UNIVERSIDAD NACIONAL DEL ALTIPLANO - PUNO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

"DISEÑO E IMPLEMENTACIÓN DE ENTORNOS SEGUROS CON ENCRIPTACIÓN Y POLÍTICAS BASADO EN SOFTWARE LIBRE PARA MEJORAR LA PRODUCTIVIDAD DE TRABAJADORES Y ESTUDIANTES DE LA INSTITUCIÓN EDUCATIVA PRIVADA UNITEK"

TESIS

PRESENTADO POR:

PAUL IVAN REYES CUBA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PUNO – PERU

2017

UNIVERSIDAD NACIONAL DEL ALTIPLANO – PUNO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

""DISEÑO E IMPLEMENTACIÓN DE ENTORNOS SEGUROS CON ENCRIPTACION Y POLÍTICAS BASADO EN SOFTWARE LIBRE PARA MEJORAR LA PRODUCTIVIDAD DE TRABAJADORES Y ESTUDIANTES DE LA INSTITUCIÓN EDUCATIVA PRIVADA UNITEK"

TESIS PRESENTADA POR:

PAUL IVAN REYES CUBA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

APROBADA POR EL JURADO REVISOR CONFORMADO POR:

PRESIDENTE : _____

DR. EUDES RIGOBERTO APAZA ESTAÑO

PRIMER MIEMBRO : _____

ING. CHRISTIAN AUGUSTO ROMERO GOYZUETA

SEGUNDO MIEMBRO : _____

ING. JASMANY RUELAS CHAMBI

DIRECTOR / ASESOR : _____

ING. FERDINAND EDGARDO PINEDA ANCCO

PUNO – PERU

2017

Área: Telecomunicaciones y redes de datos

Tema: Seguridad de Redes.

DEDICATORIA

Esta investigación está dedicada con mucho amor y cariño a mi hijo Alexus Mateo que es el motor más fiel y confiable que puedo encontrar en la vida, a mi esposa que me acompaña día a día y toda mi familia por el constante apoyo que me da.

AGRADECIMIENTOS

Quiero agradecer a toda mi familia, a quienes me acompañan y colaboran siempre, y por todo el apoyo que me brindaron para realizar la presente investigación.

A mis docentes que han colaborado y apoyado de la mejor manera, por su tiempo y disposición a esta investigación.

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE ACRÓNIMOS

10/100/1000: 10 Mbps / 100 Mbps / 1000 Mbps, es la tecnología que puede manejar Ethernet (10 Mbps), Fast Ethernet (100 Mbps) o Gigabit Ethernet (1000 Mbps).

10/100: 10 Mbps / 100 Mbps, es la tecnología que puede manejar Ethernet (10 Mbps) o Fast Ethernet (100 Mbps).

1394: Especificación de la IEEE (Institute of Electrical and Electronics Engineers) que define las características del bus serial FireWire.

2D: Two Dimensions, Dos Dimensiones.

3D: Three Dimensions, Tres Dimensiones.

4X: Four Times, Cuatro Veces.

ADSL: Assymetric Digital Subscriber Line, Línea de Suscripción Asimétrica Digital.

AEPSI: Asociación Española de Proveedores de Servicios de Internet.

AGP: Acelerated (Advanced) Graphics Port.

AI: Asociación de Internautas.

AMD: Advanced Micro Devices.

ANSI: American National Standards Institute.

AOL: America On-Line.

API: Application Programming Interface.

ARPA: Advanced Research Projects Agency.

ASCII: American Standard Code for Information Interchange.

ATA: Interface de conexión estándar.

ATM: Modo de Transferencia Asíncrona.

ATX: AT Extended, AT Extendido.

AUI: Asociación de usuarios de Internet.

AVI: Audio Video Interleaved.

BIOS: Basic Input and Output System.

BIT: Binary Digit, Dígito Binario.

BMP: Bit Map, Mapa de Bits.

CAD: Diseño asistido por ordenador.

CAP: Carrierless Amplitude and Phase Modulation.

CCD: Charge Coupled Device, Dispositivo de Cargas Acopladas.

CD: Compact Disk, Disco Compacto.

CD-R: CD(Compact Disk) Recordable, CD (Disco Compacto) Grabable.

CD-ROM: Compact Disc ROM, Disco Compacto de Lectura.

CD-RW: CD(Compact Disk) Rewritable, CD(Disco Compacto) Reescribible.

CD-W: CD(Compact Disk) Writable, CD(Disco Compacto) Escribible.

CF: Compact Flash, Destello Compacto.

CMOS: Complementary Metal Oxide Conductor, Conductor de Óxido Metálico Complementario.

CMT: Comisión del mercado de las Telecomunicaciones en España.

COM: Component Object Model, Modelo de Componentes de Objetos.

cps: Characters per Second, Caracteres por Segundo.

CPU: Central Processing Unit, Unidad Central de Proceso.

CRC: Cyclic Redundancy Check.

CRT: Cathode Ray Tube, Tubo de Rayos Catódicos.

DC: Direct Current, Corriente Directa(Continua), tipo de corriente eléctrica en la que el voltaje es constante.

DDR DRAM: Double-Data-Rate DRAM DRAM de Doble Velocidad de Datos.

DDR: Double Data Rate, ratio doble de datos.

DHTML: Dynamic HTML, HTML Dinámico.

DIMM: Double In-Line Memory Module, Módulo de Memoria en Línea Apareado.

DIVX: Formato de video con una resolución de 640x480.

DLL: Dynamic Link Library, Librería de Concatenación Dinámica.

DMA: Direct Memory Access, Acceso Directo a la Memoria.

DMCA: Acta de Copyright del Milenio Digital de 1998.

DNS: Domain Name System, Sistema de Nombres de Dominios.

DOS: Disk Operating System, Sistema Operativo de Disco.

dpi: Dots per Inch, Puntos por Pulgada.

DSL: Digital Subscriber Line, Línea de Suscripción Digital.

DV: Formato de video con una resolución de 720x576.

DVD: Digital Video Disk, Disco de Video Digital.

DVD+R DL: DVD Recordable Double Layer.

DVD+RW: Digital Video Disc Rewritable, Disco de Vídeo Digital Reescribible.

DVD-RAM: Digital Video Disk RAM, Disco de Vídeo Digital RAM.

DVD-ROM: Digital Video Disk ROM, Disco de Vídeo Digital ROM.

DVI: Digital Video Interface, conexión digital para tarjetas gráficas.

EDI: Intercambio Electrónico de Datos.

EDO RAM: Extended Data Out RAM, RAM sin Datos Extendidos.

EFF: Fundación de la Frontera Electrónica.

EPROM: Erasable Programmable ROM, Memoria ROM Programable y Borrable.

EthIR: Ethernet Infra Red, Ethernet Infra Rojo.

FAQ: Frequently Asked Questions, Preguntas Realizadas más Frecuentemente.

FAT: File Attribute Table, Tabla de Atributos de los Archivos.

FAT16: File Attribute Table - 16 bits, Tabla de Atributos de los Archivos de 16 bits.

FAT32: File Attribute Table - 32 bits, Tabla de Atributos de los Archivos de 32 bits.

FC (Fibre Channel)

FLOPS: Floting point Operation Per Second, Operación de Punto Flotante por Segundo.

FTP: File Transfer Protocol, Protocolo de Transferencia de Archivos.

Gb: Gigabit 1024 Megabits.

GB: Gigabyte 1024 Megabytes.

GHz: Gigahertz, Gigahertzio 1.000.000.000 de ciclos por segundo.

GIF: Graphical Interchange Format, Formato de Intercambio de Gráficos.

GII: Infraestructura Global de Información.

GPL: GNU Public License.

GPRS: General Packet Radio Services.

GPS: Global Positioning Satellite, Satélite de Posicionamiento Global.

GPU: Graphic Process Unit, Unidad de Procesamiento de Gráficos.

GSM: Sistema Global de Comunicaciones Móviles.

GSP: Government Security Program.

HD: High Density, Alta Densidad.

HDD: Hard Disk Drive, Unidad de Disco Duro.

HR: Alta Resolución.

HTA: Son archivos que pueden ser ejecutados en el inicio del sistema operativo mediante el Windows Scripting Host.

HTML: Hyper Text Markup Language, Lenguaje de Marcado de Hiper Texto.

HTTP: Hyper Text Transfer Protocol, Protocolo de Transferencia de Hiper Texto.

Hz: Hertz, Hertzio (1 ciclo por segundo), es la unidad de medida de frecuencia.

I/O: Input/Output, Entrada/Salida.

IA: Inteligencia Artificial.

IANA: Agencia de Asignación de Números en Internet.

IDE (Integrated Drive Electronics)

IDE: Integrated Drive Electronics, Electrónica Integrada al Drive.

IE: Internet Explorer, Internet Explorer.

IP: Protocolo de Internet.

IRC: Internet Relay Chat, Conversación en Internet.

IRQ: Interrupt Request, Requerimiento de Interrupción.

ISO 9000 Estándar orientado a la calidad total en los procesos.

ISO 9660 Estándar que define sistemas de archivos para CD-ROMs que pueden ser leídos por diversos sistemas operativos.

ISO: International Standards Organization, Organización de Estándares Internacionales.

ISP: Internet Service Provider, Proveedor de Servicios en Internet.

IT: Information Technology, Tecnología de Información.

ITU: Union Internacional de Telecomunicaciones.

JPEG: Joints Photographic Experts Group, Grupo Unido de Expertos en Fotografía.

JVM: Java Virtual Machine, Máquina Virtual de Java.

Kb: KiloBits, Kilobits, son 1024 bits.

KB: KiloBytes, KiloBytes, son 1024 bytes.

Kbps: KiloBits Per Second, Kilobits por segundo.

KHz: Kilohertz, Kilohertzio(1000 ciclos por segundo).

L1: Level 1, Nivel 1, se refiere a la Memoria Caché de Nivel 1.

L2: Level 2, Nivel 2, se refiere a la Memoria Caché de Nivel 2.

LAN: Local Area Network, Red de Área Local.

LCD: Liquid Crystal Display, Pantalla de Cristal Líquido.

LED: Light-Emitting Diode, Diodo Emisor de Luz.

MAPI: Messaging Application Programming Interface, Interfaz de Programación para Aplicaciones de Mensajería.

Mb: Megabits, Megabits, son 1024 Kilobits.

MB: MegaBytes, Megabytes, son 1024 Kilobytes.

Mbps: Megabits per second, Megabits por segundo, son 1024 Kilobits por segundo.

MDI: Multiple Document Interface, Interfaz para Múltiples Documentos.

MFLOPS: Mega FLOPS, Millón de Operaciones de Punto Flotante Por Segundo.

MHz: Megahertz, Megahertzio(1.000.000 ciclos por segundo).

MIDI: Musical Instrument Digital Interface, Interfaz Digital para Instrumento Musical.

MIME: Multipurpose Internet Mail Extensions, Extensiones de Correo Internet Multipropósito.

MMC: Multimedia Card, es una tarjeta de memoria.

MP3: MPEG-1 Layer 3, MPEG-1 Capa 3, es un sistema de compresión de música muy utilizado y con calidad CDs.

MPEG: Moving Pictures Experts Group, Grupo de Expertos en Imágenes en Movimiento.

MPEG-1 Moving Pictures Experts Group 1, Grupo de Expertos en Imágenes en Movimiento 1, Primera versión de MPEG (Moving Pictures Experts Group).

MPEG-2 Moving Pictures Experts Group 2, Grupo de Expertos en Imágenes en Movimiento 2, Segunda versión de MPEG (Moving Pictures Experts Group).

MS: Memory Stick, es una tarjeta de memoria.

MTU: Maximum Transfer Unit. Es el tamaño máximo de los paquetes que enviamos a internet.

N/A: Not Available, No Disponible.

NAP: Network Access Point, Punto de Acceso a la Red.

NAT: Network Address Translation, Traducción de Dirección de Red.

NCSA: Centro Nacional de Aplicaciones de Supercomputación.

NetBEUI: NetBios Extended User Interface, Interfaz de Usuario Extendida de NetBIOS.

NetBIOS: Network Basic Input / Output System, Sistema de Entrada / Salida Básico para Red.

NiCd: Nickel Cadmium, Níquel y Cadmio, Tecnología empleada en la fabricación de baterías de larga duración para equipos portátiles.

Ni-HM: Batería de Niquel Metal Hidruro.

NII: Infraestructura Nacional de Información.

NTFS: NT File System, Sistema de Archivos NT.

OCR: Optical Character Recognition, Reconocimiento Óptico de Caracteres.

OEM: Original Equipament Manufacturer, Fabricante Original de Equipos.

OLE: Object Linking and Embedding, Concatenación y Embebimiento de Objetos.

OLED: Organic Light Emitting Diodes.

OS: Operating System, Sistema Operativo.

PC Card: Personal Computer Card, Tarjeta para Computadora Personal.

PC: Personal Computer, Computadora Personal.

PCI Express: Personal Computer Interface Expres, Interfaz para Computadora Personal.

PCI: Personal Computer Interface, Interfaz para Computadora Personal.

PCMCIA: Personal Computer Memory Card International Association, Asociación Internacional de Tarjetas de Memoria para Computadoras Personales.

PDA: Personal Digital Assistant, Asistente Digital Personal.

PDF: Portable Document Format, Formato de Documento Portátil.

PDM :Product Data Management, Administración de Datos de Productos.

PLC: Power Line Communications, Comunicación por línea eléctrica.

PMPO: Peak Music Power Output.

POP: Post Office Protocol, Protocolo de Oficina de Correos.

ppm: Pages Per Minute, Páginas por Minuto.

ppp: Point-to-Point Protocol, Protocolo Punto a Punto.

PROM: Programmable ROM, Memoria ROM Programable.

PS/2: Puertos desarrollados por IBM para conectar el ratón y el teclado al PC usando un conector Mini Din y que es el estándar en los PC's.

RAID: Redundant Array of Inexpensive Disks, Arreglo Redundante de Discos Económicos.

RAM: Random Access Memory, Memoria de Acceso Aleatorio (Randómico).

RAMBUS: Es la memoria más rápida, pero es muy cara.

RDRAM: Rambus DRAM Memoria, DRAM Rambus.

RDSI: Red Digital de Servicios Integrados.

RFID: Radio Frequency Identification, Tecnología de identificación por radiofrecuencia.

RGB: Red, Green and Blue, Rojo, Verde y Azul.

RMS: Root Mean Square, raiz cuadrada media.

ROM: Read Only Memory, Memoria de Sólo Lectura.

RPM: RedHad Package Manager, es un gestor de las distribuciones Linux basadas en RedHat.

RTB: Red de Telefónica Básica.

RTC: Red Telefónica Conmutada.

S/N: Signal-to-Noise Ratio, Razón entre Señal y Ruido.

S/PDIF: Sony/Philips Digital Interface.

SACD: Super Audio CD.

SATA: Interface de conexión de disco duro más rápida que el estándar ATA.

SCSI (Small Computer System Interface)

SCSI: Small Computer System Interface, Interfaz de Sistema para PC.

SDRAM: Synchronous Dynamic RAM, Memoria RAM Dinámica Sincrónica, es una memoria síncrona de acceso aleatorio, funciona a la par que el procesador adaptándose a su velocidad y se emplea como memoria principal.

SFF: Small Form Factor, Factor de forma reducida, son los mini PC's.

SGML: Lenguaje Estandarizado y Generalizado de Marcado.

SIMM: Single In-Line Memory Module, Módulo de Memoria en Línea Independiente.

SLIP: Lineal Serial IP.

SMTP: Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo (Mail).

SSA (Serial Storage Architecture)

SSL: Secure Socket Layer.

SVCD: Formato de video con una resolución de 480x576.

SVGA: Super Video Graphics Adapter, Adaptador Gráfico de Super Vídeo.

TCP/IP: Transmission Control Protocol / Internet Protocol, Protocolo de Control de Transmisión / Protocolo Internet.

TDT: Televisión Digital Terrestre, es la televisión que sustituirá a la analógica.

TFT-LCD: Thin Film Transistor-Liquid Crystal Display.

UDP: User Datagram Protocol, Protocolo de Datagramas de Usuario.

UMTS: Sistema Universal de Telecomunicaciones Móviles.

URI: Identificador Universal de Recursos.

URL: Uniform Resource Locator, Localizador Universal de Recursos.

USB: Universal Serial Bus, Bus Serial Universal.

V.90: V.90 Standard, Estándar V.90.

VB: Visual Basic.

VCD: Video CD, CD de Vídeo.

VCR: Video Cassette Recorder, Grabadora de Cassettes de Vídeo.

VGA: Video Graphics Adapter, Adaptador Gráfico de Vídeo.

VML: Vector Markup Language, Lenguaje de Marcado de Vectores.

VRAM: Video RAM Memoria, RAM de Vídeo Memoria.

WAN: Wide Area Network, Red de Área Extendida.

WAP: Wireless Application Protocol, Protocolo para Aplicaciones Inalámbricas.

WWW: World Wide Web, Red Mundial de Internet.

XML: Extensible Markup Language, Lenguaje de Marcado Extensible.

ZIP: Extensión de los archivos comprimidos con el compresor WinZip.

INDICE DE ANEXOS

RESUMEN

En esta investigación se desarrolla entornos seguros y políticas, este dispositivo está basado en hardware y software, permite filtrar el acceso a Internet basado en reglas diseñadas e implementadas por el administrador. Este dispositivo logrará permitir el acceso a sitios en Internet que aportan al desarrollo y productividad de los estudiantes y trabajadores de la Institución Educativa Privada Unitek; mientras que bloquea el acceso a sitios que se encuentran en una lista negra, ya que no son deseados, entre ellos están las redes sociales, los videos musicales, entre otras ligadas al entretenimiento. Se plantea una solución sencilla y más barata que otras opciones en el mercado. Se inicia el desarrollo con el planteamiento del problema, para luego llegar a las hipótesis, a los objetivos e identificación de las variables. Se continúa con el marco teórico y conceptual; todo esto justificado en base a los antecedentes de investigación. Finalmente se elabora un cronograma para la correcta organización de las actividades.

Podemos enfocarnos en la Institución Educativa Privada Unitek y centrarnos en la cantidad de estudiantes y trabajadores quienes, al conectarse a internet, no se enfocan al 100 por ciento en sus actividades laborales, normalmente se distraen con diferentes páginas web ajenas a sus responsabilidades, provocando así un déficit del desempeño laboral. El objetivo principal es esta investigación es diseñar e implementar entornos seguros y políticas para mejorar la productividad de los trabajadores y estudiantes de la institución educativa particular UNITEK. Los objetivos específicos son diseñar e Implementar entornos seguros y políticas para el control y administración del acceso a Internet desde la red de área local de la institución educativa particular y también mejorar el rendimiento y seguridad de la red de área local de la institución educativa particular UNITEK.

Palabras clave: Cortafuego, Control de Tráfico, Filtro de Red, Listas de Acceso, Seguridad de redes.

ABSTRACT

In this research is developed Safe environments with encryption and policies, this device is based on hardware and software, allows to filter Internet access based on rules designed and implemented by the administrator. This device allows access to Internet sites that contribute to the development and productivity of students and workers of the Unitek Private Educational Institution; While access to sites that are blacklisted, as they are not desired, among them are social networks, music videos, among others linked to entertainment. It poses a simple and cheaper solution than other options in the market. Development begins with the approach of the problem, to arrive at the hypotheses, the objectives and the identification of the variables. The theoretical and conceptual framework is continued; all justified based on the research background. Finally a schedule for the correct organization of the activities is elaborated.

We can focus on the Private Educational Institution Unitek and focus on the number of students and workers who, when connected to the Internet, do not focus 100% on their work activities, are usually distracted by different web pages outside their responsibilities, thus causing A shortfall in work performance The main objective of this research is to design and implement secure and policy-based environments to improve the productivity of workers and students at the UNITEK private educational institution. The specific objectives are to design and implement secure environments and policies for the control and management of Internet access from the local area network of the particular educational institution and also to improve the performance and security of the local area network of the particular educational institution UNITEK.

Keywords: Cortafuego, Traffic Control, Network Filter, Access Lists, Network Security.

CAPITULO I

INTRODUCCIÓN

La Institución Educativa Particular Unitek no administra, ni controla de manera adecuada el acceso a Internet, los usuarios pueden hacer un mal uso de los recursos de Internet, como usar el acceso para entretenimiento, cuando está prohibido; o usarlo para otro tipo de actividad indebida del ancho de banda, sobre todo el acceso a video y audio que hacen uso significativo del ancho de banda, lo que hace que las máquinas de todos los usuarios en la red local que deseen acceder a Internet tengan una sensación de lentitud al usar el servicio lo que se convierte en una baja de la productividad de los trabajadores y estudiantes, los cuáles experimentan bajos índices de transferencia de datos. Otro ejemplo es el uso de redes sociales que bajan el desempeño de los trabajadores y estudiantes, al mismo tiempo que existen otras desventajas inherentes a ello como los riesgos de seguridad que pueden provocar ataques informáticos, porque un agente externo podría enviar malware o hacer un ataque informático a la institución usando las redes sociales. Cuando los trabajadores y estudiantes tratan de acceder a Internet para hacer una investigación o leer artículos, experimentan un bajo rendimiento, lo que provoca que desistan en su objetivo o tengan que retrasar su trabajo.

PfSense es un completo paquete de software de cortafuegos que, cuando se utiliza junto con hardware adecuado, proporciona todas las características importantes de las cajas de cortafuegos comerciales (incluida la facilidad de uso) a una fracción del precio (software libre). PfSense se basa en una versión reducida y altamente personalizada de FreeBSD, junto con un servidor web LightTPD, PHP y algunas otras utilidades.

La configuración completa del sistema se almacena en un único archivo de texto XML para mantener las cosas transparentes.

PfSense es probablemente el segundo sistema UNIX que tiene su configuración de arranque realizada con PHP, en lugar de los scripts de shell habituales, y para

tener toda la configuración del sistema almacenada en formato XML. El proyecto pfSense se basó en monowall, que fue el primer sistema de este tipo.

PfSense cuenta con un sistema de paquetes que permite ampliar el entorno con nuevas características y funciones.

CAPITULO II

REVISIÓN DE LITERATURA

2.1. CONCEPTOS SOBRE CORTAFUEGO

2.1.1. ¿QUÉ ES UN CORTAFUEGO?

Un cortafuego es una pasarela de Internet segura que se utiliza para interconectar una red privada a Internet. Hay una serie de componentes que conforman un Cortafuego.

- La política de seguridad de acceso a Internet de la organización. Esto indica, en un alto nivel, qué grado de seguridad espera la organización al conectarse a la red Internet. La política de seguridad es independiente de la tecnología y las técnicas, y debe tener toda una vida independiente del equipo utilizado. Un ejemplo de una política de seguridad de este tipo podría ser los usuarios externos en una red corporativa sin un fuerte nivel de autenticación; Cualquier información corporativa que no esté en el dominio público debe ser transferidos a través de Internet de manera confidencial (Crawley, 2010).

- El mapeo de la política de seguridad en diseños y procedimientos técnicos que se deben seguir al conectarse a Internet. Esta información se actualiza a medida que se anuncie la nueva tecnología, y como configuraciones del sistema, por ejemplo, con respecto a la autenticación, el diseño técnico podría especificar el uso de contraseñas de una sola vez. Los diseños técnicos se basan generalmente en una de las dos políticas de seguridad, ya sea, permitir cualquier servicio a menos que se deniegue expresamente, o negar cualquier servicio a menos que esté expresamente permitido.

- El sistema de cortafuegos, que es el hardware y el software que implementa el cortafuego. Los sistemas de cortafuego típicos comprenden un enrutador de filtrado de paquetes IP, y una computadora

(a veces llamada puerta de enlace de aplicación), ejecutando el filtro de aplicaciones y el software de autenticación. Cada uno de estos componentes de cortafuego son esenciales (Colvin, 2015).

Figura 1: Esquema de Cortafuego o cortafuegos.

Fuente: http://revista.seguridad.unam.mx/

2.1.2. VENTAJAS DE LOS CORTAFUEGO

Los cortafuegos tienen una serie de ventajas:

- Pueden detener las solicitudes entrantes a servicios inherentemente inseguros.
- Deshabilitar login o servicios RPC como NFS. Pueden controlar el acceso a otros servicios.
- Barra de llamadas de ciertas direcciones IP.
- Filtrar las operaciones de servicio (entrantes y salientes).
- Permite el acceso a ciertos directorios o Sistemas.
- Son más rentables que asegurar cada host en la red corporativa ya que a menudo sólo uno o unos pocos sistemas de cortafuegos para concentrarse son más seguros que asegurar cada host debido a la complejidad del software en el host, lo que facilita las brechas de seguridad. En contraste, los cortafuegos usualmente tienen sistemas operativos simplificados y no ejecuta aplicaciones complejas.

2.1.3. DESVENTAJAS DE CORTAFUEGOS

Los cortafuegos no son todo y terminan con toda la inseguridad de la red. Tienen algunas desventajas, tales como:

- Son un punto central para el ataque, y si un intruso rompe el Cortafuego pueden tener acceso ilimitado a la red corporativa.
- Pueden restringir el acceso de los usuarios legítimos a servicios, por ejemplo, los usuarios corporativos no pueden salir a la web, o cuando fuera de casa, un usuario corporativo puede no tener pleno acceso a la organización.
- No protegen contra los ataques de puerta trasera, y pueden animar a los usuarios a entrar y salir por la puerta trasera, especialmente si las restricciones de servicio son bastante graves.
- Los sistemas de cortafuego por sí mismos no pueden proteger la red contra el contrabando.
- Juegos como archivos adjuntos a mensajes de correo electrónico. El contrabando podría seguir siendo una fuente importante de infección de virus (Davis, 2016).

2.1.4. MODELOS, CAPAS Y CORTAFUEGOS

OSI usa un modelo de 7 capas para Interconexión de sistemas abiertos.

Su objetivo es controlar el acceso desde una red protegida, teniendo en cuenta que un cortafuego puede colocarse entre dos redes.

En general, un cortafuego se coloca entre un dominio de alta seguridad y un dominio de seguridad inferior. Un sistema de cortafuegos que funciona en las capas 3 y 4 a veces se llama filtro de paquetes, enrutador o un enrutador de rastreo, su propósito es filtrar los paquetes IP y ICMP y Puertos TCP / UDP. El enrutador tendrá varios puertos y podrá enrutar y filtrar los paquetes de acuerdo con las reglas de filtrado. También es posible operar un sistema de cortafuegos en la capa 2 (el nivel de enlace), configurando un puente ethernet para enviar sólo ciertos paquetes, pero esto no es muy común.

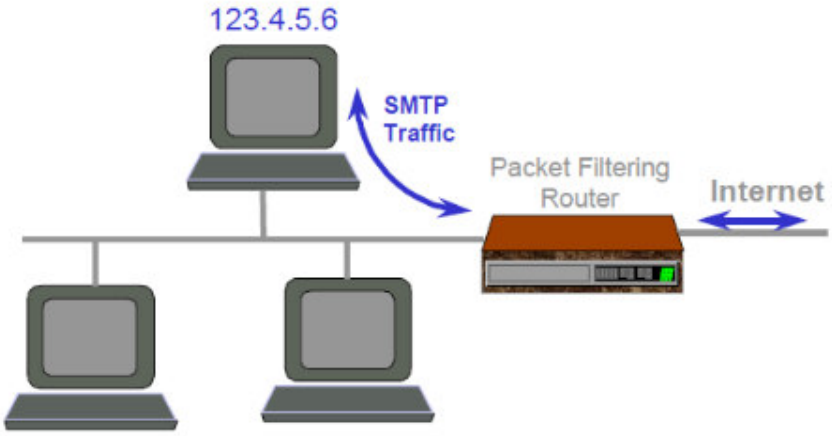


Figura 2: Filtrado de Paquetes

Fuente: IS Institute, University of Salford, Salford, M5 4WT, England.

2.1.5. ROUTER DE FILTRADO DE PAQUETES

Los routers de filtrado de paquetes fueron el primer tipo de cortafuegos que se inventó. Un filtro de paquetes Router debería ser capaz de filtrar paquetes IP basados en los cuatro campos siguientes:

- Dirección IP origen
- Dirección IP de destino
- Puerto de origen TCP / UDP
- Puerto de destino TCP / UDP

El filtrado se utiliza para:

- Bloquear conexiones desde hosts o redes específicos.
- Bloquear conexiones a hosts o redes específicos.
- Bloquear conexiones a puertos específicos.
- Bloquear conexiones desde puertos específicos (Kouka, 2015).

Al configurar un enrutador, generalmente es posible especificar todos los puertos o hosts. Los routers de filtrado de paquetes tienen un rendimiento rápido, ya que los paquetes IP son reenviados o abandonados sin inspeccionar su contenido (excepto la dirección y campos de puerto). Los routers de filtrado de paquetes

son equivalentes a los guardias que preguntan a alguien "De dónde eres y hacia dónde vas".

2.1.5. PROBLEMAS CON LOS ROUTERS DE FILTRADO DE PAQUETES

Los routers de filtrado de paquetes son un componente vital de un sistema de cortafuegos, pero pueden considerarse como una primera línea de defensa, ya que tienen una serie de deficiencias.

- Pueden ser complejos de configurar (el conjunto de reglas puede ser grande, particularmente cuando muchos servicios son compatibles), y no hay una forma automática de comprobar la corrección de las reglas, es decir, que las reglas implementan correctamente la política de seguridad. Además, si el enrutador no admite el registro de llamadas, no hay forma de saber si los paquetes supuestamente no permitidos están consiguiendo realmente acceder a través de un agujero en las normas.
- Si algunos miembros del personal tienen requisitos especiales para el acceso a internet, las reglas pueden tener que ser agregadas para sus máquinas. Esto complica aún más la regla quizás haciéndolo demasiado complejo de manejar.
- Algunos routers básicos no permiten el filtrado TCP / UDP, lo que hace imposible implementar ciertas políticas de seguridad.
- No se puede filtrar entre diferentes protocolos ISO que se ejecutan a través de TCP / IP. RFC 1006 especifica cómo se pueden ejecutar aplicaciones ISO como X.500 y X.400 TCP / IP. Sin embargo, todas las aplicaciones ISO deben conectarse al puerto 102, El RFC 1006 servicio se sienta (Petersen, 2016).
- Los routers de filtrado de paquetes no son muy seguros, ya que los contenidos de los paquetes no son inspeccionados (sólo sus encabezados) así que cualquier cosa se puede pasar a través, como virus, comandos no autorizados de borrado, etc. Finalmente, los remitentes de los paquetes no están autenticados. Con el fin de superar algunas de estas deficiencias, más de los contenidos de los paquetes necesitan ser inspeccionados. Esto llevó a cortafuegos de nivel de aplicación.

2.1.6. INSPECCIONES DE PAQUETES CON ESTADO

Se trata de un módulo de software que se ejecuta en el sistema operativo de una PC Windows o Unix, e inspecciona los paquetes que están llegando. La inspección es impulsada por la seguridad reglas configuradas en la máquina por el oficial de seguridad. Cabeceras de las siete capas del modelo ISO son inspeccionados, y la información sobre los paquetes se introduce en tablas que almacenan información acerca de la conexión. Los datos acumulados en tablas se utilizan entonces para evaluar paquetes subsiguientes en la misma conexión e intentos de conexión subsiguientes. Si bien esta tecnología es más segura que los simples routers de filtrado de paquetes, no es Segura como gateways de aplicaciones, ya que los datos de la capa de aplicación completa no se inspeccionan, sin embargo, funciona más rápido que los proxies de aplicación. La inspección de estado es similar a un guardia de seguridad que pregunta quién eres, a dónde vas y qué llevaras, antes de que te permita entrar en el edificio (Nutter, 2014).

