REPÚBLICA DEL ECUADOR

INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo

DESARROLLO DE SOFTWARE

"IMPLEMENTACIÓN DE UN FIREWALL UTILIZANDO HERRAMIENTAS OPEN SOURCE PARA EL INSTITUTO SUPERIOR TECNOLÓGICO TENA"

INFORME TÉCNICO DE EXAMEN MODALIDAD COMPLEXIVO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN DESARROLLO DE SOFTWARE TECNOLÓGICO

AUTORES: Carchi Cerda Jair Orlando,
Yumbo Grefa Jhony Bryan
TUTOR: Ing. Fausto Pantaleón Claudio Espín

Tena - Ecuador

2024-IIS

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

APROBACIÓN DEL TUTOR

ING. Fausto Pantaleón Claudio Espín

PROFESOR DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA.

CERTIFICA:

En calidad de Tutor Examen de carácter complexivo práctico denominado: **Implementación de un firewall utilizando herramientas open source para el Instituto Superior Tecnológico Tena**, de autoría del señor **Jair Orlando Carchi Cerda,** con CC. 1501135501 y **Jhony Bryan Yumbo Grefa**, con CC. 1501117954, estudiantes de la Carrera de Tecnología Superior en Desarrollo de Software del Instituto Superior Tecnológico Tena, CERTIFICO que se ha realizado la revisión prolija del Examen de carácter complexivo práctico antes citado, cumple con los requisitos de fondo y de forma que exigen el respectivo reglamento e institución.

Tena, 19 de febrero de 2025

Ing. Fausto Pantaleón Claudio Espín

TUTOR DEL EXAMEN DE CARACTER COMPLEXIVO PRÁCTICO

RESUMEN

Este proyecto aborda la implementación de un firewall eficiente utilizando herramientas de software libre, para proteger las redes internas del Instituto Superior Tecnológico Tena. El objetivo principal es implementar un software que permita filtrar el tráfico entrante y saliente, bloquear conexiones no deseadas y monitorear el flujo de datos en tiempo real, garantizando la seguridad y el buen desempeño de la red institucional.

La metodología aplicada incluye la configuración de un entorno virtualizado para simular la infraestructura de red del instituto, utilizando software como pfSense y complementos de monitoreo como Snort o Suricata. Este enfoque permite validar el rendimiento del firewall y ajustar las reglas de seguridad según las necesidades específicas del entorno académico.

El resultado esperado es un prototipo funcional que pueda servir como base para la implementación en un entorno real. Este sistema demostrará cómo las herramientas open source pueden ofrecer soluciones accesibles y efectivas para mejorar la ciberseguridad en instituciones con recursos limitados.

En conclusión, este proyecto resalta la importancia de adoptar tecnologías de código abierto para resolver problemas críticos, como la seguridad de la información, fomentando el uso de soluciones sostenibles y personalizables en el ámbito académico.

Palabras clave: Herramientas de software libre, entorno virtualizado, soluciones accesibles y efectivas.

ABSTRACT

This project addresses the implementation of an efficient firewall using free software tools to protect the internal network of the Instituto Superior Tecnológico Tena. The main objective is to implement software that allows filtering incoming and outgoing traffic, blocking unwanted connections and monitoring data flow in real time, ensuring the security and good performance of the institutional network.

The applied methodology includes the configuration of a virtualized environment to simulate the network infrastructure of the institute, using software such as pfSense and monitoring plugins such as Snort or Suricata. This approach allows validating the performance of the firewall and adjusting security rules according to the specific needs of the academic environment.

The expected result is a functional prototype that can serve as a basis for implementation in a real environment. This system will demonstrate how open source tools can offer accessible and effective solutions to improve cybersecurity in institutions with limited resources.

In conclusion, this project highlights the importance of adopting open source technologies to solve critical problems, such as information security, encouraging the use of sustainable and customizable solutions in the academic field.

Keywords: Free software tools, virtualized environment, accessible and effective solution

Reviewed by

B.A Carolina Romero, MEd
Language Center Coordinator

INTRODUCCIÓN

1.1 Contexto General

En la actualidad, las instituciones enfrentan múltiples desafíos en cuanto a la protección de sus redes informáticas, debido al incremento de ciberamenazas y la necesidad de garantizar un entorno digital seguro para estudiantes y personal administrativo. El Instituto Superior Tecnológico Tena no es ajeno a esta problemática, ya que la infraestructura de su red es fundamental para soportar los procesos académicos y administrativos que se desarrollan en la institución.

Un firewall es una herramienta esencial en la gestión de la seguridad de las redes, ya que permite controlar y filtrar el tráfico de datos, prevenir accesos no autorizados y proteger los recursos internos de posibles ataques externos. Sin embargo, el costo de soluciones comerciales puede ser un obstáculo para muchas instituciones, lo que subraya la necesidad de adoptar alternativas accesibles y eficientes.

El presente proyecto propone la implementación de un firewall utilizando herramientas open source, con el propósito de ofrecer una solución económica, personalizable y efectiva que permita proteger la red del Instituto Superior Tecnológico Tena. Mediante el uso de plataformas como pfSense, en combinación con otras herramientas de monitoreo y filtrado, se busca diseñar un sistema que no solo cumpla con los estándares de seguridad, sino que también sea fácil de mantener y adaptar a las necesidades cambiantes de la institución.

1.2 Antecedentes

1.2.1 Antecedentes generales sobre la seguridad en redes

En los últimos años, la seguridad de redes ha cobrado gran importancia debido al incremento de ataques cibernéticos en instituciones educativas y organizaciones gubernamentales. Según estudios realizados por el National Institute of Standards and Technology (NIST), más del 60% de los ataques informáticos provienen de accesos no autorizados o vulnerabilidades en la infraestructura de red. La implementación de firewalls es una de las estrategias más efectivas para proteger redes de este tipo de amenazas, permitiendo el control del tráfico entrante y saliente mediante reglas de filtrado.

1.3 2. Uso de herramientas open source en la seguridad de redes

El uso de software open source en seguridad informática ha crecido exponencialmente en las últimas décadas. Herramientas como pfSense, IPFire, Suricata y Snort han demostrado ser soluciones robustas para la protección de redes institucionales. A diferencia de soluciones propietarias, cuyos costos pueden oscilar entre $1,000 y $10,000 USD anuales en licencias y soporte, estas tecnologías permiten la implementación de firewalls eficientes con un costo significativamente menor. Si bien el software es gratuito, se deben considerar gastos en hardware adecuado (desde $300 a $2,000 USD según la capacidad requerida) y en capacitación del personal para su correcta implementación y mantenimiento. Gracias a estos menores costos, las soluciones open source facilitan la accesibilidad a instituciones con recursos limitados sin comprometer la seguridad.

1.4 Planteamiento del problema

En la actualidad, las instituciones educativas dependen en gran medida de sus infraestructuras tecnológicas para la gestión académica y administrativa. Sin embargo, la red

del Instituto Superior Tecnológico Tena si posee medidas básicas de seguridad, como un firewall generado por la Senescyt, sin embargo el Instituto no cuenta con permisos para administrar y monitorear en tiempo real el control del tráfico de datos, accesos no autorizados, ataques cibernéticos y filtraciones de información. El Instituto necesita internamente tener un firewall para tener accesos a todas las reglas y controles.

Uno de los principales problemas es la falta de un firewall virtualizado aparte del firewall generado por Senescyt, que permita filtrar conexiones y monitorear el tráfico en tiempo real, también funcionaria como una capa más de seguridad o ventaja de doble protección. Esto impide detectar y bloquear amenazas como intentos de intrusión, propagación de malware o actividades no permitidas dentro de la red del Instituto. La ausencia de mecanismos de control compromete la confidencialidad, integridad y disponibilidad de los datos, lo que puede derivar en pérdidas de información, interrupción de servicios y vulneraciones a la privacidad de los usuarios.

Ante esta situación, es necesario implementar una solución de seguridad informática que permita gestionar de manera eficiente el tráfico de red, establecer reglas de filtrado y monitorear posibles amenazas en tiempo real. La implementación de un firewall utilizando herramientas open source representa una alternativa viable, ya que proporciona un alto nivel de seguridad. Con esta solución, se busca fortalecer la protección de la red del Instituto, garantizar el acceso seguro a los servicios digitales y mejorar la administración de sus recursos tecnológicos.

1.5 Objetivos

1.5.1 Objetivo general

Analizar un firewall utilizando herramientas open source para el Instituto Superior Tecnológico Tena, para demostrar un sistema que permita filtrar el tráfico de red, bloquear accesos no autorizados y monitorear la actividad en tiempo real, contribuyendo a la seguridad y protección de la información institucional.

1.5.2 Objetivos específicos

Comprender los conceptos básicos de seguridad perimetral y el funcionamiento de firewall.

Configurar reglas de acceso y políticas de seguridad para proteger la red.

Evaluar el desempeño y la eficacia del firewall implementado mediante pruebas prácticas.

1.6 Justificación

El presente proyecto es de gran relevancia debido a la creciente necesidad de fortalecer la seguridad de redes en entornos educativos. La implementación de un firewall open source ofrece una solución económica y eficiente para proteger la infraestructura de red del Instituto. Además, el uso de herramientas open source permite una mayor flexibilidad y personalización en la configuración del firewall, favoreciendo la optimización de recursos y la formación del personal en tecnologías de código abierto.

1.7 Marco conceptual

En el ámbito de la seguridad informática, la protección de redes es un aspecto fundamental para garantizar la integridad y disponibilidad de los datos en cualquier

institución. La implementación de firewalls se ha convertido en una solución efectiva para mitigar riesgos relacionados con accesos no autorizados y ataques cibernéticos. A continuación, se presentan los conceptos clave que sustentan este proyecto.

