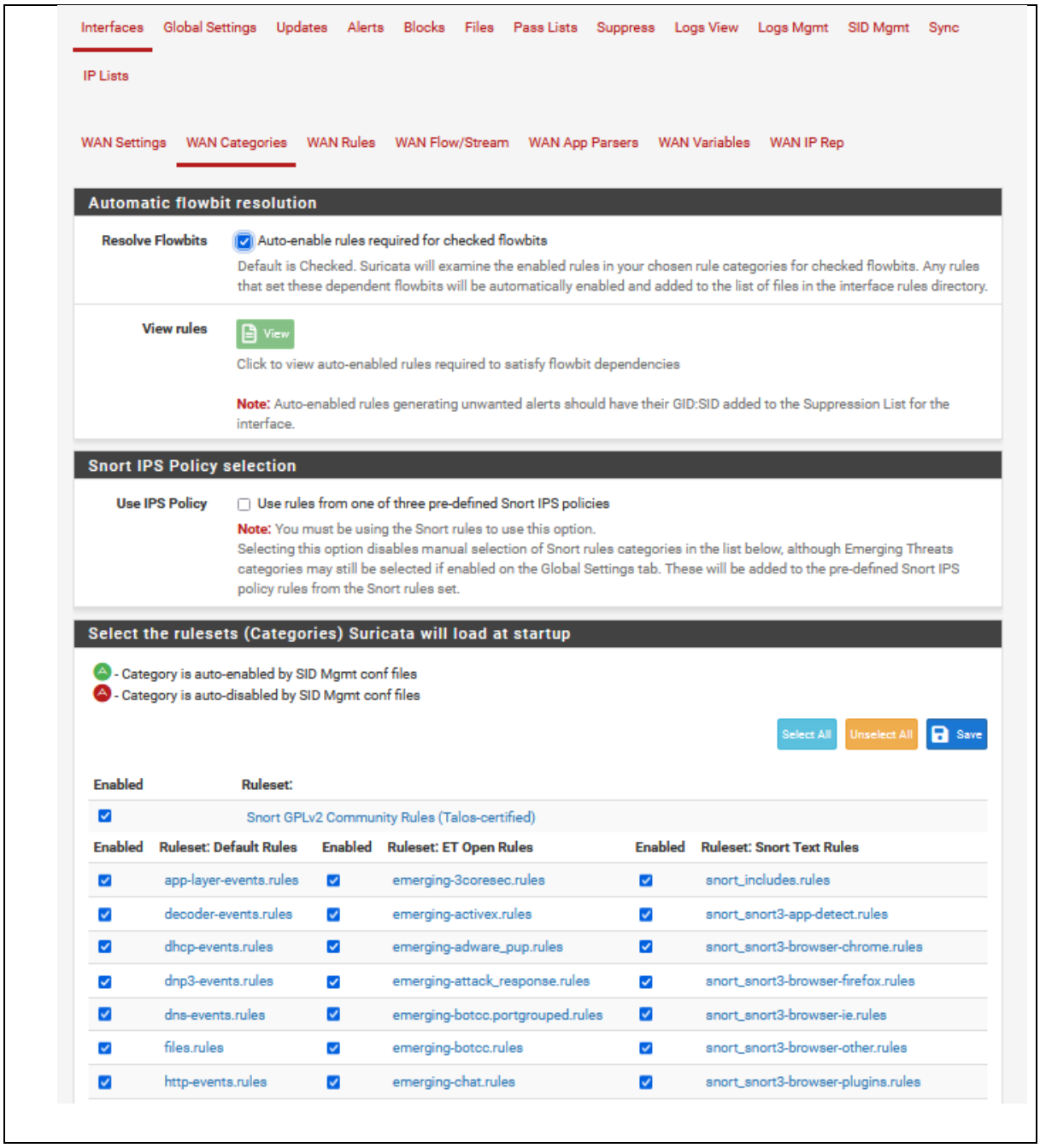
4. Confgurar la interfaz lan y wan, la configuración de ambas interfaz es lo mismo , eligiendo en clonar.

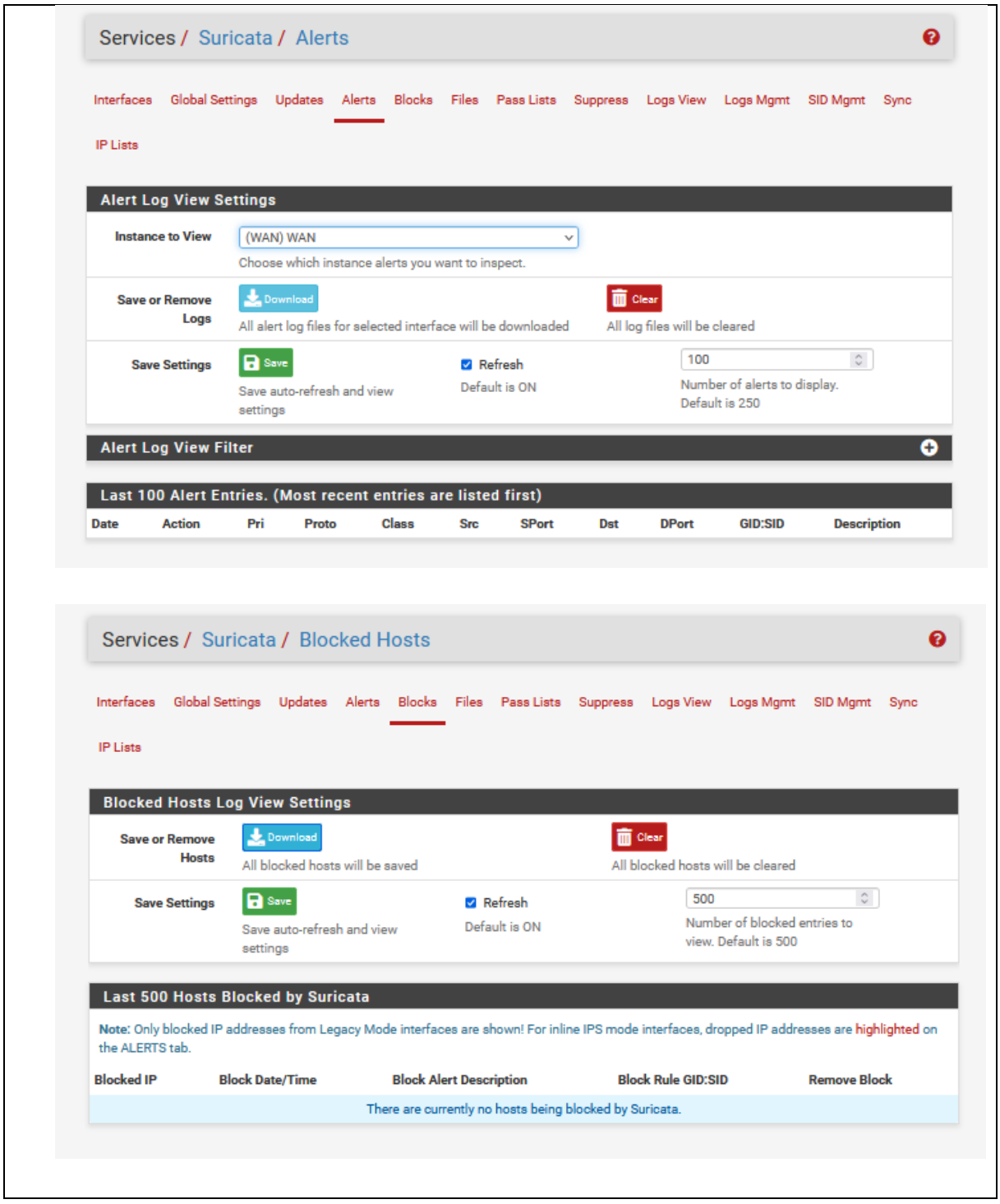

WAN Settings
General Settings
Enable
Checking this box enables Suricata inspection on the interface.
Interface
WAN (em0)
Choose which interface this Suricata instance applies to. In most cases, you will want to choose LAN here if this is the first Suricata-configured interface.
Description
WAN
Enter a meaningful description here for your reference. The default is the pfSense interface friendly description.
Logging Settings
Send Alerts to System Log
Suricata will send Alerts from this interface to the firewall's system log.
NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.
Enable Stats Collection
Suricata will periodically gather performance statistics for this interface. Default is Not Checked.
Stats Update Interval
11
Enter the update interval in seconds for collection of performance statistics. Default is 10 seconds.
Enable Stats Log
Suricata will periodically log statistics for this interface to a CSV text log file. Default is Not Checked.
Append Stats Log
Suricata will append-to instead of clearing the stats log file when restarting. Default is Not Checked.
Enable Telegraf Stats
Suricata will periodically log statistics for this interface to Telegraf via a Unix socket. Default is Not Checked.
Enable HTTP Log
Suricata will log decoded HTTP traffic for the interface. Default is Checked.
Append HTTP Log
Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked.
Log Extended HTTP Info
Suricata will log extended HTTP information. Default is Checked.
Enable TLS Log
Suricata will log TLS handshake traffic for the interface. Default is Not Checked.
Enable File-Store
Suricata will extract and store files from application layer streams. Default is Not Checked. WARNING: Enabling file-store will consume a significant amount of disk space on a busy network!
Enable Packet Log
Suricata will log decoded packets for the interface in pcap-format. Default is Not Checked. This can consume a significant amount of disk space when enabled.
Enable Verbose Logging
Suricata will log additional information to the suricata.log file when starting up and shutting down. Default is Not Checked.

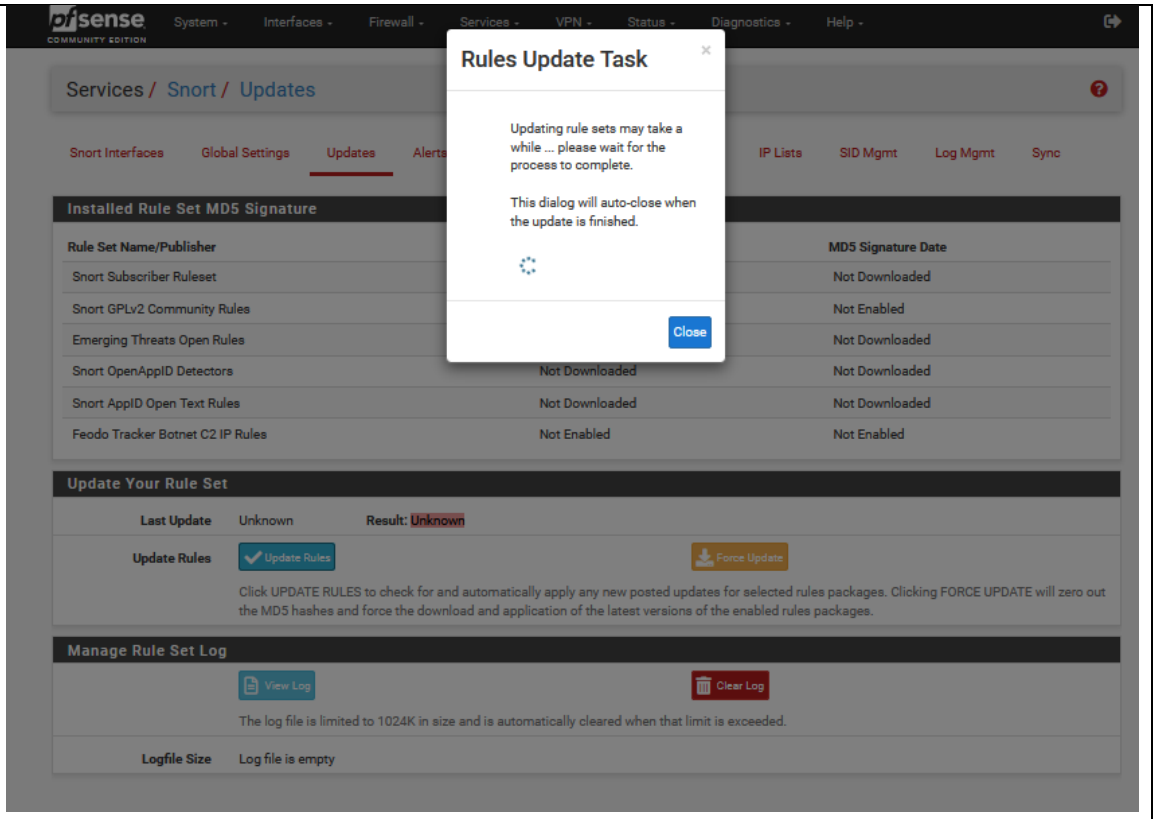

Alert and Block Settings
Block Offenders
Checking this option will automatically block hosts that generate a Suricata alert.
IPS Mode
Legacy Mode
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.
Kill States
Checking this option will kill firewall states for the blocked IP. Default is Checked.
Which IP to Block
BOTH
Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.
Block On DROP Only
Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.
Networks Suricata Should Inspect and Protect
Home Net
default
View List
Choose the Home Net you want this interface to use.
Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.
Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.
External Net
default
View List
Choose the External Net you want this interface to use.
External Net is networks that are not Home Net. Most users should leave this setting at default.
Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.
Pass List
default
View List
Choose the Pass List you want this interface to use.
Addresses in a Pass List are never blocked. Select "none" to prevent use of a Pass List.
The default Pass List adds Gateways, DNS servers, locally-attached networks, the WAN IP, VPNs and VIPs. Create a Pass List with an alias to customize whitelisted IP addresses. This option will only be used when block offenders is on. Choosing "none" will disable Pass List generation.
Alert Suppression and Filtering
Alert Suppression and Filtering
default
View List
Choose the suppression or filtering file you want this interface to use. Default option disables suppression and filtering.
Arguments here will be automatically inserted into the Suricata configuration
Advanced Configuration Pass-Through
Enter any additional configuration parameters to add to the Suricata configuration here, separated by a newline
Save



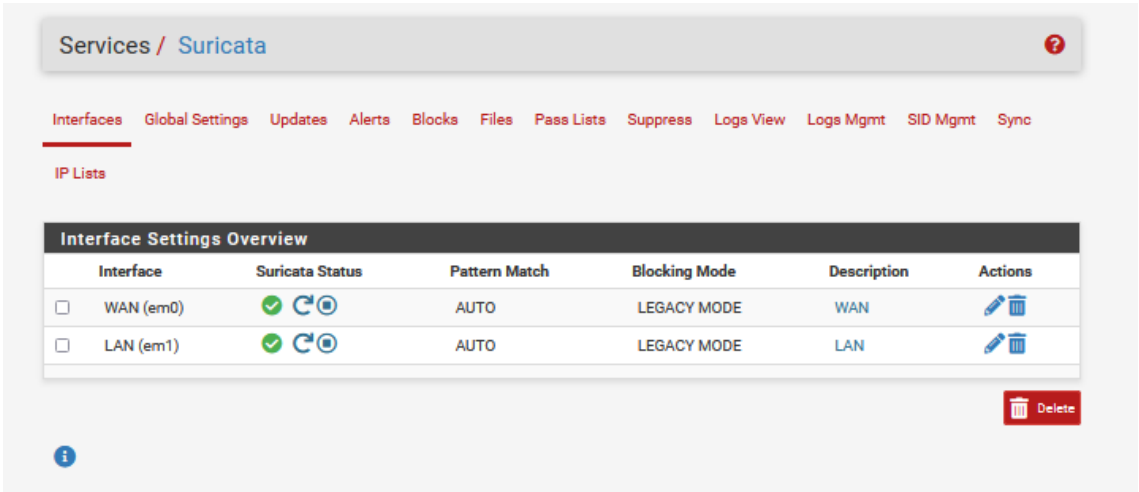
5. Se seleccionará todas las reglas de las categorías para ambas interfaces

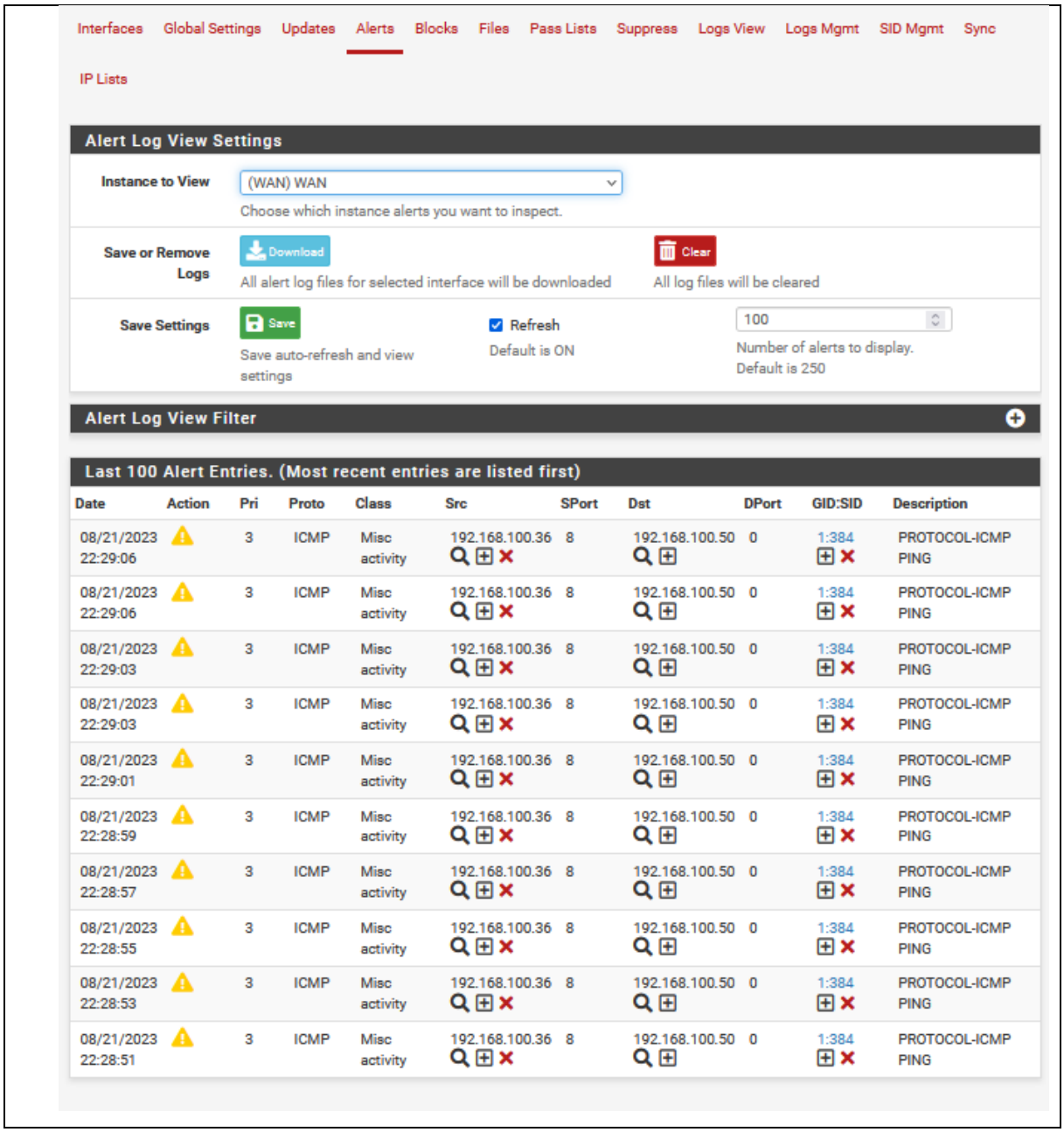

Interfaces
Global Settings
Updates
Alerts
Blocks
Files
Pass Lists
Suppress
Logs View
Logs Mgmt
SID Mgmt
Sync
IP Lists
WAN Settings
WAN Categories
WAN Rules
WAN Flow/Stream
WAN App Parsers
WAN Variables
WAN IP Rep
Automatic flowbit resolution
Resolve Flowbits
Auto-enable rules required for checked flowbits
Default is Checked. Suricata will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.
View rules
View
Click to view auto-enabled rules required to satisfy flowbit dependencies
Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.
Snort IPS Policy selection
Use IPS Policy
Use rules from one of three pre-defined Snort IPS policies
Note: You must be using the Snort rules to use this option.
Selecting this option disables manual selection of Snort rules categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort rules set.
Select the rulesets (Categories) Suricata will load at startup
- Category is auto-enabled by SID Mgmt conf files
- Category is auto-disabled by SID Mgmt conf files
Select All
Unselect All
Save
Enabled
Ruleset:
Snort GPLv2 Community Rules (Talos-certified)
Enabled
Ruleset: Default Rules
Enabled
Ruleset: ET Open Rules
Enabled
Ruleset: Snort Text Rules
app-layer-events.rules
emerging-3coresec.rules
snort_includes.rules
decoder-events.rules
emerging-activex.rules
snort_snort3-app-detect.rules
dhcp-events.rules
emerging-adware_pup.rules
snort_snort3-browser-chrome.rules
dnp3-events.rules
emerging-attack_response.rules
snort_snort3-browser-firefox.rules
dns-events.rules
emerging-botcc.portgrouped.rules
snort_snort3-browser-ie.rules
files.rules
emerging-botcc.rules
snort_snort3-browser-other.rules
http-events.rules
emerging-chat.rules
snort_snort3-browser-plugins.rules

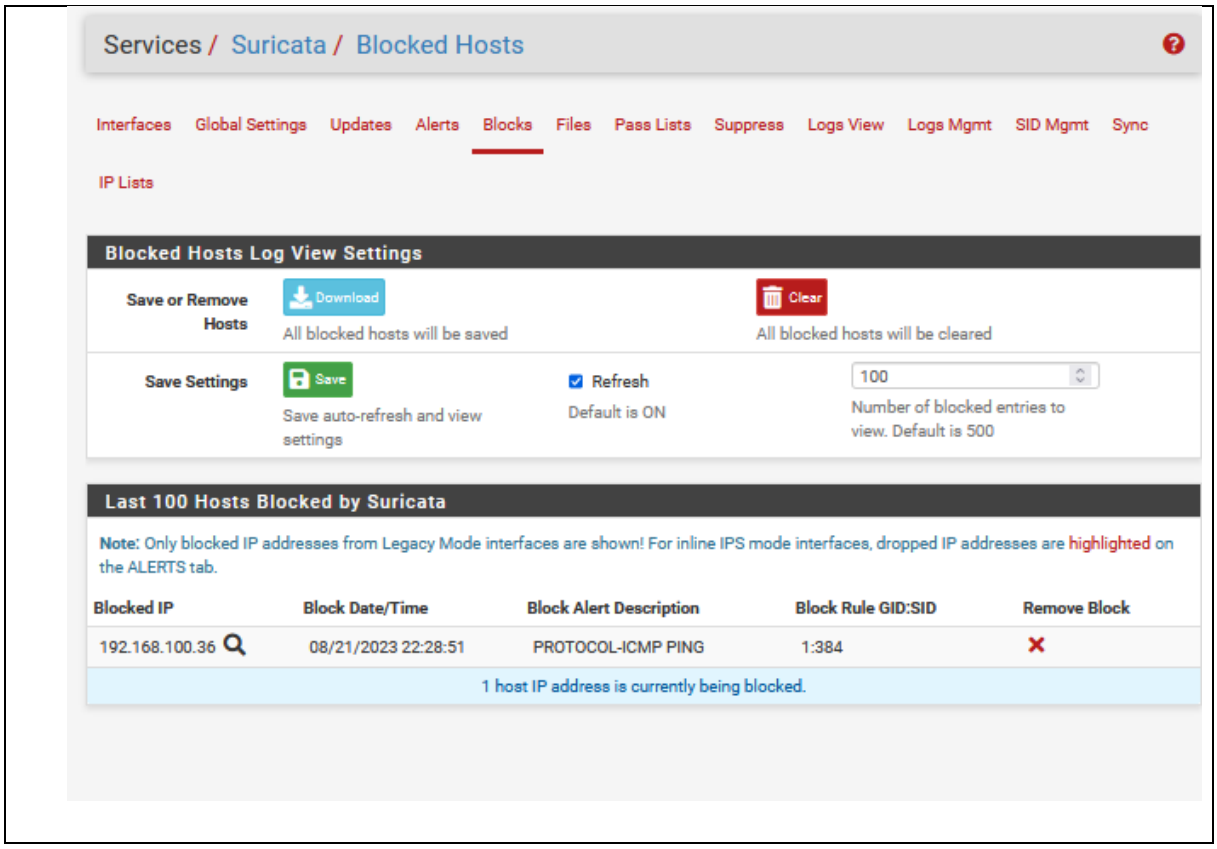

Services / Suricata / Alerts
Interfaces
Global Settings
Updates
Alerts
Blocks
Files
Pass Lists
Suppress
Logs View
Logs Mgmt
SID Mgmt
Sync
IP Lists
Alert Log View Settings
Instance to View
(WAN) WAN
Choose which instance alerts you want to inspect.
Save or Remove Logs
Download
All alert log files for selected interface will be downloaded
Clear
All log files will be cleared
Save Settings
Save
Save auto-refresh and view settings
Refresh
Default is ON
100
Number of alerts to display. Default is 250
Alert Log View Filter
Last 100 Alert Entries. (Most recent entries are listed first)
Date
Action
Pri
Proto
Class
Src
SPort
Dst
DPort
GID:SID
Description
Services / Suricata / Blocked Hosts
Interfaces
Global Settings
Updates
Alerts
Blocks
Files
Pass Lists
Suppress
Logs View
Logs Mgmt
SID Mgmt
Sync
IP Lists
Blocked Hosts Log View Settings
Save or Remove Hosts
Download
All blocked hosts will be saved
Clear
All blocked hosts will be cleared
Save Settings
Save
Save auto-refresh and view settings
Refresh
Default is ON
500
Number of blocked entries to view. Default is 500
Last 500 Hosts Blocked by Suricata
Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.
Blocked IP
Block Date/Time
Block Alert Description
Block Rule GID:SID
Remove Block
There are currently no hosts being blocked by Suricata.

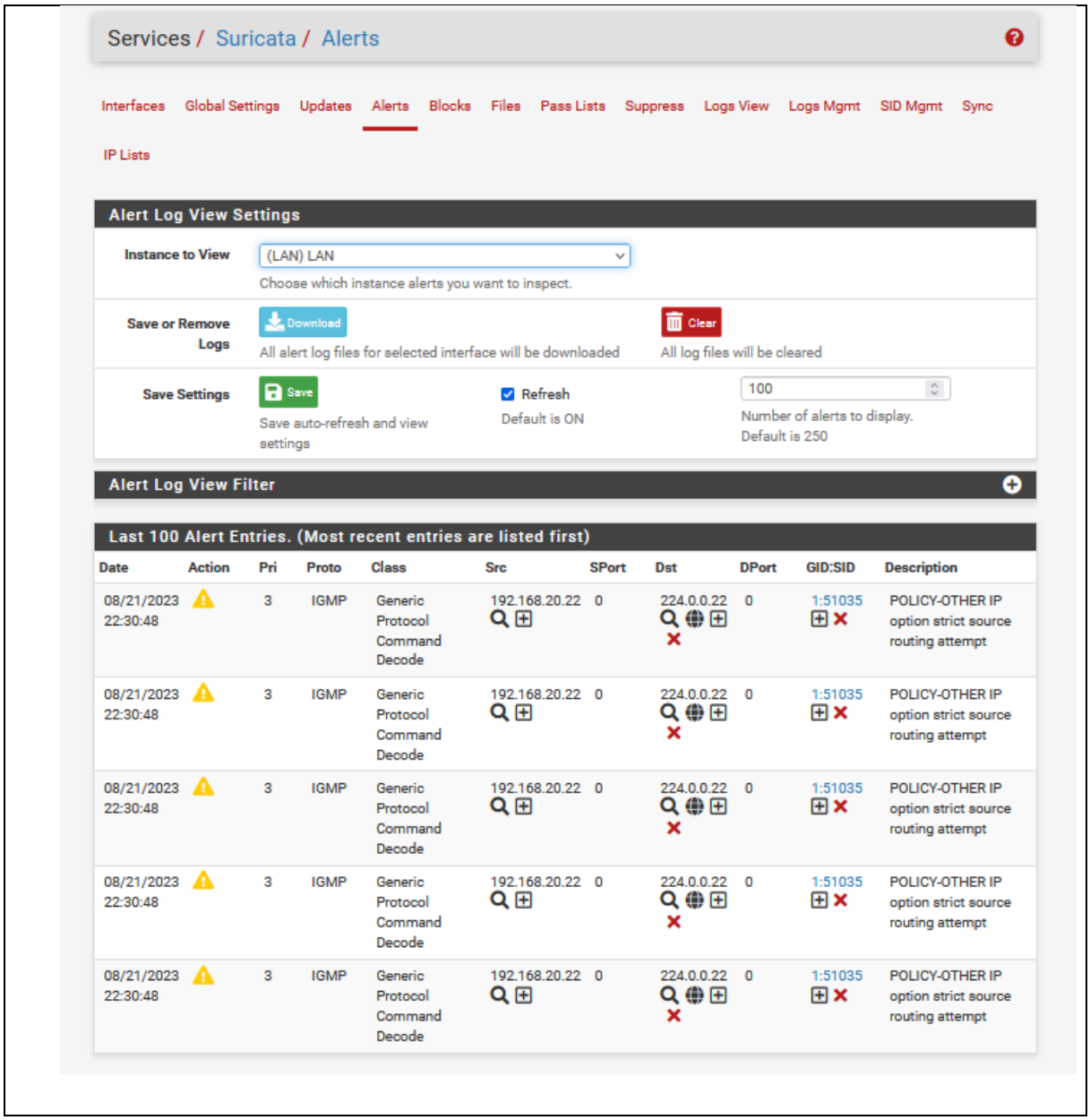


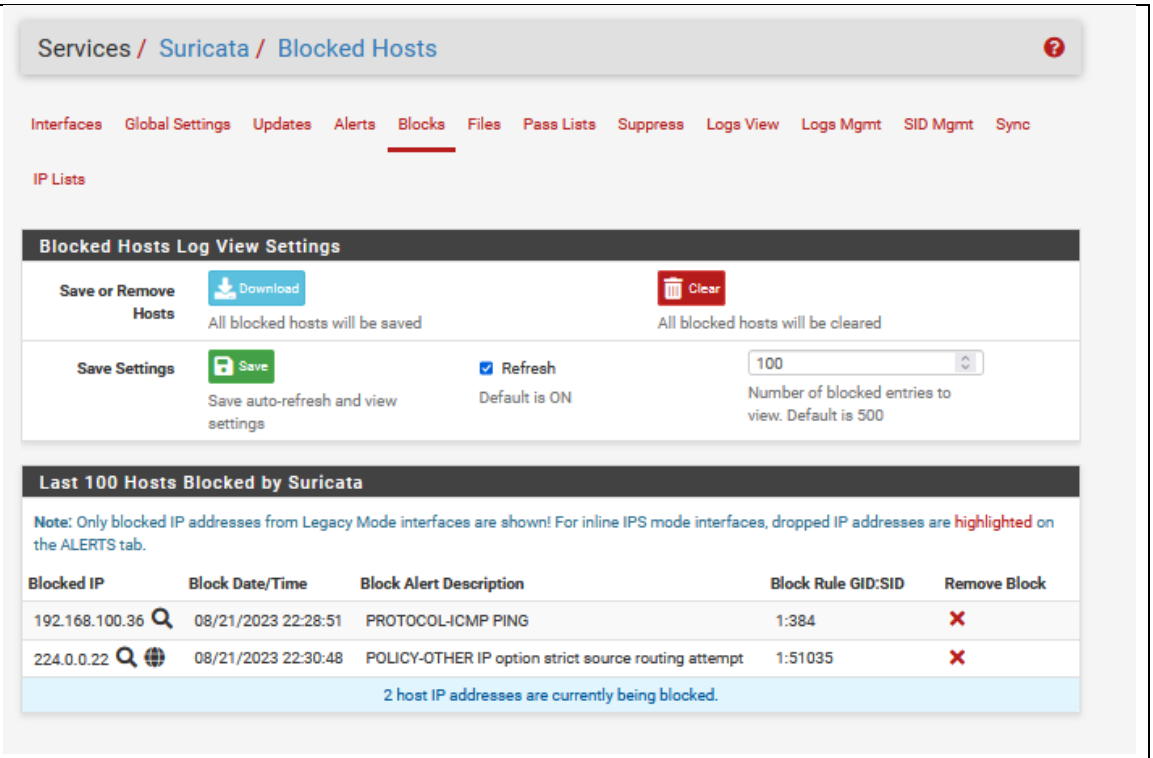
6. Regresar a suricata interfaces para iniciar y comienza a capturar ataques desde alguna celular o pc realizando un escaneos de puerto se mostrara.




Interfaces
Global Settings
Updates
Alerts
Blocks
Files
Pass Lists
Suppress
Logs View
Logs Mgmt
SID Mgmt
Sync
IP Lists
Alert Log View Settings
Instance to View
(WAN) WAN
Choose which instance alerts you want to inspect.
Save or Remove Logs
Download
All alert log files for selected interface will be downloaded
Clear
All log files will be cleared
Save Settings
Save
Save auto-refresh and view settings
Refresh
Default is ON
100
Number of alerts to display.
Default is 250
Alert Log View Filter
Last 100 Alert Entries. (Most recent entries are listed first)
Date Action Pri Proto Class Src SPort Dst DPort GID:SID Description
08/21/2023 22:29:06 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:29:06 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:29:03 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:29:03 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:29:01 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:28:59 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:28:57 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:28:55 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:28:53 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING
08/21/2023 22:28:51 3 ICMP Misc activity 192.168.100.36 8 192.168.100.50 0 1:384 PROTOCOL-ICMP PING


Services / Suricata / Blocked Hosts
Interfaces
Global Settings
Updates
Alerts
Blocks
Files
Pass Lists
Suppress
Logs View
Logs Mgmt
SID Mgmt
Sync
IP Lists
Blocked Hosts Log View Settings
Save or Remove Hosts
Download
All blocked hosts will be saved
Clear
All blocked hosts will be cleared
Save Settings
Save
Save auto-refresh and view settings
Refresh
Default is ON
100
Number of blocked entries to view. Default is 500
Last 100 Hosts Blocked by Suricata
Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.
Blocked IP
Block Date/Time
Block Alert Description
Block Rule GID:SID
Remove Block
192.168.100.36
08/21/2023 22:28:51
PROTOCOL-ICMP PING
1:384
1 host IP address is currently being blocked.


Services / Suricata / Alerts
Interfaces
Global Settings
Updates
Alerts
Blocks
Files
Pass Lists
Suppress
Logs View
Logs Mgmt
SID Mgmt
Sync
IP Lists
Alert Log View Settings
Instance to View
(LAN) LAN
Choose which instance alerts you want to inspect.
Save or Remove Logs
Download
All alert log files for selected interface will be downloaded
Clear
All log files will be cleared
Save Settings
Save
Save auto-refresh and view settings
Refresh
Default is ON
100
Number of alerts to display.
Default is 250
Alert Log View Filter
Last 100 Alert Entries. (Most recent entries are listed first)
Date
Action
Pri
Proto
Class
Src
SPort
Dst
DPort
GID:SID
Description
08/21/2023 22:30:48
3
IGMP
Generic Protocol Command Decode
192.168.20.22
0
224.0.0.22
0
1:51035
POLICY-OTHER IP option strict source routing attempt



RESULTADO(S) OBTENIDO(S):

Los estudiantes han implementado un Sistema de Prevención de Intrusiones (IPS) utilizando Suricata en la red LAN y WAN a través de la plataforma pfSense ha comprobando ser una estrategia efectiva para reforzar la seguridad de la red

CONCLUSIONES:

Los estudiantes implementan un sistema de prevención de intrusos utilizando Suricata.