2.1.7. CORTAFUEGOS DE NIVEL DE APLICACIÓN

Se crea un cortafuego de nivel de aplicación mediante la instalación de un ordenador en donde se ejecuta la aplicación apropiada, entre el enrutador de filtrado de paquetes y la intranet.

El enrutador de filtrado de paquetes dirige todas las llamadas desde internet al cortafuego de nivel de aplicación.

Las aplicaciones que se ejecutan en el host no suelen ser versiones de aplicación, sino más bien son servicios proxy simplificados que simplemente filtran el mensaje a nivel de la aplicación, dejando pasar algunos mensajes.

Si el host no ejecuta un servicio de proxy de aplicaciones en particular, la aplicación no suele pasar a través del cortafuego desde internet, en otras palabras, todos los servicios que no se ejecutan en el cortafuego están bloqueados.

Los proxy de aplicación son similares a los de un guardia de seguridad que le pregunta por qué quiere entrar en el edificio y lo que están llevando, y si no le gusta su respuesta él le rechazará la entrada, o puede dirigirle a otra persona, o incluso eliminar algunos de sus artículos antes de dejar pasar, incluso puede tomar cosas tuyas antes de que puedas salir del edificio.

El FTP representa una amenaza para la seguridad, ya que la información confidencial puede ser exportada desde una organización o información falsa, por ejemplo, si la organización tiene información que desea publicar en Internet, el proxy prohibiría el envío de comandos al servidor y directorio FTP.

SMTP plantea una amenaza de seguridad porque los servidores de correo (a menudo el sendmail buggy en sistemas UNIX) se ejecutan con permisos de nivel de sistema para correo entrante a buzones de usuarios. Los hackers pueden iniciar una sesión interactiva con un servidor de correo (escribiendo a mano comandos o escribiendo sus propios programas) y explotar sus privilegios de nivel de sistema. El proxy SMTP que se ejecuta en el cortafuego aísla el correo electrónico entrante del internet, previniendo así a los usuarios de internet interferir directamente con un servidor de correo, el correo entrante se coloca en el host del cortafuego, mediante el programa de correo SMTP de proxy que se ejecuta sin privilegios del sistema, el remitente de correo electrónico se desconecta antes de que cualquier daño pueda ser hecho. Otro proceso recoge el correo del directorio reservado y reenvía al sistema de correo electrónico interno (Odom, 2016).

TELNET permite a los usuarios iniciar sesión en máquinas remotas. Esto puede constituir un riesgo para la seguridad si los usuarios remotos pueden acceder a los ordenadores de la organización con pares de nombre de usuario-contraseña, dadas las debilidades inherentes con sistemas. El proxy Telnet se puede configurar para indicar qué sistemas pueden realizar llamadas y qué sistemas permitirá que se llamen. Una configuración típica será permitir a los usuarios internos llamar a Internet, pero no viceversa.

El proxy HTTP pueden filtrar los distintos comandos como HTTP, POST, PUT y DELETE, así como filtrar las URL.

Además, todos los proxy de aplicación proporcionarán el registro de los paquetes salientes y autenticará a los usuarios.

También queremos asegurarnos de que los datos que se están transfiriendo están libres de virus, por lo tanto, también necesita el filtrado de contenido.

Figura 3: Cortafuego de capa de aplicación

Fuente: http://slideplayer.es/

2.1.8. FILTRADO DE CONTENIDO

Los datos de la aplicación se entregan a un servidor de filtrado de contenido que descomprime los datos para ver lo que hay dentro, y entonces se elimina el contenido dañino (Nathan, 2015).

Por ejemplo, los archivos comprimidos se descomprimen primero para ver lo que hay dentro de ellos, si el contenido contiene un virus que será desechado o desinfectado, (esto requiere que las organizaciones actualicen regularmente sobre su software de verificación de virus, a medida que se encuentran nuevos virus diariamente). Los tipos de archivo se identifican (no de la extensión del nombre de archivo sino de su contenido), y después el archivo puede ser aceptado.

Los archivos de texto se pueden escanear para obtener una lista de palabras clave indeseables (por ejemplo, lenguaje sexual explícito). Finalmente, los applets Java o ActiveX de entrada pueden ser eliminados si se trata de política de la empresa. El filtrado de contenido es como el guardia de seguridad que

vacía sus bolsillos, y le da un cheque de cuerpo completo tanto al entrar y salir de un edificio.

El mayor proveedor de software de control de contenido es Checkpoint con su MIMEsweeper, familia de productos que incluyen MAILsweeper y WEBsweeper).

El mayor problema con el escaneo y filtrado de todos los contenidos del paquete a medida que pasan través del cortafuego, es la cantidad de tiempo de procesamiento que esto toma, en consecuencia, se necesitan servidores grandes para que todos los datos entrantes se muestren.

2.1.9. AUTENTICACIÓN

Ya se ha señalado que no se puede confiar en contraseñas simples para proporcionar información de autenticación a través de internet, se necesita algo más fuerte, el lugar lógico para ubicar la funcionalidad de autenticación fuerte está en el cortafuego, un método de autenticación cada vez más común es el uso de contraseñas únicas (Marshall, 2015).

El cortafuego también puede calcular el mensaje y comparar esto con el descifrado, si ambos paquetes son los mismos, el mensaje es auténtico (debe haber venido del propietario de la clave privada y sin haberse manipulado durante la transferencia).

La autenticación SOCKS fue uno de los primeros mecanismos generales de autenticación colocado en un cortafuego, que permite que las aplicaciones remotas sean autenticadas en el cortafuego.

Radius es el estándar de Internet para marcar en la autenticación de usuarios a un cortafuego.

2.2. PROCESO DE ENCAPSULAMIENTO Y EN DONDE ACTÚA UN CORTAFUEGO

Es un proceso que se encargar de reunir o agrupar datos con sus protocolos correspondientes, esto se hace con la finalidad de que los datos a enviar lleguen correctamente a su destino. La información que se envía a través de una red son datos o paquetes de datos. Si un host quiere enviar datos a otro

Host lo primero que debe de hacer es empaquetarse los datos a través de un proceso de encapsulamiento.

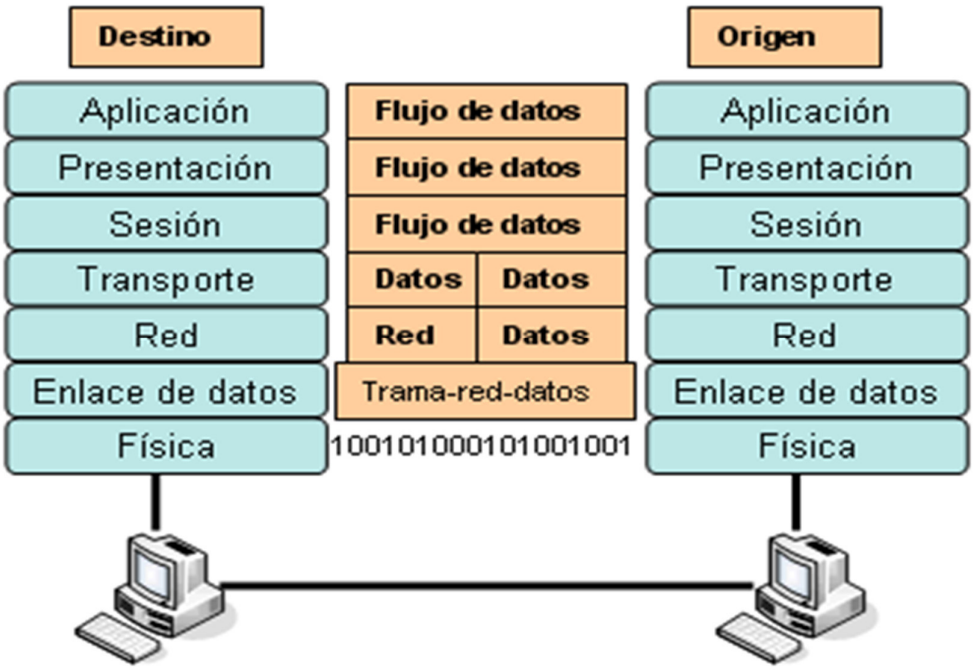


Figura 4: Proceso de encapsulamiento

Fuente: http://maxonlineblog.blogspot.pe/

Las redes deben realizar los siguientes cinco pasos a fin de encapsular los datos:

- Paso 1: Creación de datos, es cuando un usuario envía un mensaje de correo electrónico, sus caracteres alfanuméricos se formatean para convertirlos en datos que puedan reconocer la red.
- Paso 2: Empaquetar los datos, para ser transportados de extremo a extremo, los datos se empaquetan para ser transportados por la internetwork. Al utilizar segmentos, las funciones de transporte aseguran que los hosts que están en ambos extremos del sistema de comunicación (por ejemplo, brindando un servicio de correo electrónico) se puedan comunicar de forma confiable.
- Paso 3: Agregar la dirección de red IP al encabezado, los datos se colocan en un paquete o datagrama que contiene un encabezado de paquete con las direcciones lógicas de origen y destino.

- Paso 4: Agregar el encabezado y la información final de la capa de enlace de datos, cada dispositivo de la red debe de poner el paquete dentro de una trama, la trama permite conectarse al próximo dispositivo de red conectado directamente en el enlace.
- Paso 5: Realizar la conversión a bits para su transmisión, la trama debe de convertirse en un patrón de unos y ceros (bits) para su transmisión a través del medio. Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio (sincronización).

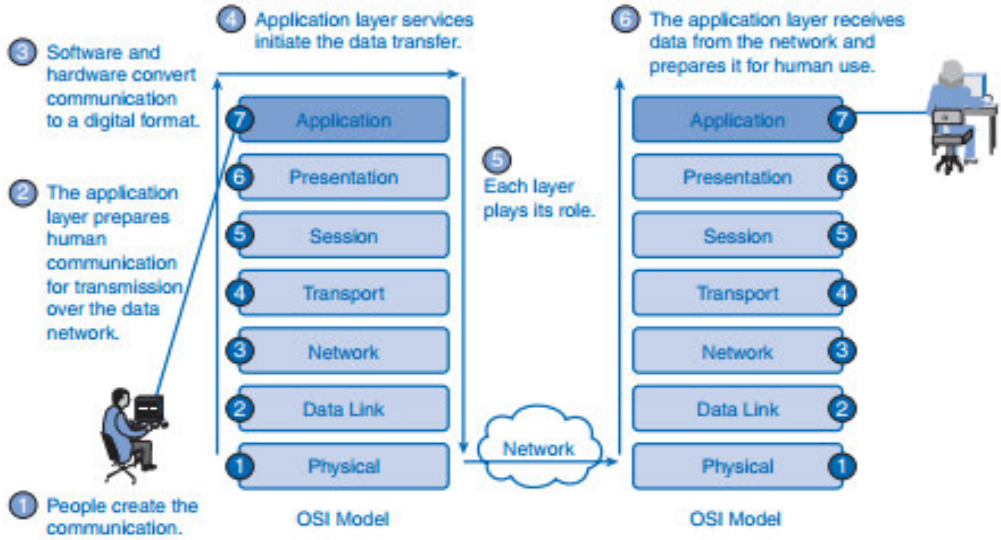


Figura 5: Unidad de paquetes de datos.

Fuente: http://revista.seguridad.unam.mx/

El modelo de interconexión de sistemas abiertos (OSI) es una herramienta de referencia para entender las comunicaciones de datos entre dos sistemas en red. Divide los procesos de comunicación en siete capas, Cada capa realiza funciones específicas para soportar las capas por encima de ella y ofrece servicios a las capas inferiores. Las tres capas más bajas se centran en pasar el tráfico a través de la red a un sistema final (Lammle, 2013)

Este modelo de funcionalidad en capas también se denomina "suit de protocolos" o "conjunto de protocolos". Los protocolos o reglas pueden hacer su trabajo en hardware o software. La naturaleza de estas suit es que las capas inferiores hacen su trabajo en hardware o firmware (Software que se ejecuta en chips de

hardware específicos) mientras que las capas superiores trabajan en software. El modelo de interconexión de sistemas abiertos es una estructura de siete capas que especifica los requisitos para las comunicaciones entre dos ordenadores. La norma ISO (Organización Internacional de Normalización) 7498-1 Definió este modelo. Este modelo permite que todos los elementos de la red funcionen juntos, independientemente de protocolos y qué proveedor de equipo los soporta. Los principales beneficios del modelo OSI son los siguientes:

- Ayuda a los usuarios a comprender el panorama general de las redes.
- Ayuda a los usuarios a entender cómo funcionan los elementos de hardware y software.
- Facilita la solución de problemas al separar las redes en partes manejables.
- Define términos que los profesionales de redes pueden utilizar para comparar relaciones funcionales básicas en redes.
- Ayuda a los usuarios a entender las nuevas tecnologías a medida que se desarrollan.
- Ayuda a interpretar las explicaciones de los proveedores sobre la funcionalidad del producto.

2.2.1. MODELO OSI Y TCP / IP

El modelo de referencia OSI es una representación abstracta en capas creada como una guía para la red diseño e instrucción del protocolo. El modelo OSI divide el proceso de siete capas lógicas, cada una de las cuales tiene una funcionalidad única, ya que se le asignan servicios y protocolos. En el modelo OSI, la información se pasa de una capa a la siguiente, comenzando en la capa de aplicación y proceder hacia la capa física según la jerarquía, pasando a través del canal de comunicaciones al host de destino, donde la información prosigue, terminando nuevamente en la capa de aplicación en el host de destino. A continuación, se explican los seis pasos:

- La gente crea la comunicación
- La capa de aplicación prepara la comunicación humana para la transmisión a través de los datos red.

- El software y el hardware convierten la comunicación a un formato digital.
- Los servicios de capa de aplicación inician la transferencia de datos.
- Cada capa desempeña su papel. Las capas OSI encapsulan datos. Los datos viajan a través de los medios hasta el destino.
- La capa de aplicación recibe datos de la red y los prepara para uso humano.

2.2.2. CAPA DE APLICACIÓN

La capa 7, la capa de aplicación proporciona una interfaz para el usuario final que opera un dispositivo conectado a una red. Esta capa es lo que el usuario ve, en términos de cargar una aplicación (como un navegador Web o un correo electrónico), es decir, Esta capa de aplicación son los datos que el usuario ve al utilizar estas aplicaciones. Ejemplos de funcionalidad de la capa de aplicación incluyen:

- Soporte para transferencias de archivos.
- Capacidad de imprimir en una red.
- Correo electrónico.
- Mensajería electrónica.
- Navegación por la World Wide Web

Los datos son creados por el usuario, al llegar a la capa de aplicación, esta coloca una cabecera, en la cual se indica simplemente a qué tipo de aplicación pertenece los datos que creo el usuario, el PDU (Protocol Data Unit) de la capa de aplicación es Application Protocol Data Unit (APDU) y el objeto es llamado datos.

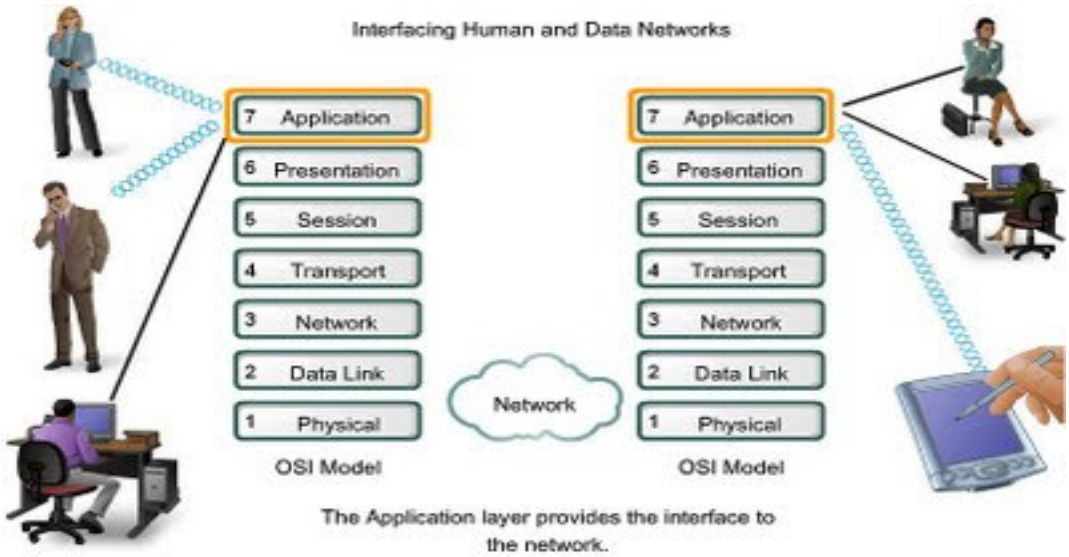


Figura 6: Capa de aplicación.

Fuente: http://dis.um.es/

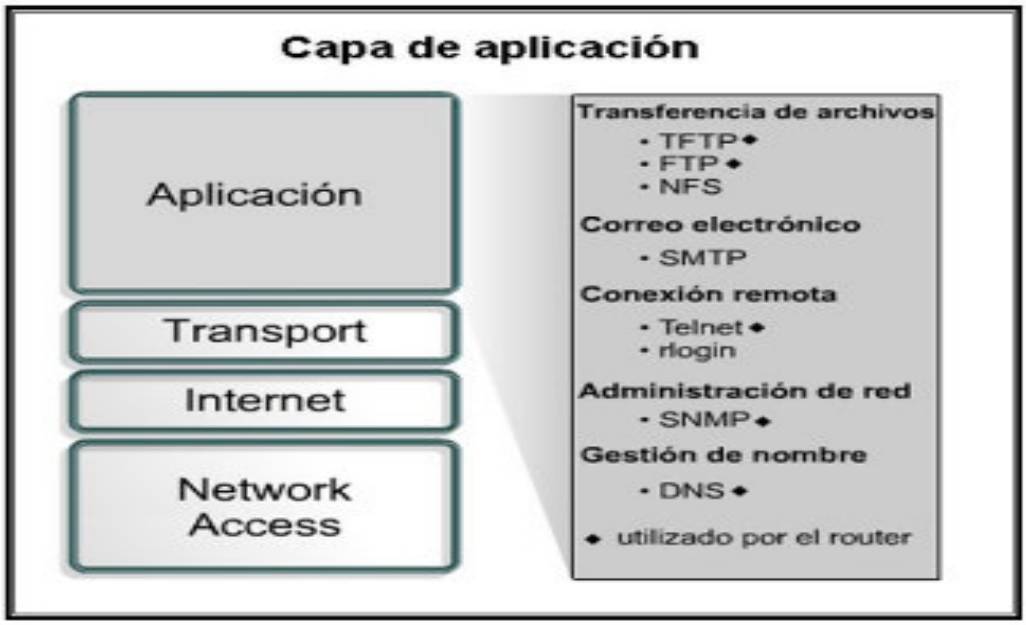


Figura 7: Algunos protocolos de la capa de aplicación.

Fuente: http://slideplayer.es/

2.2.3. CAPA DE PRESENTACIÓN

La capa 6, la capa de presentación es responsable de cómo una aplicación formatea los datos que se enviarán a la red. La capa de presentación básicamente permite que una aplicación lea (o entienda) el mensaje. Ejemplos de funcionalidad de capa de presentación incluyen:

- Cifrado y descifrado de un mensaje para seguridad.
- Compresión y expansión de un mensaje para que se desplace eficientemente.
- Formato de gráficos.
- Traducción de contenido.
- Traducción específica del sistema

En la capa de presentación además de la cabecera de aplicación, se añade una nueva cabecera que se encarga de la sintaxis y el formato de los datos que contiene los datos creados por el usuario, el PDU de la capa de presentación es PPDU (Physical layer conversion Protocol Data Unit) y el objeto con el que trabaja es llamado datos.

Figura 8: Capa de presentación.

Fuente: http://slideplayer.es/

2.2.4. CAPA DE SESIÓN

La capa 5, la capa de sesión proporciona varios servicios, incluyendo el seguimiento del número de bytes que cada extremo de la sesión ha reconocido recibir desde el otro extremo de la sesión. Esta capa de sesión permite que las aplicaciones que funcionan en los dispositivos establezcan, administren y terminen una sesión. Funciones que incluyen la capa de sesión son:

- Conexión virtual entre entidades de aplicación.

- Sincronización de flujo de datos.
- Creación de unidades de diálogo.
- Negociaciones de parámetros de conexión.
- Particionamiento de servicios en grupos funcionales.
- Reconocimientos de datos recibidos durante una sesión.
- Retransmisión de datos si no es recibido por un dispositivo.

En la capa de sesión se añade una nueva cabecera, que está orientada en mantener, iniciar, o terminar la conexión entre los hosts, el PDU de esta capa es SPDU (Session protocol data unit) y el objeto con el que trabaja son datos (Santana, 2013).

Figura 9: Capa de sesión.

Fuente: http://es.slideshare.net/

Figura 10: Funcionamiento de la capa de sesión.

Fuente: http://es.slideshare.net/

2.2.5. CAPA DE TRANSPORTE

La capa 4, la capa de transporte del modelo OSI, ofrece comunicación de extremo a extremo entre dispositivos finales a través de una red, dependiendo de la aplicación, la capa de transporte ofrece una conexión confiable.

Algunas de las funciones ofrecidas por la capa de transporte incluyen:

- Identificación de la solicitud
- Identificación de entidades del lado del cliente
- Confirmación de que todo el mensaje llegó intacto
- Segmentación de datos para el transporte de la red
- Control del flujo de datos para evitar sobrecargas de memoria
- Establecimiento y mantenimiento de los dos extremos de los circuitos virtuales
- Detección de errores de transmisión
- Realineación de datos segmentados en el orden correcto en el lado receptor
- Multiplexar o compartir varias sesiones a través de un único enlace físico

Los protocolos de capa de transporte más comunes son: TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

La capa de transporte aumenta otra información a partir de otra cabecera, esta capa se encarga de que los hosts de ambos extremos del sistema de comunicación se puedan comunicar de manera confiable, el PDU de esta capa es llamado segmento (Ward, 2014).

Figura 11: Capa de transporte.

Fuente: http://tecnologiakomando883.blogspot.pe/

Figura 12: Protocolos de la capa de transporte.

Fuente: http://es.slideshare.net/

2.2.6. CAPA DE RED

La capa 3, la capa de red del modelo OSI, proporciona un sistema de direccionamiento lógico de extremo a extremo de modo que unos paquetes de datos se pueden enrutar a través de varias redes de capa 2 (Ethernet, Token Ring, Frame Relay, etc.).

Inicialmente, los fabricantes de software, como Novell, desarrollaron un tratamiento propietario de capa 3. Sin embargo, la red la industria ha evolucionado hasta el punto de que requiere un sistema de direccionamiento de capa 3 común. La Internet, las direcciones de protocolo (IP) facilitan las redes para establecer y conectarse entre sí.

Los usos de protocolo de internet (IP) son para proporcionar conectividad a millones de redes en todo el mundo.

Para facilitar la administración de la red y controlar el flujo de paquetes, muchas organizaciones separan sus capas de red en pequeñas partes conocidas como subredes. Los enrutadores utilizan la parte de red o subred del direccionamiento IP para encaminar tráfico entre diferentes redes. Cada enrutador debe configurarse específicamente para las redes o subredes que se conectarán a sus interfaces (LaCroix, 2016).

Los enrutadores se comunican entre sí mediante protocolos de enrutamiento, como RIP (Protocolo de información de enrutamiento) y la versión abierta de la ruta más corta primero (OSPF), para aprender de otras redes que están presentes y para calcular la mejor manera de llegar a cada red basada en una variedad de criterios (como el camino con el menor número de routers).

Los enrutadores y otros sistemas en red toman estas decisiones de enrutamiento en la capa de red.

Al pasar paquetes entre diferentes redes, puede ser necesario ajustar su tamaño de salida a uno que es compatible con el protocolo de capa 2 que se está utilizando. La capa de red realiza esto a través de un proceso conocido como fragmentación. La capa de red de un enrutador suele ser responsable de la fragmentación. Todo el reensamblaje de paquetes fragmentados ocurre en la capa de red del sistema de destino final.

Dos de las funciones adicionales de la capa de red son el diagnóstico y la notificación de variaciones lógicas en funcionamiento normal de la red. Mientras que el diagnóstico de la capa de red puede ser iniciado por cualquier sistema en red, el sistema que descubre la variación lo reporta al remitente original del paquete que se encuentra fuera de lo normal.

Funcionamiento de la red; si el cálculo realizado por el sistema receptor, no coincide con el valor enviado por el sistema de origen, el receptor descarta el paquete relacionado sin Informe al remitente. La retransmisión se deja al protocolo de una capa superior.

También se puede configurar una funcionalidad de seguridad básica mediante el filtrado de tráfico mediante el direccionamiento de capa 3 en routers u otros

dispositivos similares. En la capa de red se coloca paquetes de datagrama que contiene un encabezado de paquete con las direcciones lógicas de origen y de destino estas direcciones ayudaran a que el paquete encuentre la mejor ruta hacia su destino, el PDU de la capa de red es llamado segmento.

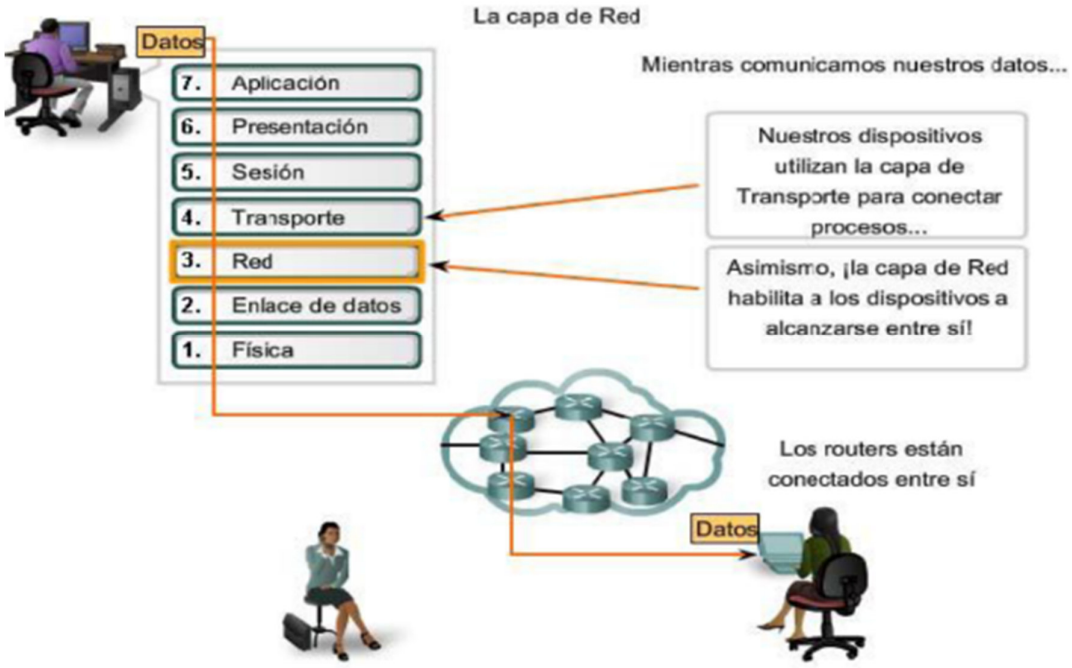


Figura 13: Capa de red.

Fuente: https://docs.google.com.

Figura 14: Protocolos de la capa de red.

Fuente: http://www.dituyi.net/

2.2.7. CAPA ENLACE DE DATOS

La capa 2 del modelo OSI proporciona las siguientes funciones:

- Permite que un dispositivo acceda a la red para enviar y recibir mensajes.
- Ofrece una dirección física para que los datos de un dispositivo puedan ser enviados a la red.

- Funciona con el software de red de un dispositivo al enviar y recibir mensajes.
- Proporciona capacidad de detección de errores.
- Los componentes comunes de red que funcionan en la capa 2 incluyen:

  •Tarjetas de interfaz de red

  •Conmutadores Ethernet

  •Puentes

Las NIC tienen dirección MAC, un switch utiliza esta dirección para filtrar y reenviar el tráfico, ayudando a aliviar la congestión y colisiones en un segmento de red.

La capa de enlace de datos tiene como función entramar, colocar los datos en una trama, cada dispositivo en la ruta de red seleccionada requiere de entramado para poder conectarse con el siguiente dispositivo, por lo que la función de esta capa es imprescindible. El PDU de la capa de enlace de datos es llamado trama (Ghori, 2015).

2.2.8. CAPA FÍSICA

La capa física del modelo OSI define especificaciones de conector e interfaz, así como el medio (cable). Se proporcionan especificaciones eléctricas, mecánicas, funcionales y de procedimiento para enviar un flujo de bits en una red informática.

La capa física se encarga de convertir las tramas en bits para ser transportada por el medio de comunicación que se esté usando. El PDU de la capa física es llamado bit.

Figura 15: Adaptador de red Ethernet Gigabit.

Fuente: http://telnetron.com

Figura 16: Protocolos de la capa de acceso a la red.

Fuente: http://es.slideshare.net/

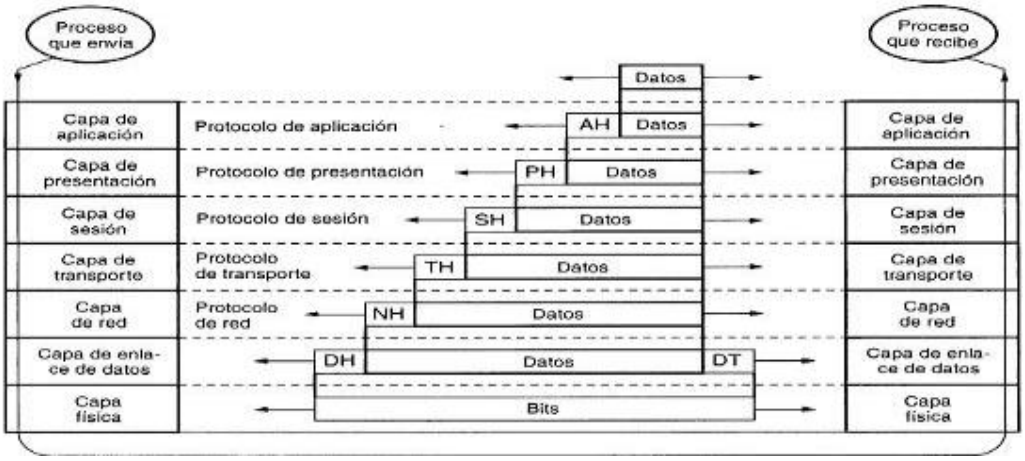


Figura 17: Encabezado de las capas del modelo OSI.

Fuente: http://www.poliredes.galeon.com/

2.3. QUE ES PFSENSE

PfSense es un cortafuego, y el propósito de un cortafuego es proporcionar seguridad. Cuanta más funcionalidad se agregue, mayor será la probabilidad de que una vulnerabilidad en esa funcionalidad adicional comprometa la seguridad del cortafuego. Es la opinión de los fundadores de pfSense y colaboradores principales que cualquier cosa fuera de los servicios básicos de un cortafuego de capas 2 a 4 no pertenece al sistema base de pfSense. Los servicios pueden extenderse a través del gestor de paquetes, pero el operador debe tener cuidado al decidir cuándo, dónde y cómo implementar estos servicios. En muchos casos, una máquina separada desplegada junto con el cortafuego principal serviría mejor para mantener la máxima seguridad.