1.8 Seguridad Informática

La seguridad informática es el conjunto de medidas y técnicas diseñadas para proteger la información y los sistemas informáticos de accesos no autorizados, ataques, daños o robos. Según Tanenbaum y Wetherall (2021), los principales principios de la seguridad informática son:

Confidencialidad: Garantiza que la información solo sea accesible por personas autorizadas.

Integridad: Asegura que los datos no sean alterados o modificados sin autorización.

Disponibilidad: Garantiza que los sistemas y la información estén accesibles cuando se necesiten.

También están los reglamentos tanto como la de Senescyt e institucional que permiten dar asistencia a la seguridad informática:

1.8.1 Reglamentos de la SENESCYT

Reglamento del Sistema Nacional de Educación Superior (SENESCYT)

Artículo 97: Establece la responsabilidad de las instituciones de educación superior para garantizar la seguridad y confidencialidad de la información en su infraestructura tecnológica.

Artículo 112: Obliga a las instituciones a implementar mecanismos de protección de datos personales y acceso restringido a la información académica y administrativa.

Artículo 129: Requiere que las plataformas digitales utilizadas para la educación y gestión académica cumplan con estándares de seguridad y accesibilidad.

Ley Orgánica de Protección de Datos Personales (LOPDP)

Regula el tratamiento de datos personales en instituciones públicas y privadas, asegurando el derecho a la privacidad y confidencialidad de la información.

Obliga a implementar medidas de seguridad en servidores, redes y bases de datos que almacenen información sensible de estudiantes y docentes.

Marco de Gobierno de Tecnologías de la Información (Gobierno Nacional de Ecuador)

Define buenas prácticas en ciberseguridad que deben adoptar las instituciones del sector público, incluyendo la aplicación de firewalls, sistemas de monitoreo y planes de contingencia.

1.8.2 Reglamentos Institucionales del Instituto Superior Tecnológico Tena

Reglamento Interno de Tecnologías de la Información

Uso adecuado de la red institucional: Establece políticas de acceso a Internet, restricciones de tráfico y prohibición de uso indebido de recursos tecnológicos.

Implementación de firewalls y medidas de seguridad: Obliga a que el área de TI instale y mantenga herramientas de protección como pfSense para filtrar tráfico y prevenir accesos no autorizados.

Responsabilidad del personal de la Unidad de Tecnología de la Información: Define que los administradores de red deben monitorear y responder a incidentes de seguridad para evitar vulnerabilidades en la infraestructura tecnológica.

Políticas de Protección de la Información y Privacidad

Establece que toda la información académica, administrativa y personal almacenada en servidores debe estar protegida con controles de acceso, cifrado y mecanismos de respaldo.

Determina que solo usuarios autorizados pueden acceder a información crítica y que las conexiones externas deben ser gestionadas mediante VPNs seguras.

Código de Ética Institucional

Promueve el uso responsable de los recursos tecnológicos dentro del instituto.

Prohíbe actividades que comprometan la seguridad de la red, como la descarga de software malicioso, el acceso no autorizado a servidores y la manipulación indebida de información.

1.9 Firewall

Un firewall es un sistema de seguridad que filtra el tráfico de red basado en reglas predefinidas. Su función principal es permitir o bloquear conexiones en función de criterios de seguridad. Puede ser implementado en hardware o software y operar en distintas capas del modelo OSI.

1.9.1 Herramienta utilizada: pfSense

pfSense es un firewall y enrutador open source basado en FreeBSD, utilizado ampliamente en redes empresariales e institucionales. Proporciona un control avanzado del tráfico de red, filtrado de paquetes, VPNs, detección de intrusos y monitoreo en tiempo real.

1.9.2 Ventajas de pfSense

- Gratuito y Open Source – No requiere licencias costosas como soluciones propietarias (Cisco ASA, Fortinet).
- Interfaz web intuitiva – Facilita la administración sin necesidad de usar comandos de terminal.
- Alta personalización – Permite crear reglas específicas para distintos tipos de tráfico.
- Soporte de VPNs – Ofrece opciones avanzadas para conexiones seguras entre redes.
- Ampliable con plugins – Puede integrarse con Snort, Suricata, pfBlockerNG, Squid, entre otros.
- Compatible con hardware diverso – Puede instalarse en servidores físicos o virtualizados en Proxmox, VMware, VirtualBox.

1.9.3 Desventajas de pfSense

- Curva de aprendizaje – Aunque tiene una interfaz gráfica, su configuración avanzada requiere conocimientos en redes.

- Altos requisitos de hardware para IDS/IPS – Funciones como Snort o Suricata pueden consumir mucha CPU y RAM.
- No incluye detección de intrusos por defecto – Es necesario instalar complementos como Snort o Suricata.
- Menor soporte oficial en comparación con soluciones comerciales – Aunque tiene una comunidad activa, no tiene un soporte técnico dedicado como Cisco o Fortinet.

1.10 Redes Informáticas y Monitoreo de Tráfico

Las redes informáticas permiten la comunicación entre dispositivos dentro de una organización. En el Instituto Superior Tecnológico Tena, existen diferentes tipos de redes, cada una con un propósito específico. La red administrativa gestiona los sistemas internos, como registros académicos, bases de datos y servidores institucionales. La red académica proporciona conectividad a docentes y estudiantes para el acceso a plataformas educativas, como Moodle y bibliotecas digitales. Además, la red inalámbrica (Wi-Fi) está disponible en áreas comunes para el acceso controlado a Internet. Para garantizar la seguridad de estas redes, es necesario implementar mecanismos de monitoreo de tráfico en tiempo real, lo que permite detectar patrones sospechosos, controlar accesos no autorizados y responder ante posibles ataques cibernéticos.

1.11 Virtualización en Seguridad de Redes

La virtualización permite simular entornos de red sin necesidad de hardware físico. En este proyecto, se utilizará un entorno virtualizado para simular la implementación del firewall antes de su posible despliegue en la infraestructura real del Instituto. La

virtualización se hará en el servidor HP ProLiant ML310e Gen8 v2, equipado con un procesador Intel Xeon CPU E3-1240 v3 (3.40 GHz, x 8), 4 GB de memoria RAM y un almacenamiento de 2TB en SSD para garantizar un rendimiento óptimo. Este servidor tiene el CentOS Stream 9, permitirá ejecutar pfSense en una máquina virtual utilizando VirtualBox como hipervisor, lo que facilitará la configuración, pruebas y monitoreo del firewall en un entorno controlado.

1.12 PfSense herramienta open source para la implementación

pfSense es una opción altamente factible para la implementación de firewalls en entornos institucionales gracias a su bajo costo, flexibilidad, facilidad de uso y robustez. Su adopción permite a las organizaciones contar con una infraestructura segura sin la necesidad de invertir grandes sumas en software propietario.

1.12.1 Beneficios de pfSense

Algunas de sus ventajas clave incluyen:

- Costo cero en licencias: Al ser open source, no requiere pago por licencias, lo que reduce significativamente los costos en comparación con soluciones como Cisco ASA o Fortinet.
- Alto rendimiento: Puede gestionar grandes volúmenes de tráfico y conexiones simultáneas con un hardware adecuado.
- Modularidad y escalabilidad: Permite agregar funciones avanzadas a través de paquetes adicionales como Snort (IDS/IPS), Squid (proxy) y pfBlockerNG (bloqueo de IPs y dominios maliciosos).

- Fácil administración: Cuenta con una interfaz web intuitiva que facilita la configuración y monitoreo sin necesidad de conocimientos avanzados en FreeBSD.

Factibilidad de Implementación

- Requisitos de hardware flexibles: Puede ejecutarse en hardware de bajo costo o en máquinas virtuales, lo que lo hace viable para organizaciones con recursos limitados.
- Compatibilidad con redes existentes: Se integra sin problemas en infraestructuras de red actuales, permitiendo configuraciones como VPNs, VLANs y balanceo de carga.
- Comunidad activa y soporte técnico: pfSense cuenta con una gran comunidad de usuarios y documentación extensa, además de la opción de soporte comercial con Netgate.

Utilización en entornos reales

- Instituciones educativas y gubernamentales: Utilizado para proteger redes y segmentar tráfico sin incurrir en costos elevados.
- Empresas y PYMEs: Brinda seguridad de nivel empresarial sin necesidad de pagar por soluciones propietarias.
- Centros de datos y telecomunicaciones: Puede manejar tráfico de alto volumen con configuraciones avanzadas de seguridad y QoS.

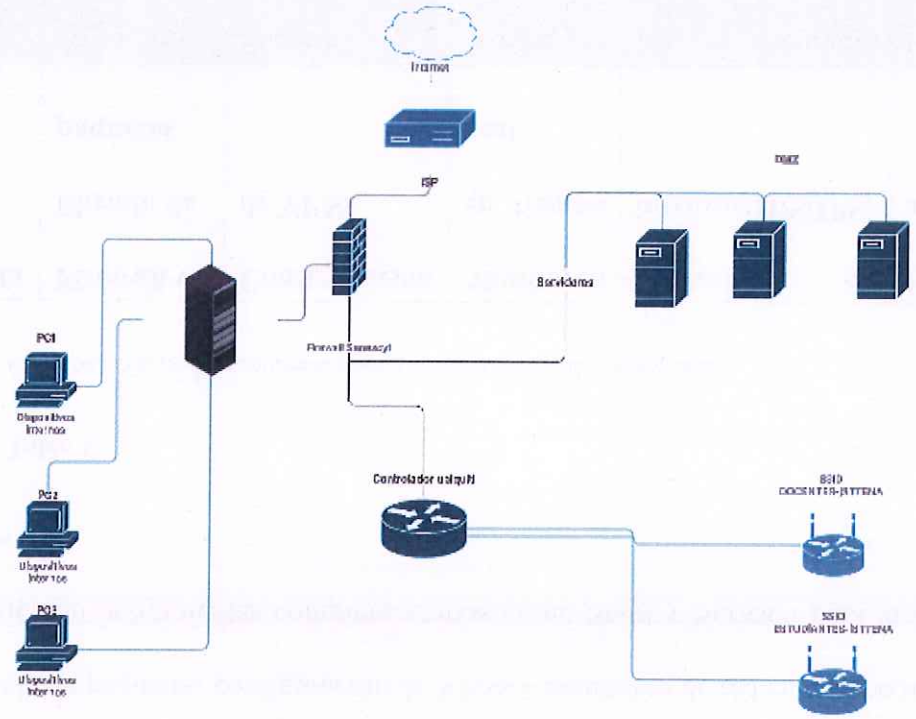
ANÁLISIS

1.13 Estado actual de la red del Instituto

Actualmente, el Instituto no cuenta con el manejo interno del firewall generado por la Senescyt de la red principal, y el responsable de la Unidad de Tecnología de la Información no monitorea, ni administra, tampoco se ha consultado sobre ataques que ha sufrido el Instituto en años atrás, el firewall es el software de protección de red que permita filtrar el tráfico y detectar amenazas en tiempo real. Esto llevo a implementar una capa más de seguridad como el pfSense donde pueda ser usado internamente.