RECOMENDACIONES:

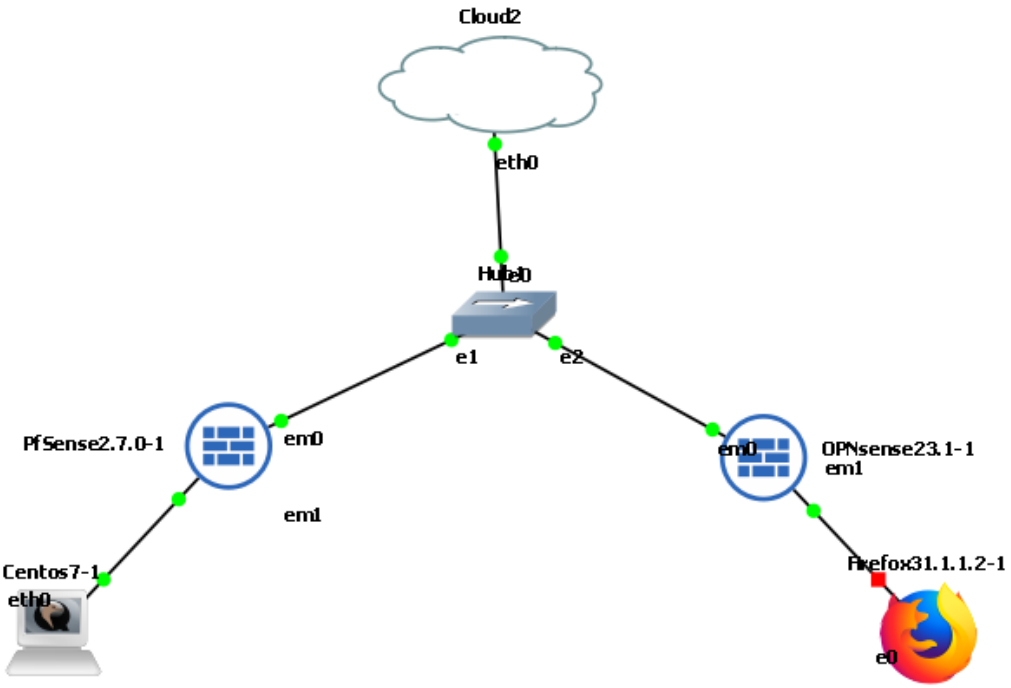
- La configuración de Suricata debe ser objeto de revisión y actualización periódica para mantener la relevancia y eficacia de las reglas de detección
- A medida que la red evoluciona y se agregan nuevos servicios y aplicaciones, se debe evaluar el impacto de estos cambios en la eficacia de Suricata y en el rendimiento general de la red

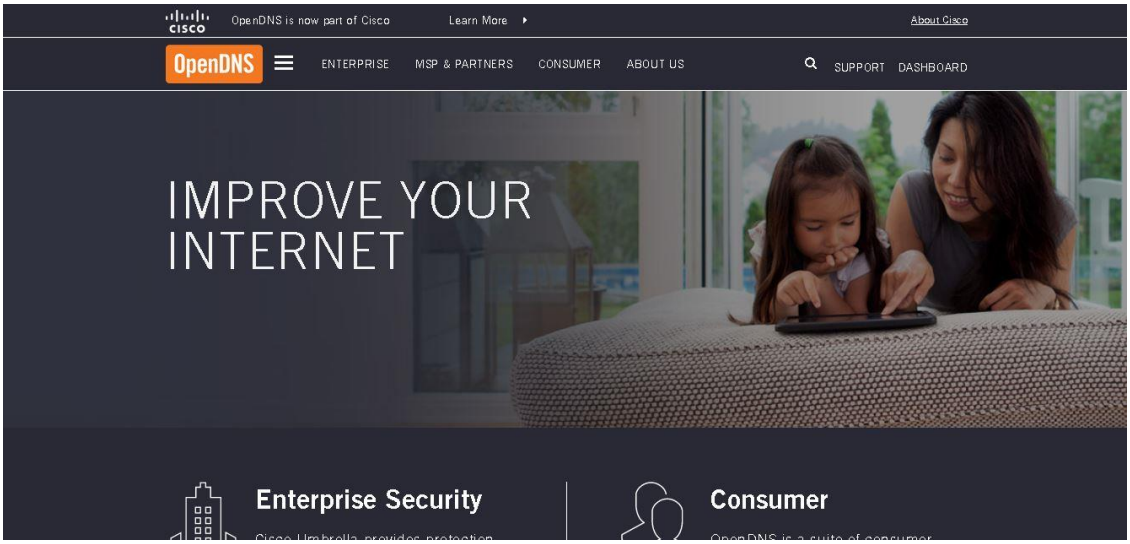
Docente: _____

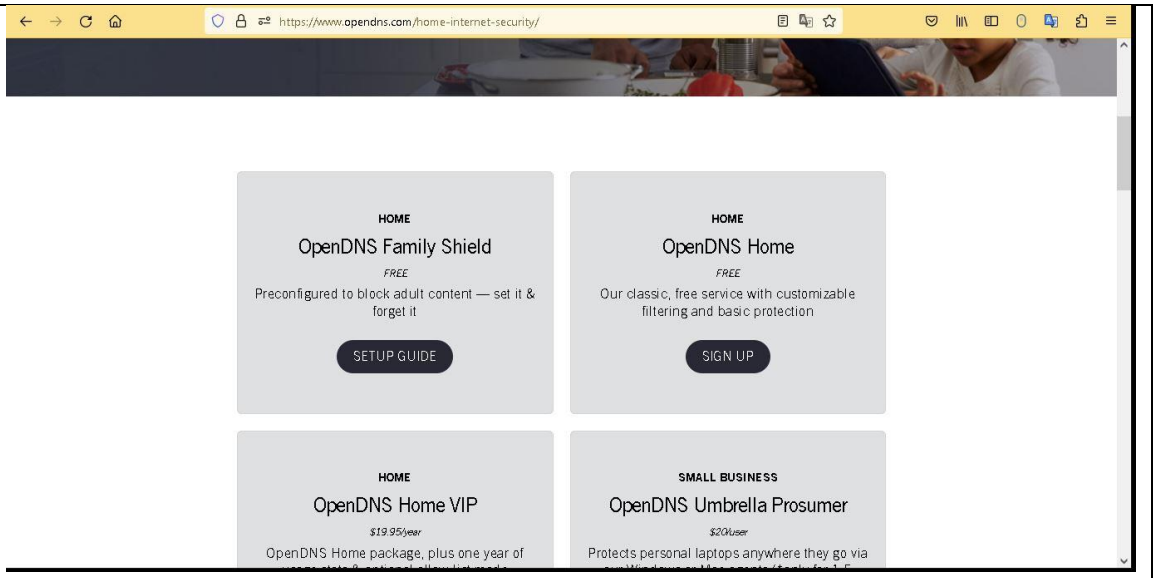
Firma: _____

4.7. PRÁCTICA # 7

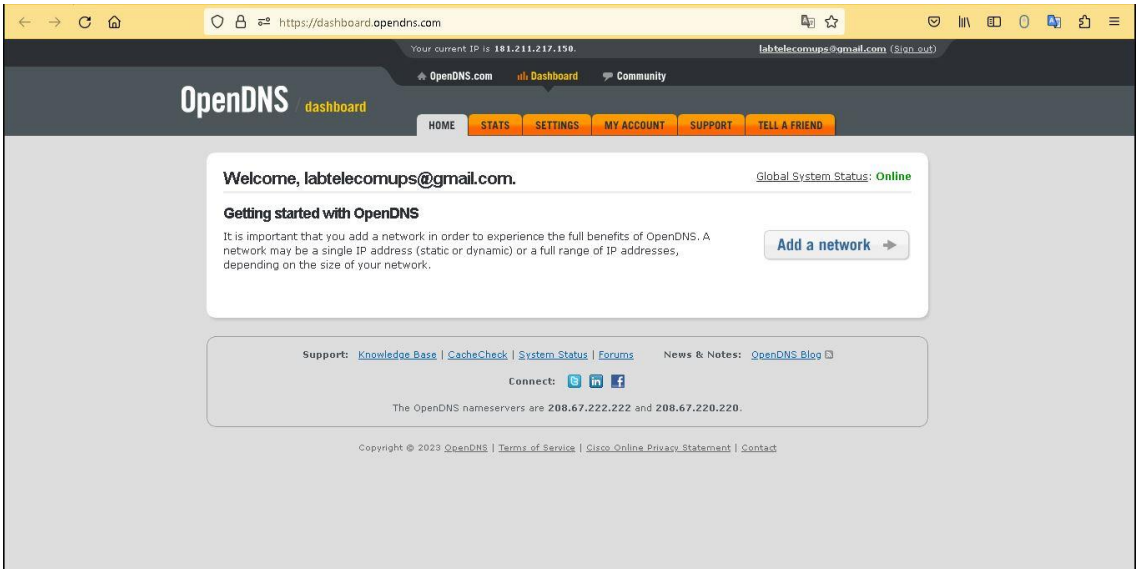
	**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES**
Carrera: Ingeniería Electrónica	**Asignatura:** Redes de Computadoras
NRO. Práctica: 7	**Título Práctica:** Integración de OPNSense y pfSense en una red con OpenDNS**.**
OBJETIVO: • **Objetivo General** Configurar una red utilizando dos sistemas de firewall de código abierto e implementar OpenDNS para filtrar y mejorar la seguridad de la navegación en la red.	
INSTRUCCIONES:	1. Configurar pfSense y OPNSense en el segmento y WAN. 2. Configurar la red en OpenDNS y configurar los servidores DNS para utilizar los servidores DNS. 3. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.
ACTIVIDADES POR DESARROLLAR	
1. Ingresar a https://www.opendns.com/ e ir a la opcion de Consumer, dentro de ella escoger la opcion OpenDNS Home. Crear un usuario para configurar el servicio de OpenDns.	


Cloud2
eth0
Hub0
e1
e2
PfSense2.7.0-1
em0
em1
em0
OPNsense23.1-1
em1
Centos7-1
eth0
Firefox31.1.1.2-1
e0

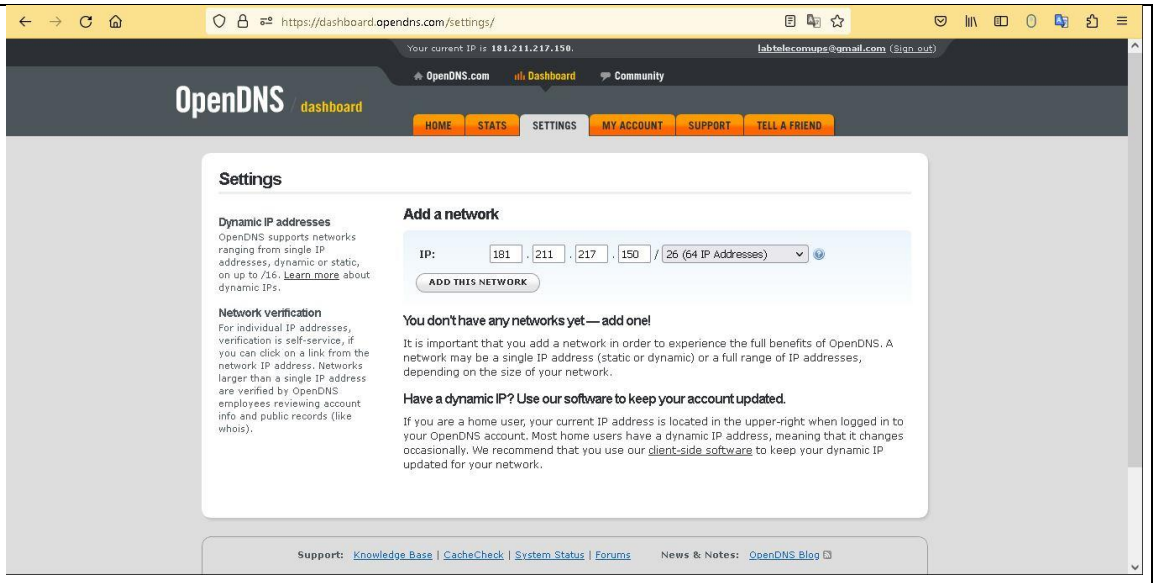

OpenDNS is now part of Cisco
Learn More
About Cisco
OpenDNS
ENTERPRISE
MSP & PARTNERS
CONSUMER
ABOUT US
SUPPORT
DASHBOARD
IMPROVE YOUR INTERNET
Enterprise Security
Consumer



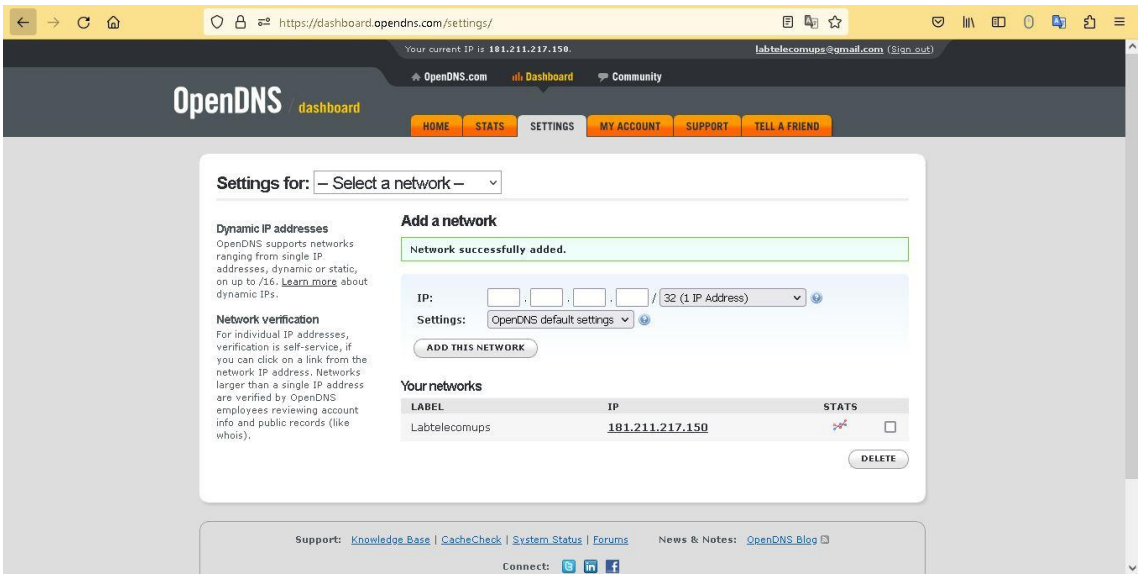
2. Una vez que se registro, se confirma el correo electrónico se ingresa a la aplicación y que brinda la pantalla de bienvenida a OpenDNS.



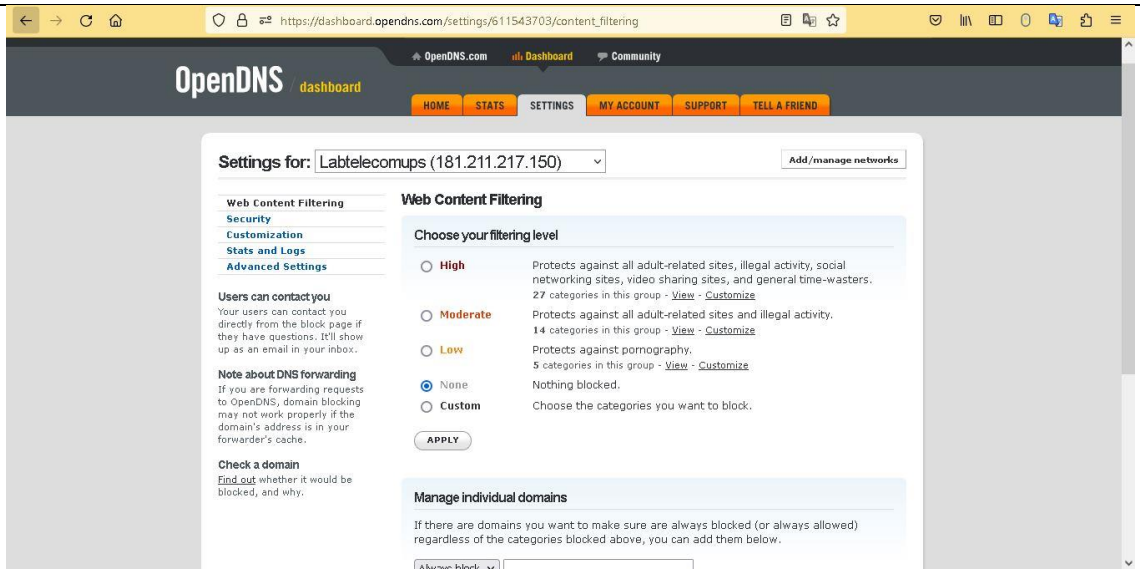
3. Dirigirse a la opción de Settings donde se añade la red pública que tiene automaticamente dectecto del proveedor de internet.

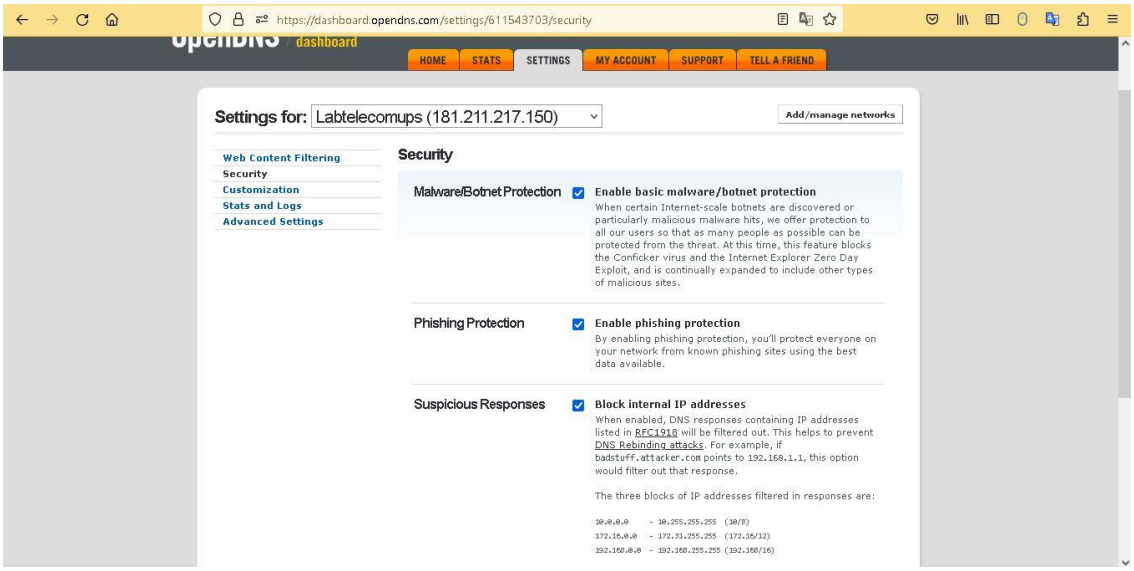


4. Añadir la red al sistema de OpenDns con un nombre sencillo para despues configurar en los firewall pfSense y OPNSense.

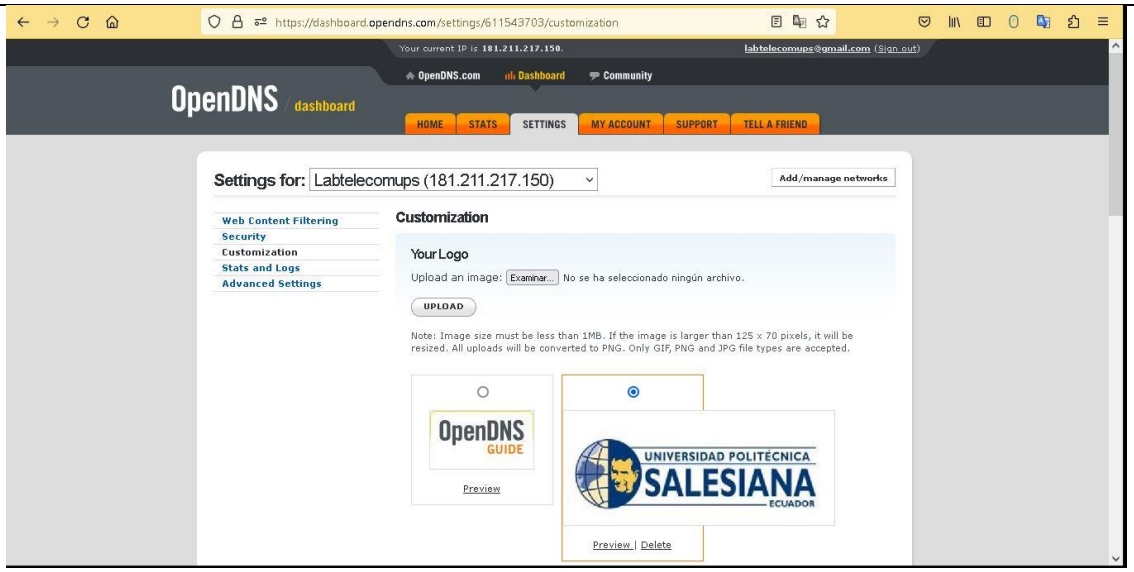


5. Seleccionar la red e ingresar en ella para proceder a configurar el WEB Content Filteringde acuerdo a la necesidad que se requiera. Se puede aplicar directamente el bloqueo del dominio que se necesite y se requiera bloquear. Dentro de esta opción existen 5 niveles de para filtrar las páginas Web.

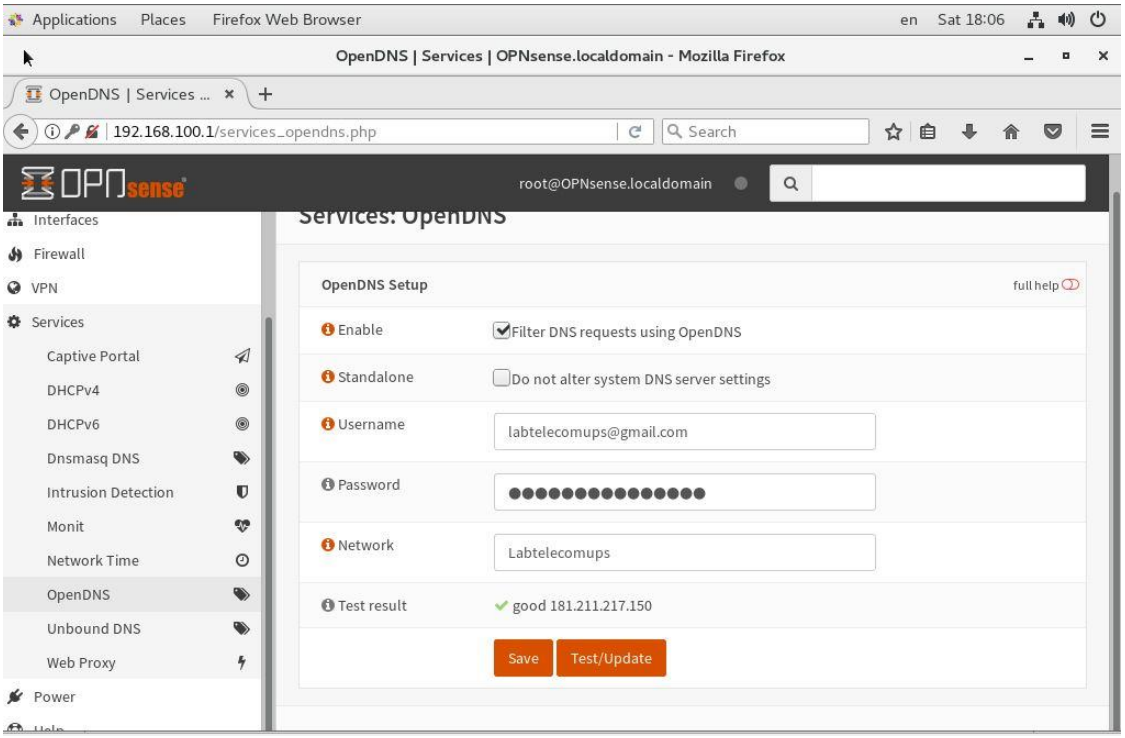




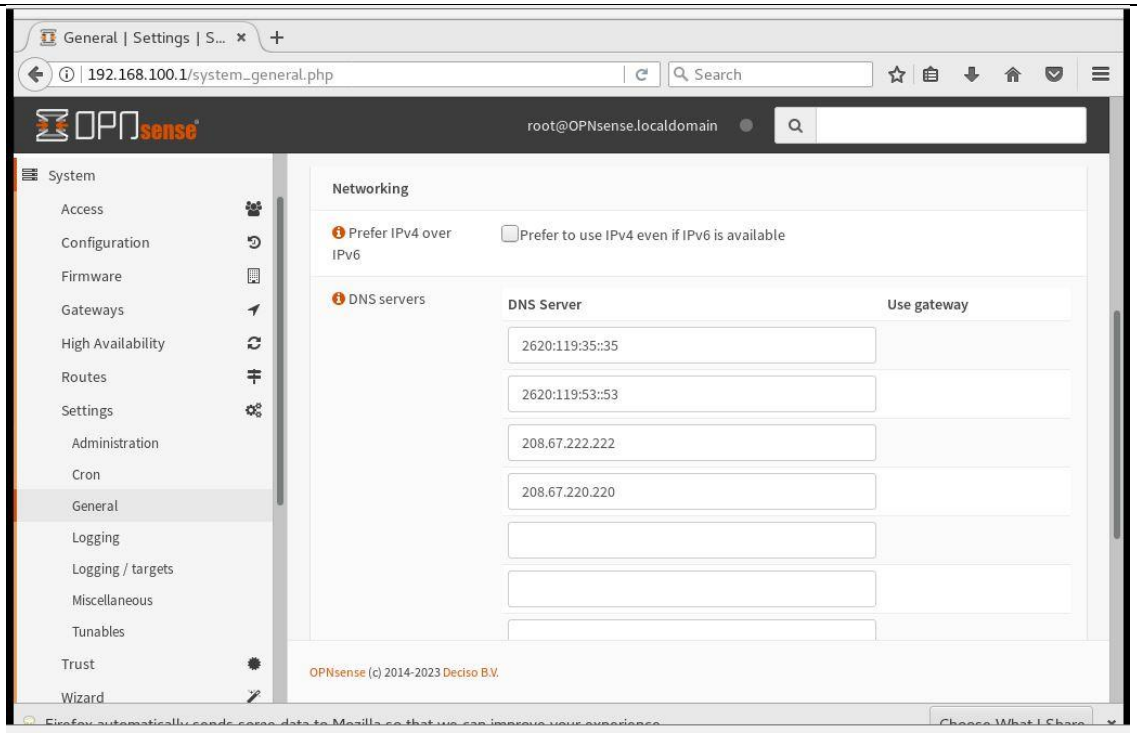
6. En la opción de seguridad queda todo por defecto ya que esta bloqueando redes maliciosas que usan DNS para acceder a las redes.



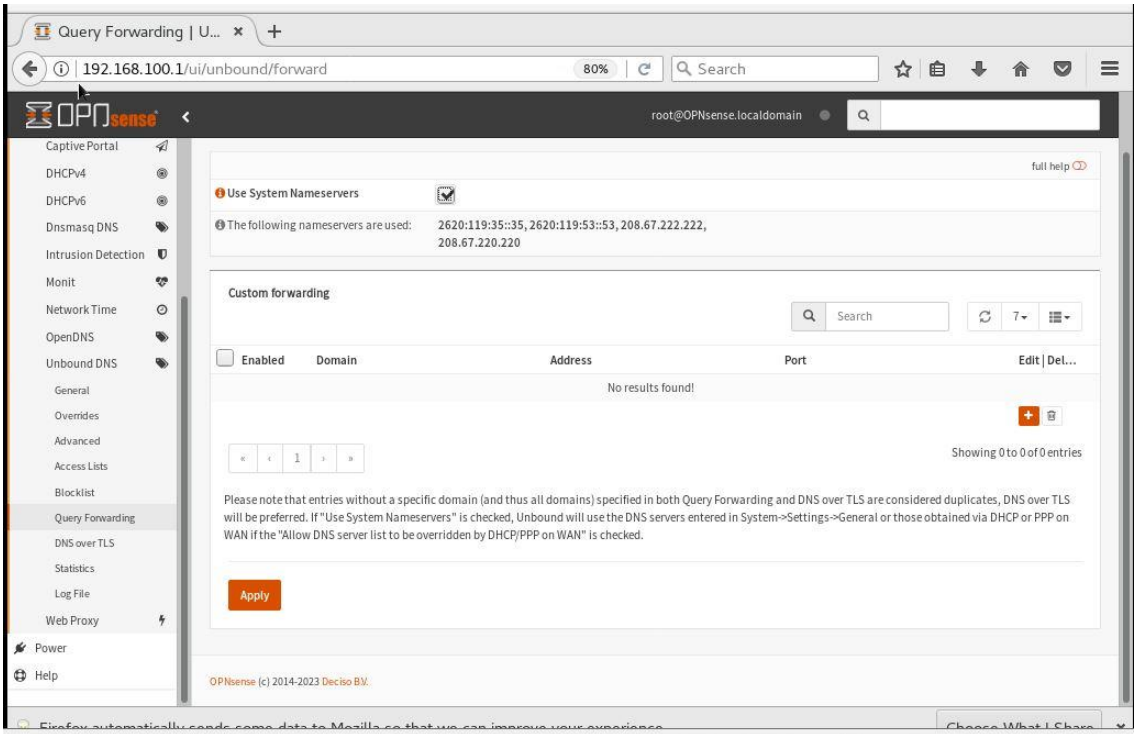
7. En la opción de Customization, se ubica el logo de la universidad, para tomar como referencia.



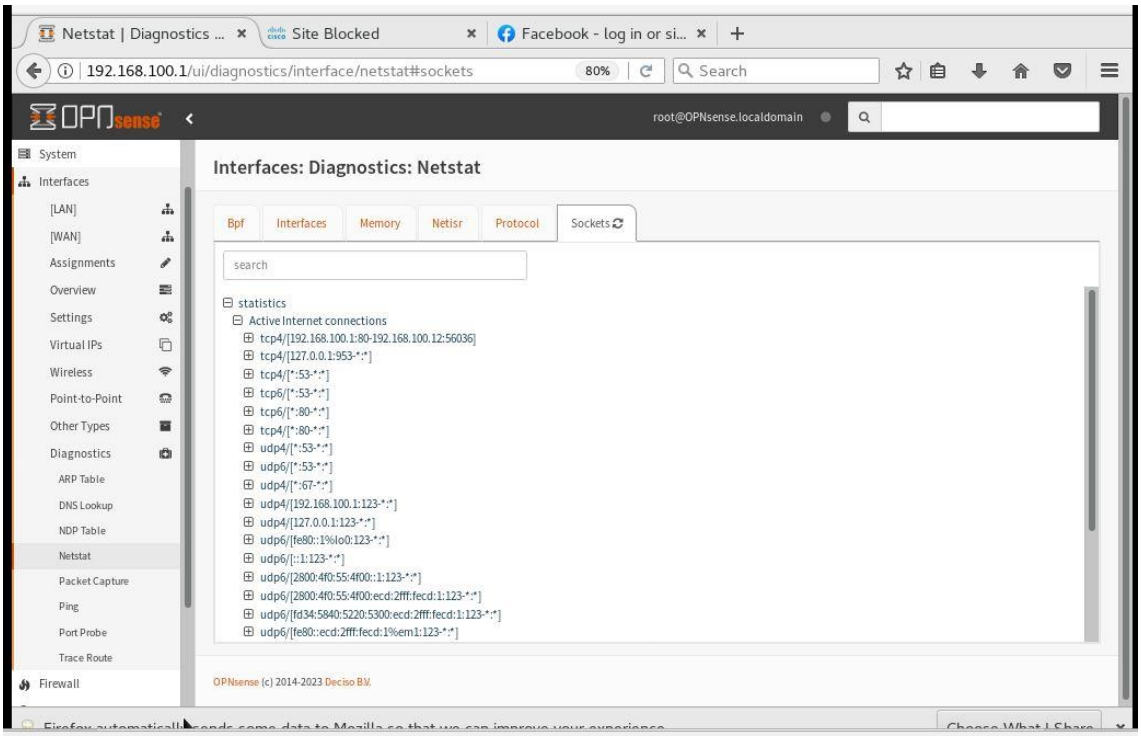
8. Se ingresa a OPNSense, dirigirse a la opcion de Services, OpenDNS y se habilita el proceso de usar OpenDNS colocando el correo que se creo al inicio con la clave del mismo y selecionando la red a usar. Se ejecuta el Test y el resultado es good cuando se conecta con el equipo.

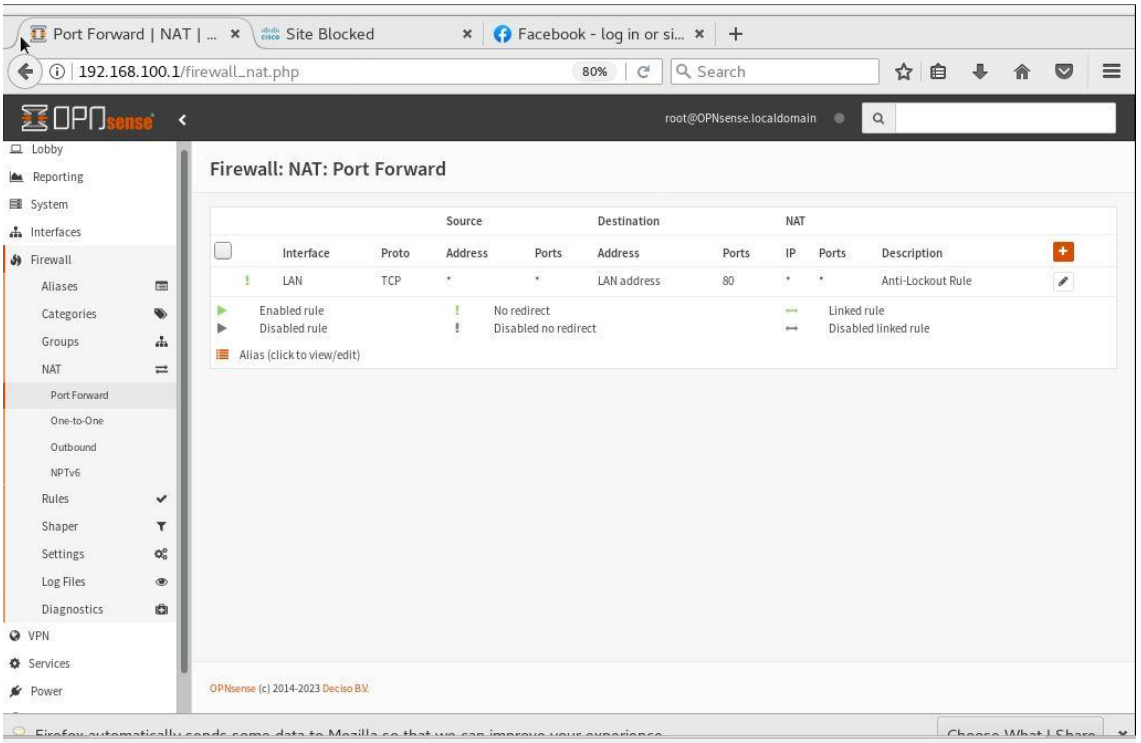


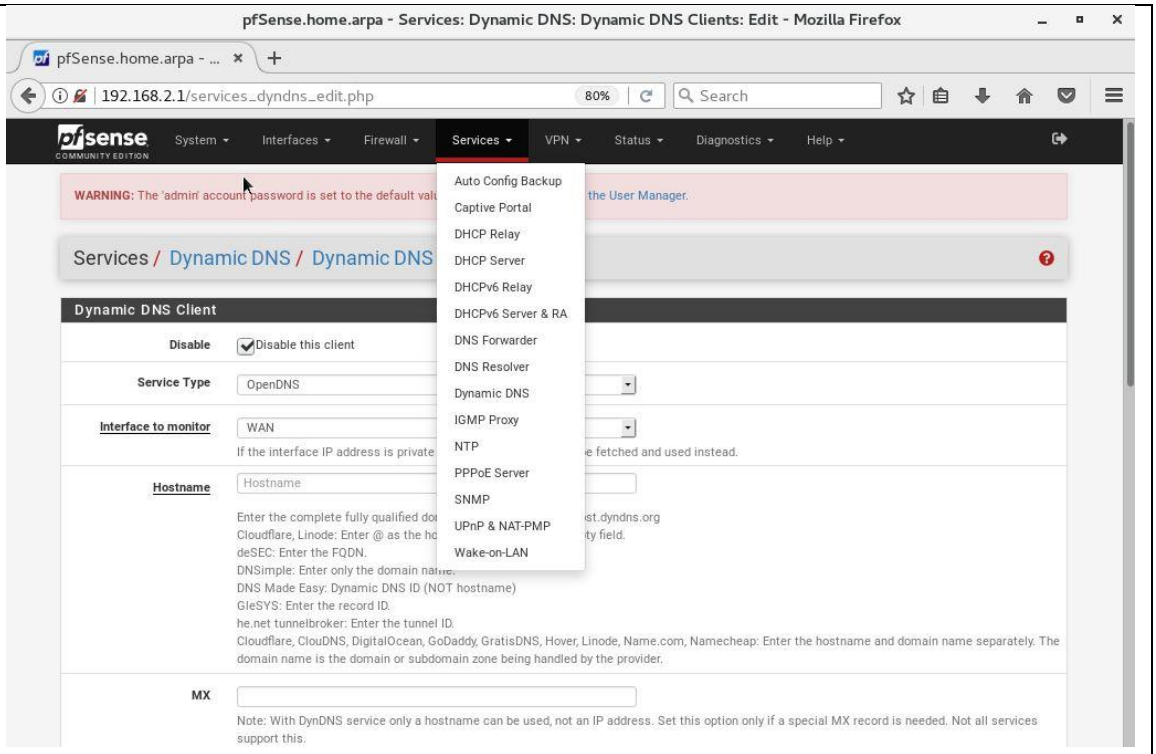
9. Dirigirse a la opción de Systema, General y dentro del mismo ir a DNS Server de OPNSense en la cual se va a reflejar los DNS que estan configurados por OPENDns.