PfSense es una distribución de software de cortafuego / router de red de código abierto que se basa en el sistema operativo FreeBSD. El software pfSense se utiliza para crear cortafuego / router dedicado a una red y se considera por su fiabilidad, y ofrece muchas características que se encuentran principalmente en cortafuegos comerciales. PfSense se puede incluir con muchos paquetes de software libre de terceros para una funcionalidad adicional (Rankin, 2013).

Los cortafuegos populares en la industria hoy en día son: Cisco ASA, Watchguard, Juniper, Sonicwall, Netgear, y tantos más. Podemos utilizar el software pfSense sin costo alguno y no tiene ninguna licencia. Tiene interfaz web rica que le permite configurar todos nuestros componentes de red. PfSense tiene herramientas de diagnóstico para ayudar con la solución de problemas de red.

2.3.1. REQUERIMIENTOS DE HARDWARE

- Procesador Intel Pentium III, hasta un Intel Xeon.
- Memoria RAM desde 256 Mb hasta 3 Gb.
- Disco Duro de 2 Gb hasta 80 Gb, IDE, SCSI, SATA Y SAS-SATA.4.
- Tarjetas de red cableadas Intel y Realtek (las redes inalámbricas solamente funcionan las tarjetas de red marca Atheros).
- 5. Debido a que este software será instalado sobre un servidor o PC dedicado-única y exclusivamente, este PC o servidor no necesitará un

mouse, solo un teclado y monitor ya que este servidor podrá ser administrado remotamente

2.3.2. COMO FUNCIONA

El software pfSense incluye una interfaz web para la configuración de todos los componentes incluidos. No hay necesidad de ningún conocimiento de UNIX, no hay necesidad de usar la línea de comandos para nada, y no hay necesidad de editar manualmente ningún conjunto de reglas.

Los usuarios familiarizados con los cortafuegos comerciales se conectan rápidamente a la Interfaz web, aunque puede haber una curva de aprendizaje para los usuarios que no estén familiarizados con los cortafuegos comerciales.

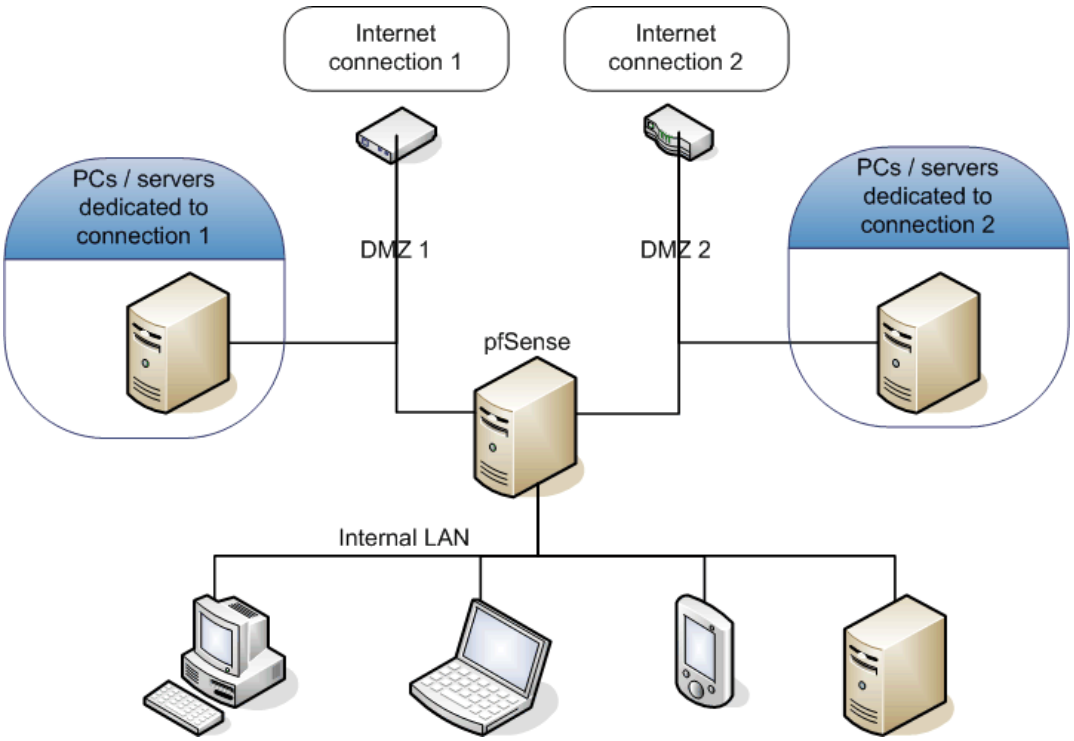


Figura 18: Funcionamiento de PfSense.

Fuente: http://www.cstonline.com.ar/

2.3.3. BSD

BSD (originalmente: Berkeley Software Distribution) se refiere a la versión particular del sistema operativo UNIX que fue desarrollada y distribuida por la Universidad de California en Berkeley. Normalmente, "BSD" está precedido por un número que indica el nivel de distribución particular del sistema BSD (por ejemplo, "4.3 BSD"). BSD UNIX ha sido popular y muchas implementaciones comerciales de sistemas UNIX se basan en o incluyen algún código BSD.

2.4. FUNCIONES DE PFSENSE

2.4.1. COMO CORTAFUEGO

- Filtrado por origen y destino IP, protocolo IP, origen y puerto de destino para el tráfico TCP y UDP
- Limitar las conexiones simultáneas por regla
- Soporte inalámbrico (punto de acceso o BSS / IBSS con dependiendo de la tarjeta y el controlador) pfsense.
- El software pfSense utiliza p0f, una utilidad pasiva avanzada de OS / network fingerprinting que le permite filtrar el sistema operativo iniciando la conexión. ¿Quiere permitir que las máquinas FreeBSD y Linux se conecten a Internet, pero bloquean las máquinas Windows? El software pfSense permite eso (entre muchas otras posibilidades) mediante la detección pasiva del Sistema Operativo en uso.
- Opción para registrar o no registrar el tráfico que coincide con cada regla.
- Ruteo de directivas muy flexible, seleccionando la puerta de enlace por regla (para balanceo de carga, conmutación por error, WAN múltiple, etc.)
- Los alias permiten agrupar y nombrar IPs, redes y puertos. Esto ayuda a mantener su conjunto de reglas de cortafuego limpio y fácil de entender, especialmente en entornos con múltiples IPs públicas y numerosos servidores.
- Filtrado de paquetes de estado
- Bloquear / pasar reglas
- Túneles VPN IPsec (IKE, con soporte para tarjetas de cifrado de hardware)

- NAT + soporte IPsec para enmascarar redes tunelizadas de fase 2
- Soporte IPsec móvil que utiliza autenticación respaldada por xauth y local, RADIUS o LDAP
- OpenVPN para instalación de sitio a sitio o acceso remoto
- Acceso remoto OpenVPN también admite la autenticación de respaldo local, RADIUS o LDAP
- PPTP VPN (con soporte de servidor RADIUS)
- Rutas estáticas
- Enrutador DNS de caché
- Cliente DynDNS
- Agente SNMP
- Formador de tráfico
- Actualización de firmware a través del navegador web o consola
- Copia de seguridad / restauración de la configuración
- Host, red y alias de puerto
- Failover activo / pasivo de alta disponibilidad utilizando CARP
- Portal cautivo
- Balanceo de carga multi-WAN (saliente)
- Equilibrio de carga del servidor (entrante)
- Servidor NTP
- Servidor PPPoE (con soporte de servidor RADIUS)
- Universal Plug-n-Play (UPnP, NAT-PMP)
- Activación de la LAN
- Transparente en capa 2, cortafuego capaz de puentear las interfaces y filtrar el tráfico entre ellos, incluso permitiendo un cortafuego IP menos (aunque es probable que desee un IP para fines de gestión).
- La directiva scrub también reorganiza los paquetes fragmentados, protegiendo algunos sistemas operativos de algunas formas de paquetes.
- Descarta paquetes TCP que tienen combinaciones de indicadores no válidos. "
- Habilitado en el software pfSense por defecto
- Puede deshabilitar si es necesario. Esta opción causa problemas para algunas implementaciones NFS, pero es segura y debe dejarse habilitada en la mayoría de las instalaciones.

- Deshabilitar filtro: puede apagar el filtro de cortafuego por completo si desea convertir su software pfSense en un enrutador puro.

2.4.2. ESTATE TABLE

- La tabla de estado del CORTAFUEGO mantiene información sobre las conexiones de red abiertas. El software pfSense es un cortafuego con estado, por defecto todas las reglas son stateful.
- La mayoría de los cortafuegos carecen de la capacidad de controlar finamente su tabla de estado. El software pfSense tiene numerosas características que permiten el control granular de su tabla de estado.
- Tamaño de tabla de estado ajustable - hay varias instalaciones de producción pfSense utilizando varios cientos de miles de estados. El tamaño de tabla de estado predeterminado varía de acuerdo con la RAM instalada en el sistema, pero se puede aumentar de forma instantánea al tamaño deseado. Cada estado toma aproximadamente 1 KB de RAM, así que tenga en cuenta el uso de memoria al dimensionar su tabla de estado. No poner arbitrariamente alto (Ferguson, 2016).

Por regla:

- Limitar las conexiones simultáneas del cliente
- Estados límite por host
- Limitar nuevas conexiones por segundo
- Definir el tiempo de espera del estado
- Definir tipo de estado
- Tipos de estado: el software pfSense ofrece múltiples opciones para el manejo del estado.
- Keep state - Funciona con todos los protocolos. Predeterminado para todas las reglas.
- Sloppy state - Funciona con todos los protocolos. Seguimiento de estado menos estricto, útil en casos de enrutamiento asimétrico.
- Estado de Synproxy: Proxies las conexiones TCP entrantes para ayudar a proteger los servidores de las inundaciones de TCP SYN falsificadas.

Esta opción incluye la funcionalidad de mantener el estado y modular el estado combinado.

- No guardar ninguna entrada de estado para este tráfico. Esto es muy rara vez deseable, pero está disponible porque puede ser útil en algunas circunstancias limitadas.

Opciones de optimización de tablas de estado, pf ofrece cuatro opciones para la optimización de tablas de estado.

- Normal: el algoritmo predeterminado
- Alta latencia - Útil para enlaces de alta latencia, como conexiones por satélite. Vence las conexiones inactivas más tarde de lo normal.
- Agresivo: expira las conexiones inactivas más rápidamente. Uso más eficiente de los recursos de hardware, pero puede eliminar las conexiones legítimas.
- Conservador - Intenta evitar caer las conexiones legítimas a expensas del aumento en el uso de la memoria y de la CPU.

2.4.3. TRADUCCIÓN DE DIRECCIONES DE RED (NAT)

- Port Forward incluyendo rangos y el uso de múltiples IPs públicos
- NAT 1: 1 para IPs individuales o subredes enteras.
- NAT de salida
- En varios escenarios de WAN, la configuración predeterminada define el tráfico de salida de NAT hacia la IP de la interfaz WAN que se está utilizando.
- Advanced Outbound: NAT permite desactivar este comportamiento predeterminado y permite la creación de reglas NAT muy flexibles.
- Reflexión NAT - La reflexión NAT es posible para que los servicios puedan ser accedidos por IP pública desde redes internas.
- Limitaciones: Limitación de PPTP / GRE. El código de seguimiento de estado en pf para el protocolo GRE sólo puede rastrear una sola sesión por IP pública por servidor externo. Esto significa que, si utiliza conexiones PPTP VPN, sólo una máquina interna puede conectarse simultáneamente a un servidor PPTP en Internet. Un millar de máquinas puede conectarse

simultáneamente a un millar de servidores PPTP diferentes, pero sólo uno simultáneamente a un solo servidor.

- El único trabajo disponible es utilizar varios IPs públicos en su cortafuego, uno por cliente o utilizar múltiples IPs públicas en el servidor PPTP externo. Esto no es un problema con otros tipos de conexiones VPN. PPTP es inseguro y ya no debe utilizarse.

2.4.4. ALTA DISPONIBILIDAD

- La combinación de CARP, pfsync y nuestra sincronización de configuración proporciona una funcionalidad de alta disponibilidad. Se pueden configurar dos o más cortafuegos como un grupo de conmutación por error. Si una interfaz falla en la primaria o la primaria se desconecta completamente, la secundaria se activa. El software pfSense también incluye capacidades de sincronización de configuración, por lo que realiza los cambios de configuración en la primaria y se sincronizan automáticamente con el cortafuego secundario.
- La tabla de estado del servidor de seguridad se replica a todos los cortafuegos configurados para conmutación por error. Esto significa que las conexiones existentes se mantendrán en caso de fallo, lo cual es importante para evitar interrupciones en la red.

2.4.5. MULTI-WAN

- La funcionalidad Multi-WAN permite el uso de múltiples conexiones a Internet, con equilibrio de carga y / o conmutación por error, para mejorar la disponibilidad de Internet y la distribución del uso del ancho de banda.

2.4.6. EQUILIBRIO DE CARGA DEL SERVIDOR

- El equilibrio de carga del servidor se utiliza para distribuir la carga entre varios servidores. Esto se utiliza comúnmente con servidores web, servidores de correo y otros. Los servidores que no responden a las solicitudes de ping o conexiones de puerto TCP se quitan del grupo.

2.4.7. RED PRIVADA VIRTUAL (VPN)

El software pfSense ofrece tres opciones para la conectividad VPN, IPsec y OpenVPN.

- IPsec: Permite la conectividad con cualquier dispositivo compatible con IPsec estándar. Esto es más comúnmente utilizado para la conectividad de sitio a sitio con otras instalaciones de pfSense y la mayoría de las demás soluciones de cortafuegos (Cisco, Juniper, etc.). También se puede utilizar para la conectividad del cliente móvil.
- OpenVPN: Es una solución VPN SSL flexible y potente que soporta una amplia gama de sistemas operativos cliente.

2.4.8. SERVIDOR PPPOE

El software de pfSense ofrece un servidor PPPoE. Se puede utilizar una base de datos de usuario local para la autenticación y también se admite la autenticación RADIUS con contabilidad opcional.

2.4.9. INFORMES Y SEGUIMIENTO

- Gráficos RRD: En el software pfSense mantienen información histórica sobre lo siguiente:

• Uso de la CPU

• Rendimiento total

• Estado de cortafuego

• Rendimiento individual para todas las interfaces

• Paquetes por segundo para todas las interfaces

• Interfaz WAN puerta (s) ping tiempo de respuesta

• Colas de shaper de tráfico en sistemas con configuración de tráfico habilitada

2.4.10. INFORMACIÓN EN TIEMPO REAL

- La información histórica es importante, pero a veces es más importante ver información en tiempo real.
- Los gráficos SVG están disponibles que muestran el rendimiento en tiempo real para cada interfaz.
- La primera página incluye medidores AJAX para mostrar la CPU en tiempo real, la memoria, el uso de swap y disco y el tamaño de la tabla de estado.

2.4.11. DNS DINÁMICO

- Un cliente de DNS dinámico está incluido para permitirle registrar su IP pública con una serie de proveedores de servicios DNS dinámicos.

2.4.12. PORTAL CAUTIVO

El portal cautivo le permite forzar la autenticación o la redirección a una página de clics para acceder a la red. Esto se utiliza comúnmente en las redes hot spot, pero también se utiliza ampliamente en las redes corporativas para una capa adicional de seguridad en acceso inalámbrico o de Internet. Para más información sobre la tecnología del portal cautivo en general. La siguiente es una lista de características en el portal pfSense Captive:

- Máximo de conexiones simultáneas - Limite el número de conexiones al propio portal por IP del cliente. Esta función evita una denegación de servicio de las PC cliente que envían tráfico de red repetidamente sin autenticar o hacer clic a través de la página de presentación.
- Tiempo de espera de inactividad: desconecta los clientes inactivos durante más de un número definido de minutos.
- Hard timeout - Forzar una desconexión de todos los clientes después del número definido de minutos.
- Ventana emergente de inicio de sesión - opción para mostrar una ventana con un botón de cierre de sesión.
- Redireccionamiento de URL: después de autenticar o hacer clic a través del portal cautivo, los usuarios pueden ser redirigidos a la URL definida.

- Filtrado MAC: de forma predeterminada, los filtros pfSense utilizan direcciones MAC. Si tiene una subred detrás de un enrutador en una interfaz habilitada para el portal cautivo, cada máquina detrás del enrutador estará autorizada después de que un usuario esté autorizado. El filtrado MAC puede desactivarse para estos escenarios.
- Opciones de autenticación: hay tres opciones de autenticación disponibles:
  - Sin autenticación: esto significa que el usuario sólo hace clic en la página del portal sin introducir credenciales.
  - Administrador de usuarios locales: se puede configurar y utilizar una base de datos de usuario local para la autenticación.
  - Autenticación RADIUS: este es el método de autenticación preferido para entornos corporativos e ISP. Puede utilizarse para autenticarse desde Microsoft Active Directory y numerosos otros servidores RADIUS.

➢ Capacidades RADIUS.
➢ Re-autenticación forzada.
➢ Capaz de enviar actualizaciones de contabilidad.
➢ La autenticación RADIUS MAC permite que el portal cautivo se autentifique en un servidor RADIUS utilizando la dirección MAC del cliente como nombre de usuario y contraseña.
➢ Permite la configuración de servidores RADIUS redundantes.
➢ HTTP o HTTPS: la página del portal se puede configurar para usar HTTP o HTTPS.
➢ Direcciones MAC e IP de paso: las direcciones MAC e IP pueden aparecer en blanco para omitir el portal. Todas las máquinas con puerto NAT hacia delante tendrán que ser anuladas para que el tráfico de respuesta no llegue al portal. Es posible que desee excluir algunas máquinas por otras razones.

- Administrador de archivos: permite cargar imágenes para su uso en las páginas del portal.

Limitaciones: No es posible el portal "Reverso", es decir, capturar el tráfico procedente de Internet y entrar en su red.

Sólo las direcciones IP y MAC completas se pueden excluir del portal, no de protocolos y puertos individuales.

2.5. OBJETIVOS

2.5.1. OBJETIVO GENERAL

Diseñar e implementar entornos seguros y políticas para mejorar la productividad de los trabajadores y estudiantes de la institución educativa particular Unitek.

2.5.1. OBJETIVOS ESPECÍFICOS

a) Diseñar e Implementar entornos seguros y políticas para el control y administración del acceso a Internet desde la red de área local de la institución educativa particular Unitek.
b) Mejorar el rendimiento y seguridad de la red de área local de la institución educativa particular Unitek.

2.6. HIPOTESIS

2.6.1. HIPOTESIS GENERAL

El diseño e implementación de entornos seguros y políticas mejorará la productividad de los trabajadores y estudiantes de la institución educativa particular UNITEK.

2.6.2. HIPOTESIS ESPECÍFICAS

a) La implementación de la solución mejorará el rendimiento y seguridad de la red de área local de la institución educativa particular UNITEK.
b) El diseño de entornos seguros y políticas controlará y administrará el acceso a Internet desde la red de área local de la institución educativa particular Unitek.

2.7. ANTECEDENTES DE LA INVESTIGACIÓN

Hasta la actualidad se han desarrollado múltiples investigaciones sobre el uso de software libre y las soluciones que esta brinda en diferentes ámbitos de la

tecnología; para esta investigación en particular se desarrolla aplicándolo como servidor proxy y las posibilidades que este software ofrece para encontrar mejores soluciones en cuanto a seguridad informática.

- **Respecto a los antecedentes locales, existen las siguientes tesis:**

TITULO: ANALISIS, DISEÑO E IMPLEMENTACIÓN DE TECNOLOGÍA CORTAFUEGO PARA MEJORAR LA GESTIÓN Y ADMINISTRACIÓN DE LA RED DE DATOS DE LA EMPRESA S&B SERVICIOS GENERALES.

AUTOR: Rafael Villanueva Castrejón

AÑO: 2013

RESUMEN

El presente trabajo tuvo como objetivo general el "Análisis, Diseño e Implementación de Tecnología Cortafuego para Mejorar la Gestión y Administración de la Red de la Empresa S&B Servicios Generales"

Actualmente se observa las preocupaciones que tienen las empresas hoy día es como llevar a cabo sus transacciones electrónicas manteniendo altos niveles de seguridad y confidencialidad.

La conectividad total se ha convertido en una necesidad para poder sobrevivir en el ambiente competitivo del nuevo milenio. Esto ha traído, al mismo tiempo, serios problemas de seguridad al facilitar el acceso desde el mundo exterior a través de internet y así exponer los recursos internos de la red. Para impedir que personas no autorizadas penetren en la red o que acceden a más información de la permitida, se utiliza un sistema de defensa peri mental llamado cortafuego (cortafuegos), el cual se coloca como una barrera de protección entre internet y la red local de la empresa. A veces se utilizan cortafuegos adicionales internamente para separar distintos departamentos. Un sistema basado en cortafuego no es la panacea para la seguridad.

Esta tesis pretende completar una mejor seguridad en la red de datos, en la cual se implementó un cortafuego el cual brinda una máxima seguridad, donde se

aplicaron políticas de seguridad en las áreas de trabajo de la empresa, además se definen las reglas que se aplican en el cortafuego. Las reglas especifican el origen, destino, servicio y acción a realizar para cualquier transacción. También definen que eventos deben guardarse (logs), puesto que las posibles brechas de seguridad son más fácilmente identificables de esta manera. Es imprescindible que las políticas de seguridad se diseñaron de acuerdo a los activos y condiciones específicas de información que quiso proteger la empresa. Creando la zona verde que está dedicada a la red LAN de la empresa, la zona naranja donde se encuentran los servidores web y la zona roja que incluye la red WAN. En las distintas zonas de aplicaron las políticas de seguridad, restringir el acceso a servicios específicos.

- **Con respecto a las Investigaciones Internacionales tenemos las siguientes:**

TITULO: SISTEMA DE CONTROL Y SEGURIDAD ENDIAN CORTAFUEGO PARA LA EMPRESA FRADA SPORT

AUTOR: Juan Jacob Bueno Rosales

AÑO: 2013

RESUMEN

Los niveles de vulnerabilidad e importancia de toda la información de la empresa, a través de la red global de datos, orienta procesos o mecanismos de seguridad, únicos centralizados, y segmentados en la empresa Frada Sport.

Constituye una parte fundamental para la empresa, ya que no solo corresponde a la herramienta de seguridad como tal, sino a representar gráficamente, sistemáticamente, procesos y modelos de desarrollo actuales, mediante la implementación de un sistema único de seguridad, que a más de brindar soluciones de seguridad, estructura y establece medios de estabilidad, vigilancia, modelos de desarrollo, altamente disponible e inteligentes, control organizativo y fundamental, entre otros

Teniendo en cuenta toda la infraestructura de la red, se realiza un diseño de la red y se levanta la información de los procesos o modelos actuales, para posteriormente brindar soporte a soluciones específicas orientadas al control mayor y seguridad.

La herramienta de seguridad y control Endian Cortafuego, es un sistema único open source, específicamente estructurado como bitácora, capaz de brindar soluciones óptimas a la red de datos, captando y estabilizando mejores formas gráficas de control organizativo en la red de datos.

CONCLUSIONES

El sistema de seguridad Endian cortafuego, representa una manera estratégica de control, seguridad, disponibilidad, rendimiento y administración de la red global de datos, lo que se describe inicialmente, es un análisis de le empresa en técnicas de la investigación, basado en observación directa, encuestas descriptivas y referencia cruzada, para determinar el eje principal de la problemática de la empresa y abarcar procesos centrales de desarrollo.

Establecido el proceso de desarrollo en base a las encuestas, se analiza los diferentes medios de información vulnerables, puntos críticos, manejo de información de cada departamento de la empresa, entre otros, para representar gráficamente la situación actual referente a los diferentes problemas de la empresa como proceso de diseño.

Después, se procedió a estructurar la propia metodología de desarrollo, basada en 6 etapas de mejoramiento, cada etapa sigue diferente proceso de administración, control, seguridad, centralización y alta disponibilidad de datos.

Además, es importante trabajar con herramientas de entorno gráfico para tareas complejas, como crear reglas de filtrado, políticas, servicios, registros, entre otros.

Teniendo en cuenta todo el proceso a seguir, se puede manifestar que en la empresa Frada Sport, es aplicable el sistema de seguridad open source, basado en costos representativos mínimos para la empresa, toda la estructura física y

lógica que gestiona el sistema de seguridad EFW, es de vital importancia, ya que cuenta con diferentes medios que ayuda a la empresa a tener principalmente seguridad centralizada de alta disponibilidad, y además, la correcta administración y control de todos los componentes de la red global de datos, destacando principalmente su alto rendimiento o performance.

TITULO: OPTIMIZACION DE LA SEGURIDAD DE LA RED DE DATOS DEL IBUNAM BAJO PFSENSE.

RESUMEN:

El Instituto de Biología es una de las instituciones con la misión del desarrollo de la investigación científica, en particular con el origen, interacción, distribución y conservación de la diversidad biológica. Los conjuntos de años de investigación conforman un banco de datos digitales el cual va cada día en aumento. La tecnología está en todas partes y el IB 1 no es una excepción, por lo que la institución cuenta con servicios de red para la compartición, generación y almacenamiento de información de tipo académica.

Dicho acervo es un activo esencial y el más importante de dentro de cualquier institución, por lo tanto, debe y necesita estar debidamente asegurado. Debido al incremento en la interconectividad de los dispositivos y el flujo de información entre ellos es necesario que la Unidad de Computo que es la encargada de proporcionar este tipo de servicio verifique la calidad del mismo.

Por lo que el objeto de esta tesis con respecto a lo antes mencionado es cubrir la totalidad del servicio y sus variantes con el objetivo de iniciar una revisión de la situación actual de los servicios de TI.

CONCLUSIONES:

Con base en los objetivos de la institución, esta tesis implementa un proceso de mejora continua en los procesos de red y seguridad informática, estos procesos describen el significado de la calidad y reflejan en el Instituto de Biología la necesidad de continuar con la misión de desarrollo de investigación científica. La seguridad se ha vuelto una característica ya obligatoria para con los datos y la

tecnología, debe tomarse como un proceso natural dentro de cualquier institución, empresa etc. Dado que es un tema universal, es de suma importancia que el análisis, implementación y administración de la seguridad se lleve a cabo por un experto en la materia, para de esta manera cubrir todos aspectos relacionados con los sistemas críticos y su aseguramiento pertinente. Es esencial que se vea este proceso como un ciclo que no termina. El objeto de esta tesis comienza con la aportación hacia el IB, con el inicio de la identificación de los procesos críticos ligados con la tecnología, los cuales hacen posible muchos de los objetivos del IB tales como correo electrónico, página web, servicio de almacenamiento masivo, intranet etc.

Esto implica la inversión por parte de la institución en infraestructura y servicios de alta tecnología lo cual haga más eficiente y mejore la calidad del servicio hacia los usuarios, con el aumento en los niveles de desempeño del recurso humano, a través de la capacitación continua se garantiza la actualización y se extienden las aptitudes del personal, de esta manera los objetivos y misión institucional se alinean con la investigación y desarrollo científico.

TITULO: DOCUMENTACIÓN DEL PROCESO DE IMPLEMENTACIÓN VIRTUAL DE UN PORTAL CAUTIVO

AUTOR: AURELIO BONIFACIO MUNGUÍA LÓPEZ

AÑO: 2010.

RESUMEN

El presente trabajo documenta el proceso de implementación de manera virtual del software para portal cautivo Pfsense, que permitirá llevar el control en el acceso a la red inalámbrica de la UAQ. Dicho software cuenta con aplicaciones para permitir, restringir y controlar el acceso a los sitios de internet por parte de los usuarios de la red inalámbrica. El primer capítulo brinda un resumen sobre el giro de la UAQ, así como también su historia y propósito. El segundo capítulo hace mención de los objetivos que se pretenden alcanzar, su justificación y el plan de trabajo que se siguió para desarrollar el proyecto. El tercer capítulo hace

referencia al área en donde se realizó el proyecto, así como los pasos que se siguieron, el desarrollo e implementación de éste.

El cuarto capítulo presenta los problemas que se identificaron en el desarrollo del proyecto, así como las soluciones que se tomaron para corregir dichos problemas; también se sugieren algunas recomendaciones para el uso pleno del software y lograr su mayor aprovechamiento.

CONCLUSIONES

Las dificultades que se presentaron en la implementación virtual del portal cautivo fueron que no se tenía conocimiento de lo que significaba un portal de este tipo. Además, la investigación resulto complicada, ya que toda la información fue recolectada en diferentes fuentes de Internet y no siempre resultaba de utilidad, por lo tanto,hubo que hacer una depuración exhaustiva de dicha información.

Se documentó con éxito la implementación virtual del software Pfsense y se comprobó el correcto funcionamiento del portal cautivo. Se implementaron correctamente las herramientas que permitirán en un futuro tener un mayor control y seguridad en el acceso a la red inalámbrica de la Universidad Autónoma de Querétaro.

Para realizar la implementación, configuración y mantenimiento del software Pfsense se recomienda el uso del manual, esto servirá para un manejo más confiable del portal cautivo y tener así la seguridad en el acceso a la red inalámbrica por parte de los usuarios de la misma.

TITULO: Sustitución de cortafuego tradicional con código abierto

AUTOR: Amit Thakur

AÑO: 2015

RESUMEN

El enfoque principal de la tesis es sustituir una solución de la vida real de un cortafuego basado en enrutador con una solución de código abierto que tiene una interfaz gráfica de usuario fácil, manejable y centralizado, extensiones de red. La tesis compara tres cortafuegos populares de código abierto, Untangle, pfSense y Zeroshell, con el fin de cumplir con los requisitos de seguridad. Estos tres cortafuegos Fueron instalados en un entorno VMware y probados para la instalación, estabilidad, Componentes, nivel de seguridad, administración de interfaces GUI y consumo de recursos. En conclusión, entre los tres cortafuegos mencionados, se encontró que pfSense era un Solución eficaz debido a su fácil actualización, configurador web simple, y su amplia gama De extensión y características.

CONCLUSIONES

El propósito de esta tesis fue configurar una solución de cortafuegos que se ajuste a los requisitos necesarios. Tres cortafuegos fueron seleccionados, a saber, Untangle, PfSense.

Y Zeroshell, ya que estos surgieron como la solución líder con un mayor alcance de la seguridad junto con las utilidades y herramientas de seguridad integradas.

TITULO: IMPLEMENTACIÓN DE VIRTUALIZACIÓN DEL SERVICIO WIRELESS EN EL DEPARTAMENTO INFORMÁTICO DE LA CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES DE LA UNIVERSIDAD DE GUAYAQUIL UTILIZANDO HERRAMIENTAS OPEN SOURCE

Analizar y probar estos tres cortafuegos de red en entorno virtual, es decir, VMware ESXi, pfSense indicó el cortafuego más apropiado ya que la mayoría de las características son Soportado por los requisitos mínimos de hardware. Se requiere cierta atención como Snort y ntop se recomienda no instalar en sistemas que tienen menos de 1GB de RAM.

Aparte de estos, los servicios gratuitos de licencias fomentan el uso de estos cortafuegos.

Open source con una gran comunidad de desarrolladores, quienes constantemente hacen un esfuerzo para mejorar la seguridad y el rendimiento.

Pfsense Proporciona soporte para características como IPsec, OpenVPN y HTTPS (TLS) tasa superior, 10GBps, superando el ancho de banda normal soportado por cortafuegos comerciales.

CAPITULO III

MATERIALES Y MÉTODOS

3.1 MATERIALES

3.2. POLÍTICAS DE LA INSTITUCIÓN

Todo el contenido sobre las políticas de esta institución se encuentra en el ANEXO B, en esta sección se presenta la parte relacionada con el acceso a internet.