Figura 1.

Estructura de red.



Fuente: Red digitalizada en lucid.app

1.14 Herramientas open source para la implementación del firewall

Entre las soluciones disponibles, se evaluaron distintas herramientas open source, concluyendo que pfSense es la opción más adecuada debido a sus características avanzadas de filtrado de paquetes, configuración de VPNs y monitoreo de red en tiempo real. También se consideran herramientas complementarias como Snort y Suricata para la detención de intrusos.

Tabla 1.

Comparación de herramientas open source de firewall y seguridad

Herramienta	**Firewall y filtrado de paquetes**	**Configuración de VPNs**	**Monitoreo en tiempo real**	**Detección de intrusos(IDS/IPS)**	**Facilidad de administración**
pfSense	Avanzado	Soporta OpenVPN. IPsec	Interfaz grafica y CLI	No integrado, requiere snort y suricata	Intuitivo con interfaz web
OPNsense	Similar a pfSense	Soporta OpenVPN. IPsec	Integrado con NetFlow	IDS integrado con suricata	Interfaz moderna
IPFire	Eficiente pero menos flexible	Soporta OpenVPN. IPsec	Limitado	IDS basico con guardian	Requiere configuracion avanzada

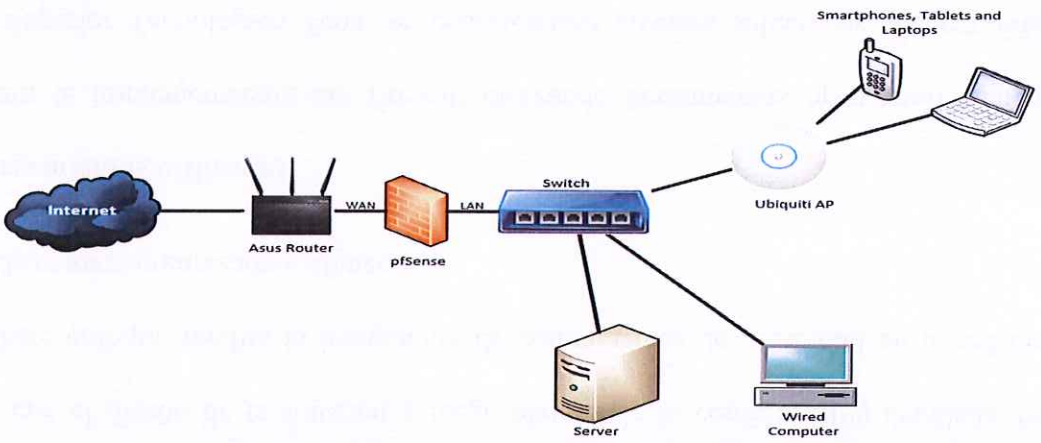
Snort	No es un firewall	No aplica	Require integración	Alta precision en deteccion de intrusos	Complejo requiere reglas personalizadas
Suricata	No es un firewall	No aplica	Require integración	Multihilo, major rendimiento que snort	Configuración avanzada necesaria

Fuente: tabla de análisis de una detección efectiva de intrusos

Con esta tabla, el análisis muestra que pfSense es la mejor opción por su combinación de firewall robusto, facilidad de administración y soporte para VPNs, aunque Snort y Suricata son necesarias para una detección efectiva de intrusos.

Figura 2.

Estructura de implementación de pfSense en una red



Fuente: Firewall con pfSense

1.15 Metodología implementada

Para llevar a cabo la implementación del firewall utilizando herramientas open source en el Instituto Superior Tecnológico Tena, se utilizará la metodología Top-Down, la cual permite diseñar y estructurar la solución desde un enfoque general hasta los detalles técnicos específicos. Consiste en dividir el proceso de implementación en etapas secuenciales, iniciando con el diseño de la solución y luego abordando la configuración detallada del sistema. Este enfoque facilita la integración de componentes de seguridad en la red del Instituto de manera organizada y eficiente.

1.16 Herramientas utilizadas

Para la implementación del firewall utilizando herramientas open source en el Instituto Superior Tecnológico Tena, se seleccionaron diversas soluciones que permiten filtrar el tráfico de red, detectar intrusos y mejorar la seguridad de la infraestructura informática. A continuación, se presentan las principales herramientas utilizadas, su concepto y su funcionamiento.

1.17 Comparación de herramientas open source

Existen diversas herramientas open source para la implementación de firewalls, cada una con características específicas que permiten filtrar tráfico, gestionar accesos y proteger redes contra amenazas002E

Tabla 2.

Cuadro comparativo de herramientas open source.

Funcionalidades	PfSense	OPNSense	IPFire

Tipo de solución	Firewall, enrutador	Firewall, enrutador	Firewall, enrutador
Enfoque	Código abierto	Código abierto	Código abierto
Interfaz Gráfica de usuario	WebGUI	WebGUI	WebGUI
Facilidad de uso	Interfaz intuitiva	Interfaz intuitive	Interfaz intuitiva
Características de seguridad	Firewall de próxima generación, VPN, IDS/IPS, filtrado web, balanceo de carga, failover, entre otros.	Firewall de próxima generación, VPN, IDS/IPS, filtrado web, balanceo de carga, QoS, entre otros.	Firewall de próxima generación, VPN, IDS/IPS, filtrado web, balanceo de carga, QoS, entre otros.
Rendimiento	Alto rendimiento	Alto rendimiento	Buen rendimiento
Licenciamiento	Licencia BSD	Licencia BSD	Licencia GPL
Soporte técnico	Comunidad de usuarios, soporte comercial disponible.	Comunidad de usuarios, soporte comercial disponible.	Comunidad de usuarios, soporte comercial disponible.
Actualizaciones y seguridad	Actualizaciones regulares, correcciones de seguridad.	Actualizaciones regulares, correcciones de seguridad.	Actualizaciones regulares, correcciones de seguridad.
Integración con otros sistemas	API disponible	API disponible	API disponible
Personalización	Altamente personalizable	personalizable	Personalizable

Compatibilidad de hardware	Amplia gama de hardware soportado	Amplia gama de hardware soportado	Amplia gama de hardware soportado

Fuente: comparación de herramientas open source.

Ahora haremos un cuadro igual al anterior cuadro comparativo pero con algunas funcionalidades que estas soluciones ofrecen.

Tabla 3.

Cuadro comparativo de funcionalidades.

Funcionalidades	PfSense	OPNSense	IPFire
Firewall	✓	✓	✓
Enrutador	✓	✓	✓
VPN	✓	✓	✓
IDS/IPS	✓	✓	✓
Filtrado Web	✓	✓	✓
Balanceo de carga	✓	✓	X
QoS	✓	✓	X
Failover	✓	✓	✓

Alta disponibilidad	✓	✓	X
Control de ancho de banda	✓	✓	X
Filtrado de contenido	✓	✓	X
Protección del malware	✓	✓	✓
Filtrado de correo no deseado	✓	✓	X
Virtualización	✓	X	X
Portal Cautivo	✓	X	X
Autenticación de usuario	✓	✓	X
Registros de eventos	✓	✓	X
Integración con servicios cloud	✓	✓	X

Fuente: Funcionalidades de herramientas open source.

1.18 PfSense

PfSense es un firewall open source basado en FreeBSD que ofrece una interfaz web intuitiva para administrar reglas de seguridad, control de tráfico y configuración de redes. Es

ampliamente utilizado en entornos empresariales y educativos debido a su robustez y facilidad de uso.

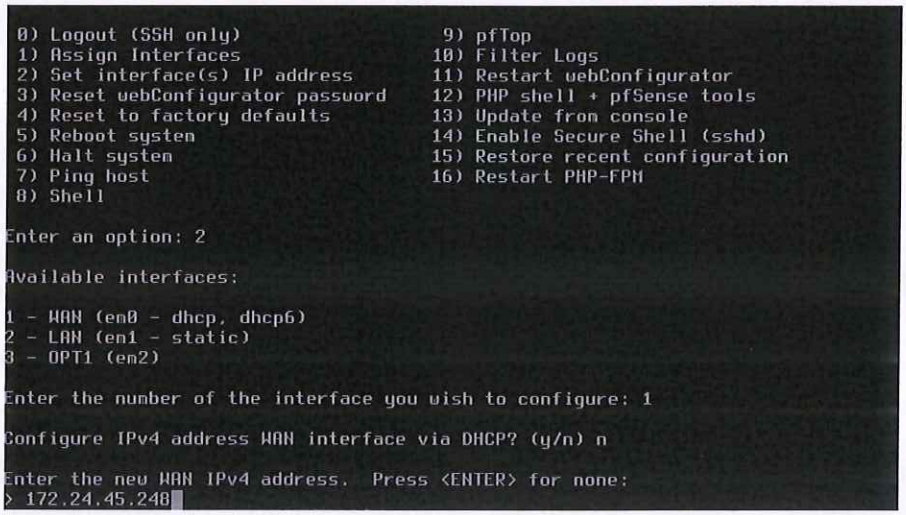
¿Cómo funciona?