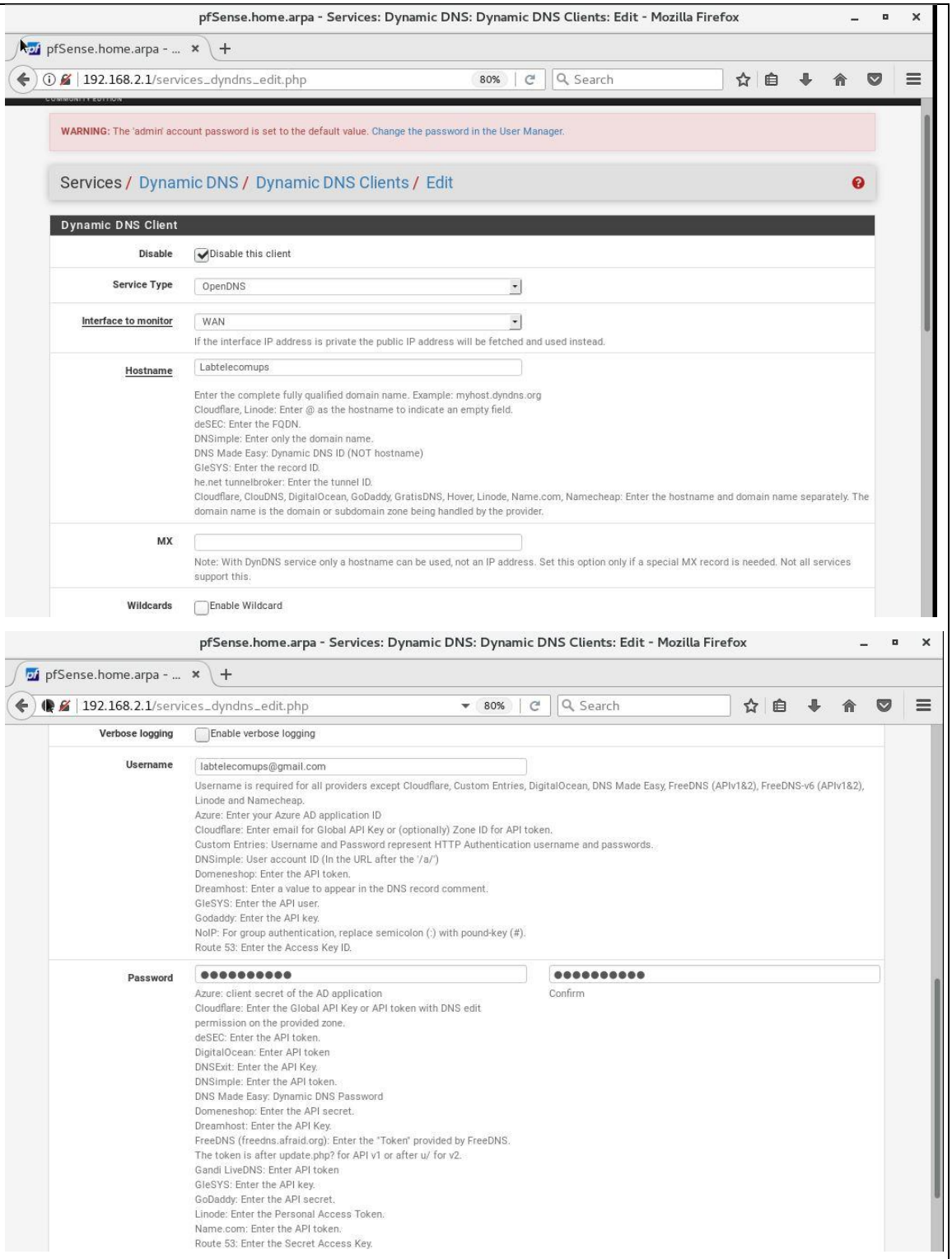
10. Dirigirse a la opción de Services Query Forwarding y dar un check en la opción de Use Systems Nameservers



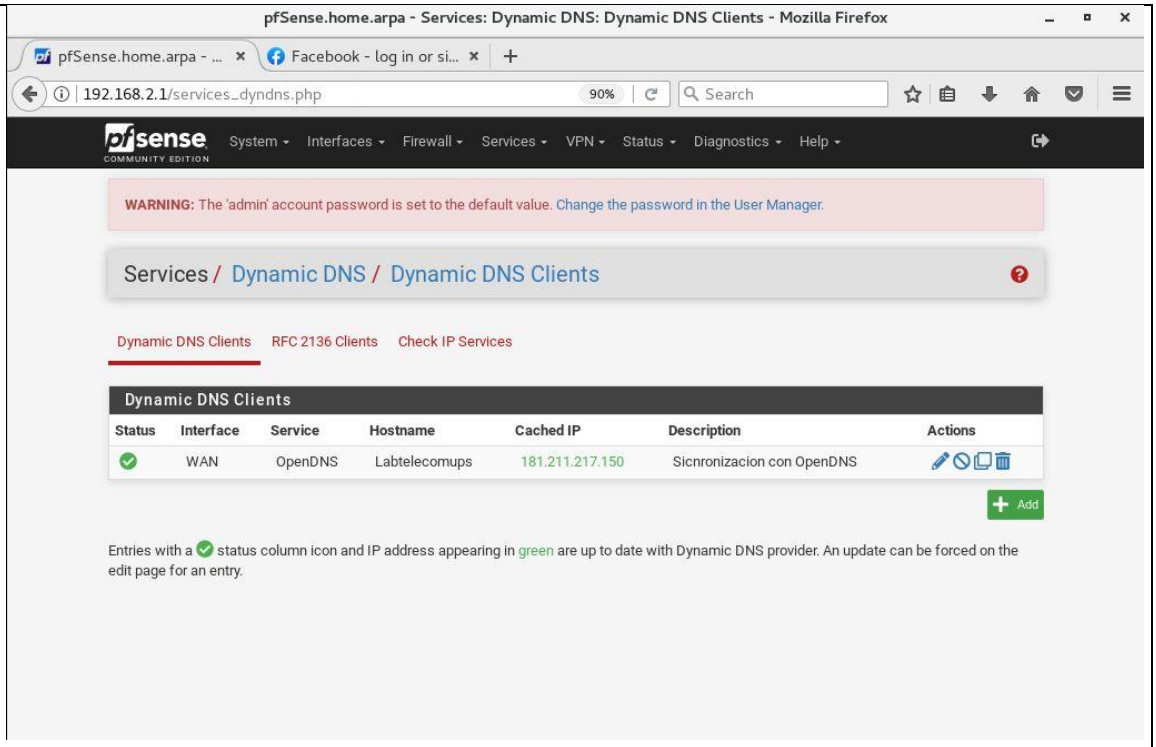




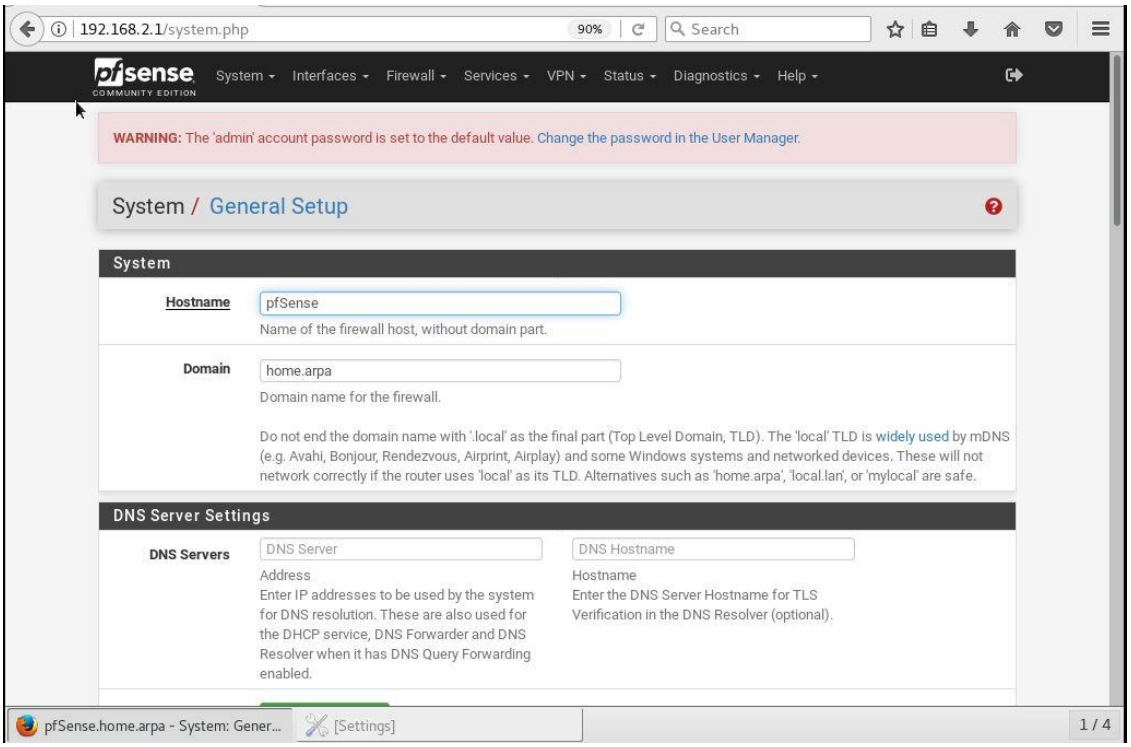
11. En pfsense, dirigirse a la opción de Services Dynamics DNS y dar check en Disable this client.

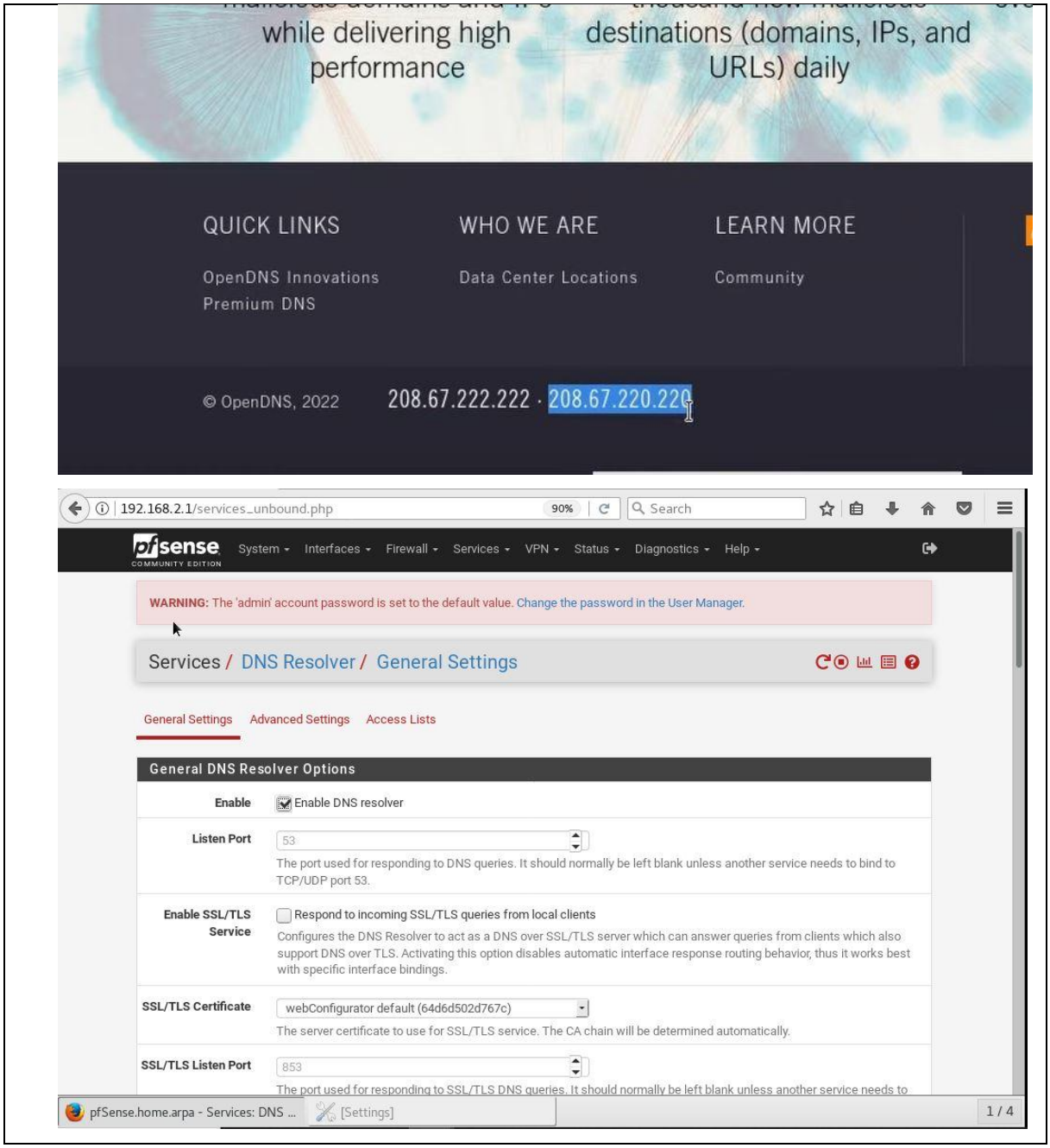


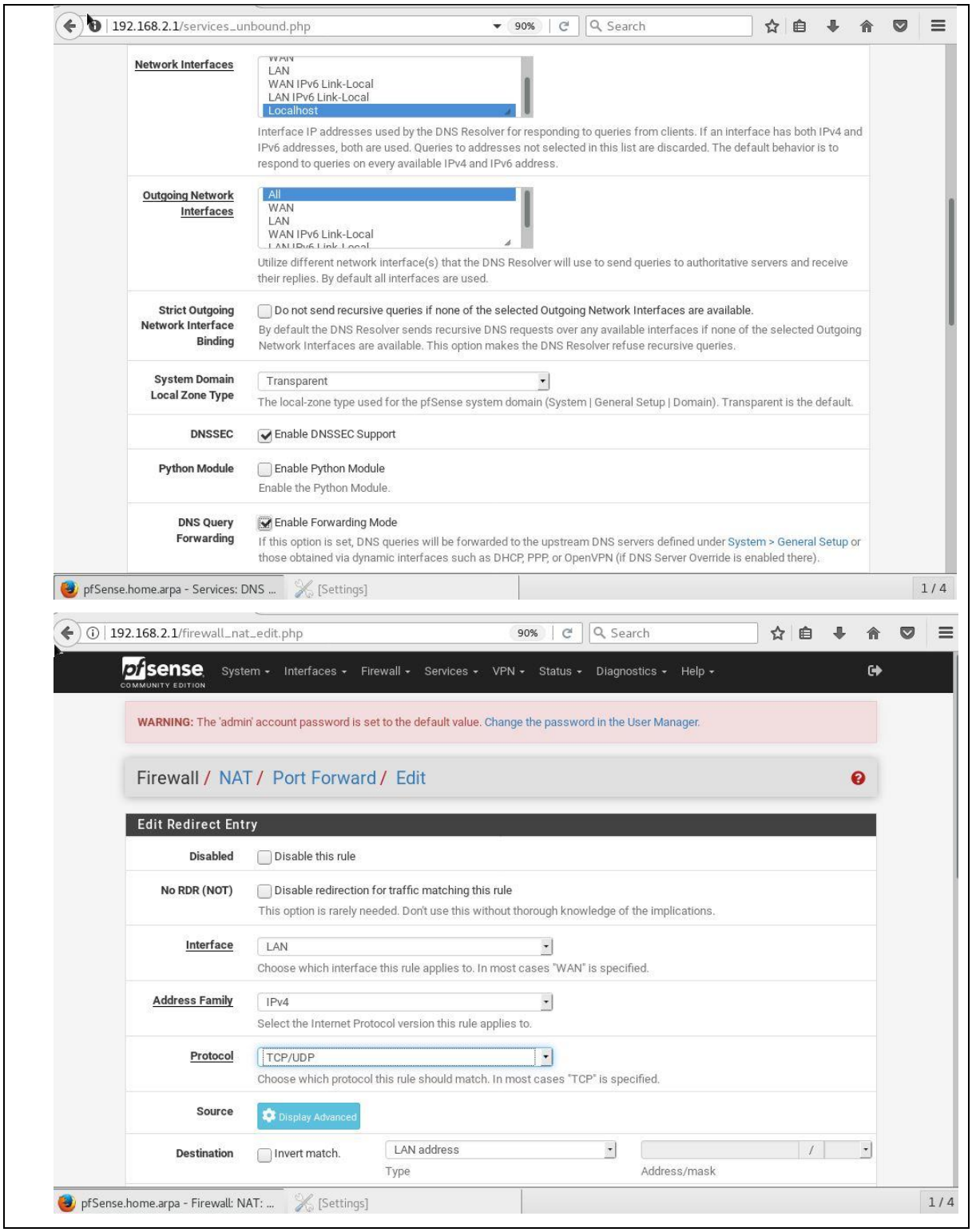
12. Se coloca el usuario y la clave de Open DNS para el registro de los DNS.

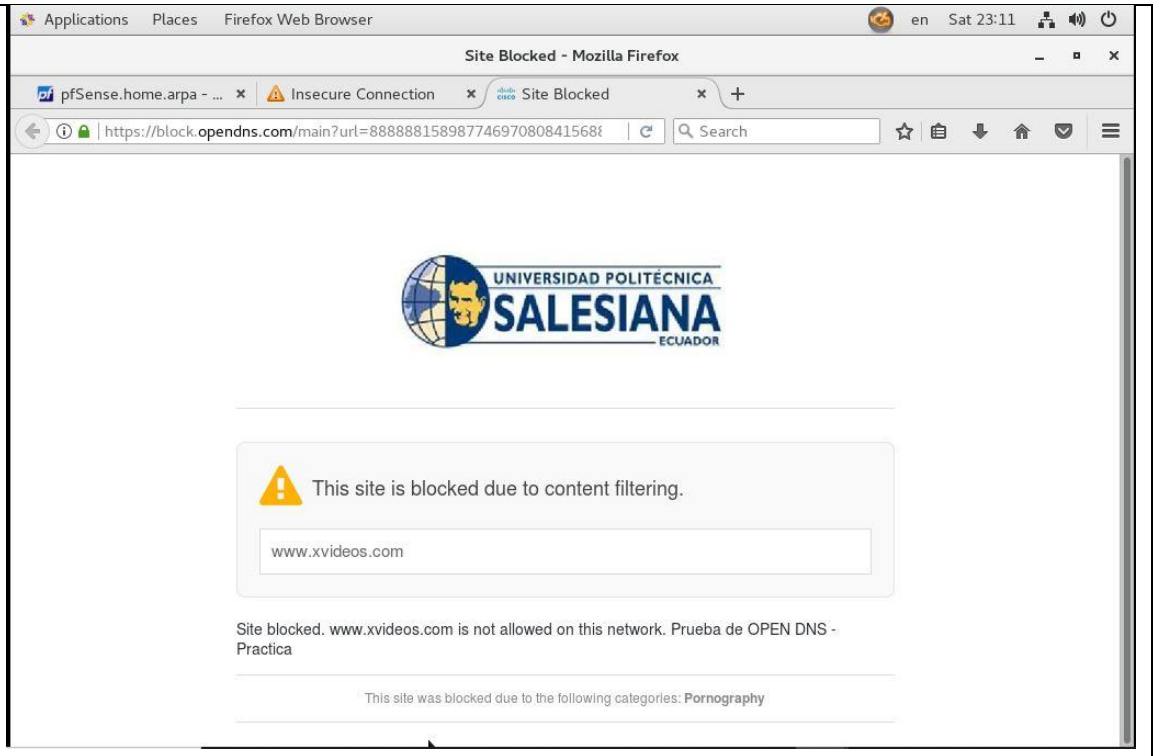


13. Con esta opción se queda sincronizada el registro de DNS con OpenDns en Pfsense.




while delivering high performance
destinations (domains, IPs, and URLs) daily
QUICK LINKS
OpenDNS Innovations
Premium DNS
WHO WE ARE
Data Center Locations
LEARN MORE
Community
© OpenDNS, 2022
208.67.222.222 · 208.67.220.220
192.168.2.1/services_unbound.php
Search
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / DNS Resolver / General Settings
General Settings
Advanced Settings
Access Lists
General DNS Resolver Options
Enable
Enable DNS resolver
Listen Port
53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.
Enable SSL/TLS Service
Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.
SSL/TLS Certificate
webConfigurator default (64d6d502d767c)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.
SSL/TLS Listen Port
853
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to
pfSense.home.arpa - Services: DNS ...
[Settings]
1 / 4


192.168.2.1/services_unbound.php
Search
Network Interfaces
LAN
WAN IPv6 Link-Local
LAN IPv6 Link-Local
Localhost
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.
Outgoing Network Interfaces
All
WAN
LAN
WAN IPv6 Link-Local
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.
Strict Outgoing Network Interface Binding
Do not send recursive queries if none of the selected Outgoing Network Interfaces are available.
By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.
System Domain Local Zone Type
Transparent
The local-zone type used for the pfSense system domain (System | General Setup | Domain). Transparent is the default.
DNSSEC
Enable DNSSEC Support
Python Module
Enable Python Module
Enable the Python Module.
DNS Query Forwarding
Enable Forwarding Mode
If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).
pfSense.home.arpa - Services: DNS ...
[Settings]
1 / 4
192.168.2.1/firewall_nat_edit.php
Search
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / NAT / Port Forward / Edit
Edit Redirect Entry
Disabled
Disable this rule
No RDR (NOT)
Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface
LAN
Choose which interface this rule applies to. In most cases "WAN" is specified.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
TCP/UDP
Choose which protocol this rule should match. In most cases "TCP" is specified.
Source
Display Advanced
Destination
Invert match.
LAN address
Type
Address/mask
pfSense.home.arpa - Firewall: NAT: ...
[Settings]
1 / 4



RESULTADO(S) OBTENIDO(S):

El estudiante se familiariza con el uso de la aplicación OPENDNS que permite configurar firewalls de tal manera que evite el ingreso de actividad maliciosa atraves del Servicio DNS.

CONCLUSIONES:

El estudiante aprende sobre el uso de la herramienta OpenDNS, configura en pfSense y OpenDNS para la gestión respectiva de la resolución de nombres como el bloqueo de las paginas por el dominio y sus diferentes categorías.

RECOMENDACIONES:

Realizar pruebas de bloqueo de dominios a través de OpenDNS.

Docente: _____

Firma: _____

4.8. PRÁCTICA # 8

UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR	**FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES**
Carrera: Ingeniería Electrónica	**Asignatura:** Redes de Computadoras
NRO. Práctica: 8	**Título Práctica:** Configuración de Doble Autenticación con pfSense y FreeRadius

OBJETIVO:

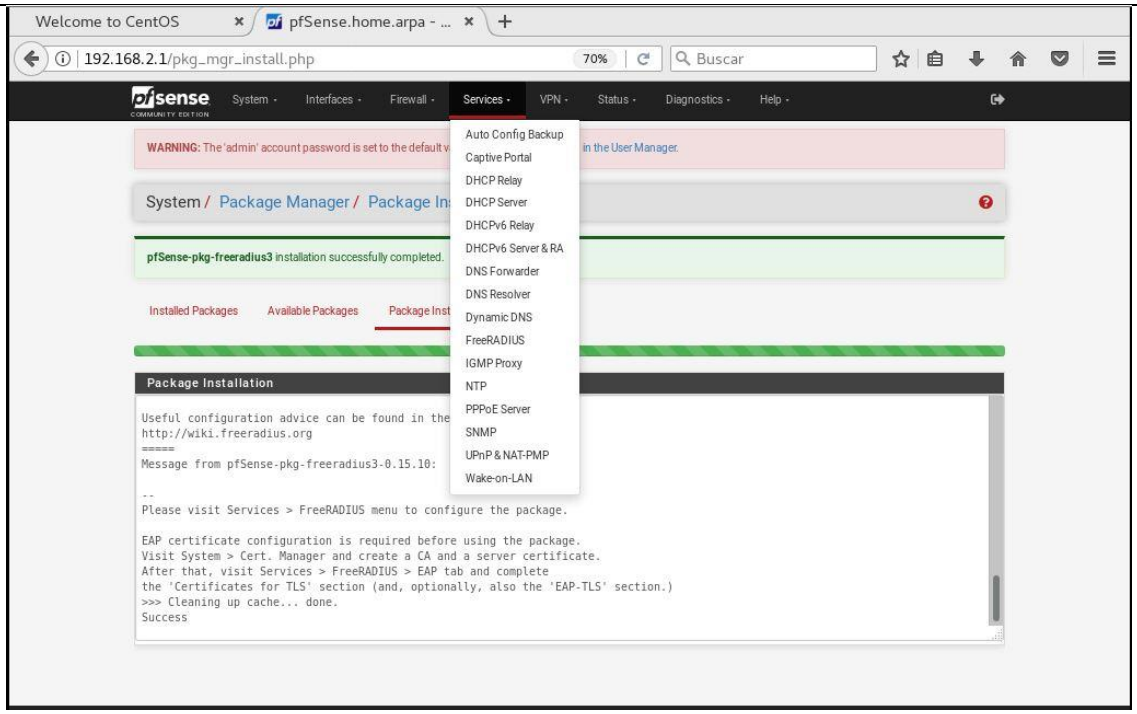
- **Objetivo General**

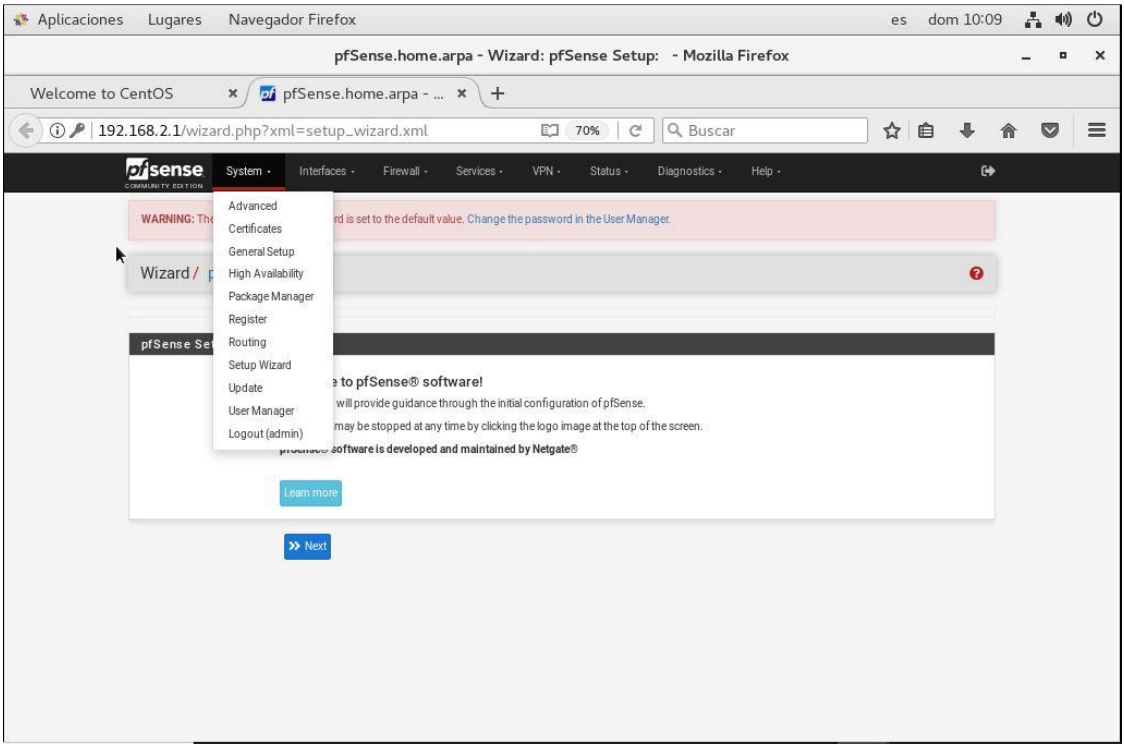
Implementar la autenticación de doble factor (Doble Autenticación) en una red utilizando pfSense como firewall y FreeRadius como servidor de autenticación.

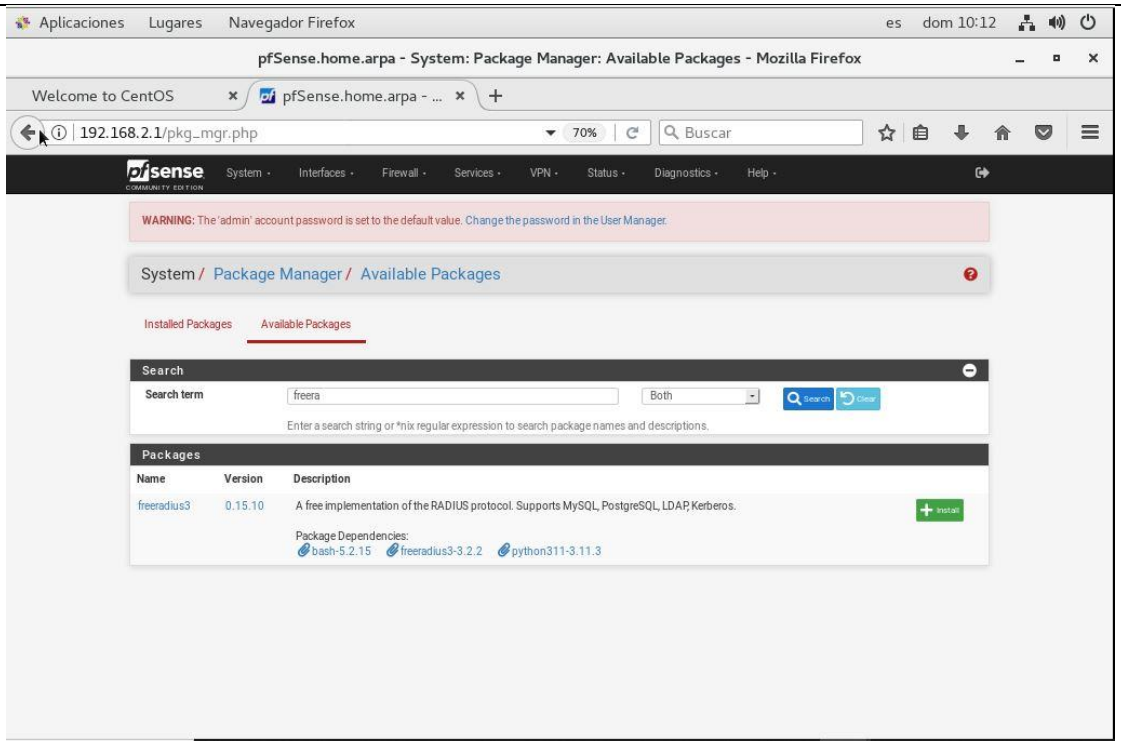
INSTRUCCIONES:	1. Configurar usuarios y contraseñas en FreeRadius para autenticación de doble factor 2. Configurar las políticas de acceso en FreeRadius para definir qué usuarios tienen acceso a la red y en qué condiciones. 3. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.

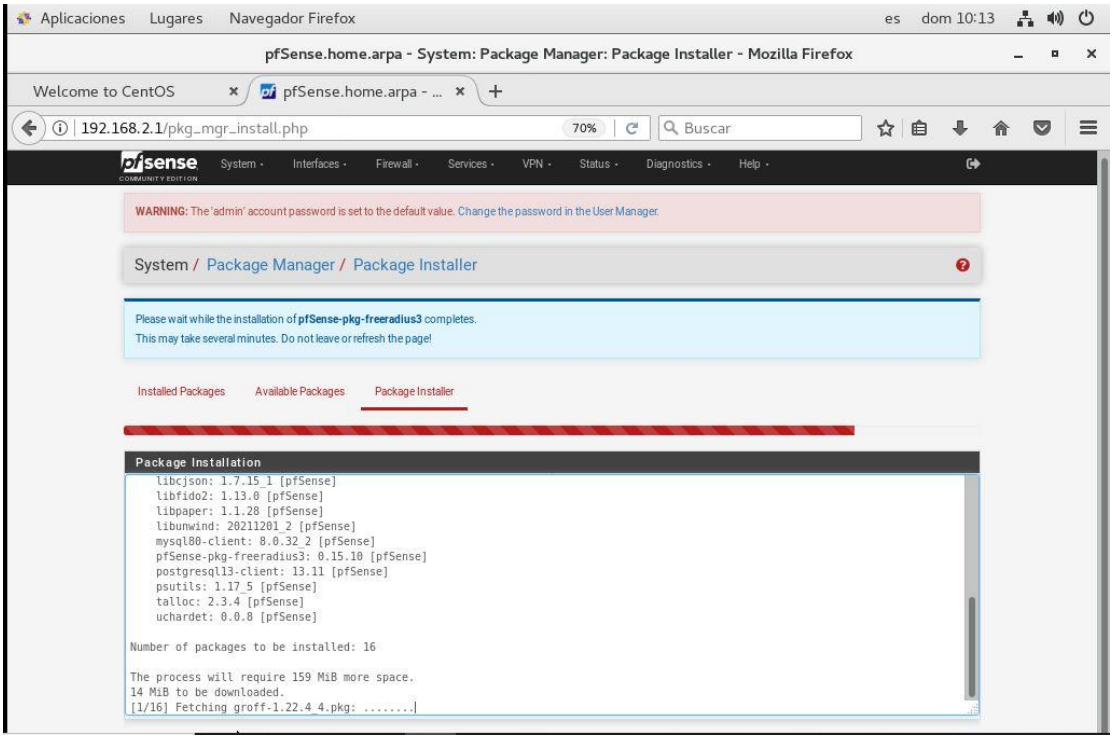
ACTIVIDADES POR DESARROLLAR

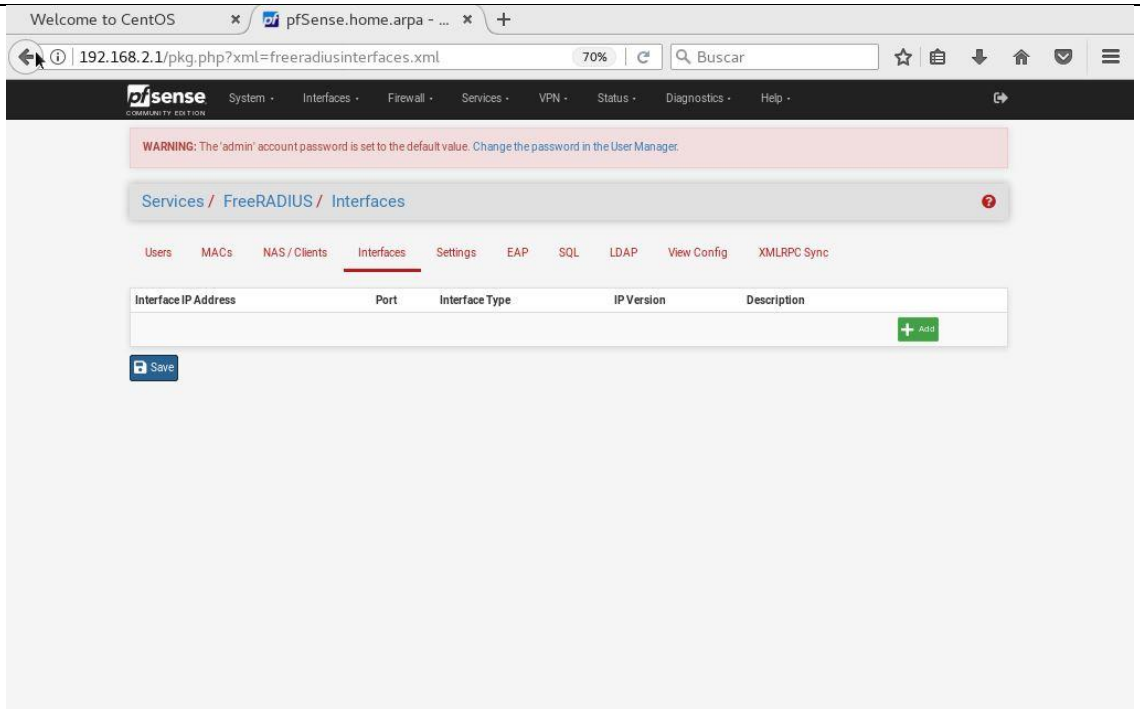
1. Instalar de la aplicación FreeRadius en pfSense


Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg_mgr_install.php
Buscar
System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -
Auto Config Backup
Captive Portal
DHCP Relay
DHCP Server
DHCPv6 Relay
DHCPv6 Server & RA
DNS Forwarder
DNS Resolver
Dynamic DNS
FreeRADIUS
IGMP Proxy
NTP
PPPoE Server
SNMP
UPnP & NAT-PMP
Wake-on-LAN
System / Package Manager / Package In
pfSense-pkg-freeradius3 installation successfully completed.
Installed Packages
Available Packages
Package Inst
Package Installation
Useful configuration advice can be found in the
http://wiki.freeradius.org
Message from pfSense-pkg-freeradius3-0.15.10:
Please visit Services > FreeRADIUS menu to configure the package.
EAP certificate configuration is required before using the package.
Visit System > Cert. Manager and create a CA and a server certificate.
After that, visit Services > FreeRADIUS > EAP tab and complete
the 'Certificates for TLS' section (and, optionally, also the 'EAP-TLS' section.)
>>> Cleaning up cache... done.
Success

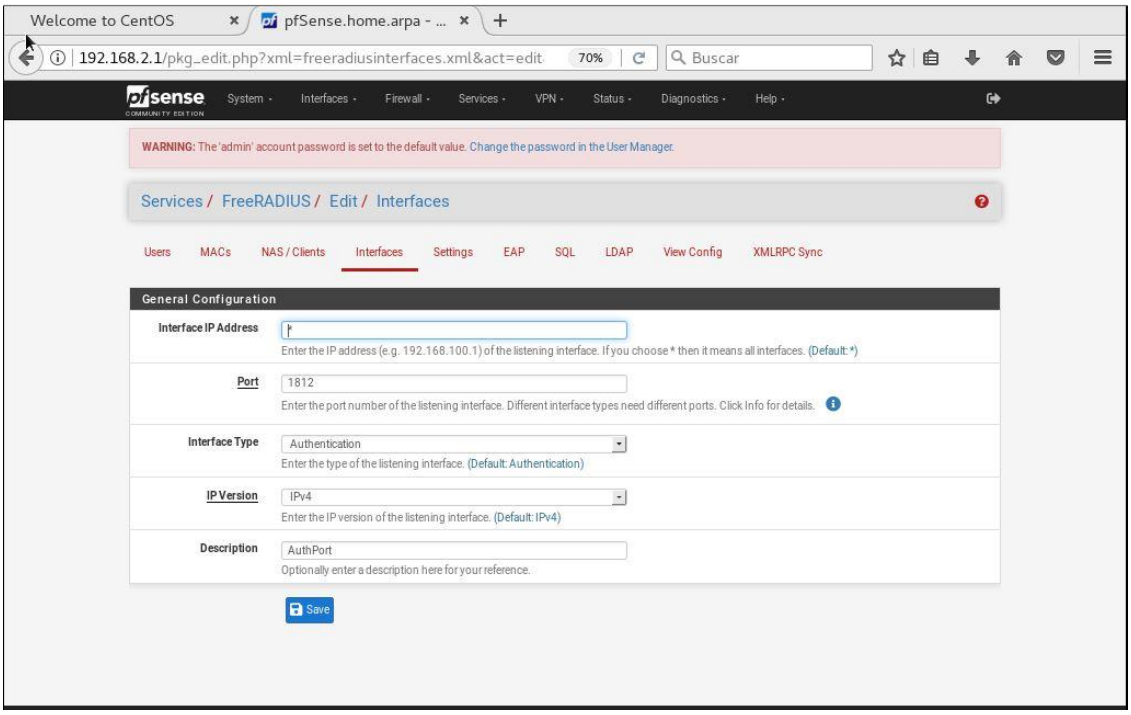

Aplicaciones Lugares Navegador Firefox
es dom 10:09
pfSense.home.arpa - Wizard: pfSense Setup: - Mozilla Firefox
Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/wizard.php?xml=setup_wizard.xml
Buscar
System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -
Advanced
Certificates
General Setup
High Availability
Package Manager
Register
Routing
Setup Wizard
Update
User Manager
Logout (admin)
Change the password in the User Manager.
Wizard /
to pfSense® software!
will provide guidance through the initial configuration of pfSense.
may be stopped at any time by clicking the logo image at the top of the screen.
software is developed and maintained by Netgate®
Learn more
Next