POLITICA DE ADMINISTRACION DE ACCESO A INTERNET

3.2.1. GENERALIDADES

1.1 El área de Informática debe definir, implementar, controlar Y mantener las políticas, normas, estándares, procedimientos, funciones y responsabilidades necesarias para preservar y proteger la confidencialidad, disponibilidad, integridad y acceso de la información de UNITEK donde ésta resida (aplicaciones, bases de datos, sistemas operativos, redes, backups y medios).

1.2 El área de Informática es la encargada de establecer, mantener y administrar una arquitectura de acceso para UNITEK y facilitar la incorporación de prácticas de acceso a la información en todas las dependencias.

1.3 El área de Informática debe estar ubicada organizacionalmente de manera que tenga autonomía e independencia frente a las demás áreas de tecnología tales como soporte, diseño y desarrollo, entre otras.

3.2.2. FUNCIONES DE CONTROL

2.1. El personal administrativo no está permitido ingresar a páginas web de ocio por ejemplo; Facebook, twitter, YouTube, y más idénticas a la anterior descritas. Para lograr una atención preferencial hacia los alumnos o visitantes a la UNITEK

2.2. Los estudiantes no están permitido ingresar a páginas web de ocio por ejemplo; Facebook, twitter, YouTube, y más idénticas a la anterior

descritas. Con fines de estudio, tratamos de evitar distracciones en el momento de aprendizaje de estudiantes.

2.3. Viendo los puntos anteriores todos, incluyendo personal administrativo y estudiantes pueden ingresar a páginas de investigaciones o blogs educativos.

2.4. El área de informática realizara el boqueo de estas páginas web, usando programas, softwares, servidores y/o cortafuegos.

2.5. El único personal autorizado para ingresar a todas las páginas web es la secretaria y la recepción.

3.3. METODOLOGÍA DE INVESTIGACIÓN

La investigación es experimental, es una implementación que se concentra más en la profundidad y comprensión de un tema que en la descripción o medición. A la investigación cualitativa le interesa sintetizar un proceso, esquematizarlo, comprenderlo, más que sólo medirlo y precisarlo. Estas investigaciones se realizan en muestras pequeñas y abarcan, a veces, muchas variables de estudio, para lo que se usan diversas técnicas de observación, registro y entrevista al mismo tiempo. En efecto, observando a los empresarios en su vida cotidiana, escuchándolos hablar sobre lo que piensan, sienten o hacen, y viendo los documentos que producen y las opiniones de los trabajadores, el investigador cualitativo obtiene un conocimiento directo de la vida empresarial. Son investigaciones que buscan descubrir la complejidad del mundo empresarial, y explicar estos hallazgos según cómo son vividos por sus protagonistas (Vara, 2010).

3.4. CONFIGURACION INICIAL DEL SISTEMA

Todo el paso para la instalación del servidor se observa en el ANEXO A. En este punto explicaremos como realizar el bloqueo de las direcciones IP de Facebook y visualizar todas las direcciones IP relacionadas con esta página web.

Para ver todas las direcciones usadas se ingresa a www.bgp.he.net la cual es de la compañía Hurricane Electric, es un backbone global en Internet (ISP), especializado en IPv6 e IPv4. Hurricane Electric controla varios backbones

IPv4/IPv6 en Asia, Norte América y Europa, que están conectados a distintos puntos neutros de todo el mundo. En 2007, obtuvieron el primer puesto en la clasificación de compañías de hosting en Internet por su fiabilidad.

Por eso es recomendable usar el servicio que ofrece esta compañía. Ingresamos la dirección web de Facebook es decir facebook.com como indica en la figura 19.

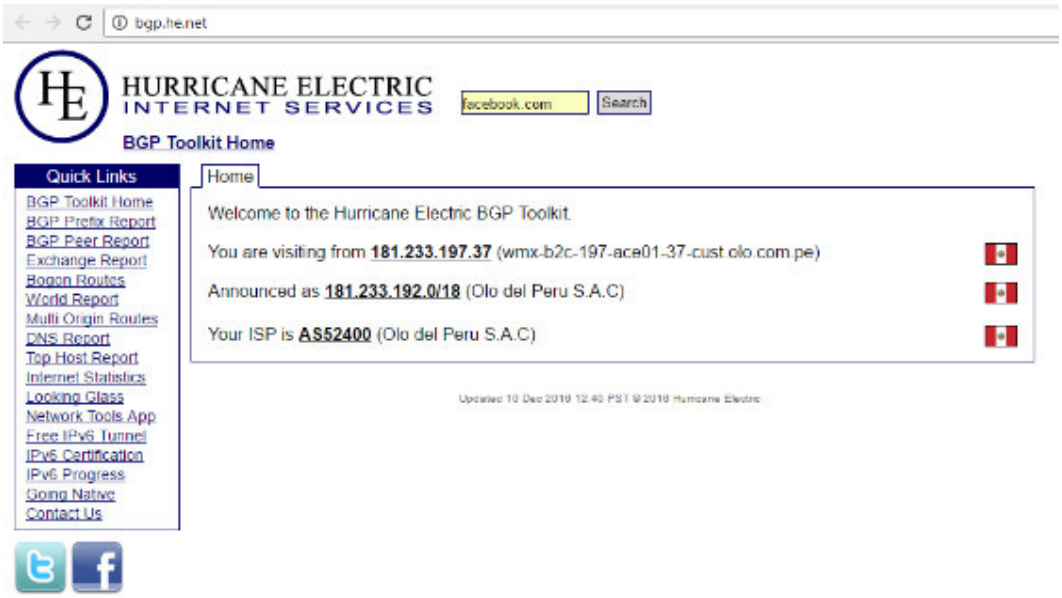


Figura 19: Búsqueda de Facebook.com en bgp.he.net.

Elaboración: Propia

En la figura 20 Al buscar se observa todos los detalles como información de DNS, pagina web de información, información IP y quien es esa página, para el bloque es necesario dirigirnos a la pestaña de información IP.

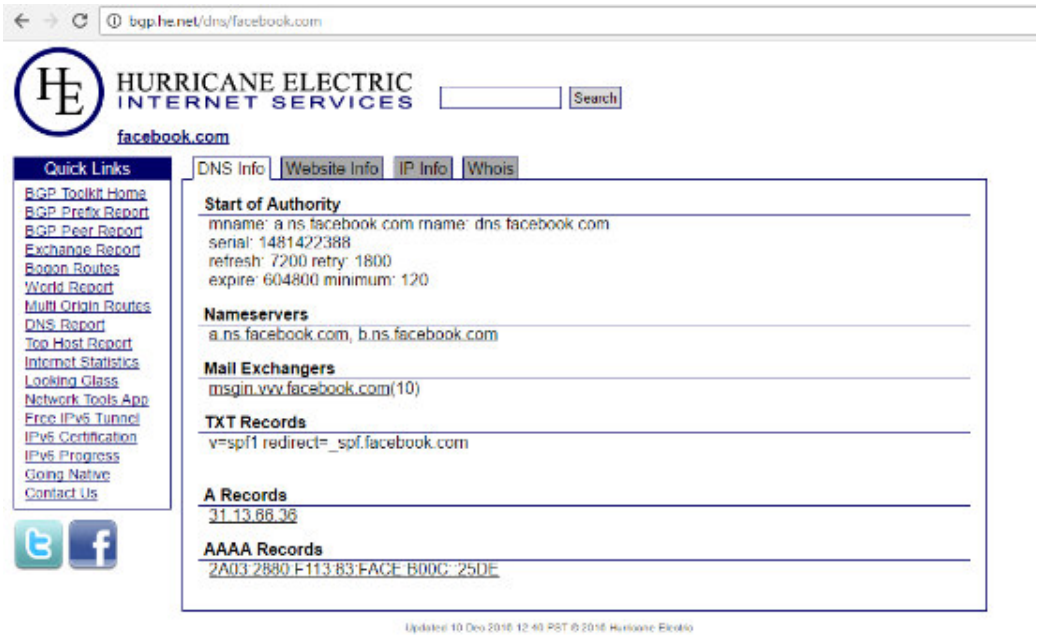


Figura 20: Información sobre Facebook.com.

Elaboración: Propia

Al ingresar podemos observar el sistema autónomo. Un sistema autónomo se define como “un grupo de redes IP que poseen una política de rutas propia e independiente”. Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet. Un número de AS o ASN se asigna a cada AS, el que lo identifica de manera única a sus redes dentro de Internet.

El sistema autónomo utilizado para Facebook es AS32934 tal como se indica en la figura 21.

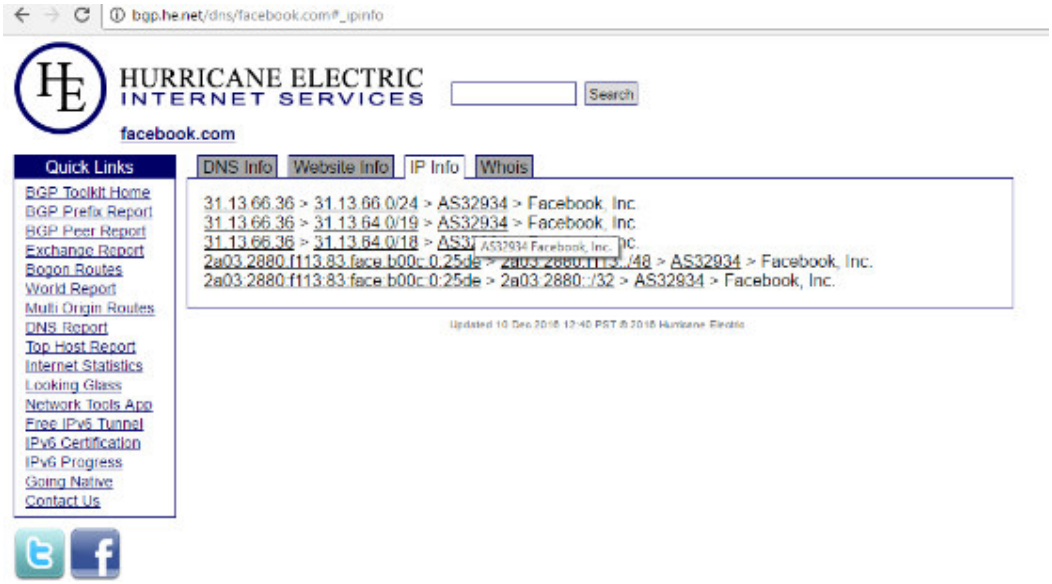


Figura 21: Sistemas autónomos en Facebook.

Elaboración: Propia

Seleccionamos el sistema autónomo, en la cual aparecerá la información de AS, gráfica de IPv4 e IPv6, prefija de IPv4 e IPv6, puntos de IPv4 e IPv6 y más observe la figura 22.

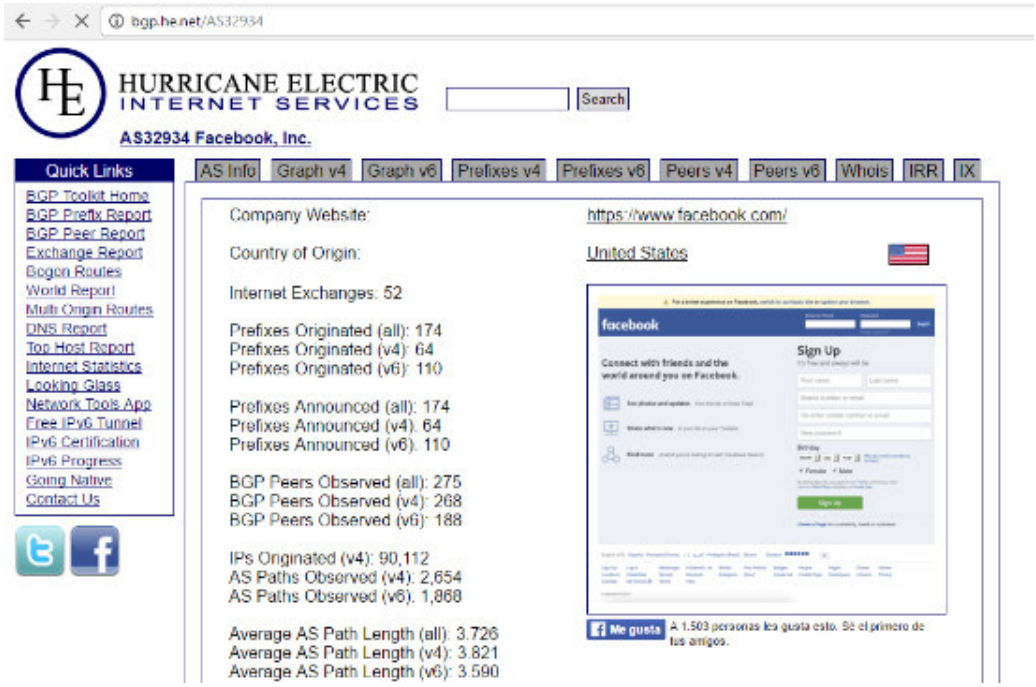


Figura 22: Prefijos de IPv4.

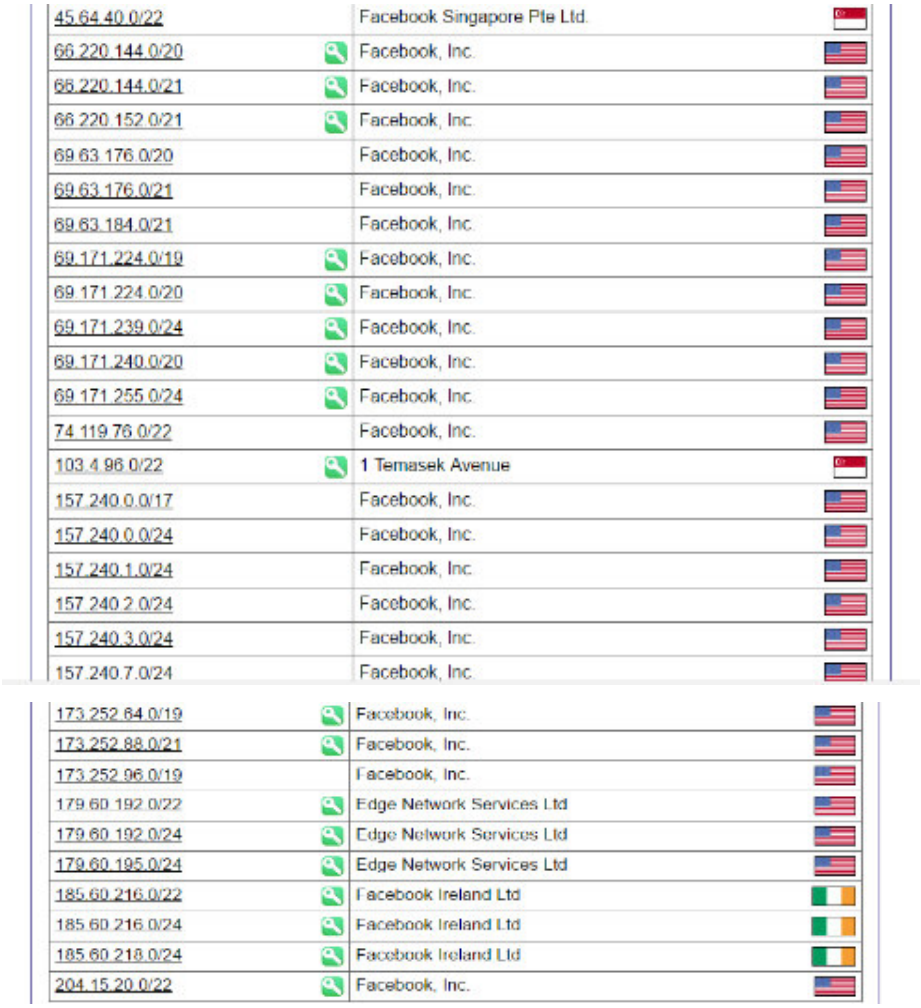
Elaboración: Propia

Después de esto nos dirigimos a la pestaña de prefijos de versión 4, es decir de IPv4. Se muestra en la figura 23.

En aquí se mostrara toda una lista de direcciones IPv4 para bloquear y estos son solo de Facebook, por lo cual será el mismo paso para otras páginas web como por ejemplo: YouTube, Twitter y más.

Figura 23: Primer bloque de direcciones IP de Facebook.

Elaboración: Propia



45.64.40.0/22		Facebook Singapore Pte Ltd.
66.220.144.0/20		Facebook, Inc.
66.220.144.0/21		Facebook, Inc.
66.220.152.0/21		Facebook, Inc.
69.63.176.0/20		Facebook, Inc.
69.63.176.0/21		Facebook, Inc.
69.63.184.0/21		Facebook, Inc.
69.171.224.0/19		Facebook, Inc.
69.171.224.0/20		Facebook, Inc.
69.171.239.0/24		Facebook, Inc.
69.171.240.0/20		Facebook, Inc.
69.171.255.0/24		Facebook, Inc.
74.119.76.0/22		Facebook, Inc.
103.4.96.0/22		1 Temasek Avenue
157.240.0.0/17		Facebook, Inc.
157.240.0.0/24		Facebook, Inc.
157.240.1.0/24		Facebook, Inc.
157.240.2.0/24		Facebook, Inc.
157.240.3.0/24		Facebook, Inc.
157.240.7.0/24		Facebook, Inc.
173.252.64.0/19		Facebook, Inc.
173.252.88.0/21		Facebook, Inc.
173.252.96.0/19		Facebook, Inc.
179.60.192.0/22		Edge Network Services Ltd
179.60.192.0/24		Edge Network Services Ltd
179.60.195.0/24		Edge Network Services Ltd
185.60.216.0/22		Facebook Ireland Ltd
185.60.216.0/24		Facebook Ireland Ltd
185.60.218.0/24		Facebook Ireland Ltd
204.15.20.0/22		Facebook, Inc.

Figura 24: Segundo bloque de direcciones IP de Facebook.

Elaboración: Propia

Empezaremos a bloquear la primera dirección IP (figura 25), y daremos a la opción guardar.

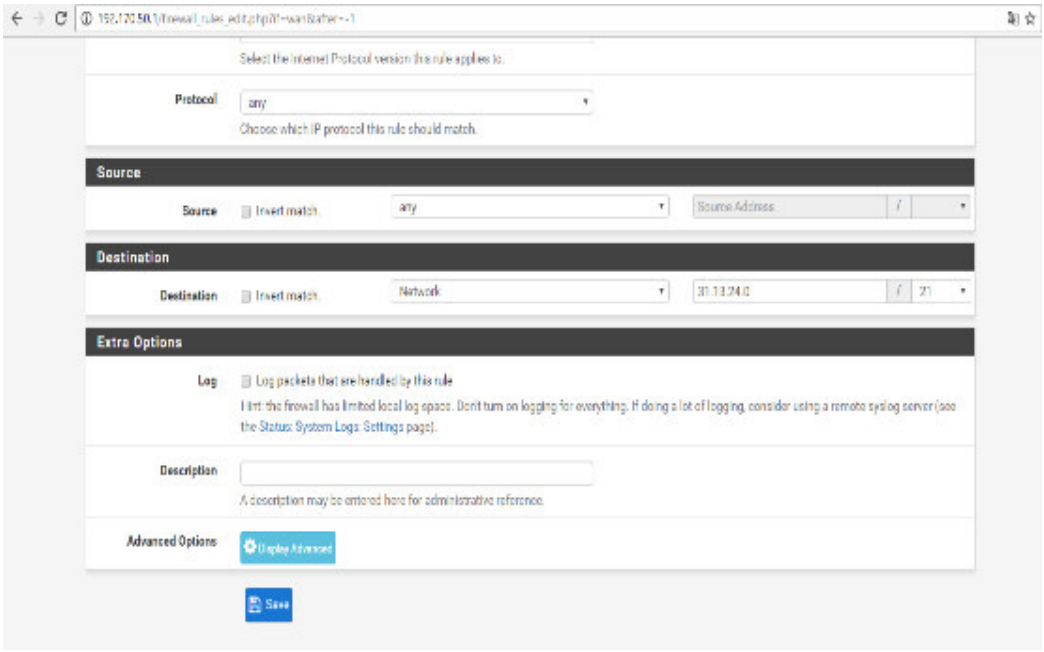


Figura 25: Procedimiento para bloquear página web.

Elaboración: Propia

Luego procederemos a hacer lo mismo para bloquear las diferentes páginas web tales como YouTube, twitter, etc., con sus respectivas direcciones ip. Nos daremos cuentas que las páginas seleccionadas, habrán sido bloqueadas.

Por último, damos clic en el botón Save y nos saldrá esta pantalla indicándonos el resumen de los parámetros de configuración de la regla, después damos clic en guardar en la parte superior de la pantalla. En el botón que dice Apply Changes. Aquí podemos apreciar los parámetros mencionados anteriormente con el estado de la regla que en este caso está en color verde.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

La cantidad de estudiantes en la institución se mostrará en la siguiente lista.

- 1er grupo: 30 estudiantes
- 2do grupo: 30 estudiantes
- 3er grupo: 30 estudiantes
- 4to grupo: 30 estudiantes
- 5to grupo: 30 estudiantes

La anterior lista son la cantidad de estudiantes asistentes al horario de la mañana, son una cantidad de 150 estudiantes. En la siguiente lista se presenta los grupos en el turno de la tarde:

- 6to grupo: 30 estudiantes
- 7mo grupo: 29 estudiantes
- 8vo grupo: 29 estudiantes

En el turno de la tarde son una cantidad de 88 estudiantes. En el turno de la noche se muestran solo dos grupos:

- 9no grupo: 29 estudiantes
- 10mo grupo: 27 estudiantes

En el turno de la noche ingresan 56 estudiantes. Al implementar el servidor tuvo que trabajar con 150 clientes en las mañanas, 88 clientes en la tarde y 56 clientes para la noche. La cantidad de clientes demandan la RAM instalada en el sistema, pero puede ser aumentada a la dimensión deseada. De esta forma es posible determinar los ajustes de hardware para un funcionamiento óptimo.

Continuando mostraremos las capturas de los resultados obtenidos al ingresar al interfaz gráfico del usuario mediante un navegador web, buscando la dirección IP del servidor (192.168.1.2). Iniciaremos con las características del servidor y las configuraciones realizadas.

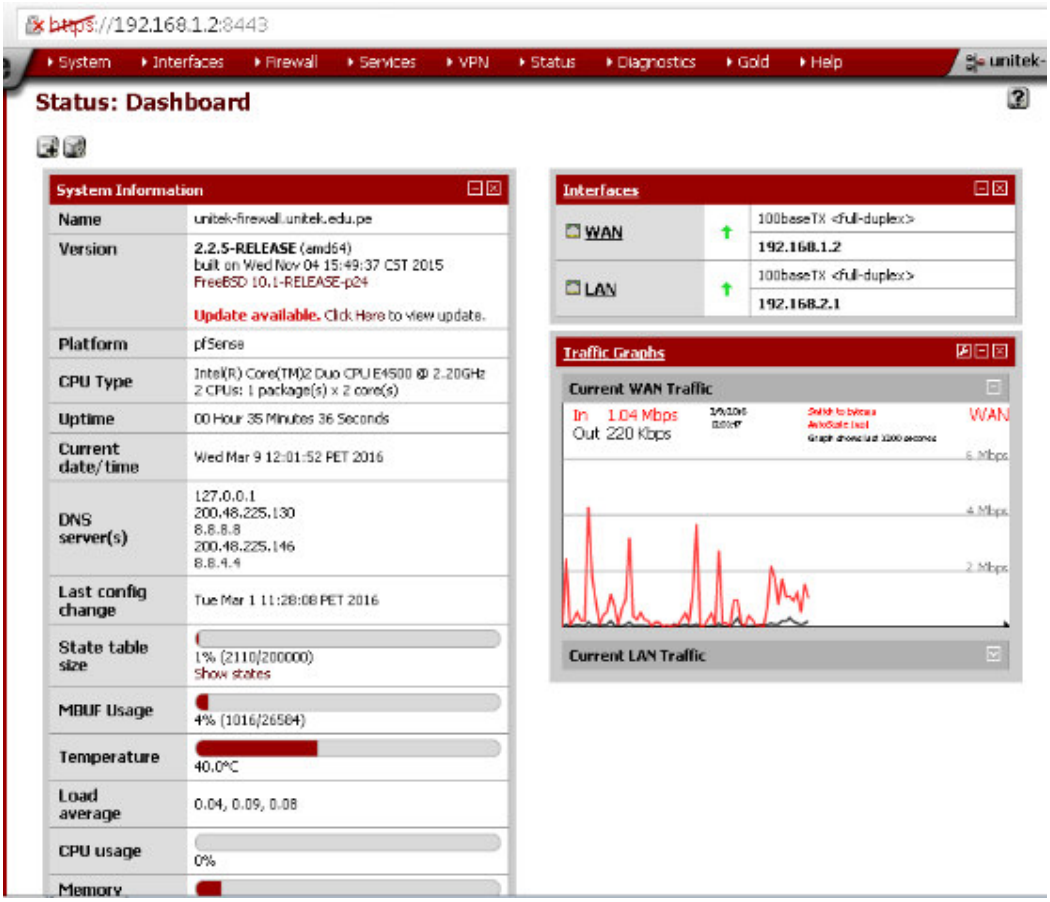


Figura 26: Captura de Dashboard (Tablero de instrumentos)

Elaboración: Propia

En la figura 26 se muestra el dashboard del servidor. Dashboard o tablero de instrumentos de pfSense es la página principal del servidor de seguridad, y hace el seguimiento de diversos aspectos del sistema. Se puede ingresar haciendo clic en el logotipo en la parte superior izquierda, o navegando a **Status > Dashboard**.

El tablero de instrumentos se compone de Widgets, cada uno de los cuales mostrar información sobre un área diferente del servidor. La lista actual de widgets incluye.

- Captive Portal Status
- Carp Status
- Dynamic DNS Status
- Cortafuego Logs
- Gateways

- Gmirror Status
- HAVP Alerts (installable add-on widget)
- Installed Packages
- Interface Statistics
- Interfaces
- IPsec Status
- Load Balancer Status
- NTP Status
- OpenVPN Status
- Pictures
- RSS Feed
- Services Status
- S.M.A.R.T. Status
- Snort Alerts (installable add-on widget)
- System Information
- Thermal Sensors
- Traffic Graphs
- Wake on LAN

Un widget puede ser añadido al tablero haciendo clic "+"en la parte superior de la pantalla, a continuación, elegir el widget de la lista. Una vez que aparezca el widget, su colocación se puede cambiar arrastrando la barra de título a otra ubicación en la pantalla. El widget puede encajar en su sitio en una de dos columnas y ser reordenado como deseado.

Haga clic en Guardar configuración en la parte superior de la pantalla después de hacer cualquier cambio de diseño de widgets.

En nuestra figura se observa tres widgets, las cuales son y revisaremos cada uno de sus resultados:

- System Information, muestra los resultados como:
  - El nombre del servidor
  - La versión del software junto el año de lanzamiento
  - La plataforma

- Tipo de CPU, indicando la capacidad del CPU.
- Tiempo de actividad.
- La fecha actual.
- Servidores DNS.
- Fecha de la última configuración.
- Capacidad de la tabla de estado.
- Uso de MBUF
- La temperatura, y mas

o Interfaces, describe la dirección IP de la WAN y LAN

- WAN: 192.168.1.2, con línea de transmisión de 100baseTX.
- LAN: 192.168.2.1, con línea de transmisión de 100baseTX

o Traffic Graphs, indica el tráfico del ancho de banda en la interface WAN. Tanto el tráfico de subida y bajada.

En la figura 27, se muestra los logs de DHCP en el servidor.

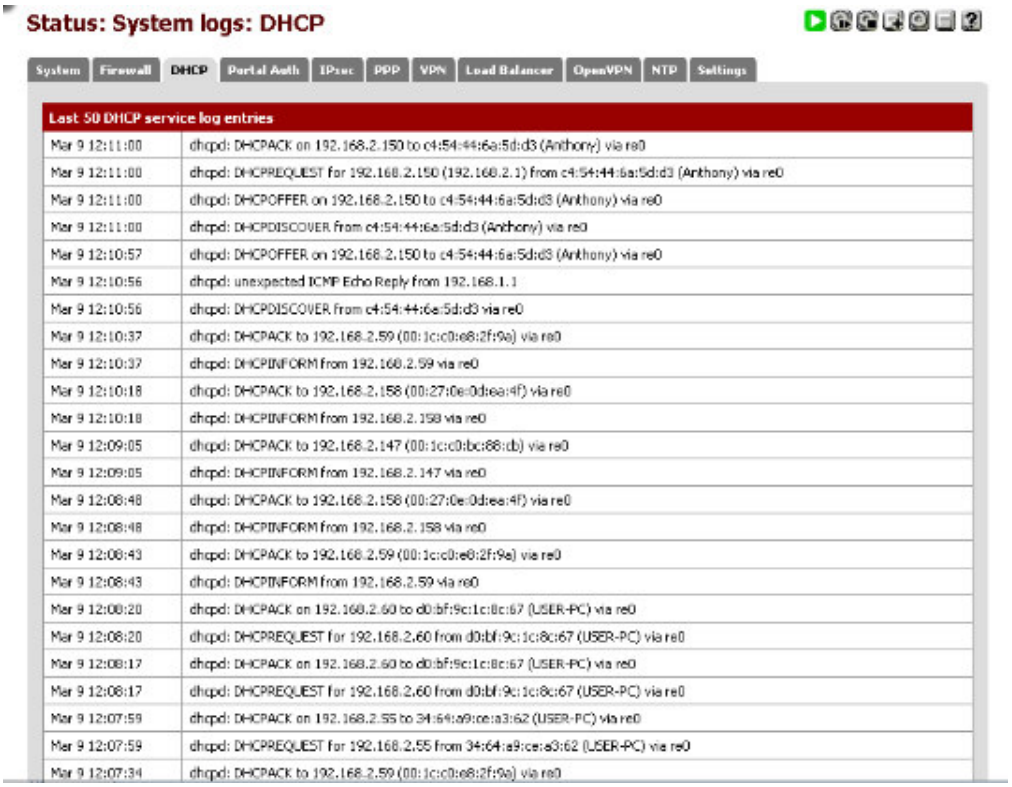


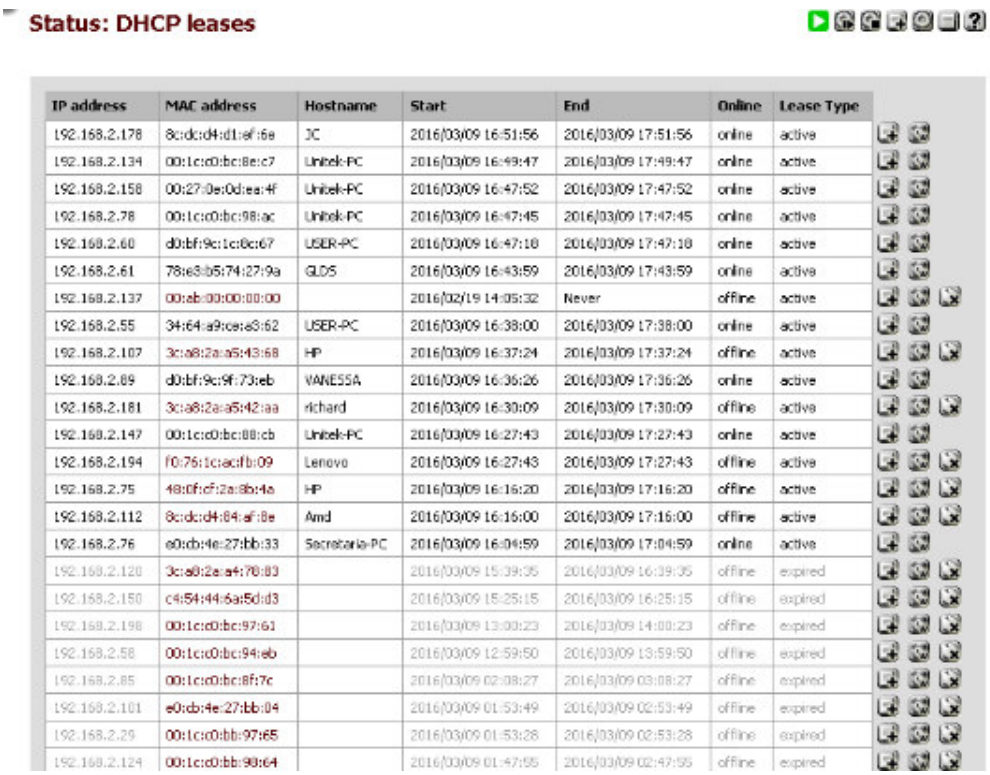
Figura 27: Captura de logs de DHCP

Elaboración: Propia

Para ver los logs de DHCP es ingresando a **Status > System Logs** en esta tabla de **DHCP**, muestra los mensajes, eventos de DHCP y eventos de cliente DHCP para redes WAN.