Se instala en un servidor físico o virtualizado.

Instalación y configuración de PFSense (Firewall). Este sistema de cortafuegos está basado en FreeBSD que permite diversas características y es de código abierto, en la figura 1, se muestra la configuración de las interfaces que manejara pfSense dentro de la arquitectura como se planteó en la imagen.

Figura 3.

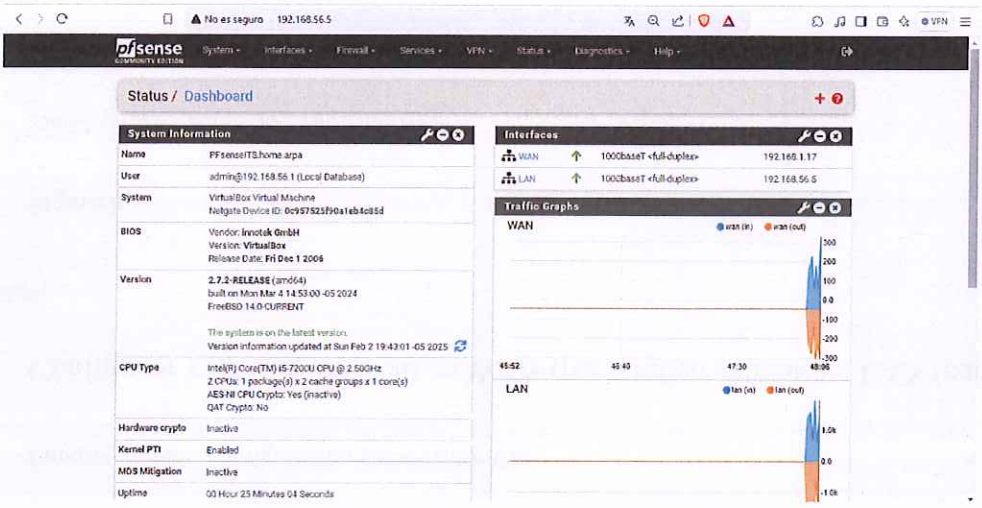
Interfaz de las configuraciones de pfSense.



Fuente: menú de administración de consola, pfSense.

Figura 4.

Entorno de la página de pfSense en su host.

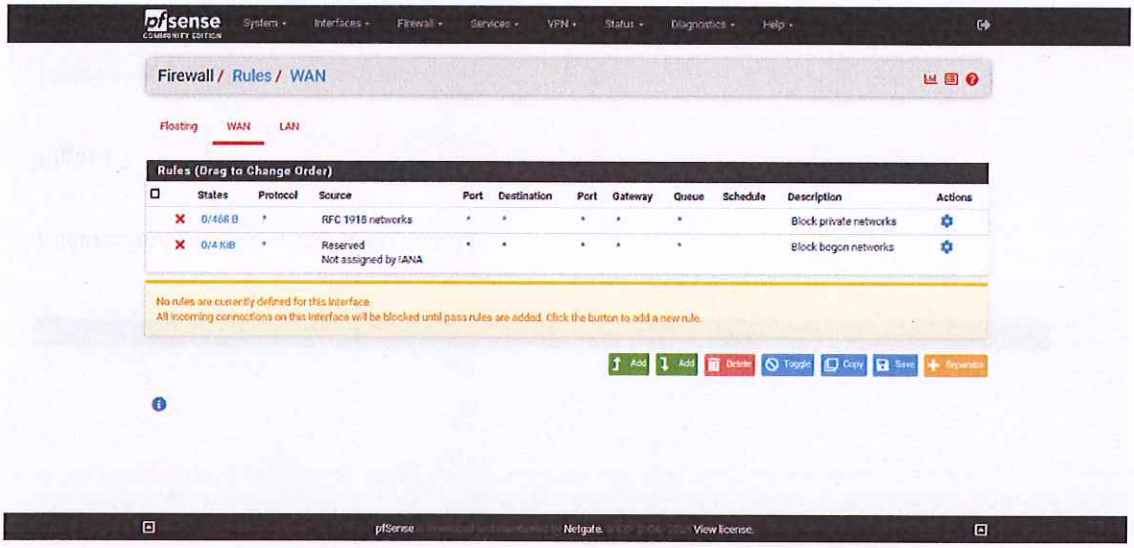


Fuente: Asistente de pfSense.

Configuración de reglas de seguridad para controlar el tráfico de la red.

Figura 5.

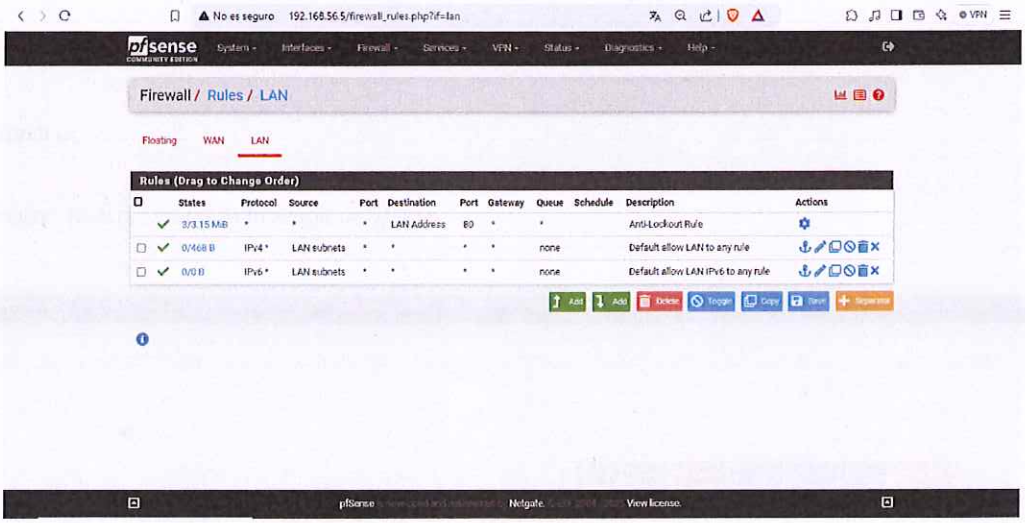
Definición de reglas para WAN-pfSense



Fuente: interfaz de configuración de WAN

Figura 6.

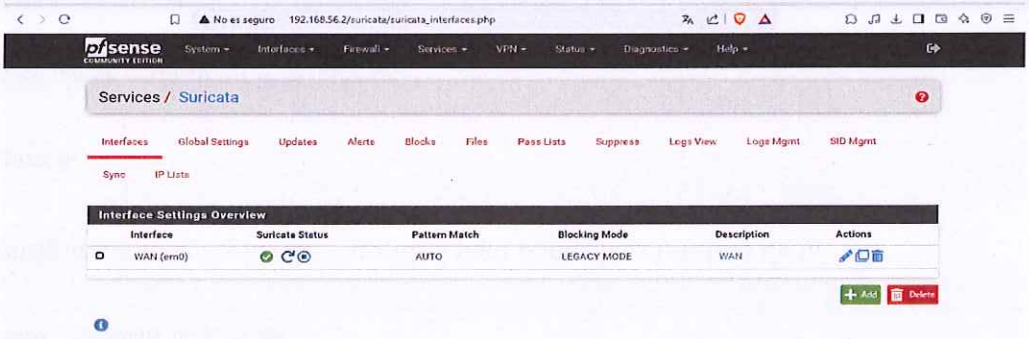
Definición de reglas para LAN-pfSense



Fuente: interfaz de configuración de LAN.

Figura 7.

Instalación de paquetes de suricata.

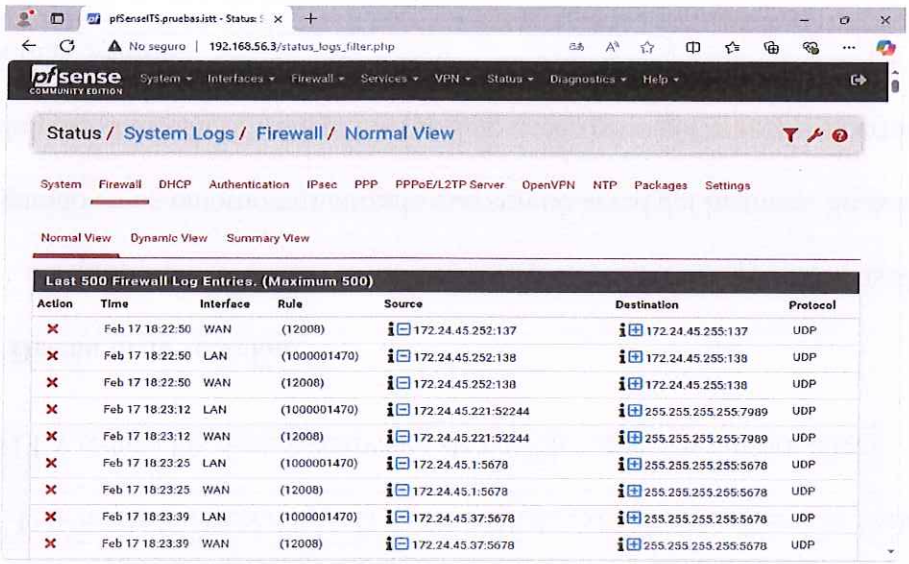


Fuente: system, configuración del servidor web.

Configurar reglas de firewall en **WAN** (para tráfico entrante) y **LAN** (para tráfico saliente).