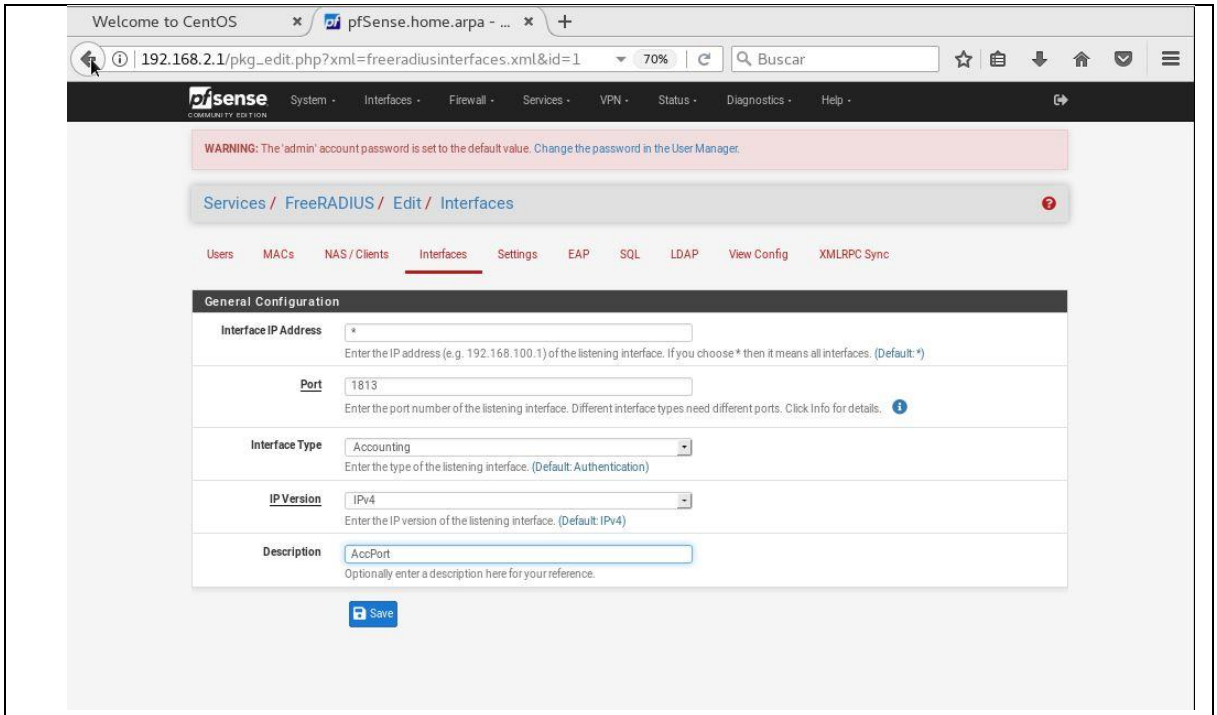

Aplicaciones Lugares Navegador Firefox es dom 10:12
pfSense.home.arpa - System: Package Manager: Available Packages - Mozilla Firefox
Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg_mgr.php
70%
Buscar
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
System / Package Manager / Available Packages
Installed Packages
Available Packages
Search
Search term
freera
Both
Search
Clear
Enter a search string or *nix regular expression to search package names and descriptions.
Packages
Name
Version
Description
freeradius3
0.15.10
A free implementation of the RADIUS protocol. Supports MySQL, PostgreSQL, LDAP, Kerberos.
Install
Package Dependencies:
bash-5.2.15
freeradius3-3.2.2
python311-3.11.3

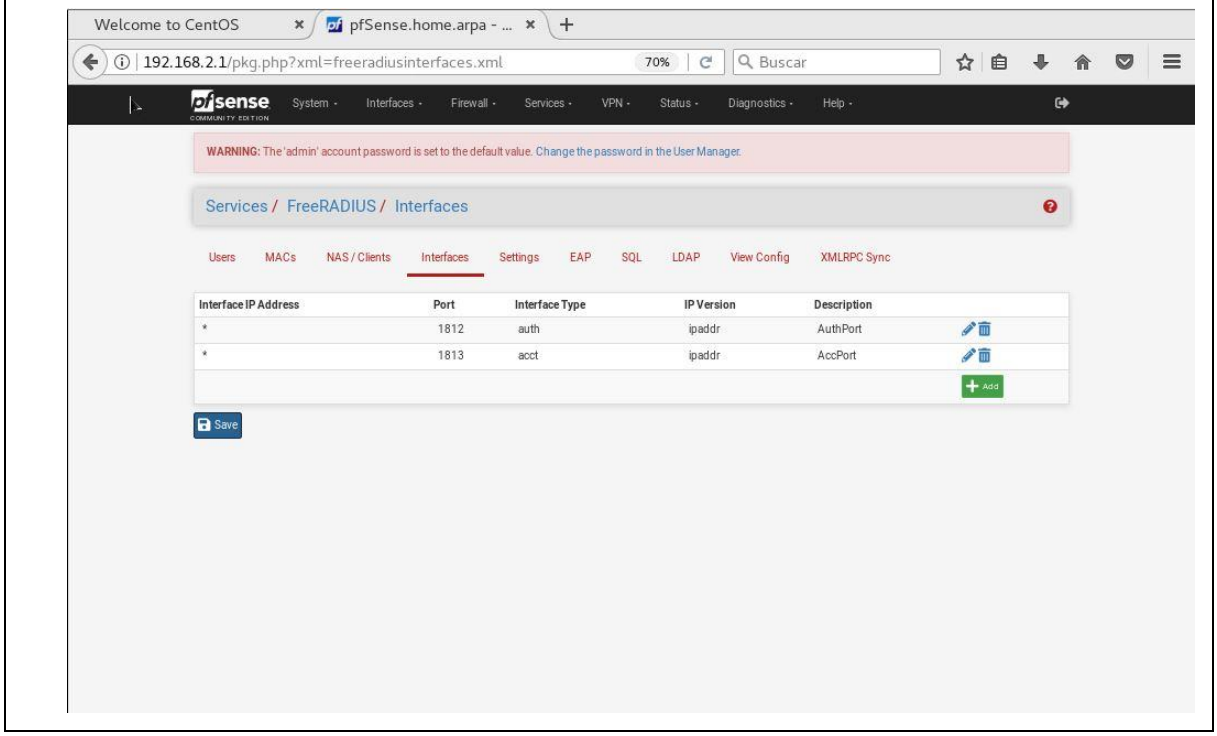

Aplicaciones Lugares Navegador Firefox es dom 10:13
pfSense.home.arpa - System: Package Manager: Package Installer - Mozilla Firefox
Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg_mgr_install.php
70%
Buscar
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
System / Package Manager / Package Installer
Please wait while the installation of pfSense-pkg-freeradius3 completes.
This may take several minutes. Do not leave or refresh the page!
Installed Packages
Available Packages
Package Installer
Package Installation
libcjson: 1.7.15_1 [pfSense]
libfido2: 1.13.0 [pfSense]
libpaper: 1.1.28 [pfSense]
libunwind: 20211201_2 [pfSense]
mysql80-client: 8.0.32_2 [pfSense]
pfSense-pkg-freeradius3: 0.15.10 [pfSense]
postgresql13-client: 13.11 [pfSense]
psutils: 1.17_5 [pfSense]
talloc: 2.3.4 [pfSense]
uchardet: 0.0.8 [pfSense]
Number of packages to be installed: 16
The process will require 159 MiB more space.
14 MiB to be downloaded.
[1/16] Fetching groff-1.22.4_4.pkg: .....

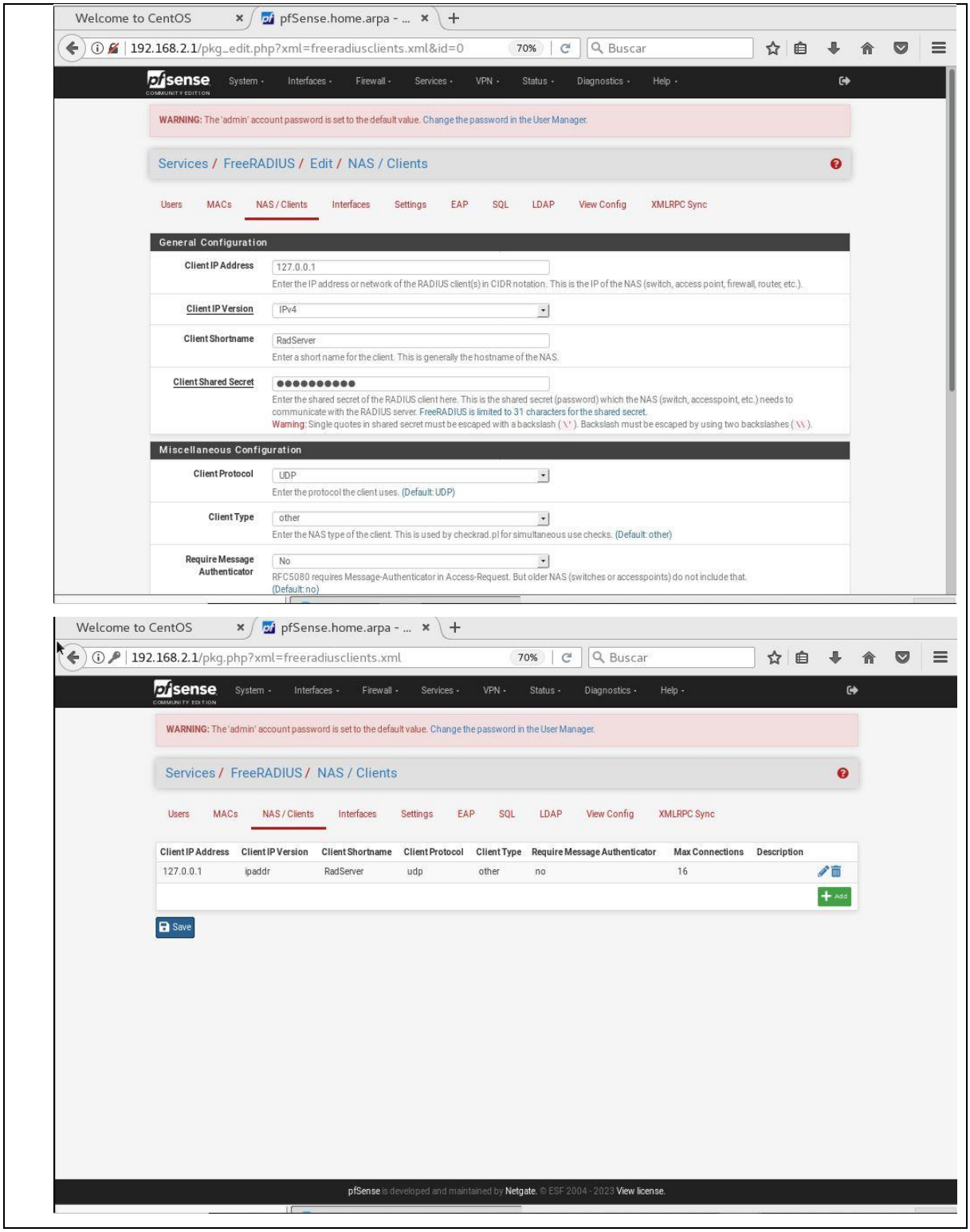


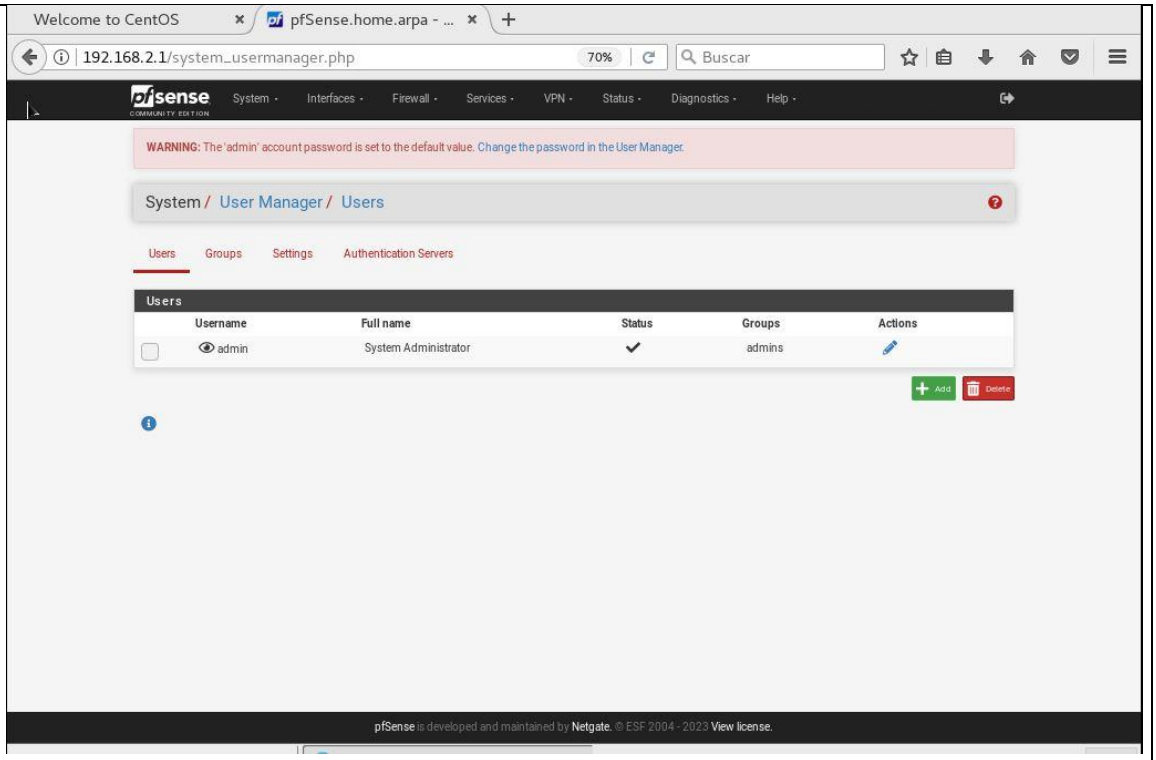
2. Dirigirse a Services – FreeRadius – Interfaces para comenzar a configurar las interfces.



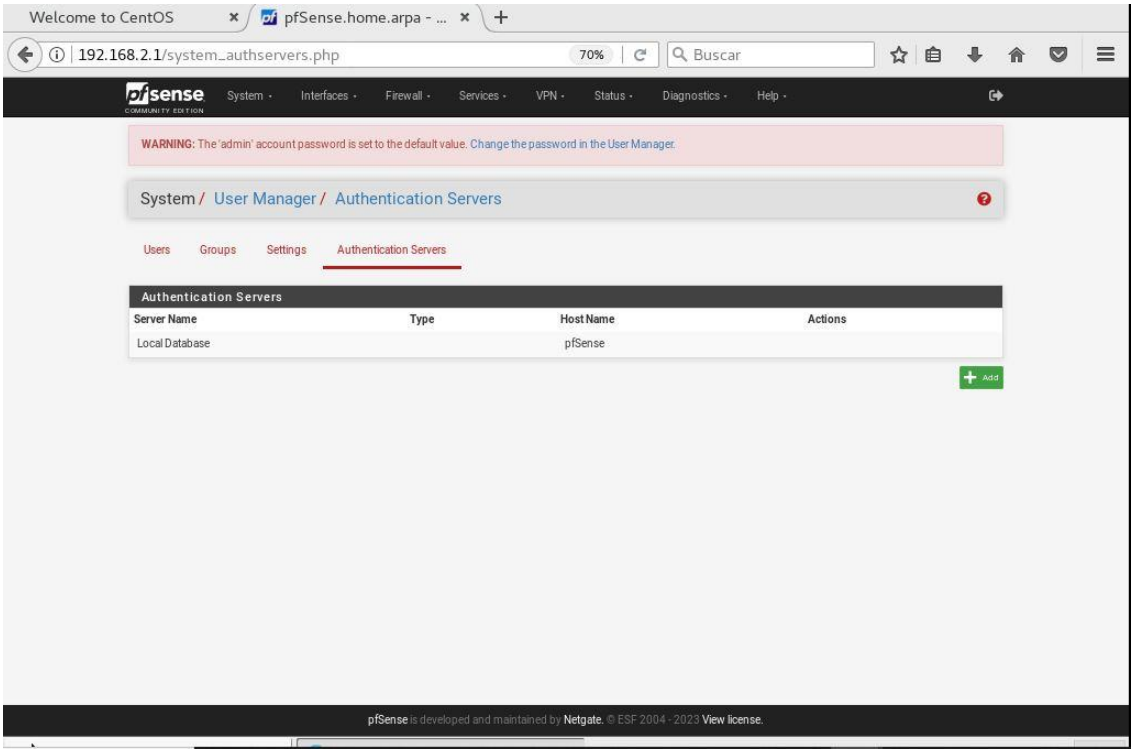

Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg_edit.php?xml=freeradiusinterfaces.xml&id=1
70%
Buscar
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / FreeRADIUS / Edit / Interfaces
Users
MACs
NAS / Clients
Interfaces
Settings
EAP
SQL
LDAP
View Config
XMLRPC Sync
General Configuration
Interface IP Address
*
Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)
Port
1813
Enter the port number of the listening interface. Different interface types need different ports. Click Info for details.
Interface Type
Accounting
Enter the type of the listening interface. (Default: Authentication)
IP Version
IPv4
Enter the IP version of the listening interface. (Default: IPv4)
Description
AccPort
Optionally enter a description here for your reference.
Save

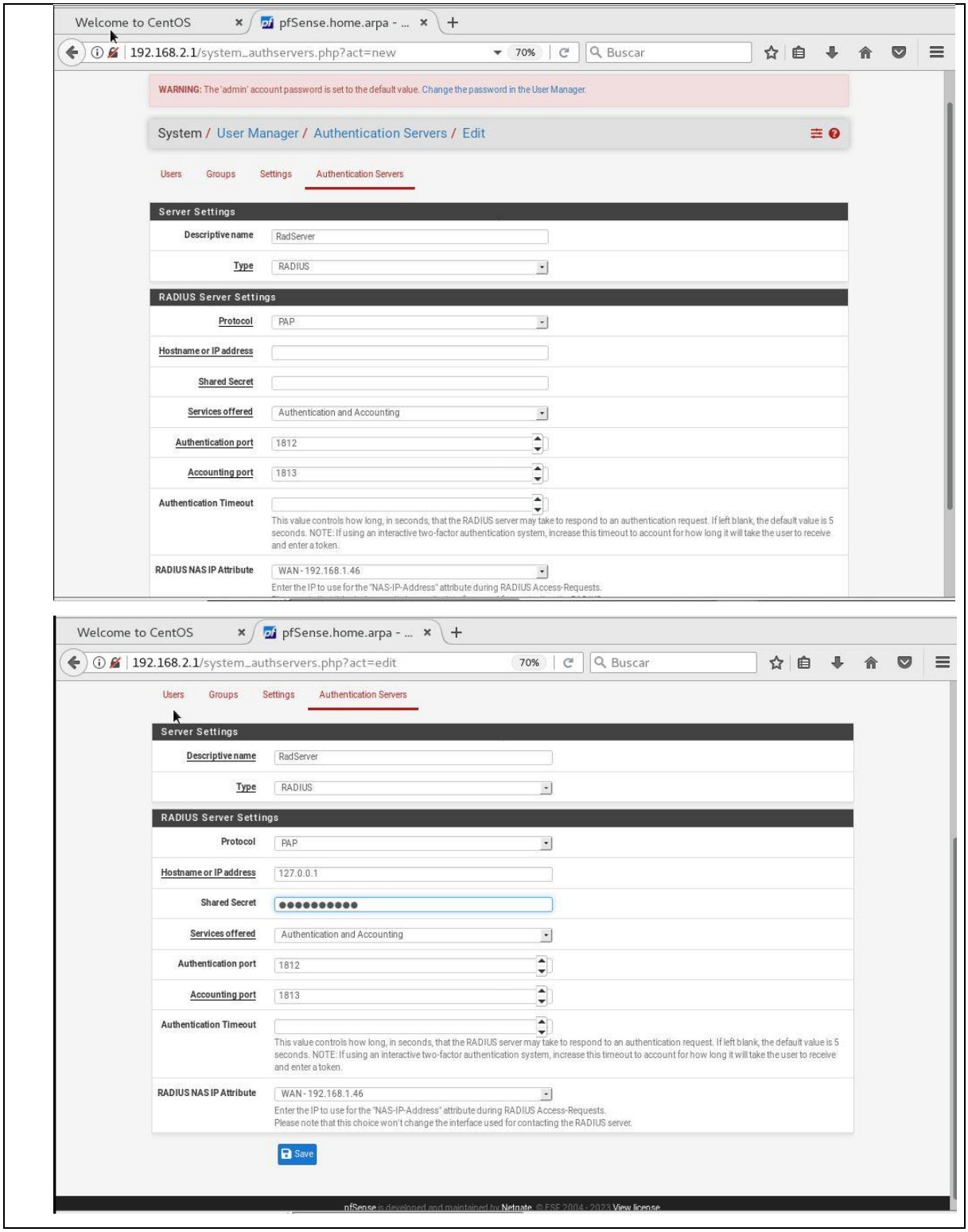

Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg.php?xml=freeradiusinterfaces.xml
70%
Buscar
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / FreeRADIUS / Interfaces
Users
MACs
NAS / Clients
Interfaces
Settings
EAP
SQL
LDAP
View Config
XMLRPC Sync
Interface IP Address
Port
Interface Type
IP Version
Description
* 1812 auth ipaddr AuthPort
* 1813 acct ipaddr AccPort
Add
Save

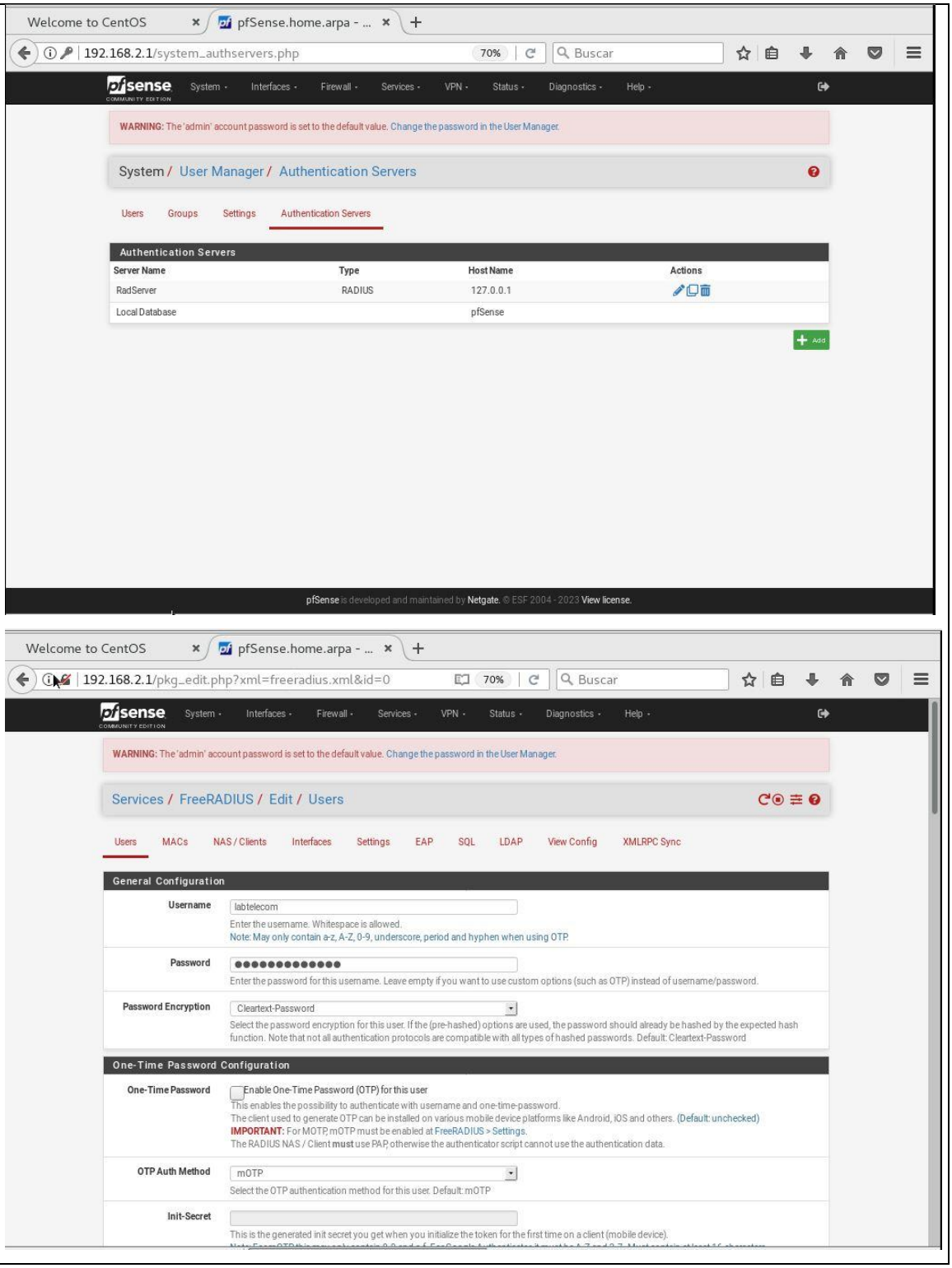

Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg_edit.php?xml=freeradiusclients.xml&id=0
Buscar
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / FreeRADIUS / Edit / NAS / Clients
Users
MACs
NAS / Clients
Interfaces
Settings
EAP
SQL
LDAP
View Config
XMLRPC Sync
General Configuration
Client IP Address
127.0.0.1
Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).
Client IP Version
IPv4
Client Shortname
RadServer
Enter a short name for the client. This is generally the hostname of the NAS.
Client Shared Secret
Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret.
Warning: Single quotes in shared secret must be escaped with a backslash (\'). Backslash must be escaped by using two backslashes (\\ ).
Miscellaneous Configuration
Client Protocol
UDP
Enter the protocol the client uses. (Default: UDP)
Client Type
other
Enter the NAS type of the client. This is used by checkrad.pl for simultaneous use checks. (Default: other)
Require Message Authenticator
No
RFC5080 requires Message-Authenticator in Access-Request. But older NAS (switches or accesspoints) do not include that. (Default: no)
Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg.php?xml=freeradiusclients.xml
Buscar
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / FreeRADIUS / NAS / Clients
Users
MACs
NAS / Clients
Interfaces
Settings
EAP
SQL
LDAP
View Config
XMLRPC Sync
Client IP Address
Client IP Version
Client Shortname
Client Protocol
Client Type
Require Message Authenticator
Max Connections
Description
127.0.0.1
ipaddr
RadServer
udp
other
no
16
Add
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

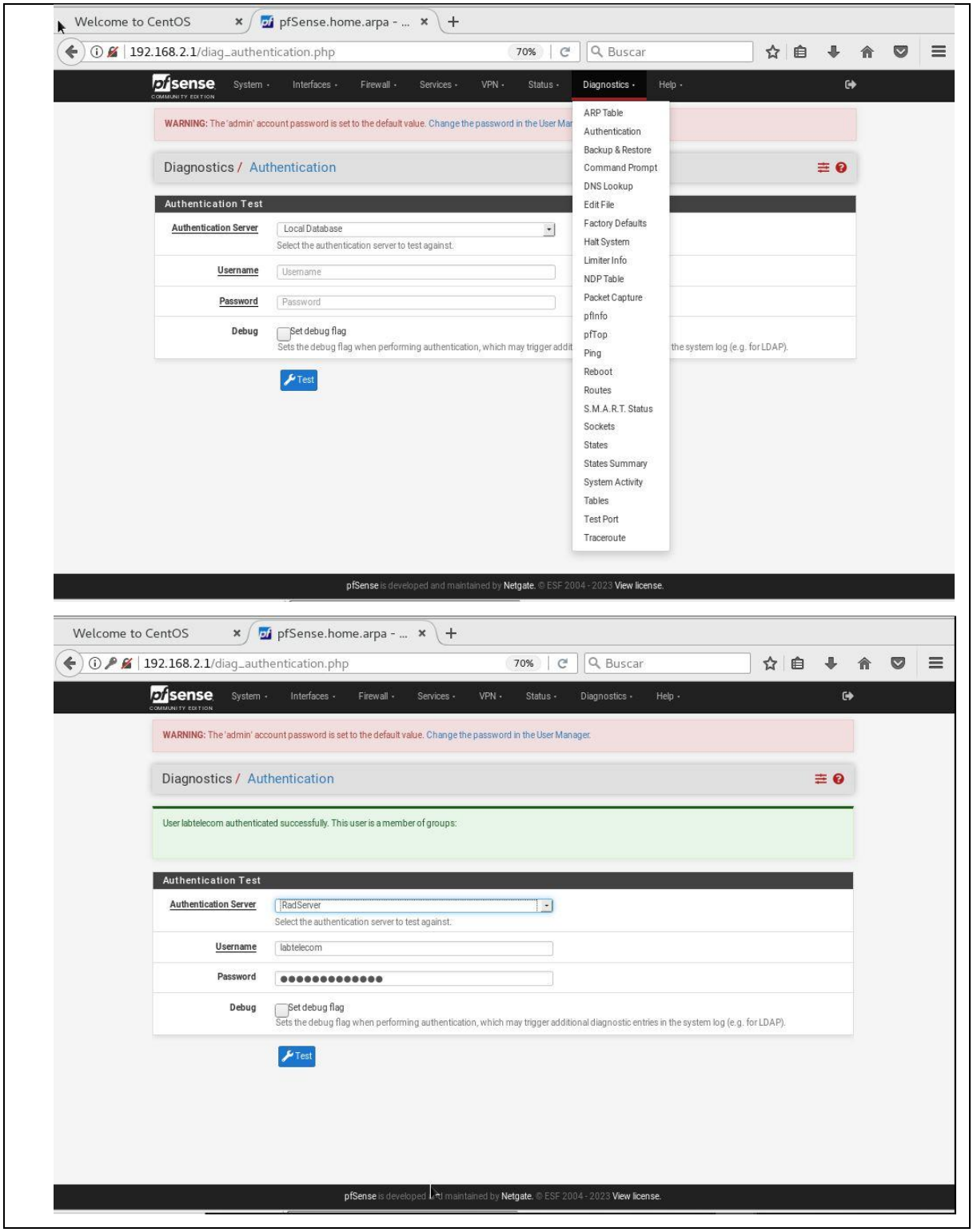


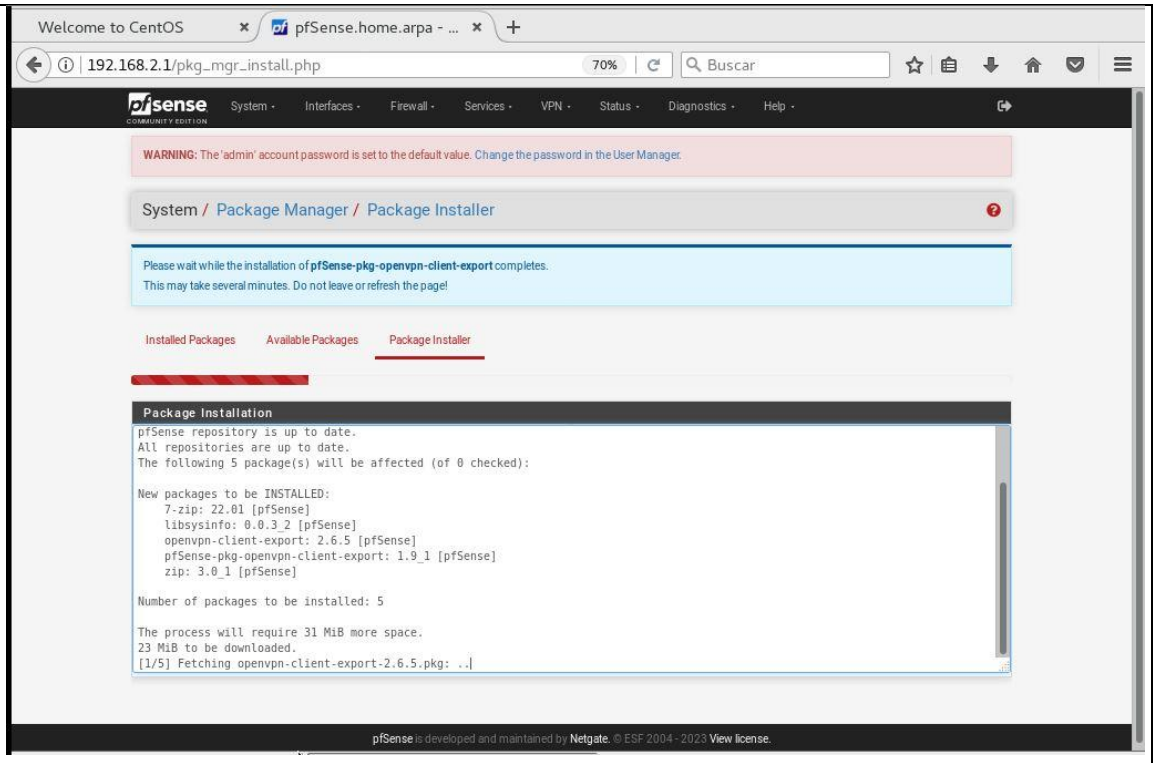
3. Dirigirse a System – User Manager – User y dirigirse a Authentication Servers agregando el FreeRadius

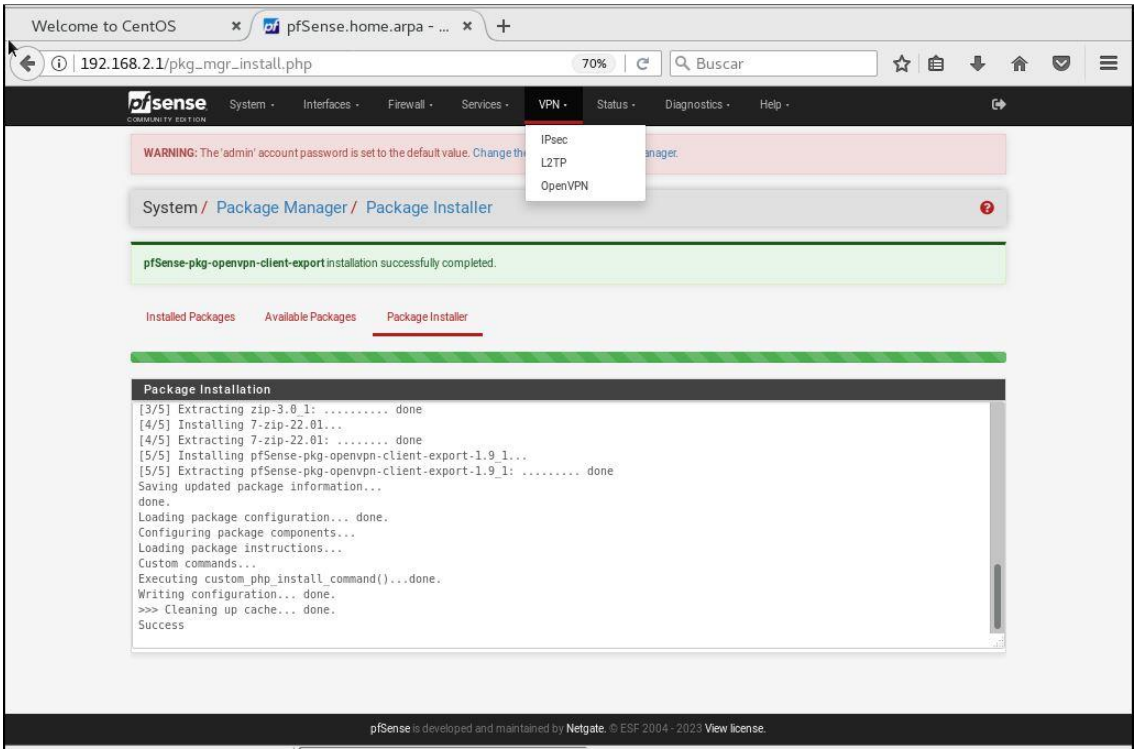


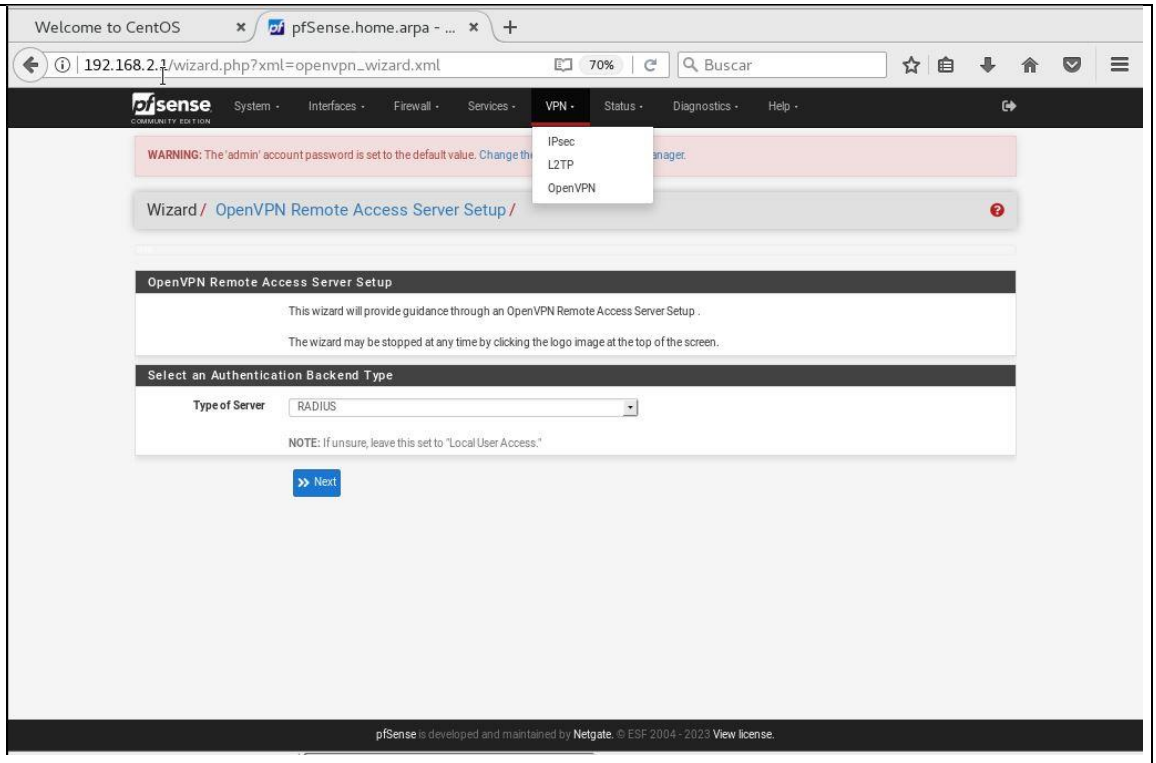

Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/system_authservers.php?act=new
70%
Buscar
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
System / User Manager / Authentication Servers / Edit
Users
Groups
Settings
Authentication Servers
Server Settings
Descriptive name
RadServer
Type
RADIUS
RADIUS Server Settings
Protocol
PAP
Hostname or IP address
Shared Secret
Services offered
Authentication and Accounting
Authentication port
1812
Accounting port
1813
Authentication Timeout
This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.
RADIUS NAS IP Attribute
WAN - 192.168.1.46
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests.
Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/system_authservers.php?act=edit
70%
Buscar
Users
Groups
Settings
Authentication Servers
Server Settings
Descriptive name
RadServer
Type
RADIUS
RADIUS Server Settings
Protocol
PAP
Hostname or IP address
127.0.0.1
Shared Secret
Services offered
Authentication and Accounting
Authentication port
1812
Accounting port
1813
Authentication Timeout
This value controls how long, in seconds, that the RADIUS server may take to respond to an authentication request. If left blank, the default value is 5 seconds. NOTE: If using an interactive two-factor authentication system, increase this timeout to account for how long it will take the user to receive and enter a token.
RADIUS NAS IP Attribute
WAN - 192.168.1.46
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests.
Please note that this choice won't change the interface used for contacting the RADIUS server.
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.


Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/system_authservers.php
Buscar
System / User Manager / Authentication Servers
Users
Groups
Settings
Authentication Servers
Server Name
Type
Host Name
Actions
RadServer
RADIUS
127.0.0.1
Local Database
pfSense
Add
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.
Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg_edit.php?xml=freeradius.xml&id=0
Buscar
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / FreeRADIUS / Edit / Users
Users
MACs
NAS / Clients
Interfaces
Settings
EAP
SQL
LDAP
View Config
XMLRPC Sync
General Configuration
Username
labtelecom
Enter the username. Whitespace is allowed.
Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP.
Password
Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password.
Password Encryption
Cleartext-Password
Select the password encryption for this user. If the (pre-hashed) options are used, the password should already be hashed by the expected hash function. Note that not all authentication protocols are compatible with all types of hashed passwords. Default: Cleartext-Password
One-Time Password Configuration
One-Time Password
Enable One-Time Password (OTP) for this user
This enables the possibility to authenticate with username and one-time-password.
The client used to generate OTP can be installed on various mobile device platforms like Android, iOS and others. (Default: unchecked)
IMPORTANT: For MOTP, mOTP must be enabled at FreeRADIUS > Settings.
The RADIUS NAS / Client must use PAP, otherwise the authenticator script cannot use the authentication data.
OTP Auth Method
mOTP
Select the OTP authentication method for this user. Default: mOTP
Init-Secret
This is the generated init secret you get when you initialize the token for the first time on a client (mobile device).

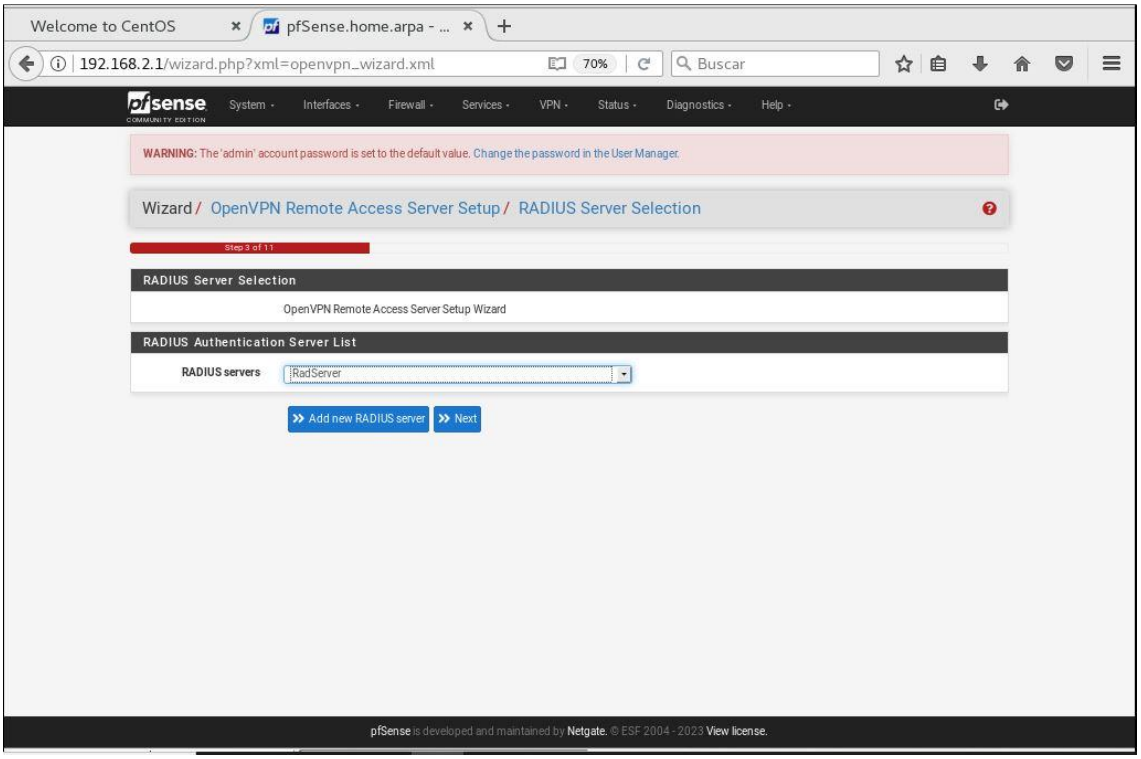

Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/diag_authentication.php
Buscar
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
ARP Table
Authentication
Backup & Restore
Command Prompt
DNS Lookup
Edit File
Factory Defaults
Halt System
Limiter Info
NDP Table
Packet Capture
pfInfo
pfTop
Ping
Reboot
Routes
S.M.A.R.T. Status
Sockets
States
States Summary
System Activity
Tables
Test Port
Traceroute
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Diagnostics / Authentication
Authentication Test
Authentication Server
Local Database
Select the authentication server to test against.
Username
Password
Debug
Set debug flag
Test
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.
Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/diag_authentication.php
Buscar
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Diagnostics / Authentication
User labtelecom authenticated successfully. This user is a member of groups:
Authentication Test
Authentication Server
RadServer
Select the authentication server to test against.
Username
labtelecom
Password
Debug
Set debug flag
Sets the debug flag when performing authentication, which may trigger additional diagnostic entries in the system log (e.g. for LDAP).
Test
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

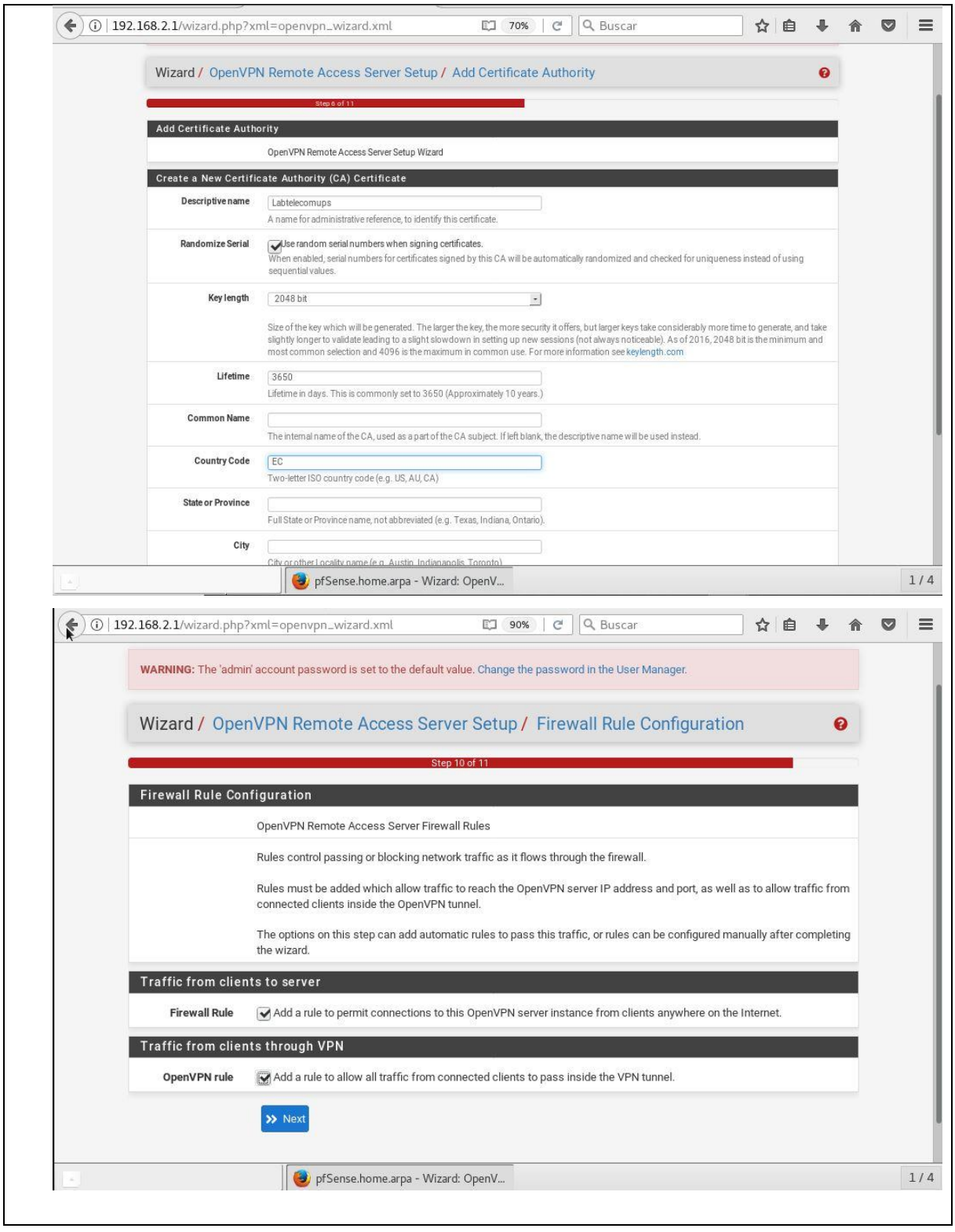

Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg_mgr_install.php
70%
Buscar
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
System / Package Manager / Package Installer
Please wait while the installation of pfSense-pkg-openvpn-client-export completes.
This may take several minutes. Do not leave or refresh the page!
Installed Packages
Available Packages
Package Installer
Package Installation
pfSense repository is up to date.
All repositories are up to date.
The following 5 package(s) will be affected (of 0 checked):
New packages to be INSTALLED:
7-zip: 22.01 [pfSense]
libsysinfo: 0.0.3_2 [pfSense]
openvpn-client-export: 2.6.5 [pfSense]
pfSense-pkg-openvpn-client-export: 1.9_1 [pfSense]
zip: 3.0_1 [pfSense]
Number of packages to be installed: 5
The process will require 31 MiB more space.
23 MiB to be downloaded.
[1/5] Fetching openvpn-client-export-2.6.5.pkg: ..
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.


Welcome to CentOS
pfSense.home.arpa - ...
192.168.2.1/pkg_mgr_install.php
70%
Buscar
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
IPsec
L2TP
OpenVPN
WARNING: The 'admin' account password is set to the default value. Change th
anager.
System / Package Manager / Package Installer
pfSense-pkg-openvpn-client-export installation successfully completed.
Installed Packages
Available Packages
Package Installer
Package Installation
[3/5] Extracting zip-3.0_1: .... done
[4/5] Installing 7-zip-22.01...
[4/5] Extracting 7-zip-22.01: .... done
[5/5] Installing pfSense-pkg-openvpn-client-export-1.9_1...
[5/5] Extracting pfSense-pkg-openvpn-client-export-1.9_1: .... done
Saving updated package information...
done.
Loading package configuration... done.
Configuring package components...
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Writing configuration... done.
>>> Cleaning up cache... done.
Success
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.

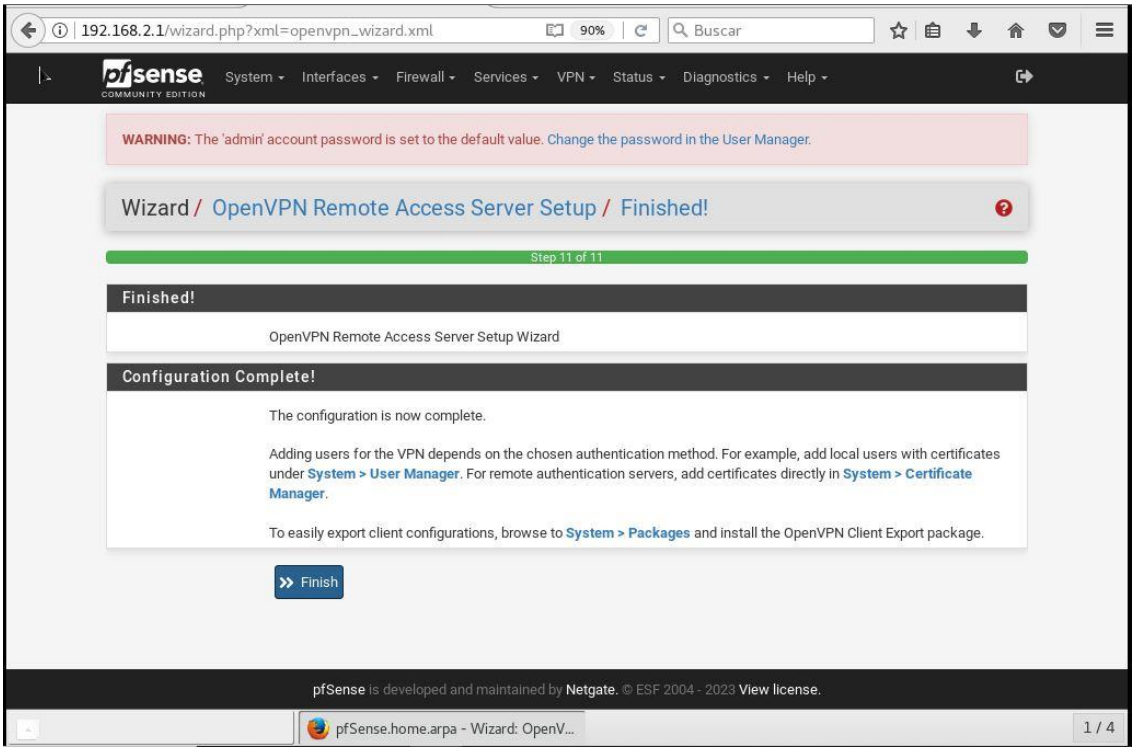


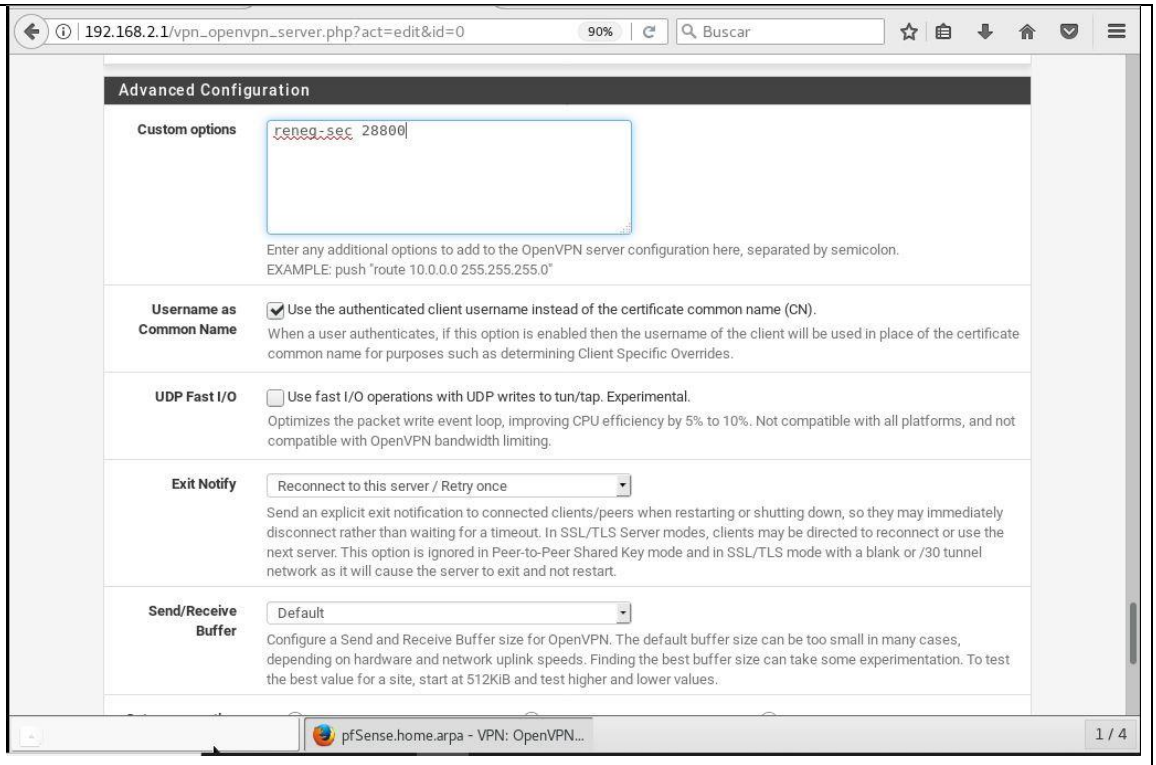
Instalación de OpenVPN y configuración.

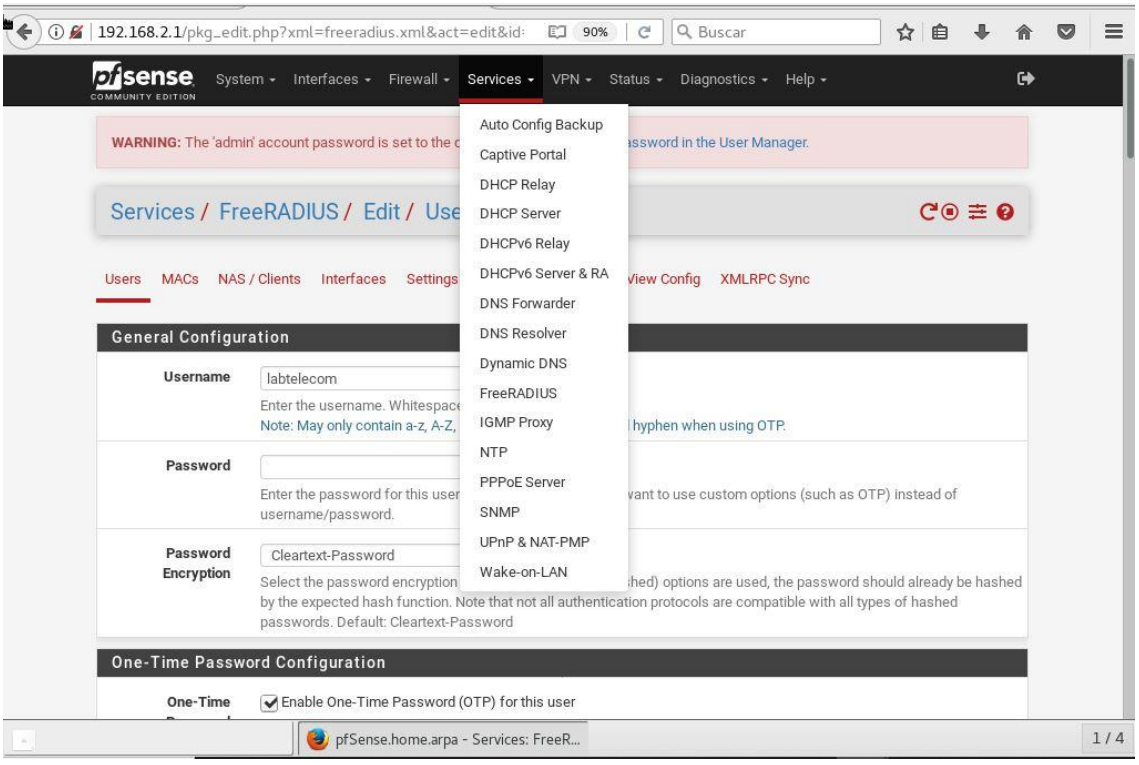



192.168.2.1/wizard.php?xml=openvpn_wizard.xml
70%
Buscar
Wizard / OpenVPN Remote Access Server Setup / Add Certificate Authority
Step 6 of 11
Add Certificate Authority
OpenVPN Remote Access Server Setup Wizard
Create a New Certificate Authority (CA) Certificate
Descriptive name
Labtelecomups
A name for administrative reference, to identify this certificate.
Randomize Serial
Use random serial numbers when signing certificates.
When enabled, serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using sequential values.
Key length
2048 bit
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Lifetime
3650
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Common Name
The internal name of the CA, used as a part of the CA subject. If left blank, the descriptive name will be used instead.
Country Code
EC
Two-letter ISO country code (e.g. US, AU, CA)
State or Province
Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).
City
City or other Locality name (e.g. Austin, Indianapolis, Toronto)
pfSense.home.arpa - Wizard: OpenV...
1 / 4
192.168.2.1/wizard.php?xml=openvpn_wizard.xml
90%
Buscar
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration
Step 10 of 11
Firewall Rule Configuration
OpenVPN Remote Access Server Firewall Rules
Rules control passing or blocking network traffic as it flows through the firewall.
Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.
The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.
Traffic from clients to server
Firewall Rule
Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.
Traffic from clients through VPN
OpenVPN rule
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.
Next
pfSense.home.arpa - Wizard: OpenV...
1 / 4

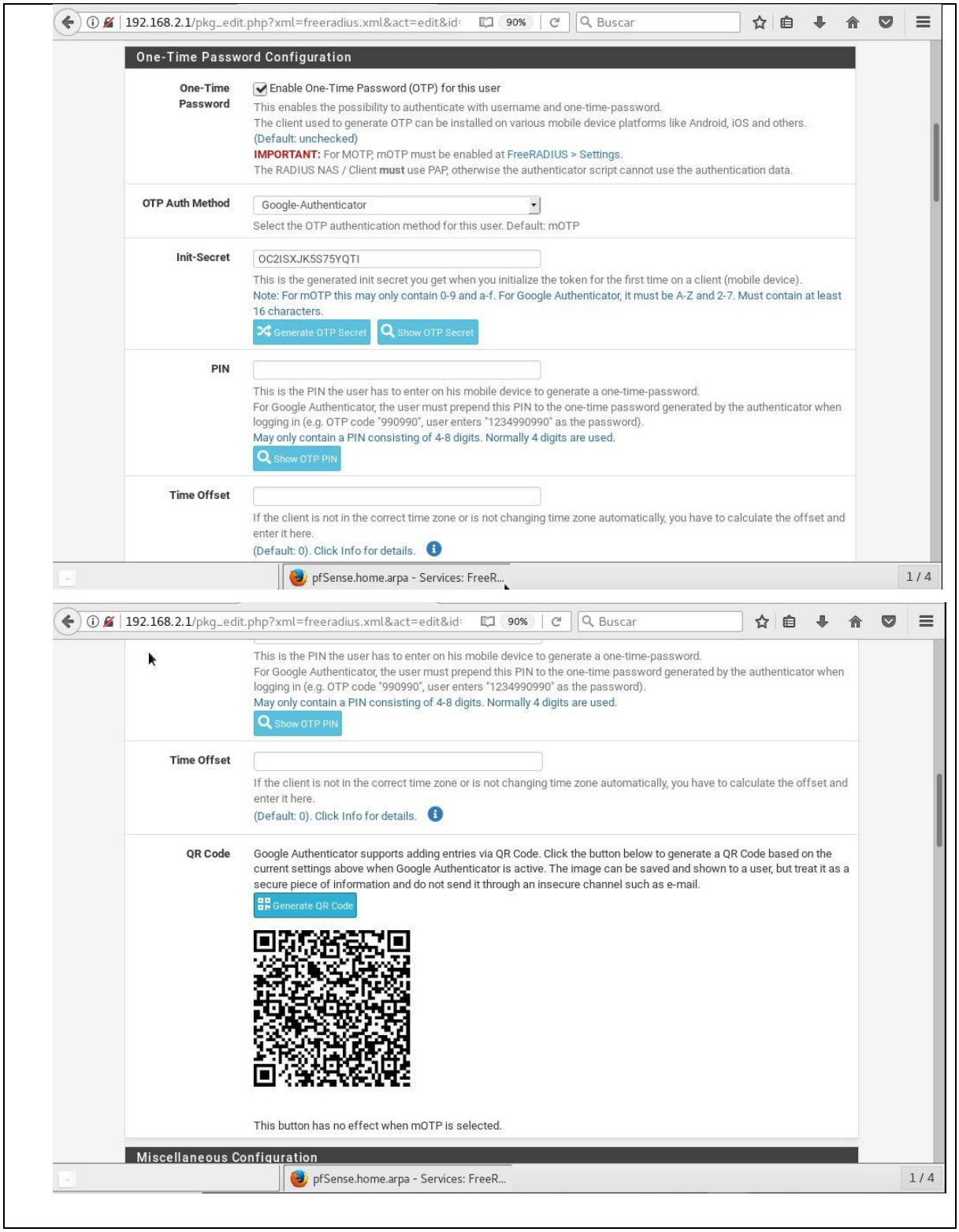
Configuracion de las relgas de firewall para OpenVPN.



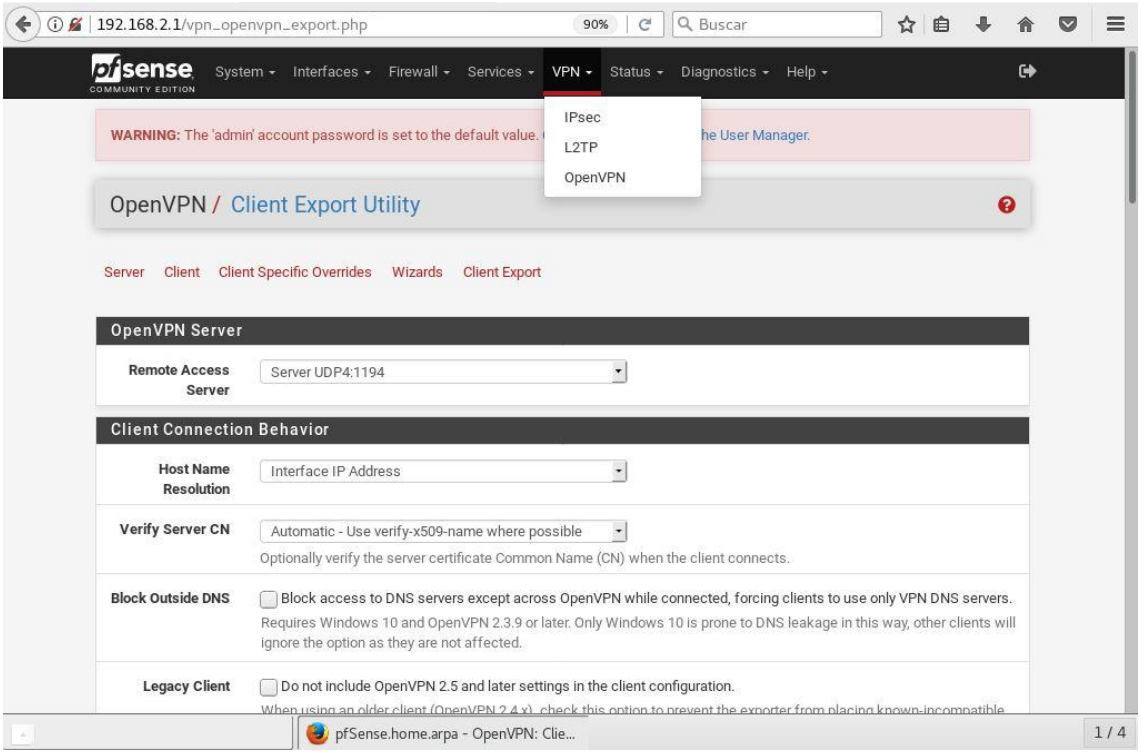




Configuración de pfSense con Google-Authenticator para el proceso de doble autenticación.


192.168.2.1/pkg_edit.php?xml=freeradius.xml&act=edit&id=
90%
Buscar
One-Time Password Configuration
One-Time Password
Enable One-Time Password (OTP) for this user
This enables the possibility to authenticate with username and one-time-password.
The client used to generate OTP can be installed on various mobile device platforms like Android, iOS and others.
(Default: unchecked)
IMPORTANT: For MOTP, mOTP must be enabled at FreeRADIUS > Settings.
The RADIUS NAS / Client must use PAP, otherwise the authenticator script cannot use the authentication data.
OTP Auth Method
Google-Authenticator
Select the OTP authentication method for this user. Default: mOTP
Init-Secret
OC2ISXJK5S75YQTI
This is the generated init secret you get when you initialize the token for the first time on a client (mobile device).
Note: For mOTP this may only contain 0-9 and a-f. For Google Authenticator, it must be A-Z and 2-7. Must contain at least 16 characters.
Generate OTP Secret
Show OTP Secret
PIN
This is the PIN the user has to enter on his mobile device to generate a one-time-password.
For Google Authenticator, the user must prepend this PIN to the one-time password generated by the authenticator when logging in (e.g. OTP code "990990", user enters "1234990990" as the password).
May only contain a PIN consisting of 4-8 digits. Normally 4 digits are used.
Show OTP PIN
Time Offset
If the client is not in the correct time zone or is not changing time zone automatically, you have to calculate the offset and enter it here.
(Default: 0). Click Info for details.
pfSense.home.arpa - Services: FreeR...
1 / 4
192.168.2.1/pkg_edit.php?xml=freeradius.xml&act=edit&id=
90%
Buscar
This is the PIN the user has to enter on his mobile device to generate a one-time-password.
For Google Authenticator, the user must prepend this PIN to the one-time password generated by the authenticator when logging in (e.g. OTP code "990990", user enters "1234990990" as the password).
May only contain a PIN consisting of 4-8 digits. Normally 4 digits are used.
Show OTP PIN
Time Offset
If the client is not in the correct time zone or is not changing time zone automatically, you have to calculate the offset and enter it here.
(Default: 0). Click Info for details.
QR Code
Google Authenticator supports adding entries via QR Code. Click the button below to generate a QR Code based on the current settings above when Google Authenticator is active. The image can be saved and shown to a user, but treat it as a secure piece of information and do not send it through an insecure channel such as e-mail.
Generate QR Code
This button has no effect when mOTP is selected.
Miscellaneous Configuration
pfSense.home.arpa - Services: FreeR...
1 / 4

Codigo QR para ser escaneado por la aplicación de Google Authenticator y gestionar la doble autenticacion mediante el celular del usuario.



RESULTADO(S) OBTENIDO(S):

El estudiante se familiariza con el uso de doble autenticación mediante FreeRadius

CONCLUSIONES:

El estudiante configura pfSense para el uso de doble autenticación con el uso de aplicaciones libres.

RECOMENDACIONES:

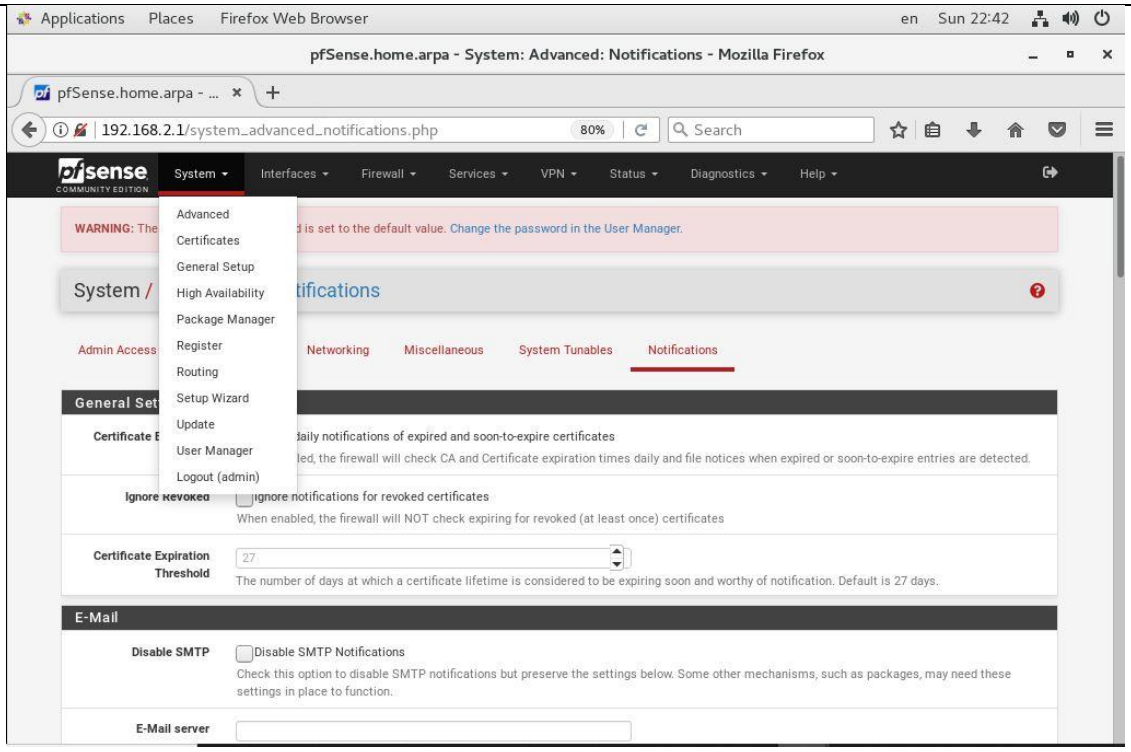
Realizar varias practicas con el uso de la aplicación.