Cada solicitud DHCP y respuesta de los clientes DHCP se muestra aquí, junto con los eventos y errores. Direcciones IP, direcciones MAC, y nombres de host proporcionados por el cliente son visibles en los registros.

En la figura 28 muestra la tabla de clientes DHCP activos y también inactivos



Status: DHCP leases

IP address	MAC address	Hostname	Start	End	Online	Lease Type
192.168.2.178	8c:dc:d4:d1:ef:6e	JC	2016/03/09 16:51:56	2016/03/09 17:51:56	online	active
192.168.2.134	00:1c:c0:bc:8e:c7	Unitek-PC	2016/03/09 16:49:47	2016/03/09 17:49:47	online	active
192.168.2.158	00:27:0e:0d:ea:4f	Unitek-PC	2016/03/09 16:47:52	2016/03/09 17:47:52	online	active
192.168.2.78	00:1c:c0:bc:98:ac	Unitek-PC	2016/03/09 16:47:45	2016/03/09 17:47:45	online	active
192.168.2.60	d0:bf:9c:1c:0c:67	USER-PC	2016/03/09 16:47:10	2016/03/09 17:47:10	online	active
192.168.2.61	78:e3:b5:74:27:9a	GLDS	2016/03/09 16:43:59	2016/03/09 17:43:59	online	active
192.168.2.137	00:ab:00:00:00:00		2016/02/19 14:05:32	Never	offline	active
192.168.2.55	34:64:a9:ce:a8:62	USER-PC	2016/03/09 16:38:00	2016/03/09 17:38:00	online	active
192.168.2.107	3c:a8:2a:a5:43:68	HP	2016/03/09 16:37:24	2016/03/09 17:37:24	offline	active
192.168.2.89	d0:bf:9c:9f:73:eb	VANESSA	2016/03/09 16:36:26	2016/03/09 17:36:26	online	active
192.168.2.181	3c:a8:2a:a5:42:aa	richard	2016/03/09 16:30:09	2016/03/09 17:30:09	offline	active
192.168.2.147	00:1c:c0:bc:88:cb	Unitek-PC	2016/03/09 16:27:43	2016/03/09 17:27:43	online	active
192.168.2.194	f0:76:1c:ac:fb:09	Lenovo	2016/03/09 16:27:43	2016/03/09 17:27:43	offline	active
192.168.2.75	48:0f:cf:2a:8b:4e	HP	2016/03/09 16:16:20	2016/03/09 17:16:20	offline	active
192.168.2.112	8c:dc:d4:84:af:8e	Amd	2016/03/09 16:16:00	2016/03/09 17:16:00	offline	active
192.168.2.76	e0:cb:4e:27:bb:33	Secretaria-PC	2016/03/09 16:04:59	2016/03/09 17:04:59	online	active
192.168.2.120	3c:a8:2a:a4:70:83		2016/03/09 15:39:35	2016/03/09 16:39:35	offline	expired
192.168.2.150	c4:54:44:6a:5d:d3		2016/03/09 15:25:15	2016/03/09 16:25:15	offline	expired
192.168.2.198	00:1c:c0:bc:97:61		2016/03/09 13:00:23	2016/03/09 14:00:23	offline	expired
192.168.2.58	00:1c:c0:bc:94:eb		2016/03/09 12:59:50	2016/03/09 13:59:50	offline	expired
192.168.2.85	00:1c:c0:bc:8f:7c		2016/03/09 02:08:27	2016/03/09 03:08:27	offline	expired
192.168.2.101	e0:cb:4e:27:bb:04		2016/03/09 01:53:49	2016/03/09 02:53:49	offline	expired
192.168.2.29	00:1c:c0:bb:97:65		2016/03/09 01:53:28	2016/03/09 02:53:28	offline	expired
192.168.2.124	00:1c:c0:bb:90:64		2016/03/09 01:47:55	2016/03/09 02:47:55	offline	expired

Figura 28: Clientes DHCP

Elaboración: Propia

Una lista de asignaciones DHCP activos e inactivos se puede ver en pfSense navegando al **Status > DHCP Leases**.

Al visualizar esa página, se muestran todas las clientes activas, junto con la dirección IP, la dirección MAC, nombre de host, las horas de inicio y final de arrendamiento, el tipo de contrato de arrendamiento, y si es o no el sistema no está en línea. (Al igual que con la tabla ARP, esto no es siempre un indicador fiable). En la figura muestra 15 clientes activos entre ellos equipos personales, equipos de la administración y equipos de laboratorios de computo (Unitek-PC).

Al final se observan clientes ya desconectados o ya expirados el tiempo de alojamiento.

Otra de las muchas opciones que ofrece pfSense en un servidor de NTP esto mostraremos en la figura.

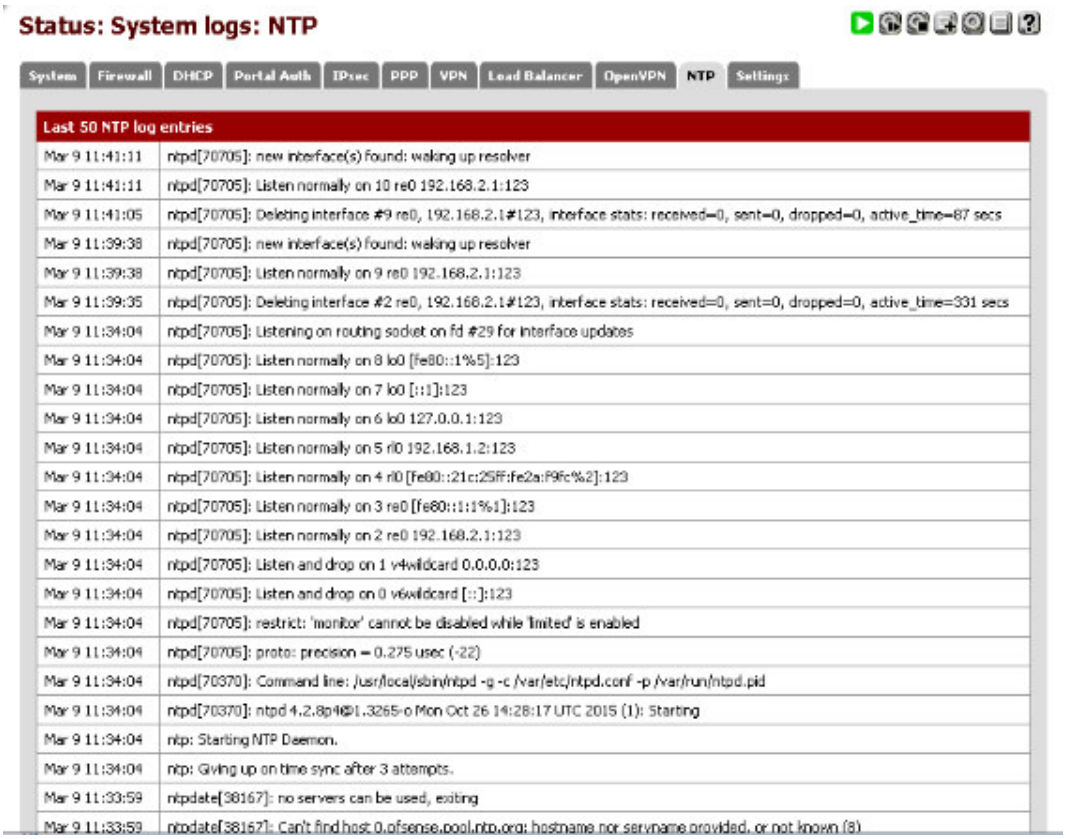


Figura 29: Captura de NTP logs

Elaboración: Propia

Estos logs Mostrará todos los registros generados por NTP en la red y grandes actualizaciones temporales, para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

Después de ver todos estos logs en el servidor, mostraremos la gráfica de uso del ancho de banda, se observa en la figura.

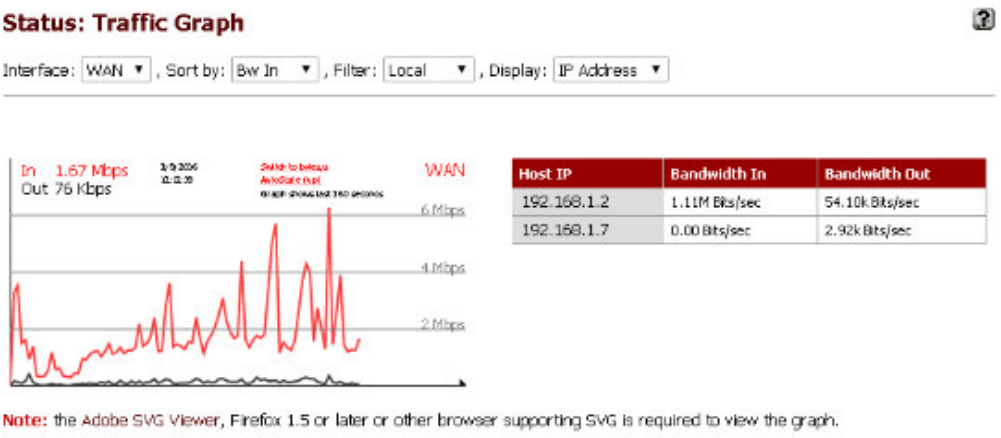


Figura 30: Grafica de tráfico

Elaboración: Propia

Para ingresar a esta grafica es mediante **Status > Traffic Graph,** donde muestra un gráfico en vivo del tráfico en una única interfaz. Esta interfaz se puede cambiar al decantarse por uno diferente de la lista desplegable disponible.

Una tabla se muestra a la derecha de la gráfica que incluye la dirección IP y la información de tráfico. Los controles de clasificación y filtrado en la parte superior de la página pueden afinar esta salida. En a la tabla se muestra que el ancho de banda usado de entrada es de un promedio de 1.11Mbps, esto indica que está usando todo el ancho de banda contratado por la institución, pero también llega a picos de más de 6Mbps. El ancho de banda de salida es de 54.10Kbps en promedio.

CPU Selection

The numbers stated in the following sections can be increased slightly for quality NICs, and decreased (possibly substantially) with low quality NICs. All of the following numbers also assume no packages are installed.

10-20 Mbps	We recommend a modern (less than 4 year old) Intel or AMD CPU clocked at at least 500MHz.
21-100 Mbps	We recommend a modern 1.0 GHz Intel or AMD CPU.
101-500 Mbps	No less than a modern Intel or AMD CPU clocked at 2.0 GHz. Server class hardware with PCI-e network adapters, or newer desktop hardware with PCI-e network adapters.
501+ Mbps	Multiple cores at > 2.0GHz are required. Server class hardware with PCI-e network adapters.

Figura 31: Selección de CPU

Elaboración: Propia

Viendo estos resultados del ancho de banda en la figura 30 y conociendo que el CPU utilizado es de 2.20 GHz de Intel con dos núcleos. El servidor puede aguantar más de 501Mbps.

Revisado ya los resultados del ancho de banda utilizado, los logs de cada servicio (DHCP y NTP) veremos las direcciones IP bloqueadas. Esto se mostrará en las imágenes.

Firewall: Rules

Floating | WAN | LAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	8443 80	*	*		Anti-Lockout Rule
	IPv4 *	192.168.2.19	*	*	*	*	none		Secretaria y Recepción
	IPv4 *	*	*	158.85.58.68	*	*	none		whatsapp
	IPv4 *	*	*	158.85.58.3	*	*	none		whatsapp
	IPv4 *	*	*	65.49.14.131	*	*	none		ultrasurf
	IPv4 *	*	*	38.229.72.16	*	*	none		block torbrowser
	IPv4 *	*	*	82.196.75.101	*	*	none		block torbrowser
	IPv4 *	*	*	86.59.30.40	*	*	none		block torbrowser
	IPv4 *	*	*	93.95.227.222	*	*	none		block torbrowser
	IPv4 *	*	*	154.35.132.70	*	*	none		block torbrowser
	IPv4 *	*	*	38.229.72.16	*	*	none		block torbrowser
	IPv4 *	*	*	179.6.255.39	*	*	none		youtube.com 2
	IPv4 *	*	*	179.6.255.50	*	*	none		youtube.com 2

Figura 32: Reglas de Cortafuego

Elaboración: Propia

Las reglas de cortafuego controlan lo que se permite el tipo tráfico de entrada en una interfaz en el servidor. Se procesan de arriba hacia abajo, donde hay reglas de cortafuegos configurados por el usuario que no coinciden, se le niega el tráfico. Normas relativas a la interfaz LAN que permite la subred LAN a cualquier destino vienen por defecto. Las reglas del cortafuego se ingresan por Cortafuego> Rules. Múltiples reglas pueden ser seleccionadas para algunas acciones haciendo clic en su fila o marcando la casilla al comienzo de su fila. Las reglas pueden ser borradas o reordenadas. Los destinos bloqueados para todo el equipo de origen son las direcciones de ultrasurf y tor browser.

En la figura 32 se observa que todas las direcciones IP pueden conectarse con cualquier dirección LAN mientras sea en el puerto 8338 (TCP) y 80(HTTP). El host con dirección 192.168.2.19 (secretaria y recepción) tiene acceso a todo internet. Las secciones opacas son las reglas deshabilitadas.

Figura 33: Reglas de Cortafuego para Facebook parte 1

Elaboración: Propia

En la figura 33 y 34 continuando con la tabla muestra todas las direcciones IP hacia Facebook. Las direcciones de Facebook bloqueadas son un total de 30.

	IPv4 *	*	*	31.13.87.0/24	*	*	none		
	IPv4 *	*	*	31.13.90.0/24	*	*	none		
	IPv4 *	*	*	31.13.91.0/24	*	*	none		
	IPv4 *	*	*	31.13.93.0/24	*	*	none		
	IPv4 *	*	*	31.13.96.0/19	*	*	none		
	IPv4 *	*	*	66.220.144.0/20	*	*	none		
	IPv4 *	*	*	66.220.144.0/21	*	*	none		
	IPv4 *	*	*	66.220.152.0/21	*	*	none		
	IPv4 *	*	*	69.63.176.0/20	*	*	none		
	IPv4 *	*	*	69.63.176.0/21	*	*	none		
	IPv4 *	*	*	69.63.184.0/21	*	*	none		
	IPv4 *	*	*	69.171.224.0/19	*	*	none		
	IPv4 *	*	*	69.171.224.0/20	*	*	none		
	IPv4 *	*	*	69.171.239.0/24	*	*	none		
	IPv4 *	*	*	69.171.240.0/20	*	*	none		

Figura 34: Reglas de Cortafuego para Facebook parte 2

Elaboración: Propia

Después de mostrar las reglas, comienza el servidor a realizar los bloqueos estos se mostrarán posteriormente.

Status: Interfaces

WAN interface (wan, rl0)	
Status	up
MAC address	00:1c:25:2a:f9:fc
IPv4 address	192.168.1.2
Subnet mask IPv4	255.255.255.0
Gateway IPv4	WANGW 192.168.1.1
IPv6 Link Local	fe80::21c:25ff:fe2a:f9fc
ISP DNS servers	127.0.0.1 200.48.225.130 8.8.8.8 200.48.225.146 8.8.4.4
MTU	1500
Media	100baseTX <full-duplex>
In/out packets	93250/89053 (89.55 MB/8.33 MB)
In/out packets (pass)	93250/89053 (89.55 MB/8.33 MB)
In/out packets (block)	3772/0 (322 KB/0 bytes)
In/out errors	0/0
Collisions	0

Figura 35: Estado de la Interface WAN

Elaboración: Propia

Ingresando a **Status> Interfaces** muestra cada interfaz, junto con diversas estadísticas sobre ellos.

Para cada interfaz, esta pantalla mostrará el estado (up /down), dirección MAC, dirección IP, máscara de subred, Gateway (si es pertinente), los servidores DNS (si es relevante), tipo de medio (por ejemplo, 100 Mbit, 1000Mbit, etc), entrada / salida de paquetes, entrada / salida paquetes que pasaron y bloqueados, errores, y colisiones. Dependiendo del tipo de interfaz, tal como Wireless, otra información también puede estar disponible.

La figura 35 muestra que entraron 93250 paquetes a la interface WAN una cantidad de 89.55 MB, también muestra que hubo 8.33MB salientes, es decir salieron 89053 paquetes del interface. Los paquetes bloqueados en esta interface son solo de entrada, esta cantidad es de 3772 paquetes con unos 322KB. Entre los datos se ve que no hay paquetes de error ni colisiones.

LAN interface (lan, re0)	
Status	up
MAC address	30:b5:c2:03:dc:16
IPv4 address	192.168.2.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::1:1
MTU	1500
Media	100baseTX <full-duplex>
In/out packets	116455/100235 (10.52 MB/94.83 MB)
In/out packets (pass)	116455/100235 (10.52 MB/94.83 MB)
In/out packets (block)	253/0 (15 KB/0 bytes)
In/out errors	0/0
Collisions	0

Using dial-on-demand will bring the connection up again if any packet triggers it. To substantiate this point: disconnecting manually will **not** prevent dial-on-demand from making connections to the outside! Don't use dial-on-demand if you want to make sure that the line is kept disconnected.

Figura 36: Estado de la Interface LAN

Elaboración: Propia

En la figura 36 hay 116455 paquetes entrantes que pasaron a la interface un total de 10.52MB y los paquetes salientes no bloqueados son 100235 esto da a 94.83MB. Los paquetes bloqueados en esta interface son de 253 en total solamente 15KB, estos son de entrada y 0 paquetes de salida.

Cada vez que un usuario trata de ingresar a una página de entretenimiento o redes sociales, como, por ejemplo, facebook.com, el sistema bloqueará esta página de acuerdo a las reglas y políticas establecidas en el plan de seguridad y buenas prácticas dentro de la institución. Un usuario que trata de usar un navegador web para acceder a estos sitios web tendrá la siguiente notificación en su aplicación.

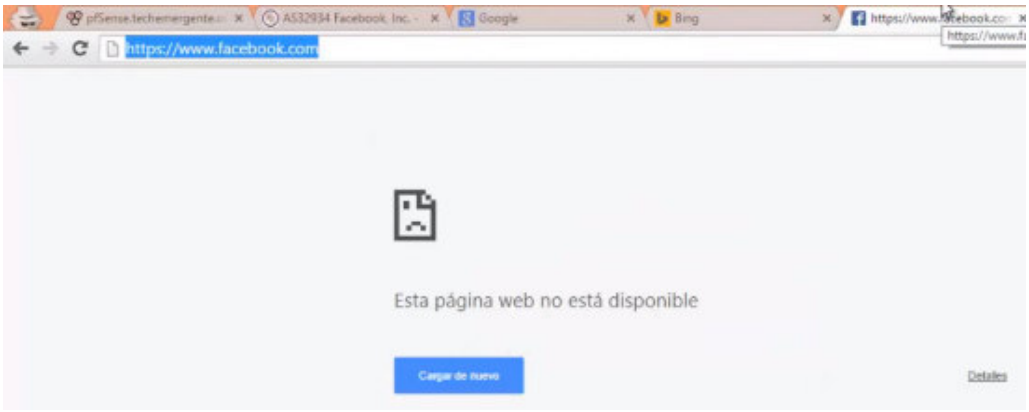


Figura 37: Un usuario falla al tratar de acceder a Facebook.com.

Elaboración: Propia

Como se ha notado el usuario no recibe notificación alguna del bloqueo al sitio web, simplemente el navegador web indica que no puede acceder al sitio o que el sitio no está disponible, de esta forma se hace efecto en comando drop que hace el bloqueo, pero no deja notificación, si se desearía notificar al usuario que está siendo bloqueado se usa el comando reject, que rechaza y notifica al usuario de la acción. Drop es recomendado para no dar información al usuario a cerca de la existencia del sistema, lo cual es una buena práctica de seguridad.

Sin embargo, el usuario si será capaz de entrar a sitios web relacionados con las políticas que favorecen a los objetivos de la institución. Por ejemplo, el caso de Wikipedia.org.

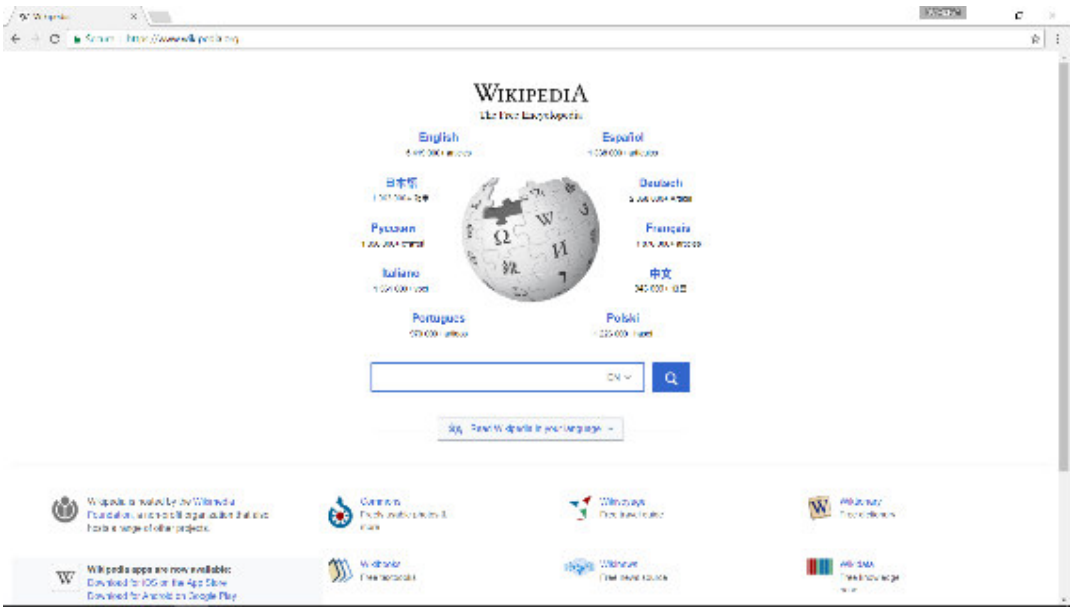


Figura 38: Un usuario logra acceder a sitios que favorecen a los objetivos de la institución.

Elaboración: Propia

Cuando se terminó todas las pruebas y se observó resultados mencionamos que las personas usaron más el ancho de banda para educación y de esa forma estas páginas tienen menor uso de recursos porque generalmente usan texto e imágenes y no video, comparando con las páginas bloqueadas.

CONCLUSIONES

PRIMERO: Esta investigación fue capaz de lograr el objetivo general que se planteó, ya que permite bloquear sitios web de redes sociales y cumple con las políticas para mejorar la productividad en trabajadores y estudiantes evitando que puedan usar un recurso tan importante como es el Internet para sitios de entretenimiento tales como a Facebook, Youtube, Twitter, Instagram y más.

SEGUNDO: El rendimiento de la red se ve óptima mediante este servicio y además el costo de implementación no es caro ya que el sistema operativo es de código abierto y este se puede instalar en cualquier ordenador de buena capacidad y con dos tarjetas de red. Además, es importante trabajar con herramientas de entorno gráfico para tareas complejas, como crear reglas de filtrado, políticas, servicios, registros, entre otros. Los recursos de la institución, como son el ancho de banda con acceso a Internet y los laboratorios de computadoras, son aprovechados para los intereses, políticas y objetivos de la organización; éstos son la investigación, la búsqueda de información educativa y técnica, y el mejor desempeño de estudiantes, administrativos y docentes en sus labores académicas.

TERCERO: Teniendo en cuenta todo el proceso a seguir, se puede manifestar que en la institución Unitek, es aplicable el sistema de seguridad de cortafuego, basado en costos representativos mínimos para la institución, toda la estructura física y lógica que gestiona el sistema de seguridad, es de vital importancia, ya que cuenta con diferentes medios que ayuda a la empresa a tener principalmente seguridad centralizada de alta disponibilidad, y además, la correcta administración y control de todos los componentes de la red global de datos, destacando principalmente su alto rendimiento o performance.

CUARTO: El cortafuego dentro de esta institución permitirá la mayor productividad de los estudiantes y trabajadores de la misma, los estudiantes podrán accedes a sitios con contenido de investigación y estudio, mientras que los sitios de entretenimiento son totalmente bloqueados. De esta forma se permitirá un mejor uso de la banda ancha de la institución educativa. El precio del hardware es muy bajo y el precio del software es cero, de esta forma se logra

una solución que consigue los mismos resultados de opciones muchísimo más caras en el mercado. La seguridad de la red también está garantizada, porque no sólo se usa los entornos seguros para restringir el acceso a ciertos sitios en Internet, sino también para proteger la red local del malware en Internet, ya que los sitios de entretenimiento son los más inseguros.

RECOMENDACIONES

PRIMERO: El uso de la página www.bgp.he.net es importante para encontrar todas las redes de las páginas web, ya que puede encontrar varios y de diferentes nacionalidades además brinda otras informaciones como información de DNS, la información de la página web, todo esto tanto en IPv4 y en IPv6.

SEGUNDO: El acceso mediante navegador puede ser tedioso por esta razón es bueno tomar estas recomendaciones, desactivar el cortafuego de ordenador que ingresara al servidor pfSense, desactivar la configuración proxy del ordenador y por último; es posible que el navegado reconozca como una página insegura por lo cual lea bien las alertas que se muestran.

TERCERO: Se recomienda a los administradores de red realizar respaldos de la información antes de realizar algún cambio en la configuración de las reglas de seguridad del Cortafuego.

CUARTO: Se recomienda realizar la suscripción par a recibir soporte de software puesto que el pfSense en una poderosa herramienta que tiene una amplia gama servicios los cuales no se los ha comprobado en este trabajo.

QUINTO: Es conveniente realizar la optimización en los segmentos de red para evitar direcciones no permitidas con esto se lograría incrementar la seguridad que proporciona el cortafuego.

REFERENCIAS

Colvin, H. (2015). VirtualBox: An Ultimate Guide Book on Virtualization with VirtualBox Paperback. United States: CreateSpace Independent Publishing Platform.

Crawley, D. R. (2010). The Accidental Administrator: Linux Server Step-by-Step Configuration Guide Paperback. United States: CreateSpace Independent Publishing Platform.

Davis, J. A. Baca, S. and Thomas, O. (2016). VCP6-DCV Official Cert Guide (Exam #2V0-621) (3rd Edition) (VMware Press Certification) 3rd Edition. United States: VMware Press.

Ferguson, B. (2016). vSphere 6 Foundations Exam Official Cert Guide (Exam #2V0-620): VMware Certified Professional 6 (VMware Press) 1st Edition. United States: VMware Press.

Ghori, A. (2015). RHCSA & RHCE Red Hat Enterprise Linux 7: Training and Exam Preparation Guide (EX200 and EX300), Third Edition 3rd Edition. United States: Endeavor Technologies Inc.

Kouka, A. (2015). Ubuntu Server Essentials Paperback. United States: Packt Publishing - ebooks Account.

LaCroix, J. (2016). Mastering Ubuntu Server Paperback. United States: Packt Publishing - ebooks Account.

Lammle, T. (2013). CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120 1st Edition. United States: Sybex.

Marshall, N. Lowe, S. Orchard, G. and Atwell, J. (2015). Mastering VMware vSphere 6 1st Edition. United States: Sybex.

Nathan, S. (2015). VirtualBox at Warp Speed: Virtualization with VirtualBox Kindle Edition. United States: Senthil Nathan.

Nutter, R. (2014). VMware - A Guide for New Admins Kindle Edition. United States: TechBytes Press.

Odom, W. (2016). CCENT/CCNA ICND1 100-105 Official Cert Guide 1st Edition. United States: Cisco Press.

Petersen, R. (2016). Ubuntu 16.04 LTS Server: Administration and Reference Paperback. United States: Surfing Turtle Press.

Rankin, K. and Mako, B. (2013). The Official Ubuntu Server Book (3rd Edition) 3rd Edition. United States: Prentice Hall.

Santana, G. A. (2013). Data Center Virtualization Fundamentals: Understanding Techniques and Designs for Highly Efficient Data Centers with Cisco Nexus, UCS, MDS, and Beyond 1st Edition. United States: Cisco Press.

Ward. B. (2014). How Linux Works: What Every Superuser Should Know 2nd Edition. United States: No Starch Press.

ANEXOS

ANEXO A1: INSTALACION DE PFSENSE

Luego de tener el sistema operativo booteado en una unidad externa en este caso un USB mediante el software libre, estos son fáciles de usar y gratis. Luego de insertar la unidad externa al ordenador se presionó la tecla F12 para ingresar a la selección de unidad de arranque, dentro de estas opciones se puso a la unidad USB como el número uno para la búsqueda del sistema operativo. Terminado eso se ingresó a la opción de instalación de pfSense tal como se muestra en la figura 39.

Figura 39: Opciones de configuración inicial de PfSense.

Elaboración: Propia

En las opciones mostradas al inicio indican opciones de boot en las cuales están de multiusuario, un solo usuario o también un reinicio del sistema, así como también se muestra la configuración de boot. La opción a elegir es la numero 1 o también esperar diez segundos, ya que, automáticamente iniciara la opción de multiusuario.

Luego del inicio de la instalación se tiene que presionar la tecla “i” eso para autorizar la instalación, luego de esto comenzara a cargar todo los archivos del USB, iniciando el kernel luego comenzara a reconocer dispositivos externos conectados en los periféricos del ordenador.

En la figura 40 se muestra en el omento en que se tiene que presionar la tecla, tomando en cuenta que el tiemplo de plazo es de diez segundos, al igual que en la anterior opción

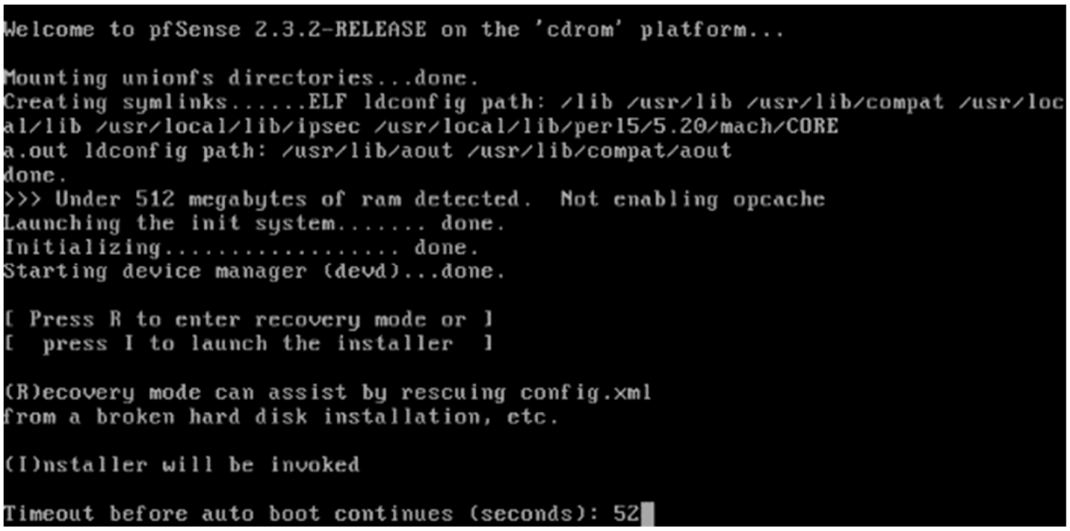


Figura 40: Opción de instalación de PFSENSE.