Figura 8

Simulación de monitoreo en tiempo real



Fuente: Configurar el Dashboard para minitoreo en pfSense

Figura 9

Habilitar monitoreo con pftop

```
pfTop: Up State 1-22/48, View: default, Order: none, Cache: 10000      16:07:45

PR    D SRC                 DEST                STATE   AGE   EXP  PKTS BYTES
icmp  O 172.24.45.22:13895  172.24.45.1:13895     0:0    429    10  1627 47183
tcp   I 192.168.56.7:51629  172.172.255.217:443   4:4    373 86274    26  8872
tcp   O 172.24.45.22:47765  172.172.255.217:443   4:4    373 86274    26  8872
tcp   I 192.168.56.7:51636  172.172.255.217:443   4:4    316 86331    27  8324
tcp   O 172.24.45.22:39740  172.172.255.217:443   4:4    316 86331    27  8324
tcp   I 192.168.56.7:51707  57.144.115.32:5222    4:4    120 86394  1523  881K
tcp   O 172.24.45.22:41150  57.144.115.32:5222    4:4    120 86394  1523  881K
tcp   I 192.168.56.7:51718  52.111.225.21:443     9:9     72    23    51 14433
tcp   O 172.24.45.22:24660  52.111.225.21:443     9:9     72    23    51 14433
tcp   I 192.168.56.7:51719  8.8.4.4:443          10:10    72    18     6  2048
tcp   O 172.24.45.22:14984  8.8.4.4:443          10:10    72    18     6  2048
tcp   I 192.168.56.7:51720  8.8.4.4:443          10:10    72    18     6  2080
tcp   O 172.24.45.22:60810  8.8.4.4:443          10:10    72    18     6  2080
tcp   I 192.168.56.7:51721  163.70.152.60:443     9:9     70    23    68 35098
tcp   O 172.24.45.22:33553  163.70.152.60:443     9:9     70    23    68 35098
tcp   I 192.168.56.7:51722  57.144.115.32:443     9:9     68    23   125   98K
tcp   O 172.24.45.22:38664  57.144.115.32:443     9:9     68    23   125   98K
tcp   I 192.168.56.7:51723  186.42.108.32:443     9:9     68    23   341  311K
tcp   O 172.24.45.22:56298  186.42.108.32:443     9:9     68    23   341  311K
tcp   I 192.168.56.7:51724  92.122.157.135:443   10:10    66    20    18  7209
tcp   O 172.24.45.22:63317  92.122.157.135:443   10:10    66    20    18  7209
tcp   I 192.168.56.7:51725  57.144.115.32:443     9:9     65    20    15  5497
```

Fuente: Ejecutar comando pftop en terminal de pfSense

Simulación de monitoreo en tiempo real y pruebas de efectividad frente a intentos de acceso no autorizados.

PROPUESTA

1.19 Levantamiento de información:

Con los datos obtenidos, se determinan los requisitos técnicos del firewall, incluyendo las reglas de filtrado, el control de accesos y los sistemas de monitoreo que garantizarán una gestión eficiente del tráfico en la red. Asimismo, se identifican los recursos tecnológicos disponibles.

Llevar a cabo un levantamiento de información detallado no solo facilita la configuración adecuada del firewall, sino que también contribuye a su efectividad a largo plazo. Una implementación basada en un análisis exhaustivo refuerza la seguridad de la red del ISTT y reduce los riesgos derivados de posibles amenazas informáticas.

1.20 Diseño de la solución

La propuesta consiste en la implementación de un firewall basado en pfSense, configurado en un entorno virtualizado que simule la red del Instituto. Se definirán reglas de filtrado para controlar el tráfico, bloqueando accesos no autorizados y permitiendo sólo las conexiones seguras.

1.21 Control de Tráfico y Políticas de Seguridad en Redes

Este principio se basa en la gestión eficiente del tráfico de red, asegurando que solo el tráfico autorizado pueda ingresar o salir del sistema, protegiendo así la integridad, disponibilidad y confidencialidad de los datos.

1.22 Aplicación en el Diseño de la Solución con pfSense

1.22.1 Importancia en el Diseño de la Solución

El control de tráfico y políticas de seguridad garantiza que la red del Instituto Superior Tecnológico Tena esté protegida contra amenazas internas y externas, manteniendo la estabilidad y seguridad de los servicios académicos y administrativos.

1.23 Estrategias de solución

Para abordar la problemática de seguridad en la red del Instituto Superior Tecnológico Tena, se propone una estrategia de solución basada en la implementación de un firewall utilizando herramientas open source, con un enfoque en la protección, monitoreo y optimización del tráfico de datos.

Un concepto clave en la estrategia de solución es el Enfoque de Seguridad Perimetral en Redes.

Enfoque de Seguridad Perimetral en Redes

Este enfoque se basa en la implementación de un sistema de defensa en el punto de entrada y salida de la red para controlar y filtrar el tráfico, protegiendo los activos internos del instituto contra amenazas externas e internas.

1.24 Recopilación de mejores prácticas para implementar un firewall en entornos educativos

1.24.1 2. Definir una política de seguridad clara

- Establecer reglas para controlar el tráfico entrante y saliente.
- Bloquear accesos no autorizados y limitar el uso de recursos según perfiles (estudiantes, docentes, administración).
- Aplicar el principio de menor privilegio: solo permitir tráfico necesario.

1.24.2 3. Filtrado de Contenido Web y Aplicaciones

- Implementar Squid Proxy con SquidGuard para:
- Bloquear sitios web inadecuados (pornografía, violencia, malware).
- Restringir redes sociales en horario de clases.
- Utilizar OpenDNS o pfBlockerNG en pfSense para control de DNS.

1.24.3 4. Control y Priorización del Ancho de Banda

Implementar Traffic Shaping en pfSense para:

- Priorizar tráfico educativo (Google Classroom, Moodle, Zoom).
- Limitar descargas de torrents o streaming no educativo.
- Usar Limiters para asignar ancho de banda por usuario o VLAN.

1.24.4 5. Protección contra Ataques y Monitoreo

- Habilitar IPS/IDS (Suricata o Snort) para detectar intrusiones.
- Activar pfBlockerNG para bloquear IPs maliciosas.

- Registrar intentos de acceso no autorizado en System Logs → Firewall.
- Usar ntopng o Darkstat para monitoreo gráfico del tráfico.

1.24.5 6. Acceso Seguro para Administración y VPN

- Deshabilitar administración remota desde WAN.
- Usar VPN (OpenVPN o WireGuard) para accesos remotos seguros.
- Implementar autenticación de dos factores (2FA) en accesos administrativos.

1.25 Importancia en la Estrategia de Solución

El Enfoque de Seguridad Perimetral es crucial en la estrategia de implementación del firewall, ya que refuerza la protección del Instituto Superior Tecnológico Tena, asegurando que solo el tráfico autorizado pueda acceder a la red y que las amenazas sean bloqueadas antes de comprometer los sistemas internos.

CONCLUSIONES

La implementación de un firewall open source permite mejorar significativamente la seguridad de la red del Instituto.

La configuración de reglas de filtrado contribuye a minimizar los riesgos de accesos no autorizados y ataques cibernéticos.

La documentación del proceso y el manual de usuario facilitan la administración del firewall pfSense.

RECOMENDACIONES

Capacitar a estudiantes sobre temas de seguridad de red, para adquirir más conocimientos que ayuden a la comunidad académica.

Implementar un monitoreo continuo del sistema para detectar y mitigar amenazas de manera oportuna.

Evaluar periódicamente las configuraciones de seguridad y realizar ajustes según las necesidades de la institución.

REFERENCIAS BIBLIOGRÁFICA

FreeBSD Foundation. (2023). *pfSense: A powerful open source firewall solution.* Recuperado de https://www.pfsense.org

Garfinkel, S., & Spafford, G. (2020). *Web Security, Privacy & Commerce*. O'Reilly Media.

Gil, J., & Zambrano, A. (2022). *Diseño e implementación de entornos virtuales para redes educativas*. Revista Técnica de Redes, 15(2), 65-78.

Misa, T. J., & Stone, A. (2021). *Open Source Security in Education*: Frameworks and Applications. Academic Press.

NIST. (2020). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).* Recuperado de https://www.nist.gov

Ruiz Andino, E. F. (2022). Evaluación del Firewall de Frontera Free Pfsense para proteger la confidencialidad, integridad y disponibilidad de la información de compañías de responsabilidad limitada en Riobamba año 2021.

PfSense Documentation Team. (2023). *pfSense Official Documentation*. Recuperado de https://docs.netgate.com/pfsense

Lema, F. S., Tutillo, J., Espinosa, L., & Grijalva, R. (2023). ANÁLISIS DE VULNERABILIDADES CON KALI LINUX EN DISPOSITIVOS ANDROID. *Revista de Ciencias de Seguridad y Defensa*, *8*(02), 12-12.

Suricata Development Team. (2023). *Suricata Documentation*. Recuperado de https://suricata.io/docs

Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer Networks (6th ed.)*. Pearson Education.

Angamarca Peña, K. E. (2023). Estudio comparativo de herramientas de procesamiento de Lenguaje Natural Open Source y Software propietario para el desarrollo de aplicaciones basadas en inteligencia artificial (Bachelor's thesis, Babahoyo: UTB-FAFI. 2023).

Chillagana, J., Gualotuña, K. G. S., & Pilataxi, J. A. S. (2023). Diseño y Despliegue de una Infraestructura de Red WAN/LAN/WLAN con Seguridad a través de FortiGate en GNS3. *Revista de Ciencias de Seguridad y Defensa*, *8*(03), 9-9.

Postigo Palacios, A. (2020). *Seguridad informática (Edición 2020)*. Ediciones Paraninfo, SA.

Garcia Vega, J. K., & Andi Cerda, B. J. (2021). IMPLEMENTACIÓN DE UN SERVIDOR CACHÉ WEB COMO MEDIDA DE SOLUCIÓN AL ALTO CONSUMO DE ANCHO DE BANDA DE INTERNET EN EL INSTITUTO SUPERIOR TECNOLÓGICO TENA (Doctoral dissertation).