Docente: _____

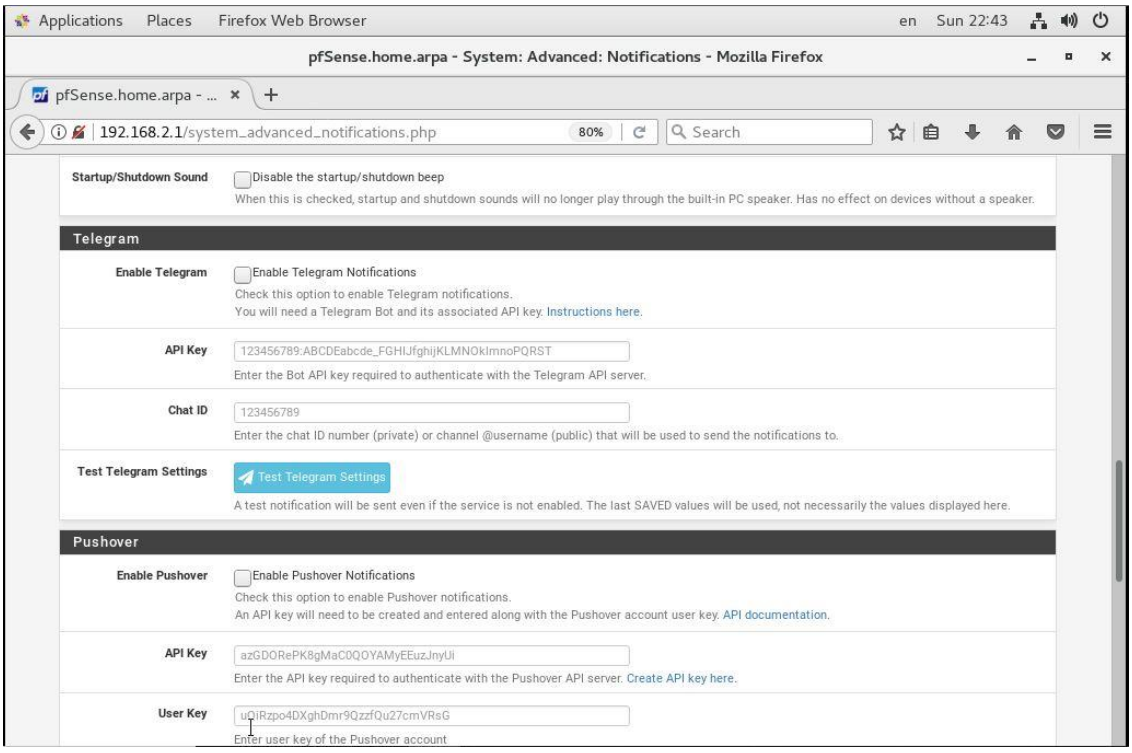
Firma: _____

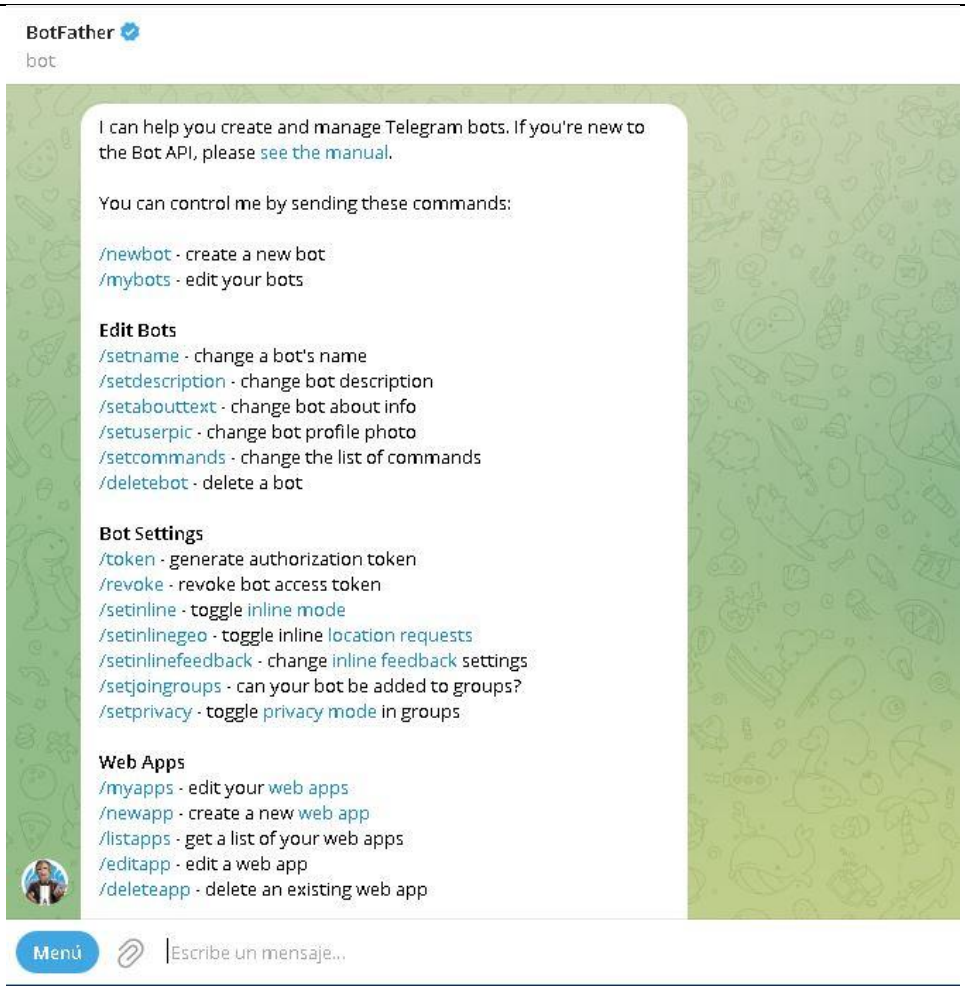
4.9. PRÁCTICA # 9

<table>
<tr><td colspan="2"> 
FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>Carrera: Ingeniería Electrónica</td><td>Asignatura: Redes de Computadoras</td></tr>
<tr><td>NRO. Práctica: 9</td><td>Título Práctica:
Habilitación de acceso a Telegram para la administración y notificación de eventos en pfSense</td></tr>
<tr><td colspan="2">OBJETIVO:
• Objetivo General
Configurar pfSense para que a través de Telegram pueda recibir notificaciones de los servicios que se monitoreen</td></tr>
<tr><td>INSTRUCCIONES:</td><td>1. Cree una nueva regla de firewall que permita el tráfico hacia los servidores de Telegram.
2. Configurar los servicios dentro de pfSense para notificar el monitoreo de procesos.
3. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.</td></tr>
<tr><td colspan="2">ACTIVIDADES POR DESARROLLAR</td></tr>
<tr><td colspan="2">1. Dirigirse a System – Advanced – Notification</td></tr>
</table>

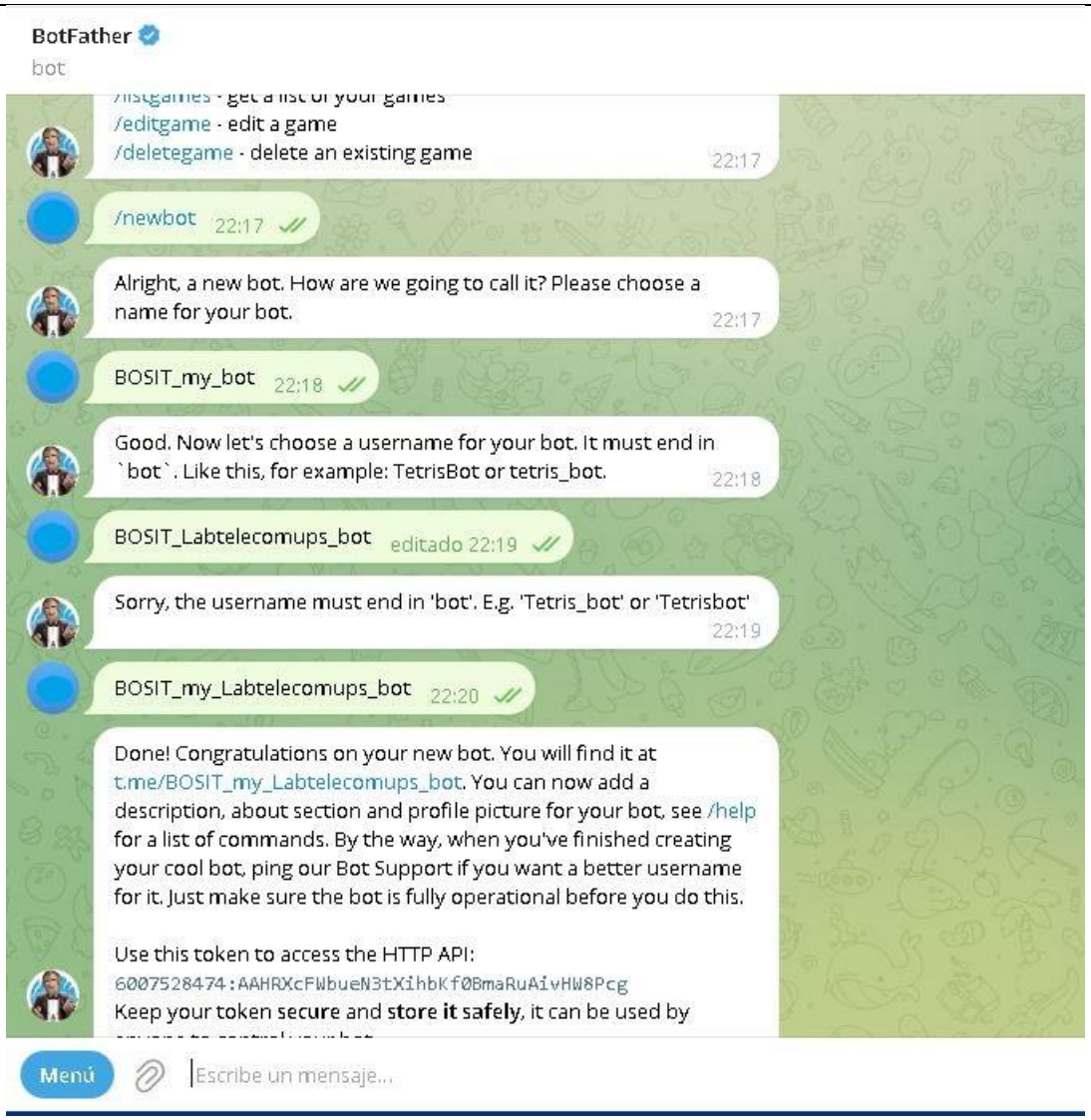


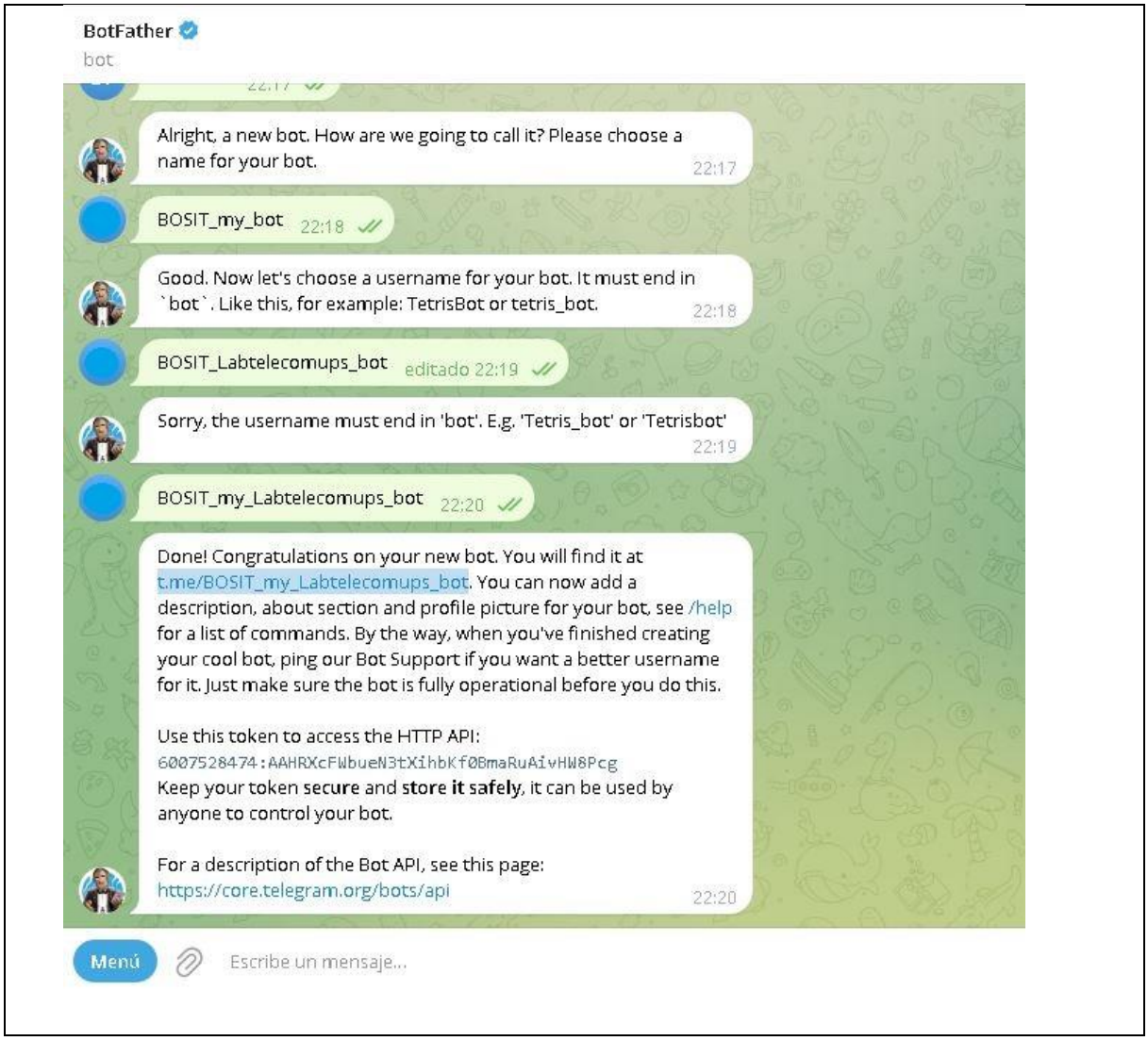
Dirigirse la seccion de Telegram, dar Check en la opcion de Enable Telegram notifications.

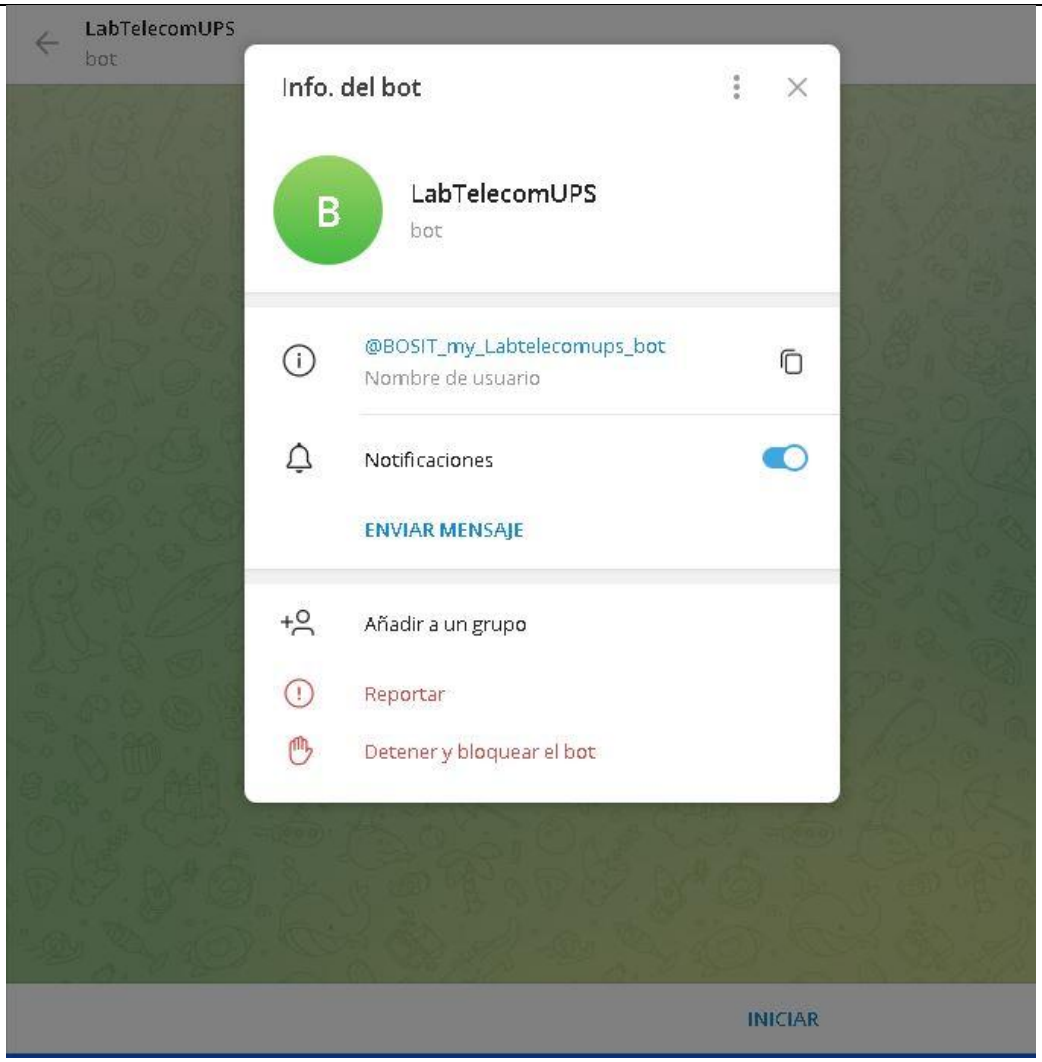




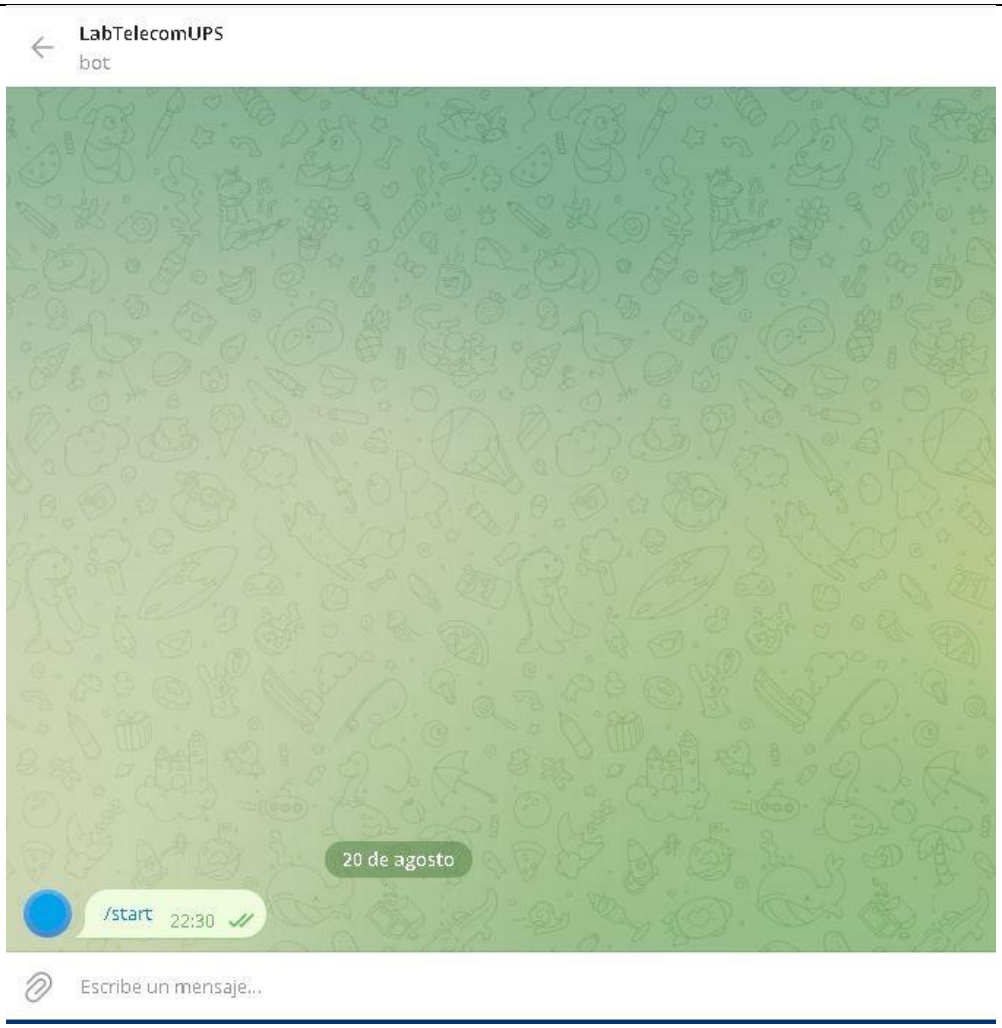
Desde Telegram dirigirse a @BotFather y configurar el sistema para las notificaciones de pfsense, de acuerdo a las opciones detalladas en las imagenes


BotFather
bot
/editgame - edit a game
/deletegame - delete an existing game
22:17
/newbot 22:17
Alright, a new bot. How are we going to call it? Please choose a name for your bot.
22:17
BOSIT_my_bot 22:18
Good. Now let's choose a username for your bot. It must end in `bot`. Like this, for example: TetrisBot or tetris_bot.
22:18
BOSIT_Labtelecomups_bot editado 22:19
Sorry, the username must end in 'bot'. E.g. 'Tetris_bot' or 'Tetrisbot'
22:19
BOSIT_my_Labtelecomups_bot 22:20
Done! Congratulations on your new bot. You will find it at t.me/BOSIT_my_Labtelecomups_bot. You can now add a description, about section and profile picture for your bot, see /help for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.
Use this token to access the HTTP API:
6007528474:AAHRXcFWbueN3tXihbKf0BmaRuAivHW8Pcg
Keep your token secure and store it safely, it can be used by
Menú
Escribe un mensaje...

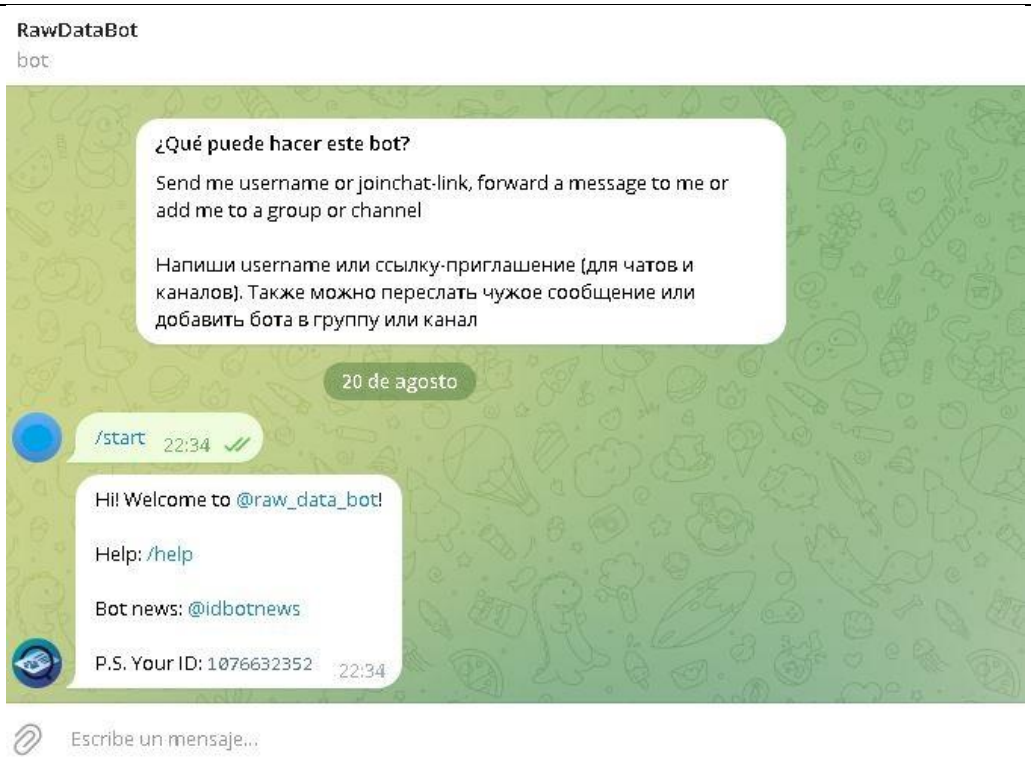

BotFather
bot
Alright, a new bot. How are we going to call it? Please choose a name for your bot.
22:17
BOSIT_my_bot
22:18
Good. Now let's choose a username for your bot. It must end in `bot`. Like this, for example: TetrisBot or tetris_bot.
22:18
BOSIT_Labtelecomups_bot
editado 22:19
Sorry, the username must end in 'bot'. E.g. 'Tetris_bot' or 'Tetrisbot'
22:19
BOSIT_my_Labtelecomups_bot
22:20
Done! Congratulations on your new bot. You will find it at t.me/BOSIT_my_Labtelecomups_bot. You can now add a description, about section and profile picture for your bot, see /help for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.
Use this token to access the HTTP API:
6007528474:AAHRXcFWbueN3tXihbKf0BmaRuAivHW8Pcg
Keep your token secure and store it safely, it can be used by anyone to control your bot.
For a description of the Bot API, see this page:
https://core.telegram.org/bots/api
22:20
Menú
Escribe un mensaje...



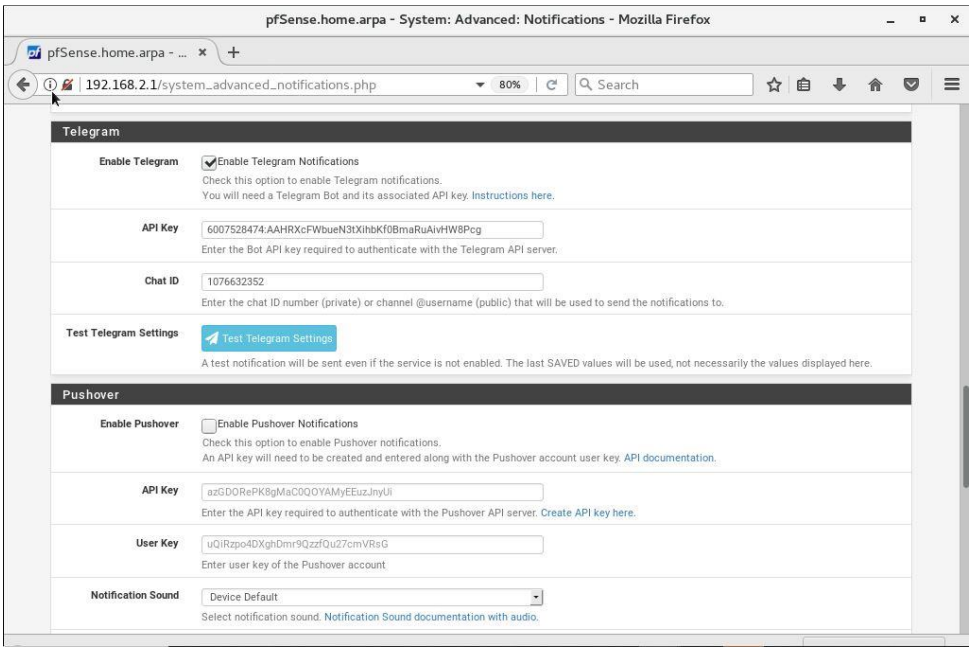
Creación de una comunidad llamada LabTelecomUPS para recibir las notificaciones desde pfSense

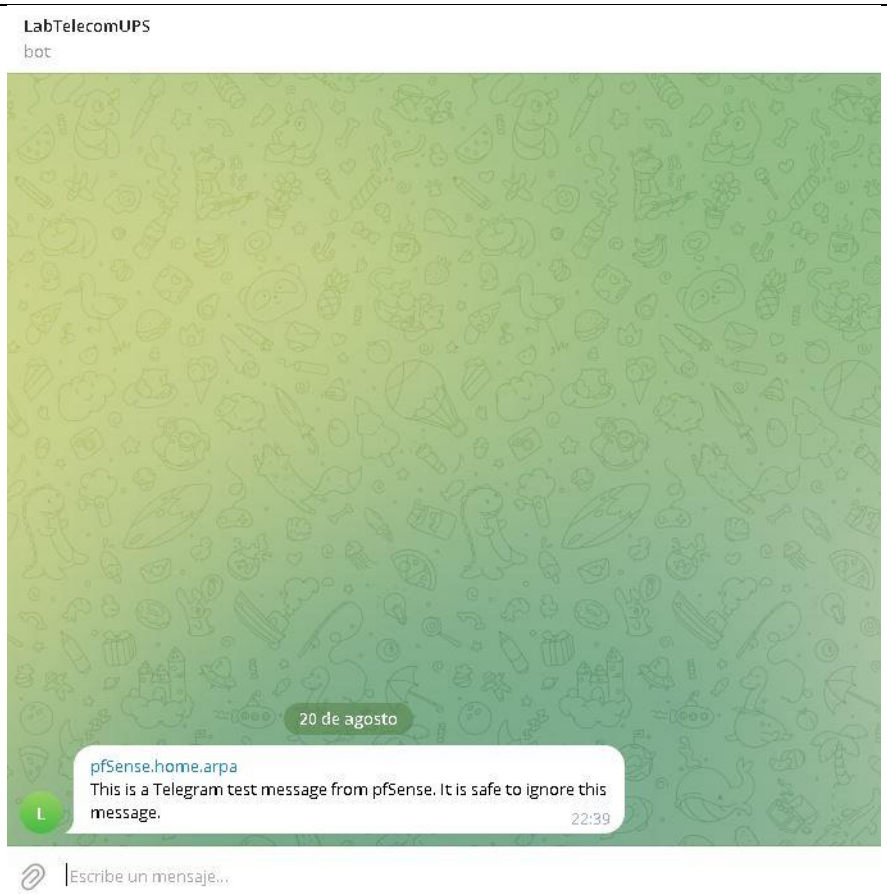


/start es la opcion para el inicio del proceso de recepcion de notificaciones.

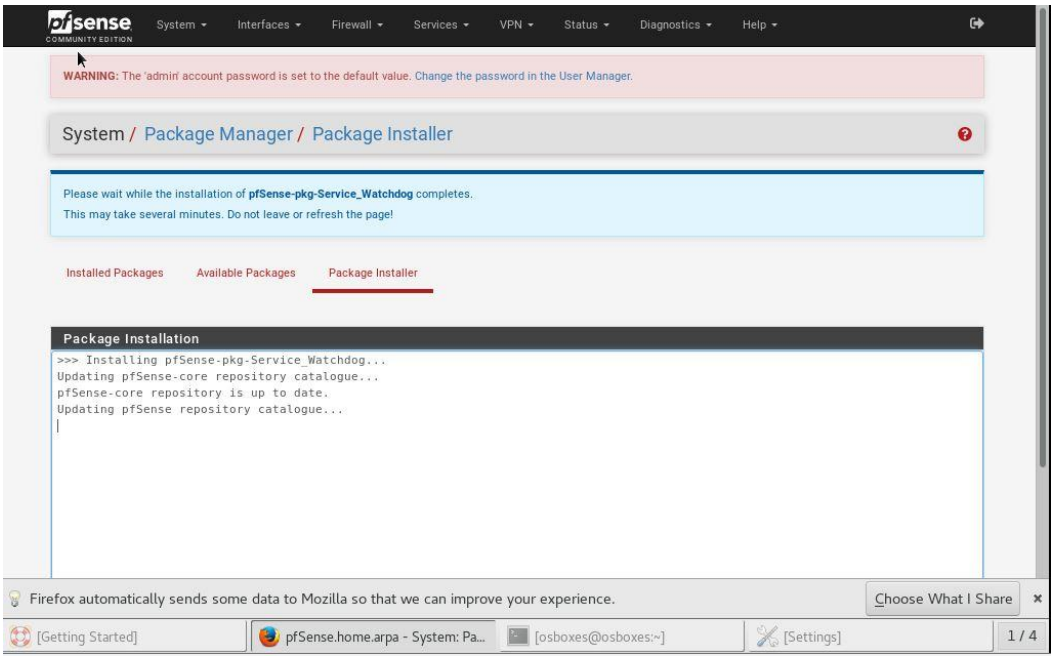


Ingresando a @RawDataBot, se obtiene el ID de la comunidad LabTelecomUPS que se anotará para llevarla a pfSense para su configuración.

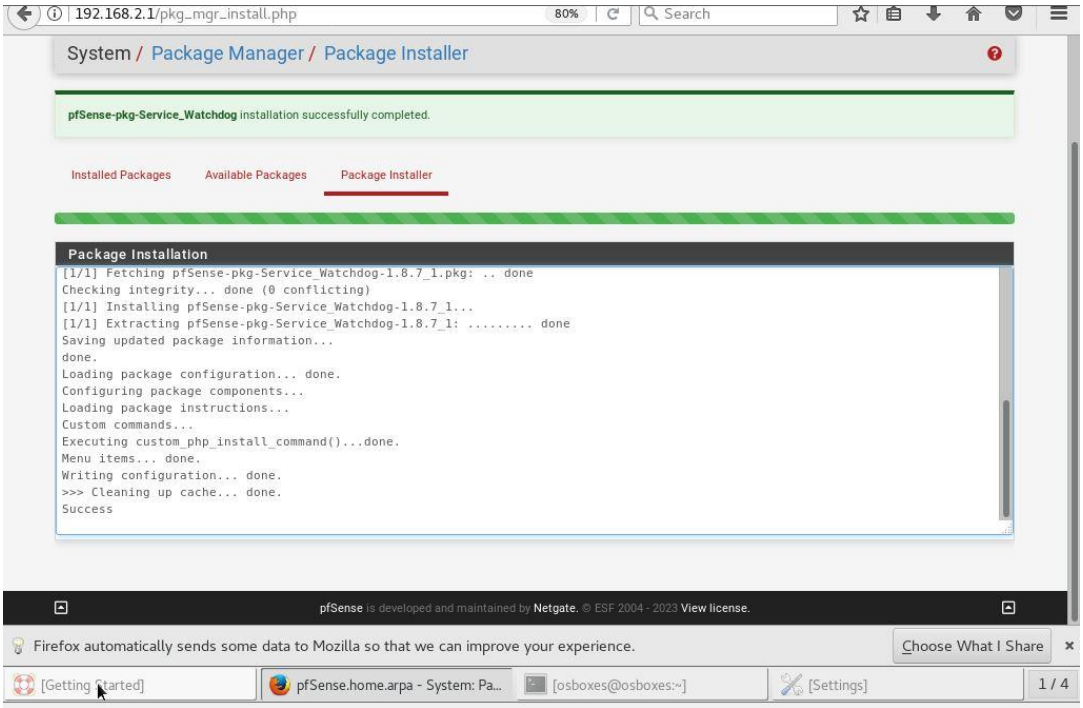


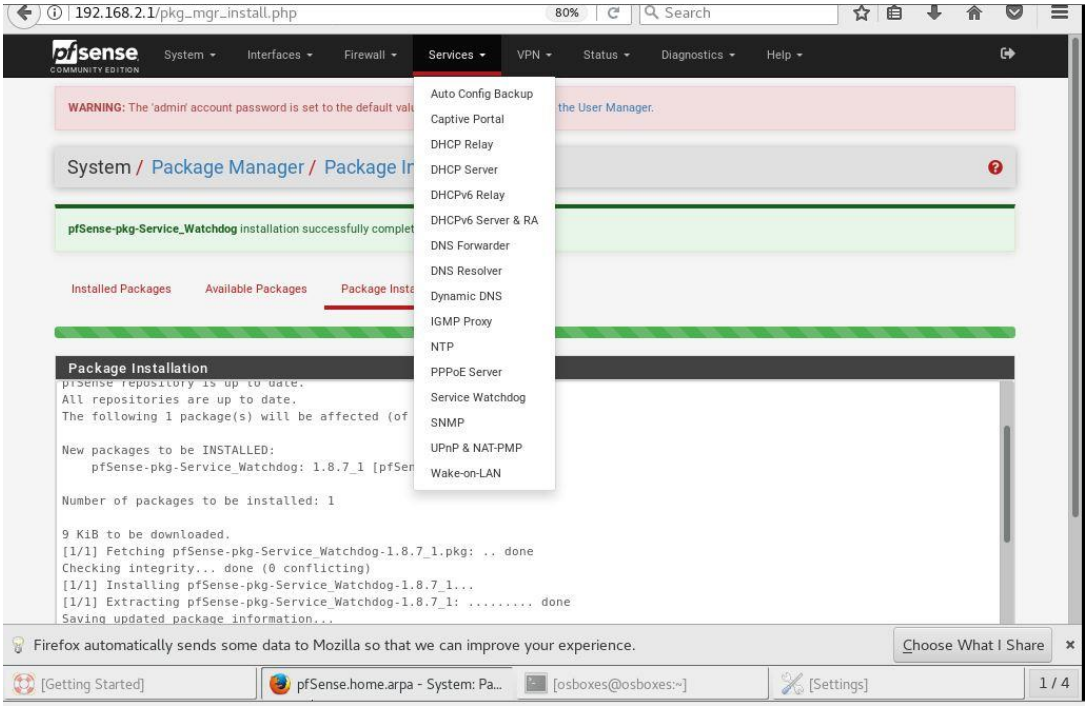


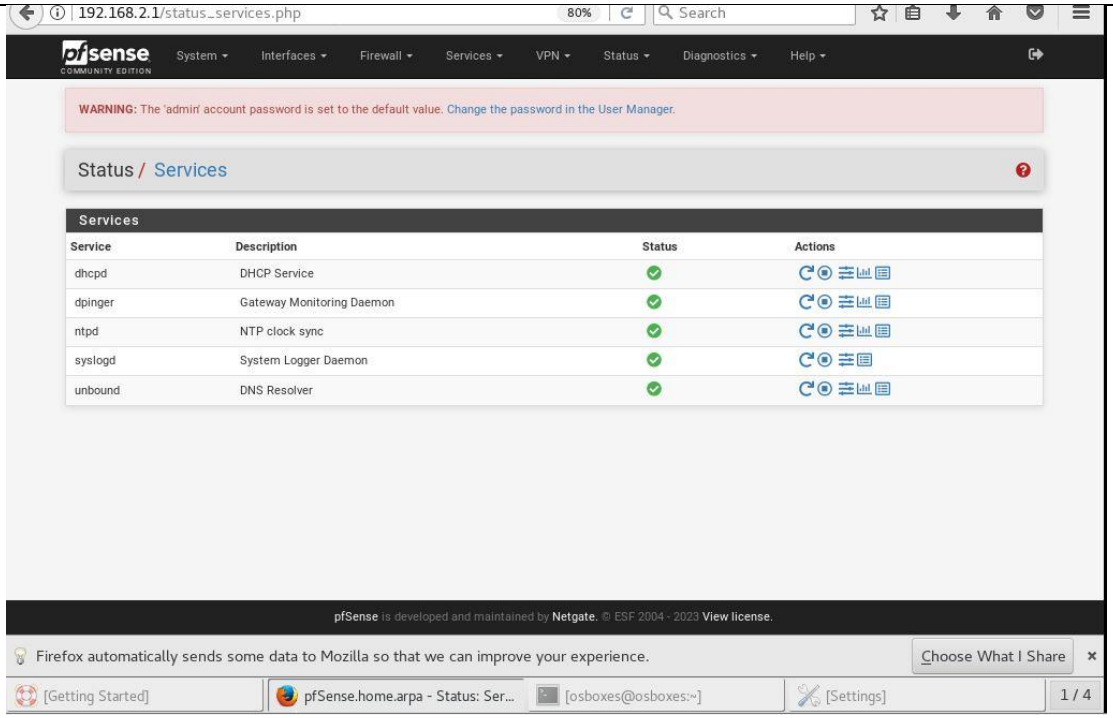
Se envia un mensaje de Prueba para verificar que desde ya esta configurado el envio de notificaciones desde prfSense a Telegram.