Elaboración: Propia

Luego de autorizar la instalación luego de unos segundos se mostrará una pantalla para la configuración de consola, esto es para configurar las opciones de entorno seleccionado que están utilizando en la configuración de consola. Seleccione cualquiera que desee cambiar del modo default.

El instalador de pfSense nos da la opción de cambiar algunos ajustes sobre el hardware, pero la instalación por defecto sugerido funciona a la perfección, así que aceptamos esta configuración.

Seleccionamos la opción de acepto estas condiciones.

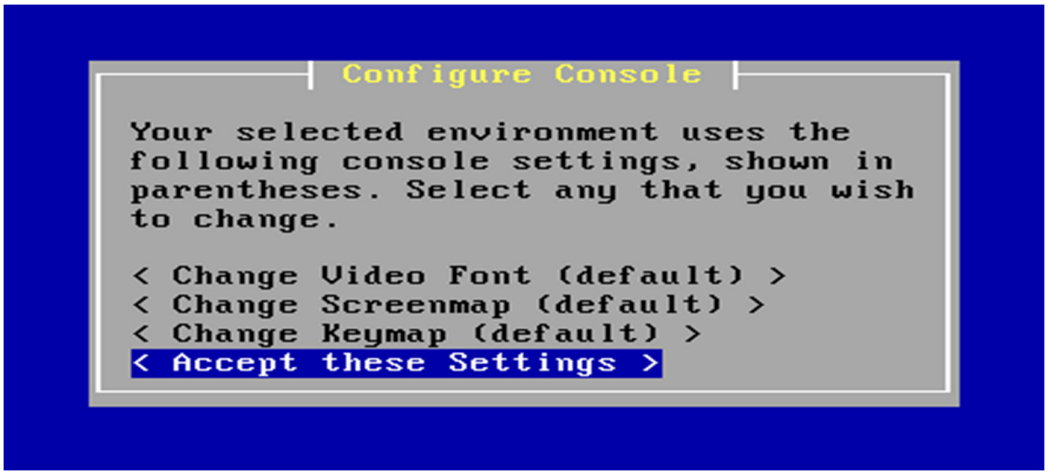


Figura 41: Aceptando las configuraciones por defecto.

Elaboración: Propia

Después de las primeras opciones de configuración, en la segunda la pregunta es sobre cómo se realizará a instalación. La primera opción indica la fácil instalación, pero en la segunda esta la opción de instalación personalizada junto a tres opciones más como indica en la figura 42

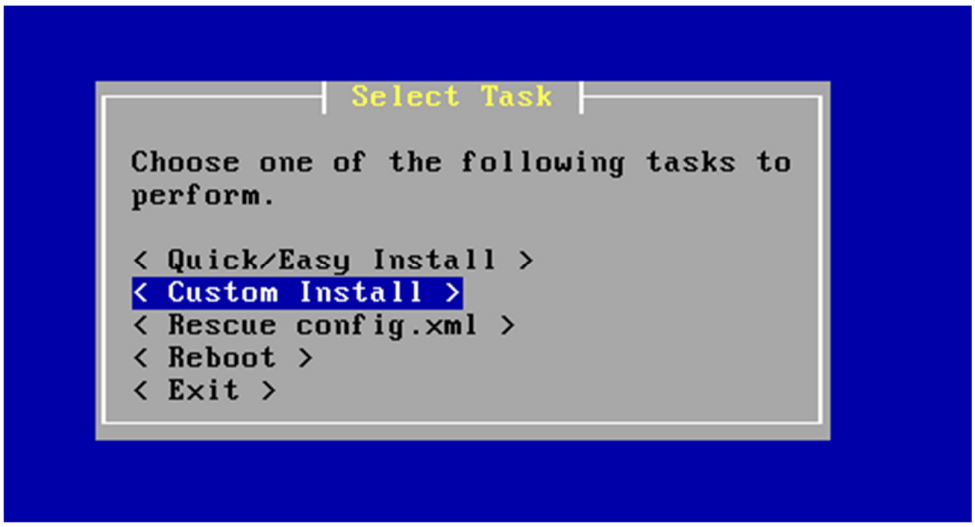


Figura 42: Selección de instalación personalizada.

Elaboración: Propia

Seleccionamos la opción de instalación personalizada esto para la partición personalizada del disco.

En el siguiente dialogo se selecciona el disco donde se realizará la instalación de pfSense, esto se observa en la figura 43.

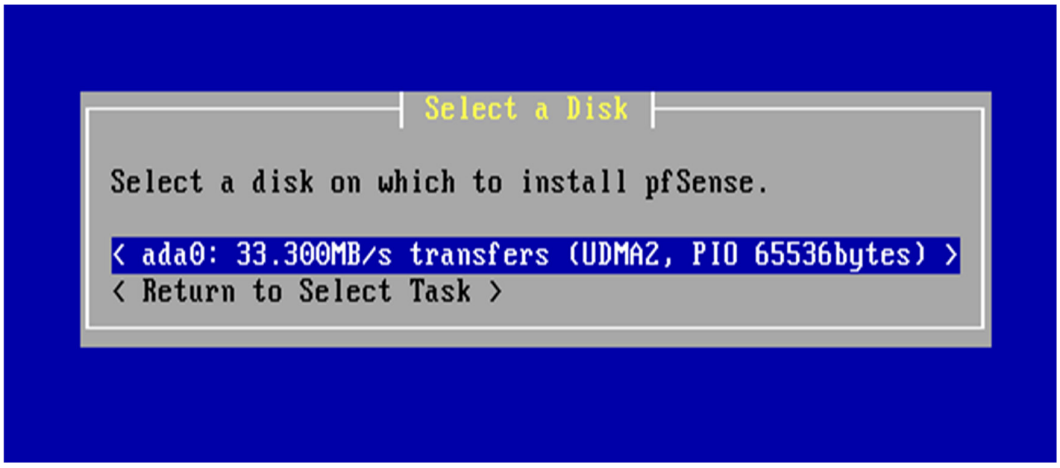


Figura 43: Selección del disco en donde se instalará el Pfsense.

Elaboración: Propia

Se observa que solo hay un disco para instalar pfSense en el ordenador, por lo cual seleccionamos este para realizar acción deseada.

Cuando ya se haya seleccionado el disco la siguiente pregunta es: ¿Desea formatear este disco? Debe formatear el disco si es nuevo, o si desea comenzar desde una pizarra limpia. Se recomienda no formatear el disco si contiene información que desea mantener.

Figura 44: Aplicar formato al disco seleccionado.

Elaboración: Propia

Las opciones en este dialogo son:

- Formatear el disco
- Salte este paso
- Regresar a seleccionar disco

Como indica en la figura 44 la opción a seleccionar es formatear el disco

En este dialogo se presenta la selección de geometría la cual indica que el sistema informa que la geometría ada0 es 16644 cilindros, 16 cabezas, 63 sectores. Esta geometría debe permitir arrancar desde este disco. A menos que tenga una razón urgente para hacer en todo el mundo, se recomienda que usted lo vea.

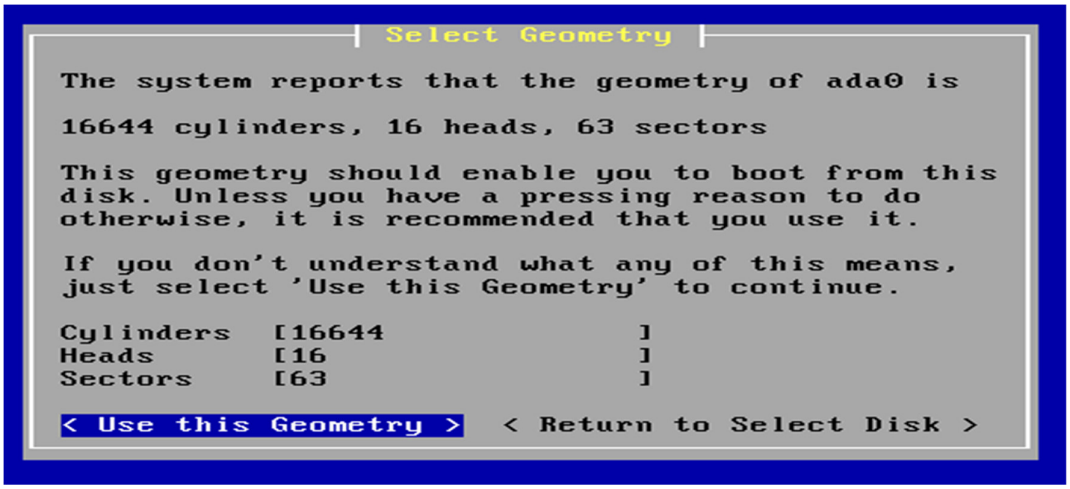


Figura 45: Usaremos la geometría por defecto.

Elaboración: Propia

Si no entiendes lo que significa esto, simplemente selecciona "Use this Geometry" para seleccionar por defecto esta geometría.

Continuando se muestra la advertencia de formatear el disco en esto usted debe estar absolutamente seguro de que desea tomar esta acción. Esta es la última oportunidad para cancelar.

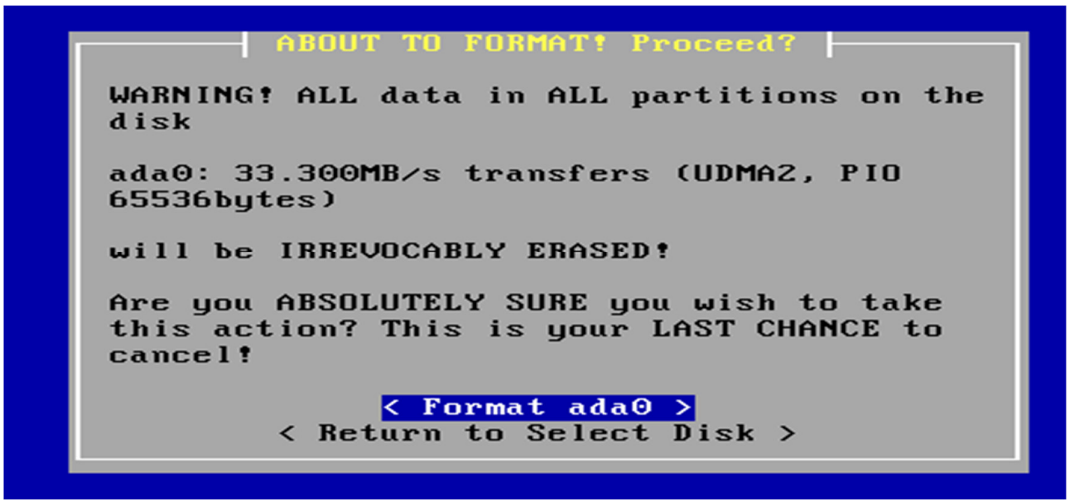


Figura 46: Aplicando formato a la unidad seleccionada.

Elaboración: Propia

En la siguiente pregunta es sobre si desea realizar la partición del disco. Si ha formateado este disco, y ahora desea instalar varios sistemas operativos en él, puede reservar una parte del disco para cada uno de ellos aquí. Crear una partición múltiple, una para cada sistema operativo.

Si el disco ya tiene sistemas operativos en él que desea mantener, debe tener cuidado de no cambiar las particiones en las que están, si decide dividir.

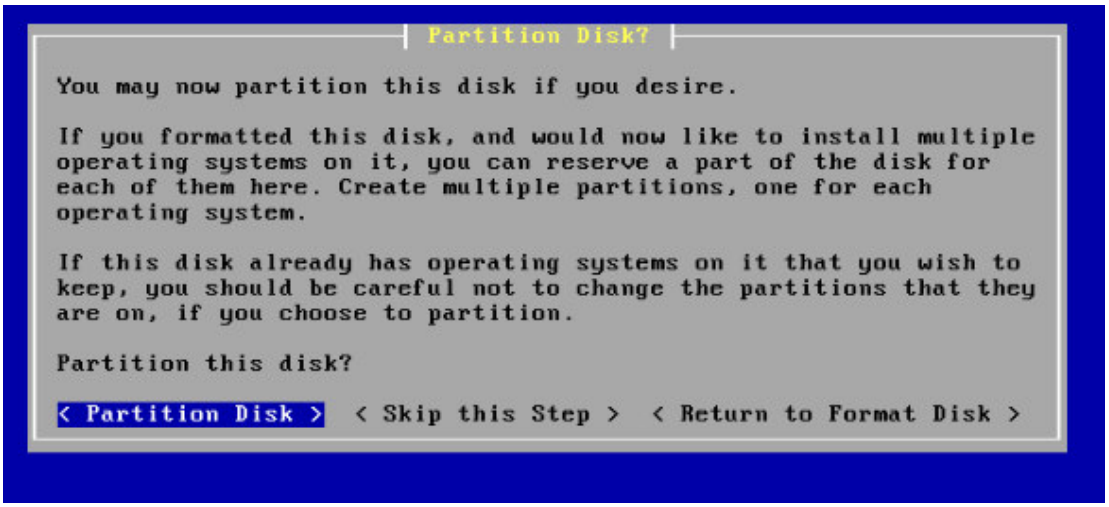


Figura 47: Confirmando la opción de aplicar formato al disco.

Elaboración: Propia

Como en varias preguntas hay la opción de omitir el paso, regresar a formatear disco y particionar disco. En este caso se erigirá la opción de particionar el disco. Seguido continua la partición de disco en la que indica seleccionar las particiones (también conocidas como "porciones" en el tradicional BSD) que desea tener en este disco. Para el tamaño ingrese un tamaño bruto en sectores (1GB = 2097152 sectores) o un solo "*" para indicar "utilizar el espacio restante en el disco"

Se seleccionó la primera opción que se observó sobre la partición aceptando y creando la partición. Como se observa en la figura 48.

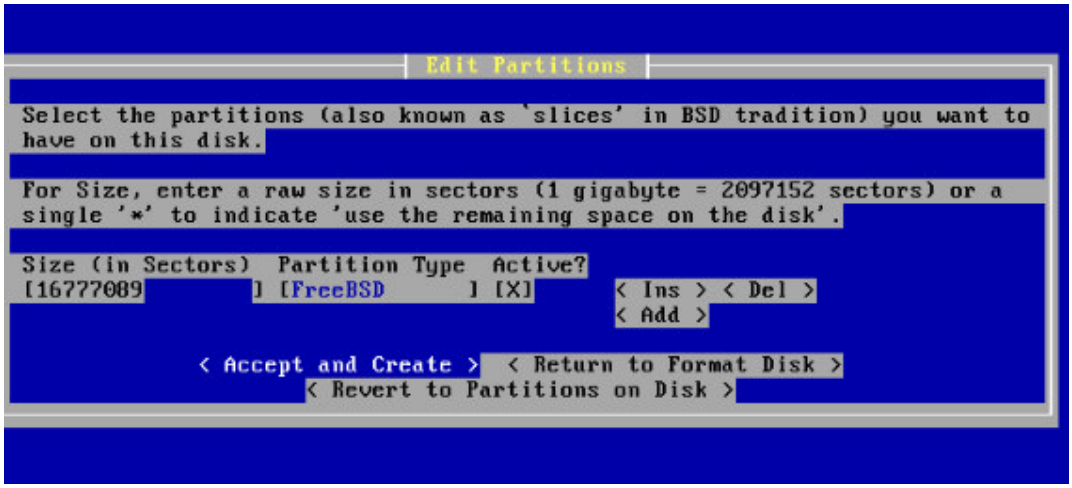


Figura 48: Creación de particiones.

Elaboración: Propia

Luego aparecerá la ventana donde indica autenticar si sigue deseando particionar, "¿partición de todos modos?"

Indica que: "No parece haberse producido ningún cambio en el diseño de la tabla de particiones". Lo que se hizo es ejecutar el comando para particionar el disco de todos modos, con la opción "si, particionar ada0".

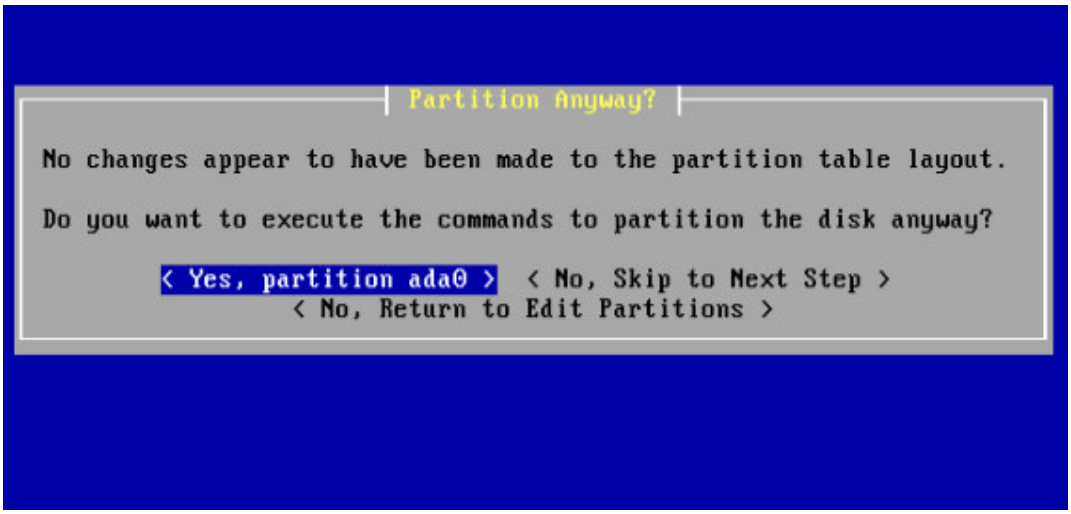


Figura 49: Confirmar el particionamiento del disco.

Elaboración: Propia

Después de aceptar que si se realizara la partición nos muestra una ventana donde nos muestra la información del disco como la cantidad de memoria y la velocidad de transición.

La única opción mostrada es la de aceptar, no hay un botón para retractarse sobre lo seleccionado anteriormente. Como indica en la figura 50 se seleccionó la opción "OK".

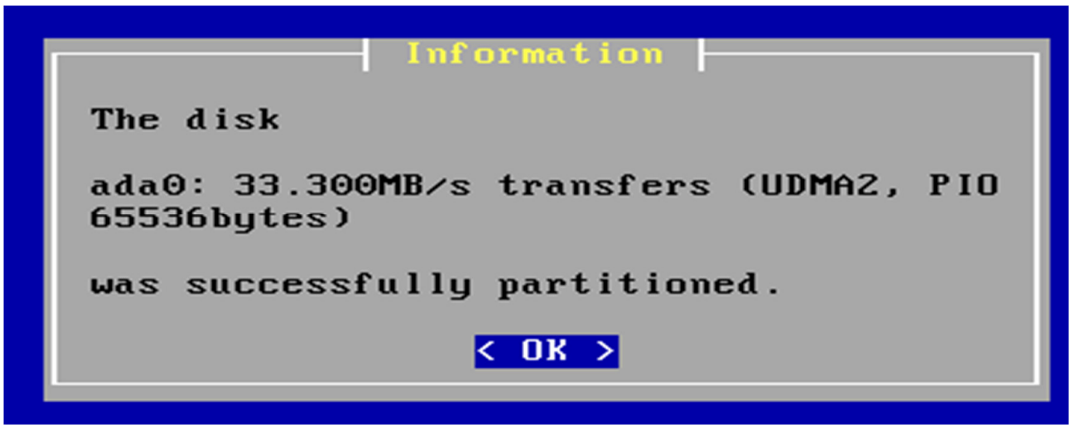


Figura 50: Partición efectuada.

Elaboración: Propia

Luego de terminar con la partición ya podemos instalar el Bootblock.

Ahora puede instalar bootblock en uno o más discos. Si ya tiene instalado un gestor de arranque, puede omitir este paso (pero puede que tenga que configurar el gestor de arranque por separado) si desea instalar pfSense en un disco su primer disco, tendrá que poner el bootblobck por lo menos en su primer disco y el disco pfSense

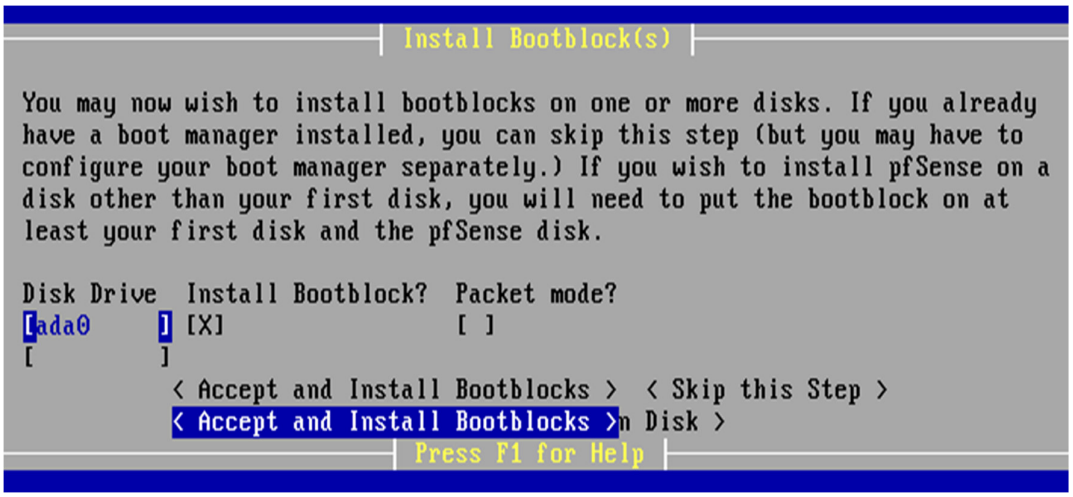


Figura 51: Creación de bootblocks.

Elaboración: Propia

Aceptamos e instalamos Bootblocks, también hay la opción de omitir este paso. Como se mostro en la partición hay un mensaje de confirmación para asegurarnos de la elección.

Figura 52: Confirmación de la creación de los bootblocks.

Elaboración: Propia

En la siguiente ventana nos da la opción de seleccionar las particiones deseadas para la instalación. Por lo tanto seleccione la partición primaria de ada0 (también conocida como "slice" en la tradición BSD) en la que instalar pfSense.

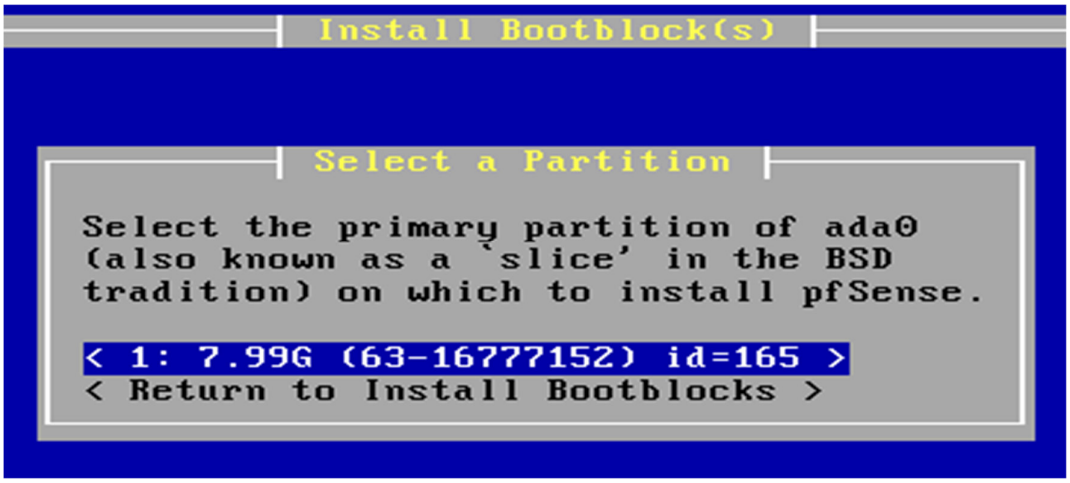


Figura 53: Seleccionamos partición primaria.

Elaboración: Propia

Se seleccionó la primera opción ya que es la única partición instalada con Bootblock, aparte de todo es la única partición.

Se puede observar que aún estamos en las ventanas de instalación de bootblock aún hay requisitos que piden para la instalación del sistema operativo.

Continuando se muestra la pregunta estas seguro?, en esto indica que toda la partición 1 va ser utilizada además señala que tiene toda la capacidad del disco, y al final indica que esto será irrevocable al borrarlo, por lo que señala seguridad en su elección, ya que es la última oportunidad.

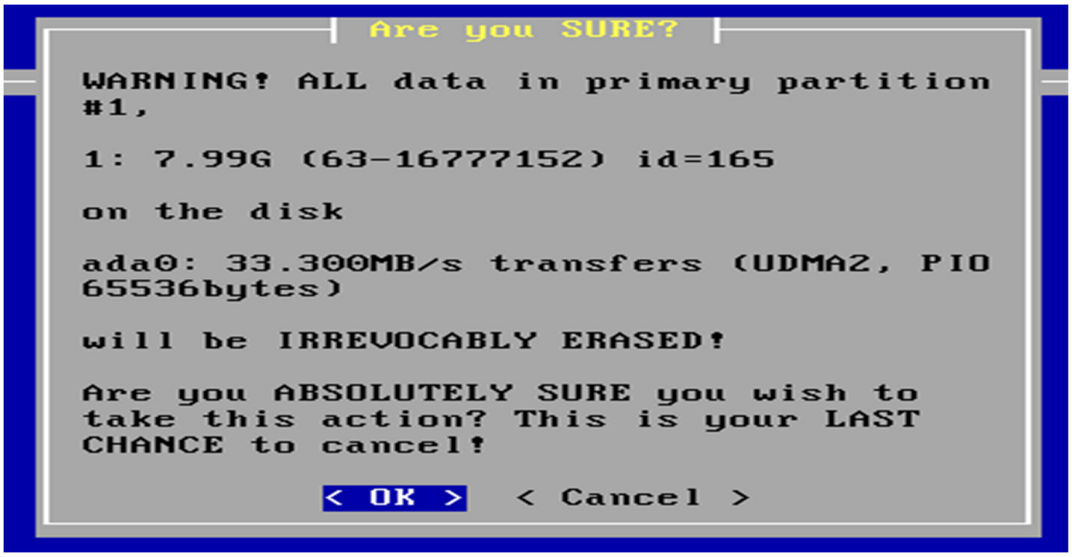


Figura 54: Confirmando la partición seleccionada.

Elaboración: Propia

Se muestra el mensaje de éxito donde e indica que la partición #1 ha sido formateado y ya es posible usarlo para la instalación de pfSense.

Figura 55: Partición formateada.

Elaboración: Propia

Con este procedimiento logramos formatear la partición. Y continuamos a los siguientes requisitos, cabe indicar que las particiones debes ser cuidadosamente realizadas junto al formateo de ellos o del disco entero.

En la figura 56 se realiza la selección de las subparticiones, configurando la subpartición que desea tener en esta partición primaria. Para uso de capacidad "M" para indicar megabytes, "G" para indicar gigabytes, o solo "*" para indicar "utilizar el espacio restante en la partición primaria".

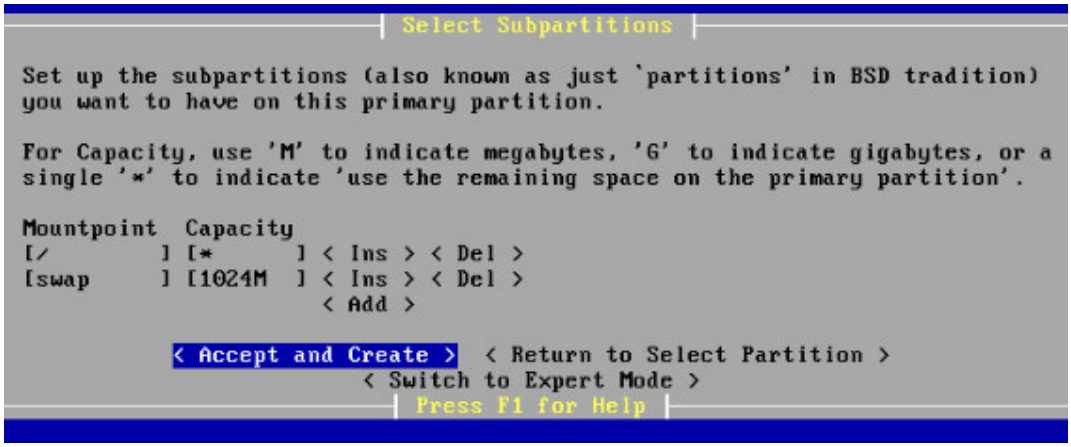


Figura 56: Aceptando la partición en donde se instalará Pfsense.

Elaboración: Propia

Como se ve en la figura 56 se puso "*" esto indica que se utilizó todo el espacio restante para la subpartición.

Luego de esto aparece la opción de instalar el kernel de sistema operativo ahora tu puede que desees instalar una configuración de kernel personalizada

Figura 57: Seleccionando configuración estándar.

Elaboración: Propia

Se observa dos opciones una es el kernel estándar y el otro es un kernel de núcleo incorporado la cual no admite la consola ni el teclado; por esta razón se elige la opción de kernel estándar.

Terminando con los requisitos para la instalación lo único que queda es el último paso la cual se muestra en la figura 58.

Figura 58: Reiniciando el sistema, Pfsense ya está instalado.

Elaboración: Propia

Esta máquina está a punto de ser cerrada. Después de que la máquina haya alcanzado su estado de apagado yo puede quitar el CD del CD-ROM o quitar la unidad USB y pulsar Enter para reiniciar desde HDD

ANEXO A2: CONFIGURACION: RED WAN.

Despues de reiniciar el ordenador se mostro la pantalla de consola como indica en la figura 59.

Figura 59: Primera figura después de instalar Pfsense.

Elaboración: Propia

Como indica en la figura 60 se procede a seleccionar la opción 2 para la asignación de IP a sus interfaces.

Se puede ver en la figura que hay varias opciones de configuración también que para la selección de una dirección estática se usara os comandos *em0* para la interface de la red WAN y *em1* el interface para la red LAN.