Caicedo Veintimilla, A. T. (2022). *Herramientas firewall basadas en tecnologías OpenSource* (Bachelor's thesis, Babahoyo: UTB-FAFI. 2022).

ANEXOS

Anexo 1: Solicitud de autorización de acceso al servidor físico, para colocar un disco solido SSD de 2tb.

REPÚBLICA DEL ECUADOR

INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo

Secretaría de Educación Superior, Ciencia, Tecnología e Innovación

Oficio N° ISTT-R-2025-091-OF
Tena, 10 de febrero de 2025

Señor
Carchi Cerda Jair Orlando
ESTUDIANTE DEL IST TENA

Señor
Yumbo Grefa Jhony Brian
ESTUDIANTE DEL IST TENA
Presente

De mi consideración:

Con un cordial saludo y en atención al documento s/n, de fecha 03 de febrero del 2025, que en su parte pertinente manifiesta: (...) nos encontramos en el proceso de titulación con el tema: "*Implementación de un firewall utilizando herramientas open source para el Instituto superior Tecnológico Tena2; por ende nos dirigimos respetuosamente para solicitar se AUTORICE* a quien corresponda el acceso al servidor fisico que se encuentra ubicado en vicerrectorado para colocar un disco solido SSD de 2 tb (...)

Por lo expuesto, se autoriza la colocación del disco sólido SSD de 2tb; para lo cual solicito muy comedidamente, coordinar la actividad con el Ing. Salomón Quilumba, Responsable de la Unidad de Tecnologías de la Información.

Con sentimiento de distinguida consideración.

Atentamente,

LORENA PILAR YÁNEZ PALACIOS

MEd. Lorena Pilar Yánez Palacios, Ing.
RECTORA DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA

c.c.: Ing. Diego Rojas, VICERRECTOR
Ing. Salomón Quilumba, RESPONSABLE DE LA UNIDAD DE TICS

Punto de Atención al Usuario: km 1 ½ vía Tena – Archidona
Teléfono: 062311709
secretaria.general@itstena.edu.ec
https://www.itstena.edu.ec

EL NUEVO ECUADOR

Anexo 2: Respuesta de la solicitud para mover el servidor al área de comunicación.

REPÚBLICA DEL ECUADOR

INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo

Secretaría de Educación Superior, Ciencia, Tecnología e Innovación

Oficio Nº ISTT-R-2025-095-OF
Tena, 12 de febrero de 2025

Señor
Carchi Cerda Jair Orlando
ESTUDIANTE DEL ISTE TENA

Señor
Yumbo Grefa Jhony Brian
ESTUDIANTE DEL IST TENA
Presente. –

De mi consideración:

Con un cordial saludo y en atención al documento s/n, de fecha 12 de febrero de 2025, que en su parte pertinente manifiesta: *(...) se AUTORICE a quien corresponda el mover el servidor físico que se encuentra ubicado en vicerrectorado con la finalidad de instalar un disco solido SSD de 2 tb, ya que en su lugar no hay espacio para realizar dicha actividad y será movido al área de comunicación (...)*

Por lo expuesto, informo a usted que se autoriza realizar dicha actividad; para lo cual solicito gentilmente coordinar con el Ing. Salomón Quilumba, RESPONSABLE DE LA UNIDAD DE TICS y con la Lic. Verónica Zuña, GESTORA DE LA UNIDAD DE COMUNICACIÓN.

Con sentimiento de distinguida consideración.

Atentamente,

LORENA PILAR YÁNEZ PALACIOS

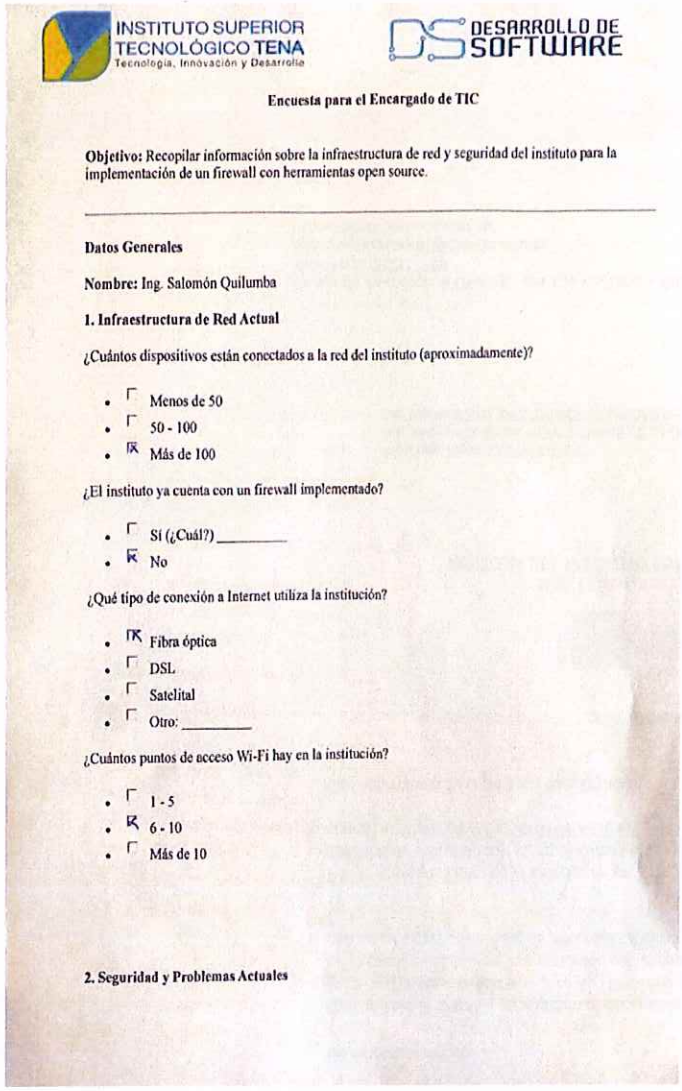
MEd. Lorena Pilar Yánez Palacios, Ing.
RECTORA DEL INSTITUTO SUPERIOR TECNOLÓGICO TENA

c.c.: Ing. Diego Rojas, VICERRECTOR
Ing. Salomón Quilumba, RESPONSABLE DE LA UNIDAD DE TICS
Lic. Verónica Zuña, GESTORA DE LA UNIDAD DE COMUNICACIÓN.

Punto de Atención al Usuario: km 1 ½ vía Tena – Archidona
Teléfono: 062311709
secretaria.general@itstena.edu.ec
https://www.itstena.edu.ec

EL NUEVO ECUADOR

Anexo 3: Entrevista al responsable de la Unidad de Tecnologías de la Información.



INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo

DESARROLLO DE SOFTWARE

Encuesta para el Encargado de TIC

Objetivo: Recopilar información sobre la infraestructura de red y seguridad del instituto para la implementación de un firewall con herramientas open source.

Datos Generales

Nombre: Ing. Salomón Quilumba

1. Infraestructura de Red Actual

¿Cuántos dispositivos están conectados a la red del instituto (aproximadamente)?

- ☐ Menos de 50
- ☐ 50 - 100
- ☒ Más de 100

¿El instituto ya cuenta con un firewall implementado?

- ☐ Sí (¿Cuál?)_____
- ☒ No

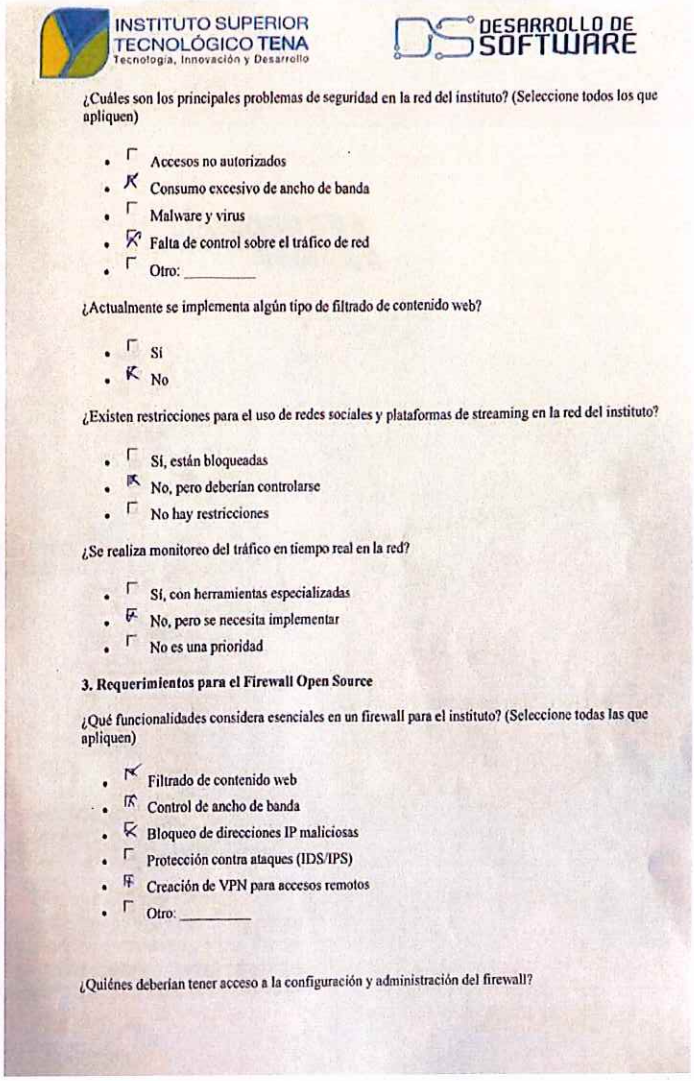
¿Qué tipo de conexión a Internet utiliza la institución?