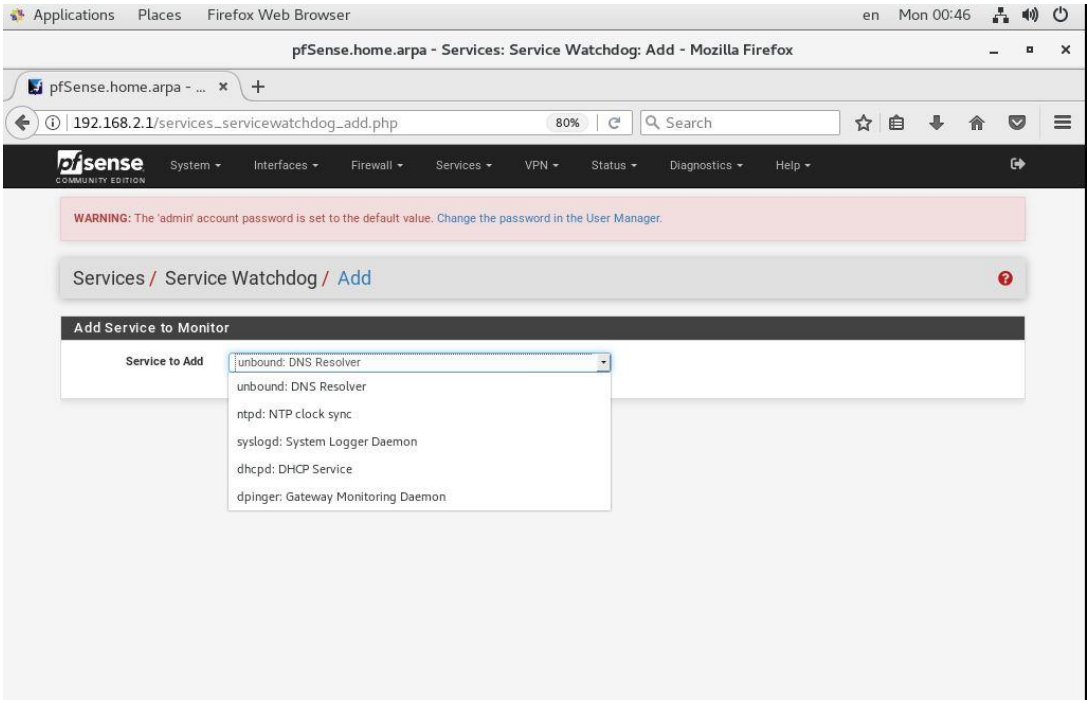
Instalación de Watchdog, un servicio que levantará automaticamente algún proceso que este caido previa configuración.

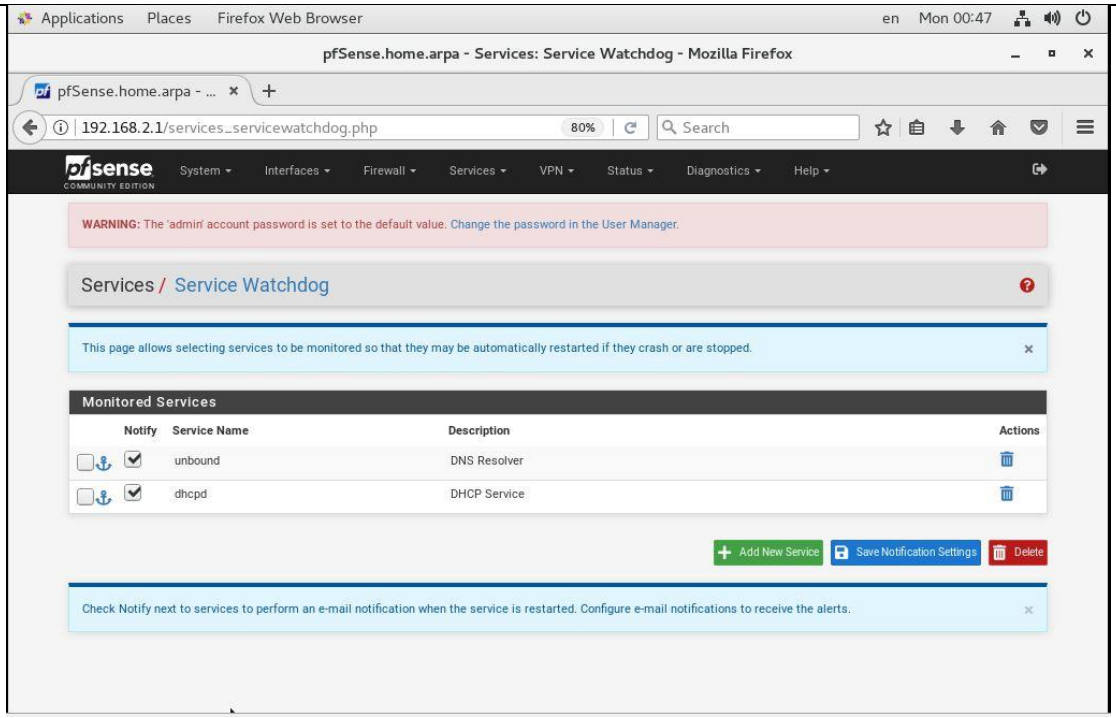


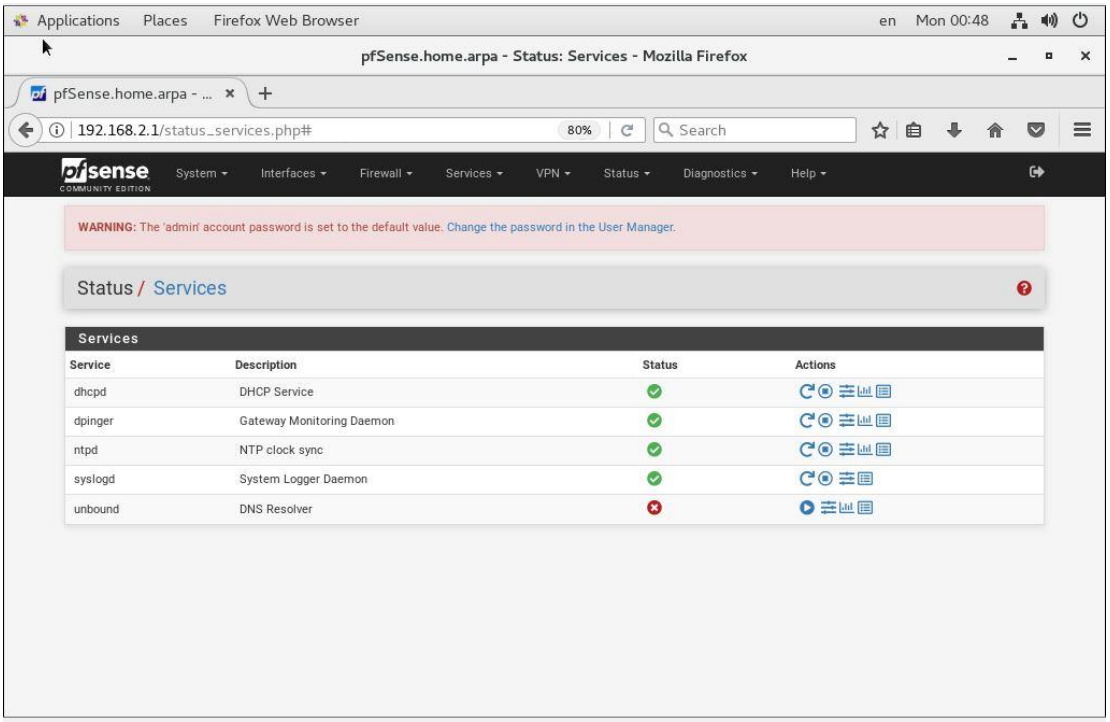


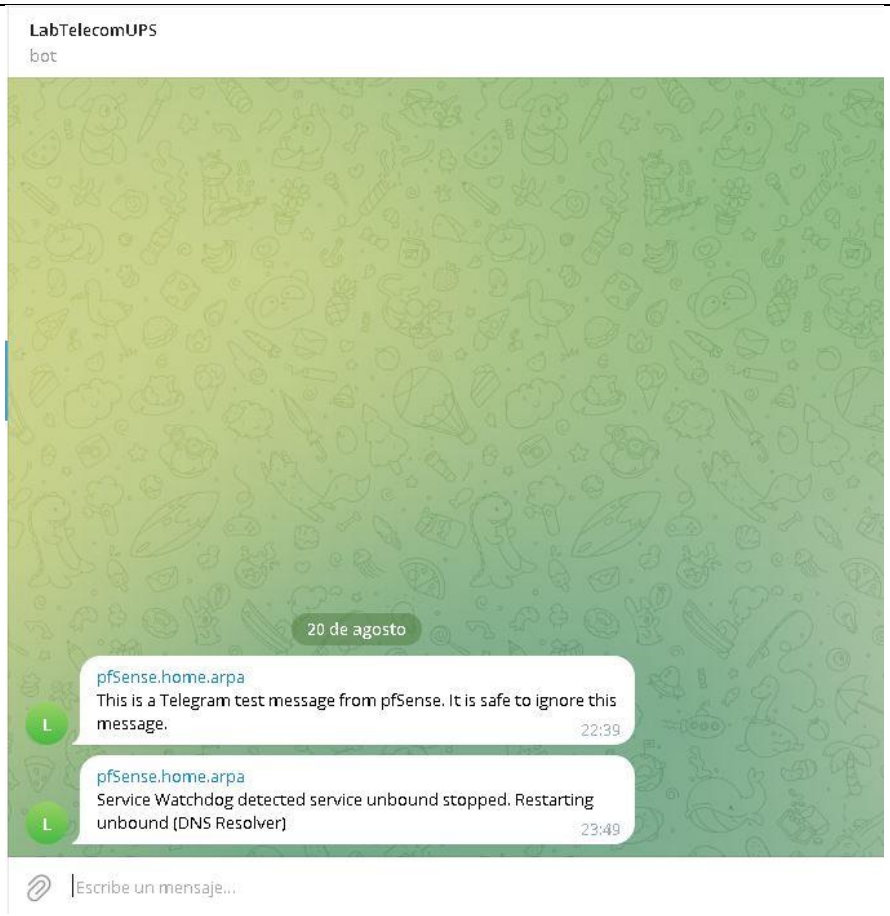


Una vez instalado direccionarse a Service – Service Watchdog – Add y se procede a escoger el servicio que desea monitorear.




Applications Places Firefox Web Browser en Mon 00:47
pfSense.home.arpa - Services: Service Watchdog - Mozilla Firefox
pfSense.home.arpa - ...
192.168.2.1/services_servicewatchdog.php
80%
Search
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / Service Watchdog
This page allows selecting services to be monitored so that they may be automatically restarted if they crash or are stopped.
Monitored Services
Notify
Service Name
Description
Actions
unbound
DNS Resolver
dhcpd
DHCP Service
Add New Service
Save Notification Settings
Delete
Check Notify next to services to perform an e-mail notification when the service is restarted. Configure e-mail notifications to receive the alerts.


Applications Places Firefox Web Browser en Mon 00:48
pfSense.home.arpa - Status: Services - Mozilla Firefox
pfSense.home.arpa - ...
192.168.2.1/status_services.php#
80%
Search
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Status / Services
Services
Service
Description
Status
Actions
dhcpd
DHCP Service
dpinger
Gateway Monitoring Daemon
ntpd
NTP clock sync
syslogd
System Logger Daemon
unbound
DNS Resolver



Realizar la prueba suspendiendo el servicio de DNS Resolver y de estar configurado correctamente llegara la notificacion a Telegram .

RESULTADO(S) OBTENIDO(S):

El estudiante se familiariza con la configuración de pfSense para recibir notificaciones a través de Telegram de los servicios que esta monitoreando.

CONCLUSIONES:

El estudiante conoce como programar el pfSense para la configuración de los servicios.

RECOMENDACIONES:

Configurar mas servicios para practicar esta configuración.

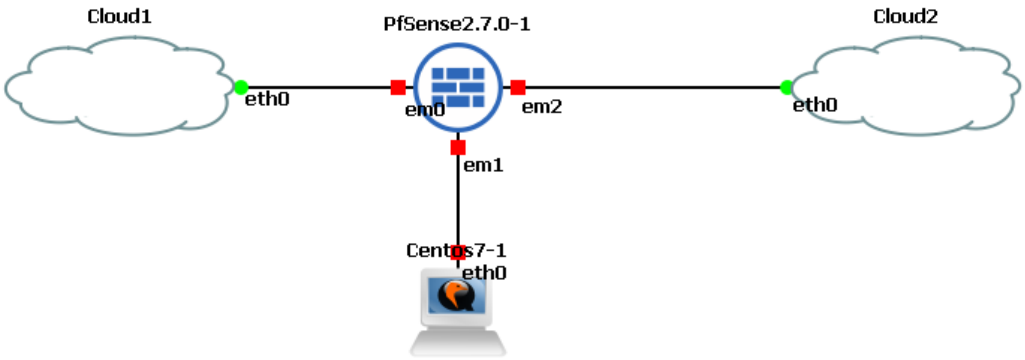
Docente: _____

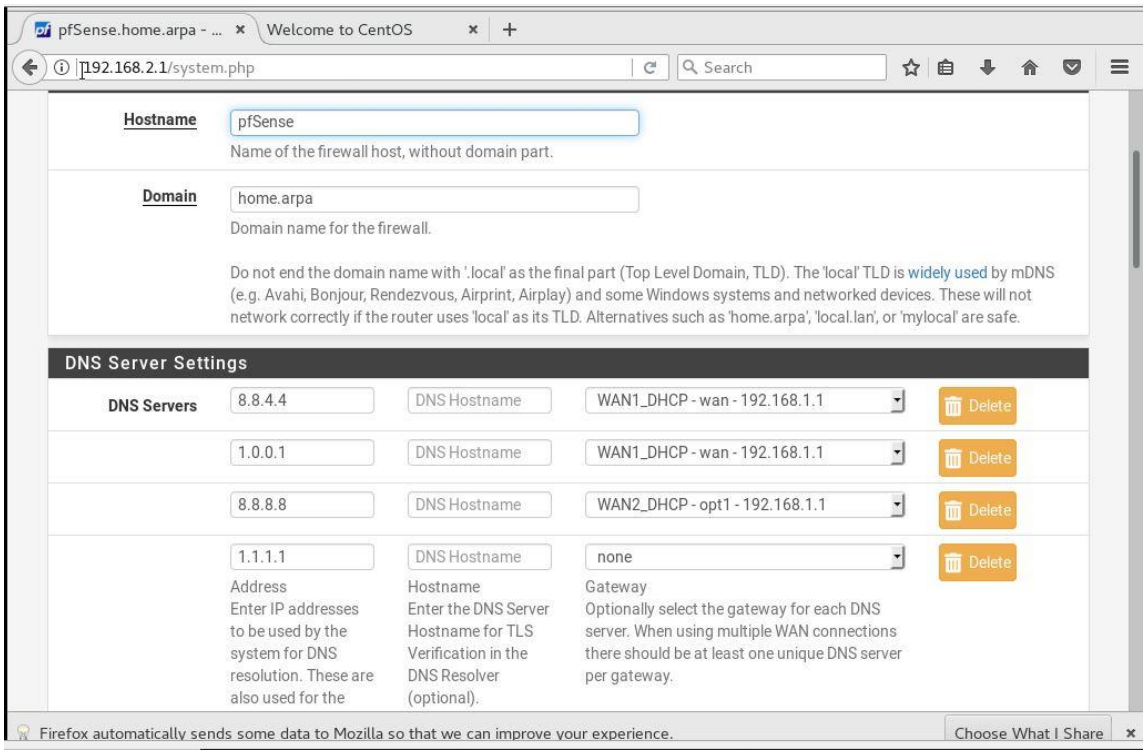
Firma: _____

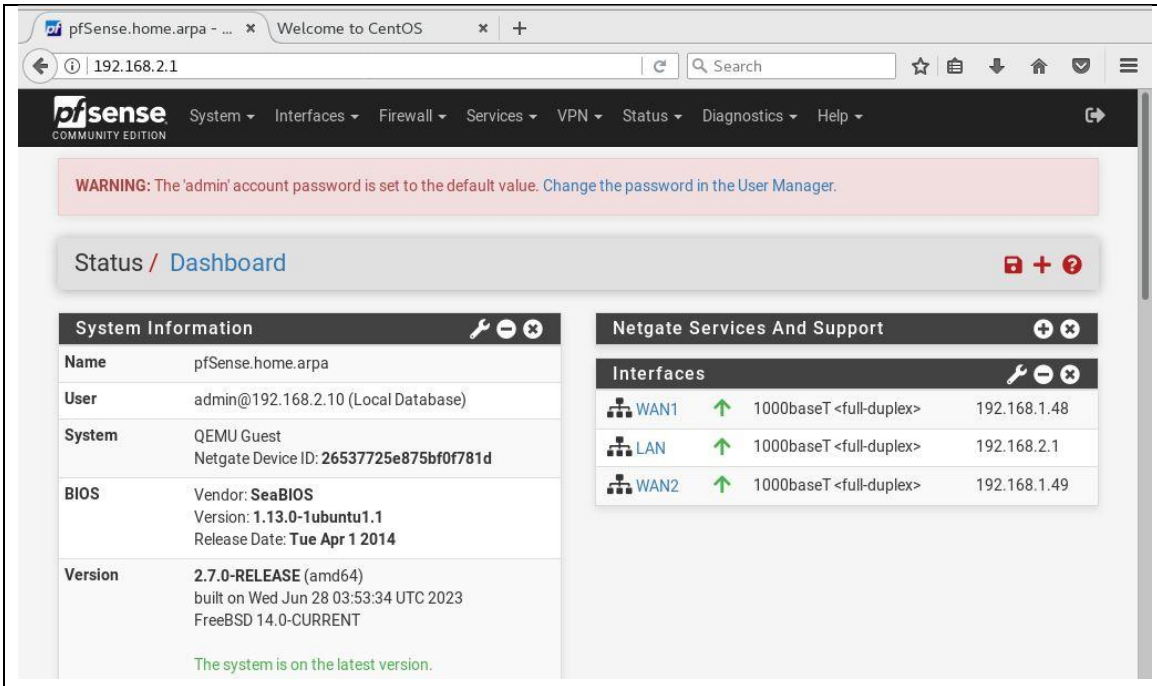
4.10. PRÁCTICA # 10

<table>
<tr><td colspan="2"> 
FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>Carrera: Ingeniería Electrónica</td><td>Asignatura: Redes de Computadoras</td></tr>
<tr><td>NRO. Práctica: 10</td><td>Título Práctica:
Configuración de Balanceo de carga y Failover con pfSense.</td></tr>
<tr><td colspan="2">OBJETIVO:
• Objetivo General
Configurar pfSense para implementar balanceo de carga y failover en una red para mejorar la disponibilidad y la velocidad de la red al distribuir el tráfico entre múltiples conexiones a Internet y proporcionar un mecanismo de respaldo en caso de que una conexión falle.</td></tr>
<tr><td>INSTRUCCIONES:</td><td>1. Configure el monitoreo de las conexiones WAN para detectar fallos automáticamente
2. Configure las reglas de failover para redirigir automáticamente el tráfico a través de una conexión funcional en caso de que una conexión falle.
3. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.</td></tr>
<tr><td colspan="2">ACTIVIDADES POR DESARROLLAR</td></tr>
</table>

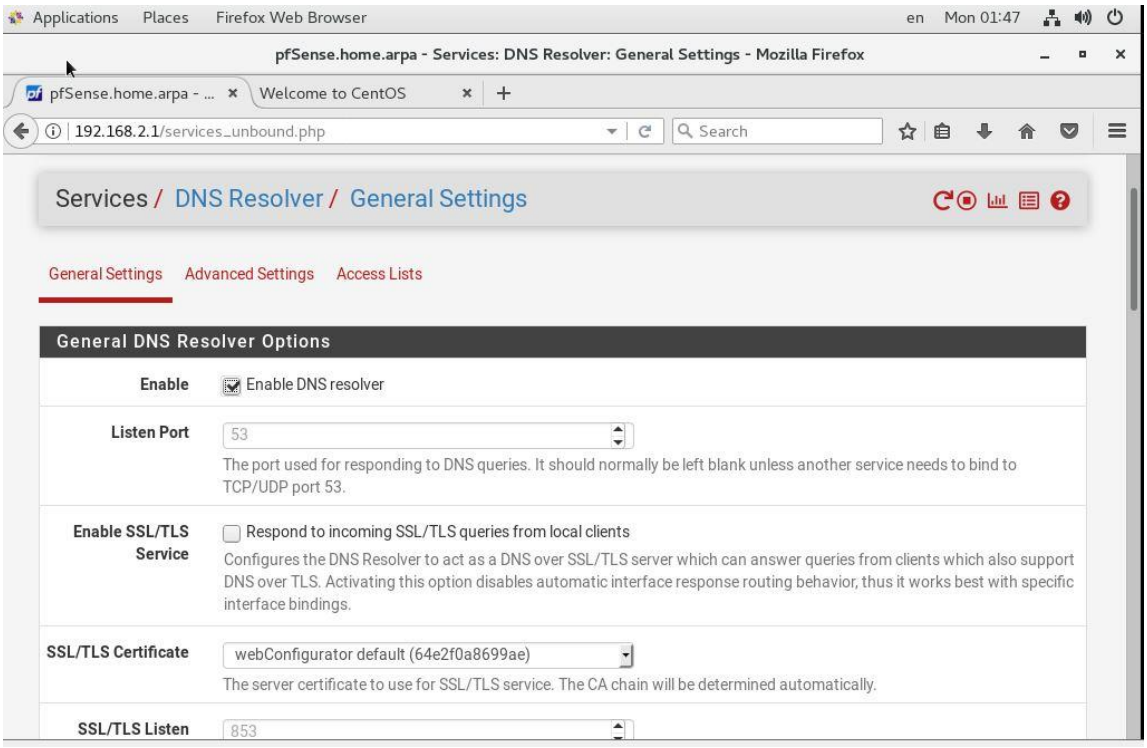
Configurar los DNS en pfSense de cada provedor de Internetasignandole a la interfaz correspondiente

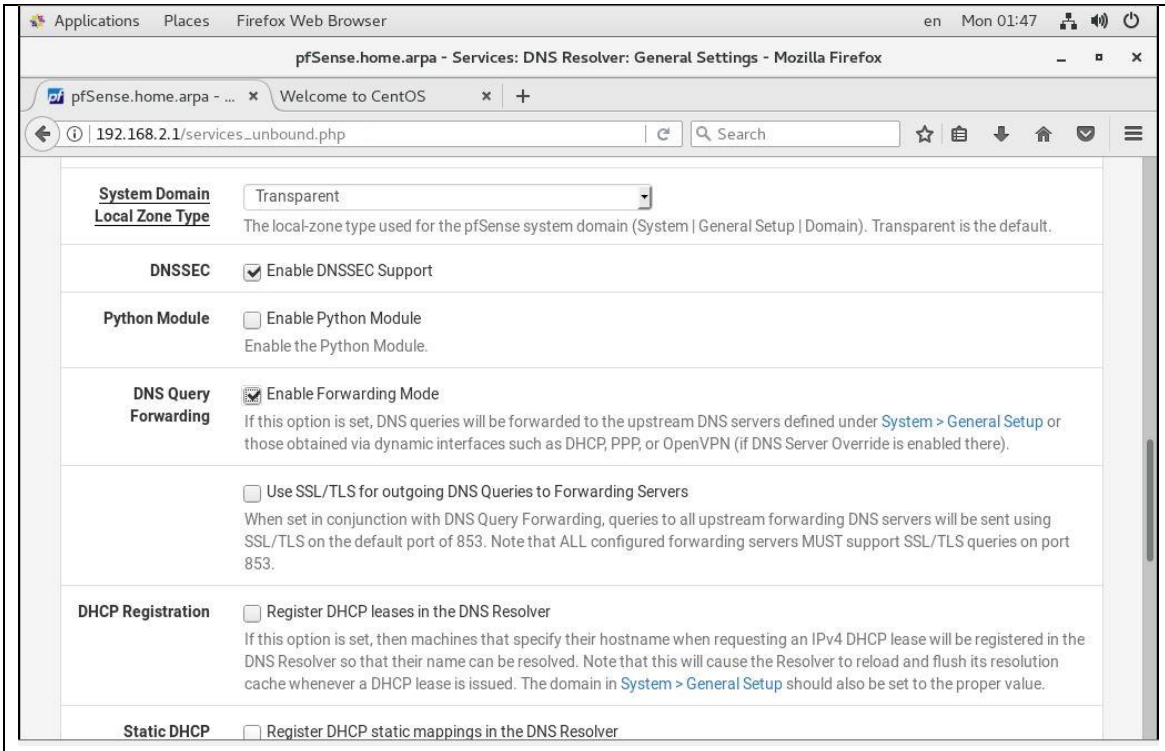


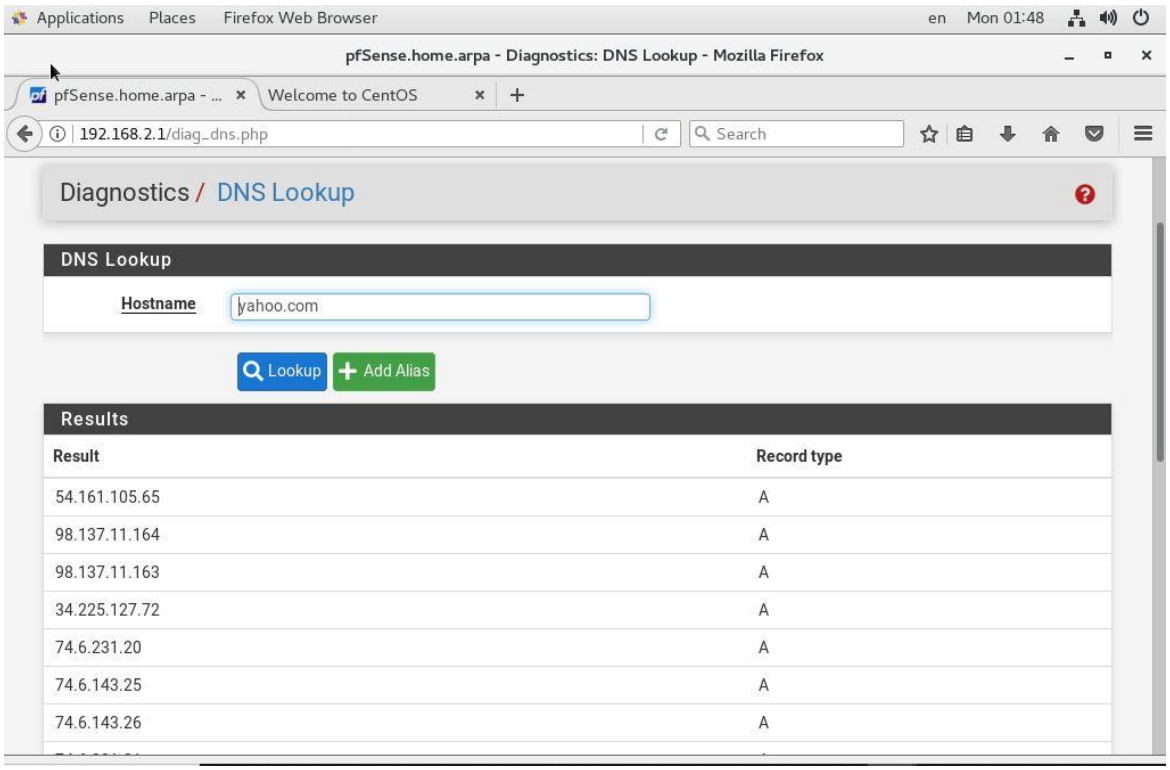




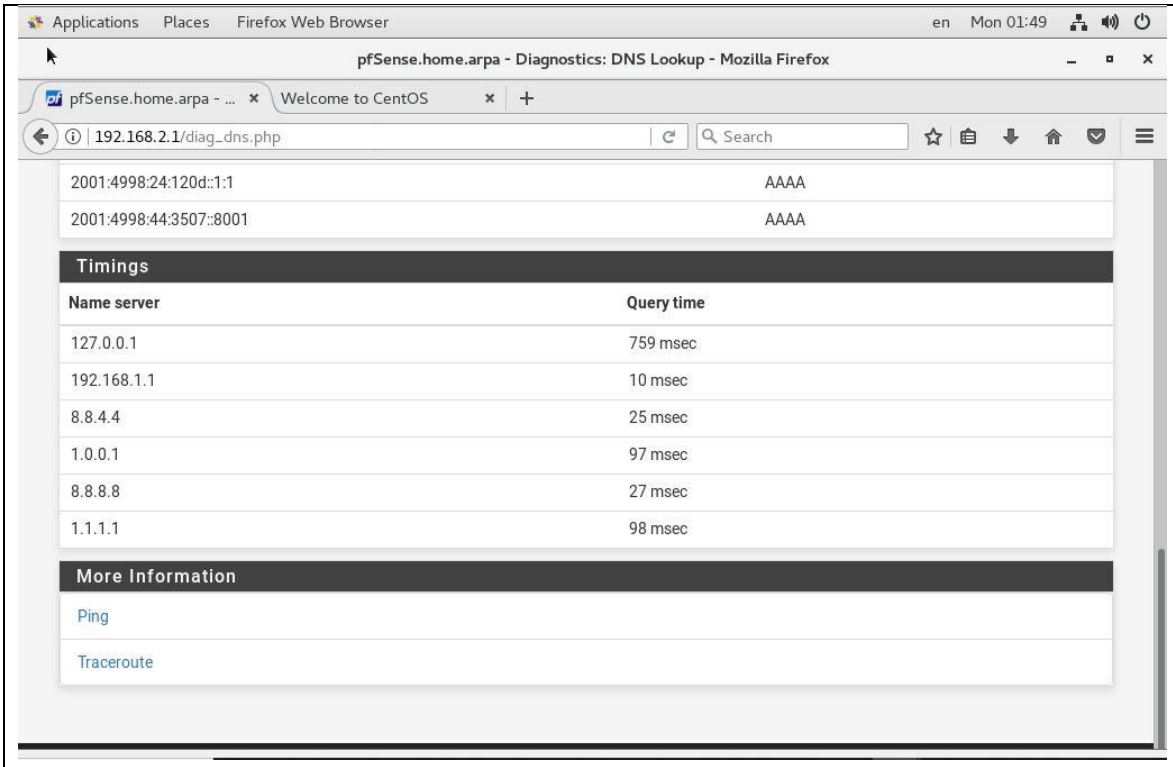
Dirigirse a Service - DNS Resolver – General Setting y habilitar el servicio.

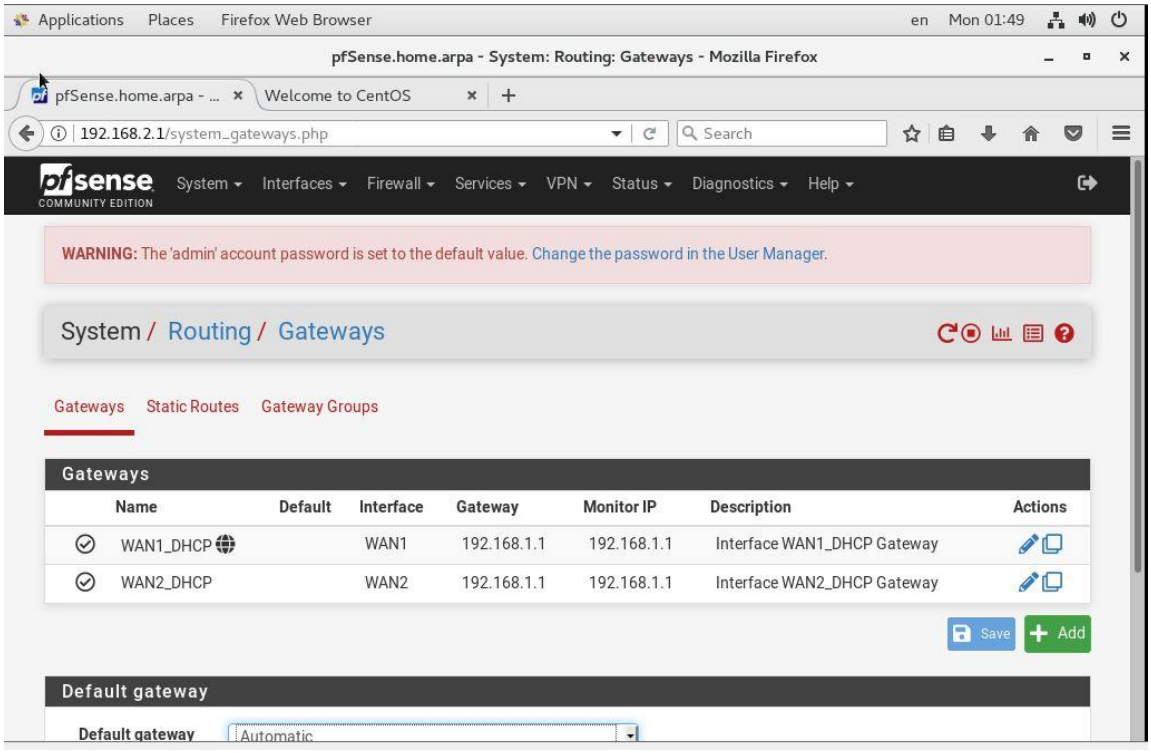


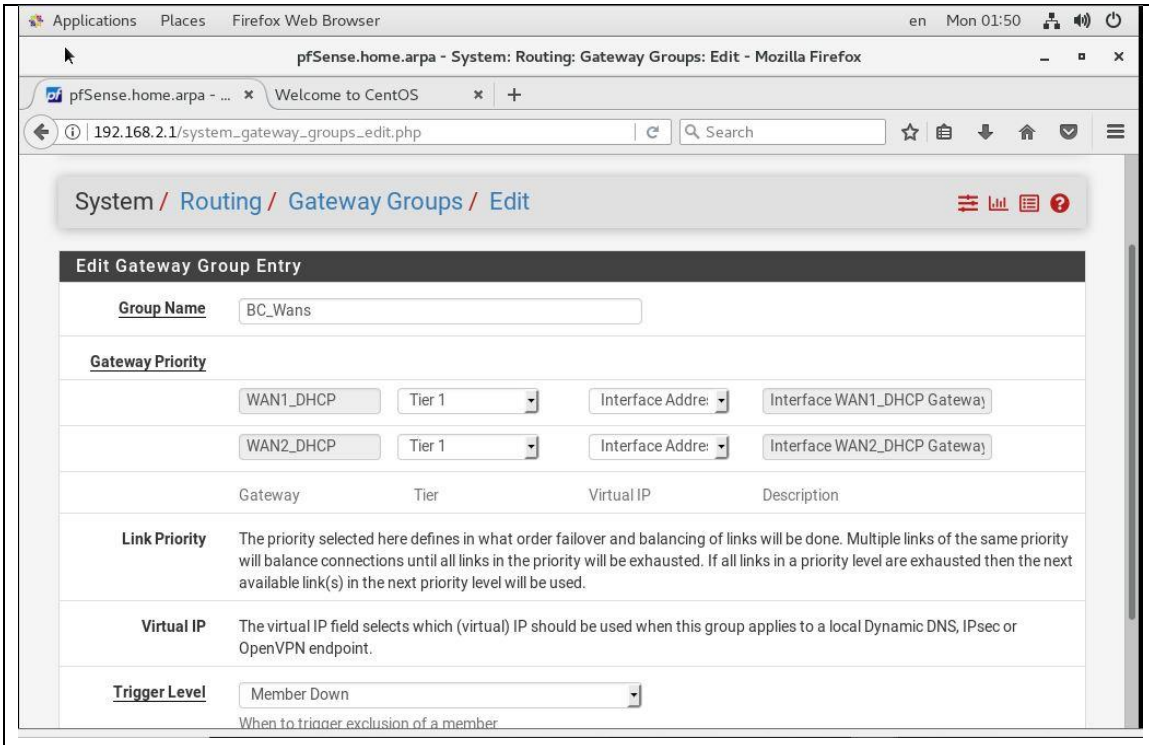




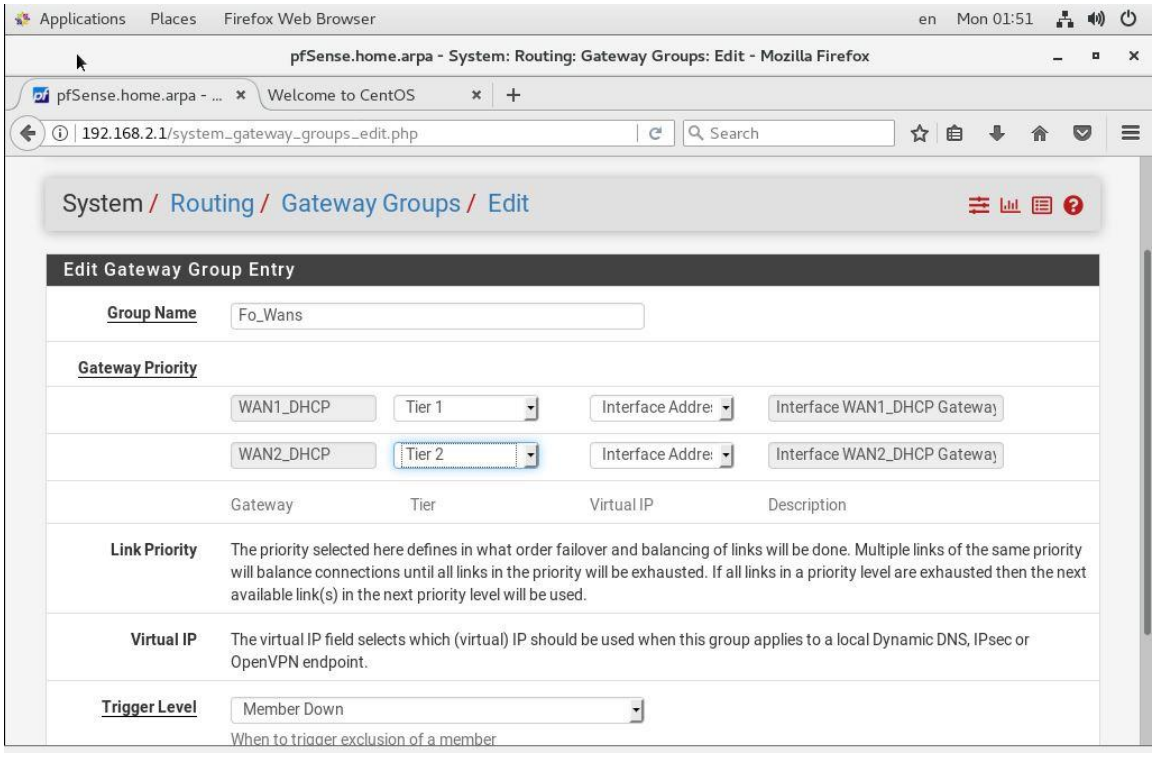
Verificacion de resolucion de DNS, realizar la consulta DNS para vrificar que los DNS estan resolviendo correctamente