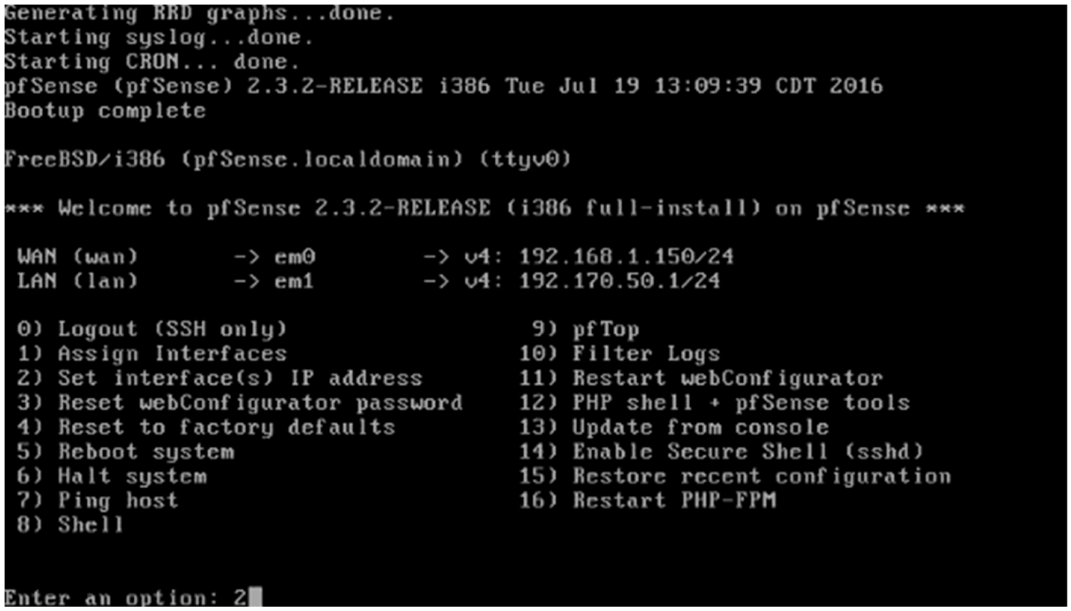


Figura 60: Asignación de IP estática a la red WAN.

Elaboración: Propia

Después de seleccionar la opción dos nos ofrecerán la opción de escoger entre la interface de la red LAN o WAN.

Como indica en la figura 41 se observa las opciones:

- 1 para elegir WAN
- 2 para elegir LAN

Por ahora elegiremos la opción 1 para iniciar con la interface WAN

Figura 61 Configuración de red WAN.

Elaboración: Propia

Luego a eso nos preguntara: configurar la dirección IPv4 del interface WAN atreves de DHCP? En esta investigación no tenemos implementado un servidor DHCP, por lo que negamos esta pregunta escribiendo “n”.

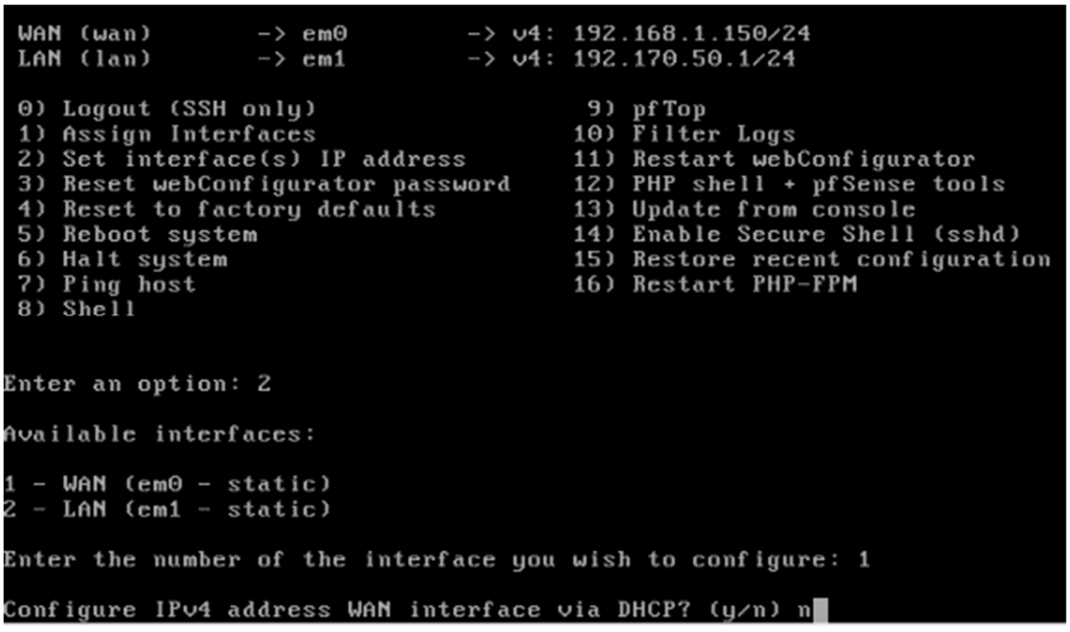


Figura 62: Configuración de dirección WAN IPv4 vía DHCP denegada.

Elaboración: Propia

Posterior a eso la siguiente petición es ingresar una nueva dirección IPv4 y presionar Enter cuando ya este, la elección es una dirección privada, lo cual no es importante ya que es con fines de investigación.

En la figura 63 se muestra que la dirección IPv4 es 192.168.1.150

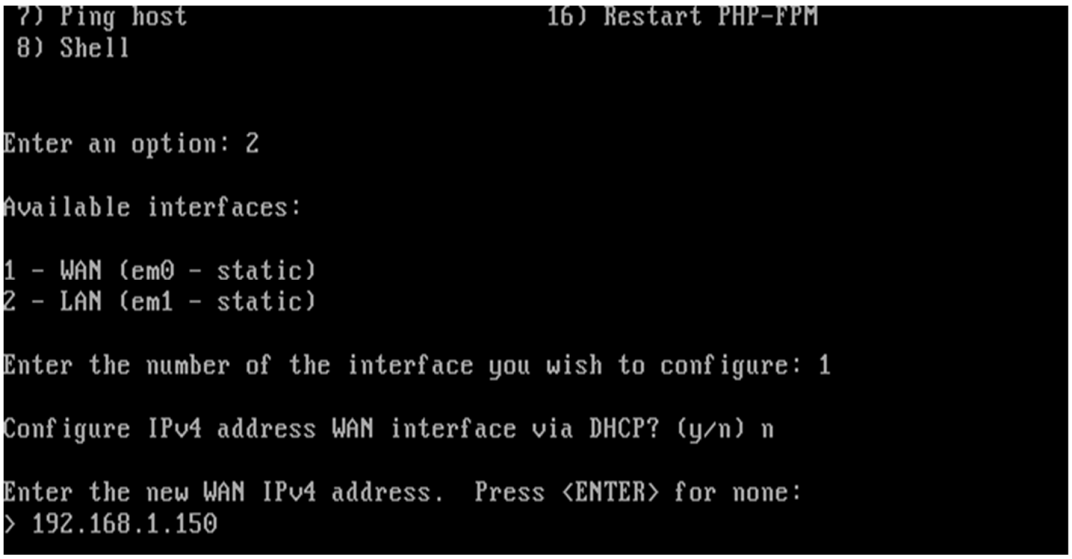


Figura 63: Elección de una IP estática.

Elaboración: Propia

Luego de esto nos pide el prefijo de la máscara de red, en la cual nos da tres ejemplos:

- 255.255.255.0=24
- 255.255.0.0=16
- 255.0.0.0=8

Nuestra mascara será lo que es usado en la IPs privadas es decir 255.255.255.0 por lo cual el prefijo es 24.

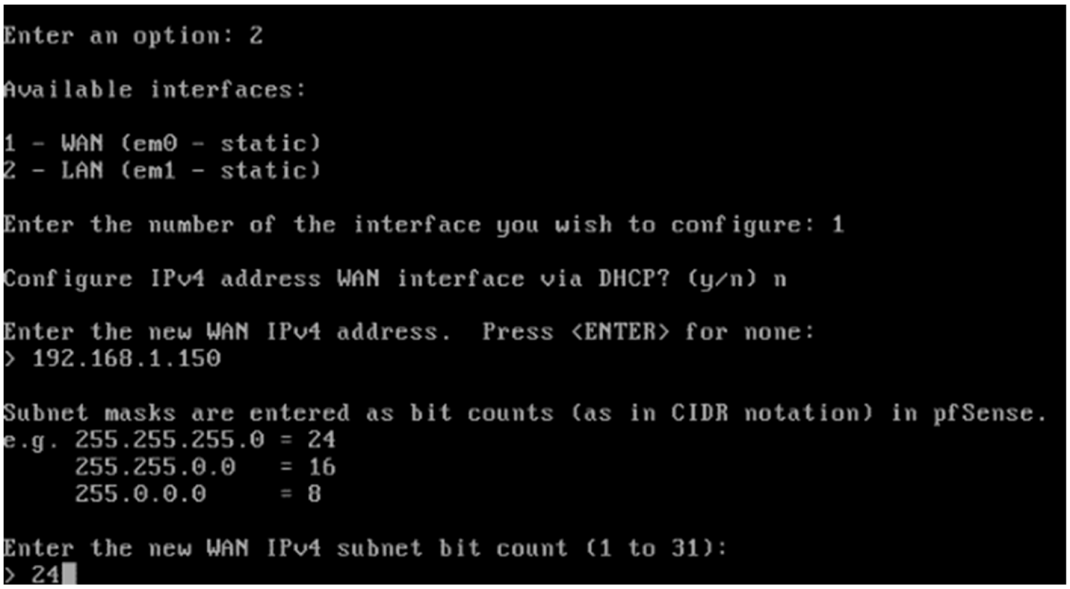


Figura 64: Elección de una máscara de red.

Elaboración: Propia

Luego de esto hay la opción de escribir la dirección de puerta de enlace lo cual ignoraremos ya que este ordenador cumplirá la función de enrutador. Y tal como los pasos anteriores para IPv4 también hay para IPv6.

En IPv6 ignoraremos todo relacionado con este protocolo como elegir si usar DHCPv6 o ingresar la dirección IPv6. Posteriormente toda la configuración es guardada.

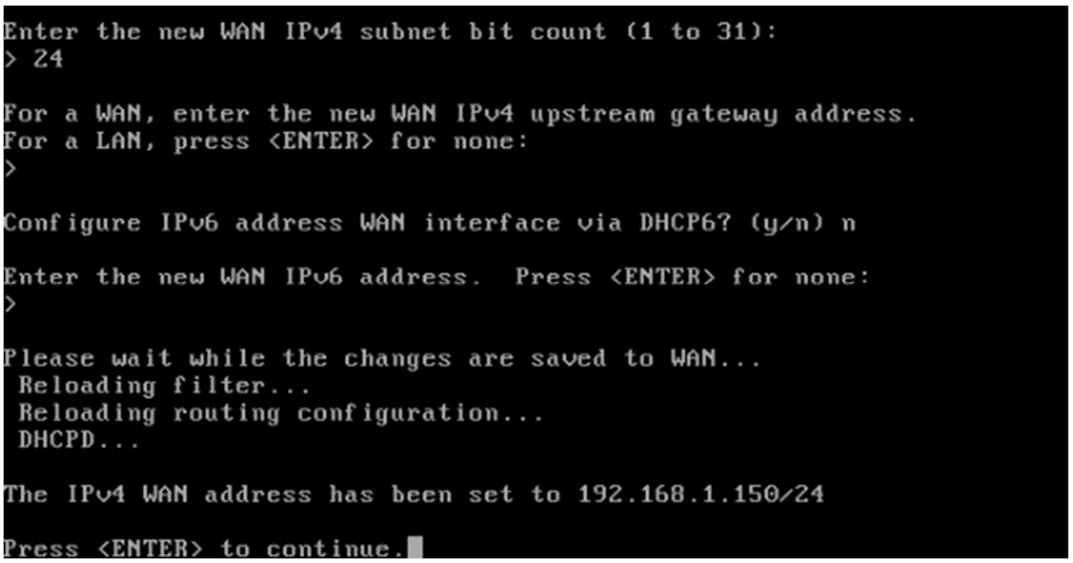


Figura 65: Opciones denegadas: introducción de Gateway y Configuración de IPv6.

Elaboración: Propia

ANEXO A3: CONFIGURACION DE RED LAN.

Como indicaba en la figura 66 se procede a seleccionar la opción 2 para la asignación de IP a sus interfaces

Se puede ver en la figura que hay varias opciones de configuración también que para la selección de una dirección estática se usara os comandos *em0* para el interface de la red WAN y *em1* el interface para la red LAN.

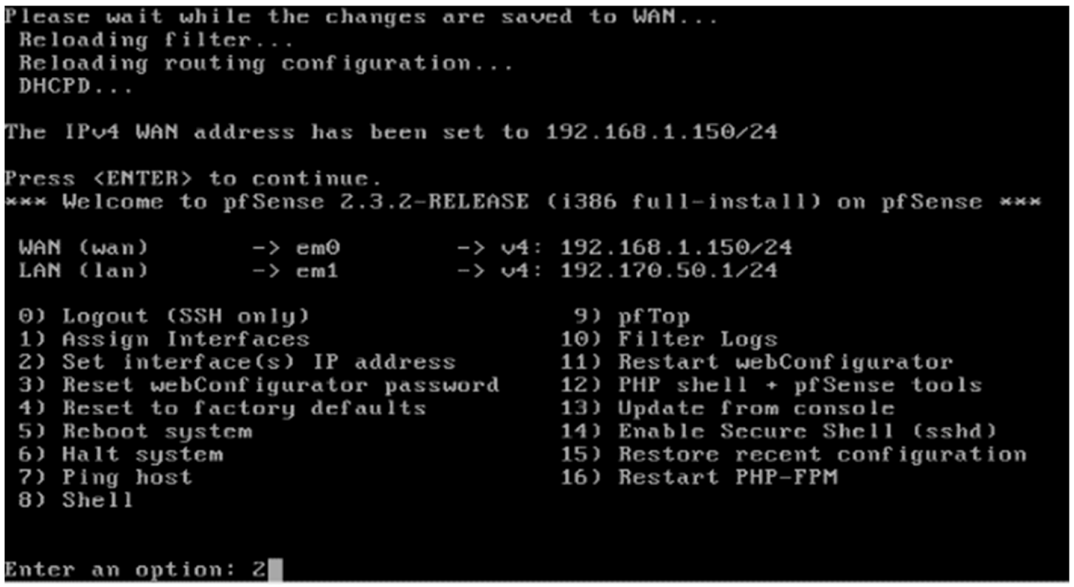


Figura 66: Configuramos la red LAN.

Elaboración: Propia

También en la figura 67 se observa las opciones:

- 1 para elegir WAN
- 2 para elegir LAN

Pero ahora elegiremos la opción 2 para iniciar con la interface WAN

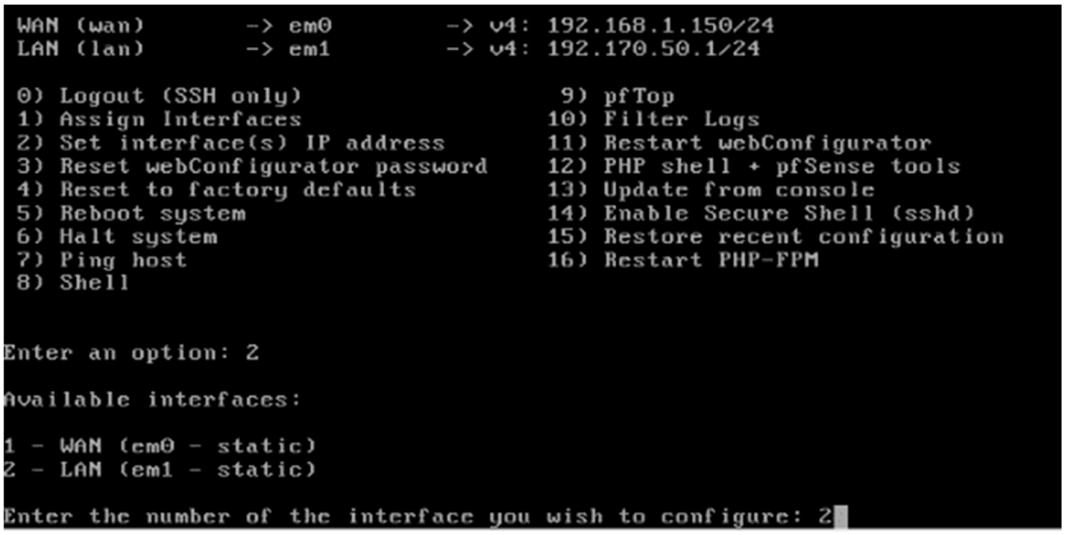


Figura 67: Confirmación de la configuración de la red LAN.

Elaboración: Propia

Posterior a eso la siguiente petición es ingresar una nueva dirección IPv4 y presionar Enter cuando ya este, la elección es una dirección privada, lo cual no es importante ya que es con fines de investigación.

En la figura 68 se muestra que la dirección IPv4 es 192.170.50.1

Figura 68: Asignación de una dirección de IP estática a la red LAN.

Elaboración: Propia

Luego de esto nos pide el prefijo de la máscara de red, en la cual nos da tres ejemplos:

- 255.255.255.0=24
- 255.255.0.0=16
- 255.0.0.0=8

Nuestra mascara será lo que es usado en la IPs privadas es decir 255.255.255.0 por lo cual el prefijo es 24.

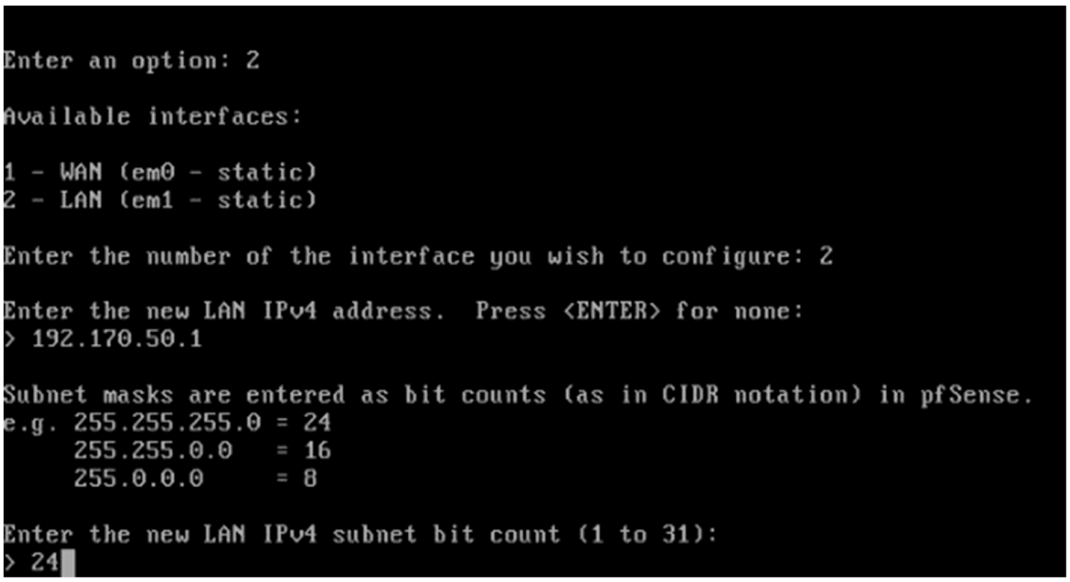


Figura 69: Introducción de mascara de red.

Elaboración: Propia

Luego de esto hay la opción de escribir la dirección de puerta de enlace lo cual ignoraremos ya que este ordenador cumplirá la función de enrutador. Y tal como los pasos anteriores para IPv4 también hay para IPv6.

En IPv6 ignoraremos todo relacionado con este protocolo como elegir si usar DHCPv6 o ingresar la dirección IPv6. Posteriormente toda la configuración es guardada.

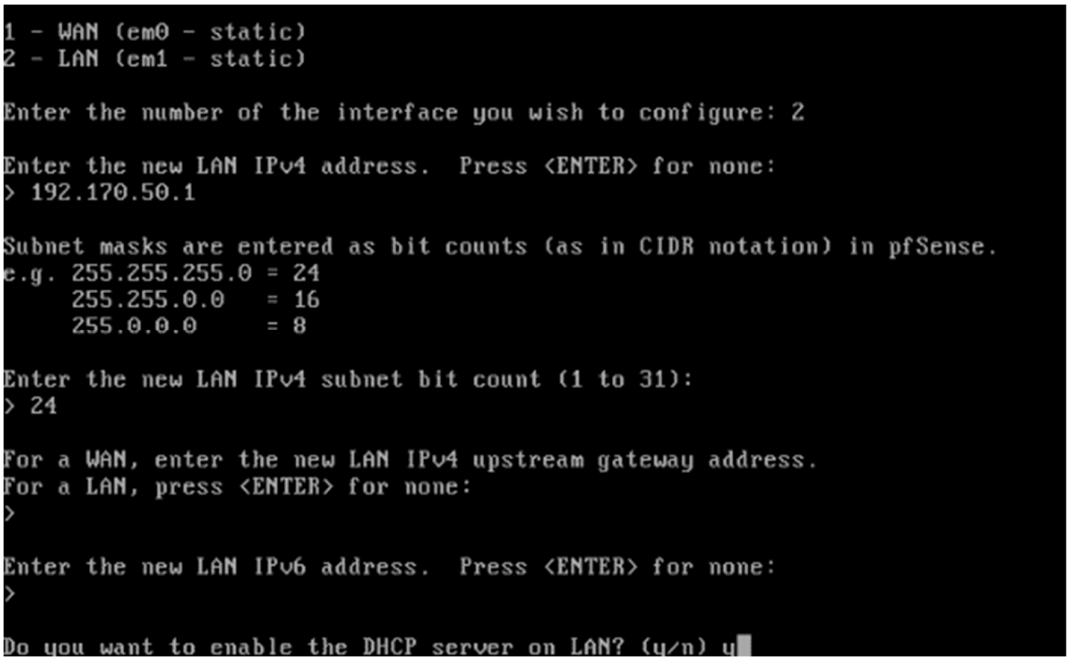


Figura 70: Omisión de las opciones de: Introducción de Gateway e introducción de dirección IPv6.

Elaboración: Propia

Posterior a eso se nos pide que ingresemos un rango de direcciones IP esto para los clientes. Esto se asignara mediante un servidor DHCP.

El rango inicia desde la dirección IP 192.168.50.10 hasta la dirección IP 192.170.50.250 es dirección tiene una cantidad de 199 direcciones IP lo cual está bien, ya que esta menos del rango máximo para una máscara de red de prefijo de 24, ya que es equivalente a 255 direcciones libres.

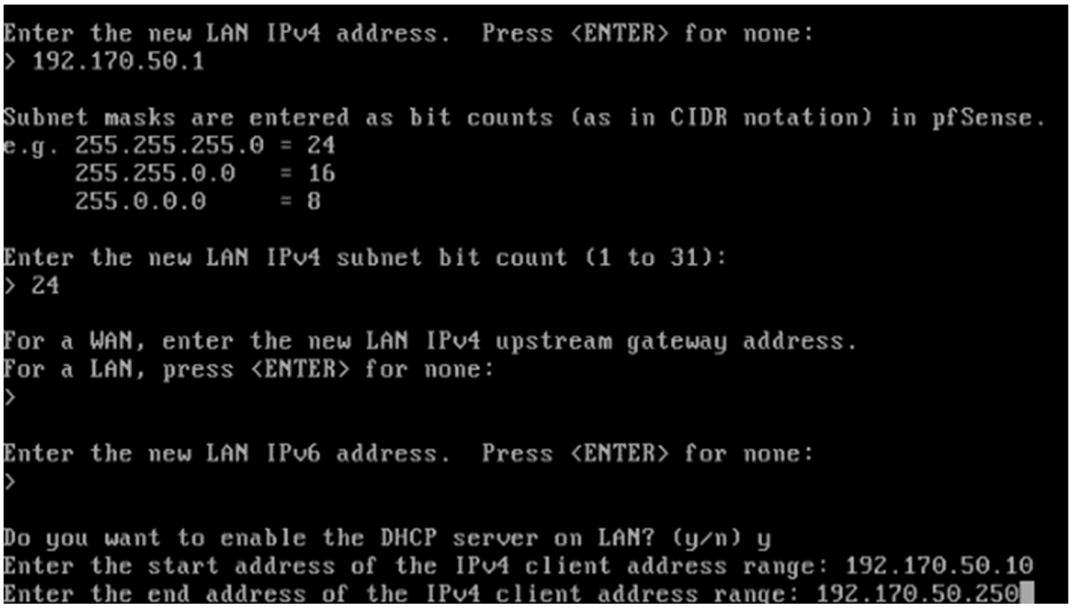


Figura 71: Estableciendo un rango de IP.

Elaboración: Propia

Luego de terminar todo los requisitos el servidor guardara sus configuraciones indicando que contiene la dirección IP 192.168.70.1 con mascara de red 255.255.255.0 o el prefijo 24.

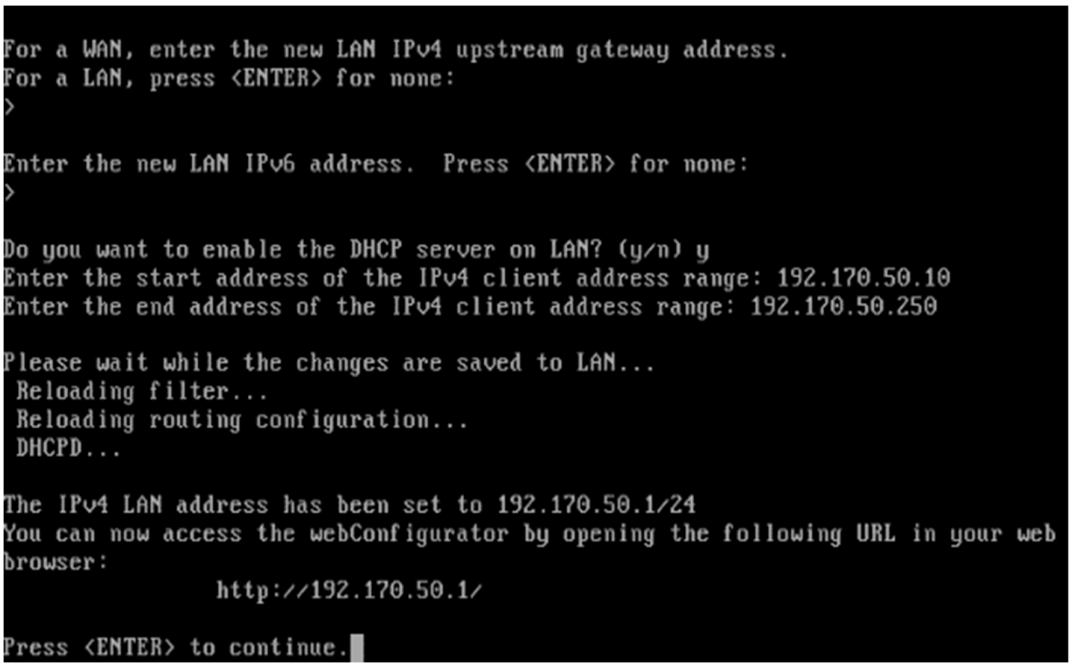


Figura 72: Culminación de la configuración de la red LAN.

Elaboración: Propia

Al terminar la configuración se puede observar la configuración de los interfaces WAN y LAN, resumiendo se observa que:

- WAN de em0 tiene la dirección IPv4 192.168.1.150 de mascara de red 255.255.255.0 prefijo 24.
- RED-ALUMNOS de em1 tiene la dirección IPv4 192.170.50.1 de mascara de red 255.255.255.0 prefijo 24.

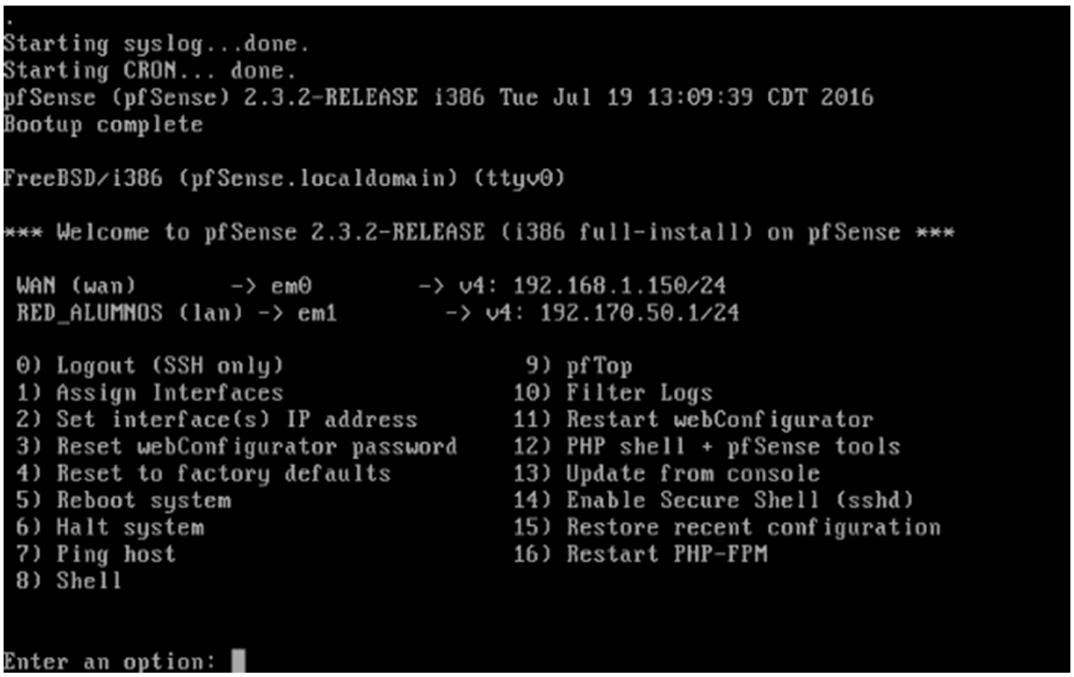


Figura 73: Configuración completa de la red WAN y la red LAN.

Elaboración: Propia

ANEXO A4: CONFIGURACIÓN MEDIANTE INTERFAZ GRAFICA

Se procede a ingresar al servidor mediante ordenador que este en la red, usando un navegado lo cual puede ser cualquiera, con tal que este desactivado el cortafuego o proxy. Para ingresar solo es necesario escribir la dirección IP del servidor es decir 192.170.50.1 y luego entrar lo que nos mostrara la pantalla de pfSense, en la cual nos pide un usuario y clave de autenticación. El usuario es

USERNAME: admin

PASSWORD: pfsense

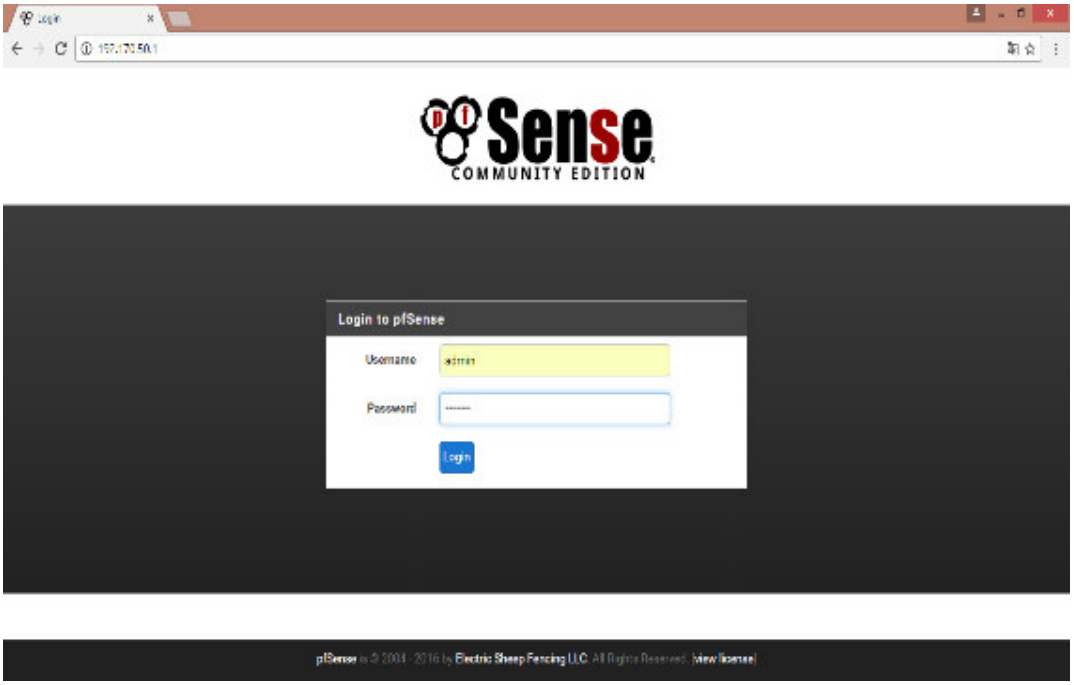


Figura 74: Configuración mediante interfaz gráfica, usuario y contraseña.