- ☒ Fibra óptica
- ☐ DSL
- ☐ Satelital
- ☐ Otro: _____

¿Cuántos puntos de acceso Wi-Fi hay en la institución?

- ☐ 1 - 5
- ☒ 6 - 10
- ☐ Más de 10

2. Seguridad y Problemas Actuales



INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo

DESARROLLO DE SOFTWARE

¿Cuáles son los principales problemas de seguridad en la red del instituto? (Seleccione todos los que apliquen)

- ☐ Accesos no autorizados
- ☒ Consumo excesivo de ancho de banda
- ☐ Malware y virus
- ☒ Falta de control sobre el tráfico de red
- ☐ Otro: _____

¿Actualmente se implementa algún tipo de filtrado de contenido web?

- ☐ Sí
- ☒ No

¿Existen restricciones para el uso de redes sociales y plataformas de streaming en la red del instituto?

- ☐ Sí, están bloqueadas
- ☒ No, pero deberían controlarse
- ☐ No hay restricciones

¿Se realiza monitoreo del tráfico en tiempo real en la red?

- ☐ Sí, con herramientas especializadas
- ☒ No, pero se necesita implementar
- ☐ No es una prioridad

3. Requerimientos para el Firewall Open Source

¿Qué funcionalidades considera esenciales en un firewall para el instituto? (Seleccione todas las que apliquen)

- ☒ Filtrado de contenido web
- ☒ Control de ancho de banda
- ☒ Bloqueo de direcciones IP maliciosas
- ☐ Protección contra ataques (IDS/IPS)
- ☒ Creación de VPN para accesos remotos
- ☐ Otro: _____

¿Quiénes deberían tener acceso a la configuración y administración del firewall?

INSTITUTO SUPERIOR TECNOLÓGICO TENA
Tecnología, Innovación y Desarrollo

DESARROLLO DE SOFTWARE

- ☐ Solo el área de TIC
- ☐ TIC y algunos docentes autorizados
- ☐ TIC y administración

¿El instituto estaría dispuesto a capacitar al personal en el uso del firewall?

- ☐ Sí ?
- ☐ No
- ☐ No es necesario

no depende de la Unidad de TIC

¿Cuál considera que es el mayor desafío en la implementación de un firewall en la institución?

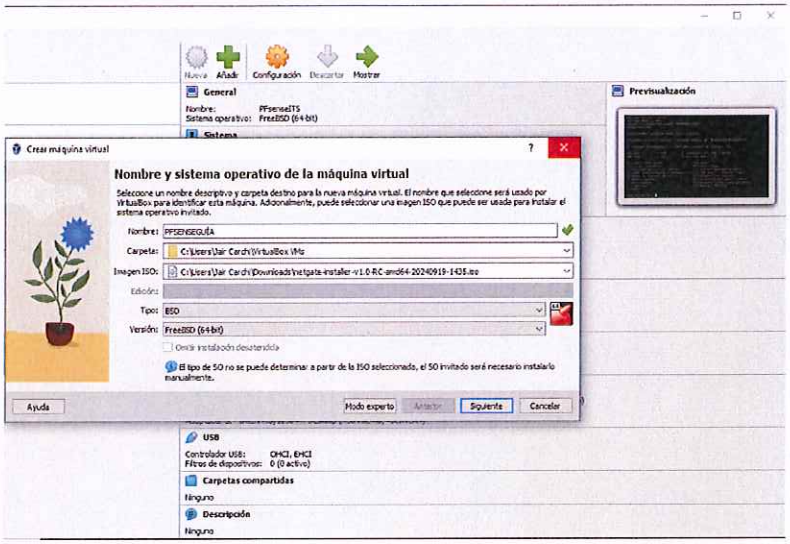
- ☐ Falta de conocimientos técnicos
- ☒ Recursos económicos
- ☐ Compatibilidad con la infraestructura actual
- ☐ Otro: _____

Alguna sugerencia adicional, de acuerdo a la implementación del firewall utilizando herramientas open source:

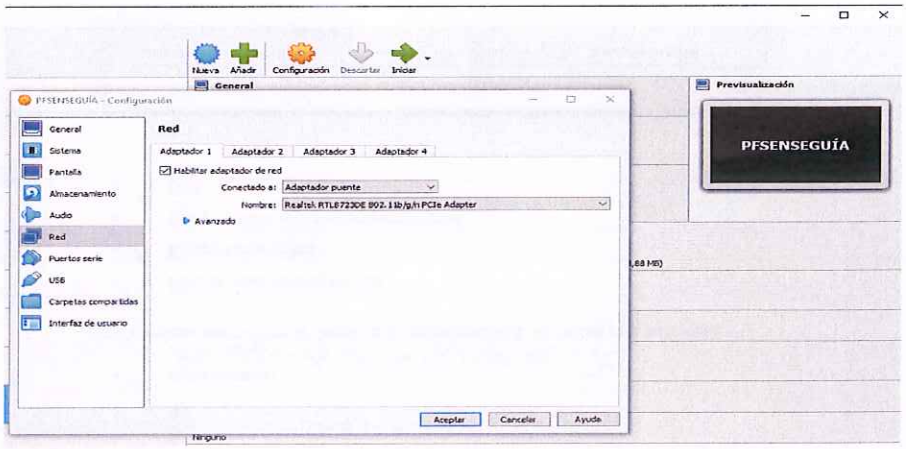
Se requiere control de ancho de banda, filtrado web historial de navegación

Anexo 4: Evidencia de instalación y configuración del firewall en el servidor institucional.

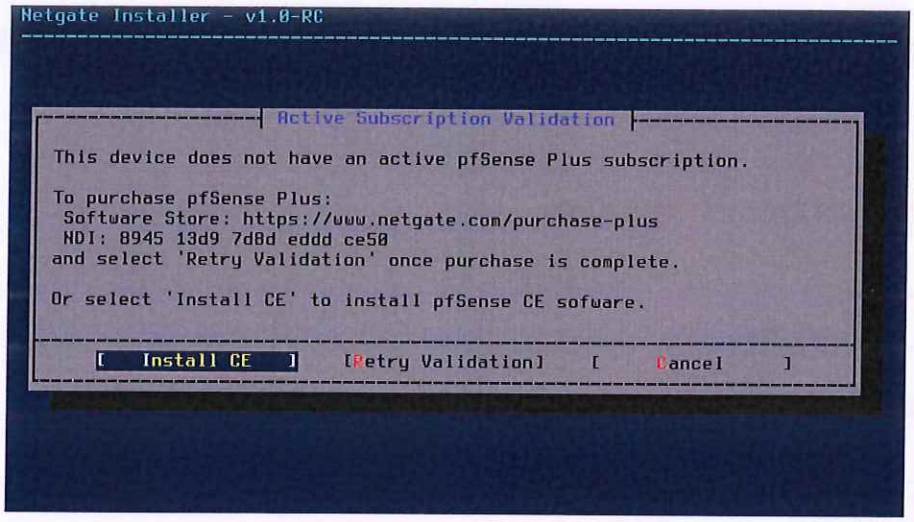
1. **Instalación del pfSense en VirtualBox mediante la imagen ISO, en el servidor físico.**



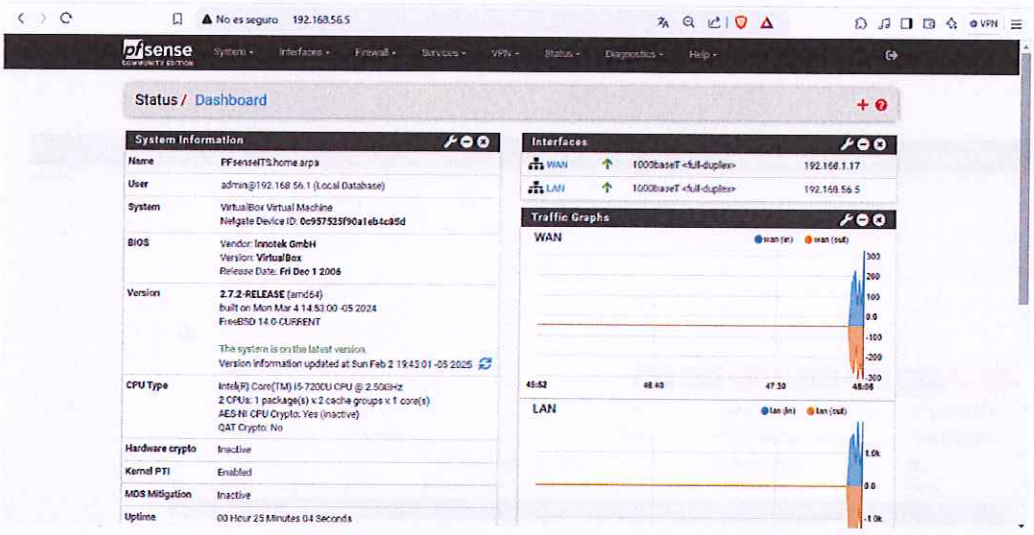
2. **Configuración inicial de la interfaz WAN y LAN durante la instalación**