Applications Places Firefox Web Browser en Mon 01:49
pfSense.home.arpa - Diagnostics: DNS Lookup - Mozilla Firefox
pfSense.home.arpa - ...
Welcome to CentOS
192.168.2.1/diag_dns.php
Search
2001:4998:24:120d::1:1 AAAA
2001:4998:44:3507::8001 AAAA
Timings
Name server Query time
127.0.0.1 759 msec
192.168.1.1 10 msec
8.8.4.4 25 msec
1.0.0.1 97 msec
8.8.8.8 27 msec
1.1.1.1 98 msec
More Information
Ping
Traceroute

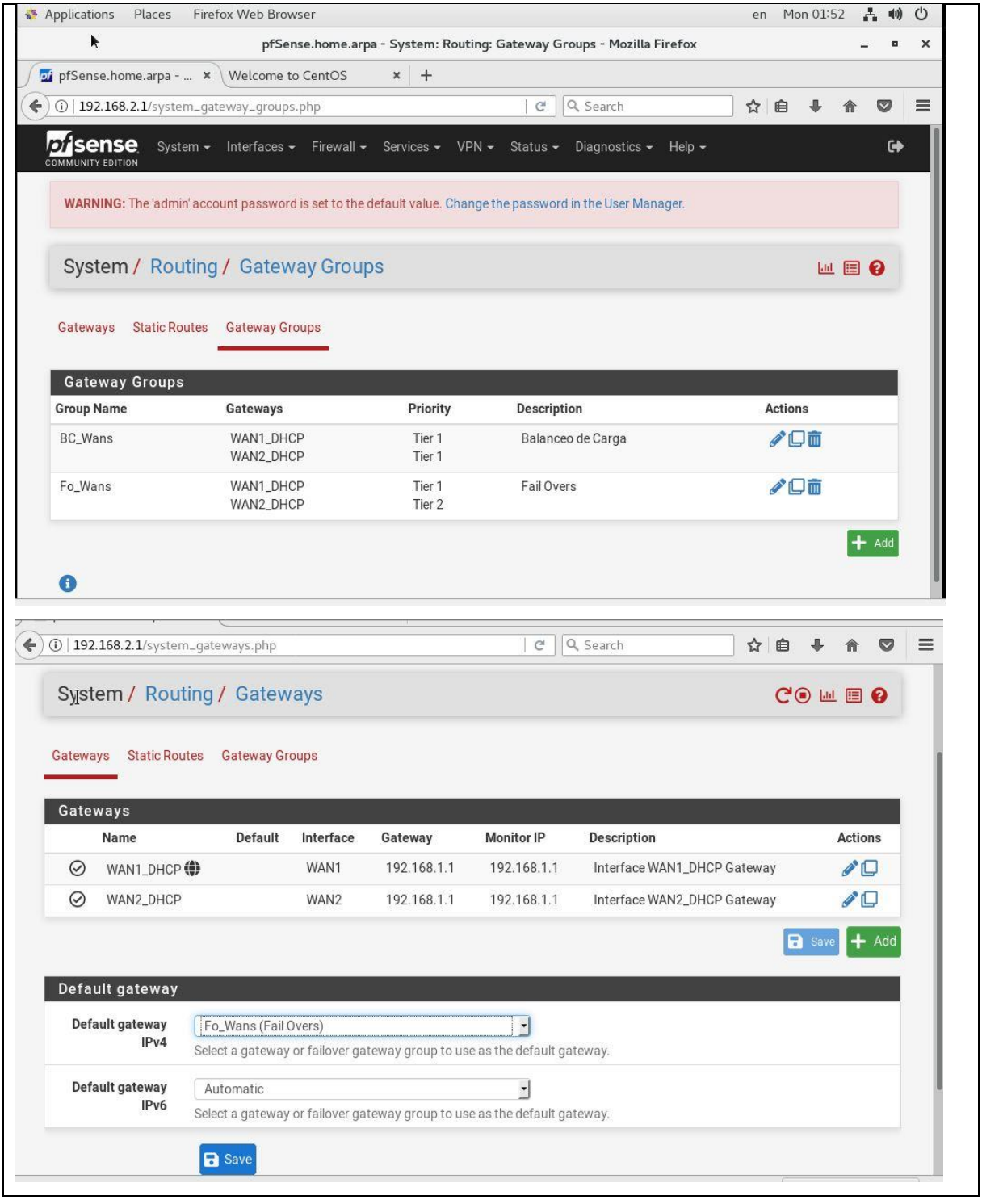

Applications Places Firefox Web Browser en Mon 01:49
pfSense.home.arpa - System: Routing: Gateways - Mozilla Firefox
pfSense.home.arpa - ...
Welcome to CentOS
192.168.2.1/system_gateways.php
Search
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
System / Routing / Gateways
Gateways Static Routes Gateway Groups
Gateways
Name Default Interface Gateway Monitor IP Description Actions
WAN1_DHCP WAN1 192.168.1.1 192.168.1.1 Interface WAN1_DHCP Gateway
WAN2_DHCP WAN2 192.168.1.1 192.168.1.1 Interface WAN2_DHCP Gateway
Save Add
Default gateway
Default gateway Automatic

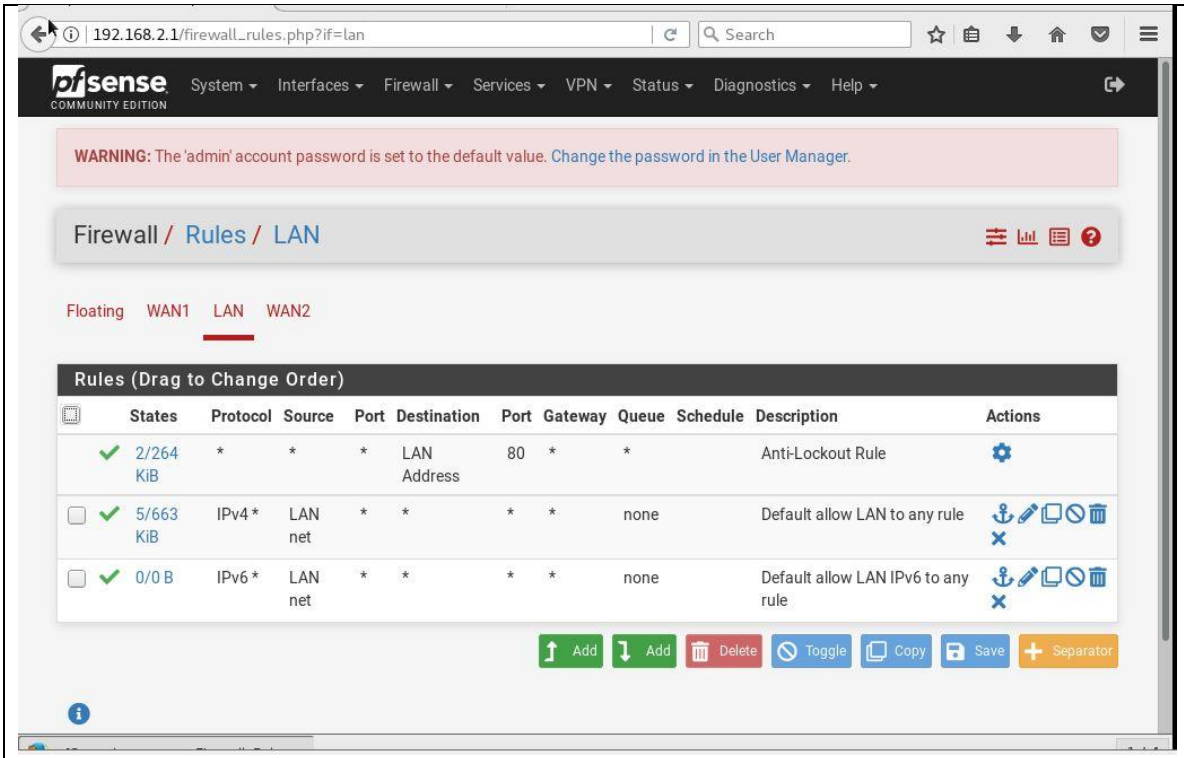


Configuración de Balanceo de Carga en las interfaces WAN.

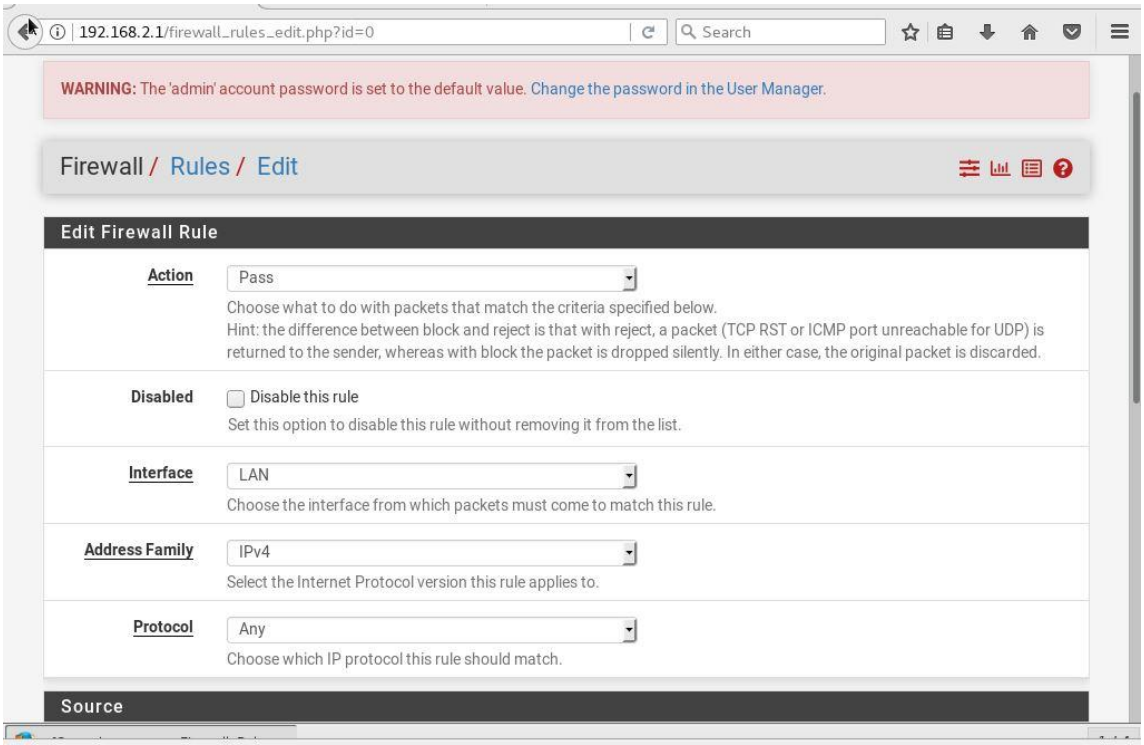


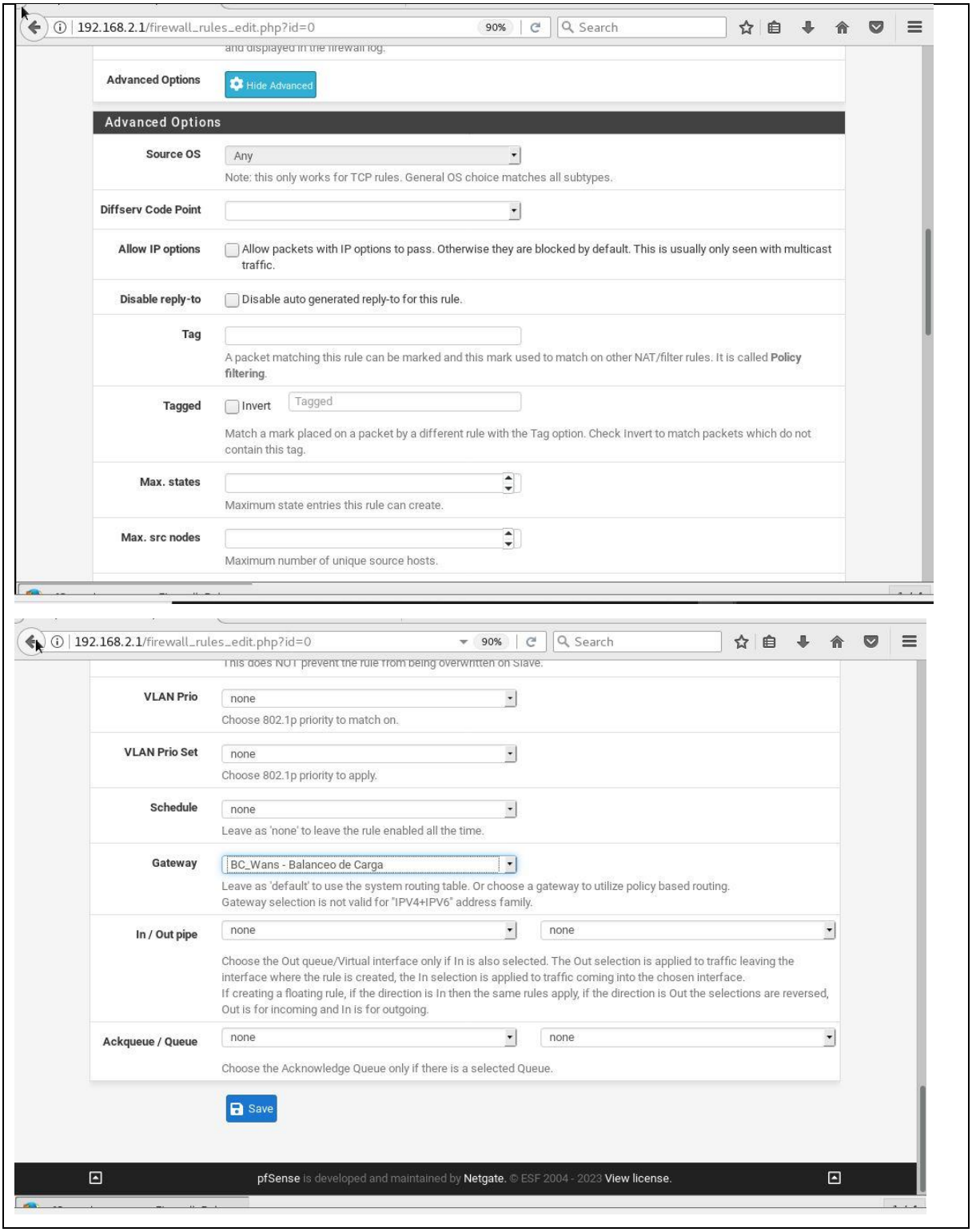
Configuracion de Failover en las interfaces WAN

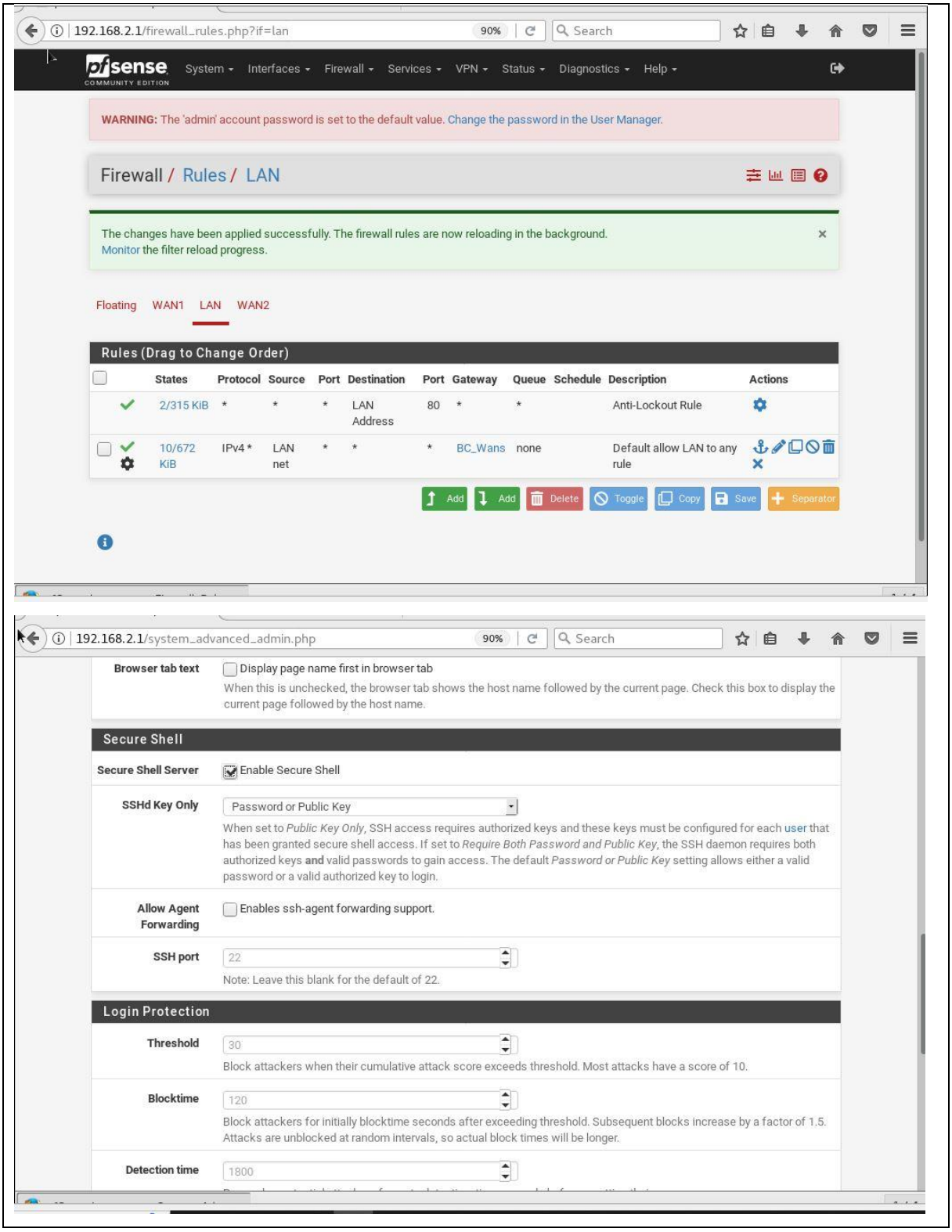

Applications Places Firefox Web Browser en Mon 01:52
pfSense.home.arpa - System: Routing: Gateway Groups - Mozilla Firefox
pfSense.home.arpa - ...
Welcome to CentOS
192.168.2.1/system_gateway_groups.php
Search
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
System / Routing / Gateway Groups
Gateways Static Routes Gateway Groups
Gateway Groups
Group Name Gateways Priority Description Actions
BC_Wans WAN1_DHCP WAN2_DHCP Tier 1 Tier 1 Balanceo de Carga
Fo_Wans WAN1_DHCP WAN2_DHCP Tier 1 Tier 2 Fail Overs
Add
192.168.2.1/system_gateways.php
Search
System / Routing / Gateways
Gateways Static Routes Gateway Groups
Gateways
Name Default Interface Gateway Monitor IP Description Actions
WAN1_DHCP WAN1 192.168.1.1 192.168.1.1 Interface WAN1_DHCP Gateway
WAN2_DHCP WAN2 192.168.1.1 192.168.1.1 Interface WAN2_DHCP Gateway
Save
Add
Default gateway
Default gateway IPv4
Fo_Wans (Fail Overs)
Select a gateway or failover gateway group to use as the default gateway.
Default gateway IPv6
Automatic
Select a gateway or failover gateway group to use as the default gateway.
Save

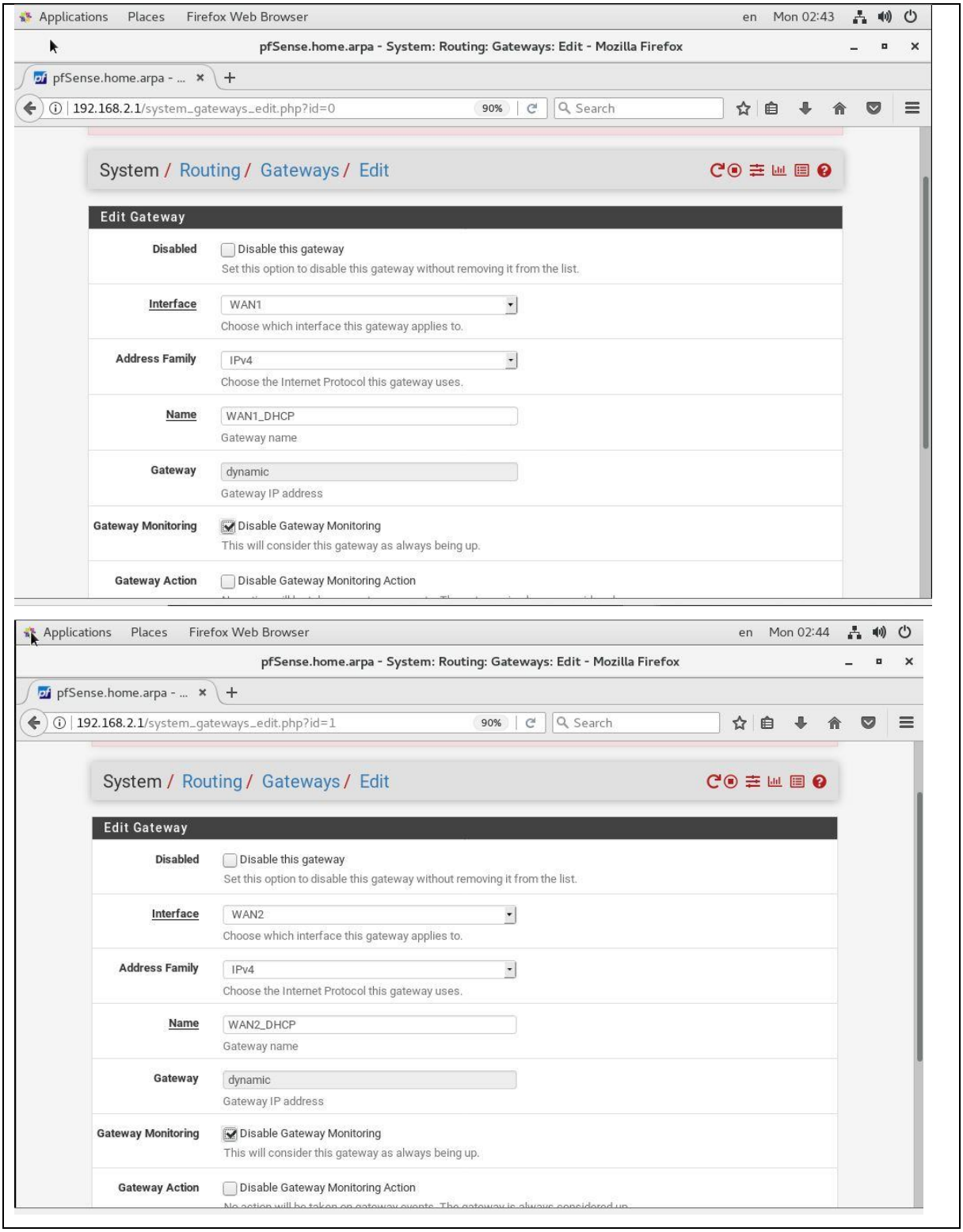


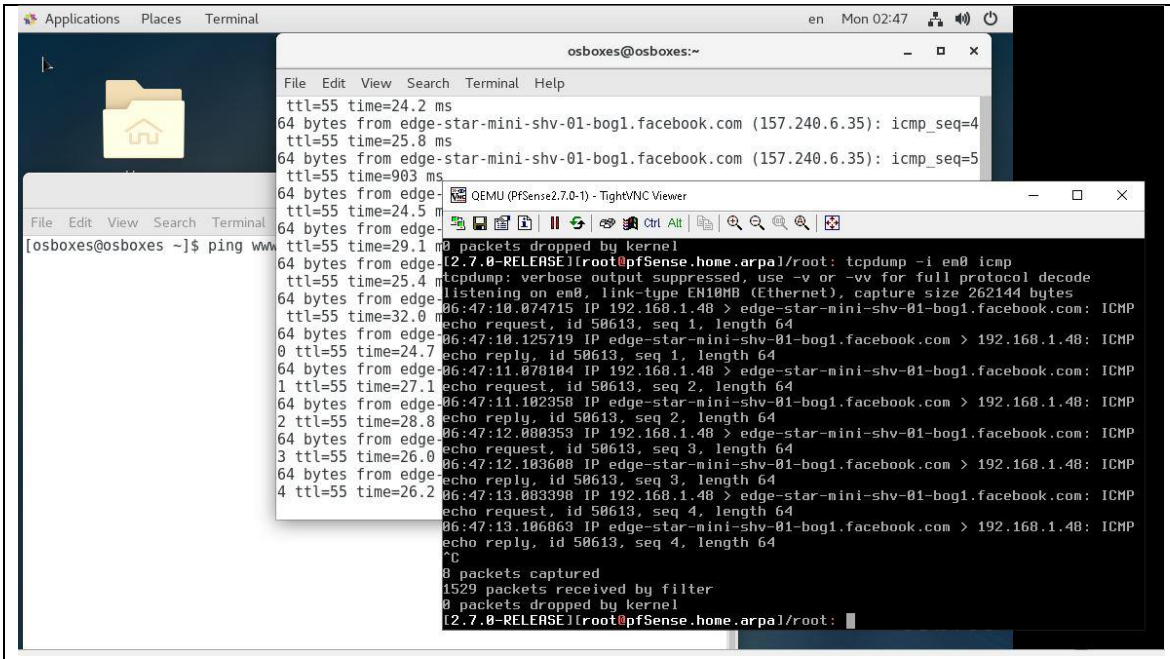
Creación de regla de Firewall para Balanceo de carga como failover




192.168.2.1/firewall_rules_edit.php?id=0
90%
Search
and displayed in the firewall log.
Advanced Options
Hide Advanced
Advanced Options
Source OS
Any
Note: this only works for TCP rules. General OS choice matches all subtypes.
Diffserv Code Point
Allow IP options
Allow packets with IP options to pass. Otherwise they are blocked by default. This is usually only seen with multicast traffic.
Disable reply-to
Disable auto generated reply-to for this rule.
Tag
A packet matching this rule can be marked and this mark used to match on other NAT/filter rules. It is called Policy filtering.
Tagged
Invert
Tagged
Match a mark placed on a packet by a different rule with the Tag option. Check Invert to match packets which do not contain this tag.
Max. states
Maximum state entries this rule can create.
Max. src nodes
Maximum number of unique source hosts.
192.168.2.1/firewall_rules_edit.php?id=0
90%
Search
This does NOT prevent the rule from being overwritten on Slave.
VLAN Prio
none
Choose 802.1p priority to match on.
VLAN Prio Set
none
Choose 802.1p priority to apply.
Schedule
none
Leave as 'none' to leave the rule enabled all the time.
Gateway
BC_Wans - Balanceo de Carga
Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.
Gateway selection is not valid for "IPV4+IPV6" address family.
In / Out pipe
none
none
Choose the Out queue/Virtual interface only if In is also selected. The Out selection is applied to traffic leaving the interface where the rule is created, the In selection is applied to traffic coming into the chosen interface.
If creating a floating rule, if the direction is In then the same rules apply, if the direction is Out the selections are reversed, Out is for incoming and In is for outgoing.
Ackqueue / Queue
none
none
Choose the Acknowledge Queue only if there is a selected Queue.
Save
pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 View license.


192.168.2.1/firewall_rules.php?if=lan
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / LAN
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.
Floating WAN1 LAN WAN2
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
2/315 KiB * * * LAN Address 80 * * Anti-Lockout Rule
10/672 KiB IPv4 * LAN net * * * BC_Wans none Default allow LAN to any rule
Add Add Delete Toggle Copy Save Separator
192.168.2.1/system_advanced_admin.php
Browser tab text
Display page name first in browser tab
When this is unchecked, the browser tab shows the host name followed by the current page. Check this box to display the current page followed by the host name.
Secure Shell
Secure Shell Server
Enable Secure Shell
SSHd Key Only
Password or Public Key
When set to Public Key Only, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to Require Both Password and Public Key, the SSH daemon requires both authorized keys and valid passwords to gain access. The default Password or Public Key setting allows either a valid password or a valid authorized key to login.
Allow Agent Forwarding
Enables ssh-agent forwarding support.
SSH port
22
Note: Leave this blank for the default of 22.
Login Protection
Threshold
30
Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.
Blocktime
120
Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.
Detection time
1800


Applications Places Firefox Web Browser en Mon 02:43
pfSense.home.arpa - System: Routing: Gateways: Edit - Mozilla Firefox
pfSense.home.arpa - ...
192.168.2.1/system_gateways_edit.php?id=0
90%
Search
System / Routing / Gateways / Edit
Edit Gateway
Disabled
Disable this gateway
Set this option to disable this gateway without removing it from the list.
Interface
WAN1
Choose which interface this gateway applies to.
Address Family
IPv4
Choose the Internet Protocol this gateway uses.
Name
WAN1_DHCP
Gateway name
Gateway
dynamic
Gateway IP address
Gateway Monitoring
Disable Gateway Monitoring
This will consider this gateway as always being up.
Gateway Action
Disable Gateway Monitoring Action
Applications Places Firefox Web Browser en Mon 02:44
pfSense.home.arpa - System: Routing: Gateways: Edit - Mozilla Firefox
pfSense.home.arpa - ...
192.168.2.1/system_gateways_edit.php?id=1
90%
Search
System / Routing / Gateways / Edit
Edit Gateway
Disabled
Disable this gateway
Set this option to disable this gateway without removing it from the list.
Interface
WAN2
Choose which interface this gateway applies to.
Address Family
IPv4
Choose the Internet Protocol this gateway uses.
Name
WAN2_DHCP
Gateway name
Gateway
dynamic
Gateway IP address
Gateway Monitoring
Disable Gateway Monitoring
This will consider this gateway as always being up.
Gateway Action
Disable Gateway Monitoring Action



RESULTADO(S) OBTENIDO(S):

El estudiante se familiariza con el concepto de alta disponibilidad de un servicio como es el de internet y practica las configuraciones a realizar en pfSense.

CONCLUSIONES:

El estudiante aprende como configurar balanceo de carga y failover dentro de pfSense para conocer el funcionamiento.

RECOMENDACIONES:

Docente: _____

Firma: _____

V RESULTADOS

5.1. ANALISIS DE RESULTADOS

El análisis de las prácticas realizadas se puede analizar lo siguiente:

1. Configuración ambiente de GNS3 para el banco de pruebas: en esta práctica se proporciona una base sólida para la simulación y prueba de redes en un entorno controlado. Los estudiantes adquieren habilidades esenciales para la configuración de topologías de red virtualizadas.

2. Configuración de una red LAN con pfSense: en esta práctica ofrece a los estudiantes la oportunidad de aprender a configurar un firewall de código abierto y realizar tareas comunes, como asignar direcciones IP y configurar NAT. Esto es fundamental para la administración de redes empresariales.

3. Configuración de un Sistema de Bloqueo de Páginas Web HTTPS: en esta práctica enseña a los estudiantes a implementar una capa adicional de seguridad en la red mediante la restricción de acceso a sitios web. Es relevante para la administración de la política de uso de Internet en entornos corporativos.

4. Configuración de un sistema antivirus con proxy Squid: Los estudiantes aprenden a mejorar la seguridad de la red identificando descargas de archivos comprometidos. Esto es fundamental para proteger una red contra malware y amenazas cibernéticas.

5. Implementación de un sistema de Detección y Prevención de Intrusiones (IDS/IPS): Esta práctica aborda la detección y prevención proactiva de amenazas en una red. Es una habilidad crítica en el campo de la seguridad cibernética y redes.

6. Implementación de IPS con Suricata en pfSense: Reforzar la seguridad de la red es un aspecto crítico en la administración de redes. Los estudiantes aprenden a utilizar herramientas de IPS para proteger la red contra amenazas en tiempo real.

7. Integración de OPNSense y pfSense en una red con OpenDNS: en esta práctica demuestra cómo integrar múltiples soluciones de firewall en una red para lograr un mayor nivel de seguridad. Es relevante para la administración de redes empresariales complejas.

8. Configuración de Doble Autenticación con pfSense y FreeRadius: Los estudiantes adquieren habilidades en autenticación de usuarios con un nivel adicional de seguridad, esto es crucial en entornos donde se requiere autenticación sólida.

9. Habilitación de acceso a Telegram: En esta práctica permite a los estudiantes aprender cómo habilitar servicios específicos en un entorno de firewall. Puede ser útil para fines de administración y notificación de eventos.

10. Configuración de Balanceo de carga y Failover con pfSense: En esta práctica introduce conceptos avanzados de alta disponibilidad y rendimiento de red. Es fundamental para administradores de redes que desean garantizar la continuidad del negocio.

CONCLUSIONES

Las prácticas mencionadas desempeñan un papel fundamental al capacitar a los estudiantes de la Universidad Politécnica Salesiana en habilidades prácticas y conceptuales, resaltando su importancia en:

Desarrollo práctico, ya que proporcionan a los estudiantes la oportunidad de aplicar teorías aprendidas en el aula de clase en entornos virtuales simulados, emulados y reales; esto fomenta un aprendizaje activo y la adquisición de habilidades concretas, esenciales en el mundo profesional de las redes.

Enfoque en Seguridad, ya que varias prácticas abordan la seguridad cibernética, inculcando una mentalidad de seguridad desde el principio; los estudiantes aprenden a mitigar amenazas y a establecer políticas de seguridad efectivas para salvaguardar las redes y los datos.

Preparación para la industria, ya que al dominar la configuración de herramientas de software libre como pfSense, Suricata, Snort, FreeRadius, OPNSense; los estudiantes se preparan para roles en administración de redes y seguridad. Adquieren habilidades relevantes para un entorno laboral en constante evolución.

Formación Multifacética, las prácticas abarcan desde la configuración básica hasta soluciones avanzadas como IPS y balanceo de carga. Esto brinda al estudiante una comprensión solida de una amplia gama de conceptos y tecnologías, enriqueciendo su base de conocimiento.

Colaboración y resolución de problemas, muchas prácticas requieren soluciones creativas y colaboración para superar desafíos técnicos, los estudiantes desarrollan habilidades de resolución de problemas y trabajo en equipo, cruciales para enfrentar los problemas complejos del mundo real.

En resumen, las prácticas empoderan a los futuros profesionales de redes al proporcionales una educación holística que combina teoría y practica a través de la simulación, emulación convirtiéndoles en administradores de redes competentes y conscientes de la seguridad preparados para enfrentar los desafíos cambiantes en el mundo de la tecnología.

RECOMENDACIONES

Las recomendaciones pueden contribuir a mejorar la experiencia de aprendizaje más efectiva y preparar a los estudiantes de manera óptima para enfrentar desafíos en el mundo de las redes y la seguridad cibernética, entre las cuales se considera las siguientes:

Realizar una evaluación continua de las prácticas realizadas a los estudiantes con el fin de alcanzar el objetivo del presente documento que están enfocadas en la administración y seguridad de redes LAN y WAN.

Animar a los estudiantes a resolver problemas relacionados con las configuraciones en lugar de simplemente seguir instrucciones, esto promoverá el pensamiento crítico y la resolución de problemas.

Animar a los estudiantes a buscar certificaciones relevantes en el campo de la seguridad y las redes.

BIBLIOGRAFÍA

Costas Santos, J. (2015). Seguridad informática. RA-MA Editorial. https://bibliotecas.ups.edu.ec:3488/es/lc/bibliotecaups/titulos/62452

Escrivá Gascó, G. (2013). Seguridad informática. Macmillan Iberia, S.A. https://bibliotecas.ups.edu.ec:3488/es/lc/bibliotecaups/titulos/43260

Molina Robles, F. J. (2015). Implantación de los elementos de la red local. RA-MA Editorial. https://bibliotecas.ups.edu.ec:3488/es/lc/bibliotecaups/titulos/62445

Robledo Sosa, C. (2002). Redes de computadoras. Instituto Politécnico Nacional. https://bibliotecas.ups.edu.ec:3488/es/lc/bibliotecaups/titulos/101803

Sánchez Rubio, M. Barchino Plata, R. y Martínez Herráiz, J. J. (2020). Redes de computadores. Editorial Universidad de Alcalá. https://bibliotecas.ups.edu.ec:3488/es/lc/bibliotecaups/titulos/131606

Abad Domingo, A. (2013). Redes locales. McGraw-Hill España. https://bibliotecas.ups.edu.ec:3488/es/lc/bibliotecaups/titulos/50228

Lancho González Alvaro. (2017). Sistema Cortafuegos de alta disponibilidad c on PfSense. Universidad Politécnica de Madrid
https://oa.upm.es/49677/1/TFG_ALVARO_LANCHO_GONZALEZ.pdf

Delgado Zambrano Pablo y Loor Antonio. (2017). Sistema perimetral firewall y fortalecimiento de la seguridad en el DATA CENTER de la ESPAM MFL. ESCUELA SUPERIOR POLITÉCNICA AGROPECUARIA DEMANABÍ MANUEL FÉLIX LÓPEZ.
https://repositorio.espam.edu.ec/bitstream/42000/477/1/TC107.pdf

Pérez Rosero Francisco. (2020). MANUAL PARA SIMULAR LA TOPOLOGIA DE RED Y SEGURIDADES DEL SERVIDOR WEB EN LA COOPERATIVA DE AHORRO Y CRÉDITO “RIOBAMBA” LTDA.
http://dspace.unach.edu.ec/bitstream/51000/6594/2/Manual%20Mejorar%20la%20Seguridad%20Inform%C3%A1tica%20en%20la%20COAC%20Riobamba%20Ltda.pdf