Elaboración: Propia

Luego de ingresar la contraseña ingresara a la pantalla que se muestra en la figura 74, donde se muestran varias pestañas como cortafuego, service VPN y mas

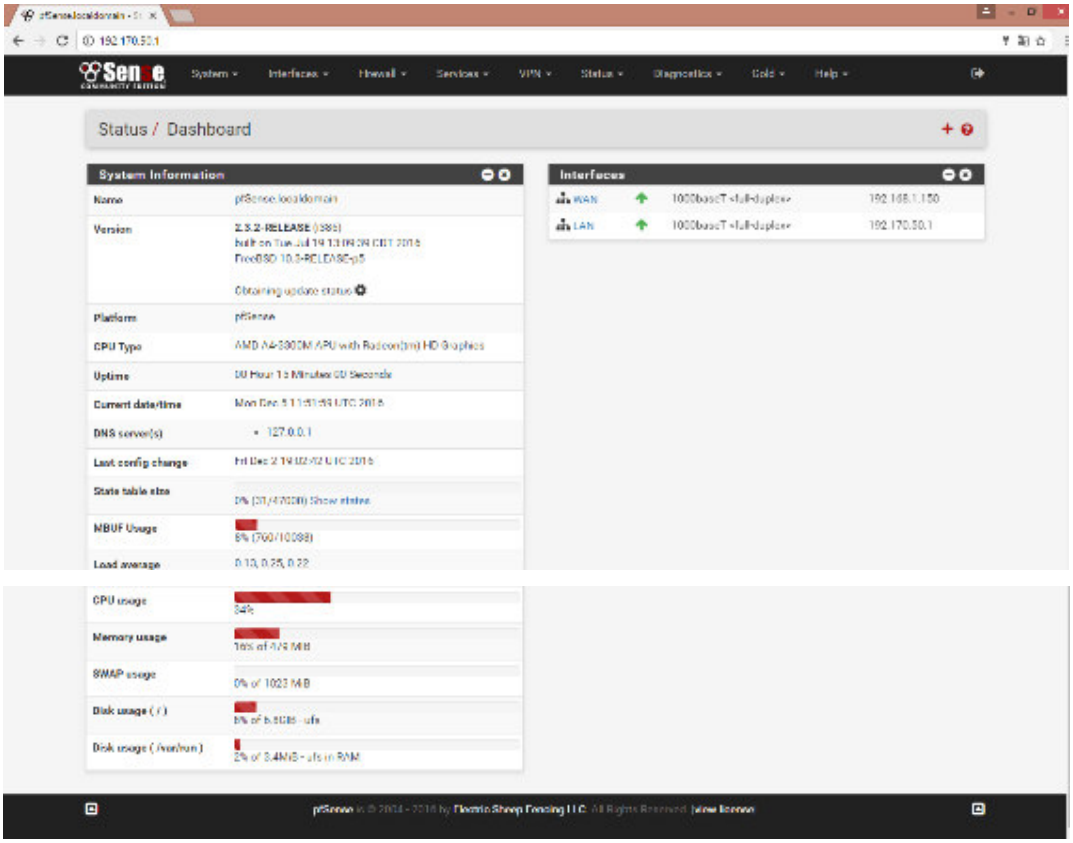


Figura 75: Interfaz principal de Pfsense.

Elaboración: Propia

Después de haber instalado el Pfsense en el disco duro y haber configurado los parámetros iniciales, procederemos a configurar las reglas de cortafuego las cuales se aplican a las interfaces configuradas previamente.

Antes de empezar a configurar las reglas de cortafuego es necesario tener clara la topología de la red donde está participando el Pfsense y de qué forma

Después ingresamos al submenú Rules desde el menú Cortafuego ubicado en la barra de menús de la interfaz gráfica de configuración del PFSense.

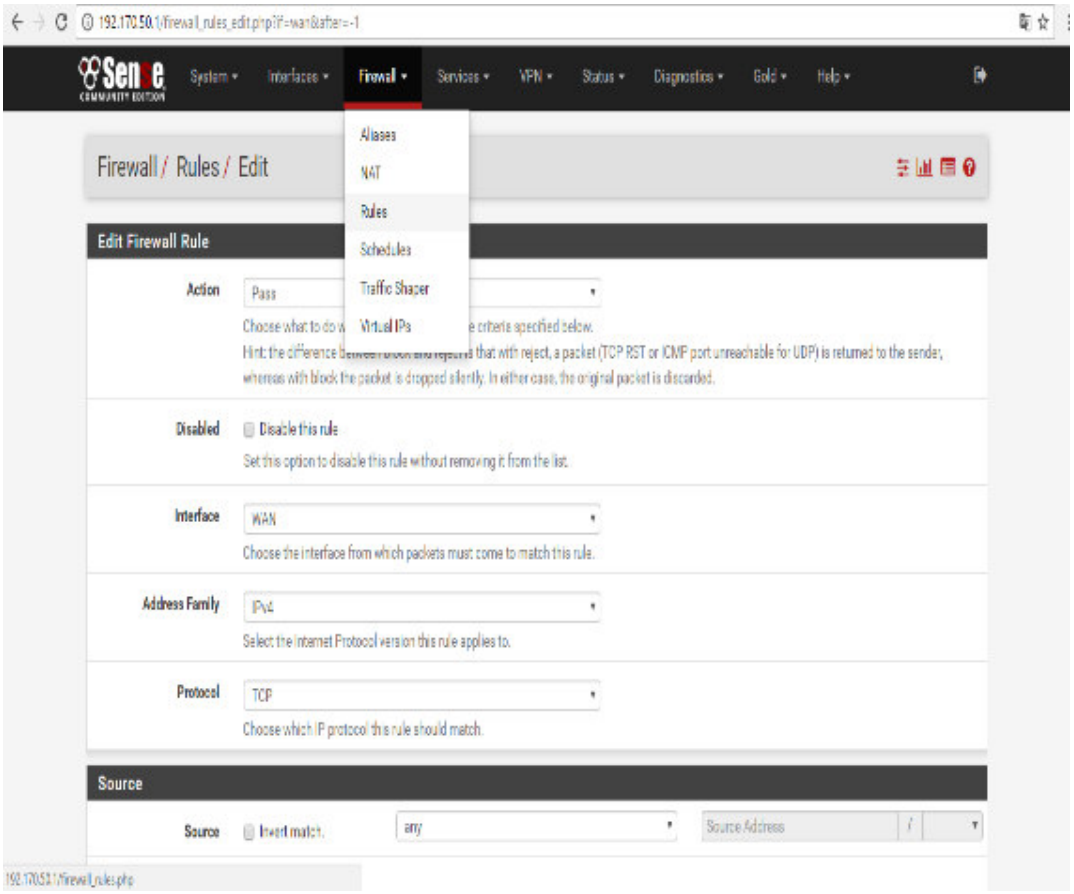


Figura 76: Estableciendo reglas para bloquear algunas páginas.

Elaboración: Propia

Al ver que no tenemos ninguna regla configurada podemos visualizar que están las dos interfaces LAN y WAN, en la parte inferior se encuentran las convenciones que indican cada uno de los estados de la regla:

PASS Permitir

PASS (Disabled) Permitir Deshabilitado

BLOCK Bloquear

BLOCK (Disabled) Bloquear Deshabilitado

Reject Rechazar

Reject (Disabled)

Log Hacer seguimiento en archivo de log

Log (Disabled) Hacer seguimiento en archivo de log deshabilitado

Si se bloquea, simplemente se ignora el paquete de información que se está recibiendo. Si se rechaza, se comunica al emisor que no se quiere el paquete.

Por tanto, normalmente se bloquea. ¿Por qué? Pues porqué bloquear es silencioso, es no hacer caso al emisor y nada más.

En la parte derecha de la pantalla de pfsense hay un icono que dice agregar nueva regla con la siguiente forma damos clic ahí para crear una nueva regla de cortafuego. Bloquearemos páginas web como redes sociales, YouTube, etc. Entramos a cortafuego – RULES.

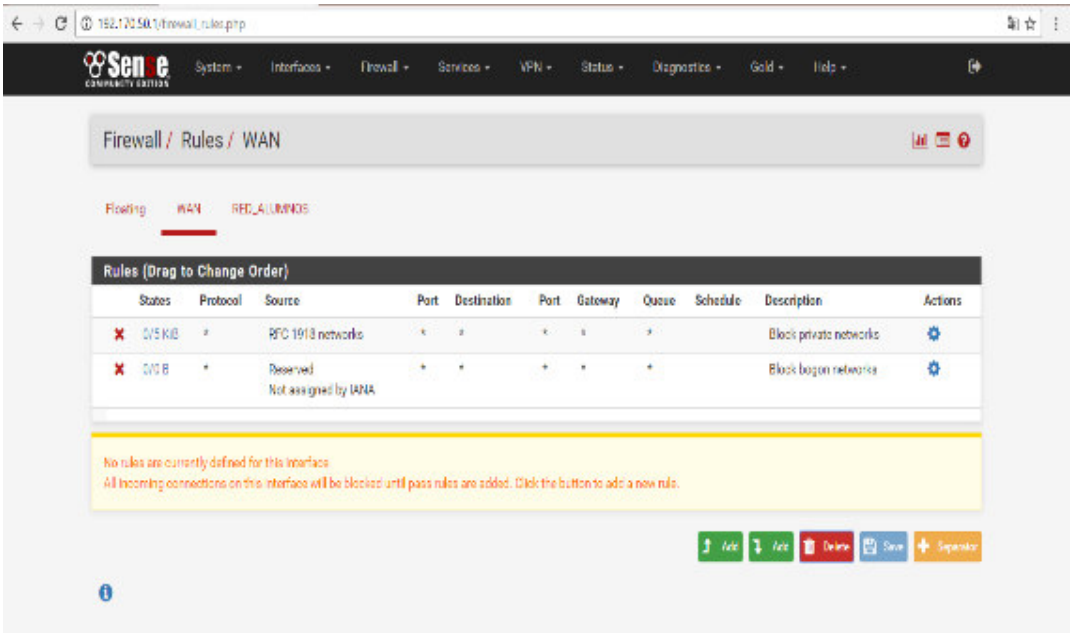


Figura 77: Agregando algunas reglas, para empezar a bloquear páginas.

Elaboración: Propia

Luego nos saldrá una pantalla con los siguientes parámetros los cuales serán definidos a continuación:

Action: Permite seleccionar que hacer con los paquetes que coinciden con el criterio seleccionado debajo en las siguientes opciones de filtrado (pass, blocked, Reject).

Disabled: Permite deshabilitar temporalmente esta regla sin ser eliminada, esto con el objetivo de administración de la red y gestión de servicios de red.

Interface: En este campo se configura a que interfaz ira aplicada la regla de cortafuego ya sea LAN, WAN, O DMZ.

Protocol: Especifica que protocolo de capa 4 se va a utilizar en el filtrado de paquetes en la regla de cortafuego (TCP, UDP, ICMP).

Source: Aquí se configura la dirección de red, o de host origen y en avanzadas se coloca el puerto de origen adicional al origen.

Source OS: En esta opción se puede filtrar el sistema operativo el cual solo funciona con el protocolo TCP.

Destination: Es la dirección de red, o de host de destino donde llegara el paquete y también tiene las mismas opciones avanzadas de configuración por puerto.

Destination Log: Selecciona los rangos de puertos para la entrega de paquetes en esta regla por protocolo de capa 7.

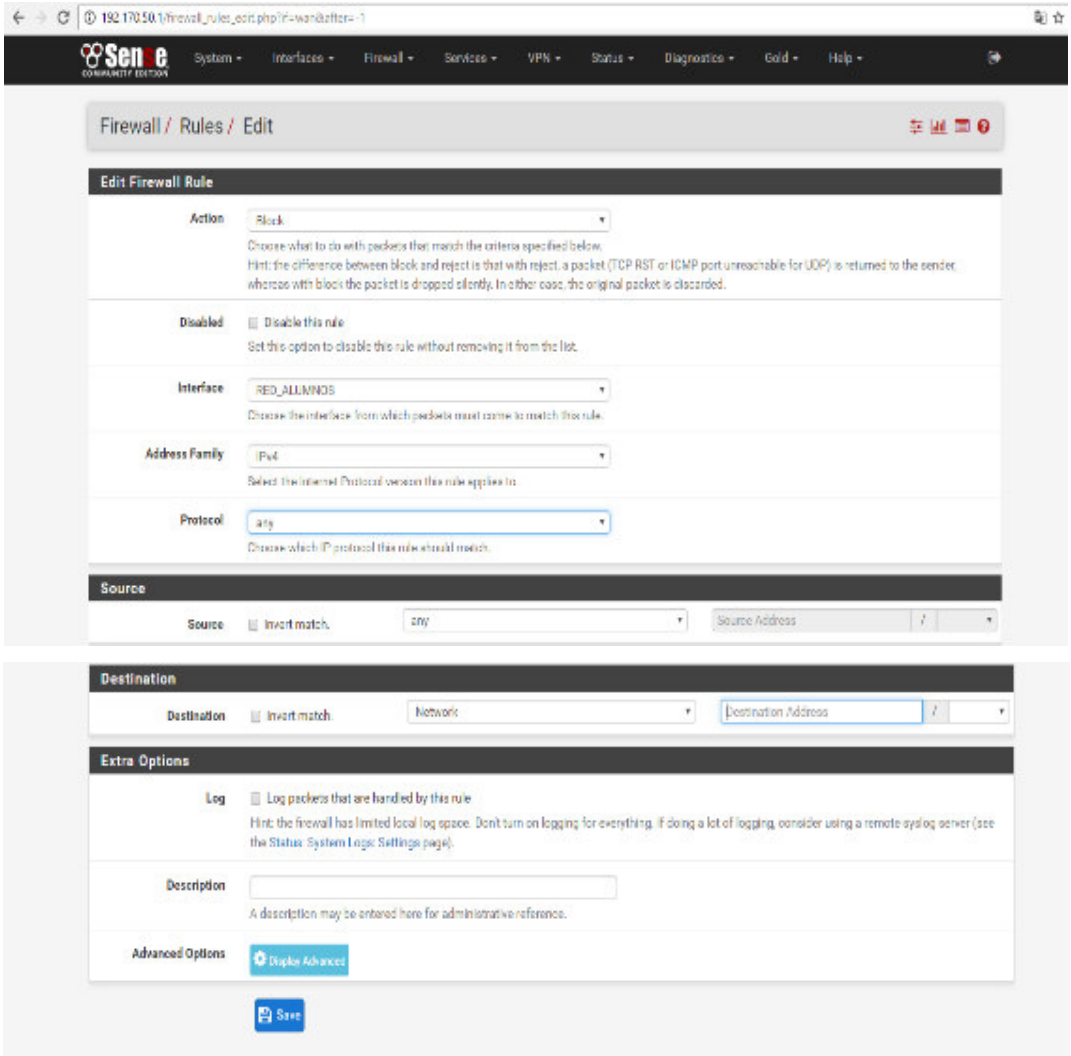


Figura 78: Configuración de la red LAN.

Elaboración: Propia

ANEXO B1: POLÍTICA DE SEGURIDAD INFORMÁTICA

ANEXO B2: PERSONAS

Los funcionarios y la seguridad informática

La responsabilidad por la seguridad de la información no sólo corresponde a las áreas de seguridad informática, sino que es una obligación de cada funcionario.

Códigos de identificación y claves

a) Los mecanismos de acceso que les sean otorgados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento legal o medie un procedimiento de custodia de llaves. De acuerdo con lo anterior, los usuarios no deben obtener las claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido.

b) Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario y clave personal.

Control de la Información

a) Los usuarios deben informar inmediatamente al área que corresponda dentro de la institución toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.

b) Los usuarios no deben instalar software en sus computadores o en servidores sin las debidas autorizaciones.

c) Los usuarios no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la institución en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

d) Los funcionarios no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas. Esto incluye los controles del sistema de información y su respectiva implementación.
e) Los funcionarios no deben destruir, copiar o distribuir los archivos de la institución sin los permisos respectivos.
f) Todo funcionario que utilice los recursos de los sistemas tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

Otros usos

Los computadores, sistemas y otros equipos deben usarse sólo para las actividades propias de la entidad, por lo tanto los usuarios no deben usar sus equipos para asuntos personales a menos que exista una autorización respectiva que avalúe el riesgo informático de tal labor. La institución debe tener definido un código de ética para la seguridad informática, el cual debe incluir tópicos relacionados con la seguridad informática y de datos.

ANEXO B3: SOFTWARE

Los empleados con funciones y responsabilidades para con el software institucional deben seguir los siguientes lineamientos para proteger este activo y la información que a través de él se maneje.

Administración del Software

a. La institución debe contar en todo momento con un inventario actualizado del software de su propiedad, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento, el entregado y el recibido en comodato. Las licencias se almacenarán bajo los adecuados niveles de seguridad e incluidas en un sistema de administración, efectuando continuos muestreos para garantizar la consistencia de la información allí almacenada. Igualmente, todo el software y la documentación del mismo que posea la institución incluirán avisos de derechos de autor y propiedad intelectual.

b. Todas las aplicaciones se clasificarán en una de las siguientes categorías: Misión Crítica, Prioritaria y Requerida. Para las de misión crítica y prioritaria

deberá permanecer una copia actualizada y su documentación técnica respectiva, como mínimo en un sitio alterno y seguro de custodia.

c. Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de producción de la institución, se modificarán únicamente por el personal autorizado, de acuerdo con los procedimientos internos establecidos y en todos los casos, y se considerarán planes de contingencia y recuperación.

Adquisición del Software

a) El software contará con acceso controlado que permita al propietario del recurso restringir el acceso al mismo. El software protegerá los objetos para que los procesos y/o los usuarios no los puedan acceder sin los debidos permisos. Cada usuario se identificará por medio de un único código de identificación de usuario y clave, antes de que se le permita el acceso al sistema.

Parametrización

a) Con el propósito de asegurar la integridad de la información, la función de Parametrización del software estará a cargo de un equipo interdisciplinario. Para el caso de aplicaciones de misión crítica y prioritaria, el grupo interdisciplinario representará a los diferentes usuarios e incluirá al proveedor. Para el paso del software al ambiente de pruebas, el documento final de Parametrización del software contará previamente con las aprobaciones correspondientes al interior de la Institución.

Desarrollo de Software

a) La institución deberá tener una metodología formal para el desarrollo de software de los sistemas de información de misión crítica y prioritaria, desarrollos rápidos del mismo y las actividades de mantenimiento, las cuales cumplirán con las políticas, normas, procedimientos, controles y otras convenciones estándares aplicables en el desarrollo de sistemas. Los controles desarrollados internamente deberán ser como mínimo el plan de cuentas, el plan de auditoría y el cierre de puertas traseras. Adicionalmente, toda solicitud de modificación al software deberá contar con estudios de

factibilidad y de viabilidad al igual que las autorizaciones respectivas dentro de la institución.

b) Con el propósito de garantizar integridad y confidencialidad de la información que administrará el software desarrollado y antes del paso a pruebas, se deberán ejecutar las pruebas intrínsecas al desarrollo y a la documentación técnica respectiva. Para todo desarrollo de software se deberán utilizar herramientas, de las cuales se tengan certeza que su comportamiento es seguro y confiable. Solamente las funciones descritas en el documento aprobado de especificaciones de la solución tecnológica podrán ser desarrolladas
c) Los programadores de software no deberán conocer las claves utilizadas en ambientes de producción.
d) Los desarrollos y/o modificaciones hechos a los sistemas de aplicación no deberán trasladarse al ambiente de producción si no se cuenta primero con la documentación de entrenamiento, operación y de seguridad adecuados. La suficiencia de este material deberá ser determinada por los usuarios responsables en la institución.

Pruebas de Software

a) Un equipo especializado deberá hacer las pruebas en representación de los usuarios finales. El área de desarrollo de sistemas deberá entregar el software desarrollado con códigos fuentes al área responsable de ejecutar las pruebas, el cual deberá ser revisado para encontrar códigos mal intencionado y debilidades de seguridad utilizando preferiblemente herramientas automáticas, para luego ser compilado e iniciar las pruebas correspondientes.
b) Los tipos de pruebas deberán ser previamente establecidos. Para garantizar la integridad de la información en producción éstas deberán ser debidamente planeadas, ejecutadas, documentadas y controlados sus resultados, con el fin de garantizar la integridad de la información en producción. Además, el ambiente de pruebas deberá ser lo más idéntico, en su configuración, al ambiente real de producción.

c) Las pruebas sobre el software desarrollado tanto interna como externamente deberán contemplar aspectos funcionales, de seguridad y técnicos. Adicionalmente, se incluirá una revisión exhaustiva a la documentación mínima requerida, así como la revisión de los procesos de retorno a la versión anterior. En caso de que se requirieran las claves de producción para ejecutar pruebas, su inserción y mantenimiento se deberá efectuar de manera segura. Se deberá poseer un cronograma para la ejecución de las pruebas con el fin de cumplir con los compromisos institucionales acordados. Éste podrá verse afectado en su calendarización por aquellos eventos en que se tengan que atender desarrollos rápidos únicamente por exigencias mandatorias de entes superiores.

Implantación del Software

a) Para implantar un software mediará una autorización por escrito del responsable para tal fin. Las características que son innecesarias en el ambiente informático se identificarán y desactivarán en el momento de la instalación del software.
b) Antes de implementar el software en producción se verificará que se haya realizado la divulgación y entrega de la documentación, la capacitación al personal involucrado, su licenciamiento y los ajustes de parámetros en el ambiente de producción. Deberá existir un cronograma de puesta en producción con el fin de minimizar el impacto del mismo.
c) Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo ni la de producción.
d) Los programas en el ambiente de producción serán modificados únicamente por personal autorizado y cuando se requiera por fuerza mayor de acuerdo con las normas institucionales establecidas.

Mantenimiento del Software

a) El área de desarrollos de sistemas no hará cambios al software de producción sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos. A su vez, se contará con un procedimiento de

control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

b) La documentación de todos los cambios hechos al software se preparará simultáneamente con el proceso de cambio. Se deberá considerar, además, que cuando un tercero efectúe ajuste al software, éste deberá firmar un acuerdo de no divulgación y utilización no autorizada del mismo.

c) Para cada mantenimiento a la versión del software de misión crítica y prioritaria se actualizará el depositado en custodia en el sitio alterno y el respaldado en la institución. Este software y su documentación se verificarán y certificará su actualización.

ANEXO B4: POLÍTICA DE HARDWARE

La administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones debe adoptar los siguientes criterios para proteger la integridad técnica de la institución.

Cambios al Hardware

a) Los equipos computacionales de UNITEK no deben ser alterados ni mejorados (cambios de procesador, memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del área responsable (Soporte Computacional).

b) Los funcionarios deben reportar a los entes pertinentes de UNITEK sobre daños y pérdida del equipo que tengan a su cuidado y sea propiedad de UNITEK. La intervención directa para reparar el equipo debe estar expresamente prohibida. UNITEK debe proporcionar personal interno o externo para la solución del problema reportado.

c) Todos los equipos de la entidad deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación.

d) Todo el hardware que adquiera la institución debe conseguirse a través de canales de compra estándares.

e) Para todos los equipos y sistemas de comunicación utilizados en procesos de producción en la entidad, se debe aplicar un procedimiento formal de control de cambios que garantice que sólo se realicen los cambios

autorizados. Este procedimiento de control de cambios debe incluir la documentación del proceso con las respectivas propuestas revisadas, la aprobación de las áreas correspondientes y la manera como el cambio fue realizado.

f) Todos los productos de hardware deben ser registrados por proveedor y contar con el respectivo contrato de mantenimiento.

g) Los equipos computacionales, sean estos PC, servidores, LAN, etc. no deben moverse o reubicarse sin la aprobación previa del Administrador o Jefe del área involucrada.

Acceso Físico y Lógico

a) Antes de conectarlos a la red interna todos los servidores de Intranet de UNITEK deben ser autorizados por el área responsable del hardware.

b) Todos los computadores multiusuario y los equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir alteraciones y usos no autorizados.

c) Las bibliotecas de cintas magnéticas, discos y documentos se deben ubicar en áreas restringidas en el DataCenter y en sitios alternos con acceso únicamente a personas autorizadas.

d) Todas las conexiones con los sistemas y redes de la entidad deben ser dirigidas a través de dispositivos probados y aprobados por la organización y contar con mecanismos de autenticación de usuario.

e) Los equipos de computación de UNITEK deben ser protegidos por mecanismos de control aprobados por el área de seguridad informática y de datos.

f) Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de UNITEK deben ser restringidas.

g) Todas las líneas que permitan el acceso a la red de comunicaciones o sistemas multiusuario deben pasar a través de un punto de control adicional (firewall) antes de que la pantalla de login aparezca en la terminal del usuario.

Respaldo y Continuidad del Negocio

a) La administración debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de computación críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios y sistemas de aire acondicionado, entre otros.

b) Los equipos del DataCenter se deben equipar con unidades suplementarias de energía eléctrica (UPS y Grupo Electrógeno).

c) El diseño de la red de comunicaciones debe estar de tal forma que se evite tener un punto crítico de falla, como un centro único que cause la caída de todos los servicios.

d) Los backups de los sistemas de computación y redes deben ser almacenados en una zona de fuego diferente de donde reside la información original. Las zonas de fuego varían de edificio a edificio y son definidas por el área de seguridad de UNITEK.

e) A todo equipo de cómputo, comunicaciones y demás equipos de soporte debe realizársele un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.

f) Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.

ANEXO B5: POLITICA DE INSTALACIONES FISICAS

Todos los funcionarios de UNITEK deberán seguir los siguientes lineamientos de seguridad física con el fin de salvaguardar los recursos técnicos y humanos de UNITEK.

Control de acceso físico

UNITEK debe contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control inteligente y sistemas de alarmas en las dependencias que se consideren críticas.

Personas

a) Los visitantes deben permanecer escoltados y portar un distintivo o escarapela claramente visible, y las personas que laboran para UNITEK que requieran ingresar a áreas críticas también deben permanecer escoltados. Además, tanto los visitantes como los empleados mencionados únicamente deben tener la información y recursos necesarios para el desarrollo de sus actividades.

b) En el evento que los funcionarios dejen de tener vínculos laborales con la entidad todos sus códigos de acceso deben ser cambiados o desactivados. Además, en caso de pérdida de la escarapela o tarjeta de acceso también deben desactivarse dichos códigos.

c) Se debe mantener el registro de acceso del personal autorizado y de ingresos con el objeto de facilitar procesos de investigación.

d) Como mecanismo de prevención todos los empleados y visitantes no deben comer, fumar o beber en el DataCenter o en instalaciones con equipos tecnológicos. Al hacerlo estarían exponiendo los equipos a daños eléctricos como a riesgos de contaminación sobre los dispositivos de almacenamiento.

e) Las reuniones de trabajo donde se discute y maneja información sensible, se deben realizar en salas cerradas para que personas ajenas a ella no tengan acceso.

f) Todos los sistemas de control de acceso deben ser monitoreados permanentemente.

Equipos y otros recursos

a) Toda sede y equipo informático ya sean propios o de terceros, que procesen información para UNITEK o posean un vínculo especial con la misma, debe cumplir con todas las normas de seguridad física que se emitan, con el fin de evitar el acceso a personas no autorizadas a las áreas restringidas donde se procese o mantenga información secreta, confidencial y privada, y asegurar la protección de los recursos de la plataforma tecnológica y su información.

b) Los equipos computacionales no deben moverse o reubicarse sin la aprobación previa del Administrador del área involucrada.

c) Todos los equipos de propiedad de UNITEK no deben retirarse de las instalaciones físicas por ningún personal, a menos que esté previamente autorizado.

d) No se debe proveer información sobre la ubicación del DataCenter o de los lugares críticos, como mecanismo de seguridad.

Protección física de la información

a) Todas las personas que trabajen para la entidad y/o aquellas designadas por las entidades para trabajar en actividades particulares (consultores y contratistas) son responsables del adecuado uso de la información suministrada para tal fin, por lo cual se debe velar por su integridad, confidencialidad, disponibilidad y auditabilidad. Toda información secreta, confidencial y privada debe estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

b) Al terminar la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de UNITEK. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

c) Las áreas donde se maneja información confidencial o crítica deben contar con cámaras que registren las actividades realizadas por los funcionarios.

Protección contra desastres

a) Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre puede afectar el nivel de servicio y la figura de UNITEK, se deba prever que los equipos de procesamiento y comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.

Planes de emergencia, contingencia y recuperación

a) Es responsabilidad de la administración de UNITEK el preparar, actualizar periódicamente y regularmente probar los planes de Contingencias, Emergencias y Recuperación previendo la continuidad de los procesos críticos para el negocio en el evento de presentarse una interrupción o degradación del servicio.

b) La Administración debe establecer, mantener y probar periódicamente el sistema de comunicación que permita a los usuarios de la plataforma tecnológica notificar posibles intromisiones a los sistemas de seguridad, estos incluyen posibles infecciones por virus, intromisión de hackers, divulgación de información no autorizada y debilidades del sistema de seguridad.

c) El Plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento de la presencia de un desastre, permitiendo que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos de negocio, en un tiempo razonable para cada caso y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad.

4.4 El mantenimiento del plan de Contingencias y Recuperación general debe incluir entre otros un proceso estándar que integre los planes de contingencia para computadores y comunicaciones, así como también el inventario de hardware, software existente y los procesos que correrán manualmente por un período de tiempo.

ANEXO B6: POLITICA DE ADMINISTRACION DE ACCESO A INTERNET

Generalidades

a) El área de Informática debe definir, implementar, controlar Y mantener las políticas, normas, estándares, procedimientos, funciones y responsabilidades necesarias para preservar y proteger la confidencialidad, disponibilidad, integridad y acceso de la información de UNITEK donde ésta

resida (aplicaciones, bases de datos, sistemas operativos, redes, backups y medios).

b) El área de Informática es la encargada de establecer, mantener y administrar una arquitectura de acceso para UNITEK y facilitar la incorporación de prácticas de acceso a la información en todas las dependencias.

c) El área de Informática debe estar ubicada organizacionalmente de manera que tenga autonomía e independencia frente a las demás áreas de tecnología tales como soporte, diseño y desarrollo, entre otras.

Funciones de Control

a) El personal administrativo no está permitido ingresar a páginas web de ocio, por ejemplo; Facebook, twitter, YouTube, y más idénticas a la anterior descritas. Para lograr una atención preferencial hacia los alumnos o visitantes a la UNITEK.

b) Los estudiantes no están permitidos ingresar a páginas web de ocio por ejemplo; Facebook, twitter, YouTube, y más idénticas a la anterior descritas. Con fines de estudio, tratamos de evitar distracciones en el momento de aprendizaje de estudiantes.

c) Viendo los puntos anteriores todos, incluyendo personal administrativo y estudiantes pueden ingresar a páginas de investigaciones o blogs educativos.

d) El área de informática realizara el boqueo de estas páginas web, usando programas, softwares, servidores y/o cortafuegos.

e) El único personal autorizado para ingresar a todas las páginas web es la secretaria y la recepción.