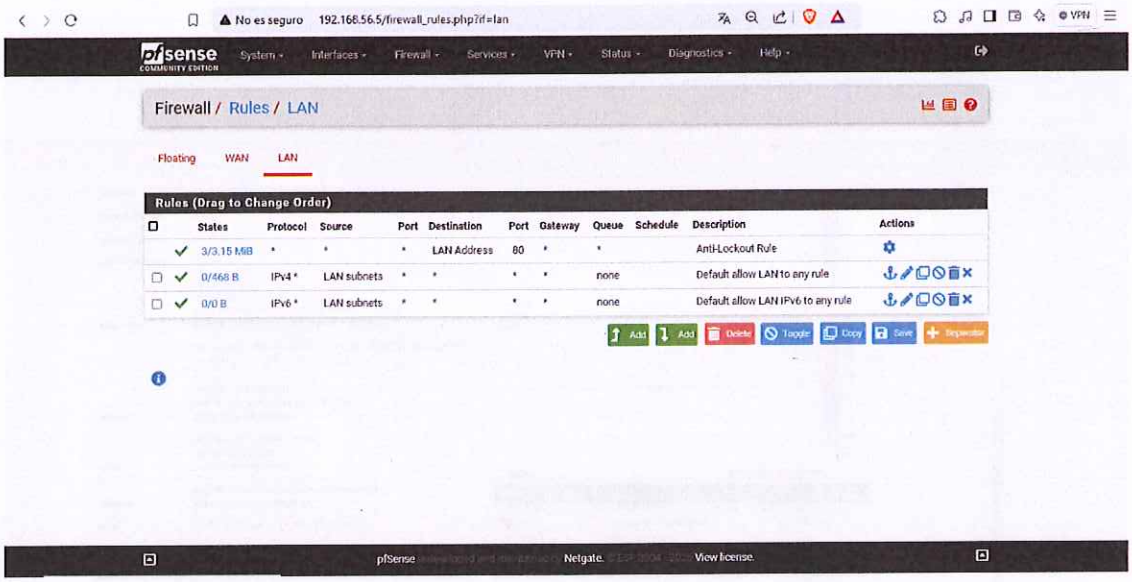
3. **De ahí solo es de aceptar y dar enter en las primeras opciones que aparecen. Aquí damos clic en install CE.**



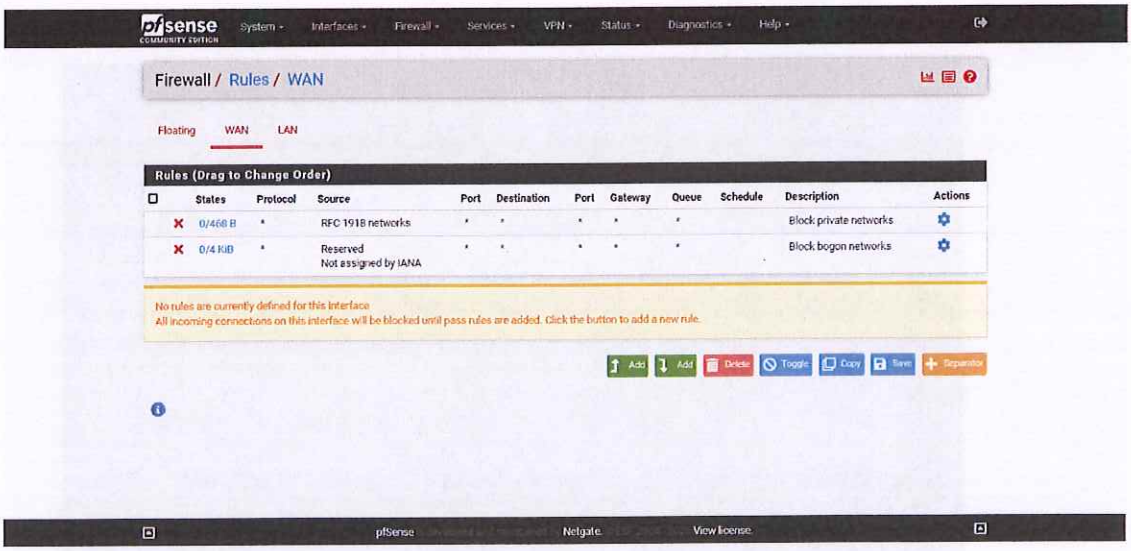
4. **Primer acceso a la interfaz web de la administración del firewall**



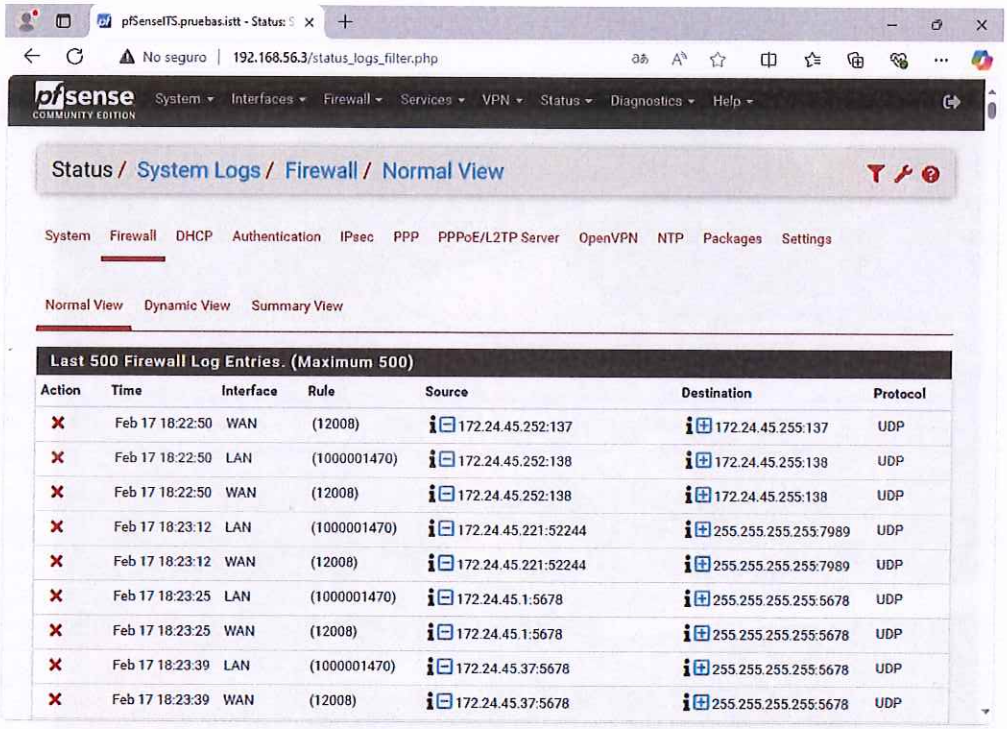
5. **Configuración de reglas de firewall para controlar el tráfico entrante y saliente**



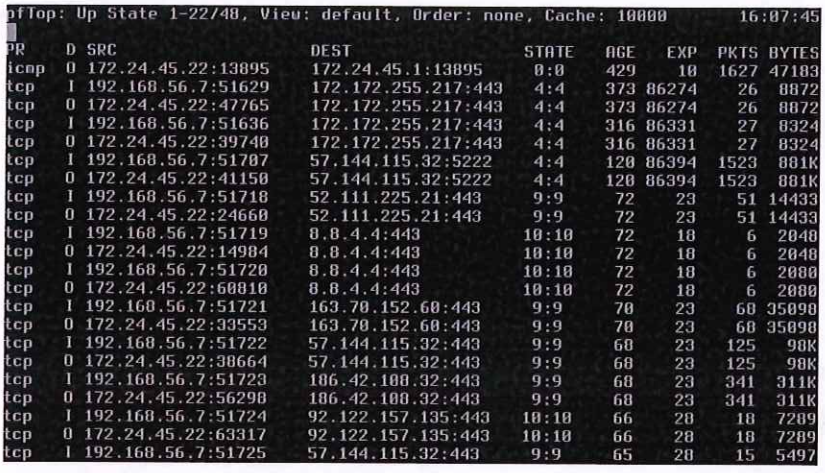
6. **Creación de reglas para bloquear accesos no autorizados y permitir tráfico seguro**



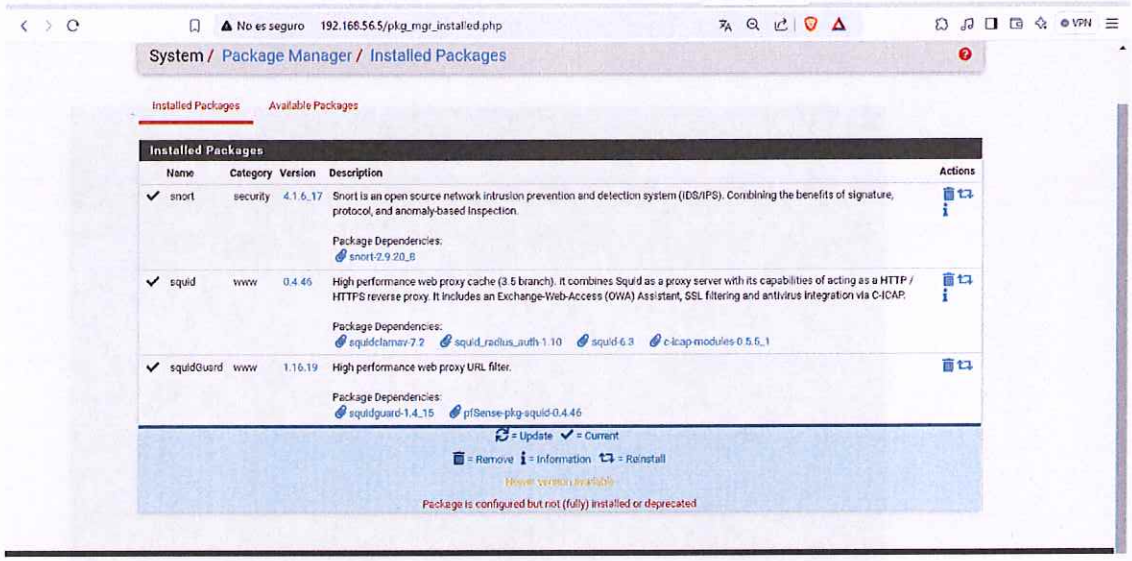
7. **Dashboard del firewall mostrando estado del sistema.**



8. **Logs de tráfico en tiempo real con detención de intentos de accesos sospechosos.**



9. Integración de Snort/Suricata para la detención de intrusos



10. Evidencia de instalación final del pfSense en el servidor físico institucional.